

# VPN

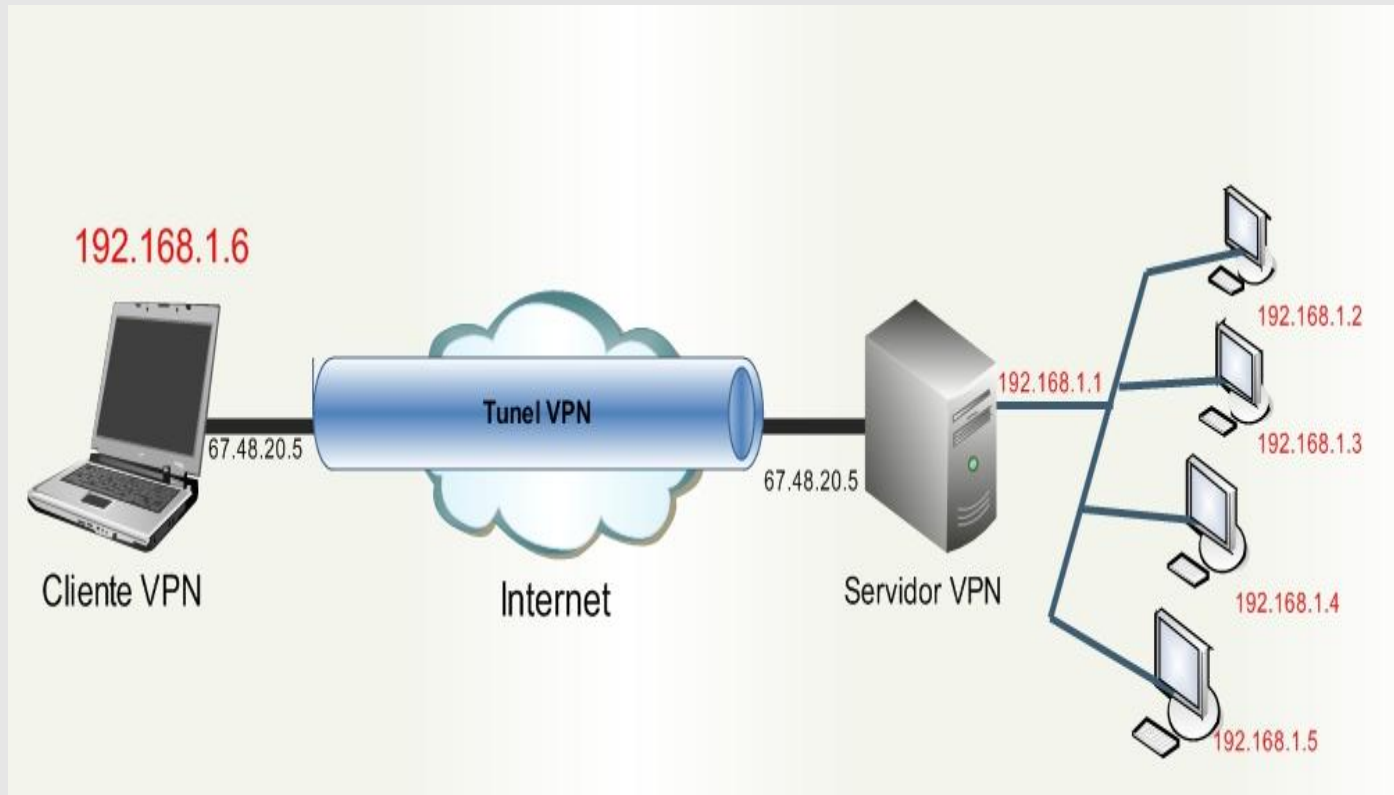
Redes Virtuales Privadas



- ❖ ¿ Qué es una VPN?
- ❖ Tecnologías Anteriores.
- ❖ Descripción de las VPN.
- ❖ Arquitecturas VPN.
- ❖ Tunelamiento.
- ❖ PPTP (Protocolo de Túnel Punto a Punto).
- ❖ L2TP (Protocolo de Túnel de Capa 2).
- ❖ VPN SSL (Secure Layer Socket).
- ❖ Servidores VPN con IP-Dinámicas.

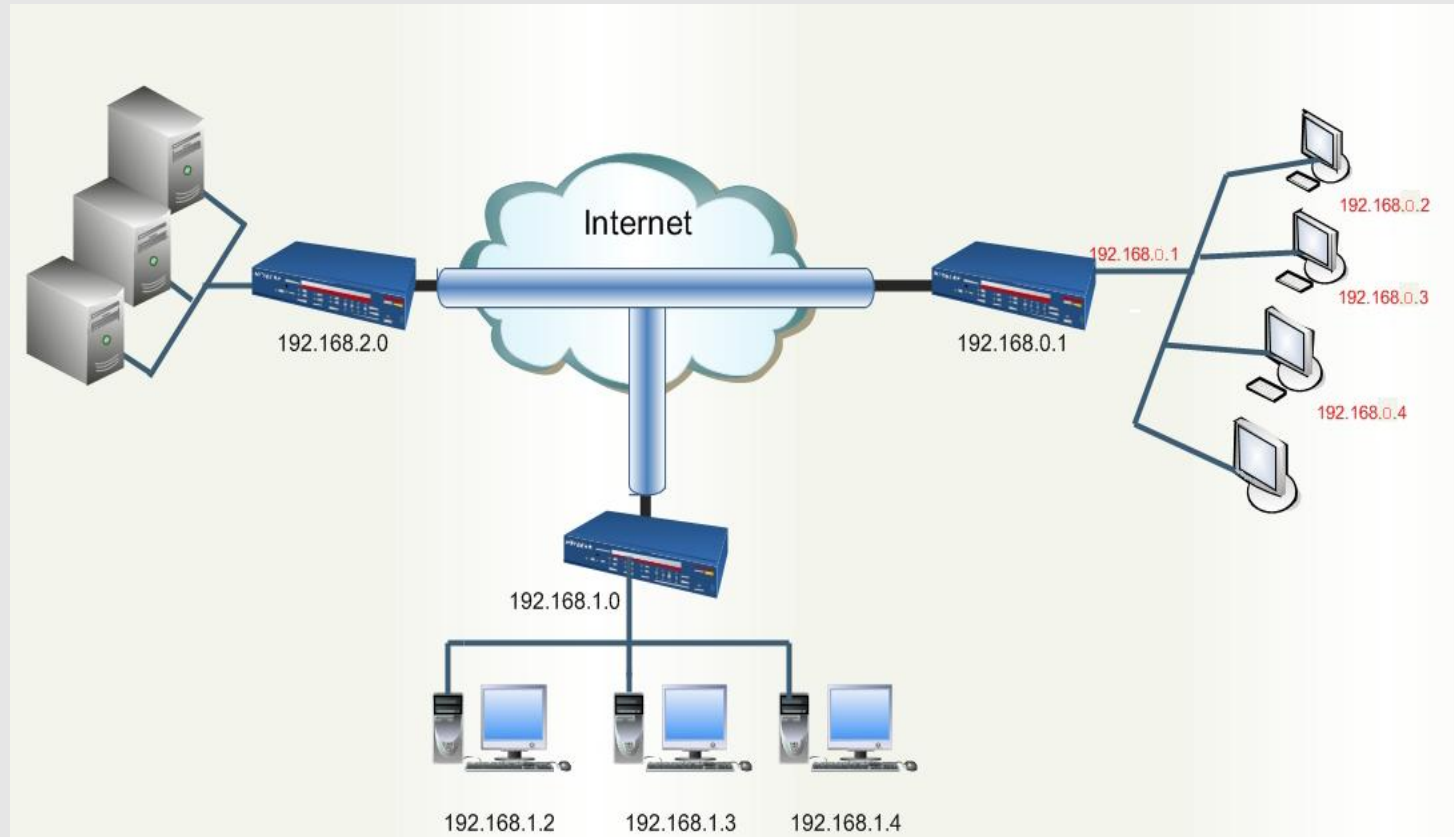
*“Las Redes Virtuales Privadas (VPN) son un concepto de tecnología que permite conectar varias LAN’s o estaciones remotas entre sí, de forma segura y confidencial, a través de un medio inseguro como INTERNET, mediante el uso de la autenticación, encriptación y túneles para las conexiones.”*

# ¿Qué se puede hacer con una VPN?



Arquitectura Cliente to Lan.

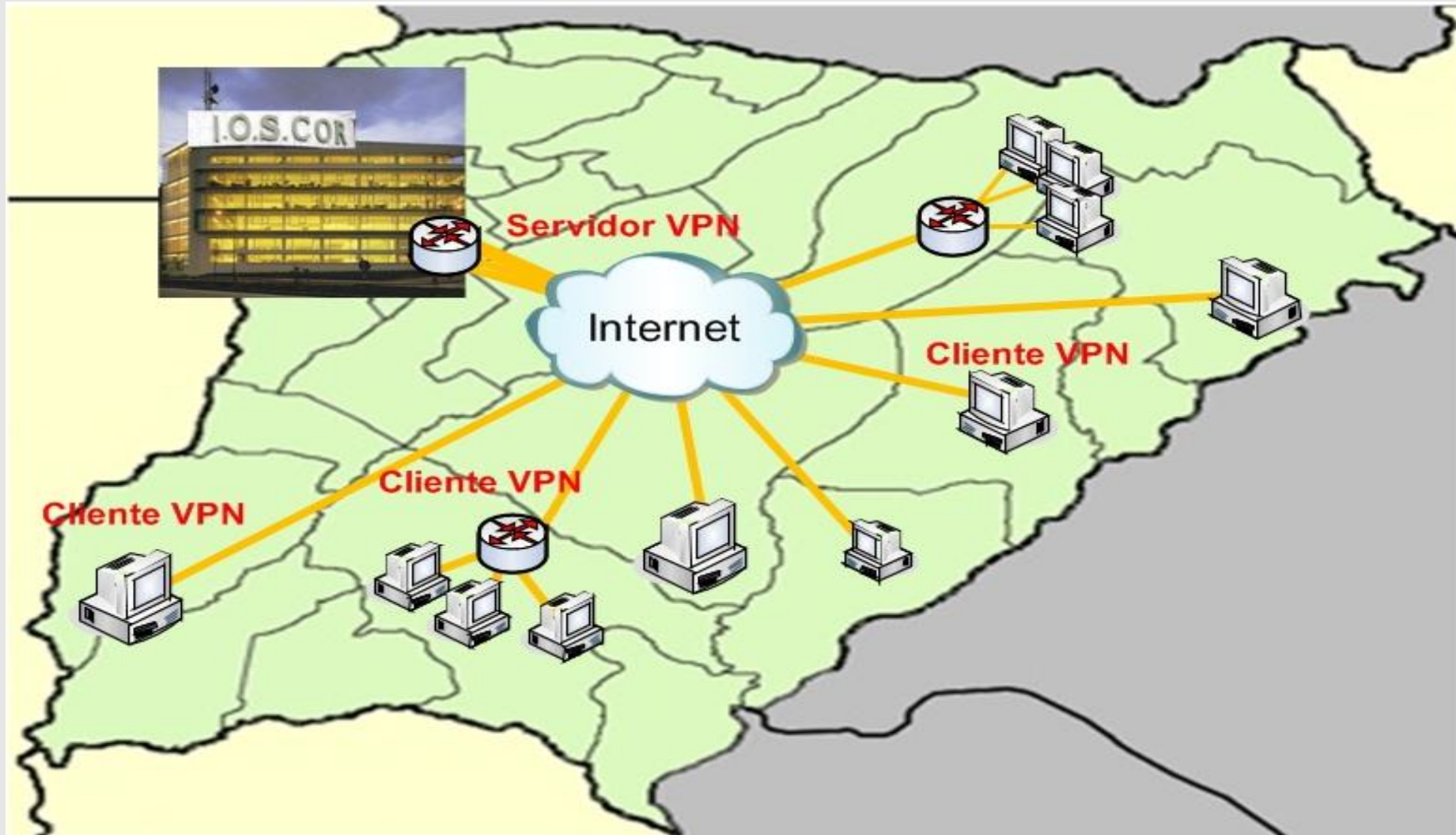
# ¿Qué se puede hacer con una VPN?



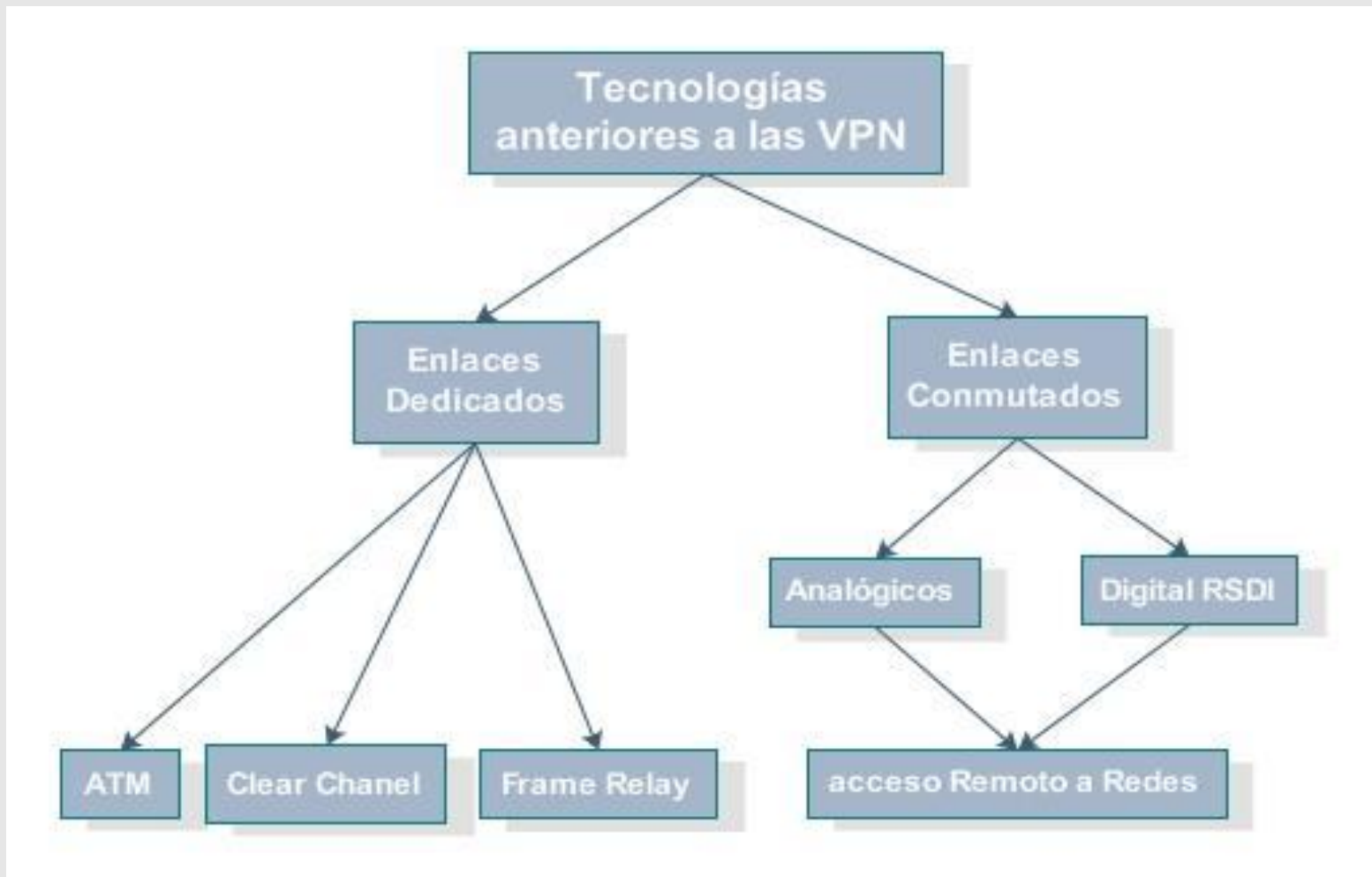
Arquitectura Lan-to-Lan.

# Ejemplo de Uso de una VPN en la Provincia de Corrientes

VPN  
Network Virtual Private



# Tecnologías Anteriores





## ENLACES DEDICADOS

Fueron la primera tecnología WAN que se adoptó usando la infraestructura de voz de los distintos operadores de telefonía.

Se necesitaban conexiones físicas reales necesitando de un proveedor en cada sitio resultando en una sola línea de comunicación entre dos partes.

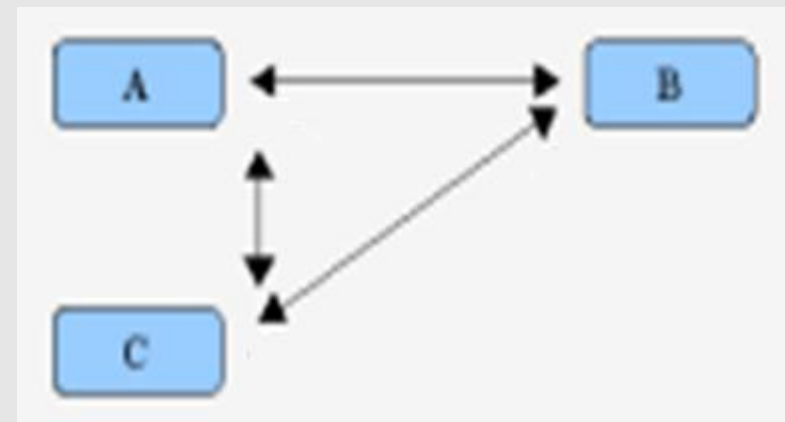




## ENLACES DEDICADOS

Fueron la primera tecnología WAN que se adoptó usando la infraestructura de voz de los distintos operadores de telefonía.

Se necesitaban conexiones físicas reales necesitando de un proveedor en cada sitio resultando en una sola línea de comunicación entre dos partes.

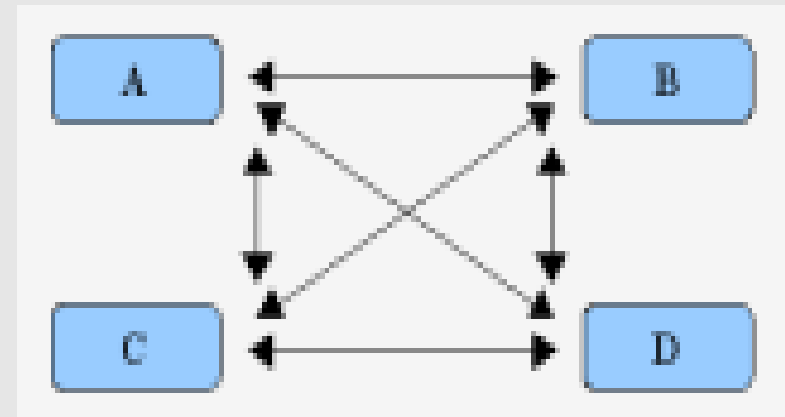




## ENLACES DEDICADOS

Fueron la primera tecnología WAN que se adoptó usando la infraestructura de voz de los distintos operadores de telefonía.

Se necesitaban conexiones físicas reales necesitando de un proveedor en cada sitio resultando en una sola línea de comunicación entre dos partes.



## ENLACES DEDICADOS

- Son enlaces donde solo interviene la red de transporte del proveedor de servicios.
- Para el mercado corporativo comúnmente van desde los 64 kbit/s hasta los 2048 kbit/s.

## ENLACES DEDICADOS

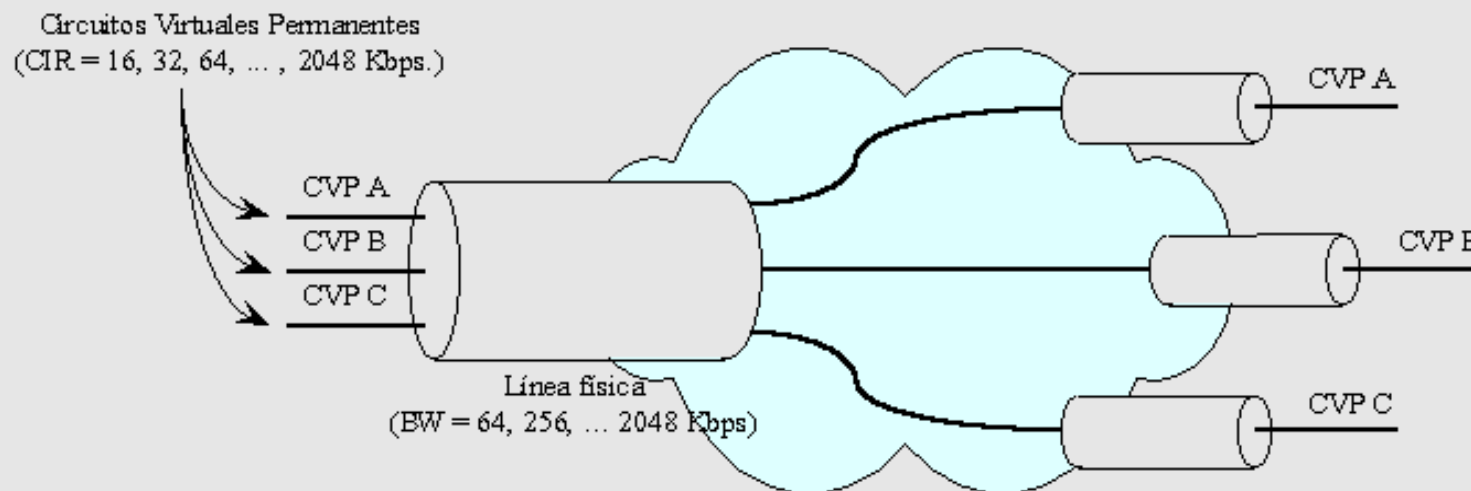
- Son enlaces donde solo interviene la red de transporte del proveedor de servicios.
- Van desde los 64 kbps a 2048 kbps.
- Elevada eficiencia en las transmisiones.
- Tarifas planas (sin influencia del tráfico cursado) en función del ancho de banda contratado.



## FRAME RELAY

- Método de comunicación orientado a paquetes para la conexión de sistemas informáticos.
- Frame Relay es un protocolo WAN de alto rendimiento que trabaja en la capa física y de enlace de datos del modelo de referencia OSI.
- Permite compartir dinámicamente el medio y por ende el ancho de banda disponible.
- Ofrece un alto desempeño y una gran eficiencia de transmisión.
- Va desde 64 kbps hasta 4Mbps.

## FRAME RELAY



Circuitos Virtuales en Frame Relay.

## FRAME RELAY

### ❖ Ventajas

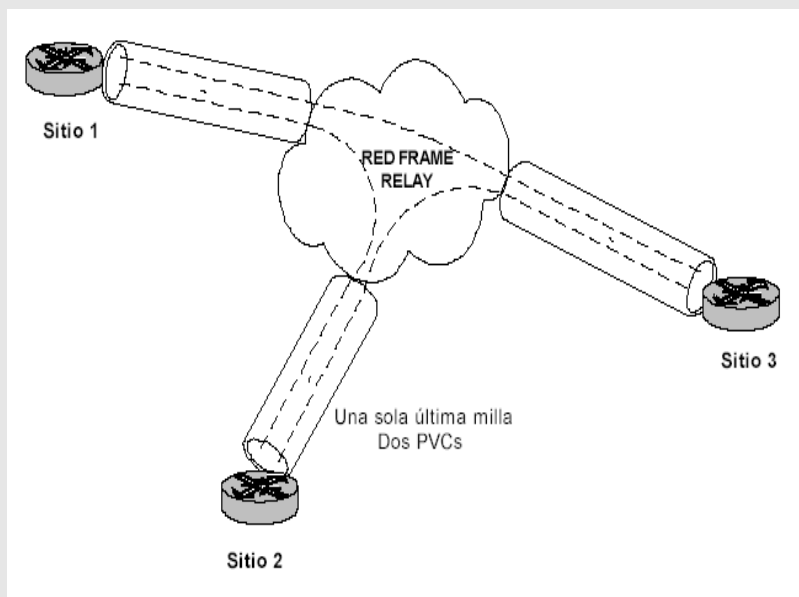
- Flexibilidad del servicio.
- Alta velocidad.
- Bajos retardos.
- Elevada eficiencia en las transmisiones.
- Gran capacidad de transmisión de información.
- Compromiso de *Calidad de Servicio (QoS)*.
- Diferentes canales pueden compartir una sola línea de transmisión.

## FRAME RELAY

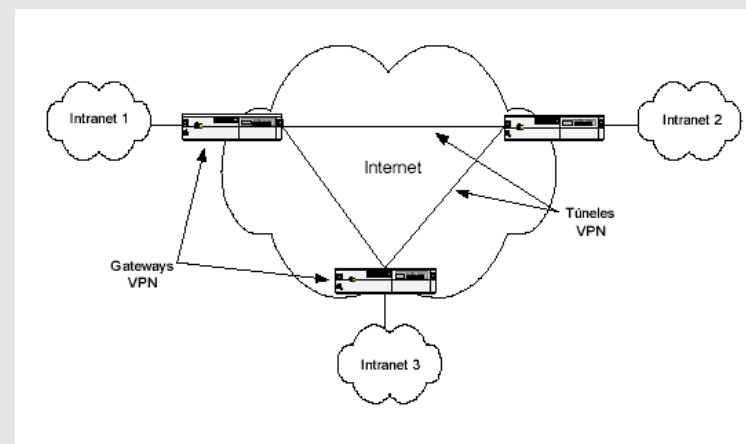
### ❖ Desventajas

- Carece de flexibilidad para alterar la topología de la red.
- Difíciles de administrar equipos de *acceso remoto*. Si, por ejemplo, se desea soportar un acceso remoto simultáneo para un total de hasta 200 usuarios, significa 200 líneas de salida, 200 módems y 200 conexiones al propio firewall.
- Estos enlaces también son susceptibles de caídas, y su montaje, en cuanto a hardware se refiere, es tan complejo que es prácticamente imposible cambiar a otro proveedor mientras el enlace se restablece.
- Costoso para conectar múltiples puntos.

## Solución Frame Relay



## Solución VPN-IP



## ATM

- ATM (Asynchronous Transfer Mode / Modo de Transferencia Asíncrono) es un protocolo de transporte de alta velocidad.
- Actualmente tiene mucho uso como red troncal (Backbone).
- La velocidad de trabajo en ATM es 155 Mbps y 622 Mbps (4 canales a 155 Mbps).

## ATM

### ❖ Aplicaciones

- Intercambio de información en tiempo real.
- Interconexión de redes LAN que requieran un gran ancho de banda.
- Interconexión de PBX.
- Acceso a Internet de alta velocidad.
- Videoconferencia.

## ENLACES CONMUTADOS

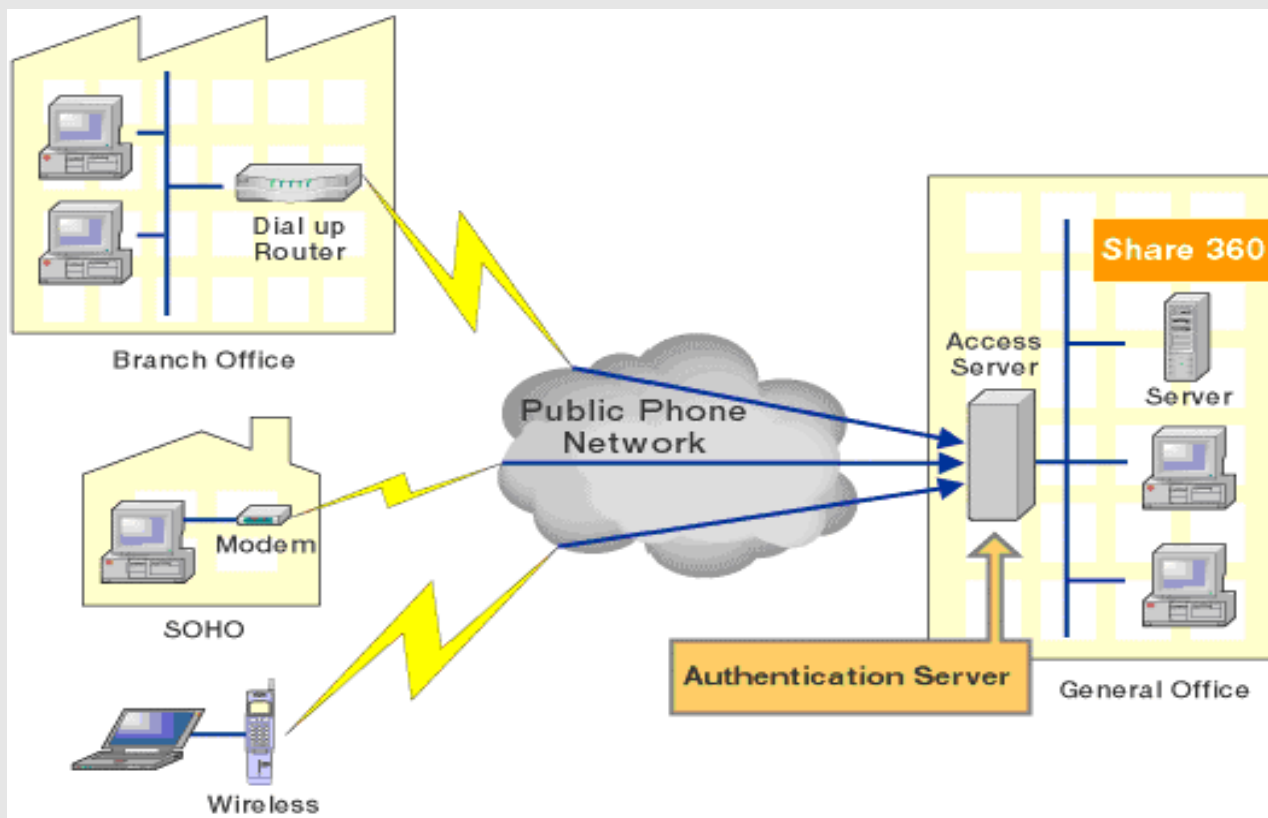
- Los enlaces conmutados se dividen en dos tipos:
  - **Analógicos:** llegan hasta velocidades de 53 kbps para el downlink y hasta de 48 kbps para el uplink.
  - **Digitales:** transmiten a 64 kbps o 128 kbps. Estos últimos son conocidos como enlaces RDSI (*Red Digital de Servicios Integrados*).



## ACCESO REMOTO A REDES (RAS)

- En este tipo de arquitecturas existe un RAS (*Remote Access Server*) que actúa como una puerta de enlace entre el *cliente remoto* y la *red*. Después de que un usuario haya establecido la conexión por medio de una llamada, la línea telefónica es transparente para el usuario, y este puede tener acceso a todos los recursos de la red como si estuviera ante un equipo directamente conectado a ella.
- Este tipo de implementación fue el antecesor más próximo de las VPN-IP, sus deficiencias radican en los costos de las llamadas que se deben efectuar, principalmente las de larga distancias y la falta de confidencialidad en la transmisión de la información ya que no soportan encriptación de datos.

## ACCESO REMOTO A REDES (RAS)



Escenario Típico de un Acceso Remoto a Redes

## ACCESO REMOTO A REDES (RAS)

También es común pero poco eficiente utilizarlo para realizar la conexión de *acceso a Internet* que luego se va a utilizar para establecer la VPN.



Red Virtual Privada sobre una conexión RAS

## PROTOCOLO PUNTO A PUNTO (PPP)

- El PPP es un protocolo de nivel de enlace estandarizado en el documento RFC 1661, 1662, 1663.
- Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet.
- Proporciona un modo estándar para transportar datagramas multiprotocolo sobre enlaces simples punto a punto entre dos pares.
- Generalmente se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico.
- Ocasionalmente también es utilizado sobre conexiones de banda ancha (como PPPoE o PPPoA).
- Otro uso es utilizarlo para conectar a *usuarios remotos* con sus oficinas a través del RAS de su empresa.

## PROTOCOLO PUNTO A PUNTO (PPP)

### ❖ Fases de PPP

- Fase Previa: se establece la conexión física, por ejemplo el cliente PPP realiza una llamada telefónica al modem del ISP.
- Fase 1: Establecer el enlace del PPP.
- Fase 2: Autenticación de Conexión.
- Fase 3 (opcional): Control de rellamado del PPP.
- Fase 4: Invocar los Protocolos de Nivel de Red.
- Fase 5: Transferencia de Datos.
- Fase 6: Finalización de la Conexión.



The screenshot shows the 'Internet Settings' page of a 3COM OfficeConnect Cable/DSL Router. On the left is a navigation menu with options: Setup Wizard, LAN Settings, Internet Settings (highlighted), DNS, Hostname & MAC, Firewall, VPN, SNMP, System Tools, Advanced, and Status and Logs. The main content area is titled 'Internet Settings' and contains a section 'Select your connection type' with the instruction: 'The following information is usually provided by your ISP. Please select the Internet sharing protocol.' Below this are four radio button options: Dynamic IP Address, PPPoE (which is selected), PPTP, and Static IP Address.

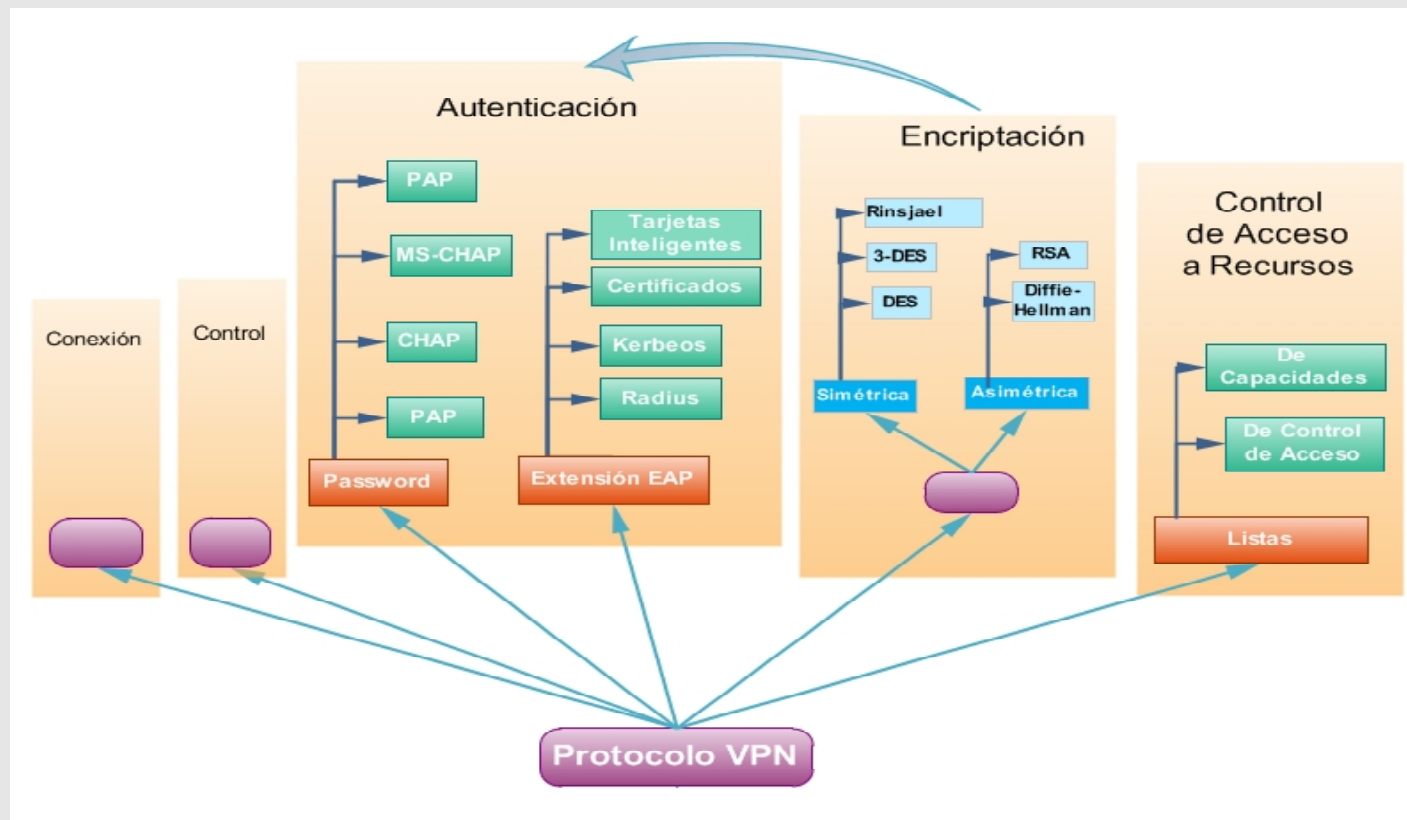
Configuración de Tipo de Conexión a Internet.

The screenshot shows the 'PPPoE Interface' configuration page of the same 3COM OfficeConnect Cable/DSL Router. The page title is 'PPPoE Interface'. It contains several input fields: 'User Name' with the value 'delegoya@arnet-corr-glc', 'Password' and 'Retype Password' both masked with dots, and 'Service Name (Optional)' which is empty. The 'MTU (1200-1492)' field is set to '1454'. Below these fields is a note: 'Do not make changes to the MTU setting unless your ISP specifically different setting than 1492.' The 'Idle Timeout' is set to '10' minutes, with a note '(time in minutes; Enter 0 to never timeout)'. The 'Auto Reconnect After Timeout' checkbox is checked. At the bottom right, there are buttons for 'Help', '<<Back', 'Next>>', and 'Cancel'.

Configuración del Cliente PPPeE.

## ❖ OBJETIVOS DE UNA IMPLEMENTACIÓN VPN

- Proporcionar movilidad a los empleados (teletrabajo).
- Acceso a la base de datos central sin utilización de operadores telefónicos.
- Interconexión total a la red de todos los comerciales (empleados), de forma segura a través de una infraestructura pública.
- Correo electrónico corporativo.
- Flexibilidad y facilidad de uso.
- Fácil adaptación a las nuevas tecnologías.
- Reducción de costos a la hora de interconectar distintos puntos.

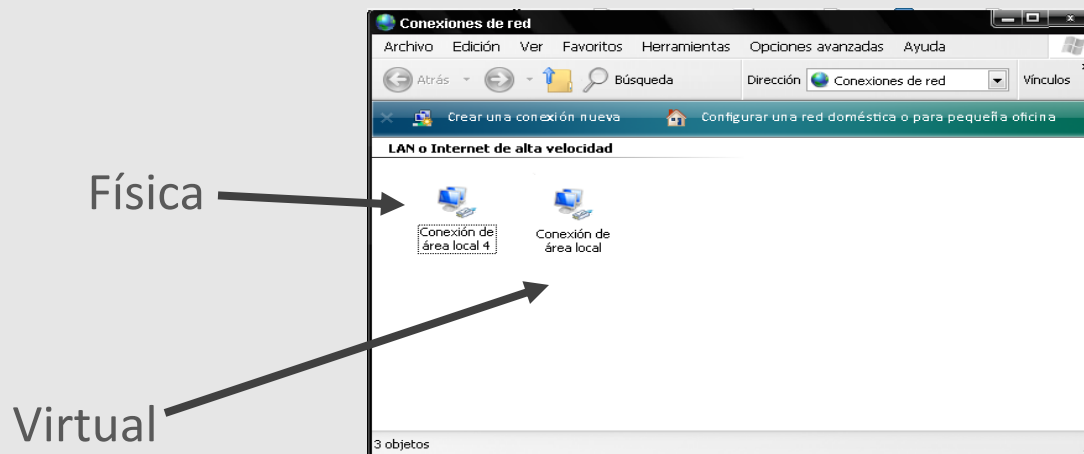


Etapas Necesarias de una Solución VPN.

# Funcionamiento Básico de una VPN

Tanto el Cliente como el Servidor cuentan, como mínimo, con lo siguiente:

- a) Conexión a Internet (condición necesaria para este ejemplo).
- b) Una *Interfaz de Red Física* para la conexión a Internet.
- c) Una *interfaz de red Virtual* que utiliza para conectarse a la Red Privada Virtual.
- d) Un *Puente Virtual* que conecta ambas interfaces.

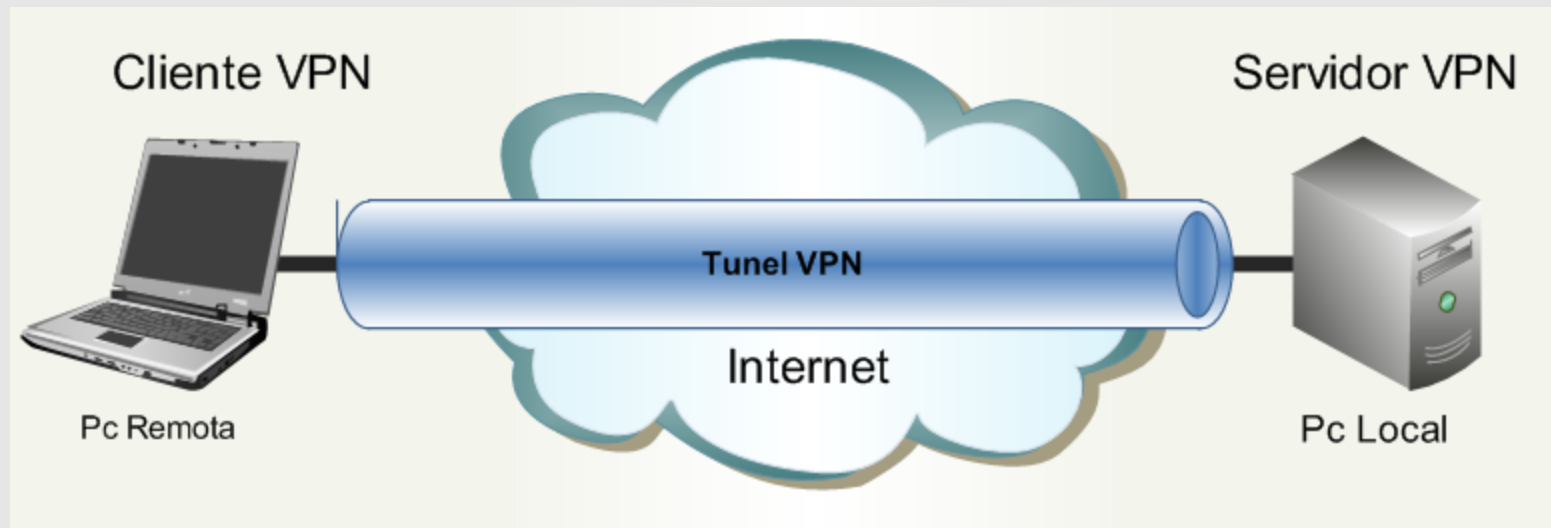


# Funcionamiento Básico de una VPN

VPN  
Network Virtual Private

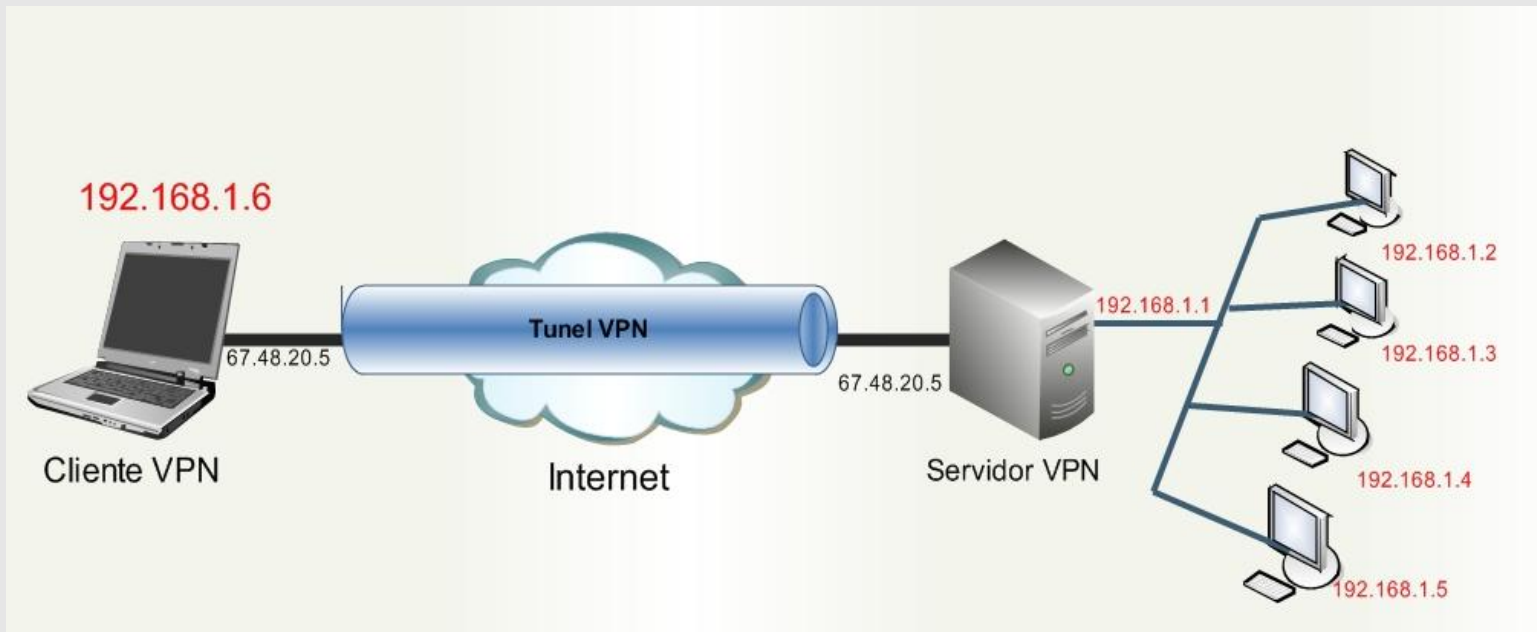
- 1 *Acceso Remoto.*
- 2 *Intranet LAN-to-LAN.*
- 3 *Extranet.*

1 Acceso Remoto.



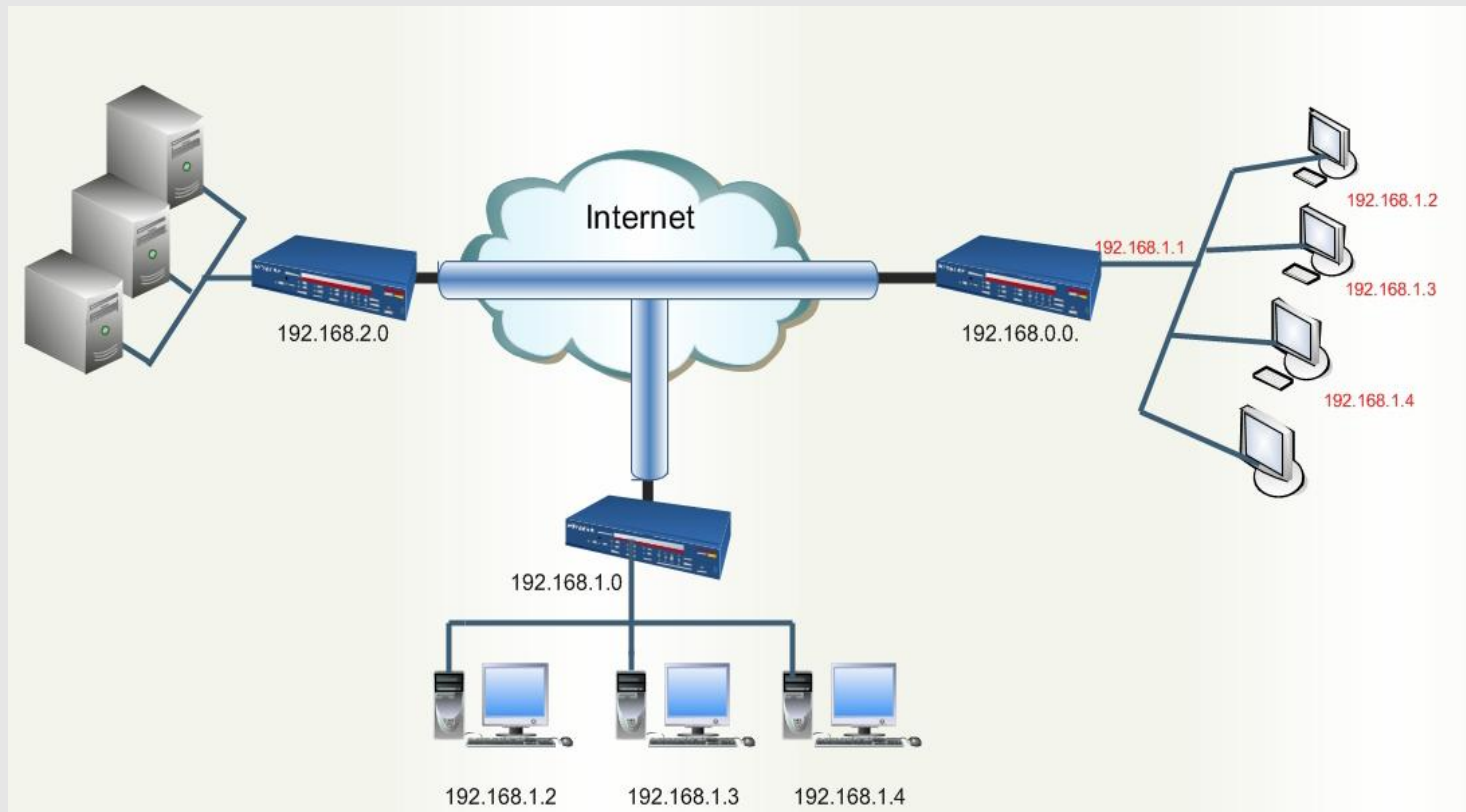
a) Clientes VPN a un Servidor VPN.

## 1 Acceso Remoto.



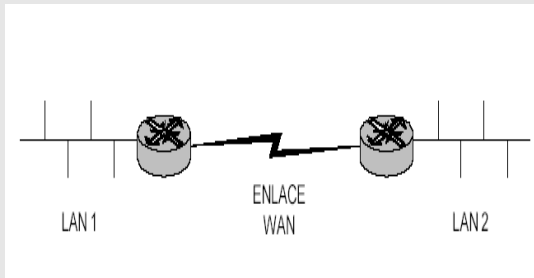
b) Clientes-VPN a una LAN.

## 2 Intranet Lan-to-Lan.

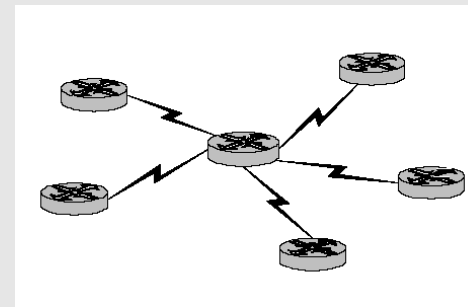


Conexión entre Distintas Redes.

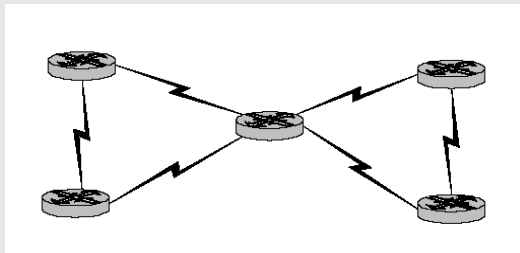
## 2 Intranet Lan-to-Lan.



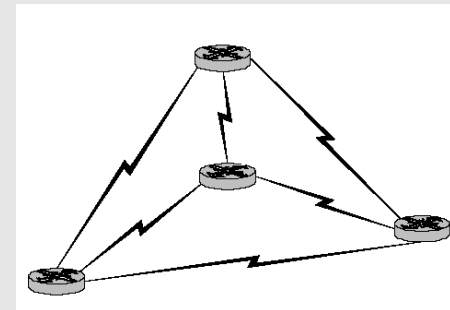
Lan-to-Lan



Estrella

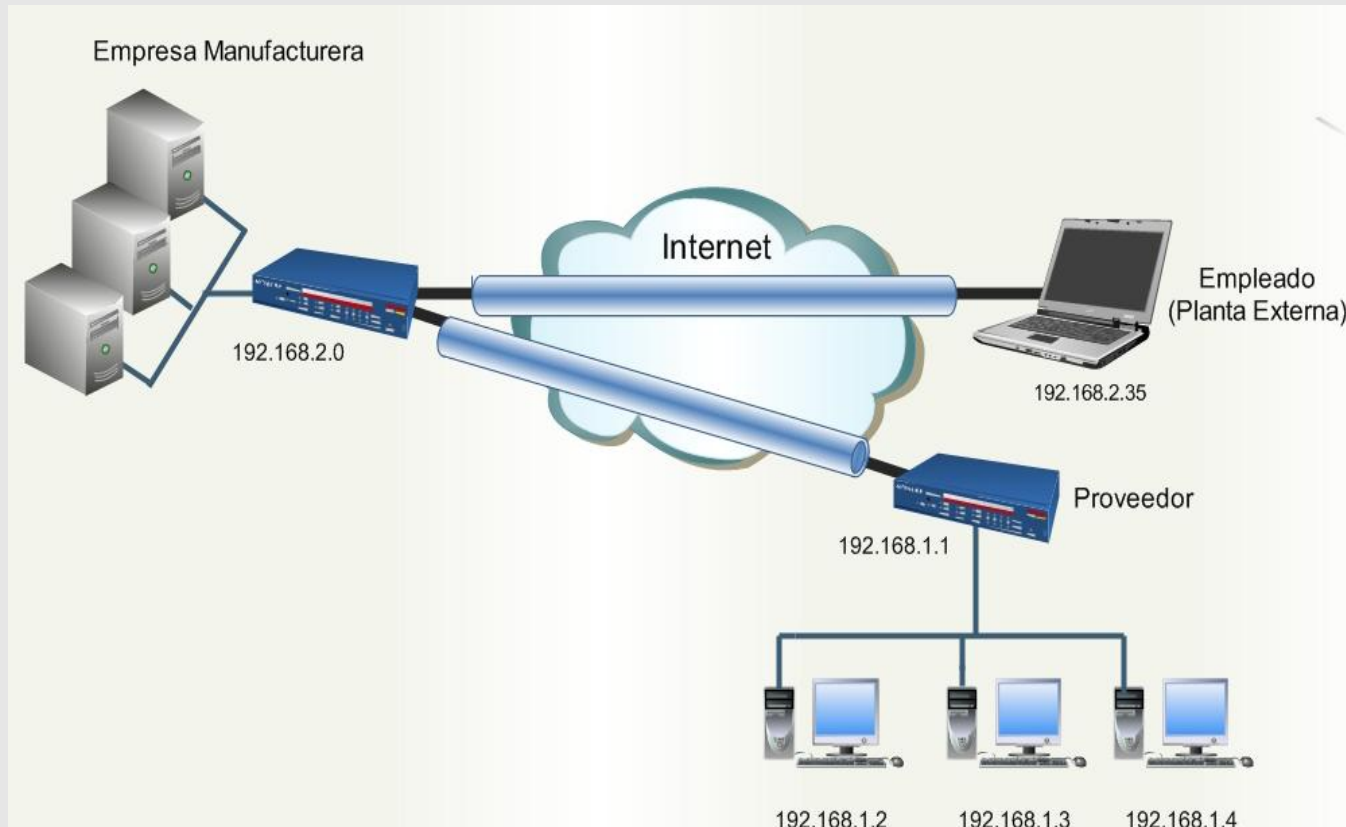


Malla Parcial



Malla Completa

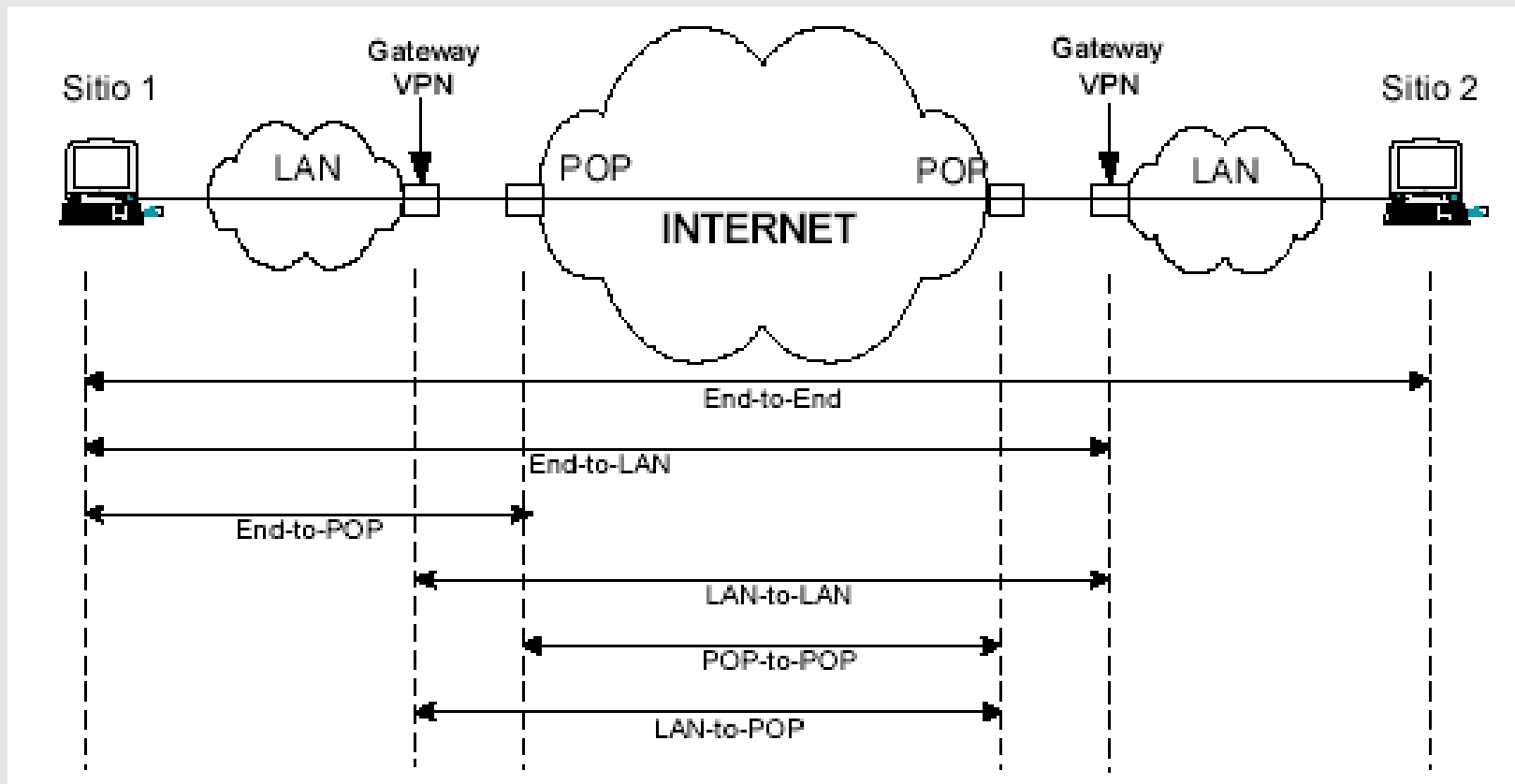
## 3 Extranet.



## Tipos de Tuneles



# Tunelamiento



Modelo de Tunelamiento.

- El proceso de Encriptación y Desencriptación se realiza a nivel físico.
- Se necesita equipos que permitan realizar esta tarea de forma transparente.
- Por lo general, los elementos utilizados son los Routers con VPN incorporada.
- Estos dispositivos llevan incorporado un procesador y algoritmos de encriptación.

## ❖ VENTAJAS DE LAS IMPLEMENTACIONES POR HARDWARE

- La instalación y la configuración son relativamente sencillas.
- No necesita personal especializado y su mantenimiento es mínimo.
- Un único elemento puede habilitar varias VPNs ubicadas en distintos sitios.
- El sistema es independiente de las máquinas conectadas a la red.
- No necesitamos máquinas dedicadas para realizar la VPN.

## ❖ INCONVENIENTES DE LAS IMPLEMENTACIONES POR HARDWARE

- El firmware de los sistemas es cerrado y se depende del fabricante para poder cambiarlo.
- Los sistemas de encriptación suelen ser cerrados y el fabricante suele utilizar un único tipo.
- En la mayoría de las ocasiones los elementos hardware de los extremos que componen la red privada virtual, deben ser iguales o por lo menos del mismo fabricante.
- La seguridad sólo se implementa desde los dos extremos de la VPN, siendo inseguro el camino que recorre la información desde el ordenador hasta el dispositivo VPN.



3Com® OfficeConnect® Cable/DSL Router

## Specifications

### Red privada virtual

- IPsec VPN, admite hasta 2 túneles IPsec
- El rendimiento de VPN IPsec es de hasta 4 Mbps+
- VPN PPTP, admite hasta 4 túneles PPTP
- El rendimiento de VPN PPTP es de hasta 10 Mbps
- Autenticación y administración de claves de Internet Key Exchange (IKE) y Manual key
- Autenticación (MD5 / SHA-1)
- Cifrado DES/3DES
- Cifrado AES 128/192/256
- Cabecera de autenticación (AH) IP
- Carga de seguridad encapsuladora (ESP) IP
- Concentrador VPN
- Compatibilidad con IPsec VPN dinámico
- NAT Traversal de IPsec (IPsec NAT-T)
- DPD (Dead Peer Detection) de IPsec
- Admite acceso remoto y conexiones IPsec oficina a oficina
- Servidor PPTP
- Netbios sobre VPN



## ZyWALL USG 100



Con integración de tecnología VPN IPSec y SSL, es la solución ideal para aplicaciones VPN a través de redes distribuidas. Mayor conectividad de red con enlaces multi-ISP, tarjetas inalámbricas y 3G

► VPN híbrida (IPSec/SSL/L2TP)

## ZyWALL OTP

### Generador de PINs

Un generador de PINs de 6 dígitos numéricos para ser utilizado junto con una contraseña en un proceso de autenticación robusto.



# Implementación de VPNs por Hardware

Modelo/licencia de la serie Cisco ASA 5500	Cisco ASA 5505 Base/Security Plus	Cisco ASA 5510 Base/Security Plus	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550
Mercado	Oficina pequeña, hogar/oficina remota, sucursal / Plataforma de switching de servicios múltiples / Trabajadores móviles empresariales	Empresas en crecimiento y empresas pequeñas	Empresas pequeñas	Empresas medianas	Grandes empresas
<b>Resumen de rendimiento</b>					
Capacidad máxima de procesamiento (Mbps) del firewall	150	300	450	650	1200
Capacidad máxima de procesamiento (Mbps) de VPN 3DES/AES	100	170	225	325	425
Cantidad máxima de sesiones de usuario de VPN de sitio a sitio y de acceso remoto	10 / 25	250	750	5000	5000
Cantidad máxima de sesiones de usuario de VPN SSL	25	250	750	2500	5000
Cantidad máxima de conexiones	10.000 / 25.000	50.000 / 130.000	280.000	400.000	650.000
Cantidad máxima de conexiones/segundo	3000	6000	9000	20.000	28.000
Paquetes por segundo (64 bytes)	85.000	190.000	320.000	500.000	600.000
<b>Resumen técnico</b>					
Memoria (MB)	256	256	512	1024	4096
Memoria flash del sistema (MB)	64	64	64	64	64
Puertos integrados	Switch de 8 puertos 10/100 con 2 puertos Power over Ethernet	5-10/100	4-10/100/1000, 1-10/100	4-10/100/1000, 1-10/100	8-10/100/1000, 1-10/100
Cantidad máxima de interfaces virtuales (VLAN)	3 (interfaces troncales desactivadas) / 20 (interfaces troncales activadas)	50/100	150	200	250
Ranura de expansión SSC/SSM	Si (SSC)	Si (SSM)	Si (SSM)	Si (SSM)	No
<b>Capacidades SSC/SSM</b>					
Compatibilidad SSC/SSM	Futura, SSC	CSC-SSM, AIP-SSM, 4GE-SSM	CSC-SSM, AIP-SSM, 4GE-SSM	CSC-SSM, AIP-SSM, 4GE-SSM	No
Prevención de intrusiones	No disponible	Si (con AIP-SSM)	Si (con AIP-SSM)	Si (con AIP-SSM)	No
Capacidad de procesamiento (Mbps) de mitigación concurrente contra amenazas (firewall + servicios IPS)	No disponible	150 (con AIP-SSM-10) 300 (con AIP-SSM-20)	225 (con AIP-SSM-10) 375 (con AIP-SSM-20)	450 (con AIP-SSM-20)	No disponible
Anti-X (antivirus, antispam, bloqueo de archivos, antiphishing y filtrado de URL)	No disponible	Si (con CSC-SSM)	Si (con CSC-SSM)	Si (con CSC-SSM)	No disponible
Cantidad máxima de usuarios por antivirus, antispam, bloqueo de archivos (sólo CSC-SSM)	No disponible	500 (CSC-SSM-10) 1000 (CSC-SSM-20)	500 (CSC-SSM-10) 1000 (CSC-SSM-20)	500 (CSC-SSM-10) 1000 (CSC-SSM-20)	No disponible
Características de licencia CSC SSM Plus	No disponible	Antispam, antiphishing, filtrado de URL	Antispam, antiphishing, filtrado de URL	Antispam, antiphishing, filtrado de URL	No disponible

Especificaciones Técnicas de la familia de dispositivos CISCO 5500.

## ❖ CARACTERISTICAS IMPORTANTES DE UN DISPOSITIVO VPN

- Protocolos VPN que soporta.
- Cantidad máxima de sesiones de usuario.
- Soporte de Arquitecturas VPN.
- Protocolos de Encriptación.
- Métodos de Autenticación.
- Soporte para DDNS (Dynamic DNS).

## ❖ INCONVENIENTES DE LAS IMPLEMENTACIONES POR SOFTWARE

- Es necesario instalar el software en una máquina, pudiendo ser necesario, si la carga de información es muy grande, tener que dedicar una máquina para este propósito.
- El sistema de claves y certificados está en máquinas potencialmente inseguras, que pueden ser atacadas.
- Si el software es de libre distribución, éste puede estar modificado y contener puertas traseras.

## ❖ Inconvenientes de las implementaciones por software

- Es necesario instalar el software en una máquina, pudiendo ser necesario, si la carga de información es muy grande, tener que dedicar una máquina para este propósito.
- El sistema de claves y certificados está en máquinas potencialmente inseguras, que pueden ser atacadas.
- Si el software es de libre distribución, éste puede estar modificado y contener puertas traseras.

- Es quizá el protocolo más sencillo de entunelamiento de paquetes.
- En general, usado por pequeñas empresas.
- Debido a la integración que hizo *Microsoft* en sus sistemas operativos, PPTP tuvo gran acogida en el mercado mundial.
- PPTP se soporta sobre toda la funcionalidad que PPP le brinda a un acceso conmutado para construir sus túneles a través de Internet.
- Es capaz de encapsular paquetes IP, IPX y NETBEUI.
- PPTP encapsula paquetes PPP usando una versión modificada del Protocolo de Encapsulamiento Ruteado Genérico (GRE - Generic Routing Encapsulation).

# PPTP (Protocolo de Tunel Punto a Punto)

- Es quizá el protocolo más sencillo de entunelamiento de paquetes.
- En general, usado por pequeñas empresas.
- Debido a la integración que hizo *Microsoft* en sus sistemas operativos, PPTP tuvo gran acogida en el mercado mundial.
- PPTP se soporta sobre toda la funcionalidad que PPP le brinda a un acceso conmutado para construir sus túneles a través de Internet.
- Es capaz de encapsular paquetes IP, IPX y NETBEUI.
- PPTP encapsula paquetes PPP usando una versión modificada del Protocolo de Encapsulamiento Ruteado Genérico (GRE - Generic Routing Encapsulation)



Paquete del Protocolo PPTP.

# L2TP (Protocolo de Tunel de Capa 2)

- L2TP fue creado como el sucesor de PPTP y L2F (CISCO).
- Las dos compañías abanderadas de cada uno de estos protocolos, *Microsoft* por PPTP y *Cisco* por L2F, acordaron trabajar en conjunto para la creación de un único protocolo de capa 2 y lograr su estandarización por parte de la IETF.
- Soporta multiprotocolo.
- Permite que un único túnel soporte más de una conexión.

# L2TP (Protocolo de Tunel de Capa 2)

<b>VPN</b>	<b>L2TP</b>	<b>L2TP</b>	<b>L2TP</b>
<b>Red Insegura</b>	Frame Relay	ATM	<b>IP</b>

# L2TP (Protocolo de Tunel de Capa 2)

- L2TP no cifra en principio el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los datos.



*Conexión , Control , Autenticación*



*Encriptación*

# SSL (Secure Layer Socket)

- **SSL (Secure Socket Layers)** es un protocolo que administra la *seguridad* de las transacciones que se realizan a través de Internet.
- El estándar SSL fue desarrollado por *Netscape*, junto con *Mastercard*, *Bank of America* y *Silicon Graphics*.
- Se basa en un proceso de *cifrado de clave pública* que garantiza la seguridad de los datos que se envían a través de Internet.
- Su principio consiste en el establecimiento de un *canal de comunicación seguro* (cifrado) entre dos equipos (el cliente y el servidor) después de una fase de autenticación.
- A mediados de 2001, la patente SSL fue adquirida por *IETF (Internet Engineering Task Force)* y adoptó el nombre de **TLS** (*Transport Layer Security*).
-

# SSL (Secure Layer Socket)

- El sistema SSL es independiente del protocolo utilizado; esto significa que puede asegurar transacciones realizadas en la Web a través del protocolo HTTP y también conexiones a través de los protocolos FTP, POP e IMAP.
- SSL es transparente para el usuario. Por ejemplo, un usuario que utiliza un navegador de Internet para conectarse a una página Web de comercio electrónico protegido por SSL enviará datos cifrados sin tener que realizar ninguna operación especial.

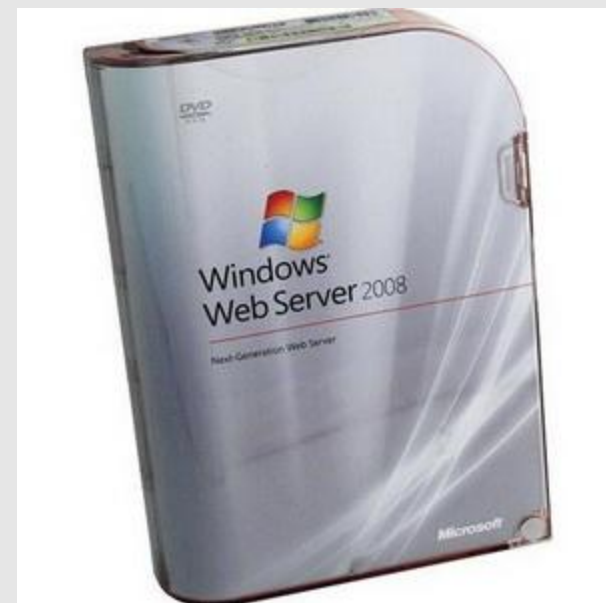


- Los objetivos iniciales de la primera generación de VPN-SSL fueron:
  - 1- Facilitar el acceso a través de cortafuegos.
  - 2- Ser una solución de *acceso remoto* que trabaje desde cualquier lugar independientemente de los dispositivos NAT.
- *SSL-VPN cliente* no necesita instalación y ofrece la funcionalidad de un VPN clientes o Web VPN.
- Software mas utilizado en VPN-SSL :
  - SSTP de Microsoft.
  - OpenVPN.
  - SSL-Explorer.

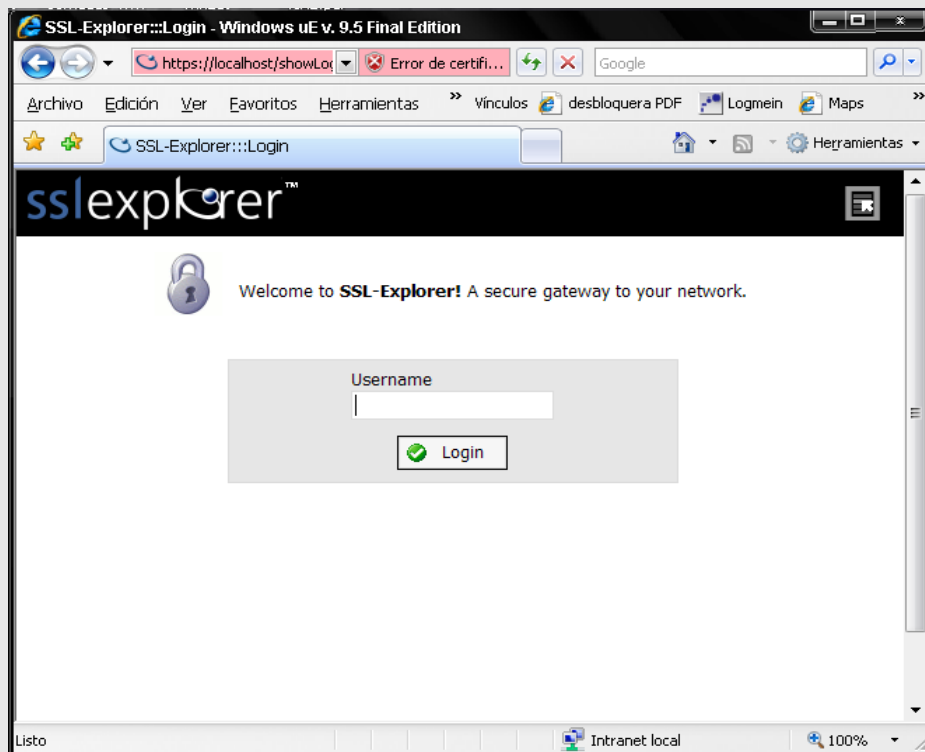
# SSTP (Secure Socket Tunneling Protocol)

El protocolo *Secure Socket Tunneling Protocol (SSTP)* de Microsoft es, por definición, un protocolo de *capa de aplicación* que encapsular tráfico PPP por el *canal SSL* del protocolo HTTPS.

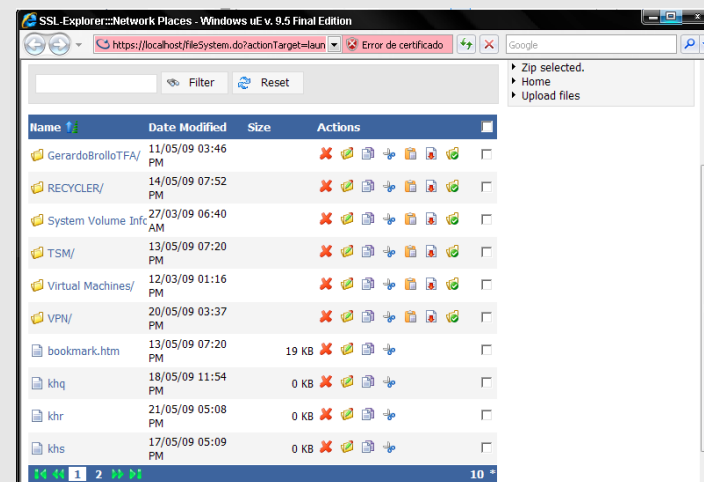
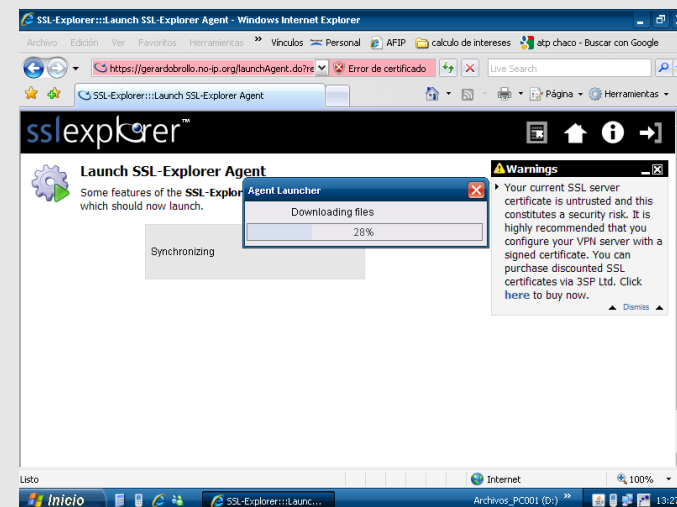
- El uso de PPP habilita la compatibilidad con todos los métodos de autenticación seguros, como EAP-TLS.
- El empleo de HTTPS significa que el tráfico pasa a través del puerto TCP 443, un puerto que se suele usar para el acceso web y eliminando así los problemas asociados con las conexiones VPN basadas en PPTP o L2TP.



# SSL - Explorer



*Autenticación en SSL-Explorer*



## ❖ Una variante al Acceso Remoto VPN



- El software IAG (Intelligent Application Gateway) de Microsoft brinda un acceso completamente granular, permite facilitar a los usuarios el acceso a las aplicaciones y servicios sin tener que abrir una VPN a la antigua.
- Al no tener una VPN abierta se evita riesgos de routing, virus, segmentos, cuarentenas o asignaciones de IP, lo cual ayuda a simplificar la red y disminuir los costes de administración a la vez que aumenta la seguridad.
- IAG es una solución de acceso seguro a aplicaciones a través de SSL que permite el control de acceso, autorización e inspección de contenidos para una amplia variedad de aplicaciones, gestionando además la seguridad del punto desde el que se accede.

# VPN con IP Dinámicas mediante DDNS

VPN  
Network Virtual Private

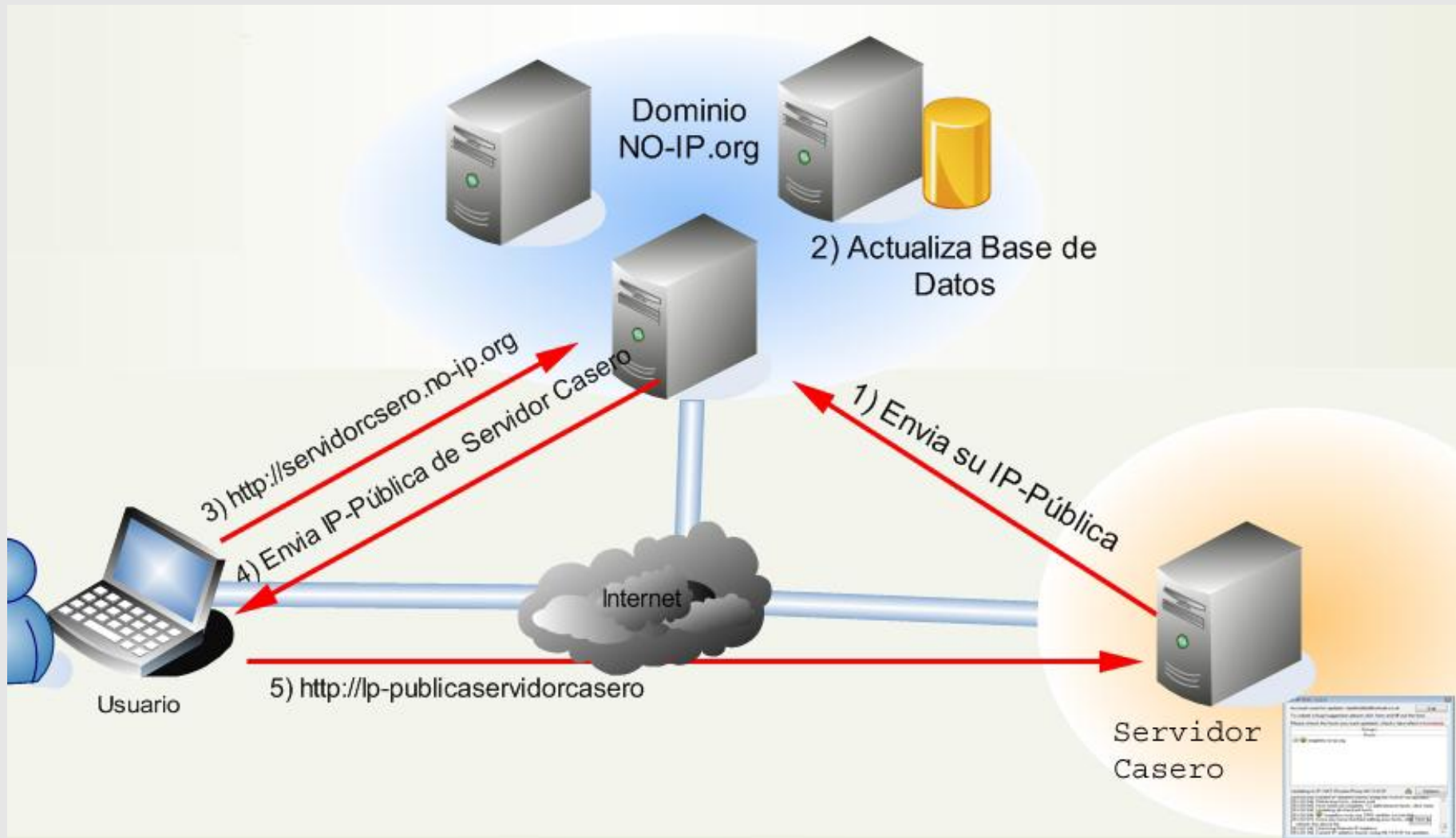


<http://minombre.no-ip.org>



<http://minombre.dyn.com>

# VPN con IP Dinámicas mediante DDNS



# VPN con IP Dinámicas mediante DDNS



Cliente DDNS de no-ip para Windows.



Soporte para servicio DDNS de dyndns.org del router Linksys RVL200.

**Gracias por su Atención**