

MODULO 2 – Introducción TCP/IP

Un **protocolo de red** es un conjunto de reglas y estándares que permiten la comunicación entre dispositivos dentro de una red. Los protocolos definen cómo se transmiten, reciben y procesan los datos, asegurando que los dispositivos puedan entenderse y trabajar juntos independientemente de su hardware o software.

Aquí tienes una tabla con diferentes protocolos y sus características:

Protocolo	Características	Ventajas	Desventajas
NetBEUI	<ul style="list-style-type: none">- Diseñado por IBM y utilizado por Microsoft.- No enrutable (solo para redes pequeñas locales).- Alta velocidad en redes pequeñas.	<ul style="list-style-type: none">- Simple de configurar.- Ideal para redes pequeñas con bajo tráfico.	<ul style="list-style-type: none">- No soporta redes grandes ni enrutamiento.- Obsoleto en la mayoría de los sistemas actuales.
AppleTalk	<ul style="list-style-type: none">- Diseñado por Apple para redes Macintosh.- Compatible con diferentes tipos de medios físicos.- Automático en configuración de red.	<ul style="list-style-type: none">- Fácil de usar en entornos Apple.- Soporte nativo para dispositivos Apple.	<ul style="list-style-type: none">- Baja escalabilidad en redes grandes.- Poco usado fuera del ecosistema Apple.
IPX/SPX	<ul style="list-style-type: none">- Desarrollado por Novell para NetWare.- IPX: Protocolo de red; SPX: Protocolo orientado a conexión.	<ul style="list-style-type: none">- Rápido en redes locales.- Bajo consumo de recursos.	<ul style="list-style-type: none">- Poco eficiente en redes modernas con alta carga de tráfico.- Reemplazado por TCP/IP.
TCP/IP	<ul style="list-style-type: none">- Protocolo estándar para redes modernas.- Arquitectura basada en capas (modelo TCP/IP).- Enrutamiento eficiente entre redes.	<ul style="list-style-type: none">- Escalable y soportado ampliamente.- Compatible con Internet y redes modernas.	<ul style="list-style-type: none">- Complejo en su configuración inicial en redes grandes.- Más consumo de recursos comparado con protocolos simples.

Si necesitas información más detallada sobre algún protocolo o ejemplo de su uso, ¡avísame! 😊

40

Tú dijiste:

creame una tabla con las capas de tcp/ip y su utilidad y protocolos en cada una de ellas

ChatGPT Plus

ChatGPT

Aquí tienes una tabla que describe las capas del modelo TCP/IP, su utilidad y los principales protocolos que operan en cada una:

Capa	Utilidad	Protocolos principales
Aplicación	<ul style="list-style-type: none">- Proporciona servicios y aplicaciones para el usuario final.	<ul style="list-style-type: none">- HTTP, HTTPS, FTP, SMTP, IMAP, POP3, SNMP, DNS, Telnet, SSH

Capa	Utilidad	Protocolos principales
Transporte	- Traduce datos al formato adecuado para ser enviados.	
	- Garantiza la entrega confiable de datos entre aplicaciones en distintos dispositivos.	- TCP (conexión confiable)
Internet	- Divide los datos en segmentos y controla errores.	- UDP (sin conexión, menor latencia)
	- Responsable del direccionamiento lógico y el enrutamiento de datos entre redes.	- IP (IPv4, IPv6), ICMP, ARP, RARP, IGMP
Acceso a la red	- Agrupa datos en paquetes.	
	- Maneja la transmisión física de datos a través de la red.	- Ethernet, Wi-Fi (IEEE 802.11), PPP, ATM, Frame Relay
	- Incluye protocolos de enlace y hardware.	

Este modelo organiza los procesos de red en capas funcionales que trabajan juntas para garantizar una comunicación eficiente y confiable. Si necesitas ejemplos de cómo se implementan estos protocolos o más detalles, ¡puedes pedírmelo! 😊

40

Tú dijiste:

¿Qué es una dirección IP? ¿para qué sirve? ipv4 tipos de redes ABC

ChatGPT Plus

ChatGPT

¿Qué es una dirección IP?

Una **dirección IP (Internet Protocol)** es un identificador único asignado a cada dispositivo conectado a una red que utiliza el Protocolo de Internet. Esta dirección permite que los dispositivos se identifiquen entre sí y se comuniquen en una red local o a través de Internet.

¿Para qué sirve una dirección IP?

1. **Identificación:** Distinguir un dispositivo en una red.
2. **Ubicación:** Prover información sobre la ubicación lógica del dispositivo dentro de la red.
3. **Comunicación:** Facilitar el envío y recepción de datos entre dispositivos.

IPv4 y tipos de redes (Clases A, B, C)

El **IPv4 (Internet Protocol versión 4)** utiliza direcciones de 32 bits, representadas en un formato de 4 números decimales separados por puntos (por ejemplo, 192.168.1.1).

El espacio de direcciones IPv4 se divide en clases según el rango de la dirección, con diferentes tamaños y propósitos:

Clase	Rango de direcciones	Nº de redes posibles	Nº de hosts por red	Uso principal
A	0.0.0.0 a 127.255.255.255	128	~16,777,216	Grandes redes (corporaciones, instituciones).

Clase	Rango de direcciones	Nº de redes posibles	Nº de hosts por red	Uso principal
B	128.0.0.0 a 191.255.255.255	16,384	~65,536	Redes medianas (empresas grandes).
C	192.0.0.0 a 223.255.255.255	2,097,152	~256	Redes pequeñas (hogares, oficinas).

Características adicionales:

- **Privadas:** Direcciones reservadas para redes internas (no enroutables en Internet).
 - Clase A: 10.0.0.0 – 10.255.255.255
 - Clase B: 172.16.0.0 – 172.31.255.255
 - Clase C: 192.168.0.0 – 192.168.255.255
- **Públicas:** Direcciones accesibles desde Internet, asignadas por autoridades como IANA.

¿Te gustaría profundizar en cómo funcionan o cómo se asignan estas direcciones? 😊

40

Tú dijiste:

puedes darme los valores de las redes clase a b y c por los primeros bits del primer byte

ChatGPT Plus

ChatGPT

Claro, los valores de las redes Clase A, B y C en función de los primeros bits del **primer byte** de una dirección IPv4 son los siguientes:

Clase	Primeros bits (en binario)	Rango del primer byte (en decimal)	Propósito
A	0xxx xxxx	0 a 127	Redes grandes (organizaciones globales).
B	10xx xxxx	128 a 191	Redes medianas (instituciones, empresas grandes).
C	110x xxxx	192 a 223	Redes pequeñas (hogares, pequeñas oficinas).

Explicación de los primeros bits:

1. Clase A:

- El primer bit es siempre 0.
- Esto deja 7 bits restantes para identificar redes.
- Rango: 00000000 (0) a 01111111 (127).

2. Clase B:

- Los dos primeros bits son siempre 10.
- Esto deja 14 bits para identificar redes.
- Rango: 10000000 (128) a 10111111 (191).

3. Clase C:

- Los tres primeros bits son siempre **110**.
- Esto deja 21 bits para identificar redes.
- Rango: **11000000** (192) a **11011111** (223).

¿Te interesa saber más sobre las clases restantes (D y E) o algo relacionado con el direccionamiento? 😊

40

Tú dijiste:

qué es la máscara de red?

ChatGPT Plus

ChatGPT

¿Qué es la máscara de red?

La **máscara de red** es un número utilizado en redes IP para separar la parte de una dirección IP que identifica la **red** de la parte que identifica a los **hosts** (dispositivos) dentro de esa red.

La máscara de red se representa de manera similar a las direcciones IP, en formato decimal punteado (por ejemplo, 255 . 255 . 255 . 0) o en formato de longitud de prefijo (por ejemplo, /24).

¿Para qué sirve?

1. **Definir la red:** Permite identificar qué parte de la dirección IP corresponde a la red y qué parte al host.
2. **Segmentar redes:** Ayuda a dividir una red en subredes más pequeñas para mejorar la organización y el rendimiento.
3. **Enrutamiento:** Es utilizada por los routers para determinar si un paquete debe permanecer en la red local o ser enviado a otra red.

Ejemplo básico de una dirección IP y su máscara:

Supongamos que tenemos la dirección IP:

192 . 168 . 1 . 10

y la máscara de red:

255 . 255 . 255 . 0

- En binario, la máscara sería:
11111111 . 11111111 . 11111111 . 00000000

Esto indica que:

- **Parte de la red:** Los primeros 24 bits (192 . 168 . 1) identifican la red.
 - **Parte del host:** Los últimos 8 bits (10) identifican al dispositivo dentro de esa red.
-

Máscaras comunes según las clases de red:

Clase	Rango de IP	Máscara de red predeterminada	Prefijo
A	0.0.0.0 – 127.255.255.255	255.0.0.0	/8
B	128.0.0.0 – 191.255.255.255	255.255.0.0	/16
C	192.0.0.0 – 223.255.255.255	255.255.255.0	/24

Relación entre la máscara y el tamaño de la red:

La máscara determina cuántos hosts puede haber en una red:

- Más bits en la parte de red (**1s en la máscara**) → Menos hosts posibles.
- Más bits en la parte del host (**0s en la máscara**) → Más hosts posibles.

Por ejemplo:

- /24 (255.255.255.0): 256 direcciones totales (254 hosts, excluyendo la dirección de red y broadcast).
- /16 (255.255.0.0): 65,536 direcciones totales (65,534 hosts).

¿Quieres más ejemplos o detalles sobre cómo calcular subredes? 😊

40

Tú dijiste:

pero para qué sirve realmente la máscara de red para el enrutamiento. puedes darme ejemplo binario con el AND y equipo red 192.168.10.10 y 192.168.10.14. Luego con 192.168.10.10 8.8.8.8

ChatGPT Plus

ChatGPT

¿Para qué sirve realmente la máscara de red en el enrutamiento?

La máscara de red permite a los dispositivos y routers determinar si dos direcciones IP están en la misma red o si necesitan enviar los datos a otra red a través de un router. Esto se hace utilizando la operación lógica **AND** entre la dirección IP y la máscara de red.

- Si el resultado de la operación AND para dos dispositivos coincide, están en la **misma red** y pueden comunicarse directamente.
 - Si el resultado es diferente, necesitan usar un router para comunicarse.
-

Ejemplo 1: 192.168.10.10 y 192.168.10.14

Datos:

- Dirección IP 1: 192 . 168 . 10 . 10
- Dirección IP 2: 192 . 168 . 10 . 14
- Máscara de red: 255 . 255 . 255 . 0 (o /24)

Paso 1: Convertir a binario

Dirección	Decimal	Binario
IP 1	192.168.10.10	11000000.10101000.00001010.00001010
IP 2	192.168.10.14	11000000.10101000.00001010.00001110
Máscara	255.255.255.0	11111111.11111111.11111111.00000000

Paso 2: Aplicar operación AND

- **IP 1 AND Máscara:**

```
scss
Copiar código
11000000.10101000.00001010.00001010
AND
11111111.11111111.11111111.00000000
=
11000000.10101000.00001010.00000000 (192.168.10.0)
```

- **IP 2 AND Máscara:**

```
scss
Copiar código
11000000.10101000.00001010.00001110
AND
11111111.11111111.11111111.00000000
=
11000000.10101000.00001010.00000000 (192.168.10.0)
```

Resultado:

Ambas IPs están en la **misma red (192.168.10.0)**, por lo que pueden comunicarse directamente sin necesidad de un router.

Ejemplo 2: 192.168.10.10 y 8.8.8.8

Datos:

- Dirección IP 1: 192.168.10.10
- Dirección IP 2: 8.8.8.8
- Máscara de red: 255.255.255.0 (o /24 para IP 1).

Paso 1: Convertir a binario

Dirección	Decimal	Binario
IP 1	192.168.10.10	11000000.10101000.00001010.00001010
IP 2	8.8.8.8	00001000.00001000.00001000.00001000
Máscara	255.255.255.0	11111111.11111111.11111111.00000000

Paso 2: Aplicar operación AND

- **IP 1 AND Máscara:**

```
scss
Copiar código
11000000.10101000.00001010.00001010
```

```
AND
11111111.11111111.11111111.00000000
=
11000000.10101000.00001010.00000000 (192.168.10.0)
```

- **IP 2 AND Máscara:**

```
SCSS
Copiar código
00001000.00001000.00001000.00001000
AND
11111111.11111111.11111111.00000000
=
00001000.00001000.00001000.00000000 (8.8.8.0)
```

Resultado:

Las redes son diferentes:

- IP 1 pertenece a la red **192.168.10.0**.
- IP 2 pertenece a la red **8.8.8.0**.

Por lo tanto, para que estas direcciones IP puedan comunicarse, es necesario utilizar un **router** que enrute los datos entre ambas redes.

Resumen del uso del AND:

1. **Determina si dos dispositivos están en la misma red o no.**
2. **Facilita el enrutamiento al identificar a qué red pertenece cada dirección.**

Si quieres más ejemplos o dudas sobre este tema, ¡puedes pedírmelo! 😊

40

Tú dijiste:

me puedes indicar que son las direcciones ip privadas? y el por qué?

ChatGPT Plus

ChatGPT

¿Qué son las direcciones IP privadas?

Las **direcciones IP privadas** son un rango específico de direcciones IP que no son accesibles directamente desde Internet. Estas direcciones están reservadas para su uso dentro de redes locales (LAN), como las de hogares, oficinas o empresas, y son definidas por la norma **RFC 1918**.

Los dispositivos en una red con direcciones privadas pueden comunicarse entre sí, pero para acceder a Internet, necesitan un dispositivo como un **router** que haga una traducción de direcciones de red (NAT, Network Address Translation).

Rangos de direcciones IP privadas

Clase	Rango de direcciones privadas	Máscara predeterminada
A	10.0.0.0 – 10.255.255.255	255.0.0.0 (/8)
B	172.16.0.0 – 172.31.255.255	255.240.0.0 (/12)
C	192.168.0.0 – 192.168.255.255	255.255.0.0 (/16)

¿Por qué existen las direcciones IP privadas?

1. **Conservación de direcciones IP públicas:**

El espacio de direcciones IPv4 es limitado, por lo que las direcciones privadas permiten que millones de dispositivos en redes locales utilicen las mismas direcciones sin agotar las públicas.

2. **Seguridad:**

Las direcciones privadas no son enroutables en Internet, lo que protege los dispositivos internos de accesos no autorizados desde el exterior.

3. **Facilita la administración de redes locales:**

Los administradores pueden reutilizar direcciones privadas en diferentes redes sin conflictos, lo que simplifica la configuración y la escalabilidad.

4. **Intermediación mediante NAT:**

Los routers traducen direcciones privadas a públicas cuando los dispositivos necesitan conectarse a Internet, ocultando la red interna y mejorando la seguridad.

Ejemplo práctico:

Supongamos una red doméstica:

- **IP privada de un dispositivo:** 192 . 168 . 1 . 10
 - **Red local:** Todos los dispositivos con direcciones como 192 . 168 . 1 . x pueden comunicarse directamente entre sí.
 - **Conexión a Internet:** El router tiene una **IP pública** (por ejemplo, 203 . 0 . 113 . 1) y utiliza NAT para permitir que los dispositivos privados accedan a Internet.
-

En resumen, las direcciones IP privadas son una solución fundamental para extender el uso de IPv4, mejorar la seguridad de redes internas y optimizar el acceso a Internet desde redes locales. Si necesitas más detalles sobre su uso o configuración, ¡puedes preguntarme! 😊

40

Tú dijiste:

qué es NAT? y para que sirve?

ChatGPT Plus

ChatGPT

¿Qué es NAT (Network Address Translation)?

El **NAT** (Traducción de Direcciones de Red) es una técnica utilizada en redes informáticas que permite modificar las direcciones IP en los paquetes de datos que transitan entre una red local (LAN) y una red externa (como Internet). Es implementado generalmente en routers o firewalls.

¿Para qué sirve NAT?

1. Conservar direcciones IPv4 públicas:

Permite que múltiples dispositivos en una red local (con IP privadas) compartan una única dirección IP pública para acceder a Internet. Esto es crucial debido a la limitada disponibilidad de direcciones IPv4.

2. Seguridad:

Oculta las direcciones IP privadas de los dispositivos en la red interna, lo que dificulta que usuarios externos accedan directamente a ellos.

3. Flexibilidad en redes privadas:

Facilita la reutilización de direcciones IP privadas dentro de redes locales, sin generar conflictos en Internet.

Tipos de NAT:

1. NAT estático:

Asigna una única dirección IP pública fija a una dirección IP privada específica. Es útil para servidores internos que necesitan ser accesibles desde Internet.

- Ejemplo: 192.168.1.10 (IP privada) ↔ 203.0.113.5 (IP pública fija).

2. NAT dinámico:

Asigna una dirección IP pública de un grupo (pool) a un dispositivo privado de manera temporal cuando este necesita acceso a Internet.

- Ejemplo: Varios dispositivos usan diferentes IP públicas según disponibilidad.

3. PAT (Port Address Translation o NAT sobrecargado):

Permite que múltiples dispositivos compartan una sola dirección IP pública mediante el uso de números de puerto.

- Ejemplo:
 - 192.168.1.10:12345 ↔ 203.0.113.1:80
 - 192.168.1.20:12346 ↔ 203.0.113.1:443
-

Ejemplo práctico de NAT:

Red local (LAN):

- Dirección IP privada del dispositivo 1: 192.168.1.10
- Dirección IP privada del dispositivo 2: 192.168.1.11

- Ambos necesitan acceder a Internet.

Router con NAT:

- IP privada del router (LAN): 192 . 168 . 1 . 1
- IP pública del router (WAN): 203 . 0 . 113 . 1

Funcionamiento:

1. El dispositivo 1 envía una solicitud para acceder a google . com.
 2. El router con NAT traduce la dirección privada (192 . 168 . 1 . 10) a su dirección pública (203 . 0 . 113 . 1) y lo envía a Internet.
 3. Cuando el servidor de Google responde, el router traduce la dirección pública de regreso a la privada y reenvía los datos al dispositivo correcto.
-

Ventajas del NAT:

- Conserva direcciones IP públicas.
- Mejora la seguridad al ocultar las direcciones privadas de la red interna.
- Compatible con redes que usan direcciones privadas.

Desventajas del NAT:

- Puede generar latencia adicional debido al proceso de traducción.
- Algunos protocolos que dependen de IP específicas pueden tener problemas (por ejemplo, algunos juegos en línea o aplicaciones de VoIP).

¿Quieres más ejemplos o una explicación más detallada? 😊

40

Tú dijiste:

qué son los puertos logicos y para qué sirven ?

ChatGPT Plus

ChatGPT

¿Qué son los puertos lógicos?

Los **puertos lógicos** son números asignados a las aplicaciones o servicios en un dispositivo de red para identificar y gestionar las comunicaciones a nivel de la capa de transporte del modelo TCP/IP. Estos puertos actúan como puntos de entrada o salida para datos que fluyen entre dispositivos, permitiendo que múltiples aplicaciones se ejecuten simultáneamente en un mismo dispositivo sin interferencias.

Los puertos lógicos se utilizan principalmente con los protocolos **TCP (Transmission Control Protocol)** y **UDP (User Datagram Protocol)**.

¿Para qué sirven los puertos lógicos?

1. Identificar servicios o aplicaciones:

Cada puerto lógico está asociado con un servicio o aplicación específica (por ejemplo, el puerto 80 para HTTP o el puerto 443 para HTTPS).

2. Gestionar conexiones simultáneas:

Permiten que un dispositivo maneje múltiples conexiones al mismo tiempo, diferenciándolas según el número de puerto.

3. Facilitar el enrutamiento interno de datos:

Cuando un dispositivo recibe un paquete, el número de puerto ayuda al sistema operativo a determinar qué aplicación o servicio debe procesar los datos.

4. Establecer seguridad:

Los firewalls y sistemas de seguridad utilizan los números de puerto para permitir o bloquear el tráfico según políticas definidas.

Tipos de puertos lógicos:

Los puertos se dividen en rangos, según su asignación y uso:

Rango	Descripción	Ejemplos
Puertos bien conocidos (0-1023):	Reservados para servicios y aplicaciones estándar reconocidos a nivel global.	- Puerto 80 (HTTP) - Puerto 22 (SSH)
Puertos registrados (1024-49151):	Usados por aplicaciones de usuario o servicios específicos que no están en el rango de los puertos bien conocidos.	- Puerto 3306 (MySQL) - Puerto 3389 (RDP)
Puertos dinámicos o privados (49152-65535):	Usados de forma temporal para conexiones cliente-servidor.	- Asignados automáticamente por el sistema operativo durante la conexión.

Ejemplo práctico:

Supongamos que un navegador web (cliente) quiere acceder a un sitio web (servidor):

1. El navegador envía una solicitud al servidor web en el puerto **80** (HTTP).
2. El sistema operativo del cliente asigna un puerto dinámico (por ejemplo, **50000**) para la conexión.
3. El servidor responde al cliente desde el puerto **80** hacia el puerto **50000** del cliente.
4. El cliente y el servidor usan estos números de puerto para comunicarse mientras dura la conexión.

Puertos comunes y su uso:

Puerto	Protocolo/Servicio
20, 21	FTP (Transferencia de archivos)
22	SSH (Acceso remoto seguro)

Puerto	Protocolo/Servicio
23	Telnet (Acceso remoto no seguro)
25	SMTP (Correo saliente)
53	DNS (Resolución de nombres)
80	HTTP (Navegación web)
443	HTTPS (Navegación segura)
3389	RDP (Escritorio remoto)

Resumen:

Los puertos lógicos son como "puertas virtuales" que permiten que las aplicaciones y servicios se comuniquen a través de la red. Gracias a ellos, los dispositivos pueden manejar múltiples conexiones simultáneamente y establecer reglas de seguridad más específicas.

¿Te interesa explorar cómo funcionan en aplicaciones específicas o en la configuración de un firewall? 😊