

UNIDAD N° 5: Protocolo TCP/IP

Arquitectura del TCP/IP. **El nivel internet. Protocolos IP, funcionamiento y encaminamiento. Clases de direcciones IP.** Relación con la interfase de red; ARP y RARP. Protocolo de control de red ICMP. Enrutamiento en redes IP. Sistemas autónomos. La nueva versión de IP, Ipv6. Ventajas de Ipv6 respecto de Ipv4. El protocolo DHCP.

EL NIVEL INTERNET. PROTOCOLO IP. FUNCIONAMIENTO Y ENCAMINAMIENTO.

- **Comprensión profunda del diseño de redes**
 - **Diseñar redes eficientes** requiere entender cómo dividir y organizar direcciones IP para minimizar el desperdicio de direcciones y facilitar el escalado.
 - Saber calcular subredes **classful y classless (CIDR)** permite diseñar infraestructuras adaptadas a necesidades específicas, por ejemplo, para segmentar redes por departamentos o servicios.
- **Diagnóstico y resolución de problemas**
 - En entornos reales, los errores de direccionamiento pueden causar conflictos, pérdida de conectividad o rutas erróneas.
 - Comprender las matemáticas detrás de las subredes permite al ingeniero **detectar y corregir errores rápidamente**, incluso cuando las herramientas fallan o no están disponibles.

EL NIVEL INTERNET. PROTOCOLO IP. FUNCIONAMIENTO Y ENCAMINAMIENTO.

- **Configuración manual y análisis de red**
 - En roles de configuración de routers, firewalls o VPNs, a menudo se necesita **introducir rutas, máscaras o resúmenes a mano.**
 - El conocimiento práctico evita errores como **rutas redundantes o solapadas**, y mejora la eficiencia del routing.
- **Optimización de tablas de enrutamiento**
 - El **resumen de rutas** es crucial en redes medianas o grandes para **reducir la cantidad de entradas en las tablas de enrutamiento y mejorar el rendimiento.**
 - Esta habilidad no solo optimiza la red, sino que también **reduce el tráfico de actualización de rutas** (como en OSPF o BGP).

EL NIVEL INTERNET. PROTOCOLO IP. FUNCIONAMIENTO Y ENCAMINAMIENTO.

- **Seguridad y control**

- La **segmentación de red a través de subredes** es clave para aplicar políticas de seguridad, VLANs o ACLs.
- Un diseño incorrecto o mal entendido **puede dejar servicios expuestos o violar principios de minimización de superficie de ataque.**

- **Liderazgo técnico**

- Un ingeniero debe ser capaz de **explicar, defender y justificar decisiones de diseño** a colegas, superiores o personal técnico.
- **Confiar únicamente en herramientas sin entender el fundamento limita la capacidad de formar equipos o tomar decisiones estratégicas.**

- **Entornos críticos o de misión**

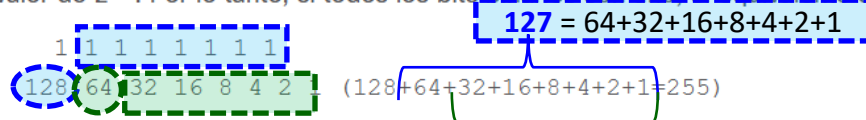
- En redes del Estado, militares, industriales o remotas, donde la automatización puede no estar disponible, la **capacidad de trabajar “a mano” es indispensable.**
Ejemplo: **durante una falla crítica, el ingeniero debe poder hacer cálculos de subred y rutas con papel y lápiz.**

PROTOCOLO IPv4. Direccionamiento lógico.

Comprender las direcciones IP

Una dirección IP se utiliza para identificar de forma única un dispositivo en una red IP. La dirección se compone de 32 bits binarios, que pueden dividirse en una porción de red y una porción de host mediante una máscara de subred. Los 32 bits binarios se dividen en cuatro octetos (1 octeto = 8 bits). Cada octeto se convierte a decimal y se separa por un punto. Por esta razón, se dice que una dirección IP se expresa en formato decimal con puntos (por ejemplo, 172.16.81.100). El valor de cada octeto varía de 0 a 255 decimal, o de 00000000 a 11111111 en binario.

Así es como los octetos binarios se convierten a decimales: el bit más a la derecha, o el bit menos significativo, de un octeto tiene un valor de 2^0 . El bit inmediatamente a la izquierda tiene un valor de 2^1 . Esto continúa hasta el bit más a la izquierda, o el bit más significativo, que tiene un valor de 2^7 . Por lo tanto, si todos los bits binarios son uno, el equivalente decimal sería 255, como se muestra aquí:



1 1 1 1 1 1 1 1
128 64 32 16 8 4 2 1 (128+64+32+16+8+4+2+1=255)
127 = 64+32+16+8+4+2+1

A continuación se muestra un ejemplo de conversión de octetos cuando no todos los bits están configurados en 1.



0 1 0 0 0 0 0 1
0 64 0 0 0 0 0 1 (0+64+0+0+0+0+0+1=65)
63 = 32+16+8+4+2+1

Y este ejemplo muestra una dirección IP representada en binario y decimal.


10. 1. 23. 19 (decimal)
00001010.00000001.00010111.00010011 (binario)

Estos octetos se descomponen para proporcionar un esquema de direccionamiento compatible con redes grandes y pequeñas. Existen cinco clases de redes, de la A a la E. Este documento se centra en las clases de la A a la C, ya que las clases D y E están reservadas y su análisis queda fuera del alcance del presente documento.

<https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html#toc-hId--1733132837>

PROTOCOLO IPv4. Ejemplo 1: Subnetting fijo (FLSM).

- **Escenario de Negocio:** SoftNova S.A. es una empresa de desarrollo de software con 4 departamentos principales: Desarrollo - Soporte Técnico – Administración - Investigación y Desarrollo (I+D).
- **Requerimiento:** Cada departamento necesita su propia subred por motivos de seguridad, segmentación de tráfico y gestión de recursos. La red disponible es 192.168.1.0/24, y se debe dividir en **4 subredes iguales**.

- **Resolución:** Red original: 192.168.1.0/24 - Se necesitan 4 subredes $\rightarrow 2$ bits ($2^2 = 4$) - Nueva máscara: /26 (255.255.255.192).

- En la máscara /26, se usan los primeros 2 bits del último octeto para identificar la subred (subred bits resaltados). Los últimos 6 bits se usan para los hosts.
- En binario, el último octeto del bloque 192.168.1.0/24 va de 00000000 a 11111111.
- **Subredes generadas:**
 - 192.168.1.0/26
 - 192.168.1.64/26
 - 192.168.1.128/26
 - 192.168.1.192/26
- **Beneficios:** Menor dominio de broadcast. ACLs más específicas. Mejor trazabilidad del tráfico.

PROTOCOLO IPv4. Ejemplo 1: Subnetting fijo (FLSM).

Subred N°	Dirección de Red	Binario (último octeto)	Rango de Hosts	Broadcast
0	192.168.1.0/ 26	00 000000	192.168.1. 1 – 192.168.1. 62	192.168.1. 63 <div> <div>00 000001</div> <div>...</div> <div>00 111110</div> </div> <div>00 111111</div>
1	192.168.1.64/ 26	01 000000	192.168.1. 65 – 192.168.1. 126	192.168.1.127
2	192.168.1.128/ 26	10 000000	192.168.1. 129 – 192.168.1. 190	192.168.1.191
3	192.168.1.192/ 26	11 000000	192.168.1. 193 – 192.168.1. 254	192.168.1.255 !

PROTOCOLO IPv4. Uso de la subred 0.

- **Uso de la subred 0 en ambientes reales:**

- Tradicionalmente, existía una restricción al uso de la "subred cero" (es decir, la subred con todos los bits de la porción de subred en 0, ejemplo 192.168.1.0/26).
- En los inicios del Subneteo, la subred cero estaba reservada y no debía usarse.
 - ¿Por qué? Porque su dirección coincidía con la dirección de red original (sin subneteo), y podría generar confusión en el ruteo. Esto estaba especificado en **antiguos estándares, como el RFC 950.**
- Sin embargo, esto ya no aplica en la mayoría de los entornos modernos. **El RFC 1878 y tecnologías modernas permiten el uso de la subred cero, siempre que el equipo lo soporte.**
- Todos los sistemas modernos (routers, switches, servidores, etc.) permiten su uso por defecto.
- Hoy es completamente válido usar la subred 192.168.1.0/26 en ambientes reales y de producción.

PROTOCOLO IPv4. Uso de la subred 0.

- **Uso de la subred 0 en ambientes reales:**

- Condiciones para usarla:

- El equipamiento de red lo debe permitir (la mayoría ya lo hace).
 - Debe configurarse de manera coherente con las demás subredes (routing, DHCP, etc.).
 - Evitar ambigüedad: asegurarse de que no haya confusión con la red original (/24).

- Conclusión:

La subred cero se puede usar sin problema en entornos reales actuales, a menos que se esté trabajando con equipamiento muy antiguo o configuraciones heredadas con restricciones explícitas.

PROTOCOLO IPv4. Subnetting con VLSM.

- **Métodos de subnetting con VLSM**

- Existen diferentes métodos para hacer subnetting con VLSM (**Variable Length Subnet Masking**), y cada uno se aplica según el escenario específico de uso.
- A diferencia del subnetting fijo (FLSM), VLSM permite crear subredes de diferentes tamaños dentro de una misma red, optimizando el uso de direcciones IP.

- **Método 1: Descendente (Top-down)**

- Descripción: Se parte del bloque de red original y se asignan las subredes de mayor tamaño hacia las más pequeñas.
- Ventajas:
 - Maximiza el aprovechamiento del espacio de direcciones.
 - Menor fragmentación.
- Escenario típico:
 - Cuando se conocen los requerimientos de hosts por cada subred.
 - Ejemplo: una empresa con sedes que necesitan 100, 50, 25, y 10 hosts respectivamente.
- Paso clave: Ordenar las subredes por cantidad de hosts descendente.

PROTOCOLO IPv4. Subnetting con VLSM.

- **Método 2: Ascendente (Bottom-up)**
 - Descripción: Se parte de subredes pequeñas y se asignan primero.
 - Ventajas: Puede facilitar la planificación si las redes pequeñas son críticas o numerosas.
 - Escenario típico: Cuando hay muchas oficinas pequeñas o sensores / IoT con pocos hosts cada uno.
 - Desventajas: Mayor riesgo de fragmentación y desperdicio de espacio si no se planifica cuidadosamente.
- **Método 3: A partir de un bloque resumido (Supernet y división)**
 - Descripción: Se toma un bloque grande (supernet) y se subdivide en diferentes tamaños de subred, ajustando el prefijo a cada caso.
 - Ventajas: Flexibilidad total.
 - Escenario típico: Diseños jerárquicos como ISP, universidades o data centers que agrupan diferentes bloques por departamentos o servicios.

PROTOCOLO IPv4. Subnetting con VLSM.

- **Método 4: VLSM jerárquico con rutas agregadas**
 - Descripción: Se organiza el subnetting con la intención de facilitar resumen de rutas en los routers.
 - Ventajas:
 - Reduce el tamaño de las tablas de enrutamiento.
 - Mejora el rendimiento de la red.
 - Escenario típico: Redes grandes con muchos routers, como en proveedores de servicios o redes corporativas distribuidas.

PROTOCOLO IPv4. Subnetting con VLSM.

Ejemplo 1 - Método 1: Top-down

- Red base 192.168.1.0/24
- Queremos asignar subredes a los siguientes departamentos y cantidades de hosts:
 - Dirección: 10 Hosts
 - Administración: 100 Hosts
 - Seguridad: 50 Hosts
 - Soporte Técnico: 25 Hosts

- Paso 1: Ordenar por tamaño de red requerido

Calcular el número de hosts más 2 (por red y broadcast), y buscar la máscara más cercana:

Departamento	Hosts requeridos	Hosts + 2	Tamaño de subred	Máscara
Administración	100	102	128	/25
Seguridad	50	52	64	/26
Soporte Técnico	25	27	32	/27
Dirección	10	12	16	/28

PROTOCOLO IPv4. Subnetting con VLSM.

Ejemplo 1 - Método 1: Top-down

- Paso 2: Asignar subredes con el método Top-Down

Empezamos desde 192.168.1.0/24.

Subred 1 – Administración (128 hosts, /25)

- Red: 192.168.1.0/25
- Rango de hosts: 192.168.1.1 – 192.168.1.126 / Broadcast: 192.168.1.127

Subred 2 – Seguridad (64 hosts, /26)

- Red: 192.168.1.128/26
- Rango de hosts: 192.168.1.129 – 192.168.1.190 / Broadcast: 192.168.1.191

Subred 3 – Soporte Técnico (32 hosts, /27)

- Red: 192.168.1.192/27
- Rango de hosts: 192.168.1.193 – 192.168.1.222 / Broadcast: 192.168.1.223

Subred 4 – Dirección (16 hosts, /28)

- Red: 192.168.1.224/28
- Rango de hosts: 192.168.1.225 – 192.168.1.238 / Broadcast: 192.168.1.239

PROTOCOLO IPv4. Subnetting con VLSM.

Ejemplo 2 - Método 2: Ascendente (Bottom-up)

- Red base: 192.168.10.0/24. Requerimientos:
 - Sensores IoT: 8 subredes con 10 hosts cada una.
 - Cámaras de Seguridad: 2 subredes con 30 hosts.
 - Administración Central: 1 subred con 100 hosts.
- Paso 1: Ordenar subredes de menor a mayor (bottom-up).

Nombre	Hosts requeridos	Hosts reales (ajustados)	Cantidad de subredes	Prefijo
IoT	10	14	8	/28
Cámaras	30	62	2	/26
Admin	100	126	1	/25

PROTOCOLO IPv4. Subnetting con VLSM.

Ejemplo 2 - Método 2: Ascendente (Bottom-up)

- Paso 2: Asignar subredes desde la más pequeña.

Partimos desde 192.168.10.0/24. Subnetting paso a paso:

Subred IoT	Dirección	Hosts válidos
IoT 1	192.168.10.0/28	.1 – .14
IoT 2	192.168.10.16/28	.17 – .30
IoT 3	192.168.10.32/28	.33 – .46
IoT 4	192.168.10.48/28	.49 – .62
IoT 5	192.168.10.64/28	.65 – .78
IoT 6	192.168.10.80/28	.81 – .94
IoT 7	192.168.10.96/28	.97 – .110
IoT 8	192.168.10.112/28	.113 – .126

Ya hemos usado 128 direcciones →
192.168.10.0 – 192.168.10.127

PROTOCOLO IPv4. Subnetting con VLSM.

Ejemplo 2 - Método 2: Ascendente (Bottom-up)

- Paso 2: Asignar subredes desde la más pequeña.

Cámaras – 2 subredes /26. Siguiendo bloque libre: 192.168.10.128/26 (64 direcciones):

Subred	Dirección	Hosts válidos
Cámara 1	192.168.10.128/26	.129 – .190
Cámara 2	192.168.10.192/26	.193 – .254

Hasta aquí, toda la red
192.168.10.0/24 ha sido utilizada.

Administración (necesita /25) ¡ya no entra! No hay un bloque libre de 128 direcciones contiguas.

Esto ilustra un riesgo del método bottom-up: si no se planifica con anticipación, puede quedarse sin espacio para las redes grandes.

- **Conclusión:** Este ejemplo comienza con las subredes más pequeñas (IoT, luego cámaras). No se reserva espacio anticipadamente para la subred más grande. **Resultado:** se puede dar lugar a fragmentación y falta de espacio, como ocurrió con la red de administración.

PROTOCOLO IPv4. Supernetting.

Ejemplo 3 - CIDR Resumen

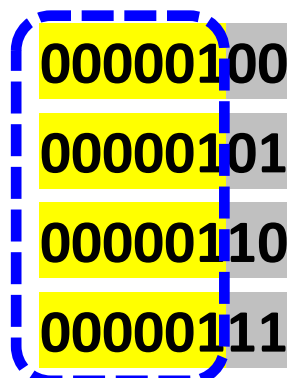
- **Escenario:** Red con múltiples subredes pequeñas, que deben resumirse.
- **Requerimiento:** reducir el tamaño de la tabla de ruteo de 4 entradas a 1.
- **Subredes configuradas:**

○ 192.168.4.0/24

○ 192.168.5.0/24

○ 192.168.6.0/24

○ 192.168.7.0/24



8+8+6 bits compartidos
en el 3er octeto /24

- **Resultado:**

- CIDR Resumen: 192.168.4.0/22 (se toma la primera de las dadas)

PROTOCOLO IPv4. Supernetting.

Ejemplo 3 - CIDR Resumen

- **Condiciones del método:**

- Direcciones de redes ordenadas en forma creciente.
- La cantidad de redes debe ser una potencia de 2. Ej: 2, 4, 8, 16... redes. Esto asegura que todas las subredes puedan ser representadas con un solo prefijo más corto.
- Sin intervalos entre redes. Las redes deben ser contiguas (no debe haber “huecos” entre ellas) y alineadas (deben alinearse con límites binarios según su máscara). Por ejemplo:
 - Se pueden resumir 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24 → **192.168.0.0/22**.
 - Pero no se pueden resumir 192.168.0.0/24, 192.168.2.0/24, 192.168.3.0/24 (**salta 192.168.1.0**).
- Todas las redes deben compartir los bits más significativos: Para encontrar el resumen, se hace una operación **bitwise AND** (operación AND a nivel de bits) sobre las direcciones IP para identificar los bits comunes más a la izquierda. Ese número de bits comunes se convierte en la nueva máscara.

PROTOCOLO IPv4. Supernetting.

Ejemplo 4 - Resumen de ruta en routers

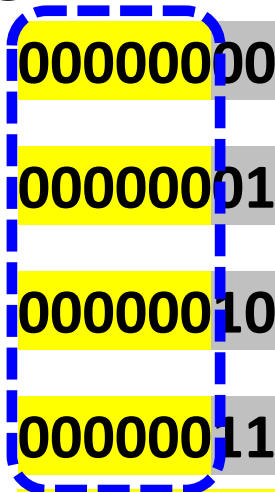
- Router A tiene las siguientes rutas:

- 10.**0**.0.0/16

- 10.**1**.0.0/16

- 10.**2**.0.0/16

- 10.**3**.0.0/16



8+6 bits compartidos en el 2do octeto /14

- Puede anunciar un resumen: 10.0.0.0/14
- Resultado: se mejora la eficiencia del enrutamiento y se reduce el uso de memoria.