Nombre de la Materia:
Fundamentos de Telecomunicaciones Aula

Nombre de la Licenciatura:
Ing. Sistemas Computacionales.

Nombre del Alumno(a):

Pool Ramírez Miguel Ángel.

Nombre de la Tarea:

IPV4 , Subneteo y Calculo de Redes

Unidad #

Nombre de la Unidad:

Nombre del Profesor(a):

Ing. Ismael Jiménez Sánchez

Fecha: 11/01/21

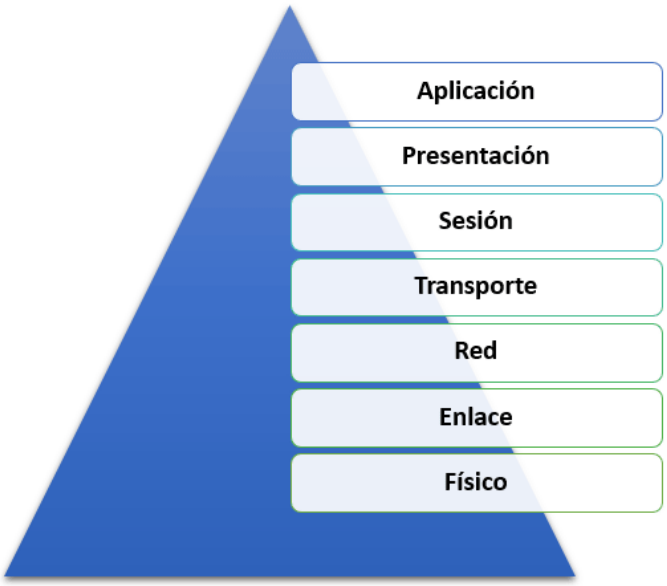
Modelo OSI el estándar de redes

Y para ello debemos hacer una rápida referencia al modelo OSI (Open System Interconection). Se trata de un modelo de referencia y no una arquitectura de red, para los diferentes protocolos de red que intervienen en las comunicaciones a través de equipos informáticos. El modelo divide en 7 niveles los sistemas de telecomunicaciones para diferenciar las distintas etapas de recorrido de los datos desde un punto a otro, así como los protocolos que intervienen en cada una.

El modelo OSI lo desarrolló allá por 1984 la organización ISO (International Organization for Standarization). Este estándar perseguía el ambicioso objetivo de conseguir interconectar sistema de procedencia distinta para que esto pudieran intercambiar información sin ningún tipo de impedimentos debido a los protocolos con los que estos operaban de forma propia según su fabricante.

El modelo OSI está conformado por 7 capas o niveles de abstracción. Cada uno de estos niveles tendrá sus propias funciones para que en conjunto sean capaces de poder alcanzar su objetivo final. Precisamente esta separación en niveles hace posible la intercomunicación de protocolos distintos al concentrar funciones específicas en cada nivel de operación.

Los niveles de los que se compone el modelo OSI son:



Ya sabemos que hay un modelo que clasifica por así decirlo los protocolos de red, y precisamente IPv4 e IPv6 son dos de estos protocolos de red. En este caso operan en uno de los niveles más bajos del modelo, la capa de red o capa 3. Esta capa se encarga del enrutamiento de paquetes entre dos redes conectadas. Hará que los datos puedan llegar desde el transmisor al receptor mediante conmutaciones y encaminamientos necesarios desde un punto a otro.

Por debajo de ella tenemos la capa de enlace de datos (capa 2) en la que trabajan los switch, y por encima la capa 4 o capa de transporte en la que interviene el protocolo TCP que transporta los paquetes mediante datagramas.

Que es una dirección IP

Hablamos de dirección IP como un conjunto numérico en decimal o hexadecimal (ya lo veremos) que identifica de manera lógica y atendiendo a una jerarquía una interfaz de red. A todo dispositivo conectado a una red se le debe asignar una dirección IP, un identificador temporal como puede ser nuestro DNI mientras estemos en este mundo o un número de teléfono mientras tengamos contratado un servicio telefónico. Gracias a la IP los distintos equipos se pueden comunicar entre ellos haciendo que los paquetes viajen por la red hasta encontrar su destinatario.

La dirección IP puede ser fija (IP fija) o dinámica (DHCP o Dynamic Host Configuration Protocol), siempre asignada por un servidor o un enrutador que trabaje en la capa de red. Cuando hablamos de IP fija quiere decir que host siempre tendrá la misma dirección IP, aunque se apague y se vuelva a encender. Mientras que en DHCP la IP se asigna de forma dinámica al host cuando se encienda, claro que a los nodos de una red se les suele entregar la misma dirección IP siempre tras asociarse la primera vez al enrutador.

Protocolo IP

La dirección IP es el identificador perteneciente al protocolo IP (Internet Protocol), el cual es el sistema de direccionamiento IPv4 e IPv6 como versión más nueva y preparada para el futuro. Es un protocolo que opera en la capa de red y no orientado a la conexión, esto significa que la comunicación entre dos extremos de una red e intercambio de datos se puede hacer si un acuerdo previo. Es decir, el receptor transmite datos sin saber si el recetor está disponible, así que a este le llegaran cuando se encienda y esté conectado.

IPv4 e IPv6 transfieren paquetes de datos conmutados a través de las redes físicas que operan según el modelo OSI. Esto se hace gracias al enrutamiento, una técnica que permite al paquete

buscar la ruta más rápida hacia el destino, aunque sin garantías de que llegue, claro que esta garantía la da la capa de transporte de datos con TCP, UDP, u otro protocolo.

Los datos que maneja el protocolo IP se dividen en paquetes llamados datagramas, los cuales no cuentan con ningún tipo de protección o control de errores para su envío. Si un datagrama se enviará solo con IP podría o no llegar, roto o completo, y en un orden aleatorio. Solamente lleva información sobre la dirección IP de origen y de destino junto a los datos.

IPv4

El protocolo IPv4, el cual lleva operando en redes desde 1983 cuando se creó la primera red de intercambio de paquetes ARPANET el cual está definido por la norma RFC 791. Y como dice su denominación es el protocolo IP en versión 4, pero es que no tenemos versiones previas implementadas y este fue el primero de todos.

IPv4 utiliza una dirección de 32 bits (32 unos y ceros en binario) dispuestos en 4 octetos (números de 8 bits) separados por puntos en notación decimal. Trasladando esto a la práctica será un número tal que así:

192.168.0.102

De esta forma podremos tener direcciones que van desde la 0.0.0.0 hasta la 255.255.255.255. si traducimos la IP anterior a su código binario tendremos:

192.168.0.102 = 11000000.10101000.00000000.01100110

Es decir 32 bits, así que con IPv4 seremos capaces de direccionar un total de:

232 = 4 294 967 296 hosts

Cabecera IPv4

Por ello conviene darle un repaso a la estructura de una cabecera IPv4 la cual tiene un tamaño mínimo de 20 Bytes y máximo de 40 Bytes.

<table>
<tr><th>Bits</th><th>0-3</th><th>4-7</th><th>8-15</th><th>16-18</th><th>19-31</th></tr>
<tr><td rowspan="6">20
Bytes
mínimo</td><td>Versión</td><td>IHL</td><td>Tipo de servicio</td><td colspan="2">Long. total</td></tr>
<tr><td colspan="3">Identificador</td><td>Flags</td><td>Offset fragmento</td></tr>
<tr><td colspan="2">TTL</td><td>Protocolo</td><td colspan="2">Checksum de cabecera</td></tr>
<tr><td colspan="5">IP de origen</td></tr>
<tr><td colspan="5">IP de destino</td></tr>
<tr><td colspan="4">Opciones</td><td>Relleno</td></tr>
<tr><td colspan="6">Datos
...
...</td></tr>
</table>

Vamos a explicar de forma rápida cada apartado, ya que luego algunos serán extensibles a IPv6

- **Versión (4 bits):** identifica la versión del protocolo, siendo 0100 para v4 y 0110 para v6.
- **IHL (4 bits):** es el tamaño de la cabecera, que puede ser de 20 bytes hasta 60 bytes o lo qu es lo mismo desde 160 bits a 480 bits.
- **Tiempo de servicio (8 bits):** un identificador en caso de que el paquete sea especial, por ejemplo, más importante en cuenta a urgencia de entrega.
- **Longitud total (16 bits):** refleja el tamaño total que tenga el datagrama o del fragmento en octetos.
- **Identificador (16 bits):** se usa si el datagrama es fragmentado para que luego pueda unirse
- **Flags (3 bits) y Offset o posición del fragmento (13 bits):** 1º bit será 0, 2º bit (0=divisible, 1 no divisible), 3º bit (0=ultimo fragmento, 1=fragmento intermedio)
- **TTL (8 bits):** tiempo de vida del paquete IPv4. Refleja la cantidad de saltos en enrutadores que puede dar, siendo de 64 o 128. Cuando se agota el paquete se elimina.
- **Protocolo:** indica el protocolo al que debe entregarse el datagrama en capas superiores, por ejemplo TCP, UDP, ICMP, etc.
- **Checksum:** para controlar la integridad del paquee recalculándose cada vez que algún valor anterior cambie.

¿Qué es el subnetting?

Definido de la forma más simple, el término subnetting hace referencia a la subdivisión de una red en varias subredes. El subneteo permite a los administradores de red, por ejemplo, dividir una red empresarial en varias subredes sin hacerlo público en Internet. Esto se traduce en que el router que

establece la conexión entre la red e Internet se especifica como dirección única, aunque puede que haya varios hosts ocultos. Así, el número de hosts que están a disposición del administrador aumenta considerablemente.

Con la aparición de IPv6, que abarca 128 bits y reemplazará a la versión IPv4 en los próximos años, las direcciones IP ausentes ya no tendrán un papel principal para la creación de subredes.

Los motivos para el subneteo de redes son múltiples. Las subredes funcionan de manera independiente las unas de las otras y la recogida de los datos se llevan a cabo con mayor celeridad. ¿Cuál es el motivo para ello? El subnetting hace que la red adquiera una mayor claridad. El denominado broadcast, en el que los participantes envían datos a toda la red, se lleva a cabo de manera descontrolada a través de subredes, pero, por medio de subnets, el router envía los paquetes de datos al destinatario específico. Si los emisores y los receptores se encuentran en la misma subred, los datos se pueden enviar directamente y no tienen que desviarse.

Cuando se introdujo el protocolo de Internet, la Internet Engineering Task Force (IETF) estableció las cinco clases de direcciones IP A, B, C, D y E. Cada una de estas clases puede identificarse por medio del rango de direcciones en el que se encuentran.

Clase A	Clase B	Clase C	Clase D	Clase E
0.0.0.0 - 127.255.255.255	128.0.0.0 - 191.255.255.255	192.0.0.0 - 223.255.255.255	224.0.0.0 - 239.255.255.255	240.0.0.0 - 255.255.255.255

La clase determina el número de direcciones de red que están disponibles y la cantidad de hosts que albergan las respectivas redes. En la clase A, el primer bloque numérico (también denominado octeto porque un bloque está compuesto por 8 bits) está reservado para la dirección de red y los tres últimos están disponibles para los ID de los hosts, lo que significa que hay pocas redes, pero muchos hosts. En la clase B, los primeros dos bloques son responsables de los Net ID, lo que da como resultado más redes, pero menos hosts. La clase C solo alberga el último octeto para las direcciones de hosts restantes. Por su parte, los rangos de direcciones de las clases D y E están reservados y no se pueden adjudicar.

¿Cómo funciona el subnetting?

En el subnetting o subneteo se toman bits del ID del host "prestados" para crear una subred. Con solo un bit se tiene la posibilidad de generar dos subredes, puesto que solo se tiene en cuenta el 0

o el 1. Para un número mayor de subredes se tienen que liberar más bits, de modo que hay menos espacio para direcciones de hosts. Cabe remarcar en este caso que tanto las direcciones IP de una subred como aquellas que no forman parte de ninguna tienen la misma apariencia y los ordenadores tampoco detectan ninguna diferencia, de ahí que se creen las llamadas máscaras de subred. Si se envían paquetes de datos de Internet a la propia red, el router es capaz de decidir mediante esta máscara en qué subred distribuye los datos.

Como ocurre con las direcciones de IPv4, las máscaras de red contienen 32 bits (o 4 bytes) y se depositan en la dirección como una máscara o una plantilla. Una típica máscara de subred tendría la siguiente apariencia: 255.255.255.128

¿Cómo se calcula una máscara de red?

Ya hemos explicado cuáles son las conclusiones que se pueden extraer de las direcciones IP y de las máscaras de red. Sin embargo, de manera habitual, los administradores de red se enfrentan a otro problema: dados la dirección de red y el número de hosts que debe alojar la subred, el administrador debe calcular una máscara de subred que permita suficientes hosts. Para ello utiliza la fórmula x = 2^n - 2.

Puesto que se trata de un sistema binario, el cálculo se hará con potencias de dos. n hace referencia al número de bits que son iguales a cero en la máscara de red. A continuación, se resta el valor 2 para hacer desaparecer las direcciones de broadcast y de red y X arroja como resultado los hosts posibles.

Si, por ejemplo, un administrador de red tiene que alojar 150 ordenadores en su red, en primer lugar, buscará la potencia más elevada de 2, donde 27 no se tiene en cuenta, ya que 128 es un número muy bajo. Por ello, escogerá 28-2, es decir, 254 hosts. Los últimos 8 bits de la máscara de red son, por lo tanto, 0.

Binario	11111111	11111111	11111111	00000000
Decimal	255	255	255	0

Con la máscara de subred 255.255.255.0 se pueden liberar suficientes hosts.

También debe tenerse en cuenta que solo deben crearse subredes tomando bits prestados de la parte del host de izquierda a derecha. De ello se deduce la estructura ordenada de la máscara de subred y el hecho de que solo puedan utilizarse nueve valores diferentes en un octeto:

¿Por qué es tan importante el subnetting?

Las secuencias numéricas, las conversiones binarias y las comparaciones lógicas tienen un efecto disuasorio. Sobre todo, en el contexto de la transición a IPv6 muchos se preguntan si realmente merece la pena. La respuesta es claramente afirmativa. Esto es lo que hace que el subneteo también sea relevante para el futuro:

Ampliación del rango de direcciones dentro de una red: el subnetting permite que el administrador de redes pueda decidir el tamaño que tendrán sus redes.
Conexión rápida entre los hosts y las subredes: los paquetes de datos llegan directamente del emisor al receptor y, en principio, no se transmiten por toda la red a través del router.
Mejor organización lógica de los participantes en la red: para obtener una visión más completa de los hosts, es conveniente hacer una segmentación de los mismos por departamentos o en función de criterios locales (edificios y plantas diferentes).
Mayor grado de seguridad: si un participante de la red es víctima de un ataque externo, la amenaza se extiende rápidamente a toda la red. El subneteo permite a los administradores de redes aislar las subredes mucho más fácilmente.

Referencias

- https://www.ionos.mx/digitalguide/servidores/know-how/subnetting-como-funcionan-las-subredes/
- https://www.profesionalreview.com/2020/02/29/ipv4-vs-ipv6/#IPv4_y_el_modelo_OSI
- https://www.profesionalreview.com/2018/11/22/modelo-osi/#Que_es_el_modelo_OSI