

Tarea para clase 7

Estudiante

Gabriel León Casto

Host: Se usa para referirse a los dispositivos conectados a una red que proveen y utilizan servicios de la misma.

Media: Hace referencia a el canal de referencia usado para interconectar nodos en una red.

Hub: Es un dispositivo que recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.

Switch: Es muy similar a un hub, diferenciándose porque el Switch puede pasar datos de un segmento a otro de acuerdo con la dirección MAC o IP. En otras palabras, el switch es más configurable y más sofisticado que un Hub.

Router: Es un dispositivo que permite interconectar dispositivos de red. Se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red.

Gateway: Es el dispositivo o configuración que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más hosts.

Firewall: Es el dispositivo o software de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

¿Qué es y por qué se crea el modelo TCP/IP? Explique sus niveles.

Es un conjunto de protocolos que permiten la comunicación entre los ordenadores pertenecientes a una red. La sigla TCP/IP significa Protocolo de control de transmisión/Protocolo de Internet.

Se creo con el fin de crear un modelo robusto y fiable de protocolos para la comunicación entre redes informáticas, ya que anteriormente a esta el ejercito de EEUU había desarrollado ARPAnet que tenía como finalidad que resistiera un ataque de la URSS. Pero esta red no resultó ser tan fiable como se esperaba y así es como empezó a desarrollarse e investigar el modelo TCP/IP.

Capa TCP/IP	Explicación
Aplicación	maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa
Transporte	está encargado de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados, así como de mantener el flujo de la red.
Internet	Acepta y transfiere paquetes para la red. Esta capa incluye el potente Protocolo de Internet (IP), el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP).
Vínculo de datos	Identifica el tipo de protocolo de red del paquete, en este caso TCP/IP. La capa de vínculo de datos proporciona también control de errores y estructuras.
Física	Especifica las características del hardware que se utilizará para la red.

¿Qué es y porque se crea el Modelo OSI? explique sus niveles.

Es un estándar que tiene por objetivo conseguir interconectar sistemas de procedencia distinta para que estos pudieran intercambiar información sin ningún tipo de impedimentos debido a los protocolos con los que estos operaban de forma propia según su fabricante.

Y se creó porque muchas de las redes eran incompatibles y se volvió muy difícil para las redes que utilizaban especificaciones distintas poder comunicarse entre sí. Para solucionar este problema, la Organización Internacional para la normalización realizó varias investigaciones acerca de los esquemas de red.

Modelo OSI	Explicación
Aplicación	Programas de aplicación que usan la red.
Presentación	Estandariza la forma en que se presentan los datos a las aplicaciones.
Sesión	Gestiona las conexiones entre aplicaciones cooperativas.
Transporte	Proporciona servicios de detección y corrección de error
Red	Gestiona conexiones a través de la red para las capas superiores.
Enlace de datos	Proporciona servicio de envío de datos a través del enlace físico.
Física	Define las características físicas de una red informática.

¿Qué es, cómo funciona y qué significa IPv4?

IPv4 es un protocolo de interconexión de redes basados en Internet, y que fue la primera versión implementada en 1983 para la producción de ARPANET.

El direccionamiento IPv4 se basa en 4 octetos que van de 0 a 255, haciendo así posible cerca de 4300 millones de IPs únicas y significa "Internet protocol version 4".

Con IPv4 cada paquete posee una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de Capa 3.

Estructura del paquete IPv4

Una serie de 32 bits es difícil de interpretar e incluso más difícil de recordar. Por lo tanto, representamos direcciones IPv4 utilizando el formato decimal punteado.

Los patrones binarios que representan direcciones IPv4 son expresados con puntos decimales separando cada byte del patrón binario, llamado octeto, con un punto. Se le llama octeto debido a que cada número decimal representa un byte u 8 bits.

Por ejemplo, la dirección: 10101100000100000000010000010100. Es expresada en puntos decimales como: 172.16.4.20

¿Qué es, cómo funciona y por qué se crea la IPv6?

IPv6 es una nueva versión de el protocolo IP y fue creada con el fin de sustituir a la IPv4 ya que esta posee mayor cantidad de direcciones que la IPv4.

A diferencia de IPv4, IPv6 se basa en un sistema hexadecimal haciendo que está tenga 340 sextillones de direcciones IP.

¿Qué es, como funciona y por qué se crea la MAC address?

Una MAC address es un identificador único de 48 bits, conformado de 6 bloques de 2 caracteres hexadecimales, que hace referencia a un numero identificador único de una tarjeta o un dispositivo de red. Y se creó con el fin de poder identificar y rastrear cada dispositivo capaz de conectarse a una red.

Explique las clases de las direcciones A, B, C, D y E

La clase A va del rango de la IP 0.0.0.0 – 126.255.255.255 y es capaz de admitir 16 777 214 de hosts en una sola red.

La clase B va del rango de la IP 128.0.0.0 – 191.255.255.255 y es capaz de admitir 65 536 de hosts en una sola red.

La clase C va del rango de la IP 192.0.0.0 – 223.255.255.255 y es capaz de admitir 254 de hosts en una sola red.

La clase D va del rango de la IP 224.0.0.0 – 239.255.255.255 y esta clase de IPs es multicast.

La clase E va del rango de la IP 240.0.0.0 – 255.255.255.255 y es un rango de IPs experimentales.

Explique el funcionamiento de los protocolos FTP, SNMP y SMTP

FTP: Su funcionamiento es poder intercambiar ficheros entre máquinas a través de la red con independencia del sistema de archivos y sistema operativo utilizado de una forma eficaz.

SNMP: Es un protocolo que les permite a los administradores de red administrar dispositivos de red y diagnosticar sus problemas. El protocolo SNMP tiene dos formas de trabajar: polling y traps. El polling se apoya en enviar consultas remotas ya sea de forma activa o bajo demanda, ejecutando una operación síncrona de consulta. Los traps, sin embargo, son más bien mensajes que lanzan los dispositivos SNMP a una dirección ya constituida, basándose en cambios o eventos, esta vez de forma asíncrona.

SMTP: Es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos