Azzolini Riccardo 2020-11-05

Network Address Translation

1 Network Address Translation

Il **NAT**, **Network Address Translation** è un software eseguito presso il *router di frontiera* di una LAN (il router al "confine" tra questa LAN e Internet), che effettua la traduzione tra gli indirizzi IP privati e pubblici.

Ogni host della LAN ha un indirizzo IP privato, che non è visibile dall'esterno della LAN, e non può quindi essere utilizzato per comunicare su Internet. Allora, grazie al NAT, il router di frontiera mette a disposizione uno o più indirizzi pubblici, che vengono temporaneamente associati in modo dinamico[1] agli host della LAN quando questi devono scambiare messaggi con host esterni. L'associazione degli indirizzi pubblici agli host è mantenuta dal NAT in una **tabella di traduzione**.

1.1 Esempio

Si consideri una LAN in cui è presente un host A, il cui indirizzo IP *privato* è 10.0.1.2. Il router di frontiera di questa LAN ha invece l'indirizzo *pubblico* 128.195.4.119. Infine, al di fuori della LAN, è presente un host B con indirizzo *pubblico* 213.168.112.3.

Si supponga che A debba inviare un datagramma di richiesta a B, e che B deve rispondere inviando a sua volta un datagramma ad A. La comunicazione avviene nel modo seguente:

1. A invia un datagramma con:
   - source address 10.0.1.2 (l'indirizzo privato di A);
   - destination address 213.168.112.3 (l'indirizzo pubblico di B).
2. Quando il datagramma passa dal router di frontiera, il NAT sostituisce il source address presente nel datagramma con l'indirizzo pubblico del router, 128.195.4.119, e salva nella tabella di traduzione l'associazione (temporanea) tra l'indirizzo privato 10.0.1.2 di A e questo indirizzo pubblico:

[1] È anche possibile configurare un'associazione statica, usata quando all'interno della LAN è presente un server che deve essere raggiungibile dall'esterno.

Indirizzo privato	Indirizzo pubblico
10.0.1.2	128.195.4.119

3. B riceve il datagramma, e invia un datagramma di risposta con source e destination address scambiati:
   - source address 213.168.112.3 (l'indirizzo pubblico di B);
   - destination address 128.195.4.119 (l'indirizzo pubblico del router di frontiera della LAN in cui si trova A).
4. Il router di frontiera riceve il datagramma di risposta, legge l'indirizzo di destinazione 128.195.4.119, e consultando la tabella di traduzione determina che il destinatario del datagramma all'interno della LAN è l'host A. Allora, aggiorna il destination address con l'indirizzo privato 10.0.1.2 e inoltra il datagramma ad A.
5. A riceve il datagramma di risposta.

Siccome le associazioni tra indirizzi pubblici e privati sono dinamiche (non permanenti), se un altro host nella stessa LAN di A avesse successivamente bisogno di comunicare, esso potrebbe riutilizzare lo stesso indirizzo pubblico.

2 Funzionalità del NAT

La traduzione degli indirizzi eseguita dal software NAT può essere sfruttata in vari modi, per realizzare diverse funzionalità:

- **pooling** di indirizzi IP;
- supporto alla **migrazione** tra ISP;
- **IP masquerading**;
- **load balancing** (distribuzione del carico) tra più server.

2.1 Pooling di indirizzi IP

Si parla di *pooling* di indirizzi IP quando il NAT gestisce un insieme, chiamato appunto *pool* di più indirizzi IP pubblici assegnati alla stessa rete. Quando un host interno alla rete, identificato da un indirizzo privato, ha bisogno di comunicare con l'esterno, il NAT sceglie uno degli indirizzi disponibili dal pool e lo associa all'indirizzo privato di tale host.

Il pooling viene spesso usato, ad esempio, nelle reti aziendali, che tendono ad avere a disposizione più di un indirizzo pubblico.

2.2 Supporto alla migrazione tra ISP

Il collegamento da una LAN a Internet è in genere fornito da un ISP, che assegna alla LAN (o meglio, al router di frontiera della LAN) uno o più indirizzi IP pubblici.

Se si passa a un altro ISP, cambiano anche gli indirizzi pubblici assegnati, ma, grazie al NAT, ciò richiede solo un aggiornamento della tabella di traduzione: la migrazione risulta del tutto trasparente agli host interni alla rete.

2.3 IP masquerading

L'*IP masquerading* permette l'associazione di un singolo indirizzo IP pubblico a più indirizzi privati contemporaneamente, ovvero consente a più host in una LAN di condividere uno stesso indirizzo pubblico.

Per distinguere i datagrammi di host diversi, la traduzione effettuata dal NAT viene estesa ai **numeri di porta** di livello 4 (TCP/UDP): ogni combinazione di indirizzo IP e numero di porta privati viene associata allo stesso indirizzo IP pubblico, ma con un numero di porta diverso. Ad esempio:[2]

Indirizzo privato	Indirizzo pubblico
10.0.1.2:2001	128.195.4.119:2100
10.0.1.3:3020	128.195.4.119:4444

Siccome la traduzione coinvolge anche i numeri di porta, la tecnica di IP masquerading è chiamata anche *Port Address Translation* (PAT) o *Network Address and Port Translation* (NAPT).

2.4 Load balancing

Quando un singolo server non è sufficiente a erogare un servizio, si predispongono all'interno della LAN più server identici, e bisogna fare in modo che:

- tutti questi server siano accessibili tramite uno stesso indirizzo pubblico;
- il carico (ovvero la quantità di richieste) sia distribuito in modo bilanciato tra i vari server.

[2] In questa tabella, i numeri di porta sono rappresentati direttamente "in coda" agli indirizzi IP, separati dai due punti.

Ciascun server ha un proprio indirizzo privato. Quando il router di frontiera riceve un datagramma di richiesta, seleziona il server a cui inoltrarlo secondo un qualche algoritmo di scheduling, che deve essere *fair*, cioè distribuire le richieste in modo equo. L'algoritmo più semplice è lo scheduling *a margherita* (*round-robin*), che manda la prima richiesta al primo server, la seconda richiesta al secondo server, e così via, fino all'ultimo server, dopodiché il ciclo si ripete.

Quando il NAT viene usato per il load balancing, come nel caso dell'IP masquerading, lo stesso indirizzo pubblico può essere associato a più indirizzi privati. Cambia però il meccanismo usato per distinguere le varie associazioni dello stesso indirizzo: siccome ciascuna associazione corrisponde a una diversa richiesta ricevuta dall'esterno, esse possono essere distinte in base all'indirizzo pubblico dell'host richiedente. La tabella di traduzione assume allora una struttura del genere:

Indirizzo privato server	Indirizzo pubblico server	Indirizzo pubblico richiedente
10.0.1.2	128.195.4.119	128.159.4.120
10.0.1.4	128.195.4.119	213.168.12.3

3 Problemi del NAT

Se da un lato, come appena visto, il NAT risulta spesso molto utile, dall'altro esso introduce anche alcuni problemi:

- *Performance*: modificando l'indirizzo IP contenuto in un datagramma, è necessario ricalcolare anche la checksum dell'header; se inoltre si modifica il numero di porta, bisogna ricalcolare anche la checksum TCP.
- *Frammentazione*: se un datagramma trasmesso da un host nella LAN viene frammentato prima di raggiungere il router di frontiera, bisogna assicurarsi che siano assegnati a tutti i frammenti lo stesso indirizzo IP e lo stesso numero di porta pubblici.
- *Connettività end-to-end*: si perde la raggiungibilità end-to-end di tutti gli host su Internet, perché un host esterno spesso non ha modo di iniziare la comunicazione verso un host situato in una rete che usa il NAT (finché quest'ultimo host non inizia a comunicare "dall'interno", non gli viene assegnato un indirizzo pubblico, quindi non c'è modo di rivolgersi a esso dall'esterno — a meno che non sia stata appositamente predisposta un'associazione statica).
- *Indirizzi IP nei dati applicativi*: alcuni protocolli applicativi utilizzano degli indirizzi IP contenuti all'interno dei pacchetti di livello applicazione, ma questi non vengono solitamente tradotti (perché il NAT esegue la traduzione solo nell'header

IP, a meno che il software non sia appositamente progettato per cercare di rimediare a questo problema). Il risultato è che tali protocolli tendono a non funzionare in presenza di NAT.