# UTN-FRBA-Dto.Sistemas
# Redes de Información

Unidad 5-Clase 4
Redes Privadas Virtuales

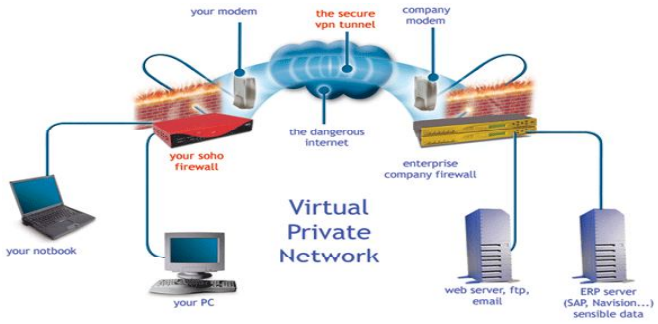
Fuente: Varias
Versión: 1

## Concepto

- Permiten conectar varias LAN o estaciones remotas entre sí
- en forma segura y confidencial a través de un medio inseguro como INTERNET
- mediante el uso de la autenticación, encriptación y túneles para las conexiones.

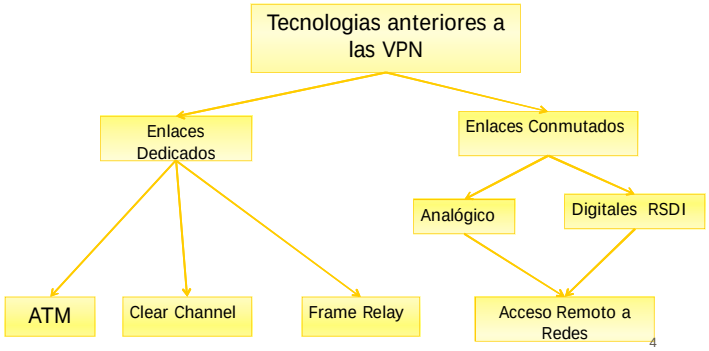


## Esquema





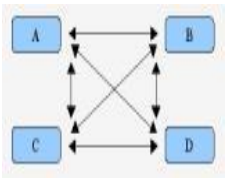

## Tecnologías anteriores






## Enlaces Dedicados

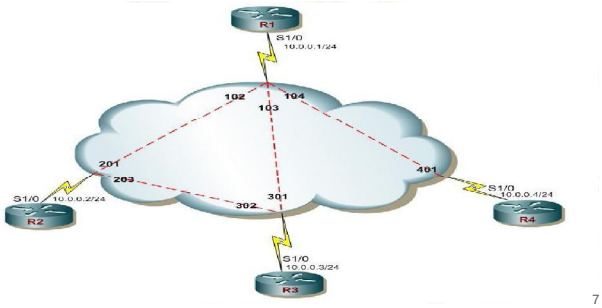
- Primera tecnología WAN
- Usaba la infraestructura de voz de los operadores de telefonía.
- Necesita conexiones físicas reales con un proveedor en cada sitio.
- Es una sola línea de comunicación entre dos partes.






## 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 el ancho de banda disponible.
- Ofrece un alto desempeño y una gran eficiencia de transmisión.
- Ofrece anchos de banda en el rango de 64 kbps hasta 4 Mbps.



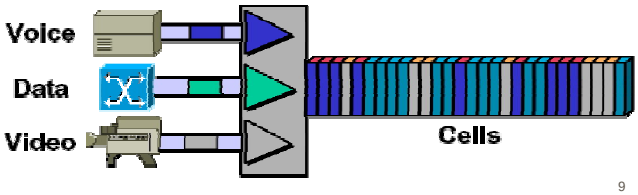



## ATM

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



ATM ha sido definido para soportar de forma flexible, la conmutación y transmisión de tráfico multimedia, comprendiendo datos, voz, imágenes y video.



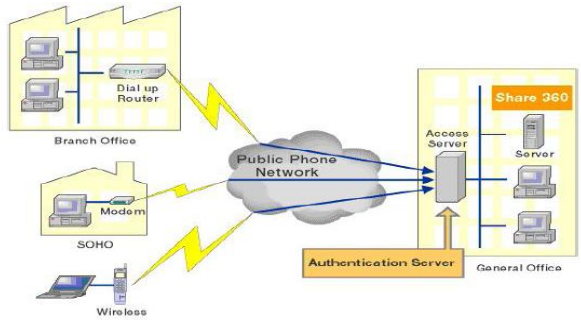



## Acceso Remoto

- Existe un RAS (*Remote Access Server)* que actúa como una puerta de enlace entre el *cliente remoto* y la red.
- El usuario establece la conexión por medio de una llamada.
- La línea es transparente para el usuario (puede tener acceso a todos los recursos de la red como si estuviera ante un equipo directamente conectado a ella).
- Altos costos de las llamadas.
- Falta de confidencialidad (no soportan encriptación de datos).



## Enlaces Conmutados



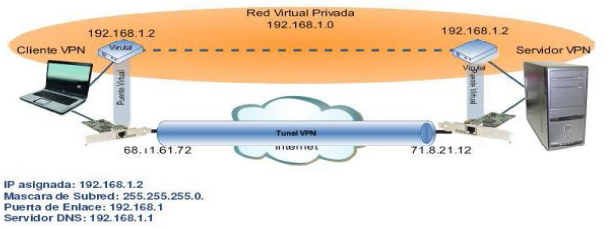

Escenario Típico de un Acceso Remoto a Redes



## PPP (Protocolo Punto a Punto)

- 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 que se ha venido dando es utilizarlo para conectar a *usuarios remotos con sus oficinas a través del RAS de su empresa.*

El servidor al verificar que se encuentra con un usuario legitimo envía los parámetros de configuración del *Protocolo de Capa 3* asignados por medio de un servidor DHCP, en este caso:




IP asignada: 192.168.1.2
Mascara de Subred: 255.255.255.0.
Puerta de Enlace: 192.168.1.1
Servidor DNS: 192.168.1.1



## Implementación por Hardware

- El proceso de encriptación y desencriptación se realiza a nivel físico.
- Se necesitan 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

- La instalación y configuración sencillas con mantenimiento mínimo.
- Un único elemento puede habilitar varias VPN en distintos sitios.
- Independiente de las máquinas conectadas a la red.
- No necesita máquinas dedicadas para realizar la VPN.



## Inconvenientes

- Firmware cerrado, se depende del fabricante para cambiarlo.
- Los sistemas de encriptación son cerrados y de un único tipo.
- El hardware de los extremos debe ser 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.



## Implementación por Software

- Existe una gran variedad de Redes Privadas Virtuales desarrolladas por software, donde elegir y que están continuamente mejorando sus prestaciones.
- El número de usuarios de este tipo de red es mucho mayor que el número de usuarios de VPNs realizadas por hardware, con lo que la posibilidad de encontrar documentación y ayuda para estos elementos es mayor.
- Pueden dar cobertura tanto a redes internas (intranet) como redes externas.
- La seguridad puede cubrir de *máquina a máquina, donde se* encuentren colocados los extremos de la VPN.



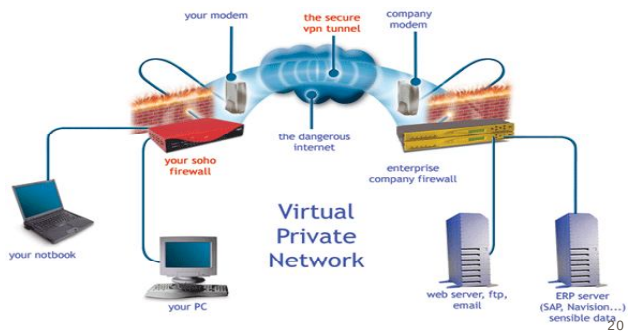
# Tecnologías VPN-IP

- PPTP (*Point to Point Protocol Tunneling).*
- L2TP (*Layer 2 Protocol Tunneling).*
- IPSec (*Internet ProtocolSecurity).*
- MPLS (*Multiprotocol Label Switching).*
- VPNs SSL/TLS (*Secure Socket Layer - Transport Layer Security).*

## Acceso Remoto

• Fue la primera aplicación que se le dio a la emergente tecnología de las VPN.
• Esta solución nació de la necesidad de poder acceder a la red corporativa desde cualquier ubicación, incluso a nivel mundial.
• Con el Acceso Remoto VPN, los RAS corporativos quedaron olvidados (mantenimiento costoso).



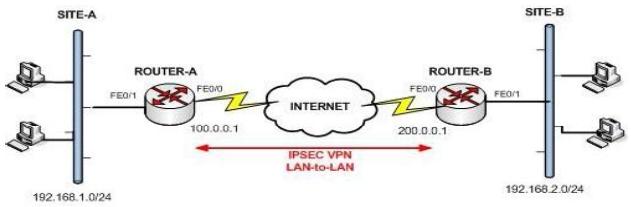





## Intranet LAN to LAN

• Para concentrar tráfico en un nodo se usa Frame Relay
• En el último kilómetro viajan todos los PVCs contratados
• Es costosa porque se cobra por PVC activado
• Para cambiar a una solución usando VPN se debe considerar:
  - costo
  - seguridad
  - la eficiencia en el manejo del ancho de banda
  - la cobertura de Internet.



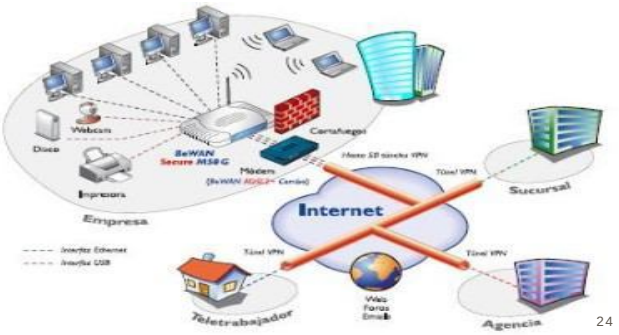





## Extranet

• Las empresas necesitan intercambiar información entre sitios de su misma organización y con otras compañías.
• Hoy en día todas las empresas tienen presencia en Internet.
• La comunicación con las otras empresas debe usar este medio.





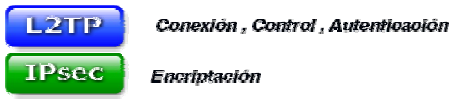
## PPTP: Protocolo de Tunel Punto a Punto

• Usado por pequeñas empresas en sistemas Microsoft en sus sistemas operativos.
• PPTP se soporta sobre PPP para construir sus túneles a través de Internet.
• Es capaz de encapsular paquetes IP, IPX y NETBEUI.
• Se encapsulan paquetes PPP usando el Protocolo de Encapsulamiento Ruteado Genérico (GRE - *Generic Routing Encapsulation*).



## L2TP: Protocolo de Tunel Capa 2

• L2TP fue creado como el sucesor de PPTP y L2F.
• Microsoft (PPTP) y Cisco por (L2F), acordaron trabajar en conjunto para la creación de un único protocolo de capa 2 y estandarizarlo por la IETF.
• Soporta multiprotocolo.
• Permite que un único túnel soporte más de una conexión.
• El Entunelamiento no depende de IP y GRE.
• No cifra el tráfico de datos de usuario (no hay confidencialidad de datos).

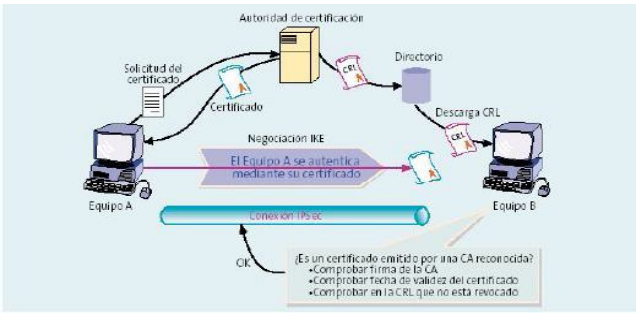





## IPSec: Protocolo de Seguridad Internet

• IPSec es un conjunto de protocolos diseñados para proveer una seguridad basada en criptografía robusta para IPv4 e IPv6 (IPSec está incluido en IPv6).
• Servicios de seguridad: control de acceso, integridad de datos, autenticación del origen de los datos, protección antirepetición y confidencialidad en los datos.
• Es un protocolo modular que no depende de un algoritmo criptográfico específico.
• Trabaja en la Capa 3 del Modelo OSI
• Independiente del nivel de transporte y de la infraestructura.
• Solo aplicable a IP (*Protocolo de Internet).*








## SSL: Secure Socket Layer

• Son Redes Virtuales Privadas sobre SSL
• Los objetivos iniciales son:
  - Facilitar el acceso a través de firewall.
  - Permitir acceso remoto independientemente de los NAT.
• SSL-VPN cliente no necesita instalación (Web VPN).
• Los productos de software más utilizados son:
  - SSTP.
  - OpenVPN.
  - SSL-explorer.



## SSTP: Secure Socket Tunneling Protocol

•El protocolo *Secure Socket Tunneling Protocol (SSTP)* de *Microsoft* , es un protocolo de *capa de aplicación* que encapsula 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, eliminando así los problemas asociados con las conexiones VPN basadas en PPTP o L2TP.