Índice

IPv6

Los motivos de IPv6

El motivo básico por el que surge ipv6 fue la evidencia de direcciones.

IPv4 tiene un espacio de direcciones de 32 bits, es decir 2^{32}, mientras que IPv6 tiene un espacio de 2^{128}.

Cabeceras

IPv4:

IPv6:

Cambios y nuevas características

Multicast:

Multicast, la habilidad de enviar un paquete único a destinos múltiples es parte de la especificación base de IPv6. Esto es diferente a IPv4, donde es opcional (aunque usualmente implementado).

IPv6 no implementa broadcast, que es la habilidad de enviar un paquete a todos los nodos del enlace conectado. El mismo efecto puede lograrse enviando un paquete al grupo de multicast de enlace-local todos los nodos (all hosts). Por lo tanto, no existe el concepto de una dirección de broadcast y así la dirección más alta de la red (la dirección de broadcast en una red IPv4) es considerada una dirección normal en IPv6.

Seguridad de Nivel de Red obligatoria:

Internet Protocol Security (IPsec), el protocolo para cifrado y autenticación IP forma parte integral del protocolo base en IPv6. El soporte IPsec es obligatorio en IPv6; a diferencia de IPv4, donde es opcional o fue un agregado posterior (pero usualmente implementado). Sin embargo, actualmente no se está usando normalmente IPsec excepto para asegurar el tráfico entre routers de BGP IPv6, aunque también se puede utilizar en OSPFv3.

Procesamiento simplificado en los routers :

Se hicieron varias simplificaciones en la cabecera de los paquetes, así como en el proceso de reenvío de paquetes para hacer el procesamiento de los paquetes más simple y por ello más eficiente.

- **El encabezado** del paquete en IPv6 es más simple que el utilizado en IPv4, así los campos que son raramente utilizados han sido movidos a opciones separadas; en efecto, aunque las direcciones en IPv6 son 4 veces más largas, el encabezado IPv6 (sin opciones) es solamente el doble de largo que el encabezado IPv4 (sin opciones).
- **Los routers IPv6 no hacen fragmentación**. Los nodos IPv6 requieren ya sea hacer descubrimiento de MTU, realizar fragmentación extremo a extremo o enviar paquetes menores al MTU mínimo de IPv6 de 1280 bytes.
- **El encabezado IPv6 no está protegido por una suma de comprobación** (checksum); la protección de integridad se asume asegurada tanto por el checksum de capa de enlace y por un checksum de nivel superior (TCP, UDP, etc.). En efecto, los routers IPv6 no necesitan recalcular la suma de comprobación cada vez que algún campo del encabezado (como el contador de saltos o Tiempo de Vida) cambian. Esta mejora puede ser menos necesaria en routers que utilizan hardware dedicado para computar este cálculo y así pueden hacerlo a velocidad de línea (wirespeed), pero es relevante para routers por software.

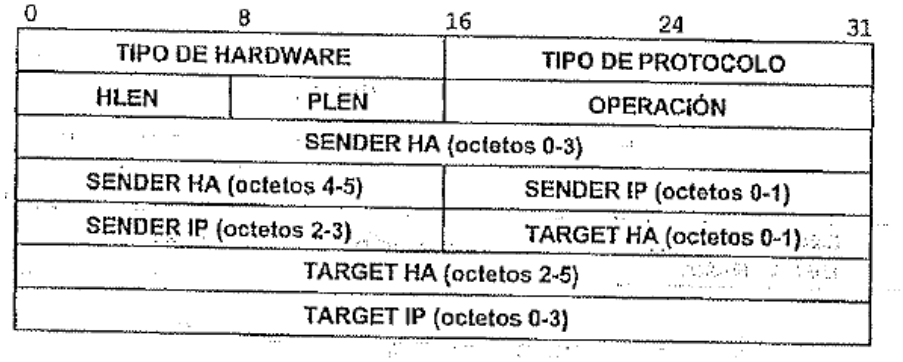
- **El campo Tiempo de Vida de IPv4, conocido como TTL (Time To Live), pasa a llamarse Límite de saltos**, reflejando el hecho de que ya no se espera que los routers computen el tiempo en segundos que tarda en atravesarlo (que en cualquier caso siempre resulta menor de 1 segundo). Se simplifica como el número de saltos entre routers que se permita realizar al paquete IPv6.

ARP

¿Cuál es la función del protocolo ARP?

Es un protocolo de la capa de enlace de datos 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 broadcast de la red que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina 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. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet.

Analizar el formato del mensaje ARP



¿Qué es RARP?

RARP son las siglas en inglés de Reverse Address Resolution Protocol (Protocolo de resolución de direcciones inverso).
Es un protocolo utilizado para resolver la dirección IP de una dirección hardware dada (como una dirección Ethernet). Es el protocolo inverso a ARP.

Explicar por qué los mensajes de ARP-request y RARP-request tienen que ser del tipo broadcast. Las correspondientes respuestas (replies) ¿De qué tipo son? ¿Por qué?

En ARP el host que desea realizar la traducción compone una petición ARP (ARP request) que se encapsula en una trama ethernet con la dirección broadcast, FF:FF:FF:FF:FF:FF, solicitando que el host con la IP buscada responda a dicha petición. Esta trama es recogida por todos los hosts de la red.
Aquellos nodos cuya dirección IP no se corresponda con la indicada en la petición ARP la ignorarán. En cambio, si un host encuentra una coincidencia en la petición (IP target) con su propia IP, enviará una trama ethernet dirigida al emisor de la petición identificándose a sí mismo (ARP reply). El host que originó la petición recibirá la respuesta ARP con la dirección MAC que deseaba averiguar como origen de la trama.

ICMP

¿Cuál es la función del protocolo ICMP?

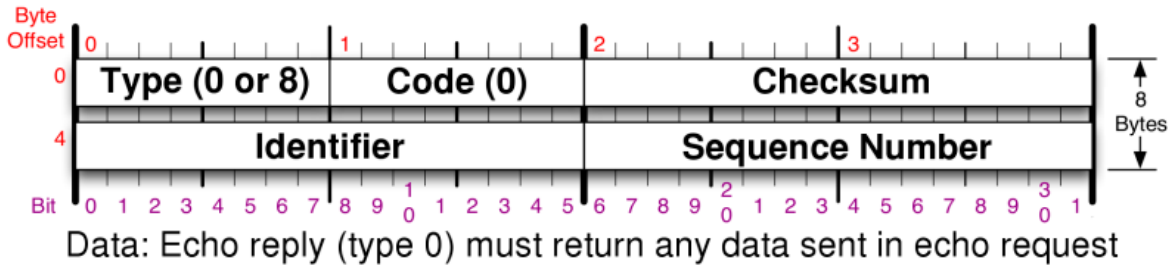
El Protocolo de Mensajes de Control (ICMP) permite que los routers envíen mensajes de error o de control hacia otros routers o terminales. El ICMP proporciona comunicación entre el software del protocolo Internet en una máquina y el mismo software en otra.

¿Qué tipos de mensajes puede llevar el protocolo ICMP?

Los tipos de mensajes que puede llevar el protocolo ICMP son:
0 – Respuesta de Eco
3 – Destino inalcanzable
4 – Disminución de tasa al origen
5 – Redireccionar Mensaje (cambiar la ruta)
6 – Dirección Alternativa de Host
8 – Solicitud de Eco
9 – Anuncio de Router
10 – Solicitud de Router
11 – Tiempo Excedido
12 – Problema de Parámetro 13 – Solicitud de Marca de tiempo (Timestamp)
14 – Respuesta de Marca de Tiempo
15 – Solicitud de Información
16 – Respuesta de Información
17 – Solicitud de Máscara de Dirección
18 – Respuesta de Máscara de Dirección
30 – Traceroute
31 – Error de Conversión de Datagrama
32 – Redirección de Host Móvil
33 – IPv6 Where-Are-You
34 – IPv6 I-Am-Here
35 – Solicitud de Registro de Móvil
36 – Respuesta de Registro de Móvil
37 – Solicitud de Nombre de Dominio
38 – Respuesta de Nombre de Dominio
39 – SKIP Algorithm Discovery Protocol
40 – Photuris – Fallas de seguridad
41 – ICMP para protocolos de movilidad experimentales como Seamoby

Analizar el formato de los siguientes mensajes ICMP

Solicitud de eco y de respuesta:



Tiempo excedido:

El campo TYPE debe tener valor 11 (que identifica el tipo de mensaje ICMP para avisar de un TTL agotado). Dentro del campo código puede ponerse el valor 0 o 1. El campo checksum se utiliza para verificar errores. Luego vienen 32 bits puestos a 0, y luego viene la cabecera IP, más los primeros 64 bits del datagrama que se utilizan para identificar el datagrama que produjo el error (ICMP Trick).

¿Qué es el ping?

Ping es una utilidad administrativa usada para testear la alcanzabilidad de un host o un router en una red. También es usado para medir el tiempo que tarda un mensaje en ir y volver desde una computadora destino. En el proceso, además, se registran las pérdidas de los paquetes, en caso de que las haya. Opera enviando paquetes "echo request" del protocolo ICMP.En el momento que un host recibe un mensaje "echo request", el mismo genera una respuesta que consiste en una copia exacta de los datos recibidos.

¿Qué es el traceroute? ¿Cómo funciona?

Es una herramienta de diagnóstico que permite seguir el camino de los paquetes que vienen desde un determinado host.
Funciona haciendo pings sucesivos al host y aumentando el TTL de cada paquete enviado. Se envía primero un paquete de un host a otro con tiempo de vida 1, al llegar al primer router de su camino el paquete muere y este nodo informa al origen por ICMP que el paquete fue descartado.
El origen recibe este mensaje y vuelve a enviar el paquete pero ahora con TTL 2.
Repite este proceso hasta llegar al destino, habiendo recorrido así toda la ruta que siguió el paquete, e interpretando los mensajes ICMP para determinar en qué nodo se fue acabando el ICMP.

IP

¿Cuál es el propósito del protocolo IP?

Es un protocolo que define el mecanismo de entrega sin conexión y no confiable. Por sin conexión se refiere a que cada paquete se trata de manera independiente a todos los demás, y no confiable significa que la entrega no está garantizada: Los paquetes se pueden perder, duplicar o entregar sin orden, pero el servicio no detectara estas situaciones.

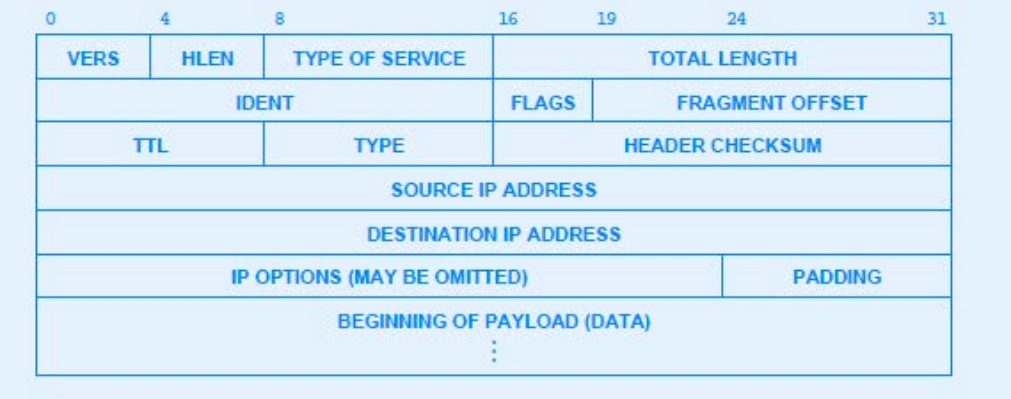
El protocolo IP proporciona 3 definiciones importantes:

- Define la unidad básica para transferencia de datos a través de una red TCP/IP

- Realiza la función de ruteo, seleccionando la ruta por la que los paquetes viajan a destino.

- Incluye un conjunto de reglas que caracterizan la forma en que las terminales y los enrutadores deben procesar los paquetes, cómo y cuándo se deben generar los mensajes de error y las condiciones bajo las cuales los paquetes deben ser descartados.

Representar el formato de un datagrama IP detallando todos sus campos



VERS: Version del protocolo IP utilizado en la creacion del datagrama.

HLEN: Longitud del encabezado, medido en palabras de 32bits (ejemplo para 20 bytes vale 5)

TYPE OF SERVICE: Esta dividido en 5 campos:
P: especifican la prioridad del datagrama, desde 0 (prioridad normal) a 7 (control, de red), permitiendo indicarle al emisor la importancia de cada datagrama.

D: delay, solicita procesamiento con retardos cortos

T: throughput, solicita alto desempeño

R: reliability, solicita alta confiabilidad

C: monetary cost
0: No usado

TOTAL LENGTH: Longitud del datagrama medido en bytes, representa encabezado y datos.

IDENT: identifica el datagrama, para que el destino conozca a qué fragmentos pertenece cada datagrama.

FLAGS: Actualmente utilizado sólo para especificar valores relativos a la fragmentación de paquetes:
bit 2: Reservado; debe ser 0

bit 1: 0 = Divisible, 1 = No Divisible (DF)

bit 0: 0 = Último Fragmento, 1 = Fragmento Intermedio (le siguen más fragmentos) (MF)

FRAGMENT OFFSET: En paquetes fragmentados indica la posición, en unidades de 64 bits, que ocupa el paquete actual dentro del datagrama original. El primer paquete de una serie de fragmentos contendrá en este campo el valor 0.

TTL: Indica el máximo número de routers que un paquete puede atravesar. Cada vez que algún nodo procesa este paquete disminuye su valor en 1 como mínimo, una unidad. Cuando llegue a ser 0, el paquete será descartado.

TYPE: Indica el protocolo usado en el siguiente nivel en el stack de prtocolos.

HEADER CHECKSUM: Suma de Contol de cabecera. Se recalcula cada vez que algún nodo cambia alguno de sus campos (por ejemplo, el Tiempo de Vida). El método de cálculo -intencionadamente simple- consiste en sumar en complemento a 1 cada palabra de 16 bits de la cabecera (considerando valor 0 para el campo de suma de control de cabecera) y hacer el complemento a 1 del valor resultante.

SOURCE IP ADDRESS: Dirección IP en formato de red del origen.

DESTINATION IP ADDRESS: Dirección IP en formato de red del destino.

OPTIONS: Se determina con un sólo octeto indicando el Tipo de opción, el cual está dividido en 3 campos.
Indicador de copia: 1 bit. En caso de fragmentación, la opción se copiará o no a cada nuevo fragmento según el valor de este campo:
0 = no se copia

1 = se copia.

Clase de opción: 2 bits. Las posibles clases son:
0 = control

1 = reservada

2 = depuración y mediciones

3 = ya esta.

Número de opción: 5 bits. Identificador de la opción.

PADDING (RELLENO): Utilizado para asegurar que el tamaño, en bits, de la cabecera es un múltiplo de 32. El valor usado es el 0.

¿Cómo se calcula la longitud de los datos en un datagrama IP?

La longitud de datos de un datagrama IP se calcula teniendo en cuenta la longitud de la cabecera, multiplicada por 4, y restando ese valor a la longitud total de datos del datagrama. Para ello vemos en la cabecera el campo Total Length (Longitud total) y le restamos a este el campo HLEN*4

¿Para qué sirve el campo IDENTIFICACIÓN en el datagrama IP?

Es un dentificador único del datagrama. Se utilizará, en caso de que el datagrama deba ser fragmentado, para poder distinguir los fragmentos de un datagrama de los de otro. El originador del datagrama debe asegurar un valor único para la pareja origen-destino y el tipo de protocolo durante el tiempo que el datagrama pueda estar activo en la red. El valor asignado en este campo debe ir en formato de red.

¿Qué es una PDU?

La unidad de datos de un protocolo se refiere a la cantidad de datos agregada o removida por una capa en el modelo OSI. Cada capa usa una PDU para comunicarse con su par en el otro extremo. Luego de que es removido en la capa n, se le pasa el resto a la capa n+1. Lo inverso sucede en la agregación.

El PDU tiene 4 campos: destino, origen, control, información.

¿Qué es el MTU?

La unidad máxima de transmisión (MTU en ingles) de un protocolo de comunicación es el tamaño en bytes de la unidad de datos más grande que puede ser enviada utilizando dicho protocolo.

Un valor grande brinda mayor eficiencia ya que cada paquete carga más información en relación a la cabecera del protocolo.

A su vez, un paquete grande puede haber sido enviado por un enlace lento causando mayores demoras a los paquetes siguientes. Esto disminuye la latencia.

Otro problema con paquetes grandes se hace visible cuando hay errores de comunicación, ya que un solo bit podría ocasionar la retransmisión completa.

¿Qué es la fragmentación? ¿Cuándo se utiliza?

La fragmentación IP denota la distribución de un paquete IP entre varios bloques de datos, y se utiliza si su tamaño sobrepasa la unidad máxima de transferencia (Maximum Transfer Unit - MTU) del canal.

Explique cómo se arma nuevamente un paquete una vez que el receptor recibe los fragmentos del mismo.

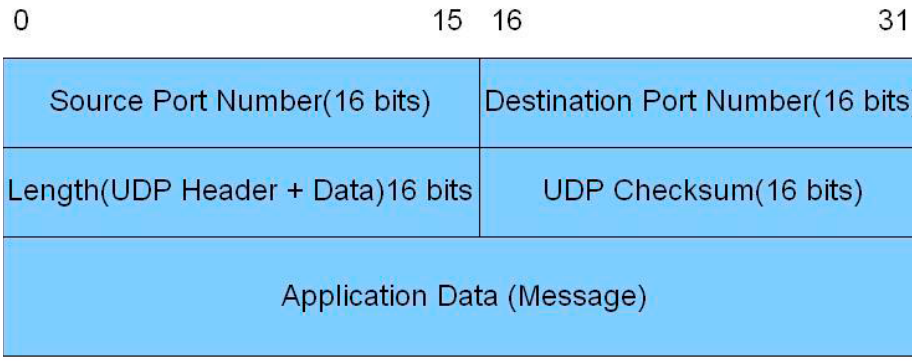
Una vez que el receptor recibe los fragmentos de un paquete, debe analizar el campo Fragment Offset (Desplazamiento de fragmento) para saber dónde debe colocar el fragmento para rearmar el paquete. Además, existe un bit del campo flags, More Fragments, que indica si un fragmento es el último (0) o no (1) del paquete. El desplazamiento es relativo a la parte de datos (no tiene en cuenta la cabecera), por lo tanto si se toma la longitud de datos, se crea un paquete de ese tamaño, y se va llenando con los fragmentos que van llegando puestos en el desplazamiento correcto, se puede reconstruir el paquete.

UDP

¿Cuál es la función del protocolo UDP?

User Datagram Protocol (UDP): protocolo de nivel de transporte basado en el intercambio de datagramas. Su función, por lo tanto, es permitir el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, y de manera no fiable, es decir sin confirmación de entrega/recepción, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros.

Analizar el formato del mensaje UDP.



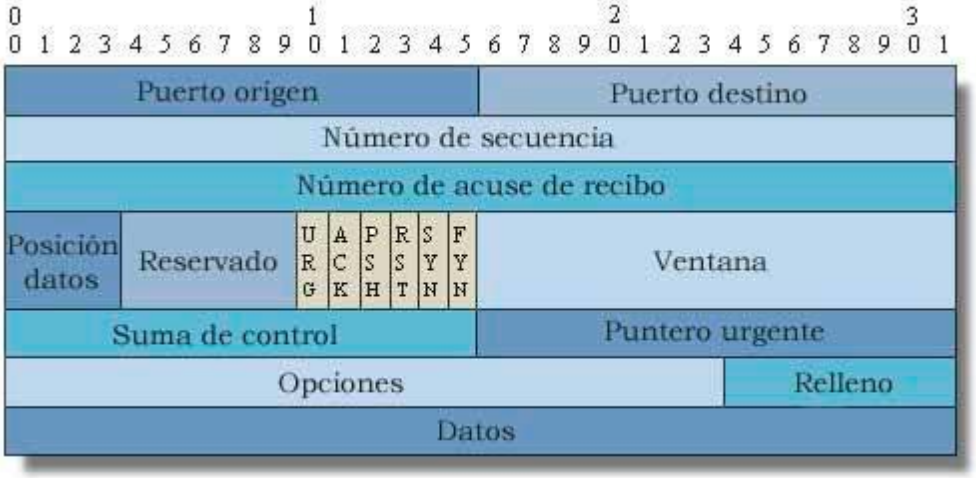
Puerto Origen: Puerto de la aplicación desde donde se envía el datagrama
Puerto Destino: Puerto de la aplicación a la que se envía el datagrama
Longitud: Especifica la longitud en bytes, del datagrama completo.
CheckSum: Para chequeo de errores en cabecera y datos. Es opcional en IPv4, siendo todo 0 si no se requiere calcularlo.

TCP

¿Cuál es la función del protocolo TCP?

Muchos programas dentro de una red de datos compuesta por computadoras, pueden usar TCP para crear conexiones entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.
TCP es un protocolo de comunicación orientado a conexión y fiable del nivel de transporte. Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y, dado que la capa IP aporta un servicio de datagramas no fiable (sin confirmación), TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe libre de errores, sin pérdidas y con seguridad.

Analizar el formato del segmento TCP



Puerto de origen: 16 bits - El número del puerto de origen.

Puerto de destino: 16 bits - El número del puerto de destino.

Número de secuencia: 32 bits - El número de secuencia del primer octeto de datos de este segmento (excepto cuando el indicador SYN esté puesto a uno). Si SYN está puesto a uno es el número de secuencia original (ISN: 'initial sequence number') y, entonces, el primer octeto de datos es ISN+1.

Número de acuse de recibo: 32 bits - Si el bit de control ACK está puesto a uno, este campo contiene el valor del siguiente número de secuencia que el emisor del segmento espera recibir. Una vez que una conexión queda establecida, este número se envía siempre.

Posición de los datos: 4 bits - El número de palabras de 32 bits que ocupa la cabecera de TCP. Este número indica dónde comienzan los datos. La cabecera de TCP (incluso una que lleve opciones) es siempre un número entero de palabras de 32 bits.

Reservado: 6 bits - Reservado para uso futuro. Debe valer 0.

Bits de control: 6 bits (de izquierda a derecha):

URG: Hace significativo el campo "Puntero urgente"

ACK: Hace significativo el campo "Número de acuse de recibo"

PSH: Función de "Entregar datos inmediatamente" ('push')

RST: Reiniciar ('Reset') la conexión

SYN: Sincronizar ('Synchronize') los números de secuencia

FIN: Últimos datos del emisor

Ventana: 16 bits - El número de octetos de datos, a contar a partir del número indicado en el campo de "Número de acuse de recibo", que el emisor de este segmento está dispuesto a aceptar.

Suma de control: 16 bits - El campo "Suma de control" es el complemento a uno de 16 bits de la suma de los complementos a uno de todas las palabras de 16 bits de la cabecera y del texto. Si un segmento contiene un número impar de octetos de cabecera y texto, el último octeto se rellena con ceros a la derecha para formar una palabra de 16 bits con el propósito de calcular la suma de control. En el cálculo de la suma de control, el propio campo suma de control se considera formado por ceros
.
Puntero Urgente: 16 bit - Este campo indica el valor actual del puntero urgente como un desplazamiento positivo desde el número de secuencia de este segmento. El puntero urgente apunta al número de secuencia del octeto al que seguirán los datos urgentes. Este campo es interpretado únicamente si el bit de control URG está establecido a uno.

Opciones: 24 bit
Relleno: variable - El relleno de la cabecera de TCP se utiliza para asegurar que la cabecera de TCP finaliza, y que los datos comienzan, en una posición múltiplo de 32 bits. El relleno está compuesto de ceros.

¿Qué características proporciona TCP?

TCP suministra una serie de servicios a los niveles superiores:
-TCP es un protocolo orientado a conexión.

-TCP debe asegurar que los datos se transmiten y reciben correctamente por los computadores atravesando las correspondientes redes.

-Cada octeto transmitido lleva asignado un número de secuencia.

-El módulo TCP receptor utiliza una rutina de checksum para comprobar la posible existencia de daños en los datos producidos en el proceso de transmisión.

-Si los datos son aceptables, TCP envía una acepción positiva (ACK) al módulo TCP remitente.

-Si los datos han resultado dañados, el TCP receptor los descarta y utiliza un número de secuencia para informar al TCP remitente del problema.

-TCP emplea temporizadores para garantizar que no transcurre un lapso de tiempo demasiado grande antes de la transmisión de aceptaciones desde el nodo receptor y/o de la transmisión de datos desde el nodo transmisor.

-TCP comprueba también la duplicidad de los datos. En el caso de que el TCP remitente decida retransmitir los datos, el TCP descarta los datos redundantes.

-TCP recibe datos de un protocolo de nivel superior de forma orientada a cadenas.

-TCP Se basa en enviar el dispositivo transmisor un valor de "ventana" sin necesidad de recibir ACK

-TCP proporciona transmisión en modo dúplex integral entre las entidades que se comunican.

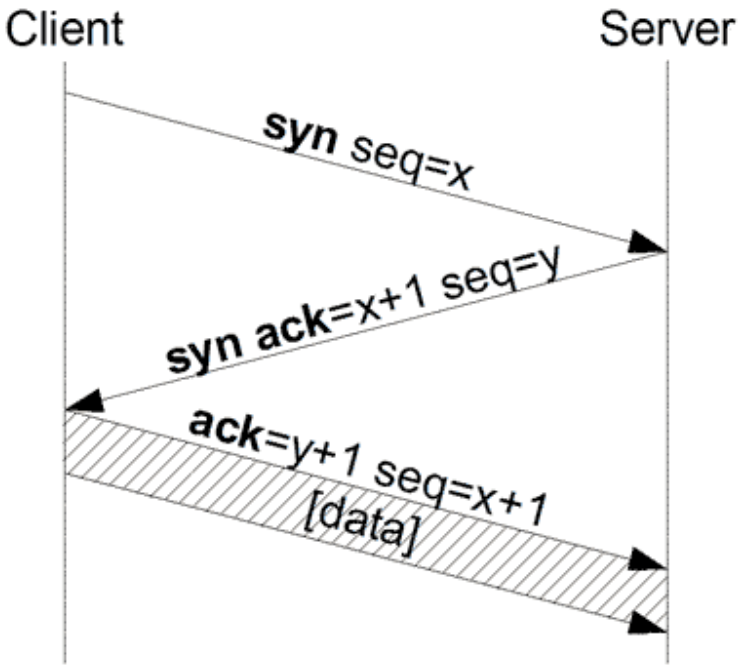
-TCP proporciona el cierre seguro de los circuitos virtuales (la conexión lógica entre dos usuarios).

¿Para qué se utiliza el protocolo de ventana deslizante en TCP? ¿Qué característica particular posee la ventana deslizante en TCP?

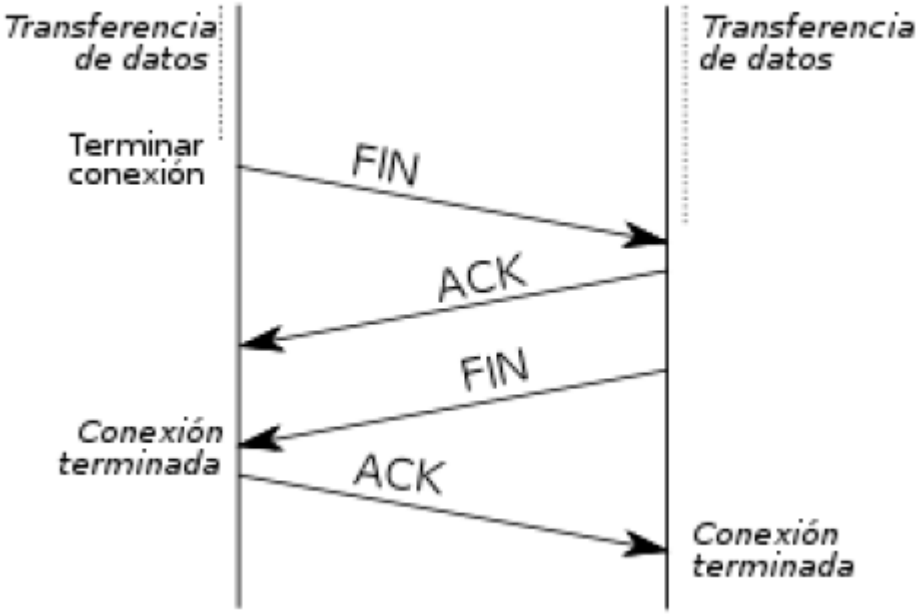
El protocolo de ventana deslizante TCP sirve para el envío de varios paquetes antes de recibir sus respectivos ACK. El tamaño de ventana indica la cantidad de paquetes que se pueden enviar. A medida que se reciben ACKs la ventana se va deslizando, permitiendo el envío de nuevos paquetes.
En TCP el tamaño de la ventana es variable, de acuerdo al estado de la red (control de congestionamiento y control de flujo).

Representar el establecimiento de una conexión TCP y la terminación de una conexión TCP.

Conexión:



Desconexión:



¿Cómo implementa el control de flujo TCP?

Para el control de flujo se utiliza el “windows advertisement”. Utilizando éste, el receptor le avisa al emisor la cantidad de paquetes que puede recibir. Este tamaño de ventana es especificado en el campo “Window” de la cabecera de un segmento TCP.

¿Cuál es la diferencia entre control de flujo y control de congestión?

El control de flujo se refiere a regular la cantidad de datos transmitidos debido a la limitación en el buffer del receptor. El mismo puede estar lleno, o próximo a llenarse, por lo que el receptor avisa al emisor esta situación, y el emisor disminuye la cantidad de datos enviados.
El control de congestión se debe a un estado de la red, en el que hay una gran cantidad de paquetes viajando, que provoca varios errores en la transmisión (o disminución de la performance), y se maneja con los routers intermedios, quienes avisan al emisor que disminuya la tasa de envío de paquetes.

¿Para qué utiliza TCP los puertos de protocolo?

TCP usa el concepto de número de puerto para identificar a las aplicaciones emisoras y receptoras. Cada lado de la conexión TCP tiene asociado un número de puerto (de 16 bits sin signo, con lo que existen 65536 puertos posibles) asignado por la aplicación emisora o receptora.

DNS

¿Qué es DNS?

Domain Name System o DNS (en español: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres legibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente. Para consultas dns corre bajo UDP, mientras que para transacciones entre los servidores corre bajo TCP.

¿Cómo se compone un nombre de dominio? ¿Qué reglas debe cumplir?

1. Los únicos caracteres operativos permitidos para un nombre de dominio son:
- Los pertenecientes al alfabeto inglés: de la 'a' a la 'z'.

- Los dígitos del 0 al 9. (No es aconsejable un nombre con sólo dígitos)

- El guión: - (no puede ser ni el primero ni el último carácter del nombre)

2. No hay distinción entre minúsculas y mayúsculas.

3. Las longitudes máximas y mínimas de un nombre de dominio son:
- Para los .com, .org, .net, hay un máximo de 64 y un mínimo de 2.

- Para el .es: como máximo 63 y como mínimo 3.

4. No se podrán registrar ninguno de los siguientes nombres: edu, com, gov, mil, org, int, net, arpa, firm, store, web, arts, rec, info, o nom.

5. No se podrá registrar ningún nombre que coincida con: protocolos, aplicaciones o terminología de Internet (por ejemplo: telnet, ftp, email, www, web, smtp, http, tcp, dns, wais, news, rfc, ietf, mbone, bbs).

Componentes

Para la operación práctica del sistema DNS se utilizan tres componentes principales:
- Los **Clientes DNS**: Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS *(Por ejemplo: ¿Qué dirección IP corresponde a nombre.dominio?);*

- Los **Servidores DNS**: Que contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.

- Y las **Zonas de autoridad**, porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.

Tipos de servidores DNS

- **Primarios o maestros:** Guardan los datos de un espacio de nombres en sus ficheros

- **Secundarios o esclavos:** Obtienen los datos de los servidores primarios a través de una transferencia de zona.

- **Locales o caché:** Funcionan con el mismo software, pero no contienen la base de datos para la resolución de nombres. Cuando se les realiza una consulta, estos a su vez consultan a los servidores DNS correspondientes, almacenando la respuesta en su base de datos para agilizar la repetición de estas peticiones en el futuro continuo o libre.

Tipos de resolución de nombres de dominio

Existen dos tipos de consultas que un cliente puede hacer a un servidor DNS:
- Iterativa:
Las resoluciones iterativas consisten en la respuesta completa que el servidor de nombres pueda dar. El servidor de nombres consulta sus datos locales (incluyendo su caché) buscando los datos solicitados. El servidor encargado de hacer la resolución realiza iterativamente preguntas a los diferentes DNS de la jerarquía asociada al nombre que se desea resolver, hasta descender en ella hasta la máquina que contiene la zona autoritativa para el nombre que se desea resolver.
- Recursiva:
En las resoluciones recursivas, el servidor no tiene la información en sus datos locales, por lo que busca y se pone en contacto con un servidor DNS raíz, y en caso de ser necesario repite el mismo proceso básico (consultar a un servidor remoto y seguir a la siguiente referencia) hasta que obtiene la mejor respuesta a la pregunta.

Tipos de Registros DNS

Tipo A – Retorna una dirección IPv4 de 32-bit, más comúnmente utilizado para ubicar nombres de host para una dirección IP de una máquina.

Tipo AAAA - Retorna una direcciónIPv6 de 128-bits, más comúnmente utilizado para ubicar nombres de host para una dirección IP de una máquina.

Tipo NS – Delega una zona DNS para utilizar los servidores autoritativos de nombres.

Tipo MX - Asigna un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio.

Tipo CNAME - (Nombre Canónico) Se usa para crear nombres de hosts adicionales, o alias, para los hosts de un dominio. Es usado cuando se están corriendo múltiples servicios (como ftp y servidor web) en un servidor con una sola dirección ip. Cada servicio tiene su propia entrada de DNS (como ftp.ejemplo.com. y www.ejemplo.com.). Esto también es usado cuando se ejecutan múltiples servidores http, con diferentes nombres, sobre el mismo host.

Tipo SOA - (Autoridad de la zona) Proporciona información sobre el servidor DNS primario de la zona, como el correo electrónico del administrador del dominio, el número serial del dominio, y los tiempos de refrescado o actualización.

Tipo PTR - También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo direcciones IP's en nombres de dominio.

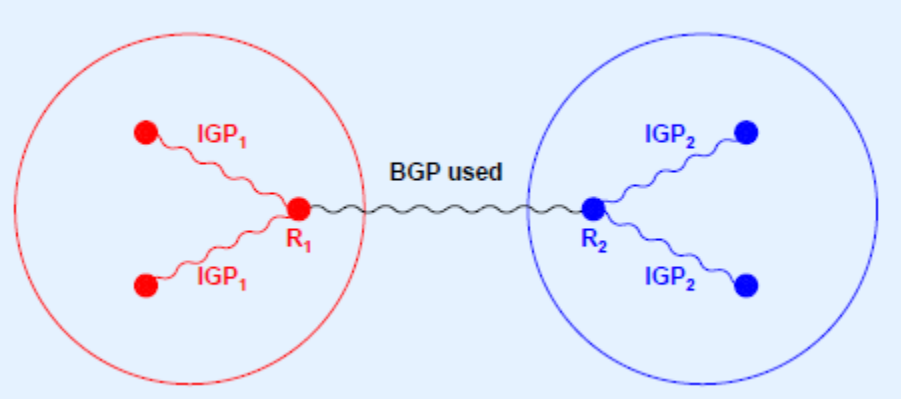
Tipo SRV - Permite indicar los servicios que ofrece el dominio.

Tipo SPF - Sender Policy Framework - Ayuda a combatir el Spam. En este registro se especifica cual o cuales hosts están autorizados a enviar correo desde el dominio dado. El servidor que recibe, consulta el SPF para comparar la IP desde la cual le llega, con los datos de este registro.

IGP

Interior Gateway Protocol (IGP, protocolo de pasarela interno) hace referencia a los protocolos usados dentro de un sistema autónomo.

Por otra parte, un Protocolo de Pasarela Externo determina si la red es accesible desde el sistema autónomo, y usa el IGP para resolver el encaminamiento dentro del propio sistema.



Los IGP se usan para el enrutamiento dentro de un dominio de enrutamiento, aquellas redes bajo el control de una única organización. Un sistema autónomo está comúnmente compuesto por muchas redes individuales que pertenecen a empresas, escuelas y otras instituciones. Un IGP se usa para enrutar dentro de un sistema autónomo, y también se usa para enrutar dentro de las propias redes individuales. Los IGP para IP incluyen RIP, IGRP, EIGRP, OSPF e ISIS.

Los protocolos de pasarela internos se pueden dividir en dos categorías:

Protocolo de enrutamiento vector-distancia:

Calculan las rutas utilizando el algoritmo de Bellman-Ford. En los protocolos de este tipo, ningún enrutador tiene información completa sobre la topología de la red. En lugar de ello, se comunica con los demás enrutadores, enviando y recibiendo información sobre las distancias entre ellos. Así, cada enrutador genera una tabla de enrutamiento que usará en el siguiente ciclo de comunicación, en el que los enrutadores intercambiarán los datos de las tablas. El proceso continuará hasta que todas las tablas alcancen unos valores estables. Este conjunto de protocolos tienen el inconveniente de ser algo lentos, si bien es cierto que son sencillos de manejar y muy adecuados para redes compuestas por pocas máquinas.

Protocolo de enrutamiento enlace-estado

En este caso, cada nodo posee información acerca de la totalidad de la topología de la red. De esta manera, cada uno puede calcular el siguiente salto a cada posible nodo destino de acuerdo a su conocimiento sobre cómo está compuesta la red. La ruta final será entonces una colección de los mejores saltos posibles entre nodos. Esto contrasta con el tipo anteriormente explicado, en el que cada nodo ha de compartir su tabla de enrutamiento con sus vecinos. En los protocolos Enlace-Estado, la única información compartida es aquella concerniente a la construcción de los mapas de conectividad

RIP

Características

RIPv1: No soporta subredes ni direccionamiento CIDR. Tampoco incluye ningún mecanismo de Autentificación de los mensajes. No se usa actualmente. Su especificación está recogida en el RFC 1058. Es un protocolo de routing con clase.

RIPv2: Soporta subredes, CIDR y VLSM. Soporta autenticación utilizando uno de los siguientes Mecanismos: no autentificación, autentificación mediante contraseña, autentificación mediante Contraseña codificada mediante MD5 (desarrollado por Ronald Rivest). Su especificación está Recogida en RFC 1723 y en RFC 2453.

El protocolo RIP, es una implementación directa del vector-distancia en los routers. Utiliza UDP Para enviar sus mensajes a través del puerto 520.

Es un protocolo de enrutamiento. Calcula la ruta más corta hacia la red de destino usando el Algoritmo del vector de distancias.

Esta distancia o métrica, la determina usando el número de saltos de router en router hasta Alcanzar la red de destino. Para ello usa la métrica informada por su vecino más próximo más uno.
La métrica máxima de conteo de saltos en RIP es de 15, 16 se considera una ruta inalcanzable.
La distancia administrativa (grado de conocimiento y confiabilidad) máxima es de 120 (RIP2) en los Equipos cisco.

Ventajas e Inconvenientes

Ventajas de RIP:
RIP es más fácil de configurar (comparativamente a otros protocolos).
Es un protocolo abierto (admite versiones derivadas aunque no necesariamente compatibles).
Es soportado por la mayoría de los fabricantes.

Desventajas de RIP:
Su principal desventaja, consiste en que para determinar la mejor métrica, únicamente toma en cuenta el número de saltos, descartando otros criterios (Ancho de Banda, congestión, carga, retardo, fiabilidad, etc.).
RIP tampoco está diseñado para resolver cualquier posible problema de enrutamiento

Modo de Operación

El valor de (AD) de RIP es de 120, por ello tiene menor prioridad sobre los demás protocolos de encaminamiento.

Cuando RIP se inicia, envía un mensaje a cada uno de sus vecinos (en el puerto bien conocido 520) pidiendo una copia de la tabla de encaminamiento del vecino. Este mensaje es una solicitud (el campo "command" se pone a 1) con "address family" a 0 y "metric" a 16. Los "routers" vecinos devuelven una copia de sus tablas de encaminamiento.

Cuando RIP está en modo activo envía toda o parte de su tabla de encaminamiento a todos los vecinos por broadcast y/o con enlaces punto a punto. Esto se hace cada 30 segundos. La tabla de encaminamiento se envía como respuesta ("command" vale 2, aun que no haya habido petición). Cuando RIP descubre que una métrica ha cambiado, la difunde por broadcast a los demás "routers".

Cuando RIP recibe una respuesta, el mensaje se valida y la tabla local se actualiza si es necesario (Para mejorar el rendimiento y la fiabilidad, RIP especifica que una vez que un "router"(o host) ha aprendido una ruta de otro, debe guardarla hasta que conozca una mejor (de coste estrictamente menor). Esto evita que los "routers" oscilen entre dos o más rutas de igual coste).

Cuando RIP recibe una petición, distinta de la solicitud de su tabla, se devuelve como respuesta la métrica para cada entrada de dicha petición fijada al valor de la tabla local de encaminamiento. Si no existe ruta en la tabla local, se pone a 16.

Las rutas que RIP aprende de otros "routers" expiran a menos que se vuelvan a difundir en 180 segundos(6 ciclos de broadcast). Cuando una ruta expira, su métrica se pone a infinito, la invalidación de la ruta se difunde a los vecinos, y 60 segundos más tarde, se borra de la tabla.

Mensajes RIP

Tipos de mensajes RIP

Los mensajes RIP pueden ser de dos tipos.

Petición: Enviados por algún encaminador recientemente iniciado que solicita información de los encaminadores vecinos.

Respuesta: mensajes con la actualización de las tablas de encaminamiento.
Existen tres tipos:

Mensajes *ordinarios*: Se envían cada 30 segundos. Para indicar que el enlace y la ruta siguen activos. Se envía la tabla de encaminado completa.

Mensajes enviados como *respuesta* a mensajes de petición.

Mensajes enviados cuando *cambia algún coste*. Se envía toda la tabla de encaminado.

OSPF

Características

Open Shortest Path First (frecuentemente abreviado OSPF) es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible. Usa cost como su medida de métrica. Además, construye una base de datos enlace-estado (link-state database, LSDB) idéntica en todos los enrutadores de la zona.

OSPF es probablemente el tipo de protocolo IGP más utilizado en grandes redes. IS-IS, otro protocolo de enrutamiento dinámico de enlace-estado, es más comun en grandes proveedores de servicio. Puede operar con seguridad usando MD5 para autentificar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado. Como sucesor natural de RIP, acepta VLSM o CIDR sin clases desde su inicio.

Una red OSPF se puede descomponer en regiones (áreas) más pequeñas. Hay un área especial llamada área backbone que forma la parte central de la red y donde hay otras áreas conectadas a ella.

OSPF puede usar tanto multidifusiones como unidifusiones para enviar paquetes de bienvenida y actualizaciones de enlace-estado. Las direcciones de multidifusiones usadas son 224.0.0.5 y 224.0.0.6. Al contrario que RIP o BGP, OSPF no usa ni TCP ni UDP, sino que usa IP directamente, mediante el protocolo IP 89.

OSPF mantiene actualizada la capacidad de enrutamiento entre los nodos de una red mediante la difusión de la topología de la red y la información de estado-enlace de sus distintos nodos.

Esta difusión se realiza a través de varios tipos de paquetes:

• Paquetes Hello (tipo 1). Cada router envía periódicamente a sus vecinos un paquete que contiene el listado de vecinos reconocidos por el router, indicando el tipo de relación que mantiene con cada uno.

• Paquetes de descripción de base de datos estado-enlace (DataBase Description,DBD) (tipo 2). Se emplean en el intercambio de base de datos enlace-estado entre dos nodos, y permiten informar al otro nodo implicado en la sincronización acerca de los registros contenidos en la LSDB propia, mediante un resumen de estos.

• Paquetes de estado-enlace o Link State Advertisements (LSA). Los cambios en el estado de los enlaces de un router son notificados a la red mediante el envío de mensajes LSA.

Características principales:

- Carga balanceada a través de multiples caminos
- Redes particionadas en subsistemas llamados áreas
- Autenticación de mensajes
- Router designado para optimización de redes compartidas
- Puede importar información de ruteo externa

OSPF organiza un sistema autónomo (AS) en áreas. Estas áreas son grupos lógicos de routers cuya información se puede resumir para el resto de la red. Un área es una unidad de enrutamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Database): de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser "parcelado" en su área.

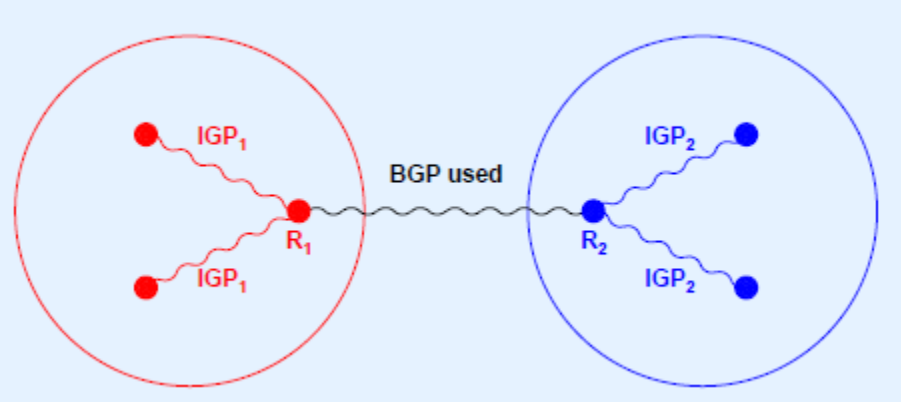
EGP

BGP

Los EGP están diseñados para su uso entre diferentes sistemas autónomos que están controlados por distintas administraciones**.**

En general, el BGP se utiliza entre ISP y a veces entre una compañía y un ISP. **El BGP es el único EGP actualmente viable y es el protocolo de enrutamiento que usa Internet.** El BGP es un protocolo de vector de ruta que puede usar muchos atributos diferentes para medir las rutas. En el ámbito del ISP, con frecuencia hay cuestiones más importantes que la simple elección de la ruta más rápida.

Surgió la necesidad de interconectar diferentes internetworks y proveer el enrutamiento entre ellas. El protocolo Border Gateway Routing (BGP) ahora se usa entre ISP y entre ISP y sus clientes privados más grandes para intercambiar información de enrutamiento



El protocolo BGP se utiliza para intercambiar información. El intercambio de información en la red se realiza mediante el establecimiento de una sesión de comunicación entre los routers de borde de los sistemas autónomos.

Para conseguir una entrega fiable de la información, se hace uso de una sesión de comunicación basada en TCP en el puerto número 179. Esta sesión debe mantenerse conectada debido a que ambos extremos de la comunicación periódicamente se intercambian y actualizan información. De modo que al principio, cada router envía al vecino toda su información de encaminamiento y después únicamente se enviarán las nuevas rutas, las actualizaciones o la eliminación de rutas transmitidas con anterioridad. Además periódicamente se envían mensajes para garantizar la conectividad.

Cuando una conexión TCP se interrumpe por alguna razón, cada extremo de la comunicación está obligado a dejar de utilizar la información que ha aprendido por el otro lado. En otras palabras, la sesión TCP sirve como un enlace virtual entre dos sistemas autónomos vecinos, y la falta de medios de comunicación indica que el enlace virtual se ha caído. Cabe destacar que esa unión virtual tendrá más de un enlace físico que conecte a los dos routers frontera, pero si una conexión virtual se cae no indica necesariamente que la conexión física se haya caído.

Características

- Conecta varios IGP entre sí.

- Permite la autenticación.

- Soporta CIDR.

- Dos routers de border generan un par BGP.

- Propaga información de accesibilidad.

- Soporte para Politicas

- Permite la agregación de las rutas.

- Permite actualizaciones incrementales.

- Envia información de la ruta.

- Utiliza TCP.

VPN

Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada
Una Red Privada Virtual (VPN) conecta los componentes de una red sobre otra red. VPN logra este objetivo mediante la conexión de los usuarios de distintas redes a través de un túnel que se construye sobre internet o sobre cualquier red pública.
La seguridad de la conexión a través de la red internet de forma lógica, aparece en el usuario como si fuera virtualmente una red privada tipo LAN. Pero trabajando sobre una red pública.
Lo que genera el nombre de RED PRIVADA VIRTUAL.

Características básicas de la seguridad

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autentificación, integridad 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.
- **Confidencialidad:** Dado que sólo puede ser interpretada por los destinatarios de la misma.
- **No repudio:** Es decir, un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envió él o ella.

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 sólo pueden ser leídos por el emisor y receptor.

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

- **Nuevo algoritmo de seguridad SEAL.**

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.

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.

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.

VPN over LAN
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.

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.

Tipos de conexión

Conexión de acceso remoto
Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión VPN router a router
Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentica ante el router que realiza la llamada y también sirve para la intranet.

Conexión VPN firewall a firewall
Una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

NAT

Características

NAT (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por encaminadores IP (routers) para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados.

La mayoría de los NAT asignan varias máquinas (hosts) privadas a una dirección IP expuesta públicamente.

- Obtiene una dirección global única por conexión de internet

- Se corre el software NAT en el router que conecta la red a internet

NAT reemplaza la dirección de fuente en un datagrama saliente y reemplaza la dirección de destino en un datagrama entrante, todo esto según una tabla de traducción NAT
NAT debe:

- Cambiar las cabeceras IP
- Posiblemente cambiar los puertos de origen tcp y udp
- Recomputar los checksum de tcp y udp
- Traducir los mensajes ICMP
- Traducir los números de puertos en una sesión FTP

FTP

Características

Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos.

Tipos de conexión

Conexión de control:
Esta la realiza el usuario a través del puerto 21, la función de esta conexión es la del envío y recepción de órdenes, estas órdenes especifican por ejemplo: puerto de datos, modo de transferencia, etc, asi como también especifican la naturaleza de la operación sobre el sistema de archivos, puede ser recuperar, añadir, borrar, etc.

Conexión de datos:
Esta se realiza haciendo uso del puerto 20 y su objetivo es el de transferir los datos en función de los parámetros que se hayan especificado en la conexión de control.

Servidor FTP

Un servidor FTP es un programa especial que se ejecuta en un equipo servidor normalmente conectado a Internet (aunque puede estar conectado a otros tipos de redes, LAN, MAN, etc.). Su función es permitir el intercambio de datos entre diferentes servidores/ordenadores.
Por lo general, los programas servidores FTP no suelen encontrarse en los ordenadores personales, por lo que un usuario normalmente utilizará el FTP para conectarse remotamente a uno y así intercambiar información con él.

Cliente FTP

Cuando un navegador no está equipado con la función FTP, o si se quiere cargar archivos en un ordenador remoto, se necesitará utilizar un programa cliente FTP. Un cliente FTP es un programa que se instala en el ordenador del usuario, y que emplea el protocolo FTP para conectarse a un servidor FTP y transferir archivos, ya sea para descargarlos o para subirlos.

Para utilizar un cliente FTP, se necesita conocer el nombre del archivo, el ordenador en que reside (servidor, en el caso de descarga de archivos), el ordenador al que se quiere transferir el archivo (en caso de querer subirlo nosotros al servidor), y la carpeta en la que se encuentra.

Algunos clientes de FTP básicos en modo consola vienen integrados en los sistemas operativos.

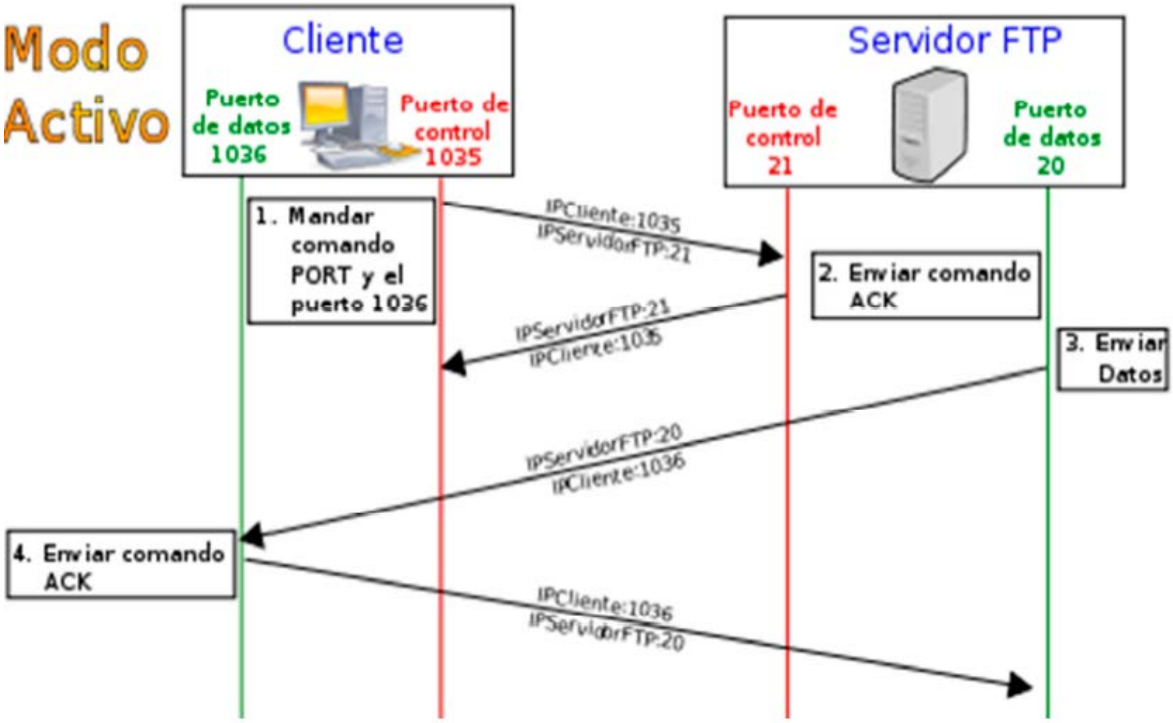
Acceso anónimo

Los servidores FTP anónimos ofrecen sus servicios libremente a todos los usuarios, permiten acceder a sus archivos sin necesidad de tener un 'USER ID' o una cuenta de usuario. Es la manera más cómoda fuera del servicio web de permitir que todo el mundo tenga acceso a cierta información sin que para ello el administrador de un sistema tenga que crear una cuenta para cada usuario.

Si un servidor posee servicio 'FTP anonymous' solamente con teclear la palabra «anonymous», cuando pregunte por tu usuario tendrás acceso a ese sistema.

Modos de conexión del cliente FTP

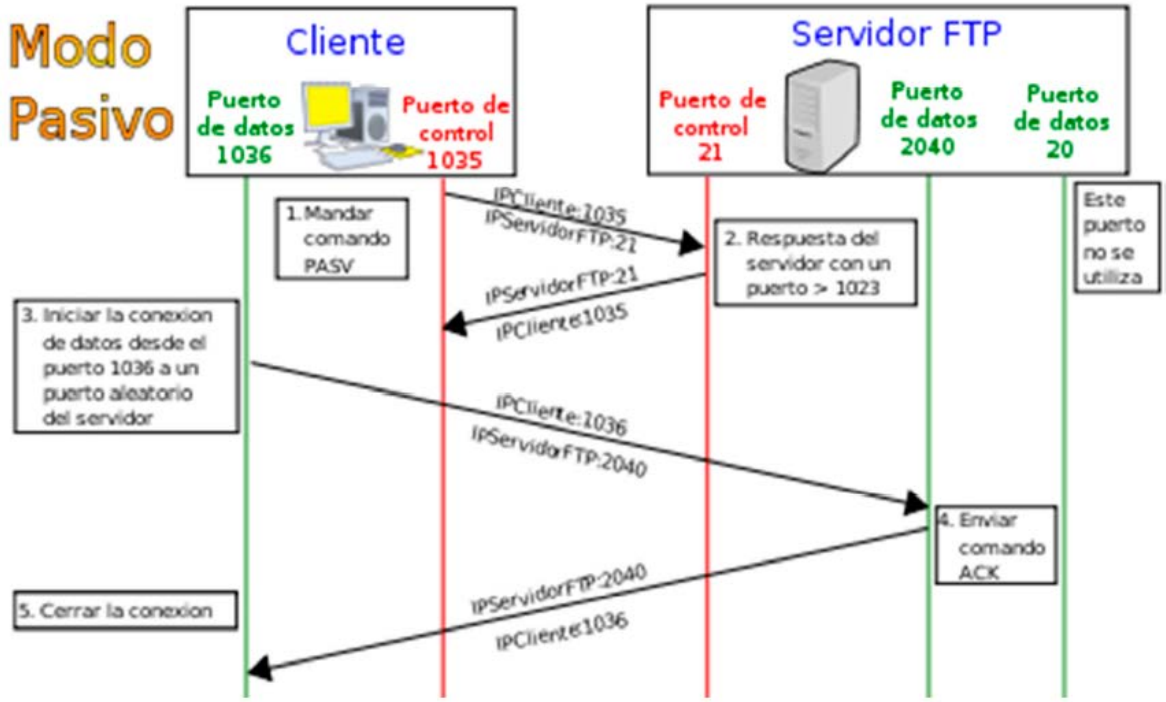
Modo activo:



En modo Activo, el servidor siempre crea el canal de datos en su puerto 20, mientras que en el lado del cliente el canal de datos se asocia a un puerto aleatorio mayor que el 1024. Para ello, el cliente manda un comando PORT al servidor por el canal de control indicándole ese número de puerto, de manera que el servidor pueda abrirle una conexión de datos por donde se transferirán los archivos y los listados, en el puerto especificado.

Lo anterior tiene un grave problema de seguridad, y es que la máquina cliente debe estar dispuesta a aceptar cualquier conexión de entrada en un puerto superior al 1024.

Modo pasivo:



Cuando el cliente envía un comando PASV sobre el canal de control, el servidor FTP le indica por el canal de control, el puerto (mayor a 1023 del servidor. Ej:2040) al que debe conectarse el cliente. El cliente inicia una conexión desde el puerto siguiente al puerto de control (ej: 1036) hacia el puerto del servidor especificado anteriormente (ej: 2040).

TFTP

Características

TFTP son las siglas de Trivial file transfer Protocol (Protocolo de transferencia de archivos trivial). Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Window o cualquier otro cliente ligero arranca desde un servidor de red.

Algunos detalles del TFTP:

- Utiliza UDP (en el puerto 69) como protocolo de transporte (a diferencia de FTP que utiliza el puerto 21 TCP).
- No puede listar el contenido de los directorios.
- No existen mecanismos de autenticación o cifrado.
- Se utiliza para leer o escribir archivos de un servidor remoto.
- Soporta tres modos diferentes de transferencia, "netascii", "octet" y "mail", de los que los dos primeros corresponden a los modos "ascii" e "imagen" (binario) del protocolo FTP.

Detalles de una sesión TFTP

Ya que TFTP utiliza UDP, no hay una definición formal de sesión, cliente y servidor, aunque se considera servidor a aquel que abre el puerto 69 en modo UDP, y cliente a quien se conecta. Sin embargo, cada archivo transferido vía TFTP constituye un intercambio independiente de paquetes, y existe una relación cliente-servidor informal entre la máquina que inicia la comunicación y la que responde.

- La máquina A, que inicia la comunicación, envía un paquete RRQ (read request/petición de lectura) o WRQ (write request/petición de escritura) a la máquina B, conteniendo el nombre del archivo y el modo de transferencia.

- B responde con un paquete ACK (acknowledgement/confirmación), que también sirve para informar a A del puerto de la máquina B al que tendrá que enviar los paquetes restantes.

- La máquina origen envía paquetes de datos numerados a la máquina destino, todos excepto el último conteniendo 512 bytes de datos. La máquina destino responde con paquetes ACK numerados para todos los paquetes de datos.

- El paquete de datos final debe contener menos de 512 bytes de datos para indicar que es el último. Si el tamaño del archivo transferido es un múltiplo exacto de 512 bytes, el origen envía un paquete final que contiene 0 bytes de datos.

NFS

Características

Es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales.

- El sistema NFS está dividido al menos en dos partes principales: un servidor y uno o más clientes. Los clientes acceden de forma remota a los datos que se encuentran almacenados en el servidor.

- Las estaciones de trabajo locales utilizan menos espacio de disco debido a que los datos se encuentran centralizados en un único lugar pero pueden ser accedidos y modificados por varios usuarios, de tal forma que no es necesario replicar la información.

- Los usuarios no necesitan disponer de un directorio “home” en cada una de las máquinas de la organización. Los directorios “home” pueden crearse en el servidor de NFS para posteriormente poder acceder a ellos desde cualquier máquina a través de la infraestructura de red.

- También se pueden compartir a través de la red dispositivos de almacenamiento como disqueteras, CD-ROM y unidades ZIP. Esto puede reducir la inversión en dichos dispositivos y mejorar el aprovechamiento del hardware existente en la organización.

SMTP

Características

Es un protocolo de la capa de aplicación. Protocolo de red basado en textos utilizados para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos
SMTP se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste enteramente en líneas de texto compuestas por caracteres ASCII. El tamaño máximo permitido para estas líneas es de 1000 caracteres.

Las respuestas del servidor constan de un código numérico de tres dígitos, seguido de un texto explicativo. El número va dirigido a un procesado automático de la respuesta por autómata, mientras que el texto permite que un humano interprete la respuesta.

En el conjunto de protocolos TCP/IP, el SMTP va por encima del TCP (utiliza TCP), usando normalmente el puerto 25 en el servidor para establecer la conexión.

Resumen simple del funcionamiento del protocolo SMTP

- Cuando un cliente establece una conexión con el servidor SMTP, espera a que éste envíe un mensaje “220 Service ready” o “421 Service non available”

- Se envía un HELO desde el cliente. Con ello el servidor se identifica. Esto puede usarse para comprobar si se conectó con el servidor SMTP correcto.

- El cliente comienza la transacción del correo con la orden MAIL FROM. Como argumento de esta orden se puede pasar la dirección de correo al que el servidor notificará cualquier fallo en el envío del correo (Por ejemplo, MAIL FROM:<fuente@host0>). Luego si el servidor comprueba que el origen es válido, el servidor responde “250 OK”.

- Ya le hemos dicho al servidor que queremos mandar un correo, ahora hay que comunicarle a quien. La orden para esto es RCPT TO:<destino@host>. Se pueden mandar tantas órdenes RCPT como destinatarios del correo queramos. Por cada destinatario, el servidor contestará “250 OK” o bien “550 No such user here”, si no encuentra al destinatario.

- Una vez enviados todos los RCPT, el cliente envía una orden DATA para indicar que a continuación se envían los contenidos del mensaje. El servidor responde “354 Start mail input, end with <CRLF>.<CRLF>” Esto indica al cliente como ha de notificar el fin del mensaje.

- Ahora el cliente envía el cuerpo del mensaje, línea a línea. Una vez finalizado, se termina con un <CRLF>.<CRLF> (la última línea será un punto), a lo que el servidor contestará “250 OK”, o un mensaje de error apropiado.

- Tras el envío, el cliente, si no tiene que enviar más correos, con la orden QUIT corta la conexión.

También puede usar la orden TURN, con lo que el cliente pasa a ser el servidor, y el servidor se convierte en cliente. Finalmente, si tiene más mensajes que enviar, repite el proceso hasta completarlos.

Puede que el servidor SMTP soporte las extensiones definidas en el RFC 1651, en este caso, la orden HELO puede ser sustituida por la orden EHLO, con lo que el servidor contestará con una lista de las extensiones admitidas. Si el servidor no soporta las extensiones, contestará con un mensaje "500 Syntax error, command unrecognized".

Formato del mensaje

Como se muestra en el ejemplo anterior, el mensaje es enviado por el cliente después de que éste manda la orden DATA al servidor. El mensaje está compuesto por dos partes:

- Cabecera: en el ejemplo las tres primeras líneas del mensaje son la cabecera. En ellas se usan unas palabras clave para definir los campos del mensaje. Éstos campos ayudan a los clientes de correo a organizarlos y mostrarlos. Los más típicos son subject (asunto), from (emisor) y to (receptor). Éstos dos últimos campos no hay que confundirlos con las órdenes MAIL FROM y RCPT TO, que pertenecen al protocolo, pero no al formato del mensaje.
- Cuerpo del mensaje: es el mensaje propiamente dicho. En el SMTP básico está compuesto únicamente por texto, y finalizado con una línea en la que el único carácter es un punto.

Seguridad y spam

Una de las limitaciones del SMTP original es que no facilita métodos de autenticación a los emisores.

POP

Características

En informática se utiliza el Post Office Protocol (POP3, Protocolo de la oficina de correo) en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de nivel de aplicación en el Modelo OSI.

Las versiones del protocolo POP, informalmente conocido como POP1 y POP2, se han hecho obsoletas debido a las últimas versiones de POP3. En general cuando se hace referencia al término POP, se refiere a POP3 dentro del contexto de protocolos de correo electrónico.

POP3 está diseñado para recibir correo, no para enviarlo; le permite a los usuarios con conexiones intermitentes o muy lentas (tales como las conexiones por módem), descargar su correo electrónico mientras tienen conexión y revisarlo posteriormente incluso estando desconectados.

Cabe mencionar que la mayoría de los clientes de correo incluyen la opción de dejar los mensajes en el servidor, de manera tal que, un cliente que utilice POP3 se conecta, obtiene todos los mensajes, los almacena en la computadora del usuario como mensajes nuevos, los elimina del servidor y finalmente se desconecta. En contraste, el protocolo IMAP permite los modos de operación conectado y desconectado.

Al igual que otros viejos protocolos de internet, POP3 utilizaba un mecanismo de firmado sin cifrado. La transmisión de contraseñas de POP3 en texto plano aún se da. En la actualidad POP3 cuenta con diversos métodos de autenticación que ofrecen una diversa gama de niveles de protección contra los accesos ilegales al buzón de correo de los usuarios.

IMAP

Características

Es un protocolo de aplicación de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. IMAP tiene varias ventajas sobre POP, que es el otro protocolo empleado para obtener correo desde un servidor. Por ejemplo, es posible especificar en IMAP carpetas del lado servidor. Por otro lado, es más complejo que POP ya que permite visualizar los mensajes de manera remota y no descargando los mensajes como lo hace POP.

IMAP es utilizado frecuentemente en redes grandes; por ejemplo los sistemas de correo de un campus. IMAP les permite a los usuarios acceder a los nuevos mensajes instantáneamente en sus computadoras, ya que el correo está almacenado en la red. Con POP3 los usuarios tendrían que descargar el correo electrónico a sus computadoras o accederlo vía web. Ambos métodos toman más tiempo de lo que le tomaría a IMAP, y se tiene que descargar el correo electrónico nuevo o refrescar la página para ver los nuevos mensajes.

Ventajas sobre POP3

Algunas de las características importantes que diferencian a IMAP y POP3 son:

- Soporte para operación en línea y fuera de línea

- Soporte para la conexión de múltiples clientes simultáneos a un mismo destinatario

- Soporte para acceso a partes MIME de los mensajes y obtención parcial

- Soporte para que la información de estado del mensaje se mantenga en el servidor

- Soporte para accesos múltiples a los buzones de correo en el servidor

- Soporte para búsquedas de parte del servidor

- Soporte para un mecanismo de extensión definido.

MIME

Para permitir la transmisión de datos no ASCII a través de e-mail, la IETF definió la **Multipurpose Internet Mail Extension (MIME)**. La MIME no cambia al SMTP ni lo remplaza. De hecho, la MIME permite que datos arbitrarios siga codificándose en ASCII y luego se envíen por medio de mensajes e-mail estándar. Para adaptarse a tipos y representaciones arbitrarias de datos, cada mensaje MIME incluye datos que informan al recipiente del tipo de datos y de la codificación utilizada.

Son una serie de convenciones o especificaciones dirigidas al intercambio a través de Internet de todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario. Una parte importante del MIME está dedicada a mejorar las posibilidades de transferencia de texto en distintos idiomas y alfabetos. En sentido general las extensiones de MIME van encaminadas a soportar:

- Texto en conjuntos de caracteres distintos de US-ASCII;
- adjuntos que no son de tipo texto;
- cuerpos de mensajes con múltiples partes (multi-part);
- información de encabezados con conjuntos de caracteres distintos de ASCII.

HTTP

Características

Hypertext Transfer Protocol o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web. HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. **Es un protocolo de capa de aplicación.**

Es un protocolo **orientado a transacciones** y sigue el **esquema petición-respuesta** entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador web o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un localizador uniforme de recursos (URL). **La transferencia de información es bi-direccional.**

HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de "sesión", y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.

Corre sobre el TCP en el puerto 80.

URL

Al identificador de páginas webs, se lo identifica con el nombre de **localizador uniforme de recursos (URL)**, el cual codifica lo siguiente:

- Protocolo de acceso a usar
- DNS
- Número del puerto del protocolo (opcional)
- Path hacia el archivo de sistema del servidor (opcional)
- Parámetros (opcional)
- Cola (opcional)

Para la WWW, existen dos estándar importantes, uno es el que se utiliza para la representación de los datos. Este protocolo es el HTML. El otro estándar es el que se utiliza para la transferencia de los datos, este es HTTP.

Operación HTTP

Una operación básica de http consiste en :

- El servidor envía solicitudes a las cuales el servidor responde
- Petición típica: **GET http://www.algo.com/archivito HTTP/1.1**

Mensajes de Error

HTTP incluye un conjunto de respuestas a los errores. Estos errores se pueden mostrar por HTML como mensajes.

Transacciones HTTP

Una transacción HTTP está formada por un **encabezado** seguido, opcionalmente, por una línea en blanco y algún dato. El **encabezado especificará cosas como la acción requerida del servidor, o el tipo de dato retornado, o el código de estado.**

El uso de campos de encabezados enviados en las transacciones HTTP le da gran flexibilidad al protocolo. Estos campos permiten que se envíe información descriptiva en la transacción, permitiendo así la autenticación, cifrado e identificación de usuario.

Pasos:

- El navegador establece una conexión TCP con el servidor.
- El navegador le envía una solicitud GET.
- El servidor devuelve la cabecera describiendo el ítem.
- El servidor devuelve el ítem.
- El servidor cierra la conexión.

Conexiones Persistentes

Antes de que esta característica existiese, se necesitaba una conexión TCP separada para cada petición. Cuando un documento utilizaba enlaces a otros ficheros externos, la transmisión era extremadamente ineficiente.

HTTP en su última versión, proporciona la posibilidad de establecer sesiones de mayor duración de manera que se permiten múltiples peticiones sobre la misma conexión TCP. Esta característica llega a proporcionar en algunos casos hasta un 50 por cien de mejora en los tiempos de latencia entre documentos HTML**. Los principales beneficios al usar conexiones persistentes son:**

- **Se abren menos conexiones TCP**, lo que ahora recursos (CPU, memoria, etc.).
- **Se pueden entubar (pipeline) peticiones y respuestas en una conexión**. Esto permite al cliente hacer múltiples peticiones sin esperar a las respuestas.
- **Se reduce la latencia** en peticiones al utilizar varias veces un canal ya abierto.

Para clientes con soporte a HTTP/1.1, las conexiones son persistentes por defecto y existen métodos de envío de documentos de longitud no conocida.

Para permitir que la conexión persista a través de múltiples solicitudes-respuestas, se envía la longitud antes de cada respuesta. Si la longitud no se conoce, el servidor le informa al cliente, le envía la respuesta y luego cierra la conexión.

Ejemplo de cabecera:

```
Content-Length: 34
Content-Language: english
Content-Encoding: ascii
<HTML> A trivial example. </HTML>
```

Negociación

- La negociación puede ser iniciada por el servidor, o por el cliente.
- Los elementos se envían en la cabecera.
- Pueden especificar representaciones con valores de preferencia.

Elementos que se negocia:

```
Accept-Encoding:
Accept-Charset:
Accept-Language:
```

Métodos de petición

HTTP define 8 que indica la acción que desea que se efectúe sobre el recurso identificado. Lo que este recurso representa, si los datos pre-existentes o datos que se generan de forma dinámica, depende de la aplicación del servidor. A menudo, el recurso corresponde a un archivo o la salida de un ejecutable que residen en el servidor.

GET

Pide una representación del recurso especificado. Por seguridad no debería ser usado por aplicaciones que causen efectos ya que transmite información a través de la URI agregando parámetros a la URL.

Ejemplo:

GET /images/logo.png HTTP/1.1 obtiene un recurso llamado logo.png

Ejemplo con parámetros:

/index.php?page=main&lang=es

HEAD

Funciona como el GET, pero sin que el servidor devuelva el cuerpo del mensaje. Es decir, sólo se devuelve la información de cabecera y no muestra el cuerpo del recurso.

POST

Somete los datos a que sean procesados para el recurso identificado. Los datos se incluirán en el cuerpo de la petición. Esto puede resultar en la creación de un nuevo recurso o de las actualizaciones de los recursos existentes o ambas cosas.

Indica al servidor que se prepare para recibir información del cliente. Suele usarse para enviar información desde formularios." este tipo de método lo que hace es hacer remitir información del cliente al servidor, aparte de hacer trabajar esta función en formularios también se podría adecuar a un login o a otra información a enviar al servidor, bueno esta información cuando llega al servidor termina siendo muchas veces valor de variables para procesar información

PUT

Sube, carga o realiza un upload de un recurso especificado (archivo), es el camino más eficiente para subir archivos a un servidor, esto es porque en POST utiliza un mensaje multiparte y el mensaje es decodificado por el servidor. En contraste, el método PUT te permite escribir un archivo en una conexión socket establecida con el servidor.

La desventaja del método PUT es que los servidores de hosting compartido no lo tienen habilitado.

Ejemplo:

PUT /path/filename.html HTTP/1.1

DELETE

Solicita al servidor que borre el recurso identificado con el URL. Este método como el mismo nombre lo dice hace la ejecución de borrar un recurso en el host

TRACE

Este método solicita al servidor que envíe de vuelta en un mensaje de respuesta, en la sección del cuerpo de entidad, toda la data que reciba del mensaje de solicitud. Se utiliza con fines de comprobación y diagnóstico. Inicia un ciclo de mensajes de petición. Se usa para depuración y permite al cliente ver lo que el servidor recibe en el otro lado

OPTIONS

Devuelve los métodos HTTP que el servidor soporta para un URL específico. Esto puede ser utilizado para comprobar la funcionalidad de un servidor web mediante petición en lugar de un recurso específico.

CONNECT

Este método se reserva para uso con proxys. Permitirá que un proxy pueda dinámicamente convertirse en un túnel. Por ejemplo para comunicaciones con SSL

CRIPTOGRAFIA

En general, se definen tres propiedades de la información fundamentales que deben garantizar los sistemas informáticos: confidencialidad, integridad y disponibilidad.

Confidencialidad

Decimos que una información posee la característica de confidencialidad si sólo pueden tener acceso a la misma las entidades que están autorizadas para ello.

Integridad

La integridad garantiza que los datos almacenados en nuestro sistema —o los colocamos en un extremo de un canal de comunicaciones—, van a ser exactamente iguales cuando los recuperemos —o al llegar al otro extremo del canal—.

Disponibilidad

La información suele alcanzar su verdadero valor cuando se utiliza. En muchos casos, es crucial poder emplearla en el momento oportuno, por lo que un buen sistema de información tendrá que proporcionar una adecuada flexibilidad a la hora de acceder a los datos. A la capacidad de tener acceso a la información en todo momento la denominaremos disponibilidad

Clave Simétrica

La criptografía simétrica (en inglés symmetric key cryptography), también llamada criptografía de clave secreta (en inglés secret key cryptography), es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes.

Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

Algunos ejemplos de algoritmos simétricos son **DES, 3DES, RC5, AES, Blowfish e IDEA.**

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para transmitirse las claves? Sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

Otro problema es el número de claves que se necesitan. Si tenemos un número **n** de personas que necesitan comunicarse entre sí, se necesitan **n/2** claves para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

Clave Asimétrica

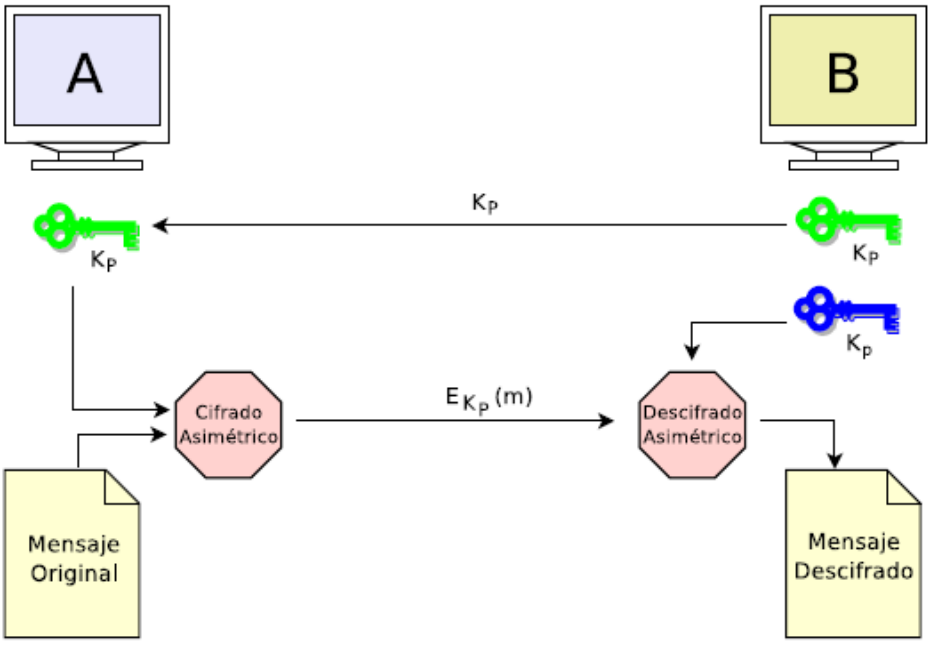
Los algoritmos asimétricos o de clave pública han demostrado su interés para ser empleados en redes de comunicación inseguras (Internet). Su novedad fundamental con respecto a la criptografía simétrica es que las claves no son únicas, sino que forman pares.

El más popular por su sencillez es RSA, que ha sobrevivido a multitud de ataques, si bien necesita una longitud de clave considerable.

Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos. Por ejemplo, mientras que para algoritmos simétricos se considera segura una clave de 128 bits, para algoritmos asimétricos se recomiendan claves de al menos 2048 bits. Además, la complejidad de cálculo que comportan estos últimos los hace considerablemente más lentos que los algoritmos de cifrado simétricos. En la práctica los métodos asimétricos se emplean únicamente para codificar la clave de sesión (simétrica) de cada mensaje o transacción particular.

Protección de la Información

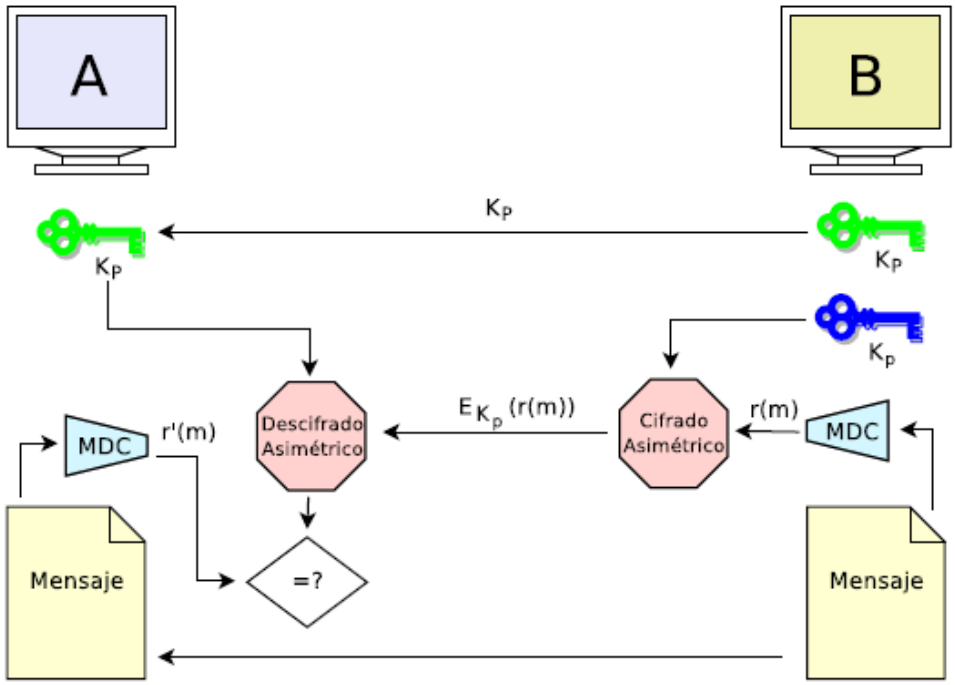
Una de las aplicaciones inmediatas de los algoritmos asimétricos es el cifrado de la información sin tener que transmitir la clave de decodificación, lo cual permite su uso en canales inseguros. Supongamos que A quiere enviar un mensaje a B (figura 12.1). Para ello solicita a B su clave pública KP. A genera entonces el mensaje cifrado EKP (m). Una vez hecho esto únicamente quien posea la clave Kp —en nuestro ejemplo, B— podrá recuperar el mensaje original m.
Nótese que para este tipo de aplicación, la clave que se hace pública es aquella que permite codificar los mensajes, mientras que la clave privada es aquella que permite descifrarlos.



Autentificación

La segunda aplicación de los algoritmos asimétricos es la autentificación de mensajes, con ayuda de funciones MDC (ver capítulo 13), que nos permiten obtener una signatura o resumen a partir de un mensaje. Dicha signatura es mucho más pequeña que el mensaje original, y es muy difícil encontrar otro mensaje diferente que dé lugar al mismo resumen. Supongamos que A recibe un mensaje de B y quiere comprobar su autenticidad. Para ello B genera un resumen del mensaje r(m) (ver figura 12.2) y lo codifica empleando la clave de cifrado, que en este caso será privada. La clave de descifrado se habrá hecho pública previamente, y debe estar en poder de A. B envía entonces a A el criptograma correspondiente a r(m). A puede ahora generar su propia r0(m) y compararla con el valor r(m) obtenido del criptograma enviado por B. Si coinciden, el mensaje será auténtico, puesto que el único que posee la clave para codificar es precisamente B.

Nótese que en este caso la clave que se emplea para cifrar es la clave privada, justo al revés que para la simple codificación de mensajes.



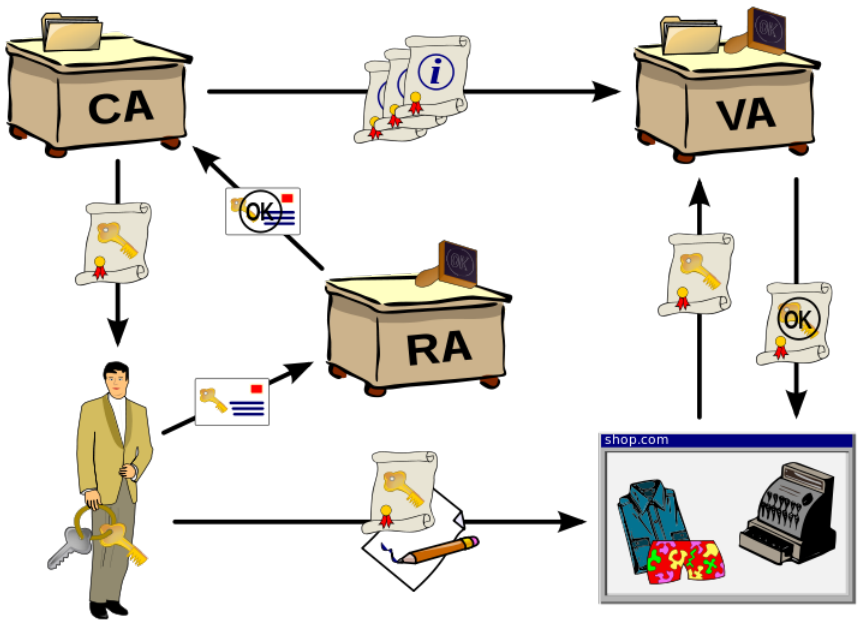
Certificados Digitales

Un certificado digital es esencialmente una clave pública y un identificador, firmados digitalmente por una autoridad de certificación, y su utilidad es demostrar que una clave pública pertenece a un usuario concreto. Evidentemente, la citada autoridad de certificación debe encargarse de verificar previamente que la clave pública es auténtica.

El formato de certificados X.509 (Recomendación X.509 de CCITT:"The Directory Autentication Framework". 1988) es uno de los más comunes y extendidos en la actualidad.
El estándar X.509 sólo define la sintaxis de los certificados, por lo que no está atado a ningún algoritmo en particular, y contempla los siguientes campos:

- Versión.
- Número de serie.
- Identificador del algoritmo empleado para la firma digital.
- Nombre del certificador.
- Periodo de validez.
- Nombre del sujeto.
- Clave pública del sujeto.
- Identificador único del certificador.
- Identificador único del sujeto.
- Extensiones.
- Firma digital de todo lo anterior generada por el certificador.

Infraestructura de clave pública (PKI)



La autoridad de certificación (CA): es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.

La autoridad de registro (RA): es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.

Los repositorios: son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados.

Lista de revocación de certificados (CRL): se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.

La autoridad de validación (VA): es la encargada de comprobar la validez de los certificados digitales.

Online Certificate Status Protocol (OCSP): es un método para determinar el estado de revocación de un certificado digital X.509 usando otros medios que no sean el uso de CRL

SSL

Características

El protocolo SSL (Secure Sockets Layer) fue diseñado con el objeto de proveer privacidad y confiabilidad a la comunicación entre dos aplicaciones.

Este se compone de dos capas:

SSL Record Protocol. Está ubicada sobre algún protocolo de transporte confiable (como por ejemplo TCP) y es usado para encapsular varios tipos de protocolos de mayor nivel.

SSL Handshake Protocol. Es uno de los posibles protocolos que pueden encapsularse sobre la capa anterior y permite al cliente y al servidor autenticarse mutuamente, negociar un algoritmo de cifrado e intercambiar llaves de acceso.

Una de las ventajas del SSL es que es independiente del protocolo de aplicación, ya que es posible ubicarlo por encima del mismo en forma transparente

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

Propiedades

Las conexiones realizadas por medio de este protocolo tienen las siguientes propiedades básicas:

Privada. Después de un proceso inicial de "handshake" en el cual se define una clave secreta, se envía la información encriptada por medio de algún método simétrico (DES, RC4).

Segura. La identidad de cada extremo es autenticada usando métodos de ciftrado asimétricos o de clave pública (RSA, DSS).

Confiable. El transporte del mensaje incluye un control de la integridad del mismo usando una MAC cifrada con SHA y MD5.

Servicios que brinda

Los servicios que brinda/n SSL/TLS son:

- Autenticación
- Confidencialidad
- Integridad
- Compresión/descompresión
- Generación y distribución de claves
- Negociación de parámetros segura.

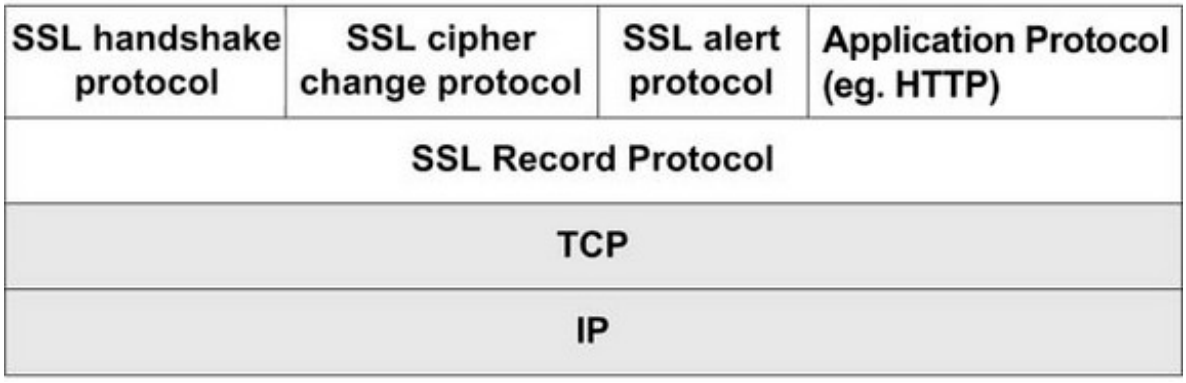
Aplicaciones

SSL se ejecuta en una capa entre los protocolos de aplicación como HTTP, SMTP, NNTP y sobre el protocolo de transporte TCP, que forma parte de la familia de protocolos TCP/IP. Aunque pueda proporcionar seguridad a cualquier protocolo que use conexiones de confianza (tal como TCP), se usa en la mayoría de los casos junto a HTTP para formar HTTPS.

TLS se puede utilizar **para proveer autenticación y encriptación** a la señalización asociada con VoIP y otras aplicaciones basadas en SIP.

Ubicación en TCP/IP

Como vemos, el protocolo SSL, proporciona seguridad entre la capa de aplicación y la capa de transporte.



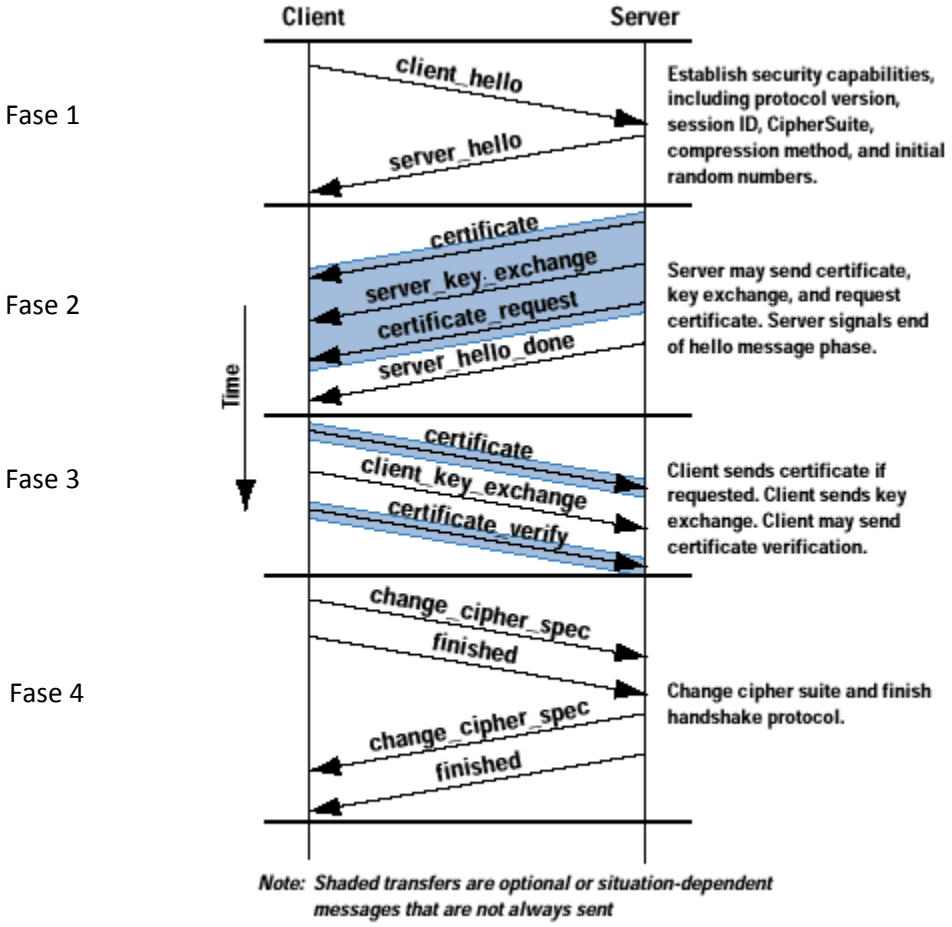
Protocolo Handshake

Se utiliza entre el cliente y el servidor básicamente para:

- Auntenticarse uno con el otro
- Negociar los algoritmos de encriptación y de MAC
- Negociar las claves criptográficas a usar

Se base en varios mensajes en fase, estas fases son:

- Establecer las capacidades de seguridad.
- Autenticación del servidor e intercambio de claves.
- Autenticación del cliente e intercambio de claves.
- Finalización.



TLS

TLS 1.0 fue definido en el RFC 2246 en enero de 1999 **y es una actualización de SSL versión 3.0**. Como dice el RFC, "**las diferencias entre este protocolo y SSL 3.0 no son dramáticas, pero son significativas en impedir la interoperabilidad entre TLS 1.0 y SSL 3.0**". TLS 1.0 incluye una forma en la cual la implementación puede conectarse en SSL 3.0, debilitando la seguridad.

Mientras que SSL y TLS difieren en forma que las hacen inoperable entre sí, por lo general se consideran iguales en términos de seguridad.

La principal diferencia es que, mientras que las conexiones SSL comienzan con la seguridad y proceder directamente a comunicaciones seguras, las conexiones TLS primero comienzan con un inseguro "hello" en el servidor y sólo cambia a comunicaciones seguras después de que el Handshake entre el cliente y el servidor se realiza correctamente. Si el protocolo de enlace TLS falla por cualquier razón, no se crea la conexión.

Ambos protocolos de seguridad de Internet aseguran que sus datos se cifra ya que se transmite a través de Internet. Ambos también le permiten estar seguro de que la comunicación es con el servidor y no con un "hombre espía medio".

Esto es posible porque los servidores que soportan SSL y TLS deben tener certificados emitidos a ellos por un tercero de confianza, como Verisign o Thawte.

Estos certificados verifican que el nombre de dominio que se emiten pertenezca realmente al servidor. El equipo emitirá advertencias si intenta conectarse a un servidor y el certificado que regresa no es de confianza o no coincide con el sitio que usted está tratando de conectarse.

SET

Transacción electrónica segura o SET (del inglés, **Secure Electronic Transaction**) es un protocolo estándar para proporcionar seguridad a una transacción con tarjeta de crédito en redes de computadoras inseguras, en especial Internet.

SET utiliza técnicas criptográficas tales como **certificados digitales y criptografía de clave pública** para permitir a las entidades llevar a cabo una autenticación entre sí y además intercambiar información de manera segura.

Requisitos

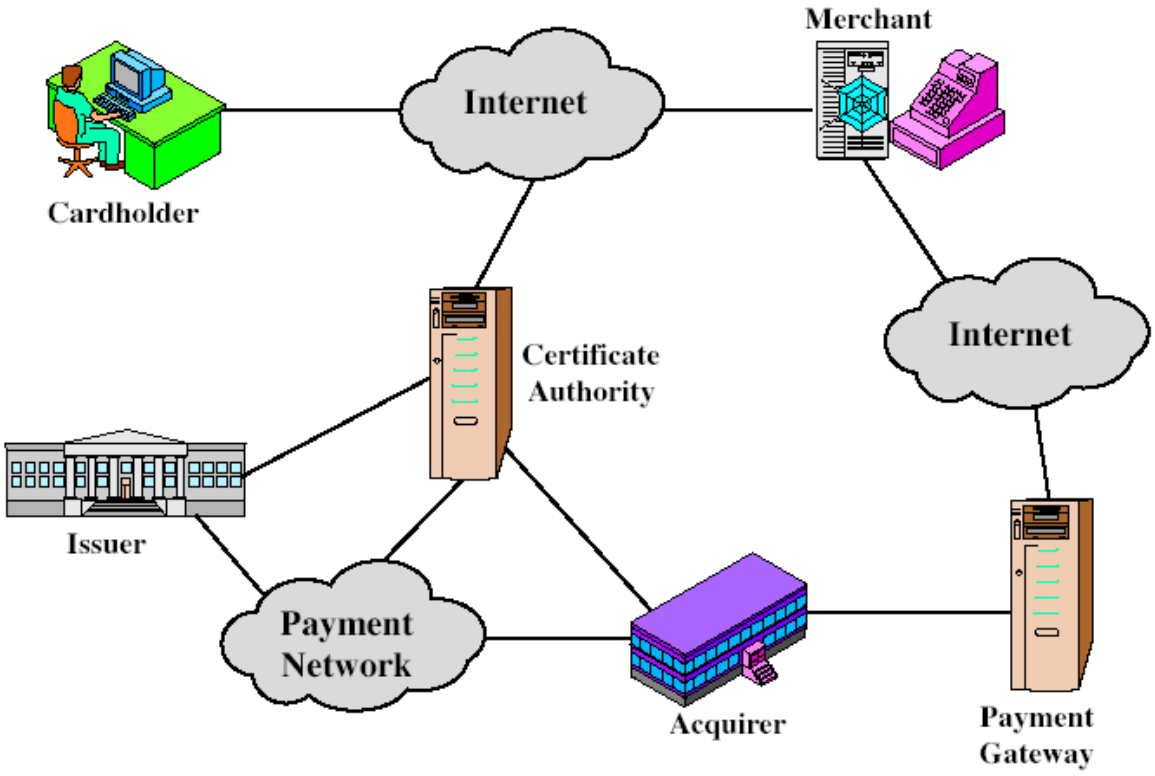
La especificación de SET enlista los siguientes requerimientos de negocio para procesamiento de pago seguro con tarjeta de crédito a través de Internet y otras redes:

- Proveer confidencialidad de pago e información de órdenes de compra
- Asegurar la integridad de la totalidad de los datos que se transmiten
- Proveer autenticación de que el portador de una tarjeta es un usuario legítimo de una cuenta de tarjeta de crédito
- Proveer autenticación de que el comerciante puede aceptar transacciones con tarjetas de crédito a través de su relación con una institución financiera
- Asegurar el uso de las mejores prácticas de seguridad y de técnicas de diseño de sistemas para proteger los involucrados legítimos en la transacción de comercio electrónico
- Crear un protocolo que no dependa de mecanismos de seguridad de transporte ni que prevenga su uso
- Facilitar y promover la interoperabilidad entre proveedores de software y redes

Entidades

El estándar SET para transacciones electrónicas seguras en redes abiertas como Internet fue desarrollado por Visa y MasterCard con la asesoría de empresas como IBM, Netscape y RSA entre otras. Está basado en la criptografía más segura, la criptografía de llaves públicas y privadas RSA. SET agrupa a las siguientes entidades en un solo sistema de pago:

- **Tarjeta habiente:** aquella persona poseedora de una tarjeta de crédito.
- **Emisor:** entidad financiera que emite la tarjeta.
- **Comerciante:** conocido en la literatura SET como el mercader, es la empresa que vende bienes o intercambia servicios por dinero.
- **Adquirente:** institución financiera que establece una cuenta con el Comerciante y procesa autorizaciones y pagos.
- **Intermediario para pago:** dispositivo operado por un adquirente o designado a un tercero para que procese los mensajes de pago, incluyendo instrucciones de pago de un tarjetahabiente.
- **Marcas:** Las instituciones financieras emiten tarjetas con marcas en ellas, para hacer publicidad a la marca y establecen ciertas reglas de uso y aceptación de sus tarjetas y proveen redes que las interconectan a las instituciones financieras.
- **Terceros:** los emisores y los adquirentes pueden asignar a terceros para el procesamiento de las transacciones.



Transacción

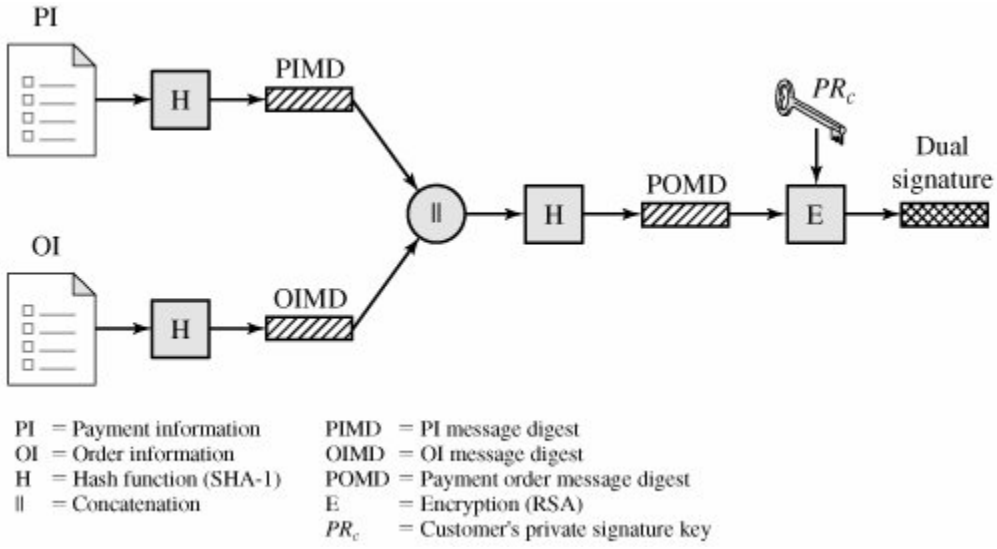
1. cliente abre cuenta
2. cliente recibe un certificado
3. los comerciantes tienen sus propios certificados
4. cliente realiza un pedido
5. se verifica comerciante
6. el orden y el pago se envían
7. comerciante de solicitudes de autorización de pago
8. comerciante confirma el pedido
9. comerciante ofrece bienes o servicios
10. comerciante solicita el pago

Dual Signature

El propósito de la **Dual Signature** es el de enlazar dos mensajes que son dirigidos a dos destinatarios diferentes.

En este caso, el comprador busca enviar la información de orden (OI) al vendedor, y la información de pago (PI) al banco. El vendedor no necesita saber el número de tarjeta de crédito del consumidor, ni el banco necesita detalles de la compra.

Sin embargo, los dos elementos deben estar vinculados de una manera que se puede utilizar para resolver los conflictos, si es necesario. El linkeo se necesita para que el cliente pueda probar que este pago está destinado para este fin y no para otros bienes o servicios



Solicitud de compra

El comerciante debe:

1 – verificar la tarjeta de crédito

2 – Verificar **la dual signature** usando la clave pública del consumidor

3 – Procesar la orden y enviar la información de pago.

4 – enviar una respuesta al titular de la tarjeta

SSH

SSH (o Secure SHell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una **arquitectura cliente/servidor** y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH **encripta la sesión de conexión**, haciendo imposible que alguien pueda obtener contraseñas no encriptadas. **Es un protocolo de capa de aplicación, el cual corre sobre TCP.**

El uso de métodos seguros para registrarse remotamente a otros sistemas reduce los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto.

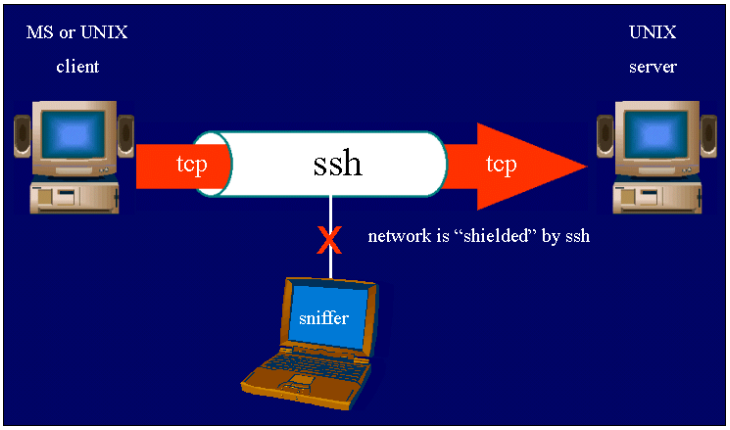
Características

El protocolo SSH proporciona los siguientes tipos de protección:

- Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.
- El cliente transmite su información de autenticación al servidor usando una encriptación robusta de 128 bits.
- Todos los datos enviados y recibidos durante la sesión se transfieren por medio de encriptación de 128 bits, lo cual los hacen extremamente difícil de descifrar y leer.
- El cliente tiene la posibilidad de reenviar aplicaciones X11 [1] desde el servidor. Esta técnica, llamada reenvío por X11, proporciona un medio seguro para usar aplicaciones gráficas sobre una red.

Seguridad

SSH trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible, evitando que terceras personas puedan descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos.



VOIP

Características

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

Los Protocolos que se usan para enviar las señales de voz sobre la red IP se conocen como protocolos de Voz sobre IP o protocolos IP. Estos pueden verse como aplicaciones comerciales de la "Red experimental de Protocolo de Voz" (1973), inventada por ARPANET.

El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo las 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 comunicar voz sobre el protocolo IP.

Telefonía sobre IP es el servicio telefónico disponible al público, por tanto con numeración E.164, realizado con tecnología de VoIP.

RTP

RSVP

Wi-fi vs Wimax

Wi-fi

Características

Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: un ordenador personal, una consola de videojuegos, un smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica. Dicho punto de acceso (o hotspot) tiene un alcance de unos 20 metros en interiores y al aire libre una distancia mayor. Pueden cubrir grandes áreas la superposición de múltiples puntos de acceso.

Ventas y desventajas

Las redes Wi-Fi poseen una serie de ventajas, entre las cuales podemos destacar:

- Al ser redes inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas porque cualquiera que tenga acceso a la red puede conectarse desde distintos puntos dentro de un rango suficientemente amplio de espacio.
- Una vez configuradas, las redes Wi-Fi permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura, no así en la tecnología por cable.
- La Wi-Fi Alliance asegura que la compatibilidad entre dispositivos con la marca Wi-Fi es total, con lo que en cualquier parte del mundo podremos utilizar la tecnología Wi-Fi con una compatibilidad total.

Pero como red inalámbrica, la tecnología Wi-Fi presenta los problemas intrínsecos de cualquier tecnología inalámbrica. Algunos de ellos son:

- Una de las desventajas que tiene el sistema Wi-Fi es una menor velocidad en comparación a una conexión con cables, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear.
- La desventaja fundamental de estas redes existe en el campo de la seguridad. Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta Wi-Fi en modo promiscuo, de forma que puedan calcular la contraseña de la red y de esta forma acceder a ella. Las claves de tipo WEP son relativamente fáciles de conseguir con este sistema. La alianza Wi-Fi arregló estos problemas sacando el estándar WPA y posteriormente WPA2, basados en el grupo de trabajo 802.11i. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad. De todos modos muchas compañías no permiten a sus empleados tener una red inalámbrica[cita requerida]. Este problema se agrava si consideramos que no se puede controlar el área de cobertura de una conexión, de manera que un receptor se puede conectar desde fuera de

la zona de recepción prevista (e.g. desde fuera de una oficina, desde una vivienda colindante).
- Hay que señalar que esta tecnología no es compatible con otros tipos de conexiones sin cables como Bluetooth, GPRS, UMTS, etc.

Seguridad y fiabilidad

Uno de los problemas a los cuales se enfrenta actualmente la tecnología Wi-Fi es la progresiva saturación del espectro radioeléctrico, debido a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad Wi-Fi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos. La mayoría de las formas son las siguientes:

- **WEP,** cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire. Este tipo de cifrado no está muy recomendado debido a las grandes vulnerabilidades que presenta ya que cualquier cracker puede conseguir sacar la clave, incluso aunque esté bien configurado y la clave utilizada sea compleja.
- **WPA**: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como dígitos alfanuméricos.
- **IPSEC** (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.
- **Filtrado de MAC**, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados. Es lo más recomendable si solo se va a usar con los mismos equipos, y si son pocos.
- **Ocultación del punto de acceso**: se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios.
- **WPA2** (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles, ya que los antiguos no lo son.

Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

WiMAX

Características

WiMAX, siglas de Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas), es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2,3 a 3,5 GHz y puede tener una cobertura de hasta 60 km.

Actualmente se recogen dentro del estándar 802.16. Existen dos variantes:

- **Uno de acceso fijo (802.16d),** en el que se establece un enlace radio entre la estación base y un equipo de usuario situado en el domicilio del usuario. Para el entorno fijo, las velocidades teóricas máximas que se pueden obtener son de 70 Mbit/s con un ancho de banda de 20 MHz. Sin embargo, en entornos reales se han conseguido velocidades de 20 Mbit/s con radios de célula de hasta 6 km, ancho de banda que es compartido por todos los usuarios de la célula.
- **Otro de movilidad completa (802.16e),** que permite el desplazamiento del usuario de un modo similar al que se puede dar en GSM/UMTS, el móvil, aun no se encuentra desarrollado y actualmente compite con las tecnologías LTE (basadas en femtocélulas, conectadas mediante cable), por ser la alternativa para las operadoras de telecomunicaciones que apuestan por los servicios en movilidad, este estándar, en su variante «no licenciado», compite con el WiFi IEEE 802.11n, ya que la mayoría de los portátiles y dispositivos móviles, empiezan a estar dotados de este tipo de conectividad (principalmente de la firma Intel).

Propiedades

- Distancias de hasta 80 kilómetros, con antenas muy direccionales y de alta ganancia.
- Velocidades de hasta 75 Mbit/s, 35+35 Mbit/s, siempre que el espectro esté completamente limpio.
- Facilidades para añadir más canales, dependiendo de la regulación de cada país.
- Anchos de banda configurables y no cerrados, sujetos a la relación de espectro.
- Permite dividir el canal de comunicación en pequeñas subportadoras (dos tipos: guardias y datos).

Comparación de tecnologías

Ventajas de WiMax por sobre el Wi-Fi:
* Mayor alcance de cobertura
* Mayor velocidad de conexión

Mientras que la **cobertura** en un sistema tipo Wi-Fi va de los 50 a los 100 metros, con la tecnología WiMax se alcanza de 40 a 100 kilómetros. Esto permite extender el alcance de Internet inalámbrico a situaciones geográficas donde es complicado o imposible realizar un cableado convencional.

Con respecto a **la velocidad de conexión**, mientras que con Wi-Fi se tiene una velocidad teórica de 56 Mbps como velocidad máxima (con el estándar actual más difundido), la tecnología WiMax alcanza 128 Mbps de velocidad teórica.

Junto con estos 2 puntos se encuentra el mayor **ancho de banda**, lo que permite transmitir para varios equipos o estaciones conectadas y ejecutando más de un servicio en forma simultánea, como ser Telefonía IP, transmisión de video, imágenes, audio, etc.

Aunque este sistema de conexión todavía se encuentre en desarrollo (el principal escollo aparenta ser la estandarización y certificación de los equipos), seguramente será un gran salto con innumerables beneficios; quizás el más importante sería tener acceso en tiempo real a la información necesaria en situaciones límites donde se vea comprometida la vida, como ser rescates en zonas muy complicadas o también cubrir toda un área de una ciudad permitiendo tener conexión continua a Internet.

Conclusión

WiMAX y Wi-fi son soluciones complementarias para aplicaciones bastantes diferentes. WiMAX fue diseñada para redes metropolitanas (MAN). Wi-fi fue diseñada para redes de área local (LAN).