Tema 2 - Xarxes Privades Virtuals

Sergi Robles

Sergi.Robles@uab.cat

Departament d'Enginyeria de la Informació i de les Comunicacions
Universitat Autònoma de Barcelona

Tecnologies avançades d'Internet

Contingut

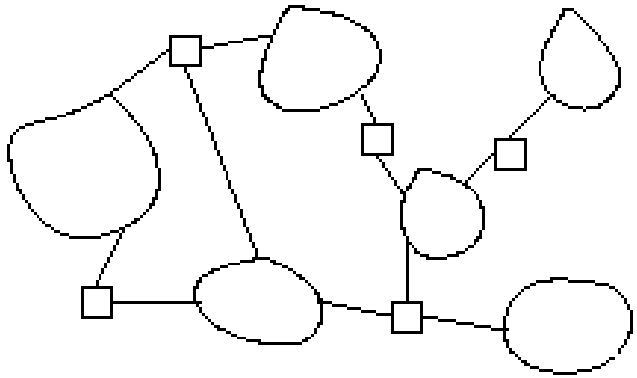
Contingut

Fins ara hem vist una internet interconnectada per routers en una arquitectura d'un nivell.

Ara veurem arquitectures de dos (o més) nivells, on podem tenir xarxes privades interconnectades a través d'altres i, fins i tot, a través d'Internet.

Esquema actual:

- Les dades estan "en clar".
- Adreçament únic.
- Infraestructura compartida.



Veurem dues tecnologies que ens permetran solucionar els problemes de:

1. **privacitat de la informació** interna,
2. de la **compartició d'infraestructures**
3. i de la **limitació de l'espai d'adreçament**

- Xarxes Privades Virtuals (VPN, *Virtual Private Network*).
- Conversió d'adreces de xarxa (NAT, *Network Address Translation*).

L'escenari més usual on es veuen aquests requisits és el de l'empresa que té seus distribuïdes geogràficament.

Datagrames **Interns**: Datagrames en els que l'origen i el destí pertanyen a la mateixa organització.

Datagrames **Externs**: Altres datagrames, que poden tenir l'origen o (exclusiva) el destí en l'organització.

Recordem que anomenem **internet** a qualsevol xarxa que utilitza la *suit* de protocols TCP/IP per a la comunicació. **Internet** (amb majúscula) és la internet d'abast mundial que passa per la UAB.

intranet

Una **intranet:** és una xarxa internet destinada exclusivament al transport de datagrames interns.

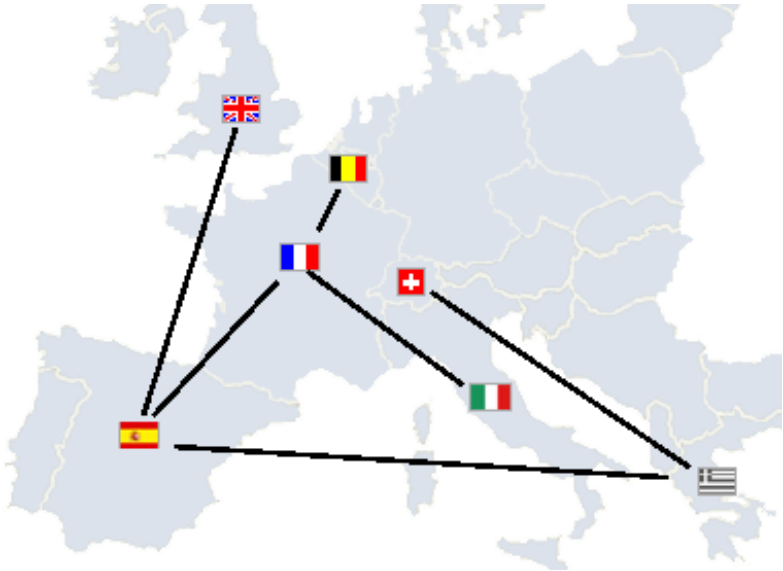
extranet

Una **extranet:** és la part d'una intranet que és parcialent accessible des de l'exterior, normalment des d'Internet.

Contingut

Existeixen dues solucions per afrontar el problema: xarxes totalment privades i xarxes privades virtuals.

Xarxes Privades



- Tots els routers són propis.
- S'utilitzen línies dedicades d'ús exclusiu.
- Es pot utilitzar qualsevol rang d'adreces IP, mentre aquestes siguin úniques dins l'organització.

Existeix un variant: Xarxes Privades Híbrides.

Xarxes Privades Híbrides

En les xarxes híbrides hi ha un accés a Internet. En aquest cas, caldrà que el rang d'adreces utilitzades sigui vàlid a Internet!

En general les xarxes privades resulten molt costoses (principalment per la contractació i manteniment de les línies dedicades).

→ L'alternativa és utilitzar la mateixa xarxa Internet per a la interconexió: Xarxes Privades Virtuals (VPN).

Contingut

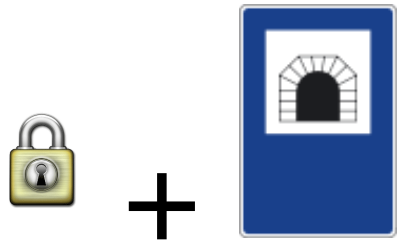
Xarxes Privades Virtuals

Una Xarxa Privada Virtual (*Virtual Private Network*, VPN) és un tipus concret de xarxa privada: la seva funció principal serà el transport de tràfic intern (de l'organització).

→ La principal diferència entre una VPN i una xarxa privada tradicional és la substitució de les línies de comunicació dedicades per Internet.

Aquesta solució és molt més econòmica i robusta!

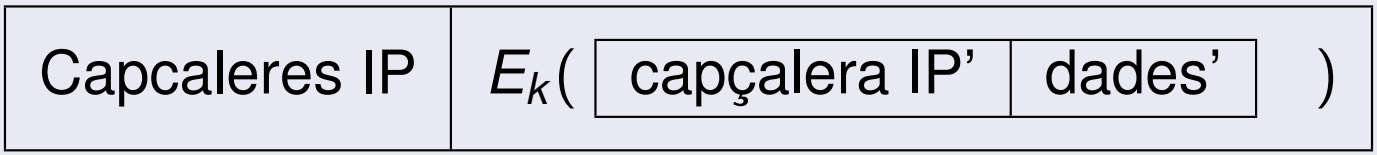
Per a conseguir les VPN es combinen dos mecanismes: Encapsulació (*Tunneling*) i Xifrat.



- **Xifrat:** Ocultar a terceres parts de la comunicació la informació que es transmet, mitjançant l'ús de tècniques criptogràfiques.
- **Tunneling:** Encapsulació de datagrames en altres protocols per a que aquests puguin travessar una xarxa determinada i continuar el seu trajecte després.
  - Exemples de tunneling són GRE i IP-in-IP.

Un túnel en una VPN és diferent a un túnel normal, ja que normalment s'utilitzen tècniques pel xifrat dels continguts.

Túnel

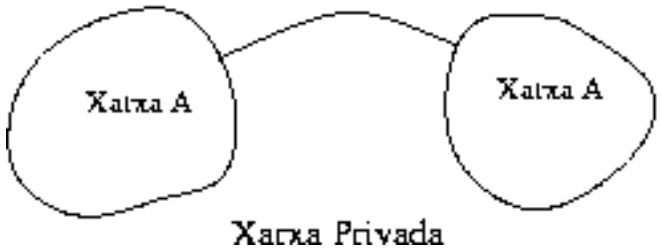


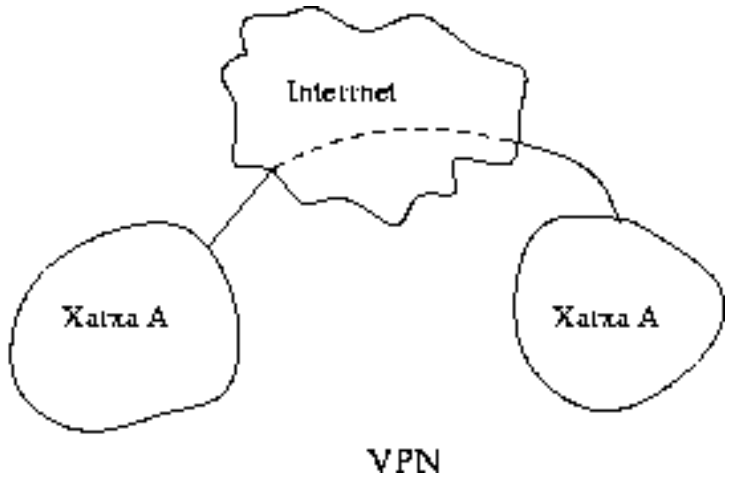
- El routers que travesa el datagrama no "veuen" el contingut.
- L'origen i el destí van també xifrats! Només seran visibles les adreces dels extrems del túnel.

Contingut

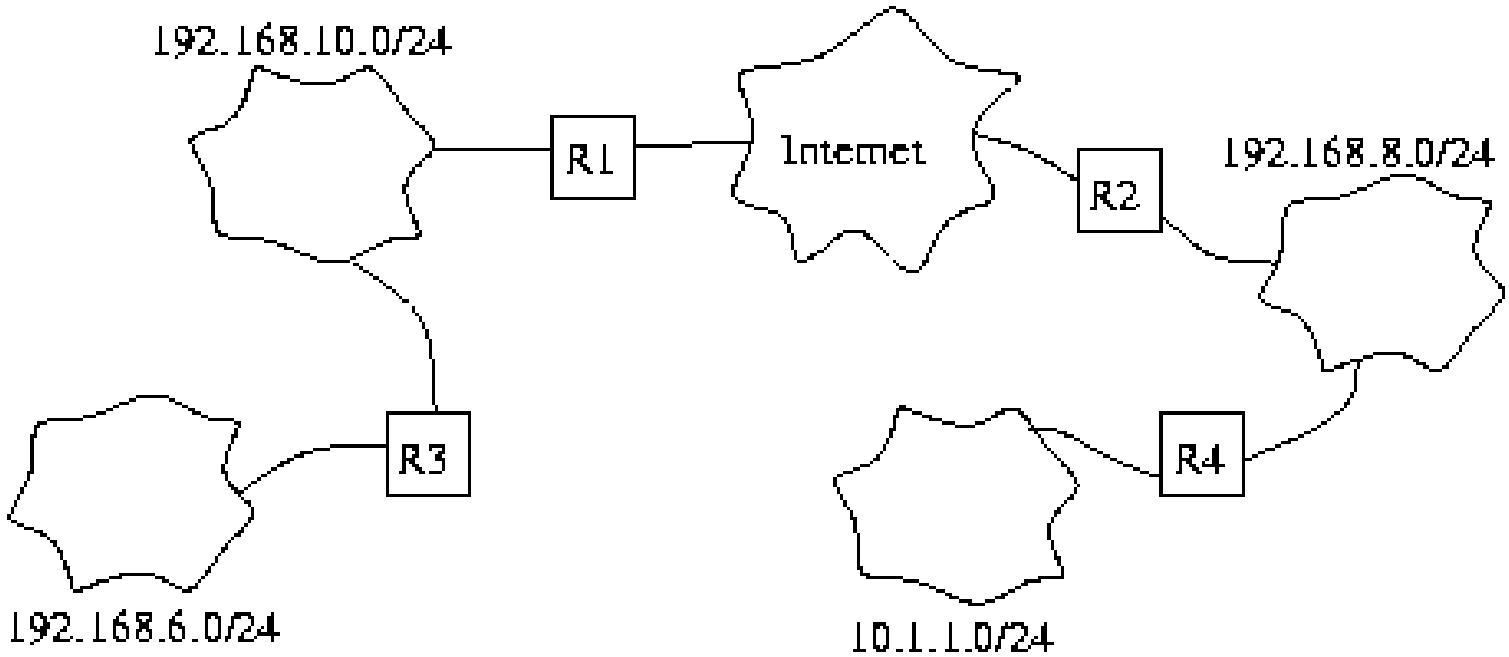
Si pensem en cada túnel com en una enllaç dedicat, l'encaminament serà com a les xarxes privades:

→ Els routers tenen rutes explícites per a les destinacions dintre de l'organització.





Exemple



Taula R1

192.168.10.0/24	*	eth0
192.168.6.0/24	R3	eth0
192.168.8.0/24	R2	tun0
10.1.1.0/24	R2	tun0

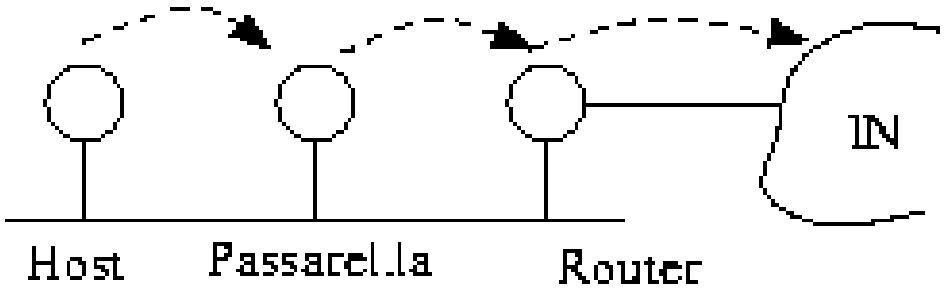
Si la VPN no ha d'estar connectada a Internet, podem utilitzar adreces arbitraries, però **els extrems del túnel han de ser adreces vàlides** a Internet.

Si la VPN ha d'estar també connectada a Internet, podem tenir un esquema d'adreçament híbrid.

Hi ha dos enfocs per la connexió VPN-Internet:

- Application Gateways (proxies d'aplicacions).
- Conversió d'adreces de xarxa (NAT)

Els *Gateways* d'aplicacions són hosts que accediran a la Internet en nom de hosts interns per a que aquests puguin utilitzar serveis externs.



- Aquesta passarel·la d'aplicació necessita tenir una adreça IP vàlida a Internet.
- Per a cada aplicació hi haurà d'haver una passarel·la.
- Hi ha serveis que podran ser transparents (com HTTP), però d'altres que no.

→ L'altre enfoc, NAT, el veurem en la següent secció.

Contingut

Una de les maneres de solucionar el problema d'accés a Internet des de xarxes privades sense utilitzar adreces IP globals és **NAT**.

Amb NAT només és necessària una adreça IP global per a connectar un conjunt de hosts a Internet.

$\rightarrow$ Aquesta IP la tindrà un router que connectarà la xarxa privada a Internet i que correra el software de NAT.

La idea bàsica darrera del NAT és convertir els datagrames que surten i que entren de la xarxa privada substituint l'adreça d'origen en els datagrames que surten i la de destinació dels que entren.

Substitucions a NAT

IP_{NAT}: Adreça IP del host que fa NAT.

Datagrama cap a Internet:	Datagrama cap a xarxa privada:
Origen=IP_{NAT}	Destinació=Adreça interna.

El software de NAT ha de mantenir els canvis al llarg de les connexions.

Com es veu NAT des de ...?

→ Des d'Internet:

- Tots els datagrames semblen venir des del host que fa NAT. Totes les respostes aniran també cap a aquest host.

→ Des de la xarxa privada:

- De manera transparent al seu funcionament, el host que fa NAT es veu com un router normal que connecta cap a la Internet.

Principals avantatges de NAT:

Generalitat: Pot adaptar-se a moltes situacions diferents. Qualsevol host intern podrà utilitzar qualsevol servei d'un host d'Internet.

Transparència: Els hosts que pertanyen a la xarxa privada no han de tenir coneixement del mecanisme que s'està utilitzant. Poden utilitzar sense problemes les seves adreces internes.

En resum:

NAT ofereix accés a Internet a nivell d'IP des d'una xarxa privada de manera transparent.

Fins ara hem vist *què* és NAT. Ara veurem *com* funciona.

L'aspecte clau del funcionament és com pot rebre un host de la xarxa privada un datagrama que vingui d'Internet.

$\rightarrow$ Per a fer això, NAT manté una taula de conversió que utilitzarà per a fer la correspondència.

Taula conversions

Cada entrada a la taula conté dos elements bàsics:

- L'adreça IP del host a Internet.
- L'adreça IP del host a la xarxa privada.

Quan un datagrama arriba d'Internet es substitueix l'adreça IP de destí segons aquesta taula.

Contingut

Si la taula de NAT no conté entrades, els datagrames d'Internet no poden arribar al destinatari correcte (el host que fa NAT no sap re-encaminar-lo).

I doncs, com s'inicialitza la taula de NAT?

Hi ha varies possibilitats:

- **Inicialització manual:** L'administrador configura aquesta taula abans de que comencin les comunicacions.

  $\rightarrow$ ***Avantatge:*** Les correspondències són permanents i per tant els datagrames poden ser enviats sempre en qualsevol direcció.

- **Per datagrames de sortida:** La taula es contrueix com a efecte dels datagrames que s'envien. Quan el host que fa NAT rep un datagrama de la xarxa privada crea l'entrada corresponent.

  → ***Avantatges:*** És automàtic, no cal administrar-la manualment.

  → ***Inconvenients:*** Les comunicacions no poden ser iniciades des d'Internet.

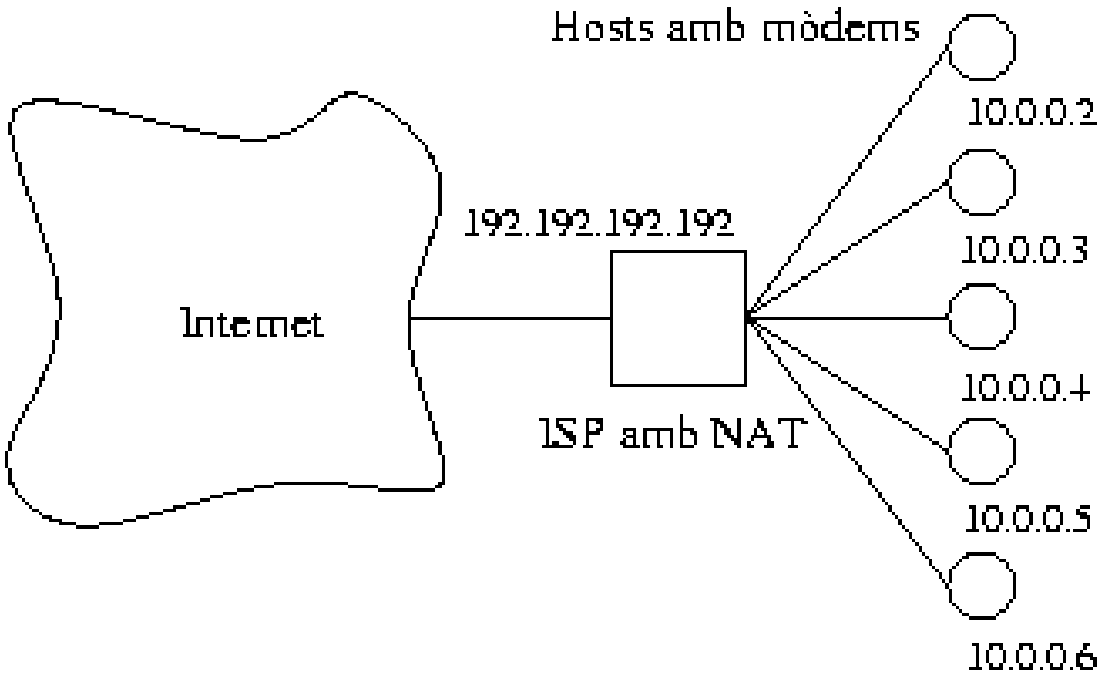
- **Per búsqueda de domini del host intern:** La taula es contrueix com a efecte de les búsquedes al DNS del nom del host intern. El software de DNS crea l'entrada a la taula i després ofereix la seva adreça IP.

  → ***Avantatges:*** És automàtic i permet comunicacions iniciades des d'Internet.

  → ***Inconvenients:*** S'ha de modificar el software de DNS. Només funciona si l'origen fa una búsqueda del domini abans d'enviar.

Normalment s'utilitza la inicialització per datagrames de sortida.

L'exemple típic és el d'un ISP que disposa d'una adreça IP global i que utilitza NAT per a oferir accés a Internet a usuaris que es connecten amb mòdem.



Contingut

El NAT que hem vist fins ara és molt simplísta: només fem una correspondència entre adreces de la xarxa privada i d'Internet (una a una).

$\rightarrow$ Aquest esquema només permet l'accés a un host d'Internet com a molt des d'un host intern!!

Les implementacions que trobem de NAT són més complexes i permeten l'accés concurrent a un determinat host d'Internet.

En veiem dos enfocs diferents per solucionar això:

- **NAT multi-adreça**
- **NAT port-mapped**.

NAT multi-adreça

Aquest tipus de NAT manté la correspondència 1 a 1 entre adreces internes i adreces Internet, però permet accés concurrent.

En aquest esquema el host que fa NAT té k adreces globals a Internet.

$\rightarrow$ Quan el primer host de la xarxa privada accedeix a un host d'Internet, el host que fa NAT tria una de les k adreces i afegeix l'entrada a la taula. Si un altre host contacta amb el mateix host d'Internet, s'utilitza una altra adreça.

Es permet fins a k hosts interns accedir a la mateixa IP.

NAT port-mapped (amb correspondència de port)

NAT *port-mapped* és potser la variant més popular de fer NAT.

→ Consisteix en proporcionar concurrència a través de la utilització dels ports TCP o UDP juntament amb les adreces.

De vegades aquest esquema s'anomena NAPT (*Network Address Port Translation*).

Els routers ADSL normalment porten preconfigurat aquest tipus de NAT.

Juntament amb les adreces d'origen i destí es guarden els ports utilitzats d'origen i destí, i el de NAT.

Exemple:

IP int	port int	IP ext	port ext	port NAT
10.0.0.5	21023	128.10.19.4	80	14003
10.0.0.1	386	128.10.19.4	80	14010
10.0.2.6	26600	207.2.75.2	21	14012
10.0.0.3	1274	128.210.1.5	80	14007

Per cada entrada també es desa el protocol (UDP/TCP).

En l'exemple, les connexions TCP vistes des dels hosts 10.0.0.5 i 10.0.0.1 són aquestes:

```
(10.0.0.5, 21023, 128.10.19.4, 80) i
(10.0.0.1, 386, 128.10.19.4, 80).
```

Des de l'extrem remot (128.10.19.4), en canvi, es veuran aquestes connexions:

```
(159.110.71.161, 14003, 128.10.19.4, 80) i
(159.110.71.161, 14010, 128.10.19.4, 80).
```

on 159.110.71.161 és l'adreça del host que està fent el NAPT.

El principal **avantatge** del NAPT és que s'aconsegueix una generalització molt gran amb una única adreça IP global.

El **desavantatge** més gran és la restricció de l'esquema a les comunicacions TCP o UDP.

Si s'utilitza TCP o UDP, NAPT permet accedir des d'un host intern a múltiples hosts d'Internet, i a múltiple hosts de la xarxa privada accedir al mateix host d'Internet sense interferències.

Limitació per número de ports

$\rightarrow$ L'espai de ports disponible permet la comunicació de fins a 2^{16} parelles d'aplicacions de manera simultània, seguint la utilització clàssica.

Modes de funcionament de NAT

- **Tradicional, de sortida, o d'origen.** Els hosts de la xarxa privada accedeixen a la xarxa externa de manera transparent, iniciant ells la comunicació i el mecanisme de NAT.
- **NAT bi-direccional.** Les sessions poden ser començades per hosts interns o externs. És la utilització conjunta de NAT d'origen i NAT de destinació.
- **Doble NAT.** Tant l'adreça d'origen del datagrama com la de destí són substituides de manera simètrica. Normalment utilitzem doble NAT quan hi ha col.lisions entre espais d'adreçament.

Contingut

NAT i ICMP

Per a mantenir la transparència del NAT s'ha de tenir en compte ICMP.

Pensem en un *ping*, per exemple:

→ Quan fem un ping des d'un host de la xarxa privada a un host d'Internet esperem que arribi la resposta!

El host que fa NAT ha d'enviar la resposta de l'eco al host que ha fet la petició. Però no ha d'enviar tot el tràfic ICMP! Alguns missatges aniran al propi host NAT.

El primer que ha de fer un host NAT quan arriba un missatge ICMP és determinar si va a la xarxa privada o no.

→ Abans de re-enviar un missatge ICMP cap a un host intern ha de convertir-li les adreces que porta dintre!!.

Per a veure això podem considerar un missatge ICMP de "*host unreacheable*". El missatge porta la capçalera del datagrama que va causar l'error... amb les adreces canviades pel NAT!

EL host que fa NAT ha d'obrir el missatge ICMP, convertir les adreces segons la seva taula, recalcular checksums, i fer-li arribar al destinatari intern.

Els problemes amb ICMP fan que NAT no sigui tan trivial d'implementar com sembla a primer cop d'ull.

NAT i les aplicacions

El protocols que realment porten problemes seriosos són el de la capa d'aplicació. En general, **NAT no funcionarà amb les aplicacions que s'intercanviin adreces IP o ports com part de les dades**.

$\rightarrow$ El **FTP** (*File Transfer Protocol*), per exemple, no funcionarà bé amb NAT: Com a part del protocol s'envia un port en format ASCII a través de la connexió TCP. Aquest port és imprescindible pel protocol.

→ Per a que el protocol FTP funcionés, el host que fa NAT hauria d'obrir el flux de dades i substituir el port enviat pel port utilitzat realment.

Algunes implementacions de NAT reconeixen alguns protocols força coneguts com el FTP i fan les conversions adients. D'altres aplicacions no poden utilitzar NAT.

Canviar dades del flux de dades incrementa la complexitat de NAT en dos sentits:

- El mecanisme de NAT ha de tenir coneixement detallat del funcionament del protocol d'aplicació.

- Algun canvi de dades podria fer que el número de bytes a enviar sigui diferent (p.e. port 1203 passa a 28536). El host de la xarxa interna no sap d'aquest canvi (és transparent a la xarxa privada) i per tant utilitza els números de seqüència originals

$\longrightarrow$ NAT hauria de convertir números de seqüència en els segments de sortida i en els de confirmació al llarg tota la connexió!!

Interconnexió espais diferents

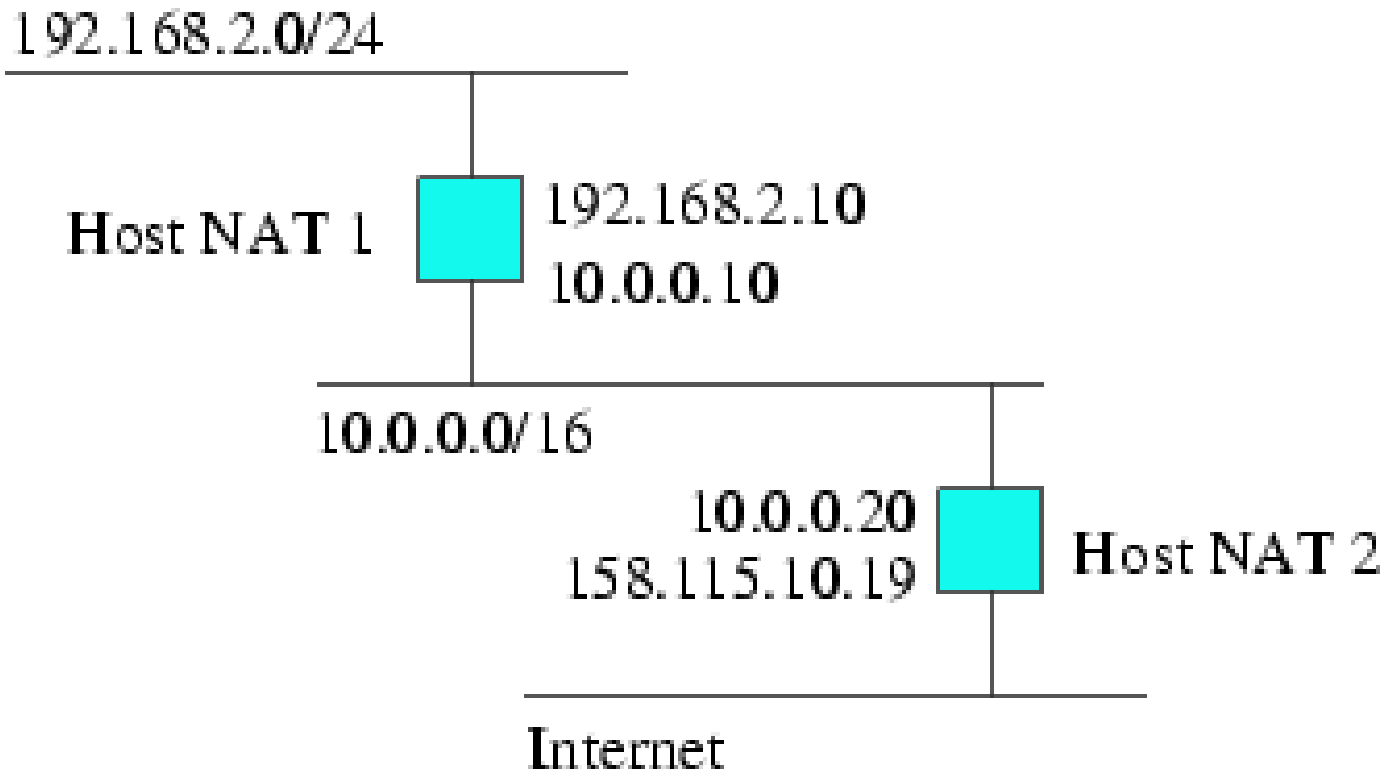
Amb NAT hem connectat fins ara una xarxa privada a Internet. NAT, però, **pot ser utilitzat per interconnectar dos espais d'adreçament qualsevols**.

Podríem utilitzar NAT, per exemple, per a interconnectar dues xarxes privades.

$\rightarrow$ Normalment NAT es combina amb VPN per a crear una arquitectura híbrida amb adreces privades que són utilitzades dins d'una organització i accés a Internet a través d'un host NAT.

NAT pot ser utilitzat en múltiples nivells.

Exemple de NAT a dos nivells:



Implementacions de NAT

Hi ha dues implementacions famoses de NAT:

- ***Slirp*:** Té l'origen en BSD 4.4. Està pensat per donar accés a Internet a una sèrie de hosts connectats per mòdem. Combina NAPT i PPP.
- ***Linux Masquerade, SNAT i DNAT*:** Aquesta és una de les implementacions més populars de NAT. Opera com un router entre dues xarxes i té implementades la majoria de les variacions NAT que hem vist.

SNAT NAT d'origen (Source NAT). Implementa l'esquema bàsic de NAT en el què l'origen activa el mecanisme en començar una comunicació.

DNAT NAT de destinació (Destination NAT). Aquí es fa l'esquema invers. El mecanisme de NAT s'activa quan una màquina de fora vol connectar a un host intern.

Masquerade Funciona com SNAT, però l'adreça d'origen a utilitzar és obtinguda dinàmicament de la interfície.

La comanda per utilitzar aquesta funcionalitat en Linux és **ipfwadm** (kernel 2.0), **ipchains** (kernel 2.2), o **iptables** (kernel 2.4 / 2.6).

El NAT ens aporta, com hem fins ara, moltes avantatges. Caldria incloure també la protecció de la xarxa interna:

$\rightarrow$ És més difícil realitzar atacs!

- El NAT sol actuar com un filtre que permet tràfic en un únic sentit (sense connexions amb origen extern).
- Els atacants no poden dirigir-se a un host concret de la xarxa privada.

És habitual trobat els routers que fan NAT treballant en combinació amb *firewalls* per a filtrar el tràfic no dessitjat.

Malgrat això, el NAT també porta alguns problemes.

Problemes amb NAT

- **Aplicacions peer-to-peer.** La mateixa adreça IP global (la del host NAT) és utilitzada per a referenciar diferents hosts interns.
- **Datagrames fragmentats.** Si dos hosts envien fragments que tenen el mateix identificador al mateix host extern, aquest no podrà determinar a quina sessió pertanyen.
- **Aplicacions amb IP o ports en payload xifrat.** Les aplicacions que s'intercanvien dades d'adreçament i que xifren el payload no podran utilitzar-se amb NAT.

- **Connexions segures a xarxa privada.** Les connexions segures, p.e. SSH, a més d'un host de la xarxa privada poden fallar, ja que seran vistes com un únic host que utilitza claus diferents.
- **Datagrames IPsec AH, ESP.** Aquest estàndard detecta alteracions en les capçaleres IP, precissament el que fa NAT. IPsec d'extrem a extrem no és possible amb NAT.
- **Protocol SNMP.** Aquest protocol, com veurem més endavant en el curs, utilitza adreces IP en el payload.

- **És més difícil trobar problemes de configuració.** Com part de la xarxa queda amagada, no resulta trivial determinar l'origen de certs malfuncionaments.
- **Detecció d'abusos a Internet.** L'origen d'un atac a un host d'Internet o el causant de l'enviament de grans quantitats de *spam* són més difícils de localitzar.
- **Augment considerable de la complexitat del re-encaminament.** La capacitat de procés del router pot causar un coll d'ampolla.

És possible saber quants hosts hi ha darrera d'un router que fa NAT?

S. M. Bellovin. *A Technique for Counting NATed Hosts*. Proc. 2nd Internet Measurement Workshop. 2002.