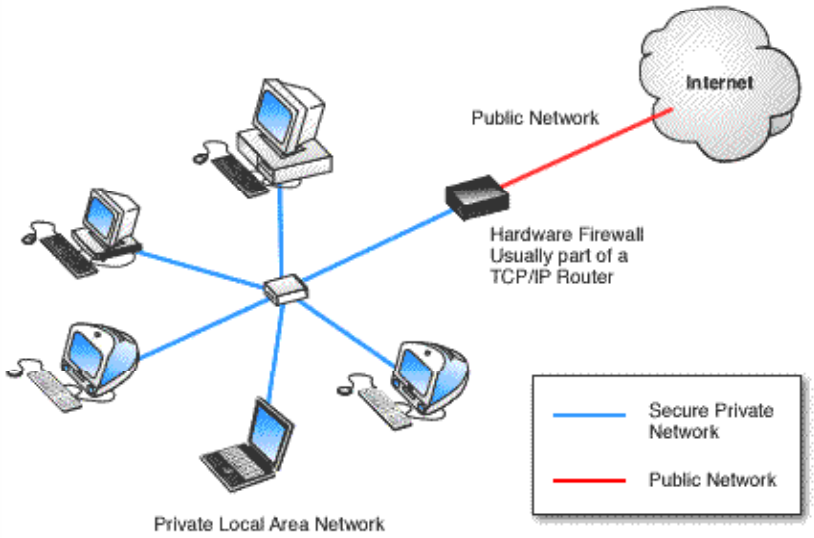
INDICE

- Motivazioni
  - Integrazione dei servizi
  - Vantaggi e problemi aperti
- Architettura di riferimento
- La codifica vocale
- Il trasporto
  - RTP e RTCP
  - QoS in reti IP e VoIP requirements
- La segnalazione
  - H.323
  - SIP
- Cenni su VoIP reliability
- *Problemi del VoIP con NAT e firewalls*
- Qualità della voce
- Valutazione oggettiva della qualità della voce
  - L'algoritmo PESQ

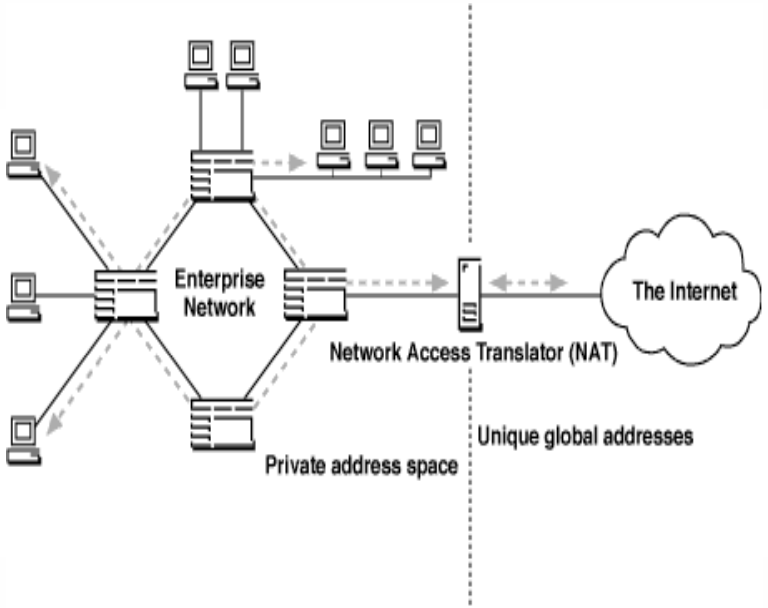
VoIP, NAT e FIREWALLS

- Il VoIP è una tra le numerose applicazioni che incorrono in parecchi problemi quando i flussi corrispondenti devono attraversare NAT e firewalls
  - Esistono soluzioni al riguardo, ma aumentano la complessità operazionale – ed il costo - della telefonia via Internet



Ma che cos'è un NAT?

- Si tratta di un Network Address Translator
  - È un dispositivo che, dislocato al confine tra rete pubblica e privata, esegue la conversione tra indirizzi privati e indirizzi IP pubblici, registrati presso l'Internet Authority, IANA
    - ✓ Il NAT deve modificare l'IP address, ma anche i checksum di IP e di TCP/UDP!
  1. Tipicamente impiegato e tollerato per far fronte alla scarsità di indirizzi IP
  2. Protegge la privacy di una rete, non rivelandone la topologia e l'attribuzione interna degli indirizzi
  - Solitamente supportato dai firewall
  - Sender e receiver non si accorgono della presenza del NAT



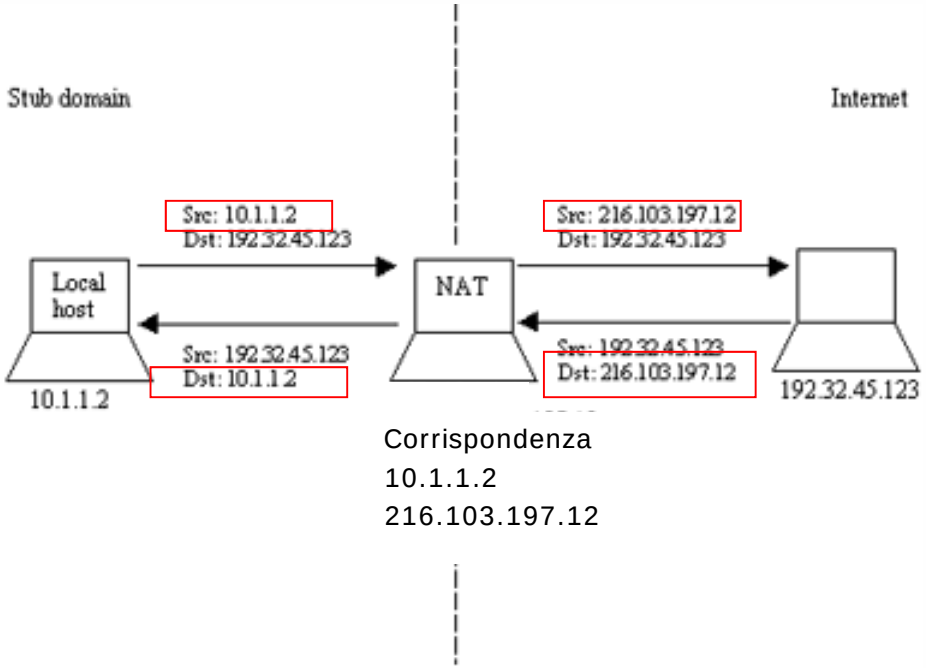
Continua

Esistono tre principali tipi di NAT

- *NAT statico*

  Il NAT router mantiene una tabella associativa tra ciascun indirizzo IP interno e quello corrispondentemente attribuito (registrato) all'esterno

  - Necessario registrare un IP address per ogni host che si connette ad Internet
  - Non comporta alcun risparmio sul numero di indirizzi IP registrati
  - Utile per consentire l'accesso dei dispositivi dall'esterno, via Internet
  - Di modesto interesse



Continua

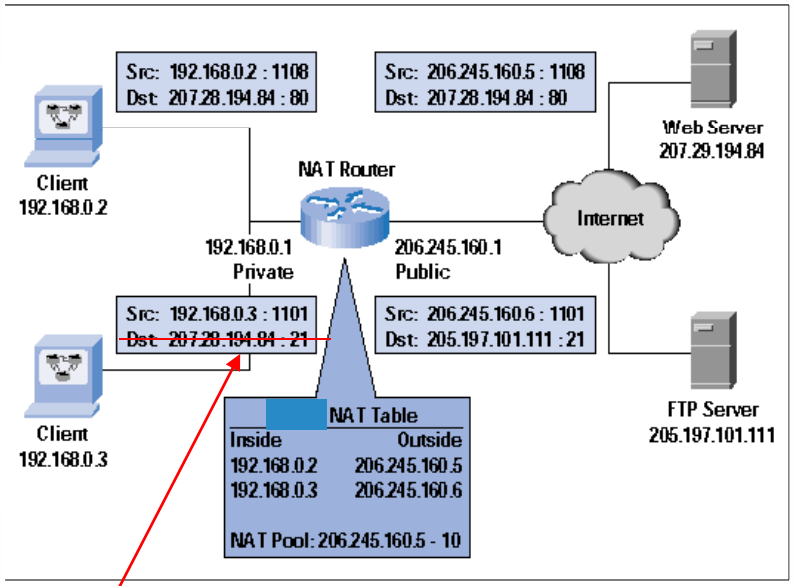
- *NAT dinamico*

  Il NAT router mantiene una lista di indirizzi IP registrati, dunque pubblici, che vengono condivisi dinamicamente da una intera sottorete privata IP

  Ogni volta che un host interno chiede di accedere ad Internet, il router mappa il suo indirizzo privato in un indirizzo pubblico che risulta attualmente non in uso

  Quando la connessione termina o va in timeout, il binding cessa di esistere, ed il NAT ricolloca l'indirizzo pubblico nel gruppo di quelli utilizzabili

  - Molto diffuso
  - È necessario un numero di indirizzi pubblici pari al numero di connessioni verso Internet che si desidera poter supportare contemporaneamente



205.197.101.111:21

E il NAPT?

- **Network Address Port Translation**

  Si tratta di una variante al NAT dinamico, noto anche come Single-Address NAT/Overloading/Masquerading

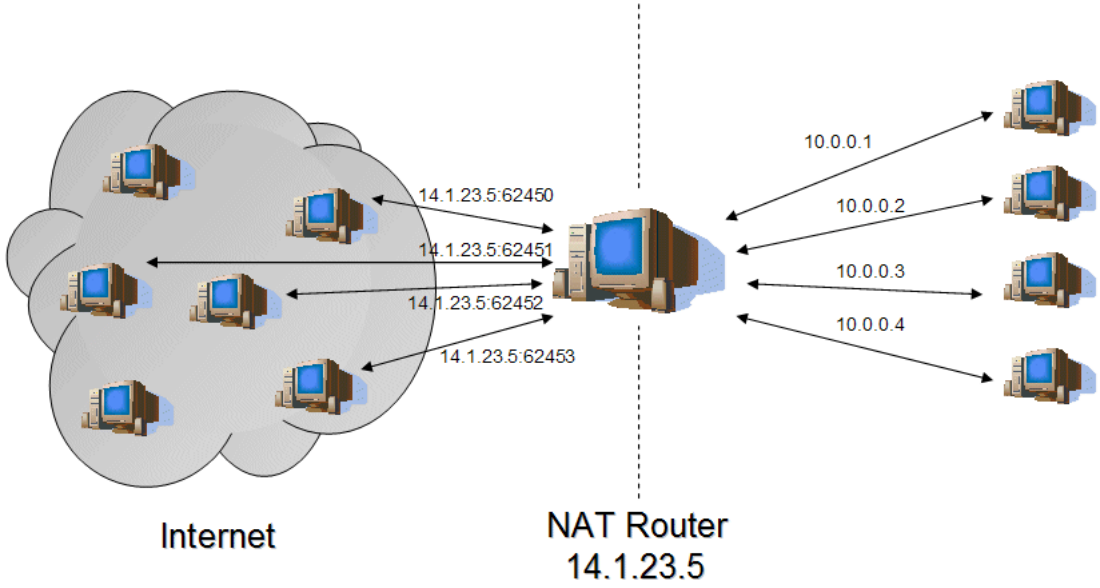
  Il NAT router possiede in tal caso un solo indirizzo IP pubblico che viene condiviso da più clienti interni attraverso un'operazione di multiplexing attuata attribuendo alle connessioni di tali client numeri di porta TCP/UDP **diversi**

  Esempio:

  - ✓ Gli host con indirizzi IP privati 10.0.0.2 e 10.0.0.3 inviano entrambi dati dalla porta 1180
  - ✓ Il router NAPT traduce entrambi nell'indirizzo pubblico 9.245.160.1, con due distinti numeri di porta sorgente, rispettivamente 5431 e 5432
  - ✓ Il NAPT instrada il traffico di risposta per la porta 5431 a 10.0.0.2:1180, mentre il traffico per la porta 5432 viene inviato a 10.0.0.3:1180

Continua

- I Provider di servizi DSL spesso assegnano un singolo indirizzo IP
  - Utenti residenziali multihost, teleworkers, piccole imprese impiegano dispositivi NAPT (chiamati talvolta SOHO routers)
    - ✓ Consente a più dispositivi di condividere il medesimo indirizzo IP



Complicazioni con il NAT

- VoIP è una tra le tante applicazioni che possono essere influenzate negativamente quando gli IP client si connettono attraverso un NAT, Network Address Translator
  - Un NAT tipicamente impiega un Application Level Gateway (ALG)
  - L'ALG ispeziona e modifica il payload dell'applicazione per consentire ai pacchetti di una specifica applicazione o protocollo di attraversare in modo trasparente il NAT
  - Pochi dispositivi NAT garantiscono tuttavia nell'ALG funzionalità per il trattamento di applicazioni VoIP!

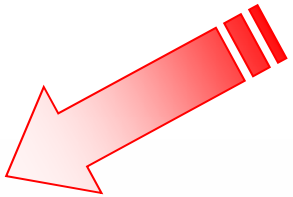
Le categorie di problemi 1 / 3

- Molte applicazioni VoIP non funzionano con il NAT in quanto il payload del livello applicativo contiene informazioni sull'IP address o sulle porte impiegate
  - Un NAT semplice modifica solo l'IP address del pacchetto (datagramma IP), non l'IP address e le porte che compaiono nel payload dell'applicazione
    - ✓ Nel caso di H.323, i pacchetti di call setup contengono proprio tali informazioni nel payload!! => Discrepanza …
- *Esempio*:
  - I messaggi SIP possono contenere degli URI che specificano indirizzi di segnalazione nei campi "Contact", "To", "From".
  - Una volta attraversato il NAT, **gli indirizzi IP ed anche i domain name** nella host portion dell'URI possono non essere più validi

Ricordiamo ad esempio che …

Messaggio INVITE

INVITE sip:bob@nice.com SIP/3.0
Via: SIP/3.0/UDP 192.2.4.4:5060
To: Bob < sip:555-6666@nice.com >
From: Aline < sip:555-1234@nice.com >
Tag=203 941 885
Call-ID: b95c5d87f7721@192.2.4.4
Cseq: 26 563 897 INVITE
Contact: < sip:555-1234@**192.2.4.4** >
Content-Type: application/SDP
Contact-Length: 142
Segue SDP



Le categorie di problemi 2 / 3

- H.323 e SIP, così come altri protocolli di livello applicazione (FTP e RTSP), impiegano sessioni “bundled”, ovvero
  - una sessione di controllo che consente di instaurare una o più sessioni dati viene aperta utilizzando numeri di porta correlati a quelli della sessione dati
  - Il NAT non può determinare la dipendenza che sussiste tra le diverse sessioni “bundled” e assegna indirizzi e numeri di porta scorrelati a tali sessioni
    - ✓ Non funziona …

Le categorie di problemi 3 / 3

- Un'applicazione che tenta di instaurare una sessione da un dominio esterno sarà in grado di individuare il chiamato di un dominio privato solo se ne conosce l'IP address assegnatogli esternamente
  - Questo è un problema per un NAT dinamico tradizionale, che consente di stabilire sessioni in una sola direzione

CARATTERISTICHE H.323

- H.323 è una suite protocollare che fa uso di diversi stream UDP e di porte assegnate dinamicamente
  - Una chiamata H.323 è costituita da svariate e diverse connessioni simultanee
    - ✓ Ci sono due o più connessioni TCP per ogni chiamata
    - ✓ Per una voice conference call, possono essere aperte fino a quattro diverse porte UDP
    - ✓ Tutte le connessioni, tranne una, sono su porte assegnate dinamicamente
  - In particolare:
    - ✓ Durante la fase di instaurazione della chiamata, una connessione TCP trasporta la segnalazione H.225 ed i messaggi Q.931
    - ✓ Durante lo Slowstart call setup, un'altra connessione TCP trasporta i messaggi H.245 con le caratteristiche del terminale ed i parametri di chiamata richiesti, senza che ci sia una well-known port associata a questo canale H.245
    - ✓ È il canale H.225 a recare le informazioni per la porta H.245!!

Continua

- ✓ *Il firewall deve monitorare il canale H.225 per la porta H.245, in quanto non è possibile implementare una regola statica sufficientemente restrittiva, che consenta il passaggio della connessione H.245 mentre blocca altre connessioni TCP*

Inoltre

- ✓ Durante il FastStart call setup, il messaggio H.245 è “nascosto” all’interno del messaggio H.225 insieme al messaggio Q.931
- ✓ Per operare correttamente, un ALG deve modificare gli indirizzi dentro tali messaggi, che sono di lunghezza variabile

Queste difficoltà non hanno impedito ai costruttori di sviluppare dei firewalls NAT-enabled con funzionalità ALG che consentano il passaggio di H.323

Tuttavia, firewalls e NAT di dimensioni modeste e poco costosi non includono ALG H.323

Problemi di NAT/Firewalls con RTP

- Molte applicazioni multimediali, VoIP incluso, impiegano RTP congiuntamente a UDP
  - Non ci sono porte associate deterministicamente a RTP, ed è pertanto impossibile definire *regole statiche* che consentano l'attraversamento dei firewall ai flussi RTP, senza permettere ad altri pacchetti indesiderati di attraversarli

Inoltre,

- Le porte RTP e RTCP sono abbinate
  - ✓ RTP riceve un numero di porta pari
  - ✓ RTCP riceve il successivo numero di porta dispari
- NAPT tipicamente assegna i nuovi numeri di porta in modo random, cancellando il precedente abbinamento
- Quanto al NAT, questo esegue una sostituzione degli indirizzi sorgente e destinazione impiegati, e in assenza di un processing ad-hoc, questi non corrispondono a quelli impiegati nelle connessioni di controllo
  - ✓ I dispositivi multimediali possono non associare correttamente le sessioni RTP alla chiamata corrispondente

Le soluzioni

- Prevedere un ALG nel NAT o nel firewall
  - L'ALG ispeziona e modifica il contenuto del payload dell'applicazione così da consentire al traffico VoIP di attraversare il NAT/firewall
    - ✓ Soluzione commerciale più diffusa
    - ✓ ALG-enabled firewalls sono costosi
    - ✓ Più ALG nello stesso firewall ne aumentano la complessità e possono degradarne le prestazioni
    - ✓ Qualsiasi modifica apportata ai protocolli VoIP richiede un upgrade per tutti quei firewalls che la chiamata VoIP attraversa

Continua

- Prevedere un proxy posizionato al confine tra due dominii (per esempio, tra uno spazio di indirizzi IP privato ed uno pubblico)
  - Solo specifici protocolli, come il SIP e l'H.323, attraversano il proxy
  - Il proxy esegue in modo trasparente il relay dei messaggi di segnalazione che l'applicazione VoIP prevede, così come dei flussi RTP
  - Tutti gli altri tipi di traffico devono necessariamente attraversare il NAT/firewall per comunicare tra i due dominii

Continua

- Un terzo approccio alternativo è quello di rimuovere la logica dell'applicazione dal NAT/firewall
  - Un firewall control proxy (FCP), posizionato sul percorso compiuto dalla segnalazione tra i dominii pubblico e privato, esegue il monitoraggio dei segnali di call setup (ad esempio quelli previsti da H.323 e SIP) e comanda al firewall di consentire l'accesso a quegli stream RTP destinati agli indirizzi IP consentiti
  - In tale caso il firewall apre dinamicamente dei "pinholes" per le chiamate VoIP, senza esporre la rete privata ad una penetrazione da parte di un ampio gruppo di indirizzi IP

Continua

- IETF sta esplorando tale approccio nel Middlebox Communications (Midcom) Working Group

  Obiettivi:

  - convergere su un protocollo di controllo che consenta ad un dispositivo terzo (il FCP) di controllare “middlebox” quali NAT e firewalls
  - Attraverso una interfaccia generalizzata standard di comunicazione per i middlebox
    - ✓ Migliorare le prestazioni
    - ✓ Diminuire i costi di sviluppo e manutenzione software
    - ✓ Facilitare lo sviluppo di nuove applicazioni
  - Entrambe le soluzioni, ALG e FCP/MidCom, richiedono modifiche al progetto dei NAT e firewalls

Continua

- Un quarto tipo di soluzione cerca di ottenere l'attraversamento del NAT e/o del firewall
  - senza modificarne il progetto
  - Senza intaccarne la security
- Due internet draft suggeriscono soluzioni al riguardo:

  entrambe prevedono l'impiego di proxy server esterni, con connessioni persistenti verso i dispositivi VoIP/multimediali
  - Le prerogative essenziali sono
    - ✓ L'utente dietro al NAT deve inviare il primo pacchetto per stabilire il binding
    - ✓ Le comunicazioni verso l'utente A devono avvenire verso la porta sorgente da cui i dati di A provengono

Riferimenti bibliografici

- J. Davidson, J. Peters, “Fondamenti di Voice Over IP”, CISCO Press.
- B. Goode, “Voice Over Internet Protocol (VoIP)”, Proceedings of IEEE, Vol.90, n.9, settembre 2002.