

# IP address

The identifier used in the IP layer of the TCP/ IP protocol suite to identify the connection of each device to the Internet is called the Internet address or IP address.

The IP address is the address of the connection, not the host or the router.

* IPv4

32-bit(8+8+8+8 bit)

0.0.0.0 ~ 255.255.255.255

* IPv6

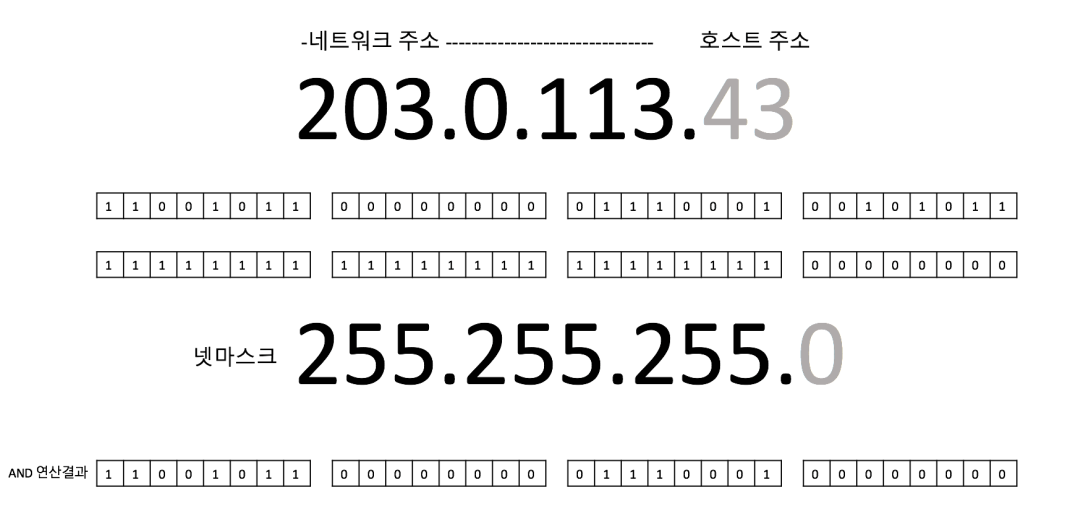
IPv4 주소의 수가 부족해지면서 등장

128-bit(32+32+32+32 bit)

# IP Address Class(IPv4)

1.Máscara de red

* La máscara de red es el reemplazo del bit en la dirección de red por 1.
* Puede obtener la dirección de red haciendo un AND con la dirección IP y la máscara de red.



**2. Máscara de subred**

**2.1 Tipo de máscara de subred**

El formato de la máscara de subred es un número binario de 32 bits idéntico a la dirección IP y se divide por 8bit(1byte)cada uno .(dot). En otras palabras, tiene la misma apariencia de OOO.OOO.OOO.OOO que IP. Sin embargo, el hecho de que sean de la misma forma no debe confundir los roles. La razón por la que son iguales es Y la dirección IP y la máscara de subred .

**2.2 Máscara de subred predeterminada**

Para comprender la máscara de subred, debe conocer la máscara de subred y la red de subred predeterminadas . De hecho, cuando dividimos IP en clases, queremos decir lo mismo que usar una máscara de subred. Lo que esto significa, por ejemplo, usar la clase C como es significa usar 2 ^ 8-2 ID de host que se pueden asignar a una red tal como está sin dividir la red de clase C, y esta 255.255.255.0es la máscara de subred predeterminada. . En otras palabras, `` La máscara de subred básica se aplica básicamente incluso sin crear una máscara de subred separada '' , y la dirección de red dividida por la máscara de subred predeterminada se denomina red de subred.

La siguiente tabla resume la máscara de subred predeterminada para cada clase de IP .

| **Una clase** | **Octeto 1** | **Octeto 2** | **Octeto 3** | **Octeto 4** |
| --- | --- | --- | --- | --- |
| Una clase IP (ejemplo) | 116 | 81 | 97 | 8 |
| Identificación de red | Identificación de red | Identificación de red | ID de host |  |
| Máscara de subred (/ 8) | 255 | 0 | 0 | 0 |

| **Clase B** | **Octeto 1** | **Octeto 2** | **Octeto 3** | **Octeto 4** |
| --- | --- | --- | --- | --- |
| IP de clase B (ejemplo) | 171 | 47 | 154 | Uno |
| Identificación de red | Identificación de red | Identificación de red | ID de host |  |
| Máscara de subred (/ 16) | 255 | 255 | 0 | 0 |

| **Clase C** | **Octeto 1** | **Octeto 2** | **Octeto 3** | **Octeto 4** |
| --- | --- | --- | --- | --- |
| IP de clase C (ejemplo) | 214 | 175 | 213 | 51 |
| Identificación de red | Identificación de red | Identificación de red | ID de host |  |
| Máscara de subred (/ 24) | 255 | 255 | 255 | 0 |

Si observa la forma de la máscara de subred predeterminada, solo los bits de la parte de red se reemplazan por 1. **La máscara de subred predeterminada también se puede denominar máscara de red.**

**Lo /24mismo después de la dirección IP significa** el **número de bits en la máscara de subred** . Si los 8 bits del octato son 1, se convierte en 255 en decimal, por lo que / 24 significa que el número de 1 bit enumerado desde la izquierda es 24. Por lo tanto, 192.168.0.3/24 significa que la dirección IP es 192.168.0.3 y la máscara de subred es 255.255.255.0.

**2.3. Diferencia entre máscara de red y máscara de subred**

En realidad, antes de conocer la máscara de subred, el objetivo que quería estudiar era

* ¿Qué es una máscara de red?
* ¿Qué es la subred de una IP con máscara de red?
* ¿Cuál es la dirección de transmisión de una subred?
* ¿Cuáles son las diferentes formas de representar una dirección IP con la máscara de red?

Eran cuatro cosas.  
La palabra "máscara de subred" no aparece en ninguna parte, pero cuando busqué en Google la máscara de red, solo salió información sobre la máscara de subred, así que estaba muy confundido. Mientras estudiaba la máscara de subred, parecía que no había mucha diferencia con la definición de la máscara de red, así que decidí si la máscara de subred predeterminada era una máscara de red, pero luego vi accidentalmente [este artículo](https://kldp.org/node/127933) y agregué esta sección.

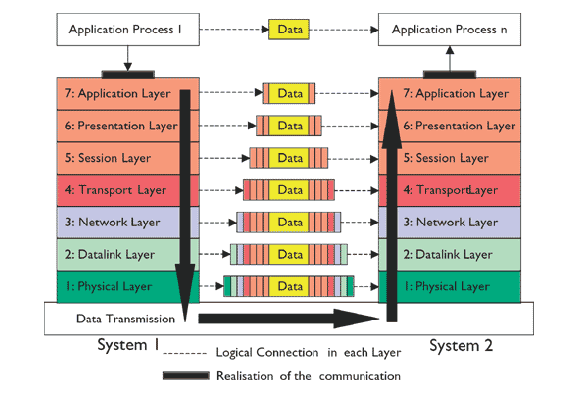
En conclusión, se dice que en estos días no hay distinción entre máscara de red y máscara de subred. Esto se debe a que después de CIDR (actualmente) solo se utiliza la máscara de subred.

**3. División en subredes**

La razón por la que estudiamos las máscaras de subred es para colocar esa máscara directamente en la dirección IP 서브넷팅. Qué es la división en subredes ... Me esforcé por resumir en la [próxima publicación](https://velog.io/@hidaehyunlee/%EC%84%9C%EB%B8%8C%EB%84%B7%ED%8C%85subnetting%EC%9C%BC%EB%A1%9C-%EB%84%A4%ED%81%AC%EC%9B%8C%ED%81%AC%EB%A5%BC-%ED%9A%A8%EC%9C%A8%EC%A0%81%EC%9C%BC%EB%A1%9C-%EA%B4%80%EB%A6%AC%ED%95%98%EC%9E%90) .

**SISTEMA OSI**

Conceptos OSI que debe conocer



Como puede ver en la primera figura de OSI, cada vez que los datos bajan de la aplicación a la capa física, cada capa envuelve los datos, que es un encabezado delante de los datos. Por ejemplo, en la tercera capa de la red, el encabezado tiene la dirección IP de destino, y en la capa física inferior, el encabezado está lleno de señales eléctricas convertidas en dígitos binarios 0 y 1 que la computadora entiende. por uno, sube a la capa de aplicación. Ahí es cuando termina la entrega de datos. Como referencia, la razón por la que la velocidad de la red es más lenta de lo indicado es debido a este paquete. Cuando cada capa que pasa a través de los datos originales se envuelve en un encabezado, los datos se vuelven más grandes, por lo que no se logra la velocidad de comunicación de red esperada.

¿Por qué nació OSI 7 Layer (Layer)?

En un lugar llamado ISO (Organización Internacional de Normalización), que es una organización de estándares internacionales para la comunicación, el proceso de comunicación se divide en 7 pasos y se estandariza . Hay tres razones principales.

1. Puede ver el flujo de datos de un vistazo.

Es natural. Es fácil comprender el proceso de comunicación de un vistazo porque divide la capa de aplicación en la capa física para ver cómo fluyen los datos a medida que se realiza la comunicación.

2. Es fácil resolver problemas.

Dado que el proceso de comunicación está dividido en 7 pasos, es conveniente identificar la causa de la falla de comunicación comprendiendo si hay un problema en cada capa cuando ocurre un problema de comunicación.

3. Incluso si usa varios dispositivos, es compatible entre redes.

La compatibilidad del equipo de comunicación en red está garantizada porque incluso las empresas que utilizan equipos de red individualmente se comunican de manera diferente mientras observan la estandarización de la comunicación.

Orden de la capa OSI 7

***Capa inferior (física -> enlace de datos -> red) -> capa superior (transmisión -> sesión -> presentación -> aplicación)***

1. Capa física

Es la capa inferior. Transmisión de datos a través de cables de comunicación utilizando principalmente características eléctricas, mecánicas y funcionales.

La unidad de comunicación utilizada en esta capa es bit, que es el estado ON / OFF del estado eléctrico representado por 0 y 1.

¡Lo físico solo transmite datos! No me importa qué tan eficiente sea enviarlo, qué tipo de datos sean , si hay errores o no.

( Cables, repetidores, hubs, etc.)

Define reglas para las características mecánicas, eléctricas, funcionales y de procedimiento del medio de transmisión requerido para la conexión real y el corte entre dos dispositivos requeridos para la transmisión + ps.

-> RS-232C, etc.

-Capa fisica

-Los datos se transmiten a través de un cable de comunicación utilizando características eléctricas, mecánicas y funcionales.

-La unidad de comunicación utiliza 0 y 1 como bits

-Esta capa es simplemente responsable de la transferencia de datos, no le importa en absoluto cuáles son los datos y qué errores hay

-Los equipos representativos incluyen cables de comunicación y hubs.

2. Capa de enlace de datos

Una capa que gestiona los errores y los flujos de información transmitidos y recibidos a través de la capa física en lugar de la capa física, y ayuda a entregar información segura.

Por tanto, también tiene una función para encontrar errores en la comunicación y retransmitir datos. Puede comunicarse con la dirección Mac que

aprendió el otro día . La unidad de comunicación en esta capa es Frame

( puente, conmutador )

+ ps Permite la transmisión de información confiable y eficiente entre dos sistemas abiertos adyacentes.

-> Control de flujo, sincronización de cuadros, control de errores, control de secuencia

-> HDLC, LAPB, PPP, LLC, etc.

-Capa de enlace de datos

- \*\* Desempeña el papel de ayudar a entregar información basada en la dirección física \*\*

-La dirección física es la dirección MAC y la dirección única dada a la tarjeta LAN.

-Gestiona errores y flujo de información transmitida y recibida a través de la capa física

-Utilizando el método punto a punto

-Proporciona los medios funcionales y procedimentales necesarios para encontrar y corregir errores que puedan ocurrir en la capa física

3. Capa de red

La función más importante de la capa, la flor de la red, es entregar los datos a su destino de la manera más segura y rápida.

Normalmente esto se llama enrutamiento . Por lo tanto, la tarea principal de esta capa es seleccionar una ruta, establecer una dirección (IP ) y entregar paquetes a lo largo de la ruta .

Este papel lo desempeña un tipo llamado enrutador. En estos días, entre los conmutadores, está saliendo un conmutador con buen rendimiento con una función de enrutamiento, por lo que el conmutador también se denomina dispositivo de 3 capas.

( Enrutador, conmutador (con función de enrutador))

+ ps Gestión de conexiones de red entre sistemas abiertos (establecimiento, mantenimiento y desmantelamiento de conexiones de red) Intercambio y retransmisión de datos

-> Enrutamiento, control de tráfico, transmisión de información por paquetes

-> X 25, IP, etc.

-Capa de red

-Determinación de la ruta de datos desde el origen hasta el destino en función de la dirección lógica

-La forma más segura y rápida de enviar datos al destino → Enrutamiento o Protocolo de enrutamiento

-Dirección lógica → IP es representativa

4. Capa de transporte

Controla todos los mensajes entre el origen y el destino (de un extremo a otro) y gestiona los errores .

Asegura una comunicación confiable al verificar si la transmisión de paquetes es válida y reenviar el paquete fallido.

El protocolo representativo es TCP (Orientado a la conexión).

También es responsable del control de errores y control de flujo .

( Protocolo TCP, UDP, ARP )

( Puerta de enlace )

+ ps Permite la transmisión de datos transparente entre sistemas de un extremo a otro

-> Configuración de conexión de transmisión, transmisión de datos, función de desconexión

-> Configuración de direcciones, multiplexación, control de errores, control de flujo

-> TCP, UDP, etc.

-Capa de transmisión

- \*\* Capa para permitir la comunicación \*\*

-Determinación del método de transmisión de datos y distinción del número de puerto del servicio

-Los protocolos representativos que pertenecen a esta capa son TCP y UDP

5. Capa de sesión

Establece una conexión entre los puertos de capa que componen una sesión de comunicación.

Compruebe si la conexión del puerto entre usuarios es válida. Tiene jurisdicción sobre la conexión, el mantenimiento, la gestión y la terminación de los equipos de comunicación .

Mantener y conectar sesiones

+ ps Responsable de mantener la relación entre los lados emisor y receptor y controlar la conversación

-> Composición de conversación y control de sincronización, función de gestión de intercambio de datos

-Capa de sesión

- \*\* Responsable de la conexión lógica para la comunicación de datos \*\*

-Proporciona un método para el proceso de solicitud en ambos extremos para gestionar la comunicación

-Comprobar el proceso de apuntado, inactivo, apagado, reinicio, etc., junto con comunicación full-duplex, half-duplex y transmisión y recepción simultáneas (Duplex)

- \*\* La capa que crea y destruye sesiones TCP / IP \*\*

-> Checkpoint (= punto de sincronización): Se utiliza para recuperar datos con errores, y existen pequeños puntos de sincronización y grandes puntos de sincronización.

6. Capa de presentación

A través de la traducción necesaria y el trabajo en los datos de entrada y salida, los datos se transforman de manera consistente para que puedan entenderse y ser compatibles entre sí.

Convierte el formato para entenderse , como extensión (jpg, gif, mpg), codificación, decodificación, cifrado y descifrado .

( Protocolo JPEG, MPEG, SMB, AFP )

+ ps Una función que convierte los datos recibidos de la capa de aplicación para adecuarlos a la capa de sesión y los datos recibidos de la capa de sesión para adecuarlos a la capa de aplicación.

-> Conversión de código, cifrado de datos, compresión de datos, búsqueda de frases, formato de información (conversión de formato), función de gestión de contexto

-Capa de expresión

-Informa al método de expresión de datos para que la computadora pueda reconocer los datos creados en la 7ma capa.

-Una capa que indica cómo se expresan los datos, incluida la extensión de datos, como .txt o .jpg

-Admite \*\* cifrado y compresión \*\* a través de este

7. Capa de aplicación

Permite a los usuarios acceder a la red. Proporciona una interfaz de red y permite el acceso de los usuarios a los recursos de la red.

Capa expuesta a los usuarios al proporcionar servicios como el correo electrónico y la gestión de bases de datos.

( Telnet, HTTP, DHCP, DNS , SSH, SMTP, FTP, etc.)

Proveedores de servicio

+ ps Sirve aplicaciones de usuario para acceder al entorno OSI

-Capa de aplicación

-Proporciona interfaz y servicio de red a los usuarios con el fin de crear datos.

- \*\* Capa directamente en contacto con el usuario \*\*

-Proporciona una serie de funciones según el tipo de red que desee realizar el usuario

-Representativamente DNS, DHCP, HTTP, FTP, SSH, Telnet, etc.

Conceptos OSI que debe conocer

Como puede ver en la primera figura de OSI, cada capa envuelve los datos cada vez que los datos pasan de la aplicación a la capa física.

Puede pensar en ello como un encabezado con datos como prefijo. Por ejemplo, en la tercera capa de la red, la dirección IP de destino se adjunta al encabezado, y en la parte inferior de la capa física, el encabezado está lleno de señales eléctricas convertidas en números binarios 0 y 1 entendidos por la computadora.

Ahora, la PC que ha recibido los datos bien empaquetados abre el paquete uno por uno y lo eleva a la capa de aplicación. Ahí es cuando termina la entrega de datos.

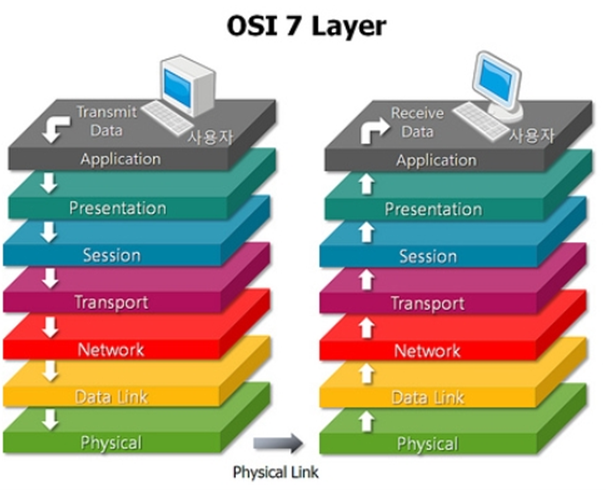
Como referencia, la razón por la que la velocidad de la red es más lenta que la velocidad indicada se debe a este trabajo de empaquetado. Cuando cada capa que pasa a través de los datos originales se envuelve en un encabezado, los datos se vuelven más grandes, por lo que no se logra la velocidad de comunicación de red esperada.

SISTEMA OSI 7 CAPAS

-Conocer el flujo de datos → Es fácil comprender el flujo general a través de la función de cada capa

-La resolución de problemas se vuelve más fácil → Es posible identificar dónde ha ocurrido el problema clasificándolo por jerarquía.

-Estandarización → En los primeros días de la red, cada empresa de equipos utilizaba diferentes protocolos, pero a través del modelo OSI, se utilizó el mismo protocolo y la comunicación entre otras empresas se hizo posible.



## 4. Modelo OSI de 7 capas

El modelo OSI 7 es un modelo de referencia estándar de la industria que divide el proceso de comunicación de red en '7 capas'. En los primeros días de la red, debido a que cada computadora tenía un sistema diferente, apareció un modelo estándar que podía comunicarse sin cambiar lógicamente el hardware y el software.

El modelo de referencia OSI consta de 7 capas, como se muestra en la figura anterior.

Qué es una PDU

La capa 7 de OSI da importancia al concepto de PDU, y una unidad de datos de proceso (PDU) es una unidad transmitida por cada capa. En la capa 1, es fácil pensar que una PDU es un bit, pero no se llama PDU, y un bit no es una unidad, sino un flujo de señales eléctricas. Las PDU son de capa 2 tramas, capa 3 paquetes , 4 Solo necesita pensar en segmentos jerárquicos. Para comprender en profundidad el proceso de comunicación de la red, es necesario saber por qué la PDU de cada capa es diferente y conocer su función.

### Capa 1: Capa física

La capa física pertenece a la capa más baja del modelo OSI y desempeña la función de transmitir señales eléctricas a otros sistemas a través de medios físicos (concentrador, enrutador, cable, etc.) para los datos transmitidos desde la capa superior.

En otras palabras, el lenguaje de la máquina se convierte en una señal eléctrica y se carga en el cable.

-PDU: Bit

-Protocolo: Módem, Cable, Fibra, RS-232C

-Equipo: Hub, Repetidor

### Capa 2: Capa de enlace

La capa de enlace sirve para transmitir datos entre dispositivos de red. Para una transmisión de datos sin errores entre sistemas, los paquetes se configuran como "tramas" y se transmiten a la capa física. Recibe información de la capa 3 y agrega información de dirección y control al encabezado y al final.

-PDU: Marco

-Protocolo: Ethernet, MAC, PPP, ATM, LAN, Wifi

-Equipo: puente, interruptor

### Capa 3: Capa de red

La capa de red es responsable de establecer la ruta del datagrama en el dispositivo. La ruta óptima se selecciona utilizando un algoritmo de enrutamiento y se transmite desde el lado de envío al lado de recepción. En este momento, los datos transmitidos se dividen en unidades de "paquetes", se transmiten y luego se recombinan. La capa 2 supervisa la entrega de nodo a nodo, mientras que la capa 3 asegura que cada paquete se entregue de manera exitosa y efectiva a su destino.

-PDU: paquete

-Protocolo: IP, ICMP, etc.

-Equipo: enrutador, interruptor L3

### Capa 4: Capa de transporte

Desde el origen hasta el destino (de un extremo a otro), control y gestión de errores. Comprueba si la transmisión del paquete es válida y garantiza una comunicación fiable, como reenviar un paquete que no se ha podido transmitir, y se incluye un "segmento" en el encabezado. Se realizan el establecimiento de direcciones, el control de flujo y error y la multiplexación.

-PDU: Segmento

-Protocolo: TCP, UDP, ARP, RTP

-Equipo: Gateway, interruptor L4

### Capa 5: Capa de sesión

Una capa que configura una sesión de comunicación y se conecta según el número de "Puerto". Establecer, mantener y sincronizar interacciones entre dispositivos de comunicación. Realiza procesos de comprobación de apuntado, retardo, apagado y reinicio, junto con transmisión / recepción simultánea (dúplex), semidúplex y comunicación dúplex completo.

-Protocolo: NetBIOS, SSH, TLS

### Capa 6: Capa de presentación

La capa de presentación determina el "formato de datos" (png, jpg, jpeg ...) entre el lado de envío y el lado de recepción. Convierte los datos recibidos en el método estándar correcto mediante el proceso de conversión de código, búsqueda de sintaxis, cifrado y compresión.

-Protocolo: JPG, MPEG, SMB, AFP

### Capa 7: Capa de aplicación

La capa de aplicación está directamente conectada al usuario y es una capa que ayuda al software de aplicación. Recibe información del usuario, la entrega a la capa inferior y entrega los datos transmitidos desde la capa inferior al usuario.

Desempeña la función de conectar varios servicios de aplicaciones, como transferencia de archivos, base de datos y transferencia de correo a la red.

-Protocolo: DHCP, DNS, FTP, HTTP

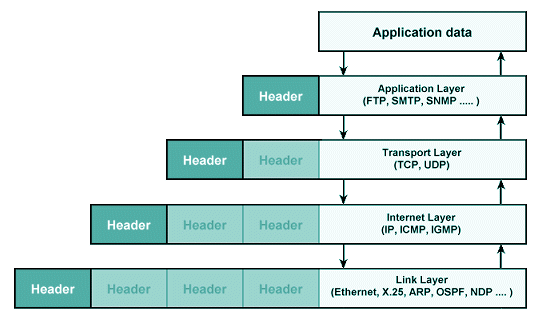
## 5. Modelo TCP / IP

Sin embargo, el modelo de referencia OSI es literalmente un modelo de referencia, y el protocolo de Internet real utilizado no sigue completamente la estructura de 7 capas. Actualmente, la pila de protocolos de Internet sigue principalmente a TCP / IP.

TCP / IP es una palabra compuesta de "TCP" e "IP", que desempeña los papeles más importantes entre los protocolos de Internet y administra el flujo de datos, verifica la precisión y garantiza el destino de los paquetes. \*\* TCP es responsable de verificar la precisión de los datos e IP es responsable de transmitir paquetes al destino.

> Capa 4 de TCP / IP A diferencia del modelo de referencia OSI, TCP / IP incluye tanto la capa de presentación como la capa de sesión en la capa de aplicación, pero de hecho, en una capa de aplicación del modelo TCP / IP, la aplicación, presentación, y se implementan capas de sesión. Es correcto entender que lo está haciendo.

Los datos se transmiten adjuntando un encabezado (Datos \*\* → \*\* Segmento \*\* → \*\* Datagrama \*\* → \*\* Marco) para cada paso como se muestra en la figura a continuación, y esto se denomina "encapsulación de datos".



**TCP/UDP**

## Protocolo de control de transmisión (TCP)

-Protocolo utilizado con IP para enviar datos en forma de mensajes en Internet

-Usualmente utilizado como TCP / IP

-IP no garantiza la entrega de paquetes y no gestiona el orden de envío y recepción de paquetes.

Para compensar las deficiencias de dicha IP, se utiliza TCP junto con IP.

-Si IP se encarga de reenviar paquetes, TCP comprueba si los paquetes han llegado correctamente o si están en el orden correcto.

-Método de conexión de circuito virtual, prestación de servicios de tipo de conexión

-Alta fiabilidad en seguridad

-Establecimiento de conexión (apretón de manos de 3 vías) y liberación (apretón de manos de 4 vías)

- [Apretón de manos de 3 vías y apretón de manos de 4 vías] (https://mindnet.tistory.com/entry/%EB%84%A4%ED%8A%B8%EC%9B%8C%ED%81%AC- % EC% 89% BD% EA% B2% 8C-% EC% 9D% B4% ED% 95% B4% ED% 95% 98% EA% B8% B0-22% ED% 8E% B8-TCP-3- WayHandshake-4-WayHandshake)

Apretón de manos de 3 vías al iniciar una conexión TCP

El protocolo de enlace de 4 vías es un procedimiento que se realiza para finalizar una sesión TCP.

-Control de flujo de datos y control de congestión

-Evita la situación en la que el búfer del receptor se desborda y evita el crecimiento excesivo de paquetes en la red

-Full-Duplex, método punto a punto

-Full-Duplex: también conocida como comunicación full-duplex, es un método en el que dos terminales usan líneas separadas para transmitir y recibir datos, y un método en el que los datos se transmiten a ambos lados al mismo tiempo.

-Punto a punto: Una estructura en la que ambos nodos o redes están conectados en un formato uno a uno durante la comunicación.

## Protocolo de datagramas de usuario (UDP)

-Protocolo que procesa datos en unidades de datagramas

-Un método en el que los datos son transmitidos unilateralmente por la parte emisora ​​sin pasar por ningún procedimiento de señalización al intercambiar información entre ellos

-La parte remitente no verifica que la parte receptora haya recibido los datos.

-Dado que es un servicio sin conexión, no hay ningún proceso para establecer y liberar una conexión.

-No hay función para controlar el flujo o reensamblaje asignando un orden a los paquetes, por lo que es más rápido que TCP y tiene menos carga de red.

-En cambio, no podemos garantizar una transmisión de datos confiable.

-Como servicio donde la continuidad es más importante que la confiabilidad, se utiliza principalmente para servicios en tiempo real.

-No hay control de flujo, por lo que es imposible verificar los paquetes

**DHCP**

## Protocolo de configuración dinámica de host (DHCP)

-En el protocolo TCP / IP, cada computadora debe tener una IP única para acceder a Internet.

-Al administrador de red se le asigna una dirección del ISP (Proveedor de servicios de Internet).

ISP (Proveedor de servicios de Internet): proveedores de servicios de Internet, empresas que brindan servicios de Internet como KT, LG Uplus y SK Broadband.

-El administrador de la red asigna y administra las direcciones IP a cada computador y host dentro del bloque de direcciones IP asignado.

-DHCP

- \*\* Gestiona automáticamente la asignación dinámica de IP → Esto se denomina arrendamiento de IP \*\*

### Configuración DHCP

-Servidor DHCP

-Cuando se recibe una solicitud de asignación de IP de un cliente, se asigna una IP y la gestión de la IP asignable está a cargo.

-Cliente DHCP

-Cuando el sistema se inicia, solicita la dirección IP de su sistema al servidor DHCP e inicializa la configuración de TCP / IP a través de él.

### 3 funciones de DHCP

-El DHCP tiene funciones de arrendamiento de IP y devolución de renovación

- alquiler

-Para prestar una IP a un cliente por un período específico

-Orden de asignación de IP DHCP

1. Descubrimiento de DHCP

-Pasos para que el anfitrión encuentre un servidor DHCP

-Dado que el host no conoce la dirección del servidor DHCP al que se conectará, transmite a todos los nodos de la subred para encontrar un servidor DHCP.

2. Oferta DHCP

-El servidor DHCP envía un mensaje proporcionado por el servidor al cliente

-El mensaje proporcionado por el servidor incluye la dirección IP del cliente, el nombre de dominio, el período de arrendamiento de la dirección IP (tiempo válido), etc.

-Este proceso también se transmite a todos los nodos de la subred porque no se conoce el host de envío.

3. Solicitud de DHCP

-Después del descubrimiento de un servidor DHCP, se envía un mensaje de solicitud DHCP al host después de seleccionar el servidor óptimo.

4. DHCP Ack

-El servidor envía un mensaje ACK al mensaje de solicitud DHCP como confirmación.

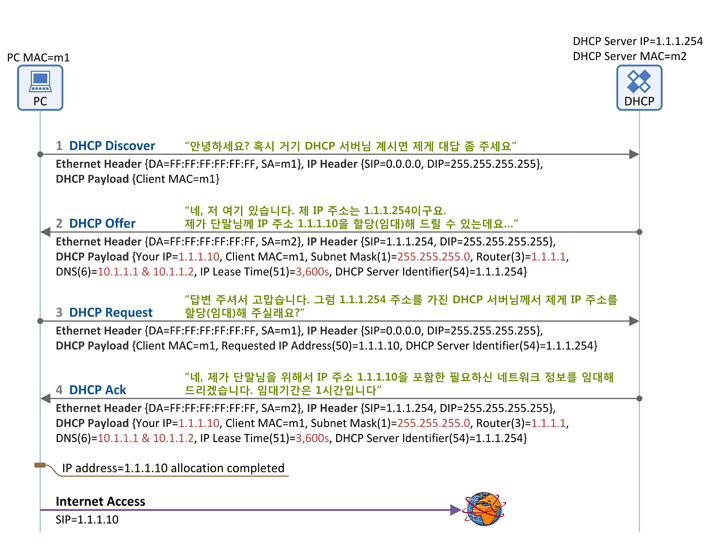
### Ventajas y desventajas de DHCP

- ventajas

-En caso de una gran cantidad de PC o muchos cambios en la propia PC, la configuración de IP se establece automáticamente y la asignación de IP es automática, por lo que se pueden evitar los conflictos de IP.

- Desventajas

-Como depende del servidor DHCP, si el servidor está inactivo, la asignación de IP no se realiza correctamente.



# DNS (Sistema de nombres de dominio)

-Sería difícil recordar si tuviéramos que escribir los sitios que usamos con direcciones IP.

-Un sistema que convierte dichas direcciones IP en dominios como [www.google.com] (http://www.google.com) para una fácil identificación

-Cuando ingresa un dominio en la barra de direcciones, el servidor busca una IP adecuada para ese dominio.

**Enroutamiento/Puertos**

Enrutamiento / Puerto

## 1.1. El concepto de enrutador

Un enrutador es un dispositivo que permite que las computadoras conectadas a una LAN utilicen Internet al mismo tiempo a través de una línea alquilada. Transmite datos a un destino. También proporciona una función de retransmisión que conecta dos o más redes diferentes e intercambia datos entre ellas. . La mayoría de los enrutadores tienen funciones de enrutamiento IP, así como funciones de puente como IPX y AppleTalk, que son protocolos LAN.

En otras palabras, un enrutador es un dispositivo que transmite paquetes a través de otras redes mientras administra una red IP y una subred, y el enrutamiento puede verse como un proceso de selección de una ruta para enviar el paquete.

## 1.2. Cómo funciona el enrutador

El enrutador utiliza la "tabla lan", la "tabla de red" y la "tabla de enrutamiento" para determinar la ruta de transmisión del paquete. Al administrar las tres tablas anteriores, el enrutador reconoce las direcciones de todos los dispositivos conectados a la red, incluidos los dispositivos conectados a otras redes, y determina la ruta de transmisión de paquetes basándose en esto.

Al enviar un paquete a un dispositivo en la misma red, el enrutador sigue los siguientes pasos cada vez.

1. Compruebe la 'tabla LAN'. Aquí, verifica si el destino del paquete está en la misma red o en una red diferente.

2. Examine la "tabla de red" para encontrar la dirección de red a la que se entregará el paquete.

3. Busque en la "Tabla de enrutamiento" para encontrar la ruta más adecuada y envíe el paquete.

-Tabla LAN

La tabla LAN administra las direcciones de los dispositivos en el segmento LAN conectados al enrutador y se utiliza para el filtrado.

-Mesa de red

Almacena las direcciones de todos los enrutadores de la red y se utiliza para identificar el enrutador de destino del paquete.

-Tabla de ruteo

Está integrado en cada enrutador y mantiene información en cada ruta, por lo que se utiliza para determinar la ruta más eficiente de los paquetes transmitidos a otros segmentos.

## 1.3. Cómo saber el destino del enrutador

### 1) Conectado

Averigua automáticamente la dirección IP del dispositivo que está conectado directamente \*\* físicamente \*\*. En este momento, la IP se almacena en la tabla de enrutamiento como una dirección de red.

### 2) Estático

Configuración enviada por el administrador seleccionando una ruta de enrutamiento directamente.

-Ventajas: Es el más eficiente para la gestión de rutas ya que el administrador establece directamente la ruta a la que se transmitirán los datos.

-Desventajas: Manejo lento de cambios en la red.

### 3) Dinámico

La información de cada enrutador se comparte entre sí y se almacena en la tabla de enrutamiento. Es un método para mantener la información de la tabla de enrutamiento calculando visualmente la ruta óptima.

-Ventajas: Respuesta rápida a cambios en la red.

-Desventajas: El consumo de recursos (uso de CPU) aumenta porque la ruta debe calcularse periódicamente.

### 4) Redistribución

Un método en el que el gerente intercambia por la fuerza dispositivos que no intercambian información.

# ¿Qué es una puerta de enlace predeterminada para el enrutamiento?

-La comunicación es posible sin un enrutador en la red interna

-Al comunicarse, primero se busca en la red interna para encontrar el destino, si no existe tal cosa, se busca el destino desde la red externa a través de la puerta de enlace predeterminada.

- \*\* Puntos de acceso a otras redes \*\*

-Básicamente, el primer anfitrión posible

# ¿Qué es un puerto desde el punto de vista de IP y para qué se utiliza cuando se conecta a otro dispositivo?

## Puerto

-El punto final de la comunicación del sistema operativo.

-Se siente como un enchufe para conectar con otros equipos externos

-El puerto se compone básicamente de 0 ~ 65535

-Puedes acceder al programa de una computadora específica usando la dirección IP y el puerto.

Ingrese una URL o dirección IP si queremos conectarnos a un servidor específico.

Esto lo llevará a la computadora donde se encuentra el servidor en Internet según la URL o IP.

Sin embargo, en la mayoría de las computadoras, se ejecutan varios programas al mismo tiempo,

Tienes que decirle a tu computadora a cuál de estos programas quieres acceder.

¡aquí! \*\* El número de puerto le dice a la computadora a qué programa acceder. \*\*

`La dirección IP representa la dirección necesaria para encontrar una computadora, y el puerto representa cuando se busca un programa en la computadora`

## \*\* PUERTO conocido \*\*

¡Finalmente, quiero hablar sobre el PORT bien conocido!

El puerto consta de un total de 0 ~ 65535. Y se divide en gran medida en tres tipos.

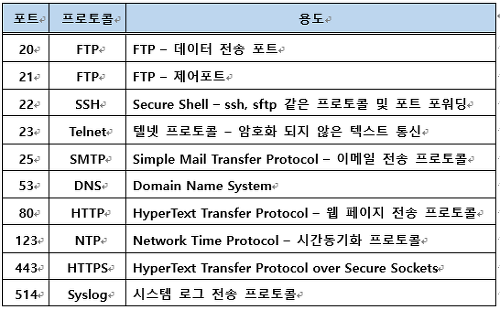
0 a 1023: puerto conocido, puerto conocido

1024 a 49151: puerto registrado, puerto registrado

49152 ~ 65535: puerto dinámico, puerto dinámico

Se clasifica en tres categorías, y el \*\* puerto conocido \*\* consta de números de puerto TCP y UDP asignados para un uso específico \*\*.

La siguiente figura resume los puertos utilizados con frecuencia entre los puertos conocidos.



ICMP / PING

## 10) ICMP (Protocolo de mensajes de control de Internet)

ICMP es un protocolo que informa o diagnostica problemas que ocurren al procesar paquetes IP en TCP / IP. ICMP es parte de la capa de red y se incluye en la parte de datos del datagrama IP y se entrega.

IP consiste solo en contenidos para llegar al destino del paquete. Por lo tanto, si llega al destino con normalidad, no hay problema ya que la comunicación es exitosa y termina en IP.

Sin embargo, si el host o enrutador de destino está apagado o no está conectado, es necesario informar al receptor de este paquete que existe tal problema, pero IP no especifica cómo lidiar con tales errores. Es ICMP que se utiliza para compensar esta falta de IP.

### ICMP Header

### https://www.notion.so/image/https%3A%2F%2Fs3-us-west-2.amazonaws.com%2Fsecure.notion-static.com%2Fe20bbb57-4d11-4488-8606-4610282afee3%2FUntitled.png?table=block&id=1f9229bb-480d-4ec9-8c6d-83ebc2524f9e&width=3840&userId=&cache=v2

### Usos de ICMP

### [1] Notificación de la fuente de la falla en la transmisión del datagrama IP (corresponde a los mensajes de informe de errores de ICMP)

### Cuando falla la transmisión de paquetes, notifica que se ha producido un error y notifica el contenido del error. Sin embargo, solo se envía cuando la fuente puede resolver el problema. El objetivo es evitar que se vuelvan a enviar paquetes incorrectos desde el lado de origen.

### \* En los siguientes casos, los mensajes ICMP no se envían a la fuente. \*

### → Si la cola que sirve para almacenar paquetes temporalmente en el enrutador está llena, el paquete se puede descartar de acuerdo con la política del enrutador. Dado que esto no es culpa de la fuente, el mensaje ICMP no se transmite.

### Los siguientes mensajes corresponden a los mensajes de informe de errores de ICMP.

### 1. \*\* Destino inalcanzable (tipo 3) \*\*

### Significa que no se puede llegar al destino. Está compuesto por varios códigos según el motivo.

### -Código 1 (Host inalcanzable): cuando el enrutador de última etapa no puede transmitir un paquete al host de destino

### -Código 2 (Protocolo inalcanzable): cuando el host de destino no puede utilizar un protocolo específico

### -Código 3 (puerto inalcanzable): cuando el puerto UDP correspondiente no está abierto en el host de destino (en el caso de TCP, si el puerto no está abierto, se devuelve un paquete TCP RST)

### -Código 4 (Se necesita fragmentación y no se configuró la fragmentación): cuando la fragmentación de un paquete IP es absolutamente necesaria, pero no se puede fragmentar porque el indicador No fragmentar en el encabezado IP está configurado, el enrutador lo devuelve.

### 2. \*\* Redirección (tipo 5) \*\*

### Este mensaje informa al waypoint anterior o al anfitrión de la nueva ruta debido a la ruta de enrutamiento incorrecta.

### 3. \*\* Source Quench (obsoleto) \*\*

### 4. \*\* Tiempo excedido (tipo 11) \*\*

### Este mensaje indica que se ha agotado el tiempo de espera y el paquete IP se ha descartado. El motivo del tiempo de espera se puede encontrar a través del código.

### -Código 0 (Tiempo de vida excedido en tránsito): este mensaje informa que el valor TTL se convierte en 0 antes de que el paquete IP llegue a su destino final, y el paquete ha sido descartado.

### -Código 1 (tiempo de reensamblado del fragmento excedido): mensaje que indica que se agotó el tiempo de espera durante el proceso de reensamblaje del paquete IP y que se descartaron todos los datagramas IP correspondientes. En general, cuando algunos fragmentos de un datagrama IP se pierden durante la transmisión, se debe a una falla en el proceso de recombinación.

### 5. \*\* Problema de parámetro (tipo 12) \*\*

### [2] Diagnóstico / entrega de información (correspondiente a los mensajes de consulta ICMP)

### El administrador lo utiliza para obtener información específica del enrutador o del host.

### PING

### Este mensaje confirma si es posible la comunicación con una dirección IP específica. Al hacerlo mediante el comando correspondiente, puede verificar el estado de respuesta, el tiempo de ida y vuelta, TTL y la tasa de pérdida de paquetes.

### Solicite con el mensaje ICMP tipo 8 y responda con el tipo 0.

### \*\* 1) ¿Qué es el tiempo de ida y vuelta? \*\*

### Tiempo (ms) que tardó en moverse desde el punto de inicio de la red al punto de destino y de regreso al punto de inicio

### \*\* 2) ¿Qué es TTL (tiempo de vida)? \*\*

### Es el tiempo establecido para existir en la red antes de que el enrutador descarte un paquete. \*\* Cada vez que el paquete pasa por el enrutador, el TTL disminuye en 1.

### La siguiente imagen es el resultado de hacer ping a [www.apple.com](http://www.apple.com).

### https://www.notion.so/image/https%3A%2F%2Fs3-us-west-2.amazonaws.com%2Fsecure.notion-static.com%2F2e058a61-01f5-47c6-b803-b32a0c9a1349%2FUntitled.png?table=block&id=8d7eed68-5f3b-4f1a-a6f0-e9fd133cde10&width=1870&userId=&cache=v2

### (BOMBILLA) El tiempo no se almacena en el paquete. El tiempo de ida y vuelta se calcula utilizando la diferencia entre el tiempo inmediatamente después de dejar la computadora y el tiempo en que regresó el mensaje.

### \*\* Tracert / Traceroute \*\*

### Devuelve una ruta de enrutamiento aproximada a una dirección IP específica. Tracert establece el TTL en 1 y transmite el paquete, luego el TTL se convierte en 0 en el siguiente enrutador y se devuelve un error ICMP. A continuación, TTL se establece en 2 y se envía el paquete. .... Y este es un método para transmitir paquetes mientras aumenta el TTL en uno al enrutador de destino. Dado que todos los enrutadores en la ruta en curso experimentan TTL 0, devuelven su dirección IP de enrutamiento a través de un error ICMP, y conocemos la ruta hasta que llegamos por esta. (Así que lleva mucho tiempo ..)

### https://www.notion.so/image/https%3A%2F%2Fs3-us-west-2.amazonaws.com%2Fsecure.notion-static.com%2Fb6e42354-d6a3-4832-8058-c3028bd1b4e2%2FUntitled.png?table=block&id=f85e94be-8d28-412c-b8d6-7708ccb7f648&width=3840&userId=&cache=v2

### Los siguientes mensajes corresponden a mensajes de consulta ICMP.

### 1. \*\* Eco (tipo 8) \*\*

### 2. \*\* Solicitud de enrutador y anuncio de enrutador \*\*

### 3. \*\* Marca de tiempo \*\*

### 4. \*\* Máscara de dirección \*\*

### (Si tiene curiosidad sobre el mensaje de Informe de errores y Consulta, encuéntrelo usted mismo)

### ### \*\* Datagrama Si el error ICMP no se envía incluso si hay un problema \*\*

### -Cuando es un error de mensaje de error ICMP

### -Cuando Checksum Error → Checksum Error no es un caso en el que la fuente pueda corregirse.

### -En caso de error de transmisión de multidifusión / difusión → Pueden transmitirse demasiados errores.

### -Cuando desde Source 0.0.0.0 → La interfaz aún no conoce la dirección IP (DHCP)

### -Cuando la fuente de IP eliminada llevaba un fragmento → No hay información en el encabezado del segundo fragmento y solo datos.