Sistemas de Computación 2

« Redes »

Protocolos

Protocolos

Cuando se conectan en red varios equipos, las reglas y los procedimientos técnicos que gobiernan su comunicación e interacción se llaman protocolos.

Hay tres puntos que deben tenerse en cuenta cuando se piensa en protocolos en un entorno de red:

1) Existen muchos protocolos. Si bien cada protocolo permite comunicaciones básicas, tienen distintos propósitos y realizan tareas distintas. Cada protocolo tiene sus propias ventajas y restricciones.
2) Algunos protocolos funcionan en varios niveles del modelo de referencia. El nivel en el que funciona un protocolo describe su función. Por ejemplo, un determinado protocolo funciona en el nivel Físico, lo que significa que el protocolo de ese nivel asegura que el paquete de datos pasa a través de la tarjeta adaptadora de red y fuera hacia el cable de la red.
3) Varios protocolos pueden funcionar juntos en lo que se conoce como una pila o conjunto de protocolos.

Tomados todos juntos, los protocolos describen todas las funciones y capacidades de la pila.

Pilas de Protocolos

TCP/IP	ISO	AppleTalk	Novell Netware
HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
IPv4 IPv6 ICMPv4 ICMPv6	CONP / CMNS CLNP / CLNS	AARP	IPX
Ethernet WLAN Frame Relay ATM PPP FDDI X.25			

Proceso de enlace

El proceso de enlace permite una gran flexibilidad a la hora de configurar una red. Los protocolos y las tarjetas adaptadoras de red se pueden mezclar y asignar según se necesite. Por ejemplo, dos pilas de protocolos, como IPX/SPX y TCP/IP, pueden estar enlazadas a una tarjeta adaptadora de red.

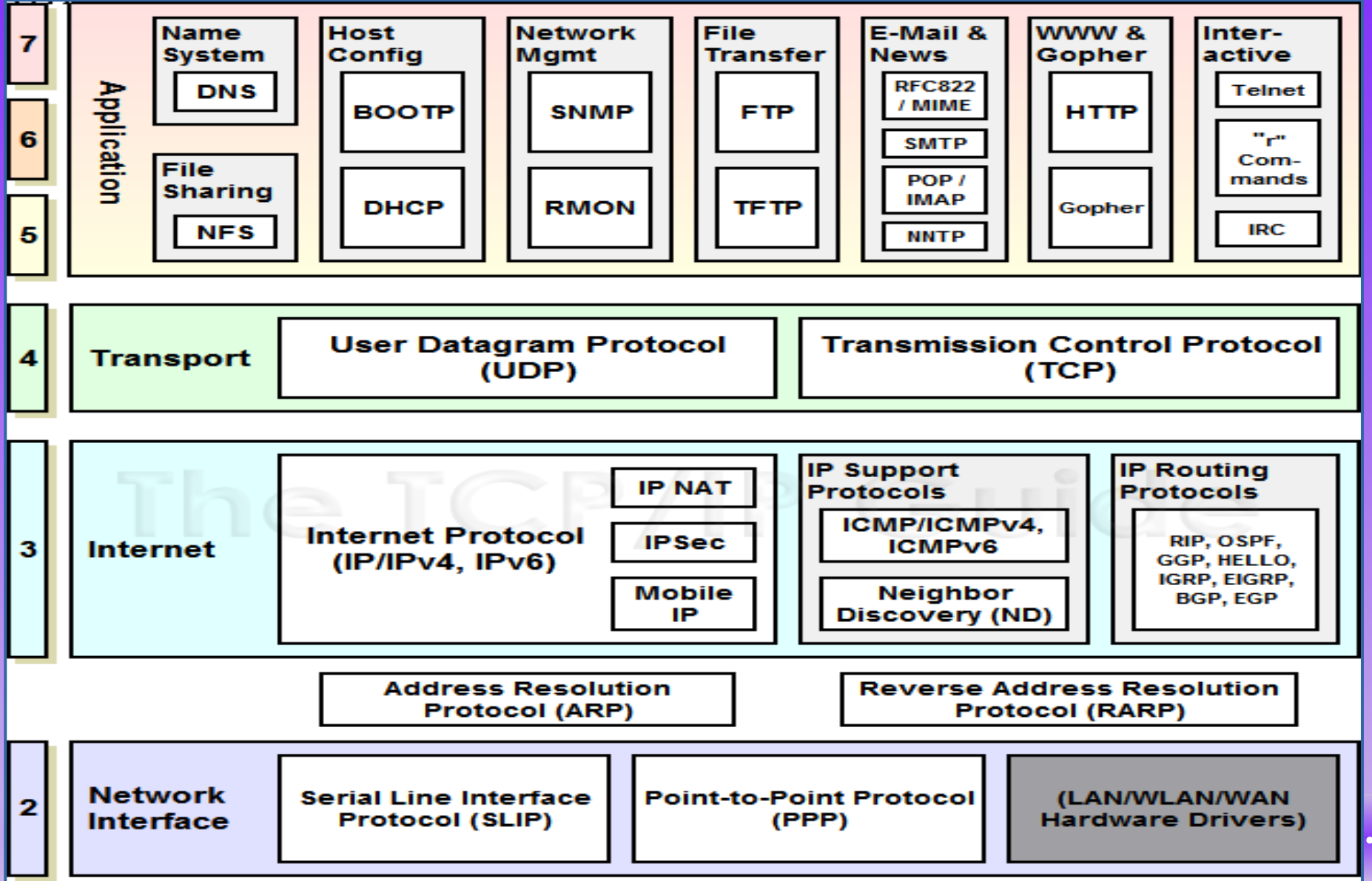
Si existe más de una tarjeta adaptadora de red en el equipo, una pila de protocolos puede enlazarse a una o a las dos tarjetas adaptadoras de red.

El orden de enlace determina el orden en que el sistema operativo ejecuta el protocolo. Si hay múltiples protocolos enlazados a una única tarjeta adaptadora, indica el orden en que se usarán los protocolos para intentar una conexión. Normalmente, el proceso de enlace ocurre cuando se instala o se inicializa el sistema operativo o el protocolo.

El enlace no está limitado a la pila de protocolos que se enlaza a la tarjeta adaptadora de red. Las pilas de protocolos necesitan estar enlazadas o asociadas con los componentes situados por encima y por debajo, de forma que los datos puedan proceder de forma natural a través de la pila durante la ejecución. Por ejemplo, TCP/IP se puede enlazar al nivel de Sesión Samba por encima y al controlador de la tarjeta adaptadora de red por debajo. El controlador de la tarjeta adaptadora de red

Protocolos TCP/IP

Capa TCP/IP	Protocolos TCP/IP					
Aplicación	HTTP	FTP	TELNET	SMTP	DNS	...
	HTTPS	TFTP	SSH	POP3	DHCP	
Transporte	TCP			UDP		
Red	IPv4	ARP	ICMP	IGRP	RIP	...
	IPv6	RARP	ND	EGP	OSPF	
Acceso al medio	Ethernet	WiFi 802.11	Token Ring	xDSL	FDDI	...


7
6
5
Application
Name System
DNS
File Sharing
NFS
Host Config
BOOTP
DHCP
Network Mgmt
SNMP
RMON
File Transfer
FTP
TFTP
E-Mail & News
RFC822 / MIME
SMTP
POP / IMAP
NNTP
WWW & Gopher
HTTP
Gopher
Inter-active
Telnet
"r" Com-mands
IRC
4
Transport
User Datagram Protocol (UDP)
Transmission Control Protocol (TCP)
3
Internet
Internet Protocol (IP/IPv4, IPv6)
IP NAT
IPSec
Mobile IP
IP Support Protocols
ICMP/ICMPv4, ICMPv6
Neighbor Discovery (ND)
IP Routing Protocols
RIP, OSPF, GGP, HELLO, IGRP, EIGRP, BGP, EGP
Address Resolution Protocol (ARP)
Reverse Address Resolution Protocol (RARP)
2
Network Interface
Serial Line Interface Protocol (SLIP)
Point-to-Point Protocol (PPP)
(LAN/WLAN/WAN Hardware Drivers)

Ethernet

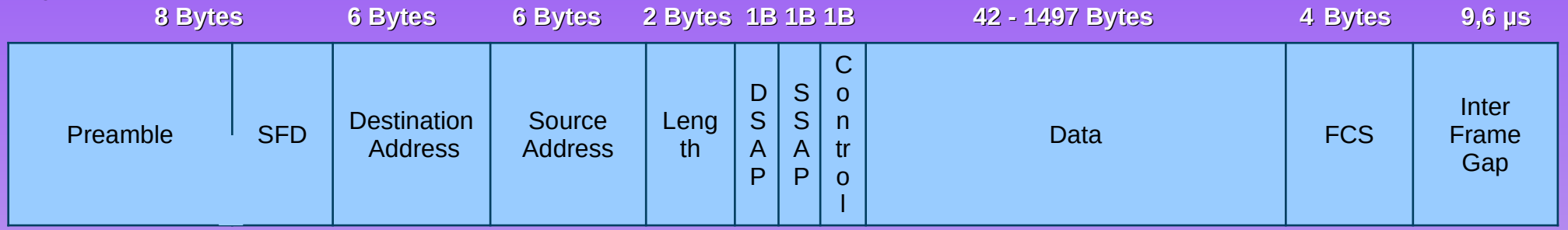
Ya vimos en el apunte anterior muchas características sobre Ethernet. Formato trama Ethernet II

Una trama Ethernet debe tener al menos 64 bytes para que funcione la detección de colisiones y puede tener un máximo de 1518 bytes.

El paquete comienza con un preámbulo, que controla la sincronización entre el emisor y el receptor, y un SFD (Start Frame Delimiter), que define la trama. Ambos valores son secuencias de bits en el formato "10101010 ….".La trama en sí contiene información sobre las direcciones de origen y destino (formato MAC), información de control (en el caso de Ethernet II el campo de tipo, una especificación de longitud), seguida por el registro de datos que se envía (Data). Una secuencia de comprobación de trama (FCS) es un código de detección de errores que cierra la trama (si no se cuenta al preámbulo y al SFD). El paquete se completa con una Inter Frame Gap, que define una pausa de transmisión de 9.6 µs.

Ethernet

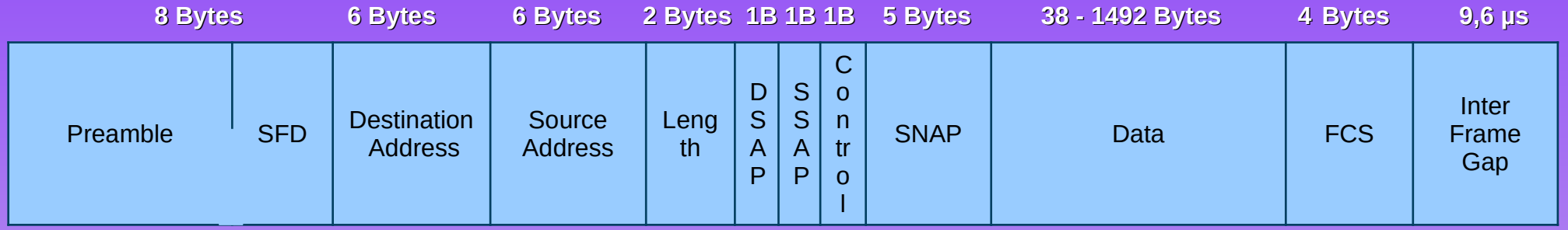
Esta versión estandarizada de la trama Ethernet 802.3 puede definir hasta 256 protocolos compatibles, con información de protocolo importante integrada en el campo de datos. Además, se incluyen el "Punto de acceso al servicio de destino" (DSAP) y el "Punto de acceso al servicio de origen" (SSAP). El nuevo campo de control define el "Logical Link" (LLC) del protocolo. Este punto garantiza la transparencia de los procedimientos de compartición de medios y puede controlar el flujo de datos.



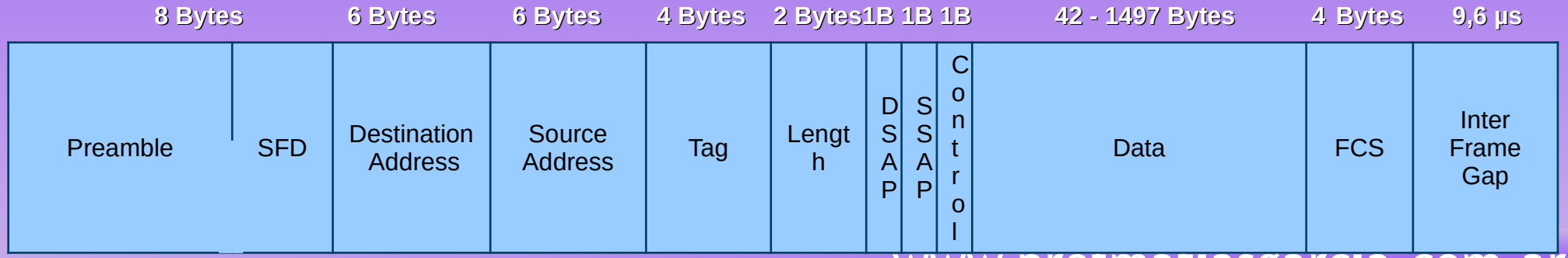
Ethernet IEEE 802.3 es la estructura de trama LAN más popular y ampliamente utilizada en la actualidad. Sin embargo, algunas redes y protocolos requieren más espacio para información específica. Por este motivo, existen variantes de la trama Ethernet IEEE 802.3 que proporcionan bloques de datos adicionales para información específica, entre ellos la extensión SNAP y la etiqueta VLAN.

Ethernet

El campo SNAP ("Sub Network Access Protocol") es útil para definir más de 256 protocolos. Para ello, se ponen a disposición 2 bytes para el número de protocolo. Además, el fabricante puede integrar un identificador único (3 bytes).



Los marcos etiquetados contienen una etiqueta “Tag” para poder ser asignados a una red de área local virtual (VLAN) que separa la estructura de la red en niveles físicos y lógicos.



WiFi

Comúnmente, el estándar IEEE 802.11 se denomina “WiFi”. No hay una conectividad física definible; por lo tanto, factores externos pueden interferir con la transferencia de datos y es difícil controlar el acceso. Para vencer estos desafíos, los estándares inalámbricos tienen controles adicionales.

Es un sistema de contienda que utiliza un proceso CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) de acceso al medio por lo que trata de evadir las colisiones. CSMA/CA especifica un procedimiento de postergación aleatoria para todos los nodos que están esperando transmitir. La oportunidad más probable para la contención de medio es el momento en que el medio está disponible. Hacer el back off de los nodos para un período aleatorio reduce en gran medida la probabilidad de colisión.

Un cliente inalámbrico transmite solo si el canal está libre. Todas las transmisiones se confirman; por ello, si un cliente inalámbrico no recibe un acuse de recibo, supone que ocurrió una colisión y lo vuelve a intentar después de un intervalo de espera aleatorio.

Los clientes inalámbricos y los AP usan las tramas de control RTS (Request To Send) y CTS (Clear To Send) para facilitar la transferencia de datos propiamente dicha.

WiFi

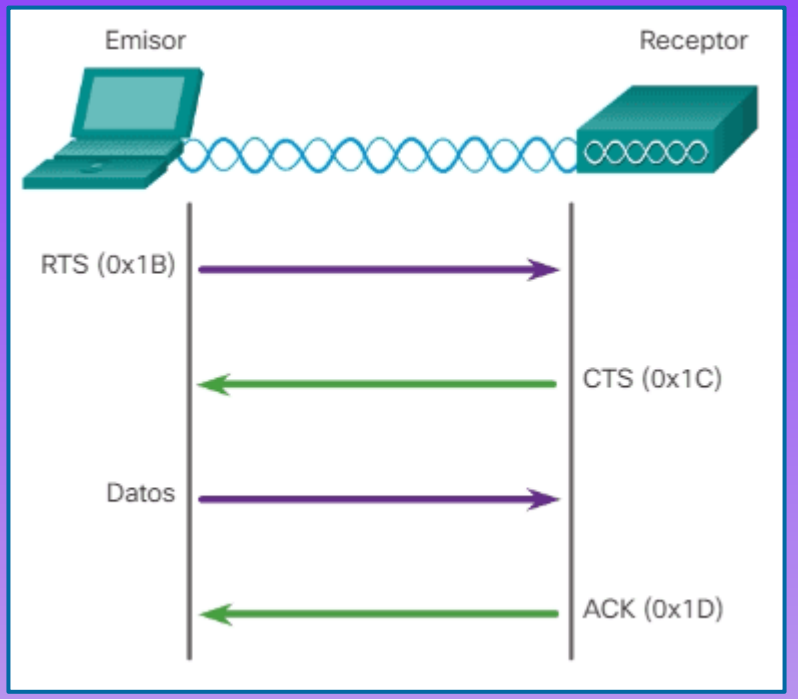
Cuando un cliente inalámbrico envía datos, primero evalúa los medios para determinar si otros dispositivos los están usando para transmitir.

De lo contrario, envía una trama RTS al AP.

Esta trama se usa para solicitar acceso dedicado al medio de RF durante un período específico.

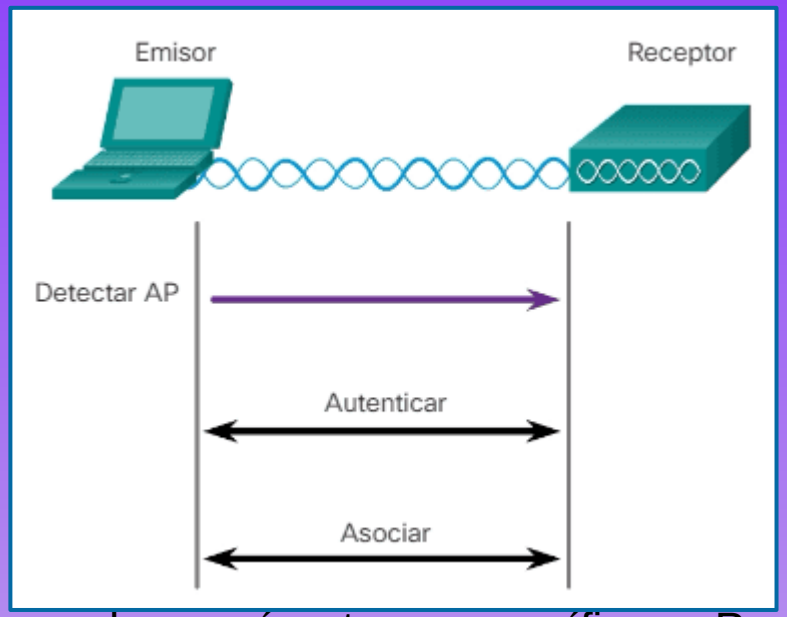
El AP recibe la trama y, si está disponible, otorga al cliente inalámbrico acceso al medio de RF mediante el envío de una trama CTS de la misma duración.

Todos los demás dispositivos inalámbricos que observan la trama CTS ceden los medios al nodo transmisor para la transmisión.



La trama de control CTS incluye el período durante el que se le permite transmitir al nodo transmisor. Otros clientes inalámbricos retienen las transmisiones durante, por lo menos, el período especificado.

WiFi



Para que los dispositivos inalámbricos se comuniquen a través de una red, primero se deben asociar a un AP o un router inalámbrico.

Los dispositivos inalámbricos usan las tramas de administración para completar el siguiente proceso de tres etapas:

- Descubrir nuevos AP inalámbricos.
- Autenticar con el AP.
- Asociarse al AP.

Para asociarse, un cliente inalámbrico y un AP deben acordar parámetros específicos. Para permitir la negociación de estos procesos, se deben configurar los parámetros en el AP y posteriormente en el cliente.

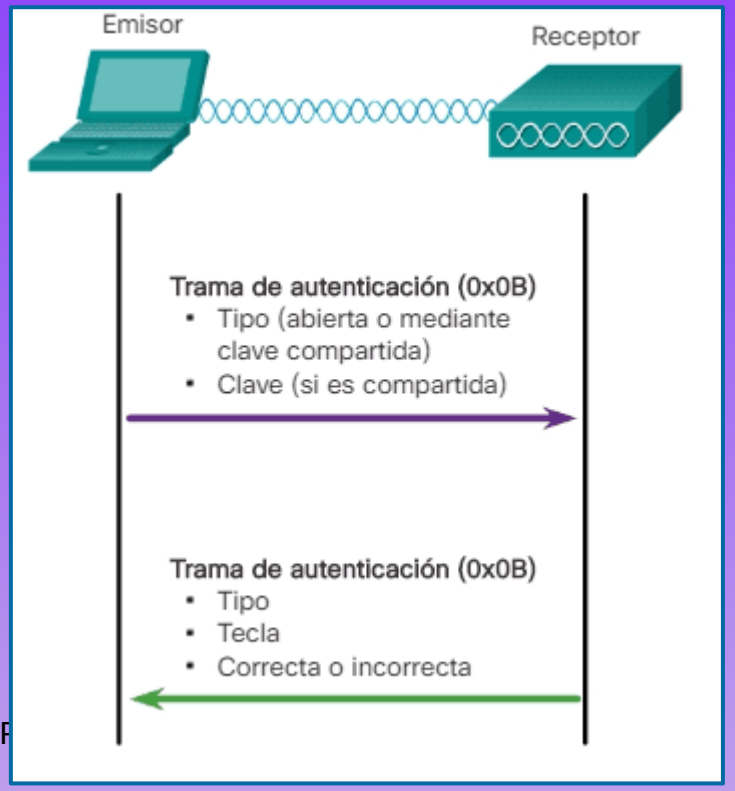
- SSID: identificador único para distinguir entre varias redes inalámbricas en la misma área.
- Password: el cliente inalámbrico la necesita para autenticarse con el AP.
- Network mode (Modo de red): se refiere a los estándares de WLAN 802.11a/b/g/n/ac/ad. Los AP y los routers inalámbricos pueden funcionar en modo Mixed (Mixto), lo que implica que pueden usar varios estándares a la vez.
- Security mode (Modo de seguridad): se refiere a la configuración de los parámetros de seguridad, como WEP, WPA o WPA2.
- Channel settings (Configuración de canales): se refiere a las bandas de frecuencia que se usan para transmitir datos inalámbricos.

WiFi

El estándar 802.11 se desarrolló originariamente con dos mecanismos de autenticación:

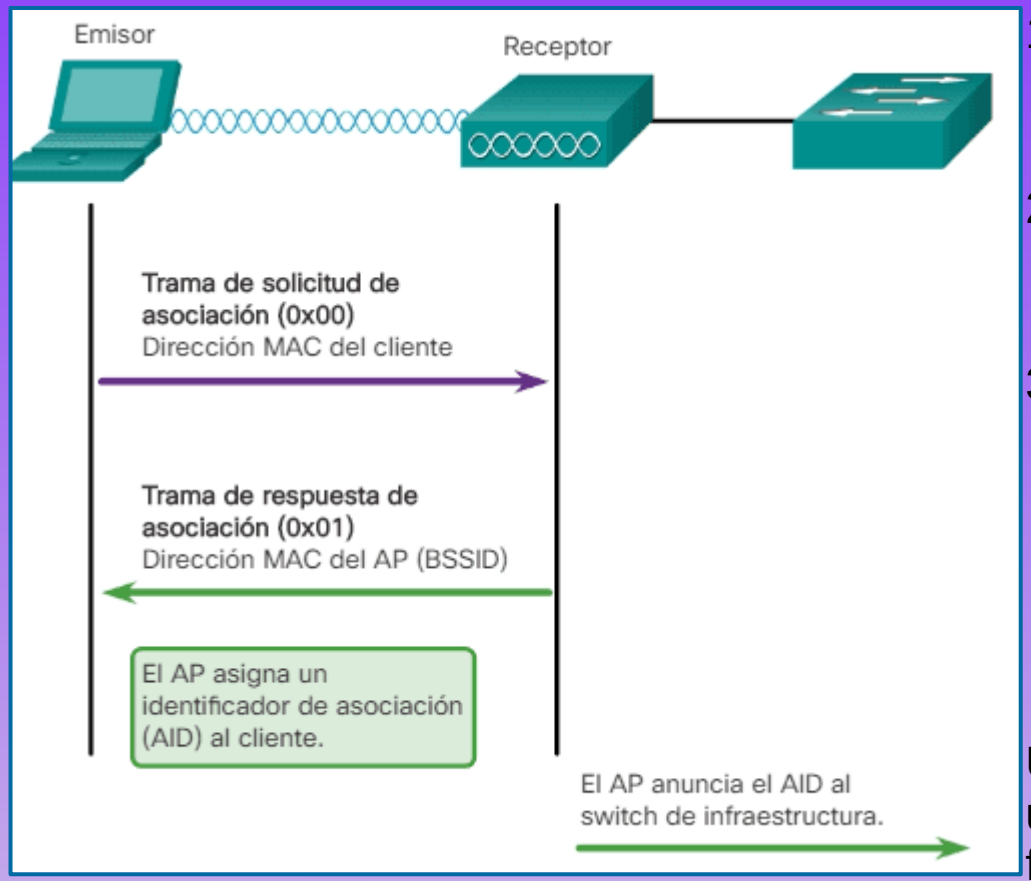
Autenticación abierta: fundamentalmente, una autenticación NULA donde el cliente inalámbrico dice “autentíqueme” y el AP responde “sí”. La autenticación abierta proporciona conectividad inalámbrica a cualquier dispositivo inalámbrico y se debe usar solo en situaciones donde la seguridad no es un motivo de preocupación.

Autenticación de clave compartida: es una técnica que se basa en una clave previamente compartida entre el cliente y el AP.



1) El cliente inalámbrico envía una trama de autenticación al AP.
2) El AP responde con un texto de desafío al cliente.
3) El cliente cifra el mensaje mediante la clave compartida y devuelve el texto cifrado al AP
4) A continuación, el AP descifra el texto cifrado mediante la clave compartida.
5) Si el texto descifrado coincide con el texto de desafío, el AP autentica el cliente. Si los mensajes no coinciden con el texto de desafío, no se autentica el cliente inalámbrico y se deniega el acceso inalámbrico.

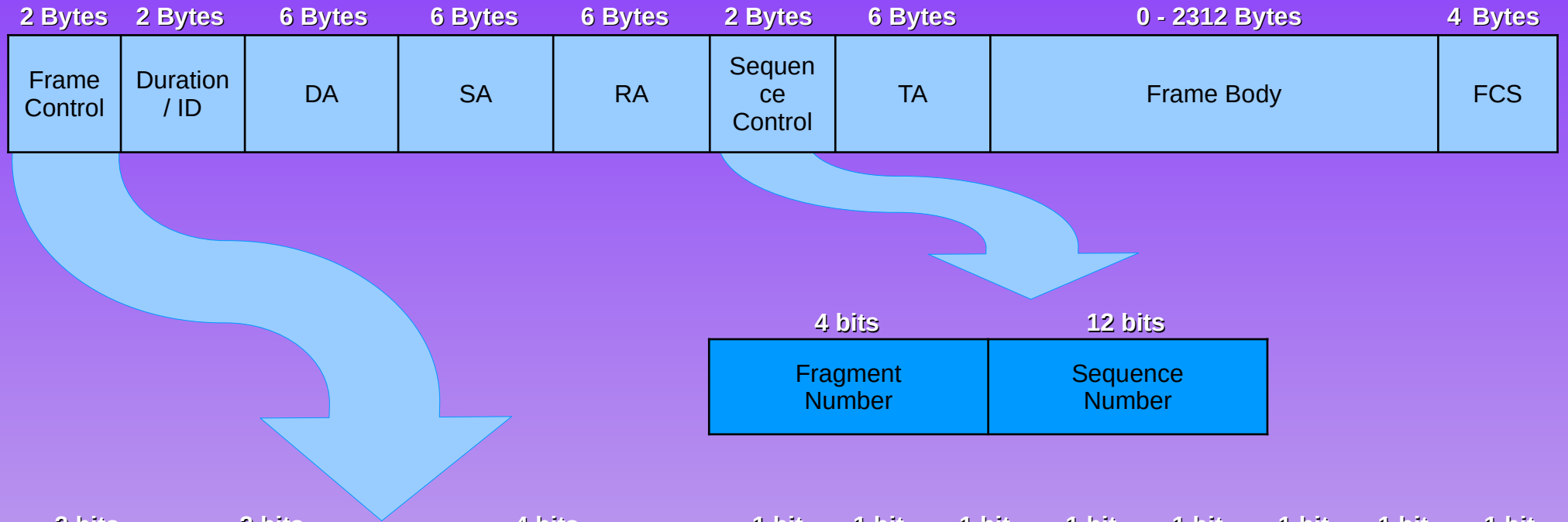
WiFi



1) El cliente inalámbrico reenvía una trama de solicitud de asociación que incluye su dirección MAC.
2) El AP responde con una respuesta de asociación que incluye el BSSID del AP, que es la dirección MAC del AP.
3) El AP asigna un puerto lógico conocido como “identificador de asociación” (AID) al cliente inalámbrico. El AID equivale a un puerto en un switch y permite que el switch de infraestructura mantenga un registro de las tramas destinadas a que el cliente inalámbrico las reenvíe.

Una vez que un cliente inalámbrico se asocia a un AP, el tráfico entre el cliente y el AP puede fluir

WiFi



WiFi

- Versión de protocolo: la versión de la trama 802.11 en uso.
- Tipo y Subtipo: identifican una de las tres funciones y subfunciones de la trama
  - Trama de administración: se utiliza para el mantenimiento de la comunicación, como la detección de un AP, la autenticación de este y la asociación a dicho AP.
  - Trama de control: se utiliza para facilitar el intercambio de tramas de datos entre clientes inalámbricos.
  - Trama de datos: indica que transportar la información de contenido
- A DS: se establece en 1 para las tramas de datos destinadas al sistema de distribución.
- Desde DS: se establece en 1 para las tramas de datos que salen del sistema de distribución.
- Más fragmentos: se establece en 1 para las tramas que tienen otros fragmentos por recibir.
- Reintentar: se establece en 1 si la trama es una retransmisión de una trama anterior.
- Administración de energía: para indicar que un nodo estará en el modo de ahorro de energía.
- Más datos: se establece en 1 para indicarle a un nodo en el modo de ahorro de energía que se almacenan más tramas en búfer para enviar a ese nodo.
- Seguridad: indica si se usan el cifrado y la autenticación en la trama.
- Orden: se establece en 1 en una trama de tipo de datos que utiliza la clase de servicio estrictamente ordenada (no requiere reordenamiento).

WiFi

- Duración/ID: según el tipo de trama, representa el tiempo que se requiere en microsegundos para transmitir la trama o una identidad de asociación (AID) para la estación que transmitió la trama, para recibir la siguiente transmisión.
- Dirección de destino (DA): contiene la dirección MAC del nodo de destino final en la red.
- Dirección de origen (SA): contiene la dirección MAC del nodo que inició la trama.
- Dirección del receptor (RA): contiene la dirección MAC que identifica al dispositivo inalámbrico que es el destinatario inmediato de la trama, como la interfaz del router (gateway predeterminado) a la que se conecta el AP.
- Control de secuencia:
  - Número de fragmento: indica el número de cada trama que se envió de una trama fragmentada.
  - Número de secuencia: indica el número de secuencia asignado a la trama. Las tramas retransmitidas se identifican con números de secuencia duplicados.
- Dirección del transmisor (TA): contiene la dirección MAC que identifica al dispositivo inalámbrico que transmitió la trama.
- Cuerpo de la trama: contiene la información que se transporta.
- FCS: contiene una comprobación de redundancia cíclica (CRC) de 32 bits de la trama.

ARP

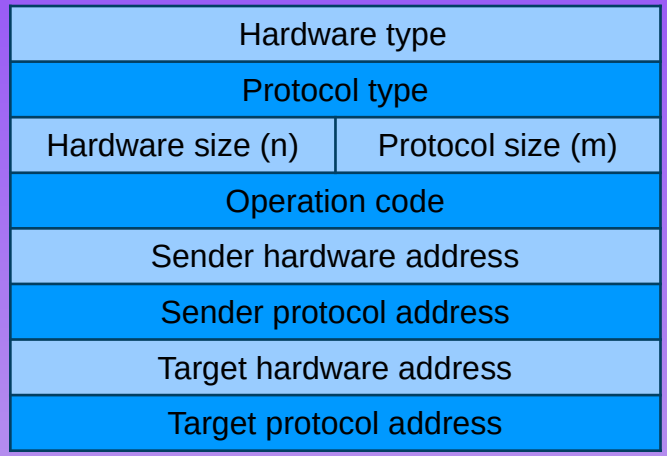
Address Resolution Protocol (ARP) – RFC 826

Cuando se transmite un datagrama IP en Ethernet se encapsula en un marco de Ethernet cuya cabecera debe incluir la dirección MAC del destinatario, la cuál puede no ser conocida por el remitente. La tarea más común de ARP es encontrar la dirección MAC asociada a una dirección IP. Para ello, envía un mensaje de petición a la dirección MAC de broadcast de la red (ff:ff:ff:ff:ff:ff) que es recibido por todos los equipos conectados a ella. Si un equipo comprueba que la dirección IP por la que se pregunta coincide con la suya, envía al peticionario su dirección MAC (el resto de los equipos ignora la petición). Cuando el equipo peticionario recibe la respuesta, almacena en una tabla, denominada caché ARP, la pareja dirección IP-dirección MAC. La misión de esta tabla es reducir el número de paquetes ARP que se envían. De esta forma, si un equipo necesita la dirección MAC asociada a una determinada dirección IP, antes de enviar un mensaje de broadcast primero comprueba si la tiene almacenada en la caché ARP.

La memoria caché ARP de un equipo no es estática, sino que se actualiza cada pocos minutos. De esta forma puede adaptarse a los posibles cambios de direcciones IP o MAC que ocurran en la red. Cuando un equipo realiza una petición ARP, incluye en el mensaje sus propias direcciones IP y MAC, de manera que al enviarlo a la dirección de broadcast el resto de los equipos de la red actualizarán su caché ARP con la pareja IP-MAC del peticionario.

ARP

La longitud de un paquete ARP está determinado por el tamaño de las direcciones del hardware y del tipo de protocolo. Con direcciones MAC de 48 bits y direcciones IP de 32 bits, el tamaño de un paquete de petición, o de respuesta, ARP es de 28 bytes. Los mensajes ARP no tienen cabecera IP y se encapsulan directamente en marcos de Ethernet.



- Hardware type (2 bytes) Especifica el tipo de hardware (0x0001 para una tarjeta Ethernet).
- Protocol type (2 bytes) Especifica el tipo de protocolo (0x8000 cuando ARP resuelve direcciones IP)
- Hardware size (1 bytes) Especifica la longitud, en bytes, de la dirección hardware (0x0006 para MAC)
- Protocol size (1 bytes) Especifica la longitud, en bytes, de la dirección del protocolo (0x0004 para IP).
- Operation code (2 bytes) Especifica si se trata de una petición (0x0001) o de una respuesta (0x0002) ARP.
- Sender/target hardware address (n bytes) Contiene las direcciones físicas del hardware.
- Source/target protocol address (m bytes) Contiene las direcciones del protocolo. En TCP/IP son 32 bits.

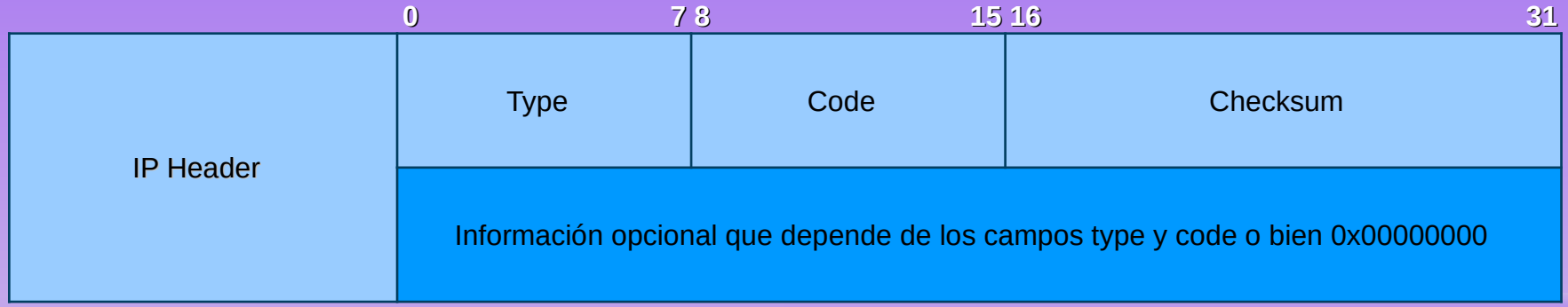
ICMP

Internet Control Message Protocol (ICMP) – RFC 792

Se utiliza como soporte al protocolo IP para enviar mensajes de error. Por ejemplo, si un router descarta un datagrama IP porque el campo TTL es nulo envía al equipo un remitente un mensaje ICMP avisando de esta circunstancia y explicando el motivo. ICMP también proporciona la posibilidad de diagnosticar el estado de la red, por ejemplo, enviando mensajes de petición de eco usando el comando PING.

Un mensaje ICMP se encapsula dentro de un datagrama IP, también se le añade la cabecera IP.

Su longitud mínima es 8 bytes, de los cuáles 4 bytes corresponden a los campos type, code y checksum y, si no hay información adicional, se completan los 4 bytes restantes con ceros.



ICMP

Los tipos de mensajes ICMP se identifican con los campos type y code.

Los mensajes ICMP pueden clasificarse en dos grandes categorías, mensajes de consulta y mensajes de error. En total hay 33 tipos de mensajes ICMP
Un mensaje de consulta consiste en un par de mensajes ICMP, uno de petición y uno de respuesta.

Type	Code	Mensaje ICMP	Tipo
0	0	Echo reply (petición de eco)	Consulta
3	0	Network unreachable (red inalcanzable)	Error
3	1	Host unreachable (equipo inalcanzable)	Error
3	2	Protocol unreachable (protocolo inalcanzable)	Error
3	3	Port unreachable (puerto inalcanzable)	Error
5	0	Network redirect (redireccionar red)	Error
5	1	Host redirect (redireccionar equipo)	Error
8	0	Echo request (respuesta de eco)	Consulta
11	0	TTL Time out (tiempo de espera excedido)	Error

Un mensaje de error informa de que ha ocurrido un error en el envío de un datagrama IP, por ejemplo, cuando un router lo descarta. El formato de un mensaje ICMP de error tiene una cabecera formada por los campos type, code y checksum seguidos de cuatro bytes a cero (0x00000000). La cabecera IP y los 8 bytes de carga útil que vienen a continuación también forman parte del mensaje ICMP y pertenecen al datagrama IP que originó el error.

ICMP

Por ejemplo, cada router que reenvía un datagrama IP tiene que disminuir el campo de tiempo de vida (TTL) de la cabecera IP en una unidad; si el TTL llega a cero, un mensaje ICMP tipo 11 ("Tiempo excedido") es enviado al originador del datagrama.

Por ejemplo, el mensaje port unreachable indica que capa de transporte no ha podido entregar los datos a la aplicación correspondiente. Esto puede ocurrir cuando se utiliza el protocolo UDP y un programa ejecutado desde un cliente intenta conectar con un servidor que no existe, por ejemplo, cuando se usa TFTP (Trivial File Transfer Protocol). Con TCP esto no ocurre porque la conexión se cierra inmediatamente.

Se lo define en la RFC 792. La versión de ICMP para IPv4 también es conocida como ICMPv4. IPv6 tiene su protocolo equivalente ICMPv6.

Muchas de las utilidades de red comunes están basadas en los mensajes ICMP. El comando traceroute puede implementarse transmitiendo datagramas con valores especiales de TTL en la cabecera, y analizando luego los mensajes de "Destino inalcanzable" y "Tiempo excedido" (tipos 3 y 11) generados como respuesta. La herramienta ping está implementada utilizando los mensajes "Echo request" y "Echo reply" de ICMP.

IP

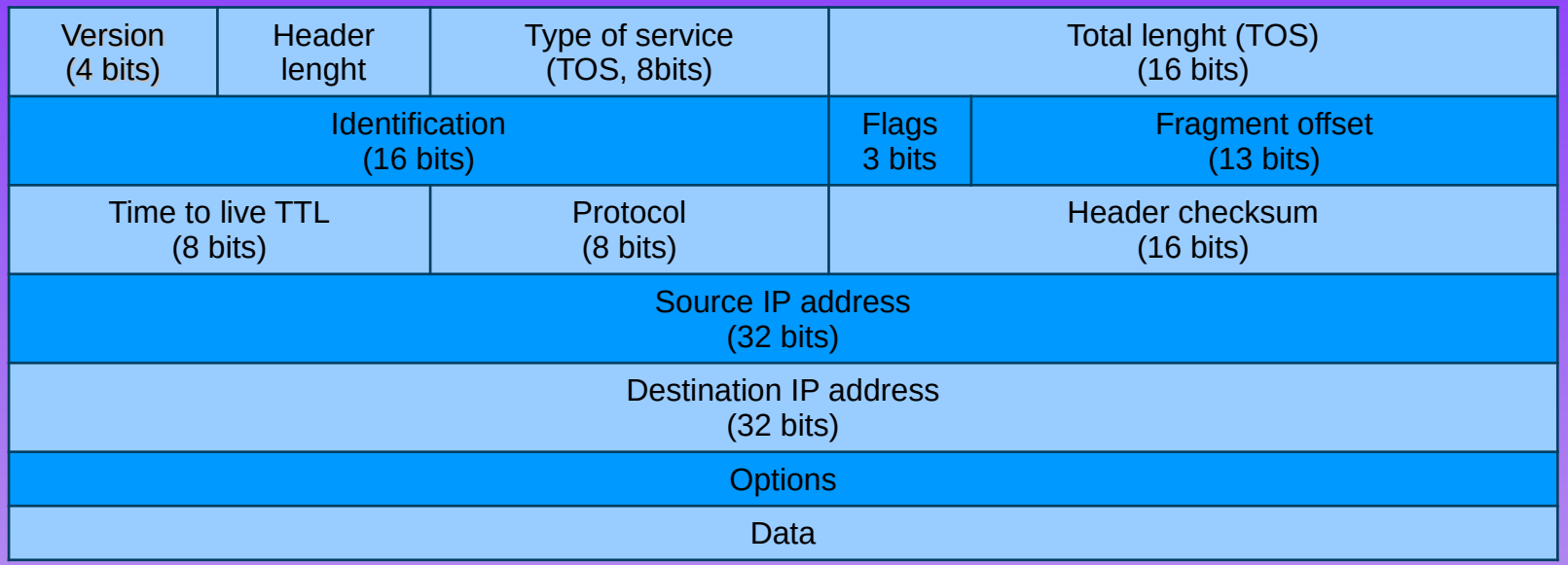
Internet Protocol (IP) - 791

El protocolo IP se encarga de transportar los datos (datagramas IP) desde el origen hasta el destino a través de la red. En el equipo remitente, IP recibe un segmento de la capa de transporte, TCP o UDP, y lo encapsula en un datagrama IP. A continuación, IP demanda el servicio del protocolo de la capa inferior (normalmente Ethernet) y encapsula el paquete en un marco que es enviado al equipo destinatario (si está en la misma red) o al router (si el equipo destinatario pertenece a una red distinta).

Cuando un router recibe un marco, demultiplexa el datagrama IP del mismo, comprueba la IP del destinatario y lo encapsula de nuevo en una traza con la dirección MAC del siguiente equipo al que tiene que ser enviado (el destinatario final u otro router). Y así sucesivamente. Cuando el marco llega finalmente a su destino, en la capa de acceso al medio se demultiplexa el marco para obtener el datagrama IP, y en la capa de red se demultiplexa el datagrama IP para obtener el segmento TCP o UDP, el cuál es enviado a la capa de transporte. Finalmente, los datos son enviados a la aplicación correspondiente.

En este proceso, el único protocolo que se encarga del transporte es IP.

IP



Cualquier envío de datos de los protocolos TCP, UDP, ICMP o IGMP es siempre transmitido como un datagrama IP. Este “monopolio” de IP tiene la ventaja de que cualquier equipo, router, etc. que utilice IP puede comunicarse con cualquier otro de la red. Pero el hecho de que no haya alternativa a IP tiene la desventaja de que cualquier aplicación, sean cuáles sean sus necesidades, sólo recibe el nivel de servicio que puede proporcionar IP, el cuál no es precisamente fiable. Por ejemplo, IP no garantiza que un paquete llegue a su destino o que los paquetes lleguen en la secuencia en la que fueron enviados.

IP

- Version: indica el número de la versión, por ejemplo, 4 para IPv4.
- header lenght: indica la longitud de la cabecera en múltiplos de cuatro bytes, lo cuál permite conocer dónde empiezan los datos (campo data). Como este campo ocupa 4 bits, puede tomar 15 como valor máximo y, por tanto, la cabecera tendrá una longitud máxima de 60 bytes (4x15bytes). La longitud mínima de la cabecera es 20 bytes, lo cuál ocurre cuando el campo options está vacío.
- TOS (Type-of-Service): indica las preferencias sobre el servicio que se desea que proporcione IP, pero sin ninguna garantía de que IP lo consiga. Hay que recordar que, IP no garantiza que los paquetes se pierdan o lleguen ordenados, ni tampoco la velocidad de transmisión o cuánto van a tardar en llegar a su destino.
- Total lenght: indica número total de bytes del datagrama IP, incluyendo la cabecera y los datos.
- Identification, flags y fragment offset: están asociados a la fragmentación de los datagramas IP. En principio, el tamaño máximo de un datagrama IP es de 65.535 bytes. Sin embargo, debido a las restricciones impuestas por el protocolo Ethernet, los datagramas IP no pueden superar los 1500 bytes (carga o “payload” máxima permitida). Este límite, denominado MTU (Maximum Transmission Unit), obliga a realizar un proceso de segmentación relativamente complejo que se especifica por medio de los tres campos mencionados.

IP

- TTL(Time-To-Live): indica la vida útil de un datagrama IP, lo cuál es útil si el datagrama queda atrapado en un bucle de la red. Cada vez que un router procesa el datagrama decrementa en 1 el valor de este campo y si llega a cero lo elimina. Es obvio que el campo TTL tiene que tener un valor inicial superior al número de routers que se pueden encontrar en la ruta más larga a través de la red, ya que en caso contrario puede que el paquete no llegue a su destino. El valor inicial de TTL suele ser mayor o igual que 64.
- Protocol: identifica el protocolo al que pertenecen los datos y que se necesita para la demultiplexación. 1 → ICMP 6 → TCP 17 → UDP
- Checksum: en el caso del datagrama IP, sólo se computan los bytes de la cabecera IP. Cuando IP detecta un error en este campo, descarta el datagrama.
- Dirección IP del remitente.
- Dirección IP del destinatario.
- Options: no es obligatorio y sirve, aunque se utiliza en raras ocasiones, para indicar algunas opciones especiales. Por ejemplo, para determinar el MTU de una ruta.
- Data: contiene la parte útil, o “payload”, encapsulada en el datagrama IP. Por ejemplo, un mensaje ICMP de la propia capa de red o un segmento TCP o UDP de la capa de transporte.

RIP

Routing Information Protocol (RIP)

Es un protocolo de puerta de enlace interna o interior (Interior Gateway Protocol, IGP) utilizado por los routers para intercambiar información acerca de redes (IP) a las que se encuentran conectados.

Su algoritmo de encaminamiento está basado en el vector de distancia, ya que calcula la métrica o ruta más corta posible hasta el destino a partir del número de "saltos" o equipos intermedios que los paquetes IP deben atravesar. El límite máximo de saltos en RIP es de 15, de forma que al llegar a 16 se considera una ruta como inalcanzable o no deseable.

A diferencia de otros protocolos, RIP es un protocolo libre, es decir, que puede ser usado por diferentes routers y no únicamente por un solo propietario como es el caso de EIGRP que es de Cisco Systems.

RIP es más fácil de configurar (comparativamente a otros protocolos). Implementa un algoritmo de encaminamiento más simple que otros protocolos, por lo que el cálculo de la "mejor" ruta (comparativamente en routers de similares prestaciones) es más rápida. Es soportado por la mayoría de los fabricantes. El protocolo EIGRP de Cisco, salva la principal desventaja porque valora la mejor métrica, además del número de saltos y otros criterios (ancho de banda, congestión, carga, retardo, fiabilidad, etc.), haciendo más eficiente la red.

RIP

RIP utiliza unos temporizadores para que apoyen su funcionamiento, las cuales son:

- Temporizador periódico: este controla la publicación de los mensajes de actualización regulares. Se debe ajustar el temporizador a 30 s, esto es para evitar se sincronicen y así sobrecargar el Internet si los routers se actualizan de forma simultánea. Cada router posee un temporizar periódico que se establece al azar a un número que va de 25 a 35 que va en decremento hasta llegar a 0 y envía un mensaje de actualización.
- Temporizador de caducidad (o timer de invalidación): establece cuanto tiempo puede estar una ruta en la tabla de ruteo sin ser actualizada. Cuando un router recibe la información actualizada para una ruta, el temporizador establece 180 s para esa ruta en particular. Si pasados los 180 s asignados no se actualiza la ruta, se considera que está caducada y el número de saltos se pone 16 considerándose una ruta inalcanzable.
- Temporizador de Colección de Basura: este temporizador controla el tiempo que pasa entre que una ruta es invalidada (o marcada como inalcanzable) y el tiempo que pasa hasta que se elimina la entrada de la tabla de ruteo. El valor predeterminado es de 240 s. Esto es 60 s más largo que el temporizador de caducidad. Entonces, por 60 s el router estará anunciando sobre la ruta inalcanzable a todos sus vecinos. El valor del temporizador debe setearse en un valor mayor que el temporizador de caducidad.

RIP

RIPv1 - RFC 1058, define RIP como un protocolo de enrutamiento con clase, es decir, basado en las clases de las direcciones IP. Por tanto, RIPv1 no soporta máscaras de tamaño variable (VLSM) ni direccionamiento sin clase (CIDR). Esto implica que las redes tratadas por este protocolo deben tener la máscara de red predefinida para su clase de dirección IP, lo que resulta poco eficiente. Además, RIPv1 tampoco incluye ningún mecanismo de autentificación de los mensajes, haciéndolo vulnerable a ataques cibernéticos.

Utiliza UDP para enviar sus mensajes a través del puerto 520.

RIPv2 - RFC 2453 Esta versión soporta subredes, permitiendo así CIDR y VLSM. Además, para tener retrocompatibilidad con RIPv1, se mantuvo la limitación de 15 saltos si se esta usando el protocolo OSPF o cualquier otro que sirva para direccionamiento en el enlace.

Se agregó una característica de "interruptor de compatibilidad" para permitir ajustes de interoperabilidad más precisos. RIPv2 soporta autenticación, utilizando uno de los siguientes mecanismos: no autentificación, autentificación mediante contraseña, y autentificación mediante contraseña codificada mediante MD5.

RIPng - RFC 2080 es RIP para IPv6.

RIP

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

Cuando RIP está en modo activo envía toda o parte de su tabla a todos los vecinos por broadcast y/o con enlaces punto a punto. Esto se hace cada 30 segundos. La tabla se envía como respuesta ("command" vale 2, aunque no haya habido petición).

Cuando RIP descubre que una métrica ha cambiado, la difunde por broadcast a los demás routers.

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

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

OSPF

Open Shortest Path First (OSPF) – RFC 1247

Es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

Su medida de métrica se denomina cost, y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. OSPF construye además una base de datos enlace-estado (Link-State Database, LSDB) idéntica en todos los routers de la zona.

OSPF puede operar con seguridad usando MD5 para autenticar sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado.

Como sucesor natural de RIP, acepta VLSM y CIDR desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o las extensiones multidifusión para OSPF (MOSPF).

Una red OSPF se puede descomponer en regiones (áreas) más pequeñas. Hay un área especial llamada backbone que forma la parte central de la red a la que se encuentran conectadas el resto de las áreas. Las rutas entre las diferentes áreas circulan siempre por el backbone, por lo tanto todas las áreas deben conectar con él. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.

TCP

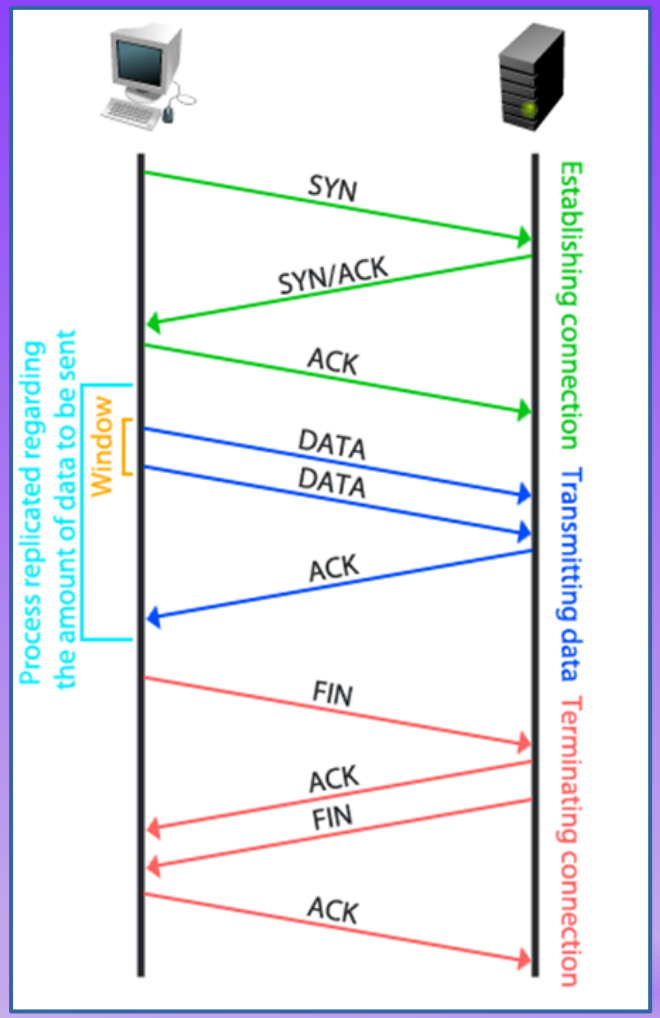
Transmission Control Protocol (TCP) – RFC 793

Muchos programas dentro de una red de datos compuesta por redes de computadoras, pueden usar TCP para crear “conexiones” entre sí a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

TCP da soporte a muchas de las aplicaciones más populares de Internet (navegadores, intercambio de ficheros, clientes FTP, etc.) y protocolos de aplicación HTTP, SMTP, SSH y FTP.

Muchas veces las aplicaciones necesitan que la comunicación a través de la red sea confiable. Para ello se implementa el protocolo TCP que asegura que los datos que emite el cliente sean recibidos por el servidor sin errores y en el mismo orden que fueron emitidos, a pesar de trabajar con los servicios de la capa IP, la cual no es confiable. Es un protocolo orientado a la conexión, ya que el cliente y el servidor deben anunciarse y aceptar la conexión antes de comenzar a transmitir los datos a ese usuario que debe recibirlos.

TCP



TCP permite establecer una conexión entre dos puntos terminales en una red informática común que posibilite un intercambio mutuo de datos. En este proceso, cualquier pérdida de datos se detecta y resuelve, por lo que se considera un protocolo fiable.

Este protocolo siempre confirma el envío y recepción de la información en 3 pasos - Sincronización - Envió de datos y Finalización de la Sesión.

Source port								Destination port
Sequence number								
Acknowledgement number								
Data Offset	Reserved	URG	ACK	PSH	RST	SYN	FIN	Window
Checksum								Urgent Pointer
Options								Padding
Data								

TCP

- Source port - Puerto de origen (16 bits): indica el número de puerto del emisor.
- Destination port - Puerto de destino (16 bits): indica el número de puerto del receptor.
- Sequence number - Número de secuencia (32 bits): el número de secuencia indica el primer byte de los datos de uso anexos o se envía en el contexto del establecimiento o la interrupción de la conexión. Sirve para la validación y clasificación (después de la transmisión) de los segmentos.
- Acknowledgement number - Número de confirmación (32 bits): en este campo se indica el número de confirmación que espera el emisor en siguiente lugar. La condición para su validez es una etiqueta ACK (en el campo “Flags”).
- Offset (4 bits): el campo “Offset” indica la longitud del encabezado en bloques de 32 bits para destacar el punto de inicio de los datos de uso. Dicho punto varía de segmento a segmento debido al campo variable de opciones.
- Reserved - Reservado (6 bits): según RFC 793, reservado para un uso futuro (sin uso hasta ahora). Este campo siempre debe tener un valor igual a “0”.

TCP

- Flags (6 bits): mediante los 6 posibles bits individuales en el campo “Flags” se pueden activar distintas acciones TCP para organizar la comunicación y el procesamiento de datos. Las flags, que se ajustan o no para estas activaciones, son las siguientes:
  - URG. La etiqueta “Urgent” (en español, “urgente”) señaliza a la aplicación TCP que los datos de uso hasta el Urgent-Pointer (véase más abajo) fijado se deben procesar inmediatamente.
  - ACK. Junto con el número de confirmación, ACK sirve para confirmar la recepción de paquetes TCP. Si no se ha ajustado la etiqueta, el número de confirmación se convierte en inválido de forma automática.
  - PSH. “Push” sirve para facilitar un segmento TCP inmediatamente sin tener que pasar por el buffer de datos del emisor y el receptor.
  - RST. Si ha surgido un error durante la transmisión, la aplicación se puede restablecer mediante un paquete TCP con flag RST (“Reset”) ajustado.
  - SYN. Los mensajes con una etiqueta SYN representan el primer paso del triple apretón de manos, es decir, inician el establecimiento de conexión.
  - FIN. “Finish” señaliza a la contraparte que uno de los interlocutores de la comunicación ha finalizado la transmisión.

TCP

- Window - Tamaño de ventana (16 bits): en este campo se le transmite al interlocutor de comunicación el número de bytes que el emisor está dispuesto a recibir.
- Checksum - Suma de comprobación (16 bits): el protocolo es capaz de reconocer errores de transmisión de manera fiable. En este contexto, se usa la suma de comprobación, que se calcula a partir del encabezado, los datos de uso y el denominado seudoencabezado.
- Urgent-Pointer (16 bits): el Urgent-Pointer (indicador “urgente”) indica la posición del primer byte después de los datos de uso que deben tratarse con carácter urgente. Por lo tanto, este campo solo es válido y relevante si tiene una etiqueta URG.
- Options - Opciones (0-320 bits): si se desea que se faciliten funciones TCP que no pertenecen al encabezado general, esta tarea se realiza mediante el campo de opciones. Un ejemplo es la definición del tamaño máximo de segmento. La longitud de las opciones siempre debe ser un múltiplo de 32 bits, en caso contrario, hay que rellenar con bits cero (padding).
- Data: Por defecto se permiten hasta 1500 bytes por segmento, de los que hay que tener en cuenta que 20 bytes son para el encabezado TCP y otros 20 bytes, para el encabezado IP, de manera que quedan 1460 bytes disponibles para datos de uso.

UDP

User Datagram Protocol (UDP) - RFC 768

Es un protocolo del nivel de transporte basado en el intercambio de datagramas. Un datagrama es un fragmento de paquete (mínimo posible) que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el receptor, de manera independiente a los fragmentos restantes.

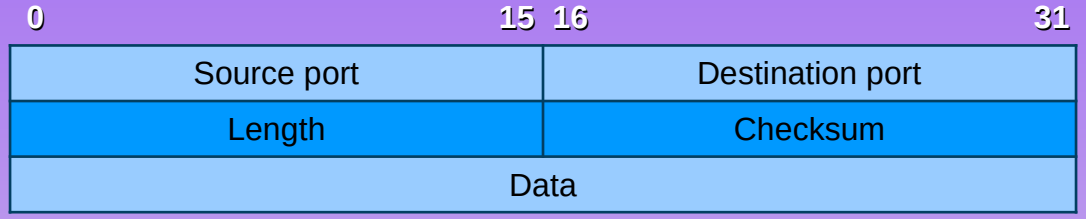
Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros;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

UDP solo añade multiplexado de aplicación y suma de verificación de la cabecera y la carga útil. Cualquier tipo de garantías para la transmisión de la información deben ser implementadas en capas superiores.

UDP

UDP utiliza puertos al igual que el TCP, el protocolo UDP utiliza puertos para permitir que los datagramas se transfieran a los protocolos correctos, es decir, a las aplicaciones elegidas del sistema de destino. Los puertos quedan definidos mediante un número conforme a un rango de valores válidos, estando reservado el rango de 0 a 1023 para los servicios fijos.

El protocolo UDP no ofrece ninguna garantía de seguridad e integridad de los datos: la ausencia de acuse de recibo mutuo entre el emisor y el receptor garantiza que la velocidad de transmisión en el protocolo UDP sea excelente; no obstante, el protocolo no puede garantizar la seguridad ni la integridad de los datagramas. Tampoco puede garantizar el orden de los paquetes enviados. Por ello, los servicios que utilizan UDP deben aplicar sus propias medidas de corrección y protección.



- Source port: puerto desde el que se ha enviado un datagrama concreto. El receptor necesita esta información para poder responder al paquete. Es opcional.

- Destination port: indica el servicio solicitado. Esta información es obligatoria, al contrario que el puerto de origen, porque si no, no sería posible asignar correctamente el datagrama.
- Checksum: se utiliza para detectar errores durante la transmisión.

Protocolos de Aplicación

- DHCP - Protocolo de Configuración dinámica de máquina - Uso para distribuir direcciones IP en forma dinámica a cada máquina de la red
- DNS - Sistema de Nombres de Dominio - Reemplaza el Nombre de Dominio por la dirección IP correspondiente. Sistema de búsqueda de Nombres de Dominio.
- FTP - TCP - Protocolo de Transferencia de Archivos bajo TCP - Conexión entre equipo cliente servidor para transferencia de archivos. Involucra un lenguaje de manejo de archivos y carpetas del servidor FTP.
- FTP - TLS - Mismo que el anterior pero bajo seguridad TLS.
- HTTP - Protocolo de Transferencia de Hipertexto - Permite la transferencia de páginas con hipervínculos.
- HTTPs - Mismo que anterior pero bajo seguridad de SSL.
- IMAP 4 - Protocolo de Acceso a Mensajes de Correo - Permite la sincronización del servidor de correo electrónico con cliente en máquina remota.
- IRC - Protocolo de comunicación en tiempo real basado en texto
- KERBEROS - Protocolo de autenticación para equipos en una red.
- LDAP - Protocolo Simplificado de Acceso a Directorio - Permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

Protocolos de Aplicación

- MUC - Protocolo de conferencia como sistema de chat entre más de 2 personas
- NFS - Permite distribuir archivos por diferentes servidores de la red.
- NIS - Servicios de Información de Red - Es un servicio idéntico al DNS.
- NTP - Protocolo del Reloj en una red - Servicio de sincronismo de la Hora en la red.
- POP3 - Protocolo de Oficina de correo - Sincronización de correo entrante.
- RPC - Protocolo que permite ejecutar código en otra máquina remota sin preocuparse por la comunicación entre ambos.
- SMTP - Protocolo Simple de Transferencia de Correo - Sincronización de correo saliente.
- SNMP - Protocolo Simple de Administración de Red - Permite Manejo de la Red.
- SSH - Protocolo de Seguridad.
- TelNet - Control Remoto de Máquina tipo Consola. Permite controlar una máquina remotamente.
- TFTP - UDP - FTP Ordinario - No orientado a la conexión - Realiza la misma función que el protocolo FTP pero sin confirmar los comandos dados.
- XMPP - Protocolo Extensible de Mensajería Instantánea - Es un protocolo de comunicaciones para middleware orientado a mensajes basado en XML (Extensible Markup Language). Permite el intercambio casi en tiempo real de datos estructurados pero extensibles entre dos o más entidades de red.

Bibliografía & Licencia

- Tanenbaum, A. y Wetherall, D. (2012). *Redes de Computadoras, 5ta. ed.* Pearson Educación.
- Kurose, J. y Ross K. (2017). Redes de computadoras. Un enfoque descendente, 7ma. ed. Pearson Educación.

- Autor:

Matías E. García

Prof. & Tec. en Informática Aplicada

www.profmatiasgarcia.com.ar

info@profmatiasgarcia.com.ar