Network Address Translation (NAT)

A.A. 2005/2006

Walter Cerroni

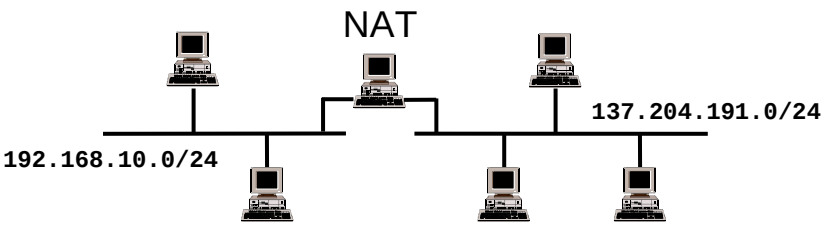
Reti IP private (RFC 1918)

- L'enorme numero di host (oltre 350 milioni nel 2005) connessi ad Internet sta rendendo il numero di indirizzi IP disponibili relativamente basso
- Utile l'adozione di **reti IP private** e di **tecniche di NAT**
  - alcuni gruppi di indirizzi sono riservati a **reti IP private**
  - essi non sono raggiungibili dalla **rete IP pubblica**
  - i router di Internet non instradano datagrammi destinati a tali indirizzi
  - possono essere riutilizzati in reti isolate
  - accesso alla rete IP pubblica attraverso NAT
- Reti IP private:
  - **10.0.0.0/8**
  - **da 172.16.0.0/16 a 172.31.0.0/16**
  - **da 192.168.0.0/24 a 192.168.255.0/24**

2

Network Address Translator (NAT)

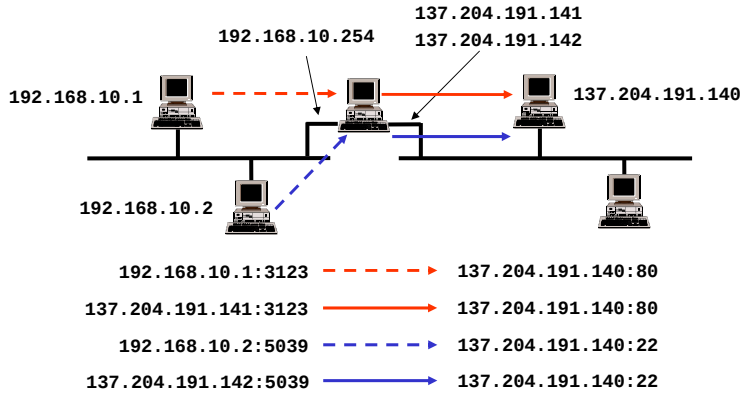
- Tecnica per il filtraggio di pacchetti IP con sostituzione degli indirizzi (mascheramento)
- Definito nella RFC 3022 per permettere a reti IP private l'accesso a reti IP pubbliche tramite un apposito gateway
- Utile per il risparmio di indirizzi IP pubblici e il riutilizzo di indirizzi IP privati e per aumentare la sicurezza



3

Basic NAT – Conversione di indirizzo

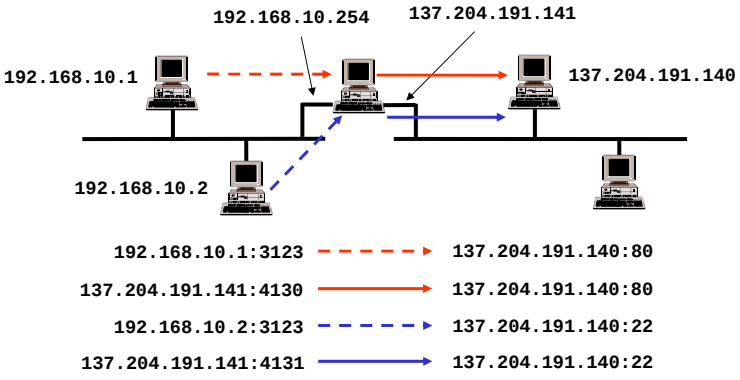
- Il NAT può fornire una semplice conversione di indirizzo IP (statica o dinamica)
- Conversioni contemporanee limitate dal numero di indirizzi IP pubblici a disposizione del gateway NAT



4

NAPT – Conversione di indirizzo e porta

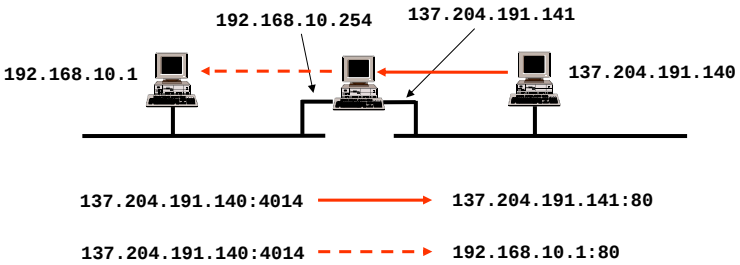
- Il NAT può fornire anche conversione di indirizzo IP e porta TCP o UDP
- Conversioni contemporanee possibili anche con un unico indirizzo IP pubblico del gateway NAT



5

Direzione delle connessioni

- Tipicamente da rete privata verso rete pubblica
  - il NAT si preoccupa di effettuare la conversione inversa quando arrivano le risposte
  - registra le traduzioni in corso in una tabella
- E' anche possibile contattare dalla rete pubblica un host sulla rete privata
  - bisogna configurare esplicitamente il NAT (**Port Forwarding**)



6

Trasparenza delle applicazioni

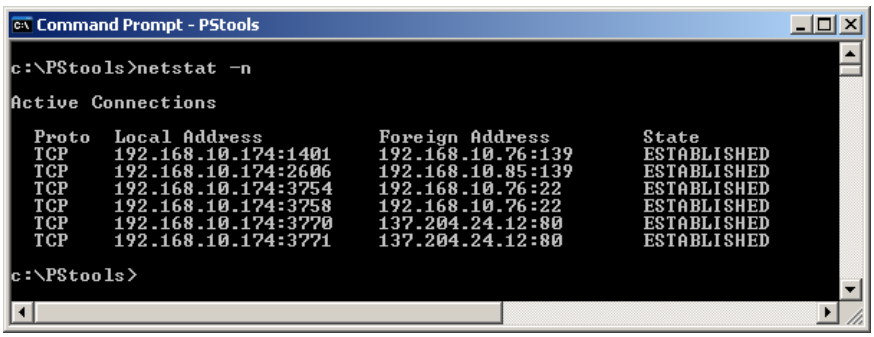
- Il NAT è indipendente dalle applicazioni
  - non altera il payload
- Alcune applicazioni non sono trasparenti al NAT
  - contengono indirizzi IP e numeri di porta nel payload
  - es.: FTP utilizza due connessioni parallele
    - connessione per l'interazione con il server tramite linea di comando (porta TCP 21)
    - connessione per il trasferimento dei dati da e verso il server
    - i parametri della seconda sono specificati nei dati trasmessi dalla prima
- Sono necessari gli **Application Specific Gateways** (**ALG**) per monitorare ed alterare il payload

7

Analisi di connessioni attraverso NAT

Connessione ad un server web

- client: 192.168.10.174
- server: 137.204.24.12
- NAT: 192.168.10.174 → 137.204.57.76



8

Analisi di connessioni attraverso NAT

Interfaccia di rete privata

NAT-int.cap - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.10.174	137.204.24.12	HTTP	GET /Ingegneria+Cesena/default.htm HTTP/1.
2	0.034608	137.204.24.12	192.168.10.174	TCP	80 > 3770 [ACK] Seq=3665385073 Ack=46511275 Win=1
3	0.896816	137.204.24.12	192.168.10.174	HTTP	HTTP/1.1 200 OK
4	0.896908	137.204.24.12	192.168.10.174	HTTP	Continuation
5	0.898068	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665387993 Win=6
6	0.899848	137.204.24.12	192.168.10.174	HTTP	Continuation
7	0.899971	137.204.24.12	192.168.10.174	HTTP	Continuation
8	0.900095	137.204.24.12	192.168.10.174	HTTP	Continuation
9	0.900913	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665389453 Win=6
10	0.901066	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665392373 Win=6
11	0.902676	137.204.24.12	192.168.10.174	HTTP	Continuation
12	0.902798	137.204.24.12	192.168.10.174	HTTP	Continuation
13	0.902921	137.204.24.12	192.168.10.174	HTTP	Continuation
14	0.903045	137.204.24.12	192.168.10.174	HTTP	Continuation
15	0.903168	137.204.24.12	192.168.10.174	HTTP	Continuation
16	0.903846	192.168.10.174	137.204.24.12	HTTP	GET /NR/Custom/web/Common/css/stile_main.c
17	0.903848	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665393833 Win=6
18	0.903850	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665396753 Win=6
19	0.904022	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665398213 Win=6
20	0.905643	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665399673 Win=6

9

Analisi di connessioni attraverso NAT

Interfaccia di rete pubblica

NAT-ext.cap - Ethereal

File Edit Capture Display Tools Help

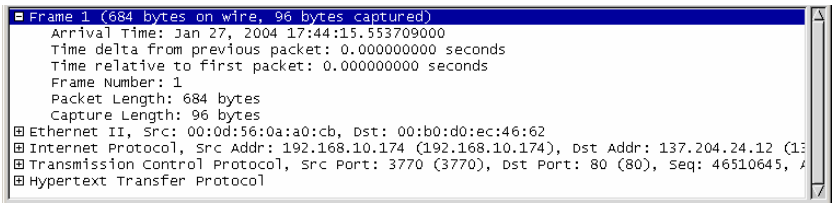
No.	Time	Source	Destination	Protocol	Info
1	0.000000	137.204.57.76	137.204.24.12	HTTP	GET /Ingegneria+Cesena/default.htm HTTP/1.
2	0.034559	137.204.24.12	137.204.57.76	TCP	80 > 3770 [ACK] Seq=3665385073 Ack=46511275 Win=1128
3	0.896736	137.204.24.12	137.204.57.76	HTTP	HTTP/1.1 200 OK
4	0.896859	137.204.24.12	137.204.57.76	HTTP	Continuation
5	0.898045	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665387993 Win=6424
6	0.899803	137.204.24.12	137.204.57.76	HTTP	Continuation
7	0.899925	137.204.24.12	137.204.57.76	HTTP	Continuation
8	0.900050	137.204.24.12	137.204.57.76	HTTP	Continuation
9	0.900889	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665389453 Win=6424
10	0.901042	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665392373 Win=6424
11	0.902630	137.204.24.12	137.204.57.76	HTTP	Continuation
12	0.902752	137.204.24.12	137.204.57.76	HTTP	Continuation
13	0.902875	137.204.24.12	137.204.57.76	HTTP	Continuation
14	0.903000	137.204.24.12	137.204.57.76	HTTP	Continuation
15	0.903122	137.204.24.12	137.204.57.76	HTTP	Continuation
16	0.903836	137.204.57.76	137.204.24.12	HTTP	GET /NR/Custom/web/Common/css/stile_main.c
17	0.903847	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665393833 Win=6424
18	0.903855	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665396753 Win=6424
19	0.903999	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665398213 Win=6424
20	0.905619	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665399673 Win=6424

10

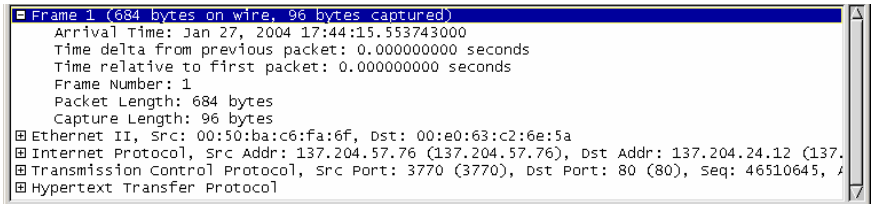
Analisi di connessioni attraverso NAT

client → server

pre-NAT



post-NAT

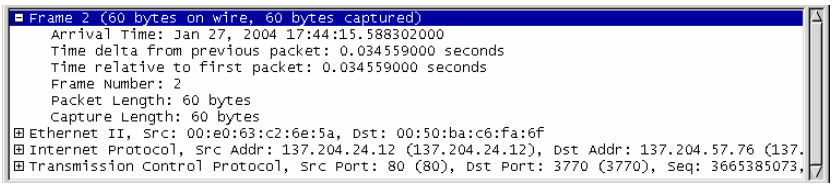


11

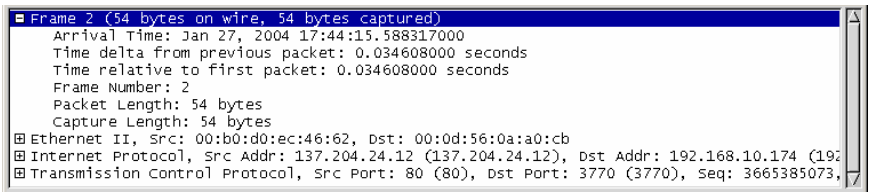
Analisi di connessioni attraverso NAT

server → client

pre-NAT



post-NAT



12