UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

"DISEÑO DE UNA RED CONVERGENTE UTILIZANDO VPN IPSEC ENTRE LA CENTRAL DE UNA FARMACIA LOCALIZADA EN LIMA METROPOLITANA Y SU SUCURSAL UBICADA EN JAUJA-JUNIN".

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

ZAPATA OSNAYO, OMAR

Villa El Salvador

2017

DEDICATORIA

Dedico este trabajo a mis padres y mis hermanas, quienes siempre me alientan para ser cada día mejor persona y mejor profesional.

AGRADECIMIENTO

Agradezco a mis padres German Zapata Castro y Soraida Osnayo Mendéz por haberme apoyado durante todos estos años de carrera y dado siempre la mejor educación.

A mis hermanas Fabiola y Wendy por apoyarme en mis estudios.

También quiero agradecer a mi asesor por el apoyo brindado durante el proceso de investigación.

ÍNDICE

CAPÍTULO III: ANÁLISIS Y DISEÑO DE UNA RED CONVERGENTE UTILIZANDO VPN

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

El presente trabajo de investigación lleva por título "**DISEÑO DE UNA RED CONVERGENTE UTILIZANDO VPN IPSEC ENTRE LA CENTRAL DE UNA FARMACIA LOCALIZADA EN LIMA METROPOLITANA Y SU SUCURSAL UBICADA EN JAUJA-JUNIN**" para optar el título de INGENIERO ELECTRONICO Y TELECOMUNICACIONES, presentado por el alumno Omar Zapata Osnayo.

La globalización del internet en los últimos años ha revolucionado la forma en que las empresas se comunican entre sus áreas o sucursales, localizadas incluso a cientos de kilómetros de su sede central, como es nuestro caso.

El protocolo Virtual Private Network (VPN) ha sido y es una herramienta de gran importancia para la transmisión de forma segura para la señal de voz, video y datos a grandes distancias donde resultaría complicado realizar un enlace privado debido al enorme costo de implementación, operación y mantenimiento que esto tendría.

El desarrollo de este proyecto de una red VPN IPsec se realiza para conseguir interconectar la sede central de una farmacia localizada en Lima Metropolitana y su sucursal localizada en Jauja-Junín, consiste en crear un túnel virtual a través de la Internet publica para que se pueda transportar datos, telefonía IP y video sin que esta pueda ser interceptada por usuarios ajenos a la empresa.

El autor

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

En el Perú existen empresas que poseen sucursales en diferentes departamentos, las cuales debido a su distancia de separación es difícil tener un cableado o enlace de comunicaciones punto a punto privado por razones técnicas o de costo para la transmisión de la información. Por lo cual están en la necesidad de transmitir su información por un medio tanto o más eficiente y a menor costo. Siendo así que esta propuesta de solución es transmitir en forma privada a través de la red de Internet pública, en donde tomaremos las medidas adecuadas mediante óptimas condiciones de seguridad y eficiente gestión, evitando que sea alterada fácilmente y ocasionar pérdidas a la empresa y su sucursal.

Los datos que se transmitirán entre la sede central y su sucursal serán considerados de máxima seguridad donde se alojaran: la base de datos de la empresa con los costos de los diferentes productos, la cantidad de productos que cuenta la empresa y su movimiento, información personal de sus clientes y de sus colaboradores. Además de garantizar la seguridad en los accesos a sus redes de telefonía IP y cámaras de video IP, con lo que usuarios ajenos a la empresa podrían manipular esta información con fines dolosos. Por ejemplo con el robo de la base de datos podrían suplantar o alterar información en los costos de los productos.

Así mismo si se lograra acceder por Internet a las cámaras de seguridad podrían desactivarlas evitando identificar los eventos ocurridos como asaltos.

En tal sentido la transmisión de datos entre la sede central de la farmacia en Lima y su sucursal en Jauja-Junín, separadas a más de 250 kilómetros, requiere crear una red segura a través de la Internet sin ser interferencias por personas ajenas a la empresa y así por garantizar un óptimo funcionamiento seguro y rápido.

1.2 JUSTIFICACIÓN DEL PROBLEMA

El presente proyecto se justifica por la necesidad que tiene la farmacéutica de crear un enlace seguro para la transmisión de datos entre su estación principal localizada en Lima Metropolitana con su nueva sucursal localizada en la ciudad de Jauja-Junín, para que puedan tener acceso a la base de datos en Lima de forma segura, además de poder controlar los gastos y seguridad de su sucursal de forma

remota a través de Internet, obteniendo así una mayor eficiencia en la gestión de la sucursal para llevar el inventario de los productos, verificar el correcto funcionamiento de las cámaras IP a fin de obtener una mejor calidad del servicio al cliente y seguridad a la sucursal.

El uso del protocolo VPN IPSsec puede ofrecer a la empresa muchos beneficios como ahorrar costos significativos en la creación de un canal privado de datos, además de ser un protocolo confiable, practico y portable con el cual se busca crear un puente virtual para acceder a la red de área local de la sucursal de forma remota sobre una red pública sin que esta sea interceptada por usuarios ajenos a la empresa.

1.3 DELIMITACIÓN DE LA INVESTIGACIÓN

1.3.1 Espacial: El desarrollo de este proyecto se realizara entre la sede central de la farmacia localizada en Lima Metropolitana con su nueva sucursal localizada en la ciudad de Jauja-Junín.

1.3.2 Temporal: El proyecto tiene una duración aproximada de 6 meses a partir del 2 de enero del 2017 al 2 de julio del 2017.

1.4 FORMULACIÓN DEL PROBLEMA

1.4.1 Problema general

¿Cómo dar una solución económica, eficaz y segura al problema de transferencia de voz, datos y video a través de la Internet en forma segura entre la sede central de una farmacia ubicada en Lima Metropolitana y su sucursal en Jauja-Junín?

1.4.2 Problemas específicos

- ¿Cuáles serán los cambios necesarios en la configuración de la red para permitir que el protocolo VPN pueda transmitir voz y data de forma encriptado sin ocasionar perdidas de información de voz y data?

- ¿Cuál es el tiempo de latencia deseable para la transmisión de ancho de banda, de tal forma que la encriptación y desencriptación de voz y data no afecte la calidad y tasa de transferencia de datos?

1.5 OBJETIVOS

1.5.1 Objetivo general

- Diseñar una red de comunicación privada a través de la Internet para transmitir voz y data entre la sede central y la sucursal de una farmacia; de tal forma que sea segura, escalable y eficaz. Logrando obtener una comunicación eficiente, sin perdidas e interferencias.

1.5.2 Objetivos específicos

- Desarrollar un servicio de red convergente utilizando encriptación AES de 128 bits de tal forma que se pueda garantizar que la información de voz y data no sea robada o modificada.

- Realizar la configuración y diseño de una red convergente de tal forma que la latencia por transferencia, encriptación y desencriptación de datos entre sede no sea mayor a 150 milisegundos para evitar pérdidas de transferencia de voz en tiempo real.

- Realizar un diseño de red de tal forma que sea escalable tanto para la implementación de nuevos usuarios finales en las sedes existentes como para la implementación de futuras sucursales en otras ciudades.

CAPÍTULO II

MARCO TEÓRICO

2.1 ANTECEDENTES

Para la presente investigación se ha hecho un estudio de distintos proyectos de investigación realizados que se encuentran relacionados al tema, obteniendo conclusiones relacionadas al objetivo de la investigación.

Eduardo Alva, (2013), realizo la investigación: Desarrollo e implementación de una herramienta gráfica para la configuración remota de una VPN con routers Cisco, en la facultad de Ciencias e Ingeniería De La Pontificia Universidad Católica del Perú. La cual presenta las siguientes principales conclusiones:

1. En la última década, con el avance de la tecnología, la Internet y las telecomunicaciones han hecho que las grandes empresas e inclusive las pymes

hallan cambiado su forma de trabajar. En la actualidad, las empresas quieren expandir sus mercados, por ello ubican sus locales en distintos distritos, provincias y/o departamentos, de lo cual se presenta la necesidad de mantener una comunicación segura, confiable, rápida y lo que es aún más importante a un costo regular, entre todos los locales de una misma empresa con el fin de compartir información importante como precios de producto, balances y otra información que pueda ser crítica en definitiva su gestión.

2. Se pueden adquirir servicios dedicados de conexión entre locales y un proveedor de servicios, pero estos son muy caros y el precio se multiplica por las variables de números de locales y distancia entre los mismos. Por tanto para poder mantener una comunicación segura, confiable, rápida y a un costo no excesivo; una solución viable es la del uso de una Red Privada Virtual o VPN (Virtual Private Network) que permita a las empresas crear su propia red privada permitiendo conectar sus locales. Sin embargo, realizar esto requiere de un conocimiento especializado en la configuración de equipos (routers), ya que podría resultar problemático e inseguro para un usuario en general si deseará realizarlo por su cuenta.

Ricardo Menéndez, (2012), realizo la investigación: Estudio del desempeño e implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos, en la Facultad De Ciencias e Ingeniería De La Pontificia Universidad Católica Del Perú. De la cual obtengo las siguientes conclusiones:

1. El crecimiento sostenido y cada vez más acelerado de Internet ha despertado un gran interés por los mecanismos de transporte de datos y sus diferentes aplicaciones, entre los que se encuentran las Redes Privadas Virtuales o VPNs (Virtual Private Networks). Para hacer posible su despliegue, tecnologías como MPLS (Multi Protocol Label Switching) han tenido gran aceptación debido a sus múltiples ventajas y características que la han convertido en la tecnología ideal para muchas grandes empresas.

2. Las soluciones MPLS-VPN, además de proporcionar escalabilidad, permiten dividir una gran red en pequeñas redes separadas, lo cual es muchas veces necesario en grandes compañías, donde la infraestructura tecnológica debe ofrecer redes aisladas a áreas individuales.

Rodoya Takele Degefa, (2015), realizo la investigación: VPN Scenarios, Configuration and Analysis, para la facultad de ingenieria e informacion de Helsinki Metropolia University of Applied Sciences, Finlandia. La cual presenta las siguientes conclusiones:

1. Las empresas actuales ofrecen a los empleados la oportunidad de trabajar desde su casa o en el camino. Cuando una empresa permite que su personal tenga acceso a la red interna, es importante que esto se haga de manera segura. Hoy en día, una conexión de banda ancha hace posible una forma rápida de enviar y recuperar información a través de Internet. Al igual que hay

personas en Internet que intentan tener acceso a las computadoras de otras personas para robar información o simplemente para destruirla. Una solución común para permitir que los usuarios tengan acceso a los recursos internos de la compañía es construir un sistema de seguridad bien organizado y proteger a sus usuarios. Esto permite a los usuarios acceder a los recursos internos de una manera segura.

2. Las empresas gastan grandes sumas de dinero para tener una conexión tan rápida, segura y confiable como sea posible. Los empleados deben ser capaces de conectarse con seguridad a su red de la empresa desde fuera de la oficina. Esto incluye dónde quieren trabajar desde casa, en un viaje de negocios, sentarse en un lugar de espera del cliente u otras situaciones posibles donde quieren acceder a la información disponible en la red interna. Para hacer esto es necesario utilizar un medio para comunicarse. Es importante tener un sistema seguro y económico para poder comunicarse de forma rápida y confiable, por esto es importante crear un túnel VPN en una LAN pequeña.

Yi Yang, (2011), realizo la investigación: VIRTUAL PRIVATE NETWORK MANAGEMENT, en la Facultad Politécnica en Mikkeli University Of Applied Sciences, Finlandia. La cual presenta las siguientes conclusiones:

1. Una VPN (Virtual Private Network) es una red informática que utiliza una Infraestructura de red pública de telecomunicaciones como Internet para

proporcionar a las oficinas remotas o a los usuarios acceso a la red de su organización. Su objetivo es evitar un costoso sistema de líneas arrendadas que debe ser utilizado por empresas para garantizar la seguridad en la transferencia de datos a través de Internet. VPN, es una red privada, utiliza la Internet pública, por lo tanto la seguridad es una tarea esencial.

2. Las VPN seguras utilizan protocolos de túnel criptográfico para proporcionar Confidencialidad mediante el bloqueo de las intercepciones y la detección de paquetes, creando un puente virtual para que pase la información del mensaje y proporcionar la integridad del mensaje mediante la prevención de la alteración del mensaje enviado.

2.2 BASES TEÓRICAS

2.2.1 Componentes de la red

(Cisco Networking Academy Program, módulo 1 capítulo 1, 2016) indica que la ruta que toma un mensaje de datos desde el origen hasta el destino puede ser tan sencilla como un solo cable que conecta una computadora con otra como tan compleja como una red que literalmente necesitaría recorrer todo el mundo.

La infraestructura de red contiene tres categorías de componentes de red:

- **Dispositivos:** son los elementos físicos o el hardware de la red, contienen una CPU que se encarga de codificar y decodificar la información para los usuarios finales o host. Se tiene de dos clases:

  A) dispositivos intermedios: son los que se encargan de llevar y procesar la información a través de la red de forma segura, como son: router, switch, firewall, etc.

  B) dispositivos finales: son los que interactúan directamente con el usuario común como son: computadoras, impresoras, teléfonos IP, etc.

- **Medios:** es el canal por donde viaja la información desde el origen hasta el destino sea por cable ethernet, fibra óptica, satelital o inalámbrico.
- **Servicios:** estos incluyen muchas de las aplicaciones de red comunes que utilizan las personas a diario, como los servicios de hosting de correo electrónico, web hosting, telefonía IP, etc.

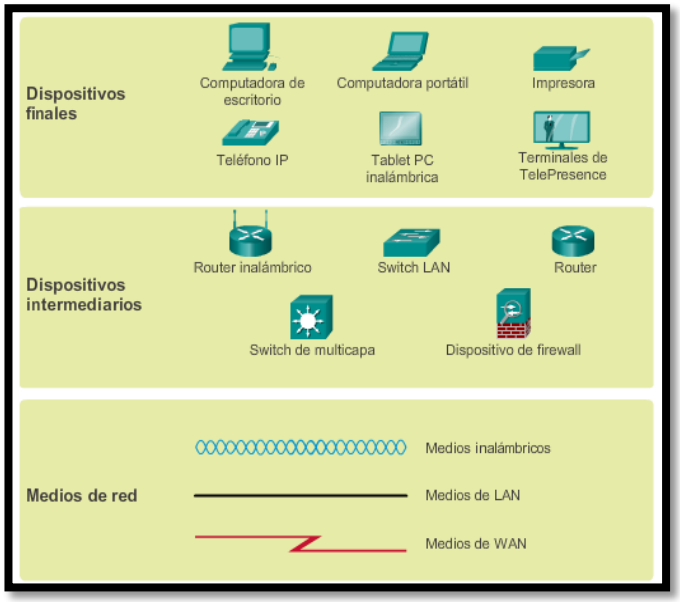


Figura 2.1: Componentes de la red
Fuente: https://goo.gl/fySFVH

2.2.1.1 Switch

(Cisco Networking Academy Program, módulo 3 capítulo 1, 2016) define Switch como un dispositivo de red que funciona a nivel de capa de enlace en el modelo OSI, se encarga de la interconexión de equipos dentro de una misma red creando una red ethernet de área local. En un modelo jerárquico de núcleo contraído (ideal en pequeñas LAN), el switch tiene como objetivo dar una adecuada distribución a la información entrante y saliente de la red para evitar que se creen bucles lo cual acelera la salida y llegada de paquetes, reduciendo el tiempo de espera además el costo por puerto resulta más rentable que el de los router el cual posee pocos puertos Ethernet.

El switch se encarga de brindar acceso a la LAN a usuarios finales tales como las computadoras, teléfonos IP, impresoras, etc. El switch brinda seguridad y orden a la red ya que puede crear redes lógicas independientes para segmentar diferentes áreas dentro de una empresa o campus tales como el área administrativa, el área de estudiantes, el área de centro de datos, etc. El switch también puede crear redes con el objetivo de separar servicios, como es el caso del proyecto que busca crear redes lógicas independientes para voz, video y datos; al segmentar la red en pequeños dominios de colisión, se reduce el costo de broadcast. El switch al segmentar una red optimiza los recursos de ancho de banda.

El switch tiene una gran herramienta de seguridad, al poder configurar cada uno de sus puertos en forma independiente, pudiendo deshabilitar los que no se

utilicen y configurar los puertos utilizados con una dirección MAC exclusiva, evitando que dispositivos ajenos se conecten a la red de forma física para consumir ancho de banda o robar información.

La necesidad de agregar usuarios finales permite crecer a la red en el futuro, por lo que existen tres factores de forma:

- **Switch de configuración fija:** no admite más puertos ethernet que los originales por lo que no es recomendable el uso en redes con planificación de crecimiento de usuarios finales.
- **Switch de configuración modular:** el chasis acepta tarjeta de línea que contiene los puertos, con lo que se obtiene más flexibilidad en el diseño.
- **Switch de configuración apilable:** estos tipos de switch permiten apilarse unos a otros para aumentar la cantidad de puertos de acceso. por ejemplo si un switch de 24 puertos se apila con otro con otro de 24 puertos que sea apilable se tendría 48 puertos finales.

Existen cinco categorías de switches para redes empresariales:

- **Switches LAN de campus:** se emplean para escalar el óptimo rendimiento de la red en una LAN empresarial, pueden utilizarse switches de núcleo, de distribución, de acceso y compactos.
- **Switches administrados en la nube:** son switches de acceso administrados a través de la nube, mediante la cual se pueden controlar y configurar miles de puertos de switch.

- **Switches de centros de datos:** promuevan una alta escalabilidad de infraestructura, continuidad de funcionamiento y flexibilidad de transporte.
- **Switches de proveedores de servicios:** se dividen en dos categorías (switches de agregación y switches de acceso Ethernet). Los switches de agregación son switches Ethernet que se utilizan a nivel de prestadora de servicios para que agregan tráfico en el perímetro de la red. En cambio los switches de acceso Ethernet de proveedores de servicios cuentan con inteligencia de aplicación, servicios unificados, virtualización, seguridad integrada y administración simplificada.
- **Redes virtuales:** Las plataformas de switches de redes virtuales proporcionan servicios multiusuarios seguros al incorporar tecnología de inteligencia de virtualización a la red del centro de datos.

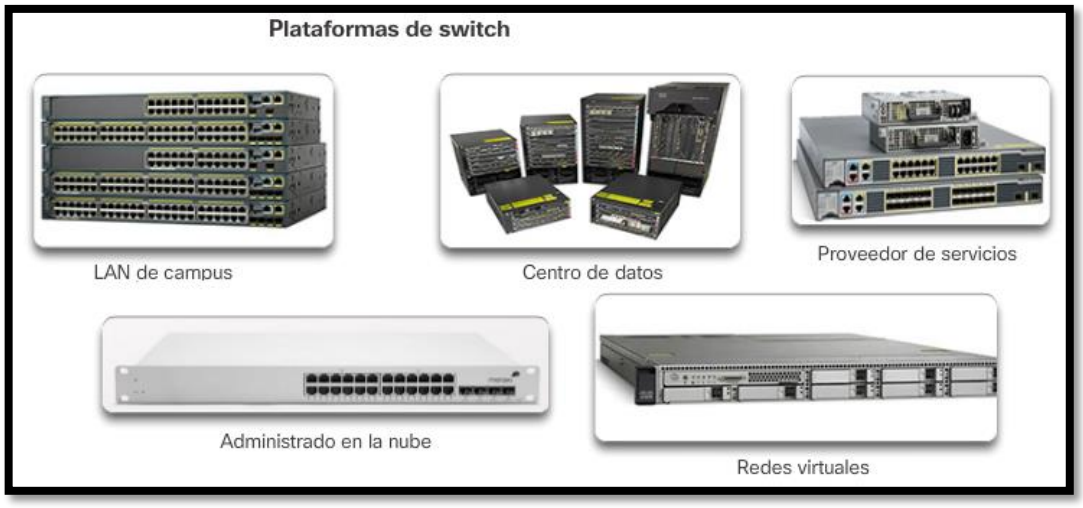


Figura 2.2: Plataformas de switch
Fuente: https://goo.gl/UV2ER1

Consideraciones para elegir un switch

- Costo: el costo de un switch depende de la cantidad y la velocidad de las interfaces.
- Densidad de puertos: los switches de red deben admitir una cantidad adecuada de dispositivos en la red.
- Alimentación: la alimentación a través de Ethernet permite al dispositivo evitar depender de una conexión a una fuente eléctrica para su funcionamiento.
- Confiabilidad: el switch debe proporcionar acceso continuo a la red.
- Velocidad del puerto: la velocidad de la conexión de red es uno de los aspectos fundamentales para los usuarios finales.
- Buffers para tramas: la capacidad que tiene el switch para almacenar tramas es importante en las redes donde los puertos se congestionan constantemente.
- Escalabilidad: el switch debe proporcionar la posibilidad de crecimiento.

2.2.1.2 Router

(Cisco Networking Academy Program, módulo 3 capítulo 1, 2016) nos indica que el routing es necesario en la capa de distribución de una red empresarial. Sin el proceso de routing, los paquetes no pueden salir de la red local. El router funciona en la capa de red del modelo OSI y tiene como función principal el reenvió de paquetes y el enrutamiento de paquetes por una ruta estática o una ruta dinámica que está en función a diferentes algoritmos de enrutamiento, para

que los paquetes puedan llegar a su destino de forma eficaz, para ello necesita almacenar los paquetes recibidos y procesarlo en función de su dirección de origen y destino, si el router encuentra la dirección de red en su tabla de routing envía el paquete al switch que se encarga de dirigirlo al usuario final si no se encontrara lo envía al router de ISP para que el paquete viaje por el Internet público hasta llegar a la dirección de destino.

Importancia del router:

- Contenido de difusión: los router limitan la difusión a la red local.
- Seguridad: se pueden configurar con lista de control de acceso para filtrar el tráfico no deseado, se puede implementar VPN, además se puede configurar diferentes firewall dependiendo del IOS del router.
- Ubicación: se pueden utilizar para interconectar áreas de la empresa separadas geográficamente.
- Agrupamiento lógico: los routers agrupan usuarios de forma lógica, como los departamentos de una empresa.

A medida que crece una red, es importante seleccionar los routers adecuados que cumplan con los requisitos de red, por lo que se tiene tres categorías de routers:

- **Routers de sucursal:** los routers de sucursal optimizan los servicios de sucursal en una única plataforma implementando un servicio de 24/7, son de menor costo y ofrecen funciones básicas es ideal para pequeñas LAN. Existen diferentes series de routers cisco como: serie 800, serie 4000.
- **Routers de perímetro de la red:** son importantes para prestar servicios confiables de alto rendimiento y de alta seguridad que unen las redes de campus, de centro de datos y de sucursal, son routers que poseen un costo alto debido a que necesitan procesar diversos tipos de protocolos de red para redes medianas. Existen diferentes series de routers Cisco como: ASR 1000, ASR 9000.
- **Routers de proveedor de servicios**: Procesan grandes cantidades de datos, su costo es elevado y existen diferentes series de routers cisco como: NCS 5500, ASR 9000.

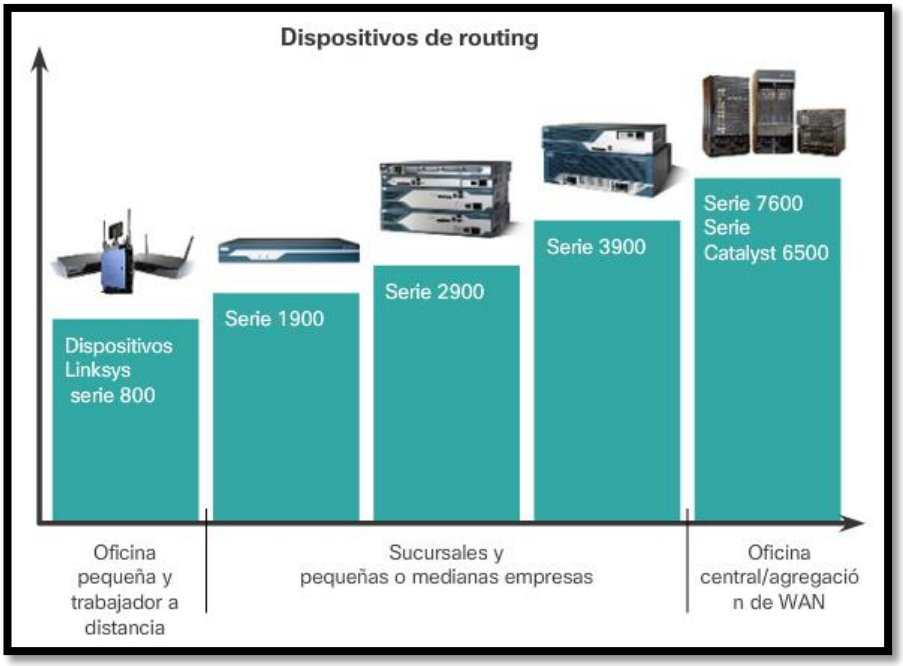


Figura 2.3: Dispositivos de routing
Fuente: https://goo.gl/V23GZj

2.2.1.3 Teléfono IP

(CCNA Voice Official Exam Certification Guide, capítulo 2, 2012) indica que los teléfonos IP funcionan de forma similar a los teléfonos tradicionales, sin embargo la diferencia se encuentra en la forma de transmisión de voz. En un teléfono IP la voz viaja usando el protocolo VoIP, que permite la transferencia de datos por la red de Internet. Los teléfonos IP posen uno a más puertos rj-45 para poder conectarse a la red. Con la Telefonía IP no hace falta tener un PC, sino solo acceso a Internet de una banda ancha. La función principal de un teléfono IP es de realizar llamadas en entornos de red a través de internet por lo que el costo varía dependiendo la calidad de servicio (QoS). Los teléfonos IP se consideran en tres categorías: gama baja, gama media y gama avanzada.

Teléfonos IP según su utilización:

- **Teléfonos SIP**: requieren tener un servicio con un operador IP para conseguir hacer las llamadas a través de Internet, aunque no están supeditados a ningún fabricante o marca de centralita; por lo tanto, pueden colocarse en una extensión de centralita IP no propietaria o directamente a su router.
- **Teléfonos IP para PABX:** sólo se pueden utilizar en centralitas IP específicas que tengan el mismo fabricante.
- **Teléfonos USB:** permiten utilizar su teléfono para comunicaciones a través de su softphone.

Figura 2.4: Teléfono IP
Fuente: https://goo.gl/1JNdyC

2.2.1.4 Cámara IP

(Wireless-N internet home monitoring camera, capítulo 2, 2011) nos indica que una cámara IP son videocámaras especialmente diseñadas para enviar las señales de video y en algunos casos de audio, a través de Internet, lo que permite poder realizar en tiempo real un proceso de video vigilancia de forma remota.

En las cámaras IP, pueden integrarse aplicaciones adicionales como detección de presencia y hacer que se envié una alarma o mensaje en caso se detecte un movimiento o sonido. También se puede grabar lo transmitido y almacenarlo en un servidor remoto de tal forma que en caso de robo u accidente se pueda tener pruebas almacenadas en lugares seguros.

La principal ventaja de un servicio de cámara IP es su costo de operación y mantenimiento ya que esta es digital, la señal se envía a través de Internet y se almacena en la memoria flash de un servidor de forma automática o manual.

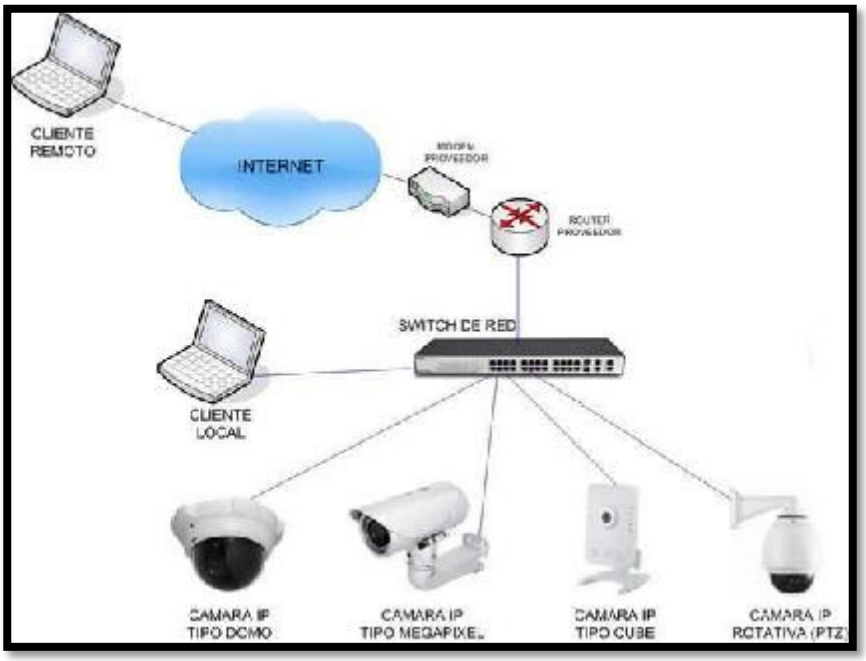


Figura 2.5: Esquema de conexión de cámaras IP
Fuente: https://goo.gl/zz9OXw

2.2.2 Tipos de red

(Cisco Networking Academy Program, módulo 3 capítulo 1.2.2, 2016) nos define los tipos de red como infraestructuras de red que pueden variar en gran medida en los siguientes aspectos:

- El tamaño del área.
- La cantidad y los tipos de servicios disponible.
- La cantidad de usuarios conectados.

La Internet se divide principalmente en 2 redes: WAN y LAN las cuales se interconectan en diferentes áreas geográficas la LAN es utilizada en redes

privadas o de cliente, mientras que la WAN es utilizada como redes de proveedor de servicios.

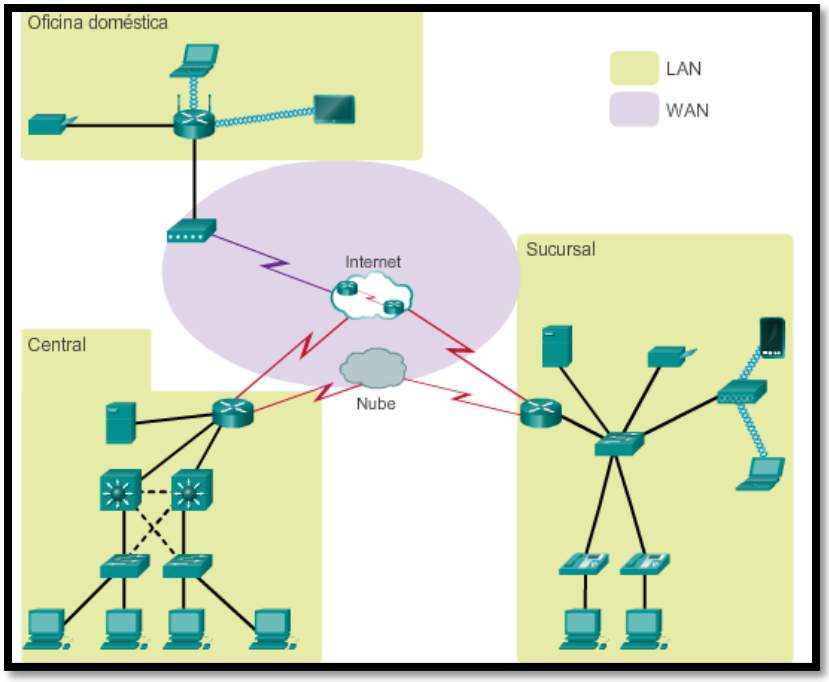


Figura 2.6: Tipos de red
Fuente: https://goo.gl/SkmqBj

2.2.2.1 WAN (Wide Area Network)

(CCNA Routing And Switching 200-125 Official Cert Guide Library, capítulo 3, 2016) define que las redes de área extensa son infraestructuras de red que proporcionan acceso a otras redes en un área geográfica extensa normalmente, la administración de las redes WAN están a cargo de los proveedores de servicios (SP) o proveedores de servicios de Internet (ISP).

Las WAN interconectan varias LAN a través de áreas geográficas extensas, por ejemplo, entre ciudades, provincias, países o continentes.

Existen varias opciones de conexión de acceso WAN que los ISP pueden utilizar para conectar las LAN. Estas opciones de acceso WAN varían en términos de velocidad, tecnología y costo.

Infraestructura WAN privada: los proveedores de servicios de Internet pueden ofrecer líneas arrendadas punto a punto dedicadas, enlaces de conmutación de circuitos, como PSTN o ISDN, y enlaces de conmutación de paquetes. Los cuales resultan ser costosos y son más utilizados para redes empresariales grandes pero sujeto a cambio tecnológico.

Infraestructura WAN pública: el proveedor de servicios puede ofrecer acceso a Internet de banda ancha mediante una línea de suscriptor digital (DSL), cable y acceso satelital. Las opciones de conexión de banda ancha son utilizadas normalmente para conectar oficinas pequeñas y trabajadores a distancia a un sitio corporativo a través de Internet.

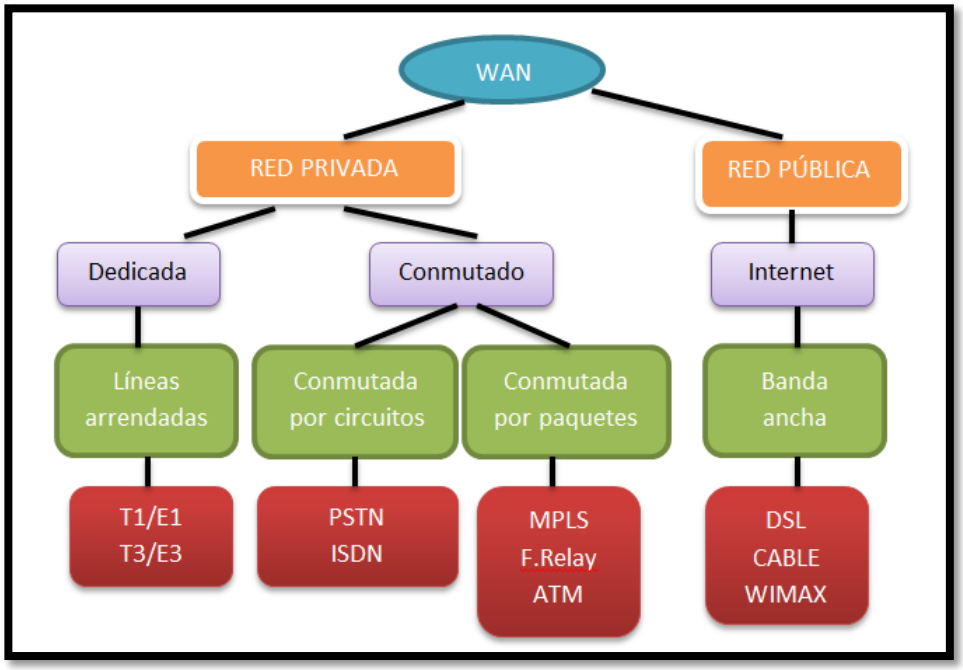


Figura 2.7: Diagrama de red WAN
Fuente: propia

2.2.2.2 LAN (Local Area Network)

(Cisco Networking Academy Program, módulo 1 capítulo 1.2.2.2, 2016) define una LAN como una red de datos que cubre una área geográfica relativamente pequeña cuya propiedad es privada pueden ser tan grandes como las LAN empresariales como tan pequeñas como son las LAN hogareñas.

Las LAN interconectan dispositivos finales en un área limitada, como una pequeña empresa, un centro de estudios o un edificio de oficinas. Para que una pc pueda conectarse a una red, debe tener una tarjeta de red (NIC), los medios utilizados para conectarse a una red de área local son a través de un cable o de forma inalámbrica, que se unen a través de un dispositivo de enlace como un switch, módem o router.

2.2.2.3 SOHO (Small Office, Home Office)

(CCNA Routing And Switching 200-125 Official Cert Guide Library, capítulo 2, 2016) indica que el modelo SOHO es un tipo de red que está diseñado a un uso profesional o semiprofesional pero que a diferencia de los modelos empresariales o de campus, este se diseña pensando en el acceso a pocos usuarios finales que necesitan acceso a la Internet con bajo tráfico de red, por lo que utiliza una conexión a Internet publica no muy costosa. Como es el caso de nuestra farmacia donde pocos usuarios finales necesitan estar conectados a la Internet por lo que no se requiere un alto ancho de banda.

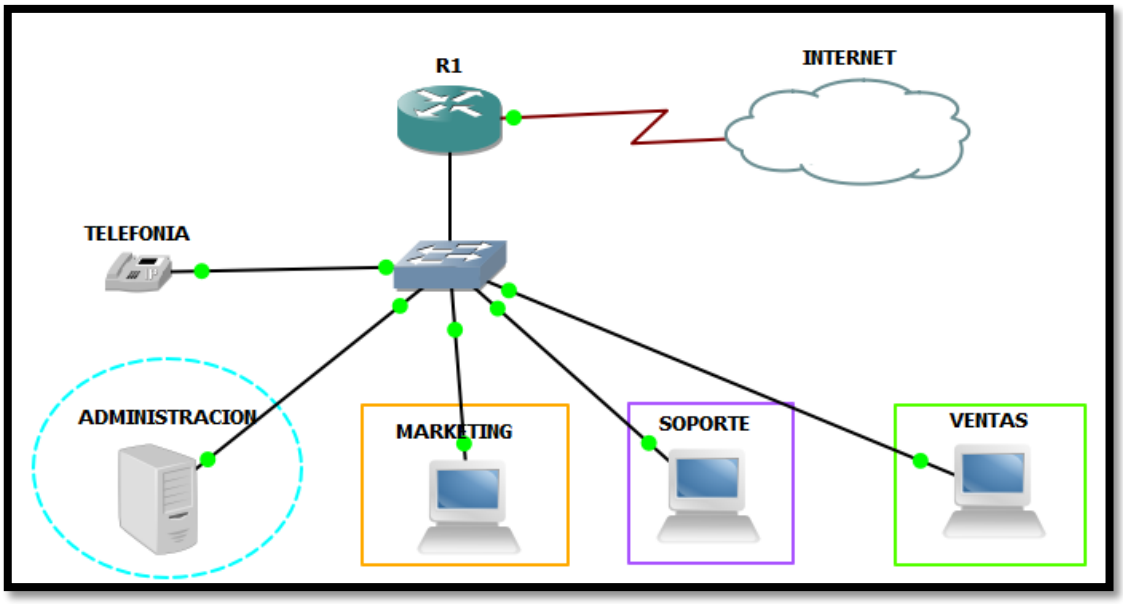


Figura 2.8: Red SOHO
Fuente: propia

2.2.2.4 Conexión de empresas a Internet

(Cisco Networking Academy Program, módulo 1 capítulo 1.2.4.2, 2016) define diferentes formas de conectar a usuarios y organizaciones a Internet. Generalmente, los usuarios domésticos, los trabajadores a distancia y las oficinas pequeñas requieren una conexión a un ISP para acceder a Internet. Las opciones de conexión varían considerablemente según los ISP y la ubicación geográfica.

- **Línea arrendada dedicada:** Es una conexión dedicada que va del proveedor de servicios de Internet a las instalaciones del cliente. Las líneas arrendadas son circuitos reservados reales que conectan oficinas que están separadas geográficamente para propósitos de comunicaciones por voz o redes de datos

privados. suelen ser servicios muy costosos como son las opciones t1 (1,54 mb/s) y t3 (44,7 mb/s).

- **MPLS:** es un Servicio de Red Privada Virtual para la interconexión de oficinas mediante líneas dedicadas de velocidad simétrica. Permite la configuración de calidad de servicio (QoS), necesaria para la priorización de aplicaciones críticas (VoIP, Video IP, otros). Permite la configuración de conectividad Extranet para conexión segura con las redes de terceros (Socios, Proveedores o Clientes) que tengan conexión con la red MPLS del proveedor. Tiene como beneficio la capacidad de formar redes privadas mixtas con oficinas conectadas con IP VPN acceso ADSL y VSAT.

  MPLS-Movistar: ofrece velocidades desde 64Kbps hasta 155Mbps. Su renta mensual es desde s/436(*)(**)

  ***** Precios referenciales incluido IGV. Sujeto a plazo de contrato de 60 meses. No incluye alquiler de equipos Modem y Router lado cliente.

  ******fuente:http://tolpre.movistar.com.pe/negocios/soluciones/conectividad/redes-privadas/ip-vpn

- **Red Metro Ethernet:** es un servicio disponible desde el proveedor a las instalaciones del cliente mediante una conexión dedicada de fibra óptica o de cable de cobre que proporcionan velocidades de ancho de banda de 100 Mbps en cable ethernet a 10 Gbps mediante fibra óptica.

- **Satelital:** el servicio satelital puede proporcionar una conexión cuando no hay soluciones de conexión por cable disponibles. los costos de equipos e instalación pueden ser elevados y la velocidad de transmisión es baja.

  Movistar-satelital: ofrece los siguientes planes mensuales los cuales no incluyen instalación ni equipo.

Incluye	Capacidad total de descarga mensual	Velocidad	Cargo fijo
Plan Movistar Internet Satelital Residencial 6 GB	6 GB 3 GB de descarga en horario normal y 3 GB de descarga en horario reducido	Hasta 256 Kbps de bajada Hasta 43 Kbps de subida	S/. 149.00
Plan Movistar Internet Satelital Negocios 24 GB	24 GB 12 GB de descarga en horario normal y 12 GB de descarga en horario reducido	Hasta 512 Kbps de bajada Hasta 85 Kbps de subida	S/. 399.00
Plan Movistar Internet Satelital Empresas 100 GB	100 GB 50 GB de descarga en horario normal y 50 GB de descarga en horario reducido	Hasta 3072 Kbps de bajada Hasta 1024 Kbps de subida	S/. 1,940.00

Tabla 1.1: Costo Internet satelital
Fuente: http://www.movistar.com.pe/negocio/soluciones/internet-satelital

- **DSL (Digital Subscriber Line):** La línea de suscripción digital proporciona el acceso a Internet mediante la transmisión de datos digitales a través de los cables de una red telefónica local. utiliza el par trenzado de hilos de cobre convencionales de las líneas telefónicas para realizar la transmisión de datos a gran velocidad. La tasa de transferencia de bits de los servicios DSL varía normalmente de 256 kbps hasta 50 Mbps. Existen de dos tipos:

Línea de abonado digital asimétrica (ADSL) la cual es la más utilizada, su característica es que la velocidad de descarga es más rápida que la de subida de datos.

Línea de abonado digital simétrica (SDSL) la velocidad de descarga es igual a la de subida por lo que su precio es mucho más alto en comparación con un ADSL.

Movistar-ADSL: costo de servicio solo internet para ciudades del Perú como Lima Metropolitana, Jauja, Huancayo, Arequipa, etc.

velocidad	costo
15 Mbps	S/ 104.00
10 Mbps	S/ 89.00
8 Mbps	S/ 79.00
4 Mbps	S/ 69.00
2 Mbps	S/ 54.00

Tabla 2.2: Costos de Internet ADSL Perú
Fuente: http://www.movistar.com.pe/hogar/internet/solo-internet

2.2.2.5 ISP (Internet Service Provider)

Es la empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, cable módem, satelital, etc. La empresa Movistar ofrece conexión a internet en varias ciudades del Perú hasta 10mbps, por lo que se escoge esta empresa ya que cuenta con conexión en Lima y en Jauja.

2.2.3 Redes convergentes

(Cisco Networking Academy Program, módulo 1 capítulo 1.3.1, 2016) indica que las redes convergentes han revolucionado la forma de transmitir información y han reducido el costo del cableado estructurado e infraestructura en las telecomunicaciones. Las redes convergentes son redes que tienen la capacidad de separar la voz, video y datos que pasan por un solo canal sin que se cree una interferencia entre ellos obteniendo una gran calidad de servicio. La convergencia de los diferentes tipos de redes en un solo canal representa la creación de una red inteligente de información.

Las redes convergentes deben admitir una amplia variedad de aplicaciones y servicios así como funcionar a través de distintos medios y dispositivos finales que componen la infraestructura de red, habiendo muchos puntos de contacto y muchos dispositivos especializados, como computadoras personales, teléfonos IP, cámaras IP, impresoras graficas entre otras, pero hay una infraestructura de red común.

Esta infraestructura de red utiliza el mismo conjunto de reglas, acuerdos y estándares de implementación para conseguir que las diferentes señales viajen de un usuario a otro por un solo canal sin que estas señales se vean modificadas, lo que garantiza la calidad de servicio (QoS) y seguridad; requisitos cada vez más importantes en una comunicación en tiempo real.

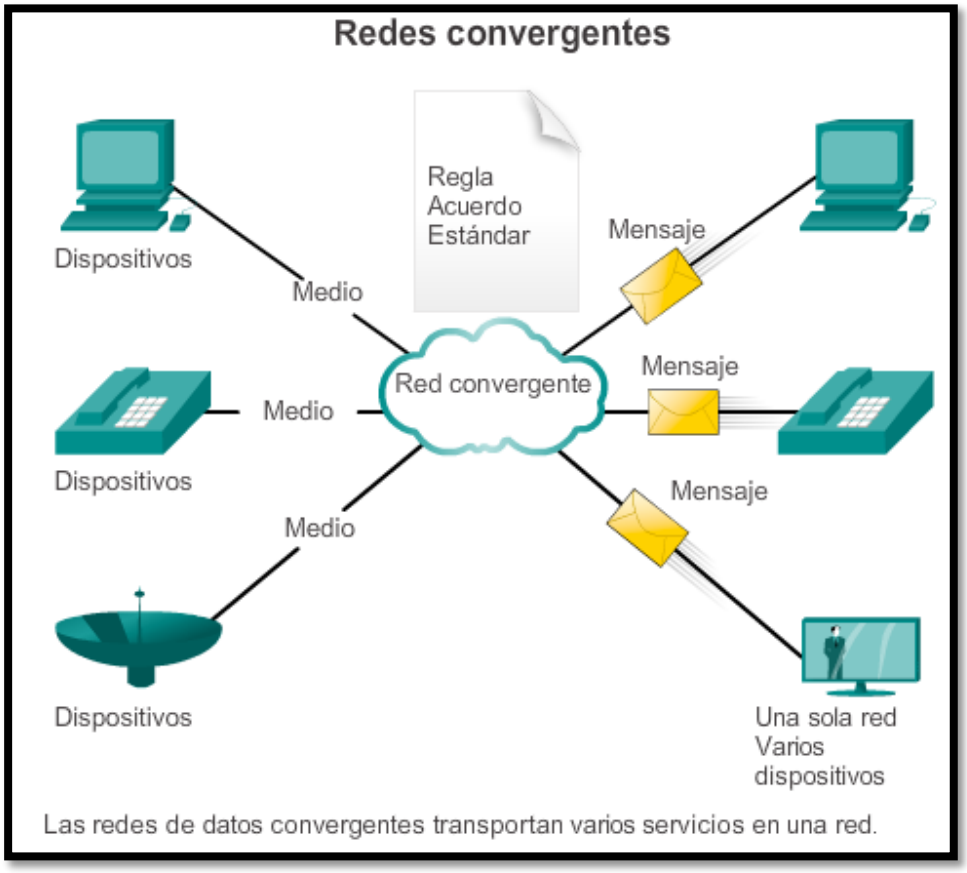


Figura 2.9: Redes convergentes
Fuente: https://goo.gl/9VxB5d

2.2.3.1 VLAN (Virtual Local Area Network)

(Cisco Networking Academy Program, módulo 2 capítulo 3, 2016) indica que las VLAN funcionan en la capa de enlace del modelo OSI, su principal función es la de agrupar dispositivos dentro de una LAN. Los dispositivos que se encuentran dentro de la misma VLAN se comunican como si estuvieran conectados al mismo cable. El funcionamiento de las VLAN se basa en conexiones lógicas, en vez de conexiones físicas.

Una VLAN crea un dominio de difusión lógico que puede alcanzar varios segmentos LAN físicos. Las VLAN mejoran el rendimiento de la red debido a que generan la división de grandes dominios de difusión en otros más pequeños. Cada puerto de switch se puede asignar a una sola VLAN (a excepción de un puerto conectado a un teléfono IP o a otro switch). Los principales beneficios de utilizar las VLAN son los siguientes:

- Seguridad: se pueden separar los grupos con información importante del resto de la red, lo que disminuye las posibilidades de que ocurran violaciones o robos de información confidencial.
- Reducción de costos: el ahorro de costos se debe a la poca necesidad de actualizaciones de red costosas y al uso más eficaz de los enlaces y del ancho de banda existentes.
- Mejor rendimiento: reduce el tráfico de broadcast innecesario en la red y mejora el rendimiento.
- Dominios de difusión reducidos: la división de una red única en varias redes VLAN reduce la cantidad de dispositivos en el dominio de difusión.
- Mayor eficiencia del personal de TI: las VLAN mejoran el manejo de la red debido a que agrupa los usuarios con requerimientos similares de red en una misma VLAN.
- Administración más simple de aplicaciones y proyectos: las VLAN agregan dispositivos de red y usuarios para admitir los requisitos geográficos o

comerciales. Al tener características diferentes, se facilita la administración de un proyecto o el trabajo con una aplicación especializada.

Tipos de VLAN:

- VLAN de datos: es una VLAN configurada para transportar diferente tráfico generado por usuarios.
- VLAN predeterminada (VLAN 1): tiene todas las características de cualquier VLAN, excepto que no se le puede cambiar el nombre ni se puede eliminar.
- VLAN nativa: está asignada a un puerto troncal 802.1Q. Los puertos de enlace troncal 802.1Q admiten el tráfico proveniente de muchas VLAN (tráfico con etiquetas), así como el tráfico que no proviene de una VLAN (tráfico sin etiquetar).
- VLAN de administración: es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch. La VLAN 1 es la VLAN de administración de manera predeterminada.
- VLAN de voz: Se necesita una VLAN separada para admitir la tecnología de voz sobre IP (VoIP). El tráfico de VoIP requiere:

  Capacidad para ser enrutado en áreas con alto tráfico de red.

  Ancho de banda garantizado para asegurar la calidad de la voz en tiempo real.

  Prioridad de la transmisión sobre los tipos de tráfico de la red.

  Una demora inferior a 150 ms a través de la red.

2.2.4 Software de red

(Cisco Networking Academy Program, módulo 1 capítulo 2, 2016) indica que la configuración de los equipos de red es importante para un correcto funcionamiento. La forma en que se configura un equipo puede variar dependiendo el fabricante se puede configurar mediante CLI, GUI o ambos.

- CLI(command-line interface): este tipo de configuración se realiza mediante comando los cuales pueden variar debido a los diferentes fabricantes, por lo que se requiere un conocimiento técnico para configurarlo, se puede configurar a través de telnet de forma remota o mediante el puerto consola usando software como putty, hyperterminal, entre otros.
- GUI(graphical user interface): este tipo de configuración puede resultar más fácil que el CLI debido a que se basa en pocas opciones de configuración, normalmente se realiza a través de un explorador aunque puede entrar en conflicto con firewall de la red.

2.2.4.1 VoIP

(CCNA Voice Official Exam Certification Guide, capítulo 3, 2012) menciona que VoIP (voice over ip) es un método por el cual las señales análogas de voz se convierten en señales digitales lo que hace posible que la señal de voz viaje a

través de Internet empleando el protocolo IP. VoIP es usada para reemplazar la telefonía analógica tradicional en un gran entorno empresarial o un SOHO.

VoIP resulta una opción económica debido a que la señal de voz viaja a través de Internet con lo cual se puede realizar una llamada desde cualquier punto del mundo que posea una conexión a la Internet, con lo que no sería necesario contratar un proveedor de telefonía fija o móvil. Además también posee servicios adicionales sin costo como son: identificador de llamadas, servicio de conferencia entre otros.

2.2.4.2 NVR (network video recorder)

(Nicolas Sosio, www.seguridadsos.com) indica que el NVR es un software o dispositivo que graba vídeo en formato digital y lo almacena en un disco duro, una unidad flash USB, u otro dispositivo de almacenamiento. Un NVR es similar a un DVR; sin embargo el DVR digitaliza, graba y administra imágenes enviadas desde cámaras de seguridad analógicas, en cambio un NVR, graba y administra imágenes ya digitales las cuales son enviadas desde las cámaras IP a través de una red, lo que lo hace muy útil para el uso de videovigilancia de una sucursal debido a su fácil transporte de información a través de la red.

Figura 2.10: Equipo NVR
Fuente: https://goo.gl/dPOHgr

2.2.5 VPN (Virtual Private Network)

(Cisco Networking Academy Program, módulo 4 capítulo 7.1.1.1, 2017) indica que la red virtual privada (VPN) se utilizan para garantizar la seguridad de los datos que viajan a través de la Internet. Una VPN crea un túnel privado a través de una red pública. Se proporciona seguridad a los datos mediante el uso de cifrado en un túnel VPN a través de la Internet y con autenticación para proteger los datos contra el acceso no autorizado. Las organizaciones requieren redes seguras, confiables y económicas para interconectar redes en diferentes lugares. Permitiendo que las sucursales y los proveedores se conecten a la red de la oficina central de una empresa.

Una VPN es una red privada creada mediante tunneling a través de una red pública de Internet. El acceso se controla de forma estricta permitiendo las conexiones se den dentro de una comunidad de interés definida.

Para implementar las VPN, se necesita un gateway VPN. El gateway VPN puede ser un router, un firewall o un dispositivo de seguridad adaptable (ASA). Un ASA es un firewall independiente que combina las funciones de un firewall, un concentrador VPN y un dispositivo de prevención de intrusiones en una imagen de software.

Los beneficios de una VPN incluyen los siguientes:

- Ahorro de costos: las VPN permiten que las organizaciones utilicen un transporte externo de Internet económico para conectar sedes remotas y

usuarios remotos al sitio principal; lo que elimina la necesidad de requerir enlaces WAN dedicados.

- Escalabilidad: las VPN permiten que las organizaciones utilicen la infraestructura de Internet dentro de los ISP, lo que facilita la tarea de agregar nuevos usuarios y equipos intermediarios. lo que beneficia a las organizaciones que pueden agregar una gran cantidad de capacidad sin necesidad de aumentar considerablemente la infraestructura.
- Compatibilidad con la tecnología de banda ancha: las redes VPN permiten que los trabajadores móviles y los empleados a distancia aprovechen la red pública para realizar conexiones de alta velocidad, para acceder a las redes de sus organizaciones sin poner en riesgo la información de la empresa.
- Seguridad: las VPN cuentan con mecanismos de seguridad que proporcionan el máximo nivel de seguridad mediante protocolos de cifrado y autenticación avanzados que protegen todos los datos enviados y recibidos contra el acceso no autorizado.

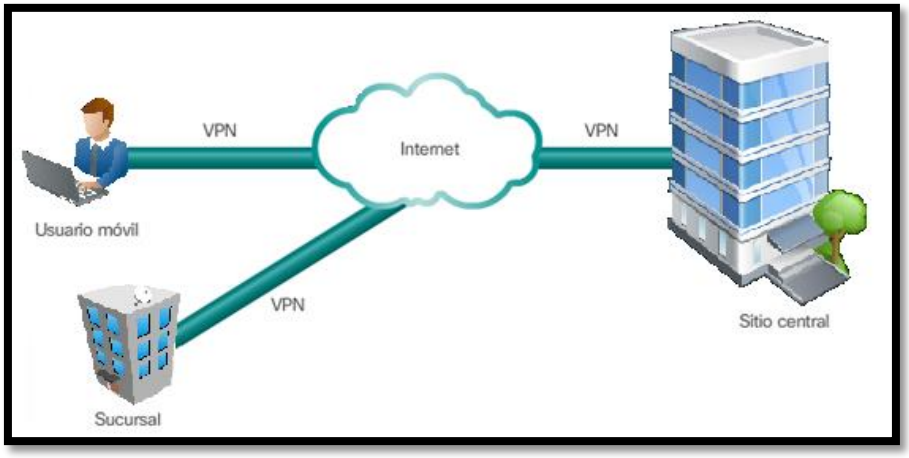


Figura 2.11: Enlace VPN
Fuente: propia

Existen dos tipos de VPN: VPN Sitio a sitio y VPN de acceso remoto

2.2.5.1 VPN de sitio a sitio

(Cisco Networking Academy Program, módulo 4 capítulo 7.1.2.1, 2017) nos indica que una VPN de sitio a sitio se establece cuando los dispositivos en ambos lados de la conexión VPN conocen la configuración de VPN con anticipación. La VPN permanece estática, y los hosts internos no saben que existe una VPN. En una VPN de sitio a sitio, los hosts terminales envían y reciben tráfico TCP/IP normal a través de un “gateway” VPN. El gateway VPN es el responsable de encapsular y cifrar todo el tráfico de una conexión en particular.

Una VPN de sitio a sitio es una extensión de una red WAN clásica. Las VPN de sitio a sitio conectan redes enteras entre sí, como es el caso del proyecto que buscar conectar la red de una sucursal a la red de la oficina central de una empresa.

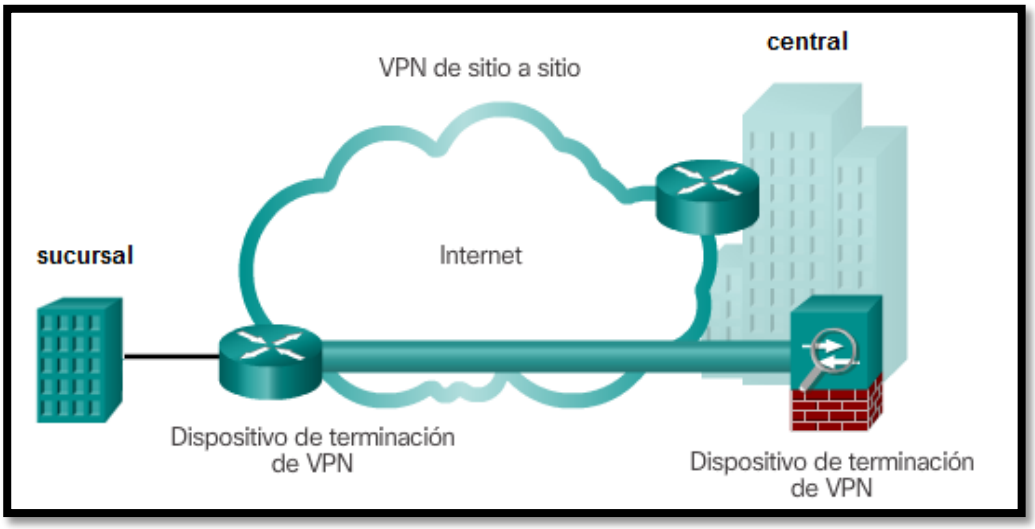


Figura 2.12: VPN sitio a sitio
Fuente: https://goo.gl/qA8uLJ

2.2.5.2 VPN de acceso remoto

(Cisco Networking Academy Program, módulo 4 capítulo 7.1.2.2, 2017) define que la VPN de acceso remoto es utilizada debido a la necesidad de los empleados a distancia, de los usuarios móviles y del tráfico de extranet de cliente a empresa. Una VPN de acceso remoto se crea cuando la información de VPN no se configura de forma estática, pero permite un intercambio de información segura, además se puede habilitar y deshabilitar de forma sencilla por el administrador de red. Las VPN de acceso remoto se utilizan para conectar hosts individuales que deben acceder a la red de su empresa de forma segura a través de Internet.

Las VPN de acceso remoto admiten una arquitectura de cliente-servidor, en la que el cliente VPN (host remoto) obtiene acceso seguro a la red empresarial mediante un dispositivo del servidor VPN en el perímetro de la red. Es posible que se deba instalar un software de cliente VPN en la terminal del usuario móvil. Este tipo de VPN resulta ideal para trabajadores que necesitan viajar a cualquier parte del mundo y conectarse a la central de forma segura, rápida y remota.

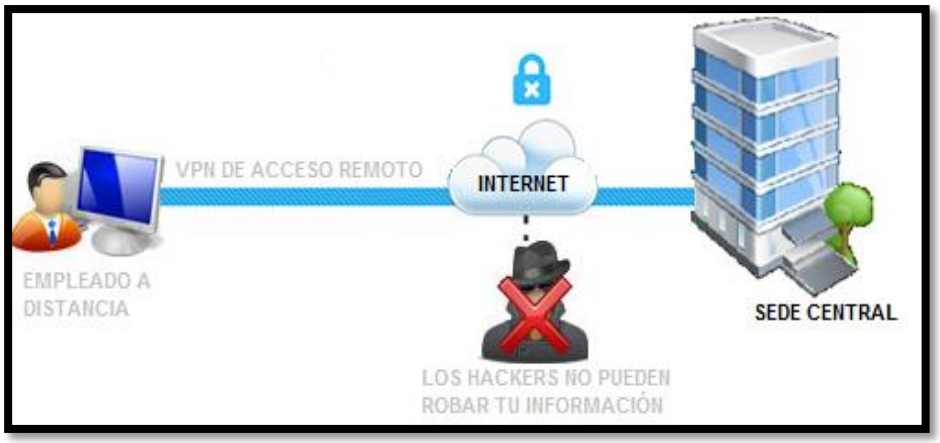


Figura 2.13: VPN de acceso remoto
Fuente: propia

2.2.5.3 Funciones de una VPN

(Cisco Networking Academy Program, módulo 4 capítulo 7.1, 2017) define las principales funciones de una VPN:

- Comprobación de usuarios: las VPN deben comprobar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.
- Direccionamiento estático: la VPN asigna una dirección al cliente en la red privada y deberá asegurarse que las direcciones privadas se mantengan tal como se entregaron.
- Cifrado de datos: los datos que se van a transmitir a través de la red pública, antes deben ser cifrados, para que así no puedan ser descifrados fácilmente por usuarios ajenos.
- Administración de claves: las VPN deben intercambiar las claves de acceso para poder crear un túnel VPN.
- Soporte a protocolos múltiples: La VPN deberá manejar múltiples protocolos utilizados en las redes públicas.

2.2.5.4 IPsec

(Cisco Networking Academy Program, módulo 4 capítulo 7.3.1.1, 2017) indica que la VPN con IPsec ofrece una conectividad flexible y escalable. Las conexiones de sitio a sitio pueden proporcionar una conexión remota segura, rápida y confiable. Con una VPN con IPsec, la información de una red privada se

transporta de manera segura a través de la Internet. El tráfico se cifra a fin de mantener la confidencialidad de los datos.

IPsec es un estándar IETF que define la forma en que se puede configurar una VPN de manera segura mediante el protocolo de Internet.

IPsec funciona en la capa de red, por lo que protege y autentica los paquetes IP entre los dispositivos IPsec participantes, conocidos como “peers”. IPsec protege la ruta entre un par de gateways, un par de hosts o un gateway y un host.

2.2.5.5 Servicios de seguridad IPsec

(Cisco Networking Academy Program, módulo 4 capítulo 7.3.1.2, 2017) indica que los servicios de seguridad IPsec proporcionan cuatro funciones fundamentales:

- Confidencialidad (cifrado): en una implementación de VPN, los datos privados se transfieren a través de una red pública. Por esta razón, la confidencialidad de los datos es fundamental. Esto se puede conseguir mediante el cifrado de todos los datos antes de transmitirlos a través de la red. Así si la comunicación es intercepta, el pirata informático no puede leer los datos transmitidos y recibidos.
- Integridad de datos: el receptor puede verificar que los datos se hayan transmitido a través de Internet sin sufrir ningún tipo de cambio. IPsec cuenta con un mecanismo para asegurarse de que la porción cifrada del paquete no

se haya modificado. IPsec garantiza la integridad de los datos mediante checksums, que es una comprobación de redundancia simple. Si se detectara una alteración en el paquete, el paquete se descarta.

- Autenticación: verifica la identidad del origen de los datos que se envían. Esto es importante para la protección contra distintos ataques que dependen de la suplantación de identidad del emisor. La autenticación asegura que se cree una conexión con el usuario de comunicación deseado. IPsec utiliza el intercambio de claves de Internet (IKE) para autenticar a los usuarios y dispositivos que establecen la comunicación de manera independiente.
- Protección antireproducción: es la capacidad de detectar y rechazar los paquetes reproducidos. La protección antireproducción verifica que cada paquete sea único y no esté duplicado.

2.2.5.6 Confidencialidad con cifrado IPsec

(Cisco Networking Academy Program, módulo 4 capítulo 7.3.2.1, 2017) indica que el tráfico VPN se mantiene confidencial mediante el cifrado de los datos. Los datos de texto no cifrado que se transportan a través de Internet pueden interceptarse y leerse por usuarios ajenos; sin embargo el cifrado digital de los datos hace que estos sean ilegibles hasta que el receptor autorizado los descifre.

Para que la comunicación cifrada funcione, el emisor y el receptor deben conocer las mismas reglas que se utilizan para transformar el mensaje original a su forma cifrada. Las reglas se basan en algoritmos y claves asociadas.

Un algoritmo es una secuencia matemática de pasos que combina un mensaje, texto, dígitos o los tres con una cadena de dígitos denominada “clave”. El resultado es una cadena de cifrado ilegible. El algoritmo de cifrado también especifica cómo se descifra un mensaje cifrado. El descifrado es extremadamente difícil o imposible sin la clave correcta.

El grado de seguridad dependerá de la longitud de la clave del algoritmo de cifrado y la sofisticación del algoritmo. Si un pirata informático intenta descifrar la clave mediante un ataque por fuerza bruta, la cantidad de intentos posibles es una función de la longitud de la clave. Cuanto más corta sea la clave, más fácil será descifrarla. Por ejemplo, un estudio de Cisco ha demostrado que una computadora relativamente sofisticada puede tardar aproximadamente un año para descifrar una clave de 64 bits, mientras que descifrar una clave de 128 bits puede llevarle al menos 10 años.

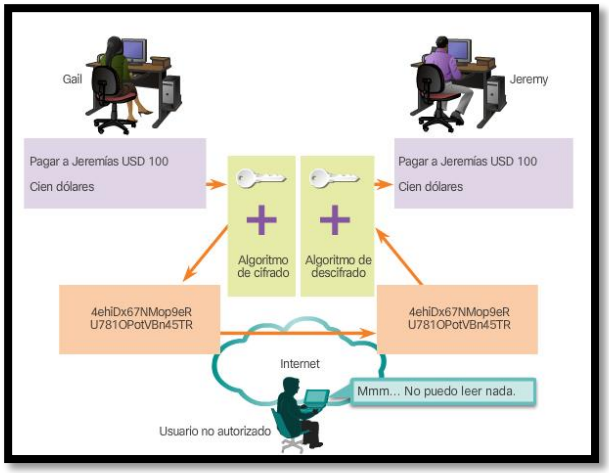


Figura 2.14: Funcionamiento del algoritmo cifrado
Fuente: https://goo.gl/BcGL5b

2.2.5.7 Algoritmos de cifrado de datos

(Cisco Networking Academy Program, módulo 4 capítulo 7.3.2.2, 2017) indica que el algoritmo de cifrado 3DES ya no se considera seguro; por lo que se recomienda utilizar AES para el cifrado de IPsec. La mejor seguridad para el cifrado de IPsec de las VPN entre dispositivos la proporciona la opción del algoritmo AES de 256 bits, el cual es considerado en nuestro proyecto. Existen dos formas de cifrado:

Cifrado simétrico: Los algoritmos de cifrado, requieren previamente de una clave secreta compartida para el cifrado y el descifrado. Cada uno de los dos dispositivos de red debe conocer la clave para decodificar la información. Se tiene diferentes algoritmos de cifrados como: DES, 3DES y AES

Cifrado asimétrico: El cifrado asimétrico utiliza claves diferentes para el cifrado y el descifrado. Aunque conozca una de las claves, un pirata informático no puede deducir la segunda clave y decodificar la información. Una clave es utilizada para cifrar el mensaje, mientras que una segunda clave descifra el mensaje. Ejemplos: RSA

2.3 MARCO CONCEPTUAL

1. 3DES (Triple Data Encryption Algorithm) : es la evolución del DES(56 bits), 3DES es un método de cifrado mucho más seguro que el DES. En teoría la

longitud de la clave usada sería de 168 bits (3x56 bits), aunque la longitud efectiva de la clave es 112 bits.

2. AES (Advanced Encryption Standard): es un algoritmo muy seguro de cifrado simétrico, soporta una longitud de bloque de 128 bits y longitudes de clave de 128, 192 y 256 bits.

3. Broadcast: es la transmisión de datos que serán recibidos por todos los dispositivos conectados a la misma LAN, donde un emisor envía información a una multitud de receptores de manera simultánea.

4. Cámara IP: es un dispositivo de video especialmente diseñado para enviar las señales de video a través de Internet.

5. Checksums: es una función computable mediante un algoritmo que tiene como propósito principal detectar cambios accidentales en una secuencia de datos para proteger la integridad de estos, verificando que no haya diferencias entre los valores obtenidos al hacer una comprobación inicial y otra final tras la transmisión.

6. Cifrado asimétrico: utiliza claves diferentes para el cifrado y el descifrado, una clave cifra el mensaje, mientras que una segunda clave descifra el mensaje.

7. Cifrado simétrico: se emplea una misma clave en el emisor y el receptor para cifrar y descifrar mensajes. Las dos partes que se comunican deben conocer la clave compartida..

8. CLI (command-line interface): permite a los usuarios dar instrucciones a algún programa informático por medio de una línea de texto simple, los comandos de configuración pueden variar debido a los diferentes fabricantes.

9. Dirección MAC (Media Access Control address): conocida como la dirección física del dispositivo, la cual es única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (primeros 24 bits) utilizando el identificador único de la organización.

10. Dirección IPV4: Las direcciones IPv4 se expresan mediante un número binario de 32 bits, que identifica de manera lógica a un dispositivo o una interfaz de red.

11. DSL (Digital Subscriber Line): proporciona el acceso a Internet mediante la transmisión de datos digitales a través de los cables de una red telefónica local, su velocidad se encuentra entre 256 kbit/s hasta 50 mbit/s. Existen de dos tipos: Línea de abonado digital asimétrica (ADSL) y Línea de abonado digital simétrica (SDSL).

12. Ethernet: es un estándar de redes que emplea el método CSMA/CD (Acceso Múltiple por Detección de Portadora con Detector de Colisiones), se encarga de definir las características de los Cables y dispositivos que se deben utilizarse para establecer en una conexión LAN.

13. Firewall: es una parte importante de una red que está diseñada con el objetivo de bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

14. GNS3: es un simulador gráfico de red que te permite diseñar, configurar y simular topologías de red complejas.

15. GUI (graphical user interface): es un software informático que actúa de interfaz de usuario, utiliza un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz de configuración.

16. IKE (Internet key exchange): es un protocolo usado para establecer una asociación de seguridad en el protocolo IPsec.

17. IP (Internet Protocol): es un protocolo de comunicación de datos digitales que funciona en la capa de red del modelo OSI.

18. IPsec (Internet Protocol security): es un conjunto de protocolos cuyo objetivo es asegurar las comunicaciones sobre IP, autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

19. ISDN (Integrated Services Digital Network): Un protocolo de comunicación ofrecido por las compañías telefónicas que permite Redes de datos, voz y video. la estructura para el canal de 1,544 Mbit/s es de 23 canales B más un canal D de 64 kbit/s.

20. ISP (Internet service provider): es la empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como cable, fibra óptica, enlace satelital entre otras.

21. LAN (Local Area Network): es una red local que pertenece a la misma organización y están conectados dentro de un área.

22. Líneas arrendadas dedicadas: es un contrato de servicios entre un ISP y un cliente, por lo que el ISP se compromete a entregar una línea de Internet simétrica.

23. Módem: es un dispositivo que convierte las señales digitales en analógicas (modulación) y las señales analógicas en digitales (desmodulación), lo cual permite la comunicación entre computadoras a través de la línea telefónica o del cable módem.

24. MPLS (Multi Protocol Label Switching): es un protocolo que funciona en la capa de enlace y de red, MPLS está desplazando rápidamente a frame relay y ATM como la tecnología más usada para llevar datos de alta velocidad y voz digital en una sola conexión. MPLS proporciona una mayor fiabilidad y un mayor rendimiento, con una mayor eficiencia de la red. MPLS da prioridad a los paquetes que transportan tráfico de voz lo que es ideal para las comunicaciones VoIP.

25. NIC (Network Interface Card): es un componente de hardware que conecta una computadora a una red informática y que posibilita compartir recursos en una red.

26. NVR (network video recorder): Es un software que se encarga de grabar vídeo en formato digital y almacenarlo en un disco duro.

27. Puerto rj-45: es una interfaz física utilizada para conectar redes de computadoras con cableado estructurado (categorías 4, 5, 5e, 6 y 6a).

28. Troncal 802.1Q: es una troncal que se configura en un switch para permitir que múltiples VLAN entren y salgan por la red sin colisionar.

29. OSI (Open System Interconnection): es un modelo de referencia para los protocolos de arquitectura de red, formado por siete niveles que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones. Los niveles son los siguientes: nivel físico, nivel enlace de datos, nivel de red, nivel de transporte, nivel de sesión, nivel de presentación y nivel de aplicación.

30. Peers: son las direcciones de extremo de salida a Internet de cada LAN, donde se configura el Gateway del VPN.

31. QoS (Quality of Service): es el promedio de la calidad de los servicios de una red, tales como tasas de errores, ancho de banda, rendimiento, retraso en la transmisión, disponibilidad, etc.

32. Router: es un dispositivo de nivel de red su función principal es de enrutar la información hasta el destino.

33. SOHO (Small office/home office): son pequeñas LAN que brindan servicio a pocos usuarios finales, por lo que no requieren de una infraestructura costosa.

34. Switch: es un dispositivo de red, su función es de agregar usuarios finales y conectarlos en una o varias VLAN para transmitir información.

35. TCP/IP: es un modelo de referencia para los protocolos de la red de arquitectura, formado por cuatro niveles que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones. los niveles son los siguientes: nivel de acceso al medio, nivel de Internet, nivel de transporte y nivel de aplicación.

36. Telefonía IP: es una tecnología que permite convertir la señal analógica en una digital para poder ser enviada a través de la red hasta el dispositivo de destino.

37. Teléfono IP: son dispositivos de red, tienen como función principal codificar y decodificar la señal de voz.

38. Topología física: es el esquema para representar la conexión física de la red, muestra los tipos de dispositivos de red, la ubicación y como se interconectan a través de cables o de forma inalámbrica.

39. topología lógica: es el esquema para representar la conexión lógica de la red, muestra el direccionamiento y el enrutamiento para intercambiar información en la red.

40. VLAN (Virtual Local Área Network): son redes virtuales creadas dentro de una LAN, su función principal es la de dividir la red para poder administrarlo de forma más segura y reducir el broadcast.

41. VPN gateway: es utilizado para conectar de forma segura dos o más redes dentro de un túnel VPN.

42. VPN client: es un dispositivo final que está buscando servicios de conexión a una VPN.

43. VPN server: se encarga de gestionar las conexiones VPN, la autenticación, gestión de clientes y otros servicios relacionados.

44. VOIP (Voice over Internet Protocol): es un estándar de telefonía que permite la transmisión de voz sobre la Internet.

CAPÍTULO III

ANÁLISIS Y DISEÑO DE UNA RED CONVERGENTE UTILIZANDO VPN

3.1 ANÁLISIS INFRAESTRUCTURA DE RED ACTUAL

3.1.1 Descripción de red actual

La red se divide en dos LAN independientes ubicadas en diferentes ciudades del Perú ambas cuentan con el mismo proveedor de Internet ADSL para facilitar el acceso a la red pública.

- Sede central en Lima Metropolitana: utiliza una topología de red en estrella la cual conecta todas las pc a un mismo dispositivo, teniendo un módem como nodo central entre la LAN y la Internet
- Sucursal en Jauja-Junín: utiliza una topología en estrella, teniendo un módem Internet como nodo central para la comunicación hacia Internet.

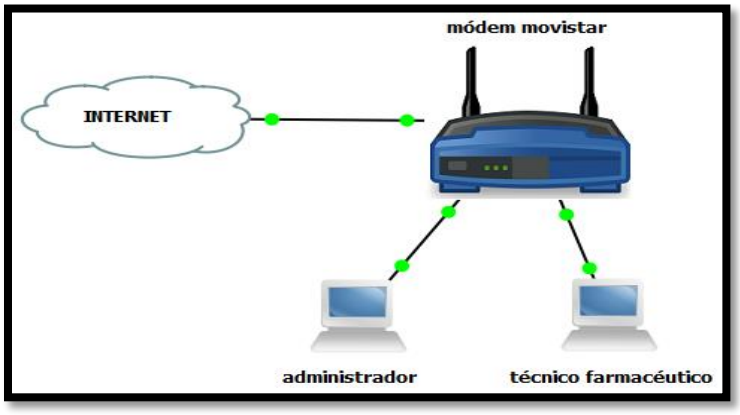


Figura 3.1: Red actual sucursal Jauja
Fuente: propia

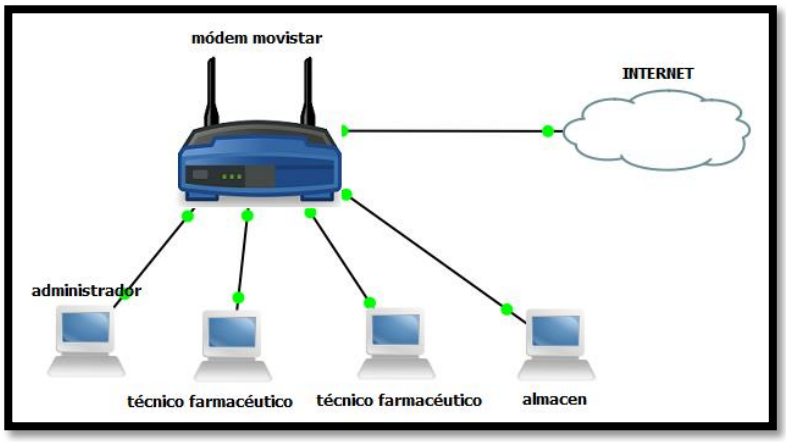


Figura 3.2: Red actual sede central Lima Metropolitana
Fuente: propia

Conexión a Internet actual: la empresa cuenta con el mismo ISP que le da acceso a la red pública con un costo fijo mensual.

- La sede central cuenta con una línea ADSL con un ancho de banda de 4Mbps provista por MOVISTAR, la cual llega a un Modem-Router que provee Internet cableado a 4 equipos (administrador, 2 y un encargado de almacén). La empresa se encuentra limitada con el servicio de telefonía que solo ofrece una línea.

- La sucursal en la ciudad de Jauja: cuenta con una línea ADSL con un ancho de banda de 4Mbps, provista por MOVISTAR, la cual llega a un Modem que provee Internet cableado a 2 equipos (administrador, técnico farmacéutico). La sucursal cuenta con una conexión a telefonía fija la cual debido a estar ubicada en otra localidad las llamadas resultan más costosas.

3.1.2 Equipos utilizados en la actual infraestructura

Modem-Router Equipo entregado por movistar ofrece una conexión por ADSL, con Wifi y 4 puertos Fastethernet; la sede en Lima Metropolitana utiliza un puerto fastethernet por cada computadora por lo que actualmente no posee más salidas fastethernet para la Internet de forma cableada. EL equipo tiene la dirección IP por defecto 192.192.90.1 y viene configurado como servidor DHCP en el rango 192.192.90.0/24. La sucursal en Jauja también posee el mismo modem y una dirección IP por defecto 201.240.162.1/24. La empresa posee una línea de telefonía fija en cada sede, la cual genera gastos extras a la empresa.

3.1.3 Observaciones

La red actual en la sede central carece de puertos adicionales para agregar equipos de red, por lo que se necesitara agregar un Switch para que la red pueda ser escalable y accesible a nuevos usuarios finales. Además la red carece de una

buena segmentación de la red y acceso a la red por lo que ocasiona pérdidas en el ancho de banda.

La red no posee ningún tipo de seguridad con lo que su sistema se encuentra vulnerable a ataques de red o suplantación de dispositivos.

La empresa requiere pagar servicios de telefonías en cada sede, el cual solo le brinda acceso a una línea telefónica en cada sede, además resulta costoso las llamadas a provincia por lo que se genera un gasto adicional cada mes.

3.2 PROPUESTA DEL DISEÑO DE LA RED VPN IPSEC

Las consideraciones primordiales del proyecto, es la de implementar una red segura ante posibles ataques de red que están sucediendo o evitar ataques en el futuro, para ello es necesario crear un entorno seguro y económico; por otro lado también se tiene que vislumbrar que tipo de equipos y sus características para poder realizar el diseño de red en ambas sedes y este pueda ser económico y escalable además de compatible con los protocolos utilizados en la simulación. Se debe tomar en cuenta todos los conocimientos adquiridos en los capítulos anteriores que ayudaran a vislumbrar las formas y funciones que son necesarias para realizar el proyecto.

Se necesita implementar un sistema de seguridad debido a que la información que viaja entre la sede central y su sucursal es importante que no sea modificada, interceptada, ni robada por usuarios ajenos a la empresa, ya que puede ocasionar grandes pérdidas a la empresa.

Se necesita implementar un VPN site-to-site para que la información viaje cifrada y segura. Un túnel VPN IPsec resulta una buena opción por su costo y la poca demanda de usuarios que usaran el servicio.

Es necesario implementar medidas de seguridad física por lo que se considera adicionar un switch con 16 puertos que soporte VLAN's para conectar todos los equipos de la LAN con lo que se podrá dividir la red en diferentes áreas que requieran diferente tipo de información.

Se requiere crear una red convergente segura y económica que ofrezca servicios de datos, voz y video. Por lo que es necesario implementar VLAN's para cada tipo de red.

Con la creación de un servicio de telefonía IP la empresa podrá realizar llamadas interprovinciales con duración indefinida y sin costo adicional alguno a través de la Internet, lo que genera un ahorro en los servicios de telefonía que se tenía que pagar en cada sede. Además de brindarle una seguridad adicional a las llamadas debido a que no podrán ser interceptadas por usuarios ajenos a las empresas debido a que la señal de voz viajara a través del túnel VPN IPsec.

3.2.1 Descripción de la nueva red propuesta

La nueva red requiere reemplazar el módem en cada sede por un router para poder configurar el protocolo VPN IPsec, VoIP además de generar el tráfico entre VLAN’s, entre otras configuraciones de seguridad. Se necesitaran nuevos equipos

de redes para poder segmentar la red, dispositivos de seguridad, dispositivo de routing y un teléfono IP para la comunicación a través de Internet.

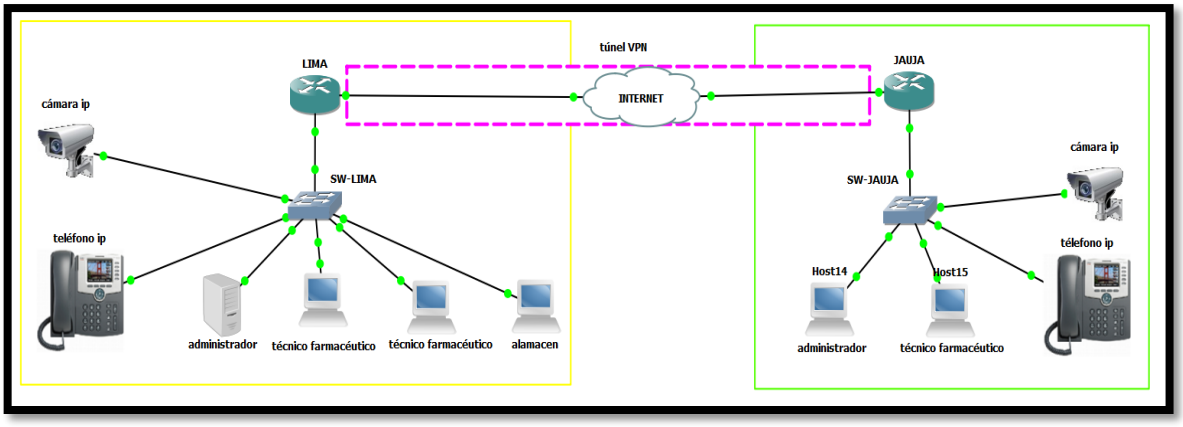


Figura 3.3: Diseño de la red VPN IPsec Lima-Jauja
Fuente: propia

Router Cisco 836

El router cisco 836 posee una entrada directa ADSL por lo que no resulta necesario un Gateway para la entrada a Internet, los routers serie 800 son routers diseñados para redes empresariales SOHO por lo que su costo es bajo en comparación con otros router que necesitan enrutar mucho tráfico.

El enrutador Cisco 836 ofrece servicios integrados de seguridad de clase empresarial, entre los que se incluyen el cifrado de seguridad IP (IPSec), el cifrado 3DES (Triple Data Encryption Standard) para redes privadas virtuales (VPN) y un firewall de inspección de estado para la conectividad segura a Internet. Funciones avanzadas opcionales, como Cisco Easy VPN Remote (una función de software que permite la implementación y administración sencillas de VPN); Seguridad de infraestructura de clave pública (PKI) que requiere certificados digitales; transparencia de traducción de direcciones de red IPSec (NAT-T); El sistema de

detección de intrusos (IDS) de Cisco; el cifrado AES y el filtrado de URL. Garantizan que la pequeña oficina reciba el nivel más alto de seguridad, lo que contribuye a la seguridad de la red corporativa.

Voz y vídeo de alta calidad y seguridad

La QoS avanzada y las funciones de encriptación de alto rendimiento del enrutador Cisco 836 proporcionan servicios de voz y video de alta calidad a usuarios remotos. Cuando los teléfonos IP están conectados en un sitio remoto, un enrutador Cisco 836 puede poner en cola y priorizar el tráfico de voz sobre el tráfico de datos para asegurar una conexión de voz sobre IP (VoIP) segura de alta calidad desde el red.

Figura 3.4: Router cisco 836
Fuente: https://goo.gl/rJvilZ

Cisco Catalyst 2960-L con 16 puertos

Es un switch de gran valor que lo ayuda a aumentar la confiabilidad en sucursales. los switch de la serie Cisco Catalyst 2960-L proporcionan una serie de funciones de seguridad para limitar el acceso a la red y mitigar las amenazas, entre ellas:

● La autenticación multidominio permite que un teléfono IP y un PC se autentiquen en el mismo puerto del conmutador mientras los colocan en las VLAN apropiadas de voz y datos.

● Listas de control de acceso (ACL) para IPv6 e IPv4 para seguridad y QoS ACE: las ACL basadas en puertos para las interfaces de capa 2 permiten que las políticas de seguridad se apliquen en puertos de conmutador individuales.

● El protocolo Secure Shell (SSH), Kerberos y el protocolo de gestión de red simple versión 3 (SNMPv3) proporcionan seguridad de red al cifrar el tráfico de administrador durante las sesiones Telnet y SNMP.

● La notificación de la dirección MAC permite a los administradores ser notificados sobre los usuarios agregados o eliminados de la red.

● La seguridad multinivel en el acceso de la consola evita que los usuarios no autorizados alteren la configuración del switch.

● La asignación de VLAN dinámica se soporta a través de la implementación de la capacidad del cliente del servidor de directivas de pertenencia a VLAN para proporcionar flexibilidad en la asignación de puertos a VLAN. VLAN dinámica facilita la asignación rápida de direcciones IP.

Figura 3.5: Catalyst 2960-L
Fuente: https://goo.gl/lyVYeb

Teléfono IP 7931G Cisco

El teléfono IP de Cisco es un teléfono con todas las funciones necesarias que permite la comunicación por voz sobre la misma red de datos que utiliza el equipo. Su funcionamiento es similar al de un teléfono analógico tradicional ya que permite realizar y recibir llamadas.

El teléfono IP 7931G de Cisco Unified está diseñado para crecer con la empresa. Un conjunto dinámico de funciones activas permite al teléfono mantenerse a la altura de las necesidades mediante actualizaciones regulares del software. Principales características:

- Los indicadores LED de color indican el estado de la llamada/línea
- No se necesita cable de alimentación eléctrica
- Botones para retención, transferencia y rellamada
- Integrado con Cisco Unified Communications Manager y Cisco Unified Communications Manager Express

Figura 3.6: Cisco Unified IP Phone 7931G
Fuente: https://goo.gl/vqpPhj

Cámara IP WVC80N

Las cámaras IP son una buena alternativa a las clásicas alarmas ya que son capaces de enviar audio y vídeo, así como fotos cuando detecta movimiento. Podemos configurar en el destino un servidor FTP o informar a través del correo electrónico del movimiento.

La cámara Linksys WVC80N ofrece un vídeo/audio de buena calidad, es una cámara que se conecta al router a través de WIFI o ethernet, el envío de audio y vídeo se hace a través del servidor web.

La resolución máxima de la cámara es 640×480, por lo que no es HD, el formato de archivo de grabación es ASF y AVI, brinda la posibilidad de ver en tiempo real el estado de nuestro hogar desde un smartphone o tablet.

Costo de equipos e instalación por sede

SEDE-LIMA			
Equipo	Cantidad	Precio(dólares)	TOTAL
Router cisco836	1	649	649
Catalyst 2960-L	1	679	679
Teléfono IP 7931G	1	120	120
Cámara IP WVC80N	1	100	100
Fuente y cableado	1	30	30
Instalación	1	200	200
TOTAL			1778

Tabla 3.1: Costo de equipos e instalación por sede
Fuente: propia

3.2.2 Configuración de la red propuesta

Para comprobar el óptimo funcionamiento del diseño de una red convergente VPN IPsec, se ha implementado la configuración del diseño de red en el simulador GNS3 y Packet tracer. Para garantizar al máximo la seguridad de la red tanto física como a través de Internet, se ha implementado los siguientes protocolos y configuraciones.

- ACL: se encarga de filtrar el tipo de contenido que ingresa o sale de la red, así como los usuarios permitidos a esta.
- DHCP: brinda direcciones automáticas a usuarios finales.
- IP static: para asignar direcciones fijas a usuarios finales.
- Loopback: brinda una dirección virtual para el diagnóstico de conectividad y validez del protocolo de comunicación.
- MOTD: mensaje para advertir acceso a usuarios finales.
- OSPF: se encarga de simular un entorno de conectividad WAN.
- Password: se han implementado diferentes contraseñas para diferentes niveles como: telnet, consola y acceso a usuario privilegiado.
- Router on stick: se encarga de generar routing entre VLANs a través de un solo puerto y otorga conectividad a la red.
- SSH: este protocolo es utilizado para acceder a la configuración de equipos de forma remota.
- Switchport security: su función es de asignar una dirección MAC a una interfaz especifica con lo que se evita la suplantación de equipos.

- VLAN: se encarga de dividir la red en grupos específicos para una mejor administración.
- VoIP: se encarga de habilitar líneas de comunicación para teléfonos IP.
- VPN IPsec: este protocolo creara un túnel virtual para que toda la información que viaje entre las sedes sea segura.

Direccionamiento de la red

El diseño de la red cuenta con dos tipos de direccionamiento: direccionamiento estático ipv4 para las computadoras y cámaras; debido a que se necesita acceder de forma remota para compartir información y para garantizar la información. Direccionamiento en DHCP es usado para asignar direcciones de un rango se le otorga a los teléfonos IP para facilitar su conectividad.

La red se ha dividido en 3 sudredes para la asignación de las diferentes VLANs y se otorgado un loopback para obtener acceso remoto.

SEDE	INTERFAZ	DIRECCION	MASCARA
ROUTER SEDE-LIMA	Fa0/1	192.200.1.1	255.255.255.252
	fa0/0.10	192.192.90.33	255.255.255.224
	fa0/0.20	192.192.90.1	255.255.255.224
	fa0/0.30	192.192.90.65	255.255.255.224
	loopback 1	192.200.90.100	255.255.255.255
ROUTER SEDE-JAUJA	Fa0/1	201.240.172.1	255.255.255.252
	fa0/0.10	201.240.162.33	255.255.255.224
	fa0/0.20	201.240.162.1	255.255.255.224
	fa0/0.30	201.240.162.65	255.255.255.224
	loopback 1	201.240.172.100	255.255.255.255

Tabla 3.2: Direccionamiento IP routers
Fuente: propia

SWITCH LIMA	INTERFAZ	CLIENTE	VLAN
LIMA	f0/2	ADMINISTRADOR	20
	f0/3	TECNICO FARMACEUTICO 1	20
	f0/4	TECNICO FARMACEUTICO 2	20
	f0/5	ALMACEN	20
	f0/6	TELEFONO IP	10
	f0/7	CAMARA IP	30
	F1/0	TRONCAL	10,20,30
JAUJA	f0/2	ADMINISTRADOR	20
	f0/3	TECNICO FARMACEUTICO 1	20
	f0/6	TELEFONO IP	10
	f0/7	CAMARA IP	30
	F1/0	TRONCAL	10,20,30

Tabla 3.3: Interfaces de switches
Fuente: propia

VLAN LIMA	NOMBRE	RED	DISPOSITIVO	IPV4 DISPOSITIVO
10	VOZ	192.192.90.32/27	TELEFONO IP	DHCP
20	DATOS	192.192.90.0/27	ADMINISTRADOR	192.192.90.10
			TECNICO FARMACEUTICO 1	192.192.90.3
			TECNICO FARMACEUTICO 2	192.192.90.4
			ALMACEN	192.192.90.5
30	VIDEO	192.192.90.64/27	CAMARA IP	192.192.90.66
VLAN JAUJA	NOMBRE	RED	DISPOSITIVO	IPV4 DISPOSITIVO
10	VOZ	201.240.162.32/27	TELEFONO IP	DHCP
20	DATOS	201.240.162.0/27	ADMINISTRADOR	201.240.162.10
			TECNICO FARMACEUTICO	201.240.162.3
30	VIDEO	201.240.162.64/27	CAMARA IP	201.240.162.66

Tabla 3.4: Asignación de VLAN's
Fuente: propia

Configuración del switch Lima Metropolitana

El switch es un medio de acceso a usuarios finales por lo cual se tomar medidas de seguridad para evitar dispositivos que pueden ocupar ancho de banda o robar información. La configuración del switch de Jauja es similar al switch de

Lima, el switch de Lima implementa servicio de contraseña modo consola, telnet y acceso a modo privilegiado. Se configura los puertos para que admitan solo una MAC específica y se define que puerto tendrá acceso a que VLAN.

La programación específica se adjunta en el anexo 1 para Lima y anexo 2 para Jauja.

Configuración del router Lima Metropolitana

La configuración en el router de Lima implementa servicio de contraseña modo consola, telnet y acceso a modo privilegiado. Se crea una interfaz loopback para el diagnóstico de conectividad además se implementa OSPF para poder simular una red WAN a través de la Internet. Se implementa el protocolo VPN IPsec en los puertos extremos de la red, con un algoritmo de cifrado simétrico aes de 256 bits.

La programación específica se adjunta en el anexo 3 para Lima, anexo 4 para Jauja.

Pruebas y Simulación

Para un mejor entendimiento y verificación del óptimo funcionamiento de una red convergente con VPN IPsec se ha optado realizar una simulación en el software Cisco packet tracer, debido a que este es un software propietario de Cisco el cual simula de manera precisa sus diferentes dispositivos de red.

Teniendo la sede central en Lima como la sucursal en Jauja se realiza pruebas de conectividad dentro y fuera de la red para garantizar que los datos puedan llegar a su dirección de destino.

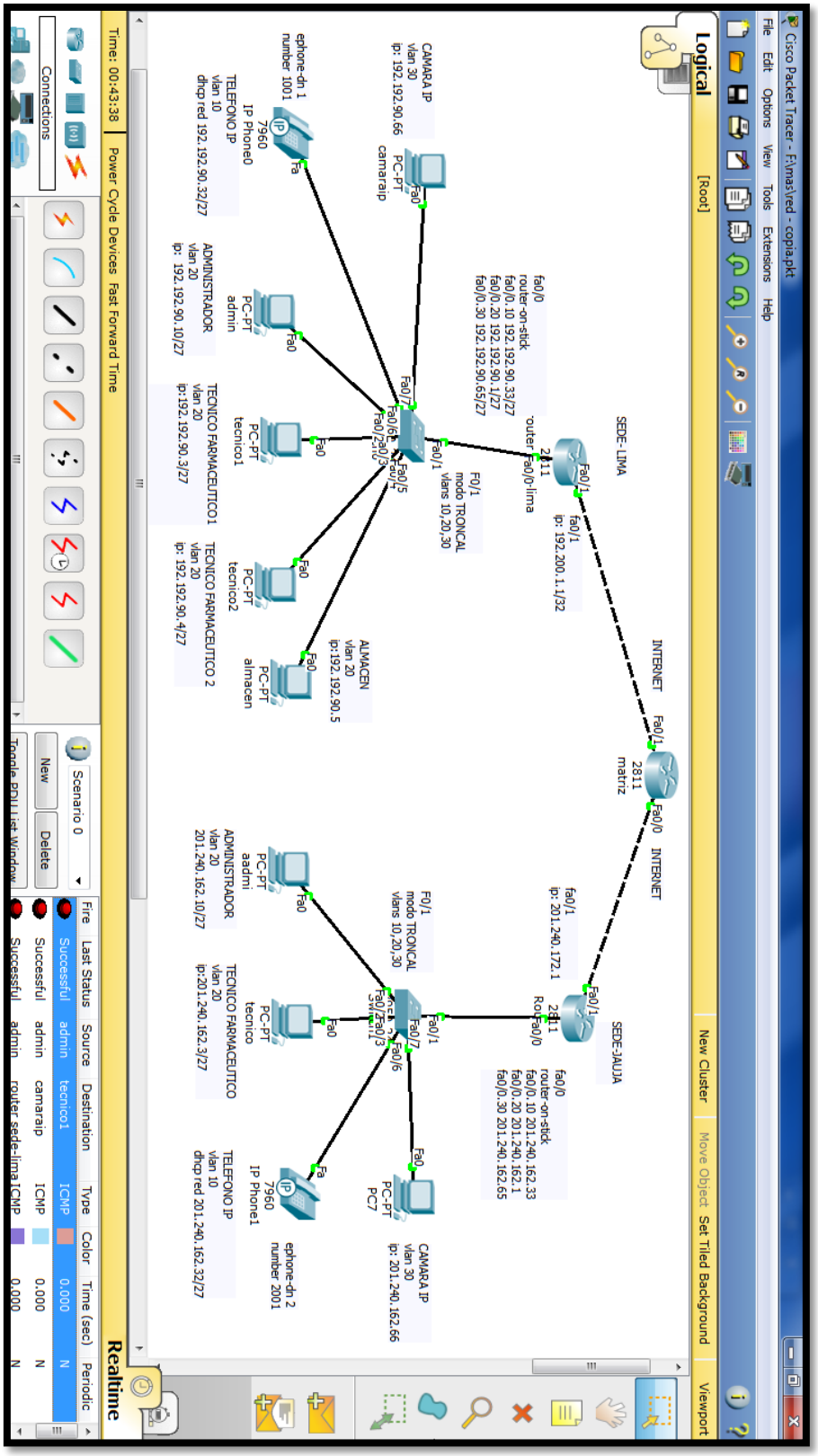


Figura 3.7: Simulación y prueba red convergente
Fuente: propia

Para verificar la conexión entre redes se realiza una llamada a través de Internet mediante telefonía IP, para la sede en jauja se tiene el numero 2001 mientras que para lima se tiene el numero 1001

Figura 3.8: Prueba de telefonía IP
Fuente: propia

La configuración de telefonía IP se realiza entre los routers de cada sede, los teléfonos IP no cuentan con una dirección IP fija por lo que se le asigna una a través de DHCP pero estos se identifican a través de un número que se configura de forma manual.

router sede lima

```
!
ip dhcp pool VOIP
 network 192.192.90.32 255.255.255.224
 default-router 192.192.90.33
 option 150 ip 192.192.90.33
 dns-server 8.8.8.8
!
!
!
!
dial-peer voice 2000 voip
 destination-pattern 200
 session target ipv4:192.192.90.33
!
telephony-service
 max-ephones 10
 max-dn 10
 ip source-address 192.192.90.33 port 2000
!
ephone-dn 1
 number 1001
!
ephone 1
 device-security-mode none
 mac-address 00D0.BA8B.4609
 type 7960
 button 1:1
```

router sede jauja

```
ip dhcp pool VOIP
 network 201.240.162.32 255.255.255.224
 default-router 201.240.162.33
 option 150 ip 201.240.162.33
 dns-server 8.8.8.8
!
!
!
!
dial-peer voice 2000 voip
 destination-pattern 200
 session target ipv4:201.240.162.33
!
telephony-service
 max-ephones 10
 max-dn 10
 ip source-address 201.240.162.33 port 2000
!
ephone-dn 1
 number 2001
!
ephone 1
 device-security-mode none
 mac-address 00D0.BA8B.9609
 type 7960
 button 1:1
```

Figura 3.9: Configuración telefonía IP
Fuente: propia

Para probar que el túnel VPN IPsec funcione correctamente debe existir conexión entre ambos extremos mediante un ping.

```
SEDE-LIMA#ping 201.240.172.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 201.240.172.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/24 ms


SEDE-JAUJA#ping 192.200.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.200.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Figura 3.10: Prueba de ping entre LANs
Fuente: propia

Se verifica el correcto funcionamiento del túnel IPSEC mediante los comandos: show crypto ISAKMP SA y show crypto IPSEC SA.

```
SEDE-LIMA#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
201.240.172.1   192.200.1.1     QM_IDLE           1037    0 ACTIVE

IPv6 Crypto ISAKMP SA


SEDE-LIMA#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: GESTION, local addr 192.200.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 201.240.172.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

    local crypto endpt.: 192.200.1.1, remote crypto endpt.:201.240.172.1
    path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
    current outbound spi: 0x176214A1(392303777)

     inbound esp sas:
      spi: 0x504559C1(1346722241)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: FPGA:1, crypto map: GESTION
        sa timing: remaining key lifetime (k/sec): (4525504/3531)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x176214A1(392303777)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: GESTION
        sa timing: remaining key lifetime (k/sec): (4525504/3531)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

Figura 3.11: Prueba de show crypto ISAKMP SA y show crypto IPSEC SA
Fuente: propia

La configuración se puede verificar que en ambos routers es muy similar solo se tiene en cuenta el cambio de vpn Gateway en cada sede que siempre debe ser diferente

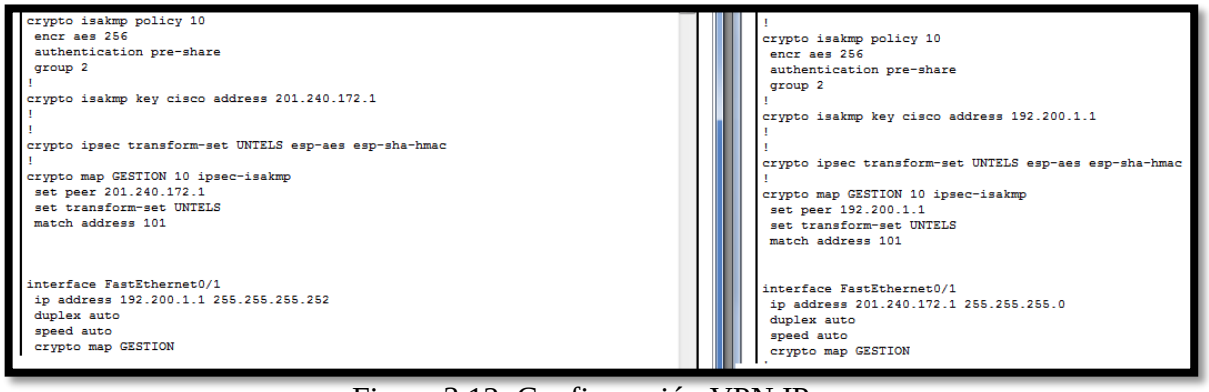


Figura 3.12: Configuración VPN IPsec
Fuente: propia

3.2.3 Pruebas y resultados

Para realizar el diseño de una red convergente utilizando VPN IPSEC entre la central de una farmacia localizada en Lima Metropolitana y su sucursal en Jauja-Junín, se diseñó la topología de red en el simulador oficial de CISCO PACKET TACER versión 6, como se puede observar en la figura 3.7. En la figura se observa 2 redes LAN las cuales se interconectadas a través de una WAN las cuales realizan ping entre ellas con resultado successfull(exitoso).

Para la topología de la red convergente se tiene 2 redes LAN del cliente (Lima y Jauja) las cuales se encuentran a cientos de kilómetros de distancia. A través de los router de borde se realiza una configuración en su puerto WAN para crear un túnel lógico mediante el protocolo VPN IPSEC una vez generado el enlace lógico se agrega los comandos para que la información viaje encriptada con el algoritmo AES la cual garantizara al cliente que su información no sea interceptada por

usuarios ajenos a la información. Siendo para el cliente una acción invisible ya el proceso de encriptación y desencriptación de datos solo se da en los puertos WAN y no en los LAN como se observa en la figura 3.10.

Para el diseño de la VLAN de voz (telefonía IP) se utiliza los módulos virtuales de telefonía donde se le asigna un número estático y propio en cada teléfono de las 2 sedes (figura 3.9). Se observa mediante la imagen 3.8 los resultados de la conectividad existente entre las 2 sedes para el enlace de voz.

Mediante el comando #show crypto isakmp sa, se puede verificar la prueba de un enlace dando como resultado un estado activo para las 2 LAN interconectadas, por la cual la información enviada entre ellas se encriptada y desencintara para que la información del cliente no pueda ser interceptada por usuarios ajenos a la empresa.

Mediante el comando #show crypto ipsec sa, se puede verificar la prueba de un enlace VPN IPSEC dando como resultado un enlace exitoso, como se puede observar en la figura 3.11 todos los datos encriptados en una sede fueron desencriptados exitosamente en la otra sede lo que garantiza que no existe perdida de información.

Mediante el comando #show running-config, se puede verificar la configuración implementada en el router. Se observa en la figura 3.12 las redes LAN implementadas en cada sede y como se implementó el protocolo VPN IPSEC con encriptación AES en cada sede para realizar la prueba de conectividad respectiva.

3.3 REVISIÓN Y CONSOLIDACIÓN DE RESULTADOS

La implementación del diseño de red convergente con seguridad IPsec representa un gran avance en el crecimiento de la empresa ya que garantiza su óptimo funcionamiento en la seguridad de la red. Al dividir la red en VLAN's se ha optimizado el uso de ancho de banda, además de brindar seguridad en los puertos de acceso físico.

Con la implementación de un sistema de telefonía IP, el uso de un proveedor de telefonía ya no resultara necesario con lo que se ahorra en gastos mensuales de telefonía cuya suma promedio era de 300 nuevos soles.

La implementación de la red convergente con seguridad VPN IPsec tiene un costo de equipo y ejecución de 1778 dólares por cada sede, el cual será recuperado a mediano plazo con el nuevo sistema de telefonía que evitara seguir pagando los 300 nuevos soles. Además se tendrá una reducción en los costos de viajes operativos para supervisión de la sucursal y se asegura la información de ventas y facturas, considerando que la sucursal factura 250 nuevos soles en productos por día mientras que la sede central tiene una factura 1500 soles por día, la empresa necesita un medio seguro para almacenar esa información en su base de datos en Lima Metropolitana por lo que es necesario un uso de un puente virtual para cifrar la información y evitar que personal ajeno conozca dicha información.

La implementación de un sistema de seguridad remoto a través de Internet mediante cámara IP, garantiza al dueño de la empresa poder observar y

supervisar la producción de su sucursal en cualquier momento sin que tenga que realizar largos viajes con lo que se genera un ahorro.

Resultado

El resultado económico de las 2 sedes se consolida en un archivo en formato Excel, el cual almacena los datos por renta de servicios de comunicaciones por los 12 meses(2016).

MES	SEDE CENTRAL	SUCURSAL
ENERO	350	300
FEBRERO	345	295
MARZO	317	267
ABRIL	295	245
MAYO	270	220
JUNIO	218	168
JULIO	258	208
AGOSTO	258	208
SEPTIEMBRE	297	247
OCTUBRE	312	262
NOVIEMBRE	321	271
DICIEMBRE	360	310
PROMEDIO	300	250

Tabla 3.5: Renta de servicios de comunicaciones 2016

Análisis de datos

Para la implementación de la red convergente de voz y data se considera una inversión inicial de 1778 dólares o 5800 soles por servicio de configuración, instalación y venta de nuevos equipos, además de una renta mensual de 79 soles solo por servicio de Internet público.

Tiempo de recuperación de inversión

Para esta evaluación se considera el tiempo en el cual se recupera la inversión inicial realizada, teniendo en cuenta que la renta promedio del servicio de telefonía e Internet que tenía la empresa en el año 2016 para la sede principal es de 300 soles y la nueva renta mensual a contratar será de 79 soles mensuales.

Se tiene:

- Precio promedio de servicio en el 2016 = 300 soles.
- Precio promedio de nuevo servicio en el 2017 =79 soles.
- Diferencia en el precio del servicio = 221 soles.

Para el nuevo servicio se tiene un ahorro de 221 soles. Sin embargo el nuevo servicio requiere de una inversión inicial por concepto de instalación, configuración y venta de equipos.

Teniendo:

- Precio de instalación, configuración y equipos en el 2016 = 0 soles.
- Precio de instalación, configuración y equipos en el 2017 = 5800 soles.
- Diferencia en el precio del servicio = 5800 soles.

A diferencia con el anterior servicio el cual la renta mensual de 300 soles incluía el servicio de alquiler de equipo, en el nuevo servicio el dueño de la empresa será el dueño de los equipos por lo cual requerirá una inversión única por conceptos de instalación configuración y equipamiento de 5800 soles.

De lo mencionado se obtiene los siguientes datos y ecuaciones para obtener el tiempo de recuperación de inversión para la sede central.

Datos:

- Renta 2016 = 300
- Renta 2017= 79
- Inversión inicial = 5800
- Cantidad de meses = M
- Tiempo = T

Ecuación 1: (Renta 2016 X M) = T

Ecuación 2: ((Inversión inicial) + (Renta 2017 X M)) = T

- Reemplazando los datos e igualando las ecuaciones se obtiene:

300M = 5800 + 79M

300M – 79M = 5800

M = 26.2443 **->** para el estudio se aproxima a 27 meses.

Para la sede central se tiene un tiempo de recuperación de inversión de 27 meses.

- Reemplazando los datos e igualando las ecuaciones para la sucursal se obtiene:

250M=5800+79M

171M=5800

M=33.91 **->** para el estudio se aproxima a 34 meses.

Para la sucursal se tiene un tiempo de recuperación de inversión de 34 meses.

CONCLUSIONES

1. En base al estudio realizado se concluye que es factible la transmisión de información a través de Internet del servicio de voz y datos en forma encriptado; sin que la información enviada y recibida se pierda o se modifique entre la sede central y su sucursal.

2. A través del estudio realizado se pudo verificar que al utilizar el protocolo VPN IPsec con algoritmo de encriptación AES, todos los paquetes que son encapsulados en una sede se desencapsulan en su totalidad en la otra sede (figura 3.11); por lo cual se verifica que no existe perdidas de datos.

3. Mediante el diseño realizado se obtuvo que al utilizar la encriptación con algoritmo AES, el tiempo de latencia para la transmisión de datos entre la sede central y su sucursal es máximo de 24 milisegundos (como se muestra en la figura 3.10) por lo que al implementar un servicio VoIP no habría retraso de transmisión en tiempo real ni interferencias.

4. Mediante el diseño realizado (figura 3.7) se verifica que al implementar un switch se liberan puertos en el router de tal forma que existen 3 puertos libres para la implementación de nuevas sucursales o servicios redundantes. Además se verifica la disponibilidad de 7 puertos libres en el switch para la implementación de nuevos usuarios finales.

5. A través del estudio realizado se concluye que en la actualidad el uso de la Internet es imprescindible para el crecimiento continuo de las empresas ya que en la actualidad las grandes empresas realizan transacciones internas como externas mediante este medio. El utilizar la Internet pública con un entorno seguro como medio de comunicación, genera un gran beneficio y una buena rentabilidad para las MYPES y PYMES ya que mediante este medio se garantiza que puedan establecer comunicación interna entre su sede principal y su sucursal de manera segura utilizando un túnel virtual y encriptado generado por el protocolo VPN IPSEC. Otorgando al cliente un servicio de calidad en un ambiente constituido por seguridad, disponibilidad, escalabilidad y compatibilidad. Mediante este medio se garantiza que la información acerca de los procesos de almacén, ventas, costos de productos, pagos internos y externos entre otros viajen por un entorno seguro dándole a la empresa una significante mejora y por ende el aumento en la imagen corporativa.

RECOMENDACIONES

1. Antes de implementar cualquier proyecto basado en redes de área local se recomienda realizar los cálculos teóricos para obtener una adecuada cantidad de usuarios finales actuales como futuros, para evitar problemas de infraestructura con el procesamiento de datos y el número de puertos en el futuro.

2. Se recomienda el uso y registro de direcciones IP estáticas para la mejor administración de la red, así como para conocer el uso del ancho de banda en cada usuario, con lo que se podrá implementar listas de control de acceso para ciertas VLAN's o solo a un usuario final en específico que utilice el ancho de banda de forma inapropiada.

3. Se recomienda utilizar claves con más de 10 caracteres que incluyan mayúsculas, minúsculas, símbolos y números; también es necesario renovar las contraseñas periódicamente para mantener la seguridad de la empresa, así como dar mantenimiento preventivo a los equipos de conectividad.

4. Se recomienda utilizar en el diseño de la red un mismo proveedor de dispositivos de red, con el fin de garantizar un óptimo funcionamiento y compatibilidad de equipos, para el caso del proyecto se ha empleado productos Cisco.

5. Se recomienda replicar esta solución en empresas similares del sector PYMES con iguales necesidades, para mejorar su gestión operativa y de control de las comunicaciones con los beneficios de seguridad y economía que ofrece VPN IPsec.

BIBLIOGRAFÍA

- Cisco System, INC. (2011). Cisco Small Business Configuration Assistant Cisco Version 3.0, U.S.A.
- Cisco System, INC. (2011). Wireless-N internet home monitoring camera, U.S.A.
- Yi Yang. (2011). Virtual Private Network Management. Facultad Politécnica en Mikkeli University of Applied Sciences, Finlandia.
- Jeremy Cioara. (2012). CCNA voice 640-461 official cert guide library, U.S.A.
- Ricardo Menéndez. (2012). Estudio del desempeño e implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos. Facultad de Ciencias e Ingeniería de La Pontificia Universidad Católica del Perú.
- Eduardo Alva. (2013). Desarrollo e implementación de una herramienta gráfica para la configuración remota de una VPN con routers Cisco. Facultad de Ciencias e Ingeniería de La Pontificia Universidad Católica del Perú.
- Todd Lammle. (2013). CCNA Routing and Switching study guide, U.S.A.
- David Hucaby. (2014). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide, U.S.A.
- Kevin Wallace. (2015). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide, U.S.A.
- Rodoya Takele Degefa. (2015). VPN Scenarios, Configuration and Analysis. Facultad de Ingenieria e Información de Helsinki Metropolia University of Applied Sciences, Finlandia.

- Wendell Odom. (2016). CCNA Routing and Switching 200-125 Official Cert Guide Library, U.S.A.
- Cisco Networking Academy Program (2016), módulo 1: Introducción a redes v5.0.
- Cisco Networking Academy Program (2016), módulo 2: Principios básicos de routing y switching v5.0.
- Cisco Networking Academy Program (2016), módulo 3: Escalamiento de Redes v5.0.
- Cisco Networking Academy Program (2017), módulo 4: conexión de Redes v6.0.
- Router-switch(2017): productos Cisco, marzo, 5,2017, de router-switch sitio web:http://www.router-switch.com

Anexo I: Configuración del switch Lima Metropolitana

Switch>enable

Switch#configure terminal

Switch(config)#hostname sw-lima

sw-lima(config)#vlan 10

sw-lima(config-vlan)#name voz

sw-lima(config-vlan)#vlan 20

sw-lima(config-vlan)#name datos

sw-lima(config-vlan)#vlan 30

sw-lima(config-vlan)#name video

sw-lima(config-vlan)#exit

sw-lima(config)#enable secret Untels2017

sw-lima(config)#line console 0

sw-lima(config-line)#password Titulacion2017

sw-lima(config-line)#login

sw-lima(config-line)#exit

sw-lima(config)#line vty 0 4

sw-lima(config-line)#password Electronica2017

sw-lima(config-line)#login

sw-lima(config-line)#exec-timeout 90

sw-lima(config-line)#transport input ssh

sw-lima(config-line)#exit

sw-lima(config)#ip domain-name cisco.com

```
sw-lima(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
sw-lima(config)#username omar secret zapata
*mar 1 0:2:13.241:  %SSH-5-ENABLED: SSH 1.99 has been enabled
sw-lima(config)#ip ssh version 2
sw-lima(config)#banner motd $ acceso restringido $
sw-lima(config)#interface fastethernet 0/2
sw-lima(config-if)#description administrador
sw-lima(config-if)#no shutdown
sw-lima(config-if)#switchport mode access
sw-lima(config-if)#switchport access vlan 20
sw-lima(config-if)#switchport port-security mac-address sticky
sw-lima(config-if)#exit
sw-lima(config)#interface fastethernet 0/3
sw-lima(config-if)#description tecnico farmaceutico 1
sw-lima(config-if)#no shutdown
sw-lima(config-if)#switchport mode access
sw-lima(config-if)#switchport access vlan 20
sw-lima(config-if)#switchport port-security mac-address sticky
sw-lima(config-if)#exit
sw-lima(config)#interface fastethernet 0/4
sw-lima(config-if)#description tecnico farmaceutico 2
sw-lima(config-if)#no shutdown
```

sw-lima(config-if)#switchport mode access

sw-lima(config-if)#switchport access vlan 20

sw-lima(config-if)#switchport port-security mac-address sticky

sw-lima(config-if)#exit

sw-lima(config)#interface fastethernet 0/5

sw-lima(config-if)#description almacen

sw-lima(config-if)#no shutdown

sw-lima(config-if)#switchport mode access

sw-lima(config-if)#switchport access vlan 20

sw-lima(config-if)#switchport port-security mac-address sticky

sw-lima(config-if)#exit

sw-lima(config)#interface fastethernet 0/6

sw-lima(config-if)#description telefono ip

sw-lima(config-if)#no shutdown

sw-lima(config-if)#switchport mode access

sw-lima(config-if)#switchport access vlan 10

sw-lima(config-if)#switchport voice vlan 10

sw-lima(config-if)#switchport port-security mac-address sticky

sw-lima(config-if)#exit

sw-lima(config)#interface fastethernet 0/7

sw-lima(config-if)#description camara ip

sw-lima(config-if)#no shutdown

sw-lima(config-if)#switchport mode access

```
sw-lima(config-if)#switchport access vlan 30
sw-lima(config-if)#switchport port-security mac-address sticky
sw-lima(config-if)#exit
sw-lima(config)#interface range fastethernet 0/8-24
sw-lima(config-if-range)#shutdown
sw-lima(config-if-range)#exit
sw-lima(config)#interface fa0/1
sw-lima(config-if)#switchport mode trunk
sw-lima(config-if)#switchport trunk allowe vlan 10,20,30
sw-lima(config-if)#end
sw-lima(config)#interface vlan 1
sw-lima(config-if)# ip address 192.200.90.101 255.255.255.224
sw-lima(config-if)# no shutdown
sw-lima(config-if)#exit
sw-lima(config)# ip default-gateway 192.200.90.100
sw-lima(config-if)#end
sw-lima#copy running-config startup-config
```

Anexo II: Configuración del switch Jauja

Switch>enable

Switch#configure terminal

Switch(config)#hostname sw-jauja

sw-jauja(config)#vlan 10

sw-jauja(config-vlan)#name voz

sw-jauja(config-vlan)#vlan 20

sw-jauja(config-vlan)#name datos

sw-jauja(config-vlan)#vlan 30

sw-jauja(config-vlan)#name video

sw-jauja(config-vlan)#exit

sw-jauja(config)#

sw-jauja(config)#enable secret Untels2017

sw-jauja(config)#line console 0

sw-jauja(config-line)#password Titulacion2017

sw-jauja(config-line)#login

sw-jauja(config-line)#exit

sw-jauja(config)#line vty 0 4

sw-jauja(config-line)#password Electronica2017

sw-jauja(config-line)#login

sw-jauja(config-line)#exec-timeout 90

sw-jauja(config-line)#transport input ssh

sw-jauja(config-line)#exit

```
sw-jauja(config)#
sw-jauja(config)#ip domain-name cisco.com
sw-jauja(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
sw-jauja(config)#username omar secret zapata
sw-jauja(config)#
sw-jauja(config)#ip ssh version 2
sw-jauja(config)#
sw-jauja(config)#banner motd $ acceso restringido $
sw-jauja(config)#interface fastethernet 0/2
sw-jauja(config-if)#description administrador
sw-jauja(config-if)#no shutdown
sw-jauja(config-if)#switchport mode access
sw-jauja(config-if)#switchport access vlan 20
sw-jauja(config-if)#switchport port-security mac-address sticky
sw-jauja(config-if)#exit
sw-jauja(config)#
sw-jauja(config)#interface fastethernet 0/3
sw-jauja(config-if)#description tecnico farmaceutico
sw-jauja(config-if)#no shutdown
sw-jauja(config-if)#switchport mode access
sw-jauja(config-if)#switchport access vlan 20
sw-jauja(config-if)#switchport port-security mac-address sticky
```

```
sw-jauja(config-if)#exit
sw-jauja(config)#
sw-jauja(config)#interface fastethernet 0/6
sw-jauja(config-if)#description telefono ip
sw-jauja(config-if)#no shutdown
sw-jauja(config-if)#switchport mode access
sw-jauja(config-if)#switchport access vlan 10
sw-jauja(config-if)#switchport voice vlan 10
sw-jauja(config-if)#switchport port-security mac-address sticky
sw-jauja(config-if)#exit
sw-jauja(config)#interface fastethernet 0/7
sw-jauja(config-if)#description camara ip
sw-jauja(config-if)#no shutdown
sw-jauja(config-if)#switchport mode access
sw-jauja(config-if)#switchport access vlan 30
sw-jauja(config-if)#switchport port-security mac-address sticky
sw-jauja(config-if)#exit
sw-jauja(config)#interface range fastethernet 0/8-24
sw-jauja(config-if-range)#shutdown
sw-jauja(config-if)#exit
sw-jauja(config)#interface range fastethernet 0/4-5
sw-jauja(config-if-range)#shutdown
```

sw-jauja(config)#interface vlan 1

sw-jauja(config-if)#ip address 201.240.162.101 255.255.255.224

sw-jauja(config-if)#no shutdown

sw-jauja(config-if)#exit

sw-jauja(config)#

sw-jauja(config)#ip default-gateway 201.240.162.101

sw-jauja(config)#

sw-jauja(config)#interface fa0/1

sw-jauja(config-if)#switchport mode trunk

sw-jauja(config-if)#switchport trunk allowe vlan 1,10,20,30

sw-jauja(config-if)#end

sw-jauja#copy running-config startup-config

Anexo III: Configuración del router Lima

Router#configure terminal

Router(config)#hostname SEDE-LIMA

SEDE-LIMA(config)#

SEDE-LIMA(config)#

SEDE-LIMA(config)#enable secret Untels2017

SEDE-LIMA(config)#line console 0

SEDE-LIMA(config-line)#

SEDE-LIMA(config-line)#password Titulacion2017

SEDE-LIMA(config-line)#login

SEDE-LIMA(config-line)#exit

SEDE-LIMA(config)#line vty 0 4

SEDE-LIMA(config-line)#password Electronica2017

SEDE-LIMA(config-line)#login

SEDE-LIMA(config-line)#exec-timeout 90

SEDE-LIMA(config-line)#transport input ssh

SEDE-LIMA(config-line)#exit

SEDE-LIMA(config)#ip domain-name cisco.com

SEDE-LIMA(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

SEDE-LIMA(config)#ip ssh version 2

SEDE-LIMA(config)#username omar secret zapata

SEDE-LIMA(config)#banner motd $ acceso restringido $

SEDE-LIMA(config)#interface loopback 1

SEDE-LIMA(config-if)#ip add 192.200.90.100 255.255.255.255

SEDE-LIMA(config-if)#exit

SEDE-LIMA(config)#interface fa0/0.10

SEDE-LIMA(config-subif)#encapsulation dot1q 10

SEDE-LIMA(config-subif)#ip address 192.192.90.33 255.255.255.224

SEDE-LIMA(config-subif)#interface fa0/0.20

SEDE-LIMA(config-subif)#encapsulation dot1q 20

SEDE-LIMA(config-subif)#ip address 192.192.90.1 255.255.255.224

SEDE-LIMA(config-subif)#interface fa0/0.30

SEDE-LIMA(config-subif)#encapsulation dot1q 30

SEDE-LIMA(config-subif)#ip address 192.192.90.65 255.255.255.224

SEDE-LIMA(config-subif)#exit

SEDE-LIMA(config)#interface fa0/0

SEDE-LIMA(config-if)#no shutdown

SEDE-LIMA(config-if)#exit

SEDE-LIMA(config)#int fa0/1

SEDE-LIMA(config-if)#ip add 192.200.1.1 255.255.255.252

SEDE-LIMA(config-if)#no shutdown

SEDE-LIMA(config-if)#exit

SEDE-LIMA(config)#router ospf 1

SEDE-LIMA(config-router)#router-id 1.1.1.1

SEDE-LIMA(config-router)#network 192.200.1.0 0.0.0.3 area 0

SEDE-LIMA(config-router)#network 192.192.90.0 0.0.0.31 area 0

SEDE-LIMA(config-router)#network 192.192.90.32 0.0.0.31 area 0

SEDE-LIMA(config-router)#network 192.192.90.64 0.0.0.31 area 0

SEDE-LIMA(config-router)#exit

SEDE-LIMA(config)#crypto isakmp policy 10

SEDE-LIMA(config-isakmp)#authentication pre-share

SEDE-LIMA(config-isakmp)#encryption aes 256

SEDE-LIMA(config-isakmp)#group 2

SEDE-LIMA(config-isakmp)#hash sha

SEDE-LIMA(config-isakmp)#exit

SEDE-LIMA(config)#

SEDE-LIMA(config)#crypto isakmp key cisco address 201.240.172.1

SEDE-LIMA(config)#crypto ipsec transform-set UNTELS esp-aes esp-md5-SHA

Router(config)# access-list 101 permit ip any any

SEDE-LIMA(config)#crypto map GESTION 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

SEDE-JAUJA(config-crypto-map)#set peer 201.240.172.1

SEDE-LIMA(config-crypto-map)#match address 101

SEDE-LIMA(config-crypto-map)#set transform-set UNTELS

SEDE-LIMA(config-crypto-map)#exit

SEDE-LIMA(config)#interface fa0/1

SEDE-LIMA(config-if)#crypto map GESTION

*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

SEDE-LIMA(config-if)#exit

Se configura un servidor VoIP para poder realizar llamadas IP entre las sedes con un máximo de 10 usuarios y 10 anexos.

SEDE-LIMA(config)#ip dhcp pool VOIP

SEDE-LIMA(dhcp-config)#network 192.192.90.0 255.255.255.224

SEDE-LIMA(dhcp-config)#default 192.192.90.33

SEDE-LIMA(dhcp-config)#dns 8.8.8.8

SEDE-LIMA(dhcp-config)#option 150 ip 192.192.90.33

SEDE-LIMA(dhcp-config)#exit

SEDE-LIMA(config)#

SEDE-LIMA(config)#telephony-service

SEDE-LIMA(config-telephony)#max-dn 10

SEDE-LIMA(config-telephony)#max-ephone 10

SEDE-LIMA(config-telephony)#ip source-address 192.192.90.33 port 2000

SEDE-LIMA(config-telephony)#ephone-dn 1

SEDE-LIMA(config-ephone-dn)#number 1001

SEDE-LIMA(config-ephone-dn)#exit

SEDE-LIMA(config)#ephone 1

SEDE-LIMA(config-ephone)#mac 00D0.BA8B.4609

SEDE-LIMA(config-ephone)#button 1:1

SEDE-LIMA(config-ephone)#type 7960

SEDE-LIMA(config-ephone)#exit

SEDE-LIMA(config)#dial-peer voice 2000 voip

SEDE-LIMA(config-dial-peer)#destination-pattern 200

SEDE-LIMA(config-dial-peer)#session target ipv4:192.192.90.33

SEDE-LIMA(config-dial-peer)#end

SEDE-LIMA#copy running-config startup-config

Anexo IV: Configuración del router Jauja

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname SEDE-JAUJA

SEDE-JAUJA(config)#

SEDE-JAUJA(config)#enable secret Untels2017

SEDE-JAUJA(config)#line console 0

SEDE-JAUJA(config-line)#password Titulacion2017

SEDE-JAUJA(config-line)#login

SEDE-JAUJA(config-line)#exit

SEDE-JAUJA(config)#line vty 0 4

SEDE-JAUJA(config-line)#password Electronica2017

SEDE-JAUJA(config-line)#login

SEDE-JAUJA(config-line)#exec-timeout 90

SEDE-JAUJA(config-line)#transport input ssh

SEDE-JAUJA(config-line)#exit

SEDE-JAUJA(config)#ip domain-name cisco.com

SEDE-JAUJA(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

SEDE-JAUJA(config)#ip ssh version 2

SEDE-JAUJA(config)#username omar secret zapata

SEDE-JAUJA(config)#banner motd $ acceso restringido $

```
SEDE-JAUJA(config)#interface loopback 1
SEDE-JAUJA(config-if)#ip add 201.240.162.110 255.255.255.255
SEDE-JAUJA(config-if)#exit
SEDE-JAUJA(config)#interface fa0/0.10
SEDE-JAUJA(config-subif)#encapsulation dot1q 10
SEDE-JAUJA(config-subif)#ip  address 201.240.162.33 255.255.255.224
SEDE-JAUJA(config-subif)#interface fa0/0.20
SEDE-JAUJA(config-subif)#encapsulation dot1q 20
SEDE-JAUJA(config-subif)#ip  address 201.240.162.1 255.255.255.224
SEDE-JAUJA(config-subif)#interface fa0/0.30
SEDE-JAUJA(config-subif)#encapsulation dot1q 30
SEDE-JAUJA(config-subif)#ip  address 201.240.162.65 255.255.255.224
SEDE-JAUJA(config-subif)#exit
SEDE-JAUJA(config)#interface fa0/0
SEDE-JAUJA(config-if)#no shutdown
SEDE-JAUJA(config-if)#exit
SEDE-JAUJA(config)#int fa0/1
SEDE-JAUJA(config-if)#ip add 201.240.172.1 255.255.255.252
SEDE-JAUJA(config-if)#no shutdown
SEDE-JAUJA(config-if)#exit
SEDE-JAUJA(config)#router ospf 1
SEDE-JAUJA(config-router)#router-id 1.1.1.1
SEDE-JAUJA(config-router)#network 201.240.172.0 0.0.0.3 area 0
```

SEDE-JAUJA(config-router)#network 201.240.162.0 0.0.0.31 area 0

SEDE-JAUJA(config-router)#network 201.240.162.32 0.0.0.31 area 0

SEDE-JAUJA(config-router)#network 201.240.162.64 0.0.0.31 area 0

SEDE-JAUJA(config-router)#exit

SEDE-JAUJA(config)#crypto isakmp policy 10

SEDE-JAUJA(config-isakmp)#authentication pre-share

SEDE-JAUJA(config-isakmp)#encryption aes 256

SEDE-JAUJA(config-isakmp)#group 2

SEDE-JAUJA(config-isakmp)#hash sha

SEDE-JAUJA(config-isakmp)#exit

SEDE-JAUJA(config)#crypto isakmp key cisco address 192.200.1.1

SEDE-JAUJA(config)#crypto ipsec transform-set UNTELS esp-aes esp-md5-sha

SEDE-JAUJA(config)#access-list 101 permit ip any any

SEDE-JAUJA(config)# crypto map GESTION 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

SEDE-JAUJA(config-crypto-map)#set peer 192.200.1.1

SEDE-JAUJA(config-crypto-map)#match address 101

SEDE-JAUJA(config-crypto-map)#set transform-set UNTELS

SEDE-JAUJA(config-crypto-map)#interface f0/1

SEDE-JAUJA(config-if)#crypto map GESTION

*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

SEDE-JAUJA(config)#ip dhcp pool VOIP

SEDE-JAUJA(dhcp-config)#network 201.240.162.32 255.255.255.224

SEDE-JAUJA(dhcp-config)#default 201.240.162.33

SEDE-JAUJA(dhcp-config)#dns 8.8.8.8

SEDE-JAUJA(dhcp-config)#option 150 ip 201.240.162.33

SEDE-JAUJA(dhcp-config)#exit

SEDE-JAUJA(config)#telephony-service

SEDE-JAUJA(config-telephony)#max-dn 10

SEDE-JAUJA(config-telephony)#max-ephone 10

SEDE-JAUJA(config-telephony)#ip source-address 201.240.162.33 port 2000

SEDE-JAUJA(config-telephony)#ephone-dn 1

SEDE-JAUJA(config-ephone-dn)#number 1001

SEDE-JAUJA(config-ephone-dn)#exit

SEDE-JAUJA(config)#ephone 1

SEDE-JAUJA(config-ephone)#mac 00D0.BA8B.4609

SEDE-JAUJA(config-ephone)#button 1:1

SEDE-JAUJA(config-ephone)#type 7960

SEDE-JAUJA(config-ephone)#exit

SEDE-JAUJA(config)#dial-peer voice 2000 voip

SEDE-JAUJA(config-dial-peer)#destination-pattern 200

SEDE-JAUJA(config-dial-peer)#session target ipv4:201.240.162.33

SEDE-JAUJA(config-dial-peer)#end

SEDE-JAUJA#copy running-config startup-config

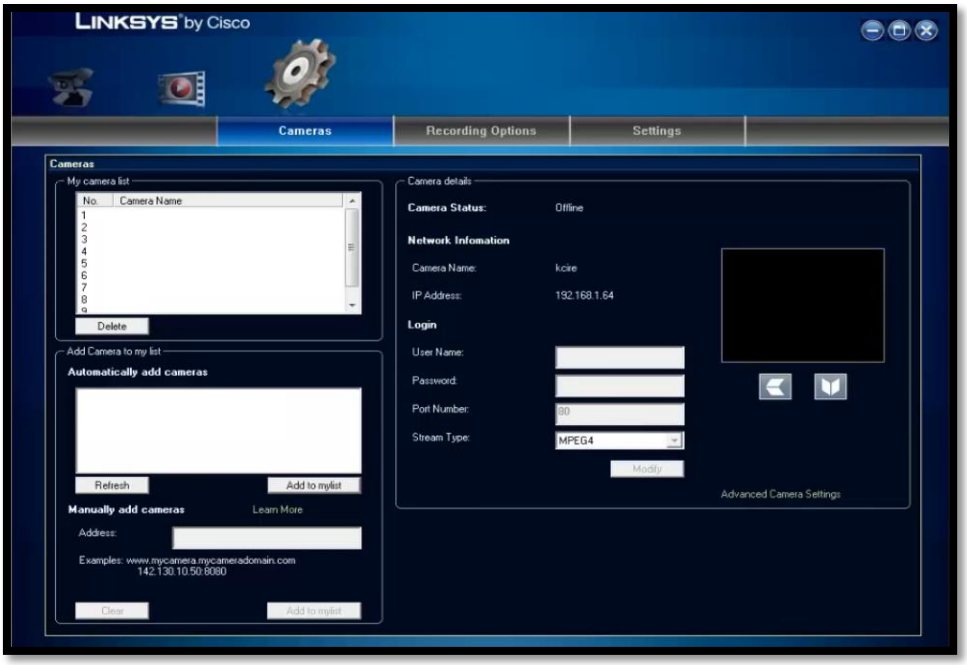
Anexo V. Configuración cámara IP

La configuración de la cámara IP es de forma GUI por lo que el proveedor te brinda un software en CD el cual te brinda los pasos básicos de configuración.

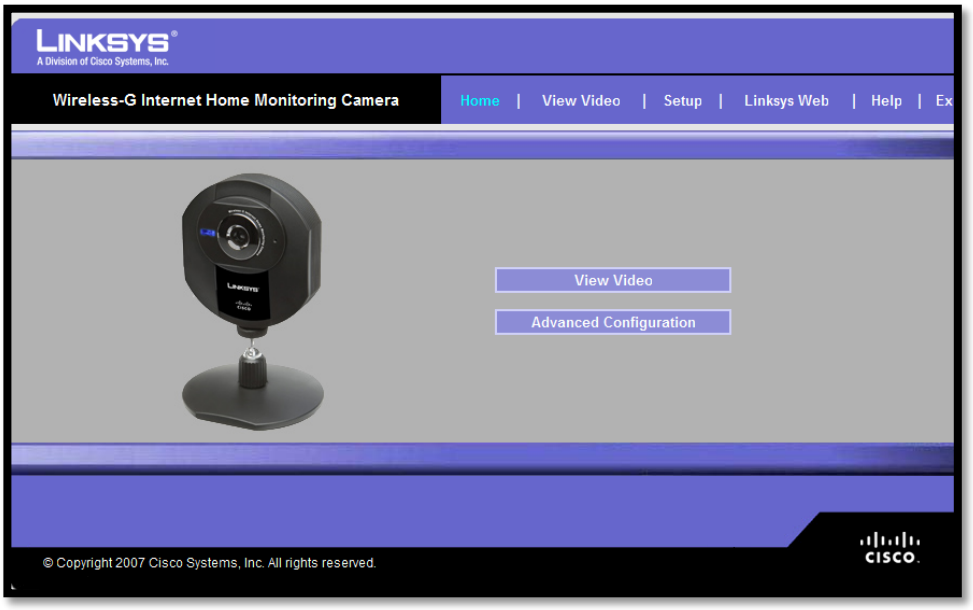
Primera parte: se necesitara ingresar el software para empezar las instalación en modo setup, luego se pedirá que acepte términos de contratos para empezar a escanear el sistema, se detectara la cámara IP y empezara a testear la red y la luz para configurarse de forma automática, después se necesitara ingresar un nombre de cámara, nombre de usuario y contraseña. La cámara ya podrá ser utilizada en un entorno LAN.

Segunda parte: en este modo es para poder habilitar una interfaz con la que se podrá observar la cámara en tiempo real y poder configurarla para un uso remoto.

La interfaz Linksys de Cisco se utiliza para agregar la cámara, dar opciones de grabado y configuraciones de seguridad.



Tercer paso: configurar la cámara para un acceso remoto usando un navegador web se ingresa la dirección IP asignada a la cámara IP en el navegador con el nombre y la clave previamente configurada.

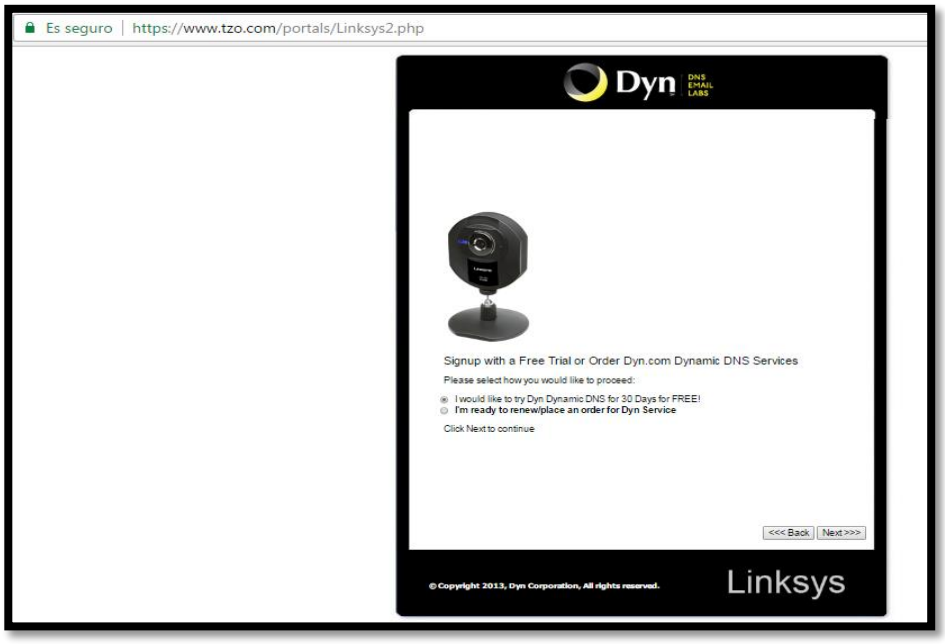


Cuarto paso: las cámaras Cisco Linksys te brindan un servicio gratuito de prueba para poder tener acceso a una cámara IP de forma remota luego se tendrá que pagar una membresía anual.

Existen 2 diferentes niveles de servicio que puede elegir, que depende del nombre de dominio que le gustaría utilizar para acceder a su dispositivo.

Servicio estándar - esto le da un nombre de dominio como Yourname.MyIPCamera.com con un costo de $ 25.00 por año.

Servicio premier: esto le da su propio nombre de dominio como Yourname.com con un costo de $ 50.00 por año.



Para evitar el gasto en membresías anuales, se puede habilitar una aplicación dentro de la web de la empresa con la cual se podrá tener acceso en tiempo real a través de Internet sin costo adicional.

Anexo VI. Especificaciones Técnicas de Router cisco836

DATA SHEET

CISCO 836 ADSL OVER ISDN SECURE BROADBAND ROUTERS ADVANCED SECURITY FOR DATA, VOICE, AND VIDEO ACCESS IDEAL FOR SMALL OFFICES AND TELEWORKERS

The Cisco® 836 router is ideal for providing secure Internet and corporate network connectivity to small remote offices and to teleworkers (Figure 1). The Cisco 836 router provides integrated security services and advanced quality of service (QoS) features for high-quality data, voice, and video applications. It offers easy deployment and remote management features with Cisco IOS® Software.

The Cisco 836 router is ideal for providing secure Internet and corporate network connectivity to small remote offices and to teleworkers (Figure 1). The Cisco 836 router provides integrated security services and advanced quality of service (QoS) features for high-quality data, voice, and video applications. It offers easy deployment and remote management features with Cisco IOS Software.

The Cisco 836 router has an integrated asymmetric digital subscriber line (ADSL) modem that supports ADSL over Integrated Services Digital Network (ISDN). It has an integrated ISDN Basic Rate Interface (BRI) S/T port for a backup ISDN line, and a four-port 10/100 Ethernet LAN switch for connecting multiple PCs or network devices in a small-office network.

ADVANCED SECURITY AND PERFORMANCE FOR ENTERPRISE-CLASS VPNS

The Cisco 836 router delivers integrated enterprise-class security services, including hardware-accelerated IP Security (IPSec), Triple Data Encryption Standard (3DES) encryption for virtual private networks (VPNs), and stateful-inspection firewall for secure Internet connectivity. Optional advanced features—such as Cisco Easy VPN Remote (a software feature that allows simple deployment and management of VPNs); public key infrastructure (PKI) security requiring digital certificates; IPSec Network Address Translation transparency (NAT-T); the Cisco Intrusion Detection System (IDS)*; AES encryption*, and URL filtering*—help ensure that the small office receives the highest level of security, which contributes to the corporate network's security.

HIGH-QUALITY, SECURE VOICE AND VIDEO

The advanced QoS and high-performance encryption features of the Cisco 836 router provide high-quality voice and video services to remote users. When IP phones are connected at a remote site, a Cisco 836 router can queue and prioritize the voice traffic over data traffic to ensure a high quality, secure voice-over-IP (VoIP) connection from the remote or home office back to the corporate network. Unique Cisco IOS software capabilities such as Preclassification of Traffic prior to Encryption* and Look-ahead Fragmentation before Encryption* ensure that traffic is correctly prioritized over a secure IPSec tunnel.

Figure 1. The Cisco 836 ADSL over ISDN Router

MANAGEABLE, SCALABLE, AND RELIABLE ACCESS

The Cisco 836 router uses valuable management and deployment tools to deliver the industry's lowest total cost of ownership for connecting small remote offices and teleworkers to the corporate network. As a remotely manageable platform, the Cisco 836 router supports advanced remote troubleshooting commands available in Cisco IOS Software; out-of-band management through an ISDN port; and Secure Shell (SSH) Protocol for secure in-band management via Telnet.

For scalability in deployment and management, the Cisco Router Web SetUp Tool (CRWS), available in several languages, allows nontechnical users to quickly set up the router and turn on key features such as the stateful firewall. Cisco provides a suite of solutions—such as Cisco Easy VPN, the Cisco IE 2100 Intelligence Engine, Cisco VPN Solution Center (VPNSC), CiscoWorks Management Center for VPN Routers (Router MC), and Cisco Configuration Express—that allow for scalable network deployment and management, including automated security policy push and configuration updates.

For reliable access, the ISDN port provides ISDN dial backup and out-of-band management. The Cisco 836 router runs Cisco IOS Software, the industry-proven software that has become the standard for reliable business access.

FEATURES AND BENEFITS

Table 1. Key Product Features and Benefits

Features	Benefits
Advanced Security and Performance for Enterprise-Class VPNs	
Stateful-inspection firewall	• Offers internal users secure, per-application dynamic access control (stateful inspection) for all traffic across perimeters • Defends and protects router resources against denial-of-service (DoS) attacks • Provides context-based access control (CBAC) • Checks packet headers and drops suspicious packets • Protects against unidentified, malicious Java applets • Details transactions for reporting on a per-application, per-feature basis
Network security features with Cisco IOS Software, including access control lists (ACLs), Network Address Translation/Port Address Translation (NAT/PAT), Lock & Key security, dynamic ACLs, and router and route authentication	Provides perimeter network security to prevent unauthorized network access
Cisco Intrusion Detection System (IDS)*	Detects and prevents DoS attacks and unauthorized network access; sends alerts to initiate appropriate action
Hardware-accelerated IPSec 3DES encryption	• Delivers high-performance IPSec VPN encryption for broadband connections • Supports Internet Key Exchange (IKE) and IPSec VPN standards for up to 10 simultaneous tunnels • Provides WAN encryption for all users on the LAN without requiring the configuration of individual PCs
AES encryption*	AES support provides impenetrable security to the IPSec sessions
Cisco Easy VPN Remote	Provides easy deployment and maintenance of VPN connections with auto-IPSec tunnel initiation and policy push from a Cisco VPN concentrator or server
URL filtering with WebSENSE and N2H2 software and server*	• Allows a network administrator to easily apply Internet use policies to permit access only to company-approved URLs or categories of sites • WebSENSE and N2H2 URL filtering software filters HTTP requests based on destination host name, destination IP address, keywords, and username • WebSENSE and N2H2 maintains and updates a URL database of more than 20 million sites, organized into more than 60 categories
IPSec NAT Transparency (NAT Traversal or NAT Aware IPSec)*	Allows reliable creation of VPN tunnels independent of the placement of firewalls and NAT across multiple networks
PKI support with digital certificates	• Standards-based robust key management allows better network scaling and enhanced key security • Facilitates extranet communications
High-Quality, Secure Voice and Video	
IP QoS—Low Latency Queuing (LLQ), Weighted Random Early Detection (WRED), Committed Access Rate (CAR)	• Ensures consistent response times for multiple applications by intelligently allocating bandwidth • Allows for classification of applications and gives the most important applications priority use of the WAN line • Provides congestion avoidance by throttling down certain Transmission Control Protocol (TCP) sessions, depending on each session's priority level
Asynchronous Transfer Mode (ATM) QoS—ATM traffic universal broadband router (UBR), nonreal-time variable bit rate (VBRnrt), VBRrt, and constant bit rate (CBR) with per-VC queuing and traffic shaping	Provides QoS guarantees for real-time traffic, with ability to send traffic over the appropriate virtual circuit to provide ATM-level shaping and ensure that no head-of-line blocking can occur between circuits of different or equal traffic classes
High-performance encryption	Provides secure connectivity without affecting performance for bandwidth-intensive applications
IP multicast technology	Reduces redundant traffic; conserves bandwidth for corporate communications, distance-learning applications such as Cisco IP/TV®, software distribution, and access to stock quotes and news applications

Advanced Management Features for Low Cost of Ownership	
Plug-and-play installation with default settings and Web-based setup tool	Nontechnical users can easily set up the router and customize advanced features
Cisco Router Web SetUp Tool	Allows nontechnical users to complete installation by simply pointing a browser at the router and providing user information
Cisco Easy VPN Remote	Provides easy deployment and maintenance of VPN connections with auto-IPSec tunnel initiation and pushed policy acceptance
Cisco Configuration Express	Lowers the cost of deployment by shipping preconfigured units directly to end users without requiring staging or storage
Router status page in CRWS	Provides a Web-based visual presentation of router configuration and feature status
Cisco IOS Software interactive debug and remote management features	Enables remote management and monitoring via Simple Network Management Protocol (SNMP), Telnet, or HTTP and local management via console port to diagnose network problems in detail
Cisco IOS Software command-line interface (CLI)	Allows customers to use existing knowledge of Cisco IOS Software CLI for easier installation and manageability without requiring additional training

Features	Benefits
Cisco IOS Software technology	Offers technology that is used throughout the backbone of the Internet and in most enterprise networks
Cisco IE 2100 Intelligence Engine management appliance	Allows remote sites to be configured to automatically contact this centrally located device for Cisco IOS Software configuration updates
Supported by Cisco VPNSC, CiscoWorks VPN/Security Management Solution (VMS), and Cisco Secure Policy Manager	Allows for scalable deployment of security policy management
SSH	Provides a secure, encrypted connection to a router that is similar to an inbound Telnet session

Table 2. Cisco 836 Series Hardware Specifications

Hardware Specifications	Cisco 836 Router
Processor	Motorola RISC
Default DRAM* Memory	64 MB
Maximum DRAM Memory	80 MB
Default Flash* Memory	12 MB
Maximum Flash Memory	24 MB
WAN	ADSL over ISDN
LAN	Four-port 10/100BASE-T with autosensing MDI/MDX for autocrossover
Console Port	RJ-45
ISDN Basic Rate Interface (BRI) S/T	RJ-45—ISDN BRI S/T port which can be configured for ISDN backup or out-of-band management
LEDs	10
External Power Supply	Universal 100–240 VAC

* DRAM and Flash memory must be obtained from Cisco.

Table 3. Memory Requirements and Software Feature Sets for the Cisco 836 Router

Cisco 836 Series with Cisco IOS Software Images	Cisco 836 Series Memory Requirements	
	Flash	**DRAM**
IP/Firewall/IPSec 3DES (Default)	8 MB	32 MB
IP/Firewall/IPSec 3DES PLUS	8 MB	32 MB
IP/Firewall/IPSec 3DES/PLUS/Dial Backup	8 MB	32 MB

Anexo VII. Especificaciones Técnicas de switch Catalyst 2960-L 16 puertos

Updated: January 17, 2017 Document ID: 1472604893644312

Product Overview

Cisco Catalyst® 2960-L Series Switches are fixed-configuration, Gigabit Ethernet switches that provide entry-level enterprise-class Layer 2 access for branch offices, conventional workspaces, and out-of-wiring closet applications. Designed for operational simplicity to lower total cost of ownership, they enable secure, and energy-efficient business operations with a range of Cisco IOS® Software features.

Product Highlights

Cisco Catalyst 2960-L switches feature:

- 8, 16, 24, or 48 Gigabit Ethernet ports with line-rate forwarding
- 2 or 4 Gigabit Small Form-Factor Pluggable (SFP) uplinks
- Power over Ethernet Plus (PoE+) support with up to 370W of power budget
- Fanless operation and operational temperature up to 45°C for deployment outside the wiring closet
- Higher mean time between failure (MTBF) because they have no moving mechanical parts
- Less than 11.5-inch depth fit in use cases with space limitation
- Reduced power consumption and advanced energy management features
- RJ45 and USB console access for simplified operations
- Intuitive web UI for easy deployment and management
- Cisco IOS® Software features
- Enhanced limited lifetime warranty (E-LLW) offering next-business-day hardware replacement

Network Security

The Cisco Catalyst 2960-L Series Switches provide a range of security features to limit access to the network and mitigate threats, including:

- **Comprehensive 802.1x** features to control access to the network, including flexible authentication, 802.1x monitor mode, and RADIUS change of authorization.
- **Multidomain Authentication** allows an IP phone and a PC to authenticate on the same switch port while placing them on appropriate voice and data VLANs.
- **Access Control Lists (ACLs)** for IPv6 and IPv4 for security and QoS ACEs:
  - **Port-based ACLs** for Layer 2 interfaces allow security policies to be applied on individual switch ports.
- **Secure Shell (SSH) Protocol, Kerberos, and Simple Network Management Protocol Version 3 (SNMPv3)** provide network security by encrypting administrator traffic during Telnet and SNMP sessions. SSH Protocol, Kerberos, and the cryptographic version of SNMPv3 require a special cryptographic software image because of U.S. export restrictions.
- **Switched Port Analyzer (SPAN),** with bidirectional data support, allows Cisco Intrusion Detection System (IDS) to take action when an intruder is detected.
- **TACACS+ and RADIUS authentication** facilitates centralized control of the switch and restricts unauthorized users from altering the configuration.
- **MAC address notification** allows administrators to be notified about users added to or removed from the network.
- **Multilevel security on console access** prevents unauthorized users from altering the switch configuration.
- **Bridge Protocol Data Unit (BPDU) guard** shuts down spanning-tree port fast–enabled interfaces when BPDUs are received to avoid accidental topology loops.
- **Spanning-tree Root Guard (STRG)** prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.
- **IGMP filtering** provides multicast authentication by filtering out nonsubscribers and limits the number of concurrent multicast streams available per port.
- **Dynamic VLAN assignment** is supported through implementation of VLAN membership policy server client capability to provide flexibility in assigning ports to VLANs. Dynamic VLAN facilitates the fast assignment of IP addresses.

Redundancy and Resiliency

Cisco Catalyst 2960-L Series Switches offer a number of redundancy and resiliency features to prevent outages and help ensure that the network remains available:

- **IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP)** provide rapid spanning-tree convergence independent of spanning-tree timers and also offer the benefits of Layer 2 load balancing and distributed processing.
- **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.
- **Switch-port autorecovery (error disable)** automatically attempts to reactivate a link that is disabled because of a network error.

Enhanced Quality of Service

The Cisco Catalyst 2960-L Series Switches offers intelligent traffic management that keeps everything flowing smoothly. Flexible mechanisms for marking, classification, and scheduling deliver superior performance for data, voice, and video traffic, all at wire speed. Primary QoS features include:

- Up to **four egress queues** and two thresholds per port supporting bandwidth control, shaping, and priority queuing so that the high priority packets are serviced ahead of other traffic.
- **Weighted Round Robin** (WRR) scheduling and **Weighted Tail Drop** (WTD) congestion avoidance.
- **802.1p class of service** (CoS) classification, with marking and reclassification on a per-packet basis by source and destination IP address, MAC address, or Layer 4 TCP/UDP port number.

Intelligent Power over Ethernet Plus

Cisco Catalyst 2960-L Series Switches support both IEEE 802.3af Power over Ethernet (PoE) and IEEE 802.3at PoE+ (up to 30W per port) to deliver lower total cost of ownership for deployments that incorporate Cisco IP Phones, Cisco Aironet® wireless access points, or other standards-compliant PoE/PoE+ end devices. PoE removes the need to supply wall power to PoE-enabled devices and eliminates the cost of adding electrical cabling and circuits that would otherwise be necessary in IP phone and WLAN deployments.

The Cisco Catalyst 2960-L Series PoE power allocation is dynamic, and power mapping scales up to a maximum of 370W PoE+ power. Intelligent power management allows flexible power allocation across all ports.

Cisco Catalyst SmartOperations

Cisco Catalyst SmartOperations is a comprehensive set of capabilities that simplify LAN planning, deployment, monitoring, and troubleshooting. Deploying SmartOperations tools reduces the time and effort required to operate the network and lowers TCO.

- **Cisco AutoConfig** services determine the level of network access provided to an endpoint based on the type of the endpoint device. This feature also permits hard binding between the end device and the interface.
- **Cisco Smart Install** services enable minimal-touch deployment by providing automated Cisco IOS Software image installation and configuration when new switches are connected to the network. This enables network administrators to remotely manage Cisco IOS Software image installs and upgrades.
- **Cisco Auto SmartPorts** services enable automatic configuration of switch ports as devices connect to the switch with settings optimized for the device type resulting in zero-touch port-policy provisioning.
- **Cisco Smart Troubleshooting** is an extensive array of diagnostic commands and system health checks in the switch, including Smart Call Home. The Cisco Generic Online Diagnostics (GOLD) and Cisco online diagnostics on switches in live networks help predict and detect failures more quickly.
- **PnP (Plug and Play)** with Cisco APIC – EM (Application Policy Infrastructure Controller Enterprise Module) support for simple, secure, unified, and integrated new branch or campus device deployments or for provisioning updates to an existing network.

For more information about Cisco Catalyst SmartOperations, visit cisco.com/go/SmartOperations.

Operational Simplicity Features

- **Cisco AutoSecure provides** a single-line command-line interface (CLI) to enable baseline security features (Port Security, DHCP snooping, Dynamic ARP Inspection (DAI)). This feature simplifies security configurations with a single touch.
- **Dynamic Host Configuration Protocol (DHCP)** autoconfiguration of multiple switches through a boot server eases switch deployment.
- **Autonegotiation** on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth.
- **Dynamic Trunking Protocol (DTP)** facilitates dynamic trunk configuration across all switch ports.
- **Port Aggregation Protocol (PAgP)** automates the creation of Cisco Fast EtherChannel groups or Gigabit EtherChannel groups to link to another switch, router, or server.
- **Link Aggregation Control Protocol (LACP)** allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad. This feature is similar to Cisco EtherChannel technology and Port Aggregation Protocol (PAgP).
- **Automatic media-dependent interface crossover (MDIX)** automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.
- **Unidirectional Link Detection Protocol (UDLD)** and aggressive UDLD allow unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.
- **Local Proxy Address Resolution Protocol (ARP)** works in conjunction with private VLAN edge to minimize broadcasts and maximize available bandwidth.
- **VLAN1 minimization** allows VLAN1 to be disabled on any individual VLAN trunk.
- **Internet Group Management Protocol (IGMP)** snooping for IPv4 and IPv6 MLD v1 and v2 snooping provide fast client joins and leaves of multicast streams and limit bandwidth-intensive video traffic to only the requestors.
- **Per-port broadcast, multicast, and unicast storm control** prevents faulty end stations from degrading overall system performance.
- **Voice VLAN** simplifies telephony installations by keeping voice traffic on a separate VLAN for easier administration and troubleshooting.
- **Cisco VLAN Trunking Protocol (VTP)** supports dynamic VLANs and dynamic trunk configuration across all switches.
- For enhanced traffic management, monitoring, and analysis, the embedded **remote monitoring (RMON)** software agent supports four RMON groups (history, statistics, alarms, and events).
- **Layer 2 trace route** eases troubleshooting by identifying the physical path that a packet takes from source to destination.
- **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 intranet switches.

Table 2. Specifications

	8 Port	16 Port	24 Port	48 Port
Console Ports				
RJ45 Ethernet	1	1	1	1
USB mini-B	1	1	1	1
USB-A port for storage and Bluetooth console	1	1	1	1
Memory and Processor				
CPU	ARMv7 800 MHz	ARMv7 800 MHz	ARMv7 800 MHz	ARMv7 800 MHz
DRAM	512 MB	512 MB	512 MB	512 MB
Flash memory	256 MB	256 MB	256 MB	256 MB

Performance				
Forwarding bandwidth	10 Gbps	18 Gbps	28 Gbps	52 Gbps
Switching bandwidth	20 Gbps	36 Gbps	56 Gbps	104 Gbps
Forwarding rate (64-byte L3 packets)	14.88 Mpps	26.78 Mpps	41.67 Mpps	77.38 Mpps
Unicast MAC addresses	8K	8K	8K	8K
Maximum active VLANs	64	64	64	64
VLAN IDs available	4094	4094	4094	4094
Maximum STP instances	64	64	64	64
Maximum SPAN sessions	1	1	1	1
MTU-L3 packet	9198 bytes	9198 bytes	9198 bytes	9198 bytes
Jumbo Ethernet frame	10,240 bytes	10,240 bytes	10,240 bytes	10,240 bytes
MTBF in hours (Data)	2,448,133	2,416,689	2,412,947	1,370,769
MTBF in hours (PoE)	315,044	313,496	909,838	437,970

Anexo VIII. Especificaciones Técnicas de teléfono IP 7931G

Data Sheet

Cisco Unified IP Phone 7931G

Cisco® Unified Communications is a comprehensive IP communications system of voice, video, data, and mobility products and applications. It enables more effective, more secure, more personal communications that directly affect both sales and profitability. It brings people together by enabling a new way of communicating—where your business moves with you, security is everywhere, and information is always available...whenever and wherever it is needed. Cisco Unified Communications is part of an integrated solution that includes network infrastructure, security, mobility, network management products, lifecycle services, flexible deployment and outsourced management options, end-user and partner financing packages, and third-party communications applications.

The Cisco Unified IP Phone 7931G meets the communication needs of retail, commercial, manufacturing workers, and anyone with moderate telephone traffic but also specific call requirements. Dedicated hold, redial, and transfer keys facilitate call handling in a retail environment. Illuminated mute and speakerphone keys give a clear indication of speaker status. A pixel-based display with a white backlight makes calling information easy to see, and Extensible Markup Language (XML) services deliver a rich user experience. The Cisco Unified IP Phone 7931G offers numerous important security features plus the choice of IEEE 802.3af Power over Ethernet (PoE) or local power through an optional power adaptor (Figure 1).

Figure 1. Cisco Unified IP Phone 7931G

Features

The Cisco Unified IP Phone 7931G is designed to grow with your organization. A dynamic, soft-key activated feature set allows the phone to keep pace with your requirements through regular software upgrades. You can easily move phones, add new phones, and change existing phone arrangements; users can simply pick up their phones and move to a new location anywhere on the network. The Cisco Unified IP Phone 7931G also provides accessibility features for those with special needs. Tables 1 through 7 present the features, specifications, and compliance information for the Cisco Unified IP Phone 7931G, Table 8 provides ordering information, and Table 9 lists available optional accessories.

Table 1. Features and Descriptions

Feature	Description
Lighted line keys	Twenty-four lighted line keys to which individual lines can be assigned—Each line key provides a busy-line indication if the line is shared with another IP phone. Lighted line keys are also used to access services and call history directories and to activate the headset port.
Dedicated hold, redial, and transfer keys	Dedicated keys for hold, redial, and transfer—The hold key is colored red to make it clearly visible in a fast-moving call environment; the redial and transfer keys facilitate rapid call handling.
Lighted message waiting indicator	Lights turn on when there is new voicemail and when the phone rings; the message waiting indicator is visible on both the phone chassis and handset, and it stays lit until the user processes new voicemail.
Graphical display	A graphical monochrome display with resolution of 192 x 64 pixels and a white backlight provides scrollable three-line intuitive access to calling features and text-based XML applications. The Cisco Unified IP Phone 7931G also supports audio-based XML applications.
Four soft keys and a four-way rocker key	These keys dynamically present calling options to the user. The four-way rocker key allows easy movement through the displayed information.
Network features	Cisco Discovery Protocol and LLDP-MED (Link Layer protocol) [1]; IEEE 802.1 p/q tagging and switching
Ethernet switch	The phone offers 10/100BASE-T Ethernet connection through two RJ-45 ports: one for the LAN connection and the other for connecting a downstream Ethernet device such as a PC.
Speakerphone	A full-duplex speakerphone enables the user to handle calls hands-free.
Volume control	A volume-control toggle provides easy decibel-level adjustments of the handset, headset, speakerphone, and ringing volume.
Headset port	A dedicated headset port eliminates the need for a separate amplifier when using a headset; it allows the handset to remain in its cradle, making headset use simpler.
Single-position foot stand	The phone offers optimum display viewing and comfortable use of buttons and keys. The foot stand can be removed for wall mounting with mounting holes located on the base of the phone.
Multiple ring tones	The phone offers more than 24 user-selectable ring tones.
American Disabilities Act (ADA) features	A hearing-aid-compatible (HAC) handset meets ADA requirements, including ADA HAC requirements for a magnetic coupling to approved hearing aids; the phone dialing pad also complies with ADA requirements.
Signaling protocol support	Compatible with Cisco Unified CallManager Express Version 4.0(2) and later, using the Skinny Client Control Protocol (SCCP), or Cisco Unified Call Manager 6.0 and later. Also compatible with the Session Initiation Protocol (SIP), starting from Cisco Unified Call Manager 7.0 or later.
Codec support	The phone supports G.711a, G.711u, G.729a, G.729b, and G.729ab audio-compression codecs.
Configuration options	Network parameters can be provisioned through the Dynamic Host Configuration Protocol (DHCP).
Voice quality	Comfort-noise generation and voice-activity-detection (VAD) programming is offered on a system basis.

Table 2. Security Features

Item	Description
Certificates	Phones shipped with factory-installed X.509v3 certificates; there is also an option to install and remove certificates at the customer's site
Device authentication and signaling encryption	Transport Layer Security (TLS) with Advanced Encryption Standard (AES)-128 encryption available with Cisco Unified CallManager Express Version 4.0(2) or later. Cryptography is not enabled by default and may only be enabled through a cryptographically enabled CUCM.
Media encryption	Secure Real-Time Transport Protocol (SRTP) with AES-128 encryption available with Cisco Unified Communications Manager Express and Cisco Unified Communications Manager in a later release. Cryptography is not enabled by default and may only be enabled through a cryptographically enabled CUCM.

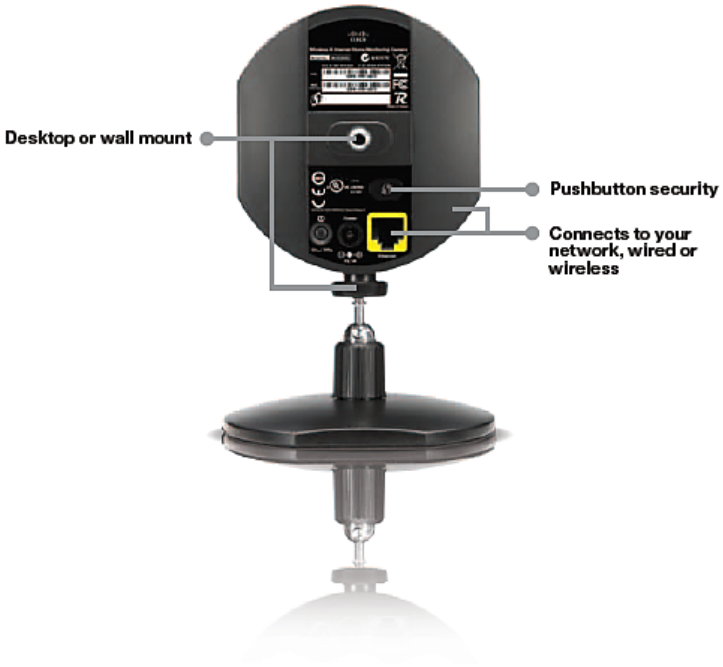
Table 3. Software and Physical Specifications

Item	Description
Firmware upgrades	Firmware upgrade supported using a Trivial File Transfer Protocol (TFTP) server
Dimensions (H x W x D)	8 x 9 x 7 in. (20.3 x 22.9 x 17.8 cm)
Weight	3.0 lb (1.36 kg)
Phone casing composition	Polycarbonate acrylonitrile butadiene styerene (ABS) plastic in textured dark gray with silver bezel

Anexo IX. Especificaciones Técnicas de Cámara IP WVC80N

Features

- Monitor your home from anywhere in the world via the Internet
- Integrated web server - viewable from most web browsers
- Supports MPEG-4 and MJPEG compression
- View video from your Wireless-N or wired Ethernet network
- Motion Detection and Email notification
- Create a database for user authentication
- Supports resolution of up to 640x480 pixels
- Time Stamp & Text Overlay
- Supports up to 5 simultaneous unicast connections
- Multicast RTP support allows multiple users to access the media stream
- Supports TZO DDNS Service for dynamic IP connection, 90-Day Free Trial
- Multi-platform support – TCP/IP, SMTP (Email), HTTP, DHCP, and FTP
- Windows-based Setup Wizard for easy setup
- WEP, WPA, and Wi-Fi Protected Access™ 2 (WPA2) Encryption
- Supports multiple resolution streams – can be used by PC and smartphone simultaneously
- Includes easy to use multi-camera monitoring utility with Snapshot feature



Minimum Requirements

For Setup

- Windows PC with Internet Explorer 6 or higher for browser-based configuration, or
- Setup Wizard software requires CD or CD/DVD drive and up-to-date Windows XP, Vista, Vista 64-bit Edition, or Mac OS X 10.4 or higher

For Viewing Video

- Windows PC with included Monitoring Utility, or
- Any computer with Internet Explorer 6, Safari 3, or Firefox 3 or higher, or a stream-enabled video player (VLC, Quicktime Player, Windows Media Player version 10 or higher, etc.)
- Smartphone with advanced web browser or RTSP

Package Contents

- Wireless-N Internet Home Monitoring Camera with stand
- Setup Wizard, Monitoring Utility, and User Guide on CD-ROM
- Ethernet Network Cable
- Quick Installation Guide
- Power Adapter

Model: WVC80N

Specifications

Model	WVC80N
Standards	IEEE 802.3u, 802.3, 802.11g, 802.11b, draft 802.11n
Ports	Ethernet, Power
Buttons	Power, Reset, Wi-Fi Protected Setup™
LEDs	Power, Wi-Fi Protected Setup™
Cabling Type	CAT5
# of Antennas	1
Detachable (y/n)	No
Modulations	802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP) in dBm	802.11b: 18 dBm (typical) @ 11Mbps 802.11g: 16 dBm (typical) @ 54Mbps 802.11n: 15dBm (typical) @ 65Mbps (HT20), 135Mbps (HT40)
Receive Sensitivity in dBm	802.11b: -87dBm (typical) @ 11Mbps 802.11g: -72dBm (typical) @ 54Mbps 802.11n: -70dBm (typical) @ MCS7, -65dBm (typical) @ MCS7
Antenna Gain in dBi	1.5 dBi
UPnP able/cert	UPnP Advertise
Wireless Security	WEP, WPA, Wi-Fi Protected Access™ 2 (WPA2)
Security Key Bits	Up to 128-bit encryption
OS Requirements	Windows XP, Vista, Vista 64-bit edition with latest updates, or Mac OS X 10.4 or higher (for Setup Wizard only)
Effective Focus	50cm to unlimited
Sensitivity	6.0V/Lux-sec
Field of View	61.2 degrees
Compression Algorithm	MPEG-4 part 2 and MJPEG
Record File Format	ASF, AVI