



GOBIERNO DE LA CIUDAD DE BUENOS AIRES

Ministerio de Educación

Dirección de Formación Técnico Superior

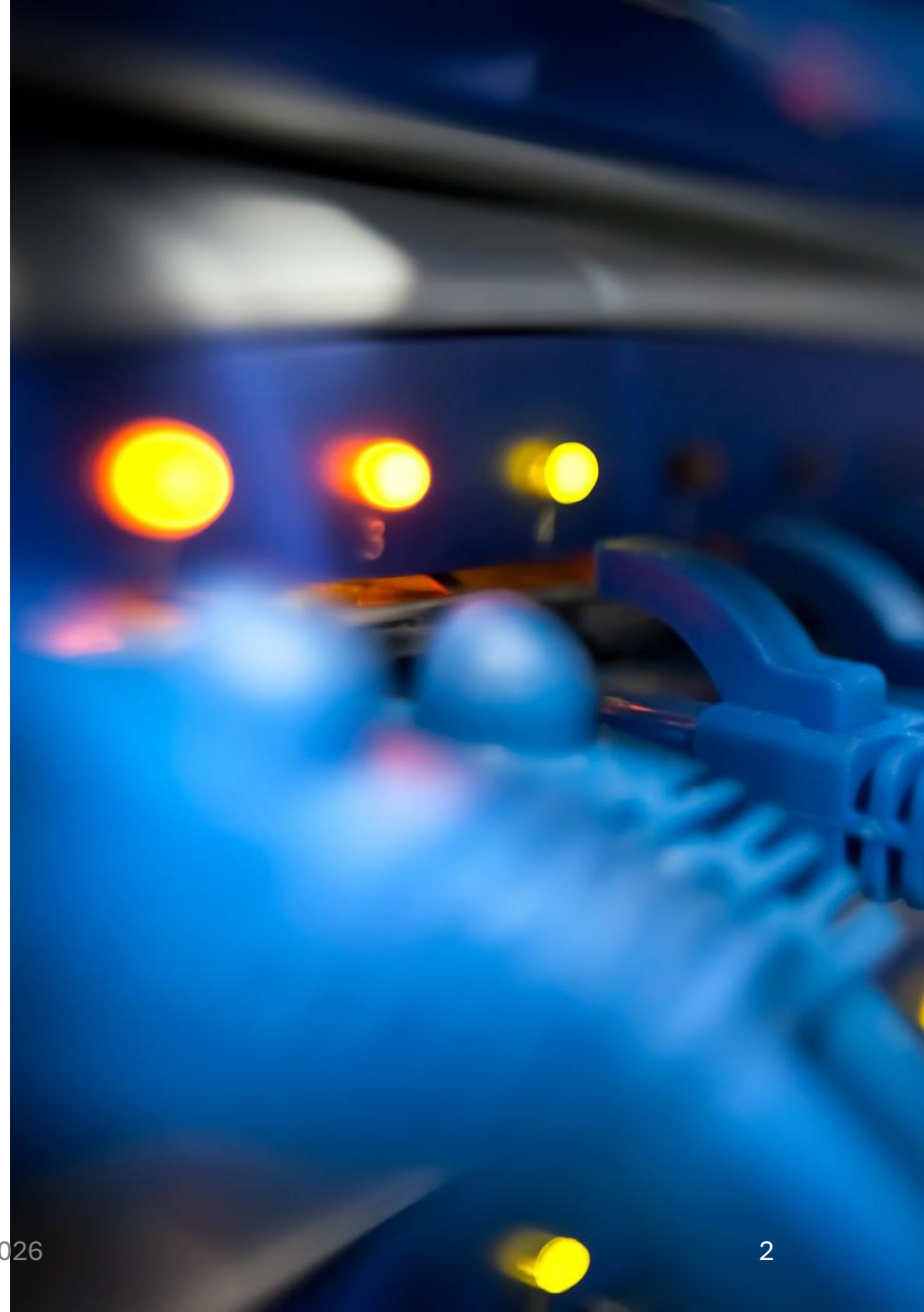
Instituto de Formación Técnico Superior N° 18

Mansilla 3643, (C1425BBW) Capital Federal

Arquitectura de sistemas en la Nube

TEMAS

- Servicio de DNS
- Servicio de DHCP
- ¿Qué es un Firewall?
- ¿Qué es una DMZ?
- ¿Qué es un Proxy?
- El modelo OSI
- Dirección IP
- Clases de Redes
- Subneteo
- NSG



Domain Name System (DNS)

- Él **DNS**, o Sistema de Nombres de Dominio, es un sistema que traduce nombres de dominio legibles por humanos (como `www.ejemplo.com`) en direcciones IP numéricas que son utilizadas por los dispositivos para comunicarse entre sí en Internet. Su función principal es facilitar la navegación y el acceso a servicios en línea sin necesidad de recordar cadenas de números.

Funciones del DNS:

1. **Resolución de nombres:** Convierte las solicitudes de nombres de dominio en direcciones IP que permiten a los navegadores acceder a sitios web.
2. **Distribución de carga:** Permite distribuir el tráfico entre varios servidores para mejorar el rendimiento.
3. **Facilitación de la movilidad:** Almacena información sobre los dispositivos en la red, lo que permite que los nuevos dispositivos obtengan una dirección IP y se conecten a la red de manera fácil.
4. **Gestión de correo electrónico:** Ayuda a dirigir el correo electrónico al servidor correcto a través de registros específicos.

Tipos de DNS:

- **DNS Autoritativo:** Contiene la información de dominio y responde a las consultas sobre los dominios que gestiona directamente.
- **DNS Recursivo:** Recibe las consultas de los clientes y realiza la búsqueda de la dirección IP correspondiente, consultando otros servidores DNS si es necesario.
- **DNS de Caché:** Almacena temporalmente las respuestas a las consultas DNS para mejorar la velocidad de resolución al evitar consultas repetidas.

Diferentes tipos de registros DNS:

- **A (Address Record):** Mapea un nombre de dominio a una dirección IPv4.
- **AAAA (IPv6 Address Record):** Mapea un nombre de dominio a una dirección IPv6.
- **CNAME (Canonical Name Record):** Permite que un dominio sea un alias de otro, redirigiendo las solicitudes a un nombre de dominio real.
- **MX (Mail Exchange Record):** Indica qué servidores de correo son responsables de recibir correo para el dominio.
- **NS (Name Server Record):** Especifica los servidores de nombres que son autoritativos para la zona del dominio.
- **TXT (Text Record):** Permite que los administradores de dominio añadan texto a sus registros; a menudo utilizado para verificación y políticas de email (como SPF).
- **SRV (Service Record):** Utilizado para definir servicios específicos disponibles en el dominio.

Un poquito más de DNS

- **Cache DNS:** Los servidores DNS y los equipos de los usuarios mantienen una caché local que almacena las respuestas a consultas DNS recientes. Esto mejora la velocidad y reduce la carga en la red al evitar consultas repetidas al servidor autoritativo.
- **Protocolo DNS:** Se utiliza para consultar y transferir información entre los servidores DNS y los clientes. La mayoría de las consultas se realizan sobre UDP, aunque también se puede usar TCP para transferencias de zona y respuestas grandes.

Flujo de consulta por DNS

- Cuando un usuario escribe un nombre de dominio en su navegador, el proceso de resolución DNS sigue estos pasos:
 1. El navegador consulta el DNS local para ver si ya tiene la dirección IP en la caché.
 2. Si no está en la caché, se consulta al servidor DNS recursivo.
 3. Si el servidor recursivo no tiene la dirección IP en su caché, envía una consulta al servidor raíz.
 4. El servidor raíz responde con los servidores TLD apropiados.
 5. El servidor recursivo consulta a uno de esos servidores TLD, que a su vez proporciona la dirección de los servidores autoritativos para el dominio.
 6. Finalmente, el servidor autoritativo proporciona la IP correspondiente al nombre de dominio, que se almacena en la caché del servidor recursivo y se devuelve al navegador del usuario.

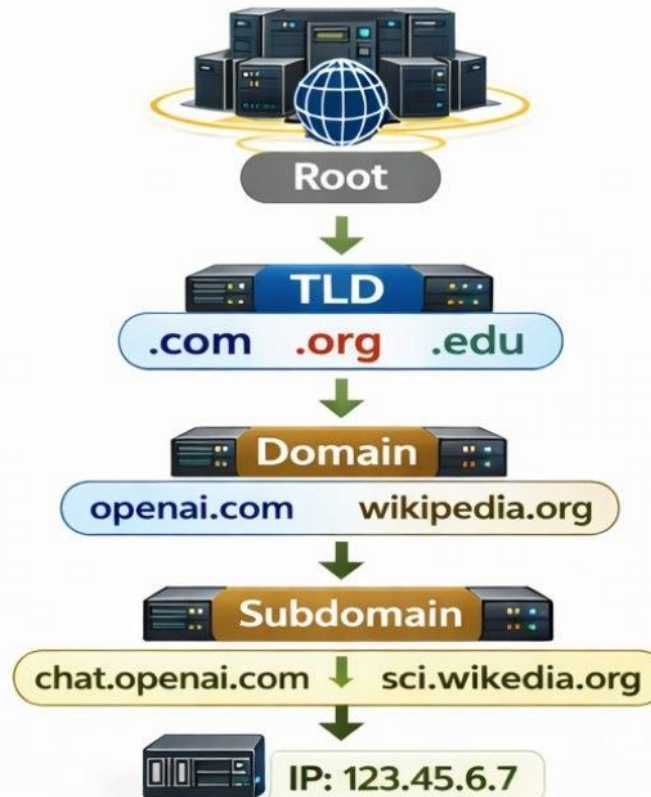
What is **DNS** hierarchy ?

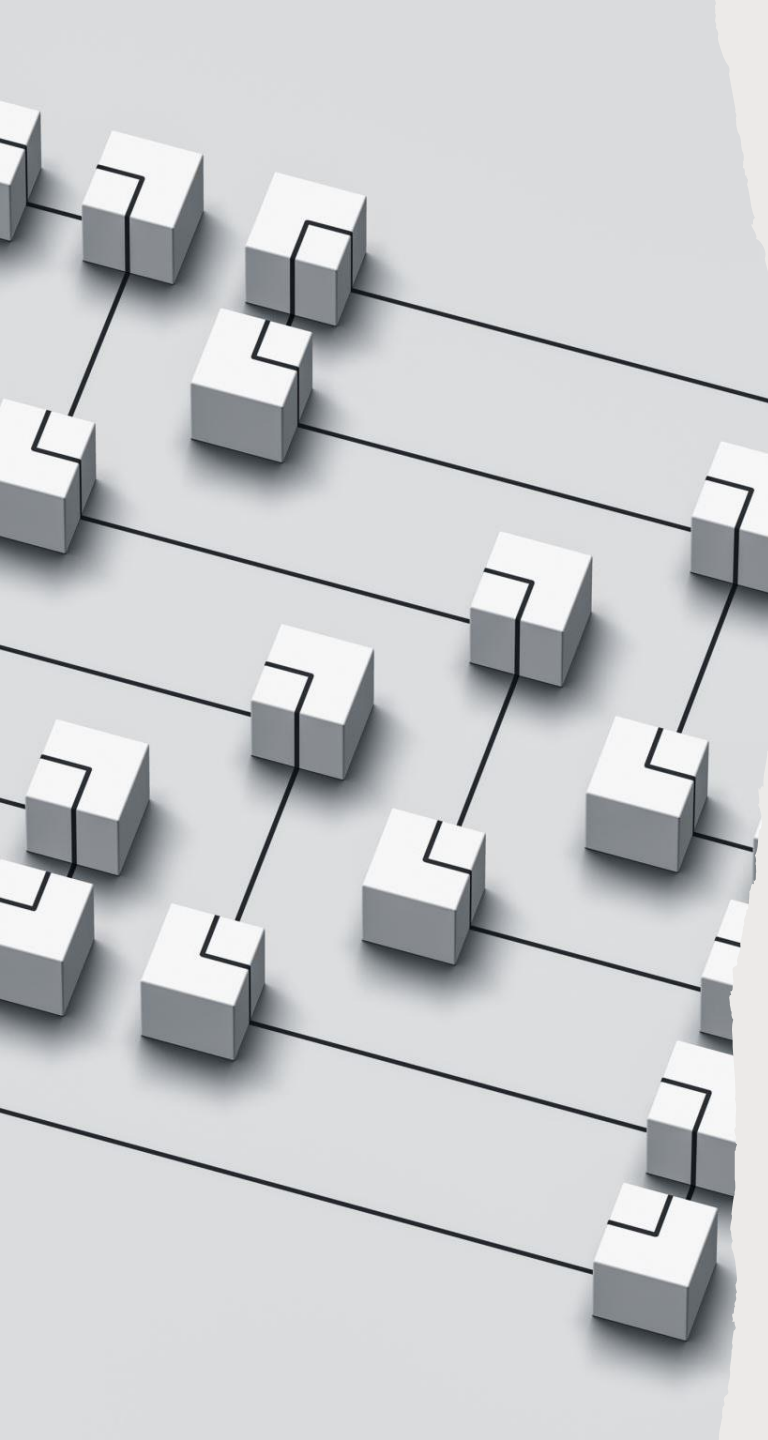
Answer: Root → TLD → Domain → Subdomain.



Explanation:

DNS queries move step by step until IP is found.





DHCP

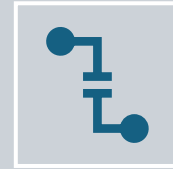
- El Protocolo de Configuración Dinámica de Host (Dynamic Host Configuration Protocol, en inglés), es un protocolo de red que permite a los servidores de red asignar direcciones IP y otros parámetros de configuración de manera automática a dispositivos (hosts) en una red. Esto facilita la administración de la red al evitar la necesidad de configurar manualmente las direcciones IP en cada dispositivo.
- DHCP es fundamental para la administración eficiente y simplificada de redes, especialmente en entornos donde muchos dispositivos se conectan y desconectan regularmente.

Función del DHCP

- La función principal del DHCP es la asignación dinámica de direcciones IP a dispositivos que se conectan a la red. Su funcionamiento incluye varios aspectos importantes:



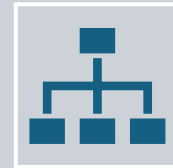
Asignación de Direcciones IP: Proporciona automáticamente una dirección IP única a cada dispositivo que se conecta a la red, evitando conflictos de direcciones.



Configuración de Parámetros de Red: Además de la dirección IP, el DHCP puede proporcionar otros parámetros de configuración, como la puerta de enlace predeterminada, la máscara de subred, los servidores DNS y otros detalles necesarios para la conexión a la red.



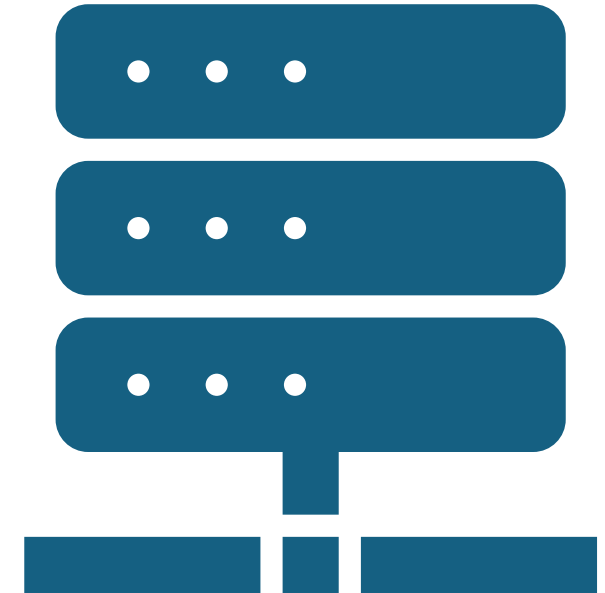
Gestión de la Alocaación: Mantiene un registro de las direcciones IP que ha asignado, lo que permite liberar las direcciones que ya no están en uso (por ejemplo, cuando un dispositivo se desconecta).



Simplificación de la Administración: Permite a los administradores de red gestionar de manera centralizada la configuración de los dispositivos de red.

Tipos de DHCP

1. **DHCP Estático:** En este caso, la dirección IP se asigna permanentemente a un dispositivo específico según su dirección MAC. Es útil para dispositivos que requieren una dirección IP fija, como servidores o impresoras.
2. **DHCP Dinámico:** Las direcciones IP son asignadas y liberadas dinámicamente a medida que los dispositivos ingresan y salen de la red. Las direcciones se mantienen en un rango definido y se reutilizan cuando los dispositivos se desconectan.
3. **DHCP de Relevó:** Esta configuración se utiliza en redes donde el servidor DHCP no está en la misma subred que los clientes que necesitan direcciones IP. Un relay DHCP ayuda a reenviar las solicitudes DHCP desde clientes a un servidor DHCP situado en otra subred.
4. **DHCPv6:** Este es la variante del protocolo DHCP diseñado para trabajar con direcciones IPv6. Proporciona funcionalidad similar al DHCP para redes que utilizan el protocolo IP de la próxima generación.



Funcionamiento General del DHCP

- El proceso de asignación de direcciones IP mediante DHCP sigue estos pasos:
 1. **Descubrimiento (DHCP Discover):** Cuando un dispositivo se conecta a la red, envía un mensaje DHCP Discover en busca de servidores DHCP disponibles.
 2. **Oferta (DHCP Offer):** Los servidores DHCP que reciben la solicitud responden con un mensaje DHCP Offer, que incluye una dirección IP disponible y otros parámetros de configuración.
 3. **Solicitud (DHCP Request):** El dispositivo selecciona una de las ofertas y envía un mensaje DHCP Request al servidor que hizo la oferta, indicando que acepta la configuración propuesta.
 4. **Confirmación (DHCP Acknowledgment):** El servidor DHCP responde con un mensaje DHCP Acknowledgment, confirmando la asignación de la dirección IP y otros parámetros al dispositivo.
- Este proceso de cuatro pasos se conoce como el "proceso DORA" (Discover, Offer, Request, Acknowledge) y asegura que cada dispositivo en la red tenga la configuración necesaria para comunicarse correctamente.



Firewall

- Un **firewall** (o cortafuegos) es una herramienta de seguridad que actúa como una barrera entre una red interna (como la red de una empresa o tu red doméstica) y una red externa (como Internet). Su propósito principal es controlar y filtrar el tráfico de red para prevenir accesos no autorizados y proteger la red interna de amenazas y ataques.
- Los firewalls pueden ser hardware, software, o una combinación de ambos. Funcionan siguiendo una serie de reglas predefinidas que determinan qué tráfico puede entrar o salir de la red. Las reglas pueden basarse en varios factores, como direcciones IP, puertos de red, protocolos, y más. Los firewalls pueden ser configurados para permitir o bloquear el tráfico según estos criterios.
- Firewall: Protege la red interna controlando el tráfico de red entre la red interna y externa.



DMZ (Zona Desmilitarizada)

- Una **DMZ** (Demilitarized Zone) es una red separada que actúa como una zona intermedia entre una red interna y una red externa. Su propósito es añadir una capa extra de seguridad y proteger los recursos internos de una red de los riesgos provenientes de Internet.
- En una configuración típica de DMZ, se colocan los servidores que deben ser accesibles desde el exterior, como servidores web, servidores de correo, o servidores FTP, en la DMZ. Estos servidores están expuestos a Internet y, por lo tanto, son más vulnerables a ataques. Sin embargo, al estar en una DMZ, cualquier posible brecha en estos servidores no comprometerá directamente la red interna y sus recursos críticos.
- La idea es que, si un atacante logra comprometer un servidor en la DMZ, aún necesitaría superar la capa de protección adicional que es el firewall entre la DMZ y la red interna para acceder a los recursos internos de la empresa.
- **DMZ:** Es una zona intermedia que aloja servidores accesibles desde el exterior, proporcionando una capa adicional de seguridad y separación entre la red externa e interna.



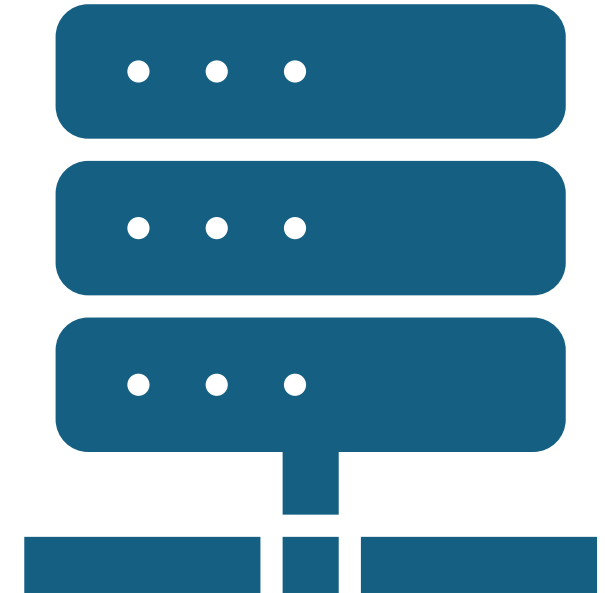
Políticas de un Firewall

- Hay dos políticas básicas en la configuración de un cortafuegos que cambian radicalmente la filosofía fundamental de la seguridad en la organización:
- **Política restrictiva:** Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar las empresas y organismos gubernamentales.
- **Política permisiva:** Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado. Esta aproximación la suelen utilizar universidades, centros de investigación y servicios públicos de acceso a Internet.
- La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido



GATEWAY

- Un **gateway** (o puerta de enlace) es un dispositivo o software que actúa como un punto de acceso o intermediario entre dos redes que utilizan diferentes protocolos o tecnologías. Su función principal es facilitar la comunicación entre estas redes distintas y permitir la transferencia de datos entre ellas.

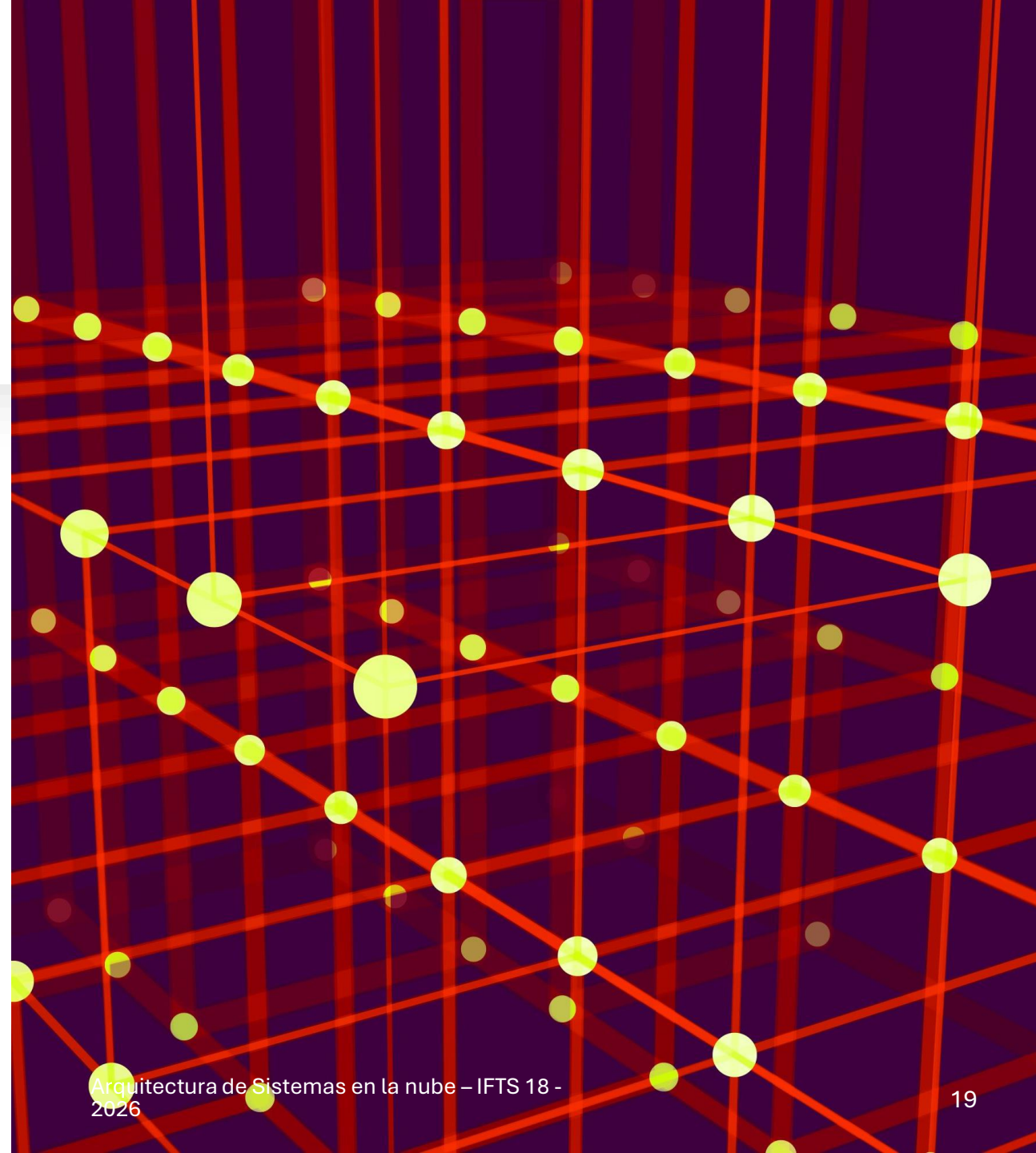


Funcionamiento de un Gateway

- **Intermediario de Protocolos:** Un gateway convierte o traduce datos entre diferentes protocolos de comunicación, asegurando que los sistemas puedan entenderse y comunicarse entre sí. Por ejemplo, un gateway puede conectar una red que usa el protocolo TCP/IP con una red que usa otro protocolo.
- **Encaminamiento de Datos:** El gateway recibe datos de una red, los convierte al formato requerido y luego los envía a la otra red. En el proceso, puede aplicar políticas de seguridad, control de acceso, o realizar transformaciones en los datos.
- **Control de Tráfico:** Puede controlar y gestionar el flujo de datos entre redes, asegurando que el tráfico se enrute adecuadamente y que se respeten las reglas de la red.

Aplicaciones y Ejemplos

- **Gateway de Red:**
 - Ejemplo: Un router que conecta una red doméstica a Internet. Este router actúa como un gateway al convertir y enrutar el tráfico entre la red local y la red global de Internet.
- **Gateway de Aplicaciones:**
 - Ejemplo: Un API Gateway en arquitecturas de microservicios, que maneja la comunicación entre clientes y servicios backend.
- **Gateway de Voz:**
 - Ejemplo: Un gateway VoIP que convierte llamadas entre una red telefónica tradicional y una red de datos IP.
- Puede controlar y gestionar el flujo de datos entre redes, asegurando que el tráfico se enrute adecuadamente y que se respeten las reglas de la red.



Proxy

- Un proxy (o servidor proxy) es un servidor que actúa como intermediario entre un cliente y el servidor al que se está intentando acceder. Su función principal es recibir las solicitudes de los clientes, enviar esas solicitudes al servidor de destino y luego devolver la respuesta del servidor al cliente.



Funcionamiento de un Proxy:

Recepción de Solicitudes:

- El cliente (por ejemplo, tu navegador web) envía una solicitud para acceder a un recurso en Internet (como una página web).

Envío al Servidor de Destino:

- El proxy recibe la solicitud, la procesa, y luego la envía al servidor de destino en nombre del cliente.

Recepción de Respuesta:

- El servidor de destino envía la respuesta al proxy, que a su vez la devuelve al cliente.

Utilidades del Proxy:



Anonimato y Privacidad:

Los proxies pueden ocultar la dirección IP del cliente, proporcionando anonimato al navegar por la web.



Control de Acceso y Filtrado:

Las organizaciones pueden usar proxies para bloquear el acceso a ciertos sitios web o contenido, y para monitorear y controlar el uso de Internet.



Caché:

Los proxies pueden almacenar en caché (guardar) copias de recursos frecuentemente solicitados para mejorar el rendimiento y reducir la carga en los servidores de destino.



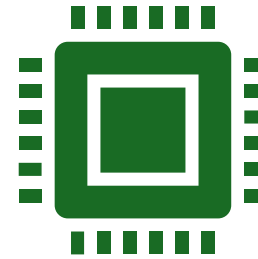
Optimización y Compresión: Algunos proxies optimizan y comprimen el contenido para mejorar la velocidad de acceso y reducir el uso del ancho de banda.

Ejemplos Prácticos:



Proxy Web:

Un servicio como HideMyAss o ProxySite Netscope que permite a los usuarios navegar por la web de manera anónima.



Proxy Corporativo:

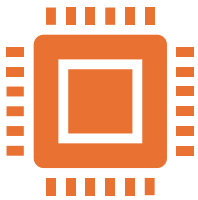
Un proxy en una red de empresa que controla el acceso a sitios web, bloquea contenido inapropiado y proporciona informes de uso.



Proxy Reverso

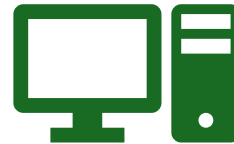
- Un proxy reverso es un servidor que actúa como intermediario para solicitudes que llegan a un servidor de backend. A diferencia de un proxy tradicional, que actúa en nombre de los clientes, un proxy reverso actúa en nombre de uno o más servidores backend, ocultando su presencia a los clientes.

Funcionamiento de un Proxy Reverso:



Recepción de Solicitudes:

El cliente envía una solicitud a un servidor que piensa que es el servidor de destino real, pero en realidad está siendo manejado por el proxy reverso.



Enrutamiento:

El proxy reverso recibe la solicitud y decide a qué servidor backend debe enviar la solicitud, basado en diversas reglas de enrutamiento.



Envío y Recepción:

El servidor backend maneja la solicitud y envía la respuesta al proxy reverso, que luego la devuelve al cliente.

Utilidades del Proxy Reverso:



Balanceo de Carga:

Distribuye las solicitudes entre múltiples servidores backend para equilibrar la carga y mejorar la disponibilidad y el rendimiento del servicio.



Seguridad:

Protege los servidores backend ocultándolos de acceso directo externo y proporcionando un punto único de acceso.



Caché:

Puede almacenar en caché respuestas de servidores backend para mejorar el rendimiento y reducir la carga en los servidores.



SSL/TLS Termination:

Maneja la encriptación y descriptación del tráfico SSL/TLS, reduciendo la carga en los servidores backend.

Ejemplos Prácticos:



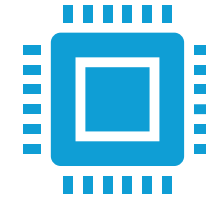
Servidor Web Corporativo:

Un servidor NGINX o Apache configurado como proxy reverso para un sitio web que maneja tráfico de múltiples servidores backend, distribuyendo la carga y manejando la caché.



Balanceo de Carga en la Nube:

Servicios como AWS Elastic Load Balancer que actúan como proxies reversos para distribuir solicitudes entre instancias de servidores en una infraestructura en la nube.

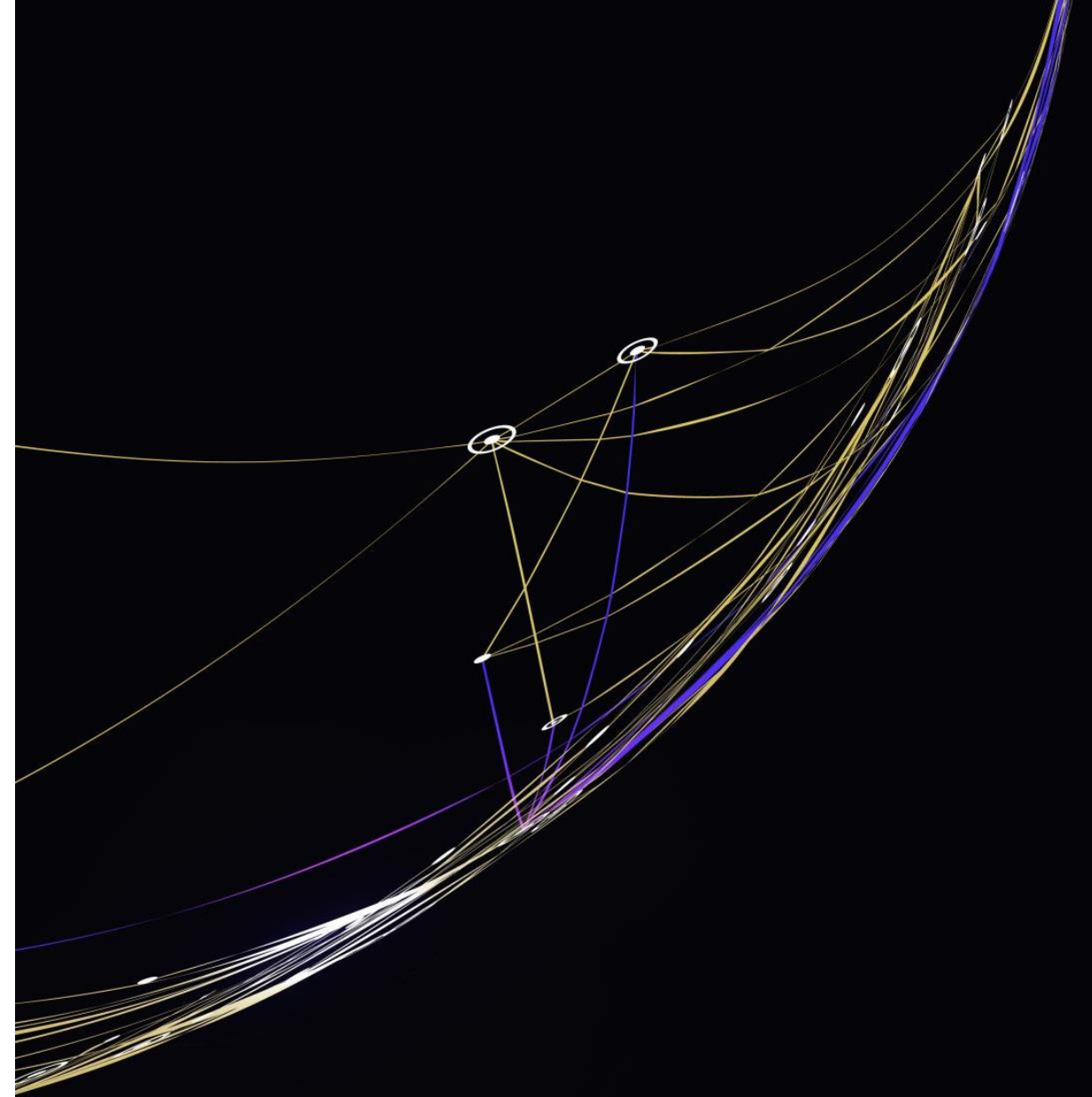


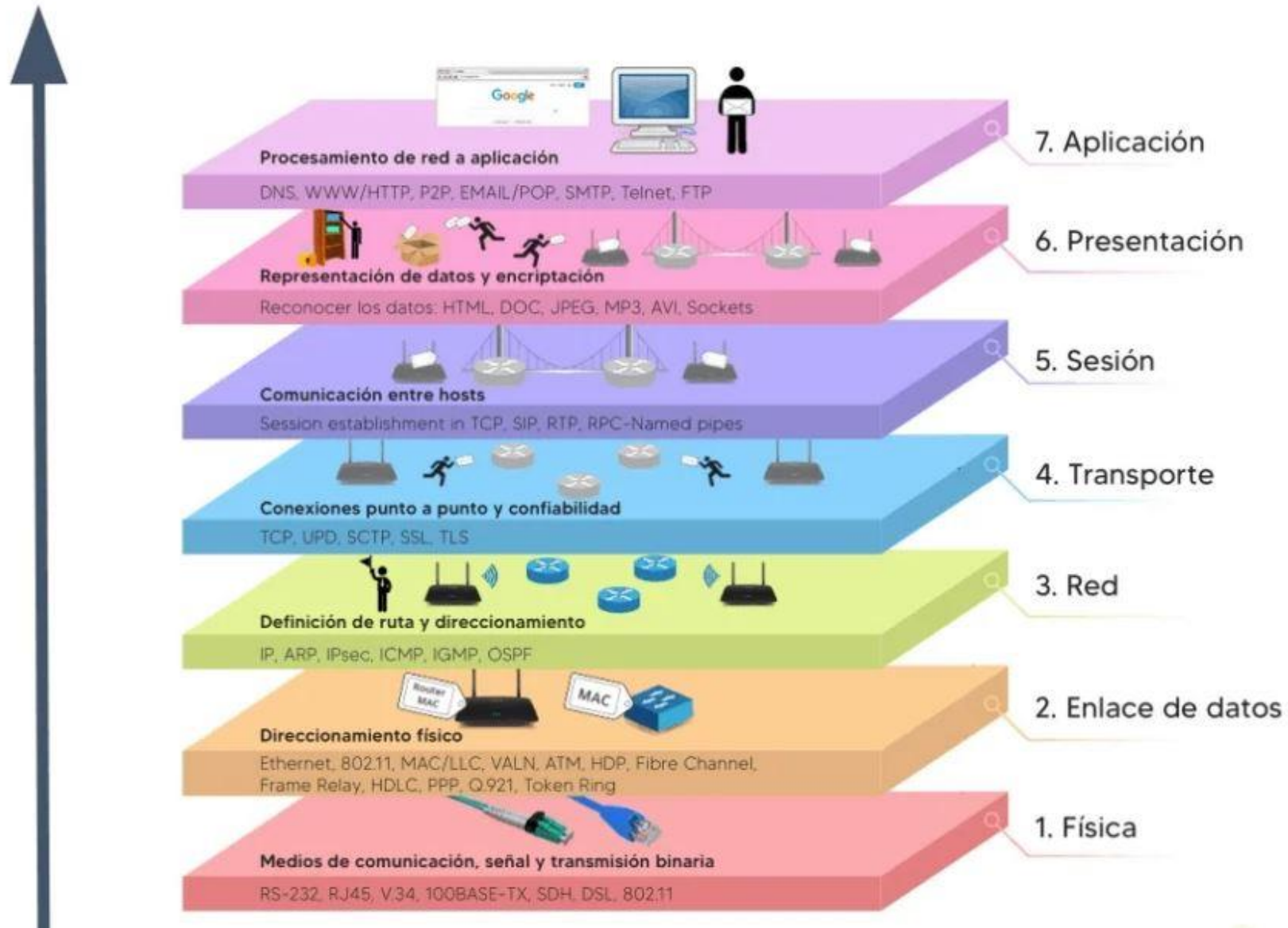
CDN (Content Delivery Network):

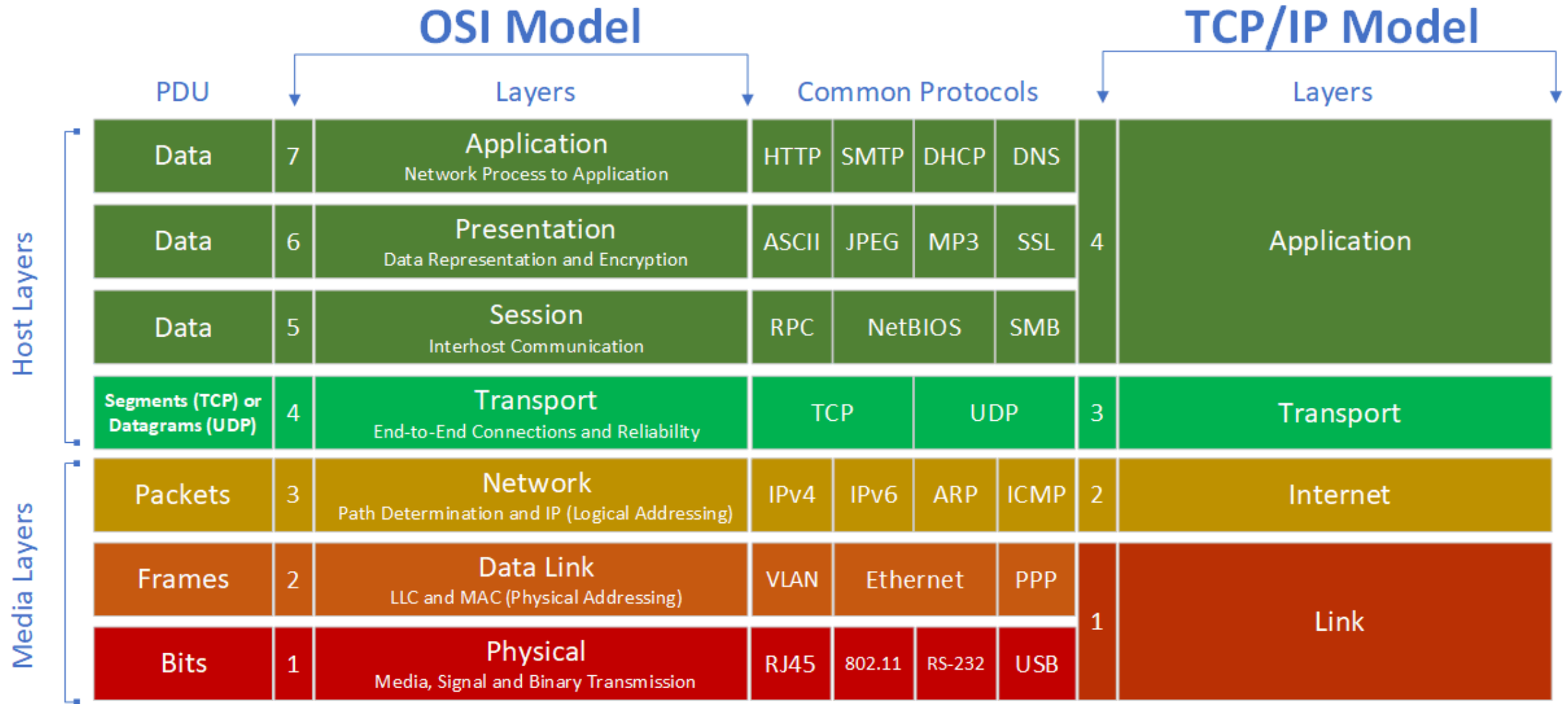
Servicios como Cloudflare que usan proxies reversos para almacenar en caché y entregar contenido a los usuarios desde ubicaciones cercanas.

Open Systems Interconnection

- Es un marco de referencia para entender y diseñar redes de comunicación. Este modelo divide el proceso de comunicación en siete capas, cada una con funciones específicas.







C:\WINDOWS\system32\cmd.exe

Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\DANK>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local 4 :

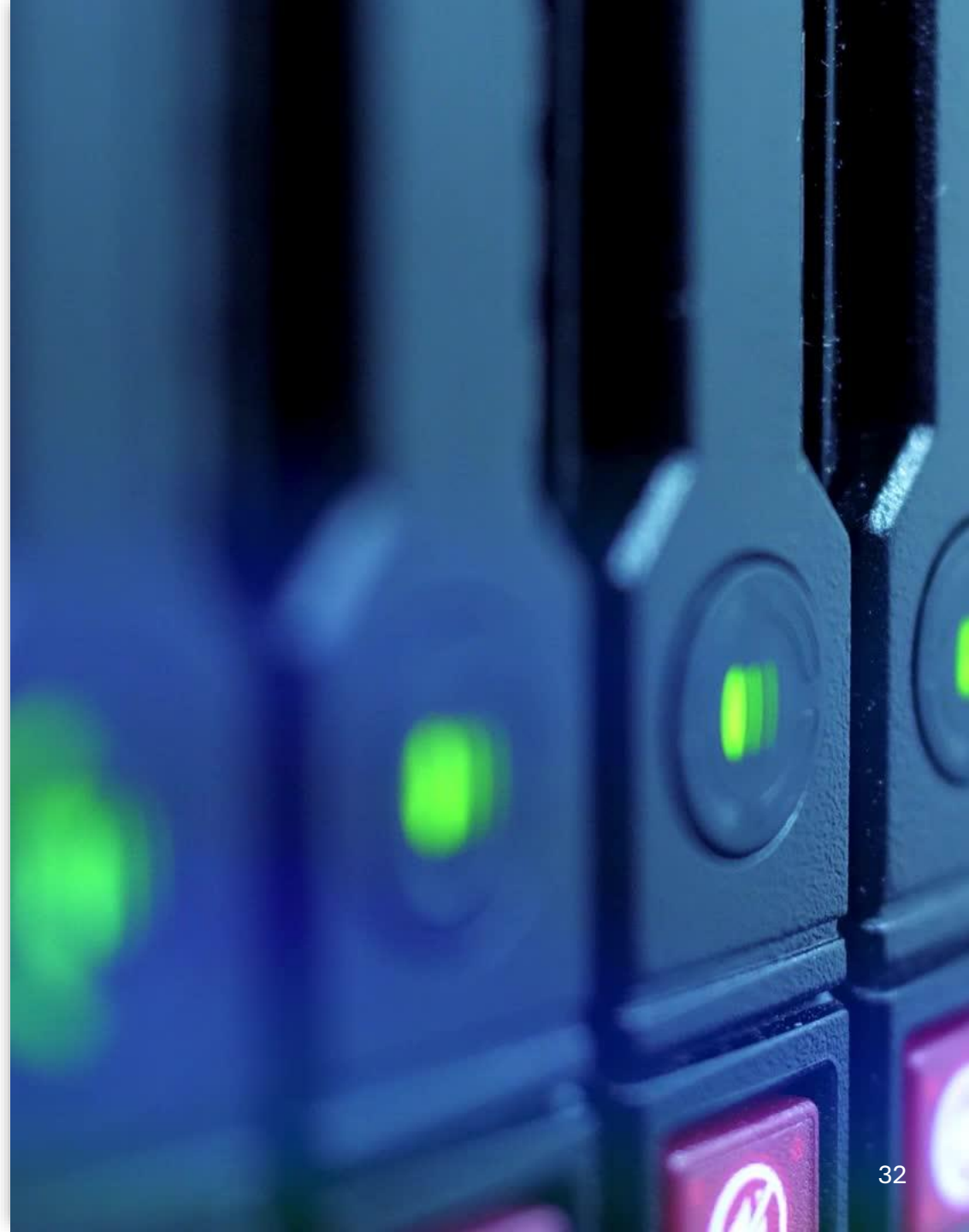
Sufijo de conexión específica DNS : WAG54GX2
Dirección IP. : 192.168.1.3
Máscara de subred : 255.255.255.0
Puerta de enlace predeterminada : 192.168.1.1

C:\Documents and Settings\DANK>_

Composición de una Dirección IP

1. Dirección IP

- Una **dirección IP** (Internet Protocol) es una etiqueta numérica asignada a cada dispositivo en una red que utiliza el protocolo de Internet para la comunicación. Su función es identificar de manera única cada dispositivo en la red.



Composición de una Dirección IP

- **2. Máscara de Subred**

- La máscara de subred define el rango de direcciones IP que pertenecen a una misma red o subred. Su propósito es separar la parte de la dirección IP que corresponde a la red de la parte que corresponde a los hosts (dispositivos) dentro de esa red.

- **3. Gateway**

- El **gateway** (o puerta de enlace) es un dispositivo que actúa como un punto de acceso o intermediario entre una red local y una red externa (como Internet). Su función principal es enrutar el tráfico que sale de la red local hacia otros destinos y viceversa.

Formato de una Dirección IP:

- IP
 - IPv4:
 - **Formato:** Una dirección IPv4 consta de 32 bits, representados en 4 octetos (bytes). Cada octeto se expresa como un número decimal entre 0 y 255, y los octetos están separados por puntos.
 - **Ejemplo:** 192.168.1.10 ---192: Primer octeto 168: Segundo octeto 1: Tercer octeto 10: Cuarto octeto
 - IPv6:
 - **Formato:** Una dirección IPv6 consta de 128 bits, representados en 8 grupos de 16 bits, separados por dos puntos. Cada grupo se expresa en hexadecimal. Ejemplo: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
 - **Ejemplo:** 2001:db8:85a3:8d3:1319:8a2e:0370:7344
2001: Primer grupo--db8: Segundo grupo--85a3: Tercer grupo--8d3: Cuarto grupo--1319: Quinto grupo--8a2e: Sexto grupo--0370: Séptimo grupo
7344: Octavo grupo

IP reservadas en una red

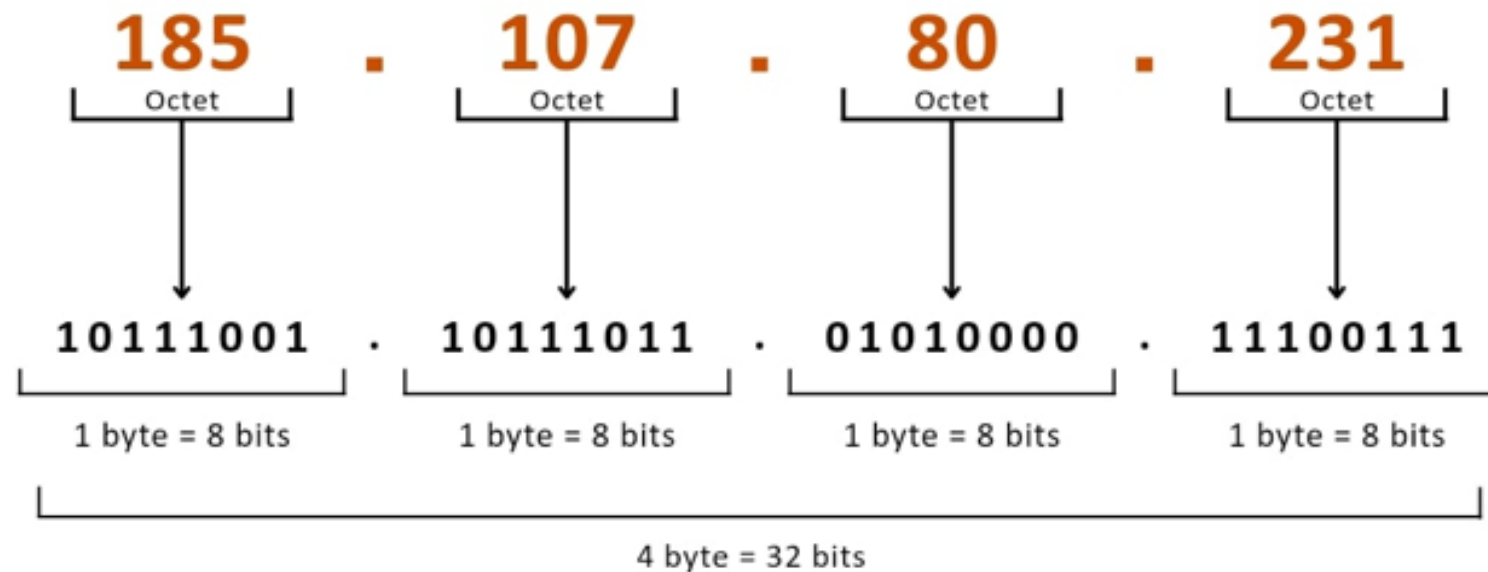
- Como regla general, la primera y última dirección IP de una red están reservadas y no se pueden usar
- **Ejemplo:** para la red privada 192.168.100.0/24, la 192.168.100.0 está reservada para la propia red, y la 192.168.100.255 está reservada para broadcast. Naturalmente, que las direcciones IP **no se deben** duplicar, es decir que múltiples dispositivos usen una misma. Esto es especialmente grave si se duplica la dirección del default gateway, habitualmente el router a internet.



IPV4 Y MÁSCARA SUBRED

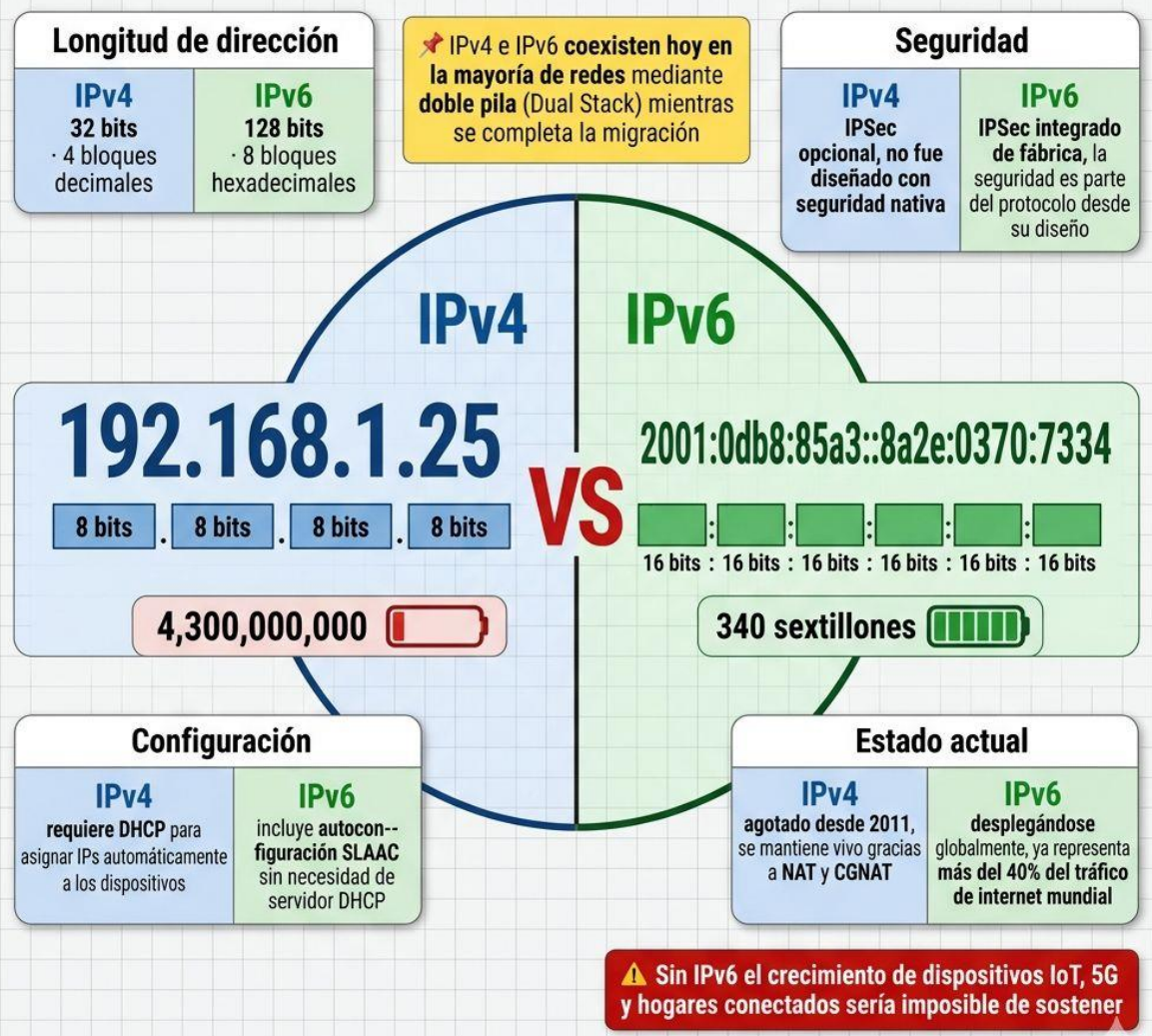
	Network Portion	Host Portion
IPv4 Address	192 . 168 . 10	10
	11000000 10101000 00001010	00001010
Subnet Mask	255 . 255 . 255	0
	11111111 11111111 11111111	00000000

IPv4 Address Format



- - dotted decimal format
- - binary format

IPv4 vs IPv6 – EL PASADO Y EL FUTURO DEL DIRECCIONAMIENTO IP



IPv4 = 4,300 millones de direcciones · IPv6 = 340,000,000,000,000,000,000,000,000,000,000,000,000,000 direcciones

Clases de Redes

- Las direcciones IP están compuestas por 32 bits divididos en 4 octetos de 8 bits cada uno. A su vez, un bit o una secuencia de bits determinan la Clase a la que pertenece esa dirección IP.
- Cada clase de una dirección de red determina una máscara por defecto, un rango IP, cantidad de redes y de hosts por red.

CLASE	DIRECCIONES DISPONIBLES		CANTIDAD DE REDES	CANTIDAD DE HOSTS	APLICACIÓN
	DESDE	HASTA			
A	0.0.0.0	127.255.255.255	128*	16.777.214	Redes grandes
B	128.0.0.0	191.255.255.255	16.384	65.534	Redes medianas
C	192.0.0.0	223.255.255.255	2.097.152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	no aplica	no aplica	Multicast
E	240.0.0.0	255.255.255.255	no aplica	no aplica	Investigación

* El intervalo 127.0.0.0 a 127.255.255.255 está reservado como dirección loopback y no se utiliza.

CLASE A,B,C

- Cada Clase tiene una máscara de red por defecto, la Clase A 255.0.0.0, la Clase B 255.255.0.0 y la Clase C 255.255.255.0. Al direccionamiento que utiliza la máscara de red por defecto, se lo denomina "direccionamiento con clase" (classful addressing).

CLASE A	Red	Host		
Octeto	1	2	3	4
Bits	11111111	00000000	00000000	00000000
Mascara (defecto)	255	0	0	0

Dirección de Red: Primer octeto (8 bits)

Dirección de Host: Últimos 3 octetos (24 bits)

CLASE B	Red		Host	
Octeto	1	2	3	4
Bits	11111111	11111111	00000000	00000000
Mascara x defecto	255	255	0	0

Dirección de Red: Primeros 2 octetos (16 bits)

Dirección de Host: Últimos 2 octetos (16 bits)

CLASE C	Red			Host
Octeto	1	2	3	4
Bits	11111111	11111111	11111111	00000000
Mascara x defecto	255	255	255	0

Dirección de Red: Primeros 3 octetos (24 bits)

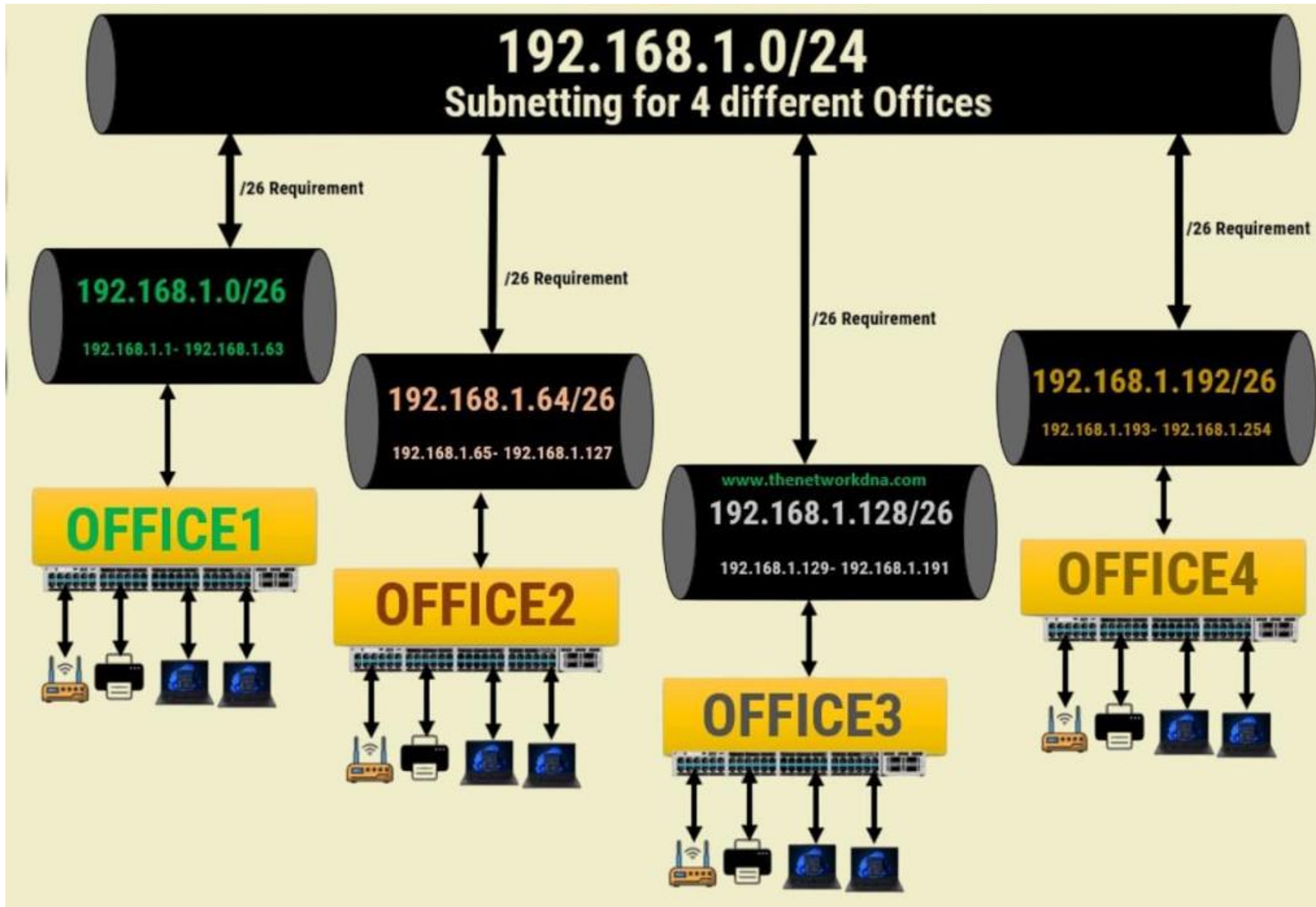
Dirección de Host: Último octeto (8 bits)

Subneteo

- Una subred es una red dentro de otra red, que permite dividir y organizar las direcciones IP de manera más eficiente. El subnetting es el proceso de dividir una red en subredes.
- Ventajas del subnetting:
 - Mejora la eficiencia
 - Los paquetes de datos viajan distancias más cortas y no necesitan pasar por routers innecesarios.
 - Reduce la congestión
 - Al limitar el uso de direcciones IP a unos pocos dispositivos, se reduce el tráfico y el broadcast.
 - Facilita la administración
 - Las subredes permiten separar recursos para diferentes departamentos, proyectos o entornos.
 - Mejora el rendimiento
 - Las subredes permiten que los datos se entreguen directamente entre emisores y receptores que están en la misma subred.
 - Contribuye a la ciberseguridad
 - Una red más eficiente tiene menos probabilidades de sufrir interrupciones o vulnerabilidades.
 - El subnetting es una técnica fundamental a medida que las redes crecen en tamaño y complejidad.

Subnets Públicas vs. Privadas

Característica	Subnet Pública	Subnet Privada
Puerta de salida	Conectada a un Internet Gateway (IGW) .	Conectada a un NAT Gateway (o sin salida directa).
Accesibilidad	Visible desde el internet público.	Solo accesible desde dentro de la VPC o vía VPN.
Residente típico	Servidores Web, Bastions o Load Balancers.	Bases de datos y lógica de negocio (Backend).



Subneteo

- Siempre que se subnetea se hace a partir de una dirección de red Clase A, B, o C y está se adapta según los requerimientos de subredes y hosts por subred. Tengan en cuenta que no se puede subnetear una dirección de red sin Clase ya que ésta ya pasó por ese proceso, aclaro esto porque es un error muy común. Al direccionamiento que utiliza la máscara de red adaptada (subneteada), se lo denomina "direccionamiento sin clase" (classless addressing).
- En consecuencia, la Clase de una dirección IP es definida por su máscara de red y no por su dirección IP. Si una dirección tiene su máscara por defecto pertenece a una Clase A, B o C, de lo contrario no tiene Clase aunque por su IP pareciese la tuviese.

Division de Mascara de RED

- La máscara de red se divide en 2 partes:
- **Porción de Red:** En el caso que la máscara sea por defecto, una dirección con Clase, la cantidad de bits "1" en la porción de red, indican la dirección de red, es decir, la parte de la dirección IP que va a ser común a todos los hosts de esa red.
- En el caso que sea una máscara adaptada, el tema es más complejo. La parte de la máscara de red cuyos octetos sean todos bits "1" indican la dirección de red y va a ser la parte de la dirección IP que va a ser común a todos los hosts de esa red, los bits "1" restantes son los que en la dirección IP se van a modificar para generar las diferentes subredes y van a ser común solo a los hosts que pertenecen a esa subred (asi explicado parece engorroso, así que más abajo les dejo ejemplos).
- En ambos caso, con Clase o sin, determina el prefijo que suelen ver después de una dirección IP (ej: /8, /16, /24, /18, etc.) ya que ese número es la suma de la cantidad de bits "1" de la porción de red.
- **Porción de Host:** La cantidad de bits "0" en la porción de host de la máscara, indican que parte de la dirección de red se usa para asignar direcciones de host, es decir, la parte de la dirección IP que va a variar según se vayan asignando direcciones a los hosts.

Ejemplo 1

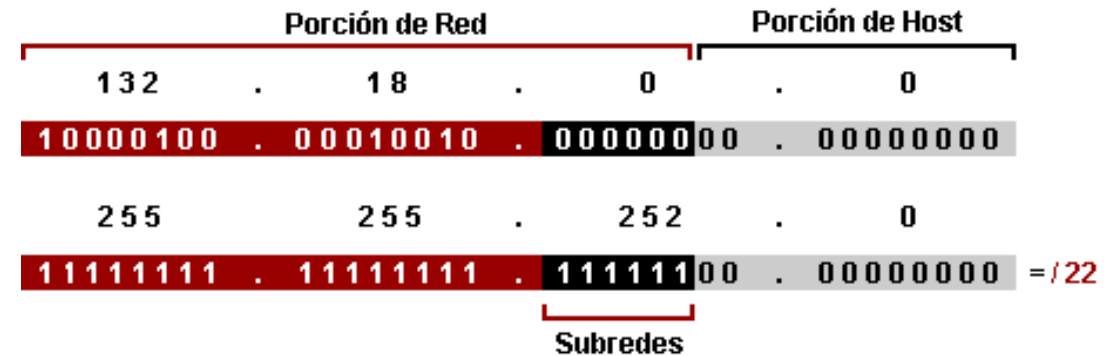
- Si tenemos la dirección IP Clase C 192.168.1.0/24 y la pasamos a binario, los primeros 3 octetos, que coinciden con los bits "1" de la máscara de red (fondo bordó), es la dirección de red, que va a ser común a todos los hosts que sean asignados en el último octeto (fondo gris). Con este mismo criterio, si tenemos una dirección Clase B, los 2 primeros octetos son la dirección de red que va a ser común a todos los hosts que sean asignados en los últimos 2 octetos, y si tenemos una dirección Clase A, el 1 octeto es la dirección de red que va a ser común a todos los hosts que sean asignados en los últimos 3 octetos.

Porción de Red			Porción de Host
192	.	168	. 1
11000000	.	10101000	. 00000001
255	.	255	. 255
11111111	.	11111111	. 11111111

00000000 = /24

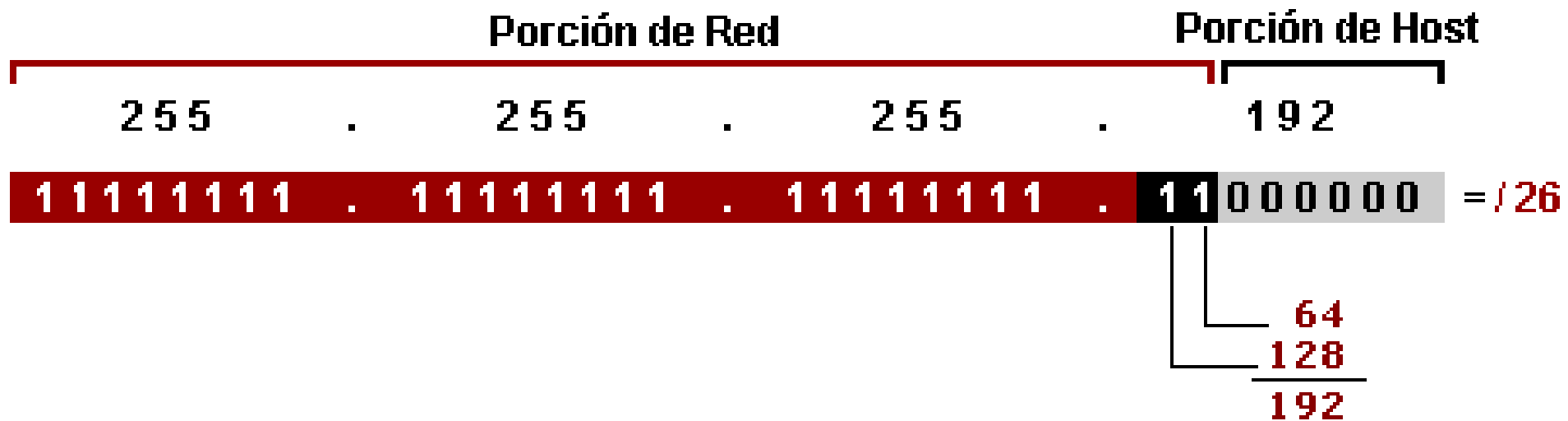
Ejemplo 2

- Si en vez de tener una dirección con Clase tenemos una ya subneteada, por ejemplo la 132.18.0.0/22, la cosa es más compleja. En este caso los 2 primeros octetos de la dirección IP, ya que los 2 primeros octetos de la máscara de red tienen todos bits "1" (fondo rojo), es la dirección de red y va a ser común a todas las subredes y hosts. Como el 3º octeto está dividido en 2, una parte en la porción de red y otra en la de host, la parte de la dirección IP que corresponde a la porción de red (fondo negro), que tienen en la máscara de red los bits "1", se va a ir modificando según se vayan asignando las subredes y solo va a ser común a los host que son parte de esa subred. Los 2 bits "0" del 3º octeto en la porción de host (fondo gris) y todo el último octeto de la dirección IP, van a ser utilizados para asignar direcciones de host.



Ejercicio de Subneteo

- Se requiere subnetear una red de clase C 192.168.1.0 /24 en 4 subredes que tengan como mínimo 50 host cada una.
- Primer paso: Adaptar la Máscara de Red por Defecto a Nuestras Subredes (1)
- Segundo paso: Obtener Cantidad de Hosts por Subred
- Tercer Paso: Obtener Rango de Subredes



Primer paso

- La máscara por defecto para la red **192.168.1.0** es **255.255.255.0**
- Usando la fórmula $2^N = X$, donde **N** es la cantidad de bits que tenemos que robarle a la porción de host (Siempre de izquierda a derecha), y **X** como resultado tiene q ser igual o mayor a la cantidad de redes q nos piden y que respete la cantidad de host. Entonces adaptamos la máscara de red por defecto a la subred.
- $2^2 = 4$ lo cual robamos 2 bit de la sección de host
- La máscara de subred va a quedar conformada así: 255.255.255.192



Segundo paso

- El ejercicio nos pedía un mínimo de 50 hosts por subred. Para esto utilizamos la fórmula $2^M - 2$, donde **M** es el número de bits "0" disponibles en la porción de host y - 2 porque la primer y última dirección IP de la subred no se utilizan por ser la dirección de la subred y broadcast respectivamente.

$$2^6 - 2 = 62 \text{ hosts por subred.}$$

Tercer paso

- Para obtener el rango subredes utilizamos la porción de red de la dirección IP que fue modificada al adaptar la máscara de red. A la máscara de red se le agregaron 2 bits en el cuarto octeto, entonces van a tener que modificar esos mismos bits pero en la dirección IP (fondo negro).
- Los 2 bits "0" de la porción de red (fondo negro) son los que más adelante modificaremos según vayamos asignando las subredes.



N° de Subred	Rango IP *		Hosts Asignables x Subred
	Desde	Hasta	
1	192.168.1.0	192.168.1.63	62
2	192.168.1.64	192.168.1.127	62
3	192.168.1.128	192.168.1.191	62
4	192.168.1.192	192.168.1.255	62

* La primera y la última dirección IP de cada Subred no se asignan ya que contienen la dirección de red y broadcast de la Subred.

Tabla de entrega

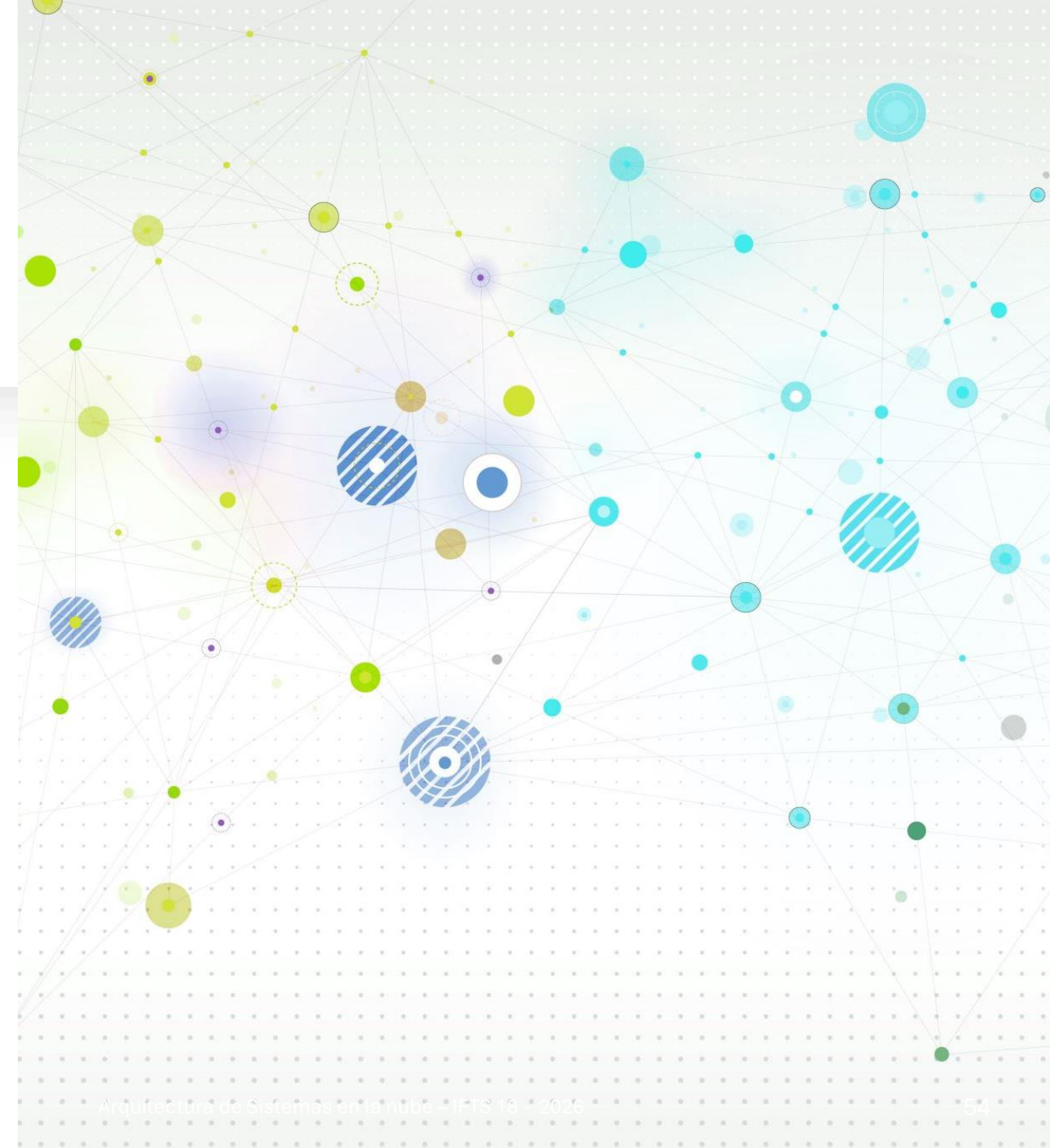
NETWORK ID	SUBNET MASK	HOST ID RANGE	N° HOSTS	BROADCAST ID
192.168.1.0	255.255.255.192	192.168.1.1-192.168.1.62	62	192.168.1.63
192.168.1.64	255.255.255.192	192.168.1.65-192.168.1.126	62	192.168.1.127
192.168.1.128	255.255.255.192	192.168.1.129-192.168.1.191	62	192.168.1.191
192.168.1.192	255.255.255.192	192.168.1.193-192.168.1.192	62	192.168.1.255

AYUDA

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

NSG: El Firewall de la Instancia

- **Network Security Groups (NSG)** (en Azure, OCI) o **Security Groups** (en AWS).
- Es una herramienta de seguridad que opera principalmente en las **capas 3 (Red)** y **4 (Transporte)**.
- **Capa 3 (IP):** Permiten filtrar tráfico basado en direcciones IP de origen y destino.
- **Capa 4 (Puerto/Protocolo):** Permiten o deniegan el acceso basado en protocolos (TCP/UDP) y puertos específicos (ej. abrir el puerto 80 para HTTP o el 22 para SSH).



Diferencia entre Ruteo y NSG

Componente	Función Principal	Analogía
Tabla de Ruteo	Define el camino físico/lógico que debe seguir un paquete.	El GPS que te dice qué carretera tomar.
NSG / Security Group	Define quién tiene permiso para entrar o salir.	El portero que revisa tu identificación en la entrada.

