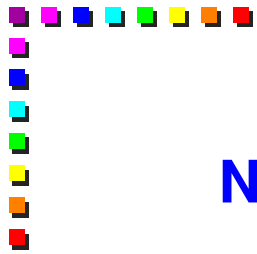


Network Address Translation

Pietro Nicoletti

www.studioreti.it



Nota di Copyright

- Questo insieme di trasparenze (detto nel seguito slides) è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali. Il titolo ed i copyright relativi alle slides (ivi inclusi, ma non limitatamente, ogni immagine, fotografia, animazione, video, audio, musica e testo) sono di proprietà degli autori indicati a pag. 1.
- Le slides possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione e al Ministero dell'Università e Ricerca Scientifica e Tecnologica, per scopi istituzionali, non a fine di lucro. In tal caso non è richiesta alcuna autorizzazione.
- Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente, le riproduzioni su supporti magnetici, su reti di calcolatori e stampate) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte degli autori.
- L'informazione contenuta in queste slides è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, reti, ecc. In ogni caso essa è soggetta a cambiamenti senza preavviso. Gli autori non assumono alcuna responsabilità per il contenuto di queste slides (ivi incluse, ma non limitatamente, la correttezza, completezza, applicabilità, aggiornamento dell'informazione).
- In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste slides.
- In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.



Indirizzi Privati RFC 1597 e RFC 1918

- Classe A (una sola rete)
 - rete: 10.x.x.x
- Classe B (16 reti adiacenti)
 - reti: 172.16.x.x ... 172.31.x.x
- Classe C (256 reti adiacenti)
 - reti: 192.168.0.x ... 192.168.255.x
- Dette anche 24 / 20 / 16-bit blocks
- ... e se si utilizzano altri indirizzi non ufficiali e non compresi in questi standard
 - fenomeno dell'accecamento

Intranet e Internet

- Cablaggio separato per la parte pubblica e privata
 - per ragioni di sicurezza
- Stessa sottorete per host con la stessa missione:
 - sottorete pubblica
 - sottorete privata
- Filtri sui router verso le reti pubbliche (FireWall)
 - si evita la propagazione di informazioni circa la rete privata
- Application gateway e proxy sugli host pubblici
 - forniscono l'accesso ai servizi pubblici agli host privati

NAT: Network Address Translator

■ Definito da:

- K. Egevang, P. Francis, "RFC 1631: The IP Network Address Translator (NAT)," Maggio 1994

■ Realizzato da:

- KA9Q TCP/IP software
- Cray Communications IP-router
- Cisco IOS dalla release 11.2

■ Limiti:

- non è idoneo per interconnettere due Intranet tramite Internet
 - utilizzare il tunneling

NAT: impieghi

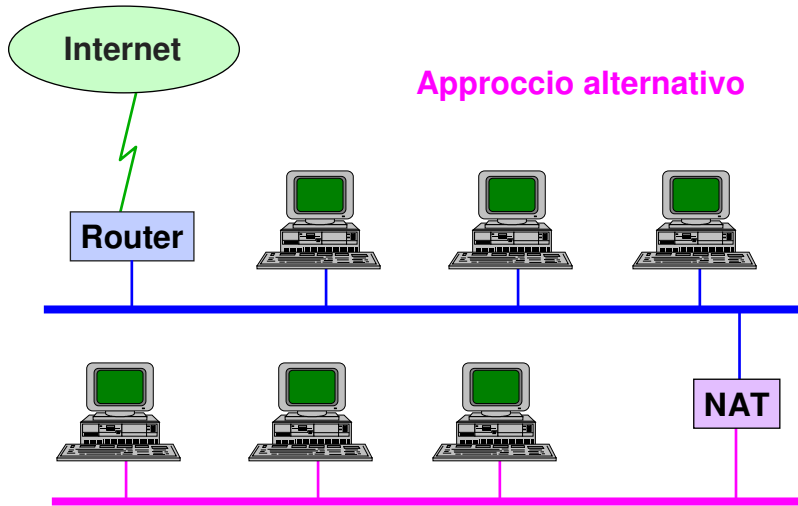
■ Mappare di indirizzi privati su un unico indirizzo pubblico o un pool di indirizzi pubblici

- risparmio di indirizzi pubblici
- sicurezza in quanto l'indirizzo privato non e' visibile da Internet

■ Mascherare un indirizzo con un altro indirizzo per ragioni di privacy e sicurezza

■ Assegnare un indirizzo pubblico a connessioni RAS utilizzando il primo indirizzo disponibile di un pool

NAT: Network Address Translator



NAT-Only - 7

Copyright: si veda nota a pag. 2

NAT: indirizzi privati e pool di indirizzi pubblici

```

ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255

```

NAT-Only - 8

Copyright: si veda nota a pag. 2

NAT: indirizzi privati mappati su un unico indirizzo pubblico

```

interface Ethernet0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
!
interface serial0
 ip address 211.1.40.1 255.255.255.252
 ip nat outside
!
ip nat inside source list 1 interface Serial0 overload
access-list 1 permit 192.168.10.0 0.0.0.255
!

```

NAT: indirizzi privati mappati su un unico indirizzo pubblico

```

router#sho ip nat translation

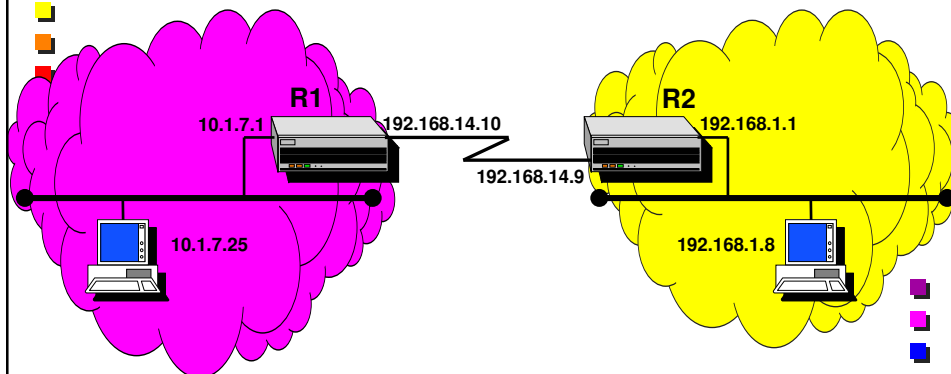
```

Pro	Inside global	Inside local	Outside local	Outside global
tcp	80.16.58.1:1056	192.168.10.4:1056	213.212.128.8:80	213.212.128.8:80
tcp	80.16.58.1:1027	192.168.10.166:1027	195.31.235.39:21	195.31.235.39:21
tcp	80.16.58.1:1028	192.168.10.166:1028	195.31.235.39:20	195.31.235.39:20
tcp	80.16.58.1:1098	192.168.10.4:1098	195.31.235.39:21	195.31.235.39:21
tcp	80.16.58.1:1099	192.168.10.4:1099	195.31.235.39:20	195.31.235.39:20
udp	80.16.58.1:137	192.168.10.166:137	151.99.125.2:53	151.99.125.2:53
udp	80.16.58.1:137	192.168.10.166:137	151.99.125.3:53	151.99.125.3:53
tcp	80.16.58.1:1058	192.168.10.4:1058	212.110.36.130:80	212.110.36.130:80
tcp	80.16.58.1:1059	192.168.10.4:1059	212.110.36.130:80	212.110.36.130:80
tcp	80.16.58.1:1060	192.168.10.4:1060	212.110.36.130:80	212.110.36.130:80

NAT: mascheramento di indirizzo IP

- Si utilizza quando c'è un conflitto di indirizzi tra 2 entità oppure non si vuol far conoscere il piano di indirizzamento ad un'organizzazione esterna
 - se si intende rendere visibile una macchina con un indirizzo diverso dal suo originale si effettua un NAT statico su quell'indirizzo
 - nell'esempio successivo si traduce l'indirizzo reale 10.1.7.25 nell'indirizzo 192.168.14.9
 - se si intende rendere visibile un certo numero di macchine con indirizzi diversi da quelli reali si devono effettuare n. traduzioni statiche
- In genere nella configurazione Cisco gli indirizzi reali appartengono alla parte *inside* e quelli tradotti alla parte *outside*

Esempio di NAT statico per ragioni di privacy



NAT: mascheramento di indirizzo IP su R1

```

!
ip nat inside source static 10.1.7.25 192.168.244.45
!
interface Ethernet0
 ip address 10.1.7.1 255.255.255.0
 ip nat inside
!
interface Serial0
 ip address 192.168.14.10 255.255.255.252
 ip nat outside
!
ip route 192.168.1.8 255.255.255.255 192.168.14.9
!

```

```

*****
router#sho ip nat translation
Pro Inside global   Inside local   Outside local   Outside global
--- 192.168.244.45   10.1.7.25     ---            ---

```

NAT-Only - 13

Copyright: si veda nota a pag. 2

Route mascherata su R2

```

!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0
 ip address 192.168.14.9 255.255.255.252
!
ip route 192.168.244.45 255.255.255.255 192.168.14.10
!

```

NAT-Only - 14

Copyright: si veda nota a pag. 2