

# **ESCUELA POLITÉCNICA NACIONAL**

## **ESCUELA DE INGENIERÍA**

**“DISEÑO DE UNA RED INTEGRADA PARA VOZ Y DATOS  
UTILIZANDO TELEFONÍA IP Y LA RED DE DATOS DEL GRUPO  
ITABSA”**

**PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN  
ELECTRÓNICA Y REDES DE INFORMACIÓN**

**CATALINA IVANOVA AVILÉS BURBANO**

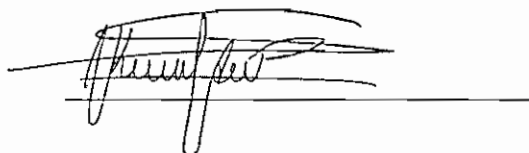
**DIRECTOR: ING. PABLO HIDALGO**

**QUITO, SEPTIEMBRE 2005**

## DECLARACIÓN

Yo, Catalina Ivanova Avilés Burbano, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

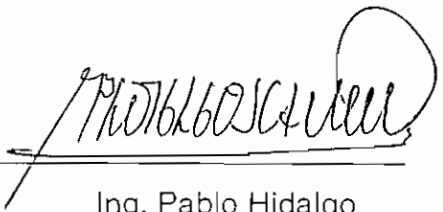
A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

A handwritten signature in black ink, appearing to read 'Catalina Avilés Burbano', is written over a horizontal line. The signature is stylized and cursive.

Catalina Ivanova Avilés Burbano

## CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por la señorita Catalina Ivanova Avilés Burbano, bajo mi supervisión.

A handwritten signature in black ink, appearing to read 'Pablo Hidalgo', is written over a horizontal line. The signature is stylized and cursive.

Ing. Pablo Hidalgo  
DIRECTOR DE PROYECTO

## **AGRADECIMIENTO**

A Dios por todas las oportunidades y cosas buenas que ha puesto en mi vida.

Al Ing. Pablo Hidaigo por su acertada colaboración en la dirección de este Proyecto.

Al Grupo ITABSA por su colaboración en la realización de este proyecto de titulación.

A mis padres y hermanas por su apoyo en el transcurso de mi carrera y todo el cariño que me brindan.

# ÍNDICE GENERAL

DECLARACIÓN.....	II
CERTIFICACIÓN.....	III
ÍNDICE GENERAL .....	VI
ÍNDICE DE TABLAS.....	X
ÍNDICE DE FIGURAS.....	XI
RESUMEN.....	XIV
PRESENTACIÓN .....	XV
<b>CAPÍTULO 1 .....</b>	<b>1</b>
<b>FUNDAMENTOS DE TELEFONÍA IP .....</b>	<b>1</b>
1.1 ARQUITECTURAS COMBINADAS.....	2
1.1.1 SEÑALIZACIÓN .....	5
1.1.1.1 Elementos de Señalización.....	6
1.1.1.2 Capas del Protocolo SS7 .....	9
1.1.2 SITUACIÓN DE LA TELEFONÍA.....	12
1.2 VoIP vs. TELEFONÍA IP .....	15
1.3 DESCRIPCIÓN DE LA TECNOLOGÍA DE TELEFONÍA IP .....	19
1.3.1 MODELO DE REFERENCIA OSI.....	20
1.3.2 <i>STACK</i> DE PROTOCOLOS DE TELEFONÍA IP .....	22
1.3.3 EL PROTOCOLO INTERNET .....	24
1.3.4 TCP/IP .....	26
1.3.5 LIMITACIONES TECNOLÓGICAS DE VoIP .....	28
1.3.5.1 Retraso y Latencia .....	28
1.3.5.2 Fluctuación de Fase.....	30
1.4 COMPONENTES DE UN SISTEMA DE TELEFONÍA IP .....	31
1.5 TELEFONÍA IP INALÁMBRICA.....	32
1.5.1 AMENAZAS EN REDES WLAN .....	34
1.5.1.1 Escuchas Ilegales .....	35
1.5.1.2 Acceso No Autorizado.....	35
1.5.1.3 Interferencias Aleatorias e Intencionadas .....	36

1.5.1.4 Amenazas físicas .....	36
1.5.2 SEGURIDAD EN REDES WLAN.....	37
1.5.2.1 Cifrado WEP .....	38
1.5.2.2 Autenticación WEP .....	39
1.5.2.3 Autenticación ESSID.....	40
1.6 PROTOCOLOS Y ESTÁNDARES .....	40
1.6.1 ESTÁNDAR H.323.....	40
1.6.1.1 Elementos H.323 .....	41
1.6.1.2 Stack de protocolos H.323.....	50
1.6.1.2.1 Señalización RAS .....	52
1.6.2 ESTÁNDAR SIP .....	56
1.6.2.1 Componentes del Sistema SIP .....	58
1.6.2.2 Direccionamiento.....	59
1.6.2.3 Mensajes SIP .....	59
1.6.2.4 Operatividad de SIP.....	63
1.6.2.5 Stack de Protocolos SIP .....	64
1.7 CALIDAD DE SERVICIO.....	66
1.7.1 LIMITACIONES DE ANCHO DE BANDA .....	67
1.7.2 GESTIÓN DE COLAS .....	68
1.7.2.1 Gestión de Colas Apropiada Ponderada.....	69
1.7.2.2 Gestión de Colas Personalizada.....	69
1.7.2.3 Gestión de Colas por Prioridad .....	70
1.7.2.4 Otros Métodos de Gestión de Colas .....	70
1.7.3 POLÍTICAS DE ENRUTAMIENTO .....	71
1.7.4 CONSIDERACIONES ADICIONALES.....	71

<b>CAPÍTULO 2 .....</b>	<b>73</b>
<b>DISEÑO DE LA RED CONVERGENTE PARA TELEFONÍA IP PARA EL</b>	
<b>GRUPO ITABSA .....</b>	<b>73</b>
2.1 ESTADO ACTUAL DE LA RED .....	73
2.2 ALTERNATIVAS TECNOLÓGICAS.....	81
2.2.1 ALTERNATIVAS DE IMPLEMENTACIÓN DE VoIP .....	82
2.2.2 ALTERNATIVAS DE EQUIPO DE TELEFONÍA IP.....	84

2.2.2.1	Equipos para Telefonía IP Cisco.....	85
2.2.2.2	Equipos para Telefonía IP Siemens.....	98
2.2.3	ANÁLISIS COMPARATIVO DE ALTERNATIVAS PRESENTADAS DE EQUIPO DE TELEFONÍA IP.....	104
2.3	CONSIDERACIONES DE DISEÑO .....	106
2.3.1	MODELO DE CAPAS.....	107
2.3.2	<i>SPANNING TREE PROTOCOL</i> .....	107
2.3.3	VTP ( <i>VLAN TRUNK PROTOCOL</i> ) .....	109
2.3.4	<i>SWITCHES</i> DE ACCESO .....	110
2.3.5	<i>SWITCHES</i> DE DISTRIBUCIÓN.....	114
2.3.6	<i>SWITCHES</i> DE <i>CORE</i> .....	115
2.4	PROPUESTA DE DISEÑO.....	116
2.4.1	CONMUTACIÓN DE LLAMADAS .....	119
2.4.2	MENSAJERÍA UNIFICADA .....	120
2.4.3	EQUIPO QUE INTERACTÚA CON EL USUARIO .....	121
2.4.4	<i>VOICE GATEWAY</i> .....	121
2.4.5	<i>SWITCH</i> CENTRAL .....	122
2.4.6	SOFTWARE DE ADMINISTRACIÓN: <i>CISCO WORKS</i> .....	124
2.4.7	<i>ROUTERS</i> REMOTOS.....	124
2.4.8	ESQUEMA DE LA PROPUESTA DE DISEÑO .....	126
2.4.9	<i>IP PLANNING</i> .....	129
2.5	ANÁLISIS DE EQUIPO ESPECÍFICO DISPONIBLE EN EL MERCADO .....	130
2.5.1	<i>CISCO CALL MANAGER 4.1</i> .....	131
2.5.2	<i>CISCO UNITY 4.0</i> .....	133
2.5.3	TELÉFONOS IP, <i>SOFTPHONES</i> Y <i>ATAs</i> .....	134
2.5.4	<i>ROUTERS</i> .....	136
2.5.5	<i>SWITCH</i> <i>CISCO CATALYST 4507</i> .....	136
2.5.6	<i>CISCO WORKS SNMS</i> .....	137
2.6	CRONOGRAMA DE ACTIVIDADES .....	137
2.7	ANÁLISIS DE COSTOS .....	139

<b>CAPÍTULO 3</b> .....	142
<b>PLANIFICACIÓN DE USO DE TELEFONÍA IP INALÁMBRICA</b> .....	142
3.1 CONSIDERACIONES .....	142
3.1.1 INFRAESTRUCTURA PARA TELEFONÍA IP INALÁMBRICA .....	143
3.1.2 REQUERIMIENTOS DE RADIO FRECUENCIA .....	146
3.1.3 SEGURIDAD .....	150
3.1.4 CALIDAD DE SERVICIO (QoS) .....	151
3.2 PROPUESTA DE DISEÑO DE LA RED .....	154
3.2.1 ACCESS POINT .....	156
3.2.2 TELÉFONOS IP INALÁMBRICOS .....	169
3.2.3 ESQUEMA DE LA PROPUESTA DE DISEÑO .....	170
3.3 COSTO TOTAL INICIAL DEL PROYECTO .....	175
3.4 ANÁLISIS DE EQUIPO ESPECÍFICO DISPONIBLE EN EL MERCADO .....	175
3.4.1 CISCO AIRONET 1200 SERIES ACCESS POINT .....	176
3.4.2 CISCO WIRELESS IP PHONE 7920 .....	177
 <b>CAPÍTULO 4</b> .....	 180
<b>CONCLUSIONES Y RECOMENDACIONES</b> .....	180
4.1 CONCLUSIONES .....	180
4.2 RECOMENDACIONES .....	183
 <b>REFERENCIAS</b> .....	 185
<b>ANEXOS</b>	
A.1 Datasheets del equipo propuesto de Telefonía IP	
A.2 Datasheets del equipo propuesto de Telefonía IP inalámbrica	



## ÍNDICE DE TABLAS

Tabla 1.1 Cabeceras SIP.....	61
Tabla 1.2 Retraso previsto de extremo a extremo .....	66
Tabla 1.3 Comparación de ancho de banda .....	67
Tabla 2.1 IP <i>Planning</i> . .....	129
Tabla 2.2 Direcciones IP fijas. ....	129
Tabla 2.3 Cuadro de Costos de Equipos Cisco. ....	139
Tabla 2.4 Cuadro de Costos de Honorarios Profesionales.....	140
Tabla 2.5 Cuadro de Costos de Enlaces. ....	141
Tabla 3.1 Atenuación de la señal causada por varios tipos de objetos . ....	149
Tabla 3.2 Cisco Aironet <i>Access Point</i> para diferentes ambientes.....	160
Tabla 3.3 Características Cisco Aironet <i>Access Points</i> . ....	160
Tabla 3.4 IP <i>Planning</i> WLAN.....	160
Tabla 3.5 Cuadro de Costos de Equipo para Telefonía IP Inalámbrica. ....	174
Tabla 3.6 Costo total inicial del proyecto. ....	175

## ÍNDICE DE FIGURAS

Figura 1.1 Distorsión de línea analógica .....	3
Figura 1.2 Distorsión de línea digital .....	3
Figura 1.3 Elementos de señalización SS7 .....	7
Figura 1.4 Pila de protocolos SS7 frente al modelo OSI .....	10
Figura 1.5 Elementos de señalización de una red VoIP .....	12
Figura 1.6 Ejemplo de una red de arquitecturas combinadas .....	13
Figura 1.7 Redes convergentes .....	14
Figura 1.8 Pila de protocolos de Telefonía IP .....	23
Figura 1.9 Formatos de dirección IP .....	25
Figura 1.10 Cabecera TCP .....	27
Figura 1.11 Ejemplo de <i>Jitter</i> .....	30
Figura 1.12 Componentes de la red de Telefonía IP .....	31
Figura 1.13 Elementos de red H.323 .....	42
Figura 1.14 Terminal H.323 .....	43
Figura 1.15 Elementos de un Gateway H.323 .....	45
Figura 1.16 Modelo de señalización directa .....	48
Figura 1.17 Modelo GK RCS .....	49
Figura 1.18 Capas del conjunto de protocolos H.323 .....	51
Figura 2.1 Red de datos grupo ITABSA .....	76
Figura 2.2 Infraestructura tecnológica de datos del grupo ITABSA .....	76
Figura 2.3 Enlace internacional .....	77
Figura 2.4 Infraestructura LAN ITABSA .....	78
Figura 2.5 Infraestructura LAN TANASA .....	80
Figura 2.6 Cisco IP Phone 7912G .....	89
Figura 2.7 Cisco IP Phone 7940G .....	90
Figura 2.8 Cisco IP Phone 7960G .....	92
Figura 2.9 Botones de acceso directo .....	93
Figura 2.10 Cisco IP Phone 7960G con módulo añadido .....	94
Figura 2.11 Cisco IP Conference Station 7936 .....	95
Figura 2.12 Cisco IP Communicator .....	96

Figura 2.13 Cisco ATA 186.....	98
Figura 2.14 Servidor Siemens Primergy RX100 S2.....	99
Figura 2.15 Siemens Opticlient .....	101
Figura 2.16 Siemens Optipoint 420. ....	102
Figura 2.17 Siemens Optipoint 600 . ....	103
Figura 2.18 <i>Switch</i> de distribución . ....	114
Figura 2.19 Arquitectura de telefonía IP. ....	117
Figura 2.20 Esquema de la propuesta de diseño de telefonía IP. ....	128
Figura 2.21 Cronograma de Actividades . ....	138
Figura 3.1 Superposición de canales en celdas inalámbricas de <i>access points</i> .....	147
Figura 3.2 Distorsión causada en la señal por mala ubicación de un <i>access point</i> .....	147
Figura 3.3 Ubicación correcta de un <i>access point</i> . ....	148
Figura 3.4 Relación señal a ruido . ....	149
Figura 3.5 Modelo DCF y EDCF . ....	153
Figura 3.6 Infraestructura telefonía IP inalámbrica. ....	156
Figura 3.7 VLANs en la red inalámbrica . ....	159
Figura 3.8 Configuración de parámetros de red en IOS Cisco 1200 <i>Access Point</i> . ....	161
Figura 3.9 Configuración de interfaz de red en IOS Cisco 1200 <i>Access Point</i> . ..	162
Figura 3.10 Configuración de interfaz de red en IOS Cisco 1200 <i>Access Point</i> . ..	163
Figura 3.11 Configuración de accesos de administrador en IOS Cisco 1200 <i>Access Point</i> . ....	164
Figura 3.12 Configuración de características de seguridad en IOS Cisco 1200 <i>Access Point</i> . ....	165
Figura 3.13 Configuración de método de encriptación en IOS Cisco 1200 <i>Access Point</i> . ....	166
Figura 3.14 Configuración de RADIUS <i>Server</i> en IOS Cisco 1200 <i>Access Point</i> .....	166
Figura 3.15 Configuración de seguridad avanzada en IOS Cisco 1200 <i>Access Point</i> . ....	167
Figura 3.16 Configuración Telnet/SSH en IOS Cisco 1200 <i>Access Point</i> .....	167

Figura 3.17 Configuración DNS en IOS Cisco 1200 <i>Access Point</i> .....	168
Figura 3.18 Configuración de HTTP en IOS Cisco 1200 <i>Access Point</i> .....	168
Figura 3.19 Configuración de VLANs en IOS Cisco 1200 <i>Access Point</i> .....	168
Figura 3.20 Configuración de SNMP en IOS Cisco 1200 <i>Access Point</i> .....	169
Figura 3.21 Esquema de la propuesta de diseño de telefonía IP Inalámbrica. ....	173
Figura 3.22 Cisco Aironet 1200 <i>Access Point</i> .....	176
Figura 3.23 Cisco Wireless IP Phone 7920 . .....	178

## RESUMEN

Este proyecto de titulación tiene como propósito realizar el diseño de una red convergente de voz y datos sobre la red de datos que actualmente posee el grupo ITABSA. La consolidación de ambas redes ayudará a mejorar la administración de la red y por lo tanto permitirá un desempeño más eficiente del área de IT (*Information Technologies*) y del grupo corporativo en general.

Es un trabajo desarrollado en cuatro capítulos. En el primer capítulo se revisan los conceptos básicos de la telefonía IP, así como protocolos y estándares que regulan esta tecnología. Además se realiza un estudio de las características de calidad de servicio que debe tener una red sobre la que se transmite tanto información de voz como de datos.

En el segundo y tercer capítulo se concentra el diseño de la red convergente de voz y datos para el Grupo ITABSA. Aquí se revisan las características de la red actual y los cambios que debe sufrir esta red para soportar sobre sí misma la transmisión de voz, sin degenerar la calidad ni de los servicios ni de voz ni de datos. Se recomienda el equipo a utilizarse detallando las características de los mismos. También se presentan esquemáticos de la topología lógica final que poseerá la red.

Este trabajo finaliza con las conclusiones y recomendaciones realizadas con el fin de obtener mejores resultados en futuras aplicaciones. En los anexos se presentan los catálogos de características técnicas del equipo sugerido en este proyecto.

# CAPÍTULO 1

## FUNDAMENTOS DE TELEFONÍA IP

En la actualidad, la influencia del acelerado avance de la tecnología ha hecho que se busque formas de facilitar la labor diaria ganando eficiencia y calidad. Es usual e incluso necesario que las compañías estén provistas de redes de datos para su funcionamiento habitual. El desarrollo en este campo impulsa cada día hacia la convergencia de las redes que se utilizan, unificando en una sola red servicios de datos, voz y multimedia. Voz sobre IP (*Internet Protocol*) es una tecnología que permite concentrar varias aplicaciones en una sola red; es decir permite converger en una sola red los servicios de datos, voz y multimedia.

Voz sobre IP es una forma de telecomunicaciones que admite la transmisión de voz y datos sobre una amplia variedad de redes. El uso de esta tecnología es cada vez más frecuente a nivel corporativo ya que permite la comunicación entre varias subsidiarias de una misma compañía sin necesidad de usar la PSTN (*Public Switched Telephone Network*), utilizando la Intranet ya implementada para la transmisión de voz y datos. Esto incluso representa una reducción en los costos de operación ya que no se está utilizando la red pública, sobre todo se tiene ventaja al momento de comunicarse a nivel internacional ya que estas tarifas siempre son elevadas.

Las tecnologías basadas en VoIP tienen varias ventajas, actualmente una de las más importantes es la disminución de los costos en planillas telefónicas, pero además se ofrece valores agregados que con la telefonía tradicional no se logra. Para el usuario es más útil porque desde su computador o cualquier equipo con acceso a la LAN empresarial podría acceder a los servicios tradicionales de telefonía y a los agregados como buzón de voz o servicios de mensajería.

Pero no todo es tan sencillo como parece, ya que es necesario preocuparse de algunos aspectos adicionales como la calidad de voz, los retrasos en las

transmisiones y las prioridades que se deben aplicar para cumplir con la QoS (*Quality of Service*). El gran avance que posee esta tecnología asegura que en un futuro no muy lejano, ésta será una de las tecnologías más usadas, no sólo a nivel corporativo, sino también a nivel de comunicaciones personales.

La telefonía IP utiliza las ventajas que ofrece la transmisión de voz sobre IP para implementar un sistema con mejores características que los sistemas telefónicos tradicionales. La telefonía tradicional se fundamenta en la conmutación de circuitos; en cambio, la telefonía IP utiliza la conmutación de paquetes. Estos paquetes al estar digitalizados son aptos para la transmisión sobre redes de datos, y a estos paquetes se les puede agregar cabeceras que permitan manejar prioridades logrando un servicio de telefonía eficaz. Algo que se debe tomar en cuenta es que al convivir tanto voz como datos sobre la misma red, no se puede degradar la calidad de servicio de ninguno de ellos. Ésta es la razón por la cual el control que se debe tener sobre la red es primordial.

El presente proyecto de titulación se basa en el diseño de un sistema de telefonía IP para un grupo corporativo afiliado a una multinacional de fabricación y comercialización de productos de consumo masivo. Se realizará el diseño para la implementación del servicio de Telefonía IP tanto en el edificio donde se encuentran las oficinas, ubicado en el norte de la ciudad, como en la planta de producción que se encuentra al sur de Quito.

## 1.1 ARQUITECTURAS COMBINADAS

La voz humana tiene una forma analógica por lo que las redes telefónicas que la transportaban en un inicio y hasta hace algunos años se basaban en una infraestructura analógica. El problema que generaba este tipo de infraestructura era básicamente el hecho de que cuando se amplificaba o se regeneraba la señal para la transmisión, el ruido de línea también se amplificaba. Esto producía una degradación en la calidad de la señal y por lo tanto un servicio pobre.

Las señales analógicas que reciben el ruido de línea pueden distorsionar la forma de onda analógica y producir una recepción desvirtuada (figura 1.1). En el caso de una señal analógica, el amplificador no “limpia” la señal que amplifica, solo amplifica la señal que recibe, la cual puede estar distorsionada, generando ruido acumulado.

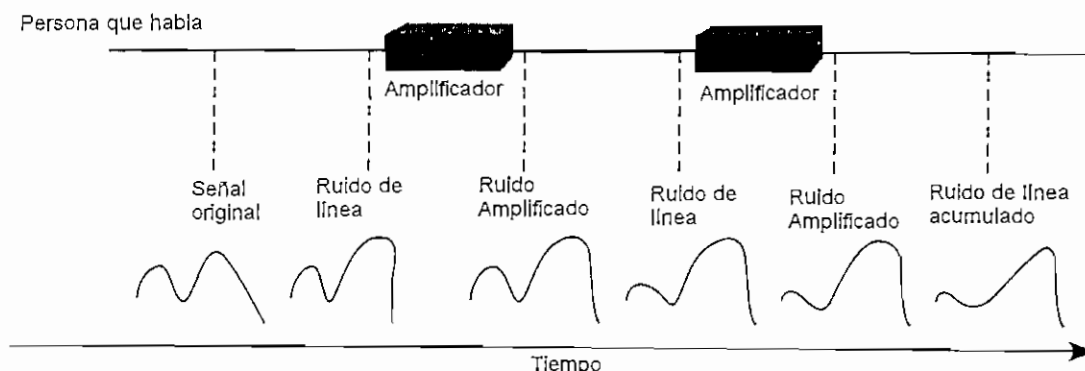


Figura 1.1 Distorsión de línea analógica [1].

En redes digitales se puede solucionar este problema porque los repetidores tienen la capacidad de, además de amplificar la señal, “limpiarla” y regresarla a su condición original. Esto es posible gracias a que las señales están compuestas de unos y ceros lo cual facilita reestablecer la señal a su estado original (figura 1.2). De esta manera, a pesar de que la señal pase por varios repetidores se puede mantener un sonido “limpio”. Por esta razón la telefonía migró a la modulación por impulsos codificados (PCM), que es la forma en la que en la actualidad trabaja la PSTN.

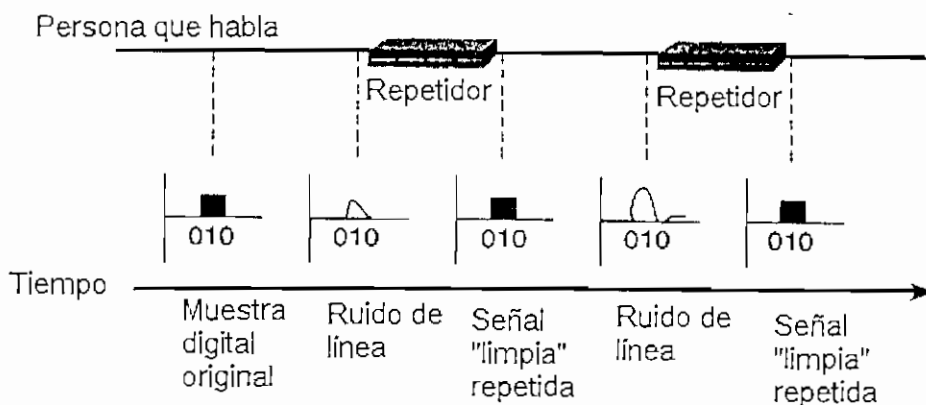


Figura 1.2 Distorsión de línea digital [2].



PCM (*Pulse Code Modulation*) utiliza el teorema de Nyquist. Este teorema indica que si se muestrea la señal de voz al doble de su frecuencia más alta se consigue una transmisión de buena calidad.

El primer paso del proceso PCM es pasar la señal analógica por un filtro de frecuencia de voz para filtrar cualquier señal que sea mayor a 4 KHz. Aplicando Nyquist, se necesita muestrear 8000 veces por segundo para obtener una transmisión de voz de buena calidad. Cada una de estas muestras es representada por un código digital que indica la amplitud de la forma de onda en el instante en que se tomó la muestra. PCM utiliza ocho bits para esta codificación.

Por lo tanto se tiene palabras de ocho bits, 8000 veces por segundo, lo que da un total de 64 kbps, valor base para la infraestructura de telefonía digital.

La PSTN fue construida para la conmutación de llamadas de voz; cuando éste era su único objetivo era muy eficiente, pero actualmente los datos han ganado espacio de tal manera que la transmisión de datos es una aplicación muy necesaria. Los datos tienen diferentes características de las que tiene la transmisión de voz como por ejemplo la utilización variable del ancho de banda y además un ancho de banda superior.

Debido a que las redes de voz no están en la capacidad de transmitir datos a la medida de la demanda requerida, la tendencia es que el tráfico de voz circule dentro de las redes construidas para datos. La voz se transmitirá sobre redes de conmutación de paquetes de la misma manera que lo hacen los datos.

El uso de una red de voz independiente de una red de datos resulta caro y hasta innecesario, por esta razón se ha incrementado el uso de telefonía IP para ofrecer servicios de voz sobre una red IP existente para datos. Ésta es la convergencia de la red de datos con la red de voz.

Las redes de datos poseen una infraestructura más abierta que la que posee la PSTN, esto ha hecho que muchos fabricantes se interesen en el desarrollo y en proporcionar aplicaciones que le dan más versatilidad a estas redes. Con la arquitectura actual de la PSTN no es posible un mayor desarrollo en el sentido de aplicaciones creadas para ella. Ya que la arquitectura de la PSTN fue construida para voz no es lo suficientemente fuerte para soportar la transmisión de datos con las características que la actualidad exige.

### 1.1.1 SEÑALIZACIÓN

La telefonía por conmutación de circuitos utiliza el método de señalización fuera de banda SS7 (Sistema de Señalización 7, también llamado C7 en países europeos). SS7 es un método de envío de mensajes entre *switches* (conmutadores). La señalización SS7 da soporte a la PSTN manejando el establecimiento de la llamada, el intercambio de información, el enrutamiento, las operaciones, la facturación y el soporte para servicios de red inteligente.

El protocolo SS7 es importante en voz sobre IP por la manera en que interactúa con la PSTN. Este *internetworking* es crítico para la aceptación y el éxito de las soluciones de voz sobre IP en las redes telefónicas actuales. SS7 provee un protocolo común para señalización, envío de mensajes entre redes y esto proporciona una interfaz para la que se pueden desarrollar dispositivos VoIP. Es un estándar global para telecomunicaciones definido por la ITU-T. Este protocolo esencialmente se utiliza para establecer, controlar y enrutar una llamada.

El sistema de señalización 7 puede encargarse de varias tareas como:

- Establecimiento, mantenimiento y finalización de llamadas.
- Servicios inalámbricos como PCS (*Personal Communications Services*)
- Autenticación de suscriptores móviles
- Servicios de llamada gratuita (1-800) o llamada con costo adicional (1-900)
- Servicios avanzados como desvío de llamadas, identificación de llamada, conferencias.

SS7 constituye una red de señalización de canal común porque toda la información de señalización se transporta separada de la información de voz. El plano de señalización y el de voz se encuentran separados lógicamente.

Los mensajes SS7 se intercambian entre los elementos de la red a través de canales bidireccionales de 56 o 64 Kbps, estos canales se los llama enlaces de señalización. El tener la señalización en planos diferentes, es decir, fuera de la banda de comunicación, proporciona varias ventajas:

- Rapidez en el establecimiento de llamadas
- Eficiencia en el uso de los circuitos
- Control integrado contra uso fraudulento de la red

#### 1.1.1.1 Elementos de Señalización

También llamados puntos de señalización [1], son los encargados de separar la red de voz de la red de señalización (figura 1.3). Cada uno de estos elementos es identificado como único mediante un código numérico de punto que es un código con el que se identifica cada uno de los elementos de señalización. Estos códigos son llevados a mensajes de señalización que contienen la dirección del código de punto de origen y de destino. Cada uno de estos puntos de señalización utiliza una tabla de enrutamiento para seleccionar el camino de señalización apropiado para cada mensaje. Los elementos de señalización son tres [9]:

- SSP (Service Switching Point): Es el punto de conmutación de servicio; estos puntos son oficinas centrales o *switches* tándem, es decir para comunicación entre centrales. Se encargan de conectar circuitos de voz y su función dentro de la señalización es el originar, trasladar y finalizar llamadas.

Los SSP son centrales que proveen mensajes de señalización que permiten conectar, desconectar y administrar las llamadas de voz. También puede enviar un requerimiento de información a una base de datos centralizada SCP para determinar cómo enrutar una llamada.

El SSP utiliza su tabla de enrutamiento para determinar los pasos a seguir para conectar la llamada. Cuando se ha localizado el destino, se envía un mensaje de señalización SS7 pidiendo una conexión con este circuito. El SSP destino otorga el acceso y responde con un acuse de recibo conectando la llamada con el destino final.

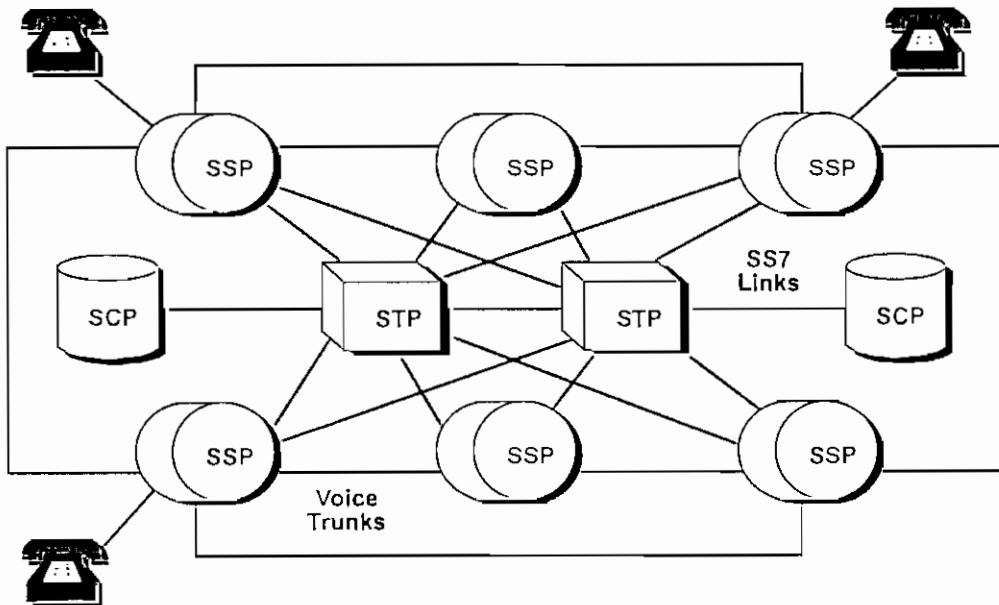


Figura 1.3 Elementos de señalización SS7 [3].

- STP (Signal Transfer Point): El punto de transferencia de señal, enruta todos los mensajes de señalización en la red SS7. Este elemento enruta el tráfico de red entre los puntos SSP, en realidad es un conmutador de paquetes pequeño. Dentro de la arquitectura SS7 es muy importante porque proporciona el acceso a la red. Los STP proporcionan mayor disponibilidad en la red.

Los STP también se utilizan para medir el tráfico y la utilización. La medición de tráfico brinda información sobre eventos de redes y tipos de mensajes. La medición de utilización proporciona información sobre acceso y número de mensajes.

La implementación STP tiene una jerarquía que es la siguiente:

- Punto de transferencia de señal local
- Punto de transferencia de señal regional
- Punto de transferencia de señal nacional
- Punto de transferencia de señal internacional
- Punto de transferencia de señal de *gateway*

Los puntos de transferencia local, regional y nacional transfieren los mensajes SS7 basados en estándares dentro de la misma red, sin conversión de formato de mensajes. Los STP internacionales están basados en estándares ITU. Los STP de *gateway* proporcionan protocolo de conversión entre los estándares utilizados, puntos de interconexión red a red y funciones de seguridad.

Un STP puede realizar la Traducción Global de Nombres que es un proceso en el cual el punto de señalización es identificado por medio de los dígitos presentes en el mensaje de señalización. Un nombre global es una dirección, por ejemplo un número 1-800 que es traducido en un código del punto de destino y un número de subsistema. El número de subsistema identifica únicamente una aplicación en el punto de señalización de destino.

La red SS7 es un elemento crítico en el procesamiento de llamadas, por lo que los puntos SCP y STP por lo general se diseñan en configuraciones de pares para poder prestar servicios de contingencia. El tráfico de la red se comparte entre todos los elementos de tal manera que si uno de los

enlaces falla, el tráfico puede ser re-enrutado a través de otro enlace. SS7 provee corrección y retransmisión de errores para lograr servicio continuo a pesar de que colapse alguno de los enlaces.

- SCP (Service Control Point): El punto de control de servicios es un elemento que proporciona acceso a las bases de datos para información adicional de enrutamiento que es necesario dentro del proceso de una llamada. SCP también es utilizado para aplicaciones de red inteligente.

Provee la interfaz de acceso a la base de datos donde se almacena la información adicional de enrutamiento e información relacionada con la aplicación para los mensajes no basados en circuitos.

El SCP utiliza el número de subsistema que es único para cada base de datos; la petición generada en la PSTN ya contiene este identificador y mediante éste el SCP puede responder a la petición.

#### 1.1.1.2 Capas del Protocolo SS7

Las funciones de hardware y software del protocolo SS7 están divididas en niveles, los cuales poco coinciden con el modelo OSI (*Open System Interconnection*). En la figura 1.4 se muestra una comparación de los dos modelos en la que se diferencia la cantidad de capas que tiene cada uno; el protocolo OSI es un modelo de siete capas y el SS7 tan solo tiene 4.

- Capa MTP (Message Transfer Protocol) Nivel 1: Define las características físicas, eléctricas y funcionales del enlace de señalización digital. A este nivel lo más común es utilizar E1 (2048 Kbps, 32 canales de 64 Kbps), T1 (1544 Kbps, 24 canales de 64 Kbps), V.35 (64 Kbps), DS-0 (64 Kbps) y DS-0A (56 Kbps).

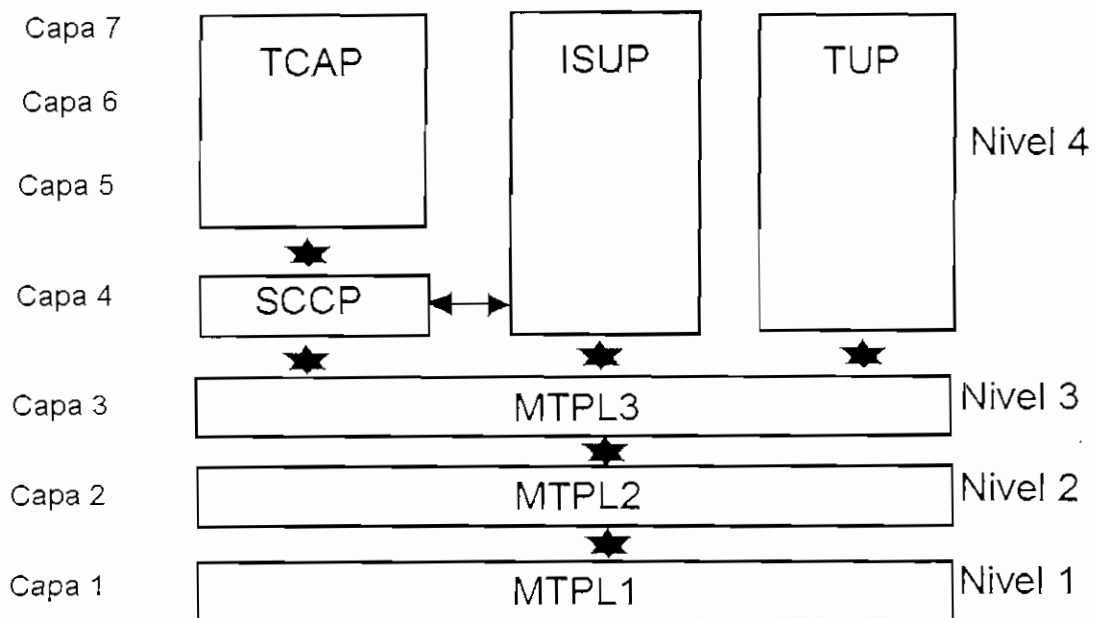


Figura 1.4 Pila de protocolos SS7 frente al modelo OSI [1].

- Capa MTP Nivel 2: Proporciona control de flujo, validación de la secuencia de mensajes, detección y corrección de errores, es decir, asegura la transmisión del mensaje.

Se crean enlaces punto a punto fiables entre los puntos finales en una red. Al ser punto a punto, no es de su alcance el garantizar el destino final del mensaje. Para detectar errores se utiliza CRC-16 (Código de Redundancia Cíclica de orden 16). En este nivel, cuando se detecta un error, se retransmite el mensaje.

Se sigue un control de la secuencia de los mensajes, si alguno se pierde MTP2 se encarga de solicitar la retransmisión de ese paquete. Además realiza un monitoreo de los enlaces para conocer su estado o si existen interrupciones en los procesos.

- Capa MTP Nivel 3 [11]: Esta capa se encarga del enrutamiento de mensajes entre los puntos de señalización SS7. Se encarga de enrutar los mensajes SS7 en condiciones normales, re-enrutar el tráfico de estos

mensajes cuando los enlaces han fallado, o controla el tráfico cuando existe congestión.

- Parte de Control de Conexión de Señalización (SCCP): Provee servicios de red en MTP3 orientado a conexión, no orientado a conexión y Traducción Global de Nombres.
- Parte de Usuario Telefónico (TUP): Fue la primera parte de usuario en definirse cuando las llamadas eran solamente de voz, por lo tanto solo maneja circuitos analógicos. Se la puede utilizar como soporte de establecimiento y corte básico de llamadas, aunque casi en su totalidad ha sido reemplazada por ISUP.
- Parte de Usuario de ISDN (ISUP): Este nivel define el protocolo usado para establecer, mantener y liberar las llamadas de voz y datos entre los usuarios llamante y llamado. ISUP se utiliza tanto en llamadas ISDN (*Integrated Service Digital Network*) y analógicas. Las llamadas que se originan y finalizan dentro de la misma central no utilizan este tipo de señalización.
- Parte de Aplicaciones con Capacidad de Transacción (TCAP): Soporta intercambio de datos no relacionados al circuito entre aplicaciones a través de la red SS7 usando servicio no orientado a conexión SCCP e invoca posibilidades de funciones remotas en elementos de la red. Los requerimientos y respuestas enviadas entre los SSP y los SCP se llevan a cabo en mensajes TCAP.

Con este tipo de señalización es posible tener mayor control y facilidades en los equipos de telefonía. Este protocolo se adapta sin problema a llamadas analógicas y a llamadas ISDN. Las nuevas tecnologías como VoIP han desarrollado *gateways* compatibles con esta tecnología para su interacción con la PSTN. Los elementos de señalización SS7 que se mencionaron se encuentran esquematizados en la figura 1.5.



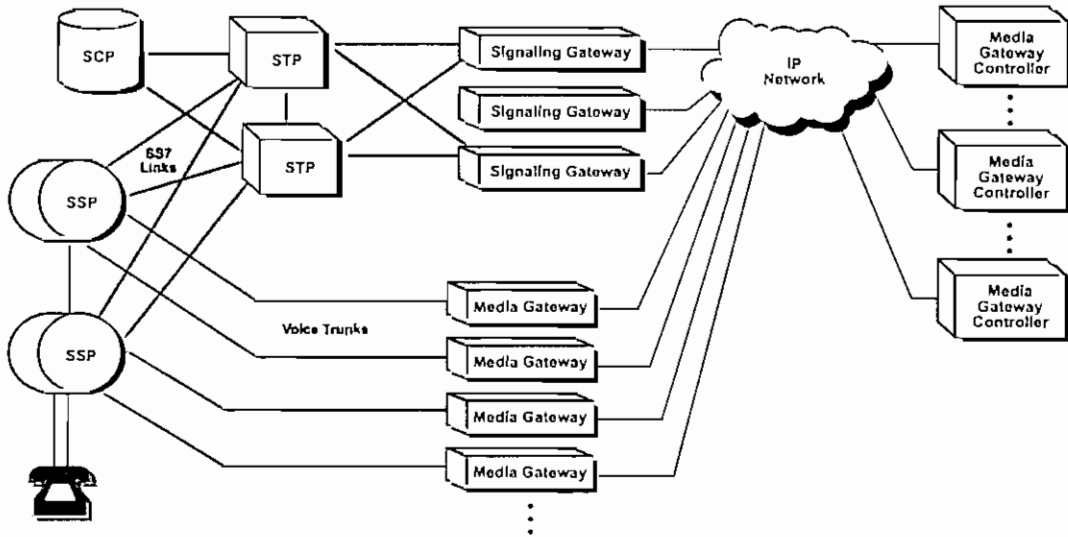


Figura 1.5 Elementos de señalización de una red VoIP [3].

### 1.1.2 SITUACIÓN DE LA TELEFONÍA

La infraestructura actual en la mayoría de lugares toma en cuenta el uso de redes independientes para comunicaciones telefónicas y para comunicaciones de datos. Con las nuevas tecnologías existentes en el mercado, esto resulta caro e innecesario, la solución de telefonía IP ofrece servicio de voz sobre la red de datos existente, enrutando las llamadas internas a través de la LAN corporativa en lugar de utilizar la PSTN o centrales telefónicas independientes para voz.

De esta manera se puede implementar de forma más eficiente el concepto de oficinas remotas u oficinas en casa utilizando la infraestructura de una red IP existente. Las llamadas a usuarios externos se siguen enrutando a través de la PSTN por lo que se requiere de arquitecturas combinadas (figura 1.6).

El teléfono y el computador han pasado de ser un simple instrumento de entretenimiento a verdaderos elementos indispensables para el correcto desarrollo de los empleados en una empresa, por más modesto que sea el puesto que desempeñen. Se puede apreciar que tanto el teléfono como el computador son indispensables para el trabajo del día a día. Si bien es cierto, hasta hace poco

no tenían ninguna relación, pero la convergencia hacia un único equipo integrado es ahora una realidad. Esto se ha conseguido debido a nuevas aplicaciones que aparecen a diario en el mercado y que las empresas las adquieren para aumentar su productividad.

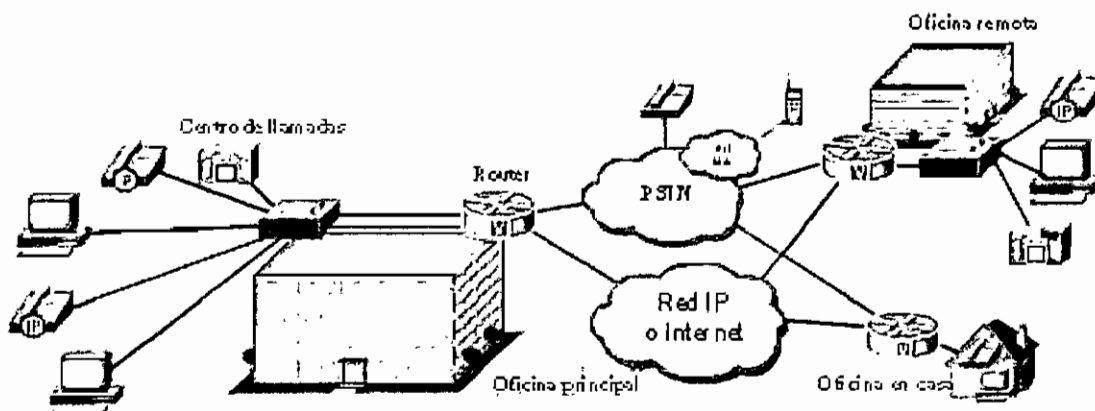


Figura 1.6 Ejemplo de una red de arquitecturas combinadas [8].

La telefonía tradicional no es muy amigable con el usuario, ya que para acceder a los servicios se requieren teléfonos sofisticados con multitud de códigos para poder hacer uso de los servicios. Ésta es la razón por la que el usuario común no utiliza estos servicios. Sin embargo, con la implementación de nuevas tecnologías como telefonía IP, se puede conseguir una interfaz mucho más amigable para el usuario y de mayor facilidad de utilización.

A pesar del desarrollo que ha tenido la telefonía, básicamente sigue siendo el mismo sistema que se poseía hace varios años. Las centrales han evolucionado y ahora son digitales y controladas por diversos programas, poseen aplicaciones pero en general, para el usuario, nada ha cambiado. Esto se debe a que la telefonía es básicamente enfocada a transmisión de voz, por lo que el soporte para datos es escaso.

En cambio, en el campo de los computadores es diferente, su evolución tecnológica es magnífica, las aplicaciones desarrolladas en este campo son cada vez mejores y todas ellas están encaminadas a facilitar el uso de estas herramientas sacando el mejor provecho de ellas.

Debido a esto, la integración entre la telefonía y la informática se presenta como una vía para conseguir aplicar todo el potencial del desarrollo de la informática en aplicaciones de voz, brindando la mayor facilidad al usuario final (figura 1.7).

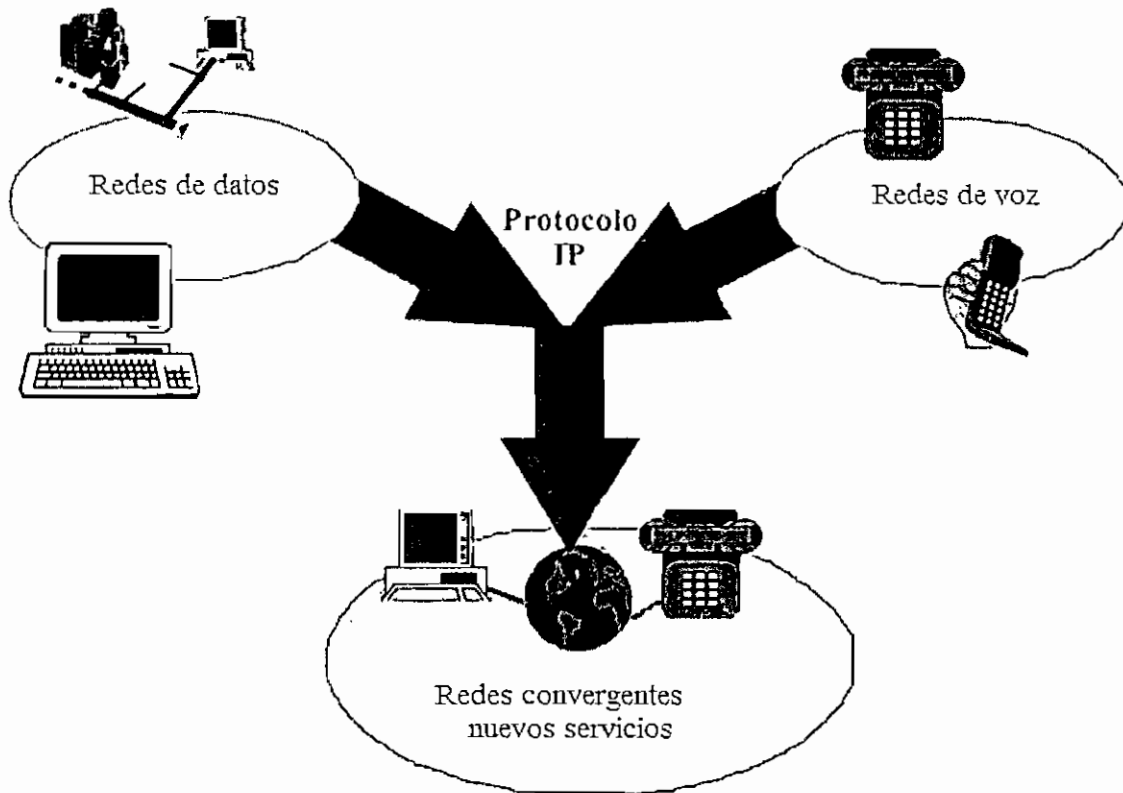


Figura 1.7 Redes convergentes [5].

La forma de enlace entre una red de telefonía IP y la PSTN es a través de la señalización. Esta información se intercambia a través de los siguientes elementos [5]:

- Gateway de medios: son los terminales de las llamadas de voz que provienen de los enlaces con la red pública de conmutación de circuitos. Se encargan de comprimir y paquetizar la voz, así como enviar los paquetes de voz comprimidos a la red IP. Para las llamadas originadas dentro de la red de telefonía IP el *gateway* de medios realiza el proceso inverso.

- Controlador de *gateway* de medios: un controlador de *gateway* de medios mantiene el registro y administración de los recursos del *gateway* de medios. También se lo llama *softswitch*.
- *Gateway* de señalización: provee una interacción transparente en la señalización entre la PSTN y la red IP. Este *gateway* se encarga de que la señalización SS7 sea traducida y pasada al controlador del *gateway*. Por su rol crítico en las redes integradas de voz los *gateways* de señalización siempre tienen un *gateway* de señalización para contingencia.

## 1.2 VoIP vs. TELEFONÍA IP [12]

La voz sobre IP inicialmente se implementó para reducir el ancho de banda mediante compresión vocal, aprovechando los procesos de compresión diseñados para sistemas celulares en la década de los años 80. Esto logró la reducción de costos en la telefonía a larga distancia. Luego tuvo aplicaciones en la red de servicios integrados sobre la LAN e Internet. Posteriormente la tecnología se fue desarrollando y sus aplicaciones ya no contemplaban solo la LAN, también incluían a la WAN. Por este crecimiento a esta tecnología ya se la consideraba un verdadero sistema de telefonía, llamado Telefonía IP.

En telefonía pública se pueden observar diferencias entre un operador local y otro de larga distancia. Cuando nos referimos a telefonía IP, nos ocupamos de la aplicación pública local. Existen varias características que hacen de la Telefonía-IP un problema de complejidad elevada respecto de la VoIP. Algunas de estas son la interoperatividad, la calidad de servicio y los servicios de valor agregado.

Una diferencia inicial entre VoIP y telefonía IP es la interoperatividad con las redes telefónicas actuales.

La calidad de servicio en telefonía IP está garantizada, mientras que en VoIP se piensa en el ámbito de interconexión mediante Internet sin calidad de servicio

asegurada. En telefonía IP se piensa en un *backbone* de alta velocidad para garantizar la calidad de servicio mediante herramientas de QoS. En telefonía IP se aplica conceptos de redundancia de equipamiento para lograr alta disponibilidad y calidad vocal garantizada.

La telefonía IP es una aplicación práctica del uso de la tecnología de voz sobre IP. VoIP se utiliza para gestionar el envío de información de voz de manera digitalizada en forma de paquetes. De esta manera los paquetes viajan sobre una red que utilice el protocolo IP de la misma forma que lo hacen el resto de paquetes de datos, pero permitiendo la diferenciación de estos paquetes para poder aplicar las prioridades que requiere la transmisión de voz.

Se debe tomar en cuenta que a nivel corporativo se utiliza en gran medida las comunicaciones de voz, los gastos generados por telefonía representan una parte fundamental de sus costes de funcionamiento. Con la voz sobre IP se ha abierto una nueva vía dentro de los parámetros de las comunicaciones de voz. Esta tecnología permite transportar llamadas telefónicas a través de la red de datos existente, reduciendo costos innecesarios que generan las redes exclusivas para voz.

La voz sobre IP es el protocolo sobre el cual se basa la telefonía IP para procesar el envío y recepción de llamadas entre sitios internos a una empresa o externos a ella.

Voz sobre IP significa transmitir la señal de voz no mediante un par de cables de cobre que es lo que la telefonía convencional hace, sino a través de una red de datos.

Actualmente, las redes son heterogéneas, es decir, como se puede transmitir a través de cable UTP, también se lo puede hacer mediante satélite, radio, o cualquier otro medio. Pero a pesar de esta heterogeneidad, la tendencia a utilizar el protocolo IP para transporte de información, ha ido creciendo. La transmisión

de voz no se ha quedado atrás. El protocolo H.323 es el aprobado por ITU para manejo de voz sobre IP y es el que se impone en el mercado.

Existían varias soluciones de VoIP en el mercado pero estas soluciones eran parciales y no cumplían a cabalidad con las necesidades y además no eran muy escalables. Para cubrir estos vacíos, se empezó a desarrollar la telefonía IP en la que se ofrecen servicios de voz, transportando sobre una sola red datos y voz. Sobre esta misma red se transporta la señalización.

La telefonía IP ofrece ventajas como plan de numeración particular, desvío de llamadas, restricciones de desvío al exterior, restricciones de llamadas entrantes y salientes, llamadas tripartitas, captura, transferencia y retención de llamadas, identificador de llamadas, extensiones de grupo, buzón de mensajes, registro de llamadas recibidas, enviadas y no contestadas, y muchos servicios más que se pueden personalizar de acuerdo a las necesidades de los usuarios. Además un teléfono IP permite tener servicios de datos como envío y recepción de correo desde el teléfono, navegación WAP (*Wireless Application Protocol*), y todos los servicios que puede prestar la red de datos.

La telefonía IP ha captado la atención de los proveedores de servicios en todo el mundo, ofreciendo una amplia gama de servicios nuevos y reduciendo al mismo tiempo sus costos de infraestructura. La telefonía IP es posible gracias al desarrollo de voz sobre IP, la cual ha cambiado la visión del acceso a la información, fusionando voz, datos, fax y funciones multimedia en una sola infraestructura de acceso convergente.

Haciendo uso de la telefonía IP, se pueden ofrecer servicios de voz básicos y ampliados a través de cualquier red IP. Cualquier servicio adicional se integrará de manera ininterrumpida a las redes conmutadas existentes, permitiendo que las llamadas se originen o terminen en teléfonos tradicionales de la PSTN cuando esto sea necesario. Dado que voz sobre IP es una norma abierta, la telefonía IP es flexible para personalizar los servicios existentes e implementar nuevos servicios con mayor rapidez y eficiencia en función de costos.

Para el éxito de la telefonía IP es necesario tomar en cuenta algunos problemas, ya que originalmente las redes fueron diseñadas para transportar solamente datos. Estos problemas que se deben tomar en cuenta se refieren a la capacidad de crecimiento y la escalabilidad de la red. Por lo menos, una red que va a proporcionar además de datos, el servicio de telefonía IP debe tener [5]:

- Calidad: La calidad de la comunicación debe ser al menos igual a la proporcionada por la telefonía tradicional. El retraso extremo a extremo tiene un impacto grande en la calidad percibida. Este retraso incluye el tiempo en el que el teléfono IP muestrea y codifica la voz, y la transforma en paquetes. También incluye el tiempo que se demora en transmitir estos paquetes a través de la red. Excesivo tiempo de retraso puede provocar varios problemas en ambientes de telefonía IP.
  - El eco de la voz es causado por reflexión de la señal de voz de los hablantes. Este problema también se puede presentar en redes de telefonía de conmutación de circuitos. Sin embargo, el eco se convierte en un mayor problema en la telefonía IP ya que puede generar un mayor retraso en estas redes. Las características de priorización deben ser usadas para controlar el retraso en las redes y así minimizar este problema.
  - La claridad de la voz también se ve impactada por el desempeño completo de la red IP. La pérdida de paquetes de voz o el retraso de los mismos puede causar un impacto negativo en la percepción de la claridad de la llamada. Los esquemas de digitalización y compresión usados para convertir las señales de voz en paquetes IP también son factores importantes en la claridad de la voz.
- Utilidad: La funcionalidad y facilidad de operación de la telefonía IP debe tener un nivel al menos igual al proporcionado por la telefonía por conmutación de circuitos. La red de telefonía IP debe tener planes de

marcación sencillos, el porcentaje de llamadas perdidas o no completadas debe ser bajo y el tiempo de acceso para realizar una llamada debe estar dentro de un nivel aceptable.

- Escalabilidad: Los sistemas de telefonía IP tienen el potencial de proveer alta calidad de servicios a un costo mucho menor del que ofrece la PSTN. Esto crea la posibilidad de altas tasas de crecimiento en estos servicios. Los sistemas de telefonía IP deben ser extensibles para soportar este crecimiento acelerado.
- Interoperabilidad e integración: Los ambientes de telefonía IP deben ser capaces de operar con productos similares de diferentes fabricantes. Estos equipos también deben trabajar simultáneamente con la actual PSTN. El hecho de que estén interactuando diferentes tipos de redes debe ser transparente para el usuario, es decir, deben aparecer como un solo ambiente para el usuario de estos servicios.

### 1.3 DESCRIPCIÓN DE LA TECNOLOGÍA DE TELEFONÍA IP

Si bien es cierto, la mayor ventaja que siempre se le ha atribuido a la telefonía IP sobre la telefonía tradicional son sus bajos costos de operación, existen más razones para pensar en implementar telefonía IP dentro de una red empresarial. El converger en una sola red datos y voz implica que la empresa puede disponer de menos circuitos de la PSTN sin que esto baje el nivel de servicio que se ofrece a los usuarios. Además el mismo hecho de eliminar la red independiente de voz ya representa una ventaja.

De la misma manera, una infraestructura bien elaborada con la utilización de teléfonos IP requiere menos añadidos, así como menos desplazamientos y cambios que los que implica una red tradicional de voz separada de una red de datos. Al tener una sola infraestructura para ambos propósitos se permite utilizar funciones que tradicionalmente se han empleado en redes de datos como sucede



con el protocolo DHCP (*Dynamic Host Configuration Protocol*). Este protocolo asigna automáticamente una dirección IP a cada dispositivo de la red, sea éste una computadora o un teléfono IP. Esto permite que la dirección IP del dispositivo no sea estática para cada uno y por lo tanto se puede llevar el teléfono a otro lugar, sin necesidad de que se reconfigure, manteniendo el mismo número telefónico.

No sólo los costos de operación están presentes, también los costos que implican el mover una línea telefónica tradicional de un lado a otro son importantes. Estos costos no se ven reflejados dentro de una infraestructura IP porque el perfil del teléfono IP ya se encuentra configurado y la red IP no diferencia estos equipos por su posición física, si no por su posición lógica. Es decir, no le importa donde esté localizado mientras se encuentre dentro de la misma red.

La telefonía IP se ha desarrollado gracias a los avances de la tecnología, así como a técnicas de digitalización de voz cada vez más eficientes, protocolos de control y priorización de tráfico en las redes, y altos estándares de seguridad y estabilidad en el envío de paquetes de voz y datos.

### **1.3.1 MODELO DE REFERENCIA OSI**

Las ventajas que posee la telefonía IP provienen del uso del protocolo IP en la capa de transporte del modelo OSI.

El modelo de capas OSI para redes es un modelo de referencia creado por ISO (*Internacional Organization for Standardization*) en 1977 [10]. De esta manera, al poseer un modelo estándar, es posible comunicarse entre sí con otros sistemas.

En el modelo OSI las funciones de comunicación se encuentran divididas en un conjunto jerárquico de capas, cada capa tiene sus funciones específicas. Cada capa necesita de las funciones realizadas en la capa anterior para así realizar las suyas. Es decir, cada capa presta servicios a la capa inmediatamente superior.

- Capa Física: Esta capa se encarga de la interfaz física entre los dispositivos. Tiene cuatro características importantes que son mecánicas, eléctricas, funcionales y de procedimiento. Las mecánicas se encargan de las propiedades físicas de la interfaz y con el medio de transmisión. Las eléctricas especifican cómo se representarán los bits en términos de voltaje. Las funcionales especifican la función que realiza cada uno de los circuitos dentro del sistema. Y por último, las de procedimiento especifican cómo se llevará a cabo el intercambio del flujo de bits a través del medio físico.
- Capa de Enlace de Datos: Proporciona un transporte fiable y seguro sobre el enlace físico, además proporciona los medios para activar, mantener y desactivar el enlace. Proporciona un enlace libre de errores ya que realiza detección y control de errores. La capa de enlace de datos posee su propio esquema de direccionamiento. De esta manera, los *switches* tradicionales Ethernet conmutan el tráfico de red sobre la base de la dirección de la capa de enlace, este procedimiento se conoce como *bridging*.

En la capa de enlace se utilizan direcciones de capa física conocidas como MAC (*Media Access Control*) y estas direcciones son únicas para cada dispositivo. Dentro de una LAN, cada dispositivo tiene su propia dirección MAC y de esta manera se la identifica dentro de la LAN. Por lo tanto, cada dispositivo sabe exactamente quien envía un determinado mensaje o a quien enviar un mensaje. Por ejemplo, en la trama Ethernet, los 12 primeros bytes son las direcciones MAC de origen y destino.

El tráfico a través de *switches* Ethernet LAN, es conmutado de acuerdo a las tablas de direcciones MAC que memoriza el *switch*. Entonces, este direccionamiento se lo realiza mediante la dirección de la capa enlace de datos.

- Capa de Red: Realiza la transferencia de información entre sistemas finales a través de algún tipo de red de comunicación. En esta capa, el

---

equipo establecerá un diálogo con la red para especificar la dirección destino. En esta capa residen los protocolos de enrutamiento. La dirección IP es el esquema de dirección más utilizado.

- Capa de Transporte: Esta capa proporciona un mecanismo para intercambiar datos entre sistemas finales. Se realiza control de flujo, verificación de errores, acuse de recibo, retransmisión y secuenciación de datos. Aquí se define si el servicio proporcionado es o no orientado a conexión.
- Capa de Sesión: Proporciona los mecanismos para controlar el diálogo entre las aplicaciones de sistemas finales. Es decir, establece, administra y termina sesiones entre aplicaciones. Las sesiones consisten en el diálogo entre dos o más entidades de presentación, y la capa sesión realiza la sincronización entre estos diálogos.
- Capa de Presentación: Define el formato de los datos que se van a intercambiar entre las aplicaciones y provee servicios de transformación de datos para los programas que “corren” sobre la capa aplicación.
- Capa de Aplicación: Esta capa proporciona a los programas de aplicación el medio para acceder al entorno de la red. En esta capa se proporcionan las funciones de administración y lo necesario para la implementación de las aplicaciones. Ésta es la capa con la que los usuarios interactúan. Algunas de las aplicaciones más conocidas son correo electrónico, navegador web, procesador de texto, transferencia de ficheros, acceso a terminales remotos, etc.

### 1.3.2 STACK DE PROTOCOLOS DE TELEFONÍA IP

El ambiente de telefonía IP comprende varios protocolos. Estos protocolos interoperan de manera jerárquica para proveer los servicios requeridos. Una

manera de representar esta pila de protocolos es la que se muestra en la figura 1.8.

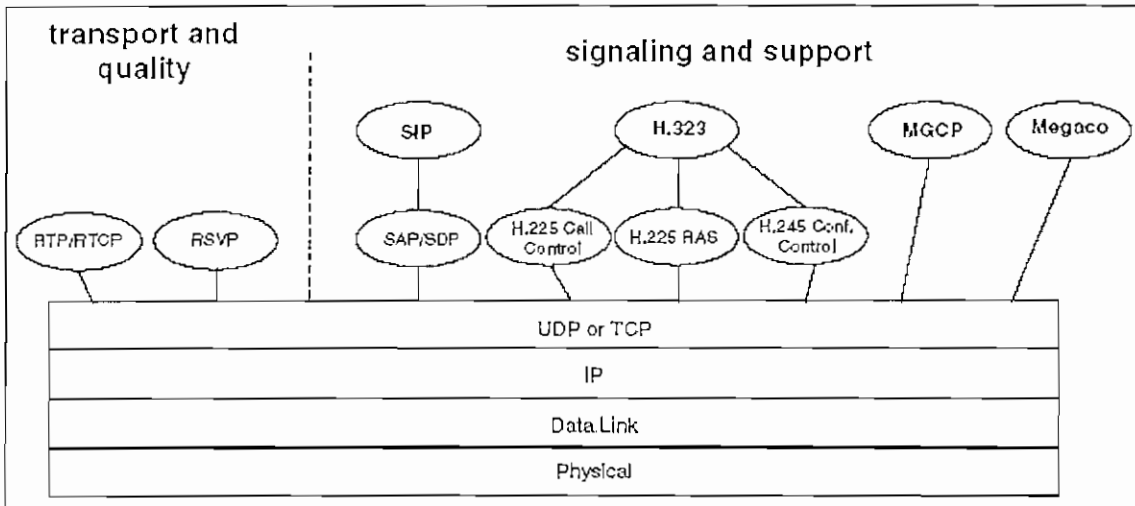


Figura 1.8 Pila de protocolos de Telefonía IP [4].

Las dos secciones de la pila de protocolos proveen las siguientes funciones:

- Protocolos de transporte y de calidad: Estos protocolos se usan para transportar la voz en tiempo real.
- Protocolos de señalización y soporte: La mayoría de las actividades de telefonía IP se encuentran dentro de los protocolos de localización de usuarios, negociación de uso de la red y manejo de llamadas de voz. Actualmente existen cuatro protocolos de señalización importantes:
  - La recomendación H.323 de ITU-T
  - SIP (*Session Initiation Protocol*)
  - MGCP (*Media Gateway Control Protocol*)
  - La recomendación H.248 de ITU-T/*Media Gateway Controller*

Estos protocolos son incompatibles entre sí y proveen funciones redundantes. Cuando éstos son usados en el mismo ambiente, la comunicación entre estos protocolos requiere un convertidor o un *gateway*.

Más adelante se tratará a mayor profundidad los protocolos que intervienen en la telefonía IP.

### 1.3.3 EL PROTOCOLO INTERNET

Con el uso del protocolo IP, la digitalización de la información y las técnicas de codificación, es posible convertir en flujo de bits y paquetizar a casi cualquier fuente de información, sea ésta datos, voz o imágenes. El protocolo IP es un protocolo no orientado a conexión que reside en la capa red (capa 3) del modelo OSI; no tiene mecanismos de fiabilidad, control de flujo, secuenciación o reconocimiento. Para esto, se utilizan otros protocolos como TCP en la capa 4 para agregar control de flujo, secuenciación y otras características.

Ya que el protocolo IP se encuentra en la capa 3, no tiene que tratar con problemas referidos al enlace, de tal manera que IP se puede transportar sobre cualquier enlace (Ethernet, ATM, SONET, etc.), siendo esto transparente para el protocolo. Esto no significa que al diseñar una red se van a ignorar las capas inferiores, solo significa que los medios que se utilicen son independientes de IP.

Un paquete IP se puede difundir de tres maneras generales: *unicast*, *multicast* o *broadcast* [4]. A continuación se explicará brevemente cada uno de éstos:

- *Unicast*: En este modo de difusión se identifica una dirección específica y este nodo es el único que envía el paquete a las capas superiores. Los paquetes transmitidos por *unicast* permiten que dos dispositivos se comuniquen entre ellos sin importar su ubicación física.
- *Broadcast*: Se envían los paquetes a todos los usuarios de una red específica, pasando por *switches* pero no atravesando *routers*. Los paquetes transmitidos por *broadcast* se utiliza para comunicarse simultáneamente con todos aquellos que se encuentren en la subred.

- Multicast: Permite enviar el paquete a múltiples usuarios que se encuentran en subredes diferentes. Los paquetes transmitidos por multidifusión permiten aplicaciones como videoconferencia o teleconferencia en la que existe un transmisor y varios receptores.

El protocolo IP utiliza las direcciones IP para enrutar paquetes. Las direcciones IP están divididas en cinco clases [10] que se esquematizan en la figura 1.9:

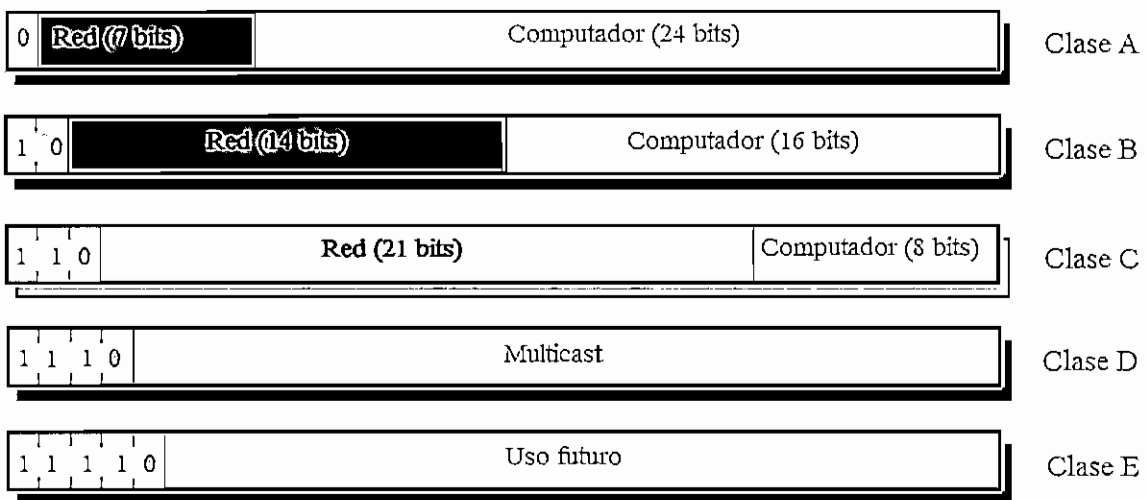


Figura 1.9 Formatos de dirección IP [10].

- Redes de Clase A: Esta clase abarca pocas redes, pero cada una con muchos computadores. Poseen 7 bits para la dirección de red.
- Redes de Clase B: Dispone de un número medio de redes, cada una con un número medio de computadores. Poseen 14 bits para la dirección de red.
- Redes de Clase C: En esta clase se tiene muchas redes y cada una con pocos computadores. Poseen 21 bits para la dirección de red.
- Redes de Clase D: Estas redes están reservadas para *multicast*.

- Redes de Clase E: Éstas se encuentran reservadas para uso futuro.

### 1.3.4 TCP/IP

El mecanismo de transporte más utilizado por IP es TCP (*Transmission Control Protocol*). TCP/IP fue creado para la interconexión de redes, para proveer servicios de comunicaciones entre redes heterogéneas. Esto significa que cada red física tiene su propia tecnología de comunicación y TCP/IP es quien se encarga de proveer todos los servicios de comunicación, teniendo una interfaz común para las aplicaciones independiente de la capa de red física. El principal beneficio de este protocolo es habilitar la comunicación entre dos dispositivos aunque estén separados a grandes distancias geográficas.

TCP/IP puede proporcionar tanto servicio orientado a conexión (TCP) como servicio no orientado a conexión (UDP).

TCP proporciona a los protocolos de capa superior un servicio dúplex completo y de flujo controlado. Los datos se transmiten de manera no estructurada pero se los identifica utilizando números de secuencia. TCP utiliza el método de ventana deslizante para el control de flujo de paquetes. TCP puede soportar varias conversaciones de capa superior simultáneas utilizando en la cabecera del paquete los números de puerto para identificar cada conversación.

Dentro de voz sobre IP, TCP se emplea en la señalización para asegurar la fiabilidad de la configuración de una llamada. No se utiliza TCP para el transporte de la voz en una llamada VoIP ya que la latencia que tiene TCP al esperar los acuses de recibo es alta. Al ser éste un servicio en tiempo real importa más la latencia que la fiabilidad de que todos los paquetes sean recibidos; en el caso de TCP la fiabilidad es lo más importante.

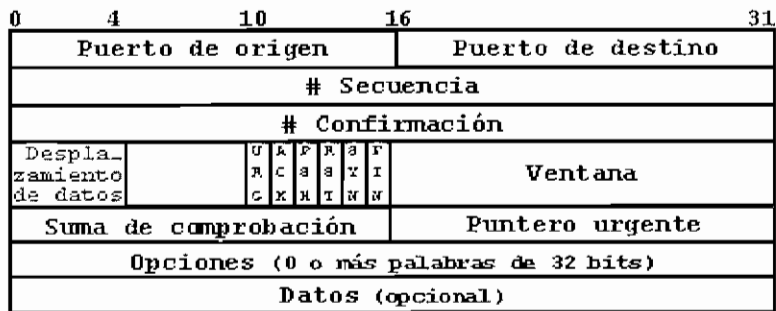


Figura 1.10 Cabecera TCP [33].

El paquete TCP posee los siguientes campos [10] (figura 1.10):

- Puerto de origen (16 bits): Usuario TCP origen.
- Puerto destino (16 bits): Usuario TCP destino.
- Número de secuencia (32 bits): Es la numeración secuencial que TCP asigna a los segmentos que envía, de tal manera que si llegan desordenados en recepción se los puede reordenar.
- Número de acuse de recibo (32 bits): Contiene el número de secuencia del siguiente octeto que la entidad TCP espera recibir.
- Longitud de la cabecera (4 bits): Número de palabras de 32 bits en la cabecera.
- Reservados (6 bits): Bits reservados para uso futuro.
- Indicadores (6 bits): Información de control variada.
- Ventana (16 bits): Para control de flujo; en octetos, cantidad que el que envía está dispuesto a aceptar.



- Suma de verificación (16 bits): El complemento a uno de la suma módulo  $2^{16} - 1$  de todas las palabras de 16 bits en el segmento más una pseudo-cabecera incorporada en el momento del cálculo. Esta pseudo-cabecera incluye campos de la cabecera IP (dirección IP origen y destino, protocolo y un campo longitud del segmento).
- Puntero urgente (16 bits): Señala el octeto que sigue a los datos urgentes.
- Opciones (variable): Especifica el tamaño máximo del segmento que será aceptado.

### 1.3.5 LIMITACIONES TECNOLÓGICAS DE VoIP

Existen varios problemas que pueden afectar a las redes de paquetes y por lo tanto a la transmisión de voz sobre IP. A continuación se explicarán algunos de ellos.

#### 1.3.5.1 Retraso y Latencia

En voz sobre IP se considera retraso y latencia al tiempo que tarda la voz desde que habla la persona que es transmisor hasta que llega al oído del receptor. Existen principalmente tres tipos de retrasos que afectan a las redes de telefonía IP y éstos son:

- Retraso de propagación: Es el retraso que se genera al propagar la voz a través del medio de transmisión, que puede ser fibra óptica, cable UTP (*Unshield Twisted Pair*) o cualquier medio que se utilice en la red.
- Retraso de manejo: También llamado retraso de procesamiento, es causado por los dispositivos que transmiten los paquetes a través de la red.

- Retraso en la gestión de colas: Otras razones para retrasos en redes de conmutación de paquetes es el tiempo que toma mover un paquete hasta la cola de salida, llamado *switching* de paquetes, y el retraso generado por la gestión de colas. El retraso en la gestión de colas se genera cuando existe congestión en una interfaz, es decir, se tiene más paquetes en cola que los que puede manejar la interfaz. Con respecto a la gestión de colas de la cola de salida, ésta debe estar por debajo de los 10 ms utilizando cualquier método de gestión de colas que sea óptimo para la red.

El retardo causa dos problemas: eco y solapamiento.

- Eco: Aparece como consecuencia de las reflexiones que la señal sufre en el otro extremo. Cuando hay presencia de eco el hablante empieza a escuchar una versión retardada de sus propias palabras, si el nivel de eco es muy alto, es imposible mantener una conversación.
- Solapamiento de la voz: Durante una conversación existen pausas, lo que invita al interlocutor a responder. Si la respuesta no llega rápido, hace que el hablante continúe la conversación y el momento de llegada de la respuesta esperada, la voz de ambos interlocutores se sobrepondría dificultando la comunicación. El umbral de retardo a partir del cual este fenómeno empieza a aparecer se encuentra alrededor de los 150 ms.

Siempre es necesario plantear un umbral de retardo, pero este umbral se lo debe establecer tomando el límite bajo el cual se considera calidad de voz aceptable. Por ejemplo, un usuario móvil puede soportar una calidad de voz inferior pero a cambio disfrutará de las ventajas que ofrece la movilidad.

Otro punto a tomarse en cuenta es determinar las fuentes de retardo para poder optimizar su comportamiento, reduciendo de esta manera el retardo que producen en la señal. Uno de los elementos que produce retardo es el CODEC. Un codificador de voz realiza la digitalización de la voz en paquetes y la compresión

de esa señal digitalizada. Este procesamiento produce retardo en la señal. La voz se procesa en tramas, por esta razón los datos no están disponibles hasta que se haya completado la trama.

### 1.3.5.2 Fluctuación de Fase

La fluctuación de fase o *jitter* es la variación del tiempo de llegada del paquete. En la transmisión se espera transmitir paquetes de forma fiable en un intervalo regular de tiempo. Si estos paquetes se retrasan al atravesar la red y el intervalo de tiempo entre cada paquete enviado por el transmisor varía del original, el receptor recibe paquetes con fluctuación de fase.

La supresión del *jitter* se la realiza almacenando los paquetes durante el tiempo necesario para que los paquetes más lentos puedan seguir la secuencia correcta. Para eliminar el *jitter*, el tamaño del *buffer* debe introducir un retardo igual a la diferencia entre el retardo máximo y el retardo mínimo de los paquetes. Si el tamaño del *buffer* es muy pequeño, los paquetes podrían perderse. Al contrario, si el tamaño del *buffer* es demasiado grande, el valor de retardo total sería muy alto.

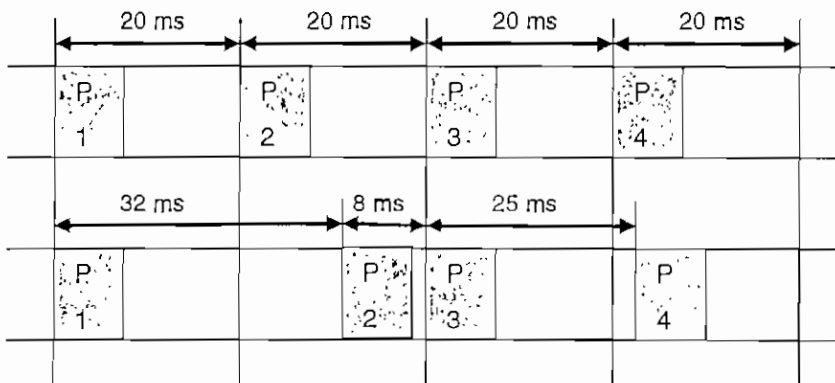


Figura 1.11 Ejemplo de *Jitter* [9].

Si un paquete se tarda más de lo debido en llegar al receptor se lo considera perdido, en ese caso se toman las medidas correspondientes como pedido de retransmisión, lo cual genera pérdida en la calidad de voz. En la figura 1.11 se

puede observar un ejemplo de *jitter*. En este caso, los paquetes P1 y P3 llegan a tiempo, pero los paquetes P2 y P4 llegan retrasados con 12 ms y 5 ms, respectivamente.

## 1.4 COMPONENTES DE UN SISTEMA DE TELEFONÍA IP

Una solución de telefonía IP típicamente necesita tres tipos de componentes de red que son (figura 1.12):

- Gateways de voz
- Procesador de llamadas
- Teléfonos IP

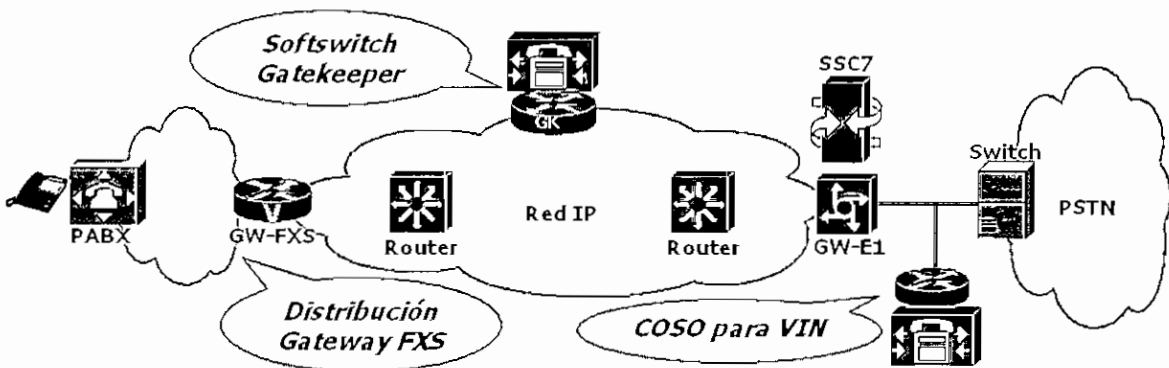


Figura 1.12 Componentes de la red de Telefonía IP [6].

El *gateway* de voz conecta la red local a la red PSTN convencional, lo que hace posible la comunicación telefónica entre teléfonos IP y teléfonos externos convencionales. Esta función también la puede cumplir un *router* especial. Los *switches* LAN pueden conmutar el tráfico de datos y de voz utilizando la característica de Calidad de Servicio (QoS) para garantizar una transmisión de voz clara y de alta calidad.

El procesador de llamadas es un software que ofrece servicios especializados y centralizados para el procesamiento de voz para los teléfonos, *gateways* y servicios adicionales. Actúa como un núcleo central inteligente en la red y se encarga de funciones como la administración de usuarios, los servicios de directorio y la conversión de números de teléfono a direcciones IP. El procesador de llamadas es un *gatekeeper* por lo que se encarga de la traslación de direcciones, control de admisión a la red, control de ancho de banda, servicio de directorio y más servicios que dependerán de las características del software.

Los teléfonos IP son los terminales reales que los usuarios tienen en sus mesas. Convierten los datos en voz y viceversa. Hay distintos tipos de teléfono en función de los servicios disponibles; algunos de ellos incluyen características adicionales, como el acceso a directorios, conferencias, e incluso el acceso a información basada en la Web.

## 1.5 TELEFONÍA IP INALÁMBRICA

Las redes locales inalámbricas, bajo el estándar 802.11 [13], son una solución práctica para redes inalámbricas, compatible con varias aplicaciones de múltiples proveedores. La telefonía IP se ha unido a ésta para crear una nueva y poderosa herramienta, la telefonía IP inalámbrica. Nuevas tecnologías emergentes como Wi-Fi (*Wireless Fidelity*) proporcionan la interoperabilidad de la WLAN y los teléfonos IP inalámbricos.

Los usuarios de telefonía IP inalámbrica tienen acceso a la red empresarial de la misma manera que la tienen los usuarios de la telefonía IP fija. La telefonía IP inalámbrica resulta muy eficiente tomando en cuenta las ventajas de una infraestructura inalámbrica. El personal al que está dirigido la telefonía IP inalámbrica son personas que por su labor no permanecen mucho tiempo en su sitio de trabajo, como es el caso de ejecutivos de la empresa, personal de seguridad, personal de sistemas, trabajadores de plantas de producción que no tienen disponible un terminal de telefonía fijo, y cualquier persona que necesite

movilidad. Es decir, los potenciales usuarios dentro de una empresa son las personas encargadas de tomar decisiones, quienes necesitan estar siempre disponibles para dar una respuesta a múltiples problemas, y personal encargado de implementación de procesos cuya labor determina que se movilicen hacia varios lugares dentro de la empresa.

El tener voz como una aplicación más sobre la red inalámbrica implica varios retos. Uno de éstos es la entrega de una calidad de audio aceptable. Un teléfono inalámbrico es un dispositivo que permite gran facilidad de movilidad, por lo que está cambiando de posición y de área de cobertura de los *Access Point*<sup>1</sup> frecuentemente. Por esta razón se requiere una transferencia inmediata y transparente de la comunicación entre los *access points*. Además se debe incluir cobertura en las áreas donde generalmente no se considera cobertura cuando la red inalámbrica va a ser usada solo para la transmisión de datos; estas áreas son pasillos, escaleras, áreas exteriores de las oficinas e incluso baños.

Otra consideración a tomarse en cuenta es la implementación de seguridad en la red inalámbrica. Esta preocupación se refiere a la integridad total de la red para evitar problemas como intrusiones y asegurar la privacidad de todos los dispositivos, sean éstos teléfonos IP, PCs o cualquier dispositivo que haga uso de la WLAN. Se debe tener en cuenta que no se puede degradar la calidad de voz al implementar seguridades.

Las soluciones para telefonía IP inalámbrica brindan comunicaciones integradas de voz y datos transmitidos sobre una sola infraestructura de red inalámbrica usando estándares basados en la norma 802.11. Existen muchos fabricantes que están desarrollando y brindando soluciones para la transmisión de voz sobre WLAN.

---

<sup>1</sup> *Access Point*: Es un dispositivo utilizado en una red inalámbrica que actúa como un *hub* de comunicaciones. Un *access point* es el punto de interconexión entre un usuario y el resto de la red.

La infraestructura de una red LAN inalámbrica incluye *access points*, antenas y dispositivos inalámbricos de recepción, incluyendo tarjetas de interfaz de red inalámbrica (NICs) y teléfonos IP inalámbricos. La infraestructura puede soportar varios tipos de clientes, tales como teléfonos basados en hardware o en software (llamados *softphones*). Una WLAN basada en el protocolo 802.11 puede transmitir voz y datos a una velocidad de hasta 54 Mbps, pero las redes inalámbricas tienen características que las hacen diferentes de una red alambrada. Una WLAN opera en un medio compartido, es decir, posee una comunicación *Half Duplex* en el que todos los dispositivos comparten la misma conexión inalámbrica. La velocidad varía dependiendo del tipo de radio que se use:

- 802.11a permite transmisiones hasta 54 Mbps.
- 802.11b permite transmisiones hasta 11 Mbps.
- 802.11g permite transmisiones hasta 54 Mbps.

Además, el ancho de banda de la WLAN también depende de la distancia existente entre el dispositivo móvil y el *access point*; a mayor distancia se tendrá menor velocidad de transmisión. Adicionalmente se deberá tomar muy en cuenta la seguridad, ya que como existen muchos dispositivos que trabajan en el rango de frecuencia de la WLAN se debe evitar que intrusos tengan acceso a la información y la roben o la manipulen.

El estándar 802.11g es una mejora al estándar 802.11b ampliamente extendido para redes inalámbricas. Ambos estándares se aplican en la banda de frecuencia de 2.4 a 2.8 GHz y son compatibles.

### 1.5.1 AMENAZAS EN REDES WLAN [14]

Existen varias amenazas de seguridad en una red inalámbrica, de las cuales se pueden nombrar: escuchas ilegales, acceso no autorizado, interferencias y amenazas físicas.

### 1.5.1.1 Escuchas Ilegales

Una amenaza potencial en una red inalámbrica es que un tercero no autorizado escuche las señales intercambiadas entre un dispositivo y el punto de acceso. Éste se lo considera un ataque pasivo. Las escuchas ilegales se las puede realizar con un dispositivo equipado con características similares a los equipos autorizados a la transmisión y recepción de señales.

### 1.5.1.2 Acceso No Autorizado

Otra amenaza es que un intruso acceda a la WLAN aparentando ser un usuario autorizado. Una vez que el intruso ha ingresado a la red, puede violar la confidencialidad e integridad del tráfico de la red, robando información o alterando y falsificando mensajes. Por esta razón es necesario implementar mecanismos de autenticación<sup>2</sup> para evitar accesos no autorizados.

Una variante de los accesos no autorizados es cuando el atacante instala un *access point* ilegal alternativo; cuando los dispositivos inalámbricos buscan un *access point* para conectarse, pueden detectar a éste basándose en la intensidad de la señal recibida y conectarse pensando que es un *access point* legal. De esta manera el atacante puede tener acceso a información que no le pertenece como claves de inicio de sesión.

El ataque en el que un intruso finge ser un usuario autorizado es muy difícil de realizarlo, porque el atacante debe poseer información a detalle de la red a la que está intentando penetrar; si no, no será capaz de engañar al *access point* y el atacante podría ser fácilmente detectado. El tipo de ataque en el que se instala un *access point* alternativo es más fácil de llevar a cabo. El atacante sólo necesita poseer un receptor y una antena con características compatibles a las de los dispositivos que desea engañar. Este tipo de ataques son difíciles de descubrir.

---

<sup>2</sup> Autenticación: Verificar que un usuario es quien dice ser.



La mejor protección contra ambos tipos de ataque consiste en usar un mecanismo eficiente de autenticación.

### 1.5.1.3 Interferencias Aleatorias e Intencionadas

Las interferencias pueden degradar seriamente el ancho de banda y por lo tanto la tasa de transferencia de datos. Existen fuentes de interferencia como otras redes WLAN cercanas, equipos que operan en la banda de 2.4 GHz, transmisores de alta potencia de radioaficionados, incluso hornos microondas que operan en esta banda. Pero también pueden existir interferencias mal intencionadas. Un atacante con un transmisor potente puede generar ondas de radio suficientemente fuertes como para interrumpir las comunicaciones dentro de la WLAN. Estas interferencias intencionadas constituyen un ataque por denegación de servicio.

### 1.5.1.4 Amenazas físicas

Con amenazas físicas se refiere al daño en cualquiera de los componentes físicos que constituyen la red inalámbrica. Los daños en estos dispositivos podrían afectar la capacidad de los usuarios para acceder a los datos y los servicios de información llegando incluso a interrumpir completamente la operación de la red WLAN.

Existen muchos factores que pueden deteriorar los equipos como pueden ser las condiciones ambientales, manejo inadecuado de los dispositivos o accidentes, pero estos equipos también pueden sufrir daños debido a ataques. Por ejemplo, un atacante podría cortar el cableado que une un *access point* con la red cableada dejando aislada a la WLAN, o puede producir un daño directo a los puntos de acceso o a los dispositivos conectados al mismo.

### 1.5.2 SEGURIDAD EN REDES WLAN

La forma más efectiva de prevenir que un intruso tenga acceso a datos transmitidos en una red inalámbrica es utilizando mecanismos de cifrado. WEP (*Wired Equivalent Privacy*) es un elemento crítico al momento de garantizar confidencialidad, integridad de los datos y control de acceso en sistemas WLAN basados en el estándar 802.11. El propósito de WEP es brindar un nivel de confidencialidad equivalente al que posee una red LAN cableada, cifrando las señales de radio. Otro propósito es evitar que usuarios no autorizados accedan a la WLAN, es decir, proporciona autenticación.

Además, se debe proteger a los componentes físicos de la WLAN para que no se encuentren propensos a accidentes, inclemencias meteorológicas o actos de vandalismo. Se debe buscar la mejor ubicación posible para antenas y puntos de acceso, evitando que existan fuentes de interferencia cercanas como pueden ser otros transmisores u hornos microondas. Si estos equipos se encuentran a la intemperie, se debe proteger de lluvia, sol, viento o cualquier efecto ambiental que pueda dañar a los equipos. El acceso a los lugares donde se encuentren los equipos como *access points* debe estar restringido sólo a personal autorizado.

Otra medida de protección incluye el adecuado control administrativo. Todas las estaciones inalámbricas asignadas a los usuarios tienen que estar registradas identificando a los usuarios en ese registro. Las listas de control de acceso se las debe actualizar y realizar revisiones frecuentemente. También se pueden etiquetar los dispositivos para poder llevar control de los mismos por si sufren daños o pérdidas.

Los usuarios representan potenciales peligros a la seguridad de la WLAN por lo que se necesita educación sobre las elementales medidas de seguridad. Por ejemplo, los usuarios nunca deben dejar sus dispositivos inalámbricos en áreas públicas. Un usuario siempre debe tener la precaución de cerrar la sesión en la red si no va usar su equipo. Un caso común es que los usuarios salen al almuerzo y dejan sus sesiones abiertas, esto constituye un peligro en la seguridad de la red.

### 1.5.2.1 Cifrado WEP

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Los datos compartidos entre un dispositivo y un *access point* pueden ser cifrados utilizando esta clave compartida. WEP proporciona funciones de cifrado de datos utilizando una clave secreta de 40 bits en el estándar 802.11 o de 128 bits en el estándar 802.11b y un generador de números pseudoaleatorios RC4. Esta clave secreta se concatena con un *vector de inicialización* aleatorio que añade 24 bits a la clave resultante. Esta nueva clave se inserta en el generador de números pseudoaleatorios el cual genera un flujo de clave pseudoaleatorio. El emisor combina mediante una operación XOR el flujo de clave con el texto en claro generando el texto cifrado. Este texto cifrado se lo transmite al receptor junto con el vector de inicialización. El receptor utiliza el vector de inicialización y su propia copia de la clave secreta para generar un flujo de clave idéntico al que generó el transmisor. El receptor, mediante una operación XOR, combina su flujo de clave con el texto cifrado para obtener el texto en claro original.

Además WEP proporciona seguridad frente a modificaciones no autorizadas del texto cifrado mientras éste se está transportando. WEP aplica un algoritmo de comprobación de integridad al texto en claro. El algoritmo utilizado es CRC-32. Al aplicar este algoritmo se genera un valor de comprobación de integridad, el mismo que se concatena al texto en claro. Este valor de comprobación de integridad viene a constituir algo como la huella digital del texto en claro.

WEP proporciona una fuerte protección a la confidencialidad e integridad de los datos, sin embargo posee algunas limitaciones que son superadas con una adecuada gestión. La primera de estas limitaciones surge con la reutilización del vector de inicialización. El vector de inicialización se encuentra en la parte no cifrada del mensaje para que el receptor pueda tomarlo al momento de generar el flujo de clave para realizar el descifrado. El estándar 802.11 recomienda, pero no exige, que se cambie este valor después de cada transmisión. Esto se

recomienda porque alguien que capture varios mensajes en los que se ha reutilizado este vector de inicialización, puede realizar análisis del flujo de clave generado por el vector y la clave secreta y descifrar la clave secreta, y por consiguiente, los posteriores mensajes que se envíen a través de la red.

Otro problema es la distribución de claves. En las WLAN todas las estaciones y puntos de acceso comparten la misma clave secreta, por esto es difícil que una clave secreta compartida entre tantos usuarios siga siendo secreta por mucho tiempo. La mejor solución para este problema consiste en asignar una clave unívoca a cada estación y efectuar cambios frecuentes de clave.

A pesar de que WEP es computacionalmente eficiente, puede reducir la capacidad de transmisión entre 1 y 2 Mbps, sin embargo, esta reducción es casi imperceptible para el usuario.

#### 1.5.2.2 Autenticación WEP

WEP proporciona dos tipos de autenticación. El primero es un sistema abierto en el que todos los usuarios tienen permiso para acceder a la WLAN y el segundo es un tipo de autenticación mediante clave compartida, la cual controla el acceso a la WLAN y evita accesos no autorizados.

La forma en que trabaja el proceso de autenticación mediante clave compartida es la siguiente. Una estación solicita acceso al punto de acceso al tratar de conectarse, éste replica un texto aleatorio, este texto constituye el desafío. La estación utiliza su copia de la clave secreta compartida para cifrar el texto del desafío y lo devuelve ya cifrado al punto de acceso para lograr su autenticación. El punto de acceso descifra la respuesta enviada por la estación utilizando la misma clave compartida y la compara con el texto de desafío que envió inicialmente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación de que la estación es aceptada dentro de la red. Si los textos no coinciden la estación es rechazada.

Los sistemas por lo general utilizan la misma clave compartida para todas las estaciones. Por lo tanto todas las estaciones o dispositivos, incluso los no autorizados, que posean la clave pueden ingresar a la red. Esta debilidad puede resultar en accesos no autorizados.

Otro medida de seguridad a tomar, es evitar que la clave utilizada para la autenticación sea la misma que la utilizada para el cifrado. Si un atacante logra obtener la clave de autenticación no sólo que podrá acceder a la red, si no que automáticamente tendría acceso a descifrar mensajes.

### 1.5.2.3 Autenticación ESSID

ESSID (*Extended Service Set Identification*, identificación mediante el conjunto de servicios avanzados) es un método de control de acceso que usualmente se utiliza. ESSID es un valor programado en cada punto de acceso que permite identificar la subred a la que pertenece el *access point*. De esta manera, sólo las estaciones que conozcan el valor ESSID podrán autenticarse y asociarse al *access point*.

## 1.6 PROTOCOLOS Y ESTÁNDARES

### 1.6.1 ESTÁNDAR H.323

H.323 es una recomendación publicada por la ITU-T para “Sistemas de Comunicaciones Multimedia Basados en Paquetes” [9]. Este estándar describe los terminales y otros dispositivos que proveen servicios de comunicaciones multimedia a través de Redes Basadas en Paquetes (PBN, *Packet Based Network*) no orientadas a conexión y que no garanticen calidad de servicio. Las entidades H.323 ofrecen audio en tiempo real, comunicaciones de vídeo y/o datos.

A finales de 1997 el VoIP forum del IMTC (*International Multimedia Teleconferencing Consortium*) llegó a un acuerdo en el que se decidió que el H.323 fuera la base de VoIP debido a que cubría la mayor parte de las necesidades para la integración de la voz sobre redes basadas en paquetes. Gracias a este acuerdo los fabricantes de productos para VoIP trabajan bajo el estándar ITU-T H.323 y existe interoperabilidad entre los distintos elementos para que se integren a la red. De este modo, VoIP se puede considerar como una implementación de H.323. Tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional.

El estándar H.323 consta de los siguientes componentes y protocolos [1]:

- *H.225* Señalización de llamadas.
- *H.245* Control de medios.
- *G.711, G.722, G.723, G.728, G.729* Códecs de audio.
- *H.261, H.263* Códecs de vídeo.
- *T.120* Compartición de datos.
- *RTP(Real Time Transport Protocol) / RTCP (Real Time Control Protocol)* Transporte de medios.

#### 1.6.1.1 Elementos H.323

Un sistema H.323 consta de varios elementos como terminales, *gateways*, *gatekeepers* y unidades de control multipunto (MCU, *Multipoint Control Units*) [1 y 5]. La figura 1.13 ilustra estos elementos.

Los terminales a los que también se los llama puntos finales, proporcionan conferencias punto a punto y multipunto para audio y opcionalmente, para vídeo y datos. Los *gateways* se encargan de la conexión con la PSTN o con redes ISDN

para *interworking*. Los *gatekeepers* proporcionan el control de admisión y servicios de traducción de direcciones. Los MCU permiten que dos o más terminales o *gateways* realicen conferencias con sesiones de audio y/o vídeo.

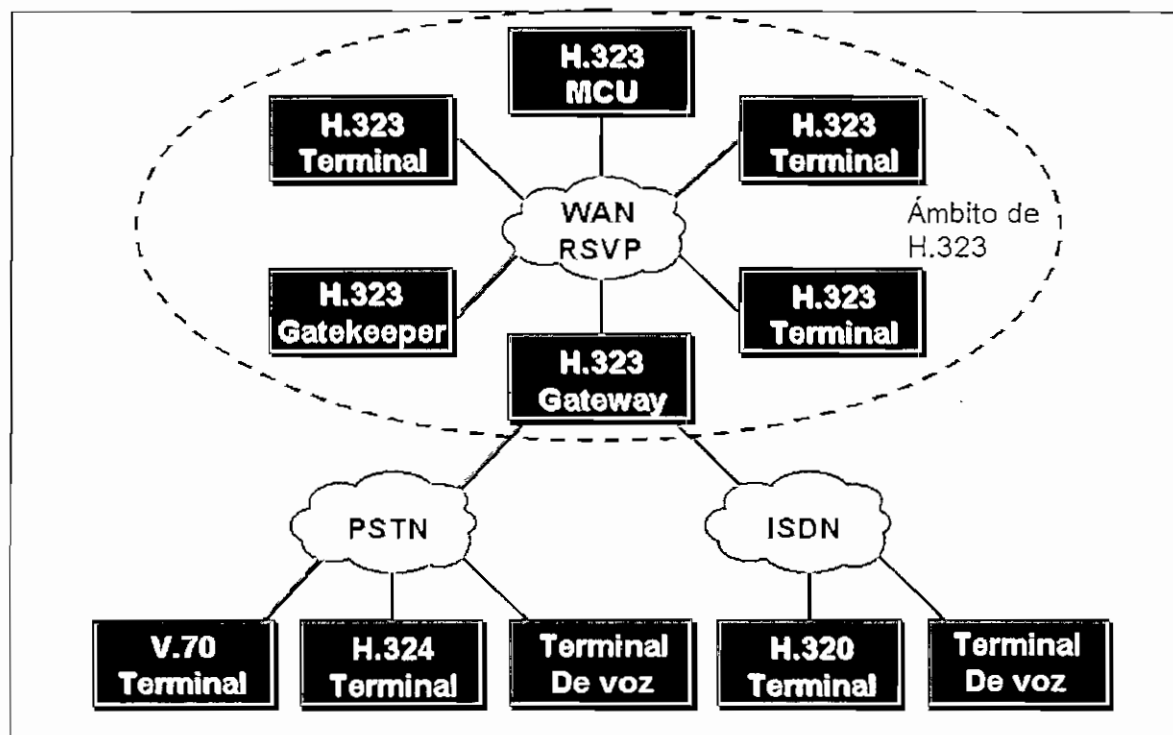


Figura 1.13 Elementos de red H.323 [1].

Además dentro de un sistema H.323 se habla de Zona H.323, que es el conjunto de terminales, *gateways* y MCU gestionadas por un único *gatekeeper*. Una zona incluye por lo menos un terminal y varios *gateways* o MCU. Una zona es independiente de la topología de la red y comprende múltiples segmentos de red conectados mediante *routers* u otros dispositivos de interconexión.

Cada entidad H.323 dispone de una dirección de red que la identifica unívocamente. Un método alternativo para direccionar un punto final es a través del uso de un alias. Este alias puede ser una dirección de correo electrónico o un número de teléfono. El alias debe ser único dentro de cada zona H.323.

### a) Terminales H.323

Un terminal H.323 es un punto final en la red el cual provee para tiempo real dos vías de comunicación con otro terminal H.323, un *gateway* o un MCU. Esta comunicación comprende voz, y adicionalmente se puede intercambiar vídeo y/o datos.

Los terminales H.323 poseen una unidad de control de sistema, códec de audio, opcionalmente también transmisión de datos y códecs de vídeo, y una interfaz de red basada en paquetes. La estructura del terminal se representa en la figura 1.14.

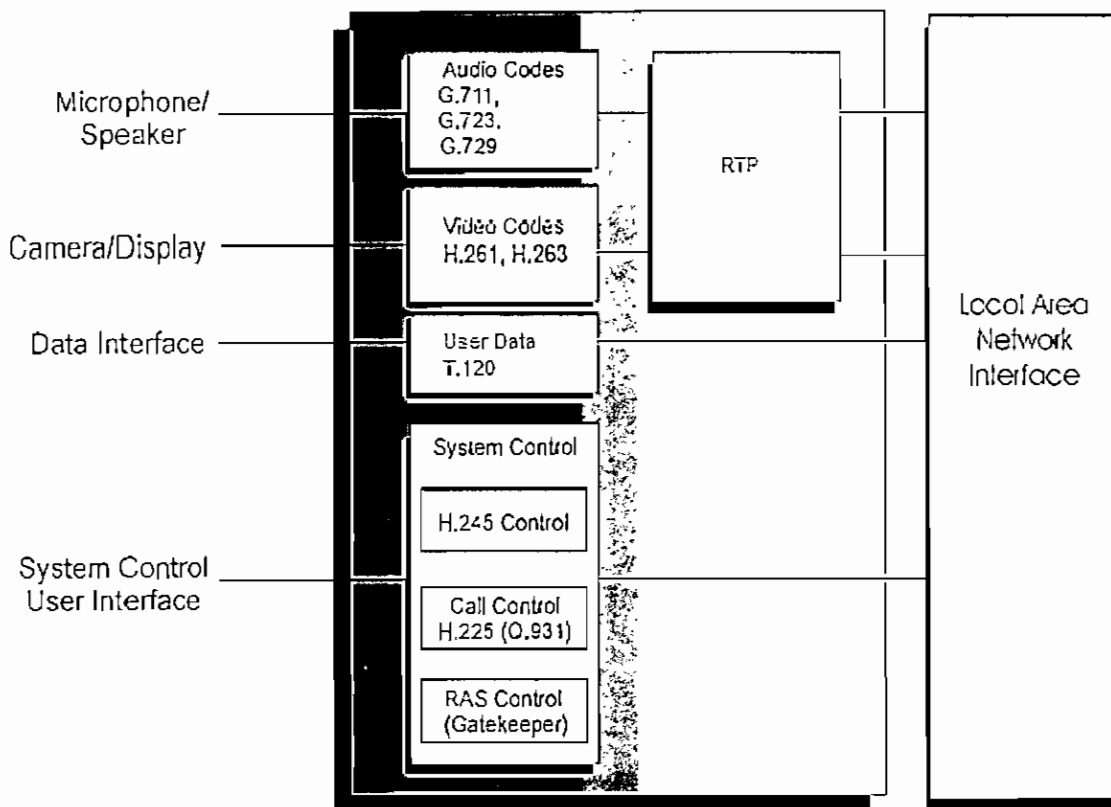


Figura 1.14 Terminal H.323 [7].

- *Unidad de control de sistema:* Proporciona a H.245 y H.225 el control de llamadas, intercambio de capacidad, mensajería y señalización de comandos para el correcto funcionamiento del terminal. H.245 se encarga



de la negociación del uso del canal y sus prestaciones. H.225 se encarga de la señalización y establecimiento de llamadas.

- *Transmisión de medios:* Para la secuenciación de los paquetes de audio y vídeo. También envía y recibe audio, vídeo y mensajes de la interfaz de red.
- *Códec de audio:* Codifica la señal recibida desde el equipo de audio para su transmisión y decodifica el código de audio que llega al códec. Las funciones requeridas incluyen codificación y decodificación de voz G.711 aceptando formatos de la ley A y ley  $\mu$ . Adicionalmente puede soportar codificación y decodificación G.722 (64, 56 y 48 kbps), G.723.1 (5,3 y 6,3 kbps), G.728 (16 kbps) y G.729 (8 kbps).
- *Interfaz de red:* Interfaz basada en paquetes que puede hacer servicios de *unicast* y *multicast* de extremo a extremo de protocolos TCP y UDP.
- *Códec de vídeo:* Este códec es opcional, en caso de existir, deberá codificar y decodificar vídeo de acuerdo con H.261. Utiliza algoritmos de digitalización y compresión de vídeo, es usado para video-conferencias. Se maneja con tasas en múltiplos de 64 Kbps.
- *Canal de datos:* De acuerdo a la recomendación T.120 que soporta aplicaciones como acceso a base de datos, transferencia de archivos y conferencias de audio-vídeo en tiempo real.

## b) Gateways

El *gateway* sirve de interfaz entre redes H.323 y redes no H.323. Conecta por un lado hacia la red de voz tradicional y por otro hacia los dispositivos basados en transmisión de paquetes. También permite la conexión con sistemas H.320, que son sistemas de vídeo-conferencia. Los *gateways* brindan muchos servicios

siendo las traslaciones más comunes tanto del medio como de la señalización entre terminales H.323 y otros tipos de terminales. En otras palabras, es el punto de unión de una red de circuito conmutado (SCN) y la red H.323, como se muestra en la figura 1.15. El *gateway* se encarga de traducir entre formatos de audio, vídeo y transmisión de datos, así como en sistemas de comunicación y protocolos.

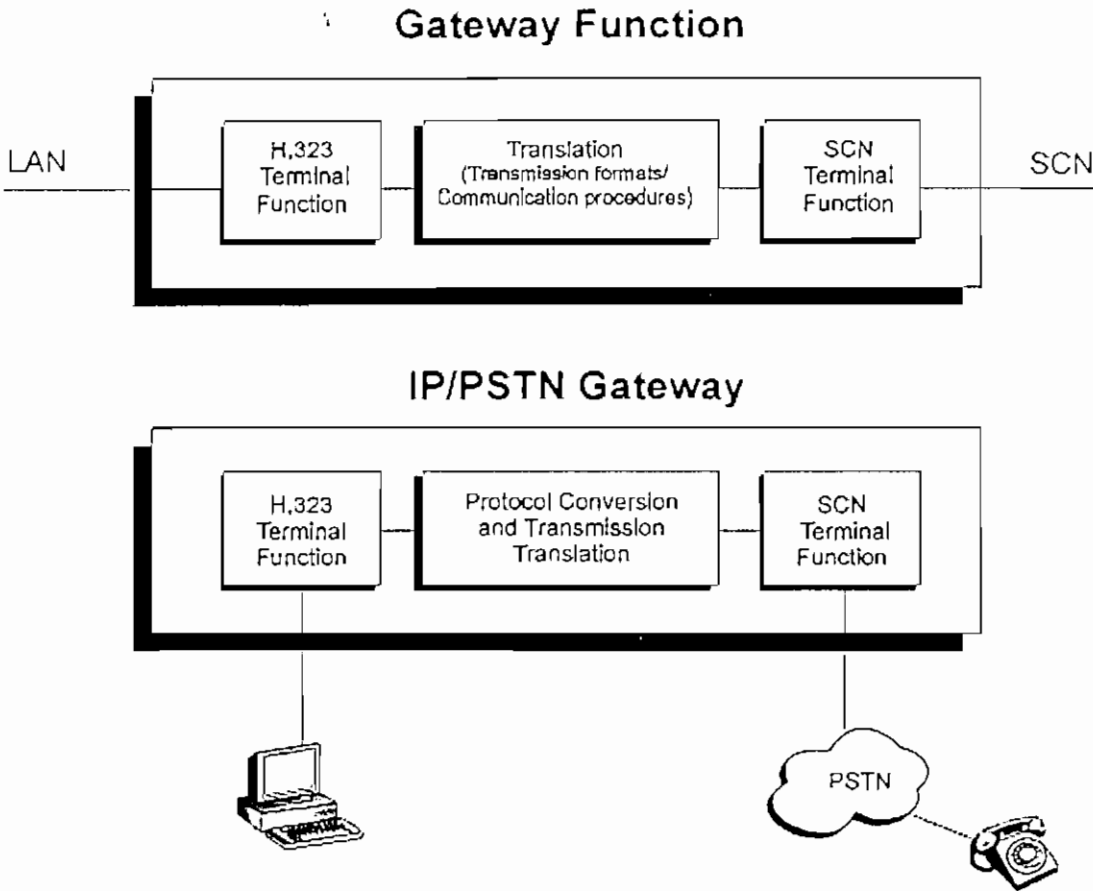


Figura 1.15 Elementos de un *Gateway* H.323 [7].

Los terminales se comunican con los *gateways* utilizando el protocolo de control de medios H.245 y el protocolo de señalización H.225. El *gateway* es el encargado de traducir estos protocolos a los de la red no H.323 con la que se está comunicando. Este proceso es transparente para ambas redes.

El *gateway* es esencial cuando se necesite interacción con la PSTN, ya que su misión es la de enlazar la red VoIP con la red telefónica pública. Por lo tanto, un *gateway* tiene por un lado la interfaz LAN y por el otro puede tener interfaces FXO

(*Foreign Exchange Office*), FXS (*Foreign Exchange Station*), E&M (*recEive and transMit*), BRI (*Basic Rate Interface*) o PRI (*Primary Rate Interface*). Si no se necesita conexión con la SCN, los puntos finales H.323 pueden comunicarse directamente sobre la red de paquetes sin conectarse con un *gateway*.

### c) *Gatekeeper*

El *gatekeeper* es una función opcional que proporciona servicios de control de prellamada y nivel de llamada a los puntos finales H.323. Provee traslación de direcciones y control de acceso a la red a terminales H.323, *gateways* y MCUs. Los *gatekeepers* están lógicamente separados de los demás elementos de la red en los entornos H.323, pero físicamente su implementación puede coexistir con un terminal, MCU, *gateway* u otras entidades no H.323 como puede ser un servidor proxy, de correo, etc.

El *gatekeeper* puede utilizar una secuencia consulta / respuesta (*Location Request* LRQ o *Location Confirmation* LCF) para localizar a los usuarios remotos. Un *gatekeeper* debe proveer los siguientes servicios:

- Traslación de direcciones: El *gatekeeper* debe realizar mediante una tabla de traslación de direcciones, la interpretación del número de extensión marcado y dirigirla hacia los terminales H.323 los cuales se identifican en el *gatekeeper* con su dirección IP asignada. Esta tabla se actualiza constantemente para identificar los terminales conectados en el sistema. El *gatekeeper* traduce el número E.164 que es un número de teléfono normal a la dirección de red del terminal de destino.
- Control de admisión: Controla el acceso autorizado a H.323 utilizando los mensajes RAS H.225.0 *Admision Request / Admision Confirm / Admision Reject* (ARQ / ACF / ARJ). El acceso puede basarse en niveles de autorización de llamadas o ancho de banda. Controla el número de

terminales que pueden estar conectados simultáneamente, lo cual también depende del ancho de banda disponible en la red.

- Control de Ancho de Banda: Se implementa utilizando mensajes RAS *Bandwidth Request / Bandwidth Confirm / Bandwidth Reject* (BRQ / BCF / BRJ). Se encarga del manejo y administración del ancho de banda que se asignará a cada llamada para obtener un nivel aceptable de QoS. Está en la capacidad de no admitir un usuario si el ancho de banda no es el suficiente.
- Administración de zona: Proporciona las funciones anteriores para terminales, *gateways* y MCUs que están dentro de su zona de control.

Opcionalmente también realiza las siguientes funciones:

- Control de señalización de llamadas: El *gatekeeper* puede encaminar mensajes de señalización entre puntos finales H.323. Esta característica se la puede emplear para utilizar al *gatekeeper* como monitor de llamadas para mejorar el control de las llamadas en la red. El *gatekeeper* puede tomar decisiones de encaminamiento basándose en factores como balance de carga en los *gateways* lo que mejora el QoS en la red.
- Autorización de llamadas: Permite que el *gatekeeper* restrinja el acceso a determinados terminales y *gateways*. Un terminal envía un mensaje de señalización a un *gatekeeper*, y éste puede aceptar o rechazar la llamada. Los rechazos pueden estar basados en restricciones de acceso o temporales hacia o desde un terminal o *gateway* en particular.
- Administración de llamadas: El *gatekeeper* mantiene una lista con información sobre las llamadas H.323 activas de modo que puede controlar su zona, balanceando carga y transmitiendo información de los terminales en uso para la función de gestión de ancho de banda.

- Administración de ancho de banda: Gracias a esta función el *gatekeeper* puede rechazar la admisión si el ancho de banda requerido no está disponible.

Un *gatekeeper* puede participar en una variedad de modelos de señalización. Los modelos de señalización determinan qué mensajes de señalización pasan a través del *gatekeeper* y cuáles pueden pasar directamente entre dispositivos como terminales y *gateways*. Para ejemplificar modelos de señalización, se puede ver las figuras 1.16 y 1.17. La figura 1.16 muestra un modelo de señalización directa en la que los mensajes de señalización para las llamadas no pasan por el *gatekeeper*. La figura 1.17 es un modelo de señalización de llamadas de *gatekeeper* enrutado (GKRCS, *Gatekeeper Routed Call Signaling*). En este modelo, todas las señales pasan a través del *gatekeeper* y solamente la transmisión de medios pasa directamente entre las estaciones.

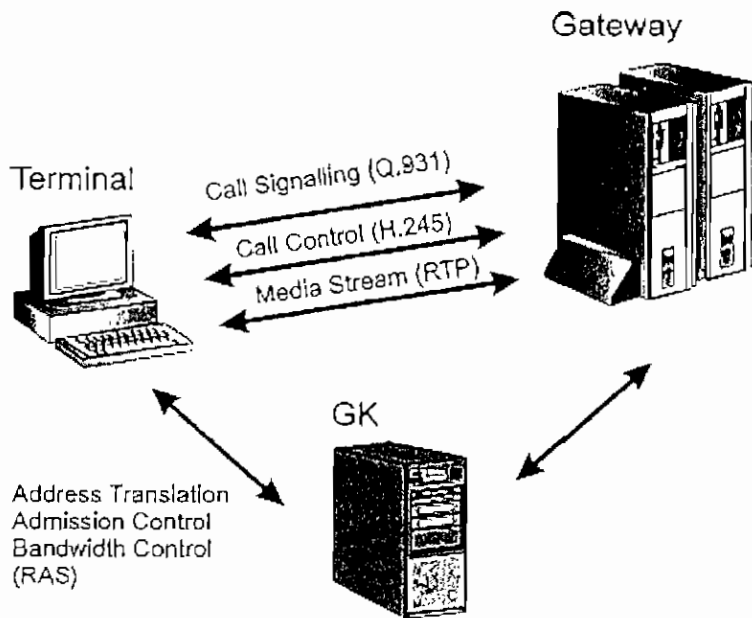


Figura 1.16 Modelo de señalización directa [7].

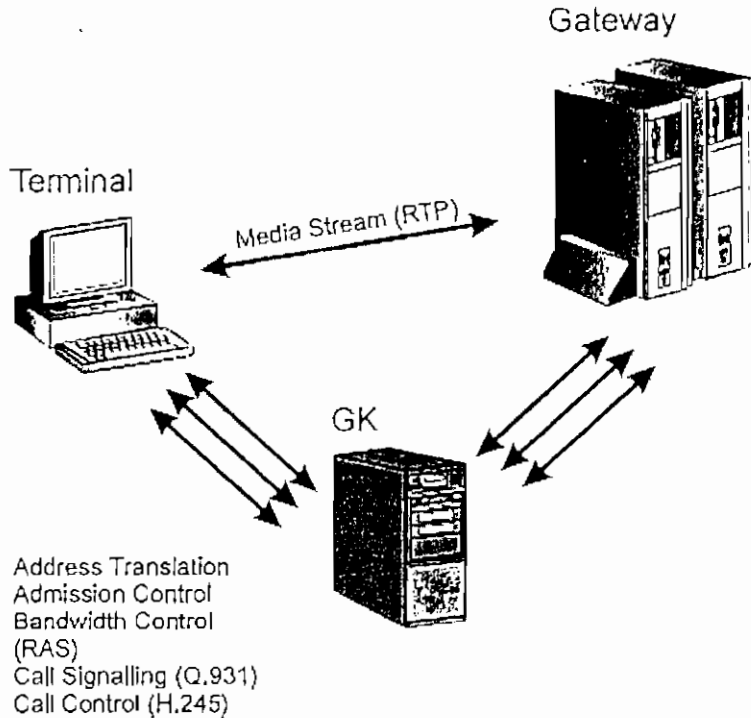


Figura 1.17 Modelo GKRCs [7].

#### d) MCU (*Multipoint Control Unit*)

Las MCU proveen funciones de control para conferencias entre tres o más terminales H.323. Un MCU consiste de un MC (*Multipoint Controller*) y un MP (*Multipoint Processor*).

El MC se encarga de la coordinación del control de llamadas para soportar conferencias entre tres o más puntos finales en conferencias multipunto y revisar las capacidades durante la conferencia. Debe existir obligatoriamente un MC en cada MCU y opcionalmente puede estar en los terminales, *gateways* y *gatekeepers*.

La función del MP es mezclar las señales de audio, vídeo y/o datos que provienen de los puntos finales involucrados en una multi conferencia. La mezcla consiste en el proceso de formatear más de una fuente de audio, vídeo y/o datos que el MP enviará a los terminales de una fuente hacia otra. El procesador multipunto es

opcional en todos los elementos de la red H.323 a excepción de los terminales donde es mandatorio que exista uno.

Un MCU que soporta conferencias multipunto centralizadas, consta de un MC y un MP que soporte audio, vídeo y datos. Se entiende como conferencia centralizada cuando el MCU controla el contenido de la conferencia, la comunicación es punto a punto. Un MCU que soporta conferencias mutipunto descentralizadas consiste en un MC y un MP que soporte la recomendación T.120. Se dice que una conferencia es descentralizada cuando cada terminal envía el audio y/o vídeo al resto de terminales sin la intervención directa del MCU. Además se tienen sistemas híbridos en el que se combinan los dos casos anteriores.

Es importante aclarar que las definiciones de los elementos dentro de la red H.323 son lógicas. No se especifica sobre la división física de los dispositivos. Por lo tanto, los MCUs pueden ser dispositivos separados que por si solos cumplen su función, o pueden estar integrados dentro de un *gateway*, un *gatekeeper* o un terminal.

### 1.6.1.2 *Stack* de protocolos H.323

H.323 está compuesto por varios protocolos. Esta familia de protocolos soporta la admisión, la preparación, el estado y el borrado de llamadas, los flujos de medios y los mensajes en los sistemas H.323. Estos protocolos están soportados por mecanismos de entrega seguros (TCP) y poco seguros (UDP), como se puede observar en la figura 1.18.

El *stack* de protocolos H.323 está dividido en tres áreas principales de control:

- Señalización de registro, admisiones y estado (RAS): Proporciona control de prellamadas en las redes basadas en *gatekeeper* H.323.

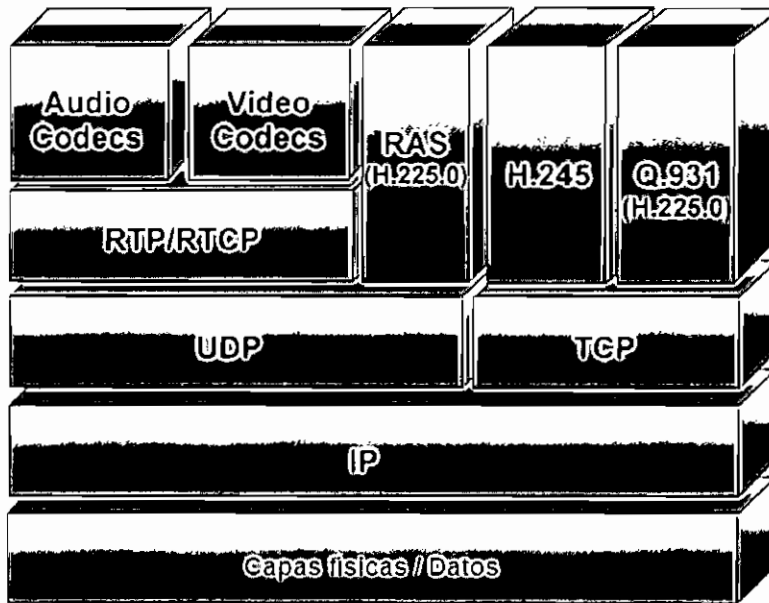


Figura 1.18 Capas del conjunto de protocolos H.323 [7].

- Señalización de control de llamadas: Utilizada para conectar, mantener y desconectar llamadas entre puntos finales.
- Control y transporte de medios: Proporciona el canal H.245 seguro, que transporta los mensajes de control de los medios.

Los mensajes de control Q.931 y H.245 son transportados sobre la capa TCP que es de entrega confiable. Esto asegura que los mensajes importantes se transmitan. El tráfico de medios es transportado sobre la capa UDP de entrega poco segura e incluyen dos protocolos definidos en el RFC 1889. Estos protocolos son RTP (*Real Time Protocol*) y RTCP (*Real Time Control Protocol*) que incluyen mensajes de control y estado periódicos. El flujo de medios es transportado sobre UDP porque no tendría sentido retransmitir paquetes de este tipo. Si se retransmitiera un fragmento de sonido perdido, probablemente éste llegaría muy tarde para cualquier uso en la reconstrucción de voz. Los mensajes RTP comúnmente se los transporta en puertos UDP de números pares, mientras que los mensajes RTCP se transportan en los puertos adjuntos de números impares.



### 1.6.1.2.1 Señalización RAS

El registro, admisión y estado (RAS, *Registration, Admission and Status*) [1 y 5] es el protocolo que se establece entre extremos finales y *gatekeepers* previamente al establecimiento de cualquier otro tipo de canal. Los mensajes RAS viajan a través de un canal no confiable (UDP). La señalización RAS proporciona un control de prellamadas en las redes H.323 donde existen *gatekeepers*. Es independiente de la señalización de control de llamadas y de los canales de transporte de medios. Las funciones de la señalización RAS son las siguientes:

- Descubrimiento del *gatekeeper*: Éste es un proceso que puede ser estático o dinámico. Este proceso lo utilizan los puntos finales para identificar a qué *gatekeeper* deben registrarse. Si es estático, el punto final debe saber *a priori* la dirección IP de su *gatekeeper*. Si es dinámico, utiliza un método conocido como autodescubrimiento.

La dirección de difusión del descubrimiento de *gatekeeper* es 224.0.1.41 y el puerto de descubrimiento UDP del *gatekeeper* es 1718; el puerto de estado y registro UDP del *gatekeeper* es 1719.

El punto final envía un mensaje *multicast* GRQ (*Gatekeeper Request*) en el que pregunta en qué *gatekeeper* debe registrarse. Este mensaje lo responden los *gatekeepers* disponibles con un mensaje GCF (*Gatekeeper Confirm*) o con un mensaje GRJ (*Gatekeeper Reject*) los *gatekeepers* que no quieran aceptar el registro.

El mensaje GCF incluye la dirección IP del canal RAS del *gatekeeper*. El punto final tiene la posibilidad de elegir el *gatekeeper* al que quiere registrarse de todos los que han enviado el mensaje GCF. Si después de un tiempo de espera ningún *gatekeeper* responde, el punto final vuelve a enviar el mensaje GCF.

- Registro del punto final: Es el proceso empleado para que los *gateways*, puntos finales y MCUs alcancen una zona e informen al *gatekeeper* de sus direcciones IP y alias en dicha zona. Este proceso se produce después del descubrimiento del *gatekeeper*. Un punto final envía una solicitud de registro RRQ (*Registration Request*) a la dirección IP del canal RAS del *gatekeeper*. El *gatekeeper* envía un mensaje de confirmación RCF (*Registration Confirmation*) o uno de rechazo RRJ (*Registration Reject*). El *gatekeeper* debe asegurarse que exista una única dirección IP por cada alias. El proceso de cancelación de registro lo puede realizar el punto final o el *gatekeeper*. Si lo realiza el punto final, éste envía un mensaje URQ (*Unregister Request*) al *gatekeeper*, el cual confirma la baja del registro con un mensaje UCF (*Unregister Confirmation*). Si la baja del registro lo realiza el *gatekeeper*, éste es quien envía el mensaje URQ al punto final que quiere cancelar el registro, el mismo que contestará con un mensaje UCF.
- Localización del punto final: Mediante este proceso un *gatekeeper* o un punto final obtienen la información de contacto de otro punto final del cual sólo poseen el alias. Para este efecto, se envía un mensaje de solicitud de localización LQR (*Location Request*). El *gatekeeper* en el que el punto final solicitado está registrado contesta con un mensaje de confirmación LCF (*Location Confirmation*) que contiene la información de contacto del punto final. El resto de *gatekeepers* en los que no se encuentra registrado el punto final solicitado responden con un mensaje de rechazo LRJ (*Location Reject*).
- Admisiones: Estos mensajes proporcionan las bases para la admisión de llamadas y control de ancho de banda. Se envía un ARQ (*Access Request*) que es una petición realizada por un punto final para iniciar una llamada. El *gatekeeper* responde con ACF (*Access Confirmation*) dando la autorización para admitir la llamada. Si la petición de llamada es negada, el *gatekeeper* responde con ARJ (*Access Reject*).

- Información de estado: También se utiliza el canal RAS para obtener el estado de un punto final, con esto se puede detectar condiciones de fallo en los puntos finales. El período típico de sondeo para los mensajes de estado es de 10 segundos. Para esta función se utilizan los mensajes IRQ (*Information Request*) e IRR (*Information Request Response*). El *gatekeeper* envía un mensaje IRQ hacia el punto final para pedir información. La respuesta a este mensaje es IRR.
- Control de ancho de banda: El control de ancho de banda se administra inicialmente el momento que se realiza el intercambio de admisiones entre un punto final y el *gatekeeper*, pero para cambiar el ancho de banda durante una llamada se utilizan mensajes que se envían por el canal RAS. Un BRQ (*Bandwidth Request*) es enviado por un punto final al *gatekeeper* pidiendo cambio en el ancho de banda de la llamada, a lo que el *gatekeeper* responde con BCF (*Bandwidth Confirmation*) para confirmar la aceptación de la petición de cambio de ancho de banda. Si la petición es rechazada, el *gatekeeper* responde con BRJ (*Bandwidth Reject*).

#### a) Señalización de Control de Llamada H.225.0/Q.931

Este canal se emplea para transportar mensajes de control. Se pueden tener dos tipos de señalización [5]:

- Señalización directa: En este caso los mensajes de señalización entre los puntos finales se intercambian directamente sin la intervención de un *gatekeeper* utilizando las direcciones de transporte de señalización de llamada CSTA (*Call Signaling Transport Address*).
- Señalización indirecta: Los mensajes de señalización son encaminados por el *gatekeeper* enviándole mensajes utilizando la dirección IP del canal RAS.

La señalización H.225 se emplea para establecer conexiones entre puntos finales H.323 para poder transportar datos en tiempo real. Debido a que la señalización necesita intercambiar mensajes H.225 sobre un canal fiable, se implementa sobre TCP.

#### b) Control H.245

El protocolo H.245 maneja mensajes de control extremo a extremo entre entidades H.323. El protocolo H.245 establece canales lógicos para la transmisión de información de audio, vídeo, datos y canal de control [5].

Un punto final establece un canal H.245 para cada llamada con el punto final que está participando. Los mensajes de control intercambiados llevan información relacionada con las capacidades de intercambio, la apertura y el cierre de canales lógicos para el transporte de flujos de datos, mensajes de control de flujo e indicaciones y comandos generales.

El canal de control H.245 es un canal lógico abierto permanentemente, a diferencia del resto de canales. Los mensajes H.245 pueden ser de dos tipos:

- Mensajes de intercambio de características de los terminales: Éste es un proceso realizado entre los terminales para intercambiar información sobre sus capacidades de transmisión y recepción con el extremo final.
- Mensajes de señalización de canales lógicos: Se utiliza para abrir o cerrar un canal lógico. Un canal lógico lleva información unidireccional desde un punto final a otro punto final en el caso de conferencias punto a punto, o desde un punto final a múltiples puntos finales en el caso de conferencias punto – multipunto.

### c) Transporte de Medios RTP/RTCP

RTP permite la entrega de extremo a extremo en tiempo real de audio, vídeo y datos sobre redes *unicast* y *multicast* en H.323. Los servicios de empaquetamiento y transmisión incluyen la identificación de carga útil, la secuenciación, la marca de temporización y la monitorización.

RTCP se encarga del monitoreo de la entrega de datos y controla e identifica los servicios. El canal de medios se crea utilizando UDP.

### 1.6.2 ESTÁNDAR SIP

*Session Initiation Protocol* (SIP) es un estándar IETF (*Internet Engineering Task Force*) de control de señalización de la capa de aplicación, que se especifica en la RFC 2543. Se lo utiliza para establecer, modificar o finalizar sesiones multimedia entre dos o más participantes. Las sesiones multimedia pueden ser de telefonía IP, videoconferencias, juegos, es decir cualquier tipo de aplicación que proporcione medios como audio, vídeo y datos.

SIP soporta sesiones *unicast* y *multicast*, así como llamadas punto a punto y multipunto. Los servicios que soporta SIP son:

- Localización de usuarios: Para determinación del sistema final que participará en la comunicación.
- Establecimiento de llamada: Permite el timbrado y acuerdo de los parámetros de la llamada entre el origen y el destino.
- Disponibilidad del usuario: Determinación del deseo del usuario de participar en la comunicación.

- Características del usuario: Determinación de los flujos y las características de los flujos que podrán ser empleados.
- Manejo de llamadas: Transferencia y terminación de llamadas.

El desarrollo de la telefonía IP requiere posibilidades adicionales de señalización, y la extensibilidad de SIP permite desarrollos de funcionalidad incremental ya que permite operar en conjunto con otros protocolos de señalización como el H.323.

El protocolo SIP es relativamente sencillo ya que emplea mensajes de texto plano que se pueden leer. Además utiliza formatos estándares como HTTP 1.1 y "mailto:". Esto facilita la integración de este protocolo con otras aplicaciones y la resolución de problemas.

El flujo de mensajes SIP consume poco ancho de banda, por lo que su impacto en la eficiencia de la comunicación es mínimo. En el mensaje inicial se incluye toda la información necesaria para el establecimiento de la llamada, lo que reduce los tiempos de conexión de llamada.

SIP utiliza SDP (*Session Description Protocol*, Protocolo de Descripción de Sesión) para identificar y negociar los códecs, por lo que puede utilizar cualquier códec registrado por la Agencia de Asignación de Números Internet (IANA). H.323 no tiene esta capacidad, ya que los códecs que utiliza son los que están definidos explícitamente en el estándar.

Además brinda soporte para las funciones de telefonía tradicional como lo son reenvío, transferencia, parqueo, conferencia de llamadas; SIP, al igual que H.323, puede utilizar el lenguaje de procesamiento de llamada (*CPL Call Processing Language*). Este lenguaje permite a los usuarios proporcionar reglas complejas sobre sus llamadas al servidor.

### 1.6.2.1 Componentes del Sistema SIP

Una red SIP está compuesta por dos tipos de entidades: los agentes de usuario y los servidores de red.

- Agente de usuario: Un agente de usuario es una aplicación final que envía y recibe peticiones SIP. Está formado por dos entidades que son cliente y servidor. Los clientes de agentes del usuario (UAC) envían peticiones SIP al llamante y los servidores de agentes del usuario (UAS) reciben las respuestas del llamado. Se asocia una dirección SIP con cada agente de usuario.
- Servidores de red: Existen varios tipos de servidores de red SIP. El servidor proxy desempeña un papel similar al de un servidor proxy en un sistema HTTP. Es decir, actúa en nombre de otros clientes y contiene funciones de cliente y de servidor ya que es capaz de recibir preguntas y respuestas. Un servidor proxy interpreta y puede reescribir cabeceras de peticiones antes de pasarlas a los siguientes servidores. Rescribir las cabeceras identifica al proxy como el iniciador de la petición y asegura que las respuestas vayan al siguiente proxy en lugar de ir hasta el cliente. Decide cuál será el siguiente servidor al que pasan las peticiones.

El servidor de redirección acepta las peticiones SIP y envía una respuesta redirigida al cliente que contiene la dirección del siguiente servidor. Los servidores de redirección no aceptan llamadas ni procesan o reenvían peticiones SIP.

El servidor de localización es empleado por un servidor proxy o un servidor de redirección para obtener información sobre la localización del usuario al que se está llamando. El servidor de registro recibe las actualizaciones de la ubicación de los usuarios.

### 1.6.2.2 Direccionamiento

A las direcciones SIP también se las llama URL (*Uniform Resource Locator*). La forma de las direcciones SIP son similares a una dirección de correo electrónico usuarios@hosts. Como se puede ver, la dirección consta de dos partes, la parte de usuario y la parte del *host*. La parte de usuario puede ser un nombre de usuario o un número de teléfono. La parte de *host* puede ser un nombre de dominio o una dirección de red.

Por defecto, los servidores SIP escuchan en los puertos TCP y UDP 5060, pero pueden utilizar cualquier número de puerto. Las direcciones SIP además del usuario y el *host*, pueden incluir parámetros e información de cabecera, añadiendo sintaxis al URL SIP básico. Pueden tener varios parámetros y campos de cabecera.

Para distinguir los puntos finales E.164 (teléfonos) de los puntos finales IP regulares, se utilizan parámetros del usuario en un URL SIP. Por ejemplo una dirección SIP para un punto final E.164 puede ser sip: 4199@voip-gw.company.com;user=phone. De esta manera se reconoce que esta dirección se asocia con un punto final E.164. Por lo general no se ve la cabecera user=ip porque es la predeterminada, por eso, cuando no tiene la cabecera *user*, se asume que es un punto final IP regular.

Un cliente puede enviar una petición SIP directamente a un servidor proxy configurado localmente, o a la dirección IP y puerto del correspondiente URL SIP. DNS tiene mucha importancia en el enrutamiento de llamadas SIP, porque la mayoría de URLs SIP incluyen normalmente nombres DNS.

### 1.6.2.3 Mensajes SIP

Las transacciones SIP se las realiza utilizando mensajes SIP. Una vez que se ha resuelto el direccionamiento, el cliente envía una o más peticiones SIP y recibe



una o más respuestas desde el servidor. Este intercambio de peticiones y respuestas se conoce como transacción SIP. Se pueden transmitir transacciones SIP utilizando TCP o UDP.

Un mensaje SIP está estructurado por tres partes: la línea de inicio, la cabecera y el cuerpo. Dentro de la línea de inicio se encuentran las peticiones de mensaje y las respuestas de mensaje.

Los mensajes SIP son de dos tipos: peticiones iniciadas por los clientes y respuestas devueltas desde los servidores. SIP es un protocolo basado en texto con una sintaxis de mensajes y campos similar a HTTP. Cada mensaje posee una cabecera que describe los detalles de la comunicación.

Las cabeceras de mensaje se utilizan para especificar la parte llamante, la parte llamada, la ruta y el tipo de mensaje de una llamada. Existen 4 grupos de cabeceras:

- Cabeceras generales que se aplica a las peticiones y a las respuestas.
- Cabeceras de entidad que define información sobre el tipo de cuerpo del mensaje y longitud.
- Cabeceras de petición que permite que el cliente incluya información adicional de petición.
- Cabeceras de respuesta que permite que el servidor incluya información de respuesta adicional.

Una cabecera SIP representa un valor variable que se transporta a través de la red. El orden en que aparecen las cabeceras SIP en el mensaje no es importante, excepto en dos casos: cuando aparecen en el orden en el que las respuestas SIP deberían fluir de regreso en los servidores proxy y las cabeceras *Hop-by-hop* que

son las que se deberían procesar en el servidor proxy que deben aparecer antes que las cabeceras *End-to-end*. Las cabeceras se las enumera en la Tabla 1.1.

Cabeceras Generales	Cabeceras de entidad	Cabeceras de petición	Cabeceras de respuesta
Accept	Content-Encoding	Authorization	Allow
Accept-Encoding	Content-Lenght	Contact	Proxy-Authenticate
Accept-Language	Content-Type	Hide	Retry-After
Call-ID		Max-Forwards	Server
Contact		Organization	Unsupported
CSeq		Priority	Warning
Date		Proxy-Authorization	WWW-Authenticate
Encryption		Proxy-Require	
Expires		Route	
From		Require	
Record-Route		Response-Key	
Timestamp		Subject	
To		User-Agent	
Via			

Tabla 1.1 Cabeceras SIP [1].

Dentro de las peticiones de mensaje, la comunicación SIP posee seis tipos de peticiones. Estas peticiones permiten que los agentes de usuarios y servidores de red localicen, inviten y administren llamadas. Los seis tipos de peticiones son los siguientes:

- *INVITE*: Que permite iniciar una llamada VoIP. Invita a la parte llamada a unirse a la sesión. Incluye una descripción de sesión y el tipo de medio.
- *ACK*: Representa la confirmación final por parte del sistema final de una petición *INVITE*. Concluye la transacción iniciada por el comando *INVITE*.

- 
- *OPTIONS*: Permite realizar consultas y encontrar posibilidades de agentes de usuarios y servidores de red. Esta petición no se utiliza para establecer sesiones.
  - *BYE*: Es un método SIP utilizado tanto para la parte llamada como para la parte llamante para liberar una llamada. Antes de que efectivamente se libere la llamada, el agente de usuario envía esta petición al servidor para indicar su deseo de liberar la sesión.
  - *CANCEL*: Esta petición permite que los agentes de usuario y los servidores de red puedan cancelar una solicitud pendiente.
  - *REGISTER*: Es un método que utilizan los clientes para registrar información de localización con los servidores SIP.

Como resultado de una petición se genera una respuesta SIP. Después de haber recibido e interpretado una petición se envía una respuesta indicando si una llamada ha tenido éxito o ha fallado, y el estado del servidor. Las respuestas se las puede clasificar en seis categorías:

- *Informational*: que proporciona información sobre el estado de la llamada, puede ser intentando, sonando, llamada está siendo reenviada o llamada puesta en cola.
- *Success*: que indica si la acción solicitada fue recibida, comprendida y aceptada.
- *Redirection*: que solicita que el cliente realice una acción adicional para completar la solicitud.
- *Request Failure*: que significa que la solicitud no es válida en el servidor al que se envió.

- *Server Failure*: que es utilizado cuando una solicitud puede ser válida, pero el servidor en concreto es quien falló por cualquier otra razón.
- *Global Failures*: que indica que la solicitud fallará siempre, en el servidor al que llegó o en cualquier otro servidor.

El contenido del cuerpo de un mensaje varía dependiendo del tipo de solicitud o respuesta SIP. El cuerpo del mensaje de los métodos *INVITE*, *ACK* y *OPTIONS* es una descripción de la sesión basada en SDP (*Session Description Protocol*). El método *BYE* nunca incluye un cuerpo. SDP está diseñado para identificar completamente todos los atributos de una sesión, incluyendo información administrativa acerca del programa y los medios.

#### 1.6.2.4 Operatividad de SIP

La operatividad básica de SIP se fundamenta en invitar a un participante a una llamada. El servidor maneja esas peticiones entrantes de dos maneras que pueden ser utilizando servidores proxy y servidores de redirección.

En el modo de operación de servidor proxy se siguen algunos pasos para que una llamada de doble vía tenga éxito. En primer lugar el servidor proxy acepta la petición *INVITE* del cliente. A continuación, el servidor proxy procede a la identificación de la localización utilizando las direcciones y los servicios de localización y la información proporcionada en el mensaje. Se emite una petición *INVITE* a la dirección de la localización devuelta. Con esta petición, el agente de llamadas de la parte llamada alerta al usuario sobre la petición y devuelve una indicación de éxito al servidor proxy que realizó la petición. Posteriormente se envía una respuesta OK desde el servidor proxy a la parte llamante, la cual confirma la recepción emitiendo una petición *ACK*.

En el intercambio de protocolo para la petición *INVITE* en un servidor de redirección también es necesario seguir ciertos pasos. La parte llamante realiza

una petición *INVITE* que es aceptada por el servidor de redirección; con la información que la petición posee se contacta los servicios de localización. Cuando el servidor de localización ha ubicado al usuario, este servidor devuelve la dirección directamente a la parte llamante. A diferencia del servidor proxy, el servidor de redirección no emite ninguna petición *INVITE*. Después el agente de usuario envía un *ACK* al servidor de redirección confirmando que la transacción se ha completado. Posteriormente el agente de usuario envía directamente una petición *INVITE* a la dirección que le envió el servidor de redirección. A esta petición tiene que responder la parte llamada con una respuesta OK que indica el éxito de la operación y la parte llamante devuelve un *ACK*.

#### 1.6.2.5 Stack de Protocolos SIP

SIP proporciona los elementos básicos de un sistema de telefonía, es decir establecimiento, liberación y configuración de llamadas. Pero además se apoya en otros protocolos para su funcionamiento.

##### a) SDP

SDP (*Session Description Protocol*) se usa para describir la configuración de sesiones multimedia. Este protocolo se encarga de proporcionar información acerca de los flujos de datos en sesiones multimedia, para que de esta manera los receptores posean información sobre la sesión al momento de formar parte de ella.

Incluye información sobre flujos de datos, direcciones, puertos, tipo de carga, tiempos de comienzo y de parada, y origen de la sesión. Una sesión multimedia tiene diferentes tipos de flujos de datos como audio, vídeo o datos. SDP asigna un número y un tipo a cada uno de estos flujos. SDP soporta flujos de audio, vídeo, datos, control y aplicación.

En cuanto a las direcciones, para cada flujo de datos se especifica una dirección destino. La dirección de destino de los flujos de datos puede ser diferente, ya que un usuario podría recibir audio en un teléfono IP y vídeo en una PC, siendo los dos flujos pertenecientes a la misma sesión. Para cada flujo además es necesario especificar los puertos UDP de transmisión y de recepción.

La información que SDP proporciona sobre el tipo de carga se refiere al formato del flujo que se utiliza durante la sesión. La información sobre los tiempos de comienzo y de parada se emplea para invitar a otros usuarios a que se integren a una sesión. El origen se utiliza para las sesiones *multicast*, en la que es necesario enviar información sobre el origen de la sesión y cómo contactarse con la persona que la origina.

#### b) CPL

El protocolo CPL (*Call Processing Language*) se lo emplea para describir y controlar servicios de telefonía IP. CPL se implementa en los servidores de red y en los agentes de usuario. Este protocolo es independiente de sistemas operativos y del protocolo de señalización. Está basado en lenguaje de *scripts*. Cuando llega una llamada a un servidor SIP, se ejecutan las instrucciones detalladas en CPL lo que permite al usuario final especificar sus propios servicios de llamadas.

#### c) GLP

GLP (*Gateway Location Protocol*) es un protocolo usado por SIP cuando se quiere conectar un usuario de la red de telefonía de paquetes a la PSTN. El usuario de telefonía IP envía una invitación SIP a un *gateway*, y la función de GLP es encontrar el *gateway* más adecuado para realizar la llamada y establecer la sesión.

## 1.7 CALIDAD DE SERVICIO

Telefonía IP es un sistema de comunicaciones que ofrece calidad de servicio garantizada. Al utilizar esta tecnología, se está empaquetando la voz; por lo tanto, lo que les pase a esos paquetes será lo que afecte la calidad en la comunicación. Calidad de servicio (QoS) hace referencia tanto a la clase de servicio (CoS) como al tipo de servicio (ToS) [1].

La aplicación de QoS ayuda a resolver algunos de los problemas relacionados con VoIP, como son la pérdida de paquetes, la fluctuación de fase y el retraso de señalización. Los problemas que QoS no puede resolver son el retraso de propagación, el retraso de códec, el retraso de muestreo y el retraso de digitalización. Esos problemas sólo se pueden disminuir con el uso de buenos equipos dentro de la red y un adecuado dimensionamiento para la misma.

Al realizar una llamada telefónica utilizando telefonía IP hay algunos parámetros cuyos valores ya están establecidos y no se pueden cambiar, como se puede ver en la Tabla 1.2.

	<b>Retraso fijo</b>	<b>Retraso variable</b>
Retraso de codificador G.729 (5 ms <i>look-ahead</i> )	5 ms	
Retraso de codificador G.729 (10 ms por trama)	20 ms	
Retraso de empaquetamiento, incluido retraso de codificador	variable	variable
Retraso de gestión de cola 64 kbps troncal		6 ms
Retraso de serialización 64 kbps troncal	3 ms	
Retraso de propagación (líneas privadas)	32 ms	
Retraso de red	variable	variable
<i>Buffer</i> de fluctuación de fase		2-200 ms
<b>Total – Asumiendo un <i>buffer</i> de fluctuación de fase de 50 ms</b>	<b>110 ms</b>	

Tabla 1.2 Retraso previsto de extremo a extremo [2].

La recomendación G.114 de la ITU-T recomienda que no exista más de 150 ms de retraso extremo a extremo para poder garantizar una buena calidad de voz.

### 1.7.1 LIMITACIONES DE ANCHO DE BANDA

El ancho de banda necesario para la transmisión de la señal de voz es función del algoritmo de codificación y compresión del códec a utilizar. En una comunicación siempre hay momentos en que los interlocutores no pronuncian palabras claras o simplemente están en silencio. Sin embargo, mientras la comunicación se mantenga activa, el envío de paquetes será constante, y por consiguiente ocupará ancho de banda. Una forma de ahorrar ancho de banda en las transmisiones de VoIP es utilizar la técnica de supresión de silencios. En la Tabla 1.3 se realiza una comparación del ancho de banda requerido utilizando y sin utilizar esta técnica.

Tipo de Códec	Duración de Trama (ms)	Bytes de Voz/Trama	Con supresión de silencios			Sin supresión de silencios		
			Bytes de Paquetes IP	Bytes de Trama Ethernet	Ancho de banda en LAN (KHz)	Bytes de Paquetes IP	Bytes de Trama Ethernet	Ancho de banda en LAN (KHz)
G.711 (64 Kbps)	10	80	120	146	116.8	240	292	233.6
	20	160	200	226	90.4	400	452	280.8
	30	240	280	306	81.6	560	612	163.2
G.729 (8 Kbps)	10	10	50	76	60.8	100	152	121.6
	20	20	60	86	34.4	120	172	68.8
	30	30	70	96	25.6	140	192	51.2
G.723(6.3 Kbps)	20	16	56	82	32.7	112	164	65.4
	30	24	64	90	23.9	127	179	47.8
G.723(5.3 Kbps)	20	13	53	79	31.7	107	159	63.4
	30	20	60	86	22.9	120	172	45.8

Tabla 1.3 Comparación de ancho de banda [1 y 2]



Al revisar los resultados de la Tabla 1.3 se puede observar que el ancho de banda requerido se reduce en una relación aproximada de 2 a 1 al utilizar la técnica de supresión de silencios. Por lo tanto, esta característica ayuda mucho en un sistema de VoIP.

Otra técnica de gestión del ancho de banda es el protocolo RSVP (*Resource Reservation Protocol*). Éste es un protocolo de control de red que permite obtener una QoS determinada para flujos de datos en las aplicaciones de una red de paquetes. Incorpora una reserva de ancho de banda junto con una lista de acceso dinámica extremo a extremo. De esta manera, si no es posible soportar en todos los dispositivos de la red la QoS requerida por un determinado flujo, se envía un mensaje de error indicando que la comunicación no puede realizarse.

RSVP se basa en conceptos como reserva de recursos, que implica que los *routers* deben mantener información sobre el estado de los distintos flujos que atraviesan para poder garantizar una cierta QoS para cada flujo. Se realiza control de admisión. Además el origen establece una caracterización del tráfico que se va a enviar tomando parámetros como ancho de banda que utiliza, retardo y *jitter*, esto permite realizar la reserva de recursos.

### 1.7.2 GESTIÓN DE COLAS

Los flujos de paquetes que se transmiten a través de la red suelen sufrir retrasos al pasar por los diferentes dispositivos que componen la red. Durante estos retrasos existen otros paquetes que también están transitando y que tienen que esperar a que los paquetes anteriores pasen el procesamiento en que se encuentren. La primera técnica de gestión de colas que se utilizó es FIFO (*First In, First Out*) [1], que significa que los primeros en llegar serán los primeros en salir. En la actualidad existen otros métodos para gestión de colas.

### 1.7.2.1 Gestión de Colas Apropriada Ponderada

WFQ (*Weighted Fair Queuing*) [1] es un método de gestión de colas en el que todos los paquetes se dividen en múltiples colas separando los flujos y asignando a cada uno de éstos la misma cantidad de ancho de banda. De esta manera, se evita que una sola aplicación consuma todo el ancho de banda. Esta técnica asegura que todas las aplicaciones posean ancho de banda disponible y el tráfico tiene un servicio previsible. WFQ se ajusta dinámicamente para utilizar el ancho de banda que está libre para los flujos que todavía se están transmitiendo, de esta manera no existe ancho de banda subutilizado.

La gestión de colas equitativa utiliza varios factores para determinar la prioridad, puede ser la cantidad de ancho de banda que un flujo consuma. Este método permite que el ancho de banda sea compartido equitativamente sin la utilización de listas de acceso u otras tareas administrativas que consumen tiempo. WFQ sólo se puede ejecutar en interfaces que trabajan a 2.048 Mbps o menos.

### 1.7.2.2 Gestión de Colas Personalizada

En la gestión de colas CQ (*Custom Queuing*) [1] se determina un porcentaje de ancho de banda disponible para un protocolo determinado. Permite definir hasta 16 colas y una adicional para mensajes de sistema. En este método cada cola es atendida secuencialmente de manera cíclica, se transmite un porcentaje de tráfico de un flujo y después se pasa a la siguiente cola.

Se configura en el *router* cuántos *bytes* de cada cola se transmitirán. Si una cola no utiliza el total del ancho de banda, otra cola puede utilizarlo. Este método de gestión de colas requiere que se conozcan los tipos de puerto y de tráfico de cada aplicación. Esto implica gran sobrecarga administrativa, pero una vez pasada esta etapa, es muy eficiente.

### 1.7.2.3 Gestión de Colas por Prioridad

Al utilizar PQ (*Priority Queuing*) [1] es necesario definir cuatro prioridades de tráfico dentro de la red: alta, normal, media y baja. El tráfico de entrada se asigna a una de estas cuatro colas de salida. De esta manera, todo el tráfico de prioridad alta posee todo el ancho de banda que necesita hasta que termine su transmisión. Cuando la cola de prioridad alta esté vacía, se transmiten los paquetes de la cola de prioridad normal, luego la de media y por último la de baja.

Este método asegura que el tráfico crítico, como son las aplicaciones en tiempo real, siempre reciban todo el ancho de banda necesario para su transmisión. Por esta razón, es muy importante realizar una buena clasificación de los flujos de tráfico para que no existan aplicaciones que carezcan de la atención y del ancho de banda necesario para su correcto funcionamiento.

### 1.7.2.4 Otros Métodos de Gestión de Colas

CB-WFQ (*Class Based Weighted Fair Queuing*) [1] posee las ventajas ofrecidas por WFQ pero además proporciona soporte especial para clases de tráfico definidas por el administrador de la red. Este método permite crear clases específicas para determinadas aplicaciones, por ejemplo, para el tráfico de voz. El administrador de la red define esas clases que determinan cómo se agrupan los paquetes en las diferentes colas mediante listas de acceso.

Con CB-WFQ el administrador de la red tiene control sobre la cantidad exacta de ancho de banda que se asigna por clase de tráfico. Puede manejar 64 clases diferentes con características de ancho de banda específicas para cada clase. Se puede asignar cantidades de ancho de banda mínimos para garantizar un servicio.

Otro método es PQ dentro de CB-WQF, el cual es un método de gestión de colas de baja latencia, está diseñado específicamente para dar prioridad absoluta al

tráfico de voz sobre cualquier otro tráfico. Éste es un mecanismo que ha demostrado ser muy potente y proporciona a los paquetes de voz la prioridad, latencia y fluctuación de fase necesarios para una buena calidad de voz.

### 1.7.3 POLÍTICAS DE ENRUTAMIENTO

El enrutamiento determina en gran medida la eficiencia del acceso a los recursos limitados de la red, por lo que forma parte de los aspectos críticos a tomarse en cuenta. Las técnicas de QoS (QoS *Routing*) [5] se aplican a todos los aspectos del enrutamiento, como son los algoritmos de optimización de rutas, algoritmos y gestión de encaminamiento, y todo lo relacionado al enrutamiento.

Una manera de desarrollar protocolos QoS es aplicar algoritmos a los protocolos de enrutamiento tradicionales para que éstos sean sencillos y eficientes. Estos algoritmos deben ser estables y robustos para reaccionar de manera óptima a las variaciones dinámicas de la carga de la red.

Las políticas de enrutamiento son especificadas en la interfaz que recibe el paquete, no en la interfaz que envía el paquete.

### 1.7.4 CONSIDERACIONES ADICIONALES

Por lo general se entiende como calidad de servicio en redes que transportan voz a las características ofrecidas por la red una vez que la llamada ya se ha establecido. Pero existen otras características que también se deben tomar en cuenta al momento de brindar calidad en el servicio al usuario. Los parámetros que se deben tomar en cuenta son el tiempo que toma establecer una llamada y el porcentaje de llamadas con éxito.

El tiempo de establecimiento de la llamada es el tiempo que transcurre desde que el usuario marca el número hasta que la conexión de voz se hace efectiva. En la

telefonía tradicional este tiempo es muy corto, por lo tanto, en la telefonía IP también debe serlo ya que ese es el servicio que el usuario espera.

El porcentaje de éxito de llamadas se refiere a la relación total del intento de llamadas con la cantidad de llamadas que efectivamente se logran realizar.

## CAPÍTULO 2

# DISEÑO DE LA RED CONVERGENTE PARA TELEFONÍA IP PARA EL GRUPO ITABSA

### 2.1 ESTADO ACTUAL DE LA RED

El grupo ITABSA, empresa afiliada a Philip Morris International (PMI), es una compañía dedicada a la producción y comercialización de cigarrillos, con marcas de gran representación en el país. El índice de representatividad en el mercado ecuatoriano es de aproximadamente el 98%, por lo tanto, es una empresa altamente consolidada en Ecuador.

Es el grupo ITABSA quien se encarga de proveer de servicios de informática y comunicaciones para si misma y para el resto de empresas afiliadas a PMI en el país, esto es PROESA y TANASA, así como para Philip Morris Perú y Bolivia. Para este proyecto se presentará una primera etapa de la migración de la red de dos localidades del grupo corporativo hacia telefonía IP. Se prevé la migración de la central telefónica del edificio Belmonte, donde funcionan las oficinas de ITABSA y la parte administrativa de PROESA, y la planta de producción TANASA. Ambas localidades se encuentran en la ciudad de Quito, la primera al norte en la zona comercial de la ciudad (Av. Corea 126 y Amazonas) y la segunda al sur de la ciudad (Panamericana sur Km 5 ½). Posteriormente, se migrará el resto de las oficinas a esta misma tecnología; esta segunda etapa no se la cubre dentro del presente trabajo ya que el mismo representa otro proyecto dentro de la empresa. En el país existen: otra planta de producción en Durán, una oficina central de PROESA en Guayaquil, bodegas de PROESA en San Rafael, y 8 zonas (oficinas de PROESA) alrededor del país. Las centrales telefónicas analógicas que actualmente está usando el grupo corporativo son centrales antiguas que necesitan ser renovadas por nueva tecnología como lo es telefonía IP.

La misión del área de informática es “ser un grupo creativo y asesor que identifique, promueva y entregue soluciones innovadoras de tecnología y sistemas integrados a los procesos, para lograr una ventaja competitiva hacia la alta productividad en el desarrollo del negocio” [15]. Ésta es la motivación que impulsa a buscar nuevas soluciones eficientes para los sistemas de comunicaciones dentro de la empresa. Además una de las estrategias manejadas por PMI es el retiro de las aplicaciones obsoletas y la tecnología asociada a ellas.

La figura 2.1 muestra la red de datos que actualmente posee el grupo ITABSA en el Ecuador. Los tipos de enlaces que forman la red WAN son satelital y terrestre. Además ITABSA dispone de un enlace internacional de 512 Kbps que al momento se utiliza para Internet *browsing*, *e-mail* y aplicaciones globales.

En la parte de telefonía, en el edificio Belmonte existe una central telefónica Definity y una base celular, en la que se realiza el enrutamiento automático según el tipo de llamadas sean éstas locales, nacionales, internacionales o celulares. En TANASA Quito se tiene igualmente una central telefónica Definity con los mismos servicios de enrutamiento automático, existiendo adicionalmente una base celular.

Todos los empleados de la empresa tienen a su cargo una PC y un teléfono. También existen teléfonos en salas de reuniones. Las centrales telefónicas digitales Definity son centrales antiguas. Tanto en ITABSA como en TANASA ya no tienen capacidad de crecimiento, están llegando al límite de su capacidad de usuarios. Todos los teléfonos de la empresa están conectados a estas centrales telefónicas, y a través de éstas se tiene acceso a la PSTN.

La infraestructura tecnológica de la red de datos del grupo ITABSA para Ecuador consta de un AS/400, 22 servidores, 306 PCs y 63 impresoras (Figura 2.2). La red LAN es de arquitectura Ethernet 10/100 Mbps *Full Duplex*, con cable UTP categoría 5e. Como *backbone* se tiene un enlace a 1 Gbps con fibra óptica. El enlace internacional es satelital y lo provee Impsat (figura 2.3). El enlace satelital utilizado soporta la tecnología *Frame Relay*, para el cual Impsat ha designado un canal con una velocidad de transmisión de 512 Kbps (CIR).

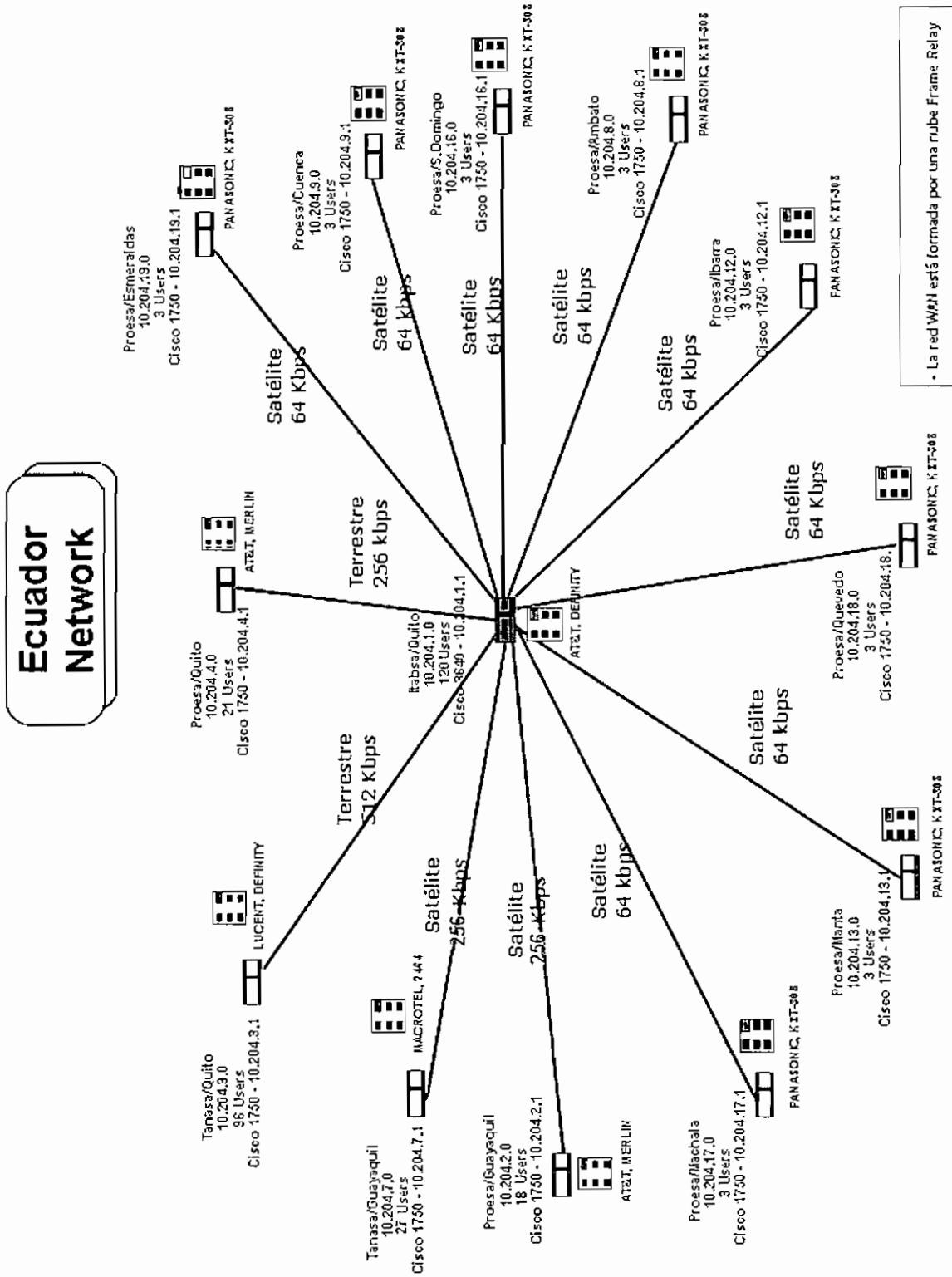
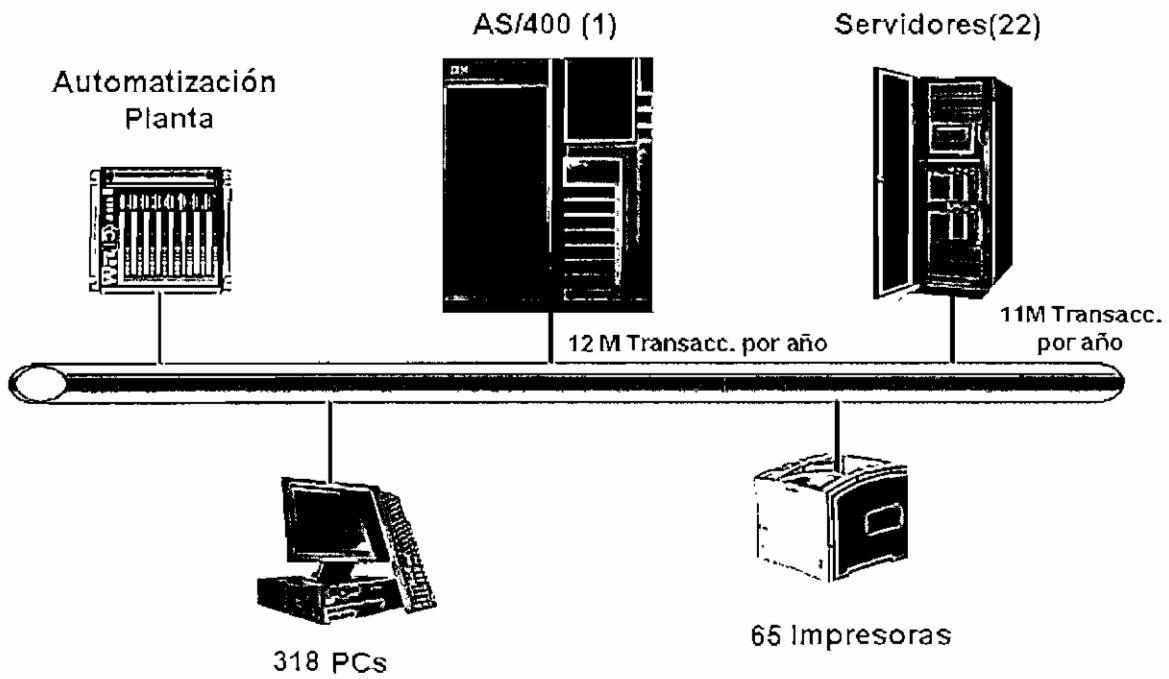


Figura 2.1 Red de datos grupo ITABSA [15].





SERVIDORES		IMPRESORAS		PCS	
		Localidad	Impresoras	Localidad	PCs
2	Exchange	Itabsa UIO	18	Itabsa UIO	120
5	Ventas	Tanasa UIO	19	Tanasa UIO	96
1	ESSBASE	Proesa UIO	6	Proesa UIO	21
6	BD Aplicaciones	Tanasa GYE	6	Tanasa GYE	27
	Merchandising	Proesa GYE	5	Proesa GYE	18
	EZDs	Machala	1	Machala	3
	Genesis/	Manta	1	Manta	3
	S.Personal	Quevedo	1	Quevedo	3
	PLCs	Ibarra	1	Ibarra	3
	Secundario	Ambato	1	Ambato	3
	Intranet	Sto.Dom.	1	Sto. Domingo	3
	Tesorería	Cuenca	1	Cuenca	3
6	Archivos e	Esmeraldas	1	Esmeraldas	3
	impresoras	Loja	1	PM Perú	11
1	Respaldos	PM Perú	2	Bolivia	1
1	Aplicaciones CITRIX				
1	Perú				
<b>TOTAL</b>	<b>23</b>	<b>TOTAL</b>	<b>65</b>	<b>TOTAL</b>	<b>318</b>

Figura 2.2 Infraestructura tecnológica de datos del grupo ITABSA [15].

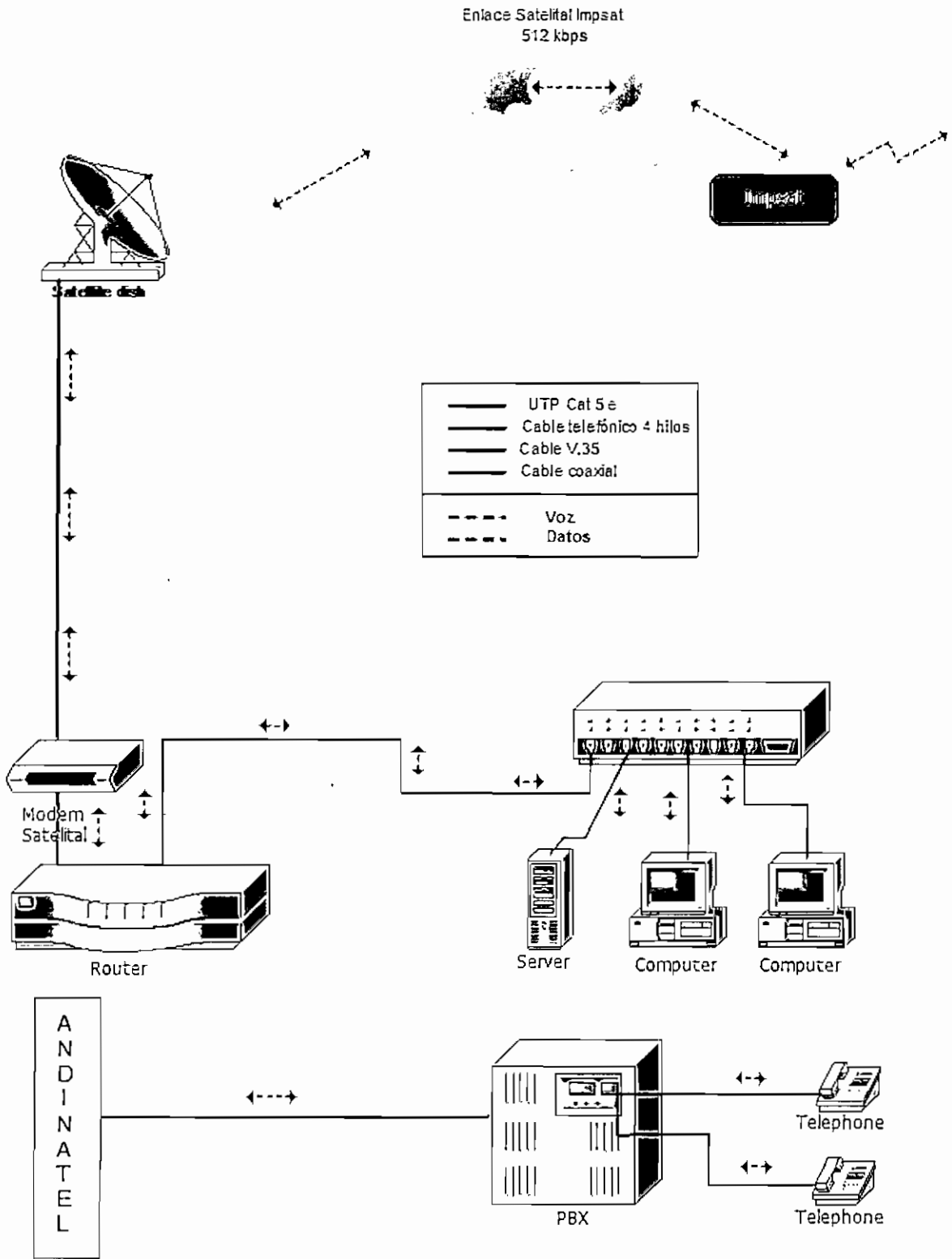


Figura 2.3 Enlace internacional [15].

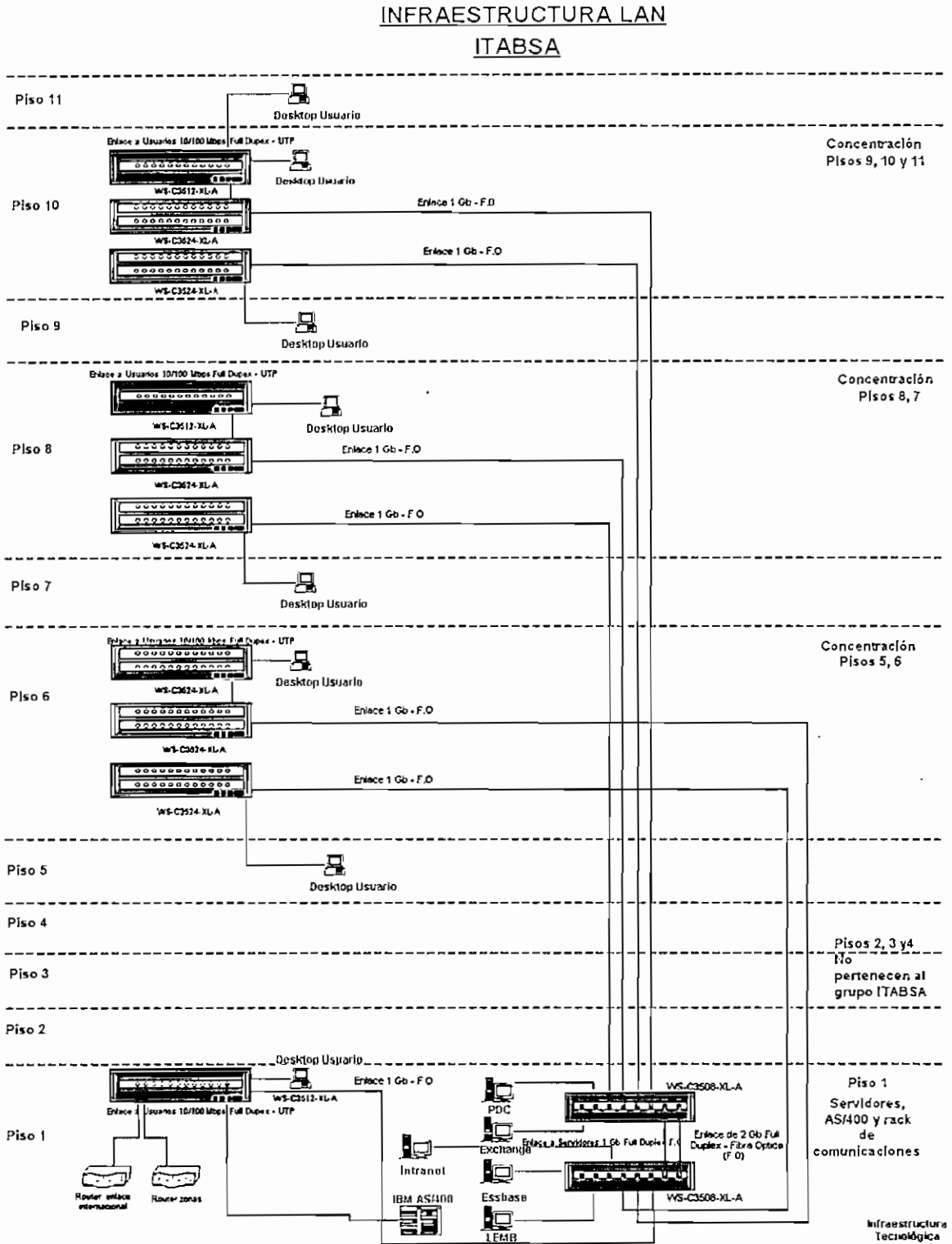


Figura 2.4 Infraestructura LAN ITABSA [15].

En el centro de cómputo de Belmonte, que se encuentra en el piso 1, se tiene un *router* para el enlace internacional y otro para los enlaces a las distintas zonas del país. Todos estos enlaces los provee Impsat. Existe un *switch* para los usuarios del piso 1. En el piso 10 se tiene un punto de concentración que consta de 3 *switches* para atender a los usuarios de los pisos 9, 10 y 11. Se dispone de un punto de concentración en el piso 8 para los usuarios de los pisos 7 y 8, este punto de concentración también posee 3 *switches*. Por último se tiene otro punto de concentración con 3 *switches* en el piso 6 para los usuarios de los pisos 5 y 6. Los pisos 2, 3 y 4 no los utiliza el grupo ITABSA, pertenecen a otra empresa. Esta distribución se la puede ver en la Figura 2.4.

En TANASA se tiene igualmente una red LAN Ethernet. Su hardware de conectividad consta de 1 *router* Cisco 1605R, 1 *router* Cisco 1750, 4 *switches* Cisco 3512, 6 *switches* Cisco 3524 y 1 *hub* 3Com, los cuales se emplean para dar servicio a los usuarios de la planta. Esta red utiliza como medio de transmisión cable UTP categoría 5e. TANASA, al ser una planta de producción cuenta con varios galpones donde se encuentran distribuidos los equipos de acuerdo a las fases de producción; además existe un lugar destinado al personal administrativo y otro donde se encuentra el comedor. En los galpones de producción existen puntos de red para las computadoras que controlan los sistemas. En la figura 2.5 se puede observar la red de TANASA.

Tanto la LAN como la WAN del grupo ITABSA poseen las características necesarias de ancho de banda para soportar los componentes y las transmisiones de tecnologías de convergencia de voz y datos sobre la red de datos existente. Es decir, una solución de telefonía IP es factible sobre la red actual. Además, los *switches* y *routers* existentes poseen las capacidades necesarias, tanto en puertos libres como en características tales como calidad de servicio y otras necesarias para que se pueda aplicar esta tecnología de manera óptima.

El sistema de cableado estructurado es de categoría 5e el cual está certificado y tiene cobertura total sobre las localidades en las que se realizará el diseño del sistema. Los centros de cómputo y cuartos de servidores presentan las

condiciones necesarias para el alojamiento de equipos; es decir, cumplen con las normas de temperatura y con suficientes tomas de fuerza para los equipos que se agregarán a los sistemas existentes. Las instalaciones eléctricas se encuentran en buenas condiciones. Además la empresa cuenta con sistemas de UPS (*Uninterruptible Power Supply*) para la totalidad de equipos existentes.

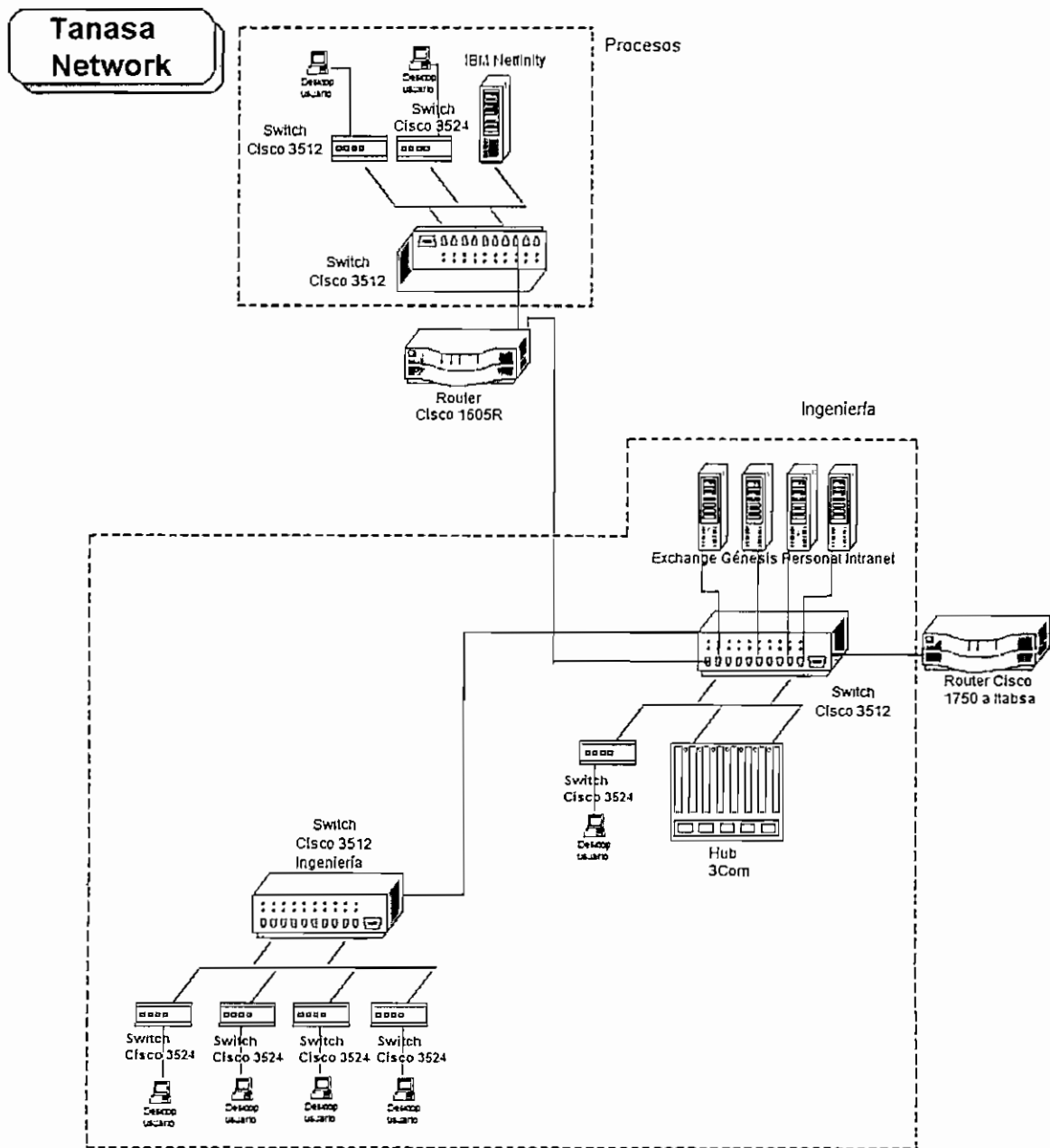


Figura 2.5 Infraestructura LAN TANASA [15].

En la parte de telefonía, el grupo ITABSA en la actualidad cuenta con varias centrales telefónicas analógicas y digitales distribuidas a nivel nacional. Esta arquitectura no es escalable y las centrales tienen varios años de funcionamiento por lo que ya no resultan suficientes para el correcto funcionamiento y para las perspectivas de crecimiento de la empresa. Para brindar el servicio que los usuarios requieren, sería necesaria la compra de nuevas centrales para dar soporte al crecimiento de usuarios. El disponer de centrales adicionales crearía dificultad en la interconexión de las mismas por la gran cantidad de marcas y modelos con las que se cuenta y limitando las funciones de las centrales ya que no todas son totalmente compatibles entre sí. Esto también dificulta la administración de los servicios de voz.

Una solución de telefonía basada en IP es una solución escalable, que permitirá, en un futuro, la implementación de esta tecnología a todas las zonas de la empresa. El diseño que se presentará permitirá la interconexión con el resto de las centrales telefónicas del grupo, así como con los elementos de *networking* necesarios para su funcionamiento.

Actualmente, tanto en TANASA como en ITABSA los *switches* que están en funcionamiento son *switches* de capa 3; sin embargo, no están realizando funciones de capa 3, por ejemplo, en la red no se realiza enrutamiento en VLANs ya que no están implementadas VLANs.

## 2.2 ALTERNATIVAS TECNOLÓGICAS

La telefonía tradicional al no ser escalable poco a poco va perdiendo territorio y quedando en desuso y tiende a ser reemplazada por nuevas tecnologías. El visionario de Internet Vinton Cerf en una entrevista al periódico El Mundo de España afirma que "VoIP terminará siendo tan natural como el correo electrónico" y que Internet integrará todas las comunicaciones. Al preguntarle si cree que VoIP acabará con la telefonía tal y como se la conoce hoy en día, el respondió que "no

tiene ningún sentido mantener redes separadas cuando hay capacidad y calidad suficiente para unificar las redes" [16].

Al momento son muchas las compañías que ofrecen equipo completo y servicio para tecnologías de voz sobre IP. Los grandes en redes como Cisco y 3Com toman muy seriamente el desarrollo de la telefonía IP y han dedicado áreas exclusivas al desarrollo de estos productos. Con la misma fuerza, compañías que durante décadas se han dedicado a la telefonía tradicional como Northern Telecom o Siemens están presentando al mercado sus propuestas para Telefonía IP.

### 2.2.1 ALTERNATIVAS DE IMPLEMENTACIÓN DE VoIP [17]

A continuación se analizarán tres diferentes escenarios que se pueden presentar al momento de implementar telefonía IP en una red corporativa privada. Éstos son:

- La voz se transmite sobre el mismo enlace virtual (PVC, *Private Virtual Circuit*) que los datos, utilizando fragmentación, intercalado, compresión de encabezados y priorizando el tráfico de voz frente a los datos. En este caso, se limita a los datos de tal manera que se deje un ancho de banda suficiente para la voz. Se definen límites de velocidad para un determinado tráfico de paquetes. En este caso, a los paquetes que se limita son a los de datos cuando éstos no cumplen con condiciones que previamente se establecen. Estas condiciones se define con parámetros como la tasa media de transmisión; todo tráfico que esté por debajo de este valor cumple con las condiciones. Otros parámetros son el tamaño de ráfaga máximo (*Normal Burst*) y el tamaño de una ráfaga adicional cuando el tamaño de ráfaga supera al normal (*Exceed Burst*).

Al momento de configurar los equipos para que funcionen de esta manera, se toman tamaños de *Normal Burst* y de *Exceed Burst* de tal manera que

se asegure que máximo un paquete de datos pueda anteponerse a un paquete de voz. De esta manera se obtiene una calidad de voz aceptable pero un retardo mayor al esperado (aproximadamente 200 ms).

- La voz se transmite sobre el mismo PVC que los datos, pero en este caso la única garantía que se da a la transmisión de voz es la priorización de paquetes de voz sobre los de datos. En esta alternativa se utiliza el método de gestión de colas LLQ (*Low Latency Frequency*, también llamado CB-WQF). Este tipo de priorización trabaja a nivel de capa 3.

Todos los paquetes se colocan en un *buffer* circular llamado "*transmit ring*" [17] donde esperan por su segmentación para ser transmitidos. Si un paquete de voz llega, éste es colocado al inicio de la cola de paquetes; sin embargo, al paquete de voz le toca esperar que sean liberados los paquetes que se encuentran en el *transmit ring*, lo que causa retardo. Por defecto, el tamaño de este *buffer* circular es 16 paquetes y el valor mínimo es 2. Por lo tanto, un paquete de voz tiene que esperar por lo menos que pasen 2 paquetes IP produciendo un retardo aproximado de 190 ms. Para bajar este retardo se puede disminuir el tamaño de la MTU (*Maximum Transfer Unit*) de los paquetes, con lo que se puede conseguir una disminución en el retardo de hasta 100 ms. Esto asegura una buena calidad de voz, sin embargo, puede producir problemas a nivel de aplicaciones IP.

- La voz y los datos se transmiten sobre dos PVCs distintos. Se crean dos PVCs por cada conexión entre *routers*, uno exclusivamente para la transmisión de voz y otro exclusivamente para la transmisión de datos. En esta alternativa de implementación, se posee un retardo de *jitter* aproximado de 70 ms, con lo que el retardo punto a punto alcanza un valor promedio de 115 ms, el cual es aceptable en las aplicaciones de voz sobre una red de conmutación de paquetes.



Ésta es una solución robusta, de simple configuración, escalable y de buen funcionamiento tanto en el servicio de voz como en el de datos. La desventaja que presenta es el hecho de que se deben mantener 2 PVCs por cada enlace entre *routers* lo que puede generar inconvenientes en la administración.

### 2.2.2 ALTERNATIVAS DE EQUIPO DE TELEFONÍA IP

Al hablar de alternativas tecnológicas, también es necesario referirse al equipo que se puede utilizar al momento de implementar telefonía IP. Se va a analizar dos alternativas de diferentes fabricantes, de acuerdo al equipo que cada uno de ellos ofrece. Más adelante, se ampliará la información de acuerdo a la alternativa que se escoja.

En el mercado ecuatoriano, Cisco es una marca que ha tenido gran acogida al momento de implementar redes de datos. Actualmente, Cisco ofrece equipos para la implementación de redes de convergencia de datos, voz y multimedia, y estos equipos presentan la fiabilidad que siempre ha caracterizado a esta marca.

Otra opción que se va a tomar en cuenta es el equipo para telefonía IP que ofrece Siemens. Siemens es una compañía con gran trayectoria en el área de las telecomunicaciones y especialmente en telefonía. Por la tendencia de convergencia de redes, esta compañía ha visto la necesidad de incluir entre su cartera de productos soluciones completas para la implementación de telefonía IP.

La cantidad de productos que se puede encontrar para la implementación de telefonía IP es amplia. Existen muchos fabricantes, cada uno con sus propias ventajas, con rangos de precios muy variables. Existen muchas opciones, pero se analizará a estos dos fabricantes mencionados anteriormente por su trayectoria en el mercado. El primero tiene mucha experiencia en *networking*, el segundo en telefonía, lo que permitirá realizar una comparación entre dos fabricantes en los

que su punto de partida es diferente, pero su meta es la misma: servicio de telefonía IP de alta calidad, que asegure la satisfacción del usuario, y además provea las ventajas de permitir transmisión de voz y datos sobre una misma red, lo cual es una ventaja al momento de administrar los servicios de comunicaciones dentro de una corporación.

### 2.2.2.1 Equipos para Telefonía IP Cisco

La solución de telefonía IP que contempla Cisco incluye:

- a) *Call Manager*
- b) *Cisco Unity Unified Messaging*
- c) *Gateway de voz*
- d) *Teléfonos IP*
- e) *Softphones*
- f) *ATAs (Analog Telephone Adaptor)*

#### a) *Call Manager* [18]

Cisco *Call Manager* es un componente basado en software para el procesamiento de llamadas al utilizar una solución de telefonía IP. Provee procesamiento de llamadas en telefonía IP, siendo escalable, distribuible y altamente disponible.

El software Cisco *Call Manager* provee a la telefonía corporativa características y capacidades para agrupar los dispositivos de telefonía IP como teléfonos IP, dispositivos de procesamiento de medios, *gateways* de VoIP, y aplicaciones multimedia. Servicios como datos adicionales, voz y servicios de vídeo, así como también mensajería unificada, conferencias multimedia, centros de contactos colaborativos, y sistemas multimedia de respuesta interactiva, pueden interactuar en una solución de telefonía IP a

través de los APIs (*Application Programming Interfaces*) del Cisco *Call Manager*.

El software Cisco *Call Manager* tiene utilidades y aplicaciones integradas de voz como Cisco *Call Manager Attendant Console* que es una consola para manejo de servicios; *Bulk Administration Tool* (BAT) para administración de aplicaciones de conferencias; el *CDR Analysis and Reporting* (CAR), *Real Time Monitoring Tool* (RTMT); *Tool for Auto-Registered Phone Support* (TAPS) y la aplicación *IP Manager Assistant* (IPMA).

Los servidores Cisco *Call Manager* están agrupados y se los puede manejar como una sola entidad. Su arquitectura distribuida permite mejorar la disponibilidad en el sistema, el balance de carga y la escalabilidad. Posee un sistema de control de admisión de llamadas que permite mantener alta calidad de servicio de voz en enlaces WAN.

Cisco *Call Manager* 4.1 permite a servidores y teléfonos IP la capacidad de verificar la identidad de los dispositivos o servidores que se están comunicando con él, asegura la identidad de los datos y su recepción, y permite realizar encriptación para proveer privacidad en las comunicaciones.

#### **b) Cisco Unity Unified Messaging [19]**

El Cisco *Unity Unified Messaging* es un poderoso servidor para la unificación de comunicaciones que provee la convergencia de los servicios de comunicaciones, integrándolos con las aplicaciones de negocios que utilizan los profesionales y trabajadores a diario. Esto permite mejorar el servicio al cliente y la productividad.

Cisco *Unity* permite que los usuarios puedan acceder y manejar sus mensajes, llamadas y *e-mails* desde cualquier parte y a cualquier momento, sin importar el dispositivo que se esté usando para acceder a los mismos. Los usuarios pueden escuchar sus *e-mails* por teléfono, o revisar sus mensajes de voz

desde Internet; también permite desviar los faxes a cualquier otra máquina de fax, siempre y cuando exista un servidor de fax. Las características de mensajería de voz incluyen ruteo inteligente y varias opciones para notificación de mensajes recibidos.

Este servidor es el complemento ideal en redes que proveen servicios de voz y datos. Provee una transición suave hacia telefonía IP y ayuda a proteger la infraestructura existente. Es escalable por lo que puede crecer de acuerdo a las necesidades.

Posee varias características útiles tanto para los usuarios como para el personal de informática. La principal ventaja para los usuarios es que poseen control centralizado de comunicaciones ya que todos los mensajes de voz, correo electrónico, y mensajes de fax se envían a la dirección de correo electrónico del usuario. La interfaz usada es amigable para el usuario porque le permite adelantar, retroceder o pausar cualquier mensaje. Además se puede acceder a los mensajes de voz y fax desde cualquier PC, a través de Internet o desde cualquier teléfono de tonos, y enviar mensajes de voz y fax a cualquier *mail*. Con un servidor de fax permite que los faxes recibidos se los pueda ver en pantalla o enviarlos a cualquier máquina de fax. Gracias al módulo *text-to-speech* (texto a hablado), se pueden escuchar los *e-mail* claramente a través de un teléfono, configurando el idioma en que se quiere que la aplicación los lea.

Para el personal de sistemas también existen beneficios, permite descentralizar la administración de las cuentas de usuarios porque son los usuarios mismos quienes se encargan del manejo de sus cuentas. Su interfaz de administración está basada en *browsers* lo que facilita su manejo. Se consigue una infraestructura de comunicaciones avanzadas integrando con Cisco *Call Manager* para la transición a telefonía IP. Esta arquitectura unificada permite al personal de informática realizar un solo procedimiento de *back up*, una sola política de almacenamiento de mensajes y una sola política de seguridad.

### c) *Gateway* de voz [20]

Cisco posee varios *routers* que prestan el servicio de *gateway* de voz. El *router* Cisco 3825 es un *router* de servicios integrados como seguridad y servicios de voz. Entre las características de este *router* se encuentran el procesamiento embebido de seguridad, memoria de alto desempeño, interfaces de alta densidad, telefonía IP, vídeo, análisis de red, aplicaciones web. La integración de tecnologías es transparente, provee comunicaciones empresariales seguras en un único sistema flexible.

Los servicios embebidos de voz que posee el *router* permiten máximo desarrollo, flexibilidad, así como alta densidad de estaciones, enlaces y conferencias. Ofrece la solución perfecta para la convergencia de redes de voz y datos. El *router* 3825 puede ser utilizado por empresas medianas y grandes, centraliza las comunicaciones IP, incluso con accesos remotos con el uso de SRST (*Survivable Remote Site Telephony*). SRST es un componente importante de la solución extremo a extremo que se ofrece para telefonía IP, que combinada con Cisco *Call Manager* provee alta capacidad de procesamiento de llamadas. Cisco SRST es un componente crítico dentro de una arquitectura centralizada de procesamiento de llamadas. Cisco lo ha diseñado para instalarlo junto con el IOS de los equipos Cisco.

### d) Teléfonos IP

Cisco tiene una gran variedad de teléfonos IP que se adaptan a las necesidades del cliente. Se analizará tres modelos de teléfonos IP: Cisco IP *Phone* 7912G, Cisco IP *Phone* 7940G, Cisco IP *Phone* 7960G y la estación para conferencias Cisco IP *Conference Station* 7936.

El teléfono Cisco IP *Phone* 7912G [21] está diseñado tanto para tráfico bajo como para tráfico medio, con características ideales para cualquier trabajador (figura 2.6). Es un teléfono de fácil uso con teclas de navegación que ayudan al usuario a encontrar las opciones y características que desea. Posee una

pantalla de capacidad gráfica que facilita la búsqueda de las opciones y provee información de las llamadas. Además, las aplicaciones XML (*Extensible Markup Language*) permiten el acceso a información y a datos de la red. Este teléfono tiene un *switch* ethernet integrado que permite la conexión a la LAN junto con una PC que ya exista con anterioridad, por lo tanto no se necesita puntos extras de red. También ofrece la posibilidad de *inline power*, lo que significa que puede recibir alimentación eléctrica a través de la red LAN.



Figura 2.6 Cisco IP Phone 7912G [21].

Este teléfono está diseñado para ser de fácil uso, posee una pantalla basada en pixels que tiene buena resolución, 4 teclas que permiten al usuario navegación dinámica ya que las opciones a las que se accede con estas teclas se presentan en la pantalla, por lo tanto cambian de acuerdo a la opción en que se encuentre; dispone también de una tecla de menú que permite el acceso a los registros de llamadas y a la configuración del teléfono como tonos de timbre y contraste de la pantalla. En pantalla se puede desplegar información sobre las llamadas perdidas, recibidas y realizadas. El teléfono permite la recuperación de mensajes de voz, llamada en espera y botón para el control del volumen. Soporta aplicaciones XML las cuales se despliegan en la pantalla.

El software que opera en este teléfono puede ser actualizado. Se puede presentar en pantalla el número y nombre de la persona a la que se llama y la que llama, es decir posee servicio de identificación de llamadas. Tiene llamada

en espera, desvío de llamadas, transferencia de llamadas, conferencias tripartita, remarcado y *speaker* (no posee micrófono, solo alto parlante).

El teléfono Cisco IP *Phone 7940G* [22] igualmente está diseñado para tráfico bajo y medio. Este teléfono da la posibilidad de cuatro llamadas simultáneas, posee cuatro botones dinámicos que guían al usuario al acceso de las características de las llamadas y sus funciones. Este teléfono, como se puede observar en la figura 2.7, posee una amplia pantalla de alta capacidad gráfica en la que se presentan datos como fecha y hora, contador de tiempo de las llamadas y números marcados.



Figura 2.7 Cisco IP *Phone 7940G* [22].

Las capacidades de sistema de este teléfono pueden crecer mediante la actualización del software instalado en el mismo. Posee diferentes métodos de acceso a las variadas opciones que ofrece este teléfono, botones dinámicos, teclas de navegación, y acceso directo con el uso de dígitos correspondientes a cada uno de estos accesos.

El teléfono Cisco IP *Phone 7940G* identifica los mensajes de entrada y los presenta en pantalla por nombre o número al que pertenece el mensaje; esto brinda al usuario facilidad, eficiencia y rapidez de búsqueda. Permite retornar las llamadas usando la característica *direct dialback* (remarcado directo). Provee acceso al directorio corporativo utilizando el protocolo LDAP3

(*Lightweight Directory Access Protocol 3*, Protocolo liviano de acceso al directorio 3).

Existe un botón para configuración de características que permite al usuario ajustar el contraste de la pantalla, volumen, tono de timbrado, auriculares y micrófono. Las especificaciones de configuración de red normalmente las realiza el administrador del sistema, pero también permite especificar estas preferencias desde el mismo teléfono. La configuración también puede ser manual o automática usando DHCP (*Dinamic Host Configuration Protocol*), TFTP (*Trivial File Transfer Protocol*) y Cisco Call Manager.

El usuario tiene acceso a cualquier información basada en web proporcionada por el administrador del sistema como información sobre el clima, valores de bolsa, o cualquier otra información de importancia para la empresa utilizando XML. En la pantalla también se puede desplegar información sobre ayuda en línea acerca del uso de los botones y las características.

Se lo puede usar como un teléfono manos libres de dos vías ya que tiene micrófono y alto parlante, y un botón para silenciar el micrófono; tanto el botón de encendido y apagado del *speaker* como el de silenciar poseen LEDs para indicar si están activados.

El *switch* Ethernet incorporado de dos puertos permite la conexión del teléfono y la PC usando un sólo punto de red, pero dejando la posibilidad de colocar en diferentes VLANs (*Virtual LANs*) al computador y al teléfono, esto dependerá de la forma de administración de red que se aplique.

Las características físicas del teléfono están diseñadas para la completa comodidad del usuario, por lo que su inclinación puede variar de cero a sesenta grados para que la visualización de la pantalla y el acceso a los botones sean adecuados de acuerdo a las necesidades del usuario. Permite alimentación eléctrica a través de la LAN, siempre y cuando la LAN posea estas características.



Para seguridad adicional en el tráfico de voz tiene implementado un proceso de enmascaramiento de tonos DTMF (*Dual-tone multifrequency*). Soporta métodos de compresión de audio G.711 y G.729a, compatibilidad con el protocolo H.323 y Microsoft *NetMeeting* y un puerto EIA/TIA RS-232 para opciones que se quiera añadir en un futuro.

El teléfono Cisco IP *Phone* 7960G [23] posee características que lo hacen adecuado para el uso de ejecutivos y gerentes ya que da la posibilidad de seis líneas programables y un sistema telefónico manos libres de dos vías de alta calidad. Posee cuatro botones dinámicos para acceso a las características de las llamadas y funciones. Tiene un puerto integrado para auriculares e incorporando un *switch* Ethernet. La pantalla con la que cuenta este teléfono es LCD como se puede ver en la figura 2.8 y en ella se presentan datos, número y nombre de llamadas entrantes y salientes. La capacidad gráfica permite la inclusión de XML. El teléfono Cisco IP *Phone* 7960G tiene soporte multiprotocolo como H.323, SIP (*Session Initiation Protocol*), y MGCP (*Media Gateway Control Protocol*).



Figura 2.8 Cisco IP *Phone* 7960G [23].

El software de este teléfono se lo puede actualizar. Provee varios métodos de acceso de acuerdo a las preferencias del usuario. Incluye botones con íconos para accesos directos, botones dinámicos y teclas de navegación. Como se puede ver en la figura 2.9 existe una tecla para acceso directo a mensajes de voz y para la lectura de *e-mails* directamente en la pantalla del teléfono.

Identifica los mensajes recibidos y los categoriza por usuario en la pantalla, y gracias a *dial-back* el usuario puede devolver una llamada fácilmente. Existe un botón de acceso directo para configuración de características como contraste y tonos de timbrado, volumen tanto para el auricular y el teléfono manos libres. De esta misma tecla se puede acceder a configuración de red, que también puede ser asignada usando DHCP, TFTP y Cisco *Call Manager*. También tiene una tecla de acceso directo a información obtenida de la red basada en web usando XML.

El botón de ayuda presenta información útil para el usuario sobre el funcionamiento del teléfono. Los botones para encendido y apagado de manos libres y el botón del silenciador del micrófono también son de acceso directo.

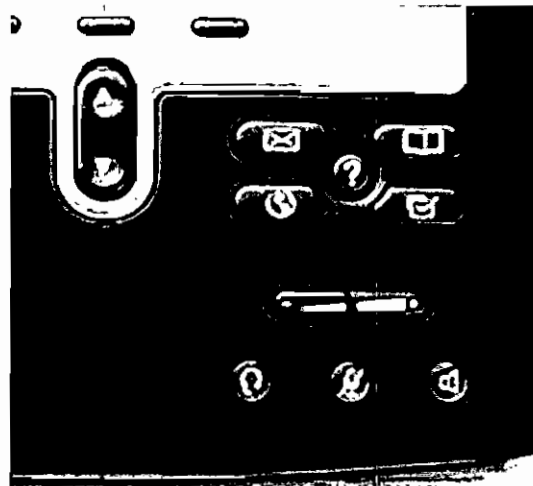


Figura 2.9 Botones de acceso directo [23].

El *switch* Ethernet que se encuentra integrado al teléfono tiene dos puertos para que no sea necesario más de un punto de red para poder conectar el teléfono y la PC, en donde la PC ya se encontraba localizada. Tanto la PC como el teléfono pueden colocarse en VLANs independientes.

Al igual que el Cisco IP *Phone* 7940G, el nivel de inclinación del teléfono es ajustable y va desde cero a sesenta grados, esto permite que el usuario lo coloque de tal manera que su visibilidad a la pantalla sea adecuada. Como

una característica de seguridad adicional, este teléfono posee enmascaramiento de tonos DMTF. Los métodos de compresión de audio que utiliza son G.711 y G.729a.

El control de configuración de red se lo puede hacer desde el teléfono; esta configuración puede ser manual o automática utilizando DHCP. Este teléfono permite añadir módulos para diferentes propósitos, como se puede observar en la figura 2.10, por ejemplo para directorio adicional con mayor capacidad y mayor facilidad de manejo.



Figura 2.10 Cisco IP Phone 7960G con módulo añadido [23].

Cisco *Conference Station* 7936 [24] es una estación de conferencias con importantes características, basado en IP, manos libres que ofrece superior calidad de voz y micrófono, muy útil en salas de conferencia. Además se puede añadir a esta estación micrófonos externos extras ya que posee puertos para micrófonos externos, parlantes o una pantalla LCD adicional.

Esta estación de conferencias ofrece excepcional calidad de voz, elimina ecos y palabras truncadas lo que permite una conversación más natural, además los parlantes tienen afinación digital mejorando la calidad del sonido; posee tres micrófonos que minimizan el sonido de *background*, esto permite que los participantes de la conferencia se muevan alrededor de la sala mientras hablan sin que esto afecte en la calidad de la conversación. Se puede observar el Cisco IP *Conference Station* 7936 en la figura 2.11.

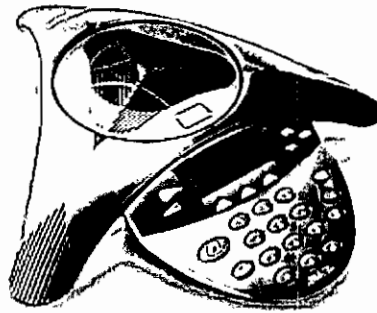


Figura 2.11 Cisco IP *Conference Station* 7936 [24].

El teclado de este módulo de conferencia telefónica posee tres botones dinámicos y dos botones de navegación. En la pantalla LCD que posee se presenta información como fecha y hora, números marcados, tiempo de duración de las llamadas y características y estado de la línea.

Las características de esta estación de conferencias incluyen llamada en espera, transferencia de llamadas, liberación de llamadas y silenciador. Permite conversaciones naturales en dos vías sin recortes o distorsiones ya que la operación es *full duplex*; el sistema se adapta automáticamente a los cambios en las condiciones acústicas de la sala. Los tres micrófonos ofrecen cobertura a los 360° de la sala con igual intensidad de voz sin importar la posición del hablante.

La configuración de dirección de red se la puede hacer utilizando DHCP o asignando una dirección estática; la conexión es simple ya que solo necesita un punto de red Ethernet 10/100. Posee auto configuración de número telefónico, imágenes de software y características personalizadas usando Cisco *Call Manager*.

### **e) *Softphone***

El *softphone* que Cisco pone en el mercado es el Cisco IP *Communicator* [25]. Ésta es una aplicación basada en software que brinda soporte avanzado para telefonía a través de computadores personales. Esta aplicación da a las computadoras la funcionalidad de teléfonos IP. La utilidad de esta aplicación

es que provee llamadas de alta calidad desde cualquier lugar en donde se tenga acceso a la red corporativa. Las ventajas son muchas, principalmente cuando un usuario se encuentra de viaje, es como si se llevara su extensión telefónica con él, y posee los mismos servicios telefónicos que posee en su oficina.

Cisco IP *Communicator* usa el sistema de procesamiento de llamadas Cisco *Call Manager* lo que le da características avanzadas de telefonía IP. Tiene todas las características de un teléfono IP Cisco, esto es llamada en espera, transferencia de llamadas y conferencias. Maneja una interfaz similar al teclado de un teléfono IP Cisco, como se puede ver en la figura 2.12, lo que hace que su uso sea más familiar para el usuario.

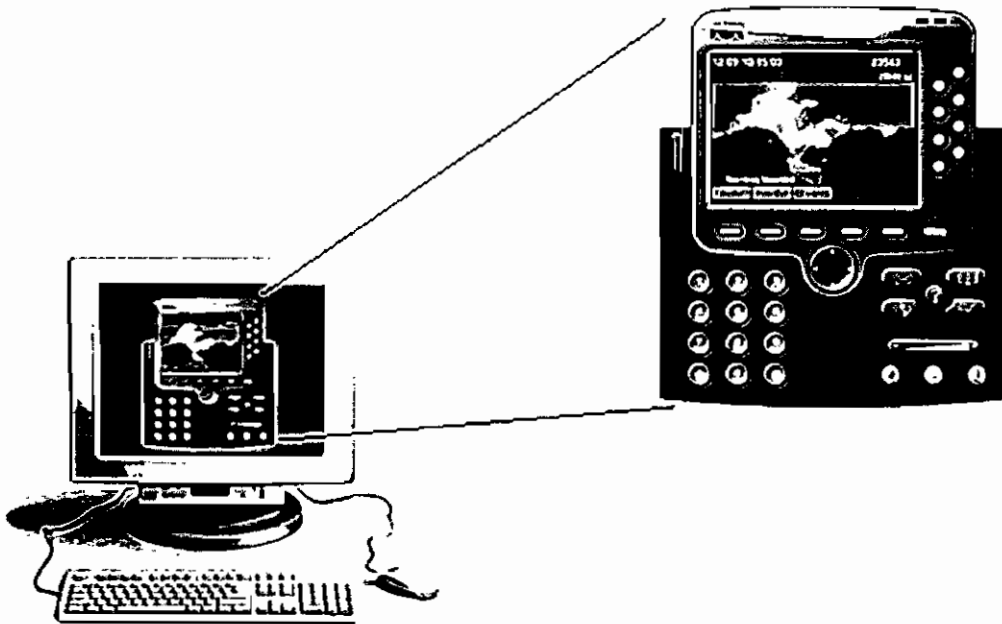


Figura 2.12 Cisco IP *Communicator* [25].

En la interfaz de la aplicación se puede observar botones que dinámicamente presentan opciones de características de las llamadas y botón para acceso directo a mensajes de voz. También da la opción de acceso al directorio telefónico usando el protocolo LDAP3, configuraciones de tonos de timbrado e imágenes de fondo y servicios de información basados en web.

Cisco IP *Communicator* puede trabajar en tres modos diferentes. El primero es el modo *headset* (auricular) con lo que se consigue alta calidad de voz. El segundo modo es *handset* (microteléfono), en el que se conecta un aparato telefónico vía USB para realizar y recibir las llamadas. El tercer modo es manos libres, en el que la computadora se convierte en un teléfono manos libres *half duplex*.

La buena calidad de audio que ofrece Cisco IP *Communicator* se debe a que posee sintonizador de audio, *buffer* para supresión de *jitter*, cancelación de ruido, supresión de eco, detección de actividad de voz, supresión de silencios y prioridad de audio.

Dentro de las características de red que posee Cisco IP *Communicator* se puede enunciar que toma los parámetros de red que necesita utilizando DHCP. La compresión de audio soporta los protocolos G.711, G.711a, G.729 y G.729a y codificación de audio de banda ancha.

Los requerimientos computacionales mínimos son Windows 2000 Professional o superior, Pentium III de 450 MHz, 128 MB en memoria RAM, 100 MB de espacio en disco, tarjeta de sonido Non-ISA full duplex, tarjeta de vídeo 800x600x16bit o superior y conexión de red mínima de 128 Kbps.

#### **f) ATAs (*Analog Telephone Adaptor*)**

El Cisco ATA 186 [26] es un adaptador de teléfono analógico a teléfono IP. Posee dos puertos de voz para dos teléfonos independientes, cada uno con su propio número telefónico. Esta solución es muy útil para equipos de fax. Se lo puede observar en la figura 2.13.

Permite configuración automática de características de red utilizando DHCP, o también se puede configurar manualmente. Se puede acceder a la configuración vía web lo que facilita este proceso, pero también existe la opción de configurar el ATA utilizando el teclado de cualquiera de los teléfonos

conectados a los puertos de voz. El administrador puede ingresar un *password* para proteger el acceso a la configuración.

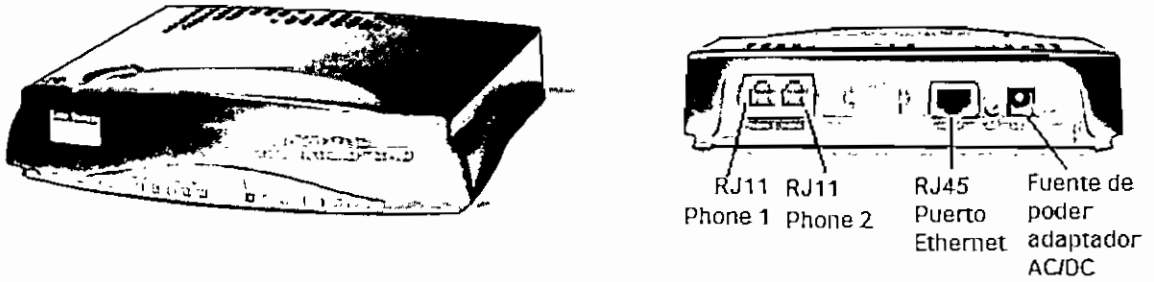


Figura 2.13 Cisco ATA 186 [26].

La calidad de voz que se tiene al utilizar Cisco ATA es muy buena ya que el pre-procesamiento de compresión de voz para conversaciones *full duplex* es avanzado. Adicionalmente, su desempeño en funciones como cancelación de eco, eliminación de ruido y reflexión de sonido, supresión de silencios es significativo. Soporta los protocolos H.323 y SIP, y los estándares de compresión de voz G.711, G.711a, G.723.1 y G.729a.

### 2.2.2.2 Equipos para Telefonía IP Siemens

Como se había mencionado previamente, Siemens es una empresa líder en el mercado de telefonía. Por esta razón se ha decidido analizar el equipo que ofrece este fabricante para servicios de telefonía IP.

La arquitectura que propone Siemens para telefonía IP comprende:

- a) Servidor de voz sobre IP HiPath 5500
- b) Gateway Siemens RG2500
- c) Opticlient 360
- d) Teléfonos IP

### a) Servidor de voz sobre IP HiPath 5500

Físicamente, es un servidor Siemens Primergy RX100 S2 con un procesador Pentium 4 de 800 MHz, 256 MB de memoria SDRAM, dos discos de 80 GB. A estos discos se les pone a trabajar en espejo para tener respaldo de los datos almacenados. En este servidor se dispone la aplicación HiPath 5500 encargada de validar y controlar el ancho de banda del sistema y el manejo de usuarios; es decir, esta aplicación funciona como el *gatekeeper* del sistema. En la figura 2.14 se puede observar el servidor Siemens Primergy RX100 S2.

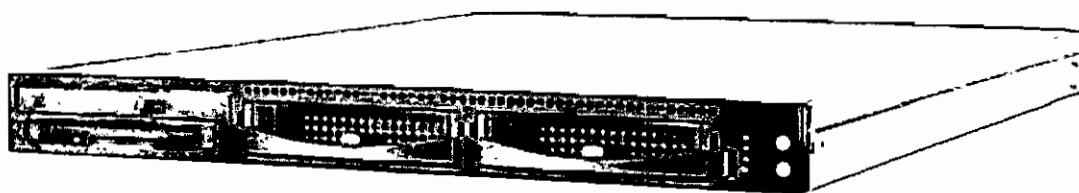


Figura 2.14 Servidor Siemens Primergy RX100 S2 [27].

El sistema HiPath 5500 se configura y administra mediante una interfaz WBM (*Web Based Management*) mediante el puerto 8085. Aquí se fijan los valores de ancho de banda correspondiente a cada usuario, las características de asignación de extensiones, direcciones IP y prefijo de enlace para comunicarse con la PSTN.

La configuración es sencilla, después de las configuraciones generales de características de red, se crean los usuarios del sistema, la extensión asignada y se **habilitan** las opciones de llamada que cada usuario posee. Con estos pasos queda configurado el servidor de VoIP.

El sistema además permite realizar pruebas de conexión entre el servidor y el *gateway*, lo que es indispensable para el correcto funcionamiento del sistema. Además esta aplicación permite ofrecer servicios de mensajería unificada.



### b) Gateway Siemens RG2500

Este equipo permite enlazar el ambiente LAN con la PSTN. Este *gateway* posee interfaz Ethernet, interfaces ISDN y puerto serial para programación del equipo mediante consola. El *gateway* Siemens RG2500 permite que la búsqueda de los canales libres sea de forma circular, es decir, se busca el siguiente canal libre disponible para establecer una comunicación.

La configuración de este equipo primeramente se la realiza por consola utilizando el puerto serial, aquí se definen los parámetros básicos de red como son dirección IP, máscara e identificación. Posteriormente se puede acceder al *gateway* por *Web Based Management*, que es un modo de configuración basado en web, utilizando el puerto 8085.

Utilizando la interfaz WBM se configuran los parámetros H.323, definiendo prioridad en los codificadores de voz a ser utilizados. Aquí también se define un prefijo que utilizarán los usuarios para realizar llamadas a través de la PSTN y el plan de discado. Esta configuración es muy importante porque es la que permite que las llamadas entrantes lleguen a su destino y que los usuarios de telefonía IP dentro de la empresa puedan realizar sin problemas llamadas a la red pública.

### c) Opticlient 360

El software Opticlient es un *softphone* que se lo instala en cada uno de los computadores de los usuarios. A cada una de las estaciones se le asigna una dirección IP. Este software permite la comunicación entre el computador del usuario y el *gateway*, lo que implica que el *gatekeeper* también reconocerá a cada uno de estos usuarios.

El usuario Opticlient 360 ofrece importantes características tales como: transferencia de llamadas, llamada en espera, opción de dos llamadas

simultáneas permitiendo el intercambio de llamadas entre los dos usuarios y conferencias. También ofrece la posibilidad de mantener directorio telefónico, acceso directo a correo electrónico, al explorador de Internet y a ayuda en línea.

Éste es un software de fácil operación, con una interfaz amigable con el usuario como se puede observar en la figura 2.15 y con las opciones de telefonía necesarias para cualquier trabajador de una empresa. Pero sobre todo cumple con la meta de integrar las comunicaciones sobre una sola red.

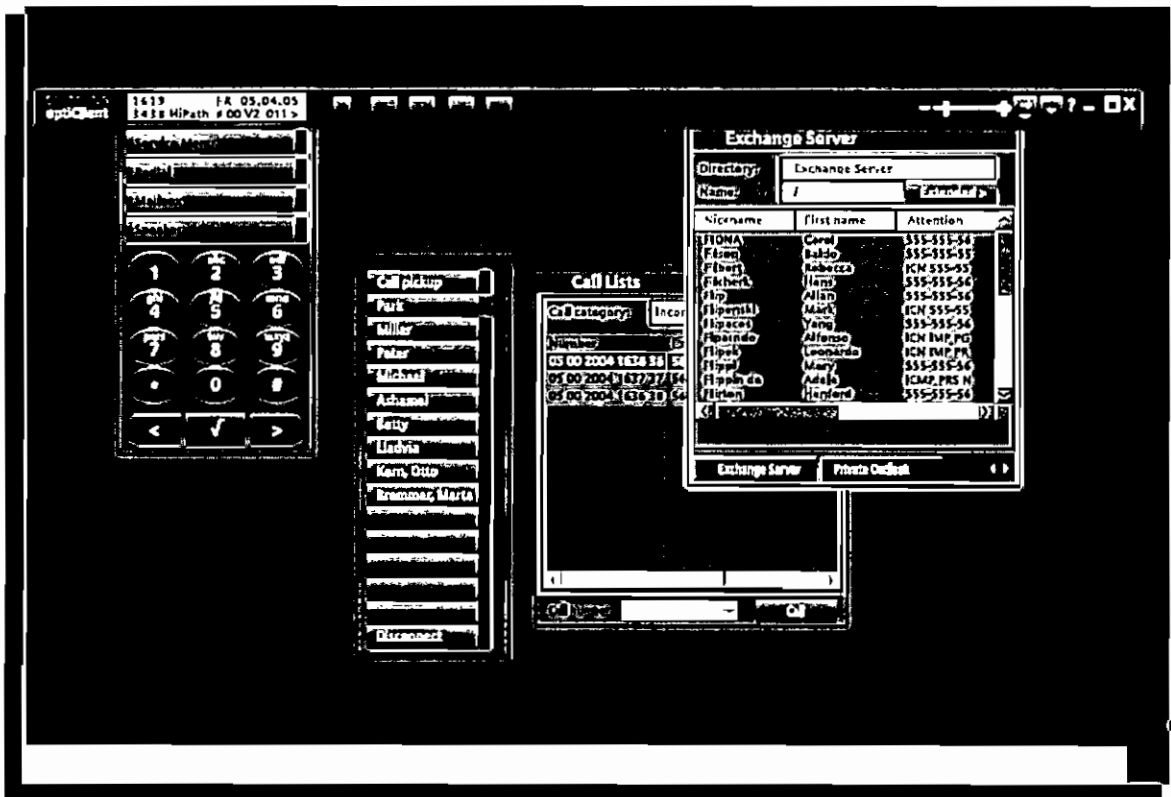


Figura 2.15 Siemens Opticlient [27].

#### d) Teléfonos IP

La gama de teléfonos IP que Siemens pone a disposición en el mercado busca la alta versatilidad para el uso corporativo de telefonía IP. Se va a presentar dos modelos de teléfonos, Optipoint 420 y Optipoint 600.

El teléfono Optipoint 420 [27] es un teléfono IP versátil que soporta múltiples protocolos. Los botones de este teléfono permiten que sea el usuario o el administrador de la red quien asigne la función de cada uno de sus 12 botones. Existe una pequeña pantalla al lado de cada botón para indicar la funcionalidad de cada uno. La programación de cada botón puede ser manual, lo cual es tedioso, o cargando archivos de configuración desde el servidor, lo que facilita el proceso y da uniformidad a todos los teléfonos de la compañía. Gracias a esta característica, el teléfono Optipoint 420 se ajusta a las necesidades personales de cualquier empresa.

El teléfono Siemens Optipoint 420 posee una pantalla alfa-numérica que permite observar la funcionalidad de los botones dinámicos del teléfono. Se puede colocar un módulo extra con botones igualmente programables. Este teléfono es manos libres *full duplex*. La figura 2.16 muestra el teléfono IP Optipoint 420.



Figura 2.16 Siemens Optipoint 420 [27].

Este teléfono trae un *switch* Ethernet integrado para permitir la colocación de estos teléfonos junto a la computadora del usuario sin ser necesario un punto de red adicional; este equipo soporta VLANs. Dispone de alimentación eléctrica a través de la red LAN, siempre y cuando exista esta característica dentro de la red que se está usando. Además posee un puerto USB. Este teléfono está diseñado para trabajar con el sistema Siemens HiPath (series 3000, 4000, 5000 y 8000).

El teléfono Optipoint 600 posee características que lo hacen adecuado para gerentes y personal que tienen alto uso de servicios de telefonía. Este teléfono soporta configuraciones tanto para voz sobre IP como para teléfono convencional para la red de conmutación de circuitos. Posee las mismas características que el teléfono Optipoint 420, pero con algunas características adicionales como una pantalla mucho más grande *touch screen* y soporta varios tipos de protocolos web (WAP, HTTP, LDAP) y un puerto para conexión de auriculares.



Figura 2.17 Siemens Optipoint 600 [27].

El teclado de este teléfono lo puede programar el usuario o el administrador de red cargando archivos con las especificaciones de la funcionalidad de cada botón. También permite la actualización del software vía FTP.

Este teléfono posee un *switch* Ethernet para poder utilizar el mismo punto de red de la conexión de un computador para el teléfono. El hecho de que en la pantalla del teléfono se pueda desplegar cualquier tipo de información HTML permite a los usuarios ingresar a información de la intranet y al Internet. Tiene acceso al directorio corporativo usando el protocolo LDAP. La asignación de una dirección de red se la puede hacer utilizando DHCP.

Como características importantes de este teléfono se puede mencionar que el volumen de tonos y el contraste de pantalla se lo puede regular con los botones que posee bajo el teclado numérico. Además posee JAVA Virtual Machine con SDK para el desarrollo de aplicaciones en JAVA. Permite

identificar las llamadas entrantes y los números marcados, y agenda electrónica.

### 2.2.3 ANÁLISIS COMPARATIVO DE ALTERNATIVAS PRESENTADAS DE EQUIPO DE TELEFONÍA IP

Cisco es un líder mundial en redes de datos IP, y al momento, también en hardware y software para telefonía IP. Cisco usa sus conocimientos y su experiencia en comunicaciones para ofrecer un nuevo reto en las compañías: la convergencia de redes de datos y voz. A diferencia de los servicios telefónicos analógicos tradicionales, la telefonía IP divide las conversaciones de voz en paquetes digitales separados. Cada día son más las compañías que se suman al grupo que usan los productos Cisco para telefonía IP para eliminar sus PBX propietarias basadas en conmutación de circuitos. Realmente la telefonía analógica dentro del ambiente corporativo se ha vuelto costosa, inflexible, redundante e innecesaria ya que existen tecnologías mucho mejores que vienen a reemplazarla.

La arquitectura Cisco para integración de voz, vídeo y datos (AVVID, *Architecture for Voice, Video and Integrated Data*) provee una infraestructura basada en estándares para la convergencia de redes. Comunicaciones IP Cisco es el nombre que Cisco ha dado a sus tecnologías para comunicaciones de tipo empresarial.

Las comunicaciones IP Cisco permiten a las compañías consolidar todas las comunicaciones en una sola red, ayudando a bajar los costos de infraestructura y de administración, además de aumentar la productividad de los trabajadores que se desenvuelven día a día con este tipo de infraestructura convergente.

Los mecanismos de alta calidad de servicio implementados en los productos Cisco para telefonía IP aseguran una calidad de voz igual e incluso mejor a la de los servicios de telefonía tradicionales. Y ya que el servicio de telefonía opera en

una red integrada, los usuarios se benefician de la flexibilidad y productividad de usar aplicaciones multimedia con los teléfonos que poseen a su disposición.

La gran ventaja de Cisco es que provee una amplia serie de aplicaciones que trabaja en conjunto con los equipos de telefonía IP Cisco. Un ejemplo de esto es Cisco *Unity* que ayuda al usuario en el manejo de sus mensajes que provengan de cualquier dispositivo que puede ser de otro teléfono, de fax, *email* o un buscapersonas.

Como se puede entender, Cisco es una compañía solidamente establecida en el campo de *networking* por la gran fiabilidad de sus productos, la constante innovación que estos productos tienen y el respaldo que da a sus clientes.

Sin embargo, debido al gran apogeo que la tecnología de telefonía IP ha tenido en los últimos tiempos, muchas empresas han visto la necesidad de invertir esfuerzos en la investigación y desarrollo de carteras de productos que brinden una solución completa para la implementación de telefonía IP en el ambiente corporativo.

Siemens al ser una empresa líder en productos para telefonía, no podía quedarse atrás viendo como las tecnologías IP poco a poco iban entrando y apoderándose de su mercado. Por esta razón, desde hace algunos años Siemens ya brinda soluciones completas para la integración de redes de voz sobre redes de datos, y de esta manera, seguir presentes en el campo de la telefonía.

Siemens *Communications* es uno de los mayores representantes en la industria de las telecomunicaciones alrededor del mundo, se encuentra presente en más de 160 países. Siemens siempre ha marcado su fortaleza en cada segmento de mercado en el que ha entrado, y la telefonía IP no ha sido la excepción.

Siemens *Communications* ofrece un portafolio completo de hardware y software desarrollado específicamente para telefonía IP. El concepto que esta empresa

maneja es la innovación en las tecnologías de comunicaciones, haciéndolas más fáciles y efectivas.

Como se detalló anteriormente, ambas compañías poseen todo el equipamiento necesario para la convergencia de la red de voz con la red de datos dentro del grupo ITABSA. Pero en este momento hay que tomar en cuenta los lineamientos internacionales que *Philip Morris International* impone a todas sus afiliadas y la red actual que posee la compañía.

Actualmente el grupo ITABSA posee una red que mayoritariamente utiliza equipos Cisco. Tanto *routers* como *switches* que actualmente operan en la red de datos del grupo ITABSA pertenecen a Cisco Systems.

De acuerdo a las características analizadas de cada equipo Cisco, necesario para la implementación de telefonía IP, se puede observar que cumplen con las expectativas que tiene el grupo ITABSA al migrar a este tipo de tecnología. Son equipos robustos, confiables, que ofrecen gran soporte tanto para el usuario como para los administradores de red.

La razón por la que la infraestructura de la red actual está basada en equipos Cisco es por uniformidad con el resto de afiliadas a *Philip Morris International* en el mundo. Por este motivo, se ha visto que la mejor opción es optar por equipo Cisco para la implementación de telefonía IP. Así no se tendrá problemas de compatibilidad con la red de datos que funciona actualmente.

### 2.3 CONSIDERACIONES DE DISEÑO [28]

Una pieza clave en la implementación de telefonía IP es la infraestructura de *switching*. A continuación se va a hablar de los elementos más críticos a tener en cuenta en la infraestructura LAN de tal manera que al momento de implementar telefonía IP no exista problemas.

### 2.3.1 MODELO DE CAPAS

El modelo clásico de *switching* ha sido el modelo de dos capas que son *core* y acceso. Debido a la demanda de mejoras se introdujo el modelo de tres capas, que considera las capas de *core*, distribución y acceso. Este modelo de tres capas se puede implementar gracias a la existencia de los llamados *switches* de capa tres, que no son más que *switches* que permiten adicionalmente realizar algunas opciones de enrutamiento entre VLANs. En el modelo de dos capas, las funciones de acceso y distribución están unificadas en la capa de acceso. La principal característica de los modelos por capas constituye su jerarquía.

Cada capa se dedica a su rol específico, por lo que el crecimiento de la red se lo puede realizar de manera ordenada y esto simplifica la búsqueda de errores. Al tener bien definidas las capas de *core*, distribución y acceso se puede balancear de mejor manera las cargas, así como organizar de mejor manera las conexiones a los servidores; además la creación de VLANs permite separar la LAN de acuerdo a las necesidades de la red, dando mejores características de seguridad.

Algo a tomar en cuenta en modelos de tres capas es el diseño de los *uplinks*, el cual se lo hace sobre un cierto valor de sobre-suscripción. Es necesario entender este concepto para tomar las medidas de precaución necesarias para que el tráfico de tiempo real no se vea perjudicado por el resto de aplicaciones de la red. No hay que olvidar que gran parte del desempeño de la red depende de la capacidad de los *uplinks*, que complementado con buenas políticas de calidad de servicio proporciona buena calidad de tráfico en tiempo real.

### 2.3.2 SPANNING TREE PROTOCOL

Debido a que la naturaleza de la telefonía IP es tráfico en tiempo real, cualquier perturbación que se tenga en la red afectará directamente en la calidad de voz. El protocolo *Spanning Tree* juega un rol primordial para mantener la red estable, por eso es importante que se implemente RSTP (*Rapid STP*, 802.1w). Al implementar



RSTP se puede mantener los tiempos de convergencia por debajo de los dos segundos. Para activar RSTP en los *switches* Cisco de la familia 3500 se lo hace desde el modo global, de la siguiente forma:

```
SW(config)# spanning-tree mode ?
    mst          Multiple spanning tree mode
    pvst         Per-Vlan spanning tree mode
    rapid-pvst   Per-Vlan rapid spanning tree mode
SW(config)# spanning-tree mode rapid-pvst
```

En la configuración anterior se puede observar que los modos de configuración de *spanning tree* que ofrecen los *switches* Cisco 3500 son MST, PVST y RPVST. Al escoger RPVST se está implementando el protocolo *Rapid Spanning Tree Protocol*. La ventaja de este protocolo es la rápida transición entre los estados de los puertos. RSTP permite confirmar si es seguro que un puerto pase al estado *forwarding* sin tiempo de espera antes de pasar a este estado.

Otra configuración necesaria que se debe realizar en todos los *switches* de la red es la de filtrar las VLANs para que no se propaguen por todos los *uplinks*; de esta manera, no se sobrecargará a los *switches* de acceso con los BPDU de todas la VLANs de la red. A continuación se mostrará la configuración en los *uplinks* de todos los *switches*:

```
SW config-if)# switchport trunk allowed ?
    Vlan          Set allowed vlans when interface is in
                  , trunking mode
SW(config-if)# switchport trunk allowed vlan 10,20
```

En la configuración antes mostrada, lo que se hace es habilitar la opción de *trunk* en las VLANs. La información sobre las VLANs se encuentra en la base de datos de cada *switch*, y si se activa la opción de *trunk*, la información sobre las VLANs no se pasa de un *switch* a otro. Esta opción se habilita a una VLAN en específico;

a las VLANs se las reconoce por su nombre, en este caso se está habilitando esta opción para las VLANs 10 y 20.

Algo que también es importante tener en cuenta es que cuando se hace la numeración de las VLANs y se las asigna a un servicio particular (voz, datos, vídeo), siempre es mejor asignar los VLAN Id más bajos a los servicios de telefonía IP. Esta recomendación se la hace debido a que internamente el IOS (Sistema operativo que opera en los equipos Cisco) cuando realiza las operaciones del servicio STP, siempre empieza por los VLAN Id menores. Al realizar esta operación se conseguirá que las VLANs de telefonía converjan más rápido que las de datos; hay que recordar que en telefonía 50 ms hacen diferencia.

### 2.3.3 VTP (VLAN TRUNK PROTOCOL)

VTP es un protocolo de mensajes de capa 2 que mantiene la consistencia de la configuración de las VLANs que maneja el aumento, eliminación y mantenimiento de las mismas. VTP es un protocolo propietario de Cisco. Este protocolo se utiliza para propagar a toda la infraestructura de red la inclusión o eliminación de las VLANs disponibles en un dominio. Esto es muy útil al momento de la administración del mantenimiento de las VLANs, aunque genera un poco de tráfico adicional.

En el caso de existir muchas VLANs es mejor definir VTP en modo transparente. De esta manera se debe crear las VLANs necesarias en cada uno de los *switches* individualmente; así no se sobrecargará el CPU del *switch* que funcionaría como VTP Server.

Pero si por razones administrativas se prefiere centralizar la administración de las VLANs desde el *switch* de *core* de la red entonces se debe tomar la precaución de hacer *pruning*. VTP *pruning* mejora el uso del ancho de banda de la red reduciendo el tráfico innecesario que se envía a todos los *switches* (*flooding*).

Este tráfico de *flooding* puede ser tráfico de *broadcast*, *multicast*, o tráfico desconocido. VTP *pruning* aumenta el ancho de banda disponible. Para hacer esto se habilita el comando `switch port pruning` de las VLANs que no sean necesarias definir sobre los *switches* de acceso o distribución.

#### 2.3.4 SWITCHES DE ACCESO

Se llama *switch* de acceso al conmutador que interactúa con los dispositivos finales, es decir, PCs de usuarios, teléfonos IP, ATAs, etc. En los *switches* de acceso es muy importante que se realice la asignación correcta de los *hosts* a las diferentes VLANs.

En primer lugar se deben considerar los puertos que darán servicio a la infraestructura de telefonía, los cuales pueden o no tener un computador conectado al *switch* del teléfono, eso no impide la creación de VLANs separadas. Luego se seguirá con los puertos que tendrán sólo PCs y por último los puertos de *uplink*.

- Puertos de infraestructura de telefonía: Para implementar la VLAN de telefonía y de datos se deben implementar los parámetros de QoS, seguridad y STP. Además es necesario implementar el concepto de *SmartPorts* en un puerto o rango de puertos. Para definir puertos como *SmartPorts* primero se pone al puerto en su estado por defecto, esto se puede conseguir con el comando *default interface* como se muestra a continuación:

```
SW(config)# default interface range fa 0/10 - 19
SW(config)# do sh runn interface fa 0/10
Building configuration...
```

Luego se aplica la macro "cisco-phone", la cual requiere de dos variables, una para identificar la VLAN de telefonía (\$VVID) y otra para identificar la

VLAN de acceso (\$AVID) que tendrán tanto las PCs que estén detrás de un teléfono o cuando éstas se las conecta directamente. A continuación se presentará un ejemplo del modo de configuración:

```
SW(config)# interface range fa 0/10 -19
SW(config-if-range)# macro apply cisco-phone $AVID 2
                        $VVID 10
SW(config-if-range)# do sh running interface fa 0/10
Building configuration...
```

```
Current configuration : 544 bytes
```

```
!
```

```
interface FastEthernet0/10
  switchport access vlan 2
  switchport mode access
  switchport voice vlan 10
  switchport port-security
  switchport port-security maximum 3
  switchport port-security aging time 2
  switchport port-security violation restrict
  switchport port-security aging type inactivity
  mls qos trust device cisco-phone
  mls qos trust cos
  auto qos voip cisco-phone
  macro description cisco-phone
  spanning-tree portfast
  spanning-tree bpduguard enable
end
```

En el ejemplo de configuración anterior, se identifica que la VLAN 10 es para voz (\$VVID 10). El comando `do sh running interface fa 0/10` lo que hace es mostrar la configuración de la interfaz, donde se

puede ver que la VLAN 10 ha sido definida como una VLAN que transporta voz.

En el caso de los ATAs, se debe aplicar la misma macro al puerto en el cual se lo tiene conectado, pero en este caso deben coincidir los valores de \$VVID con el de \$AVID ya que el ATA deberá pertenecer a la VLAN de telefonía y no a la de datos.

- Puertos de infraestructura de datos: Al igual que para la implementación de puertos de infraestructura de voz, los de datos también necesitan la implementación de *SmartPorts* en un puerto o rango de puertos. Primero se pone el puerto en su estado por defecto.

```
SW(config)# default interface range fa 0/20 - 24
SW(config)# do sh runn interface fa 0/20
Building configuration...
```

Luego se aplica la macro "cisco-desktop", la cual requiere de una variable para identificar la VLAN de acceso (\$AVID) que tendrán las PCs:

```
SW(config)# interface range fa 0/20 -24
SW(config-if-range)# macro apply cisco-desktop $AVID 2
%Warning: portfast should only be enabled on ports
connected to a single host. Connecting hubs,
concentrators, switches, bridges, etc... to this interface
when portfast is enabled, can cause temporary bridging
loops.
Use with CAUTION.
%Portfast will be configurated in 5 interfaces due to
the range command but will only have effect when the
interfaces are in a non-trunking mode.
SW(config-if-range)# do sh running interface fa 0/20
Building configuration...
```

```

Current configuration : 353 bytes
!
interface FastEthernet0/20
  switchport access vlan 2
  switchport mode access
  switchport port-security
  switchport port-security aging time 2
  switchport port-security violation restrict
  switchport port-security aging type inactivity
  mls qos trust cos override
  macro description cisco-desktop
  spanning-tree portfast
  spanning-tree bpduguard enable
end

```

En la configuración que se muestra anteriormente, se usa el comando `macro apply cisco-desktop $AVID 2` para especificar que la VLAN 2 es para datos. El comando `do sh running interface fa 0/20` muestra la configuración actual de la interfaz.

- Puertos de *uplink*: Para este tipo de puertos se posee una macro denominada "cisco-switch" que permite configurar el puerto en modo *trunk* sin negociación, identificará la *native* VLAN mediante la variable \$NVID y configurará el QoS en modo *trust*. Esta configuración permite reducir los tiempos de convergencia.

```

SW(config)# default interface gi 0/1
Interface GigabitEthernet 0/1 set to default
configuration
SW(config)# interface gi 0/1
SW(config-if)# macro apply cisco-switch $NVID 1
SW(config-if)# do sh runn int gi 0/1

```

Building configuration..

Current configuration : 196 bytes

!

```
interface GigabitEthernet0/1
  switchport mode trunk
  switchport nonegotiate
  mls qos trust cos
  auto qos voip trust
  macro description cisco-switch
  spanning-tree link-type point-to-point
end
```

### 2.3.5 SWITCHES DE DISTRIBUCIÓN

En este punto de la red por lo general no se tiene ni teléfonos ni computadores, solo hay concentración de *uplinks* desde el acceso y un *Etherchannel* hacia el *core*. En estos *switches* se aplica la macro "cisco-switch" en todos los puertos. Si fuese necesario aquí se hace ruteo entre VLANs. Éstas son funciones de capa 3. La figura 2.18 esquematiza los *switches* de distribución.

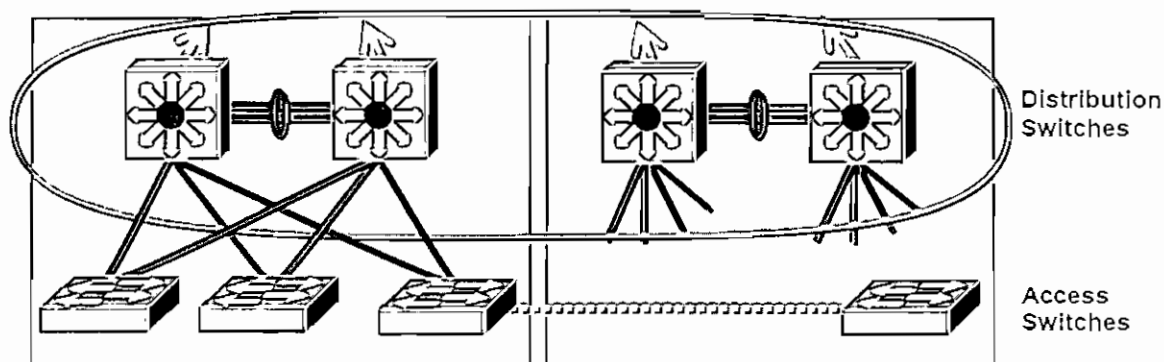


Figura 2.18 Switch de distribución [28].

### 2.3.6 SWITCHES DE CORE

Los *switches* de *core* se pueden disponer de dos maneras. La primera en la que los servidores van conectados directamente al *switch* de *core* y el segundo diseño en el cual se agrega una capa adicional parecida a una capa de acceso pero solo para la granja de servidores.

En el centro de cómputo del edificio Belmonte del grupo ITABSA los servidores no se encuentran conectados directamente al *switch* de *core*, es decir, se crea esta capa adicional exclusiva para servidores. Es necesario definir los puertos de acuerdo a los servidores que están conectados al mismo y al servicio que dan estos servidores.

Los puertos donde estén los servidores de telefonía (*Call Manager*, *Unity*, *Personal Assistant*, etc) se los define en modo acceso (modo de configuración de las interfaces) y se los asigna a la VLAN de telefonía. A continuación se mostrará un ejemplo de la configuración de los puertos en modo de acceso.

```
SW(config)# int fa0/2
SW(config-if)# switchport acces vlan 10
SW(config-if)# switchport mode access
```

Otra cosa importante es que en los *switches* de *core* también se conectan los *routers* para acceso a la WAN. Para tener una buena política de QoS de extremo a extremo es necesario realizar la configuración adecuada en el puerto del *switch* en donde se conectará el *router*. Para esto es necesario implementar la macro *SmartPort* denominada "cisco-router".

```
SW(config)# int fa0/8
SW(config-if)# macro apply cisco-router $NVID 1
%Warning: portfast should only be enabled on ports connected
to a single host. Connecting hubs, concentrators, switches,
```



bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops.

Use with CAUTION

%Portfast has been configured on FastEthernet0/8 but will only have effect when the interface is in a non-trunking mode.

```
SW(config-if)# do sh runn int fa0/8
```

Building configuration...

Current configuration : 210 bytes

:

```
interface FastEthernet0/8
  switchport mode trunk
  switchport nonegotiate
  mls qos trust dscp
  auto qos voip trust
  macro description cisco-router
  spanning-tree portfast
  spanning-tree bpduguard enable
end
```

## 2.4 PROPUESTA DE DISEÑO

El presente diseño busca la renovación de la central telefónica actual Definity del edificio Belmonte y de la planta de producción TANASA Quito. En esta propuesta de diseño se incluye una solución basada en tecnología IP para transmisión de voz sobre la red de datos, la que podrá interconectarse con las otras centrales telefónicas del grupo; también se interconectará con los elementos de *networking* necesarios para su funcionamiento. El beneficio de telefonía IP dentro del grupo ITABSA será tener un sistema de telefonía centralizado y escalable, a diferencia de las centrales telefónicas que actualmente posee, con la posibilidad de extender

este sistema de telefonía al resto de oficinas del grupo ITABSA ubicadas a nivel nacional.

El sistema de telefonía IP propuesto para el grupo ITABSA se lo va a realizar utilizando equipo Cisco, que permitirá aprovechar al máximo la infraestructura de datos que posee la compañía ya que la misma actualmente dispone de equipos Cisco. La arquitectura propuesta para telefonía IP se muestra en la figura 2.19. El lado izquierdo del gráfico presenta la arquitectura de una central telefónica convencional y en el lado derecho se muestran los componentes Cisco que realizan las funciones equivalentes en telefonía IP.

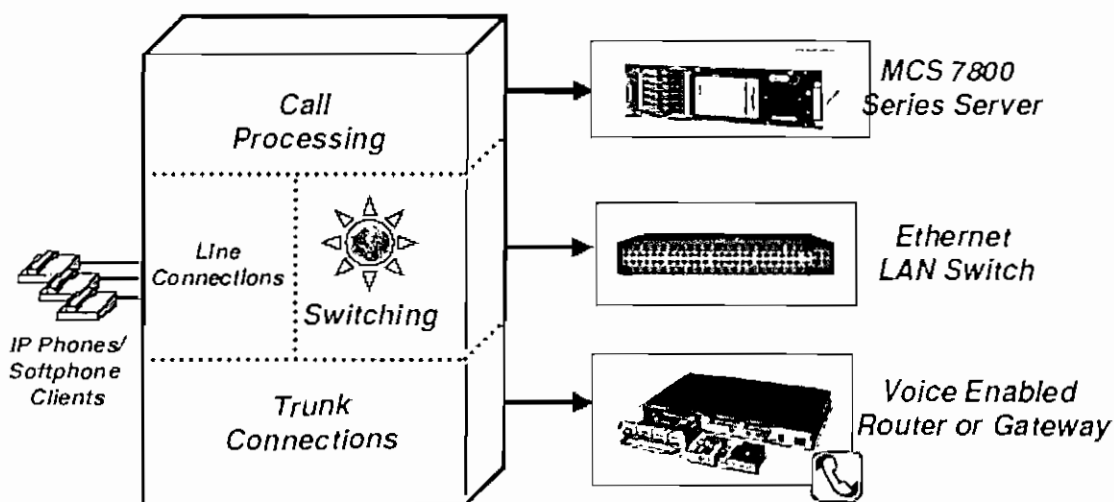


Figura 2.19 Arquitectura de telefonía IP [8].

La telefonía IP presenta una arquitectura distribuida, esto quiere decir que las diferentes funciones de telefonía se distribuyen entre varios equipos que no necesariamente tienen que estar instalados en el mismo lugar. Esto permite que el sistema de telefonía IP sea escalable y que no importe la disposición geográfica de los usuarios mientras éstos tengan conexión mediante una red de datos.

Para el sistema de telefonía IP se contará con los elementos básicos indicados en la figura 2.19, es decir un servidor que contendrá el *Call Manager*, *Switches* y un *gateway* de voz. Para realizar la función de procesamiento de llamadas se tendrá

un servidor en el que se cargue el software *Call Manager* 4.1. Para la función de conmutación y conexión de teléfonos se utilizan los *switches* de la red LAN. Para la función de manejo de conexiones troncales, es decir las líneas externas, se tiene *routers* con módulos E1; los dispositivos que permitirán la interacción entre el usuario y la red son los teléfonos IP y softphones, además de ATAs para la conexión de equipos analógicos.

Esta solución plantea una arquitectura combinada y robusta en la que se pueden manejar datos, voz y vídeo sobre la misma red LAN y WAN que se posee al momento en el grupo corporativo.

El servidor donde se instalará el *Call Manager* 4.1 se lo debe colocar en un lugar centralizado, por esta razón se lo dispondrá en el centro de cómputo del edificio Belmonte donde se encuentran las oficinas del grupo ITABSA, con lo que se tendrá administración centralizada de todas las funciones de la red de telefonía IP. Además, el centro de cómputo principal del grupo es el centro de cómputo del edificio Belmonte, aquí se encuentran los principales servidores y desde aquí se realizan los enlaces internacionales. Otro servidor que también se lo ubicará en el centro de cómputo del edificio Belmonte será el servidor donde residirá el software *Unity* 4.0 de Cisco para mensajería unificada.

Dentro de la empresa se puede diferenciar a los usuarios de acuerdo a la labor que cada uno hace, por lo tanto se asignará un teléfono de acuerdo a las necesidades que requiera el tipo de trabajo que realicen. La mayoría de usuarios sólo tienen la necesidad de un teléfono con las características básicas de comunicación, como lo es el Cisco IP *Phone* 7912G. Personal como secretarías o algunos jefes se les asignará el teléfono Cisco IP *Phone* 7940G que les permite algunas opciones como manos libres y conferencias. En tanto que gerentes y directores usarán el teléfono Cisco IP *Phone* 7960G que es el que más se adapta a las necesidades de este tipo de personal. Estos teléfonos se ubicarán en las distintas localidades y de acuerdo a los requerimientos de cada usuario. En las extensiones en las cuales se maneja dispositivos analógicos como fax se colocarán ATAs (*Analog Telephone Adaptator*).

Como se vio en las características del *router* 3825, el cual hace las veces de *gateway*, este equipo proporcionará las características necesarias para el correcto funcionamiento de una red de convergencia de voz y datos. Este *router* viene equipado con 8 puertos FXS, los cuales se puede aprovechar para colocar algunos dispositivos analógicos. El grupo ITABSA contratará dos E1s los cuales serán necesarios para la interconexión con la PSTN. El grupo, al estar ubicado en la ciudad de Quito, el proveedor de la PSTN es Andinatel.

#### 2.4.1 CONMUTACIÓN DE LLAMADAS

La función de conmutación de llamadas en el sistema que se propone lo realizará un servidor en el que se instalará la aplicación *Call Manager* versión 4.1. Junto con este software se incluye el software Cisco IPCC (*IP Contact Center*) *Express Edition Standard* que incluye el licenciamiento para el manejo de cinco agentes / supervisores.

La cantidad de usuarios de telefonía que se tiene en el grupo ITABSA es de 158 usuarios en el edificio Belmonte y 105 usuarios en TANASA. El equipo propuesto está configurado para soportar hasta 300 usuarios, Por lo que cubre perfectamente las necesidades del grupo ITABSA, soportando la cantidad de usuarios actuales y permitiendo el incremento de nuevos usuarios en caso de requerirlo.

Para fines de contingencia de este servidor crítico se ha considerado que el *router gateway* de voz 3825 haga las veces de *Call Manager* de *backup*, utilizando la licencia Cisco SRST (*Survivable Remote Site Telephony*) que incorpora. Cisco SRST es una característica extra que se incluye en el IOS del *router*. Éste es un componente crítico que permite realizar procesamiento de llamadas en el caso de que exista algún problema con el Cisco *Call Manager*. Esto permitirá ofrecer telefonía local y comunicación con las otras oficinas en el resto del país a través de la PSTN, en caso de contingencia y caída del *Call Manager* principal.

La aplicación Cisco *Call Manager* 4.1 se la instalará en un servidor Cisco MCS 7815l. El servidor donde se instalará el *Call Manager* dará servicio tanto a los usuarios del edificio Belmonte como a los usuarios de TANASA. Esto se puede realizar gracias a que este software presenta una arquitectura centralizada con capacidad de ser distribuida para lo que se necesita licencias de supervivencia remotas en el *router* de TANASA.

#### 2.4.2 MENSAJERÍA UNIFICADA

Se opta por el sistema de mensajería unificada Cisco Unity 4.0. Esta aplicación se instalará en un servidor Cisco MCS 7815l. En este tipo de mensajería unificada también se incluye una plataforma de *voice mail* (mensajería de voz). Estos mensajes se almacenarán en Microsoft Exchange.

Al utilizar este sistema de mensajería unificada, el usuario tiene mayor control sobre todas sus aplicaciones tanto de mensajería de voz como de datos. Esto permite descentralizar la administración de estas aplicaciones ya que no es necesario que exista una persona dedicada a la administración de los servicios de mensajería. Es cada usuario quien se encarga de personalizar su propio sistema, de acuerdo a sus necesidades.

Los usuarios tendrán acceso a sus mensajes de voz, *mails* y otros tipos de mensajes como fax desde cualquier lugar donde se encuentren y tengan acceso a la red de la empresa. Microsoft Exchange es una herramienta robusta, que ya se la ha venido utilizando en la empresa desde hace muchos años, por lo tanto los usuarios ya están acostumbrados a ella. Por esta razón para los usuarios no habrá mucho impacto al momento de aprender a usar los nuevos servicios que tienen a su disposición dentro del mismo sistema de Microsoft Exchange al que ya están familiarizados.

### 2.4.3 EQUIPO QUE INTERACTÚA CON EL USUARIO

Los dispositivos finales que son los que están a disposición de los usuarios son los teléfonos IP. Para este diseño se recomienda el uso de tres diferentes tipos de teléfonos, éstos son: Cisco IP *Phone* 7912G, 7940G, 7960G. Se utilizarán diferentes tipos de teléfonos porque unos poseen más servicios que otros, y por lo tanto la asignación de teléfonos se la realiza de acuerdo a las necesidades de cada usuario. Para los usuarios de *laptops* además se instalará un *softphone*, que es el software Cisco IP *Communicator*. De esta manera, cuando los ejecutivos que poseen *laptops* viajen, tendrán su extensión a disposición en cualquier lugar en donde se encuentren.

A pesar de que la mayoría de documentos en la actualidad se los envía utilizando *e-mail*, en ITABSA se ve la necesidad de seguir manteniendo equipos de fax. El fax es un dispositivo analógico que utiliza la red telefónica para la transmisión de información. En este caso, como se desea mantener los equipos de fax que se tienen en funcionamiento en la empresa, se considera la utilización de ATAs (*Analog Telephone Adaptor*). Se empleará el Cisco ATA 186.

### 2.4.4 VOICE GATEWAY

Al implementar telefonía IP es necesario contar con un *gateway* de voz. Para este diseño se contempla la utilización de un *router* Cisco 3825 para que realice las funciones de *gateway*. Este *router* puede soportar 2 interfaces E1 lo que da un total de 60 canales de voz hacia la PSTN. Posee 8 interfaces de voz analógica tipo FXO que se las utilizará para recibir las líneas troncales analógicas de Andinatel.

Este *router* también posee 8 puertos FXS para conectar dispositivos telefónicos analógicos o equipos de fax. El *gateway* de voz 3825 posee la licencia SRST para realizar las funciones de *backup* del *Call Manager* principal.

### 2.4.5 SWITCH CENTRAL

Por las características que posee telefonía IP, en esta solución se incluye un *switch* central robusto de capa 3: el Cisco Catalyst 4507R que será el *switch* central de la red de voz y datos. Será necesario un *switch* Catalyst 4507R como *switch* central para el centro de cómputo de ITABSA y otro para ser *switch* central del centro de cómputo de TANASA. Este cambio se lo realiza para dotar de una red LAN escalable con altas prestaciones de servicios con lo que se conseguirá explotar de mejor manera los recursos de red con nueva tecnología y reducción de costos en el tiempo.

La red del grupo ITABSA al momento no está dividida en VLANs. Como se dijo anteriormente en las condiciones de diseño, es necesario crear VLANs diferentes para voz y datos, esto permitirá aplicar las condiciones de priorización para asegurar QoS. Por esta razón, la red del grupo ITABSA se encuentra formando un solo dominio de *broadcast*. Éste es un verdadero problema de seguridad ya que cualquier problema que se produzca en cualquier parte de la red afectará a toda la red pudiendo dejarla incluso deshabilitada.

Para la implementación de telefonía IP se segmentará la red actual en VLANs para evitar problemas, además de esta manera se puede asignar una VLAN exclusiva para telefonía. La necesidad de realizar esto es por políticas de QoS.

El *switch* Cisco 4507R que se propone tiene alta disponibilidad. Es capaz de soportar redundancia en fuentes de poder, tarjetas supervisoras con soporte de capa 2, capa 3 y múltiples capas.

Los *switches* de acceso se deberán conectar al *switch* central utilizando *uplinks* gigabit Ethernet con enlaces de *trunking* que permitan transmitir información de diferentes VLANs. También necesita soporte TCP/IP y enrutamiento entre VLANs.

El *switch* 4507R es un conmutador de *core* robusto, por lo tanto dará el soporte que necesita la red de ITABSA y la de TANASA para soportar servicios de voz. Es

un *switch* redundante en fuentes de poder; es decir que posee dos fuentes de poder, si una falla la otra la reemplaza. Además posee la capacidad de soportar módulos de tipo *in line power*, si en un futuro se planea mantener la alimentación eléctrica a través de la red LAN; por el momento no se utilizará *in line power*. El switch 4507R posee puertos del tipo 1000 base SX para fibra óptica para la interconexión de los *switches* de acceso y servidores de red al *switch* de *core*. Con este tipo de puertos se puede alcanzar distancias de hasta 250 m.

Además este *switch* dispondrá de 24 puertos Ethernet 10/100/1000 con interfaz RJ45 para la conexión de servidores o usuarios críticos de la red y sus teléfonos IP.

Para los enlaces de *trunk* hacia el *switch* de core se utilizará el estándar de encapsulación 802.1q<sup>3</sup> que mediante *frame tagging* (etiquetado de las tramas) es más eficiente para transmitir información de aplicaciones actuales de múltiples VLANs por el mismo enlace. Para configurar los enlaces de *trunk* se utilizará las interfaces gigabit Ethernet conectando con estos enlaces a los *switches* de acceso hacia el *switch* de core.

Con el objetivo de disminuir el tiempo de convergencia en caso de cambios topológicos, los puertos de los *switches* de *core* se configurarán como *BackboneFast* y los enlaces de los *switches* de acceso se los configurará como *UplinkFast*.

Para mantener centralizada la administración de las VLANs se configurará un solo dominio VTP, en el que el *switch* principal será el *switch* de *core* Cisco Catalyst 4507. El objetivo de esta configuración es que cualquier VLAN que sea creada o eliminada en el VTP Server automáticamente será transmitida y creada o eliminada en el resto de *switches*.

---

<sup>3</sup> 802.1q: Estándar de IEEE para etiquetado de tramas. Introduce un encabezado de etiqueta dentro del encabezado Ethernet, después de la dirección MAC origen. 12 bits del encabezado de etiqueta especifican el VLAN-ID.



Será necesario utilizar las características de VTP *pruning*. El enviar la información solamente a las VLANs necesarias permite ahorrar ancho de banda en los enlaces. Al crear VLANs se disminuye el tamaño de los dominios de *broadcast*.

#### 2.4.6 SOFTWARE DE ADMINISTRACIÓN: CISCO WORKS

La versión de Cisco *Works* que se utilizará será Cisco *Works* SNMS 1.5.1 (*Small Network Management Solution*). Provee las herramientas necesarias para monitoreo avanzado, configuración y herramientas de manejo que simplifican la administración de la red. Ésta es una óptima solución basada en web para trabajar en ambientes corporativos con capacidad de monitorear 30 a 40 dispositivos de red como *routers*, *switches*, *firewalls*, y servidores.

#### 2.4.7 ROUTERS REMOTOS

Los *routers* Cisco 2800 son *routers* de servicios integrados que permitirán la comunicación con las centrales telefónicas de los sitios remotos. Es decir, se dispondrán de *routers* Cisco 2800 en TANASA Durán y en PROESA Atarazana, ambos ubicados en la ciudad de Guayaquil. Estas dos localidades también migrarán a telefonía IP en un futuro por lo que se ve la necesidad de cambiar los *routers*; además al momento también será necesaria la conexión hacia sus centrales telefónicas.

Tanto en TANASA Durán como en PROESA Atarazana al momento se tiene centrales telefónicas analógicas. Actualmente no hay ningún tipo de conexión entre las centrales telefónicas del grupo ITABSA y para comunicarse entre ellas se utiliza la PSTN.

Para este objetivo se ha configurado cada uno de los equipos con al menos 2 puertos WAN y con 8 interfaces FXS para que desde TANASA Durán y PROESA

Atarazana se puedan manejar hasta 8 llamadas simultáneas hacia Belmonte, que es en donde se ha centralizado la solución de telefonía IP.

Algo que es importante considerar es el impacto en ancho de banda que implica el incrementar tráfico de voz en la red de datos. El ancho de banda que utiliza cada canal de voz transmitido en la red WAN es de 12 KHz a 16 KHz. Se plantea que se podrán tener 8 canales de voz simultáneos. Para planificar el ancho de banda del enlace WAN se utiliza el valor de ancho de banda usado por cada canal y el número de canales simultáneos que se van a tener. Hay que considerar también que los *links* en la WAN no deben sobrepasar el 75% de uso del ancho de banda contratado con el *carrier*. Esto quiere decir, que por 8 canales de 16 KHz se tendrían 128 KHz de ancho de banda extras al uso normal que actualmente ya tiene el enlace. El enlace actual que se tiene de PROESA Atarazana con Belmonte es un enlace satelital de 256 Kbps; y el enlace desde TANASA Durán a Belmonte también es un enlace satelital de 256 Kbps.

Al incrementar servicios de voz se tendría que incrementar el ancho de banda en los enlaces para que la solución trabaje sin afectar el actual desempeño de la red de datos. Los enlaces actuales para la transmisión de datos son enlaces de 256 kbps; como se dijo anteriormente, para asegurar el correcto funcionamiento se presume que el tráfico promedio es del 75% del enlace contratado. Por lo tanto, actualmente para tráfico de datos se hace uso de una velocidad de transmisión de 192 Kbps. Si a este tráfico se suma 128 Kbps que se presume será el promedio de uso de aplicaciones de voz se tendría un promedio de 320 Kbps. Este tráfico debe representar el 75% del enlace contratado; por lo tanto se debería contratar un canal de 426,66 Kbps. Pero los enlaces se contratan en valores de  $n \times 64$  Kbps, por lo que se debería contratar enlaces de capacidad de 448 Kbps.

Será importante que en el *router* Cisco 3725 que actualmente posee ITABSA para la conexión con los sitios remotos se configuren los parámetros de QoS en IP para que soporte la solución de telefonía IP.

## 2.4.8 ESQUEMA DE LA PROPUESTA DE DISEÑO

Dentro de la propuesta de diseño planteada se tratará de reutilizar al máximo los equipos que posee actualmente el grupo ITABSA. El esquema del diseño de telefonía IP tanto para el edificio Belmonte como para la planta de producción de Quito se lo puede observar en la figura 2.20. A continuación se hace un resumen de los equipos a utilizarse en la solución de telefonía IP propuesta y que se han descrito anteriormente:

- Cisco *Call Manager* 4.1 con soporte para 300 usuarios.

Incluye: Software Cisco *Call Manager* 4.1, Servidor Cisco MCS 7815I (Pentium 4, 1024 MB memoria RAM, 80 GB Disco duro), licencia para 300 usuarios, Software Cisco IPCC *Express Edition Standard*.

- Cisco *Unity Server* para 300 usuarios.

Incluye: Software *Unity* 4.0, Servidor Cisco MCS 7815I, *Unity for CallManager IP Integration*, *Unity for Exchange*, *Unity Data Store*, *Unity Message Store 5.5*, Cisco *Unity Operating System*.

- Gateway Cisco Router 3825.

Incluye: 8 puertos FXS, 6 puertos FXO, 2 puertos para *Voice Interface Card* FXO, 2 puertos RJ-48 *Multiflex Trunk* E1, 256 MB de memoria SDRAM, 64 MB de memoria Flash, licencia SRST.

- Switch central Cisco Catalyst 4507R tanto para ITABSA (1) como para TANASA (1).

Incluye: Cisco IOS, licencia para agente RMON, 6 puertos Gigabit Ethernet (GBIC), 24 puertos Ethernet 10/100/1000.

- Teléfonos Cisco IP *Phone* 7912G para ITABSA (60) y TANASA (40).

Incluye: *Patch cord* y transformador para alimentación eléctrica.

- Teléfonos Cisco IP *Phone* 7940G para ITABSA (40) y TANASA (30).

Incluye: *Patch cord* y transformador para alimentación eléctrica.

- Teléfonos Cisco IP *Phone* 7960G para ITABSA (30) y TANASA (16).

Incluye: *Patch cord* y transformador para alimentación eléctrica.

- Consola 7914 para teléfono IP 7960 para ITABSA (1) y para TANASA (1).

Incluye: Teléfono Cisco IP *Phone* 7960G, módulo de expansión Cisco 7914 para teléfono IP, *patch cord* y transformador para alimentación eléctrica.

- Cisco ATA 186 para ITABSA (6) y para TANASA (5).

Incluye: *Patch cord* y transformador para alimentación eléctrica.

- Estación de conferencia Cisco IP *Conference Station* 7936 para ITABSA (6) y para TANASA (3).

Incluye: *Patch cord* y transformador para alimentación eléctrica.

- *Softphones* Cisco IP Communicator para ITABSA (9) y para TANASA (5).

- Router Cisco 2800 para TANASA Quito (1), para TANASA Durán (1) y para PROESA Atarazana (1).

Incluye: 2 puertos con tarjeta de interfaz WAN, 8 puertos FXS, 64 MB de memoria.

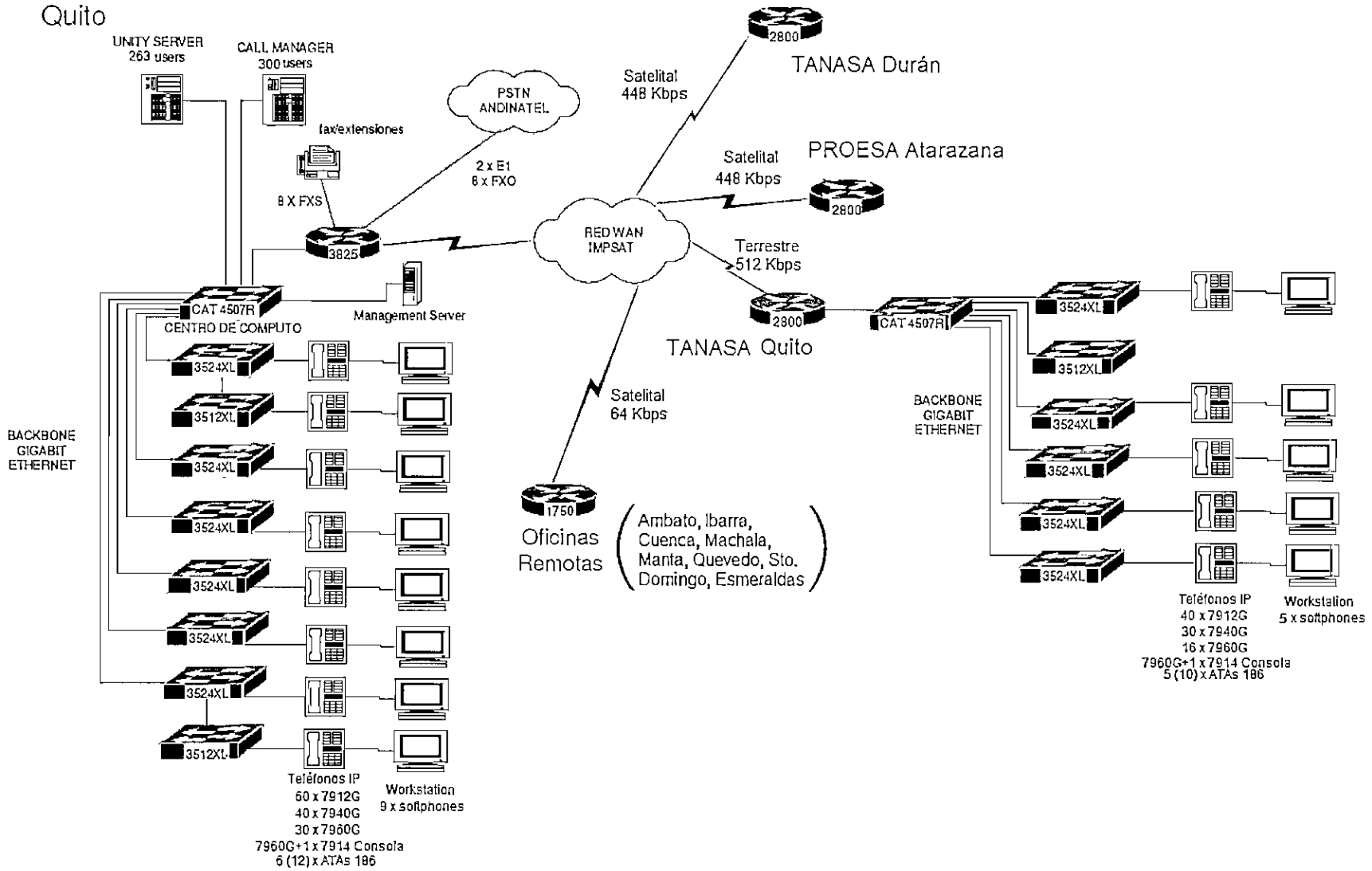


Figura 2.20 Esquema de la propuesta de diseño de telefonía IP.

### 2.4.9 IP PLANNING

Las direcciones IP se asignarán a los teléfonos IP utilizando DHCP. Por lo tanto es necesario definir las subredes que se utilizarán para este efecto. Se definirá una subred para los teléfonos IP y los dispositivos que se encuentran en Belmonte y otra subred para los teléfonos IP y los dispositivos que se encuentran en TANASA. Ambas subredes se definirán dentro de la misma VLAN ya que las dos prestarán servicios de voz. En la Tabla 2.1 se puede ver la planificación IP.

UBICACIÓN	SUBRED	MÁSCARA DE SUBRED	RANGO IP	# HOSTS
ITABSA	10.204.21.0	255.255.255.0	Desde: 10.204.21.1 Hasta: 10.204.21.254	254
TANASA	10.204.22.0	255.255.255.0	Desde: 10.204.22.1 Hasta: 10.204.22.254	254

Tabla 2.1 IP Planning.

De las subredes que se ha definido, hay que tomar algunas direcciones para asignarlas como direcciones IP fijas para algunos dispositivos como servidores y *routers*. En la Tabla 2.2 se puede observar las direcciones IP que se asignarán a estos equipos.

UBICACIÓN	DISPOSITIVO	DIRECCIÓN IP	MÁSCARA
ITABSA	Gateway router Cisco 3825	10.204.21.1	255.255.255.0
ITABSA	Servidor Call Manager	10.204.21.2	255.255.255.0
ITABSA	Servidor Unity	10.204.21.3	255.255.255.0
TANASA	Router Cisco 2800	10.204.22.1	255.255.255.0

Tabla 2.2 Direcciones IP fijas.

En el servidor de DHCP se definirá el rango de direcciones IP 10.240.21.10/24 – 10.204.21.254/24 para la asignación automática de direcciones IP para los

teléfonos IP del edificio Belmonte. Se empieza desde la dirección 10.240.21.10 para dejar las primeras direcciones para uso de direcciones fijas que se necesiten en un futuro. Al momento de definir este rango también es necesario definir qué direcciones IP son fijas y han sido asignadas previamente a algún determinado equipo. Al definir esto, el servidor de DHCP no usará esas direcciones. Lo mismo se hará para TANASA, con la diferencia de que su rango de direcciones IP es 10.204.22.10/24 – 10.204.22.254/24. Igualmente se dejan libres las primeras direcciones para requerimientos futuros de direcciones fijas.

Estas dos subredes pertenecerán a una sola VLAN, ya que esa VLAN será exclusiva para servicios de voz y en ésta se aplicarán las políticas de QoS. Además es importante recordar que en la configuración de los *routers* se debe indicar que el puerto WAN que sale desde ITABSA hacia TANASA pertenece a la VLAN de voz. Esto es necesario para poder realizar el enrutamiento del tráfico a través de la WAN. Físicamente se tiene un solo enlace desde ITABSA hacia TANASA, pero al segmentar la red en VLANs, se está realizando una separación lógica del tráfico de voz y de datos en el mismo enlace que sale por el mismo puerto.

## 2.5 ANÁLISIS DE EQUIPO ESPECÍFICO DISPONIBLE EN EL MERCADO

Todo el equipo propuesto para el diseño de la solución de telefonía IP para el Grupo ITABSA existe en el mercado local, pudiéndolo adquirir a cualquiera de la gran variedad de proveedores de equipo Cisco en el país.

En la sección de alternativas tecnológicas ya se hizo una descripción general de los dispositivos a utilizarse. Ahora se hará una descripción de las características específicas que serán útiles en el presente diseño, así como a las características específicas de configuración. En el anexo A.1 se encontrarán los *datasheets* de todos los equipos a utilizarse.

### 2.5.1 CISCO *CALL MANAGER* 4.1

El sistema utilizado por Cisco *Call Manager* 4.1 está basado en una arquitectura cliente-servidor sobre plataforma Windows 2000 server o Windows 2003 server. El grupo ITABSA al momento trabaja con Windows 2000 server, pero para los siguientes meses tiene planificado la migración a Windows 2003 server; por esta razón los servidores para las aplicaciones de telefonía IP ya se los implementará sobre Windows 2003 server.

Cisco *Call Manager* 4.1 permite soportar usuarios (clientes) distribuidos en una red LAN o WAN, utilizando un solo sistema centralizado. Este sistema también permite integrarse con otros servidores dentro de una red LAN o WAN distribuida dentro del ámbito nacional. Para esto el servidor permite la interconexión en red utilizando tecnologías de transporte pública o privada como TDM (E1 o nx64 Kbps), ISDN, ATM, *Frame Relay*, IP, entre otros. En el caso de redes WAN, permite la implantación de un sistema centralizado sin necesidad de servidores locales en sitios remotos. La red WAN del grupo ITABSA es una red *Frame Relay*.

La configuración y programación del servidor de voz se puede realizar a través de un puerto V.24 o vía LAN por un puerto Ethernet usando HTML o un emulador como *PC Anywhere*, el mismo que es utilizado por el grupo ITABSA para acceso remoto a servidores. Esta programación se la realiza sin generar desconexión del sistema. Este software además posee capacidad SNMP para el monitoreo de los terminales IP y PCs multimedia conectados al servidor de voz.

La comunicación que permite es de cualquier tipo contra cualquier tipo, es decir, de teléfono IP a teléfono IP, de teléfono IP a teléfono analógico, de teléfono IP a teléfono de la red pública, de teléfono analógico a teléfono de la red pública, o de PC a cualquiera de los anteriores. Para el caso de dispositivos analógicos se utilizan adaptadores como ATAs que transforman la señal analógica a señal IP para así poder transmitir la información por la LAN o por la WAN.



Trabaja bajo los estándares de codificación G.729 y G.711. La asignación de los codecs es de manera dinámica al momento de configurar los teléfonos. Soporta los estándares H.323, H.225, H.245, SIP y MGCP. En cuanto a la administración del sistema, cuenta con diferentes niveles de acceso protegidos con nombres de usuario y contraseña.

Las facilidades telefónicas que el equipo ofrece son variadas. Se puede definir grupos de troncales, grupos de extensiones, restricción de llamadas, captura de llamadas, código personal, conferencia tripartita, desvío de llamadas, llamada en espera, rellamada, llamada externa, llamada interna, marcación por nombre, marcación rápida, operación de múltiples jefe – secretaria, operación multilínea, remarcación de números almacenados tanto internos como externos, servicio de mensajes, transferencia de llamadas, identificación de llamadas, movilización de la extensión, habilitación y deshabilitación de teléfonos usuario y aplicaciones XML.

Cuando ya se ha instalado el *Call Manager* en el servidor, lo primero que se debe hacer es validar la información referente a la configuración de troncales a la red PSTN. Después se define el plan de numeración detallado, esto quiere decir el formato de las extensiones y los códigos para salida a la PSTN. Posteriormente se definen los métodos de restricción de llamadas ya sea por código o por extensión y se definen los recursos de conferencia y MoH (*Music on Hold*, música en espera).

A continuación se deberán definir *passwords* de administración del servidor, DNS y *passwords* para la administración de la base de datos SQL. Se configura el servidor para definir los parámetros de direccionamiento IP del *Call Manager* para que se integre en la red LAN. Seguidamente se define el nombre del *Call Manager*, puerto TCP, descripción y parámetros.

El siguiente paso es definir los grupos de teléfonos IP pertenecientes a cada *gateway*. Se configuran los valores por omisión que poseerán los teléfonos al momento de ser conectados y el *pool* de extensiones de los teléfonos IP. Se crea

el *dial-plan* donde se definen las extensiones y las salidas a través del plan de marcación. Después de esto se determinan los grupos de captura de llamadas, grupos de búsqueda para las operadoras y servicio automático de operadora (*Cisco IP Automatic Attendant*).

El *Cisco IP Automatic Attendant* se configurará para que en la contestación de las llamadas, ejecute el mensaje de bienvenida, así como un menú de instrucciones invitando al llamante a seleccionar alguna opción, que puede ser comunicarse con una operadora o si conoce el número de la extensión, marcarlo.

Junto con *Cisco Call Manager 4.1* se integra *Cisco IPCC (IP Contact Center)* [8]. IPCC provee funcionalidad y facilidad de implementación de *contact centers* (centros de contacto). Brinda soluciones avanzadas para *contact centers* en una sola plataforma, como son distribución automática de llamadas (*ACD, Automatic Call Distribution*), respuesta de voz interactiva (*IVR, Interactive Voice Response*) e integración de telefonía por computación (*CTI, Computer Telephony Integration*). IPCC ofrece un grupo comprensible y flexible de encolamiento y opciones de enrutamiento, además tiene la capacidad de proporcionar reportes.

El software *Cisco IP Contact Center* se instalará en el mismo servidor del *Call Manager*. Lo primero que se tiene que hacer es definir los agentes del *Contact Center*, que por las características de la licencia que viene junto al *Call Manager*, tendrá un número de agentes máximo de cinco. A continuación se valida la información referente a la configuración de colas de servicio y se definen perfiles de los agentes. Después se configuran los usuarios y la asignación como agentes, se asocian los agentes con las extensiones y se instalan los agentes en las PCs.

### 2.5.2 CISCO UNITY 4.0

*Cisco Unity 4.0* es un sistema de mensajería unificada basado en software. La principal ventaja es que todo tipo de mensajes como *e-mail*, voz, y fax son

enviados a la bandeja de entrada del usuario, permitiendo a los usuarios tener control centralizado de las comunicaciones. El acceso a los mensajes puede ser tanto desde una PC o desde un teléfono. Posee una interfaz muy amigable para el cliente, con botones para adelantar, retroceder o parar.

La administración de este sistema está basada en *browser* y es muy fácil de usar. Ofrece alta escalabilidad, fiabilidad y desempeño. Además da la posibilidad de interoperación con Microsoft Exchange que es la plataforma que actualmente utiliza el grupo ITABSA.

Este software se instalará en un servidor dedicado a esta aplicación. Una vez instalado, es necesario validar la información referente a la integración con el *Call Manager*, se define la numeración que tendrán los puertos de *voice mail* y números piloto, los cuales se incluyen en el plan de numeración detallado que se realizó en el *Call Manager*. Se definen las contraseñas de administración para Windows, DNS, base de datos SQL, y *password* para instalación de servicios *Unity*.

Una vez realizadas estas configuraciones, se procede a configurar los parámetros generales del *Unity* como son calidad de servicio, perfiles de usuarios por defecto, manejo de las llamadas y tipos de saludos. Posteriormente se configuran a los usuarios utilizando su nombre completo, alias y número de anexo.

### 2.5.3 TELÉFONOS IP, *SOFTPHONES* Y ATAs

Para este diseño se ha recomendado la utilización de Cisco IP Phone 7912G, 7940G y 7960G, *IP Conference Station* 7936 y además el adaptador Cisco ATA 186.

Los teléfonos IP Cisco poseen características avanzadas con facilidad de manejo. Permiten rapidez en el marcado, remarcado, transferencia de llamadas, identificación de llamadas, llamadas en conferencia, acceso a mensajes de voz y

envío de *mails* a través del teléfono. La ventaja de un teléfono IP sobre un teléfono analógico es que al ser parte de una red IP puede proveer servicios de datos como información actualizada a todo momento o servicio de ayuda en línea.

De las ventajas que proveen estos teléfonos se pueden destacar los botones dinámicos tipo "*soft*" que permiten acceder a las opciones que posee el teléfono a manera de un menú interactivo. Estos botones *soft* se los puede programar de acuerdo a las necesidades del usuario, por lo que se podría considerar que cada teléfono podrá personalizarse a las preferencias de cada persona. Pero además existirá una configuración por defecto que se la carga en el *Call Manager*.

Estos teléfonos poseen una pantalla en la que se despliega toda la información necesaria para acceder a las distintas opciones que ellos ofrecen. Tiene alta capacidad gráfica lo que también permite desplegar información basada en web.

Los teléfonos IP a diferencia de los teléfonos analógicos se los puede cambiar de lugar sin cambiar sus características como su número de la extensión, ya que el mismo no depende de su ubicación física. La dirección IP la puede obtener de manera estática o automática utilizando DHCP, como lo hacen todas las PCs del grupo ITABSA.

Los equipos de conferencia que se instalarán en las salas de reuniones son equipos altamente aptos para este tipo de salones. La disposición de sus micrófonos y altavoces permiten que el sonido sea claro desde cualquier punto de la sala, además de brindar las mejores características para realización de teleconferencias.

De la misma manera, los ATAs brindan una solución fácil y efectiva para conectar equipo analógico a la red IP. La utilización de equipos de fax dentro del grupo ITABSA es muy frecuente, por lo que no se va a prescindir de estos equipos, pero para transmitir su información se utilizarán estos adaptadores.

IP *Communicator* es un *softphone* de características muy buenas, que brinda todas las funciones y comodidades que posee un teléfono IP. Este software se instalará en *laptops*.

Después de energizar y conectar los equipos a la red, se les asigna la dirección IP, la numeración, y se realiza la configuración básica de cada uno.

#### 2.5.4 ROUTERS

Los *voice gateways* que se van a utilizar son el *Router Cisco 3825* para ITABSA y *Router Cisco 2800* para TANASA. Para la configuración de estos equipos se debe tener en cuenta el lado LAN y WAN de la red. Los puertos seriales WAN sincrónicos son de alta velocidad del tipo V.35 o RS232 y se los configura con protocolos TCP/IP o *Frame Relay*. Los puertos LAN 10/100 baseT se los configura en modo TCP/IP.

Posteriormente se configuran los puertos de voz en configuración de voz sobre IP según el diseño propuesto. Posteriormente se pasa a la configuración del IOS y de SRST para que cumpla con las funciones de *backup* del *Call Manager* principal.

#### 2.5.5 SWITCH CISCO CATALYST 4507

Este *switch* incluye excelentes prestaciones de calidad de servicio, lo cual es deseable en arquitecturas de convergencia de redes de voz y datos. Este *switch* brinda rápida actualización en los cambios de topología de la red, permite la creación de VLANs, monitoreo de tráfico y valoración de desempeño de la red. Soporta el protocolo de administración SNMP (*Simple Network Management Protocol*) y MIB (*Management Information Base*). Posee opción de monitoreo remoto RMON (*Remote Monitoring*).

Dentro de la instalación y configuración de este *switch* lo primero que se hace es el plan de direccionamiento IP, ya que éste va a ser el *switch* de *core*. Después se realiza la creación de las redes virtuales VLANs y el enrutamiento de las mismas. Se definen los enlaces de *trunk* y el dominio VTP; por último, los servicios de SNMP en el *switch*.

### 2.5.6 CISCO WORKS SNMS

Cisco Works es un software para administración de los equipos de la red. Para su funcionamiento necesita los módulos *Resource Manager Essentials* (RME) versión 3.5, *Cisco View* 6.0 y *What's up Gold* versión 8.0. Todos estos módulos vienen en el paquete de Cisco Works SNMS.

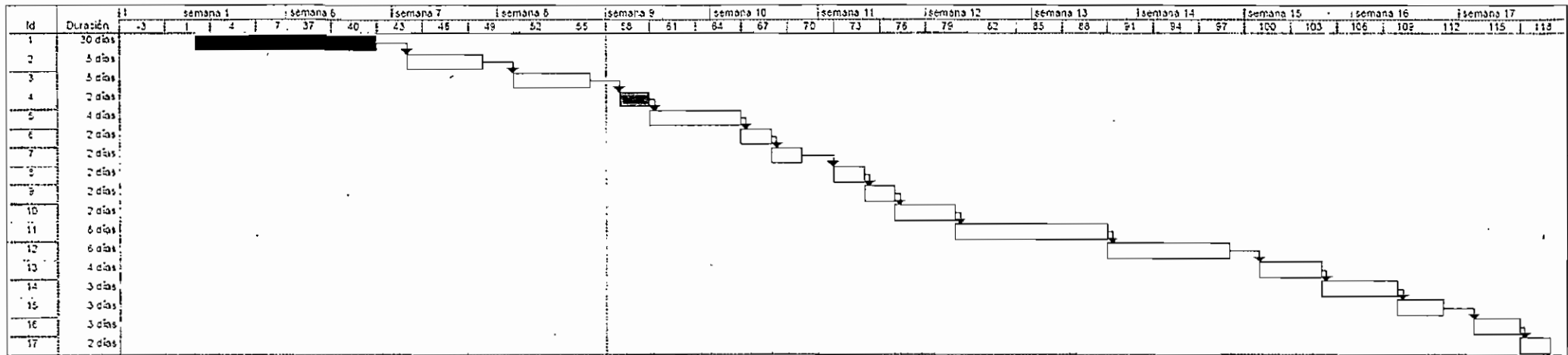
Estos módulos van a permitir el acceso, monitoreo y configuración gráfica de los dispositivos Cisco de la red LAN/WAN del grupo ITABSA.

## 2.6 CRONOGRAMA DE ACTIVIDADES

La solución de telefonía IP para el grupo ITABSA se la puede realizar en cuatro etapas. En una primera etapa se desarrollaría el diseño de la red para la implementación de telefonía IP, que es todo lo que contempla este proyecto de titulación.

La segunda etapa comprendería la instalación y configuración de los servidores en donde residirá el software para manejo de llamadas *Call Manager* y el software para mensajería unificada *Unity*.

Una tercera etapa que es muy importante es la de pruebas, ésta se la realiza antes de poner en producción los equipos para detectar posibles errores o fallas en la configuración de los sistemas. Aquí se realiza pruebas de todas las funcionalidades que poseen los equipos.





















- |    |  |   |         |
|----|--|---|---------|
| ID | TAREAS   |    | Etapa 1 |
| 1  | Diseño de Red Telefonía IP                                   |    | Etapa 2 |
| 2  | Configuración e instalación Call Manager                     |    | Etapa 2 |
| 3  | Configuración e instalación Unity                            |    | Etapa 2 |
| 4  | Pruebas de los servidores                                    |   | Etapa 2 |
| 5  | Configuración e instalación gateway router 3625 ITABSA       |  | Etapa 2 |
| 6  | Configuración e instalación gateway router 2800 TANASA Quito |  | Etapa 2 |
| 7  | Configuración e instalación Switch 4507 ITABSA               |  | Etapa 2 |
| 8  | Configuración e instalación Switch 4507 TAJIASA Quito        |  | Etapa 2 |
| 9  | Configuración e instalación router 2800 TAJIASA Durán        |  | Etapa 2 |
| 10 | Configuración e instalación router 2800 PROESA Alarazana     |  | Etapa 2 |
| 11 | Configuración de 100 teléfonos 7912G                         |  | Etapa 2 |
| 12 | Configuración de 70 teléfonos 7940G                          |  | Etapa 2 |
| 13 | Configuración de 46 teléfonos 7960G                          |  | Etapa 2 |
| 14 | Configuración de 14 Softphones                               |  | Etapa 2 |
| 15 | Configuración de 9 equipos de estaciones de conferencia 7936 |  | Etapa 2 |
| 16 | Configuración de 11 ATAs 186                                 |  | Etapa 2 |
| 17 | Pruebas con equipos en producción                            |  | Etapa 2 |

Figura 2.21 Cronograma de Actividades.

La tercera etapa es crítica ya que de ésta depende el correcto funcionamiento al momento de migrar la antigua red a la nueva red de convergencia que se propone.

La última etapa es la de instalación y puesta en marcha de todos los equipos. En este momento se definen los parámetros para la PSTN de los *gateways*, reemplazo de teléfonos analógicos por teléfonos IP, salida de producción de la antigua central telefónica y pruebas de correcto funcionamiento de la solución de telefonía IP.

En la figura 2.21 se detalla más claramente los tiempos estimados para la implementación de telefonía IP en el grupo ITABSA. Según el cronograma propuesto que se esquematiza, la implementación duraría 17 semanas.

## 2.7 ANÁLISIS DE COSTOS

A continuación, en la Tabla 2.3 se detallan los costos de los equipos que se necesitan para la solución de telefonía IP para el grupo ITABSA.

ITEM	CANTIDAD	PRECIO UNITARIO (USD)	PRECIO TOTAL (USD)
CALL MANAGER 4.1 PARA 300 USUARIOS	1	\$5.860,00	\$5.860,00
UNITY SERVER 4.0 PARA 300 USUARIOS	1	\$36.210,00	\$36.210,00
ROUTER GATEWAY 3825	1	\$13.573,00	\$13.573,00
SWITCH CENTRAL 4507R	2	\$27.500,00	\$55.000,00
TELÉFONOS IP 7912G	100	\$263,00	\$26.300,00
TELÉFONOS IP 7940G	70	\$360,00	\$25.200,00
TELÉFONOS IP 7960G	46	\$430,00	\$19.780,00
CONSOLA 7914 PARA TELÉFONO IP 7960	2	\$1.040,00	\$2.080,00
ATA 186	11	\$145,00	\$1.595,00
ESTACIÓN DE CONFERENCIA 7936	9	\$938,00	\$8.442,00
IP COMMUNICATOR	14	\$167,00	\$2.338,00
CISCO WORKS SNMS	1	\$2.090,00	\$2.090,00
ROUTER 2800	3	\$3.500,00	\$10.500,00
<b>TOTAL (sin impuestos)</b>			<b>\$208.968,00</b>

Tabla 2.3 Cuadro de Costos de Equipos Cisco.



Los precios presentados en la Tabla 2.3 son precios locales, a los que el grupo ITABSA adquiere a su proveedor. Además de los costos de los equipos se tiene los costos por el diseño y honorarios profesionales por trabajo de implementación. En la Tabla 2.4 se detallan estos costos.

ITEM	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
Servicios de diseño de red integrada de voz y datos para el grupo ITABSA	1	\$5.000,00	\$5.000,00
Servicios de implementación del sistema	1	\$10.000,00	\$10.000,00
<b>TOTAL (sin impuestos)</b>			\$15.000,00

Tabla 2.4 Cuadro de Costos de Honorarios Profesionales.

La implementación del sistema se la ha programado en un lapso de 8 semanas y media, como se puede observar en el cronograma de actividades previamente presentado. Para la implementación del sistema se contará con un equipo de 4 profesionales en el área de *networking*.

Adicionalmente, para la integración de la red de voz y datos del grupo ITABSA se requiere la contratación de 2 E1s, y además se necesita incrementar el ancho de banda de dos de los enlaces WAN del grupo ITABSA. Los enlaces que requieren aumentar en capacidad son los enlaces satelitales hacia PROESA Atarazana y TANASA Durán. Los costos de arriendo de estos enlaces se pagan mensualmente, por lo tanto hay que tomar en cuenta que éste es un gasto extra permanente que generará este proyecto. Estos enlaces se los seguirá contratando a Impsat. Actualmente, por los enlaces satelitales de 256 Kbps el grupo ITABSA paga 470 USD mensuales. Al aumentar la capacidad de estos enlaces a 448 Kbps, el valor a pagar sería de 614,40 USD. Al ser dos enlaces, supone un incremento mensual de 288,80 USD. Este incremento en los gastos mensuales se compensa en las planillas telefónicas, ya que no se usará la PSTN para las llamadas entre las oficinas de la empresa. En la Tabla 2.5 se detallan los valores a pagar por los enlaces que se requiere contratar.

ITEM	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
<b>COSTOS DE INSTALACIÓN</b>			
Contratación de E1s a Andínatel	2	\$2.000,00	\$4.000,00
<b>TOTAL (sin impuestos)</b>			<b>\$4.000,00</b>
<b>COSTOS DE OPERACIÓN</b>			
Costo mensual E1s	2	\$380,00	\$760,00
Enlace Belmonte - PROESA Atarazana (Enlace satelital 448 Kbps)	1	\$614,40	\$614,40
Enlace Belmonte - TANASA Durán (Enlace satelital 448 Kbps)	1	\$614,40	\$614,40
<b>TOTAL (sin impuestos)</b>			<b>\$1.988,80</b>

Tabla 2.5 Cuadro de Costos de Enlaces.

El grupo corporativo paga un rubro por el mantenimiento de las centrales telefónicas analógicas y cuando hay problemas puntuales se requiere de un técnico quien factura por cada visita. Además, actualmenté se usa el software tarifador Factel; este software también supone un gasto ya que se lo actualiza anualmente y se requiere una PC para que haga las veces de servidor para este software. Además como es un software propietario, cada vez que se tiene problemas con el mismo, es necesario llamar al proveedor de este software. Cada vez que el proveedor da soporte, cobra por ese servicio. El implementar telefonía IP en el grupo corporativo evitará todos estos gastos, ya que el mantenimiento de la red la seguirá realizando el administrador de la red. Y las aplicaciones extras que se necesita para telefonía, como es tener un control de tarificación y tráfico de llamadas, lo realiza el procesador de llamadas.

## CAPÍTULO 3

# PLANIFICACIÓN DE USO DE TELEFONÍA IP INALÁMBRICA

### 3.1 CONSIDERACIONES

La implementación de redes inalámbricas dentro del ambiente corporativo poco a poco se ha convertido en una necesidad. Son muchos los escenarios en los que las redes inalámbricas son útiles, y éste es el caso de TANASA, que al ser una planta de producción existen muchos usuarios con necesidad de movilidad. La flexibilidad que ofrece la telefonía IP inalámbrica incrementa la productividad y satisfacción en los usuarios.

La implementación de VoIP en una red inalámbrica es uno de los retos que las empresas de fabricación de equipo para *networking* se han puesto desde hace algunos años, y en la actualidad ya tienen soluciones eficientes y confiables. Al implementar voz sobre una red inalámbrica es necesario lidiar con los problemas inherentes a la transmisión de voz más los problemas de las redes WLAN. Cisco es uno de los fabricantes que posee el equipo necesario para este tipo de implementaciones. Cisco *Wireless IP Communications* ofrece soluciones para integración completa permitiendo acceder a una infraestructura inalámbrica de voz, vídeo y datos. Provee alta capacidad mientras mantiene un alto nivel de accesibilidad, calidad de servicio y seguridad.

La telefonía IP inalámbrica permite que un usuario esté disponible todo el tiempo, ya que puede llevar su teléfono consigo a cualquier lugar dentro del área de cobertura de la red inalámbrica. Está diseñado especialmente para usuarios que necesitan ser localizados en todo momento, usuarios que tienen que estar disponibles para dar decisiones de último minuto que siempre se presentan. La forma de ubicarles al momento es utilizando teléfonos celulares, pero esto es muy

costoso, pudiendo ahorrar costos y dar además mayor facilidad a los usuarios. El diseño que se hará en este Proyecto de Titulación corresponde a la planta de producción TANASA en Quito, pero este diseño en un futuro puede extenderse a las demás oficinas del grupo corporativo, ya que por su implementación será de gran beneficio dentro de la empresa.

Incrementar servicios de voz en una red inalámbrica de datos requiere políticas de calidad de servicio en la red. Además se debe tener muy en cuenta la seguridad, que siempre debe estar presente en las redes inalámbricas. Se debe recordar que con un buen receptor, un intruso podría acceder a la información de la red inalámbrica por lo que se deben aplicar políticas de acceso y encriptación.

Los beneficios de la telefonía IP inalámbrica son visibles, no necesita ningún otro tipo de dispositivo como celulares, *paggers* o servicio de radio. Por ejemplo, a los guardias de la planta se los podría proveer de teléfonos IP inalámbricos en lugar de radios, sin incrementar costos ya que se está utilizando la red propietaria de la empresa. Para los usuarios la ventaja de tener su extensión en todo momento es incomparable, siempre se los puede ubicar sin importar donde se encuentren. Además los teléfonos IP inalámbricos dan los mismos servicios que los teléfonos IP estacionarios, por lo que tienen todas las prestaciones de mensajería unificada en sus manos.

Existen varias consideraciones que se deben tomar en cuenta al momento de implementar voz sobre una red inalámbrica. Se detallarán estos tópicos a continuación.

### 3.1.1 INFRAESTRUCTURA PARA TELEFONÍA IP INALÁMBRICA

Para telefonía IP inalámbrica, la infraestructura necesaria es una red inalámbrica WLAN formada por *access points* y dispositivos finales de telefonía IP los cuales pueden estar basados en hardware y/o software. Una WLAN 802.11 brinda las mismas capacidades que una red cableada, es decir, transmisión de datos, voz y

vídeo. Una WLAN opera como un medio compartido, esto quiere decir que la transmisión de información desde y hacia todos los dispositivos que conforman la red se da sobre la misma conexión inalámbrica. El ancho de banda que posee un dispositivo para su transmisión depende de la distancia de éste hacia el *access point*, mientras más lejos esté, su ancho de banda será menor y por lo tanto también disminuirá su velocidad de transmisión.

El estándar IEEE 802.11 tiene algunos anexos en los cuales se define la frecuencia de trabajo y la velocidad de transmisión que alcanza en la transmisión de información al momento de utilizar la red WLAN. 802.11a establece una frecuencia de 5 GHz, alcanzando una velocidad de transmisión de 54 Mbps. El anexo 802.11b define una frecuencia de trabajo de 2.4 GHz, permitiendo obtener velocidades de transmisión de hasta 11 Mbps. El anexo que poco a poco va adquiriendo mayor popularidad es el 802.11g. Éste permite transmitir información hasta una velocidad de transmisión de 54 Mbps usando la frecuencia 2.4 GHz.

Un teléfono IP inalámbrico posee las mismas características de un teléfono IP cableado como es su similar funcionalidad en las llamadas y pantalla en la cual se pueden escoger diferentes opciones de configuración. Adicionalmente, un teléfono IP inalámbrico tiene características de seguridad que lo hacen tan confiable como un teléfono IP fijo e implementa calidad de servicio de acuerdo a lo requerido en una red inalámbrica 802.11.

Además se necesita un procesador de llamadas, que es el mismo que se emplea en la telefonía IP fija. Cisco *Call Manager* tiene excelentes capacidades para procesamiento de llamadas para cualquier infraestructura de red.

Dentro de la infraestructura para telefonía IP inalámbrica otro punto que se debe tomar en cuenta es la creación de VLANs separadas para voz y datos, así como se lo hace en las redes cableadas. Las VLANs proveen un mecanismo para segmentar las redes en dominios de *broadcast* más pequeños. Esto es importante en telefonía IP porque es necesario separar el tráfico de voz y datos en diferentes dominios.

Se recomienda configurar VLANs separadas para tráfico de voz y para tráfico de datos: una VLAN nativa para tráfico de datos y una VLAN auxiliar para tráfico de voz [29]. Una VLAN separada para voz permite dar prioridad de encolamiento, asegurando la calidad de servicio brindada. Cada VLAN se la debe mapear a un único SSID (*Service Set Identifier*) y a los usuarios se los asigna a su respectiva VLAN basados en este SSID. Cada VLAN puede usar un diferente mecanismo de seguridad.

Otra recomendación que Cisco realiza al momento de implementar telefonía IP inalámbrica es no mantener más de 15 a 25 dispositivos 802.11b por cada *access point* [29]. Con esto se garantiza una calidad de servicio adecuada para todos los usuarios. Al momento de dimensionar la red se debe tomar en cuenta que no se puede mantener más de 7 llamadas G.711 al mismo tiempo, o más de 8 llamadas G.729 simultáneamente.

Estas consideraciones se deben tener en cuenta ya que con más dispositivos simultáneos en el mismo *access point* se disminuye el ancho de banda para cada dispositivo, lo que reduce notablemente la calidad de servicio y por lo tanto la calidad de las llamadas se degradará. También se debe controlar la transmisión de datos con políticas de priorización de la voz ya que si no se realiza esto también se afecta la calidad de las transmisiones de voz.

De acuerdo a estudios realizados por Cisco, se recomienda que no se mantenga más de 450 a 600 teléfonos IP Cisco por subred o por VLAN [29]. El tráfico que se debe mantener sobre la red en ambientes de telefonía IP inalámbrica debe ser tráfico *unicast*, no *multicast*. Esto se recomienda porque los teléfonos inalámbricos funcionan en modalidad de conservación de energía para mantener por más tiempo las baterías cargadas y el tráfico *multicast* desgasta innecesariamente la batería con tráfico que no está destinado específicamente para ese dispositivo.

### 3.1.2 REQUERIMIENTOS DE RADIO FRECUENCIA

Existen varios requerimientos de radio frecuencia que se deben tomar en cuenta dentro de la infraestructura inalámbrica necesaria para construir un sistema de telefonía IP inalámbrica en un ambiente empresarial. Lo primero que se debe hacer es localizar los sitios donde los *access point* y las antenas deberán ubicarse para evitar interferencias. Esto también determinará la cantidad de *access points* necesarios para mantener total cobertura sobre el área que se necesita.

Para mejorar las características de *roaming* y asegurar un adecuado funcionamiento de los teléfonos IP inalámbricos se recomienda que al programar los *access points* se usen solamente canales que no se superpongan entre ellos. Además se debe deshabilitar la opción de búsqueda del canal menos congestionado. Si esta opción está habilitada, el *access point* cambiará a un canal diferente cada vez que por alguna razón se lo reinicie. Una selección randómica de canales causa incremento en los tiempos de *roaming* porque el teléfono tiene que revisar todos los canales en lugar de solo un grupo pequeño de canales activos.

Se deben usar canales que tengan una diferencia de mínimo 5 canales de radio de separación, por ejemplo los canales 1, 6 y 11, de esta manera no se superpondrán. En la figura 3.1 se puede ver la disposición de las celdas con los diferentes canales para que no se superpongan entre ellos. Este gráfico muestra las celdas de los *access point* superpuestos en un porcentaje del 15% al 20% con las celdas adjuntas. Esta configuración además de proveer redundancia cumple con los requerimientos para superposición de los canales. Esto reduce el ambiente de ruido en cada canal. Además se puede usar el mismo grupo de canales en toda la red, lo que ayuda a reducir los tiempos de *roaming*.

Se debe tener cuidado al escoger el lugar donde se colocarán los *access points*, ya que si se los ubica en lugares no apropiados se puede tener problemas de distorsión en la propagación de la señal. Por ejemplo, si se coloca sobre vigas que posean muchos vértices como las vigas tipo I, éstas crean muchas

reflexiones de la señal. Estas reflexiones generan una pobre calidad de la señal porque existirán puntos en los cuales se anulará la señal y otros puntos generarán interferencia por múltiples caminos que tomen las señales reflejadas. Esto se puede ver más claramente en la figura 3.2.

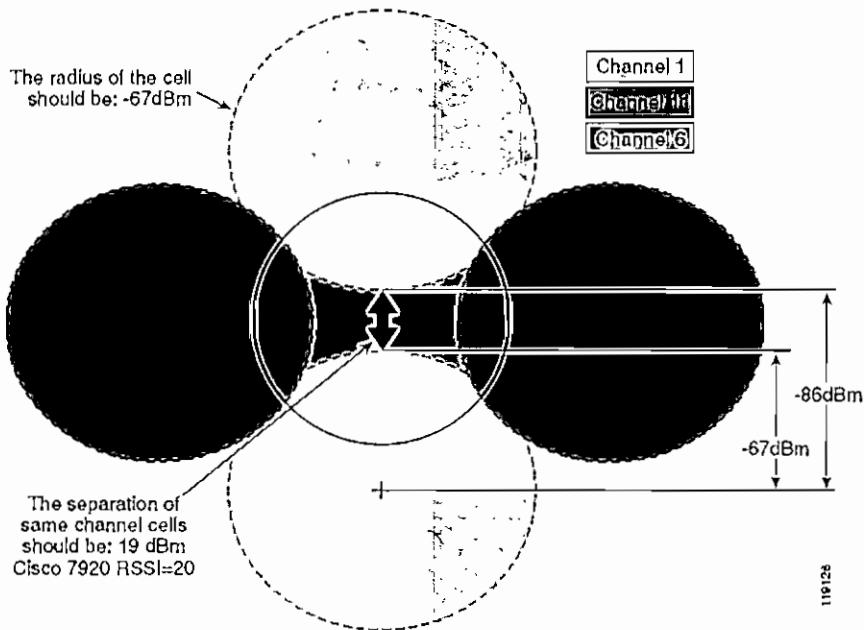


Figura 3.1 Superposición de canales en celdas inalámbricas de *access points* [29].

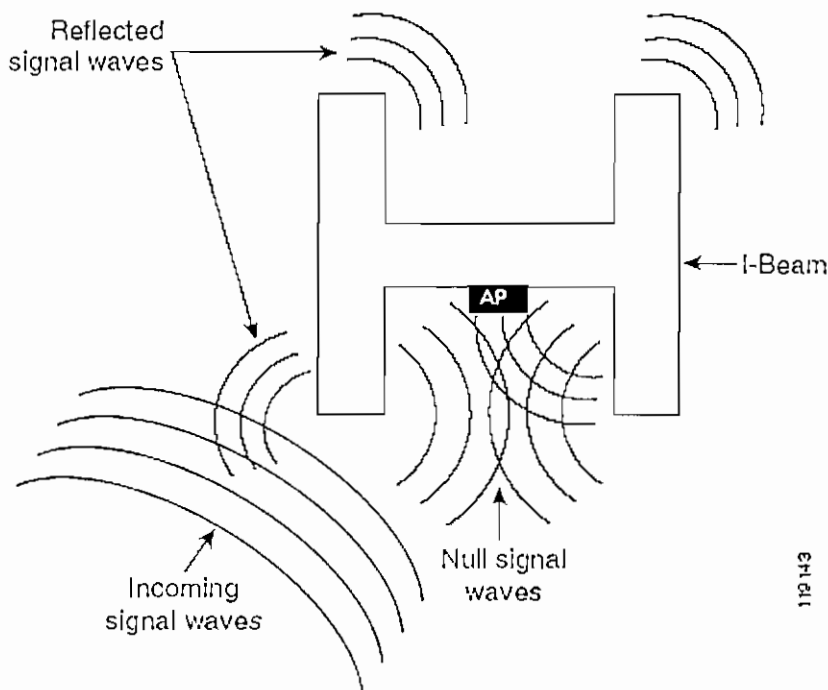


Figura 3.2 Distorsión causada en la señal por mala ubicación de un *access point* [29].



Éste es solo un ejemplo de lo que causa una mala ubicación de un *access point*. En la figura 3.3 se indica un *access point* Cisco AP 1200 colocado de forma correcta en el techo con las antenas en una posición omni-direccional o en la parte alta de una pared. Ésta es una buena ubicación ya que no se producirán reflexiones de señal perjudiciales.

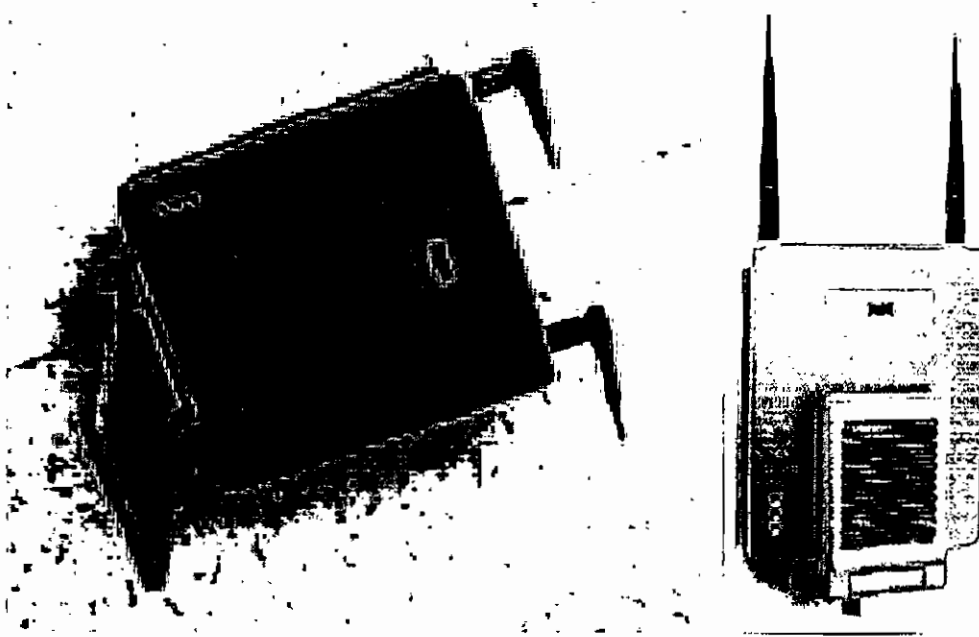


Figura 3.3 Ubicación correcta de un *access point* [29].

Hay que recordar que existen otras fuentes de interferencia que afectan una WLAN. Esta interferencia puede ser generada por hornos microonda, dispositivos *bluetooth*, o cualquier dispositivo que opere en la banda de 2.4 GHz. La interferencia y la distorsión causada por múltiples señales reflejadas causan la fluctuación de la señal transmitida.

La interferencia disminuye la relación señal a ruido (SNR). Para los teléfonos IP inalámbricos Cisco la relación señal a ruido ideal es de 25 dB. Por ejemplo, si la potencia de la señal de ruido es de 73 dBm y la potencia de la señal recibida por el teléfono es de 98 dBm, entonces la relación señal a ruido será de 25 dB. La figura 3.4 esquematiza esta relación.

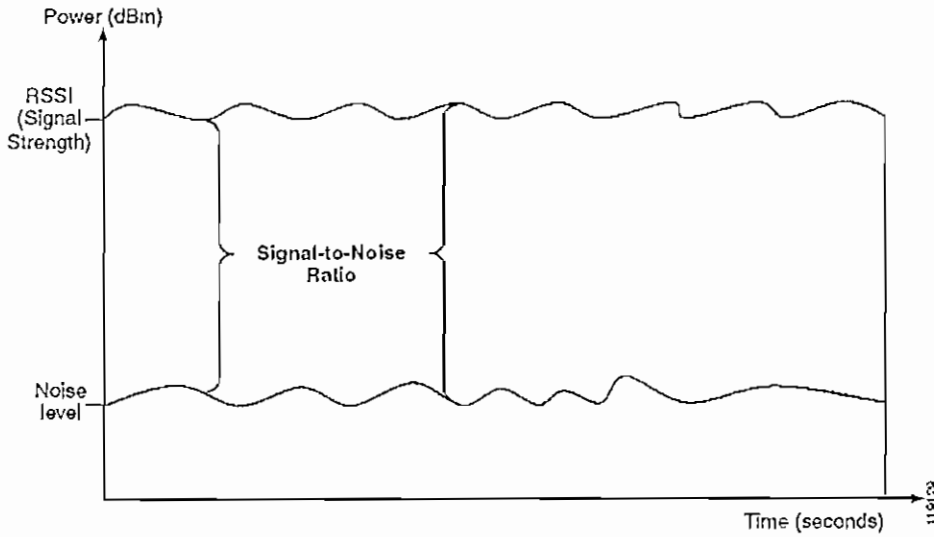


Figura 3.4 Relación señal a ruido [29].

Los objetos por los que una señal atraviesa también atenúan esta señal. En la Tabla 3.1 se indican valores de atenuación de la señal que producen varios objetos.

Objeto en el camino de la señal	Atenuación de la señal (dB)
Pared	3
Pared de ladrillo	6
Ventana de vidrio	3
Puerta de metal	6
Cuerpo humano	3

Tabla 3.1 Atenuación de la señal causada por varios tipos de objetos [29].

Por lo tanto se debe tomar en cuenta algunos aspectos al momento de decidir donde colocar los *access point* para asegurar que los niveles de recepción de la señal sean los adecuados para todos los dispositivos que están dentro del área de cobertura de la red inalámbrica.

### 3.1.3 SEGURIDAD

La seguridad es uno de los temas más importantes siempre que se esté hablando de redes inalámbricas. Las señales inalámbricas pueden ser receptadas utilizando un receptor lo suficientemente potente, por lo tanto se debe tener en cuenta políticas de autenticación y de encriptación de la señal. Las redes inalámbricas en las que se implementa telefonía IP inalámbrica deben asegurar que el tráfico de voz se encuentre protegido.

Los métodos más utilizados para autenticación y encriptación son: *static WEP (Wired Equivalent Privacy)* y *EAP (Extensible Authentication Protocol)*.

WEP es un mecanismo utilizado para proteger las transmisiones entre un *access point* y un dispositivo inalámbrico. Trabaja en la capa de enlace del modelo OSI y se basa en compartir una misma clave secreta entre el *access point* y los dispositivos que conforman la WLAN.

Una clave estática WEP es una clave compuesta de 40 o 128 bits que la define estáticamente el administrador de la red. Esta clave se la define en el *access point* y en todos los dispositivos que se conectan con éste, y deberá ser ingresada manualmente. La autenticación de los dispositivos la realiza el *access point* verificando la coincidencia de la clave que posee el dispositivo que intenta ingresar a la red.

EAP provee autenticación centralizada y distribución dinámica de las claves. Busca autenticación mutua entre el cliente y el servidor de autenticación. Las claves de encriptación se las envía después de que el cliente se ha autenticado. Tiene una política de control centralizada, con tiempos de caducidad para las sesiones, y re-autenticación y regeneración de claves al volver a ingresar en la red [30].

Posterior a la autenticación EAP mutua entre el dispositivo y el *access point*, se proporciona la clave WEP que se utilizará para esa sesión. Al transmitir de esta

manera la clave, ésta nunca se la transmite en claro por lo que la clave está protegida.

Cisco posee una versión propietaria de EAP que se encuentra implementada en todos sus equipos. Esta versión se llama LEAP (*Lightweight Extensible Authentication Protocol*).

LEAP permite a los dispositivos de la red autenticarse mutuamente desde el teléfono hacia el *access point* y del *access point* hacia el teléfono. Esta autenticación se basa en un nombre de usuario y un *password*. Después de la autenticación, una clave dinámica se usa para la encriptación de la información.

### 3.1.4 CALIDAD DE SERVICIO (QoS)

La calidad de servicio es primordial para asegurar tráfico en tiempo real como lo es el tráfico de voz. Es necesario que la transmisión de voz sea fiable, con bajo nivel de retraso, bajo *jitter* y poca o ninguna pérdida de paquetes. QoS asegura que el tráfico de voz sea prioritario cuando está atravesando la red.

La calidad de servicio en una WLAN es un poco más difícil de mantener que en redes cableadas porque una red inalámbrica posee un medio compartido. Al decir que una WLAN opera como un medio compartido se quiere decir que todos los dispositivos de la red ingresan a ella compartiendo la misma conexión inalámbrica.

Una WLAN 802.11b emplea el método de acceso al medio CSMA/CA (*Carrier Sense Multiple Access / Collision Avoidance*). Una red inalámbrica no utiliza detección de colisión, las WLAN usan prevención de colisión [29]. En lugar de que cada estación trate de transmitir al instante en que el medio de transmisión está libre, los dispositivos en una WLAN usan mecanismos de prevención de colisión para evitar que muchas estaciones transmitan al mismo tiempo, así se evitan colisiones.

Para calidad de servicio en redes WLAN el modelo utilizado para la transmisión de datos es DCF (*Distributed Coordination Function*). DCF se encarga de algunos eventos dentro del proceso de transmisión. Para empezar, después de que una trama ha sido transmitida y detectada por otros dispositivos finales de la red, cada uno de estos dispositivos espera un lapso de tiempo llamado IFS (*Inter-Frame space*, espacio entre tramas). Después de que el IFS ha pasado, los dispositivos empiezan el proceso para prevención de colisiones.

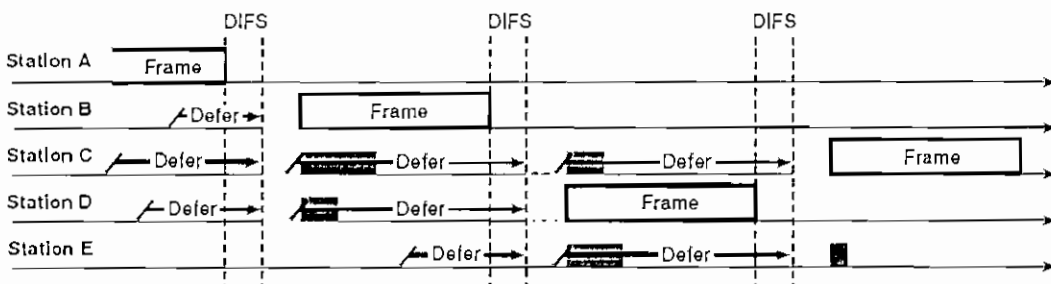
El proceso de prevención de colisiones utiliza dos valores para su procedimiento. Estos valores son CWmin (*Contention Window minimum*) y CWmax (*Contention Window maximum*). El valor de CW determina la cantidad de tiempo adicional que el dispositivo final debe esperar después del IFS para poder transmitir un paquete. El valor de CW se lo determina con un procedimiento sencillo. Después de que el tiempo IFS ha pasado, el dispositivo final selecciona un valor entre 0 y CWmin. Este dispositivo espera ese tiempo después del cual evalúa si el medio está disponible para la transmisión. Si es así, el dispositivo transmite su paquete, de lo contrario espera a que termine el tiempo de transmisión de ese paquete, más un tiempo IFS al que se adiciona el doble del tiempo CW que se tomó en el anterior intento de transmisión del paquete. El dispositivo continúa realizando este procedimiento, duplicando el tiempo CW anterior hasta lograr transmitir el paquete o hasta alcanzar el CWmax.

EDCF (*Enhanced DCF*) es una técnica de Cisco aplicada en sus equipos. EDCF permite que los dispositivos finales sean sensitivos al retraso del tráfico multimedia y que modifiquen sus valores de CWmin y CWmax, permitiendo acceso más frecuente al medio. En la figura 3.5 se esquematiza el modelo DCF y EDCF.

En la figura 3.5 se puede ver los eventos que ocurren cuando un dispositivo final intenta transmitir información, DCF es el responsable de que estos eventos ocurran. A continuación se realizará una explicación de los eventos DCF [29].

1. Después de que una trama ha sido enviada y detectada por el resto de dispositivos finales, cada uno de éstos espera por un periodo de tiempo IFS. El IFS que utilizan los dispositivos finales se llama DIFS (*Distributed IFS*).
2. Después de que ha terminado el tiempo de espera IFS los dispositivos finales empiezan su proceso de prevención de colisiones. Este proceso utiliza los valores CW de los cuales ya se habló anteriormente. El CW determina el tiempo adicional al IFS que debe esperar el dispositivo final antes de intentar transmitir un paquete.
3. Si después de este tiempo de espera el dispositivo final verifica que puede enviar su trama, lo hace. De lo contrario, si el medio sigue ocupado, vuelve a repetir el paso 2 duplicando el valor CW que tomó en ese paso. Este proceso se repite hasta que se haya duplicado tantas veces el valor CW que alcanza el valor CWmax.

802.11b DCF Model



802.11b EDCF Model

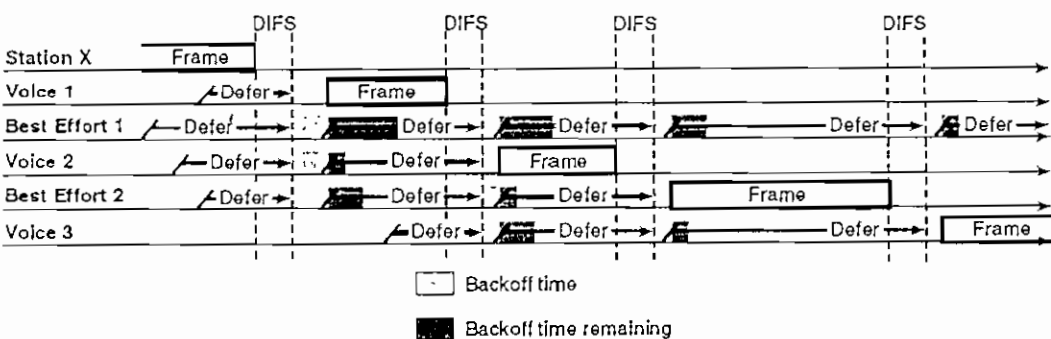


Figura 3.5 Modelo DCF y EDCF [29].

EDCF es una técnica especial utilizada por los teléfonos IP inalámbricos porque permite a los dispositivos finales detectar el tráfico multimedia que es sensible al retraso. Esto permite modificar los valores de CWmin y CWmax para permitir acceso más frecuente al medio. En la figura 3.5 se puede observar que los dispositivos de voz poseen tiempos CW menores que los de los dispositivos de datos, por lo tanto su acceso al medio es más rápido que el de los dispositivos de datos.

El proceso de encolamiento se lo puede realizar de acuerdo al ToS (*Type of Service*), basado en listas de acceso de capa 2 o capa 3, en VLANs, o en registro dinámico de los dispositivos, como los teléfonos IP.

Los *access point* soportan varias colas, por ejemplo, los *access point* Cisco soportan hasta ocho colas. Se recomienda tener solo dos colas para de esta manera asegurar la mejor calidad de servicio para voz. Todo el tráfico en tiempo real que es el tráfico de voz se lo debe colocar en una cola de alta prioridad; y el resto de tráfico, que es el de datos, se lo colocará en otra cola basada en la técnica del mejor esfuerzo.

Existe un número ideal de equipos que se pueden asociar a un mismo *access point* simultáneamente. Este número es entre 15 y 25 ya que se está utilizando equipos de transmisión de voz y de datos. Si se excede este número, se incrementa la posibilidad de introducir retraso en la transmisión de los paquetes y *jitter*.

### **3.2 PROPUESTA DE DISEÑO DE LA RED**

En el capítulo anterior se analizó el diseño de la convergencia de voz y datos sobre la red de datos del grupo ITABSA. Ahora, se analizará el diseño de telefonía IP inalámbrica. El diseño de telefonía IP inalámbrica se basa en la misma infraestructura básica para telefonía IP que ya se la desarrolló anteriormente.

Se utilizará el mismo servidor para procesamiento de llamadas y para mensajería unificada. Esto quiere decir que el servidor en el que está la aplicación *Cisco Call Manager 4.1* y el servidor donde se encuentra *Unity 4.0* serán los servidores que también soporten la infraestructura de telefonía IP inalámbrica. De igual manera se utiliza el mismo *gateway* que el de la telefonía IP fija; es decir, la telefonía IP inalámbrica se unirá a la infraestructura ya antes diseñada.

La propuesta que se presenta pretende incluir una WLAN en TANASA Quito, que es la planta de producción. Sobre esta WLAN se transmitirá tanto voz como datos. Esta red también se incluye dentro del plan de convergencia de voz y datos sobre una sola red. La razón por la que se ha escogido TANASA para el diseño de telefonía IP inalámbrica es por su necesidad de este tipo de servicio.

TANASA al ser una planta de producción está conformada por varios sectores dentro de una extensa área, por lo tanto las distancias entre un sitio y otro son algo lejanas. Aquí existe personal que necesita movilizarse todo el tiempo, por ejemplo, el personal de ingeniería muy pocas veces se encuentra en sus respectivas oficinas. Los ingenieros de la planta tienen que movilizarse por todas las áreas para controlar los procesos; ellos necesitan ser ubicados en todo momento porque se los puede necesitar en otro sitio. Al momento, en TANASA lo que se hace es mantener un sistema de altavoces por donde se llama a la persona que se busca. Esta persona se comunica con la recepcionista y ésta le informa si se le necesita en algún lado o si tiene una llamada. Este método no es eficiente ya que muchas veces la persona buscada no escucha el llamado, o no tiene un teléfono cerca para comunicarse. Es así como se ve la necesidad de telefonía IP inalámbrica, con la que la persona que posea un teléfono IP inalámbrico estará directamente disponible en todo momento.

La infraestructura que se tendrá es el teléfono Cisco 7920 como dispositivo final al usuario, éste se asociará a un *access point* Cisco 1200 el cual se unirá a la infraestructura de la red cableada de TANASA. De aquí tendrá el mismo tratamiento que la telefonía IP fija, es decir, su procesador de llamadas será Cisco



*Call Manager 4.1* y *Unity 4.0* será la aplicación para mensajería unificada. Como se dijo en el capítulo anterior, ambos servidores se encontrarán centralizados en el edificio Belmonte en el centro de cómputo principal del grupo ITABSA. En la figura 3.6 se esquematiza esta infraestructura.

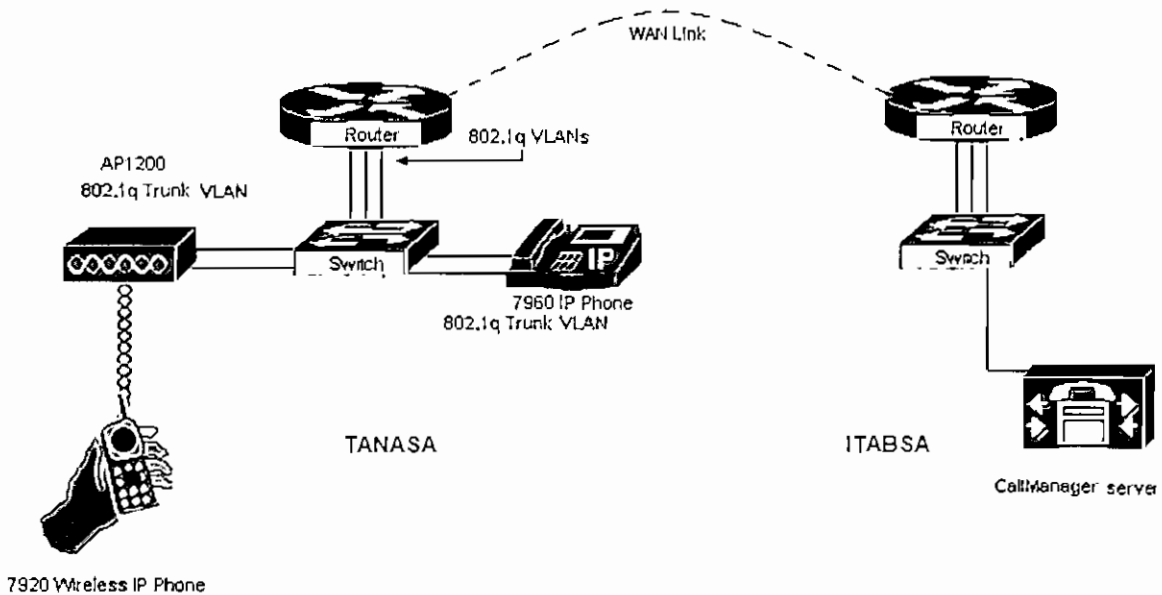


Figura 3.6 Infraestructura telefonía IP inalámbrica.

### 3.2.1 ACCESS POINT

Para el diseño de telefonía IP inalámbrica para TANASA se propone el uso de Cisco Aironet 1200 *Access Point*. Éste es un *access point* que soporta los estándares 802.11 a/b/g. Se ha escogido este *access point* porque sus características técnicas permiten la transmisión de información de datos y de voz.


Existen dos series de *access point* Cisco que nos ofrecen las características técnicas necesarias para los servicios que se van a brindar, estas son la serie 1200 y la serie 1300. La serie 1200 está diseñada para ambientes como oficinas o áreas cubiertas en las que se pueda tener interferencias de radiofrecuencia. La serie 1300 está diseñada para ser usada en áreas descubiertas. Como el ambiente en el cual va a ser usado es una fábrica, la serie 1200 es la que más se adapta a las necesidades. Todos los *access points* se los colocará dentro de los

galpones, por lo tanto se encontrarán en áreas cubiertas, y además son áreas que pueden estar propensas a sufrir interferencias de radiofrecuencia debido a los equipos y maquinarias que están operando todo el tiempo dentro de la fábrica. La tabla 3.2 muestra las recomendaciones del fabricante.

Cisco Series	Ambientes de oficina o similares	Ambientes de áreas cubiertas propensas a interferencias RF	Áreas descubiertas
1200 Series	Recomendado	Recomendado	Recomendado
1300 Series	No Recomendado	No Recomendado	Ideal

Tabla 3.2 Cisco Aironet *Access Point* para diferentes ambientes [8]

La tabla 3.3 muestra las características técnicas de los *access point* Cisco Series 1200 y 1300, como lo muestra el fabricante.

Producto	Características/Beneficios
<p>Cisco Aironet 1200 Series Access Point</p>  <p>Access point con conectores para antena de diversidad dual para ambientes con interferencias RF.</p>	<p>Trabaja con los estándares 802.11b y 802.11g ofreciendo capacidad de hasta 54 Mbps</p> <p>Puede ser actualizado para soportar 802.11a con un módulo para actualización de hardware</p> <p>Conectores externos para antenna 2.4 GHz dual-diversity</p> <p>Carcasa metálica resistente</p> <p>16 MB de memoria con 8 MB of almacenamiento</p> <p>Rango de temperatura de operación de -4 a 131°F (-20 a 55°C)</p> <p>Soporta alimentación eléctrica en línea</p> <p>Puerto de consola para administración</p> <p>Sistema completo integrado para montaje</p>


<p>Cisco Aironet 1300 Series Outdoor Access Point/Bridge</p>  <p>Access point de una sola banda y bridge inalámbrico con wireless bridge con carcasa NEMA-4 para colocación en áreas externas</p>	<p>Trabaja bajo el estándar 802.11g ofreciendo capacidad de 54 Mbps</p> <p>Conectores externos para antenna 2.4 GHz dual-diversity</p> <p>Se lo puede configurar como un access point autónomo, un bridge inalámbrico o un bridge de grupo de trabajo</p> <p>Soporta configuraciones punto a punto o punto multipunto</p> <p>Carcasa NEMA-4 resistente a todo tipo de clima</p> <p>Antenas externas opcionales para mayor flexibilidad</p> <p>16 MB de memoria con 8 MB of almacenamiento</p> <p>Rango de temperature de de -22 a 131°F (-30 a 55°C)</p> <p>Soporta alimentación eléctrica en línea</p> <p>Puerto de consola para administración</p> <p>Sistema completo integrado para montaje.</p>
--	--

Tabla 3.3 Características Cisco Aironet *Access Points* [8]

Para el correcto funcionamiento de la red inalámbrica se deben considerar algunos parámetros en la configuración de los *access point*. Esta configuración asegurará buenas características de seguridad y de calidad de servicio en la red inalámbrica.

Una WLAN mal configurada compromete la seguridad de toda la red corporativa. La red inalámbrica posee acceso total a todas las funciones de la red de la empresa y se conecta a la infraestructura de la red cableada. El manejo de las interfaces y el acceso a las opciones de configuración de los *access points* debe ser asegurada usando nombres de usuario y *passwords*.

Como ya se ha remarcado anteriormente, es necesario tener diferentes VLANs para las aplicaciones de voz y datos. Cada una de estas VLANs se identifica utilizando un nombre SSID. Los *access points* se conectan al ambiente cableado por un enlace de *trunk* a los *switches* de la red cableada. La razón de realizar un enlace de *trunk* es porque éste provee identificación de las VLANs para las tramas que están ingresando de la red inalámbrica a la cableada y viceversa. Es necesario este proceso para poder identificar si el tráfico pertenece a la VLAN de voz o a la de datos.

Para realizar la conexión de los *access points* a la red cableada con enlaces de *trunk* se debe utilizar un *switch* que brinde funcionalidades de capa 3. Todos los *switches* de la red cableada de TANASA son *switches* que permiten funcionalidades de capa 3, por lo que no hay ningún problema al momento de conectar los *access points* a los *switches* de la red cableada. Para este diseño se prevé que la red inalámbrica tenga acceso total a la red cableada, por lo tanto no es necesario configurar restricciones de acceso en el *switch*.

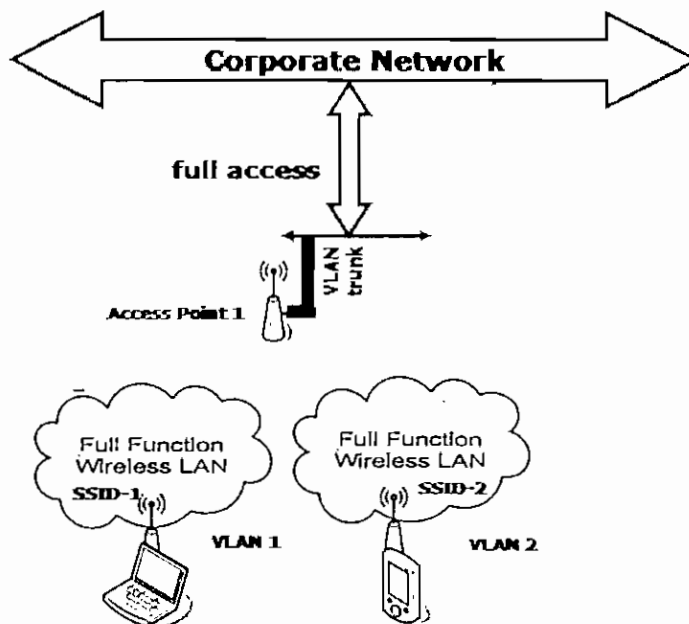


Figura 3.7 VLANs en la red inalámbrica [15].

En cada *access point* se ingresa manualmente el SSID para la seguridad de la identidad de los *access point* que conforman la red inalámbrica. Por

características de seguridad, se debe implementar un método de autenticación de dos pasos. Primero se tiene una autenticación abierta para asociarse con el *access point*. Esta asociación requiere el uso de LEAP. Después se asegura la transferencia de información en la red inalámbrica habilitando WEP tanto en los *access points* como en los dispositivos finales. Se tendrán claves dinámicas por sesión.

En el *access point* se habilitará la opción de que el vector de inicialización sea randómico y de prevención de vectores de inicialización débiles que es una opción que proporcionan los *access point* Cisco para prevenir ataques. Además se debe habilitar BKR (*Broadcast Key Rotation*) en los *access points* y en los dispositivos finales. Es mandatorio el proceso de autenticación de *MAC Address*.

En el capítulo anterior se realizó el *IP planning* para definir qué direcciones IP se utilizarán para los dispositivos que forman parte de la infraestructura de telefonía IP. Se tomó la subred 10.204.22.0/24 para TANASA. De esta subred se tomará las direcciones IP para los *access points* que formarán parte de la red inalámbrica. En la Tabla 3.2 se definen las direcciones IP asignadas a los *access points*, más adelante se indicará por qué se definieron seis *access points*. Es necesario recordar que estas direcciones IP que se definen estáticamente se las debe excluir del rango de direcciones IP usadas en el servidor DHCP para los teléfonos IP.

UBICACIÓN	DISPOSITIVO	DIRECCIÓN IP	MÁSCARA
TANASA	<i>Access Point 1</i>	10.204.22.2	255.255.255.0
TANASA	<i>Access Point 2</i>	10.204.22.3	255.255.255.0
TANASA	<i>Access Point 3</i>	10.204.22.4	255.255.255.0
TANASA	<i>Access Point 4</i>	10.204.22.5	255.255.255.0
TANASA	<i>Access Point 5</i>	10.204.22.6	255.255.255.0
TANASA	<i>Access Point 6</i>	10.204.22.7	255.255.255.0

Tabla 3.4 IP *Planning* WLAN.

La configuración del IOS de los Cisco 1200 *Access Points* se lo puede hacer vía *browser*. La autenticación para ingresar a la configuración se la debe proteger por un *password* de administrador. Se pueden configurar las características de las interfaces de red, las características de seguridad donde se tiene el *SSID manager*. También se debe configurar el *RADIUS Server* que es el que provee el acceso a la base de datos de usuarios.

Para mostrar el proceso de configuración de los *access points*, se mostrará paso a paso las pantallas de configuración. La figura 3.8 muestra la configuración de los parámetros básicos de red como son dirección IP, máscara de subred y *gateway*. Aquí también se define el *SSID*.

Close Window [http://10.204.22.200:45533/ap\\_express-setup.htm](#) Copyright (c) 1992-2003 by Cisco Systems, Inc.

Figura 3.8 Configuración de parámetros de red en IOS Cisco 1200 *Access Point*.

A continuación se configura la interfaz de red. La figura 3.9 muestra esta pantalla de configuración.

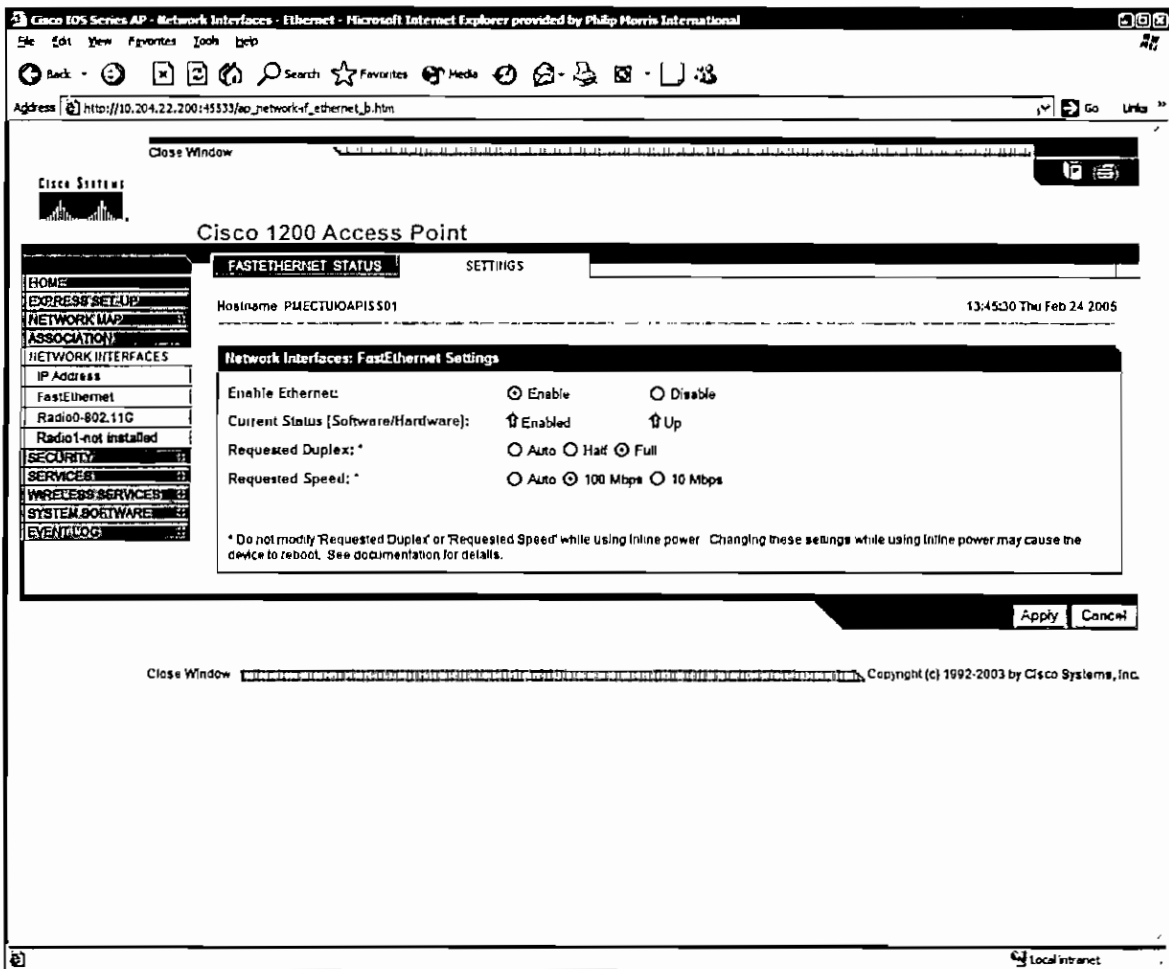


Figura 3.9 Configuración de interfaz de red en IOS Cisco 1200 Access Point.

Como siguiente paso se tiene la configuración de los parámetros de radio en los cuales operará el *access point*. La figura 3.10 muestra esta configuración.

Para prevenir accesos no autorizados se configura los accesos de administrador (figura 3.11). Para la autenticación se definen los parámetros de SSID y los métodos de autenticación que se van a usar. La configuración de los parámetros de seguridad que se hará para los *access points* de la WLAN de TANASA se la puede ver en la figura 3.12.

RADIO0-802.11G STATUS DETAILED STATUS SETTINGS CARRIER BUSY TEST

Hostname: PMECTUCAP15501 15:52:15 Thu Feb 24 2005

**Network Interfaces: Radio0-802.11G Settings**

Enable Radio:  Enable  Disable

Current Status (Software/hardware): Enabled ↑ Up ↑

Role In Radio Network: (Fallback mode upon loss of Ethernet connection)

- Access Point Root (Fallback to Radio Island)
- Access Point Root (Fallback to Radio Shutdown)
- Access Point Root (Fallback to Repeater)
- Repeater Non-Root

Data Rates:

	Best Range	Best Throughput	Default
1.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
2.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
5.5Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
6.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
9.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
11.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
12.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
18.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
24.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
36.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
48.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
54.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable

CCK Transmitter Power (mW):  1  5  10  20  30  50  Max

OFDM Transmitter Power (mW):  1  5  10  20  30  Max

L1rth Client Power (mW):  1  5  10  20  30  50  Max

Default Radio Channel: Channel 1 - 2412 MHz Channel 1 2412 MHz

Least Congested Channel Search:  
(Use Only Selected Channels)

- Channel 1 - 2412 MHz
- Channel 2 - 2417 MHz
- Channel 3 - 2422 MHz
- Channel 4 - 2427 MHz
- Channel 5 - 2432 MHz
- Channel 6 - 2437 MHz
- Channel 7 - 2442 MHz
- Channel 8 - 2447 MHz
- Channel 9 - 2452 MHz
- Channel 10 - 2457 MHz
- Channel 11 - 2462 MHz
- Channel 12 - 2467 MHz
- Channel 13 - 2472 MHz

World Mode Multi-Domain Operation:  Enable  Disable

Radio Preamble:  Short  Long

Receive Antenna:  Diversity  Left  Right

Transmit Antenna:  Diversity  Left  Right

Aironet Extensions:  Enable  Disable

Ethernet Encapsulation Transform:  RFC1042  802.1H

Reliable Multicast to WGB:  Disable  Enable

Public Secure Packet Forwarding:  Enable  Disable

Short Slot-Time:  Enable  Disable

Beacon Period:  (20-4000 Kusec) Data Beacon Rate (DTIM):  (1-100)

Max. Data Retries:  (1-128) RTS Max. Retries:  (1-128)

Fragmentation Threshold:  (256-2346) RTS Threshold:  (0-2347)

Repeater Parent AP Timeout:  (0-65535 sec)

Repeater Parent AP MAC 1 (optional):  (HH:HH:HH:HH:HH:HH)

Repeater Parent AP MAC 2 (optional):  (HH:HH:HH:HH:HH:HH)

Repeater Parent AP MAC 3 (optional):  (HH:HH:HH:HH:HH:HH)

Repeater Parent AP MAC 4 (optional):  (HH:HH:HH:HH:HH:HH)

Figura 3.10 Configuración de interfaz de red en IOS Cisco 1200 Access Point.



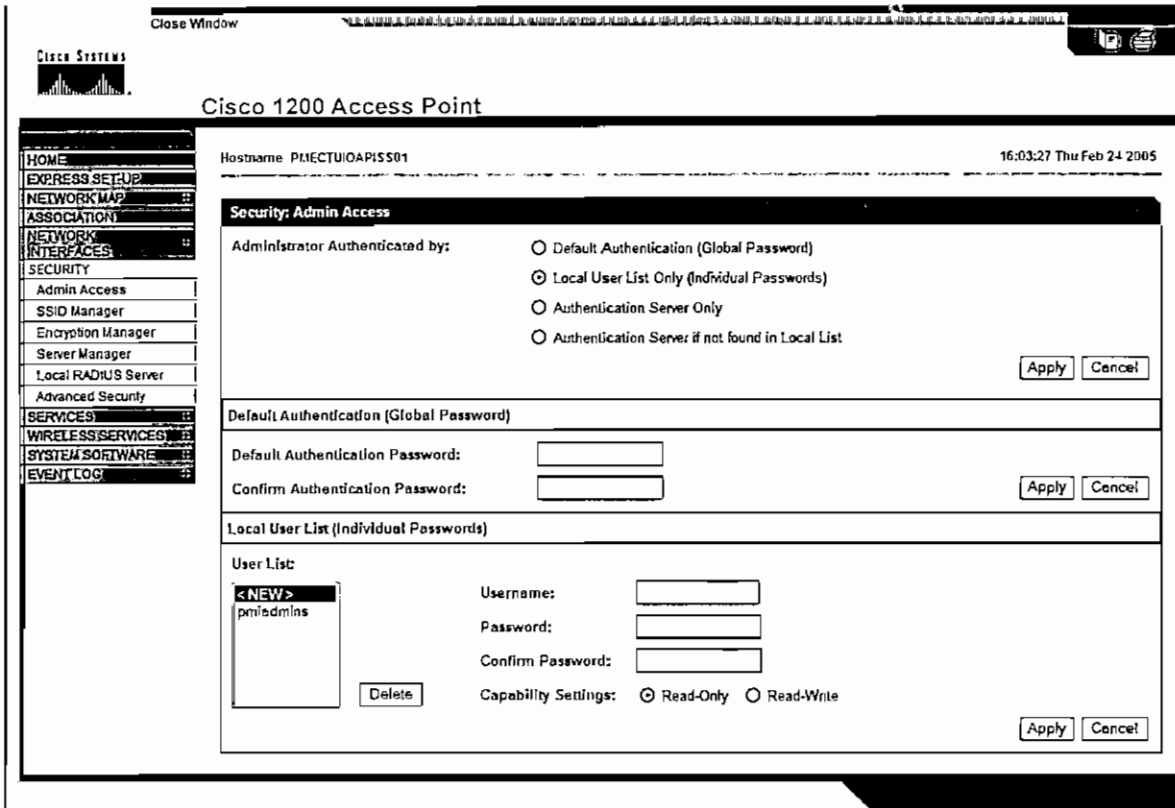


Figura 3.11 Configuración de accesos de administrador en IOS Cisco 1200 Access Point.

En la parte de la configuración de la seguridad, se configura el método de encriptación que se va a usar. En el caso de la red inalámbrica de TANASA se usará WEP con clave de 128 bits. Esta pantalla de configuración se la puede ver en la figura 3.13.

Posteriormente se configura el RADIUS Server (*Remote Authentication Dial in User Service*). El RADIUS Server es el encargado de la autenticación, autorización y mantenimiento de cuentas de usuarios. La figura 3.14 muestra esta configuración. El *access point* también ofrece la opción avanzada de seguridad, en la que se autentica utilizando la *MAC Address*. Esta pantalla de configuración se presenta en la figura 3.15.

El *access point* da la posibilidad de configurar algunos servicios. Se va a configurar Telnet/SSH (figura 3.16), DNS (figura 3.17), HTTP (figura 3.18), VLAN (figura 3.19) y SNMP (figura 3.20).

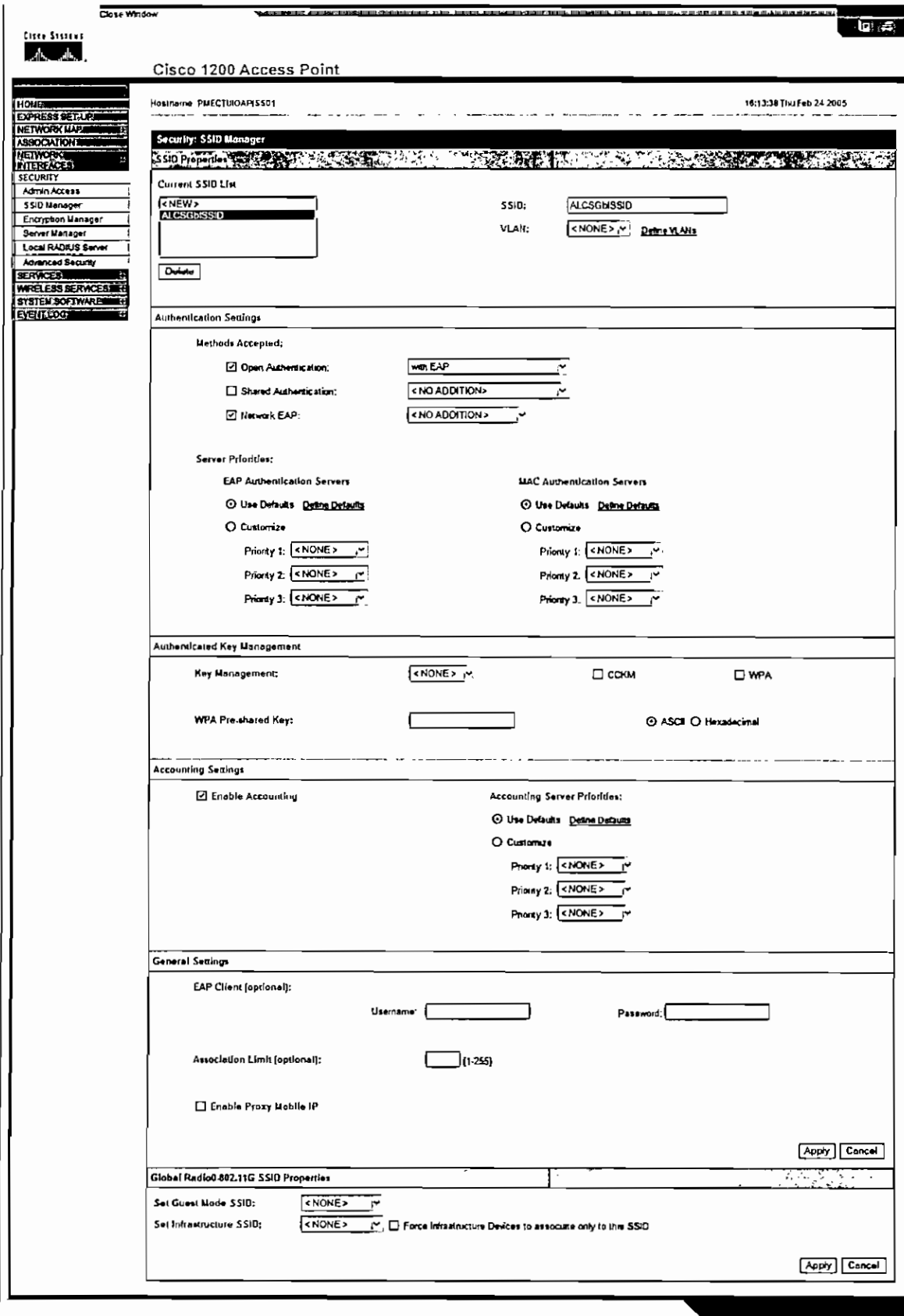


Figura 3.12 Configuración de características de seguridad en IOS Cisco 1200 Access Point.

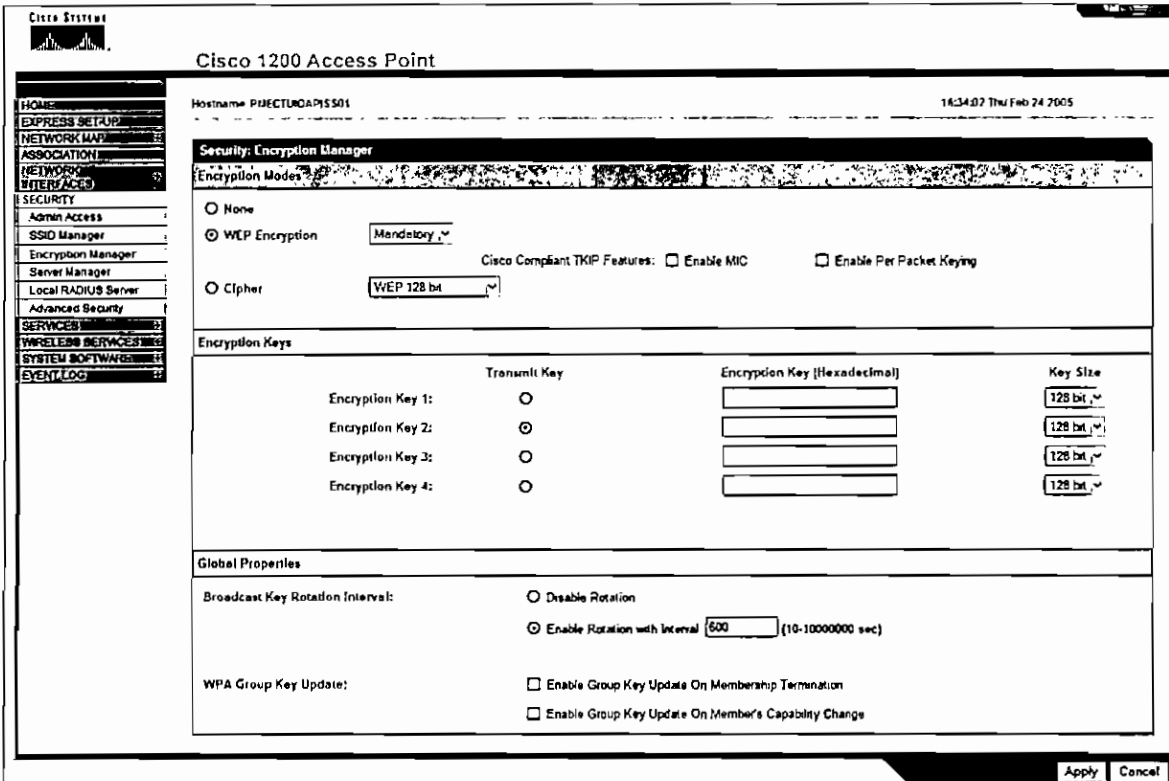


Figura 3.13 Configuración de método de encriptación en IOS Cisco 1200 Access Point.

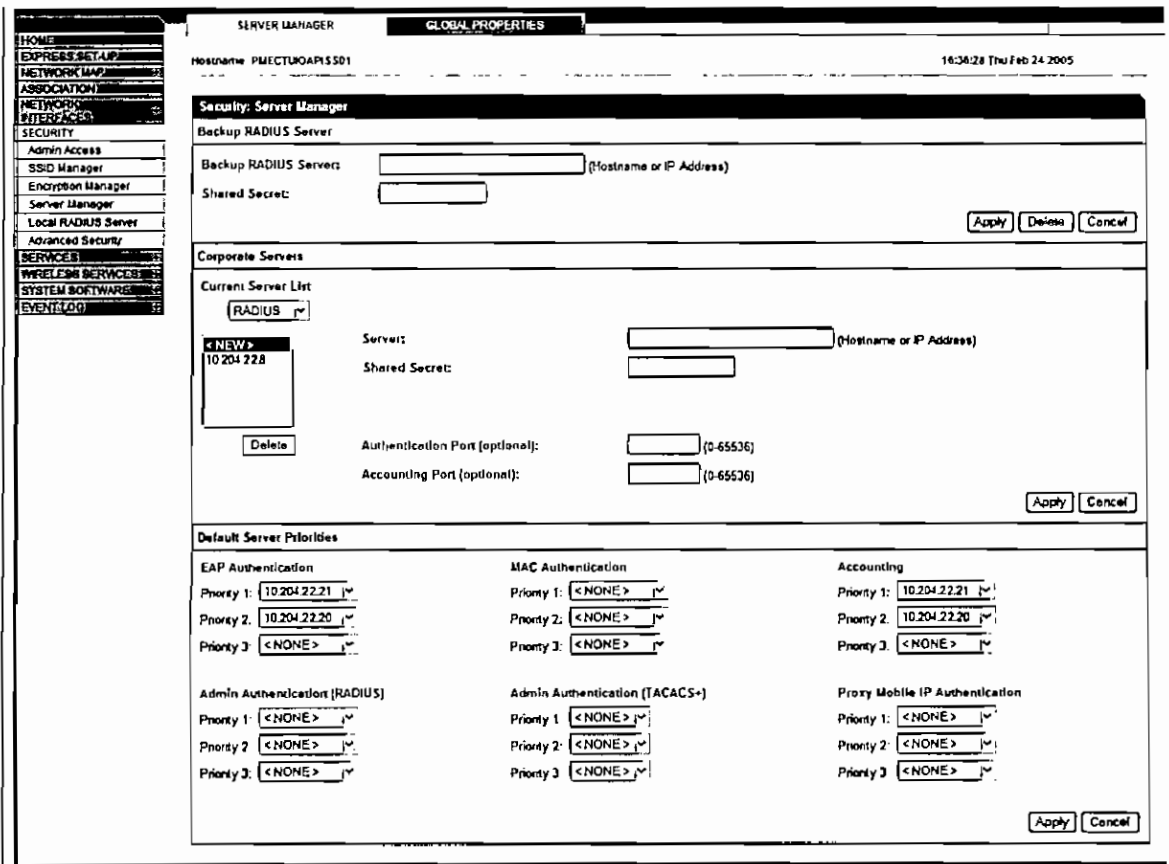


Figura 3.14 Configuración de RADIUS Server en IOS Cisco 1200 Access Point.

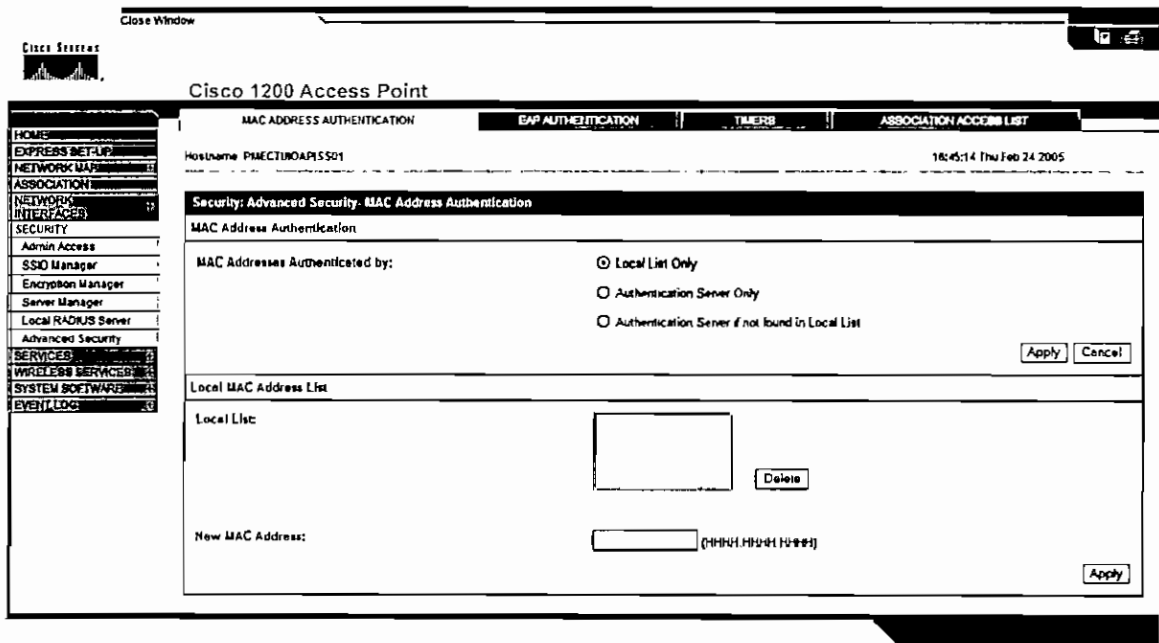


Figura 3.15 Configuración de seguridad avanzada en IOS Cisco 1200 Access Point.

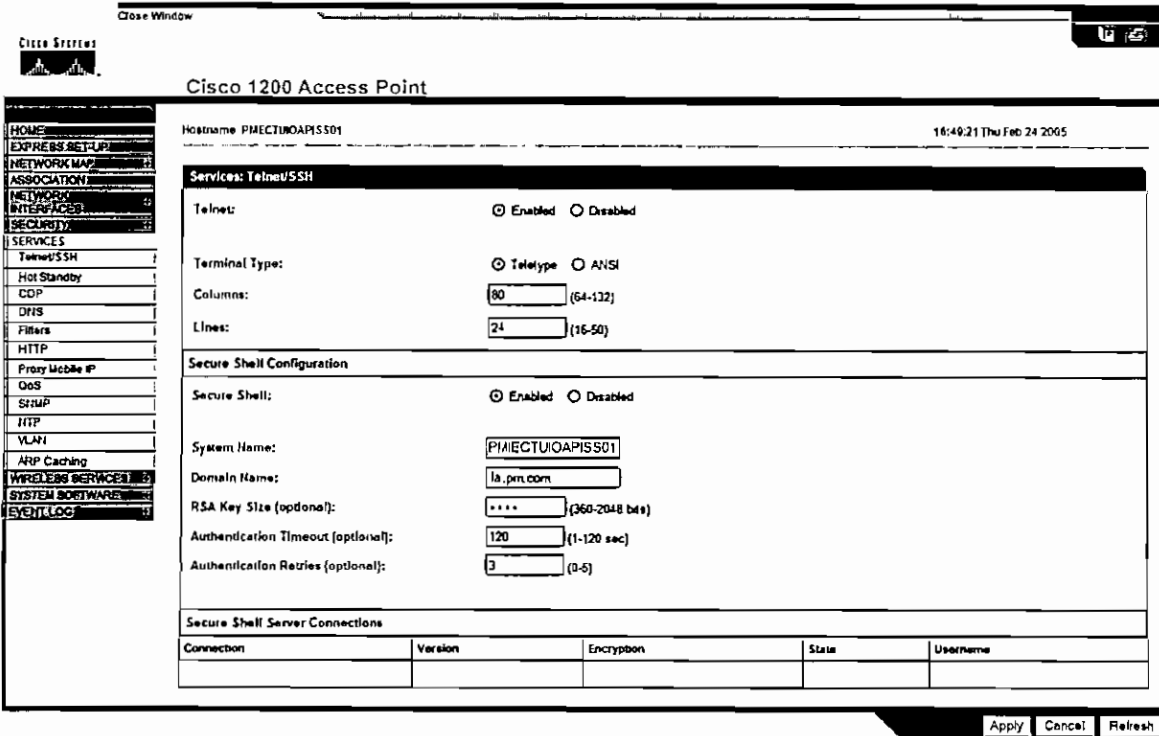


Figura 3.16 Configuración Telnet/SSH en IOS Cisco 1200 Access Point.

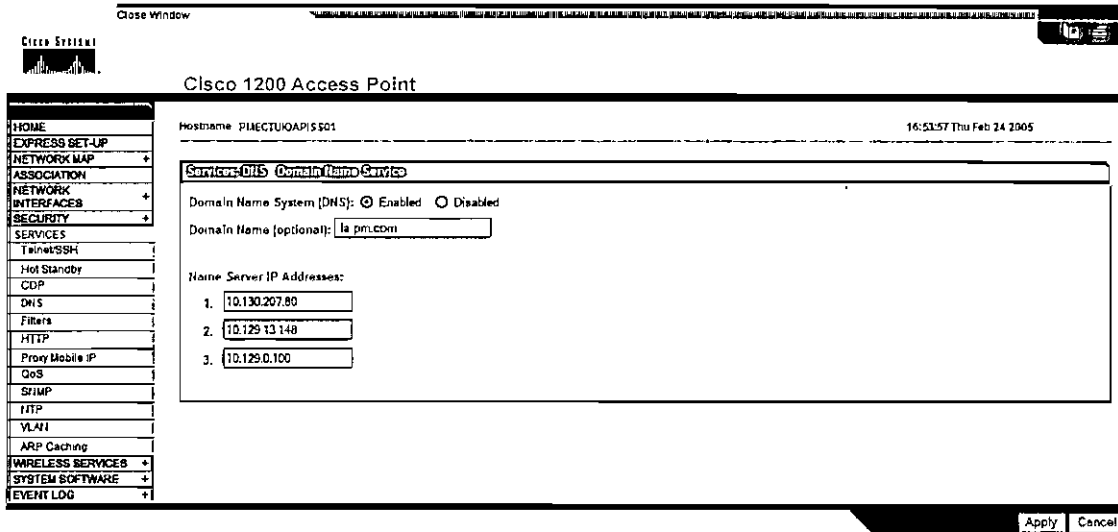


Figura 3.17 Configuración DNS en IOS Cisco 1200 Access Point.

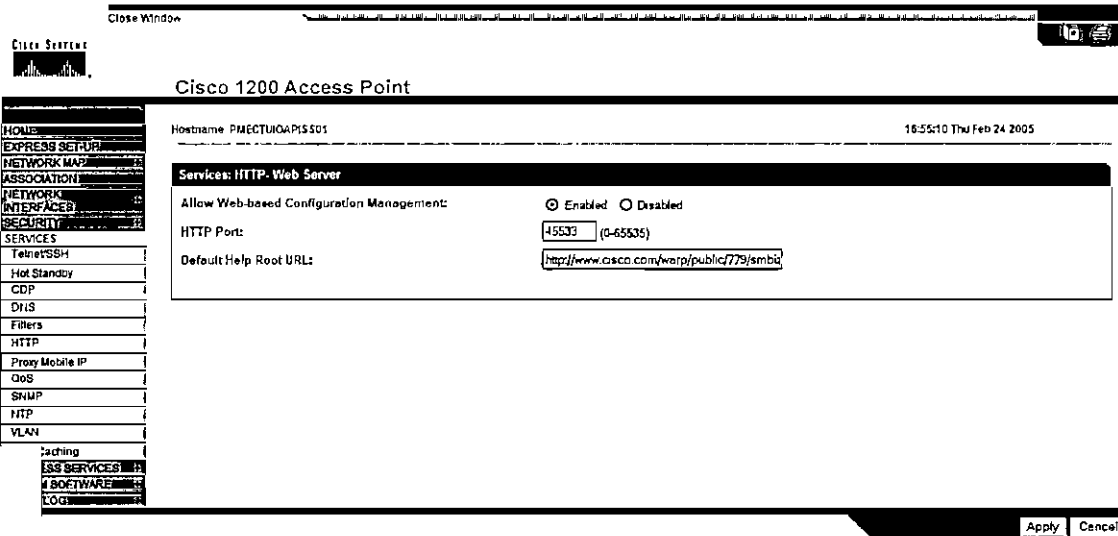


Figura 3.18 Configuración de HTTP en IOS Cisco 1200 Access Point.

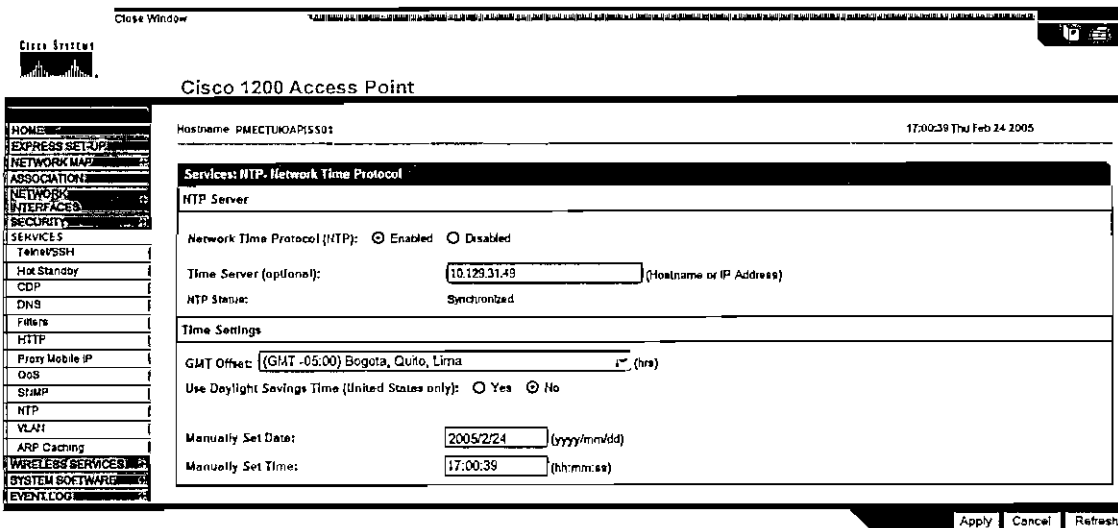


Figura 3.19 Configuración de VLANs en IOS Cisco 1200 Access Point.

Hostname: PMIECTUOAPISS01 PMIECTUOAPISS01 16:57:10 Thu Feb 24 2005

Services: SNMP - Simple Network Management Protocol

SNMP Properties

Simple Network Management Protocol (SNMP):  Enabled  Disabled

System Description: Cisco 1200 Access Point 12.2

System Name (optional): PMIECTUOAPISS01

System Location (optional):

System Contact (optional):

Apply Cancel

SNMP Request Communities

Current Community Strings	New/Edit Community Strings
<NEW>	
snmpcomm	SNMP Community: snmpcomm
	Object Identifier (optional):
	<input type="radio"/> Read-Only <input type="radio"/> Read-Write

Apply Cancel

SNMP Trap Community

SNMP Trap Destination: (hostname or IP Address)

SNMP Trap Community: snmpcomm

Enable All Trap Notifications

Enable Specific Traps

802.11 Event Traps  Encryption Key Trap

OOS Change Trap  Syslog Trap

Standby Switchover Trap  Rogue AP Trap

Apply Cancel

Figura 3.20 Configuración de SNMP en IOS Cisco 1200 Access Point.

### 3.2.2 TELÉFONOS IP INALÁMBRICOS

En este diseño se propone el uso de los teléfonos Cisco 7920 *Wireless IP Phone*. Éste es un teléfono IP inalámbrico Wi-Fi que trabaja de acuerdo al estándar 802.11b; provee servicios de seguridad, movilidad y calidad de servicio como dispositivo final en una red inalámbrica.

Este teléfono IP se configura utilizando una computadora en la que se instala *PC-based Configuration Utility*. El teléfono trae un cable USB para conectarlo a la computadora y el CD con el software para configuración antes mencionado. El teléfono aparecerá en la computadora como si fuera un dispositivo de red y se puede comprobar que el teléfono IP inalámbrico está conectado a la PC

ingresando a **Start > Control Panel > Network and Internet Connections**; esta interfaz desaparece al momento de desconectar el dispositivo.

Para la configuración de los parámetros de red, el teléfono permite la asignación de una dirección IP estática y también la asignación dinámica usando DHCP. Dentro de la configuración de *RF Network* se ingresa el SSID, el cual es necesario para la asociación al *access point*. También se ingresa la clave WEP, que para este caso será de 128 bits.

Como se va a trabajar con VLANs, al momento de realizar la configuración del teléfono se debe especificar el SSID de la VLAN a la que pertenece el teléfono. El teléfono Cisco 7920 utiliza su SSID para determinar qué VLAN debe usar.

### 3.2.3 ESQUEMA DE LA PROPUESTA DE DISEÑO

Las características que debe poseer una WLAN cuando va a soportar tanto tráfico de voz como de datos son un poco más exigentes que cuando solo transporta datos. Esto se debe a que el nivel de recepción de la señal a todo momento debe ser buena, y además como se mencionó anteriormente, debe existir superposición de las celdas de cobertura de al menos un 15 a 20%. De esta manera se garantiza que el proceso de *roaming* sea imperceptible para el usuario. Si el teléfono llega a un nivel muy bajo de potencia de recepción de señal empieza a perder paquetes, lo que ocasiona aminoramiento en la calidad de señal. Incluso se puede perder la llamada si la recepción de la señal en el teléfono es deficiente antes de encontrar otro *access point* con mejor recepción al que pueda asociarse.

Por esto es importante realizar pruebas de sitio para comprobar la distancia de alcance que tiene el *access point* en un determinado lugar. Cisco 1200 *access point* tiene un alcance entre 50 metros en áreas muy cerradas y con paredes densas, y hasta 300 metros en áreas abiertas.

TANASA se compone de varias áreas abiertas. Las oficinas son grandes áreas divididas por modulares, los cuales no generan mucha interferencia. Está conformada de varios galpones en donde se encuentran bodegas y áreas de producción, éstas no tienen paredes para separaciones internas. Sin embargo, las paredes de cada galpón están hechas en ladrillo, lo que si produce algo más de interferencia y disminuye el alcance de cobertura de señal de los *access points*.

Los *access points* Cisco 1200 poseen antenas omni direccionales, y de acuerdo a pruebas realizadas en sitio para comprobar el alcance de la señal, se determinó que posee buen alcance de la señal en una distancia de 100 metros a 130 metros a la redonda del lugar de ubicación del *access point*. Manteniendo estas distancias se tiene cobertura total con buena calidad de la señal.

Las pruebas en sitio para determinar el alcance de recepción de la señal se lo realizó utilizando un *access point* Cisco 1200 y una laptop IBM T41. El programa cliente que trae el CD de instaladores del *access point* permite verificar niveles de recepción. Estos niveles se califican de la siguiente forma: excelente, muy bueno, bueno, regular, malo.

Las pruebas de sitio consistieron en configurar un *access point* de prueba, posteriormente con la *laptop* se recorrió el área cercana al *access point*. Poco a poco se alejó el dispositivo final que en este caso era la *laptop*. El programa cliente Cisco para redes inalámbricas indicaba el nivel de recepción de la señal. Anteriormente se indicó que el área de cobertura que se tiene en la planta es de 100 a 130 m a la redonda del lugar en donde se encuentra instalado el *access point*. Estas distancias se las definió tomando en cuenta la distancia hasta que el nivel de recepción era bueno, un poco antes de pasar a nivel de recepción regular. Esto se conseguía cuando la velocidad de transmisión se encontraba entre 5.5 Mbps y 8 Mbps.

Si el dispositivo final al usuario, que en este caso va a ser el teléfono IP, tiene en todo momento y en cualquier lugar, nivel de recepción por lo menos bueno, se puede asegurar un nivel de servicio aceptable.



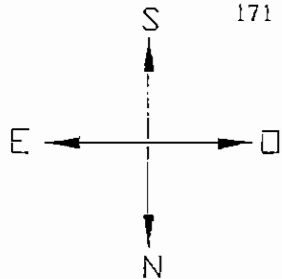
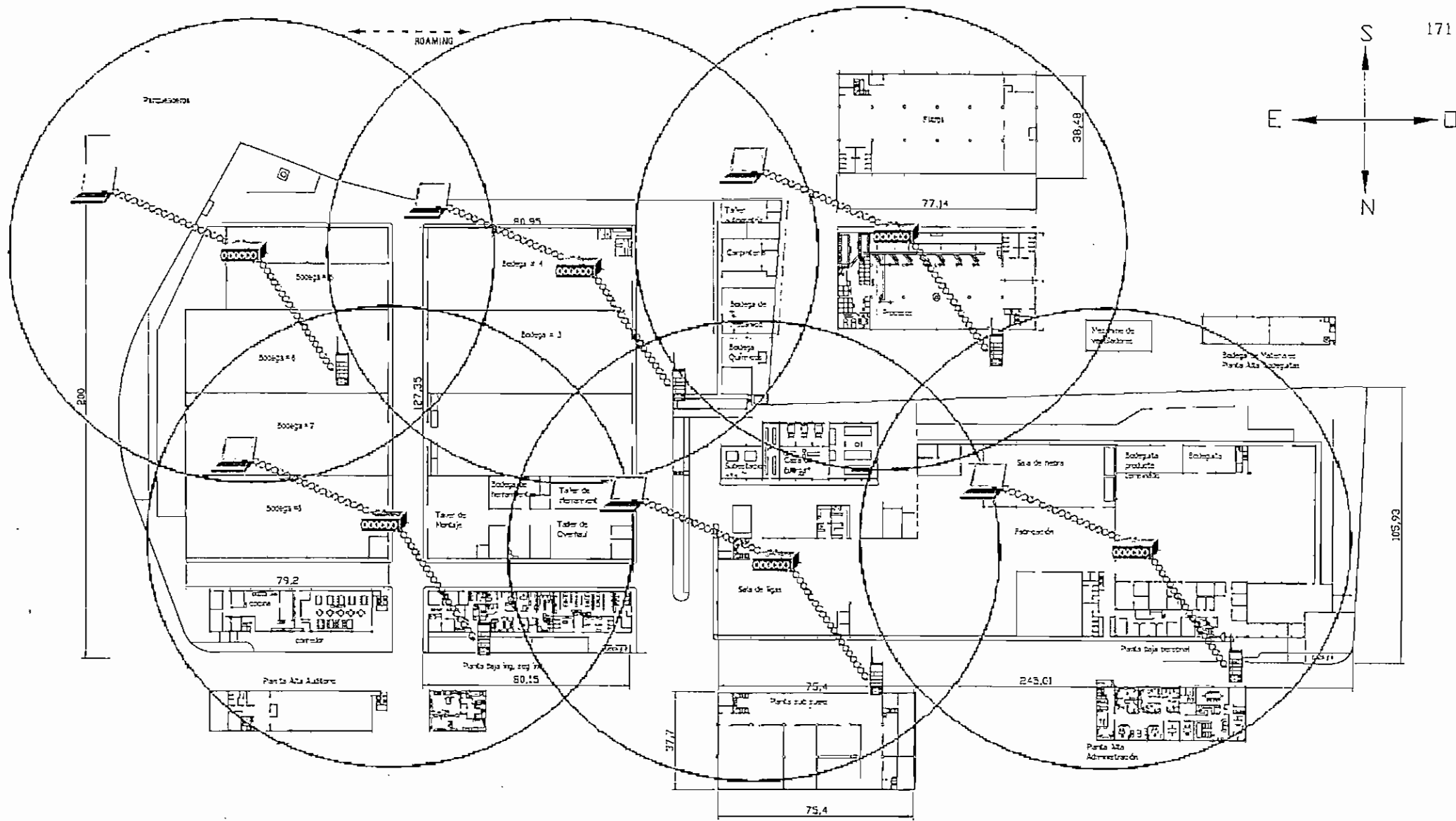
La infraestructura de la planta de producción es muy homogénea; es decir, toda la infraestructura física está conformada por galpones. Tanto las áreas de producción como las bodegas son galpones de ladrillo. Pero además existen 3 sectores que son de concreto en donde se encuentran las oficinas de ingeniería, oficinas de personal administrativo, algunas salas de reuniones y el comedor. El tener una infraestructura homogénea permite tener celdas de cobertura con áreas muy similares en todos los *access points* instalados.

En la figura 3.21 se puede observar un plano de TANASA en donde se esquematiza el área de cobertura de cada *access point*. El área de terreno de TANASA es de 1178.5 m<sup>2</sup>, dentro de los cuales funcionan oficinas, bodegas para materia prima y para producto terminado, y áreas destinadas a los procesos de fabricación. Todas estas áreas están claramente identificadas en el gráfico.

Para tener cobertura sobre toda el área de la planta de producción se van a utilizar seis *access points* Cisco 1200. Cada *access point* cubrirá un área de aproximadamente 100 metros de radio. Como se dijo anteriormente, de acuerdo a pruebas de sitio se definió que ésta es la distancia más conveniente con la que se posee una buena recepción de la señal. Además se ha tomado en cuenta recomendaciones del fabricante sobre la superposición de las celdas de cobertura.




Los canales que se utilizarán serán 1, 6 y 11. Estos canales se los va alternando para que no existan problemas de interferencia entre ellos. La disposición de los canales se la puede observar en la figura 3.21.

La banda de frecuencia que utilizan los *access points* es la banda de 2.4 GHz. La configuración del Cisco 1200 *Access Point* se la revisó anteriormente. Allí se definió que trabajará bajo el estándar 802.11g; este estándar trabaja en la banda de 2.4 GHz y además soporta dispositivos que trabajen tanto el estándar 802.11g y 802.11b. La ubicación de los *access points* será en los techos, no en las paredes. De esta manera no se encuentran al alcance de todas las personas y se evita que los manipulen personas no autorizadas.



- Canal 1
- Canal 6
- Canal 11

Figura 3.21 Esquema de la propuesta de diseño de telefonía IP Inalámbrica.

-  Aironet 1200 Series 802.11g Access Point
-  Cisco Wireless IP Phone 7920 (802.11b)
-  Laptop with 802.11a/b/g Client Adapter

En el capítulo anterior se diseñó el sistema para telefonía IP fija para TANASA. El diseño de telefonía IP inalámbrica es adicional al servicio de telefonía IP que ya se lo hizo. Por lo tanto, la telefonía IP inalámbrica se integra a los servicios que provee la telefonía IP fija. La inversión para incluir telefonía IP inalámbrica será muy baja, porque se utiliza la infraestructura de telefonía IP fija, que realmente es en donde se hace una inversión mayor.

Los servidores para procesamiento de llamadas y para mensajería unificada, Cisco *Call Manager* y *Unity* respectivamente, se diseñaron con licencias para 300 usuarios. Adicional a los 263 usuarios de telefonía IP fija, se adicionarán 20 usuarios de telefonía IP inalámbrica con lo que los servidores estarían trabajando con 283 usuarios activos. Esto permite poseer algunas licencias libres para eventuales necesidades. Sin embargo, como se ha mencionado anteriormente, la infraestructura que posee Cisco para telefonía IP inalámbrica es totalmente escalable. Esto permite agrandar la red de acuerdo a las necesidades.

En la Tabla 3.3 se indican los costos de los dispositivos necesarios para la implementación de telefonía IP. Lo único que hace falta son los *access points* y los teléfonos IP, porque lo necesario para la infraestructura de telefonía IP ya se lo obtiene con la telefonía IP fija. Es decir, la inversión en servidores, *gateways* y enlaces se la reutiliza con los dispositivos inalámbricos, optimizando el uso de recursos disponibles. Con estos valores se puede observar que adicionar telefonía IP inalámbrica al diseño de telefonía IP fija representa un costo razonable tomando en cuenta la inversión que ya se realiza en la infraestructura de telefonía IP fija. Con todas las ventajas que la telefonía IP inalámbrica ofrece se justifica la inversión.

ITEM	CANTIDAD	PRECIO UNITARIO (USD)	PRECIO TOTAL (USD)
Cisco 1200 Access Point	6	\$569,00	\$3.414,00
Cisco 7920 Wireless IP Phone	20	\$535,00	\$10.700,00
<b>TOTAL (sin impuestos)</b>			<b>\$14.114,00</b>

Tabla 3.5 Cuadro de Costos de Equipo para Telefonía IP Inalámbrica.

### 3.3 COSTO TOTAL INICIAL DEL PROYECTO

El costo total inicial del proyecto incluye el proyecto de telefonía IP para el edificio Belmonte y para la planta de producción TANASA. Además se incluye el valor de la contratación de los enlaces E1 y de los servicios de instalación y diseño del proyecto. En la Tabla 3.4 se puede observar estos valores.

ITEM	PRECIO TOTAL (USD)
Equipo para telefonía IP	\$208.968,00
Equipo para telefonía IP inalámbrica	\$14.114,00
Costo de instalación de los enlaces E1	\$4.000,00
Servicios de diseño e implementación del proyecto	\$15.000,00
<b>TOTAL (sin impuestos)</b>	<b>\$242.082,00</b>

Tabla 3.6 Costo total inicial del proyecto.

### 3.4 ANÁLISIS DE EQUIPO ESPECÍFICO DISPONIBLE EN EL MERCADO

Los equipos que se proponen en este diseño de telefonía IP inalámbrica son Cisco 1200 *Access Point* y Cisco 7920 *Wireless IP Phone*. Se ha escogido los productos Cisco por la fiabilidad que tiene este fabricante y porque el diseño de telefonía IP fija se lo realizó utilizando esta cartera de productos. Por lo tanto para que no se tenga problemas de compatibilidad en los equipos se ve que la mejor opción es continuar con esta línea de productos.

Los equipos Cisco cumplen con el estándar 802.11a/b/g para redes inalámbricas. Además poseen las características de seguridad y calidad de servicio que se recomiendan en las consideraciones de diseño. En el anexo A.2 se pueden observar los catálogos con las especificaciones de los equipos recomendados para telefonía IP inalámbrica.

### 3.4.1 CISCO AIRONET 1200 SERIES ACCESS POINT [31]

El *access point* Cisco Aironet 1200 Series es un producto que compatible con los estándares IEEE 802.11a, 802.11b y 802.11g puede trabajar tanto en la banda de 2.4 GHz o en la de 5 GHz. Este *access point* puede soportar en un ambiente combinado varios clientes utilizando cualquiera de las bandas que soporta o cualquiera de los estándares bajo los cuales trabaja. Tiene un alcance de 50 m en espacios cerrados y hasta 300 metros en ambientes abiertos. Éste es un equipo de alto desempeño, seguro y con prestaciones de calidad de servicio.

Este *access point* por sus características brinda muchas facilidades para montarlo en casi cualquier lugar, ambiente y orientación ya que sus antenas son omni direccionales. Puede trabajar bajo un amplio rango de temperatura. Posee una carcasa de aluminio que lo hace más resistente para su colocación en fábricas y plantas de producción, pero manteniendo una elegante línea estética. El sistema de montaje está diseñado para colocar el *access point* en paredes o en techos. El método de alimentación de energía puede ser *inline power* a través de la Ethernet, si la red tiene esta capacidad, y alimentación local. Se puede observar a este *access point* en la figura 3.22.

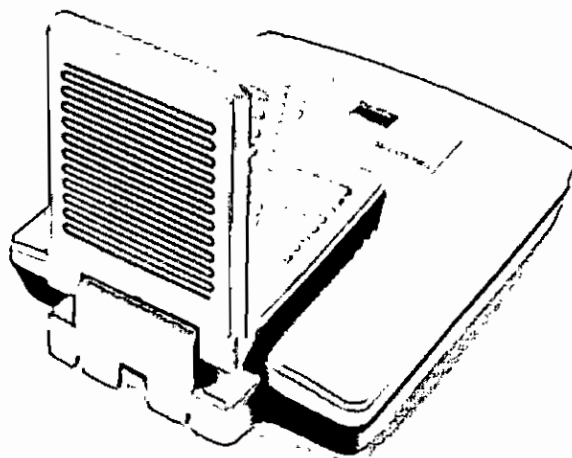


Figura 3.22 Cisco Aironet 1200 Access Point [31].

Cisco 1200 *access point* soporta VLANs, QoS y *proxy mobile* IP. Se pueden configurar hasta 16 VLANs, cada una con sus propias políticas de seguridad y servicios. Por ejemplo, se pueden usar VLANs para segregar diferente tipo de tráfico, lo que permite aplicar políticas de priorización para cada tipo de tráfico, o separar de acuerdo a usuarios, discriminando usuarios que tengan acceso total a la red de los que tienen acceso restringido.

Soporta el estándar 802.1p para QoS, lo que permite proveer priorización de tráfico para paquetes que viajan desde y hacia el *access point*. El tráfico que es sensible al retraso, como voz y vídeo, puede ser priorizado sobre el tráfico de datos lo que brindará una óptima utilización de la red. Además permite actualizaciones de estándares de QoS que soporten esquemas de priorización de voz para teléfonos IP móviles que trabajen bajo el estándar 802.11b.

*Proxy mobile* IP permite que los usuarios mantengan similar conectividad de red en *roaming*. Las características de *proxy mobile* IP permiten crear un túnel entre los *routers* entre la red remota y otra red que puede ser una red en la casa del usuario.

Entre las características de seguridad que posee Cisco 1200 *access point* se encuentra el protocolo EAP (*Extensible Authentication Protocol*) que es un método de autenticación basado en la autenticación del usuario. LEAP es la versión de EAP propietaria de Cisco que tiene este *access point*. También soporta WPA (*Wi-Fi Protected Access*) que es la especificación de *Wi-Fi Alliance* para seguridad en LANs inalámbricas.

### 3.4.2 CISCO WIRELESS IP PHONE 7920 [32]

El Cisco *Wireless IP Phone* 7920 es un teléfono diseñado para trabajar en redes WLAN 802.11b. Es un teléfono de fácil uso, que ofrece todos los servicios de un teléfono IP fijo. Provee grandes prestaciones en comunicaciones de voz al ser utilizado junto con la arquitectura de telefonía IP y de redes inalámbricas que

Cisco ofrece. Este teléfono puede trabajar en redes inalámbricas formadas por *access points Wi-Fi Cisco Aironet* de las series 1200, 1100, 350 y 340.

Entre sus características principales se encuentra una pantalla *pixel-based* en la que se puede acceder a detalles de las llamadas, como son número marcado o desde el que llaman, tiempo de llamada, etc. Posee dos teclas tipo *soft* dinámicas con las que el usuario puede escoger opciones de menú, y una tecla de navegación para facilidad de movimiento entre esas opciones. Entre las opciones que se puede encontrar están las de recuperación de mensajes de voz, llamadas perdidas, llamadas entrantes y salientes, tipos de tonos y volumen y preferencias de usuario. En la figura 3.23 se puede ver a este teléfono.

Entre las características de llamadas el teléfono Cisco Wireless IP Phone 7920 están sus capacidades de servicio muy útiles y fáciles de usar. Entre éstas se puede encontrar el despliegue en pantalla de los números marcados e identificador de llamadas, llamada en espera, reenvío de llamadas, transferencia de llamadas, conferencia tripartita y captura de llamadas. Otras características son los botones directos para activar modo de vibración o de timbre, bloqueo del teclado y acceso a mensajes de voz. Además en pantalla se despliega fecha y hora, icono de indicación si se encuentra en modo timbre o vibración e indicador de nivel de batería y RF.



Figura 3.23 Cisco Wireless IP Phone 7920 [32].

Dentro de las características inalámbricas se puede destacar que trabaja bajo el estándar 802.11b, utilizando velocidades de 1, 2, 5.5 y 11 Mbps. El rango de frecuencia con el que trabaja es de 2.4 – 2.497 GHz. El nivel de alcance va de 15 m en ambientes totalmente cerrados a 300 m en ambientes abiertos.

Para configuración de red soporta configuración para VLANs. La asignación de dirección IP puede ser utilizando DHCP o asignando una dirección IP fija. Compresión de audio G.711 (64 Kbps), y G.729 (8 Kbps).



## CAPÍTULO 4

### CONCLUSIONES Y RECOMENDACIONES

#### 4.1 CONCLUSIONES

- Las capacidades que posee la telefonía por conmutación de circuitos están destinadas exclusivamente a la transmisión de voz, no de datos. Sin embargo, las redes de conmutación de paquetes sí tienen la capacidad de ampliar sus tipos de servicio. Por esta razón es que la telefonía tradicional no tiene mayor capacidad de crecimiento y el futuro de las comunicaciones de voz, vídeo y datos se encuentra en las redes de conmutación de paquetes, en la que si pueden converger todos estos servicios.
- Si bien es cierto, voz sobre IP en sus inicios no era competencia para la telefonía tradicional porque no ofrecía la misma calidad de voz, sin embargo, ahora se tienen verdaderos sistemas de telefonía IP en el mercado. Estos sistemas cuando se encuentran bien dimensionados y se aplican políticas de calidad de servicio y seguridad han demostrado ser mucho más eficientes que los sistemas de telefonía tradicionales. Esto es debido a que al digitalizar la señal de voz y paquetizarla, se puede hacer mucho más con todo a lo que servicios se refiere.
- Durante mucho tiempo se ha visto que la principal ventaja que telefonía IP brinda es su bajo costo. Pero se debe tomar en cuenta que ésta es solo una de las ventajas, porque la inversión es grande, pero los beneficios en sentido económico se los verá algunos meses después de la implementación. La verdadera ventaja es la cantidad de servicios que presta al usuario, creando un sistema unificado en la que el usuario no tiene que preocuparse por la forma de mantenerse siempre en contacto con su trabajo diario. La convergencia de voz y datos es un sistema que

permite agilizar procesos y actuar con eficiencia sin importar el lugar en donde se encuentre el usuario,

- En el caso del grupo ITABSA, las centrales telefónicas digitales que poseen actualmente son centrales que ya tienen muchos años de vida, su capacidad es limitada y además son de marcas tan variadas que inclusive generan problemas de conectividad. Estas centrales no tienen posibilidad de crecer al ritmo que la empresa lo hace por lo que es necesario el cambio del sistema de telefonía. La mejor opción es unirse al ritmo que el mundo exige y optar por un sistema tecnológicamente estable y competente como lo es la telefonía IP.
- Siempre se debe tener en cuenta la aplicación de políticas de calidad de servicio, si estas políticas no están bien desarrolladas se tendrá un servicio pobre que no refleja al máximo las capacidades que la telefonía IP ofrece.
- Si se cumplen los requerimientos básicos descritos en este documento, el grupo ITABSA logrará obtener el mayor provecho de la infraestructura de datos que posee actualmente. Implementar el servicio de voz sobre la infraestructura de datos es un reto que traerá muchas satisfacciones a la empresa.
- En este proyecto de titulación se analizan las características generales que un sistema de telefonía IP debe tener. Así mismo se analizan las características particulares de configuración para el caso específico del grupo ITABSA, tomando las mejores opciones de la variedad existente para llegar a la convergencia de redes de voz y datos.
- El diseño que se presenta en este proyecto de titulación está destinado para el grupo ITABSA, pero posee las características básicas que cualquier sistema de telefonía IP exige. Por esta razón, este diseño puede ser extendido para ampliarse al resto de la red del grupo ITABSA, así como guía para cualquier otra organización que opte por este sistema.

- Cisco es una marca líder en el mercado de redes, por la fiabilidad que ha demostrado durante muchos años. La red actual del grupo ITABSA es una red basada prácticamente sólo en productos Cisco. Esto se debe a lineamientos internacionales que tiene Philip Morris International. Por estos motivos se escogió la marca Cisco para el diseño de telefonía IP. Además al utilizar equipo Cisco se evitará problemas de compatibilidad entre los equipos y la red será estable.
- Las ventajas que las redes inalámbricas ofrecen son muchas. Una de éstas es la posibilidad de transmitir voz sobre esta red. Cisco posee el equipo necesario para proveer redes inalámbricas confiables y con total prestación de servicios. Incluir telefonía IP inalámbrica dentro del grupo ITABSA es un logro que traerá muchas facilidades a los usuarios que la posean y el rendimiento de personal que necesita movilidad será mayor.
- La tendencia mundial a la unificación de redes demuestra que nadie puede quedarse atrás si pretende seguir a la vanguardia de cualquier negocio. La tecnología y las comunicaciones son un elemento clave en cualquier empresa. El proveer mejores servicios de comunicaciones aumenta la eficiencia de los trabajadores además que el proporcionar nuevas herramientas que optimicen la labor diaria crea un mejor ambiente de trabajo.
- El equipo de telefonía usado actualmente por el grupo ITABSA ya no tiene posibilidades de crecimiento. Además, las centrales telefónicas son antiguas y todas de diferentes modelos e incluso de diferentes fabricantes. Esto genera la existencia de algunos problemas de compatibilidad entre el equipo de telefonía que actualmente poseen. El costo total de la inversión se justifica al tomar en cuenta que se consolidarán todos los servicios de voz y datos sobre una misma red, lo que reduce costos de administración y operación. Las centrales telefónicas que poseen actualmente ya necesitan ser cambiadas, y pensar en cambiar por tecnología de telefonía IP es la mejor solución.

## 4.2 RECOMENDACIONES

- La migración hacia la convergencia de voz y datos debe ser un proceso paulatino, que debe seguir un orden cronológico para no afectar el desempeño de la red de datos sobre la que se va a implementar servicios de voz.
- Se recomienda realizar pruebas de conectividad y funcionamiento con los equipos ya configurados. Estas pruebas se las debe hacer antes de poner en producción los equipos. Allí se simulará el funcionamiento que tendrá el sistema cuando esté en producción. Esta etapa es muy importante porque permitirá detectar errores que podrán ser corregidos previamente y así no afectar todo el sistema de comunicaciones.
- Es necesario realizar charlas de capacitación y de información al personal de la empresa antes de implementar nuevas tecnologías. Esto se recomienda porque existe mucha gente que le teme al cambio, pero si están instruidos sobre las diferencias y ventajas que se aproximan al migrar de una tecnología a otra esos temores se desvanecen. Además al proporcionar capacitación los usuarios podrán hacer uso de todas las ventajas que la telefonía IP les ofrece.
- La propuesta que se presenta abarca las características que debe tener el sistema de telefonía IP para su correcto funcionamiento, por lo tanto se pide tomar en cuenta todas las consideraciones de diseño que en este documento se incluyen. Esto asegurará un sistema robusto, seguro, óptimo y estable que aportará al crecimiento del grupo ITABSA y del personal que la conforman.
- Se recomienda realizar pruebas de cobertura de la red inalámbrica una vez que ésta se ha instalado. Estas pruebas se las realiza porque puede existir alguna fuente de interferencia que afecte el correcto desempeño de la red

inalámbrica y por lo tanto el desempeño del sistema de telefonía IP inalámbrica. A pesar de que se ha realizado pruebas de alcance de la señal para realizar el dimensionamiento de la red inalámbrica, el comportamiento en conjunto de la red puede variar un poco.

- El diseño que se presenta en este proyecto de titulación incluye las oficinas y la planta de producción del grupo corporativo en la ciudad de Quito, se recomienda extender este diseño como una segunda etapa del proyecto al resto de oficinas en el país.

---

## REFERENCIAS

- [1] **Davidson, J. y Peters, J.** "Fundamentos de Voz sobre IP", Pearson Educación, S.A., Madrid, 2001.
- [2] <http://www.hermesgroup.com/whitepapers/VoIP/voip.htm>.
- [3] [http://www.pt.com/tutorials/iptelephony/tutorial\\_ss7\\_ip\\_interworking.pdf](http://www.pt.com/tutorials/iptelephony/tutorial_ss7_ip_interworking.pdf).
- [4] **Rodríguez, A., Gatrell, J., Karas, J. y Peschke, R.** "TCP/IP Tutorial and Technical overview". IBM Corporation, International Technical Support Organization, USA, 2001.
- [5] **Huidrobo, J. y Roldán, D.** "Integración de voz y datos", Mc Graw Hill, España, 2003.
- [6] <http://www.iplan.com.ar>.
- [7] <http://www.radcom-inc.com>.
- [8] <http://www.cisco.com>.
- [9] **Keagy, S.** "Integración de Redes de Voz y Datos". Pearson Educación, S. A., Madrid, 2001.
- [10] **Stallings, W.** "Comunicaciones y Redes de Computadores". Pearson Educación, S. A., Madrid, 2000.
- [11] <http://www.c7.com>.
- [12] **Brown, K.** "IP Telephony unveiled", Cisco Press, USA, 2004.

- 
- [13] **Broadcom Corporation.** "The New Mainstream Wireless LAN Standard", Broadcom Corporation, USA, 2003.
- [14] **Nichols, R. y Lekkas, P.** "Seguridad para comunicaciones inalámbricas", McGraw-Hill, España, 2003.
- [15] Intranet Philip Morris International – P MEC (Philip Morris Ecuador).
- [16] <http://www.elmundo.es/navegante/2004/05/14/entrevistas/1084522811.html>
- [17] **Ferreira, A., Pepe, M., Lopez, F. y Guani, J.** "VoIP en Redes Corporativas". <http://cita2003.fing.edu.uy/articulosvf/53.pdf>.
- [18] Cisco Call Manager version 4.1 datasheet. <http://www.cisco.com>.
- [19] Cisco Unity Unified Messaging datasheet. <http://www.cisco.com>.
- [20] Cisco 3800 Series Routers datasheet. <http://www.cisco.com>.
- [21] Cisco IP Phone 7912G datasheet. <http://www.cisco.com>.
- [22] Cisco IP Phone 7940G datasheet. <http://www.cisco.com>.
- [23] Cisco IP Phone 7960G datasheet. <http://www.cisco.com>.
- [24] Cisco IP Conference Station 7936 datasheet. <http://www.cisco.com>.
- [25] Cisco IP Communicator datasheet. <http://www.cisco.com>.
- [26] Cisco ATA 186 datasheet. <http://www.cisco.com>.
- [27] <http://enterprise.usa.siemens.com>.

- 
- [28] **Padin, N.** "Implementación de IP Telephony". <http://www.cisco.com>.
- [29] Cisco 7920 Wireless IP Phone Design and Deployment Guide. <http://www.cisco.com>.
- [30] Cisco SAFE: Wireless LAN Security in Depth. <http://www.cisco.com>.
- [31] Cisco Aironet 1200 Series Access Point datasheet. <http://www.cisco.com>.
- [32] Cisco Wireless IP Phone 7920 datasheet. <http://www.cisco.com>.
- [33] [http://eia.udg.es/~atm/tcp-ip/tema\\_4\\_6\\_2.htm](http://eia.udg.es/~atm/tcp-ip/tema_4_6_2.htm).





## CISCO CALLMANAGER VERSION 4.1

Cisco<sup>®</sup> IP Communications is a comprehensive system of powerful, enterprise-class solutions, including IP telephony, unified communications, IP video and audio conferencing, and customer contact. It helps organizations realize business gains by improving operational efficiencies, increasing organizational productivity, and enhancing customer satisfaction. Cisco CallManager is the software-based call-processing component of the Cisco enterprise IP telephony solution; it is enabled by Cisco AVVID (Architecture for Voice, Video and Integrated Data).

Cisco CallManager software extends enterprise telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, voice over IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems interact with the IP telephony solution through Cisco CallManager open telephony application programming interfaces (APIs). Cisco CallManager is installed on Cisco 7800 Series media convergence servers (MCSs) and selected third-party servers. Cisco CallManager software is shipped with a suite of integrated voice applications and utilities, including the Cisco CallManager Attendant Console—a software-only manual attendant console; a software-only ad-hoc conferencing application; the Bulk Administration Tool (BAT); the CDR Analysis and Reporting (CAR) tool; the Real-Time Monitoring Tool (RTMT); a simple, low-density Cisco CallManager Auto Attendant (CM-AA); the Tool for Auto-Registered Phone Support (TAPS); and the IP Manager Assistant (IPMA) application.

### FEATURES AND BENEFITS

Cisco CallManager Version 4.1 provides a scalable, distributable, and highly available enterprise IP telephony call-processing solution. Multiple Cisco CallManager servers are clustered and managed as a single entity. Clustering multiple call-processing servers on an IP network is a unique capability in the industry, and highlights the leading architecture provided by Cisco AVVID. Cisco CallManager clustering yields scalability of from 1 to 30,000 IP phones per cluster, load balancing, and call-processing service redundancy. By interlinking multiple clusters, system capacity can be increased up to one million users in a 100+ site system. Clustering aggregates the power of multiple, distributed Cisco CallManagers, enhancing the scalability and accessibility of the servers to phones, gateways, and applications. Triple call-processing server redundancy improves overall system availability.

The benefit of this distributed architecture is improved system availability, load balancing, and scalability. Call Admission Control (CAC) helps ensure that voice quality of service (QoS) is maintained across constricted WAN links, and automatically diverts calls to alternate public switched telephone network (PSTN) routes when WAN bandwidth is not available. A Web interface to the configuration database enables remote device and system configuration. HTML-based online help is available for users and administrators.

The enhancements provided by Cisco CallManager Version 4.1 offer improved security, interoperability, capability, supportability, and productivity as well enhancements to video telephony introduced in Cisco CallManager 4.0.

Cisco CallManager 4.1 has many security features that give Cisco CallManager servers and IP phones the ability to verify identity of the devices or servers that they communicate with, ensure the integrity of data they are receiving, and provide privacy of communications via encryption. The devices that can participate in secure communications now includes the Cisco IP Phone 7940G, IP Phone 7960G, IP Phone 7970G, and Media Gateway Control Protocol (MGCP) gateways. Secure administration and troubleshooting is now capable with CallManager 4.1 using HTTPS.

Improvements in the CallManager Q.SIG signaling interface expands the range of functions with which Cisco CallManager can connect to other Q.SIG compatible systems. Features like path replacement and call completion allow Cisco CallManager to integrate with other Q.SIG compatible systems closer than ever before. H.323 Annex M.1 support now gives users improved feature transparency between CallManager clusters.

Enhancements to the CallManager APIs (AXL, JTAPI, TSP) provide customers and 3<sup>rd</sup> party vendors increased ability to develop improved applications that can be integrated with CallManager and IP Phones.

Other key features provided by Cisco CallManager 4.1 include call coverage, time-of-day routing and restrictions, forced authorization codes (FAC) and client matter codes (CMC) and enhancements for Video Telephony that was provided in Cisco CallManager 4.0.

New administration features such as Cisco Unity User Integration allow a CallManager system administrator to easily configure a Cisco Unity voice mail box while configuring an IP phone for that user.

## SPECIFICATIONS

### Platforms

- Cisco 7815, 7825, 7835, and 7845 MCSs
- Selected third-party servers; for details, visit: <http://www.cisco.com/go/swonly>

### Bundled Software

- Cisco CallManager Version 4.1—Call-processing and call-control application.
- Cisco CallManager Version 4.1 configuration database—Contains system and device configuration information, including dial plan.
- Cisco CallManager administration software.
- Auto attendant—Bundled with Cisco CallManager via the Extended Services CD.
- Cisco CallManager CDR Analysis and Reporting Tool (CAR)—Provides reports for calls based on call detail records (CDRs). Reports that are provided include calls on a user basis, calls through gateways, simplified call quality, and a CDR search mechanism. In addition, CAR provides limited database administration; for example, deleting records based on database size.
- Cisco CallManager Bulk Administration Tool (BAT)—Allows the administrator to perform bulk add, delete, and update operations for devices and users.
- Cisco CallManager Attendant Console—Allows a receptionist to answer and transfer/dispatch calls within an organization. The attendant can install the attendant console, which is a client-server application, on a PC that runs Windows 98, ME, NT 4.0 (Service Pack 4 or greater), 2000, or XP. The attendant console connects to the Cisco Telephony Call Dispatcher (TCD) server for login services, line state, and directory services. Multiple attendant consoles can connect to a single Cisco TCD server. In Cisco CallManager Version 4.1, Attendant Console now supports accessibility enhancements for sight-impaired individuals.
- Cisco CallManager Real-Time Monitoring Tool (RTMT)—A client tool that monitors real-time behavior of the components in a Cisco CallManager cluster. RTMT uses HTTP and TCP to monitor device status, system performance, device discovery, and computer telephony integration (CTI) applications. It connects directly to devices by using HTTP for troubleshooting system problems.
- Cisco CallManager Trace Collection Tool—Collects traces for a Cisco CallManager cluster into a single zip file. The collection includes all traces for Cisco CallManager and logs such as Event-Viewer (application, system, and security), Dr. Watson log, Cisco Update. Prng logs, RIS DC logs, and SQL and IIS logs.
- Cisco Conference Bridge—Provides software conference bridge resources that can be used by Cisco CallManager.
- Cisco Customer Directory Configuration Plugin—Guides the system administrator through the configuration process for integrating Cisco CallManager with Microsoft Active Directory and Netscape Directory Server.
- Cisco IP Phone Address Book Synchronizer—Allows users to synchronize Microsoft Outlook or Outlook Express address books with Cisco Personal Address Book. The synchronizer provides two-way synchronization between the Microsoft and Cisco products. After the user installs and configures Cisco Personal Address Book, users can access this feature from the Cisco IP Phone Configuration Website.

- Cisco IP Telephony Locale Installer—Provides user and network locales for Cisco CallManager, adding support for languages other than English. Locales allow users to view translated text, receive country-specific phone tones, and receive TAPS prompts in a chosen language when working with supported interfaces. Install the Cisco IP Telephony Locale Installer on every server in the cluster. Click the icon to download one or more locale installers from the Web (you must have an Internet connection and a Cisco.com user account and password to download the executable).
- Cisco JTAPI—This plug-in is installed on all computers that host applications that interact with Cisco CallManager via JTAPI. JTAPI provides the standard programming interface for telephony applications written in the Java programming language. JTAPI reference documentation and sample code are included. Cisco CallManager Version 4.1 adds support for new features as well as the ability to disable device validation, which would allow applications to monitor or control a large amount of devices without requiring the devices to be specified in those applications' controlled device lists. JTAPI Device State Server is new in Cisco CallManager Version 4.1, as is notification of status (busy, idle, etc.) of a CTI device without having to monitor individual lines.
- Cisco Telephony Service Provider—Contains the Cisco TAPI service provider (TSP) and the Cisco Wave Drivers. Install the application on the Cisco CallManager server or on any other computer that is running a Microsoft Windows operating system that interacts with the Cisco CallManager server via TCP/IP (TAPI runs on the Microsoft Windows operating system). The Cisco TAPI Developer's Guide describes the TAPI interfaces that are currently supported. Install the Cisco TSP and the Cisco Wave Drivers to allow TAPI applications to make and receive calls on the Cisco IP Telephony Solution.
- Cisco TAPS—Loads a preconfigured phone setting on a phone.
- Cisco Dialed Number Analyzer—Serviceability tool that analyzes the dialing plan for specific numbers.
- Cisco IP Manager Assistant (IPMA)—Provides "boss"/administration features along with administration Web pages for improved call handling.

#### SYSTEM CAPABILITIES SUMMARY

- Alternate automatic routing (AAR)
- Attenuation and gain adjustment per device (phone and gateway)
- Automated bandwidth selection
- Auto route selection (ARS)
- AXL Simple Object Access Protocol (SOAP) API with performance and real-time information
- Basic Rate Interface (BRI) endpoint support; registers BRI endpoints as SCCP devices\*
- CAC—intercluster and intracluster
- Call coverage\*
  - Forwarding based on internal/external calls\*
  - Forwarding out of a coverage path\*
  - Timer for maximum time in coverage path\*
  - Time of day\*
- Call display restrictions\*
- Coder-decoder (codec) support for automated bandwidth selection
  - G.711 mu-law, a-law
  - G.723.1
  - G.729A/B
  - GSM-EFR, FR
  - Wideband audio—Proprietary 16-bit resolution, 16-kHz sampled audio

- Digit analysis and call treatment (digit string insertion, deletion, stripping, dial access codes, digit string translation)
- Distributed call processing
  - Deployment of devices and applications across an IP network
  - "Clusters" of Cisco CallManager servers for scalability, redundancy, and load balancing
  - Maximum of 7500 IP phones per Cisco CallManager server (configuration-dependent)
  - Maximum of 100,000 busy-hour call completions (BHCCs) per Cisco CallManager server (configuration-dependent)
  - Eight Cisco CallManager servers per cluster
  - Maximum of 250,000 BHCCs per Cisco CallManager cluster (configuration-dependent)
  - Maximum of 30,000 IP phones per cluster (configuration-dependent)
  - Intercluster scalability to more than 100 sites or clusters through H.323 gatekeeper
  - Intracluster feature transparency
  - Intracluster management transparency
- Fax over IP—G.711 pass-through and Cisco Fax Relay
- Forced authorization codes/client matter codes (account codes) \*
- H.323 interface to selected devices
- H.323 FastStart (inbound and \*outbound)
- Hotline and private line automated ringdown (PLAR)
- Hunt groups—broadcast, circular, longest idle, and linear
- \* Interface to H.323 gatekeeper for scalability, CAC, and redundancy
- Language support for client user interfaces (languages specified separately)
- Multilevel precedence and pre-emption (MLPP)—\*Enhancements made in Cisco CallManager Version 4.1
- \* Multilocation—Dial-plan partition
- Multiple ISDN protocol support
- Multiple remote Cisco CallManager platform administration and debug utilities
  - Prepackaged alerts, monitor views, and historical reports with RTMT
  - Real-time and historical application performance monitoring through operating system tools and Simple Network Management Protocol (SNMP)
  - Monitored data collection service
  - Remote terminal service for off-net system monitoring and alerting
  - Real-time event monitoring and presentation to common syslog
  - Trace setting and collection utility
  - Browse to onboard device statistics
  - Clusterwide trace setting tool
  - Trace collection tool

- Multisite (cross-WAN) capability with intersite CAC
- Dial-plan partitioning
- Off-premises extension (OPX)
- Outbound call blocking
- Out-of-band dual tone multifrequency (DTMF) signaling over IP
- PSTN failover on route nonavailability--AAR
- Q.SIG (International Organization for Standardization [ISO])
  - Alerting name specified in ISO 13868 as part of the SS-CONP feature, \*
  - Basic call
  - ID services
  - General functional procedures
  - Call back—ISO/IEC 13870: 2nd Ed, 2001-07 (CCBS, CCNR) \*
  - Call diversion (SS-CFB [busy], SS-CFNR [no answer], SS-CFU [unconditional]); service ISO/IEC 13872 and ISO/IEC 13873, first edition 1995
    - Call diversion by forward switching
    - Call diversion by reroute \*
  - Call transfer by join
  - H.323 Annex M.1 (Q.SIG over H.323) --ITU recommendation for Annex M.1 \*
  - Identification restriction (Calling Name Identification Restriction [CNIR], Connected Line Identification Restriction [COLR]), Connected Name Identification Restriction [CONR])
  - Loop prevention, diversion counter and reason, loop detection, diverted to number, diverting number, original called name and number, original diversion reason, redirecting name
  - Message waiting indicator (MWI)
  - Path replacement ISO/IEC 13863; 2nd Ed, 1998 and ISO/IEC 13974; 2nd Ed, 1999. \*
- Redundancy and automated failover on call-processing failure
  - Call preservation on call-processing failure
- Station to station
- Station through trunk (Media Gateway Control Protocol [MGCP] gateways)
  - JTAPI and TAPI applications enabled with automated failover and automatic update
  - Triple Cisco CallManager redundancy per device (phones, gateway, applications) with automated failover and recovery
  - Trunk groups
  - MGCP BRI support (ETSI BRI basic-nc3 user-side only) \*
- Security
  - Configurable operation modes—Nonsecure or secure

- Device authentication—Embedded X.509v3 certificate in new model phones; certificate authority proxy function (CAPF) used to install locally significant certificate in phones
  - Data integrity—TLS cipher “NULL-SHA” supported. Messages are appended with SHA1 hash of the message to ensure that the message is not altered on the wire and can be trusted.
  - Secure HTTP (HTTPS) support for the following applications: Cisco CallManager Admin, Cisco CallManager Serviceability, Cisco CallManager User, RTMT, Cisco CallManager TraceAnalysis, Cisco CallManager Service, Trace Collection Tool, and CAR. \*
  - Privacy—Cisco CallManager supports encryption of signaling and media, Phone types include Cisco IP Phone 7940, 7960, and 7970; Survivable Remote Site Telephony (SRST), and MGCP gateways \*
  - Secure Sockets Layer (SSL) for directory—Supported applications include BAT, CAR, Cisco CallManager Admin User Pages, Cisco CallManager Admin IPMA Pages, Cisco CallManager User Pages / IP Phone Options Pages, Cisco Conference Connection, CTI Manager, Extension Mobility, IP Manager Assistant, and Multilevel Administration (MLA). \*
  - USB eToken containing a Cisco rooted X.509v3 certificate is used to generate a Certificate Trust List (CTL) file for the phones as well as configuring the security mode of the cluster.
  - Phone security—Trivial File Transfer Protocol (TFTP) files (configuration and firmware loads) are signed with the self-signed certificate of the TFTP server. The Cisco CallManager system administrator will be able to disable HTTP and Telnet on the IP phones.
- Session Initiation Protocol (SIP) trunk
  - SRST
  - Shared resource and application management and configuration
    - Transcoder resource
    - Conference bridge resource
    - Topological association of shared resource devices (conference bridge, music on hold [MoH] sources, transcoders)
    - Media termination point (MTP)—Support for SIP trunk and RFC 2833
    - Annunciator
  - Silence suppression, voice activity detection
  - Simplified North American Numbering Plan (NANP) and non-NANP support
  - T.38 fax support (H.323 only) \*
  - Third-party applications support
    - Broadcast paging—through foreign exchange station (FXS)
    - SMDI for MWI
    - Hook-flash feature support on selected FXS gateways
    - TSP 2.1 interface
    - JTAPI 2.0 service provider interface
    - Billing and call statistics
    - Configuration database API (Cisco AXL)

- Time of day, day of week, day of year routing/restrictions\*
- Toll restriction—Dial-plan partition
- Toll fraud prevention
  - Prevent trunk to trunk transfer\*
  - Drop conference call when originator hangs up\*
  - Forced authorization codes\*
- Unified device and system configuration
- Unified dial plan
- Video (SCCP and H.323)

\*Indicates new feature or service for Cisco CallManager Version 4.1

### Summary of User Features

- Abbreviated dial
- Answer and answer release
- Autoanswer and intercom
- Barge
- Call-back busy, no reply to station
- Call connection
- Call coverage\*
- Call forward—All (off-net and on-net)
- Call forward—Busy
- Call forward—No answer
- Call hold and retrieve
- Call join
- Call park and pickup
- Call pickup group—Universal
- Call status per line (state, duration, number)
- Call waiting and retrieve (with configurable audible alerting)
- Calling line identification (CLID)
- Calling line identification restriction (CLIR) call by call
- Calling party name identification (CNID)
- Conference barge
- Conference list and drop any party (ad-hoc conference)
- Direct inward dial (DID)
- Direct outward dial (DOD)
- Directory dial from phone—Corporate, personal
- Directories—Missed, placed, received calls list stored on selected IP phones
- Distinctive ring (on-net vs. off-net)
- Distinctive ring per line appearance
- Distinctive ring per phone
- Drop last conference party (ad-hoc conferences)

- Extension mobility support
- Hands-free, full-duplex speakerphone
- HTML help access from phone
- Immediate divert to voicemail
- Last number redial (off-net and on-net)
- Malicious call ID and trace
- Manager-assistant service (IPMA application)
  - Proxy line support
    - Manager features—Immediate divert or transfer, do not disturb, divert all calls, call intercept, call filtering on CLID, intercom, speed dials.
    - Assistant features—Intercom, immediate divert or transfer, divert all calls, manager call handling through assistant console application.
  - Shared line support
    - Manager features—Immediate divert or transfer, do not disturb, intercom, speed dials, barge, direct transfer, join.
    - Assistant features—Handle calls for managers; view manager status and calls; create speed dials for frequently used numbers; search for people in the corporate/Cisco CallManager directory; handle calls on their own lines; immediate divert or transfer, intercom, barge, privacy, multiple calls per line, direct transfer, join; send DTMF digits from console, MWI status of manager phone.
  - System capabilities—Multiple managers per assistant (up to 33 lines), redundant service.
- MWI
- Multiparty conference—Ad-hoc with add-on, meet-me features
- Multiple calls per line appearance
- Multiple line appearances per phone
- MoH
- Mute capability from speakerphone and handset
- On-hook dialing
- Operator attendant—Cisco Attendant Console
  - Call queuing
  - Broadcast hunting
  - Shared line support
- Privacy
- Real-time QoS statistics through HTTP browser to phone
- Recent dial list—Calls to phone, calls from phone, autodial, and edit dial
- Service URL—Single button access to IP phone service
- Single directory number, multiple phones—Bridged line appearances
- Speed dial—Multiple speed dials per phone
- Station volume controls (audio, ringer)
- Transfer
  - Blind
  - Consultative
  - Direct transfer of two parties on a line.



- User-configured speed dial and call forward through Web access
- Video (SCCP and H.323)
- Web services access from phone
- Web dialer—Click to dial
- Wideband audio codec support—Proprietary 16-bit resolution, 16-kHz sampling rate codec

\*Indicates new feature or service for Cisco CallManager Version 4.1

### Summary of Administrative Features

- Application discovery and registration to SNMP manager
- AXL SOAP API with performance and real-time information
- BAT
- CDRs
- CAR tool
- Call forward reason code delivery
- Centralized, replicated configuration database; distributed Web-based management viewers
- Configurable and default ringer WAV files per phone
- Configurable call forward display
- Database automated change notification
- Date and time display format configurable per phone
- Debug information to common syslog file
- Device addition through wizards
- Device-downloadable feature upgrades—Phones, hardware transcoder resource, hardware conference bridge resource, VoIP gateway resource
- Device groups and pools for large system management
- Device mapping tool—IP address to Media Access Control (MAC) address
- Dynamic Host Configuration Protocol (DHCP) block IP assignment—Phones and gateways
- Dialed Number Analyzer (DNA)
- Dialed number translation table (inbound and outbound translation)
- Dialed number identification service (DNIS)
- Enhanced 911 service
- H.323-compliant interface to H.323 clients, gateways, and gatekeepers
- JTAPI 2.0 computer telephony interface
- Lightweight Directory Access Protocol (LDAP) Version 3 directory interface to selected vendor's LDAP directories
  - Active Directory
  - Netscape Directory Server
- MLA access
- MGCP signaling and control to selected Cisco VoIP gateways
- Native supplementary services support to Cisco H.323 gateways
- Paperless phone DNIS—Display-driven button labels on phones
- Performance-monitoring SNMP statistics from applications to SNMP manager or to operating system performance monitor
- QoS statistics recorded per call
- Redirected DNIS (RDNIS), inbound, outbound (to H.323 devices)

- Select specified line appearance to ring
- Select specified phone to ring
- Single CDR per cluster
- Single point system and device configuration
- Sortable component inventory list by device, user, or line
- System event reporting—To common syslog or operating system event viewer
- TAPI 2.1 CTI
- Time-zone configurable per phone
- Cisco Unity™ software user integration\*
- TAPS
- Extensible Markup Language (XML) API into IP phones (Cisco IP Phone 794x/796x)
- Zero-cost automated phone moves
- Zero-cost phone adds

\*Indicates new feature or service for Cisco CallManager Version 4.1

## CISCO CALLMANAGER VERSION 4.1 ENHANCEMENTS

### User Feature Enhancements

- Attendant Console has been “accessibility enabled” to simplify use for visually handicapped attendants.
  - Works in conjunction with JAWS screen reader software.
  - Shortcut keys provided for easy navigability; mouseless operation of Attendant Console is possible.
  - Audible alerts provided to alert the user when certain events occur.
  - Attempt to transfer, consult transfer, or conference a call results in the call being put on hold while the dial pad is displayed.
- Video has added the following new capabilities:
  - Support for the SCCP H.264 video codec. The H.264 video codec delivers significantly higher quality at a given bandwidth than H.263. H.264 will be supported for intracluster SCCP calls only. Devices that will support SCCP H.264 include:
    - Tandberg SCCP phones (550 and T1000)
    - IPVC 3.6plus (3511 and 3540)
  - Midcall video for Cisco VT Advantage—If both parties are SCCP video endpoints, the call will immediately become a video call. If one party is an H.323 endpoint, the call will become a video call. But if the H.323 endpoint rejects the incoming channel or does not open a channel, the video call will be either one-way video or no video.
  - Video display mode for IPVC 3.6plus. IPVC 3.6plus will include a SCCP version of the message control unit (MCU) that supports both voice-activated and continuous presence videoconferencing modes. Video display mode is a softkey (called VidMode) that allows users on a SCCP videophone to toggle incoming videos between voice-activated and continuous presence mode.
  - Participant information for IPVC 3.6plus. Cisco CallManager will provide participant information to the SCCP version of the IPVC MCU, including the user name and number. The IPVC MCU will display this information in the participant list on its Web management interface. The IPVC MCU can overlay this information in the video if it has an Enhanced Media Processor (EMP) module.

- Dynamic H.323 addressing (E.164 addressing)—H.323 clients can be configured in Cisco CallManager via an E.164 address. This simplifies H.323 client administration for deployments where H.323 clients are configured for DHCP. E.164 addressing can be paired with an Cisco IOS Software Release 12.3(8)T gatekeeper to simplify H.323 client dialing.

#### System Capability Enhancements

- BRI support—Support for secure communications using legacy BRI and analog secure endpoints (STE/STU) and support for IP-STE.
  - V.150.1 Modem-Relay-over-IP support—Cisco CallManager will respond to the Session Description Protocol (SDP) sent by the gateway with default parameters. V.150.1 is required by the secure mode of IP-STEs and BRI-STEs.
  - BRI station pre-emption.
- Call coverage—Cisco CallManager Version 4.1 provides the ability to set up coverage paths to route calls to individuals or groups, helping to ensure that calls are answered. Call coverage features include:
  - Forwarding out of a coverage path.
  - Ability to set up different coverage paths based on time of day, day of week, or day of year.
  - Ability to provide separate forwarding treatment for internal versus external Call Forward No-Answer (CFNA) calls.
  - Ability to provide separate forwarding treatment for internal versus external Call Forward Busy (CFB) calls.
  - Support of a maximum timer for hunt lists.
  - Ability to allow a line to appear in multiple line groups, which was a limitation in previous versions of Cisco CallManager.
  - Ability to allow a gateway to appear in multiple route groups, which was a limitation in previous versions of Cisco CallManager.
  - Ability to divert to a final forwarding location when a hunt list terminates, either through exhaustion or expiration of its maximum hunt timer. This location may be a dialed number (voicemail pilot, another hunt pilot, a route pilot, or any allowed dialed number) or a checkbox to select personal treatment based on settings for the original called party's line.
  - Splitting the existing route-list/hunt-list GUI into two separate forms—one for hunt list and one for route list.
- Call display restrictions—Ability for the system administrator to block calling/called/connected name/number between certain phones. This is frequently used in areas where, for security reasons, this calling information cannot be displayed on phones. A hotel is an example where calls from room to room would not display calling information.
- Forced authorization codes/client matter codes
  - Forced authorization codes—Allows a system administrator to require that an authorization code be entered prior to extending a call to a specific route pattern. This is often used as a mechanism to prevent fraudulent toll calls by individuals that might have access to the phones. The system administrator can assign authorization levels to allow some codes to have full calling capability and others to not be able to call certain numbers.
  - Client matter codes or account codes—Ability for a system administrator to require that a client matter code be entered prior to extending a call to a specific route pattern. This code is often used by companies to track calls made to specific accounts and use this data for billing purposes.
  - Client matter code and forced authorization code (CMC/FAC) information is recorded in the Cisco CallManager CDR database.

- H.323 FastStart—Support for inbound and outbound H.323 FastStart. This feature reduces the number of signals exchanged before voice is extended on a call. By using H.323 FastStart voice will be extended or cut-through using 10 less message exchanges. This can eliminate voice clipping connections that are separated by large distances with more than 50ms WAN delay. MTPs are required for outbound H.323 FastStart.
- MGCP BRI ETSI BRI basic-net3 (user-side only)—Allows a smaller, more cost-effective ISDN connection between Cisco CallManager and the PSTN for small offices where the cost of a Primary Rate Interface (PRI) is prohibitive.
- MLPP enhancements
  - BRI station pre-emption.
  - Support for MLPP-enabled, user-to-user information element (UUIE)-based PRI-4ESS interface.
  - Executive override precedence level; gives an additional precedence level that was previously unsupported.
  - Location-based MLPP through locations over intracluster and intercluster limited bandwidth WAN links.
  - Support for intercluster MLPP.
  - The signal information element, as described in 4.5.24 of ANSI T1.607.
- Q.SIG enhancements
  - Alerting name—Support of alerting name presentation and restriction for Q.SIG facilities. “alerting name” is the capability to send and receive a CalledName application protocol data unit (APDU) encapsulated in a facility information element within the ISDN Q.931 message. This is an optional capability specified in ISO 13868 as part of the SS-COMP feature; it provides “alerting on ring” only. “Alerting on busy” (an optional service that provides the name of the called user who cannot be reached) is not supported by this feature.
  - Call back/call completion—Support for ISO/IEC 13870: 2nd Ed, 2001-07 for Call Completion Supplementary Service:
    - Call Completion to Busy Subscriber (CCBS)
    - Call Completion on No Reply (CCNR)
  - Call diversion by reroute in addition to call diversion by forward switching—Call Diversion Supplementary Service ISO/IEC 13872 and ISO/IEC 13873, first edition 1995.
  - H.323 Annex M.1 (Q.SIG over H.323)—Delivers the Q.SIG feature set across intercluster trunks by the tunneling of Q.SIG messages by the Cisco CallManager over H.323, based on recommendations in the ITU recommendation for Annex M.1: “Tunneling of QSIG in H.323 07/2003”. This development is limited to Q.SIG tunneling over Cisco CallManager H.323 intercluster trunks (both gatekeeper- and nongatekeeper-controlled). Interoperability between Cisco CallManager servers is the focus of this first release of Annex M.1.
  - Path replacement—Replace the existing time-division multiplexing (TDM) circuit(s) in use between two parties on an active call with new ones, to use TDM resources more efficiently. The Q.SIG path replacement feature will be implemented based on ISO/IEC 13863 – 2nd Ed, 1998 and ISO/IEC 13974 – 2nd Ed, 1999.
- Security features
  - Encryption to additional Cisco IP Phone 7940 and IP Phone 7960 devices, in addition to the already supported Cisco IP Phone 7970.
  - Encryption for MGCP gateways.
  - Encryption for SRST.
  - HTTPS for secure administration of Cisco CallManager. Supported by the following applications:
    - Cisco CallManager Admin

- Cisco CallManager Service
- Cisco CallManager User
- RTMT
- Cisco CallManager Trace Analysis
- Cisco CallManager Service Trace Collection Tool
- CDR Analysis and Reporting Tool

-- Locally significant certificates on Cisco IP Phone 7970G systems.

- SSL for secure transport of user information between Cisco CallManager applications and directories. Supported by the following applications:

- BAT
- CAR
- Cisco CallManager Admin User Pages
- Cisco CallManager Admin IPMA Pages
- Cisco CallManager User Pages and IP Phone Options Pages
- Cisco Conference Connection
- CTI Manager
- Extension Mobility
- IPMA
- MLA

- T.38 fax support (H.323 only)—Support for T.38 fax when using H.323 gateways. When a fax call is placed, the call is initially established as a voice call. The gateways advertise capabilities during connection establishment. If both gateways support T.38, they will attempt to switch to T.38 upon fax tone detection by either gateway.
- Time of day, day of week, day of year routing/restrictions
  - Ability to assign time schedules to partitions to determine when a phone, gateway, translation pattern, or route pattern can be reached. The time schedule can be based on time of day, day of week, or day of year. Using partitions, this feature can be used to assign time schedules for outbound calls (TOD restrictions) or inbound calls (TOD routing).
- Toll fraud improvements
  - Ability to drop an ad-hoc conference when the conference originator hangs up
  - Ability to drop an ad-hoc conference when all internal callers hang up
  - Ability to block transfers from external trunks or gateways to external trunks or gateways
- Video enhancements
  - SCCP support for H.264 video

- Midcall video for Cisco VT Advantage
- Video display mode for IPVC 3.6plus
- Participant information for IPVC 3.6plus
- Dynamic H.323 addressing (E.164 addressing)

#### Administrative Enhancements

- BAT has been enhanced to provide support for the following:
  - FAC/CMC
  - CAPF configuration
  - Option for removing duplicate IP services
  - Option for deleting unassigned dialed number
  - Call coverage
  - Video
  - Call display restrictions
  - MLPP DOD enhancements
  - Security
  - Q.SIG alerting name
  - Trunk-to-trunk transfer and drop conference feature
  - CTI super provider
- Serviceability enhancements
  - HTTPS support for secure troubleshooting.
  - New services added to the service activation and control center pages
    - Cisco dial number analyzer is not shown
    - Cisco CAPF has been added.
  - Dialed number analyzer enhancements
- Security
  - CAPF improvements
    - Runs as a Windows NT service
    - Can be managed from Cisco CallManager Administration interface
    - CAPF device database integrated in to Cisco CallManager database
    - Support for automatic certificate install/upgrade

- Support for certificates as phone credentials for CAPF operation (MIC/LSC) [EXPAND ACRONYMS HERE ON FIRST INSTANCE]
- Support for external certificate authority; includes KEON CA, Microsoft CA
- BAT support for CAPF
- CTL client direct support for CAPF
- The phone find list has new search options.

- Toll fraud improvements—Ability to mark gateways and trunks as internal or external.
- Cisco Unity user integration—Allows easy integration between Cisco CallManager directory number or user admin pages and Cisco Unity voice mailbox configuration. This helps shorten the time it takes for a system administrator to complete the task of adding a phone and voice mailbox for a user.

## ORDERING INFORMATION

### Software Upgrades

A downloadable upgrade package is available for Cisco CallManager clusters that are already running Cisco CallManager Version 4.0 at:

<http://www.cisco.com/cui-bin/tablebuild.pl/callmgr-4.1>

For all other upgrades or new Cisco CallManager 4.1 installations, Cisco CallManager CDs can be ordered.

Customers with a Cisco Software Application Support plus Upgrades (SASU) contract that is running Cisco CallManager versions 3.2, 3.3, or 4.0 who want to upgrade to Cisco CallManager Version 4.1 can order free upgrades using the Product Upgrade Tool (PUT) located at:

<http://www.cisco.com/upgrade>

For customers with no upgrade maintenance contract or upgrades from a previous version of Cisco CallManager one of the part numbers in Table 1 can be ordered.

**Table 1. Cisco CallManager Part Numbers**

SKU	Description
CM4.0-4.1-K9-UPG=	Cisco CallManager 4.0 to 4.1 upgrade
CM4.1-U-K9-7815SE=	Cisco CallManager 3.3 to 4.1 upgrade, MCS-7815s, 100-server user license
CM4.1-U-K9-7815=	Cisco CallManager 3.3 to 4.1 upgrade, MCS-7815s, 300-server user license
CM4.1-U-K9-7825SE	Cisco CallManager 3.3 to 4.1 upgrade, MCS-7825s, 100-server user license. Please note that Cisco CallManager 3.3 for a MCS-7825 with 100-server user license only shipped with MMIPC bundles MID-MKT-IPC-B and MID-MKT-IPC-C.
CM4.1-U-K9-7825=	Cisco CallManager 3.3 to 4.1 upgrade, MCS-7825s, 1000-server user license
CM4.1-U-K9-7835=	Cisco CallManager 3.3 to 4.1 upgrade, MCS-7835s, 2500-server user license
CM4.1-U-K9-7845=	Cisco CallManager 3.3 to 4.1 upgrade, MCS-7845s, 5000-server user license
CM4.1-U-K9-DL320=	Cisco CallManager 3.3 to 4.1 upgrade, HP DL320s, 1000-server user license
CM4.1-U-K9-DL380=	Cisco CallManager 3.3 - 4.1 upgrade, HP DL380s/1-CPU, 2500-server user license
CM4.1-U-K9-DL380D=	Cisco CallManager 3.3 - 4.1 upgrade, HP DL380s/2-CPU, 5000-server user license
CM4.1-U-K9-X306=	Cisco CallManager 3.3 to 4.1 upgrade, IBM xSeries 306, 1000-server user license

SKU	Description
CM4.1-U-K9-X345=	Cisco CallManager 3.3 to 4.1 upgrade, IBM xSeries 345/1-CPU, 2500-server user license
CM4.1-U-K9-X345D=	Cisco CallManager 3.3 to 4.1 upgrade, IBM xSeries 345/2-CPU, 5000-server user license

### New Installations

For new Cisco CallManager installations, Cisco CallManager software and server hardware must be ordered. Table 2 lists these part numbers.

**Table 2. New Cisco CallManager Order Numbers**

Server Model	SKU	Number of Phones
HP DL320-G2	CM4.1-K9-DL320=	1000
HP DL380-G3 with a single CPU	CM4.1-K9-DL380=	2500
HP DL380-G3 with dual CPUs	CM4.1-K9-DL380D=	5000
IBM x306	CM4.1-K9-X306=	1000
IBM x345 with a single CPU	CM4.1-K9-X345=	2500
IBM x345 with dual CPUs	CM4.1-K9-X345D=	5000
Cisco MCS 7825H-3000 or Cisco MCS 7825I-3000	CM4.1-K9-7825=	1000
Cisco MCS 7835H-3000 or Cisco MCS 7835I-3000	CM4.1-K9-7835=	2500
Cisco MCS 7845H-3000	CM4.1-K9-7845=	5000
Cisco MCS 7845H-3000	LIC-CCM4,X-2500=	2500 additional; 7500 total

The following servers will support Cisco CallManager Version 4.1:

- MCS-7815-1000
- MCS-7815I-2.0-EVV1
- MCS-7815I-3.0-IPC1
- MCS-7825-1133
- MCS-7825-800
- MCS-7825H-2.2-EVV1
- MCS-7825H-3.0-IPC1
- MCS-7825I-3.0-IPC1
- MCS-7835
- MCS-7835-1000
- MCS-7835-1266
- MCS-7835H-2.4-EVV1
- MCS-7835H-3.0-IPC1
- MCS-7835I-2.4-EVV1
- MCS-7845-1400
- MCS-7845H-2.4-EVV1
- MCS-7845H-3.0-IPC1
- HP DL320\*
- HP DL380/1CPU\*
- HP DL380/2CPU\*



- IBM x306\*
- IBM x330 1.2GHz only\*
- IBM x342\*
- IBM x345/1CPU\*
- IBM x345/2CPU\*

\*See <http://www.cisco.com/go/swonly> for details.

If you don't have one of supported servers, but wish to upgrade to Cisco CallManager Version 4.1, please refer to the server upgrade program can be found at:

<http://www.cisco.com/go/swonly>

Non-MCS servers that are supported with Cisco CallManager Version 4.1 can be found at:

<http://www.cisco.com/go/swonly>



**Corporate Headquarters**  
 Cisco Systems, Inc.  
 170 West Tasman Drive  
 San Jose, CA 95134-1706  
 USA  
[www.cisco.com](http://www.cisco.com)  
 Tel: 408 526-4000  
 800 553-NETS (6387)  
 Fax: 408 526-4100

**European Headquarters**  
 Cisco Systems International  
 BV  
 Haarlerbergpark  
 Haarlerbergweg 13-19  
 1101 CH Amsterdam  
 The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
 Tel: 31 0 20 357 1000  
 Fax: 31 0 20 357 1100

**Americas Headquarters**  
 Cisco Systems, Inc.  
 170 West Tasman Drive  
 San Jose, CA 95134-1706  
 USA  
[www.cisco.com](http://www.cisco.com)  
 Tel: 408 526-7660  
 Fax: 408 527-0883

**Asia Pacific Headquarters**  
 Cisco Systems, Inc.  
 168 Robinson Road  
 #28-01 Capital Tower  
 Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
 Tel: +65 6317 7777  
 Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus  
 Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
 Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
 Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
 Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Cisco IOS, and Cisco Unity are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0402R)  
 204121.30\_ETMG\_JM\_10.04

Printed in the USA

---

# Cisco Unity Unified Messaging

## Product Overview

Cisco Unity is a powerful Unified Communications server that provides advanced, convergence-based communication services and integrates them with the desktop applications business professionals use everyday, improving customer service and productivity. Designed for enterprise-scale organizations, Cisco Unity delivers unified messaging that gives subscribers the ability to access and manage messages and calls from anywhere, at any time, regardless of device or media type. Subscribers can listen to e-mail over the telephone, check voice messages from the Internet, and if a fax server is present, forward faxes to any local fax machine. Cisco Unity voice messaging features robust automated attendant functionality that includes intelligent routing, and easily customizable call screening and message notification options.

## Key Features and Benefits

Cisco Unity is designed for an IP environment. With IP, it's less expensive for organizations to deploy a comprehensive communications solution because there is a single network for both voice and data. Cisco Unity is the ideal IP telephony solution since it supports both Cisco CallManager and leading legacy telephone systems—even simultaneously—to help smooth the transition to IP telephony and protect existing infrastructure investments.

As an integral part of the Cisco Architecture for Voice, Video and Integrated Data (AVVID) environment, Cisco Unity complements the full range of Cisco IP-based voice solutions by providing advanced capabilities that unify data and voice. Also, because it's designed for a converged network, Cisco Unity provides a solid foundation for rolling out future convergence-based communications services, such as real-time desktop call control.

Cisco Unity features server architecture that is truly unified with an organization's data network, minimizing installation, administration, and maintenance costs. Built on a platform that can scale to meet a company's needs as it grows, Cisco Unity also uses streaming media and an intuitive HTML browser-style system administration interface that makes life easier for IT professionals, ultimately lowering an organization's total cost of ownership.

Cisco Unity is localized to meet the needs of customers around the globe. Localized versions are available in multiple languages—including Dutch, four dialects of English (Australian, New Zealand, U.K., and U.S.), French, German, Norwegian, and Spanish—and, depending on the language, feature everything from system prompts and subscriber conversations to the browser-based administration consoles and product documentation in the customer's language of choice. Cisco Unity also supports multiple languages on a single system, giving IT staff the ability to meet the individual needs of your employees.

Cisco Unity's optional digital networking module enables the system to connect to other Cisco Unity servers at the same site via the LAN, or remote sites using a WAN or the Internet. Digital networking makes communicating with coworkers at remote locations fast and efficient by giving users the ability to send subscriber-to-subscriber messages anywhere in the world.

## Cisco Unity Feature List

- E-mail, voice, and fax messages are delivered to a subscriber's e-mail inbox, giving users centralized communications control.
- Voice and fax messages can be accessed from a desktop PC, laptop computer using the Internet, or any touchtone telephone.
- Text-to-speech module reads e-mail messages over the telephone in clear, spoken US, UK and Australian English, French, German, Dutch, or Spanish.
- Send voice and fax messages to anyone who can receive Internet e-mail.
- VCR-style interface lets you play, rewind, pause, or fast forward messages with a few mouse clicks.
- With a fax server, store faxes for on-screen viewing or printing from any networked PC and forward faxes to any fax machine from a touchtone telephone.
- Browser-based personal administrator makes it easy to customize message notification options, allowing users to respond to messages as quickly as they would like. This also allows IT staff to enable end users to manage more of their own accounts, saving time and decentralizing routine administration.

- 
- Compound messaging capability provides the option to combine different media (i.e. attach a Word file to a voice message) in one message.
  - Global addressing speeds up the communications process.
  - Download all message types and respond or create new messages off line.
  - Save voice and fax messages along with e-mail in public or personal Exchange/Outlook folders for a complete record of communications.
  - Apply Microsoft Exchange's Inbox Assistant rules to voice and fax mail.
  - Delivers advanced voice mail and powerful unified messaging in a unified environment.
  - Leverages an organization's communications infrastructure investment by integrating with Cisco CallManager and leading legacy telephone system seven simultaneously paving the way for a smooth transition to IP telephony.
  - Easy-to-use browser-based system administration interface enables maintenance from any PC on the network, saving time, expense, and effort.
  - True unified architecture allows IT staff to set one back-up procedure, one message storage policy, and one security policy.
  - Designed for convergence, Cisco Unity provides optimum scalability, reliability, and performance.
  - Superior component-based server architecture provides a solid and flexible foundation for future growth.
  - Intuitive browser-based system administration console and tools simplify installation, maintenance, and daily use.
  - Fault-tolerant system tools include robust security, file replication, event logging, and optional software RAID levels 0-5.
  - International product offering localized versions in multiple languages including Dutch, four dialects of English (Australian, New Zealand, U.K., and U.S.), French, German, Norwegian, and Spanish-and, depending on the language, feature everything from system prompts and subscriber conversations to the browser-based administration consoles and product documentation in the customer's language of choice.

## Specifications

Cisco Unity is available as Voice Mail (VM) or as Unified Messaging (UM).

## Configurations

- Cisco Unity Voice Mail available in 4, 8, 12, 16, 24, 32, and 40 sessions  
configured for CallManager, or  
configured for legacy PBX/dual integration (contact your Cisco Software Sales Representative for integration information)
- Cisco Unity Unified Messaging available in 4, 8, 12, 16, 24, 32, and 40 sessions  
configured for CallManager, or  
configured for legacy PBX/dual integration (contact your Cisco Software Sales Representative for integration information)

## Options

- Voice Mail
- Voice Mail with Multi-lingual option
- Unified Messaging with Text-to-Speech (TTS) option
- Unified Messaging with Multi-lingual option

# Cisco Catalyst 4500

The Cisco Catalyst 4500 Series integrates resiliency for advanced control of converged networks.

### Overview

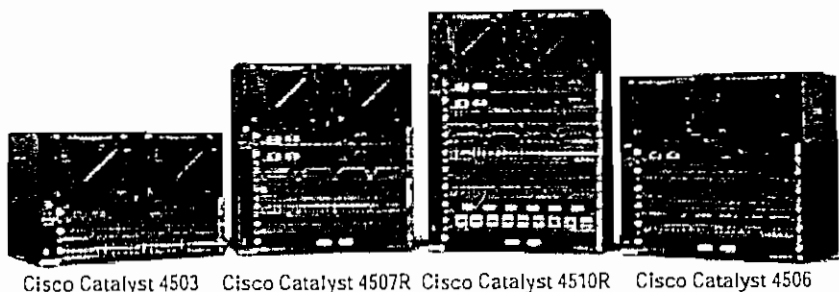
The Cisco® Catalyst® 4500 Series offers nonblocking Layers 2 through 4 switching with integrated resiliency, further enhancing control of converged networks. Converged voice, video, and data networks with high availability enable business resiliency for enterprise and metropolitan (metro) Ethernet customers deploying Internet-based business applications.

The next-generation Cisco Catalyst 4500 Series includes four Cisco Catalyst chassis: the Cisco Catalyst 4510R (ten slots), the Cisco Catalyst 4507R (seven slots), Cisco Catalyst 4506 (six slots), and Cisco Catalyst 4503 (three slots). Integrated resiliency enhancements offered in the Cisco Catalyst 4500 Series include 1+1 supervisor engine redundancy (Cisco Catalyst 4507R/4510R), integrated IEEE 802.3af compliant Power over Ethernet, software-based fault tolerance, and 1+1

power supply redundancy. Integrated resiliency in both hardware and software minimizes network downtime, helping to ensure workforce productivity, profitability, and customer success.

An important component of Cisco AVVID (Architecture for Voice, Video and Integrated Data), the Cisco Catalyst 4500 Series extends control to the network edge with intelligent network services, including sophisticated quality of service (QoS), predictable performance, advanced security, comprehensive management, and integrated resiliency. Offering compatibility with Cisco Catalyst 4000 Series line cards and Supervisor Engines, the Cisco Catalyst 4500 Series provides an extended window of deployment for the Cisco Catalyst 4000 Series in converged networks. This reduces the cost of ownership by minimizing recurring operational expenses, improving return on investment (ROI).

Figure 1  
 Cisco Catalyst 4500 Series



Cisco Systems, Inc.

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Page 1 of 12



### Cisco Catalyst 4500 Series Chassis

The Cisco Catalyst 4500 Series offers four chassis options and three Supervisor Engine options. It provides a common architecture that can scale up to 384 ports. The Cisco Catalyst 4507R and 4510R provides increased high availability in supporting 1+1 redundant supervisor engines with sub-minute failover time. Using the same line cards and Supervisor Engines as the widely deployed Cisco Catalyst 4000 Series, the Cisco Catalyst 4500 Series enhances the Cisco commitment to affordable enterprise and branch scalability. It provides a cost-effective, flexible network solution that scales to meet today's high-performance needs with investment protection (Table 1).

**Table 1** Cisco Catalyst 4500 Series Chassis Features

Feature	Cisco Catalyst 4503 Chassis	Cisco Catalyst 4506 Chassis	Cisco Catalyst 4507R Chassis	Cisco Catalyst 4510R Chassis
Total number of slots	3	6	7	10
Supervisor engine slots	1 <sup>1</sup>	1 <sup>1</sup>	2 <sup>2</sup>	2 <sup>2</sup>
Supervisor engine redundancy	No	No	Yes (Supervisor Engine II-Plus, IV, V)	Yes (Supervisor Engine V only)
Supervisor engines supported	Supervisor Engine II-Plus, IV, V	Supervisor Engine II-Plus, IV, V	Supervisor Engine II-Plus, IV, V	Supervisor Engine V only
Line card slots	2	5	5 <sup>2</sup>	8 <sup>2</sup>
Number of power supply bays	2	2	2	2
AC input power	Yes	Yes	Yes	Yes
DC input power	Yes	Yes	Yes	Yes
Integrated PoE (IP phone and wireless access point) support	Yes	Yes	Yes	Yes
Minimum number of power supplies	1	1	1	1
Number of fan tray bays	1	1	1	1
Location of 19-inch rack-mount <sup>3</sup>	Front	Front	Front	Front
Location of 23-inch rack-mount	Front (option)	Front (option)	Front (option)	Front (option)

1. Slot 1 is reserved for supervisor engine only; slots 2 and higher are reserved for line cards.

2. Slots 1 and 2 are reserved for supervisor engines only in Cisco Catalyst 4507R and 4510R; slots 3 and higher are reserved for line cards.

3. Chassis can be mounted in racks and cabinets that meet ANSI/EIA-310-D and ETS 300 119-3

**Note:** Supervisor engine slots do not support switching line card modules. Line card slots do not support supervisor engines.



## Configuration Alternatives

The Cisco Catalyst 4500 Series offers a powerful and flexible network solution that can be built with three Supervisor Engine alternatives. Each provides a high-performance, centralized, shared-memory switch fabric, protecting your line card investment by supporting the addition of optional higher-layer engines (Table 2).

**Table 2** Cisco Catalyst 4500 Series Supervisor Engine Support and Performance

Feature	Supervisor Engine II-Plus (WS-X4013+)	Supervisor Engine IV (WS-X4515)	Supervisor Engine V (WS-X4516)
Cisco Catalyst 4503 Chassis	Supported 28 Gbps, 21 Mpps	Supported 28 Gbps, 21 Mpps	Supported 28 Gbps, 21 Mpps
Cisco Catalyst 4506 Chassis	Supported 64 Gbps, 48 Mpps	Supported 64 Gbps, 48 Mpps	Supported 64 Gbps, 48 Mpps
Cisco Catalyst 4507R Chassis	Supported 64 Gbps, 48 Mpps	Supported 64 Gbps, 48 Mpps	Supported 68 Gbps, 51Mpps
Cisco Catalyst 4510R Chassis	Not supported	Not supported	Supported 96 Gbps 72 Mpps

The Cisco Catalyst 4500 Series has flexible interface types and port densities that allow network configurations to be mixed and matched to meet the specific needs of any campus network (Table 3).

**Table 3** Cisco Catalyst 4500 Series Port Densities

Cisco Catalyst 4500 Series Switching Modules	Number of Interfaces Supported per Line Card	Cisco Catalyst 4503	Cisco Catalyst 4506	Cisco Catalyst 4507R	Cisco Catalyst 4510R
Switched 10/100 Fast Ethernet (RJ-45)	32 or 48	96	240	240	384 <sup>1</sup>
Switched 10/100 Fast Ethernet (RJ-21)	48	96	240	240	384 <sup>1</sup>
Switched 100 Fast Ethernet (MT-RJ)	4 <sup>2</sup> , 24, or 48	96	240	240	384 <sup>1</sup>
Switched 1000 Gigabit Ethernet (fiber)	2, 6, 18, or 48	96	240	240	384 <sup>1</sup>
Switched 10/100/1000BASE-T Gigabit Ethernet	24 or 48	96	240	240	384 <sup>1</sup>

1. When using the Cisco Catalyst 4500 Supervisor Engine V, 336 ports are supported. The 4510R can support up to 384 ports with future Supervisor Engines. When Supervisor Engine V is used in the 4510R chassis, Slot 10 (Flex-slot) will support a sub-set of linecards: 2-port GBIC (WS-X4302-GB) and Access Gateway Module (WS-X4604-GWY). This is due to the switching capacity of the Supervisor Engine V, and not a limitation of the 4510R chassis. Future Supervisor Engines will allow Slot 10 to accommodate any and all linecards.

2. Four 100 Base FX, MMF interfaces are supported via the uplink module (WS-U4504-FX-MT) using the Cisco Catalyst 32-port, 10/100, RJ-45 (WS-X4232-RJ-XX) line card.



## Configuration Flexibility and Modular Superiority

The Cisco Catalyst 4503, 4506, 4507R, and 4510R offer the same comprehensive, scalable suite of 10/100/1000-Mbps Ethernet switch modules as the Cisco Catalyst 4006. Several Cisco Catalyst 4500 Series modules are available, which can be mixed and matched to suit numerous wiring closet, data center, or branch office deployments. Any Gigabit Ethernet port can be 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, or coarse wavelength-division multiplexing (CWDM) by using flexible, hot-swappable gigabit-interface-converter (GBIC) modules. The Cisco Catalyst 4500 Series supports the following switching modules:

- WS-F4531—Cisco Catalyst 4500 NetFlow Services Daughter Card
- WS-X4148-FE-LX-MT—Cisco Catalyst 4500 Fast Ethernet Switching Module, 48-port 100BASE-LX10 single-mode fiber (SMF) (MT-RJ)
- WS-X4148-FX-MT—Cisco Catalyst 4500 Fast Ethernet Switching Module, 48-port 100BASE-FX multimode fiber (MMF) (MT-RJ)
- WS-X4148-RJ—Cisco Catalyst 4500 10/100 Module, 48 ports (RJ-45)
- WS-X4148-RJ21—Cisco Catalyst 4500 10/100 Module, 48-port telco (4 x RJ-21)
- WS-X4248-RJ21V—Cisco Catalyst 4500 PoE 802.3af 10/100, 48-Ports(RJ21)
- WS-X4148-RJ45V—Cisco Catalyst 4500 Cisco Prestandard 10/100, 48 ports (RJ-45)
- WS-X4248-RJ45V—Cisco Catalyst 4500 PoE 802.3af 10/100, 48-Ports(RJ45)
- WS-X4232-GB-RJ—Cisco Catalyst 4500 32-port 10/100 (RJ-45), 2-Gigabit Ethernet (GBIC) Module
- WS-X4232-RJ-XX—Cisco Catalyst 4500 32-port 10/100 (RJ-45), plus modular uplink slot
- WS-X4302-GB—Cisco Catalyst 4500 Gigabit Ethernet Module, 2 ports (GBIC)
- WS-X4306-GB—Cisco Catalyst 4500 Gigabit Ethernet Module, 6 ports (GBIC)
- WS-X4418-GB—Cisco Catalyst 4500 Gigabit Ethernet Module, server switching 18 ports (GBIC)
- WS-X4424-GB-RJ45—Cisco Catalyst 4500 24-port 10/100/1000 Module (RJ-45)
- WS-X4448-GB-LX—Cisco Catalyst 4500 48-port 1000BASE-LX (SFP)
- WS-X4448-GB-RJ45—Cisco Catalyst 4500 48-port 10/100/1000 Module (RJ-45)
- WS-X4548-GB-RJ45—Cisco Catalyst 4500 Enhanced 48-port 10/100/1000 Module (RJ-45)
- WS-X4548-GB-RJ45V—Cisco Catalyst 4500 PoE 802.3af 10/100/1000, 48-Ports(RJ45)
- WS-U4504-FX-MT—Cisco Catalyst 4500 Fast Ethernet Uplink Daughter Card, 4-port 100BASE-FX (MT-RJ)
- WS-X4604-GWY—Cisco Catalyst 4500 Access Gateway Module with IP and firewall software
- WS-X4124-FX-MT—Cisco Catalyst 4000 Fast Ethernet Switching Module, 24-port 100BASE-FX (MT-RJ)
- WS-G5483—Cisco 1000BASE-T GBIC
- WS-G5484—Cisco 1000BASE-SX Short-Wavelength GBIC (multimode only)
- WS-G5486—Cisco 1000BASE-LX/LH Long-Haul GBIC (single mode or multimode)
- WS-G5487—Cisco 1000BASE-ZX Extended-Reach GBIC (single mode)
- Cisco coarse wavelength-division multiplexing (CWDM) GBIC solution



**Table 4** Cisco Catalyst Supervisor Engine Software Minimum Requirements

Specification	Cisco Catalyst 4503, 4506, and 4507R with Supervisor Engine II-Plus	Cisco Catalyst 4503, 4506, and 4507R with Supervisor Engine IV	Cisco Catalyst 4503, 4506, 4507R, and 4510R with Supervisor Engine V
Minimum software requirement	Cisco IOS <sup>®</sup> Software Release 12.1(19)EW or higher	Cisco IOS Software Release 12.1(12c)EW or higher	Cisco IOS Software Release 12.2(18)EW

**Table 5** Comparison Between Cisco Catalyst Chassis

Feature	Cisco Catalyst 4006	Cisco Catalyst 4503	Cisco Catalyst 4506	Cisco Catalyst 4507R	Cisco Catalyst 4510R
Power over Ethernet (PoE)	Yes—With external power shelf	Yes—Integrated	Yes—Integrated	Yes—Integrated	Yes—Integrated
PoE per line card slot maximum	400W	830W	830W	830W	830W
Power supply redundancy	2 + 1	1 + 1	1 + 1	1 + 1	1 + 1
Supervisor engine redundancy	No	No	No	Yes	Yes
Supported line cards	All Cisco Catalyst 4000 line cards	All Cisco Catalyst 4000 line cards	All Cisco Catalyst 4000 line cards	All Cisco Catalyst 4000 line cards	All Cisco Catalyst 4000 line cards
Supervisor engines supported	Supervisor Engines II-Plus, IV and V	Supervisor Engines II-Plus, IV and V	Supervisor Engines II-Plus, IV and V	Supervisor Engines II-Plus, IV and V	Supervisor Engines V only
Internal Power supplies supported	400-watt AC	1000-watt AC 1400-watt AC 1300-watt ACV 2800-watt ACV 1400-watt DC	1000-watt AC 1400-watt AC 1300-watt ACV 2800-watt ACV 1400-watt DC	1000-watt AC 1400-watt AC 1300-watt ACV 2800-watt ACV 1400-watt DC	1400-watt AC <sup>1</sup> 2800-watt ACV <sup>1</sup> 1400-watt DC

<sup>1</sup> The 1400W AC and 2800W AC power supplies are required to support a fully loaded Catalyst 4510R. The 1000W AC and 1300W AC power supplies can be deployed in the 4510R; however, power management is required.



## Standard Network Protocols

- Ethernet
  - IEEE 802.3, 10BASE-T
- Fast Ethernet
  - IEEE 802.3u, 100BASE-TX
  - IEEE 802.3, 100BASE-FX
- Gigabit Ethernet
  - IEEE 802.3z
  - IEEE 802.3x
  - IEEE 802.3ab
- 1000BASE-X (GBIC)
  - 1000BASE-SX
  - 1000BASE-LX/LH
  - 1000BASE-ZX
- Virtual LAN (VLAN) trunking/tagging
  - IEEE 802.1Q
  - IEEE 802.3ad
- Spanning-Tree Protocol
  - IEEE 802.1D
  - IEEE 802.1w
  - IEEE 802.1s
- Security
  - IEEE 802.1x
- Power over Ethernet (PoE)
  - IEEE 802.3af

## Network Management

- Support provided by Cisco Works Resource Manager Essentials (a component of LAN Management Solution [LMS])
  - Builds and maintains an up-to-date hardware and software inventory
  - Maintains an active archive and simplifies deployment of configuration changes to multiple devices
  - Simplifies and accelerates software image analysis and automates deployment
  - Records and displays comprehensive reports of software, hardware, and configuration changes
  - Highlights critical devices and their ability to respond
  - Isolates network error conditions and suggests probable causes
- Support provided by Cisco Works Resource Manager Essentials (a component of LMS)
  - Network topology discovery and display services
  - VLAN provisioning and logical display representation
  - Traffic monitoring and performance assessment
  - End station tracking with search utilities
  - CiscoView graphical device management
  - Network topology integrity checking
  - Cisco Discovery Protocol
  - Cisco Virtual Trunking Protocol (VTP)
  - Simple Network Management Protocol (SNMP) Version 1 (RFCs 1155-1157)
  - SNMP Version 2c
  - Cisco Workgroup Management Information Base (MIB)

Cisco Systems, Inc.

All contents are Copyright © 1992-2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Page 6 of 12

- Ethernet MIB (RFC 1643)
- Ethernet Repeater MIB (RFC 1516)
- SNMP MIB II (RFC 1213)
- Remote Monitoring (RMON) (RFC 1757)
- RMON II (RFC 2021)
- Interface table (RFC 1573)
- Bridge MIB (RFC 1493)
- Switched Port Analyzer (SPAN)
- Enhanced Switched Port Analyzer (ESpan)
- Port snooping and connection steering
- Standard Cisco IOS Software security capabilities: passwords and Terminal Access Controller Access Control System (TACACS+)
- Telnet, Trivial File Transfer Protocol (TFTP), and Bootstrap Protocol (BOOTP) for management access

### Physical Specifications

**Table 6** Physical Specifications of Cisco Catalyst 4500 Series Chassis

Specification	Cisco Catalyst 4503	Cisco Catalyst 4506	Cisco Catalyst 4507R	Cisco Catalyst 4510R
Dimensions (H x W x D)	12.25 x 17.31 x 12.50 in. (31.12 x 43.97 x 31.70 cm)	17.38 x 17.31 x 12.50 in. (44.13 x 43.97 x 31.70 cm)	19.19 x 17.31 x 12.50 in. (48.74 x 43.97 x 31.70 cm)	24.35 x 17.31 x 12.50 in. (61.84 x 43.97 x 31.70 cm)
Rack units (RU)	7 RU	10 RU	11 RU	14 RU
Chassis weight (w/fan tray)	31.25 lbs./14.18 kg.	40.50 lbs./18.37 kg.	44.25 lbs./20.07 kg.	51.50 lb/23.36 kg.
Mounting	19- and 23-Inch rack compatible (19-inch rack and cable guide hardware included)	19- and 23-Inch rack compatible (19-inch rack and cable guide hardware included)	19- and 23-inch rack compatible (19-inch rack and cable guide hardware included)	19- and 23-Inch rack compatible (19-Inch rack and cable guide hardware included)

### Power Supply Indicators and Interfaces

- Fan cooling: Integrated in hot-insertion/hot-extraction unit
- Good: Green (good)
- Fail: Red (faulty)
- SNMP MIB supported

**Table 7** Cisco Catalyst 4500 Series Power Supply Specifications

Power Supply	1000W AC	1400W AC	1300W AC	2300W AC	1400W DC	2500W AC—Power Shelf P/S
Integrated Power over Ethernet (PoE)	No (Data only)	No (Data Only)	Yes (Up to 800W)	Yes (Up to 1400W)	Up to 7500W (minus the power consumed for data) when connected directly to a DC power plant or 2 External AC Power Shelves	2500W per power supply; 5000W per shelf (minus the power consumed for data)
IEEE 802.3af Compliant PoE	No	No	Yes	Yes	Yes	Yes
Input current (rated)	12A @ 100 VAC, 5A @ 240 VAC	16A @ 100 VAC, 7A @ 240 VAC	16A @ 100 VAC, 7A @ 240 VAC	16A @ 200 VAC	31A @ -60 VDC (Data only) 180A @ -48 VDC (PoE)	15A @ 200 VAC
Output current (data)	12V @ 83.4A 3.3V @ 12.2A	12V @ 113.4A 3.3V @ 12.2A	12V @ 84.7A 3.3V @ 12.5A	12V @ 113.3A 3.3V @ 12.1A	12V @ 120A 3.3V @ 10A	-52 VDC @ 50A (total output per supply)
Output current (PoE)	N/A	N/A	-50V @ 16.7A	-50V @ 28A	140A @ -48/-60 VDC	-52 VDC @ 50A (total output per supply)
Output power redundant mode (Data)	1000W + 40W	1360W + 40W	1000W + 40W	1360W + 40W	1360W + 40W	Up to 1400W (via DC supply)
Output power redundant mode (PoE)	N/A	N/A	800W max. per power supply	1400W max. per power supply	Up to 7500W (minus the power consumed for data)	2500W per supply (minus the power consumed for data)
Output power combined mode (Data)	1667W	2473W	1667W	2473W	N/A	N/A
Output power combined mode (PoE)	N/A	N/A	1333W	2333W	N/A	N/A
Heat dissipation <sup>1</sup>	943 BTU/Hr.	1048 BTU/Hr.	1568 BTU/Hr.	2387 BTU/Hr.	Data only: 1591 BTU/Hr. Data and voice: 2905 BTU/Hr.	1210 BTU/Hr. per power supply
Holdup time	20 ms	20 ms	20 ms	20 ms	4 ms	20 ms
Number of 802.3af Class 2 PDs Supported with one power supply (1+1)	N/A	N/A	102	179	384 <sup>2</sup>	384 <sup>2</sup>
Number of 802.3af Class 0 & 3 PDs Supported with one power supply (1+1)	N/A	N/A	46	80	384 <sup>2</sup>	384 <sup>2</sup>
Cisco phones with integrated PoE <sup>3</sup>	None	N/A	126	222	384 <sup>2</sup>	384 <sup>2</sup>
Hot swappable	Yes	No (Data Only)	Yes	Yes	Yes	Yes

1. Note that calculations for heat dissipation is based on one power supply operating at maximum output power.

2. Measured when two AC power shelves are strapped together and contain 3x2500W AC power supplies.

3. Measured when using Cisco prestandard PoE line cards (WS-X4148-RJ45V).



Notes for Table 7:

1. Output power is per power supply, unless otherwise stated.
2. Heat dissipation numbers represent the power conversion losses of the power supply in operation.
3. The number of power devices (PD's) supported will depend on customer configuration.

### Fan Trays

Each Cisco Catalyst 4500 Series chassis uses a single fan tray for cooling. All fan trays are composed of independent fans. If one fan fails, the system will continue to operate without a significant degradation in cooling. The system will detect and notify the user (via LED, CLI, and SNMP) that a fan has failed and the tray needs to be replaced.

### Fabric Redundancy Modules (Cisco Catalyst 4507R and 4510R Only)

The Cisco Catalyst 4500 redundancy scheme uses removable fabric redundancy modules on the passive backplane to switch traffic to the active supervisor. There is one fabric redundancy module per line cards. Fabric redundancy modules and redundant clocks ship standard with every Cisco Catalyst 4507R and 4510R chassis. Spare fabric redundancy modules and clock modules are available for serviceability.

### Environmental Conditions

- Operating temperature: 32° to 104°F (0° to 40°C)
- Storage temperature: -40° to 167°F (-40° to 75°C)
- Relative humidity: 10 to 90%, noncondensing
- Operating altitude: -60 to 2000 m

### Regulatory Standards Compliance

**Table 8** Regulatory Standards Compliance of Cisco Catalyst 4500 Series

Specification	Standard
Regulatory compliance	CE marking
Safety	<ul style="list-style-type: none"><li>• UL 60950</li><li>• CAN/CSA-C22.2 No. 60950</li><li>• EN 60950</li><li>• IEC 60950</li><li>• TS 001</li><li>• AS/NZS 3260</li></ul>

**Table 8** Regulatory Standards Compliance of Cisco Catalyst 4500 Series (Continued)

Specification	Standard
EMC	<ul style="list-style-type: none"> <li>• FCC Part 15 (CFR 47) Class A</li> <li>• ICES-003 Class A</li> <li>• EN55022 Class A</li> <li>• CISPR22 Class A</li> <li>• AS/NZS 3548 Class A</li> <li>• VCCI Class A</li> <li>• EN 55022</li> <li>• EN 55024</li> <li>• EN 61000-6-1</li> <li>• EN 50082-1</li> <li>• EN 61000-3-2</li> <li>• EN 61000-3-3</li> <li>• ETS 300 386</li> </ul>
Industry EMC, safety, and environmental standards	<ul style="list-style-type: none"> <li>• GR-63-Core Network Equipment Building Standards (NEBS) Level 3</li> <li>• GR-1089-Core Level 3</li> <li>• ETS 300 019 Storage Class 1.1</li> <li>• ETS 300 019 Transportation Class 2.3 (pending)</li> <li>• ETS 300 019 Stationary Use Class 3.1</li> <li>• ETS 300 386</li> </ul>
Telecom (E1)	<ul style="list-style-type: none"> <li>• CTR 12/13</li> <li>• CTR 4</li> <li>• ACA TS016</li> </ul>
Telecom (T1)	<ul style="list-style-type: none"> <li>• FCC Part 68</li> <li>• Canada CS-03</li> <li>• JATE Green Book</li> </ul>

**Ordering Information****Table 9** Cisco Catalyst 4500 Series Common Equipment Ordering Information

Product Number	Description
WS-C4503	Cisco Catalyst 4500 (3-slot chassis), fan, no power supply
WS-C4506	Cisco Catalyst 4500 (6-slot chassis), fan, no power supply
WS-C4507R	Cisco Catalyst 4500 (7-slot chassis), fan, no power supply, redundant supervisor capable
WS-C4510R	Cisco Catalyst 4500 (10-slot chassis), fan, power supply; redundant supervisor capable
PWR-C45-1000AC	Cisco Catalyst 4500 1000-watt AC power supply (Data only)
PWR-C45-1400AC	Cisco Catalyst 4500 1400-watt AC power supply (Data only)
PWR-C45-1300ACV	Cisco Catalyst 4500 1300-watt AC power supply (with integrated PoE)
PWR-C45-2800ACV	Cisco Catalyst 4500 2800-watt AC power supply (with integrated PoE)

**Table 9** Cisco Catalyst 4500 Series Common Equipment Ordering Information (Continued)

Product Number	Description
PWR-C45-1400DC-P	Cisco Catalyst 4500 1400W DC power supply with Integrated PEM
WS-P4502-1PSU	Catalyst 4500 Aux. Power Shelf (2 slot), incl. 1 PWR-4502
PWR-4502	Catalyst 4500 Aux. Power Shelf Redundant Power Supply
WS-X4013+	Cisco Catalyst 4500 Series Supervisor Engine II-Plus
WS-X4515	Cisco Catalyst 4500 Series Supervisor Engine IV
WS-X4515/2	Cisco Catalyst 4507R Series Redundant Supervisor Engine IV
WS-X4516	Cisco Catalyst 4500 Series Supervisor Engine V
WS-X4516/2	Cisco Catalyst 4507R Series Redundant Supervisor Engine V
S4KL3-12218EW <sup>1</sup>	Cisco IOS Software: Basic Layer 3 software Image (RIP, static routes, IPX, AppleTalk)
S4KL3K91-12218EW	Cisco IOS Software: Basic Layer 3 software image, (RIP, static routes, IPX, AppleTalk, 3DES)
S4KL3E-12218EW	Cisco IOS Software: Enhanced Layer 3 software Image, (OSPF, EIGRP, and IS-IS)
S4KL3EK91-12218EW	Cisco IOS Software: Enhanced Layer 3 software Image, (OSPF, EIGRP, and IS-IS, 3DES)
MEM-C4K-FLD64M	Cat 4500 IOS-based Supervisor, Compact Flash memory, 64-MB option
MEM-C4K-FLD128M	Cat 4500 IOS-based Supervisor, Compact Flash memory, 128-MB option

1. Enhanced Layer 3 software (S4KL3E-12218EW and S4KL3EK91-12218EW) is available for the IV, and V only

### Licensing

Use of RMON on Cisco Catalyst 4500 Series switches requires the RMON agent license (Table 9). Use of Border Gateway Protocol Version 4 (BGP4) on the Supervisor Engine IV/V requires an InterDomain Routing license. Only one RMON agent license or InterDomain Routing license is required per chassis.

**Table 10** RMON on the Cisco Catalyst 4500 Series

Product Number	Description
WS-C4503-EMS-LIC(=)	Cisco Catalyst 4503 RMON Agent license
WS-C4006-EMS-LIC	Cisco Catalyst 4006 RMON Agent license
WS-C4506-EMS-LIC(=)	Cisco Catalyst 4506 RMON Agent license
WS-C4507R-EMS-LIC(=)	Cisco Catalyst 4507R RMON Agent license
WS-C4510R-EMS-LIC(=)	Cisco Catalyst 4510R RMON Agent license
FR-IRC4(=)	Cisco Catalyst 4000 Supervisor Engine IV/V InterDomain Routing feature license

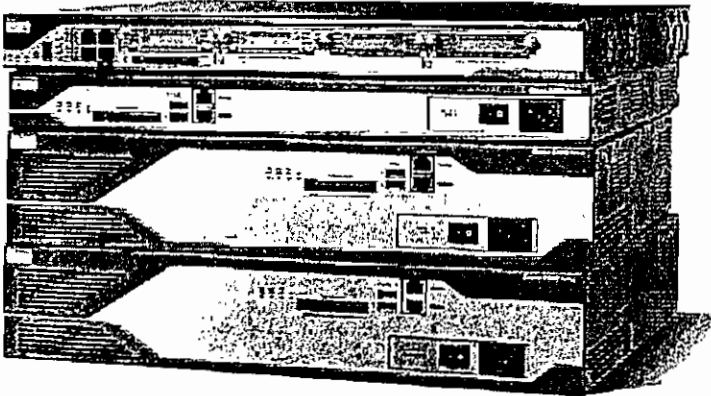


DATA SHEET

## CISCO 2800 SERIES INTEGRATED SERVICES ROUTERS

Cisco Systems<sup>®</sup>, Inc. is redefining best-in-class enterprise and small- to- midsize business routing with a new line of integrated services routers that are optimized for the secure, wire-speed delivery of concurrent data, voice, and video services. Founded on 20 years of leadership and innovation, the Cisco<sup>®</sup> 2800 Series of integrated services routers (refer to Figure 1) intelligently embed data, security, and voice services into a single, resilient system for fast, scalable delivery of mission-critical business applications. The unique integrated systems architecture of the Cisco 2800 Series delivers maximum business agility and investment protection.

Figure 1  
Cisco 2800 Series



### PRODUCT OVERVIEW

The Cisco 2800 Series comprises four new platforms (refer to Figure 1): the Cisco 2801, the Cisco 2811, the Cisco 2821, and the Cisco 2851. The Cisco 2800 Series provides significant additional value compared to prior generations of Cisco routers at similar price points by offering up to a fivefold performance improvement, up to a tenfold increase in security and voice performance, new embedded service options, and dramatically increased slot performance and density while maintaining support for most of the more than 90 existing modules that are available today for the Cisco 1700, Cisco 2600, and Cisco 3700 Series.

The Cisco 2800 Series features the ability to deliver multiple high-quality simultaneous services at wire speed up to multiple T1/E1/xDSL connections. The routers offer embedded encryption acceleration and on the motherboard voice digital-signal-processor (DSP) slots; intrusion prevention system (IPS) and firewall functions; optional integrated call processing and voice mail support; high-density interfaces for a wide range of connectivity requirements; and sufficient performance and slot density for future network expansion requirements and advanced applications.

## SECURE NETWORK CONNECTIVITY FOR DATA, VOICE, AND VIDEO

Security has become a fundamental building block of any network. Routers play an important role in any network defense strategy because security needs to be embedded throughout the network. The Cisco 2800 Series features advanced, integrated, end-to-end security for the delivery of converged services and applications. With the Cisco IOS<sup>®</sup> Software Advanced Security feature set, the Cisco 2800 provides a robust array of common security features such as a Cisco IOS Software Firewall, intrusion prevention, IPsec VPN, Secure Shell (SSH) Protocol Version 2.0, and Simple Network Management Protocol (SNMPv3) in one secure solution set. Additionally, by integrating security functions directly into the router itself, Cisco can provide unique intelligent security solutions other security devices cannot, such as network admissions control (NAC) for antivirus defense; Voice and Video Enabled VPN (V3PN) for quality-of-service (QoS) enforcement when combining voice, video, and VPN; and Dynamic Multipoint VPN (DMVPN) and Easy VPN for enabling more scalable and manageable VPN networks. In addition, Cisco offers a range of security acceleration hardware such as the intrusion-prevention network modules and advanced integration modules (AIM) for encryption, making the Cisco 2800 Series the industry's most robust and adaptable security solution available for branch offices. As Figure 2 demonstrates, using a Cisco 2800 Series uniquely enables customers to deliver concurrent, mission-critical data, voice, and video applications with integrated, end-to-end security at wire-speed performance.

## CONVERGED IP COMMUNICATIONS

As shown in Figure 2, the Cisco 2800 Series can meet the IP Communications needs of small-to-medium sized business and enterprise branch offices while concurrently delivering an industry-leading level of security within a single routing platform. Cisco CallManager Express (CME) is an optional solution embedded in Cisco IOS Software that provides call processing for Cisco IP phones. This solution is for customers with data-connectivity requirements interested in deploying a converged IP telephony solution for up to 72 IP phones and—as of Cisco IOS 12.3(11) release—for up to 96 IP phones. With the Cisco 2800 Series, customers can securely deploy data, voice, and IP telephony on a single platform for their small-to-medium sized branch offices, helping them to streamline their operations and lower their network costs. The Cisco 2800 Series with optional Cisco CME support offers a core set of phone features that customers require for their everyday business needs and takes advantage of the wide array of voice capabilities that are embedded in the Cisco 2800 Series (as shown in Table 1) together with optional features available in Cisco IOS Software to provide a robust IP telephony offering for the small to medium-sized branch-office environment.

## INTEGRATED SERVICES

Figure 2 also highlights the fact that with the unique integrated services architecture of the Cisco 2800 Series, customers can now securely deploy IP Communications with traditional IP routing while leaving interface and module slots available for additional advanced services. With the optional integration of a wide array of services modules, the Cisco 2800 Series offers the ability to easily integrate the functions of standalone network appliances and components into the Cisco 2800 Series chassis itself. Many of these modules, such as the Cisco Network Analysis Module, Cisco Voice Mail Module, Cisco Intrusion Detection Module, and Cisco Content Engine Module, have embedded processors and hard drives that allow them to run largely independently of the router while allowing management from a single management interface. This flexibility greatly expands the potential applications of the Cisco 2800 Series beyond traditional routing while still maintaining the benefits of integration. These benefits include ease of management, lower solution costs (CAPEX and OPEX), and increased speed of deployment.

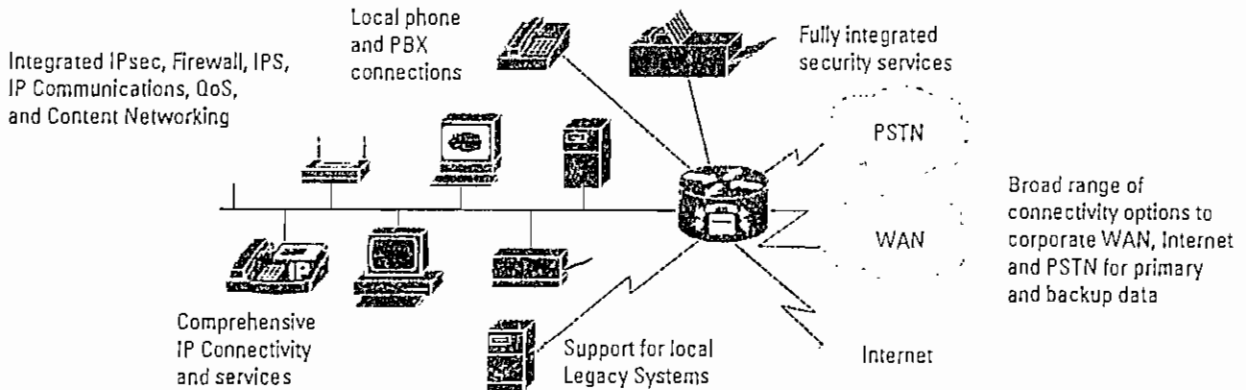


## APPLICATIONS

### Secure Network Connectivity with Converged IP Communications

Figure 2

Secure Network Connectivity with Converged IP Communications



## KEY FEATURES AND BENEFITS

### Architecture—Features and Benefits

The Cisco 2800 Series architecture has been designed specifically to meet the expanding requirements of enterprise branch offices and small-to-medium-sized businesses for today's and future applications. The Cisco 2800 Series provides the broadest range of connectivity options in the industry combined with leading-edge availability and reliability features. In addition, Cisco IOS Software provides support for a complete suite of transport protocols, Quality-of-Service (QoS) tools, and advanced security and voice applications.

Table 1. Architecture—Features and Benefits

Feature	Benefit
Modular architecture	<ul style="list-style-type: none"> <li>A wide variety of LAN and WAN options are available. Network interfaces can be upgraded in the field to accommodate future technologies.</li> <li>Several types of slots are available to add connectivity and services in the future on an "integrate-as-you-grow" basis.</li> <li>The Cisco 2800 supports more than 90 modules, including most of the existing WICs, VICs, network modules, and AIMs (Note: the Cisco 2801 router does not support network modules).</li> </ul>
Embedded security hardware acceleration	<ul style="list-style-type: none"> <li>Each of the Cisco 2800 Series routers comes standard with embedded hardware cryptography accelerators, which when combined with an optional Cisco IOS Software upgrade help enable WAN link security and VPN services.</li> </ul>
Increased default memory	<ul style="list-style-type: none"> <li>The Cisco 2811, 2821, and 2851 Routers offer 64 MB of Flash and 256 MB of DRAM memory.</li> <li>The Cisco 2801 router comes with 64 MB Flash and 128 MB DRAM memory.</li> </ul>
Integrated dual Fast Ethernet or Gigabit Ethernet ports	<ul style="list-style-type: none"> <li>The Cisco 2800 Series provide two 10/100 on the Cisco 2801 and Cisco 2811 and two 10/100/1000 on the Cisco 2821 and Cisco 2851</li> </ul>

Feature	Benefit
Support for Cisco IOS Software Release 12.3T feature sets	<ul style="list-style-type: none"> <li>The Cisco 2800 helps enable end-to-end solutions with full support for the latest Cisco IOS Software-based QoS, bandwidth management, and security features.</li> <li>Common feature and command set structure across the Cisco 1700, 1800, 2600, 2800, 3700 and 3800 series routers simplifies feature set selection, deployment, management, and training.</li> </ul>
Optional integrated power supply for distribution of Power over Ethernet (PoE)	<ul style="list-style-type: none"> <li>An optional upgrade to the internal power supply provides in-line power (802.3af-compliant Power-over-Ethernet [PoE] and Cisco standard inline power) to optional integrated switch modules.</li> </ul>
Optional integrated universal DC power supply	<ul style="list-style-type: none"> <li>On the Cisco 2811, 2821, and 2851 routers an optional DC power supply is available that extends possible deployments environments such as central offices and industrial environments (Note: not available on the Cisco 2801).</li> </ul>
Integrated redundant-power-supply (RPS) connector	<ul style="list-style-type: none"> <li>On the Cisco 2811, 2821, and 2851 there is a built in external power-supply connector that eases the addition of external redundant power supply that can be shared with other Cisco products to decrease network downtime by protecting the network components from downtime due to power failures.</li> </ul>

#### Modularity—Features and Benefits

The Cisco 2800 Series provides significantly enhanced modular capabilities (refer to Table 2) while maintaining investment protection for customers. The modular architecture has been redesigned to support increasing bandwidth requirements, time-division multiplexing (TDM) interconnections, and fully integrated power distribution to modules supporting 802.3af PoE or Cisco in-line power, while still supporting most existing modules. With more than 90 modules shared with other Cisco routers such as the Cisco 1700, 1800, 2600, 3700, and 3800 series, interfaces for the Cisco 2800 Series can easily be interchanged with other Cisco routers to provide maximum investment protection in the case of network upgrades. In addition, taking advantage of common interface cards across a network greatly reduces the complexity of managing inventory requirements, implementing large network rollouts, and maintaining configurations across a variety of branch-office sizes.

**Table 2. Modularity—Features and Benefits**

Feature	Benefit
Enhanced network-module (NME) slots	<ul style="list-style-type: none"> <li>The NME slots support existing network modules (Note: NM and NME support on Cisco 2811, 2821, and 2851 only)</li> <li>NME Slots offer high data throughput capability (up to 1.6Gbps) and support for Power over Ethernet (POE).</li> <li>NME slots are highly flexible with future support for extended NMEs (NME-X on Cisco 2821 and 2851 only) and enhanced double-wide NMEs (NME-XDs) (Note: Cisco 2851 only).</li> </ul>
High-performance WIC (HWIC) slots with enhanced functionality	<ul style="list-style-type: none"> <li>Four integrated HWIC slots on Cisco 2811, 2821, and 2851 and two integrated HWIC slots on Cisco 2801 allow for more flexible and dense configurations.</li> <li>HWICs slots can also support WICs, VICs, and VWICs</li> <li>HWIC slots offer high data throughput capability (up to 400 Mbps half duplex or 800 Mbps aggregate throughput) and Power over Ethernet (POE) support.</li> <li>A flexible form factor supports up to two double-wide HWIC (HWIC-D) modules.</li> </ul>
Dual AIM slots	<ul style="list-style-type: none"> <li>Dual AIM slots support concurrent services such as hardware-accelerated security, ATM segmentation and reassembly (SAR), compression, and voice mail (Refer to Table 7 for more details on specific platform support).</li> </ul>

Feature	Benefit
Packet voice DSP module (PVDM) slots on motherboard	<ul style="list-style-type: none"> <li>• Slots for Cisco PVDM2 Modules (DSP Modules) are integrated on the motherboard, freeing slots on the router for other services.</li> </ul>
Extension-voice-module (EVM) slot	<ul style="list-style-type: none"> <li>• The EVM supports additional voice services and density without consuming the network-module slot (Note: available only on Cisco 2821 and 2851).</li> </ul>

### Secure Networking—Feature and Benefits

The Cisco 2800 Series features enhanced security functionality as shown in Table 3. Integrated on the motherboard of every Cisco 2800 Series router is hardware-based encryption acceleration that offloads the encryption processes to provide greater IPsec throughput with less overhead for the router CPU when compared with software-based solutions. With the integration of optional VPN modules (for enhanced VPN tunnel count), Cisco IOS Software-based firewall, network access control, or content-engine network modules, Cisco offers the industry's most robust and adaptable security solution for branch-office routers.

Table 3. Secure Networking—Feature and Benefits

Feature	Benefit
Cisco IOS Software Firewall	<ul style="list-style-type: none"> <li>• Sophisticated security and policy enforcement provides features such as stateful, application-based filtering (context-based access control), per-user authentication and authorization, real-time alerts, transparent firewall, and IPv6 firewall.</li> </ul>
Onboard VPN encryption acceleration	<ul style="list-style-type: none"> <li>• The Cisco 2800 Series supports IPsec Digital Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES) 128, AES 192, and AES 256 cryptology without consuming an AIM slot.</li> </ul>
Network Admissions Control (NAC)	<ul style="list-style-type: none"> <li>• A Cisco Self-Defending Network initiative, NAC seeks to dramatically improve the ability of networks to identify, prevent, and adapt to threats by allowing network access only to compliant and trusted endpoint devices.</li> </ul>
Multiprotocol Label Switching (MPLS) VPN support	<ul style="list-style-type: none"> <li>• The Cisco 2800 Series supports specific provider edge functions plus a mechanism to extend customers' MPLS VPN networks out to the customer edge with virtual routing and forwarding (VRF) firewall and VRF IPsec. For details on the MPLS VPN support on the different versions of the Cisco 2800 Series, please check the feature navigator tool on <a href="http://www.cisco.com">www.cisco.com</a>.</li> </ul>
Onboard USB 1.1 port(s)	<ul style="list-style-type: none"> <li>• The USB port(s) will be used for future capabilities and will initially support secure token and flash memory</li> </ul>
AIM-based security acceleration	<ul style="list-style-type: none"> <li>• Support for an optional dedicated security AIM can deliver 2 to 3 times the performance of embedded encryption capabilities with Layer 3 compression.</li> </ul>
Intrusion Prevention System (IPS)	<ul style="list-style-type: none"> <li>• Flexible support is offered through Cisco IOS<sup>®</sup> Software or a high-performance intrusion-detection-system (IDS) network module.</li> <li>• The ability to load and enable selected IDS signatures in the same manner as Cisco IDS Sensor Appliances</li> </ul>
Cisco Easy VPN remote and server support	<ul style="list-style-type: none"> <li>• The Cisco 2800 Series eases administration and management of point-to-point VPNs by actively pushing new security policies from a single headend to remote sites.</li> </ul>
Dynamic Multipoint VPN (DMVPN)	<ul style="list-style-type: none"> <li>• DMVPN is a Cisco IOS Software solution for building IPsec + generic routing encapsulation (GRE) VPNs in an easy and scalable manner.</li> </ul>
URL filtering	<ul style="list-style-type: none"> <li>• URL filtering is available onboard with an optional content-engine network module or external with a PC server running the URL filtering software.</li> </ul>

Feature	Benefit
Cisco Router and Security Device Manager (SDM)	<ul style="list-style-type: none"> <li>This intuitive, easy-to-use, Web-based device-management tool is embedded within the Cisco IOS Software access routers; it can be accessed remotely for faster and easier deployment of Cisco routers for both WAN access and security features.</li> </ul>

#### IP Telephony Support—Features and Benefits

The Cisco 2800 Series allows network managers to provide scalable analog and digital telephony without investing in a one-time solution (refer to Table 4 for more detail), allowing enterprises greater control of their converged telephony needs. Using the voice and fax modules, the Cisco 2800 Series can be deployed for applications ranging from voice-over-IP (VoIP) and voice-over-Frame Relay (VoFR) transport to robust, centralized solutions using the Cisco Survivable Remote Site Telephony (SRST) solution or distributed call processing using Cisco Call Manager Express (CME). The architecture is highly scalable with the ability to support up to 12 T1/E1s trunks, 52 foreign-exchange-station (FXS) ports, or 36 foreign-exchange-office (FXO) ports concurrent with data routing and other services.

**Table 4.** IP Telephony Support—Features and Benefits

Feature	Benefit
IP phone support	<ul style="list-style-type: none"> <li>Optional support for Cisco in-line power distribution to Ethernet switch network modules and HWICs can be used to power Cisco IP phones.</li> </ul>
EVM module slots	<ul style="list-style-type: none"> <li>Extension Voice Module Slots, available only on the Cisco 2821 and Cisco 2851, provide support for the Cisco High-Density Analog and Digital Extension Module for Voice and Fax, providing support for up to 24 total voice and fax sessions without consuming a Network Module Slot.</li> </ul>
PVDM (DSP) slots on motherboard	<ul style="list-style-type: none"> <li>DSP (PVDM2) modules deliver support for analog and digital voice, conferencing, transcoding, and secure Real-Time Transport Protocol (RTP) applications.</li> </ul>
Integrated call processing	<ul style="list-style-type: none"> <li>Cisco CME is an optional solution embedded in Cisco IOS Software that provides call processing for Cisco IP phones. Cisco CME delivers telephony features similar to those that are commonly used by business users to meet the requirements of the small to medium-sized offices.</li> </ul>
Integrated voice mail	<ul style="list-style-type: none"> <li>Support for up to a 100 mailboxes using the Cisco Unity<sup>®</sup> Express voice messaging system is possible with the integration of an optional voice-mail AIM or network module.</li> </ul>
Broad range of voice interfaces	<ul style="list-style-type: none"> <li>Interfaces for local telephone, private branch exchange (PBX), and gateway connections include FXS; FXO; direct inward dialing (DID); ear and mouth (E&amp;M); Centralized Automated Message Accounting (CAMA); ISDN Basic Rate Interface (BRI); and T1, E1, and J1 with ISDN Primary Rate Interface (PRI); QSIG; and several additional channel-associated-signaling (CAS) signaling schemes.</li> </ul>
Support of Survivable Remote Site Telephony (SRST) Feature	<ul style="list-style-type: none"> <li>Branch offices can take advantage of centralized call control while cost-effectively providing local branch backup using SRST redundancy for IP telephony.</li> </ul>

#### Cost of Ownership and Ease of Use—Features and Benefits

The Cisco 2800 Series continues the heritage of offering versatility, integration, and power to branch offices. The Cisco 2800 Series offers many enhancements to help enable the support of multiple services in the branch office as shown in Table 5.

**Table 5.** Cost of Ownership and Ease of Use—Feature and Benefits

Feature	Benefit
Integrated channel service unit/data	<ul style="list-style-type: none"> <li>Consolidates typical communications equipment found in branch-office wiring closets into a</li> </ul>

Feature	Benefit
service unit (CSU/DSU), add/drop multiplexers, firewall, modem, compression, and encryption	single, compact unit; this space-saving solution provides better manageability
Optional network analysis module	<ul style="list-style-type: none"> <li>Provides application-level visibility into network traffic for troubleshooting, performance monitoring, capacity planning, and managing network-based services (Note: Cisco 2811, 2821, and 2851 only)</li> </ul>
Cisco IOS Software Warm Reboot	<ul style="list-style-type: none"> <li>Reduces system boot time, and decreases downtime caused by Cisco IOS Software reboots (Note: Cisco 2801 will support the Cisco IOS Software Warm Reboot at a later point in time)</li> </ul>
Enhanced Setup feature	<ul style="list-style-type: none"> <li>Optional setup wizard with context-sensitive questions guides the user through the router configuration process, allowing faster deployment</li> </ul>
CiscoWorks support	<ul style="list-style-type: none"> <li>Offers advanced management and configuration capabilities through a Web-based GUI</li> </ul>
Cisco AutoInstall	<ul style="list-style-type: none"> <li>Configures remote routers automatically across a WAN connection to save cost of sending technical staff to the remote site</li> </ul>

## SUMMARY AND CONCLUSION

As companies strive to lower the cost of running their network and increase the productivity of their end users with network applications, more intelligent branch-office solutions are required. The Cisco 2800 Series offers these solutions by providing enhanced performance and increased modular density to support multiple services at wire speed. The Cisco 2800 Series is designed to consolidate the functions of many separate devices into a single, compact package that can be managed remotely. Because the Cisco 2800 Series routers are modular devices, interface configurations are easily customized to accommodate a wide variety of network applications, such as branch-office data access, integrated switching, voice and data integration, dial access services, VPN access and firewall protection, business-class DSL, content networking, intrusion prevention, inter-VLAN routing, and serial device concentration. The Cisco 2800 Series provides customers with the industry's most flexible, adaptable infrastructure to meet both today's and tomorrow's business requirements for maximum investment protection.

## PRODUCT SPECIFICATIONS

Table 6. Chassis Specifications

Cisco 2800 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
<b>Product Architecture</b>				
DRAM	Default: 128 MB Maximum: 384 MB	Default: 256 MB Maximum: 760 MB	Default: 256 MB Maximum: 1 GB	
Compact Flash	Default: 64 MB Maximum: 128MB		Default: 64 MB Maximum: 256 MB	
Fixed USB 1.1 ports	1		2	
Onboard LAN ports		2-10/100		2-10/100/1000
Onboard AIM (internal) slot		2		

## Cisco IP Phone 7912G

As the market leader in IP telephony, Cisco continues to deliver unsurpassed end-to-end data and true voice-over-IP (VoIP) solutions, offering the most complete, stylish, and fully featured IP phone portfolio to enterprise and small to medium-size customers. Cisco IP phones provide unmatched levels of integrated business functionality and converged communications features beyond today's conventional voice systems.

Cisco IP phone products include pixel-based displays to bring productivity-enhancing applications to the phone, customization options that can be modified as needs change, and inline power support over Ethernet.

The Cisco IP Phone 7912G provides core business features and addresses the communication needs of a cubicle worker

who conducts low to medium telephone traffic. The Cisco IP Phone 7912G offers four dynamic soft keys that guide a user through call features and functions. The graphic capability of the display provides a rich user experience by providing calling information and intuitive access to features. In addition, XML applications deliver impressive applications and network data to the Cisco IP Phone 7912G display.

The Cisco IP Phone 7912G supports an integrated Ethernet switch, providing LAN connectivity to a colocated PC. In addition, the Cisco IP Phone 7912G supports inline power, which allows the phone to receive power over the LAN. This capability gives the network administrator centralized power control, translating into greater network availability. The combination of inline power and Ethernet switch support reduces cabling needs to a single wire to the desktop.

### Cisco IP Phone 7912G Features

The Cisco IP Phone 7912G is designed to be easy to use with conveniently placed features.

- Pixel-based display—A pixel-based display provides intuitive access to calling features.
- Four soft keys dynamically present calling options to the user. The scroll toggle bar allows easy movement through the displayed information.
- "Menu" key—This key allows users to quickly access information such as call logs and phone settings.





- The user can retrieve voice-mail messages.
- The user can display missed calls, outgoing calls that have been placed, and incoming calls that have been received.
- The user can set various preferences such as ring types and display contrast.
- “Hold” key—This lighted key provides users a red visual indication that they have placed a call on hold.
- A volume-control toggle provides easy decibel-level adjustments of the handset and ringer.
- The handset is hearing-aid compatible (meets American Disabilities Act [ADA] requirements).
- A single-position foot stand provides optimum display viewing and comfortable use of buttons and keys. The foot stand can be removed to allow wall mounting via mounting holes located on the base of the phone.
- XML Applications can be delivered to the display.

### **Calling Features**

The Cisco IP Phone 7912G is designed to grow with system capabilities. Features will keep pace with new changes via software updates to the phone Flash memory. Examples of currently available features include:

- Support of a single line or directory number
- Calling name and number display
- Call waiting
- Call forward
- Call transfer
- Three-way calling (conference)
- On-hook dialing, predialing, and off-hook dialing
- Redial
- Call hold
- Call monitor (speaker only, no microphone)
- “Messages” soft key that allows access to voicemail messages
- Four speed dials configurable at the Cisco CallManager

### **Network Features**

- Cisco Discovery Protocol
- Automatic IEEE 802.1q (virtual LAN [VLAN]) configuration
- G.711a, G.711u, and G.729ab audiocompression coders-decoders (codecs)
- Integrated Ethernet switch
- 10/100BASE-T Ethernet connection through an RJ-45 interface for LAN connectivity
- Software upgrade supported using a Trivial File Transfer Protocol (TFTP) server
- Provisioning of network parameters through Dynamic Host Configuration Protocol (DHCP)
- Voice activity detection, silence suppression, comfort-noise generation, and error concealment

### **Protocols Supported**

- Compatible with Cisco CallManager Version 3.3(2) and later, using the Skinny Client Control Protocol (SCCP) protocol
- SIP (RFC 2543)

### **Physical Specifications**

- Dimensions (H x W x D): 6.5 x 7 x 6 in. (20.3 x 17.67 x 15.2 cm)
- Weight: 1.9 lb (0.9 kg)

### **Power Supply**

- Inline power
- Power can also be supplied locally using an optional AC to 48-VDC power adapter (CP-PWR-CUBE), which requires one of the following country-specific cords:
  - CP-PWR-CORD-NA (North America)
  - CP-PWR-CORD-CE (Central Europe)
  - CP-PWR-CORD-UK (United Kingdom)
  - CP-PWR-CORD-AU (Australia)
  - CP-PWR-CORD-JP (Japan)
  - CP-PWR-CORD-AP (Asia Pacific)

### **Temperature**

- Operating temperature: 32 to 104 F (0 to 40 C)
- Relative humidity: 10 to 95% (noncondensing)
- Storage temperature: 14 to 140 F (-10 to 60 C)

### **Certification**

#### **Regulatory Compliance**

- CE Marking

#### **Safety**

- UL 60950
- CSA-C22.2 No. 60950
- EN 60950
- IEC 60950
- AS/NZS 3260
- TS 001





#### EMC

- FCC Part 15 (CFR 47) Class B
- ICES-003 Class B
- EN55022 Class B
- CISPR22 Class B
- AS/NZS 3548 Class B
- VCCI Class B
- EN55024
- EN50082-1
- EN 61000-3-2
- EN 61000-3-3
- EN 61000-6-1

#### Telecom

- FCC Part 68 (CFR 47) (HAC)

#### Service and Support

Cisco IP Communications services and support reduce the cost, time, and complexity associated with implementing a converged network. Cisco and its partners have designed and deployed some of today's largest and most complex IP communications

networks—meaning that they understand how to integrate an IP communications solution into your network. Cisco design tools and best practices ensure that the solution best fits your business needs from the start, eliminating costly redesigns and downtime. Cisco proven methods ensure a sound implementation that will deliver the functions and features you expect—on time. Support services include remote network operations, network management tools to administer the converged application and network infrastructure, and technical support services.

Through these services, your organization benefits from the experience gained by Cisco and its partners. Taking advantage of this valuable experience, you can create and maintain a resilient, converged network that will meet your business needs today—and in the future.

#### Ordering Information

Table 1 lists part numbers for the Cisco IP Phone 7912G and Cisco CallManager.

**Table 1** Part Numbers

Part Number	Description
CP-7912G	Cisco IP Phone 7912 hardware
SW-CCM-UL-7912	Station user license for Cisco CallManager
SW-SMH-UL-7912	Station user license for SIP


Cisco offers a standard one-year warranty. A Cisco SMARTnet<sup>®</sup> optional service agreement is available.

Cisco Systems, Inc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Page 4 of 5

## Cisco IP Phone 7940G



The second-generation Cisco IP phones bring state-of-the-art technology to voice communication solutions. Cisco Systems, the worldwide leader in networking for the Internet, now delivers new opportunities for rapid deployment of classic and New World voice applications by providing high-quality voice instruments that use IP transport technology. This allows for the consolidation of data and voice into a single network infrastructure, including a single cable plant, a single switched Ethernet fabric for campus or branch offices, and unified systems for operations, administration, and management (OAM) for data and voice.

The Cisco IP Phone is a standards-based communications appliance. The Cisco IP Phone 7940G is a second-generation, full-featured IP phone for low to medium traffic users who require a minimum of directory numbers. It provides two programmable line/feature buttons capable of four simultaneous calls and four interactive soft keys that guide a user through call features and functions. The Cisco IP Phone 7940G also has a large, pixel-based LCD display. The display provides features such as date and time, calling party name, calling party number, and digits dialed. The graphic capability of the display allows for the inclusion of present and future features.

Figure 1 Cisco IP Phone 7940G



## Features

The Cisco 7940G is dynamic and designed to grow with system capabilities. Features will keep pace with new changes via software updates to the phone's Flash memory. The phone provides several different accessibility methods, according to user preference. Various methods or paths include buttons, softkeys, a navigation key, and direct access with the use of corresponding digits. Each of the features below will have expanded capabilities in the future:

- *Messages*—The Cisco 7940G identifies incoming messages and categorizes them for users on the screen. This allows users to quickly and effectively return calls using direct dialback capability.
- *Directories*—The corporate directory integrates with the Lightweight Directory Access Protocol 3 (LDAP3) standard directory.
- *Settings*—The Settings feature key allows users to adjust display contrast and select a ringer tone and volume settings for all audio such as ringer, handset, headset, and speaker. Network Configuration preferences can also be set up. Network configuration is usually set up by the System Administrator. Configuration can either be auto or manually set up for Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), Cisco CallManager, and backup Cisco CallManagers.
- *Services*—The Cisco 7940G allows users to quickly access diverse information such as weather forecasts, stock prices, or any other Web-based information services configured by the system administrator. Using standards such as extensible markup language (XML), the Cisco IP Phone 7940G provides a portal to an ever-growing world of features and information destinations, displayed on the large screen.
- *Help*—The online help feature gives users information about the phone's keys, buttons, and features. The pixel display allows for greater flexibility of features and significantly expands the information viewed when using features such as Services, Information, Messages, and Directory. For example, the Directory button can show local and server-based directory information.

Cisco IP Phones feature high-quality, Polycom, full-duplex, speakerphone technology. They also include an easy-to-use speaker on/off button and microphone mute button. These buttons are lit when active.

The Cisco two-port Ethernet switch in each Cisco IP Phone allows for a direct connection to a 10/100BaseT Ethernet network via an RJ-45 interface with single LAN connectivity for both the phone and a co-located PC. The system administrator can designate separate virtual LANs (VLANs) (802.1Q) for the PC and Cisco IP phones.

A dedicated headset port eliminates the need for a separate amplifier when using a headset. This allows the handset to remain in its cradle, making headset use simpler. The Cisco IP Phone 7940G convenient volume control button provides easy decibel-level adjustments for the speakerphone, handset, headset, and ringer.

The footstand of the Cisco 7940G is adjustable from flat to 60 degrees to provide optimum display viewing and comfortable use of all buttons and keys.

The Cisco IP Phone 7940G can also receive power down the LAN from any of the new Cisco inline power-capable blades and boxes.

Masking of dual-tone multifrequency (DTMF) tones in speaker mode provide added security.

Other Cisco IP Phone 7940G features include:

- 24 user-adjustable ring tones
- A hearing-aid-compatible handset (meets American Disabilities Act [ADA] requirements)
- G.711 and G.729a audio compression
- H.323 and Microsoft NetMeeting compatibility
- An IP address assignment—DHCP client or statically configured
- Comfort noise generation and voice activity detection (VAD) programming on a system basis
- EIA/TIA RS-232 port for future add-on options such as line expansion, security access, and more

The phone also includes the following settings:

- Display contrast
- Ring type
- Network configuration and network status
- Call status



## Service and Support

Cisco AVVID (Architecture for Voice, Video and Integrated Data) support solutions are designed for one purpose—to ensure customer success by delivering a suite of proactive services. The award-winning Cisco internetworking service and support offerings provide presales network audit planning, design consulting, network implementation, operational support, and network optimization. Cisco interactive knowledge-transfer solutions enhance customer success by leveraging Cisco expertise and experience. By including service and support when purchasing Cisco AVVID products, customers can confidently deploy Cisco AVVID networks using Cisco expertise, experience, and resources.

## Specifications

- Download firmware changes from Cisco CallManager
- Dimensions: 8<sup>1</sup> x 10.5 x 6 in. (20.32 x 26.67 x 15.24 cm) (H x W x D)
- Phone weight: 3.5 lb (1.6 kg)
- Polycarbonate acrylonitrile butadiene styrene (ABS) plastic in textured dark gray color with silver bezel
- 48 VDC required, supplied locally at the desktop using an optional AC to DC power supply (CP-PWR-CUBE=)

Also requires one of the following country cords:

- CP-PWR-CORD-NA (North America)
- CP-PWR-CORD-CE (Central Europe)
- CP-PWR-CORD-UK (United Kingdom)
- CP-PWR-CORD-AU (Australia)
- CP-PWR-CORD-JP (Japan)
- CP-PWR-CORD-AP (Asia Pacific)

## Temperature

- Operating temperature: 32 to 104 F (0 to 40 C)
- Relative humidity: 10% to 95% (noncondensing)
- Storage temperature: 14 to 140 F (-10 to 60 C)

## Regulatory Compliance

- CE Marking

## Safety

- UL-1950
- EN 60950
- CSA-C22.2 No. 950
- IEC 60950
- AS/NZS 3260
- TS 001

## Electro-Magnetic Compatibility

- 47CFR Part 15 Class B
- ICES-003 Class B
- EN55022 Class B
- CISPR22 Class B
- AS/NZ 3548 Class B
- VCCI Class B
- EN55024
- CE Marking

## Telecom

- FCC CFR47, Part 68 (HAC)
- IC CS-03

1. The footstand is adjustable from flat to a maximum angle of 60 degrees. In the flat position (for wall mounting) the height of the phone is 4.25 inches. In the maximum upright position on a desk, the phone is 8 inches.

## Cisco IP Phone 7960G



The second-generation Cisco IP phones bring state-of-the-art technology to voice communication solutions. Cisco Systems, the worldwide leader in networking for the Internet, now delivers new opportunities for rapid deployment of classic and New World voice applications by providing high-quality voice instruments that use IP transport technology. This allows for the consolidation of data and voice into a single network infrastructure, including a single cable plant, a single switched Ethernet fabric for campus or branch offices, and unified systems for operations, administration, and management (OAM) for data and voice.

The Cisco IP Phone series is a standards-based communication appliance. The Cisco IP series phones can interoperate with IP telephony systems based on Cisco CallManager<sup>1</sup> technology, H.323, or Session Initiated Protocol (SIP) and, in the future, Media Gateway Control Protocol (MGCP), with system-initiated software updates. This multiprotocol capability is an industry first and provides investment protection and migration capability.

The Cisco IP Phone 7960G is a second-generation, full-featured IP phone primarily for manager and executive needs. It provides six programmable line/feature buttons and four interactive soft keys that guide a user through call features and functions. The Cisco IP Phone 7960G also features a large, pixel-based LCD display. The display provides features such as date and time, calling party name, calling party

number, and digits dialed. The graphic capability of the display allows for the inclusion of present and future features.

Figure 1 Cisco IP Phone 7960G



1. Version 3.0 or higher is required.

## Features

The Cisco 7960G is dynamic and designed to grow with system capabilities. Features will keep pace with new changes via software updates to the phone's flash memory. The phone provides many accessibility methods according to user preference. Various methods or paths include buttons, softkeys, a navigation key, and direct access with the use of corresponding digits. Each of the features below will have expanded capabilities in the future:

- **Messages**—The Cisco IP Phone 7960G identifies incoming messages and categorizes them for users on the screen. This allows users to quickly and effectively return calls using direct dial-back capability.
- **Directories**—The corporate directory integrates with the Lightweight Directory Access Protocol (LDAP3) standard directory.
- **Settings**—The Settings feature key allows the user to adjust display contrast and select a ringer tone and volume settings for all audio such as ringer, headset, headset, and speaker. Network Configuration preferences can also be set up. Network configuration is usually set up by the System Administrator. Configuration can either be automatic or manually set up for Dynamic Host Control Protocol (DHCP), Trivial File Transfer Protocol (TFTP), CallManager, and backup CallManagers.
- **Services**—The Cisco 7960G allows users to quickly access diverse information such as weather, stocks, quote of the day or any Web-based information using extensible markup language (XML) to provide a portal to an ever-growing world of features and information.
- **Help**—The online help feature gives users information about the phone's keys, buttons, and features. The pixel display allows for greater flexibility of features and significantly expands the information viewed when using features such as Services, Information, Messages, and Directory. For example, the Directory button can show local and server-based directory information.

The Cisco IP Phone 7960G features high-quality, Polycom, full-duplex speakerphone technology. It also includes an easy-to-use speaker on/off button and microphone mute buttons. These buttons are lit when active.

The internal Cisco two-port Ethernet switch allows for a direct connection to a 10/100BaseT<sub>x</sub> Ethernet network via an RJ-45 interface with single LAN connectivity for both the phone and a co-located PC. The system administrator can designate separate virtual LANs (VLANs) (802.1Q) for the PC and Cisco IP Phones.

A dedicated headset port eliminates the need for a separate amplifier when using a headset. This allows the headset to remain in its cradle, making headset use simpler. The Cisco IP phone's convenient volume control button provides for easy decibel-level adjustments for the speakerphone, headset, headset, and ringer.

The footstand of the Cisco 7960G is adjustable from flat to 60 degrees to provide optimum display viewing and comfortable use of all buttons and keys. The Cisco IP Phone 7960G can also receive power down the LAN from any of the new Cisco inline power-capable blades and boxes.

For added security, the audible dual-tone multifrequency (DTMF) tones are masked when the speakerphone mode is used.

Other Cisco IP Phone 7960G features include:

- 24+ user-adjustable ring tones
- A hearing-aid-compatible handset (meets American Disabilities Act [ADA] requirements)
- G.711 and G.729a audio compression
- H.323 and Microsoft NetMeeting compatibility
- An IP address assignment—DHCP client or statically configured
- Comfort noise generation and voice activity detection (VAD) programming on a system basis
- EIA/TIA RS-232 port for future add-on options such as line expansion, security access, and more.

The phone also includes the following settings:

- Display contrast



- Ring type
- Network configuration
- Call status

### Service and Support

Cisco AVVID (Architecture for Voice, Video and Integrated Data) support solutions are designed for one purpose—to ensure customer success by delivering a suite of proactive services. The award-winning Cisco internetworking service and support offerings provide presales network audit planning, design consulting, network implementation, operational support, and network optimization. Cisco interactive knowledge-transfer solutions enhance customer success by leveraging Cisco expertise and experience. By including service and support when purchasing Cisco AVVID products, customers can confidently deploy Cisco AVVID networks using Cisco expertise, experience, and resources.

### Specifications

- Download firmware changes from Cisco CallManager
- Dimensions: 8<sup>2</sup> x 10.5 x 6 in. (20.32 x 26.67 x 15.24 cm) (H x W x D)
- Phone weight: 3.5 lb (1.6 kg)
- Polycarbonate acrylonitrile butadiene styrene (ABS) plastic in textured dark gray color with silver bezel
- 48 VDC required, supplied locally at the desktop using an optional AC to DC power supply (CP-PWR-CUBE=)

Also requires one of the following country cords:

- CP-PWR-CORD-NA (North America)
- CP-PWR-CORD-CE (Central Europe)
- CP-PWR-CORD-UK (United Kingdom)
- CP-PWR-CORD-AU (Australia)

- CP-PWR-CORD-JP (Japan)
- CP-PWR-CORD-AP (Asia Pacific)

### Temperature

- Operating temperature: 32 to 104 F (0 to 40 C)
- Relative humidity: 10 percent to 95 percent (noncondensing)
- Storage temperature: 14 to 140 F (-10 to 60 C)

### Certification

#### Regulatory Compliance

- CE Marking

#### Safety

- UL-1950
- EN 60950
- CSA-C22.2 No. 950
- IEC 60950
- AS/NZS 3260
- TS 001

#### Electro-Magnetic Compatibility

- 47CFR Part 15 Class B
- ICES-003 Class B
- EN55022 Class B
- CISPR22 Class B
- AS/NZ 3548 Class B
- VCCI Class B
- EN55024

#### Telecom

- FCC CFR47, Part 68
- IC CS-03

2. The footstand is adjustable from flat to a maximum angle of 60 degrees. In the flat position (for wall mounting) the height of the phone is 4.25 inches. In the maximum upright position on a desk, the phone is 8 inches.

## Cisco IP Conference Station 7936

The Cisco® IP Phone family provides industry-leading levels of integrated business functionality and converged communications features beyond today's conventional voice systems—surpassing competitive offerings. Cisco Systems® continues to deliver one of the industry's best end-to-end data and true voice over IP (VoIP) solutions, offering the most complete, stylish, and feature-rich IP phones to enterprise and small to midsize customers.

The new Cisco IP Conference Station 7936 combines state-of-the-art speakerphone conferencing technologies with award-winning Cisco voice communication technologies. The net result is a conference room phone that offers superior voice and microphone quality, with simplified wiring and administrative cost benefits. A full-featured, IP-based, hands-free conference station, the new Cisco IP Conference Station 7936 is designed for use on desktops, conference rooms, and in executive suites.

The Cisco IP Conference Station 7936 offers improvements over the existing Cisco IP Conference Station 7935 with external microphone ports, optional external microphone kit, newly audio-tuned speaker

grill, and a new backlit liquid crystal display (LCD) display. The optional microphone kit includes two microphones with six-foot cords. This places microphones across a 12-foot area, effectively expanding a suggested conference room size of 20 feet by 30 feet. The new backlit LCD display improves visibility in low light conditions. The display font size is also adjustable for improved distant viewing.


The Cisco IP Conference Station 7936 easily joins a Cisco Catalyst® 10/100 Ethernet switch port with a Cisco RJ-45 cable connection, and configures itself to the IP network via the Dynamic Host Control Protocol (DHCP).

The Cisco IP Conference Station 7936 offers exceptional voice quality—virtually eliminating echoes, reverberations, and truncated words to help deliver a more natural conversation. It features superb sound quality with a digitally tuned speaker and three microphones that minimize background noise, allowing conference participants to move around the room while speaking. Connecting two optional extension microphones to the base unit enables both voice coverage for larger rooms and enhanced speaker volume output.

Figure 1  
Cisco IP Conference  
Station 7936







In addition to the regular telephony keypad, the Cisco IP Conference Station 7936 provides three soft keys and menu navigation keys that guide a user through call features and functions. The Cisco IP Conference Station 7936 also features a pixel-based LCD display, which exhibits the date and time, calling party name, calling party number, digits dialed, and feature and line status.

### **Cisco IP Conference Station 7936 Features**

The Cisco IP Conference Station 7936 provides the following:

- Standard business telephony features—Includes call hold, call transfer, call release, mute, conference ("ad-hoc" and "meet-me" conferencing, park, and pick up.
- Feature updates—Facilitates Cisco CallManager software upgrades along with advances in system capabilities.
- Full-duplex operation—Permits natural, two-way conversations without clipping or distortion; the system automatically adapts to changes in the acoustic conditions of the room using state-of-the-art acoustic technology.
- Integrated keypad—Eliminates the need to receive and place calls on a separate telephone.
- 360-degree room coverage—A powerful, digitally-tuned custom speaker and three sensitive microphones provide uniform coverage of small-to-midsize conference rooms or offices.
- Single cable design—Reduces clutter on the tabletop by combining a single cable from the power interface module (PIM) cable with network and power.
- Simple to install—Configures easily with Cisco CallManager.
- Freedom from special end-user training—Works like a regular telephone.
- Dynamic Host Configuration Protocol (DHCP) for auto address configuration to the IP network
- Cisco Discovery Protocol for Cisco IP Conference Station 7936 to Cisco Catalyst switch port discovery—Provides powerful protocol for E911 services, phone tracking, and asset/theft management.
- Auto configuration of phone number, software images, and personalized settings—Simplifies installation, reconfiguration, and future feature enhancements such as Web browsing capabilities.
- The Cisco IP Conference Station 7936 uses a single Cisco 10/100BaseTx Ethernet LAN connection to the network via a Cisco RJ-45 cable interface.

The Cisco IP Conference Station 7936 also features:

- Convenient volume control buttons
- Five user-adjustable ring tones
- G.711 (A-law and -Law) and G.729a audio compression
- IP address assignment —DHCP client or statically configured
- Comfort noise generation and voice activity detection
- Web and LCD-based configuration
- Local 20 entry directory

This product also features settings for:

- Display contrast
- Ring type
- Network configuration
- Call status



## **Cisco IP Conference Station 7936 Specifications**

- Audio bandwidth: 300 to 3500 Hz
- RMC: Speaker volume: 86.5 dB peak volume at 0.5 meters
- Recommended room conditions: Closed offices and conference rooms up to 20 feet by 30 feet in dimension without major glass or ceramic surfaces and with normal background air-conditioning noise. (Significant echoes need to be less than one-eighth of a second in duration.)
- Firmware updates: Download from Cisco CallManager
- Dimensions: 12.5 x 12 x 2.25 in. (31.5 x 30.2 x 5.7 cm) (H x W x D)
- Phone weight: 1.75 lb (0.8 kg)
- Covering: Acrylonitrile butadiene styrene (ABS) plastic in textured Cisco gray color
- Power interface: PIM provides power interface and network connection

A universal power supply is included with the Cisco IP Conference Station 7936; however, the Cisco IP Conference Station 7936 requires one of the following country cords:

- CP-PWR-CORD-NA (North America)
- CP-PWR-CORD-CE (Central Europe)
- CP-PWR-CORD-UK (United Kingdom)
- CP-PWR-CORD-AU (Australia)
- CP-PWR-CORD-JP (Japan)
- CP-PWR-CORD-AP (Asia Pacific)
- CP-PWR-CORD-AR (Argentina)
- CP-PWR-CORD-SW (Sweden)

### **Temperature**

- Operating temperature: 32 to 104 F (0 to 40 C)
- Relative humidity: 20 percent to 85 percent (non-condensing)
- Storage temperature: -22 to 131 F (-30 to 55 C)

### **Regulatory Compliance**

#### **Safety**

- UL1950
- CSA C22.2, No. 950
- EN60950
- IEC60950
- AS/NZS3260

## EMC

- FCC (47 CFR Part 15) Class B
- ICES-003 Class B
- EN55022 Class B
- CISPR22 Class B
- AS/NZS 3548 Class
- VCCI Class B
- EN55024

## Service and Support

Cisco AVVID (Architecture for Voice, Video and Integrated Data) support solutions help to ensure customer success by delivering a suite of proactive services. The award-winning Cisco internetworking service and support offerings provide presales network audit planning, design consulting, network implementation, operational support, and network optimization. Cisco interactive knowledge-transfer solutions enhance customer success by taking advantage of Cisco expertise and experience. By including service and support when purchasing Cisco AVVID products, customers can confidently deploy Cisco AVVID networks utilizing Cisco expertise, experience, and resources.

## Ordering Information

Part Number	Description
CP-7936	Includes Cisco IP Conference Station 7936 and CP-7936-PWR-CS-KIT
SW-CCM-7936-UL	Station user license. Required, one per Cisco IP Conference Station 7936 unit
CP-7936-MIC-KIT=	Two (2) optional outboard microphones for use with Cisco IP Conference Station 7936
CP-7936-PWR-KIT=	Replacement power kit. Includes power cube, PIM, and cables. This power kit also fits the Cisco IP Conference Station 7935. Note: Country-specific power cord not included
CP-PWR-CORD-NA=	Country-specific power cord for North America
CP-PWR-CORD-CE=	Country-specific power cord for Central Europe
CP-PWR-CORD-UK=	Country-specific power cord for United Kingdom
CP-PWR-CORD-JP=	Country-specific power cord for Japan
CP-PWR-CORD-AP=	Country-specific power cord for Asia Pacific
CP-PWR-CORD-AU=	Country-specific power cord for Australia
CP-PWR-CORD-AR=	Country-specific power cord for Argentina
CP-PWR-CORD-SW=	Country-specific power cord for Sweden

## Cisco IP Communicator

Cisco® IP Phones provide unmatched levels of integrated business capabilities and converged communications features that go beyond today's conventional voice systems and surpass competitive offerings as well. Cisco Systems® delivers unparalleled end-to-end data and IP Telephony solutions, offering the most complete, full-featured IP Phone portfolio to enterprise and small- and mid-sized-business customers.

Cisco IP Communicator—a software-based application that delivers enhanced telephony support through personal computers—features the latest technology and advancements available with VoIP today. This application endows computers with the functionality of IP Phones, providing high-quality voice calls on the road, in the office, or from wherever users may have access to the corporate network.

Cisco IP Communicator is designed to meet diverse customer needs as a supplemental telephone when traveling, a telecommuting device, or a primary desktop telephone. When using Cisco IP Communicator remotely, users

aren't just taking their office extension with them, they also have access to the same familiar phone services they have in the office.

Cisco IP Communicator uses Cisco CallManager call processing system to provide advanced telephony features and VoIP capabilities. When registered to Cisco CallManager system, Cisco IP Communicator has the features and functionality of a full-featured Cisco IP Phone, including the ability to transfer calls, forward calls, and conference additional participants to an existing call. This also means that system administrators can provision Cisco IP Communicator as they would any other Cisco IP Phone, greatly simplifying IP Phone management.

This solution also enables customers and developers to deliver more innovative and productivity-enhancing Extensible Markup Language (XML)-based applications to the display. Access to eight telephone lines (or a combination of lines and direct access to telephony features) is included.

Cisco IP Communicator is a dynamic solution that is designed to grow with new system capabilities. Features will keep pace with new changes via automatic software updates.



Cisco IP Communicator

## Cisco IP Communicator Features

Cisco IP Communicator is intuitively-designed, easy to use, and delivers convenient access to a host of features:

- **Eight Line Keys**—These keys provide telephone lines and direct access to telephony features.
- **Five Softkeys**—These keys dynamically present call feature options to the user.
- **Messages**—This key provides direct access to voice-mail messages.
- **Directories**—Cisco IP Communicator identifies incoming messages and categorizes them on the screen. This allows users to return calls quickly and effectively using direct dial-back capability. The corporate directory integrates with the Lightweight Directory Access Protocol 3 (LDAP3) standard directory.
- **Settings**—This key allows users to select from a large number of ringer sounds and background images.
- **Services**—Cisco IP Communicator allows users to quickly access diverse information such as weather, stocks, quote of the day, or any other Web-based information. The phone uses XML to provide a portal to an ever-growing world of features and information.
- **Help**—The online help feature gives users information about the phone's keys, buttons, and features.

## Cisco IP Communicator Modes

Cisco IP Communicator offers handset, headset, and high-quality speakerphone modes.

- **Headset Mode**—In this mode, Cisco IP Communicator offers the highest quality voice communications capabilities.
- **Handset Mode**—Cisco IP Communicator interoperates with third-party USB telephony handsets.
- **Speakerphone Mode**—Cisco IP Communicator converts a computer into a half-duplex, hands-free speakerphone.

## Calling Features

Cisco IP Communicator is a dynamic solution that is designed to grow with new system capabilities. Features will keep pace with new changes via automatic software updates. A number of advanced features are currently available, including:

- Support of multiple lines or directory numbers
- Configurable speed dials
- Calling name and number display
- Call waiting
- Call forward
- Call transfer
- Three-way calling (conference)
- Park
- Pick-up
- Redial
- Call hold
- Barge

## High-Quality Audio

Cisco IP Communicator offers premium audio quality. Examples of audio features include:

Cisco Systems, Inc.

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Page 2 of 5

- Audio Tuning Wizard
- Advanced jitter buffer
- Echo suppression and noise cancellation
- Voice activity detection, silence suppression, and error concealment
- USB Human Interface Device (HID) support
- IP precedence (DSCP) audio priority

#### Additional Cisco IP Communicator Features

- More than 24 user-adjustable ring tones
- Auto-detection of Cisco VPN client
- Automated support for most VPN clients (including Microsoft PPTP client)
- Multiple display (skin) options:

#### Cisco IP Communicator Skin Options



Default skin



Additional skin option



Screen only view

#### Network Features

Cisco IP Communicator includes the following network features:

- Cisco Discovery Protocol for integration with Cisco Emergency Responder
- G.711a, G.711, G.729, and G.729a audio codecs
- Wideband audio codec
- Software upgrade supported using TFTP or HTTP
- Provisioning of network parameters through DHCP
- Compatible with Cisco CallManager Version 3.3(3) SR3 and later versions using the Skinny Client Control Protocol (SCCP)

Cisco Systems, Inc.

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Page 3 of 5



#### Minimum Computer Requirements

- Microsoft Windows 2000 Professional (SP3) or Windows XP (SP1)
- 450 MHz or higher Pentium III or compatible processor
- 128 MB RAM for Windows 2000 or 192 MB RAM for Windows XP
- 100 MB free disk space
- Non-ISA full-duplex sound card (integrated or PCI-based) or USB sound device
- Graphics card at 800x600x16bit or better
- 128 kbps network connection

#### Service and Support

Cisco IP Communications services and support reduce the cost, time, and complexity associated with implementing a converged network. Cisco and its partners have designed and deployed some of today's largest and most complex IP communications networks—meaning that they understand how to integrate an IP communications solution into any customer's network. Cisco design tools and best practices help ensure that the solution best fits specific business needs from the start, eliminating costly redesigns and downtime. Proven Cisco methods facilitate a sound implementation that will deliver the required functions and features—on time. Support services include remote network operations, network management tools to administer the converged application and network infrastructure, and technical support services.

Through these services, customers benefit from the experience gained by Cisco and its partners. Taking advantage of this valuable experience, customers can create and maintain a resilient, converged network to meet their business needs today—and in the future.

#### Ordering Information

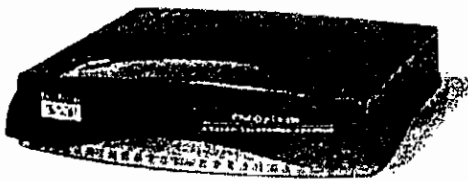
Table 1 lists part numbers for Cisco IP Communicator and Cisco CallManager.

Table 1 Part numbers for Cisco IP Communicator and Cisco CallManager

Description	Part Number
Cisco IP Communicator Software	SW-IPCOMM-E1
Station User License for Cisco CallManager	SW-CCM-UL-IPCOMM-E

# Cisco ATA 186 Analog Telephone Adaptor

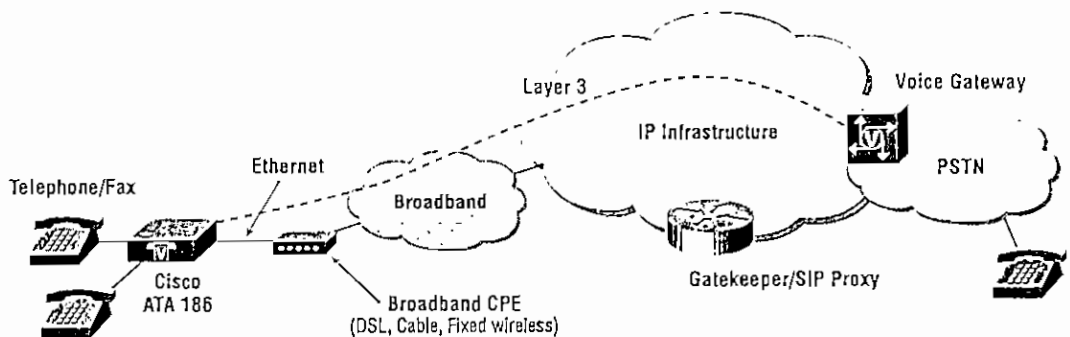
Enabling service providers to bring IP telephony to the residential market



The Cisco ATA 186 Analog Telephone Adaptor is a handset-to-Ethernet adaptor that interfaces regular analog phones with IP-based telephony networks. The Cisco ATA 186 is installed at the subscriber's premises and supports two voice ports, each with its own independent phone number. This adaptor takes advantage of broadband pipes being deployed through digital subscriber line (xDSL), fixed wireless, cable modems, and other Ethernet connections.

The Cisco ATA 186 is the ideal solution for service providers deploying IP telephony services in the residential market while taking advantage of the installed base of handsets. By deploying IP-based telephones as a second-line, service providers can now offer additional revenue-generating services for emerging telephony applications in their residential services portfolio. Service providers can also realize a rapid return on investment (ROI) by utilizing their existing networks and move to converged network architectures (see Figure 1). Thus, saving capital costs along with operational and administrative costs.

**Figure 1** Cisco ATA 186—Endpoint for an end-to-end broadband solution







## Cisco ATA 186 Features and Benefits

### Interfaces legacy telephones to IP-based networks

- Two voice ports support legacy (analog) touch-tone telephones
- RJ-45 connection to 10/100Base-T Ethernet hub/switch

### Flexible configuration and provisioning options

- Auto-provisioning with provisioning servers
- Automatic assignment of IP address, network route IP, and subnet mask via Dynamic Host Configuration Protocol (DHCP)
- Web configuration through built-in Web server
- Voice prompt configuration via touch-tone telephone keypad (IVR menu)
- Administration password to protect configuration and access
- Remote upgrades through network

### Clear, natural-sounding voice quality

- Advanced pre-processing to optimize full-duplex voice compression
- High performance line-echo cancellation eliminates noise and feedback

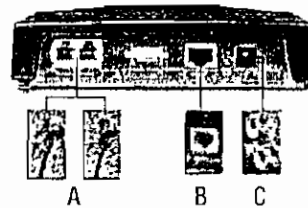
- Voice activity detection (VAD) saves bandwidth by delivering voice, not silence
- Regular telephone call experience with comfort noise generation (CNG) and virtual dial-tone
- Dynamic network monitoring to reduce jitter artifacts

### Supports standard protocols for interoperability and deployment flexibility

- H.323
- SIP

### Small form-factor design to fit in all environments

### System Requirements



- A** Regular analog, touch-tone telephones
- B** 10Base-T category-3 cable or better (access to an IP network)
- C** Power for AC/DC power adaptor

**Table 1** Cisco ATA 186 Software Specifications

Category	Specification
Control protocols	H.323 v.2 SIP RFC 2543 bis
Voice Codecs	G.729A (only one port at a time) <sup>1</sup> G.723.1 (both 5.3 kbps and 6.3 kbps operation) G.711A G.711
Provisioning	DHCP (RFC 2131) Web configuration via built-in Web server Voice prompt configuration via telephone keypad (IVR menu) Basic boot provisioning (TFTP Profiling) Dial plan provisioning
DTMF	DTMF tone detection and generation
Out-of-band DTMF	H.245 out-of-band DTMF (H.323) RFC 2833 AVT tones (SIP)



**Table 1** Cisco ATA 186 Software Specifications (Continued)

Category	Specification
<b>Transmission protocols</b>	TCP/UDP/IP
<b>Line echo cancellation</b>	One line echo canceller (LECs) for each port 8 ms echo length Non-linear echo suppression (ERL greater than 28 dB for $f = 300$ to 3400 Hz) Convergence time = 250 ms ERLE = 10 to 20 dB Double-talk detection
<b>Voice features</b>	VAD (silence suppression) CNG (comfort noise generation) Dynamic jitter buffer (adaptive and configurable)
<b>Fax</b>	G.711 fax pass-through (manual or automatic switching) <sup>2</sup> Fax answer tone detection

1. When using G.729A in simultaneous dual port operation, second port is limited to G.711

2. Silence suppression, echo cancellation, and call-waiting disabled

**Table 2** Cisco ATA 186 Physical Specifications

Category	Specification
<b>Dimensions</b>	6.5 x 6 x 1.5 in. (16.5 x 15.25 x 3.8 cm) (H x W x D)
<b>Weight</b>	15 oz (425 gm)
<b>Power</b>	
Power consumption	0.25 to 7.5 W (idle, maximum)
DC Input voltage	+5.0 VDC at 1.5 A maximum
Power adaptor	Universal AC/DC ~ 3.3 x 2.0 x 1.3 in (~8.5 x 5.0 x 3.2 cm) ~ 4.8 oz (135 gm) for the AC-input external power adaptor ~ 4 ft (1.2 m) DC cord ~ 6 ft (1.8 m) cord UL/CUL, CE agency approvals Class II transformer
<b>Physical interfaces</b>	
Ethernet	RJ-45 8-wire connector, IEEE 802.3 10Base-T standard
Analog Telephone	Two RJ-11 FXS voice ports
Power	5 VDC power connector
Ringer equivalence number (REN)	5 REN per RJ-11 FXS port
Indicators	Function button with integrated status indicator Activity LED indicating network activity
Operating temperature	32 to 122 F (0 to 50 C)
Storage temperature	-22 to 149 F (-30 to 65 C)
Relative humidity	10 to 90% non-condensing, operating and non-operating/storage



**Table 3** Cisco ATA 186 Ringing Characteristics

Category	Specification
<b>Ring load (per RJ-11 FXS port)</b>	<b>Maximum distance</b>
5 REN	200 ft (61 m)
4 REN	1000 ft (305 m)
3 REN	1700 ft (518 m)
2 REN	2500 ft (762 m)
1 REN	3200 ft (975 m)
<b>On-hook/off-hook characteristics</b>	
On-hook voltage (tip/ring)	-50 V
Off-hook current	27 mA
RJ-11 FXS port terminating Impedance option	600 ohms resistive or 270 ohm + 750 ohm // 150 nF complex Impedance
<b>SLIC (Tip/ring interfaces for each RJ-11 FXS port)</b>	
Ring voltage	40 to 42 V <sub>RMS</sub> (balanced ringing only)
Ring frequency	25 Hz
Ring waveform	Trapezoidal with 1.2 to 1.6 crest factor

**Table 4** Cisco ATA 186 Regulatory and Standard Compliance

Category	Specification
<b>Agency approvals</b>	UL/C-UL FCC (Declaration of Conformity) European Union, CE mark (Declaration of Conformity) Industry Canada (Declaration of Conformity) ACA (Declaration of Conformity) VCCI (Declaration of Conformity)
<b>Safety standards</b>	UL60950 CAN/CSA-C22.2 No. 60950-00 IEC 60950 (Second Edition with Amendments 1, 2, 3, and 4) EN60950:1922 (with Amendments 1, 2, 3, 4, and 11) AS/NZS 3260:1963 (with Amendments 1, 2, 3, and 4) TS001:1997
<b>Emissions</b>	CFR 47 Part 15 Class B 1997 EN55024, EN50082-1 EN55022/CISPR22 Class B VCCI Class B AS/NZS 3548:1992 Class B ICES-003 (Issue 2, Class B, April 1997)
<b>Immunity</b>	EN50082-1 including the following EN61000-4-2, ESD EN61000-4-3, Radiated Immunity EN61000-4-4, Burst Transients EN61000-4-5, Surge EN61000-4-6, Injected RF EN61000-4-11, Dips and Sags

## CiscoWorks **Small Network Management Solution** Version 1.5

CiscoWorks Small Network Management Solution (SNMS) is an end-to-end network management solution from Cisco Systems. It is ideal for small networks which might include two or three branch offices. CiscoWorks SNMS is a comprehensive, cost-effective, and user-friendly solution that provides advanced monitoring, and configuration capabilities. It also provides management capabilities that simplify network administration.

Built upon popular Internet-based standards, CiscoWorks SNMS enables network operators to more efficiently and effectively manage the network through a simplified browser-based interface that can be accessed anytime from anywhere within the network. CiscoWorks SNMS provides tools that make the job of configuring, monitoring, and troubleshooting routers, switches and other business applications, quicker and helps reduce the likelihood of human errors. Businesses that use CiscoWorks SNMS can enjoy the twin advantages of decreasing downtime (based on the monitoring and troubleshooting tools) and the ability to easily roll out changes in the network (based on the configurations tools).

**Figure 1**  
 Typical Small Network Deployment

- Topology  
 80% Small Campus,  
 Single Building/Site  
 20% Small WAN (Couple  
 of Locations, Limited VPN)
- Device Mix (Example)  
 35 Switches  
 3 Routers  
 2-3 Firewalls  
 5-10 Servers
- 500 PCs

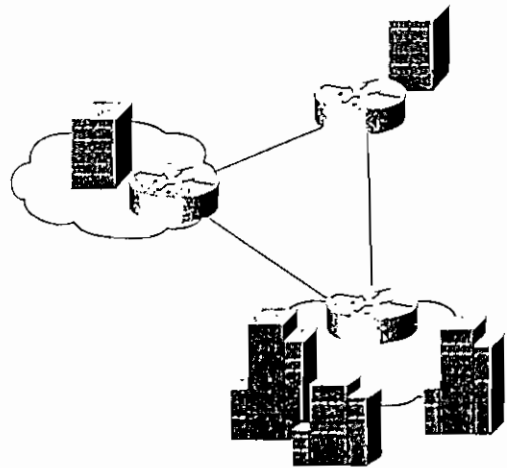


Figure 1 shows a typical Small Network deployment with a couple of remote locations and a head office that has a larger network setup. Today's business challenges for such networks go beyond high uptime and quick troubleshooting capabilities. The tools should help not only in the regular network management tasks, but, they should also help in configuring/re-configuring the various changes in the network. Typically, the administrators of small networks, are required to monitor and manage every aspect of the infrastructure including,

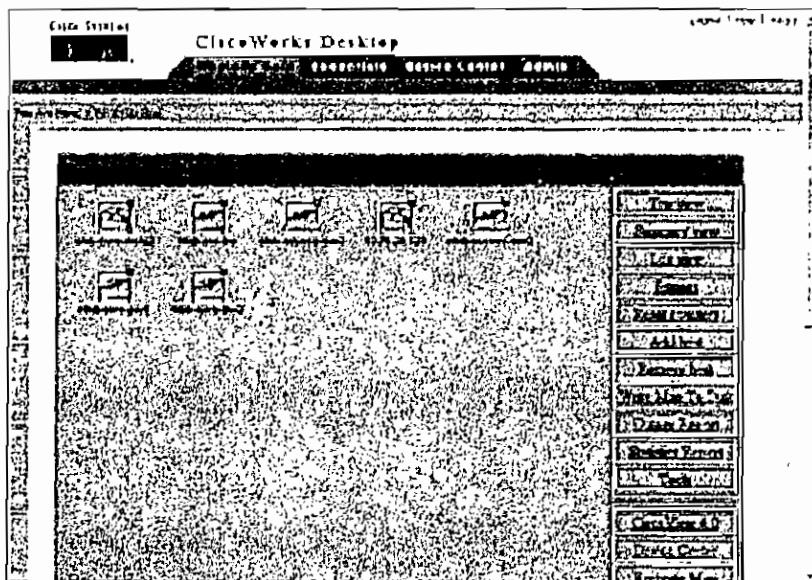


periodically updating the software images running on local and remote devices, implementing configurations changes, optimizing network utilization, deploying policies, and capacity planning. This is a challenging task, especially with the constraints on resources which most organizations face.

CiscoWorks SNMS enables customers to monitor, manage, and deploy new network devices and get them up and running in a very short time. Some of the features infrastructure for small network deployments, are the following:

- Easy to use and access via a Web Browser, CiscoWorks SNMS has a simple, easy-to-learn graphical interface. It provides multiple applications that can be launched from a well-organized, tab-oriented interface. CiscoWorks SNMS provides an elegant security model that allows multiple level access rights. Users can access all SNMS functionality via a web browser, allowing them flexibility and remote access.

Figure 2



- Device lifecycle management

CiscoWorks SNMS provides a comprehensive set of tools for device lifecycle management encompassing both hardware and software elements. Initial configuration is only a small part of a series of ongoing tasks that need to be done, so as to make the device work efficiently. For example the need to change passwords and community strings is regular event. Using CiscoWorks SNMS this task can be automated. CiscoWorks SNMS also provides tools to track changes in the configuration of network devices. As the network grows, new features and updates have to be incorporated in the device operating system, such as Cisco IOS / Cisco Catalyst OS. Often these updates become necessary to ensure the security of the network.

- Integrated Infrastructure Management

CiscoWorks SNMS provides a single window to the network that not only includes Cisco network devices, but includes PCs, servers, and applications. This integrated approach gives the common infrastructure to be used for both monitoring and managing non-network elements. Users do not have to switch between several disparate applications to manage network operations.

### CiscoWorks SNMS Functions

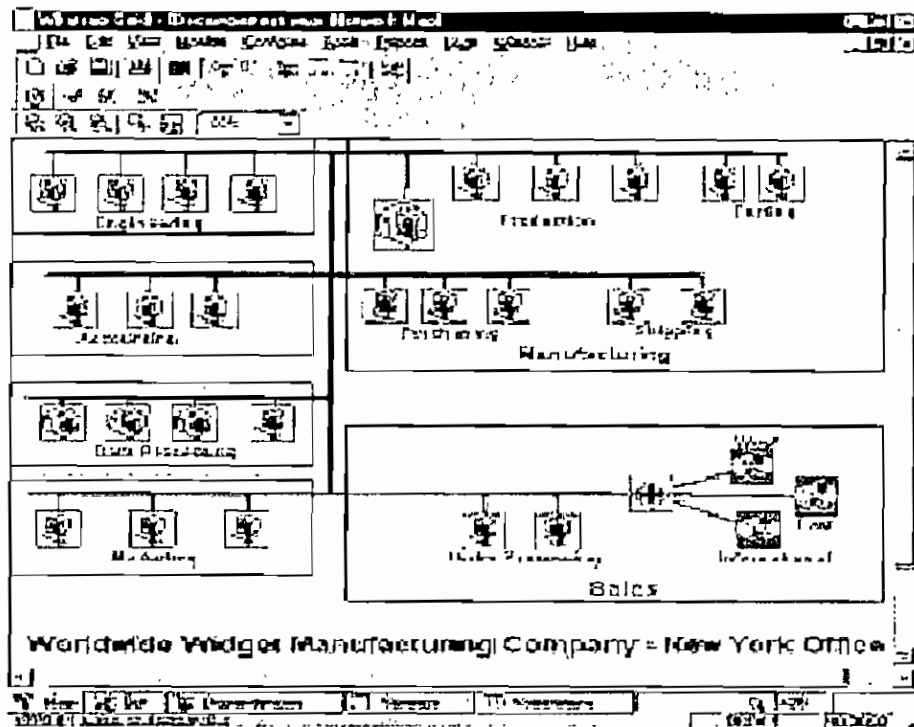
The functionality of CiscoWorks SNMS can be categorized under three functional areas:

- Network Discovery and Policy Management
- Device Configuration
- Device Management

Network discovery and policy management is done using WhatsUp Gold. Device configuration tasks are taken care of by CiscoView, and Device Management is done using RME.

Brief discussions on these topics are given below along with screenshots.

Figure 3  
WhatsUp Gold—Network Discovery



### Network Discovery

CiscoWorks SNMS discovers SNMP-enabled elements in the network and builds a topology map using WhatsUp Gold. WhatsUp Gold, from Ipswitch, has powerful features that work well for both network elements and other IT assets such as, servers, applications and PCs. SNMS leverages these capabilities to manage network elements and add more value. WhatsUp Gold is integrated very closely with the other CiscoWorks SNMS components, and device data is shared. Users may cross launch WhatsUp Gold from within any part of SNMS application.

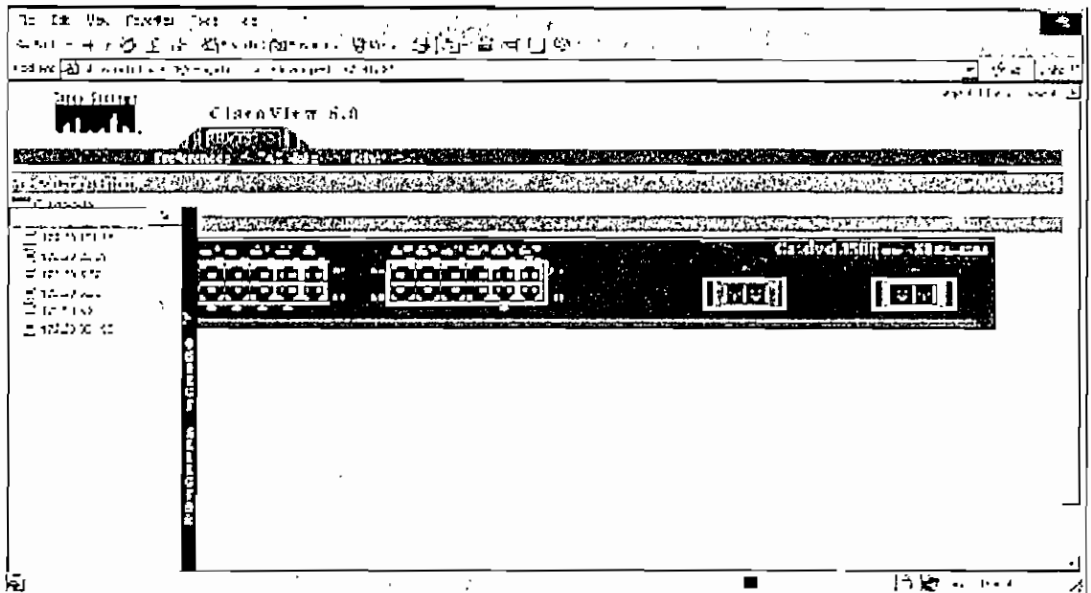


The topology maps, discovered by WhatsUp Gold, can be organized based on logical or physical entities. Users can use either the GUI version of the application or the web version. Other features of WhatsUp Gold include:

- User-defined device maps
- Performance monitoring of devices and historical performance data export
- Update of device details into RME
- Net tools to troubleshoot device
- Web-based reporting
- Event notification and filtering capabilities

### Device Configuration

Figure 4  
CiscoView: Device Configuration tool



The CiscoView device manager is the most widely-deployed device management software application provided by Cisco Systems. Being web-based, CiscoView allows ubiquitous access from a standard browser or over the network. CiscoView web-based management helps network management by displaying a physical view of Cisco devices and color-coding device ports for at-a-glance port status, allowing users to quickly grasp vital information. CiscoView provides dynamic status, device monitoring, and comprehensive configuration information for Cisco internetworking products (routers, switches, and access products). CiscoView features include:

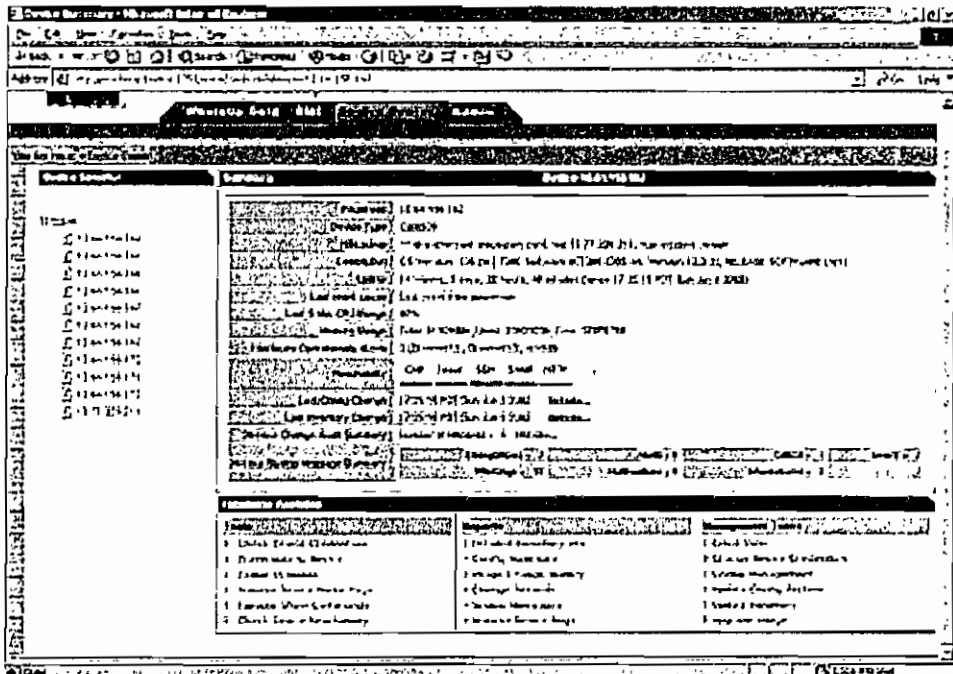
- Web-based displays of Cisco products from a single location, giving network managers a complete view of Cisco products without physically checking each device (see Figure 2)
- A continuously updated physical view of routers, hubs, switches, or access servers in a network
- Real-time monitoring and tracking of key information and data relating to device performance, traffic, and environment, with metrics such as utilization percentage, frames transmitted and received, errors, and a variety of other device-specific indicators

- The ability to modify device configurations across router, switch, and access server products.
- The ability to access the support for existing and new Cisco devices via the Web-based Package Support Updater (PSU), without having to purchase and install new versions of CiscoView

### Device Management

The heart of the Device Management module is CiscoWorks Resource Manager Essentials (RME). As the name suggests, this is one function an IT administrator cannot live without. CiscoWorks RME serves many purposes; it can be used as a troubleshooting tool, a repository of configuration details, an asset management database, and a platform to automate multiple routine activities.

Figure 5  
Device Center: Trouble Shooting Dashboard



CiscoWorks SNMS provides operational management for the network, allowing network managers to:

- Quickly build a complete network inventory
- Manage device credentials information
- Monitor and report hardware, software, configuration, and inventory changes
- Manage and deploy configuration changes and software image updates to multiple devices
- Monitor and troubleshoot critical LAN and WAN resources.
- Quickly identify device upgrade requirements to run specific Cisco IOS or Cisco Catalyst OS versions.
- Isolate problems by running customized Syslog reports.





## Licensing

CiscoWorks SNMS has been optimized to work with small networks. Some applications within CiscoWorks SNMS have restrictions on the number of devices they can manage for that application. As explained earlier, a small network comprises of a few routers, switches, and a significant number of PCs. The WhatsUp Gold application, which is used for topology mapping, monitoring and escalation can be used for any number of devices. WhatsUp Gold gives the user substantial flexibility to monitor PC-related resources. Cisco View and RME are primarily used for managing Cisco devices like routers and switches. These two applications can work with a maximum of 40 Cisco devices on the network. Networks that have more than 40 Cisco devices can choose to use LAN Management Solution (LMS).

## Server Specifications (Minimum Requirements)

### Server Hardware

- PC-compatible computer with 1 GHz or faster Pentium processor
- CD-ROM drive
- 100Base-T or faster connection
- 512 MB RAM
- 9 GB available disk drive space
- 1 GB virtual memory

### Server Operating System

- Windows 2000 Professional, Server, and Advanced Server (Service Pack 3)

**Note:** Support for Advanced Server requires that Terminal Services be turned off.

## Client Requirements

### Hardware

- PC-compatible computer with 1 GHz or faster Pentium processor

### Client Operating System

- Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP SP1 with Microsoft VM.

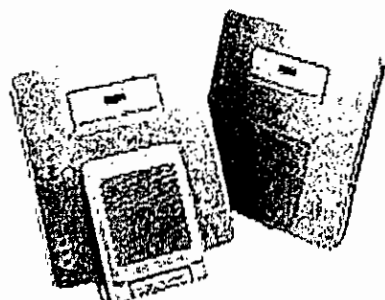
### Client Browser

- Internet Explorer 6.0 Service Pack 1, on Windows operating systems

## Service and Support

CiscoWorks products are eligible for coverage under the Cisco Software Application Service (SAS) program. This service program offers customers contract-based 24-hour access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and software maintenance updates. A SAS contract ensures that customers have easy access to the information and services needed to stay current with newly supported device packages, patches, and minor updates. For further information about service and support offerings, contact your local sales office.

## CISCO AIRONET 1200 SERIES ACCESS POINT



### PRODUCT OVERVIEW

The Cisco Aironet<sup>®</sup> 1200 Series IEEE 802.11 a/b/g Access Point sets the enterprise standard for high-performance, secure, manageable, and flexible wireless LANs (WLANs). The modular design of the Cisco Aironet 1200 allows single or dual radio configuration for up to 54 Mbps connectivity in both the 2.4 and 5 GHz bands and is fully compliant with IEEE 802.11a, 802.11b, and 802.11g standards. Providing numerous configuration and upgrade options, the Cisco Aironet 1200 Series supports a variety of clients in mixed frequency and mixed throughput environments. Whether configured for single 802.11a coverage, single 802.11g coverage, 802.11b/g coverage or for tri-mode 802.11a/b/g coverage, the Cisco Aironet 1200 offers the greatest flexibility and investment protection, allowing network administrators to deploy a wireless network optimized for their particular application.

The Cisco Aironet 1200 takes advantage of Cisco IOS<sup>®</sup> Software for ease-of-use and familiarity and is a key component of the Cisco Structured Wireless-Aware Network (SWAN), a comprehensive framework that delivers an integrated, end-to-end wired and wireless network. The Cisco Aironet 1200 Series provides customers with maximum freedom and flexibility, enabling constant connection to all network resources from virtually anywhere wireless access is deployed (Figure 1).

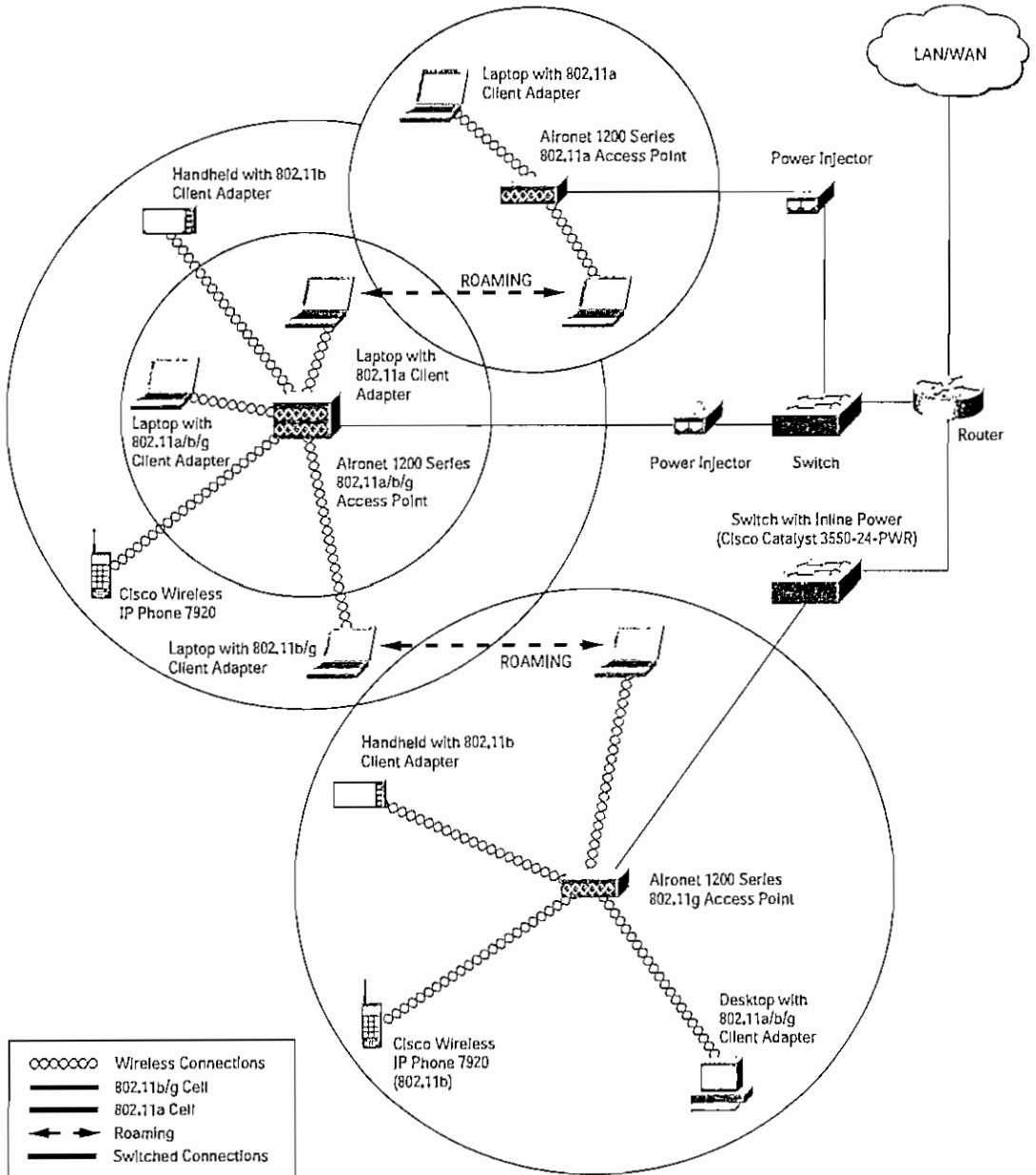
### MODULAR DESIGN FOR CUSTOMER-SPECIFIC FUNCTIONALITY AND UPGRADE CAPABILITY FOR INVESTMENT PROTECTION

The Cisco Aironet 1200 Series is specifically designed to protect current and future network infrastructure investments. The 802.11a radio supports data rates of up to 54 Mbps on eight non-overlapping 5 GHz channels to offer high performance as well as maximum capacity and scalability. The 802.11g radio supports data rates up to 54 Mbps in the 2.4 GHz band. When using an 802.11g radio, the access point may be configured to support only 802.11g clients for high-bandwidth applications, or, for added investment protection, it may be configured to support both 802.11g and legacy 802.11b clients.

The 1200 Series provides the flexibility to change capabilities as customer requirements and technologies evolve. CardBus-based 802.11a upgrade modules can be easily installed into Cisco Aironet 1200 Series Access Points originally configured for 802.11b or 802.11g. The 802.11b Mini-PCI radio module in installed Aironet 1200 Series access points can be replaced with an 802.11g upgrade module to provide increased performance with complete backward compatibility.

**Figure 1**

The Cisco Aironet 1200 can be configured to support 802.11b/g, 802.11a, or all three technologies in a single device. Clients supporting multiple 802.11 standards can roam between access points while maintaining reliable and uninterrupted access to all network resources.

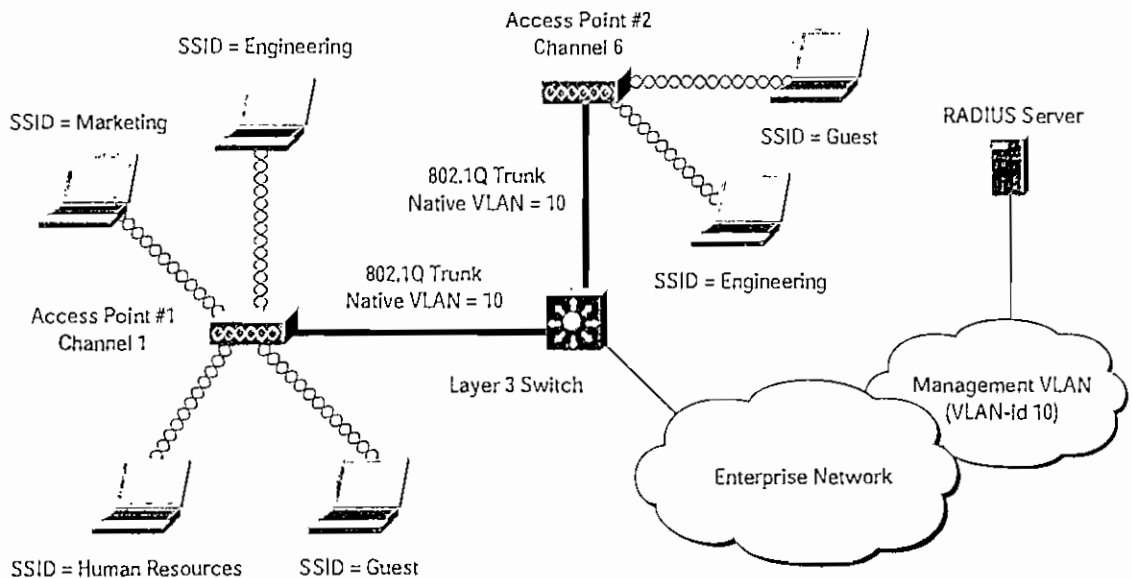


## INTELLIGENT NETWORKING FEATURES FOR A SCALABLE, MANAGEABLE SOLUTION

The Cisco Aironet 1200 Series extends end-to-end intelligent networking to the wireless access point. Cisco command-line interface (CLI) allows customers to quickly and consistently implement the extended capabilities available in Cisco IOS Software. Customers can manage and standardize their networks using tools they have developed internally for their Cisco routers and switches.

An ideal choice for enterprise installations, the Cisco Aironet 1200 Series supports enterprise-class virtual LANs (VLANs), quality of service (QoS) and proxy mobile Internet Protocol (IP). The Cisco Aironet 1200 Series can manage up to 16 VLANs in single-mode or dual-mode operation (Figure 2), which allows customers to differentiate LAN policies and services—such as security and QoS—for different users. For example, enterprise customers can use different VLANs to segregate employee traffic from guest traffic, and further segregate those traffic groups from high-priority voice traffic. Traffic to and from wireless clients with varying security capabilities can be segregated into VLANs with varying security policies. For example, VLANs allow educational institutions to secure faculty and administrator traffic from student traffic traveling over the same infrastructure. Implementing VLAN segmentation increases wireless LAN manageability and security.

Figure 2  
Indoor Wireless VLAN Deployment



With support for IEEE 802.1p QoS, the Cisco Aironet 1200 Series provides traffic prioritization for packets traveling to and from the access point over Ethernet. Delay-sensitive traffic, such as voice and video, can be prioritized over data traffic for improved user experience and optimal network utilization. Software and radio firmware upgrades allow upgrade to future QoS standards such as IEEE 802.11e. Supporting the voice prioritization schemes for 802.11b mobile phones, the Aironet 1200 Series further enables quality voice-over-wireless-LAN solutions.

With proxy mobile IP, users can maintain seamless network connectivity as they roam across subnets. The proxy mobile IP feature creates a tunnel between routers on the remote network and the user's home network. This allows users to consistently maintain their home IP address and access to their home network applications as they roam

beyond their home subnet. Proxy mobile IP also enhances a mobile IP-enabled network by enabling subnet roaming capabilities on IEEE 802.11 clients so that these devices do not need specialized mobile IP client software, resulting in cost-savings. These proxy mobile IP features allow IT professionals to use their existing IP addressing scheme to cost-effectively design the wireless LAN in a manner more consistent with the wired LAN, while still maintaining user mobility.

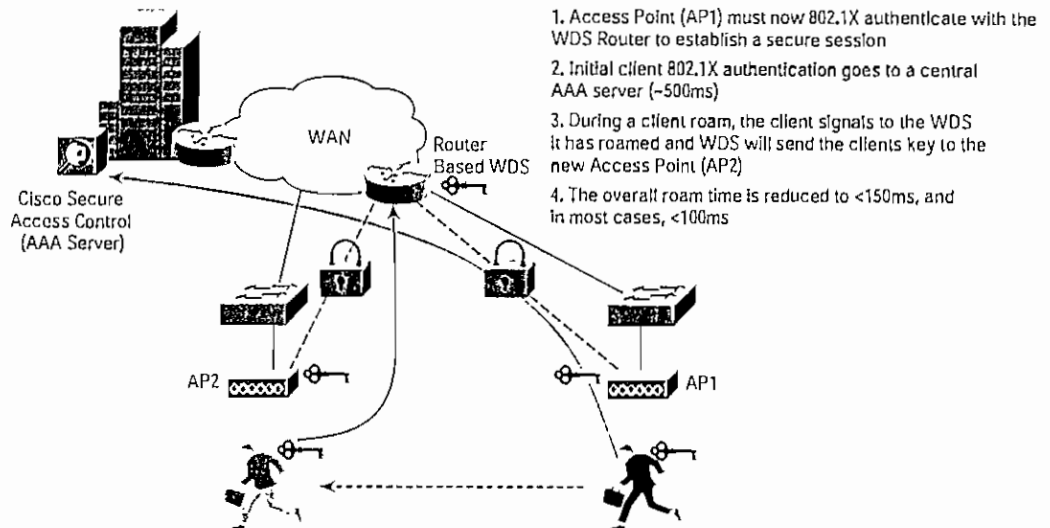
#### CISCO STRUCTURED WIRELESS-AWARE NETWORK

The Cisco Aironet 1200 Series is a key component of Cisco SWAN—an innovative, comprehensive Cisco framework for deploying, operating and managing hundreds to thousands of Cisco Aironet access points using the Cisco infrastructure. Cisco SWAN provides the wireless LAN with the same level of security, scalability, and reliability that customers have come to expect in their wired LAN by introducing “wireless-aware” capabilities into the Cisco infrastructure.

To take advantage of the innovative features of the 1200 Series, not only can Cisco client adapters be used, but now a wide variety of Cisco Compatible devices are available from leading WLAN client suppliers. For example, wireless domain services (WDS) was introduced with Cisco SWAN. WDS is a collection of Cisco IOS Software features that enhance WLAN client mobility and simplify WLAN deployment and management. These services—currently supported on access points and client devices and scheduled to be supported on specific Cisco LAN switches and routers in 2004—include radio management aggregation, fast secure roaming, and WAN link remote site survivability. WDS radio management aggregation supports radio frequency (RF) managed services such as rogue access point detection, interference detection and assisted site surveys.

Fast secure roaming is supported by the Cisco Aironet 1200 Series in conjunction with Cisco and Cisco Compatible client devices. With fast secure roaming, authenticated client devices can roam securely from one access point to another without any perceptible delay during reassociation. Fast secure roaming supports latency-sensitive applications such as wireless voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions (Figure 3).

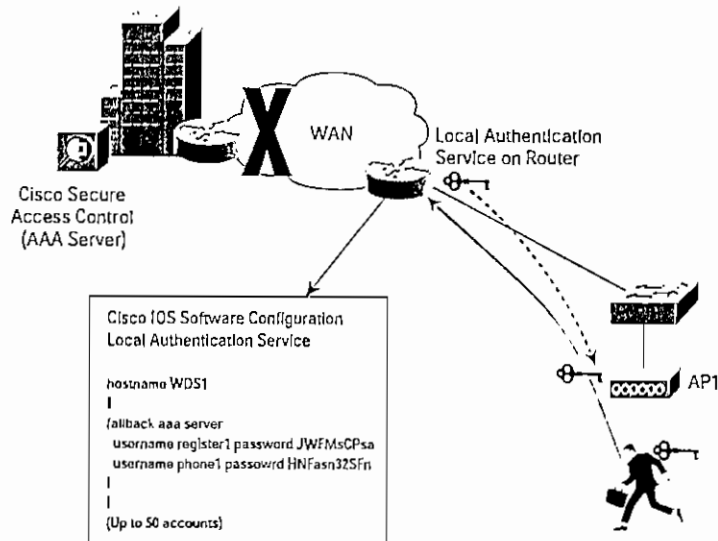
Figure 3  
Fast Secure Roaming



Note: Because the WDS handles roaming and reauthentication, the WAN link is not used

WAN link remote site survivability allows the access point to act as a local RADIUS server to IEEE 802.1X authenticate wireless clients when the authentication, authorization, and accounting (AAA) server is not available. This provides remote site survivability and backup authentication services during a WAN link or server failure, allowing users in remote site deployments with nonredundant WAN links access to local resources such as file servers or printers (Figure 4).

Figure 4  
WAN Link Remote Site Survivability



#### ENTERPRISE-CLASS SECURITY SOLUTION

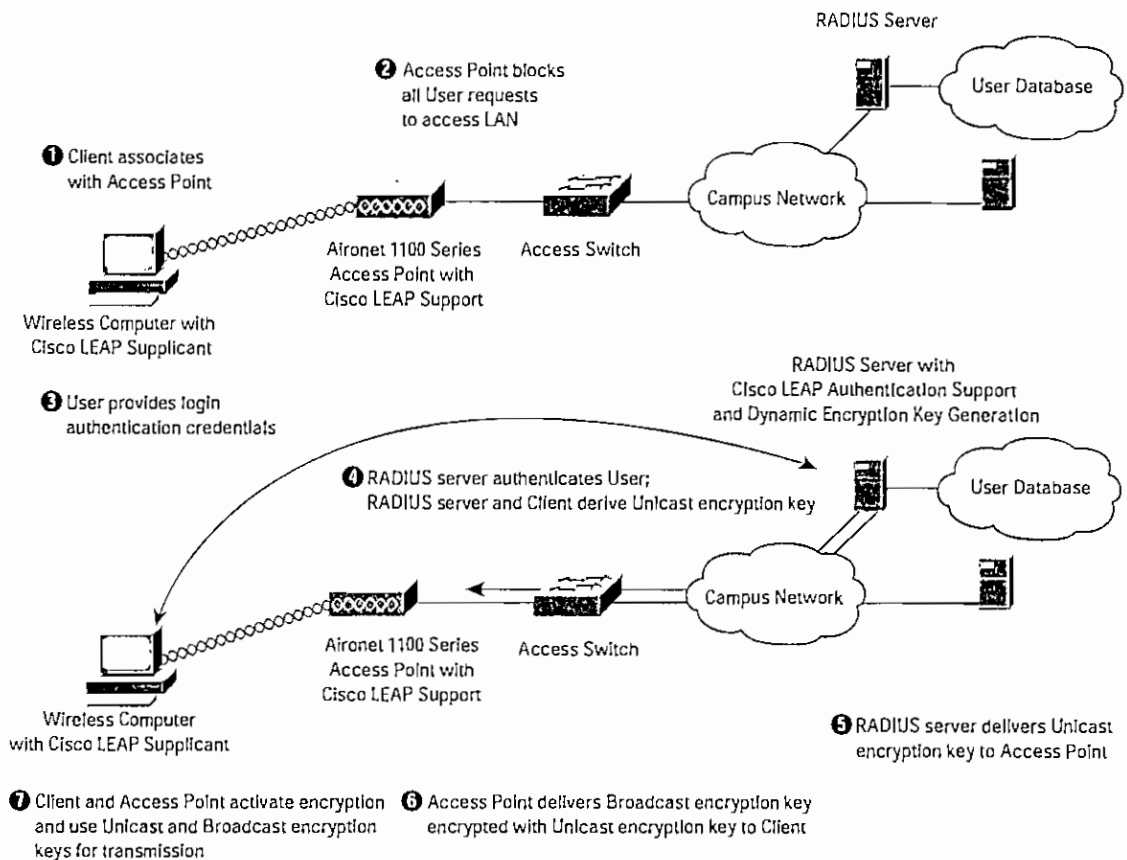
Wireless LAN security is a primary concern. The Cisco Aironet 1200 Series secures the enterprise network with a scalable and manageable system featuring the award-winning Cisco Wireless Security Suite. Based on the IEEE 802.1X standard for port-based network access, the Cisco Wireless Security Suite takes advantage of the Extensible Authentication Protocol (EAP) framework for user-based authentication (Figure 5). This solution also supports Wi-Fi Protected Access (WPA), the new Wi-Fi Alliance specification for interoperable, standards-based wireless LAN security.

The Cisco Wireless Security Suite interoperates with a range of client devices. It supports all 802.1X authentication types, including Cisco LEAP, Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) and types that operate over EAP-TLS, such as Protected Extensible Authentication Protocol (PEAP), EAP-Tunneled TLS (EAP-TTLS) and EAP-Subscriber Identity Module (EAP-SIM). A wide selection of RADIUS servers, such as the Cisco Secure Access Control Server (ACS), can be used for enterprise-class centralized user management that includes:

- Strong, mutual authentication to ensure that only legitimate clients associate with legitimate and authorized network RADIUS servers via authorized access points
- Dynamic per-user, per-session encryption keys that automatically change on a configurable basis to protect the privacy of transmitted data
- Stronger encryption provided by Temporal Key Integrity Protocol (TKIP) enhancements such as message integrity check (MIC), per-packet keys via initialization vector hashing, and broadcast key rotation
- 802.11g version is ready for Advanced Encryption Standard (AES) support
- RADIUS accounting records for all authentication attempts

Figure 5

The Cisco Wireless Security Suite is an enterprise-class security system based on the 802.1X architecture



### INVESTMENT PROTECTION FOR FUTURE-PROOF NETWORKS

With large storage capacity and support for Cisco management tools, the Cisco Aironet 1200 Series provides the capacity and the means to upgrade firmware and deliver new features as they become available. It features more than twice the amount of storage required by the initial Cisco IOS firmware load and the tools for IS professionals to centrally and automatically upgrade firmware on often remote access points across the enterprise. For additional investment protection, the Cisco Aironet 1200 Series comes complete with an integrated mounting system that secures the device using the customer's choice of laptop security cables or standard padlocks (Figure 6). The reliability of the 2.4 GHz solution also makes the Cisco Aironet 1200 Series a wise investment for enterprise customers. It provides field-proven reliability, featuring a Cisco Aironet fifth-generation 2.4 GHz radio. The 5 GHz radio maximizes capacity and performance, delivering up to 54 Mbps data rates on all eight available channels and allowing the wireless network to scale to accommodate a large number of users. With the Cisco Aironet 1200 Series, a single access point can add capacity to support new users by simultaneously operating one radio for 802.11a networked clients while maintaining another radio for 802.11b or 802.11b/g clients. The redundant hot-standby feature also aids in the overall reliability of the network by providing a backup access point in the rare case of a failure.

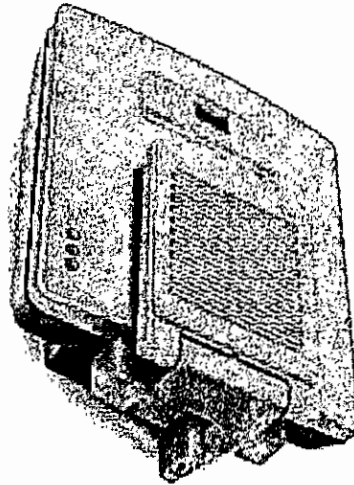
Cisco Systems, Inc.

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Page 7 of 22



**Figure 6**  
Cisco Aironet 1200 Series Mounting Bracket



#### **INSTALLATION OPTIONS INCREASE FLEXIBILITY**

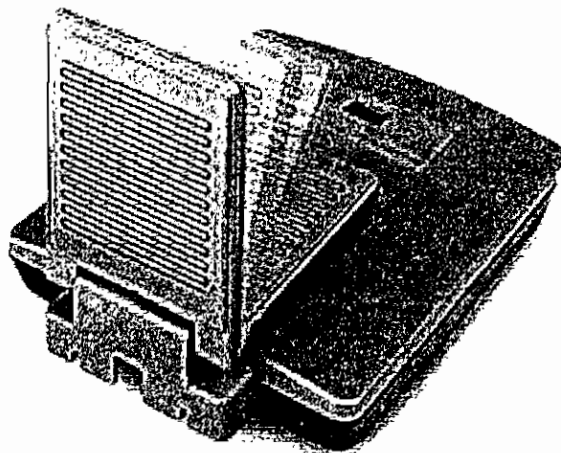
As the popularity of wireless LANs increases, enterprises are installing access points in a growing variety of facilities, locations, and orientations. The Cisco Aironet 1200 Series is designed with this in mind. With its broad operating temperature range, the cast aluminum-cased device provides the ruggedness required in factories and warehouse installations while still meeting the aesthetic requirements of the enterprise. Support for both inline power over Ethernet, as well as local power, maximizes powering options. The access point and integrated mounting system are designed for installation on walls, below ceilings, and, with its plenum ratable metal case, above suspended ceilings. All three radios (802.11a, 802.11b, and 802.11g) provide a variety of transmit power settings to adjust coverage area size. This, coupled with the broadest selection of 2.4 GHz and integrated 5 GHz antennas in the industry, provides users with unparalleled flexibility in cell size and coverage patterns.

#### **UNIQUE 802.11A 5 GHZ ANTENNA DESIGN FOR OPTIMAL COVERAGE**

To extend the flexibility of deployments, the 802.11a radio module incorporates an articulating antenna paddle that contains both omni-directional and patch antennas (Figure 7). For ceiling, desktop, or other horizontal installations, the omni-directional antenna provides optimal coverage pattern and maximum range. For wall mount installations, the patch antenna provides a hemispherical coverage pattern that uniformly directs the radio energy from the wall and across the room (Figure 8). Both the omni-directional and patch antennas provide diversity for maximum reliability even in high multipath environments such as offices and other indoor environments. Cisco provides this level of 5 GHz antenna flexibility and reliability to suit all installation scenarios.

**Figure 7**

Integrated Omni-Directional and Patch Antenna Featured in the 802.11a Radio Module



## Cisco **Wireless** IP Phone 7920

As the leader in IP Communications, Cisco continues to deliver unsurpassed end-to-end data and IP telephony solutions, offering the most complete and fully featured IP Phone portfolio. Cisco IP phones provide unmatched levels of integrated business functionality and converged communications features beyond today's conventional voice systems.

Cisco® extends the power of IP Communications throughout the enterprise by delivering a powerful converged wireless solution with intelligent wireless infrastructure and an innovative product with the introduction of the Cisco Wireless IP Phone 7920. The Cisco Wireless IP Phone 7920 is an easy-to-use IEEE 802.11b wireless IP phone that provides comprehensive voice communications in conjunction with Cisco CallManager and Cisco Aironet® 1200, 1100, 350, and 340 series of Wi-Fi (IEEE 802.11b) access points. As a key component of the Cisco AVVID Wireless Solution, the Cisco Wireless IP Phone 7920

delivers seamless intelligent services such as security, mobility, quality of service (QoS), and management, across an end-to-end Cisco network. (For more information on the AVVID portfolio please visit: <http://www.cisco.com/go/avvid>)

The Cisco Wireless IP Phone 7920 is equally adaptable for all mobile professionals, from managers on the move within an office environment to associates working in the warehouse, on the sales floor, or in the call center. Nurses, doctors, educators, and IT personnel can also increase their reachability as an ever-broadening range of industries adopt wireless LANs.

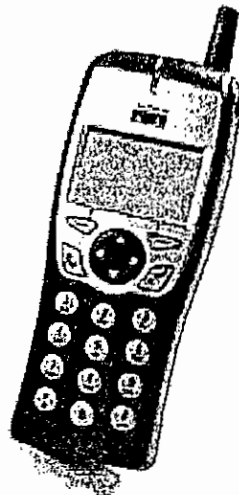
The Cisco Wireless IP Phone 7920 provides the first generation of wireless IP phones for Cisco's IP Communications solution. The Cisco Wireless IP Phone 7920 supports a host of calling features and voice quality enhancements.

### Cisco Wireless IP Phone 7920 Features

The Cisco Wireless IP Phone 7920 is designed for ease-of-use:

- Pixel-based display—Provides intuitive access to calling features.
- Two soft keys—Dynamically present calling options to the user.

Figure 1:  
Cisco Wireless  
IP Phone 7920



Cisco Systems, Inc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Page 1 of 6



- Four-way rocker switch—Allows easy movement through the displayed information.
- “Hold” key and “Mute” key—Provides users with the flexibility to either place an active call on hold or to ‘listen only’ to the conversation without background noise interference.
- Volume-control—Provides easy decibel-level adjustments of the handset and ringer when in use.
- “Menu” key—Allows for quick access to information such as directories, call history and phone settings such as:
  - Easy retrieval of voice-mail messages
  - Display missed calls, outgoing calls that have been placed, and incoming calls that have been received
  - Various preferences such as Cisco CallManager ring types, user profiles, and preferred language

### **Calling Features**

The Cisco Wireless IP Phone 7920 is designed to grow with system capabilities. Features will keep pace with new system enhancements. Currently available, easy-to-use, features include:

- Multi-line appearance (six extensions/speed dials)
- Calling name and number display
- Call waiting
- Call forward
- Call transfer
- Three-way calling (conference)
- Pre-dialing before sending
- Redial
- Call hold / resume
- Call mute
- Call park
- Call pick-up / group pick-up
- “You Have Voice Mail” message on display

### **Other Features**

Hotkey for vibration / ring toggle

- Hotkey for keypad lock
- Hotkey for voice-mail access
- Nine speed dials configurable in the set
- Programmable speed-dial hotkeys 2-9
- Comfort noise generation (CNG), voice activity detection (VAD), adaptive jitter buffer, and echo cancellation
- Language support: English, French, German in the first release
- Local phone book
- Time / date display
- Keypad lock / vibration icon indicators
- Idle / call state-based soft-keys
- RF and battery level indication

### Wireless Characteristics

- Wireless Access Protocol: IEEE 802.11b, Direct Sequence with Dynamic Rate Scaling at 1, 2, 5.5, 11 Mbps.
- RF channels: Up to 14 depending on regulatory domain. North America: 11, ETSI: 13, Japan: 14
- Frequency range: 2.4-2.497 GHz
- Wireless output power: 100mW Effective Isotropic Radiated Power (EIRP) with scaling at 1, 5, 20, 50, 100mW
- Range: 500-1000 ft / 15-300m indoors depending on environment
- Access point support: Cisco Aironet series access points including the 1200, 1100, 350 and 340 series

### Network Features

- Cisco Discovery Protocol (CDP)
- Automatic IEEE 802.1q (Virtual LAN [VLAN]) configuration
- G.711a, G.711u, and G.729a audio-compression coder-decoders (codecs)
- SNMP Manager
- DHCP or Static Configuration Option
- Alternate TFTP Support
- Over-the-air firmware upgrades supported using a Trivial File Transfer Protocol (TFTP) server
- Provisioning of network parameters through Dynamic Host Configuration Protocol (DHCP)
- Site Survey, Trace Route (Hidden Feature), Seamless-Secure Roaming, and VLAN Support

### Protocols Supported

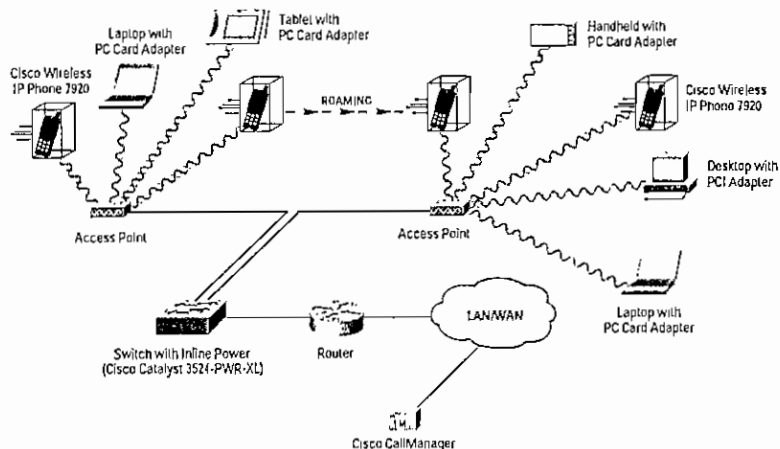
- Compatible with Cisco CallManager Version 3.2 and later, using the Skinny Client Control Protocol
- Compatible with Cisco Survivable Remote Site Telephony (SRST) Version 2.0 and later.

### Security

- Cisco Wireless Security Suite IEEE 802.1X Cisco LEAP authentication: Optional password prompt at power up
- 40 and 128 bit static Wired Equivalent Privacy (WEP)
- Optional phone lock password

Figure 2:

Multiple Aironet access points can be placed throughout a facility to provide uninterrupted connectivity to users equipped with the Cisco Wireless IP Phone 7920.



Cisco Systems, Inc.

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.



### **Physical Specifications**

- Cisco Wireless IP Phone 7920 dimensions (H x W x D): 5.2" x 2.1" x 1.0"; 132.1mm x 53.3mm x 25.4mm
- Cisco Wireless IP Phone 7920 Series Desktop Charger dimensions (H x W x D): 3.0" x 3.7" x 5.1"; 75mm x 93mm x 129mm
- Weight (with standard battery): 4.8 oz; 136.1g
- High frequency response ringer / vibration / visual display alerts
- 128 x 80 pixel-graphical display, backlit
- 4-way rocker switch
- Send and End/PWR keys
- Built-in speaker / MIC
- 2.5mm headset jack
- USB slave

### **Accessories**

- Desktop charger with USB
- 1440mA standard Li-ion battery
- 1960mA extended Li-ion battery
- 2.5mm ear-bud
- Additional headsets available at <http://www.cisco.getheadsets.com>
- Choice of holster and full-cover carry cases
- W2K-based administration utility for quick phone configuration
- AC-adapters (by geographical region)

### **Power Supply**

- Standard 1440mA Li-ion battery life: 3.5 hour talk-time, 21 hour standby
- Extended 1960mA Li-ion battery life: 4.25 hour talk-time, 30 hour standby
- AC-adapters (by geographical region)

### **Environmental**

- Operating temperature: 32 to 113 F (0 to 45 C)
- Storage temperature: -22 to 140 F (-30 to 60 C)
- Relative humidity: 10 to 95% (noncondensing)
- Drop specification: 1 meter to concrete
- Thermal shock: -30C 24 hours / +70C 24 hours
- Vibration: 1.5 Grms maximum, 0.1" double amplitude @ 0.887 octaves per minute form 5-500-5 Hz sweep, 10 minute dwell on 3 major peaks, in each of the three major mutually perpendicular axes



## **Certification/Compliance**

### **USA**

- Safety: UL 60950, 3rd. Edition
- FCC Part 15 B, FCC Part 15.247
- OET 65 C

### **Industry Canada**

- Safety: CAN/CSA-C22.2/UL No. 60950
- RSS-102, RSS-210

### **Europe**

- Directive 1999/5/EC
- EN 300.328
- EN 301.489.1
- EN 301.489.17

### **Australia \ New Zealand**

- Safety: AS/NZS 3260, ACA TS001, AS/NZS 60950-1
- AS/NZS 4771
- AS/ACIF S004
- DR PTC220
- ACA Radio communications (Electromagnetic Radiation---Human Exposure) Standard

### **Japan**

- Safety: MITI
- TELEC 33a, VCCI Class B
- TELEC Std 66

### **Emission:**

- EN 55022, class B
- CISPR22, class B
- EN 300 328
- CFR47, Part 15, Subpart B, 1999, class B

### **Immunity:**

- CISPR24
- EN 55024
- EN50082-1
- EN 301 489-1 & -17

## Service and Support

Cisco IP Communications services and support reduces the cost, time, and complexity associated with implementing a converged network. Cisco and its partners have designed and deployed some of today's largest and most complex IP Communications networks—which means that they understand how to integrate an IP Communications solution into your network. Cisco design tools and best practices help ensure a solution that best fits your business needs from the start, eliminating costly redesigns and downtime. Our proven methods help ensure a sound implementation that will deliver the functions and features you expect—on time. Support services include remote network operations, network management tools to administer the converged application and network infrastructure, and technical support services.

Through these services, your organization benefits from the experience gained by Cisco and its partners. Leveraging this valuable experience, you can create and maintain a resilient converged network that will meet your business needs today—and in the future.

## Ordering Information

Table 1 lists some of the common part numbers for the Cisco Wireless IP Phone 7920 and Cisco CallManager:

**Table 1** Part Numbers

Part Number	Description
	Cisco Wireless IP Phone 7920, Standard Li-Ion Battery, and AC Adapter
	Station User License for Cisco CallManager (CCM)
	Cisco Wireless IP Phone 7920 Series Desktop Charger
	Cisco Wireless IP Phone 7920 Series Configuration Utility CD, and USB Cable
	Cisco Wireless IP Phone 7920 Standard Battery, Li-Ion, 1440mA
	Cisco Wireless IP Phone 7920 Extended Battery, Li-Ion, 1960mA
	Cisco Wireless IP Phone 7920 Series Ear-bud—2.5mm plug
	Cisco Wireless IP Phone 7920 Holster Carry Case, Leather
	Cisco Wireless IP Phone 7920 Full-Cover Carry Case, Leather

Cisco offers a standard one-year warranty on all Cisco Wireless IP Phone 7920 Series components. A Cisco SMARTnet<sup>®</sup> optional service agreement is available on the CP-7920-K9 hardware only and not the accessories such as batteries.

## For More Information

For more information about Cisco products, call or visit:

- United States and Canada: (toll free) 800 553-NETS (6387)
- Europe: 32 2 778 4242
- Australia: 1 800 678 808
- Other: 408 526-7209
- Web: <http://www.cisco.com>

## CISCO SYSTEMS



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. ETMC 203159—CM 10/03 (0304R)