TEMA 7

Formato de una dirección IPv4:

Tienen 32 bits: cuatro campos de 8 bits (octeto) separados por puntos (por ejemplo, 192.168.0.1).

Una dirección IPv4 tiene dos partes:

* Identificador de red: la parte de la dirección que identifica la red donde se encuentra el equipo.
* Identificador de host: nombre del PC en la red.

Máscara de subred IPv4:

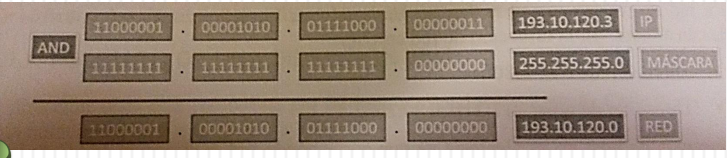
* Se usa para diferencias los bits de red de los de host en una dirección IPv4.
* La máscara formada por 32 bits de los que tendrán el valor ‘1’ los que identifican la red y ‘0’ los que identifiquen el host.



Dirección de Red IPv4:

* Se obtiene poniendo a cero todos los bits de host de una dirección IP.
* Dirección formada por 32 bits de los que tendrán el valor ‘1’ los que identifican la red y ‘0’ los que identifiquen el host.

Se puede obtener la dirección de red de una dirección IP si realizamos la operación AND de la IP y su máscara de red



Dirección de Boadcast IPv4

La dirección de broadcast Ipv4 es una dirección especial para cada red que permite la comunicación a todos los host en esa red.

La dirección de broadcast utiliza la dirección más alta en el rango de la red. Ésta es la dirección en la cual los bits de la porción de host son todos1 (se obtiene poniendo a uno todos los bits de host de una dirección de red IP.)

**Direcciones IP públicas**: Son direcciones IP únicas e irrepetibles en Internet.

**Direcciones IP privadas**: Son aquellas que se dejan para uso privado a nivel de red internamente. De forma que pueden existir varias empresas que usen para configurar su red la misma dirección IP.

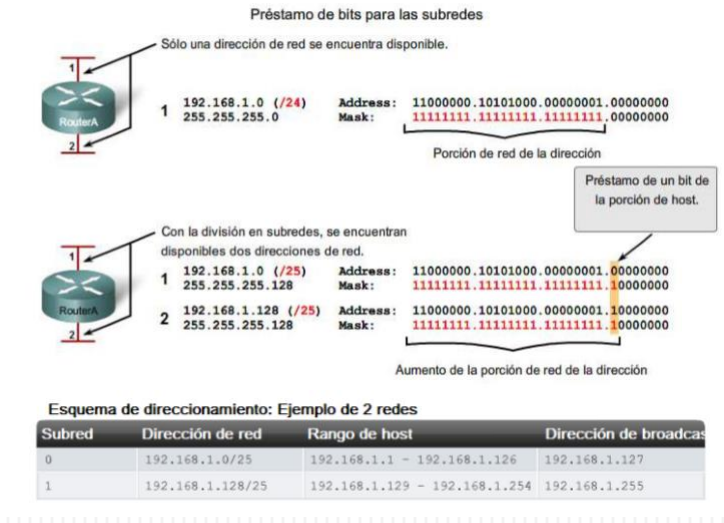
Traducción de direcciones de red (NAT)

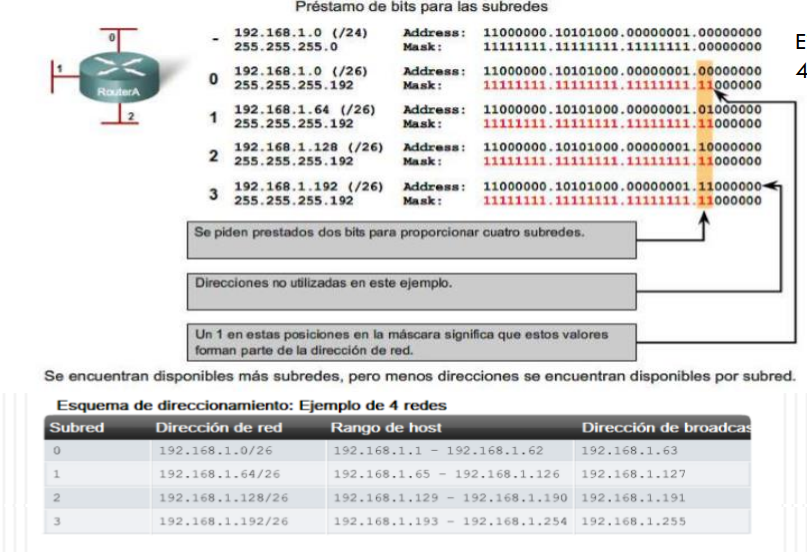
Con este servicio para traducir las direcciones privadas a direcciones públicas, los hosts en una red direccionada en forma privada pueden tener acceso a recursos a través de Internet. NAT permite a los hosts de la red “pedir prestada” una dirección pública para comunicarse con redes externas.

DIVISIÓN EN SUBREDES

La división en subredes permite crear múltiples redes lógicas de un solo bloque de direcciones.

Creamos las subredes utilizando uno o más de los bits del host como bits de la red. Esto se hace ampliando la máscara para tomar prestado algunos de los bits de la porción de host de la dirección, a fin de crear bits de red adicionales. Cuanto más bit de host se usen, mayor será la cantidad de subredes que puedan definirse.





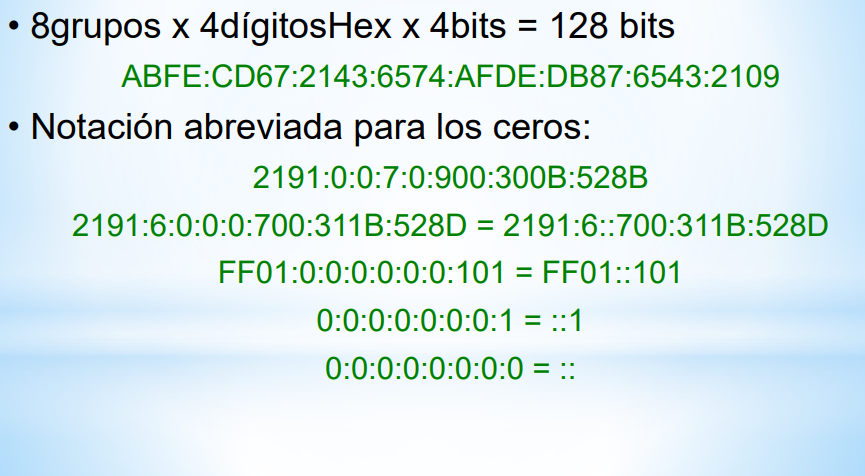
IPV6

Direcciones de 128 bits. • Capacidad de direccionamiento = 2¹²⁸. 667.134.927.874.467.426.204.012 direcciones.

Parece suficiente para hacer frente a cualquier necesidad presente y futura

Tipos

|  |  |  |
| --- | --- | --- |
| UNICAST | MULTICAST | ANYCAST |
| un paquete enviado a esta dirección es recibido sólo por el propietario de la dirección. | es el sustituto del broadcast de IPv4. Diferencia, broadcast envía paquetes a todos los equipos que se encuentran en la misma subred. Multicast envía paquetes solo a los equipos que tienen la misma dirección multicast. | una dirección para varios dispositivos. Un paquete enviado a esta dirección, se entrega al equipo más cercano propietario de dicha dir. |



Direcciones Unicast Globales (RFC 4291)

* Direcciones reconocidas a nivel global,
* Equivalen a las direcciones públicas IPv4.
* Empiezan por 001, por lo que el prefijo es 2000::/3
* Si una dirección empieza por 0010 o por 0011, estaremos ante una dirección unicast global

COMANDOS

IPCONFIG ->comprobar tu ip

Ping -> mandas paquetes a la ip que pongas ej ping 8.8.8.8 (le mandas paquetes a google)

ARP ->

TRACERT -> seguir la pista a los paquetes tracert Google.es

NETSTAT -> muestra un listado de las conexiones activas

NSLOOKUP -> muestra la ip conociendo el nombre y viceversa

Herramientas de monitorización de la red

Las herramientas para la monitorización de una red de comunicaciones pueden ser muy variadas: desde dispositivos que analizan la señal que circula por un cable a programas que monitorizan todo el tráfico de los enlaces.

1. **Comprobadores de red:** se utilizan para comprobar la continuidad en un cable u otros parámetros más avanzados.
2. **Monitores de red:** muestran un mapa de la actividad de la red en un intervalo de tiempo determinado
3. **Analizadores de red:** son dispositivos parecidos a los monitores de red pero que son capaces de comprender y mostrar la información que lleva cada mensaje

Redes inalámbricas

Las redes inalámbricas o WLAN (Wireless Local Area Networks) utilizan ondas electromagnéticas como medio de transmisión.

Aunque se pueden usar como una alternativa a las redes cableadas, es más frecuente emplearla como una extensión de las mismas.

Ventajas

* **La movilidad y libertad** de movimientos de los equipos.
* **La facilidad de implementar** la red en un tiempo mucho menor que el que llevaría una red convencional
* **La flexibilidad**, porque con la misma facilidad con que se instala, se desinstala.

Desventajas

* **Alcance.** Afectado por todo tipo de circunstancias
* **Velocidad de transmisión**. Dependiente del número de puestos de la red. Interferencias.
* **Seguridad.** Vulnerabilidades no existentes en redes cableadas.

Podemos encontrar múltiples configuraciones de una WLAN

Redes Ad Hoc

Modo infraestructura.

Modo infraestructura con Roaming.

Modo Repetidor.

Modo Bridge.

Redes Ad Hoc

se utiliza para conectar mediante Wi-Fi dos dispositivos de forma sencilla.

Modo infraestructura.

Los puestos se conectan a un nodo central llamado punto de acceso (AP). El punto de acceso se encarga de reenviar la información al resto de los nodos.

El Punto de Acceso se conecta a una red cableada, permitiendo que las máquinas inalámbricas se comuniquen con las de dicha red cableada

Modo infraestructura con Roaming.

en esta configuración existen varios puntos de acceso pertenecientes a una misma red, de forma que se pueda cubrir un área mayor.

El dispositivo que se conecta a la red es capaz de ir cambiando de un punto de acceso a otro según la potencia de la señal emitida y sin pérdida de la conexión.

Modo Repetidor.

En esta configuración existen varios puntos de acceso pertenecientes a una misma red, pero sólo uno de ellos está conectado a la red cableada

El resto de los Aps repiten la señal emitida por el primero para ampliar el alcance de la red inalámbrica.

Modo Bridge

En esta configuración se crea un puente entre dos redes distintas. Cada AP sólo se comunicará con el otro.

Se emplea típicamente cuando se desea conectar dos edificios de una forma económica y sin grandes requisitos de velocidad o calidad del servicio

Cifrado WPA/WPA2

Algoritmos más seguros: TKIP, AES, tanto por el algoritmo en sí como por el aumento de la longitud de las claves, lo que dificulta los ataques.

Rotación automática de claves. Cada cierto tiempo el AP y el cliente negocian una nueva clave de cifrado

Ámbito personal y empresarial:

* WPA/WPA2 PSK: Una única clave que conocen todos para autenticarse en la red.
* WPA/WPA2 Empresarial: Introduce un servidor RADIUS donde poder almacenar un usuario y una clave para cada empleado.

Para evitar accesos no deseados a una WLAN pueden tomarse las siguientes medidas básicas:

1. Ocultar el SSID. ∉ Deshabilitar el servidor DHCP.
2. Filtrado por dirección MAC.
3. Usar una clave WPA2 con una password larga, de complejidad suficiente y que no aparezca en los diccionarios de claves. (Las claves WEP son fácilmente vulnerables).
4. Usar WPA2 Enterprise en lugar de WPA2 Personal si estás en un entorno empresarial para evitar ataques internos. (Servidor Radius)