

MODULO 3

SEGMENTACION DE RED



REDES INFORMATICAS

Ing. Yarisol A. Castillo Q.

yarisol.castillo@utp.ac.pa



Introducción

La segmentación de red:

- mejorar la seguridad,
- la eficiencia y
- la administración de las **redes** de comunicación al dividir una red en partes más pequeñas y manejables.

Al implementar esta estrategia, puedes optimizar el tráfico de red y mitigar riesgos de seguridad.

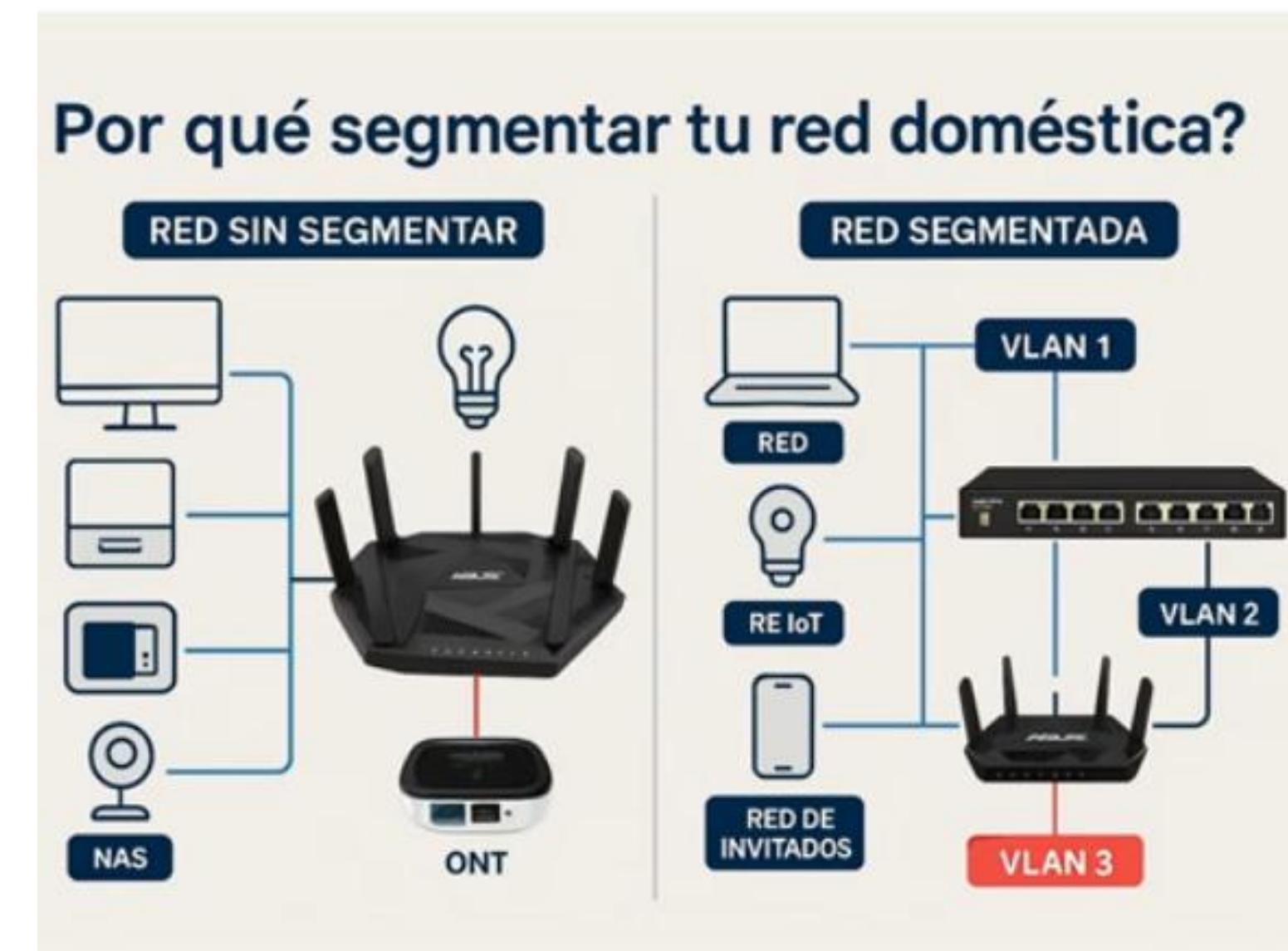


¿Qué es la segmentación de red?

Segmentación de red: se refiere al proceso de dividir una red computacional grande en subredes más pequeñas, conocidas como segmentos o subredes.

De esta manera, se facilita la administración de la red y se aumenta la seguridad al limitar el alcance de posibles fallos o ataques.

- Modelo arquitectónico que consiste en dividir una red informática grande en subredes o segmentos más pequeños y aislados.
- Cada segmento opera como una red propia, con sus propias políticas de seguridad y tráfico.



Tipos de Segmentación

Varios enfoques para dividir una red, se pueden combinar.

1. Segmentación Lógica (Virtual)

Tecnología: Principalmente a través de **VLANs (Redes de Área Local Virtual)** y Listas de Control de Acceso (**ACLs**).

Ventaja: Flexible, más económica, no requiere hardware adicional para cada segmento.

2. Segmentación Física

Tecnología: Uso de **hardware dedicado** (switches y firewalls separados).

Ventaja: Proporciona un **aislamiento total** y un rendimiento más predecible. Ideal para datos altamente sensibles.

3. Microsegmentación

Concepto: Un enfoque aún más granular que aplica políticas a **cargas de trabajo o aplicaciones individuales**, a menudo utilizando Redes Definidas por Software (**SDN**) o *firewalls* internos.

Objetivo: Máxima contención.

Cómo funciona:

Subredes (subnetting): Dividir una red en subredes más pequeñas mediante operaciones en la capa de red.

VLANs (Redes de Área Local Virtual): Crear redes virtuales independientes dentro de una red física.

Firewalls: Configurar barreras que controlan y protegen el tráfico entre segmentos.

DISPOSITIVO	REGLA
NAS	192.168.1.10
Monitor	192.168.1.20
WiFi	192.168.1.100

Ejemplo de reglas de firewall o acceso por IP

Tipos de segmentación de red en casa			
	Red de invitados	VLANs	Reglas de acceso por IP
Nivel de dificultad	🔒 🔒	🔒 🔒	✓
Seguridad	👍	👍 👍	✓
Equipo necesario	✗	✳✳✳✳	✓
Facilidad de configuración	✓	✗	✗

Ventajas de la segmentación de red

Aplicar la segmentación de red conlleva múltiples beneficios, que incluyen:

- Mejora de la seguridad: Al aislar segmentos de la red, se limita la propagación de amenazas y se refuerza la protección de datos sensibles.
- Optimización del rendimiento: La segmentación permite reducir el tráfico redundante, mejorando así la velocidad y la capacidad de respuesta.

Riesgo de dispositivos IoT sin segmentación



Fácil administración: Las redes segmentadas son más fáciles de manejar y solucionar problemas, facilitando la labor del personal de IT.



Configuración red de invitados en router

Red de invitados

Nombre de la red	Invitados
Contraseña	••••• <input checked="" type="checkbox"/>
Aislar de la red principal	<input checked="" type="checkbox"/>

Router

Internet

Red de invitados

The configuration interface shows settings for a guest network (Red de invitados) on a router. The network is named "Invitados" and has a password of "•••••". The "Isolate from main network" option is enabled. To the right, a schematic shows the router connected to the Internet and a mobile device, with a blue line labeled "Red de invitados" connecting the router to the mobile device.

Ejemplo:

Imagina una empresa que maneja cuatro departamentos principales: **IT, finanzas, recursos humanos e invitados**.

Con la segmentación de red, cada departamento tiene su propia subred o VLAN, lo que permite un mejor control sobre quién puede acceder a los recursos específicos de cada área.

Esquema de red de oficina segmentada por departamentos

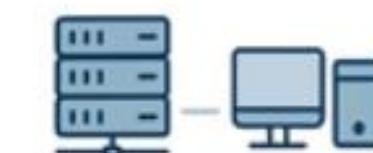
Segmentación por departamentos:

IT

Servidores, ordenadores y switch gestionado

Recursos Humanos

Estaciones de trabajo y acceso a HRMS



Departamento IT
Servidores, ordenadores y switch gestionado



Recursos Humanos
Estaciones de trabajo y acceso a HRMS

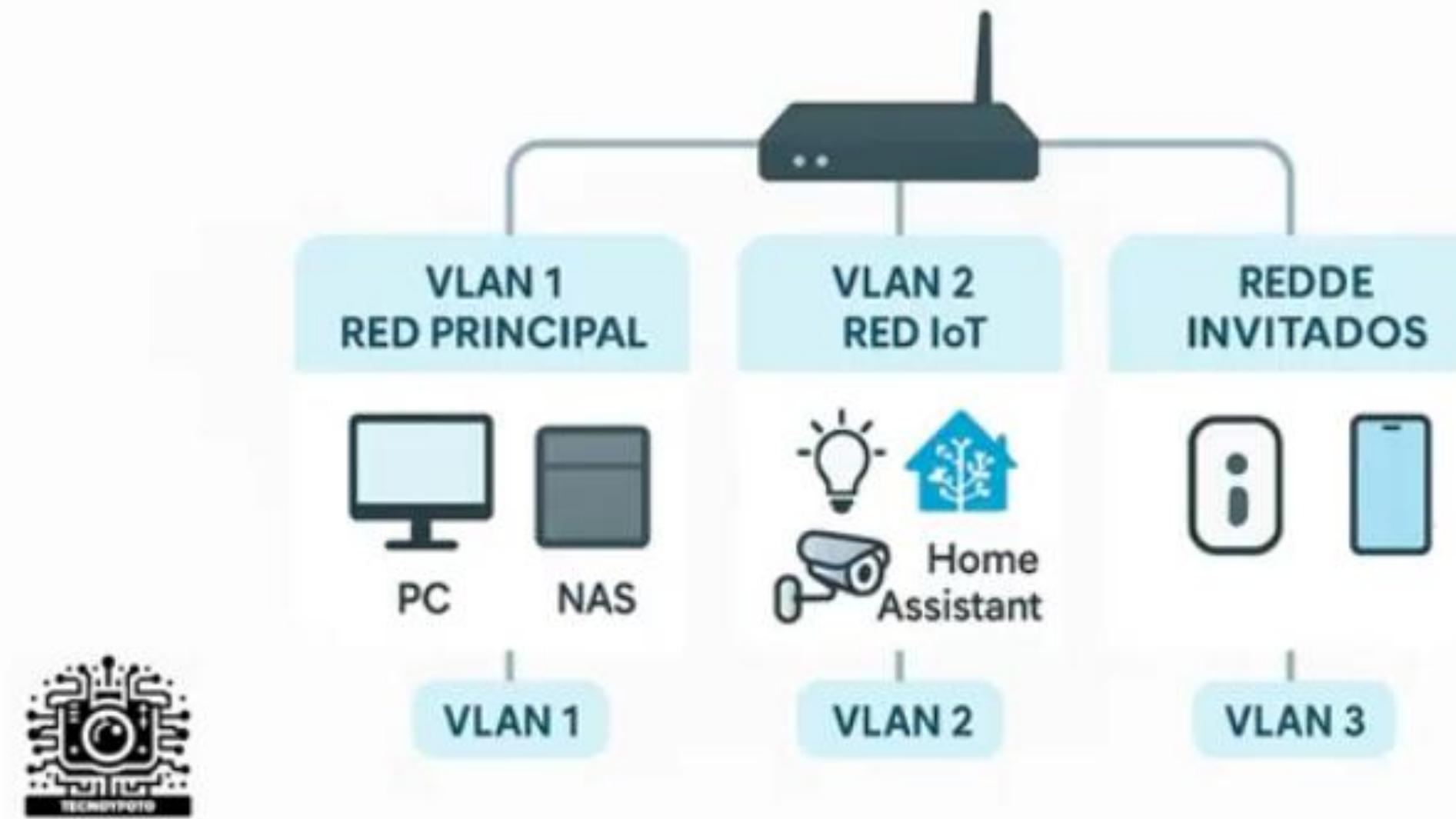


Finanzas
PCs y sistema contable



Invitados
Para visitantes y dispositivos móviles

Ejemplo de red doméstica segmentada



La segmentación de red no solo es útil para grandes empresas; incluso redes domésticas pueden beneficiarse al implementar este enfoque para separar dispositivos críticos de otros de menor importancia

Segmentación empresarial

Mejoras en la seguridad mediante la segmentación

Al segmentar una red, se establece una barrera natural que puede contener posibles amenazas y proteger los datos confidenciales de manera más efectiva.

Esta práctica actúa como un sistema de contención, limitando el acceso de posibles atacantes solo a segmentos específicos.



Optimización del rendimiento de la red

La segmentación también beneficia al rendimiento de la red.

Al limitar el tráfico de datos a los segmentos necesarios, se disminuye la congestión, lo que resulta en un acceso a la red más rápido y eficiente.

Esto es especialmente útil en redes de alta demanda.

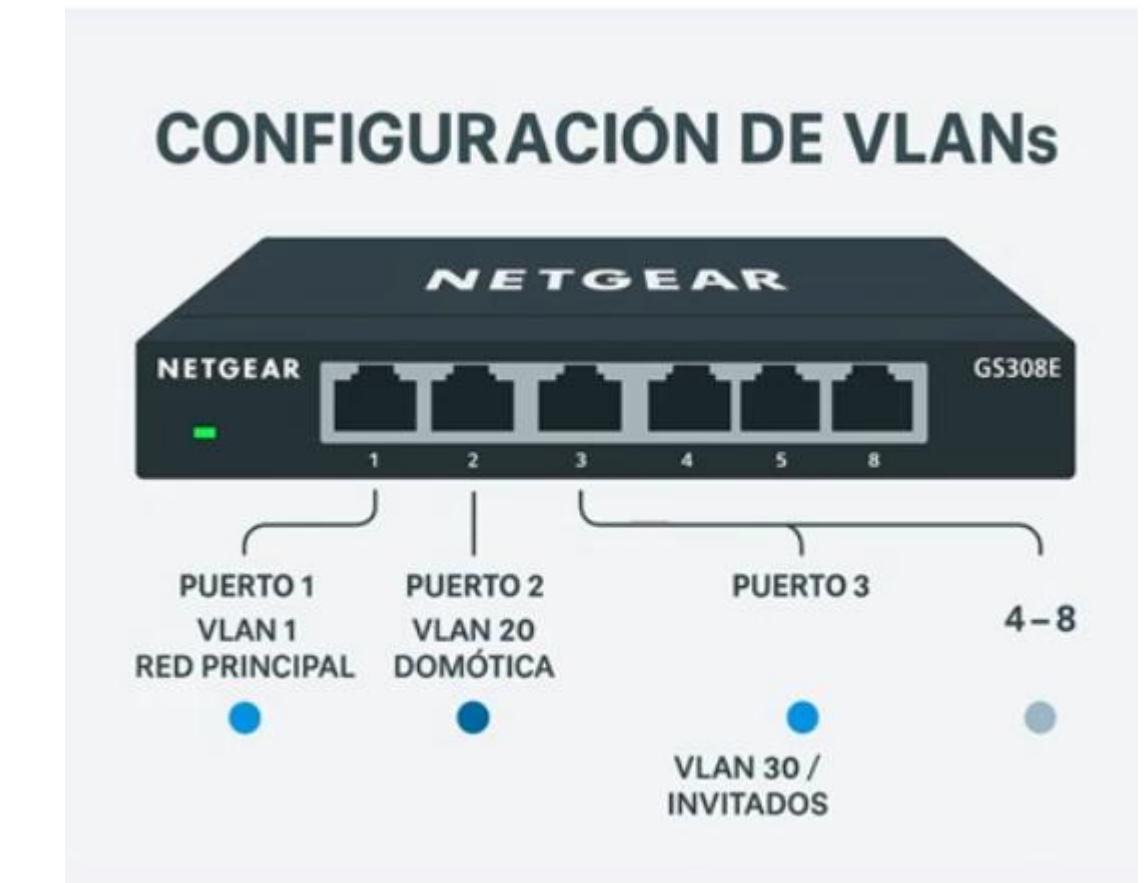
Una segmentación adecuada permite utilizar técnicas avanzadas como el **balanceo de carga** y la **calidad de servicio (QoS)**, que optimizan el tráfico hacia los segmentos prioritarios. Por ejemplo, en un entorno empresarial, podrías priorizar el tráfico de videoconferencias sobre el tráfico de **navegación** regular.

Segmentación de la red mediante VLANs

Las **Redes de Área Local Virtual (VLANs)** permiten separar lógicamente una red física en múltiples subredes, cada una actuando como una red independiente.

Esto es particularmente útil para mejorar la seguridad y el rendimiento dentro de una misma organización.

- **Flexibilidad:** Las VLANs permiten una gran adaptabilidad, ya que se pueden reconfigurar sin necesidad de cambiar físicamente el hardware.
- **Seguridad mejorada:** El tráfico entre VLANs puede ser controlado a través de listas de control de acceso (ACL), protegiendo datos sensibles.



Ejemplo:

Imagina un campus universitario: mediante VLANs, puedes segmentar el tráfico de la facultad, los estudiantes y el personal administrativo, asegurando que cada grupo tenga acceso solo a los recursos necesarios.

Segmentación de redes IPv4

La segmentación de redes IPv4 implica dividir una dirección IP de red en varias subredes más pequeñas.

Esto se logra mediante el uso de máscaras de subred, lo que optimiza el uso de direcciones IP y mejora la gestión del tráfico.

- **Escalabilidad:** Permite crear subredes más pequeñas para diferentes departamentos o ubicaciones geográficas.
- **Eficacia en la dirección:** Optimiza el uso de direcciones IP, reduciendo el desperdicio.

EJEMPLO:

Si una compañía tiene una red IPv4 con la dirección 192.168.1.0/24, puedes dividirla en varias subredes más pequeñas como 192.168.1.0/28
192.168.1.16/28,

cada una destinada a diferentes sucursales.

Ejemplo de segmentación en una empresa multinacional

Cada oficina regional puede tener su propia subred, conectada a través de una red de área amplia (**WAN**).

Esto permite a cada oficina gestionar su propio tráfico mientras se mantiene conectada a la oficina central.

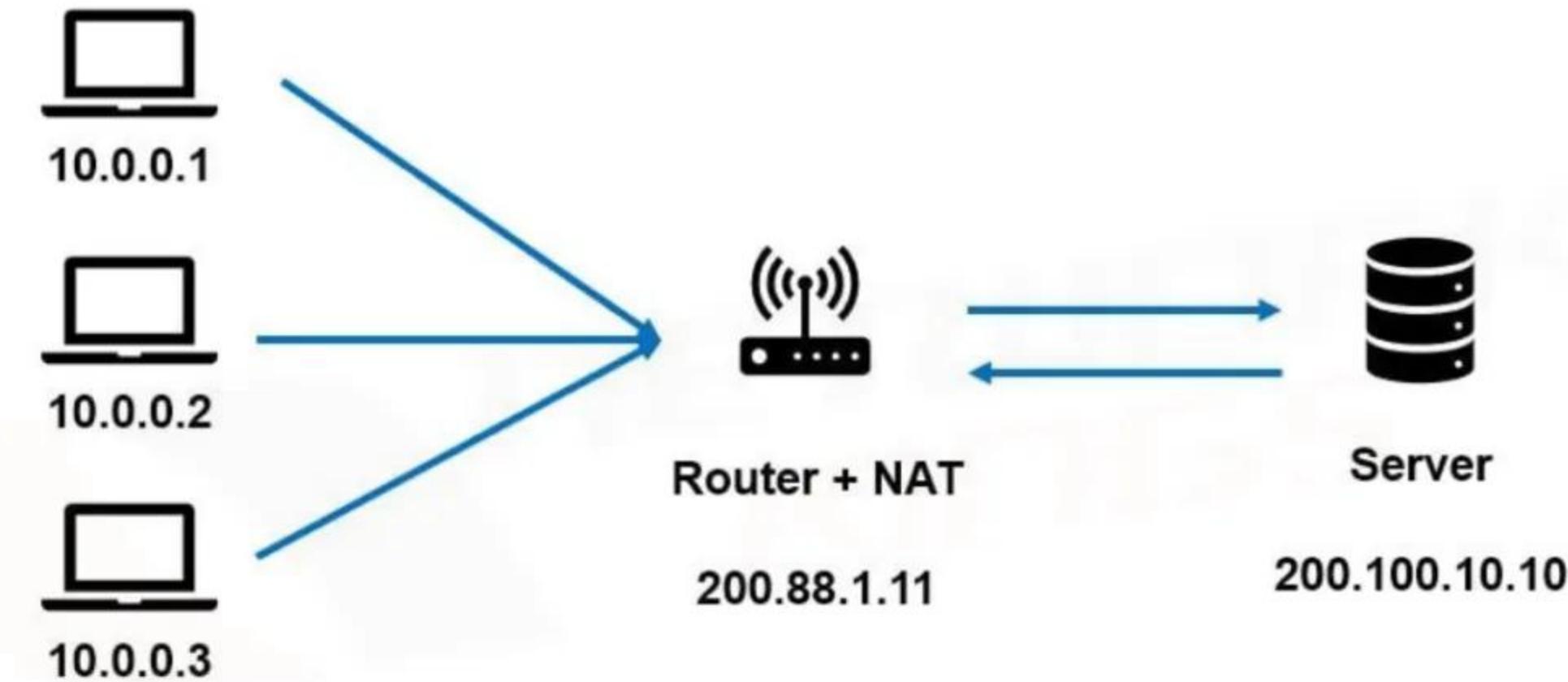
- Reducción de la carga de tráfico mediante la segmentación de sucursales.
- Implementación de políticas de seguridad específicas para cada región.
- Facilitación del acceso seguro a recursos corporativos compartidos.

Un ejemplo típico:

la sede de una empresa tecnológica ubicada en Nueva York utiliza una red 10.0.0.0/8, y cada oficina satélite, como las de Londres y Tokio, tiene segmentos 10.1.0.0/16 y 10.2.0.0/16 respectivamente.

Esto permite un mejor enrutamiento y gestión del tráfico.

Cómo es la arquitectura NAT?



Devices behind the
router with private IP
addresses

www.nwkings.com

El **dominio interno** está compuesto por los hosts o dispositivos con direcciones IP privadas. El **dominio externo** está compuesto por el servidor.

La solicitud del host se envía desde el origen con una dirección IP privada y se convierte a una dirección IP pública al llegar a la dirección IP de destino mediante NAT. Por lo tanto, el NAT funciona en línea recta.

Pasos clave para una segmentación efectiva.

- Identificación de Activos: Clasificar datos y activos según su valor y sensibilidad.
- Mapeo de Flujos: Entender cómo se comunican los datos y los usuarios a través de la red (Tráfico Norte-Sur y Este-Oeste).
- Definición de Zonas de Confianza: Crear grupos lógicos (p. ej., Servidores Web, Bases de Datos, Dispositivos IoT, Red de Invitados, Usuarios Finales).
- Implementación de Políticas: Usar Firewalls o VLANs para establecer políticas de control de acceso estricto entre segmentos, permitiendo solo el tráfico esencial.
- Auditoría y Monitoreo: Realizar revisiones periódicas de las políticas y monitorear el tráfico entre segmentos para detectar anomalías.

En resumen:

- **Segmentación de red:** Proceso de dividir una red grande en subredes más pequeñas para mejorar seguridad, eficiencia y administración.
- **Técnicas de segmentación:** Incluyen subredes, VLANs y firewalls para controlar y proteger el tráfico.
- **Seguridad mejorada:** La segmentación de red ayuda a limitar la propagación de amenazas y proteger datos sensibles.
- **Optimización del rendimiento:** Al reducir el tráfico innecesario, mejora la velocidad y capacidad de respuesta de la red.
- **Segmentación de redes IPv4:** Usa máscaras de subred para dividir direcciones IP en subredes, optimizando su gestión.
- **Ejemplos de segmentación de red:** Usada en empresas para separar departamentos y aumentar el control accesos a recursos específicos.