mi aporte para los q rindan redes
este resumen está casi completo, faltan los temas IPSec, ssl, tls
y completar temas como firewalls, ospf y bgp, voip y vpn. para eso recomiendo clases grabadas. con esto saque 10 en el final.
ya q le dedique tantas horas a este resumen pido colaboración -> sigan mi emprendimiento en instagram, regálenle algo a sus amigas/novias q me ayudan un monton <3 @carolia.lenceria
https://www.instagram.com/carolia.lenceria/
éxitos a todos

Unidad Nro. 1: ARQUITECTURA DE REDES

- Concepto de Red de telecomunicación
- Clasificación de las redes
- Arquitectura de protocolos TCP/IP, historia, evolución.
- Modelo de referencia TCP/IP: función de cada nivel. Conjunto de Protocolos. Encapsulamiento y desencapsulamiento. Ejemplos.
- Internet: Orígenes. Características. Servicios básicos. Arquitectura de Internet (niveles).
- Organismos Internacionales de Normalización: ITU, ISO, IEEE, Estándares IETF: R

Unidad Nro. 2: CAPA DE ACCESO EN REDES LOCALES

- Métodos de acceso al medio: CSMA/CD. CSMA/CA. Token Ring. Dominio de colisión y dominio de broadcast.
- Estándares IEEE 802.3: Ethernet. Fast-Ethernet. Giga-Ethernet. 10 Giga-Ethernet.
- Dispositivos: NIC. Hub. Bridge. Switch. IEEE 802.1D. Access Point.
- Wireless LAN: IEEE 802.11.

Unidad Nº 3: CAPA DE INTERRED – DIRECCIONAMIENTO

- Direccionamiento IP: Protocolo IPv4. Formato del datagrama. Direccionamiento IPv4. Clases de direcciones. Máscara de red. Ejercitación.
- Direcciones privadas y públicas. División de una red en subredes. Máscara de subred. Ejercitación.
- VLANs. IEEE 802.1q. Agotamiento de las direcciones IPv4.
- VLSM. CIDR.
- Protocolo IPv6: características, ventajas con respecto a IPv4, formato del datagrama de IPv6.
- ICMP: funcionamiento, tipos de mensajes.
- ARP: funcionamiento, tablas ARP.
- Direccionamiento estático. Direccionamiento dinámico. BOOTP: características. DHCP: características, funcionamiento, agente relay de DHCP.

Unidad Nº 4: CAPA DE INTERRED – ENCAMINAMIENTO Y CONGESTIÓN

- Encaminamiento. Concepto. Algoritmos de encaminamiento. La ruta más corta. Inundación. Algoritmo Jerárquico. Vector de distancia: características, problema de conteo al infinito, horizonte dividido, actualizaciones por eventos. Estado de enlace: características, funcionamiento. Análisis comparativo entre protocolos de vector de distancia y de estado de enlace.
- Encaminamiento en Internet. Sistemas autónomos. Protocolos de gateway interior. RIP: características, funcionamiento. OSPF: características, funcionamiento. BGP: características, funcionamiento.
- Routers: componentes, puertos, principio de funcionamiento, configuración básica.
- Enrutamiento entre VLANs.
- Congestión. Algoritmos de control de congestión. Diferencia entre control de congestión y control de flujo. Principios generales del control de congestión. Políticas de prevención de congestión.
- Calidad de Servicio. Requerimientos. Técnicas para alcanzar buena calidad de servicio (sobreaprovisionamiento, almacenamiento en buffer, modelado de tráfico, algoritmo de cubeta con goteo, algoritmo de cubeta con tokens, reserva de recursos, control de admisión).
- MPLS. Herramientas de Administración de Red.
- Comandos: arp, ping, pathping, tracert, ifconfig (linux), ipconfig, route print, netstat, nslookup, telnet, ssh, nmap.

Unidad Nº 5: CAPA DE TRANSPORTE Y CAPA DE APLICACIÓN

- Capa de Transporte: Servicios de la capa de transporte: orientado a conexión y sin conexión.
- Protocolo TCP: características, funcionamiento, formato del segmento. Establecimiento y liberación de una conexión.
- Protocolo UDP: características, formato del encabezado. Puertos. Aplicaciones de TCP y UDP.
- Traducción de Direcciones de Red: características, NAT estática, NAT dinámica, PAT.
- DNS. Funcionamiento. Espacio de nombres de DNS. Registros de recursos. Servidores de nombres.
- FTP: Características, aplicaciones.
- TFTP: características, aplicaciones.
- SNMP. Modelo SNMP (componentes). Funcionamiento. MIB. Protocolo SNMP.
- Correo Electrónico: Arquitectura y servicios, agente de usuario, formatos de mensaje, transferencia de mensajes. Protocolo SMTP, Protocolo MIME.
- WWW: arquitectura. URL. Localización de información en la Web.
- HTTP. HTTPs.
- Voz sobre IP: estándar H 323, estándares de codificación de voz, protocolo RTTP, SIP.

Unidad Nº 6: SEGURIDAD

- Concepto de seguridad. Políticas de seguridad informática en una red. Confidencialidad. Autenticación. Integridad. Disponibilidad.

- Firmas digitales. Concepto. Implementación. Firmas de clave simétrica. Firmas de clave pública.
- Firewalls. Características. Tipos.
- Servidor Proxy. Filtrado de paquetes.
- Aplicaciones.
- Seguridad en la capa de red: IPSec. Seguridad en la Web: Protocolo de seguridad SSL y TLS. VPN. Características. Aplicaciones.

Unidad 1: Arquitectura de redes

Redes

Concepto de red de telecomunicaciones

Una red es un conjunto de dispositivos interconectados. Una red informática sirve para compartir recursos e información entre nodos cercanos, y una red de telecomunicaciones está conformada por nodos lejanos interconectados para permitir la comunicación a distancia.

Clasificación

1) Según área de cobertura
    - PAN
      Redes de área personal, conforman un radio de 1 metro.
    - LAN
      Redes de área local, privadas dentro de un edificio, abarcan 1km. Cada pc de la red puede comunicarse con un enrutador inalámbrico llamado Access Point o con otro PC. Pueden ser inalámbricas (WiFi 802.11) o alámbricas (Ethernet 802.3) y operan a velocidades de hasta 10 Gbps. Se pueden dividir en subredes lógicas llamadas VLANs, por ejemplo, para seguridad y organización. También se pueden usar diversas topologías, como punto a punto, bus, estrella, anillo, árbol o malla. El acceso al medio puede hacerse con diseños estáticos y dinámicos, y los dinámicos pueden ser centralizados o descentralizados según quién decide qué canales acceden y usan el medio.
    - MAN
      Redes de área metropolitana, alcanzan los 10km y generalmente se implementan con topología anillo. Ejemplo: WiMAX 802.16, TV por cable.
    - WAN
      Redes de área amplia, abarcan países o continentes, son públicas. En cuanto a su concepto, es muy parecida a una LAN alámbrica extensa, con

ciertas consideraciones como que los hosts y subredes que pertenecen a ella son de diferentes personas, y pueden contener subredes (interredes) de diferentes tipos, usadas por los usuarios o controladas por los proveedores de servicios (Internet Service Provider, ISP). Topología punto a punto, estrella o malla.

2) Según direccionalidad de los datos
    - Simplex (único sentido de transmisión)
    - Half dúplex (doble sentido pero no simultáneo)
    - Full dúplex (doble sentido y simultáneo)
3) Según la topología
    - Anillo
    - Estrella
    - Bus
    - Malla
4) Según la tecnología de implementación
    - Conmutación por circuitos (de extremo a extremo, se envía un mensaje por el canal a través de un circuito virtual previamente establecido que se mantiene desde el comienzo hasta el final de la transmisión).
    - Conmutación por paquetes (la información se divide en paquetes que se envían por diferentes caminos).
    - Conmutación por trama (tecnología WAN, se establece un circuito virtual y se transmiten paquetes - mezcla de los dos anteriores).
    - Conmutación por celda (tecnología WAN y LAN, igual que el anterior pero los datos se dividen en celdas iguales de 53 B)
5) Según la tecnología de transmisión
    - De difusión o broadcast
    - Punto a punto
6) Según el ancho de banda
    - Banda angosta
    - Banda ancha
7) Según el propietario
    - Públicas
    - Privadas

TCP/IP

Arquitectura, historia

Alrededor de 1980, estábamos frente a una rápida expansión de las redes y el uso de las mismas por diferentes empresas privadas. El problema era que no había un acuerdo o estándar a seguir para estas redes, por lo que al intentar comunicar o conectar las redes de diferentes empresas entre sí, surgieron incompatibilidades. Para solucionar esto, la Organización Internacional de la Estandarización ISO investigó modelos de networking para encontrar un conjunto de reglas aplicables a todas las redes, y con esto nació el modelo OSI, un modelo basado en 7 capas con diferentes funcionalidades que resolvían la comunicación entre redes. A partir del modelo OSI y de la llamada ARPANet, nace el

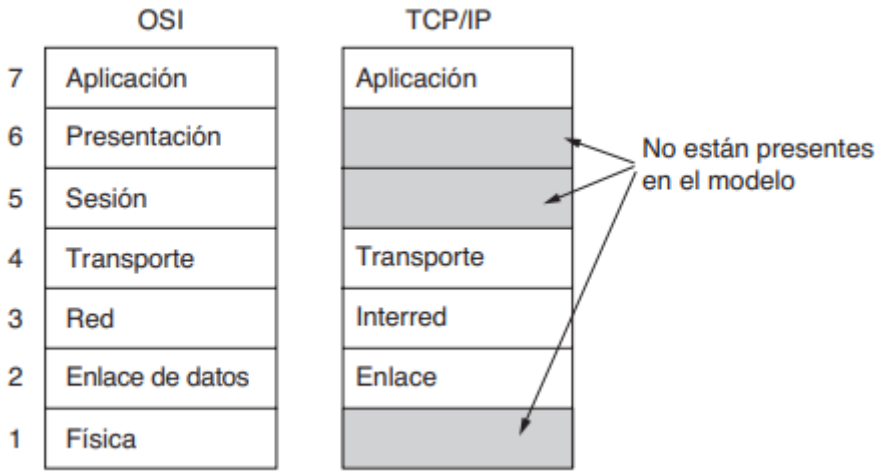
modelo TCP/IP, una pila de protocolos que trabajan en conjunto con el objetivo de ofrecer una conectividad permanente por más que un nodo se caiga, independencia del medio de transmisión, del hardware y del software, que soporte transmisiones de cualquier tipo de información. La idea fundamental es que cada capa provea un servicio a una capa superior a través del uso de un conjunto de reglas de la capa, que conforman protocolos. Un protocolo es un acuerdo entre las partes que se comunican para establecer la forma en que se llevará a cabo la comunicación.

Características:

- Fiabilidad: se basa en conmutación de paquetes, busca una conexión permanente por más que un nodo se caiga.
- Independencia de HW y sistema operativo.
- Transmisión de cualquier tipo de información.

Las capas del mismo nivel de diferentes redes se llaman homólogas o pares. Estas no se comunican directamente entre sí a nivel físico, pero sí a nivel lógico. Las capas adyacentes se comunican únicamente, a través de interfaces que definen los servicios que la capa inferior provee a la superior. A un conjunto de capas y protocolos se lo conoce como arquitectura de red, y al conjunto de protocolos que usa una arquitectura de red se le llama pila de protocolos.

TCP/IP está conformada por 4 capas: de aplicación, de transporte, de interred y de enlace.



Modelo de referencia. Función de cada nivel. Protocolos. Encapsulamiento y desencapsulamiento.

Para enviar datos desde un nodo emisor a través de una red, estos pasan de la capa de aplicación a la inferior, donde se le agrega un encabezado. En la capa de transporte, se recibe el dato, se le agrega otro encabezado generando un segmento, y se pasa a la capa inferior. Así, los datos van pasando capa por capa hacia abajo, ya que cada una habla un idioma distinto al usar diferentes protocolos. Esto es encapsulamiento. El desencapsulamiento es el proceso inverso, el router toma los datos y elimina el encabezado de cada capa y estos van “subiendo” hasta la última capa del nodo destino.

La capa de enlace es la más baja del modelo. Describe qué enlaces se necesitan para cumplir con las necesidades de esta capa de interred sin conexión. Es una interfaz entre los dispositivos hosts y los enlaces de transmisión. Su función es recibir y emitir mensajes en un mismo segmento de conexión. Los datos se llaman tramas.

La capa de interred es el eje de la arquitectura. Define el protocolo IP, que en conjunto con ICMP hacen que la capa funcione. Permite que los hosts inyecten paquetes IP en cualquier red y que éstos se envíen a un destino de la misma u otra red, sin importar cómo. Sus funciones son **direccionamiento, encaminamiento y control de congestión**. Los datos se llaman paquetes.

La capa de transporte está diseñada para permitir que las capas homólogas se comuniquen, a través de los protocolos TCP y UDP. Esta capa no ve nodos, sino un enlace. Los datos se llaman segmentos.

La capa de aplicación contiene los protocolos de alto nivel.

Internet

Internet es una red de redes, que surgió por la necesidad de interconectar redes LANs. Internet se organiza jerárquicamente con ISPs de diferentes niveles. Hay diferentes tipos de acceso a Internet, como por módem (Dial-up), ADSL, cable módem (redes CATV), etc. La interconexión de todas las redes de comunicación a escala global forma una única red descentralizada, la Internet, que ofrece servicios básicos y avanzados y posee una arquitectura de 3 capas (primero el backbone, que interconecta redes de diferentes continentes con fibra óptica, luego la segunda capa para empresas regionales, y la tercera para los ISP que brindar Internet a usuarios finales).

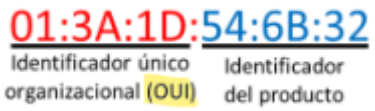
Organismos internacionales

Organismos de estandarización que nacen para conectar y compatibilizar redes aisladas.

- ITU - Unión Internacional de Telecomunicaciones: brinda estándares a las telecomunicaciones.
- IEEE - Instituto de Ingenieros Electrónicos y Eléctricos: define estándares para redes LAN.
- ISO - Organización Internacional de Estándares: integrada por distintos países, estandariza cualquier cosa.
- Internet: estándar de facto. Organizaciones como IAB, IETF e IRTF velan por su futuro.

Unidad 2: Capa de acceso en redes locales

Dirección MAC: dirección física grabada en la ROM de la placa de red, formada por 48 bits expresados en 12 dígitos hexadecimales. Son asignadas por la IEEE, identifican una interfaz de red de manera única. Se dividen en dos partes, identificador del fabricante e identificador del producto.



La capa de enlace de datos controla aspectos de acceso al medio, detección y corrección de errores y control de tráfico. Permite la conexión de dispositivos de un mismo segmento de red. Se subdivide en:

- Subcapa MAC - control de acceso al medio: se relaciona con las capas inferiores y define la forma de acceso al medio, es decir, la forma en que los dispositivos de una red comparten y usan un medio de comunicación. Se encarga del encapsulamiento y envío de tramas.
- Subcapa LLC - control de enlace lógico: norma 802.2, trabaja como interfaz entre la subcapa inferior y la capa superior, se encarga de controlar el flujo y errores. También participa en el armado de la trama.

Métodos de acceso al medio

- CSMA /CD: Estandarizado en la norma IEEE 802.3, sirve para medios guiados y consiste en obligar a las estaciones a escuchar el canal antes de transmitir para evitar colisiones. Tiene 3 variantes.
  ○ CSMA persistente 1: la estación primero escucha el canal y si este está inactivo envía sus datos. Sino, espera a que se desocupe y transmite la trama. Si hay una colisión, frena el envío y espera un tiempo aleatorio para retransmitir. Puede haber colisiones si dos estaciones están esperando que termine otra estación para transmitir, y al finalizar la tercera, los primeros dos envían datos al mismo tiempo.
  ○ CSMA no persistente: antes de enviar, una estación detecta el canal y si nadie está transmitiendo, empieza a transmitir. Sino, espera un tiempo aleatorio y vuelve a revisar, no se queda observando. Esto reduce las colisiones del método anterior.

○ CSMA persistente-p: se aplica a canales ranurados. La estación primero escucha el canal y si está inactivo empieza a transmitir con una probabilidad p. Luego, espera hasta la siguiente ranura, y si esta está en reposo la estación espera o transmite según la probabilidad 1-p. Esto se repite hasta terminar el envío o hasta que otra estación transmita. Si se detecta una colisión, se frena el envío, se espera un tiempo aleatorio y se intenta nuevamente.

Beneficios de CSMA /CD:

- Elevada eficacia, sobre todo en utilizaciones medias y bajas.
- La flexibilidad de conexión y facilidad de adicionar o suprimir estaciones de la red.
- Bajo retardo, aunque no acotable deterministicamente.
- La ausencia de establecimientos físicos o lógicos al conectarse en red una estación.

Desventajas:

- Bajo carga pesada, la performance del sistema se degrada severamente. Ocurren cada vez más colisiones y la red es atascada con intentos de retransmisión de tramas que han sufrido colisiones.
- La cantidad de demoras experimentada cuando se intenta retransmitir una trama es impredecible después que una transmisión ha sufrido una colisión

- CSMA/CA: con evitación de colisiones, estandarizado por la 802.11 y sirve para medios no guiados, en los que es más difícil detectar colisiones. Al encontrar el canal libre, la estación espera un tiempo aleatorio y vuelve a revisar el canal. Si está libre, envía un RTS request to send al nodo destino, y si este está libre, responde con un CTS clear to send; sino responde con un RxBusy. El nodo origen, al recibir el CTS, envía la trama y el receptor responderá ACK si se recibió bien, NACK sino.
- Token Ring: norma 802.5, topología de anillo en la que circula un token, y sólo la estación de trabajo que posea el token puede transmitir. Libre de colisiones, pero se pierde mucho tiempo del canal.

Dominios de colisión y de broadcast

Un dominio de colisión es un área física de una red donde las tramas pueden colisionar. Los repetidores y los hubs los extienden, pero los switches los dividen.

Un dominio de broadcast es un área lógica de una red donde los dispositivos pueden comunicarse directamente entre sí, sin routers. Los switches, puentes y hubs los extienden, routers los dividen.

Estándares IEEE 802.3

CSMA/CD fue usada por Ethernet clásica, las primeras LAN conectadas por cables coaxiales en topología de bus. Más adelante, con UTP y fibra óptica se comenzaron a usar hubs, y luego a puentes, que dividían los dominios de colisión. Se pasaron luego a los switches, eliminando los dominios de colisión y dando lugar a la Ethernet Conmutada, de la que se desprendieron muchas variantes con diferentes velocidades.

- Ethernet
  Usa CSMA/CD en redes LAN. Hasta 10 Mbps.
  - 10BASE2
    Funciona en capa de enlace MAC y capa física del modelo OSI. Usa codificación Manchester y cable coaxial fino.
  - 10BASE5
    Muchas colisiones, dificultad para conectar nuevos dispositivos. Usa cable coaxial grueso y topología de bus.
  - 10BASET
    Usa UTP, hubs y opera en half-dúplex. Hot plug and play.
- Fast Ethernet - 802.3u
  Opera a hasta 100 Mbps, usa switches y hubs y puede operar en half o full-dúplex. Implementa la autonegociación de velocidades y topología estrella.
  - 100BASETX: 2 cables UTP cat5.
  - 100BASEFX: 2 cables de fibra óptica.
  - 100BASET4: 4 cables UTP cat3.
- Giga Ethernet - 802.3ab
  Soporta half y full-dúplex, y autonegociación. Opera a hasta 1 Gbps.
- 10 Giga Ethernet - 802.3ae
  Estándar de fibra mono o multimodo, cable de cobre blindado y UTP. Se usa para conectar dispositivos de alta gama, ya que llega a 10 Gbps. Full-dúplex e implementa autonegociación con la velocidad más alta. Se usa en LANs, MANs y WANs.

Ethernet	**IEEE 802.3**	**IEEE 802.3z**
Topología: Bus Medio físico: coaxial fino (10BASE2) y coaxial grueso (10BASE5) Velocidad: 3 – 10 Mbps Codificación Manchester Protocolo MAC: CSMA/CD Sincronismo en capa 2 Modulación PAM2 Half – dúplex	Topología: Estrella Medio físico: UTP – CAT3 (10BASET) Velocidad: 10Mbps Half – dúplex Sincronismo en capa 2	Topología: Estrella Medio físico: FO Monomodo (1000BASESx) Multimodo (1000BASELx) Modulación NRZ Codificación 8B10D Full Duplex Sincronismo en capa física

IEEE 802.3u	**IEEE 802.3z**
Topología: Estrella Medio físico: UTP – CAT5/5e (10BASETx) o FO (Monomodo (100BASESx), Multimodo (100BASEFx) Modulación MLT-3 Codificación 4B5D Sincronismo en capa física Half o Full	Topología: Estrella Medio físico: UTP – CAT6 (1000BASETx) Modulación PAM5 Codificación 8B10D Sincronismo capa física Full Duplex

Tramas 802.3 y Ethernet

Hay dos tramas diferentes porque la creación de los Hubs permitió transformar las topologías de bus a estrellas, y se comenzó a usar UTP en lugar de cable coaxial.

Ethernet II

Bytes	8	6	6	2	46	4
	Preámbulo	Dirección de destino	Dirección de origen	Tipo	Datos	Secuencia de verificación de trama

IEEE 802.3

Bytes	7	1	6	6	2	De 46 a 1500	4
	Preámbulo	Delimitador de inicio de trama	Dirección de destino	Dirección de origen	Longitud	Encabezado y datos 802.2	Secuencia de verificación de trama

- Preámbulo y **SFD**: sirven para sincronizar, son el delimitador de inicio de trama. Termina de la forma 10101010**10101011**. En Ethernet, sólo existe el preámbulo, con 8 bytes de ceros y unos alternados.
- Dirección destino: la MAC de la estación destino, la cual puede ser una específica (transmisión unicast), o más de una, lo que se puede diferenciar con el bit menos significativo de la dirección. Si este es impar es para muchas estaciones, multicast. Si todos los bits son 1, es para todas las estaciones, broadcast.
- Dirección origen: la MAC de la estación origen.
- Longitud: me dice el tamaño del campo de datos de la trama. En Ethernet, es el campo tipo, que especifica el protocolo de capa superior que recibe los datos.
- Datos y relleno: en Ethernet, se esperan 46 bytes. En 802.3 se esperan como mínimo 46 bytes.
- CRC: secuencia de detección de errores de la trama con código de redundancia cíclico.

Dispositivos

NIC - Tarjeta de interfaz de red

Placa de red, se usa para que una máquina tenga conectividad. Brinda acceso físico al medio usando la dirección MAC- Realiza las funciones de la capa de enlace.

HUB - Concentrador

Sirve para conectar varios dispositivos en topología estrella, es un repetidor multipuerto half-dúplex de capa física.

Bridge - Puente

Segmenta la red para dividir dominios de colisión. Dispositivo de capa de enlace que interconecta protocolos.

Switch - Conmutador

Dispositivo de capa de enlace y red multipuerto que permite conectar equipos en red en topología estrella, full-dúplex. Cada puerto es un dominio de colisión.

Los bridges y los switches trabajan con una tabla de direcciones MAC. La de los switches se llama CAM (Content Addressable Memory) y se usa para saber a qué dispositivo debe conmutar los datos que le llegan. Esta tabla es dinámica y se va llenando a medida que el switch recibe y envía tramas. Al recibir una, el switch revisa su tabla CAM y si encuentra la dirección MAC a la que va dirigida la trama, la envía. Sino, envía un broadcast a todos los puertos que poseen conexión (excepto el puerto de origen) preguntando quién es el dueño de esa dirección. El dueño responderá con un unicast, y el switch crea la entrada a la tabla asociando la MAC con el puerto correspondiente, y envía la trama. Estas tablas tienen un tiempo de vida limitado.

Hay factores a tener en cuenta, como la densidad o cantidad de puertos, sus velocidades, si son fijos o modulares, si son de acceso o troncales, y si trabajan con UTP o fibra. Con respecto al switch en sí, pueden tener buffer para las tramas, y pueden o no ser administrables. Además, pueden conmutar tramas por almacenamiento y reenvío (espera toda la trama, la almacena y busca errores con CRC, y la reenvía sólo si es correcta) o por método de corte (Cut through envía la trama apenas va ingresando, y libre de fragmentos la envía sólo cuando llegan los primeros 64 bits).

802.1D

Tanto el switch como el bridge usan el protocolo Spanning Tree para manejar el dominio de broadcast. Este protocolo se encarga de prevenir una tormenta de broadcast, permitiendo a los switches conectarse entre ellos al inicio, armando un camino lógico desde el switch raíz hacia todos los demás, armando el mejor camino hacia cada uno con un algoritmo de árbol de expansión y mensajes BPDU que llevan información del ID del switch raíz, del emisor y del costo para llegar al raíz. En base a eso, se designa un puerto.
Estados de los puertos de un switch:

- Bloqueo: inician bloqueados y reciben BPDUs.
- Escucha: quedan esperando si hay otra mejor ruta hacia el switch raíz, y si es así, vuelven a bloqueo.
- Aprendiendo: el switch arma su tabla CAM, se descartan las tramas de datos.
- Enviando: se pueden enviar y recibir datos, y se va actualizando la tabla mientras se siguen procesando BPDUs.
- Desactivado

Access Point - Punto de acceso

Dispositivo de capa de enlace que permite la comunicación en una red de forma inalámbrica. Se puede conectar a una red cableada.

Router - Enrutador

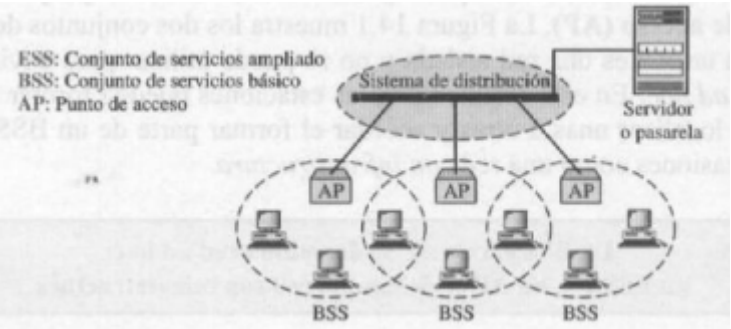
Dispositivo de capa de red encargado de interconectar redes.

IEEE 802.11 Wireless LAN

Servicios

Norma que estandariza el uso de redes inalámbricas, a través del uso de dos servicios:

- Conjunto de servicios básicos BSS:
  Son lo esencial para montar una LAN inalámbrica. Tenemos estaciones móviles y fijas. Tenemos dos tipos:
  - Access point: toda la comunicación se realiza por un AP, que centraliza las comunicaciones y se conecta con otras BSS.
  - Ad Hoc: los dispositivos se conectan entre ellos directamente, pero la red queda aislada de otras BSS.
- Conjunto de servicios ampliados ESS:
  Se compone de varias BSS que usan AP. Es una estructura de red más grande, creada por la unión de varios AP a través de un sistema de distribución DS.



Las estaciones se manejan a través un identificador SSID, igual para todas las que estén bajo un mismo AP.
El DS puede ofrecer diferentes servicios:

○ Asociación: de una estación a un AP, con tramas de administración en las que se envían el SSID, contraseña para la autenticación (conexión a la red), modo de red (protocolo), modo de seguridad y configuración de la banda de frecuencia.

○ Disociación: le avisa al AP que una estación saldrá de la red.

○ Reasociación: o roaming, una estación se desplaza a otra BSS.

○ Distribución: se trasladan datos de un AP a otro.

○ Integración: permite la conversión de protocolos entre redes.

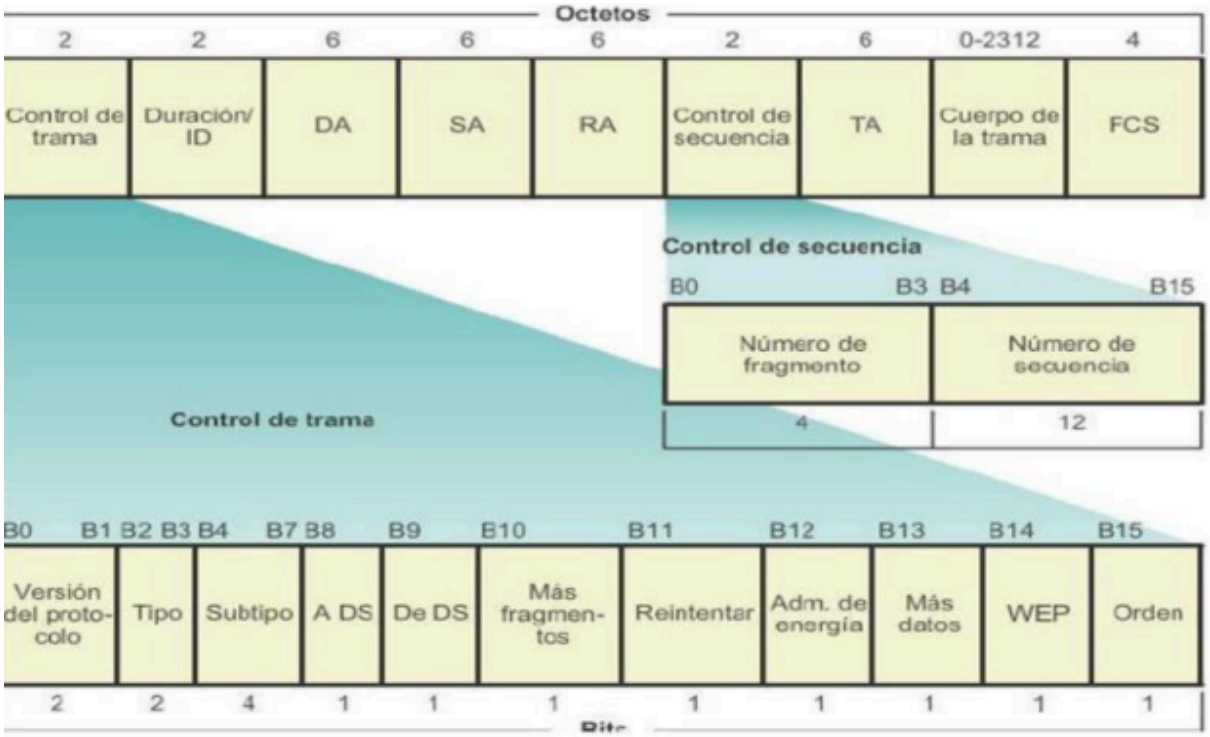
A considerar, esta red no es confiable, sufre interferencias y ruido, y no se envía un fragmento si el anterior no llegó y se avisó con un ACK. Transmite en bandas de frecuencia de 2,4 o 5 GHz. Además, los rangos de transmisión de diferentes estaciones pueden ser distintos, y algunas estaciones pueden estar muy lejos aún dentro de la misma celda y no recibir algunas transmisiones.

Pila de protocolos

Protocolo	Frecuencia [5GHz]	Velocidad Máxima	Técnica de multiplexación
802.11a	5	54 Mbps	OFDM
802.11ac	5	6 Gbps (utiliza MIMO)	OFDM
802.11b	2.4	22 Mbps	FDMA
802.11g	2.4	54 Mbps	OFDM
802.11n	2.4	600 Mbps - MIMO	OFDM

Tramas 802.11

- De datos: transportan información.
- De control: brindan asistencia a las estaciones con tramas RTS, CTS y ACK.
- De administración: permiten usar los servicios del DS.



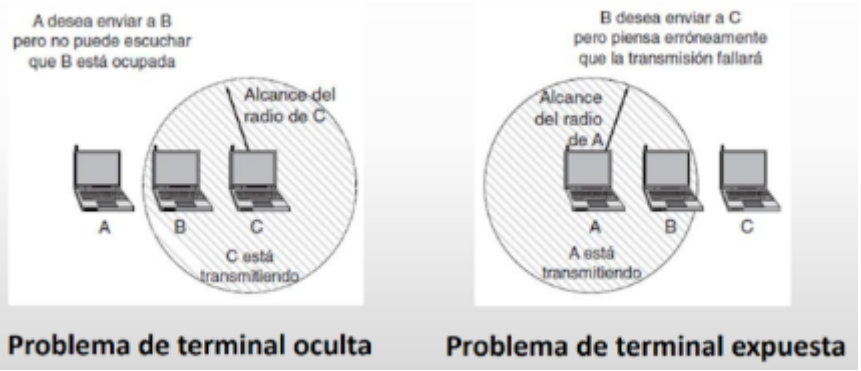
Campos:

1. Control de trama
    a. Versión del protocolo
    b. Tipo de trama
    c. Subtipo (para control, CTS o RTS)
    d. Para DS (si la trama va al DS)

    e. De DS (si la trama viene del DS)
    f. Más fragmentos
    g. Reintentar (si es retransmisión)
    h. Administración de energía (si el emisor entra en ahorro de batería)
    i. Más datos (si el emisor aún tiene tramas para enviar)
    j. Trama protegida (si está cifrada)
    k. Orden (si se necesita que las tramas lleguen en orden)
2. Duración (de la trama en el canal en microsegundos)
3. Dirección MAC destino
4. Dirección MAC origen
5. Dirección MAC del AP receptor inmediato
6. Secuencia (numera las tramas)
7. Dirección MAC del AP transmisor
8. Datos (hasta 2312 bytes)
9. CRC

Problemas

- Terminal oculta:
  Una estación no puede detectar a un potencial competidor por el medio, debido a que está muy lejos en la celda.
- Terminal expuesta:
  Una estación no transmite porque cree que el receptor está en una zona en la que ya se está transmitiendo y puede haber interferencia, y no es así.



Seguridad

WiFi ofrece autenticaciones de sistemas abiertos o de clave compartida, que requiere contraseña que puede ser WEP, WPA, WPA2 o WPA3.

Autenticación de clave compartida.

- WEP (Wired Equivalent Privacy)
  - Sistema de cifrado incluido en el estándar original 802.11
  - Utiliza el algoritmo de cifrado RC4 con claves de 62 o 128 bits.
- WPA (WiFi Protected Access)
  - Estándar de WiFi Alliance.
  - Diseñado para utilizar un servidor de autenticación RADIUS.
  - Implementa el Protocolo de Integridad de Clave Temporal (TKIP) que cambia claves dinámicamente.
- WPA2
  - Ratificado en 2004.
  - Utiliza el algoritmo de cifrado AES.
- WPA3
  - Sucesor de WAP2, anunciado en 2018.

Extras: 802.15 es conocida como Bluetooth, opera en la banda de 2,4 GHz. 802.16 es conocida como WiMAX, apunta a zonas rurales con bandas de 2,4 y 5,8 GHz, trabaja con OFDM, MIMO Y es multipunto.

Unidad 3 : Capa de Interred - direccionamiento

La capa de interred brinda un servicio de comunicación de datos entre dispositivos en una misma red o en diferentes redes. Es equivalente a la capa de red del modelo OSI y trabaja con conmutación de paquetes. Es **no orientado a conexión**, el router no establece una conexión de extremo a extremo antes de transmitir y enviar los paquetes a la red. Tiene como objetivo permitir el ingreso de paquetes a la red, y transportarlos a destino.

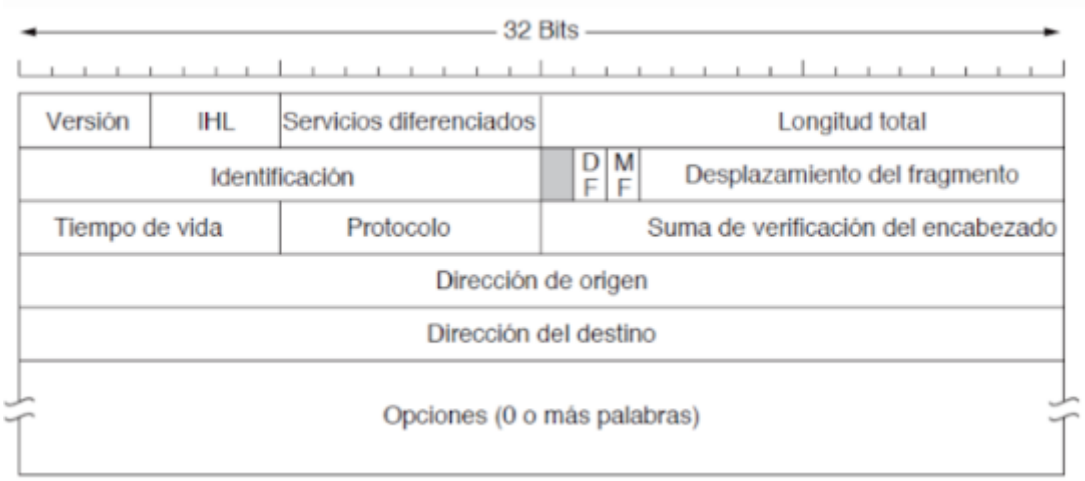
Funciones:

- Direccionamiento
  Los dispositivos tendrán una dirección IP (internet protocol) para tener conectividad.
- Encaminamiento
  Los routers encaminan los paquetes hacia destino.
- Control de congestión
  Se controla en la red que no haya colapso para que no se sature.

IPV4

Es el protocolo que mantiene unida la Internet, se ejecuta en routers. Recibe segmentos de la capa de transporte y los encapsula en paquetes agregándoles una cabecera IPv4, y los encamina de manera independiente por diferentes circuitos, sin seguir un orden. Para esto, cada paquete debe contener toda la información de direcciones, por lo que es algo lento. Sin embargo, es robusto, si un enlace se cae se puede encaminar el paquete para que vaya por otro enlace.

IP se basa en usar máscaras de red y tablas de enrutamiento, además de la propia dirección IP. En las tablas habrá direcciones de redes o subredes generales. Es no orientado a conexión y es de máximo esfuerzo (IP intenta entregar paquetes, pero no garantiza que lleguen a destino, puede haber congestión o puede caerse un enlace).



Esta es una cabecera IPv4. Se divide en renglones llamados palabras. Es de longitud mínima de 20 bytes, variable según el campo opciones. Sus campos son:

- Versión: puede ser 4 o 6.

- IHL: longitud de la cabecera en palabras de 32 bits.
- Servicios diferenciados: permite distinguir entre diferentes clases de servicios para brindar confiabilidad y/o velocidad.
- Longitud total: de la cabecera y los datos, todo junto.
  Para la fragmentación:
- Identificación del paquete, sirve por si fragmentamos los datos (normalmente lo hacemos, porque los paquetes pueden pesar hasta 64 KB y muchos medios no soportan tanto). Todos los fragmentos de un mismo paquete llevan el mismo ID.
- Bit libre.
- DF: bool, no fragmentado. Si está activo, indica que el router no puede fragmentar el paquete y lo descarta, por lo que el origen debe fragmentarlo en un trozo más pequeño. Esto último se avisa con otro protocolo.
- MF: bool, si hay más fragmentos.
- Desplazamiento de fragmento: orden del fragmento.

- Tiempo de vida: cantidad de saltos entre routers que puede dar un paquete. Esto para evitar un bucle por enlaces redundantes.
- Protocolo: qué tipo de segmento se encapsula.
- Checksum para controlar la integridad del paquete, para saber que ningún router intermedio modificó la cabecera. Puede modificarse el valor por el campo TTL.
- Dirección de origen IP
- Dirección de destino IP
- Opciones: se usan si quiero analizar el estado de la red. Pueden ser seguridad, encaminamiento estricto desde el origen, encaminamiento libre desde el origen, registrar ruta o marca de tiempo.

Direccionamiento IP

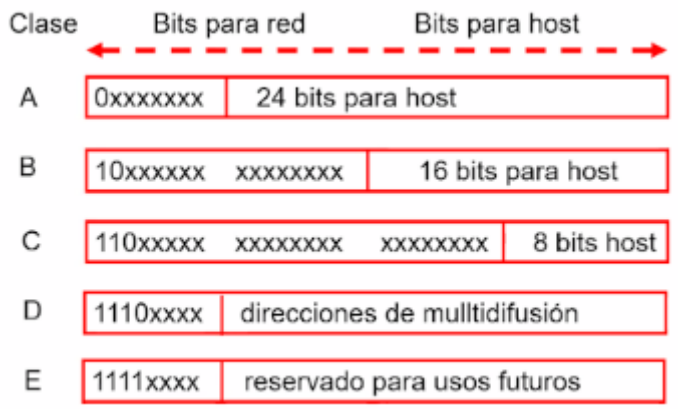
Actualmente tenemos las versiones 4 y 6. Una dirección IP identifica un dispositivo de una red. Estas direcciones son lógicas y jerárquicas, por lo que permiten determinar la ubicación física del dispositivo. Están formadas por 32 bits, tandas de a 8 separadas por puntos.

El corte de red/host puede variar, y según el tipo de corte es la clase de IP que tenemos.

Clases de direcciones

- Clase A: el primer byte refiere a la red, los otros refieren al host.
- Clase B: el corte está a la mitad.

- Clase C: los primeros tres bytes refieren a la red, el último es para el host.
- Clase D: multidifusión, es para manejo de grupos.
- Clase E: reservadas para usos futuros.



Clase A → 1.0.0.0 – 127.255.255.255

Clase B → 128.0.0.0 – 191.255.255.255

Clase C → 192.0.0.0 – 223.255.255.255

Clase D → 224.0.0.0 – 239.255.255.255

Cualquier dirección de red o dirección de broadcast de una red estará reservada. También 0.0.0.0 (indica al host actual), 0.0.0.24 (un host de esta red) y 127.x.x.x (loopback).

Máscara de red

Identifica a la parte de red de una dirección IPv4. Se denota con /x, donde x es la cantidad de bits que le corresponden a la red. Por defecto, para clase A la máscara es /8, para B es /16 y así. Sin embargo, podemos hacer variar esta máscara para la creación de subredes.

Subredes y máscara de red

Las subredes se crean a partir de modificaciones de la máscara de red y permiten dividir los dispositivos de una red en grupos más pequeños, lo que otorga más seguridad, menos tráfico y más dominios de broadcast.

- Jerárquicas: otorgan otro nivel de jerarquía a la dirección.
- Son creadas por el administrador de la red.
- Son visibles únicamente dentro de la red interna, de una organización por ejemplo.
- Permiten dividir el direccionamiento de una red interna y aumentar la seguridad con firewalls y otras configuraciones de permisos.

Las máscaras de red se modifican tomando bits prestados del host. Quitarle bits a la parte de host de la dirección implica que podré tener menos hosts en la red. Siempre hay

que considerar que en una red tendré 2^n - 2 hosts, con n = cantidad de bits para host. Con subredes, tendré 2^m subredes con 2^n - 2 hosts en cada subred, con m = cantidad de bits para subred.

Agotamiento de direcciones IPv4

El agotamiento de las direcciones IPv4 se dio por un crecimiento exponencial de Internet y de usuarios de la misma que necesitaban una dirección IP, que no se había previsto, además de un uso ineficiente del direccionamiento. La IANA (Internet Assigned Number Authority) y la RIR (Regional Internet Registry) son las responsables de distribuir direcciones IP. Frente al agotamiento de direcciones IPv4, surgieron 4 técnicas para solucionar el problema parcialmente, antes de la llegada de la versión 6.

1. Direccionamiento privado y NAT - Net Address Translation

RFC son normas que rigen los protocolos de Internet. La RFC 1918 habla de direcciones IP privadas, que se pueden usar dentro de empresas, casas y organizaciones. Invisibles para la Internet, quedan ocultas. Por lo tanto, se pueden repetir en todo el mundo (excepto dentro de la red interna). Nacen porque llegó un punto en el que se comenzaban a agotar las direcciones. Con ellas, nace la necesidad de traducir direcciones, de privadas a públicas para salir a Internet, y al revés. Se determinó un rango de direcciones privadas para cada clase:

- 10.0.0.0 a 10.255.255.255 para A
- 172.16.0.0 a 172.31.255.255 para B
- 192.168.0.0 a 192.168.255.255 para C

Para que una PC tenga conectividad con una LAN, necesitará una IP con su máscara de red. Si quiere conectarse a Internet, necesitará un gateway y una dirección IP de su servidor DNS (que resuelve el nombre de un dominio a una dirección IP).

NAT implica que en el paquete se reemplace la dirección de origen o destino privada por una pública. El router tendrá tablas para las traducciones, considerando 4 direcciones NAT:

- Local interna: la privada del host de la red interna
- Global interna: la pública del host origen
- Local externa: la pública del host destino/externo
- Global externa: la real del host destino/externo, pública o privada

Tabla NAT		
Dirección IP local interna	Dirección IP global interna	Dirección IP global externa
10.0.0.3	179.9.8.80	128.23.2.2

La local externa suele ser la misma que la global externa

PAT o NAT con sobrecarga, Port Address Translation. Esta técnica es útil cuando necesito que una misma IP pública se pueda usar para direccionar muchos hosts privados, se comienzan a usar los puertos para direccionar. Tenemos dos configuraciones

- Un ISP otorga una única dirección pública a una red interna.

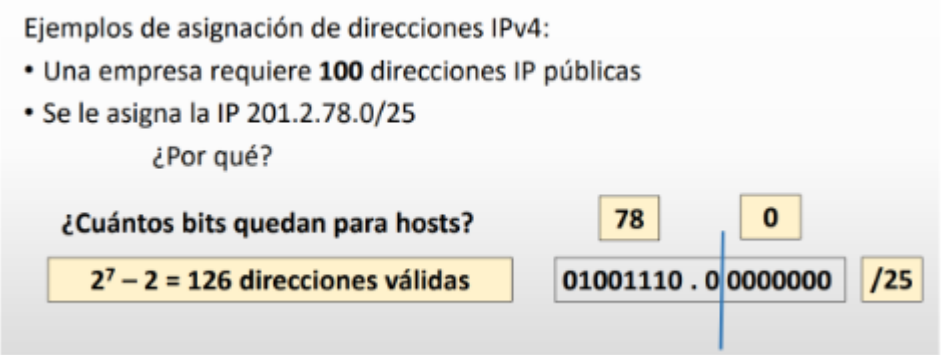
- Un ISP otorga más de una dirección pública a una red interna.

Tabla NAT con sobrecarga			
Dirección IP local interna	Dirección IP global interna	Dirección IP local externa	Dirección global externa
10.0.0.2:1331 10.0.0.4:1555	179.9.8.80:1331 179.9.8.80:1555	202.6.3.2:80 128.23.2.2:80	202.6.3.2:80 128.23.2.2:80

2. CIDR

Classless Inter Domain Routing, se buscaba lograr encaminamiento entre dominios sin usar clases, distribuyendo geográficamente las direcciones públicas que aún no se habían asignado. Al quedar tan pocas sobrantes, y al haberse desperdiciado muchas direcciones por el uso de clases (una red de clase B, por ejemplo, permitía 2^16 hosts, y muchas veces esas direcciones no se llegaban a ocupar), el direccionamiento se comenzó a hacer a nivel de bits, según la cantidad de hosts necesarios en una red, y ya no según la clase de la dirección. Esto logró repartir las direcciones sobrantes en bloques de tamaño variable, reduciendo las tablas de encaminamiento de los routers y agilizando la transmisión de paquetes. Permite implementar la sumarización de rutas.

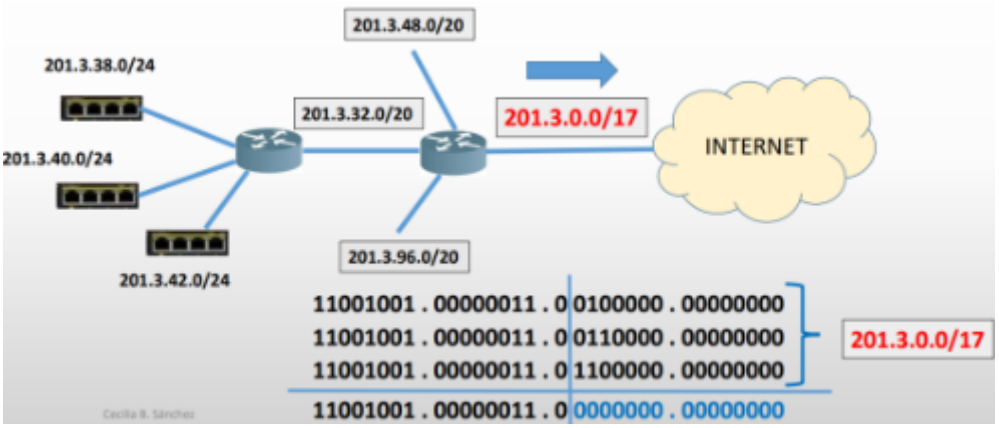
Por ejemplo, si una empresa necesita una red con 500 direcciones públicas, necesitaríamos una red clase B (con una C, tendríamos hasta 2^8 = 128 hosts), que permite 2^16 = 65536 hosts, y sólo necesitamos 500. Es un desperdicio. Por lo tanto, aplicamos CIDR, y si tenemos una dirección como 201.2.76.0, nos enfocamos únicamente en cuántos bits de host necesitamos. 2^9 = 512 - 2, nos sobran apenas 10 hosts. Esto implica mucho menos desperdicio que usar una clase B. Por lo tanto, asignamos 9 bits para host, lo que nos deja con 16 + 7 = 23 bits para red. Así, obtenemos la dirección de red 201.2.76.0 /23



Subnetting: desplazar la máscara hacia la derecha, se agranda.
Supernetting: desplazar la máscara hacia la izquierda, se achica.

Sumarización de rutas

Es un resumen de rutas, el administrador de red debe configurarla en el router. Al tener varias direcciones de red, se buscan los bits que coincidan desde el inicio. Al encontrar un bit diferente, se marca el final del resumen. La máscara será la cantidad de bits iguales, y desde el corte en adelante van todos 0. Esto lleva a tener un encaminamiento más rápido, al encontrar rutas más rápidamente.

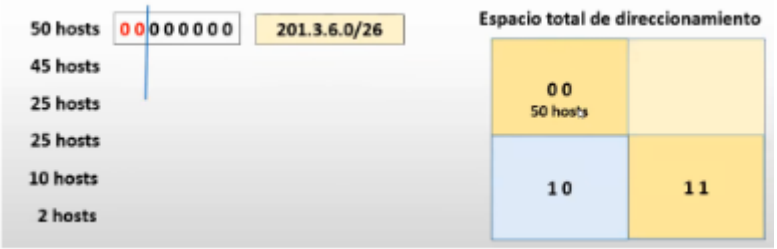


Básicamente, es una dirección IP que abarca varias direcciones.

3. VLSM - Variable Length Subnet Mask

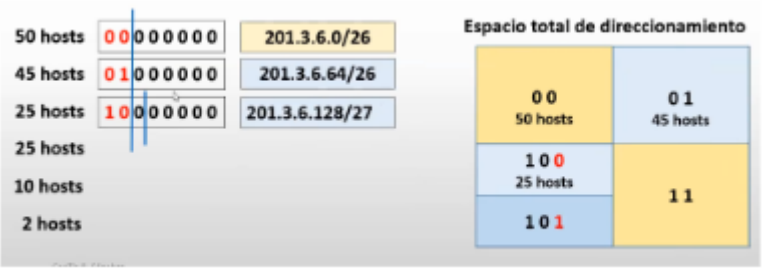
Permite crear esquemas de direccionamiento eficientes y escalables, creando subredes dentro de subredes en las redes públicas. Se obtiene un nivel más de jerarquía. Se usan máscaras largas para direcciones de pocos hosts, y viceversa.

a) Ponemos en orden de mayor a menor la cantidad de hosts necesarios en cada subred.
b) Siguiendo el orden, vemos cuántos bits para hosts necesitamos en cada subred.



Determinamos la dirección de subred, con su máscara y el rango válido. Sigo resolviendo hacia abajo, hasta notar que necesito menos bits para hosts.

c) Al notar que necesito menos bits, debo cambiar de subred y recalcular lo del paso b. Es decir, recalcular la máscara y el resto de las configuraciones.



4. IPv6

IEEE 802.1q y VLANs

Técnica que consiste en crear redes virtuales en una misma red física, provocando la separación de dominios de broadcast, aumentando la seguridad y dando orden y organización a áreas lógicas de empresas. Se crean con switches administrables, que se conectarán con otros de otras VLANs mediante routers. Cada VLAN formará parte de una red o subred.

La norma 802.1q de etiquetado de trama es un protocolo en el que se les agrega una etiqueta a las tramas enviadas, la cual es útil para los switches troncales para identificar a qué VLAN pertenecen.

Tenemos dos tipos de VLAN:

- Estáticas: se configura cada puerto especificando a qué VLAN pertenece.
- Dinámicas: se configuran con un servidor.

IPv6

Con el agotamiento de direcciones IPv4, vino la aparición de IPv6, un nuevo protocolo que permite mayor espacio direccionamiento y un manejo más eficaz de direcciones en los routers. Son direcciones de la forma

2001:0DB8:AC10:FE01:0000:0000:0000:0000

con 8 grupos de 16 bits, escritos en hexadecimal.

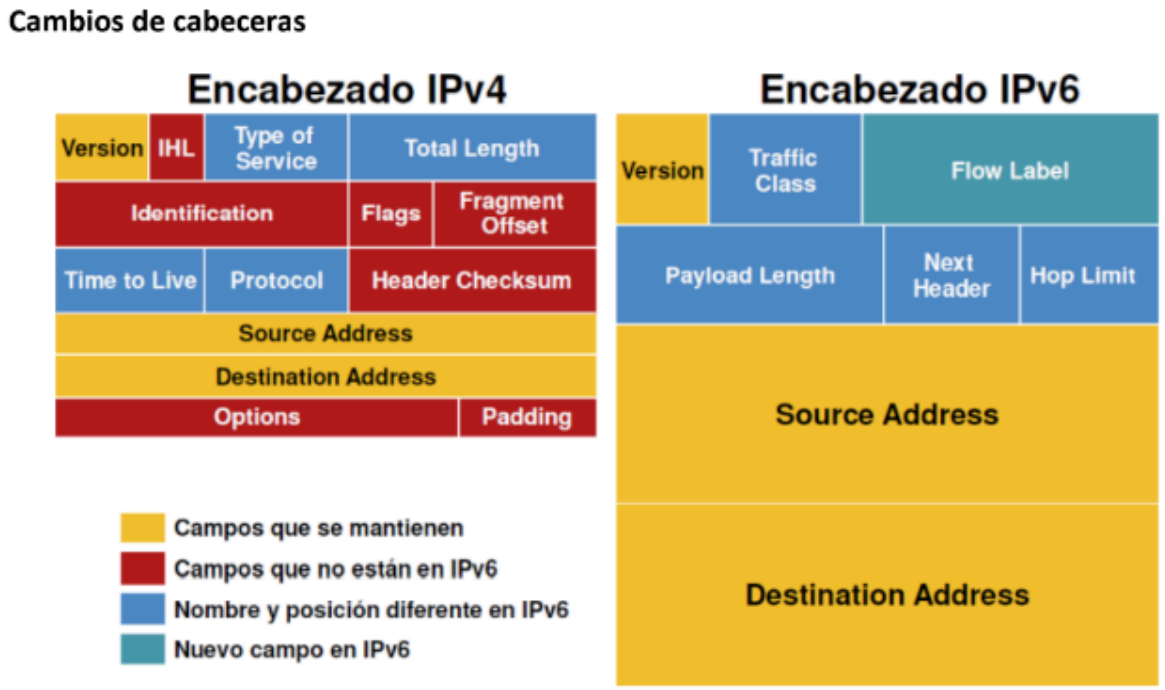
IPv6 permite:

- Más hosts
- Tablas de enrutamiento más pequeñas, al usar sólo los primeros bits de la dirección para encaminar
- Menos cabeceras
- Más seguridad
- Compatibilidad con la versión 4

Características:

- Alcance y flexibilidad global: un dispositivo puede tener más de una IP, las cuales se dividen en locales (FE80), únicas para comunicaciones locales, no encaminadas en Internet, como una dirección privada (FC_ _) o globales (2___).
- Implementa sumarización
- Plug and play
- End to end sin NAT, ya que NAT era una técnica para el agotamiento de direcciones IPv4
- Cabecera más simple
- Encaminamiento eficiente por zonas geográficas
- No hay broadcast, sí direcciones multicast
- No hay checksum
- Cabecera de extensión
- Etiquetas de flujo

Cabecera



Ahora el tamaño del paquete es fijo, por lo que IHL ya no nos sirve. No se usa fragmentación ni el checksum ya que los routers no se encargan más de la integridad. Opciones también se eliminó, pero por cabecera de extensión se puede agregar. Traffic access era Type of service. Next header era protocol, y Hop limit era TTL. Se agrega el flow label o etiqueta de flujo, que sirve para identificar a todos los paquetes de un mismo flujo.

Podemos tener 3 tipos de direcciones:
- unicast
- multicast, uno a muchos, comienzan con FF
- anycast, hacia máquinas con la misma dirección IP

Resumen de prefijos:

Tipo de dirección	Prefijo binario	Notación IPv6
No especificada	00…0 (128 bits)	::/128
Loopback	00…1 (128 btis)	::1/128
Multicast	1111 1111	FF00::/8
Unicast local de enlace	1111 1110 10	FE80::/10
ULA (Unique Local Address)	1111 110	FC00::/7
Unicast Global	001	2000::/3
IPv4-mapeada	00…0:1111 1111:IPv4	::FFFF:139.1.56.3/128
Unicast Local de Sitio (desuso)	1111 1110 11	FEC0::/10
IPv4-compatible (desuso)	00…0 (96 bits)	::113.45.5.6/128
Prefijo de Documentación	0010 0000 0000 0001 0000 1101 1011 1000	2001:DB8::/32

Estructura de IPs globales

Se divide en dos partes, 64 bits para el prefijo de red y otros 64 para la ID de la interfaz o host. El prefijo de red tiene su estructura: los primeros bits son 001, y luego trae el prefijo de enrutamiento global, que indica la zona geográfica, y por último el id de la subred. Tendremos, entonces, 2^16 subredes y 2^64 hosts. No se usan máscaras de red sino prefijos. Cualquier prefijo menor a 64 implica una ruta sumarizada, y uno mayor implica un prefijo de red.

La asignación de direcciones IPv6 puede ser por autoconfiguración sin estado o por autoconfiguración de ID de interfaz.

ICMP - Internet Control Message Protocol

Protocolo de capa de interred, usada para diagnosticar problemas de comunicación en la red. Nace porque IPv4 es un protocolo de máximo esfuerzo, por lo que si se pierden paquetes en la transmisión no avisa al origen. No hace control de errores, sino que lleva información de los errores e intenta informar por qué un paquete no llegó a destino y el estado de la red. Trabaja en conjunto con IP para que sea más fiable, con los siguientes paquetes:

- Mensajes de error
    - TTL excedido.
    - Problema de parámetro: error en la cabecera IPv4.
    - Source quench: permite el control de la congestión de la red, se envía al origen para pedir que baje la tasa de transmisión si el buffer del router se está llenando.
    - Redirect: para que un host pueda modificar momentáneamente su gateway, qwswredireccionar al router de salida correcto.

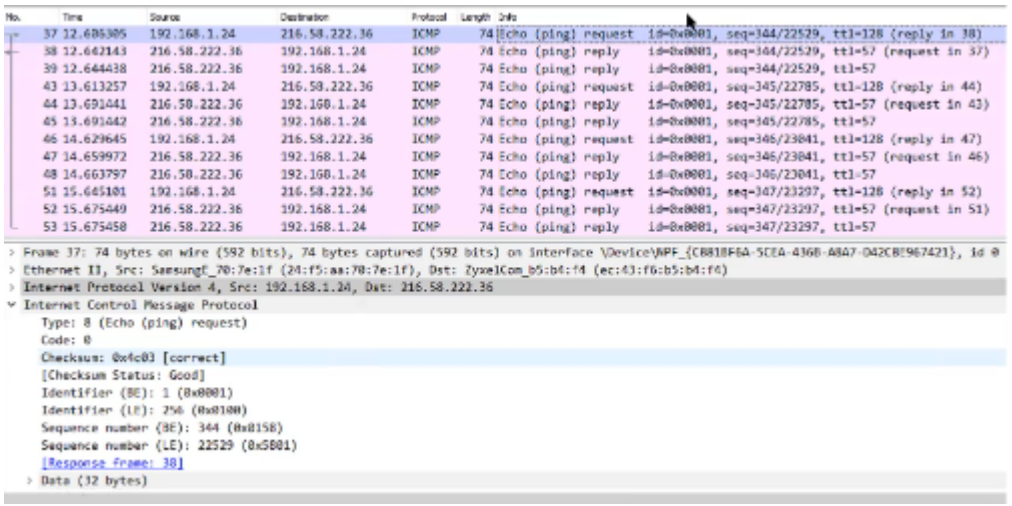
- Destino inalcanzable: informa que el paquete no llegó a destino, sea por red, host, protocolo o puerto inalcanzable, paquete muy grande (fragmentación necesaria) o destino desconocido.

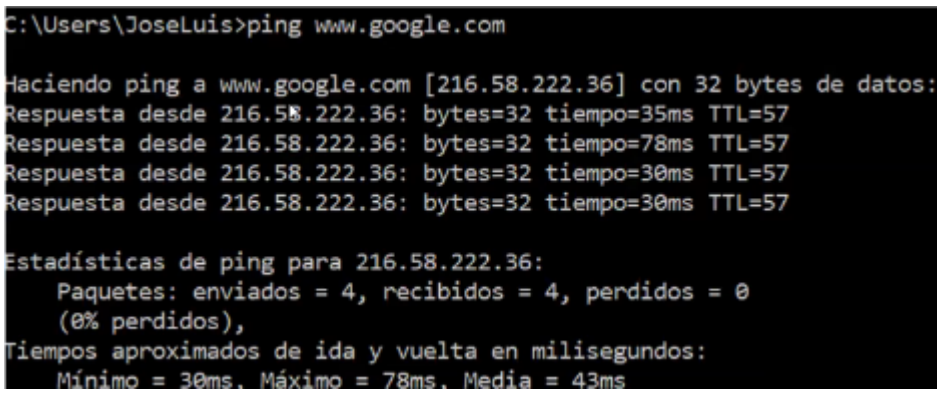
- Mensajes de información
  - Echo y Echo reply: enviado para comprobar la conectividad entre dispositivos. Forzado con los comandos tracert (Windows) y traceroute (Linux).
  - Solicitud de máscara de red
  - Respuesta de máscara de red

Los paquetes ICMP tienen la siguiente estructura:

Campo tipo y código o subtipo, indican el tipo de mensaje ICMP. Checksum para controlar la integridad del paquete y encabezado opcional. En datos se puede enviar información adicional o parte del mensaje original del paquete descartado.

Ping

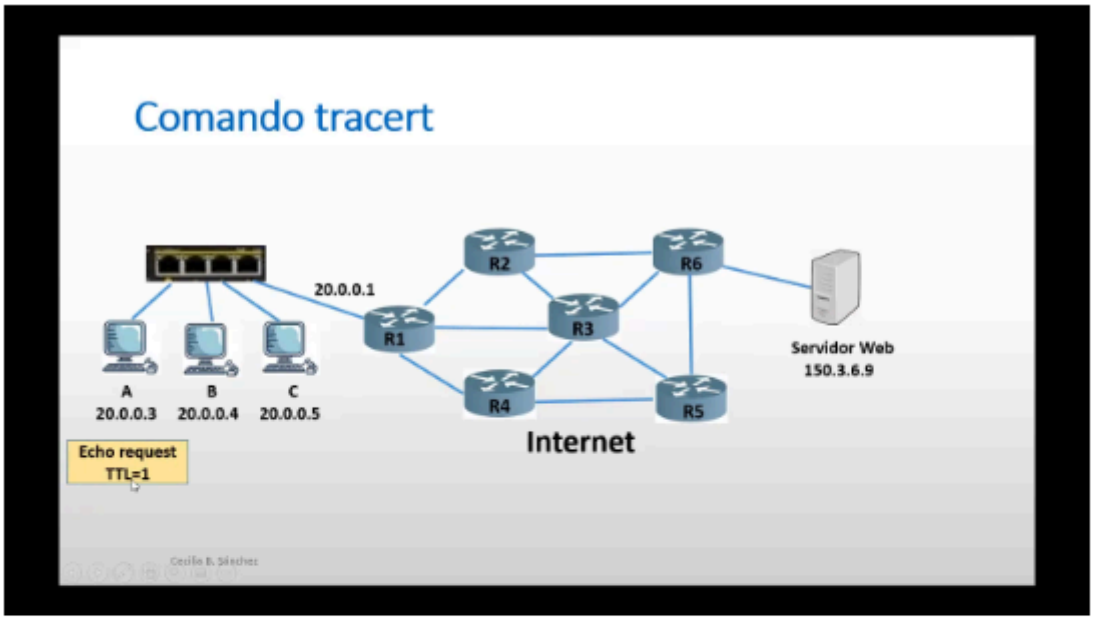




Tracert (o traceroute en Linux)

Determina la ruta que sigue un paquete para llegar a destino, mostrando las IPs intermedias

```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19042.1083]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Gonzalo Martínez>tracert www.google.com

Traza a la dirección www.google.com [172.217.172.100]
sobre un máximo de 30 saltos:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     2 ms     2 ms     2 ms  KAREN-GRILL.lan [169.254.1.2]
  3    20 ms    28 ms    33 ms  10.14.187.1
  4     *      357 ms     *     200.0.19.201
  5    56 ms    67 ms    56 ms  200.115.95.158
  6    35 ms    37 ms    38 ms  172.253.53.17
  7    44 ms    54 ms    43 ms  172.253.71.13
  8    42 ms    60 ms   127 ms  eze06s02-in-f4.1e100.net [172.217.172.100]

Traza completa.

C:\Users\Gonzalo Martínez>_
```



- La máquina A ejecuta un tracert al servidor.
- El primer paquete que manda, le pone TTL=1. Ese paquete llega al router uno y el TTL disminuye en 1. El TTL llega a 0 y el router construye un mensaje ICMP de tipo tiempo excedido y se lo manda a la máquina A.
- La máquina A descubre quién es el primer salto.
- Cuando llega el paquete, construye otro paquete con TTL=2. Y así va a ir armando el camino.
- Finalmente, llega al servidor. El servidor web manda un echo reply, no uno de tiempo excedido.
- Cuando llega la respuesta echo reply, la máquina A ya no sigue controlando o aumentando el TTL

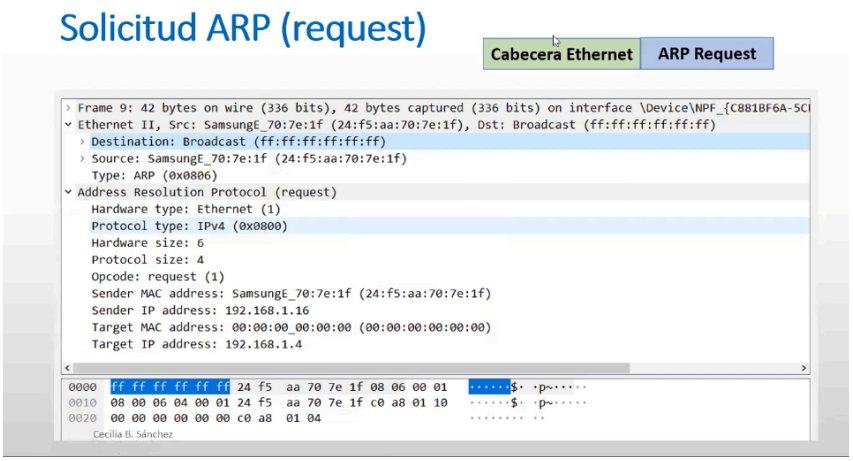
IGMP (Internet group messages protocol) permite a los hosts comunicar si les interesa o no pertenecer a grupos multicast de forma dinámica.

ARP - Address Resolution Protocol

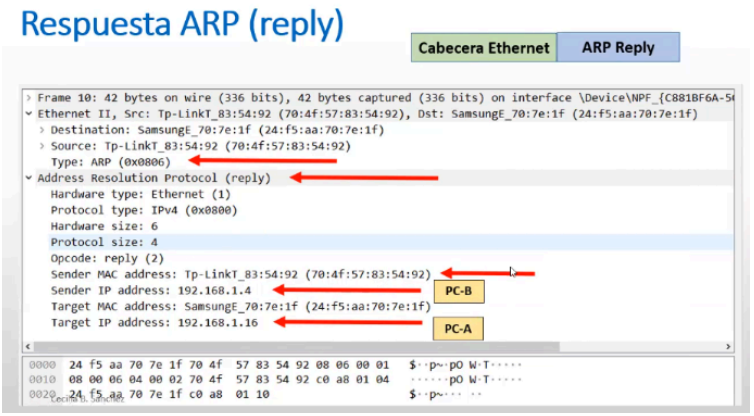
Protocolo de capa de enlace. Se usa para averiguar la MAC de un dispositivo, a través de una dirección IP. El host debe estar en la misma red, y si no lo está y necesito salir

a la Internet, la tabla guardará la IP y MAC del router gateway. A través de una trama ARP Request enviado en formato de broadcast a todos los hosts de la red, el cual será contestado únicamente por el host dueño de la IP a través de una trama ARP Reply con la dirección MAC. Esta información se guarda en la tabla ARP del host. Funciona parecido a las tablas CAM de los switches.

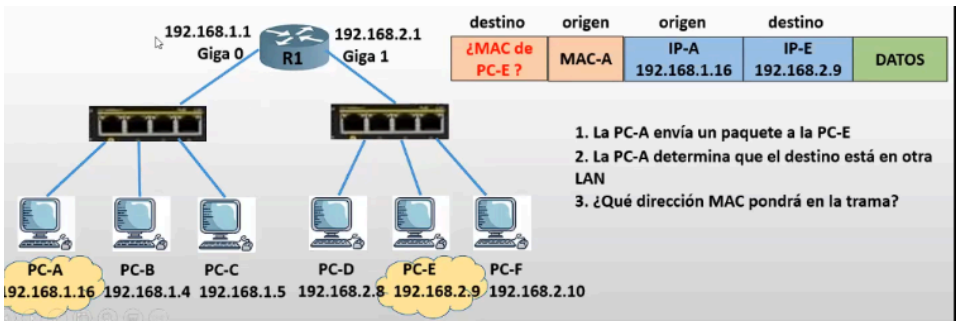
- Qué hace el protocolo:
    - 1 - La PC-A consulta la tabla ARP.
    - 2 - Si está la MAC de la PC-B, la usa para encapsular.
    - 3 - Si no está envía una solicitud ARP (broadcast)
        - Sólo responde la PC B, con una respuesta ARP. Esa respuesta ya es unicast. Va dirigida a la PC-A.
        - La PC-A actualiza su tabla ARP, y ahora ya tenemos la MAC-B

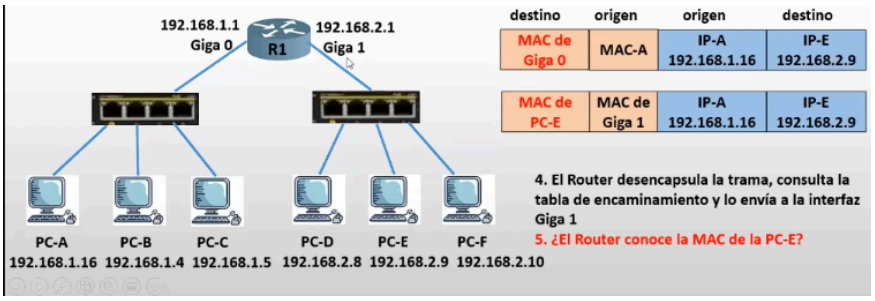


- Funciona en la capa de enlace
- Vemos que es broadcast



- ¿Qué sucede si el destino está en otra LAN? ¿Cómo averiguar la MAC del destino? La única forma de llegar a otra red es a través de la puerta de enlace, entonces la trama va a viajar de la PC-A hasta la interfaz del router o gateway. Por esto es importante configurar gateway, porque si no, no van a poder tener conectividad hacia afuera. Si la máquina tiene configurada la puerta de enlace, entonces va a encapsular en la mac del router. Así se trabaja cuando el destino está en otra red.





- Después, desencapsula el router. El router va a mirar la IP de destino, consulta la tabla de encaminamiento, y sale por la interfaz Giga1.
- Después, el router lo va a encapsular en otra trama, donde la mac de origen va a ser la mac de giga 1. Entonces, se va a fijar si tiene la mac de la PC-E en su tabla ARP (tiene dos tablas en este caso, una tabla ARP de la lan de la izquierda y otra tabla ARP de la LAN de la derecha). Si tiene la MAC, envía el paquete, si no, envía una petición ARP y después envía el paquete.

Sobre las tablas ARP:

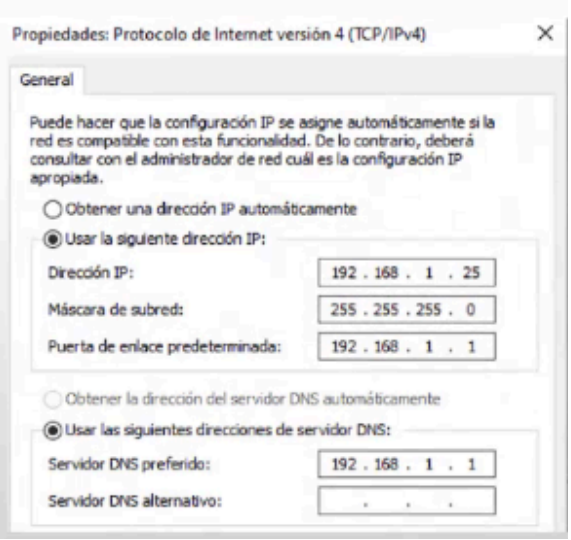
- Las entradas no son permanentes, tienen un temporizador. Esto es porque si el administrador le cambia la placa de red de una computadora, la dirección IP de la máquina sigue siendo la misma pero la MAC cambió. Cada dos minutos se borran los registros.
- Opciones del comando arp
    - -s: define una entrada estática. Esto quiere decir que le asocio una entrada estática. Entonces le digo arp -s ip mac. Esto va a quedar grabado en el dispositivo. No va a desaparecer la entrada. Cuando se inicia una computadora, va a estar vacía la tabla ARP, excepto las ip estáticas.
    - -d: elimina entradas de la tabla. Comando: arp -d * (el asterisco es por todos, pero también puede ser una entrada en particular)
    - -a: visualiza la tabla ARP.

Se utiliza el comando arp -a , se conforma de la dirección IP, la dirección MAC y el tipo de entrada (estática o dinámica)

```
Interfaz: 192.168.1.16 --- 0x13
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1           ec-43-f6-b5-b4-f4     dinámico
  192.168.1.3           5c-93-a2-7a-fe-95     dinámico
  192.168.1.4           70-4f-57-83-54-92     dinámico
  192.168.1.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

Métodos de configuración de direcciones

- Estáticos
  Se configuran IPs de manera estática, para que si un dispositivo inicia, ya tenga una dirección asignada. Así, ya conocemos de antemano la dirección, pero si la red cambia hay que reconfigurarlo.



```
netsh interface ip set address "Description" static %adresse% %netmask%
%gateway% %metric%
```

- **Description**: designa un texto que describe el nombre de la conexión.
- **%adresse%**: designa la dirección IP.
- **%netmask%**: representa la máscara de la subred.
- **%gateway%**: representa la dirección IP de la puerta de enlace.
- **%metric%**: representa el *metric* de la tarjeta de red (por lo general igual a 1).

Por ejemplo:

```
netsh interface ip set address "Red local" static 192.168.0.3 255.255.255.0
192.168.0.1 1
```

RARP - Reverse Address Resolution Protocol

Es un protocolo para asignar IP a dispositivos que no tienen discos rígidos, a partir de su dirección MAC. Es el inverso de ARP, ya que tendremos un servidor RARP con una tabla que relaciona una dirección MAP con una IP. Es lento y se necesita un servidor por cada LAN.

BOOTP - Bootstrap Protocol

Reemplazo de RARP, funciona muy parecido, pero ahora no hace falta un servidor por LAN. Las tablas se configuran en un servidor BOOTP, pudiendo ahora configurar servidor DNS, gateway, y otros parámetros. Es un protocolo cliente servidor de la capa de aplicación, que corre sobre UDP en puertos 67 y 68.

- El cliente inicia y determina su dirección MAC.
- Envía un mensaje BOOTP sobre UDP al medio.
- Al llegar al servidor, éste busca la MAC en su tabla.
- El servidor completa los campos del mensaje con la dirección IP y la ruta del archivo del sistema operativo a descargar.
- El cliente obtiene su dirección y el S.O. desde un servidor TFTP.

Como desventaja, tenemos que cargar manualmente las relaciones IP-MAC, lo que complica los cambios y traslados. Necesitamos un administrador de red.

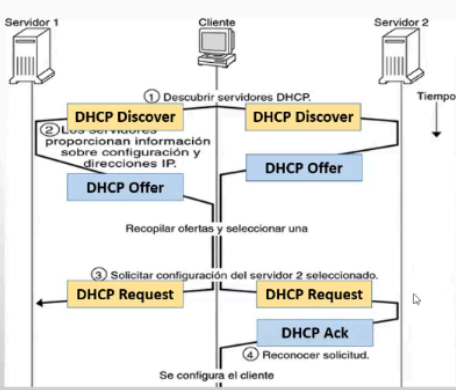
- Dinámicos
  Se obtiene una nueva dirección IP desde un servidor cada vez que un dispositivo inicia.

DHCP - Dynamic Host Configuration Protocol

Protocolo cliente-servidor de capa de sesión que trabaja en los puertos 67 (servidor) y 68 (cliente). Ofrece direcciones IPs temporales a los hosts con 3 formas de trabajo, manual, automática y dinámica. Al terminar de usarlas los hosts, se liberan para poder ser ofrecidas por el servidor otra vez.

1. El cliente inicia sin IP, envía a los servidores DHCP un mensaje para encontrarlos, DHCP Discover.
2. Los servidores responden ofreciendo direcciones IP y otros parámetros de configuración temporales, DHCP Offer.
3. El cliente pide la configuración de la dirección al seleccionar una, la primera que llega, DHCP Request.
4. El servidor valida si está todo bien y envía un DHCP Ack.

Si el servidor no acepta la dirección elegida por el cliente (por ejemplo, porque justo otro host ya la pidió) puede responder con DHCP Nack. Con DHCP Decline, el cliente informa al servidor que una de las IPs ofrecidas ya está en uso. Con DHCP Release, el cliente libera la IP porque ya no la necesita. y DHCP Inform se usa para que el cliente consulte al servidor la configuración local.



DHCP Relay es una configuración del router para que una PC que no está en el mismo dominio de broadcast del servidor DHCP pueda conectarse a él.

Comandos en Windows

```
Ejemplos:
    > ipconfig                    ... Muestra información.
    > ipconfig /all               ... Muestra información detallada.
    > ipconfig /renew             ... Renueva todos los adaptadores.
    > ipconfig /renew EL*         ... Renueva cualquier conexión cuyo nombre
                                      comience con EL.
    > ipconfig /release *Con*     ... Libera todas las conexiones
                                      coincidentes, por ejemplo:
                                          "Conexión cableada Ethernet 1" o
                                          "Conexión cableada Ethernet 2".
```

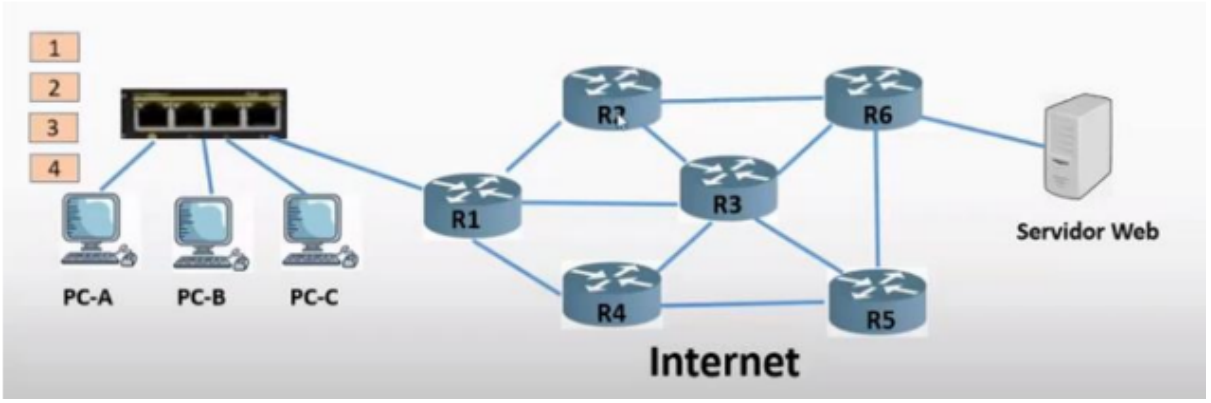
- renew: la máquina hace todo el proceso de asignación de IP de nuevo.
- release: libera la dirección IP. Si después de este comando, mando ipconfig va a mostrar que no tiene conexión de red. IP = 0.0.0.0

Unidad 4: Capa de Interred - Encaminamiento y congestión

Encaminamiento

Búsqueda de rutas desde un origen a un destino para buscar la más adecuada, considerando varios caminos posibles y aspectos como costo, retardo de un camino y criterio administrativo. Es una de las funciones principales de la capa de interred de TCP/IP.

Para poder encaminar, se puede representar la topología de red como un grafo, en el que los routers son los nodos y los enlaces son los arcos.



Podemos encontrar redes de circuitos virtuales o de datagramas.

- Redes de circuitos virtuales:
  Se establece una conexión, se transfieren los datos y finaliza la conexión. El primer paquete va “abriendo camino”, a medida que los routers van creando sus tablas de encaminamiento, habiendo desencapsulado sólo el primer paquete. Los demás viajan sobre el mismo camino, en orden. Se reserva el ancho de banda para toda la transmisión Es rápido pero si se cae un nodo, se pierde el camino y hay que crear un nuevo circuito.
- Redes de datagramas:
  O conmutación de paquetes, son no orientadas a conexión, lentas pero robustas. No importa si un nodo se cae, el paquete se puede enviar por otro camino, pero es lento porque los routers deben desencapsular cada paquete que llega hasta la cabecera IP para saber el destino (ya que no hubo otro paquete que llegó primero e indicó el destino), consultar la tabla de encaminamiento, volver a encapsular y enrutar el paquete. Los paquetes llegan desordenados, sólo se ordenan por TCP en la capa de transporte.

Algoritmos de encaminamiento

El router debe decidir por qué interfaz o camino enrutar cada paquete que llega. Esta decisión, qué algoritmo usar para enrutar, la toma considerando diferentes requisitos:

- Exactitud: que lo haga correctamente, apuntando al destino correcto.
- Sencillez: que elija un camino que no consuma tantos recursos, que sea liviano.
- Robustez: teniendo en cuenta que las redes son dinámicas y un router puede desconectarse, que el algoritmo elegido se adapte a los cambios, que sea tolerante a fallas.
- Estabilidad: que no cambie las tablas de encaminamiento y llegue a un estado de convergencia.
- Equidad: que trate a los paquetes de igual prioridad con equidad.
- Eficiencia: que aproveche los recursos de la red de manera óptima.

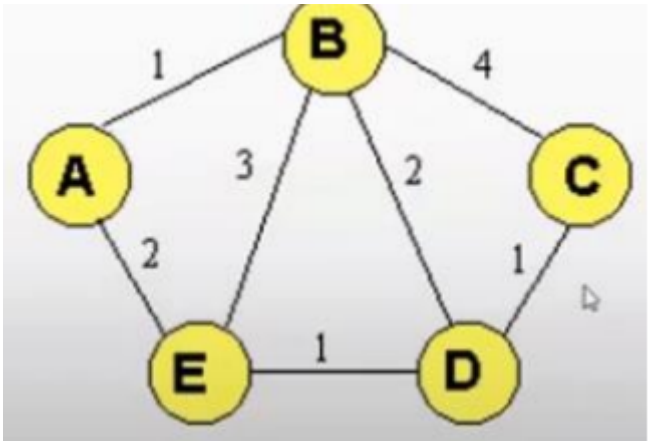
Estado de convergencia (de un router): que el router, luego de ser inestable al principio, logra armar su tabla de encaminamiento y sabe llegar a toda las redes. Una red estable es una red que siempre enruta por los mismos enlaces, que las tablas de encaminamiento no cambian.

Tipos de encaminamiento

- Estático

  Las tablas de enrutamiento son configuradas manualmente por el administrador de red. No es robusto, pero es simple y se conoce el movimiento de la red de antemano.

  1. Basado en flujo
     Se consideran métricas asignadas a los enlaces: número de saltos, distancia, tráfico promedio, ancho de banda (deberíamos elegir el camino que tenga mayor B, pero como se eligen los enlaces con menor valor, podemos eleva el valor de B a la -1 para que quede como una fracción), costo, retardo promedio.



  2. Algoritmo de inundación

A un router le llega un paquete y lo retransmite por todas las interfaces excepto por la que llegó. Se puede controlar con un contador de saltos para evitar bucles, o usar Spanning Tree. Es robusto, rápido y garantiza que el paquete llegue a todos los nodos, pero consume mucho ancho de banda. Hay que implementarlo con un control para evitar bucles, normalmente con un TTL o con número de secuencia a los paquetes.

3. Algoritmo jerárquico
   Plantea que los routers se agrupen en regiones. Cada router sabe cómo llegar a las redes de su región y cómo llegar a un router de otra región, no su estructura interna.

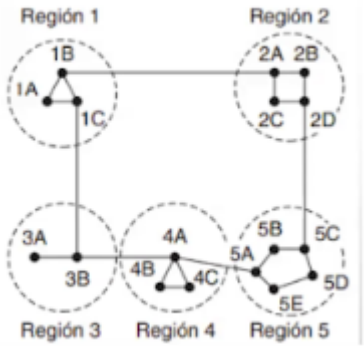


Tabla completa para 1A

Dest.	Línea	Saltos
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

Tabla jerárquica para 1A

Dest.	Línea	Saltos
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

Con el algoritmo, la tabla es mucho más corta.

- Dinámico

  Es robusto y se adapta, pero consume muchos recursos del router. Se subdivide en centralizado (un router decide el enrutamiento e informa a los demás), distribuidor (es colaborativo, los routers vecinos comparten sus tablas de enrutamiento) o aislado.

  1. Vector distancia o Bellman Ford. **RIP, BGP, IGRP.**

Algoritmo dinámico distribuido. El router que lo aplica no conoce la topología de la red, sólo cómo y cuánto le cuesta llegar a otra red, según alguna métrica. Tiene actualizaciones periódicas (cada 30s por defecto) para detectar cambios de la red. Al no conocer la topología real, pueden generarse bucles, que se pueden solucionar con criterios de corte. Converge lentamente, ya que al ser distribuido, los routers les “cuentan rumores” a sus vecinos hasta que la red converge.
Las métricas usadas para calcular costos son cantidad de saltos, retardo y longitud de la cola de paquetes.
Pueden generarse bucles por una “mala interpretación”; como las actualizaciones periódicas se realizan simultáneamente en diferentes routers, un router A puede avisarle a B que una red X está caída. Entonces, B borra esa red de la tabla de enrutamiento. Sin embargo, justo al mismo tiempo, B envía a A información de cómo llegar a la red X a través de él, creyendo que no está caída. Entonces, A agrega a su tabla de enrutamiento que a la red X se puede llegar con un salto (a través de B). Así comienza el **problema de la cuenta a infinito**; la métrica de cómo llegar a X crece. Esto también puede provocar bucles, ya que el router A le enviará un paquete a B para que llegue a la red X, y B se lo devolvería a A porque cree que él puede transmitir el paquete, y así. Para esto, se usan como criterios de corte:

- Contador de saltos, llegado a un máximo (normalmente 16 saltos) se descarta el paquete.
- Horizonte dividido, si el router A sabe de una red caída, sólo ese router podrá enviar nueva información de la red.
- Envenenamiento de rutas, el router avisa a los vecinos que una red está caída y “envenena” ese camino para que no se transmita hacia allá.
- Temporizador de espera, si se cae una ruta el router avisa a los vecinos, pone un temporizador y si la ruta sigue caída, la borra de su tabla de enrutamiento.

2. Estado de enlace. **OSPF.**
Algoritmo dinámico distribuido. Cada router conoce la topología de la red, y arma un paquete LSP (paquete de estado de enlace) con información sobre él mismo y la distancia a sus vecinos, el cual envía por inundación. Las actualizaciones se realizan con este paquete sólo al ocurrir eventos y cambios en la topología. Consume muchos recursos al necesitar mantener información sobre la topología, e implementa el algoritmo de Dijkstra para armar un grafo de la red y calcular la ruta más corta, pero no presenta bucles y converge más rápidamente al trabajar por inundación. Como métrica se considera el costo de enlace por ancho de banda.
    1. Un router envía un paquete HELLO para conocer a sus vecinos, direcciones y protocolo con el que trabajan.
    2. El router, al descubrir a sus vecinos, mide los costos a cada uno con paquetes ECHO y luego calcula promedios de costos.
    3. El router construye el paquete LSP con la IP de los vecinos y los costos de los enlaces. Este paquete tiene una identificación del router que lo construye, la versión del paquete (para descartar viejos y

desactualizados), la edad (algo como el TTL) y la información de los routers.

4. El router inunda la red con ese paquete. Esto ocurre simultáneamente en todos los routers de la red.
5. Al tener toda la información todos los routers, construyen un grafo de la red y con Dijkstra calculan los caminos más cortos a otros routers y arman sus tablas.

Al conectar un nuevo router a la red, éste no ejecuta todos estos pasos sino que pide a los vecinos datos de la topología para ahorrar tiempo. Además, los routers envían paquetes HELLO (o keep alive) continuamente a sus vecinos para saber su estado.

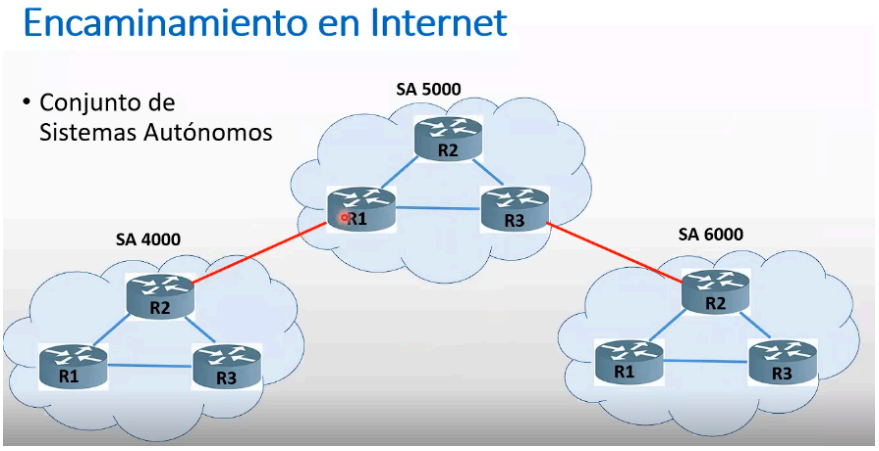
3. Algoritmos híbridos. **EIGRP.**

Principio de optimalidad: si B está en la ruta óptima de A a C, entonces la ruta óptima de B a C está incluida en la primera.

Un protocolo enrutado es aquel que transporta datos a través de la red. Un protocolo de enrutamiento es aquel que permite a un router encontrar la ruta más óptima de un origen a un destino.
Un protocolo de enrutamiento es un conjunto de reglas mediante las cuales un router se comunica con otro para intercambiar información, construir y mantener tablas de enrutamiento. Un algoritmo de enrutamiento es un proceso que permite decidir por qué línea de salida transmitir un paquete, en base a la información obtenida por los protocolos de enrutamiento.

Encaminamiento en Internet

Un sistema autónomo es un conjunto de routers de una misma unidad organizativa o empresa, que tienen la misma política de administración y el mismo protocolo de enrutamiento. Tienen un número único de sistema autónomo otorgado por la IANA, de 16 o 32 bits. Se organizan en jerarquía, en la que el nivel 1 es troncal y debería llegar a todas las redes de Internet. Existen protocolos que interconectan SA.

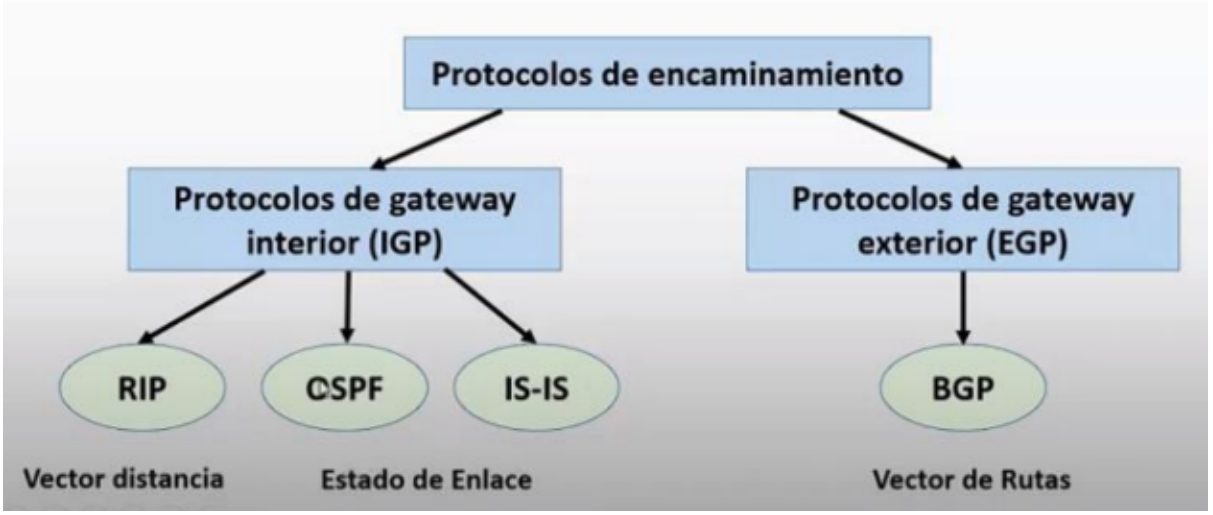


La distancia administrativa es un valor establecido por el fabricante de cada router que nos sirve para desempatar si encontramos más de una ruta óptima según diferentes métricas.

PROTOCOLO	DISTANCIA ADMINISTRATIVA
Redes directamente conectadas	0
Rutas estáticas	1
OSPF	110
IS-IS	115
RIP	120

No es lo mismo distancia administrativa que métricas:

- Si yo estoy comparando dos caminos que tiene 10 saltos y 7 saltos, voy a elegir la de 7 saltos. Tienen el mismo protocolo.
- Ahora, si yo aprendo que una ruta está a 10 saltos y otra a 1/2554 (ancho de banda de un enlace), no puedo compararlos. Entonces ahí entra en juego la distancia administrativa. Tienen distintos protocolos.



Protocolos de gateway interior

Se ejecutan dentro de un SA.

RIP - Routing Information Protocol

Protocolo del tipo vector distancia. Corre sobre UDP 520 y se usa en redes pequeñas. Usa como métrica un contador de saltos con máximo de 15. Este protocolo plantea que cada router envíe su tabla a los vecinos cada 30 segundos, y usa temporizadores de espera y envenenamiento de rutas para solucionar el problema de la cuenta a infinito. No soporta subredes ni máscaras variables. Usa 4 temporizadores variables: update (para las actualizaciones periódicas), invalid (tiempo necesario para que una ruta sea declarada como inválida), hold down (tiempo necesario para suprimir información de una ruta inválida) y flushed (tiempo necesario para borrar una entrada de la

tabla). Este protocolo implementa balanceo de cargas si se encuentran dos caminos óptimos.

RIP fue adaptándose a la aparición de diferentes tecnologías. Es necesario que todos los routers de una red tengan la misma versión de RIP.

- RIPv1:
  Es classfull, maneja las clases pero no soporta VLSM ni CIDR ya que las actualizaciones periódicas por broadcast no envían la máscara.
- RIPv2:
  Es classless, ya soporta máscaras de longitud variable. Las actualizaciones van por direcciones multicast 224.0.0.9. Además, se pueden autenticar las actualizaciones y soporta IPv6.

- R1#configure terminal
- R1(config)#**router** rip
- R1(config-router)#**network** 16.0.0.0
- R1(config-router)#**network** 18.0.0.0

Si deseamos trabajar con router RIPv2 se agrega el comando

- R3(config-router)#**version 2**

- Cada router debe publicar sus redes directamente conectadas.
  - Router 1:
    - R1#configure terminal
    - R1(config)#router rip (rip sería el protocolo. El (config) es el modo de configuración global)
    - R1(config-router)#network 16.0.0.0 (red que se va a publicar o enseñar a los otros routers. Por lo general se enseñan las redes que están directamente conectadas. El router 1 tiene dos).
    - R1(config-router)#network 18.0.0.0 (cada vez que se haga una actualización de encaminamiento le voy a estar enseñando sobre esa red)

RIP - Tabla de encaminamiento

```
Router_1700#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter are
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 5 subnets
C       172.16.4.0 is directly connected, Serial0
C       172.16.5.0 is directly connected, Serial1
R       172.16.1.0 [120/3] via 172.16.4.1, 00:00:22, Serial0
R       172.16.2.0 [120/2] via 172.16.4.1, 00:00:22, Serial0
R       172.16.3.0 [120/1] via 172.16.4.1, 00:00:22, Serial0
R    192.168.4.0/24 [120/2] via 172.16.4.1, 00:00:22, Serial0
R    192.168.5.0/24 [120/1] via 172.16.4.1, 00:00:22, Serial0
C    192.168.6.0/24 is directly connected, FastEthernet0
R    192.168.7.0/24 [120/1] via 172.16.5.2, 00:00:12, Serial1
R    192.168.1.0/24 [120/4] via 172.16.4.1, 00:00:24, Serial0
R    192.168.2.0/24 [120/3] via 172.16.4.1, 00:00:24, Serial0
```

- C y R (primer columna): cómo aprendió esa red:
  - C: Directamente conectada. No tiene que atravesar ningún router para atravesar
  - R: La aprendió a través del protocolo RIP.
- [120/3]
  - La métrica es 3 [120/3]. Así se grafica la métrica.
  - El 120 es la distancia administrativa.
- via 172.16.4.1: para llegar a la red lo tengo que ir por ese router 172.16.4.1 y lo tengo que sacar por mi interfaz Serial0.
- 00:00:22 (22 segundos): tiempo en que el router aprendió sobre esa red.

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 2 subnets
O        10.1.1.0 [110/2] via 192.0.2.2, 00:00:35, GigabitEthernet0/1
O        10.2.2.0 [110/2] via 192.0.2.2, 00:00:35, GigabitEthernet0/1
      192.0.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.0.2.0/24 is directly connected, GigabitEthernet0/1
L        192.0.2.1/32 is directly connected, GigabitEthernet0/1
D     192.168.1.0/24 [90/3072] via 203.0.113.2, 00:00:22, GigabitEthernet0/2
D     192.168.2.0/24 [90/3072] via 203.0.113.2, 00:00:22, GigabitEthernet0/2
      203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/24 is directly connected, GigabitEthernet0/2
L        203.0.113.1/32 is directly connected, GigabitEthernet0/2
R2#
```

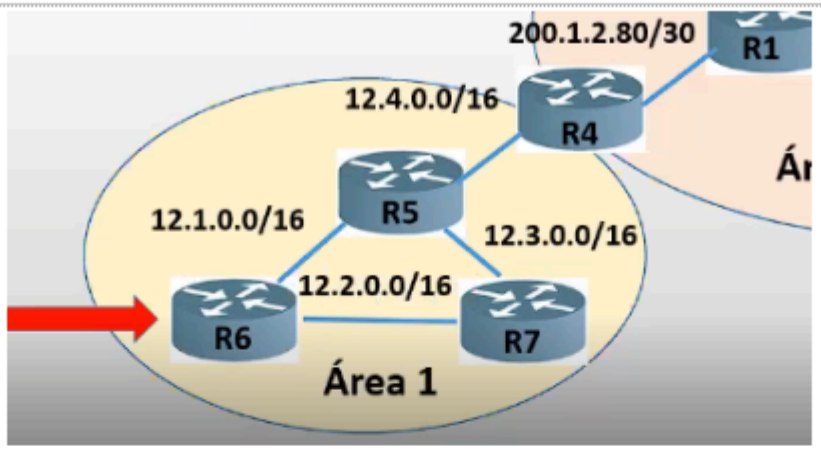
- L es de la propia interfaz
- C son aquellas que están directamente conectadas.
- Vemos que es un router multiprotocolo. Tenés el protocolo EIGRP y OSPF.

OSPF - Open Shortest Path First

Protocolo de estado de enlace. Corre sobre el puerto 89. Usa como métrica el ancho de banda y soporta VLSM y CIDR. Permite autenticar las actualizaciones de enrutamiento, las cuales se envían por multicast a 224.0.0.5 y 224.0.0.6. Envía los paquetes HELLO cada 10 segundos en enlaces WAN punto a punto, redes troncales. También considera los tipos de redes broadcast, LAN, para los usuarios. Se usa para redes más grandes, por lo que también se puede implementar un enrutamiento estático jerárquico.

Tenemos diferentes tipos de rutas: intra área (determinadas en el router), inter área (hacia el backbone) e inter SA (hacia el router frontera más próximo). Si mi SA es muy grande, conviene agruparlo en áreas para reducir el tamaño de las tablas. Existen dos niveles jerárquicos: backbone, troncal y está siempre en los SA como área 0, y áreas adicionales, que se comunican a través del área 0, como una topología estrella.
También tenemos routers *internos*, que encaminan dentro de un área, de *red troncal* que encaminan dentro del área 0, de *frontera de área* que conectan áreas entre sí y forman parte de la red troncal (resumen todas las redes de un área y envían el resumen a las otras áreas) y de *frontera de SA* que intercambian información de enrutamiento con routers de otros SA.

Configuración de OSPF



- Router6 (interno)
  - R6#configure terminal
  - R6(config)#router ospf 10. El número es el id de proceso que tiene identificado local.
  - R6(config-router)#network 12.1.0.0 0.0.255.255 area 1: acá publicamos las redes. El 0.0.255.255 es una máscara al revés. Es la inversa a la máscara (Máscara de wildcard). Esta máscara es potente. Permite filtrar paquetes que cumplen con ciertas características. Ejemplo: tenemos los dos primeros ceros adelante, quiere decir que esos 16 bits tienen que coincidir exactamente con los 16 primeros bits (12 1) de la dirección anterior. En el caso de la dirección 200.1.2.80 0.0.0.3: tienen que coincidir los primeros 30 bits exactamente con la dirección 200.1.2.80. También hay que indicarle a qué área pertenece.
  - R6(config-router)#network 12.2.0.0 0.0.255.255 area 1: va un network por cada red directamente conectada que tengamos (conexión entre R6 y R7. El anterior era con R5). Al asignar dos networks (o conexiones) entre routers de la misma área, el protocolo ya sabe que es un router interno.
- Router4 (ABR - de frontera de área)
  - R4#configure terminal
  - R4(config)#router ospf 15
  - R4(config-router)#network 12.4.0.0 0.0.255.255 area 1
  - R4(config-router)#network 200.1.2.80 0.0.0.3 area 0: acá el router pasa a ser un router de borde de área.

Protocolos de gateway exterior

BGP - Border Gateway Protocol

Protocolo orientado a conexión, corre sobre TCP en el puerto 179 y sirve para intercambiar información de enrutamiento entre sistemas autónomos. Soporta CIDR y sumarización de rutas. Implementa un algoritmo de vector de rutas basado en políticas definidas por el administrador de red. En las rutas, encontramos los identificadores de SA

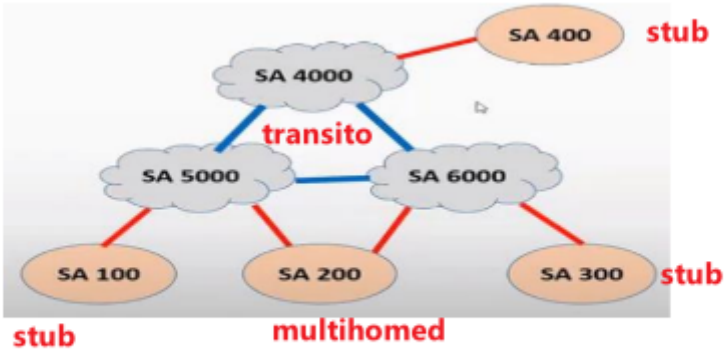
que el paquete debe atravesar para llegar a una red. La métrica es la cantidad de SA a atravesar. El objetivo del protocolo es encaminar por una cadena de SA evitando generar bucles, al descartar rutas que incluyan a su propio SA de la tabla.

Los pares BGP (routers vecinos) intercambian información de rutas manteniendo una sesión TCP activa todo el tiempo.

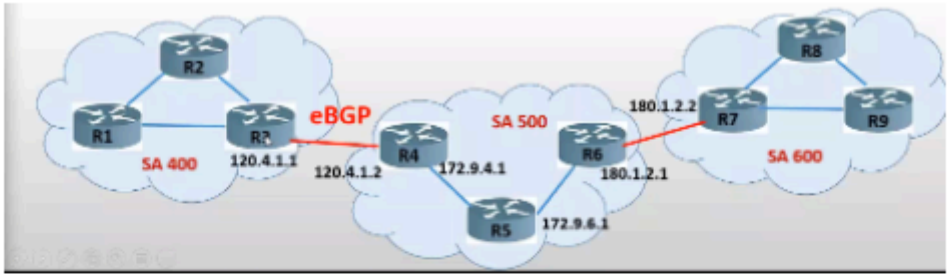
El algoritmo **vector de rutas** hace que los routers envíen anuncios de rutas cada 30 segundos en conexiones punto a punto. Estos anuncios informan la dirección de red en formato CIDR, una lista explícita de todos los SA que hay que atravesar para llegar a esa red y el router del próximo salto. Al llegar esta información a un router, de parte de uno o más routers vecinos, éste va a tomar y agregar a su tabla la ruta que tenga el camino más corto (la menor cantidad de SA a atravesar), luego de haber filtrado por las políticas que configuró el administrador.

Según cómo se conecten los SA, podemos tener tres tipos de redes:

- Stub: aquellos sistemas autónomos que sólo tienen un enlace hacia otro.
- Multihomed: aquellos que se conectan a más de un SA.
- De tránsito: suelen ser los ISP de nivel 1.



Configuración de BGP



- BGP maneja dos tipos de configuraciones: el externo y el interno
- Externo: interconecta dos sistemas autónomos distintos
- Router3
  - R3(config)#router bgp 400: 400 es porque tenemos que especificar a qué sistema autónomo pertenece ese router
  - R3(config-router)#neighbor 120.3.1.2 remote-as 500: esto es para configurar el par BGP. 500 es a que sistema autónomo pertenece.
- Router7:
  - R7(config)#router bgp 600
  - R7(config-router)#neighbor 180.1.2.1 remote-as 500
- Para que el 400 se comunique con el 600, tiene que atravesar el sistema autónomo 500. Para hacer esto, adentro del 500 se tiene que manejar información BGP. Esta es la configuración interna.
- Router4:
  - R4(config)#router bgp 500
  - R4(config-router)#neighbor 120.4.1.1 remote-as 400
  - R3(config-router)#neighbor 180.1.2.1 remote-as 500: esto es para que pueda atravesar. Vemos que pertenece al mismo sistema autónomo, y es por eso que se hace configuración interna (iBGP)
  - R3(config-router)#network x.x.x.x mask x.x.x.x: esto se hace en todos. Es para publicar redes. Las máscaras siempre tienen que estar sumarizadas.

El enrutamiento es de tránsito cuando se conectan ISPs de diferentes niveles. Es de peering si se conectan ISPs del mismo nivel.

Routers

Enrutamiento entre VLANs

Cada VLAN tiene una dirección de red o subred diferente. Los hosts de una VLAN no pueden comunicarse directamente con los de otra, a menos que los interconectemos con routers o switches de capa 3.

El enrutamiento entre VLANs es el proceso de permitir el tráfico de una VLAN a otra, y se hace a través de subinterfaces del router. Tendremos puertos de acceso y puertos troncales.

Congestión

La congestión se da cuando ingresa más información a una red de la que está preparada para procesar y encaminar. Cuando hay demasiados paquetes en una red o en parte de una red, aumenta el retardo y se degrada el rendimiento. Es una situación que va empeorando cada vez, porque al congestionarse una red de forma parcial o total, los acuses de recibo de paquetes (ACK) no llegan al origen, y éste vuelve a transmitir los paquetes, congestionando más la red.

La congestión se puede dar por diferentes factores, normalmente por routers con baja capacidad de memoria o con procesadores lentos, enlaces con poco ancho de banda o por modernización incompleta (comenzamos un recambio de tecnologías y queda algún router viejo con menor capacidad, que se convierte en cuello de botella). Lo ideal es que para controlar la congestión tengamos a la capa de red y la de transporte trabajando en conjunto, decidiendo qué hacer con los paquetes sobrantes y reduciendo la carga respectivamente.

Cada router va a tener dos buffers por interfaz; uno para los paquetes que llegan y otro para los que están por salir. Considerando esto, podemos intentar controlar la congestión de la red, para que pueda transportar todo el tráfico que ingresa. Además, podemos detectar la congestión a nivel de red (porcentaje de paquetes descartados o longitud media de las queues en los buffers de los routers) o a nivel de transporte (retardo medio, jitter, porcentaje de paquetes perdidos). Al presentarse congestión, esta se puede notificar de manera implícita, descartando paquetes, o explícita a través de paquetes informativos -piggybacked-.

Algoritmos de control de congestión

- Soluciones preventivas
  Buscamos aumentar los recursos o ajustar las rutas según patrones del tráfico, para prevenir la congestión y evitar que ocurra. Aprovisionamiento, enrutamiento consciente del tráfico.

- Soluciones reactivas
  Detectan, informan y corrigen. Son soluciones que se dan cuando la congestión ya existe en la red. El problema es identificar la congestión y avisar al origen del problema que pare de transmitir sin provocar más congestión. Reduciremos la carga a través del control de admisión, desprendimiento de carga y regulación del tráfico.

Control de congestión vs. control de flujo

El control de congestión garantiza que la red pueda transportar todo el tráfico que ingresa, e involucra a todos los dispositivos de la red. El control de flujo garantiza que un

emisor rápido no sature a un destino lento. Es un control de extremo a extremo, independiente del estado de la red, y sólo interesan emisor y receptor. En control de flujo, un receptor lento puede pedirle al emisor que baje su tasa de transferencia, es un control de capa de transporte.

Principios generales del control de congestión

- Métodos de ciclo abierto:
  El objetivo es que nunca se produzca la congestión, por lo que se implementa un buen diseño de red. Se controla lo que ingresa a la red, cuándo aceptar tráfico, cuándo descartar paquetes, qué paquetes descartar, independientemente del estado de la red. PREVENTIVOS.

- Métodos de ciclo cerrado
  Con retroalimentación de la misma red, para saber cuándo está congestionada a través del monitoreo constante. Estos métodos informan sobre la congestión a quienes pueden solucionar el problema, los transmisores de paquetes, y toman medidas correctivas. Para detectar, pueden hacer un análisis de retardo del acuse de recibo ACK de los paquetes, análisis de buffer de interfaces (colas de los routers), análisis de porcentaje de descarte de paquetes y análisis de temporizador. REACTIVOS.

  - Control de admisión: se aplica en redes de circuitos virtuales, en los que para una comunicación debe haber un establecimiento de enlace que ocupa y reserva recursos de los routers involucrados en el camino. Se rechazarán nuevas conexiones frente a una congestión.

    Y los siguientes se aplican en redes de conmutación de paquetes:
  - Notificación explícita de congestión: al detectar una interfaz congestionada, el router toma los paquetes IP y enciende 2 bits del campo Tipo de servicio (IPv4) o Clase de tráfico (IPv6) y los envía a destino. Cuando se reciben, el receptor activa un bit de la capa de transporte en los paquetes que van como respuesta al origen. Así, el origen sabe que debe bajar la tasa de transmisión.
  - Paquete regulador: el receptor, al detectar congestión, envía al origen paquetes ICMP de Source Quench, para pedirle que baje la tasa de transmisión. Los envía hasta que se descongestiona la red.
    ○ Paquete regulador que afecta al origen: como fue explicado.
    ○ Paquete regulador salto por salto: los routers intermedios entre destino y origen absorben parte de la congestión aliviando rápidamente al router congestionado.
  - Desprendimiento de carga: como último recurso, se descartan paquetes según el análisis de prioridad (campo prioridad). Se puede descartar frente a transferencia de archivos (es más importante un paquete viejo que uno nuevo), a multimedia en vivo (es más importante uno nuevo) o a transferencia de video.

- Detección temprana aleatoria - RED: se descartan conjuntos paquetes de manera aleatoria.

QoS - Calidad de servicio

Los paquetes que van desde un origen hacia un destino se pueden agrupar en flujos. Un flujo se identifica con dirección ip de origen y destino, puerto origen y destino y el protocolo de transporte usado. Son unidireccionales. Para brindar calidad de servicio, le prestamos atención a un flujo de paquetes que necesita más o menos requerimientos para su transmisión. Este no es un flujo cualquiera, no podemos brindar mejor calidad de servicio ni más recursos a cualquier tráfico, esto es sobreaprovisionamiento y es costoso. Por lo tanto, podremos brindar mejor calidad de servicio siendo selectivos con paquetes con mayor prioridad, los que transportan datos en tiempo real.

Para brindar QoS, hay que tener en cuenta los requerimientos de las aplicaciones, controlar el tráfico de la red para evitar que se congestione, cómo reservar recursos en los routers para mantener la performance y el permiso de aceptar o no más tráfico en la red.

Se dice que una red tiene calidad de servicio cuando el proveedor cumple con al menos uno de los aspectos definidos en el SLA (Service Level Agreement, contrato del usuario con el proveedor). Se define por los siguientes requerimientos:

- Ancho de banda
- Retardo, sensibilidad al retardo
- Jitter, sensibilidad al jitter
- Confiabilidad, sensibilidad a la pérdida

Técnicas para garantizar QoS

- Sobreaprovisionamiento
  El objetivo es construir una red con la suficiente capacidad para manejar cualquier tipo de tráfico. Es costoso brindar suficientes recursos al router, como memoria y procesador, o mejorar el ancho de banda de los enlaces, para evitar la congestión. Esta técnica hace hincapié en toda la red.
- Modelado de tráfico
  Implementado en servidores, busca regular la tasa promedio de paquetes y ráfagas de un flujo de datos que entran a la red. Esto se logra implementando patrones de tráfico; acuerdos entre usuario y proveedor sobre cuánto flujo de datos manejará el usuario. Se pacta una tasa máxima, y el proveedor deberá controlar que el usuario se mantenga dentro de lo acordado para poder seguir manteniendo la QoS pactada. Esto es supervisión de tráfico, y si hay exceso se pueden marcar paquetes para ser descartados en caso de congestión.
  - Algoritmo de cubeta con goteo
    Al llegar una ráfaga de paquetes, sin importar la rapidez con la que llegue, ingresará a una “cubeta” que gotea el flujo de salida a una tasa constante. La cubeta es el buffer del router, que es una cola finita que transforma un flujo desigual en uno continuo que transmite por cada pulso de un reloj, lo que

reduce la posibilidad de congestión porque no se largan todos los paquetes de golpe a la red. Si el buffer se llena, se descartan paquetes.

- Algoritmo de cubeta con ficha
  Surge porque el anterior no se adapta bien al tráfico real. Este se adapta mejor a las ráfagas de paquetes. La cubeta contiene fichas generadas por tiempo de reloj que no se transmita. Cada ficha es un derecho a transmitir un paquete en forma de ráfaga, que se irá acumulando por los hosts inactivos. Cada paquete enviado consume una ficha.

- Almacenamiento en buffer
  Implementado en el cliente, se basa en almacenar bytes en un buffer antes de entregarlos a destino, generando un retardo que atenuará el jitter, para que el destino no reciba los paquetes cortados sino todos juntos.
- Programación de paquetes
  Se implementa en los routers, se basa en reservar recursos en el circuito de los paquetes por la red, ya sea ancho de banda, espacio en los buffers o ciclos de CPU. El router coloca los paquetes en colas en los buffers. Hay 4 algoritmos de procesamiento de estas colas:
  - Algoritmo FIFO
    Primero en llegar, primero en salir. Si el buffer se llena, se descartan paquetes, y no brinda muy buena QoS ya que si llegan muchos paquetes de un origen, no permite la transferencia de otros flujos.
  - Prioridad
    Se marcan los paquetes con prioridad para ser enviados primeros. Para los de igual prioridad se aplica FIFO. Si llega una ráfaga grande de paquetes de alta prioridad, puede producir inanición, es decir, perjudica la transferencia de otros flujos.
  - Encolamiento justo - FQ
    Los routers tienen colas separadas, una por cada flujo de paquetes, y se exploran con round-robin, tomando el primer paquete de cada cola y enviándolo. Se pierde el concepto de prioridad.
  - Encolamiento justo ponderado - WFQ
    Igual que el anterior, pero tiene en cuenta las prioridades y envía más bytes de la cola con más prioridad.

Técnicas de QoS en Internet

Al comienzo, para dar trato preferencial a un usuario en una red, se usaban técnicas basadas en reserva o prioridad. La reserva daba garantía de QoS casi total, sin necesidad de etiquetas que hicieran más lento el proceso. Sin embargo, requería mantener información de estado de las transferencias y una forma de avisar y efectuar la reserva. En cuanto a la prioridad, los routers no necesitaban mantener información de estado pero sí necesitaba que los paquetes estuvieran marcados y darles un buen manejo a las prioridades.

La IETF buscó técnicas para brindar QoS en Internet, y usó el método de mejor esfuerzo y el de IntServ.

Mejor esfuerzo

En la definición de la cabecera IPv4, se incluyó el octeto ToS:

- Precedencia: prioridad (ocho niveles). Mayor es mejor
- D,T,R,C: flags para indicar la ruta que se quiere utilizar:
  - D: Delay (mínimo retardo)
  - T: Throughput (máximo rendimiento)
  - R: Reliability (máxima fiabilidad)
  - C: Cost (mínimo costo), RFC 1349
- X: bit reservado

Servicios Integrados

Tecnología capaz de manejar diferentes flujos extremo a extremo en una red, garantizando QoS para cada uno al reservar recursos para las transferencias de cada usuario. Esto se logra con RSVP - Reservation Protocol, un protocolo de señalización. Este protocolo hace que en la transmisión se establezca una especie de camino o circuito virtual, aunque IP es no orientado a conexión, para mantener a los paquetes de un mismo flujo moviéndose por un mismo camino, para reducir el retardo. En este camino se hace una reserva de recursos, para la cual los routers deben mantener información de estado. Los routers que aplican servicios integrados brindan **servicio garantizado** a las aplicaciones en tiempo real, **servicio controlado** al tráfico web y **servicio de mejor esfuerzo** al resto de los flujos con menor prioridad.

Funciones:

- Control de admisión: se reservan recursos en toda la ruta con RSVP.
- Enrutamiento: los routers encaminan según la QoS que requiera cada flujo.
- Manejo de colas de los routers: con FIFO y WFQ.
- Descarte de paquetes: con tail drop (últimos en llegar), RED y prioridad.

Al requerir mantener información del estado de cada flujo y reserva de recursos en los routers, es aplicable en redes pequeñas pero no es escalable.

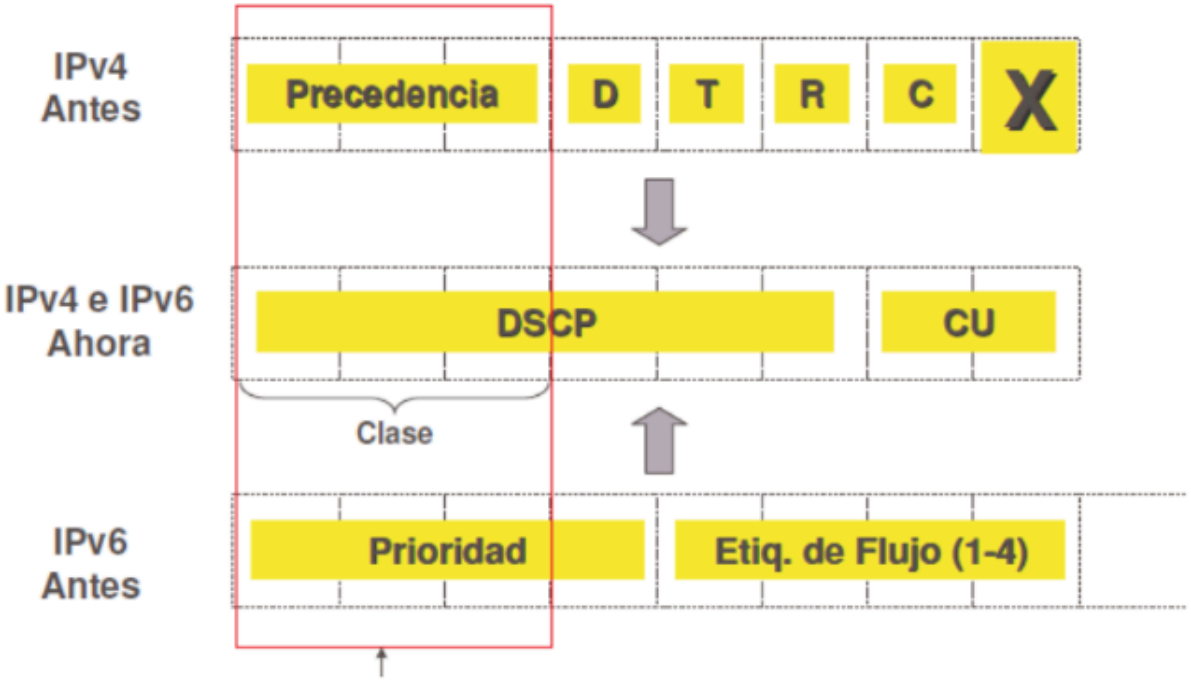
Servicios diferenciados

Es una mejora a IntServ, apunta a redes más grandes y es escalable. Usa la misma idea de reserva de recursos, aplicándolo a clases o tipos de tráfico. Se usan los campos Tipo de Servicio (IPv4) o Clase de tráfico (IPv6) para marcar o clasificar los paquetes en clases que tendrán asignadas cierta cantidad de recursos. No se mantiene información de estado de una conexión, sino de clases, y se otorga QoS según la clase de los paquetes. Ya no hay reserva de recursos ni información de estado almacenada en los routers.

Para no usar más el RSVP (que es poco escalable y era un protocolo extra), se aprovechó el nacimiento de IPv6 para agregar un campo que nos sirviera para otorgar

calidad de servicio. Así surgen los campos prioridad y etiqueta de flujo. Prioridad ocupaba 4 bits, hasta 16 niveles de prioridad posibles. Etiqueta de flujo era un identificador de flujos, usado para que los paquetes de diferentes flujos que debían tener el mismo tratamiento en cuanto a QoS se puedan transmitir por igual, otorgando la calidad necesaria según su clase, y que en destino se identificaran todos los paquetes que pertenecían a un mismo flujo. Los routers configurados con DiffServ no ven este campo (tipo de servicio o clase de tráfico) de esta manera, sino que tratan este octeto como el campo DS, en el que se usan 6 bits para la clase de tráfico, otorgando 64 posibles clases a los paquetes.

- Reenvío expedito:
  Se consideran las clases de servicio normal o expedito. Cada router tiene dos colas que se manejan con WFQ. A través de un SLA, asegura la transmisión de todo.
- Reenvío asegurado:
  Se definen cuatro clases de prioridades, también manejadas con WFQ. No asegura el envío sino un trato preferente. No hay SLAs.
- Mejor esfuerzo, sin garantías.



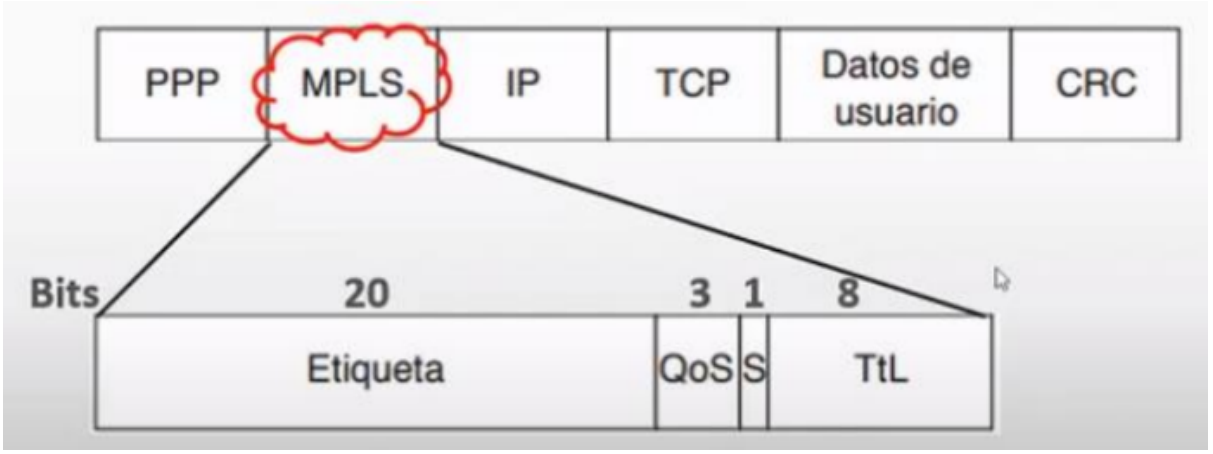
Se agrega el campo DSCP - Differentiated Services Codepoint, de 6 bits que indica el tratamiento que debe recibir el paquete, lo que permite indicar hasta 64 niveles de prioridad. CU - Currently unused sirve para el control de congestión.

Funciones QoS desempeñadas por los routers:

1. Clasificación de paquetes en clases.
2. Policing, descarte de paquetes que excedan el SLA. Necesario para lograr un tráfico que ingrese a la nube de manera controlada.
3. Marking, asignación del campo DSCP correspondiente a cada paquete.
4. Queueing y dropping, encolado de paquetes en donde corresponda y descarte
5. Shaping, control de tráfico y ráfagas a enviar por las interfaces.

MPLS - Multiprotocol Label Switching

Con este protocolo, no se encamina por IP sino por etiquetas. Se “genera” una capa intermedia entre la de red y la de enlace, por eso es multiprotocolo, por lo que el router no debe desencapsular hasta llegar a la dirección IP. Es más rápido el encaminamiento. Al obtener la etiqueta MPLS, busca en su tabla la entrada correspondiente para saber por qué interfaz sacar el paquete. Es una tecnología orientada a conexión en la que se tiene que establecer un circuito virtual para que todos los datos viajen por el mismo camino físico.



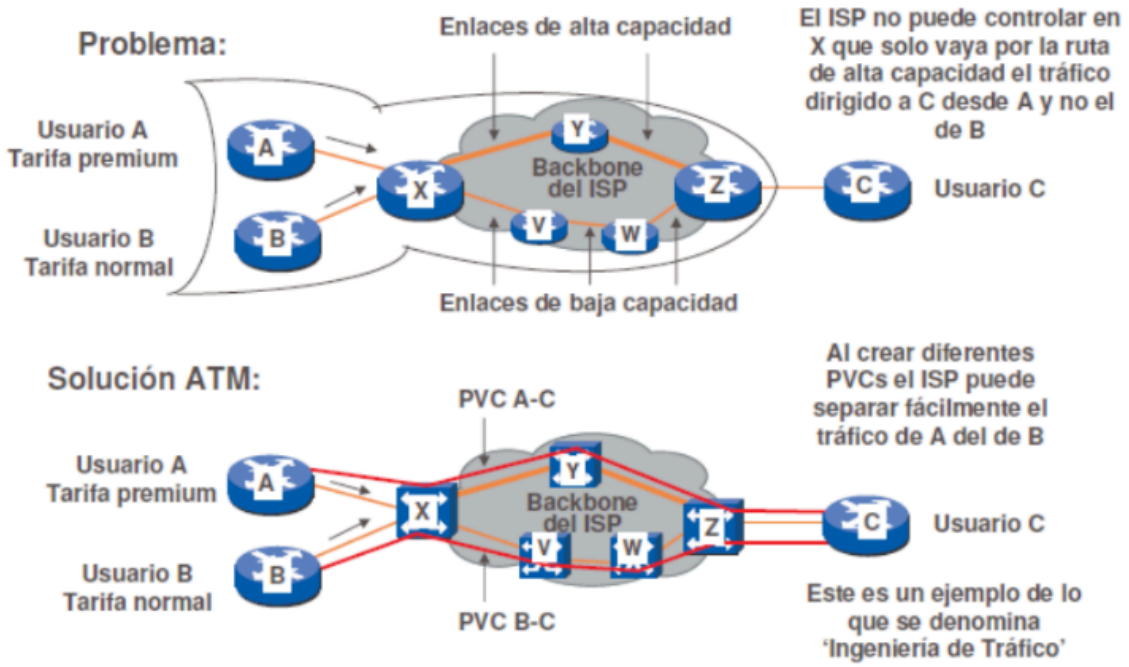
Se incorporan 32 bits:

- 20 bits para la etiqueta
- 3 bits para implementar calidad servicio, para avisarle qué tan importante es ese paquete (lo marca el proveedor de servicio), con 3 sobra porque tenemos 7 niveles de prioridad distintos.
- 8 bits para TTL, las funciones siempre la misma. De salto en salto o de router en router se va reduciendo en uno, si llega a cero se descarta. Porque a veces se producen bucles en internet y para que no queden dando vueltas surge TTL
- 1 bit que se llama Stack, porque puedo crear una etiqueta dentro de otra etiqueta. Puedo agregarle una etiqueta MPLS que llega hasta un determinado proveedor de servicio, ese otro proveedor de servicio puede ignorar esa etiqueta y volverla a encapsular en otra etiqueta distinta MPLS. Parecido a las cabeceras de extensión de ipv6, si está en 1 o en 0 avisa que hay otra etiqueta MPLS al lado.

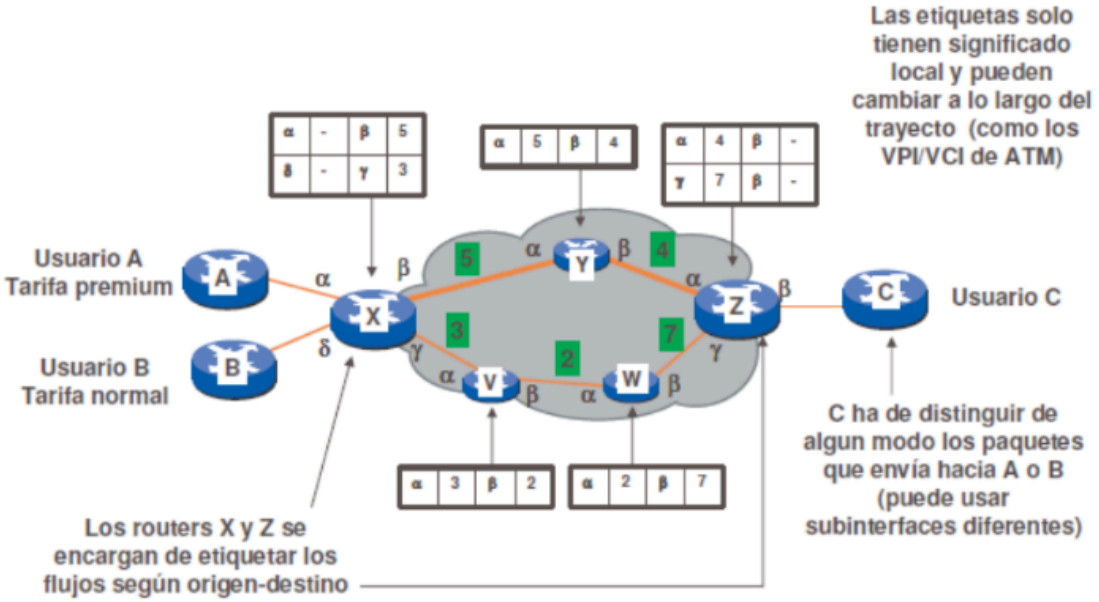
El TTL se agrega nuevamente, porque los routers no van a desencapsular y leer el TTL de IP, sino que desencapsulan PPP, leen los 20 bits y cambian el TTL. No llegan al TTL del paquete IP.

La idea es que se conmute, los routers pasarían a ser switches o conmutadores porque tiene una tabla que tiene cuatro entradas. Una tabla con cuatro entradas interfaz de entrada interfaz de salida etiqueta de entrada etiqueta de salida Entonces las tramas llegan con una etiqueta, si hace falta se la cambia, si no se mantiene la misma. Se la recibe por una interfaz y se conmuta hacia la otra interfaz. Simplemente viendo esa tabla de etiquetas, no tiene ni que ver la tabla de encaminamiento. Solo ve la tabla encaminamiento cuando desencapsula hasta el paquete IP. Se encamina muchísimo más rápido. - Ventajas → enrutamiento flexible, reenvío rápido y adecuado para brindar QoS

MPLS nació como solución al problema del pez.



Solución MPLS:



Básicamente, MPLS se creó para unificar diversos tipos de datos transmitidos en la misma red para enviar paquetes a mayor velocidad, gracias a la etiqueta que contiene toda la información para saber a dónde enviar los datos sin desencapsular hasta la dirección IP. Se pueden agrupar varios flujos con mismo origen y destino.

Comandos

arp

arp -a para visualizar la tabla (arp -n en linux)
arp -s para definir una entrada estática
arp -d para eliminar una entrada

```
C:\Users\Acer>arp -a

Interfaz: 192.168.1.19 --- 0x9
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1           8c-fd-de-2c-14-8d     dinámico
  192.168.1.8           b8-ab-62-c0-d6-57     dinámico
  192.168.1.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.102.18        01-00-5e-7f-66-12     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

arp -n

```
Address                  HWtype  HWaddress           Flags Mask            Iface
10.1.1.46                ether   00:0F:1F:B1:71:14   C                     enp0s8
10.1.1.70                ether   00:11:25:F6:A2:52   C                     enp0s8
10.1.1.73                ether   00:11:25:F6:93:F1   C                     enp0s8
10.1.1.40                ether   00:0D:60:6E:27:34   C                     enp0s8
10.1.1.34                ether   00:0D:60:6E:26:6F   C                     enp0s8
```

ping

```
C:\Users\Acer>ping -n 3 172.217.172.100

Haciendo ping a 172.217.172.100 con 32 bytes de datos:
Respuesta desde 172.217.172.100: bytes=32 tiempo=14ms TTL=116
Respuesta desde 172.217.172.100: bytes=32 tiempo=14ms TTL=116
Respuesta desde 172.217.172.100: bytes=32 tiempo=39ms TTL=116

Estadísticas de ping para 172.217.172.100:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 14ms, Máximo = 39ms, Media = 22ms
```

pathping

Combinación de ping y tracert, rastrea saltos intermedios entre origen y destino proporcionando datos de latencia y pérdida de paquetes e indicando en qué routers hay problemas.

```
C:\Users\Acer>pathping www.google.com

Seguimiento de ruta a www.google.com [142.251.133.36]
sobre un máximo de 30 saltos:
  0  AcerNitro5.home [192.168.1.19]
  1  home [192.168.1.1]
  2  host71.181-88-78.telecom.net.ar [181.88.78.71]
  3  host188.181-89-50.telecom.net.ar [181.89.50.188]
  4     *        *        *
Procesamiento de estadísticas durante 75 segundos...
              Origen hasta aquí   Este Nodo/Vínculo
Salto  RTT    Perdido/Enviado = Pct  Perdido/Enviado = Pct  Dirección
  0                                           AcerNitro5.home [192.168.1.19]
                                 0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  home [192.168.1.1]
                                 0/ 100 =  0%   |
  2    3ms     0/ 100 =  0%     0/ 100 =  0%  host71.181-88-78.telecom.net.ar [181.88.78.71]
                                 0/ 100 =  0%   |
  3    3ms     0/ 100 =  0%     0/ 100 =  0%  host188.181-89-50.telecom.net.ar [181.89.50.188]

Traza completa.
```

tracert

```
C:\Users\Acer>tracert www.google.com

Traza a la dirección www.google.com [142.251.133.196]
sobre un máximo de 30 saltos:

  1     1 ms     1 ms    <1 ms  home [192.168.1.1]
  2     4 ms     4 ms     3 ms  host71.181-88-78.telecom.net.ar [181.88.78.71]
  3     3 ms     2 ms     2 ms  host182.181-89-50.telecom.net.ar [181.89.50.182]
  4     *        *        *     Tiempo de espera agotado para esta solicitud.
  5     *        *        *     Tiempo de espera agotado para esta solicitud.
  6   236 ms     *       13 ms  host234.181-96-113.telecom.net.ar [181.96.113.234]
  7    12 ms    12 ms    12 ms  72.14.194.198
  8    13 ms    15 ms    13 ms  142.250.62.85
  9    13 ms    12 ms    12 ms  142.251.239.149
 10    15 ms    14 ms    17 ms  eze10s07-in-f4.1e100.net [142.251.133.196]

Traza completa.
```

ifconfig

Muestra las interfaces en estado up y consulta la dirección IP del host
ifconfig

```
root@RIN-UTNFRC:/$ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:85 errors:0 dropped:0 overruns:0 frame:0
          TX packets:85 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:17486 (17.0 KiB)  TX bytes:17486 (17.0 KiB)
```

Para levantar o dar de baja una interfaz
ifconfig eth0 up/down

```
root@simred:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:70:f8:bb
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3606 (3.5 KiB)  TX bytes:3744 (3.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Para ver la dirección MAC del host

ifconfig -a

Para setear dirección IP del host

ifconfig eth0 192.168.0.10 netmask 255.255.255.0 up

Setear una dirección IP a una interfaz

IPv4
ifconfig eth0 192.168.0.10 netmask 255.255.255.0

IPv6
ifconfig eth0 inet6 add 2001:db8::30/64

Levantar interfaz: ifconfig eth0 up
Activar o desactivar interfaz preconfigurada en /etc/network/interfaces: ifup/ifdown eth

ipconfig

```
C:\Users\Acer>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 1:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 10:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . : home
   Vínculo: dirección IPv6 local. . . : fe80::2789:6ba:7b53:8dd7%9
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.19
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.1

Adaptador de Ethernet Conexión de red Bluetooth:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :
```

Listar placas de red del equipo
ipconfig /all

Para liberar la IP que tenemos actualmente y obtener una nueva

ipconfig /release
ipconfig /renew

netstat y routeprint

netstat se usa para visualizar el estado de la red y estadísticas de protocolos TCP, SCTP y UDP, e información de la tabla de enrutamiento e interfaces.

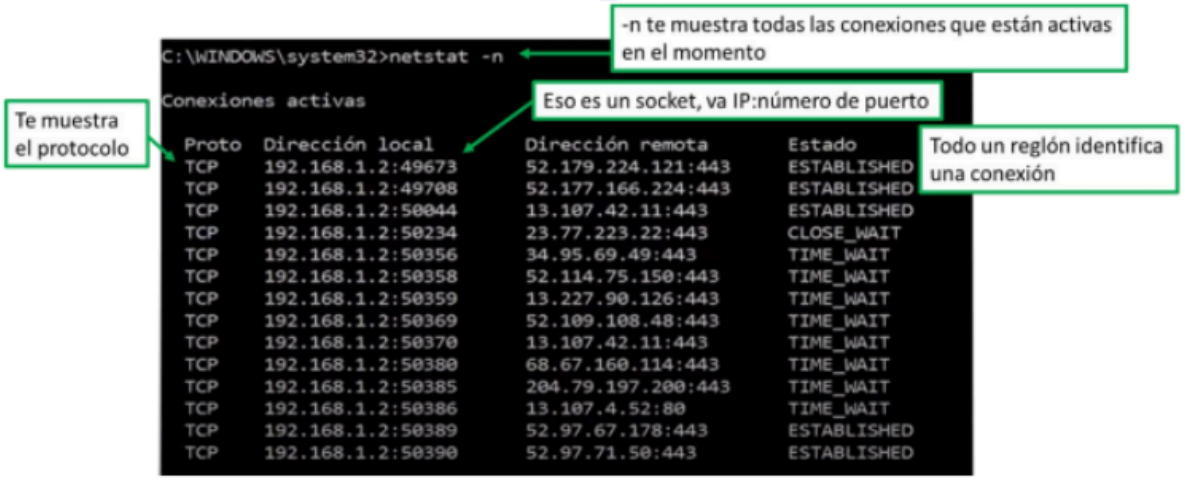
En Windows

netstat -m

```
C:\Users\flor>netstat -rn
===========================================================================
ILista de interfaces
 12...24 4b fe 50 ab 9a ......Realtek PCIe GbE Family Controller
 21...d2 37 45 1f f7 9e ......Microsoft Wi-Fi Direct Virtual Adapter
 14...d0 37 45 1f f7 9e ......Microsoft Wi-Fi Direct Virtual Adapter #2
  5...00 09 0f fe 00 01 ......Fortinet Virtual Ethernet Adapter (NDIS 6.30)
 10...d0 37 45 1f f7 9e ......TP-Link Wireless USB Adapter #2
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.208     50
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1    331
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1    331
  127.255.255.255  255.255.255.255      En vínculo         127.0.0.1    331
      192.168.0.0    255.255.255.0      En vínculo     192.168.0.208    306
    192.168.0.208  255.255.255.255      En vínculo     192.168.0.208    306
    192.168.0.255  255.255.255.255      En vínculo     192.168.0.208    306
        224.0.0.0        240.0.0.0      En vínculo         127.0.0.1    331
        224.0.0.0        240.0.0.0      En vínculo     192.168.0.208    306
  255.255.255.255  255.255.255.255      En vínculo         127.0.0.1    331
  255.255.255.255  255.255.255.255      En vínculo     192.168.0.208    306
===========================================================================
```

netstat

Para ver qué se está ejecutando en mi máquina



Estados posibles:

- ESTABLISHED: El socket tiene una conexión establecida.
- SYN_SENT: El socket está intentando iniciar una conexión.
- FIN_WAIT: el socket está cerrado, y la conexión está finalizando.
- TIME_WAIT: el socket está esperando después de cerrarse que concluya los paquetes que siguen en la red.
- CLOSED: El socket no está siendo usado.
- CLOSE_WAIT: La conexión remota ha finalizado, se espera que se cierre el socket.
- LISTEN: El socket está esperando posibles conexiones entrantes, solo para servidores.

• CLOSING: Ambos sockets han finalizado, pero aún no fueron enviados todos los datos.

```
C:\Users\Acer>route print
===========================================================================
ILista de interfaces
  4...98 28 a6 47 26 9b ......Realtek(R) PCI(e) Ethernet Controller
 19...48 89 e7 62 f0 94 ......Microsoft Wi-Fi Direct Virtual Adapter
 13...4a 89 e7 62 f0 93 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  9...48 89 e7 62 f0 93 ......Intel(R) Wireless-AC 9560 160MHz
 10...48 89 e7 62 f0 97 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.19     35
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1    331
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1    331
  127.255.255.255  255.255.255.255      En vínculo         127.0.0.1    331
      192.168.1.0    255.255.255.0      En vínculo      192.168.1.19    291
     192.168.1.19  255.255.255.255      En vínculo      192.168.1.19    291
    192.168.1.255  255.255.255.255      En vínculo      192.168.1.19    291
        224.0.0.0        240.0.0.0      En vínculo         127.0.0.1    331
        224.0.0.0        240.0.0.0      En vínculo      192.168.1.19    291
  255.255.255.255  255.255.255.255      En vínculo         127.0.0.1    331
  255.255.255.255  255.255.255.255      En vínculo      192.168.1.19    291
===========================================================================
Rutas persistentes:
  Ninguno

IPv6 Tabla de enrutamiento
===========================================================================
Rutas activas:
```

Configurar la tabla de enrutamiento estática de un router Linux

En este caso seteamos un gateway para ir a cierta red (172.16.2.0 /24)
route add -net 172.16.2.0 netmask 255.255.255.0 gw 172.16.1.1
route add -a gw 192.168.4.1
Este último es para que un host pueda acceder a cualquier punto de la red. Setea un gateway por defecto para cualquier caso

Para verificar la anterior configuración tenemos que ver la tabla de enrutamiento del router
route
netstat -r

En Windows:
route add 172.16.2.0 MASK 255.255.255.0 172.16.1.1

y para verificar
route print
netstat -m

nslookup

Para ver el DNS local.

```
C:\Users\Acer>nslookup
Servidor predeterminado:  home
Address:  192.168.1.1
```

Agregando un nombre de dominio, nos devuelve la dirección IP asociada.

Ver y vaciar la caché DNS en Windows

Windows (y cualquier sistema operativo, por defecto) emplea una memoria cache local para resolución de nombres. Las entradas almacenadas en caché podemos verlas así:

```
ipconfig /displaydns
```

```
C:\WINDOWS\system32\cmd.exe

Configuración IP de Windows

    173.168.217.172.in-addr.arpa
    ----------------------------------------
    Nombre de registro  . : 173.168.217.172.in-addr.arpa
    Tipo de registro  . . : 12
    Período de vida . . . : 4344
    Longitud de datos . . : 8
    Sección . . . . . . . : respuesta
    Registro PTR. . . . . : mad07s10-in-f13.1e100.net


    51.208.106.212.in-addr.arpa
    ----------------------------------------
    Nombre de registro  . : 51.208.106.212.in-addr.arpa
    Tipo de registro  . . : 12
    Período de vida . . . : 4344
    Longitud de datos . . : 8
    Sección . . . . . . . : respuesta
    Registro PTR. . . . . : 51.208.106.212.static.jazztel.es


    220.51.85.52.in-addr.arpa
    ----------------------------------------
-- Más  --
```

Y para borrar

```
C:\Users\alsam>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.
```

telnet
ssh
nmap

Unidad 5: Capa de transporte y capa de aplicación

Capa de transporte

Capa 4 en el modelo OSI, 3 en el modelo TCP/IP, es una capa que brinda diferentes servicios:

- Comunicación lógica extremo a extremo, lógica porque ya no nos interesa el camino físico de los datos, y de extremo a extremo porque se da una conexión entre origen y destino antes de la transmisión. No nos importa lo que ocurra en la red.
- Direccionamiento por puertos, surge el concepto de puerto como una dirección lógica de transporte de 16 bits (0 a 65535). Se usan para distinguir los diferentes procesos que se ejecutan en un dispositivo de manera simultánea. Dentro de los puertos tenemos sockets que son identificadores formados por IP + N° de puerto para procesos que se ejecutan en simultáneo en un mismo puerto.
- Multiplexación y demultiplexación, ya que todos los segmentos a enviar salen de la misma placa de red, el mismo medio físico.
- Servicio orientado a conexión, se establece una conexión lógica entre emisor y receptor antes de la transmisión. Primero se hace el establecimiento de la conexión o handshaking, luego la transferencia y por último la liberación de la conexión. Se reservan recursos y setean parámetros de conexión. Otorga más seguridad.
- Servicio no orientado a conexión, la transferencia de datos se hace sin establecer una conexión previamente, el origen simplemente envía los datos. Es inseguro porque no se garantiza que los datos lleguen.
- Servicio fiable, garantiza que los datos lleguen a destino con un ACK, que lleguen en orden y la integridad de los datos.
- Servicio no fiable, hay posibilidad de pérdida de datos, de su integridad o de desorden.

En resumen, sus funciones son la multiplexación de las comunicaciones en un dispositivo, el armado y ordenamiento de segmentos y el establecimiento de una sesión de comunicación entre aplicaciones de los usuarios. Logra esto a través del uso de sockets que son direcciones únicas formadas por una dirección IP + n° de puerto, y provee servicios confiables y no confiables, orientados o no a conexión.

Puertos

Asociados a cada aplicación y asignados por la IANA. Cuando el origen intenta conectarse a un servicio de una aplicación, a menos que el origen tenga un puerto asignado (como cliente), usa un puerto aleatorio de los puertos privados o dinámicos.
1 al 1023 - puertos públicos o bien conocidos.
1024 al 49151 - puertos registrados, propios de los fabricantes para sus aplicaciones.
49152 al 65535 - puertos privados.

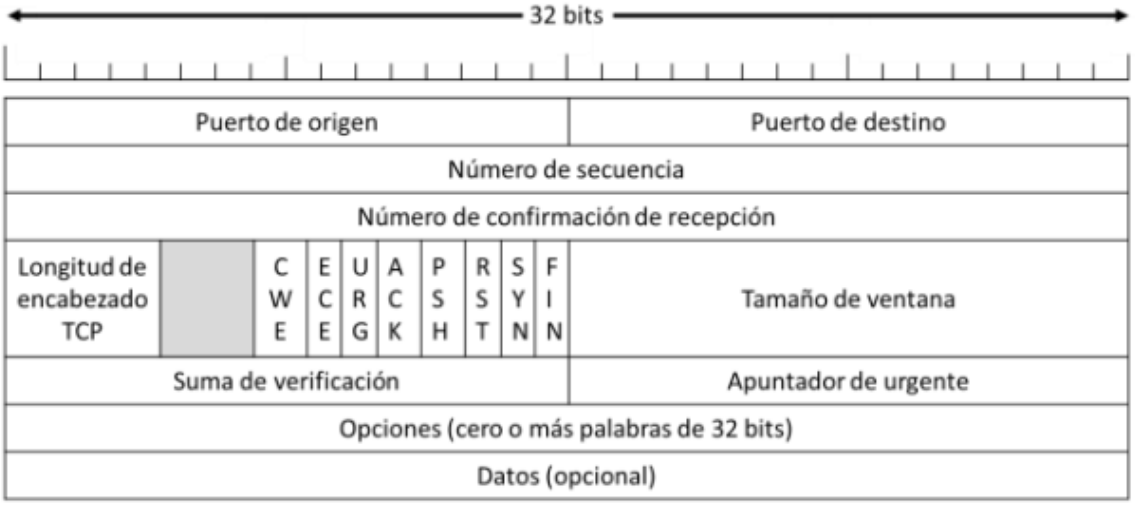
PUERTO	PROTOCOLO	APLICACIÓN
80	HTTP	Transferencia de páginas Web
21,20	FTP	Transferencia de archivos
443	HTTPS	Transferencia segura de páginas Web
25	SMTP	Correo electrónico
53	DNS	Resolución de dominios
67,68	DHCP	Asignación de direcciones IP
520	RIP	Protocolo de encaminamiento IGP
89	OSPF	Protocolo de encaminamiento IGP

TCP - Transmission control protocol

Características

Protocolo orientado a conexión que brinda un servicio fiable. Establece una conexión lógica de extremo a extremo sobre una red no fiable (por el uso de IP). TCP toma los datos de origen y los encapsula en segmentos, y en destino los desencapsula y reordena si es necesario. Trabaja con ACK para informar que un segmento llegó correctamente, o retransmitir si no. Multiplexa y demultiplexa datos a enviar de diferentes procesos. Además, implementa control de flujo entre origen y destino. Brinda conexiones dúplex y punto a punto.

Formato del segmento

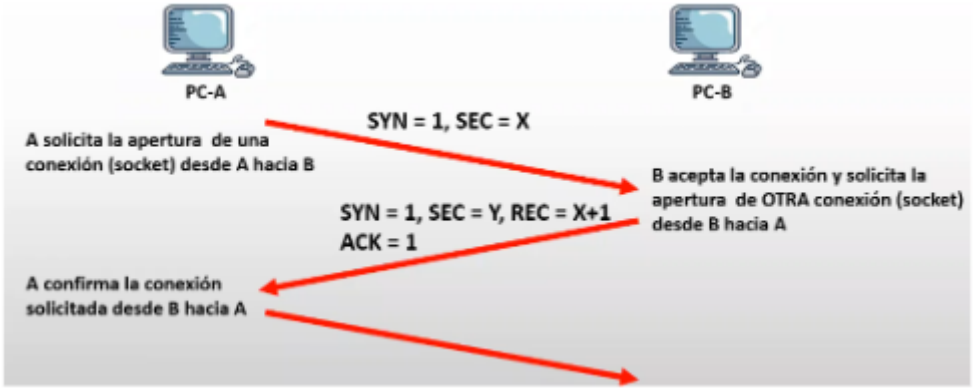


- Puerto de origen y destino, 16 bits cada uno
- Número de secuencia, es la cantidad de bytes enviados en el segmento, permite ordenarlos en destino. Como máximo podrán ser 1500 bytes, definido por la MTU de Ethernet (a menos que se use otro protocolo de capa de enlace).
- Número de confirmación de recepción: se usa como ACK, contiene el valor del siguiente byte esperado por quien envía el segmento. Es decir, si un emisor envía 10 bytes, el receptor responderá con un n° de ACK 11 porque espera el siguiente byte 11.<
- Longitud del encabezado, es la cantidad de palabras que contiene el encabezado.
- Flag CWE: se activa para indicar que se bajó la tasa de transferencia.
- Flag ECE: se activa para pedirle al emisor que reduzca el tamaño de ventana.
- Flag URG: urgente.
- Flag ACK: se activa para indicar que el campo Número de confirmación de recepción es válido.
- Flag PSH: se activa para indicar que los datos se deben entregar a la aplicación inmediatamente.
- Flag RST: se activa para restablecer una conexión o rechazar un segmento inválido.

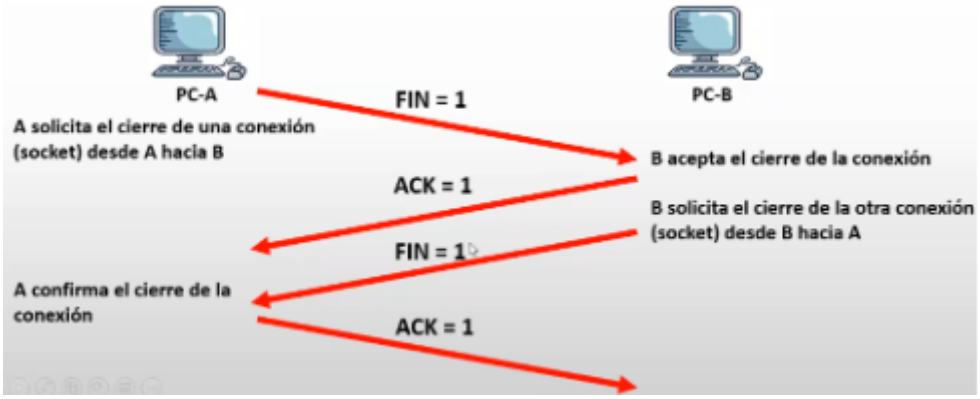
- Flag SYN: se activa para solicitar establecimiento de conexión.
- Flag FIN: se activa para liberar la conexión.
- Tamaño de ventana, se usa para el control de flujo, varía en función del espacio libre del buffer de cada dispositivo. Se envía la cantidad de bytes que puede tener el emisor en ese momento.
- Suma de verificación, para control de integridad del segmento.
- Apuntador de urgente, si URG está encendido, el destino comienza a leer desde este campo.
- Opciones: se usa para agregar datos como el tamaño de ventana o del segmento.

Funcionamiento, establecimiento y liberación de una conexión

El cliente A inicia la conexión con B para realizar una transferencia de datos. A envía un segmento sin datos a B, con los parámetros de conexión en la cabecera. El bit SYN estará encendido, y se enviará un número de secuencia. Si B puede, aceptará la conexión enviando otro segmento sin datos, con los bits SYN y ACK encendidos, el número de secuencia con el que va a enumerar sus bytes, y el número de reconocimiento de los X + 1 bytes enviados por A. Luego, A responderá el último mensaje con el bit ACK, la secuencia X+1 y el número de reconocimiento de los Y+1 bytes enviados por B. Este es el handshaking o saludo de 3 vías.



Para la desconexión, debemos hacer un saludo de 4 vías. Si A quiere terminar la conexión debe enviar un segmento sin datos con el bit FIN encendido, y B responderá con un ACK. Lo mismo sucede al revés.



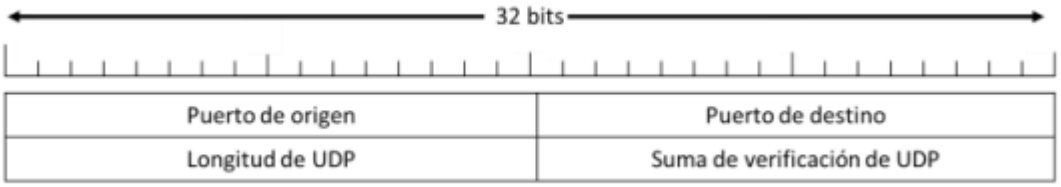
TCP ayuda al control de congestión a través del uso de una variable llamada ventana de congestión, que se fija cuánto demora el emisor en recibir un ACK del mensaje enviado. Si demora, sabe que debe bajar la tasa de transmisión (decremento multiplicativo), y si llega de inmediato, se puede aumentar (incremento aditivo).

UDP - User Datagram Protocol

Características

Protocolo no orientado a conexión que brinda un servicio no fiable. No mantiene el estado de la conexión, simplemente manda los datos a la red y si el receptor está saturado, no recibe los datos y se pierden. UDP no intenta una retransmisión ni implementa control de flujo o de congestión. Es mucho más rápido y sencillo, y se usa para aplicaciones en tiempo real.

Formato del segmento



La longitud UDP incluye la cabecera y los datos.

Captura Wireshark – Protocolo UDP

```
> Ethernet II, Src: SamsungE_70:7e:1f (24:f5:aa:70:7e:1f), Dst: ZyxelCom_b5:b4:f4 (ec:43:f6:b5:b
v Internet Protocol Version 4, Src: 192.168.1.9, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 61
    Identification: 0x2c1f (11295)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x8b36 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.9
    Destination: 192.168.1.1
v User Datagram Protocol, Src Port: 60753, Dst Port: 53
    Source Port: 60753
    Destination Port: 53
    Length: 41
    Checksum: 0x522f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 15]
  > [Timestamps]
> Domain Name System (query)
```

Esta consulta se encapsula en un paquete.

Muestra que cosa se esta encapsulando

Consulta que va desde la PC al servidor porque el puerto destino es público

Esta es la parte del protocolo con

Consulta DNS

Captura Wireshark – Protocolo TCP

```
> Ethernet II, Src: SamsungE_70:7e:1f (24:f5:aa:70:7e:1f), Dst: ZyxelCom_b5:b4:f4 (ec:43:f6:b5:b4:f4)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 65.55.65.172
v Transmission Control Protocol, Src Port: 57547, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 57547
    Destination Port: 443
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 3720953791
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 8192
    [Calculated window size: 8192]
    Checksum: 0x0a6e [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitte
  > [Timestamps]
```

Consulta que va desde la PC al servidor por el puerto 443 (https)

Todo esto es TCP

Es el primer segmento que manda porque esta estableciendo la conexión.

Campo opciones donde salen las configuraciones de la conexión

Captura Wireshark (transferencia de datos desde el host) – Protocolo TCP

```
> Ethernet II, Src: SamsungE_70:7e:1f (24:f5:aa:70:7e:1f), Dst: ZyxelCom_b5:b4:f4 (ec:43:f6:b5:b4:f4)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 65.55.65.172
v Transmission Control Protocol, Src Port: 57547, Dst Port: 443, Seq: 197, Ack: 2905, Len: 0
    Source Port: 57547
    Destination Port: 443
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 197    (relative sequence number)
    Sequence number (raw): 3720953988
    [Next sequence number: 197    (relative sequence number)]
    Acknowledgment number: 2905    (relative ack number)
    Acknowledgment number (raw): 1300610711
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 260
    [Calculated window size: 66560]
    [Window size scaling factor: 256]
    Checksum: 0x5d4c [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
```

Desde mi máquina

Hacia un servidor https

Número de secuencia

Número de reconocimiento, es el siguiente valor esperado desde el servidor

Todo esto es TCP

Solo prendido el bit ACK, porque son segmentos de datos.

Traducción de direcciones

NAT surge como herramienta de la capa de transporte. Los routers de borde mantienen tablas NAT para realizar la traducción de direcciones privadas a públicas y viceversa, y se les puede aplicar políticas de seguridad para mantener la privacidad de una empresa.

NAT estática

A cada IP privada se le asigna una pública. No hay ahorro de direcciones públicas, pero se usa para que los servidores de una empresa sean vistos desde Internet.

NAT dinámica

Se posee un pool de direcciones públicas que se asignan de manera dinámica a equipos internos que necesitan conectarse a Internet. Con esto logramos un ahorro de direcciones públicas. A medida que mis hosts privados necesitan conectarse a Internet, se les va asignando una dirección pública registrando el dispositivo en la tabla NAT del router borde, y si dejan de usar Internet, se libera la IP pública y vuelve al pool de direcciones disponibles.

No todos los hosts podrán acceder a Internet al mismo tiempo, y el router debe mantener el estado de las conexiones.

PAT

Es el que más IP públicas ahorra. Los dispositivos pueden conectarse a Internet con una única dirección IP pública, usando diferentes puertos.

NAT puede generar cuellos de botella en los routers borde y puede demorar en la traducción si tengo muchos paquetes. Sin embargo, ayudan con el ahorro de direcciones públicas, permite implementar más seguridad en la red interna y permite mantener el direccionamiento privado de la empresa en caso de cambio de ISP.

Capa de aplicación

Capa 4 del modelo TCP/IP, es la última capa y tiene funcionalidades más cercanas al usuario, de más alto nivel.

DNS - Domain Name System

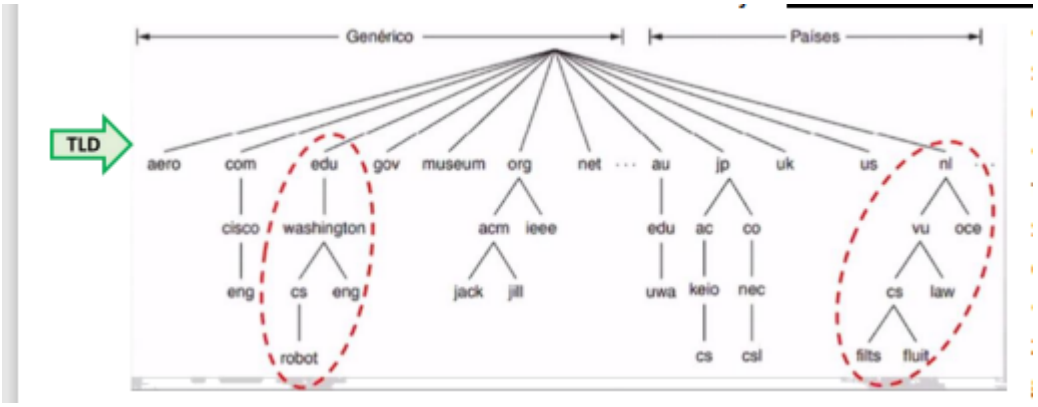
Los dispositivos con acceso a Internet tienen un identificador llamado dirección IP. Las direcciones IP son números, son difíciles de recordar. Por esto, nacen los nombres de dominio, que son nombres únicos que se traducen a direcciones IP, que son más fáciles de recordar por el usuario. La traducción del nombre de dominio a dirección IP es tarea del DNS, que es una aplicación que permite que los hosts se comuniquen con servidores DNS para pedir traducciones. DNS es una base de datos distribuida (al haber tantos dominios y

direcciones, no puede haber un único servidor que contenga toda la información), implementada en una jerarquía de servidores de nombres repartidos por todo el mundo, que corre sobre UDP en el puerto 54.

Un dominio no está en un único servidor, por lo que el DNS puede devolver más de una dirección IP correspondiente a un dominio; esto es distribución de carga. Por lo tanto, un dominio es un conjunto de servidores que prestan servicio a una misma organización y se conoce con una misma denominación, trabajando bajo una misma política de administración.

Los servicios ofrecidos por DNS son resolución de nombres, resolución de direcciones, alias de sistemas finales, registro de nombres de servidores de correo y distribución de carga.

Espacio de nombres de DNS



Como se mencionó, DNS trabaja como una jerarquía administrada por la ICANN. La Internet está dividida en más de 250 dominios de nivel superior o Top Level Domain - TLD. Los nombres de dominio reflejan límites organizacionales. Tenemos un árbol de dominios dividido en zonas no superpuestas de seguridad con servidores primarios y secundarios. Cada zona del espacio de dominios contiene una parte de este árbol con un servidor primario y varios secundarios.

Hay diversos tipos de servidores de DNS:

- Servidores locales: propios de cada organización, están más cerca del cliente. No conocen todas las direcciones, por lo que si le solicitan la traducción de un nombre de dominio desconocido, debe pasarle la consulta al servidor raíz.
- Servidores raíz: contienen información de cada dominio de nivel superior. Están replicados y derivan consultas a servidores autorizados.
- Servidores autorizados de nombres: registran a todos los hosts.

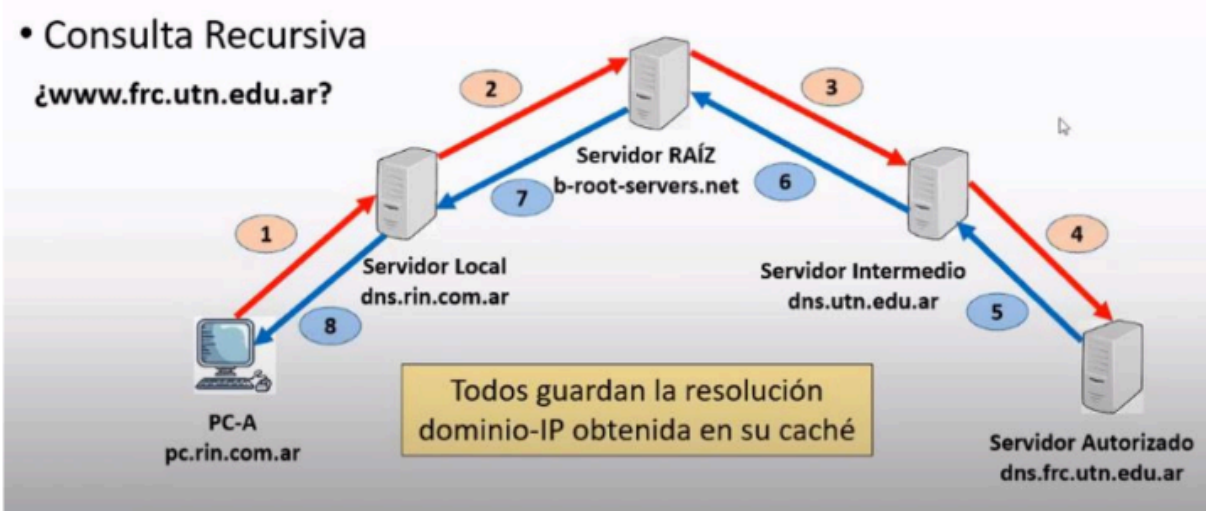
FQDN - Fully qualified domain name, es el nombre completo de dominio, la dirección completa y única necesaria para tener presencia en Internet. Se usa para localizar hosts específicos, y consta de al menos tres etiquetas o niveles: el dominio de nivel superior, el nombre del dominio y el nombre del host. Puede haber subdominios. La estructura es en forma de árbol, tendremos la etiqueta raíz como el punto más alto.

TLD - Top level domain, es el dominio de nivel superior, se encuentra en el segundo nivel jerárquico más alto, debe estar presente sí o sí en el espacio de nombres de dominio. Está en segundo nivel porque en primer nivel está el "." que actualmente no es necesario colocar. Especifica el tipo de organización.

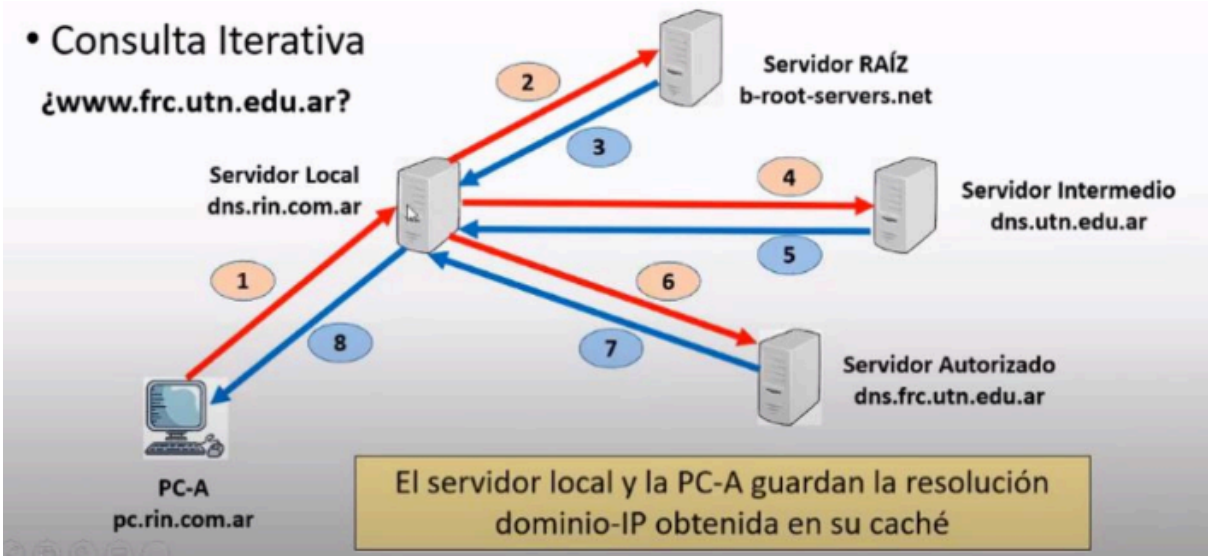
Si se necesita un dominio, lo buscamos en el navegador y éste pide servicio a un servidor DNS para obtener la IP. Al obtener la dirección, guarda en la caché la relación. Así, si queremos volver a acceder a ese dominio, el navegador no debe volver a solicitar la dirección al servidor de nombres. Sin embargo, esta entrada tiene un tiempo de duración TTL y luego se borra. Este borrado se hace para no mantener eternamente direcciones que pueden no volver a ser usadas, y además, porque un dominio puede cambiar sus datos. Cuando se registra un nuevo dominio o se modifica uno existente, se deben actualizar los datos de la base de datos de registros de dominio. El período desde que se realiza el cambio hasta que se evidencia la actualización en los servidores se llama propagación DNS y puede demorar días. Recién al borrarse la entrada de la caché por acabarse el TTL (o por borrarla manualmente con un comando), se vuelve a consultar al servidor DNS.

- ipconfig /all: permite ver el servidor local DNS configurado.
- ipconfig /displaydns: permite ver la caché DNS.
- ipconfig /flushdns: vacía la caché DNS.
- nslookup: permite ver la dirección IP de un dominio.

Tipos de consulta



La máquina origen A busca en la caché DNS la dirección que está buscando. Si no la tiene, saldrá a hacer la consulta al primer servidor local DNS que tenga. Si este servidor no tiene la dirección IP, dejará el pedido pendiente y reenviará la consulta al servidor raíz. Si el servidor raíz tampoco tiene la entrada, dejará el pedido pendiente y reenviará la consulta a un servidor intermedio, que podrá preguntarle al servidor autorizado correspondiente que debería tener la IP solicitada. Al obtener la dirección, la respuesta se irá propagando. En la consulta recursiva hay que mantener información del estado de las consultas en cada servidor, por lo que consume más recursos.



La consulta iterativa es diferente y es más rápida, no necesita mantener información de estado. El cliente consulta la caché DNS, y si no tiene la dirección, le consulta al servidor local más próximo. Si este no la tiene, sale a buscarla al servidor raíz, y si este tampoco la tiene, le responde al servidor local en qué otro servidor puede encontrar la dirección. Le delega al servidor local nuevamente la responsabilidad de seguir buscando otro servidor DNS que posea la información solicitada.

Registros de recursos

Cada dominio tiene asociado uno o varios registros de recursos, almacenados en la base de datos DNS. El DNS debe devolver diferentes respuestas en cada solicitud para que no todos los clientes accedan a la misma IP, para no saturar al servidor.

A nivel de base de datos, cada registro del DNS se conoce como registro de recurso, y tiene 5 campos:

1. Nombre: PK, es el nombre de dominio.
2. Clase: permite evolucionar al DNS, se establece con qué pila de protocolos se usa el dominio.
3. Tipo: de varios tipos, sirven para pedir un valor determinado del recurso.
4. Valor: el que se devuelve cuando se pide un tipo.
5. TTL: tiempo de vida máximo del registro, antes de ser borrados de la caché.

¿Qué relación existe entre el DNS server y un servidor WINS?

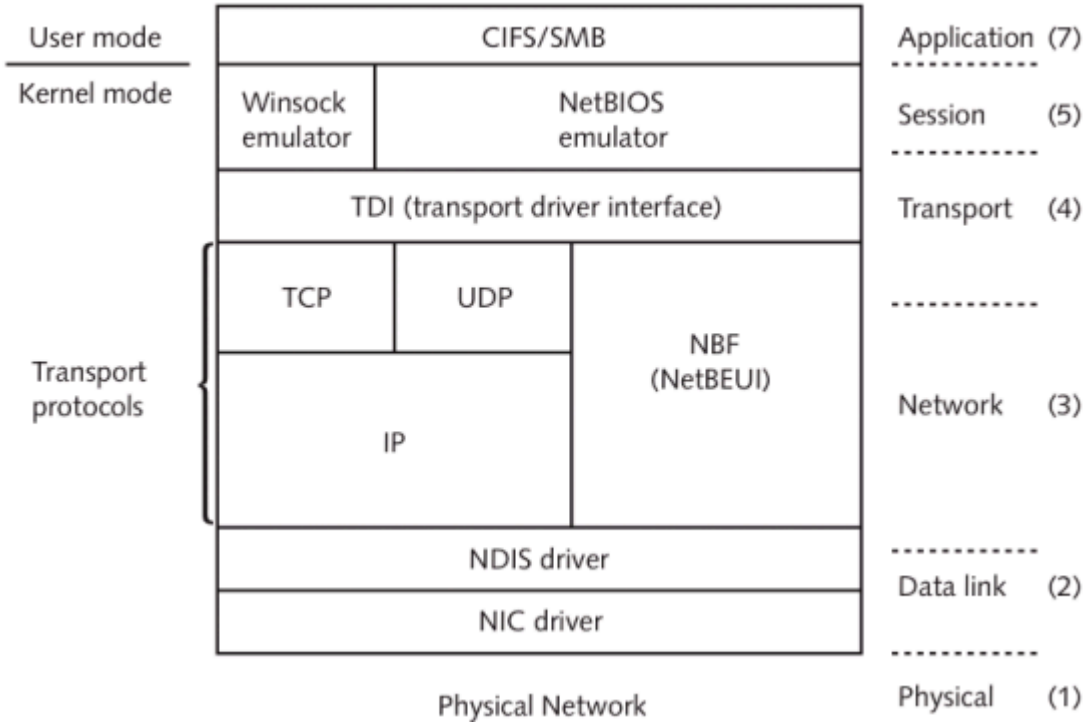
El DNS cambia los nombres de host a direcciones IP, y WINS cambia los nombres de NetBIOS de ordenadores de una misma red a direcciones IP. Su funcionamiento es muy similar. Además, DNS tiene un espacio de nombre jerárquico y WINS tiene un espacio de nombres plano.
Una diferencia que me parece que es clave es que los DNS Server se usan en el modelo TCP/IP mientras que los servidores WINS únicamente tienen utilización en sistemas de trabajo WINDOWS ya que dependen de protocolos propios de Windows (NetBeui/ NetBios)

15) ¿Qué es y cómo funciona el servicio WINS?

WINS- Windows internet naming service, es un servicio de registro y resolución de nombres de equipo NetBIOS a direcciones IP a través de una tabla de correspondencia que permitirá localizar a otro ordenador de la red rápidamente. Corre sobre los puertos TCP y UDP 42.
El funcionamiento se da en base al siguiente esquema:
1. Determinan si el nombre contiene más de 15 caracteres o si contiene puntos ("."). Si es así, consultan el nombre en DNS.
2.Determinar si el nombre está almacenado en la caché de nombres remotos del cliente.
3.Se ponen en contacto y prueban con los servidores WINS configurados para resolver el nombre mediante WINS.
4.Utilizan difusiones IP locales en la subred.
5. Comprueban en el archivo Lmhosts si “Habilitar la búsqueda de LMHOSTS” está habilitado en las propiedades de Protocolo Internet (TCP/IP) de la conexión.
6. Comprueban el archivo Hosts.
7. Consultan a un servidor DNS.

17) Relaciones SMB, NetBeui y TCP

SMB - Server message block es un protocolo cliente/servidor que corre sobre TCP 139 y 445, que gobierna el acceso a archivos y directorios y otros recursos de red abiertos a la red. Puede controlar el intercambio de información entre los procesos de un sistema. Es un protocolo de intercambio de archivos. Permite al cliente comunicarse con otros participantes de una misma red. Al igual que TCP, este protocolo crea una conexión entre origen y destino enviando mensajes de solicitud y respuesta.
NetBEUI - NetBIOS extended user interface, es un protocolo de nivel de red que corre sobre TCP 139 sin encaminamiento. Permite que los dispositivos se comuniquen en un ambiente LAN de forma rápida. Como este protocolo no es ruteable, si quiero enviar datos fuera de mi LAN la performance baja, por lo que se recomienda usar TCP/IP para comunicaciones fuera de mi LAN.



18) Diferencie entre archivo HOSTS y LMHOST. ¿Para qué se utilizan?

Hosts es un archivo que guarda correspondencia entre dominios de Internet y direcciones IP. LMHosts es un archivo usado por los equipos que usan WINS server que contiene esa misma correspondencia entre un nombre de equipo NetBIOS y su dirección IP. Sus funciones son las mismas.

FTP - File Transfer Protocol

Protocolo cliente/servidor que permite la transferencia bidireccional de archivos entre sistemas, corre sobre TCP puertos 20 y 21. No usa cifrado SSH, pero es autenticado, con usuario y contraseña, y brinda dos servicios

- público: se inicia sesión con el usuario anonymous y como contraseña el correo electrónico propio del servidor público al que esté accediendo. Podré descargar archivos visibles del servidor.
- privado: se pide usuario y contraseña registrados.
  SFTP es FTP seguro de extremo a extremo, cifrado, basado en SSH.

Tipos de conexión

- Conexión de control: permite iniciar sesión y enviar comandos al servidor. La conexión es persistente hasta terminarla manualmente, y el servidor mantendrá el estado del cliente, atento a lo que pida. Se usa el puerto 21.
- Conexión de datos: permite interactuar con archivos en el servidor. La conexión no es persistente, sólo se usa al subir o bajar archivos y se libera. Se usa un socket distinto por cada usuario y se puede subir/bajar más de un archivo. Se usa el puerto 20.

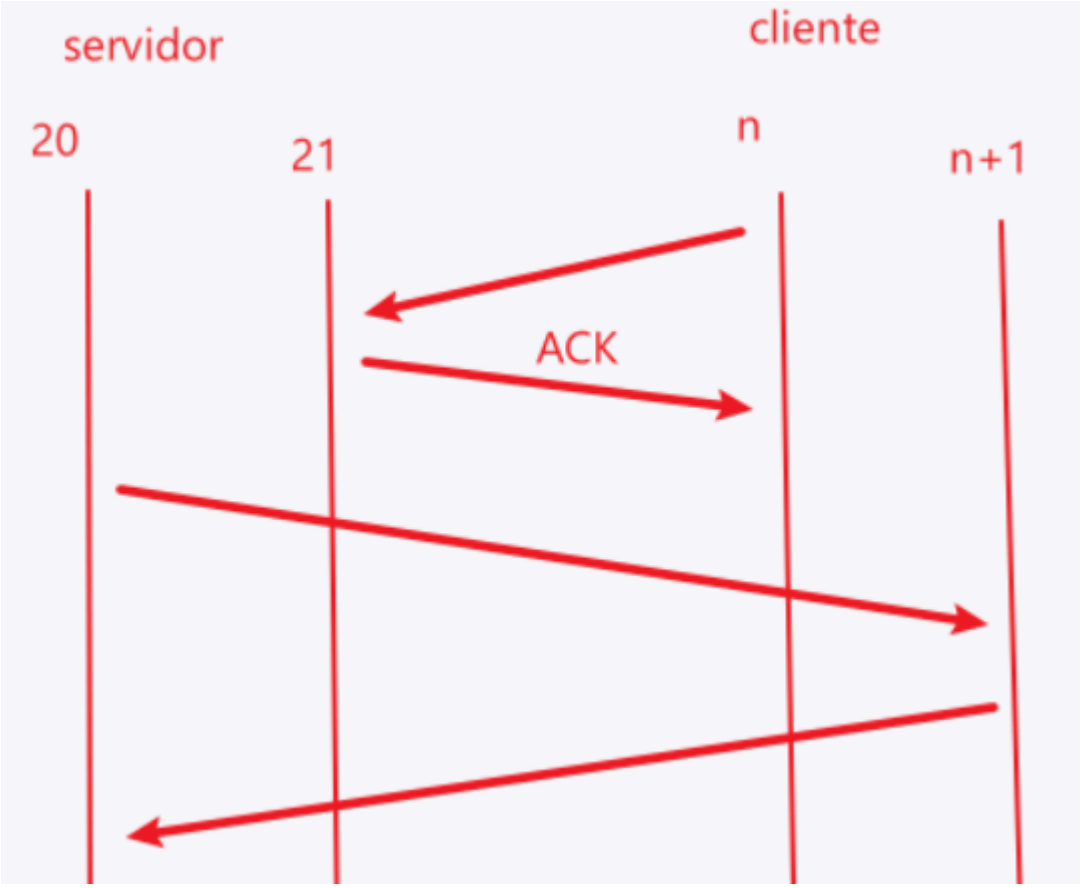
Comandos

- USER R User name, userid for access control
- PASS O Password for access control
- ACCT O Account info
- CWD O Change working directory
- CDUP O Change to parent directory
- SMNT O Structure mount, mount a different file system
- QUIT R informs server that client wants out
- REIN O restarts session at authentication phase
- PORT R Host addr and data port to use

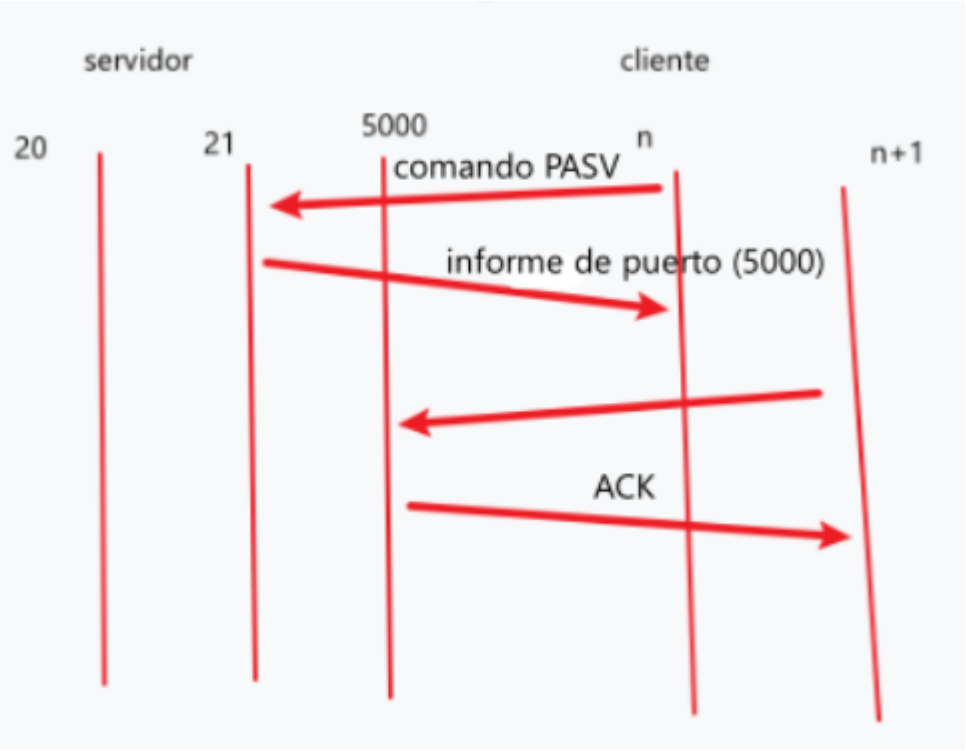
- PASV O Passive; informs server that client will contact to set up data connections, ask server to sent port info
- TYPE R Data type, type of subsequent transfers
- STRU R File structure
- MODE R Transfer mode
- RETR R Retrieve, download the file from server
- STOR R Store, upload the specified to server
- STOU O Store unique, same as store but server picks unique file name

Modos de conexión

- Modo activo
  El cliente usa un puerto aleatorio n para conectarse con el servidor por el puerto 21, y le envía el puerto aleatorio n+1 al servidor para que sepa a dónde enviar los datos. El servidor establece conexión con ese puerto y el cliente le envía comandos y datos.



- Modo pasivo
  O FTP seguro, los clientes usan dos puertos aleatorios, se conectan con el servidor, envían puertos y el comando PASV para que el servidor le envíe los datos al cliente desde otro puerto aleatorio.



TFTP - Trivial FTP

Protocolo igual que el FTP pero no fiable, corre sobre UDP en el puerto 69. Se suele usar para enviar archivos de configuración o de booteo desde estaciones sin memoria en distancias cortas y en entornos de baja interferencia. Básicamente, en situaciones en las que la pérdida del archivo no es un gran problema ni tampoco es muy probable.

El cliente envía un RRQ o WRQ y el servidor responde un ACK, y se envían los datos.

SFTP es una versión segura de FTP, con algoritmos de cifrado.

SNMP - Simple Network Management Protocol

Protocolo de capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Corre sobre UDP en los puertos 161 y 162. Sirve para gestionar los dispositivos de redes grandes, configurarlos y monitorearlos de forma remota mediante la normalización de comunicaciones con una interfaz que me abstraiga de cada objeto.

Interfaz de usuario (diferentes en cada empresa y dentro de una misma empresa)
Sistema de gestión (diferentes en cada empresa y dentro de una misma empresa)
Elementos a gestionar

Paquete SNMP:

- **Versión**: versión del protocolo SNMP (RFC1157 es versión 1).
- **Comunidad**:cadena de caracteres que indica la comunidad con la que se realiza la(s) operación(es) solicitada(s).
- **SNMP pdu**: el comando depende del tipo de comando. Contiene OIDs que identifican objetos y el valor correspondiente (caso de operación SetRequest o GetResponse).

Modelo de gestión de red definido por la ISO

Áreas a controlar:

- Gestión de rendimiento
  Cuantificar, medir, registrar y controlar el rendimiento de los componentes de una red.
- Gestión de fallos

Registrar, detectar y solucionar los fallos de una red.
- Gestión de configuración
  Controlar que la configuración sea correcta.
- Gestión de cuentas
  Especificar, registrar y controlar los accesos de usuarios y dispositivos a recursos de la red.
- Gestión de seguridad
  Controlar el acceso a recursos según políticas de red (no crear).

Componentes

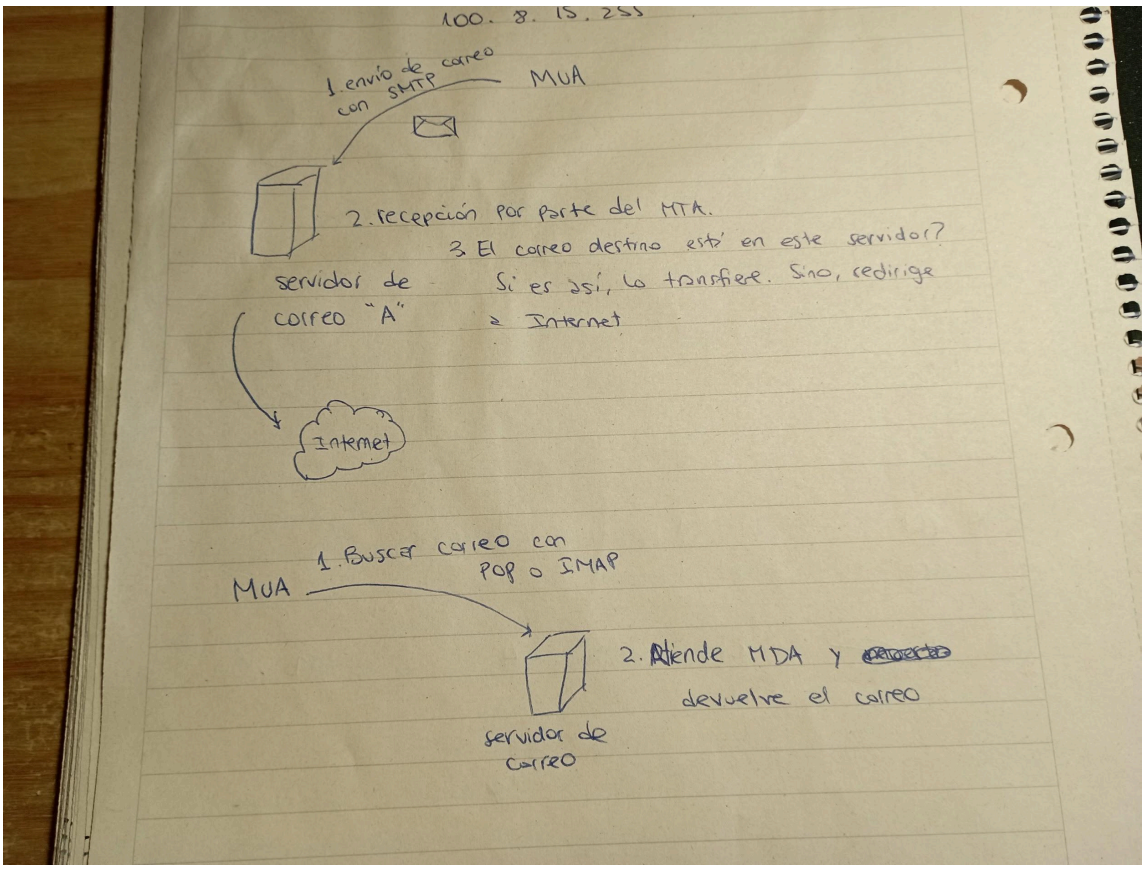
- Dispositivos administradores
- Agentes - software que ejecutan los objetos administrados, que informan del estado de estos objetos
- NMS - estaciones de administración de red
- MIB - base de datos con los objetos a administrar

La MIB es una base de datos que contiene todos los objetos que se pueden gestionar en una red. Es un conjunto de información organizada jerárquicamente con una estructura de árbol con niveles. Se puede acceder a cada objeto a través de una instancia del mismo con su identificador OID que se forma por los niveles a los que pertenece, separando cada nivel con un punto (ejemplo, 1.2.2.4).
Las estaciones de administración NMS contienen todo el software de administración, y envían y reciben mensajes SNMP. Existen 3 arquitecturas:
- Centralizada, hay una sola NMS
- Jerárquica, se instala parte del cliente SNMP en cada sucursal y tenemos una NMS central con la que todas las secundarias se comunican.
- Distribuida, cada estación tiene igual jerarquía y responsabilidad, tiene cada una su base de datos local y pueden intercambiar información.

SNMP puede trabajar con RMON - Remote Monitoring, que es una aplicación de SNMP en una empresa con muchas sucursales. La idea es obtener información en redes distribuidas a través de Internet.

Correo electrónico

El modelo de correo en Internet está compuesto por diferentes agentes y un servidor de correos.
- Agente de usuario de correo MUA: permite leer y enviar correo a través de una interfaz gráfica. Brindan herramientas avanzadas como reenvío automático, listas, prioridad, búsquedas, organización, etc. Está en el cliente.
- Agente de transferencia de mensajes MTA: mueve los mensajes de origen a destino con SMTP. Se ejecutan en segundo plano en los servidores de correo. Está en el servidor.
- Agente de entrega de correo MDA: entrega correos a los buzones de usuarios. Está en el servidor.



Un emisor quiere enviar un correo, para esto usa el MUA que con SMTP logra enviar el correo al servidor de correos. En este servidor, el MTA recibe el correo y lo transfiere a la casilla destino correspondiente. Si el MTA define que el receptor no pertenece a su servidor de correo, lo redirige a Internet para que se envíe al servidor correspondiente.
Un receptor quiere recuperar sus correos, entonces el MUA busca correos con POP o IMAP en el servidor. El MDA atiende la solicitud.

SMTP - Simple Mail Transfer Protocol

Protocolo de capa de aplicación, corre sobre TCP en el puerto 25. Sólo puede enviar datos ASCII. Tiene conexiones persistentes. Si quiero enviar y recibir mensajes de forma segura, uso SSL o TLS para usar SMTPS sobre el puerto 465.

ENVOLTURA	ENCABEZADO	CUERPO DEL MENSAJE
Información para la transferencia del mensaje (MTA)	Información de control para los agentes de usuario (UA)	Datos para el destinatario final

Campos relacionados con el transporte del mensaje

Encabezado	Significado
To:	Dirección/es del receptor/es primario
Cc:	Dirección/es receptor/es secundarios
Bcc:	Dirección/es para las copias al carbón ocultas
From:	Persona/s que crearon el mensaje
Sender:	Dirección del emisor actual
Received:	Linea que agrega cada agente de transferencia a lo largo de la ruta
Return-path:	Se puede usar para identificar una ruta de vuelta al emisor

Campos utilizados por los agentes de usuarios (UA) o los destinatarios

Encabezado	Significado
Date:	Fecha y hora de envío del mensaje
Reply-To:	Dirección a la que se debe enviar las respuestas
Message-Id:	Número único para hacer referencia a este mensaje después
In-Reply-To:	Identificador del mensaje al que éste responde.
References:	Otros identificadores de mensaje revelantes.
Keywords:	Palabras clave seleccionadas por el usuario
Subject:	Resumen corto del mensaje para desplegar en una línea

POP3 - Post Office Protocol versión 3

Este protocolo corre sobre TCP en el puerto 110 (ó 995 para conexiones seguras), sirve para consultar el correo. Nació cuando se usaba Dial-Up, y su funcionamiento se basaba en que, al consultar el correo, los mensajes se descargaban al agente del usuario y desaparecían del servidor. Es simple y rápido, y no necesita conexión a Internet. Como desventaja está que se borraban los mensajes del servidor al descargarlos una única vez, y no permitía movilidad.

Fases:

1. Autorización: el UA envía usuario y contraseña.
2. Transacción: el UA descarga los mensajes del servidor.
3. Actualización: se finaliza la sesión POP3.

IMAP - Internet Message Access Protocol

Corre sobre TCP en los puertos 143 o 993 para conexiones seguras. Permite el acceso a correos almacenados en un servidor de Internet, descargando una copia de ellos sin eliminarlos del servidor. Se puede consultar el correo desde cualquier dispositivo muchas veces y organizar los mensajes en carpetas en el servidor.

Correo basado en la Web

Me permite consultar el correo desde mi navegador con un cliente de correo que brinda una interfaz web. Es el agente de usuario que se comunica con su buzón de correo remoto mediante el protocolo HTTP.

MIME - Multipurpose Internet Mail Extensions

Es una convención para poder transmitir cualquier tipo de datos, no sólo ASCII. Se usa con SMTP para extender su funcionamiento, y define reglas de codificación de mensajes no ASCII. El mensaje original se encapsula en una cabecera MIME, y luego éste se encapsula en un mensaje SMTP.

Encabezado	Significado
MIME-Version:	Identifica la versión MIME (actual: 1,0)
Content.Descripcion:	Cadena legible por humanos que indica lo que contiene el mensaje.
Constent-Id:	Identificador único.
Constent-Transfer-Encoding:	Cómo se envuelve el mensaje para su transmisión.
Content-Type:	Tipo y formato del contenido que se envía.

HTTP - Hypertext Transfer Protocol

Protocolo sin estado usado en la World Wide Web (WWW) para el intercambio de recursos a través de Internet. Corre sobre TCP en el puerto 80, y de forma segura sobre 443. Define la sintaxis y semántica usada por clientes y servidores para comunicarse.

- Comandos HTTP:

Comando	Descripción del protocolo HTTP
GET	Solicita leer una página de la Web
HEAD	Solicita leer la cabecera de una página Web
PUT	Envía datos al servidor (actualización de contenidos)
POST	Envía datos para que sean procesados por el recurso de la URL
DELETE	Elimina la página Web
LINK	Conecta dos recursos existentes
UNLINK	Rompe una conexión existente entre dos recursos

Permite localizar un recurso en Internet a través del uso de URLs - Uniform Resource Locator, formado por un protocolo de acceso (rojo), un dominio (celeste) y una ruta de acceso al recurso (negro):

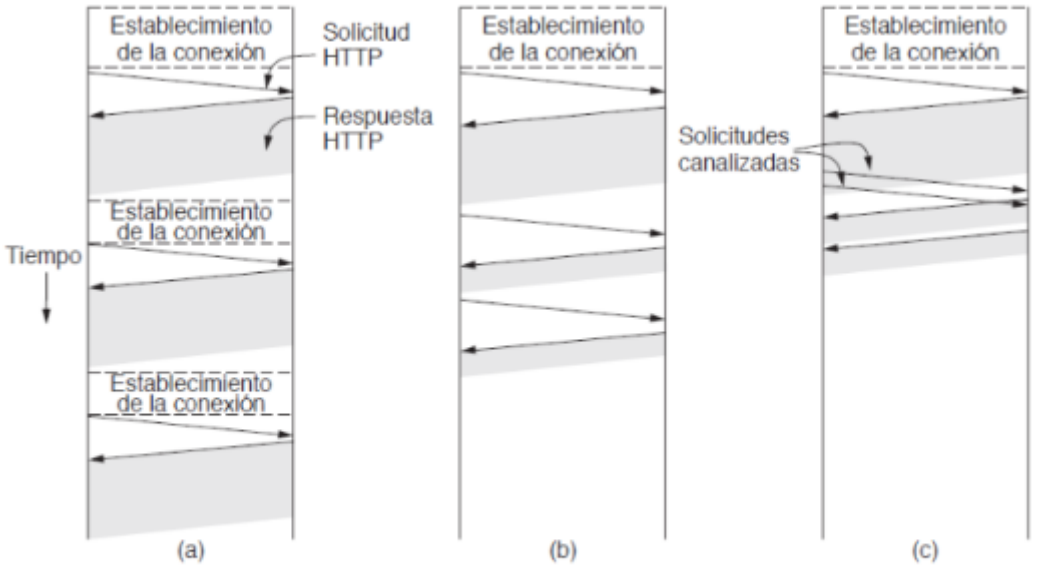
https://uv.frc.utn.edu/mod/folder/view.php?id=213104

El navegador solicita a un servidor de nombres la IP del dominio o URL ingresada, al obtener la dirección IP la guarda en la caché y establece una conexión TCP con el puerto 80. Con una solicitud HTTP GET al servidor correspondiente, el servidor le envía el archivo HTML de la página web, se libera la conexión TCP y el cliente le da un formato a la página. Del lado del servidor, éste debe aceptar la conexión TCP, obtener la ruta del recurso solicitado, obtener el contenido del recurso y enviarlo al cliente para luego liberar la conexión.

Se dice que HTTP es un protocolo sin estado porque no guarda información de conexiones anteriores. Para almacenar información de las conexiones, es decir, generar un estado y guardarlo en la caché del usuario y del servidor, y hacer seguimiento del usuario, se usan las cookies que se guardan en el navegador.

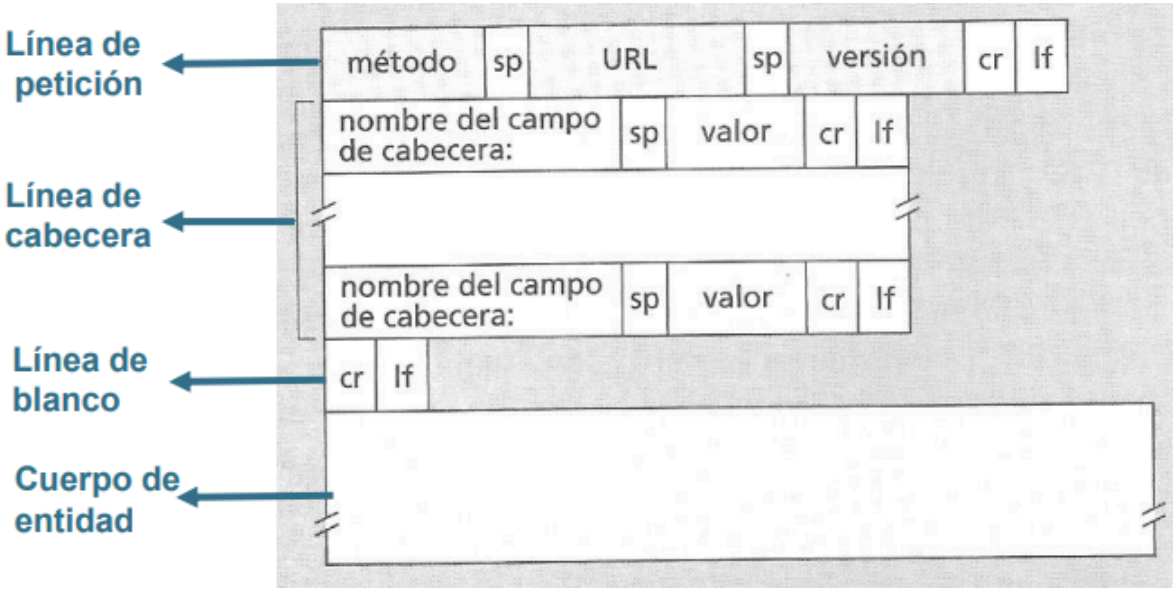
Tipos de conexiones:

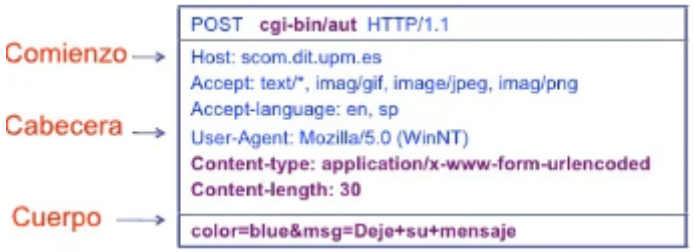
- No persistentes:
  Luego de recuperar el archivo HTML, el navegador se desconecta del servidor. Si necesita algo más, debe volver a conectarse. Era muy lento y usaba mucho ancho de banda.
- Persistentes:
  Se puede mantener la sesión abierta
  - Seriales: el servidor responde consultas del navegador una por una, en orden manteniendo la conexión.
  - No seriales: el cliente manda solicitudes al servidor sin esperar una respuesta de la consulta anterior. Se aprovechan mejor los recursos del servidor, es más rápido y hay menos retardos.



HTTP con (a) varias conexiones y solicitudes secuenciales. (b) Una conexión persistente y solicitudes secuenciales. (c) Una conexión persistente y solicitudes canalizadas.

Encabezado HTTP



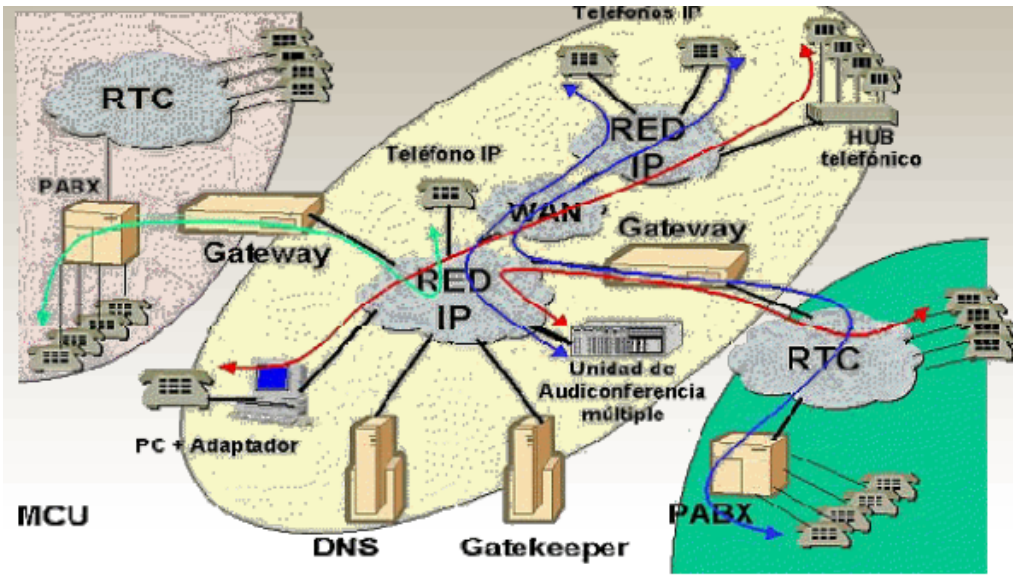


HTTPS - HTTP Secure

Con el uso de TLS (Transport Layer Security) o SSL (Secure Socket Layer) para conexiones se construye una conexión segura entre dos sockets. SSL maneja compresión y encriptación luego de la conexión. HTTPS corre en el puerto 443 sobre TCP, es lo mismo que HTTP pero los datos viajan cifrados entre cliente y servidor. La seguridad se da sobre la capa de transporte.

Voz sobre IP

Un proceso genérico de voz sobre IP o VoIP se puede explicar con la siguiente imagen:



Si un usuario de una LAN desea establecer una comunicación telefónica, la voz primero debe pasar por un proceso de digitalización con PCM para poder encapsularla en paquetes IP. De manera general, si un usuario con un teléfono desea llamar a otro fuera de su LAN deberá usar Internet. Enviará los datos digitalizados sobre UDP con RTC (protocolo de control del paquete) de la voz a su gateway (que es un dispositivo que conecta una red RTC o red de telefonía pública con una red IP), que será el encargado del direccionamiento del paquete hacia un teléfono IP o hacia otro gateway para conectarse a otra red RTC. Se comienza a usar conmutación de paquetes y el ancho de banda es compartido.

La telefonía IP está asociada a los sistemas de telefonía digital IP en una LAN, que usan IP para las comunicaciones de voz. La voz se digitaliza y transmite por paquetes IP. Por otro lado, en VoIP, la voz analógica pasa a digital y se transmite en paquetes IP de un dispositivo a otro. La diferencia está en que VoIP consiste en enviar el audio analógico a través de Internet, y la telefonía IP es mucho más amplia; implica enviar audio y muchos otros servicios a través de Internet, como llamadas en espera, conferencias y otras funcionalidades extras. VoIP da la base para que la telefonía IP la use.

RTP es un estándar que se ejecuta sobre UDP usado para transportar formatos multimedia que dispone de una estructura de paquete estandarizada, que incluye campos específicos para los datos de audio y video. El emisor encapsula un fragmento multimedia en una cabecera RTP de normalmente 2 bytes, que incluye el tipo de codificación, un número de secuencia y una marca de tiempo (indica el instante de muestreo para cada tipo de codificación).

Los paquetes RTP sólo son identificados como RTP en las terminales con software que puede trabajar con este estándar. Para los routers, son paquetes IP comunes.

RTCP es un protocolo de control de RTP, que envía periódicamente los paquetes RTP con informes del emisor o receptor que anuncian estadísticas útiles para la aplicación que ejecuta RTP.

H.323

Protocolo de la ITU, de conferencia multimedia que incluye transmisión de voz, video y conferencia de datos en tiempo real. Posee

- Terminales: dispositivos finales a los que llegan los paquetes.

- MCU o multipoint control units: administran conferencias multipunto con un controlador que administra la señal de llamada y permite un procesador multipunto para manejar muchos enlaces.
- Gateways: compuesto por un Media Gateway Controller, que maneja la señalización de llamadas y otras funciones, y un Media Gateway que administra el enlace. Son los que vinculan las redes PSTN con otras redes H.323.
- Gatekeeper: opcional, se usa para control de admisión y resolución de direcciones, y otras funciones específicas.
- Elementos de borde: dispositivos que funcionan junto con el gatekeeper para agregar más información de direccionamiento, y asistir en la autorización y autenticación de llamadas entre diferentes dominios.

H.323 es un documento que describe cómo funcionan sus partes en conjunto. Precisa de otros protocolos para permitir la comunicación, como RAS, H245 y Q931. Es un conjunto completo e integrado por protocolos para conferencias multimedia.

SIP - Session Initiation Protocol

Protocolo de la IETF basado en TCP/IP. Corre sobre UDP en el puerto 5060 (también puede correr sobre TCP). Es un protocolo de señalización que define el inicio, modificación y terminación de comunicaciones entre sesiones de usuario. Proporciona mecanismos para establecer llamadas entre usuarios a través de una dirección de la forma de correo electrónico, de un número de teléfono o por nombre de usuario, que se traduce a una dirección de la forma usuario@ip. Posee

- Clientes (teléfonos SIP, softphones, gateways, etc).
- Agentes de cliente UAC y agentes de servidores UAS.
- Servidores:
    - Servidor proxy: recibe los mensajes INVITE del usuario que quiere iniciar la conexión, realiza la consulta DNS al registrador SIP. Es el intermediario necesario para establecer el enlace de comunicación.
    - Servidor de redireccionamiento
    - Servidor de registración: permite registrar a los teléfonos que se comunicarán mediante VoIP. Traduce identificadores fijos a direcciones IP dinámicas.

SIP simplifica la implementación de voz sobre IP, ya que sólo necesita servidores SIP para dar soporte a este servicio.

El proceso de establecimiento de llamada inicia con un intento de conexión de un origen A a un destino B a través de, por ejemplo, un nombre de usuario. A crea para B un mensaje INVITE que se envía a un servidor proxy. El proxy devolverá una respuesta SIP que incluya la dirección IP asociada al usuario o una URL hacia una página que dé otra respuesta. El proxy determina la dirección IP del usuario solicitado gracias al registrador SIP, que puede realizar estas traducciones (funciona como un servidor DNS).

```
REGISTER sip:dominio.com SIP/2.0
Via: SIP/2.0/UDP 193.64.210.89
From: sip:benito@dominio.com
To: sip:benito@dominio.com
Expires: 3600
```

así se registra una dirección IP de un usuario

El proxy, al conocer ahora la IP de B, puede reenviar el mensaje de INVITE al proxy de B, y así A y B podrán comunicarse a través de SIP.

	SIP	H.323
Propósito	Resolver multimedia transportada en paquetes IP para permitir llamadas entre dos o más terminales con negociación de parámetros	
Funcionamiento	Intercambio sencillo de mensajes ASCII	Trabaja con muchos protocolos en cada capa del modelo OSI intercambiando mensajes en binario
Diseñado por	IETF	ITU
Llamadas llegan a	User agent	Gateway y terminales
Transporte de medios	RTP y RTCP	
Direccionamiento	Mediante URL	Mediante números telefónicos

Unidad 6: Seguridad

La seguridad en las redes es ahora una parte integral de las redes informáticas. Consiste en protocolos, tecnologías, dispositivos, herramientas y técnicas que aseguran los datos y reducen las amenazas.

Las políticas de seguridad de una red definen en un documento las restricciones y el comportamiento que deberían tener los miembros de una organización, se especifica quiénes acceden a qué datos y cómo lo hacen. Este documento debe ser aplicable a las operaciones de cada organización, por lo que es diferente en cada empresa. Debe servir de guía para el diseño y configuración de la red, estableciendo una jerarquía de permisos justos y necesarios y controles a realizar. Es un documento que varía en el tiempo a medida que se encuentran vulnerabilidades o aparecen nuevas tecnologías. Para saber cómo construirlo hay que tener en cuenta las necesidades de la empresa (sean relacionadas a su rubro o necesidades de seguridad) y las amenazas y los riesgos identificados. La idea es mantener los 4 pilares de la seguridad:

- Confidencialidad: la información debe ser accedida únicamente por partes autorizadas. Para lograrlo, me valgo de técnicas de cifrado. Si se pierde la confidencialidad, puedo sufrir de interceptación.

  Un criptosistema está compuesto por un conjunto de textos claros, textos cifrados y algoritmos que transforman el original en cifrado. Estos algoritmos se dividen en diferentes grupos, según:
  - naturaleza del algoritmo:
    - sustitución, se intercambian símbolos
    - transposición, se cambia el orden de los símbolos
    - producto, se aplican los métodos anteriores más de una vez
  - clave:

        - simétricos, se usa la misma clave para cifrar y descifrar
        - asimétricos, se usan diferentes claves
        - irreversibles
    - número de símbolos cifrados a la vez:
        - bloque, se divide el texto original en bloques de igual longitud y se cifra cada uno
        - flujo, se cifra bit a bit
- Integridad: la información debe ser modificada únicamente por partes autorizadas. Debe llegar de origen a destino completa y sin modificaciones. Para lograrlo puedo usar hash.
- Disponibilidad: la información debe estar disponible para las partes autorizadas siempre que se deba. Si no, puedo sufrir de interrupción.
- Autenticación: se debe verificar la identidad de cada cliente. Si no, puede haber invención. Forma parte de AAA (autenticación, autorización, auditoría).
- Extra: no repudio. No puedo negar algo que hice, debe haber trazabilidad de cada actividad.

Una función hash es una operación que se aplica a un conjunto de datos de cualquier tamaño y da como resultado otro conjunto de datos de tamaño fijo, independientemente del tamaño del texto original. Es un algoritmo de cifrado irreversible que da como resultado un “resumen” único, que garantiza la integridad de los datos. Por ejemplo, si tengo un mensaje X que quiero mantener íntegro y transmitir a un destino, puedo enviar el mensaje y su hash. Así, en destino vuelven a aplicar el hash al mensaje original y pueden corroborar su integridad, es decir, que no cambió durante la transferencia.

	Simétricos	Asimétricos
Claves	Misma clave privada en ambos extremos	Diferentes claves en los extremos, una privada y una pública
Ventajas	Son rápidos, fuertes	No hay que distribuir la clave
Desventajas	Distribución de la clave	Lentos, consumen muchos recursos, y perder la clave privada es muy peligroso
Técnicas usadas	Cifrado por bloques	

Firmas digitales

Son herramientas tecnológicas que permiten garantizar la autoría (no repudio) e integridad de documentos digitales.

Funcionamiento

Se basan en el uso de claves públicas y funciones de hash. Iniciamos con un mensaje de texto claro a enviar. A este mensaje C lo pasamos por una función de hash que

nos dará un texto resumen R, y también lo ciframos con nuestra clave privada obteniendo un texto plano cifrado C. Enviamos al receptor ambos mensajes R y C. Así, el receptor podrá descifrar el mensaje con la clave pública del emisor, obteniendo el texto claro C nuevamente. A este mensaje le aplica la función de hash y compara R' con R, para verificar la integridad del mensaje. La autoría se verifica en el momento de usar la clave pública del emisor: si al usar la clave pública de quien, el receptor cree, es el emisor, no logra descifrar el mensaje, entonces no se puede comprobar la autoría. Si el receptor logra descifrar el mensaje, se sabe que quien lo envió es el emisor conocido.

Firmas de clave simétrica

Se cifra en origen y se descifra en destino. Se necesita un intermediario de confianza que distribuya la clave que usarán origen y destino, que será el KDC- Key Distribution Center. Cada vez que se necesita establecer una comunicación, se da aviso al KDC para que genere una contraseña de sesión, es decir, una nueva clave simétrica que será usada en toda la transacción y luego de terminar la sesión, pierde la vigencia. Cada usuario debe encargarse de crear y entregar la clave de sesión, que se usará para cifrar el mensaje y garantizar la confidencialidad.

Firmas de clave pública

Se cifra toda la transacción, garantizando la confidencialidad. Se necesita una autoridad de certificación CA. El emisor cifra su mensaje con su clave privada (para garantizar la autenticación), y luego con la clave pública del receptor (para garantizar la confidencialidad). En destino se descifra con la clave privada del destinatario y luego con la clave pública del origen.

Resumen de mensajes

Se cifra con la clave privada del origen y se envía el mensaje cifrado y un hash del texto claro. No garantiza la confidencialidad

Sobres digitales

Si quiero tener garantizado integridad, autoría, confidencialidad y no repudio, necesitaré aplicar una PKI - Public Key Infrastructure, que es un grupo de componentes y servicios que permiten gestionar la tarea de generar, brindar o revocar certificados digitales:

- Certificados digitales: documento digital otorgado por un tercero de confianza, que vincula una clave pública con una entidad.
- Autoridad de certificación: tercero de confianza responsable del mantenimiento, emisión y revocación de los certificados.
- Autoridad de registro: se encarga de la alta y baja de emisión y revocación de certificados, autenticando usuarios, solicitando y entregando los certificados.
- Autoridad de validación: proporciona información sobre el estado de los certificados.

- Sistema de distribución de certificados
- Aplicaciones habilitadas por PKI

Se basa en el uso de sobres digitales. Primero, se firma digitalmente un mensaje (lo que comprende el cálculo de su resumen, el cifrado del mensaje original con la clave privada del emisor y el envío de ambos resultados - autoría, confidencialidad e integridad). Luego, se encripta el mensaje con un algoritmo simétrico usando claves privadas en ambos extremos de la comunicación. Estas claves privadas se deben distribuir, usando un algoritmo de cifrado asimétrico que se logra con la PKI, es decir, el emisor usa su clave privada que se puede descifrar con la pública que el receptor conoce gracias a la CA. Entonces, el emisor usa la clave pública del receptor y cifra la clave privada que se debe usar para desencriptar la firma digital.

El receptor podrá descifrar la clave privada cifrada del origen usando su clave privada. Usando esta clave privada del algoritmo simétrico, descifra el mensaje recibido y obtiene la firma digital y el hash. Aplica la función de hash a la firma para verificar la integridad comparando los hash. Además, el hash también podría ser cifrado.

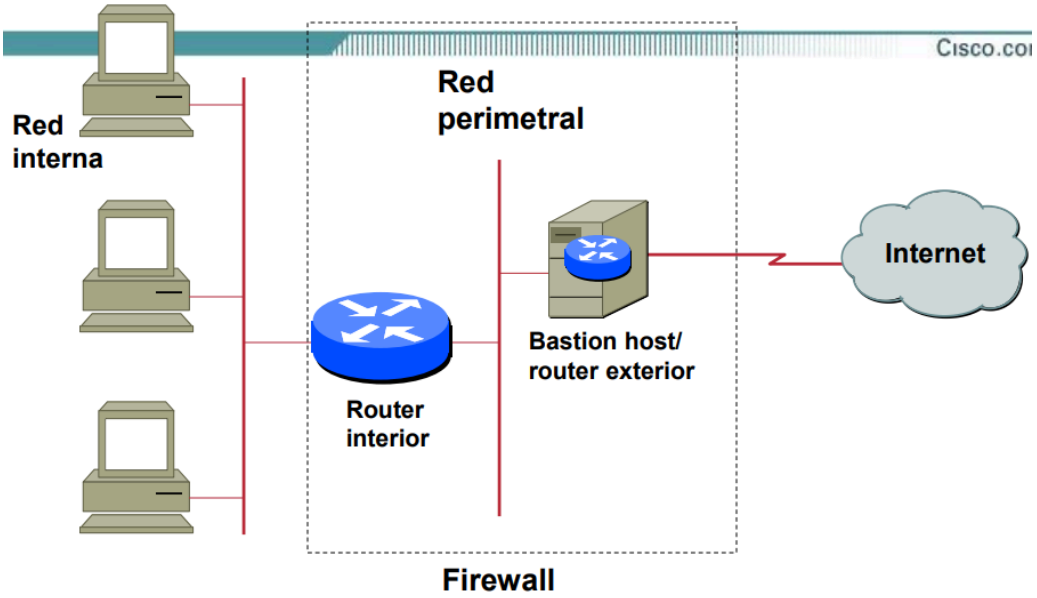
Firewall

Un firewall es un sistema de control centralizado, conformado por hardware y software que hace cumplir una política de control de acceso entre redes, aislando la red interna de una organización de Internet para controlar lo que entra y sale de la misma. Idealmente, son resistentes a los ataques, ayudan a hacer cumplir las políticas de seguridad y son el único punto de tránsito entre redes.

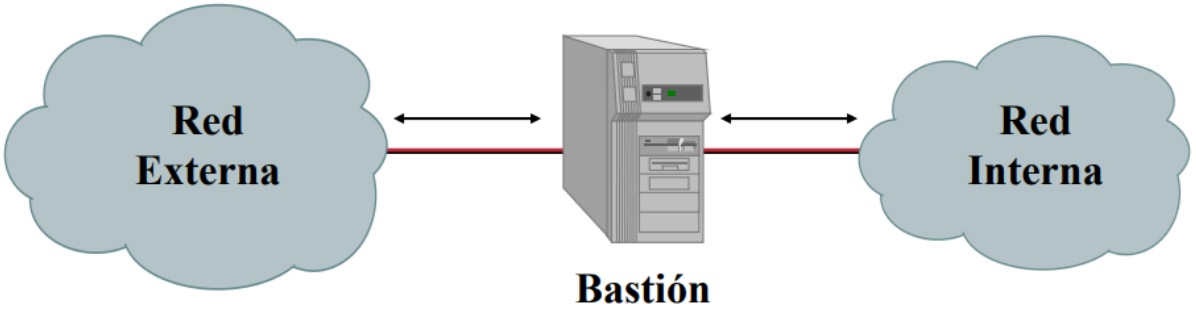
Tendremos ACL, listas de control de acceso, y en base a ellas podremos setear reglas de permisos y denegaciones de ingreso o salidas.

Clasificación de firewalls

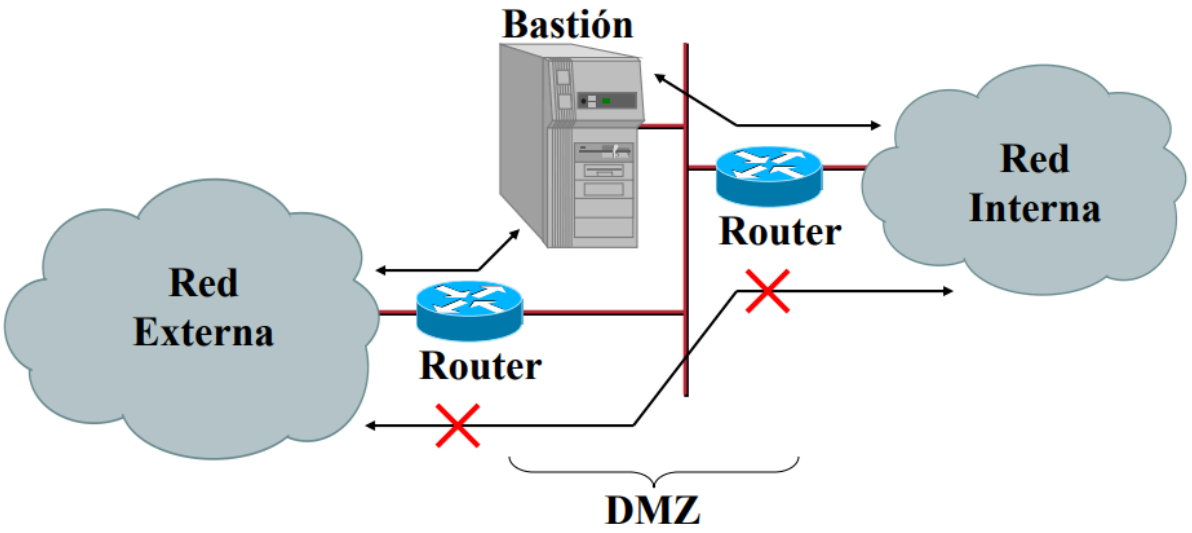
- Screened host firewall
  Tendremos un router separando la red interna de la Internet. La Internet podrá enviar tráfico de entrada sólo al host bastión, un router exterior que actúa de barrera y define una red perimetral.



- Dual homed gateway
  Tendremos un host bastión para aplicaciones permitidas, que filtra hasta la capa de aplicación separando las redes interna y externa. Este host tiene dos placas de red, conectadas a redes diferentes.



- Screened subnet
  Tenemos dos routers separando las redes interna y externa, y un host bastión en medio de los dos que recibe el tráfico sospechoso. Si un atacante entra al bastión, todavía debe pasar por un router más para llegar a la red interna. Esta zona se llama zona desmilitarizada.



DMZ - Zona Desmilitarizada

Usada en servidores que deben ser accesibles desde redes externas, define qué partes de la red son confiables y cuáles no. Es como una zona no controlada. Este firewall se configura así:

Deny es para denegar direcciones. Permit es para permitir direcciones con ciertos protocolos.

Tipos de firewall

- Filtrado de paquetes
  De la capa de interred (?).Controlamos ciertos aspectos de cada paquete que ingresa o sale de la red interna. Es un proceso lento. Tendremos políticas restrictivas, con las que no ingresarán paquetes a menos que estén permitidos explícitamente con sentencias PERMIT, y políticas permisivas, con las que ingresarán todos los paquetes menos los que estén restringidos explícitamente. Las reglas se establecen en un orden de lo particular a lo general.

- Firewalls con estado
  De la capa de transporte. Van creando reglas de manera dinámica a medida que el usuario utiliza los dispositivos de la red interna. Al establecer una conexión TCP con algún servidor externo, se agrega un renglón en la lista de transmisiones permitidas que se elimina cuando se libera la conexión. Entonces, sólo se controlan las comunicaciones que salen de la empresa, no las que ingresan: sólo se permiten paquetes que ingresan a la red si la conexión se inició en la red interna. Para todo esto, el firewall debe mantener tablas dinámicas en las que registra la IP y el puerto con sus permisos.

- Pasarelas de aplicación

De la capa de aplicación. Además de filtrar por IP y puerto, con estos firewalls puedo filtrar por los permisos del usuario. Es lento porque cada usuario tendrá diferentes niveles de acceso para cada aplicación, registrados en diferentes servidores.

Configuración

- 0.0.0.255 wildcard, o máscara invertida.
- Permit tcp any host 192.168.2.5 eq 25: permitir cualquier paquete que llegue desde internet a esa dirección por el puerto 25.
- Las reglas son de entrada o de salida.

```
R1(config)# ip access-list extended ACL-1
R1(config-ext-nacl)# remark LAN ACL
R1(config-ext-nacl)# deny ip host 192.168.1.6 any
R1(config-ext-nacl)# permit tcp 192.168.1.0 0.0.0.255 any established
R1(config-ext-nacl)# deny ip any any
R1(config-ext-nacl)# exit
R1(config)# interface Fa0/0
R1(config-if)# ip access-group ACL-1 in
R1(config-if)# exit
R1(config)# ip access-list extended ACL-2
R1(config-ext-nacl)# remark DMZ ACL
R1(config-ext-nacl)# permit tcp any host 192.168.2.5 eq 25
R1(config-ext-nacl)# permit tcp any host 192.168.2.6 eq 80
R1(config-ext-nacl)# deny ip any any
R1(config-ext-nacl)# exit
R1(config)# interface Fa0/1
R1(config-if)# ip access-group ACL-2 out
R1(config-if)# exit
```

VPN -Virtual Private Network

Red privada que se crea mediante el uso de túneles sobre una red pública. Las redes privadas físicas son muy seguras pero tienen un alto costo de implementación, por lo que surgen las VPNs como una solución de **costo reducido** ya que pueden existir sobre Internet, **segura** porque usan protocolos de cifrado y autenticación, **escalable** al poder expandirse usando la infraestructura de Internet ya existente y que **facilita la implementación de teletrabajo**.

Tipos

- Punto a punto: usadas para conexiones entre redes de sucursales y una casa central. Es estática. El gateway de la VPN encapsula y cifra el tráfico saliente de un sitio, y lo envía por el túnel de VPN sobre Internet a otro gateway VPN. Ejemplo: frame relay, ATM o MPLS.
- Acceso remoto: usadas para el teletrabajo, se crean de manera dinámica con una arquitectura cliente/servidor. Tenemos VPN SSL (a través de un navegador web y cifrado SSL en capa de transporte) y VPN IPSec (permite el acceso seguro a todas las aplicaciones cliente/servidor de la organización con cifrado en capa de red).

IPSec - IP Secure

IPSec es un protocolo de seguridad IP, que proporciona seguridad en la capa de red usada para la creación de VPNs. Se agrega una cabecera IPSec antes de la cabecera IP, que cifra la carga útil del paquete enviado. Trabaja en conjunto con dos protocolos principales (además de muchos otros):

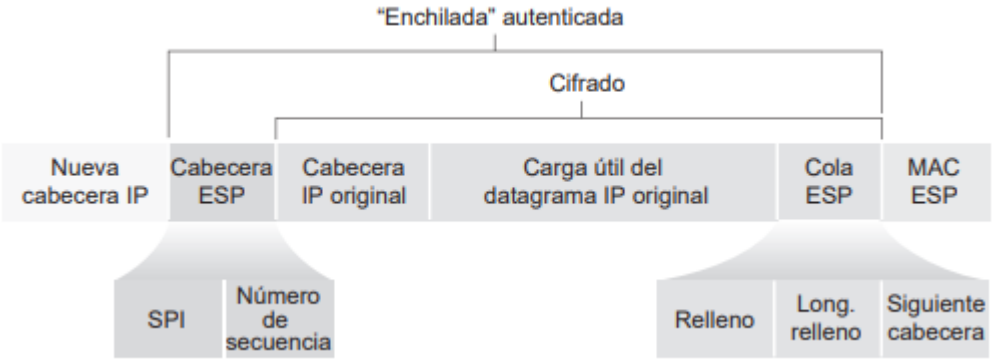
- Authentication Header AH: proporciona autenticación del origen e integridad de los datos.

- Encapsulation Security Payload ESP: proporciona autenticación del origen, integridad y confidencialidad.

Antes de enviar los paquetes, origen y destino establecen una conexión lógica llamada asociación de seguridad SA, que es una conexión simplex, unidireccional.

IPSec tiene dos formas de paquete.

- Modo túnel: más apropiado para las VPNs



- Añade al final del datagrama IPv4 original (¡que incluye los campos originales de cabecera!) un campo de "cola ESP".
- Cifra el resultado utilizando el algoritmo y la clave especificados por la asociación de seguridad.
- Añade al principio de este paquete cifrado un campo denominado "cabecera ESP"; el paquete resultante se conoce como "enchilada".
- Crea un valor MAC de autenticación para *toda la enchilada* utilizando el algoritmo y la clave especificados en la SA.
- Añade el valor MAC al final de la enchilada formando así la *carga útil.*
- Por último, crea una nueva cabecera IP con todos los campos clásicos de la cabecera IPv4 (que suman normalmente 20 bytes de longitud) y añade dicha cabecera al principio de la carga útil.

- Modo transporte