# Unidad V: PROTOCOLOS DE REDES DE COMUNICACIÓN:PROTOCOLOS DE INTERNET

## Introducción. Un poco de Historia

La **familia de protocolos de Internet** es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se le denomina *conjunto de protocolos* ***TCP/IP***, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia. Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra el popular HTTP (HyperText Transfer Protocol), que es el que se utiliza para acceder a las páginas web, además de otros como el ARP (Address Resolution Protocol) para la resolución de direcciones, el FTP (File Transfer Protocol) para transferencia de archivos, y el SMTP (Simple Mail Transfer Protocol) y el POP (Post Office Protocol) para correo electrónico, TELNET para acceder a equipos remotos, entre otros.

El TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el Departamento de Defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa de dicho departamento.

La familia de protocolos de Internet puede describirse por analogía con el modelo OSI (Op*en System Interconnection)*, que describe los niveles o capas de la pila de protocolos, aunque en la práctica no corresponde exactamente con el modelo en Internet. En una pila de protocolos, cada nivel soluciona una serie de problemas relacionados con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos. Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables.

El modelo de Internet fue diseñado como la solución a un problema práctico de ingeniería.

El modelo OSI, en cambio, fue propuesto como una aproximación teórica y también como una primera fase en la evolución de las redes de ordenadores. Por lo tanto, el modelo OSI es más fácil de entender, pero el modelo TCP/IP es el que realmente se usa. Sirve de ayuda entender el modelo OSI antes de conocer TCP/IP, ya que se aplican los mismos principios, pero son más fáciles de entender en el modelo OSI.

El 1 de enero de 2010 el Protocolo TCP/IP cumplió 27 años.

Un ordenador denominado *router* (un nombre que fue después cambiado a **gateway**, puerta de enlace, para evitar confusiones con otros tipos de Puerta de enlace) está dotado con una interfaz para cada red, y envía Datagramas de ida y vuelta entre ellos. Los requisitos para estos routers están definidos en el RFC 1812.

Esta idea fue llevada a la práctica de una forma más detallada por el grupo de investigación que Cerf tenía en Stanford durante el periodo de 1973 a 1974, dando como resultado la primera especificación TCP (Request for Comments 675,) Entonces DARPA fue contratada por BBN Technologies, la Universidad de Stanford, y la University College de Londres para desarrollar versiones operacionales del protocolo en diferentes plataformas de hardware. Se desarrollaron así cuatro versiones diferentes: TCP v1, TCP v2, una tercera dividida en dos TCP v3 y IP v3 en la primavera de 1978, y después se estabilizó la versión TCP/IP v4 — el protocolo estándar que todavía se emplea en Internet.

En 1975, se realizó la primera prueba de comunicación entre dos redes con protocolos TCP/IP entre la Universidad de Stanford y la University College de Londres (UCL). En 1977, se realizó otra prueba de comunicación con un protocolo TCP/IP entre tres redes distintas con ubicaciones en Estados Unidos, Reino Unido y Noruega. Varios prototipos diferentes de protocolos TCP/IP se desarrollaron en múltiples centros de investigación entre los años 1978 y 1983. La migración completa de la red ARPANET al protocolo TCP/IP concluyó oficialmente el día 1 de enero de 1983 cuando los protocolos fueron activados permanentemente.

En marzo de 1982, el Departamento de Defensa de los Estados Unidos declaró al protocolo TCP/IP el

estándar para las comunicaciones entre redes militares. En 1985, el Centro de Administración de Internet (Internet Architecture Board IAB por sus siglas en inglés) organizó un Taller de Trabajo de tres días de duración, al que asistieron 250 comerciales promocionando así el protocolo lo que contribuyó a un incremento de su uso comercial.

Kahn y Cerf fueron premiados con la Medalla Presidencial de la Libertad el 10 de noviembre de 2005 por su contribución a la cultura Americana.

**Ventajas e inconvenientes**

El conjunto TCP/IP está diseñado para enrutar y tiene un grado muy elevado de fiabilidad, es adecuado para redes grandes y medianas, así como en redes empresariales. Se utiliza a nivel mundial para conectarse a Internet y a los servidores web. Es compatible con las herramientas estándar para analizar el funcionamiento de la red.

Un inconveniente de TCP/IP es que es más difícil de configurar y de mantener que NetBEUI o IPX/SPX; además es algo más lento en redes con un volumen de tráfico medio bajo. Sin embargo, puede ser más rápido en redes con un volumen de tráfico grande donde haya que enrutar un gran número de tramas.

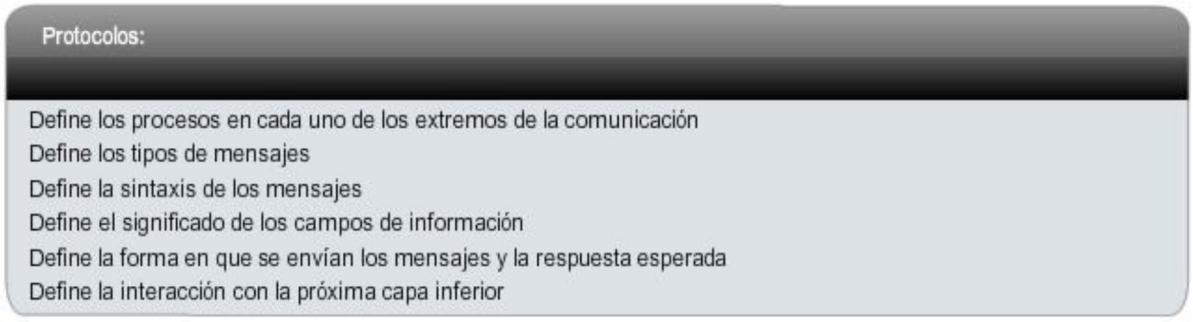
El conjunto TCP/IP se utiliza tanto en redes empresariales como por ejemplo en campus universitarios o en complejos empresariales, en donde utilizan muchos enrutadores y conexiones a mainframe o a ordenadores UNIX, así como también en redes pequeñas o domésticas, y hasta en teléfonos móviles.

**Funciones Básicas de los Protocolos**

Los protocolos establecen reglas consistentes para intercambiar datos entre las aplicaciones y los servicios cargados en los dispositivos participantes. Los protocolos especifican cómo se estructuran los datos dentro de los mensajes y los tipos de mensajes que se envían entre origen y destino. Estos mensajes pueden ser solicitudes de servicios, acuses de recibo, mensajes de datos, mensajes de estado o mensajes de error. Los protocolos también definen los diálogos de mensajes, asegurando que un mensaje enviado encuentre la respuesta esperada y se invoquen los servicios correspondientes cuando se realiza la transferencia de datos.

Cada protocolo tiene un fin específico y contiene las características requeridas para cumplir con dicho propósito. Deben seguirse los detalles del protocolo correspondiente a

cada capa, así las funciones en una capa se comunican correctamente con los servicios en la capa inferior.

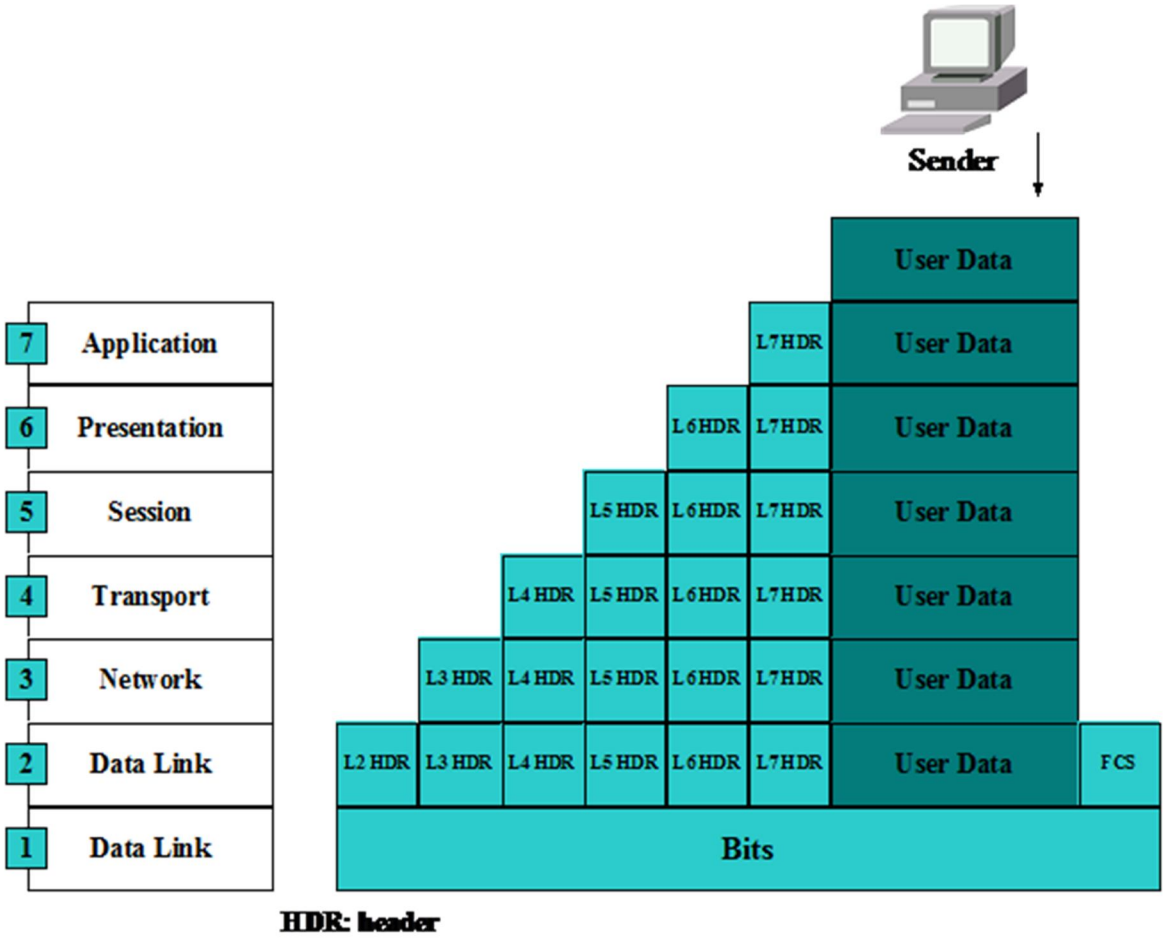



**Encapsulamiento**

Todas las comunicaciones de una red se originan en una fuente y son enviadas a un destino, aquí se explica cómo es el proceso de transmitir la información de un sitio a otro.

Si una *computadora A* quiere enviar datos a una *computadora B*, los datos deben ser empacados primero por un proceso llamado encapsulamiento. Este proceso puede pensarse como poner una carta dentro de un sobre, y poner las direcciones correctas del destinatario y el remitente para que sea entregada apropiadamente por el sistema postal.

El encapsulamiento envuelve los datos con la información de protocolo necesaria antes de transitar por la red. Así, mientras la información se mueve hacia abajo por las capas del modelo OSI, cada capa añade un encabezado, y un trailer si es necesario, antes de pasarla a una capa inferior. Los encabezados y trailers contienen información de control para los dispositivos de red y receptores para asegurar la apropiada entrega de los datos y que el receptor interprete correctamente lo que recibe.




**Paso 1**: los datos de usuario son enviados por una aplicación a la capa de aplicación.

**Paso 2**: La capa de aplicación añade el encabezado (layer 7 Header) a los datos, el encabezado y los datos originales pasan a la capa de presentación.

**Paso 3**: La capa de presentación recibe los datos provenientes de la capa superior, incluyendo el encabezado agregado, y los trata como sólo datos, añade su encabezado a los datos, y los pasa a la capa de sesión

**Paso 4**: la capa de sesión recibe los datos y añade su encabezado, lo pasa a la capa de transporte.

**Paso 5**: la capa de transporte recibe los datos y añade su encabezado, pasa los datos a la capa inferior.

**Paso 6**: la capa de red añade su encabezado y los pasa a la capa de enlace de datos.

**Paso 7**: la capa de enlace de datos añade el encabezado y un trailer (cola) a los datos, usualmente es un *Frame Check Sequence*, que usa el receptor para detectar si los datos enviados están o no en error. Esto envuelve los datos que son pasados a la capa física.

**Paso 8**: la capa física entonces transmite los bits hacia el medio de red.

**Des-encapsulamiento**

Es el proceso inverso, cuando un dispositivo recibe el stream de bits, la capa física del dispositivo remoto los pasa a la capa de enlace de datos para su manipulación.

**Paso 1**: checa el trailer de la capa de enlace de datos (*FCS*) para ver si los datos están en error.

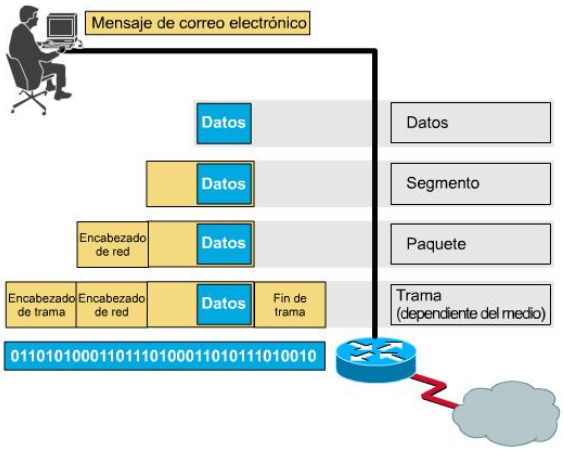
**Paso 2**: si los datos están en error, pueden ser descartados, y la capa de enlace de datos puede pedir la retransmisión.

**Paso 3**: si no hay ningún error, la capa de enlace de datos lee e interpreta la información de control en el encabezado (*L2 header*)

**Paso 4**: quita el header y trailer y pasa lo que queda hacia la capa superior basada en la información de control del header.

**Comunicación de Par a Par**

Cuando los paquetes van de origen a destino, cada capa en el nodo de origen se comunica con su capa par o igual en el nodo destino, esto es lo que se llama comunicación *Peer to Peer*, durante dicho proceso, los protocolos de cada capa intercambian información en unidades llamadas *protocol data unit (PDU)*, entre las capas pares.



Cada capa depende de la función de servicio de la capa inferior, para dar el servicio, la capa inferior encapsula la información para poner el PDU de la capa superior dentro de su campo de datos, entonces agrega el encabezado que sea necesario para ejecutar su función. Mientras se mueve la información de la capa 7 a la 5, se añaden encabezados adicionales, el agrupamiento en la capa 4 es llamado *segmento*.

La capa de red provee el servicio a la capa de transporte, y la capa de transporte presenta los datos al subsistema de internetwork. La capa de red mueve los datos encapsulando la información y agregando un header, lo cual crea un paquete (*Packet*), el header trae información necesaria, como las direcciones lógicas de origen y destino.

La capa de enlace de datos provee servicio a la capa de red encapsulando el paquete de la capa de red dentro de una trama (*Frame*), la trama contiene las direcciones físicas requeridas para completar la entrega, y además pone un trailer (frame check sequence)

La capa física da el servicio a la capa de enlace de datos codificando el frame en un patrón de 1 y 0 (bits) para transmitirlos en el medio de red, normalmente un alambre, dentro de la capa física.

Los Hubs operan en la capa 1, los switches en la capa 2, los routers en la capa 3.

**Segmentación y Reensamblaje**

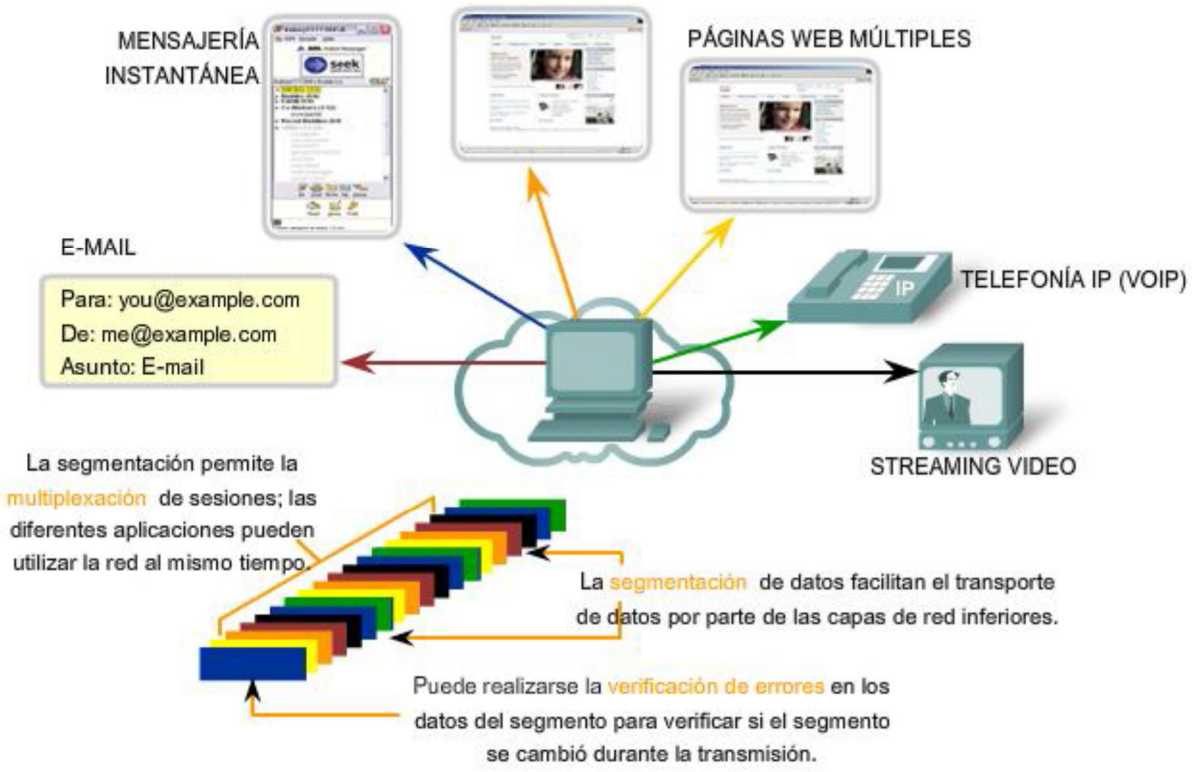
La mayoría de las redes poseen una limitación en cuanto a la cantidad de datos que pueden incluirse en una única PDU (Unidad de datos del protocolo). La capa de Transporte divide los datos de aplicación en bloques de datos de un tamaño adecuado. En el destino, la capa de Transporte reensambla los datos antes de enviarlos a la aplicación o servicio de destino.

**Multiplexación**

Pueden existir varias aplicaciones o servicios ejecutándose en cada host de la red. A cada una de estas aplicaciones o servicios se les asigna una dirección conocida como puerto para que la capa de Transporte pueda determinar con qué aplicación o servicio se identifican los datos.

Además de utilizar la información contenida en los encabezados para las funciones básicas de segmentación y reensamblaje de datos, algunos protocolos de la capa de Transporte proveen:

- conversaciones orientadas a la conexión,
- entrega confiable,
- reconstrucción ordenada de datos, y
- control del flujo




**Establecimiento de una sesión**

La capa de Transporte puede brindar esta orientación a la conexión creando una sesión entre las aplicaciones. Estas conexiones preparan las aplicaciones para que se comuniquen entre sí antes de que se transmitan los datos. Dentro de estas sesiones, se pueden gestionar de cerca los datos para la comunicación entre dos aplicaciones.

**Entrega confiable**

Por varias razones, es posible que una sección de datos se corrompa o se pierda por completo a medida que se transmite a través de la red. La capa de Transporte puede asegurar que todas las secciones lleguen a destino al contar con el dispositivo de origen para volver a transmitir los datos que se hayan perdido.

**Entrega en el mismo orden**

Ya que las redes proveen rutas múltiples que pueden poseer distintos tiempos de transmisión, los datos pueden llegar en el orden incorrecto. Al numerar y secuenciar los segmentos, la capa de Transporte puede asegurar que los mismos se reensamblen en el orden adecuado.

**Control del flujo**

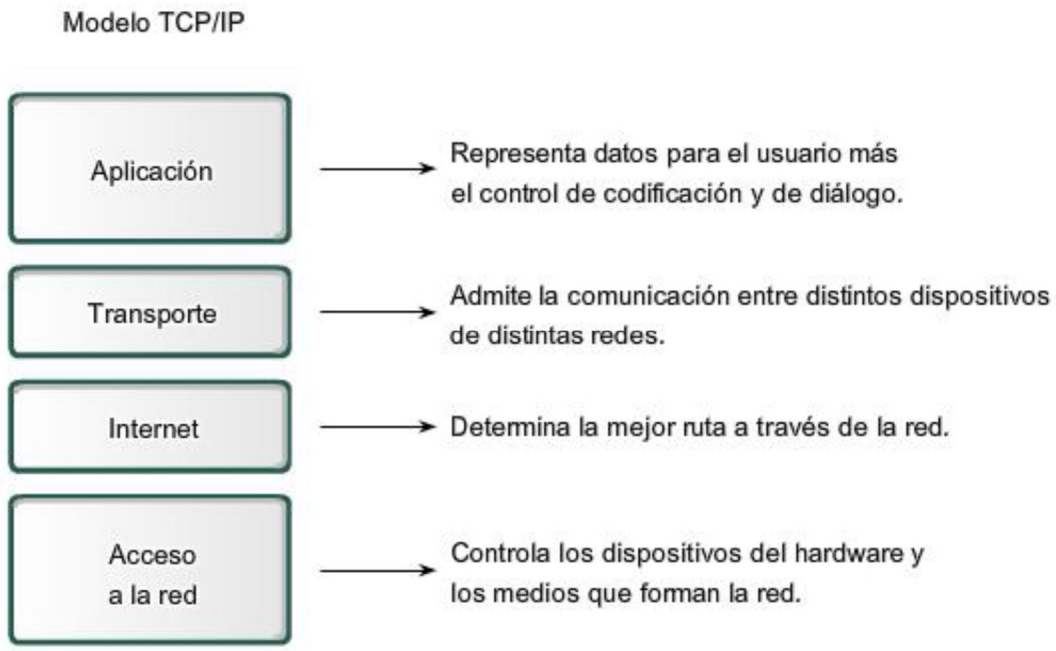
Los hosts de la red cuentan con recursos limitados, como memoria o ancho de banda. Cuando la capa de Transporte advierte que estos recursos están sobrecargados, algunos protocolos pueden solicitar que la aplicación que envía reduzca la velocidad del flujo de datos. Esto se lleva a cabo en la capa de Transporte regulando la cantidad de datos que el origen transmite como grupo. El control del flujo puede prevenir la pérdida de segmentos en la red y evitar la necesidad de retransmisión.

**MODELO TCP / IP**

El primer modelo de protocolo en capas para comunicaciones de internetwork se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. Define cuatro categorías de funciones que deben tener lugar para que las comunicaciones sean exitosas. La arquitectura de la suite de protocolos TCP/IP sigue la estructura de este modelo. Por esto, es común que al modelo de Internet se lo conozca como modelo TCP/IP.

La mayoría de los modelos de protocolos describen un stack de protocolos específicos del proveedor. Sin embargo, puesto que el modelo TCP/IP es un estándar abierto, una compañía no controla la definición del modelo. Las definiciones del estándar y los protocolos TCP/IP se explican en un foro público y se definen en un conjunto de documentos disponibles al público. Estos documentos se denominan Solicitudes de comentarios (RFCS). Contienen las especificaciones formales de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

Las RFC (Solicitudes de comentarios) también contienen documentos técnicos y organizacionales sobre Internet, incluyendo las especificaciones técnicas y los documentos de las políticas producidos por el Grupo de trabajo de ingeniería de Internet (IETF).




El modelo TCP/IP describe la funcionalidad de los protocolos que forman la suite de protocolos TCP/IP.

Esos protocolos, que se implementan tanto en el host emisor como en el receptor, interactúan para

proporcionar la entrega de aplicaciones de extremo a extremo a través de una red.

Un proceso completo de comunicación incluye estos pasos:

1. Creación de datos a nivel de la capa de aplicación del dispositivo final origen.

2. Segmentación y encapsulación de datos cuando pasan por la stack de protocolos en el dispositivo final de origen.

3. Generación de los datos sobre el medio en la capa de acceso a la red de la stack.

4. Transporte de los datos a través de la internetwork, que consiste de los medios y de cualquier dispositivo intermediario.

5. Recepción de los datos en la capa de acceso a la red del dispositivo final de destino.

6. Desencapsulación y rearmado de los datos cuando pasan por la stack en el dispositivo final.

7. Traspaso de estos datos a la aplicación de destino en la capa de aplicación del dispositivo final de destino.

**Direcciones IP**

El Protocolo Internet posibilita la transmisión de bloques de datos llamados datagramas desde el origen al destino. Origen y destino son host identificados por direcciones lógicas de una longitud fija de 4 bytes (direcciones IP).

También se encarga el protocolo IP de la fragmentación y del reensamblado de datagramas largos si es necesario, para su posterior transmisión a través de pequeños paquetes de red.

**Formato de las direcciones IP**

Tenemos diversas formas para identificar un host: nombres, direcciones y rutas.

Un nombre nos indica lo que buscamos, una dirección nos indica dónde está y una ruta nos indica cómo llegar hasta él.

Las direcciones IP serán direcciones binarias que posibilitan la computación y la selección de la ruta de forma eficiente, de todas formas se establecerá una relación entre direcciones binarias y nombres, ya que para nosotros será mucho más fácil su uso.

A cada host en Internet le es asignado una dirección de 32 bits, esta será su dirección IP. Esta dirección IP estará formada por dos partes una, la que nos identifica la máquina, el host con el que queremos trabajar y otra que hace referencia a la red dentro de la cual nos encontramos. Conceptualmente cada dirección IP será un par (Identificador de red, Identificador de host).

Podemos encontrar diferentes formas de direcciones IP:

**Clase A:**

Se trata de grandes redes que tienen más de 216 hosts.

Se utilizan 7 bits para identificar la red y 24 bits para la identificación del host

**Clase B:**

Se utilizara para redes de clase media que tienen entre 28 y 216 hosts.

Se utilizan 14 bits para identificar la red y 16 bits para la identificación del host.

**Clase C:**

Se utilizará para redes pequeñas que tienen menos de 28 hosts.

Se utilizan 21 bits para identificar la red y 8 bits para la identificación del host.

Debemos tener en cuenta que algunas de estas direcciones están reservadas para otros propósitos.

En realidad las direcciones nos especifican una conexión de red más que una computadora individual, así un router conectando n redes tiene n direcciones IP distintas, una para cada conexión de red.

También hemos de tener en cuenta que si un host se mueve de una red a otra, su dirección IP deberá cambiar (es una red lógica y no física).

Para encontrar la ruta (routing) de los datagramas se basará en las direcciones IP así como en sus máscaras, se usará la porción de la dirección IP que nos especifica la red para tomar las diferentes decisiones en cuanto a la ruta a seguir. Esto supondrá grandes ventajas.

**Direcciones especiales**

Poniendo todo a ceros en la dirección haremos referencia a 'Este host'. Hemos de tener en cuenta que esta forma especial de dirección sólo será consentida durante el proceso de arranque, de esta manera se le permite a la maquina establecer una comunicación temporal hasta adquirir la dirección real. Una vez que la máquina conoce la dirección correcta no deberá utilizar esta dirección de todo ceros.

Poniendo todo ceros en la parte que hace referencia a la red y la dirección del host en la parte que hace referencia a la máquina individual hacemos referencia al 'Host en esta red'.

Dejando inalterada la parte que hace referencia a la red y poniendo todo unos en la parte referente al host realizaremos un 'Broadcast directo' para la red.

Haciendo referencia a la dirección 127 nos encontraremos frente a la 'Dirección de loopback'.

**Máscara de Subred**

La función de una máscara de subred consiste en identificar la parte de la red, de la subred y del host de una dirección IP. Las máscaras de subred sirven para dividir la red y separar una red grande o sumamente grande en segmentos, o subredes, mas pequeños, eficientes y manejables.

Para mas información sobre TCP/IP visiten el siguiente link:

http://www.saulo.net/pub/tcpip/index.html#2-7

Ejemplos:

8bit x 4 octetos = 32 bit. (11111111.11111111.11111111.11111111 = 255.255.255.255)

8bit x 3 octetos = 24 bit. (11111111.11111111.11111111.00000000 = 255.255.255.0)

8bit x 2 octetos = 16 bit. (11111111.11111111.00000000.00000000 = 255.255.0.0)

8bit x 1 octetos = 8 bit. (11111111.00000000.00000000.00000000 = 255.0.0.0)

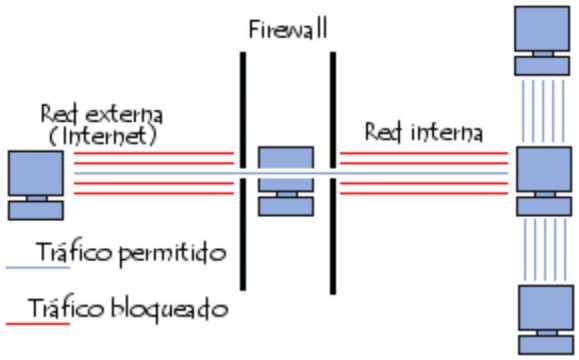
En el ejemplo 10.0.0.0/8, según lo explicado anteriormente, indicaría que la máscara de red es 255.0.0.0

Las máscaras, se utilizan como validación de direcciones realizando una operación AND lógica entre la dirección IP y la máscara para validar al equipo cosa que permite realizar una verificación de la dirección de la Red y con un OR y la máscara negada se obtiene la dirección del broadcasting.

**FIREWALL**

Un **firewall** es un sistema que protege a un ordenador o a una red de ordenadores contra intrusiones provenientes de redes de terceros (generalmente desde internet). Un sistema de firewall filtra paquetes de datos que se intercambian a través de internet. Por lo tanto, se trata de una pasarela de filtrado que comprende al menos las siguientes interfaces de red:

- una interfaz para la red protegida (red interna)
- una interfaz para la red externa.




El sistema firewall es un sistema de software, a menudo sustentado por un hardware de red dedicado, que actúa como intermediario entre la red local (u ordenador local) y una o más redes externas. Un sistema de firewall puede instalarse en ordenadores que utilicen cualquier sistema siempre y cuando:

- La máquina tenga capacidad suficiente como para procesar el tráfico
- El sistema sea seguro
- No se ejecute ningún otro servicio más que el servicio de filtrado de paquetes en el servidor

**Cómo funciona un sistema Firewall**

Un sistema firewall contiene un conjunto de reglas predeterminadas que le permiten al sistema:

- Autorizar la conexión (*permitir*)
- Bloquear la conexión (*denegar*)
- Rechazar el pedido de conexión sin informar al que lo envió (*negar*)

Todas estas reglas implementan un método de filtrado que depende de la **política de seguridad** adoptada por la organización. Las políticas de seguridad se dividen generalmente en dos tipos que permiten:

- la autorización de sólo aquellas comunicaciones que se autorizaron explícitamente:
  "Todo lo que no se ha autorizado explícitamente está prohibido"
- el rechazo de intercambios que fueron prohibidos explícitamente

El primer método es sin duda el más seguro. Sin embargo, impone una definición precisa y restrictiva de las necesidades de comunicación.

**Filtrado de paquetes Stateless**

Un sistema de firewall opera según el principio del filtrado simple de paquetes, o *filtrado de paquetes stateless*. Analiza el encabezado de cada paquete de datos (datagrama) que se ha intercambiado entre un ordenador de red interna y un ordenador externo.

Así, los paquetes de datos que se han intercambiado entre un ordenador con red externa y uno con red interna pasan por el firewall y contienen los siguientes encabezados, los cuales son analizados sistemáticamente por el firewall:

- La dirección IP del ordenador que envía los paquetes
- La dirección IP del ordenador que recibe los paquetes
- El tipo de paquete (TCP, UDP, etc.)
- El número de puerto (recordatorio: un puerto es un número asociado a un servicio o a una aplicación de red).

Las direcciones IP que los paquetes contienen permiten identificar el ordenador que envía los paquetes y el ordenador de destino, mientras que el tipo de paquete y el número de puerto indican el tipo de servicio que se utiliza.

La siguiente tabla proporciona ejemplos de reglas del firewall:

| Regla | Acción | IP fuente | IP destino | Protocolo | Puerto fuente | Puerto destino |
|---|---|---|---|---|---|---|
| 1 | Aceptar | 192.168.10.20 | 194.154.192.3 | tcp | cualquiera | 25 |
| 2 | Aceptar | cualquiera | 192.168.10.3 | tcp | cualquiera | 80 |
| 3 | Aceptar | 192.168.10.0/24 | cualquiera | tcp | cualquiera | 80 |
| 4 | Negar | cualquiera | cualquiera | cualquiera | cualquiera | cualquiera |

Los puertos reconocidos (cuyos números van del 0 al 1023) están asociados con servicios ordinarios (por ejemplo, los puertos 25 y 110 están asociados con el correo electrónico y el puerto 80 con la Web). La mayoría de los dispositivos de firewall se configuran al menos para filtrar comunicaciones de acuerdo con el puerto que se usa. Normalmente, se recomienda bloquear todos los puertos que no son fundamentales (según la política de seguridad vigente).

Por ejemplo, el puerto 23 a menudo se bloquea en forma predeterminada mediante dispositivos de firewall, ya que corresponde al protocolo TELNET, el cual permite a una persona emular el acceso terminal a una máquina remota para ejecutar comandos a distancia. Los datos que se intercambian a través de TELNET no están codificados. Esto significa que es probable que un hacker observe la actividad de la red y robe cualquier contraseña que no esté codificada. Generalmente, los administradores prefieren el

protocolo SSH, el cual tiene la reputación de ser seguro y brinda las mismas funciones que TELNET.

**Filtrado Dinámico**

El Filtrado de paquetes Stateless sólo intenta examinar los paquetes IP independientemente, lo cual corresponde al nivel 3 del modelo OSI (Interconexión de sistemas abiertos). Sin embargo, la mayoría de las conexiones son admitidas por el protocolo TCP, el cual administra sesiones, para tener la seguridad de que todos los intercambios se lleven a cabo en forma correcta. Asimismo, muchos servicios (por ejemplo, FTP) inician una conexión en un puerto estático. Sin embargo, abren un puerto en forma dinámica (es decir, aleatoria) para establecer una sesión entre la máquina que actúa como servidor y la máquina cliente.

De esta manera, con un filtrado de paquetes stateless, es imposible prever cuáles puertos deberían autorizarse y cuáles deberían prohibirse Para solucionar este problema, el sistema de **filtrado dinámico de paquetes** se basa en la inspección de las capas 3 y 4 del modelo OSI, lo que permite denominar este proceso es "**inspección stateful**" o "*filtrado de paquetes stateful*".

Un dispositivo de firewall con "inspección stateful" puede asegurar el control de los intercambios.

Esto significa que toma en cuenta el estado de paquetes previos cuando se definen reglas de filtrado. De esta manera, desde el momento en que una máquina autorizada inicia una conexión con una máquina ubicada al otro lado del firewall, todos los paquetes que pasen por esta conexión serán aceptados implícitamente por el firewall.

El hecho de que el filtrado dinámico sea más efectivo que el filtrado básico de paquetes no implica que el primero protegerá el ordenador contra los hackers que se aprovechan de las vulnerabilidades de las aplicaciones. Aún así, estas vulnerabilidades representan la mayor parte de los riesgos de seguridad.

**Filtrado de aplicaciones**

El filtrado de aplicaciones permite filtrar las comunicaciones de cada aplicación. El filtrado de aplicaciones opera en el nivel 7 (capa de aplicaciones) del modelo OSI, a diferencia del filtrado simple de paquetes (nivel 4). El filtrado de aplicaciones implica el conocimiento de los protocolos utilizados por cada aplicación.

Como su nombre lo indica, el filtrado de aplicaciones permite filtrar las comunicaciones de cada aplicación. El filtrado de aplicaciones implica el conocimiento de las aplicaciones

en la red y un gran entendimiento de la forma en que en ésta se estructuran los datos intercambiados (puertos, etc.).

Un firewall que ejecuta un filtrado de aplicaciones se denomina generalmente "pasarela de aplicaciones" o ("**proxy**"), ya que actúa como relé entre dos redes mediante la intervención y la realización de una evaluación completa del contenido en los paquetes intercambiados. Por lo tanto, el proxy actúa como intermediario entre los ordenadores de la red interna y la red externa, y es el que recibe los ataques. Además, el filtrado de aplicaciones permite la destrucción de los encabezados que preceden los mensajes de aplicaciones, lo cual proporciona una mayor seguridad.

Este tipo de firewall es muy efectivo y, si se ejecuta correctamente, asegura una buena protección de la red. Por otra parte, el análisis detallado de los datos de la aplicación requiere una gran capacidad de procesamiento, lo que a menudo implica la ralentización de las comunicaciones, ya que cada paquete debe analizarse minuciosamente.

Además, el proxy debe interpretar una gran variedad de protocolos y conocer las vulnerabilidades relacionadas para ser efectivo.

Finalmente, un sistema como este podría tener vulnerabilidades debido a que interpreta pedidos que pasan a través de sus brechas. Por lo tanto, el firewall (dinámico o no) debería disociarse del proxypara reducir los riesgos de comprometer al sistema.

**El concepto de Firewall personal**

El término **firewall personal** se utiliza para los casos en que el área protegida se limita al ordenador en el que el firewall está instalado.

Un firewall personal permite controlar el acceso a la red de aplicaciones instaladas en el ordenador y prevenir notablemente los ataques de programas como los troyanos, es decir, programas dañinos que penetran en el sistema para permitir que un hacker controle el ordenador en forma remota. Los firewalls personales permiten subsanar y prevenir intrusiones de aplicaciones no autorizadas a conectarse a su ordenador.

**Limitaciones del Firewall**

Por supuesto que los sistemas firewall no brindan seguridad absoluta; todo lo contrario. Los firewalls sólo ofrecen protección en tanto todas las comunicaciones salientes pasen sistemáticamente a través de éstos y estén configuradas correctamente. Los accesos a la red externa que sortean el firewall también son puntos débiles en la seguridad. Claramente, éste es el caso de las conexiones que se realizan desde la red interna mediante un módem o cualquier otro medio de conexión que evite el firewall.

Asimismo, la adición de medios externos de almacenamiento a los ordenadores de sobremesa o portátiles de red interna puede dañar enormemente la política de seguridad general.

Para garantizar un nivel máximo de protección, debe ejecutarse un firewall en el ordenador y su registro de actividad debe controlarse para poder detectar intentos de intrusión o anomalías.

Además, se recomienda controlar la seguridad (por ejemplo, inscribiéndose para recibir alertas de seguridad de CERT) a fin de modificar los parámetros del dispositivo de firewall en función de las alertas publicadas.

La instalación de un firewall debe llevarse a cabo de la mano de una política de seguridad real.

**Protocolos**

**RIP:** son las siglas de **R**outing **I**nformation **P**rotocol (Protocolo de encaminamiento de información). Es un protocolo de puerta de enlace interna o **IGP** (**I**nternal **G**ateway **P**rotocol) utilizado por los routers (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP. RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancias. La distancia o métrica está determinada por el número de saltos de router hasta alcanzar la red de destino.

**ARP:** son las siglas en inglés de **A**ddress **R**esolution **P**rotocol (Protocolo de resolución de direcciones). Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast (MAC = ff ff ff ff ff ff)) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga.

**ICMP**: El **Protocolo de Mensajes de Control de Internet** o **ICMP** (por sus siglas de ***I**nternet **C**ontrol **M**essage **P**rotocol*) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

ICMP difiere del propósito de TCP y UDP ya que generalmente no se utiliza directamente por las aplicaciones de usuario en la red. La única excepción es la herramienta ping y

traceroute, que envían mensajes de petición Echo ICMP (y recibe mensajes de respuesta Echo) para determinar si un host está disponible, el tiempo que le toma a los paquetes en ir y regresar a ese host y cantidad de hosts por los que pasa.

**UDP**: **User Datagram Protocol** (**UDP**) es un protocolo del nivel de transporte basado en el intercambio de datagramas (Paquetes). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción. Su uso principal es para protocolos como DHCP, DNS, RSTP, SIP, IAX y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

**Conexión de Redes LAN privadas a Internet: NAT**

**NAT** es un servicio que surge de la necesidad de ampliar la cantidad de nodos que se pueden conectar a una red pública ante la falta de direcciones IP del protocolo IPv4.

Es un mecanismo de traducción de direcciones reservadas como “privadas” a una sola IP pública. Esto logra una reducción importante de las direcciones públicas utilizadas y como efecto colateral nos brinda una cierta protección por invisibilidad para los equipos de la red privada.

**Funcionamiento**

El protocolo TCP/IP tiene la capacidad de generar varias conexiones simultáneas con un dispositivo remoto. Para realizar esto, dentro de la cabecera de un paquete IP, existen campos en los que se indica la dirección origen y destino. Esta combinación de números define una única conexión.

Una pasarela NAT cambia la dirección origen en cada paquete de salida y, dependiendo del método, también el puerto origen para que sea único. Estas traducciones de dirección se almacenan en una tabla, para recordar qué dirección y puerto le corresponde a cada dispositivo cliente y así saber donde deben regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la red interna no existe en la tabla de traducciones, entonces es descartado. Debido a este comportamiento, se puede definir en la tabla que en un determinado puerto y dirección se pueda acceder a un

determinado dispositivo, como por ejemplo un servidor web, lo que se denomina **NAT inverso** o **DNAT** (Destination NAT).

## REDES PRIVADAS VIRTUALES

Una red privada virtual o VPN (siglas en inglés de virtual private network), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

### Medios

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autentificación, integridad y confidencialidad de toda la comunicación:

- Autentificación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
- Integridad: de que los datos enviados no han sido alterados. Para ello se utiliza funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).
- Confidencialidad: Dado que solo puede ser interpretada por nadie más que los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).
- No repudio: es decir, un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envió él.

### Requerimientos básicos

- Identificación de usuario: las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.
- Codificación de datos: los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos. Esta tarea se realiza con algoritmos de cifrado como DES o 3DES que solo pueden ser leidos por el emisor y receptor.

- Administración de claves: las VPN deben actualizar las claves de cifrado para los usuarios.

**Tipos de VPN**

Básicamente existen tres arquitecturas de conexión VPN:

**VPN de acceso remoto**

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y lineas telefónicas).

**VPN punto a punto**

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet

provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamadotecnología de túnel o tunneling.

**Tunneling**

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no

se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

**VPN Virtual LAN VLAN**

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes WIFI haciendo uso de Túneles encriptados IPSEC o SSL que además de pasar por los métodos de autenticación tradicionales (WAP, WEP , MAcaddress etc) agregan las credenciales de seguridad del túnel VPN creado en la LAN Interna.

**Implementaciones**

El protocolo estándar de hecho es el IPSEC, pero también tenemos PPTP, L2F, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

Actualmente hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS, que intenta hacer más amigable la configuración y operación de estas soluciones.

- Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Dentro de esta familia tenemos a los productos deFortinet, SonicWALL, WatchGuard, Nortel, Cisco, Linksys, Netscreen (Juniper Networks), Symantec, Nokia, U.S. Robotics, D-link, etc.
- Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperatividad en los modelos anteriores.

Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general. Aquí tenemos por ejemplo a las soluciones nativas de Windows, GNU/Linux y los Unix en general. Por ejemplo productos de código abierto como OpenSSH, OpenVPN y FreeS/Wan.

En ambos casos se pueden utilizar soluciones de firewall ("barrera de fuego" en castellano o cortafuego), obteniendo un nivel de seguridad alto por la protección que brinda, en detrimento del rendimiento.

**Ventajas**

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costos y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.
- Se utiliza más en campus de universidades.

**VOIP**

Voz sobre Protocolo de Internet, también llamado Voz sobre IP, VozIP, VoIP (por sus siglas en inglés), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Internet Protocol). Esto significa que se envía la señal de voz en forma digital en paquetes en lugar de enviarla (en forma digital o analógica) a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional o PSTN (sigla de Public Switched Telephone Network, Red Telefónica Pública Conmutada).

El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo redes de área local (LAN).

Es muy importante diferenciar entre Voz sobre IP (VoIP) y Telefonía sobre IP.

VoIP es el conjunto de normas, dispositivos, protocolos, en definitiva la tecnología que permite la transmisión de la voz sobre el protocolo IP.

Telefonía sobre IP es el conjunto de nuevas funcionalidades de la telefonía, es decir, en lo que se convierte la telefonía tradicional debido a los servicios que finalmente se pueden llegar a ofrecer gracias a poder portar la voz sobre el protocolo IP en redes de datos.

Los principales protocolos utilizados por Voip son: H.323, SIP, IAX y otros subprotocolos utilizados internamente por ellos como RSTP (del inglés Real Time Streaming Protocol)

**Protocolo Ethernet**

Un sistema Ethernet consiste de 3 elementos básicos que son:

- El medio físico; utilizado para llevar las señales entre los dispositivos
- Un conjunto de reglas de control de acceso al medio, o protocolo, en cada interfaz Ethernet, que permite el acceso ordenado al canal Ethernet compartido.
- Un marco (trama) Ethernet, que consiste en un conjunto estandarizado de bits utilizado para llevar datos a través del sistema.

**Funcionamiento de Ethernet**

El protocolo de acceso al medio CSMA/CD, y el marco Ethernet son idénticos para todas las variantes de Ethernet, sin importar la velocidad de transmisión, sin embargo, cada dispositivo equipado con una interfaz Ethernet, también conocido como estación, opera de manera independiente de todas las demás estaciones en la red, no existe un controlador central. Todas las estaciones unidas al Ethernet son conectadas a un sistema de señalamiento compartido, también conocido como medio compartido que puede ser un cable, aire o una Fibra Óptica.

Las señales Ethernet son transmitidas de manera serial, un bit a la vez, sobre el canal, a todas las estaciones conectadas. Para enviar datos, una estación escucha el canal y cuando está sin transmisión, la estación transmite sus datos en la forma de un marco Ethernet o paquete.

Después de la transmisión de cada paquete, todas las estaciones en la red entran nuevamente en una contienda por la siguiente oportunidad de transmisión, lo cual asegura que el acceso al canal es equitativo, y ninguna estación puede asegurar el medio a otras estaciones. El acceso al canal compartido es determinado por el mecanismo de control de acceso al medio, integrado en la interfaz Ethernet de cada estación. El mecanismo de acceso al medio está basado en un sistema llamado Acceso Múltiple por Sensado de Portadora con Detección de Colisión (Carrier Sense Multiple Access with Collision Detect, CSMA/CD).

Las ventajas del protocolo Ethernet residen fundamentalmente en la simplicidad de su implementación y la velocidad que se puede lograr mejorando el control de las colisiones en redes pequeñas. Las desventajas justamente tienen que ver con el aumento logarítmico de las colisiones cuando el número de estaciones aumenta. Para

solucionar esta desventaja, la separación en Dominios de Broadcast como las Virtual LANS (VLAN) aparece como la solución a implementar.

**Spanning Tree Protocol**

**(Spanning Tree Protocol)** es un protocolo de red de nivel 2 de la capa OSI. Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de bucles. STP es transparente a las estaciones de usuario. Trabaja a nivel de los switches de interconexión.

Los bucles infinitos ocurren cuando hay rutas alternativas hacia una misma máquina o segmento de red destino. Estas rutas alternativas son necesarias para proporcionar redundancia, ofreciendo una mayor fiabilidad. Si existen varios enlaces, en el caso que uno falle, otro enlace puede seguir soportando el tráfico de la red. Los problemas aparecen cuando utilizamos dispositivos de interconexión de nivel de enlace, como un puente de red o un conmutador de paquetes.

Cuando hay bucles en la topología de red, los dispositivos de interconexión de nivel de enlace reenvían indefinidamente las tramas Broadcast, al no existir ningún campo TTL (Time To Live,*Tiempo de Vida*) en la Capa 2, al contrario que en la Capa 3. Se consume entonces una gran cantidad de ancho de banda, y en muchos casos la red queda inutilizada. Un router, por el contrario, sí podría evitar este tipo de reenvíos indefinidos. La solución consiste en permitir la existencia de enlaces físicos redundantes, pero creando una topología lógica libre de bucles. STP permite solamente una trayectoria activa a la vez entre dos dispositivos de la red (esto previene los bucles) pero mantiene los caminos redundantes como reserva, para activarlos en caso de que el camino inicial falle.

Si la configuración de STP cambia, o si un segmento en la red redundante llega a ser inalcanzable, el algoritmo reconfigura los enlaces y restablece la conectividad, activando uno de los enlaces de reserva.

Existen múltiples variantes del *Spaning Tree Protocol*, debido principalmente al tiempo que tarda el algoritmo utilizado en converger. Una de estas variantes es el Rapid Spanning Tree Protocol

El árbol de expansión (Spanning tree) permanece vigente hasta que ocurre un cambio en la topología, situación que el protocolo es capaz de detectar de forma automática. El máximo tiempo de duración del árbol de expansión es de cinco minutos. Cuando ocurre uno de estos cambios, el puente raíz actual redefine la topología del árbol de expansión o se elige un nuevo puente raíz.

**Trunking**

El **trunking** es una función para conectar dos switches, routers o servidores, del mismo modelo o no, mediante 2 cables en paralelo en modo Full-Duplex. Así se consigue un ancho de banda del doble para la comunicación entre los equipos. Esto permite evitar cuellos de botella en la conexión de varios segmentos y servidores. El protocolo es 802.1ad

**Port Mirroring**

El **puerto espejo** o **port mirroring** es utilizado con un switch de red para enviar copias de paquetes de red vistos en un puerto del switch (o una VLAN entera) a una conexión de red monitoreada en otro puerto del switch. Esto es comunmente utilizado para aplicaciones de red que requieren monitorear el tráfico de la red, tal como una intrusión-detección al sistema.

**Sistemas de validación con protocolo 802.1x**

La **IEEE 802.1X** es una norma del IEEE para el control de acceso a red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible (EAP– RFC 3748).

802.1X está disponible en ciertos switches y puede configurarse para autenticar nodos que están equipados con software *suplicante*. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos.

Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones en las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corrigiendo deficiencias de seguridad

de WEP. Esta autenticación es realizada normalmente por un tercero, tal como un servidor de RADIUS. Esto permite la autenticación sólo del cliente o, más apropiadamente, una autenticación mutua fuerte utilizando protocolos como EAP-TLS.

**Radius**

**RADIUS** (acrónimo en inglés de ***R****emote* ***A****uthentication* ***D****ial-****I****n* ***U****ser* ***S****erver*). Es un protocolo de autenticación y autorización (AAA) para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cable módem, Ethernet o WiFi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo Network Access Server (NAS) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes)....

RADIUS es extensible; la mayoría de fabricantes de software y hardware RADIUS implementan sus propios dialectos.

**Protocolos de LAN inalámbricas**

**Descripción general de las redes LAN inalámbricas**

Las redes LAN inalámbricas de alta velocidad ofrecen las ventajas de la conectividad de red sin las limitaciones que supone estar atado a una ubicación o por cables. Existen numerosos escenarios en los que este hecho puede ser de interés; entre ellos, se pueden citar los siguientes.

Las conexiones inalámbricas pueden ampliar o sustituir una infraestructura con cables cuando es costoso o está prohibido tender cables. Las instalaciones temporales son un ejemplo de una situación en la que la red inalámbrica tiene sentido o incluso es necesaria. Algunos tipos de construcciones o algunas normativas de construcción pueden prohibir el uso de cableado, lo que convierte a las redes inalámbricas en una importante alternativa.

Y, por supuesto, el fenómeno asociado al término "inalámbrico", es decir, no tener que instalar más cables además de los de la red de telefonía y la red de alimentación eléctrica, ha pasado a ser el principal catalizador para las redes domésticas y la experiencia de conexión desde el hogar.

Los usuarios móviles, cuyo número crece día a día, son indudables candidatos a las redes LAN inalámbricas. El acceso portátil a las redes inalámbricas se realiza a través de equipos portátiles y NIC inalámbricas. Esto permite al usuario viajar a distintos lugares (salas de reunión, vestíbulos, salas de espera, cafeterías, aulas, etc.) sin perder el acceso a los datos de la red. Sin el acceso inalámbrico, el usuario tendría que llevar consigo pesados cables y disponer de conexiones de red.

Más allá del campo empresarial, el acceso a Internet e incluso a sitios corporativos podría estar disponible a través de zonas activas de redes inalámbricas públicas. Los aeropuertos, los restaurantes, las estaciones de tren y otras áreas comunes de las ciudades se pueden dotar del equipo necesario para ofrecer este servicio. Cuando un trabajador que está de viaje llega a su destino, quizás una reunión con un cliente en su oficina, se puede proporcionar acceso limitado al usuario a través de la red inalámbrica local. La red reconoce al usuario de la otra organización y crea una conexión que, a pesar de estar aislada de la red local de la empresa, proporciona acceso a Internet al visitante.

En todos estos escenarios, vale la pena destacar que las redes LAN inalámbricas actuales basadas en estándares funcionan a alta velocidad, la misma velocidad que se consideraba vanguardista para las redes con cable hace tan solo unos años. El acceso del usuario normalmente supera los 11 MB por segundo, de 30 a 100 veces más rápido que las tecnologías de acceso telefónico o de las redes WAN inalámbricas estándar. Este ancho de banda es sin duda adecuado para que el usuario obtenga una gran experiencia con varias aplicaciones o servicios a través de PC o dispositivos móviles. Además, los

avances en curso de estos estándares inalámbricos continúa aumentando el ancho de banda, con velocidades de 22 MB.

Muchos proveedores de infraestructura están dotando de cable zonas públicas de todo el mundo. En los próximos 12 meses, la mayoría de los aeropuertos, centros de conferencias y muchos hoteles proporcionarán acceso de 802.11b a sus visitantes.

**Protocolos Ethernet para LAN inalámbrica**

Para mejorar el acceso a las LAN inalámbricas, se suele utilizar una modificación del protocolo CSMA/CD llamado CSMA/CA o CSMA/CAW, (**C**arrier **S**ense **M**ultiple **A**ccess **C**ollision **A**voidance for **W**ireless) donde la diferencia fundamental con el CSMA/CD es que el emisor estimule al receptor a enviar una trama corta que será detectada por las estaciones cercanas, evitando así transmitir durante la siguiente trama de datos.