Tema 4 REPRESENTACIÓN Y CODIFICACIÓN BINARIA

Representación posicional de magnitudes

Sistema de numeración: Conjunto de símbolos y reglas que permiten representar datos numéricos.

Los sistemas actuales son posicionales (cada símbolo tiene un valor según la posición que ocupa)

- Decimal (0-9) → potencia de base 10
- Binario (0-1) → potencia de base 2
- Hexadecimal (0-F)

<table>
<tr><th>TCP/IP</th><th>OSI</th></tr>
<tr><td rowspan="3">CAPA APLICACIÓN</td><td>CAPA APLICACIÓN</td></tr>
<tr><td>CAPA PRESENTACIÓN</td></tr>
<tr><td>CAPA SESIÓN</td></tr>
<tr><td>CAPA TRANSPORTE</td><td>CAPA TRANSPORTE</td></tr>
<tr><td>CAPA INTERNET</td><td>CAPA RED</td></tr>
<tr><td rowspan="2">CAPA ACCESO A LA RED</td><td>CAPA ENLACE DE DATOS</td></tr>
<tr><td>CAPA FÍSICA</td></tr>
</table>

TEMA 5 SUBNETTING Y DIRECCIONAMIENTO IP

1. INTRODUCCIÓN

La capa de red/internet/ip es la que acepta y transfiere paquetes para la red

En esta capa se incluye el Protocolo de Internet (IP), el Protocolo de Resolución de Direcciones (ARP) y el Protocolo de Mensajes de Control de Internet (ICMP)

- Protocolo IP: Encamina los paquetes/datagramas a su destino final.
  Para hacerlo necesita una dirección IP
  - Identifica un ordenador en concreto y la red a la que pertenece
  - El sistema de direcciones IP es un sistema jerárquico
  - Dirección única a nivel mundial que la concede INTERNIC(Centro de información de la Red Internet)
    - Las asignaciones son hasta 18/10/98
    - Después asignadas por ICANN

2. PREFIJOS BINARIOS EQUIVALENCIAS

La principal confusión que se produce al utilizar los prefijos a la hora de representar cantidades de almacenamiento de datos. En el **SI los prefijos están basados en potencias de 10**, mientras que en el contexto **binario, están basados en potencias de 2**.

Para solucionar este problema, la **Comisión Electrotécnica Internacional (IEC)**, creó en 1998 los llamados prefijos binarios.

3. SUBNETTING/ DIRECCIONAMIENTO IP

3.1. CLASES DE DIRECCIONES

Las direcciones IP tienen una estructura jerárquica y están divididas en dos partes:

- Netid: Indica la red
- Hostid: indica el host/equipo

Cuando un router recibe un mensaje/datagrama compara la parte de la red con sus tablas (suelen contener solo direcciones de red) y lo envía por la interfaz correspondiente.
Dependiendo del número de bits que se utilicen para indicar la red o el equipo, hay diferentes tipos de direcciones de red.

- Red Clase A
    - Netid → primer octeto (8 bits)
    - Hostid → 3 últimos octetos (24 bits)
    - Cantidad máxima hosts → $2^{24} - 2(Direcciones\ de\ red\ y\ broadcast)$
    - Bits iniciales: 0
    - Intervalo: 0.0.0.0 - 127.255.255.255
- Red Clase B
    - Netid → 2 primeros octetos (16 bits)
    - Hostid → 2 últimos octetos (16 bits)
    - Cantidad máxima hosts → $2^{16} - 2(Direcciones\ de\ red\ y\ broadcast)$
    - Bits iniciales: 10
    - Intervalo: 128.0.0.0 - 191.255.255.255
- Red Clase C
    - Netid → 3 primeros octetos (24 bits)
    - Hostid → último octeto (8 bits)
    - Cantidad máxima hosts → $2^{8} - 2(Direcciones\ de\ red\ y\ broadcast)$
    - Bits iniciales: 110
    - Intervalo: 192.0.0.0 - 223.255.255.255

Máscara de red: Consiste en poner todos los bits de la red a 1 y todos los bits del host a 0, para indicar que parte de la dirección pertenece a la red y que parte al host.

3.2. DIRECCIONES ESPECIALES

- Dirección de red: Indica la red, **Hostid a 0**
- Dirección de broadcast: Para envíos broadcast a toda la red. **Hostid a 1**
- Dirección loopback: Todas las direcciones IPs devuelven a la dirección de orígen los datagramas enviados a esta dirección (127.0.0.0)

3.3. DIRECCIONES PRIVADAS

Las siguientes direcciones de red están reservadas para redes privadas(intranets) por el RFC1918

Clase	Rango
A	10.x.x.x
B	172.16.x.x - 172.31.x.x
C	192.168.x.x - 192.168.255.x

3.4. SUBREDES

- Dominio de colisión: Parte física de la red donde las tramas pueden colisionar (interferir) con otras.
    - Los hub no dividen dominios de colisión pero los routers y los switches si.
- Dominio de difusión o broadcast: Área en la que un pc conectado a la red puede transmitir directamente a cualquier otro en el dominio sin necesidad de dispositivo de encaminamiento

4. SEGURIDAD

Uno de los aspectos más importantes a la hora de asegurar la red es la arquitectura de red

Arquitectura de red: Diseño de la red en la que se emplean unos determinados componentes, con finalidad de canalizar, permitir o denegar el tráfico con los elementos apropiados.

Elementos básicos:

- Router:
    - Equipo que permite o deniega las comunicaciones entre dos o más redes
    - Debe estar especialmente protegido
    - Puede ser un dispositivo o un servidor que actúe como router
- Red Interna
    - Red interna de la empresa donde se encuentran los equipos y disp internos
    - Se puede dividir en varias redes para permitir o denegar el tráfico de una red a otra
- Zona neutra / red perimetral
    - Red añadida entre dos redes para dar mayor protección a una de ellas
    - Suelen estar en los servidores de la empresa
    - Su objetivo principal es aislar una posible intrusión y que no tenga acceso a la red interna

4.1. ESQUEMA DE RED BÁSICO

Es la configuración más simple y consiste en el uso de un router para comunicar la red interna con la empresa de internet.

Esta arquitectura es la más sencilla de configurar pero la más insegura ya que toda la seguridad reside en el router.

Si se quiere tener un servidor ofrezca servicios a internet hay que ponerlo dentro de la red interna.

4.1. ESQUEMA DE RED CON ZONA NEUTRA

Zona desmilitarizada (DMZ) / Red perimetral: Red local que se coloca entre la red interna de la empresa y una red externa (generalmente internet).

- Permite conexiones desde la red interna a la red externa.
- No permite conexiones a la red interna.
- Los equipos de la DMZ no deben conectarse directamente con la red interna.
- Las conexiones que se hacen desde la red externa hacia la DMZ se controlan usando PAT(Port Address Translation).

La **DMZ** se utiliza para **colocar servidores** que necesitan ser accedidos desde fuera **(Correo, web y DNS).**

4.1. REDES INALÁMBRICAS

Requisitos para poder considerar una red inalámbrica como segura:

- Aislar la red inalámbrica de la red interna con una zona neutra.
- Confinar ondas de radio todo lo posible.
- Cifrar los datos utilizando protocolos de encriptación:
    - WEP
        - Basado en el algoritmo RC4 .
        - Clave de 40 o 104 bits + IV de 24 bits.
    - WPA
        - Corrige los fallos de WEP.
        - Utiliza un servidor de autenticación (RADIUS).
        - Cada usuario tiene su clave.
        - Usa algoritmo RC4 .
        - Clave de 128 bits + IV de 48 bits.

- Autenticación en doble vía.
- Filtrado de dirección MAC .

5. CONFIGURACIÓN DE ROUTERS

5.1. TABLAS DE ENRUTADO

Tabla de enrutado/ directiva de firewall: Guarda las acciones que hay que realizar sobre los mensajes que recibe el router para redirigirlos a su destino.

- Encaminamiento clásico
    - Encaminan paquetes en la dirección de destino que aparece en la cabecera del paquete.
    - Reglas:
        - Permitir un equipo de nuestra red.
        - Permitir cualquier equipo de nuestra red .
        - Permitir cualquier equipo de nuestra red.
        - Permitir un equipo de otra red.
        - permitir cualquier equipo de otra red.

- Encaminamiento regulado (Actual gracias a la llegada de QoS)
    - Interfaz: Interfaz de red por donde se recibe la información.
    - Origen/Destino: Origen y destino del mensaje.
    - Protocolo: Permite o deniega acceso a los puertos.
    - Seguimiento: Indica si el router tiene que hacer un seguimiento de por donde pasa un mensaje.
    - Tiempo: Espacio temporal en el que es válida la regla
    - Autenticación de usuarios: Si el usuario tiene que estar autenticado o no.
    - Acción: Indica la acción que tiene que realizar el router:
        - Aceptar: Deja pasar la info .
        - Denegar: No deja pasar la info.
        - Reenviar: Envía un paquete a una dirección IP.

5.2. ELEMENTOS DE CONFIGURACIÓN DE UN ROUTER

Usamos firewalls(FW) para asegurar la red. Los más utilizados son:

- FireWall 1 de CheckPoint
- Private Internet Exchange(PIX) de Cisco System
- IOS Firewall Feature Set de Cisco System
- Firewall del núcleo de Linux, Iptables
- Enterprise Firewall de Symantec
- Internet Security and Acelerador (ISA Server) de Microsoft

Los elementos más utilizados a la h de realizar la tabla de enrutado son:

- Interfaz
- Dirección de origen y destino
- Puerto
- Acción que debe realizar el router

A la hora de indicar la dirección de origen o la dirección de destino es importante usar la máscara de red para indicar la cantidad de ordenadores

Durante el filtrado de paquetes se aplica la regla de **coincidencia total**.

- Todos los criterios tienen que coincidir con el paquete entrante,
- Si no se cumplen no se aplica la regla pero no se rechaza el paquete

Las formas de implementar filtros de paquetes más usadas son:

- Construir reglas de las más específicas a la más general
- Las reglas más usadas primero

5.3. CREACIÓN DE UNA TABLA DE ENRUTADO

Tabla de enrutado: Conjunto de reglas que sirven como medida de seguridad para ver si se deja pasar un paquete o no

Las dos funciones claves del nivel de red hacen uso de la tabla de enrutamiento(TE)

- Enrutamiento: Modifica su contenido
- Reenvio: Consulta la tabla y saber por la interfaz que hay que reenviar una R_PDU

Tanto los sistemas finales como los routers tienen tabla de enrutamiento

Una TE tiene como mínimo:

- Red: Identificador de red
- Próximo salto: Dirección de nivel 3 del router del próximo salto
- Interfaz: Interfaz de red de salida

PDU: Unidad de datos de protocolo

- Estructura de información
- Definida en cada capa de la pila de protocolos
- Se transmite a la entidad par en otro sistema remoto
- Puede ser de **datos** o de **control**
- Estructura PCI + SDU
    - PCI: Información de control del protocolo(cabeceras)
        - Lógica desde la perspectiva del correspondiente protocolo de comunicación
    - SDU: Unidad de datos de servicio
        - Datos desde la perspectiva del correspondiente protocolo de comunicación
        - PDU de la capa inmediatamente superior
- Límites de tamaño
    - El servicio no impone límites al tamaño de la SDU
    - La especificación del protocolo puede poner límites de tamaño a la PDU

Cómo rellenar una tabla de enrutamiento

Se suele incluir una entrada especial que es la ruta por defecto, que se utiliza cuando no existe una entrada específica para una red.

- Automáticamente
- Manualmente
- Dinámicamente

Protocolos típicos de Internet

- RIP (Routing information Protocol)
    - Intercambia info de las redes del IP a la que está conectado
    - Calcula la ruta más corta posible a partir del nº de saltos
    - Máx 15 saltos (16 = ruta inalcanzable / no deseada)
    - Protocolo libre
- EIGRP : Cisco System
- OSPF(Open Shortest Path First)
    - Encaminamiento jerárquico de pasarela interior (IGP)
    - Usa el algoritmo Dijkstra
    - Construye una base de datos enlace-estado (LSDB) en todos los routers
- BGP (Border Gateway Protocol)
    - Intercambia información entre sistemas autónomos