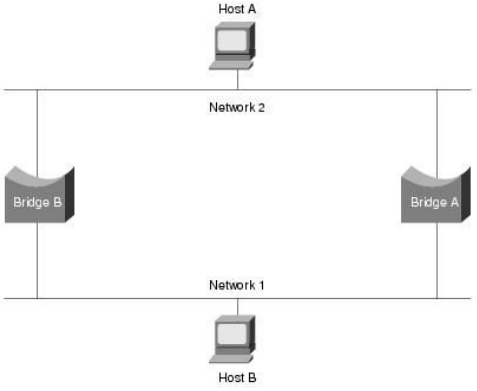
Transparent Bridging Operation (Operación de puenteado transparente)

Los puentes transparentes se denominan así porque su presencia y operación son transparentes para los hosts de la red. Cuando se activan puentes transparentes, aprenden las ubicaciones de la estación de trabajo analizando la dirección de origen de las tramas entrantes de todas las redes conectadas. Por ejemplo, si un puente ve una trama que llega al puerto 1 desde el Host A, el puente concluye que el Host A puede ser alcanzado a través del segmento conectado al puerto 1. A través de este proceso, los puentes transparentes construyen una tabla (el proceso de aprendizaje).
El puente utiliza su tabla como base para el reenvío de tráfico. Cuando se recibe una trama en una de las interfaces del puente, el puente busca la dirección de destino de la trama en su tabla interna. Si la tabla contiene una asociación entre la dirección de destino y cualquiera de los puertos del puente aparte de aquél en el que se recibió la trama, se remite la misma al puerto indicado. Si no se encuentra ninguna asociación, la trama se envía a todos los hosts (provoca inundación) excepto en el puerto de entrada.
Los puentes transparentes aíslan el tráfico con éxito, reduciendo así el tráfico visto en cada segmento individual. Esto se denomina filtrado y ocurre cuando las direcciones MAC de origen y destino residen en la misma interfaz de puente.
El filtrado por lo general mejora los tiempos de respuesta de la red, según lo visto por el usuario.

Bridging Loops (bucles de puente)

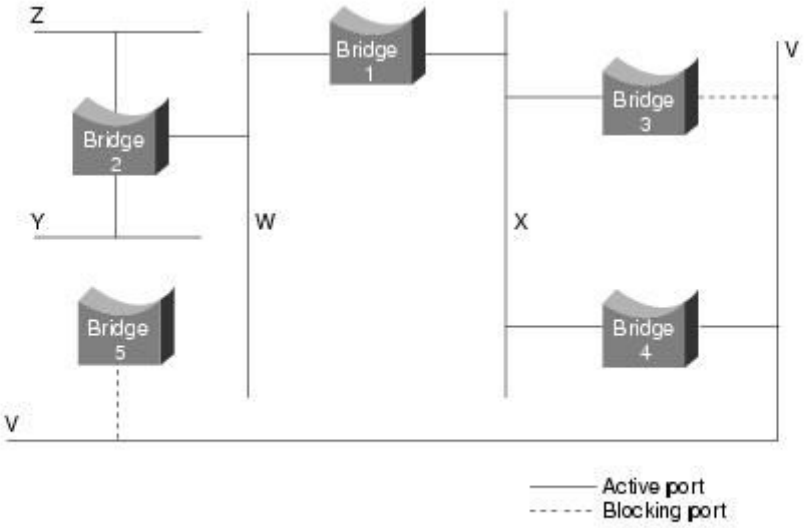


Sin un protocolo puente-a-puente (bridge-to-bridge), el algoritmo de puente transparente falla cuando existen múltiples rutas de puentes y redes de área local (LANs) entre dos LANs cualesquiera de la red. Figura: Bridging Loops puede resultar en reenvío y aprendizaje inexactos en entornos de puentes transparentes.
Supongamos que el Host A envía una trama al Host B. Ambos puentes reciben la trama y aprenden correctamente que el Host A está en el segmento 2. Cada puente reenvía la trama al segmento 1. Lamentablemente, no sólo el Host B recibirá dos copias de la trama (una vez desde el puente 1 y una vez desde el puente 2), sino que además cada puente cree que el Host A reside en el mismo segmento que el Host B. Cuando el Host B responde la trama del Host A, ambos puentes recibirán y posteriormente filtraran las respuestas porque el puente-tabla indicará que el destino (Host A) está en el mismo segmento de red que el origen de la trama.
Además de los problemas básicos de conectividad, la proliferación de mensajes de difusión en redes con bucles representa un problema de red potencialmente serio. Suponga que la trama inicial del Host A es una emisión. Ambos puentes remiten las tramas sin fin, utilizando todo el ancho de banda de red disponible y bloqueando la transmisión de otros paquetes en ambos segmentos.
Un bucle implica la existencia de múltiples rutas de acceso a través de la red interna y una red con múltiples rutas de origen a destino puede aumentar la tolerancia a fallos de red general a través de una mejor flexibilidad topológica.

Algoritmo Spanning-Tree (STA)

Se desarrolló el algoritmo spanning-tree (STA) para preservar los beneficios de los bucles y eliminar sus problemas.
El STA designa un subconjunto sin bucle de la topología de la red colocando los puertos puente que, si estaban activos, crearían bucles en una condición de reserva (bloqueo). Pueden activarse los puertos de puente de bloqueo en caso de un fallo de enlace primario, proporcionando una nueva ruta a través de la red interna.
El STA utiliza una conclusión de la teoría de los gráficos como base para construir un subconjunto sin bucles de la topología de la red. La teoría de los gráficos dice lo siguiente: Para cualquier grafo conectado que

consista en nodos y bordes que conectan pares de nodos, un árbol de expansión (spanning-tree) de bordes mantiene la conectividad del gráfico pero no contiene bucles.
El STA pide que se asigne a cada puente un identificador único. Normalmente, este identificador es una de las direcciones de control de acceso al medio (MAC) del puente, más una prioridad asignada administrativamente. A cada puerto de cada puente se le asigna un identificador único (dentro de ese puente), que es típicamente su propia dirección MAC. Finalmente, cada puerto de cada puente está asociado con un coste de trayectoria, que representa el costo de transmitir una trama a una LAN a través de ese puerto. Los costos de ruta suelen ser predeterminados pero pueden ser asignados manualmente por los administradores de red.
La primera actividad del spanning-tree es la selección del puente raíz, que es el puente con el identificador de puente de menor valor. A continuación, se determina el puerto raíz en todos los demás puentes. El puerto raíz de un puente es el puerto a través del cual se puede alcanzar el puente raíz con el coste de ruta de acceso mínimo, un valor que se denomina coste de la ruta raíz.
Finalmente, se determinan los puentes designados y sus puertos designados. Un puente designado es el puente en cada LAN que proporciona el coste mínimo de la trayectoria de la raíz. El puente designado de una LAN es el único puente permitido para reenviar tramas hacia y desde la LAN para la cual es el puente designado. El puerto designado por una LAN es el puerto que lo conecta al puente designado.



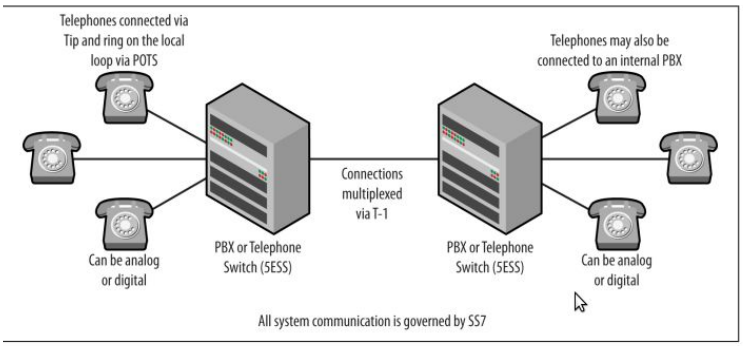
Utilizando este proceso, todos menos uno de los puentes directamente conectados a cada LAN son eliminados, eliminando así todos los bucles de dos LAN. El STA también elimina los bucles que implican más de dos LAN, mientras que todavía preserva la conectividad.
Los estados en los que puede estar un puerto son los siguientes:

- Bloqueo: En este estado se pueden recibir BPDU's pero no las enviará. Las tramas de datos se descartan y no se actualizan las tablas de direcciones MAC (mac-address-table). Los switch comienzan en este estado ya que si realizan envíos (forwarding) podrían estar generando un loop o bucle.
- Escucha: A este estado se llega desde *Bloqueo*. En este estado, los switches determinan si existe alguna otra ruta hacia el puente raíz. En el caso que la nueva ruta tenga un coste mayor, se vuelve al estado de Bloqueo. Las tramas de datos se descartan y no se actualiza la tabla de direcciones MAC (mac-address-table). Se procesan las BPDU.
- Aprendizaje: A este estado se llega desde *Escucha*. Las tramas de datos se descartan pero ya se actualizan las tablas de direcciones MAC (aquí es donde se aprenden por primera vez). Se procesan las BPDU.
- Envío: A este estado se llega desde *Aprendizaje*, en este estado el puerto puede enviar y recibir datos. Las tramas de datos se envían y se actualizan las tablas de direcciones MAC (mac-address-table). Se procesan las BPDU.
- Desactivado: A este estado se llega desde cualquier otro. Se produce cuando un administrador deshabilita el puerto o éste falla. No se procesan las BPDU.

VoIP

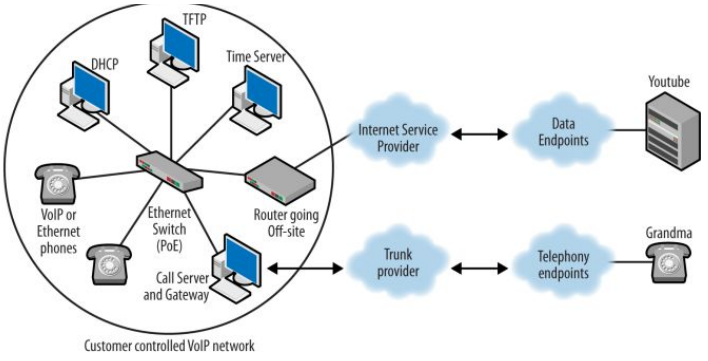
VoIP está enviando voz (y vídeo) a través de una red basada en IP.

Estas señales se envían entre los dispositivos como la central privada (PBX) antes de que pueda producirse cualquier comunicación humana.
VoIP toma todos estos mensajes de señalización y los coloca dentro de los paquetes IP.
El nombre de PBX se conserva, aunque ahora se llama IP PBX, lo que realmente significa que es un servidor que se ejecuta en una computadora.
También vale la pena mencionar que, dado que el Protocolo de Internet puede y funciona sobre casi todos los tipos de arquitectura de comunicación de bajo nivel, la Voz sobre IP también puede hacerlo.
VoIP usa el Protocolo TCP / IP.



Probablemente la mayor razón para adoptar una arquitectura basada en VoIP es el dinero. En lugar de pagar por una serie de líneas telefónicas o circuitos, los clientes sólo necesitan pagar por una conexión de datos. Esto se debe a que el tráfico VoIP viaja en paquetes IP que pueden compartir la conexión de datos. Además, los paquetes IP pueden fluir a cualquier destino conectado a Internet, y las tarifas de peaje se reducen mucho. Las redes que despliegan VoIP a menudo se llaman redes convergentes porque comparten la red de datos. Una vez que la red de datos está instalada, todos los demás dispositivos están conectados a ella. Softphones (software del teléfono que se ejecuta en un ordenador portátil o dispositivo de mano) puede ser mucho menos costoso y más fácil de manejar.

El lado izquierdo de la figura es la red interna, que alberga los servidores utilizados para soportar los nodos VoIP y los propios teléfonos VoIP. La empresa está conectada al mundo exterior a través del proveedor de servicios de Internet, o ISP. Antes de VoIP, una compañía también poseía una red de voz separada, y éstas estarían conectadas al LEC (local site carrier) para proporcionar conectividad a los puntos finales de telefonía. Los puntos finales de VoIP también tienen que estar conectados a los puntos finales de telefonía en el exterior. La señalización de tráfico fluye desde el servidor de llamadas interno y el gateway al gateway externo.



Servidor de llamadas
Los teléfonos se registran en el servidor de llamadas. El servidor de llamadas puede controlar la seguridad y el control de admisión mientras conecta los teléfonos. Los datos de voz para la llamada, normalmente transportados por el protocolo de transporte, pueden o no fluir a través del servidor de llamadas.
Gateway
Este dispositivo se suele utilizar para conectar una red interna al resto del mundo, o al menos un sistema diferente. El sistema al que se está conectando puede ser una tecnología diferente o la misma. El gateway conectará terminales a cada lado, traducirá entre los dos sistemas o proporcionará características. Por otro lado, un gateway puede simplemente conectar empresas o proveedores juntos. En este caso, los grupos interconectados pueden estar ejecutando el mismo protocolo de señalización.
Protocolos VoIP
Existen dos tipos de protocolos VoIP: señalización y transporte. Los protocolos de señalización se ocupan de todas las funciones realizadas por los protocolos tradicionales, como la Red Digital de Servicios Integrados. El protocolo de transporte se utiliza para encapsular o transportar los datos de voz reales, y el único

protocolo utilizado universalmente para el transporte es el protocolo de transporte en tiempo real (RTP). Los paquetes de datos de voz se crean con un códec y luego se encapsulan dentro de RTP.

Codecs

Esto es corto para un codificador-decodificador usado con el propósito de convertir la señal de voz analógica a una serie de muestras digitales en la fuente y luego de nuevo en el receptor. Para un sistema tradicional, el códec puede ubicarse físicamente en el teléfono o en la PBX, dependiendo del tipo y el modelo. Los teléfonos VoIP siempre contienen el códec. Los codecs también pueden comprimir los datos de voz.

Teléfonos de escritorio y softphones

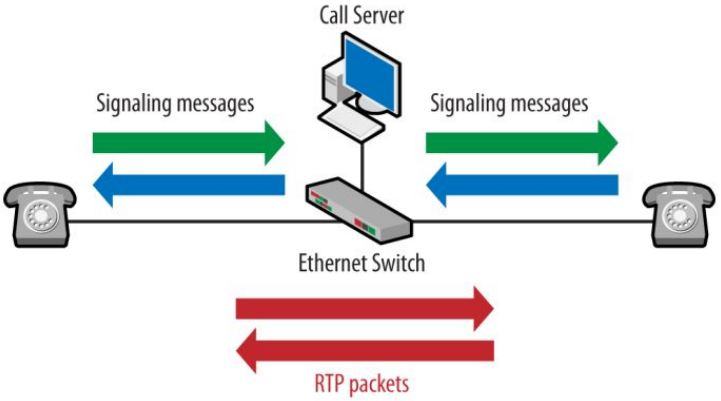
Los teléfonos (también conocidos como puntos finales) en una topología VoIP realizan el mismo servicio que cualquier otro teléfono, aunque de una manera diferente.

Componentes no VoIP

El sistema VoIP depende de una serie de servicios que no son específicos de VoIP. Muchos de los servicios, como el Protocolo de configuración de host dinámico (DHCP), ya forman parte de la arquitectura de red y pueden ampliarse para incluir los componentes de VoIP. Otros servicios incluyen Protocolo Trivial de Transferencia de Archivos (TFTP), Servicio de Nombres de Dominio (DNS), y Network Time Protocol, o NTP.

PROTOCOLO VOIP

Los protocolos de señalización manejan las funciones derivadas de la arquitectura del sistema telefónico y los protocolos de transporte llevan los paquetes de voz generados desde el códec. Una vez que se ha establecido una llamada, los paquetes de datos de voz normalmente se envían directamente entre los teléfonos que utilizan encapsulación RTP, aunque existen excepciones. Los paquetes RTP que transportan los datos de voz también pueden fluir desde el teléfono al servidor de llamadas y luego al otro teléfono.



Protocolos de señalización

Protocolo de Iniciación de Sesión:

El formato de los mensajes SIP es muy similar al de los paquetes HTTP (Hypertext Transfer Protocol), por lo que es muy familiar para las personas en el mundo de las redes de datos. SIP tuvo un comienzo lento, pero ha tomado en gran medida el mundo.

```
Internet Protocol Version 4, Src: 10.210.200.111 (10.210.200.111), Dst: 10.210.200.112
Transmission Control Protocol, Src Port: sip (5060), Dst Port: sip (5060), Seq: 1, Ack:
Session Initiation Protocol
⊟ Status-Line: SIP/2.0 180 Ringing
    Status-Code: 180
    [Resent Packet: False]
⊟ Message Header
  ⊞ v: SIP/2.0/TCP 10.210.200.112:5060;branch=z9hG4bK2965924072-14
  ⊞ f: <sip:10.210.200.112>;epid=10021002000112;tag=plcm_2965924072-15
  ⊞ t: <sip:10.210.200.111>;tag=plcm_1663913224-7
    i: 2965924072-13
  ⊞ CSeq: 1 INVITE
    k: timer
  ⊞ m: <sip:10.210.200.111:5060;transport=tcp>
    User-Agent: Polycom ViaVideo Release 8.0
    l: 0
```

Podemos ver que el paquete es fácil de leer, tiene un propósito obvio, y las partes involucradas están claramente definidas. Estas características y la integración con muchas formas de direccionamiento son algunas de las razones de la popularidad del protocolo.

-- Componentes:

-- User Agent

-- Register Server

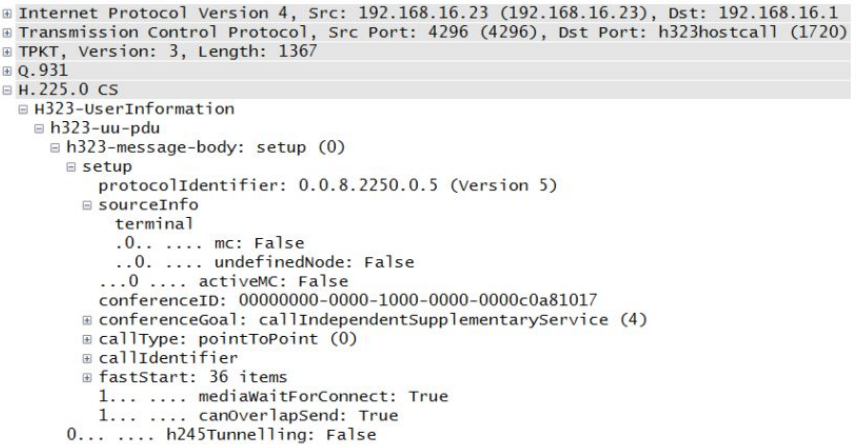
-- Proxy Server

-- Redirect Server

Estructura de Mensajes (Request)
Los métodos funcionales son los siguientes:

- ❖ REGISTER, registra información de contacto. Utilizado por el agente de usuario contra el servidor de registro.
- ❖ INVITE, ACK, CANCEL, para hacer la llamada.
- ❖ BYE, terminar la llamada.
- ❖ OPTIONS, saber capacidades del otro.

H.323



Este es en realidad un conjunto de estándares ITU-T que se centra en la videoconferencia. Utiliza muchas de las ideas de señalización de la telefonía tradicional, y algunos podrían decir que sufre como resultado de los antecedentes correspondiente. Examinando el paquete en la figura, no tenemos que ir muy lejos para ver el número de subcapas y campos involucrados. Dentro del paquete TCP hay tres subcapas antes de llegar a la información del mensaje real. Un poco más adelante está la sección "fastStart", que tiene 36 elementos. Esta complejidad podría ser una de las razones de su declinante popularidad. Sin embargo, algunos expertos de VoIP señalan que la complejidad SIP puede aumentar dependiendo de los puntos finales y sus capacidades.

-- Componentes:

-- Terminales: los teléfonos o software involucrados.

-- GateKeeper: Autoridad de registro.

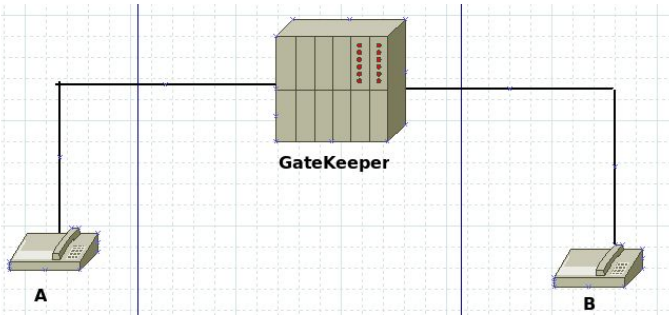
-- Multipoint Control Unit: replicador de streaming para hacer multiconferencias. Multiplica la señal.

PROTOCOLO DE TRANSPORTE
El protocolo de transporte en tiempo real (RTP) es el favorito para el transporte de paquetes de voz . RTP es un protocolo simple que utiliza identificadores de origen para recopilar paquetes de la misma fuente y tiene un campo que identifica la carga útil para que el receptor pueda determinar qué códec se utiliza para crear el paquete de voz.
El paquete RTP proporciona una indicación del códec utilizado para crear el paquete de voz, el identificador de fuente y los datos en sí.
Provee:

- Identificación del tipo de carga
- Número de secuencia para que el extremo receptor pueda hacer el reordenamiento ya que se emplea UDP.
- Marcas de tiempo para sincronizar el audio que está llegando en el tiempo.
- Monitoreo de entregas (sobre TCP)

Operación básica VoIP
Un servidor TFTP se utiliza para actualizar el firmware utilizado por el teléfono y tal vez proporcionar un archivo de configuración que puede contener parámetros operativos para la red VoIP. Sin embargo, los

servidores TFTP también se utilizan para proporcionar archivos que describen códigos o tonos utilizados en una región en particular.



1. Antes de que se estableciera la conexión A y B tuvieron que hacer un registro hacia el GateKeeper.
2. Cuando A quiera llamar a B envía un mensaje solicitando al gatekeeper informando que quiere hacer una llamada y éste le da su confirmación. También le informa a A la dirección IP de B
3. A envía un mensaje H.323 con el SETUP de conexión.
4. B le contesta a A diciéndole que esta procesando.
5. B verifica contra el gatekeeper si hay una autorización para que A lo llame.
6. Si la confirmación es válida entonces el teléfono suena y le manda a A un ALERT avisando que está sonando.
7. Cuando se levanta el tubo, ahí le envía el mensaje H.323 CONNECT

Registro del teléfono
Antes de que un terminal de VoIP pueda realizar una llamada, primero debe registrarse con el servidor de llamadas, o portero. El registro ocurre a través del protocolo de señalización, y cada protocolo de señalización utiliza un conjunto de mensajes ligeramente diferente para realizar la tarea.

Configuración y conexión de llamadas
En una red tradicional, al levantar el receptor se cierra un circuito en preparación para la señal de voz. Los usuarios marcan números, creando tonos que se envían al interruptor telefónico. El conmutador convierte los tonos en información digital a través del códec. Los conmutadores deben establecer un circuito de extremo a extremo hacia el destino. El protocolo de señalización VoIP envía mensajes al servidor de llamadas, indicando el número marcado, y el servidor de llamadas debe ponerse en contacto con el destino.

Conversación RTP
RTP se utiliza para transmitir datos de voz. Una vez que los paquetes RTP están fluyendo, se ha establecido la llamada. Sin embargo, RTP también se puede utilizar para transmitir muestras creadas para otros sonidos. El paquete RTP contiene un ID de carga útil que indica el códec utilizado. Cuando el usuario final habla en el auricular, el códec toma la voz analógica y crea los paquetes de voz enviados en el flujo RTP. Las implementaciones SIP también utilizan RTP.

Terminación de llamada
En la mayoría de las implementaciones de VoIP, cada intento de facilitar una desconexión graciosa se hace. Esto garantiza que el canal o la sesión se cierre, que se recuperen los recursos,
Se determina, y no se aceptan otros datos de conexión para ese ID de llamada.

ARQUITECTURA VOIP

- Señalización: se encuentra la localización de los dispositivos (ubicación del destino), el establecimiento de la llamada y su finalización y, las características de la sesión (audio, video, calidad, formatos, etc).

- Transmisión: Encapsulamiento de datos de audio (y video) junto con la segmentación del mismo. Cuando se transmite, se le agrega una marca de agua o un identificador.
- Soporte: Autoconfiguración del servicio, calidad del servicio. Autenticación, autorización y estadísticas entre dominios (no cualquiera puede aplicar las prioridades).

SEGURIDAD EN REDES

-- Arquitectura de Seguridad:

Ataque a la seguridad: (Security attack): Cualquier acción que comprometa la seguridad de la información perteneciente a una organización.
Mecanismo de seguridad (Security mechanism): Un proceso (o un dispositivo que incorpora dicho proceso) que tiene por objetivo detectar, prevenir o restaurar un ataque a la seguridad. (cifrado, firma digital, control de acceso, control de ruteo, padding de tráfico, etc.)
Servicio de seguridad (Security service): Un proceso o servicio de comunicación que realza la seguridad de los sistemas de procesamiento de datos y de las transferencias de información de una organización. Los servicios buscan contrarrestar los ataques a la seguridad, y pueden valerse de uno o más mecanismos de seguridad para proveerlo.

-- Servicios de Seguridad

Confidencialidad: La información que circula por la red solo puede ser accedida (leída) por las partes autorizadas.
Autenticación: Asegurar la identidad del emisor, y que esta no es falsa.
Integridad: La información debe llegar a destino sin modificaciones.
Disponibilidad: Los recursos deben estar disponibles para las partes autorizadas.
Control de acceso: Determinar los recursos que son accesibles por el usuario
No repudio: El transmisor y/o receptor de un mensaje no pueden negarlo.

-- Impacto potencial

Bajo: ante la pérdida de confidencialidad, integridad o disponibilidad puede esperarse que tenga un efecto adverso limitado en las operaciones de la organización, sus recursos o individuos
Moderado: ante la pérdida de confidencialidad, integridad o disponibilidad puede esperarse que tenga un efecto adverso serio en las operaciones de la organización, sus recursos o individuos
Alto: ante la pérdida de confidencialidad, integridad o disponibilidad puede esperarse que tenga un efecto adverso severo o catastrófico en las operaciones de la organización, sus recursos o individuos

-- Ataques

Interrupción: La información nunca llegará a su destino (disponibilidad).
Intercepción: El destino recibe la información enviada por el origen, pero ésa ha sido interceptada por un tercero (confidencialidad).
Generación: El intruso genera y envía la información al destino haciéndose pasar por el origen real (autenticación).
Modificación: La información enviada por el origen es interceptada por el atacante, modificada y reenviada al destino (integridad).

-- Intrusos

Intruso pasivo: Es aquél que accede a recursos e información que se suponen confidenciales sin realizar ninguna acción sobre ellos, es decir, visualiza datos de archivos, BD, o monitoriza el tráfico de una red determinada.
Intruso activo: Es el que modifica archivos, BD, o reenvía deliberadamente la información que es capaz de capturar. Además, es capaz de generar nuevos datos/mensajes.

-- Seguridad por

Profundidad: Implementar mecanismos de seguridad a distintos niveles:Hardware, Software, Mantenimiento y Actualización, Revisión de procesos.

Diseño: Desde la concepción de un sistema debe tenerse en cuenta la seguridad.

Transparencia: Evitar basarse en secretos, utilizando algoritmos y mecanismos bien evaluados.

-- Políticas de seguridad

Paranoica: todo está prohibido, aun aquello que debería estar permitido; como si no hubiera interconexión.

Prudente: todo está prohibido, excepto aquello que se permita de manera explícita.

Permisiva: todo está permitido, excepto aquello que se prohíba de manera explícita.

Promiscua: se permite todo, aun aquello que debería prohibirse.

-- Cortafuegos (Firewalls)

Un cortafuegos es un medio que sirve para regular el tráfico entre redes. (Por ej. el tráfico entrante y saliente entre la red de computadoras de una organización e Internet) .

Consulta la información identificativa asociada a cada mensaje entrante y saliente. La información mínima que un cortafuegos obtiene normalmente de un paquete IP es: dirección IP origen, dirección IP destino, puerto origen, puerto destino y protocolo utilizado (TCP o UDP).

Permite o no la comunicación de acuerdo a una política de seguridad que ha sido configurada previamente por un administrador. Implementadas mediante Listas de Control de acceso, las cuales tinen la siguiente lógica:

- ➔ Si el paquete viene por la red X, entonces dejar pasar.
- ➔ Si el paquete viene por la red Y, entonces no dejar pasar.

Servicios estándar

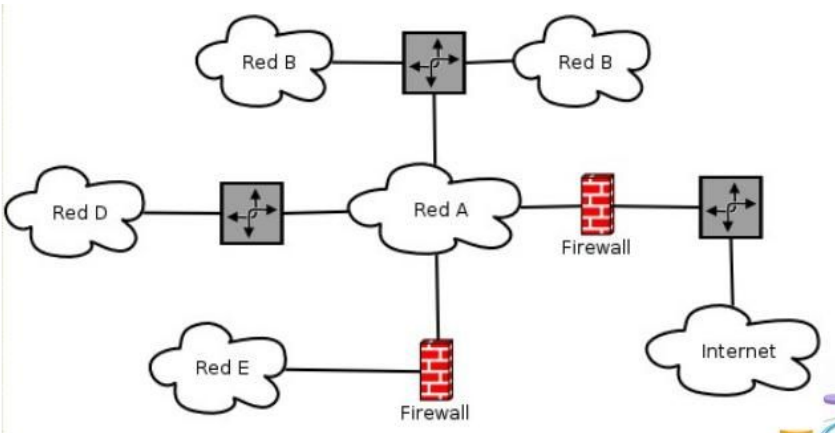
Control de acceso: Este servicio lo consigue obteniendo tanta información como sea posible de los paquetes que pasan por el. Con esta información y con una política de seguridad determina si autoriza o no el paso de un paquete hacia/desde la intranet. La política de un buen cortafuegos es denegar cualquier acceso no autorizado explícitamente.

Registro de actividades: Un cortafuegos registra todas las actividades, autorizadas y denegadas, que lo atraviesan. Este registro es una herramienta muy valiosa para supervisar la actividad de un intruso para averiguar las áreas susceptibles de haber sido dañadas, e incluso para identificarlo (y posiblemente atraparlo).

Tipos

Filtro de paquetes: Analizan los encabezados de los paquetes IP y de acuerdo a una política de seguridad definida por el administrador se desechará dicho paquete o no (implementada como ACLs).

Gateways a nivel aplicación: Los gateways impiden el paso directo de los paquetes de una red a otra, obligando que la conexión se haga a una aplicación específica denominada proxy que se encuentra en el cortafuegos.



SISTEMA DE CONTROL DE INTRUSOS (IDS)

Un Sistema de detección de intrusiones (IDS) busca identificar patrones que puedan indicar un ataque, ya sea a la red o a sistemas en particular .Un IDS identifica ataques una vez que éstos están en proceso, o que ya ocurrieron. (No previene).
Puede implementarse de tal manera que es posible analizar también el tráfico generado dentro del perímetro que se busca asegurar (Detección de ataques internos).
Puede generar alertas e interactuar con firewalls para contener un ataque en proceso.

> *Forma de operación:* Analizando la información que recolecta y comparándola con una base de datos que contiene firmas (signaturas) de ataques conocidos.
> Buscando "anormalidades" en el patrón de tráfico que analiza, tomando como referencia parámetros definidos por el administrador tal como volumen de tráfico normal, picos, tamaño de paquetes, protocolos, etc.

SISTEMAS DE PREVENCIÓN DE INTRUSOS (IPS)

Se denomina Sistema de Prevención de Intrusiones (IPS) a los dispositivos de red especializados que al igual que los IDSs monitorean el tráfico tratando de identificar posibles ataques, pero que actúan “en el medio” y activamente intentan prevenir o bloquear dichos ataques. Operan utilizando signaturas y/o análisis estadístico.

> *Posibles acciones*: Generar alarmas, descartar paquetes maliciosos, bloquear todo el tráfico desde determinada dirección IP, resetear conexión TCP.

Sistemas Criptográficos: Clasificación

Por tipo de operaciones usadas para transformar el texto plano en texto cifrado:

> *Sustitución:* cada elemento del texto plano (bit, letra) se mapea a otro elemento.
> *Transposición:* los elementos del texto plano son reacomodados.

Por el número de claves utilizadas:

> *Simétricos:* emisor y receptor utilizan la misma clave. También se los suele denominar como de una clave, de clave secreta o cifrado convencional.
> *Asimétricos:* Emisor y receptor utilizan claves diferentes. Denominados también de doble clave, o cifrado de clave pública

Por la forma en que el texto plano es procesado:

> *Cifrado por bloque*: procesa un bloque de elementos por vez, produciendo un bloque de salida por cada bloque de entrada.
> *Cifrado continuo (stream)*:Procesa los elementos de manera continua, produciendo un elemento de salida por vez, a medida que se va alimentando

Esteganografía

Estudia los procedimientos encaminados a ocultar la existencia de un mensaje en lugar de ocultar su contenido. El objetivo de la esteganografía es ocultar el mensaje dentro de otro sin información importante, de forma que el atacante ni siquiera se entere de la existencia de dicha información oculta.
No se trata de sustituir al cifrado convencional sino de complementarlo: ocultar un mensaje reduce las posibilidades de que sea descubierto; no obstante, si lo es, el que ese mensaje haya sido cifrado introduce un nivel adicional de seguridad.

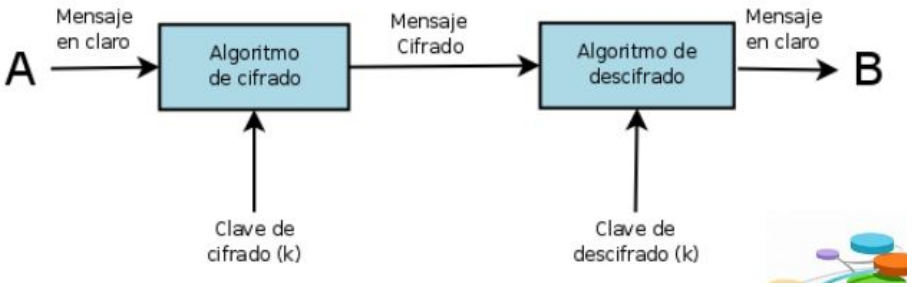
Cifrado por sustitución "Algoritmo de César"
Se realiza siempre la misma sustitución: 1ª letra por 4ª; 2ª letra por 5ª; 3ª letra por 6ª... Es decir, la A en el mensaje original pasaría a ser la D en el mensaje cifrado. La expresión matemática de este algoritmo es: C = (m + 3) mod L
donde C es el mensaje cifrado, m es el manaja en claro, 3 sería la contraseña (que no es tal), L es el número de letras del alfabeto en cuestión. Esta expresión supone que cada letra esta asociada a un número (A=0, B=1, p. ej.)
Cifrado por sustitución "Cifrado de Vigenère"
Este es un ejemplo de cifrado polialfabético (la sustitución aplicable a cada carácter varía en función de la posición que ocupe en el mensaje en claro), en el que la clave es un secuencia de símbolos (una palabra; K = {k0, k1, ... , kd-1).

Cifrado por transposición
Otra técnica de cifrado consiste, en vez de sustituir símbolos, en realizar permutaciones, es decir, cambiar su lugar. (ubicación, orden).

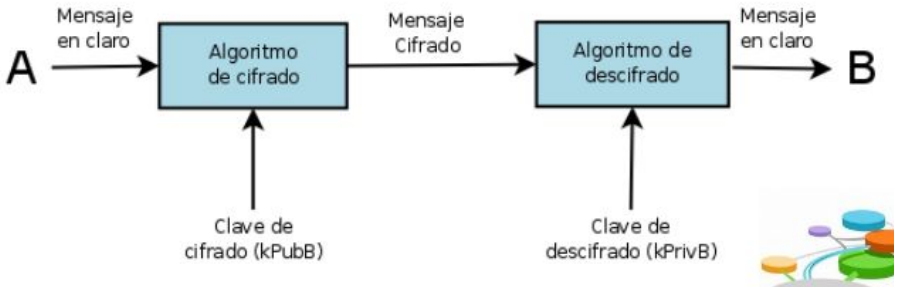
Rail Fence: El texto se escribe en diagonal hacia abajo en "rieles" de una valla imaginaria hasta el último riel, luego se escribe en diagonal hacia arriba y así sucesivamente. Luego se toma el mensaje por filas.
Rotor Machine: Compuesta por cilindros independientes con contactos eléctricos que implementan cada uno una sustitución monoalfabética. Los cilindros giran a distinta velocidad, (como un velocímetro), logrando una sustitución polialfabética compleja

Criptografía simétrica (convencional, o de clave secreta)

La criptografía simétrica se basa en la utilización de la misma clave para el cifrado y para el descifrado. La robustez de un algoritmo de cifrado simétrico recae en el conocimiento de dicha clave.
Ventajas: sencillez de implementación, rapidez y robustez.
Desventajas: Administración de claves no escalable.
Garantiza: Privacidad, autenticidad e integridad.
No Garantiza: No repudio.
El emisor cifra el mensaje con la clave k y se lo envía al receptor. Este último, que conoce dicha clave, la utiliza para descifrar la información



Criptografía asimétrica (clave pública)
Se basa en la utilización de dos claves relacionadas, una para cifrar y otra para descifrar. (Denominadas clave pública y clave privada). La seguridad está basada en la dificultad de deducir una clave a partir del conocimiento de la otra. (la clave privada a partir de la clave pública).
Ventajas: Mayor escalabilidad en la distribución de claves.
Desventajas: Mayor tiempo de procesamiento. Necesidad de autenticar las claves públicas
El usuario A cifra un mensaje con la clave pública del usuario B (destinatario), éste para descifrarlo utiliza su clave secreta correspondiente, únicamente conocida por él.



Funciones HASH
Una función hash es una función computable que aplicada a un mensaje (m) de tamaño variable genera una representación de tamaño fijo del propio mensaje (H(m)). H(m) es mucho menor que m; por ejemplo, m puede tener una longitud de 1Mb, mientras que H(m) se puede reducir a 64 0 128 bits.
Una función hash unidireccional es una función hash H de modo que para cualquier mensaje m' es difícil encontrar un mensaje m tal que m'=H(m). Este tipo de función se denomina función resumen, y al valor H(m) se le suele llamar el resumen o digesto de m.

Autenticación de mensajes
Procedimiento para verificar que el mensaje recibido ha sido generado por la supuesta fuente que lo envía, y que no ha sido modificado. Adicionalmente, puede verificarse la secuencia y tiempo oportuno. (Que no ha ocurrido alteración en el orden de los mensajes, retraso o retransmisión).

Código de Autenticación de Mensajes
Una función MAC es una función que aplicada a un mensaje (m) de tamaño variable y una clave (k) genera una representación de tamaño fijo del propio mensaje MAC=C k (m).
La clave secreta es compartida por emisor y receptor.

Firma digital

Mecanismo de autenticación que permite al creador de un mensaje anexar un código que actúa como una firma, garantizando origen e integridad.
Proceso de firmado: El usuario A genera una huella digital H(m) del mensaje m y cifra dicha huella con su clave privada (kPrivA). A continuación A envía al usuario B el mensaje sin cifrar (m) y su correspondiente resumen (H(m)) cifrado. El usuario B obtiene la huella digital calculada por A utilizando la clave pública de A

(kPubA) sobre el H(m) cifrado y continuación genera la huella digital del mensaje enviado por el usuario A (H(m)'). B realiza una comparación de las dos huellas obtenidas. Si no coinciden (H(m) y H(m)') es que el mensaje o la huella enviada por A han sido modificados y por tanto la firma no es correcta.

Redes Privadas Virtuales (VPN)

Una VPN es un conjunto de herramientas que permite a redes de diferentes lugares conectarse de forma segura, utilizando una red pública como capa de transporte.
Proveen un medio de establecer comunicaciones seguras sobre redes públicas o inseguras.
Utilizan cifrado para proveer confidencialidad, autenticidad e integridad.
Objetivos:

- ➢ Conectar usuarios de forma segura a sus redes empresariales (Acceso Remoto)
- ➢ Vincular sucursales con una red empresarial (Intranet).
- ➢ Ampliar la existente infraestructura de red de una organización para incluir socios, proveedores y clientes (Extranet)

Servicios:

- ➢ *Autenticación de usuarios:* Solamente usuarios autorizados pueden tener acceso a la VPN.
- ➢ *Administración de claves:* Se debe generar y actualizar las claves de cifrado para los clientes VPN y el servidor VPN: La tecnología VPN debe encapsular los datos privados agregando una cabecera adicional que permita a estos transitar por la red pública, esto se conoce como túnel.
- ➢ *Administración de direcciones*: Se debe asignar a los clientes de la VPN las direcciones IP dentro de la intranet corporativa y asegurar que dichas direcciones se mantengan privadas.
- ➢ *Cifrado de datos:* Los datos transmitidos sobre la infraestructura de red pública tienen que ser ilegibles para los clientes no autorizados de la VPN.
- ➢ *Encapsulamiento:* La tecnología VPN debe encapsular los datos privados agregando una cabecera adicional que permita a estos transitar por la red pública, esto se conoce como túnel.
- ➢ *Soporte a múltiples protocolos* : Proveer soporte para los protocolos utilizados en la red pública.

Tipos

- ➢ *De acceso remoto (Remote access)*: Conectan usuarios a redes a través de un Servidor de Acceso a la Red (NAS) (Interactúa con server de Autenticación, Autorización y Contabilidad).
- ➢ *Sitio a sitio(site-to-site):* Conectan redes con redes mediante gestores de tráfico. (conexiones iniciadas en 1 sentido o ambos)

IPSec

Dos Modos de Operación:

- ❖ Transporte
- ❖ Túnel

Servicio de Autenticación ---> Authentication Header
Servicio de Confidencialidad y/o integridad ----> IP Encapsulating Security Payload, encapsulamiento de carga segura.

AH Protocol

- ❖ Provee autenticación, integridad y protección frente a reenvíos. (no confidencialidad).
- ❖ Asegura la carga de un paquete IP, y porciones del header IP.

ESP Protocol

- ❖ Puede proveer autenticación, integridad, protección frente a reenvíos y confidencialidad.

- ❖ Asegura todo la carga de un paquete IP. (no sus headers).

Asociaciones de seguridad
Describe cómo se van a tratar los paquetes entre dos puntos. O sea se va a alcanzar la protección deseada en la conexión.
Dice que algoritmos de cifrado se utilizan, qué claves, funciones hash, etc.
Se establece manualmente (hay problemas de escalabilidad en cada máquina se guarda) o de manera automática.

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.
Para decidir qué protección se va a proporcionar a un paquete saliente, IPsec utiliza el índice de parámetro de seguridad (SPI), un índice a la base de datos de asociaciones de seguridad (SADB), junto con la dirección de destino de la cabecera del paquete, que juntos identifican de forma única una asociación de seguridad para dicho paquete. Para un paquete entrante se realiza un procedimiento similar; en este caso IPsec toma las claves de verificación y descifrado de la base de datos de asociaciones de seguridad.

Modo transporte: En modo transporte, sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada o autenticada. El ruteo permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. El modo transporte se utiliza para comunicaciones ordenador a ordenador.

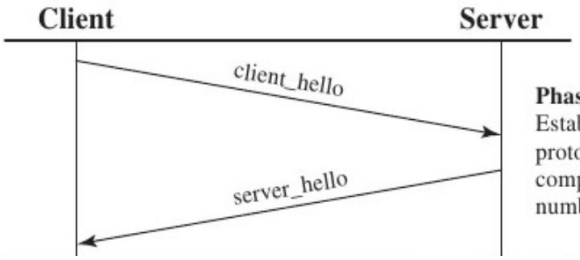
Modo túnel: En el modo túnel, todo el paquete IP (datos más cabeceras del mensaje) es cifrado o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el ruteo. El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre routers, p.e. para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.

Transport Layer Security (TLS) Protocol

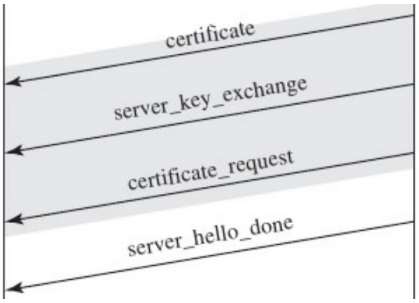
Se establece una conexión segura por medio de un canal cifrado entre el cliente y el servidor. Le brinda seguridad a TCP sin modificarlo.
Provee cifrado y autenticación X.509 de uno o ambos extremos.
Está formado por cuatro protocolos:

- ➔ TLS Record Protocol: encargado de cifrar y enviar los mensajes. Toma un mensaje de capa superior, lo fragmenta en bloques (propia de TLS), opcionalmente comprime los fragmentos, aplica un código de autenticación (hash aplicado a los datos que vienen y la clave secreta que se tiene) luego cifra el mensajea utilizando una clave privada y agrega un encabezado.
- ➔ HANDSHAKE Protocol: negocia una sesión TLS dentro de una sesión TCP identificada con un número.
- ➔ Alert Protocol: mensajes de 2 bytes para mandar alertas. El primer byte indica si es un warning o un fatal (en caso de ser fatal, la sesión TLS se da por terminada). El segundo indica la alerta específica. Dado que estos mensaje viajan sobre TLS pueden ir cifrados y comprimidos.
- ➔ Change Chiper: es un mensaje con un solo byte que indica que a partir de ahora se van a empezar a usar protocolos que se negociaron. O sea, cuando se está negociando el handshake no se está utilizando ningún cifrado porque se está negociando.

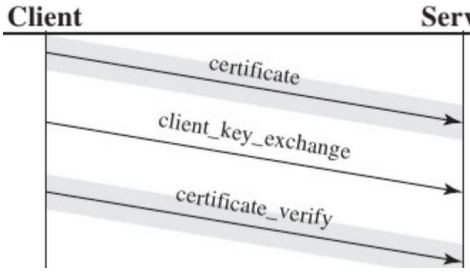
Fases del HANDSHAKE



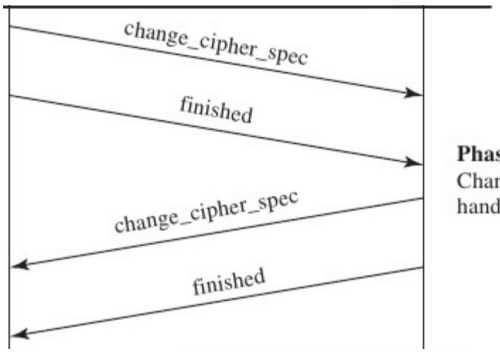
Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.



Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.



Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.



Phase 4
Change cipher suite and finish handshake protocol.

Secure Shell (SSH)

Su uso más común es el logue remoto. Sirve para acceder a máquinas a través de una red.
La información que viaja por el medio de comunicación va de manera no legible.
Puede hacer túneles para conexiones y transportar cualquier tipo de datos.
La autenticación se hace por Host-Key. Se crean las claves públicas y privadas, se le pasa la clave pública a otro host y se establece la conexión SSH.
Cuando se establece la conexión SSH hay negociaciones de intercambio de claves , algoritmos de cifrado y de clave pública, autenticación de mensajes y hash.
No trabaja con certificados X.509 como TLS sino que hay dos tipos de autenticación:

1. Cuando se establece la conexión SSH entre dos hosts, se utiliza la host key del otro host.
2. Luego viene el protocolo de autenticación.

Compuestos por protocolos:

- SSH Transport Layer Protocol: es el que realmente cifra y autentica. Provee autenticación, confidencialidad e integridad.
- SSH User authentication protocol: autentica al usuaria frente al servidor.

- ❖ SSH Connection Protocol: Luego de establecer la conexión SSH se abren canales de comunicación para intercambiar datos. Multiplexa distintos canales de comunicación lógicos.

Virtual LANs

Subred lógica a nivel 2 definida por software.
Segmentan una red en diferentes dominios de broadcast.
Se utilizan para agrupar servers, pc's, etc. de acuerdo a requerimientos similares de manejo de datos y seguridad.
La comunicación entre dispositivos de diferentes VLANs debe realizarse a nivel 3.
Sirven para aislar cierto tipo de tráfico dentro de una LAN. La idea es que dos dispositivos se tienen que ver entre sí pero con el resto de los dispositivos. Entonces para no tener redes físicas separadas, se pueden crear redes LAN virtuales.
Ventajas:

- ➢ Independiza la ubicación física de los dispositivos. Cambiar su dominio y acceso a recursos sin moverlos físicamente.
- ➢ Todo se configura por software.
- ➢ Reducir tráfico de la red, ya que dirigen tráfico de red solo a los dispositivos que lo tienen que recibir.

La comunicación entre los equipos de una LAN está regido en la arquitectura física. Gracias a las VLANs las limitaciones geográficas quedaron atrás. Se arman redes lógicas según los puertos de un conmutador, según la dirección MAC y la dirección IP del datagrama. Los dispositivos se conectan como si estuvieran al mismo cable, y en realidad están conectados a diferentes segmentos de una red física.

Virtualización

Abstracción de los recursos de computación.
Desde el punto de vista de S.O.: memoria, dispositivos, archivos.
System Virtualization: Abstracción de una computadora completa, incluyendo memoria, cpu y periféricos.
Hoy día la virtualización es capaz de proveer un entorno virtual para la ejecución de aplicaciones (o VMs), almacenamiento, memoria, red.
Genera una versión virtual (lógica) de un recurso físico.

Tipos de Virtualización:

-- Máquina: Virtualización de una máquina completa donde se le hace creer al SO que tiene una PC completa.

-- Almacenamiento: Se unen varios dispositivos de almacenamiento donde aparentar ser un único dispositivo.

-- Red: VLANs.

-- Escritorio: De forma remota. Se separa el escritorio con los datos y programas de usuario y se alojan en un lugar remoto.

-- Servicio de Aplicación: Un servidor pasa a ser utilizado en varios entornos virtuales.

Componentes:

-- Host: Servidor físico real.

-- Capa de virtualización: Capa de abstracción.

-- Guest: El SO que se cree que corre en una máquina.

Características:

-- Compartir: se comparte un servidor entre N máquinas virtuales.

-- Agregación: Varias fuentes de cómputos que se presentan como una sola. También puede ser de almacenamiento.

-- Emulación: de redes.

-- Aislamiento: Entre componentes.

Propiedades de las VMs

-- Eficiencia: Todas las instrucciones inocuas son ejecutadas por el Hardware directamente, sin intervención alguna por parte del programa de control.

-- Control de Recursos: Se invoca cuando un programa quiere afectar a los recursos del sistema, es decir, a la memoria, a su disposición.

-- Equivalencia: Si dos VM corren, deberían producir el mismo resultado con la excepción del tiempo y de los recursos que puede haber.

-- Instrucciones privilegiadas: Generan un trap si CPU en modo usuario, no en supervisor.

-- Instrucciones sensibles: Cambian la configuración del sistema. Deben ser ejecutadas en modo supervisor.

TEOREMA 1: Para cualquier ordenador de generación convencional, se puede construir un monitor de máquina virtual si el conjunto de instrucciones sensibles para ese ordenador es un subconjunto del conjunto de instrucciones privilegiadas.

TEOREMA 2: Una computadora es recursivamente virtualizable si es: (a) virtualizable, y (b) puede construirse un VMM sin ninguna dependencia de temporización.

TEOREMA 3: Se puede construir un monitor de máquina virtual híbrido para cualquier máquina en la que el conjunto de instrucciones sensibles al usuario sea un subconjunto del conjunto de instrucciones privilegiadas.

Hipervisor

Es el elemento del SO o de software que administra y hace que funcionen las VM.

-- Tipo I : Controla todos los accesos al hardware. Se instala el Hipervisor antes del SO. No se instala uno dentro de otro sino uno al lado del otro y los recursos son supervisados por el hipervisor.

-- Tipo II : Se ejecuta en modo usuario como un proceso más del SO.

Aislación: La máquina virtual puede hacer todo lo que quiera pero no en los recursos del hardware, si quiere hacer algo sobre el hardware debe enviar un trap al programa que controla el hardware para que lo supervise.

Software-Defined Networking (SDN) -- Redes definidas por Software

Un conjunto de técnicas que permite programar, orquestar, controlar directamente
Y gestionar los recursos de red, lo que facilita el diseño, la entrega y el funcionamiento de los servicios de red de forma dinámica y escalable.
La separación física del plano de control de red del plano de reenvío, y donde un plano de control controla varios dispositivos.

Planos tradicionales

-- Data Plane

- -- Manejo y reenvío de paquetes (shaping y policing).
- -- Tablas de reenvío y de MPLS.
- -- El Data Plane es manejado por el Control Plane.
- -- Recalcula las rutas por si se cae algún enlace para los cambios de topología (Ventaja).
- --(Desventaja) Tiempo de convergencia, es decir, el tiempo que se pierde hasta que se restablece la red. No puede ser óptimo el uso de la red ya que la elección de la ruta alternativa es en base al destino y no por el tráfico de las redes.

-- Control Plane

-- Configura el data plane indicándole cómo tratar los paquetes acorde al hardware/software particular
-- Administra las tablas de reenvío.
--Management Plane
--Configuración del control plane (y posiblemente del data plane directamente)

Propuesta OpenFlow
Es como armar VLANs, se tiene una red y cierta personas quiere hacer pruebas, entonces la red se particiona y se dan ciertos recursos de la red. No se utiliza la interfaz del switch como en las VLANs sino que se utiliza un protocolo estándar que maneje todos los switches a la vez y tengo una versión centralizada (red gestionada como un todo).
Es una canal seguro (TLS) con el controlador.
Protocolo para definir las tablas de flujo.
Es un protocolo que permite a un servidor decirlo a los routers donde enviar los paquetes. En una red convencional es el software del router que lo decide. El router y el controlador se comunican por OpenFlow.

Actualizaciones Proactivas: Generadas por el usuario. Cambian el estado de la red.
Actualizaciones Reactivas: Generadas por los switches por medio de mensajes.

Cada entrada en las flowtable contiene:
-- Campos de matcheo
-- Acciones (conjunto de instrucciones)
-- Contadores
Procesamiento de Ingreso: Los paquetes que entran por el puerto comienzan a ser procesados por las tablas de flujos. Se realiza el matcheo con la dirección MAC o con algún campo del protocolo IP o TCP. Las tablas están numeradas y en ellas se agregan las acciones a realizar sobre el paquete. Las diferentes tablas pueden indicar que un paquete debe ser reenviado mientras que otra puede indicar que hay que cambiarle la IP destino y así sucesivamente.
Procesamiento de Egreso: Se encuentran las tablas de salida. El procedimiento es similar al de ingreso salvo que cambian los valores iniciales de la metadata (ya que en cada acción puede irse agregando metadata). La metadata inicial puede tener el puerto por donde ingresó el paquete.

Procesamiento: Entra el paquete, el conjunto de acciones está vacía, y se comienza con la tabla cero. A medida que se pasa de tabla se va a una tabla de numeración superior. Si hay coincidencia en la tabla, se actualizan los contadores y se ejecutan las instrucciones como por ejemplo: agregar acciones al conjunto de acciones. Puede haber salto de tabla.
En el caso de que no hubiera entrada, se fija si hay una entrada de fallos (default) y si no está se dropea el paquete. En el caso de que si hubiera en la entrada de fallos, se ejecutan las instrucciones correspondiente. Después de haber procesado todas las tablas, algunas pudieron haber decremetado el TTL, modificaron los headers de los paquetes, etc. Luego se ejecuta un Group Action (lista de acciones predeterminadas por grupos). Después, si hay alguna acción de salida se rutea el paquete al puerto que sigue, y si no se descarta. En cuanto a las tablas de egreso, se procesan de la misma manera que las de ingreso.

Mensajes (TCP/TLS port 6653)
-- Controller-to-switch:
-- Administrar o inspeccionar el estado del switch
-- Puede o no requerir respuesta del switch
-- Features, Configuration, Modify-state, Read-state, Packe-out, Barrier, Role-request, Asynchronous-configuration
-- Asynchronous:

-- Enviados por el switch sin que lo solicite el controlador
-- Informan de paquetes que arriban, cambios en el estado del switch, errores.
-- Packet-in, Flow-removed, Port-status, Error

-- Symmetric:
-- Enviados por switch o controlador sin ser solicitados
-- Hello, Echo, Experimenter

INFRAESTRUCTURA DE DATA CENTER

Diseñado para albergar gran cantidad de equipos de cómputo y componentes asociados, tales como sistemas de almacenamiento y telecomunicaciones.
Debe contemplarse:

-- Espacios y distribución.
-- Infraestructura de cableado.
-- Niveles de Confiabilidad.
-- Consideraciones Medioambientales.

Uptime Institute -- > Institución
Clasificación “Tier Performance Standard”,
No presenta una “checklist”, se determina el nivel del DataCenter de acuerdo a sus prestaciones.
(Performance confirmation tests)
Certificación en tres categorías: diseño, construcción y sustentabilidad operacional.

Nivel I - Infraestructura básica del sitio (no redundante), si se corta un componente no hay disponibilidad, en caso de requerir mantenimiento se necesita apagar todo.

Nivel II - Componentes de capacidad redundante infraestructura del sitio (redundante), en caso de requerir mantenimiento se necesita apagar todo.

Nivel III - Infraestructura del sitio que se puede mantener simultáneamente, todo por duplicado,en caso de requerir mantenimiento se puede realizar de manera concurrente.

Nivel IV - Infraestructura del sitio tolerante a fallos, todo absolutamente redundante, disponibilidad “eterna”.