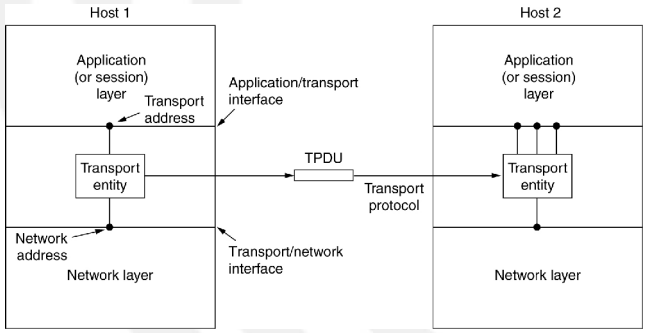
Livello Trasporto
Protocolli TCP e UDP

Davide Quaglia

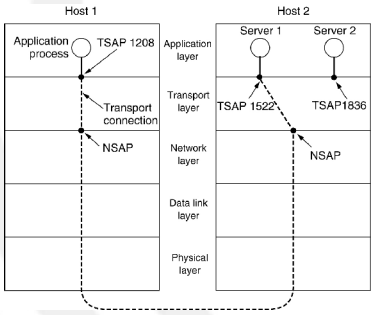
Motivazioni

- Su un host vengono eseguiti diversi processi che usano la rete
- Problemi
  - Distinguere le coppie di processi che si stanno scambiando i dati
  - Fornire meccanismi adatti al tipo di applicazione coinvolta
    - Affidabilità
    - ecc...

Servizi forniti ai livelli soprastanti

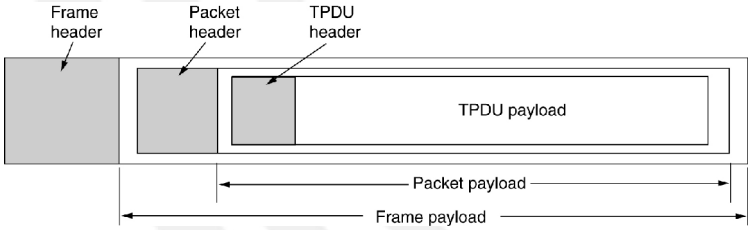


Indirizzamento e multiplexing

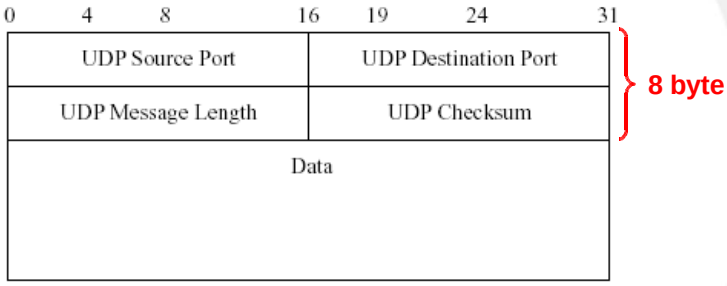


Indirizzo visto dall'applicazione --> NSAP:TSAP
es: 157.27.242.32:3450

Imbustamento



User Datagram Protocol (UDP)



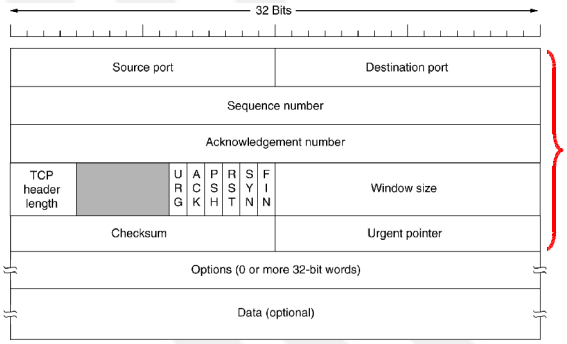
UDP (2)

- Servizio non orientato alla connessione e non confermato
  - Solo multiplex delle applicazioni
  - La checksum copre la PDU UDP e parte del header IP
- Utilizzato per applicazioni in cui:
  - l'affidabilità non è richiesta (multimedia)
  - i dati scambiati stanno tutti in un pacchetto (es. Network Time Protocol)

Transmission Control Protocol (TCP)

- Multiplex delle applicazioni
- Servizio orientato alla connessione
- Trasmissione
  - affidabile (con acknowledge)
  - ordinata
  - byte-oriented
  - full duplex
- Controllo di flusso
- Controllo di congestione

Transmission Control Protocol (TCP)

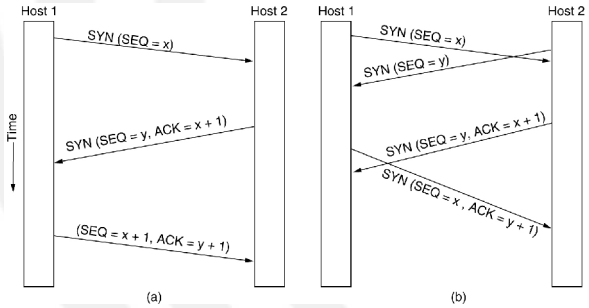


20 byte obbligatori

Transmission Control Protocol (TCP)

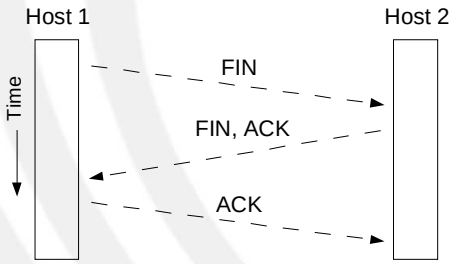
- La *source port* e la *destination port* sono i numeri delle porte cui sono associati gli applicativi che usano la connessione TCP.
- Il *sequence number* è il numero di sequenza del primo byte del campo dati del messaggio. È utilizzato anche come identificatore della sliding window.
- Lo *acknowledge number* è il campo di acknowledge con tecnica di piggybacking della trasmissione nella direzione opposta. Contiene il numero di sequenza del primo byte che il mittente si aspetta di ricevere.
- *Offset*: numero di parole da 32 bit che compongono l'header TCP, variabile in funzione del campo option.
- *Flags*: contiene i bit SYN, ACK, FIN per la creazione/distruzione della connessione
- Il campo *window* contiene la dimensione della receiving window e quindi lo spazio disponibile nei buffer per il traffico entrante.
- La *checksum* copre la PDU TCP e parte del header IP
- Il campo *urgent pointer* punta al primo byte urgente nel pacchetto.

Creazione di una conn TCP



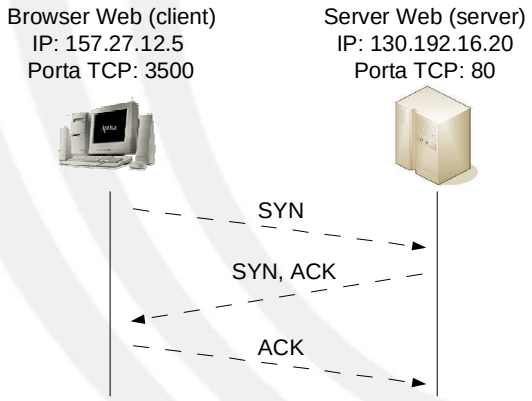
(a) Caso normale
(b) Collisione tra chiamate → viene creata 1 sola connessione

Distruzione di una conn TCP



La connessione deve essere esplicitamente chiusa in entrambe le direzioni; quando il FIN riceve l'ack la direzione corrispondente viene chiusa.

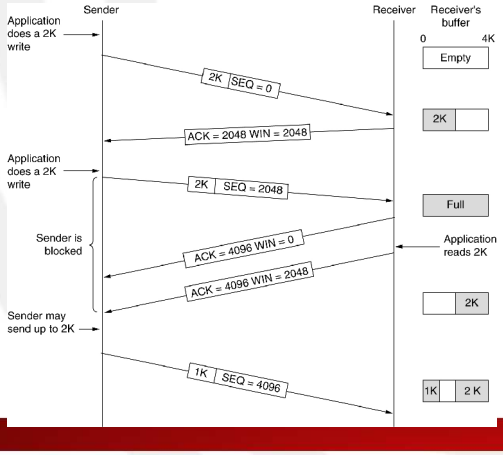
Liv. trasporto e modello client/server



Osservazione

- Il servizio TCP “fa vedere” alle applicazioni un “tubo” simile ad un file o ad una pipe in cui leggere e scrivere gruppi di byte di dimensione arbitraria (anche 1 solo)
- Attenzione che questo servizio “virtuale” è implementato sopra un livello network (IP) che non prevede connessioni
  - Tra due host di una connessione TCP i pacchetti IP possono fare strade differenti nelle due direzioni

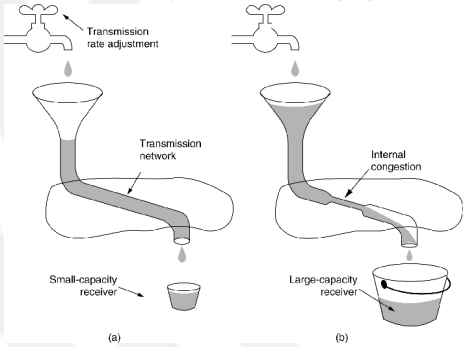
Controllo di flusso



Congestioni

- L'architettura di rete TCP/IP adotta un modello di comportamento chiamato **Best Effort**
  - La rete fa il suo meglio per recapitare pacchetti
  - Non rifiuta mai nuovi utenti (a differenza della rete telefonica)
- Possono verificarsi **congestioni** nelle code dei router
  - Un pacchetto IP che arriva ad una coda piena viene scartato

Congestioni (2)

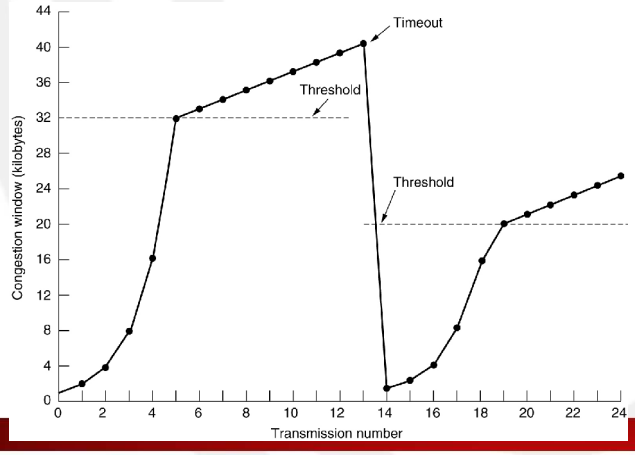


a) un trasmettitore veloce che sovraccarica il ricevitore
b) un trasmettitore veloce che sovraccarica la rete

Controllo delle congestioni

- TCP permette di ridurre il presentarsi di congestioni
- Il trasmettitore mantiene
  - una **finestra di congestione** che corrisponde al numero di byte che può inviare
    - cresce esponenzialmente ogni volta che arriva un ack
    - viene resettata al timeout di un acknowledge (= pck perso)
  - una **soglia** oltre la quale la finestra cresce linearmente
    - viene dimezzata al timeout di un acknowledge (= pck perso)

Controllo delle congestioni (2)



Controllo delle congestioni (3)

- Questo meccanismo assume l'ipotesi che un pacchetto perso sia sintomo di congestione
- Ipotesi non sempre vero nel caso di wireless (WLAN e IP su cellulari)
  - Basse prestazioni del TCP su reti wireless

Interfaccia programmazione socket

Primitive socket per TCP

Primitive	Meaning
SOCKET	Create a new communication end point
BIND	Attach a local address to a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Block the caller until a connection attempt arrives
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

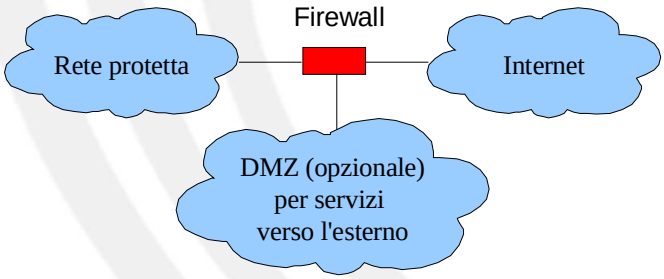
Firewall

- Dispositivo che protegge una rete IP da attacchi provenienti da altre reti IP
- Tutto il traffico IP in entrata/uscita passa per il firewall
- Spesso il router fa anche da firewall
- Eventuale presenza di una rete non protetta per servizi accessibili dall'esterno come il web e la posta (de-militarized zone = DMZ)

Firewall (2)

- Sul firewall si possono mettere regole di accettazione/rifiuto su tipi di traffico
  - IP_{sorg}
  - IP_{dest}
  - tipo di protocollo di trasporto (TCP|UDP)
  - Valore dei Flags TCP: SYN, ACK, FIN
  - $Porta_{sorg}$
  - $Porta_{dest}$

Firewall (3)



NAT e PAT

- Reti private = Intranet
  - Non possono essere usati come destinazioni IP
- Network Address Translation (NAT)
  - Utilizzato dai client interni alla rete privata
- Path Address Translation (PAT) o NAT inverso
  - Utilizzato dai server interni alla rete privata
- Indirizzi privati + NAT/PAT è una soluzione ad alta sicurezza

Network Address Translation (NAT)

- Network address translation o NAT = traduzione degli indirizzi di rete = network masquerading = native address translation
- E' una tecnica che consiste nel modificare gli indirizzi IP dei pacchetti in transito su un sistema.
- Spesso implementato dai router e dai firewall.
- Si può distinguere tra source NAT (SNAT) e destination NAT (DNAT), a seconda che venga modificato l'indirizzo sorgente o l'indirizzo destinazione del pacchetto che inizia una nuova connessione.

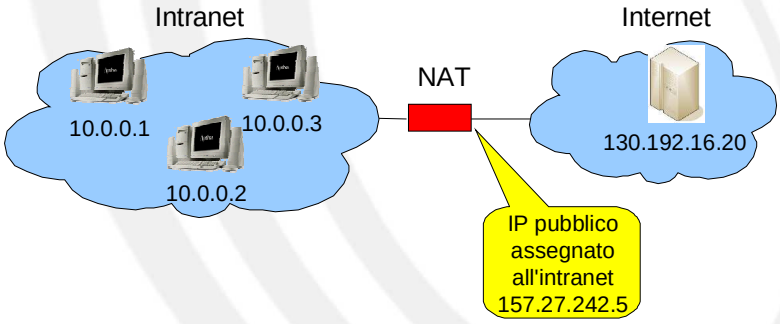
NAT (2)

- I pacchetti che viaggiano in senso opposto verranno modificati in modo corrispondente, in modo da dare ad almeno uno dei due computer che stanno comunicando l'illusione di parlare con un indirizzo IP diverso da quello effettivamente utilizzato dalla controparte.
- Storicamente il NAT si è affermato come mezzo per ovviare alla scarsità di indirizzi IP pubblici disponibili
  - gli indirizzi IP pubblici, essendo una risorsa limitata, hanno un prezzo; per molti utenti Internet (soprattutto residenziali) questo costo è inutile.
  - Il metodo NAT rende i calcolatori non direttamente raggiungibili da internet, per cui spesso questa configurazione viene scelta per ragioni di sicurezza.

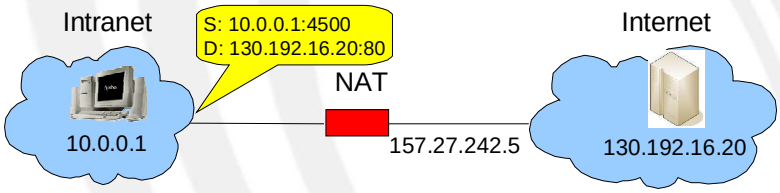
Indirizzi privati

- Definiti in RFC 1918 - Address Allocation for Private Internets
- Tre lotti di indirizzi
  - 10.0.0.0 - 10.255.255.255 (10.0.0.0/8)
  - 172.16.0.0 - 172.31.255.255 (172.16.0.0/12)
  - 192.168.0.0 - 192.168.255.255 (192.168.0.0/16)
- Non vengono mai “annunciati” dai protocolli di routing distribuito

NAT: un esempio



NAT: un esempio (2)



NAT: un esempio (2)

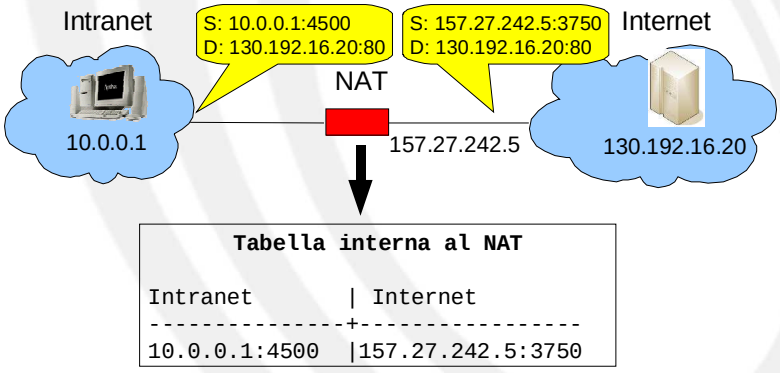


Tabella interna al NAT

Intranet	Internet
10.0.0.1:4500	157.27.242.5:3750

NAT: un esempio (2)

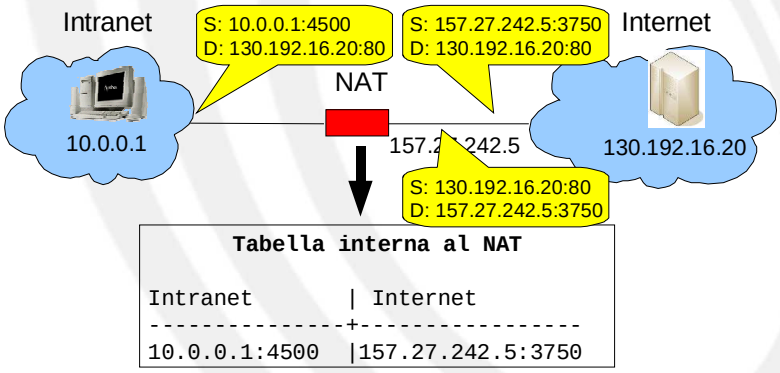


Tabella interna al NAT

Intranet	Internet
10.0.0.1:4500	157.27.242.5:3750

NAT: un esempio (2)

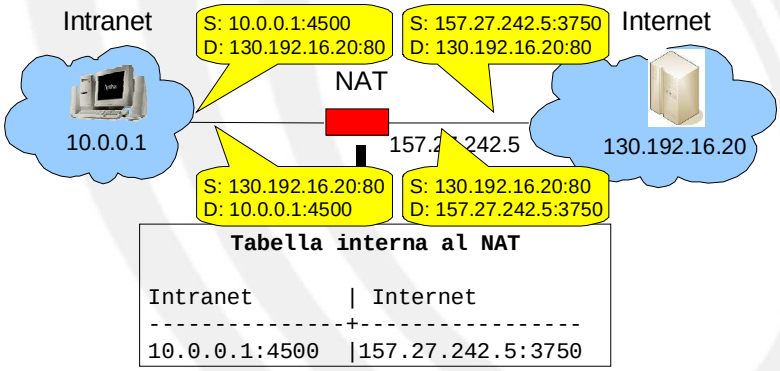


Tabella interna al NAT

Intranet	Internet
10.0.0.1:4500	157.27.242.5:3750

NAT: PROBLEMI

- Il NAT non è ben visto dai puristi delle reti, in quanto mina profondamente la semplicità di IP, e in particolare viola il principio della comunicazione “da qualsiasi host a qualsiasi host”. Questa critica "filosofica" si ripercuote in conseguenze pratiche:
  - Le configurazioni NAT possono diventare molto complesse e di difficile comprensione.
  - L'apparato che effettua il NAT ha bisogno di mantenere in memoria lo stato delle connessioni attive in ciascun momento. Questo a sua volta viola un principio insito nella progettazione di IP, per cui i router non devono mantenere uno stato relativo al traffico che li attraversa.

NAT: PROBLEMI (2)

- Possono essere necessarie grandi quantità di memoria sul router.
  - E' più costoso realizzare architetture di router ridondati perché è necessario che il router di backup mantenga sempre aggiornata una copia della tabella NAT del router principale.
- Alcune applicazioni inseriscono nel payload info relative al livello IP o TCP/UDP. Questo rende difficile attraversare un NAT, ed è necessario che il dispositivo NAT analizzi il traffico di controllo riscrivendo queste informazioni.
  - VoIP
  - FTP

Port Address Translation (PAT)

- Il procedimento NAT descritto è scatenato dall'apertura di una connessione dall'intranet all'Internet e non al contrario
  - non è possibile raggiungere un server web dall'esterno verso l'interno perché all'interno ci sono IP privati
- Occorre mappare un indirizzo pubblico in un indirizzo privato --> PAT o destination NAT

PAT: un esempio

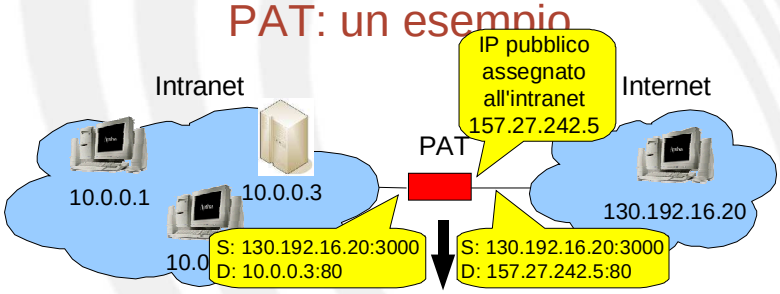


Tabella interna al PAT

Internet	Intranet
157.27.242.5:80	10.0.0.3:80