



UT1.1 Repaso Arquitecturas de protocolos.

(Curso 2015 - 2016)



Modelo OSI

- Para entender la forma en que los protocolos TCP/IP permiten las comunicaciones de red, es necesario comprender los conceptos subyacentes a las comunicaciones en la red. El modelo OSI es un **modelo conceptual** que se utiliza habitualmente como referencia para comprender las comunicaciones de red.



Modelo OSI

- El modelo OSI es un modelo de arquitectura que representa las comunicaciones de red. Lo presentó en 1978 la **ISO** (International Standards Organization, Organización Internacional de Normalización) para explicar las comunicaciones de red entre hosts en una LAN o WAN, presentar un sistema de clasificación de familias de protocolos de comunicaciones y mostrar cómo las diferentes familias de protocolos pueden comunicarse entre ellas.



Modelo OSI

- Para entender la forma en que los protocolos TCP/IP permiten las comunicaciones de red, es necesario comprender los conceptos subyacentes a las comunicaciones en la red. El modelo OSI es un **modelo conceptual** que se utiliza habitualmente como referencia para comprender las comunicaciones de red.

Modelo OSI

- Cuando se hace referencia a “diferentes familias de protocolos” es principalmente porque hay que tener en cuenta que TCP/IP no es la única familia de protocolos existente, aunque sí que sea la más conocida. Si dispositivos TCP/IP necesitan comunicarse con otros dispositivos a través de diferentes protocolos, el modelo OSI puede ayudar a entender cómo se realiza dicha comunicación. Además de poder ser definido bajo el modelo OSI, TCP/IP tiene su propio modelo de comunicaciones, como veremos más adelante.



Modelo OSI

- Es importante darse cuenta de que el modelo OSI se creó después de existir las comunicaciones de redes. Este modelo se creó como una abstracción para clasificar las comunicaciones que ya existían. De hecho, este modelo fue creado para ayudar a los administradores de comunicaciones a entender qué ocurre con las diferentes comunicaciones entre protocolos. Esto es lo que les llevó a dividir el modelo OSI en diferentes capas, cada una con su función.



1 - Física

- Establece la interfaz física y los mecanismos necesarios para colocar el flujo de bits de datos sin formato en el cable. Incluye entre otros los cables, conectores, paneles de parcheo, hubs, repetidores. La unidad de medida en esta capa es bits.

2- Enlace

- Permite transferir sin errores tramas de datos desde un equipo a otro a través de la capa física. En el contexto del modelo de referencia OSI, una trama es un sobre electrónico de información que incluye el paquete y otros datos que agregan las siete capas del modelo OSI. Las capas que se encuentran por encima de la capa de enlace pueden realizar transmisiones a través de la red prácticamente sin errores. Los dispositivos que se pueden incluir en esta capa son las tarjetas de red, puentes y switches, entre otros. Trabaja con MACs y su unidad de medida es tramas.

3 - Red

- Determina la ruta física de los datos que se van a transmitir en función de las condiciones de la red, la prioridad del servicio y otros factores. Los dispositivos que trabajan en esta capa son entre otros los routers y los IPswitches (switches de capa 3). Trabaja con direcciones lógicas (por ejemplo direcciones IP). La unidad de medida en esta capa es paquetes.

4 - Transporte

- Garantiza que los paquetes sean entregados en el orden en que fueron enviados sin que se pierdan ni se dupliquen. En el contexto del modelo de referencia OSI, un paquete es un sobre electrónico que contiene información generada entre la capa de sesión y la capa física del modelo OSI. Cuando hablamos de “puertos” estamos haciendo referencia a esta capa. La unidad de medida es segmentos o mensajes.



5 - Sesión

- Permite que dos aplicaciones creen una conexión de comunicación persistente. Los famosos log on o log off operan en esta capa. El protocolo Netbios (Network Basic Input Output System) trabaja en esta capa.

6 - Presentación

- Convierte los datos entre los distintos sistemas de una red. La capa de presentación convierte los datos generados por la capa de aplicaciones de su propia sintaxis a una sintaxis de transporte común para su transmisión a través de una red. Cuando los datos llegan al equipo de destino, la capa de presentación de dicho equipo convierte la sintaxis en la del propio equipo.



7- Aplicación

- Proporciona un punto de entrada para que programas como los exploradores de Web y los sistemas de correo electrónico puedan obtener acceso a los servicios de red.



Relación entre capas

- Pueden estar o no involucradas todas la capas:
- Por ejemplo, si hacemos un ping a otro equipo sólo las capas 1, 2 y 3 son utilizadas. Todo depende del tipo de comunicación y del número de protocolos implicados en cada transmisión.

Switches

- Los switches de capa 2 son los más comunes. Estos switches utilizan la dirección MAC para decidir las diferentes comunicaciones entre sus puertos. Normalmente este tipo de switches no modifican las tramas y cada puerto del switch es considerado como un único segmento y por lo tanto un dominio de colisión.
- Algunos switches de capa 2 permiten configurar VLANs. Cuando se realiza esto se reducen las colisiones, se organiza la red, se mejora el rendimiento y sobre todo, se incrementa la seguridad. Sin embargo para que esto sea seguro será necesario que el acceso físico al switch esté restringido.

Switches

- Existen switches que pueden trabajar en capa 3. Las principales diferencias con los de capa 2 son que en algunas comunicaciones utilizan las direcciones IP en lugar de las MAC. Se parecen a los routers. Los switches de capa 3 trabajan con paquetes y los de capa 2 trabajan con tramas. Los switches de capa 3 son generalmente administrables utilizando el protocolo SNMP, entre otras utilidades. Esto permite a los administradores de red analizar los paquetes que atraviesan los switches, algo que generalmente no permiten los switches de capa 2. Los switches de capa 3 se suelen utilizar en grandes redes en las que se quieren comunicar diferentes redes IP.

Protocolos, capas y dispositivos

CAPA	PROTOCOLOS	DISPOSITIVOS
7- Aplicación	FTP, HTTP, POP3, SMTP	Gateway (enrutamiento por servicio)
6 - Presentación	Compression, Encryption	-
5 - Sesión	Logon/Logoff	-
4 - Transporte	TCP, UDP	-
3 - Red	IP, ICMP, ARP, RIP	Routers
2 - Vínculo de Datos (DLL- Data Link Layer)	802.3, 802.5	NICs, switches, bridges, WAPs
1 - Física	100BASE-T, 1000BASE-X	Physical Hubs, patch panels, RJ45 jacks

TCP / IP

- TCP/IP es un paquete estándar de protocolos que facilita la comunicación en un entorno heterogéneo. Las tareas que conlleva el uso de TCP/IP en el proceso de comunicación se distribuyen entre los protocolos, los cuales están organizados para formar cuatro capas distintas de la pila de TCP/IP.

Capas TCP / IP

- Las cuatro capas de la pila de protocolos TCP/IP son:
 - 4.- Capa de aplicación
 - 3.- Capa de transporte
 - 2.- Capa de Internet
 - 1.- Capa de vínculo (enlace o acceso al medio)

1- Capa de vínculo

- La capa de vínculo (denominada a veces capa de red o capa de vínculo de datos) corresponde a las capas de vínculo de datos y física del modelo OSI. Esta capa especifica los requisitos necesarios para enviar y recibir paquetes. Se encarga de colocar datos en la red física y de recibir datos de dicha red



2- Capa de Internet

- La capa de Internet corresponde a la capa de red del modelo OSI. Los protocolos de esta capa encapsulan datos de la capa de transporte en unidades denominadas paquetes, las dirigen y las enrutan hasta sus destinos. Existen cuatro protocolos principales en la capa de Internet, como muestra la tabla siguiente

2- Capa de Internet

Protocolo	Descripción
IP Internet Protocol, Protocolo Internet.	Direcciona y enruta paquetes entre los hosts y las redes.
ARP Address Resolution Protocol, Protocolo de resolución de direcciones.	Obtiene direcciones de hardware de los hosts ubicados en una misma red física.
IGMP Internet Group Management Protocol, Protocolo de administración de grupos de Internet.	Administra la pertenencia a un host de grupos de multidifusión IP.
ICMP Internet Control Message Protocol, Protocolo de mensajes de control de Internet.	Envía mensajes y notifica errores relacionados con la entrega de paquetes.



3- Capa de Transporte

- La capa de transporte corresponde a la misma capa del modelo OSI y es la responsable de garantizar la entrega y la comunicación entre ambos extremos, para lo que utiliza uno o dos de los protocolos descritos en la tabla siguiente.

3- Capa de Transporte

Protocolo	Descripción
UDP User Datagram Protocol, Protocolo de datagrama de usuario.	Proporciona comunicaciones sin conexiones y no garantiza la entrega de los paquetes. La aplicación se encarga de garantizar la entrega. Las aplicaciones utilizan UDP para agilizar la comunicación con menos sobrecarga general que si se utiliza TCP. SNMP utiliza UDP para enviar y recibir mensajes por la red. Generalmente las aplicaciones transfieren pequeñas cantidades de datos a la vez utilizando UDP.
TCP Transmission Control Protocol, Protocolo de control de transporte.	Proporciona comunicaciones fiables mediante conexiones para aplicaciones que habitualmente transfieren grandes cantidades de datos a la vez o que necesitan una confirmación de la recepción de los datos.

3- Capa de Transporte

- La capa de transporte trabaja con la transmisión de mensajes a través de subredes. Dos protocolos muy comunes son el TCP (fiable y orientado a conexión) y el UDP (no orientado a conexión). Un ejemplo de aplicación que utiliza TCP es un navegador web mientras que los servicios de retransmisión de vídeo en tiempo real utilizan UDP. Cuando nos descargamos una página web no queremos perder información. Al utilizar TCP nos aseguramos de que todos los datos llegan a su destino. Si un paquete se pierde se vuelve a enviar. Sin embargo en el caso de la retransmisión de un partido de fútbol no tiene sentido parar la transmisión para reenviar un paquete ya que la pérdida de un frame es aceptable.

3- Capa de Transporte

- Las comunicaciones orientadas a conexión (conocidas como Modo CO) requieren que tanto emisor como receptor estén pendientes de la comunicación estableciendo una conexión entre ellos.
- Las comunicaciones no orientadas a conexión (conocidas como Modo CL) no establecen una conexión previa entre emisor y receptor sino que el emisor simplemente transmite los paquetes. El paquete se envía a la dirección de destino que figura en la cabecera del paquete.

3- Capa de Transporte

- Esta capa también trabaja con los puertos que los diferentes hosts utilizan para la transmisión de datos. Existen un total de 65536 puertos (desde el 0 al 65535).
- Los números de puerto se corresponden con aplicaciones específicas. Por ejemplo el puerto 80 es utilizado por los navegadores web para acceder al protocolo HTTP. Es muy importante entender la diferencia entre puertos de entrada y puertos de salida.

3- Capa de Transporte

NÚMERO DE PUERTO	PROTOCOLO	NOMBRE COMPLETO
20 y 21	FTP (datos y control)	File Transfer Protocol
22	SSH	Secure Shell
23	Telnet	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name System
67 y 68	DHCP (cliente y servidor)	Dinamic Hosts Control Protocol
80	HTTP	Hypertext Transfer Protocol
88	Kerberos	Kerberos
110	POP3	Post Office Protocol Version 3
119	NNTP	Network News Transfer Protocol
137-139	NetBIOS	NetBIOS Name, Datagram, and Session Services, respectively
143	IMAP	Internet Access Message Protocol
443	HTTPS	Hipertext Transfer Protocol Secure

4- Capa de Aplicación

- La capa de aplicación corresponde a las capas de aplicación, presentación y sesión del modelo OSI. Esta capa proporciona servicios y utilidades que permiten el acceso de las aplicaciones a los recursos de la red.
- Dos de los servicios de esta capa que dan acceso a los recursos del sistema son Windows Sockets y el sistema básico de entrada y salida de red (NetBIOS). Tanto Windows Sockets como NetBIOS proporcionan interfaces de aplicación estándar para que los programas tengan acceso a los servicios de la red.

4- Capa de Aplicación

Protocolo	Descripción
HTTP Hypertext Transfer Protocol, Protocolo de transferencia de hipertexto.	Especifica los procesos de interacción cliente/servidor entre los exploradores de Web y los servidores Web.
FTP File Transfer Protocol, Protocolo de transferencia de archivos.	Realiza transferencias de archivos y tareas básicas de administración de archivos en equipos remotos.
SMTP Simple Mail Transport Protocol, Protocolo simple de transferencia de correo.	Lleva mensajes de correo electrónico de un servidor a otro y de clientes a servidores.
DNS Domain Naming System, Sistema de nombres de dominio.	Resuelve nombres de host de Internet en direcciones IP para las comunicaciones de red.
RIP Routing Information Protocol, Protocolo de información de enrutamiento.	Permite a los enrutadores recibir información acerca de otros enrutadores de una red.
SNMP Simple Network Management Protocol, Protocolo simple de administración de redes.	Permite recopilar información acerca de dispositivos de red, como concentradores, enrutadores y puentes. Cada fragmento de información que se recopila se define en una MIB (Management Information Base, Base de datos de información).



Herramientas para analizar protocolos. Wireshark

- Wireshark es un analizador de protocolos de red ("sniffer") que sirve para visualizar el tráfico de paquetes que circulan por las redes de computadores, permitiendo analizar su comportamiento, detectar errores, cuellos de botella, etc.



Herramientas para analizar protocolos. Wireshark

- Este monitor de red captura una copia de estos paquetes para que podamos realizar un análisis posterior. Está programado para reconocer la estructura de los diferentes protocolos de red. Esto le permite mostrar la encapsulación y los campos individuales de una PDU e interpretar su significado. Es una herramienta útil para cualquiera que trabaje con redes y se puede utilizar para el análisis de datos y el diagnóstico de fallas.



Herramientas para analizar protocolos. Wireshark

- Wireshark es un analizador de protocolos de red ("sniffer") que sirve para visualizar el tráfico de paquetes que circulan por las redes de computadores, permitiendo analizar su comportamiento, detectar errores, cuellos de botella, etc.