CCNA Exploration 4 – Acceso a la WAN

Capítulo 6: Servicios de Trabajadores a Distancia

Ricardo José Chois Antequera

INSTITUTO TECNOLÓGICO DE SOLEDAD ATLÁNTICO - ITSA

Objetivos

- Describir los requisitos empresariales para proporcionar servicios de trabajadores a distancia.
- Explicar como los servicios de banda ancha extiendes las redes empresariales mediante DSL, cable modem y tecnologías inalámbricas.
- Describir como la tecnología VPN se puede utilizar para proporcionar a una red empresarial servicios seguros de trabajo a distancia.

Beneficios del trabajo a distancia

- Cada vez más empresas consideran beneficioso tener trabajadores a distancia.
- Cuando se diseñan las arquitecturas de redes de este tipo, los diseñadores deben lograr un equilibrio entre los requisitos de la:
  - Organización de seguridad,
  - Administración de infraestructura,
  - Escalabilidad y viabilidad económica, y
  - Las necesidades prácticas de los trabajadores a distancia de facilidad de uso, velocidades de conexión y fiabilidad del servicio.

Beneficios del trabajo a distancia:

Beneficios organizativos:

- Continuidad de las operaciones
- Mayor capacidad de respuesta
- Acceso a la información seguro, confiable y fácil de administrar
- Integración económica de datos, voz, video y aplicaciones
- Mayor productividad, satisfacción y retención de empleados

Beneficios sociales:

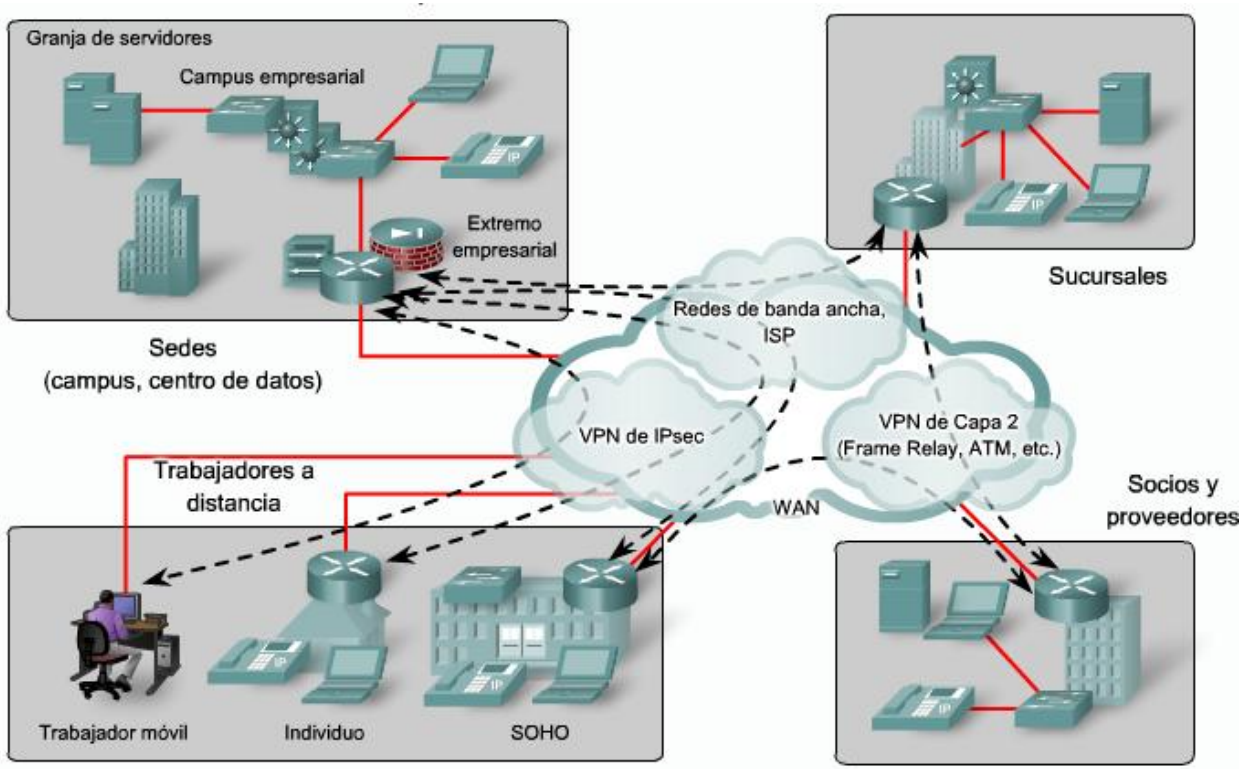
- Mayores oportunidades de empleo para grupos marginados
- Menos viaje y menos tensión relacionada con el traslado

Beneficios ambientales:

- Huellas de carbono reducidas, tanto para trabajadores individuales como para las organizaciones

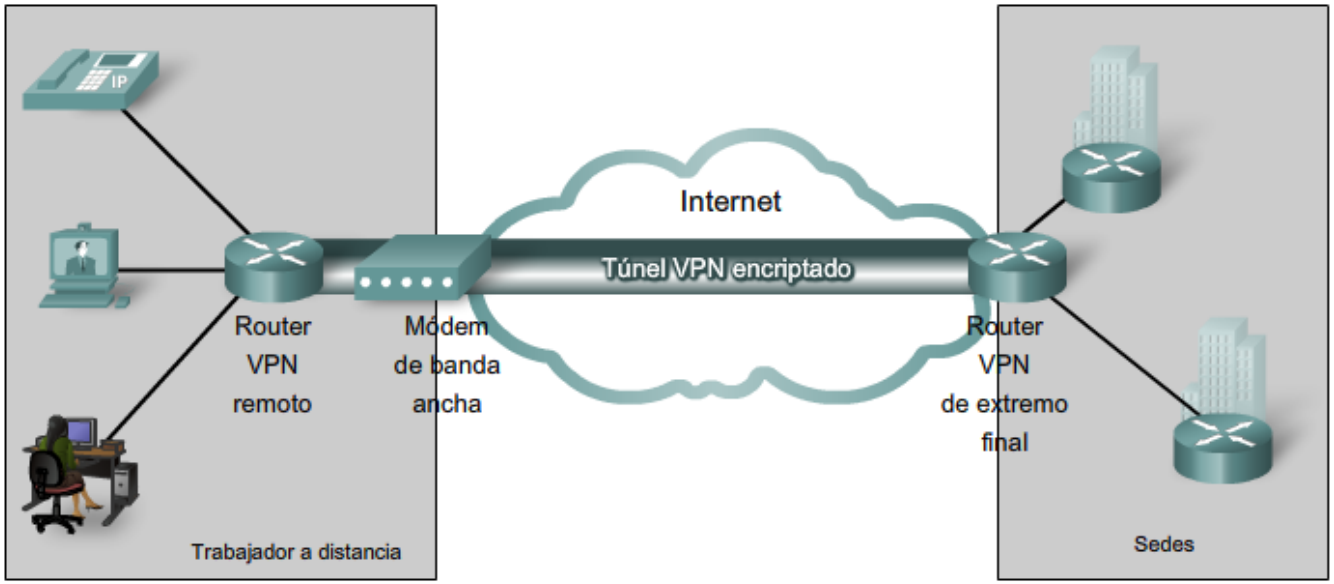
Opciones de conexión remota

- Tecnologías de capa 2 tradicionales
  - Frame Relay, ATM, líneas arrendadas
- Redes Privadas Virtuales (VPN) con IPSec
  - Conectividad Flexible y escalable
- Conexiones sitio a sitio
  - La más frecuente
  - Combina conexión de banda ancha para crear tunel VPN.



Requisitos de conectividad

- Componentes de oficina doméstica
  - Portátil o PC
  - Acceso a banda ancha (cable o DSL)
  - Router VPN o Software cliente de VPN
- Componentes corporativos
  - Router con capacidades de VPN
  - Concentradores VPN
  - Aplicaciones de seguridad

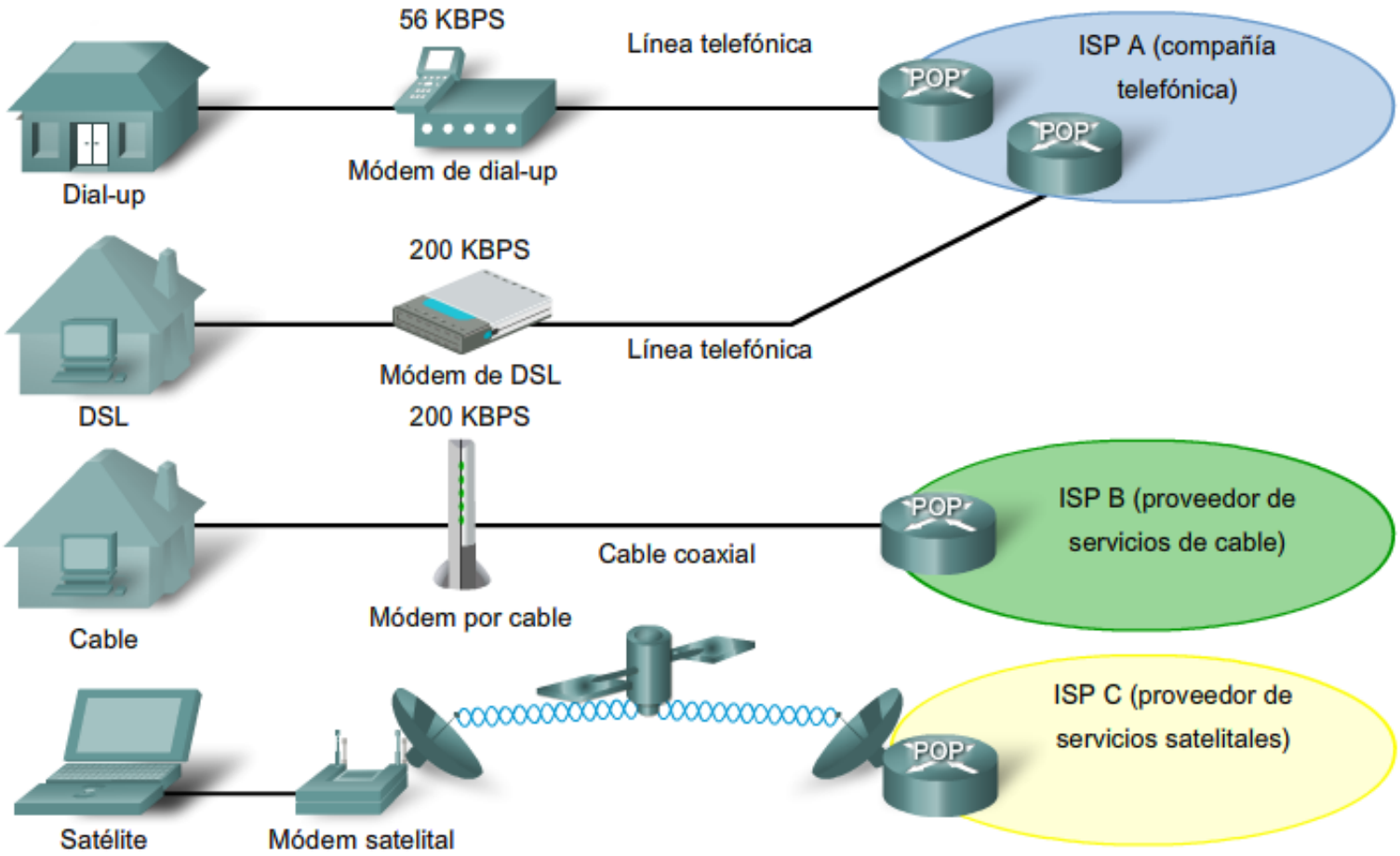


Componentes de soluciones de trabajadores a distancia

- Componentes de la oficina hogareña
- Componentes corporativos
- Componentes corporativos de telefonía IP opcionales

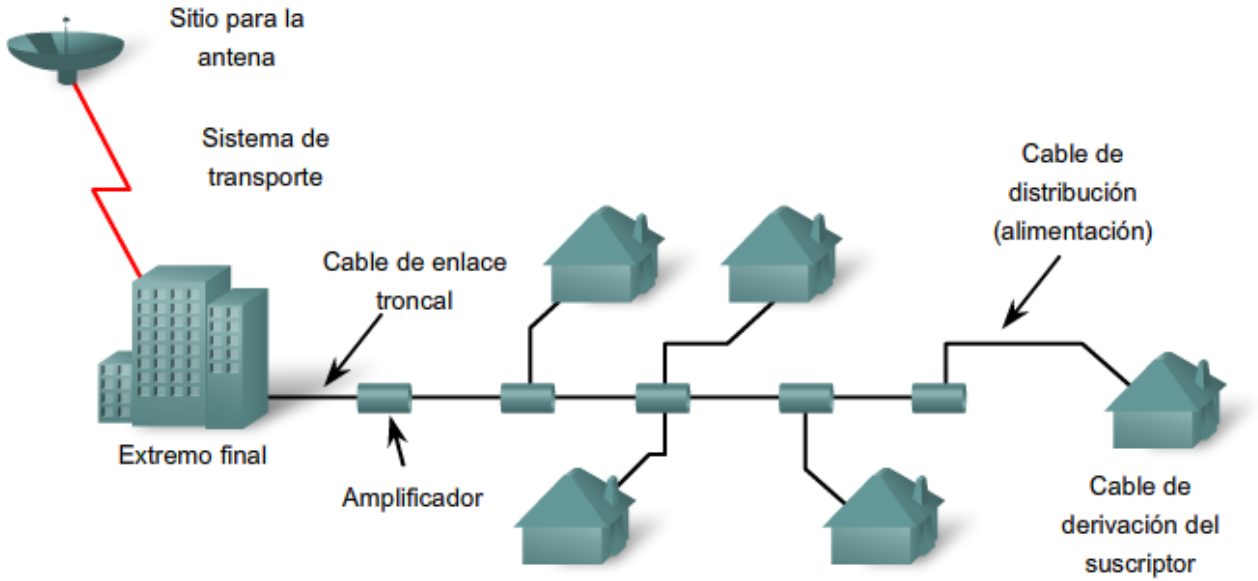
Servicios de banda ancha

- La elección de la tecnología de red de acceso y la necesidad de garantizar el ancho de banda adecuado son las primeras consideraciones que deben tenerse en cuenta cuando se conecta a los trabajadores a distancia.



Cable modem

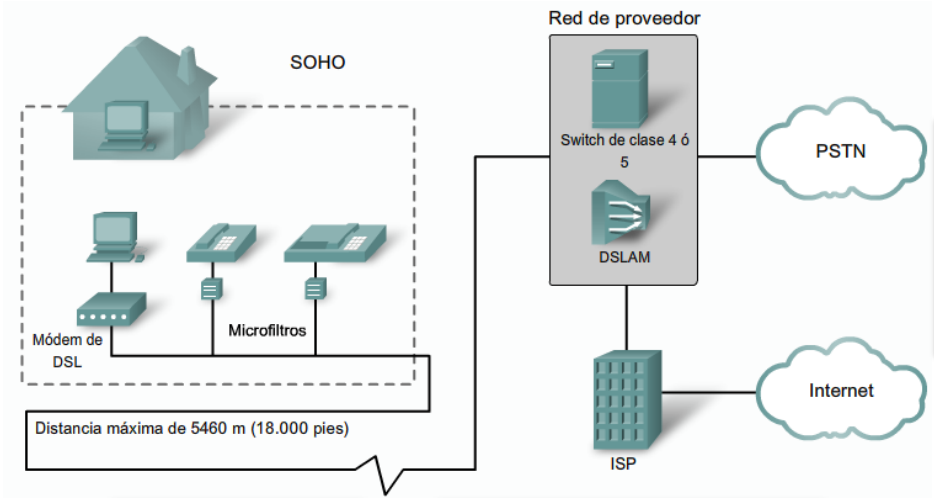
- Extremo final
  - Se reciben, se procesan y se formatean las señales.
- Red de Distribución
  - Enlaces troncales y de alimentación
- Cable de derivación del suscriptor
  - Conexión entre la parte de alimentación y dispositivo terminal.



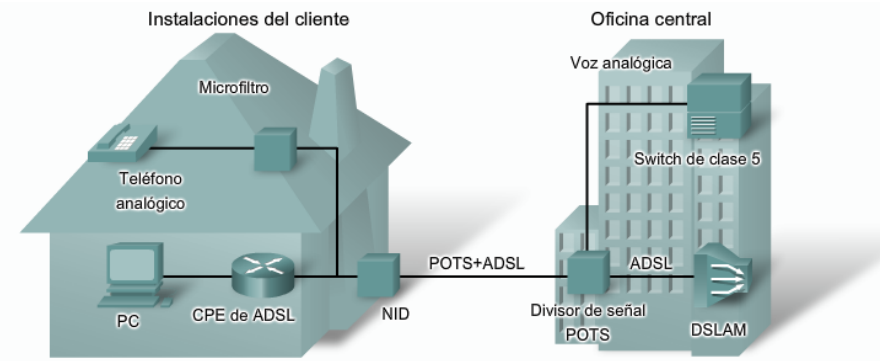
- Originalmente, CATV significaba "televisión por antena comunitaria" (Community Antenna Television). Este modo de transmisión compartía señales de televisión.
- Los sistemas de cable se construyeron originalmente para extender el alcance de las señales de televisión y mejorar la recepción de televisión por aire.
- Los sistemas de cable modernos utilizan cables de fibra y coaxiales para la transmisión de señales.

DSL

- Es una forma de proveer conexiones de alta velocidad mediante cables de cobre instalados
- DSL asimétrica (ADSL) usa un rango de frecuencia de 20 kHz a 1 MHz aprox.
- Para obtener un servicio satisfactorio, el bucle debe ser menor a 5,5 Km.



DSLAM: ubicado en la CO de la empresa de telecomunicaciones, combina conexiones DSL individuales de los usuarios en un enlace de alta capacidad al ISP y, por lo tanto, a Internet.

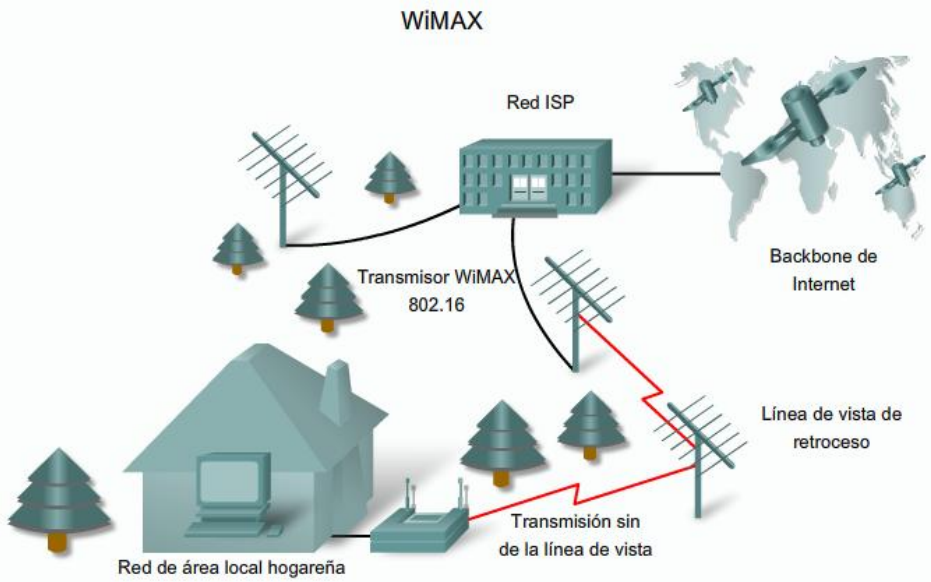


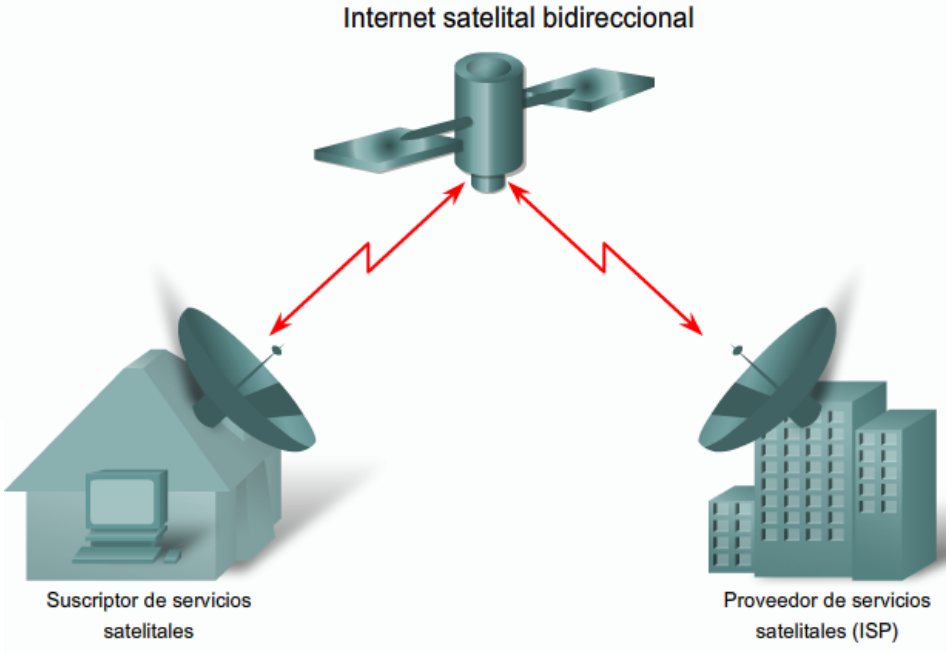
- Una función clave de ADSL es la coexistencia con POTS.
- La transmisión de señales de voz y datos se realiza en el mismo par de cables.
- Los circuitos de datos se descargan del switch de voz.

- Utiliza frecuencias de transmisión elevadas (hasta 1 MHz)
- Tecnología para enviar ancho de banda alto por líneas de cobre comunes
- Conexión entre el suscriptor y la CO

Conexión Inalámbrica de Banda Ancha

- Existen 3 tipos:
  - Wi-Fi Municipal (802.11)
  - WiMAX (802.16)
  - Internet Satelital





Estándares 802.11

- Wi-Fi es una certificación de interoperatividad de la industria que se basa en un subconjunto de 802.11.
- Los más populares hoy son 802.11b y 802.11g
- El reciente 802.11n, es una modificación propuesta que se basa en los estándares 802.11 anteriores por medio de la incorporación de entrada múltiple, salida múltiple (MIMO).

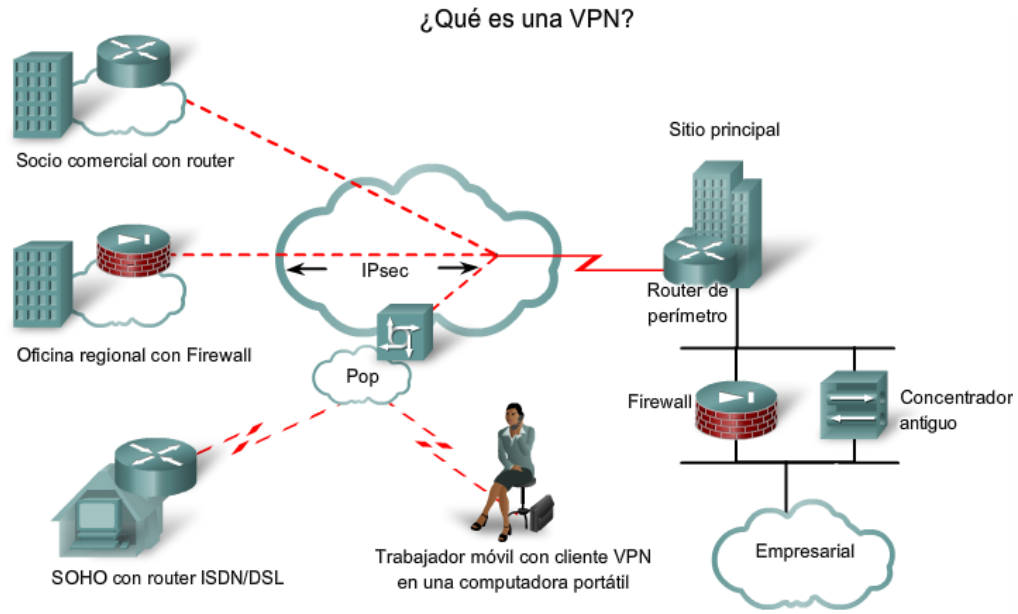
El estándar 802.16 (o WiMAX) permite transmisiones de hasta 70 Mbps y tiene un rango de hasta 50 km (30 millas). Puede funcionar en bandas con licencia o sin licencia del espectro desde 2 hasta 6 GHz.

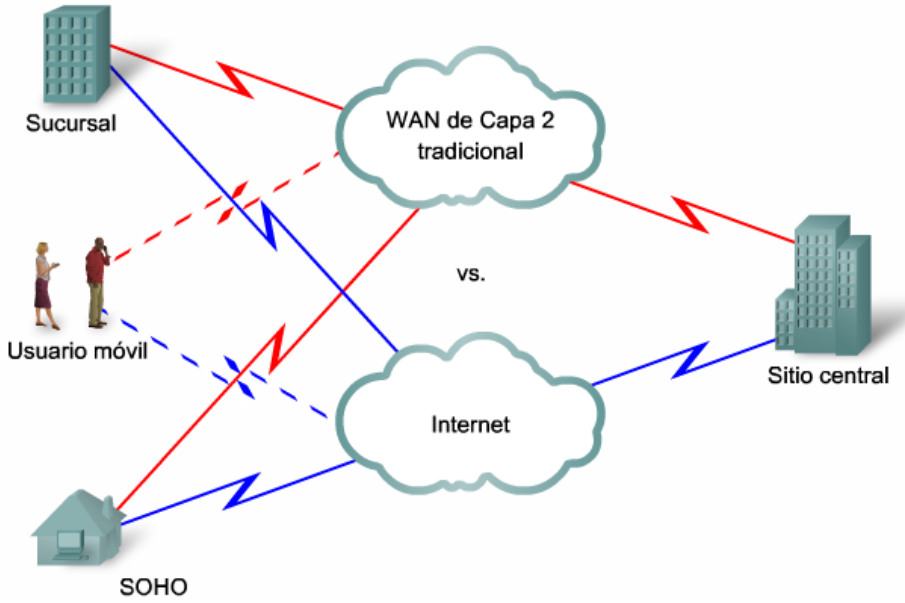
Generalmente, el equipo del trabajador a distancia utiliza el rango de 2,4 GHz que cumple con los siguientes estándares:

- 802.11b - 11 Mbps, 2,4 GHz
- 802.11g - 54 Mbps, 2,4 GHz
- 802.11e > 54 Mbps, MIMO, 2,4 GHz

Las redes VPN y sus beneficios

- Beneficios:
  - Rápidas
  - Fácil de llevar con usted donde sea que vaya (Escalables)
  - Permite ocultarse por completo del resto de la red.
  - Confiable (Seguras)
  - Cuesta poco agregar conexiones adicionales (Económicas)
- En vez de usar una conexión de Capa 2 exclusiva, como una línea alquilada, la VPN usa conexiones virtuales que se enrutan a través de Internet.

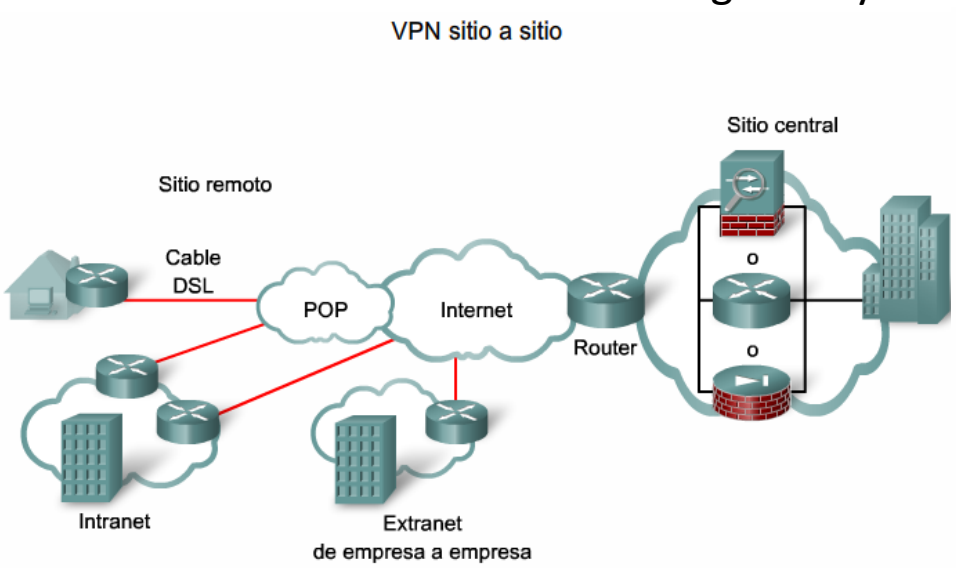




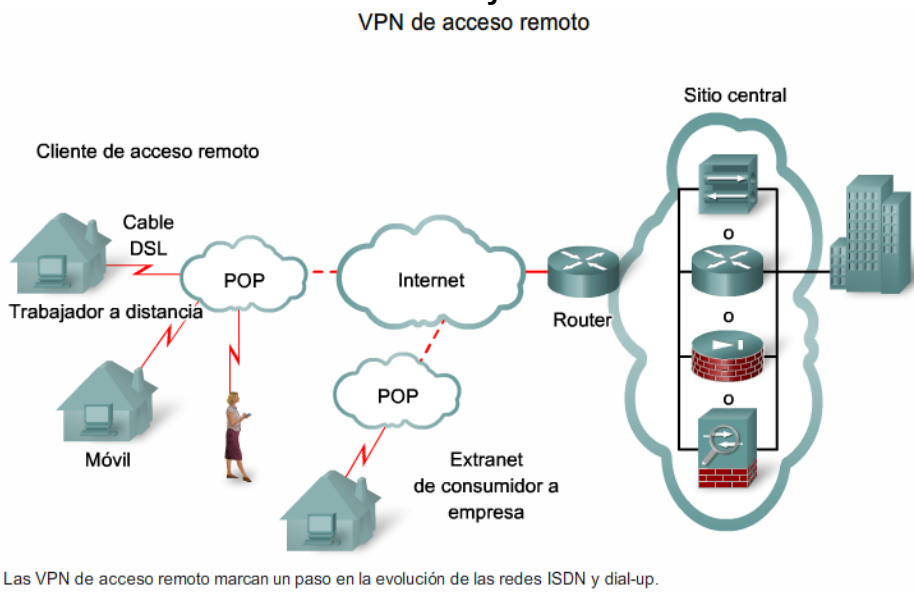
- Virtual: la información dentro de una red privada se transporta por una red pública.
- Privada: el tráfico está encriptado para que los datos sean confidenciales.

Tipos de VPNs

- Sitio a sitio
  - En una VPN de sitio a sitio, los hosts envían y reciben tráfico TCP/IP a través de un gateway VPN, el cual podría ser un(a):
    - Router,
    - Aplicación firewall PIX o
    - Aplicación de seguridad adaptable (ASA).
- Acceso Remoto
  - Cada host en general tiene software cliente de VPN.
  - El software cliente de VPN encapsula y encripta ese tráfico antes del envío a través de Internet hacia el gateway VPN en el borde de la red objetivo.



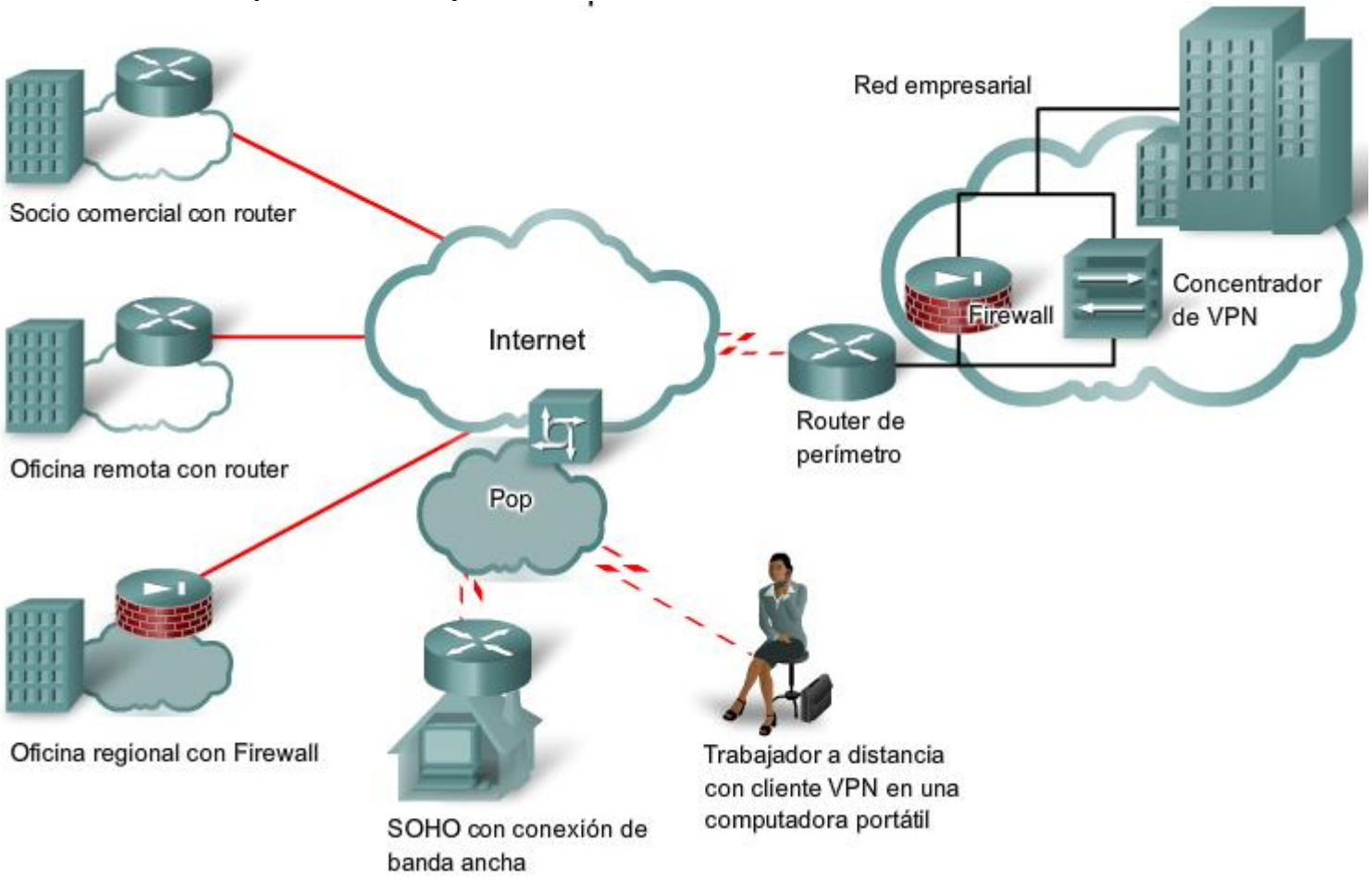
Las VPN de sitio a sitio son extensiones de la WAN clásica.



Las VPN de acceso remoto marcan un paso en la evolución de las redes ISDN y dial-up.

Componentes de una VPN

- Una red existente con servidores y estaciones de trabajo
- Una conexión a Internet
- Gateways VPN, como routers, firewalls, concentradores VPN y ASA, que actúan como extremos para establecer, administrar y controlar las conexiones VPN
- Software adecuado para crear y administrar túneles VPN



Características de una VPN segura

- Utilizan técnicas de encriptación avanzada y tunneling para permitir que las conexiones de red privadas de extremo a extremo que establezcan las organizaciones a través de Internet sean seguras.
- Las bases son:

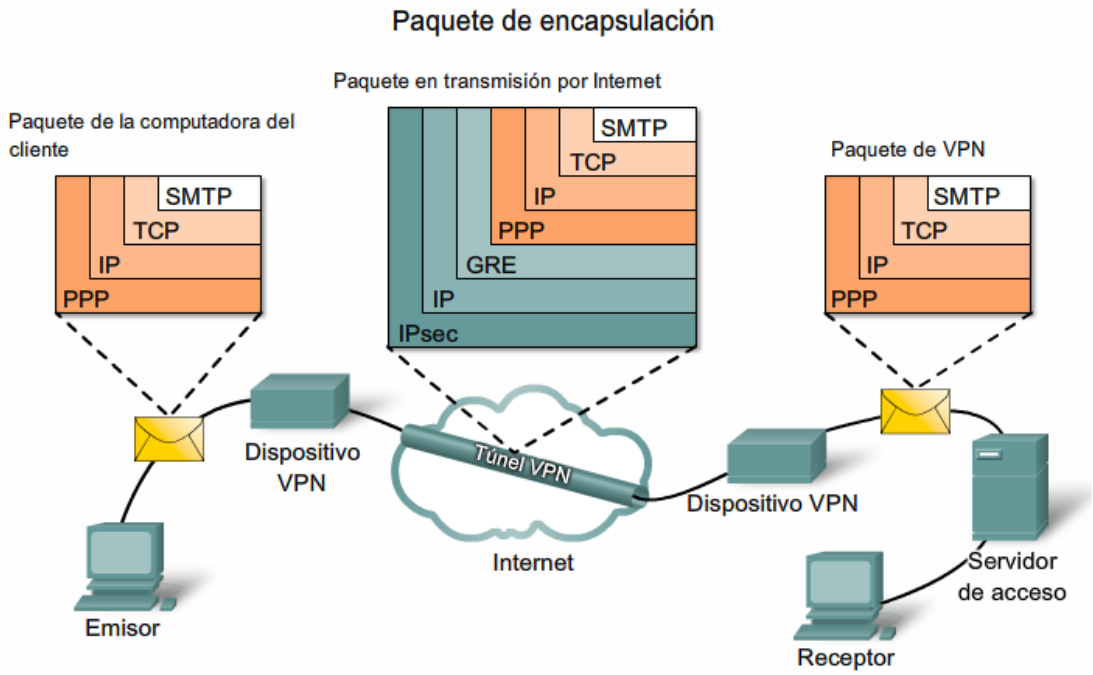
Característica	Propósito
Confidencialidad de datos	Protege los datos contra personas que puedan ver o escuchar subrepticiamente información confidencial (spoofing).
Integridad de datos	Garantiza que no se realicen cambios indebidos ni alteraciones en los datos.
Autenticación	Garantiza que sólo ingresen en la red emisores y dispositivos autorizados.

La confidencialidad de datos y la integridad de datos dependen de la encriptación y la encapsulación

Tunneling VPN

- El tunneling permite el uso de redes públicas como Internet para transportar datos para usuarios, siempre que los usuarios tengan acceso a una red privada.

En envió de tarjeta navideña:
Tarjeta → Pasajero
Sobre → Encapsulación
Oficina → Portador



Protocolos de tunneling

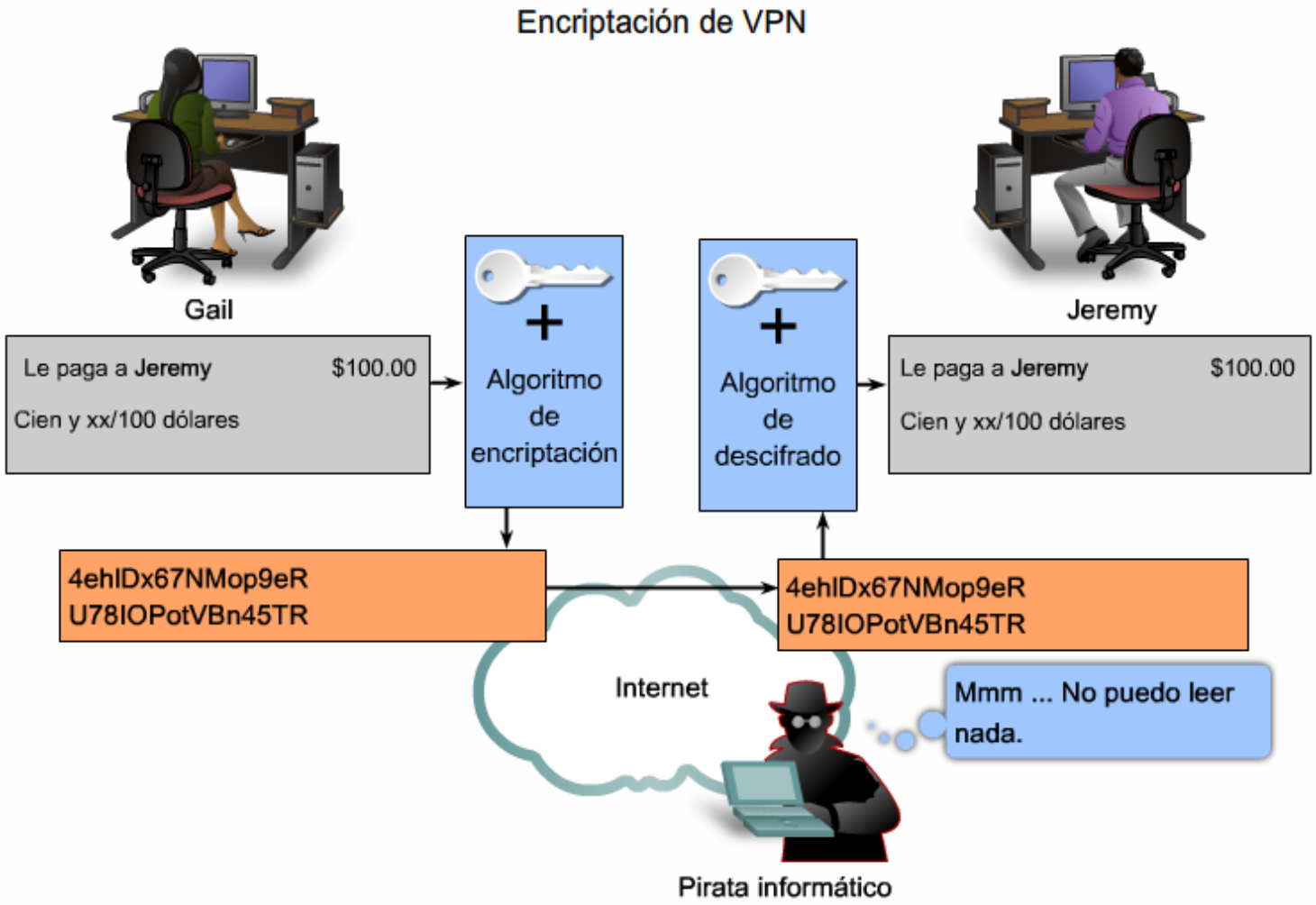
Protocolo portador:
- protocolo por el cual viaja la información (Frame Relay, ATM, MPLS).

Protocolo de encapsulación:
- protocolo que envuelve los datos originales (GRE, IPSec, L2F, PPTP, L2TP).

Protocolo pasajero:
- protocolo por el cual se transportan los datos originales (IPX, AppleTalk, IPv4, IPv6).

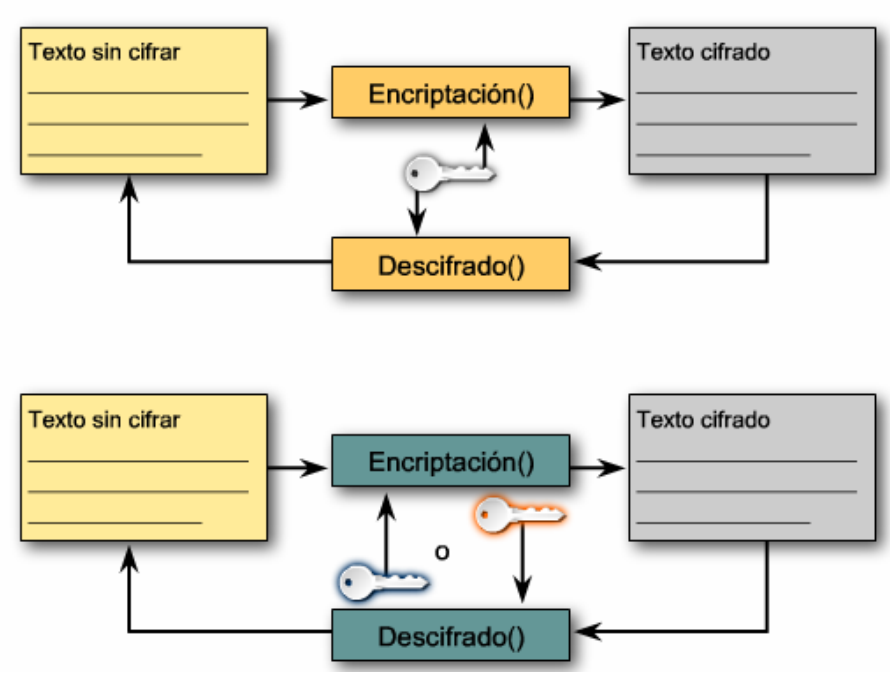
Integridad de datos en las VPN

- Para mantener la privacidad de los datos, es necesario cifrarlos.
- Para que la encriptación funcione, tanto el emisor como el receptor deben conocer las reglas que se utilizan para transformar el mensaje original en la versión codificada.



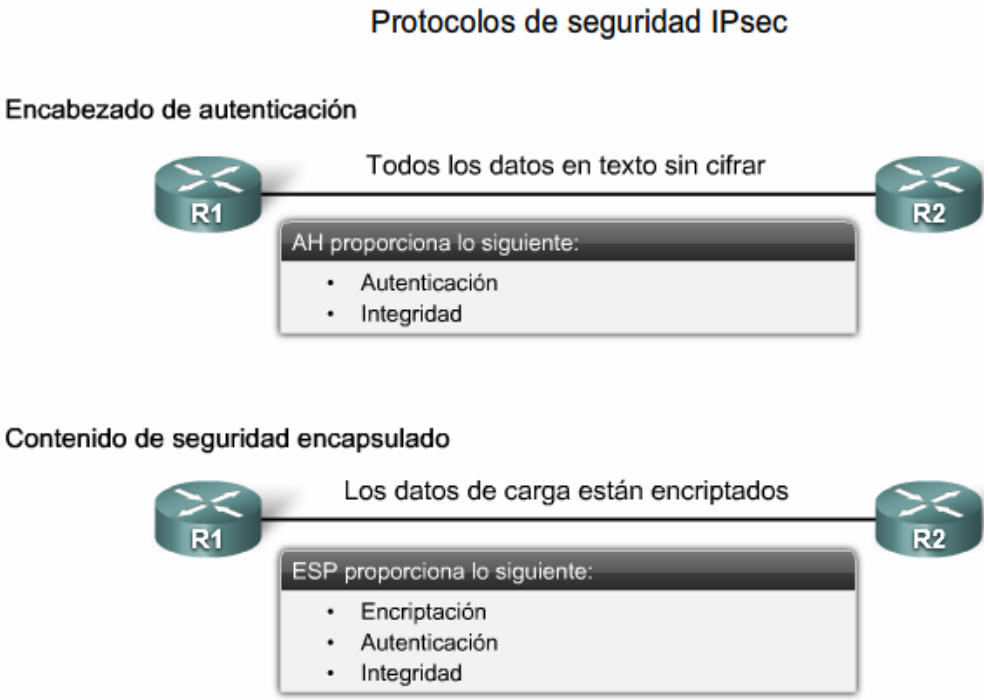
Algoritmos de Cifrado

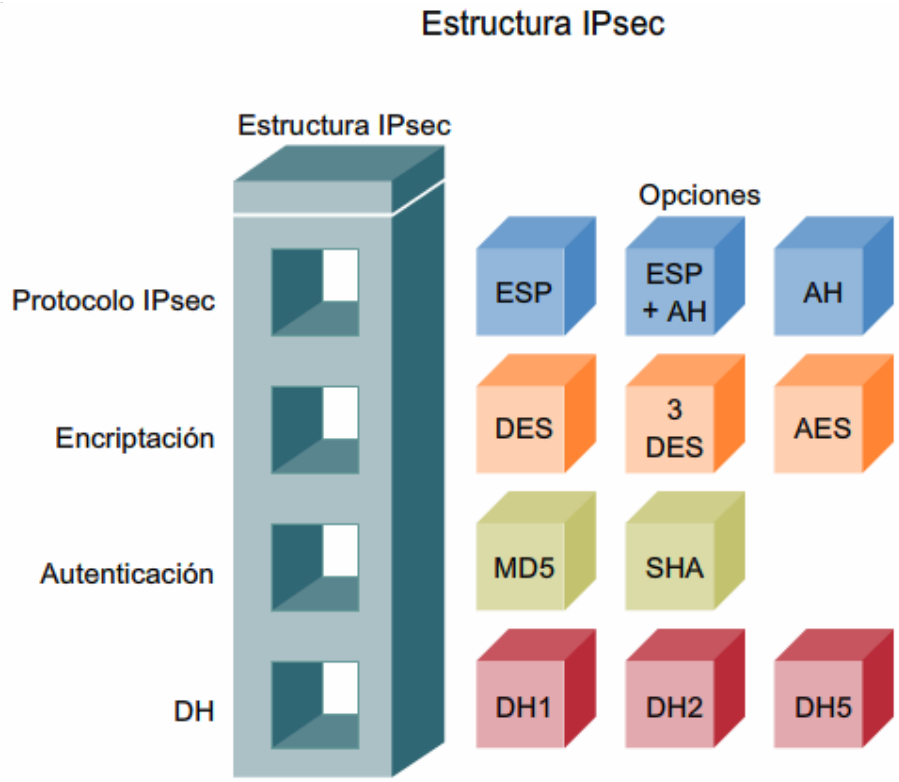
- Simétricos
  - Criptografía de llaves secretas
  - El cifrado y descifrado utilizan la misma llave
  - Ejemplo: DES, 3DES, AES
- Asimétricos
  - Criptografía de claves privadas
  - El cifrado y descifrado utilizan llaves diferentes
  - Ejemplo: RSA



Integridad de datos en las VPN

- Existen 2 protocolos de estructura IPSec.
  - AH (Authentication Header)
    - Se utiliza cuando no se requiere confidencialidad
  - ESP (Encapsulating Security Payload)
    - Cifra el paquete IP
- IPsec se basa en algoritmos existentes para implementar la encriptación, la autenticación y el intercambio de claves.





Resumen

- Proporcionar servicios de trabajadores a distancia nos brinda:
  - Continuidad en las operaciones
  - Provee servicios adicionales
  - Acceso seguro y confiable a la información
  - Económicos
  - Escalables
- Componentes necesarios por los trabajadadores a distancia para conectarse a la red empresarial:
  - Componentes en la casa
  - Componentes corporativos

Resumen

- Servicios de Banda Ancha usados:
  - –Cable
    - Transmite la señal en ambas direcciones simultáneamente
  - –DSL
    - Requiere cambios mínimos a la infraestructura telefónica disponibles
    - Proporciona altos anchos de banda a los usuarios.
  - –Inalámbricos
    - Incrementa la movilidad
    - Están disponibles vía:
      - »WiFi municipal
      - » WiMax
      - » Internet Satelital

Resumen

- Asegurando los servicios de trabajadores a distancia:
  - Se logra la seguridad de las VPN usando:
    - Técnicas avanzadas de cifrado
    - Tunneling
  - Características de una VPN segura:
    - Confidencialidad de datos
    - Integridad de datos
    - Autenticación