Capítulo 20

Redes Privadas

Al terminar este capítulo, entenderás:

- Qué es una red privada y por qué es útil.
- Los diferentes tipos de redes privadas: LAN, interredes privadas, redes híbridas, intranets y extranets.
- Qué es el direccionamiento privado y cuáles son bloques de direcciones reservadas.
- Qué el NAT, qué problema resuelve y cuáles provoca.

Una red privada, tal como su nombre indica, es una red[1] de uso privado. Su objetivo principal suele ser compartir recursos dentro de una organización, por lo que todos los elementos físicos que conforman la red (computadores, dispositivos de interconexión, cableado, etc.) están bajo el control exclusivo[2] de dicha organización, y por tanto, también es responsable de su diseño, implementación, gestión y explotación.

El concepto «red privada» no es equivalente a «red aislada». La red privada más común hoy día es la red WiFi doméstica que encontramos en la mayoría de los hogares y que, obviamente, está conectada a Internet a través del llamado router doméstico y la red del ISP.

20.1. Líneas alquiladas

También una interred puede ser privada, es decir, puedosmo tener una colección de LAN interconectadas mediante routers, ya sea en una o varias localizaciones, todo eso bajo el control y gestión de una misma organización (eso es lo que la hace privada). Durante las años 80 a 90, cuando Internet no existía o era demasiado caro, era habitual que muchas empresas tuvieran una red privada que conectaba las LAN de sus oficinas (por ejemplo,

[1] Habitualmente una LAN

[2] No necesariamente debe ser su propietario.

los concesionarios de una marca de automóviles). Para conectar estas oficinas entre sí, la organización podía instalar cableado propio o bien alquilar líneas a una compañía de telecomunicaciones. La primera opción solo era económicamente viable para distancias muy cortas (muy pocos cientos de metros). Este planteamiento es el que muestra la Figura 20.1.

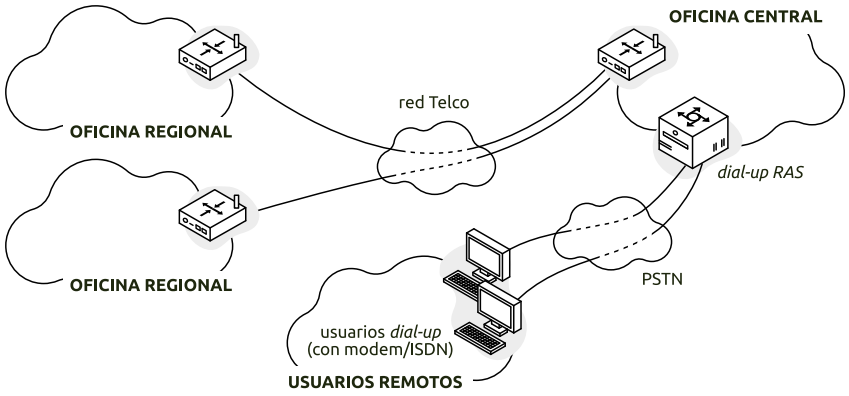

FIGURA 20.1: Red privada que utiliza líneas alquiladas

Cuando partiendo de una topología de este tipo, alguno de las oficinas tiene acceso a Internet puede ofrecer conectividad a algunas o todas las demás oficinas. Este esquema (que se muestra en la Figura 20.2) y es lo que se denomina *red híbrida*.

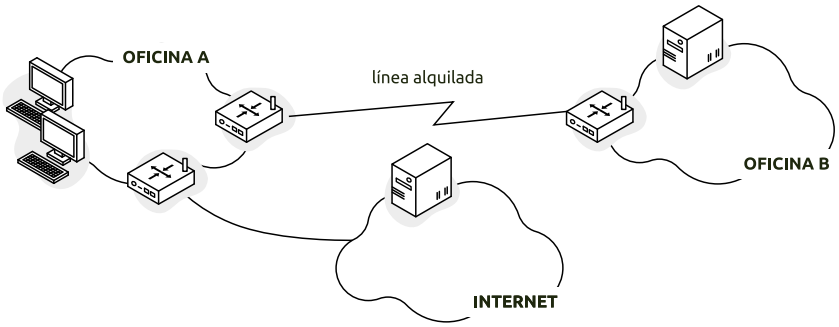

FIGURA 20.2: Red privada híbrida

20.2. Redes privadas TCP/IP

Precisamente por ser privada, la organización tiene plena libertad para elegir cualquier pila de protocolos disponible, o incluso implementar una tecnologías propia; algo común en redes de datos industriales.

En la práctica, parece buena utilizar la pila TCP/IP por variedad y disponibilidad de software, hardware de red, soporte y sobre todo, como forma de simplificar la conexión de la red privada con otras redes. La única razón para no utilizar TCP/IP es que la red privada es que no cumpla con algún requisito técnico específico.

Durante los primeros 90, Novel NetWare IPX tuvo gran popularidad como protocolo para redes privadas, debido a varios factores: tarjetas NIC asequibles, incorporación en Microsoft Windows, los primeros videojuegos multijugador en red (local) como *p. ej.* Quake, etc. Pocos años después, con la llegada de Internet, IPX fue desbancado rápidamente por IP.

Una *intranet* es justamente una red privada que utiliza tecnología TCP/IP y que únicamente es accesible para los dispositivos y usuarios de la organización. Sin embargo, el nombre *intranet* se utiliza hoy día, erróneamente, para identificar una o varias aplicaciones o servicios (normalmente web) destinados específicamente al personal de una organización para lo que requiere autenticación específica.

Como caso particular de *intranet*, la *extranet* permite a ciertos usuarios o servicios acceder a los recursos de la red privada desde el exterior. Este acceso está controlado mediante algún sistema de autenticación y autorización.

20.2.1. Direccionamiento privado

Como la red privada es responsabilidad exclusiva de la organización, ésta tiene la libertad de elegir cómo plantear el direccionamiento de sus dispositivos. El diseñador de la red privada tiene tres alternativas:

- Solicitar un bloque de direcciones públicas globales. Implica realizar una petición, y su correspondiente pago, a las autoridades de Internet: IANA o las entidades regionales FIXME RIR en las que haya delegado la tarea de asignación de direcciones. Si la red privada está aislada, o al menos sus computadores no van a proporcionar servicios hacia Internet, puede ser un gasto injustificado.

- Utilizar un bloque público arbitrario sin conocimiento de las autoridades. Si efectivamente la red privada va a estar esencialmente aislada, no supone ningún problema técnico, pero puede plantear graves problemas logísticos y administrativos si en el futuro esa red acaba formando parte de Internet.
- Utilizar uno de los bloques reservados específicamente para redes privadas.

Esta tercera alternativa es la recomendada por las autoridades según la RFC 1918 [34] y consiste en la elección arbitraria de uno de los bloques definidos en el Cuadro 20.1. A estas direcciones se las denomina simplemente «direcciones privadas».

inicio		fin	prefijo CIDR
10.0.0.0	-	10.255.255.255	10 /8
172.16.0.0	-	172.31.255.255	172.16 /12
192.168.0.0	-	192.168.255.255	192.168 /16

CUADRO 20.1: Bloques IP reservados para direccionamiento privado

La direcciones privadas deben ser consideradas *no rutables* en Internet, es decir, los routers del ISP y de la WAN en general descartarán cualquier paquete IP que tenga como destino una dirección privada. Precisamente por esto, cualquier organización puede elegir uno de estos bloques privados sin necesidad de autorización. Aunque existan millones de redes alrededor del mundo que estén utilizando exactamente el mismo bloque no hay problema, ya que su tráfico nunca podrá ser confundido con el de otra red. Es decir, las direcciones privadas deben ser localmente únicas, pero al contrario de las públicas, no son globalmente únicas.

Aunque el núcleo de Internet (esencialmente BGP) y los ISP descarten este tráfico, la organización puede encaminarlos dentro de su interred corporativa. Esto le otorga gran flexibilidad a la organización, pudiendo crear varias subredes interconectadas para diferentes propósitos o comunidades de usuarios.

20.3. Conectividad en redes privadas

Las redes domésticas actuales, y la mayoría de las que se utilizan en empresas y organizaciones pequeñas y medianas, técnicamente son *redes privadas híbridas con tecnología TCP/IP*. En una red doméstica, el ISP proporciona un dispositivo (ver Figura 20.3), que llamamos informalmente como *router doméstico*. Este router es el que proporciona la conexión de tus dispositi-

vos a Internet. En realidad ese dispositivo (esa caja) es más que un router. Incorpora normalmente varios dispositivos y funciones:

- Un router IP con 2 interfaces: LAN y WAN.
- Un conmutador Ethernet.
- Un punto de acceso WiFi.
- Un módem que puede utilizar distintas tecnologías: ADSL, SDSL o actualmente fibra óptica con FTTH, HFC y otras. En las conexiones de fibra, el módem puede ser un dispositivo aparte llamado ONT o estar integrado también en la misma caja.
- Un pequeño computador habitualmente con una alguna variante de Linux empotrado.
- Un servidor DHCP.

En la figura puedes ver las conexiones del router doméstico. El primer conector de la derecha (WAN) conecta el equipo con el ONT. Los conectores amarillos numerados de 1 a 4 son los puertos del conmutador Ethernet incorporado. Y la antena, es parte del punto de acceso WiFi.

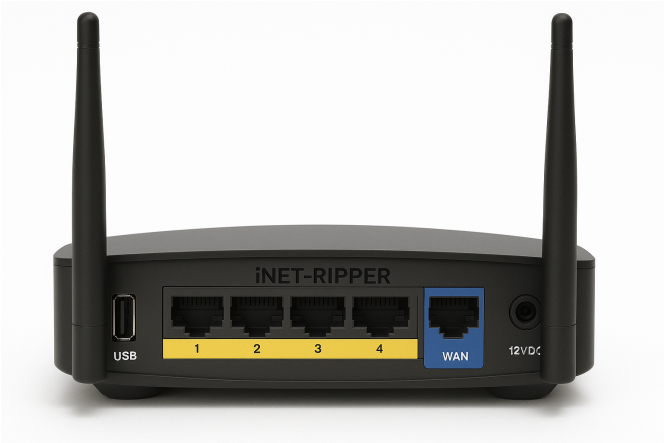

Figura 20.3: Conexiones de un router doméstico

Cuando conectas tu computador, móvil, televisor, etc. —sea con Ethernet o WiFi— el servidor DHCP incorporado le asigna una dirección privada. El bloque de direcciones configurado suele ser `192.168.0.0/24`, aunque puede ser cualquiera del Cuadro 20.1, y normalmente el propio usuario tiene la posibilidad de cambiarlo accediendo a la web de administración del router.

Si como hemos dicho, la Internet pública descarta los paquetes IP dirigidos a direcciones privadas ¿cómo pueden entonces estos nodos comunicarse con

servidores públicos? La solución consiste en *traducir* las direcciones privadas a direcciones públicas al salir de la red privada. Esta traducción la realiza un proceso llamado NAT que se ejecuta en el router doméstico, y por eso se le llama «router NAT».

20.3.1. Traducción de Direcciones de Red (NAT)

NAT (Network Address Translation) [35] es un programa (software) que interconecta la red privada con la red del ISP, y traduce (reescribe) las direcciones de los paquetes IP que reenvía. La topología es similar a la Figura 20.4. El router NAT tiene una interfaz WAN (la que conecta con la red del ISP) con una dirección IP pública (*p. ej.* `180.20.30.13`) y una interfaz LAN con una dirección privada (`192.168.0.1`) que, como en la figura, suele ser la primera del bloque. Los tres nodos tienen direcciones privadas del mismo bloque `192.168.0.0/24` asignadas por el servidor DHCP.

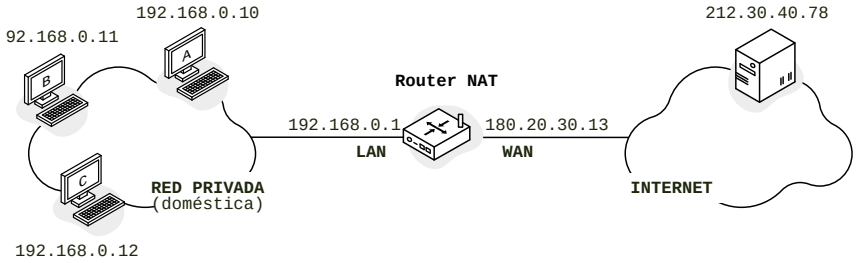

FIGURA 20.4: Ejemplo de configuración NAT en una red doméstica

El uso más habitual de NAT es el que permite a los nodos de la red privada establecer conexiones con servidores de la red pública. Es el llamado SNAT que se muestra en la Figura 20.5. Si por ejemplo, el nodo A quiere conectar con un servidor público, cuando sus paquetes IP salen de la red, el router substituye la dirección **origen**[3] (privada) por la dirección pública (WAN) del router. Al volver la respuesta procedente del servidor remoto, el router substituye la dirección destino (que es la pública del router) de nuevo por la dirección privada del nodo (ver Figura 20.5). Ten en cuenta que este mecanismo es transparente para el servidor y para cualquier otro elemento en Internet, es decir, ni participan ni son conocedores de que esta traducción está ocurriendo.

Para que la traducción de la respuesta funcione, el router debe saber cuál de los computadores de la red privada hizo la petición. Para ello, el soft-

[3]Por eso se llama *Source* NAT

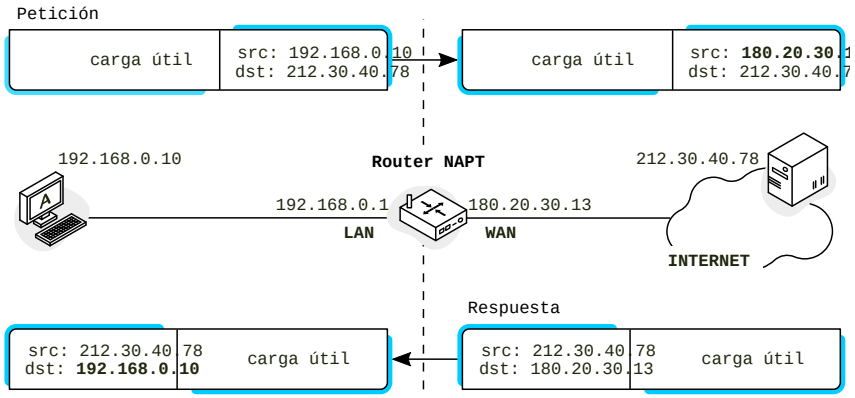

FIGURA 20.5: Ejemplo de SNAT

ware NAT apunta en la tabla NAT[4] esas correspondencias en el momento de hacer la traducción de salida. Lógicamente, estas entradas en la tabla desaparencen tras un tiempo de inactividad o bien cuando se detecta el cierre de la conexión (si es que el flujo es TCP). El Cuadro 20.2 muestra la tabla tras dos conexiones desde los nodos `A` y `B` a dos servidores remotos diferentes.

Dirección local	Dirección remota
192.168.0.10	212.30.40.78
192.168.0.12	200.25.34.56

CUADRO 20.2: Tabla NAT para el envío de la Figura 20.5

Sin embargo, la información de esta tabla es insuficiente. Tiene una limitación muy importante. La traducción de direcciones en la respuesta es ambigua si dos o más nodos de la red privada contactan con el mismo servidor remoto a la vez. Es ambigua en el sentido de que el router no tiene forma de saber qué nodo privado fue el que envió la petición que corresponde a esta respuesta.

Para reducir esta ambigüedad existe una técnica mejorada denominada NAPT (Network Address Port Translation) [36]. Consiste en incorporar a la tabla NAT los puertos origen y destino TCP o UDP. La probabilidad de que dos nodos de la red privada elijan el mismo puerto origen en conexiones simultaneas a un mismo servidor remoto es realmente muy baja, y ese sería el único caso en el que se presentaria la ambigüedad. La Figura 20.6 y la Tabla 20.3 ilustran esta técnica.

[4]Formalmente: *Address Translation Table*

Dirección local	P. local	Dirección remota	P. remoto	Proto
192.168.0.10	4045	180.20.30.13	80	TCP
192.168.0.12	32400	130.0.23.12	22	TCP

CUADRO 20.3: Tabla NAPT para el envío de la Figura 20.6

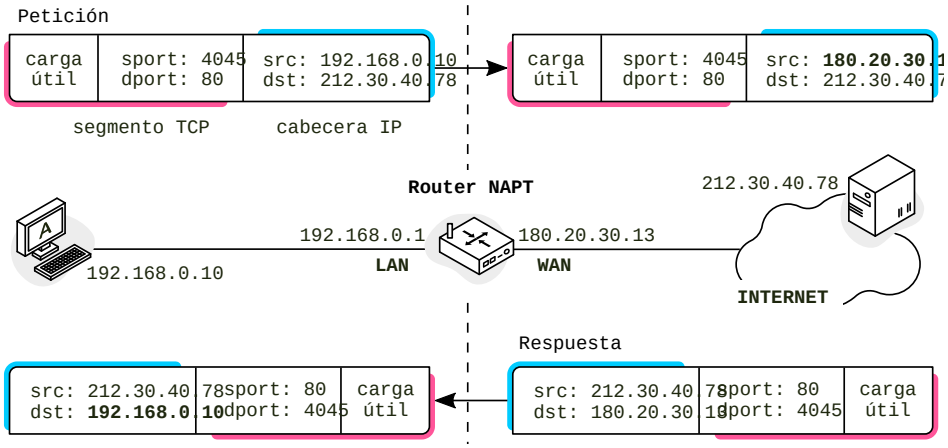

FIGURA 20.6: Ejemplo de NAPT

En todo caso, muchas implementaciones de NAT optan por evitar completamente la ambigüedad traduciendo el puerto del cliente local por un puerto ficticio que el router puede elegir garantizando así que será único en la tabla. Este puerto se conoce como «puerto mapeado» o «sintético». Esta situación se muestra en la Figura 20.7 y la Tabla 20.4.

Dirección local	P. local	**P. mapeado**	Dirección remota	P. remoto	Proto
192.168.0.10	4045	7312	180.20.30.13	80	TCP
192.168.0.12	32400	45012	130.0.23.12	22	TCP

CUADRO 20.4: Tabla NAPT con puertos mapeados para el envío de la Figura 20.6

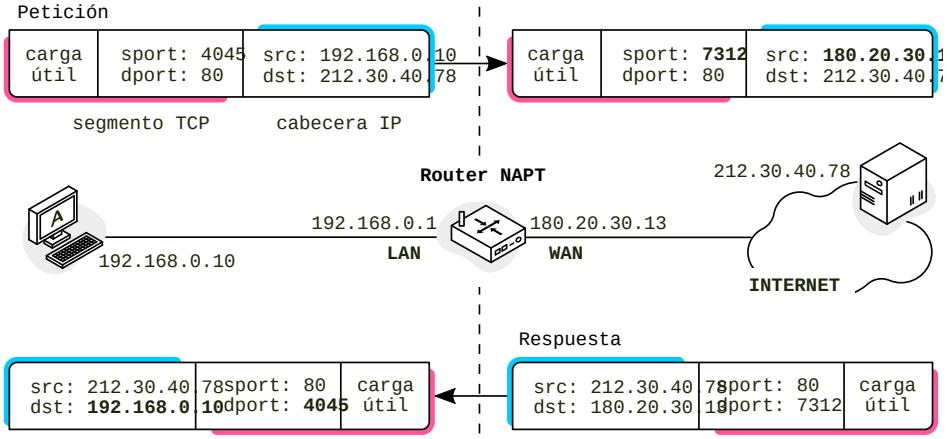

FIGURA 20.7: Ejemplo de NAPT con puertos mapeados

20.4. Reenvío de puertos

Otro inconveniente de NAT, que NAPT tampoco resuelve es que todo el mecanismo se basa en que el router aprende del tráfico saliente de la red privada, y usa esa información para realizar la traducción inversa. Eso implica que no es posible poner servidores en los nodos privados que puedan ser alcanzados desde clientes fuera de la red privada. Para resolver esto, el router proporciona un medio para incluir filas permanentes en la tabla NAT.

Estas entradas en la tabla se conocen como «reenvío de puertos» *(port forwarding)*. Ten en cuenta que en este caso, el router traduce la dirección IP destino, en lugar de la origen, y por eso se denomina *Destination NAT* (DNAT). Como esta configuración está pensada para dar acceso a un servidor interno, lo habitual es que el usuario que crea una entrada DNAT en la tabla indique tanto el puerto destino del router como el puerto destino del nodo privado, que es donde realmente hay un servidor vinculado.