**Redes: Tema 6**

Direccionamiento a nivel de enlace de datos

Las redes WAN utilizan enlaces punto a punto para comunicar todos sus nodos, formando así una topología irregular. Estos nodos (router, switch…) comunican dos equipos, uno a cada extremo.

La mayoría de redes LAN utilizan Internet como red troncal debido a su bajo coste y simplicidad

Debido a esto los protocolos de bajo nivel de las redes LAN y WAN son bastante diferentes

* Cuando un mensaje es enviado, este permanece en el medio hasta ser recogido por el receptor por lo que todas las otras estaciones conectadas a la red pueden “ver” el mensaje. Solo el nivel de enlace de datos del equipo receptor puede recibir el mensaje. Por lo que es necesario un mecanismo que identifique los equipos entre sí.
* Las direcciones a nivel de enlace se identifican gracias a la dirección MAC
* Esta dirección MAC es la dirección física del adaptador, está formada por números binarios y está formada por 48 bits representados de manera hexadecimal. Los primeros 24 corresponden al fabricante y los 24 siguientes a cada adaptador, de esta manera cada dirección MAC es única.
* Existen direcciones MAC reservadas como la dirección MAC FF.FF.FF.FF.FF.FF es usada para la inundación de la red por lo que no puede ser usada por ningún fabricante
* Se puede obtener usando el comando “getmac” o para ver todo usar el comando “ipconfig/all”. También es posible acceder a ella a través del entorno gráfico
* Una dirección MAC equivale al nombre y apellido de una persona. En una casa pueden vivir varias personas, pero el cartero las puede identificar por su nombre y apellido

Direccionamiento a nivel de red

Facilita la localización del destinatario en la red por lo que se puede escoger el mejor camino. Coexiste con la dirección MAC

La dirección IP permite identificar a un dispositivo en la red más fácilmente. Este es un protocolo para enviar paquetes a través de redes heterogéneas (diferentes). El protocolo IP no está orientado a la conexión y no es del todo fiable por lo que se apoya en el protocolo TCP

* Las direcciones IP tienen un tamaño fijo de 32 bits (versión 4) ó 128 bits (versión 6)
* **IP V4**
* Las direcciones se pueden especificar en binario, pero es más cómodo y común hacerlo en decimal.
* Se representan como grupos de 8 bits de la siguiente manera:

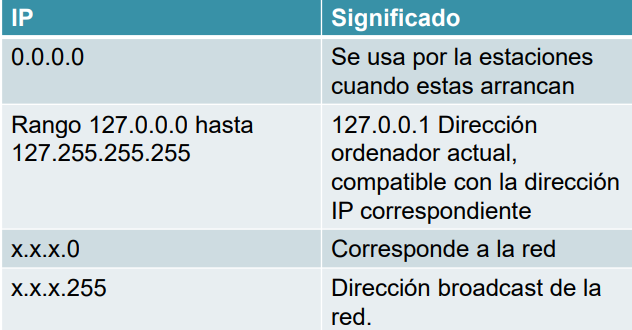
10001111010101100011110101100001 → 10001111.01010110.00111101.01100001

143.86.61.97

* De esta manera se pueden representar 232 direcciones únicas, aunque no se pueden usar todas
  + Tipo A: 8 primeros bits para la red y 24 para las estaciones por lo que se obtiene 256 redes distintas con 16 millones de equipos en cada red
  + Tipo B: 16 primeros bits para la red y 16 para las estaciones por lo que se obtienen 65536 de redes y equipos
  + Tipo C: 24 primeros bits para la red y 8 para las estaciones por lo que se obtiene 16 millones de redes distintas con 256 equipos por red



* No todas las combinaciones de IP pueden ser utilizadas, existe un gran número de rango las cuales están restringidas para un uso específico y no pueden ser utilizadas por dispositivos de red



* Un equipo se conecta al router mediante una dirección privada que solamente el router conoce (192.168.1.X) y el router es el único dispositivo de la red que realmente está conectado a internet, lo hace mediante una dirección pública (80.84.6.7) esto es lo que se conoce como protocolo NAT

NAT

Existen unas direcciones que se conectan a Internet gracias al protocolo NAT. Estas direcciones son privadas mientras que las direcciones en Internet son públicas y únicas

* Para la clase A se reserva la dirección de red 10.0.0.0
* Para la clase B se reserva desde 172.16.0.0 a la 172.31.0.0
* Para la clase C se reserva desde 192.168.0.0 a la 192.168.255.0

Todas estas direcciones pueden ser utilizadas a la vez por distintas redes enmascaradas gracias a un router que utilice el protocolo NAT

Este router enmascara (sustituye) las direcciones privadas de la red por una dirección pública de tal manera que la dirección privada de la LAN queda ocultada a Internet. Además, el router es el encargado de llevar una tabla con los registros de los paquetes enviados en caso de respuesta de la otra red

Gracias al protocola NAT se aumenta la capacidad de direcciones IP disponibles ya que las direcciones privadas pueden repetirse infinitamente para cada red local. El uso de este protocolo también se puede denominar enmascarado y se puede configurar en los router y algunos equipos conectados a la red.

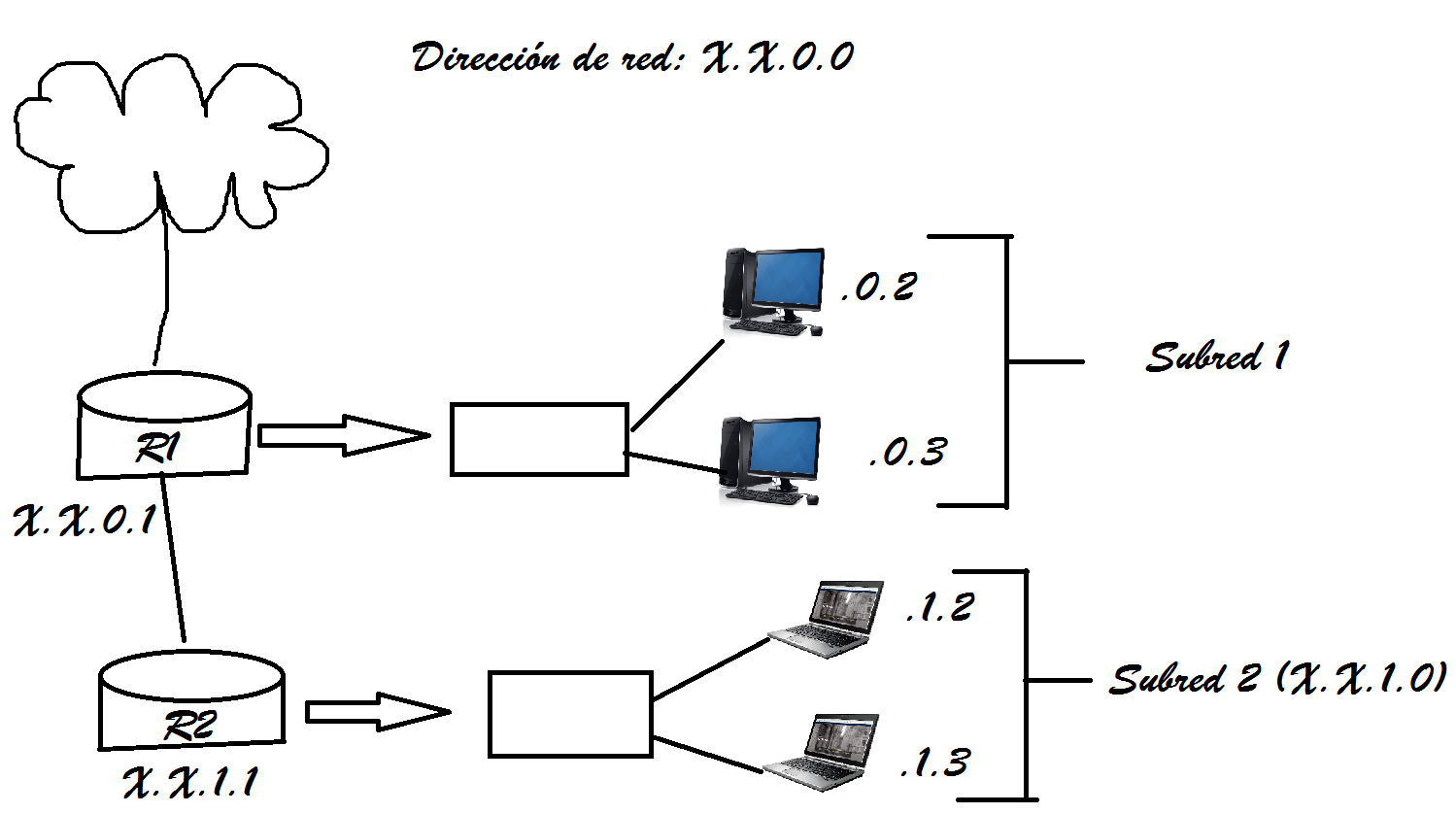
* Funcionamiento del protocolo NAT:
* Un equipo con dirección X.X.X.X quiere enviar un paquete al exterior con dirección Z.Z.Z.Z
* El primer paso el equipo manda el paquete a la red el cual es detectado por el router y determina si la red de destino pertenece a su propia red o es externa. Al ser externa enmascara la dirección privada X.X.X.X a una dirección pública Y.Y.Y.Y. Además, guarda toda esta información en una tabla local propia del router
* El destinatario recibe el paquete y contesta al emisor con otro paquete uwu???

Las direcciones IP clase A son también conocidas como /8, clase B como /16 y clase C como /24

Esto forma la máscara de red, el cual es un numero utilizado por la red para realizar una prueba lógica AND y conocer si una dirección pertenece a su red o es exterior.

Cada estación conectada a la red troncal (Internet) debe disponer de una IP única (IP pública). Los routers también asignaran direcciones únicas a los equipos conectados ya que ningún equipo ni ningún puerto puede tener más de una dirección asignada

**Asignar direcciones IP a los equipos de una red**

****

**IPv6**

Permite extender el rango de direcciones IP y otros problemas como las redes de clase B, ya que para las empresas una red de clase A es muy grande y una clase C muy pequeña por lo que se agotan

* Utiliza el algoritmo RIPing
* Contiene miles de millones de estaciones únicas
* Se simplifica la configuración de estaciones
* Reduce el tamaño de las tablas de encaminamiento
* Permite mayor velocidad de procesamiento ya que el formato solo tiene siete campos en su cabecera ¿?
* Es compatible con IPv4

La IPv6 está formada por 128 bits, siguiendo las siguientes reglas

* 8 grupos de 16 bits cada uno, representados en hexadecimal
* Se pueden suprimir los 0 consecutivos usando “::”
* Notación mixta ¿?

Una dirección IPv6 también tiene varios campos: un prefijo que indica el tipo dirección, el número de red y el número de estación

* El protocolo DHCP permite asignar IP automáticamente a las estaciones sólo cuando la necesitan. Este protocolo es utilizado en las redes LAN y los ordenadores conectados a ella deberán solicitar una dirección a un ordenador especial dedicado como servidor DHCP

Es un protocolo abierto por lo que puede ser utilizado por cualquier SO

Es posible que existan varios servidores de DHCP en una red y para que no existan conflictos cada uno tendrá un rango de direcciones único.

Direccionamiento a nivel de transporte

Una de las funciones del nivel de transporte es la multiplexación, es decir compartir varias conexiones utilizando una única conexión de red. Esto nos permite diferenciar las diferentes aplicaciones (formatos) de comunicaciones “si es un paquete de correo, encriptado…)

En la arquitectura TCP/IP existen dos protocolos que gestionan este direccionamiento

* TCP: para conexiones fiables por lo que es un diseño complejo. Destinado para redes de clase C)
* UDP: no lleva control de errores por lo que solo añade una cabecera a la dirección IP y es sencillo de implantar

Cada dirección TCP está formada por 16 bits situados al final de la dirección IP. Esto se llama puerto. Existen tres tipos de puertos

* Puertos bien conocidos: Entre 1 y 1023. Tienen una función bien definida por la ICANN. Son utilizados por el SO o programas con privilegios
* Puertos registrados: Son usados de forma temporal por los programas. Son bien conocidos, pero no registrados oficialmente
* Puertos dinámicos o privados: Utilizados de forma puntual por las aplicaciones para algo concreto y estos puertos carecen de significado fuera de este contexto

La dirección IP junto al puerto recibe el nombre de socket

Un puerto se dice que está abierto cuando un programa es el encargado de controlar las comunicaciones a través de ese puerto ¿?

Direccionamiento a nivel de aplicación

No existen direcciones a nivel de aplicación

Existe un protocolo denominado DNS (Domain Name System) el cual define direcciones de dominio y las traduce a direcciones binarias de transporte, es decir, el socket (IP + puerto)

Están formadas por unas extensiones que hacen referencia a países u organizaciones

Coordinación entre los distintos niveles

* Entre nivel de enlace y nivel de red
  + Protocolo ARP: Relaciona la dirección IP con la MAC. Primero intenta encontrar la dirección en una tabla local. En caso de no encontrarse la dirección realizará un broadcast a la MAC de difusión de la IP del destinatario. De este modo sólo el equipo con esa IP contesta al broadcast y responde con sus direcciones MAC de este como el emisor conoce las MAC de esa estación y la guarda en la tabla.

1. Comprobación tabla local
2. Envío solicitud ARP → MAC de difusión
3. Se añade la entrada a la tabla
4. Envío de respuesta ARP
5. Se añade la entrada a la tabla

Este protocolo también es usado por los routers y puentes para transmitir una trama de una red a otra

El Protocolo RARP asocia una MAC a una IP, es decir, realiza el proceso inverso. Lo realiza consultando en la tabla o bien enviando mensajes de difusión

* Entre nivel de transporte y nivel de aplicación

Los servidores DNS almacenan información relativa a los dominios, toda esta información constituye una zona que está definida por un conjunto de dominios o subdominios. Esta información está estructurada en forma de registros de recursos con el fin de utilizar las zonas de DNS de una manera eficiente en cuanto a tráfico, velocidad, etc…

Todo equipo accede a un servidor DNS primario, pero además será necesario un servidor de DNS secundario en caso de fallo. Pueden existir infinitos DNS secundarios, pero solo un servidor DNS primario.