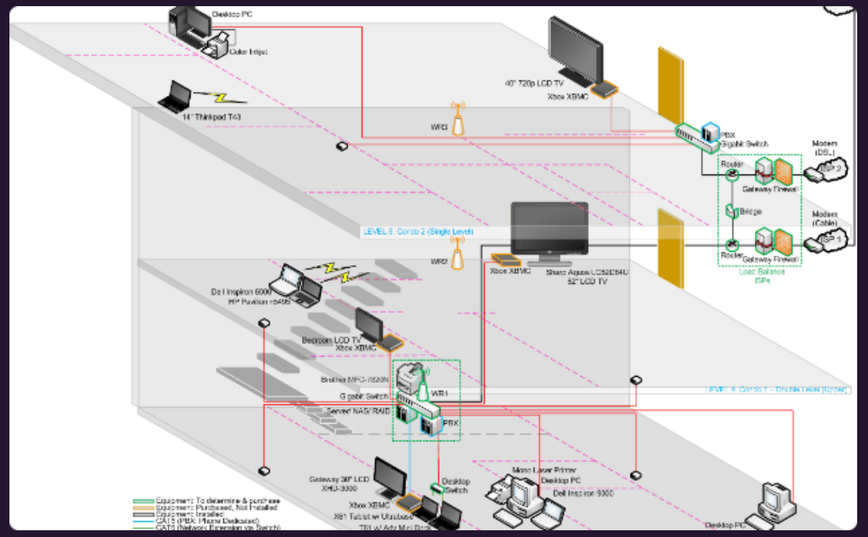
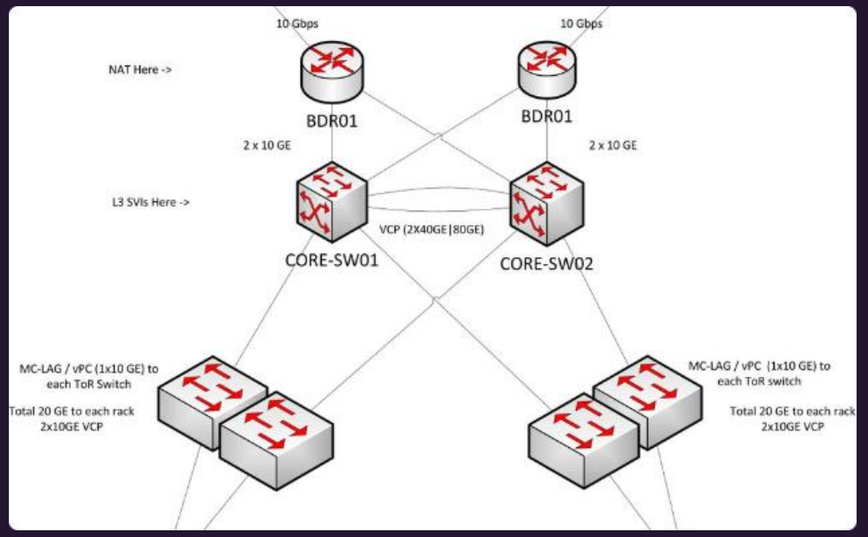
6.1 Características de una VPN

Una VPN ofrece varias características importantes para garantizar la seguridad y la privacidad en línea. Estas incluyen el cifrado de datos, el ocultamiento de la dirección IP, el acceso a redes restringidas y la protección contra ataques cibernéticos.

6.1.1 Niveles de seguridad en una conexión de red





Cifrado de Datos

Una VPN garantiza un alto nivel de seguridad mediante el cifrado de los datos transmitidos. Esto evita el acceso no autorizado a la información confidencial, protegiendo la privacidad de los usuarios.

Firewalls y Seguridad Perimetral

Las VPNs suelen incorporar firewalls y mecanismos de seguridad perimetral para proteger las redes locales y los dispositivos de los usuarios contra amenazas externas y ataques cibernéticos.

6.1.1 Niveles de seguridad en una conexión de red

Seguridad en el nivel de enlace

Puesto que la capa de enlace es el de más bajo nivel (solo por encima del físico) su seguridad está muy próxima al adaptador de red. Por tanto, si se consigue algún método para asegurar este nivel, su implementación será transparente a los protocolos de alto nivel y, en concreto, a las aplicaciones de los usuarios. Un ejemplo de protocolo de seguridad en este nivel es L2TP, al que nos referiremos más adelante.

6.1.1 Niveles de seguridad en una conexión de red

Seguridad en el nivel de red

Se trata de asegurar el protocolo IP que es el protocolo que produce el transporte de paquetes. Este es el tipo de seguridad que se consigue con IPsec. Para que una aplicación pueda asegurar sus conexiones deberá encapsular los datos a enviar en paquetes IP que serán asegurados mediante IPsec, haciendo también las aplicaciones transparentes al método de seguridad elegido.

6.1.1 Niveles de seguridad en una conexión de red

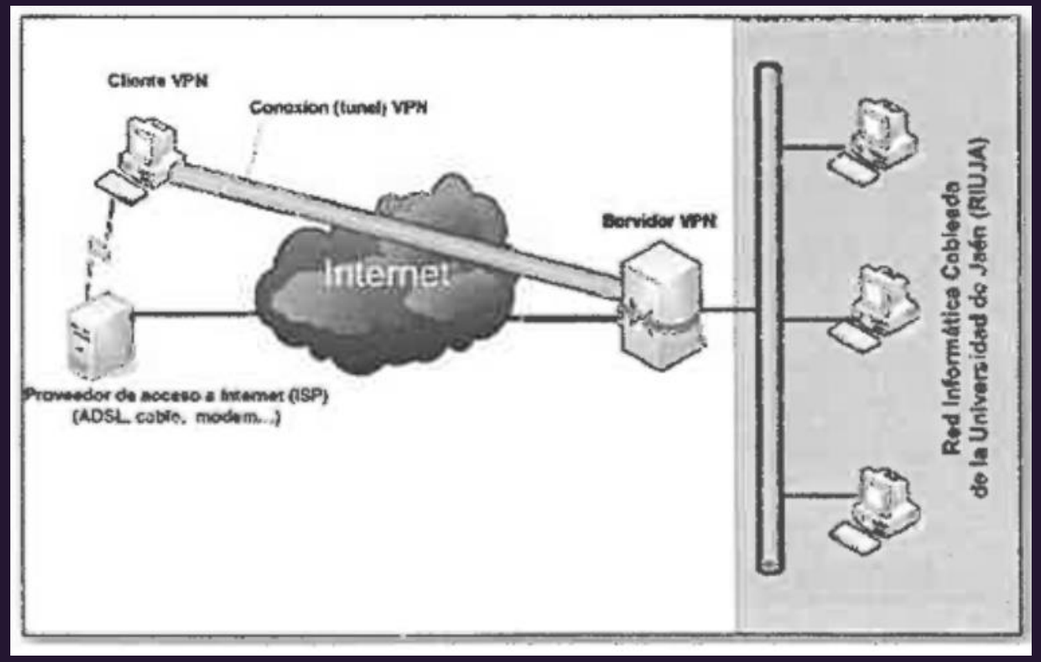
Seguridad en el nivel de aplicación

En este caso se trata de sustituir el protocolo inseguro por otro más seguro pero funcionalmente equivalente. Así, sustituiríamos las conexiones http por conexiones https, smtp por smtps, etc. En este caso la seguridad no es transparente a las aplicaciones puesto que estas deben ser reprogramadas para que puedan utilizar las versiones seguras de protocolos de comunicación.

6.1.2 Arquitecturas básicas de VPN

La técnica de tunelización

Consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de ordenadores, que se implementa incluyendo una PDU (Protocol Data Unit) determinada dentro de otra PDU de nivel inferior con el objetivo de transmitirla entre los extremos del túnel sin que sea necesaria una inspección intermedia de los valores de control del protocolo encapsulado, que pasará totalmente desapercibido al protocolo encapsulador. Obviamente, una tunelización evita ataques del tipo Man-In-The-Middle.



6.1.2 Arquitecturas básicas de VPN

La técnica de tunelización

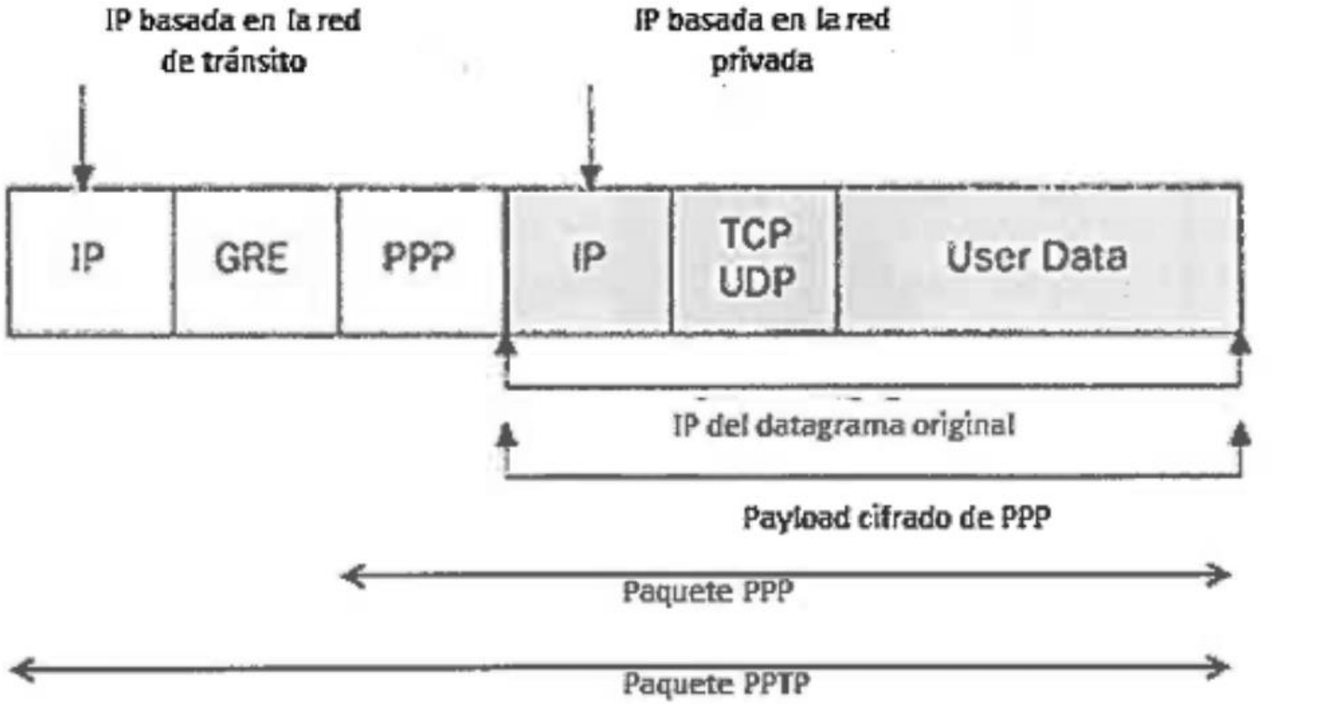


Figura 6.2. Encapsulamiento PPP y PPTP para la tunelización de datagramas IP.

6.1.2 Arquitecturas básicas de VPN

La técnica de tunelización

• Campo PPP, que lleva el control de autenticación y cifrado propio del protocolo PPP (Point to Point Protocol).

• Campo GRE, que lleva información sobre el túnel que establece PPTP.

• Campo IP, que especifica las direcciones IP de todo el paquete completo en la red de tránsito según las especificaciones de PPTP.

6.1.2 Arquitecturas básicas de VPN

La técnica de tunelización

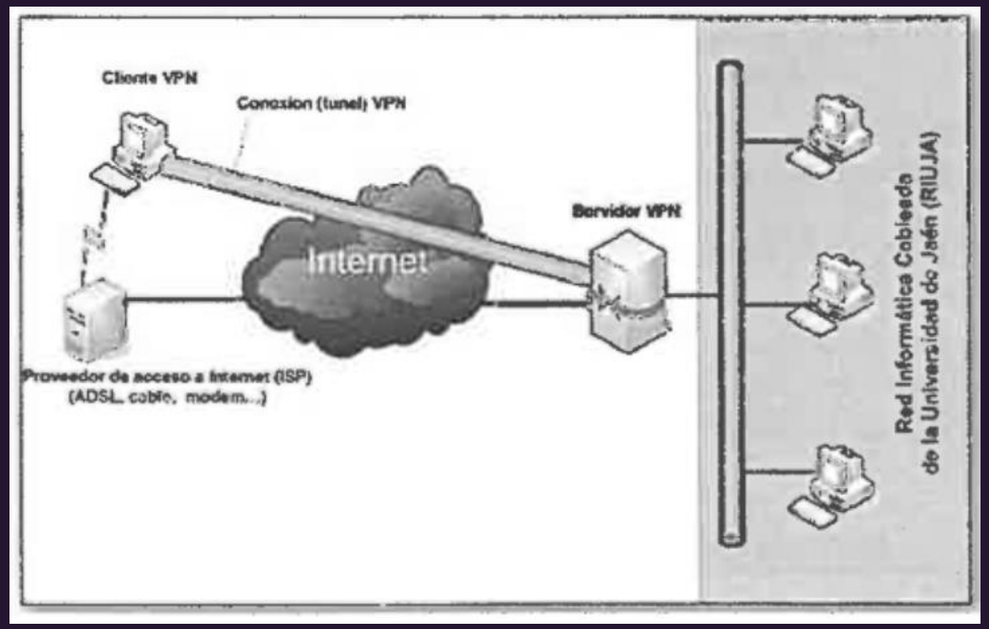
La información de enrutado en la red de tránsito se hace de acuerdo con la IP del paquete encapsulador (nunca el del encapsulado). Una vez que el paquete completo ha llegado al destino, el otro extremo del túnel extrae el paquete encapsulado, descifrándolo y poniéndolo en la red local de destino cuyas direcciones IP serán compatibles con las que tiene el paquete encapsulado.

6.1.2 Arquitecturas básicas de VPN

Acceso Remoto

Este tipo de VPN permite a los usuarios conectarse de forma segura a una red privada desde ubicaciones remotas a través de Internet, como desde sus hogares o sitios de teletrabajo. Se conectan al servidor VPN remoto que le proporciona el acceso a una red local.

Para la creación del túnel el usuario debe autenticarse en el servidor remoto. Solo aquellos usuarios con permiso podrán establecer el túnel.



6.1.2 Arquitecturas básicas de VPN

Acceso Punto a Punto

Este tipo de VPN el tunel se establece entre dos redes locales, por lo que cada red local debe tener su propio servidor VPN.

Los clientes de cada red podrán conectarse con el resto de clientes de la otra red como si estuvieran en la misma red local.

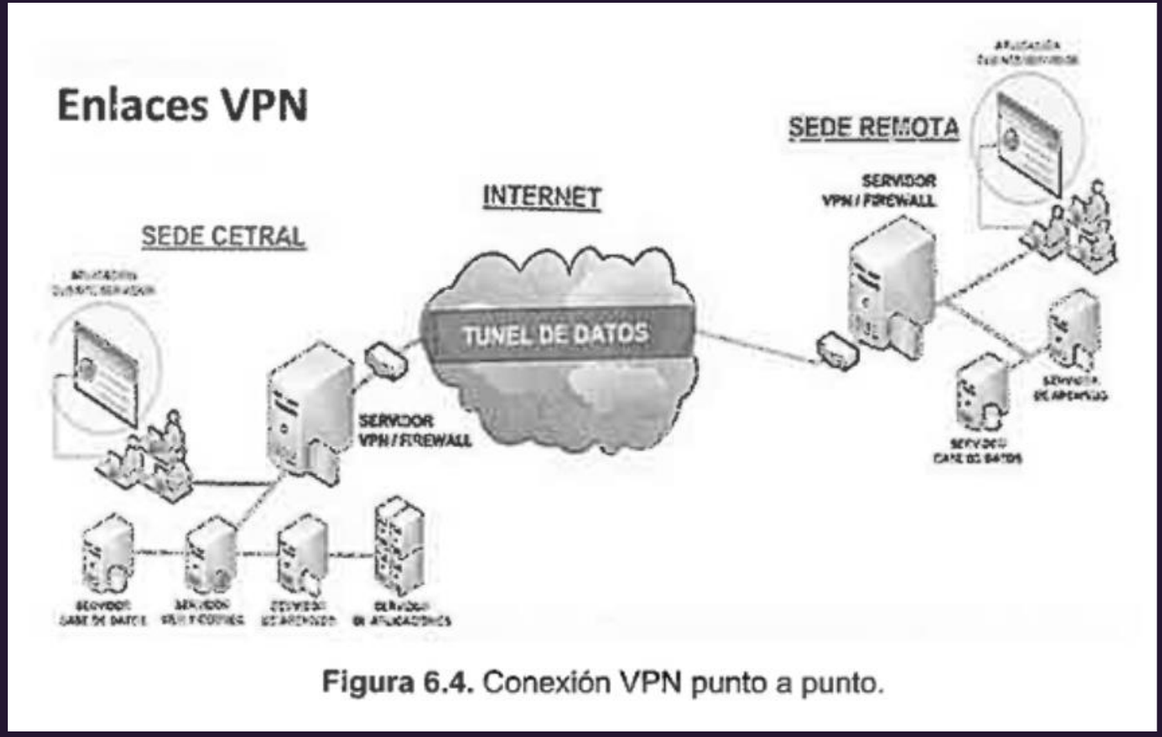


Figura 6.4. Conexión VPN punto a punto.

6.1.2 Arquitecturas básicas de VPN

VPN sobre LAN

Este tipo de VPN es muy eficaz para asegurar conexines dentro de las redes locales. El esquema es semejante al del acceso remoto, pero sustituyendo Internet por la red local, impidiendo escuchas o suplantaciones dentro de la propia LAN.

Se suele utilizar para aislar servidores o conjunto de ellos dentro de la LAN.

6.1.3 Implementación de una VPN

El protocolo más utilizado es IPsec, pero también se pueden utilizar PPTP, LF2, L2TP, SSL/TLS, SSH, etc.

Las soluciones VPN se pueden implementar pos hardware o por software. Las soluciones hardware tienen mayor rendimiento y son más fáciles de configurar, sin embargo, tienen menos flexibilidad que las de software.

6.2.1 Dial-up networking

El Dial-Up Networking (conexión mediante marcado) es una antigua tecnología que permitía a los usuarios conectarse a Internet o a una red utilizando una línea telefónica estándar.

RAS (Remote Access Server) es el software servidor de dial-up que Microsoft proveía en sus sistemas operativoshasta su versión Windows 2000. Posteriormente, RAS pasó a ser parte de un paquete software más amplio denominado RRAS (Routing and Remote Access Service).

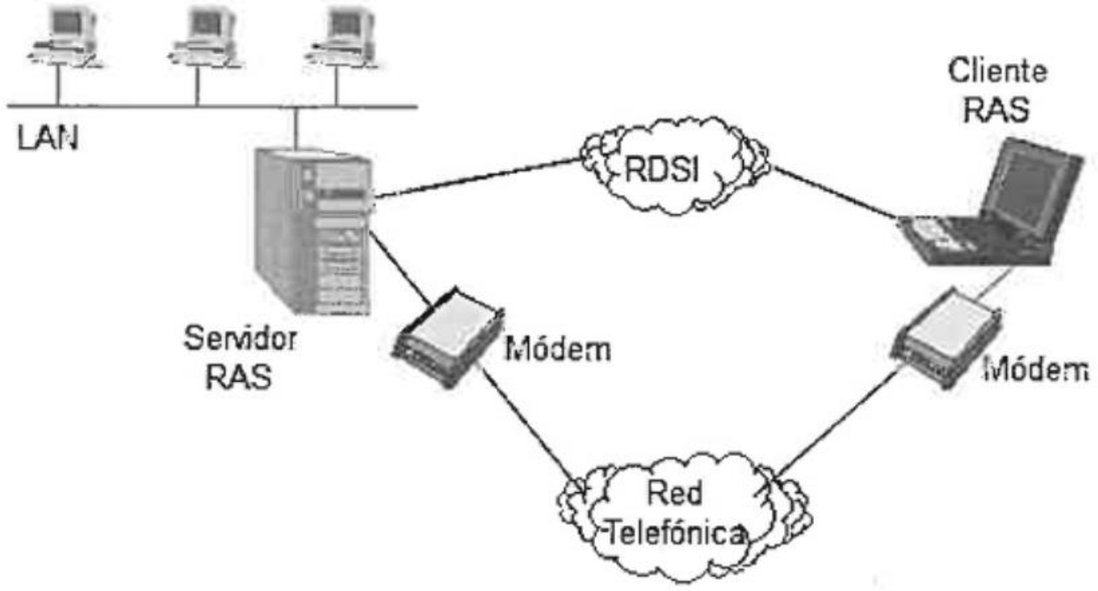


Figura 6.5. Conexiones posibles entre un cliente RAS y un servidor RAS.

6.2.3 Protocolos de acceso remoto

SLIP y PPP

SLIP (Serial Line Internet Protocol) y PPP (Point-to-Point Protocol) son dos protocolos que permiten a un cliente conectarse a un servidor utilizando una conexión serie (módem o clable serie, normalmente).
Encapsulan los protocolos de alto nivel TCP e IP en tramas de datos de bajo nivel para ser transmitido por las líneas serie.

6.2.3 Protocolos de acceso remoto

SLIP

-Anterior y más simple

-Sólo puede transportar paquetes IP

- La IP del cliente y servidor hay que configurarla de manera estática

- No hace corrección de errores ni compresión

- No soporta cifrado

- Sólo soporta transmisiones asíncronas

PPP

-Posterior

- Puede transportar paquetes de otras capas de red.

- La IP del cliente y servidor se puede asignarautomáticamente con técnicas de DHCP

- Sí hace corrección de errores y compresión

- Soporta cifrado

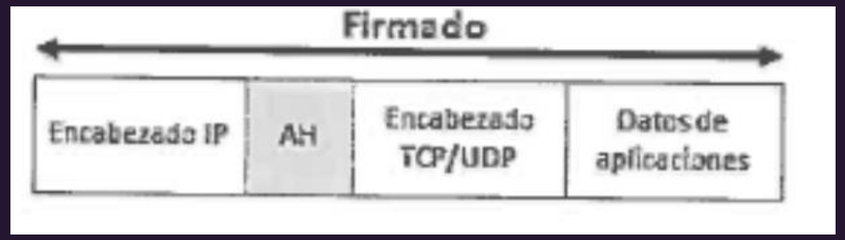
- Soporta tato transmisiones síncronas como asíncronas

6.2.5 Protocolo IPsec

IPsec

IPsec puede funcionar en dos modos distintos, modo transporte y modo túnel.

• En modo transporte, IPsec solo encapsula los datos del datagrama IP, conservando la cabecera IP original del datagrama. En este caso, el cifrado se realiza de extremo a extremo, es decir, desde el host de origen al host de destino. Para implantar esta solución es necesario que todos los nodos de las redes origen y destino implementen la tecnología IPsec.



6.2.5 Protocolo IPsec

IPsec

• En nodo túnel, el datagrama IP es encapsulado completamente dentro de IPsec, por lo que se requiere una nueva cabecera IP para poder enviar el datagrama por la red. En este caso el cifrado se implementa exclusivamente entre los routers de fontera en cada una de las redes origen y destino, implementando una VPN de tipo punto a punto.

6.3.1 Protocolos de autenticación en la red

PAP (Password Authentication Protocol)

Protocolo de autenticación de contraseña. En PAP las credenciales del usuario, representadas por el nombre de usuario y su contraseña, se envían por la red sin cifrar, por lo que es un método de autenticación inseguro. Una captura de la trama PPP permitiría un examen libre de la contraseña

6.3.1 Protocolos de autenticación en la red

CHAP (Challenge Handshake Authentication Protocol)

Protocolo de autenticación por desafio mutuo. En CHAP el cliente envía una petición de acceso con un hash de la contraseña (no la contraseña, que nunca viaja por la red). Entonces el servidor manda al cliente un desafío. El cliente utiliza un algoritmo hash (MDS) para calcular un resultado con su contraseña y el desafío, y lo envía al servidor. El servidor hace el mismo cálculo con la contraseña que él posee y compara el resultado con el recibido por el cliente. Solo si son iguales se permite el acceso.

6.3.1 Protocolos de autenticación en la red

EAP (Extensible Authentication Protocol)

Protocolo de autenticación extensible. EAP admite diversos modos de autenticación. Es más una arquitectura que un único protocolo. Puede utilizar tanto certificados digitales como tokens e incluso parejas usuario/contraseña. Es muy utilizado en la autenticación sobre redes inalámbricas y en conexiones punto a punto.

6.3.1 Protocolos de autenticación en la red

Kerberos

Creado por el MIT (Instituto Tecnológico de Massachusetts) y estandarizado en la RFC 4120. Cliente y servidor se autentican recíprocamente. Utiliza cifrado AES (RFC 3962). Cada servidor, usuario o servicio dispone de una clave que se registra en una base de datos unificada en el servidor Kerberos. Cliente y servidor confían en el servidor Kerberos, quien les proporciona tickets de sesión que posteriormente serán utilizados para autenticarse frente a los servicios de red. Tanto los sistemas Windows como los GNU/Linux pueden usar Kerberos.