TESIS PUCP

PONTIFICIA **UNIVERSIDAD CATÓLICA** DEL PERÚ

Esta obra ha sido publicada bajo la licencia Creative Commons
Reconocimiento-No comercial-Compartir bajo la misma licencia 2.5 Perú.
Para ver una copia de dicha licencia, visite
http://creativecommons.org/licenses/by-nc-sa/2.5/pe/

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UNA RED DE VIGILANCIA RESIDENCIAL BASADO EN EL PROTOCOLO DE COMUNICACIÓN IP SOBRE LAS LÍNEAS ELÉCTRICAS DE BAJA TENSIÓN

Tesis para optar el Título de Ingeniero Electrónico

Presentado por:

CÉSAR MANUEL GARAY KANESHIMA

Lima - Perú

2007

SOME RIGHTS RESERVED

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

RESUMEN

La elaboración de este documento parte de dos premisas claramente visibles en el entorno sobre el cual nos desarrollamos. La primera de ellas tiene su origen en la sociedad, se desenvuelve negativamente al interior de las instancias que la componen y actúa de tal manera, que cualquier estudio que busque demostrar sus consecuencias adquiere casi de inmediato un cierto nivel de insignificancia frente a lo cotidianamente experimentado. La segunda premisa parte de un fenómeno también social y que ha adquirido carácter masivo con el transcurrir de las últimas décadas; su expansión y desarrollo, por el contrario, son auspiciosos dado que sus objetivos están orientados a resolver problemas.

En primer término está la delincuencia, que de acuerdo a lo definido anteriormente, forma parte de una realidad que estamos obligados a erradicar. Sus efectos van dirigidos no sólo a los bienes materiales de los ciudadanos sino que en muchos casos llegan a dañar su propia integridad.

El segundo término se refiere a las tecnologías de la información, en la que sus técnicas y sistemas de comunicación pueden ser usados como herramientas para enfrentar problemas de larga data como la delincuencia. Considerando que el accionar delictivo es un problema que va más allá de cualquier medida de contingencia (ya que su solución tiene que ver más con factores sociales, económicos y culturales); es importante, sin embargo, plantear que mediante el uso de los recursos tecnológicos se puede dotar de un mayor nivel de 'inteligencia' al entorno y limitar el accionar de cualquier organización antisocial con el uso de diversas opciones como la del seguimiento visual y el registro continuo de sus acciones.

Para este trabajo se ha tomado en cuenta las medidas en favor de la seguridad ciudadana al interior de un recinto urbano en la que conviven centenares de personas, esto último se plantea por medio de herramientas tecnológicas ampliamente extendidas como la voz y el vídeo para mantener monitoreado todos los alrededores. La forma y las tecnologías con las que se implementarán dichas medidas, sin

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

embargo, no han sido del todo popularizadas en otros proyectos similares; por lo que este documento intenta proponer una variante más al complejo abanico de posibilidades ya existente.

Para las soluciones de voz y vídeo se ha optado por los protocolos de comunicación extendidos en las redes de Internet aun cuando este esquema se trata, en principio, de una red de área local (más ligado al concepto de Intranet). Para la implementación se ha considerado en primer lugar, la calidad que deben tener las soluciones; en segundo término, el reto de enfrentar el alto precio de los equipos y un bajo presupuesto asumido, por lo que se termina formulando diferentes opciones para reemplazar algunos equipamientos convencionales. Finalmente se reconoce a las líneas eléctricas de baja tensión como un medio más por el que puede circular una gran variedad de información digital a través del uso de la tecnología PLC (Power Line Communications); con ello se piensa utilizar la infraestructura ya extendida para soportar las diversas aplicaciones multimedia y así diseñar una red de equipos que converjan como una plataforma de seguridad residencial.

La estructura del presente documento se divide en cuatro capítulos, cada uno de los cuales surge progresivamente como consecuencia del anterior. En el primero se da una visión general acerca de la problemática delincuencial, tanto en los sectores urbanos como en los sectores rurales de la sociedad peruana; en dicho análisis se recurre a material de diversas fuentes que incluyen estadísticas, gráficas, notas periodísticas, entre otras. Seguidamente se da paso a un análisis de aquello que se relaciona más con este fenómeno a nivel de la localidad en estudio, que en este caso se refiere al Conjunto Habitacional Alfredo Dammert Muelle ubicado en el distrito de Surquillo en la ciudad de Lima.

El segundo capítulo representa, por el contrario, el planteamiento de una alternativa de solución a lo antes declarado; en este capítulo se busca entender claramente cómo es que trabaja la tecnología de transmisión bajo las líneas eléctricas de baja tensión y cómo es que ella se puede perfilar como una alternativa seria, eficaz y económica para resolver estos problemas. El estudio de esta herramienta de comunicación abarca temas que van desde sus fundamentos teóricos y el análisis de sus prestaciones y desventajas, hasta la evaluación de su modo de funcionamiento y los equipos

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

involucrados en su desempeño.

A partir de lo desarrollado en los dos capítulos anteriores, nace un tercero que se ubica en este trabajo como la esencia principal de todos los objetivos planteados. Dicho de otro modo, cada proposición, esquema de diseño, equipo y tecnología de aplicación seleccionados representan el gran conjunto solución con el que se piensa enfrentar la ineficiencia en el campo tecnológico y la amenaza delincuencial que vienen tomando un valor protagónico en las últimas décadas, en éste y muchos otros sectores de convivencia social.

Para la elaboración de este capítulo se ha tenido en cuenta, primero, las aplicaciones y el grupo de protocolos de red con el que se dará valía a las soluciones; por este motivo su desarrollo comienza con un breve repaso de cómo es que trabaja la tecnología "Internet Protocol (IP)", luego se procede con un pequeño estudio de las técnicas de voz y vídeo basadas en este protocolo. Sobre la base de esa información introductoria surgirán una serie de propuestas y elecciones pertinentes que se puedan adaptar al medio de comunicación elegido para este diseño (líneas eléctricas de baja tensión) y se considerará en todo momento un factor de análisis costo – beneficio para que, consecuentemente, las soluciones adoptadas no escapen de la realidad económica, ni pierdan su sentido de eficacia.

Finalmente se concluye la documentación técnica con el capítulo 4, en el que se presentan algunas pruebas de voz y vídeo sobre IP que usan como medio de transmisión las líneas eléctricas de los laboratorios de la Universidad. Aun cuando las condiciones no son exactamente las mismas con las que se trabajaría en caso de una eventual implementación, la ejecución de estas experiencias sirve para demostrar, en gran medida, su capacidad para soportar aplicaciones de usuario y la validez de esta tecnología para condiciones exigentes como son las aplicaciones en tiempo real.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ÍNDICE GENERAL

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ÍNDICE DE FIGURAS

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

INTRODUCCIÓN

En nuestro país los temas relacionados a la calidad de vida de los peruanos han ido cobrando importancia con el transcurrir de los años. Actualmente, bajo la óptica de una realidad cada vez más alentadora a nivel económico se puede diferenciar, por ejemplo, una tendencia masiva hacia la construcción de viviendas y complejos residenciales. Por otro lado, los temas ligados a la seguridad ciudadana han dejado de ser un objetivo superficial dentro de la escala que involucra el nivel de vida de los pobladores, debido a que actualmente forman una de las aristas fundamentales en los planes de gobierno y en el presupuesto futuro de las autoridades locales, provinciales y nacionales.

A pesar de lo recientemente señalado, la realidad nos indica que el sistema aún no atraviesa por la metamorfosis masiva y contundente que se espera; contrario a lo que si viene experimentando la tecnología desde hace ya varios años, por ejemplo en el campo de las comunicaciones. Hoy en día, por citar un caso, la red de redes mundial (Internet) ha cubierto en gran medida las expectativas creadas en torno a la necesidad de comunicación de las personas; sobre todo ahora, en un contexto en el que la globalización se ha tornado imperante.

Si tomamos como punto de partida las necesidades sociales en el campo de la seguridad ciudadana y rescatamos los medios de comunicación como una herramienta para solucionar dichos problemas estaríamos frente a una posible solución, siempre y cuando se garantice la factibilidad de los recursos tecnológicos. En tal sentido, las tecnologías que brindan soporte a las herramienta de comunicación deben ser capaces de asegurar la transmisión de la información (voz, vídeo y datos) asumiendo un ámbito global; es decir, que llegue a la mayor cantidad de usuarios en el planeta.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

Una manera de cubrir este inconveniente surgió con el desarrollo de las tecnologías de acceso de banda ancha denominadas XDSL, su desempeño consiste en la transmisión de información utilizando las redes de telefonía ya desplegadas. Sin embargo, últimamente se está dando importancia a un medio de transmisión con mayor cobertura, cuya concepción y usos se centraban exclusivamente en la distribución de grandes niveles de potencia, pero dadas sus características vienen siendo usadas, también, para la transferencia de información digital en banda ancha. Nos referimos a la tecnología PLC: Power Line Communications.

En efecto, el procedimiento mediante el cual se hace uso de las líneas eléctricas para la transmisión de información digital es una alternativa más dentro del campo de la telecomunicaciones. Su implementación en algunos sectores industriales tomó forma desde hace ya algunas décadas; aunque las condiciones adversas del medio, la ineficiencia para controlar las interferencias causadas o padecidas por el entorno, sumadas a la desatención para desarrollar normativa con carácter universal y herramientas de alto nivel de procesamiento a precios accesibles; hicieron que PLC no impacte con relevancia en las aplicaciones más comerciales y cotidianas que exige hoy en día la sociedad.

El panorama actual, empero, es radicalmente distinto a partir de los últimos años. La demanda creciente de los usuarios por mayores niveles de ancho de banda y la necesidad de los grandes grupos empresariales por imponerse en el mercado, han originado que las miradas vuelvan con mayor interés sobre PLC. De esta manera se dio impulso a la fabricación de circuitos integrados de alta tecnología para mejorar el desenvolvimiento del producto, principalmente en lo referente a niveles de ancho de banda, ahorro en el consumo de potencia, y la creación de algoritmos de seguridad y mecanismos adecuados para la atenuación de interferencias.

El mercado alrededor de esta tecnología creció inconmensurablemente y originó que el precio de los equipos sea comparable al de las otras ya posicionadas. Hace algún tiempo se impulsó a la creación de alianzas corporativas para emitir las normativas generalizadas que le hacen falta para terminar de adquirir solvencia como una solución valedera y presta a soportar mayores inversiones.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

El desarrollo de este trabajo busca, a partir de las afirmaciones vertidas líneas arriba, proponer una alternativa tecnológica frente a la problemática delincuencial y todo ello a partir del uso de los beneficios que PLC puede asegurar como tecnología de información.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

CAPÍTULO 1
LA PROBLEMÁTICA DELINCUENCIAL: EVALUACIÓN DESDE UNA PERSPECTIVA GLOBAL Y LOCAL

1.1. Delincuencia, Violencia y Sociedad

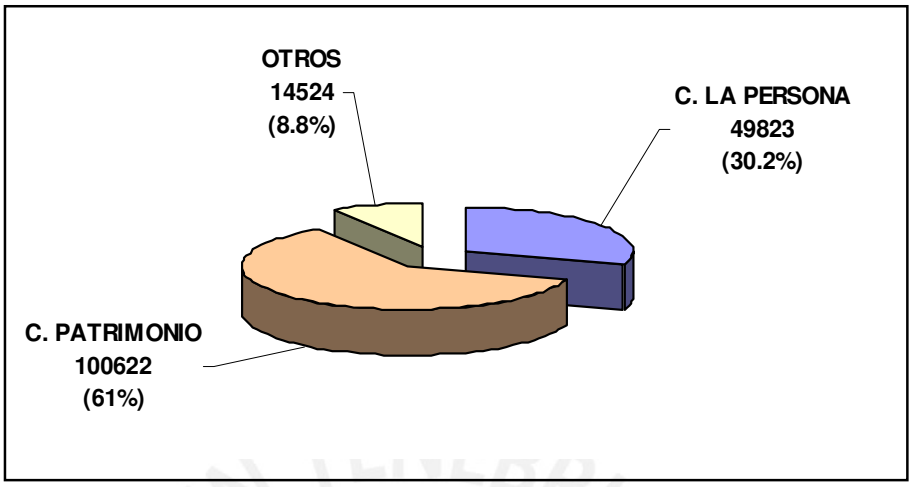
Cualquier trabajo exhaustivo en el que se pretenda analizar el rostro más crudo de la sociedad, terminaría concluyendo que el entorno social sobre el cual nos desarrollamos está cubierto, como mínimo, de deficiencias de índole moral, económico y cultural.

Estos factores, por demás conocidos, son resultado de una gran cadena de producción que viene detrás. En un esquema en el que la familia, la escuela, la comunidad y los medios de comunicación constituyen espacios de socialización muy importantes pero que históricamente no han articulado una clara orientación de sus objetivos, contribuyendo así a una débil formación ciudadana [43].

La espiral de violencia, cuya raíz es el delito común, tiene una serie de variantes que van desde el pandillaje hasta los asaltos a entidades privadas; incluyendo además acciones en contra de la integridad física de las personas (ver gráfico 1.1). Los daños contra el patrimonio que incluyen el robo de vehículos, la sustracción o deterioro de bienes públicos y privados, entre otros; representan más del 60% de los atropellos a los derechos sociales. Aunque esta estadística revela el panorama de hace algunos años, no es difícil predecir que esta situación tiene aún vigencia; dado que el grueso de la problemática está centrado, si no en el patrimonio, en la persona que es el elemento social por excelencia.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP



FUENTE: EMG-PNP
ELABORACIÓN: OFICINA DE INVESTIGACIÓN Y ESTADÍSTICA/SECRETARÍA TÉCNICA-CONASEC

Gráfico 1.1. Denuncias de Faltas Registradas por la PNP/ año: 2003 [43]

Y es que, siendo rigurosos en el análisis de la delincuencia en el Perú, se puede ir más allá identificando por ejemplo el estrecho vínculo que existe entre el nivel de urbanismo que presenta determinada sociedad y el índice de delincuencia presentado en dicha zona. El gráfico 1.2, por ejemplo, detalla la cantidad de detenidos en el mes de junio del año 2006; es por demás ilustrativo observar como la ciudad de Lima (Capital de la República) lidera esta medición, evidenciando no sólo la mayor concentración de efectivos policiales en esta ciudad, sino que indica que es en ella donde se desenvuelven en mayor medida las acciones delictivas.

Si se aprecia con detenimiento, son las ciudades más densamente pobladas y con mayor desarrollo urbano, aquellas en donde predominan los elementos delincuenciales. Un axioma que se desprende sobre la base de esto último, sería señalar que mientras más crece la población dentro de un limitado espacio geográfico; crece con ella la lucha por conseguir una ocupación en un país con problemas de desempleo, aumenta la frustración y la ignorancia; lo que a la larga nos lleva a cerrar el circulo vicioso de la delincuencia.

La criminalidad y violencia en el Perú constituyen, en la actualidad, un problema político social de primer orden que exige la necesidad de implementar medidas concretas para disminuir la violencia urbana en Lima y las principales ciudades del

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

país; en particular contra la delincuencia común, cuyos efectos los padece transversalmente toda la población [43].

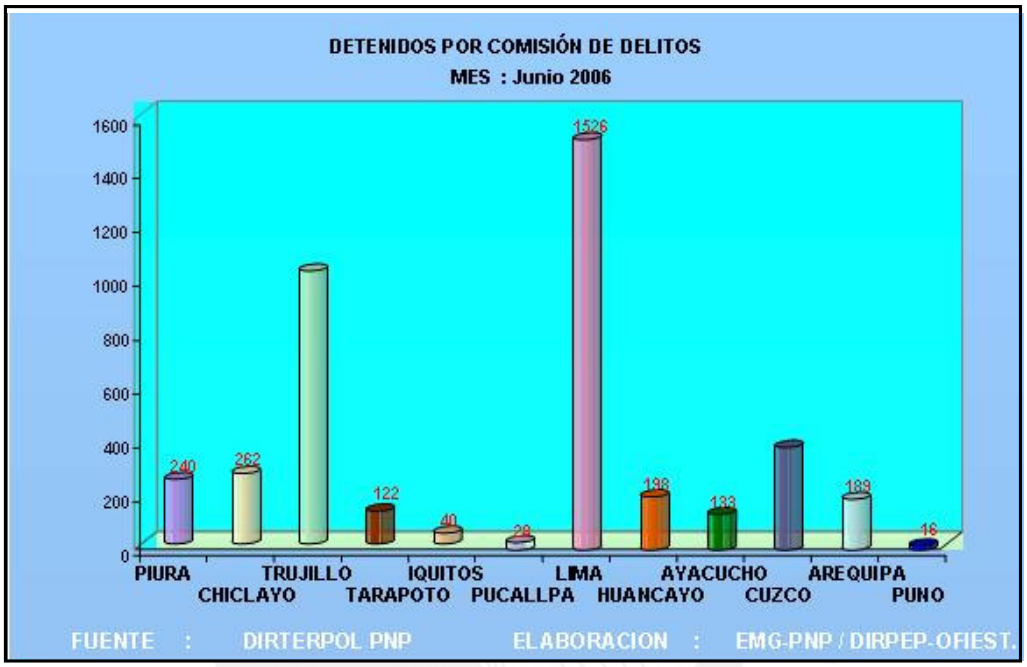


Gráfico 1.2. Detenidos por Comisión de Delitos [43]

1.2. Seguridad Ciudadana

La Seguridad Ciudadana, para efectos de la Ley 27933 (Ley del Sistema Nacional de Seguridad Ciudadana), es la acción integrada que desarrolla el Estado con la colaboración de la ciudadanía, destinada a asegurar su convivencia pacífica, la erradicación de la violencia y la utilización mesurada de las vías y espacio público. Del mismo modo, contribuir a la prevención de la comisión de delitos y faltas.

En otros términos, la Seguridad Ciudadana es el conjunto de medidas y previsiones que adoptada el Estado, a través de sus instituciones y de la comunidad organizada, dentro del marco de la Ley y los derechos humanos, con la finalidad que las personas puedan desarrollar sus actividades libres de riesgos y amenazas que genera la delincuencia [43].

Ambas definiciones denotan una clara inclusión de la sociedad civil en este tema, que antes era vista como una responsabilidad exclusiva de las instituciones públicas. Y es

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

que, como se verá más adelante, es esta participación activa de los ciudadanos la que ha dado pie a los grandes resultados a favor del orden comunitario. En tal sentido, las estrategias para luchar contra la violencia deben incluir necesariamente cuatro aspectos: prevención, represión, cooperación institucional y participación comunitaria [43].

1.3. Análisis de la Delincuencia en la Localidad en Cuestión

En cuanto a los temas relacionados a la seguridad ciudadana dentro de un contexto local; la realidad indica que las medidas de contingencia y prevención del delito son aún ineficientes. Un análisis profundo en los sistemas de seguridad, aplicados por ejemplo al servicio de las residenciales, indica que estos son sumamente dependientes del personal de seguridad encargado (si es que lo hubiera) y que ellos, a su vez, están sometidos a un trabajo totalmente inseguro y provisto de herramientas precarias. De ellos depende en muchos casos el acceso de los foráneos al interior de las residenciales; en todo caso, el nivel de identificación de las personas se remite a su capacidad de memoria y el grado de eficiencia, a su nivel de honestidad y compromiso con la seguridad de la residencial.

Los procedimientos que involucran la labor de los vigilantes están acompañados de una rutina totalmente mecánica; es decir, el medio que diferencia el interior con la vía pública es, en muchos casos, un portón o una reja la cual deben abrir o cerrar constantemente de manera manual, lo que hace de este proceso un mecanismo lento, tedioso e inseguro. Debemos sumarle además a todo lo antes descrito, la ineficiencia que se tiene para la comunicación entre vecinos y el personal de seguridad, ya que de presentarse alguna emergencia como un asalto, un incendio, etc.; la manera con la que se actúa casi en la totalidad de los casos es sumamente improvisada y depende simplemente de la iniciativa de las personas que se percataron del hecho en primera instancia.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

1.4. Análisis Secuencial de los Mecanismos de Seguridad Residencial

Problemas	Causas
Los vigilantes inician sus labores fuera del horario establecido.	Nulidad de personal encargado que lleve un control riguroso de la hora de entrada y salida en sus labores por lo que se genera un clima de inseguridad e incertidumbre por parte de los vecinos.
Procesos discontinuos, mecánicos e ineficientes.	La etapa en la que los vigilantes cierran y abren las puertas de acceso implica que los mismos estén todo el tiempo atentos a cualquier acontecimiento, siguiendo un recorrido constante entre su caseta y el portón de seguridad lo cual hace que estos procedimientos sean lentos y poco confiables.
El vigilante tiene la facultad de dejar ingresar a quien crea conveniente.	Ausencia de un mecanismo que permita saber si las personas que ingresan o salen son realmente residentes, familiares o conocidos; por lo que este proceso es relativo al nivel de compromiso con la seguridad de la residencial por parte del vigilante.
Se han presentado casos de asalto y robo durante el periodo de trabajo del personal de seguridad.	Las medidas organizadas de reacción en estos casos son inexistentes, lo que se evidencia en la falta de un mecanismo que active una alarma en caso se produzca un hecho anormal.
En caso de alguna emergencia, la reacción ha sido ciertamente deficiente.	Los vigilantes y/o los vecinos llaman a las unidades de contingencia pertinentes. Procedimiento que depende de la iniciativa y sensibilidad de los residentes, lo cual toma un tiempo de reacción variable y en muchos casos excesivo.

Tabla 1.1. Inseguridad Residencial: Problemas y Causas

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

1.5. Diagrama de Flujo de los Mecanismos de Seguridad Residencial

Rutina Normal

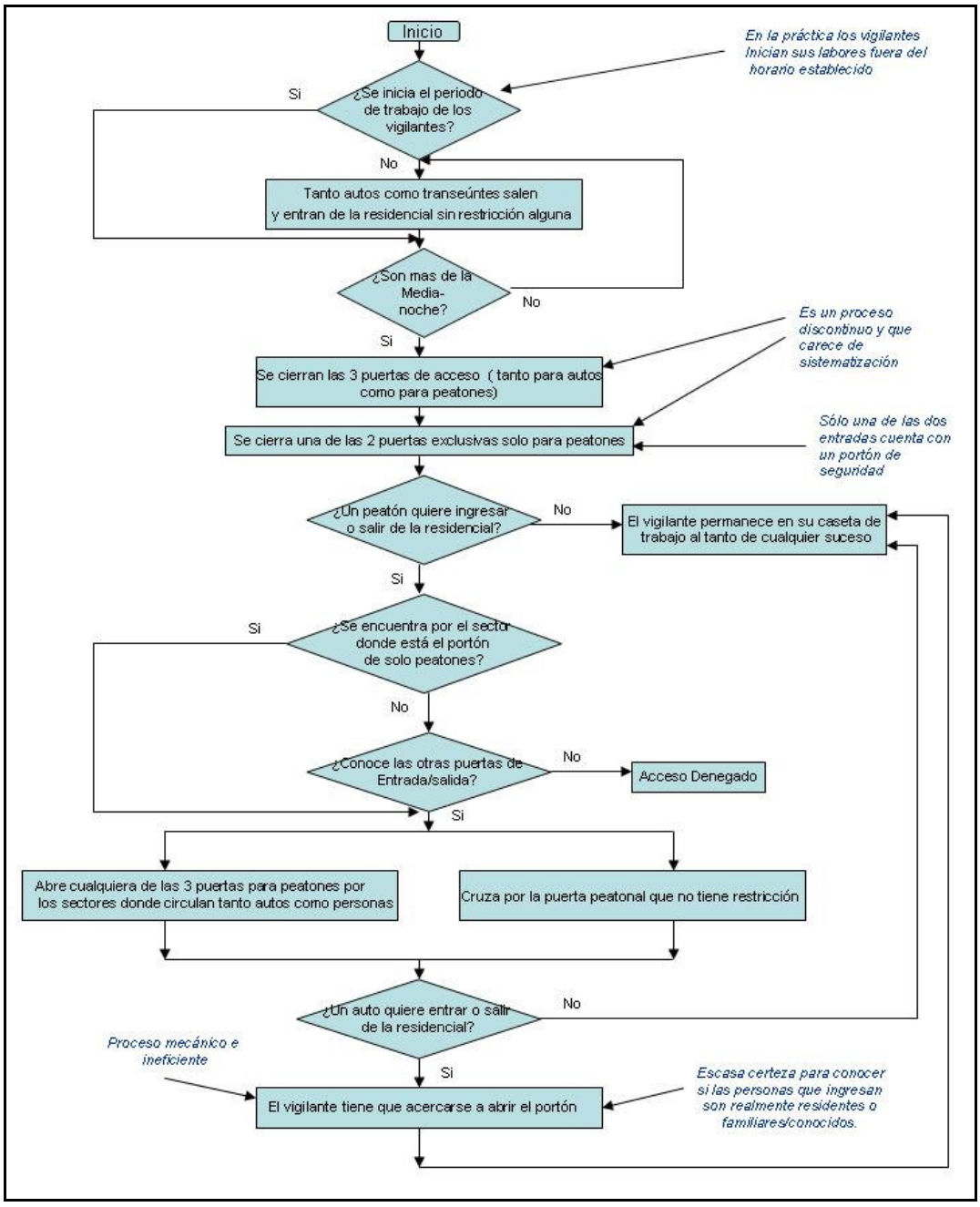


Figura 1.1. Mecanismo Actual del Control de Acceso Residencial

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

1.6. Análisis Global del Entorno

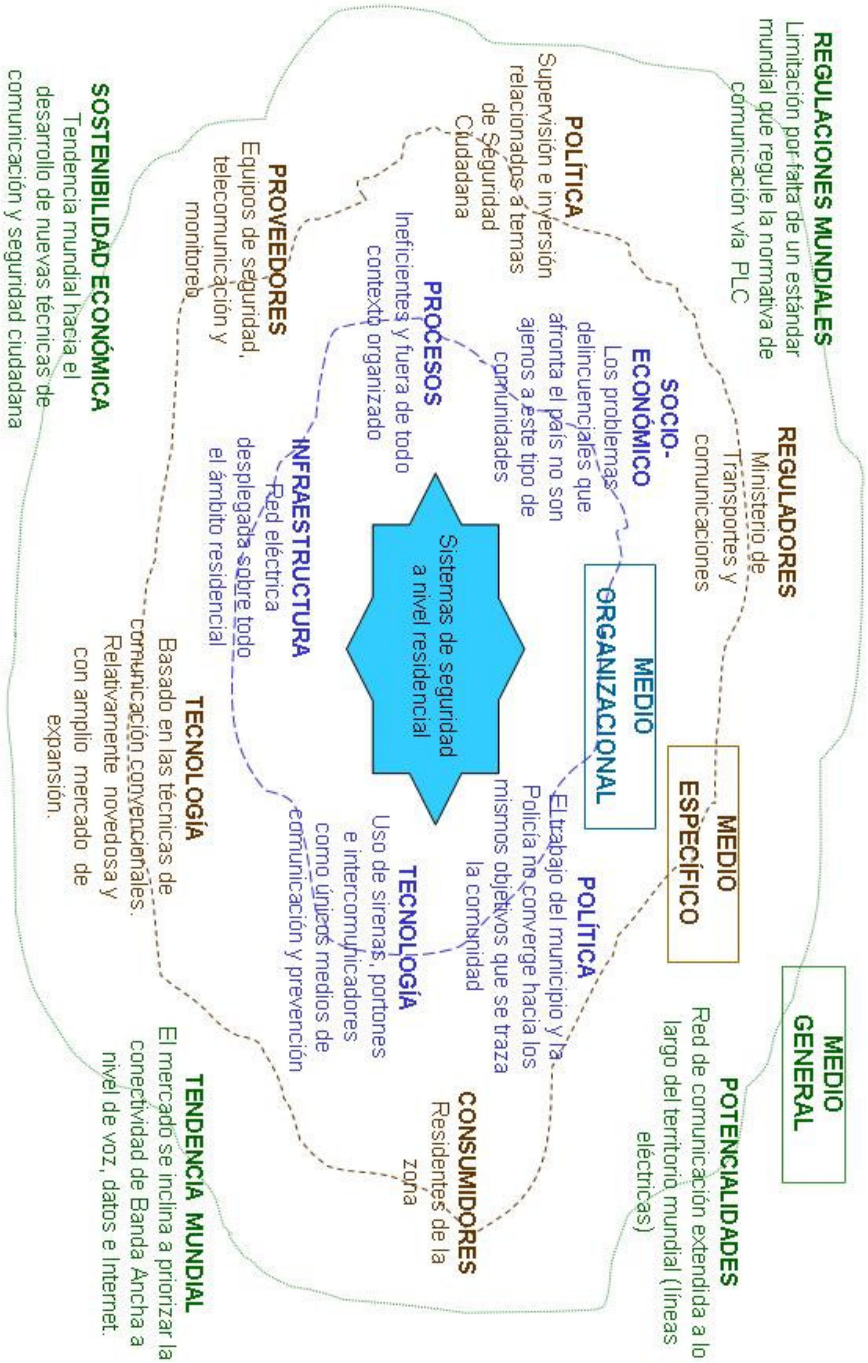


Figura 1.2. Análisis Global del Entorno

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

1.7. Medidas Adoptadas

La evolución de los recursos humanos en la Policía Nacional revela un progresivo decrecimiento, al pasar de 120,000 efectivos que existían en 1985 durante la unificación de las Fuerzas Policiales, a 92,000 policías que tenía para el año 2003; en términos numéricos, esta realidad indica que en 18 años la institución policial ha sufrido una disminución del 24%, mientras que la población se ha incrementado en 59.7% (27'148,101 hab.); aquello permite inferir que la demanda de la población por protección y seguridad es cada vez mayor en comparación a la oferta de servicios policiales [43].

Considerando que en la actualidad es casi inviable una adecuada relación de la demanda con la oferta de estos servicios, se hace imperativo encontrar alternativas que compensen esta brecha. La participación de los gobiernos regionales, gobiernos locales y de la comunidad organizada para apoyar el esfuerzo de la policía nacional contra la criminalidad y la delincuencia, constituye una necesidad prioritaria que es necesario alentar y fortalecer. Sugiere la necesidad, por tanto, de desarrollar políticas preventivas y de control que cuenten con la participación activa de la comunidad [43].

Para el mejor desempeño de esta función, la Policía Nacional se encuentra en un constante proceso de modernización y reestructuración de sus estrategias, en concordancia con las necesidades de seguridad de la sociedad, las cuales tienen como finalidad potenciar la tecnología existente y sistemas de intervención que les permita brindar un servicio más eficiente y oportuno [44].

Desde hace ya algunos años las instituciones llamadas a solucionar los problemas concernientes al orden ciudadano han empezado a solidificar su labor comprendiendo la importancia de las herramientas tecnológicas. En ese contexto, no es extraño identificar, por ejemplo, el uso de equipos de comunicación como radios, celulares, Internet, etc. ; todos ellos destinados a interconectar básicamente las sedes policiales y estrechar relaciones directas con los vecinos de las diversas comunas.

Múltiples experiencias han sustentado terminantemente esta postura, casos como el de la Comisaría de Surquillo cuya labor en temas de seguridad ciudadana le ha valido para obtener importantes laureles, entre ellos, el de haber sido elegida como la Comisaría del Año 2004. Su labor estuvo enmarcada dentro del programa piloto

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

ejecutado por el Ministerio del Interior, en el que la tecnología desempeña un rol destacado específicamente en dos frentes: sistema de vigilancia a través de cámaras de vídeo y el uso de los sistemas computarizados.

La palabras del Comisario de Surquillo, el Comandante Briones, deja clara la labor en el primer frente, cuando señala lo siguiente: “Ahora, el Personal Operativo se ha distribuido tanto para el Patrullaje Motorizado, Patrullaje a Pie, Control de Tránsito, así como para la ejecución de labores de Investigación y sobre todo realización de labores de Inteligencia Operativa; es decir, realizar labores de seguimiento, vigilancia y captura de los delincuentes comunes, sistema que está dando muy buenos resultados, dado que actualmente el Poder Judicial le está dando un valor importante” [44].

Por otro lado, el Comisario de este distrito también es enfático en señalar las medidas y los resultados en el segundo frente: “El sistema de denuncias computarizadas permite almacenar denuncias de toda índole, lo cual evita el uso de los libros de denuncias tradicionales. De esta manera se reduce el tiempo en 7 minutos aproximadamente, lo que antes demoraba cuatro horas. Además, se ha logrado entregar la copia de la denuncia en sólo 7 minutos, lo que anteriormente representaba tiempos de 24 horas a más. Con la tecnología se está haciendo mucho más viable el trámite, lo cual trae buenos resultados, sobre todo en el trato al público” [44].

Afortunadamente experiencias como las recientemente descritas se están volviendo una constante en los planes de desarrollo urbano de los demás distritos. Es necesario incluir, por ejemplo, los recientes planes implementados en los distritos de Miraflores y San Isidro; en ambos casos el uso de herramientas informáticas interconectadas a lo largo de sus territorios han maniatado los intentos de delincuencia común.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

CAPÍTULO 2
DESARROLLO DE LA TECNOLOGÍA POWER LINE COMMUNICATIONS

2.1. Introducción

La Comunicación por las Líneas de Potencia (PLC, por sus siglas en inglés referidas a Power Line Communications) es un nombre genérico que se le otorga a la transmisión de datos por el segmento de baja y media tensión de las redes eléctricas; su campo de acción involucra diversas áreas que van desde la subestación eléctrica, pasando por las líneas que componen su estructura medular, hasta el domicilio u oficina del cliente. PLC representa a un conjunto de elementos y sistemas que se basan en una plataforma de transmisión ya existente y que cuentan, además, con una gran cobertura a lo largo de cualquier territorio en el mundo. Con el apoyo de lo afirmado recientemente, no sería descabellado pensar en este medio como el indicado para cubrir los vacíos que las tecnologías anteriores no pudieron llenar.

A continuación se desarrolla, sobre la base de diversas fuentes de información, un estudio acerca de las redes de comunicación local y las redes de acceso implementadas a partir del contexto de las líneas eléctricas. El análisis tomará lugar a partir de una información genérica que describe sus principios de funcionamiento, un estudio de los tipos de transmisión involucrados y una descripción acerca de la infraestructura que respalda toda la tecnología en estudio.

Por otro lado, se buscará ahondar en el modelo lógico a partir del cual se maneja esta solución, con el estudio de los equipos que la componen y la identificación de las principales dificultades que tiene que afrontar en el proceso de transmisión de información. Esto último dará paso al análisis del sistema de transmisión escogido para PLC (nivel físico) y permitirá seguir con el desarrollo de sus características relacionadas a la capa de enlace.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Como síntesis presentamos un análisis global del sistema de comunicación por PLC, describiendo sus usos actuales y aquellas futuras investigaciones y campos en los cuales puede desarrollarse como herramienta de solución de problemas.

2.2. Fundamentos Teóricos acerca de la Tecnología PLC

2.2.1. Estructura General

La tecnología PLC utiliza las redes de distribución de electricidad para la transmisión de datos a pesar de no haber sido diseñadas para ese propósito. Su despliegue utiliza el tendido eléctrico de media y baja tensión. Para este último sector, PLC cubre desde el transformador existente en el centro de distribución hasta el enchufe eléctrico en casa del abonado [9].

La energía eléctrica llega a los usuarios en forma de corriente alterna de baja frecuencia (50 ó 60 Hz). Para la transmisión de datos, voz y vídeo, PLC utiliza alta frecuencia (1,6 - 30 MHz); sin embargo, la respuesta del canal es todo lo contrario a la ideal: es variante en el tiempo dependiendo de la carga (del consumo de energía en cada momento) y tiene grandes fluctuaciones en frecuencia; es decir, es hostil y muy ruidosa. A estas frecuencias de trabajo la señal sufre una gran atenuación con la distancia y la función de transferencia del canal presenta desvanecimientos selectivos.

Por todo ello se hace imprescindible utilizar sistemas de modulación muy robustos y adaptativos a las características del canal [28]. En tal sentido, es relevante destacar que actualmente no hay estándares que seguir, aunque si un grupo de sistemas (incompatibles entre ellos) caracterizados por la modulación de la señal empleada.

Esencialmente se utilizan tres tipos de modulación [29]:

- DSSSM (*Direct Sequence Spread Spectrum Modulation*), o simplemente DSS se caracteriza porque puede operar con baja densidad espectral de potencia.
- OFDM (*Orthogonal Frecuency Division Multiplex*), que utiliza un gran número de portadoras con anchos de banda muy estrechos.
- GMSK (*Gaussian Minimum Shift Keying*), optimiza el uso del ancho de banda.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

El DSS, o técnicas de espectro disperso, tiene como ventaja la robustez frente a las interferencias de banda angosta, la posibilidad de realización de CDMA (Code Division Multiple Access) y su operación con un bajo nivel de energía a lo largo del rango de frecuencia reduce los problemas de compatibilidad electromagnética (EMC). Para mayor información sobre EMC revisar la sección 3.3 de la bibliografía [32].

Sin embargo DSS tiene una pobre eficiencia espectral y es sensible al desvanecimiento selectivo de la frecuencia. Por este motivo es necesario aumentar la complejidad de las señales para la ecualización en las conexiones de punto a multipunto. Por otro lado la técnica OFDM permite una gran reducción en la complejidad del ecualizador del canal y un incremento en la resistencia a las señales de distorsión. Una descripción detallada del sistema OFDM, junto con sus propuestas de transmisión y esquemas de modulación son presentadas extensamente en la sección 4.2 de la bibliografía [32] y abordado más adelante en la sección 2.2.5.1.

OFDM se adapta dinámicamente a las condiciones del canal monitorizando cada 10ms las condiciones de relación señal a ruido (SNR) de cada portadora y adaptando en función de ésta la tasa de bits a transmitir por la misma (véase figura 2.1).

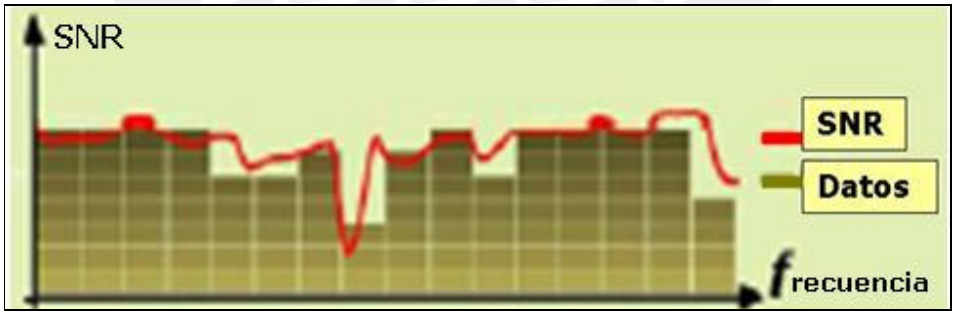


Figura 2.1. Adaptación de OFDM a las Condiciones del Canal [33]

La capacidad de transmisión del PLC también varía en función del fabricante, aunque un promedio suele establecerse en 45 Mbps (27 Mbps en el sentido red-usuario y 18 Mbps en el sentido usuario-red). Sin embargo, los circuitos integrados de segunda y tercera generación han elevado el límite por encima de los 130 y 200 Mbps respectivamente, lo que le permite al PLC competir con ventaja con otros sistemas de comunicación de banda ancha [29].

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

La evolución de estas tecnologías a lo largo del tiempo, toma lugar en la figura 2.2.

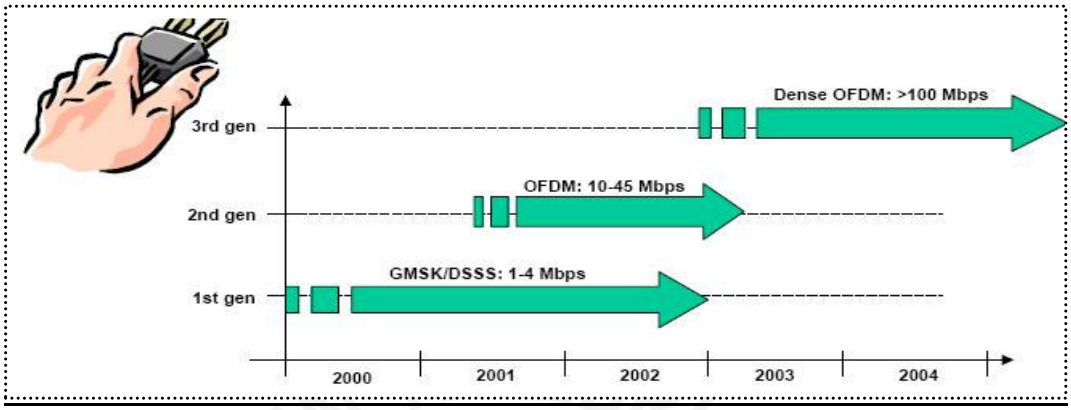


Figura 2.2. Evolución de las Tecnologías de Modulación [34]

2.2.2. Ámbito de PLC: Red de Distribución Eléctrica [9]

Las redes eléctricas pueden dividirse conceptualmente en varios tramos:

- Un primer tramo de Media Tensión (entre 15 y 50 Kilovoltios) que abarca desde la central generadora de energía hasta el primer transformador elevador.
- Un tramo de Transporte o de Alta Tensión (entre 220 y 400 Kilovoltios) que conduce la energía hasta la subestación de transporte.
- Tramo de Media Tensión (de 66 a 132 Kilovoltios) entre la subestación de transporte y la subestación de distribución.
- Otro último tramo de Media Tensión (entre 10 y 50 Kilovoltios) desde la subestación de distribución hasta el centro de distribución.
- Y por último la red de Baja Tensión (entre 220 y 380 Voltios) que distribuye la energía dentro de los centros urbanos para uso doméstico, comercial e industrial.

La zona de aplicación del PLC involucra estos dos últimos tramos de la red eléctrica, la Media y la Baja Tensión (ver figura 2.3). La Baja Tensión se utiliza como una auténtica red de área local; mientras que la Media Tensión hace las veces de red de distribución, transportando los datos hacia la red WAN del proveedor de Internet [9].

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

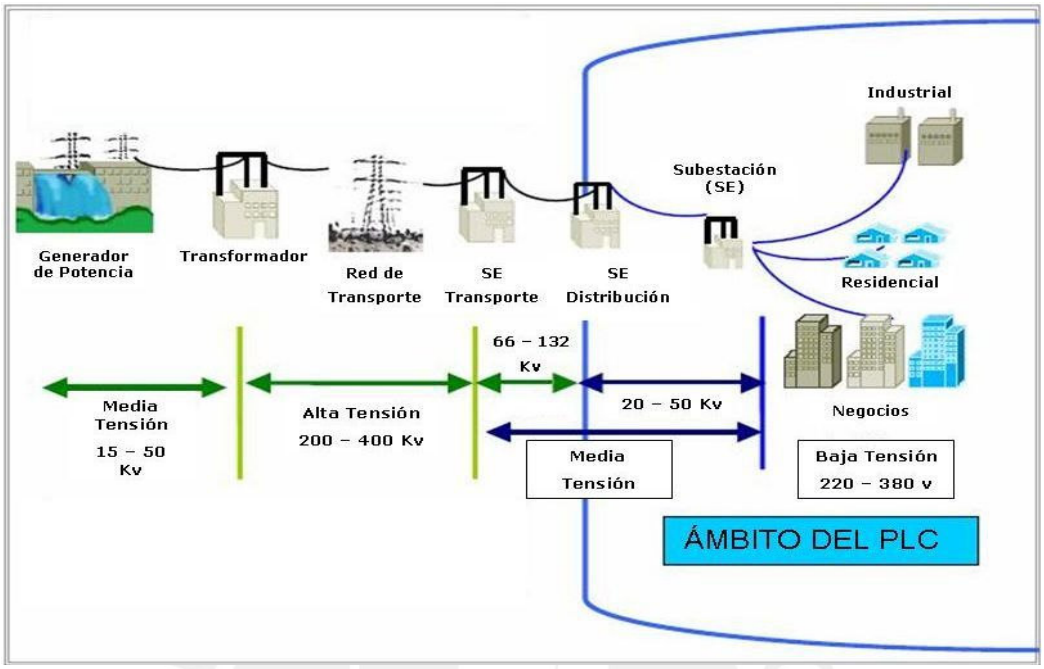


Figura 2.3. Red Eléctrica y PLC [9]

En general se puede decir que los factores de impedancia y ruido son mucho menores en las líneas de alta tensión en comparación con las de baja. Esto debido a que las primeras han sido diseñadas con cableados de mayores prestaciones; es decir, sus diámetros son más amplios y el metal con el que están fabricadas es más consistente. Las redes de baja tensión, sin embargo, son consideradas las más adaptables a los sistemas PLC dado que requieren menores distancias para la transmisión y no se necesita de rutas alternas para evitar transformadores intermediarios [42].

2.2.3. Arquitectura de Red

De manera general, el sistema de comunicaciones sobre la red eléctrica consiste en una red full dúplex punto a multipunto con los elementos siguientes:

• El Head End (HE)

Es el componente principal en la topología de una red PLC, conocido también como módem de cabecera. Este equipo actúa como maestro de la red ya que autentica y coordina la frecuencia y actividad del resto de equipos que la conforman; su función está orientada a mantener siempre constante el flujo de datos a través de la red.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Además, el HE permite conectar el sistema con la red externa (WAN, Internet, etc.) por lo que es el interfaz adecuado entre la red de datos y la red eléctrica. La elección de su ubicación es un aspecto clave en la arquitectura de red, ya que es esencial que la inyección de datos se produzca de manera ventajosa y permita proporcionar la máxima cobertura posible dentro de la red [29].

Estos módems de cabecera se suelen colocar en la estación transformadora de media a baja tensión, de esta manera los datos pueden ser inyectados hacia toda la red de suscriptores a partir de un único punto de conexión.

La última generación de HE's presenta una configuración flexible basada en la instalación de diferentes tarjetas electrónicas, entre las cuales destacan los siguientes tres ejemplares [31]:

- Tarjeta de baja tensión: Inyecta la señal PLC en la red de acceso a través de los cables de Baja Tensión.
- Tarjeta de media tensión: Se usa para la comunicación con los HE de las otras subestaciones incluidas en la red de distribución.
- Tarjeta de Fast Ethernet o Gigabit Ethernet: Usadas para permitir la interconexión con otras redes existentes (fibra óptica, XDSL, LMDS, etc.)

• Equipamiento de Abonado (CPE)

El CPE (Customer Premises Equipment), también conocido como adaptador o módem de usuario, permite conectar un equipo a la red de datos establecida gracias al Head End. Su misión es convertir cada toma eléctrica en un punto de red al cual poder conectar un equipo informático [29].

Los datos son transmitidos desde el CPE al HE, el CPE es el esclavo en la red y su acceso ha debido ser autorizado previamente por el maestro (HE). Este último, también asigna intervalos específicos de frecuencia o tiempo en el canal de comunicación a diversos CPE' s para permitirles transmitir simultáneamente [30].

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Los módems PLC están divididos interiormente en una parte digital y una parte analógica. La parte digital es responsable del esquema de modulación y la codificación de algoritmos sobre los datos. Por otro lado, la parte analógica representa la sección más importante ya que incluye los elementos para el acoplamiento y las unidades de transmisión/ recepción. La sensibilidad de esta unidad tiene un mayor impacto sobre la distancia que la señal PLC puede cubrir (80 metros en promedio para el módem)[42].

Tanto el HE como el CPE poseen una serie de elementos encargados de filtrar y separar la corriente alterna (50-60 Hz) de las señales de alta frecuencia, que son las que soportan los servicios de vídeo, voz y datos [29].

• El Home Gateway (HG)

Como se evidencia en la figura 2.4, el HG sirve como una estación base local que controla la red, coordinando la comunicación entre los módems internos. Dicho de otro modo, el HG actúa simultáneamente como maestro de los CPE' s en una red local y como uno de los esclavos del HE para la red de acceso.

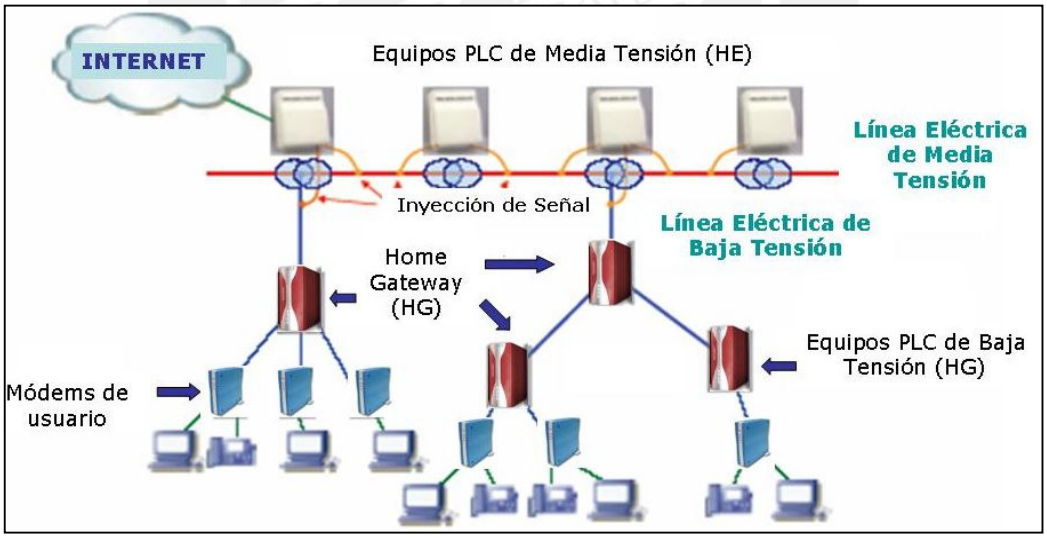


Figura 2.4. Arquitectura de Red PLC [9]

Conocido también como repetidor, es una combinación de un CPE y un HE, amplifica la señal transmitida a grandes distancias (mayores a 300 metros) o donde exista excesiva atenuación y trabaja incluso como un router para implementar una LAN domestica [30].

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Un HG es usado para dividir una red de acceso y una red PLC de área local ('in home'). Es decir, ajusta las señales transmitidas entre las frecuencias que están especificadas según su uso en redes de acceso o locales; de esta manera los módems PLC conectados al interior de una red local pueden comunicarse internamente sin la necesidad que fluya información hacia la red que cubre el área de acceso [32].

Este dispositivo se encarga de hacer de puente en los tableros de tarificación para darle paso a la señal de datos de alta frecuencia; de este modo distribuye la señal PLC desde la acometida general entre cada una de las acometidas individuales. Este elemento cumple, además, la función de arbitrar el acceso al medio entre todos los módems o dispositivos PLC instalados en el edificio, pudiendo atender hasta un máximo teórico de 256 módems [9].

2.2.4. Fuentes de Interferencia y Ruido bajo las Líneas de Potencia

Dado que los circuitos de transmisión eléctrica no fueron creados para propósitos de comunicación, la transmisión de señales a altas frecuencias por ese medio se vuelve un reto para el desenvolvimiento de esta tecnología [10].

Una serie de investigaciones llevadas a cabo como consecuencia de lo recientemente señalado, han sido orientadas a la búsqueda de un modelo más adecuado para la red de potencia de manera que se comporte como un verdadero canal de comunicación; observando que la necesidad de adaptación y la atenuación de interferencias denota un proceso íntimamente ligado al ámbito de las frecuencias.

En general, la comunicación sobre las líneas de potencia se presenta difícil por factores relacionados básicamente a tres elementos:

a) Fuentes de Ruido sobre las Líneas de Potencia [4].-

La interferencia por fuentes de ruido se acopla directamente en la señal de datos y se llega a extremos de pérdida o distorsión de la información. Las fuentes de ruido incluyen interferencias eléctricas y electro-mecánicas (siendo los motores y bobinados en general la principal fuente).

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Los conmutadores y lámparas halógenas fluorescentes están también dentro de este grupo creando ruido impulsivo sobre los ciclos de 60 Hz. Las fuentes de energía crean armónicos relacionados a esta frecuencia fundamental, lo que sumado a las transmisiones externas como la interferencia RF de medios radiales, generan un efecto negativo en la calidad del canal de la línea de potencia.

b) El Efecto 'Multipath' [4].-

Las reflexiones de la señal original (datos) sobre el medio de transmisión pueden acarrear ligeros desfases que el receptor puede tomar como un símbolo erróneo dado que aquello no fue exactamente lo que se transmitió. Los efectos de la distorsión 'Multipath' varían según las características físicas del medio, los cuales son dependientes de las variaciones en la carga. Con ello, la combinación de esta distorsión, con las topologías complejas del cableado y las características de la línea, crean una tediosa función de transferencia del canal.

c) Rango de Conexión Dinámico [4].-

La atenuación de la señal puede ocurrir debido a topologías físicas de la red al interior de una casa u oficina; es decir las variaciones de impedancia (diferentes distancias entre nodo y nodo), los diferentes tipos de cargas en cada tomacorriente provocan una heterogeneidad en el comportamiento del medio físico que soportará la información digital.

Las herramientas de comunicación sobre las líneas eléctricas necesitan, por tanto, un poderoso código de detección y corrección de errores; lo mismo que se logra con una técnica de modulación adecuada que se analizará en las líneas sucesivas.

2.2.5. Proceso de Transmisión : Modo de Funcionamiento

2.2.5.1. Sistemas de Transmisión en Banda Ancha

Los problemas analizados en cuanto al canal de comunicación y las interferencias electromagnéticas requieren, como hemos visto, que el esquema de modulación adoptado encare con efectividad estas adversidades. Al igual que la técnica DMT de ADSL, PLC utiliza codificación OFDM para transmitir los datos. Esta modulación es la más inmune a las interferencias presentes en las redes eléctricas y aporta el mayor

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

nivel de rendimiento y eficiencia espectral [4], [10].

El método requiere cálculos complejos como la transformada rápida directa e inversa de Fourier lo que origina un mayor costo en la implementación. En los sistemas basados en espectro disperso (DSS), por el contrario, la onda portadora es transmitida por dispersión sobre toda la banda de frecuencia y la señal original es recuperada nuevamente en la etapa de recepción; por este motivo, aquí se requiere sólo un procesamiento de cálculo simple y el costo se ve atenuado considerablemente, sin embargo actualmente su velocidad de transmisión no es tan rápida como la que presenta OFDM [5].

El sistema de múltiples portadoras, OFDM, es eficiente y flexible para trabajar en un medio como la red eléctrica. Su rango espectral queda dividido para trabajar en intervalos y el ajuste de cada uno de ellos permite que los equipos se adapten dinámicamente a las condiciones del medio, potenciando así aquellas frecuencias donde el ruido es menor y anulando aquellas donde el ruido es elevado [29].

Otro punto a ser considerado es que la banda del orden de los MHz (sobre la cual trabaja PLC) es usada para difusiones de onda corta y radioaficionados. Es decir, la transmisión de datos sobre PLC originaría emisiones electromagnéticas contraproducentes a las aplicaciones externas. Ahora, si consideramos que el tipo de cableado no apantallado de las redes eléctricas no atenúa esas interferencias; es necesario suprimirlas únicamente con técnicas adecuadas de transmisión.

Por tal razón, los autores adoptaron el sistema OFDM, el cual permite controles de salida para cada portadora. Más aún, el mecanismo de ventana OFDM permite el ajuste programable de un determinado rango con un declive de hasta 30 dBs con una despreciable pérdida en la calidad de la señal de datos aledaña [24].

En este sistema, numerosas frecuencias portadoras (desde el orden de las decenas hasta unos cuantos millares) son densamente superpuestas. De tal manera que, los extensos símbolos OFDM pueden transportar desde 917 hasta 1536 portadoras. Cada una de éstas, a su vez, pueden transportar tasas de bits que van desde la unidad (en caso de la modulación BPSK) hasta 10 bits de información por portadora para el caso de la modulación 1024 QAM. La elección del tipo de modulación a emplear es

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

independiente para cada portadora y dependerá de las características del canal entre el transmisor y el receptor. En general se usa la siguiente premisa: “Los parámetros de transmisión para cada par transmisor/receptor son adaptados en tiempo real. La relación señal a ruido (SNR) es medida para cada portadora y con ello, el sistema escoge la modulación adecuada para lograr la máxima velocidad de transmisión mientras se mantenga el BER deseado” [24].

La ortogonalidad brindada por OFDM permite, además, el traslape espectral para mejorar la eficiencia a casi el doble sobre los sistemas de banda ancha con portadoras únicas. Lo señalado se aprecia en la figura siguiente:

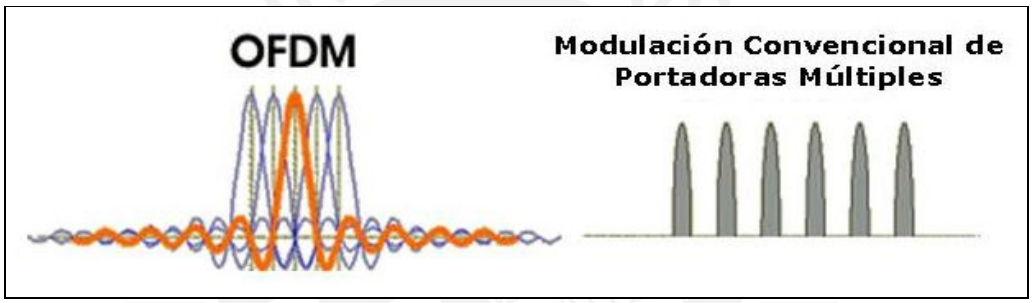


Figura 2.5. El Espectro de OFDM se Traslapa [34]

2.2.5.2. Eficiencia de la Capa de Enlace

Los sistemas PLC tienen que ofrecer una muy buena utilización de la red sobre el medio de transmisión compartido y garantizar, al mismo tiempo, una satisfactoria calidad de servicio (Quality of Service: QoS) exigida por aplicaciones como la transmisión de voz sobre IP (VoIP) y la de vídeo en tiempo real (‘video streaming’). Ambos requerimientos pueden ser logrados con la aplicación de capas de enlace eficientes; para ello se trabaja con tres capas superiores a la capa física, la capa MAC (algoritmos de acceso al medio), la capa LLC (formatos de trama y control de errores) y la capa de Convergencia (Encapsula a data en paquetes PLC a partir de las tramas Ethernet). Capas que, a su vez, son manejadas por una Capa de Administración.

a) Capa MAC [32]

La funcionalidad de la capa MAC (control de acceso al medio) es administrar el acceso al canal de comunicación. Se desarrolla en un entorno de red que considera múltiples

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

suscriptores, los cuales, en un mismo intervalo de tiempo, manejarán diversos servicios de comunicación; por tanto la capa MAC debe asegurar, por un lado, la utilización dinámica y por otro, prevenir colisiones entre paquetes de distintas fuentes.

La mayoría de los esquemas de acceso en las actuales redes PLC implican la técnica TDMA (Time Division Multiple Access). Los paquetes de datos pueden ser segmentados en pequeñas unidades y transmitidos a lo largo de la longitud de un intervalo de tiempo especificado por este esquema (ver figura 2.6). De esta manera, si ocurre alguna interferencia sólo los segmentos de datos erróneos son retransmitidos, consumiendo así una menor capacidad de red.

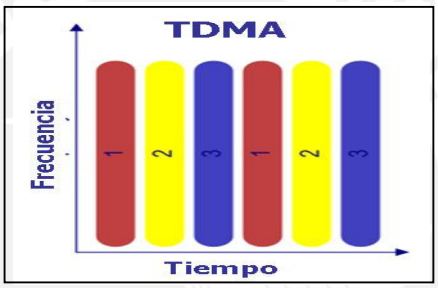


Figura 2.6. Esquema de Acceso TDMA [34]

La segmentación TDMA asegura un mejor desenvolvimiento de QoS y trabaja, además, con dos esquemas de acceso: fijo y dinámico. Estos a su vez manejan una serie de algoritmos de acceso que se resumen a continuación:

i) **Acceso Fijo.-** Involucra el esquema TDM usado en la telefonía clásica.

ii) **Acceso Dinámico.-** Se divide a su vez en tres subgrupos de protocolos:

- Protocolos de Contención, asume el uso aleatorio del canal y se enfrenta al problema de colisiones cuando dos o más estaciones transmiten sus datos al mismo tiempo. Destacan los protocolos CSMA/ CD y CSMA/ CA.

- Protocolos de Arbitraje, las estaciones tienen un acceso dedicado al medio por un intervalo de tiempo predeterminado y asignado según el nivel de prioridad de los datos. Presenta problemas para trabajar en tiempo real y destacan el Pooling (topología de árbol como la de PLC) y el Token Passing (cuando de trabaja con topología en anillo).

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

- Protocolos Híbridos, mejoran el desempeño de las aplicaciones considerando un intervalo de contención y uno de arbitraje de acuerdo al estado de la red.

Una solución efectiva es también el método FDMA ilustrado en la figura 2.7 (Frecuency Division Multiple Access); en este caso, la transmisión se hace considerando intervalos de frecuencia para cada usuario que quiera transmitir en un mismo instante de tiempo. Una de sus ventajas es que las frecuencias particulares pueden ser eliminadas si se encontrasen afectadas por el ruido externo. Este esquema se emplea para diferenciar tráficos de subida (upstream) y bajada (downstream) bajo el sistema conocido como FDD; además es útil para segmentar las frecuencias asignadas para el tráfico local y para el tráfico al interior de la red de acceso.

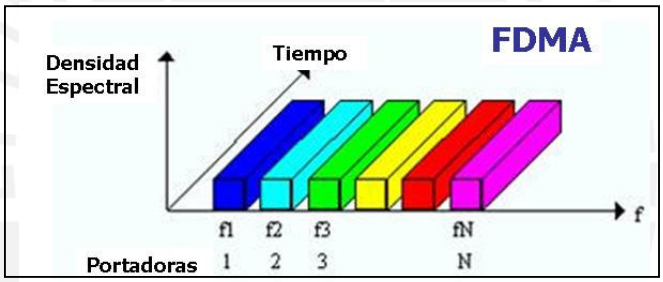


Figura 2.7. Esquema de Acceso FDMA [34]

De acuerdo a ello, una combinación TDMA/FDMA parece ser una solución razonable para las redes PLC (figura 2.8). Aplicaciones de la técnica FDMA en los sistemas basados en OFDM produce los esquemas OFDMA (acceso OFDM), el cual puede ser también combinado con el TDMA desarrollando el sistema OFDMA/ TDMA.

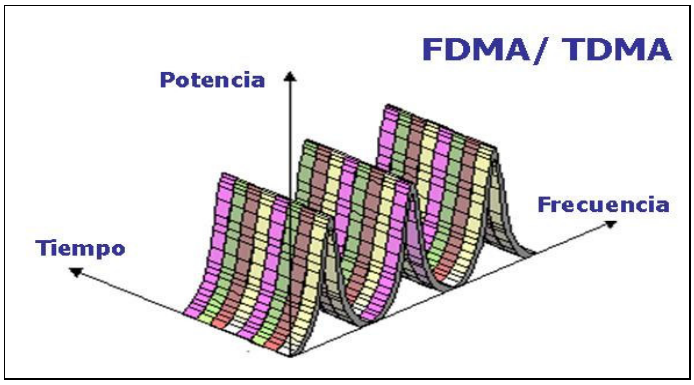


Figura 2.8. Esquema de Acceso FDMA/ TDMA [34]

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

b) Capa LLC [24]

Asegura la transmisión de datos libre de errores entre pares de nodos PLC. Esto se logra a través de la transmisión de una carga de datos codificada provista por la capa de convergencia en secuencias de código de palabras (paquetes).

Homeplug y Opera, entidades que agrupan a los principales fabricantes de equipos PLC, modelan un formato de tramas basado en el estándar IEEE 802.3 (Ethernet), lo cual simplifica la integración con este formato ampliamente extendido. En otros términos, los equipos bajo estas especificaciones reciben una trama Ethernet y le añaden una cabecera extra. El nuevo paquete es dividido en múltiples secciones para conformar cada una, un código de palabra; en este caso se le agrega a cada división un pequeño código de redundancia según el patrón Reed-Solomon para luego aplicarles un nuevo bloque identificador (estas cabeceras manejan información que se necesitará más adelante cuando se reensamble los códigos en una trama Ethernet original). Finalmente, un grupo de códigos de palabras son concatenados en un solo gran paquete powerline.

c) Capa de Convergencia

Su función es encapsular los paquetes que vienen de una aplicación externa (típicamente las tramas Ethernet 802.3) antes de pasarlas hacia la capa LLC para su transmisión.

d) Capa de Administración

El esquema de acceso PLC considera excepciones a los mecanismos vistos anteriormente. Esto es, considera la importancia de ciertos paquetes agrupándolos en cuatro esquemas de prioridad (remitirse a la información en el anexo número 2 para mayor detalle sobre el estándar Homeplug):

- Prioridad 3: Aplicaciones de voz sobre IP.
- Prioridad 2: Transmisión de audio y vídeo.
- Prioridad 1: Transferencia de datos.
- Prioridad 0: Tráfico con algoritmo del mejor esfuerzo.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Debido a la naturaleza asimétrica y cambiante del tráfico de datos en las áreas de acceso, la capa de administración usa esquemas dúplex dinámicos que se adaptan al estado actual de congestión de la red. Por este motivo, los sistemas PLC tienen que implementar estrategias organizadas de tráfico, las cuales incluyen el control de conexión (CAC) que se encarga de limitar el número de suscriptores activos, con lo cual asegura una satisfactoria QoS para las conexiones actuales admitidas. En este sentido una parte de los recursos de la red tienen que ser reservados para una posible reutilización en caso de interferencias externas dañinas [32].

2.2.6. Ventajas y Desventajas

Como todo medio de transmisión de datos, la tecnología PLC cuenta con aspectos positivos y negativos, aquellos definen sus características particulares y permiten inferir acerca de su desempeño en diversas aplicaciones. De esta manera, como parte del objeto de estudio, se describirá de manera concisa y organizada los factores ventajosos y perjudiciales que presenta:

a) Ventajas [11]

- Prácticamente ubicuo, la red eléctrica es aún más extendida que la red telefónica, por lo que se podría llegar a cualquier punto residencial.
- No existirían costos de desarrollo de “última milla”, ya que la red ya está desplegada.
- Permite la transmisión de datos a alta velocidad, siendo un soporte válido para el ancho de banda requerido a nivel residencial.
- Las velocidades probadas alcanzables manejan cifras que bordean los 200 Mbps (troncales), lo que es un ancho de banda respetable.
- Permite la creación “gratuita” de una red local dentro del edificio o vivienda.
- Puede ser una alternativa real de ADSL y cable, por lo que incrementaría la competencia.
- Cualquier enchufe del domicilio se convierte en un punto de acceso a la red.
- Permite la concepción de una nueva prestación en domótica: control y automatización de electrodomésticos en el hogar, vía remota y desde cualquier rincón del mundo.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

b) Desventajas [11]

- Estandarización inconclusa, por lo que las empresas importantes son aún reacias a invertir del todo por temor a perder su inversión.
- No existe marco legal regulador uniforme en nuestro país.
- Desde un punto de vista tecnológico los canales PLC presentan numerosos inconvenientes:
    - Baja impedancia, están pensados para transmisión de electricidad, lo que implica altas potencias de emisión.
    - Muy alta atenuación a altas frecuencias, no están pensados para transmitir datos, por lo que sólo se pueden usar en distancias cortas.
    - Puede no existir tierra, problemas con las referencias.
    - Medio muy ruidoso y no está protegido con cables apantallados.
    - Los electrodomésticos están conectados al mismo medio de transmisión de datos, por lo que se producen variaciones de impedancia asíncronas cada vez que se encienden o se enchufan.
    - La propia tecnología PLC crea interferencias. Con un espectro saturado se pueden usar bandas de frecuencias de radioaficionados y otras.

2.2.7. Modelo Teórico

La concepción de la red de acceso PLC como una alternativa viable dependerá de muchos factores, los cuales pueden ser manejados de manera inherente por esta tecnología o por el entorno que en ella se avizora. Ver figura 2.9.

En tal sentido cabe señalar, por ejemplo, que dos de los factores primordiales para que un avance tecnológico tenga impacto y beneficio en la sociedad, es manejar siempre un ideal de eficiencia y eficacia del servicio dentro de un contexto global.

El concepto de eficiencia se resume como el uso racional de los medios con que se cuenta para alcanzar un objetivo predeterminado con el mínimo de recursos y tiempo disponibles. Para ello la tecnología PLC ha desarrollado herramientas a nivel hardware como los circuitos integrados y FPGA' s que hacen de la labor de conversión de datos y adaptación de la señal al medio, un procedimiento rápido, seguro y reducido a nivel de costos y espacio. A la par, la amplia extensión de la red eléctrica colabora notablemente en hacer que su cobertura de difusión sea inimaginable a lo largo de

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

casi todo el territorio nacional y que se evite altos costos de implementación.

El concepto de eficacia se define como la capacidad para cumplir en el lugar, tiempo, calidad y cantidad los objetivos establecidos. Dentro de este contexto se debe resaltar la labor irrefutable que lleva a cabo el método de modulación elegido como el OFDM que permite, entre otras ventajas, atenuar las interferencias y ruidos externos y conseguir grandes rangos de velocidad de comunicación. Es fundamental, además, el surgimiento de estrategias, protocolos y arquitecturas de transmisión que hacen de la red eléctrica un verdadero soporte de las redes multimedia.

La tecnología de acceso PLC presenta además una serie de características que la resaltan como una seria alternativa de comunicación en un futuro próximo. Dicho de otro modo, la presencia de las tecnologías XDSL en la actualidad le dan un soporte y un punto de apoyo sobre el cual pueda desarrollarse, lo que hace que PLC sea concebido en la actualidad como un medio adaptable a mejoras. Es más, la interfaz de comunicación a través de las líneas de potencia puede impulsar a nuevas prestaciones en el campo de la domótica, como la de manejar los aparatos electrodomésticos a distancia e interconectarlos entre sí para que cumplan una determinada labor de manera automatizada.

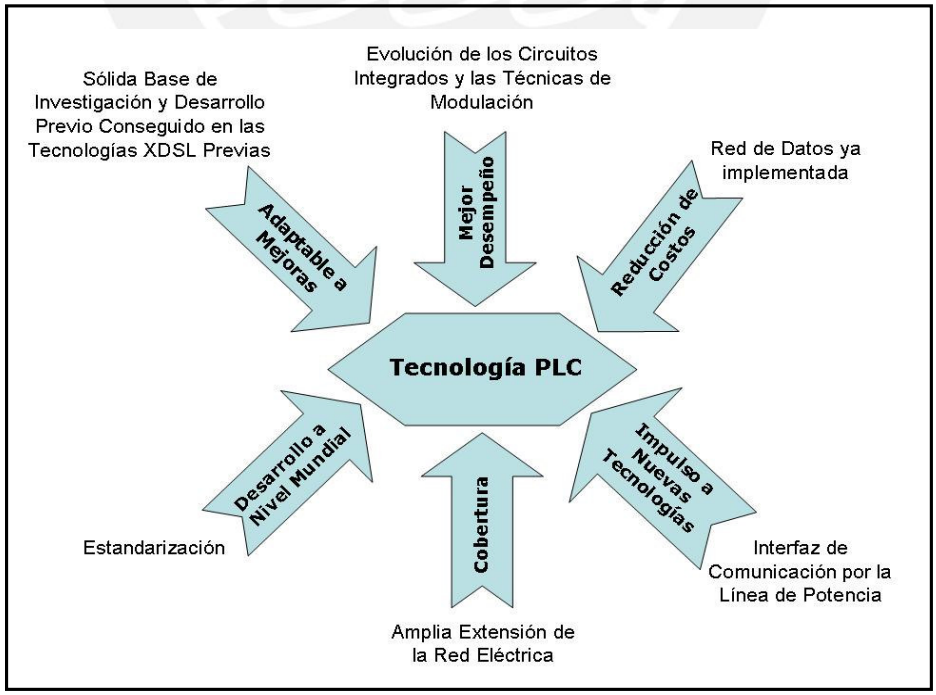


Figura 2.9. Representación Gráfica del Modelo Teórico

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

2.2.8. Síntesis sobre el Asunto de Estudio

Durante muchos años las compañías eléctricas han utilizado la red de alta y media tensión para transmitir datos y así cubrir las necesidades de su propio funcionamiento como la apertura remota de presas, vigilancia de redes e identificación de fallos, pero se limitaban a la transmisión de datos a bajas velocidades con fines internos.

La tecnología PLC permite la transmisión de información digital usando las mismas redes existentes de distribución. Sin embargo, esta tecnología supone una alternativa real a las actuales soluciones de 'última milla', permitiendo el acceso de usuarios finales a las redes de los operadores usando una infraestructura ya instalada que llega incluso en el interior de las viviendas, haciendo que cualquier enchufe se convierta en un posible punto de acceso a la red con sólo conectar el correspondiente módem PLC. Gracias a la banda ancha, la tecnología PLC permite la distribución de aplicaciones multimedia (datos, voz y vídeo) [28].

Si las limitaciones en el campo regulador se superan lo suficientemente pronto, PLC podría influir en la forma futura del mercado debido a su adaptabilidad frente al crecimiento mundial de las aplicaciones en Internet que necesitan anchos de bandas y cobertura superiores. Las compañías eléctricas, ayudadas por una fuerte presencia en el mercado por su red omnipresente, pueden acelerar fuertemente el ritmo con que los distribuidores alternativos de bucle local ocupan cuotas de mercado que ahora dominan los operadores oficiales de telecomunicaciones. Esta tecnología podría, por tanto, considerarse como un impulsor de la competencia en un sector en el que hasta ahora la competitividad de los distribuidores locales ha sido difícil y como un catalizador de la sociedad de la información.

Las pruebas demuestran que PLC es una tecnología válida y que incluso puede incursionar en posible aplicaciones como [7] :

- Servicios de telefonía: Local y a larga distancia, incluyendo videoconferencia.
- Próximos servicio de comunicaciones: E-commerce, atención médica desde el hogar, aprendizaje a distancia, etc.
- Servicios residenciales: Seguridad en el hogar, automatización de edificios a distancia, etc.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Finalmente se debe aclarar que ésta, por ser una tecnología relativamente nueva, urge de un estándar para que su servicio sea normado y por tanto capaz de imponerse en el mercado global.

2.3. Definiciones Operativas [32]

Una red PLC es usada para la realización de varios servicios de telecomunicaciones, por tanto las capas de red especificas deben asegurar la realización de estos servicios a través de la interacción con la pila de protocolos del modelo OSI.

2.3.1. Soporte de los Servicios PLC

Una red PLC puede ser considerada como una portadora de servicios que brinda plataformas de comunicación a los suscriptores que conforman las redes de suministro eléctrico de baja tensión. Permite además la interacción con otras redes de servicios como redes de telefonía, red de paquetes X.25, redes ATM, entre otras. Los usuarios juzgan a un servicio de red según la calidad de las aplicaciones que brinda. De acuerdo a esta premisa, las redes PLC tienen que ofrecer una gran variedad de servicios de comunicación, con una QoS satisfactoria y estar ávida a intercambiar información, competir y ser compatible con otras tecnologías aplicadas a las redes de acceso.

2.3.2. Clases de Tráfico

Según la clasificación para las redes UMTS, los servicios de telecomunicación están divididos en cuatro grupos: conversación, secuencia, interacción cliente / servidor y aplicaciones estáticas. Cada clase de tráfico tiene una QoS específica dependiendo de la naturaleza de las aplicaciones usadas. De acuerdo a ello, típicas aplicaciones dentro de la clase conversación (como la voz) requieren, por ejemplo, minimizar los retrasos. La clase de tráfico secuencial (como la del vídeo) necesita asegurar una secuencia de imágenes transmitidas en periodos de tiempo conocidos y predeterminados. El mismo requerimiento es necesario para el tráfico de conversación si se trabajase con paquetes de voz (Voz sobre IP).

Para la clase de tráfico interactivo (como las aplicaciones Web) la relación del tiempo con los paquetes transmitidos no es tan crítica y los retrasos no son tan influyentes.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Sin embargo, los usuarios Web esperan una respuesta de un servidor remoto dentro de un intervalo de tiempo razonable. La clase de tráfico estático tiene requerimientos de tráfico aún menos críticos e incluyen aplicaciones que pueden ser usadas por una red con una menor prioridad como los servicios de correo y la transferencia de archivos.

2.3.3. Categoría de los Servicios

Para proveer varios servicios de telecomunicaciones con diferentes características de tráfico, las redes de servicios integrados tienen que asegurar una transmisión simultánea de diversas aplicaciones con variantes en su QoS. Para este propósito, este servicio se agrupa en las siguientes tres categorías:

- Servicio garantizado (GS).- Está diseñada para solucionar los requerimientos de QoS y servicios en tiempo real como vídeo y voz. Asegura muy fuertes límites de retraso y baja pérdida de paquetes. Para esto se asigna una capacidad de red determinada mientras dure la aplicación en tiempo real.

- Carga controlada (CL).- Sirve para conexiones y servicios que pueden tolerar cierto grado de pérdidas de paquetes y retrasos mayores con relación a la categoría GS. Esta categoría no asigna una determinada capacidad a ciertos servicios, sino que busca el uso eficiente de los recursos de red.

- Servicios del mejor esfuerzo.- El control del flujo está localizado en la capa de transporte y no garantiza QoS.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

CAPÍTULO 3
DISEÑO DE LA RED PLC SOBRE UNA ESTRUCTURA RESIDENCIAL

El capítulo que se desarrollará a continuación descansa esencialmente en la utilización de herramientas basadas en la pila de protocolos IP y en la manera como éstas se relacionan para formar una red de recursos compartidos. En este caso, el medio que dará cabida a este conjunto de recursos será la tecnología PLC, analizada de manera extensa en el capítulo 2. Ambas herramientas, sin embargo, tienen una característica común basada en la convergencia hacia un mismo objetivo, destinado a resolver la problemática planteada en el primer capítulo de este documento.

Ahora bien, queda claro a estas alturas como la transmisión por las líneas eléctricas de baja tensión nos puede asegurar un medio de comunicación presto a soportar diversas aplicaciones y usuarios; nos garantiza, por otro lado, su ubicuidad a lo largo del área de interés. Resulta entonces evidente que este siguiente paso busca implementar una estructura de red a través de equipos, accesorios y esquemas de conexión con el objeto de aprovechar la red eléctrica desplegada desde hace varias décadas y que al parecer estuvieron allí todo el tiempo a la espera ser optimizadas en su uso.

Un primer paso a realizar en el sentido de todo lo antes descrito será situarnos sobre el área de interés y analizar sus características más relevantes con relación a los objetivos planteados. Luego de ello definiremos algunos conceptos claves respecto a los equipos y estándares que maneja el protocolo IP, seguidamente se trabajará sobre esquemas de conexión, organización de equipos, características de funcionamiento y diagramas de red; con lo cual se planteará una postura que cubra en gran parte las deficiencias actuales y que no sea, de modo alguno, una solución alejada de la realidad.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

Dicho de otro modo, la solución tendrá que despejar las trabas que puedan ocurrir a la hora de su implementación y de la misma forma optar por la practicidad en cuanto a las estrategias de solución, adoptando un mecanismo ligado a soluciones eficientes y económicas.

3.1. Características Físicas del Área de Interés

Tal como se detalló en el marco problemático, el área que se ha considerado para desarrollar este diseño de red es el Conjunto Habitacional Alfredo Dammert Muelle ubicado en el distrito de Surquillo. A continuación, se procederá con el estudio aproximado de sus características de manera que nos permita sentar una base sobre la cual se pueda diseñar un esquema de red.

3.1.1. Ubicación Geográfica

Antes de comenzar con los procedimientos que implican el diseño de la red y la ubicación y conexión de equipos; es importante dejar claro sobre que medio se desarrollará este planteamiento. Es decir, evaluar las características físicas sobre las cuales se desplegará la red de comunicaciones.

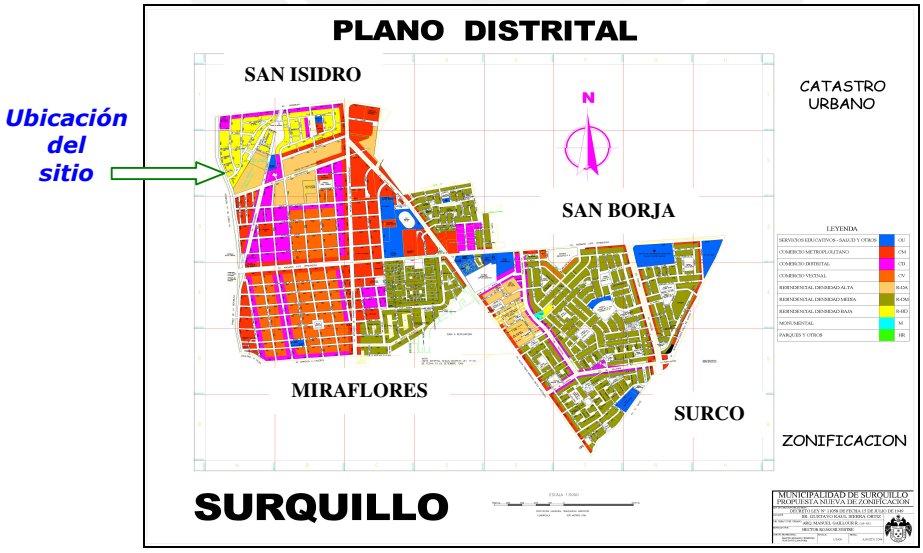


Figura 3.1. Mapa Geográfico del Distrito en Cuestión [46]

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

El área mencionada se ubica en la intersección de las avenidas Paseo de la República (altura de la cuadra 42) y Domingo Orué, ambas pertenecientes al distrito de Surquillo. De acuerdo a lo esperado con relación a los factores determinantes para la estructura de red y las características geográficas del sector (ilustradas en las figuras 3.1 y 3.2), se procede a señalar lo siguiente: la ejecución de este trabajo está destinado a implementar un diseño de red de comunicaciones sobre un Conjunto Habitacional (entiéndase como un complejo formado por edificios dentro de un sector urbano). La topología, por cierto, se define por la infraestructura ya instalada (topología de árbol) y se considera que el centro de transformación de media a baja tensión está situado a distancias prudentes respecto a los usuarios (máximo 150 metros respecto al más alejado).

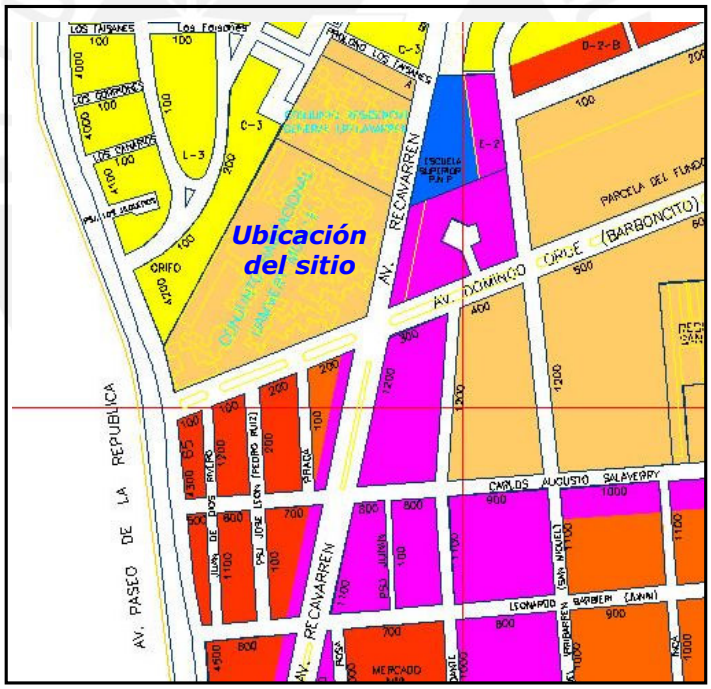


Figura 3.2. Ubicación Específica del Sector [46]

3.1.2. Características Eléctricas

Según la resolución suprema número 107-96-EM del Ministerio de Energía y Minas, el sistema de distribución eléctrica de este sector de Lima está a cargo de la empresa privada Luz del Sur S.A. Por tal motivo, y dado que el sector residencial pertenece al

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

distrito de Surquillo, se especifica que éste se acoge al suministro de esta empresa privada.

La subestación de media tensión que alimenta a este sector lo define una de las dos ternas provenientes de la línea principal de 60 KV. En este caso es la subestación San Isidro con una potencia de 40 MVA la encargada de suministrar la tensión de 10 KV a todo el sector residencial. Lo señalado se resume en la figura siguiente:

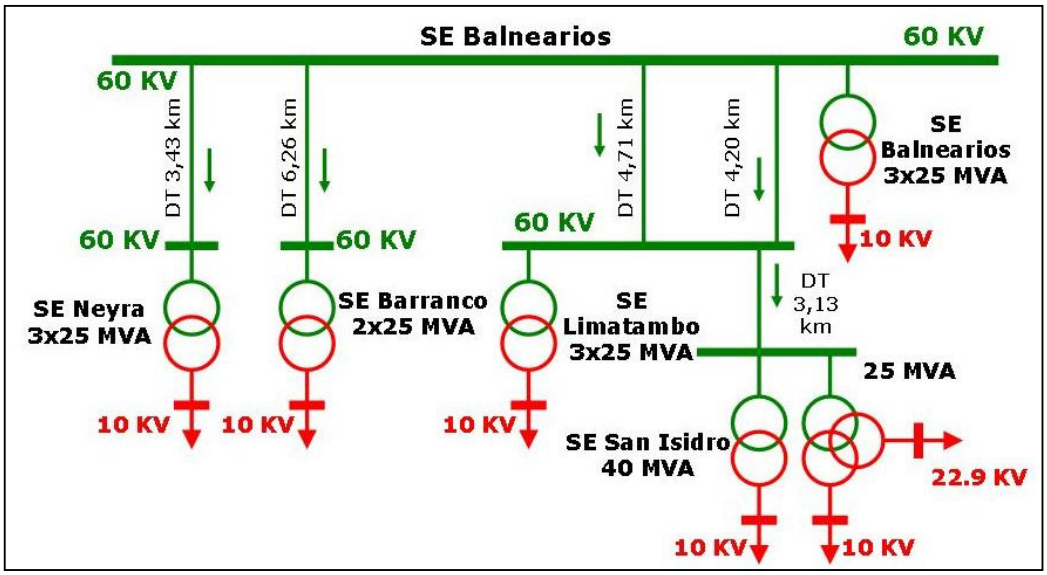


Figura 3.3. Sistema Eléctrico del Sector en Estudio

El área del Conjunto Habitacional en estudio cuenta con una subestación eléctrica cuyos valores de potencia aparente se estiman cercanos a los 630 KVA para proveer de electricidad a un sector de 10 edificios. La estación transformadora recibe las líneas de energía de media tensión (10 KV) y la transforma a 220 V para el uso dentro de cada una de las viviendas. Con relación a los diagramas eléctricos de distribución de energía, resulta prudente aclarar que no se tiene una información detallada de los mismos; sin embargo, para efectos de análisis de esquemas eléctricos de referencia, en caso de una eventual implementación; se adjunta un documento que incluye el plano eléctrico de un edificio ubicado sobre un sector residencial con similares características y su vez una descripción detallada de las características eléctricas que conforman el interior de los departamentos.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.1.3. Factores Determinantes en la Topología Eléctrica de la Red

Este tipo de redes ha sido diseñado mediante el uso de varias tecnologías (diferentes tipos de cableado, múltiples unidades de transformación, etc.) y son implementadas de acuerdo al estándar existente, el cual varía de país en país. En general depende de los siguientes factores [32]:

- **Ubicación:** Una red PLC puede ubicarse en una residencial, una industria o un área de negocios. Incluso existen diferencias si hablamos de áreas residenciales, ya sean rurales o urbanas. De acuerdo a esta clasificación variará el número potencial de usuarios por cada red eléctrica.

- **Densidad:** Los usuarios son ubicados generalmente en casas independientes (relativamente baja densidad); en edificios con un gran número de departamentos u oficinas, o en grandes centros empresariales con muy alta densidad de suscriptores.

- **Longitud de la Red:** Se refiere a la variación que existe entre la unidad de transformación y el usuario, parámetro que varía también de lugar en lugar. Generalmente hay una diferencia sustancial entre las longitudes de las redes urbanas y las rurales.

- **Diseño de la Red:** Las redes de baja tensión generalmente están constituidas de múltiples secciones de red (ver figura 3.4). En la figura se aprecia una posible estructura de red PLC. Hay, generalmente, numerosas secciones de red conectadas a la estación transformadora. Cada una de ellas puede tener diferente concentración de usuarios.

A pesar de las variantes que poseen las redes eléctricas, existe una característica que le es común a todo ese universo antes descrito; en tal sentido, tanto la red de baja tensión como sus secciones de red tienen una topología física de árbol. Es decir, la red de comunicaciones heredará la morfología del árbol que se expande proveniente de las redes eléctricas y desarrolla sobre la misma un complejo sistema de red lógico para la interconexión de sus equipos y la instauración de la red de comunicaciones.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

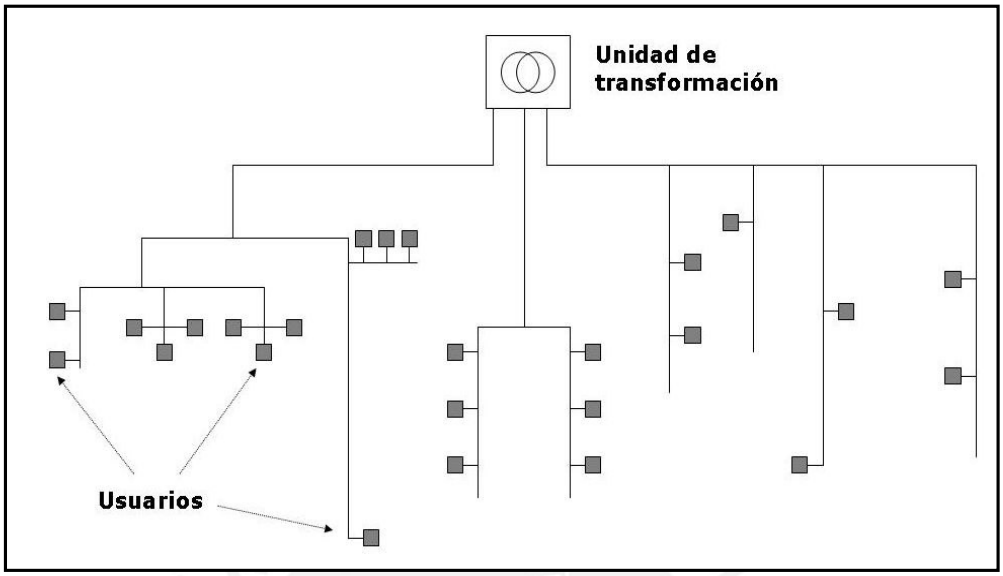


Figura 3.4. Topología de una Red de Suministro de Baja Tensión [32]

3.2. Estudio de las Herramientas de Comunicación a Utilizar

3.2.1. Protocolo IP: Conceptos Básicos

Hace algunos años, el intercambio de información a considerables distancias no concebía otra forma de ejecución que la que se hacía a través de la distribución exclusiva de canales a quienes se disponían a usarlos. Es decir, para un determinado instante de tiempo se habilitaba un espacio de comunicación a un número limitado de usuarios; sin embargo, este esquema no usa la capacidad de manera eficiente debido a que hay momentos en el que muchos usuarios 'compiten' por el medio y hay otros, en el que se libera súbitamente el canal sin que se pueda aprovechar el servicio disponible.

A diferencia de las tecnologías de red convencionales (conmutación de circuitos), el protocolo IP se basa en la transmisión de información a partir de la conmutación de paquetes. Con este procedimiento se abrió paso a un esquema totalmente distinto al tradicional, en el que se manejan segmentos con gran capacidad de ancho de banda a los que pueden acceder múltiples usuarios de manera indistinta en cualquier momento y desde cualquier parte del mundo.

Los datos viajan sobre una red en forma de paquetes IP (unidad de datos). Cada paquete incorpora una cabecera y los datos del propio mensaje; en la cabecera se

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

especifican el origen, el destino y otra información acerca del control de los datos. Entonces, cada paquete se envía a través de la red y cada nodo intermedio o router de la misma determina a donde va el paquete. Un paquete no necesita ser 'enrutado' sobre los mismos nodos por los que circularon los otros paquetes relacionados. De esta forma, los paquetes enviados entre dos dispositivos de red pueden ser transmitidos por diferentes rutas en el caso de que se caiga un nodo o no funcione adecuadamente (asegura respaldo y velocidad de transmisión) [40].

El protocolo IP es, en realidad, una familia que trabaja sobre niveles, en la que cada nivel se construye a partir del nivel inferior, añadiéndole nuevas funcionalidades. El nivel más bajo está ocupado exclusivamente en el envío y la recepción de datos utilizando el nivel de transmisión. Los superiores son diseñados para tareas específicas como son el envío y la recepción de aplicaciones en tiempo real e información de control. Los protocolos intermedios gestionan aspectos como la división de los mensajes en paquetes y el envío fiables entre los dispositivos de red [40].

Cada dispositivo tiene al menos una dirección IP que lo identifica de forma única del resto de los dispositivos de la red. De esta manera, los nodos intermedios (computadoras con capacidad de manejar tablas de enrutamiento) pueden guiar correctamente un paquete enviado desde el origen hacia su destino.

La familia del protocolo IP tiene la capacidad de adaptarse a las diversas variantes que presentan los medios de transmisión. Esto es muy ventajoso dado que las capas superiores mantienen su esquema de funcionamiento independientemente del medio que se esté usando, y son los equipos de acceso los que sirven como intermediarios para 'montar' un protocolo superior sobre otro que sea legible para cada uno de los diferentes medios de acceso. En general hay tres factores principales que crean las condiciones para la convergencia: la tecnología digital, la tecnología de transmisión y los protocolos de comunicación estandarizados.

3.2.2. Voz sobre IP (VoIP)

Es una tecnología que permite la transmisión de la voz a través de las redes IP; es decir, la voz es captada por un transductor (convierte las vibraciones sonoras a señales eléctricas). Internamente pasa por un proceso de digitalización, con el cual se habilita la opción para procesar y comprimir esta información; adicionalmente se

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

adecua los datos al formato de tramas que maneja IP, para finalmente ser transmitido casi como cualquier paquete de datos convencional.

Sin embargo, es importante aclarar que la voz, por ser una aplicación en tiempo real, se clasifica como información de alta prioridad a través de cierta información extra en las cabeceras IP. La señal vocal se transmite sobre el protocolo de tiempo real RTP (con el protocolo de control RTPC) y con transporte sobre UDP (no orientado a la conexión).

Se debe precisar, además, las diferencias marcadas entre los conceptos de voz sobre IP y telefonía IP. El primero de ellos no asegura la calidad de servicio (QoS); en telefonía IP, por otro lado, se considera medios de mayor ancho de banda con equipos que soporten QoS. La telefonía IP mantiene, por ejemplo, propuestas de redundancia de equipamiento para lograr disponibilidad elevada (con cifras del 99,99%) y calidad vocal garantizada (bajos indicadores de errores, retardo, 'jitter' y de eco) [37].

Los retardos o la latencia se deben al tiempo de procesamiento interno (verificación de errores y compresión de datos) que toma cuando la información transcurre de un equipo a otro. El 'jitter' es el efecto por el cual el retardo entre paquetes no es constante (latencia variable producida por la congestión de tráfico en la red), su presencia se soluciona con un incremento en el ancho de banda. Ambas características producen un fenómeno sobre la señal telefónica conocido como eco; para este caso se adoptó medidas estándar (ITU G.168) que considera la presencia de canceladores de eco, mediante técnicas de ecualización transversal auto adaptativas [37].

3.2.2.1. Protocolos de Sesión y Codificación Involucrados

El procesador que administra las sesiones de telefonía IP es un servidor que hace las veces de central IP; este último se basa en protocolos de señalización como H.323 y SIP. El primero de ellos (H.323) es una recomendación del ITU-T y fue una de las primeras tecnologías para las aplicaciones de voz sobre IP; permite la transmisión en tiempo real de vídeo y audio por una red de paquetes. El tráfico de señal vocal se realiza sobre los protocolos UDP/IP. La codificación de audio puede ser de diferentes tipos como G.711, G.729 y G.723.1 para las aplicaciones de VoIP. En tanto, la

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

codificación de vídeo se realiza de acuerdo con H.263. Ambos servicios se soportan en el protocolo de tiempo real RTP [37].

Por otro lado, SIP (Session Initiation Protocol) fue desarrollado por el IETF y es un protocolo más simple que H.323 (está basado en HTTP). Se creó con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el vídeo y la voz. Su función principal es la de simular las mismas características de señalización que tiene la telefonía por conmutación de circuitos. Sus prestaciones más destacadas incluyen el uso de herramientas software para reemplazar teléfonos y centrales IP con el uso de computadoras personales.

El tráfico de voz sobre IP brinda un cierto grado de 'inteligencia' a la telefonía convencional puesto que le otorga un sinnúmero de variantes como el de minimizar el consumo de ancho de banda (16Kbps mediante 'códecs' como el estandarizado G.729), aprovechar la red de datos existente (independiente del medio físico), identificador de número destino, entre otros.

Aunque, la calidad de la voz todavía no es tan eficiente como la de la telefonía tradicional; ambas redes, sin embargo, no son incompatibles gracias a los gateways de voz, con lo que su cobertura está por demás garantizada.

3.2.3. Videovigilancia IP [41]

Un sistema de vídeo en red utiliza como troncal (backbone) las redes de área local o extendidas para la transmisión de la información proveniente de sus fuentes de datos; a diferencia de los sistemas de vídeo analógicos que utilizan las líneas punto a punto dedicadas. La tecnología de vídeo en red, incluso, utiliza y amplía esta misma infraestructura para la monitorización remota y local desde cualquier parte del mundo; basándose en accesos por medio de usuarios y contraseñas, en vez de restringir el acceso físico a un monitor y a un teclado de operario.

En el entorno del vídeo digital toda la información se trata como ficheros de datos, que pueden contener secuencias de vídeo o imágenes estáticas. Estos ficheros se pueden distribuir fácilmente a un número ilimitado de receptores y por ser información digital, las réplicas y retransmisiones puede realizarse sin degradación alguna de la calidad

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

de las imágenes. Además el vídeo en red, al igual que todas aquellas que trabajan sobre el estándar IP, tiene la capacidad de proporcionar un mayor nivel de integración con otras funciones y servicios, lo que lo convierte en un sistema en continuo desarrollo.

Otro aspecto a tomar en cuenta es su practicidad, los sistemas de vídeo IP tienen la capacidad de contar con equipos diseñados para conectarse a la red y funcionar casi automáticamente ('plug and play') y la plataforma de red se puede adecuar para soportar cuantos equipos sean necesarios sin necesidad de cambiar la infraestructura existente.

3.2.3.1. Formatos de Vídeo Digital

El consumo de ancho de banda para un sistema de vídeo digital depende básicamente de cuatro factores:

- Secuencia de imágenes por segundo
- Tamaño de las imágenes
- Estándar de compresión
- Resolución de la imagen

Existe una relación directamente proporcional entre el consumo de ancho de banda y la cantidad de imágenes que se transmiten por unidad de tiempo. La figura adjunta describe a grandes rasgos esta característica:

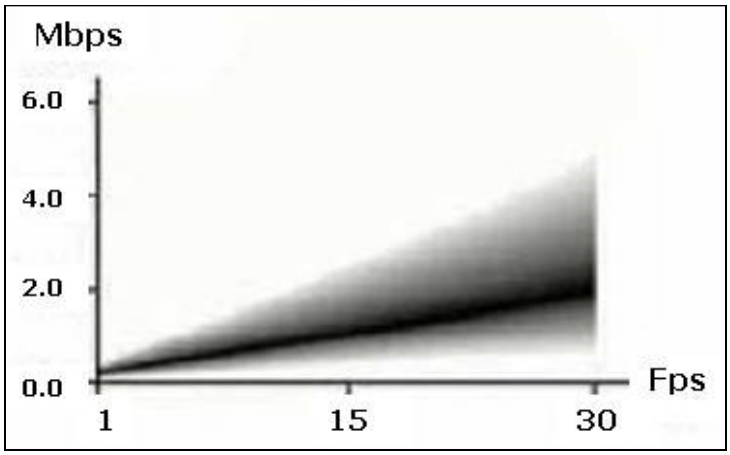


Figura 3.5. Ancho de Banda según la Transmisión de Vídeo [41]

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

El tamaño de las imágenes varía de acuerdo a la extensión del cuadro que se esté capturando y tiene dimensiones definidas como para el de los formatos PAL (720 x 576) y NTSC (720 x 486). Considera además otras dimensiones, cuya dependencia con el ancho de banda se detallará más adelante en la tabla 3.1.

Las imágenes digitales de alta resolución necesitan mayor ancho de banda para su transmisión y más espacio en disco para su almacenamiento. Sin embargo, se han desarrollado algoritmos de compresión para ayudar a asegurar transmisiones de alta calidad sobre mecanismos de menor ancho de banda. Existe un conflicto entre la tasa de transferencia de paquetes y la calidad de la imagen: JPEG, JPEG2000, MPEG-1, 2, 4, Wavelet y H.261/H.263 son todos ellos métodos de compresión que tratan con estas transmisiones.

Las factores arriba descritos pueden ser clasificados según la siguiente tabla que presenta, a manera de esquema, una información resumida acerca de las características de los principales formatos de compresión:

Esquema de compresión	BW promedio	Compresión espacial	Compresión temporal	Tamaño de cuadro	Cuadros por segundo
MPEG-4	0.5-1.2	Si	Si	720x480	25 a 30
M-JPEG	1-100	Si	No	160x120 640x480	1 a 30
H-263	1.5-2	Si	Si	1408x1152	10 a 30
Wavelet	0.1-4	Si	Si	160x120 320x240	8 a 30

Tabla 3.1. Características de los Principales Esquemas de Compresión

MPEG (Motion Picture Experts Group) es el desarrollador predominante de las normas de compresión para fuentes de vídeo digital, con MPEG-4 como la solución más reciente.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.2.3.2. Componentes de la Red de Vídeo IP [38]

Las cámaras IP, el software de red, los servidores de vídeo y, eventualmente, los teclados IP constituyen la columna vertebral de la red. A continuación se describirá las características principales de estos elementos:

a) La Cámara de Red

Las cámaras son el componente esencial en todas las instalaciones de vídeo. Este dispositivo recoge la luz y la convierte en señales eléctricas que representan a un conjunto de imágenes reconocible que puede, a partir de entonces, enviarse a través de la red. Todas las cámaras generan imágenes estáticas que se envían a un visualizador con una secuencia de imágenes por segundo. El ojo humano precisa aproximadamente 17 imágenes (o 'frames') por segundo para percibir el vídeo como en directo.

Existen dos tipos de cámaras de acuerdo a su formato de trabajo, estas pueden ser : cámaras de red fijas y cámaras de red dinámicas. Las cámaras del primer tipo proporcionan una visión estática del área que está frente a ella. Además de la unidad de cámara se necesita una lente para que la cámara opere correctamente. Por otra parte, las cámaras dinámicas o también llamadas PTZ (con movimiento horizontal, vertical y zoom) combinan en un solo producto una cámara fija, una lente de zoom, un dispositivo que permite a usuarios remotos mover la cámara para cambiar su campo de visión y una interfase de red. La cámara puede moverse tanto manual como automáticamente.

b) Software

Aunque el vídeo se puede visualizar directamente desde un navegador Web normal sin la necesidad de software dedicado, se puede usar una aplicación de software en combinación con las cámaras. Este software puede ofrecer al usuario opciones de visualización más flexibles, así como la posibilidad de almacenar y gestionar el vídeo. El software puede ser una solución autónoma para un único ordenador o una aplicación cliente/servidor más avanzada que proporcione soporte a múltiples usuarios simultáneos.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

c) Servidores de Vídeo

Son computadoras con alta capacidad de procesamiento de información y aseguran la implementación de aplicaciones de vídeo en red gracias a su poderosa habilidad de almacenamiento. Es decir, estos equipos manipulan la información proveniente de las cámaras y la distribuyen a los usuarios que la soliciten a través de un mecanismo configurable en unicast (enlace punto a punto con consumo acumulativo) o multicast (enlace lógico en topología de anillo con difusión a un grupo de usuarios en la red que comparten la misma información y al mismo tiempo). Véase la figura siguiente:

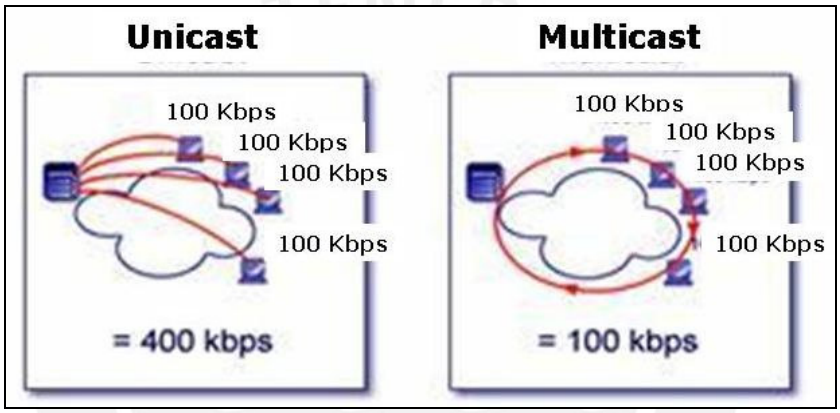


Figura 3.6. Esquemas de Transmisión en Modo Unicast y Multicast [40]

En una configuración Unicast, el servidor hace un réplica de la transmisión para cada visualizador terminal, el efecto de este método de transmisión sobre los recursos de la red es de consumo acumulativo (cada usuario que se conecta a una transmisión multimedia consume tantos kilo bits por segundo como la codificación del contenido lo permita). En una configuración Multicast, la misma señal es enviada sobre la red como una sola transmisión, pero hacia varios puntos terminales.

d) Teclados IP

Los teclados IP pueden controlar actualmente las funciones PTZ (Pan, Tilt y Zoom) de cualquier videocámara con base en su dirección IP. Como cualquier protocolo IP, las funciones de administración son incorporadas en la transmisión. Esto incluye: manejo de alarmas, grabación, capacidades de búsqueda y/o archivo, calendarización y automatización. Estas funciones de administración y control utilizan SNMP (Simple Network Management Protocol) y otros cuadros de control.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

e) Otros componentes

Además de los componentes principales descritos anteriormente existen accesorios para los sistemas de vídeo en red que, en la mayoría de los casos, son útiles para otras aplicaciones y sistemas que también están en red. Estos sistemas incluyen impresoras, almacenamiento en red, unidades de CD/DVD-RW, servidores de correo electrónico y otros, que pueden añadir un valor sustancial a la instalación.

3.3. Consideraciones Importantes en el Diseño de la Red

3.3.1. Distancias a Considerar para Evitar la Atenuación de las Señales

La determinación de las distancias óptimas no es una labor arbitraria, sino que se debe tener en cuenta una serie de parámetros que varían de acuerdo a la red eléctrica con la que se esté trabajando, el nivel de ruido existente y las pérdidas ocasionadas en la distribución de la energía.

Frente a este impedimento se puede adoptar dos estimaciones empíricas. La primera de ellas asegura la eficacia de la red sin repetidores hasta distancias de 300 metros en un ambiente libre de interferencias y de 100 metros para ambientes más hostiles (mayor concentración de usuarios y equipos eléctricos). La segunda alternativa planteada por la empresa Ascom define una relación sustancial entre la atenuación de la señal de acuerdo a la distancia para distintos rangos de frecuencia (ver el gráfico adjunto).

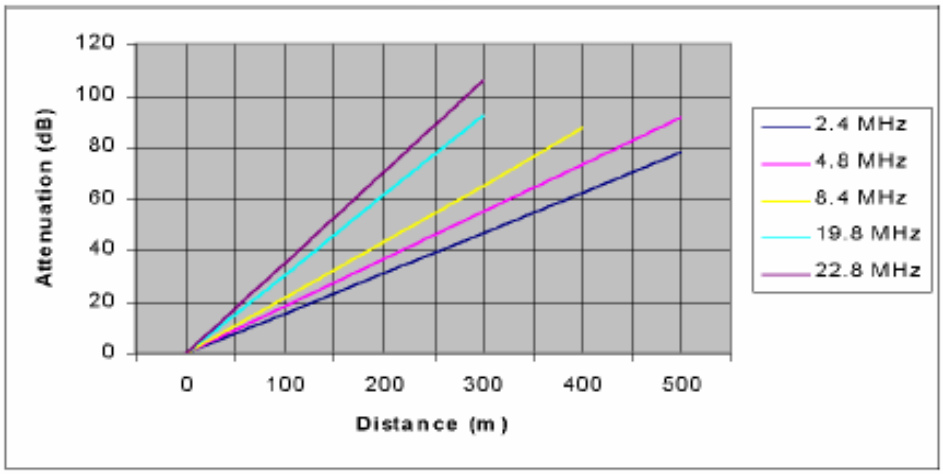


Gráfico 3.1. Atenuación de la Señal en Función de la Distancia [35]

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.3.2. Consideraciones en el Servicio de Voz sobre IP

En primer lugar es necesario definir bajo que contexto se está desarrollando este diseño de red. Es decir, evaluar las potencialidades y necesidades en el campo de las comunicaciones; al respecto, se estima que en el Conjunto Habitacional estudiado existe una población con un aproximado de 95 % de hogares con línea telefónica habilitada. Por otro lado, se sabe que casi la totalidad de las llamadas por parte de cada usuario en la residencial tiene un destino hacia el exterior de la misma; dicho en otros términos, no existe mayor tráfico de llamadas entre vecinos debido a la cercanía y a los altos costos por el uso de la telefonía pública conmutada.

Esta información nos hace pensar que no es urgente destinar los recursos de red hacia la comunicación entre los miembros de la comunidad por medio de las tecnologías de voz sobre IP, más aún si consideramos que el diseño está orientado a una solución en seguridad ciudadana por encima de cualquier otra necesidad de intercambio de información. Entonces, la comunicación de voz planteada en este diseño considera únicamente la comunicación telefónica entre usuarios y el centro de vigilancia ante la eventualidad de cualquier ocurrencia.

Siguiendo con la información estadística, se manejan cifras con un porcentaje de alrededor de 60 % de familias con una computadora en su hogar y una cifra más reducida en cuanto al número de usuarios que cuentan con servicio de Internet (30 % del total del subconjunto de familias con computadoras); es decir, aproximadamente la quinta parte del complejo residencial cuenta con una conexión a Internet. A raíz de estas cifras se puede pensar en el uso de herramientas de software para suplantar algunos servicios de comunicación, los cuales no resultan ser accesibles económicamente.

En consecuencia a lo recientemente señalado, se procederá con un cuadro comparativo entre 2 posibles formas de implementar el servicio de voz sobre IP (ver tabla 3.2 en la siguiente página). Dicha comparación estará orientada a los esquemas tradicionales de evaluación costo/beneficio, asumiendo que se implementarán soluciones de telefonía para 9 usuarios con la administración de una central.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Características	VoIP Convencional	VoIP Vía Software
Tecnología	Telefonía IP	Softphone
Equipos necesarios (*)	- Central IP (1) - Teléfonos IP (9)	- Computadora (10) - Software de aplicación
Proceso de implementación	Requiere trabajos de Hardware y software.	Manejo de herramientas de software.
Costo de implementación aproximado (*)	$ 1,500 + (9 x $ 300)	$ 500 + (9 x $ 350)
Costo total aproximado	$ 4,200	$ 3, 650

(*): Se considera la comunicación de 9 usuarios más una central IP.

Tabla 3.2. Comparación entre Tecnologías de Voz sobre IP

Aparentemente las cifras no distan mucho en cuanto al monto global; sin embargo, si se opta por la tecnología softphone se puede prescindir de la compra de los teléfonos y de la central IP, para optar por el uso de herramientas de software gratuitas. Por otra parte, es evidente que el grueso del costo en el servicio de VoIP vía software se sustenta en la adquisición de las computadoras; egreso que puede reducirse casi completamente si se aprovechan los equipos ya existentes en muchos de los hogares del Conjunto Habitacional.

3.3.3. Consideraciones en el Servicio de Videovigilancia

A diferencia de la tecnología analógica, el vídeo digital por comunicación IP presenta múltiples ventajas tanto en el campo tecnológico como en el plano económico (analizado a mediano plazo). En este caso ya no se requiere de extensas y costosas conexiones punto a punto a través de cable coaxial; se prescinde también del uso de cintas de vídeo y se reemplazan los equipos de grabación por técnicas de procesamiento y almacenamiento digital. El procesamiento de los sistemas digitales,

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

tales como herramientas para buscar, localizar y distribuir imágenes de vídeo interesantes aumentan la eficiencia y la eficacia de los operadores.

La ventaja real de un sistema de vídeo en red es que la visualización se puede hacer desde cualquier punto de la red y simultáneamente desde varias localizaciones. Para proporcionar seguridad y una mejor gestión del sistema, el acceso al vídeo puede restringirse con protección por contraseñas en las cámaras. Un sistema en red ofrece condiciones para asegurar que el vídeo puede ser monitorizado de la forma más eficiente y sencilla consiguiendo mejores resultados [41].

3.3.3.1. Topologías de Red

Los sistemas digitales se basan en redes informáticas para el transporte de sus contenidos, por lo tanto es importante considerar el diseño de red como factor primordial en el rendimiento global del sistema de vídeo. Para nuestro propósito las estructuras de estrella y de bus son las más relevantes. Como se describió previamente la topología de la red eléctrica nos obliga a seguir este modelo para la red de comunicaciones; es decir, el modelo de conexión físico es una variante de la topología en bus (un mismo medio compartido), aunque con la estructura jerárquica del árbol que se expande que desarrolla PLC similar a un modelo de topología estrella a nivel lógico.

3.3.3.2. Consumos de Ancho de Banda [41]

Una red puede estar compuesta de segmentos con diferentes anchos de banda. Múltiples usuarios acuden por medio de un canal de comunicación y éstos a su vez se interconectan con otros equipos a través de un único punto de conexión. En esta situación la mejor solución es crear un plan para definir el ancho de banda disponible (mínimo ancho de banda y máximo uso) para la aplicación. Esto garantizará el nivel de rendimiento del que es preciso disponer para asegurar la operativa de un sistema de seguridad y al mismo tiempo previene que el consumo sea superior a la capacidad, de esta forma se evita la reducción en el rendimiento de los otros sistemas de la misma red.

Otra característica a tener en cuenta, con relación al consumo de ancho de banda del sistema de vídeo, es el formato de trabajo que siguen las cámaras IP para cumplir con

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

su tarea. Es decir, estas cámaras, a diferencia de las convencionales, incorporan características superiores tales como la tasa de transmisión controlada por actividad (ACF) y los procesos de analítica avanzada. El mecanismo del ACF ha sido pensado para reducir el tráfico en la red; de esta manera si no se detecta ningún movimiento en la imagen, el ancho de banda de transmisión se reduce drásticamente. Se puede configurar, incluso, el sensor adherido a la cámara para ejecutar una grabación automática sólo cuando se presente alguna alarma.

Por otro lado, los procesos de analítica avanzada sirven para colaborar en la búsqueda de incidentes y la toma de decisiones por parte del equipo de vigilancia. Ellos pueden valerse del procesamiento que incorpora la cámara, o a través de un software de gestión instalado en una computadora para evaluar continuamente la probabilidad de riesgo en la seguridad a lo largo del día; estos procesos involucran acciones como la identificación de automóviles extraños estacionados demasiado tiempo fuera de un edificio, ingreso de las personas al recinto urbano, etc.

Entonces, valiéndonos de las características recientemente expuestas, procedemos con una estimación del ancho de banda que consumiría el sistema de videovigilancia que adoptará la residencial. Para esto es importante señalar que se considerará un conjunto de 6 cámaras estratégicamente ubicadas de manera que recoja, si no todos, al menos los sectores más críticos del Conjunto Habitacional en estudio. Usamos, para tal efecto, la herramienta de diseño que proporciona una de las empresas líderes en el mercado (AXIS Communications). Sus resultados se muestran en la figura 3.7 y para mayor detalle sobre el software revísese la fuente [39].

Red de Seguridad en un Conjunto Habitacional

AXIS Design Tool exportar archivo, Martes 5. Nov 2006 16.16.17

El proyecto se basa en la interconexion de camaras de video IP sobre las redes electricas

Nombre	Modelo	Núm de cámaras	Ancho de banda (Ver, grab., evento)	Almacenamiento
1 Camara 1	AXIS225FD	1	2.0 Mbit/sec, 0 bit/sec, 396 kbit/sec	28.5 Gb
2 Camara 2	AXIS225FD	1	2.0 Mbit/sec, 0 bit/sec, 396 kbit/sec	28.5 Gb
3 Camara 3	AXIS225FD	1	2.0 Mbit/sec, 0 bit/sec, 396 kbit/sec	28.5 Gb
4 Camara 4	AXIS225FD	1	2.0 Mbit/sec, 0 bit/sec, 396 kbit/sec	28.5 Gb
5 Camara 5	AXIS225FD	1	2.0 Mbit/sec, 0 bit/sec, 396 kbit/sec	28.5 Gb
6 Camara 6	AXIS225FD	1	2.0 Mbit/sec, 0 bit/sec, 396 kbit/sec	28.5 Gb
Resumen del proyecto			12.1 Mbit/sec, 0 bit/sec, 2.3 Mbit/sec	171.3 Gb

Figura 3.7. Consumo de BW para el Sistema de Videovigilancia [39]

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

El modelo de cámara elegido pertenece a la serie 225FD (excelentes prestaciones técnicas, diseñadas especialmente para aplicaciones de videovigilancia y con equipamiento para soportar condiciones hostiles de trabajo). Se ha considerado además una resolución estándar de 480 x 360 para un nivel de complejidad de imagen promedio.

En el ámbito de la tasa de transmisión de imágenes, hay que considerar que no nos encontramos en un medio extremadamente dinámico; es decir, no hay mayores variaciones en el área objetivo para un intervalo de tiempo considerado (a diferencia de un casino, un aeropuerto o un banco). Por tal razón, se propone una secuencia prudente de 10 imágenes por segundo para la visualización y una secuencia de 15 tramas por segundo para el caso en el que la alarma active la función de grabación automática de imágenes (se asume por precaución que se produce con una estadística del 10%; es decir, si el tiempo transcurrido es un día, se entiende que la secuencia de imágenes almacenadas será un tanto superior a las dos horas).

Finalmente se ha tomado como referencia el estándar de compresión MJPEG, aun cuando el modelo de cámara elegido trabaja también bajo el 'códec' MPEG-4; sin embargo, para efectos de diseño, conviene situarnos en el caso del mecanismo que nos pueda ocupar un mayor ancho de banda. Todas las características señaladas se aprecian directamente en la figura siguiente:

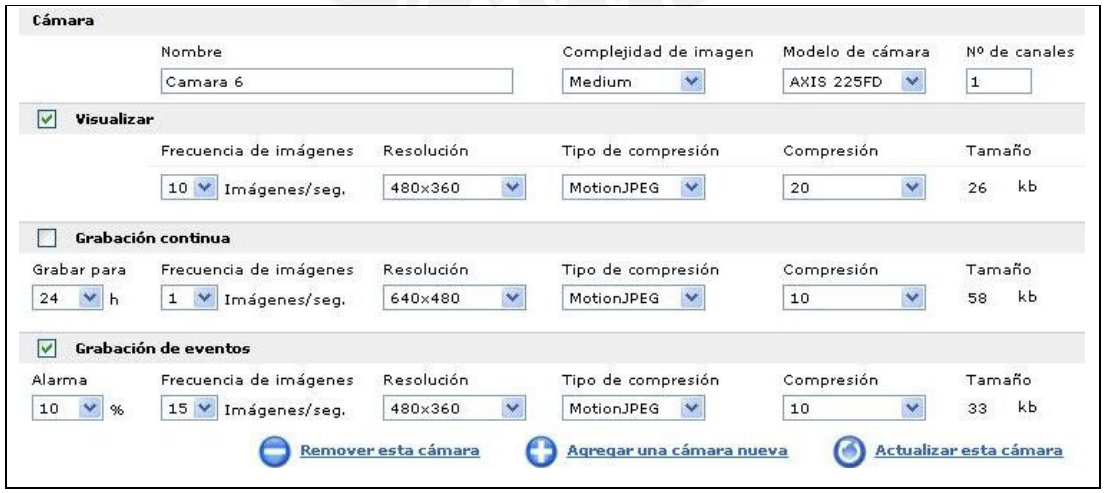


Figura 3.8. Configuraciones para la Operación de las Cámaras IP [39]

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.3.3.3. Instalación de la Cámara IP [41]

Dado que las cámaras van a ser usadas en exteriores y sometidas a condiciones adversas. Entonces, se requiere que éstas estén instaladas en carcasas adecuadas que las protejan de las condiciones climatológicas, del polvo y de la humedad, de las temperaturas extremas, así como de otros factores ambientales no deseados. Las carcasas deben igualmente incorporar un sistema de calentamiento o enfriamiento para ofrecer una temperatura de operación adecuada.

En este punto debemos también considerar el campo visual para la cámara. Se debe prever cualquier factor que pueda bloquear en cualquier momento su visibilidad (árboles que crecen, un camión aparcado o una puerta que se queda abierta). Otro factor que se debe tomar en consideración es la posición del sol respecto a la cámara, se debe evitar que ésta esté en la dirección hacia la que se pone el sol.

Un elemento clave, además, es la iluminación. Generalmente cuanto más luz haya mejor será la imagen. Si la iluminación no es suficiente puede ser preciso instalar luces adicionales. Para asegurar una iluminación adecuada pueden usarse dispositivos externos de control como sensores de luz, detectores sensibles a movimientos en el área, etc. Debemos igualmente considerar la instalación en un entorno dinámico (donde los niveles de iluminación pueden variar considerablemente). Para compensarlo, las cámaras deben ir equipadas con un lente que ajuste el iris automáticamente en función de la cantidad de luz circundante, de esta manera se atenúan los cambios de contraste y brillo .

Como solución, dentro del entorno de la instalación de las cámaras, se ha optado por un modelo de cámara IP especial para trabajar en entornos difíciles y sobrellevar condiciones adversas en los exteriores. A pesar de ello se recomienda la ubicación estable y segura sobre una carcasa con las características descritas anteriormente; su ubicación en la parte superior de los edificios le garantiza una gran visibilidad (buen panorama e iluminación desde el alumbrado público) y evita el contacto con medios externos que puedan mermar su visión.

El suministro de energía y punto de red de la cámara estará soportado por sus interfases respectivas con conexión hacia el departamento ubicado en el quinto piso.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.4. Organización de una Red PLC

La topología de una red PLC está dada por la topología de la red de suministro eléctrico de baja tensión usada como medio de transmisión. Sin embargo una red PLC puede ser organizada de diferentes maneras (distintas posiciones del HE, segmentación de la red, modo de distribución en subredes, etc.), lo cual implica una serie de variantes en el modo de operación de la red.

De acuerdo a lo señalado recientemente y conforme a las características reales del medio, se procederá a desarrollar las variantes que influyen en la organización de una red PLC y sus implicancias en el modelo de red con el que se va a trabajar.

3.4.1. Posición de la Estación Base (HE)

El Head End (HE) conecta el sistema de acceso PLC al backbone de la red (WAN), por lo que tiene una posición privilegiada en la estructura de red PLC. Existen dos posibles sectores en donde se puede ubicar al equipo maestro de la red [32]:

a) **Ubicado en la Estación Transformadora.-** De esta manera se puede aprovechar la concentración de todos los usuarios a la subestación eléctrica y desde allí inyectar los datos o recibirlos para distribuirlos a través de la WAN.

b) **Ubicado en un Sector de Usuario.-** Ya que la ubicación del HE depende, básicamente, de su posibilidad de conectarse a un backbone de red. Entonces este equipo podría ubicarse al interior de una cabina pública con acceso a la red de baja tensión. Este cambio involucraría una variación en las distancias entre la estación base y los suscriptores, lo cual puede implicar el uso o no de un Home Gateway (HG); sin embargo este procedimiento no altera la estructura de árbol de la red.

En el caso de este diseño, la ubicación de la estación transformadora no representa una traba para la cobertura sobre el sector y se aprovecha su ubicación para instalar allí el HE; de esta forma los datos inyectados en un único punto pueden transcurrir a lo largo del medio de interés.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.4.2. Segmentación de Red

Para efectos de una mejor distribución y organización de la red involucrada en este diseño, se considerará un HG en cada uno de los edificios del conjunto (ver figura 3.9). De esta forma, cada uno de ellos trabajará administrando su red local en cada edificio e intercambiará información con la estación base central donde se encuentra el maestro de la red (HE).

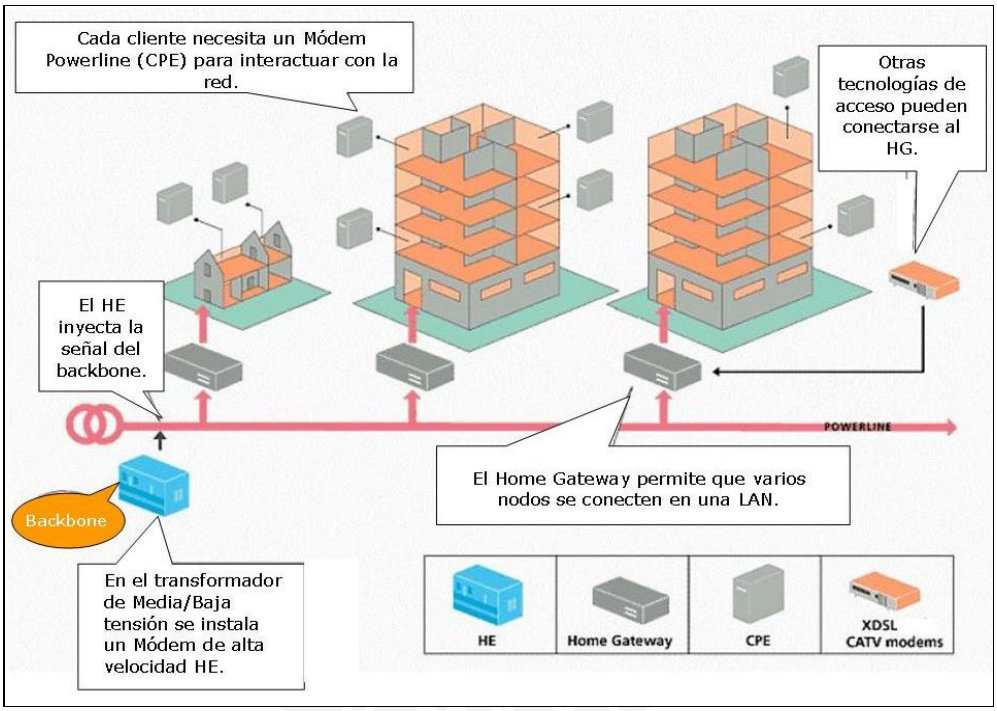


Figura 3.9. Topología de Red PLC [33]

Las redes PLC que superan grandes distancias pueden ofrecer muy bajas tasas de transmisión de datos; sin embargo se puede adoptar medidas contempladas en su tecnología para superar este escollo, gracias a los repetidores simples o los Home Gateway (HG). Estos elementos tienen la función de regenerar la señal de datos y en el caso del HG, la responsabilidad adicional de administrar los segmentos de red. Generalmente un número opcional de estos equipos puede ser empleado en las redes PLC para dividirla en pequeños segmentos. Sin embargo, un factor limitante para su realización es la interferencia entre los segmentos vecinos; de esta manera, una porción del espectro tiene que ser usado y dividido entre todos los segmentos de red

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

[32]. Por otro lado, estos equipos causan desfases adicionales en la propagación debido al tiempo requerido para el procesamiento en la conversión de la señal; motivo por el cual el número de repetidores aplicados a la red PLC, así como el de los HG, tienen que ser controlado.

Teóricamente cada HG puede soportar cerca de 256 usuarios; sin embargo, todo depende del ancho de banda de las aplicaciones que cada uno maneje. En este caso se ha elaborado un esquema en el que cada HG controlará dos usuarios por edificio, aunque con aplicaciones en tiempo real y alto consumo de ancho de banda. No se descarta, sin embargo, la opción de que este número sea ampliado en caso se presenten nuevas necesidades de comunicación y en caso la red pueda recibir mayor carga de trabajo sin menguar su rendimiento.

3.4.3. Distribución en Subredes

La red de comunicaciones involucrada en este estudio centra su funcionamiento en un esquema de interrelación continua entre subredes, cada una de ellas está destinada a fortalecer el desempeño del conjunto a través del manejo eficiente de sus capacidades individuales. Esta segmentación, por tanto, ayudará a administrar con eficiencia la red y permitirá detectar en menor tiempo las fallas eventuales que puedan presentarse, todo ello gracias a la distribución y organización de funciones.

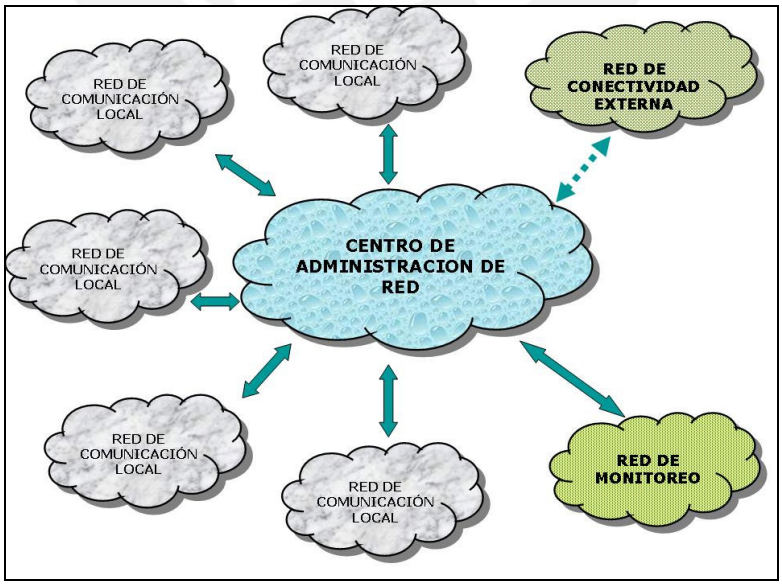


Figura 3.10. Diagrama de Distribución de Subredes

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

La red cuenta, básicamente, con 3 subredes principales: red de comunicación local, centro de administración de red y red de monitoreo (ver figura 3.10). Estas redes están destinadas fundamentalmente al manejo de las funciones primarias (comunicación usuario-vigilancia y captación y envió de señales de vídeo). Sin embargo, se considera la posibilidad de una cuarta subred (de conectividad externa), de esta manera se deja abierta la posibilidad de una mayor cobertura de comunicaciones.

3.5. Desarrollo de las Subredes

Antes de proponer los esquemas de red se debe aclarar algunos conceptos respecto a la redes sobre las líneas eléctricas. De acuerdo a ello se define, primero, las dos direcciones de transmisión en una red PLC:

- Downlink/ downstream, desde la estación base hasta los suscriptores.
- Uplink/ upstream, desde los suscriptores hasta la estación base.

La información enviada por el Head End ubicado en la estación base (dirección downlink) es transmitida a todas las secciones de red internas y es recibida por todos los usuarios. En la dirección uplink la información enviada por un usuario de red es recibida e interpretada por el HE, pero también puede transcurrir eventualmente a través de los demás usuarios en esa subred. Desde el punto de vista de una capa superior de red (como la capa MAC) , una red de acceso PLC puede ser considerada como una red lógica en topología bus, conectando un número de estaciones con su estación base [32].

3.5.1. Red de Comunicación Local

Esta red se desarrolla al interior de cada uno de los edificios que conforman el sector del conjunto habitacional con el que se está trabajando. El diseño acoge, entonces, a un grupo de 6 edificios que conforman gran parte del área de interés; en cada uno de ellos se instalará una cámara de vídeo IP (en el piso más alto) y una computadora que funcionará como un teléfono IP, por medio de la instalación de un software libre para las aplicaciones Softphone.

La existencia de estos dos equipos de comunicación (cámara de vídeo y teléfono) cubrirá en gran medida las necesidades más urgentes en cuanto a la seguridad

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

residencial; sin embargo, esto no impide una futura ampliación de equipos provenientes de cada domicilio en caso se busque aprovechar la red desplegada para cubrir otras necesidades como la de telefonía, Internet, entre otras. Todo ello, siempre que la red principal esté en condiciones de manejar mayores exigencias.

En la figura 3.11 se aprecia la relación entre los equipos antes descritos y además aquellos que intervienen para la inyección de la señal a través de las líneas eléctricas (equipos PLC).

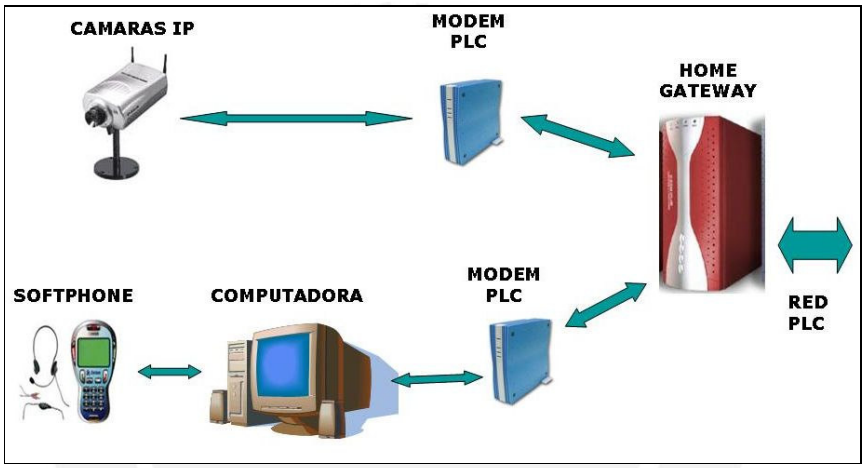


Figura 3.11. Diagrama de Red de Comunicación Local

Para el servicio de vídeo en red, se debe aclarar que el módem PLC se ubicará, por seguridad, al interior de una de las viviendas situadas en el nivel superior (quinto piso) y que sólo la cámara IP se acomodará, por necesidad de visualización, en el área que conformaría la terraza del edificio. La computadora y los accesorios para el servicio de voz sobre IP (auricular y micrófono) tendrán lugar en el primer piso de cada edificio y únicamente el módem PLC lo hará al interior de uno de los departamentos que conforman el primer piso del mismo.

3.5.1.1. Selección de Equipos

A) Cámaras IP

Lo primero que nos debe asegurar una cámara de estas características es un buen desenvolvimiento para aplicaciones profesionales de vigilancia y monitorización

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

remota (visualización y control de imágenes a distancia). Todo esto añadido a las características básicas de una cámara IP, como el de trabajar bajo estándares eficientes de compresión, tener buen desempeño en la captura de imágenes, opciones de giro, acercamiento, detección de eventos y todo lo que en general le pueda ofrecer la capacidad de procesamiento e inteligencia con las que son diseñadas.

De acuerdo a esas características mencionadas, es importante señalar que existe una voluminosa gama de opciones entre cámaras de distintos fabricantes que cumplen con dichos requerimientos, a pesar de ello se procede con el análisis de dos principales modelos cuyas aplicaciones van acorde con la vigilancia en sectores urbanos:

a) Domo IP fijo AXIS 225FD

Esta cámara está exclusivamente diseñada para trabajar en los entornos más difíciles (a prueba de adversidades externas y agresiones); de gran resistencia a impactos y de fácil instalación en diversos entornos como paredes, columnas, techos y demás. Maneja estándares de compresión MJPEG y MPEG-4 con interfases Ethernet 10Base-T/100Base-TX (conectores RJ-45) y compatible con Windows. Presenta detección de movimiento y ajuste de rangos de transmisión según el evento (ver figura 3.12).

b) Domo IP fijo FW1150

El FlexWATCH 1150 está formado por una cámara con movimiento, por un servidor Web de vídeo y un software de grabación digital, que convierten a este equipo en todo un sistema de tele vigilancia de altas prestaciones totalmente integrado. Compatible con formatos de vídeo NTSC y PAL, incluye navegador compatible con cualquier sistema operativo como Windows, Linux, Unix, etc. Y no necesita descargar ningún tipo de software, ni ninguna aplicación propietaria para ver las imágenes de vídeo.

Una de las principales desventajas de este último modelo (FW 1150) es que presenta un sólo esquema de compresión basado en MJPEG, con tasas de compresión máxima de 30 frames por segundo; es decir sus procesos exigen mayores anchos de banda a la red. Por otro lado el precio resulta ser 10 a 15 % superior respecto al modelo de AXIS. Aunque una descripción más detallada acerca de las capacidades técnicas de estas cámaras son mencionadas en las hojas de datos de los equipos utilizados (anexo número 1); se opta, empero, por aquella que se ajusta más a los

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

requerimientos del sistema planteado. Por tanto, se elige el modelo 225FD perteneciente a la familia del fabricante AXIS Communications.

AXIS 225FD

FW 1150

Figura 3.12. Modelos Considerados de Cámaras IP

B) Softphone

Las prestaciones de este producto deben asegurar la realización de llamadas de la misma forma como las que se harían con las llamadas convencionales pero con el valor añadido que ofrece el trabajar sobre IP. Adicionalmente se debe reemplazar un equipo telefónico a través de un software instalado sobre una computadora y un conjunto de accesorios de acuerdo a lo ilustrado en la figura 3.13.

En este caso se ha optado por el paquete "X-Lite", que comprende un software gratuito compatible con Windows (98SE/ ME/ 2000/ XP) para el uso de llamadas de PC a PC y de PC a teléfono cumpliendo con los protocolos SIP versión 2.0 y H.323 versión 4. Para este efecto la computadora debe tener una tarjeta de sonido, debe tener instalado uno de los sistemas operativos mencionados anteriormente y tener deshabilitada la función Proxy HTTP en la configuración de conexión a red.

Software de VoIP

Accesorios Corinex

Figura 3.13. Accesorios para el Sistema de Voz sobre IP

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Se reemplazará el hardware telefónico por el uso de accesorios como micrófonos y audífonos que vienen incluidos en el paquete del fabricante Corinex. Una información más detallada acerca de las funcionalidades, modo de instalación y características del producto es presentada en la sección dedicada a las herramientas de voz sobre IP del anexo 1.

C) Equipos PLC

La descripción y las características principales que deben seguir los equipos PLC fueron detalladas en el capítulo anterior. A partir de esa información se han identificado dos fabricantes líderes que ofrecen similares características de funcionamiento, considerados para entornos de red eléctrica en baja tensión y destinados a sectores residenciales. Sin embargo, la elección acertada de la familia de equipos PLC con los que se contará para este diseño se realizará luego de analizar la particularidad de cada fabricante y de cada equipo.

En tal caso se rescatan las siguientes dos compañías: CORINEX e ILEVO; cuyos productos ofrecen, entre otras, las siguientes funciones descritas en la tabla 3.3:

Características	Ambos Fabricantes
Interfase de Red	10/100Base T
Velocidad de Transmisión	200 Mbps
Cobertura	300 metros
Protocolo de Acceso al Medio	CSMA/ CA
Tipo de Modulación	OFDM
Frecuencia de Trabajo	2 – 34 MHz
Encriptación de Datos	Si
Estándares de Capa 2	IEEE 802.1P (Priorización de trafico) IEEE 802.1Q (VLAN) IEEE 802.1D (Spanning Tree Protocol)

Tabla 3.3. Características Básicas de los Equipos PLC

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

a) Módem PLC

Las diferencias más relevantes entre ambos fabricantes respecto a los módems PLC se pueden resumir en la tabla 3.4; de igual forma, sus características físicas se pueden apreciar en las figuras inmediatamente adjuntas:

Módem CORINEX – Modelo AV200 ETHC **Módem ILEVO – Modelo ILV220**

Figura 3.14. Modelos Considerados para los Módems PLC

Características	CORINEX	ILEVO
Protocolo de Enlace de Datos	IEEE 802.3u (Fast Ethernet –200Mbps)	Propietario
Voltaje de Alimentación	85 - 265 V	85 - 265 V
Frecuencia de la Fuente de Energía	50 / 60 Hz	50 / 60 Hz
Consumo de Potencia	10 W	8 - 13 W
Densidad Espectral de potencia	-56 dBm/Hz	-50 dBm/Hz
Estándares Compatibles	DHCP	SNMP, DHCP, TFTP
Servicios Adicionales	Filtro para las direcciones MAC no admitidas	Telefonía IP por medio de un gateway de voz incorporado.

Tabla 3.4. Características Destacadas de los Módems PLC

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

b) Home Gateway

De manera similar se procederá con una comparación de las características que diferencian a ambas tecnologías de fabricación de estos equipos, para ello es relevante ver las características básicas de la figura 3.15 y leer la información más detallada de la tabla 3.5:

HG CORINEX- Modelo AV200 MDU **HG ILEVO – Modelo ILV2120**

Figura 3.15. Modelos Considerados para los Home Gateways

Características	CORINEX	ILEVO
Protocolo de Enlace de Datos	IEEE 802.3u (Fast Ethernet –200Mbps)	Propietario
Voltaje de Alimentación	100 - 240 V	100 - 240 V
Frecuencia	50 / 60 Hz	50 / 60 Hz
Consumo de Potencia	10 W (sin acoplamiento)	18 W incluyendo acopladores
Densidad Espectral de Potencia	-50 dBm/Hz	-46 dBm/Hz @ 10 MHz -49 dBm/Hz @ 20 MHz -50 dBm/Hz @ 30 MHz
Estándares Compatibles	SNMP	SNMP, DHCP
Segmentación	Actúa como maestro de hasta 32 módems PLC	Soporta 64 conexiones PLC activas
Mecanismo de Acceso Múltiple	División en el tiempo y frecuencia	División en frecuencia

Tabla 3.5. Características Destacadas de los Home Gateways

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.5.2. Centro de Administración de Red

Esta subred representa el núcleo de la red de comunicaciones principal y centra su funcionamiento en dos funciones vitales: funciona como el soporte de las aplicaciones de red (manejo de voz y vídeo), y como plataforma para recibir la información proveniente de todos y cada uno de los usuarios de la red por medio de la comunicación con los Home Gateway' s (HG). Su tarea no sólo se justifica en la dirección de subida (usuario – centro de administración) sino que envía además los datos almacenados hacia el sector que lo solicite, en nuestro caso será el puesto de vigilancia el principal receptor de la información (ver figura 3.16).

La ubicación de esta subred en el conjunto habitacional se ha determinado indirectamente en la sección 3.4.1. (posición de la estación base). Y es que, la presencia de la estación transformadora de energía eléctrica de media a baja tensión nos da el referente para la ubicación del equipo maestro de la red PLC (HE); a partir de este equipo se manejan los datos mediante otra interfase (Fast Ethernet sobre cableado CAT-5) y a muy altas velocidades; por este motivo la sala de comunicaciones deberá estar ubicada en el domicilio aledaño a la subestación eléctrica, acondicionando un ambiente especial para la preservación óptima de los equipos.

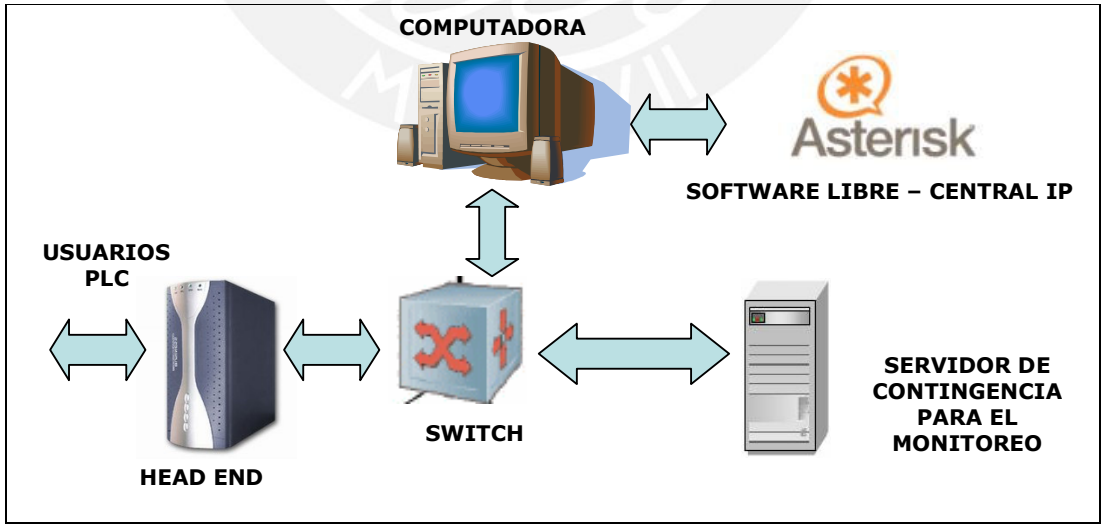


Figura 3.16. Diagrama del Centro de Administración de Red

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.5.2.1. Selección de Equipos

A) Head End

A continuación se elaborará otro esquema de comparación para determinar las diferencias entre los fabricantes de equipos PLC ahora relacionado a los módems de cabecera (HE), para ello remitirse a la tabla 3.6 y a la figura 3.17:

HE CORINEX - Modelo AV200 LVA-GWY **HE ILEVO – Modelo ILV2010**

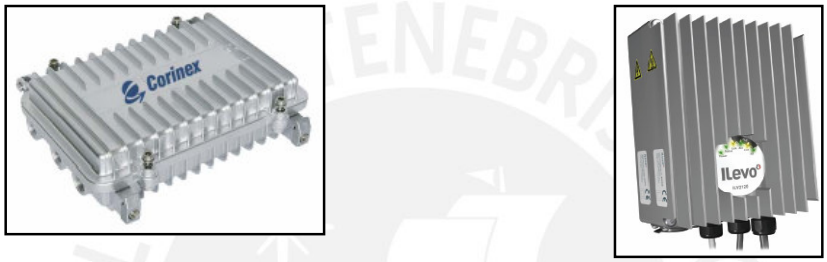


Figura 3.17. Modelos Considerados para la Elección del HE

Características	CORINEX	ILEVO
Protocolo de Enlace de Datos	IEEE 802.3u (Fast Ethernet –200Mbps)	Propietario
Voltaje de Alimentación	100 - 240 V	100 - 240 V
Frecuencia de la Fuente de Energía	50 / 60 Hz	50 / 60 Hz
Consumo de Potencia	7 W (sin acoplamiento)	18 W incluyendo acopladores
Densidad Espectral de Potencia	-50 dBm/Hz	-46 dBm/Hz @ 10 MHz -49 dBm/Hz @ 20 MHz -50 dBm/Hz @ 30 MHz
Estándares Compatibles	SNMP	SNMP, DHCP
Segmentación	Tabla de difusión para 64 direcciones MAC	Soporta 64 conexiones PLC activas
Servicios Adicionales	Soporte para la optimización de trafico: broadcast y multicast	Interacción con servidores de auto configuración: SNMP, RADIUS, FTP, NTP.

Tabla 3.6. Características Destacadas de los Head End

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

B) Servidor de Contingencia para el Monitoreo

En este caso se utilizará una computadora extra para que trabaje como un mecanismo de respaldo en el manejo, almacenamiento y distribución de las imágenes de vídeo provenientes de todas las cámaras (la red de monitoreo cuenta con un mecanismo similar). Con este planteamiento se asegura principalmente dos ventajas, la primera es que la información crítica contará con redundancia y la segunda, y no por ello menos importante, es que se deja abierta la posibilidad futura para que otros usuarios accedan a su información de manera independiente tanto al interior como al exterior de la red. En otras palabras, ya que este servidor estará activo en todo momento y se conecta directamente al switch de comunicaciones, su interoperabilidad con Internet dependerá básicamente de una conexión de última milla sin que ésta merme el rendimiento ni el ancho de banda de la red PLC cuando los usuarios externos soliciten información.

Por otro lado, al interior de la red se crea un canal de tráfico de vídeo directo entre cada usuario y el centro de administración de red diferente al que existía entre ellos y la red de monitoreo (en donde se tiene pensado instalar otro equipo con similares prestaciones). De esta forma no se satura el canal PLC formado por la red de monitoreo y el módem de cabecera Head End (véase la figura 3.23 en la página 71).

Con relación a las características técnicas de la computadora y del software de monitoreo que se dispondrán para esta función véase la sección correspondiente a la red de monitoreo.

C) Central IP Vía Software

Todas las características que ofrecen las centrales de telefonía convencional, sumadas al amplio rango de opciones que ofrecen las comunicaciones de voz sobre IP; se pueden resumir en un solo instrumento software, cuya instalación en una computadora con buen nivel de procesamiento, puede proveer de enormes prestaciones a diversos entornos empresariales, industriales, de convivencia social, etc. (véase figura 3.18). En nuestro caso esta solución estará destinada a la comunicación dentro del complejo residencial para actuar, en principio, como nexo entre los residentes y el personal de seguridad.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Asterisk es un software de central telefónica IP basado en código abierto. Se ejecuta sobre sistemas operativos Linux, lo que le brinda una fuerte ventaja competitiva debido a la gratuidad de su uso y a que está evolucionando continuamente por ser un código abierto a múltiples programadores. El protocolo de manejo de sesión con el que trabaja Asterisk es el SIP (Session Initiation Protocol), el cual genera un entorno de señalización entre los usuarios simulando una conversación telefónica tradicional. En términos generales cumple con las siguientes cuatro funciones:

1. Localización de usuario. Es decir, traduce un número de usuario en una dirección IP.

2. Negociación de la sesión, de tal forma que todos los participantes acuerden qué protocolos de transporte y aplicaciones están soportadas.

3. Administración de sesiones, como por ejemplo agregar, eliminar o transferir participantes.

4. Administración de propiedades de una sesión mientras que está en progreso.

Computadora con Sistema Operativo Linux **Software Central IP**

Figura 3.18. Accesorios para la Simulación de la Central IP

D) Switch de Administración de Red

Este equipo intermediario tiene la misión de hacer efectiva la conmutación de las tramas provenientes de diversas fuentes, la de garantizar un intercambio de información dinámico y organizar en cierta forma la red para evitar la saturación del medio por el que se está transmitiendo.

Al respecto es importante señalar que actualmente se manejan dos tipos de tecnologías de conmutación para estos equipos: switch con operación en capa 2

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

(conmutación basada en las direcciones MAC) y switch de manejo de tramas en capa 3 (conmutación basada en direcciones IP). Para la ejecución de este proyecto se podría considerar ejemplares que basan su operación en este último tipo de conmutación, debido a una serie de razones que se describen a continuación [25]:

- Previenen el colapso de la red, ante la presencia de tormentas de Broadcast y manejan eficientemente el tráfico multicast.
- Manejan Calidad de Servicio (diferenciación del tipo de tráfico) y manejo efectivo de los recursos de red.
- Son capaces de identificar si la información que arriba a sus puertos tiene que ser conmutada en capa 2 ó 3, y si ésta debe de tratarse de manera local o enviarla hacia la red externa.
- Pueden filtrar información no deseada, incluso de los usuarios que tienen permitido el acceso a la red, para prevenir ataques a servidores, bases de datos, o proteger aplicaciones con ciertos niveles de seguridad.
- Un switch de capa 3 tiene la capacidad para distinguir cuando los puertos donde se conectan los servidores de la empresa están, ocupados, saturados o 'caídos', de tal manera que puede reenviar eficientemente el tráfico y las peticiones de los usuarios de la red hacia aquellos puertos que puedan responder.

A partir de estas funcionalidades se procede a detallar dos modelos de switch, uno de capa 2 (CISCO) y otro que trabaja en capa 2 y 3 (3COM). Ambos adquieren relevancia para efectos de este diseño. La figura 3.19 y la tabla 3.7 aportan en tal sentido:

Switch CISCO Catalyst 2950-12 **Switch 3COM 3226 - Capa 3**

Figura 3.19. Modelos de Switch Considerados en el Diseño de Red

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

CARACTERÌSTICAS PRINCIPALES

Características	CISCO	3COM
MAC Address	8K direcciones MAC	8K direcciones MAC
VLAN	IEEE 802.1x Consideración de VLAN's para aplicaciones de voz	255 VLAN's (IEEE 802.1Q)
Auto negociación	Automática de todos sus puertos	De cada puerto y conexión (MDI/MDIX)
Control de Tráfico	Modo Half o Full Dúplex	Full Dúplex 802.3x
Spanning Tree Protocol (STP)	• IEEE 802.1D • IEEE 802.1W • STP rápido por VLAN's (PVRSTP)	• Mecanismo rápido IEEE 802.1w (RSTP) compatible con STP
Soporte Multicast	• IGMPv3 (mecanismo snooping) • Multicast VLAN Registration (MVR)	• IGMPv1 y v2 • Filtro por grupo Multicast de 64 usuarios
Protocolos de Red	• SSHv2 (encriptación) • SNMPv3 (administración)	• DHCP • ARP/ARP Proxy • SNMPv1
Priorización de Tráfico	• IEEE 802.1p (CoS) • Valor de CoS por defecto asignado por el administrador de red	• IEEE 802.1p (CoS) • Considera priorización de VLAN's
Interfases	12 puertos 10/100 Base T	• 24 puertos 10/100 Base T • 2 puertos 10/100/100 o SFP Gigabit
Procesamiento	1.8 Millones de paquetes por segundo (Mpps)	6.6 Millones de paquetes por segundo (Mpps)
Alimentación	• 100 – 127 VAC • 200 – 240 VAC / 47 a 63 Hz	200 – 240 VAC / 47 - 63 Hz

Tabla 3.7. Características de los Switchs de Administración

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.5.3. Red de Monitoreo

Como su nombre lo indica, esta red se encarga de solicitar, recibir, almacenar y distribuir la información proveniente de todas las fuentes de datos. Aquí se encuentra ubicado el personal capacitado para interpretar la información recibida y para actuar en concordancia a los hechos. A diferencia de la red de comunicación local, en esta red el flujo de datos de mayor intensidad está en el sentido descendente; es decir, el tráfico enviado por esta red es similar al de las redes locales de cada edificio, pero la información recibida es mucho mayor dado que proviene del centro de administración de red y trae recursos de todas las fuentes de datos. Para mayor detalle remitirse a la figura 3.20.

Para establecer la comunicación de voz se cuenta, al igual que las redes de usuarios, con una computadora adaptada a aplicaciones de voz sobre IP. En este caso, esta máquina también ayudará a soportar las aplicaciones de vídeo mediante un software de monitoreo que se incluye en los equipos del fabricante de las cámaras. Finalmente cabe resaltar que los equipos PLC, las cámaras y los equipos para el servicio de VoIP que conforman la subred estarán ubicados estratégicamente al interior del edificio más cercano a la entrada principal del recinto residencial (edificio número 4 en la figura 3.25 de la pág. 73) que es donde se ubica actualmente la caseta de vigilancia.

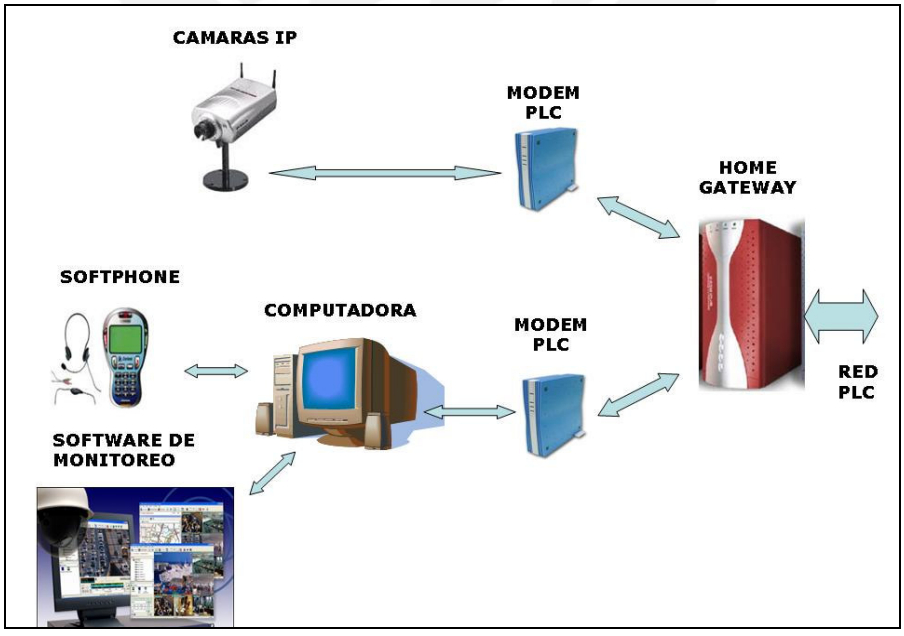


Figura 3.20. Diagrama de la Red de Monitoreo

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.5.3.1. Selección de Equipos

A) Software de Monitoreo

Mediante esta herramienta se puede tomar dominio sobre las imágenes de las cámaras de vídeo y de algún eventual servidor (en caso se usen cámaras analógicas); sus beneficios involucran la captación de información visual desde cualquier punto de la red (local o remoto) y con sólo instalar un software sobre una computadora convencional. Sus prestaciones deben involucrar, además, funciones de grabación de alta calidad y gestión de eventos (búsqueda de episodios importantes y visualización simultánea de un suceso desde diversas fuentes).

Específicamente, el software de monitoreo como tal, debe garantizar las siguientes funciones:

- Visualización y grabación de varias cámaras de forma simultánea.
- Diferentes modos de grabación: continua, programada, por detección de movimiento y/o alarma. La detección de movimiento del software funciona comparando las diferencias entre zonas específicas de las imágenes.
- Detección de movimiento integrada, lo que involucra el envió de imágenes y grabación de la hora en el momento que se detecta un movimiento con el respectivo ahorro de ancho de banda que esto involucra.
- Grabaciones de alta calidad.
- Sin limitación de grabación en el software.
- Múltiples funciones de búsqueda de eventos grabados.
- Acceso remoto vía navegador o cliente Windows con previa autenticación de nombre de usuario y contraseña.
- Permite el control de cámaras PTZ y domos.
- Función de notificación de alarmas (vía e-mail).

Para la ejecución de este proyecto se ha tomado en cuenta dos principales opciones que emergen como dos de las soluciones más destacadas, manejan un grupo de hasta 25 cámaras y sus costos van acorde con los precios que se manejan en el mercado:

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

a) NetCamCenter Professional Edition

Esta primera opción tiene la ventaja de adaptarse a una gran variedad de cámaras IP provenientes de diversos fabricantes y de ser completamente adaptable a la tecnología de "Microsoft Windows Media". La instalación de este paquete requiere de algunas características de software y hardware que se procederán a mencionar en las líneas siguientes:

- **Software**

  - Sistema Operativo Microsoft Windows XP/2000/2003.
  - Windows Service Pack 4 para Windows 2000 o Service Pack 2 para XP.
  - Microsoft DirectX 9.0 o superior para Windows 2000.
  - Windows Media Player 10.

- **Hardware**

  - CPU: Intel Pentium 4 / 2.0 GHz o superior.
  - 128 MB de memoria RAM (256 MB recomendado).
  - Tarjeta de sonido compatible con Windows.
  - Tarjeta gráfica de 32 MB de memoria o superior.
  - Tarjeta de red (10/100 Mbps).
  - 80 GB de Disco Duro para la grabación de vídeo o superior.

b) AXIS Camera Station

El sistema de monitoreo de Axis también tiene la ventaja de trabajar sobre cualquier computadora con sistema operativo Windows. Incluso ofrece una opción para optimizar las imágenes obtenidas bajo condiciones atmosféricas adversas como niebla, humo, lluvia o nieve, mediante un componente adicional al software, el "AXIS Image Enhancer".

Los requisitos mínimos de software son los mismos que para el anterior software de monitoreo. Por otro lado, en cuanto al hardware tenemos:

Hardware para un sistema de 4 cámaras:

- Procesador Pentium 4, 2 GHz, unidad de CD.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

- 512 MB de RAM.
- Disco duro: 1 GB para la instalación.
- Sistema de archivos NTFS.
- Monitor XGA (1024 x 768) o de mayor resolución.
- Tarjeta gráfica AGP, Direct Draw (para MPEG-2/4), con memoria de 32MB.
- Ethernet de 100 Mbits.

Requisitos mínimos del hardware para un sistema de 25 cámaras:

- Dual XEON 3 GHz, 1024 MB RAM, varios discos SCSI.
- Red troncal Ethernet de 1000 Mbits.
- Disco duro independiente para el Sistema Operativo y las grabaciones.

En nuestro caso se ha optado por la opción que ofrece el mismo fabricante de las cámaras IP, se trata del software "AXIS Camera Station" de la figura 3.21. Su rendimiento parece ofrecer mayores garantías en cuanto se trate de un sistema con red de cámaras de la misma marca.

Figura 3.21. Software de Monitoreo de la Compañía AXIS

3.5.4. Red de Conectividad Externa

Como se mencionó anteriormente, esta subred no está contemplada en el diseño propuesto para la red de seguridad residencial. Sin embargo, dada la magnitud actual de las telecomunicaciones, su existencia se considera casi inminente en un futuro no muy lejano. Las características actuales del diseño de red, por tanto, no descartan

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

esta posibilidad y más aún, la breve descripción de este párrafo es un esfuerzo por sustentarla. La distribución de equipos de la misma se observa en la figura 3.22.

En ese caso, la red de seguridad podría, mediante este esquema, interactuar con las redes de telefonía pública y con la inmensidad de aplicaciones que brinda Internet (conexión directa a las redes de la policía nacional, telefonía IP, entre otras).

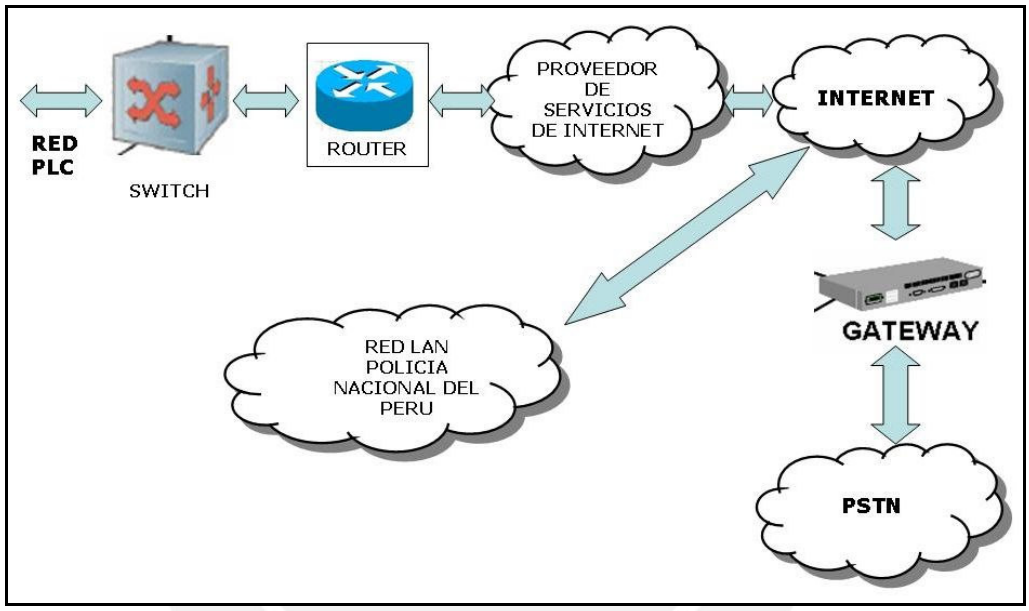


Figura 3.22. Diagrama de la Red de Conectividad Externa

3.6. Diagramas de Red

A partir de la información obtenida luego de analizar extensamente cada una de las subredes, se procede con la organización del esquema globalizado que mostrará tanto la interconexión a nivel lógico, como aquella que se da con relación a la interconexión física (ya sea en el contexto de un departamento, un edificio y así como el que se da en el sector residencial en análisis).

3.6.1. Diagrama Lógico de Distribución

A continuación, se elabora el esquema mediante el cual se piensa organizar la red de seguridad pública, se toma en cuenta los equipos de red involucrados, la relación que existe entre ellos, se aprecia el modelo de jerarquías con el que trabaja la tecnología PLC y por último se manejan cifras aproximadas en cuanto al consumo de ancho de

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

banda que representa cada uno de los segmentos de red que conforman este diagrama de la figura 3.23.

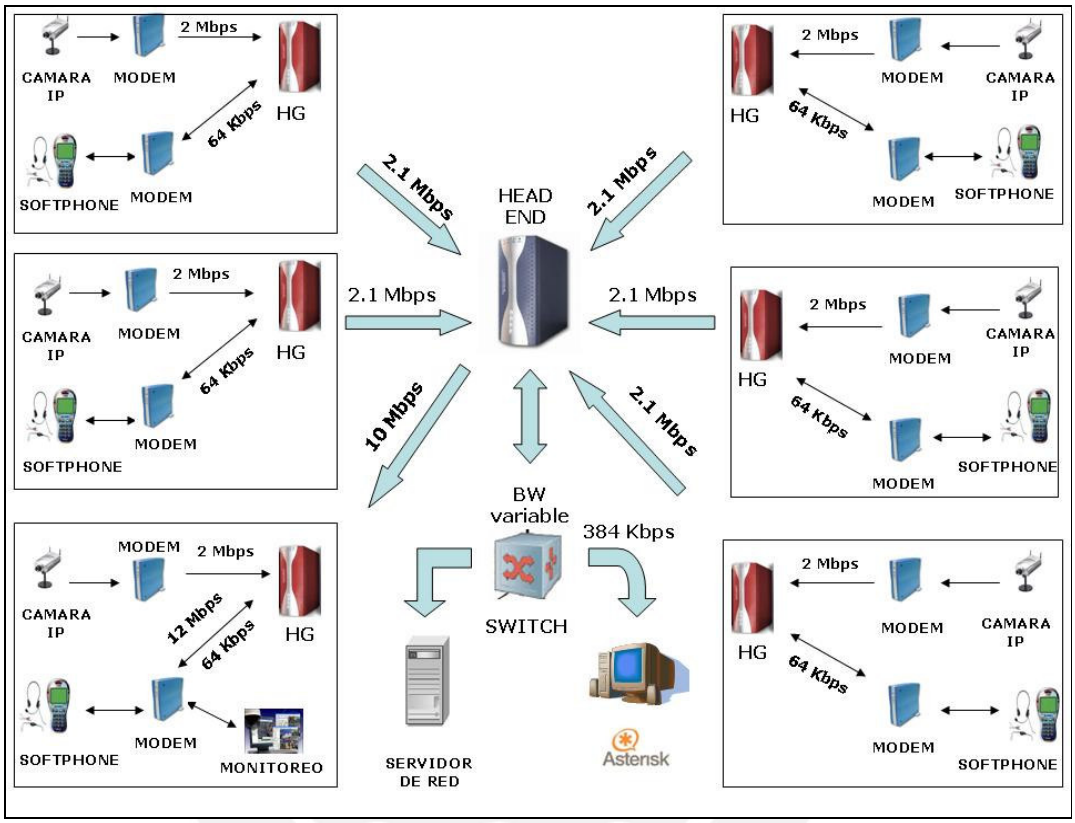


Figura 3.23. Diagrama Completo de la Red

3.6.2. Diagramas de Conexión e Instalación Eléctrica

Hasta este punto del diseño de la red no se había tratado directamente con los factores de interconexión física y eléctrica que están inmersos en el proyecto como tal; de manera que, las siguientes páginas representan una contribución en dicho aspecto, y para conseguirlo se ha organizado el desarrollo de la red en tres entornos principales: interconexión en la localidad, desarrollo en un edificio y finalmente en un departamento:

3.6.2.1. En la Localidad

El despliegue de la red está destinado a cubrir un área aproximada de 3000 m^2 , conformada por 10 edificios y una población cercana a 800 residentes. La figura

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

adjunta muestra con mayor detalle su ubicación geográfica y el área sobre la cual se desarrolla.

Figura 3.24. Ubicación Geográfica del Sector

De la cantidad total de edificios que conforman la zona, se han escogido 6 ejemplares como referencia para este diseño. La ubicación de los equipos sobre estas 6 estructuras responde, sobre todo, a una consideración estratégica en el campo de la seguridad. Es evidente, por ejemplo, que las 3 entradas principales tanto de vehículos como de transeúntes tienen que ser cubiertas y vigiladas constantemente (equipos ubicados en los edificios 2, 3 y 5 de la figura 3.25); por otro lado, se requiere cubrir durante la mayor parte del tiempo las áreas de estacionamiento vehicular, para ello se ha dispuesto específicamente los equipos en los edificios 4 y 6; por último, se ha considerado un equipamiento extra para dar cobertura a la zona donde se encuentra el centro de transformación eléctrica y el centro de administración de red, que es la zona alrededor de la cual se desenvuelve la red de comunicación residencial (para mayor detalle e ilustración de las tomas reales del recinto remitirse al anexo número 5).

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

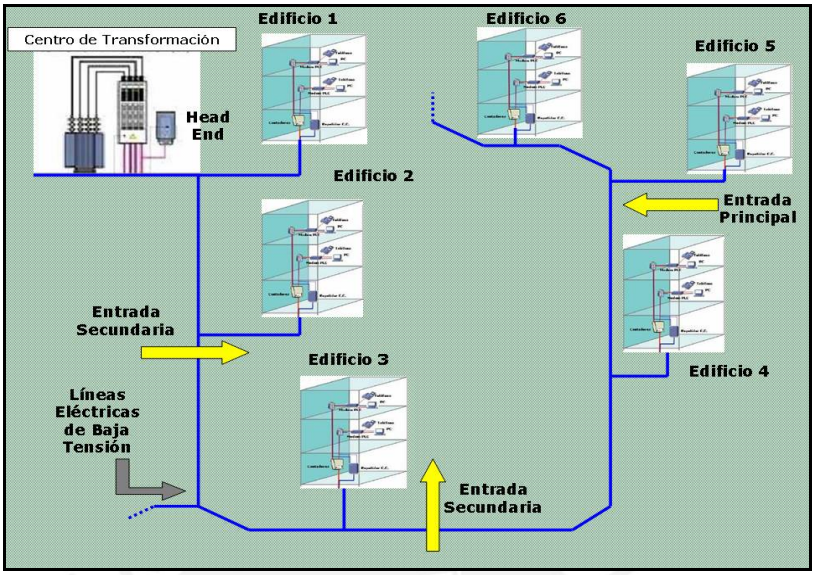


Figura 3.25. Esquema de Interconexión de Red Local

La figura 3.26 permite una visión más real de cómo quedaría la distribución física de los equipos PLC sobre el área de interés; considerando que cada uno de los edificios escogidos trabajará como una especie de nodo de la red (por medio de los HG 's), cumpliendo funciones de regeneración de la señales de datos y administración de los equipos a su cargo en cada edificio según sea necesario.

Figura 3.26. Ubicación Estratégica de Equipos

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.6.2.2. En un Edificio

Para detallar la ubicación y conexión de equipos al interior de esta infraestructura es importante recordar primero que el equipo que realiza una tarea fundamental en este sector es el Home Gateway (HG). Más allá de sus labores de manejo de red local y elemento intermediario con el maestro de la red, la función que lo hace sumamente útil bajo este entorno es la de servir como interfase lógico - eléctrica entre los usuarios y la red de suministro del edificio (véase figura 3.27).

Es decir, el HG recibe la señal de datos diferenciada proveniente de cada uno de los departamentos y cuando lo hace las procesa y modula en una sola señal para reinyectarla luego hacia el exterior. Hay que tomar en cuenta que los tableros de tarificación donde se ubican los medidores son ciertamente perjudiciales para los datos sobre las líneas eléctricas (actúan como filtros pasa bajos); para evitarlos, el HG se vale de los acopladores eléctricos para poder obviar este tramo (ver figura 3.28).

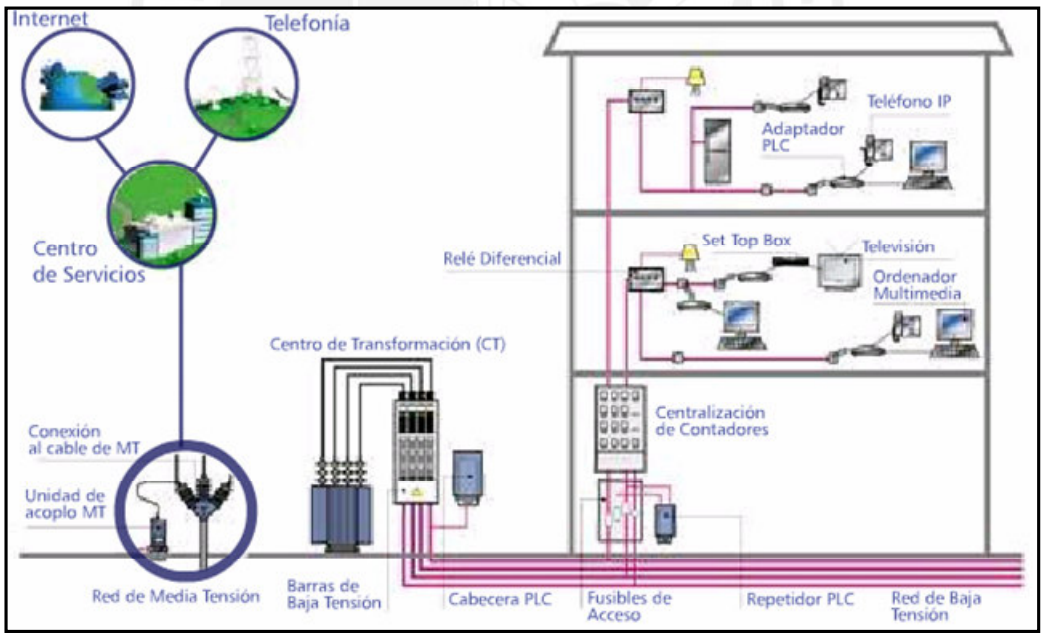


Figura 3.27. Ubicación de Equipos PLC [11]

Las unidades de acoplamiento sirven para adaptar la señal de datos sobre los medios eléctricos de baja o media tensión. Para ello manejan dos tipos de técnica de acuerdo al modo de inyección de la señal: acoplamiento inductivo y acoplamiento capacitivo. El primer método usa la teoría de inducción electromagnética para el acople de la señal

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

mientras que el segundo si realiza un contacto directo con las líneas de potencia para incluir en ellas la señal de datos (ver figura 3.28). Para mayor información técnica sobre acopladores remitirse al anexo número 1 (hojas de datos de los equipos utilizados).

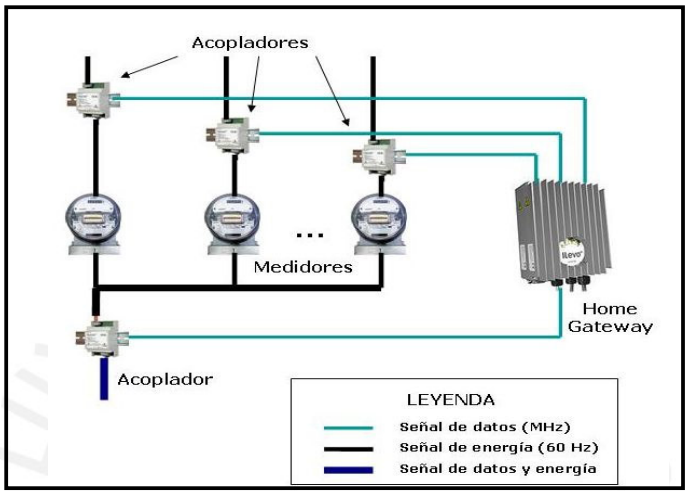


Figura 3.28. Conexión en un Edificio con Acoplamiento Capacitivo

3.6.2.3. En un Departamento

Finalmente, la instalación de los equipos PLC concluye con el trabajo realizado al interior del departamento en donde se ubicarán los equipos de comunicación (en nuestro caso una cámara IP y una computadora). El equipo principal en este entorno es el módem PLC que sirve como interfaz entre la red Ethernet local y las líneas eléctricas del domicilio. En este punto basta con conectar el módem como se indica en la figura 3.29 y luego establecer una conexión hacia los equipos de red (cámara IP o computadora), mediante cableado estructurado categoría 5 EIA/TIA 568B entre cada uno de los puertos 100 Base-T.

Figura 3.29. Diagrama de Conexión en un Departamento [34]

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

3.7. Direccionamiento IP

Debido a que las aplicaciones de voz y vídeo se desarrollan bajo la plataforma del protocolo de Internet, es necesario definir la organización de las direcciones IP a través de las cuales se identificará a cada uno de los usuarios dentro de la red; todo esto bajo el esquema de trabajo de la capa 3 del modelo de referencia OSI (configuraciones en la capa de red).

Antes de definir los parámetros de configuración de la capa de red, se debe tener presente las siguientes especificaciones:

- La ejecución de este diseño comprende el funcionamiento de una red de área local cuyos servicios multimedia se proveen de manera autónoma (sin la necesidad de acceder a una red de área extensa). Sin embargo, dado que existe la posibilidad latente de una futura expansión hacia Internet, se considerará además la presencia de un router que funcione como interfaz entre los paquetes provenientes de la red LAN hacia las redes WAN.
- Se empleará el concepto de subnetting, procedimiento con el cual se limita un intervalo de direcciones IP de acuerdo al número de usuarios que conforman la red; para este efecto se crean rangos de menor magnitud dentro la clasificación tradicional conocidas como clases A, B, C, D y E.
- Se utilizará el rango de direcciones IP privadas pertenecientes a la clase C, la misma que permite rangos desde la dirección 192.168.0.0 hasta la dirección 192.168.255.255.
- Se considera a la red total como un conjunto de segmentos conformado por seis edificios cada uno de los cuales trabajará con un promedio de cuatro direcciones IP (una para la cámara de vídeo IP, otra para la computadora con aplicaciones 'softphone' y 2 extras para futuros usuarios y/o servicios). Es decir, se considera un aproximado de 24 direcciones para el sector usuarios.
- Para la identificación de los equipos de red, se ha determinado un grupo de tres direcciones IP, las cuales están destinadas básicamente al servidor de vídeo, a la central IP y a la puerta LAN del router.
- Se debe garantizar un grupo de direcciones extra para soportar cualquier eventual expansión de la red.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

- Se tiene en cuenta además que el rango de direcciones de la subred debe reservar dos ejemplares tanto para la identificación de la red como para el uso de un dominio de broadcast (dirección mediante la cual se maneja como destino a todos los usuarios de la red mediante la transmisión en difusión).

Considerando todo lo antes descrito se infiere que 32 direcciones IP, con 30 de ellas habilitadas para la designación de equipos, es un número suficiente para cubrir los requerimientos planteados; se procede, bajo esa premisa, con la distribución de la direcciones IP que les serán asignadas a esta red (ver además la tabla 3.8):

Número de Red : 192.168.1.0

Máscara de subred : 255.255.255.224 (/ 27)

Dirección puerta LAN del router : 192.168.1.1 / 27

Dirección de Broadcast : 192.168.1.31 (por defecto)

Equipos	Dirección IP	Máscara de Subred	Puerta de Enlace
Central IP	192.168.1.2	255.255.255.224	192.168.1.1
Servidor de Vídeo	192.168.1.3	255.255.255.224	192.168.1.1
Edificio 1	192.168.1.4-192.168.1.7	255.255.255.224	192.168.1.1
Edificio 2	192.168.1.8-192.168.1.11	255.255.255.224	192.168.1.1
Edificio 3	192.168.1.12-192.168.1.15	255.255.255.224	192.168.1.1
Edificio 4	192.168.1.16-192.168.1.19	255.255.255.224	192.168.1.1
Edificio 5	192.168.1.20-192.168.1.23	255.255.255.224	192.168.1.1
Edificio 6	192.168.1.24-192.168.1.27	255.255.255.224	192.168.1.1

Tabla 3.8. Distribución de Direcciones IP

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.8. Consideraciones en las Fuentes de Energía

Debido a que este trabajo se desarrolla considerando la misma fuente de energía eléctrica tanto para soportar el sistema de comunicación como para la cobertura a lo largo de todo el recinto. Es necesario manejar ciertos parámetros tanto del consumo que ocasionarán los principales equipos, como el relacionado al planteamiento de una propuesta alternativa en caso se vea afectado el suministro.

3.8.1. Consumo de Potencia

Para desarrollar este punto nos valemos de una esquema que muestre los principales equipos de la red y sus respectivos consumos de potencia obtenidos a partir de sus hojas de especificaciones, la tabla referida es la siguiente:

Lista de Equipos	Número de ejemplares	Consumo de Potencia por Unidad (W)	Consumo de Potencia Total (W)
Cámaras de vídeo IP	6	15	90
Central IP (PC)	1	200	200
Switch de comunicaciones	1	55	55
Servidor de gestión de red	1	200	200
Módem PLC	12	8	96
Home Gateway PLC	6	18	108
Equipo cabecera PLC	1	18	18
PC de monitoreo	1	200	200
Consumo de Potencia Total			**967**

Tabla 3.9. Consumo de Potencia de la Red

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Los niveles de consumo de potencia no representan mayor carga considerable a la estación transformadora, ya que el consumo total de la misma equivaldría al consumo que originarían 5 computadoras.

3.8.2. Mecanismo de Contingencia Eléctrica

Frente a un eventual corte en el suministro eléctrico, se puede salvaguardar el funcionamiento de los equipos de alumbrado y fuerza de cada uno de los residentes y a la vez aquellos que brindarán soporte de comunicaciones a la red. Todo ello mediante los grupos electrógenos, que son máquinas que generan energía eléctrica a partir de la fuerza de sus potentes motores de combustión interna. Las características de está maquinaria deberán, por supuesto, simular las condiciones anteriores; es decir, con relación a los detalles eléctricos, ésta deberá proveer de 220 v / 60 Hz a la red con una potencia aparente de 630 KVA (valor aproximado con el que bastaría para mantener el sector de interés). Debe contar con un equipo de arranque por baterías y rectificado en continuo, el motor deberá trabajar con Diesel (menor contaminación), considerando un deposito incorporado de alrededor de 1000 litros de combustible para un promedio de 10 horas de respaldo. La parte física deberá estar asegurada con mecanismos de reducción de vibraciones y ruido y finalmente se debe organizar un accionar inmediato de conmutación en caso de fallas en el suministro principal, mediante un acoplamiento en paralelo.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.9. Evaluación Económica

3.9.1. Descripción y Costo de los Equipos Involucrados

Descripción de Equipos	Marca	Número de Ejemplares	Costo por Unidad ($)	Costo Total ($)
Cámaras de vídeo IP	Axis	6	937.72	5,626.32
Central IP (PC)	Compatible	1	500	500
Central IP (Software)	Asterisk	1	0	0
Switch de comunicaciones	Cisco	1	550	550
Servidor de Monitoreo	Compatible	1	500	500
Software de Monitoreo	Axis	1	832.47	832.47
Software de gestión de red PLC	Corinex	1	166.6	166.6
Paquete de auriculares+ micrófono	Corinex	6	3	18
Software de voz sobre IP	X-Lite	6	0	0
Módem PLC	Corinex	12	138.34	1,660.08
Home Gateway PLC	Corinex	6	300	1,800
Equipo cabecera PLC	Corinex	1	270	270
PC de monitoreo	Compatible	1	500	500
COSTO TOTAL DE EQUIPOS				**12,423.47**

Tabla 3.10. Descripción y Costo de los Equipos

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.9.2. Estudio de las Ventajas Presupuestales que Ofrece PLC

A partir de lo analizado en la sección anterior (3.9.1), queda claro que los gastos relativos a la tecnología de red empleada involucran, hasta el momento, lo relacionado a los equipos PLC y el software para su administración en campo (ver tabla 3.11).

Equipos PLC	Cantidad	Costo Unitario ($)	Costo Total ($)
SW de gestión de red PLC	1	166.6	166.6
Módem PLC	12	138.34	1,660.08
Home Gateway PLC	6	300	1,800
Equipo cabecera PLC	1	270	270
COSTO TOTAL DE EQUIPOS			**3,896.68**

Tabla 3.11. Costo de los Equipos PLC

Una gran parte del presupuesto, sin embargo, debe considerar además los gastos en la implementación. Para tal efecto la tecnología PLC tiene una gran ventaja sobre las demás, dado que esa labor abarca exclusivamente la instalación de los equipos en las posiciones determinadas previamente y no se requiere ningún tendido del medio físico a lo largo del sector ya que éste ya está desplegado.

En la tabla 3.12 de la siguiente página se infieren algunas cifras aproximadas con relación a los costos de instalación de los equipos PLC. Para ello, se ha tomado como base las cifras que se manejan en otros tipos de servicios de telecomunicaciones pero que representan un nivel de exigencia similar.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Procedimientos	Costo por Equipo ($)	Cantidad de Equipos a Instalar	Costo Total ($)
Instalación de los HG	200	6	1,200
Instalación del Módem Cabecera (HE)	300	1	300
COSTO TOTAL DE INSTALACION			**1,500**

Tabla 3.12. Costos de Instalación

En términos globales los costos de implementación referentes a la tecnología PLC implican un gasto que bordea los $ 5, 500. Esta cifra adquiere relevancia al ser contrastada con aquella que se obtendría con otra tecnología de red; para tal efecto, analizamos brevemente un presupuesto considerando otras variantes.

Dos de las opciones que se podrían manejar como alternativa son la implementación de la red con fibra óptica o con soluciones inalámbricas. Para nuestro caso habrá que descartar esta última opción (WLAN), ya que no es muy eficiente cuando se trata de soluciones multimedia de gran ancho de banda; más aún, la topología y las mínimas distancias consideradas en el diseño hacen que su elección sea desacertada.

Por otro lado, la solución con fibra óptica parece ser la que más se podría ajustar a nuestro caso. Su implementación, empero, es mucho más exigente que la estudiada con PLC. Los costos relacionados a la misma se describirán en breve en la tabla 3.13.

La cifra que bordea los 19,000 dólares se ha estimado a partir de la creación de una anillo de fibra óptica a lo largo de la residencial. Para menor probabilidad de error en los cálculos y siendo consecuentes con la idea inicial de minimizar costos, se ha considerado que los equipos conversores de fibra a cobre se ubicarán en el primer piso de cada edificio y que los usuarios accederán a la red mediante tendido de cableado UTP a lo largo del edificio. En este caso las cifras exactas no han sido calculadas pero se prevé que los gastos por el material y el tendido del mismo en cada

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

uno de los 6 edificios hará que la suma se redondee a los 20,000 dólares como un monto más aproximado.

Descripción	Cantidad	Valor Unitario ($)	Valor Total ($)
Cable de Fibra Óptica Multimodo	500 metros	3.69	1,845
Tendido de la Fibra	500 metros	4.55	2,275
Jumper de FO Multimodo Dúplex	6	45.45	272.7
Conversor de Fibra a UTP Fast Ethernet	6	500	3,000
Cabecera de Fibra para 6 Filamentos	6	206.25	1,237.5
Obras Civiles	500 metros	20	10,000
COSTO TOTAL DE IMPLEMENTACIÓN			**18,630.2**

Tabla 3.13. Costos Relacionados a una Solución con Fibra Óptica

A pesar de que las soluciones con fibra óptica presentan un excelente desempeño en las aplicaciones de telecomunicaciones, es evidente que su desarrollo no es del todo adecuado en nuestro caso dado que el mismo involucra una fuerte inversión económica de cerca del cuádruple del que se necesitaría para el mismo propósito usando tecnología PLC.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

CAPÍTULO 4
ANÁLISIS DE LA TECNOLOGÍA DE RED EMPLEADA

En rigor a las alternativas de solución planteadas en el capítulo anterior; no queda sino demostrar en cierta forma la validez de las tecnologías con las que se piensa trabajar para su desarrollo. Bajo esa premisa se procederá con la presentación de algunas pruebas de laboratorio realizadas en virtud de este trabajo de investigación, considerando la implementación de una pequeña red LAN en la que se ejecuten funciones similares a las de la red originalmente propuesta.

4.1. Condiciones de Simulación

En dichas experiencias se ha considerado el uso de diversas aplicaciones de usuario que se realizan a través de la plataforma de protocolos IP y que usan como medio de transporte la red eléctrica de baja tensión. En cuanto a las aplicaciones, sirve decir que se trata básicamente de soluciones de voz y vídeo sobre IP implementadas con diversos accesorios de comunicación (hardware y software) adecuados a las computadoras, las mismas que trabajan como el eje rector del entorno.

Para efectos de estos procedimientos; se ha ensayado con equipos que se asemejen, en la medida de las posibilidades de equipamiento del laboratorio, a los que se usarían realmente en caso de una implementación. Por ejemplo, para los servicios de voz sobre IP se ha hecho uso de un software de aplicación que simule la labor de un teléfono IP y otro que haga las veces de central telefónica; para los de vídeo se ha empleado una cámara Web y para la interconexión por las redes eléctricas del laboratorio se ha usado un conjunto de 3 módems PLC de primera generación con los que cuenta la Universidad. La figura adjunta muestra el esquema de conexión empleado.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Figura 4.1. Esquema Básico Usado para las Pruebas de Laboratorio

El elemento de red que nos permitirá interactuar con las aplicaciones multimedia es, para efectos de estas pruebas, el módem PLC. Dada su importancia se mostrará brevemente la forma en la que se lleva a cabo su instalación y puesta en marcha para el inicio de las operaciones.

La figura 4.2 muestra el equipo con la tecnología 'Power Line Communications' y sus dos interfases de red. Para la comunicación con la PC cuenta con un puerto Ethernet y la lleva a cabo mediante un cable del tipo UTP categoría 5. Para la transmisión de los datos a través de la red eléctrica lo hace mediante el puerto que usa también para la toma de energía (ver figura 4.3).

Figura 4.2. Módem PLC y sus Interfases de Red Eléctrica y Datos

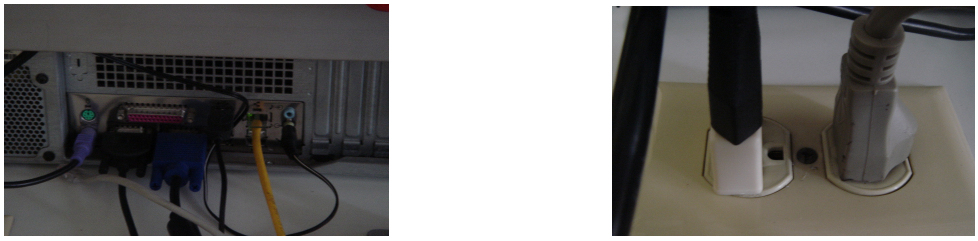


Figura 4.3. Conexiones hacia la Computadora y el Suministro Eléctrico

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

A nivel de configuración, la detección del módem por parte de la PC es automática luego de que se le asigne a ésta, los parámetros de red adecuados. Es decir, en caso de una configuración en red local, cada una debe tener una dirección IP única agrupadas mediante la identificación de la submáscara adecuada; en nuestro caso bastará con que ésta sea de la clase C (con opción hasta 256 direcciones). Se eligió por tanto la 255.255.255.0, con el rango de direcciones a partir de la 192.168.1.0.

4.2. Pruebas de Voz sobre IP

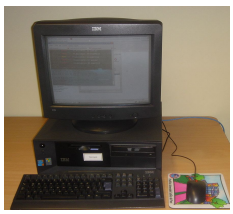
Con relación a estas pruebas se debe afirmar que éstas, a diferencia de las otras simulaciones, si se han resuelto por medio de una solución muy similar a la que se usará en condiciones reales; dado que las herramientas de software y los equipos de interfase son prácticamente los mismos, la diferencia radica principalmente en la topología de red empleada (punto a punto a través de módems); a diferencia de la configuración punto a multipunto con estructura jerárquica con la que ha sido pensada la verdadera red (uso adicional de módem de cabecera: Head End y un administrador local Home Gateway).

4.2.1. Equipos y Accesorios Requeridos

Para llevar a cabo las experiencias señaladas anteriormente se utilizaron los siguientes equipos y accesorios que se describen en la figura 4.4.

Módem PLC (3)

Computadora Personal (3)



Softphone X – Lite (2)

Auriculares más Micrófono (2)

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

Tomacorriente 220V – 60 Hz

Cable de Red CAT – 5 (3)

Analizador de Protocolos de Red (2)

Software Libre Central IP (1)

Figura 4.4. Equipos y Accesorios Usados en las Pruebas de VoIP

4.2.2. Desarrollo de las Pruebas

Para llevar a cabo los objetivos trazados se ha considerado el siguiente procedimiento:

Se habilitó tres máquinas del laboratorio, una de las cuales fue configurada como central IP a través del Software libre provisto por Asterisk y que se ejecuta sobre Sistema Operativo Linux. La dirección IP de esta máquina se registró como la 192.168.35.48. Las otras computadoras asumieron el rol de usuarios entre los cuales se establecerá la comunicación, para ello se tuvo por un lado la PC con dirección IP 192.168.35.24 y por otro, su par con dirección 192.168.35.27.

A la computadora con IP 192.168.35.24 se le asignó el anexo 445 y a la 192.168.35.27, el 444. La configuración se realizó en la PC servidor y el modo de iniciación de llamada mediante el software de aplicación usado se ilustra a continuación en las figuras 4.5 y 4.6 respectivamente:

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Figura 4.5. Inicio de Sesión

Figura 4.6. Llamada Establecida

Quisimos comprobar, en primer lugar, el modo de funcionamiento de este protocolo (SIP), para lo cual se manejo como herramienta un software analizador de paquetes y tráfico en la red (WireShark). Con ello se verificó que este protocolo trabaja bajo dos procedimientos: SIP para establecer la comunicación (parámetros de señalización) y RTP para hacer efectivo el intercambio de información luego de que se habilitó la llamada.

```
192.168.35.24 192.168.35.48  SIP/SDF Request: INVITE sip:445@192.168.35.48, with session description
192.168.35.48 192.168.35.24  SIP     Status: 407 Proxy Authentication Required
192.168.35.24 192.168.35.48  SIP     Request: ACK sip:445@192.168.35.48
192.168.35.24 192.168.35.48  SIP/SDF Request: INVITE sip:445@192.168.35.48, with session description
192.168.35.48 192.168.35.24  SIP     Status: 100 Trying
192.168.35.48 192.168.35.24  SIP     Status: 180 Ringing
192.168.35.48 192.168.35.24  SIP/SDF Status: 200 OK, with session description
```

Figura 4.7. Captura de Paquetes de Inicialización

La figura 4.7 muestra el intercambio de información entre las máquinas con extensión '.24' y '.48' las cuales se encuentran negociando el establecimiento de la comunicación. Posteriormente se envían unos paquetes de confirmación como se muestra en la figura 4.8:

```
192.168.35.24 192.168.35.48  RTCP    Receiver Report
192.168.35.48 192.168.35.24  RTP     Payload type=GSM 06.10, SSRC=1771735631, Seq=48299, Time=80
```

Figura 4.8. Captura de Paquetes de Confirmación

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Finalmente se establece la comunicación por RTP entre las 2 máquinas en donde la central hace de intermediaria, como se aprecia a continuación e la figura 4.9 :

192.168.35.48	192.168.35.24	SIP	Status: 180 Ringing
192.168.35.48	192.168.35.24	SIP/SDP	Status: 200 OK, with session description
192.168.35.24	192.168.35.48	RTCP	Receiver Report
192.168.35.48	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=1771735631, Seq=48299, Time=80
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7738, Time=202160
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6164, Time=2971900
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7739, Time=202320
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6165, Time=2972060
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7740, Time=202480
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6166, Time=2972220
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7741, Time=202640
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6167, Time=2972380
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7742, Time=202800
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6168, Time=2972540
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7743, Time=202960
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6169, Time=2972700
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7744, Time=203120
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6170, Time=2972860
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7745, Time=203280
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6172, Time=2973180
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7747, Time=203600
192.168.35.24	192.168.35.48	SIP	Request: ACK sip:445@192.168.35.48
192.168.35.48	192.168.35.24	SIP/SDP	Request: INVITE sip:alice@192.168.35.24:5910, with session desci
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6173, Time=2973340
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7748, Time=203760
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6174, Time=2973500
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7749, Time=203920
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6175, Time=2973660
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7750, Time=204080
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6176, Time=2973820
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7751, Time=204240
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6177, Time=2973980
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7752, Time=204400
192.168.35.24	192.168.35.48	SIP/SDP	Status: 200 OK, with session description
192.168.35.48	192.168.35.24	SIP	Request: ACK sip:alice@192.168.35.24:5910

Figura 4.9. Captura de Paquetes de Negociación

Después de ese procedimiento ambos usuarios pueden comenzar una comunicación directamente (véase la figura 4.10). El estándar de compresión usado es el GSM que es una variante del que se emplea para la comunicación celular, está regulado por la ETSI y maneja anchos de banda de alrededor de 13 Kbps. Los protocolos de compresión, sin embargo, son múltiples y configurables, todo dependerá de los dos principales parámetros que hay que tener en cuenta para la comunicación de voz: calidad en la comunicación o consumo de ancho de banda.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

192.168.35.24	192.168.35.48	SIP/SDP	Status: 200 OK, with session description
192.168.35.48	192.168.35.24	SIP	Request: ACK sip:alice@192.168.35.24:5910
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6178, Time=2974140
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7753, Time=204560
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6179, Time=2974300
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7754, Time=204720
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6180, Time=2974460
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7755, Time=204880
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6181, Time=2974620
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7756, Time=205040
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6182, Time=2974780
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7757, Time=205200
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6183, Time=2974940
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7758, Time=205360
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6184, Time=2975100
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7759, Time=205520
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6185, Time=2975260
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7760, Time=205680
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6186, Time=2975420
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7761, Time=205840

Figura 4.10. Establecimiento de la Comunicación

4.2.3. Resultados

En la gráfica que se analizará en breve (figura 4.11) se puede apreciar también el modo con el que opera el protocolo SIP; es decir, se muestra en un inicio dos pequeños picos que indican la transferencia de datos debido al inicio de sesión y luego de ello un consumo constante de 0.05 % de 100 Mbps durante la conversación (aproximadamente 50 Kbps).

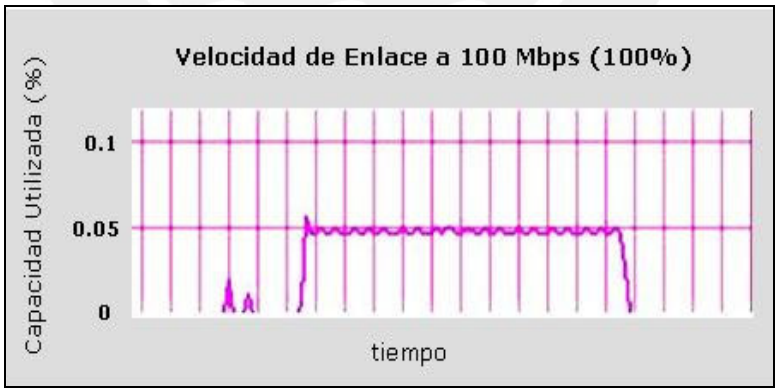


Figura 4.11. Inicio y Establecimiento de la Llamada

La conversación se realizó por un breve intervalo de tiempo que también fue capturado por el software de monitoreo de tráfico, cuando se termina la llamada se nota una caída prominente de la gráfica. Ver figura 4.12.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

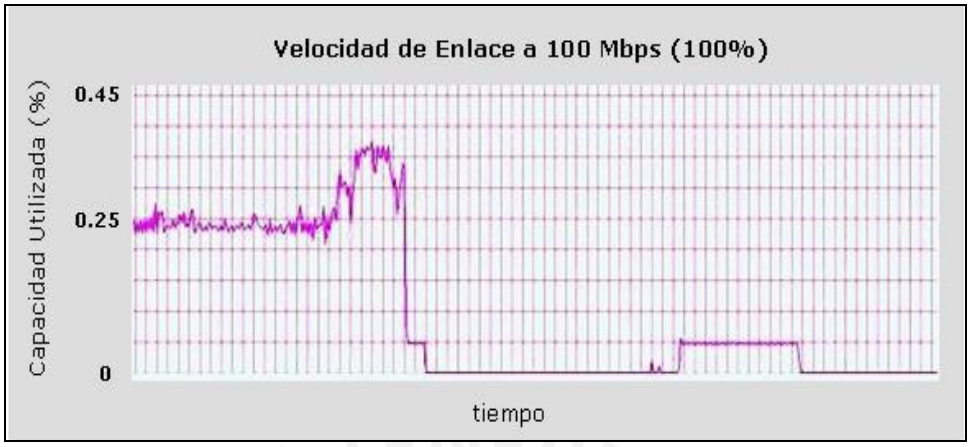


Figura 4.12. Captación del Intervalo de Conversación

4.3. Pruebas de Vídeo IP

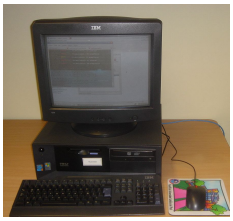
Para simular las condiciones reales se manejó el mismo esquema que el planteado en el diseño; es decir, una computadora (192.168.35.24) se encargó de generar la información audiovisual a partir de una cámara Web y un software de aplicación cliente/ servidor (NetMeeting). La segunda computadora (1962.168.35.27) recibía la información de vídeo a través de una conexión punto a punto sobre la red eléctrica y estuvo habilitada para intercambiar cualquier otro tipo de información. Aunque no se mencionó anteriormente, es importante señalar que las condiciones de las pruebas se hicieron bajo ciertas exigencias de interferencia y ruido, ya que se encendieron las lámparas fluorescentes y los ventiladores del laboratorio durante el periodo en que se realizaron las mismas (ver figura 4.13).

Figura 4.13. Laboratorio de Software para Telecomunicaciones

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

4.3.1. Equipos Requeridos

Módem PLC (2)



Computadora Personal (2)

Cámara Web (1)

Software NetMeeting (2)

Tomacorriente 220V – 60 Hz

Cable de Red CAT – 5 (2)

Analizador de Protocolos de Red (2)

Figura 4.14. Equipos y Accesorios Usados en las Pruebas de Vídeo IP

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

4.3.2. Desarrollo de Pruebas y Resultados

NetMeeting es una herramienta de Microsoft Windows con la que se pueden llevar a cabo diversas aplicaciones múltiples de voz, vídeo y transferencia de datos. En nuestro caso se usó, básicamente, para lo relacionado a vídeo y voz, este último para comparar características de conversación con relación a lo llevado a cabo en la experiencia anterior. La solicitud de comunicación se realiza por medio de la dirección IP de la máquina destino (figura 4.15) y no es, sino hasta cuando ésta acepta la llamada, que se puede proceder con la comunicación (ver figura 4.16).

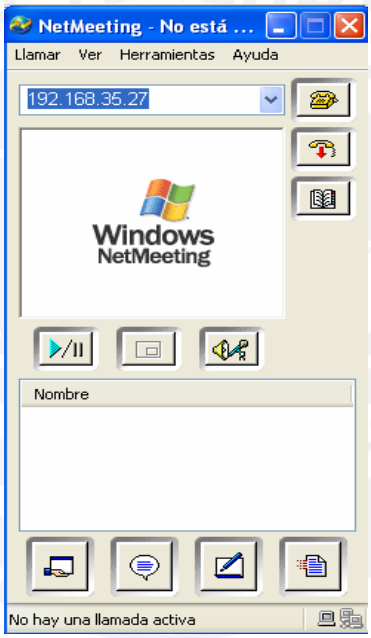


Figura 4.15. Solicitud de Llamada mediante su Dirección IP

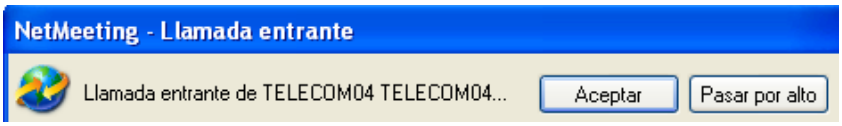


Figura 4.16. Aviso de Llamada Entrante

a) NetMeeting para Aplicaciones de Voz

En este procedimiento se estableció una llamada y se capturó el consumo de ancho de banda durante su duración. De acuerdo a los resultados obtenidos se aprecia con claridad de que este software propietario de Microsoft exige menor ancho de banda de

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

la red y según ello se aprecia que éste representa casi la mitad de lo que consume la aplicación de voz con X - Lite.

Tal como se aprecia en la figura 4.17, se obtienen valores promedio que indican el 0.02 % del total de 100 Mbps, lo que representa consumos de alrededor de 20 Kbps.

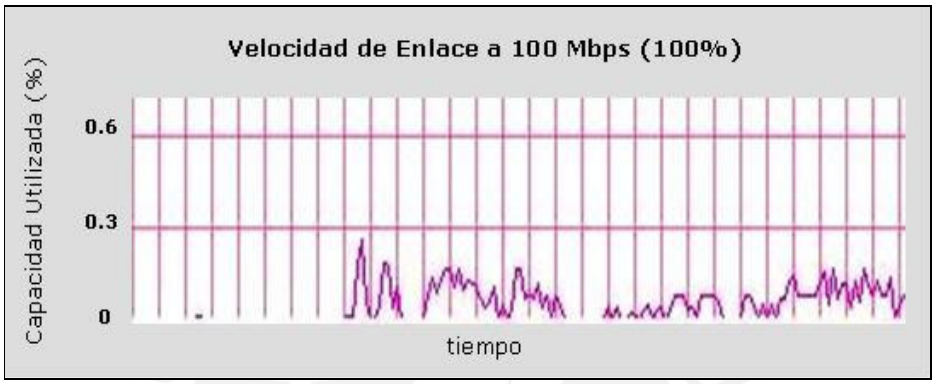


Figura 4.17. Consumo de Ancho de Banda para Aplicaciones de Voz

b) NetMeeting para Aplicaciones de Vídeo

Luego de establecida la comunicación entre las dos computadoras se puede hacer una solicitud de uso de vídeo en la sesión, para lo cual la interfase de NetMeeting se muestra como sigue en la siguiente figura:

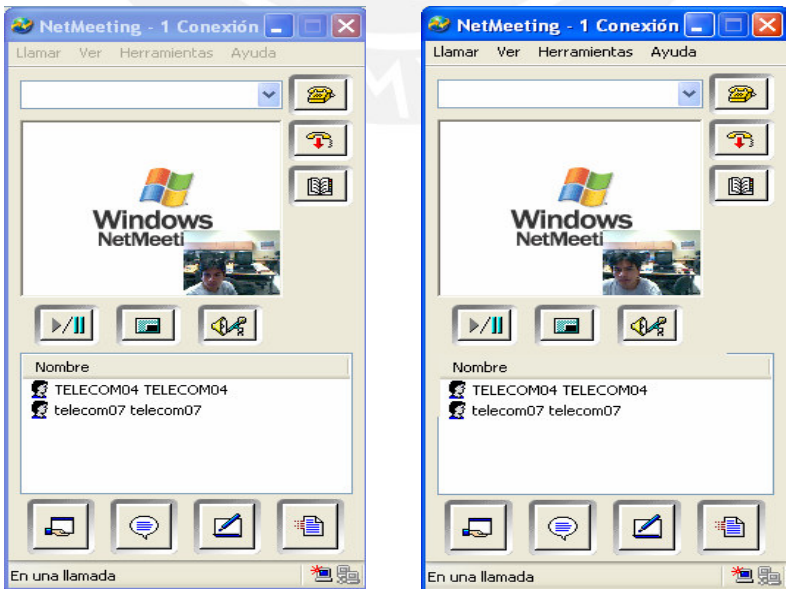


Figura 4.18. Consumo de Ancho de Banda para Aplicaciones de Vídeo

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Cuando se verifica el consumo de ancho de banda se observa valores de 0.25 % del total (equivale a 250 Kbps). Luego se probó con captura de imágenes sin movimiento (imagen estática) y se verificó que los 'códecs' de compresión de vídeo disminuyeron la transferencia, lo que se evidencia en los dos picos caídos de la figura 4.19.

Figura 4.19. Comparación entre el Consumo de Voz y el de Vídeo

c) NetMeeting para Aplicaciones de Vídeo más VoIP con X - Lite

Durante este procedimiento se activó las dos aplicaciones; es decir, se habilitó una llamada con el Softphone X – Lite y se mantuvo la transmisión de vídeo con NetMeeting. Al hacerlo, se consideró primero la transmisión de conversación junto con la de vídeo y los resultados mostraron consumos del orden del 0.46 % del total; finalmente con la transmisión de 'silencios' la tasa cae hasta 0.35 %. Véase las figuras 4.20 y 4.21.

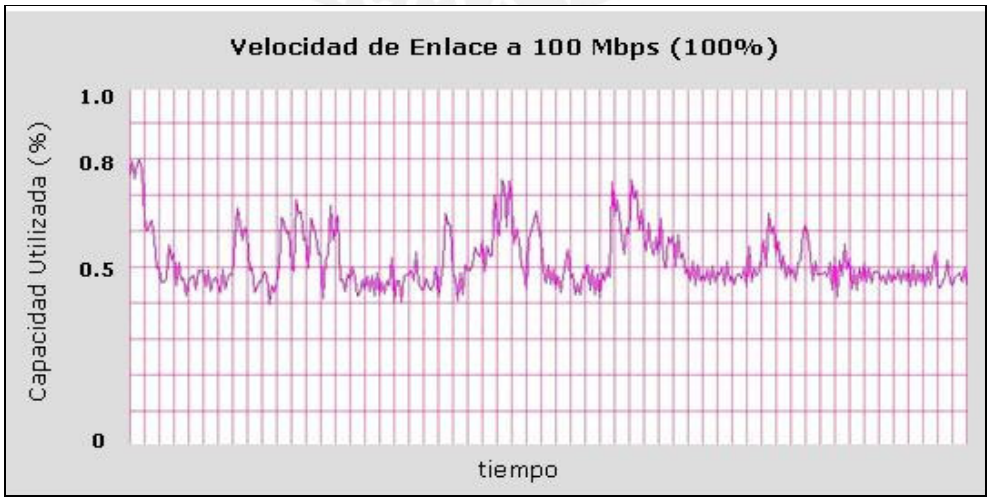


Figura 4.20. Consumo entre Aplicaciones de Voz y Vídeo

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Figura 4.21. Periodo de Tiempo de Transmisión de Vídeo y 'Silencios'

d) NetMeeting para Aplicaciones de Vídeo con Ampliación de Imagen

Se configuró el programa para que la imagen captada sea mucho mayor a la que se estuvo transmitiendo en la experiencia anterior. Los resultados se muestran en la figura adjunta:

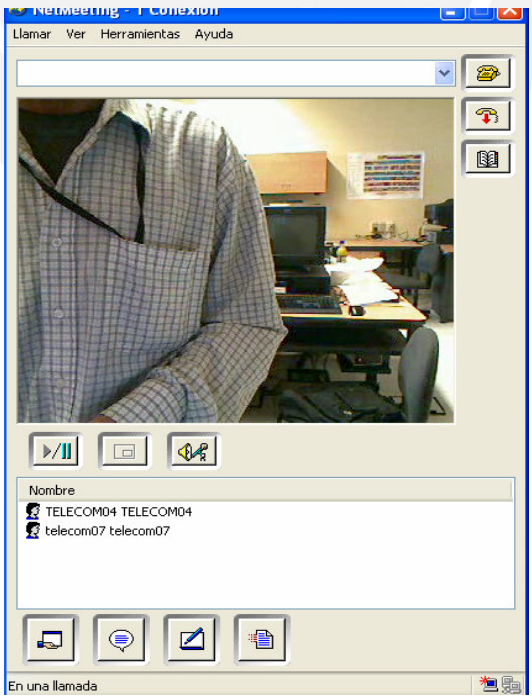


Figura 4.22. Transmisión de Vídeo IP con Imágenes de Mayor Tamaño

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Se observa que la imagen mantiene una excelente resolución y que la secuencia es sumamente fluida y con una muy buena calidad.

Con relación al consumo de ancho de banda se puede apreciar que éste, como es lógico, se ha incrementado hasta un porcentaje representativo de 0.55, lo que representa un valor cercano a 550 Kbps respecto a los 250 del consumo de la secuencia de vídeo anterior. Esto último se aprecia claramente en la figura siguiente.

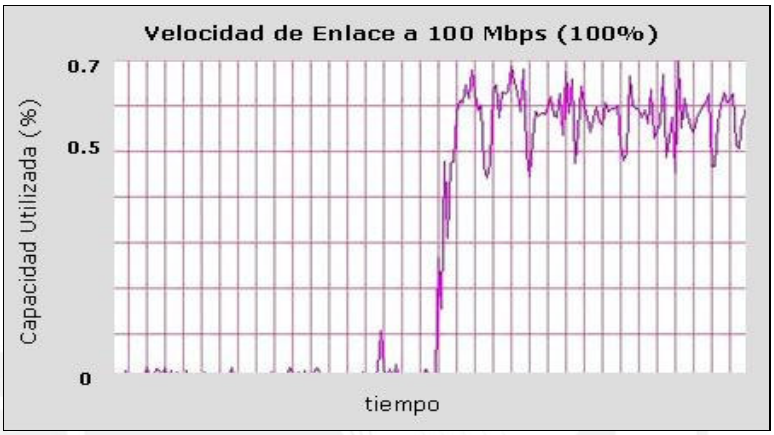


Figura 4.23. Consumo de Ancho de Banda (Mayor Tamaño de Imagen)

Por último se procedió a capturar las diferencias en el consumo de ancho de banda para las diversas aplicaciones en una sola gráfica. Al inicio se considera sólo la transmisión de vídeo con NetMeeting, luego de un tiempo se adhiere el servicio de VoIP con X – Lite, posteriormente se deja trabajando sólo a éste último y finalmente se termina de cerrar ambas aplicaciones, en donde el tráfico cae completamente (ver figura 4.24).

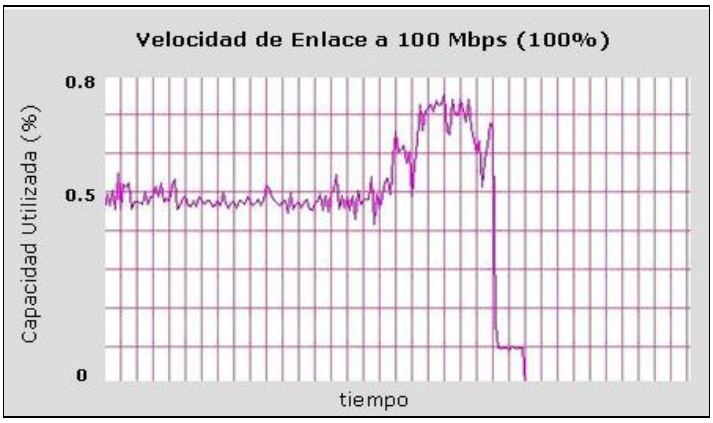


Figura 4.24. Variación Continua de Aplicaciones Multimedia

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

CONCLUSIONES

El inicio de este proyecto de investigación surgió como un aporte a la lucha contra la delincuencia común experimentada a diario por muchos de nosotros. Su desarrollo, sin embargo, implicaba ahondar más en las tecnologías con las que se pensase resolver esa problemática y fue allí donde, sobre la base de muchas otras técnicas estudiadas y ampliamente extendidas, se eligió la tecnología de acceso y red PLC a manera de plataforma de comunicaciones aprovechando su cobertura globalizada. Luego de su estudio se concluye, en términos por demás alentadores, lo siguiente:

1. La tecnología considerada para la puesta en marcha de este diseño (PLC) representa una opción sencilla y rápida de implementar si la comparamos con el desgaste que implicaría las soluciones con fibra óptica (tendido subterráneo o aéreo de la fibra) o a través de medios inalámbricos (instalación de antenas de gran magnitud).

2. Desde el punto de vista económico, una red de comunicaciones implementada a partir de la red eléctrica existente resulta ser conveniente si se toma en cuenta el ahorro que implica no invertir en material ni obras de infraestructura.

3. Los equipos PLC considerados en este diseño soportan grandes niveles de ancho de banda (200 Mbps) y total disponibilidad para el despliegue de aplicaciones en tiempo real (protocolos de priorización de tráfico, detección y corrección de errores hacia delante, clasificador de servicios, etc.). Estas características garantizan una red interactiva, rápida y sin limitaciones de cobertura.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

4. Los software de aplicación masivos, la plataforma de protocolos IP y el poder de procesamiento y memoria que poseen actualmente las computadoras personales, hacen que sea factible reemplazar los complejos sistemas de soporte de servicios como las centrales telefónicas y los servidores de vídeo, generando así una notable disminución en los costos de implementación.

5. Las pruebas de laboratorio permitieron constatar el buen desempeño de la tecnología PLC frente a los retos que implica trabajar con las aplicaciones en tiempo real. Aquello es aún más meritorio si consideramos que estos ensayos se realizaron al interior del pabellón con mayor contaminación a nivel de interferencia electromagnética, al interior de una sala con equipos eléctricos encendidos y con módems PLC de primera generación.

6. La red de comunicaciones planteada en este diseño ha sido pensada para interactuar sin mayor problema con cualquier otra red de acceso de área extensa (WAN). Este despliegue significaría que en un futuro su nivel de servicio no sólo se limitaría al campo de la seguridad automatizada sino que impulsaría a que los usuarios la puedan tomar como una red de última milla capaz de interactuar con el exterior a partir de aplicaciones como la voz y el vídeo sobre IP.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

RECOMENDACIONES

Luego de evaluar extensamente las diversas estrategias de solución, se consideró un diseño que para entonces se avizoraba como el idóneo para cubrir con los objetivos planteados de manera eficaz y eficiente. A pesar de ello, no deja de tener validez cualquier otro aporte que emerja como una forma de mejorar el rendimiento del producto. Bajo esa óptica es que las siguientes líneas, a manera de recomendaciones, intentarán enrumbarse en caso de cualquier opción de implementación o mejora del planteamiento original.

1. Se debe, antes de cualquier intento de implementación, asegurar o impulsar la existencia de una normativa vigente al respecto en los sectores de regulación públicos. De manera que las redes eléctricas puedan ser reconocidas como medios de transmisión válidos en la puesta en marcha de cualquier proyecto de telecomunicación en el Perú.

2. Materializar el diseño propuesto en este documento implica además tramitar los permisos respectivos con la empresa que administra la red eléctrica, con la municipalidad del distrito involucrado y con la junta de vecinos que representan los intereses del recinto.

3. Para efectos de una futura implementación se debe obtener, o estimar con técnicas seguras, el diagrama de conexiones de todo el recinto residencial para facilitar y agilizar su desarrollo.

4. A pesar de que la solución asumida para la comunicación de voz sobre IP considera la instalación de un módulo público conformado por una computadora y sus respectivos accesorios. Dicho equipamiento se puede

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

reemplazar o complementar con teléfonos IP con las prestaciones necesarias o incluso por teléfono analógicos, siempre y cuando se garantice su competitividad costo – beneficio.

5. Los mecanismos de contingencia eléctrica para salvaguardar la red y los otros servicios se suelen implementar en situaciones de alto riesgo o en la que las medios de comunicación son sumamente críticos (empresas bancarias, administrativas, etc.); en este caso se ha planteado como una alternativa que existe y que no debe ser descartada de plano en caso se precise de un grado de funcionamiento totalmente ininterrumpido.

6. Se debe tener presente que la lista con los precios de los equipos ha sido incluida como una referencia que puede variar en el tiempo.

7. Los gastos extraordinarios por trabajos de mano de obra en la instalación y configuración de los equipos se han considerado a partir de referencias provenientes de otros trabajos de puesta en marcha; es decir la misma no está exactamente dimensionada para este proyecto, pero si nos da un buen nivel de referencia.

8. El hecho de garantizar la tecnología necesaria para resolver problemas implica también la capacitación del personal de seguridad o de cualquier otro que tenga acceso privilegiado a los equipos. Sólo de esta manera se puede pensar en la eficiencia de cualquier solución planteada.

9. Aún cuando las medidas consideradas en el diseño de este proyecto involucran servicios de voz y vídeo sobre IP; las características del mismo hacen posible, también, la adaptación de soluciones en banda angosta que se puedan complementar y hacer más robusto al sistema. Dicho en otros términos, se podría adaptar diversos mecanismos digitales como el de apertura y cierre de portones, activación de alarmas sonoras o visuales, entre otros.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ANEXOS

La información relacionada a los anexos de este documento se encuentra adjunta en un CD. La organización de sus contenidos es como sigue:

- ANEXO 1: HOJAS DE DATOS DE LOS EQUIPOS UTILIZADOS
- ANEXO 2: ESTÁNDARES PLC
- ANEXO 3: PLANOS ELÉCTRICOS
- ANEXO 4: PRUEBAS DE LABORATORIO
- ANEXO 5: FOTOS DE LA RESIDENCIAL EN ESTUDIO

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FUENTES

[1] ELLIOTT NEWCOMBE INTELLON CORPORATION
2000 Intellon High Speed Power Line Communications [en línea] California: Hot Interconnects. [consultado 2006/05/10] <http://www.hoti.org/archive/hoti8_toc.html>

[2] PAUL, Ho
2006 Transmission Techniques for Broadband Satellite Communications [en línea] California: Simon Fraser University. [consultado 2006/05/08] <http://pdf.aiaa.org/preview/CDReadyMICSSC06_1269/PV2006_5447.pdf>

[3] DALELA, Paul y MOHAN, Anand
2005 A New Concept of Digital Power Line Carrier Communication for Rural Applications [en línea] New Delhi (India): IEEE ICPW2005. [consultado 2006/05/10] <http://www.ursi.org/Proceedings/ProcGA05/pdf/C01.4(0115).pdf >

[4] COGENCY SEMICONDUCTOR INC.
2001 Data Communications over Power Lines [en línea] California: Cryptography & Network Security. [consultado 2006/04/15] <http://cnscenter.future.co.kr/resource/hot-topic/homenet/Data_Communications.pdf>

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

[5] SUMITOMO ELECTRIC INDUSTRIES
2004 Development of High Speed Power Line Communication Modem [en línea] Tokio : Information & Communication Systems. [consultado 2006/04/01] <http://www.sei.co.jp/tr_e/t_technical_e_pdf/58-06.pdf>

[6] BUZID, Trent y Reinhardt Simon
2005 A Comparison of OFDM and Non-linear SC/FDE Signals: Non-linear Amplification [en línea] Erlangen (Germany): University of Erlangen-Nuernberg, Institute of Electronics Engineering. [consultado 2006/04/23] <http://www.lfte.de/~reinhardt/publications/EW2005.pdf>

[7] CORRIDOR SYSTEMS, INC.
2004 Power line communications - Electrifying the broadband [en línea] California: PC Magazine M&NE. [consultado 2006/04/05] <http://www.corridor.biz/pdf/PC-mag-article.pdf>

[8] ROJO, Ignacio
2005 PLC: Internet por el enchufe [en línea] Madrid : Internet y Telecomunicaciones. [consultado 2006/04/01] <http://www.consumer.es/web/es/tecnologia/internet/2005/07/21/143900.php>

[9] TECNOCOM
2005 Power Line Communications [en línea] Madrid : Soluciones Basadas en Tecnología PLC . [consultado 2006/04/01] <http://www.upaplc.com/_files/fichas_ingls1.pdf >

[10] CENTRO POLITÉCNICO SUPERIOR, UNIVERSITY OF ZARAGOZA
2004 Research Areas for Efficient Power Line Communication Modems [en línea] Zaragoza (España) : Department of Electronics and Communications Engineering. [consultado 2006/05/15]

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

<http://www.isplc2004.unizar.es/Research%20Areas%20for%20
Efficient%20Power%20Line%20Communication%20Modems.pdf>

[11] UNIVERSIDAD COMPLUTENSE DE MADRID
2005 La Tercera Alternativa de Red Residencial: Comunicaciones a través de Red eléctrica [en línea] Madrid: [consultado 2006/05/15]
<http://www.fdi.ucm.es/profesor/jse ptien/WEB/Docencia/
AVRED/Documentos/PLC.ppt>

[12] HERNÁNDEZ REZA, Aslhey
2004 Transmisión de Voz y Datos a Alta Velocidad a través de los Cables Eléctricos. *Telemática* [en línea] , III (7). [consultado 2006/04/01]
<http://www.cujae.edu.cu/revistas/telematica/Articulos/110.htm>

[13] LÓPEZ C, Carlos Enrique
2003 ¿Internet por el cable de la luz? [en línea] Madrid:
Alambre Weblog de Tecnología y Sociedad. [consultado 2006/04/01]
<http://www.alambre.info/2003/11/03/internet-por-el-cable-de-la-luz/>

[14] ROMO ZAMUDIO, José Fabián
2005 PLC: no más cables [en línea] México DF :
Universidad Nacional Autonoma de México. [consultado 2006/04/01]
<http://www.enterate.unam.mx/Articulos/2005/marzo/plc.htm>

[15] Comunicación por la Línea de Potencia
2005 Comunicación por la Línea de Potencia [en línea] Madrid:
Institute for Prospective Technological Studies. [consultado 2006/04/01]
<http://www.jrc.es/pages/iptsreport/vol29/spanish/ICT2S296.htm>

[16] UNIVERSIDAD DEL CAUCA.
Facultad de Ingeniería Electrónica y Telecomunicaciones.
2004 Transmisión de datos por la red eléctrica empleando la modulación FSK. Proyecto: Nuevas Tecnologías de Telecomunicaciones (Marzo). Popayán

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

[17] LOPES TEIXEIRA, Catarino
2003 PLC. Una solución para los países del tercer mundo.
Telemática [en línea] , II (22). [consultado 2006/04/01]
<http://www.cujae.edu.cu/revistas/telematica/Publicaciones/
Telem@tica_AnoII_No22.pdf>

[18] ALCÒCER, Carlos
2000 Redes de Computadoras. 2a. Ed.
Lima : Infolink

[19] ZINC NETWORKS
2003 Accelérate User's Manual : ADSL MODEM ANI1020E

[20] HOME PLUG POWERLINE ALLIANCE
2006 Whitepapers . [En línea] Global Inventures. Camino Ramon, California
[consultado 2006/07/14]
<http://www.homeplug.com/en/products/whitepapers.asp>

[21] THE INTERNATIONAL ENGINEERING CONSORTIUM
2003 Web ProForums. [En línea] Home Networking. Santa Clara, California
[consultado 2006/05/12]
<http:// www.iec.org/online/tutorials/home_net/>

[22] PALET, Jordi y GOMEZ, Chano
2003 Head End Router HW and SW Specification
[en línea] Madrid : 6POWER Consortium. [consultado 2006/09/28]
<http://www.6power.org/open/6power_pu_d4_1_v1_5.pdf>

[23] ESPINOSA DE LOS MONTEROS, Julián ; LOPEZ, Oscar y GARCIA, Santiago
2002 Técnico en telecomunicaciones. Nuevas Tecnologías.
Madrid: Cultural. 3 v.

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

[24] PLC FORUM
2006 Web ProForums. [En línea] Noticias y Regulaciones. Francia [consultado 2006/07/12] <http://www.plcforum.org/frame_news.html >

[25] NETJER NETWORKS
2005 Soluciones de Conmutación de Datos en Capa 2 y Capa 3 [En línea] Colonia del Valle, Ciudad de México: Soluciones Hardware [consultado 2006/11/15] <http://www.netjernetworks.com/hardware/switcheo23.html>

[26] UNIVERSAL POWERLINE ASSOCIATION
2006 Opera Information. [En línea] Technology White paper. UK [consultado 2006/09/22] <http://www.upaplc.org/_files/opera_wp2.pdf>

[27] DS2 : World Leader in Broadband Powerline Communication
2006 PLC Products. [En línea] Tecnologías Avanzadas. Valencia (España) [consultado 2006/07/12] <http://www.ds2.es/products/chipset.aspx>

[28] PORRAS MAYANS, Ignacio
2004 PLC (Power Line Communications). Internet sobre Red Eléctrica [en línea] Madrid : Universidad Politécnica de Madrid. [consultado 2006/05/22] <http://casafutura.diatel.upm.es/rrssmd/trabajos/2004/powerpoint/18.-%20PowerLineCommunic%20(I.Mayans).pdf>

[29] GONZÀLEZ PUYOL, Juan y GARCIA VIEIRA, Francisco
2004 La tecnología PLC en los programas de fomento a la sociedad de la información de Red.es. [en línea] Madrid : Boletín de RedIRIS. [consultado 2006/05/22] < http://www.rediris.es/rediris/boletin/68-69/enfoque4.pdf>

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

[30] PALET, Jordi
2003 Cómo IP puede llegar ... a todo el planeta: 6POWER
[en línea] Madrid : Boletín de RedIRIS. [consultado 2006/07/28]
<http://www.rediris.es/rediris/boletin/62-63/ponencia15.pdf>

[31] COBOS, Sergio
2005 Introducción a la tecnologia PLC (Power Line Communications).
Revista Española de Electrónica, 1 (611) : 72-75. Madrid

[32] HRASNICA, Halid ; HAIDINE, Abdelfatteh y LEHNERT, Ralf
2004 Broadband Powerline Communications Networks. Network Design
Germany : John Wiley & Sons, Ltd.

[33] PEREZ, Ricardo
2003 Ingeniería y Telecomunicaciones S.A.. Tecnología PLC. [en línea]
Extremadura (España) : III Jornada de Telecomunicaciones Avanzadas y Tecnologías IP. [consultado 2006/07/02]
<http://www.informandote.com/jtatip03/articulos/ponencia5.pdf>

[34] CHAUCA SAAVEDRA, Mario
2006 Power Line Communications. Desarrollo de proyectos
Jornada de Conferencias – CONEIMERA – Huancayo Perú
Universidad Ricardo Palma [correo electrónico]. Noviembre 15.

[35] HüBSCHER, Beat
2002 Powerline Communications. High Speed Internet on the Power Grid.
[en línea] Mägenwil (Switzerland): Ascom Power Line Communications
[consultado 2006/07/02]
<http://www.currenttechnologies.ch/documents/2002-02-02.pdf>

[36] MUGICA, Daniel
2006 Ethernet Extremo a Extremo a través de PLC y SDH. *Robotiker-Tecnalia*
[en línea] , [consultado 2006/10/08]
<http://revista.robotiker.com/revista/articulo.do;jsessionid

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

=DAA2A135EFC4F16DF5067CBCDB45D28C?method=detalle&id=92>

[37] CACERES, Jack
2005 Ùltimos Avances en Telecomunicaciones y Telefonía sobre IP [en línea] Lima: Red Científica Peruana [consultado 2006/10/28] <http://www.rcp.net.pe/downloads/ultimos_avances_en_telecomunicaciones_y_telefonia_sobre_IP_(UNIFE).ppt>

[38] SIEMON
2006 CCTV y Vigilancia por Video sobre 10G IP™. [En línea] Technology White paper. UK [consultado 2006/10/16] <http://www.siemon.com/es/white_papers/SD-03-08-CCTV.asp>

[39] AXIS COMMUNICATIONS
2006 Herramienta de Diseño de Axis. [En línea] Software Interactivo. Sweden [consultado 2006/10/18] <http://www.axis.com/products/video/design_tool/index.es.htm>

[40] AXIS COMMUNICATIONS
2002 Las redes IP: Conceptos básicos. [En línea] White Paper. Sweden [consultado 2006/10/18] <http://www.axis.com/documentation/whitepaper/ip_networks_basics.pdf

[41] AXIS COMMUNICATIONS
2003 Vídeo en red : Nuevas instalaciones. [En línea] White Paper. Sweden [consultado 2006/10/18] <http://www.axis.com/documentation/whitepaper/video/a_new_installation.pdf>

[42] TOPFER, Paul
2003 Technology Review of Powerline Communications (PLC). Technologies And their Use in Australia. [En línea] Australia : Parsons Brinckerhoff Associates. [consultado 2006/12/02]

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TESIS PUCP

<http://www.dcita.gov.au/__data/assets/pdf_file/21754/Technology_Review_of_Powerline_Communication_Technologies_and_their_use_in_Australia.pdf>

[43] POLICIA NACIONAL DEL PERU
2003 Plan Nacional del Sistema de Seguridad Ciudadana. [En línea] Lima: Oficina de Comunicación Social - Ministerio del Interior [consultado 2006/08/11] <http://www.seguridadidl.org.pe/sistema.htm>

[44] POLICÍA NACIONAL DEL PERÚ
2006 Seguridad Ciudadana. [En línea] Lima: Área de Comunicaciones- PNP [consultado 2006/08/11] <http://www.pnp.gob.pe/comunidad/seguridad_ciudadana.asp>

[45] DIARIO EL COMERCIO PERU
2005 Cámaras de Vigilancia evitarán Robos en Calles de Miraflores y San Isidro. [En línea] Lima: Oficina de Redacción [consultado 2006/08/11] <http://www.elcomercioperu.com.pe/EdicionImpresa/Html/2005-12-08/impLima0417044.html>

[46] MUNICIPALIDAD DE SURQUILLO
2006 Mapa Político del Distrito de Surquillo. [En línea] Lima: Oficina de Recursos Informáticos [consultado 2006/08/11] <http://www.munisurquillo.gob.pe/>

SOME RIGHTS RESERVED
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3Com® SuperStack® 3 Switch 3200 Family

DATA SHEET

- Wirespeed, Layer 2/3 switches with 10/100 desktop connections and Gigabit downlinks
- Dynamic Layer 3 routing simplifies implementation
- IEEE 802.1X network login and RADIUS authentication

Key Benefits

Performance

Wirespeed, non-blocking Layer 2/3 switching for 10/100 desktop connections with built-in Gigabit downlinks. Packet prioritization gives optimal performance to real-time applications such as voice and video. Link aggregation of the downlinks enables high-performance connectivity to the core of the network, with resiliency to improve availability and uptime. Layer 3 switching at the edge enables fast switching of traffic between local subnets while offloading routers in the core of the network.

Flexibility

Available in managed 50- or 26-port configurations, with 48 or 24 auto-sensing 10/100 ports and two dual-personality ports for 10/100/1000 or SFP connectivity.

Ease of Use

Supports dynamic routing through RIP, with automatic updating of the Layer 3 network without any manual intervention. Much easier than implementing static routes.

Automatically auto-negotiates speed and duplex mode of cables connected to it preventing misconfiguration of the network. Switches detect and adjust to cross-over or straight-through cable connections– a feature called auto MDI/MDIX– eliminating the need for specific crossover cables.

Scalability

Supports up to 2,000 external routes, allowing the switch to scale as the network grows–ideal for deployments at the edge of a network. Supports up to 255 VLANs and standards-based IEEE 802.3ad trunking (LACP).

Rate limiting enables the bandwidth on each port to be restricted, preserving network bandwidth and allowing maximum control of network resources.

Security

Supports IEEE 802.1X network login to secure user entry into the network, with access control directed from a central standards-based RADIUS server for ease of management. Intrusion prevention features protect the network and will discard all packets from unauthenticated users.

Port-based Access Control Lists further enhance security. Communication of attached stations can be restricted to certain destinations, in essence segmenting the network into more secure areas.

Management of the switch can be implemented using Secure Shell (SSH) and Secure Sockets Layer (SSL/HTTPS) encryption (56 or 168 bit) preventing unauthorized remote access to the switch over IP networks or from a web browser.

Network Control

Network management through embedded web interface, command line interface, or an SNMP management station. Network management is further simplified with the use of 3Com Network Supervisor for configuration and troubleshooting of multiple devices on the network.

Limited Lifetime Hardware Warranty

Limited Lifetime Hardware Replacement. See www.3com.com/warranty for details.

Service

3Com products are backed by 3Com Global Services and authorized partners with demonstrated expertise in network assessment, implementation, and maintenance. Ask about 3Com's Network Health Check, installation services, and maintenance service packages available in your area.

3Com® SuperStack® 3 Switch 3200 family switches are wirespeed, Layer 3 switches with 10/100 desktop connections and Gigabit downlinks for high performance connectivity to the rest of the network. These switches support dynamic Layer 3 routing, simplifying the implementation of Layer 3 networks by automatically configuring and updating the switch with all topology changes. This ability to dynamically reconfigure the routing provides a significant benefit over the use of static routes, avoiding the drawback of many Layer 3 switches which require manual intervention when changing the topology of the network.

The SuperStack 3 Switch 3200 is optimized for edge desktop connections. Layer 3 switching for the network's edge, with the Switch 3200's hardware-based wirespeed routing, improves performance by routing locally without data having to travel back to the network core. This is especially useful in organizations having or anticipating multiple subnets in their workgroups, where even local traffic may otherwise need to be routed via a core switch.

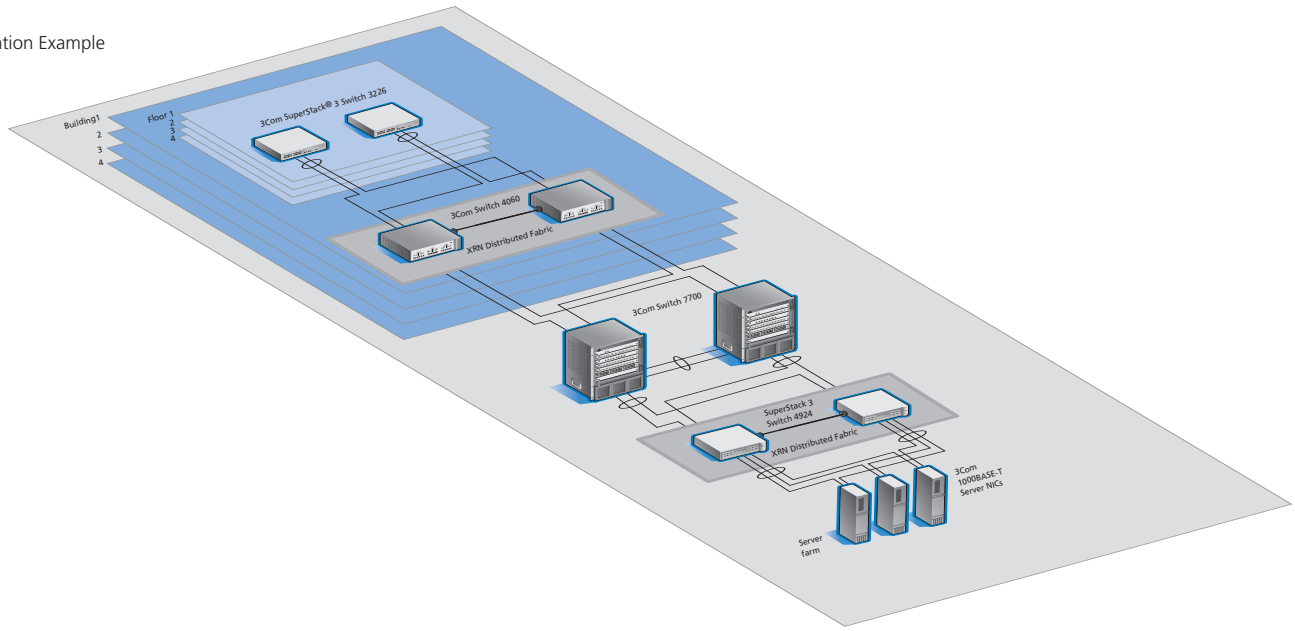
Also, for edge-optimized deployment, the SuperStack 3 Switch 3200 supports the learning of up to 2,000 IP routes through an uplink to a core router using Router Internet Protocol (RIP). This high number of routes enables the switch to operate in larger networks than can other switches which have significantly smaller numbers of routes.

The SuperStack 3 Switch 3200 also supports core-level switching in smaller networks, with local routing for 32 IP interfaces and up to 14 routes distributed from other local Layer 3 devices.

The SuperStack 3 Switch 3200 family confirms 3Com's commitment to strong network security. Its implementation of IEEE 802.1X network login security helps ensure all users are authorized before being granted access to any network resource. User authentication is carried out using any standards-based RADIUS server, avoiding any proprietary authentication mechanisms.

Containment of users to specific areas of the network can be easily controlled through Access Control Lists (ACLs), restricting the IP addresses with which a port can communicate.

Configuration Example



Features

PERFORMANCE	
Switching capacity	SuperStack 3 Switch 3226, 8.8 Gbps; Switch 3250, 13.6 Gbps
Forwarding rate	Switch 3226, 6.6 Mpps; Switch 3250, 10.1 Mpps Store-and-forward switching; latency <12 µs
LAYER 2 SWITCHING	
MAC Address	8K MAC addresses
VLAN	255 VLANs (IEEE 802.1Q)
Link Aggregation	IEEE 802.1ad (LACP), Gigabit ports only
Auto-negotiation	Auto-negotiation of port speed, duplex, and connection (MDI/MDIX)
Traffic control	IEEE 802.3x full-duplex flow control Back pressure flow control for half-duplex Supports Broadcast Storm Suppression (3,000 pps threshold)
Spanning Tree Protocol / Rapid Spanning Tree Protocol	IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) Backward-compatible with Spanning Tree Protocol (STP) Fast-start mode Spanning tree enable/disable per port
LAYER 3 SWITCHING	
Routes	Hardware based routing 2,001 IP routes: 1,990 dynamic and 10 static Address Resolution Protocol (ARP) entries with 1 user default route
IP Routing	32 IP interfaces Multi-netting (multiple IP interfaces per VLAN) Routing Information Protocol (RIP), v1 and v2 • Split Horizon • Split Horizon with poisoned reverse • Triggered updates • MD5 authentication of the RIP packets • Password authenticated RIP packets • Host route advertisements
Multicast	Filtering for 64 multicast groups Internet Group Management Protocol (IGMP) snooping on Layer 2 interfaces IGMP v1 and v2 IGMP Querier
Network protocol	Dynamic Host Configuration Protocol (DHCP) Helper/Relay UDP Helper ARP, ARP Proxy
CONVERGENCE	
Priority Queues	Four hardware queues per port Weighted Round Robin queuing
Traffic Prioritization	Priority based on: • DiffServ Code Point (DSCP) • IEEE 802.1p Class of Service (CoS) VLAN priority • TCP/UDP destination port number • Default port priority • Auto classification of 3Com NBX® telephony traffic
Bandwidth Management	Port-based bandwidth management: • 1 Mbps increments (10/100 ports) • 8 Mbps increments (Gigabit ports)

Features *continued*

SECURITY	
Network Login	IEEE 802.1X user authentication • RADIUS authentication • Secure Mode (locks MAC address)
Access Control Lists	Port-based ACLs • Filtered on destination IP address / mask • One ACL per port • 32 unique ACLs per switch • 32 rules per ACL (10/100 ports)
Switch Protocol Security	MD5 cipher-text and clear-text authentication for RIP v2 packets
Switch Management	Local or RADIUS management of switch passwords Trusted IP Management Addresses Telnet • SSH v1 (56bit DES) • SSH v2 (requires free software upgrade) SSL (HTTPS) • 40 Bit • 56 Bit DES • 128 Bit RC4 (requires free software upgrade)
RESILIENCY	
	Support for 3Com Advanced Redundant Power Supply; provides backup power to the switch Dual software images Backup and restore of switch settings
MANAGEMENT	
Remote Management	SNMP v1
Software	Dual software images Backup and restore Trivial File Transfer Protocol (TFTP) configuration: upload/download TFTP agent: upload
Configuration	Command line Serial (9-pin, D-type connector) Telnet Web-based SNMP
Mirror port / RAP (Roving Analysis Port)	One-to-one
RMON (Remote Monitoring)	Four groups: statistics, history, alarm, and events
IP address allocation	DHCP Manual User-selectable management VLAN
Switch access levels	2 access levels 16 user accounts
Remote GUI management	3Com Network Supervisor for basic, turn-key network management for small and medium businesses (copy provided with product) • Topology discovery • Change management reporting • Capacity planning • Event logging • Fault identification and troubleshooting • Utilization monitoring Other 3Com Management Applications: • 3Com Network Director for comprehensive, turn-key network management for the enterprise. • 3Com Enterprise Management Suite for flexible, extensible management in advanced enterprise IT environments

Specifications

All information in this section is relevant to the 3Com SuperStack 3 Switch 3226 and Switch 3250, unless stated otherwise.

Port Capacities

SuperStack 3 Switch 3226:
24 10/100 ports
2 dual-personality 10/100/1000 or SFP Gigabit ports

SuperStack 3 Switch 3250:
48 10/100 ports
2 dual-personality 10/100/1000 or SFP Gigabit ports

Dimensions

Height: 45 mm (1.7 in or 1U)
Width: 440 mm (17.3 in)
Depth:
Switch 3226: 252 mm (9.9 in)
Switch 3250: 333 mm (13.1 in)
Weight:
Switch 3226: 4.3 kg (9.5 lbs)
Switch 3250: 5.3 kg (11.7 lbs)

Performance

SuperStack 3 Switch 3226:
Bandwidth: 8.8 Gbps
Throughput: 6.6 Mpps

SuperStack 3 Switch 3250:
Bandwidth: 13.6 Gbps
Throughput: 10.1 Mpps

Power Supply

Input voltage: 100-240 VAC autoranging
Operating frequency: 47-63 Hz
Maximum current: 2A
Maximum power:
Switch 3226: 55 W
Switch 3250: 84 W
Heat dissipation:
Switch 3226: 184 BTU
Switch 3250: 287 BTU

CPU

MPC8245 (333Mhz)
16MB Flash memory
32MB Processor memory

Packet Buffer Memory

Switch 3226: 32MB
Switch 3250: 64MB

Environmental Requirements

Operating temperature:
0° to 40°C (32° to 104°F)
Storage temperature:
-40° to 70°C (-40° to 158°F)
Humidity:
10% to 90% non-condensing

MTBF

SuperStack 3 Switch 3226:
51 years (447,000 hours)

SuperStack 3 Switch 3250:
38 years (333,000 hours)

Industry Standards Supported

Ethernet Protocols
IEEE 802.1p (CoS)
IEEE 802.1Q (VLANs)
IEEE 802.1w (RSTP)
IEEE 802.1X (Security)
IEEE 802.3ab (Copper Gigabit)
IEEE 802.3ad (Link Aggregation)
IEEE 802.3i (10BASE-T)
IEEE 802.3u (Fast Ethernet)
IEEE 802.3x (Flow Control)
IEEE 802.3z (Fiber Gigabit)

Administration Protocols
RFC 1812 (IPv4)
RFC 1518, 1519 (CIDR)
RFC 826 (ARP)
RFC 783 (TFTP)
RFC 768 (UDP)
RFC 791 (IP)
RFC 793 (TCP)
RFC 2474 (DiffServ)
RFC 2131 (DHCP)
RFC 1058 (RIP v1)
RFC1723 (RIP v2)
RFC 2138 (Radius Authentication)

Management, including MIBs Supported
RFC 1157 (SNMP v1/v2c)
RFC 1213 (MIB II)
RFC 1398 Ethernet MIB
RFC 1493 (Bridge MIB)
RFC 1573 (Private IF MIB)
RFC 1724 (RIP V2 MIB Extension)
RFC 1757 RMON MIB
RFC 2011 IP-MIB
RFC 2012 TCP-MIB
RFC 2013 UDP-MIB
RFC 2037 Entity MIB
RFC 2618 (RADIUS Authentication Client MIB)
RFC 2665 Ethernet-MIB
RFC 2674P P-BRIDGE-MIB
RFC 2674Q Q-BRIDGE-MIB
RFC 2737 Entity MIB
RFC 2819 RMON MIB
RFC 2863 IF-MIB
IEEE8021-PAE-MIB (IEEE) (Network Login)
Router MIB

Emissions / Agency Approvals

CISPR 22: 1995; Class A
FCC Part 15 subpart B, Class A
EN 55022: 1998; Class A
ICES -003 Class A
AS/NZS 3548 Class A
EN 61000-3-2: 2000
EN 61000-3-3: 1995 +A1

Immunity

EN 55024: 1998

Safety Agency Certifications

UL 60950-1
IEC 60950: 2001; all national deviations
EN 60950: 2001; all national deviations
CSA 22.2 # 60950-00

Management

Web interface
Command line interface
SNMP compatibility
Management through 3Com management applications
- 3Com Network Supervisor
- 3Com Network Director
- 3Com Enterprise Management Suite

Warranty

Limited Lifetime Hardware Warranty. Limited Software Warranty for ninety (90) days. See www.3com.com/warranty for details.

Other Benefits

Other Service Benefits: Advance hardware replacement with same day shipment for North America and Western Europe. Next day shipment for rest of world. Calls must be received by published cut-off times.
90 days of telephone technical support. Limited software updates.
See www.3com.com/warranty for more detail.
Register products at http://eSupport.3com.com/.

Service

Americas:
http://www.3com.com/products/en_US/global_services/
International:
http://emea.3com.com/globalservices

Ordering Information

PRODUCT DESCRIPTION	3COM SKU
3Com SuperStack 3 Switch 3226 24-port 10/100 Layer 3 switch with two dual-personality 10/100/1000 or SFP ports	3CR17500-91
3Com SuperStack 3 Switch 3250 48-port 10/100 Layer 3 switch with two dual-personality 10/100/1000 or SFP ports	3CR17501-91
SFPs (LC connectors)	
3Com 1000BASE-SX SFP	3CSFP91
3Com 1000BASE-LX SFP	3CSFP92
3Com 1000BASE-LH70 (70km) SFP	3CSFP97
Redundant Power	
3Com SuperStack 3 Advanced Redundant Power System	3C16071B
3Com SuperStack 3 Advanced Redundant Power System, 325W Power Module Type 3	3C16075

3Com Corporation, Corporate Headquarters, 350 Campus Drive, Marlborough, MA 01752-3064

To learn more about 3Com solutions, visit www.3com.com. 3Com is publicly traded on NASDAQ under the symbol COMS.

Copyright © 2005 3Com Corporation. All rights reserved. 3Com, the 3Com logo, NBX, and SuperStack are registered trademarks of 3Com Corporation. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, 3Com does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.

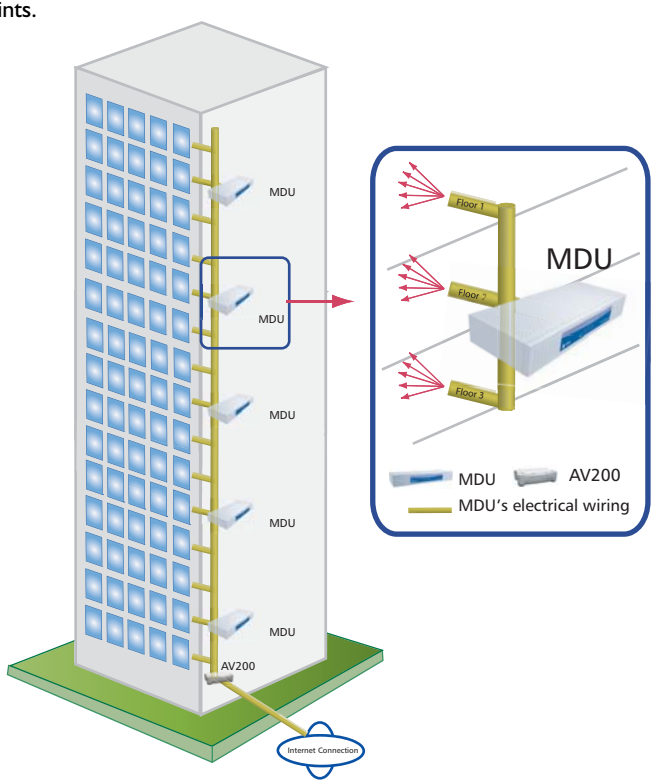
400842-006 08/05

Corinex
AV200 MDU Gateway

The only 200 Mbps Powerline and Coax Solution for MDU's

Introducing the most powerful solution for delivering broadband access to every room in a Multi Dwelling Unit (MDU), the Corinex AV200 MDU Gateway. The 200 Mbps MDU Gateway allows distribution of broadband signals over existing electrical wiring or coax cabling within hotels, apartment buildings, hospitals, schools, and all other MDUs, every electrical or coax outlet in the MDU becomes a high-bandwidth connection. Corinex's AV200 powerline technology, based on the pre-UPA standard achieves data rates of up to 200 Mbps and propagates signals throughout an entire MDU, all without the need for pulling new wiring. Deployment of the Gateway is simple and fast, allowing Installers, System Integrators, and End Customers to deploy Internet Access, VoIP, and even Streaming Video in every room in an MDU in a few short days.

Built on the Corinex AV200 technology, the MDU Gateway can communicate with other Corinex AV200 devices such as the successful Corinex AV200 Powerline Ethernet Adapter, Corinex AV200 Powerline Router, and the Corinex AV200 CableLAN adapter. Deploying an AV200 powerline network in an MDU is simple – simply connect a single head-end AV200 modem to inject an MDU's Internet signal onto the powerlines or coax cables, connect one MDU Gateway every few floors, connect an AV200 modem in each room requiring broadband access – and you are done! The MDU Gateway is able to process signals so that even the most distant electrical or coax outlets will be able to serve as broadband connection access points.



Features

- Repeating: Extends the range of a network
- Segmentation: Allows an unlimited number of users
- Modularity: Optimizes performance while minimizing costs
- Management: Configures and Controls devices on the network

Technical description

Repeating

The MDU Gateway supports two different types of repeating depending on the customers needs, time division and frequency division. Time division repeating divides time into timeslots – in each timeslot the repeater either receives the data, or repeats them further to the network. Time Division repeating cannot send and receive data at the same time, however, if latency is a critical parameter (such as for video streaming), frequency division repeating can be used. Frequency division repeating allows one module within the gateway to receive data while a second module repeats the data. Each module operates in a different non-overlapping frequency band. Frequency Division repeating allows repeating of data with non-measurable latency.

Segmentation

A standard AV200 powerline or coax network is limited to 32 AV200 Powerline or CableLAN modems, in order to maintain peak performance. This maximum user limitation can be a problem in larger buildings, such as hotels, where up to 100 users or more may need to have internet access at the same time. The Corinex MDU Gateway's proprietary patent pending algorithms remove the maximum user limitation and allow an installer to use a virtually unlimited number of nodes in the powerline or coax network. Each MDU Gateway can act as a master modem for a powerline or coax network segment with 32 AV200 Powerline Ethernet or CableLAN Adapter nodes.

Modularity

Modularity is a critical advantage for installers using Corinex's unique AV200 MDU technology. A maximum of three AV200 powerline modules can be included in the gateway, allowing installers to optimize the cost and performance of AV200 powerline or coax networks in an MDU.

For simple gateways using time-division multiplexing for simply repeating the signal, only one powerline module is required. A more advanced device with two powerline modules can serve as a time-division repeater and a network segment master device simultaneously. Segments may be cascaded in order to allow as many users (or rooms) required for the installation. All three variants of the Corinex AV200 MDU Gateway can be combined in a network in order to minimize latency in the network. At the same time the three module gateway acts as a master device for a network segment. All three variants of the Corinex AV200 MDU Gateway can be combined in a network in order to create the highest performance, lowest cost powerline or coax network available for MDU's.

Management

The Corinex AV200 MDU Gateway and all other AV200 powerline or CableLAN products from Corinex can be easily configured using the Corinex AV200 Network Management software using SNMP. From monitoring and configuration to remotely accessing and controlling devices, Corinex's powerful GUI based management software gives network managers control of the network from any web enabled PC.

Technical Specifications

Hardware

Standards compliance	pre-UPA standard IEEE 802.3, IEEE 802.3u FCC and UL (US), CE (Europe)
Data rate	Powerline: up to 200 Mbps on physical layer Ethernet: 10/100 Mbps
Cabling Type	1 Ethernet cable AC power cord
LED Status Lights	POWER PLC1,Ethernet1, PlC2, Ethernet2, PLC3, Ethernet3 Switch1, Switch2, Swith 3
Interfaces	1-3 x Powerline port 1x Ethernet/ Debug / Configuration AC power connector for both Powerline networking and power supply
Electrical Parameters	Input Voltage: AC 100V~240V Line Frequency: 60/50Hz (USA/Europe)

Software

Supported OS (Setup Tool)	Windows 98, ME, 2000, XP Linux Mac OS X
Management	AV200 Network management software

Product Specifications

Product Code: CXP-MDU-GWY

Please refer to the Price List for the exact product code specification for your region.

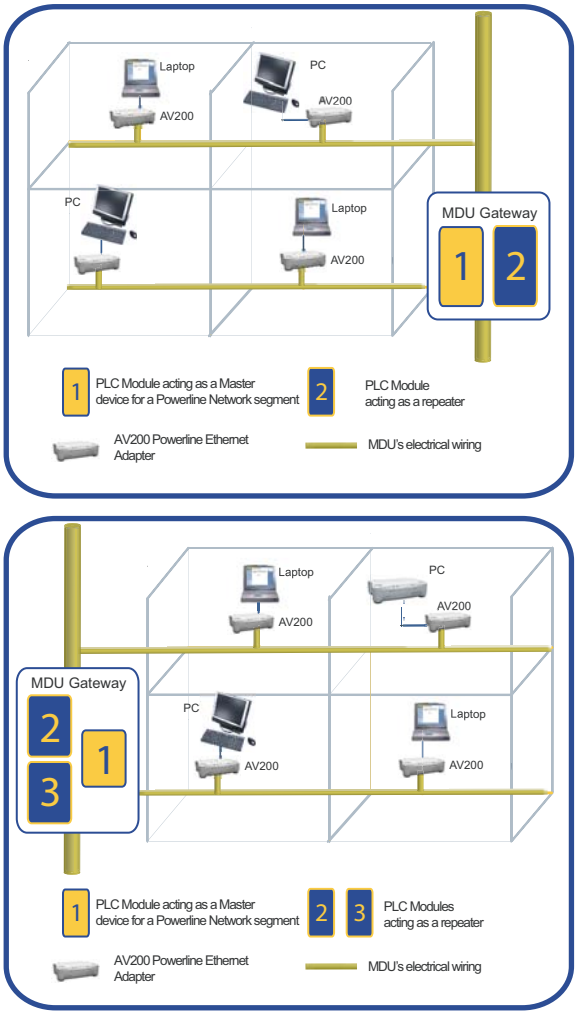
Related products

The Corinex family of 200 Mbps AV products consists of:

- Corinex AV200 Powerline Ethernet Adapter
- Corinex AV200 CableLAN Adapter
- Corinex AV200 Powerline Router

Product Package Contents

- Corinex AV200 MDU Gateway
- CD with documentation
- Quick Start Guide



UPA UNIVERSAL POWERLINE ASSOCIATION

Products features and design may vary by version and region.

Corinex AnyWire Connectivity™

Corinex is a registered trademark of Corinex Communications Corp.

Corinex Communications Corp.
#670 - 789 West Pender Street
Vancouver, BC
Canada V6C 1H2
Tel: +1 - 604 - 692 0520
Fax: +1 - 604 - 694 0061
E-mail: global@corinex.com
http://www.corinex.com

Corinex Global, a.s.
Ruzova dolina 19
821 08 Bratislava
Slovak Republic
Tel.: +421 - 2 - 5021 4811
Fax: +421 - 2 - 5556 7309
E-mail: global@corinex.com

2005-08-12 ver.1.1

The content of this document is furnished for informational use only, it is subject to change without notice, and it does not represent a commitment on the part of Corinex Communications Corp.

Corinex

AV200 Powerline Ethernet Wall Mount

200 Mbps PLC

200 Mbps over existing electrical wires!

Introduction

The Corinex AV200 Powerline Ethernet Wall Mount is the world's first wall mount outlet adapter to support the distribution of video, voice, and broadband internet access over a premises existing electrical wires. With transfer rates of up to 200 Mbps, the Corinex AV200 Powerline Ethernet Wall Mount has ample bandwidth to stream several high quality video signals, such as HDTV, while simultaneously delivering high speed internet access throughout an entire premise! The AV200 Powerline Product family consists of an Adapter, Router, ADSL2+ Wireless Gateway and a CableLAN adapter and CableLAN router for coaxial networking applications, all offering 200Mbps communications.

The AV200 Powerline technology by Corinex provides numerous networking possibilities with amazingly fast physical layer transfer rates up to 200 Mbps. Finally, real world multimedia network applications can be created without adding any new wiring, simply plug in a Corinex AV200 Powerline Ethernet Wall Mount and any computing device in the entire premise is ready to receive high bandwidth multimedia signals.

Application priority levels are retained, ensuring that applications with real-time requirements, such as VoIP, streaming video and multiplayer head-to-head games do not experience glitches, frame loss, or delays, even if other users in the network are downloading large files, websurfing or downloading or listening to MP3 songs.

The Corinex AV200 Powerline Ethernet Wall Mount allows users to create a high-speed local area network, without the need for new cabling. Users can connect the AV200 Powerline Ethernet Wall Mount to virtually any electrical socket in their home or office to create a link to the powerline network. The network can be connected to an internet gateway, such as an ADSL or cable modem, providing a convenient extension of the internet to the powerline within a premise.

Any ethernet-enabled device, such as a desktop computer, network printer, laptop computer, or a security camera connect to the AV200 powerline network.

There are two versions of the Corinex AV200 Powerline Ethernet Wall Mount. The Home Users Edition of the product is meant for home networking applications and simple plug and play installations. The Commercial Edition of the product is used for advanced networking applications, deployments in Multi dwelling Units and operators providing BPL Access.

Features

- 10/100BaseT Fast Ethernet interface
- Physical data rate in the powerline up to 200 Mbps with distances up to 300 m.
- Built-in repeating capabilities for increased coverage
- CSMA/CARP (Carrier Sense Multiple Access with Collision Avoidance and Resolution using Priorities) protocol
- Bridge Forwarding Table for 64 MAC Addresses
- 802.1Q VLAN & Optimized VLANs
- Powerful DES/3DES encryption
- OFDM technology and powerful error correction system allow robust performance under harsh conditions in the electrical network
- Integrated 802.1D Ethernet Bridge With Optimized Spanning Tree Protocol
- 8-level priority queues, with programmable priority-classification engine
- Priority classification according to 802.1P tags, IP coding (IPv4 or IPv6) or TCP source/destination ports
- Optimized support for broadcast and multicast traffic
- MAC filtering - can discard Ethernet frames if they come from a source MAC address which is not present in a list of allowed MAC addresses
- Configuration using an embedded web interface

Commercial Edition:

- Console Interface
- Dynamic IP Address with auto-config
- Manual MASTER / SLAVE configuration
- VLAN and OVLAN Support
- RADIUS server authentication support
- Programmable bandwidth allocation
- Master Node HE or Repeater
- Slave CPE Node
- Can be used for MV/LV BPL networks

Home User Edition:

- Web interface
- Fixed IP or DHCP
- Default IP 10.10.1.69
- The MASTER and SLAVE can be set manually or automatically
- VLAN tagging without filtering

Technical Specifications

Standards Compliance	IEEE 802.3u 802.1 P 802.1 Q
Speed	Up to 200 Mbps on physical layer
AC Plug Type	US, EU, UK and AUS
LED Status Lights	Power on, PLC Link/Activity Ethernet link
Interface	10/100BaseT Fast Ethernet, Powerline
Frequency Range used	2 – 34 MHz
Power Input	85 to 265 V AC, 50/60 Hz
Dimensions	107 mm L x 72 mm W x 79 mm H
Transmitted Power spectral density	-58 dBm/Hz
Power Consumption	4 W
Safety & EMI	FCC Part 15, EN 55022 EMC limits
Operating Temperature	0° to 40°C (32°F to 104°F)
Operating Humidity	10% to 80% non-condensing

Product features and design may vary by version and region.

Standards

- 802.3u
- 802.1P
- 802.1Q
- Compliant with FCC Part 15, EN 55022 EMC limits

Package Contents

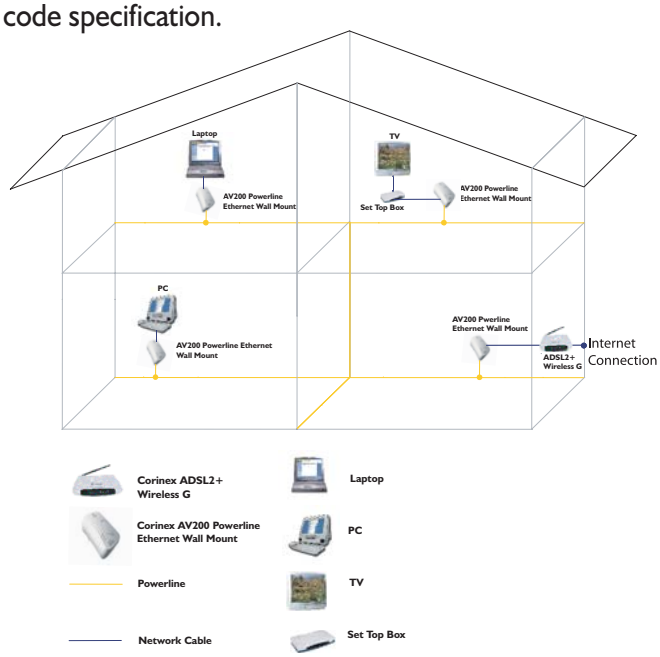
- Corinex AV200 Powerline Ethernet Wall Mount
- One standard CAT5 ethernet cable
- CD with documentation
- Printed Quick Start Guide

Product Specification

Product code: CXP-AV200-WME

CXP-AV200-WME - Home Edition
CXP-AV200-WMEC - Commercial Edition

Please refer to the Price List for the exact product code specification.



Corinex is a registered trademark of Corinex Communications Corp.
HomePlug® is a registered trademark of HomePlug® Powerline Alliance.
All products or company names mentioned herein may be the trademarks of their respective owners.
The content of this document is furnished for informational use only, it is subject to change without notice, and it does not represent a commitment on the part of Corinex Communications Corp.

Corinex Communications Corp.
#670 - 789 West Pender Street
Vancouver, BC
Canada V6C 1H2
Tel: 604 - 692 0520
Fax: 604 - 694 0061
E-mail: global@corinex.com
http://www.corinex.com

Corinex Global, a.s.
Ruzova dolina 19
821 08 Bratislava
Slovak Republic
Tel.: +421 - 2 - 5021 4811
Fax: +421 - 2 - 5556 7309
E-mail: global@corinex.com

2006-02-01 ver.2.0

AXIS 225FD
Fixed Dome Network Camera

Professional video surveillance in tough conditions

The AXIS 225FD Fixed Dome Network Camera is a high-performance camera for professional surveillance and remote monitoring. Its discreet, vandal-resistant and outdoor-proof design provides maximum protection in tough environmental conditions. The built-in heater and fan protect against low temperatures and help prevent the glass from misting over. Supported by the industry's largest base of video management software, the AXIS 225FD provides the perfect solution for securing schools, railway stations, car park buildings and other facilities over the local area network or across the Internet.

The compact and cost-efficient design enables easy and flexible installation with tamper-proof mounting on wall or ceiling. It allows for versatile adjustment by panning, tilting and rotating the varifocal lens to any camera angle desired.

The built-in Power over Ethernet (IEEE 802.3af) support enables power to the camera to be delivered via the network, eliminating the need for a power outlet and reducing installation costs. In addition, the consolidation of power gives higher reliability if connected to a central Uninterruptible Power Supply (UPS). The AXIS 225FD also offers a comprehensive set of network security features such as multi-level password protection, IP address filtering and HTTPS encryption.

The AXIS 225FD features an automatically removable infrared cut filter, which enables color video in high and low light conditions as well as IR sensitive black/white video at night. Thanks to the high-quality lens, progressive scan CCD sensor and advanced image processing, this camera delivers crisp, clear images even of objects moving at high speed in the dark.

- Vandal-resistant, outdoor-proof design for maximum protection
- Superior image quality with progressive scan and Day/Night function
- Power over Ethernet for reduced cabling and consolidated power
- Simultaneous Motion JPEG and MPEG-4 for optimized quality and bandwidth
- Up to 30 frames per second in VGA 640x480 resolution
- Multi-window motion detection with alarm image buffering

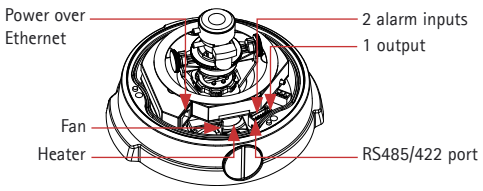
AXIS® COMMUNICATIONS
Make your network smarter

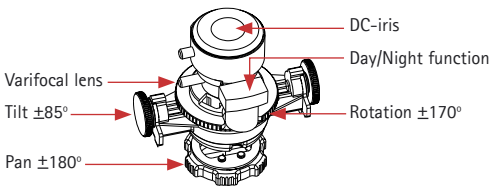
AXIS 225FD Fixed Dome Network Camera

Specifications

Models	AXIS 225FD Also available bundled with outdoor power supply
Image sensor	1/4" Sony Wfine progressive scan RGB CCD
Lens	Pentax QD2V2814BE-DN, F1.4 varifocal 2.8 – 5.8 mm, DC-iris, horizontal viewing angle: 75°-36° focus range: 0.3 m to infinity
Camera angle adjustment	pan ±180°, tilt ±85°, rotation ±170°
Minimum illumination	Color mode: 1 lux at F1.4 Black/white mode: 0.2 lux at F1.4
Video compression	Motion JPEG MPEG-4 Part 2 (ISO/IEC 14496-2), Profiles: ASP and SP
Resolutions	16 resolutions from 640x480 to 160x120 via API, 5 selections via configuration web page
Frame rate	Motion JPEG: Up to 30 frames per sec in all resolutions MPEG-4: Up to 30 frames per sec in 480x360 or lower
Video streaming	Simultaneous Motion JPEG and MPEG-4 Controllable frame rate and bandwidth Constant and variable bit rate (MPEG-4)
Image settings	Compression levels: 11 (Motion JPEG)/23 (MPEG-4) Rotation: 90º, 180º, 270º Configurable color level, brightness, sharpness, contrast, white balance, exposure control, exposure area, backlight compensation, fine tuning of behavior at low light Overlay capabilities: time, date, text, privacy mask or image
Shutter time	2 sec to 1/12500 sec
Security	Multiple user access levels with password protection, IP address filtering, HTTPS encryption
Users	20 simultaneous users Unlimited number of users using multicast (MPEG-4)
Alarm and event management	Events triggered by built-in multi-window motion detection, external inputs or according to a schedule Image upload over FTP, email and HTTP Notification over TCP, email, HTTP and external output Pre- and post alarm buffer of 9 MB (approx 5 min of 320x240 resolution video at 4 frames per sec)
Connectors	Ethernet 10BaseT/100BaseTX, RJ-45 Terminal block for 2 alarm inputs, 1 output, RS-485/422 half duplex port and power connection
Casing	IP66-rated, 1000 kg (2200 lbs) impact-resistant casing Polycarbonate clear dome glass, metal base Tamper-proof mounting
Processors, memory and clock	CPU: ETRAX 100LX 32bit Video processing and compression: ARTPEC-2 RAM: 32 MB, Flash: 8 MB Battery backed-up real-time clock
Power	Camera, heater and fan: 12 V DC, max 20 W 24 V AC, max 25 VA Camera and fan: 9-24 V DC, max 5.5 W 10-24 V AC, max 8 VA Power over Ethernet (IEEE 802.3af) with power classification according to Class 2 Heater only (can be powered separately when camera and fan are powered over Ethernet): 12 V DC, max 15 W 24 V AC, max 17 VA

Operating conditions	Camera, Heater powered: -20 — 50 °C (-4 — 122 °F) Heater not powered: 0 — 50 °C (32 — 122 °F) Indoor power supply: 0 — 50 °C (32 — 122 °F) Humidity 20 — 80% RH (non condensing)
Temperature warning	Warning issued when temperature is below or above limits
Installation, management and maintenance	AXIS Camera Management tool on CD and web-based configuration, configuration of backup and restore Firmware upgrades over HTTP or FTP, firmware available at www.axis.com
Video access from Web browser	Camera live view, sequence tour capability for up to 20 Axis video sources, customizable HTML pages
Minimum Web browsing requirements	Pentium III CPU 500 MHz or higher, or equivalent AMD 128 MB RAM AGP graphic card, Direct Draw, 32 MB RAM Windows XP, 2000, NT4.0*, ME* or 98*, DirectX 9.0 or later Internet Explorer 5.x or later For other operating systems and browsers see www.axis.com/techsup ** Motion JPEG only*
System integration support	Powerful API for software integration available at www.axis.com including HTTP API, AXIS Media Control SDK, event trigger data in video stream, embedded scripting and access to serial port peripherals over TCP Watchdog secures continuous operation, can be monitored by other systems via event notification Embedded operating system: Linux 2.4
Supported protocols	IP, HTTP, HTTPS, SSL/TLS*, TCP, ICMP, SNMPv1/v2c/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, ARP, DNS, DynDNS, SOCKS, NTP etc. More information on protocol usage available at www.axis.com ** This product includes software developed by the Open SSL Project for use in the Open SSL Tool kit (www.openssl.org)*
Video management software (not incl.)	AXIS Camera Station - Surveillance application for viewing, recording and archiving up to 25 cameras AXIS Camera Explorer – Basic software for viewing and manual recording See www.axis.com/partner/adp_partners.htm for more software applications via partners
Included accessories	Installation Guide, CD with User's Manual, demo software, installation and management tools, connector kit, MPEG-4 licenses (1 encoder, 1 decoder), MPEG-4 decoder (Windows), indoor power supply PS-K: 9 V DC, 9 W (for powering camera and fan)
Accessories (not incl.)	Drop ceiling mount bracket, smoked dome glass AXIS PS-24 outdoor power supply Power over Ethernet midspans AXIS 292 Network Video Decoder AXIS MPEG-4 Decoder 10 user license pack
Approvals	EN55022 Class B, EN55024, EN61000-3-2, EN61000-3-3, EN61000-6-1, EN61000-6-2, FCC Part 15 Subpart B Class B, VCCI Class B, C-tick AS/NZS 3548, ICES-003 Class B, EN60950 UL, CSA (indoor power supply)
Dimensions and weight	Height: 115 mm (4 1/2"), diameter: 175 mm (6 1/8") Weight: 1250 g (2 3/4 lbs) excl. power supply





www.axis.com

AXIS® COMMUNICATIONS
Make your network smarter

©2005. Axis Communications AB. The Axis logo is a registered trademark of Axis Communications AB. All other company names and products

AXIS Camera Station

Un completo software de gestión de vídeo para la monitorización, grabación, reproducción y gestión de eventos

AXIS COMMUNICATIONS

Make your network smarter

Obtenga la mejor imagen

Capacidades de gestión de vídeo ilimitadas, dondequiera que se encuentre...

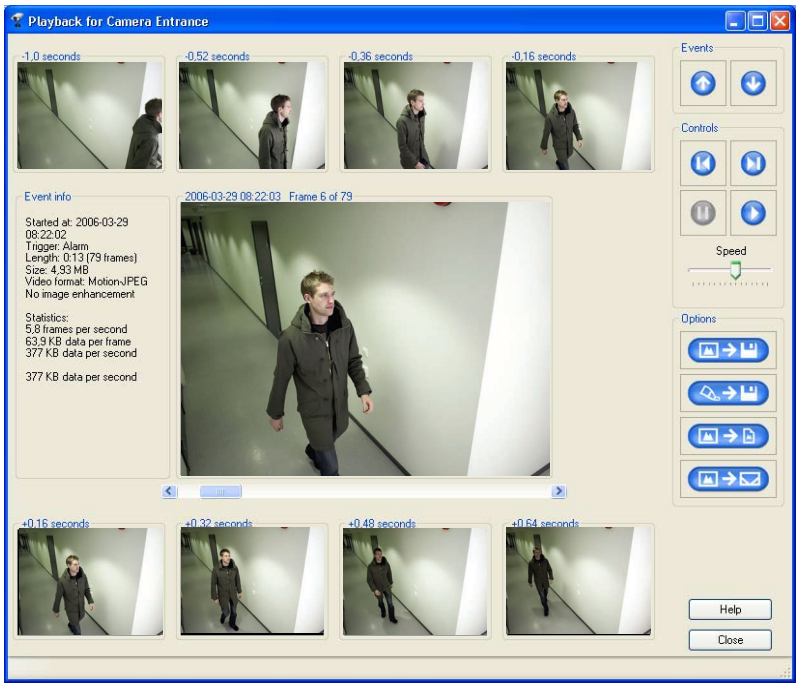
AXIS Camera Station es un completo software de gestión de vídeo especialmente diseñado para las cámaras IP y los servidores de vídeo de Axis. Ofrece monitorización y grabación de vídeo remota, una avanzada gestión de eventos y una excelente calidad de imagen. AXIS Camera Station ofrece las funciones más avanzadas para sus necesidades de vigilancia a través de vídeo.

Grabación de gran calidad

Con AXIS Camera Station instalado en su PC con Windows, puede monitorizar sus cámaras y, al mismo tiempo, grabar vídeo digital de gran calidad, de forma continua o programada, con alarma y/o detección de movimiento. La detección de movimiento del software funciona capturando una imagen varias veces cada segundo y comparando las diferencias en el área indicada de la imagen. AXIS Camera Station admite grabaciones en Motion-JPEG y MPEG-4 para conseguir una calidad de imagen y un uso del ancho de banda óptimos. Las grabaciones digitales se guardan directamente en el disco o discos duros del PC servidor local que ejecuta AXIS Camera Station.

Acceso remoto y reproducción de multivisualización

AXIS Camera Station proporciona formas sencillas de buscar los eventos grabados. Además, gracias a la característica de reproducción de multivisualización, los usuarios pueden ver grabaciones simultáneas procedentes de diferentes cámaras y obtener una imagen global de un evento determinado. También es posible la visualización y reproducción remota mediante un navegador Web o el cliente Windows de AXIS Camera Station.

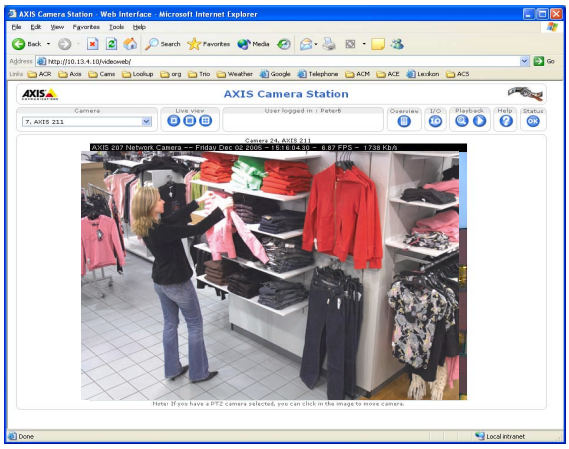


Reproduzca eventos imagen a imagen a velocidad variable. Imprima, envíe por correo electrónico y guarde eventos o expórtelos a los formatos AVI o ASF para usarlos más adelante o para guardarlos. También puede buscar grabaciones con movimiento en un área seleccionada de la imagen.

- Visualice y grabe vídeo en directo desde varias cámaras de forma simultánea
- Varios modos de grabación: continua, programada, por alarma y/o por detección de movimiento
- Grabaciones de gran calidad en MPEG-4 y Motion JPEG
- El componente opcional* AXIS Image Enhancer mejora la claridad de las imágenes en condiciones de mala visibilidad, tales como niebla, humo, lluvia y nieve
- Sin limitación de grabación en software
- Múltiples funciones de búsqueda para eventos grabados
- Registro de auditoría
- Acceso remoto a través de un navegador Web o un cliente de Windows
- Control de cámaras PTZ y domo
- Funciones de alerta de alarma (pitido y correo electrónico)
- Soporte de audio en tiempo real, semidúplex, sin grabación
- Interfaz multilingüe en español, inglés, francés, alemán, italiano y ruso

*Funcionalidad complementaria que se integra en AXIS Camera Station (versión 1.20 y superior) y se activa con una clave de licencia independiente. Puede adquirir claves de licencia en paquetes de 1 y 5 a su distribuidor más cercano. Se requiere una licencia de AXIS Image Enhancer por cada canal de vídeo.

Puede utilizar un navegador Web estándar en las estaciones de trabajo clientes para ver remotamente las cámaras y las grabaciones desde cualquier lugar que disponga de acceso a Internet.



Funciones de mejora de imagen

Gracias a AXIS Image Enhancer, un componente de software complementario para AXIS Camera Station, puede mejorar la calidad de las imágenes grabadas en condiciones como niebla, humo, lluvia y nieve. Una vez aplicado a grabaciones de vídeo en color en directo o grabadas, proporciona resultados en tiempo real y muestra detalles visuales que de lo contrario serían difíciles de ver en malas condiciones de visibilidad.

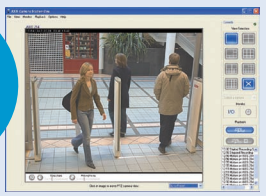
El vídeo se muestra sin elementos de distorsión, lo que hace que este componente sea la solución perfecta para cualquier situación donde la calidad de imagen pueda verse afectada por unas condiciones meteorológicas adversas y se pueda perder información crucial.

La funcionalidad exclusiva AXIS Image Enhancer integrada en el software AXIS Camera Station se activa con una clave de licencia independiente. Trabaja con fuentes de vídeo digitales en color o con fuentes de vídeo analógicas, funciona con todas las cámaras IP de Axis y admite la visualización de frecuencia de imagen completa en directo.

Ejemplo de la mejora de imagen usando AXIS Image Enhancer

- Mejora la calidad de imagen en condiciones de niebla, humo, lluvia y nieve; amplía la visibilidad en puertos, aeropuertos, carreteras y túneles
- Resultados excelentes comparados con los ajustes de brillo/contraste; se consigue una óptima mejora de la imagen al tomar el vídeo entre el amanecer y el anochecer
- Para su uso con vídeo en color en directo o grabado
- Perfecto para cámaras en exteriores

Completamente gratis!



AXIS Camera Station One

Axis Camera Station One es la versión gratis para una cámara del AXIS Camera Station, diseñado para visualizar y grabar una sola cámara.
El software esta disponible en el sitio corporativo AXIS y puede ser actualizado a una versión con licencia del AXIS Camera Station de 4 o 10 cámaras.

¿AXIS Camera Station o DVR?

Comparado con las grabadoras de vídeo digitales (DVR), la combinación de las cámaras IP con AXIS Camera Station presenta una serie de ventajas:

- **Una solución abierta**
  AXIS Camera Station es una solución de software de gestión de vídeo abierta. Se basa en componentes de hardware estándar, no en equipos patentados como los DVR.
- **Escalabilidad**
  Se pueden añadir de forma sencilla cámaras y licencias, y el hardware del sistema se puede ampliar para satisfacer nuevas necesidades de rendimiento. Elija lo que necesita hoy, y amplíe el sistema en cualquier momento en que sus necesidades crezcan.
- **Inteligencia al nivel de la cámara**
  Use la potencia informática de la cámara IP al detectar el movimiento para descargar de trabajo al servidor de grabaciones.
- **Calidad de imagen**
  Gracias a la exploración progresiva y a su resolución en megapíxels, la tecnología de las cámaras IP ha superado a la calidad de las cámaras analógicas usadas por las DVR.
- **Audio bidireccional**
  El audio es transportado a través del propio cable de red, de forma que pueda integrar su sistema de vigilancia IP y hablar y escuchar a través de la red.
- **Infraestructura rentable**
  La mayoría de las instalaciones de hoy día disponen de un cableado de red, así que no necesitará otros cables para implantar una solución de vigilancia IP con AXIS Camera Station y cámaras IP. Al usar un hardware para servidores de PC estándar para grabar y guardar, en lugar de un equipo patentado como los DVR, reducirá enormemente los costes de gestión y equipamiento, en particular en sistemas de gran tamaño, donde el almacenamiento y los servidores son una parte considerable del coste total de la solución. Además, la mayoría de cámaras IP ofrecen la opción Power over Ethernet (PoE), que permite que la alimentación eléctrica de las cámaras se realice a través de la red, lo que elimina completamente la necesidad de cables de alimentación y de tomas de corriente.
- **Componentes integrados estándar**
  Pueden utilizarse servidores de PC standar y arquitectura de almacenamiento de cualquier fabricante, lo que reduce el tiempo de espera y simplifica las actualizaciones y recambios.

Paquetes de vigilancia de Axis: la forma más sencilla de empezar

Los paquetes de vigilancia de Axis consisten en cuatro cámaras IP y el software AXIS Camera Station, con licencias para 4 cámaras IP/canales del servidor de vídeo. Estos paquetes se pueden ampliar fácilmente con más cámaras y licencias de AXIS Camera Station.

PREVENIR, MEJORAR, VERIFICAR, SIMPLIFICAR

La demanda de soluciones completas de vídeo en red para tiendas, fábricas, oficinas, servicios, hoteles, colegios y muchos otros sectores no deja de crecer día a día. AXIS Camera Station, junto con los productos de vídeo de Axis, puede ayudarle de muchas maneras:

- > **Prevenir** hurtos y robos
- > **Mejorando** la seguridad del personal y de las propiedades
- > Añadiendo otras funciones, como la monitorización de los clientes y la mejora de sus instalaciones
- > **Verificando** las alarmas de intrusión y reduciendo al mínimo las falsas alarmas
- > Viendo todo con claridad, en cualquier momento, y dondequiera que se encuentre
- > Proporcionando pruebas eficaces

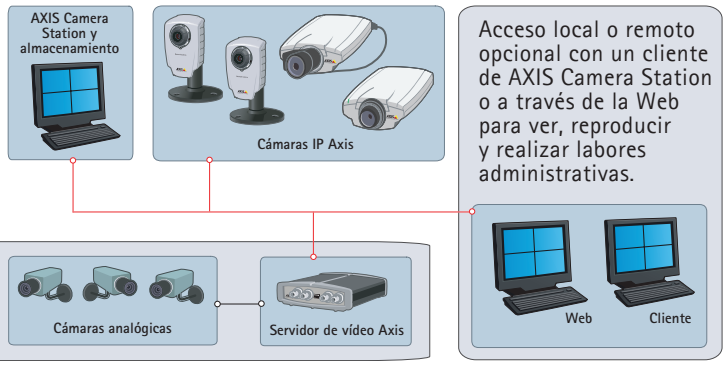
Y **Simplificar...**
Todo el sistema se basa en una infraestructura de red que usted ya posee, una tecnología que ya conoce.

Escenarios de instalación

Soluciones para cualquier situación y necesidad

Escenario 1

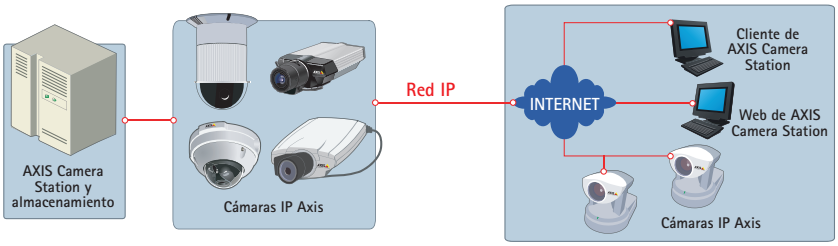
AXIS Camera Station y las cámaras IP de Axis instaladas en la misma red local. Un entorno típico de este tipo de instalación sería una pequeña oficina o una tienda. La visualización, reproducción y administración se realizan directamente en el AXIS Camera Station.



Esto mismo se puede conseguir con su sistema de circuito cerrado de televisión analógico existente, conectando cámaras analógicas a un servidor de vídeo de Axis.

Escenario 2

Los escenarios típicos serían colegios o tiendas con ubicaciones diferentes y un sistema de vigilancia común, al que un supervisor o una empresa de seguridad contratada puede acceder remotamente desde cualquier lugar a través de Internet.



"En cuanto a capacidad, escalabilidad, rentabilidad, sencillez de instalación, calidad de imagen, integración en la red, o por simple tranquilidad, no hay nada mejor que pueda hacer."

Especificaciones de AXIS Camera Station

Compatibilidad	Compatible con la serie de productos de vídeo IP AXIS 2xx con firmware 4.03 o posterior y la serie 2xxx con firmware 2.34 o posterior. Visite www.axis.com para ver la lista completa
Velocidad de grabación	Frecuencia de imagen total > 500 imágenes por segundo con el hardware recomendado
Almacenamiento de las grabaciones	Base de datos de grabación limitada sólo por el espacio en disco La duración por cámara puede estar limitada debido a requisitos legales locales. El valor predeterminado es de 5 días
Canales de vídeo	Hasta 25
Compresión de vídeo	Grabación en Motion JPEG o MPEG-4 Visualización en directo en Motion JPEG o MPEG-2/4
Resoluciones	Hasta 1280x1024 (las resoluciones dependen del producto de vídeo Axis conectado).
Visualización en directo	Puede visualizar en directo a través de hasta 16 cámaras a la vez en vistas divididas por 4, 6, 9, 10, 13, 16 o bien 4, 9 ó 16 en pantalla completa Visualización emergente con una cámara División de vistas definible por el usuario
Modo de secuencia en vivo	Secuencia de varias cámaras (ronda)
Audio	Soporte de audio en tiempo real, semidúplex, sin grabación
Compatibilidad con PTZ	Control de cámaras PTZ y posiciones preestablecidas
Grabación de alarmas	Eventos activados por detección de movimiento, entradas externas o según un programa Grabación acelerada en movimiento o en alarma de I/O
Frecuencia de imágenes de la grabación de alarma	Desde 1 imagen por minuto hasta 60 imágenes por segundo por cámara Búfer configurable de alarma anterior/posterior
Notificación de alarma	Indicación visual, imagen en directo emergente, correo electrónico y registro de eventos
Detección de movimiento	Detección de movimiento avanzada con filtro de exclusión para las áreas de la imagen que no sean de interés. Ajustes diferentes para día y noche Detección de movimiento en la cámara, opción para ahorrar ancho de banda Detección de "ausencia de movimiento"
Grabaciones programadas	Las grabaciones se pueden programar por cámara, para carga continua, por días de la semana o por fechas concretas
Grabación de manipulaciones	Advertencias de imágenes borradas o alteradas en eventos grabados
Almacenado	Las grabaciones se pueden trasladar diariamente a un medio de almacenamiento remoto
Reproducción	Velocidad controlable o imagen a imagen
Reproducción sincronizada	Reproducción de vídeo sincronizada temporalmente de hasta 4 fuentes de vídeo a la vez
Búsqueda de grabaciones	Búsqueda de grabaciones por fecha, hora o movimiento Búsqueda de movimiento en grabaciones continuas
Exportación de clips de vídeo	Exporta imágenes JPEG para guardarlas en un archivo, imprimirlas o enviarlas por correo electrónico Exporta secuencias de vídeo en formato AVI o ASF
Notificación de alarmas del sistema	Notificación en el registro de eventos y por correo electrónico para: alarma, ausencia de señal de la cámara, disco duro lleno y fallo al archivar
Control de entrada/salida	Panel de control avanzado para las entradas/salidas digitales de la cámara
Acceso remoto	Cliente Web para la visualización y la reproducción remota Cliente de AXIS Camera Station (para Windows) incluido para la visualización, reproducción y administración remota

Seguridad	Protección multiusuario mediante contraseña para restringir los niveles de acceso a la cámara Usuarios de dominios locales o de Windows (Active directory)
Registros	Todos los eventos, filtro por día y/o por cámara. Registro de auditoría filtrado por día, cámara, evento y usuario
Idiomas	Español, inglés, francés, alemán, italiano y ruso
Instalación	Búsqueda automática y detección de cámaras
Licencias	Licencias básicas de AXIS Camera Station para 4 ó 10 cámaras/canales para su uso en un único PC/servidor dedicado. Licencias adicionales para +1 o +5 y hasta 25 cámaras/canales. Licencia de actualización de un año incluida en la licencia básica 4/10. Las actualizaciones futuras requieren una licencia de actualización por año. La versión de prueba de 30 días se puede actualizar a una versión con licencia
Registro de licencia	Puede registrarse automáticamente a través de Internet, o manualmente en www.axis.com en el periodo de gracia de cinco días
Requisitos mínimos del sistema	Windows XP Professional SP2, 2000 (SP4), 2003 Server (SP1), Internet Explorer 6.0 o posterior, DirectX 9.0c o posterior (para MPEG-2/4) Compatibilidad con TCP/IP Internet Information Services (IIS) (para el cliente Web) Entorno de ejecución Microsoft. NET (incluido en el paquete de instalación)
Requisitos mínimos del hardware para un sistema de 4 cámaras	Procesador Pentium 4, 2 GHz, unidad de CD 512 MB de RAM Disco duro: 1 GB para la instalación Sistema de archivos NTFS Monitor XGA (1024 x 768) o de mayor resolución Tarjeta gráfica AGP, Direct Draw (para MPEG-2/4), con memoria de 32MB o más Ratón Microsoft o dispositivo apuntador compatible Ethernet de 100 Mbits Para otras recomendaciones de hardware, visite www.axis.com/techsup
Requisitos mínimos del hardware para un sistema de 25 cámaras	Dual XEON 3 GHz, 1024 MB RAM, varios discos SCSI Red troncal Ethernet de 1000 Mbits (disco duro independiente para el SO y las grabaciones)
Configuración de disco duro recomendada	A 5 imágenes por segundo en CIF, hasta 10 cámaras por disco duro A 25 imágenes por segundo en CIF, 3-4 cámaras por disco duro
Requisitos mínimos para el cliente de AXIS Camera Station y acceso remoto a través de la Web	Procesador Pentium 4 a 1 GHz 256 MB de RAM Monitor XGA (1024 x 768) o de mayor resolución Tarjeta gráfica AGP, Direct Draw (para MPEG-2/4), con memoria de 32 MB o más Windows XP Professional SP2, 2000 (SP4), 2003 Server (SP1), Internet Explorer 6.0 o posterior, DirectX 9.0c o posterior (para visualización en MPEG-2/4) Compatibilidad con TCP/IP Entorno de ejecución Microsoft. NET (incluido en el paquete de instalación) para el cliente
Protocolos compatibles	IP, HTTP, TCP, ICMP, RTSP, RTP, SMTP, FTP, DNS
Accesorios incluidos	Guía de instalación en inglés, francés, italiano, alemán y español, CD con el software y manual del usuario en inglés Clave de licencia
Aplicaciones (incluidas)	Cliente de AXIS Camera Station (para Windows) para la visualización, reproducción y administración remota. Interfaz Web de AXIS Camera Station para la visualización y reproducción remota
Accesorios (no incluidos)	AXIS Image Enhancer para mejorar la calidad de imagen en condiciones de niebla, humo, lluvia y nieve

Especificaciones de AXIS Image Enhancer

Compatibilidad	Compatible con todos los productos de vídeo IP de Axis excepto los productos MPEG-2. Se obtienen mejoras óptimas con vídeo en color grabado entre el amanecer y el anochecer
Visualización en directo	Mejora la visualización en directo a de todos los canales a velocidad de imagen completa
Reproducción	Mejora durante la reproducción de grabaciones (debe activarse en la grabación)

Exportación de clips de vídeo	Se puede aplicar la mejora durante la exportación
Instalación	Se incluye en la instalación de AXIS Camera Station y se desbloquea con claves de licencia
Licencias	Se requiere una clave de licencia para cada canal de vídeo. Puede adquirir claves de licencia en paquetes de 1 ó 5

Acerca de Axis

Axis mejora las inversiones en soluciones de red. Es una empresa innovadora que lidera el mercado de soluciones de vídeo IP y servidores de impresión. Axis fabrica productos y soluciones destinados a vigilancia, seguridad, supervisión remota y gestión de documentos. La empresa diseña su propia tecnología de chips, que utiliza tanto para sus productos, como para otros fabricantes.

Axis se fundó en 1984 y cotiza en el mercado bursátil de Estocolmo (XSSE : AXIS, Lista Attract-40). Asimismo, dispone de oficinas en 16 países y colabora con distribuidores, integradores de sistemas y socios fabricantes de equipos originales de 70 países. El 95% de sus ventas se realiza fuera de Suecia. Encontrará más información acerca de Axis en **www.axis.com**

www.axis.com/es

©2006 Axis Communications AB. Axis is a registered trademark of Axis Communications AB. All other company names and products are trademarks or registered trademarks of their respective companies. We reserve the right to introduce modifications without notice.

AXIS COMMUNICATIONS

Make your network smarter

Power Line Communication

CC1 DIN

1-Phase Low Voltage Capacitive Coupler

Unified IP platform for both multimedia and energy applications over existing power grid

Function

- Connection interface between PLC devices and the power lines

Technology

- Flexible DIN mount
- Capacitive coupling technique
- Proprietary solution (patented)
- Galvanic injection

Performance

- Low insertion loss: < 1,5 dB @ 50 Ω
  < 1.2 dB @ 100 Ω
- Large bandwidth: 1 - 34 MHz

Ilevo PLC System

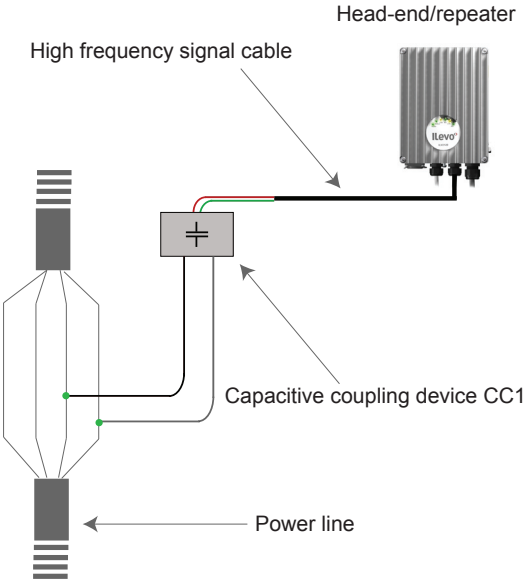
- CPEs
- Intermediate repeaters
- Head-ends
- **Net conditioning**
- Services
- Management software suite

Use

- Permanent PLC injection between 2 poles (phase-phase or phase-neutral)

Installation

- Meter rooms
- Transformer substations
- Street cabinet
- Any distribution panel



Main Benefits

- **Linear coupling performance**
- **Overvoltage category IV**
- **Industrialised DIN for fast deployments**
- **Designed for electrical network environment**
- **Impedance matching (compatibility with both 50 & 100 Ohm devices)**

a company of Schneider Electric

Ilevo

Specifications

Part Number		
50 Ω version	**PP1104/1**	
100 Ω version	**PP1104/2**	
Physical Features		
Weight	Approx. 90 g	
Dimensions	3 modules: 53 x 90 x 58 mm	
Material	Plastic	
Ports & connectors:	2 screw terminals	
Mounting	DIN mount, standard EN 50022	
Electrical Characteristics		
Rating(s)	240/415 V, 50/60 Hz	
Input impedance	50 Ω balanced **(PP1104/1)** 100 Ω balanced **(PP1104/2)**	
Bandwidth	1- 34 MHz	
Mean signal power admitted	1 W	
Attenuation from input to output	**PP1104/1** Approximately: 0.4 dB @ 1 MHz 1.5 dB @ 34 MHz	**PP1104/2** Approximately: 0.4 dB @ 1 MHz 1.2 dB @ 34 MHz
Environmental		
Ingress protection	IP20	
Operating		
Relative humidity	5% to 95% relative humidity non-condensing	
Ambient operating temperature	-25°C to +55°C	
Storage		
Relative humidity	5% to 95% non-condensing. According to ETS300019-1-1Class 1.1	
Temperature	-5°C to +45°C	
Standards		
Electrical Safety	IEC 60 950-1:2001 (EN 60 950-1:2001), Over voltage category IV. The product satisfies the provisions for CE marking according to the Low voltage Directive 72/23/EEC and 93/68/ECC.	
Labels		
CC1 DIN labeled with product number, model number and electrical data.		

In compliance with its continuous improvement policy, SEPC reserves the right to change those specifications without prior notice

Member of the leading global association for PLC companies

Schneider Electric Powerline Communications (SEPC)

Lagergrens gata 4,
Box 1561
652 26 Karlstad Sweden
Tel: + 46 (0) 54 22 39 00
Fax: + 46 (0) 54 22 39 99

59, chemin du vieux chêne
38240 Meylan France
Tel: +33 (0)4 76 60 51 54
Fax: +33 (0)4 76 60 59 11

Publication: SEPC
Pictures: Schneider Electric

DATA SHEET

CISCO CATALYST 2950 SERIES SWITCHES WITH STANDARD IMAGE SOFTWARE

PRODUCT OVERVIEW

The Cisco® Catalyst® 2950SX48, 2950T-48, 2950SX-24, 2950-24, and 2950-12 switches, members of the Cisco Catalyst 2950 Series, are standalone, fixed-configuration, managed 10/100 Mbps switches providing basic workgroup connectivity for small to midsize networks. These wire-speed desktop switches come with Standard Image software features and offer Cisco IOS® Software functions for basic data, voice, and video services at the edge of the network.

Embedded in all Cisco Catalyst 2950 Series switches is the Cisco Device Manager software, which allows users to easily configure and monitor the switch using a standard Web browser, eliminating the need for more complex terminal emulation programs and knowledge of the command-line interface (CLI). Customers can easily initialize the switch with web-based Cisco Express Setup, without using the CLI. In addition, with Cisco Network Assistant, a standalone network management software, customers can simultaneously configure and troubleshoot multiple Cisco Catalyst desktop switches. Cisco Device Manager, Cisco Express Setup, and Cisco Network Assistant reduce the cost of deployment by enabling less-skilled personnel to set up switches quickly. Furthermore, Cisco Catalyst 2950 Series switches provide extensive management tools using Simple Network Management Protocol (SNMP) network management platforms such as CiscoWorks.

This product line offers two distinct sets of software features and a range of configurations to allow small, midsize, and enterprise branch offices to select the right combination for the network edge. For networks that require additional security, advanced quality of service (QoS), and high availability, Enhanced Image software delivers intelligent services such as rate limiting and security filtering for deployment at the network edge.

The Cisco Catalyst 2950SX-48, 2950T-48, 2950SX-24, 2950-24 and 2950-12 switches (Figures 1–5) are available only with the Standard Image (SI) software for the Cisco Catalyst 2950 Series. They cannot be upgraded to the Enhanced Image (EI) software.

- **Cisco Catalyst 2950SX 48 Switch**—48 10/100 Mbps ports with two fixed 1000BASE-SX uplinks
- **Cisco Catalyst 2950T 48 Switch**—48 10/100 Mbps ports with two fixed 10/100/1000BASE-T uplinks
- **Cisco Catalyst 2950SX 24 Switch**—24 10/100 Mbps ports with two fixed 1000BASE-SX uplinks
- **Cisco Catalyst 2950 24 Switch**—24 10/100 Mbps ports
- **Cisco Catalyst 2950 12 Switch**—12 10/100 Mbps ports

Figure 1. Cisco Catalyst 2950-12 Switch

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 2. Cisco Catalyst 2950-24 Switch

Figure 3. Cisco Catalyst 2950SX-24 Switch

Figure 4. Cisco Catalyst 2950T-48 Switch

Figure 5. Cisco Catalyst 2950SX-48 Switch

These switches provide customers with many connectivity and port-density options. The Cisco Catalyst 2950-12 and Cisco Catalyst 2950-24 switches provide 12 and 24 10/100 Mbps ports, respectively, for edge connectivity. Depending on port-density requirements, customers with gigabit fiber uplink connectivity needs can choose between the Cisco Catalyst 2950SX-24 Switch, which provides 24 10/100 Mbps ports and 2 integrated 1000BASE-SX ports, and the Cisco Catalyst 2950SX-48 Switch, which provides 48 10/100 Mbps ports and 2 integrated 1000BASE-SX ports.

With these integrated ports, customers get an extremely cost-effective solution for delivering gigabit speeds using fiber. These switches are ideal for education and government segments where fiber uplinks are required. For customers that do not need fiber connectivity, the Cisco Catalyst 2950T-48 Switch with 48 10/100 Mbps ports and two integrated 10/100/1000 BASE-T ports is a cost-effective alternative. The 10/100/1000 BASE-T ports can be used for server connectivity or for uplink connectivity to distribution or other switches. Dual ports also provide redundancy and increased availability, as well as provide a cost-effective means for cascading switches and managing them as a cluster. The Cisco Catalyst 2950 Series Intelligent Ethernet switches with Enhanced Image software are fixed-configuration models that bring intelligent services, such as advanced QoS, enhanced security, and high availability to the network edge while maintaining the simplicity of traditional LAN switching. Combining a Cisco Catalyst 2950 Series Intelligent Ethernet Switch with a Cisco Catalyst 3550 Series Switch enables IP routing from the edge to the core of the network. Refer to the Cisco Catalyst 2950 Series Enhanced Image Data Sheet for more information: http://www.cisco.com/en/US/products/hw/switches/ps628/products_data_sheet09186a00801cfb64.html

© 2004 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

NETWORK AVAILABILITY WITH WIRE-SPEED PERFORMANCE IN CONNECTING END STATIONS TO THE LAN

With a switching fabric of 13.6 Gbps and a maximum forwarding bandwidth of 13.6 Gbps, Cisco Catalyst 2950 Series switches deliver wire-speed performance on all ports in connecting end stations and users to the company LAN. Cisco Catalyst 2950 Series switches with basic services support performance-boosting features such as Cisco Fast EtherChannel® to provide high-performance bandwidth between Cisco Catalyst switches, routers, and servers.

NETWORK SECURITY

Cisco Catalyst 2950 Series switches offer enhanced data security through a wide range of security features. These features allow customers to provide network security based on users or MAC addresses. The security enhancements are available free by downloading the latest software for the Cisco Catalyst 2950 Series switches.

Secure Shell version 2 (SSHv2) protects information from being eavesdropped or being tampered with by encrypting information being passed on the network, thereby guarding administrative information. Private VLAN Edge isolates ports on a switch, ensuring that traffic travels directly from the entry point to the aggregation device through a virtual path and cannot be directed to another port. In addition, for authentication of users with a TACACS+ or a RADIUS server, 802.1x provides port-level security. Simple Network Management Protocol Version 3 (SNMPv3) (non-cryptographic) monitors and controls network devices as well as manages configurations, performance, collection of statistics, and security.

For authentication of users with a Terminal Access Controller Access Control System (TACACS+) or RADIUS server, 802.1x provides port-level security. 802.1x, in conjunction with a RADIUS server, allows for dynamic port-based user authentication. 802.1x-based user authentication can be extended to dynamically assign a VLAN based on a specific user, regardless of where they connect on the network. With 802.1x with Guest VLAN, guests are allowed access to the Internet via the Guest VLAN but cannot access the customer's internal network. This intelligent adaptability allows IT departments to offer greater flexibility and mobility to their stratified user populations. By combining access control and user profiles with secure network connectivity, services, and applications, enterprises can more effectively manage user mobility and drastically reduce the overhead associated with granting and managing access to network resources.

With the Cisco Catalyst 2950SX-48, 2950T-48, 2950SX-24, 2950-24, and 2950-12 switches, network managers can make ports and consoles highly secure. MAC-address-based port-level security prevents unauthorized stations from accessing the switch. Multilevel access security on the switch console and the Web management interface prevents unauthorized users from accessing or altering switch configurations and can be implemented using an internal user database on each switch or a centrally administered TACACS+ or RADIUS server. Using 802.1x in conjunction with a RADIUS server allows dynamic port-based user authentication. In addition, 802.1x can coexist with port security on a per-port basis. Security features can be deployed using Cisco Network Assistant software security wizards, which ease the deployment of security features that restrict user access to a server or portion of the network or restrict the applications used in certain areas of the network.

NETWORK CONTROL

Cisco Catalyst 2950SX-48, 2950T-48, 2950SX-24, 2950-24, and 2950-12 switches deliver LAN-edge QoS, supporting two modes of reclassification. One mode—based on the IEEE 802.1p standard—honors the class-of-service (CoS) value at the ingress point and assigns the packet to the appropriate queue. In the second mode, packets can be reclassified based on a default CoS value assigned to the ingress port by the network administrator. In the case of frames that arrive without a CoS value (such as untagged frames), these Cisco Catalyst 2950 Series switches support classification based on a default CoS value per port assigned by the network administrator. After the frames have been classified or reclassified using one of the above modes, they are assigned to the appropriate queue at the egress. Cisco Catalyst 2950 Series switches support four egress queues, which allow the network administrator to be more discriminating and granular in assigning priorities for the various applications on the LAN. Strict Priority Scheduling configuration ensures that time-sensitive applications, such as voice, always follow an expedited path through the switch fabric. Weighted Round Robin (WRR) scheduling, another significant enhancement, ensures that lower-priority traffic receives attention without comprising the priority settings administered by a network manager. These features allow network administrators to prioritize mission-critical, time-sensitive

© 2004 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

traffic, such as voice (IP telephony traffic), enterprise resource planning (Oracle, SAP, etc.), and computer-assisted design and manufacturing, over less time-sensitive applications such as FTP or e-mail (Simple Mail Transfer Protocol).

NETWORK AVAILABILITY

To provide efficient use of resources for bandwidth-hungry applications like multicasts, Cisco Catalyst 2950 Series switches support Internet Group Management Protocol Version 3 (IGMPv3) snooping in hardware. Through the support and configuration of IGMP snooping through the Cisco Network Assistant software, these Cisco Catalyst 2950 Series switches deliver outstanding performance and ease of use in administering and managing multicast applications on the LAN.

The IGMPv3 snooping feature allows the switch to “listen in” on the IGMP conversation between hosts and routers. When a switch hears an IGMP join request from a host for a given multicast group, the switch adds the host’s port number to the group destination address list for that group. And when the switch hears an IGMP leave request, it removes the host’s port from the content-addressable memory (CAM) table entry.

Multicast VLAN Registration (MVR) is designed for applications using wide-scale deployment of multicast traffic across an Ethernet ring-based service provider network (for example, the broadcast of multiple television channels over a service-provider network). MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the networkwide multicast VLAN.

Per VLAN Spanning Tree Plus (PVST+) allows users to implement redundant uplinks while also distributing traffic loads across multiple links. This is not possible with standard Spanning Tree Protocol implementations. Cisco UplinkFast technology ensures immediate transfer to the secondary uplink, much better than the traditional 30- to 60-second convergence time. This is yet another enhancement of the Spanning Tree Protocol implementation. An additional feature that enhances performance is voice VLAN. This feature allows network administrators to assign voice traffic to a VLAN dedicated to IP telephony, thereby simplifying phone installations and providing easier network traffic administration and troubleshooting.

NETWORK MANAGEMENT

Customers can configure one switch at a time with the embedded Cisco Device Manager, or configure and troubleshoot multiple switches with Cisco Network Assistant, a free standalone network management software application optimized for LANs of small and medium-sized businesses with up to 250 users. Cisco Device Manager offers a simple and intuitive GUI interface for configuring and monitoring the switch. The software is Web-based and embedded in Cisco Catalyst 3750, 3650, 3550, 2970, 2950, and 2940 Switches. Cisco Express Setup simplifies the switch initialization. Users now have the option to set up the switch through a Web browser, eliminating the need for more complex terminal emulation programs and knowledge of the CLI. Cisco Device Manager and Cisco Express Setup reduce the cost of deployment by enabling less-skilled personnel to quickly and simply set up switches.

With Cisco Network Assistant, customers can configure multiple ports and switches simultaneously, perform software updates across multiple switches at once, and copy configurations to other switches for rapid network deployments. Bandwidth graphs and link reports provide useful diagnostic information, and the topology map gives network administrators a quick view of the network status. Cisco Network Assistant supports a wide range of Cisco Catalyst intelligent switches from Cisco Catalyst 2950 through Cisco Catalyst 4506. Through a user-friendly GUI, users can configure and manage a wide array of switch functions and start the device manager of Cisco routers and Cisco wireless access points

The Cisco Network Assistant Software Guide Mode leads the user step-by-step through the configuration of advanced features and provides enhanced online help for context-sensitive assistance. Cisco AVVID (Architecture for Voice, Video and Integrated Data) Wizards provide automated configuration of the switch to optimally support video streaming or video conferencing, voice over IP (VoIP), and mission-critical applications. In addition, Smartports offers a set of verified feature macros per connection type in an easy-to-apply manner. With these macros, users can consistently and reliably configure essential security, availability, quality of service, and manageability features recommended for Cisco Business Ready Campus solutions with minimal effort and expertise. These Wizards and Smartports can save hours of time for network administrators, eliminate human errors, and ensure that the configuration of the switch is optimized for these applications.

© 2004 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

In addition to Cisco Network Assistant, Cisco Catalyst 2950 Series switches provide extensive management tools using SNMP network management platforms such as CiscoWorks. Managed with CiscoWorks, Cisco Catalyst family switches can be configured and managed to deliver end-to-end device, VLAN, traffic, and policy management. Coupled with CiscoWorks, Cisco Resource Manager Essentials, a Web-based management tool, offers automated inventory collection, software deployment, easy tracking of network changes, views into device availability, and quick isolation of error conditions.

PRODUCT FEATURES AND BENEFITS

Feature	Benefit
Availability	
Superior Redundancy for Fault Backup	• IEEE 802.1D Spanning Tree Protocol support for redundant backbone connections and loop-free networks simplifies network configuration and improves fault tolerance. • IEEE 802.1w Rapid Spanning- Tree Protocol (RSTP) provides rapid convergence of the spanning tree, independent of spanning-tree timers. • Per VLAN Rapid Spanning Tree (PVRST+) allows rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances. • Support for Cisco Spanning Tree Protocol enhancements such as UplinkFast, BackboneFast, and PortFast technologies ensures quick failover recovery and enhances overall network stability and availability. • Support for Cisco's optional RPS 675, 675-watt redundant AC power system, which provides a backup power source for one of six switches, for improved fault tolerance and network uptime. • Unidirectional link detection (UDLD) and aggressive UDLD detect and disable unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults.
Integrated Cisco IOS Software Features for Bandwidth Optimization	• Bandwidth aggregation through Cisco EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches to routers and individual servers. Port Aggregation Protocol (PagP) is available to simplify configuration. • VLAN1 minimization allows VLAN1 to be disabled on any individual VLAN trunk link. • IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) allows a spanning-tree instance per VLAN, enabling Layer 2 load sharing on redundant links. • Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall system performance. • Per VLAN Spanning Tree Plus (PVST+) allows for Layer 2 load sharing on redundant links to efficiently use the extra capacity inherent in a redundant design. • VLAN Trunking Protocol (VTP) pruning limits bandwidth consumption on VTP trunks by flooding broadcast traffic only on trunk links required to reach the destination devices. Dynamic Trunking Protocol (DTP) enables dynamic trunk configuration across all ports in the switch. • IGMPv3 snooping provides for fast client joins and leaves of multicast streams and limits bandwidth-intensive video traffic to the requestors. MVR, IGMP filtering, and fast-join and immediate leave are available as enhancements. IGMP Snooping time can be adjusted to optimize the performance of multicast data flows.
Security	
Networkwide Security Features	• A private VLAN edge provides security and isolation between ports on a switch, ensuring that voice traffic travels directly from its entry point to the aggregation device through a virtual path and cannot be directed to a different port. • Support for the 802.1x standard allows users to be authenticated regardless of which LAN ports they are accessing, and it provides unique benefits to customers who have a large base of mobile (wireless) users accessing the network. – 802.1x with voice VLAN permits an IP phone access to the voice VLAN regardless of the authorized or unauthorized state of the port. – 802.1x with Port Security authenticates the port and manages network access for all MAC addresses, including

© 2004 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Feature	Benefit
	that of the client. – IEEE 802.1x with Guest VLAN allows guests without 802.1x clients to have limited network access on the Guest VLAN. – IEEE 802.1x with VLAN assignment allows a dynamic VLAN assignment for a specific user regardless of where the user is connected. • SSHv2 provides network security by encrypting administrator traffic during Telnet sessions. SSHv2 requires a special cryptographic software image due to US export restrictions • Port Security secures the access to a port based on the MAC address of a user's device. The aging feature removes the MAC address from the switch after a specific time to allow another device to connect to the same port. • MAC Address Notification allows administrators to be notified of new users added or removed from the network. • Multilevel security on console access prevents unauthorized users from altering the switch configuration. • Trusted Boundary provides the ability to trust the QoS priority settings if an IP phone is present and disable the trust setting in the event that the IP phone is removed, thereby preventing a rogue user from overriding prioritization policies in the network. • TACACS+ and RADIUS authentication enables centralized control of the switch and restricts unauthorized users from altering the configuration. • SPAN support of Intrusion Detection Systems (IDSs) to monitor, repel, and report network security violations • SNMPv3 (non-crypto) monitors and controls network devices, manages configurations, statistics collection, performance, and security. • Cisco Network Assistant software security wizards ease the deployment of security features for restricting user access to a server, a portion of the network, or access to the network.
Quality of Service	
Layer 2 QoS	• Support for reclassifying frames is based either on 802.1p class-of-service (CoS) value or default CoS value per port assigned by network manager. • Four queues per egress port are supported in hardware. • The Weighted Round Robin (WRR) scheduling algorithm ensures that low-priority queues are not starved. • Strict priority queue configuration via Strict Priority Scheduling ensures that time-sensitive applications such as voice always follow an expedited path through the switch fabric.
Management	
Superior Manageability	• SNMP and Telnet interface support delivers comprehensive in-band management, and a CLI management console provides detailed out-of-band management. • An embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis. • A Switched Port Analyzer (SPAN) port can mirror traffic from one or many ports to another port for monitoring all nine RMON groups with an RMON probe or network analyzer. • Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location. • Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all switches within the intranet. • Layer 2 traceroute eases troubleshooting by identifying the physical path that a packet takes from the source device to a destination device. • Multifunction LEDs per port for port status, half-duplex/full-duplex, 10BASE-T/100BASE-TX/1000BASE-T indication, as well as switch-level status LEDs for system, redundant power supply, and bandwidth utilization provide a comprehensive and convenient visual management system. • Crash information support enables a switch to generate a crash file for improved troubleshooting.

© 2004 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Feature	Benefit
	• Show-interface-capabilities provide information about the configuration capabilities of any interface. • Response Time Monitoring (RTTMON) MIB allows users to monitor network performance between a Cisco Catalyst switch and a remote device.
Cisco Network Assistant Software	• Cisco Network Assistant Software is a free, standalone network management application software that simplifies the administration of networks of up to 250 users. It supports a wide range of Cisco Catalyst intelligent switches from Cisco Catalyst 2950 through Cisco Catalyst 4506. With Cisco Network Assistant, users can manage Cisco Catalyst switches plus launch the device managers of Cisco integrated services routers (ISRs) and Cisco Aironet WLAN access points by simply clicking on its icon in the topology map. • Cisco AVVID (Architecture for Voice, Video and Integrated Data) wizards use just a few user inputs to automatically configure the switch to optimally handle different types of traffic: voice, video, multicast, and high-priority data. • One-click software upgrades can be performed across the entire cluster simultaneously, and configuration cloning enables rapid deployment of networks. • Cisco Network Assistant Guide Mode helps users configure powerful advanced features by providing step-by-step instructions. • Cisco Network Assistant provides enhanced online help for context-sensitive assistance. • Easy-to-use graphical interface provides both a topology map and front-panel view of the switches. • Multidevice- and multiport-configuration capabilities allow network administrators to save time by configuring features across multiple switches and ports simultaneously. • User-personalized interface allows users to modify polling intervals, table views, and other settings within Cisco Network Assistant and retain these settings the next time they use Cisco Network Assistant. • Alarm notification provides automated e-mail notification of network errors and alarm thresholds.
Support for CiscoWorks	• Manageability is enabled through CiscoWorks network management software on a per-port and per-switch basis, providing a common management interface for Cisco routers, switches, and hubs. • SNMPv1, v2, and v3 (non-cryptographic) and Telnet interface support delivers comprehensive in-band management, and a command-line-interface (CLI) management console provides detailed out-of-band management. • Cisco Discovery Protocol (CDP) versions 1 and 2 enable a CiscoWorks network management station to automatically discover the switch in a network topology. • Support is provided by the CiscoWorks LAN Management Solution.
Ease of Use and Deployment	• Cisco Device Manager is an embedded web-based software that allows the customer to easily configure and troubleshoot the switch, eliminating the need for more complex terminal emulation programs and CLI knowledge, and reducing the cost of deployment by enabling less-skilled personnel to quickly and simply set up switches. • Cisco Express Setup allows the customer to quickly and easily initialize a switch with a web browser • Smartports offers a set of verified feature macros per connection type in an easy-to-apply manner. With these macros, users can consistently and reliably configure essential security, availability, quality of service, and manageability features recommended for Cisco Business Ready Campus solutions with minimal effort and expertise. • Auto-configuration eases deployment of switches in the network by automatically configuring multiple switches across a network using a bootp server. • Autosensing on each port detects the speed of the attached device and automatically configures the port for 10 or 100 Mbps operation, easing the deployment of the switch in mixed-speed environments. • Auto-negotiating on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth. • Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad. This is similar to Cisco EtherChannel and PagP. • Cisco Discovery Protocol versions 1 and 2 enable a CiscoWorks network management station to automatically discover the switch in a network topology. • Cisco VTP supports dynamic VLANs and dynamic trunk configuration across all switches.

© 2004 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Feature	Benefit
	• Support for dynamic VLAN assignment through implementation of VLAN Membership Policy Server (VMPS) client functions provides flexibility in assigning ports to VLANs. • Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier network administration and troubleshooting. • The default configuration stored in Flash memory ensures that the switch can be quickly connected to the network and can pass traffic with minimal user intervention.

PRODUCT SPECIFICATIONS

Feature	Description
Performance	• 13.6-Gbps switching fabric (Catalyst 2950T-48-SI and 2950SX-48-SI) • 8.8-Gbps switching fabric (Catalyst 2950SX-24, 2950-24, 2950-12) • Cisco Catalyst 2950-12: 2.4 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950-24: 4.8 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950SX-24: 8.8 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950T-48: 13.6 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950SX-48: 13.6 Gbps maximum forwarding bandwidth (Forwarding rates based on 64 byte packets) • Cisco Catalyst 2950-12: 1.8 Mpps wire-speed forwarding rate • Cisco Catalyst 2950-24: 3.6 Mpps wire-speed forwarding rate • Cisco Catalyst 2950SX-24: 6.6 Mpps wire-speed forwarding rate • Cisco Catalyst 2950T-48: 10.1 Mpps wire-speed forwarding rate • Cisco Catalyst 2950SX-48: 10.1 Mpps wire-speed forwarding rate • 8 MB packet buffer memory architecture shared by all ports • 16 MB DRAM and 8 MB Flash memory • Configurable up to 8000 MAC addresses

Feature	Description/Part Numbers
Management	• BRIDGE-MIB • CISCO-2900-MIB • CISCO-BULK-FILE-MIB • CISCO-CDP-MIB • CISCO-CLASS-BASED-QOS-MIB • CISCO-CONFIG-COPY-MIB • CISCO-CONFIG-MAN-MIB • CISCO-ENVMON-MIB • CISCO-FLASH-MIB • CISCO-FTP-CLIENT-MIB • CISCO-IMAGE-MIB • CISCO-IPMROUTE-MIB • CISCO-MAC-NOTIFICATION-MIB • CISCO-MEMORY-POOL-MIB • CISCO-PAGP-MIB • CISCO-PING-MIB

© 2004 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Feature	Description/Part Numbers
	• CISCO-PORT-SECURITY-MIB • CISCO-PROCESS-MIB • CISCO-PRODUCTS-MIB • CISCO-RTTMON-MIB • CISCO-SMI • CISCO-STACKMAKER-MIB • CISCO-STP-EXTENSIONS-MIB • CISCO-SYSLOG-MIB • CISCO-TC • CISCO-TCP-MIB • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VTP-MIB • ENTITY-MIB • IANAifType-MIB • IF-MIB (RFC 1573) • OLD-CISCO-CHASSIS-MIB • OLD-CISCO-CPU-MIB • OLD-CISCO-INTERFACES-MIB • OLD-CISCO-IP-MIB • OLD-CISCO-MEMORY-MIB • OLD-CISCO-SYSTEM-MIB • OLD-CISCO-TCP-MIB • OLD-CISCO-TS-MIB • RFC1213-MIB (MIB-II) • RFC1398-MIB (ETHERNET-MIB) • RMON-MIB (RFC 1757) • RS-232-MIB • SNMPv2-MIB • SNMPv2-SMI • SNMPv2-TC • TCP-MIB • UDP-MIB
Standards	• IEEE 802.1x support • IEEE 802.3x full duplex on 10BASE-T and 100BASE-TX ports • IEEE 802.1D Spanning-Tree Protocol • IEEE 802.1p class-of-service (CoS) prioritization • IEEE 802.1Q VLAN • IEEE 802.1s • IEEE 802.1w • IEEE 802.3 10BASE-T specification • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ad

© 2004 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Feature	Description/Part Numbers
	• IEEE 802.3z 1000BASE-X specification
Connectors and Cabling	• 10BASE-T ports: RJ-45 connectors, two-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling • 100BASE-TX ports: RJ-45 connectors; four-pair Category 5 UTP cabling • 1000BASE-SX ports: MT-RJ connectors, up to 1800 feet (550 meters) cable distance for 50/125 or up to 900 ft (275 m) cable distance for 62.5/125 micron multimode fiber-optic cabling • Management console port: 8-pin RJ-45 connector, RJ-45-to-DB9 adapter cable for PC connections; for terminal connections, use RJ-45-to-DB25 female data-terminal-equipment (DTE) adapter (can be ordered separately, Cisco part number ACS-DSBUASYN=)
MT-RJ Patch Cables for Cisco Catalyst 2950SX 24 Switch	*Type of cable, Cisco part number:* • 1-meter MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-1M • 3-meter MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-3M • 5-meter MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-5M • 1-meter MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-1M • 3-meter MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-3M • 5-meter MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-5M
Power Connectors	Customers can provide power to a switch by using the internal power supply, the Cisco RPS 675 Redundant Power System. The connectors are located at the back of the switch. • Internal power supply connector – The internal power supply is an auto-ranging unit. – The internal power supply supports input voltages between 100 and 240 VAC. – Use the supplied AC power cord to connect the AC power connector to an AC power outlet. • Cisco RPS 675 connector – The connector offers connection for an optional Cisco RPS 675 that uses AC input and supplies DC output to the switch. – The connector offers a 675W redundant power system that supports one of up to six external network devices and provides power to one failed device at a time. – The connector automatically senses when the internal power supply of a connected device fails and provides power to the failed device, preventing loss of network traffic. – Attach only the Cisco RPS 675 (Model PWR675-AC-RPS-NI=) to the redundant power supply receptacle with this connector.
Indicators	• Per-port status LEDs: link integrity, disabled, activity, speed, and full-duplex indications • System status LEDs: system, RPS, and bandwidth-utilization indications
Dimensions and Weight (H x W x D)	• 1.72 x 17.5 x 9.52 in. (4.36 x 44.45 x 24.18 cm) (Cisco Catalyst 2950SX-24, 2950-24, 2950-12) • 1.72 x 17.5 x 13 in. (4.36 x 44.45 x 33.02 cm) (Cisco Catalyst 2950SX-48, 2950T-48) • 1 RU high (1.72 in./4.36 cm) • 6.5 lb (3.0 kg) (Cisco Catalyst 2950SX-24, 2950-24, 2950-12) • 10.b lb (4.8 kg) (Cisco Catalyst 2950SX-48, 2950T-48)

© 2004 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Feature	Description/Part Numbers
Environmental Ranges	• Operating temperature: 32 to 113°F (0 to 45°C) • Storage temperature: –13 to 158°F (–25 to 70°C) • Operating relative humidity: 10–85% (non-condensing) • Operating altitude: Up to 10,000 ft (3000 m) • Storage altitude: Up to 15,000 ft (4500 m)
Power Requirements	• Power consumption: 30W (maximum), 102 BTUs per hour (Cisco Catalyst 2950SX-24, 2950-24. 2950-12) • Power consumption: 45W (maximum), 154 BTUs per hour (Cisco Catalyst 2950T-48, 2950SX-48) • AC input voltage: 100 to 127, 200 to 240 VAC (auto-ranging) • AC input frequency: 47 to 63 Hz • DC input voltages for Cisco RPS 675 and Cisco RPS 300: +12V at 4.5A
Acoustic Noise	ISO 7770, bystander position, operating to an ambient temperature of 86°F (30°C): • WS-C2950-24, WS-C2950-12, WS-C2950SX-24: 46 dBa • WS-C2950T-48-SI, WS-C2950SX-48-SI: 48 dBa
Predicted Mean Time Between Failure	• 398,240 hours (Cisco Catalyst 2950-24) • 482,776 hours (Cisco Catalyst 2950-12) • 480,346 hours (Cisco Catalyst 2950SX-24) • 268,876 hours (Cisco Catalyst 2950T-48-SI) • 274,916 hours (Cisco Catalyst 2950SX-48-SI)
Regulatory Agency Approvals	
Safety Certifications	• UL 60950/CSA 22.2 No. 950 • IEC 60950/EN 60950 • AS/NZS 3260, TS001 • CE Marking
Electromagnetic Emissions Certifications	• FCC Part 15 Class A • EN 55022: 1998 (CISPR 22) Class A • EN 55022: 1998 (CISPR 22) • VCCI Class A • AS/NZS 3548 Class A • CE Marking • CNS 13438 Class A • CLEI Code • MIC
Warranty	• Lifetime limited warranty

© 2004 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

SERVICE AND SUPPORT

The services and support programs described here are available as part of the Cisco Desktop Switching Service and Support solution and are available directly from Cisco Systems® and through resellers.

Service and Support	Features	Benefits
Advanced Services		
Total Implementation Solutions (TIS)—Available direct from Cisco **Packaged Total Implementation Solutions (Packaged TIS)**—Available through resellers	• Project management • Site survey, configuration deployment • Installation, text, and cutover • Training • Major moves, adds, changes • Design review and product staging	• Supplements existing staff • Ensures that functions meet needs • Mitigates risk
Technical Support Services		
Cisco SMARTnet® services and Cisco SMARTnet Onsite services—Available direct from Cisco **Packaged Cisco SMARTnet services**—Available through resellers	• Around-the-clock access to software updates • Web access to technical repositories • Telephone support through the Technical Assistance Center • Advance replacement of hardware parts	• Enables proactive or expedited issue resolution • Lowers cost of ownership by using Cisco expertise and knowledge • Minimizes network downtime

ORDERING INFORMATION

Model Numbers	Configuration
WS-C2950-12	• 12 10/100 Mbps ports • 1-RU standalone, fixed-configuration, managed 10/100 Mbps switch • Standard Image (SI) Software
WS-C2950-24	• 24 10/100 Mbps ports • 1-RU standalone, fixed-configuration, managed 10/100 Mbps switch • Standard Image (SI) Software
WS-C2950SX-24	• 24 10/100 Mbps ports with two fixed 1000BASE-SX uplinks • 1-RU standalone, fixed-configuration, managed 10/100 Mbps switch • Standard Image (SI) Software
WS-C2950T-48-SI	• 48 10/100 Mbps ports with two fixed 10/100/1000BASE-T uplinks • 1-RU standalone, fixed-configuration, managed 10/100 Mbps switch • Standard Image (SI) Software
WS-C2950SX-48-SI	• 48 10/100 Mbps ports with two fixed 1000BASE-SX uplinks • 1-RU standalone, fixed-configuration, managed 10/100 Mbps switch • Standard Image (SI) Software

© 2004 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

FOR MORE INFORMATION

For more information about Cisco products, contact:

- United States and Canada: 800 553-NETS (6387)
- Europe: 32 2 778 4242
- Australia: 612 9935 4107
- Other: 408 526-7209
- World Wide Web: http://www.cisco.com

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
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
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
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
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.**

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. Aironet, Catalyst, Cisco, Cisco Systems, the Cisco Systems logo, EtherChannel, and SMARTnet are registered 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)

204108.62_ETMG_MS_12.04

Printed in the USA

© 2004 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Corinex Low Voltage Access Gateway

The Corinex Low Voltage Access Gateway is the latest development in 200Mbps AV200 technology from Corinex. The LV Gateway allows an easy installation to neighborhoods or Multi Dwelling Units (MDUs) where the LV Gateway acts as a head-end modem, extending an internet connection (Fiber, ADSL, Satellite) either to a powerline or coaxial cable infrastructure, depending on the customers requirements.

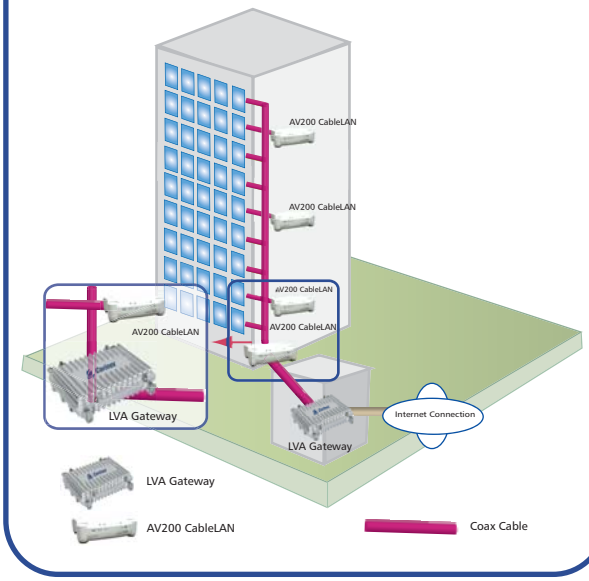
The Corinex LV Access Gateway allows users to extend an internet connection to a powerline or cable network within an MDU, without the need for installing new wiring. End users can connect their Ethernet enabled devices such as PC's, VoIP phones, Media Centers, etc., using the Corinex AV200 Powerline Ethernet Adapter or Corinex AV200 CableLAN Adapter, to any electrical or coaxial socket in a premise to create a link to the internet.

By combining the Corinex LV Access Gateway with the Corinex MDU Gateway, MDU's can avoid the problem of excessive delays associated with traditional Time Division Repeaters being used for multiple MDU's within the same community. Corinex's powerful patent pending technology ensures that each LV Access Gateway communicates only with each head-end MDU Gateway, not with the hundreds or thousands of end users that other LV Access products must share time slots between. The net effect is a network topology that delivers maximum performance and has virtually unlimited scalability.

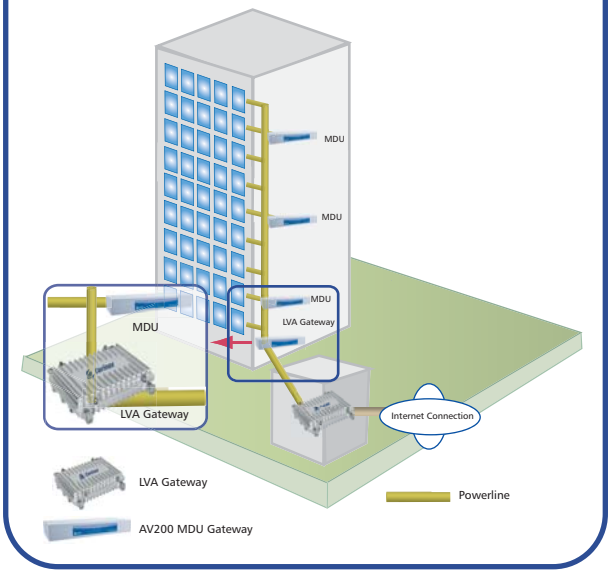
AV200 Powerline technology by Corinex provides numerous networking possibilities with amazingly fast physical layer transfer rates of up to 200 Mbps. OFDM technology and the powerful error correction system used in AV200 technology allow for robust performance under harsh conditions in electrical or coaxial networks. Combined with other Corinex Access and In-Premise products such as the Corinex Medium Voltage Access Gateway, Corinex AV200 Router, Corinex AV200 Powerline Ethernet Adapter, and Corinex AV200 CableLAN Adapter, the Corinex Low Voltage Access Gateway rounds out the largest 200 Mbps Powerline product portfolio in the world.

The Corinex Low Voltage Access Gateway also supports external low voltage couplers that can be used to inject an internet signal into different phases within the MDU or to couple into other voltages such as the 480v power found in many MDU's.

Coax network



Powerline network



Features:

- Physical data rates of up to 200 Mbps over distances of 300 meters (powerline) or 1200 meters (coax).
- Powerline and coaxial network interface ports allowing an internet connection to be extended over electrical wiring or existing cable infrastructure.
- 802.1Q VLAN & Optimized VLANs
- Powerful DES/3DES encryption
- Integrated 802.1D Ethernet Bridge With Optimized Spanning Tree Protocol
- 8-level priority queues, with programmable priority-classification Engine
- Priority classification according to 802.1P tags, IP coding (IPv4 or Ipv6) or TCP source/destination ports
- 10/100BaseT Fast Ethernet interface for connection to the Internet Gateway
- CSMA/CARP (Carrier Sense Multiple Access with Collision Avoidance and Resolution using Priorities) protocol
- Bridge Forwarding Table for 64 MAC Addresses
- OFDM technology and powerful error correction system allow robust performance under harsh conditions in the electrical/cable network
- Optimized support for broadcast and multicast traffic
- Optional external coupling on coaxial port
- Configuration via web interface or via Corinex AV200 Network Management software

Standards

- 802.3u
- 802.1P
- 802.1Q
- Compliant with FCC Part 15, EN 55022 EMC limits
- UPA-compliant

Package Contents

- Corinex Low Voltage Access Gateway
- Power cable
- Coax cable
- Installation Guide and CD with documentation

Product Specification

Product code: CXP-LVA-GWY

Technical Specifications

Standards Compliance	IEEE 802.3u Pre-UPA compliant
Backbone Speed	Up to 200 Mbps on physical layer 100 Mbps on ethernet
AC Plug Type	US, EU, UK and AUS
LED Status Lights	Power, PLC Link/Act, Eth Link/Act
Interface	10/100BaseT Fast Ethernet, Powerline Port, Coaxial Port
Frequency Range	2 – 34 MHz
Power Input	85 to 265 V AC, 50/60 Hz
Weight	7 kg
Dimensions	230 x 185 x 80 mm
Transmitted Power spectral density	-50 dBm/Hz
Power Consumption	7 W
Safety & EMI	FCC Part 15, EN 55022 EMC limits
Operating Temperature	0° to 50°C (32°F to 122°F)
Operating Humidity	10% to 80% non-condensing

Product features and design may vary by version and region.

UPA UNIVERSAL POWERLINE ASSOCIATION

Corinex AnyWire Connectivity™

Corinex Communications Corp.
#670 - 789 West Pender Street
Vancouver, BC
Canada V6C 1H2
Tel: +1 - 604 - 692 0520
Fax: +1 - 604 - 694 0061
E-mail: global@corinex.com
http://www.corinex.com

Corinex Global, a.s.
Ruzova dolina 19
821 08 Bratislava
Slovak Republic
Tel.: +421 - 2 - 5021 4811
Fax: +421 - 2 - 5556 7309
E-mail: global@corinex.com

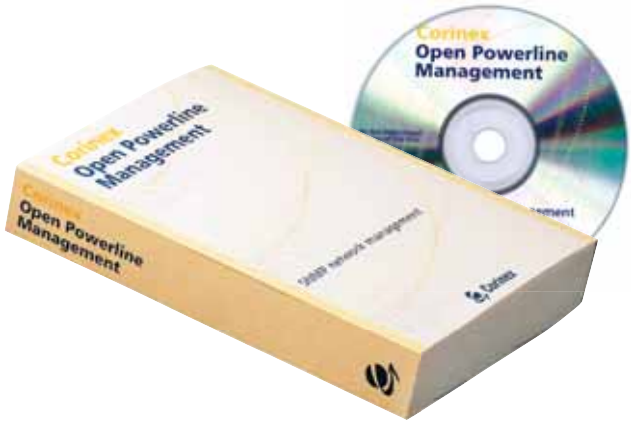
Corinex is a registered trademark of Corinex Communications Corp.

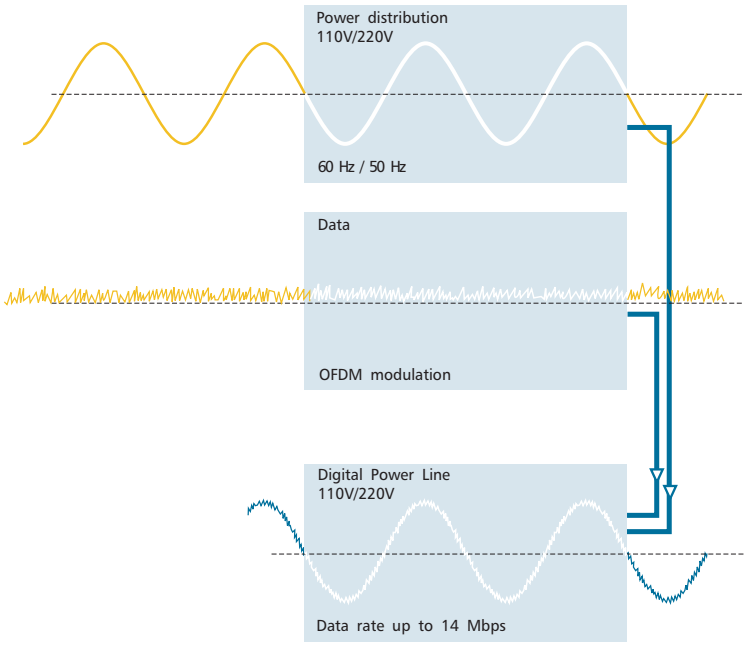
2005-08-18 ver.1

The content of this document is furnished for informational use only, it is subject to change without notice, and it does not represent a commitment on the part of Corinex Communications Corp.

Corinex
Open Powerline Management

Over the last few years, Multi Service Operators (MSOs) have upgraded their access networks to a high bandwidth communication infrastructure to offer Internet, streaming video, interactive Digital TV, online gaming and entertainment services for their customers. These new services allow to restructure the potential revenue per each subscriber easily and increase the flat revenues from Internet, basic TV and voice access services. The operators who are targeting the residential and small business market gain now a new opportunity to capitalize upon their market position by employing technologies that allow them a total control of the infrastructure all the way from the access up to the last device in the network.





Powerline Communications

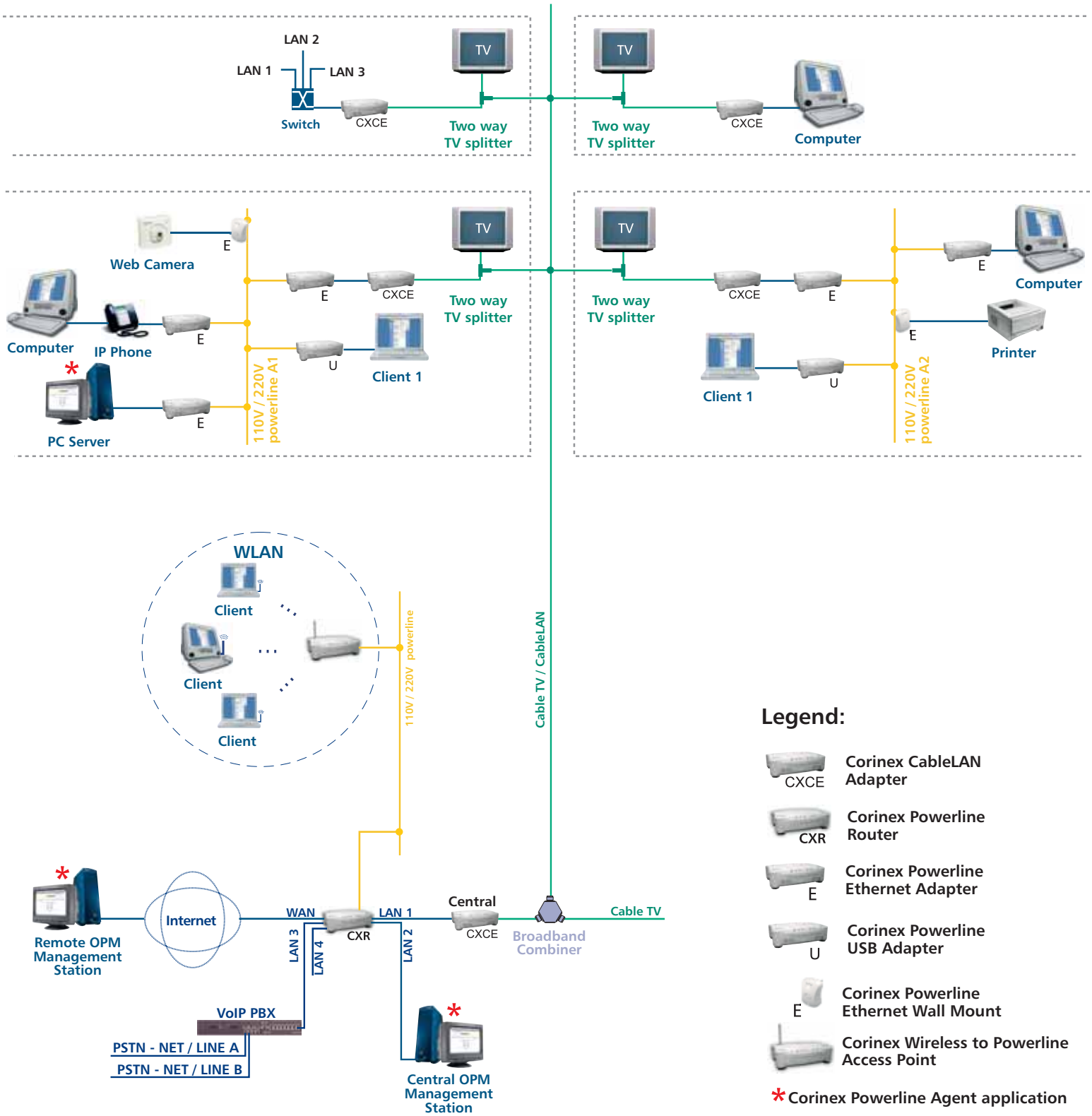
Corinex Powerline products (USB, Ethernet, Wall Mount, Router and Wireless) are designed to use existing AC electrical wiring within the home as a networking physical medium. Robust performance in the electrical noisy power line channel is enabled by the use of the Orthogonal Frequency Division Multiplexing (OFDM) technology. This multi-carrier modulation scheme allows devices to dynamically "surf the channel" - instantly shifting data from one carrier to another as noise and attenuation conditions change. The OFDM technology finds the low noise, low attenuation portions of the spectrum available to it and continues data transmission.

Corinex Powerline products have been optimized for high-reliability networking applications. Internet and network access is available through every power outlet in the home or office. Corinex's HomePlug certified Powerline networking technology supports up to 14 Mbps data rates. Corinex Powerline adapters are certified by and compliant with the HomePlug Powerline Alliance Industry Specification 1.0.1. This ensures interoperability with other HomePlug devices. Powerline technology provides a high quality of service for the adapters to ensure secure, reliable channels for transferring files, streaming audio, video, or voice data and even online gaming.

What Can a Corinex Open Powerline Management Provide?

Corinex Open Powerline Management (OPM) is a powerful and versatile network management software tool that allows the operator to configure, monitor and test all CableLAN and powerline devices across their entire network. Corinex Open Powerline Management is based on SNMP (Simple Network Management Protocol) - a standard protocol for enhanced management and testing of communication devices. The management is independent from any hardware configuration and as a worry-free system, designed for future network expansion with support for HomePlug standard certified powerline devices. A standalone management system for the Corinex CableLAN and powerline devices in the network is build into the Corinex SNMP platform.

The platform's flexibility allows the integration of any SNMP communication device upon demand easily. A very interesting aspect for service providers, who would like to manage their combined wireless, CableLAN and powerline network efficiently!



Legend:

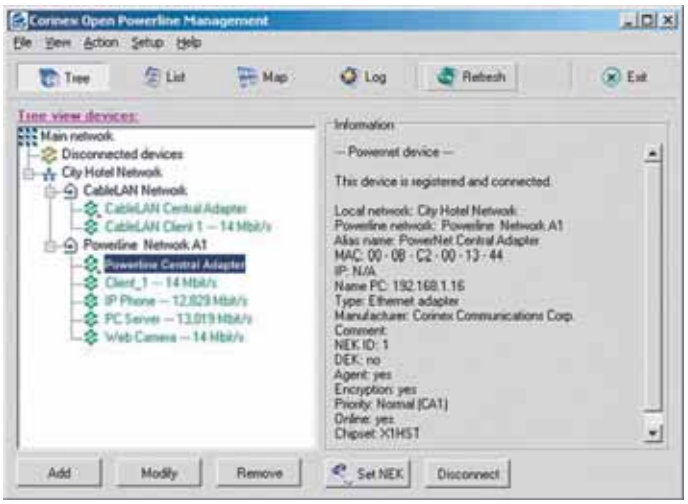
- CXCE — Corinex CableLAN Adapter
- CXR — Corinex Powerline Router
- E — Corinex Powerline Ethernet Adapter
- U — Corinex Powerline USB Adapter
- E — Corinex Powerline Ethernet Wall Mount
- Corinex Wireless to Powerline Access Point
- * Corinex Powerline Agent application

The Corinex Open Powerline Management is designed to manage the entirely new designed and enhanced Corinex Powerline and CableLAN products family, consisting of:

- Corinex Powerline Ethernet Adapter
- Corinex Powerline USB Adapter
- Corinex Powerline Ethernet Wall Mount
- Corinex Powerline Router
- Corinex Wireless to Powerline Access Point
- Corinex CableLAN Adapter

Product Features

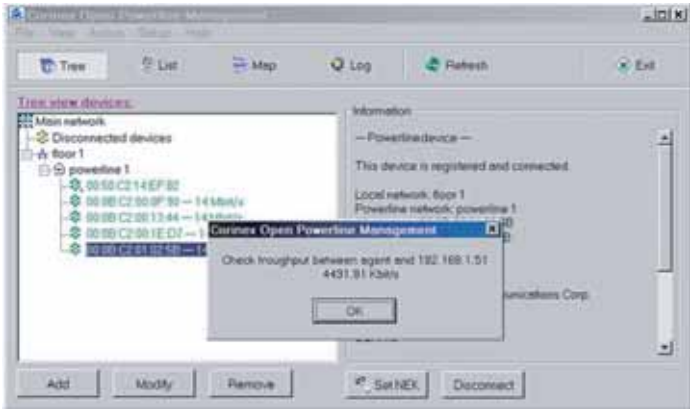
- **Seamless Management of Complex Networks over Long Distances**



Creating a Logical Structure of Networks

One Corinex Open Powerline Management enabled computer can act as a base station and collect management data from all other CableLAN and powerline network nodes efficiently. Each network can be managed by the OPM, either locally or remotely, as long as one computer or router in the network carries a Powerline Agent application responsible for the translation of encrypted SNMP commands. The OPM enabled computer uses SNMP commands to activate the agents to look for all CableLAN and powerline devices in their networks. This makes any customer's network completely manageable and delivers high flexibility. The network is easily remotely accessible by Operator's network administrator through the Internet.

- **High Usability and Manageability**



Real Throughput Measurement - Result

The OPM's wizard helps the administrator to create a logical structure of all managed networks and to define the Agent by exploring the network segment (to add or delete devices).

- **Powerline Network Testing Makes the Installation Easy and Effective**

Another very exciting feature of the management software is its ability to monitor and test the quality for all electrical outlets within a building before a powerline network installation!

This is a unique feature many service providers are looking for in combination with the ability to collect statistical data and having an event logging capability on hand. Corinex Powerline Agent implemented in a network enables the administrator to measure a maximum theoretical throughput level for each powerline device in the connection to the Agent's powerline device. The OPM allows measuring the real throughput between the Agent's device and any other device having assigned an IP address connected to the same network as the Agent's device.

The powerline management software offers also easy to use and intuitive graphical interfaces for all networking utilities and enables an easy and effective installation of CableLAN and Powerline communication equipment.

Operator's network administrator can change a customer's device security settings even remotely and is able to create secure networks for user groups. It is not possible to reach the operator service from the powerline or the CableLAN adapter without a unique password dedicated by the operator to the adapters.

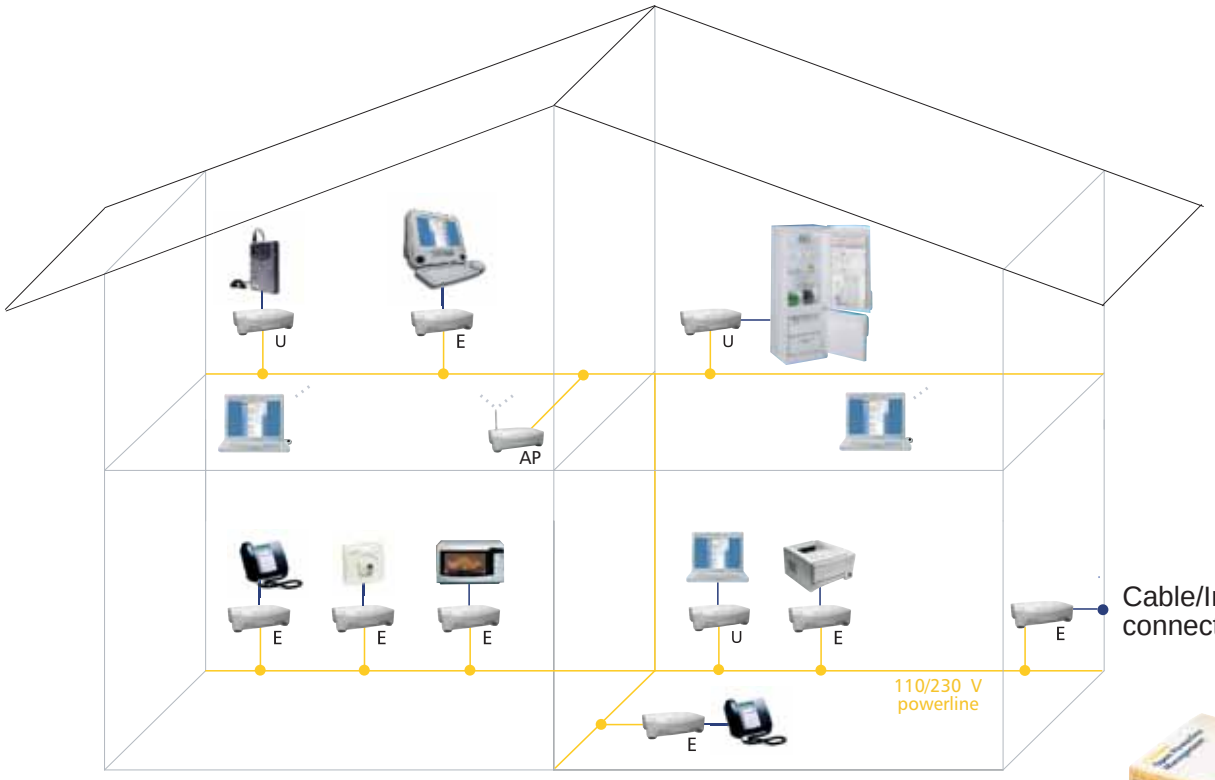
- **Remote Password Management**

A password management enables the operator to choose which CableLAN or powerline device will be allowed to access the service. An installation for connectivity of any additional device (for example if bought in a retail channel) requires an interaction between the user and the operator. The Operator is immediately in control and can change a customer password without her/his knowledge or approval - in accordance with a potential service agreement in place.

Adding Powerline Device - Powerline Agent Settings

- Creating a logical structure of networks
- 56 Bit DES link encryption with key management for secured communication
- GUI Interface for easy communication, running on Windows 98SE, 2000, NT, XP
- Managing Powerline Adapters, Corinex Wireless Access Points, Corinex Powerline Routers, CableLAN Adapters, disregarding on which OS is the attached host running
- SNMP platform compatibility
- Easy to use and install

Manage your Household Devices with Powerline



OPM

E Corinex Powerline Ethernet Adapter

U Corinex Powerline USB Adapter

AP Corinex Wireless to Powerline Access Point

MP3 Player

Web Camera

VoIP Phone

Notebook

Printer

Computer

Home Appliances

Powerline Connected Household - Future of Home Networking

Product Specifications

Product Code: CXM-OPM
Please refer to the Price List for the exact product code specification.

Product Content
- Installation CD
- Printed Manual

Technical Specifications

- Protocol Support:
  SNMP v.1, SNMP v.2, HomePlug 1.0.1
- GUI Operating System Support:
  Windows 98SE, 2000, ME, NT, XP
- Agent Operating System Support:
  Windows 98SE, 2000, ME, NT, XP, Linux

Corinex

HomePlug 14 Mbps CERTIFIED

Corinex Communications Corp.
World Trade Center
404-999 Canada Place
Vancouver, B.C.
Canada V6C 3E2
Tel: +1 - 604 - 692 0520
Fax: +1 - 604 - 694 0061
E-mail: global@corinex.com
http://www.corinex.com

Corinex Global, a.s.
Ruzova dolina 19
820 05 Bratislava
Slovak Republic
Tel.: +421 - 2 - 5021 4811
Fax: +421 - 2 - 5556 7309
E-mail: global@corinex.com

Corinex is a registered trademark of Corinex Communications Corp.
HomePlug® is a registered trademark of HomePlug® Powerline Alliance.

2003-10-20 ver.2

The content of this document is furnished for informational use only, it is subject to change without notice, and it does not represent a commitment on the part of Corinex Communications Corp.

Corinex

AV200 Powerline Ethernet Adapter

200Mbps over existing electrical wires!

The Corinex AV200 Powerline Ethernet Adapter is the world's first product that supports the distribution of video, voice, and broadband internet access over a premises existing electrical wires. With transfer rates of up to 200 Mbps, the Corinex AV200 Powerline Ethernet Adapter has ample bandwidth to stream several high quality video signals, such as HDTV, while simultaneously delivering high speed internet access thoughout an entire premise! The AV200 Powerline Product family consists of an Adapter, Router, ADSL2+ Wireless Gateway and a CableLAN adapter and CableLAN router for coaxial networking applications, all offering 200Mbps communications.

The AV200 Powerline technology by Corinex provides numerous networking possibilities with amazingly fast physical layer transfer rates up to 200 Mbps. Finally, real world multimedia network applications can be created without adding any new wiring, simply plug in a Corinex AV200 Powerline Ethernet Adapter and any computing device in the entire premise is ready to receive high bandwidth multimedia signals.

Application priority levels are retained, ensuring that applications with real-time requirements, such as VoIP, streaming video and multiplayer head-to-head games do not experience glitches, frame loss, or delays, even if other users in the network are downloading large files, websurfing or downloading or listening to MP3 songs.

The Corinex AV200 Powerline Ethernet Adapter allows users to create a high-speed local area network, without the need or new cabling. Users can connect the AV Powerline Ethernet Adapter to virtually any electrical socket in their home or office to create a link to the powerline network. The network can be connected to an internet gateway, such as an ADSL or cable modem, providing a convenient extension of the internet to the powerline within a premise.

Any ethernet-enabled device, such as a desktop computer, network printer, laptop computer, or a security camera connect to the AV200 powerline network.

There are two versions of the Corinex AV200 Powerline Ethernet Adapter. The Home Users Edition of the product is meant for home networking applications and simple plug and play installations. The Commercial Edition of the product is used for advanced networking applications, deployments in Multi dwelling Units and operators providing BPL Access.

Features

- 10/100BaseT Fast Ethernet interface
- Physical data rate in the powerline up to 200 Mbps with distances up to 300 m.
- Built-in repeating capabilities for increased coverage
- CSMA/CARP (Carrier Sense Multiple Access with Collision Avoidance and Resolution using Priorities) protocol
- Bridge Forwarding Table for 64 MAC Addresses
- 802.1Q VLAN & Optimized VLANs
- Powerful DES/3DES encryption
- OFDM technology and powerful error correction system allow robust performance under harsh conditions in the electrical network
- Integrated 802.1D Ethernet Bridge With Optimized Spanning Tree Protocol
- 8-level priority queues, with programmable priority-classification engine
- Priority classification according to 802.1P tags, IP coding (IPv4 or IPv6) or TCP source/destination ports
- Optimized support for broadcast and multicast traffic
- MAC filtering - can discard Ethernet frames if they come from a source MAC address which is not present in a list of allowed MAC addresses
- Configuration using an embedded web interface

Commercial Edition:

- Console Interface
- Dynamic IP Address with auto-config
- Manual MASTER / SLAVE configuration
- VLAN and OVLAN Support
- RADIUS server authentication support
- Programmable bandwidth allocation
- Master Node HE or Repeater
- Slave CPE Node
- Can be used for MV/LV BPL networks

Home User Edition:

- Web interface
- Fixed IP or DHCP
- Default IP 10.10.1.69
- The MASTER and SLAVE can be set manually or automatically
- VLAN tagging without filtering

Technical Specifications

Standards Compliance	IEEE 802.3u
Speed	Up to 200 Mbps on physical layer
AC Plug Type	US, EU, UK and AUS
LED Status Lights	Power on, PLC Link/Activity Ethernet link
Interface	10/100BaseT Fast Ethernet, Powerline
Frequency Range used	2 – 34 MHz
Power Input	85 to 265 V AC, 50/60 Hz
Dimensions	148 mm L x 106 mm W x 47 mm H 5.82" L x 4.17" W x 1.85" H
Weight	0.28 kg (0.61 lb)
Transmitted Power spectral density	-56 dBm/Hz
Power Consumption	10 W
Safety & EMI	FCC Part 15, EN 55022 EMC limits
Operating Temperature	0° to 50°C (32°F to 122°F)
Operating Humidity	10% to 80% non-condensing

Standards

- 802.3u
- 802.1P
- 802.1Q
- Compliant with FCC Part 15, EN 55022 EMC limits

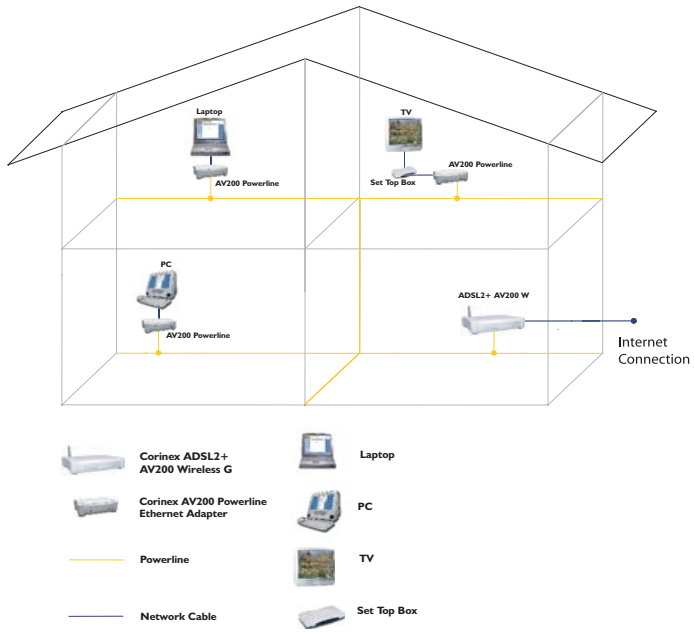
Package Content

- Corinex AV200 Powerline Ethernet Adapter
- One straight-forward CAT5 ethernet cable
- One AC power cable
- CD with documentation
- Printed Quick Start Guide

Product Codes:

Corinex AV200 Powerline Ethernet Adapter

CXP-AV200-ETH - Home Edition
CXP-AV200-ETHC - Commercial Edition



UPA UNIVERSAL POWERLINE ASSOCIATION

Product features and design may vary by version and region.

Corinex Communications Corp.
#670 - 789 West Pender Street
Vancouver, BC
Canada V6C 1H2
Tel: +1 - 604 - 692 0520
Fax: +1 - 604 - 694 0061
E-mail: global@corinex.com
http://www.corinex.com

Corinex Global, a.s.
Ruzova dolina 19
821 08 Bratislava
Slovak Republic
Tel.: +421 - 2 - 5021 4811
Fax: +421 - 2 - 5556 7309
E-mail: global@corinex.com

Corinex is a registered trademark of Corinex Communications Corp.

2006-02-08 ver.3

The content of this document is furnished for informational use only, it is subject to change without notice, and it does not represent a commitment on the part of Corinex Communications Corp.

Corinex
Internet Phone with Headset

Corinex

Manual

Este Documento, y el software descrito en ella es ofrecida bajo licencia y pueden ser utilizadas y copiadas de acuerdo con las condiciones de esta licencia. El contenido de este documento es para fines informativos solamente, y pueden cambiar sin previo aviso, y no representa una promesa o contrato de parte de Corinex Communications Corp.

Corinex Communication Corp no se responsabiliza por cualquier error y incongruencias que puedan aparecer en este documento.

Es nuestra política mejorar nuestros productos, a medida de que la tecnología, el hardware, el software y el firmware sean mejorados. Por lo tanto, la información en este documento puede cambiar sin previo aviso.

Puede ser que algunas funciones, y operaciones descrito en este documento no sean disponible en cierto países donde este producto es vendido, debido a regulaciones locales y políticas de mercadeo.

La manera usar el producto y las funciones mencionadas en este documento pueden ser restringidas y reguladas por la ley en algunos países. Si, UD no esta seguro de las restricciones y regulaciones aplicables en su región, consulte con la oficina de Corinex más cercano, o a su proveedor más cercano.
Publicado por:

Corinex Communications Corp.
#670-789 West Pender Street
Vancouver, B.C.
Canadá V6C 1H2
Tel.: +1 604 692 0520
Fax: +1 604 694 0061

Corinex es una marca registrada de Corinex Communications Corp.

Microsoft, MS-DOS, MS, Windows son marcas registradas propiedad de Microsoft Corporation en los EE.UU., y/o otros países.

Todos los productos y los nombres de las compañías mencionadas aquí son propiedad de sus respectivos dueños.

Derechos reservados (c) 2001-2005 Corinex Communications Corp.

2005-01-11 ver 1.1

CORINEX COMMUNICATIONS CORPORATION

Acuerdo de licencia para usuario final

Este acuerdo de licencia para usuario final ("EULA") es un acuerdo legal entre usted y CORINEX COMMUNICATIONS CORPORATION ("CORINEX") con respecto al software con derechos de autor ("copyright") proporcionado con este EULA.

El uso de cualquier software y documentación relacionada ("Software") suministrado con un producto de hardware de CORINEX, o puesto a su disposición mediante descarga o de otro modo por CORINEX en cualquier forma o medios, constituirá su aceptación de estos términos, a menos que se proporcionen términos separados por parte del proveedor de software, en cuyo caso pueden ser aplicables términos adicionales o diferentes. Si no está de acuerdo con los términos de este EULA, no descargue, instale, copie o utilice el Software.

1. Otorgamiento de licencia. CORINEX le otorga un derecho personal, intransferible y no exclusivo para utilizar la copia del Software proporcionado con este EULA. Usted conviene en que no copiará el Software excepto como sea necesario para utilizarlo en un solo sistema del producto de hardware. Usted conviene en que usted no puede copiar los materiales escritos que acompañan al Software. El modificar, traducir, alquilar, copiar, transferir o asignar la totalidad o partes del Software, o cualesquier derechos otorgados a continuación, a cualquier otras personas, y quitar cualesquier avisos, etiquetas o marcas propietarios del Software está estrictamente prohibido. Además, usted está de acuerdo por este medio de no crear trabajos derivados basados en el Software. Usted puede transferir permanentemente todas sus derechos bajo este EULA, dado que no retenga copias, transfiera todo el software, y el recipiente convenga con los términos de este EULA. Si el Software es una mejora, cualquier transferencia debe incluir todas las versiones anteriores del Software.

2. Copyright. El Software es entregado bajo licencia, no vendido. Usted reconoce que no se le transfiere ningún derecho a la propiedad intelectual en el Software. Usted reconoce además que el título y las derechos completos de propiedad del Software seguirán siendo la propiedad exclusiva de Corinex Communications Corporation y/o sus proveedores, y usted no adquirirá ningún derecho al Software, excepto según lo expresamente dispuesto con anterioridad en este documento. Todas las copias del software contendrán los mismos avisos de propiedad según lo contenido en o sobre el Software.

3. Ingeniería inversa. Usted conviene en que usted no procurará, y si usted es una corporación, utilizará sus mejores esfuerzos para prevenir que sus empleados y contratistas intenten compilar en forma inversa, modificar, traducir o desensamblar el Software en su totalidad o parcialmente. Cualquier falla en el cumplimiento de los antedichos o de cualesquier otros de términos y condiciones aquí contenidos dará lugar a la terminación automática de esta licencia y a la reversión a CORINEX de los derechos concedidos abajo .

4. Denegación de responsabilidad sobre la garantía. El Software es suministrado "COMO ESTÁ" sin garantía de ninguna clase. CORINEX y sus proveedores declinan y no ofrecen ninguna garantía expresa o implícita y específicamente niegan las garantías de capacidad de ser mercadeado, aptitud para un propósito particular y no infracción de los derechos de terceros. La totalidad del riesgo en cuanto a la calidad y el funcionamiento del Software está a su cargo. Ni CORINEX ni sus proveedores garantizan que las funciones contenidas en el Software cumplirán con sus requisitos o que la operación del software será in-interrumpida o libre de errores.

5. Limitación de responsabilidad. La responsabilidad total de Corinex y su remedio exclusivo bajo este EULA no excederán el precio pagado por el Software, si lo hay. En ningún evento CORINEX o sus proveedores serán responsables ante usted por daños consecuentes, especiales, fortuitos o indirectos de ninguna clase resultantes del uso o de la inhabilidad de utilizar el software, aún si CORINEX o su proveedor han sido notificados acerca de la posibilidad de tales daños, o cualquier reclamo por parte de un tercero.

6. Leyes aplicables. Este EULA se regirá por los leyes del Canadá, excepto su conflicto con las disposiciones legales.

7. Leyes sobre exportación. Este EULA involucra productos y/o datos técnicos que pueden estar controlados bajo cualesquier leyes y regulaciones sobre control de la exportación aplicables, y puede estar sujeto a cualquier aprobación requerida bajo tales leyes y regulaciones.

8. Precedencia. Con la excepción de lo precisado arriba, donde se proporcionen términos separados por parte del proveedor de software, entonces, conforme a este EULA, esos términos también se aplican y prevalecen, al alcance de cualquier inconsistencia con este EULA.

CORINEX COMMUNICATIONS CORPORATION

USO DE CORINEX MULTIMEDIA HEADSET

1. Conecte los enchufes de los audífonos estéreos y del micrófono en el receptáculo “line-out” o “audio-out” y en el receptáculo para micrófono, respectivamente, en la tarjeta de sonido de su computador. También es posible conectar los audífonos a otros dispositivos de audio, tales como un reproductor de CD. En ese caso, conecte solamente el enchufe del auricular estéreo en el receptáculo del dispositivo de audio.

2. Desactive el volumen en la caja de control antes de activar la fuente de audio. Después de activar la fuente de audio, ajuste el volumen según sea necesario.

3. Coloque los audífonos sobre su cabeza y disponga la banda para que se ajuste a su cabeza. Ajuste el tubo del micrófono para que quede cerca de su boca. Encienda el interruptor del micrófono cuando lo vaya a utilizar.

PARA USUARIOS SKYPE VAYA AL PASO 1
PARA USUARIOS DIFERENTES A SKYPE (O SI NO ESTÁ SEGURO) VAYA AL PASO 2.

1. **Skype (Llamadas PC a PC gratuitas para usuarios Skype; llamadas Premium PC a Teléfono)**
   Diríjase a la página de Internet **www.skype.com** Regístrese siguiendo las instrucciones en la página de la web. Descargue e instale el software Skype. En el panel frontal Skype, seleccione **Archivo->Opciones ->Microteléfono/Auricular** (File->Options->Hand/Headset) y seleccione su tarjeta de sonido interna (internal sound card) que aparecerá en todos los tres menús desplegables. Ahora, Corinex Multimedia Headset pueden ser usados como un dispositivo de entrada/salida con Skype. Usted necesita el software Skype para marcar un número. No es necesario ningún paso adicional para utilizar el servicio Skype. (Para más detalles, vea la sección 2.3.)

SE HA COMPLETADO LA INSTALACIÓN DE USUARIO SKYPE

2. Inserte el CD ROM incluido en la unidad de CD ROM. En el menú que aparece automáticamente, haga clic en **Instalar Corinex Softphone**, elija un lenguaje en el menú desplegable y haga clic en **Instalar** para iniciar la instalación. Siga las instrucciones que le indica el Asistente de Configuración. Cuando sea requerido, ingrese el número de serie que está impreso en la estuche del CD. (Para más detalles, vea la sección 3.3.)

3. **Registrarse con un proveedor de servicios:**
   Para registrarse con un proveedor de servicios Voice Over IP, siga las instrucciones en la pagina web del proveedor de servicios. Dependiendo del proveedor de servicios se tendrá que instalar diferente software y configuraciones requeridas para usar el servicio. Tenga en cuenta que la mayoría de los proveedores de servicios requieren que abran una cuenta con ellos para usar los servicios. E instrucciones de cómo abrir una cuenta le podrá ser enviadas a su correo electrónico.

Este es un ejemplo de cómo se puede registrar con un proveedor de servicios, Free World Dialup, otros proveedores de servicios pueden ser similares.

Abra su Browser y vaya a la dirección web: **www.freeworlddialup.com**

Para iniciar el proceso de registro presione en **Get FWD!** en el lado derecho y la siguiente pantalla aparecerá:

Seleccione **Sign up** link. Y en la próxima pantalla le pedirá su información personal.

Escriba la información pedida en los espacios correspondientes, y presione en **Next** (Siguiente). Después el proveedor de servicios le enviara a su correo electrónicos su numero de usuario y su contraseña. Y así ya estará registrado con este servicio.

4. Inicie el Softphone software, La cual lo encontrara en su menú de programas en **Inicio->Programas ->Corinex->Softphone**. Cuando el Software este corriendo por primera vez, el asistente de instalación lo ayudara a configurar el software. Seleccione el protocolo SIP y presione en **Siguiente**. En la lista de proveedores de servicios, seleccione Free World Dialup y presione en **Siguiente**, y escribe su FWD number en el espacio de **Su Numero** Y su **Contraseña** la cual fue dada por el proveedor de servicios al registrarse con ellos presione en **Siguiente** y después en **Aceptar** para concluir la configuración.

Nota: El Asistente de Configuración puede ser iniciado en cualquier momento para agregar otro proveedor de servicios. Presione en el botón de **Inicial asistente** (Start wizard) en el menú de Cuenta.

5. Corinex Softphone se conectara a Free World Dialup. Después de haber configurado su software y registrado con el proveedor de servicios. Este nombre aparecerá en la ventana del Softphone. Ahora podrá usar su audífonos multimedia y su Softphone para hacer llamadas por la Internet con voz simultáneamente!

6. Para probar si su cuenta y software están funcionando correctamente con su proveedor de servicios. Lo puede hacer marcando los números mencionados a continuación, la cual puede ser marcados por medio de su teclado o su interfase en el Softphone, si es por Free World Dialup:

Free World Dial Up	Marque
Probador de Eco	613
Servicio del tiempo	612
Servicio de Información “Tellme”	411

Visite **www.corinex.com** para bajar las ultimas versiones y obtener mas información sobre sus dispositivos.

Índicie

1 Introducción

1.1 Generalidades

Con el *Corinex Internet Phone with Headset*, los usuarios pueden hacer llamadas vía el Internet y ahorrar en costos de llamada a larga distancia e internacional. La instalación es tan fácil como insertar los audífonos en los receptáculos de entrada y de salida de su tarjeta de sonido, sin necesidad de controladores. Los audífonos se pueden utilizar con NetMeeting, Skype y otras aplicaciones de "softphone" basadas en PC. *Corinex Multimedia Headset* vienen con diseño aerodinámico y de moda y ofrecen un control de volumen.

El software gratis de Softphone de Corinex está incluido en el CD de instalación que es compatible con Windows 98SE/ME/2000/XP. Soporta servicios gratis de VoIP en Internet tales como Free World Dialup o SIPphone, y se puede configurar para trabajar con cualquier servicio de VoIP que dé soporte a los protocolos SIP versión 2.0 y H.323 versión 4, para hacer llamadas de PC a PC y de PC a teléfono.

1.2 Contenido del paquete

Cuando reciba su *Corinex Internet Phone with Headset*, compruebe que su paquete contiene:

- *Corinex Multimedia Headset*
- CD de instalación que contiene el software y este manual
- Guía rápida impresa

Características de los audífonos

- Operan con NetMeeting, Skype, Hicall, software de "softphone" basado en PC
- Funcionan con cualquier software de grabación / reproducción de audio
- Control de volumen

Características del Softphone

- Cumple con los protocolos SIP versión 2.0 y H.323 versión 4
- Permite múltiples codecs para VoIP (G711, G721 y GSM)
- CD de instalación con la posibilidad de elegir entre múltiples proveedores de servicio (Free World Dialup o SIPphone)
- Registro de llamadas (llamadas salientes, entrantes y perdidas)

- Directorio telefónico
- Diferentes skins

Como innovamos constantemente nuestros productos, puede suceder que tengamos versiones de las herramientas de software y de la documentación más recientes que las incluidas en el CD de instalación. Si usted desea verificar (y descargar) las últimas versiones para su producto de Corinex, vaya a www.corinex.com

1.3 Requerimientos del sistema

- PC compatible con IBM con una tarjeta de sonido
- Sistema operativo Microsoft Windows 98SE/ME/2000/XP
- DirectX 8.1 (o versión más reciente)
- Proxy HTTP inhabilitado en la configuración de conexión a red

2 Para usar el Internet Phone with Headset

Usted puede utilizar el *Corinex Internet Phone with Headset* de tres maneras:

1. Como dispositivo de entrada salida de audio conjuntamente con cualquier software que permita grabación o reproducción de audio. Esto incluye reproductores de música y vídeo, editores de sonido y otro software.
2. Como dispositivo de entrada salida de audio conjuntamente con software común de terceros que permita comunicación de voz (Ver capítulos 2.2, 2.3)
3. Como dispositivo de entrada salida de audio conjuntamente con el software para Softphone de Corinex incluido en el CD, el cual le permite usar servicios de VoIP de diferentes proveedores (ver capítulo 3.)

La siguiente imagen muestra la descripción física de sus audífonos:

2.1 Instalación de hardware

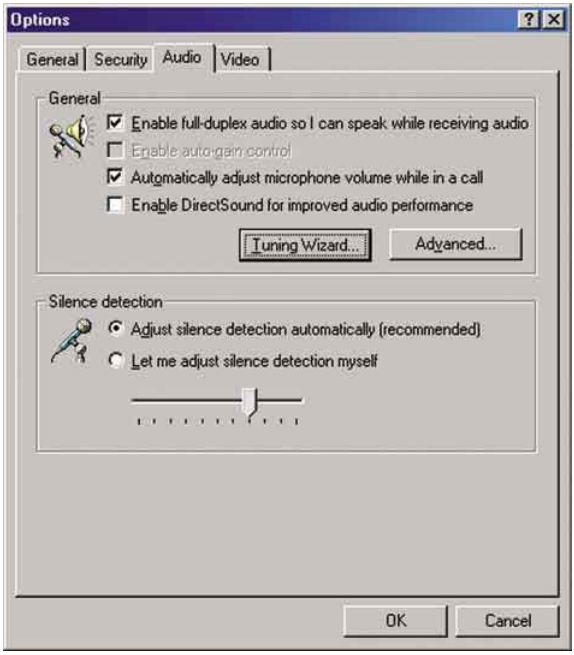
Esta sección bosqueja cómo conectar su *Corinex Multimedia Headset* con su computador. La instalación es muy simple, todo lo que usted necesita hacer es conectar el cable de los audífonos con los receptáculos de entrada y de salida de su tarjeta de sonido.

Ahora los audífonos están listos para ser usados con el software que escoja. Para comenzar a usar el teléfono con NetMeeting o Skype, refiérase por favor al capítulo siguiente. Si quiere usar el teléfono con el software para Softphone de Corinex (incluido en el CD) y el proveedor de servicio de VoIP de su elección, proceda al capítulo 3.

2.2 Para usar los audífonos con NetMeeting

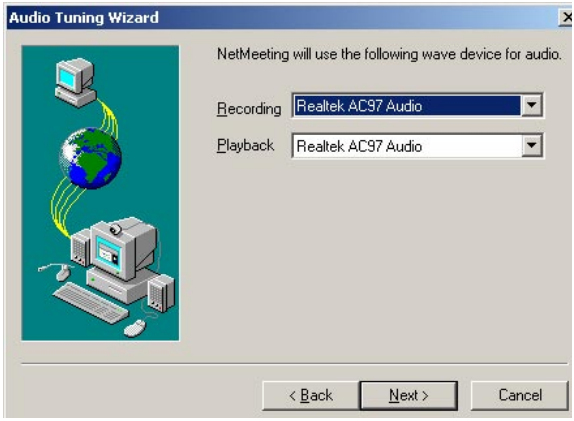
Después de insertar los audífonos en su computador, usted puede utilizarlos con Microsoft NetMeeting. Todo lo que usted tiene que hacer es configurar NetMeeting para utilizar el tarjeta de sonido interna como dispositivo de salida / entrada. Siga por favor los pasos siguientes:

1. Inicie NetMeeting y haga clic en **Herramientas** (Tools) -> **Opciones** (Options). Luego, vaya a la pestaña de **Audio**.



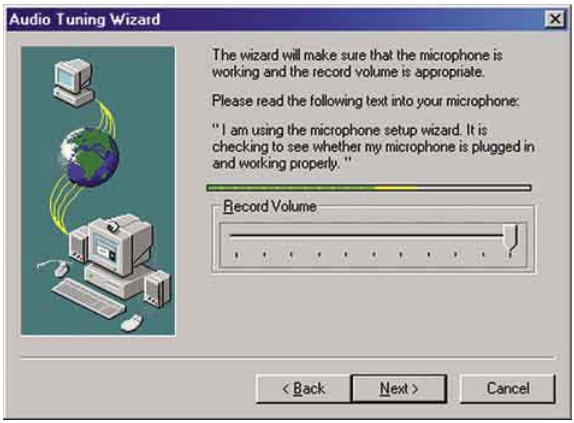
2. Haga clic en **Asistente para Afinación** (Tuning Wizard). Aparecerá la ventana siguiente.

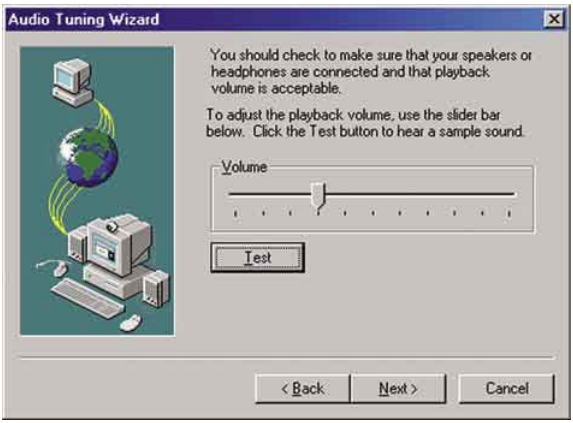
Haga clic en **Siguiente** (Next) para continuar a la pantalla siguiente.



3. Aquí usted puede seleccionar el dispositivo de audio para entrada / salida. Seleccione por favor el nombre de su tarjeta de sonido y haga clic en **Siguiente** (Next).

4. En las dos pantallas siguientes usted puede ajustar el volumen para reproducción y grabación.



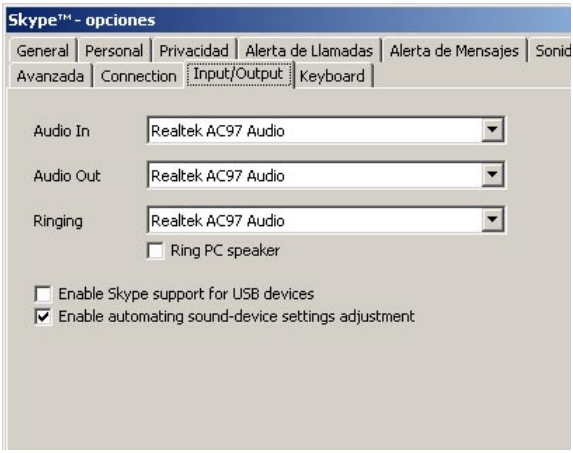


Después de esta configuración, haga clic en **Siguiente** (Next) y termine con el asistente para configuración. Ahora el software de NetMeeting está configurado para utilizar *Corinex Multimedia Headset* para hacer y recibir llamadas de voz.

2.3 Para usar los audífonos con Skype

Después de instalar el teléfono (sección 2.1), este se puede usar con el programa de Skype que es gratuito (**www.skype.com**), así podrá comunicarse por medio de voz. Para configurarlo con Skype inicie el programa y siga los siguiente pasos:

1. Presione **File** (Archivo) -> **Options** (Opciones) y dirijase para **Hand/Headsets** (Audiófonos).



2. En esta pantalla usted puede ver tres configuraciones para el dispositivo de sonido. Por favor coloque en Entrada de audio (Audio in), Salida de audio (Audio out) y Repique (Ringing) el nombre de su tarjeta de sonido.

3. Haga clic en **Guardar** (Save) para validar la configuración modificada. Ahora Skype está listo para ser utilizado con *Corinex Multimedia Headset*.

3 Para usar los audífonos con Softphone de Corinex

El *Corinex Internet Phone with Headset* viene con un CD incluyendo el software de Softphone de Corinex que le permite utilizar los servicios de VoIP de diversos proveedores. Para utilizarlo, usted tiene que registrarse primero con un proveedor y así conseguir la información de acceso necesaria para comenzar a hacer llamadas telefónicas. Refiérase por favor a los capítulos siguientes para aprender cómo lograrlo.

3.1 Usando el teléfono con los operadores SIP gratis predefinidos

Para su conveniencia, el Softphone de Corinex contiene las configuraciones para algunos operadores predefinidos: Ecuity, Free World Dialup, SIP Phone y VoIP Talk. Las siguientes secciones describen como registrarse para una cuenta de VoIP.

3.1.1 Free World Dialup

Abra su aplicación para navegación por Internet y vaya al sitio Web http://www.freeworlddialup.com.

Para comenzar el proceso de registro, haga clic sobre el botón rojo **Get FWD!** al lado derecho. Aparecerá la pantalla siguiente:

Ahora haga clic en el vínculo Registrarse (**Sign up**). La siguiente pantalla pedirá su información personal.

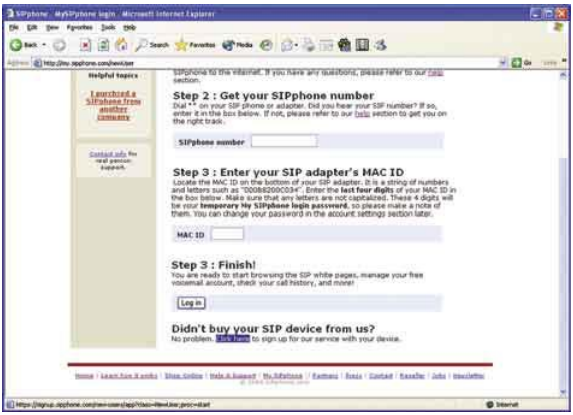
Complete los campos con su información personal y continúe con el botón Siguiente (**Next**). Después de esto, su número de usuario (número FWD) y contraseña serán enviados a su dirección de correo electrónico. Para empezar a usar el servicio para el cual se ha registrado proceda a la sección 3.3.

3.1.2 SIP Phone

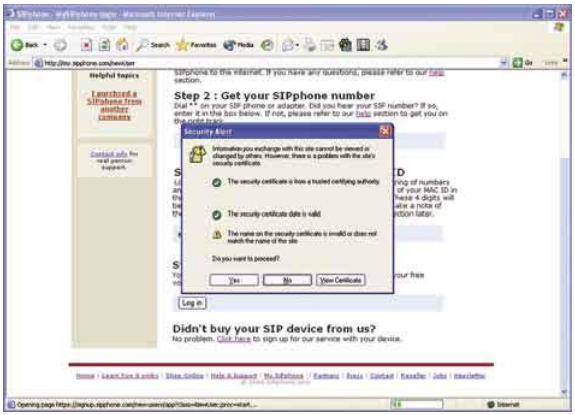
Abra su aplicación para navegación por Internet y vaya al sitio Web **http://www.sipphone.com**. Luego haga clic en el vínculo Mi SIPphone (**My SIPphone**).

Ahora haga clic en el vínculo Registrarse (**Sign up**) en la mitad del texto.

El vínculo apropiado para continuar está localizado en la parte de debajo de la página Web. Haga clic sobre él **Click here**.



Puede aparecer una alerta de seguridad. Para continuar, haga clic en el botón **Sí** (Yes).



Luego llene los campos con su información personal y haga clic sobre el botón **Registrarse** (Register).

Después de esto, su número de usuario (número SIP / nombre de usuario y contraseña serán enviados a su dirección de correo electrónico. Para empezar a usar el servicio para el cual se ha registrado proceda a la sección 3.3.

3.2 Usando el teléfono con los operadores H.323 gratis predefinidos

La mayoría de los operadores de VoIP H.323 cobran por sus servicios en momento de la impresión de este documento.No se dispone actualmente de ninguna configuración predefinida para VoIP libre usando H.323 .Para configurar el Softphone para usarse con un proveedor de servicio de VoIP H.323, por favor refiérase a la sección 3.3 para instalación del software y a la sección 4 para la configuración del Softphone.

3.3 Instalación de software

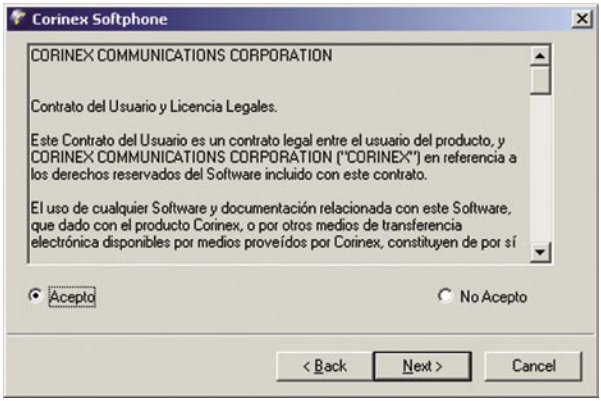
Para poder utilizar el Corinex Internet Phone with Headset con servicios de VoIP de diversos operadores, primero tiene que instalar el cliente de Softphone de Corinex.

1. Inserte el CD de la instalación, esta debe comenzar automáticamente. Si no, inicie la aplicación seleccionando **Mi computador** (My Computer), encontrado generalmente en la pantalla de inicio del computador de escritorio o portátil. Navegue hasta llegar a la **Unidad de CD** (CD drive), y haga doble clic sobre la unidad. Debe aparecer la siguiente pantalla:

2. Para leer la documentación (este manual), escoja **Leer Documentación** (Read documentation).

3. Haga clic sobre **Instalar Corinex Softphone** (Install Corinex Softphone) para comenzar el proceso de la instalación. Aparece la pantalla siguiente:

4. Haga clic en **Siguiente** (Next). En la pantalla siguiente, por favor lea el aviso sobre "copyright".



Haga clic sobre **Acepto** (I agree) para confirmar que usted ha leído y ha entendido el aviso sobre "copyright". Haga clic en **Siguiente** (Next) para continuar a la pantalla siguiente.

5. Para proceder con la instalación, ahora usted tiene que registrar el Softphone de Corinex. La pantalla siguiente muestra el diálogo para registro. Complete el número de serie, que está impreso en la estuche del CD. Haga clic en **Siguiente** (Next) para continuar.

Nota: Para instalar y ejecutar con éxito el software del Softphone de Corinex, por favor cerciórese de que el uso del HTTP proxy está inhabilitado en su computador (para información adicional vea por favor el manual de su sistema operativo o pregunte a su administrador de red local).

6. La pantalla siguiente le pregunta dónde instalar el *Softphone de Corinex*.

Haga clic en **Siguiente** (Next) para continuar.

7. Espere mientras el instalador copia todos los archivos a su disco duro y crea un acceso rápido en su escritorio. La información siguiente aparece después de una acertada instalación:

Una vez que el *Corinex Softphone* esté instalado en su computador, usted tiene que iniciarlo y realizar las configuraciones iniciales descritas en el capítulo siguiente.

4 Para usar el software Softphone de Corinex

4.1 Operación inicial del Softphone de Corinex

Cuando se ejecute el Softphone por primera vez, se iniciará automáticamente un asistente que le ayudará a ingresar la configuración correcta en el Softphone. El asistente puede ser ejecutado en cualquier momento presionando la barra **MENÚ->Inicial asistente** (Start wizard). Seleccione el protocolo que soporta su proveedor de servicio. El protocolo SIP es actualmente el más difundido entre los proveedores de servicio de telefonía de Internet gratuito. Presione **Siguiente** (Next). Si su proveedor de servicio VoIP está entre la lista que se muestra, seleccione el nombre del proveedor de servicio. Digite su número de usuario en el campo llamado **Su Nombre** (Your number) y su contraseña en el campo **Contraseña** (Password), tal como se los proporcionó su proveedor de servicio y presione **Siguiente** (Next). Presione **OK** para salir del asistente.

Si no puede encontrar su proveedor en la lista, seleccione las configuraciones personalizadas en la lista e ingrese toda la información proporcionada por su proveedor de VoIP en todos los campos en las pestañas **Cuenta** (Account) y **Conexión** (Connection). Esto incluye los datos de autenticación (su **número** (your number), **ID** (Login name) y **Contraseña** (Password), el servidor del **entorno** (realm) que se utiliza para la autenticación, direcciones del **proxy de SIP** (SIP Proxy) y servidores **STUN**.

Nota: Algunos proveedores (p.e. Ecuity) requieren información adicional para autenticación - el campo **ID** (Login name). En caso de que su abastecedor le dé un nombre de inicio de sesión, junto con el número y la contraseña, por ingréselo en el campo **ID** (Login name). De otra manera, usted puede dejar el campo vacío. Si usted utiliza un perfil predefinido para el proveedor, puede suceder que el campo de inicio de sesión esté sombreado sobre gris y usted no pueda editarlo. Esto significa que el proveedor no requiere esta información.

Nota: Por favor cerciórese que los campos **Dispositivo de Audio In** (Audio In Device) y **Dispositivo de Audio Out** (Audio Out Device) estén configurados de acuerdo con su tarjeta de sonido para utilizar los audífonos para comunicación.

Puede cambiar el proveedor de servicio en cualquier momento, haciendo clic en **MENÚ->Cambiar proveedor de servicios** (Change service provider). Resalte el nombre del proveedor de servicio (o ajustes personalizados). Si usted ha configurado la cuenta anteriormente, la configuración de su escogencia será cargada automáticamente en el Softphone y el teléfono estará listo para ser utilizado. De lo contrario, ejecute el asistente e ingrese sus nuevos detalles.

4.2 Configuración avanzada

Esta sección cubre la configuración del software Softphone de Corinex cuando se utiliza un enrutador para la conexión de la red al Internet. El enrutador debe ser configurado para pasar los paquetes de VoIP del computador del usuario hacia el Internet y viceversa. Hay una función en el enrutador llamada Transferencia desde puerto (Port Forwarding). Usted debe instalar esta función para abrir los puertos por defecto 5060 y 8000 a ser transferidos al computador con Softphone de Corinex.

Nota: Si hay más usuarios en la red utilizando el software de SIP, no pueden utilizar los mismos puertos SIP y RTP para las llamadas de VoIP. Si utilizan los mismos puertos, el enrutador no podrá reconocer a los usuarios y el software no trabajará correctamente. Por favor configure la transferencia de puerto para todos los usuarios.

Ejemplo:

-El usuario A tiene la dirección IP 192.168.0.2, el puerto SIP 5060 y el puerto RTP 8000
-El usuario B tiene la dirección IP 192.168.0.3, el puerto SIP 5061 y el puerto RTP 8001
-El enrutador debe remitir todos los paquetes UDP dirigidos a los puertos 5060 y 8000 a la dirección IP 192.168.0.2 y todos los paquetes UDP dirigidos a los puertos 5061 y 8001 a la dirección IP 192.168.0.3.

Después de realizar estas configuraciones haga clic en **Aplicar** (Apply). En el Softphone, aparecerá el mensaje siguiente mientras que el software está intentando registrarse con el proveedor de servicio de VoIP.

Después de un registro exitoso, será visualizado el nombre del proveedor de servicio, por ejemplo Free World Dialup, como se ve a continuación. Ahora el software está esperando su entrada, usando la interfaz en la pantalla.

Si el software no puede registrarse con el proveedor de VoIP elegido, mostrará uno de los mensajes de error siguientes

Mensaje del programa	Explicación
Error de conexion, identificador o contraseña equivocada (Registering problem, bad username or password)	El servidor de la autenticación rechazó su nombre de usuario / contraseña. Probablemente los ingresó incorrectamente. Por favor verifique la configuración.
Error de conexion o se pudo conectar (Registering problem, couldn't find registrar)	La aplicación no pudo encontrar un servidor de autenticación en la dirección que usted introdujo en las configuraciones. Por favor verifique la configuración.

4.3 Para usar el Softphone de Corinex

Después de configurar adecuadamente, usted debería ver la ventana principal con un gran despliegue y botones. Se puede tener acceso a todas las funciones del software usando esta ventana.

4.3.1 Presentación

Esta sección cubre la visualización del Softphone. La visualización tiene tres secciones, según lo visto en la imagen siguiente, usadas para visualizar diversos tipos de información.

La sección superior se utiliza para presenta información sobre el estatus de la conexión. Aquí usted puede ver el estatus del proceso del registro, el nombre del proveedor con el que usted está conectado, o los mensajes de error si hay un problema con la conexión con el proveedor de servicio de VoIP.

Mensaje del programa	Significado
Conectando… (Registering…)	El Softphone intenta conectarse con un proveedor de servicio de VoIP.
Error de conexion, identificador o contraseña equivocada (Registering problem, bad username or password)	El Softphone recibió un mensaje de error del proveedor, el cual no validó su nombre de usuario o contraseña. Por favor verifique su configuración.
Error de conexion o se pudo conectar (Registering problem, couldn't find registrar)	El Softphone no pudo encontrar una Pasarela (Gateway) de VoIP en la dirección que usted ingresó en el diálogo para la configuración. Por favor verifique su configuración.
[nombre del proveedor de servicio]	El Softphone está conectado y usted puede utilizar los servicios del proveedor de servicio de VoIP.

La línea del centro muestra información sobre las llamadas actuales - el número que está marcando, el número o el contacto al que está llamando o la duración de la llamada actual.

Mensaje	Significado
[número que está marcando]	Si usted marca un número usando el teclado del computador o los botones del Softphone, se muestra el número.

[número / apodo] está llamando ([number/ nickname] is calling)	Alguien intenta llamarle. Si usted no tiene este número en su directorio telefónico, sólo se está mostrando el número o el apodo. Si usted tiene este número en su directorio telefónico, se está mostrando el nombre del directorio telefónico.
[tiempo visualizado]	Información sobre la duración de la llamada actual.
Aguardar (Hold)	La llamada fue puesta en espera por su interlocutor.

La línea inferior muestra información sobre el estatus del Softphone y mensajes de sistema del proveedor del servicio VoIP.

Mensaje	Significado
Reiniciar (Reset)	El módulo SIP fue reiniciado. Todos los mensajes del servidor fueron suprimidos y si había una llamada en curso, fue cancelada. Este mensaje desaparece después de algunos segundos.
Tiempo Fuera (Time out)	Su última petición pasada al servidor fue cancelada por tiempo y fue exitosa.
Conexión cancelada por el peer (Connection cancelled by peer)	El servidor proxy del SIP devolvió un mensaje de CANCELACIÓN (CANCEL). Probablemente hubo un error de comunicación o error interno del proxy.
La llamada fue rezechada (Call wasn't accepted)	El corresponsal marcado rechazó su llamada.
Destino inconcluso (Unresolvable destination)	El número marcado no existe.
Ocupado (Busy)	El número que usted está marcando está ocupado. Junto con este mensaje, usted oirá un tono de ocupado en el altavoz de los audífonos.

Conectado [codec] (Connected [codec])	Cuando hace una llamada se vera el codec usado para esta llamada.
Colgando (Hanging up)	El programa esta enviando una señal para finalizar la llamada.
Colgado (Hung up)	llamada fue finalizada.

Nota: Si el corresponsal marcado no permite el códec que usted ha seleccionado en la configuración, el códec será cambiado automáticamente a uno permitido.

4.3.2 Controles del teléfono

Esta sección explica las funciones de los botones en el interfaz del Softphone.

1. Al hacer clic en el botón de **Ayuda** (Help) (signo de interrogación) iniciará su navegador por Internet y le llevará a la página de la ayuda en línea para el teléfono para Internet de Corinex con audífonos, en el cual puede ser encontrado en **http://www.corinex.com/voip/help**

2. Al hacer clic en el botón **Reducir** (Minimize) reduce al mínimo la aplicación a la bandeja del sistema. Puede ser restaurado haciendo doble clic sobre el **ícono de Softphone** en la bandeja del sistema, o haciendo clic derecho sobre el ícono y seleccionando **Restaurar** (Restore) en el menú contextual que aparece al lado del ícono. Para cerrar la aplicación, oprima **ALT-F4** o seleccione **Salir** (Exit) len el menú contextual.

3. En el lado izquierdo de la presentación usted puede ver la configuración del nivel del micrófono. La sensibilidad del micrófono puede ser ajustada haciendo clic en + ó -.

4. En el lado derecho de la presentación usted puede ver la configuración del volumen del altavoz del teléfono. El volumen del altavoz del teléfono puede ser ajustado haciendo clic en + ó en -. El volumen del altavoz se puede también ajustar con el control de volumen de los audífonos.

5. El botón **Llamar** (Dial) se utiliza para marcar un número después de ingresarlo o de seleccionar un contacto del directorio telefónico. También se utiliza para recibir llamadas, tener acceso a los registros de llamada y marcar un número desde allí. La siguiente tabla muestra la función asignada al botón de **Llamar** en diferentes situaciones.

Estado del Softphone	Funcionalidad del botón de Llamar
Modo en espera	Abre el registro de llamadas con las llamadas últimas marcadas, recibidas y perdidas
Cuando alguien le llama	Acepte la llamada
En el registro de llamadas	Marca el número que se seleccione
En el directorio telefónico	Marca el contacto que se seleccione

6. El botón de **Cancelar** (Cancel) tiene múltiples significados según el estatus de la aplicación. Para los detalles vea por favor la tabla siguiente.

Estado del Softphone	Funcionalidad del botón de Cancelar
Modo en espera	Reiniciar módulo SIP
Al ingresar un número	Suprime el último carácter pulsado
Cuando alguien le llama	Rechaza la llamada
Durante la llamada	Finaliza la llamada
En el registro de llamadas o directorio telefónico	Vuelve al modo de espera

7. El botón de **Menú** abre el diálogo de configuración.
8. El botón con el símbolo del libro abre el directorio telefónico.
9. El teclado numérico se utiliza para pulsar un número, cuando se está en el modo de espera.

NOTA: Usted también puede utilizar el teclado del computador para pulsar los números al marcar.

4.3.3 Para hacer una llamada de VoIP

Para llamar a un número

La manera más simple de hacer una llamada es pulsar el número usando el teclado numérico del teléfono y oprimiendo el botón verde **Llamar** (Dial). El programa enviará una petición de la llamada al proveedor. Si su corresponsal está en línea y listo para aceptar llamadas, usted verá un mensaje de **Llamando…** (Dialing…) en la visualización y oirá un tono en el altavoz del teléfono. Si su corresponsal está ocupado, usted recibirá un mensaje relacionado en la visualización y oirá un tono de ocupado en el auricular Si su corresponsal no está en línea, habrá una conexión inmediata por aproximadamente 3 segundos y la llamada será cancelada. Si usted desea cancelar la marcación, oprima el botón **Cancelar** (Cancel).

Para terminar una llamada
En cualquier momento durante una llamada, usted puede presionar el botón rojo de **Cancelar** (Cancel) para terminar la llamada

Para aceptar o rechazar una llamada
Si alguien intenta llamarle, el teléfono empieza a sonar y el apodo o el número de la persona aparecerán en la visualización. Usted puede aceptar la llamada presionando el botón **Llamar** (Dial) o rechazar la llamada presionando el botón **Cancelar** (Cancel).

Registros de llamadas
El Softphone contiene una lista de las llamadas salientes, entrantes y perdidas de modo que usted pueda ver estadísticas de todas sus llamadas y las llamadas perdidas.

Se puede tener acceso a la lista desde el modo en espera haciendo clic en el botón **Llamar** (Dial) en la interfaz de software.

Todas las llamadas están marcadas según el tipo de la llamada.

Marca de la llamada	Tipo de llamada
->	Saliente
<-	Entrante
X	Perdida

A la derecha de los números, usted puede ver el tiempo cuando ocurrió la llamada. Si hace doble clic en la entrada en el registro, usted cambiará a la vista detallada, mostrando detalles adicionales. Para marcar un número desde la lista haga clic sobre el número y oprima el botón **Llamar** (Dial). Puede navegar en la lista usando las teclas 2 para desplazarse hacia arriba y 8 para desplazarse hacia abajo. Para borrar la lista, oprima el botón 3.
Si el registro de llamadas está vacío, el Softphone volverá al modo de espera después de algunos segundos.

Directorio telefónico
El Softphone de Corinex contiene un directorio telefónico personalizable por parte del usuario, donde usted puede guardar los números de las personas a quienes llama con regularidad, para que no necesite recordar los números.

Presentación del directorio telefónico
El directorio telefónico es visualizado haciendo clic en el botón con el símbolo de libro, haciendo doble clic en el botón # en la interfaz de Softphone. Después de seleccionar un contacto con el ratón, usted puede llamar o borra el contacto del directorio telefónico.

Tecla	Función
2	Se desplaza hacia arriba en el directorio telefónico
8	Se desplaza hacia abajo en el directorio telefónico
3	Borra el número actualmente seleccionado
Llamar (Dial)	Marca el número actualmente seleccionado
Cancelar (Cancel)	Cierra el directorio telefónico y vuelve al modo en espera

Para agregar nuevos contactos
Para agregar un nuevo contacto al directorio telefónico, haga clic una vez sobre el campo **Nueva entrada** (New Entry). Ingrese el nombre del contacto y oprima **Intro** (Enter). Haga clic sobre el número visualizado al lado del nombre del contacto. Ingrese el número y oprima **Intro** (Enter). De aquí en adelante, usted puede llamar a este contacto seleccionándolo en el directorio telefónico y oprimiendo la tecla verde **Llamar** (Dial).

Para borrar contactos
Si usted desea borrar un contacto del directorio telefónico, selecciónelo en el directorio telefónico usando el ratón o las teclas de teléfono y oprimiendo la tecla **3**.

4.3.4 Configuración del Softphone

Se puede tener acceso al diálogo de configuración haciendo clic en el botón **Menú**. Consiste en cuatro secciones.

1a. Configuraciones de la cuenta para el SIP

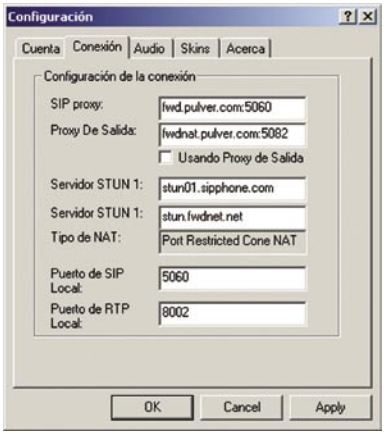
Aquí usted puede establecer las configuraciones de autenticación para su cuenta de VoIP. Usted puede seleccionar uno de los proveedores de servicio de VoIP predefinidos para una disposición fácil de las configuraciones de la cuenta y de la conexión usando el asistente de configuración, o seleccionar configuraciones personalizadas si su proveedor no está en la lista.

Para la mayoría de los proveedores de servicio de VoIP, todo lo que usted necesita inscribir en la pestaña Cuenta es su número de usuario (**Su número**) y contraseña. Algunos proveedores (p.e. Ecuity) requieren información adicional para autenticación - el campo **ID** (Login name). En caso de que su proveedor le dé un nombre de inicio de sesión, junto con el número y la contraseña, por ingréselo en el campo **ID** (Login name). De otra manera, usted puede dejar el campo vacío. Si usted utiliza un perfil predefinido para el proveedor, puede suceder que el campo de **ID** (Login name) esté sombreado sobre gris y usted no pueda editarlo. Esto significa que el proveedor no requiere esta información.

En el campo **Nombre de cuenta** (Account name), ingrese el nombre de su proveedor de servicio, o cualquier otro texto a su opción, que será visualizado en la presentación del Softphone cuando esté conectado con su abastecedor. Usted puede también ingresar un apodo en el campo Apodo (**Nickname**), que será su identificación como llamante al marcar un número.

Nota: El número del usuario (**Your number**), la contraseña (**password**) y el entorno (**realm**) deben ser proporcionados por su proveedor de servicio de VoIP. Para mayores detalles vea el capítulo 3.

2a. Configuraciones para conexión para el SIP



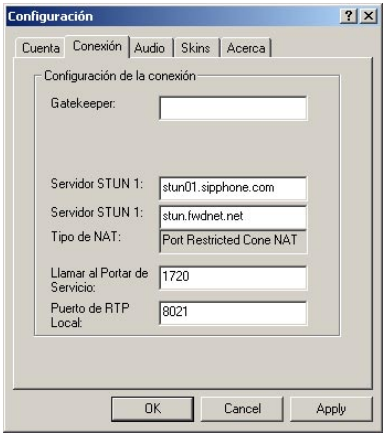
En esta sección usted puede configurar los servidores y los puertos que se utilizan para la conexión del Softphone con un proveedor de servicio de VoIP. Toda la información debe ser proporcionada por su proveedor de VoIP, con la excepción del puerto local de SIP y del puerto local de RTP. Si usted está conectado en una LAN, usted puede necesitar especificar el puerto local de SIP y el puerto local de RTP. Por favor refiérase al capítulo 4.2 para mayor información sobre como configurar estos puertos.

1b. Configuraciones de la cuenta para H.323

Aquí usted puede establecer las configuraciones de autenticación para su cuenta de VoIP. Todo lo que usted necesita inscribir en la pestaña **Cuenta** (Account) es su número de usuario (**Su número**) y **Contraseña**. En el campo **Nombre de cuenta** (Account name), ingrese el nombre de su proveedor de servicio, o cualquier otro texto a su opción, que será visualizado en la presentación del Softphone cuando esté conectado con su abastecedor. Usted puede también ingresar un apodo en el campo Apodo (**Nickname**), que será su identificación como llamante al marcar un número.

Nota: El número del usuario y la contraseña deben ser proporcionados por su proveedor de servicio de VoIP.

2b. Configuraciones para conexión para H.323



En esta sección usted puede configurar la dirección IP o nombre de dominio del guardabarrera (gatekeeper) que se utiliza para la conexión del Softphone con un proveedor de servicio de VoIP. Esta información debe ser proporcionada por su proveedor de servicio de VoIP. Opcionalmente, usted puede especificar servidores STUN y puerto de señalización de llamada, pero esto no es obligatorio. Si usted está conectado en una LAN, usted puede necesitar especificar el puerto local de RTP. Por favor refiérase al capítulo 4.2 para mayor información sobre como configurar este puerto.

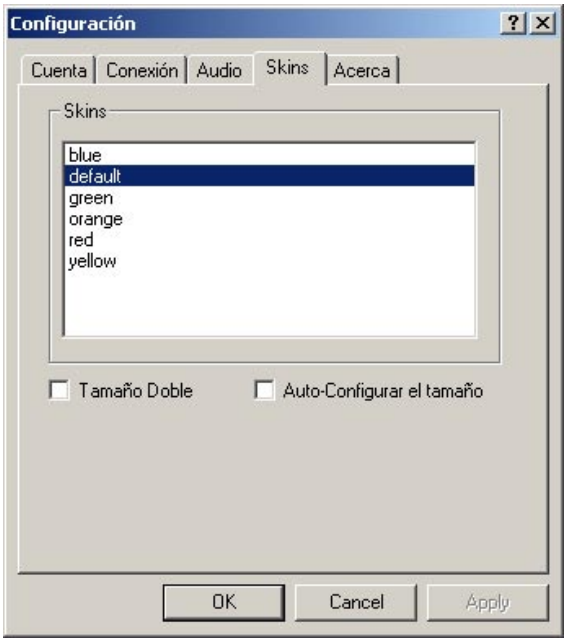
3. Configuraciones de audio

Aquí usted puede configurar los tonos de repique del Softphone, seleccionar el códec usado para la comunicación y seleccionar el dispositivo de sonido, que será utilizado para anunciar las llamadas entrantes y la comunicación de voz.

Timbre de Entrada	El sonido que será reproducido cuando alguien intenta llamarle Cualquier archivo de sonido en el formato WAV puede ser utilizado haciendo clic en el botón '... ' y seleccionando el archivo en el diálogo Abrir archivo (Open File).
Timbre de Salida	El sonido que será reproducido en el altavoz del teléfono USB al marcar un número. Cualquier archivo de sonido en el formato WAV puede ser utilizado haciendo clic en el botón '...' y seleccionando el archivo en el diálogo Abrir archivo (Open File).

Dispositivo del Timbre	El dispositivo de sonido que será utilizado para anunciar las llamadas entrantes.
Dispositivo de Audio Out	El dispositivo de sonido que será utilizado para reproducir el tono de repique seleccionado cuando alguien intenta llamarle
Dispositivo de Audio In	El dispositivo de sonido que se utiliza para grabar voz.
Codec de Salida	El códec que será utilizado para la comunicación de voz.

4. Configuraciones para Skin



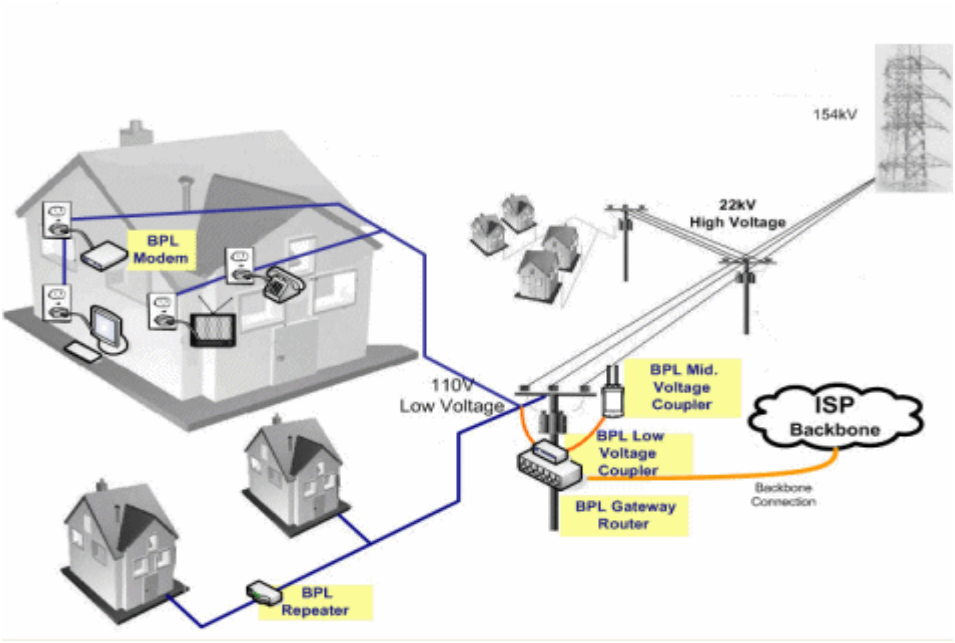
Aquí usted puede seleccionar una de las Skins instaladas. Corinex Softphone está limitado a su aspecto por omisión. Corinex provee varios esquemas de color para la interfaz del Softphone. Para cambiar la piel, por favor selecciónela de la lista y haga clic en el botón **OK**. El Softphone desaparecerá y después de algunos segundos aparecerá con la "piel" nueva.

Puede suceder que el interfaz del Softphone sea demasiado pequeño para usted, especialmente si utiliza una alta resolución de la pantalla (p.e. 1600 x 1200) . En tal caso, usted puede hacer clic sobre **Tamaño doble** (Doublesize) para permitir la ampliación de la interfaz de Softphone. Usted también puede permitir al software el cambiar el tamaño automáticamente, según la resolución de su escritorio. Para resoluciones mayores que 1024x768, el Softphone cambiará al modo magnificado. De otro modo, la interfaz será presentada con el tamaño estándar. Si usted desea habilitar esta configuración automática, por favor elija **Auto-Configurar del tamaño** (Autosize).

Para más skins, por favor dé una mirada a **http://www.corinex.com/voip**.

Low Voltage Systems

The Gridline low voltage system will support Customer Premise Equipment units (CPEs) at the business or consumer location. Our PLC (Power Line Communications) low voltage coupler is positioned at the electric service pole. The low voltage PLC Coupler superimposes broadband signals into a 110V electric power line, and removes broadband signals from the same electrical line which enables the clean delivery of high speed broadband to the end user. While providing the high speed Internet connection, the Gridline delivery system can provide voice services over the Internet (VoIP), with optional VoIP equipment and video on demand. The system can serve multi-unit homes, a building with many apartments or offices. The current data rate for Gridline Communications Corp.'s low voltage is 14 Mbps-25 Mbps, and can reach up to 5 miles. The low voltage PLC will be set to operate with Discreet Multi-Tone (DMT) modulation, with adaptive bit loading for each sub channel. The PLC repeaters can be used to connect homes further apart from the substation to extend range.



PLC CPE equipment will be able to obtain instant access to the Internet and also to the home network through the power outlet. Each CPE has its own security feature, due to added individual key encryption. Other features of PLC CPEs include:

- Packet based data communication
- Readiness for value added service features such as VoIP, video conferencing, video on demand (VOD), and security monitoring for homes and offices

The Gridline CPE specification will include the ability to support standard hub and router hardware. Other target specification for our CPE is:

- Data rate of between 14 Mbps and 25 Mbps, although practical average data rate need for most end-users, will be in the range of 1.5 Mbps and 4 Mbps
- Reach: of up to 5 miles
- Channel specific adaptive loading
- Forward error correction
- Individual encryption
- USB
- Plug and play capabilities with Microsoft Windows®

A PLC Repeater is used to relay frames between the PLC router, and the CPE. It will automatically detect existing PLC device, with a very simple installation process. Our PLC router can support 5 to 10 repeaters both extending the range and number of end user connections.

Our PLC low voltage network management software and server is responsible for monitoring and management of the network and basic remote operation of the network (power reset). iPLC low voltage network management software includes a proprietary simple network management protocol ("SNMP") which is responsible for subscriber registration, authentication, and activity monitoring.

Last-mile Services

Gridline Communications Corp. has developed a set of proprietary Integrated Distributed Powerline Communications ("IDP") technologies as a solution for "last mile" broadband access. The "last mile" is generally

referred to as the connection from the termination of a fiber optical ring to a user's computer. However, deploying the fiber optic lines to end users is currently too expensive to be a realistic option for most consumers or small businesses. In response to this problem, existing telephone lines and television cable networks became delivery mediums of broadband service in the name of DSL and cable modem Internet access. We believe that delivering a large bandwidth via power lines is the most practical solution for Internet access to most end users, given the fact that putting optical cable in every home and business location is expensive and time consuming. The Gridline IDPC technology has evolved around a combination of low power differential electrical signals, improved common-mode noise management and auto-equalization processes.

The IDPC technologies integrate power line communications technologies with fiber-optic based access, dedicated phone lines, CATV signaling, and IP based signaling protocol, to deliver a proprietary set of "bundled telecommunications technologies" that will have the capability to offer the following services:

- POTS or plain old telephone service
- Information monitoring and control services, such as remotely monitored security systems, home and building management systems, telemedicine services for remote diagnosis of patients' symptoms, and long distance educational learning services
- Video teleconferencing
- Multimedia teleconferencing, with voice, video, graphics, and electronic file transfer, etc.
- Video-on-demand, where the subscriber customer requests a certain TV programming, such as a movie, at a time he or she specifies
- Database and information and retrieval services, for home, business, homeland security, law enforcement and other security agencies, where an individual or agent can access a database from his terminal
- Telemarketing services for video catalogue shopping for home-shopping, business to business, and business to residence

- Long distance learning, where students are connected from a remote location, such as their homes, or classroom, through a one-way video basis, or in a group

Other services that will be available to utility companies from the IDPC technologies include, but are not limited to, energy management services, such as:

- Remote and automated meter reading
- Spot pricing of electrical energy
- Load balancing

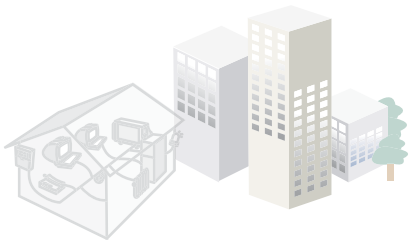
Remote meter readings and accurate spot pricing of electrical energy have already provided saving measures to utility companies, which should subsequently benefit utility customers.

Power Line Communications (PLC) Access and Mini-access

Utility companies can avail themselves of the opportunity to offer PLC access to their existing end-users, creating a brand new revenue stream by implementing Gridline's PLC system to deliver telecommunications services and a number of broadband access applications such as Internet services, video-on-demand, audio, security alarm monitoring and energy management services over the utility company's existing medium and low power electrical grids. Many electrical utility companies already own their fiber optic infrastructure, which have remained unutilized or underutilized. These fiber optic infrastructures can be utilized by utility companies by extending Gridline's PLC to Fiber to the home ("FTTH"), office ("FTTO") or building ("FTTB") services. This connectivity can now be shared by multiple dwellings, campus environments and office buildings.

XPAS-200B

24Mbps Broadband PLC Internet Access System



Welcome to the world of Powerline Communication

Powerline Communication (PLC) uses the existing powerline network - the largest global network by far - as a medium for data transmission. PLC can provide simplified in-house interconnection of computers and cost effective last-mile delivery of broadband data services, as well as energy management systems for the utility companies.

XPAS-200B System Overview

Xeline's XPAS-200B PLC Internet Access System supports data rates of up to 24Mbps and is based on Xeline's new proprietary Cell-Structured MAC (CMAC), which offers virtually unlimited number of nodes per physical network. Repeaters are also supported to expand coverage and offer stable services in unfavorable powerline conditions.

The XPAS-200B systems supports both Master/Slave and Ad-hoc topology, guaranteeing inter-house security through the Master/Slave topology, while Ad-hoc home networking is supported at the same time for effective networking.

The XPAS-200B system also focuses on the needs of the ISP by fully supporting remote registration, management, and firmware upgrade of the PLC units through the EMS (Element Management System) Unit. Because there is no manual configuration needed at the time of installation, end-users can easily install the Slave Unit by simply plugging the unit into a power outlet. All PLC units are authorized, monitored, and managed remotely by the EMS Administrator.

Combining communciation reliability, system flexibity and ISP-friendly functions, the XPAS-200B is the most advanced and optimal solution for commercial deployment of PLC technology.

Everywhere & Anywhere

- Uses existing powerline infrastructure
- Broadband connection availabe from every power outlet
- Virtually unlimited number of nodes per network
- Connect entire building networks via PLC
- No need for complicated and expensive cabling

Easy Installation & Remote Management

- Plug & Play installation for the end-user
- No manual configuration needed.
- Remote registration & firmware upgrade of the PLC units
- Remote management & monitoring through EMS
- Patented magnetic coupling method

Communication Reliability

- Adaptive bit loading per each subchannels
- Fast adaptation in time-varying channels
- Repeater function supported for reliable communication
- RTS/CTS for hidden node detection

Security and Network Management

- Supports blocking of inter-Slave communication
- 56bit DES for node-based encryption
- VLAN support
- EMS based on SNMP
- Programmable forbidden bands

Product Line Up

MM-202B PLC Master Unit

The MM-202B is the Master Unit that controls all Slave and Repeater Units in a logical network. It is the access point to the backbone network and can support up to 128 Slaves per Master Unit. A total of 16,384 Master Units can co-exist in a physical network.

SU-200B PLC Slave Unit

The SU-200B is the Slave Unit equivalent to the customer premise equipment (CPE). With its slim and compact design, the Slave is designed to enable the end-user to instantly access the Internet or home network from any electrical outlet in the home. The Slave supports Ethernet (RJ-45) interface and one Slave Unit is needed for each PC or device.

RU-200B PLC Repeater Unit

The RU-200B is the Repeater Unit that extends system reliability and coverage in unfavorable conditions. The Repeater can be installed at any location between the Master and Slaves.

CU-100A PLC Coupler

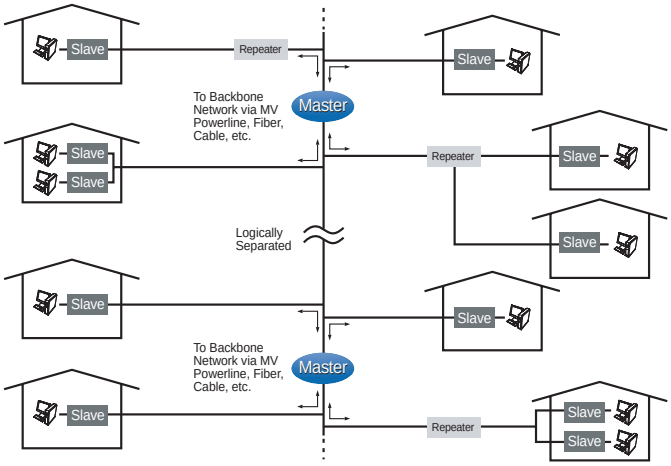
The CU-100A is the low voltage Coupler for the XPAS PLC Internet access systems. The Coupler is used to couple the PLC signals to the powerlines. Xeline's patented magnetic coupling method ensures that the procedure is simple and safe.

EU-200B PLC EMS Unit

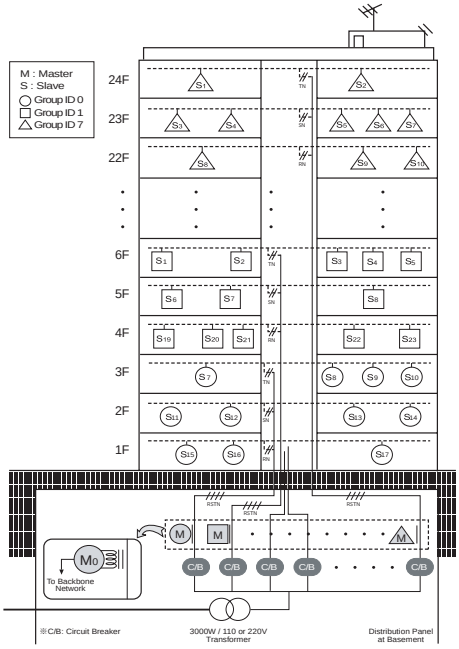
The EU-200B is the EMS (Element Management System) Unit that is essential for the remote registration, management, monitoring, and firmware uprgrade of the XPAS-200B PLC system.

XPAS-200B 24Mbps Broadband PLC Internet Access System

Single Residential House Topology



Apartment / High-Rise Building Toplogy



XPAS-200B System Specifications

Applications	Broadband Internet access
Payload rate	24Mbps
UDP/TCP rate	Up to 16Mbps / 10Mbps
Coverage	Up to 600 ~ 800m (varies according to power grid)
Used band	2 ~ 23MHz
Modulation	DMT (Discrete Multi-Tone)
FEC	Convolutional and R/S codes with Interleaver
Multiple access	Cell-structured MAC

MM-202B PLC Master Unit

Master Co-existence	16,384 Masters per physical network
No. of Slaves	128 Slaves per Master Unit
Interface	SIG1/SIG2 (PLC signals) 10/100 base-T - UPLINK (backbone) - EXT (extension) - LAN (test)
LED	PWR/UPLINK/ACT1/ACT2
Supply Voltage	220V or 110V ± 10% (50Hz or 60Hz)
Dimensions	260 x 154 x 35mm (W x D x H)
Certifications	FCC Part 15 / CE approved

SU-200B PLC Slave Unit

Supported O/S	Windows 98 SE, ME, 2000, XP
PC requirements	CPU: Pentium or higher Memory: 32M RAM or higher
Interface	10/100 base-T
LED	PWR/ACT/SYNC/LAN
Supply Voltage	220V or 110V ± 10% (50Hz or 60Hz)
Dimensions	150 x 90 x 35mm (W x D x H)
Certifications	FCC Part 15 / CE approved

RU-200B PLC Repeater Unit

Coverage	Expands coverage by 600 ~ 800m per Repeater (varies according to power grid)
Interface	SIG1/SIG2 (PLC signals)
LED	PWR/UPLINK/ACT1/ACT2
Supply Voltage	220V or 110V + 10% (50Hz or 60Hz)
Dimensions	260 x 154 x 35mm (W x D x H)
Certifications	FCC Part 15 / CE approved

CU-100A PLC Coupler

In/out signals	Input signal, External output
Terminals	4 port powerline coupling (patented magnetic coupling method)
Dimensions	97 x 50 x 34mm (W x D x H)

EU-200B PLC EMS Unit

Protocol	SNMP V1/V2
Monitoring Interface	Network status / Remote control 10/100 base-T (backbone) RS-232 (console port)
Dimensions	320 x 200 x 44mm (W x D x H)

xeline

Contenido

Comisión de Tarifas
de Energía

DISTANCIAS EQUIVALENTES Y DIAGRAMAS UNIFILARES DE TRANSMISIÓN SECUNDARIA DE LOS SISTEMAS ELÉCTRICOS DE DISTRIBUCIÓN AL 31/12/1999

Presentación

La Comisión de Tarifas de Energía con el propósito de mantener informados a los diversos agentes del mercado eléctrico interesados en la regulación tarifaria, se complace en presentar la versión actualizada al 31/12/1999 del documento técnico denominado "Distancias Equivalentes y Diagramas Unifilares de Transmisión Secundaria de los Sistemas Eléctricos de Distribución".

El documento recoge las modificaciones de las distancias equivalentes y diagramas unifilares de transmisión secundaria, realizadas durante 1999. Dichas modificaciones están relacionadas con la incorporación de nuevas líneas de transmisión y centros de transformación, y aumento de la capacidad instalada de centros de transformación existentes, realizadas por las empresas de distribución con la finalidad de mejorar la calidad del servicio eléctrico e interconectar nuevas localidades. Asimismo, se incluye las distancias equivalentes y diagramas unifilares de aquellos sistemas que han pasado de ser sistemas aislados a interconectados como es el caso de los sistemas eléctricos de Tumbes, Bajo Piura, Córdova-Querco y Colca.

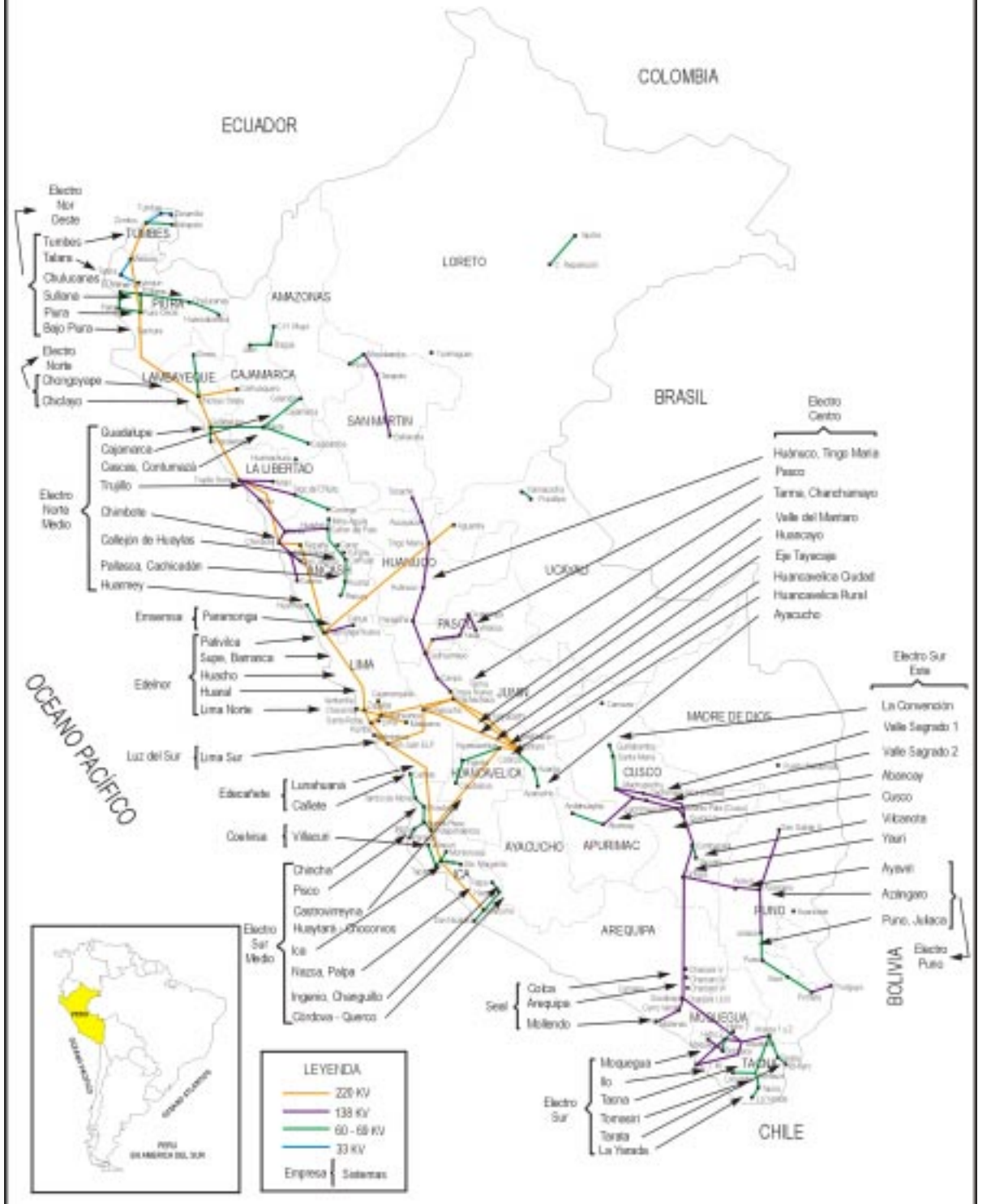
La distancia equivalente para cada sistema eléctrico de distribución, se calcula a partir de la barra base correspondiente, publicada en las resoluciones semestrales de generación, y los diagramas unifilares de transmisión secundaria. Dicha distancia se utiliza para el cálculo de los precios en barra equivalente de media tensión de los sistemas eléctricos de distribución, con los cuales se determina el pliego tarifario aplicable a los clientes finales del servicio público de electricidad.

El procedimiento de cálculo de la distancia equivalente es el establecido en las Resoluciones de la CTE, vigentes a la fecha de publicación del presente documento: Resolución N° 004-99 P/CTE, Resolución N° 008-98 P/CTE, Resolución N° 023-97 P/CTE y Resolución N° 015-95 P/CTE.

Finalmente, deseo agradecer especialmente al personal de la Secretaría Ejecutiva, las Empresas de Distribución Eléctrica y las personas que de una u otra forma prestaron su colaboración y contribuyeron en la actualización del presente documento.

EDUARDO ZOLEZZI CHACÓN
Presidente
Comisión de Tarifas de Energía

UBICACIÓN DE SISTEMAS ELÉCTRICOS



DISTANCIAS EQUIVALENTES
DE LOS SISTEMAS ELÉCTRICOS INTERCONECTADOS

EMPRESA	SISTEMA ELÉCTRICO	SECTOR TÍPICO	BARRA DE REFERENCIA		Tensión de Cálculo kV	Leq km
			Barra	Tensión kV		
Coelvisa	Villacurí	3	Ica	220	60	34,20
Edecañete	Cañete	2	Independencia	220	60	92,50
	Lunahuaná	3	Independencia	220	60	92,50
Edelnor	Huacho-Supe-Barranca	2	Paramonga	220	60	40,41
	Huaral	2	Lima (1)	220	60	66,83
	Lima Norte (4)	1	Lima (1)	220	-	-
	Pativilca	2	Paramonga (3)	138	-	0,00
Electro Centro	Ayacucho	2	Mantaro	220	60	115,91
	Eje Tayacaja	3	Mantaro	220	33	22,62
	Huancavelica Ciudad	2	Huancavelica	220	60	8,35
	Huancavelica Rural	4	Huancavelica	220	60	8,35
	Huancayo	2	Huayucachi	220	60	19,97
	Huánuco	2	Huánuco	138	-	0,00
	Pasco	2	Oroya (3)	50	50	26,41
	Tarma-Chanchamayo	2	Condorcocha	138	44	42,50
	Tingo María	2	Tingo María	220	138	5,93
	Valle del Mantaro	3	Huayucachi	220	60	19,97
Electro Nor	Bajo Piura	2	Piura Oeste	220	60	51,68
Oeste	Chulucanas	2	Piura Oeste	220	60	60,00
	Piura	2	Piura Oeste	220	60	7,00
	Sullana-El Arenal-Paita	2	Piura Oeste	220	60	50,39
	Talara	2	Talara	220	33	5,88
	Tumbes	2	Zorritos (3)	60	60 y 33	25,36
Electro Norte	Chiclayo-Íllimo	2	Chiclayo Oeste	220	60	8,40
	Chongoyape	3	Carhuaquero	10	-	0,00
Electro Puno	Ayaviri	3	Ayaviri	138	-	0,00
	Azángaro	3	Azángaro	138	-	0,00
	Puno-Juliaca-Pomata	2	Juliaca	138	60	53,04
Electro Sur	Ilo	2	Toquepala	138	-	0,00
	La Yarada	2	Tacna	66	66	27,30
	Moquegua	2	Toquepala	138	66	25,00
	Tacna	2	Tacna	66	66	2,24
	Tarata	3	Aricota	66	33	59,51
	Tomasiri	3	Tomasiri	66	-	0,00

EMPRESA	SISTEMA ELÉCTRICO	SECTOR TÍPICO	BARRA DE REFERENCIA		Tensión de Cálculo kV	Leq km
			Barra	Tensión kV		
Electro Sur	Abancay	3	Cachimayo	138	138	150,74
Este	Cusco	2	Cusco (2)	138	-	0,00
	La Convención	2	Machupicchu	138	60	40,23
	Valle Sagrado 1	4	Cachimayo	138	33	17,92
	Valle Sagrado 2	4	Cusco (2)	138	33	25,70
	Vilcanota-Sicuani	4	Combapata	138	66	13,08
	Yauri	2	Tintaya	138	-	0,00
Electro Sur	Castrovirreyna	4	Huancavelica	220	60	85,30
Medio	Chincha	2	Independencia	220	60	39,77
	Córdova-Querco	3	Marcona	220	60	93,96
	Huaytará-Chocorvos	3	Huancavelica	220	60	85,30
	Ica	2	Ica	220	60	7,05
	Ingenio-Changuillo	4	Marcona	220	60	93,96
	Nazca-Palpa	2	Marcona	220	60	93,96
	Pisco	2	Independencia	220	60	32,68
Emsemsa	Paramonga	2	Paramonga (3)	138	-	0,00
Hidrandina	Cajamarca	2	Guadalupe	220	60	127,39
	Callejón de Huaylas	2	Huallanca	138	66	60,93
	Cascas-Contumazá	3	Guadalupe	220	60	127,39
	Chimbote	2	Chimbote 1	220	138	19,73
	Guadalupe-Chepén-Pacasmayo	2	Guadalupe	220	60	9,00
	Huarmey	2	Paramonga	220	66	80,00
	Pallasca-Cachicadán	3	Huallanca	138	66	60,93
	Trujillo	2	Trujillo Norte	220	138	24,53
Luz del Sur	Lima Sur (4)	1	Lima (1)	220	-	-
Seal	Arequipa	2	Socabaya	138	33	9,04
	Colca	2	Callalli	138	-	0,00
	Mollendo-Matarani	2	Mollendo	138	33	12,54

Notas:

(1): S.E.B. Lima: Constituida por las Subestaciones Base Chavarría 220 kV, Santa Rosa 220 kV y San Juan 220 kV

(2): S.E.B. Cusco: Constituida por las Subestaciones Base Dolorespata 138 kV y Quencoro 138 kV

(3): Barra de referencia no publicada.

(4): Cargos de transmisión secundaria fijados por la Resolución N° 004-99 P/CTE

Simbología y Leyenda de los Diagramas Unifilares

Naranja		= Barra o Línea de 220 kV
Morado		= Barra o Línea de 138 kV
Verde		= Barra o Línea de 50 kV; 60 kV; 66 kV; 69 kV
Celeste		= Barra o Línea de 30 kV; 33 kV
Rojo		= Barra o Línea de 10 kV; 13,2 kV; 22,9 kV
Negro		= Otra distinta
Cualquier color		= Línea de otra empresa


= Barra de Referencia


= Centro de Generación


= Transformador de 3 arrollamientos


= Transformador de 2 arrollamientos


= Autotransformador

= Límite de central, sistema, etc.


= Sentido de flujo predominante


= Cruce de línea, sin conexión


= Carga en la barra

Leq	= Distancia Equivalente en km
C	= Valor C
17,33 km	= Longitud en km
DT 4,46 km	= Doble Terna; Longitud en km
(AA 120 mm2)	= (Tipo y calibre)
MW; MVA	= Demanda máxima; Potencia instalada
CT; CH	= Central térmica; Central hidráulica
SE	= Subestación

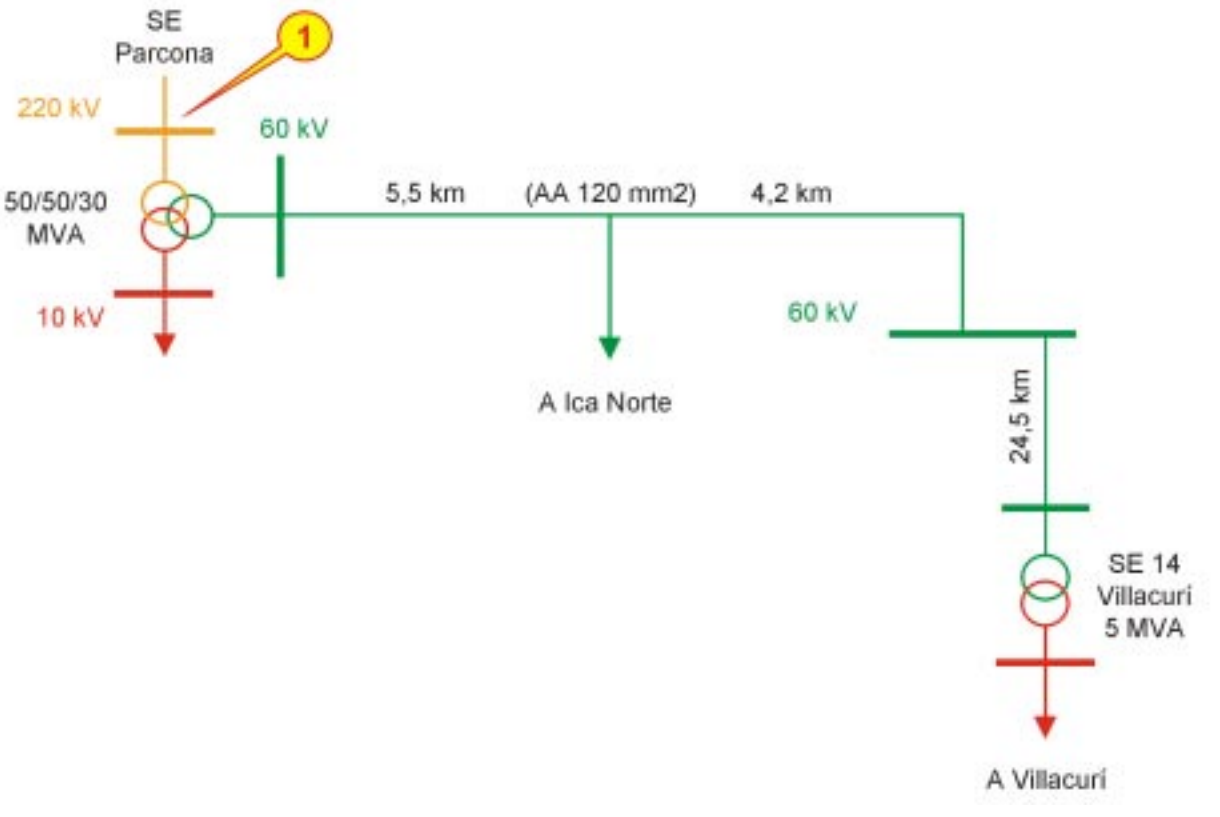
EMPRESA

C O E L V I S A

SISTEMA

Villacurí

V I L L A C U R Í



SISTEMA ELÉCTRICO: Villacurí	**EMPRESA ELÉCTRICA:** COELVISA			
	Sector Típico: 3	Leq: 34,20 km	Fecha: 12/99	Pág. 1/1

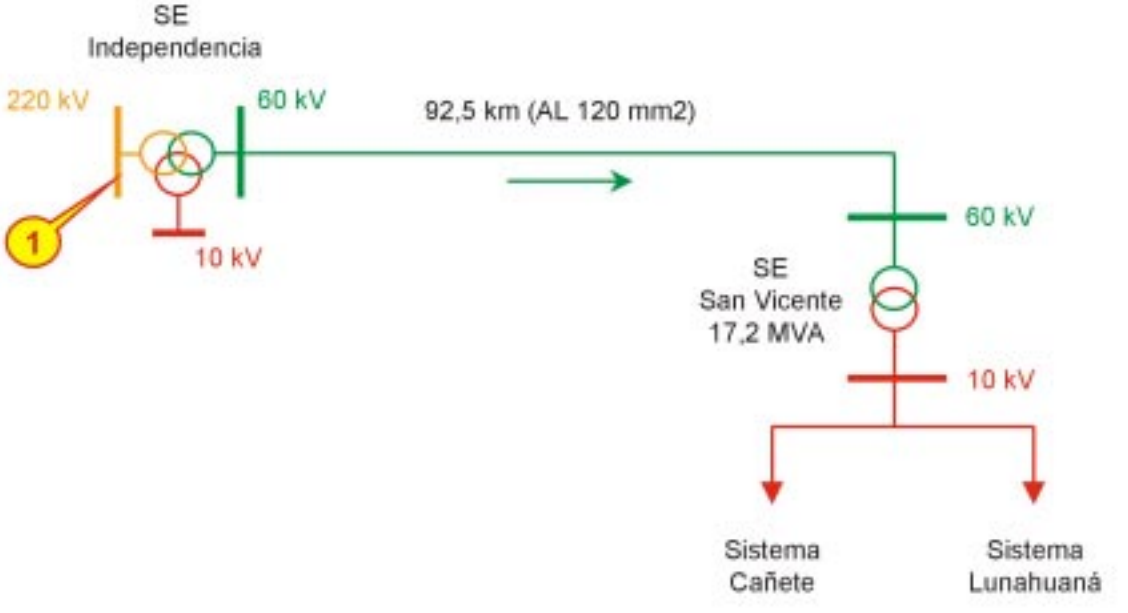
EMPRESA

E D E C A Ñ E T E S. A.

SISTEMAS

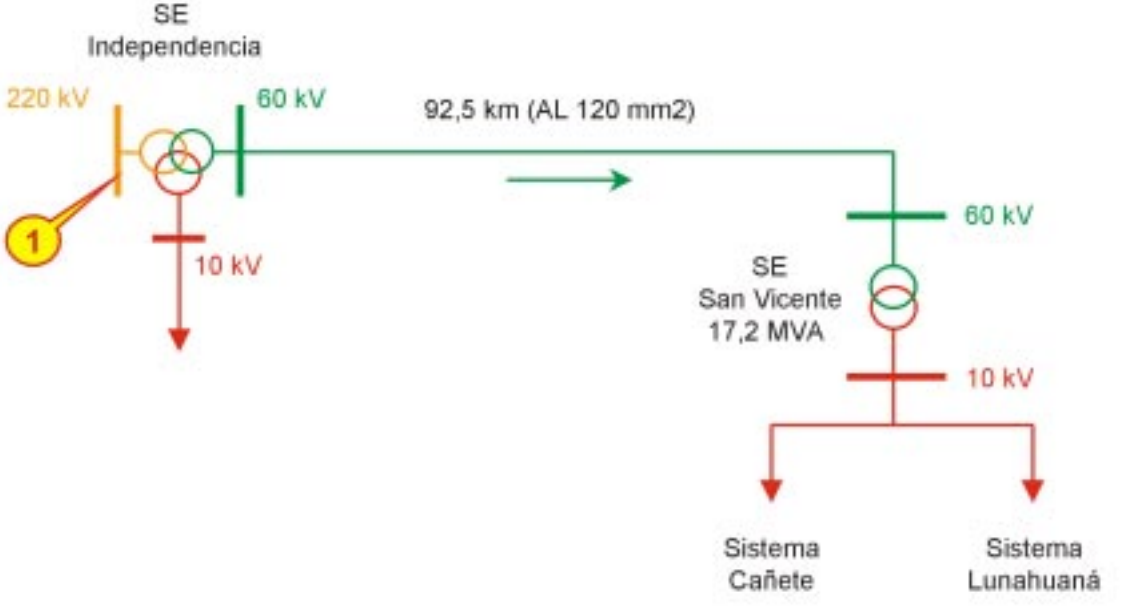
Cañete
Lunahuaná

C A Ñ E T E



SISTEMA ELÉCTRICO: Cañete	EMPRESA ELÉCTRICA: EDE CAÑETE S.A.			
	Sector Típico: 2	Leq: 92,5 km	Fecha: 12/99	Pág. 1/2

L U N A H U A N Á



SISTEMA ELÉCTRICO: Lunahuaná	**EMPRESA ELÉCTRICA:** EDE CAÑETE S.A.			
	Sector Típico: 3	Leq: 92,5 km	Fecha: 12/99	Pág. 2/2

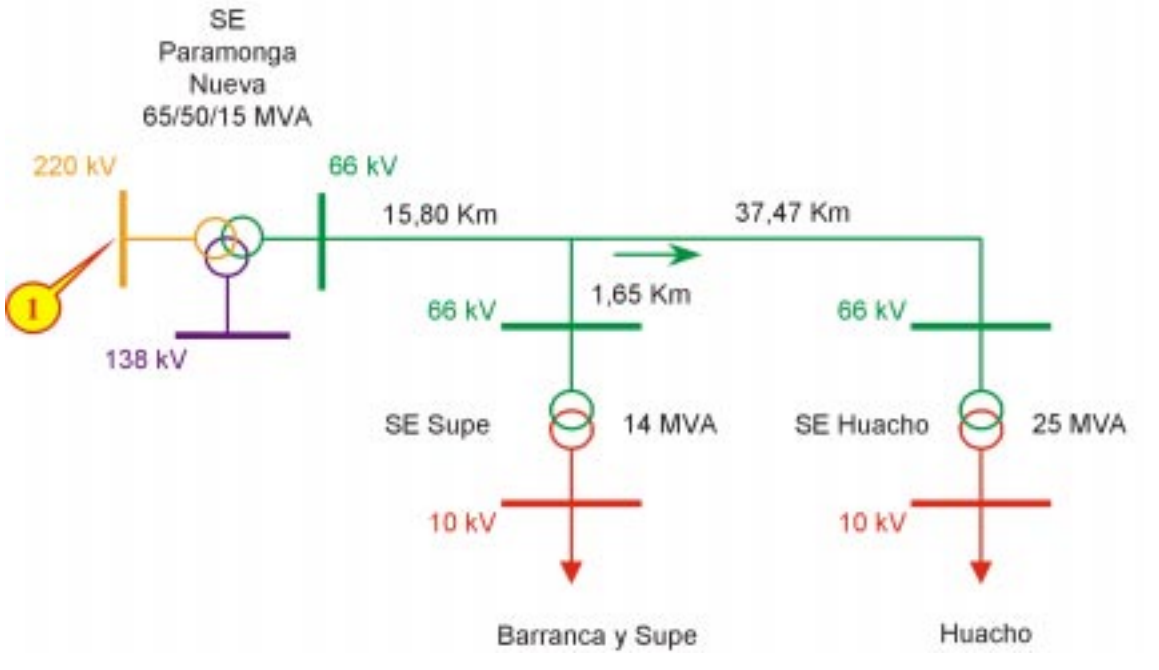
EMPRESA

E D E L N O R S. A.

SISTEMAS

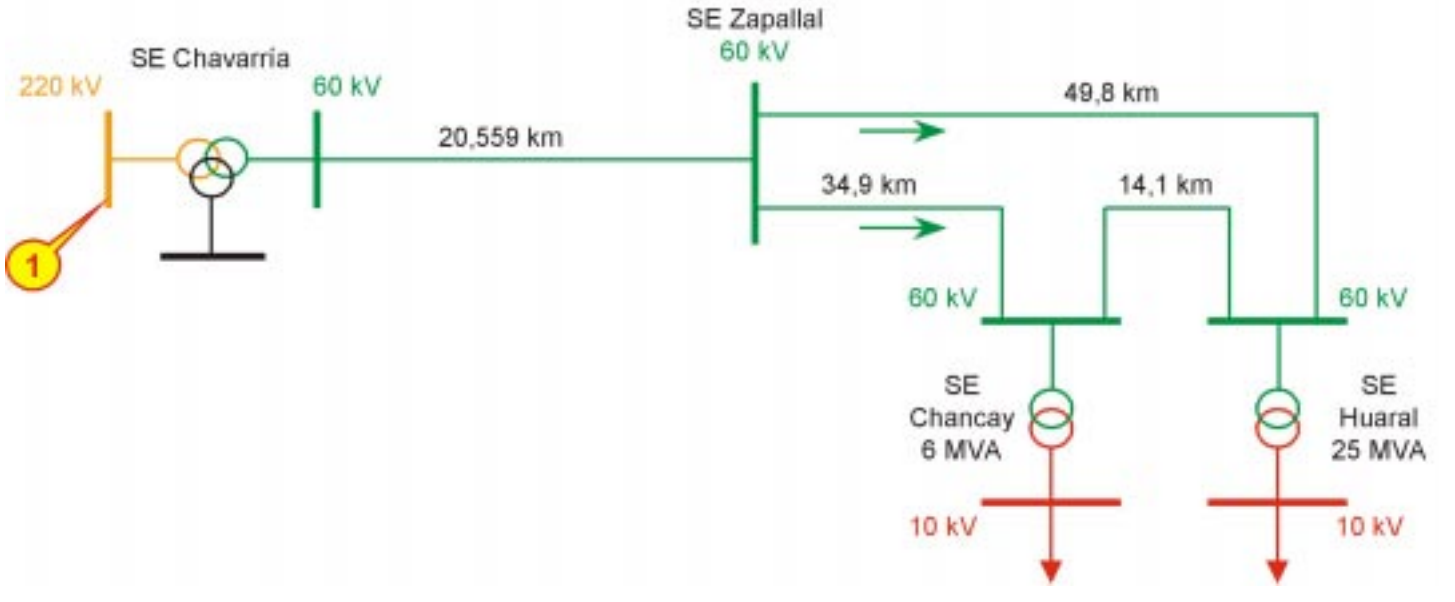
Huacho - Supe - Barranca
Huaral
Lima Norte
Pativilca

H U A C H O - S U P E - B A R R A N C A



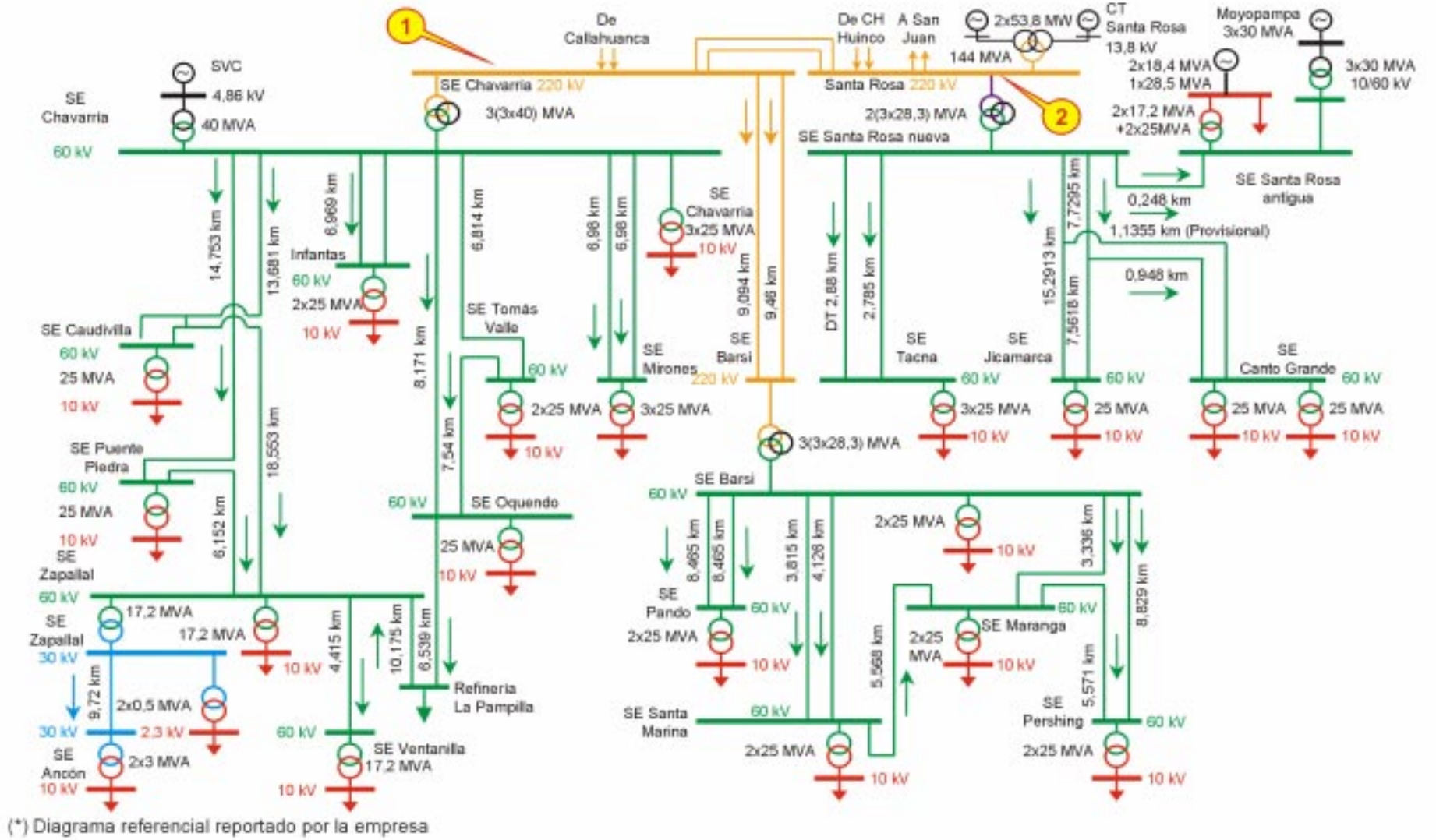
SISTEMA ELÉCTRICO: Huacho - Supe - Barrranca	**EMPRESA ELÉCTRICA:** EDELNOR S.A.			
	Sector Típico: 2	Leq: 40,41 km	Fecha: 12/99	Pág. 1/4

H U A R A L



SISTEMA ELÉCTRICO: Huaral	**EMPRESA ELÉCTRICA:** EDELNOR S.A.			
	Sector Típico: 2	Leq: 66,83 km	Fecha: 12/99	Pág. 2/4

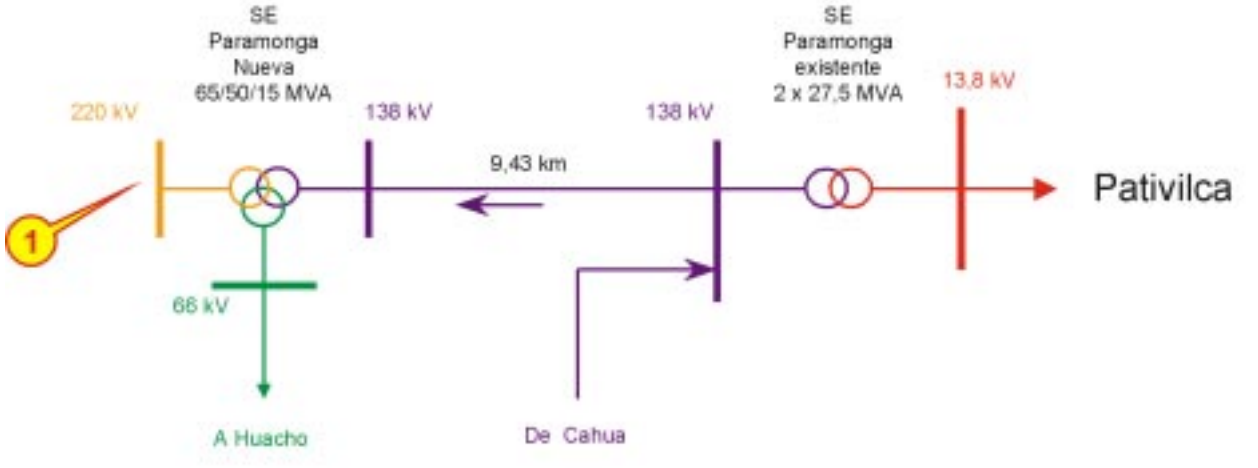
L I M A N O R T E (*)



(*) Diagrama referencial reportado por la empresa

SISTEMA ELÉCTRICO: Lima Norte y Callao	**EMPRESA ELÉCTRICA:** EDELNOR S.A.	
	Sector Típico: 1	Fecha: 12/99	Pág. 3/4

P A T I V I L C A



SISTEMA ELÉCTRICO: Pativilca	**EMPRESA ELÉCTRICA:** EDELNOR S.A.			
	Sector Típico: 2	Leq: 0 km	Fecha: 12/99	Pág. 4/4

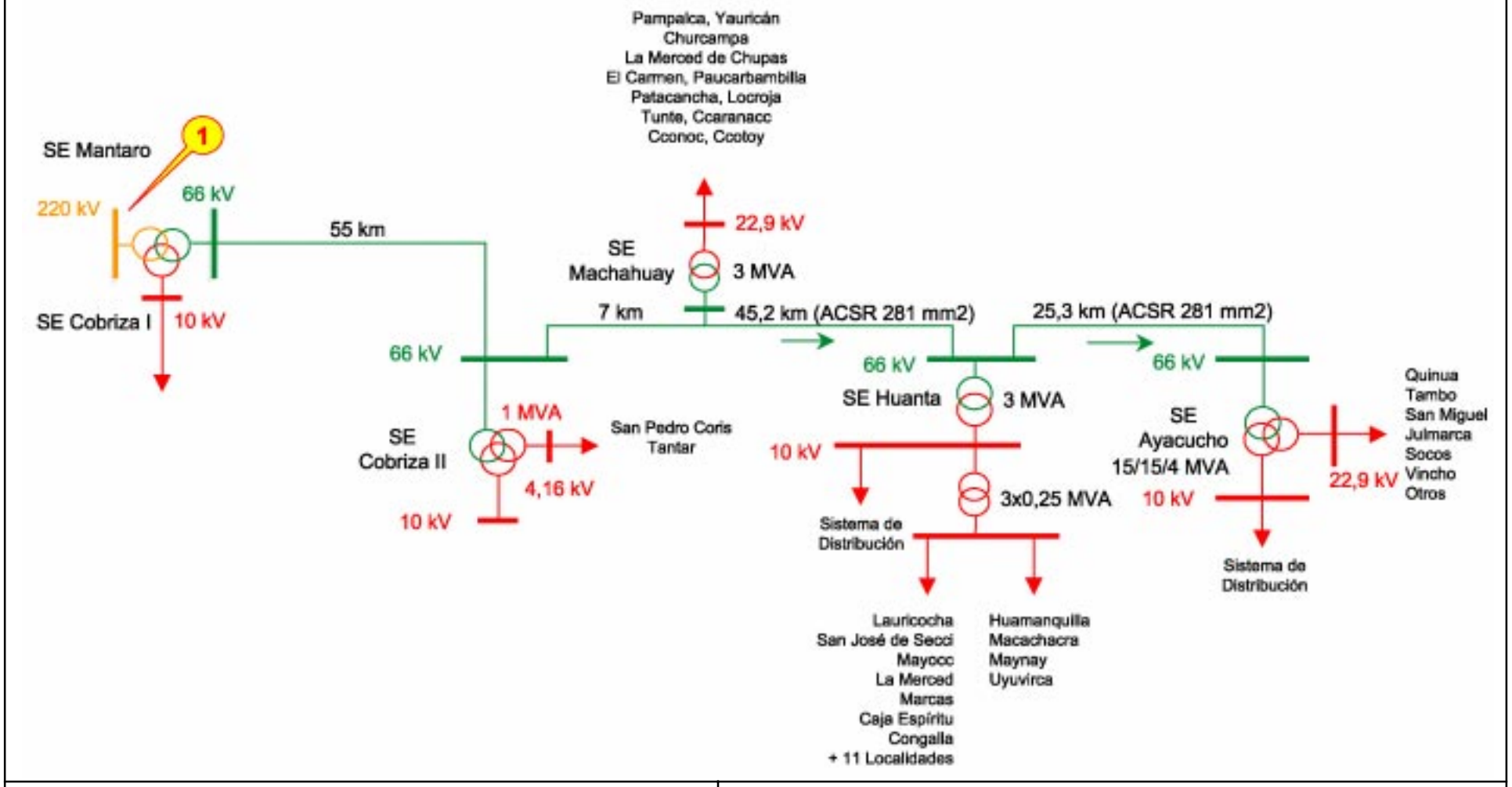
EMPRESA

E L E C T R O
C E N T R O S. A.

SISTEMAS

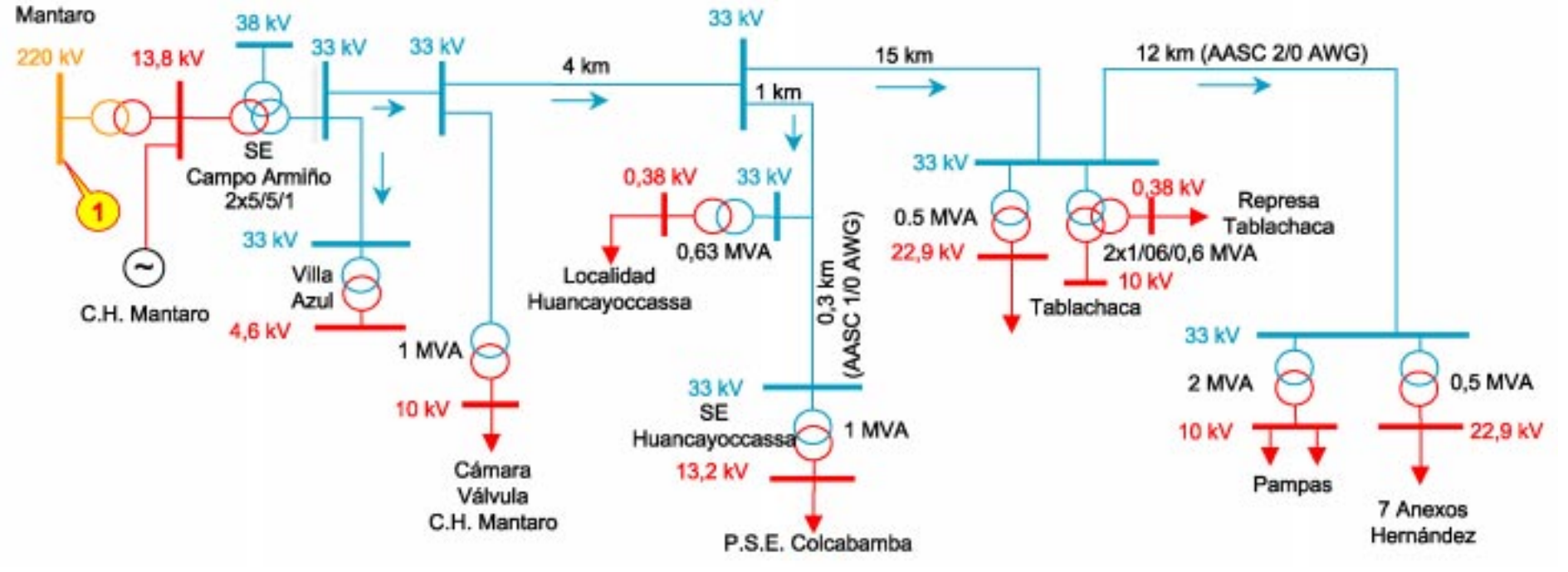
Ayacucho
Eje Tayacaja
Huancavelica Ciudad
Huancavelica Rural
Huancayo
Huánuco
Pasco
Tarma - Chanchamayo
Tingo María
Valle del Mantaro

A Y A C U C H O



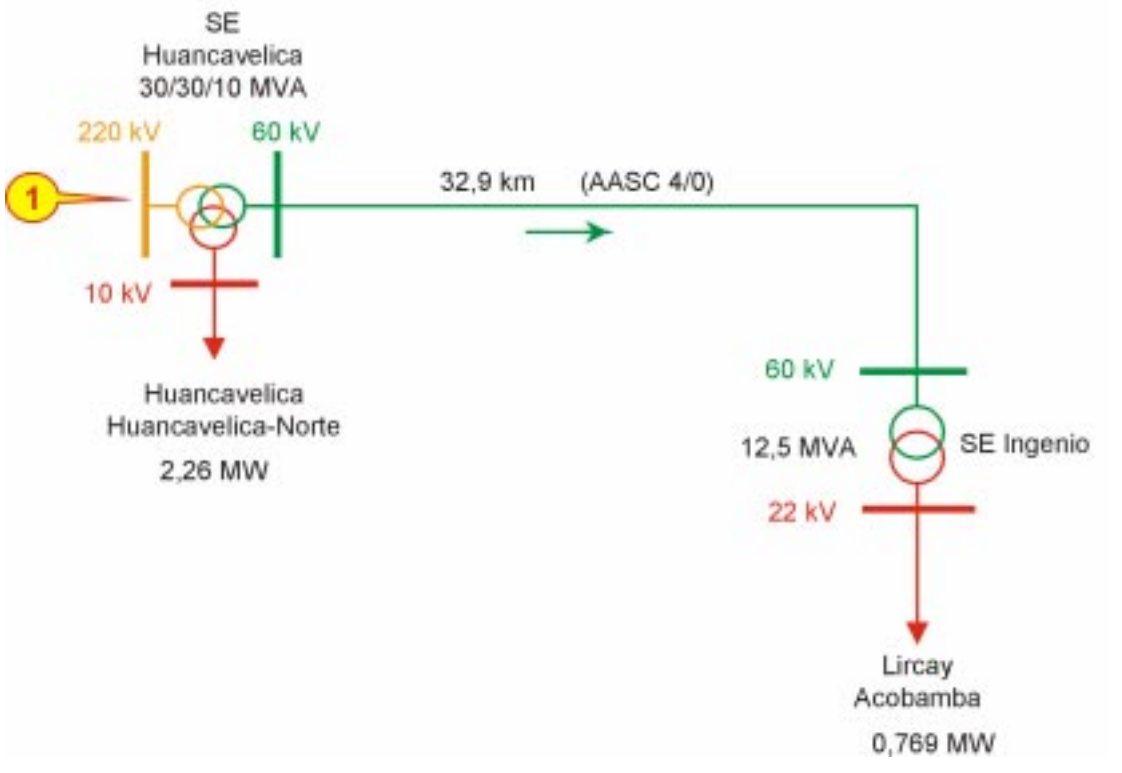
SISTEMA ELÉCTRICO: Ayacucho	**EMPRESA ELÉCTRICA:** ELECTRO CENTRO S.A.			
	Sector Típico: 2	Leq: 115,91 km	Fecha: 12/99	Pág. 1/10

E J E T A Y A C A J A



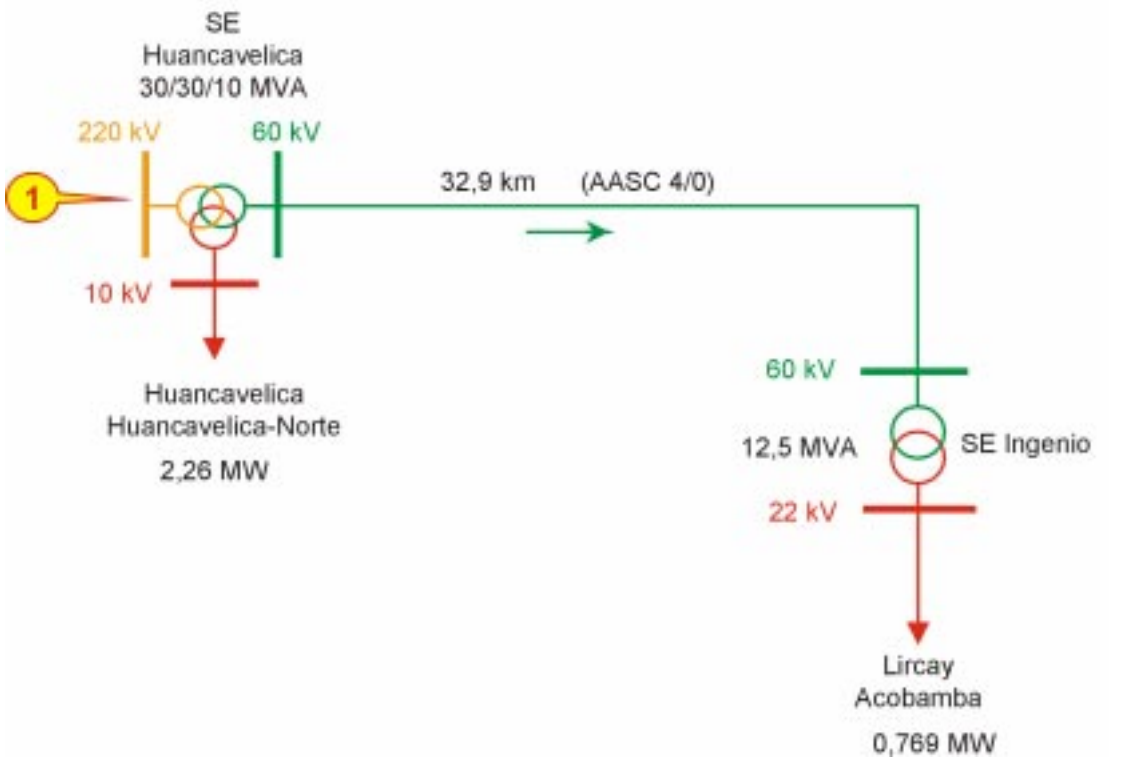
SISTEMA ELÉCTRICO: Eje Tayacaja	**EMPRESA ELÉCTRICA:** ELECTRO CENTRO S.A.			
	Sector Típico: 3	Leq: 22,62 km	Fecha: 12/99	Pág. 2/10

H U A N C A V E L I C A C I U D A D



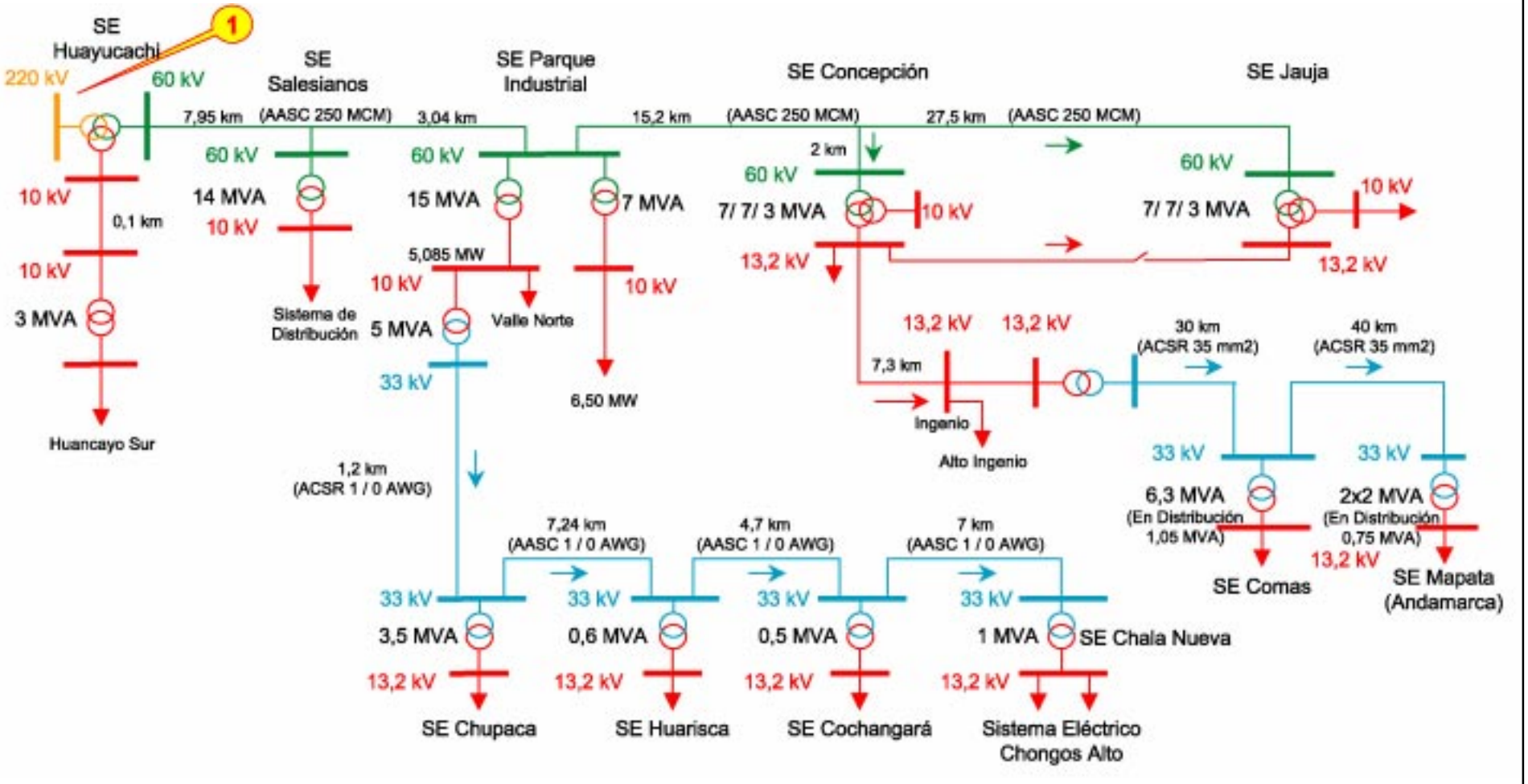
SISTEMA ELÉCTRICO: Huancavelica Ciudad	**EMPRESA ELÉCTRICA:** ELECTRO CENTRO S.A.			
	Sector Típico: 2	Leq: 8,35 km	Fecha: 12/99	Pág. 3/10

H U A N C A V E L I C A R U R A L



SISTEMA ELÉCTRICO: Huancavelica Rural	**EMPRESA ELÉCTRICA:** ELECTRO CENTRO S.A.			
	Sector Típico: 4	Leq: 8,35 km	Fecha: 12/99	Pág. 4/10

H U A N C A Y O

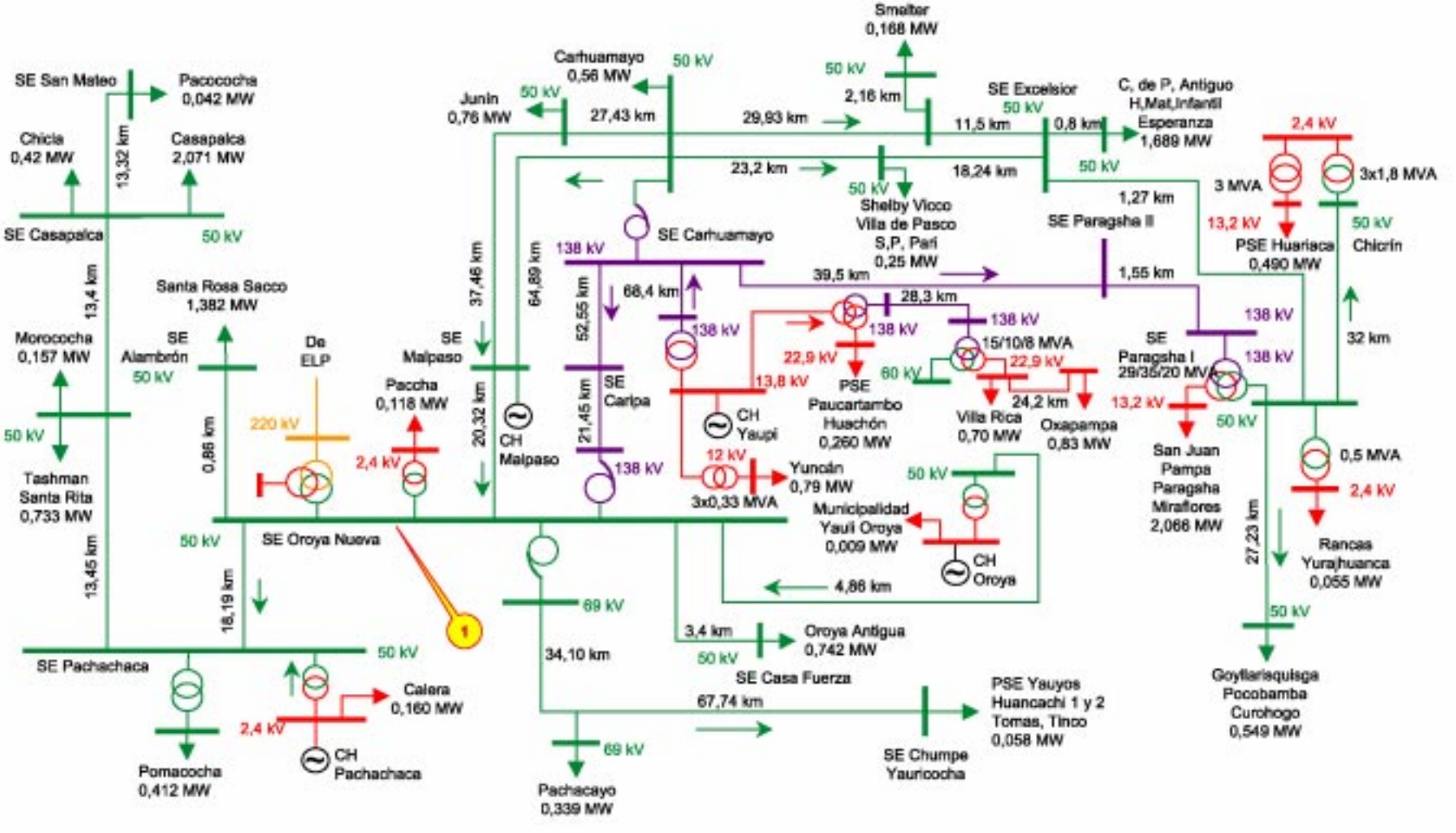


SISTEMA ELÉCTRICO: Huancayo	**EMPRESA ELÉCTRICA:** ELECTRO CENTRO S.A.		
	Sector Típico: 2	Leq: 19,97 km	Fecha: 12/99	Pág. 5/10

H U Á N U C O

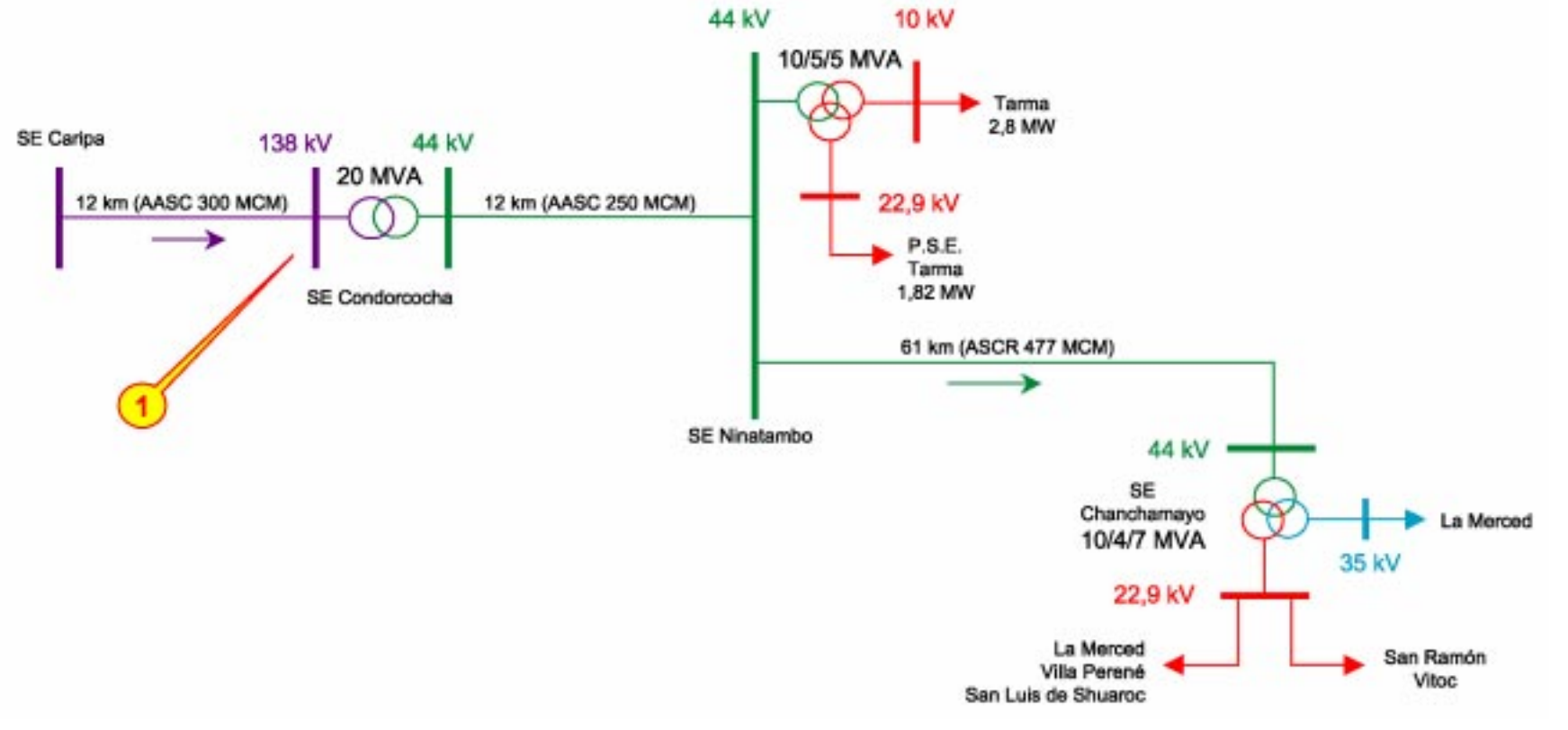
SISTEMA ELÉCTRICO: Huánuco	**EMPRESA ELÉCTRICA:** ELECTRO CENTRO S.A.			
	Sector Típico: 2	Leq: 0 km	Fecha: 12/99	Pág. 6/10

P A S C O



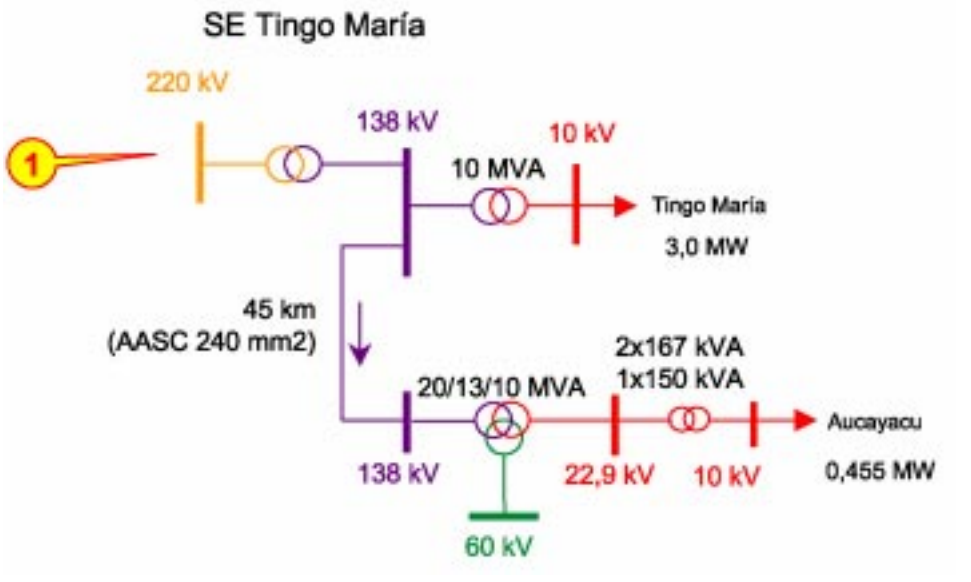
SISTEMA ELÉCTRICO: Pasco	**EMPRESA ELÉCTRICA:** ELECTRO CENTRO S.A.		
	Sector Típico: 2	Leq: 26,41 km	Fecha: 12/99	Pág. 7/10

T A R M A - C H A N C H A M A Y O



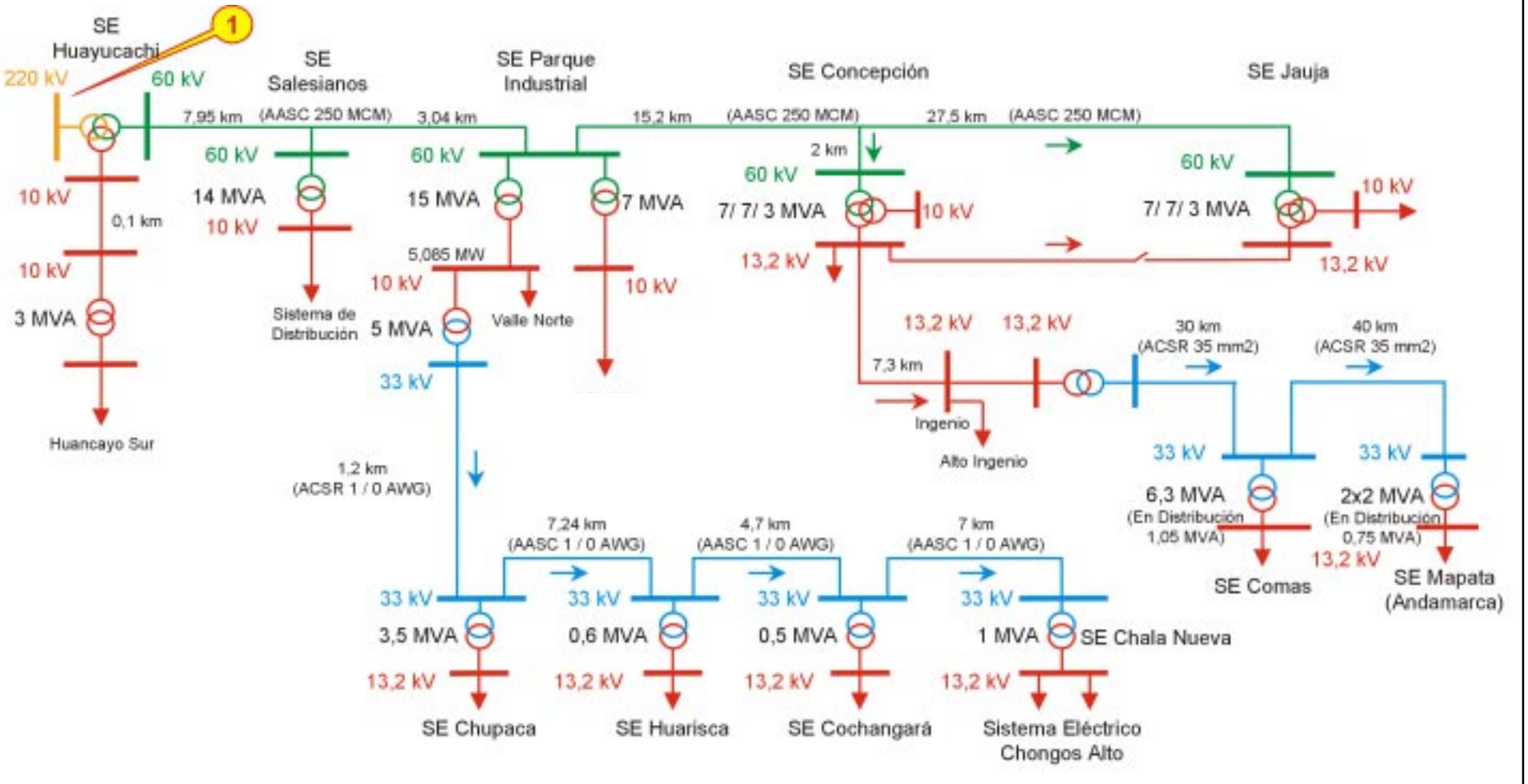
SISTEMA ELÉCTRICO: Tarma - Chanchamayo	EMPRESA ELÉCTRICA: ELECTRO CENTRO S.A.			
	Sector Típico: 2	Leq: 42,50 km	Fecha: 12/99	Pág. 8/10

TINGO MARÍA



SISTEMA ELÉCTRICO: Tingo María	**EMPRESA ELÉCTRICA:** ELECTRO CENTRO S.A.			
	Sector Típico: 2	Leq: 5,93 km	Fecha: 12/99	Pág. 9/10

V A L L E D E L M A N T A R O



SISTEMA ELÉCTRICO: Valle del Mantaro	**EMPRESA ELÉCTRICA:** ELECTRO CENTRO S.A.			
	Sector Típico: 3	Leq: 19,97 km	Fecha: 12/99	Pág. 10/10

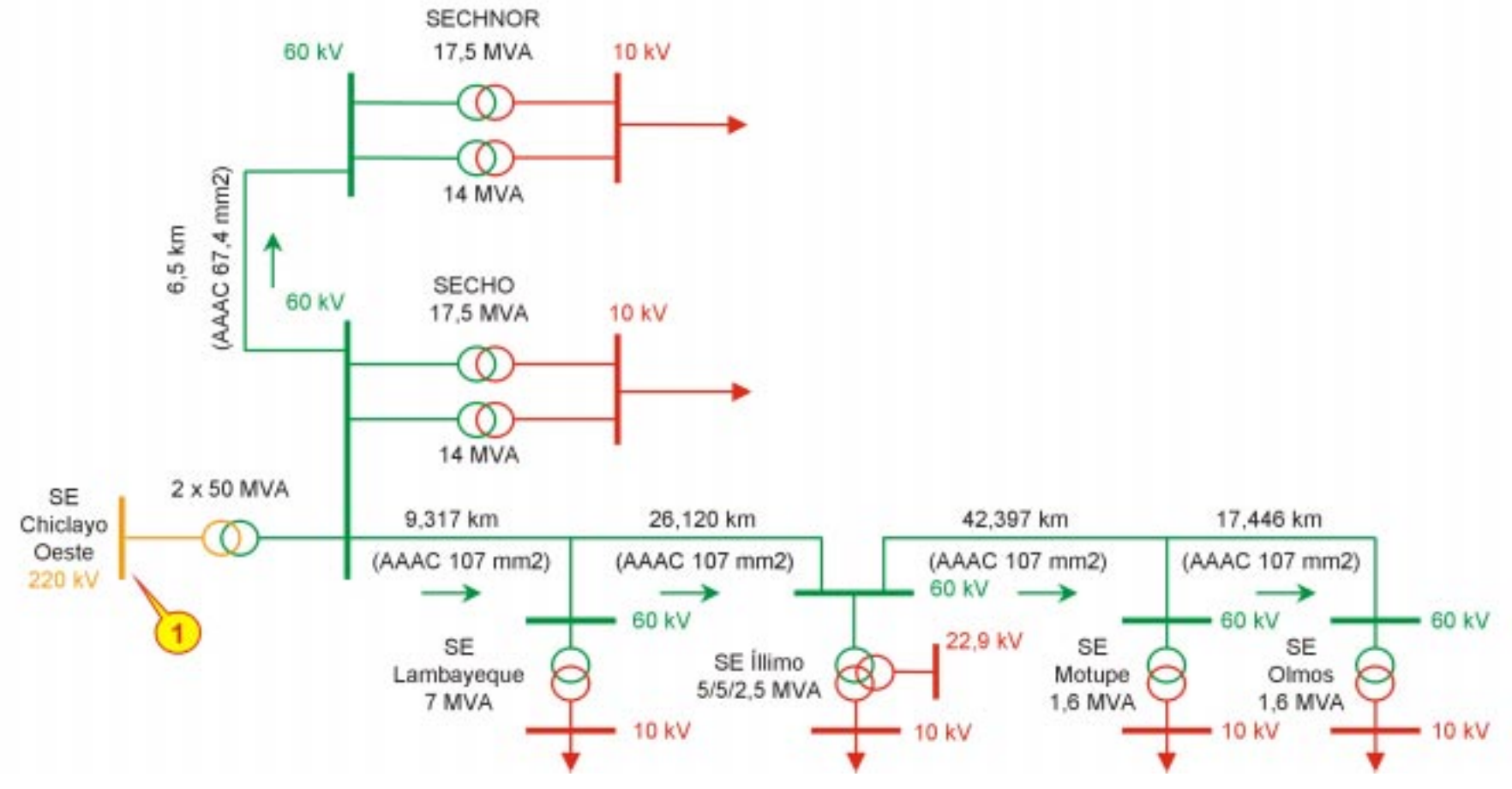
EMPRESA

E L E C T R O
N O R T E S. A.

SISTEMAS

Chiclayo - Íllimo
Chongoyape

C H I C L A Y O - Í L L I M O



SISTEMA ELÉCTRICO: Chiclayo - Íllimo	**EMPRESA ELÉCTRICA:** ELECTRO NORTE S.A.			
	Sector Típico: 2	Leq: 8,40 km	Fecha: 12/99	Pág. 1/2

C H O N G O Y A P E

* Utilizado en Distribución

SISTEMA ELÉCTRICO: Chongoyape	EMPRESA ELÉCTRICA: ELECTRO NORTE S.A.			
	Sector Típico: 3	Leq: 0 km	Fecha: 12/99	Pág. 2/2

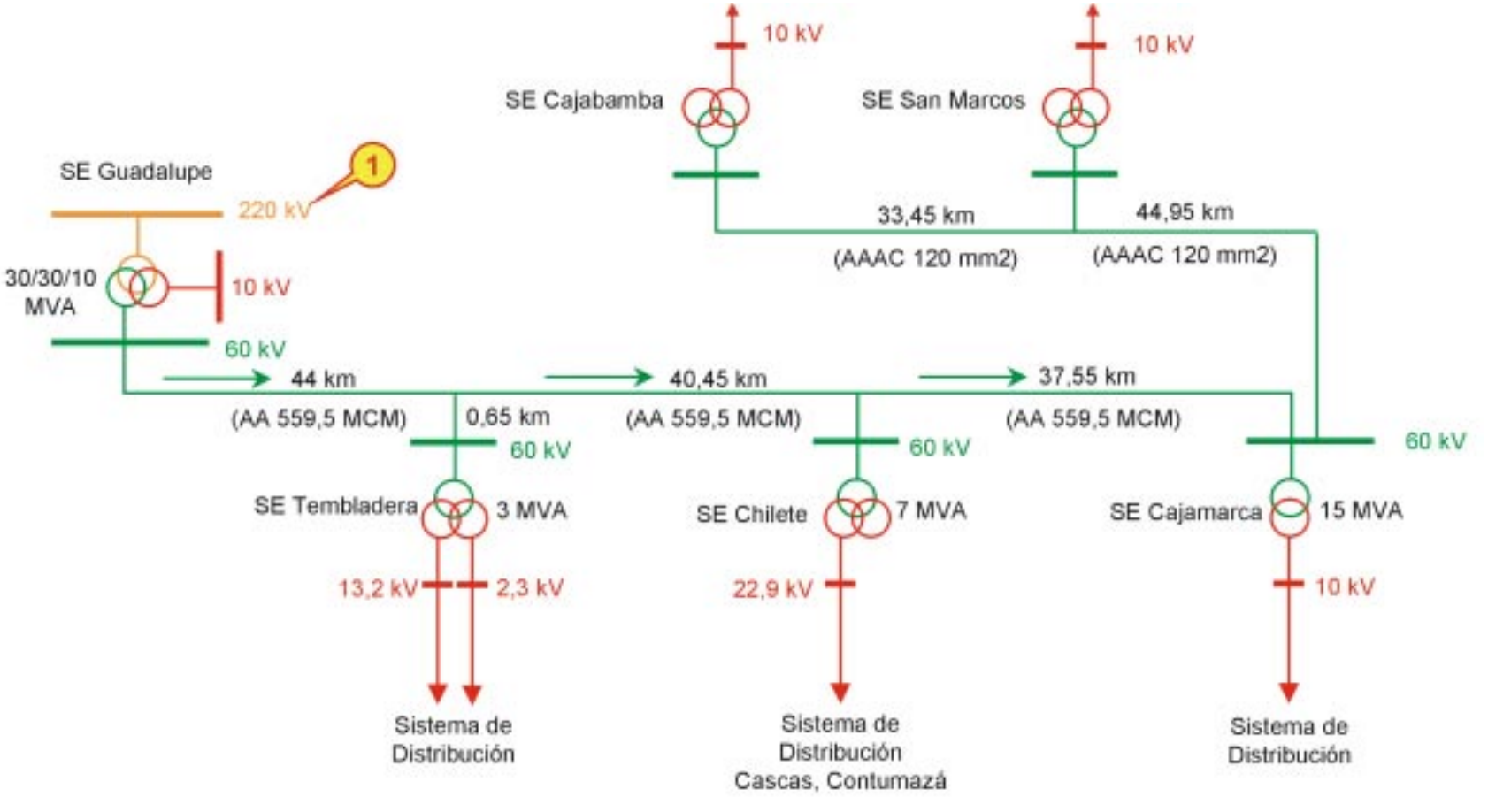
EMPRESA

E L E C T R O N O R T E M E D I O S. A.

SISTEMAS

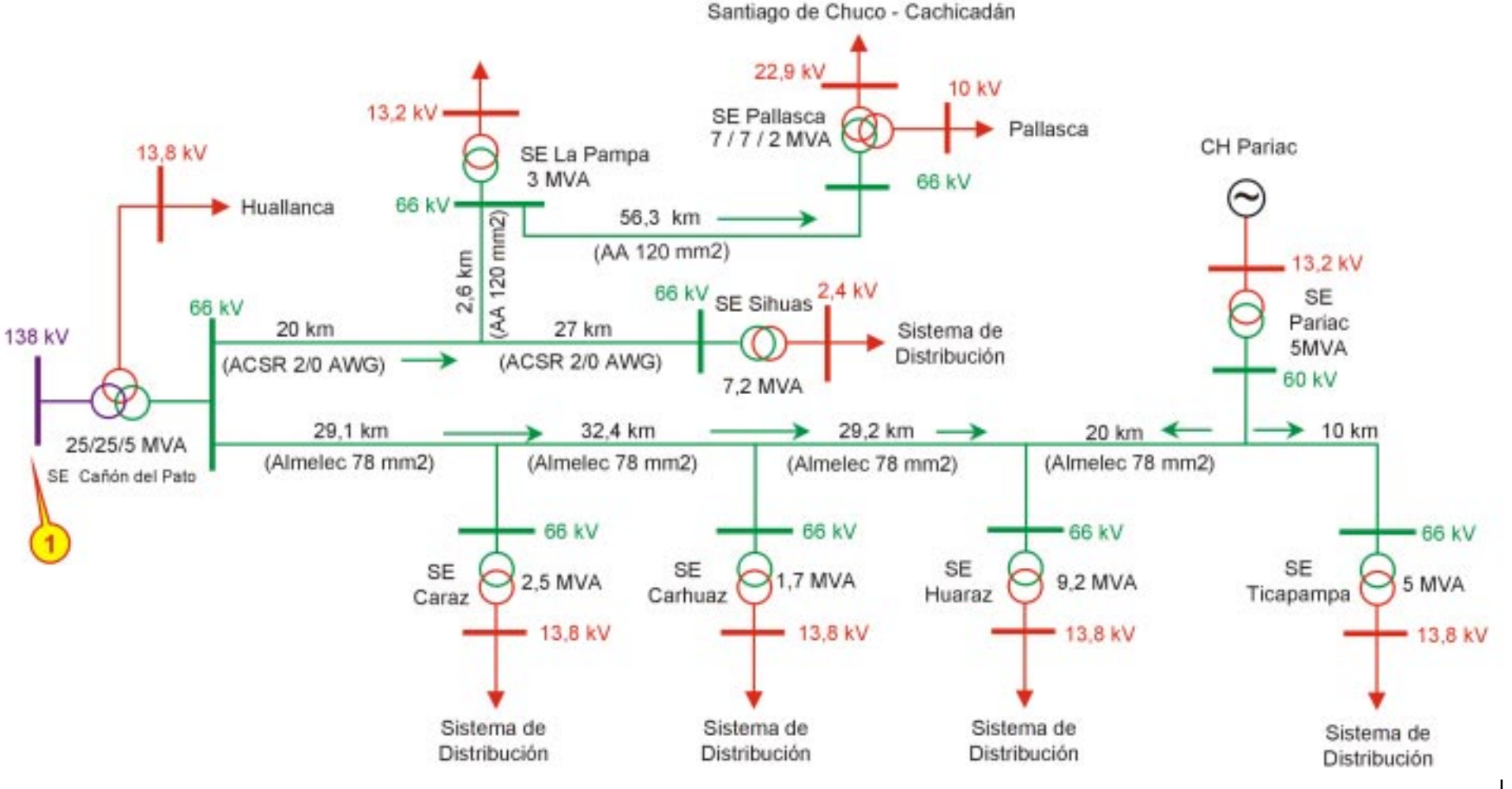
Cajamarca
Callejón de Huaylas
Cascas - Contumazá
Chimbote
Guadalupe - Chepén - Pacasmayo
Huarmey
Pallasca - Cachicadán
Trujillo

C A J A M A R C A



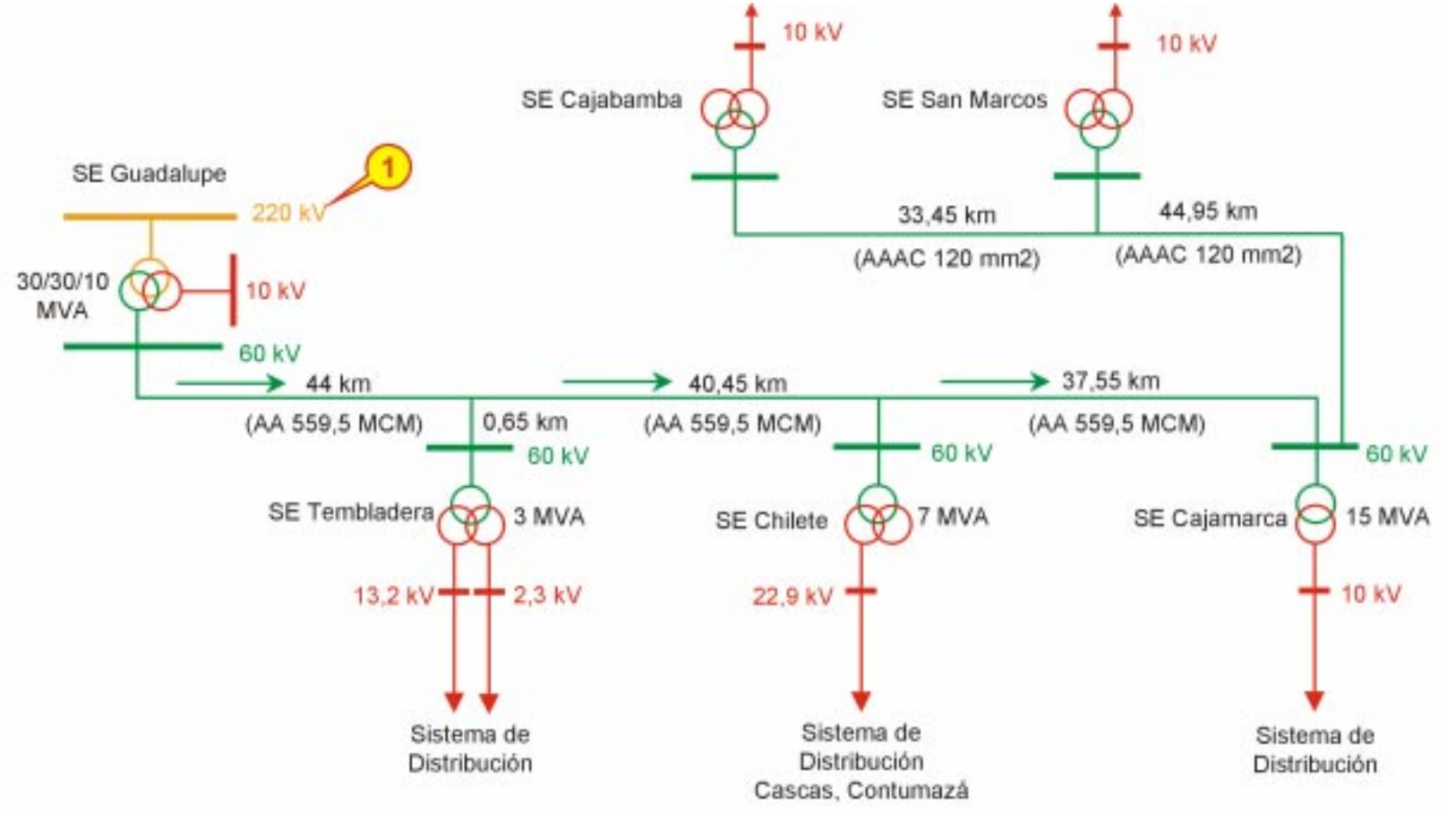
SISTEMA ELÉCTRICO: Cajamarca	**EMPRESA ELÉCTRICA:** ELECTRO NORTE MEDIO S.A.			
	Sector Típico: 2	Leq: 127,39 km	Fecha: 12/99	Pág. 1/8

CALLEJÓN DE HUAYLAS



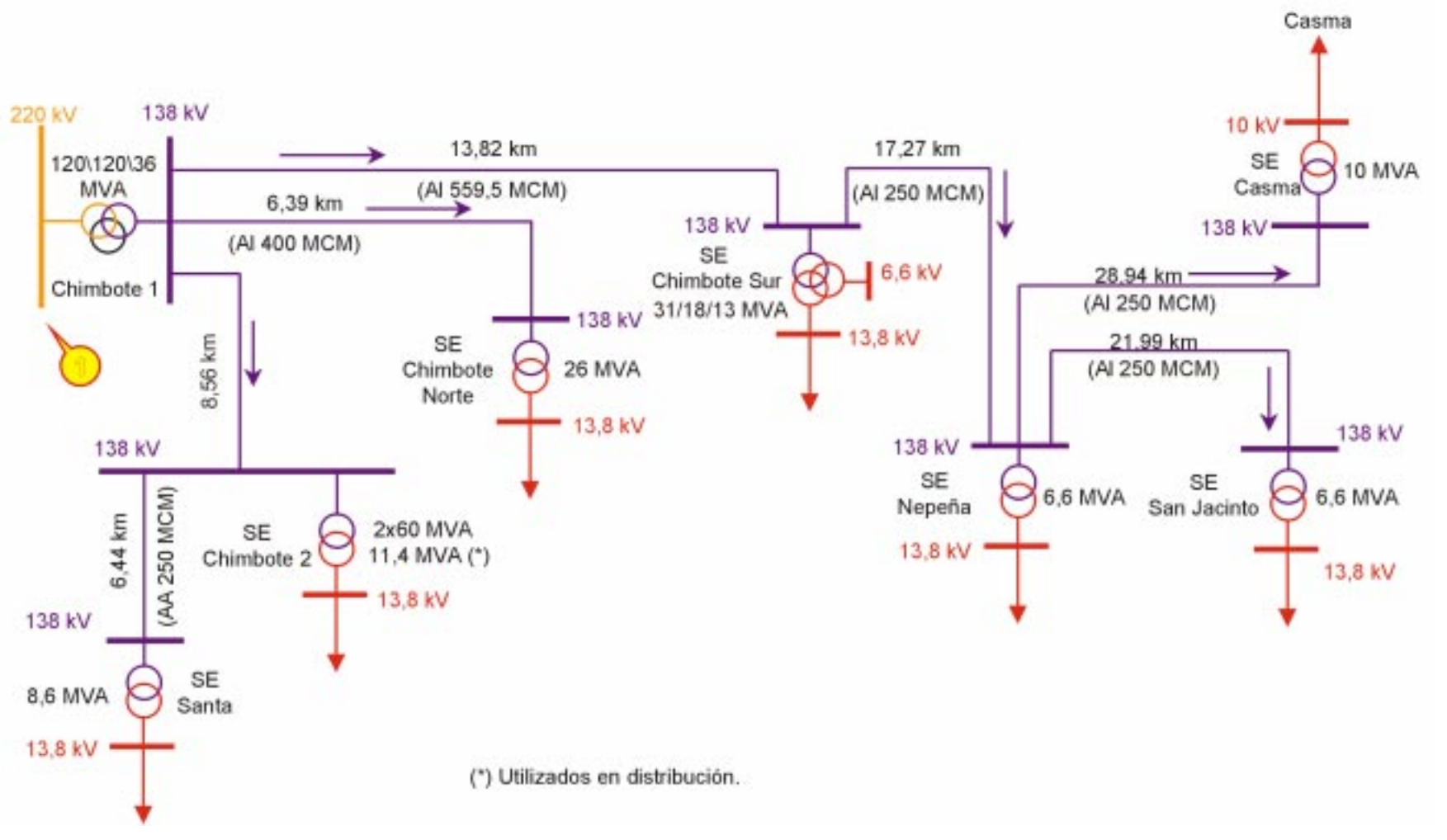
SISTEMA ELÉCTRICO: Callejón de Huaylas	**EMPRESA ELÉCTRICA:** ELECTRO NORTE MEDIO S.A.			
	Sector Típico: 2	Leq: 60,93 km	Fecha: 12/99	Pág. 2/8

C A S C A S - C O N T U M A Z Á



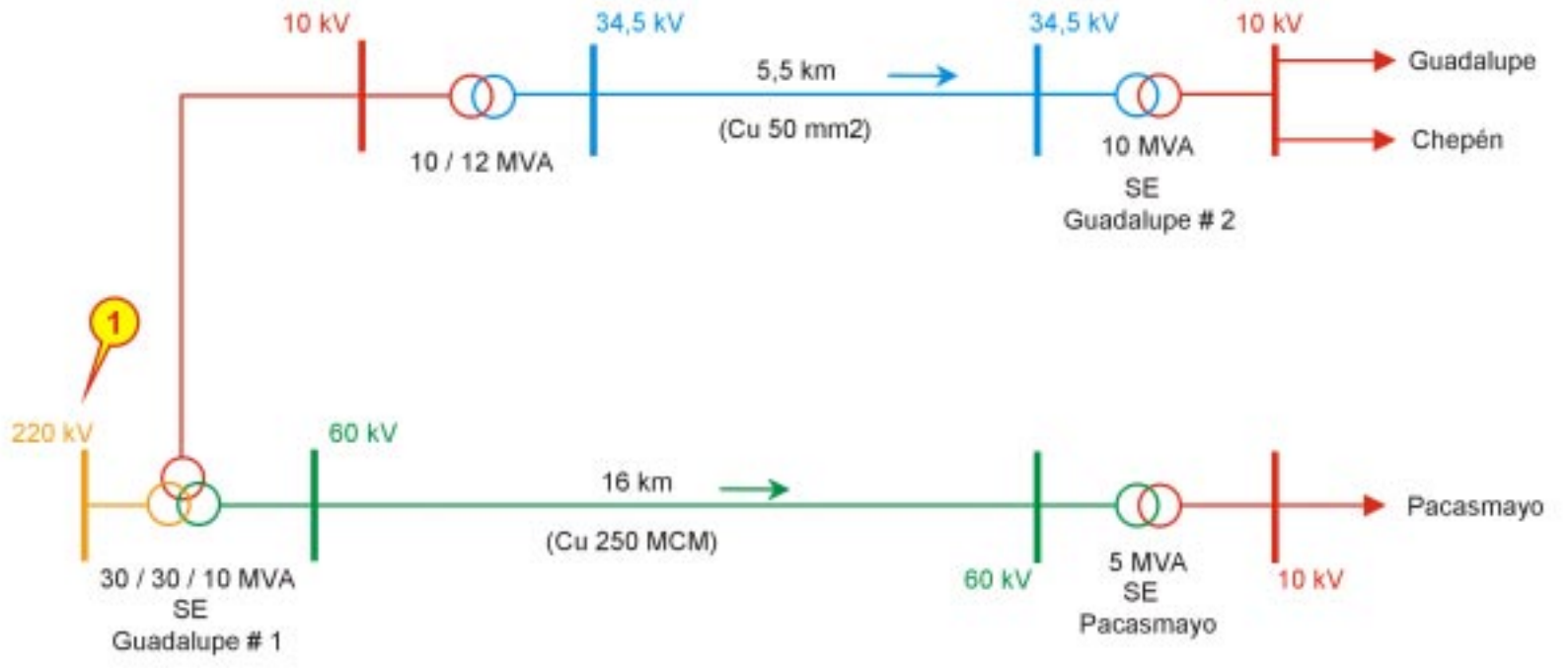
SISTEMA ELÉCTRICO: Cascas - Contumazá	**EMPRESA ELÉCTRICA:** ELECTRO NORTE MEDIO S.A.			
	Sector Típico: 3	Leq: 127,39 km	Fecha: 12/99	Pág. 3/8

C H I M B O T E



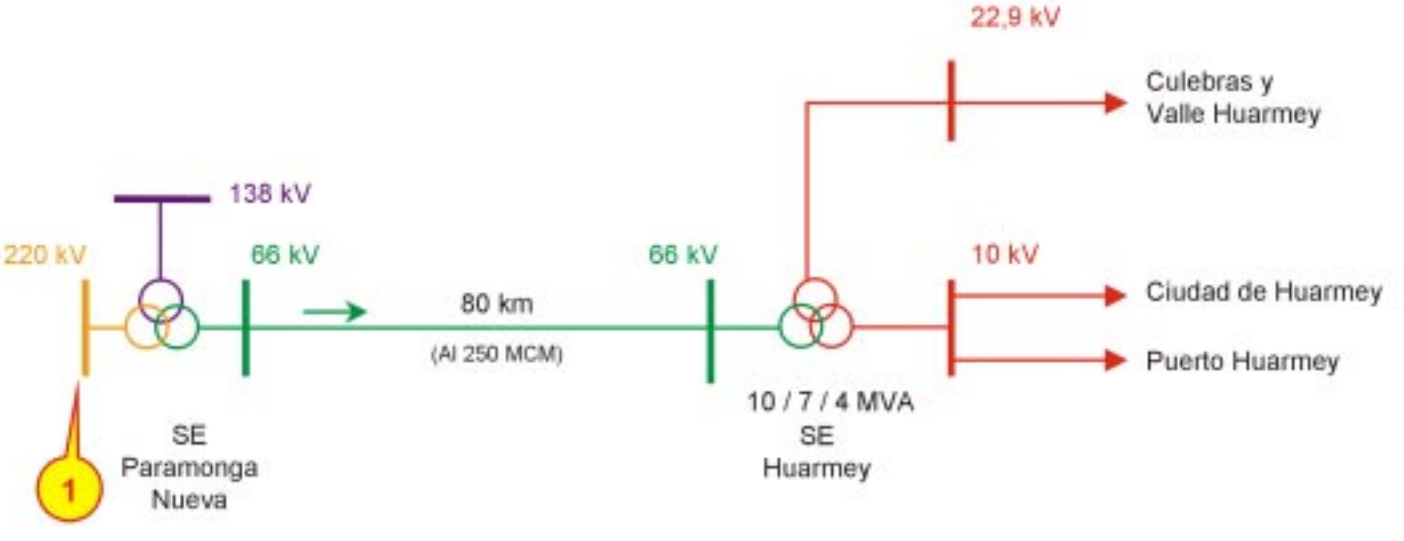
SISTEMA ELÉCTRICO: Chimbote	**EMPRESA ELÉCTRICA:** ELECTRO NORTE MEDIO S.A.		
	Sector Típico: 2	Leq: 19,73 km	Fecha: 12/99	Pág. 4/8

G U A D A L U P E - C H E P É N - P A C A S M A Y O



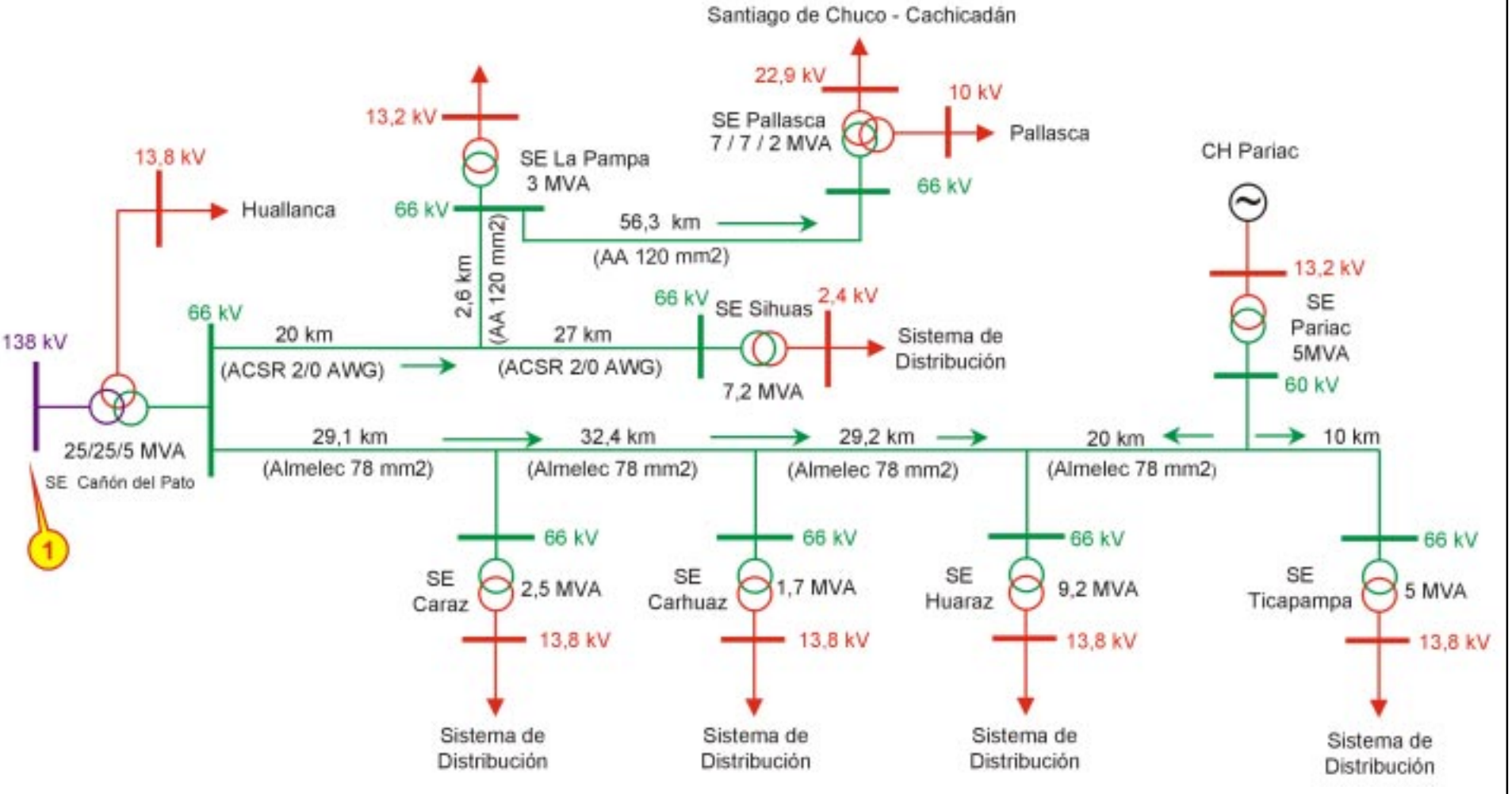
SISTEMA ELÉCTRICO: Guadalupe, Chepén y Pacasmayo	**EMPRESA ELÉCTRICA:** ELECTRO NORTE MEDIO S.A.			
	Sector Típico: 2	Leq: 9 km	Fecha: 12/99	Pág. 5/8

H U A R M E Y



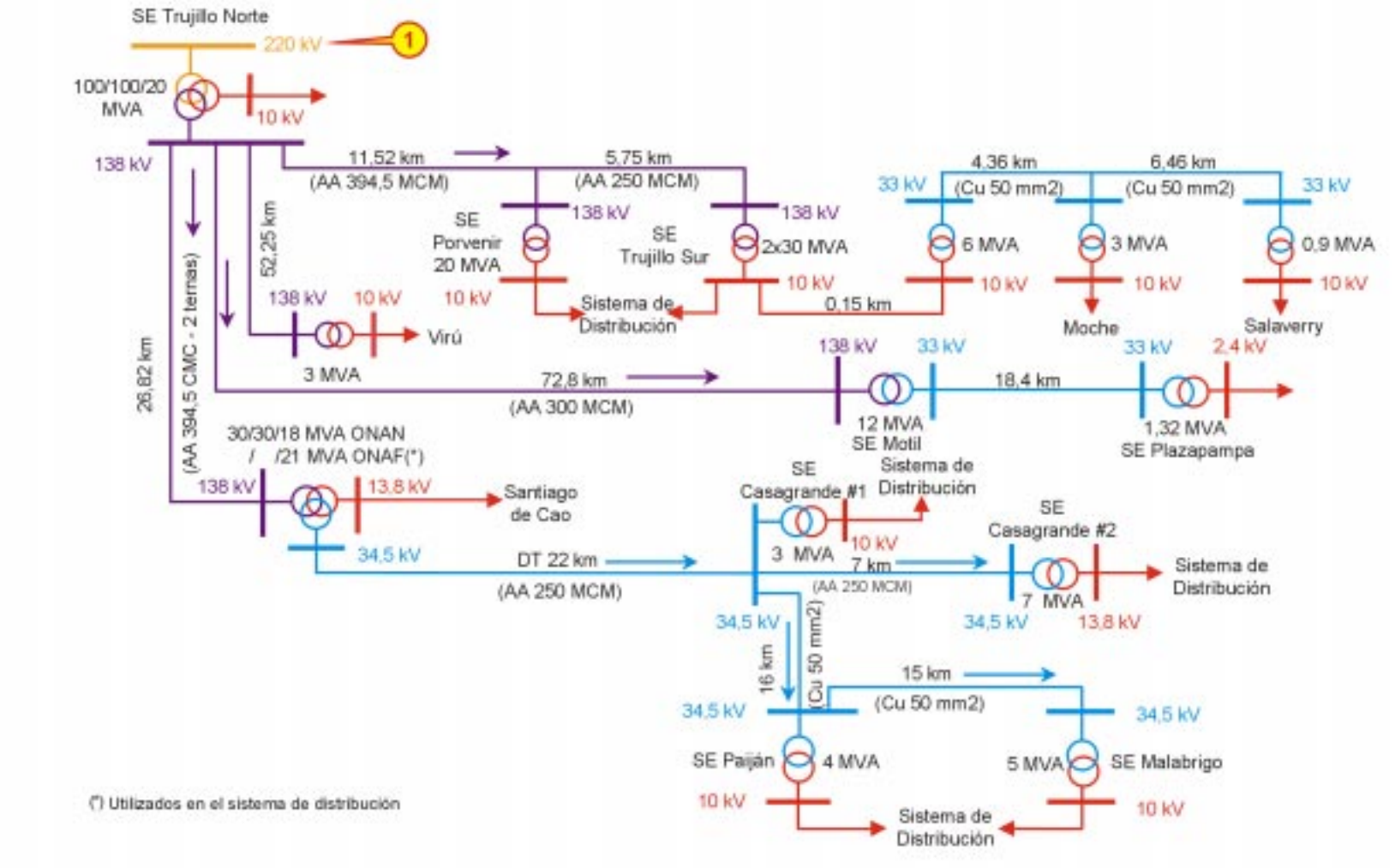
SISTEMA ELÉCTRICO: Huarmey	EMPRESA ELÉCTRICA: ELECTRO NORTE MEDIO S.A.			
	Sector Típico: 2	Leq: 80 km	Fecha: 12/99	Pág. 6/8

P A L L A S C A - C A C H I C A D Á N



SISTEMA ELÉCTRICO: Pallasca - Cachicadán	**EMPRESA ELÉCTRICA:** ELECTRO NORTE MEDIO S.A.			
	Sector Típico: 3	Leq: 60,93 km	Fecha: 12/99	Pág. 7/8

T R U J I L L O



SISTEMA ELÉCTRICO: Trujillo y Servicios	**EMPRESA ELÉCTRICA:** ELECTRO NORTE MEDIO S.A.		
	Sector Típico: 2	Leq: 24,53 km	Fecha: 12/99	Pág. 8/8

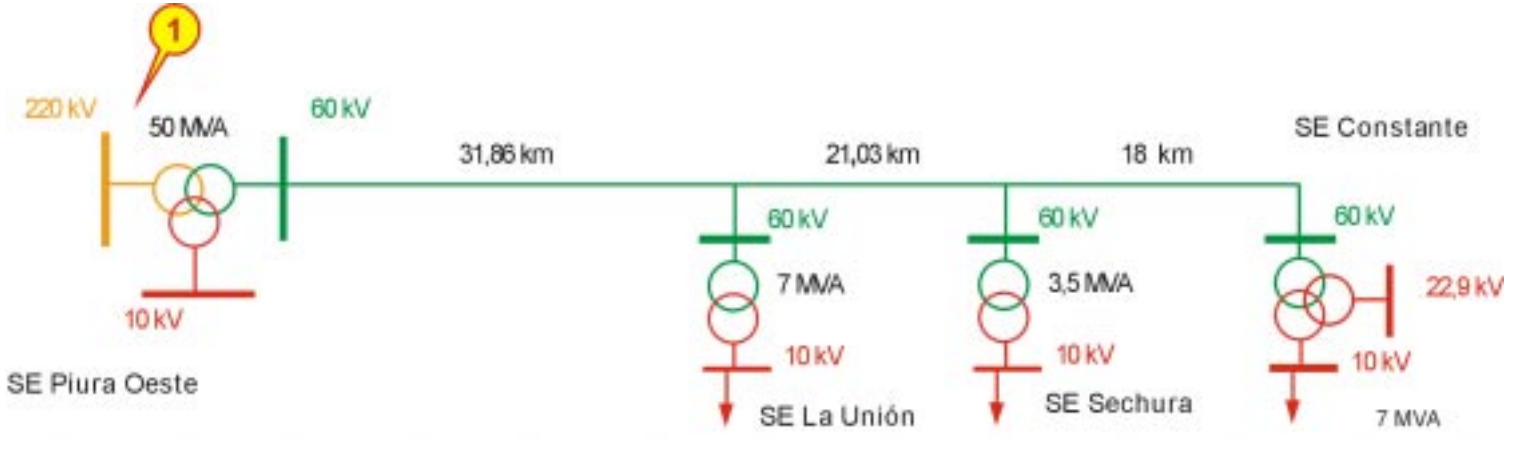
EMPRESA

E L E C T R O
N O R O E S T E S. A.

SISTEMAS

Bajo Piura
Chulucanas
Piura
Sullana - El Arenal - Paita
Talara
Tumbes

B A J O P I U R A

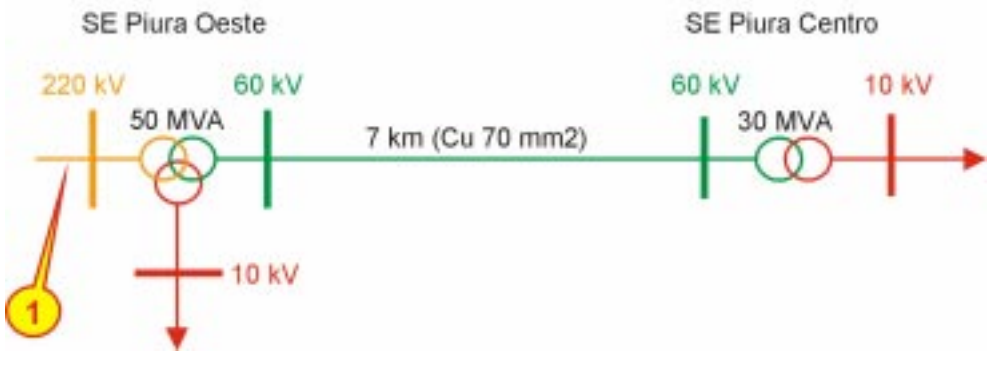


SISTEMA ELÉCTRICO: Bajo Piura	EMPRESA ELÉCTRICA: ELECTRO NOROESTE S.A.			
	Sector Típico: 2	Leq: 51,68 km	Fecha: 12/99	Pág. 1/6

C H U L U C A N A S

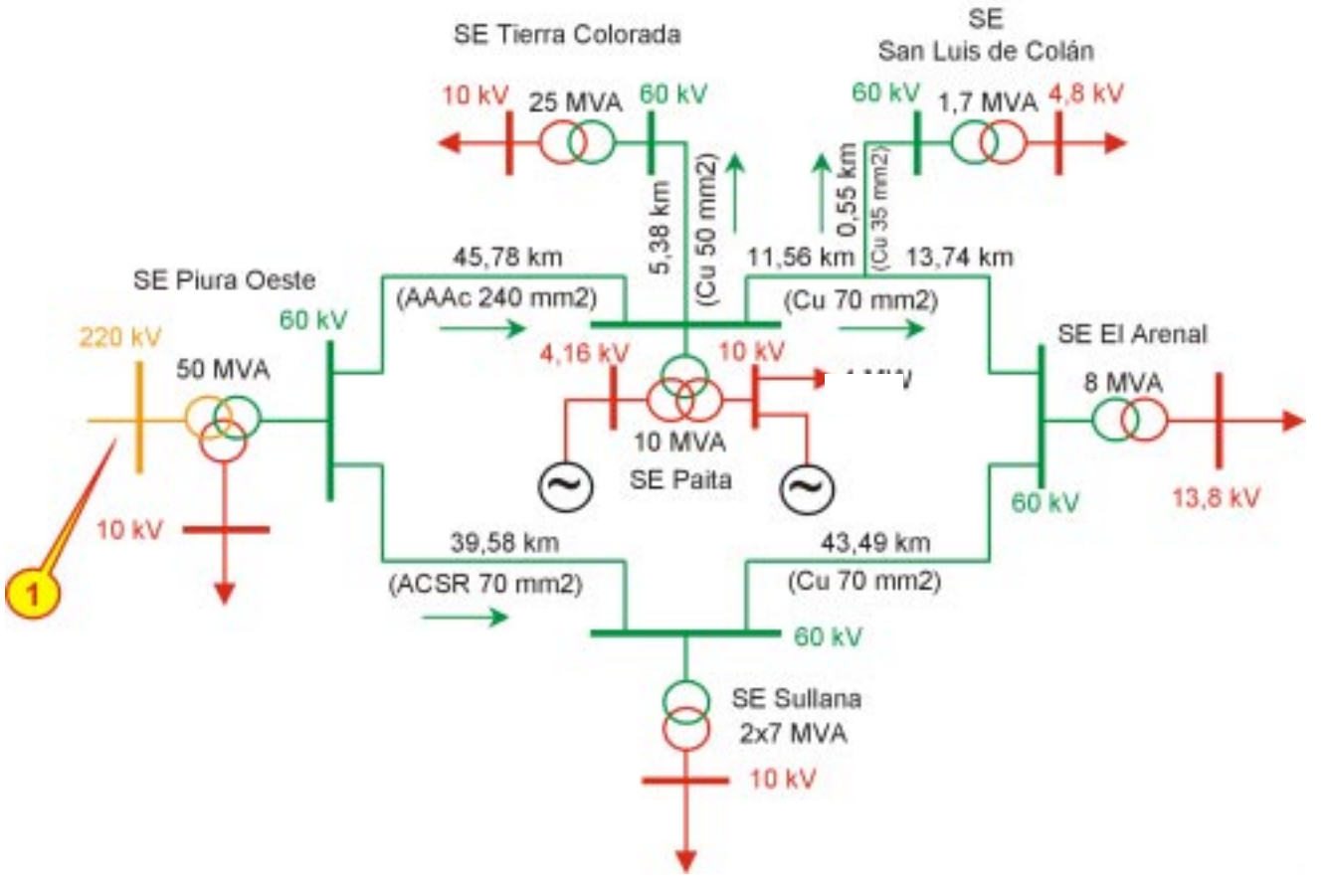
SISTEMA ELÉCTRICO: Chulucanas	EMPRESA ELÉCTRICA: ELECTRO NOROESTE S.A.			
	Sector Típico: 2	Leq: 60 km	Fecha: 12/99	Pág. 2/6

P I U R A



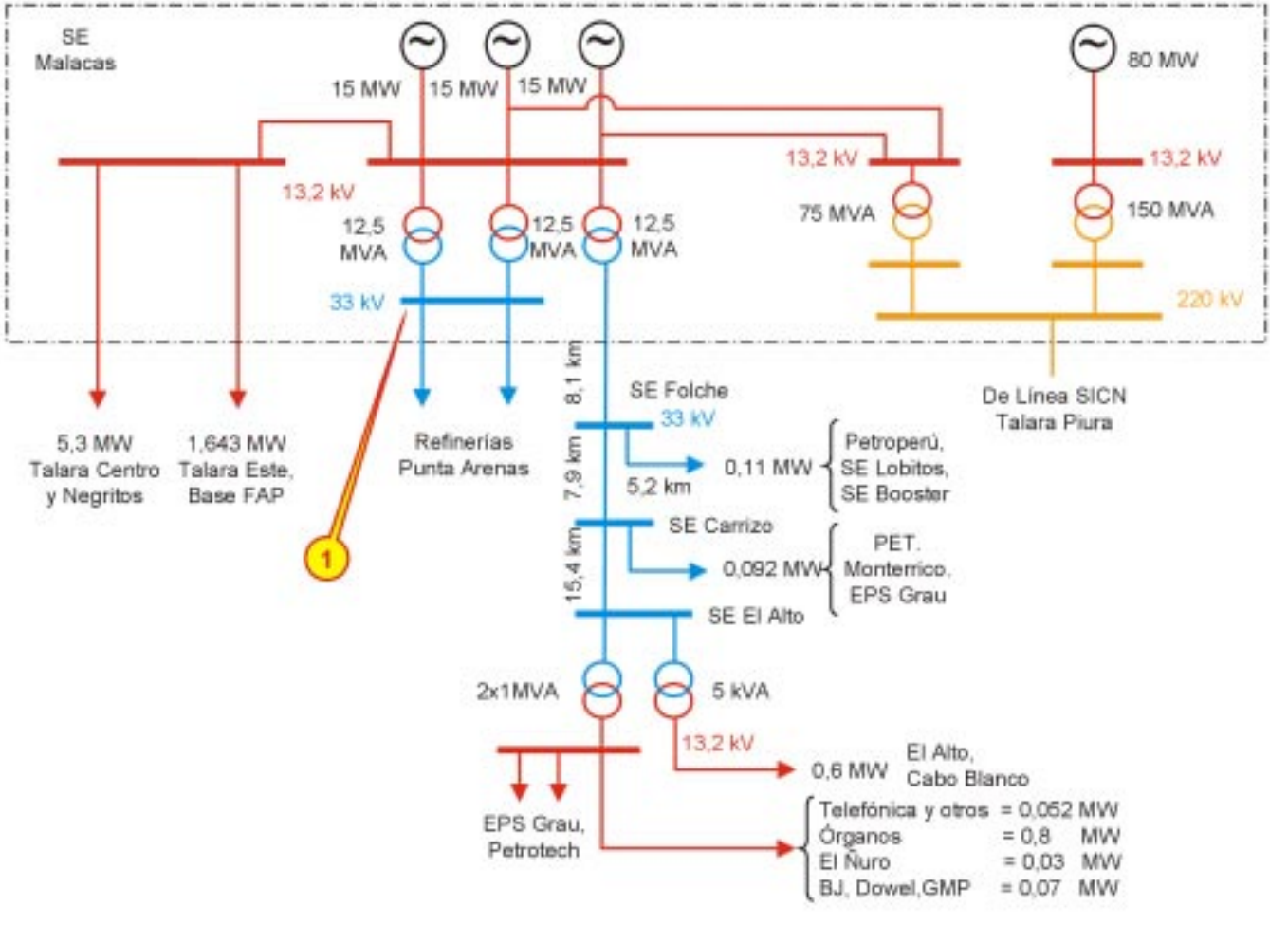
SISTEMA ELÉCTRICO: Piura	EMPRESA ELÉCTRICA: ELECTRO NOROESTE S.A.			
	Sector Típico: 2	Leq: 7 km	Fecha: 12/99	Pág. 3/6

SULLANA - EL ARENAL - PAITA



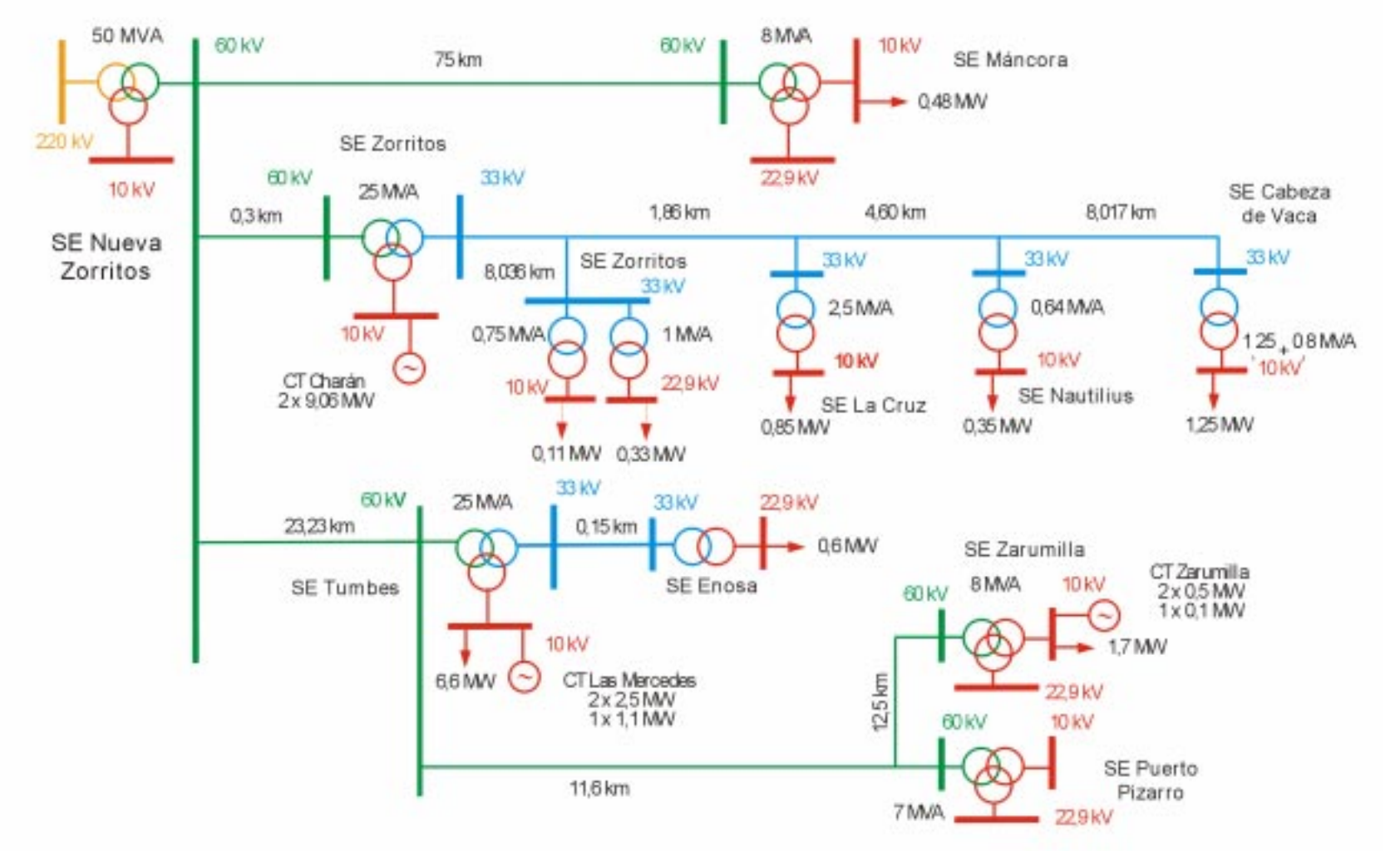
SISTEMA ELÉCTRICO: Sullana - El Arenal - Paita	**EMPRESA ELÉCTRICA:** ELECTRO NOROESTE S.A.			
	Sector Típico: 2	Leq: 50,39 km	Fecha: 12/99	Pág. 4/6

T A L A R A



SISTEMA ELÉCTRICO: Talara	**EMPRESA ELÉCTRICA:** ELECTRO NOROESTE S.A.			
	Sector Típico: 2	Leq: 5,88 km	Fecha: 12/99	Pág. 5/6

T U M B E S



SISTEMA ELÉCTRICO: Tumbes	**EMPRESA ELÉCTRICA:** ELECTRO NOROESTE S.A.			
	Sector Típico: 2	Leq: 25,36 km	Fecha: 12/99	Pág. 6/6

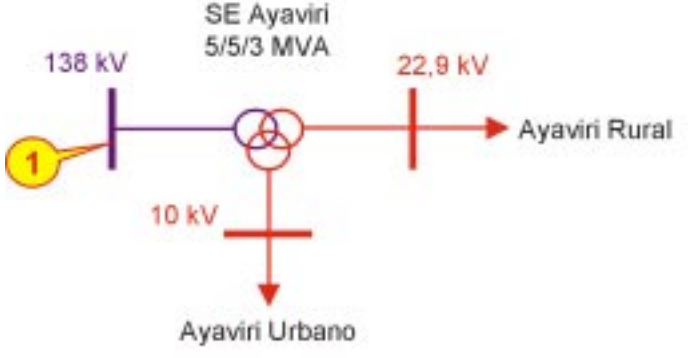
EMPRESA

E L E C T R O P U N O S. A.

SISTEMAS

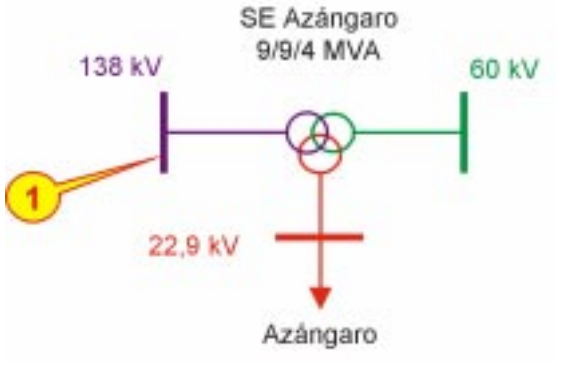
Ayaviri
Azángaro - Putina
Puno - Juliaca - Pomata

A Y A V I R I



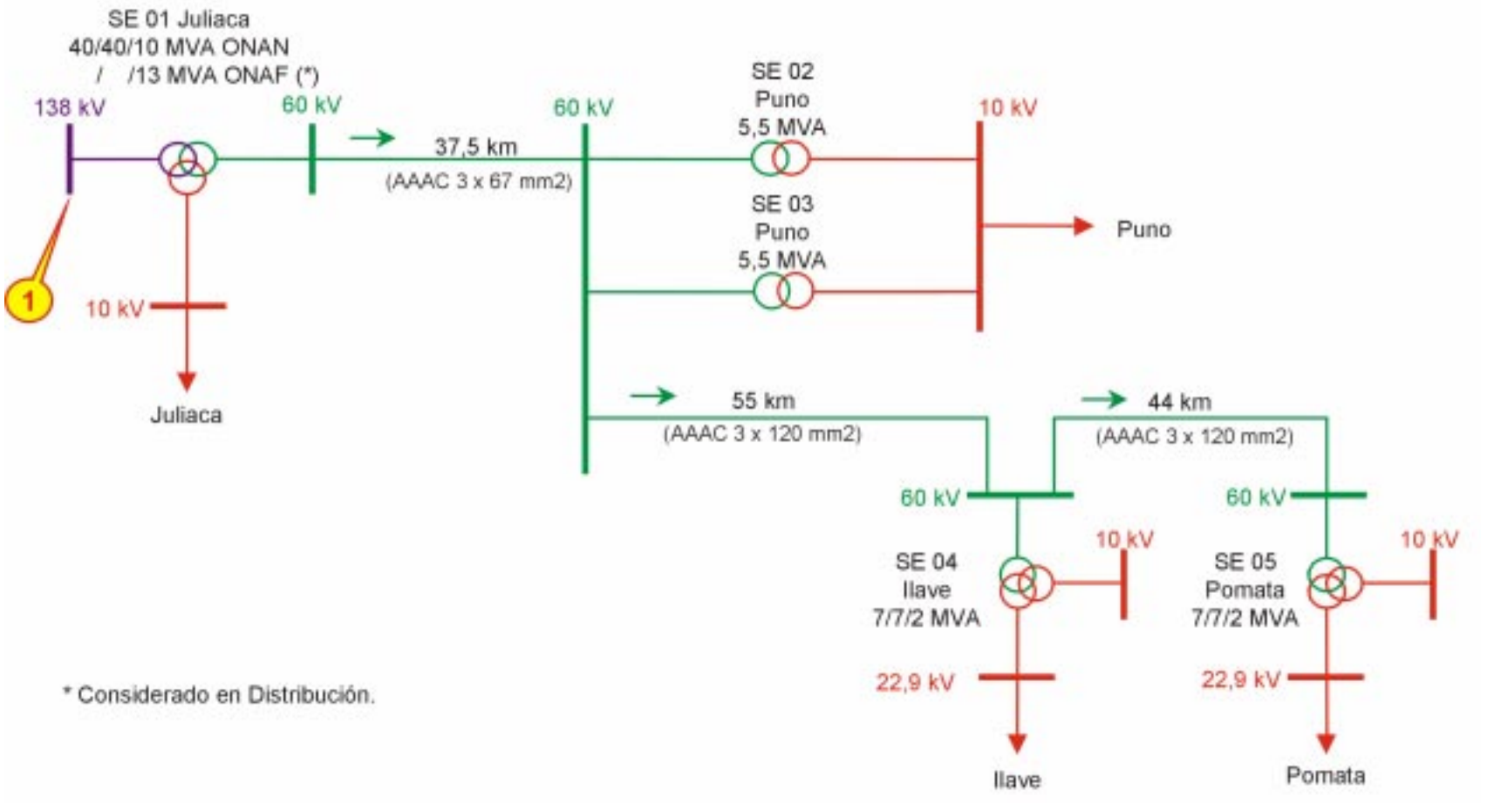
SISTEMA ELÉCTRICO: Ayaviri	**EMPRESA ELÉCTRICA:** ELECTRO PUNO S.A.			
	Sector Típico: 3	Leq: 0 km	Fecha: 12/99	Pág. 1/3

A Z Á N G A R O - P U T I N A



SISTEMA ELÉCTRICO: Azángaro - Putina	**EMPRESA ELÉCTRICA:** ELECTRO PUNO S.A.			
	Sector Típico: 3	Leq: 0 km	Fecha: 12/99	Pág. 2/3

P U N O - J U L I A C A



SISTEMA ELÉCTRICO: Puno, Juliaca, Huancané, Lampa, Chucuito, Ilave, Pomata, Yunguyo, Juli y Tinicachi	**EMPRESA ELÉCTRICA:** ELECTRO PUNO S.A.			
	Sector Típico: 2	Leq: 53,04 km	Fecha: 12/99	Pág. 3/3

EMPRESA

E L E C T R O S U R S. A.

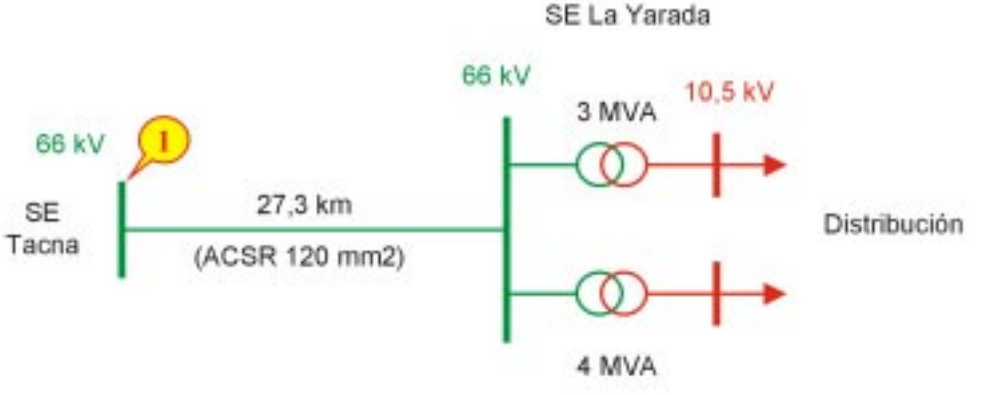
SISTEMAS

Ilo
La Yarada
Moquegua
Tacna
Tarata
Tomasiri

I L O

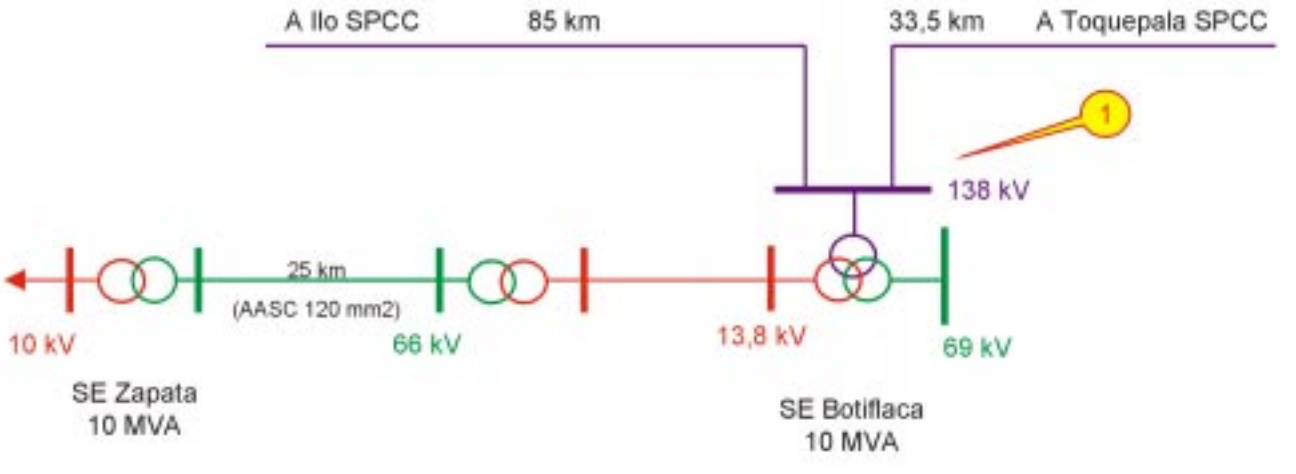
SISTEMA ELÉCTRICO: Ilo	**EMPRESA ELÉCTRICA:** ELECTROSUR S.A.			
	Sector Típico: 2	Leq: 0 km	Fecha: 12/99	Pág. 1/6

L A Y A R A D A



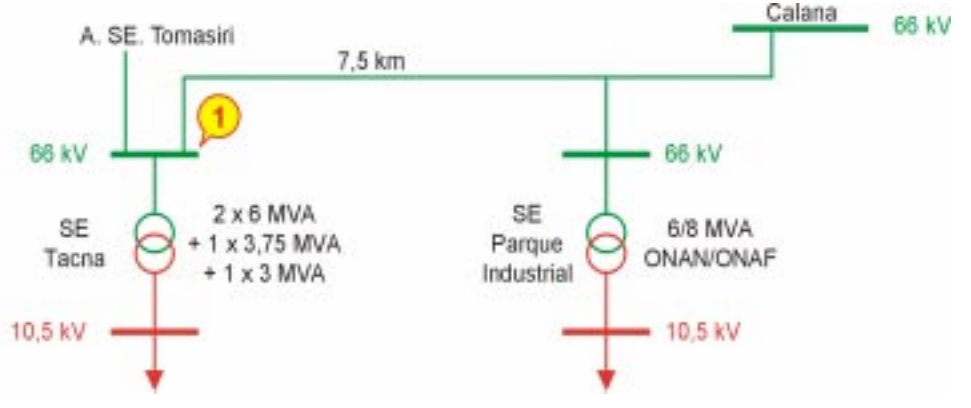
SISTEMA ELÉCTRICO: La Yarada	**EMPRESA ELÉCTRICA:** ELECTROSUR S.A.			
	Sector Típico: 2	Leq: 27,3 km	Fecha: 12/99	Pág. 2/6

M O Q U E G U A



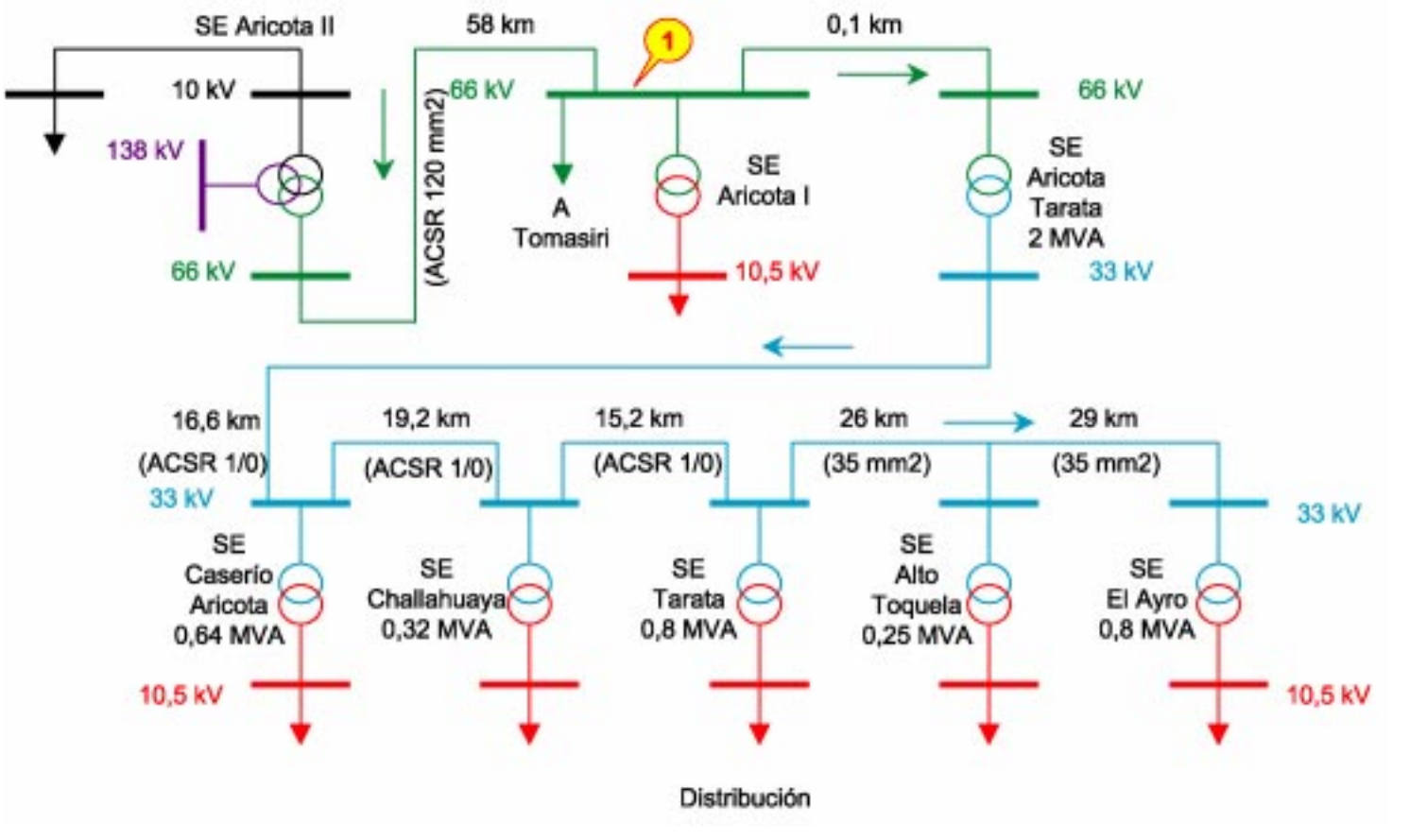
SISTEMA ELÉCTRICO: Moquegua	EMPRESA ELÉCTRICA: ELECTROSUR S.A.			
	Sector Típico: 2	Leq: 25 km	Fecha: 12/99	Pág. 3/6

T A C N A



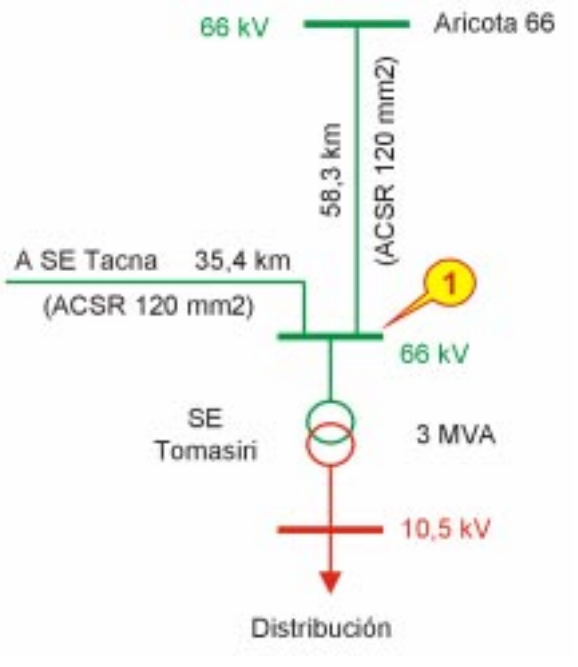
SISTEMA ELÉCTRICO: Tacna	EMPRESA ELÉCTRICA: ELECTROSUR S.A.			
	Sector Típico: 2	Leq: 2,24 km	Fecha: 12/99	Pág. 4/6

T A R A T A



SISTEMA ELÉCTRICO: Tarata	EMPRESA ELÉCTRICA: ELECTROSUR S.A.			
	Sector Típico: 3	Leq: 59,51 km	Fecha: 12/99	Pág. 5/6

T O M A S I R I



SISTEMA ELÉCTRICO: Tomasiri	**EMPRESA ELÉCTRICA:** ELECTROSUR S.A.			
	Sector Típico: 3	Leq: 0 km	Fecha: 12/99	Pág. 6/6

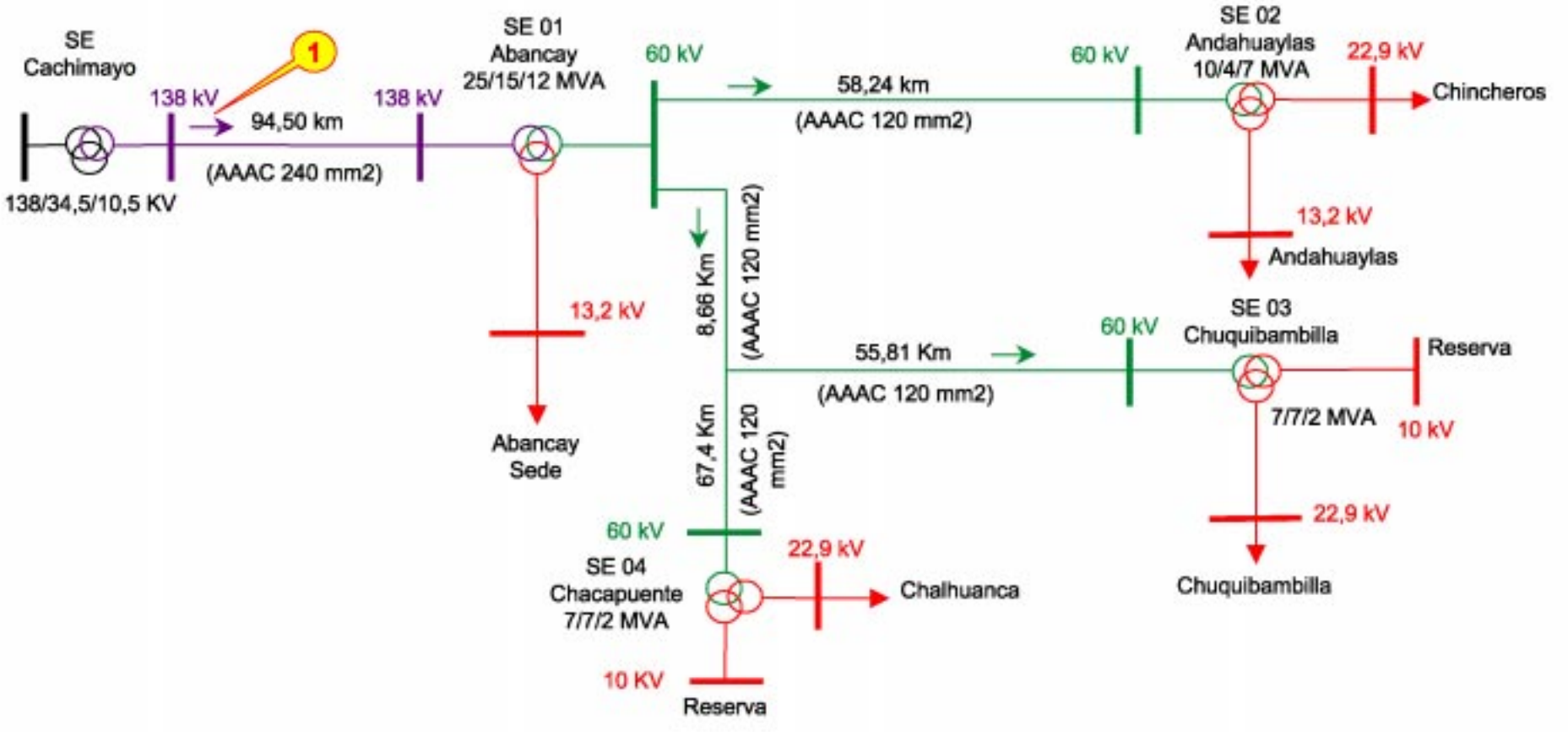
EMPRESA

E L E C T R O
S U R E S T E S. A.

SISTEMAS

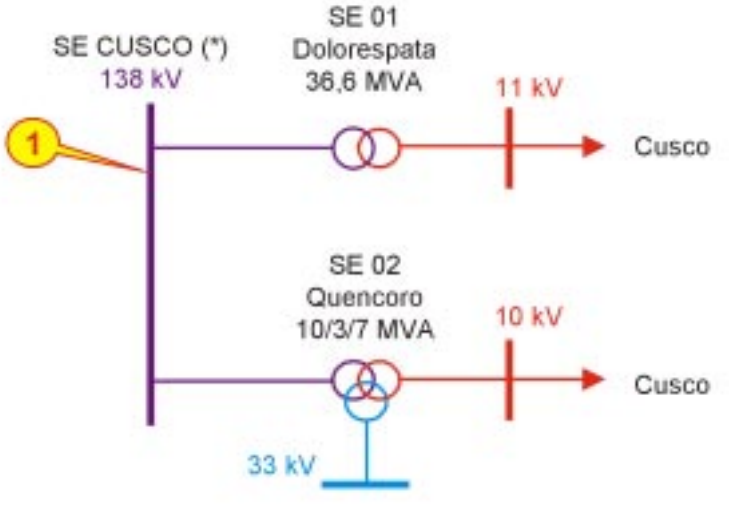
Abancay
Cusco
La Convención
Valle Sagrado 1
Valle Sagrado 2
Vilcanota - Sicuani
Yauri

ABANCAY



SISTEMA ELÉCTRICO: Abancay, Andahuaylas, Chincheros, Grau y Chalhuanca	**EMPRESA ELÉCTRICA:** ELECTRO SUR ESTE S.A.			
	Sector Típico: 3	Leq: 150,74 km	Fecha: 12/99	Pág. 1/7

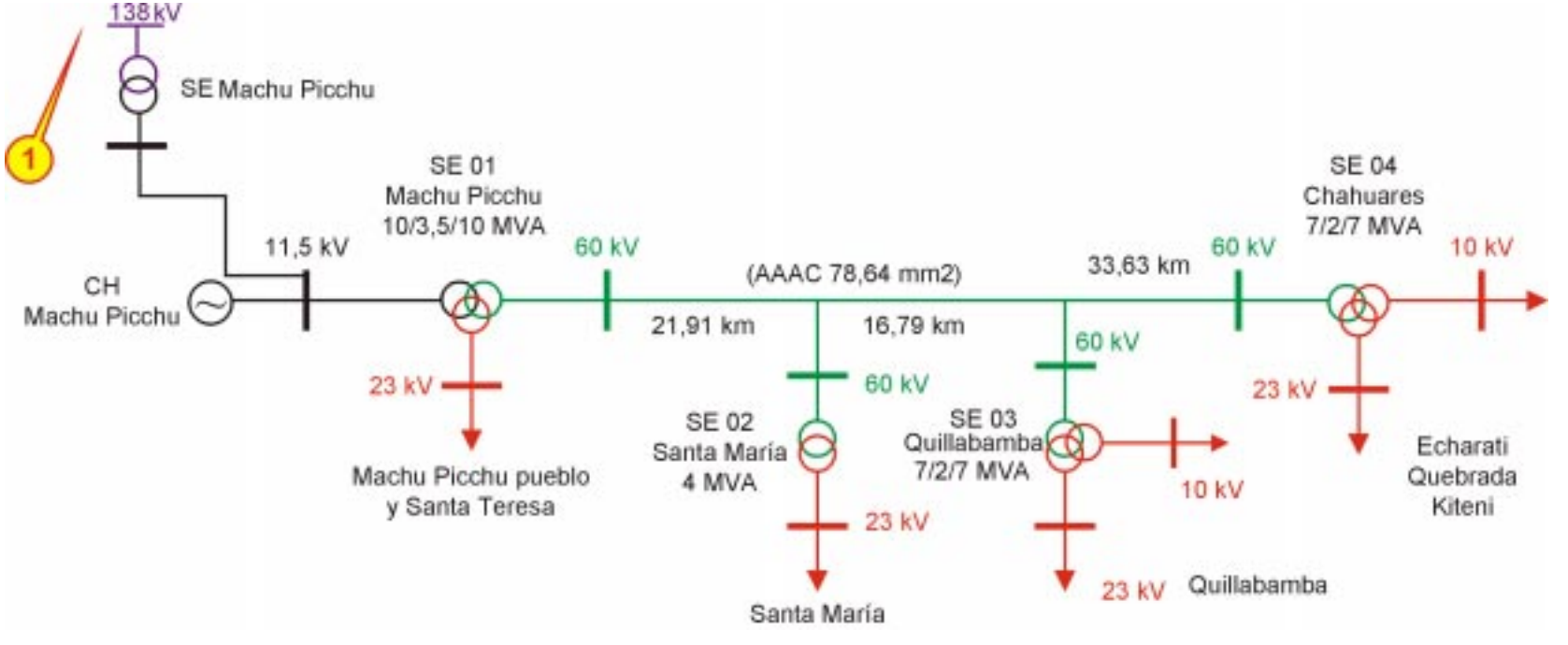
C U S C O



* Considerada una sola barra según Resolución. Constituida por las SE Base Dolorespata 138 KV y Quecoro 138 KV.

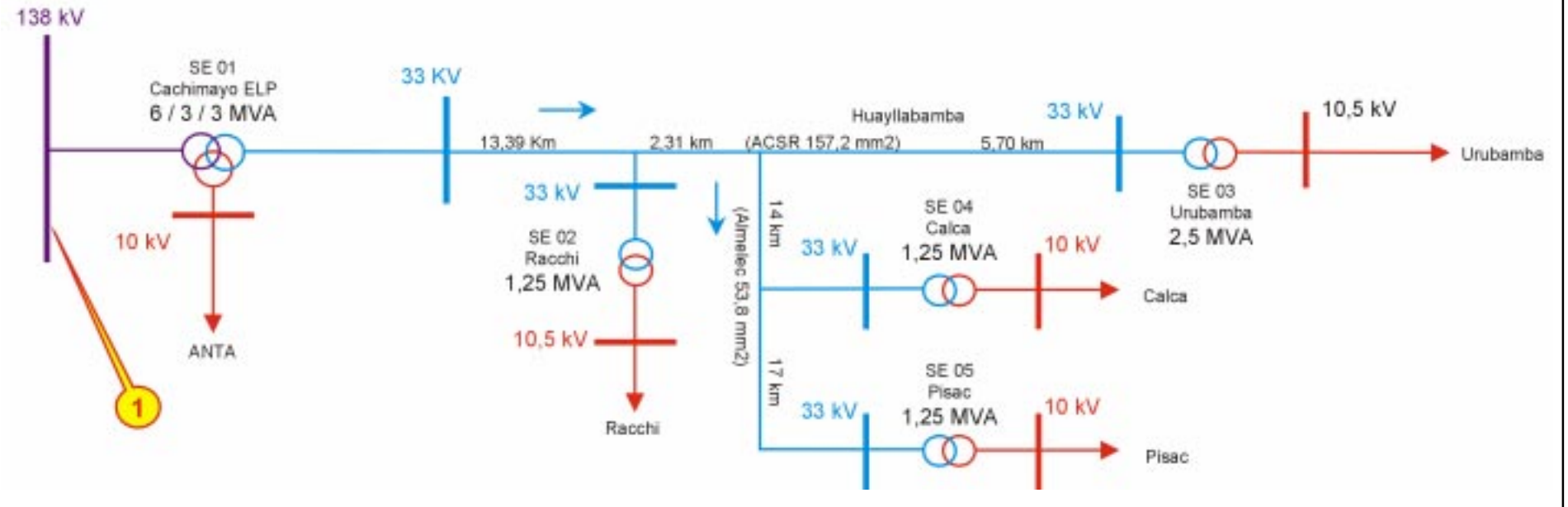
SISTEMA ELÉCTRICO: Cusco	**EMPRESA ELÉCTRICA:** ELECTRO SUR ESTE S.A.			
	Sector Típico: 2	Leq: 0 km	Fecha: 12/99	Pág. 2/7

L A C O N V E N C I Ó N



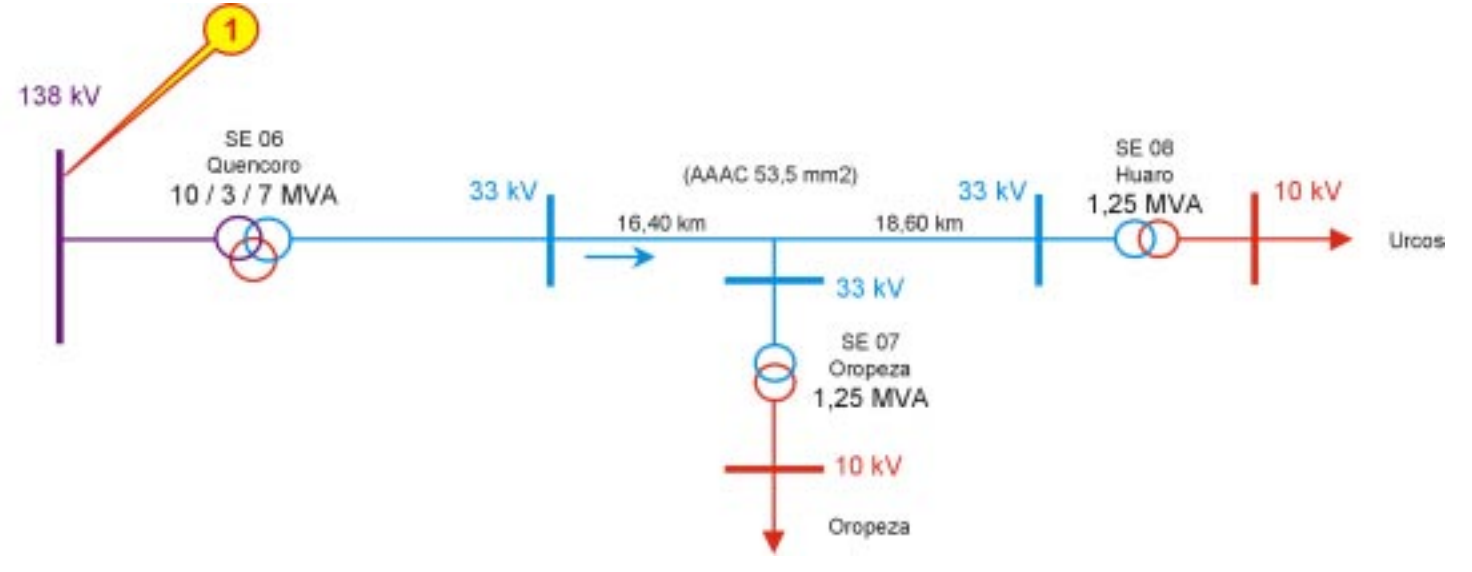
SISTEMA ELÉCTRICO: La Convención	**EMPRESA ELÉCTRICA:** ELECTRO SUR ESTE S.A.			
	Sector Típico: 2	Leq: 40,23 km	Fecha: 12/99	Pág. 3/7

V A L L E S A G R A D O 1



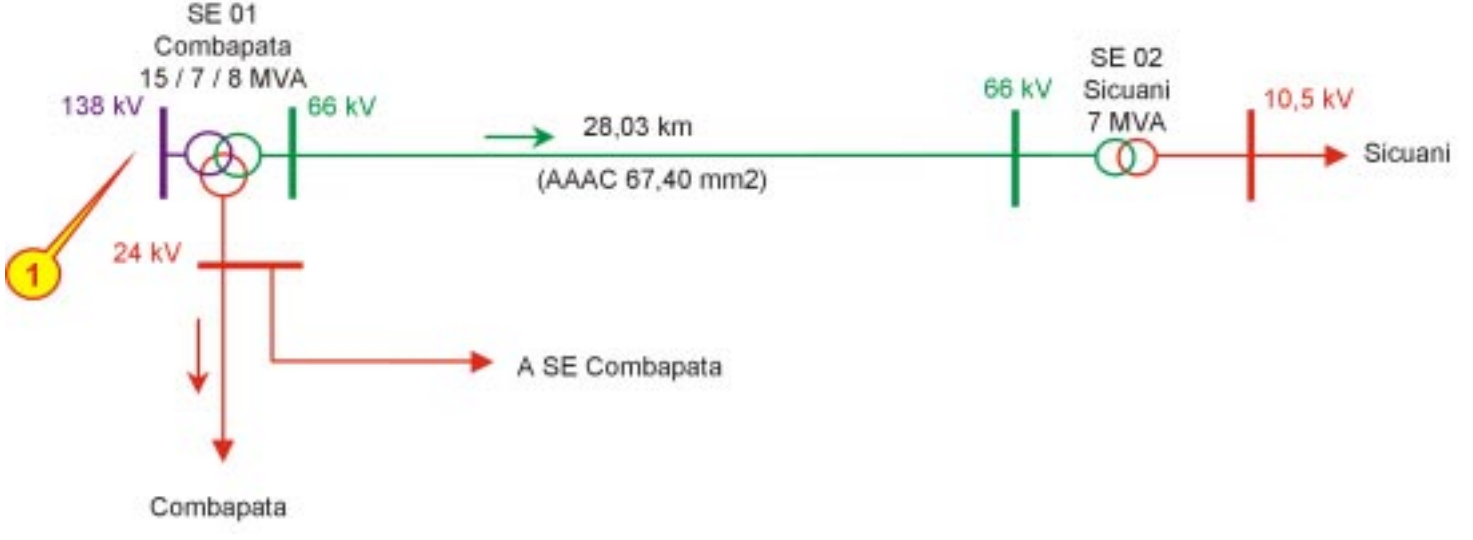
SISTEMA ELÉCTRICO: Valle Sagrado 1, Urubamba Anta - Rachi - Calca - Pisac	**EMPRESA ELÉCTRICA:** ELECTRO SUR ESTE S.A.			
	Sector Típico: 4	Leq: 17,92 km	Fecha: 12/99	Pág. 4/7

V A L L E S A G R A D O 2



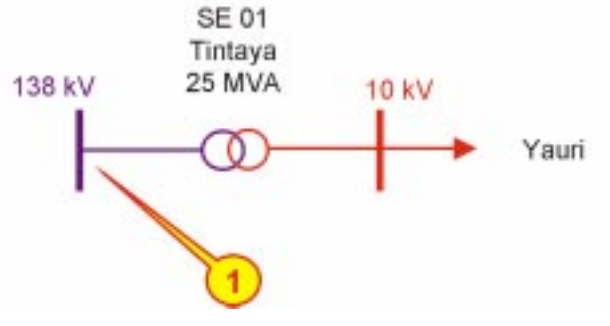
SISTEMA ELÉCTRICO: Valle Sagrado 2, Urcos Oropeza	**EMPRESA ELÉCTRICA:** ELECTRO SUR ESTE S.A.			
	Sector Típico: 4	Leq: 25,70 km	Fecha: 12/99	Pág. 5/7

V I L C A N O T A - S I C U A N I



SISTEMA ELÉCTRICO: Vilcanota, Sicuani	**EMPRESA ELÉCTRICA:** ELECTRO SUR ESTE S.A.			
	Sector Típico: 4	Leq: 13,08 km	Fecha: 12/99	Pág. 6/7

Y A U R I



SISTEMA ELÉCTRICO: Yauri	**EMPRESA ELÉCTRICA:** ELECTRO SUR ESTE S.A.			
	Sector Típico: 2	Leq: 0 km	Fecha: 12/99	Pág. 7/7

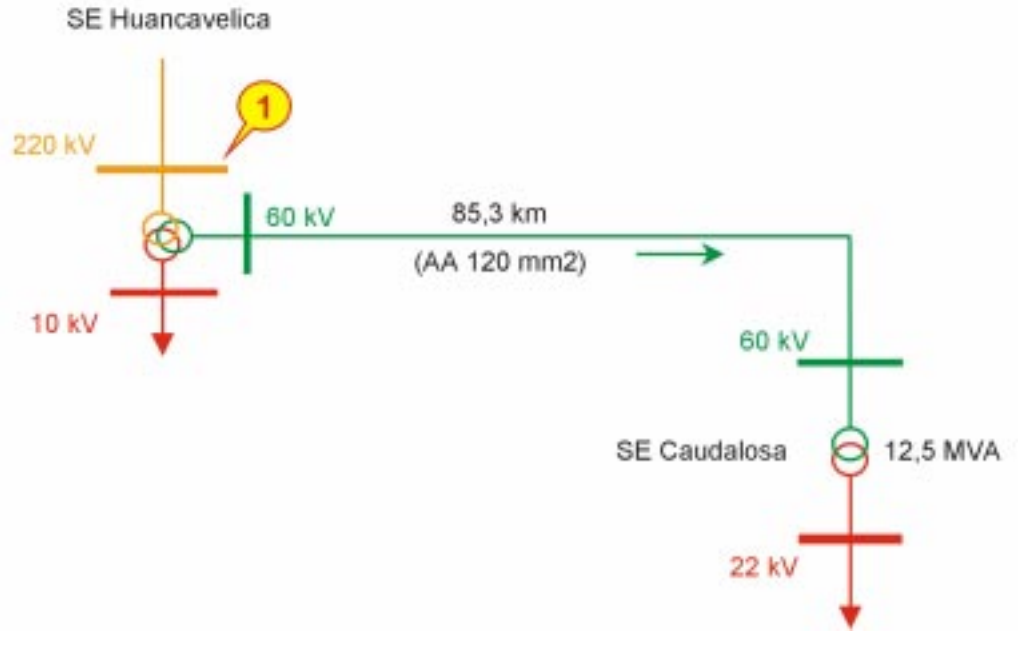
EMPRESA

E L E C T R O S U R M E D I O S. A.

SISTEMAS

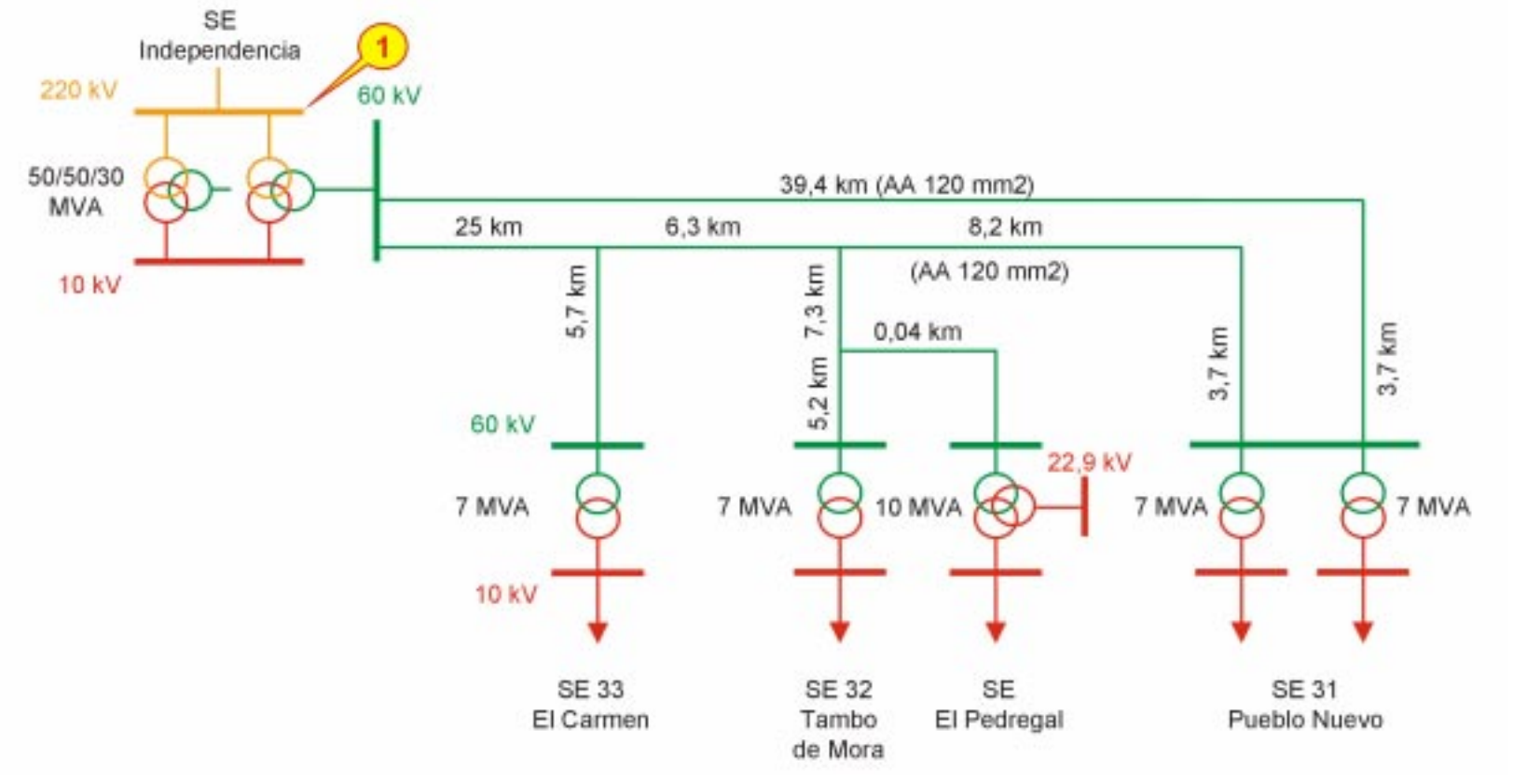
Castrovirreyna
Chincha
Córdova - Querco
Huaytará - Chocorvos
Ica
Ingenio - Changuillo
Nazca - Palpa
Pisco

C A S T R O V I R R E Y N A



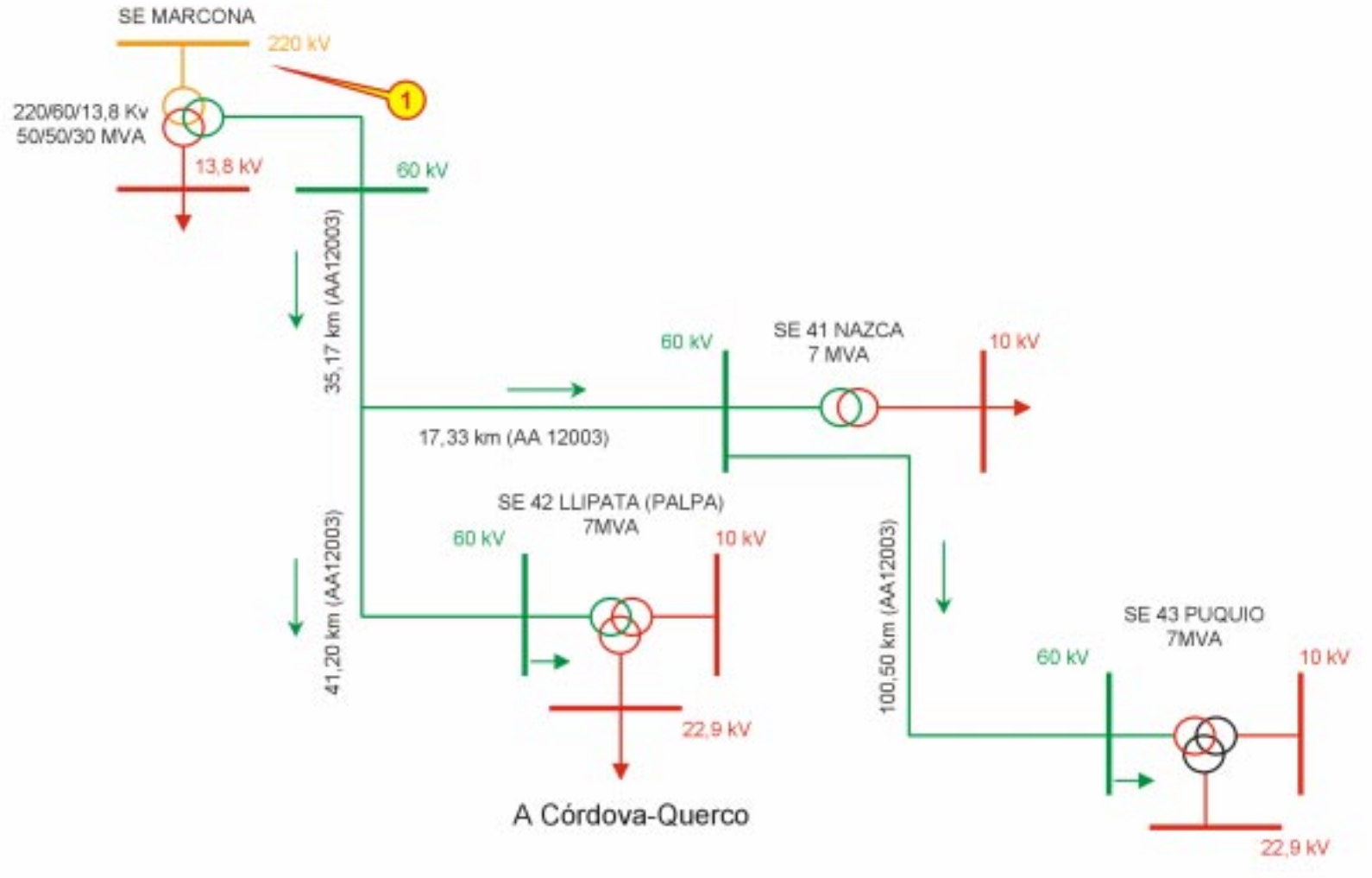
SISTEMA ELÉCTRICO: Castrovirreyna	**EMPRESA ELÉCTRICA:** ELECTRO SUR MEDIO S.A.			
	Sector Típico: 4	Leq: 85,3 km	Fecha: 12/99	Pág. 1/8

C H I N C H A



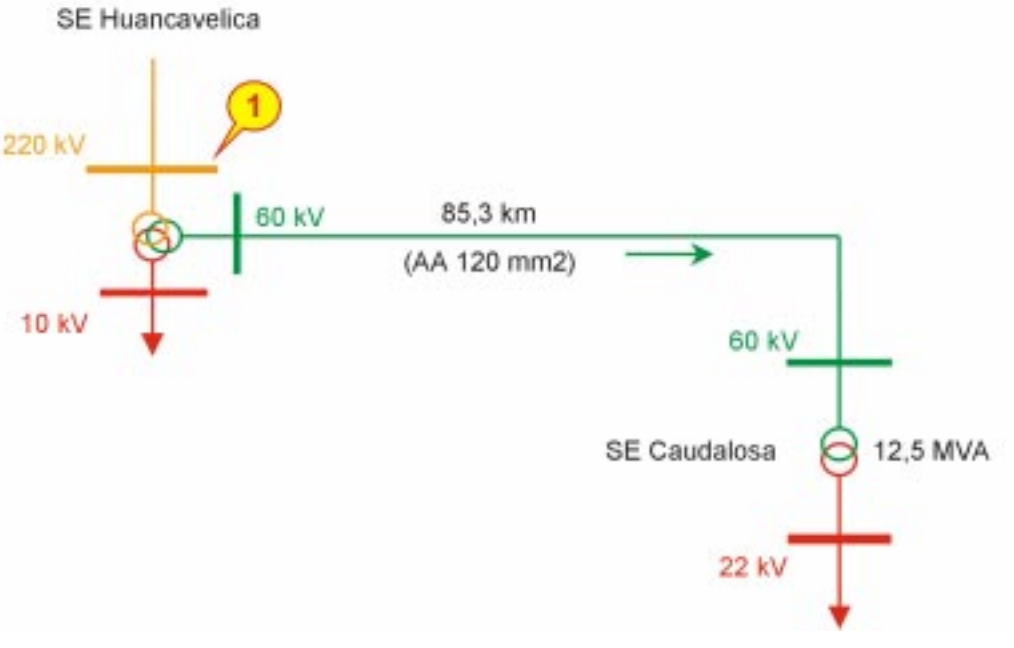
SISTEMA ELÉCTRICO: Chincha	**EMPRESA ELÉCTRICA:** ELECTRO SUR MEDIO S.A.			
	Sector Típico: 2	Leq: 39,77 km	Fecha: 12/99	Pág. 2/8

C Ó R D O V A - Q U E R C O



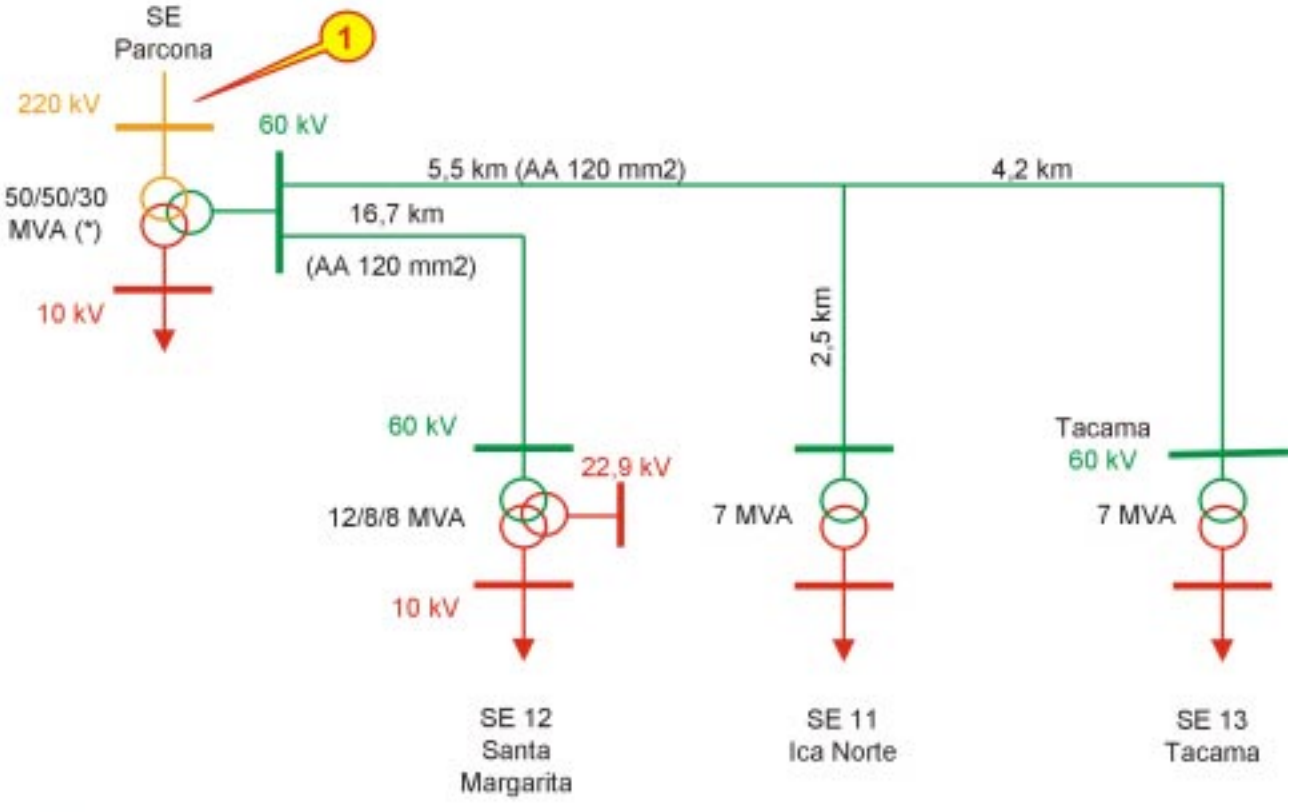
SISTEMA ELÉCTRICO: Córdova- Querco	**EMPRESA ELÉCTRICA:** ELECTRO SUR MEDIO S.A.			
	Sector Típico: 3	Leq: 93,96 km	Fecha: 12/99	Pág. 3/8

H U A Y T A R Á - C H O C O R V O S



SISTEMA ELÉCTRICO: Huaytará - Chocorvos	**EMPRESA ELÉCTRICA:** ELECTRO SUR MEDIO S.A.			
	Sector Típico: 3	Leq: 85,3 km	Fecha: 12/99	Pág. 4/8

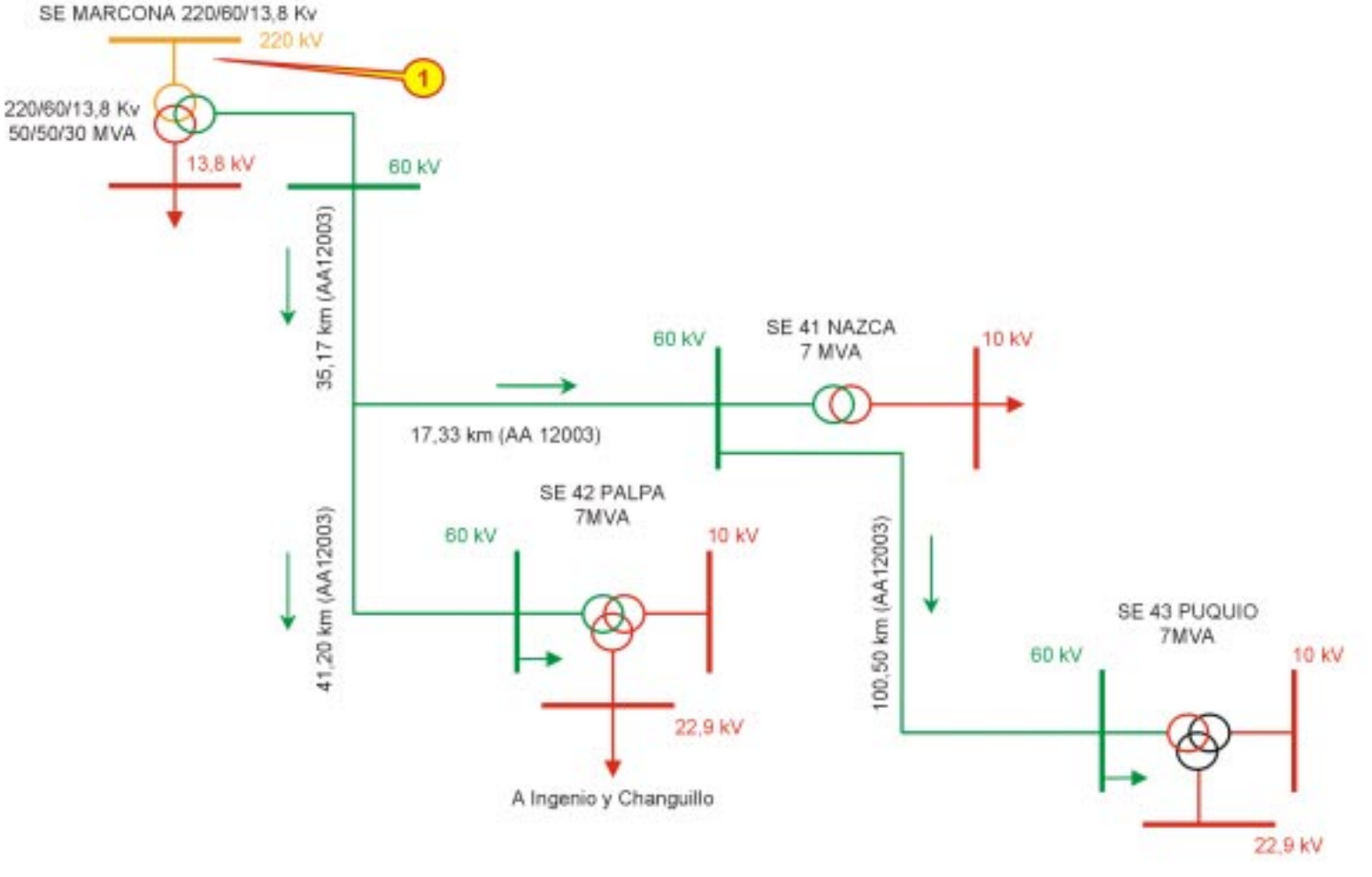
I C A



(*) Se considera 20 MVA en distribución

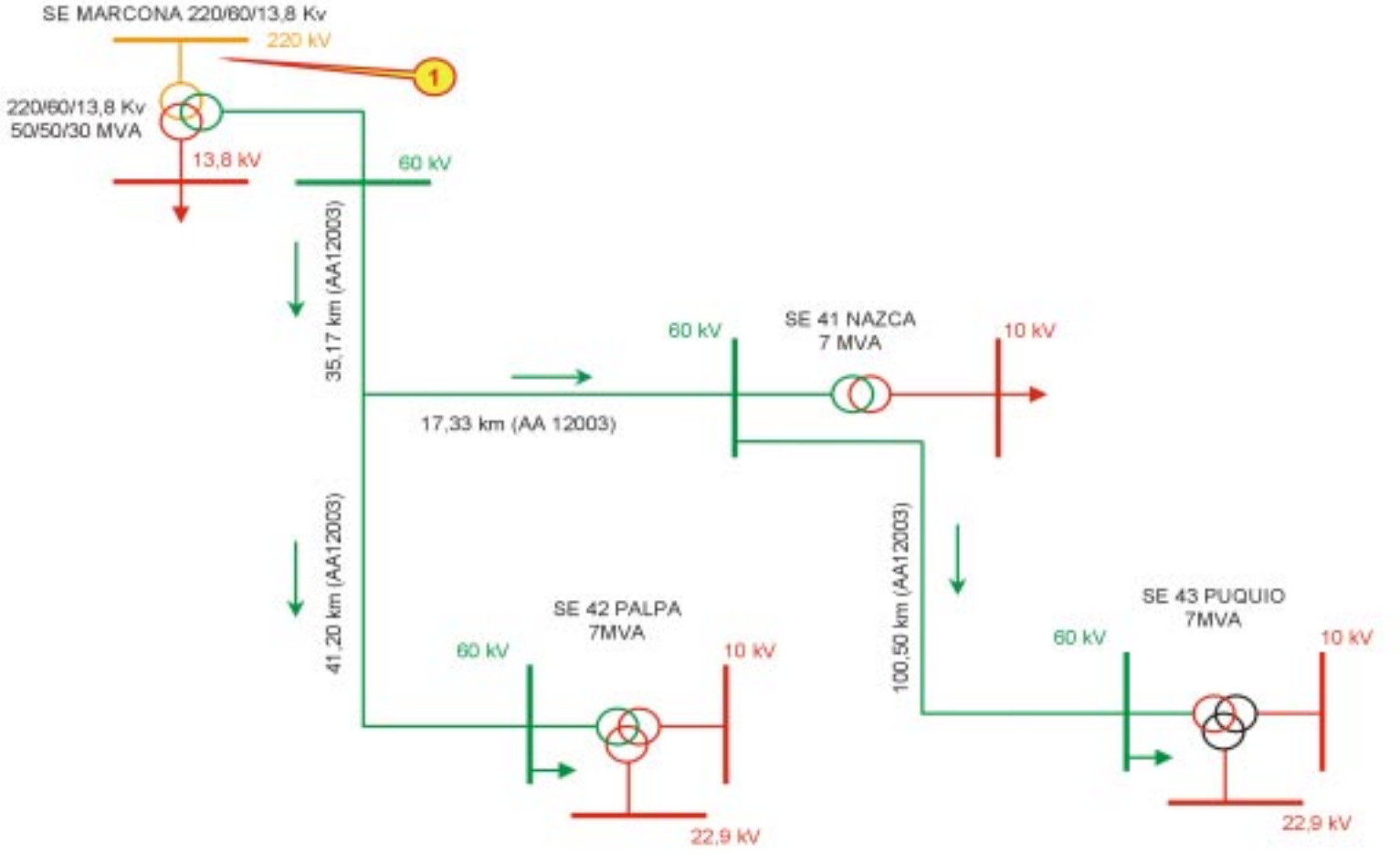
SISTEMA ELÉCTRICO: Ica	**EMPRESA ELÉCTRICA:** ELECTRO SUR MEDIO S.A.			
	Sector Típico: 2	Leq: 7,05 km	Fecha: 12/99	Pág. 5/8

I N G E N I O - C H A N G U I L L O



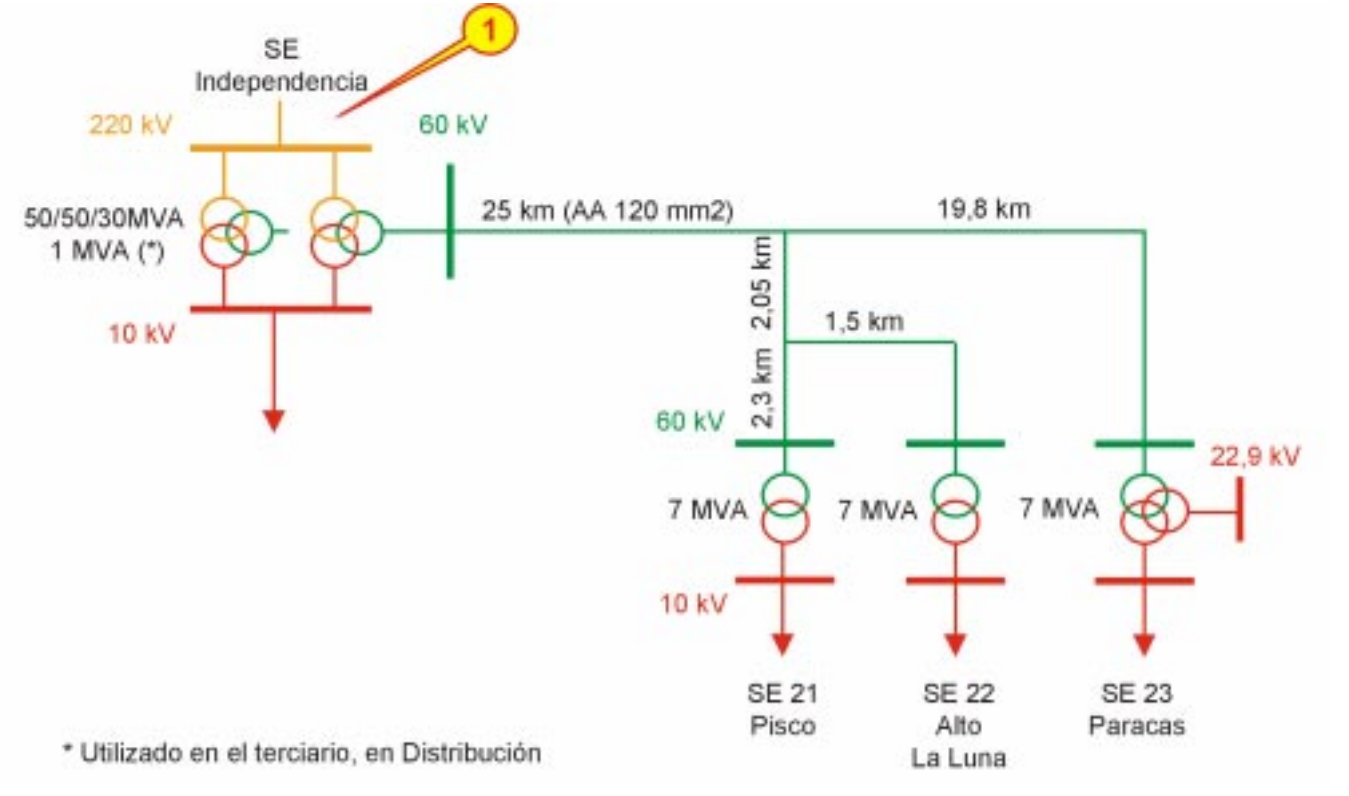
SISTEMA ELÉCTRICO: Ingenio, Changuillo	**EMPRESA ELÉCTRICA:** ELECTRO SUR MEDIO S.A.			
	Sector Típico: 4	Leq: 93,96 km	Fecha: 12/99	Pág. 6/8

N A Z C A - P A L P A



SISTEMA ELÉCTRICO: Nazca, Palpa, Puquio	**EMPRESA ELÉCTRICA:** ELECTRO SUR MEDIO S.A.			
	Sector Típico: 2	Leq: 93,96 km	Fecha: 12/99	Pág. 7/8

P I S C O



SISTEMA ELÉCTRICO: Pisco	EMPRESA ELÉCTRICA: ELECTRO SUR MEDIO S.A.			
	Sector Típico: 2	Leq: 32,68 km	Fecha: 12/99	Pág. 8/8

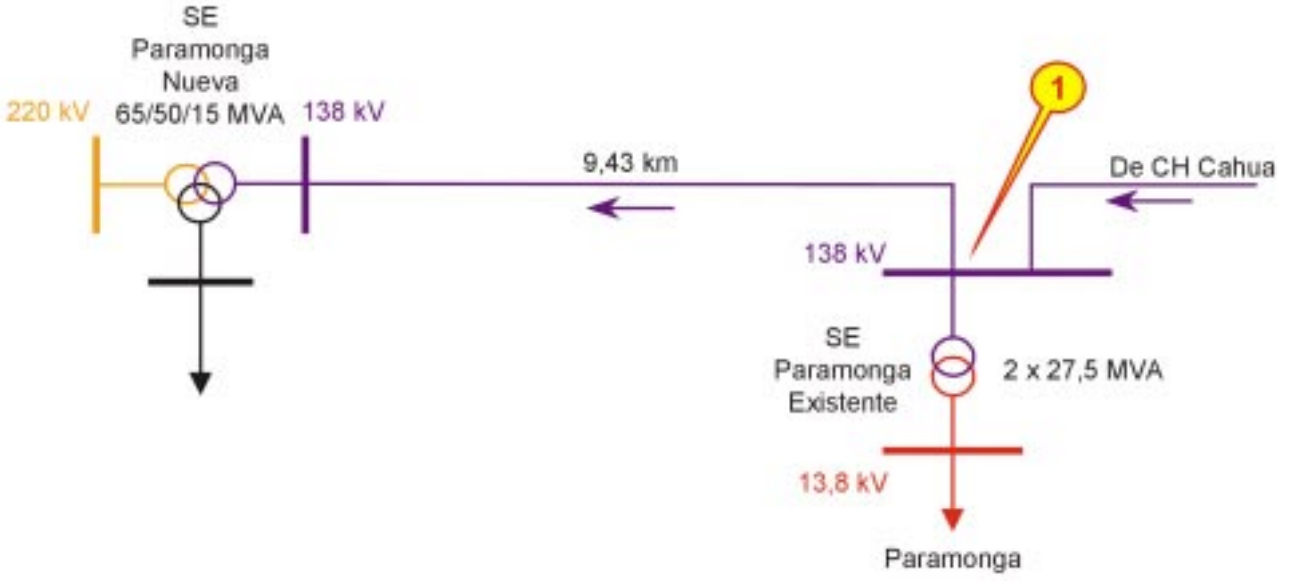
EMPRESA

E M S E M S A

SISTEMAS

Paramonga

P A R A M O N G A



SISTEMA ELÉCTRICO: Paramonga	EMPRESA ELÉCTRICA: EMSEMSA			
	Sector Típico: 2	Leq: 0 km	Fecha: 12/99	Pág. 1/1

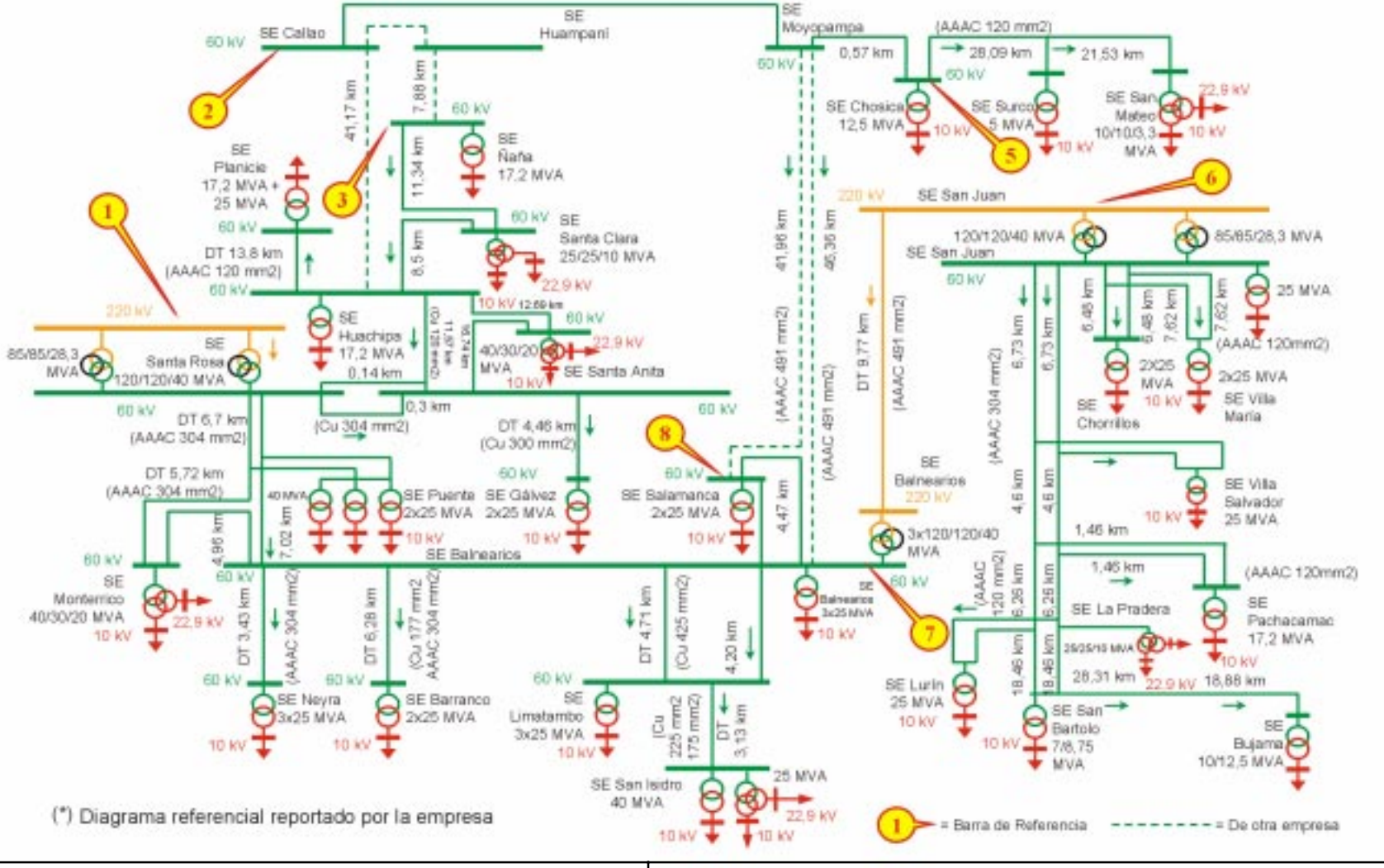
EMPRESA

L U Z D E L S U R S. A.

SISTEMA

Lima Sur

L I M A S U R (*)



SISTEMA ELÉCTRICO: Lima Sur	**EMPRESA ELÉCTRICA:** LUZ DEL SUR S.A.	
	Sector Típico: 1	Fecha: 12/99	Pág. 1/1

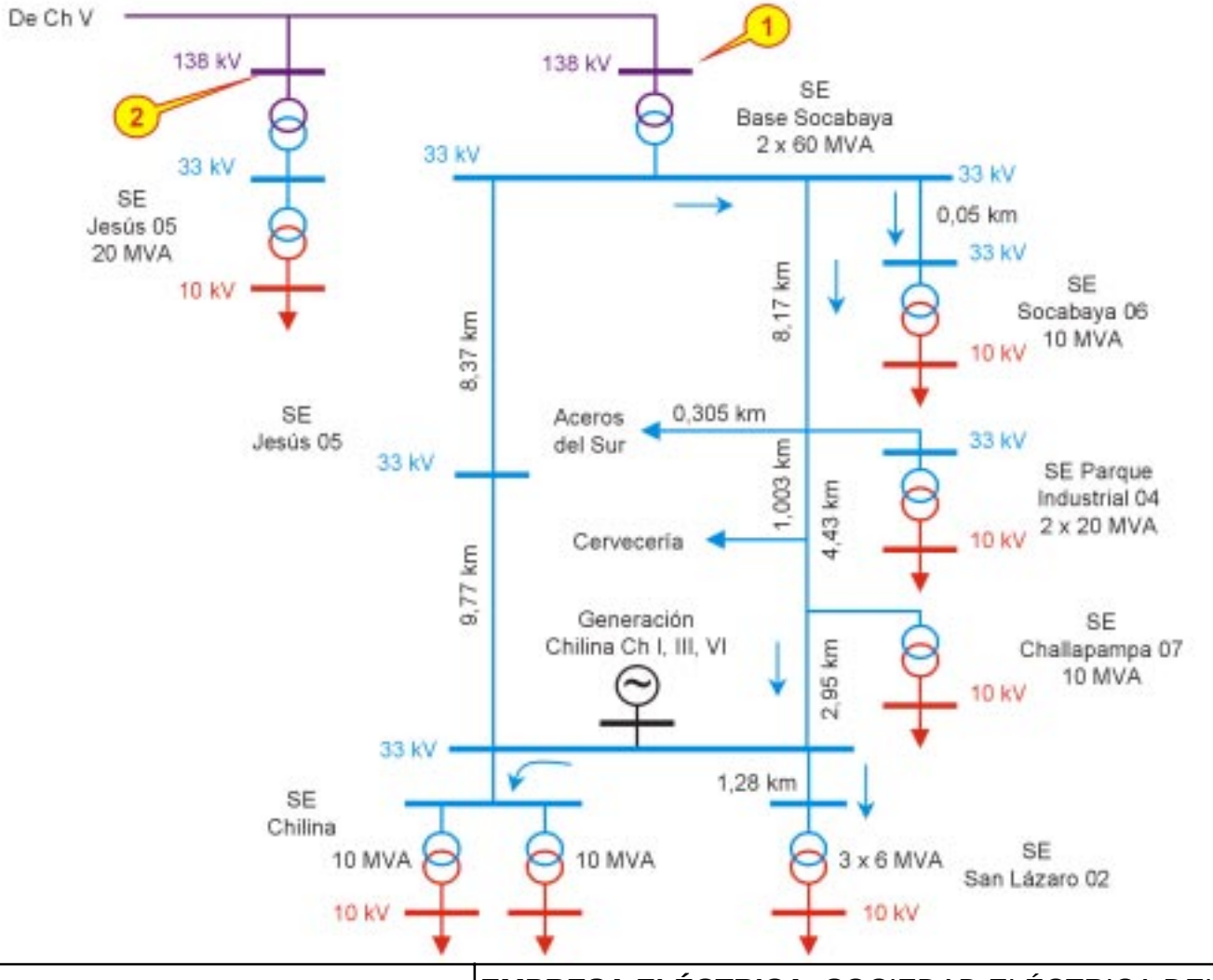
EMPRESA

SOCIEDAD ELÉCTRICA DEL SUR OESTE (SEAL)

SISTEMAS

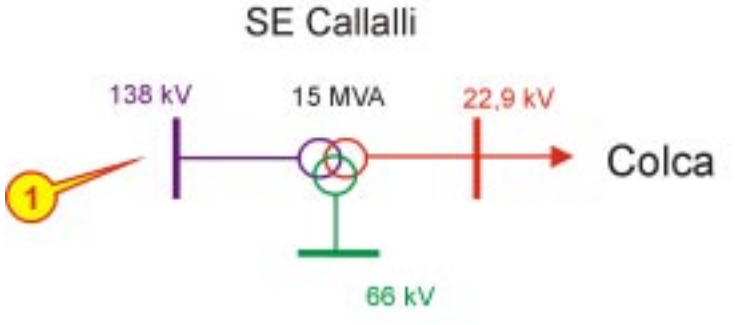
Arequipa
Colca
Mollendo - Matarani

A R E Q U I P A



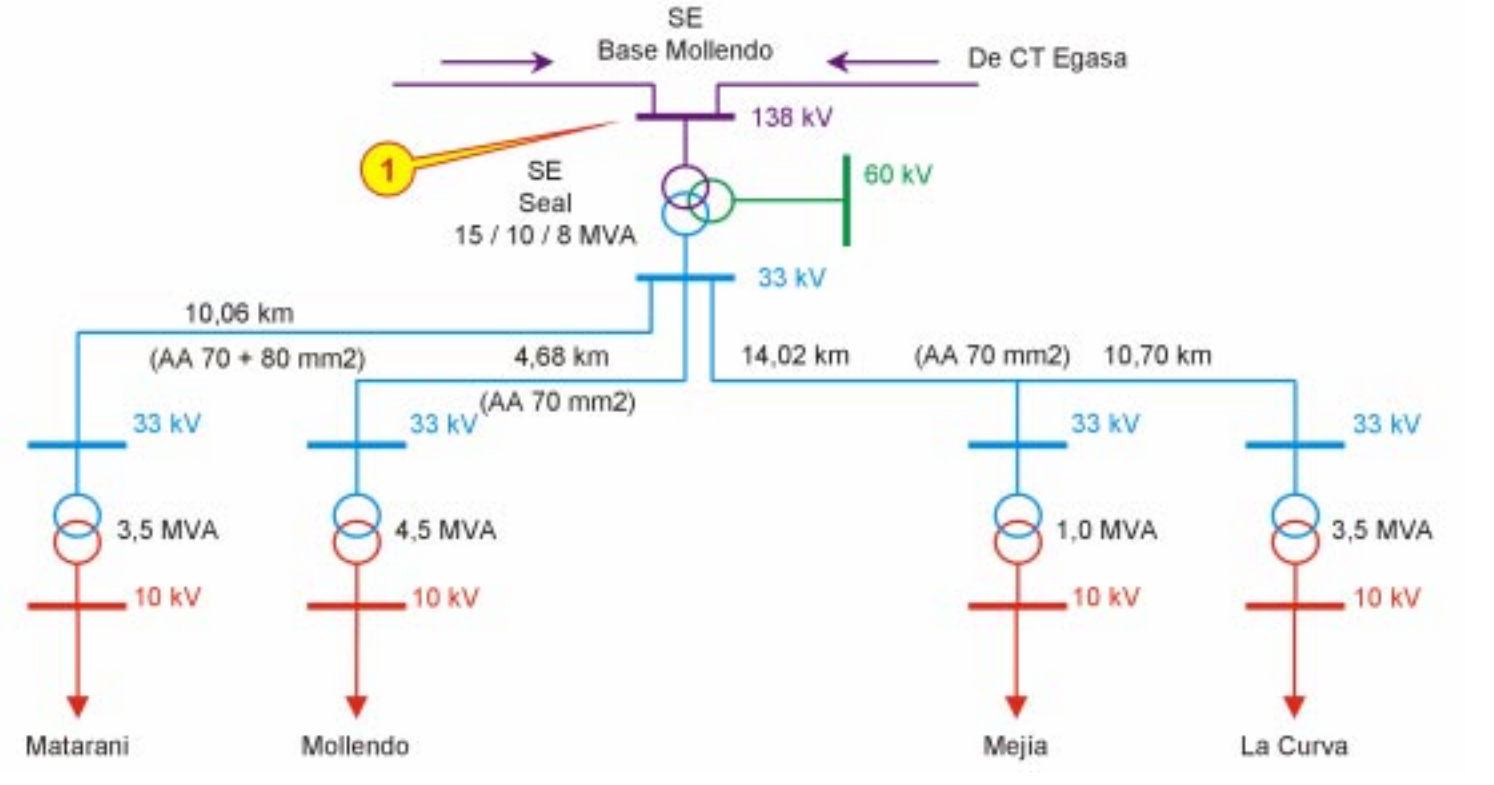
SISTEMA ELÉCTRICO: Arequipa	**EMPRESA ELÉCTRICA:** SOCIEDAD ELÉCTRICA DEL SUR OESTE S.A.			
	Sector Típico: 2	Leq: 9,04 km	Fecha: 12/99	Pág. 1/3

C O L C A



SISTEMA ELÉCTRICO: Colca	**EMPRESA ELÉCTRICA:** SOCIEDAD ELÉCTRICA DEL SUR OESTE S.A.			
	Sector Típico: 2	Leq: 0 km	Fecha: 12/99	Pág. 2/3

M O L L E N D O - M A T A R A N I



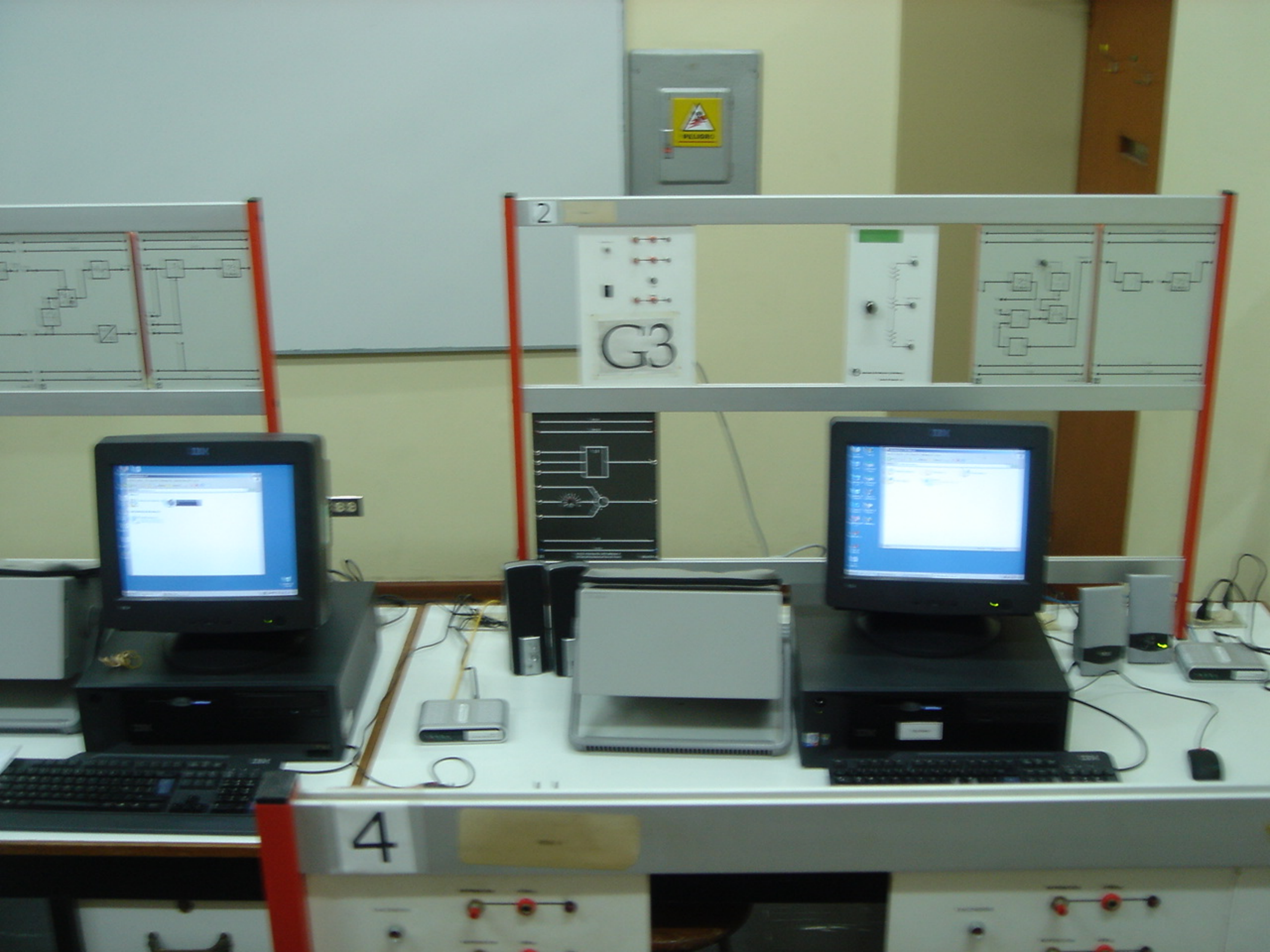
SISTEMA ELÉCTRICO: Mollendo - Matarani	**EMPRESA ELÉCTRICA:** SOCIEDAD ELÉCTRICA DEL SUR OESTE S.A.			
	Sector Típico: 2	Leq: 12,54 km	Fecha: 12/99	Pág. 3/3


Gridline Communications
Subscriber Unit 1-3


IBM
IBM


IBM
IBM
IBM


2
G3


2
G3
4

Corinex

Internet Phone con Auriculares

La solución Corinex para audio y Vídeo:

- Llamadas telefónicas gratis a través de Internet
- Escuchar música en el PC
- Juegos -PC, comunicación directa
- Grabación de Voz y Audio

El Corinex Internet Phone con Auriculares es un sólo dispositivo de Audio para todas sus aplicaciones PC, tales como llamadas telefónicas a través de Internet, musícales y juegos en línea.

El Corinex Internet Phone con Auriculares puede ser utilizado con otros dispositivos (Consolas de juegos, Set-Top-Box, unidades de CD o unidades portátiles). Disfrute de alta calidad de audio cuando escuche música, juegue en línea o realice llamadas teléfonicas con el software Softphone.

Con el Corinex Internet Phone con Auriculares, podrá hacer llamadas a través de Internet a cualquier lugar del mundo, a bajo costo o completamente gratis. Usando la telefonía vía Internet ahorrará mucho dinero, espacialmente en llamadas de larga distancia. Todo lo que necesita es un Corinex Internet Phone con Audifonos, un PC con Windows, una conexión a banda ancha de Internet y una cuenta con un proveedor Voice over IP

La instalación de los Auriculares es muy sencilla, Sólo conectelos junto el micrófono en sus respectivos enchufes de la computadora o el dispositivo que desee utilizar. No se necesitian controladores adicionales, tan solo conecte y disfrute (Plug &Play).

El paquete del Corinex Internet Phone con Auriculares consta de juego de audifonos con micrófono y el software Softphone. Éste software maneja la codificación digital de las señales de audio y las funciones de llamada. El dispositivo trabaja con cualquier proveedor de servicios VoIP compatible con los protocolos SIP o H.323 versión 4 (por ejemplo Free World Dialup, AddaVoice, Ecuity, SIP Phone o VoIP Talk), permitiéndole escoger el que más le convenga. El Softphone es compatible con Windows (98SE/ME/2000/XP).

Es de fácil configuración, y algunos proveedores de servicio (AddaVoice, Free World Dialup o SIPphone) vienen preconfigurados de fabrica. El uso del Internet Phone con Auriculares es practico gracias a características como el registro de llamadas(enviadas, recibidas y perdidas), directorio telefónico, y la personalización de apariencias y timbres.

Corinex también provee el equipo necesario, basado en tecnología Powerline, para el uso de servicios VoIP en cada lugar de su casa o oficina.

Corinex Softphone

Especificaciones del set de Auriculares

- Control de volumen y ajuste del micrófono desde el cable
- Diadema ajustable
- Micrófono omni-direccional

Contenido de la caja

- Auriculares multimedia Corinex con micrófono
- CD-ROM con Corinex Softphone para telefonía a través de Internet y documentación
- Guía rápida de instalación

Especificaciones del producto

Código del producto: CXV-IPH

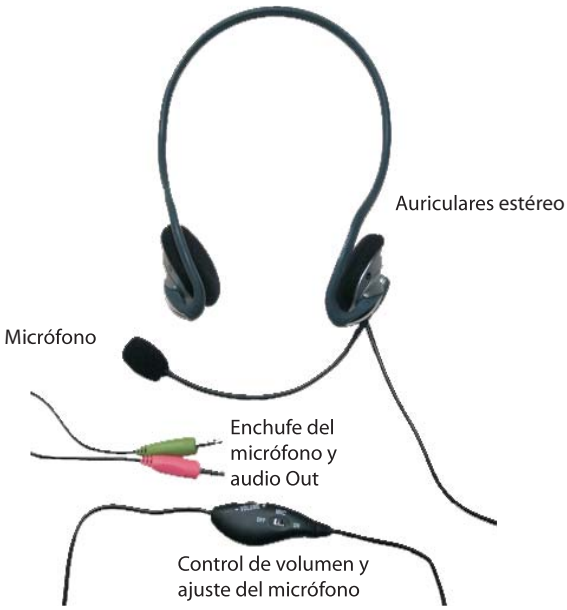
Por favor diríjase a la lista de precios para el código exacto y las especificaciones de su región.

Qué necesita para empezar a disfrutar de la telefonía IP

- Corinex Internet Phone con Auriculares
- Conexión banda ancha a Internet (mínimo a 64 kbps)
- PC con Windows 98SE, 2000, XP o ME con tarjeta de sonido
- Una cuenta con un proveedores de servicios VoIP (como Free World Dialup, Ecuity, SIP Phone o VoIP Talk)

Especificaciones del Softphone

- Compatible con los protocolos SIP y H.323 versión 4
- Preconfigurado para fácil instalación con varios operadores
- Registro de llamadas (hechas, recibidas y perdidas)
- Compatible con: Free World Dialup, Ecuity, SIP Phone, VoIP Talk y otros proveedores de servicios VoIP
- Personalización de la presentación gráfica
- Personalización de timbres WAV



Corinex Auriculares Multimedia con microfóno

Las ultimas actualizaciones del Corinex Internet Phone con Auriculares están disponibles en www.corinex.com/voip

Corinex

Corinex es marca registrada de Corinex Communications Corp.

Corinex Communications Corp.
#670 - 789 West Pender Street
Vancouver, BC
Canada V6C 1H2
Tel: +1 - 604 - 692 0520
Fax: +1 - 604 - 694 0061
E-mail: global@corinex.com
http://www.corinex.com

Corinex Global, a.s.
Ruzova dolina 19
821 08 Bratislava
Slovak Republic
Tel.: +421 - 2 - 5021 4811
Fax: +421 - 2 - 5556 7309
E-mail: global@corinex.com

2005-3-7 ver.1

El contenido de este documento es de uso informativo, puede ser cambiado sin previo aviso y no representa compromiso para Corinex Communications Corp.

HomePlug AV White Paper

Copyright © 2005, HomePlug® Powerline Alliance, Inc., All Rights Reserved

THE DOCUMENT IS PROVIDED "AS IS," AND THE HOMEPLUG POWERLINE ALLIANCE (INCLUDING ANY THIRD PARTIES THAT HAVE CONTRIBUTED TO THE DOCUMENT) MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE; THAT THE CONTENTS OF THE DOCUMENT ARE SUITABLE FOR ANY PURPOSE; NOR THAT THE IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

NEITHER THE HOMEPLUG POWERLINE ALLIANCE NOR ANY THIRD PARTY WILL BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO ANY USE OR DOCUMENT OF THE DOCUMENT.

Document version number: HPAVWP-050818

HomePlug AV White Paper

Introduction

HomePlug AV (HPAV) represents the next generation of technology from the HomePlug Powerline Alliance. Its purpose is to provide high-quality, multi-stream, entertainment oriented networking over existing AC wiring within the home, while addressing interoperability with HomePlug 1.0. HPAV employs advanced PHY and MAC technologies that provide a 200 Mbps (million bits per second) class powerline network for video, audio and data. The Physical (PHY) Layer utilizes this 200 Mbps channel rate to provide a 150 Mbps information rate with robust, near-capacity communications over noisy power line channels. The Medium Access Control (MAC) Layer is designed to be highly efficient; supporting both TDMA and CSMA based access with AC line cycle synchronization. The TDMA access provides Quality of Service (QoS) guarantees including guaranteed bandwidth reservation, high reliability and tight control of latency and jitter. The CSMA access provides four priority levels. AC line cycle synchronization provides superior channel adaptation in the face of common line cycle-synchronized noise. The Central Coordinator (CCo) controls the activities of the network, allocating time for CSMA use and scheduling the TDMA use.

Homeplug AV also provides advanced capabilities consistent with new networking standards. Advanced Network Management functions and facilities are capable of supporting user plug-and-play configuration as well as service provider set-up and configuration. HPAV offers tight security based on 128-bit AES and makes provision for dynamic (automatic) change of the encryption keys and for several different user experiences in setting up security and admitting stations to the network. The design allows a station to participate in multiple AV networks. HPAV is backward compatible with HomePlug 1.0 and offers several mandatory and optional co-existence modes enabling multi-network operation, hidden node service and Broadband over Powerline (BPL) co-existence.

HPAV aims to be the network of choice for the distribution of data and multi-stream entertainment including HDTV, SDTV, and audiophile quality audio throughout the home. It is designed to provide the best connectivity at the highest QoS of the home networking technologies competing for these applications. HomePlug AV enables all devices with a power plug to have network access through HPAV. HPAV was designed to provide this capability at a cost that is competitive with other competing technologies.

A glossary at the end of the paper defines the acronyms used in the paper.

System Architecture

Figure 1 shows an architectural diagram of the HPAV system. The Higher Layer Entities (HLEs) above the H1 (Host) Interface may be bridges, applications or servers that provide off-chip services to clients below the H1 Interface. The Data Service Access Point (SAP) accepts Ethernet format packets, so all IP based protocols are easily handled.

The Architecture defines two planes as shown in Figure 1. The data plane provides the traditional layered approach with the M1 interface between the Convergence Layer (CL) and the MAC, and the PHY interface between the MAC and the PHY. In the control plane, the MAC is a monolith without conventional layering. In Figure 1 it is labeled as the Connection Manager (CM) since that is its primary function. The approach adopted for the control plane was chosen to provide more efficient processing and to provide implementers greater flexibility for innovation. Although part of the control plane in all stations, the Central Coordinator (CCo) entity will be active in one and only one station in a single HPAV network.

Copyright © 2005, HomePlug® Powerline Alliance, Inc.

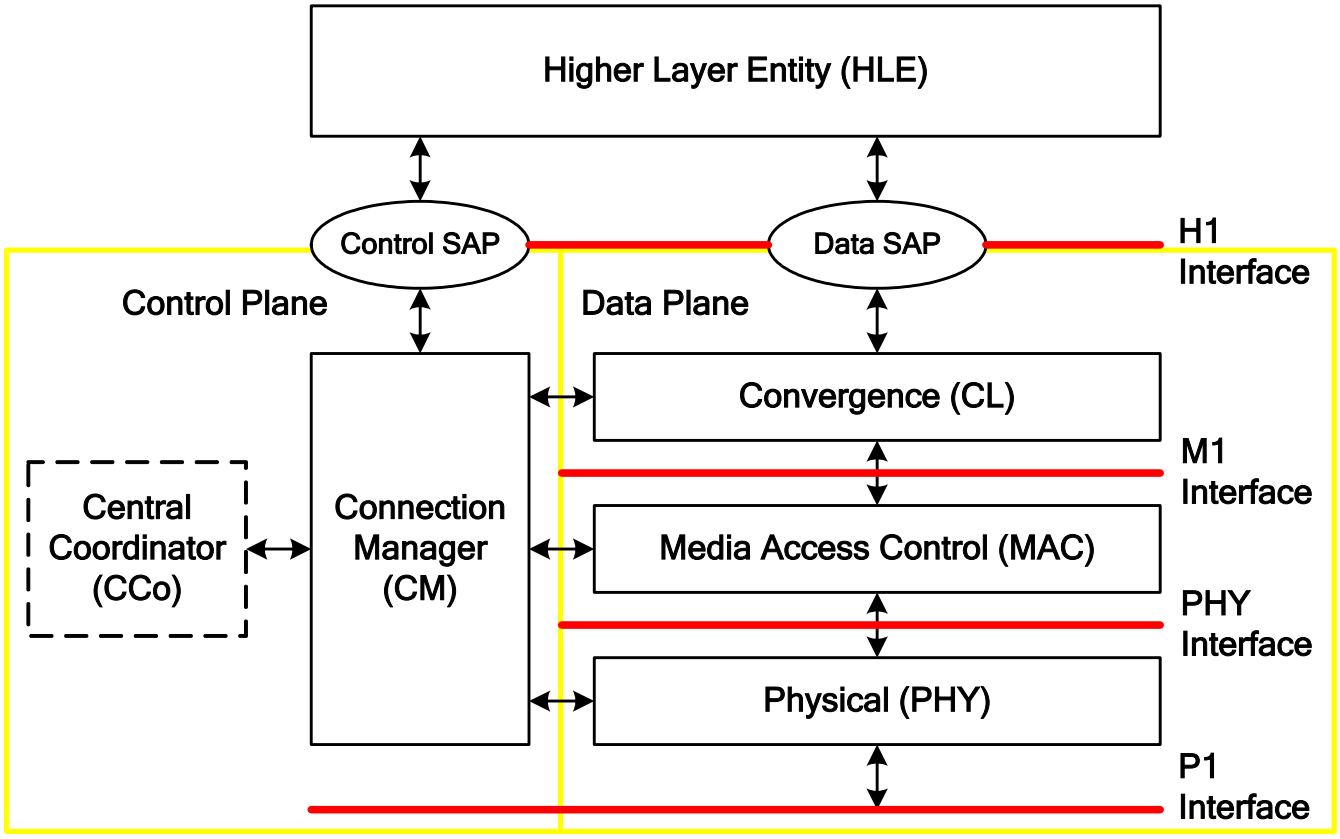


Figure 1 HPAV Architecture

Physical (PHY) Layer

The Physical Layer (PHY) operates in the frequency range of 2 - 28 MHz and provides a 200 Mbps PHY channel rate and a 150 Mbps information rate. It uses windowed OFDM and a powerful Turbo Convolutional Code (TCC), which provides robust performance within 0.5 dB of Shannon Capacity. Windowed OFDM provides flexible spectrum notching capability where the notches can exceed 30 dB in depth without losing significant useful spectrum outside of the notch. Long OFDM symbols with 917 usable carriers (tones) are used in conjunction with a flexible guard interval. Modulation densities from BPSK (which carries 1 bit of information per carrier per symbol) to 1024 QAM (which carries 10 bits of information per carrier per symbol) are independently applied to each carrier based on the channel characteristics between the transmitter and the receiver

Figure 2 shows a block diagram representation for the physical layer of a HPAV transmitter and receiver.

Copyright © 2005, HomePlug® Powerline Alliance, Inc.

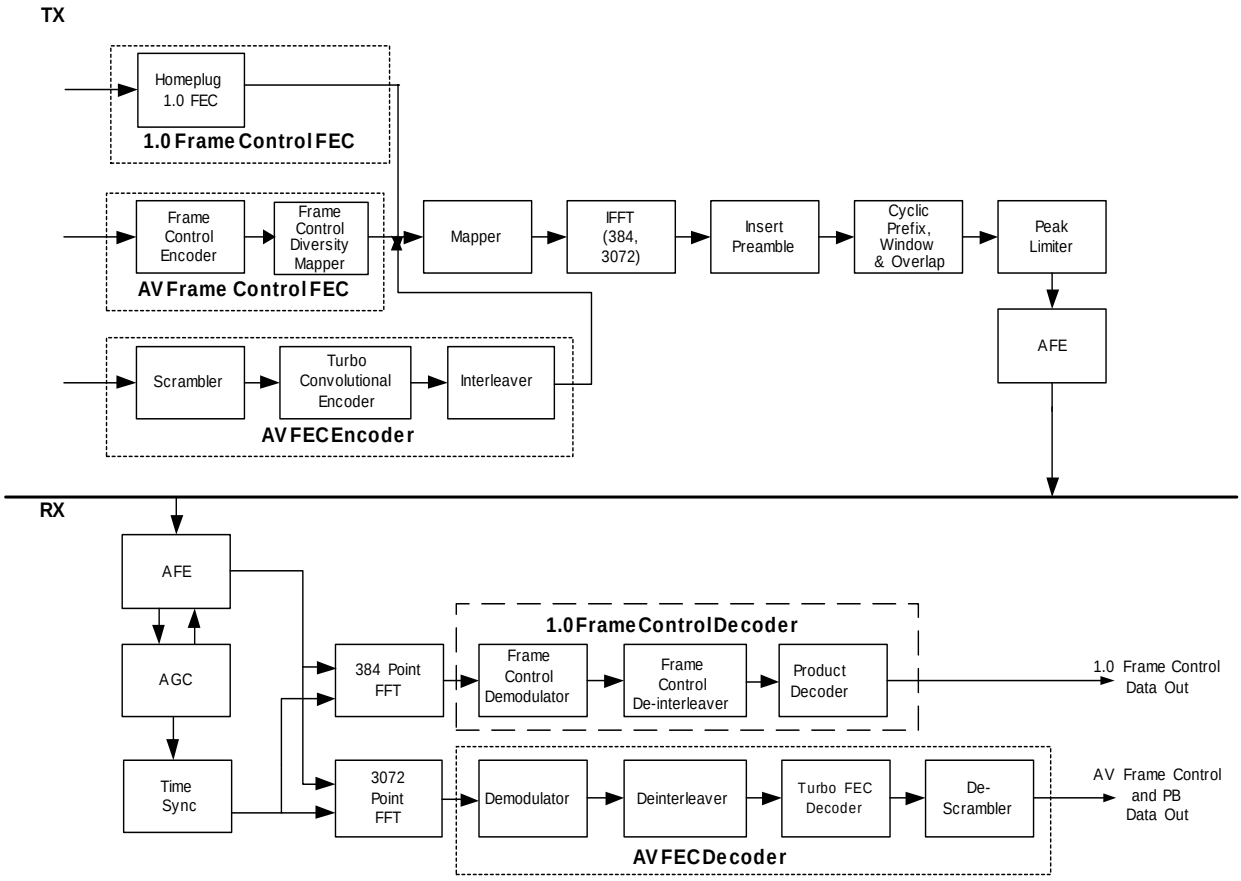


Figure 2 HPAV OFDM Transceiver

On the transmitter side, the PHY layer receives its inputs from the Medium Access Control (MAC) layer. There are separate inputs for HPAV data, HPAV control information, and HomePlug 1.0 control information (the latter in order to support HomePlug 1.0 compatibility). HPAV control information is processed by the Frame Control Encoder block, which has an embedded Frame Control FEC block and Diversity Interleaver. The HPAV data stream passes through a Scrambler, a Turbo FEC Encoder and an Interleaver. The outputs of the three streams lead into a common OFDM Modulation structure, consisting of a Mapper, an IFFT processor, Preamble and Cyclic prefix insertion and a Peak Limiter. This output eventually feeds the Analog Front End (AFE) module which couples the signal to the Powerline medium.

At the receiver, an AFE operates in conjunction with an Automatic Gain Controller (AGC) and a time synchronization module to feed separate data information and data recovery circuits. The HPAV Frame Control is recovered by processing the received stream through a 3072-point FFT, a Frame Control Demodulator and a Frame Control Decoder. The HomePlug 1.0 Frame Control, if present, is recovered by a 384-point FFT. In parallel, the data stream is retrieved after processing through a 3072-point FFT for HPAV, a demodulator with SNR estimation, a De-mapper, De-interleaver, Turbo FEC decoder, and a De-scrambler for HPAV data.

The HPAV PHY provides for the implementation of flexible spectrum policy mechanisms to allow for adaptation in varying geographic, network and regulatory environments. Frequency notches can be applied easily and dynamically, even in deployed devices. Region-specific keep-out regions can be set under software control. The ability to make soft changes to alter the device's tone mask (enabled tones) allows for implementations that can dynamically adapt their keep-out regions.

MAC Protocols/Services

HPAV provides connection-oriented Contention Free (CF) service to support the QoS requirements (guaranteed bandwidth, latency and jitter requirements) of demanding AV and IP applications. This Contention Free service is based on periodic Time Division Multiple Access (TDMA) allocations of adequate duration to support the QoS requirements of a connection.

Copyright © 2005, HomePlug® Powerline Alliance, Inc.

HPAV also provides a connectionless, prioritized Contention based service to support both best-effort applications and applications that rely on prioritized QoS. This service is based on Collision Sense Multiple Access/Collision Avoidance (CSMA/CA) technology which is applied to only traffic at the highest pending priority level after the pending traffic with lower priority levels has been eliminated during a brief Priority Resolution phase at the beginning of the contention window.

To efficiently provide both kinds of communication service, HPAV implements a flexible, centrally-managed architecture. The central manager is called a Central Coordinator (CCo). The CCo establishes a Beacon Period and a schedule which accommodates both the Contention Free allocations and the time allotted for Contention-based traffic. As shown in Figure 3, the Beacon Period is divided into 3 regions:

- Beacon Region
- CSMA Region
- Contention-Free Region

The CCo broadcasts a beacon at the beginning of each Beacon Period; it uses the beacon to communicate the scheduling within the beacon period. The beacons are extremely robust and reliable. The schedules advertised in the Beacon are persistent—i.e., the CCo promises not to change the schedule for a number of Beacon Periods—and the persistence is also advertised in the beacon so that the transmitting station for a connection can confidently transmit during its persistent allocation(s) even if it has missed several beacons within the advertised persistence of the schedule. This provides additional continuity even if a few beacons are missed. The CSMA periods are also persistent so that stations wishing to send CSMA traffic can do so even if they miss a few beacons.

The MAC layer provides both Contention (CSMA) and Contention Free (CF) services through the respective regions in the Beacon Period. The CCo-managed Persistent Contention Free (PCF) Region enables HPAV to provide a strict guarantee on Higher Layer Entity (HLE) QoS requirements. An HLE uses the Connection Specification (CSPEC) to specify its QoS requirements. The Connection Manager (CM) in the station evaluates the CSPEC and, if appropriate, communicates the pertinent requirements to the CCo and asks the CCo for a suitable Contention Free allocation. QoS features specified in the CSPEC include:

- Guaranteed bandwidth
- Quasi-Error free service
- Fixed Latency
- Jitter control

If the CCo is able to accommodate the connection request, it will ask the stations to “sound” the channel. This allows the stations to perform the initial channel estimation (i.e., establish a Tone Map specifying the optimal modulation on each OFDM tone). The Tone Map is communicated from the receiver to the transmitter; the channel estimation is also communicated in abbreviated form to the CCo to help it determine how much time should be allocated to the connection. Based on the CSPEC and the channel sounding results, the CCo provides one or more persistent time allocations—Transmit Opportunities (TXOPs)—for the connection within the PCF Region.

The PCF Region also contains time for non-persistent allocations good only in the current beacon period. These non-persistent allocations are used to provide additional short term bandwidth to connections that require it (e.g., because of transient errors or changing channel conditions) to meet their QoS requirements, providing that the transmitting station hears the beacon at the beginning of the Beacon Period. When this time is not used for non-persistent CF allocations, in may be used for CSMA traffic. Again, stations must hear the beacon in order to know whether the time is available for CSMA traffic.

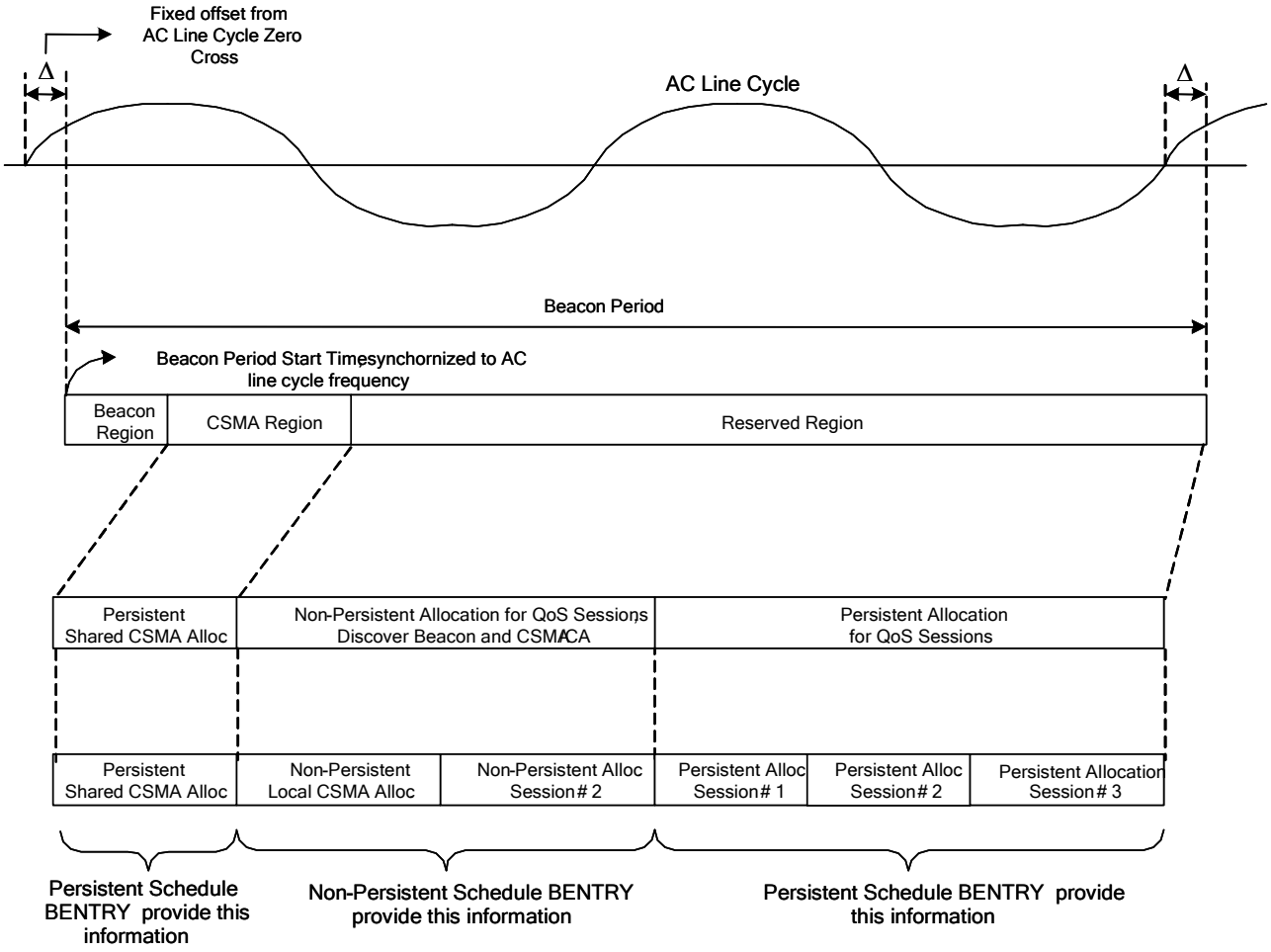
Messaging in HPAV is direct from station to station; however, the CCo monitors the messages. The header of each message contains information about how much data is pending for transmission on the connection; if this amount becomes large on a given connection, the CCo may allocate additional non-persistent time to the connection in the PCF Region.

The Persistent CSMA Region provides prioritized contention-based communication. It is used where there is no CSPEC and/or the traffic is of short duration. When operating in 1.0 Coexistence mode, or “Hybrid Mode”, AV coordinates with HomePlug 1.0 devices and permits them to communicate during the CSMA period.

As shown in Figure 3, the Beacon Period is synchronized to the AC line cycle. By synchronizing to the line cycle, HPAV provides stability of the periodic allocations relative to the line cycle. This, in turn, provides better channel adaptation to the synchronous (to the line cycle) interference, resulting in improved throughput. The beacon provides announcements of where the beacon will occur over the next few beacon periods—i.e., beacon persistence—to enable continued communications by stations that miss an occasional beacon.

Figure 3 Example of Beacon Period Structure

Copyright © 2005, HomePlug® Powerline Alliance, Inc.



MAC Control Plane

The Medium Access Control (MAC) Layer contains an integrated Connection Manager (CM). HLEs provide a Connection Specification (CSPEC) that details QoS requirements for application data. For bridged traffic, CSPECs may be generated dynamically by the Auto Connection Service (ACS) or by a higher layer QoS Manager that coordinates QoS over multiple network segments; otherwise the traffic is transmitted as prioritized CSMA traffic.

The Control Plane provides a seamless interface to the application layer. Application requirements are received at the H1 Control SAP in the CSPEC and are interpreted by the CM. The CM is responsible for evaluating the CSPEC and setting up the appropriate connection in conjunction with the CM in the station at the other end of the connection and with the CCo. It is the Connection Manager's responsibility to ensure that the appropriate AV mechanisms are engaged in order to provide the application with the bandwidth it requires. It must also monitor the level of service that the connection is receiving and take remedial action if the guaranteed QoS is not being provided.

The MAC also maintains a clock that is tightly synchronized to the CCo's clock (the CCo includes a timestamp in the beacon). This means that the entire HPAV network shares a common network clock for use by HLEs that have tight timing constraints (e.g., to synchronize surround sound speakers).

MAC Data Plane

In the Data Plane, the MAC accepts MSDUs (e.g., Ethernet packets) arriving from the Convergence Layer and encapsulates them with a header, optional Arrival Time Stamp (ATS) and Check Sum to create a MAC Frame. The MAC Frames are then enqueued into the appropriate MAC Frame Stream. It is the MAC's responsibility to ensure that the MSDUs related to a given connection are delivered to the PHY in a timely fashion for transmission during the time allocated for the connection. For this purpose, it maintains individual queues for each connection's data, for each priority level of CSMA traffic and for each priority level of Control Messages.

Copyright © 2005, HomePlug® Powerline Alliance, Inc.

Each MAC frame stream is divided into 512 octet segments each of which is encrypted and encapsulated into a serialized PHY Block (PB). As shown in Figure 4, the PBs are packed into an MPDU which is delivered to the PHY. The PHY transmitter applies forward error correction and places the resulting PPDU onto the powerline as described in the PHY section above.

As the receiver reconstructs the MSDUs, it selectively acknowledges the PBs; those that are not positively acknowledged are retransmitted during the next TXOP. The Selective Acknowledge (SACK) is an integral part of the TDMA allocation. When all the PBs composing an MSDU have been received correctly, the segments are decrypted and the resulting MSDU is passed to the Convergence Layer for delivery to the appropriate HLE.

Control messages are processed in an analogous fashion.

Since FEC and Selective Acknowledgment (SACK) are performed on relatively small blocks of data, the FEC is more robust and retransmissions are minimized. These two features contribute to HPAV's ability to operate at near channel capacity.

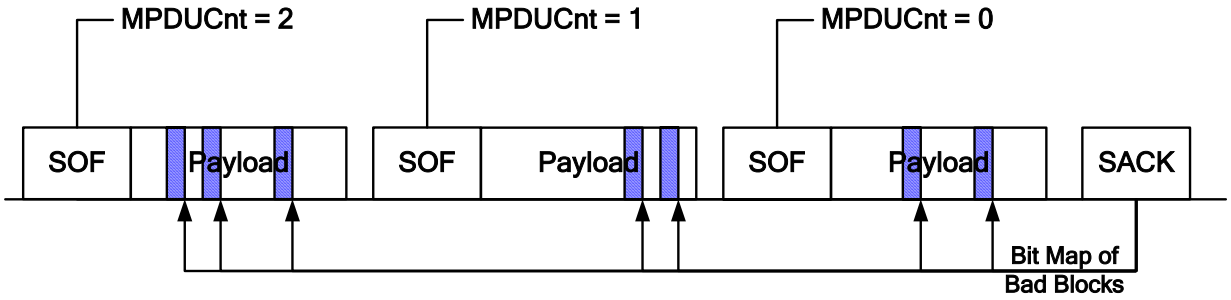


Figure 4 MAC Segmentation and MPDU Generation

Central Coordinator (CCo)

Each CCo controls an AV Logical Network (AVLN) which consists of several AV stations which all share a common Network Membership Key (NMK). The NMK and other details of security and encryption are discussed below. For now, it is sufficient to know that the NMK provides exclusive access to an AVLN so that the member stations can communicate in a private and secure environment.

As described above, the CCo provides bandwidth management services for the AVLN. These include admission control (determining whether to admit a new connection when it is requested). If the connection is admitted, the CCo schedules time allocations for the connection in the PCF Region. It manages this schedule via the beacon, which contains:

- the current schedule and the minimum number of Beacon Periods for which it will remain valid, and/or
- the new schedule and the number of Beacon Periods which will pass before it becomes valid.

When an AV Station is powered on, it listens to the medium. If it hears an existing AVLN, it will attempt to join it. If it does not hear an existing AVLN, it will form its own network by becoming a CCo and broadcasting a beacon. Eventually, another AV Station will be powered up and the two will associate and form an AVLN. (This is a highly simplified description; in reality, the HPAV specification provides for various cases of encountering more than a single AVLN, encountering HomePlug 1.0 devices, encountering other Powerline Networks and combinations thereof.)

The CCo attempts to learn the topology of its AVLN and of any neighboring AVLNs. To achieve this, each AV station broadcasts a Discover Beacon periodically (at a time allocated by the CCo in the non-persistent portion of the PCF Region). This Discover Beacon contains information about the station and the AVLN to which it belongs.

Each station that hears the Discover Beacon adds the information it contains to a Discovered Station List (DSL). While building its DSL, if the station encounters a Discover Beacon from a station in a different AVLN, it adds the information about the other network to a Discovered Networks List (DNL). Periodically the CCo asks each station for its DSL and DNL and use the collected lists to compose a topology map.

The CCo uses the topology map it builds from the collected DSLs and DNLs to determine if there is another station in the AVLN that would make a better CCo than it. The criteria for making this decision, in order of priority, are:

1. User's Selection
2. CCo Capability
3. Number of discovered STAs in the Discovered Station List
4. Number of discovered AVLNs in the Discovered Network List

Copyright © 2005, HomePlug® Powerline Alliance, Inc.

If the current CCo finds another station that would make a better CCo, it will negotiate a handover of CCo functions to the new CCo. Depending upon the capabilities of the old and new CCos, the handover may or may not result in existing connections being torn down.

The CCo may also select another CCo-capable station to be its backup in case of failure. If the station accepts the backup role, it will monitor the AVLN and, if the CCo's beacon is not heard by any stations in the AVLN for a specified number of Beacon Periods, the backup CCo will assume the role of CCo and attempt to maintain the existing connections without disruption.

Since a station must be capable of communicating with the CCo in order to join an AVLN and establish connections, a proxy capability is provided to support stations that are hidden from (i.e., unable to communicate with) the CCo. This capability provides for the creation of a Proxy Coordinator (PCo) to repeat the beacon information in Proxy Beacons and to relay control messages between the hidden station and the CCo. Note that only control messages are relayed. The station must be able to communicate directly with any stations with which it wishes to establish a connection. The PCo also transmits a Proxy Beacon during each Beacon Period to convey scheduling and other information to the hidden station.

When all stations are idle, the CCo causes the AVLN to enter a power saving mode. In this mode, there is only a small CSMA Region (so stations can initiate communication) and a small PCF Region (just long enough for Discover and Proxy beacons). Stations must have their receivers on during these small regions to participate in the AVLN; they may turn their transmitters and receivers off for the remainder of the Beacon Period. This makes it easier for stations to qualify for Energy Star certification.

Convergence Layer

The Convergence Layer (CL) serves as the interface between the HLEs and the MAC in the Data Plane. It accepts data payloads through Service Access Points (SAPs) at the H1 Interface and processes them as needed prior to handing them off to the MAC through the M1 interface. The only Data SAP specified by AV is the Ethernet II-class stack. This stack supports packet formats as specified by IEEE 802.3 with or without IEEE 802.2 (LLC), IEEE 802.1H (SNAP) extensions, and/or VLAN tagging. Using the Ethernet format makes it easy for AVLNs to interface to other LANs.

Among the services the CL provides on the transmit side are classification and auto connection. If requested for a connection, the CL will also associate an Arrival Time Stamp (ATS) with the data payload. On the receive side, the CL provides (optional) smoothing and insures that the received MSDUs are delivered to the appropriate H1 Service Access Point (SAP). On both sides, it provides the Connection Manager sufficient information to monitor the level of QoS being provided by the connection.

When a connection is established, the CM provides the classifier with a set of rules that will enable the classifier to uniquely associate incoming packets with the connection. For example, a set of rules might specify the source and destination MAC addresses and the TCP source and destination ports of the connection.

The classifier examines each packet received at the H1 interface and attempts to match it with a connection using the classification rules that have been provided to it. If it finds a match it will label the packet with the Connection ID (CID) of the appropriate connection, otherwise the classifier will release the packet for transmission in the CSMA region at the appropriate priority level.

If the transmitting station supports the optional Auto Connect Service (ACS), all packets which are released by the classifier without being associated with a connection will be examined by the ACS which will evaluate the data flow(s) between a given source and destination and attempt to identify flows which are worthy of a connection. This evaluation and identification may be based on a mix of the following:

- Policies established by an HLE (or a manufacturer),
- Templates such as traffic associated with ports known to have a particular usage,
- Heuristics such as the volume and regularity of data which is being transmitted.

Until the ACS identifies a connection, it releases the packets for transmission in the CSMA period immediately upon completion of the packet's inspection.

If the ACS identifies a particular data flow as connection worthy, it behaves in a manner analogous to an HLE and asks the CM to set up a connection, providing classifier rules, etc. When the CM establishes the connection, the Classifier will start associating the packets with the newly established connection and the ACS will no longer see them. The ACS is, however, responsible for servicing the connection in the same way that an HLE would.

At the receiving station, the CL demuxes the received packets. If the packets are associated with a connection for which smoothing (a.k.a. de-jittering) has been requested, the CL will buffer the packets for the appropriate time so that all packets

Copyright © 2005, HomePlug® Powerline Alliance, Inc.

are released to the HLE at a fixed interval after they arrived at the H1 interface at the transmitter, which the receiver knows from the ATS it received with the packet and the synchronized network clock.

On both ends of a connection, the CLs provide sufficient information to the CM that it can monitor the level of QoS being provided to a connection to insure that the guarantees are being met. The CM will take corrective measures specified by the CSPEC if there are any violations to the QoS guarantees.

HPAV Security

Admission control procedures ensure that only permitted devices are allowed into the AVLN. A station's ability to maintain multiple security keys allows it to participate in multiple AVLNs.

All data traffic and nearly all control traffic within the AVLN—the exception being a strictly limited set of control messages that simply cannot be encrypted—is secured by 128-bit AES encryption, providing a high level of security. This encryption uses the Network Encryption Key (NEK) and is performed on individual segments as the MPDUs are created. The NEK may be automatically and dynamically changed.

In order to join an AVLN, a station must obtain a Network Membership Key (NMK). If it already possesses an NMK it may join the network immediately; otherwise is must be provided with the NMK. This provisioning may occur in a variety of ways, including:

- Using the default NMK that is programmed into all AV stations. While this default NMK provides a seamless, plug and play experience for the user when the equipment is initially installed, it does not provide any privacy since it is known by every HPAV-certified station.
- The user can define and enter a Network Password (NPW) directly into a new station. This NPW is hashed to create the NMK, a 128 bit AES encryption key. The user must enter a NPW on at least one station to initially define the NMK for the AVLN.
- All AV stations are also programmed with a unique Device Access Key (DAK). The user may enter this key into any suitably programmed station already in the AVLN and that station will use the DAK to encrypt the NMK and broadcast it. Since only the new station has the DAK, it will be the only station that is capable of decrypting the broadcast message and so it and only it will receive the new NMK.
- Using asymmetric Public/Private Key encryption, the AV stations may provide the user the ability to join the new station to the AVLN without needing to remember or enter passwords. This may be as simple as having the user press a button or make a menu selection on the new station and on a station already in the AVLN.

When a station has the correct NMK and actually joins the AVLN, it will be given the current Network Encryption Key (NEK) which is used to encrypt data during segmentation in the MAC.

The design also permits encryption key management by higher layer Security and Authentication Standards such as 802.1x and EAP.

Multiple Networks

AV incorporates mechanisms to provide for the coordination of Neighboring Networks (NNs). Once detected, neighboring CCo's can cooperatively schedule transmissions in their own networks without causing interference in the other. In the case of multiple AVLNs, each CCo maintains an Interfering Network List (INL). The INL identifies all the nearby CCos that the CCo can hear. Each CCo then communicates it's INL to the other CCo's. HPAV requires that a CCo must recognize all of the INLs that it is aware of and not interfere with those networks.

When the CCo in an AVLN discovers another CCo, it attempts to coordinate with the discovered CCo. It negotiates for a beacon slot within the beacon region—which may need to be expanded to provide room for another beacon slot—and for any time it requires for its PCF Region. When the negotiations are completed, both CCos synchronize a schedule change which results in each AVLN having a space for its own PCF Region, which is identified by its neighbors as a Stayout Region in their beacons. All of the NNs share a common CSMA region. An example is shown in Figure 5.

Copyright © 2005, HomePlug® Powerline Alliance, Inc.

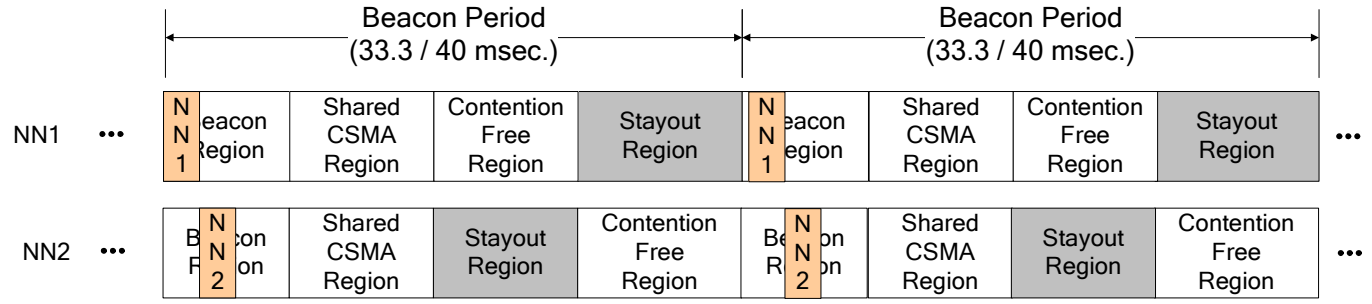


Figure 5 Neighbor Network Coordination

When multiple AVLNs are coexisting, each has a bandwidth quota, i.e., a portion of the Beacon Period that it uses for its PCF Region. The quota is defined by policies which are suitable for the regulatory region in which the AVLN is operating. The default quota is equal shares.

After allowances are made for the Beacon Region and for a minimal Shared CSMA region, a CCo may allocate as much of the remaining bandwidth as is available to service its connections. It may even exceed its quota if the bandwidth is available. If an AVLN is using more than its quota—which depends upon the number of NNs—it must relinquish bandwidth down to its quota if requested by its neighbors, even if it has to reconfigure (squeeze) or release connections in order to fit within its quota. It is not required to drop below its quota or to release bandwidth to another NN if the release would cause that NN to exceed its quota.

Coexistence

HomePlug 1.0 Coexistence

The AV PHY enables coexistence and interoperability with HomePlug 1.0 devices. The specification requires coexistence but interoperability is optional. Coexistence means that AV devices are capable of the low-level communications with 1.0 devices needed to share the medium, but not necessarily the ability to communicate payload data. An optionally interoperable device has the ability to communicate payload data with 1.0 devices.

Coexistence is achieved with the use of preambles that all devices (AV and 1.0) can use for synchronization, as well as the addition of 1.0 Frame Controls. The additional Frame Controls and 1.0 coexistence mechanisms are only activated when one or more 1.0 devices are detected.

BPL Coexistence

HPAV employs BPL Coexistence through one of two methods: Coexistence of Services, and Coexistence of Technologies. Coexistence of Services provides an efficient, integrated extension of services, while Coexistence of Technologies allows simultaneous use of the powerline by differing technologies.

The Coexistence of Services method uses TDM with beacon signaling and messaging to coordinate the in-home and BPL networks. Network coordination allows flexible time allocation and re-use. Flexible allocation provides increased efficiency and throughput for both networks by allowing either network to utilize unused time in the other network. In addition, both networks can communicate allowing service-level integration from providers to in-home devices

The Coexistence of Technologies method uses FDM to allow differing technologies to coexist. While allowing unique technologies to share the powerline, it lacks the ability to share unused bandwidth with the other network(s).

Conclusion

In this paper, an overview of HomePlug AV has been presented. An overview of the architecture and some details of each of the functional blocks have been presented. In order to get complete details and access the specification, any company may join the HomePlug Alliance. Instructions on how to do this can be found at http://www.homeplug.org/en/join/index.asp.

Copyright © 2005, HomePlug® Powerline Alliance, Inc.

Glossary

Acronym	Meaning
ACS	Auto Connection Service
AES	Advanced Encryption Standard
AFE	Analog Front End
AGC	Automatic Gain Controller
ATS	Arrival Time Stamp
AVLN	HomePlug AV Logical Network
BPL	Broadband over Powerline
BPSK	Binary Phase Shift Keying
CCo	Central Coordinator
CF	Contention Free
CID	Connection ID
CL	Convergence Layer
CM	Connection Manager
CSMA/CA	Collision Sense Multiple Access/Collision Avoidance
CSPEC	Connection Specification
DAK	Device Access Key
DNL	Discovered Networks List
DSL	Discovered Station List
EAP	Extensible Authentication Protocol
FDM	Frequency Division Multiplexing
FEC	Forward Error Control
FFT	Fast Fourier Transform
HDTV	High Definition Television
HLE	Higher Layer Entity
HPAV	HomePlug AV
IFFT	Inverse Fast Fourier Transform
INL	Interfering Network List

Acronym	Meaning
MAC	Medium Access Control
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
NEK	Network Encryption Key
NMK	Network Membership Key
NN	Neighboring Network
NPW	Network Password
OFDM	Orthogonal Frequency Division Multiplexing
PB	PHY Block
PCF	Persistent Contention Free
PCo	Proxy Coordinator
PHY	Physical Layer
PPDU	PHY Protocol Data Unit
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
SACK	Selective Acknowledge
SAP	Service Access Point
SDTV	Standard Definition Television
SNR	Signal-to-Noise Ratio
SOF	Start of Frame
STA	Station
TCC	Turbo Convolutional Code
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TXOP	Transmit Opportunity
VLAN	Virtual LAN

Copyright © 2005, HomePlug® Powerline Alliance, Inc.

The Asterisk Handbook

Version 2

Mark Spencer
Mack Allison
Christopher Rhodes
The Asterisk Documentation Team

Last Edit Date: 3/30/03

DRAFT

The Asterisk Handbook
Version 2

About this book

Authors:

Mark Spencer
Mack Allison
Christopher Rhodes
The Asterisk Documentation Team

Special thanks to all the users, contributers, and developers who have made Asterisk a reality.

Copyright © 2003 Digium, Inc. All rights reserved. ***This document may not be duplicated, copied, or redistributed in any form, electronic or physical, without the prior written consent of Digium, Inc.***

The latest version of this document may be downloaded for free from http://www.digium.com.

This book was created using OpenOffice, available at http://www.openoffice.org.

DRAFT

Table of Contents

DRAFT

DRAFT

Chapter 1: Introduction

1.1 What is Asterisk?

Officially, Asterisk is an Open Source hybrid TDM and packet voice PBX and IVR platform with ACD functionality. Unofficially, Asterisk is quite possibly the most powerful, flexible, and extensible piece of integrated telecommunications software available. Its name comes from the asterisk symbol, *, which in UNIX (including Linux) and DOS environments represents a wildcard, matching any filename. Similarly, Asterisk the PBX is designed to interface any piece of telephony hardware or software with any telephony application, seamlessly and consistently.

Traditionally, telephony products are designed to meet a specific technical need in a network. However, many applications of using telephony share a great deal of technology. Asterisk takes advantage of this synergy to create a single environment that can be molded to fit any particular application, or collection of applications, as the user sees fit.

Asterisk can, among other things, be used in any of these applications:

Heterogeneous Voice over IP gateway (MGCP, SIP, IAX, H.323)
Private Branch eXchange (PBX)
Custom Interactive Voice Response (IVR) server
Softswitch
Conferencing server
Number translation
Calling card application
Predictive dialer
Call queuing with remote agents
Remote offices for existing PBX

Perhaps more importantly, it can fill all of those roles simultaneously and seamlessly between interfaces.

1.2 Obtaining Asterisk

Released versions of Asterisk can be freely downloaded from ftp://ftp.asterisk.org via anonymous FTP. The preferred method of accessing Asterisk for most installations is via the anonymous repository located at cvs.digium.com, with the CVSROOT of :pserver:anoncvs@cvs.digium.com. For more information, see *Downloading and Installing*.

1.3 Licensing

Asterisk is generally distributed under the terms of the GNU General Public License, or GPL. This license permits you to freely distribute Asterisk in source and binary forms, with or without modifications, provided that when it is distributed to anyone at all, it is distributed with source code (including any changes you make) and without any further restrictions on their ability to use or distribute the code. For more information, refer to the GNU General Public License, included as an appendix.

The GPL does not extend to the hardware or software that Asterisk talks to. For example, if you are using a SIP soft phone as a client for Asterisk, it is not a requirement that that program also be distributed under GPL. Additionally, AGI applications, which are simply launched by Asterisk and communicate

For those applications in which the GNU GPL is not appropriate (because of some sort of proprietary linkage, for example), Digium is the solely capable of licensing Asterisk *outside* of the terms of the GPL at their discression. For more information on licensing Asterisk outside of GPL, contact sales@digium.com.

1.4 Supported Technologies

Asterisk is designed to allow new interfaces and technologies to be added easily. Its lofty goal is to support every kind of telephony technology possible. The latest hardware and protocol compatibility list can be found at http://www.digium.com or http://www.asterisk.org. In general, interfaces are divided into three categories, Zaptel hardware, non-Zaptel hardware, and packet voice:

1.4.1 Zaptel Pseudo TDM interfaces

These interfaces provide integration with traditional and legacy digital and analog telephone interfaces (including connection to the public phone network itself). In addition, Zaptel compatible interfaces support Pseudo-TDM switching between them, to keep latency nearly nonexistent on strictly TDM calls, conferences, etc. Zaptel interfaces are available from Digium (http://www.digium.com) for a variety of network interfaces including PSTN, POTS, T1, E1, PRI, PRA, E&M, Wink, and Feature Group D interfaces among others. Among the hardware available at the time of writing:

T100P - Single span T1 or PRI connection (mixed data/voice permitted)
E100P – Single span E1 or PRA connection (mixed data/voice permitted)
T400P – Quad span T1 or PRI connection (mixed data/voice permitted)
E400P – Quad span E1 or PRA connection (mixed data/voice permitted)
X100P – Single analog PSTN connection
S100U – Single analog POTS connection (USB)
S400P – Single to Quad analog POTS connection (PCI)

Note that for technical reasons, you *must* have at least one Zaptel interface (of any kind) installed in your Asterisk system if you wish to use conferencing.

1.4.2 Non-Zaptel hardware interfaces

These interfaces provide connectivity to the traditional and legacy telephone services, but do not support Pseudo-TDM switching. These include:

ISDN4Linux – Basic Rate ISDN interface for Linux
OSS/Alsa – Sound card interfaces
Linux Telephony Interface (LTI) – Quicknet Internet Phonejack/Linejack
Dialogic hardware[1] – Full-duplex Intel/Dialogic hardware

1.4.3 Packet voice protocols

These are standard protocols for communication over packet (IP and Frame Relay) networks and are the only interfaces that do not require specialized hardware of some kind.

Session Initiation Protocol (SIP)
Inter-Asterisk eXchange (IAX) versions 1 and 2
Media Gateway Control Protocol (MGCP)
ITU H.323[2]
Voice over Frame Relay (VOFR)

1.5 Contributing

Although Asterisk is primarily the work of Digium, its main corporate sponsor, like many Open Source projects, Asterisk grows thanks greatly to contributions, both big and small, from countless individuals. Contributing to Asterisk can be done in many ways:

1 Dialogic hardware is not supported by standard Asterisk but is available as a pay-for add-on for customers with Intel/Dialogic hardware.
2 At the time of writing, H.323 support is freely available as an add-on for Asterisk from third parties

1.5.1 Code Contributions

If you are a developer, you can contribute to the Asterisk codebase through bug fixes, feature enhancements, and new applications and channel drivers. Contributions are typically made as patches against current CVS, and should be submitted in "unified diff" format, which you can generate by executing:

```
# cvs diff -u > mypatch.diff
```

The resulting file (mypatch.diff in the above example) should then be e-mailed to the author (markster@digium.com). Before any patches can be merged with standard Asterisk, the author of the patch is must submit a *copyright disclaimer* which gives Digium (Asterisk's copyright holder) unlimited rights to use the patch. Two versions of the disclaimer are included at the end of this document. Either version may be used (whichever the patch author is more comfortable with). After being filled out and signed, the document should be faxed (and preferably mailed) to Digium. Contact information is available at http://www.digium.com.

1.5.2 Documentation Contributions

Even if you are not a developer, you can contribute to Asterisk in an extremely important way by converting your experience in getting to use Asterisk into a document which can accelerate someone else's entry into the software. Documents can include entries for The Asterisk Handbook (commonly referred to as simply "the book"), application notes for using Asterisk in a specific environment or for a specific use (known as "App Notes"), or in documenting Asterisk's programming API.

1.5.3 Asterisk IRC Channel and Mailing List

One important way to contribute is by assisting in programming discussions, and providing technical support for other Asterisk users on the Asterisk IRC channel, or on the Asterisk mailing list. The Asterisk IRC channel is called (not surprisingly) "#asterisk" and is available on irc.freenode.net. More information on the Asterisk mailing list is available at http://lists.digium.com.

1.5.4 Supporting Asterisk Sponsors

Shameless plug as it may be, when you purchase hardware, support or development from Digium, Asterisk's primary corporate sponsor, you directly benefit the advancement of Asterisk.

1.5.5 Core Developer Wishlists

Several independent core Asterisk developers have "wishlists" at companies such as Amazon, ThinkGeek, and others. Sponsoring their wishlists is one way to encourage them to continue their contributions and participation in Asterisk development.

DRAFT

Chapter 2: Asterisk's Architecture

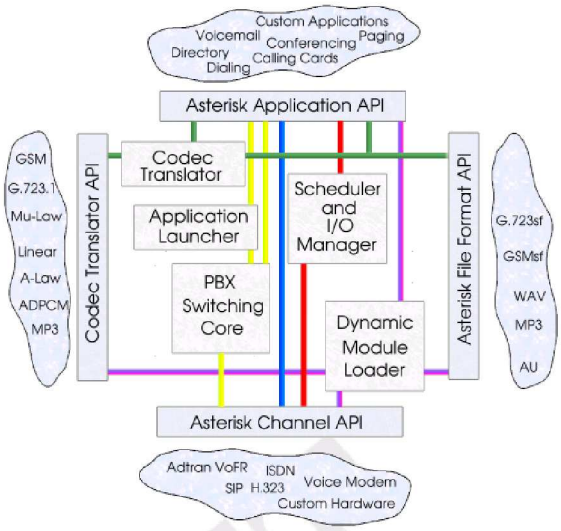
2.1 Asterisk Architecture Overview

Asterisk's architecture is fundamentally very simple, but different from most telephony products. Essentially Asterisk acts as middleware, connecting telephony technologies on the bottom to telephony applications on top, creating a consistent environment for deploying a mixed telephony environment. Telephony technologies can include VoIP services like SIP, H.323, IAX, and MGCP (both gateways and phones), as well as more traditional TDM technologies like T1, ISDN PRI, analog POTS and PSTN services, Basic Rate ISDN (BRI), and more. Telephony applications include things such as call bridging, conferencing, voicemail, auto attendant, custom IVR scripting, call parking, intercom, and more.

2.2 Detailed Asterisk Architecture

Asterisk's core contains several engines that each play a critical role in the software's operation. When Asterisk is first started, the *Dynamic Module Loader* loads and initializes each of the drivers which provide channel drivers, file formats, call detail record back-ends, codecs, applications and more, linking them with the appropriate internal APIs. Then, Asterisk's *PBX Switching Core* begins accepting calls from interfaces and handling them according to the dialplan, using the *Application* Launcher for ringing phones, connecting to voicemail, dialing out outbound trunks, etc. The core also provides a standard *Scheduler and I/O Manager* that applications

and drivers can take advantage of. Asterisk's *Codec Translator* permits channels which are compressed with different codecs to seamlessly talk to one another. Most of Asterisk's usefulness and flexibility come from the applications, codecs, channel drivers, file formats, and more, which plug into Asterisk's various programming interfaces.



2.3 Network Examples

Asterisk is extremely flexible in the networks that can be built, but it's probably useful to present a few sample network diagrams.

2.3.1 The Mythical 1x1 PBX

One question that is often heard is “How small of a PBX can you build with Asterisk?”. Well, you can make a PBX as small as one port of PSTN and one port of analog or IP phone. Yes, it is true that you can make a PBX with just one port, but it isn't very useful unless

you just enjoy leaving yourself voicemail or talking to an autoattendant. In the above diagram an analog phone could be connected directly to PC running Asterisk, and in turn either to an IP phone over ethernet, or to an analog phone over an S100U USB to FXS converter, for example. Such a PBX can provide voicemail, act as a gateway, or provide some sort of basic IVR script, (such as controlling your lights with X10, for all you home automation geeks out there).

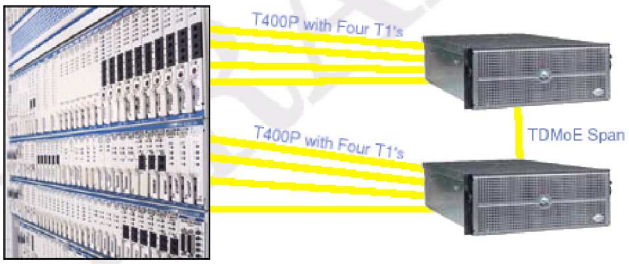
2.3.2 An 8x16 Small Office PBX

A more typical office scenario is to provide greater density of phones on the inside of phone network than is presented on the outside of a network. In the above example, eight phone lines and 16 analog telephones are brought into a *channel bank* which multiplexes the channels into a single T1 interface, which would then run on a cable just a few feet to a Linux PC (with a T1 card such as the T100P), where Asterisk would provide dialtone. In addition, VoIP phones could be connected via Ethernet, augmenting the number of phones that can be deployed. Even with such a relatively small setup, you can take advantage of call conferencing, voicemail (with individual mailboxes for everyone), the ability to check voicemail over the web, custom IVR scripting, autoattendant, and other features to make all your friends jealous.

2.3.3 SME with Remote Offices

One of Asterisk's most powerful features is its ability to link remote offices of a SME (that's “Small to Medium Enterprise”) together. The above diagram shows how you can build individual small PBX's for multiple offices using Asterisk, and then link them together transparently into a single network.

2.3.4 High Density IVR and Conferencing



Asterisk can be used as a high density IVR and conferencing platform, using traditional PRI/T1 interfaces, and providing redundancy, scalability, and intercommunication using TDM over Ethernet, which permits Asterisk to extend the TDM bus across the ethernet network, while retaining minimal latency.

2.4 Filesystem Organization

Asterisk's organization is designed to follow Linux tradition, and is grouped into several directories.

/etc/asterisk

The */etc/asterisk* directory contains all of Asterisk's configuration files. For more information on configuration files, see the configuration section of this document.

/usr/sbin

The system binary directory */usr/sbin* contains actual Asterisk executables and scripts, including *asterisk*, *astman*, *astgenkey* and *safe_asterisk.*

/usr/lib/asterisk

Contains binary objects related to Asterisk which are architecture specific.

/usr/lib/asterisk/modules

Contains runtime modules for applications, channel drivers, codecs, file format drivers, etc.

/usr/include/asterisk

Contains header files required for building asterisk applications, channel drivers, and other loadable modules.

/var/lib/asterisk

Contains variable data used by Asterisk in its normal operation.

/var/lib/asterisk/agi-bin

Location of AGI scripts to be used by the AGI application in the dialplan.

DRAFT

/var/lib/asterisk/astdb

Asterisk database, roughly the Asterisk equivalent of the "Windows Registry." This file is never used directly, but its contents can be displayed and modified at the Asterisk command line with the "database" set of functions.

/var/lib/asterisk/images

Storage area for images referenced in dialplan and applications.

/var/lib/asterisk/keys

Storage area for public and private keys used for RSA authentication within Asterisk (especially IAX).

/var/lib/asterisk/mohmp3

Storage area for MP3 music on hold. Should contain any mp3's you want to be available for musiconhold. Note that musiconhold must still be configured in */etc/asterisk/musiconhold.conf*.

/var/lib/asterisk/sounds

Storage area for audio files, prompts, etc. used by Asterisk applications. Some prompts are further organized as subdirectories under the */var/lib/asterisk/sounds* directory.

/var/run

Asterisk stores runtime named pipes and PID files in the system standard /var/run directory

/var/run/asterisk.pid

Contains the primary process identifier (PID) of the running Asterisk process.

DRAFT

/var/run/asterisk.ctl

A named pipe used by Asterisk for enabling the "remote mode" of operation.

/var/spool/asterisk

Used for runtime spooled files of voicemail, outgoing calls, etc.

/var/spool/asterisk/outgoing

Monitored by Asterisk for outbound calls. When a file is created in */var/spool/asterisk/outgoing*, Asterisk parses the file and attempts an outbound call which is then dumped into the PBX if it is answered. For more information see the section "Outbound Calls"

/var/spool/asterisk/qcall

Used for the now deprecated qcall application. Do not use.

/var/spool/asterisk/vm

Storage of voicemail boxes, announcements, and folders

2.5 Naming Channels

Understanding Asterisk channel naming convention is critical to using it effectively. Outgoing channel names (used, for example, with the Dial application) are named in the format:

```
<technology>/<dialstring>
```

The <*technology*> parameter represents which sort of interface one is trying to create or reference (e.g. SIP, Zap, MGCP, IAX, etc). The <*dialstring*> is a driver-specific string representing the destination desired. This section describes the naming convention for each channel type.

2.5.1 Zap: Zaptel TDM Channels

Outgoing:

The basic formats of a Zap channel name are:

> Zap/*[g]*<*identifier*>*[c][r*<*cadence*>*]*

Where <*identifier*> is a numerical identifier for the physical channel number of the desired channel. If the identifier is prefixed by the letter *g*, then the number is interpreted as a *group* number instead of as a channel (See Zapata.conf). The identifier may be followed by one or more options. If the letter *r* and a number follow, that number is used as a "distinctive ring" for this dial command (valid numbers are 1-4). If the letter *c* follows, then "Answer Confirmation" is requested, in which the call is not considered answered until the *called* user presses '#'.

> **Zap/1** – TDM Channel 1
> **Zap/g1** – First available channel in group 1
> **Zap/3r2** – TDM Channel 3 with 2nd distinctive ring
> **Zap/g2c** – First available channel in group 2 with confirmation

Incoming:

Incoming Zap channels are labeled simply:

> Zap/<channel>-<instance>

Where <*channel*> is the channel number and <*instance*> is a number from 1 to 3 representing which of up to 3 logical channels associated with a single physical channel this is.

> **Zap/1-1** – First call appearance on TDM channel 1
> **Zap/3-2** – Second call appears on TDM channel 3

2.5.2 SIP: Session Initiation Protocol Channels

Outgoing:

Outgoing channels typically take the form:

> SIP/[<*exten*>@]<peer>[:<*portno*>]

Where <*peer*> is the name of the peer (or hostname/IP of the remote server), <*portno*> is an optional port number (the default is the SIP standard port 5060), and <*exten*> is an optional extension.

> **SIP/ipphone** – SIP peer "ipphone"
> **SIP/8500@sip.com:5060** – Extension 8500 at sip.com, port 5060

Incoming:

Incoming SIP channels are of the form:

> SIP/<*peer*>-<*id*>

Where <*peer*> is the identified peer and <*id*> is a random identifier to be able to uniquely identify multiple calls from a single peer.

> **SIP/192.168.0.1-01fb34d6** – A SIP call from 192.168.0.1
> **SIP/sipphone-45ed721c** – A SIP call from peer "sipphone"

2.5.3 IAX: Inter-Asterisk eXchange Channels

Outgoing

Outgoing IAX channels take the form:

```
IAX/[<user>[:<secret>]@]<peer>[:<portno>][/<exten>[@<context>][
/<options>]]
```

Where <*user*> and <*secret*> are optional username and secret to use to connect to the host identified by <*peer*> and an optional port number <*portno*>, optionally requesting a specific extension <*exten*> at an optional context <*context*>, and optionally with <*options*> connection options, of which only "a" is currently defined for "request autoanswer."

IAX/mark:asdf@myserver/6275@default – Call to "myserver" using "mark" as username and "asdf" as password, and requesting extension 6275 in default context

IAX/iaxphone/s/a – Call to "iaxphone" requesting immediate answer.

IAX/guest@misery.digium.com – Call Digium

Incoming:

Incoming IAX channels are of the form:

```
IAX[[<username>@]<host>]/<callno>
```

Where <*username*> is the username, if known, <*host*> is the apparent host connecting, and <*callno*> is the local call number.

IAX[mark@192.168.0.1]/14 – Call number 14 from user "mark" at 192.168.0.1

IAX[192.168.10.1]/13 – Call 13 from 192.168.10.1

Chapter 3: Running Asterisk

Running Asterisk is actually rather straight forward. Asterisk, if run with no arguments, is launched as a daemon process. Often, it is useful to execute Asterisk in a verbose, console mode, providing you with useful debugging and state information, as well as access to the powerful Asterisk command line interface.

3.1 Asterisk Command Line Arguments

Like most Linux applications, Asterisk has several command line options. These are tpyically preceeded by a "-", and several options may be specified in a row after a single "-". For example:

```
# asterisk -vvvgc
```

The above example is probably the most commonly used asterisk command line.

-c

Enables console mode. If console mode is enabled, Asterisk will provide a command line that can be used to issue commands and view the state of the system. Implies **-f** as well

-C *<configfile>*

Executes Asterisk with a different configuration file.

-d

Enables extra debugging across all modules.

-f

Prevents Asterisk from daemonizing into the background.

DRAFT

-g

Forces Asterisk to dump core in the unlikely event of a segmentation violation.

-h

Displays basic command line help.

-i

Forces Asterisk to prompt for cryptographic initialization passcodes at startup.

-n

Disables ANSI color support.

-p

Run with a real-time priority.

-q

Run in quiet mode.

-r

Connects to an already running instance of Asterisk.

-v

Causes asterisk to produce more verbose output. More -*v*'s mean more verbose.

-x <*command*>

Executes a command in Asterisk (when combined with -r)

DRAFT

3.2 Asterisk Command Line Interface

The Asterisk command line is one of the most powerful interfaces for obtaining status on a running Asterisk. Although a complete description of all options is beyond the scope of this document, a brief introduction is certainly in order. When running Asterisk with the **-r** or **-c** flag, the user is provided with the Asterisk CLI prompt, which looks, unimpressively, like this:

```
*CLI>
```

or

```
localhost*CLI>
```

In any case, once you are at the command line, you enter instructions by typing them in and pressing enter. The Asterisk CLI includes command completion, available by pressing the *tab* key. The most obvious, and useful, command is `help`, which will show you a list of all the Asterisk CLI commands you can enter:

```
*CLI> help
    add extension Add new extension into context
.
.
.
 zap show channel Show information on a channel
*CLI>
```

DRAFT

For more information about a *specific* command, you can type `help <command>`. For example:

```
*CLI> help soft hangup
Usage: soft hangup <channel>
       Request that a channel be hung up.  The
       hangup takes effect the next time the
       driver reads or writes from the channel
*CLI>
```

This shows you that the soft hangup command takes an argument (a channel name) and that it requests the channel be hungup. This command can be used, for example, to hangup any active call in the system.

A few more extremely useful commands:

iax debug:	Enable IAX debugging
mgcp debug:	Enable MGCP debugging
reload:	Reload configuration files
restart when convenient:	Restarts Asterisk when all calls are gone
show agi:	Displays AGI commands
show applications:	Shows all Asterisk apps
show application <*app*>:	Shows usage of a specific Asterik app
show channels:	Shows all active channels
show channel <*channel*>:	Shows information on a specific channel
sip debug:	Enable SIP debugging
stop now:	Stops Asterisk immediately

Chapter 4: The Asterisk Dialplan

The most important part of understanding Asterisk is understanding its dialplan. It is the dialplan which routes every call in the system from its source through various applications, to its final destination. Everything from voicemail, to conferencing, to autoattendant voice menus is done through a consistent concept and logic.

4.1 Introduction to Extension Contexts

4.1.1 Extension Contexts Uses

The dialplan is composed of one or more *extension contexts*. Each extension context is itself simply a collection of extensions. Each extension context in a dialplan has a unique name associated with it. The use of contexts can be used to implement a number of important features including:

Security – Permit long distance calls from certain phones only
Routing – Route calls based on extension
Autoattendant – Greet callers and ask them to enter extensions
Multilevel menus – Menus for sales, support, etc.
Authentication – Ask for passwords for certain extensions
Callback – Reduce long distance changes
Privacy – Blacklist annoying callers from contacting you
PBX Multihosting – Yes, you can have "virtual hosts" on your PBX
Daytime/Nighttime – You can vary behavior after hours
Macros – Create scripts for commonly used functions

The goal of this chapter is to familiarize you with the concepts behind the dialplan, show some examples, and empower you with the knowledge you need to perform neat tricks and impress friends, coworkers, and competitors with your Asterisk-foo like a pro.

4.1.2 Basic Extension Context

An example extension context might look something like this:

default	
Extension	***Description***
101	Mark Spencer
102	Wil Meadows
103	Greg Vance
104	Check voicemail
105	Conference Room
0	Operator

In this example context (called "default"), the first three extensions (101 to 103) all would be associated with ringing phones belonging to various employees. The fourth extension (104) would be associated with allowing someone to check their voicemail. The fifth extension (105) would be associated with a conference room. Finally, the "0" extension would be associated with the operator.

4.1.3 Sample Voice Menu

Another example extension context might look like this:

mainmenu	
Extension	***Description***
s	Welcome message and instructions
1	Sales
2	Support
3	Accounting
9	Directory
#	Hangup

This example, called “mainmenu” has only single digit extensions. The “s” extension is the *start* extension, where the caller begins. This extension would play a message along the lines of “Thank you for calling OurCompany. Press 1 for sales, 2 for support, 3 for accounting, 9 for a company directory, or # to hangup.” Each menu option is, in fact, an extension and could either dial someone's real extension, or could send someone to another menu for example.

4.1.4 Pattern Matching

Extensions can also match patterns, instead of being single digits. Patterns to be pattern matched must start with the underscore character (“_”) and may use any of the following special characters:

X	– Any digit from 0-9
N	– Any digit from 2-9
[14-6]	– Any a 1,4, 5, or 6
.	– Matches anything

Consider the following context for example:

routing	
Extension	***Description***
_61XX	Dallas Office
_62XX	Huntsville Office
_63XX	Dallas Office
_7[1-3]XX	San Jose Office
_7[04-9]XX	Los Angeles Office

This context (called “routing”) splits calls according to their extension to be sent to various servers. In this example, it is assumed all extensions are four digits long (Asterisk has no such requirement, of course, nor is there a requirement that all extensions be the same length. Anyway, anything starting with 61, would be sent to the

Dallas office, 62 would go to the Huntsville office and so on. Anything starting with 71, 72, or 73 would go to San Jose.

4.1.5 Context Inclusion

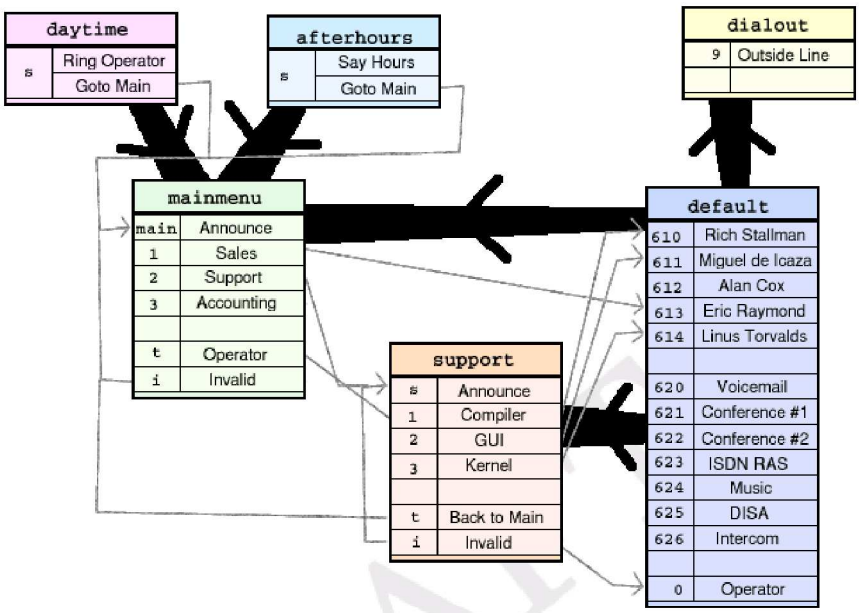
One extension context can include the contents of another. For example, consider the following contexts:

longdistance	
Extension	***Description***
_91NXXNXXXXXX	Long distance calls
include => “local”	

local	
Extension	***Description***
_9NXXXXXX	Local calls
include => “default”	

Here, a context called “local” provides a single extension for dialing local calls, and includes the “default” extension as well. Then, there is a “longdistance” context which includes an extension for long distance calling, and includes the “local” context. Phones which are in the “longdistance” context would be able to make long distance calling. Those in “local” could only make 7 digit local calls, and those in the “default” context would not have outside line access at all. Thus, using extension contexts, you can carefully control who has access to toll services.

4.2 Complete Set of Contexts



A more complete example of a dialplan may be helpful. Here is a dialplan for a fictional Open Source company. Several contexts are listed with familiar names. Thick black lines indicate an extension context being included in another. A slim gray line indicates one extension sending you into another extension or extension context. In general, extensions that are local to your company should be listed under *default* context since they should be accessible by anyone at more-or-less anytime. Typically, no actual phones would be associated with the default context alone, but it could be associated with a VoIP "guest" account, for example. A *local* (in this case *dialout*) context can include the default context as well as either local only or long distance dialing. It is important that access to the local context not be permitted from "guest" accounts, unless it is your intention to let people use your local phone resources. Next we have a couple of menu contexts, *mainmenu* and *support*. Both of these present menus while including the default context so that direct extensions may be dialed at any time. The mainmenu context

includes both *daytime* and *afterhours* so that an incoming call rings to an operator first during the day, and directly to an announcement about company hours in the evening.

4.3 Defining Extensions

Unlike a traditional PBX, where extensions are associated with phones, interfaces, menus, and so on, in Asterisk an extension is defined as a list of *applications* (and arguments) to run. Each step of an extension is referred to as a *priority*. Each priority is generally executed in-order, although applications (especially "Dial" and "Goto" may redirect a call to a different priority. When an extension is dialed, each priority is executed until either the call is hungup, an application returns -1, or the call is routed to a new extension. Each step in an extension is typically notated as follows:

```
exten => <exten>,<priority>,<application>, [(<args>)]
```

4.3.1 Basic Extension Example

Consider the following example:

```
exten => 100,1,Wait(1)
exten => 100,2,Answer
exten => 100,3,Playback(demo-congrats)
exten => 100,4,Hangup
```

This creates an extension with four steps. When a call enters this extension, the first thing that happens is that Asterisk waits for one second. Then, Asterisk answers the call (if it hasn't already been answered). Third, it plays back an audio file called "demo-congrats" and finally it hangs upon the caller. If the caller hungup at any point while Asterisk was processing the extension, processing would be terminated at that point.

4.3.2 Dialing a Phone

The most common sort of extension is that for dialing out another interface. Calling out another interface is done with the "Dial" application. While the "Dial" application has a very extensive list of options (see Dial reference), this example uses it only in its most basic form:

```
exten => 100,1,Dial(Zap/1,20)
exten => 100,2,Voicemail(u100)
exten => 100,102,Voicemail(b100)
```

This example illustrates one of the few exceptions to execution of an extension being out of order. When this extension is entered, the first thing Asterisk does is attempt to dial out the "Zap/1" interface for a maximum of 20 seconds. If the interface is busy, it will jump to priority *n+101* if such a priority exists in this extension. In this case, we have such a priority (102), which sends the caller to voice mailbox 100, preceeded with a "busy" announcement (something like "The person at extension 100 is on the phone"). If there was simply no answer (or if there was a busy and we didn't have a step 102), then execution would continue at step 2, where the caller is put into voice mailbox 100, but with an unavailable announcement (something like "The person at extension 100 is currently unavailable").

4.3.3 Routing by Caller ID

This example, often known as the "Anti-Ex Girlfriend" extension, shows how Asterisk can route not only by called number, but by *calling* number.

```
exten => 100/2565551212,1,Congestion
exten => 100,1,Dial(Zap/1,20)
exten => 100,2,Voicemail(u100)
exten => 100,102,Voicemail(b100)
```

This example builds upon the previous by adding a special rule that if the caller is 2565551212 (routing by Caller ID is indicated by placing a "/" and the Caller ID number to match immediately following), they are immediately presented with Congestion tone. Other callers proceed normally. A more common example of routing by CallerID is:

```
exten => 100/,1,Zapateller
exten => 100,1,Wait(0)
exten => 100,2,Dial(Zap/1)
```

In this example, if a call is received with *no* Caller ID, then the Zapateller application is run (which plays the familiar "special information tone" which you hear when you call a number that is not in service, often times causing autodialers to disconnect). If Caller ID is provided, then "Wait" is executed for 0 seconds (in otherwords, "do nothing"). In either case, the Zap/1 channel is then rung indefinitely (i.e. No timeout).

4.3.4 Ringing Phones in Sequence

Often it is desired that a given extension first ring one phone, and then if there is no answer, ring another phone (or set of phones). Consider this "Operator" example:

```
exten => 0,1,Dial(Zap/1,15)
exten => 0,2,Dial(Zap/1&Zap/2&Zap/3,15)
exten => 0,3,Playback(companymailbox)
exten => 0,4,Voicemail(100)
exten => 0,5,Hangup
```

In this example, when a caller would dial "0" for the operator, we first trying ringing the interface Zap/1 (which is the phone that the receptionist uses for example). If that interface is busy, or there is no answer after 15 seconds, we try ringing a group of phones (including

the receptionist's phone again) for another 15 seconds. If there is still no answer (or if everyone is busy) then it will playback a message announcing that no one is available, and to please leave a message in the company mailbox. Finally the caller is dumped into voice mailbox 100, without having any additional announcement played.

4.3.5 Basic Voice Menu

A voice menu is typically implemented as its own extension context.

```
[sales]
exten => s,1,Background(welcome-sales)
exten => 1,1,Goto(default,100,1)
exten => 2,1,Goto(default,101,1)

[mainmenu]
exten => s,1,Background(welcome-mainmenu)
exten => 1,1,Goto(sales,s,1)
exten => 2,1,Dial,Zap/2
exten => 9,1,Directory(default)
exten => 0,1,Dial,Zap/3
```

An announcement is usually played on the “s” extension, upon entering the menu. Then, the “Background” application plays a prompt, while waiting for the user to enter an extension. The above example presents two menus, one called “mainmenu” and one called “sales.” When a caller entered the “mainmenu” context, they would hear some sort of announcement (like “Press 1 for sales, 2 for support, 9 for a directory, or 0 for an operator”). Upon entering a “1”, the caller would be transferred to the “sales” menu, which would in turn present other options. Dialing 2 would ring Zap/2, 0 would ring Zap/3, and 9 would present the user with a company directory.

4.3.6 Using Variables

Asterisk can make use of global and channel specific variables for arguments to applications. Variables are expressed in the dialplan using ${foo} where “foo” is the name of the variable. A variable

DRAFT

may be any alphanumeric string beginning with a letter, but there are some variables whose names have special meanings. Specifically:

${CONTEXT}	– The current context
${EXTEN}	– The current extension
${EXTEN:*x*}	– The current extension with *x* leading digits dropped
${PRIORITY}	– The current priority
${CALLERID}	– The current Caller ID (name and number)
${CALLERIDNUM}	– The current Caller ID number
${CALLERIDNAME}	– The current Caller ID name
${RDNIS}	– The current redirecting DNIS

Global variables may be specified in the [globals] section of the dialplan. Consider the following example:

```
[globals]
MARK => Zap/1
GREG => Zap/2&SIP/pingtel
WIL => Zap/3
JUDY => Zap/4

[mainmenu]
exten => 1,1,Dial(${GREG}&${MARK})
exten => 2,1,Dial(${WIL}&${JUDY})
exten => 3,1,Dial(${JUDY}&${MARK})
```

By organizing the dialplan in this fashion, it is easy to change the physical interfaces for any particular user and have all references to them in the dialplan update instantly as well.

4.3.7 Including Contexts

One context can include zero or more other contexts, optionally with a date/time limitation. Contexts are included in the order they are listed. The format for include is:

```
include => <context>[|<hours>|<weekdays>|<monthdays>|<months>]
```

Where <*context*> is the context to be include, <*hours*> are the hours in which this include is considered valid (in the form of a range, in military time, e.g. 9:00-17:00), <*weekdays*> are the days of the week considered valid (e.g. mon-fri), <*monthdays*> are the days of the month considered valid (e..g 22-25), and <*months*> are the months considered valid. Consider the following example:

```
[salespeople]
exten => 1000,1,Dial(Zap/1)
exten => 1000,2,Voicemail(u1000)
exten => 1001,1,Dial(Zap/2)
exten => 1001,2,Voicemail(u1001)

[techpeople]
exten => 2000,1,Dial(SIP/2000)
exten => 2000,2,Voicemail(u2000)
exten => 2001,1,Dial(SIP/2001
exten => 2001,2,Voicemail(u2001)

[default]
include => salespeople
include => techpeople
```

DRAFT

In this example, the default context simply includes two other contexts, thus making the contexts smaller and easier to track someone down in.

4.3.8 Daytime/Nighttime Modes

Including contexts can be used to implement daytime and nighttime modes (and even holiday modes) by taking advantage of the ability to make includes based upon times and dates. Consider the following example:

```
[newyears]
exten => s,1,Playback(happy-new-years)

[daytime]
exten => s,1,Dial(Zap/1,20)

[nighttime]
exten => s,1,Playback(after-hours-msg)

[default]
include => newyears||||1|jan
include => daytime|9:00-17:00|mon-fri
include => nighttime
```

In this example, the normal mode of operations is the nighttime mode.

4.3.9 Outbound Dialing

Outbound dialing can be done either by directly connecting a short extension (e.g. "9") with an outbound line, or by establishing full length extensions for numbers to be dialed. Consider the following example:

```
[directdial]
ignorepat => 9
exten => 9,1,Dial(Zap/g2/)
exten => 9,2,Congestion

[international]
ignorepat => 9
exten => _9011.,1,Dial(Zap/g2/${EXTEN:1})
exten => _9011.,2,Congestion
include => longdistance

[longdistance]
ignorepat => 9
exten => _91NXXNXXXXXX,1,Dial(Zap/g2/${EXTEN:1})
exten => _91NXXNXXXXXX,2,Congestion
include => local
```

```
[local]
ignorepat => 9
exten => _9NXXXXXX,1,Dial(Zap/g2/${EXTEN:1})
exten => _9NXXXXXX,2,Congestion
include => default
```

This example creates 4 separate contexts with various levels of access to the phone network. First, it is assumed that one wants "9" to be the number for connecting to an outside line. The *ignorepat* lines instruct Asterisk's channel drivers not to take away dialtone when that pattern is dialed, so that even after the caller dials 9, they still have a dialtone. The *local* context is able to dial only 7 digit numbers, in addition to anything in the default context. The calls are sent out using any channel in "group 2" of the Zaptel driver, after stripping the "9" off. The *longdistance* context is permitted to dial any 1+ number as well as anything in the local context. The *international* context gives the caller the ability to connect to any number starting with 011+, in addition to anything in the *longdistance* context. The *directdial* context connects a user directly to a trunk when the caller dials 9.

4.3.10 Failover Trunking and LCR

One of Asterisk's most useful cost-saving features is the ability to build simple Least Cost Routing (LCR) tables, including with failover. Consider the following optimized dialplan:

```
[tolllongdistance]
exten => _91NXXNXXXXXX,1,Dial(Zap/g2/${EXTEN:1})
exten => _91NXXNXXXXXX,2,Congestion

[hsvlongdistance]
exten => _91256NXXXXXX,1,Dial(IAX/hsv/${EXTEN})
exten => _91256NXXXXXX,2,Dial(Zap/g2/${EXTEN:1})
exten => _91256NXXXXXX,3,Congestion

[longdistance]
include => hsvlongdistance
include => tolllongdistance
```

```
include => local
```

In this example, the long distance context is setup to attempt to use a remote VoIP host called *hsv* (presumably in Huntsville) to dial calls with a 256 area code. Failing that, it will use the TDM group 2 interface (presumably a toll call) to dial (in case the host is unavailable or unreachable for example).

4.3.11 Using Macros

While the Asterisk extension logic is very flexible, it can also be very verbose when creating many extensions which are very similar. In order to ease this task, you can take advantage of *macros* which simplify dialplans and make it easier to modify flows on a large scale. Macros are implemented by creating an extension context whose name begings with "macro-", followed by the name of the macro. Execution begins at the "s" extension and ends as soon as the extension drops to a location that is no longer within the macro. Macros define some useful local variables, specifically:

${MACRO_EXTEN}	– The extension calling the macro
${MACRO_CONTEXT}	– The extension context calling the macro
${MACRO_PRIORITY}	– The active priority when the macro was called
${MACRO_OFFSET}	– If set, causes the macro to attempt to return to *n* + *${MACRO_OFFSET}*
${ARG*n*}	– The *n*th argument passed to the macro.

Consider the following example:

```
[macro-oneline]
;
; Standard one-line phone.
;
; ${ARG1} - Device to use
;
exten => s,1,Dial(${ARG1},20)
exten => s,2,Voicemail(u${MACRO_EXTEN})
exten => s,3,Hangup
exten => s,102,Voicemail(b${MACRO_EXTEN})
exten => s,103,Hangup

[macro-twoline]
;
; Standard two-line phone.
;
; ${ARG1} - First phone
; ${ARG2} - Second phone
;
exten => s,1,Dial(${ARG1},20)
exten => s,2,Voicemail(u${MACRO_EXTEN})
exten => s,102,Dial(${ARG2},20)
exten => s,103,Voicemail(b${MACRO_EXTEN})

[default]
exten => 1000,1,Macro(oneline,Zap/1)
exten => 1001,1,Macro(oneline,SIP/1001)
exten => 1002,1,Macro(twoline,Zap/3,Zap/4)
```

After doing the complex work of defining the *oneline* macro for a single line phone and the *twoline* macro for a two-line phone, implementing the default context becomes extremely easy, and each extension requires only a single line instead of several similar lines.

Chapter 5: Configuration Files

5.1 Introduction to Config Files

Most of Asterisk's flexibility is controlled through configuration files located in the /etc/asterisk directory. Its configuration syntax was designed to be easily parseable both by software (like configuration GUI interfaces) and by humans (like, presumably, you). The format of Asterisk config files is , ironically,most similar to the *win.ini* format back in the days of Microsoft® Windows 3.1. The file is a flat ASCII formatted file divided into sections, which are titled with a section name in square brackets, followed by keyword value pairs separated by the equals sign, or equals greater-than. Semicolon is the comment character (since '#' can be useful, especially in extensions). Blank lines are ignored. Here is an example configuration file:

```
;
; The first non-comment line in a config file
; must be a section title
;
[section1]
keyword = value      ; Variable assignment

[section2]
keyword = value
object => value      ; Object declaration
```

Asterisk's configuration parser interprets "=" and "=>" identically, and the syntax is used solely for the benefit of making more obvious to a person reading the file which pairs represent options, and which pairs represent the creation of some sort of object.

5.2 Configuration File Grammars

Although all of Asterisk's configuration files share the same syntax, there are at least three distinct grammars that are typically used.

5.2.1 Simple Groups (e.g. voicemail.conf

The "Simple Groups" format is (not surprisingly) the simplest format and is used by configuration files in which objects are declared with *all options on the same line*. Examples include extensions.conf, meetme.conf, voicemail.conf and others. Consider this example:

```
[mysection]
object1 => option1a,option2a,option3a
object2 => option1b,option2b,option3b
```

In this example, "object1" is created with options "option1a," "option2a" and "option3a" while "object2" is created with "option1b," "option2b" and "option3b."

Individual Entities

The "Individual Entities" configuration syntax is used by configuration files in which objects are declared with many options, and where those options are rarely shared with other objects. In this format, a section is associated with each object (there is sometimes a *general* or similar section for any global configuration options). For example:

```
[general]
globaloption1=globalvalue1
globaloption2=globalvalue2

[object1]
option1=value1a
option2=value2a

[object2]
option1=value1b
option2=value2b
```

In this example, a general section defines two global variables "globaloption1" and "globaloption2" with values "globalvalue1" and

"globalvalue2" respectively. Then, two objects are created ("object1" and "object2") with two options each.

5.2.2 Inherited Option Object (e.g. zapata.conf)

The "Inherited Option Object" format is used by zapata.conf, phone.conf, mgcp.conf and other interfaces in which there are many options, but where most interfaces or objects share the same value for options as others. In this class of configuration file, typically there are one more sections which contain declarations of one or more channels (or objects). The options for the object are specified above the declaration of the object and may be changed afterwords for another object declaration. This is probably one of the more unusual concepts to understand, but once you do, you will almost certainly find it extremely easy to use. Consider this very basic example:

```
[mysection]
option1 = foo
option2 = bar
object => 1
option1 = baz
object => 2
```

The first two lines set the value of options "option1" and "option2" to "foo" and "bar" respectively. When object "1" is instantiated, it is created with its option1 being "foo" and its option2 being "bar." After declaring object "1", we change the value of option1 to "baz" and create a new object "2." Now, object "2" is created with its option1 being "baz" and its option2 remaining "bar" just as with object "1." Again, changing the value of "option1" *after* the declaration of object "1" does not affect its value in object 1, only in object 2.

DRAFT

5.2.3 Complex Entity Object (e.g. iax.conf)

The "Complex Entity Object" format is used by iax.conf, sip.conf, and other interfaces in which there are numerous entities, with many options, which typically do not share a great deal of common settings. Each entity receives its own context (sometimes there is a reserved context such as "general" for global settings). Options are then specified in the context declaration. Consider:

```
[myentity1]
option1=value1
option2=value2

[myentity2]
option1=value3
option2=value4
```

The entity *myentity1* has values *value1* and *value2* for options *option1* and *option2* respectively. Entity *myentity2* has values *value3*and *value4* for options *option1* and *option2* respectively.

5.3 Channel Interfaces

This section defines, in detail, the configuration files for various Asterisk channel drivers.

5.3.1 zapata.conf

Synopsis

The zapata.conf file contains parameters relating to TDM channels provided by the Zaptel interface layer. Channels must be defined in this file before they can be used by Asterisk. In addition, a number of features relating to Asterisk's operation of the channels may be configured here.

DRAFT

Arrangement

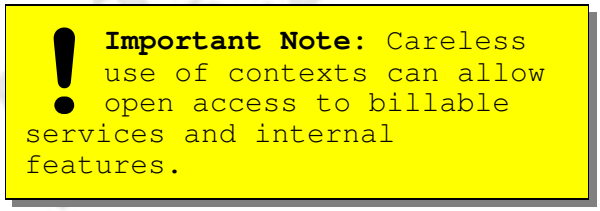
The zapata.conf file consists of keyword and value pairs. Keywords set parameters for the operation of channels. They may be boolean (yes/no) or contain values specific to the keyword. Most keywords set parameters for the operation of channels. Values remain in effect for all following channel definitions until they are overidden.

Keywords

These keywords are available in zapata.conf.

context: Defines the initial context for the channel. This will be the context available to the channel upon the initiation of a call. Note that contexts are an important part of maintaining site security. The initial context will govern the availability of extensions to a given channel. If an extension is placed in a different context from the initial context, that extension is unavailable to the caller.

```
context = default
```



channel: Define a channel or range of channels. Each channel definition will inherit all options stated ahead of it in the file. Channels maybe specified individually, separated by commas, or as a range separated by a hyphen.

```
channel => 16
channel => 2,3
channel => 1-8
```

group: Allows a number of channels to be treated as one for the purpose of dialing. For dialing out, the channels will be called on a first available basis. For the purpose of ringing stations, all channels in the group will ring at once. Multiple group memberships may be specified with commas, and to signify no group membership, the portion after the equals sign may be omitted

```
group = 1
group = 2,3
group =
```

***switchtype*:** Sets the type of signalling used for a PRI line. Acceptable values are:

national:	National ISDN
dms100:	Nortel DMS100
4ess:	AT&T 4ESS
5ess:	Lucent 5ESS
euroisdn:	EuroISDN

```
switchtype = national
```

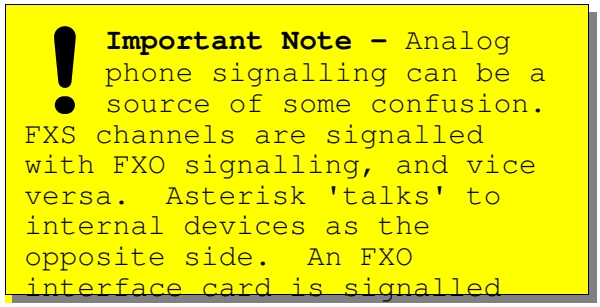
pri_dialplan: Sets an option required for some (rare) switches that require a dialplan parameter to be passed. This option is ignored by most PRI switches. It may be necessary on a few pieces of hardware. Valid options are: *unknown, local*, *private, national,* and *international*.

```
pri_dialplan = national
```

This option can almost always be left unset.

***signalling*:** Sets the signaling type for following channel definitions. These parameters should match the channels as defined in /etc/zaptel.conf. Correct choices are based on the hardware available. Asterisk will fail to start if a channel signaling definition is incorrect or unworkable, if the statements do not match zaptel.conf, or if the device is not present or properly configured.
Legal values for signalling are:

fxo_ks: FXO Kewlstart signalling. Used to signal an FXS device within the system, which would normally drive a handset or other station device. Kewlstart is Loopstart with Disconnect Supervision.
fxs_ks: The opposite side of fxo_ks. To signal an internal (or T1 connected) FXO device.
fxo_gs: Use FXO groundstart signalling.
fxs_gs: Use FXS groundstart signalling.
fxo_ls: Use FXO loopstart signalling
fxs_ls: Use FXS loopstart signalling
pri_cpe: Use PRI signalling, customer equipment side. Used when terminating a PRI line into Asterisk channels.
pri_net: Use PRI signalling, network side.
em: Use E&M signalling
em_w: Use E&M wink signalling
featd: Feature Group D, Adtran compatible. For use with the Atlas and similar equipment made by Adtran (DTMF version).
featdmf: Standard Feature Group D (MF version).
featb: Feature Group B



```
with FXS signalling by
Asterisk, and should be
configured as such.
```

```
signalling => fxs_ks
signalling => featd
```

Analog Call Progress

These items are used to attempt to emulate having a smarter line (like a PRI) that gives us call progress information, when using analog channels that don't pass us any digital information.

busydetect: Attempt to detect a standard busy signal on analog (FXS and FXO) or certain T1 signalling types (E&M, Wink, Feature Group D). This option can be used to determine when to hang up a call or to have Asterisk handle the busy condition internally. Takes 'yes' or 'no'.

callprogress: Used in combination with a variety of phone lines, enabling call progress will cause Asterisk to attempt to monitor the state of the call, and detect ringing, busy, and answered line. Note that this is not explicitly supported by the line technology, and is subject to errors, especially false answer detection. This only works with US phone tones at the time of writing. Takes yes or no.

```
busydetect = yes
callprogress = yes
```

Multi-link PPP Options (for PRI, requires network support):

These options are used to set adjust multi-link PPP options on PRI lines that support it. Multi-link PPP is a technology that allows channels on a PRI to be dynamically allocated between

voice and data. Asterisk can take voice channels allocated to it, dial a Remote Access Server, and dump the channels into a special extension that delivers the channel to the zaptel data layer. See ZapRAS.

minunused: The minimum number of unused channels available. If there are fewer channels available, Asterisk will not attempt to bundle any channels and give them to the data connection. Takes an integer.

minidle: The minimum number of idle channels to bundle for the data link. Asterisk will keep this number of channels open for data, rather than taking them back for voice channels when needed. Takes an integer.

idledial: The number to dial as the idle number. This is typically the number to dial a Remote Access Server (RAS). Channels being idled for data will be sent to this extension. Takes an integer that does not conflict with any other extension in the dialplan, and has been defined as an idleext.

idleext: The extension to use as the idle extension. Takes a value in the form of 'exten@context'. Typically, the extension would be an extension to run the application ZapRAS.

```
minunused => 2
minidle => 1
idleext => 6999@idle
idledial => 6999
```

Timing Parameters:

These keywords are used only with (non-PRI) T1 lines. All values are in milliseconds. These do not need to be set in most configurations, as the defaults work with most hardware. It has been noted that the common Adtran Atlas uses long winks of about 300

milliseconds, and channels from them should be configured accordingly.

prewink: Sets the pre-wink timing.
preflash: Sets the pre-flash timing.
wink: Sets the wink timing.
rxwink: Sets the receive wink timing.
rxflash: Sets the receive flash timing.
flash: Sets the flash timing.
start: Sets the start timing.
debounce: Sets the debounce timing.

```
rxwink => 300
prewink => 20
```

Caller ID Options:

These keywords set various Caller ID options, including turning certain features off and setting the Caller ID string for channels. Most Caller ID features default to on.

The following three options are boolean (yes/no).

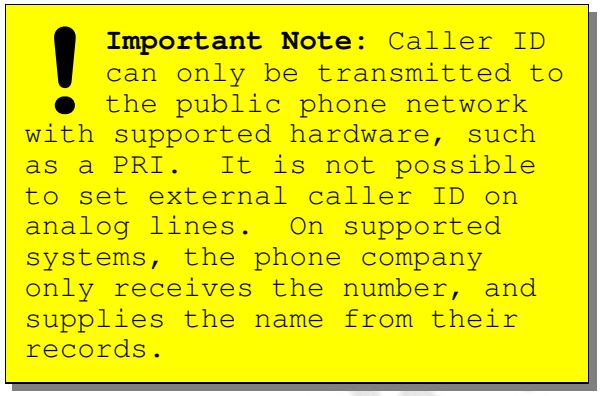
usecallerid: Disables or enables Caller ID transmission for the following channels.

hidecallerid: Sets whether to hide outgoing Caller ID. Defaults to no.

calleridcallwaiting: Sets whether to receive Caller ID during call waiting indication.

```
usecallerid => yes
hidecallerid => no
```

callerid: Sets the caller ID string for a given channel. This keyword takes a properly formatted string containing the name and phone number to be supplied as caller ID. Caller can be set to *asreceived* on trunk interfaces to pass the received Caller ID forward.




```
callerid = "Mark Spencer" <256 428-6000>
callerid =
callerid = asreceived
```

Call Feature Options

These options enable or disable the availability of advanced call features offered by Asterisk such as three-way calling and call forwarding on FXS (FXO signalled) interfaces. All of these options are boolean (yes/no).

threewaycalling: Sets whether to allow three-way calling from the channel.

cancallforward: Disables or enables call forwarding. Call forwarding is activated with *72 and deactivated with *73.

transfer: Disables or enables flash-hook call transferring. In order for this option to work, *threewaycalling* must also be set to yes.

immediate: When Asterisk is in immediate mode, instead of providing dialtone and reading digits, it immediately jumps into the "s" extension. This is often referred to as *batphone* mode.

adsi: Explicitly enables or disables support for ADSI. The ADSI specification is system similar to Caller ID to pass encoded information to an analog handset. It allows the creation of interactive visual menus on a multiline display, offering access to services such as voicemail through a text interface.

```
threewaycalling = yes
transfer = yes
immediate = no
adsi = yes
cancallforward = yes
```

Audio Quality Tuning Options:

These options adjust certain parameters of Asterisk that affect the audio quality of Zapata channels.

echocancel: Disable or enable echo cancellation. In almost every configuration it is recommended that this be left on (or left unstated, as the default is always on.) Takes 'yes', 'no', or a number of taps. Valid values of taps are 16, 32, 64, 128, or 256.

echocancelwhenbridged:? Enables or disables echo cancellation during a bridged TDM call. In principle, TDM bridged calls should not require echo cancellation, but often times audio performance is improved with this option enabled. Should be set on or left unset. Takes 'yes' or 'no'.

DRAFT

rxgain: Adjusts receive gain. This can be used to raise or lower the incoming volume to compensate for hardware differences. Takes a percentage of capacity, from -100% to +100%

txgain: Adjusts transmit. This can be used to raise or lower the outgoing volume to compensate for hardware differences. Takes the same argument as rxgain.

```
echocancel = yes
echocancelwhenbridged = no
rxgain = 20%
```

Call Logging Options:

These options change the way calls are recorded in the call detail records generated by Asterisk.

amaflags: Sets the AMA flags, affecting the categorization of entries in the call detail records. Accepts these values:

billing: Mark the entry for billing
documentation: Mark the entry for documentation.
omit: Do not record calls.
default: Sets the system default.

accountcode: Sets the account code for calls placed on the channel. The account code may be any alphanumeric string.

```
accountcode = spencer145
amaflags = billing
```

Miscellaneous Options

There are a few other keywords that don't fit neatly into the previous categories.

mailbox: This keyword can be set to allow Asterisk to offer an audible (and visual, if supported by the handset) message waiting indication when the station handset is picked up. When the *mailbox* keyword is defined and an unheard message exists in the associated Inbox, Asterisk will produce a stutter dialtone for one seconds after the phone is picked up. On supported hardware, the message waiting light will be activated. Takes as an argument a mailbox number (which must be defined in voicemail.conf).

language: Turn on internationalization and set the language. This feature will set all system messages to a given language. Though the feature is prepared, English is the only language that has been completely recorded for the default Asterisk installation.

stripmsd: Strip the 'Most Significant Digit,' the first digit or digits from all calls outbound on the given trunk channels. Takes as an argument the number of digits to strip. This option is deprecated, see the application 'StripMSD' or use ${EXTEN:*x*} for this functionality.

Complete File Example:

This is a complete example of a functional zapata.conf file. It is based on an 8 FXO by 16 FXS T1 channel bank.

```
[channels]

;set the FXO's in a group so we can dial out of
;them
;on a first-available basis

group = 1

;set the correct context for our dialout lines

context = pstn

;set the signalling (remember that we signal fxs
;channels
;with fxo, and vice versa)
```

```
signalling = fxs_ls

;set the AMA flags for clarity in the logs

amaflags = documentation

;define the channels that will be covered by the
;previous declarations (in this case all of our
;FXO's)

channel => 1-8

;reset the group, so we don't send outgoing
calls to
;the internal lines

group = 2

;change the context, so we can allow greater
;access to
;services to internal users

context = internal

;set the signalling on the station lines (fxs)
signalling = fxo_ks

;set a mailbox number on the following channels
mailbox = 1234

;set the callerid string (though since we don't
;have a PRI
;it's only seen inside, not on the PSTN.)

callerid = "Dave Schools" <256 555 1234>

;and state the channel this will apply to

channel => 9

;continue and state more channels with mailbox
;indication
;and caller id strings

mailbox = 1235
callerid = "Michael Houser" <256 555 1235>
channel => 10
```

DRAFT

```
mailbox = 1236
callerid = "John Bell" <256 555 1236>
channel => 11

mailbox = 1237
callerid = "Grace Slick" <256 555 1237>
channel => 12

;remember the downward inheritance of options.
;if the next channel doesn't have a voicemail
;box, we need
;to set an empty string, or he'll know whenever
;Grace has a message.  Also the callerid should
;be nulled as well

mailbox =
callerid =

;define a bunch of channels with no other
options

channel => 13-22

;Put this phone in a different context, so we
;can give it
; a different initial dialplan...perhaps a lobby
;phone
;with public access

context = lobby
callerid = "Lobby" <5000>
channel => 23
;and turn the callerid off

callerid =

;we can create a 'hotline' phone by placing a
;phone in a special context
;and setting it to answer immediately. In
;extensions.conf we can route
;the phone to an IVR, direct to security, or
;make it call Steak-Out

context => hotline
immediate => yes
channel => 24
```

DRAFT

5.3.2 sip.conf

Synopsis

The sip.conf file contains parameters relating to the configuration of Session Initiation Protocol (SIP) access to the Asterisk server. Clients must be configured in this file before they can place or receive calls using the Asterisk server.

Arrangement

The sip.conf file is read from the top down. The first section is for general server options, such as the IP address and port number to bind to. The following sections define client parameters such as the username, password, and default IP address for unregistered clients. Sections are delineated by a name in brackets. The first section is called general (which cannot be used as a client name.) The following sections begin with the client name in brackets, followed by the client options.

Keywords

The following keywords are defined in sip.conf.

General Section Keywords:

These settings are for the [general] section of sip.conf and adjust global settings for the SIP stack.

port: The port Asterisk should listen for incoming SIP connections. The default is 5060, in keeping with standards. Takes as an argument a port number (which must not be in use by any other service.)

bindaddr: The IP address Asterisk should listen on for incoming SIP connections. If the machine has multiple real or aliased IP addresses, this option can be used to select which IP addresses Asterisk listens on. The default behavior is to listen on all available interfaces and

aliases. Takes as it's argument an IP address (which must be an interface available on the system.)

context: Sets a default context all further clients are placed in, unless overridden within their entity definition.

allow: Explicitly allows a SIP codec. Note that codecs are preferred in the order they are allowed.

disallow: Explicitly disallows a SIP codec from being used.

tos: Configures type of service (TOS) used for SIP and SIP+RTP transmissions. Acceptable values are: *lowdelay, throughput, reliability,* and *mincost*. Also, an integer (0-255) may be specified.

maxexpirey: Maximum permitted length of a registration request in seconds.

defaultexpirey: Default length of a registration request in seconds.

register: Registers this Asterisk instance with another host. Takes a SIP address (without the sip:) optionally followed by a forward slash ('/') and an extension to use for contact.

```
[general]
port = 5060
bindaddr = 192.168.0.1
context = default
disallow = g729
allow = ulaw
allow = gsm
maxexpirey = 180
defaultexpirey = 160
register => 1234@mysipprovider.com/1234
register => 2345@myothersipprovider.com
```

Entity options:
After the general section are listed each entity in the SIP configuration. Entities are divided into three categories:

> *peer*: A SIP entity to which Asterisk sends calls (a SIP provider for example)
> *user*: A SIP entity which places calls through this Asterisk (A phone which can place calls only)
> *friend*: An entity which is both a user and a peer. This make sense for most desk handsets and other devices.

type: The type option sets the connection class for the client. Options are *peer*, *user*, and *friend*.

host: Sets the IP address or resolvable host name of the device. This can alternately be set to *'dynamic'* in which case the host is expected to come from any IP address. This is the most common option, and normally necessary within a DHCP network.

defaultip: This option can be used when the *host* keyword is set to *dynamic*. When set, the Asterisk server will attempt to send calls to this IP address when a call is received for a SIP client that has not yet registered with the server.

username: This option sets the username the Asterisk server attempts to connect when a call is received. Used when for some reason the value is not the same as the username the client registered.

canreinvite: This option is used to tell the server to *never* issue a reinvite to the client. This is used to interoperate with some (buggy) hardware that crashes if we reinvite, such as the common Cisco ATA 186.

context: When defined *within* a client definition, this keyword sets the default context for *this client only*.

dtmfmode: Selects whether DTMF digits should be sent in-band or out of band. Valid values are:

> *inband*: DTMF is send as audio in-band, and is detected in-band.
> *rfc2833*: DTMF is sent out-of-band using RFC2833 (default)
> *info*: DTMF is sent and received out of band using INFO messages (very rarely used)

mailbox: One or more mailboxes may be listed (separated by commas) for sending Message Waiting Indicator (MWI) messages to a given SIP peer.

qualify: A maximum time in milliseconds for a peer to respond. This causes Asterisk to poll the device periodically and consider it down if it takes longer than this number of milliseconds to respond.

secret: A shared secret used for authenticating registrations for peers and for users making calls.

nat: Causes Asterisk to interpret a peer or user as a potentially network address translated host. This is useful when peers are behind firewalls.

> ! Note that enabling the nat functionality causes Asterisk to violate the RFC specified ways of dealing with Contact: and SDP portions of calls, in order to try to work with NATed hosts. At the time of this writing, nat=yes is incompatible with Pingtel phones.

DRAFT

Complete SIP File Example:

The following is a complete example of a workable sip.conf file.

```
[general]
port=5060
bindaddr=192.168.0.10
context=default
register => 1234@mysipprovider.com

[snom]
type=friend
secret=snom100
host=dynamic
defaultip=192.168.0.15
mailbox=2345,1234

[cisco]
type=friend
secret=mysecret
host=192.168.0.20
canreinvite=no
mailbox=1234
context=trusted
```

DRAFT

5.3.3 iax.conf

Synopsis

This file is used to configure clients connecting via the Inter-Asterisk eXchange protocol. IAX is primarily used for passing calls between Asterisk servers. Frequently Multiple Asterisk servers are configured to intercommunicate with each other using this file. The iax.conf file is shared by both IAX version 1 and version 2 implementations.

Arrangement

The iax.conf file begins with a general section, which sets global server options. Within the general section, we can also configure the

Asterisk server to register as a client with a remote server, for access to the dialplan of another Asterisk system.

Following the general section, clients are defined, one per section. Sections are delineated by their name in brackets.

Keywords

The following keywords are used in iax.conf.

In the *general* section:

port: The port to listen on for incoming connections. The default is port 5036. Takes as it's argument a port number (which must not be in use by another service.)

bindaddr: If multiple IP addresses are available in the same system, this option may be set to bind Asterisk to a single interface.

```
port = 5036
bindaddr = 0.0.0.0
```

amaflags: Sets the AMA flags, affecting the categorization of entries in the call detail records. This keyword may also be set on a per client basis, within their client definition. Accepts these values:

billing: Mark the entry for billing
documentation: Mark the entry for documentation.
omit: Do not record calls.
default: Use the system default.

accountcode: Sets the default account code to log IAX calls to. This keyword can also be used within a client definition to set the account code for that client.

```
accountcode = wmeadows
amaflags = documentation
```

bandwidth: This option is used to control which codecs are used generally. Rather than allowing or disallowing specific codecs, this option may be set to *'low'* to automatically avoid some codecs that don't work well in low bandwidth sitiuations. Takes an option of *low* or *high.*

allow: Specifically allow a certain codec to be used. Takes a codec, or *all.* Using *all* is the same as specifying *bandwidth=high.*

disallow: Specifically disallow a certain codec. See *allow.*

```
bandwidth=low
disallow=all
allow=gsm
```

jitterbuffer: Turn on or off the jitter buffer. The jitter buffer is used to maximize audio quality by balancing latency against the number of dropped packets. A number of keywords exist to fine tune the jitterbuffer.

dropcount: Sets the maximum number of packets to be dropped in order to reduce latency, per memory size.

maxjitterbuffer: Sets the maximum size of the jitterbuffer.

maxexcessjitterbuffer: Sets the the maximum excess jitter buffer, which if exceeded, causes the jitter buffer to slowly shrink in order to improve latency.

register: Register is used to tell the Asterisk server to register with another Asterisk server. This is normally only needed if our local

server has a dynamic IP address and needs to tell the other server where to find it. The format of a register statement is:

```
register => username:secret@server
```

The 'secret' field is optional, if no secret has been specified on the server being connected to. If RSA encryption is in use, specify the key to send to the server with this format:

```
register => username:[key]@server
```

tos: Specify the type of service bits to set on IAX packets, which may improve routing of the packets. Available values are:

lowdelay: minimize delay
throughput: maximize throughput
reliability: maximize reliability
mincost: use the lowest cost path
none: use no routing flags

```
tos = lowdelay
```

Options for Entities

Entity definitions begin with the entity name in brackets. The name is followed by a number of keyword/value pairs applying to the entity in which they are set.

The following keywords are available for users:

type: This sets the type of entity for the client. Valid types are:

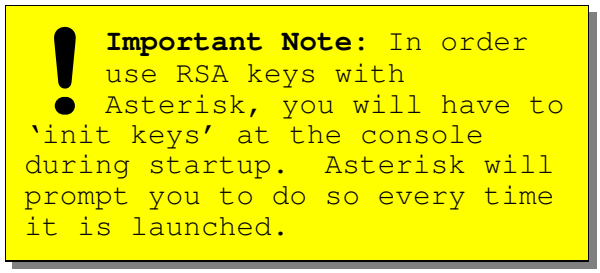
user: A user can place calls to or through the Asterisk server.
peer: A peer receives calls from the Asterisk server, but does not place them
friend: A friend both sends and receives calls through the Asterisk server. This makes the most sense for handsets or other station devices. When in doubt use this type.

context: When used within a client definition, this keyword overrides the default incoming context set in the general section for the user only.

callerid: Sets the Caller ID string to be used for this entity. This callerid string will be used internally, and sent to the PSTN if a PRI line is used to route the call to the outside world. If left blank, the Caller ID sent by the entity will be used instead

```
callerid => "Judy" <256 555-1234>
```

auth: Sets the authentication type. IAX supports three methods of authentication. The first (and least secure) is *plaintext*. The passwords (or secrets) are sent in clear text over the network. The second is *md5*, which uses an md5 challenge response algorithm. Both machines will have cleartext access to the passwords, but they will be confirmed using an md5 hash while passing over the network. The most secure option is to use RSA public/private key encryption to store and transmit the secret. Public/private key pairs can be generated using the included program astgenkey. The public key will need to be manually tranfered to the server and stored in /var/lib/asterisk/keys/*name*.pub. Server private keys are stored in the same location as *name*.key.



inkeys: The public keys to use to decrypt authentication for an incoming client request or registration.

outkey:The private key to encrypt outgoing authentication communication for this client.

```
auth=md5
secret=password
```

```
auth=rsa
inkeys=theirkey
outkey=mykey
```

permit: Hosts to permit to connect as this user. This can be a single host or a host/netmask pair.

deny: Hosts to deny for any incoming connection attempt as this user. *deny* takes the same argument format as *permit.*

```
deny = 0.0.0.0/0.0.0.0
permit=192.168.0.1/255.255.255.0
permit=216.207.245.45
```

host: Sets the expected outgoing host for this client. Can be set to an ip address or *dynamic,* which will allow incoming connections from any host (that is not explicitly denied.)

DRAFT

defaultip: The default IP address for an IAX client. This field is consulted if Asterisk receives a call for an IAX client that is dynamic and has not registered to let Asterisk know the current IP address. Takes as it's argument an IP address.

```
host=dynamic
defaultip=192.168.0.1
```

accountcode: When used within a client definition, sets the account code for that client only. This is used by the call logging service.

qualify: Tells Asterisk whether to test whether the peer is alive before attempting to connect the call. If set to yes Asterisk will periodically contact the peer before forwarding any call information. The argument specified is the maximum number of milliseconds that a peer can take to respond before it is considered "unavailable."

```
qualify=1000
```

mailbox: Provides a mailbox to associate with a given peer, so that when it registers it can be notified of any pending messages waiting.

```
mailbox=1234
mailbox=1002,1003
```

trunk: Enables or disables trunking for a given user or peer. Trunk mode is a more efficient method of operating IAX *if* there are typically many calls running on the link. Trunk mode *requires* having a Zaptel interface in the Asterisk server.

```
trunk=yes
```

Complete File Example

```
[general]
;set up some general items
port=5036

accountcode=iaxcalls
amaflags=default

bandwidth=low
allow=gsm
disallow=lpc10

jitterbuffer=yes
dropcount=3
maxjitterbuffer=500
maxexcessjitterbuffer=100

register =>
asterisk1:opensecret@telco.digium.com

context=iax

;from here on it's client definitions

[trustedhost]
host=192.168.0.50
trunk=yes
context=trusted

[authhost]
secret=foobar
host=dynamic
defaultip=68.62.178.239

[rsahost]
auth=rsa
inkeys=rsapublickey
host=dynamic
defaultip=216.207.245.55
accountcode=log1234
callerid="Mark Spencer" <256 428 6000>
```

DRAFT

5.4 Application Configurations

This section details the configuration file syntax for various Asterisk applications.

5.4.1 voicemail.conf

Synopsis

The voicemail.conf file configures system wide parameters for the voicemail system, and stores mailbox information including mailbox number to passcode mapping, box owner names, and e-mail addresses for message received notification.

Arrangement

The voicemail.conf file is arranged in two sections. The first section, *general*, contains system wide parameters such as the formats messages are to be stored in and the address e-mail from the voicemail system should appear to originate from. The second section, *default*, contains the configurations for individual voicemail boxes.

Keywords

The general section takes these keywords and options:

***format*:** Format sets the file formats for saving voicemails. If multiple formats are specified, all formats will be written, and the best available format will be used for playback. The format listed last is used for e-mailing voicemails, if that options is enabled. Available formats are:

> *gsm* : use raw gsm encoding. Best for VoIP.
> *wav*: MS wav format, 16 bit linear
> *WAV*: MS wav format, gsm encoded

g723sf: G.723.1 simple frame (note that Asterisk cannot directly encode , due to licensing issues. It can, however, store and transmit file received from an external source, i.e. from a SIP phone with a built in codec).

```
format=gsm|wav|WAV
```

In this example each received voicemail will be written in gsm, MS-GSM, and linear wav formats.

```
format=gsm
```

This example will store voicemails in raw gsm format only.

serveremail: Serveremail sets the e-mail address that voicemail-waiting e-mails should appear to originate from. This value will be used in the 'From:' field of the e-mail. Available options are any alphanumeric string, or any alphanumeric

Examples:

```
serveremail=asterisk
```

In this example the 'From:' field will be set to 'asterisk'. In most cases the outgoing mail server will append the local hostname.

```
 serveremail=asterisk@myhost.com
```

This example will set the e-mail to . This will normally NOT be rewritten by the outgoing mail server. This is useful if you want the

e-mail to appear to come from a hostname other than the hostname of the local machine.

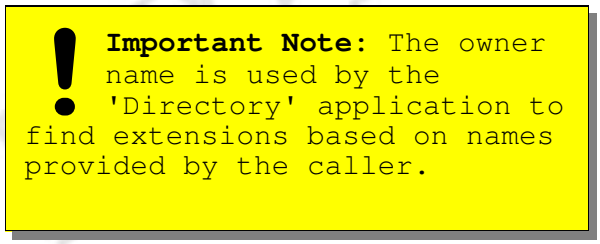
***append*:** Append set whether to append the voicemail sound file as an attachment to the notification e-mail. Takes an argument of yes or no.

```
append=yes
```

```
append=no
```

The default section takes as a keyword the mailbox number. The keyword takes as parameters the passcode, owner name, and owner e-mail address to send message waiting notification to.

```
1234 => 4321,John Doe,jdoe@misc.com
```



maxmesssage: Sets the maximum length for a voicemail message in seconds. This option can be useful for keeping people from leaving too lengthy of messages.

maxgreet: Sets the maximum length in seconds of the greeting that a user can record for their busy, unavailable, and name messages.

Complete File Example

This is a complete example of a working voicemail.conf file.

```
[general]
format=gsm|wav
serveremail=asterisk@mymachine.com
append=yes
maxgreet=30
maxmessage=90

[default]
1234 => 4321,John Doe,jdoe@mycompany.com
```

DRAFT

Power Line Communication

ILV2010 Head End

Outdoor

Solutions for broadband communication infrastructures using electrical networks

Application

- Intended for 400/230 volts
- Last mile access network

Services

- High-speed Internet access over existing power lines up to 200 Mbps.
- Symetrical bandwidth for better performance
- High performance for PLC infrastructure

Installation

- Meter rooms
- Distribution substations

Package Content

- Head End
- Mounting bracket

Optional Acessories

- Ilevo netconditioning products
- IP67 RJ45 Ethernet cable

Ilevo Head End

- Specifically designed for electrical networks environment
- DS2 200 Mbps Wisconsin PLC technology

Main Function

- Head-End access point for PLC
- DS2 Wisconsin 9002 chipset inside for large PLC deployment

Main Benefits

- Small size, Open PLC European Research Alliance (OPERA) compliant
- Ethernet interface for backbone connection
- Possibility to security seal the product
- Designed for use in any electrical grid conditions
- Intelligent temperature guard, protects against thermal damage.

Requirements

- DS2 Wisconsin PLC network
- Autoconfiguration servers SNMP, RADIUS, FTP, NTP

UNIFIED IP PLATFORM
FOR BOTH MULTIMEDIA & ENERGY APPLICATIONS
OVER EXISTING POWER GRID

a company of Schneider Electric

Ilevo

Specifications

Chipset	
DSS9002	Forwarding table: max 1024 MAC addresses Active PLC connections: 64
Data rate	Up to 200 Mbps
Physical Layer	
Modulation	OFDM with 1536 carriers uplink/ downlink, symmetrical, up to 10 bit per symbol adaptive per carrier.
Transmission Power Step	1 dB
PSD (Power Spectral Density)	-46dBm/Hz @ 10MHz bandwidth -49dBm/Hz @ 20MHz bandwidth -50dBm/Hz @ 30MHz bandwidth
Programmable transmission gain	33dB and 21dB
Programmable reception gain	-12dB down to +30dB, in 6dB steps
Dynamic Range	90 dB min
Protocols Layer 2	
Mac	LV Access for large LAN networks Master-slave mechanism
Dynamic QoS	Configuration using service classifier
Spanning Tree Protocol	IEEE 802.1D
VLAN	IEEE 802.1Q
Traffic Prioritization	IEEE 802.1p
Clock synchronization	NTP
Security	
Authentication	LMAC addresses are optionally authenticated using RADIUS to prevent unauthorized intrusion.
Separation at layer 2	Ilevo devices support VLANs based on the IEEE 802.1Q standard protocol.
Separation at physical layer	The communication between one HE and its IRs relies on specific coding preventing from decoding the signal.
Configuration & Management	
Remote management of all Ilevo equipment is made via standard SNMP management.	
MIB Version	MIB II/ IETF RFC1213, 1493, 2674
SNMP	Supports SNMP v2c
Interoperability with routers and other network devices such as DNS servers, DHCP servers, and boot servers are handled via standard protocols.	

Physical Features	
Weight	Approx 2.2 kg
Dimensions	Approx 190x150x80 mm
Color	Grey
Material	Aluminum
Ports & Connectors	1 coupler interface RJ45 10/100 BASE-T RS485 serial port
Status indicators (LEDs)	Power, Status, PLC Link, PLC Act, Ethernet Link and Ethernet Act.
Electrical Characteristics	
Power Consumption	Max 10W (+8W with optional active accessories)
Voltage	100-240 VAC
Frequency	50/60 Hz
Environmental	
Ingress Protection (IP)	IP54
Acoustic Noise level	Fan less. Less than 25 dB(A)
Operating	
Operating environment	IEC 60721-3-3 standard: - 3K3 (Schneider Standard FT15005 Category C2)
Relative humidity	10% to 100% non-condensing
Ambient operating temperature	-25C° to 45C° -25C° to 55C° in restricted areas according to EN 60950
Storage	
Storage environment	According to ETS 300 019-1-1 Class 1.1
Relative humidity	5% to 95% non-condensing
Temperature	-5°C to +45°C
Transport	
Transport environment	According to ETS 300 019-1-2 Class 2.3
Relative humidity	95% non-condensing
Temperature	-40°C to +70°C, < 30days
CE Approval and labels	
EMC	EN55022 class B EN55024 prEN50412-1 type 1, class 2
Electrical safety	EN 60950-1:2001 IEC 60950-1:2001
Labels	Labeled with product number, MAC address, and serial number

In compliance with its continuous improvement policy, SEPC reserves the right to change those specifications without prior notice

Member of the leading global association for PLC companies

Schneider Electric Powerline Communications (SEPC)

Lagergrens gata 4,
Box 1561
652 26 Karlstad Sweden
Tel: + 46 (0) 54 22 39 00
Fax: + 46 (0) 54 22 39 99

59, chemin du vieux chêne
38240 Meylan France
Tel: +33 (0)4 76 60 51 54
Fax: +33 (0)4 76 60 59 11

Publication: SEPC
Pictures: Schneider Electric

Power Line Communication

Outdoor Intermediate Repeater

- *ILV2110 Time Division*
- *ILV2120 Frequency Division*

Solutions for broadband communication infrastructures using electrical networks

Application

- Local loop repetition point
- Intended for 400/230 volts
- Last mile access network

Services

- Transparent repetition of Head End services
- Time division repetition, ILV2110
- Frequency division repetition, ILV2120

Installation

- Street cabinets
- Meter rooms
- Distribution substations

Package Content

- Repeater
- Mounting bracket

Optional Acessories

- Capacitive Coupling Unit
- Inductive Coupling Unit
- Signal Distribution Box
- Integrated filters for optimal network deployment

Ilevo Intermediate Repeater

- Specifically designed for electrical networks' environment
- Used to extend the range of PLC network
- DS2 200 Mbps Wisconsin PLC technology

Main Function

- Low voltage repeater
- DS2 Wisconsin 9002 chipset inside

Main Benefits

- Small size, Open PLC European Research Alliance (OPERA) compliant
- Ethernet interface for local management
- Low-pass and high-pass filter selection
- Easy installation without power off
- Possibility to security seal the product
- Modular units for TDD and FDD
- Intelligent temperature guard, protects against thermal damage.

Requirements

- DS2 Wisconsin PLC network
- Autoconfiguration servers SNMP, RADIUS, FTP, NTP

UNIFIED IP PLATFORM
FOR BOTH MULTIMEDIA & ENERGY APPLICATIONS
OVER EXISTING POWER GRID

a company of Schneider Electric

Ilevo

Specifications

In compliance with its continuous improvement policy, SEPC reserves the right to change those specifications without prior notice

Chipset	
DSS9002	Forwarding table: max 1024 MAC addresses Active PLC connections: 64
Data rate	Up to 200 Mbps
Physical Layer	
Modulation	OFDM with 1536 carriers uplink/ downlink, symmetrical, up to 10 bit per symbol adaptive per carrier.
Transmission Power Step	1 dB
PSD (Power Spectral Density)	46dBm/Hz @ 10MHz bandwidth 49dBm/Hz @ 20MHz bandwidth 50dBm/Hz @ 30MHz bandwidth
Programmable transmission gain	33dB and 21dB
Programmable reception gain	-12dB down to +30dB, in 6dB steps
Dynamic Range	90 dB min
Protocols Layer 2	
Mac	LV Access for large LAN networks Master-slave mechanism
Dynamic QoS	Configuration using service classifier
Spanning Tree Protocol	IEEE 802.1D
VLAN	IEEE 802.1Q
Traffic Prioritization	IEEE 802.1p
Clock synchronization	NTP
Security	
Authentication	LMAC addresses are optionally authenticated using RADIUS to prevent unauthorized intrusion.
Separation at layer 2	Ilevo devices support VLANs based on the IEEE 802.1Q standard protocol.
Separation at physical layer	The communication between one IR and the master relies on specific coding preventing from decoding the signal.
Configuration & Management	
Remote management of all Ilevo equipment is made via standard SNMP management.	
MIB Version	MIB II/ IETF RFC1213, 1493, 2674
SNMP	Supports SNMP v2c
Interoperability with routers and other network devices such as DNS servers, DHCP servers, and boot servers are handled by standard protocols.	

Physical Features	
Weight	Approx 2.5 kg
Dimensions	Approx 190x150x80 mm
Color	Grey
Material	Aluminum
Ports & Connectors	1 coupler interface (ILV2110) 2 coupler interfaces (ILV2120) RJ45 10/100 BASE-T RS485 serial port
Status indicators (LEDs)	Power, Status, PLC Link, PLC Act
Integrated filter	FIF100. Applicable for frequencies 12/13, 7/7.8, 23.5/24 MHz.
Electrical Characteristics	
Power Consumption	ILV2110 - Max 10W (+8W with optional active accessories) ILV2120 - Max 17W (+15W with optional active accessories)
Voltage	100-240 VAC
Frequency	50/60 Hz
Environmental	
Ingress Protection (IP)	IP54
Acoustic Noise level	Less than 25 dB(A)
Operating	
Operating environment	IEC 60721-3-3 standard: - 3K3 (Schneider Standard FT15005 Category C2)
Relative humidity	10% to 100% non-condensing
Ambient operating temperature	-25C° to 45C° (ILV2110) -25C° to 40C° (ILV2120) -25C° to 55C° in restricted areas according to EN 60950
Storage	
Storage environment	According to ETS 300 019-1-1 Class 1.1
Relative humidity	5% to 95% non-condensing
Temperature	-5°C to +45°C
Transport	
Transport environment	According to ETS 300 019-1-2 Class 2.3
Relative humidity	95% non-condensing
Temperature	-40°C to +70°C, < 30days
CE Approval and labels	
EMC	EN55022 class B EN55024 prEN50412-1 type 1, class 2
Electrical safety	EN 60950-1:2001 IEC 60950-1:2001
Labels	Labeled with Product number, MAC address, and serial number

Member of the leading global association for PLC companies

Schneider Electric Powerline Communications (SEPC)

Lagergrens gata 4,
Box 1561
652 26 Karlstad Sweden
Tel: + 46 (0) 54 22 39 00
Fax: + 46 (0) 54 22 39 99

59, chemin du vieux chêne
38240 Meylan France
Tel: +33 (0)4 76 60 51 54
Fax: +33 (0)4 76 60 59 11

Publication: SEPC
Pictures: Schneider Electric

UPA UNIVERSAL POWERLINE ASSOCIATION

Power Line Communication

ILV220 Data & VoIP CPE Modem

Solutions for broadband communication infrastructures using electrical networks

Ilevo Customer Premises Equipment (CPE)
- End-user modem
- Professional and residential use
- DS2 200 Mbps Wisconsin PLC technology

Application
- Local Loop last mile access point
- LAN networking

Services
- High-speed Internet
- Telephony using embedded Voice-over-IP (VoIP)
- Video services using video streaming over IP
- Voice-Data-Image (VDI) compliant

Package Content
- Data & VoIP Modem
- Power cable
- Phone cable
- Ethernet cable
- User manual - in English*

* *Other language on request*

Installation
- Located on desk top close to user's appliance (computer, phone set, etc.)
- Connected to both power outlet selected by the client and customer computer
- "Plug and play" set up
- Led indicators to show the conditions of both PLC signal from the power line and connected equipment on the end user side.

Main Function
- Ethernet/PLC bridge
- DS2 Wisconsin 9001 chipset inside

Main Benefits
- Small size
- Embedded power supply
- Various colors on request
- Home environment look and feel
- Telco or ISP logo on request

Requirements
- PLC network for access point application
- USB cable and drivers are not recommended but available on request
- Analogue telephone only
- Standard PC and MAC

UNIFIED IP PLATFORM
FOR BOTH MULTIMEDIA & ENERGY APPLICATIONS
OVER EXISTING POWER GRID

a company of Schneider Electric

ilevo

Specifications

Chipset	
DS2 Wisconsin chipset inside	
Data rate	Up to 200 Mbps through the powerline interface
Physical Layer	
Modulation	OFDM with 1536 carriers uplink/ downlink, symmetrical, up to 10 bit per symbol adaptive per carrier.
Transmission Power Step	1 dB
PSD (Power Spectral Density)	≤ - 50 dBm/Hz
Programmable transmission gain	33dB and 21dB
Programmable reception gain	-12dB down to +30dB, in 6dB steps
Dynamic Range	90 dB min
Protocols Layer 2	
MAC	In-Home MAC for small LAN networks. LV Access for large LAN networks Master slave mechanism.
Dynamic QoS	Configuration using service classifier
Spanning Tree Protocol	IEEE 802.1D
VLAN	IEEE 802.1Q, Up to 4094 VLAN_ID Up to 256 active VLANs in LV interface
Traffic Prioritization	IEEE 802.1p
Clock synchronization	NTP
Voice-over-IP	ITU-T H.323 Version 4 compliant H.450, including supplementary services.1, 2, 4, 7, H.245 Version 8, H.245 tunneling, H.225 Version 4, Caller ID through Q.931 messages H245 User Input Indication for out-of-band DTMF signaling G.711 (A-law and u-law), G.723.1, G.726 and G.729A/B
Security Aspects	
Authentication	CPE LMAC addresses are registered in masters to prevent from unauthorized intrusion. Compliant with RADIUS protocol.
Separation at Layer 2	Ilevo devices support VLANs based on the IEEE 802.1Q standard protocol.
Separation at physical layer	The communication between one CPE and the master relies on specific coding preventing other CPE from decoding the signal.

Configuration & Management	
Remote management of all Ilevo modems is made via standard SNMP protocols.	
MIB Version	MIB II/ IETF RFC1213, 1493, 2674
SNMP	Supports SNMP v2c
Provisioning	IP configuration by DHCP FTP client, configuration and upgrade files by TFTP
Interoperability with routers and other network devices such as DNS servers, DHCP servers, and boot servers are handled via standard protocols.	
Physical Features	
Weight	730 grams
Dimensions	200x160x70 mm
Color	Transparant (by default), blue, yellow, red on request.
Material	**Central enclosure**; ABS, F20, GR, Cycolac, GE Flammability class V1 **Side covers**; PMMA, 8N, BK, RÖHM, BEGUSSA Flammability class HB
Ports & Connectors	1 IEC EN60 320-1 1 Ethernet RJ45 port 1 USB 1.0/1.1 1 RJ-11 telephone interface
Status indicators (LEDs)	Power, Data, Power line quality, Link
Electrical Characteristics	
Power Consumption	8 W typical 13 W max
Voltage	85-265V
Frequency	50/60Hz
Environmental	
Ingress Protection (IP)	IP20
Acoustic Noise level	Less than 25dB(A) as ILV220 does not use any fan.
Operating	
Operating environment	According to ETS300019-1-3 Class 3.1
Relative humidity	5% to 85% non-condensing
Ambient operating temperature	0 to +40ºC with 100% performance -5 to +55C° without damage
Storage	
Storage environment	According to ETS300019-1-1 Class 1.1
Relative humidity	5% to 95% non-condensing
Temperature	-5 to +45ºC
Transport	
Transport environment	According to ETS300019-1-2 Class 1.2
Relative humidity	95% non-condensing
Temperature	-40 to +70ºC
CE Approval and labels	
EMC	EN 55022:1994 Class B, EN 55 024:1998
Safety	EN 60950-1:2001
Labels	Modem labeled with PLC MAC address, USB MAC address and serial number.

In compliance with its continuous improvement policy, SEPC reserves the right to change those specifications without prior notice

Member of the leading global association for PLC companies

Schneider Electric Powerline Communications (SEPC)

Lagergrens gata 4,
Box 1561
652 26 Karlstad Sweden
Tel: + 46 (0) 54 22 39 00
Fax: + 46 (0) 54 22 39 99

59, chemin du vieux chêne
38240 Meylan France
Tel: +33 (0)4 76 60 51 54
Fax: +33 (0)4 76 60 59 11

Publication: SEPC
Pictures: SEPC

IMÁGENES CAPTADAS DESDE EL EDIFICIO 1

Fig.1. Centro de Transformación (CT)

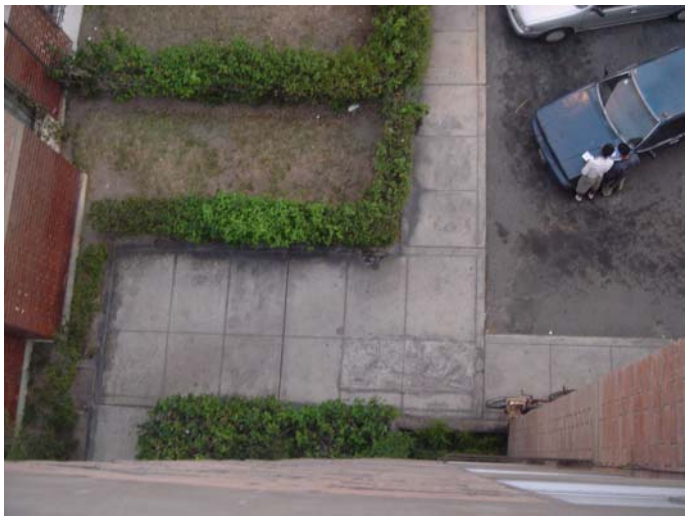


Fig.2. Toma de la Entrada al CT

Fig.3. Toma Abierta de los Alrededores del CT

Fig.4. Sector Aledaño al CT

IMÁGENES CAPTADAS DESDE EL EDIFICIO 2

Fig.5. Toma Centralizada del Sector Residencial

Fig.6. Captación Cercana de la Zona de Vehículos

Fig.7. Extremo Derecho del Recinto

Fig.8. Vigilancia Entrada Secundaria

IMÁGENES CAPTADAS DESDE EL EDIFICIO 3

Fig.9. Imagen de la Entrada Secundaria

Fig.10. Angulo Contrario de la Entrada Secundaria

IMÁGENES CAPTADAS DESDE EL EDIFICIO 5

Fig.11. Imagen de la Entrada Principal

Fig.12. Entrada y Salida de Vehículos y Peatones

IMÁGENES CAPTADAS DESDE EL EDIFICIO 6

Fig.13. Toma Panorámica del Àrea de Interés

Fig.14. Toma Específica de los Vehículos en la Zona

CAPÍTULO 4
ANÁLISIS DE LA TECNOLOGÍA DE RED EMPLEADA

En rigor a las alternativas de solución planteadas en el capítulo anterior; no queda sino demostrar en cierta forma la validez de las tecnologías con las que se piensa trabajar para su desarrollo. Bajo esa premisa se procederá con la presentación de algunas pruebas de laboratorio realizadas en virtud de este trabajo de investigación, considerando la implementación de una pequeña red LAN en la que se ejecuten funciones similares a las de la red originalmente propuesta.

4.1. Condiciones de Simulación

En dichas experiencias se ha considerado el uso de diversas aplicaciones de usuario que se realizan a través de la plataforma de protocolos IP y que usan como medio de transporte la red eléctrica de baja tensión. En cuanto a las aplicaciones, sirve decir que se trata básicamente de soluciones de voz y vídeo sobre IP implementadas con diversos accesorios de comunicación (hardware y software) adecuados a las computadoras, las mismas que trabajan como el eje rector del entorno.

Para efectos de estos procedimientos; se ha ensayado con equipos que se asemejen, en la medida de las posibilidades de equipamiento del laboratorio, a los que se usarían realmente en caso de una implementación. Por ejemplo, para los servicios de voz sobre IP se ha hecho uso de un software de aplicación que simule la labor de un teléfono IP y otro que haga las veces de central telefónica; para los de vídeo se ha empleado una cámara Web y para la interconexión por las redes eléctricas del laboratorio se ha usado un conjunto de 3 módems PLC de primera generación con los que cuenta la Universidad. La figura adjunta muestra el esquema de conexión empleado.

Figura 4.1. Esquema Básico Usado para las Pruebas de Laboratorio

El elemento de red que nos permitirá interactuar con las aplicaciones multimedia es, para efectos de estas pruebas, el módem PLC. Dada su importancia se mostrará brevemente la forma en la que se lleva a cabo su instalación y puesta en marcha para el inicio de las operaciones.

La figura 4.2 muestra el equipo con la tecnología 'Power Line Communications' y sus dos interfases de red. Para la comunicación con la PC cuenta con un puerto Ethernet y la lleva a cabo mediante un cable del tipo UTP categoría 5. Para la transmisión de los datos a través de la red eléctrica lo hace mediante el puerto que usa también para la toma de energía (ver figura 4.3).

Figura 4.2. Módem PLC y sus Interfases de Red Eléctrica y Datos

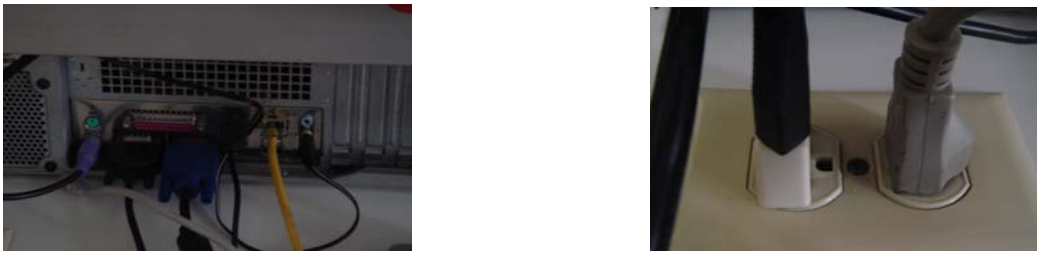


Figura 4.3. Conexiones hacia la Computadora y el Suministro Eléctrico

A nivel de configuración, la detección del módem por parte de la PC es automática luego de que se le asigne a ésta, los parámetros de red adecuados. Es decir, en caso de una configuración en red local, cada una debe tener una dirección IP única agrupadas mediante la identificación de la submáscara adecuada; en nuestro caso bastará con que ésta sea de la clase C (con opción hasta 256 direcciones). Se eligió por tanto la 255.255.255.0, con el rango de direcciones a partir de la 192.168.1.0.

4.2. Pruebas de Voz sobre IP

Con relación a estas pruebas se debe afirmar que éstas, a diferencia de las otras simulaciones, si se han resuelto por medio de una solución muy similar a la que se usará en condiciones reales; dado que las herramientas de software y los equipos de interfase son prácticamente los mismos, la diferencia radica principalmente en la topología de red empleada (punto a punto a través de módems); a diferencia de la configuración punto a multipunto con estructura jerárquica con la que ha sido pensada la verdadera red (uso adicional de módem de cabecera: Head End y un administrador local Home Gateway).

4.2.1. Equipos y Accesorios Requeridos

Para llevar a cabo las experiencias señaladas anteriormente se utilizaron los siguientes equipos y accesorios que se describen en la figura 4.4.

Módem PLC (3)

Computadora Personal (3)

Softphone X – Lite (2)

Auriculares más Micrófono (2)

Tomacorriente 220V – 60 Hz

Cable de Red CAT – 5 (3)

Analizador de Protocolos de Red (2)

Software Libre Central IP (1)

Figura 4.4. Equipos y Accesorios Usados en las Pruebas de VoIP

4.2.2. Desarrollo de las Pruebas

Para llevar a cabo los objetivos trazados se ha considerado el siguiente procedimiento:

Se habilitó tres máquinas del laboratorio, una de las cuales fue configurada como central IP a través del Software libre provisto por Asterisk y que se ejecuta sobre Sistema Operativo Linux. La dirección IP de esta máquina se registró como la 192.168.35.48. Las otras computadoras asumieron el rol de usuarios entre los cuales se establecerá la comunicación, para ello se tuvo por un lado la PC con dirección IP 192.168.35.24 y por otro, su par con dirección 192.168.35.27.

A la computadora con IP 192.168.35.24 se le asignó el anexo 445 y a la 192.168.35.27, el 444. La configuración se realizó en la PC servidor y el modo de iniciación de llamada mediante el software de aplicación usado se ilustra a continuación en las figuras 4.5 y 4.6 respectivamente:

Figura 4.5. Inicio de Sesión

Figura 4.6. Llamada Establecida

Quisimos comprobar, en primer lugar, el modo de funcionamiento de este protocolo (SIP), para lo cual se manejo como herramienta un software analizador de paquetes y tráfico en la red (WireShark). Con ello se verificó que este protocolo trabaja bajo dos procedimientos: SIP para establecer la comunicación (parámetros de señalización) y RTP para hacer efectivo el intercambio de información luego de que se habilitó la llamada.

```
192.168.35.24 192.168.35.48  SIP/SDP Request: INVITE sip:445@192.168.35.48, with session description
192.168.35.48 192.168.35.24  SIP     Status: 407 Proxy Authentication Required
192.168.35.24 192.168.35.48  SIP     Request: ACK sip:445@192.168.35.48
192.168.35.24 192.168.35.48  SIP/SDP Request: INVITE sip:445@192.168.35.48, with session description
192.168.35.48 192.168.35.24  SIP     Status: 100 Trying
192.168.35.48 192.168.35.24  SIP     Status: 180 Ringing
192.168.35.48 192.168.35.24  SIP/SDP Status: 200 OK, with session description
```

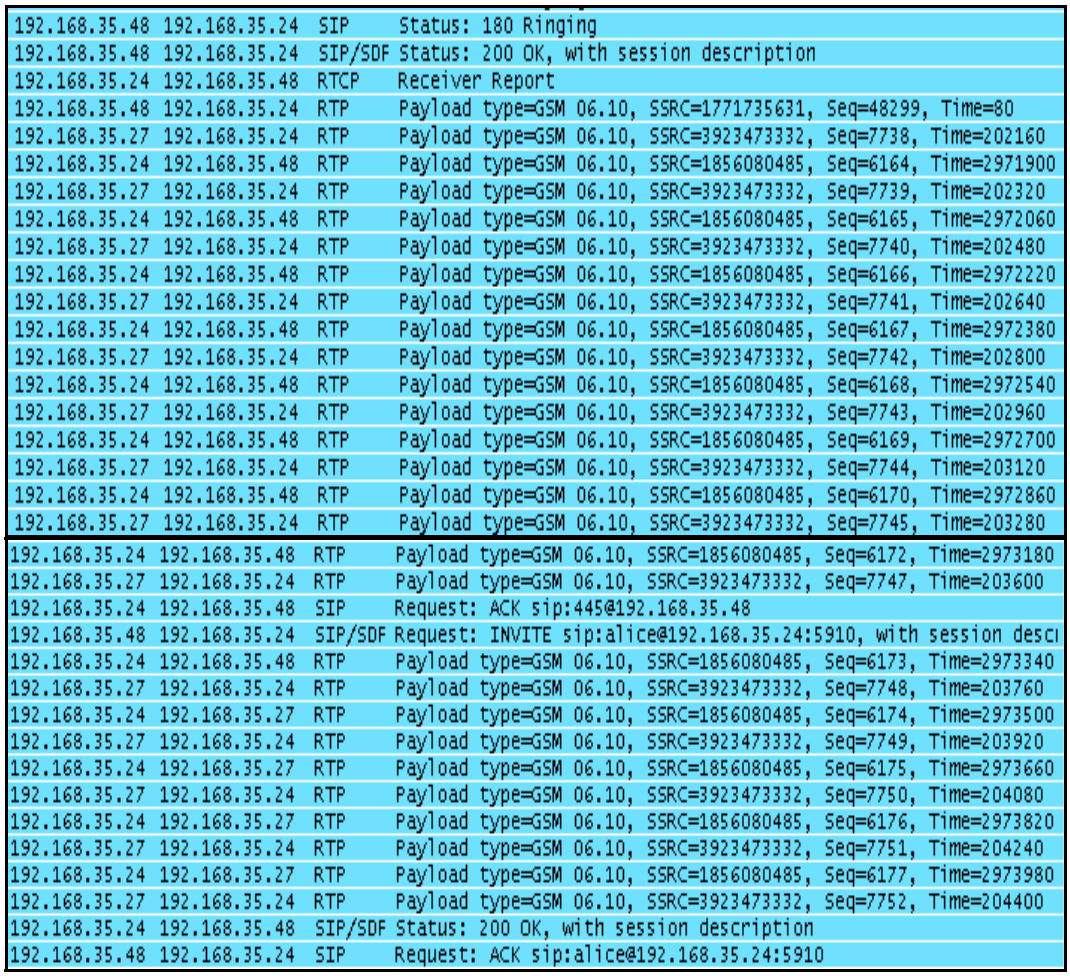
Figura 4.7. Captura de Paquetes de Inicialización

La figura 4.7 muestra el intercambio de información entre las máquinas con extensión '.24' y '.48' las cuales se encuentran negociando el establecimiento de la comunicación. Posteriormente se envían unos paquetes de confirmación como se muestra en la figura 4.8:

```
192.168.35.24 192.168.35.48  RTCP    Receiver Report
192.168.35.48 192.168.35.24  RTP     Payload type=GSM 06.10, SSRC=1771735631, Seq=48299, Time=80
```

Figura 4.8. Captura de Paquetes de Confirmación

Finalmente se establece la comunicación por RTP entre las 2 máquinas en donde la central hace de intermediaria, como se aprecia a continuación e la figura 4.9 :



192.168.35.48	192.168.35.24	SIP	Status: 180 Ringing
192.168.35.48	192.168.35.24	SIP/SDP	Status: 200 OK, with session description
192.168.35.24	192.168.35.48	RTCP	Receiver Report
192.168.35.48	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=1771735631, Seq=48299, Time=80
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7738, Time=202160
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6164, Time=2971900
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7739, Time=202320
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6165, Time=2972060
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7740, Time=202480
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6166, Time=2972220
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7741, Time=202640
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6167, Time=2972380
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7742, Time=202800
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6168, Time=2972540
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7743, Time=202960
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6169, Time=2972700
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7744, Time=203120
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6170, Time=2972860
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7745, Time=203280
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6172, Time=2973180
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7747, Time=203600
192.168.35.24	192.168.35.48	SIP	Request: ACK sip:445@192.168.35.48
192.168.35.48	192.168.35.24	SIP/SDP	Request: INVITE sip:alice@192.168.35.24:5910, with session desci
192.168.35.24	192.168.35.48	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6173, Time=2973340
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7748, Time=203760
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6174, Time=2973500
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7749, Time=203920
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6175, Time=2973660
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7750, Time=204080
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6176, Time=2973820
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7751, Time=204240
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6177, Time=2973980
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7752, Time=204400
192.168.35.24	192.168.35.48	SIP/SDP	Status: 200 OK, with session description
192.168.35.48	192.168.35.24	SIP	Request: ACK sip:alice@192.168.35.24:5910

Figura 4.9. Captura de Paquetes de Negociación

Después de ese procedimiento ambos usuarios pueden comenzar una comunicación directamente (véase la figura 4.10). El estándar de compresión usado es el GSM que es una variante del que se emplea para la comunicación celular, está regulado por la ETSI y maneja anchos de banda de alrededor de 13 Kbps. Los protocolos de compresión, sin embargo, son múltiples y configurables, todo dependerá de los dos principales parámetros que hay que tener en cuenta para la comunicación de voz: calidad en la comunicación o consumo de ancho de banda.

192.168.35.24	192.168.35.48	SIP/SDP	Status: 200 OK, with session description
192.168.35.48	192.168.35.24	SIP	Request: ACK sip:alice@192.168.35.24:5910
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6178, Time=2974140
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7753, Time=204560
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6179, Time=2974300
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7754, Time=204720
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6180, Time=2974460
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7755, Time=204880
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6181, Time=2974620
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7756, Time=205040
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6182, Time=2974780
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7757, Time=205200
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6183, Time=2974940
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7758, Time=205360
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6184, Time=2975100
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7759, Time=205520
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6185, Time=2975260
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7760, Time=205680
192.168.35.24	192.168.35.27	RTP	Payload type=GSM 06.10, SSRC=1856080485, Seq=6186, Time=2975420
192.168.35.27	192.168.35.24	RTP	Payload type=GSM 06.10, SSRC=3923473332, Seq=7761, Time=205840

Figura 4.10. Establecimiento de la Comunicación

4.2.3. Resultados

En la gráfica que se analizará en breve (figura 4.11) se puede apreciar también el modo con el que opera el protocolo SIP; es decir, se muestra en un inicio dos pequeños picos que indican la transferencia de datos debido al inicio de sesión y luego de ello un consumo constante de 0.05 % de 100 Mbps durante la conversación (aproximadamente 50 Kbps).

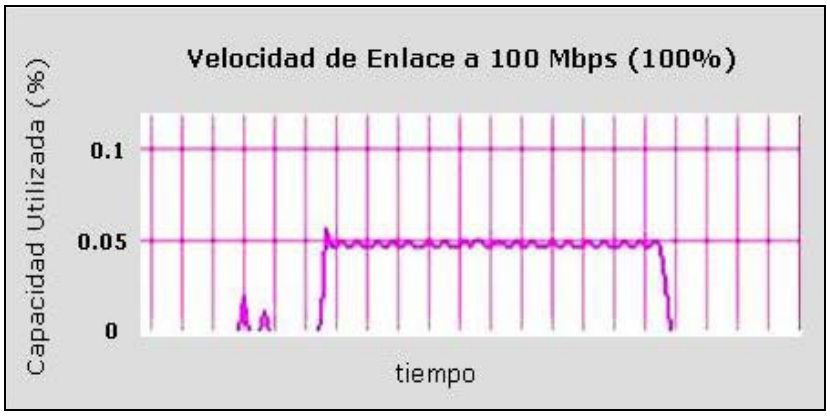


Figura 4.11. Inicio y Establecimiento de la Llamada

La conversación se realizó por un breve intervalo de tiempo que también fue capturado por el software de monitoreo de tráfico, cuando se termina la llamada se nota una caída prominente de la gráfica. Ver figura 4.12.

Figura 4.12. Captación del Intervalo de Conversación

4.3. Pruebas de Vídeo IP

Para simular las condiciones reales se manejó el mismo esquema que el planteado en el diseño; es decir, una computadora (192.168.35.24) se encargó de generar la información audiovisual a partir de una cámara Web y un software de aplicación cliente/ servidor (NetMeeting). La segunda computadora (1962.168.35.27) recibía la información de vídeo a través de una conexión punto a punto sobre la red eléctrica y estuvo habilitada para intercambiar cualquier otro tipo de información. Aunque no se mencionó anteriormente, es importante señalar que las condiciones de las pruebas se hicieron bajo ciertas exigencias de interferencia y ruido, ya que se encendieron las lámparas fluorescentes y los ventiladores del laboratorio durante el periodo en que se realizaron las mismas (ver figura 4.13).

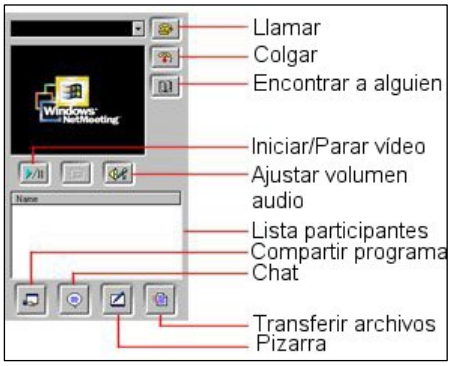
Figura 4.13. Laboratorio de Software para Telecomunicaciones

4.3.1. Equipos Requeridos

Módem PLC (2)

Computadora Personal (2)

Cámara Web (1)



Software NetMeeting (2)

Tomacorriente 220V – 60 Hz

Cable de Red CAT – 5 (2)

Analizador de Protocolos de Red (2)

Figura 4.14. Equipos y Accesorios Usados en las Pruebas de Vídeo IP

4.3.2. Desarrollo de Pruebas y Resultados

NetMeeting es una herramienta de Microsoft Windows con la que se pueden llevar a cabo diversas aplicaciones múltiples de voz, vídeo y transferencia de datos. En nuestro caso se usó, básicamente, para lo relacionado a vídeo y voz, este último para comparar características de conversación con relación a lo llevado a cabo en la experiencia anterior. La solicitud de comunicación se realiza por medio de la dirección IP de la máquina destino (figura 4.15) y no es, sino hasta cuando ésta acepta la llamada, que se puede proceder con la comunicación (ver figura 4.16).

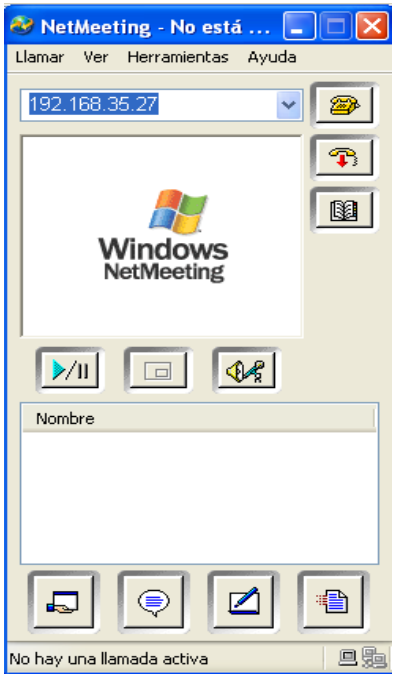


Figura 4.15. Solicitud de Llamada mediante su Dirección IP

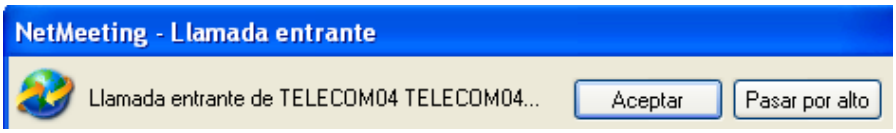


Figura 4.16. Aviso de Llamada Entrante

a) NetMeeting para Aplicaciones de Voz

En este procedimiento se estableció una llamada y se capturó el consumo de ancho de banda durante su duración. De acuerdo a los resultados obtenidos se aprecia con claridad de que este software propietario de Microsoft exige menor ancho de banda de

la red y según ello se aprecia que éste representa casi la mitad de lo que consume la aplicación de voz con X - Lite.

Tal como se aprecia en la figura 4.17, se obtienen valores promedio que indican el 0.02 % del total de 100 Mbps, lo que representa consumos de alrededor de 20 Kbps.

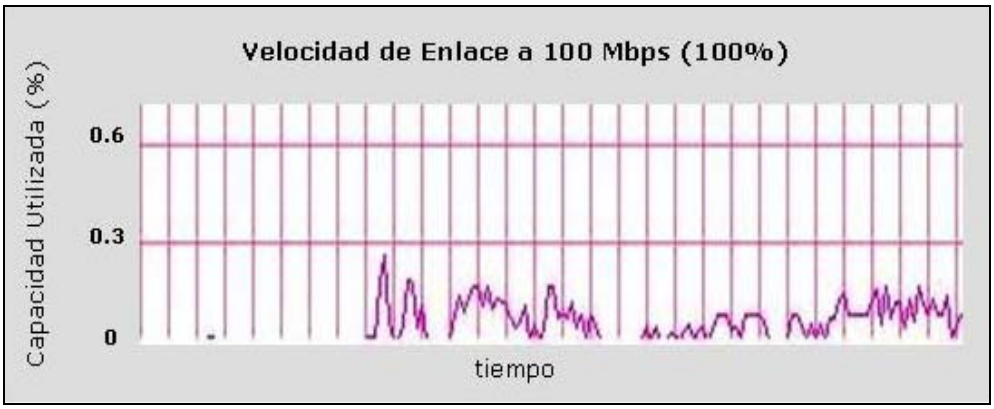


Figura 4.17. Consumo de Ancho de Banda para Aplicaciones de Voz

b) NetMeeting para Aplicaciones de Vídeo

Luego de establecida la comunicación entre las dos computadoras se puede hacer una solicitud de uso de vídeo en la sesión, para lo cual la interfase de NetMeeting se muestra como sigue en la siguiente figura:

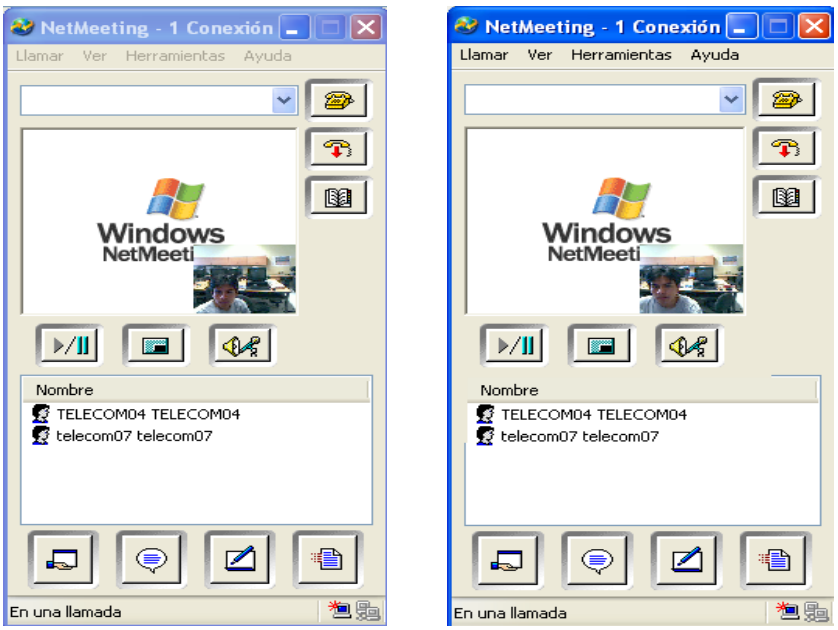


Figura 4.18. Consumo de Ancho de Banda para Aplicaciones de Vídeo

Cuando se verifica el consumo de ancho de banda se observa valores de 0.25 % del total (equivale a 250 Kbps). Luego se probó con captura de imágenes sin movimiento (imagen estática) y se verificó que los 'códecs' de compresión de vídeo disminuyeron la transferencia, lo que se evidencia en los dos picos caídos de la figura 4.19.

Figura 4.19. Comparación entre el Consumo de Voz y el de Vídeo

c) NetMeeting para Aplicaciones de Vídeo más VoIP con X - Lite

Durante este procedimiento se activó las dos aplicaciones; es decir, se habilitó una llamada con el Softphone X – Lite y se mantuvo la transmisión de vídeo con NetMeeting. Al hacerlo, se consideró primero la transmisión de conversación junto con la de vídeo y los resultados mostraron consumos del orden del 0.46 % del total; finalmente con la transmisión de 'silencios' la tasa cae hasta 0.35 %. Véase las figuras 4.20 y 4.21.

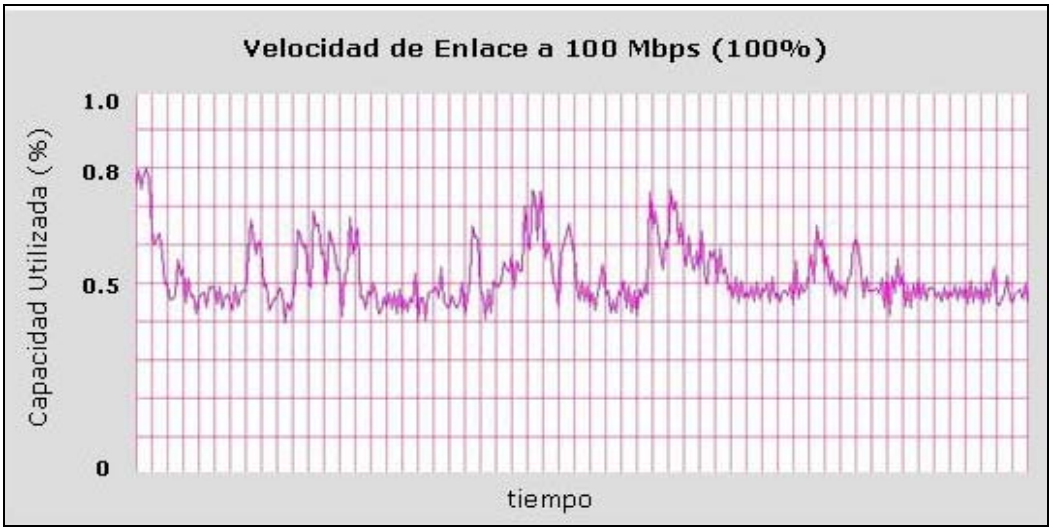


Figura 4.20. Consumo entre Aplicaciones de Voz y Vídeo

Figura 4.21. Periodo de Tiempo de Transmisión de Vídeo y 'Silencios'

d) NetMeeting para Aplicaciones de Vídeo con Ampliación de Imagen

Se configuró el programa para que la imagen captada sea mucho mayor a la que se estuvo transmitiendo en la experiencia anterior. Los resultados se muestran en la figura adjunta:

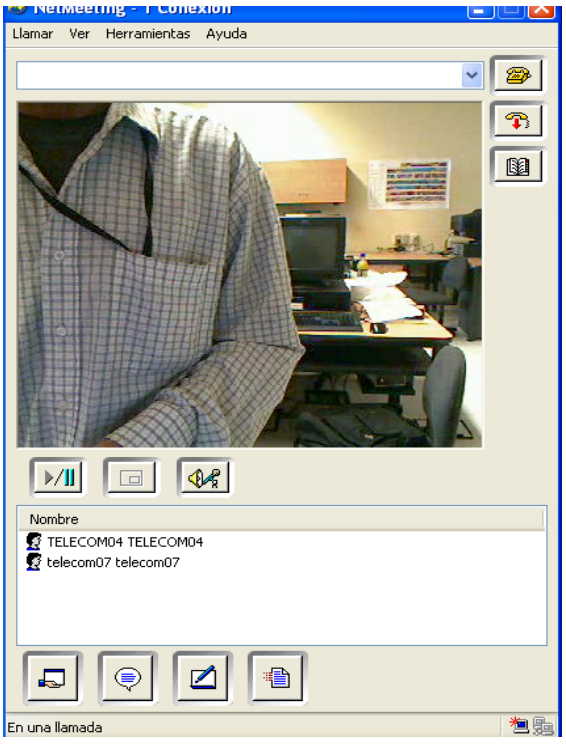


Figura 4.22. Transmisión de Vídeo IP con Imágenes de Mayor Tamaño

Se observa que la imagen mantiene una excelente resolución y que la secuencia es sumamente fluida y con una muy buena calidad.

Con relación al consumo de ancho de banda se puede apreciar que éste, como es lógico, se ha incrementado hasta un porcentaje representativo de 0.55, lo que representa un valor cercano a 550 Kbps respecto a los 250 del consumo de la secuencia de vídeo anterior. Esto último se aprecia claramente en la figura siguiente.

Figura 4.23. Consumo de Ancho de Banda (Mayor Tamaño de Imagen)

Por último se procedió a capturar las diferencias en el consumo de ancho de banda para las diversas aplicaciones en una sola gráfica. Al inicio se considera sólo la transmisión de vídeo con NetMeeting, luego de un tiempo se adhiere el servicio de VoIP con X – Lite, posteriormente se deja trabajando sólo a éste último y finalmente se termina de cerrar ambas aplicaciones, en donde el tráfico cae completamente (ver figura 4.24).

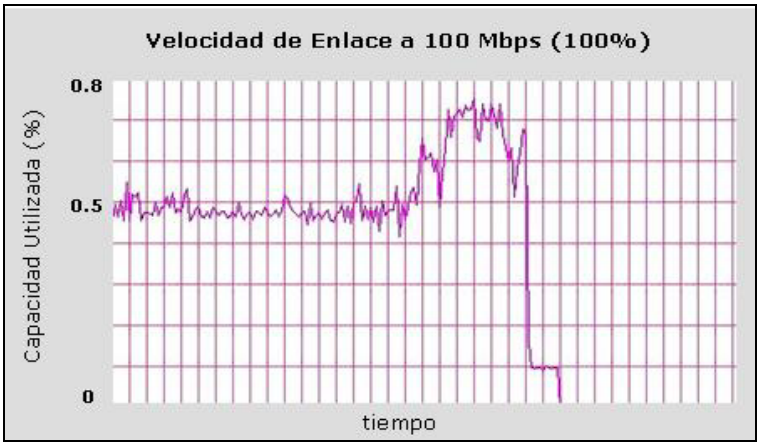


Figura 4.24. Variación Continua de Aplicaciones Multimedia


2
G3

Corinex

AV200 Powerline Ethernet Wall Mount

Corinex

Manual del usuario

Declaración de Conformidad

CE

Modelo: **Corinex AV200 Powerline Ethernet Wall Mount**

Fabricante: Corinex Communications Corp.
#670-789 West Pender Street
Vancouver, B.C.
Canada V6C 1H2

Directivas declaradas conformes:

EMC: 89/336/EEC
LVD: 73/23/EEC
R&TTE: 1999/5/EEC

Conformidad con estándares declarados:

EN 55022
EN 55024
EN 60950
EN 61000-3-2
EN 61000-3-3

Los firmantes declaran solemnemente que el equipo especificado en este documento es conforme con las directivas y estándares mencionados.

Nombre Impreso / Posición **Peter Sobotka / CEO** Lugar / Fecha **Vancouver / Marzo.21.2006**

Firma 

Este documento, así como el software descrito en él, se otorgan bajo licencia para su uso o reproducción únicamente de conformidad con los términos establecidos en dicha licencia. El contenido de este documento es solamente para uso interno y está sujeto a cambios sin previo aviso, sin que ello represente un compromiso por parte de Corinex Communications Corp.

Corinex Communication Corp no asume responsabilidad u obligación alguna por cualquier error o incongruencia que pudiese aparecer dentro del presente documento.

Es nuestra política mejorar nuestros productos en tanto la nueva tecnología, los componentes de hardware, software y firmware se encuentren disponibles, por lo tanto, la información contenida dentro del presente documento está sujeta a cambio sin previo aviso..

Algunas características, funciones u operaciones descritas en este documento pudiesen no estar incluidas o disponibles en ciertos países debido a regulaciones gubernamentales o políticas de mercado.
Así mismo, el uso de este producto y/o las características del mismo pueden estar restringidas o reguladas por las leyes de ciertos países. Si Usted no está seguro de que restricciones o regulaciones aplican para dicho producto, deberá consultar con la oficina regional de Corinex o con su distribuidor autorizado.

Publicado por:
Corinex Communications Corp.
#670-789 West Pender Street
Vancouver, B.C.
Canada V6C 1H2
Tel.: +1 604 692 0520
Fax: +1 604 694 0061

Corinex es una marca registrada de Corinex Communications Corp.
Microsoft, MS-DOS, MAC OS, MS, Windows son marcas registradas propiedad de Microsoft Corporation en EE.UU., y/u otros países.
Todos los productos y nombres de las compañías mencionados en este documento, son propiedad de sus respectivos dueños.

Derechos reservados 2001-2006 Corinex Communications Corp.

Nota: Este dispositivo ha sido probado y como resultado se encontró que cumple con los limites establecidos para la Clase B de la Tecnología Informática. Estos límites se encuentran diseñados para proveer una protección razonable contra interferencia que pudiese resultar dañina dentro de una instalación doméstica. El dispositivo genera, utiliza y puede irradiar energía de radio frecuencia, por tal razón si no es instalado y utilizado de acuerdo a las instrucciones de uso, éste puede provocar interferencia dañina en las radio comunicaciones. Sin embargo, no existe garantía alguna de que dicha interferencia no ocurra en alguna instalación en particular. Por ello, si el dispositivo causa interferencia que resulte dañina, se recomienda al usuario tomar las medidas adecuadas al respecto.

2006-04-26 ver. 2

CORINEX COMMUNICATIONS CORPORATION

Este es un contrato legal entre el usuario del producto (Usted), y CORINEX COMMUNICATIONS CORPORATION ("CORINEX") referente a los derechos reservados del Software incluido con este contrato.

El uso de cualquier Software y documentación relacionada con este Software, dado con el producto Corinex, o por otros medios de transferencia electrónica disponibles por Corinex, constituyen de por si mismos sí la prueba de aceptación de los términos del mismo, Y si el usuario, esta en desacuerdo con las condiciones de este Contrato, no archive electrónicamente, instale, copie o use el Software.

1. Licencias. CORINEX da al usuario derechos personales de uso exclusivo, por lo cual el usuario no puede transferir o poseer derechos sobre el Software incluido con este contrato. El usuario, acepta no copiar el Software, con excepción de que sea para el fin de instalarlo en una sola maquina, El usuario, acepta no hacer copias del material escrito incluido en el Software. Tampoco, modificara, traducirá, alquilará, copiara, o asignara transferencia de derechos parte o de todo de este Software, y tampoco podrá dar derechos de este software a otra persona. Las etiquetas y los logos en este Software son propiedad de reservada de Corinex. Además, el usuario acepta no fabricar otros productos derivados de este Software. El usuario puede transferir los derechos de este Software siempre y cuando este no guarde ninguna copia del Software, y si el software es una versión mas nueva, usuario no puede tener la copia más antigua.

2. Derechos Reservados. Este Software es dado bajo licencia y no es vendido, el usuario reconoce que no posee titulo sobre la propiedad intelectual de este Software. También acepta los derechos de propiedad exclusivos de Corinex Communications Corporation y/o sus proveedores, y el usuario no poseerá ningún derecho al Software, excepto por las condiciones mencionadas anteriormente. Todo los Softwares distribuidos tienen el mismo contrato.

3. Ingeniería. UD., el usuario, Y si es una empresa, el usuario sus empleados y asociados, acepta que no tratará de modificar, cambiar, traducir, o tomar parte del Software para producir otro producto. La falta a cualquier cláusula en las condiciones mencionadas anteriormente resultará en la automática terminación de la licencia, dada por Corinex.

4. Nota de Garantía. El Software es proveído sin ningún tipo de garantía. Corinex y sus proveedores no garantiza o se hace responsable de las aplicaciones especificas en la que el Software es utilizado. Y también no se hace responsable de la asociación y funcionalidad con otros productos. Corinex y sus proveedores tampoco se hace responsable de los errores del Software que pueda comprometer la integridad de su sistema.

5. Limitaciones de Responsabilidad. Corinex solamente garantiza o, tiene responsabilidad sobre daños por costos no excedentes al valor pagado por el Software. En cualquier situación, si existiera alguno, por consecuencia, del Software en manera directa o indirecta, Corinex y sus proveedores no se hacen responsables, incluso en situaciones en la cuales Corinex y sus distribuidores han sido notificados de este problema.

6. Leyes Aplicables. Este contrato esta administrado y gobernado por las leyes del país de Canadá, excluyendo provisiones de leyes de conflicto.

7. Leyes de Exportación. Este contrato se refiere a productos y/o datos técnicos pueden ser cubiertos bajo leyes y regulaciones de controles de exportación, por lo tanto esta sujeto a dichas leyes y regulaciones.

8. Precedente. Diferente a las excepciones explicadas anteriormente, las condiciones mencionas son aplicables y permanentes como condición de uso del Software. Estas condiciones pueden ser más detalladas en caso de cualquier cláusula aparezca inconsistentes.

Índice

1 Introducción

1.1 Descripción general

El *Corinex AV200 Powerline Wall Mount* es una interfase de red capaz de usar cableado eléctrico existente, como medio de comunicación. Después de una instalación exitosa el AV200 Powerline puede ser usado como una LAN tradicional con velocidad de transmisión hasta de 200 Mbps

La ventaja de nuestro producto son sus bajos costos de mantenimiento sin necesidad de cableado extra u otros componentes electrónicos externos.

El *Corinex AV200 Powerline Wall Mount*:

- Permite a usuarios conectar PC u otros dispositivos a Ethernet, a redes locales a través del cableado eléctrico existente.
- Permite compartir archivos y aplicaciones
- Permite compartir periféricos a través de una red
- Permite compartir accesos de conexión a banda ancha
- Permite compartir banda ancha para transmisión de multimedia.
- Elimina la acumulación de cables en su casa u oficina.
- Es una solución rentable costo/beneficio para comunicaciones de alta velocidad en su casa u oficina

1.2 Acerca de este manual

Este manual incluye todo lo necesario para el uso e instalación de su *Corinex AV200 Powerline Wall Mount*, con esta información usted podrá:

- Analizar la eficiencia de su red
- Planear la configuración *Corinex AV200 Powerline Wall Mount*
- Instalar y configurar su *Corinex AV200 Powerline Wall Mount*
- Verificar y optimizar el funcionamiento de su *Corinex AV200 Powerline Wall Mount*

2 Guía de Instalación

2.1 Contenido del paquete

Cuando abra la caja de su *Corinex AV200 Powerline Wall Mount*, revise que contenga:

- *Corinex AV200 Powerline Wall Mount*
- Cable directo a Ethernet
- Guía rápida de instalación
- CD con documentación

Nosotros estamos constantemente innovando nuestros productos. Para descargar las últimas versiones de hardware/software e información adicional por favor visite la Web **www.corinex.com**.

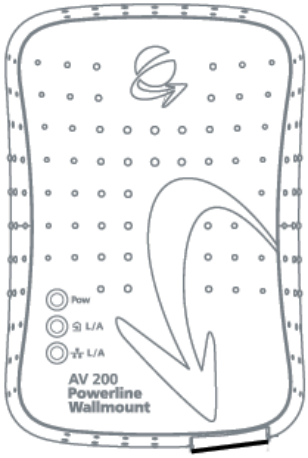
También lo invitamos a que visite la página Web del programa socios autorizados Powerline Corinex (**http://cappp.corinex.com/**), donde encontrará valiosa información sobre aplicaciones e instalaciones complejas, así como socios que le pueden proveer servios en el área que necesite.

2.2 Requerimientos del sistema

- Compatible con el PC de IBM o con Macintosh
- Un puerto Ethernet disponible con 10/100 Mbps
- Windows 98/ME/2000/NT/XP, Mac OS X o sistema operativo Linux
- Javascript compatible con el navegador de Internet (Netscape, Internet Explorer, Opera…)

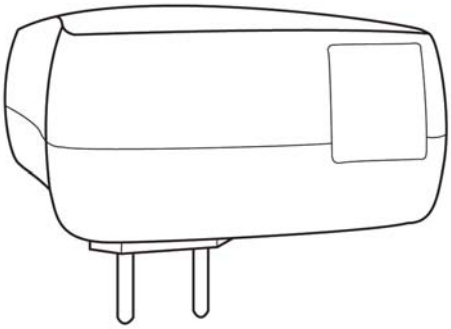
2.3 Descripción Física

Definiciones de la señal de luz LED
(LEDs de izquierda a derecha)



1. Encendido	Verde	On: Encendido Off: Apagado
2. PLC	Verde	On: Powerline activity Off : No hay actividad Powerline Intermitente: Recibiendo/Transmitiendo datos
3. ETHERNET	Verde	On: Enlace a LAN Off: No hay enlace a LAN Intermitente: Recibiendo/Transmitiendo datos

Definiciones de los conectores



1. LAN: Puerto Ethernet 1x RJ-45 LAN10/100

2.4 Especificaciones Técnicas

Estándar	IEEE 802.3u
Velocidad	200 Mbps en nivel físico
AC Enchufe de corriente	USA, EU , UK y Australia
LED Señal de luz	Power, Enlace/Actividad PLC, Enlace Ethernet
Interfase	10/100BaseT Fast Ethernet, Powerline
Rango de alcance	2 – 34 MHz
Entrada de poder	85 a 265 V AC, 50/60 Hz
Dimensiones	148 mm L x 106 mm W x 47 mm H
Densidad espectral de la energía transmitida	-56 dBm/Hz
Consumo de energía	5W
Seguridad y EMI	UL/EN 60950, FCC Part 15, limites EN 55022 EMC

2.5 Instalando el AV200 Powerline Wall Mount

Para conectar el *Corinex AV200 Powerline Wall Mount* a su ordenador siga los pasos descritos a continuación.

1. Conécte un extremo del cable Ethernet al puerto LAN del adaptador y el otro extremo al puerto Ethernet de su ordenador.
2. Conécte el *Corinex AV200 Powerline Wall Mount* directamente al enchufe eléctrico AC, nunca a una extensión eléctrica.

NOTA: Por favor use un cable directo a Ethernet para conectar el adaptador AV200 Powerline a su ordenador. Si está conectando el adaptador AV200 Powerline a un MODEM o un interruptor por favor utilice un cable cruzado.

2.6 Prueba básica de la configuración TCP/IP y la red AV200

Para verificar que su equipo está conectado y funciona correctamente, use la herramienta **Ping**. En Windows, presione en menú **Inicio** -> **Ejecutar**, luego escriba el comando **ping IPADDRESS -t**, donde IPADDRESS (es la dirección IP de su ordenador a la cual se conecta el AV Powerline Adapter) por ejemplo. **ping 192.168.4.1 -t** (el proceso se puede interrumpir presionando **CTRL+C**).

1. Use la herramienta **Ping** para verificar la dirección IP del computado al cual esta conectado el AV200 Powerline Adapter. Si esto falla, debe existir un problema con la tarjeta de red Ethernet o con el protocolo TCP/IP.
2. Repita el proceso en otros computadores de su red AV200 Powerline.
3. Si los computadores hacen el Ping automáticamente, trate de usar la herramienta Ping con otro computador de su red AV200 Powerline. Si esto falla, debe existir un problema con la conexión en su red AV200 Powerline o con la configuración del adaptador AV. Revise la conexión el enchufe, o conéctelo en uno diferente. Verifique la configuración de su adaptador, especialmente su número de red, para más información por favor diríjase al capitulo 3 para detalles de configuración.

Si tiene problemas con la instalación, trate de desconectar su AV200 Powerline Adapter y reinicie su ordenador, algunas veces esto resuelve el problema. Si el problema persiste, por favor diríjase a la guía de solución de problemas que encontrará dentro de este manual.

3 Configuración Web

Para poder acceder a la página de configuración Web, es necesario conocer la dirección Web del adaptador y estar conectado a ella (a través de un cable de Ethernet). Los adaptadores que no hayan sido configurados poseen la dirección IP **10.10.1.69**. Abra un navegador de Internet (Microsoft Internet Explorer v6.0, Mozilla v1.7.2 y Mozilla Firefox v1.0 han sido modificados para su uso con estos productos.), y escriba la dirección IP en la barra de direcciones – el URL debe ser **http://10.10.1.69/** a menos que lo haya cambiado anteriormente por uno diferente.

Se requiere cambiar la dirección IP que viene por defecto, **10.10.1.69**, para permitir acceso a un adaptador, cuando una o más unidades están activas en la misma red. La dirección IP es la identificación única de un dispositivo en la red, así que los adaptadores no se podrán identificar en la red si poseen la misma dirección.

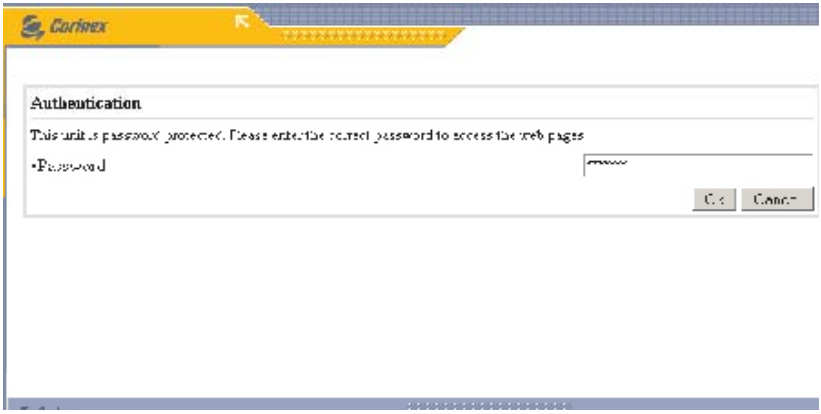
Siga los pasos descritos a continuación para configurar una dirección IP en cada computador.

1. En los ajustes de red de su ordenador, digite una dirección con un rango de 10.10.X.X y un valor Netmask 255.255.0.0. Esto es necesario para la compatibilidad con los ajustes por defecto del adaptador. Para más detalles acerca de cómo ajustar una dirección IP en su ordenador por favor lea el capitulo 5.
2. Enchufe su AV200 Powerline Adapter y conéctelo a su PC a través del cable de Ethernet.
3. Abra su navegador Web y digite el siguiente URL: **http://10.10.1.69**. Así llegara a la configuración de su AV200 Powerline Adapter.

3.1 Página de Autentificación

Si la contraseña de configuración está habilitada, usted necesitará registrarse antes de acceder a la página de configuración Web para efectuar modificaciones en la red. Por ello, será dirigido primeramente a una página de autentificación, donde necesitará ingresar su contraseña. El servidor tiene un receso de autentificación de 5 minutos, por ejemplo si una página de Internet no se ha descargado en 5 minutos la autentificación expirará y usted necesitará registrarse nuevamente.

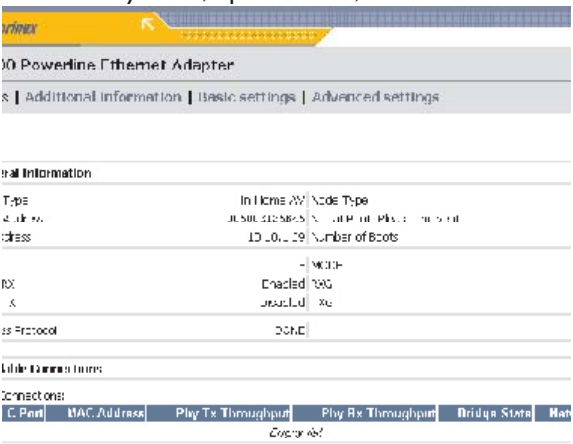
NOTA: La contraseña por default "**paterna**".



NOTA: Si la protección de la contraseña se encuentra deshabilitada, usted será dirigido directamente a la página principal en lugar de ser dirigido a la página de Autentificación.

3.2 Página Principal

Ésta es la primera página que usted verá después de registrarse, o simplemente la primera si la contraseña de configuración está deshabilitada. Muestra el estatus de la información correspondiente al adaptador, una lista de conexiones Powerline disponibles, direcciones IP y MAC, tipo de MAC, etc.



En la parte superior se encuentran las categorias principales „**Status**," „**Additional Information**," „**Basic Settings**" y „**Advanced Settings**". El menú muestra su posición actual en la interfase Web. (La categoria es de un color diferente y no tiene la opción para hacer click)

3.3 Página de Información Adicional

Ésta página muestra información detallada acerca de los ajustes del módem

Información del Sistema	
Uptime	Muestra el tiempo en que el módem ha estado funcionando desde el último reinicio .
Firmware Version	Muestra la versión detallada del Firmware.

Estatus del MAC	
MAC Address	Muestra la única dirección MAC del módem AV200 Powerline .
MAC Type	Tipo de MAC – en Spirit es Inhome AV.
Node Type	Muestra el tipo de nodo – este puede ser **EP** (Slave), **AP** (Master) o **Static AP** (Static Master).
Network Identifier	Muestra la secuencia del identificador de red. Solamente los dispositivos con el mismo identificador de red pueden comunicarse entre sí.
Encryption Key	Muestra si la encriptación de datos se encuentra o no habilitada .

Estatus de la Red	
IP Configuration	Muestra „**Fixed**“ para la configuración de un IP estático o „**DHCP**“ si el dispositivo está configurado como un DHCP client.
IP Address	Muestra la dirección actual IP del módem.
Subnet Mask	Muestra la máscara de subred.
Default Gateway IP Address	Muestra el Gateway por default.

Estatus del PHY	
Notches	Indica si las muescas de frecuencia están permitidas o no. En la Unión Europea, las muescas deben ser permitidas siempre, para poder eliminar la interferencia con las bandas del Radio Amateur especificadas por la IARU (International Amateur Radio Union).
Power Control	Indica el estatus del mecanismo del control de la energía (descrito en la sección 3.4.4).

Estatus Multicast	
IGMP Aware Multicast Syndication	Muestra el estatus del soporte para protocolos IGMP (descrito en la sección 3.4.5).
Multicast Bindings	Muestra todos los bindings multicast entre direcciones IP y direcciones MAC de AV200 Powerline.

Estatus de la VLAN	
VLAN Configuration	Indica si la Red Virtual de Área Local (VLAN) está permitida o no.
VLAN Tag	Muestra la etiqueta VLAN seleccionada. Todo el tráfico del puerto Ethernet se marca con esta etiqueta.
VLAN Priority	Muestra la prioridad seleccionada, la cual es insertada en la etiqueta VLAN.

Estatus de Prioridad	
Default Priority	Muestra la prioridad por default para la transmisión de tráfico.
Criterion 1 & 2	Muestra qué criterio es utilizado para la clasificación del tráfico. Éste puede ser TOS, 802.1p o personalizado. Si elige personalizarlo, los parámetros completos del criterio se muestran. a continuación. Vea el capítulo 3.4.7 para mayor información.

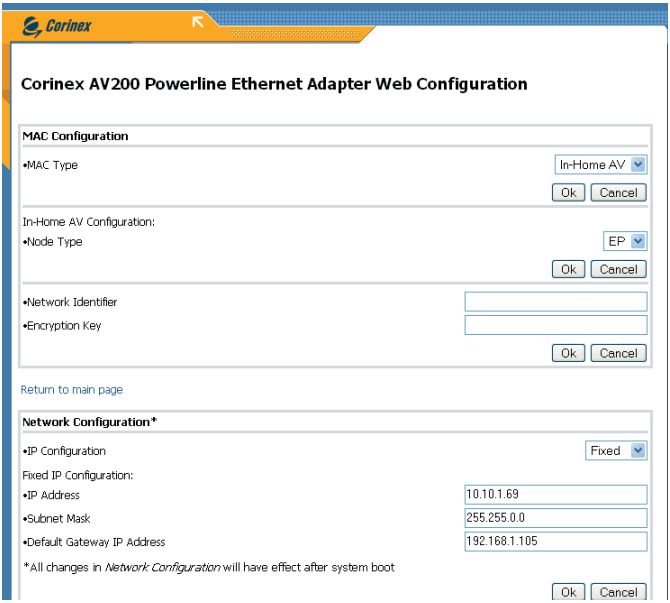
Estatus del sistema de seguridad	
Status	Indica si la interfase WEB se encuentra protegida con alguna contraseña o no.

3.4 Página para cambio de Configuración

3.4.1 Descripción General

La página de configuración le permite efectuar cambios en los ajustes del adaptador. Cualquier parámetro que cambie será almacenado inmediatamente en la memoria permanente del adaptador, así mismo será cargado y configurado automáticamente después de reiniciar el sistema. Cualquier cambio tomará efecto inmediatamente después de reiniciar el sistema, a excepción de los ajustes de configuración de red (éstos requieren que se restaure el adaptador)

La configuración está dividida en dos secciones: „**Basic settings**“ (Ajustes básicos) y „**Advanced settings**“ (Ajustes avanzados).



Notas :

- Se debe configurar un IP distinto para cada adaptador dentro de una misma red. El IP del adaptador no necesita estar en el mismo rango de dirección que su PC o de los dispositivos con los que se está comunicando, únicamente cuando acceda a la página de configuración, su PC deberá tener el mismo rango de dirección que el adaptador (10.10.X.X y la máscara de red 255.255.0.0 en estado de default)

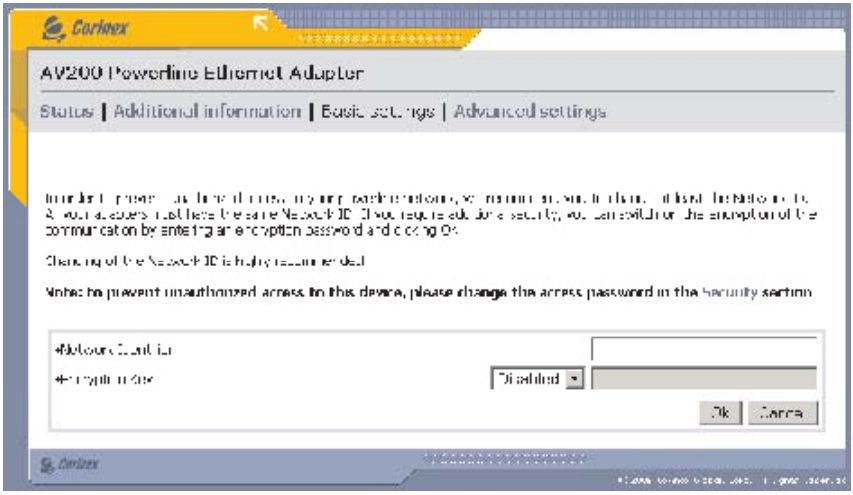
- Si lo requiere, la máscara de red del adaptador también puede cambiarse, por ejemplo tipo C (255.255.255.0). Ésta es una opción más avanzada, por ello le recomendamos ignorarla si no está familiarizado con la misma.

- Si el adaptador será accesado a través de un router (por ejemplo en una oficina con una red amplia), la entrada del IP necesita ser configurada. En caso contrario, puede ignorar esta opción.

LOS CAMBIOS EN EL IP DEL ADAPTADOR TENDRÁN EFECTO DESPÚES DE REINICIARLO. LE RECOMENDAMOS PONER UNA ETIQUETA EN CADA ADAPTADOR CON LA DIRECCIÓN IP, PARA EVITAR PERDER LA LA HABILIDAD DE ACCEDER AL EQUIPO.

3.4.2 Ajustes Básicos

En muchos casos, lo único que necesita ser cambiado es el identificador y/o la encriptación para evitar interferencia con otras redes y para proteger los datos transmitidos. Muchos usuarios no necesitarán accesar a la sección de Ajustes Avanzados para brindar seguridad total a su red Powerline.



La Tecnología AV200 soporta redes múltiples en un mismo circuito eléctrico. Las redes son diferenciadas por los Identificadores de red, los cuales pueden ser configurados en esta sección. El identificador de red es una cadena de caracteres (campo del identificador de red) que actúa simplemente como un nombre para la red. Debe ser el mismo valor para todos los adaptadores en una misma red. Los adaptadores con diferentes identificadores de red no pueden comunicarse entre sí.

La secuencia del identificador de la red puede tener hasta 20 caracteres ASCII. La coma y las comillas son caracteres no soportados. No se recomiendan el uso de caracteres amplios ASCII.

Si desea habilitar en su red la Encriptación 3DES, por favor seleccione alguno de los métodos de entrada siguientes y teclee la contraseña.

Métodos de entrada disponibles:

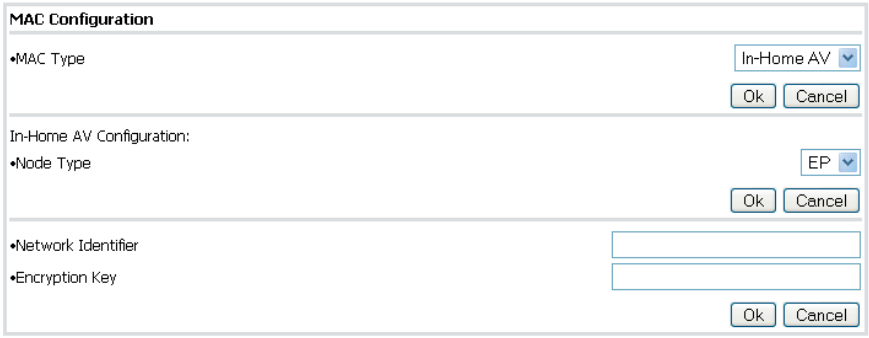
ASCII	Si selecciona **ASCII**, la secuencia de la contraseña de Encryptación puede tener hasta 24 caracteres ASCII que no sean amplios. La coma y las comillas no son caracteres admitidos ni los caracteres amplios.
HEX	Por otra parte, si selecciona la opción **HEX**, la secuencia de la contraseña de Encriptación puede tener hasta 42 dígitos hexadecimales (por ejemplo 34AE4F54B38D). La secuencia en HEX brinda contraseñas más seguras

3.4.3 Configuración Avanzada

La sección de configuración avanzada de la interfase Web se encuentra dividida en varias sub-secciones, las cuales son descritas a continuación.

3.4.3.1 Configuración MAC

Los siguientes parámetros se relacionan con la topología de red. La versión actual del Firmware (Spirit 2.0.21 al momento de esta publicación) soporta una sola topología: In-Home AV. En esta topología dos diferentes tipos de nodos pueden ser configurados, ajustando un nodo para funcionar ya sea como un EP/AP automático (Punto Final o Punto de Acceso, dependiendo de los otros nodos en la red) o como un AP fijo (Punto de Acceso asignado). En la sección 4 (Topología de red In-Home AV) encontrará mayor información sobre las topologías de red disponibles.



Si desea configurar el adaptador para actuar como un EP/AP automático, seleccione la opción **EP** de la lista. Si desea que el adaptador se comporte como un Master, entonces seleccione la opción „**Fixed AP**". En cualquier caso, presione „**OK**" para confirmar su selección.

Nota: El AP fijo se encuentra disponible sólo cuando el adaptador está configurado con un identificador de red que no este vacío.(Por favor lea el siguiente párrafo para más detalles referentes a los Identificadores de red).

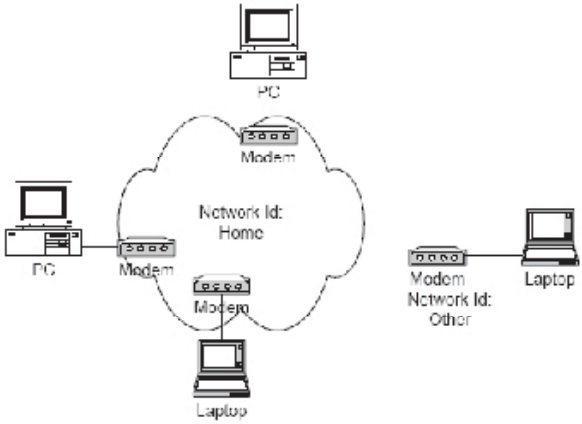
La Tecnología AV200 soporta redes múltiples en un mismo circuito eléctrico. Las redes son diferenciadas por los Identificadores de red, los cuales pueden ser configurados en la sección MAC. El identificador de red es una cadena de caracteres (campo del identificador de red) que actúa simplemente como un nombre para la red. Debe ser el mismo valor para todos los adaptadores en una misma red. Los adaptadores con diferentes identificadores de red no pueden comunicarse entre sí.

Nota : Por favor diríjase a la sección 4.2 para mayor información acerca de los tipos de redes y sus Identificadores de red.

En caso de dejar vacio el campo de Network Identifier, por default, se configurará una red pública y el adaptador podrá comunicarse con el resto de otros adaptadores con el campo de Network Identifier vacio.Cuando ingrese un ID de red, se configurará una red privada.

Nota : La secuencia del Identificador de Red puede tener hasta 20 caracteres ASCII. La coma y las comillas no son caracteres admitidos No se recomienda el uso de caracteres amplios ASCII.

El siguiente esquema muestra un ejemplo de dos redes AV200 con diferentes Identificadores de Red:



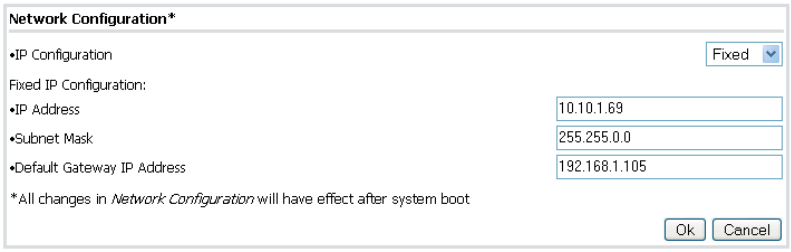
La transmisión de datos entre los adaptadores (llamados módems en el gráfico) está encriptada con un algoritmo 3DES. Esta llave de encriptación puede ser configurada con una secuencia de caracteres (Campo **Encryption Key**), la cual es simplemente una contraseña. Las tres llaves de 56-bit para una encriptación 3DES se obtienen a través de esta contraseña por medio de la función resumen (Hash function). Registrar una cadena nula (dejarla en blanco) deshabilita la encriptación. Después de seleccionar el método de entrada deseado e ingresar una contraseña, presione „**OK**“ para confirmar su selección.

Nota : La encriptación será habilitada solo si se configura un Identificador de Red que no se encuentre vacio.

Nota : Si selecciona la opción **ASCII**, la secuencia de la contraseña de Encriptación puede tener hasta 24 caracteres ASCII que no sean amplios. La coma y las comillas no son caracteres admitidos ni los caracteres amplios. Por otra parte, si selecciona la opción **HEX**, la secuencia de la contraseña de Encriptación puede tener hasta 42 dígitos hexadecimales (por ejemplo 34AE4F54B38D). La secuencia en HEX brinda contraseñas más seguras.

3.4.3.2 Configuración de la Red

Su Corinex AV200 Powerline Wall Mount puede ser configurado para utilizar un DHCP (Asignación automática de la dirección IP), o un IP fijo.
Los siguientes parámetros son utilizados para la configuración con la opción de un IP fijo. Para poder utilizar el adaptador conjuntamente con otros productos dentro de una red In-Home AV, es necesario definir una dirección válida IP única en la red, así como una máscara apropiada de subred y una dirección de entrada. Estos parámetros serán almacenados en el adaptador e implementados una vez que lo reinicie.



Una vez que haya modificado alguno de estos parámetros, presione „**OK**“ para salvar sus cambios

Nota: Cualquier cambio en la configuración de red requiere que usted reinicie el adaptador para tomar efecto.

Nota: Si olvido la dirección IP de su dispositivo, usted podrá recuperarla con la opción „**getIP**“, la cual se encuentra en el CD con la documentación, o podrá descargarla directamente desde el sitio en internet de Corinex en www.corinex.com.

3.4.4 Configuración PHY

Por default, los adaptadores transmiten sobre un rango de frecuencia en cualquier lugar de 2 hasta 32 MHz, y cuando detectan un acceso a la red, sobre un rango de 13.3 hasta 33.3 MHz para poder funcionar sin interferir uno con otro. Este cambio de modalidad se hace automáticamente y no se puede configurar por el usuario. Únicamente es posible habilitar o deshabilitar esta función de muesqueo. Las muescas predefinidas en el adaptador corresponden al plan de banda de la IARU (Unión Internacional de Radio Amateur) para cada región del mundo. Si el adaptador está funcionando en un ambiente donde puede estar causando interferencia a un radio receptor HAM, se recomienda habilitar la función de muesqueo para bloquear la señal Powerline de las bandas de frecuencia usadas por el Radio Amateur.

Nota: Le recomendamos altamente habilitar la función de muesqueo.

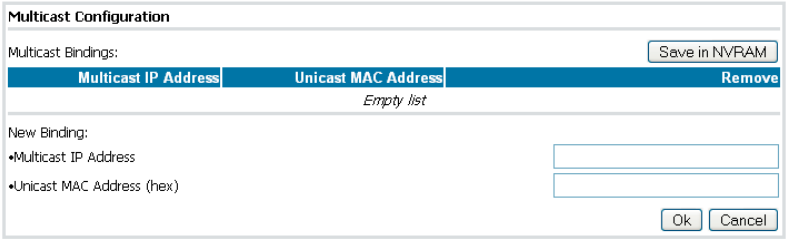
Power Control, es un control automático de la transmisión de la energía que aísla las redes con diferentes Identificadores de red.

La opción de Power Control es activada solamente si hay otras redes presentes en el canal. Si la fuerza de transmisión alcanza el punto del aislamiento entre las redes, la transmisión de la energía permanece en un nivel bajo. Pero si no se alcanza el punto del aislamiento, los nodos continúan transmitiendo en sus niveles originales

3.4.5 Configuración Multicast

Para optimizar el tráfico multicast (corrientes de video, etc.) entre los adaptadores AV200 Powerline, usted podrá especificar que adaptadores desea que reciban el tráfico. De esta manera, otros no podrán recibir la comunicación multicast, y por lo tanto el ancho de banda será utilizado solamente para la transmisión a los destinatarios seleccionados, logrado así que su transmisión y todo en su red sea más eficiente.

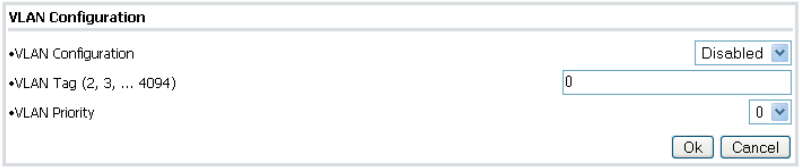
Este esquema muestra la lista de los multicast bindings, donde las direcciones IP del multicast son asignadas a una dirección MAC unicast (fuente de la corriente). Esta lista puede ser almacenada en el adaptador (**guardar en NVRAM**). Por otra parte, usted puede eliminar los bindings marcando las casillas de selección y presionando **OK**. Agregue un binding nuevo a la lista ingresando la dirección multicast de IP en formato decimal (ddd.ddd.ddd.ddd) y la dirección MAC unicast en formato hexadecimal (XXXXXXXXXXXX) dentro de los campos correspondientes y oprima **OK.**
La nueva característica *IGMP Aware Multicast Syndication* incluída en el Spirit 2.0 puede ser habilitada en este formulario. Ésta característica está disponible para redes privadas (con un Identificador de red válido) y Puntos Finales (End Points - EP).



3.4.6 Configuración VLAN

Cuando los adaptadores *AV200 Powerline* son utilizados para una extensión ADSL, es importante que el operador pueda distinguir el tipo de tráfico que cada adaptador está generando. Esto se hace generalmente por medio de etiquetado en la VLAN. La Tecnología AV200 brinda la posibilidad de etiquetar todo el tráfico que ingresa a la red Powerline a través de la interfase Ethernet de cada adaptador. Se trata solamente de etiquetado, no hay filtración VLAN dentro de la red AV200 Powerline.

Los parámetros para la configuración de VLAN se pueden configurar en el formulario que se muestra a continuación. Primeramente, el VLAN Spirit puede ser habilitado o deshabilitado (seleccione la opción Spirit VLAN). Si está habilitado, la etiqueta VLAN (casilla Spirit VLAN Tag) y la prioridad (casilla Spirit VLAN Priority) pueden ser configuradas también.

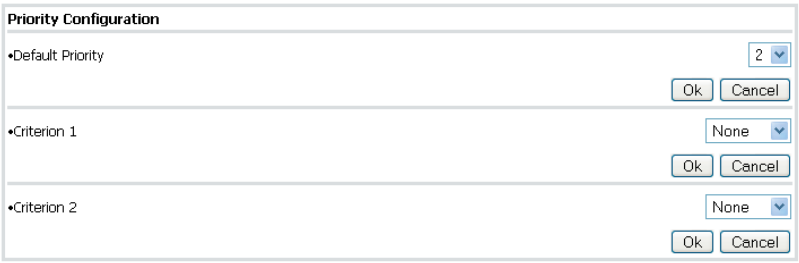


3.4.7 Configuración de Prioridades

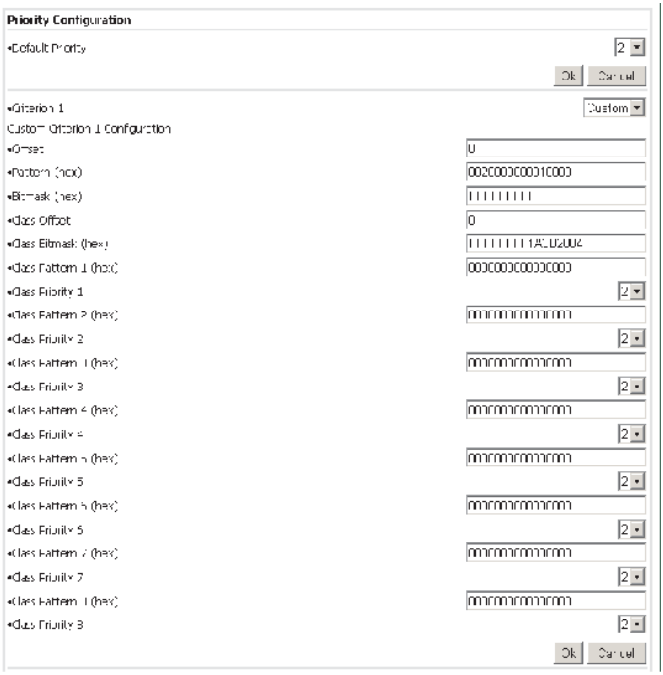
En esta sección, se encuentran varias opciones disponibles. La primera y más sencilla de entender y utilizar es el Valor Predefinido de la Prioridad (**Default Priority value**). La salida del tráfico de datos generada por los adaptadores que se encuentre configurada con una prioridad mayor, tendrá preferencia en la red. El resto de los parámetros le permiten al usuario configurar dos clases de criterios de servicio (casillas de selección **Criterion 1** y **Criterion 2**).

Si selecciona la opción Ninguno (**None**), **802.1p** o **TOS**, los parámetros personalizados permanecerán ocultos, dejando una configuración predefinida.

.

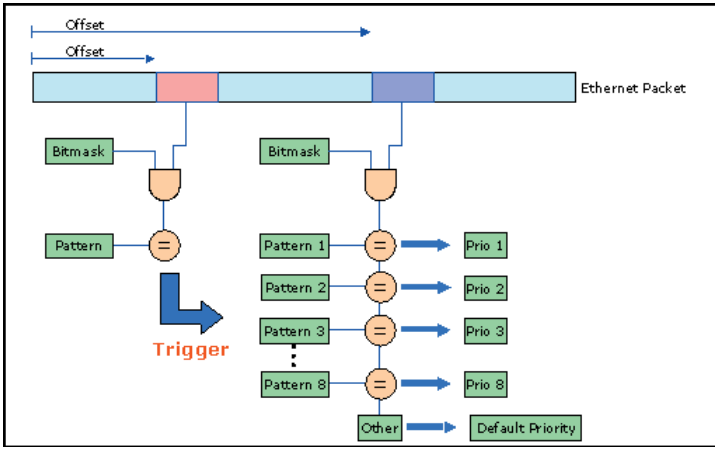


En cambio, si selecciona la opción Personalizar (**Custom**), aparecerán los parámetros personalizados como se muestra en el siguiente gráfico y podrán ser configurados.



Algunas veces cuando existen diversas corrientes de tráfico de datos en una misma red, es necesario establecer varios niveles de prioridad para garantizar que las aplicaciones sensibles de banda ancha tales como vídeo o telefonía mantengan un óptimo funcionamiento aún cuando exista congestión en la red.

El clasificador de tráfico es un paquete de inspección capaz de distinguir varios patrones dentro de una estructura Ethernet y asignar diferentes niveles de prioridad a cada uno de ellos. Para asegurar que la clasificación esté hecha correctamente, existe un mecanismo Trigger previo a la clasificación final. El mecanismo está basado también en el reconocimiento de patrones en una locación determinada en cada paquete Ethernet. El siguiente esquema describe el mecanismo de clasificación de paquetes.



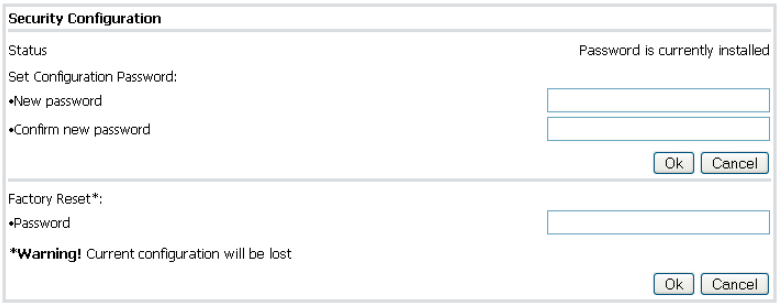
Existe un offset, un bitmask y un patrón para el condicionamiento Trigger. Este condicionamiento es utilizado para asegurar por ejemplo que la estructura de Ethernet contenga una estructura IP. Para verificar esta condición, el offset deberá ser configurado a 16 y el bitmask a 0xFFFF. Si el patrón resultante es 0x0800, entonces la estructura de Ethernet contiene un paquete IP y la clasificación puede ser hecha a un campo conocido.

También hay otras opciones disponibles de offset y de bitmask para la condición de clasificación. El valor que resulte se compara con una serie de patrones. Si el valor coincide con el de algún patrón determinado, el paquete será clasificado con la prioridad especificada. Por el contrario, si el valor no coincide con ninguno de los patrones proporcionados, se mantendrá la prioridad por default.

Hay una serie de criterios predefinidos para la clasificación de tráfico, que se encuentran en el campo **802.1p** del paquete Ethernet o el campo **TOS** del paquete IP.

3.4.8 Configuración de Seguridad

La aplicación Web le permite cambiar la configuración de la contraseña, solamente necesita ingresar una nueva en la casilla especificada (deberá escribir dos veces su contraseña para confirmarla). Si se dejan ambas casilllas vacias, la configuración de la contraseña será deshabilitada (aparecerá el siguiente mensaje en el formulario de configuración de seguridad: '*Ninguna contraseña ha sido configurada*'. Por lo tanto, la configuración Web estará deshabilitada también. La autentificación puede ser activada nuevamente una vez que ingrese una contraseña.



Si desea restaurar los ajustes del adaptador configurados por default, puede solicitar restablecer los valores iniciales de fábrica. Para ello, escriba la contraseña „**betera**" en la casilla correspondiente y presione **OK**. El adaptador reiniciará con la siguiente configuración:

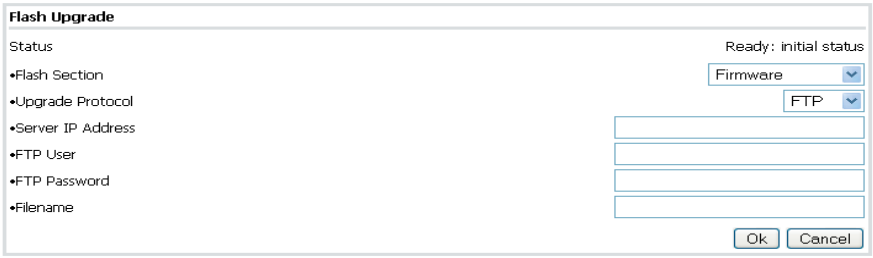
- Dirección IP = 10.10.1.69
- Contraseña para la configuración de la interfase = paterna
- Contraseña para restablecer los valores iniciales de fábrica = betera
- El tipo de dispositivo será un EP/AP automático
- El Identificador de red (Network Identifier) permanecerá vacío
- No habrá encriptación ni ajustes VLAN

3.4.9 Reinicio del Hardware

Si presiona este botón hará que su adaptador se restaure (o reinicie). Se mantendrá la misma configuración, y se aplicará cualquier cambio realizado en los ajustes de configuración de red. Esto significa que si usted por ejemplo cambió la dirección IP, el adaptador se reiniciará con esa nueva dirección.

3.4.10 Actualización Flash

El firmware, el loader y los ajustes de fábrica son almacenados en la memoria Flash. Para actualizarlos, primero elija la sección Flash (**Firmware, Loader** o **Ajustes de fábrica**) y el protocolo (**FTP o TFTP**). Posteriormente escriba la dirección IP del servidor **FTP** o **TFTP** (casilla **Server IP Address**). En caso de que el servidor sea tipo FTP, ingrese el nombre del usuario (**FTP User**) y la contraseña (**FTP Password**). Ya sea para FTP o para TFTP, escriba el nombre de la imagen del archivo Firmware (**File Name**). Por último, presione **OK**.

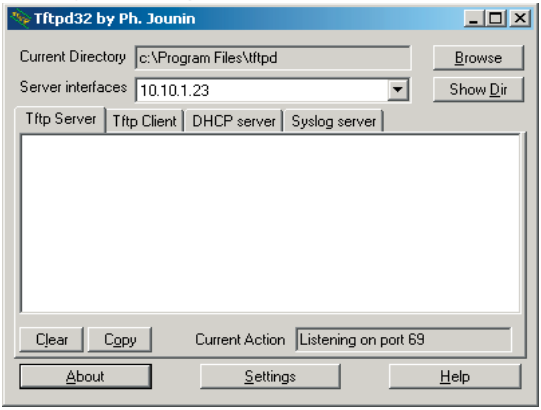


3.4.11 Actualización del Firmware utilizando un servidor TFTP

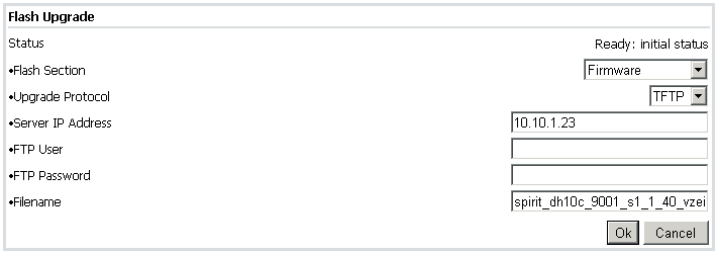
Para actualizar el firmware del módem, utilizando un servidor TFTP, este servidor deberá estar funcionando en su ordenador. Le recomendamos una herramienta llamada **TFTPD32**, la cual es gratis. Usted podrá descargarla en la siguiente dirección de internet **http://tftpd32.jounin.net/**. La imagen del archivo Firmware es proporcionada por Corinex.

Siga los pasos descritos a continuación para actualizar el Firmware del módem:

1. Ejecute **TFTPD32**. Esta aplicación muestra la GUI (Interfaz gráfica de usuario en el siguiente esquema.



2. Coloque el archivo firmware en el directorio actual (**Current Directory**) o especifique la ruta donde se encuentra el archivo.
3. Abra su navegador Web e ingrese el IP del módem que desea actualizar
4. Cuando se descargue la página, presione cambio de configuración (**Change configuration)**.
5. En la ventana de **Firmware Update** seleccione TFTP, escriba el IP del servidor TFTP y el nombre del archivo Firmware como se muestra en la imagen siguiente:

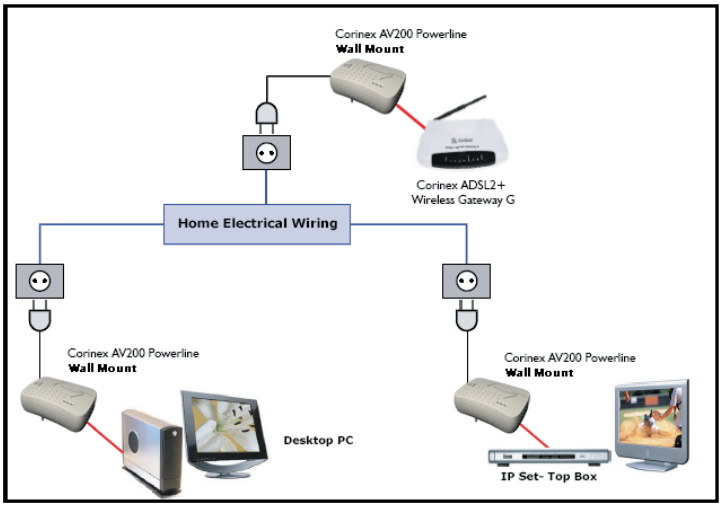


6. Presione **OK** para iniciar el proceso. El progreso de la información es mostrado en la página Web cada 30 segundos.
7. El módem descargará primero el archivo y después calculará el CRC
8. Si el CRC es correcto, el botón para reiniciar el Hardware (**Hardware Reset**) estará resaltado. El módem deberá ser reiniciado para que el nuevo firmware empiece a funcionar.

3.4.12 Configurando Aplicaciones de Video

En el caso de una red donde el tráfico en tiempo real debe coexistir con altos volúmenes de transferencia de datos, el clasificador de servicios debe ser configurado para priorizar el tráfico de las aplicaciones sensibles de banda ancha sobre otros tipos de tráfico.

Como ejemplo, considere la red que se muestra en el siguiente esquema.



El nodo conectado al módem ADSL es el punto de acceso. Los datos y el video son transmitidos a través del ADSL. El punto de acceso tiene que dar prioridad al video UDP sobre los datos para evitar daños en las imágenes cuando exista una descarga de un alto volúmen de datos.

Antes que nada, el campo de **Criterion** debe estar configurado como personalizado (**Custom**), para poder configurar las reglas de acuerdo a las necesidades del usuario para la clasificación de tráfico.

Para priorizar el tráfico UDP, primeramente se deberán identificar los paquetes Ethernet que contengan paquetes IP. Debido a que la casilla de inspección es de dos bytes, el bitmask debe cubrir también el mismo espacio. Por lo tanto, el OxFFFF es utilizado como bitmask. Estos valores son introducidos en las casillas de **Custom Criterion Offset**, **Custom Criterion Pattern** y **Custom Criterion Bitmask**

Una vez que el condicionamiento Trigger sea ingresado, se deberán especificar las reglas de clasificación. Sólo las casillas que se encuentren actualmente modificadas tomarán efecto. El resto serán ignoradas. Los paquetes IP tienen una casilla de un byte y un offset configurado en 27 que indica el tipo de protocolo. El protocolo UDP tiene un patrón 0x11. Debido a que la casilla de inspección es de un byte, el bitmask debe cubrir también el mismo espacio Los valores son registrados dentro de la primera regla disponible (1) como **Class Pattern 1** (Patrón de clasificación) y **Class Priority 1** (Prioridad de clasificación).

El resto del tráfico (FTP, Navegador Web, etc.) tendrá la prioridad 2 por default. En el otro lado de la red, el módem conectado al ordenador también clasificará la salida de tráfico de datos con la prioridad por default 2 debido a que ninguna regla ha sido establecida.

Nota: Cuando el valor del offset se encuentre en formato decimal, los patrones y los bitmsks estarán en formato hexadecimal por default.

3.5 Página de Actualización del Firmware

Ésta página aparecerá cuando una actualización del firmware sea requerida por la página de cambio de configuración (**Change Configuration)**, muestra el estado actual de la actualización del firmware. La página de actualización del Firmware (**Firmware Update)** es descargada automáticamente cada 30 segundos. Cuando la línea de estatus muestre el siguiente mensaje: **Ready: finished correctly**, el adaptador podrá ser reiniciado, y el nuevo firmware será descargado.

Si el proceso de actualización falla, un mensaje indicando un error aparecerá. En este caso el adaptador podrá ser reiniciado sin ningún riesgo, pero el firmware previo estará aún presente en el adaptador.

4 Topología de Red In-Home AV

4.1 Introducción

Una red In-Home AV está formada por un nodo (Punto de Acceso AP) y a su vez por varios puntos terminales (End Points EP's). Este tipo de red puede tener un solo punto de acceso (AP). Sin embargo, es posible que varias redes In-Home AV puedan coexistir simultáneamente, puesto que cada una de ellas cuenta con su propio Punto de Acceso (AP), y cada uno de estos puntos es separado de los otros por medio de un identificador de red distinto. Un módem puede ser configurado como un Punto de Acceso Fijo (por ejemplo este será siempre un AP) o como un EP/AP automático. En caso de elegir una configuración automática, el protocolo de la red In-Home AV decidirá dinámicamente si el nodo se convertirá en un EP o en un AP. Esto significa, que en una red donde no ha sido definido ningun AP, al menos uno de los puntos terminales (EP's) se redefinirá a sí mismo como un AP automático.

Nota: Se recomienda definir un IP fijo, esto proporcionara una mayor estabilidad para la reconfiguración y en ambientes con diferentes redes

Nota: No es necesario tener una conectividad completa entre todos los nodos dentro de una red. La topología de red será configurada automáticamente, permitiendo el uso de repetidores si la conectividad entre dos nodos falla

A continuación se presentan los pasos necesarios para la configuración básica de una red In-Home AV para cada nodo:

- Configure la **dirección IP.** Deberá ser una dirección **IP** única (por ejemplo una dirección privada como 10.10.1.<*el último byte de la dirección MAC* >).
- Seleccione la configuración espectral (Las **Ranuras** deben estar habilitadas o deshabilitadas).
- Configure el identificador de red (**Network Identifier**), deberá ser el mismo valor para todos los nodos en la red.
- Configure la llave de encriptación (**Encryption Key**),deberá ser el mismo valor para todos los nodos en la red.
- No es necesario configurar el MAC de la red In-Home AV, ya que existe unicamente una sola topología de red disponible en la versión actual del firmware. La configuración de un AP fijo (**Fixed AP**), es opcional.

4.2 Escenarios de red

En ésta sección se presentan los diferentes tipos de escenarios de red para el usuario, así como su aplicación y configuración.

Existen dos tipos de redes In-Home AV.

• **Red Pública** - Ésta es la configuración por default para una red In-Home AV. Si el usuario no desea configurar su red, el protocolo de configuración de la red configurará todos los nodos automáticamente. Por defautl, todos los nodos son considerados como EP's y tienen un ID de Red Pública. Si el protocolo no detecta un AP en el canal, seleccionará un EP como un AP automático. Todos los EP's se conectarán directamente al AP automático si es que tienen visibilidad directa, o a un EP que actúe como un repetidor. De esta manera, la red será establecida.

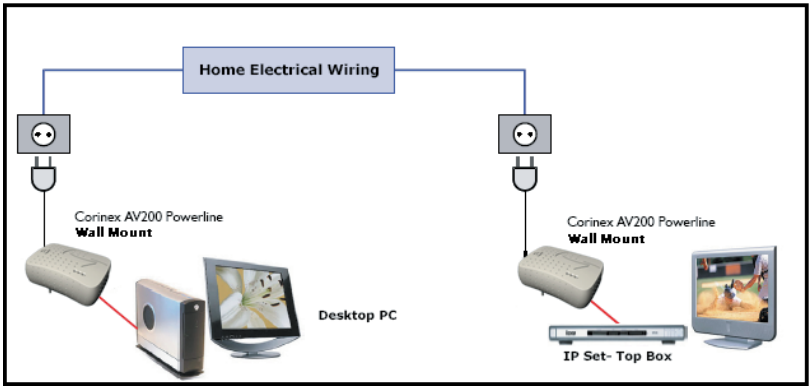
• **Red Privada**- Para configurar una red privada (es decir, para asegurar la privacidad de sus datos), un ID de red debe ser asignado a todos los nodos utilizando la herramienta de configuración. Se recomienda configurar un nodo como AP fijo (por ejemplo el nodo con el servidor de video o para acceso a Internet). Si el AP fijo es desactivado o no es definido por el usuario, el protocolo de configuración seleccionará un EP para ser transformado en un AP (automático) y así configurar la red.

4.2.1 Escenarios simples de red

Las siguientes dos secciones le muestran ejemplos de una red simple In-Home AV

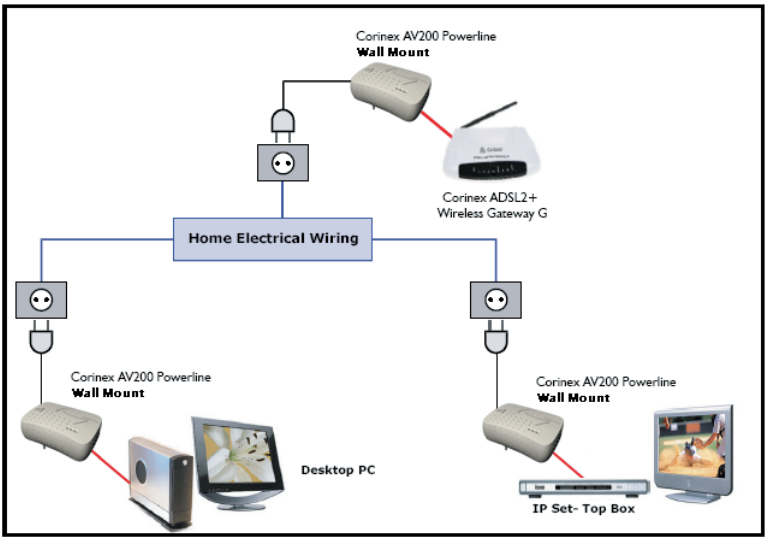
4.2.1.1 Red de Área Local utilizando dos adaptadores AV200

El siguiente esquema muestra una red simple PLC (Powerline), donde dos adaptadores son utilizados para crear una conexión de área local disponible en todos los enchufes dentro del hogar. Este el el ejemplo más sencillo, donde no se requiere ninguna configuración de QoS (Calidad del Servicio).



4.2.1.2 Extendiendo una conexión de internet a una red AV200 Powerline

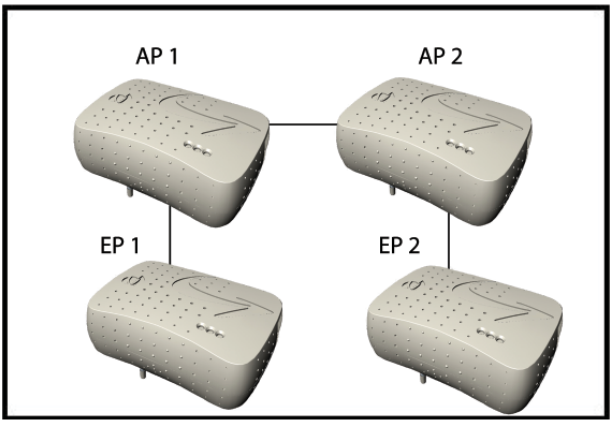
El siguiente esquema muestra una red PLC (Powerline) más avanzada, con 3 adaptadores Corinex AV200. Ésta es una configuración común de red, donde el acceso a internet y video digital son trasmitidos a tráves de la misma línea ADSL. Ésta configuración requiere algunos ajustes en el Qos para garantizar una óptima calidad de video aún cuando la red tenga altos volúmenes de datos a través de la conexión a Internet.



Nota: Cualquiera de estos dos escenarios básicos puede ser ampliado, agregando más adaptadores, computadores o módulos de conexión (set-top boxes).

4.2.2 Escenarios de redes múltiples

Un escenario de red múltiple ocurre cuando existen dos o más nodos de diferentes redes In-Home AV (diferentes identificadores de red) con visibilidad directa. En este caso, se activa un mecanismo coexistente que permite una forma de comunicación segura y sin interferencia entre los nodos de redes diferentes



En escenarios de redes múltiples, tales como el que se muestra en el gráfico de arriba, existe un nuevo componente, llamado controlador QoS. La función de este controlador es asignar canales de acceso a las diferentes redes. El controlador QoS actúa al mismo tiempo que esl AP de alguna de las redes. Cuando se presentan diversas redes In-Home, el protocolo de coexistencia selecciona automáticamente uno de los puntos AP como el QoS controlador.

4.2.2.1 Dos redes que no cuentan con visibilidad directa

Si se configuran dos redes In-Home AV que no cuentan con visibilidad directa entre alguno de los nodos pertenecientes a las diferentes redes, entonces estas redes se comportarán como dos redes independientes. Ambos Puntos de acceso actuarán como controladores QoS.

4.2.2.2 Dos redes con visibilidad directa

Diferentes redes son definidas por diferentes identificadores de red

Si dos redes In-Home AV son configuradas como redes públicas, el protocolo de coexistencia actuará como si fuesen una sola red. El Identificador de Red es transmitido nodo por nodo para comunicar la existencia del mismo en la red. Si un nodo con un ID de red A recibe un nodo con ID de red B, entonces reconoce que hay al menos dos redes compartiendo el mismo canal.

For example, one In-Home AV network is configured and running. A second network is configured and starts working after the first network is configured. Then the second network will notify its presence to the first network in some specified access slots, and both networks will automatically be reconfigured and will share the channel. If both networks are configured at the same time, the QoS controller will be selected from all of the present APs.

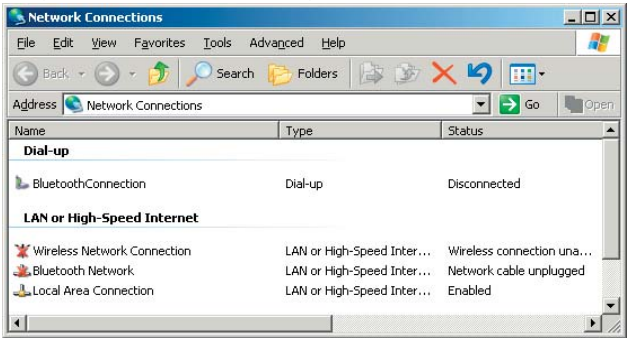
5 Configuración de Red

5.1 Configurando una dirección IP en su ordenador

Esta sección le indica como configurar un IP estático en su sistema operativo, para poder conectar y configurar su *AV200 Powerline Adapter*.

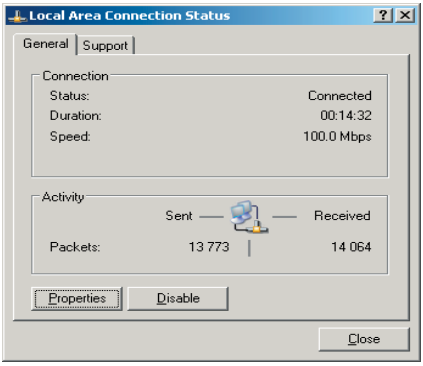
5.1.1 Configurando un IP estático en Windows XP

1. Presione el botón de Inicio (**Start**), abra el Panel de Control (**Control Panel).** Seleccione el ícono de Conexiones de Red (**Network Connections**), posteriormente aparecerá la ventana de Conexiones de Red (**Network Connections**).

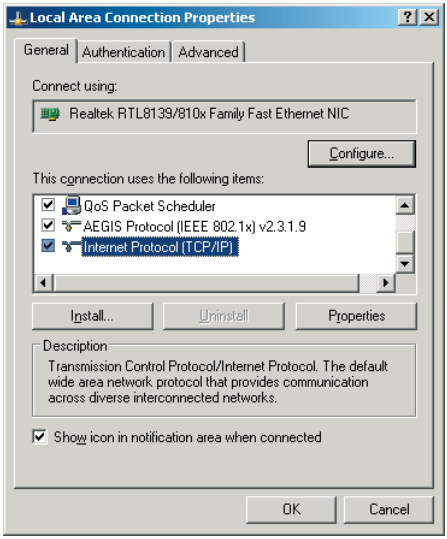


2. Seleccione el ícono Conexión de área local (**Local Area Connection)** para el adaptador correspondiente (Ethernet o Powerline generalmente el primer adaptador en la lista). Haga doble click en la conexión de área local (**Local Area Connection**)

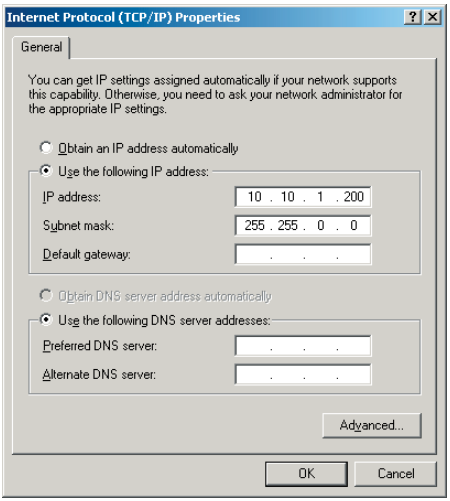
3. La pantalla que muestra el estatus de la conexión de área local aparecerá. Oprima el botón de Propiedades (**Properties**).



4. Seleccione el protocolo de Internet (**Internet Protocol) (TCP/IP)** y oprima el botón de Propiedades (**Properties**).



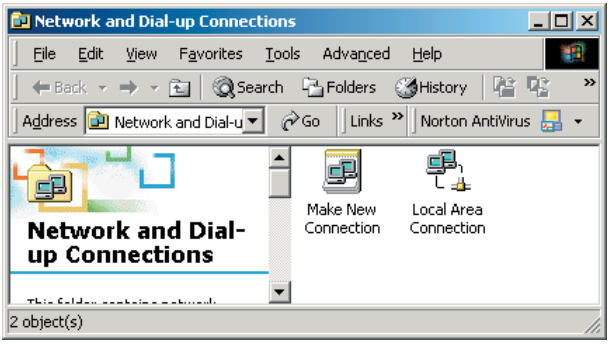
5. Seleccione la opción Usar la siguiente dirección IP (**Use the following IP address)**. Ajuste la dirección IP manualmente en formato 10.10.1.X (por ejemplo 10.10.1.200) y la máscara 255.255.0.0 en los ajustes TCP/IP. La casilla de Entrada Predeterminada (**Default gateway)** puede dejarla vacia.



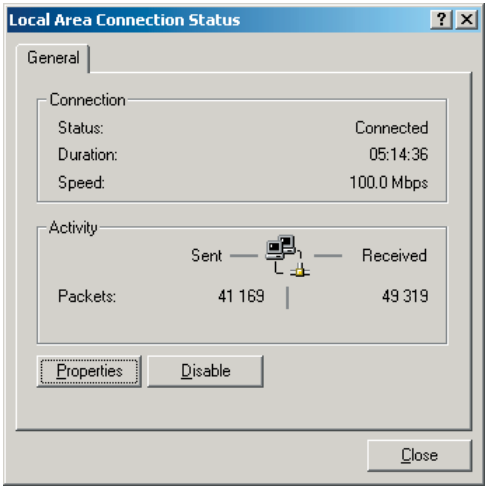
6. Presione el botón **OK** de la ventana de Propiedades TCP/IP para completar la configuración de su ordenador y finalmente para cerrar la ventana oprima cerrar o el botón **OK**.

5.1.2 Configurando un IP estático en Windows 2000

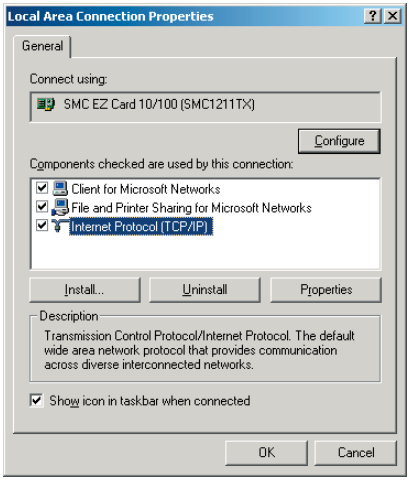
1. Diríjase a la pantalla de Redes, para ello, oprima el botón de Inicio (**Start**) Seleccione la opción Ajustes (**Settings**) y después elija Panel de Control (**Control Panel**). Una vez hecho esto, de doble click en el ícono Red y conexiones de marcado (**Network and Dial-up Connections**).



2. Seleccione el ícono de Red y Conexiones de marcado (**Network and Dial-up Connections)** para el adaptador Ethernet correspondiente (generalmente el primero en la lista de conexión de área local). No elija una entrada TCP/IP cuyo nombre sea DUN, PPPoE, VPN o AOL. Haga doble click en la conexión de área local (**Local Area Connection**). Aparecerá la siguiente ventana:

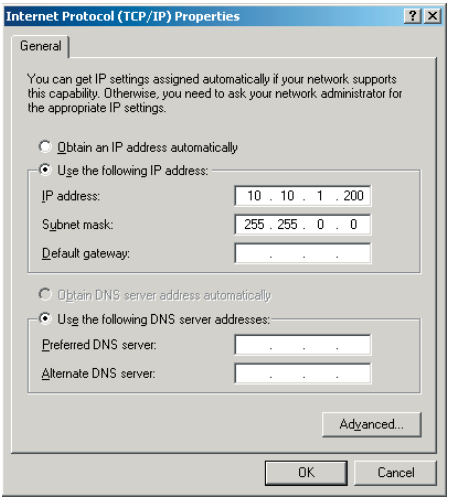


3. Presione el botón de Propiedades (**Properties**) para visualizar las propiedades de la conexión de área local.



4. Seleccione el protocolo de Internet (**Internet Protocol) (TCP/IP)** y oprima el botón de Propiedades (**Properties)**

5. Seleccione la opción Usar la siguiente dirección IP (**Use the following IP address)**. Ajuste la dirección IP manualmente en formato 10.10.1.X (por ejemplo 10.10.1.200) y la máscara 255.255.0.0 en los ajustes TCP/IP. La casilla de Entrada Predeterminada (**Default gateway)** puede dejarla vacia.



6. Presione el botón **OK** de la ventana de Propiedades TCP/IP para completar la configuración de su ordenador y finalmente para cerrar la ventana oprima cerrar o el botón **OK**.

5.1.3 Configurando un IP estático en Windows 98

1. Diríjase a la pantalla de Redes, para ello, oprima el botón de Inicio (**Start**) Seleccione la opción Ajustes (**Settings**) y después elija Panel de Control (**Control Panel**).Una vez hecho esto, de doble click en el ícono Redes (**Network**).

2. En el tabulador de configuración, seleccione la línea TCP/IP para el adaptador Ethernet correspondiente. No elija una entrada TCP/IP cuyo nombre sea DUN, PPPoE, VPN o AOL. Si solamente aparece la palabra TCP/IP, seleccionela. Si la opción TCP/IP no se encuentra listada, porfavor diríjase al Manual de Usuario en la sección cómo instalar un protocolo TCP/IP. Después oprima el botón de Propiedades (**Properties**).

3. Si no cuenta con un servidor DHCP en la red, entonces seleccione la opción Usar la siguiente dirección IP (**Use the following IP address)**. Ajuste manualmente la dirección IP en el formato 10.10.1.X (por ejemplo 10.10.1.200) y la máscara 255.255.0.0 en los ajustes locales TCP/IP y después presione **OK**

4. Presione nuevamente el botón **OK**. Windows probablemente le pedirá el CD de instalación de Windows o archivos adicionales. Selecciónelos indicando la ubicación de los archivos, por ejemplo D:\win98, D:\win9x, c:\windows\options\cabs, etc. (En caso de que "D" sea la letra de su unidad de CD-ROM).

5. Windows le pedirá que reinicie su ordenador. Presione el botón Si (**Yes**). Si Windows no le pide reiniciar su sistema automáticamente, reinícielo de cualquier manera.

5.1.4 Configurando un IP estático en Linux

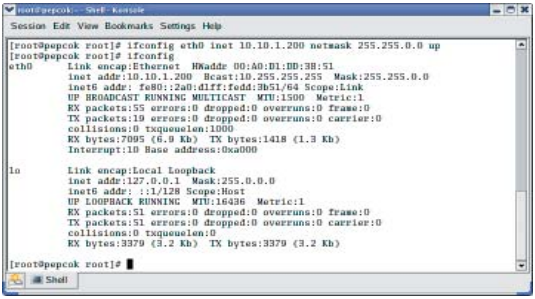
1. Usted deberá estar registrado como un usuario (*root*) para poder cambiar la dirección IP en su sistema Linux.

2. Ingrese a la consola, en caso de estar utilizando alguna interfase gráfica de usuario (KDE, Gnomo).

3. Para cambiar la dirección IP a 10.10.1.200, ingrese el siguiente comando:

   ifconfig eth0 inet 10.10.1.200 netmask 255.255.0.0 up

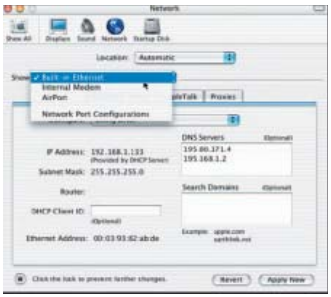
   y presione **Enter**. El comando anterior tomará eth0 como el nombre de la interfase Ethernet, aunque puede variar en su sistema. Usted podrá verficar el estatus de todas las interfases de red ejecutando el comando **ifconfig** en la consola.



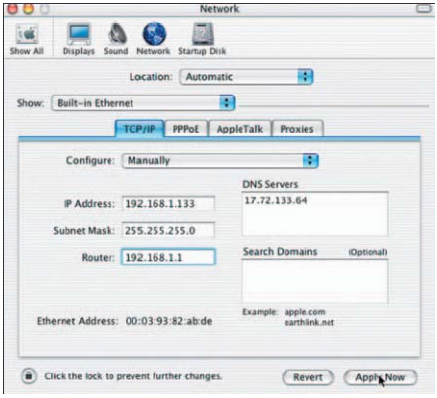
5.1.5 Configurando un IP estático en el Sistema Operativo Mac

1. Abra el Panel de Control de Redes (**Network Control Panel**) dentro de Preferencias del Sistema (**System Preferences)**.

2. Seleccione la opcion **Built-in Ethernet** (Ethernet incorporado) del menú emergente (pop-up menu).



3. Ajuste manualmente la dirección **IP** en el formato 10.10.1.X (por ejemplo 10.10.1.200) y la máscara de sub-red (**Subnet Mask)** en 255.255.0.0.



4. Presione Aplicar ahora (**Apply Now)** y cierre el panel de Redes (**Network)**, sin olvidar guardar sus ajustes.

5.2 Mejorando el funcionamiento de la Red

El período de latencia en una red PLC es mayor que en una red Ethernet. La mayoría de los sistemas operativos tienen una configuración por default para el período de latencia en la red basada en estructuras de Ethernet. Para obtener un máximo funcionamiento para un tráfico TCP (descarga de archivos a través de FTP por ejemplo) el sistema operativo tiene que ser ajustado conforme a las nuevas condiciones de la red.
Para mejorar el funcionamiento de la red, le proporcionamos los scripts para los sistemas operativos Windows y Linux, los cuales encontrará en el CD adjunto, dentro de la carpeta scripts. Los scripts configurarán el tamaño de la ventana TCP a 512 kB.

Para el sistema operativo Windows, simplemente haga doble click en el archivo **tcpwin.reg**, que encontrará dentro del CD de la documentación en la carpeta de „scripts“ Usted podrá ejecutar también el script mediante la opción de arranque automático (autorun) del CD.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"TcpWindowSize"=dword:00080000
"GlobalMaxTcpWindowSize"=dword:00080000
"Tcp1323Opts"=dword:00000003
```

tcpwin.reg para el sistema operativo Windows

Para el sistema operativo Linux, con kernel 2.4 o superior funcionando, abra la consola y ejecute el comando **./tcpwin.sh 512** deberá estar registrado como usuario (*root*).

```
#!/bin/sh

#
# Corinex TCP Window Size Tweak
#

if [ "$#" -eq 0 ]
then
        echo "Usage: $0 <window size in KB>"
        exit
fi

WIND=`expr $1 \* 1024`

echo $WIND > /proc/sys/net/core/rmem_default
echo 8388608 > /proc/sys/net/core/rmem_max
echo $WIND > /proc/sys/net/core/wmem_default
echo 8388608 > /proc/sys/net/core/wmem_max

echo 4096 $WIND 8388608 > /proc/sys/net/ipv4/tcp_rmem
```

tcpwin.sh para el sistema operativo Linux

Una vez aplicado el script, por favor reinicie su sistema. Esto deberá realizarse para ambos sistemas operativos ya sea Windows o Linux.

5.3 Verificando el funcionamiento de la Red

En la página principal, bajo el encabezado de conexiones PLC disponibles (**Available PLC Connections**), hay una lista de direcciones MAC de todos los adaptadores cercanos que tienen una conexión con el adaptador. La lista también indica el rendimiento (velocidad actual en transferencia de datos), en términos de transmisión y recepción, que el adaptador alcanza con cada adaptador en la red.

Available PLC Connections

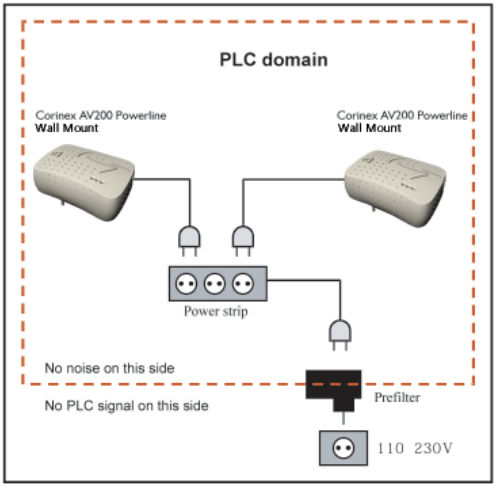
PLC Port	MAC Address	Phy Tx Throughput	Phy Rx Throughput	Bridge State
10	0050C22CF6B8	116 Mbps	114 Mbps	Forwarding
9	0050C22CF6C6	112 Mbps	110 Mbps	Forwarding

5.4 Utilizando Filtros PLC

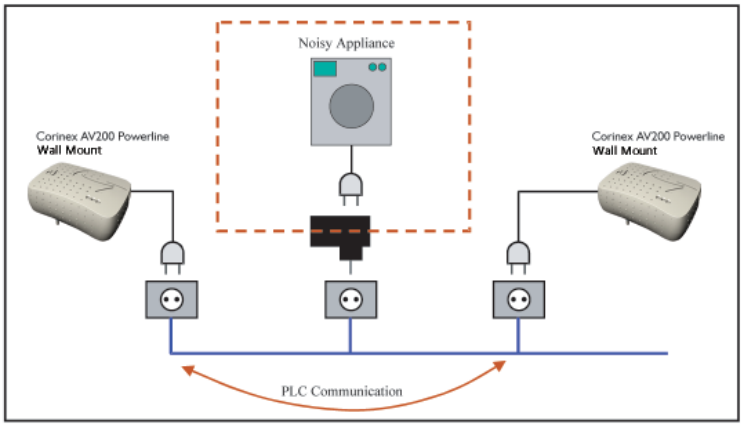
Un filtro PLC (Powerline) es un filtro paso-bajo (low-pass) que sólo permite un voltaje principal de 50/60 Hz. Este filtro bloquea la señal Powerline.

Cuando utilizar este filtro:

- Cuando desee aislar una red de prueba Powerline del resto de la red eléctrica, o si no desea que la señal de la red de prueba Powerline salga e interrumpa el funcionamiento de otros adaptadores, o simplemente porque desea asilar esta red del ruido o del tráfico del resto de la red eléctrica. Esta configuración se ilustra a continuación en el siguiente gráfico.



- Cuando desee aislar el ruido eléctrico ocasionado por algun electrodomésticos, considerando que el ruido recae en la bands del PLC e interrumple la señal de los adaptadores. Esta configuración se muestra en la siguiente imagen.



6 Guía de Solución de Problemas

El *Corinex AV200 Powerline Wall Mount* ha sido diseñado como un dispositivo para una conexión confiable y de fácil instalación. Por favor diríjase a la lista que se presenta a continuación para ayudarle en la solución de problemas.

El indicador de encendido (POWER LED) se encuentra apagado

1. Verifique la conexión del cable eléctrico a la entrada del adaptador
2. Asegúrese que el cable del adaptador se encuentre conectado directamente al enchufe y que este último tenga corriente eléctrica.
3. Intente con otro enchufe.

El indicador de transmisión Powerline se encuentra apagado

1. Asegúrese que el adaptador se encuentre conectado directamente al enchufe, en vez, de estar conectado as un supresor de picos o a un cable eléctrico.

El indicador Ethernet (Ethernet LED) se encuentra apagado.

1. Asegúrese que el adaptador se encuentre conectado con un dispositivo Ethernet, habilitado con un cable tipo RJ-45 y que ambos dispositivos estén activados.

Si los problemas persisten, por favor visite nuestro sitio en internet: **www.corinex.com** y diríjase a la sección correspondiente para mayor información de acuerdo a su producto. Usted también encontrará novedades, manuales y actualizaciones de software, así como una serie de preguntas frecuentes (FAQ)

Para evitar accidentes personales y daños en el sistema:

1. El método principal es desconectar el dispositivo completamente de la red eléctrica, es decir, desconectarlo totalmente del enchufe eléctrico.
2. Nunca instalar el dispositivo en áreas húmedas o cerca de radiadores o calefactores.
3. Nunca utilizar el dispositivo en la intemperie
4. Desconécte inmediatamente el dispositivo durante fuertes tormentas
5. Por ningun motivo abra el empaque del adaptador

Si su problema no pudo ser resuelto utilizando los recursos de informacion que se mencionan en el presente documento, por favor enviénos la descripción del mismo a través de la siguiente dirección de internet http://www.corinex.com/web/com.nsf/Doc. Así mismo, deberá adjuntar toda la información posible acerca de su dispositivo en la Red cuando nos contacte por este medio. Esto último incluye:

- Tipos de dispositivos con los que cuente, si es posible también con los números de serie de cada uno de ellos (impresos en las etiquetas de seguridad)
- Señalar cuales dispositivos funcionan incorrectamente o no funcionan del todo (indicando los problemas presentados)
- Si es posible, envienos un esquema de su topología de red con las direcciones IP para los computadores/router/puntos de acceso, esto agilizará la estimación de su problema.Si utiliza algún producto que no sea Corinex, por favor especifique de que tipo de producto se trata. El esquema podrá ser elaborado en cualquier editor de gráficos, exportándo el archivo a algun formato para gráficos (JPEG, GIF) o simplemente elabore en una hoja el dibujo, escaneelo y anexelo con el resto de la información.
- Especifique el sistema operativo utilizado con los dispositivos
- Por favor envienos la versión del firmware y la confirguración de dichos dispositivos. Refierase al manual del usuario para las intrucciones detalladas de este último punto

NetCamCenter

The Leading IP Video Surveillance Solution for Network Camera and Video Server

NetCamCenter is a control center designed for monitoring and recording multiple network cameras and video servers. Enables you to integrate your network cameras at different locations and monitor with one IP address.

Enhanced digital video recording

By utilizing our proprietary video engine and Microsoft Windows Media™ technology, NetCamCenter provides the best compression but also ensures the best quality for your video. This brings you significant saving on the hard drive space.

- Auto deletes the oldest video file for you to recycle the hard disk space.
- Playback video and monitor remotely while recording video.
- You can assign each camera to a different recording folder for maximum storage.
- Supports various compression ratio that best suit your needs.
- Recording video format: Windows Media™

High quality video for real-time streaming

If you are using network cameras and NetCamCenter on LAN, you can use NetCamCenter's Windows Media™ streaming feature to boost the remote viewing frame rate.

Search video by date or event

Simply enter date and time to search the video or search the video by event.

Motion Detection

Supports setting up multiple areas for motion detection. You can choose the following methods to have NetCamCenter alert you whenever motion is detected.

- Email notification with captured images
- Play an alarm sound to deter the intruder.
- Alert you by phone

Flexible display mode

- Display mode: 1x1, 2x2, 3x3, 4x3, 4x4, 5x5, 6x6, 7x7, 8x8, 9x9 and 10x10
- Rotates video windows if there are more cameras than available video windows on the screen.
- Hide particular camera in Kiosk mode.

128 bit file fingerprint assure the video file is authentic

NetCamCenter can generate 128 bit file fingerprint for each video file to assure the video file is authentic.

Built-in web server

Enables you to view your network cameras with just one IP address.

Authentication

You can setup multiple usernames and passwords to control the web access.

Error recovery

NetCamCenter will try to reconnect to the cameras upon network or camera errors.

Monitoring from your Pocket PC

Enables you to monitor on Pocket PC. You can watch the remote video clip on your network ready Pocket PC!

Hardware supported by NetCamCenter

- Axis
- Canon
- D-Link
- IQinVision
- JVC
- MOBOTIX
- NetComm
- Panasonic
- Pixord
- Sony
- Stardot
- Toshiba
- TrendNet
- VEO
- Vivotek

Software requirements

- Microsoft Windows XP/2000/2003 operating system (Windows Service Pack 4 for Windows 2000 and Service Pack 2 for XP)
- Microsoft Internet Explorer 5.0 or above
- Windows Media™ Player 7.0 or above

Hardware requirements

- CPU: Intel Pentium 4 2.0 GHz processor and above
- 128 MB RAM or above (256 MB RAM recommended)
- One free USB port for 2, 4, 8, 12, 16, 25 versions.

- Specifications are subject to change without notice.

P/T/Z camera control

Allows you to adjust the position of your PTZ camera. Simply click on arrow key to control the camera.

Remote viewing

- Supports ActiveX and Java applets
- Remote Video playback by Windows Media Player.
- Control network PTZ camera through the built-in web server.
- Supports zoom to 150%, 200% and full screen.

Image enhancement

- Rotate the image 180 degree.
- Adjust brightness and contrast

Supports dual monitor

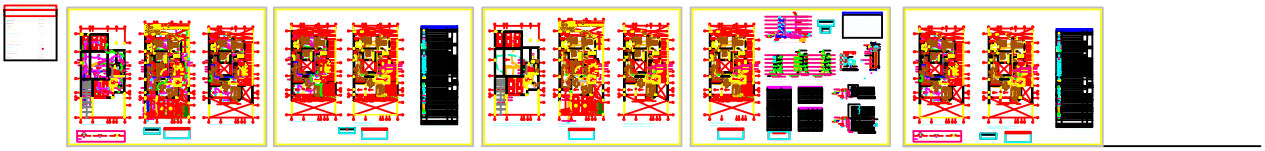
Reference performance data:

- CPU: Intel Pentium 4 3.0 GHz with HT
- OS: Windows XP
- Memory: 1 GB
- Display card: 128M AGP, 32 bits color mode
- Network: 100Mb/sec
- Camera : MJPEG based camera
- Max recording and display frame rate: 120 fps at 320x240 resolution and compressed with Windows Media™ Video 7
- Max recording and display frame rate: 200 fps at 320x240 resolution and compressed with Webcam WVC1

Note: actual performance highly depends on camera hardware, usage and various factors.

Webcam Corp.
100 Menlo Park, Suite 206,
Edison, NJ 08837,
U.S.A

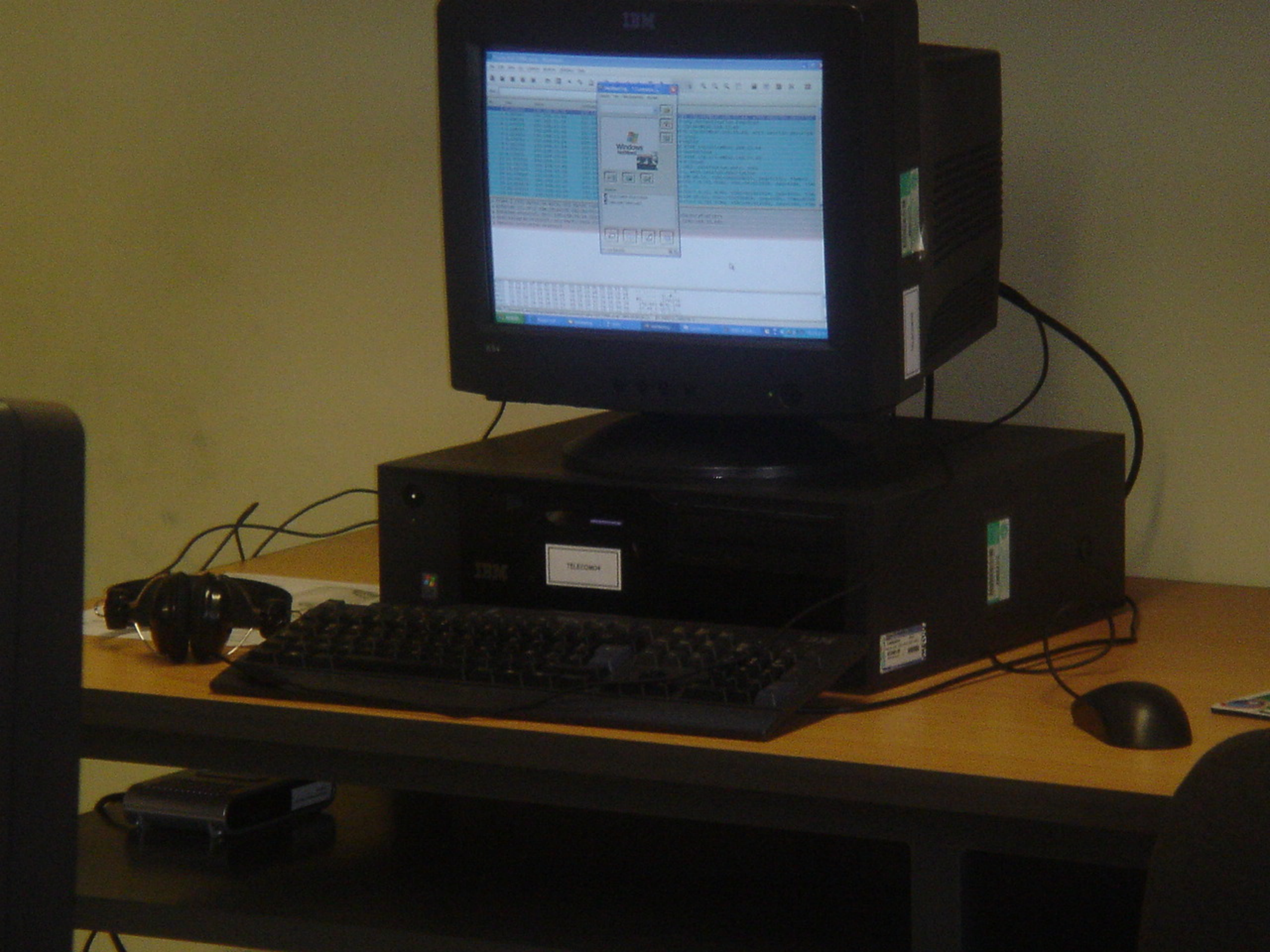
Copyright © 2006 Webcam Corp. All Rights Reserved.
All trademarks are owned by respective company.

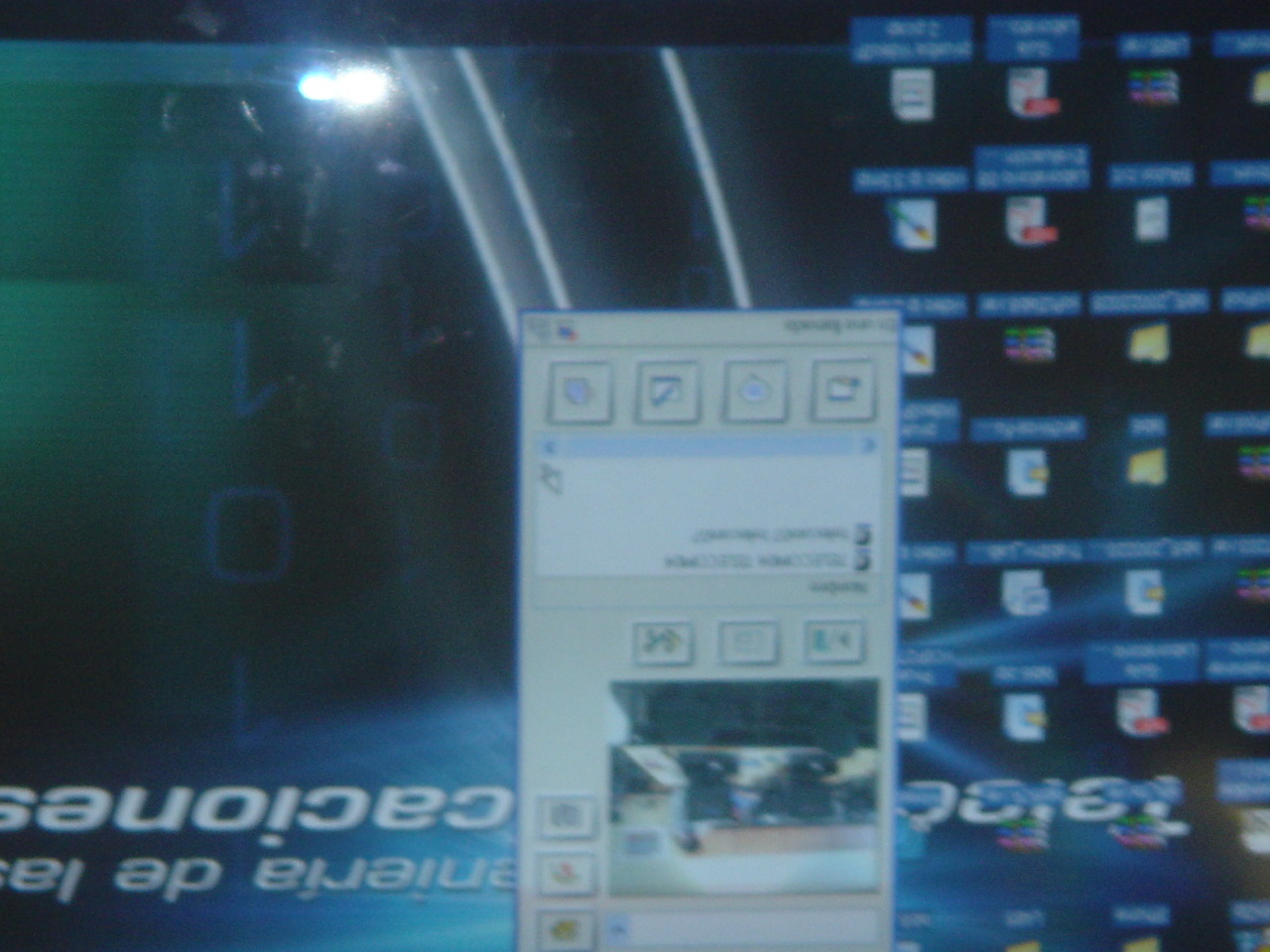



IBM
E54
IBM
TELECOM04
IBM


IBM
E54
WIRESHA
WinPcap
AirPcap
Source code
Verifying Downloads
IBM
YELECOM07
IBM


IBM
E54





May 2006

Digital Home Specification

White-paper

About this Document

Name/ Number of Functionality	
Author(s)	Corinex Communications Corp., Design of Systems on Silicon DS2
Technical Reviewer(s)	Ambient Corporation, Toyo networks, Sumitomo, Toshiba, ST&T, ILEVO
Editor(s)	Serafin Arroyo
Version Number	1.0
Last Updated	May 24th, 2006
Authorization	UPA Board of Directors
Notes	

Table of Contents

1. Executive Summary

The Universal Powerline Association (UPA) is an industry group formed with the objective of creating specifications for coexistence and interoperability of different broadband powerline technologies. The UPA has a universal scope, and its specifications are focused on both access and in-home applications, including worldwide coverage and considering requirements from manufacturers, service providers and all parts related to the PLC world.

On March 2005, UPA announced an initiative for the creation of a Digital Home Standard (DHS). The purpose of UPA DHS is to provide a complete specification for silicon vendors for designing integrated circuits for voice, video and data distribution using power lines.

This white paper provides an overview of UPA DHS specification v1.0, which was approved by UPA in February 2006, and covers the key areas of the PHY and MAC layers as well as descriptions of the higher layers.

The main features of UPA DHS technology are:

- 1536 carrier-OFDM modulation;
- adaptive bitloading, with physical layer data rate of 200 Mbps
- collision-free and flexible TDMA MAC;
- master/slave control architecture;
- peer-to-peer data transmission architecture;
- two operational bandwidth modes (normal mode and coexistence mode);
- physical spectral efficiency up to 8 bits/sec/Hz.;
- flexible PSD mask allowing frequency band notching dynamically and remotely;
- technology independent coexistence layer to allow coexistence between Access/In-home, In-home/In-home and future systems;
- 3DES encryption;
- advanced QoS with 8 priority levels;
- data isolation between neighbouring networks;
- compatible with the Open PLC European Research Alliance (OPERA).

2. About UPA

2.1 Mission

The Universal Powerline Association (UPA) [http://www.upaplc.org/] aligns industry leaders in the global Power Line Communications (PLC) market and covers both access and in-home PLC technology to ensure a level playing field for the deployment of interoperable and coexisting PLC products to the benefit of consumers worldwide. UPA members share a vision of openness and a federated PLC world to harmonize and share standards and regulations globally.

2.2 Objective

The UPA aims to act as a catalyst for the growth of PLC technology by delivering UPA certified products that comply with agreed specifications. The UPA focuses on time-to-market, guaranteeing high performance and maximizing the usage of the spectrum for both access and in-home audiovisual and data networking PLC applications to the benefit of all players in the PLC value chain.

2.3 UPA Coexistence Standard

On June 2005, UPA published a document that specified a protocol for ensuring coexistence of several powerline technologies sharing the same medium. This document, which is available from specs@upaplc.org, describes an advanced protocol for dynamic sharing of the channel using both dynamic frequency-division and time-division mechanisms. The specification supports simultaneous operation of one access network and up to three different in-home networks.

2.4 UPA DHS

On March 2005, UPA announced its initiative to create a Digital Home Standard (DHS). The purpose of DHS is to provide a complete specification for silicon vendors for designing integrated circuits for voice, video and data distribution using power lines.

Continuing the effort that had already been made by the Open PLC European Research Alliance (OPERA) [http://www.ist-opera.org/] project that focused on the specification of Broadband Access, UPA has undertaken the task of developing the PHY and MAC for in-home applications, achieving compatibility between Access and In-home networks.

2.5 UPA certification

The UPA Certification Working Group celebrated an UPA plugtest during first quarter 2006 as the first step on a path to the future certification of UPA products. This event was focused on digital home products, testing against the UPA DHS version 1.0 and UPA Coexistence Specification.

Several products from different manufacturers passed the tests, and were labelled as “UPA Plug Tested”, ensuring performance, coexistence and interoperability.

In the next certification event, products certified by the UPA will bear the UPA compliance label, a customers' guarantee of reliability, on all UPA certified power line products and applications.

2.6 UPA DHS Key Features

UPA DHS specification will include all the necessary features required for high-speed audio/video distribution inside the home. The specification has been designed with two different scenarios in mind: managed and unmanaged in-home powerline networks:

- 1536 carrier-OFDM modulation;
- adaptive bitloading, with physical layer data rate of 200 Mbps;
- collision-free and flexible TDMA MAC;
- master/slave control architecture;
- peer-to-peer data transmission architecture;
- two operational bandwidth modes (normal mode and coexistence mode);
- physical spectral efficiency up to 8 bits/sec/Hz.;
- flexible PSD mask allowing frequency band notching dynamically and remotely;
- technology independent coexistence layer to allow coexistence between Access/In-home, In-home/In-home and future systems;
- 3DES encryption;
- advanced QoS with 8 priority levels;
- data isolation between neighbouring networks;
- compatible with the Open PLC European Research Alliance (OPERA).

3. Applications of indoors powerline technology

Several applications take advantage of powerline technology. This whitepaper focuses on two of them:

- high-speed Audio/Video (AV) Home Networking;
- Triple-Play Services Distribution.

3.1 High-speed AV Home Networking

Applications like high-definition video streaming between Media Center computers, Set-Top-Boxes, Personal Video Recorders, etc require performance levels that are currently only achievable with UPA DHS PLC technology. These devices share two key needs: very high speed requirements (20-40 Mbps) and no mobility advantage (TVs and STBs cannot move around the home).

In this document, these applications are grouped under the name of “High-speed AV (Audio/Video) Home Networking”.

Because it is not attenuated by concrete/brick/metal walls, UPA DHS technology is the only technology that provides whole-house coverage solution for High-speed AV (Audio/Video) Home Networking. UPA DHS’ transmission characteristics are very stable and predictable, thus improving the end-user experience. Two examples of application are shown in the figures below.

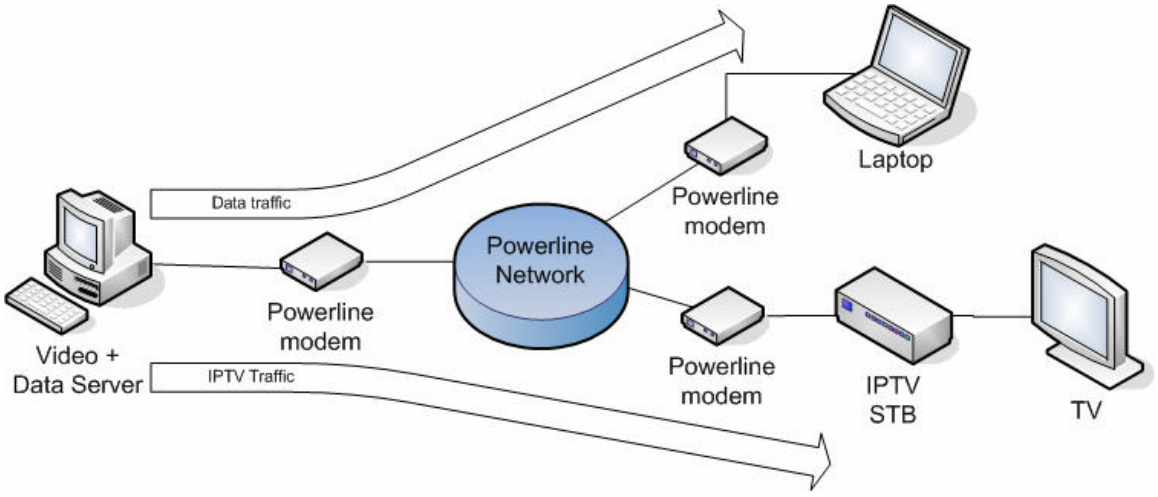


Figure 1 Video distribution In-home, internal server, no external connection.

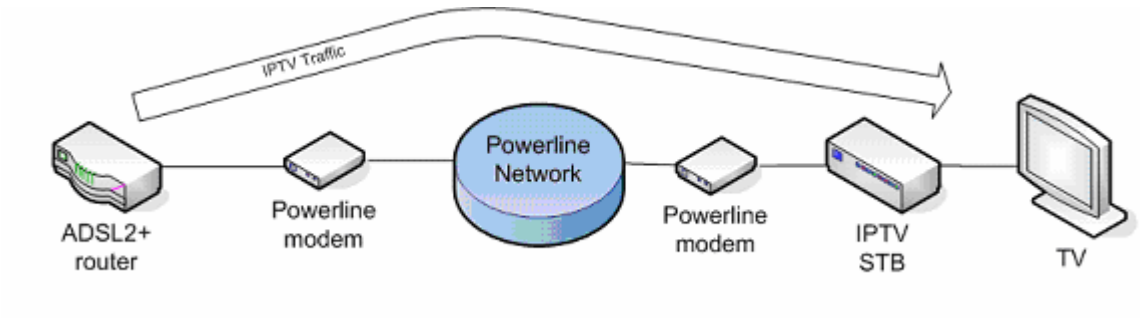


Figure 2 Video distribution In-home, external signal from other technologies.

3.2 Triple-Play Services Distribution

Competitive pressures in the broadband market are forcing telecommunications service providers to offer more complete services. One key trend is the provision of video services by DSL providers, who are competing with cable companies to provide "Triple Play" services consisting of video, voice and data, using only the telephone twisted pair.

One of the most important barriers to the provision of these services is the fact that the entry points of the twisted pair into the home are seldom close to the television. This leaves the home owner and the service provider with the problem of bridging the distance between the television with the phone socket, or more specifically between the set top box and the residential gateway. This connection poses a problem for operators because potential customers are not willing to add new cabling in their home, and because the installation of customer premises wiring represents an expensive contribution to the operator's costs.

Installing fixed wiring to distribute digital video around the home is not only expensive for operators and unappealing for subscribers, but also restricts where in the home subscribers can use services to those where new wiring has been installed. With UPA DHS technology, it is possible to enjoy Triple Play services anywhere in the home, or deploy multiple services, for example having one set top box for video in the living room and another in the bedroom.

In many cases, subscribers are unwilling to upgrade to Triple Play services either because of the inconvenience of home wiring or for aesthetic reasons. Consumer resistance to new home wiring places a severe limitation on the available market for Triple Play services. UPA DHS is solution that does not require new wiring. This means that a complete home installation can be made without drilling a single hole or extending any structured cabling.

Many operators are currently looking at ways to make their offer more attractive by adding value to their broadband services. UPA DHS technology allows operators to provide subscribers with a complete home media network, allowing photos, home-movies and other content stored on a home PC, as well as IPTV and video-on-demand services, to be viewed on a TV set anywhere in the home.

3.2.1 Using broadband powerline technology over other media

Although UPA DHS technology was designed for usage over powerlines, this does not preclude its usage over different "metallic" media.

The UPA DHS high-frequency signal is transmitted independently of whether there is power in the line or not (a coupling unit isolates 50-60 Hz power from the transmitter/receiver).

Several companies have developed products that make use of UPA DHS' PHY and MAC over non-powerline media, mainly coaxial cables. This application is especially interesting for two reasons:

- in some geographical areas (mainly the North American residential market) there is a large installed base of in-home coaxial cables for TV distribution. For obvious reasons (shielding, controlled impedance, fewer devices connected), the coaxial cable is a much better transmission media than power lines. Any UPA DHS will operate at nominal speed (200 Mbps) almost 99.9% of the time when coaxial cables are used for transmission;
- device manufacturers can develop hybrid powerline/coaxial devices that make use of coaxial cable when it is available in a specific location, but use power lines when coaxial cable is not available (see Figure 3 for a sample block diagram of a hybrid device).

The possibility of deploying hybrid coaxial/powerline networks (see Figure 3) represents a huge advantage of UPA DHS technology over any other alternative.

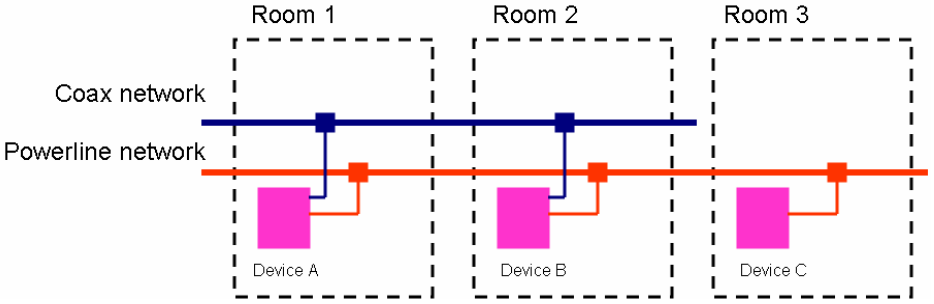


Figure 3 Block diagram of Hybrid coaxial/powerline network

Devices A and B transmit their high-frequency signal over both coaxial cable and power lines simultaneously. When Device B receives the signal from A, it will probably receive a much stronger signal from the coaxial cable than from the power line. As propagation over coaxial cable is very good, the signal-to-noise ratio will be very high, thus guaranteeing transmission data rates of 200 Mbps in 99.99% of situations. On the other hand, when Device B receives the signal from C, it will only receive signal from the power line, and no signal from the coaxial cable. In this case, performance will be dependent on the signal-to-noise ratio in the power lines, which will typically provide data rates in the 100-200 Mbps range.

4. UPA DHS Technology Specification

4.1 Layered Reference Model

The UPA DHS specification uses a Layered Reference Model, shown in Figure 4, to describe the different levels of its protocol stack. The Layers are defined as:

- PHY Layer defines the physical data transmission format on the medium;
- MAC Layer defines how different nodes are allocated transmission opportunities;
- LLC Layer defines how error free communication is achieved between nodes;
- Convergence Layer defines how standard protocols such as 802.3 Ethernet are mapped to the UPA DHS protocol and how the data encapsulation is made;
- Layer Management defines how each of the layers is configured and adapted to changing network conditions.

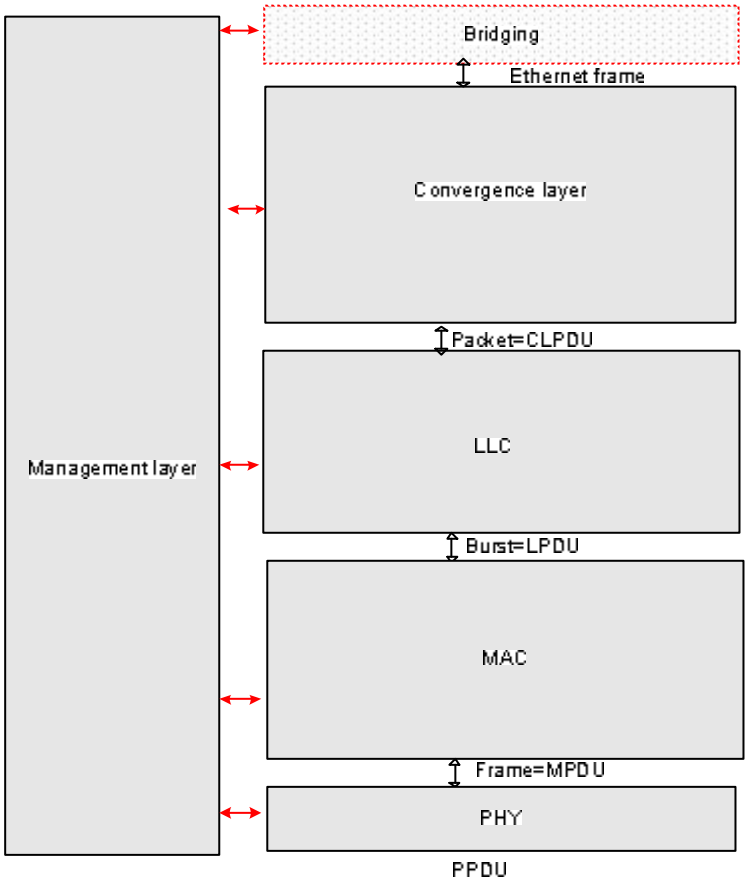


Figure 4 UPA DHS Layered Reference Model

In addition to these layers, mechanisms are provided for Encryption and Coexistence.

4.2 Physical Layer

The Physical Layer is based on Orthogonal Frequency Division Multiplexing (OFDM). OFDM has been chosen as the modulation technique because of its inherent adaptability in the presence of frequency selective channels, its resilience to jammer signals, its robustness to impulsive noise and its capacity of achieving high spectral efficiencies.

Concatenation of four-dimensional trellis Reed-Solomon forward error correction, specially tuned to cope with the very special powerline channel impairments, assures high performance in the worst case.

4.2.1 Bandwidth Capabilities

Most of the features that allow 200 Mbps data transmission reside in the Physical layer. The UPA DHS PHY features configurable frequency bands, with bandwidths of 20 or 30 MHz.

This bandwidth flexibility has been included in the system in order to support Frequency-Division (FD) coexistence mechanisms between UPA DHS in-home networks and OPERA access networks.

In its 30 MHz mode, UPA DHS systems provide a maximum physical throughput of exactly 240 Mbps, with information rates up to 158 Mbps.

4.2.2 Notching Capabilities

Broadband powerline employs frequencies that in some particular locations may be licensed to different radio services, like amateur radio, etc. Legal regulation in different countries may impose limitations on which frequencies can be used by powerline communications and which frequencies must be avoided (exclusion bands). Regulations are typically country-specific, so powerline communications products may be forced to use different frequencies depending on the country were they are used.

Spectral notching is a technique used for avoiding exclusion bands. Notches are created by turning off those OFDM sub-carriers that fall in the exclusion bands, thus eliminating the amount of energy transmitted in those bands.

UPA DHS uses windowed-OFDM modulation that allows programmable notches with a depth of up to 40 dBs, with a negligible loss of performance.

UPA DHS technology allows device manufacturers to create customised notch configuration for each country, without requiring any hardware changes.

Figure 5 shows an example of the type of arbitrary Power Spectral Mask that the UPA DHS system can achieve.

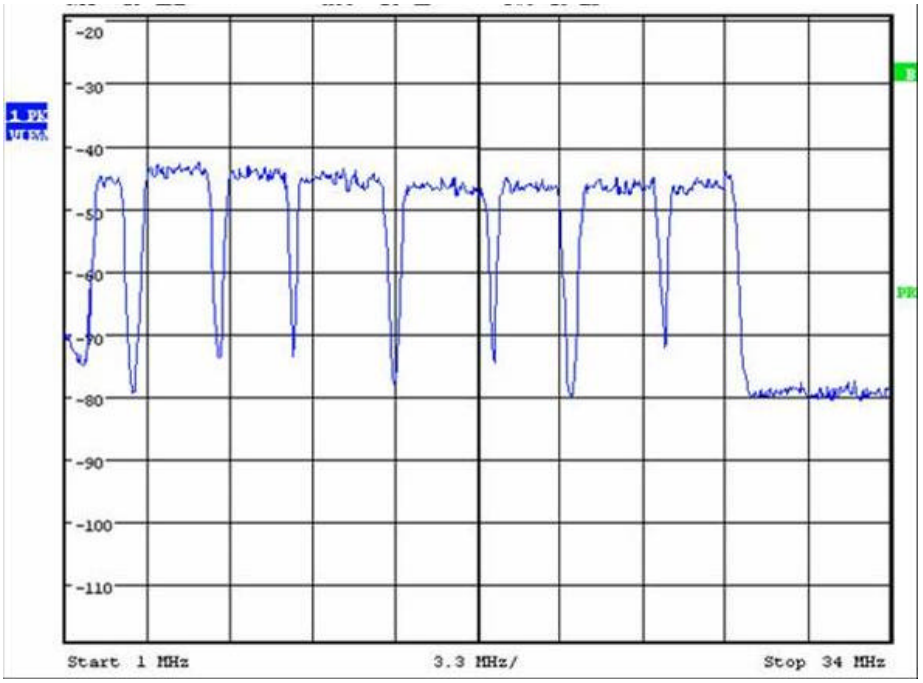


Figure 5 Example of a Power Spectral Mask with arbitrary nocthes

Additionally, in the case of a change in regulation, products that are already deployed in the field can be upgraded easily in order to guarantee compliance, avoiding costly product replacements.

4.2.3 The UPA DHS OFDM Symbol

The OFDM symbol uses 1536 sub carriers, with modulation densities from 2 to 10 bits per sub carrier applied independently to each of the sub carriers. The reason for choosing this high number of sub carriers is two-fold:

- achieves high accuracy when estimating channel Signal-to-Noise Ratio and adapting the modulation of each carrier accordingly;
- achieves very narrow notches, with small impact in neighbouring sub carriers.

4.2.4 Adaptive Bit-loading

Modulation parameters for each transmitter/receiver pair are adapted in real-time depending on channel quality parameters for each carrier. Figure 6 depicts an example of this functionality. The Signal-to-Noise Ratio (SNR, in black) is measured for each carrier and the optimum modulation (Bits-per-Carrier, BPC, in blue) is chosen, with the objective of achieving the maximum transmission speed while maintaining the desired Bit Error Rate (BER).

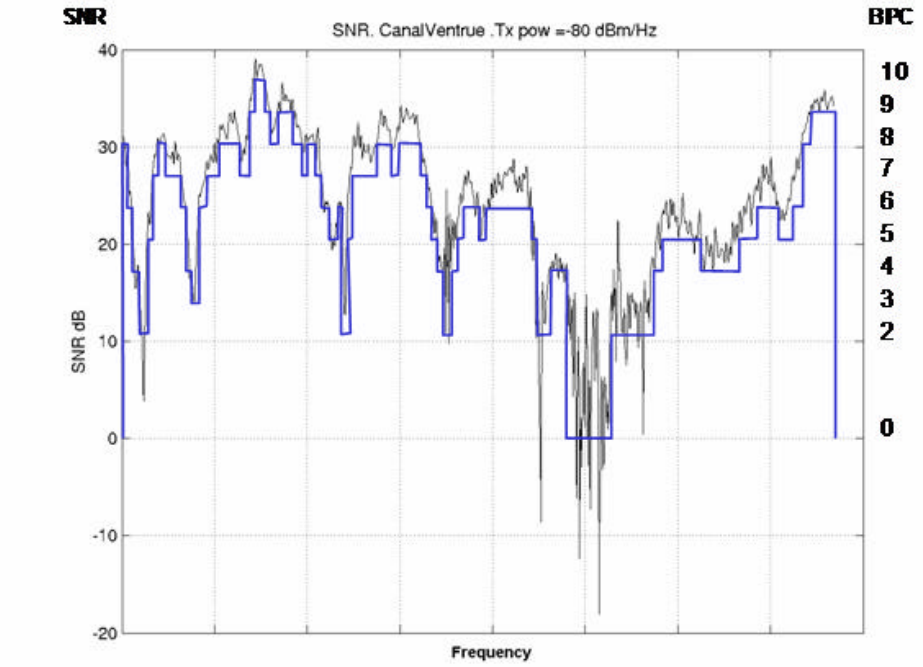


Figure 6 Sample "Signal-to-Noise Ratio" (SNR) and bitloading map for a sample powerline channel

4.2.5 Forward Error Correction

The PHY provides two different levels of reliability represented as two different bit streams.

The most reliable mode, known as HURTO, is reserved for information such as frame headers and control information that is critical for the correct operation of the system. In order to achieve such a high reliability, special Forward Error Correction, interleaving and frequency redundancy (depicted in the diagram as HURTO mapping) are used, jointly with a very robust modulation, to ensure the correct demodulation in the reception side, even in the worst channel conditions.

Normal data information can be transmitted using adaptive mapping to match tightly the channel characteristics in order to obtain the highest possible throughput for each case. This adaptation includes not only the bits per carrier that can be used for a certain desired bit error rate, but also a dynamic Reed-Solomon configuration for each of the transmitted packet, depending on the channel state.

Once the OFDM symbol has been constructed, a four-dimensional Trellis Coded modulation is performed, increasing the reliability of the transmitted signal.

4.2.6 Symbol Transmission

After each carrier has been independently modulated, the whole frequency-domain signal is processed by an IFFT block. After this block, the cyclic prefix is added, and the transmission window is applied.

The final block represents the Analog Front End and the coupling unit to inject the final OFDM signal into the power line channel

4.3 Medium Access Control (MAC) Layer

4.3.1 Advanced Dynamic Time Division

UPA DHS technology uses an Advanced Dynamic Time Division (ADTDM) MAC that is optimized for Audio/Video distribution scenarios, where high performance, stringent bandwidth reservation, strict traffic prioritization and QoS are a must. The ADTDM MAC provides collision-free access for the channel to all the nodes in the power line network according to different service priorities. These can be adjusted to suit different types of applications, ranging from data, VoIP, Video on demand, etc.

The arbitration of the channel access is controlled by a centralized entity in the network in a way that adapts to the different topology possibilities, ensuring that all transmissions are compliant with the defined QoS profile. All nodes in the network are considered in the sharing mechanism, including hidden nodes, ensuring that any node in the network could have access to the channel if required.

UPA DHS MAC also provides flexibility, including different scheduling transmission formats depending on impulsive noise and channel impedance.

4.3.2 MAC Network Entities

At the MAC level, any UPA DHS device can play one of the following roles:

- Access Point: Access Point (also known as “master”) devices control the access to the channel of the other devices, and make sure that resources are allocated in a way that satisfies QoS requirements. Access Points are responsible for generating the channel “token” and distributing this token to the rest of devices in the network. The master will be also responsible to assign resources only to active nodes, avoiding loss of performance and ensuring maximum throughput at all times;
- Repeater: a repeater is a device that receives packets addressed to another device and re-transmits them;
- End-Points: an end-point (also known as “slave”) is a device that is not an Access Point or a Repeater.

At boot time, every device is an End Point. Access Points and Repeaters are elected automatically once the network starts operation.

UPA DHS provides mechanisms to ensure that:

- there is always one and only one Access Point in a given UPA DHS network;
- every device is connected to the network either directly through the Access Point or indirectly through a repeater.

4.3.3 Channel Arbitration and Tokens

At any given time, the Access Point is responsible for deciding:

- the optimum set of parameters for the operation of the MAC protocol depending on the number of devices in the network, the type of traffic that is being transmitted, etc;
- how much channel time is given to each device.

A graphical example of the operation of the MAC protocol is given in Figure 7 and Figure 8. Figure 7 depicts a sample network with three nodes (one Access Point and two End Points). All three nodes have direct visibility of each other, so they can communicate directly. The time evolution of a possible communication scenario is shown in Figure 8:

1. Node A (the Access Point) starts the communication process:
    a. It transmits a short control message, announcing that the following powerline frames come from Node A. This short control message also includes additional PHY-level information (required for the receivers to configure the right reception gain and the OFDM demodulators).
    b. It then transmits a data burst addressed to Node B, followed by another burst of data addressed to Node C.
    c. Finally, it sends another control message yielding the channel control to Node B. This control message includes information about the maximum time that node B can make use of the channel.
2. After receiving the token from Node A, Node B can start transmission over the power line channel:
    a. As before, it transmits a short control message, announcing that the following powerline frames come from Node B.
    b. It then transmits a data burst addressed to Node A, followed by another burst of data addressed to Node C.
    c. Finally, it returns the channel control to node A (the Access Point).
3. After having the token returned from B, A is now the “channel owner” again:
    a. As before, it transmits a short control message, announcing that the following powerline frames come from Node A.
    b. It then transmits a data burst addressed to Node C.
    c. Finally, it sends another control message yielding the channel control to Node C.
4. After receiving the token from Node A, Node C can start transmission over the power line channel. In this specific case, Node C does not have any data to transmit, so it will return the token immediately to Node A.
    a. Node C transmits a short control message, announcing that the following powerline frames come from Node C.
    b. It immediately returns the channel control to node A (the Access Point).

5. Now Node A is again the channel owner, and the cycle can start over again.

This dynamic MAC mechanism has several advantages:

- only one node is transmitting at any given time;
- collisions are completely avoided;
- the Access Point has total control over how much time each node has control of the channel;
- there is a deterministic upper bound on how much time it will take for a given node to gain access to the channel (bounded channel access latency), which is critical for AV applications;
- negligible bandwidth is wasted if a given node does not have any data to transmit, as channel control can be returned immediately to the Access Point.

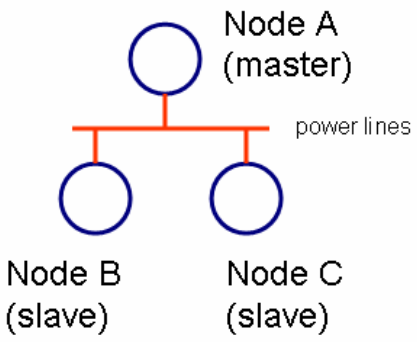


Figure 7 Sample network with complete visibility

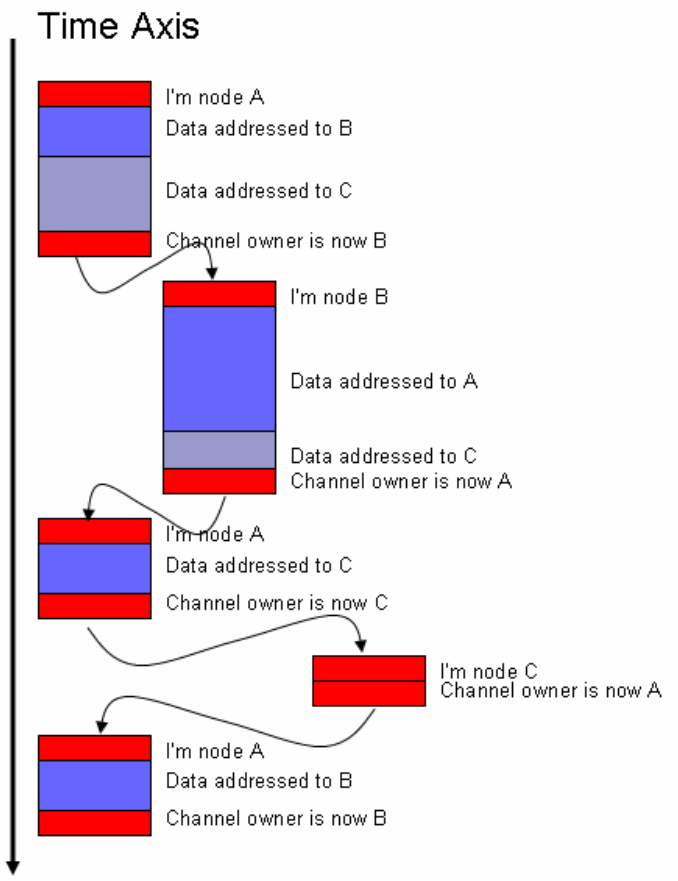


Figure 8: Time diagram of control and data messages transmitted over powerline

This token-passing scheme is very powerful and flexible, and it can be extended to networks were not all nodes can “see each other” directly (partial or incomplete

visibility). In these situations, one device can act as a repeater for both data and control messages.

Figure 9 shows a network with “incomplete visibility” (Node A and Node C cannot communicate directly). Figure 10 shows the time diagram of a sample communication scenario in such a network, in which Node B (repeater) must play the role of a bridge between Node A and Node C:

1. Node A (the Access Point) starts the communication process:
    a. It transmits a short control message, announcing that the following powerline frames come from Node A.
    b. It then transmits a data burst addressed to Node B. After this, it sends another burst of data which is addressed to Node C. This mechanism allows Node A to transmit data to Node C using Node B as an intermediate repeater.
    c. Finally, it sends another control message yielding the channel control to Node B.
2. After receiving the token from Node A, Node B can start transmission over the power line channel:
    a. It transmits a short control message, announcing that the following powerline frames come from Node B.
    b. It then transmits a data burst addressed to Node A, followed by another burst of data addressed to Node C (part of the data information in this burst comes from Node A, and part may come from Node B itself).
    c. Finally, it forwards the channel control to node C.
3. After receiving the token from Node B, Node C can start transmission over the power line channel:
    a. It transmits a short control message, announcing that the following powerline frames come from Node C.
    b. Node C sends a burst of data which is addressed to Node A
    c. Finally, it returns the channel control to node B (the Repeater).
4. After receiving the token back from Node C, Node B can start transmission over the power line channel:
    a. It transmits a short control message, announcing that the following powerline frames come from Node B.
    b. Node B sends a burst of data which is addressed to Node A (with information originated at C).
    c. Finally, it returns the channel control to node A.
5. Now Node A is again the channel owner, and the cycle can start over again.

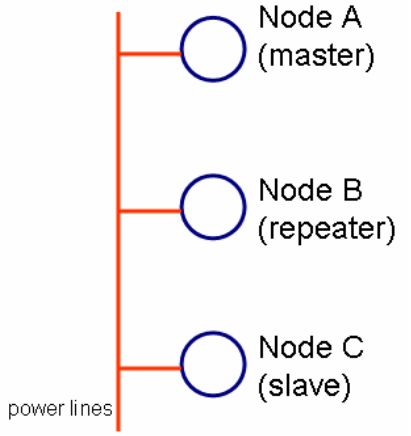


Figure 9 Sample network with incomplete visibility (Node A and Node C cannot communicate directly)

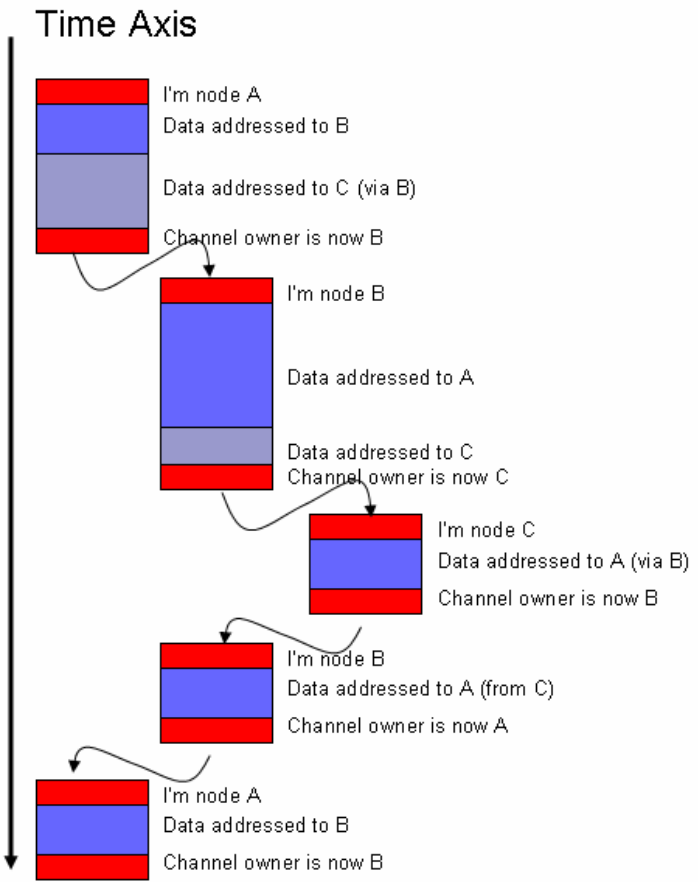


Figure 10 Time diagram of control and data messages transmitted over powerline

The MAC protocol includes a whole set of auxiliary mechanisms (not discussed in this whitepaper) to guarantee the correct operation of the protocol. There are sub-protocols for:

- handling new nodes joining the network;
- automatic discovery of the network topology, allowing nodes with incomplete visibility to communicate with other nodes out their reach, making use of intermediate repeaters;
- optimization of communication topology, ensuring maximum performance and throughput between two nodes of the network, using direct communication or allowing repetition mechanism;
- learning which hosts/devices are reachable via each powerline device, based on an 802.1d learning model;
- handling nodes being disconnected from the network;

- token recovery in case of having one node disconnected while it was the channel owner;
- new Access Point selection in case of having the Access Point disconnected from the network.

4.3.4 Types of MAC Frames

There are three main types of frames:

- *data frames* contain PLC bursts as payload. UPA DHS nodes may include PLC bursts addressed to several destinations in the same frame in order to maximize efficiency;
- *channel estimation frames* are sent periodically by every node so that communicating nodes can estimate their channel and adjust the number of bits per carrier suited for that channel;
- *access frames* are used by Access Point and Repeater nodes to invite new nodes to join the power line network. Upon reception of an access frame, new nodes contend for access to the channel using a back-off algorithm. After contention is won, both nodes (the Access Point or Repeater that sent the Access frame and the new node joining the network) initiate the connection (setting up QoS parameters, negotiation of modulation parameters, etc).

4.3.5 Burst Format

Each frame is made up of a series of Bursts, which contain data transmissions between individual logical links in the system. Within each burst, a burst header indicates the logical link identifying the receiving and transmitting nodes, followed by the payload data formatted as a series of Codewords.

4.3.6 Codeword Format

Codewords are transmission sequences consisting of a pure Data Payload followed by a number of bits of Redundancy. Codewords are formed using a variable-rate Reed-Solomon block encoder.

4.4 Link Layer Control (LLC) Layer

The LLC Layer in UPA DHS ensures the error free transmission of data between pairs of power line nodes. This is done in transmission by encoding the Data Payload provided by the Convergence Layer into sequences of Codewords. These Codeword Sequences, called Bursts, are transmitted between node pairs using an optional acknowledgement scheme.

4.4.1 Burst structure

A burst is composed of a Burst Header delimiter followed by a data payload including one or several fragmented and/or completed packets. A Burst Header delimiter without any following data payload is used to send ACK when there are no data to be sent.

Figure 11 shows how the mapping/encapsulation of an Ethernet 802.3 frame is performed in UPA DHS, in the case that a packet has to be fragmented in several bursts.

1. The packet is split to fill the payload sections of the codewords, to which Reed-Solomon redundancy data will be added.
2. A header is added to each codeword that carries information required for later merging all codewords together into the original Ethernet frame.
3. Groups of codewords are concatenated into a burst.

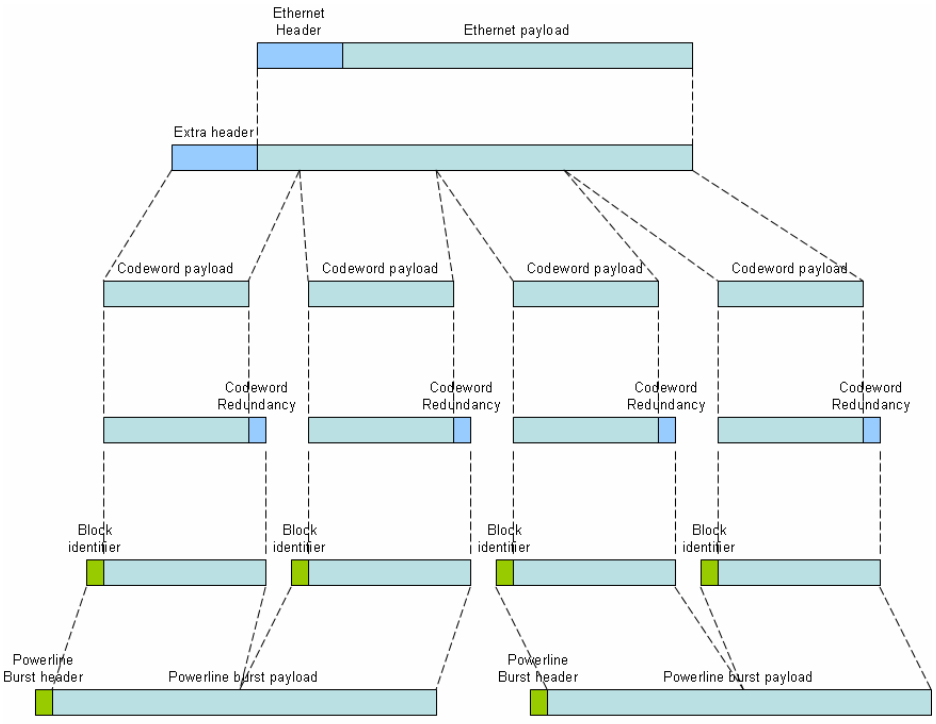


Figure 11 Generic Mapping of an Ethernet frame into PLC-level bursts

4.4.2 Burst Acknowledgement Scheme

UPA DHS uses a “Sliding Window” protocol for managing reliable end-to-end transmission of data frames. Each burst has a “burst identification number”. During normal system operation, the receiver sends an acknowledgement (ACK) of the last “burst identification number” correctly received.

The ACK protocol, shown in Figure 12, works as follows:

1. firstly, the “left node” transmits a series of bursts (with identification numbers 1, 2 and 3) to the “right node”. The “left node” keeps those bursts in the transmission buffer, in case they need to be retransmitted;
2. due to channel noise, burst #3 is corrupted. Only bursts 1 and 2 are correctly received;
3. the “right node” nexts sends a control message to the “left node”, acknowledging that the last successfully received burst was burst #2;
4. the “left node” then removes bursts #1 and #2 from the transmission buffer and retransmits burst #3;
5. this time, burst #3 is correctly received, so the “right node” sends a new control message acknowledging that burst #3 has been correctly received;
6. after receiving the ACK, the “left node” removes burst #3 from the transmission buffer.

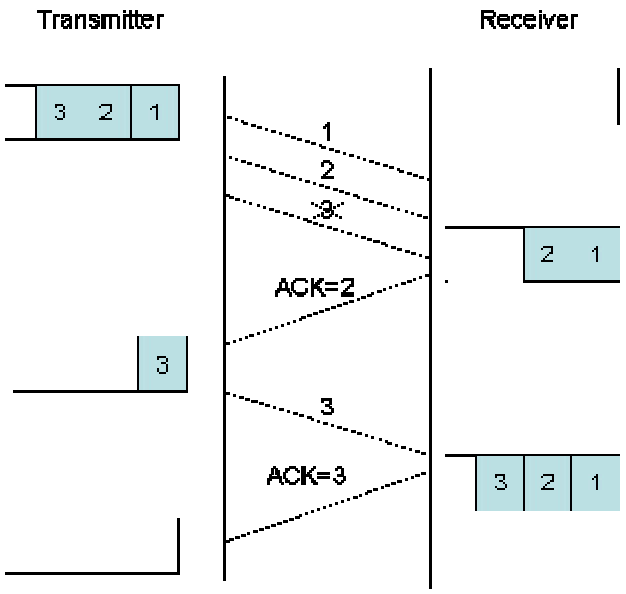


Figure 12 Burst Acknowledgement Scheme

This ACK protocol provides several advantages:

- a group of several bursts can be sent to a given node, without waiting for each specific burst to be acknowledged. This allows for longer transmission frames, which increases efficiency;
- packet losses at the power line level are hidden from the application layer, which only perceives an “Ethernet-like” zero-loss channel.

4.5 Convergence Layer

The function of the Convergence Layer is to encapsulate packets coming from external applications (typically 802.3 Ethernet frames, although other encapsulations could be defined) before passing them to the LLC for transmission.

The Ethernet frame is encapsulated into a powerline packet, which is basically formed from the original Ethernet frame plus a powerline header that includes information such as powerline-level priority, OVLAN (an extension of VLAN), broadcast control information, etc.

4.5.1 Virtual LAN Management

Virtual LAN (VLAN) management allows an UPA DHS network to be separated into different independent isolated sub-networks that can be managed independently.

In addition, the standard 802.1q VLAN, is extended with additional OVLAN tagging capabilities, providing an additional tagging field that can be used independently of the standard 802.1q VLAN tags.

4.6 Layer Management

4.6.1 Control protocols

UPA DHS defines a specific format for exchanging control information between nodes that uses SNAP encapsulation in regular Ethernet frames. The main control protocols are:

- adaptive bit-loading protocol used to exchange bit-loading tables to adapt the transmission characteristics to the channel;
- access protocol used to accept new nodes in the network;
- port solver protocol used to exchange addressing information between nodes;
- cluster discovery protocol used to discover nodes that can transmit simultaneously without interfering each other, so that spatial reuse can be achieved;
- connection admission protocol to reserve resources for data flows;
- automatic management of crosstalks between not synchronized systems used when two independent networks interfere each other.

4.6.2 Spanning Tree Protocols

Spanning Tree protocols are fully configurable by the operator, including the improved Rapid Spanning Tree algorithm specially developed and optimized to match powerline network topology particularities. This advanced algorithm takes into account not only the structure at network level, but also PHY layer parameter to obtain the best networks paths in the network.

4.7 Quality of Service (QoS)

High-speed AV Home Networking or Triple Play Services distribution using power lines are very demanding applications, for one simple reason: they must provide huge amounts of bandwidth (in the 20-40 Mbps range) with very high stability and QoS, at a very large percentage (99%) of outlets in the home.

The system must provide smooth video delivery even under difficult conditions like intermittent noise, interference from neighbouring powerline networks or a network with simultaneous low priority data traffic.

UPA DHS implements capabilities to transport traffic with different service requirements and to handle each traffic type with the appropriate Quality-of-Service (QoS) level.

UPA DHS includes several mechanisms to enforce QoS for powerline applications:

- traffic classification;
- Centralized Bandwidth management.

4.7.1 Traffic classification

In order to handle different services and applications adequately, UPA DHS devices identify the class of service to which each specific Ethernet frame belongs. Although the way to do this is implementation-specific, the recommended mechanism is using a "Service Classifier" module. The Service Classifier module is responsible for determining the priority level of each frame according to a set of established rules.

The Service Classifier entity, shown in Figure 13, works as follows:

- incoming frames are inspected, one by one, looking for patterns that the Service Classifier can use for determining priorities;
- once the priority has been determined, a "tag" is added to the frame, so that it can later be identified by other entities of the UPA DHS specification;
- the set of programmable rules are typically of the following type:
    - Rule 1: If the byte in offset AA of the Ethernet frame is BB, then the priority of the packet is CC;
    - Rule 2: If the byte in offset DD of the Ethernet frame is EE, then the priority of the packet is FF, and so on.
- typical default rules for the Service Classifier could be: decide priorities according to bits in 802.1p field, or according to bits in IPv4 TOS field, etc.

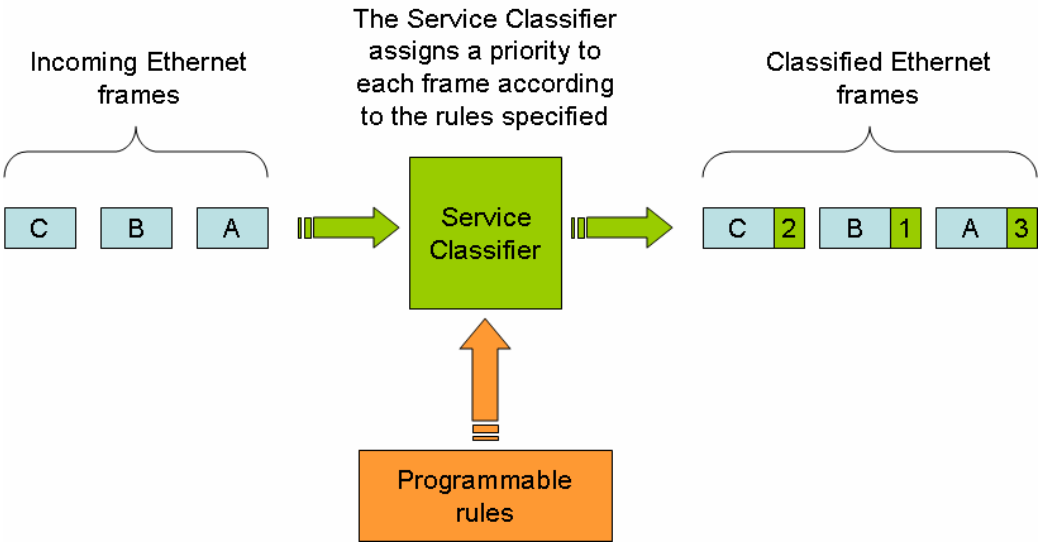


Figure 13 Service Classifier Module

4.7.2 Centralized bandwidth management

One of the advantages of having a master/slave dynamic ATDMA MAC is that the system can easily support very sophisticated QoS algorithms, including bandwidth reservation, latency guarantees, etc.

In UPA DHS MAC, the Access Point device allocates channel access time to each device in a centralized manner, having complete information about the network, including the bandwidth requirements of each application, the available data rate between any pair of devices, etc.

The UPA DHS specification is very flexible, in the sense that it allows device manufacturers to implement very flexible QoS algorithms, specifically optimized for their application, while maintaining compatibility with UPA DHS baseline specification.

4.8 Security Mechanisms

UPA DHS implements two mechanisms to ensure privacy and security:

- isolation of logical networks, using the concept of “Network Identifier”;
- encryption of data communications, using a hybrid 3DES/DES encryption scheme.

Both mechanisms are independent and can be used either with or without the other.

4.8.1 Network Identifier and neighbouring networks

Two UPA DHS will only communicate (i.e. exchange data) if they have the same “Network Identifier” (Net-ID). Devices with different Net-IDs will still “see each other”, and they will peacefully share channel bandwidth.

The Network Identifier in UPA DHS is similar in functionality to the 802.11 Service Set Identifier (SSID).

In addition, Ethernet filtering is implemented, preventing:

- Ethernet frames from one customer leaking into a neighbouring customer (for security reasons);
- Ethernet frames from one powerline sub-network (for example, an LV cell) leaking into another powerline sub-network (for security reasons and in order to avoid the problem of bridge tables filling up with unnecessary MAC addresses).

4.8.2 3DES Encryption

UPA DHS specification includes a powerful security structure based on 168-bit Triple DES (3DES) encryption that guarantees the privacy of communications established between UPA DHS devices.

UPA DHS specifies that each device must support several encryption keys, thus having the possibility of communicating with different devices, using different encryption keys.

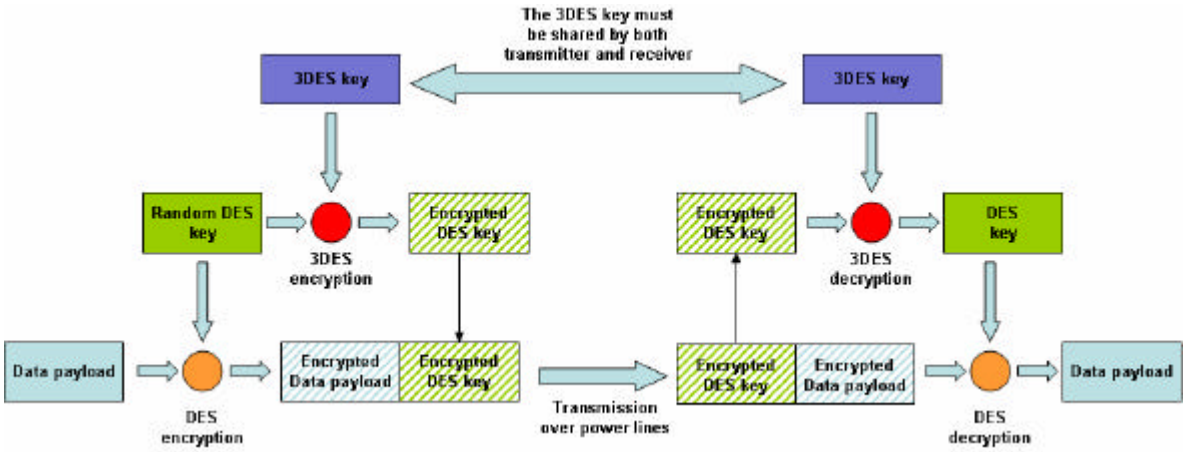


Figure 14 Hybrid DES/3DES encryption mechanism

UPA DHS encryption is based on a hybrid 3DES/DES encryption architecture. A diagram of this architecture is depicted in Figure 14. The encryption mechanism works as follows:

1. both transmitter and receiver have to agree on a common 3DES (168 bits) encryption key. This is achieved typically by having the end-user enter the same key in both devices using a configuration tool or any other mechanism;
2. once a new data frame needs to be transmitted, a new random DES (56 bits) encryption key is created;
3. the data frame is encrypted with the DES key;
4. the Random DES key is encrypted with the common 3DES encryption key, and appended to the encrypted data frame;
5. both the encrypted data frame and the encrypted DES key are transmitted through the powerline channel;

6. the receiver obtains the encrypted DES key and decrypts it using the common 3DES key;
7. the receiver uses the decrypted DES key for decrypting the encrypted data frame;
8. the receiver obtains the decrypted data frame.

The advantages of this system are:

- the 3DES key is never transmitted over the powerline channel;
- a new random DES key is generated for every new data frame, thus completely eliminating the risk of a potential eavesdropper guessing the DES key by doing a long term analysis of the transmitted data;
- the rather resource intensive process of performing 3DES encryption is only applied to the short DES key (56 bits), instead of being applied to the whole data frame (potentially several kilobytes);
- a relatively simple encryption process (DES encryption) is applied to the data frame, thus saving silicon area and computing power.

4.9 Coexistence Mechanisms

On June 2005, UPA published a document that specified a protocol for ensuring coexistence of several powerline technologies sharing the same medium. This document, which is available from specs@upaplc.org, describes an advanced protocol for dynamic sharing of the channel using both dynamic frequency-division and time-division mechanisms. The specification supports simultaneous operation of one access network and up to three different in-home networks.

References

[1] UPA - Digital Home Specifications (UPA DHS), v 1.0.

[2] UPA – Digital Home Specifications - Market Requirements Document, v 1.0.

[3] UPA, Powerline Communication Systems -Access/In-home & In-home/In-home coexistence mechanism - General specifications. v 1.0

[4] OPERA, IST-integrated project, D45, Specification of PLC System Requirements, v1.0

[5] OPERA, IST-integrated project, D59, Specification of PLC System, v1.0

[6] DSL Forum TR-094, Multi-Service Delivery Framework for Home Networks Services.

[7] Digital Living Network Alliance (DLNA), Overview and Vision, White Paper, June 2004

[8] OSGi Alliance, About the OSGi Service Platform, Technical Whitepaper, Revision 3.0, 12 July 2004

[9] ETSI TR 102 049 V1.1.1, PowerLine Telecommunications (PLT); Quality of Service (QoS) requirements for in-house systems