Politecnico di Torino

Facoltà di ingegneria dell'informazione

Laurea specialistica in ingegneria informatica

Corso di Infrastrutture e servizi per reti geografiche – Anno 2004

NAT
Network
Address
Translation

Vincenzo Buttazzo
Marco Vallini

Indice

Network Address Translation
1. Concetti Generali
1.1 Session Flow e Packet Flow
1.2 Identificazione di una sessione
1.3 Rete pubblica, globale ed esterna
1.4 Rete privata o locale
1.5 Application Level Gateway
1.6 Cos'è il NAT
1.7 Le tipologie di NAT
1.8 Realm Specific IP
1.8.1 Realm Specific Address IP
1.8.2 Realm Specific Address and Port IP
1.9 Reti private e tunnel
1.10 Caratteristiche operazionali del NAT
1.11 Supporto FTP (File Transfer Protocol)
1.12 Limitazioni del NAT
Traditional NAT
2. Traditional NAT
2.1 Caratteristiche del Basic NAT
2.2 Caratteristiche del NAPT
2.3 Le fasi di traduzione per una sessione
2.4 Traduzione dei pacchetti
2.5 Problematiche
2.6 Limitazioni del NAT
2.7 Implementazioni
Implicazioni architetturali dei NAT
3. Introduzione
4. Il modello End-to-End
5. Vantaggi derivanti dall'uso dei NAT
6. Problemi con i NAT
7. Scenari
7.1 Singolo punto di rottura
7.2 Complessità degli ALG
7.3 Violazione degli stati di TCP
7.4 Gestione simmetrica degli stati
8. Considerazioni sulla sicurezza
8.1 IPSec
Traduzione degli indirizzi di rete – Traduzione di protocollo
9. Introduzione
10. Connessione da IPv.6 a IP.4 - Basic-NAT-PT
11. Connessione da IPv.6 a IPv.4 - NAPT-PT
12. Connessione da IPv.4 a IPv.6 – NAPT-PT
13. Uso di DNS-ALG per l'assegnamento degli indirizzi
13.1 Assegnamento di indirizzi V4 per connessioni entranti (da V4 a V6)
13.2 Vulnerabilità
13.3 Assegnamento di indirizzi V4 per connessioni uscenti (da V6 a V4)
14. Problematiche derivanti dall'uso di NAT-PT

NAT – Network Address Translation

1.Concetti Generali

Il Network Address Translation (NAT) è un metodo che consente di mettere in relazione e far comunicare indirizzi IP appartenenti a domini differenti, rendendo trasparente il processo di routing per gli host coinvolti.
La necessità della trasformazione degli indirizzi IP è utile quando gli indirizzi interni di una rete privata non sono utilizzabili all'esterno, tipicamente sulla rete pubblica.
In generale, il meccanismo del NAT consente agli host di una rete privata di comunicare con host facenti parte della rete pubblica e viceversa in modo trasparente. Esistono diverse tipologie di NAT a seconda delle esigenze e delle problematiche da risolvere.
Le problematiche fondamentali dell'adozione del meccanismo del NAT riguardano quelle applicazioni che utilizzano gli indirizzi IP all'interno del proprio protocollo di comunicazione. Per esempio, l'uso di servizi DNS può in taluni casi provocare problematiche, così come pure l'uso di IPsec. Considerando che il meccanismo del NAT non supporta la trasparenza delle applicazioni è spesso impiegato insieme alle Application Level Gateway (ALG) che permettono di risolvere alcune di queste problematiche.

1.1 Session Flow e Packet Flow

Un indirizzo IP identifica in modo univoco un particolare nodo in una rete che può essere pubblica o privata.
Si voglia distinguere il concetto di Session flow da quello di Packet flow.
Session Flow: indica la direzione verso cui è iniziata la sessione con riferimento ad un'interfaccia di rete.
Packet Flow: indica la direzione che il pacchetto ha intrapreso con riferimento ad un'interfaccia di rete.
Una definizione per sessione è la seguente: una sessione è definita come l'insieme (set) del traffico gestito in modo unitario per una transazione. Le sessioni dei protocolli TCP/UDP sono identificate dalle tuple source IP address, source TCP/UDP port, target IP address, target TCP/UDP port. Il protocollo ICMP è identificato dalle tuple source IP address, ICMP query ID, target IP address. Le altre sessioni sono identificate dalle tuple source IP address, target IP address, IP protocol. Più semplicemente è possibile individuare la direzione di una sessione considerando la direzione del primo pacchetto. Si osservi che l'idea della sessione considerata dal NAT può essere differente da quella considerata da un'applicazione. Generalmente, infatti, l'applicazione vede un insieme di sessioni di NAT come un'unica sessione per se stessa.

1.2 Identificazione di una sessione

L'inizio di una sessione per il protocollo TCP si può riconoscere con la presenza del SYN bit e l'assenza dell'ACK bit nel TCP flags. Tutti i pacchetti TCP ad eccezione del primo devono contenere l'ACK bit settato. Tuttavia non esiste un modo deterministico per riconoscere l'inizio di una sessione basata sul protocollo UDP. Un approccio euristico (di buon senso) assume che il primo pacchetto non contenga parametri di sessione. La fine di una sessione con protocollo TCP è determinata quando il bit FIN è settato da entrambe le estremità connesse. Parimenti, è necessario che una delle due entità riceva un segmento con l'RST bit settato nel TCP flags.
Il NAT device non può assumere che i segmenti con i FIN o SYN bit settati siano gli ultimi o i primi di quella sessione. Di conseguenza, si assume che la sessione sarà terminata solo dopo un periodo di tempo pari a 4 minuti dopo il rilevamento del bit di FIN.
E' inoltre possibile che una connessione TCP termini senza che il NAT sia consapevole. Conseguentemente è necessario che il garbage collection del NAT elimini queste connessioni. Tuttavia non è possibile distinguere tra le connessioni che si trovano nello stato di idle (inattive) da quelle che non hanno superato il tempo massimo di 4 minuti. Nel caso del protocollo UDP non esiste un singolo modo per determinare quando termina una sessione. Esistono diversi approcci euristici per determinare le sessioni inutilizzate. Per esempio si può assumere che le sessioni TCP non utilizzate per 24 ore e quelle degli altri protocolli non

utilizzate per pochi minuti sono terminate. Non sempre questa assunzione è efficace. Il periodo di idle (inattività) dipende dall'applicazione, conseguentemente è necessario che il tempo di time-out sia configurabile. Tuttavia, anche con questo approccio non è garantito che un certo valore possa risolvere questa problematica. Inoltre non è garantito che il termine della sessione, rilevato dal NAT coincida con quello dell'applicazione. Un altro approccio consiste nell'introduzione di timestamp.

1.3 Rete pubblica, globale ed esterna

Una rete globale o pubblica consiste in un insieme di indirizzi unici assegnati dall' Internet Assigned Numbers Authority (IANA) o da registri equivalenti. Queste vengono denominate 'esterne' nella terminologia del NAT.

1.4 Rete privata o locale

Una rete privata consiste in un insieme di indirizzi unici all'interno della rete stessa ma indipendenti rispetto alla rete esterna. Non è quindi necessario formulare una richiesta all'autorità competente per l'assegnazione degli indirizzi interni.

1.5 Application Level Gateway (ALG)

Non tutte le applicazioni possono attraversare il NAT in modo semplice, specialmente quelle che includono un indirizzo IP nel payload. Le Application Level Gateway (ALG) sono applicazioni specifiche, basate su agenti di traduzione, che permetto alle applicazioni residenti su un host, con un particolare indirizzo (all'interno di un dominio), di connettersi con un'altra parte dell'applicazione residente su un altro host con indirizzo differente (all'interno di un altro dominio) in modo trasparente. Un ALG può interagire con il NAT per modificare lo stato, usare le informazioni di stato del NAT, modificare il payload e compiere tutte le azioni necessarie per permettere all'applicazione di funzionare in modo corretto. Le applicazioni ALG sono simili ai proxy nel favorire la comunicazioni fra client e server, e viceversa. Le ALG, si differenziano dai proxy perché non utilizzano un protocollo per far comunicare le applicazioni e perché non sono necessarie modifiche sulle applicazioni client.

1.6 Cos'è il NAT

Il Network Address Translation è il metodo con cui gli indirizzi IP vengono associati da un dominio ad un altro, rendendo trasparente il routing tra gli host. Ci sono differenti tipologie di traduzione degli indirizzi, utili per servire diverse tipologie di applicazioni. Tuttavia, tutte le diverse tipologie dei NAT, condividono le seguenti caratteristiche:

a. Assegnamento degli indirizzi in modo trasparente
b. Routing trasparente attraverso la traduzione degli indirizzi (inteso come l'inoltro di pacchetti)
c. Traduzione del payload dei pacchetti di errore ICMP

Assegnamento degli indirizzi in modo trasparente

Il NAT associa gli indirizzi della rete privata con gli indirizzi della rete esterna e vice versa provvedendo al routing trasparente per i datagrammi scambiati tra domini differenti. L'associazione, in qualche caso può essere estesa al livello trasporto in particolare alle porte TCP/UDP. L'associazione degli indirizzi è effettuato all'inizio della sessione. Vi sono due tipologie di assegnazione:

1. Assegnazione statica: associazione uno ad uno per gli host della rete privata con quelli della rete esterna per tutta la durata delle operazioni del NAT. L'assegnazione statica assicura che il NAT non debba amministrare la gestione degli indirizzi con i flussi delle sessioni.
2. Assegnazione dinamica: è effettuata in modo dinamico basandosi sulle esigenze e sui flussi delle sessioni determinate in modo euristico dal NAT. Quando l'ultima sessione

che utilizza un indirizzo associato è terminata, il NAT libera l'associazione così che l'indirizzo esterno potrà essere riutilizzato successivamente.

Routing trasparente

Il router NAT si trova ai bordi tra due domini con il compito di tradurre gli indirizzi IP così che i pacchetti da e verso un dominio differente possano essere inoltrati correttamente. Data la caratteristica di interconnettere domini differenti, esiste una problematica nel propagare le informazioni che devono rispettare alcuni vincoli. Vi sono tre fasi necessarie per tradurre un indirizzo che riguardano rispettivamente la creazione, il mantenimento e la terminazione delle sessioni:

1. Associazione dell'indirizzo: è la fase in cui si crea l'associazione tra un indirizzo della rete privata con quello della rete esterna. Se statico, l'indirizzo è fisso, altrimenti è associato dinamicamente all'inizio della sessione. Tutte le interazioni all'interno della sessione utilizzeranno quindi la medesima associazione. Ogni sessione prevede una nuova associazione se questa non è stata già realizzata. Vi possono essere più sessioni simultanee associate allo stesso indirizzo.
2. Ricerca e traduzione: dopo che la sessione è stata inizializzata, ogni pacchetto è sottoposto alla ricerca dell'indirizzo e alla relativa traduzione.
3. Eliminazione dell'associazione dell'indirizzo: il NAT esegue l'eliminazione dell'associazione quando ritiene che l'ultima sessione che utilizza un particolare indirizzo sia terminata.

Traduzione del payload dei pacchetti di errore ICMP

Tutti i messaggi di errore ICMP, esclusi i messaggi di redirect devono essere modificati quando attraversano un NAT. I tipi di messaggi modificati dal NAT sono i seguenti: Destination-Unreachable, Source-Quence, Time-Exceeded e Parameter-Problem. I cambiamenti riguardano l'indirizzo IP originale inserito nel payload del messaggio ICMP. Più precisamente, l'indirizzo IP dell'header IP contenuto nel payload ed il campo di checksum dello stesso IP header devono essere rettificati. E' necessario cambiare anche il checksum header e l'IP header per riflettere le altre variazioni effettuate.

1.7 Le tipologie di NAT

Ci sono diverse tipologie di NAT per soddisfare i requisiti di applicazioni diverse. Le più significative sono:

1. Traditional NAT o Outbound NAT
2. Bi-directional NAT o Two-Way NAT
3. Twice NAT
4. Multihomed NAT

Traditional NAT o Outbound NAT

Il Traditional NAT permette agli host presenti all'interno di una rete privata di accedere in modo trasparente agli host della rete esterna. In questa tipologia, le sessioni sono unidirezionali, esclusivamente in partenza dalla rete interna verso quella esterna.
Gli indirizzi IP, sia della rete interna che di quella esterna sono unici, tuttavia quelli della rete interna non sono validi per la rete esterna perché esclusivi sono all'interno della rete privata. Ciò implica che gli indirizzi della rete interna non possano essere pubblicati all'esterno, ma può avvenire il contrario. Gli indirizzi della rete interna non possono sovrapporsi a quelli della rete esterna. Questo significa che un indirizzo può essere esclusivamente interno oppure esterno. Nel Traditional NAT, un host della rete interna può iniziare una sessione verso la rete esterna, ma non vice versa. Questa caratteristica è spesso utilizzata quando è necessario disporre di un accesso verso la rete esterna, evitando che un host esterno inizializzi una sessione verso la rete interna.
Esistono due possibili variazioni del Traditional NAT:

1. Basic NAT: esistono un insieme di indirizzi IP esterni associabili agli indirizzi interni della rete. Per i pacchetti in partenza dalla rete interna, l'indirizzo sorgente ed i campi correlati come IP, TCP, UDP e ICMP header checksum sono modificati. Per i pacchetti in

arrivo dall'esterno sono modificati gli indirizzi IP di destinazione e gli altri elementi precedentemente elencati.

2. NAPT: estende il concetto di traduzione anche alle porte TCP ed UDP e alle query ICMP interessate. Questo permette che gli identificatori di trasporto degli host privati, siano multiplati sugli identificatori di trasporto di un singolo indirizzo esterno. Il NAPT consente ad un insieme di host di una rete privata, di condividere un unico indirizzo esterno. Spesso il NAPT è combinato con il Basic NAT per aumentare le possibilità di connettività verso l'esterno, quando gli indirizzi esterni validi sono terminati. Per i pacchetti in partenza dall'interno, il NAPT modifica l'indirizzo IP sorgente, la sorgente dell'identificatore del trasporto ed i campi relativi ai header checksum di IP, TCP, UDP e ICMP. Per i pacchetti in arrivo dall'esterno, sono cambiati l'IP di destinazione, l'identificatore di destinazione del trasporto ed i checksum di IP e degli altri relativi al trasporto.

Bi-directional NAT o Two-Way NAT

Con il Bi-directional NAT, le sessioni possono essere iniziate sia dagli host della rete esterna che da quelli della rete interna. Gli indirizzi della rete privata, sono associati ad indirizzi globali della rete esterna, staticamente oppure dinamicamente, così che le connessioni possano essere stabilite in tutte le direzioni. Si assume che i name space (spazio dei nomi) tra la rete privata e quella esterna, siano unici ed end-to-end. Gli host della rete esterna, possono accedere a quelli della rete interna utilizzando il servizio DNS per la risoluzione dell'indirizzo. Il DNS-ALG deve essere impiegato insieme al Bi-directional NAT per facilitare l'associazione tra nome ed indirizzo degli host. Più precisamente, il DNS-ALG è una funzionalità che gestisce la sostituzione degli indirizzi nelle Query/Response DNS sulla base delle associazioni eseguite dal NAT tra indirizzo privato e corrispondente indirizzo pubblico.

Twice NAT

Il Twice NAT è una variazione del NAT in cui sia l'indirizzo sorgente che quello di destinazione sono modificati dal NAT per permettere il transito di un datagramma. Questa soluzione è in contrasto sia con il Traditional NAT che con il Bi-directional NAT, dove il transito di un datagramma comporta solo la traduzione di un indirizzo.
Il Twice NAT è necessario quando lo spazio di indirizzamento della rete interna e di quella esterna si sovrappongono. Il caso che specifica meglio questa situazione riguarda l'utilizzo sulla rete privata di indirizzi riservati alla rete esterna, assegnati ad un'altra organizzazione. Il problema risiede nell'utilizzo di un indirizzo unico per rappresentare due host: uno della rete interna l'altro della rete esterna. Se questo indirizzo è presente in un pacchetto, sarà instradato verso l'interno e non verso la rete pubblica. Il meccanismo del Twice NAT per risolvere questa problematica consiste nella traduzione degli indirizzi sorgente e destinazione dei pacchetti IP. Questo consente al Twice NAT, di collegare rete pubblica e privata come se avessero indirizzi non sovrapposti. Anche nel Twice NAT viene impiegato il DNS-ALG, che permette di intercettare le query DNS e di sostituire gli indirizzi ammettendo la comunicazione tra gli host della rete interna ed esterna.

Multihomed NAT

Spesso, per un'organizzazione, la connettività verso la rete Internet è di primaria importanza, così da rendere necessaria l'introduzione di sistemi di ridondanza. L'introduzione di più NAT, può risolvere questa problematica, introducendone un'altra riguardo alla configurazione di questi dispositivi. Sistemi a più NAT, possono essere installati, a condizione di mantenere il loro stato sempre aggiornato ed allineato. Nel caso di guasto di un sistema, l'altro NAT deve sostituirlo in modo trasparente. Il Multihomed NAT, consente di condividere la stessa configurazione tra più sistemi NAT o connessioni multiple allo stesso NAT. Tuttavia, la sostituzione di un sistema NAT con un altro, è più semplice se l'associazione è di tipo statico rispetto a quella dinamica.

1.8 Realm Specific IP (RSIP)

Realm Specific IP (RSIP), è un protocollo che può essere utilizzato come alternativa al NAT. Il campo di maggiore interesse di RSIP, è quello delle condivisioni delle connessioni di una rete

privata verso una rete esterna. RSIP, è stato sviluppato come alternativa al NAT, preservando l'integrità dei pacchetti end-to-end, caratteristica non soddisfatta dal NAT.
Il NAT è limitato da applicazioni come gli 'streaming media', che trasmettono indirizzi IP o numeri di porta nel payload dei pacchetti. Queste applicazioni, richiedono che il NAT abbia una conoscenza specifica dell'applicazione, ed esegua calcoli addizionali. L'aspetto negativo è che il NAT risiede tipicamente su un router di confine, tra le reti pubbliche e private; non può quindi funzionare con IP Security (IPSec), tecnologia di cifratura per le reti private virtuali. L'IPSec richiede l'handshaking end-to-end reale in modo da impostare le regole iniziali di cifratura. Una volta cifrati su un sistema client, i pacchetti IPSec non possono essere alterati, o riconosciuti, dal NAT.
Come il NAT, l'RSIP traduce tra gli indirizzi IP pubblici e privati, ma, invece di richiedere un router di confine, RSIP usa un semplice protocollo tra host dell'utente e un router di confine, per eseguire la generazione preparatoria di un segnale. Attraverso la generazione di segnale, l'host è in grado di preparare ciascun pacchetto in modo tale da rimuovere il limite di traduzione. Il protocollo RSIP utilizza una struttura 'challenge-response' ed impiega un vocabolario composto da 'parametri' e 'messaggi'. Il protocollo è composto da due entità: RSIP Client e RSIP Server. Il Client, è un host della rete privata, che adotta un indirizzo della rete esterna quando è connesso ad un host di quel dominio per una comunicazione end-to-end. I pacchetti generati dagli host sono basati su indirizzi unici della rete esterna, perciò non richiedono di essere tradotti. Il Server, presente sia nella rete esterna che in quella interna, permette di instradare i pacchetti provenienti dall'esterno verso l'interno. Questi pacchetti, possono essere stati orginati o diretti ad un client. Inoltre, il Server, è il responsabile dell'assegnazione degli indirizzi della rete esterna ai client.
L'operazione, inizia quando il software client RSIP sull'host, invia un segnale al software sul server RSIP in un router o gateway di confine. Attraverso questo scambio, il client RSIP richiede un indirizzo IP pubblico insieme a una o più porte del router/gateway. In risposta, il software server RSIP del router/gateway, assegna un indirizzo IP pubblico e uno o più numeri di porta, oltre al 'lease time', al tipo di 'tunnel' e ad altri parametri. Quando il pacchetto raggiunge il server/gateway RSIP, l'unicità del pacchetto viene identificata dalla combinazione dell'indirizzo IP assegnato e dei numeri di porta. Come nel NAT, il server RSIP, utilizza un indirizzo IP privato (per esempio 10.0.0.4), per il proprio schema di indirizzamento interno all'azienda, ma, diversamente da NAT, il gateway di confine non deve necessariamente essere in grado di eseguire la traduzione: il server/gateway RSIP, rintraccia nell'intestazione del pacchetto, le informazioni di cui ha bisogno, quindi consulta la tabella RSIP per determinare la destinazione del pacchetto. E' chiaro che RSIP, rappresenta un grande miglioramento rispetto al NAT. Ad esempio, con una semplice estensione, RSIP può supportare IPSec end-to-end, sebbene IPSec cifri i numeri di porta. Le due tecniche, hanno comunque molto in comune. RSIP propone due importanti vantaggi:

1. lo stretto legame con lo schema di indirizzamento di NAT, fornisce una compatibilità verso il basso, un vantaggio per migliaia di utenti NAT che vorranno migrare verso RSIP.
2. considerato che il protocollo RSIP, impiega la generazione preparatoria del segnale, è adatto anche per il networking basato su policy.

Vi sono due variazioni al RSIP, denominate rispettivamente Realm-Specific Address IP (RSA-IP) e Realm-Specific Address and Port IP (RSAP-IP).

1.8.1 Realm Specific Address IP (RSA-IP)

Il componente client di RSA-IP, adotta un indirizzo IP dallo spazio degli indirizzi della rete esterna, quando si connette ad un host della rete pubblica. Una volta che l'RSA-IP client assume un indirizzo esterno, nessun altro host della rete interna potrà assumere lo stesso indirizzo, finché questo non sarà rilasciato dal client.
Considerando una comunicazione end-to-end all'interno della rete interna, vi sono due possibili approcci:

1. Utilizzare un 'tunnel' per condurre il pacchetto alla destinazione, l'header esterno può essere tradotto dal NAT normalmente, senza influenzare l'indirizzo utilizzato nell'header interno.

2. Costituire un tunnel bi-direzionale tra l'RSA-IP Client ed il border router. I pacchetti, da e verso il client, potranno essere inseriti nel tunnel, ma saranno inoltrati normalmente tra il router di confine e la destinazione.

Si noti che il tunnel dal client verso il router di confine potrebbe non essere necessario, in quanto i pacchetti potrebbero essere inoltrati direttamente.

Caratteristiche di RSA-IP Client

Un RSA-IP Client, ha le seguenti caratteristiche:

1. Conoscenza del dominio di appartenenza degli altri client
2. Assumere un indirizzo esterno quando necessita di comunicare con altri host esterni. L'indirizzo può essere assegnato staticamente o dinamicamente dall'RSA-IP Server.
3. Instradare i pacchetti verso gli host esterni, utilizzando un meccanismo in accordo con l'RSA-IP Server. In tutti i casi, l'RSA-IP Client può comportarsi come un tunnel end-point. E' in grado di incapsulare i pacchetti end-to-end inoltrandoli, riceverli e trattarli in modo corretto.

Caratteristiche di RSA-IP Server

Un RSA-IP Server, è residente sia all'interno che all'esterno della rete privata, per facilitare l'instradamento dei pacchetti verso gli RSA-IP Client. L'RSA-IP Server ha le seguenti caratteristiche:

1. Può essere configurato per assegnare indirizzi esterni agli RSA-IP Client, sia di tipo statico che dinamico
2. Deve essere un router residente sia all'interno che all'esterno della rete privata
3. Deve utilizzare un meccanismo per instradare i pacchetti provenienti dall'esterno verso la rete interna. Esistono due approcci:
    a. È necessario che il RSA-IP Server possa utilizzare la funzionalità di NAT router, provvedendo all'instradamento trasparente per gli header esterni. Questo richiede che ci sia un altro Server esterno che sia un tunnel end-point.
    b. L'RSA-IP Server, può essere un router qualsiasi (anche di tipo NAT) che possa essere utilizzato come tunnel end-point con i RSA-IP Client. Più precisamente, deve essere in grado di intercettare i pacchetti provenienti dagli RSA-IP Client ed inoltrarli verso l'esterno. Per il percorso inverso (return path), deve localizzare l'RSA-IP Client tunnel (basato sull'indirizzo di destinazione del pacchetto end-to-end), incapsulare i pacchetti nel tunnel per inoltrarli verso il Client corretto.

Gli RSA-IP Client, possono supportare diverse tecniche di IPsec denominate transport o tunnel mode Authentication and confidentiality.

1.8.2 Realm Specific Address and Port IP (RSAP-IP)

Il Realm Specific Address and Port IP (RSAP-IP), è una variazione dell'RSA-IP, che permette a due o più host di utilizzare lo stesso indirizzo esterno. Il meccanismo, simile al NAPT, permette di multiplare più connessioni sullo stesso indirizzo utilizzando gli identificatori di trasporto (porte TCP/UDP e ICMP Query IDs).

L'RSAP-IP Client, si distingue dall'RSA-IP Client, per l'utilizzo delle tuple (indirizzo esterno, identificatore di trasporto) per connettersi ad un host esterno. Inoltre, la comunicazione con i nodi esterni è limitata alle sessioni TCP, UDP ed ICMP.

L'RSAP-IP Server, si distingue dall'RSA-IP Server, per l'assegnazione degli indirizzi esterni ai client. Il Server assegnerà ai Client non solo l'indirizzo esterno ma anche gli identificatori di trasporto.

Nell'utilizzare l'RSAP-IP, vi sono alcune limitazioni riguardo al protocollo IPsec, basato sulla sicurezza end-to-end dei pacchetti. La modalità di trasporto, basata sull'autenticazione e sull'integrità, può essere realizzata correttamente, mentre la riservatezza (confidentiality), non è permessa. Questo perché l'RSAP-IP Server, deve essere in grado di esaminare l'identificatore di trasporto della destinazione (destination transport Identifier) per identificare l'RSAP-IP tunnel, utilizzato per inoltrare i pacchetti. Per questa ragione, solo i pacchetti TCP, UDP ed ICMP protetti, possono attraversare un RSAP-IP Server, utilizzando questo approccio.

1.9 Reti private e tunnel

Si vuole considerare il caso in cui, una rete privata, sia connessa alla rete esterna, utilizzando un meccanismo chiamato tunnel. Questo automatismo, spesso è utilizzato per interconnettere due reti con le stesse caratteristiche, ma separate da una rete differente. Il traffico, che viaggia nel tunnel, può contenere pacchetti che hanno subito modifiche (per esempio una traduzione d'indirizzo). Più precisamente, ci sono due tipologie di scenario: tunneling di pacchetti tradotti (translated packets) e la ripartizione del Backbone per le reti private.

1.10 Caratteristiche operazionali del NAT

I dispositivi NAT, senza l'inclusione di ALG, non esaminano né modificano i payload. Per questa ragione, questi sono trasparenti alle applicazioni in molti casi. Tuttavia, vi sono due casi in cui il NAT può introdurre delle difficoltà:

1. quando i payload delle applicazioni includono indirizzi IP
2. quando è richiesta qualche tipologia di sicurezza end-to-end

(Si noti che questa non è una lista completa)
Tutte le tecniche di Application layer security, che non utilizzano l'indirizzo IP, sono trasparenti rispetto al NAT, ma non si verifica per le tecniche di livello trasporto (transport layer) come IPsec (trasport mode) o TCP MD5.
Nell'IPsec transport mode, sia AH (Authentication Header) che ESP (Encapsulating Security Payload), utilizzano il controllo dell'integrità sul payload. Questo controllo, se il payload è di tipo TCP, UDP, è responsabile anche della verifica del checksum TCP/UDP. Quando il NAT modifica un indirizzo, il checksum non è più valido. Normalmente, il NAT modifica anche il checksum, ma questo non è valido se si utilizzano AH ed ESP. Di conseguenza, l'host che riceve il pacchetto, lo scarterà perché non sarà garantito il controllo d'integrità da parte di IPsec. Se il NAT non modifica il checksum, sarà il checksum a non essere valido. Si osservi, che IPsec in modalità tunnel ESP è permesso, sebbene questo non sia supportato dal Traditional NAT. La modalità ESP, basata sul transport mode authentication and confidentiality, per comunicazioni end-to-end è permessa per i pacchetti come ICMP, in cui il contenuto dell'IP payload non è affetto dalla traduzione dell'IP header. Anche l'utilizzo di Secure DNS non è supportato dal NAT, perché le firme digitali non possono essere verificate correttamente.
E' interessante osservare che l'IKE (Session key negotiation protocol), utilizza una sessione UDP, e solo una piccola porzione è protetta. Questo permette, alle sessioni IKE, di attraversare un NAT, se il payload non contiene indirizzi IP o trasport ID specifici di un dominio.

1.11 Supporto FTP (File Transfer Protocol)

I comandi 'PORT' e 'PASV', nel control session payload del servizio FTP, identificano l'indirizzo IP e la porta TCP, che saranno utilizzati per la session data. Gli argomenti dei comandi, rispettivamente, indirizzo IP e porta TCP, sono memorizzati con codifica ASCII.
Per permettere il supporto del servizio FTP, attraverso un dispositivo NAT, è necessario introdurre un FTP ALG. Questo, ha il compito di monitorare ed aggiornare l'FTP control session payload, quando queste informazioni sono rilevanti per i nodi della rete. Inoltre, l'ALG deve aggiornare il NAT con le informazioni: tuple di data session e session orientation. In questo modo, il dispositivo, potrà aggiornare le informazioni di stato per supportare le sessioni FTP.
Siccome l'indirizzo IP e le porte TCP, sono memorizzate con la codifica ASCII, questo introdurrà una variazione nella dimensione del pacchetto. Per ovviare a questa problematica, l'ALG utilizza una tabella per correggere le informazioni di TCP sequence ed acknowledge numbers, quando necessario.

1.12 Limitazioni del NAT

Applicazioni che contengono indirizzi IP

Non tutte le applicazioni sono trasparenti al passaggio attraverso un dispositivo NAT, specialmente, quelle che contengono indirizzi IP e porte TU (TCP/UDP) all'interno del payload.

Per risolvere questa problematica, spesso si utilizzano applicazioni particolari denominate ALG (Application Level Gateway), che provvedono a modificare i payload utilizzando le informazioni dei dispositivi NAT.
Per esempio, il servizio SNMP è un'applicazione che contiene all'interno del payload indirizzi IP, perciò il NAT, non è in grado di effettuare una traduzione corretta. Per questo motivo, spesso i router con NAT, sono dotati di un ALG utile ad effettuare la traduzione per il servizio SNMP.

Applicazione con controllo interno delle sessioni
I dispositivi NAT, operano con l'assunzione che ogni sessione sia indipendente. Le caratteristiche delle sessioni, come la direzione, la destinazione, il protocollo utilizzato sono determinati indipendentemente all'inizio di una sessione. Tuttavia, esistono applicazioni come H.323, che utilizzano uno o più controlli di sessione, per modificare le caratteristiche all'interno dei payload. Questa tipologia di applicazione, richiede l'impiego di ALG per garantire la corretta traduzione delle informazioni, contenute nei pacchetti ed un'integrazione con i device NAT.

Considerazioni sul debugging
Il NAT, aumenta la probabilità di una cattiva gestione dell'indirizzamento, perché lo stesso indirizzo pubblico può essere associato, in tempi diversi, ad indirizzi privati differenti. Il risultato è che ogni studio basato sull'indirizzo globale e sulle porte TU può non essere efficace.
Se un host, abusa della rete Internet in qualche modo, non è possibile individuarlo con precisione, ma è possibile individuare esclusivamente il suo dominio di appartenenza, tramite l'indirizzo globale.

Traduzione dei pacchetti FTP di controllo frammentati
La traduzione dei pacchetti FTP di controllo frammentati, è complicato quando i pacchetti contengono i comandi di 'PORT' o le risposte ai comandi 'PASV'. Questo, tuttavia, è un caso patologico. Il router NAT, deve inizialmente assemblare insieme tutti i frammenti e successivamente tradurli ed inoltrarli.
La problematica, si verifica anche nel caso in cui ogni caratteristica del pacchetto contenga comandi 'PORT' e risposte 'PASV', inviati in datagrammi separati e non frammentati. Il NAT, viene semplicemente attraversato, senza che vi sia traduzione dei payload TCP, quindi se la traduzione fosse necessaria, l'applicazione fallirà. Se però, il contenuto del payload fosse valido in entrambi i domini, l'applicazione avrà successo.

Elaborazione
I dispositivi NAT, quando devono collaborare con algoritmi atti a modificare i checksum, possono diminuire notevolmente la capacità di throughput nell'inoltro dei pacchetti. Tuttavia, molto spesso, questo non rappresenta un problema.

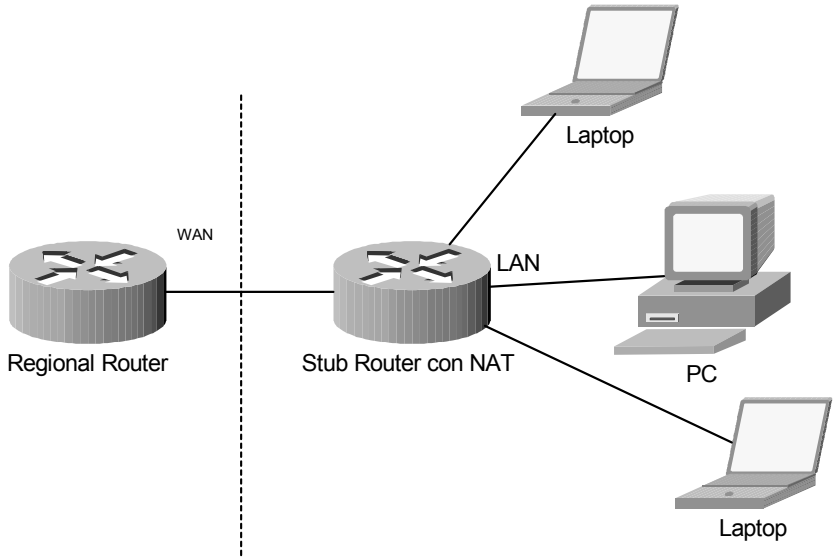
Considerazioni sulla sicurezza
Molto spesso, si considera il traditional NAT come un filtro di traffico a senso unico. Ciò permette di bloccare parte del traffico diretto dall'esterno della rete verso l'interno, rendendo un host privato, non identificabile dall'esterno. I dispositivi NAT, possono essere anche utilizzati insieme ai firewall, per migliorare la sicurezza globale di una rete privata.
Se il NAT device ed il dispositivo ALG non si trovano all'interno dello stesso 'dominio di sicurezza', ciò rappresenta il maggiore problema di sicurezza, perché l'ALG può intercettare il traffico contenuto nel payload inviato dall'host. I payload, possono essere crittografati, ma non devono contenere indirizzi IP o quant'altro sia valido esclusivamente all'interno del dominio.
La combinazione delle funzionalità del NAT, affiancate da applicazioni ALG e firewall, provvedono ad un ambiente di lavoro trasparente per una rete privata. Questi dispositivi, assicurano che un datagramma, inviato alla rete esterna, non conterrà indirizzi privati nell'header o nel payload. I dipositivi NAT gateway, possono essere utilizzati come tunnel per provvedere al trasporto sicuro di pacchetti end-to-end, attraverso la rete geografica. Le applicazione per cui si utilizzano spesso questi dispositivi sono le reti private virtuali (VPN).
Altre considerazioni, inerenti alla sicurezza sono:

1. Le sessioni UDP non sono sicure, perché la risposta ad un datagramma, può provenire da un indirizzo differente da quello target. Come risultato, questo può provocare una

parziale corrispondenza con le informazioni in possesso del traditional NAT, compromettendo la sicurezza della rete.
2. Le sessioni multicast basate sul protocollo UDP non sono sicure.
3. I dispositivi NAT, possono essere l'obiettivo di un attacco SYN flood o ping flood. E' necessario che implementino meccanismi di protezione, simili a quelli utilizzati dai server Internet-based.

2. Traditional NAT

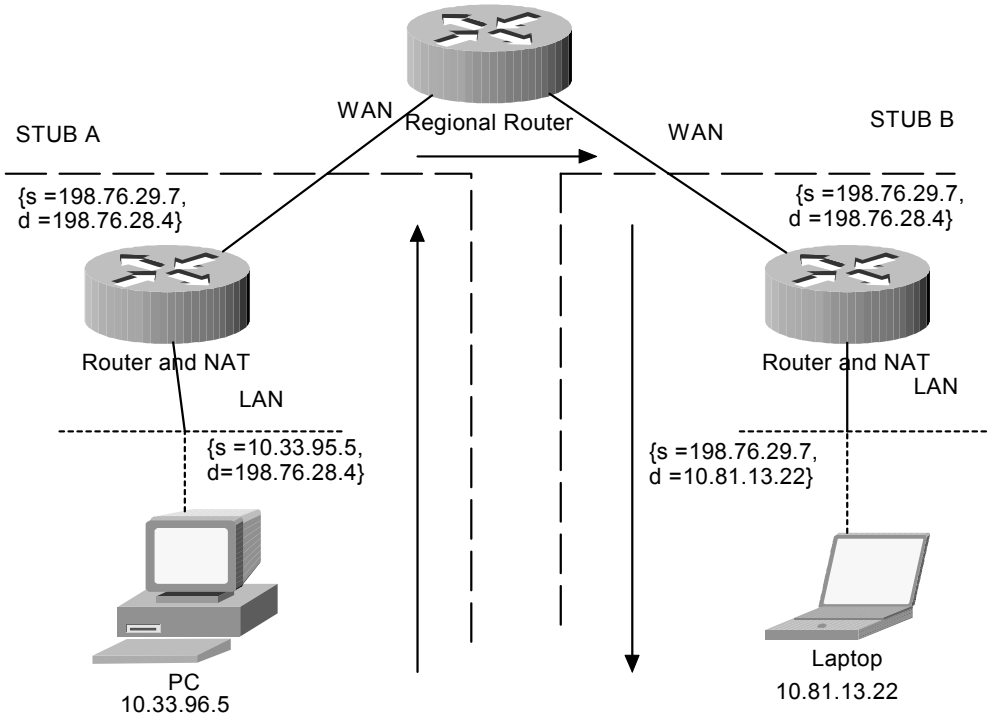
Come descritto in precedenza, il meccanismo del Traditional NAT, permette agli host interni ad una rete locale, di comunicare con gli host esterni. Un esempio concreto, può essere descritto adottando lo scenario di un ambiente SOHO (Small Office Home Office), in cui, un ristretto numero di calcolatori, accedono alla rete Internet per scambiare informazioni. Per ragioni di sicurezza, è necessario, che gli host della rete esterna, non possano contattare direttamente i calcolatori della rete locale. Il Traditional NAT consente, salvo in alcuni casi particolari, che le sessioni siano inizializzate dalla rete privata, inibendo la possibilità di un primo contatto, proveniente dall'ambiente esterno. Per questa tipologia di problema, il Traditional NAT, offre due soluzioni: il Basic NAT ed il NAPT.



2.1 Caratteristiche del Basic NAT

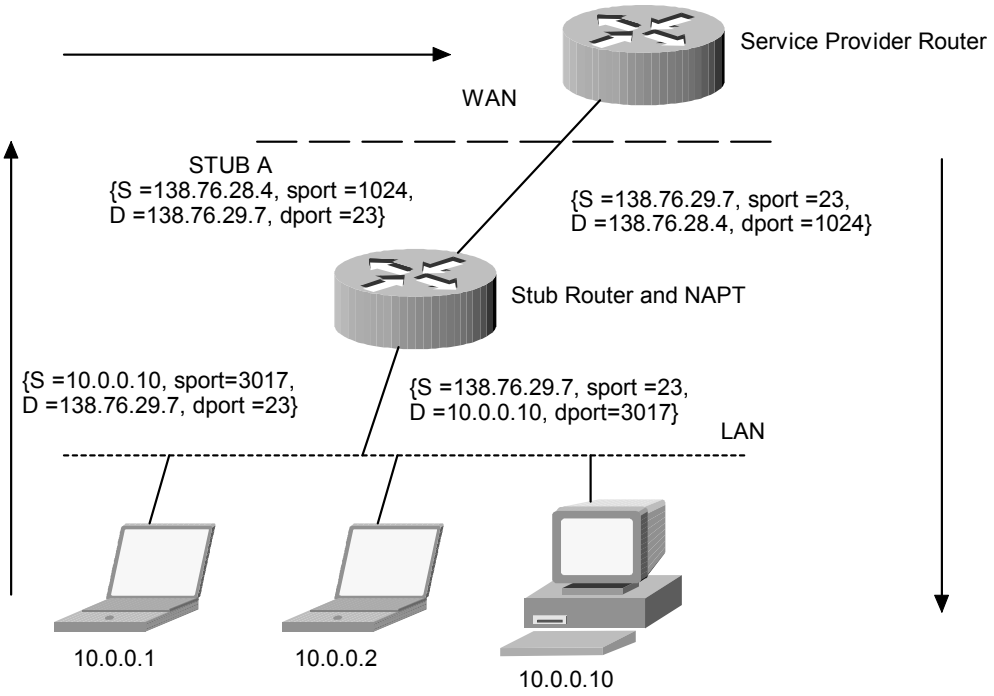
Uno stub domain, con un insieme di indirizzi privati, può comunicare con la rete esterna associando dinamicamente, gli indirizzi privati agli indirizzi pubblici in suo possesso. Con il termine 'possesso', si indica che gli indirizzi pubblici sono stati assegnati da un'autorità competente, come la IANA o un registro equivalente.
Se il numero degli host della rete locale, è uguale, o inferiore al numero degli indirizzi pubblici in possesso, allora, tutti i nodi, possono comunicare con l'esterno contemporaneamente. Altrimenti, solo alcuni nodi, potranno accedere alla rete esterna simultaneamente. E' possibile associare gli indirizzi pubblici a quelli locali, sia in modo statico che dinamico. Se si utilizza l'assegnazione statica, gli host, in qualche caso, potranno essere contattati direttamente dall'esterno. L'associazione dinamica, è una soluzione più flessibile, utilizzata soprattutto, quando il numero di indirizzi pubblici, è inferiore al numero di nodi della rete interna. Inoltre, con questa soluzione, è possibile associare in tempi diversi, nodi diversi allo stesso indirizzo globale. E' importante sottolineare, che gli indirizzi della rete locale, non sono validi all'esterno, ed è una buona regola, non utilizzare mai, un indirizzo pubblico per identificare un host privato. In questo modo, lo stesso indirizzo privato, potrà essere utilizzato in altre reti locali (stub).
Per esempio, consideriamo la figura sottostante in cui entrambi gli stub A e B, utilizzano internamente un indirizzamento di classe A, 10.0.0.0/8. Al NAT dello stub A è assegnato l'indirizzo 198.76.29.0/24 e al NAT dello stub B, l'indirizzo 198.76.28.0/24. Quando l'host

10.33.96.5 dello stub A vuole comunicare con l'host 10.81.13.22 dello stub B, utilizza come destinazione l'indirizzo 198.76.28.4. L'host dello stub A procede inviando il pacchetto al suo router, che successivamente lo inoltrerà al router regionale. Il dispositivo NAT dello stub A, modificherà l'indirizzo da 10.33.96.5 a 198.76.29.7. Il Regional Router, conoscendo gli indirizzi delle sotto reti, lo distribuirà al router dello stub B. Questo inoltrerà il pacchetto all'host corretto.



2.2 Caratteristiche del NAPT

Si ipotizzi che un'organizzazione, con una rete privata, sia connessa all'esterno per mezzo di un collegamento WAN ad un service provider. Allo stub router, è assegnato un indirizzo globale, mentre gli indirizzi degli host privati, hanno esclusivamente significato locale. In questo caso, se due o più nodi, hanno l'esigenza di connettersi simultaneamente alla rete esterna, non possono utilizzare la soluzione del Basic NAT. Il NAPT, Network Address Port Translation, consente di associare ad un unico indirizzo globale, un insieme di indirizzi privati, sfruttando le porte TCP ed UDP (TU). Più precisamente, il NAPT, può associare le tuple del tipo (local IP address, local TU port number) alle tuple del tipo (registered IP address, assigned TU port number), consentendo di utilizzare lo stesso indirizzo globale per più nodi contemporaneamente, grazie al meccanismo delle porte.



Si consideri la figura soprastante, in cui, lo stub A utilizza internamente gli indirizzi di classe A 10.0.0.0/8. Il service provider ha assegnato all'interfaccia WAN dello stub router l'indirizzo 138.76.28.4. Quando l'host 10.0.0.10 spedisce un pacchetto telnet all'host 138.76.29.7, utilizza come destinazione l'indirizzo globale 138.76.29.7 inviando il pacchetto allo stub router. Il router, che può instradare il pacchetto, lo invia sull'interfaccia WAN. Tuttavia, il NAPT, presente sullo stub router, traduce la tupla, formata dall'indirizzo e dalla porta sorgente in un indirizzo globale 138.76.28.4 e nella porta 1024, prima di inviare il pacchetto. I pacchetti di ritorno subiranno una traduzione simile.
Questo modello, può essere esteso, per associare staticamente un nodo con l'indirizzo globale e le porte (TU) per ogni servizio, rendendo l'host, raggiungibile direttamente dall'esterno. Più precisamente, è possibile configurare staticamente le porte TU sullo stub router, in modo che il traffico sia 'rediretto' su uno specifico nodo, all'interno della rete locale. Spesso, per permettere di iniziare sessioni dall'esterno verso l'interno, si utilizza un servizio DNS.
Il NAPT, gestisce oltre che le sessioni TCP ed UDP, anche i messaggi ICMP, con l'eccezione dei messaggi di tipo 'REDIRECT'. I pacchetti del tipo ICMP query, sono tradotti in modo simile a quelli TCP/UDP, in modo che il campo identificatore nell'header ICMP, sia unicamente associato. Più precisamente, il campo identificatore delle query ICMP, è impostato dal Query sender e ritorna inalterato in risposta al messaggio del Query responder. Quindi le tuple (Local IP address, local ICMP query identifier), sono associate alle tuple (registered IP address, assigned ICMP query identifier) dal NAPT router. In questo modo, è possibile identificare in modo univoco, qualsiasi tipo di query appartenente a qualsiasi degli host locali.
Nella configurazione del NAPT router, dove il registered IP address, corrisponde all'IP address dello stub router (WAN interface), è necessario distinguere le sessioni TCP, UDP, ICMP query originate da se stesso, rispetto a quelle originate dagli host della rete locale. Si assume, che tutte le sessioni in ingresso, siano destinate al NAPT router, come se fosse il nodo finale, salvo che la 'porta' del servizio obiettivo (target service port), sia associata staticamente, ad un altro indirizzo della rete locale. Le altre sessioni, ad esclusione di quelle citate, non sono permesse ai nodi della rete locale.

2.3 Le fasi di traduzione per una sessione

Le fasi di traduzione, per una sessione da parte del Traditional NAT, sono tre:

1. Associazione dell'indirizzo
2. Address lookup e traduzione
3. Rilascio dell'indirizzo associato

Associazione dell'indirizzo
E' necessario distinguere i casi a seconda che si utilizzi il Basic NAT o il NAPT.
Con il Basic NAT, un indirizzo privato è associato ad un indirizzo esterno, durante l'inizializzazione della prima sessione, diretta dall'host locale verso l'esterno. Successivamente, tutte le altre sessioni originate dallo stesso indirizzo locale, utilizzeranno questa associazione.
Nel caso del NAPT, in cui diversi indirizzi privati, sono associati ad un unico indirizzo globale, l'assegnazione, è realizzata con il meccanismo delle porte, specificato precedentemente all'inizializzazione della prima sessione, diretta verso l'esterno.
E' possibile, anche se non è una buona soluzione, per un'applicazione residente su un host locale, instaurare simultaneamente sessioni multiple, utilizzando la stessa tupla.

Address lookup e traduzione
Dopo l'associazione degli indirizzi e delle porte, i pacchetti appartenenti alla stessa sessione, saranno soggetti al session lookup per gli scopi di traduzione.

Rilascio dell'indirizzo associato
Quando l'ultima sessione, basata su un particolare indirizzo, oppure sulla tupla (address, TU port) nel caso del NAPT, termina, l'associazione dell'indirizzo sarà terminata. In questo modo, l'indirizzo sarà rilasciato e diventerà disponibile per altre sessioni.

2.4 Traduzione dei pacchetti

I pacchetti delle sessioni pertinenti alla gestione del NAT, sono sottoposti a traduzione in tutte le direzioni. La traduzione di ogni singolo pacchetto è illustrata di seguito.

Manipolazione gli header IP, TCP, UDP e ICMP
Nel Basic NAT, l'header IP deve essere modificato. Le modifiche si riferiscono all'indirizzo IP (source IP per i pacchetti in partenza e destination IP per i pacchetti in arrivo) ed al checksum IP.

Nelle sessioni TCP ed UDP, le modifiche, includono l'aggiornamento del checksum nei campi header. Questo, è necessario, in quanto i checksum TCP/UDP sono calcolati considerando anche uno pseudo header, contenente gli indirizzi IP sorgente e destinazione. Da questa modifica, sono esclusi i pacchetti con header UDP, che contengono checksum con valore '0'. Anche nei pacchetti ICMP Query, non è necessario eseguire modifiche, in quanto gli header non contengono indirizzi IP.

Nella variazione, denominata NAPT, le modifiche agli header IP sono simili alle precedenti. Tuttavia, in questo modello, per le sessioni TCP/UDP, è necessario estendere le modifiche alla traduzione delle porte TU (source TU port per i pacchetti in partenza e destination TU port per i pacchetti in arrivo) negli header TCP/UDP.
Nei pacchetti ICMP Query, è necessario modificare gli header per sostituire i query ID e i checksum. Più precisamente, le query ID degli host privati, devono essere tradotti negli ID assegnati per i pacchetti in partenza, ed esattamente l'opposto per i pacchetti in arrivo. Successivamente, è necessario correggere l'ICMP header checksum, per riflettere le modifiche delle Query ID.

Adattamento dei checksum
Le modifiche che il NAT deve eseguire, sono basate sul pacchetto, e coinvolgono una o più manipolazioni dei checksum per ogni campo tradotto. Queste operazioni, sono dunque intensive. Fortunatamente, esiste un algoritmo, che permette di effettuare queste modifiche in modo relativamente semplice ed efficace. Questo, può essere applicato agli header IP, TCP, UDP ed ICMP eseguendo poche operazioni aritmetiche. Considerando che questi header, utilizzano la somma a complemento a due, è sufficiente calcolare la differenza aritmetica tra il valore precedente e quello successivo alla traduzione, aggiungendolo successivamente a quello presente nel checksum.

Modifica dei pacchetti di errore ICMP

Le modifiche ai pacchetti di errore ICMP, includono cambiamenti agli header IP e ICMP così come agli header dei pacchetti inclusi nel payload. Per consentire al NAT, di essere trasparente rispetto agli host, è necessario procedere con le seguenti operazioni:

1. modificare l'indirizzo IP, contenuto nell'IP header incapsulato nel payload del messaggio di errore
2. modificare il checksum dell'header IP
3. modificare il checksum del messaggio ICMP, per riflettere le modifiche effettuate nel payoad

Nella configurazione del NAPT, se il messaggio IP è incapsulato all'interno del pacchetto ICMP, è di tipo TCP, UDP o ICMP Query, è necessario anche modificare in modo appropriato le porte TU dentro l'header TCP/UDP, oppure il campo Query Identifier, all'interno dell'header ICMP Query. L'ultima modifica riguarda l'intestazione IP del pacchetto ICMP.

Supporto per FTP

Una delle applicazioni più diffuse che richiede l'utilizzo di ALG è l'FTP, File Transfer Protocol. Questo genere di applicazione, utilizza un ALG per controllare i payload ed intercettare i parametri di sessione. Spesso, l'FTP ALG è parte integrante del NAT.
Il funzionamento di questa applicazione, prevede che l'FTP ALG utilizzi una speciale tabella per correggere le sequenze e gli acknowledge dei pacchetti TCP, con le porte sorgenti e destinazione di FTP. Le tuple della tabella, devono contenere queste informazioni:

1. indirizzo sorgente
2. indirizzo di destinazione
3. porta sorgente
4. porta destinazione
5. delta, per i numeri di sequenza
6. timestamp

Una nuova riga della tabella, viene inserita solo quando, il comando FTP PORT o le risposte PASV, sono intercettate. Il numero di sequenza 'delta', viene incrementato o decrementato per ogni comando FTP PORT o risposta PASV. I numeri di sequenza, sono incrementati quando i pacchetti sono in partenza, e gli acknowledge sono decrementati quando i pacchetti sono in arrivo.
Nel Basic NAT, i payload FTP, vengono tradotti solo per gli indirizzi privati e dei loro rispettivi globali. Per la configurazione NAPT, tuttavia, le traduzioni vengono estese anche alle porte TCP interessate.

Supporto DNS

Si consideri che nel Traditional NAT, sono predominanti le sessioni instaurate verso l'esterno, piuttosto che verso l'interno. Il servizio DNS ALG, può essere utilizzato insieme al NAT, come descritto di seguito. Uno o più server DNS interni alla rete privata, mantengono l'associazione dei nomi con gli indirizzi per gli host interni, e a volte, anche per alcuni host esterni. I server DNS esterni, mantengono l'associazione solo per gli host esterni, e non per quelli interni. Se in una rete privata, non esiste un server DNS, è possibile inviare tutte le richieste DNS ad un server esterno.

Trattamento delle opzioni di IP

Un datagramma IP, con una delle seguenti opzioni: Record Route, Strict Source Route, o Loose Source Route, può portare come conseguenza, la registrazione o l'utilizzo degli indirizzi IP dei router intermedi. Un router intermedio, che supporta il NAT può decidere di non utilizzare queste opzioni, oppure, di non tradurre gli indirizzi, mentre processa queste opzioni. Il risultato della scelta di non procedere alla traduzione, può esporre gli indirizzi della rete privata lungo tutto il percorso del pacchetto. Questo però, non dovrebbe mettere a repentaglio il percorso del pacchetto, in quanto si suppone che ogni router si rivolga esclusivamente al next hop router.

2.5 Problematiche

Esistono diverse problematiche legate all'utilizzo del Traditional NAT, le più rilevanti sono:

1. Suddivisione tra indirizzi locali e globali
2. Raccomandazioni sullo spazio di indirizzamento privato
3. Instradamento attraverso il NAT
4. Passaggio da Basic NAT a NAPT

Suddivisione tra indirizzi locali e globali

Il NAT, deve operare una suddivisione tra gli indirizzi utilizzati all'interno della rete privata, rispetto a quelli unici, utilizzati a livello globale. E' importante sottolineare, che un indirizzo, deve essere esclusivamente privato oppure globale, non rispettare questa regola, implica l'insorgere di problemi di sovrapposizione. Questo è illustrato di seguito.

Si consideri il caso in cui un host nello stub A, voglia spedire un pacchetto ad un host dello stub B. Lo stub B, utilizza un indirizzo globale, uguale all'indirizzo privato dello stub A. In questo caso, il router dello stub A, non può distinguere se il pacchetto è destinato all'indirizzo globale dello stub B o alla rete interna.

Raccomandazioni sullo spazio di indirizzamento privato

L'Internet Assigned Numbers Authority (IANA), ha assegnato tre blocchi di indirizzi IP, destinati all'utilizzo nelle reti private. Questi sono:

1. 10.0.0.0/8
2. 172.16.0.0/12
3. 192.168.0.0/16

Un'organizzazione, che decide di utilizzare questi blocchi di indirizzi, non deve confrontarsi con la IANA. In questo modo, ogni organismo, può utilizzare al suo interno gli stessi indirizzi IP di un altro, attivando però, un router di confine (border router) con il device NAT abilitato.

Instradamento attraverso il NAT

Il dispositivo NAT presente su un router di confine, pubblica la struttura della rete globale verso l'interno della rete, ma non il contrario. Tipicamente, il router di confine, possiede un indirizzo per inoltrare il traffico verso la WAN, questo di solito corrisponde con il gateway del service provider.

Passaggio da Basic NAT a NAPT

Una rete privata, solitamente dispone di pochi indirizzi globali. Questo, si traduce in problema quando il numero di host, che si devono collegare verso l'esterno, è superiore al numero di indirizzi globali assegnati. Per ovviare a questo problema, è possibile passare dalla configurazione Basic NAT a NAPT. Tuttavia, un'applicazione che cambia improvvisamente configurazione, può provocare alcuni inconvenienti.

2.6 Limitazioni del NAT

Il meccanismo del NAT ha diverse limitazioni, tuttavia, in questo paragrafo si tratteranno solo quelle legate al Traditional NAT.

Privacy e sicurezza

Il Traditional NAT, è in grado di assicurare meccanismi per la protezione della privacy, sfruttando la comunicazione unidirezionale dagli indirizzi privati a quelli esterni. La stessa caratteristica, rende però difficile il debugging. Ciò, perché non è possibile identificare quale degli host appartenenti alla rete privata, abbia utilizzato o abusato di un servizio esterno.

Risposte ARP e NAT

Il NAT, deve essere abilitato esclusivamente sui router di confine di uno stub domain, altrimenti, potrebbero insorgere alcune problematiche. Tipicamente, un router di confine è collegato ad un WAN link, tuttavia, potrebbe capitare, che questo fosse sostituito con una connessione LAN. Se parte o tutti gli spazi di indirizzamento globale utilizzati dal NAT, appartengono alla stessa sottorete, il NAT sarebbe escluso dal fornire supporto di tipo ARP agli

host della sottorete. Il NAT, risponde alle richieste ARP con il proprio indirizzo MAC quando, configurato come Basic NAT. Se il NAT router, non risponde alle richieste, nessun altro nodo risponderà, quindi gli host, non potranno essere identificati e raggiunti.
Questo scenario, è improbabile utilizzando il NAPT, eccetto quando si ha il passaggio da Basic NAT a NAPT.

Traduzione dei pacchetti TCP/UDP frammentati in partenza nella configurazione NAPT

La traduzione di pacchetti TCP/UDP frammentati, nella configurazione del NAPT, è destinata a fallire. Questo perché solo il primo frammento contiene le intestazioni TCP/UDP, che sono necessarie per associare il pacchetto alla sessione, e utilizzate per gli scopi di traduzione. I pacchetti successivi, non contengono le informazioni circa le porte TCP/UDP, ma semplicemente, trasportano lo stesso identificatore di frammentazione, specificato nel primo frammento.
Si consideri il caso in cui, due host privati, originano pacchetti frammentati verso la medesima destinazione, utilizzando gli stessi identificatori di frammentazione. Quando l'host di destinazione riceve i pacchetti, con identificatori e indirizzo identico non sarà in grado di distinguere le due sessioni. La conseguenza di tutto ciò, è la corruzione di entrambe le sessioni.

2.7 Implementazioni

Sono disponibili molte implementazioni, sia commerciali che sotto licenza GNU, che aderiscono alle caratteristiche del Traditional NAT citate in questo documento.

Architectural Implications of NAT

Implicazioni architetturali dei NAT

3. Introduzione

Nella prima versione dei NAT (Maggio 1994) si intendeva realizzare un modo semplice per permettere un uso più intensivo dello spazio di indirizzamento offerto da IPv4 in previsione di un suo rapido esaurimento. Gli stessi autori si resero però conto che la soluzione portava con sè alcuni inconvenienti e lo specificarono in più punti della raccomandazione da loro redatta. In particolare erano preoccupati della corretta funzionalità di programmi che subissero la modifica delle intestazione dei pacchetti inviati e ricevuti. La preoccupazione era talmente radicata negli autori che nel documento si legge testualmente 'I NAT possiedono alcune caratteristiche negative che li rendono inappropriati per soluzioni a lungo termine e potrebbero renderli inappropriati anche per soluzioni a breve termine'.

Malgrado questi dubbi in pochi anni i NAT si diffusero ampliamente in Internet e in generale le caratteristiche negative non ebbero ripercussioni se non su una minoranza ristretta di applicazioni con particolari esigenze. L'opinione sui NAT rimane comunque divisa tra chi ne vede i vantaggi e chi ne fa notare gli svataggi.

I primi sono concordi nel continuare ad usare e anche ad incrementare il numero di NAT nella rete perché si è dimostrata l'utilità di questo sistema per sfondare i limiti di indirizzamento di IPv4 e si è altresì dimostrata la trasperenza del sistema sui servizi più usati quali Web e Mail.

D'altro canto gli oppositori vedono la miriade di problemi che i NAT comportano e prevedono che prima o poi finiranno per bloccare lo sviluppo di Intenet. Pur considerando l'effettivo problema dello spazio di indirizzamento ridotto di IPv4 vedono nei NAT solo un artificio che non potra essere una soluzione definitiva.

Sicuramente la realtà si pone a metà tra queste due posizioni estreme e in ogni caso il problema sarà risolto dallo spazio di indirizzamento di IPv6. Il problema principale dei NAT rimane però il fatto di non essere perfettamente trasparenti nelle comunicazioni tra nodi e la cosa risulta evidente per quelle applicazioni che trasportano le informazioni di indirizzo anche in punti diversi dall'intestazione IP.

Inoltre l'applicazione dei NAT contrasta con quella che dovrebbe essere la filosofia architetturale di Internet, filosofia da cui deriva la flessibilità e di conseguenza il successo di Internet stessa. Il principio è quello dell'*End-to-End*. Questo principio assume che le funzioni complesse dovrebbero essere svolte solo dai nodi terminali (si identifica qui con il termine 'terminale' ogni nodo che si trovi sul bordo della rete, a prescindere dalla sua funzione) in quanto sono questi a controllare la comunicazione. La rete dovrebbe essere semplicemente un servizio che trasporta i bit tra due (o più) nodi terminali. Le applicazioni eseguite sui terminali sono spesso le uniche che sanno maneggiare correttamente i flussi di dati, senza per altro avere a disposizione strumenti per influenzare il processo instradamento nella rete.

Un'altro vantaggio di Internet è che la rete non conserva informazioni di sessione. Questo permette una reazione rapida ad eventuali malfunzionamenti di alcuni nodi riadattando rapidamente la rete stessa. La mancanza della creazione di sessioni non crea la necessità di notificare connessioni che si formano o che si distruggono agli altri nodi della rete. E allo stesso modo i terminali non devono preoccuparsi di altri nodi se non quello che vogliono raggiungere, il primo router a cui inviare il pacchetto e il nodo che fornisce il serivizio di traduzione dei nomi (DNS).

I NAT (in particolare i NAPT) infrangono molti dei principi del modello End-to-End e introducono le sessioni. Quindi riducono la flessibilità complessiva mentre aumentano la complessità delle operazioni e limitano le capacità diagnostiche della rete.

Alcune varianti di NAT (come RSIP) cercano di recuperare alcuni concetti dell'End-to-End cercando di associare al nodo privato un indirizzo pubblico (ammesso che il numero di porte sia sufficiente), ma non riescono a eliminare problemi come quelli derivanti dall'utilizzo di porte conosciute. Inoltre non risolvono i problemi di DNS (lo stesso dei NAPT) in quanto più nodi avranno lo stesso indirizzo pubblico. Infine i nodi privati dovrebbero subire importanti aggiornamenti per poter utilizzare RSIP (per il funzionamento si veda l'apposito capitolo di questo documento).

Verrebbe da pensare che anche i Firewall comportano molte delle problematiche dei NAT e addirittura ne aggiungono di proprie senza che questo sia presentato come un problema critico. Ma bisogna considerare che i Firewall sono inseriti col preciso obiettivo di interferire con flusso di dati ed è quindi previsto e accettabile che comportino delle complicazioni. Le stesse problematiche non sono tanto accettabili per i NAT in quanto questi si prefiggono la transparenza come uno degli obiettivi primari.

4. Il modello End-to-End

Verranno qui di seguito proposti più in dettaglio le proprietà del modello End-to-End.

L'aspetto fondamentale del modello End-to-End è la proprietà chiamata "fate-sharing" (condivisione del destino). Secondo questa proprietà lo stato di una connessione è determinato solo dai due nodi estremi che la utilizzano. Di conseguenza una connessione può essere interrotta solo se è uno dei due estremi a interromperla, sia in maniera volontaria che a causa di un guasto. Questo è alla base della robustezza delle connessioni di Internet anche con una rete cresciuta a dismisura rispetto alle sue dimensioni iniziali. Se le informazioni di connessione fossero contenute nei nodi attraverso cui la comunicazione si realizza, nel caso di danneggiamento di uno dei nodi intermedi la cominicazione si interromperebbe, venendo a mancare delle informazioni fondamentali a quella comunicazione, mentre sarebbe ancora tecnicamente possibile. Al contrario se le informazioni sono contenute solo negli estremi, un guasto di questi causerebbe l'interruzione della comunicazione in ogni caso.

Nel caso dei NAT si realizza un punto fondamentale per il transito della comunicazione che in caso di guasto interrompe la comunicazione, anche nel caso in cui ci siano dei NAT in parallelo e anche nel caso in cui il guasto corrisponda a una breve interruzione che faccia perdere al NAT le informazioni sulla sessione.

Ci sono altre importanti aspetti del modello End-to-End, sempre in relazione ai NAT:

- se lo stato della comunicazione è tenuto all'interno della rete allora il traffico di quella comunicazione, in caso di guasto, non può essere deviato se non dopo la replicazione delle informazioni di stato in un altro nodo, cosa difficilmente realizzabile in modo efficiente
- se lo stato della comunicazione è tenuto all'interno della rete allora nel caso in cui la rete cresca di dimensioni i nodi centrali della rete stessa sarebbero chiamati a tenere traccia di un numero di sessioni molto più grande di quello per cui sono stati progettati. Risulta perciò conveniente spostare queste informazioni verso i bordi se non proprio sul bordo

Bisogna anche fare una parentesi per quanto riguarda le connessioni sicure. Le applicazioni che richiedono una connessione sicura richiedono che i loro pacchetti attraversino inalterati la rete, cosa che non può accadere in presenza di un NAT. Questi quindi limitano la flessibilità della comunicazione.

Anche le applicazioni che richiedono un indirizzo globale statico (nel tempo di attività dell'applicazione stessa) per il loro funzionamento sono impedite se la loro comunicazione attraversa un NAT (specie un NAPT) in quanto l'indirizzo e la porta vengono associate in modo dinamico all'instaurazione di ogni comunicazione.

Tutte queste limitazioni non sono un problema secondario perché una parte del successo di Internet è dato dalla sua flessibilità che permette a applicazioni sempre nuove di utilizzarlo senza dover richiedere un qualsiasi tipo di aggiornamento, cosa che sarebbe invece richiesta in presenza di un NAT. Tutto questo si ritradurrebbe in un rallentamento nell'introduzione delle innovazioni.

5. Vantaggi derivanti dall'uso dei NAT

Si riportano di seguito i punti che hanno determinato l'ampia diffusione dei NAT in quanto utili per la risoluzione di una serie di problemi.

- Maschera i cambi di indirizzo da parte dell'ISP eliminando la necessità di riassegnare gli indirizzi della rete locale
- Indirizzi globali possono essere riutilizzati per utenti ad accesso intermittente. Questo permette un utilizzo di indirizzi pari al valore dei numero di nodi attivi piuttosto che del numero totale dei nodi
- La possibilità che NAT forniti e gestiti dall'ISP riducano il supporto che questo deve fornire al cliente in quanto si tratterà di dispositivi semplici e a cui questo si collegherà facilmente avendo un'intefaccia conosciuta
- Spezzando Internet in una serie di piccole autorità che gestiscono per conto loro delle piccole reti si facilità il lavoro degli amministratori dei nodi adetti al routing che non dovranno implementare sofisticate tecniche di routing per la gestione di sottoreti a dimensione variabile
- Non sono necessarie modifiche di alcun tipo alle applicazioni che non si basano sull'integrita dal pacchetto IP
- I NAT possono svolgere anche la funzione di Firewall per le connessioni in ingresso

Ancora alcune considerazioni sui punti appena elencati.

Eliminando nodi che non sono attivi in un determinato istante riduce la richiesta di indirizzi pubblici. Anche nei casi in cui i provider non prevedono l'aggregazione di connessioni provenienti da più nodi su un un solo indirizzo si riduce sensibilmente il numero di indirizzi necessari (aumentando la vita dello spazio di indirizzamento di IPv4) e si facilità il lavoro di routing della rete.

Un'altra conseguenza è che lo spazio di indirizzamento della rete locale potrà essere ben più ampio di quello che si potrebbe avere utilizzando indirizzi pubblici in quanto la penuria di indirizzi di IPv4 impone una politica di assegnazione molto restrittiva, votata al risparmio. I NAT dunque permettono anche di risolvere i problemi di crescita imprevista di una rete locale che rimarrebbe bloccata dal numero insufficiente di indirizzi a disposizione.

L'uso dei NAT da parte degli ISP permette una riduzione delle spese per il cliente nei casi in cui l'ISP cambia spazio di indirizzamento e nel caso in cui il cliente voglia cambiare ISP in quanto gli unici indirizzi che dovranno essere modificati saranno quelli del NAT. Gli indirizzi dei terminali potranno rimanere invariati risparmiando sui costi di manuntenzione.

Un'altra pratica applicazione dei NAT è quella in cui una serie di server fornisce un servizio (o una serie di servizi) attraverso un'unico indirizzo IP. Al cliente sembrerà di accedere a un'unico server che ha la capacità di calcolo pari alla somma delle macchine del gruppo e una capacità di trasferimento pari a quella del NAT.

6. Problemi con i NAT

- Spezzano il modello End-to-End e quindi riducono la flessibilità di Internet
- Creano un ulteriore nodo da cui dipende la comunicazione in quanto contiene le informazioni di stato
- Impediscono meccanismi di sicurezza a livello IP
- Permettono l'assegnazione arbitraria di indirizzi all'interno di una rete locale. Questi indirizzi possono essere causa di collisioni quando due reti vengono fuse assieme fisicamente o logicamente
- I NAT che operano a livello 4 (NAPT e RSIP) aumentano la complessità operativa quando dei server pubblici risiedono nel lato privato di una rete
- Alcuni prodotti possono implementare dei NAT senza indentificarsi come tali

L'utilizzo dei NAT impone delle limitazioni della flessibilità. In particolare per tutte quelle applicazioni che presentano un NAT come servizio nascosto, come nei routers di bilanciamento dove il loro utilizzo è completamente trasparente ai due estremi della comunicazione, ma che ugualmente incrina l'integrità del modello End-to-End.

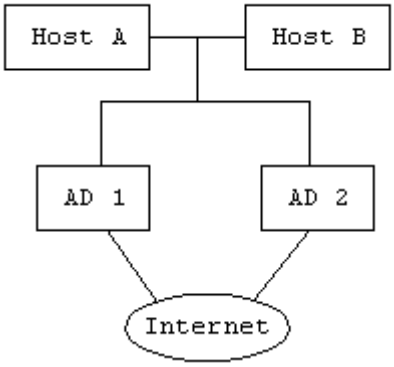
I NAT ipotizzano che ogni connessione sia una comunicazione indipendente. Però alcune applicazioni come FTP e H.323 utilizzano una o più sessioni per controllare il flusso effettivo di dati. Inoltre i NAT non prevedono che gli indirizzi IP possano essere trasmessi in punti diversi dall'intestazione IP. Quindi protocolli che presumono l'integrità del pacchetto non possono lavorare in presenza di NAT. In questi casi è necessario affiancare al NAT un Application Level Gateway (ALG). Si tratta di un dispositivo a Livello 7 integrato nel NAT, o che ci collabora in qualche modo, realizzato specificatamente per ogni applicazione che ne richieda la presenza. In questo caso il NAT dovrà provvedere a ricomporre i frammenti di pacchetto per permettere la traduzione a livello applicativo e dovrà provvedere a modificare i numeri di sequenza TCP prima di inoltrare i singoli pacchetti.

Infine le versioni NAPT (port-multiplexing) di NAT (di largo utilizzo perché permettono l'accesso a Internet attraverso un solo indirizzo) è utile solo nel caso in cui dei nodi privati si devono connettere a dei server pubblici. Nel caso di server pubblici posizionati dietro al NAT il problema può essere risolto solo associando un server locale a una determinata porta logica sull'indirizzo pubblico. Questo perché è necessario considerare la questione delle porte note che non possono essere associate arbitrariamente. In questo modo si limita ogni servizio a un solo terminale. Questa sembrerebbe una limitazione solo per delle reti medio-grandi, ma in realtà causerebbe anche un rallentamento dello sviluppo di reti piccole che in caso di crescita dovrebbero modificare la propria struttura.

7. Scenari

7.1 Singolo punto di rottura

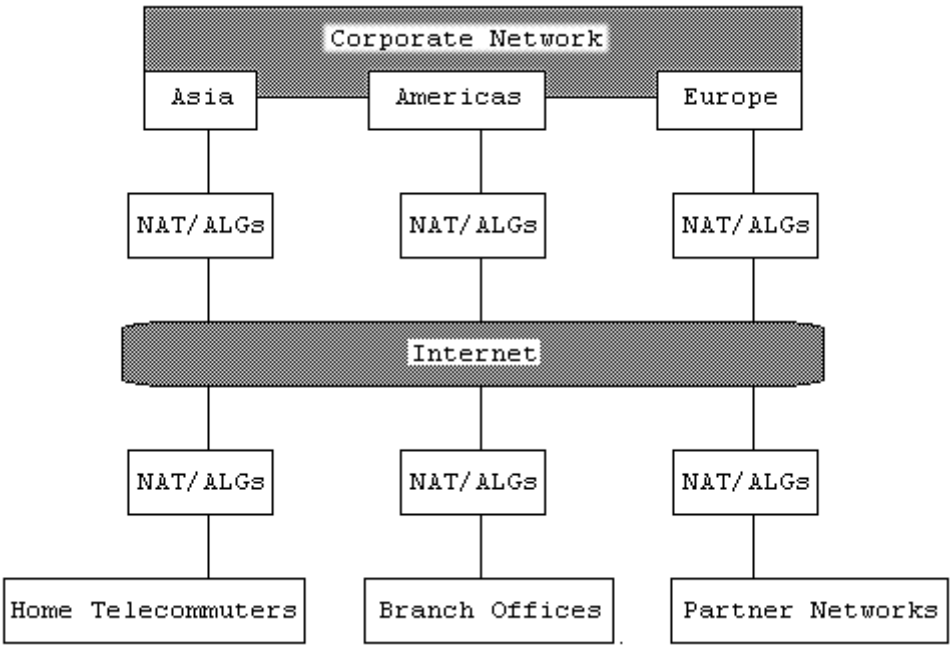
Una caratteristica dei dipositivi a stati come i NAT è la creazione di un punto singolo di rottura, ovvero l'interruzione della comunicazione a causa di un solo punto all'interno della rete e non di uno dei due punti estremi. Tentativi di evitarli tramite la creazione di NAT ridondanti crea una nuova serie di problemi relativi alla tempestiva comunicazione degli stati e problemi relativi al routing. Questi comprendono problematiche quali la frequenza degli aggiornamenti, l'influenza sulle prestazioni di tali aggiornamenti e l'affidabilità degli aggiornamenti stessi. Di fatto tutti i NAT presenti richiedono le informazioni di tutte le sessioni per poter intervenire tempestivamente e tutti i nodi sul bordo della rete devono essere informati sulle alternative esistenti e quindi devono essere costantemente in ascolto.



Nel caso tradizionale in cui i dispositivi di accesso (Access Device - AD) 1 e 2 sono routers, gli unici punti critici sono gli estremi. La soluzione per recuperare la comunicazione in seguito alla rottura del router principale è la redirezione sul router secondario. Notifica che proviene dal router secondario stesso. Nel caso in cui gli AD siano dei NAT la connessione può essere recuperata solo se prima del guasto del NAT principale questo può trasferire le informazioni sulla sessione sul NAT secondario. Si crea quindi un punto fondamentale nella comunicazione al di fuori dei due punti estremi, fatto evidentemente in contrasto con i principi del modello End-to-End di Internet.

7.2 Complessità degli ALG

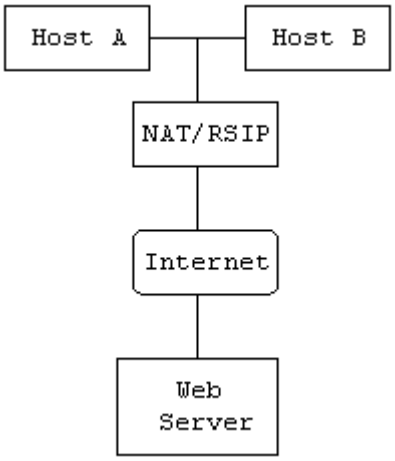
Nel seguente esempio è rappresentata una rete di grosse dimensioni composta da più reti collegati tra di loro dalla rete pubblica. Ognuno degli NAT/ALG rappresentati rappresenta uno o più dispositivi reali in quella determinata località.



La necessità di aggiornare il software a questi livelli darà sicuramente molti grattacapi, anche quando tutti i dispositivi presenti sono dello stesso produttore e dello stesso modello, a causa del tempo necessario. L'utilizzo degli ALG permette invece alle singole reti di usare versioni diverse del software senza che si creino situazioni di incompatibilità nel periodo di transizione.

7.3 Violazioni degli stati di TCP

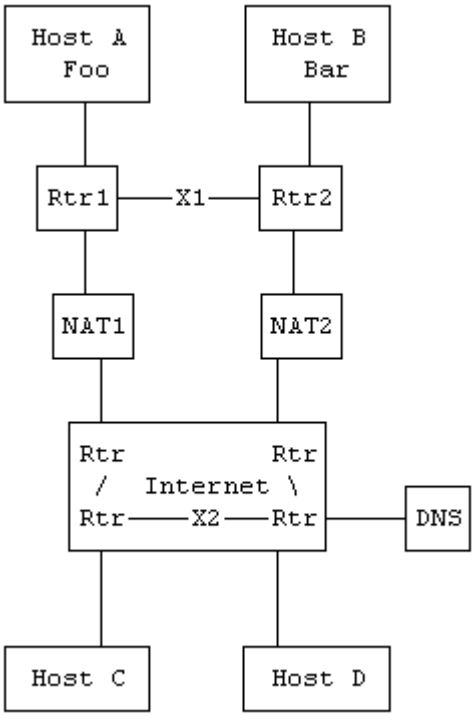
Le incompatibilità dei NAT con i protocolli di livello superiore, come TCP, vengono a galla nella loro interezza solo in situazione di distribuzione molto ampia grazie all'aumentata diversità tra i singoli utilizzatori. Nell'esempio è rappresentato uno scenario delle problematiche analizzate nel capitolo precedente.



Si ipotizzi che l'Host A completi la sua transazione e chiuda la connessione TCP sulla porta 80 del Web Server e che RSIP liberi l'indirizzo pubblico utilizzato dall'Host A. Successivamente l'Host B apre una connessione con lo stesso Web Server e il NAT gli assegna il prossimo indirizzo pubblico libero, che nel nostro esempio sarà la stesso assegnato precedentemente all'Host A. Può succedere che la porta locale utilizzata dall'Host B per la connessione sia la stessa utilizzata dall'Host A in precedenza. Il Web Server rifiuterà la connessione in quanto dal suo punto di vista l'host remoto ritenta di collegarsi con la stessa tupla TCP senza aspettare il TIME WAIT di 4 minuti imposto dal protocollo. Un nuovo tentativo di collegamento da parte dell'Host B andrà a buon fine. Si tratta quindi di un problema occasionale che però rimane non risolto.

7.4 Gestione simmetrica degli stati

La gestione operativa di reti che incorporano dispositivi a stati che modificano i pacchetti è molto più semplice se le connessioni entranti e quelle uscenti seguono gli stessi percorsi. Anche se formalmente semplice non ne è altrettanto semplice l'implementazione utilizzando un protocollo privo di stati quale IP. La soluzione del problema sta nel fare in modo che le connessioni entranti e uscenti passino da un'unico dispositivo, ma questo può causare problemi nel caso in cui si modifica la topologia dei collegamenti interni e/o esterni. Si consideri la situazione rappresentata in figura dove la -X- indica un collegamento interrotto.



Per motivi di efficienza i Router 1 e 2 utilizzano il NAT1 per accedere alla rete pubblica. Allo stesso modo le connessioni provenienti dall'esterno utilizzano il NAT1 per accedere alla rete locale. Nel momento in cui si rompe il percorso X1 il Router 2 sarà costretto a utilizzare il NAT2, ma il percorso di ritorno continuerà ad essere NAT1 in quanto questo continuerà a mettere a disposizione i suoi indirizzi. Si crea una situazione in cui per l'Host B non è possibile comunicare. Se al posto dei NAT ci fossero dei router, questi notificherebbero la modificata struttura della rete risolvendo il problema. In questo caso la ridondanza di NAT è addirittura inutile.

Si ipotizzi invece la rottura del collegamento X2 e che il DNS risponda a una richiesta di risoluzione per gli Host A e B con gli indirizzi di entrambi i NAT. Quando l'Host D tenta di accedere all'Host B la richiesta passa attraverso NAT2, ma a causa del routing interno la risposta passerà attraverso NAT1 che inizializzerà un'altra sessione. Anche a collegamento X2 ripristinato la connessione non potrà avvenire perché le risposte continueranno ad attraversare NAT1 e quindi l'indirizzo a cui si invia una richiesta e l'indirizzo da cui arriverà la risposta continueranno ad essere diversi.

Una terza situazione può essere quella in gli Host A e B tentano di contattare l'Host D mentre i collegamenti X1 e X2 sono danneggiati. L'Host B non ha problemi. L'Host A non è in grado di raggiungere la destinazione. La situazione è tanto più caotica se gli amministratori degli Host A e B non conoscono la struttura della rete Internet (cosa probabile) e quindi non riescono a spiegarsi perché funziona solo uno dei due collegamenti quando entrambi gli accessi alla rete funzionano. Ancora una volta il fatto che i NAT contengano informazioni sugli stati aumenta le problematiche e riduce il vantaggio della ridondanza.

8. Considerazioni sulla sicurezza

I NAT (e in particolar modo i NAPT) hanno le potenzialità per abbassare il livello medio di sicurezza perché creano l'illusione di una barriera protettiva senza che abbiano effettivamente le proprietà di un firewall.

8.1 IPsec

IPsec (IP Secure) definisce una serie di meccanismi per l'autenticazione e la cifratura a livello IP dei pacchetti. Chiaramente questo sistema è meno efficiente dei sistemi di sicurezza a livello superiore, ma potenzialmente è un sistema che si può diffondere basandosi sulla sua robustezza.

Purtroppo, come detto più volte, i NAT impediscono il passaggio di pacchetti IPsec in quanto modificano i pacchetti stessi. Tale limite impedisce la diffusione di questo sistema di sicurezza. In particolare:

- Non è possibile proteggere l'IP dell'intestazione
- I certificati d'autenticazione contengono l'indirizzo IP
- L'Encrypted Quick Mode contiene anch'esso l'indirizzo IP e il numero di porta
- Il Revised Mode a chiave pubblica codificata contiene l'identità del peer

Potrebbe essere possibile adattare il NAT ai diversi sistemi di sicurezza, ma un uso su larga scala di questo metodo, considerando il numero di NAT e di sistemi di sicurezza, rende questa soluzione impraticabile. I NAT quindi pongono un serio ostacolo alla diffusione di queste tecnologie.

Fortunatamente sistemi diffusi di sicurezza quali TLS, SSL e SSH posso convivere con i NAT in quanto non utilizzano l'indirizzo IP come identificatore. Questi sistemi non sono però sufficienti per particolari applicazioni in quanto l'intestazione del paccheto TCP/IP non è protetto.

Network Address Translation - Protocol Translation (NAT-PT)

Traduzione di indirizzi di rete - Traduzione di protocollo

9. Introduzione

IPv6 è una nuova versione del protocollo IP pensato in relazione all'enorme crescita che ha avuto Internet in questi anni. Il vecchio protocollo IPv4, ideato negli anni '70, ha uno spazio di indirizzamento piccolo e male organizzato, in relazione alle dimensioni attuali della rete. Inoltre impedisce l'uso di tecniche di routing più sofisticate e aggressive. IPv6 dovrebbe risolvere i problemi attuali di Internet. E probabilmente anche quelli futuri.

Il passaggio dal vecchio standard a quello nuovo non sarà immediato, ma obbligherà a un periodo di transizione in cui una parte di Internet continuerà ad utilizzare ancora IPv4, mentre il resto della rete passerà a IPv6. Le reti di Internet che adottano versioni di IP diverse dovranno però continuare a comunicare pur non essendo direttamente compatibili tra di loro.

Si illustrerà di seguito un sistema per la comunicazione tra nodi che adottano esclusivamente IPv4 e nodi che adottano esclusivamente IPv6, una soluzione che evita l'utilizzo di macchine che supportino contemporaneamente entrambi gli standard (dual-stack) o di altre tecniche (tunneling).

NAT-PT si basa su due raccomandazioni preesistenti:

- NAT - Network Address Translation - (trattato in un'altra parte di questo documento) che descrive la traduzione trasparente degli indirizzi di nodi con identificativo locale per permettere la comunicazione di questi con l'esterno
- SIIT - Stateless IP/ICMP Translation Algorithm - che descrive un meccanismo per la traduzione di indirizzi V6 in indirizzi V4 con un algoritmo senza stati e indipendente dal protocollo di livello superiore utilizzato. Questa raccomandazione propone di assegnare a un nodo V6 un nodo V4 per comunicare con la rete che utilizza IPv4, ma non specifica come questi indirizzi vengano assegnati.

NAT-PT compone quindi le proprietà di un NAT con lo schema di traduzione SIIT tra IPv4 e IPv6. NAT-PT utilizza un gruppo di indirizzi IPv4 che verranno assegnati dinamicamente ai nodi V6 in modo trasparente sia ai nodi V4 che ai nodi V6. Quindi il NAT-PT deve gestire la comunicazione come una sessione per mantenere l'associazione per tutta la durata della connessione e si comporta di fatto come un NAT per reti V4 con la differenza che la sua rete locale è una rete basata su IPv6.

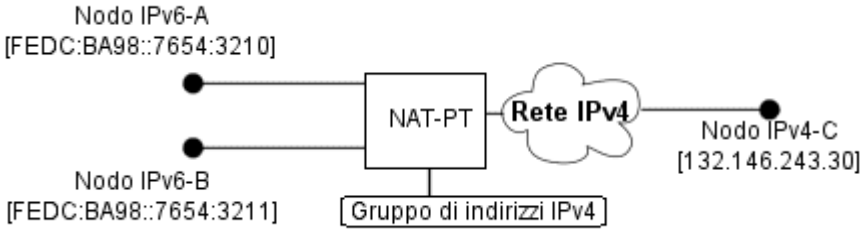
Analogamente ai NAT, NAT-PT prevede due modalità:

- BASIC-NAT-PT che prevede l'associazione univoca tra il gruppo di indirizzi V4 a disposizione del NAT-PT e il gruppo di indirizzi V6 da servire.
- NAPT-PT che permette di associare a più nodi V6 lo stesso indirizzo V4

10. Connessione da IPv6 verso IPv4 - Basic-NAT-PT

Questa prima modalità permette l'associazione di un nodo V6 a uno degli indirizzi V4 a disposizione. Essendo probabile una situazione in cui il numero di nodi V6 supera quello degli indirizzi V4 a disposizione è necessario un'associazione dinamica in luogo di una statica.

Ipotizziamo una situazione come quella rappresentata in figura 1



Si ipotizza quindi l'invio di un pacchetto dal nodo IPv6-A al nodo IPv4-C. Il pacchetto conterrà le informazioni di mittente e destinatario, ovvero:

- Indirizzo mittente: SA=FEDC:BA98::7654:3210
- Indirizzo destinatario: DA=PREFIX::132.146.243.30

Nota: gli indirizzi IPv6 saranno indicati su 64 bit per semplicità di lettura

L'indicazione *PREFIX::* indica l'indirizzo del NAT-PT all'interno della rete IPv6. Ogni pacchetto recante questo prefisso verrà quindi ricevuto dal NAT-PT. Questa soluzione permette di gestire il raggiungimento del NAT-PT sfruttando l'instradamento della rete e quindi senza dover salvare alcun tipo di dato nei terminali. Di fatto una soluzione molto flessibile.

Il NAT-PT, ricevendo il pacchetto, verifica se questo è un pacchetto di inizializzazione di una comunicazione (che verrà chiamata sessione), per esempio il pacchetto SYN di TCP. Se il pacchetto non è di inizializzazione e la sessione ancora non esiste il pacchetto verrà scartato senza notifiche.
In caso contrario il NAT-PT inizializza una sessione associando un indirizzo IPv4 tra quelli a disposizione al nodo IPv6, ovvero inizializza i parametri per la traduzione degli indirizzi.

Si ipotizza che l'indirizzo IPv4 da associare al nodo V6 sia 120.130.26.10. In questo caso il pacchetto verrà modificato affinché abbia i seguinti dati di mittente e destinatario:

- Indirizzo mittente: SA=120.130.26.10
- Indirizzo destinatario: DA=132.146.243.30

Il pacchetto verrà quindi normalmente inoltrato alla rete V4. L'eventuale risposta dal nodo IPv4-C avrà le informazioni di mittente e destinatario invertiti rispetto a quelli del pacchetto ricevuto. Il NAT-PT modificherà nuovamente i dati preparando un pacchetto IPv6 da inoltrare alla rete V6 per consegnarlo al nodo IPv6-A:

- Indirizzo mittente: SA=PREFIX::132.146.243.30
- Indirizzo destinatario: DA=FEDC:BA98::7654:3210

11. Connessione da IPv6 verso IPv4 - NAPT-PT

L'acronimo NAPT-PT sta per *Network Address Port Translator - Protocol Translator*. In questa modalità il NAT-PT può associare più nodi V6 a un solo indirizzo IPv4. Questo è possibile modificando, oltre che l'indirizzo, anche il numero di porta, quindi lavorando a livello 3, ovvero TCP/UDP.

In questo modo si supera una delle problematiche più ovvie derivante dall'uso del Basic-NAT-PT, ovvero il fatto che una volta associati tutti gli indirizzi IPv4 a disposizione, i nodi V6 che in seguito richiedono una connessione con la rete IPv4 non possono essere accontentati, quindi il

numero di indirizzi V4 deve essere comparabile a quelli V6 o per lo meno al numero atteso di connessioni contemporanee da terminali V6 verso nodi V4. Una condizione molto restrittiva.

NAPT-PT invece permette a 63k connessioni TCP e 63k connessioni UDP di utilizzare lo stesso indirizzo IPv4, aumentando quindi in modo determinante il numero di nodi V6 per ogni indirizzo V4 a disposizione.

Ritornando all'esempio precedente modifichiamo la *figura 1* sostituendo il NAT-PT con un NAPT-PT. Il nodo IPv6-A crea quindi il suo pacchetto diretto al nodo IPv4-C:

- Indirizzo mittente: SA=FEDC:BA98::7654:3210 / Porta TCP=3017
- Indirizzo destinatario: DA=PREFIX::132.146.243.30 / Porta TCP=23

Il NAPT-PT utilizzarà una delle porte TCP a disposizione dell'indirizzo IPv4 per tradurre nel seguente modo il pacchetto ricevuto:

- Indirizzo mittente: SA=120.130.26.10 / Porta TCP=1025
- Indirizzo destinatario: DA=132.146.243.30 / Porta TCP=23

Il traffico di ritorno dalla porta 23 del nodo IPv4-C verrà quindi inoltrato al corrispondente nodo V6 tramite un'ulteriore traduzione delle informazioni di mittente e destinazione del pacchetto:

- Indirizzo mittente: SA=PREFIX::132.146.243.30 / Porta TCP=23
- Indirizzo destinatario: DA=FEDC:BA98::7654:3210 / Porta TCP=3017

12. Connessione da IPv4 verso IPv6 - NAPT-PT

Se si ha la necessità di permettere l'accesso a terminali V6 si può utilizzare un NAPT-PT, ma in questo caso a ogni servizio che si vuole fornire (quindi per ogni porta TCP/UDP) può essere associato un solo terminale nella rete V6. Il NAPT-PT dispone di una tabella di associazione statica tra porta TCP/UDP e nodo V6.

Ancora nella *figura 1* ipotizziamo il nodo IPv6-A come l'unico server HTTP (porta 80) del dominio V6. Se il nodo IPv4-C invia una richiesta del tipo:

- Indirizzo mittente: SA=132.146.243.30 / Porta TCP=1025
- Indirizzo destinatario: DA=120.130.26.10 / Porta TCP=80

Il NAPT-PT tradurrà nel seguente modo:

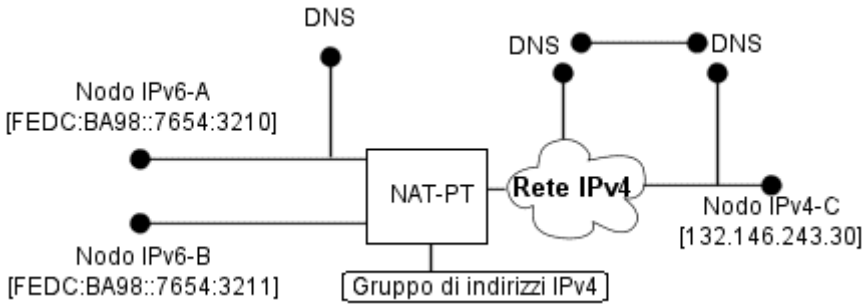
- Indirizzo mittente: SA=PREFIX::132.146.243.30 / Porta TCP=1025
- Indirizzo destinatario: DA=FEDC:BA98::7654:3210 / Porta TCP=80

Risulta evidente che tutte le connessioni sulla porta 80 dal lato V4 del NAPT-PT verranno inoltrate allo stesso nodo V6.

13. Uso di DNS-ALG per l'assegnamento degli indirizzi

13.1 Assegnamento di indirizzi V4 per connessioni entranti (da V4 a V6)

Si ipotizzi una situazione come quella rappresentata in figura 2



In questa situazione il nodo IPv4-C richiede al suo DNS la risoluzione del nome del nodo IPv6. La richiesta verrà inoltrata fino al DNS presente nella rete V6 e quindi tale richiesta attraverserà il NAT-PT.

Il NAT-PT, che identifica i pacchetti TCP/UDP DNS in quanto indirizzati alla Porta 53, esegue le seguenti operazioni:

1. Per le richieste di risoluzione da Nome a Indirizzo del nodo: modifica della richiesta da tipo 'A' a tipo 'AAAA' o 'A6'
2. Per le richieste di risoluzione da Indirizzo a Nome del nodo: sostituzione della stringa "IN-ADDR.ARPA" con la stringa "IP6.INT" e dell'indirizzo V4 che precede la detta stringa con il corrispondente indirizzo V6

Allo stesso modo dovrà essere trattata la risposta del DNS nella rete V6 e diretta ai DNS della rete V4:

1. Traduzione dei record di tipo 'AAAA' o 'A6' in record di tipo 'A'. Se la risoluzione dell'indirizzo è completa è necessario tradurre solo i record di tipo 'A6'
2. Traduzione dell'indirizzo V6 risolto dal DNS con l'indirizzo V4 assegnato dal NAT-PT.

Nel caso in cui il NAT-PT non ha ancora assegnato nessun IPv4 all'indirizzo V6 risolto dal DNS della rete V6 ne viene assegnato uno.

Per esempio se la risposta del DNS per una richiesta di risoluzione dell'indirizzo di IPv6-A da parte di IPv4-C è:

- IPv6-A AAAA FEDC:BA98::7654:3210

Il DNS-ALG integrato nel NAT-PT provvederà a modificarlo nel seguente modo:

- IPv6-A A 120.130.26.1

e terrà in memoria l'associazione tra i due indirizzi, ovvero inizializza una sessione.

A questo punto IPv4-C riceverà il risultato della risoluzione e potrà instaurare una connessione inviando un pacchetto con i seguenti campi di mittente e destinatario:

- Indirizzo mittente: SA=132.146.243.30 / Porta TCP=1025
- Indirizzo destinatario: DA=120.130.26.1 / Porta TCP=80

Il pacchetto, nel momento in cui è ricevuto dal NAT-PT sarà tradotto, con l'ausilio della tabella di traduzione che contiene il record, in questo modo:

- Indirizzo mittente: SA=PREFIX::132.146.243.30 / Porta TCP=1025
- Indirizzo destinatario: DA=FEDC:BA98::7654:3210 / Porta TCP=80

e quindi la comunicazione può continuare in modo abituale.

Nel caso in cui il NAT-PT associ gli indirizzi in modo dinamico i campi TTL (Time To Life - Tempo di vita) delle risposte DNS dovrebbero avere valore 0 per evitare che l'associazione rimanga salvata nei DNS della rete V4 in quanto l'associazione sarà limitata a una singola sessione. Nel caso di assegnamenti statici è possibile lasciare il valore TTL originale.

13.2 Vulnerabilità

L'assegnazione degli indirizzi IPv4 per i nodi IPv6 descritto è suscettibile ad attacchi DOS (Denial of Service) in quanto un numero eccessivo di richiesta di risoluzioni (e quindi altrettante inizializzazioni di sessione) può causare l'esaurimento degli indirizzi IPv4 a disposizione e quindi il blocco di ulteriori connessioni, sia in uscita, che in entrata. Si consiglia quindi di utilizzare un tempo massimo di vita per ogni sessione ed eventualmente riservare un indirizzo IPv4 per le connessioni uscenti in modo da evitare un blocco totale delle comunicazioni verso l'esterno in caso di attacco.

13.3 Assegnamento di indirizzi V4 per connessioni uscenti (da V6 a V4)

Un nodo V6 che volesse connettersi verso un nodo V4 richiede al suo DNS la risoluzione del nome del nodo V4. Il server DNS può contenere le informazioni necessarie a tale scopo e in questo caso non viene richiesto l'intervento del DNS-ALG presente nel NAT-PT in quanto la richiesta non passerà nella rete V4.

E' stato già spiegato che i nodi V6 che volessero connettersi a nodi V4 pongono il prefisso PREFIX:: nel campo destinatario del pacchetto in modo che raggiunga il NAT-PT e che questo lo inoltri nella rete V4. Questo permette anche al NAT-PT di inizializzare le sessioni per le connessioni uscenti e quindi di assegnare un indirizzo IPv4 e una porta alla sessione stessa.

Utilizziamo la *figura 2* per un secondo esempio. In questo caso il nodo IPv6-A vuole connettersi al nodo IPv4-C. Quindi fa una richiesta al suo DNS di risolvere il nome. Il DNS inoltra la richiesta al DNS-ALG del NAT-PT che non sapendo se il nodo di destinazione sia IPv4 o IPv6 inoltra alla rete V4 due richieste DNS, una in formato 'A' e l'altra in formato 'AAAA' o 'A6'. Nel caso ritorni risolta la richiesta AAAA/A6 questa viene inoltrata inalterata al DNS presente sulla rete V6. In caso contrario il DNS-ALG è costretto a modificare la risposta come nel seguente modo:

- Risposta: IPv4-C A 132.146.243.30
- Traduzione:
  IPv4-C AAAA PREFIX::132.146.243.30 oppure
  IPv4-C A6 PREFIX::132.146.243.30

La risposta verrà quindi salvata dal DNS nella rete V6 per poter essere utilizzata in seguito.

14. Problematiche derivanti dall'uso di NAT-PT

Le problematiche derivanti dall'uso di NAT-PT sono le stesse che riguardano i NAT e si rimanda alla relativa sezione di questo documento (Architectural Implications of NAT).

Un'ulteriore limitazione deriva dalla traduzione dei messaggi DNS in quanto incompatibile con l'uso di DNSSEC (DNS Secure) a causa delle connessioni autorizzate non supportate dal NAT-PT.