Modelo OSI - TCP / IP

Modelo OSI

MODELO OSI (lanzado en 1984 por la ISO *International Organization for Standarization*)

El proceso de transferir datos a través de una red es muy estructurado.
Puede visualizarse mejor mediante el empleo del modelo de Interconexión de sistema abierto (OSI, Open Systems Interconnection) de siete capas más conocido como el modelo OSI.

El modelo OSI divide las comunicaciones de red en varios procesos.

Cada proceso es una parte pequeña de una tarea más grande.

Por ejemplo, en una planta de fabricación de vehículos, una persona no ensambla todo el vehículo.
El vehículo se mueve entre estaciones o niveles en donde equipos especializados agregan diferentes componentes.
Cada estación agrega los componentes que tiene asignados y luego el vehículo pasa a la estación siguiente.
La compleja tarea de ensamblar un vehículo se simplifica cuando se divide en tareas lógicas más fáciles de manejar. Cuando ocurre un problema en el proceso de fabricación, es posible aislar el problema en la tarea específica donde se presentó el defecto para luego solucionarlo.

De manera similar, el modelo OSI puede ser utilizado como referencia en la resolución de problemas para identificar y resolver problemas de red.

Modelo OSI

El modelo OSI esta conformado por 7 capas, divididas en dos grupos principales:

Capas superiores

Definen como deben comunicarse las aplicaciones entre sí y con los usuarios. Involucra capas 5, 6 y 7.

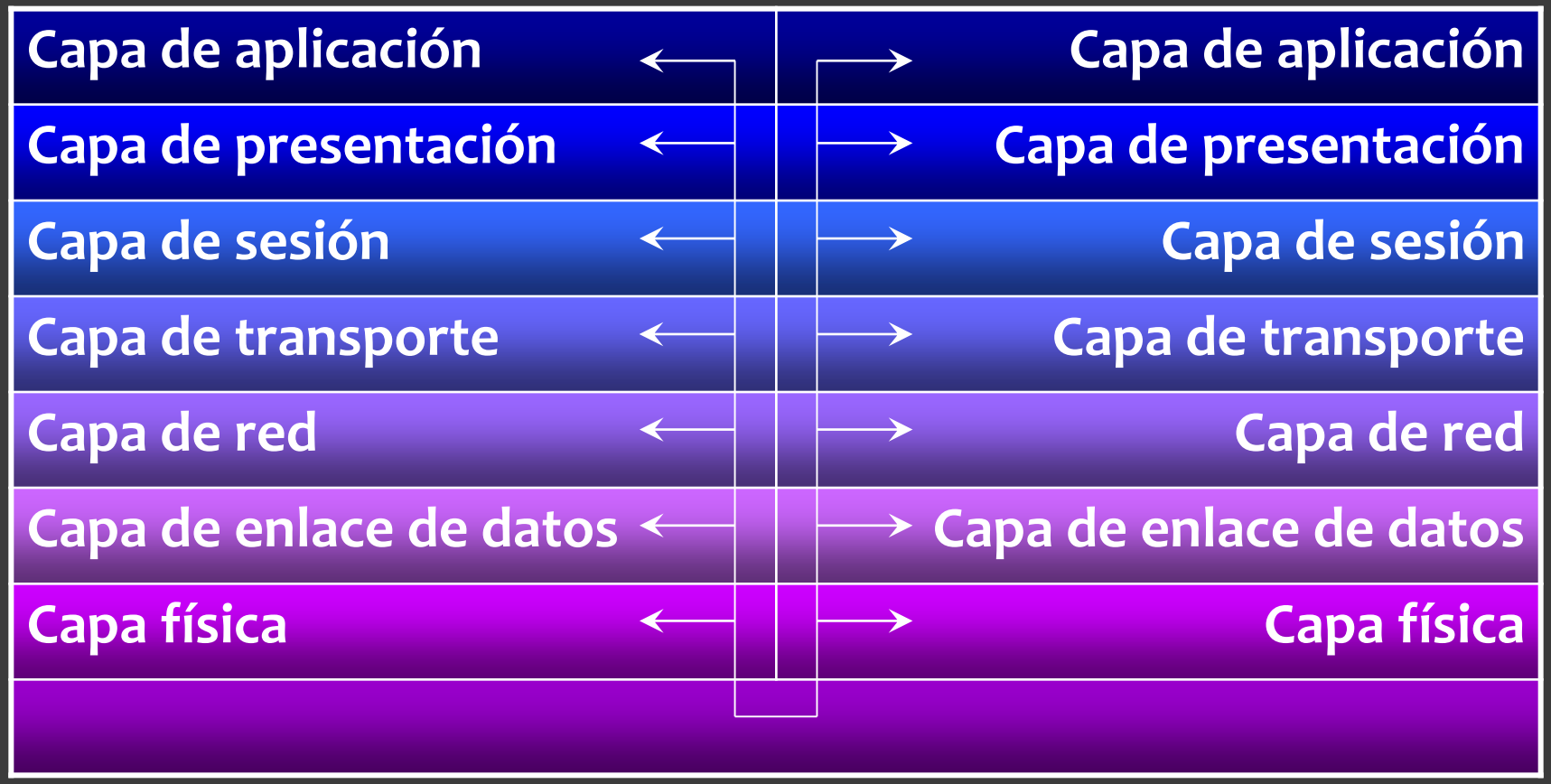
Capas inferiores

Definen como deben ser transmitidos los datos extremo a extremo. Involucra capas 1, 2, 3 y 4.

Esquema del modelo OSI:

Capa 7	Aplicación	Provee la interfaz entre las aplicaciones y los servicios de red
Capa 6	Presentación	Provee funciones de codificación, compresión y encriptación de datos
Capa 5	Sesión	Provee funciones de administración y control de comunicación
Capa 4	Transporte	Provee conexiones seguras y no seguras Provee corrección de errores
Capa 3	Red	Provee direccionamiento lógico
Capa 2	Enlace de Datos	Provee direccionamiento físico Provee funciones de detección de errores
Capa 1	Física	Envía la información de las capas superiores en forma de bits Define niveles de señal, medios de transmisión y conectores

OSI


Capa de aplicación
Capa de aplicación
Capa de presentación
Capa de presentación
Capa de sesión
Capa de sesión
Capa de transporte
Capa de transporte
Capa de red
Capa de red
Capa de enlace de datos
Capa de enlace de datos
Capa física
Capa física

Modelo OSI

- Capa de Aplicación: Es el nivel que se encarga de mostrar los datos al usuario. Aquí las aplicaciones como el Internet Explorer toman forma. Por ejemplo, este programa es la interfase entre el usuario y el modelo de capas.

- Capa de Presentación: Es la responsable de la traslación de datos y de la codificación y decodificación de la misma. Básicamente adapta los datos a formatos estándar. Por ejemplo ASCII, para que el host receptor pueda entenderlos.

- Capa de Sesión: es la encargada de negociar el modo de transmisión, ya sea half, simplex o dúplex.

- Capa de Transporte: esta capa se encarga de segmentar y reensamblar los segmentos de datos, y secuenciarlos de tal manera que en el otro extremo sean nuevamente ensamblados. Estable canales lógicos entre los dispositivos. Básicamente permite la multiplexación. Además posee funciones de control de flujo, con el objetivo de que un host no envíe más información de la cual el vecino no pueda procesar. La última función importante de esta capa, es asegurar el flujo orientado a la conexión.

- Capa de Red: se encarga del direccionamiento lógico de los datos, por medio de las direcciones IP. A su vez, proporciona mecanismos para encontrar la ruta óptima hacia el destino.

- Capa de Enlace: se encarga del control de flujo, notificación de errores, direccionamiento físico y de definir la topología física de la red. Se divide en dos partes: IEEE 802.3 MAC, que se encarga de definir como los paquetes son colocados en el medio, de direccionamiento físico y de cómo los host acceden al medio; y de IEEE 802.2 LCC que responde a la tarea específica de encapsular los protocolos de capa red, realizar el control de flujo e identificar los protocolos de nivel 3.

- Capa Física: es la responsable de la traducción de los frames en bits. Especifica los conectores, las señales eléctricas, los códigos, etc. Además indica la frontera entre el proveedor y el cliente, por medio de los Data Terminal Equipment –DTE- y los Data Communication Equipment –DCE-.

OSI - Protocolos

A continuación comenzaremos a explicar los protocolos empleados en la suite TCP/IP, según cada capa.

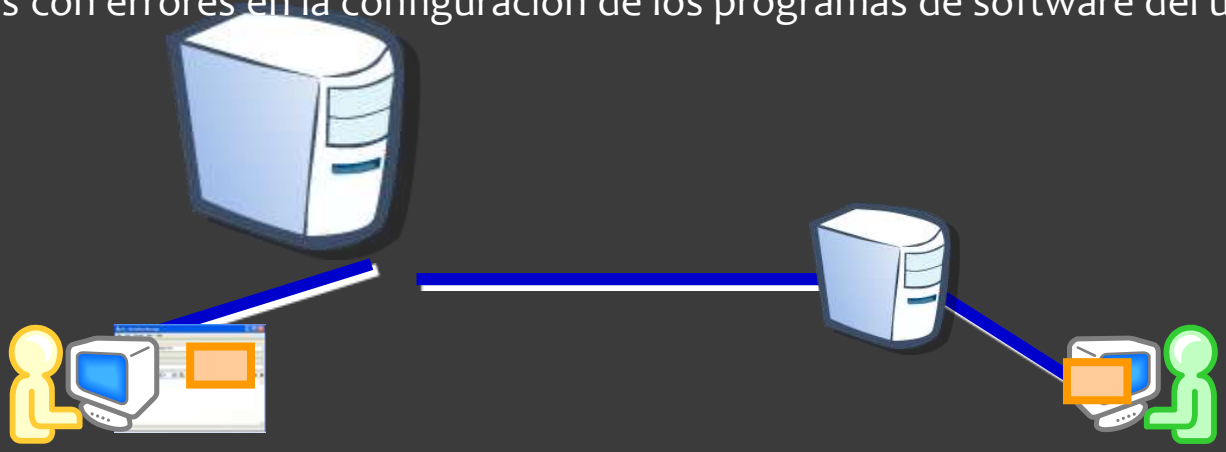
Grupo	#	Nombre	Tecnologia y protocolos	Componentes comunes
Capas superiores	7	Aplicación	DNS – DHCP – SNMP – FTP – POP3 – HTTP – TELNET	Aplicaciones compatibles con la red, correo electrónico, navegadores, servidores WEB
	6	Presentación	SSL – Shells – MIME	
	5	Sesión	NetBIOS Llamadas de procedimiento remoto	
Capas inferiores	4	Transporte	TCP & UDP	VoIP & Video – Firewall
	3	Red	IPv4 – IPv6 IPNAT – ARP RARP - ICMP	Direccionamiento IP – Ruteo
	2	Enlace de datos	Frame Ethernet – WLAN - ATM	Interfaces de red y controladores – WAN
	1	Física	Señales electricas – Ondas luminosas – Radio	Medios físicos, hubs y repetidores

OSI – Paso 1

Por ejemplo, para que el correo electrónico viaje exitosamente desde el cliente al servidor es necesario que se lleven a cabo muchos procesos. Observemos cómo el modelo OSI divide la tarea común de enviar y recibir correos electrónicos en pasos individuales y diferentes.

Paso 1: las capas superiores crean los datos.

Cuando un usuario envía un mensaje de correo electrónico, los caracteres alfanuméricos dentro del mensaje se convierten en datos que pueden viajar a través de la red.
Las Capas 7, 6 y 5 son responsables de asegurar que el mensaje sea colocado en un formato que pueda ser comprendido por la aplicación que se ejecuta en el host de destino.
Este proceso se denomina **codificación**.
Luego, las capas superiores envían los mensajes codificados a las capas inferiores para que sean transportados a través de la red.
El transporte del correo electrónico al servidor correcto depende de la información de configuración proporcionada por el usuario. Con frecuencia, los problemas que ocurren en la capa de aplicación están relacionados con errores en la configuración de los programas de software del usuario.



Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física

OSI – Paso 2

Paso 2: la Capa 4 empaqueta los datos para su transporte de extremo a extremo.

Los datos que componen el mensaje de correo electrónico son empaquetados para su transporte a través de la red en la Capa 4. La Capa 4 divide el mensaje en segmentos más pequeños. Se coloca un encabezado sobre cada segmento que indica el número de puerto TCP o UDP que corresponde con la capa de aplicación correcta. Las funciones de la capa de transporte indican el tipo de servicio de entrega.

El correo electrónico utiliza segmentos TCP; por lo tanto la entrega del paquete es reconocida por el destino. Las funciones de la Capa 4 se implementan en el software que se ejecuta en los host de origen y de destino. Sin embargo, los firewalls a veces utilizan los números de puerto TCP y UDP para filtrar el tráfico. En consecuencia, los problemas que se presentan en la Capa 4 pueden ser causados por la configuración incorrecta de las listas de filtros del firewall.

Capa de transporte
• **Agrupa los datos en paquetes para transportarlos a través de la red**
• **Agrega números a los puertos TCP y UDP**
• **Especifica una entrega confiable de los datos utilizando TCP**
• **Habilita el streaming ininterrumpido de datos utilizando UDP**

OSI – Paso 3

Paso 3: El Nivel 3 agrega la información de la dirección IP de la red.

Los datos de correo electrónico recibidos de la capa de transporte son colocados en un paquete que contiene un encabezado con las direcciones IP lógicas de origen y de destino. Los routers utilizan la dirección de destino para dirigir los paquetes a través de la red por la ruta apropiada.

La configuración incorrecta de la información de la dirección IP en los sistemas de origen y de destino puede ocasionar problemas en la Capa 3. Debido a que los routers también utilizan la información de la dirección IP, los errores de configuración del router también pueden ocasionar problemas en esta capa.

Capa de red
• **Rutea entre redes** • **Asigna direcciones IP** • **Encapsula datos en paquetes para la transmisión.**

OSI – Paso 4

Paso 4: la Capa 2 agrega el encabezado y tráiler de la capa de enlace de datos.

Cada dispositivo de red en la ruta desde el origen hasta el destino, inclusive el host emisor, encapsula el paquete en una trama. La trama contiene la dirección física del siguiente dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo. Los switches y las tarjetas de interfaz de red (NIC, network interface cards) utilizan la información en la trama para entregar el mensaje al dispositivo de destino correcto. Los controladores de NIC incorrectos, las tarjetas de interfaz o los problemas de hardware con los switches pueden ocasionar problemas en la Capa 2.

Capa de enlace de datos
• **Transmite datos al próximo dispositivo directamente conectado en la ruta** • **Agrega la dirección de hardware (MAC)** • **Encapsula los datos en una trama.**

OSI – Paso 5

Paso 5: La Capa 1 convierte los datos en bits para su transmisión.

La trama se convierte en un patrón de unos y ceros (bits) para la transmisión en el medio. Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio. El medio puede cambiar a lo largo de la ruta entre el origen y el destino. Por ejemplo, el mensaje de correo electrónico puede originarse en una LAN Ethernet, atravesar un backbone de fibra de universidades y atravesar un enlace serial WAN hasta que alcanza su destino en otra LAN Ethernet remota. Los problemas de Nivel 1 pueden ocasionarse por cables sueltos o incorrectos, tarjetas de interfaz en mal funcionamiento o interferencia eléctrica.

En el host receptor, los procesos descritos en los pasos 1 a 5 son a la inversa, el mensaje viaja de regreso a las capas superiores hacia la aplicación correcta.

Capa física
• **Convierte los datos a bits para su transmisión**
• **Genera señales y temporización**
• **1100010100101110110101001101010101001011101010101010101010101.**

Actividad

TCP | FTP | Ondas de radio | HTTP | UDP | Tramas | Direcciones IP | Software

HUBS | Direcciones MAC | Router | Telnet | Ethernet | NIC | Paquetes | Par trenzado

Capa Física	Capa de enlace de datos	Capa de red	Capa de transporte	Capas superiores

OSI – Resolucion de problemas

Capa 5 a 7: Capas superiores
¿Su explorador puede abrir el sitio web?
Capa 4: Transporte
¿Tiene un firewall configurado en su PC?
Capa 3: Red
¿Puede hacer un ping a su default gateway?
Capa 2: Enlace de datos
¿Esta encendido el LED de su NIC?
Capa 1: Física
¿Su cable de red esta enchufado?

Modelo TCP/IP

A pesar de que el modelo ampliamente usado es el OSI, con el advenimiento de Internet ha surgido otro modelo que se ha adaptado de una manera más simple a las comunicaciones, haciendo más incapie y detalle en las primeras 4 capas del OSI: Capa Física, Enlace, Red y Transporte.

Este modelo TCP/IP es también conocido como DoD.

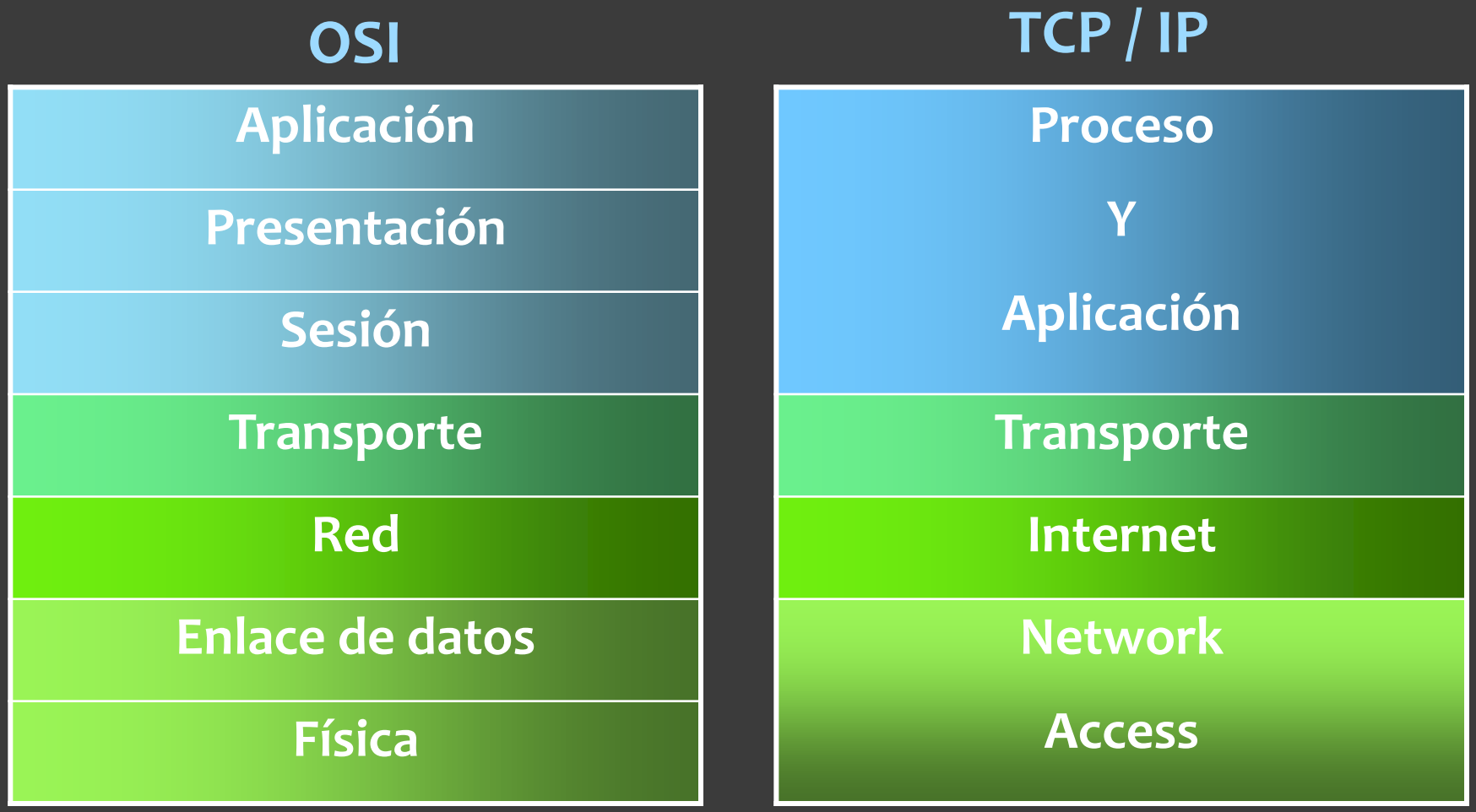
El modelo DoD (Departament of Defense) simplifica las funciones de las capas superiores del OSI, en *Aplicación*, en donde se detallan todas las especificaciones técnicas requeridas a usuarios, programas y protocolos que funcionan de host a host.

En la Capa de *Transporte*, o Host to Host, se asegura una comunicación confiable entre entidades, por medio de los circuitos virtuales, y además permite el traspaso de datos libre de errores. Como en la capa de Transporte, se mantiene la secuencia de los segmentos y el control de flujo.

La Capa de Internet, designa el camino óptimo hacia un destino por medio de los protocolos de enrutamiento, y de las direcciones lógicas. Como sabemos, esta capa no se encarga de mantener un flujo orientado a la conexión.

La Capa de Acceso del Modelo DoD, es la encargada del intercambio de datos entre los host, por medio de las direcciones físicas, y más abajo del modelo por medio de los bits.

Modelo TCP/IP



Protocolo TCP

Protocolo TCP

Es uno de los protocolos que le da nombre a la suite. Recibe unidades de datos de la Capa de Aplicación y la va desarmando en bloques más pequeños denominados Segmentos.

A estos segmentos, antes de enviar a la Capa de Red, lo enumera o secuencia, de modo tal que el host receptor pueda reensamblar los paquetes. Luego de que los paquetes son enviados a la red, el protocolo espera un acuse de recibo –ack- por parte del par TCP, debido a que este es un protocolo *orientado a la conexión*.

Este ack es utilizado además para un fin muy importante: el *control de flujo*.

El control de flujo evita que se saturen los buffers de los routers o host, de manera tal de no atravesar la situación en donde el receptor no pueda procesar toda la información que el emisor está enviando. Herramientas para evitar esto, son las siguientes:

No se enviarán más segmentos que el tamaño de la ventana TCP, sin haber recibo los ack.
Cualquier segmento sin ack es retransmitido.
Se administra el flujo de datos de manera de evitar la congestión y la pérdida de paquetes.

Como ya hemos mencionado, TCP es un protocolo confiable. No en el significado subjetivo de la palabra, sino que es "confiable" porque se estable una comunicación entre los host antes de intercambiar cualquier tipo de datos.

Esta sesión consta de tres pasos, denominados Handshake. Veamos a continuación el ejemplo.

Protocolo TCP

Como ya hemos mencionado, TCP es un protocolo confiable. No en el significado subjetivo de la palabra, sino que es “confiable” porque se estable una comunicación entre los host antes de intercambiar cualquier tipo de datos.

Esta sesión consta de tres pasos, denominados Handshake. Veamos a continuación el ejemplo.

Como observamos el primer paso es un requerimiento de sincronización, probablemente inducido por una aplicación. Luego el receptor envía un ack indicando que recibió la petición, y negocia con el par, los parámetros principales del la sesión TCP.

El ultimo paso consiste en el ack por parte del emisor, de que la sesión ha quedado establecida, que el circuito virtual se ha creado y que ahora es viable intercambiar información.

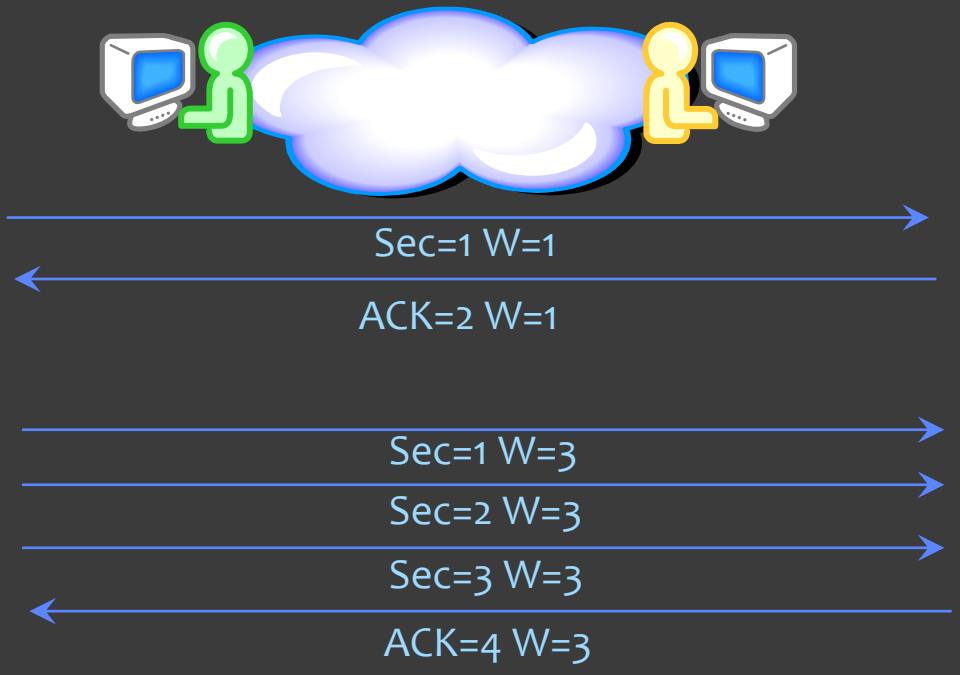
TCP - Window

Supongamos, que uno de los host empieza a enviar demasiada información al receptor, y este para atender esta tarea, dedica gran cantidad de recursos y CPU al descongestionamiento del búffer de memoria. Esta acción atentaría contra los demás procesos del Host.

Otra característica de los protocolos orientados a la conexión, además de los circuitos virtuales y los acuses de recibo y retransmisión, es el *control de flujo por medio de la Ventana*.

"La Ventana o Window TCP es la cantidad segmentos que puedo enviar al receptor sin haber recibido un ack por parte del host par."

Veamos el siguiente esquema donde tenemos una ventana de 1 y luego de 3 segmentos.



TCP - Window

Positive Acknowledment & retransmition, es la técnica que emplea TCP para poder asegurarse que la transmisión de datos sea íntegra y fiable. Básicamente un ack es un paquete en sentido contrario al original que indica al emisor que la recepción del segmento ha sido exitosa. Esta acción tiene como consecuencia, que el contador que indica la ventana aumente en 1 nuevamente.

Por otra parte, el host emisor además de esperar el ack, inicia un contador por un tiempo determinado.

Si el segmento no posee ack o bien este contador expira, el segmento es retransmitido.

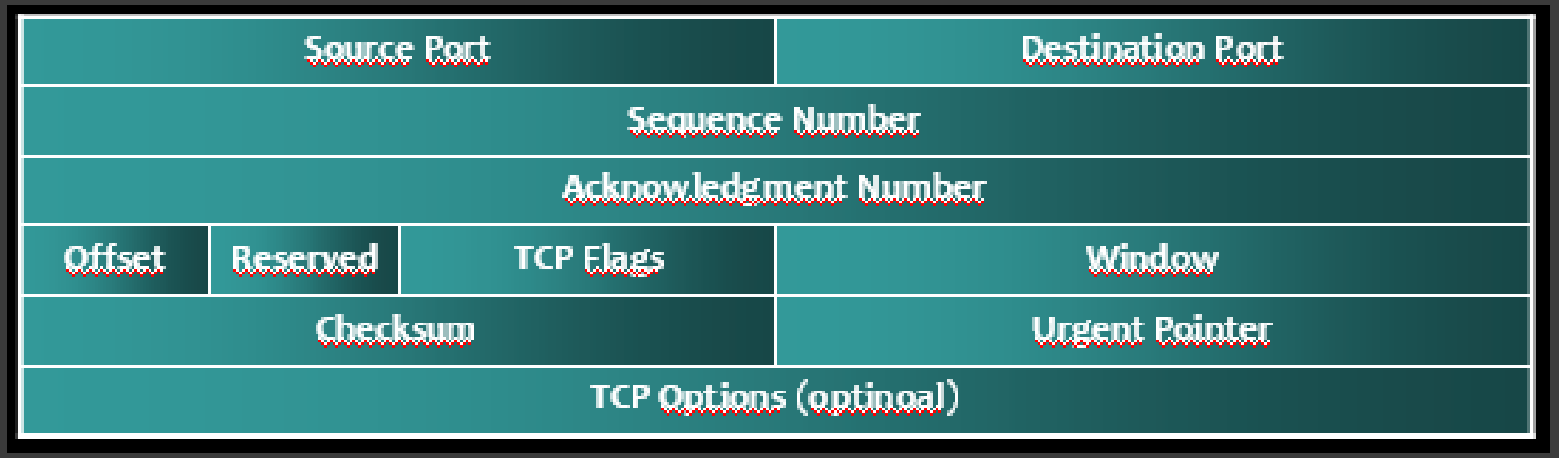
TCP asegura que los paquetes llegan en orden, y cuando no lo hacen posee el mecanismo de ack para arreglar el inconveniente.

El receptor detecta que recibió un segmento sec=6, pero que el segmento sec=5 nunca llegó. Por lo tanto antes de enviar el ack para el segmento 6, solicita por un ack la retransmisión del segmento 5

TCP - Window

Protocolo TCP – Acuses de recibo

TCP - Formato



- Source Port: identifica el puerto origen de la aplicación.
- Destination Port: identifica el puerto destina de la aplicación.
- Sequence Number: campo utilizado para poder reordenar los segmentos.
- ACK Number: es el SN que se espera recibir.
- Header Length: indica la longitud del encabezado, ya que con el campo “Options” puede ser más extenso.
- Reserved: campo en 0s.
- Code Bits: campo usado para iniciar y cerrar la sesión TCP.
- Window: el tamaño de la ventana, en octetos.
- Checksum: campo usado para verificar que el segmento esté libre de errores. Usa CRC.
- Urgent: solo se setea según el campo “code bits” actue o no.
- Options: múltiplos de 32 bits, que permite tener opciones adicionales, según la aplicación que se monte.

Protocolo UDP

Protocolo UDP

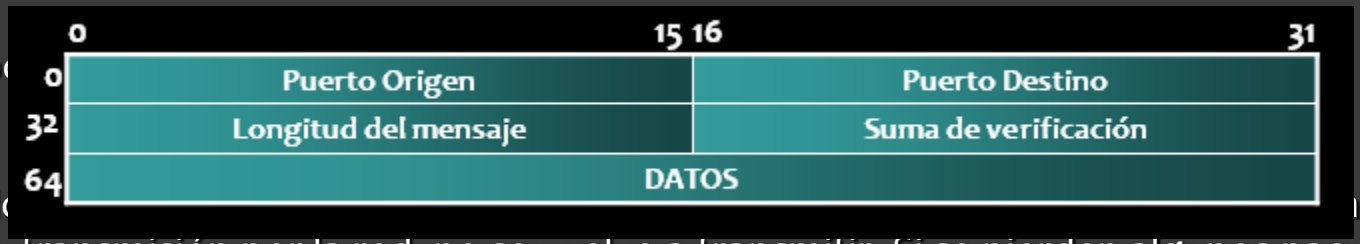
User Datagram Protocol, es al versión simplificada de TCP, permitiendo a las aplicaciones que no requieran una conexión confiable brindar un servicio más flexible, y que requiera menos ancho de banda.

UDP no es Orientado a la conexión, de manera tal que no asegura que los datagramas lleguen a destino, o bien puedan llegar en desorden, ya que solo toma los puertos origen/destino y el checksum.

Por ejemplo si usted desea emplear SNMP, no hace falta que este tenga una conexión abierta con cada host, por ende UDP es ideal para este caso.

Solo cabe mencionar, que aquí el campo Length marca la longitud de todo el datagrama, y no solo el Header como en TCP.

UDP tamp

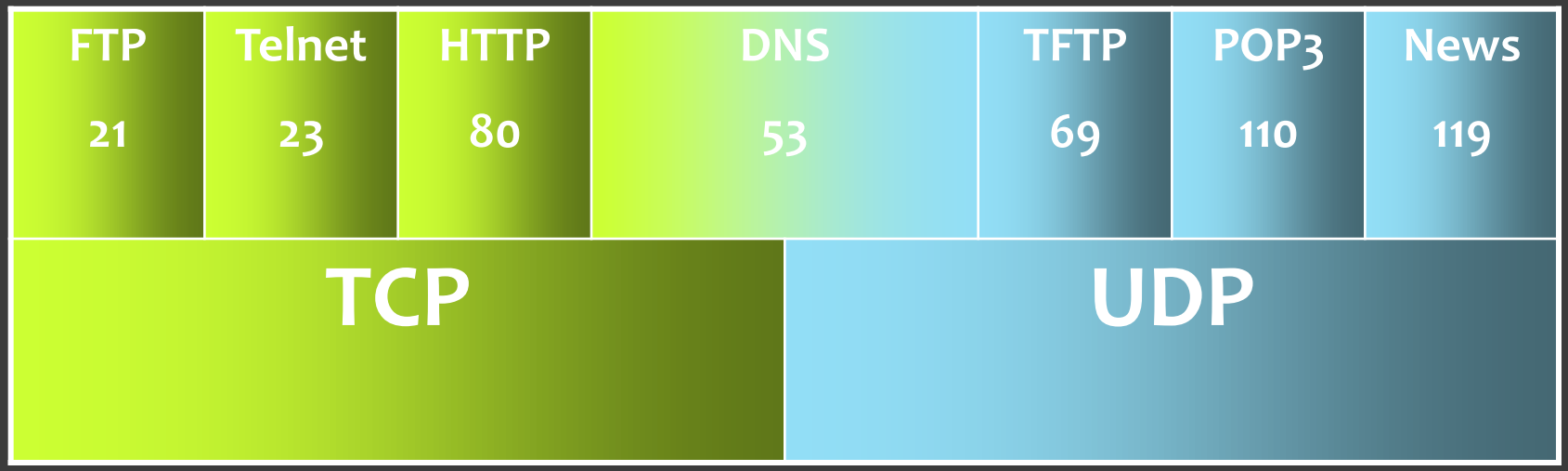


Un ejemplo saje se pierde durante su transmisión por la red, no se vuelve a transmitir. Si se pierden algunos paquetes, el oyente podrá escuchar una breve interrupción en el sonido. Si se utilizara TCP y se volvieran a enviar los paquetes perdidos, la transmisión haría una pausa para recibirlos, y la interrupción sería más notoria.

Protocolo UDP

Según la RFC 3232 los puertos menores a 1024 son denominados “bien conocidos” y son estándar para la Industria.

Los números por encima de 1024 pueden ser usados por cualquier aplicación, para comunicarse con otros host.



Protocolos TCP/UDP - Puertos

Actividad

1) Utiliza confirmaciones para garantizar la entrega

UDP TCP

2) Se adapta a las transmisiones de voz

UDP TCP

3) No vuelve a transmitir lo que se descartaron

UDP TCP

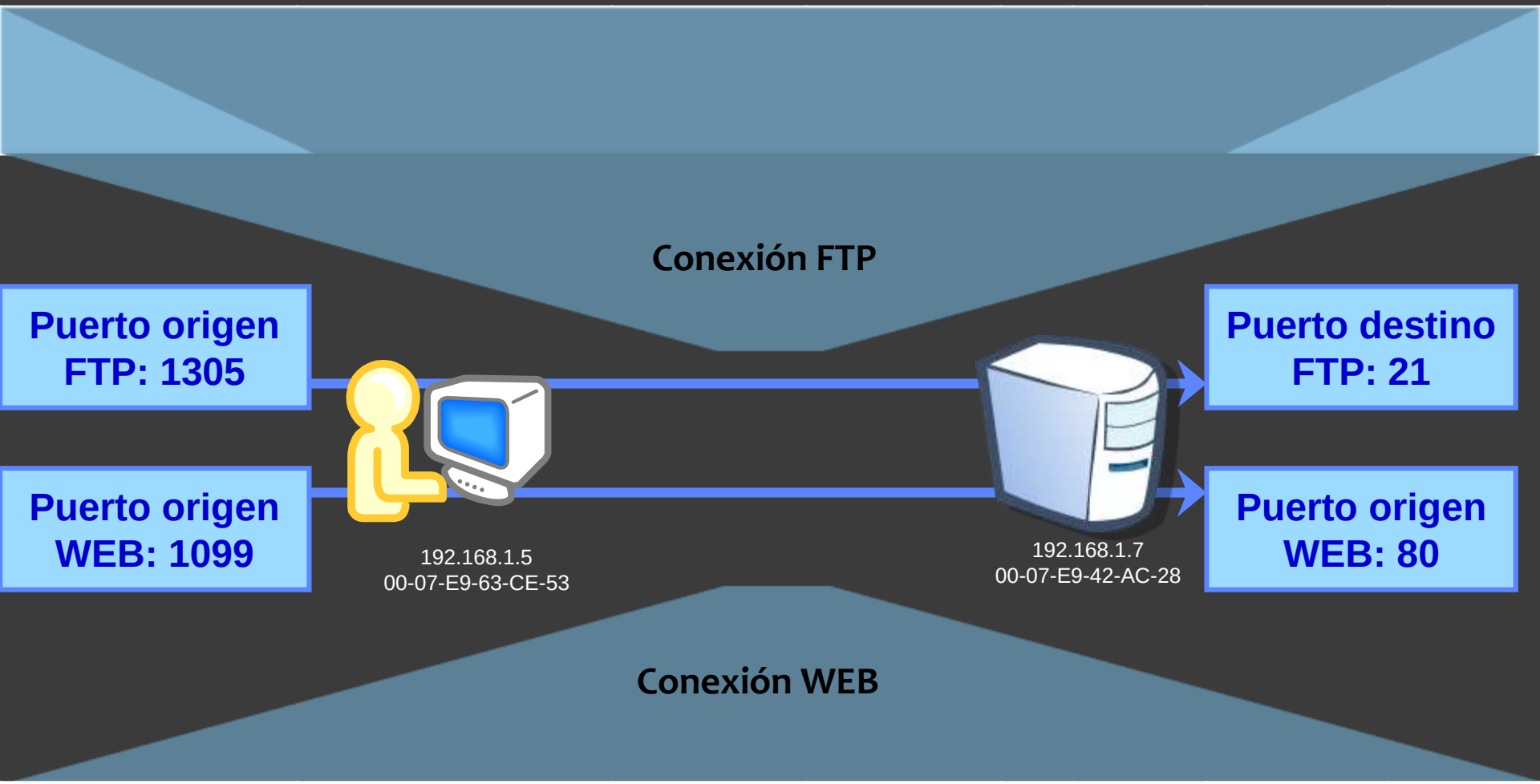
4) Se utiliza en aplicaciones de tiempo real (straming de video)

UDP TCP

5) Se utiliza en aplicaciones como HTTP

UDP TCP

Números de puertos – TCP/IP



00-07-E9-42-AC-28	00-07-E9-63-CE-53	192.168.1.7	192.168.1.5	80	1099	Datos de usuario	Tráilers
MAC Destino	MAC Origen	IP Destino	IP Origen	Puerto Destino	Puerto Origen		

TCP/IP - Protocolos

Protocolo Telnet

Telnet es un emulador de terminal en modo texto básicamente, que permite a un usuario remoto ingresar a un equipo que posee un Telnet Client, simulando que el terminal remoto está en la red local. "Telnetearse" a un equipo, le permite al administrador de la red, simular como si estuviese conectado desde la consola del equipo, facilitando la administración total de toda la red desde un punto central. Este protocolo emplea el puerto TCP 23, que lo identifica en la capa 4, o host to host según el modelo.

Protocolo FTP

File Tranfer Protocol, es el protocolo por excelencia para el envío de archivos de gran tamaño de una manera confiable y segura. Además de ser un protocolo, es una aplicación a diferencia de la mayoría. Se puede acceder por FTP a un host para bajar un archivo, y a partir de tal acción, el programa de FTP puede contener una variedad de funciones como loggin, validación, etc.
Utiliza TCP como protocolo de transporte.

TCP/IP - Protocolos

Protocolo NFS

Network File System es un protocolo que se emplea para compartir archivos en una red, permitiendo a 2 tipos diferentes de sistema de archivos interoperar. NFS puede correr sobre Win NT o bien sobre Unix.
Permite por ejemplo que usuarios de Unix y Win NT compartan archivos, alojando en la RAM del servidor NT algunos archivos Unix.

Protocolo Line Printer Daemon (LDP)

Se emplea para compartir impresoras, o sea para que las mismas estén en red vía un print server.

X WIndow

Por medio de un esquema cliente/servidor define la manera en que las aplicaciones funcionan bajo esa modalidad por medio de una Interfase visual.

Protocolo SNMP

Simple Network Managment Protocol (SNMP) almacena información recolectada por traps enviados por los dispositivos que funcionan con SNMP, a los fines de facilitar el managment de la red. Por medio de este protocolo, se puede verificar el estado de los equipos, de las interfases, etc.

TCP/IP - Protocolos

Protocolo POP3/SMTP/IMAP4

Protocolo simple de transferencia de correo (SMTP, Simple Mail Transfer Protocol)

SMTP es utilizado por un cliente de correo electrónico para enviar mensajes a su servidor de correo electrónico local. El servidor local entonces decide si el mensaje se destina a un buzón local o si se remite a un buzón de otro servidor.

Si el servidor tiene que enviar el mensaje a un servidor diferente, también se utiliza SMTP entre los dos servidores. Las solicitudes de SMTP se envían al puerto 25.

Protocolo de oficina de correos (POP3, Post Office Protocol)

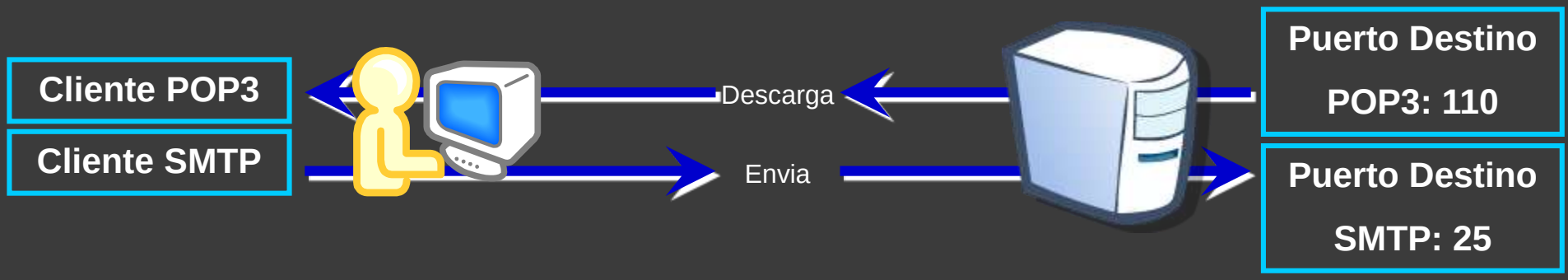
Un servidor que soporta clientes POP recibe y almacena mensajes dirigidos a sus usuarios. Cuando el cliente se conecta con el servidor de correo electrónico, los mensajes se descargan al cliente. Por defecto, los mensajes no se retienen en el servidor una vez que el cliente accede a ellos. Los clientes se ponen en contacto con los servidores POP3 en el puerto 110.

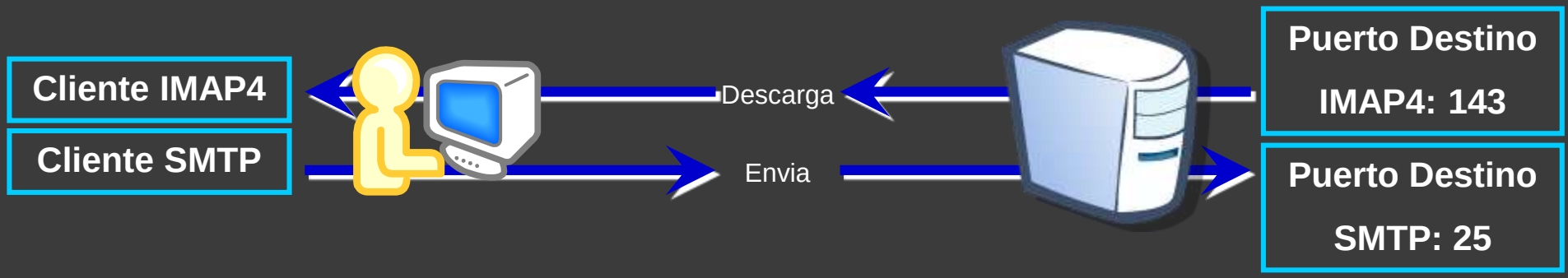
Protocolo de acceso a mensajes de Internet (IMAP4, Internet Message Access Protocol)

Un servidor que soporta el cliente IMAP también recibe y almacena los mensajes dirigidos a sus usuarios. Sin embargo, conserva los mensajes en los buzones del servidor, a menos que el usuario los elimine. La versión más actual de IMAP es IMAP4, que espera las solicitudes del cliente en el puerto 143.

Existen muchos servidores de correo electrónico diferentes para las diversas plataformas de sistema operativo de la red.

TCP/IP - Protocolos





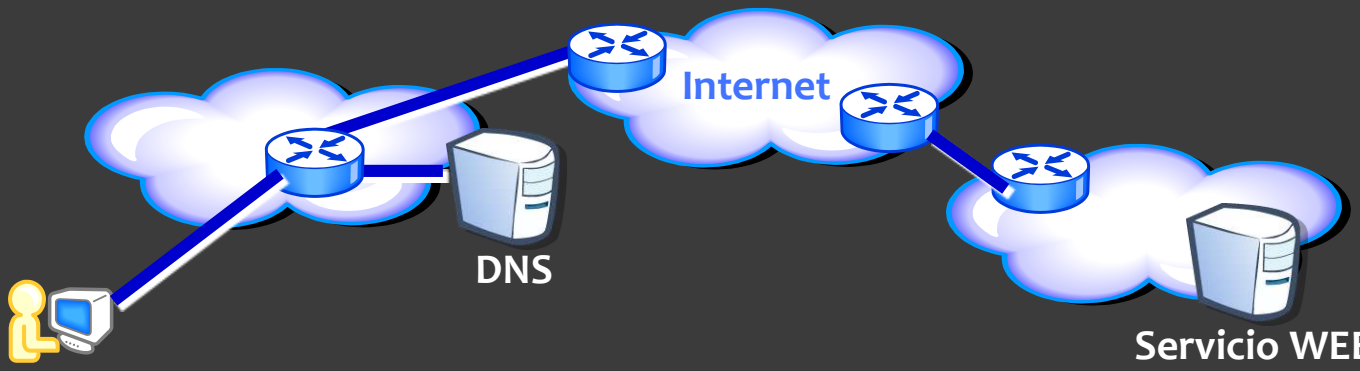
TCP/IP - Protocolos

Protocolo DNS

Domain Name Server, es el encargado de resolver todos los nombres de dominios de Internet. Cuando en un buscador ingresamos www.google.com, el IE genera un requerimiento a un Servidor de DNS que traduce esa palabra en una Dirección IP de un servidor. Emplea la nomenclatura jerárquica para resolver los dominios. Por ejemplo: www.ole.clarin.com.ar indica al protocolo que comience la búsqueda en páginas de Argentina, luego en páginas comerciales, luego en Clarin, y finalmente en el html "ole".

Un servidor DNS contiene una tabla que asocia los nombres de hosts de un dominio con las direcciones IP correspondientes. Cuando un cliente tiene el nombre de un servidor, como un servidor Web, pero necesita encontrar la dirección IP, envía una solicitud al servidor DNS en el puerto 53. El cliente utiliza la dirección IP del servidor DNS configurada en los parámetros DNS de la configuración IP del host.

Cuando el servidor DNS recibe la solicitud, verifica la tabla para determinar la dirección IP asociada con ese servidor Web. Si el servidor DNS local no tiene una entrada para el nombre solicitado, realiza una consulta a otro servidor DNS dentro del dominio.



Nslookup (*Name System Lookup*)

Es una herramienta que permite consultar un servidor de nombres y obtener información relacionada con el dominio o el host y así diagnosticar los eventuales problemas de configuración que pudieran haber surgido en el DNS.

Utilizado sin ningún argumento, el comando *nslookup* muestra el nombre y la dirección IP del servidor de nombres primario y una invitación de comando para realizar consultas. Basta con introducir el nombre de un dominio en la invitación de comando para detallar las características. De la misma manera, es posible solicitar información sobre un host indicando su nombre seguido del comando *nslookup*:

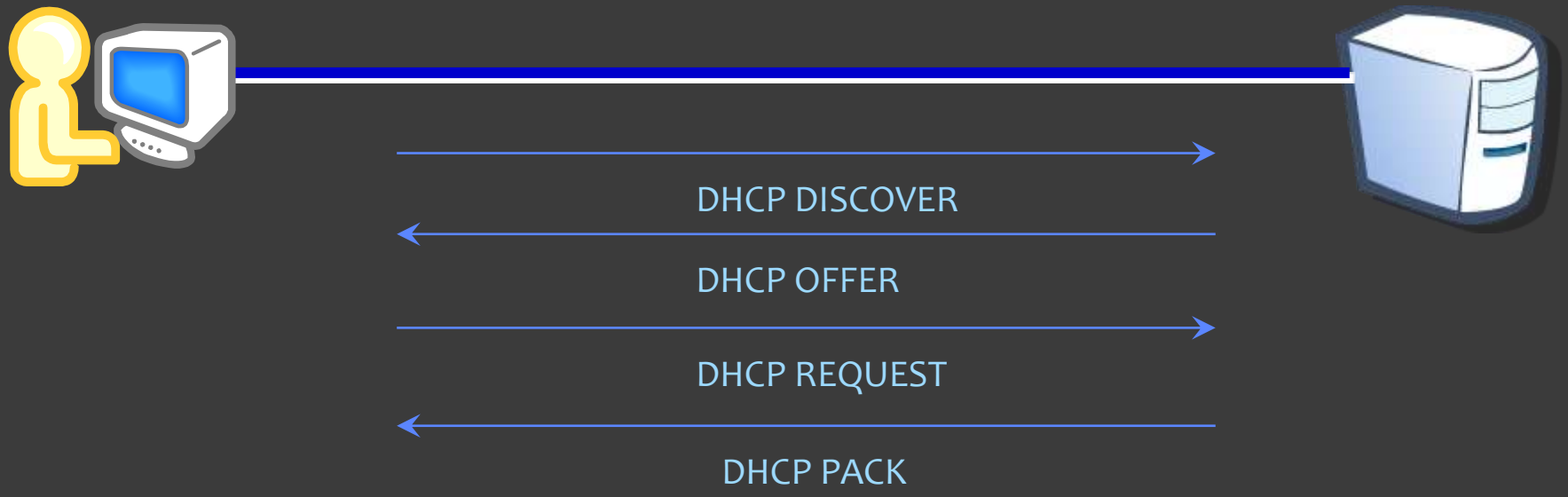
nslookup nombre.del.host

TCP/IP - Protocolos

Protocolo DHCP

Dinamic Host Configuration Protocol (DHCP) asigna de manera dinámica direcciones IP a los host de una red, evitando así que el administrador tenga que localmente configurar las mismas. Es muy útil para redes grandes, y trabaja bajo el esquema de un DHCP Server.
DHCP puede enviarle a un host, cuando se conecta a un red, la siguiente información: IP address, Máscara de subred, Default Gateway, nombre de dominio, información de WINS.

Los host para recibir esta información envían un DHCP "Discover Message", realizando un broadcast de nivel 2 y 3, o sea un FF:FF:FF:FF:FF:FF y 255.255.255.255. Emplea UDP, por ende no es orientado a la conexión. Una vez que todos los host reciben el paquete con la solicutud DHCP, el DHCP Server responde mínimamente con la IP, la máscara y el DG.



Protocolo IP
Internet Protocol

Protocolo IP

- **Internet Protocol es el segundo pilar de la Suite. En él se define el direccionamiento lógico y los protocolos de enrutamiento.**

IP, es un protocolo ruteado, no fiable y no orientado a la conexión. A diferencia del direccionamiento de nivel 2, en IP se rutean redes (en nivel 2 se direcciona mac a mac). Por ende las tablas de enrutamiento de los routers se poblan de entradas a redes, y no host particulares, como lo hace una tabla mac-address de un switch por ejemplo.

El rol fundamente de IP, es brindar del direccionamiento lógico.

Al tener esta función principal, IP debe ser complementado con otra serie de protocolos para diferentes fines, por ejemplo:

ICMP: para diagnósticos de fallas.
IPSec: para poder encriptar el tráfico IP.
DNS: para resolver las direcciones IP en nombres de dominio.
…
…
…

IP - Formato

- **Version**: la actual Version 4, pero el IPv6 está creciendo a nivel mundial.
- **Header Length**: longitud del encabezado.
- **Type of Service**: campo que se emplea para dar prioridad a ciertos paquetes sobre otros. Se modifica con el Diffserv y el creciemiento de las redes IP/MPLS con QoS
- **Total Length**: longitud de todo el paquete.
- **ID**: único valor para IP.
- **Flags**: se marca cuando hay fragmentación.
- **Fragment offset**: se emplea cuando la fragmentación ocurre, de modo tal de poder reemsamblar los paquetes en el otro extremo.
- **Time to Live**: campo que se emplea para evitar loops de ruteo.
- **Protocol**: identifica el protocolo de nivel 4 que se está transportando. TCP=6; UDP=17; ICMP=1; OSPF=89; EIGRP=88; L2TP=115; IGRP=9; IP en IP (túnel) = 4
- **Header Checksum**: se verifica con un CRC solo el encabezado.
- **Source IP**: dirección IP de 32 bits origen.
- **Destination IP**: dirección IP de 32 bits destino.
- **Options**: usado para debug, seguridad, etc.
- **Data**: información a transportar.

Clases

Para poder hacer frente a la demanda, se requerían más números únicos de red. Para crear más designaciones posibles de red, el espacio de dirección de 32 bits fue organizado en cinco clases. Tres de estas clases, A, B y C, otorgan direcciones que pueden ser asignadas a hosts o redes individuales. Las otras dos clases, D y E, se reservan para multicast y uso experimental. La división de las redes originales de ocho bits en clases más pequeñas aumentó de 256 a más de dos millones la cantidad de designaciones de red disponibles.

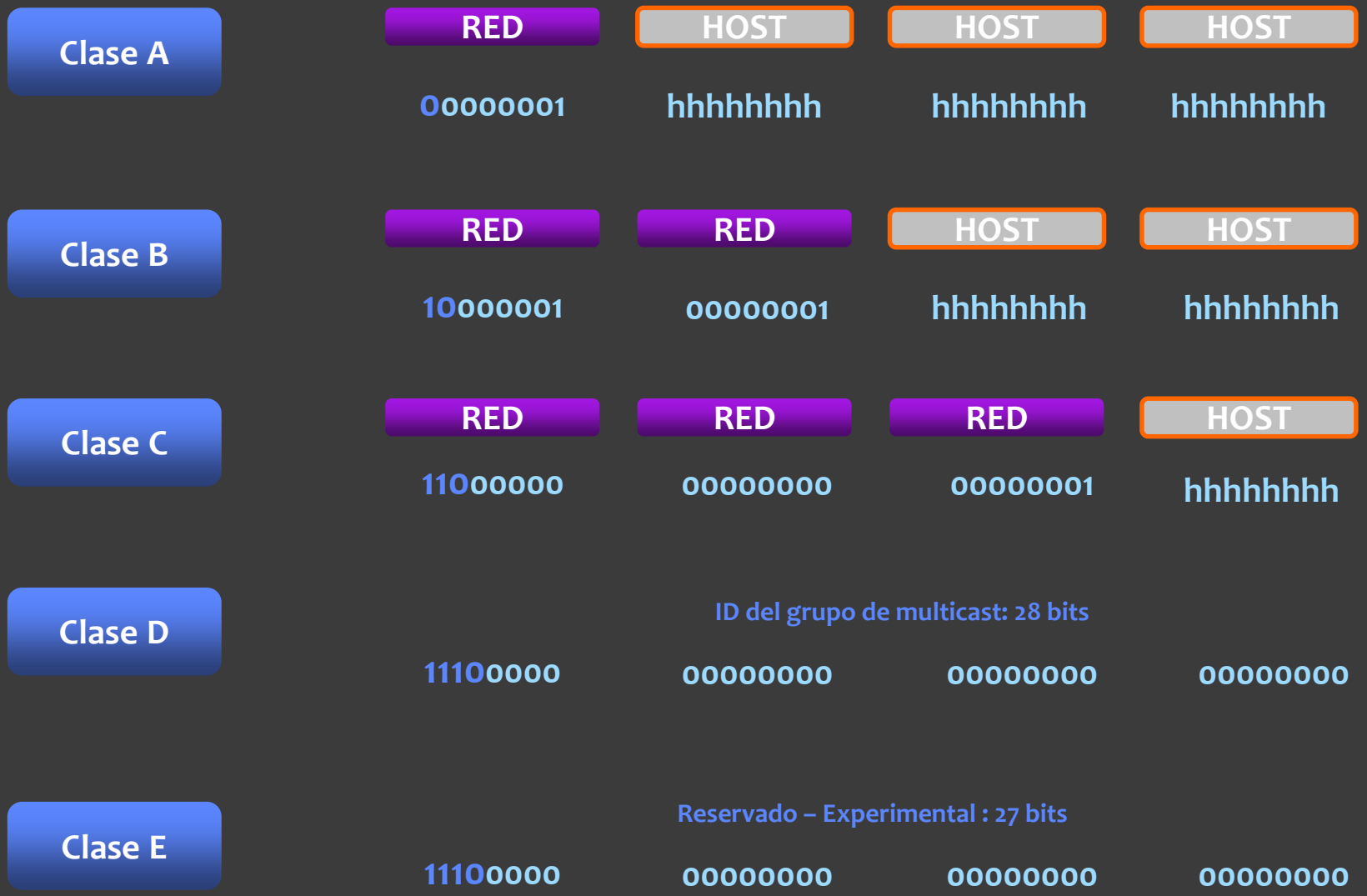
Antes de este cambio, los routers examinaban sólo los primeros 8 bits de una dirección IP para la ID de red. ¿Cómo sabrían los routers ahora mirar más allá de los primeros 8 bits para identificar las redes clase B o C?

Se decidió dividir las redes de modo tal que fuese sencillo para los routers determinar la cantidad correcta de bits de identificación de la red. Los valores de los primeros bits de las direcciones IP, denominados bits de orden superior, son los que indican la clase de red.

Si el primer bit es 0, la red es de Clase A y el primer octeto representa el ID de la red, y los otros 3 para identificar al host. Cuando el primer bit es 1, el router examina el segundo bit. Si ese bit es 0, la red es de Clase B, y el router utiliza los primeros 16 bits para el ID de la red. Si los primeros tres bits son 110, indica que la dirección es de Clase C. Las direcciones clase C utilizan los primeros 24 bits, o tres octetos, para designar la red, y 1 octeto para designar el Host.

A lo mencionado anteriormente, debemos mencionar por obviedad, que las redes Clases A por defecto utilizan máscaras de red del 255.0.0.0; las Clases B 255.255.0.0; las Clases C 255.255.255.0.

Clases

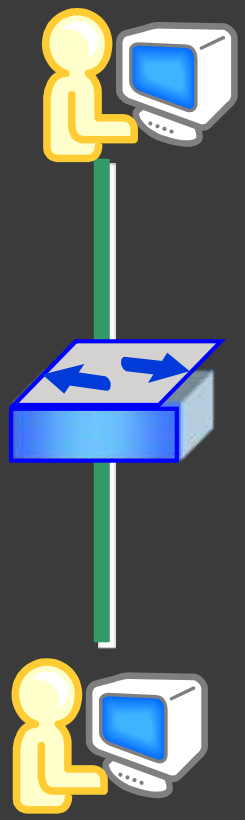

Clase A
RED
HOST
HOST
HOST
0oooooo1
hhhhhhhh
hhhhhhhh
hhhhhhhh
Clase B
RED
RED
HOST
HOST
10ooooo1
oooooooo1
hhhhhhhh
hhhhhhhh
Clase C
RED
RED
RED
HOST
110ooooo
oooooooo
oooooooo1
hhhhhhhh
Clase D
ID del grupo de multicast: 28 bits
1110oooo
oooooooo
oooooooo
oooooooo
Clase E
Reservado – Experimental : 27 bits
1110oooo
oooooooo
oooooooo
oooooooo

Clases

Clase de dirección	Rango primer octeto (decimal)	Bits del primer octeto	Red (N) Host (H)	Mascara de Subred por defecto	Cantidad de redes y host
A	1 – 126	00000000 01111111	N.H.H.H	255.0.0.0	126 Redes 16777214 host por red
B	128 – 191	10000000 10111111	N.N.H.H	255.255.0.0	16382 Redes 65534 host por red
C	192 - 223	11000000 11011111	N.N.N.H	255.255.255.0	2097150 redes 254 hosts por red
D	224 - 239	11100000 11101111	No es para uso comercial		Multicast 224.0.0.0 239.255.255.255
E	240 – 255	11110000 11110111	No es para uso comercial		*Reservada* 240.0.0.0 255.255.255.255

Interacción entre las IP y máscaras

192.168.1.44
255.255.255.0



192.168.1.66
255.255.255.0

192.168.1.44 255.255.255.0

11000000.10101000.00000001.00101100 11111111.11111111.11111111.00000000

11000000.10101000.00000001.00000000

192.168.1.0

Cada dirección IP consta de dos partes. ¿Cómo saben los hosts qué parte pertenece a la red y cuál al host? Éste es el trabajo de la máscara de subred.

Cuando se configura un host IP, se asigna una máscara de subred junto con una dirección IP. Como sucede con la dirección IP, la máscara de subred tiene una longitud de 32 bits. La máscara de subred identifica qué parte de la dirección IP corresponde a la red y cuál al host.

La máscara de subred se compara con la dirección IP, de izquierda a derecha, bit por bit. Los 1 en la máscara de subred representan la porción de red, los 0 representan la porción de host. En el ejemplo que se muestra, los primeros tres octetos pertenecen a la red y el último octeto representa el host.

Cuando un host envía un paquete, compara su máscara de subred con su propia dirección IP y la dirección IP de destino (acción lógica AND). Si los bits de la red coinciden, tanto el host de origen como el de destino se encuentran en la misma red, y el paquete puede ser enviado localmente. Si no coinciden, el host emisor envía el paquete a la interfaz del router local para que sea enviado a otra red.

Internet Protocol Version 6

IPv6

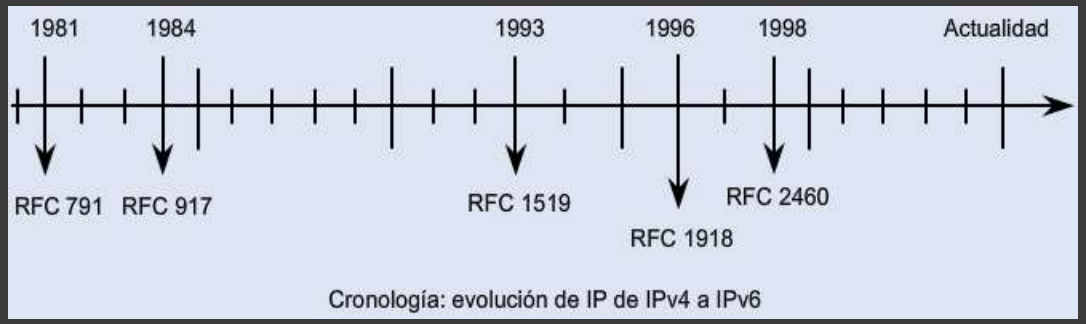
CIDR y el direccionamiento IP privado fueron desarrollados para brindar una solución temporal al problema del agotamiento de las direcciones IP. Estos métodos, a pesar de ser útiles, no creaban más direcciones IP. IPv6 lo hace.

IPv6 fue el primero propuesto en 1998 con RFC 2460.

Aunque su finalidad principal era solucionar el agotamiento de direcciones IP de IPv4, hubo otras buenas razones para su desarrollo. Desde que se estandarizó IPv4, Internet ha crecido de manera significativa. Este crecimiento ha revelado ventajas y desventajas de IPv4 y la posibilidad de actualizaciones para incluir nuevas capacidades.

Una lista general de las mejoras que IPv6 propone incluye:
más espacio de dirección
Mejor administración del espacio de dirección;
administración de TCP/IP simplificada;
capacidades de enrutamiento modernizadas; y
soporte mejorado para multicast, seguridad y movilidad.

El desarrollo de IPv6 intenta abordar tantos de estos requisitos y problemas como sea posible.



Cronología: evolución de IP de IPv4 a IPv6

Comparación de IPv4 e IPv6

El espacio de direcciones IPv4 proporciona aproximadamente 4,3 mil millones de direcciones. De dicho espacio de direcciones, aproximadamente 3,7 mil millones de direcciones son realmente asignables. Las otras direcciones se reservan para casos especiales como multicast, espacio de direcciones privadas, loopback de prueba, e investigación. Hay pocos rangos de dirección IPv4 disponibles para asignar. Algunos ISP están comenzando a repartir asignaciones de dirección IPv6.

Una dirección IPv6 es un valor binario de 128 bits, que puede mostrarse como 32 dígitos hexadecimales. Proporciona direcciones IP de 3,4 X 10^38.

IPv4
- 32 bits o 4 bytes de longitud.
- 4200000000 nodos direccionables posibles.

IPv6
- 128 bits o 16 bytes: Cuatro veces los bits de IPv4
- 340282366920938463374607432768211456 nodos direccionables posibles

Comparación IPv4 e IPv6

El IPv6 ofrece potentes mejoras sobre el IPv4. Las mejoras incluyen:

- Movilidad y seguridad.
- Encabezado más simple.
- Formato de dirección.

Movilidad y seguridad

La movilidad permite a las personas que tienen dispositivos de red móviles desplazarse por las redes. IP móvil es un estándar IETF que está disponible tanto para IPv4 como para IPv6. Este estándar permite a los dispositivos móviles trasladarse sin interrupciones en las conexiones de red establecidas. El IPv4 no admite este tipo de movilidad. La movilidad es una característica de IPv6.

IPSec es el estándar IETF para la seguridad de la red IP. Está disponible tanto para IPv4 como para IPv6. Las funciones de seguridad de la red IP son esencialmente idénticas en ambos entornos. IPSec está más estrictamente integrado al IPv6 y puede habilitarse en todos los nodos IPv6.

Encabezado más simple

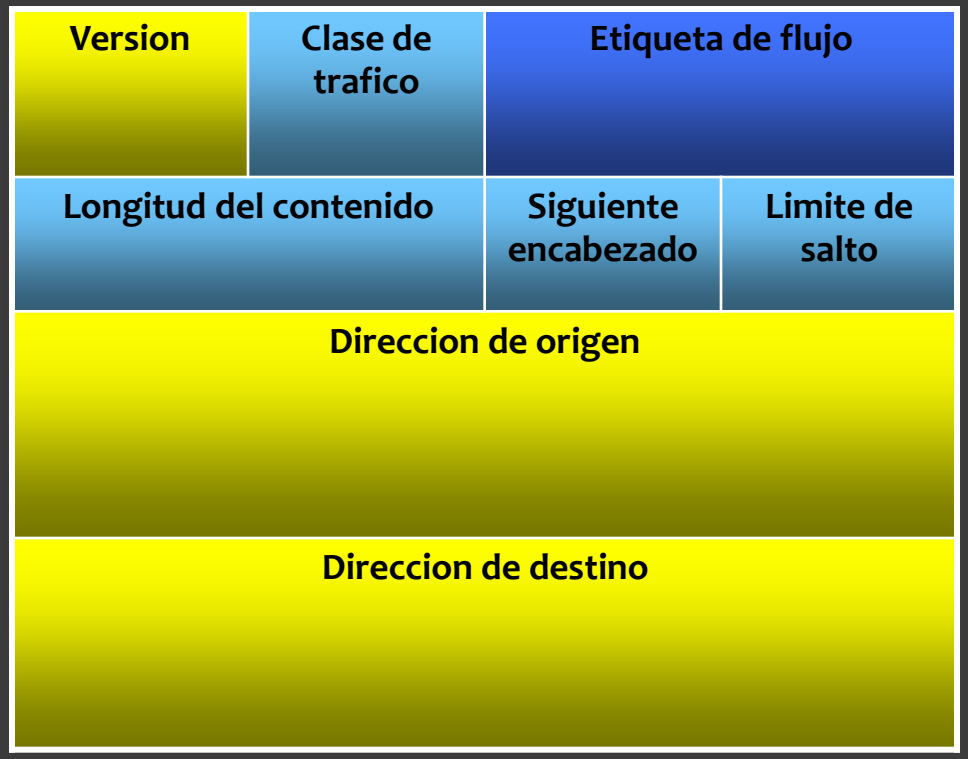
El encabezado que se utiliza para IPv6 aumenta la eficiencia de enrutamiento al reducir el número de entradas en las tablas de enrutamiento.

No se asocian broadcasts al IPv6. Con el IPv4, los broadcasts creados generan un alto nivel de tráfico dentro de la red. Este tráfico crea un evento que se conoce como una tormenta de broadcast y toda la red deja de funcionar. El IPv6 reemplaza los broadcasts con multicasts y anycasts.

Comparación IPv4 e IPv6

IPv4

IPv6



- -Nombre de los campos retenidos de IPv4 a IPv6
- - Campos no tetenidos en IPv6
- - Cambio de nombre y posicion en IPv6
- - Nuevo campo en IPv6

IPv6

Con IPv6, las direcciones IP tienen un tamaño de 128 bits con un potencial espacio de dirección de 2^128. En notación decimal esto es aproximadamente un 3 seguido de 38 ceros. Si el espacio de dirección IPv4 se representaba con el volumen de una cucharada de té, el espacio de dirección IPv6 sería representado con un volumen prácticamente equivalente al planeta Saturno.

Es difícil trabajar con números de 128 bits, por ello la notación de la dirección IPv6 representa los128 bits como 32 dígitos hexadecimales que a su vez están subdivididos en ocho grupos de cuatro dígitos hexadecimales usando dos puntos y delimitadores. La dirección IPv6 tiene una jerarquía de tres partes. El prefijo global está compuesto por los primeros tres bloques de la dirección y se lo asigna a una organización mediante un registro de nombres de Internet. La subred y el Identificador de interfaz (ID, Interface Identifier) son controlados por el administrador de red.

Los administradores de red dispondrán de determinado tiempo para adaptar esta nueva estructura IPv6. Antes de que se adopte de manera generalizada el IPv6, los administradores de red aún necesitan un modo para usar con mayor eficiencia los espacios de dirección privada.

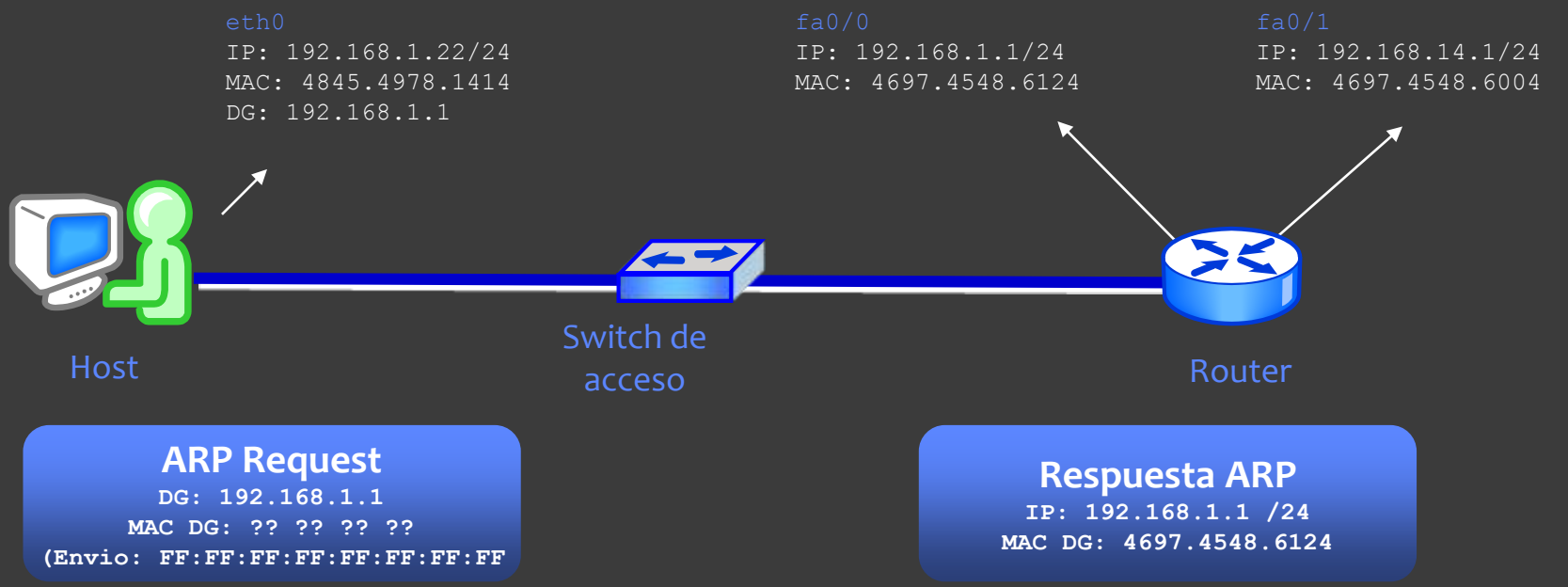
Protocolo ARP
Address Resolution Protocol

Protocolo ARP

Address Resolution Protocol es un protocolo empleado para encontrar la dirección física (MAC) de un equipo, conociendo su dirección lógica (IP). Veamos el siguiente ejemplo:

Si la tabla ARP, en donde se matchean las IP con las MAC de cada host, no posee la dirección física del default gateway, el direccionamiento a nivel 2 nunca podrá ser resuelto, y enviar la trama por broadcast siempre, atentaría contra el rendimiento de la red.

Entonces supongamos que el Host desea hacer un ping a la ip 192.168.14.2, que es un servidor en otra red. El primer paquete ICMP conocerá la IP donde enviar el paquete, el default gateway, porque es configurado en el sistema operativo (o bien puede haber sido enviada por DHCP), pero no conocerá la MAC del router.



Protocolo ICMP

Protocolo ICMP

Internet Control Message Protocol, es un protocolo de nivel 3 que se utiliza diversas tareas. Es un protocolo que se emplea para trabajar en conjunto con IP, debido a que provee a este último de funciones de notificación y administración que son muy útiles para los operadores de la red.

Los paquetes ICMP son encapsulados en IP y además proveen información de diagnóstico sobre problemas en la red.

Hay 5 tipos de paquetes ICMP

- Destination Unreachable: cuando un paquete es enviado a otro host, que no lo puede recibir por algún motivo, el último router antes de droppear el paquete, se encarga de generar un "DU" en sentido contrario con destino la IP origen, para advertir que el host destino no está operativo a nivel IP.

- Buffer Full: si el router comienza a ser saturado en alguna interfase por la llegada masiva de paquetes IP, el mismo genera este aviso hasta que la congestión finalice.

- Hops: cuando el paquete IP supera una cantidad determina de hops, saltos en routers, el último router que posea el TTL en 1, envía un ICMP indicando que la red es inaccesible. Es para prevenir loops de ruteo.

- Ping: es un paquete empleado para verificar la integridad física y lógica hacia un destino en particular. En el paquete ping se envía el alfabeto en el campo de datos.

- Traceroute: Es utilizado para descubrir el camino que se emplea para llegar a un destino en particular. El trace va enviando un paquete ICMP de retorno cuando pasa el paquete por un hop.

Comando TRACERT

La utilidad de diagnóstico TRACERT determina la ruta tomada hasta un destino enviando al destino paquetes de eco del Protocolo de mensajes de control de Internet (ICMP) con distintos valores de tiempo de vida (TTL) IP. Cada enrutador existente a lo largo de la ruta debe disminuir el TTL de un paquete por lo menos en 1 antes de reenviarlo, por lo que el TTL es un número de saltos eficaz. Cuando el TTL de un paquete alcanza el valor 0, el enrutador debe devolver al equipo de origen un mensaje ICMP de Tiempo agotado.

TRACERT determina la ruta enviando el primer paquete de eco con un TTL de 1 y aumentando el TTL en 1 en cada transmisión posterior, hasta que el destino responde o hasta que se alcanza el TTL máximo. La ruta se determina examinando los mensajes de ICMP Tiempo agotado devueltos por los enrutadores intermedios. Tenga en cuenta que algunos enrutadores eliminan de forma silenciosa los paquetes cuyos TTL han caducado y estos son invisibles para TRACERT.

El comando TRACERT puede utilizarse para determinar en qué lugar de la red se detuvo un paquete. En el siguiente ejemplo, la puerta de enlace predeterminada ha determinado que no existe una ruta válida para el host en 22.110.0.1. Probablemente haya un problema de configuración del enrutador o no existe la red 22.110.0.0 (una dirección IP incorrecta).

```
C:\>tracert 22.110.0.1
```

Comando PING

PING el acrónimo de **Packet Internet Groper**, el que puede significar "Buscador o rastreador de paquetes en redes".

Como programa, **ping** es una utilidad diagnóstica en redes de computadoras que comprueba el estado de la conexión del host local con uno o varios equipos remotos de una red TCP/IP por medio del envío de paquetes ICMP de solicitud y de respuesta.Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada.

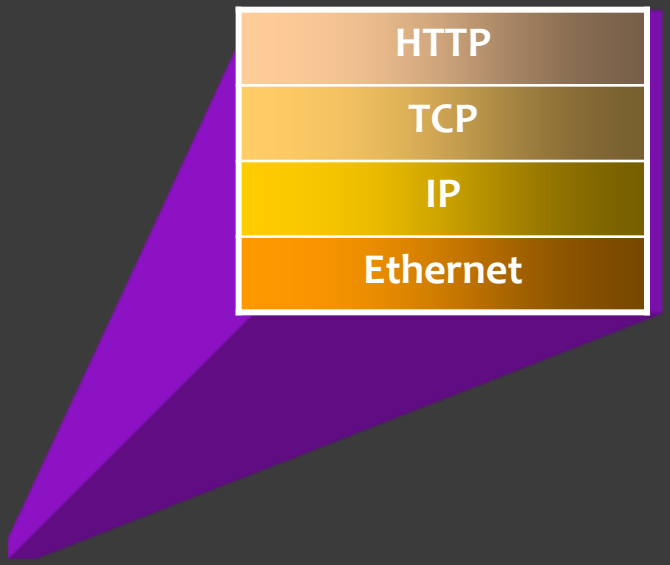
Ejecutando Ping de solicitud, el Host local envía un mensaje ICMP, incrustado en un paquete IP. El mensaje ICMP de solicitud incluye, además del tipo de mensaje y el código del mismo, un número identificador y una secuencia de números, de 32 bits, que deberán coincidir con el mensaje ICMP de respuesta; además de un espacio opcional para datos.

Stack de protocolos

Para la comunicación correcta entre hosts, es necesaria la interacción entre una serie de protocolos. Estos protocolos se implementan en software y hardware que se cargan en cada host y dispositivo de red.

La interacción entre los protocolos se puede describir como una stack de protocolos. Esta stack muestra los protocolos como una jerarquía en capas, donde cada protocolo de nivel superior depende de los servicios de los protocolos que se muestran en los niveles inferiores.

El gráfico muestra una stack de protocolos con los protocolos principales necesarios para ejecutar un servidor Web mediante Ethernet. Las capas inferiores de la stack tienen que ver con la transferencia de datos por la red y con la provisión de servicios a las capas superiores. Las capas superiores se concentran en el contenido del mensaje que se envía y en la interfaz de usuario.



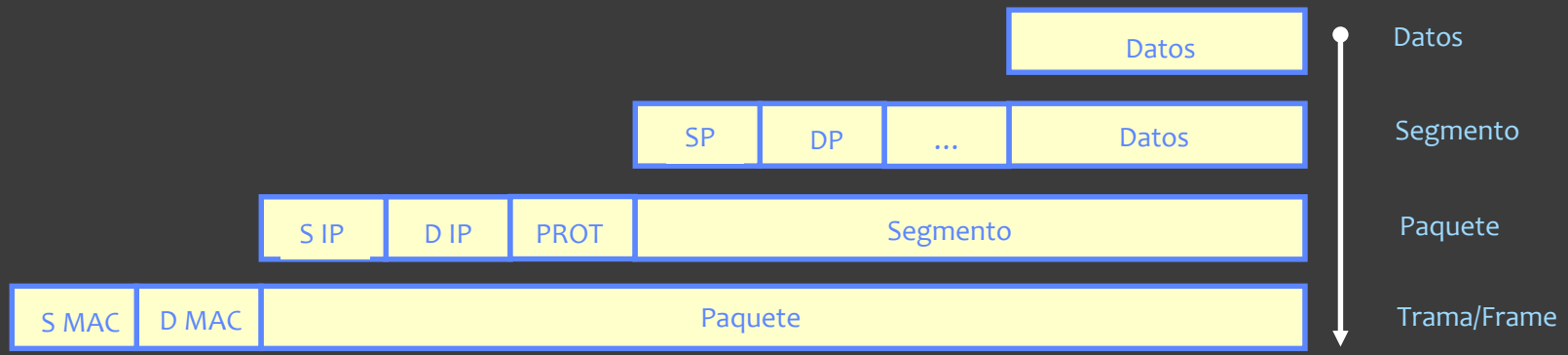
Encapsulación de datos

Una vez que la unidad de datos es procesada en las capas superiores, los mismos llegan a la Capa de Transporte.

En este nivel, los datos se encapsulan en un Segmento, el cual agrega un "header" que contiene en otros campos, un número de secuencia, que permite a la unidad de Transporte mantener un orden en los segmentos al momento de reensamblar la información.

En la capa 4 del OSI, el campo clave para el direccionamiento es el campo "port". Este posee el "port origen" y "port destino", como lo vemos en la figura.

Una vez que esta información se encuentra encapsulada, se envía a la capa de red. La misma toma los datos enviados por Transporte, y le agrega el header de nivel 3. Este encabeza contiene principalmente la dirección IP origen y destino, que emplea para rutear los paquetes en la red.



Interacción de protocolos

El modelo en capas presenta muchos beneficios:

- Ayuda en el diseño de protocolos, ya que los protocolos que operan en una capa específica tienen información definida según la cual actúan, y una interfaz definida para las capas superiores e inferiores.
- Fomenta la competencia, ya que los productos de distintos proveedores pueden trabajar en conjunto.
- Evita que los cambios en la tecnología o en las capacidades de una capa afecten otras capas superiores e inferiores.
- Proporciona un lenguaje común para describir las funciones y las capacidades de red.

Ethernet

Los estándares del protocolo Ethernet definen muchos aspectos de la comunicación de las redes, incluidos el formato de la trama, el tamaño de la trama, la sincronización y la codificación.

Cuando se envían mensajes entre hosts a través de una red Ethernet, los hosts asignan un formato a los mensajes según la configuración de trama que especifican los estándares.

El formato para las tramas de Ethernet incluye:

- Preámbulo para el secuenciamiento y la sincronización
- Delimitador de inicio de trama
- Longitud y tipo de trama
- Secuencia de verificación de trama para detectar errores de transmisión

Bytes	Nombre del campo
7	Preámbulo
1	Delimitador de inicio de trama.
6	Dirección MAC de destino
6	Dirección MAC origen
2	Campo Longitud/tipo
de 46 a 1500	Datos encapsulados
4	Secuencia de verificación de trama (suma de comprobación CRC)

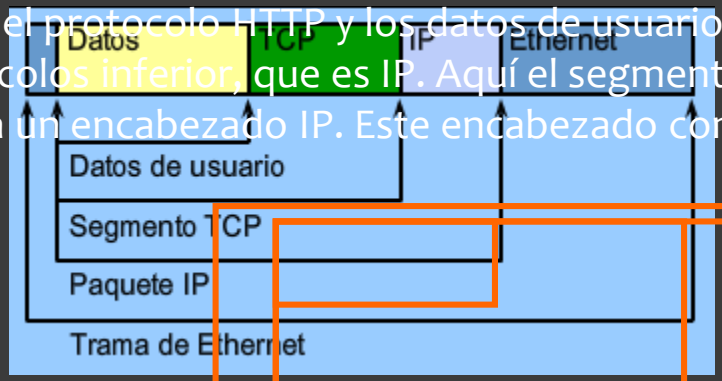
El tamaño de las tramas de Ethernet está restringido a un máximo de 1518 bytes y un mínimo de 64 bytes. Las tramas que no cumplen con estas limitaciones no son procesadas por los hosts receptores. Además de los formatos, los tamaños y la sincronización de las tramas, los estándares Ethernet definen cómo se codifican en el canal los bits que conforman las tramas.

Operación del protocolo para enviar

Cuando se envían mensajes en una red, la stack de protocolos de un host opera desde las capas superiores hacia las capas inferiores. En el ejemplo del servidor Web, el explorador del cliente solicita una página Web a un servidor Web del puerto de destino 80. Con esto se inicia el proceso de enviar una página Web al cliente.

A medida que la página Web va bajando a la stack de protocolos del servidor Web, los datos de la aplicación se dividen en segmentos TCP. A cada segmento TCP se le asigna un encabezado que contiene un puerto de origen y de destino.

El segmento TCP encapsula el protocolo HTTP y los datos de usuario HTML de la página Web, y los envía a la siguiente capa de protocolos inferior, que es IP. Aquí el segmento TCP se encapsula dentro del paquete IP, el cual le agrega un encabezado IP. Este encabezado contiene direcciones IP de origen y de destino.

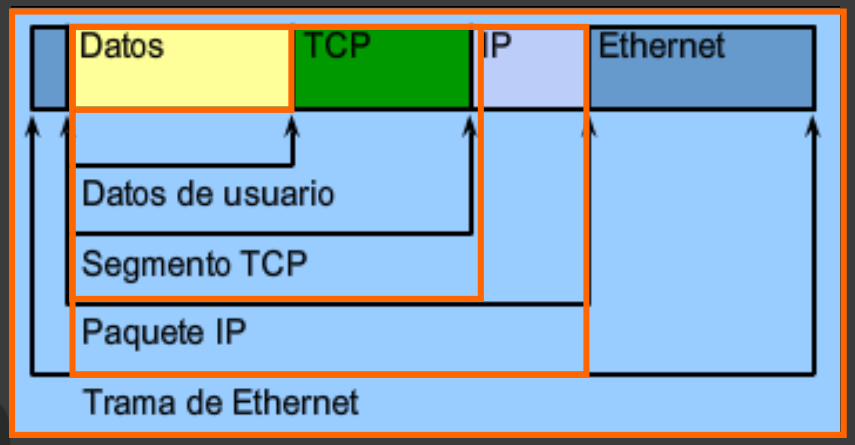


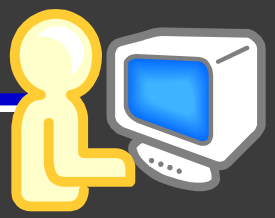
Operación del protocolo para enviar

Cuando se reciben mensajes provenientes de la red, la stack de protocolos de un host opera desde las capas inferiores hacia las capas superiores.

A medida que la NIC del cliente recibe bits, éstos se decodifican y el cliente reconoce la dirección MAC de destino como propia. La trama se sube a la stack de protocolos del cliente Web, donde el encabezado Ethernet (direcciones MAC de origen y de destino) y el tráiler se eliminan (desencapsulan). El resto del paquete IP y del contenido asciende a la capa IP. Ahí, el encabezado IP (direcciones IP de origen y de destino) se elimina y el contenido asciende a la capa TCP.

En esta capa, el encabezado TCP (puertos de origen y de destino) se elimina y el contenido de los datos de usuario de la página Web asciende a la aplicación del explorador mediante HTTP. A medida que se reciben los segmentos TCP, éstos se van rearmando para generar la página Web.





Actividad

192.168.0.1

11010101110011010010

DNS

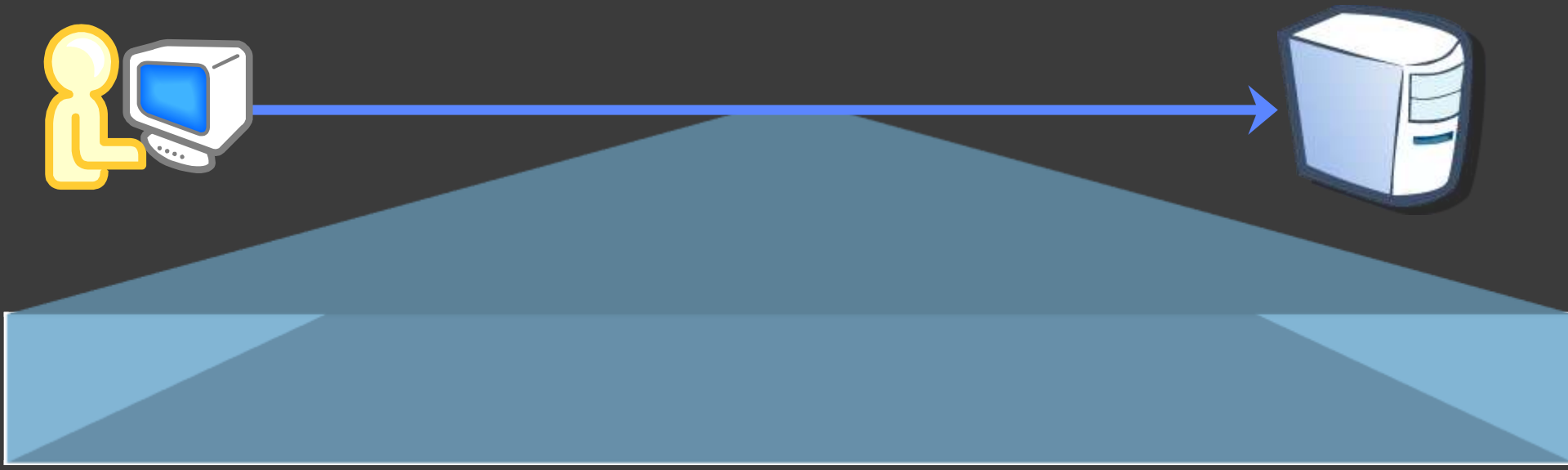
00-E0-87-BE-88-9A

143

Actividad

Dirección IP: 172.24.90.138
Dirección MAC: 00-E0-D8-E1-B5-1E
Numero de puerto: 33262

Dirección IP: 172.27.66.22
Dirección MAC: 00-E0-25-FE-B0D5
Numero de puerto: 21



33262 00-E0-D8-E1-B5-1E 21 172.24.90.138 00-E0-25-FE-B0D5 172.27.66.22