Corso “DOMOTICA ED EDIFICI INTELLIGENTI” – UNIVERSITA’ DI URBINO
Docente: Ing. Luca Romanelli
Mail: romanelli@baxsrl.com

Networking

NAT

Sommario

- L’indirizzamento privato e pubblico
- I meccanismi di address translation

Indirizzi IP privati

IANA-Allocated, Non-Internet Routable, IP Address Schemes

Class	Network Address Range
A	10.0.0.0-10.255.255.255 (10.0.0.0/8)
B	172.16.0.0-172.31.255.255 (172.16.0.0/12)
C	192.168.0.0-192.168.255.255 (192.168.0.0/16)

NAT: network address translation

Benefici:

- Accedere alla Internet pubblica senza richiedere indirizzi IP registrati
- Interconnettere reti IP con spazi di indirizzamento sovrapposti
- Ridurre il consumo di indirizzi ufficiali (Port Address Translation - PAT)
- Migliorare la sicurezza della rete “nascondendo” gli indirizzi reali degli host
- Flessibilita’ (possibilita’ di mantenere il proprio schema di indirizzamento anche nel caso di un cambiamento di ISP)

NAT: caratteristiche

- Descritto in RFC 1631 (Maggio 1994)
- Modifica gli indirizzi IP nell'header IP (e se serve nel campo applicativo) secondo la politica definita dal gestore
- La traduzione puo' essere:
  - **statica**: la mappatura e' statica uno-a-uno tra indirizzi interni ed esterni
  - **dinamica**: la corrispondenza tra indirizzo interno ed indirizzo esterno e' definita solo all'occorrenza

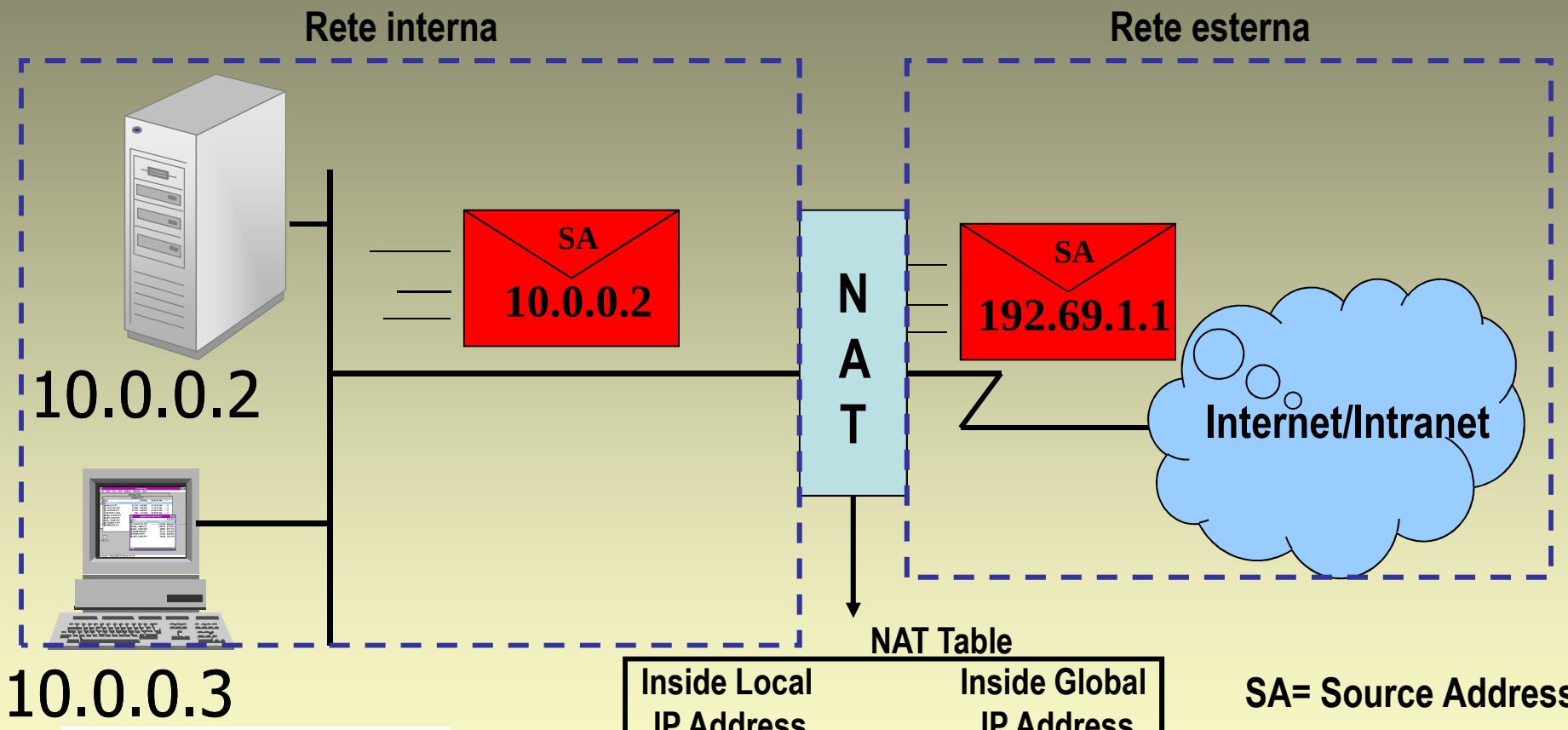
NAT: terminologia

- **Inside local (IL)**
  - L'indirizzo IP di un host della rete interna. Questo indirizzo puo' essere pubblico ed univoco, pubblico ma ufficialmente assegnato ad un'altra organizzazione oppure privato
- **Inside global (IG)**
  - L'indirizzo IP di un host interno cosi' come appare alla rete esterna
- **Outside Local (OL)**
  - L'indirizzo IP di un host esterno cosi' come appare alla rete interna
- **Outside Global (OG)**
  - L'indirizzo IP di un host della rete esterna

NAT: tipi di traduzione

- **Network Address Translation (NAT)**
  - Traduce solo gli indirizzi
  - Traduzione uno-a-uno, statica o dinamica
  - Funzione in ambedue i versi (interno<->esterno)
- **Port Address Translation (PAT)**
  - Traduce le coppie indirizzo/port
  - Traduzione uno-a-N
  - Riduce il consumo di indirizzi IP registrati
  - Funziona in un solo verso (interno->esterno)

NAT: traduzione SA interno -> esterno



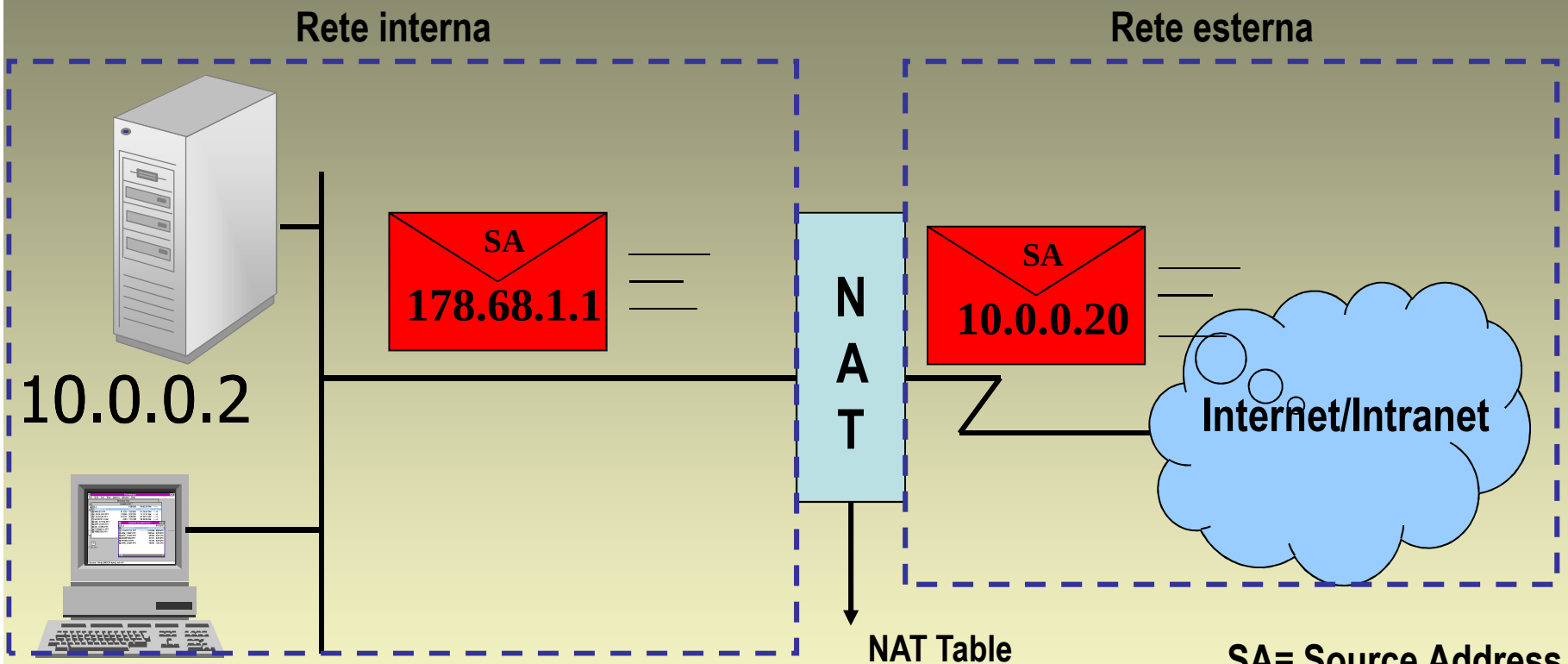
NAT Table

Inside Local IP Address	Inside Global IP Address
10.0.0.2	192.69.1.1
10.0.0.3	192.69.1.2

SA= Source Address

Viene anche tradotto il Destination Address (DA) da esterno ad interno nei messaggi di risposta

NAT: traduzione SA esterno->interno



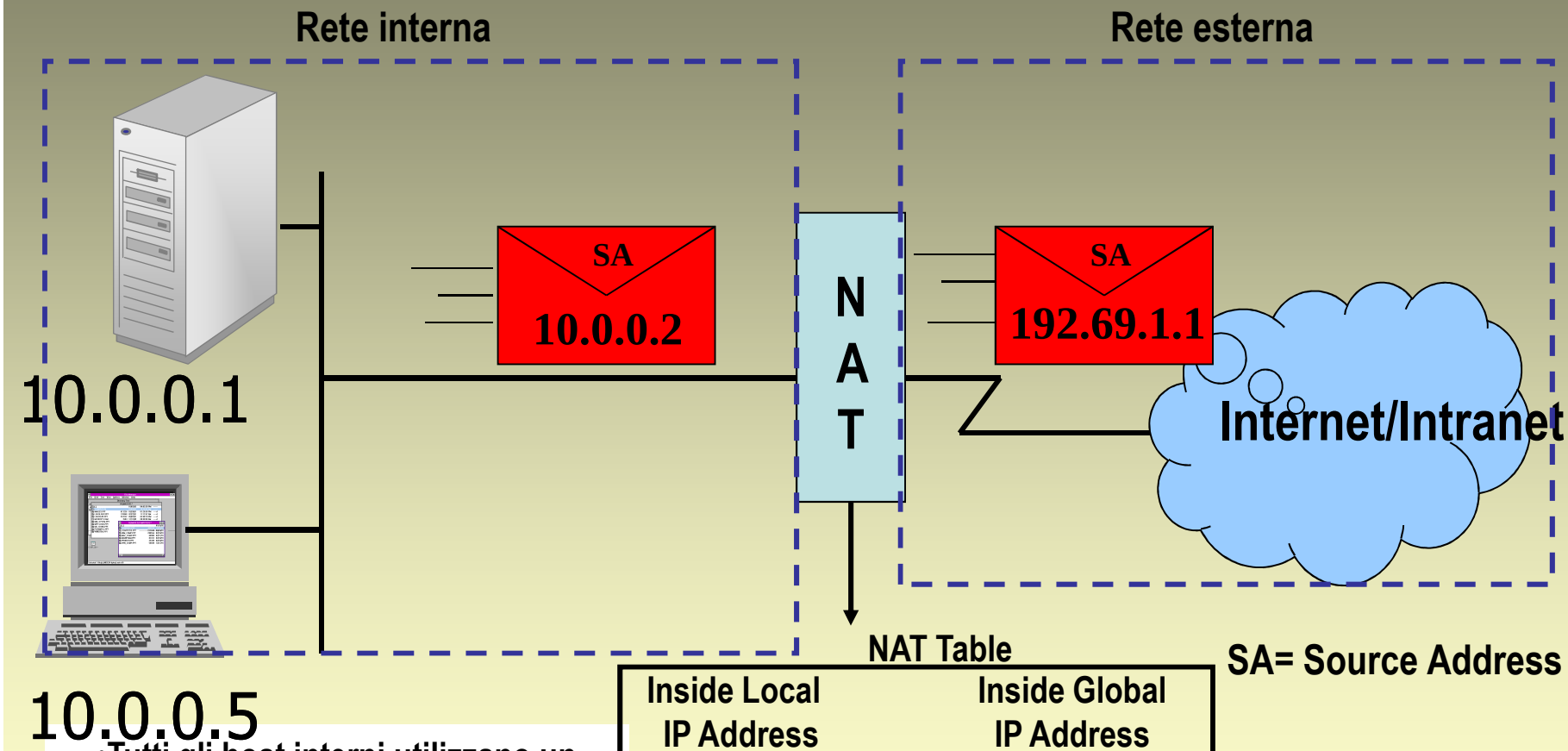
NAT Table

Outside Local IP Address	Outside Global IP Address
171.68.1.1	10.0.0.20
171.68.1.2	10.0.0.21

SA= Source Address

Consente di utilizzare indirizzi interni ed esterni che si sovrappongono

Port Address Translation (PAT)



NAT Table

Inside Local IP Address	Inside Global IP Address
10.0.0.2:1026	192.69.1.1:5001
10.0.0.3:1029	192.69.1.1:5002

SA= Source Address

- Tutti gli host interni utilizzano un singolo indirizzo IP registrato
- vengono utilizzate le porte TCP/UDP per individuare il reale mittente/destinatario del pacchetto

NAT: considerazioni / 1

- Il numero di sessioni concorrenti supportate dal NAT dipende dalla quantita' di memoria disponibile sull'apparato
- E' possibile utilizzare contemporaneamente sia traduzioni statiche che dinamiche facendo attenzione che gli indirizzi statici siano esclusi dal pool di indirizzi dinamici
- Solo una parte degli indirizzi della rete possono essere tradotti attraverso il NAT configurando una access-list che include l'insieme di host/reti che richiedono la traduzione
- Si possono mappare su un unico indirizzo pubblico attraverso il PAT al massimo fino a 65535 indirizzi

NAT: considerazioni / 2

- Oltre a modificare l'indirizzo IP nell'intestazione del pacchetto devono essere effettuate anche altre operazioni:
  - Ricalcolo della checksum IP
  - Ricalcolo della checksum TCP
  - Modifica del campo dati se questo contiene riferimenti all'indirizzo IP da tradurre

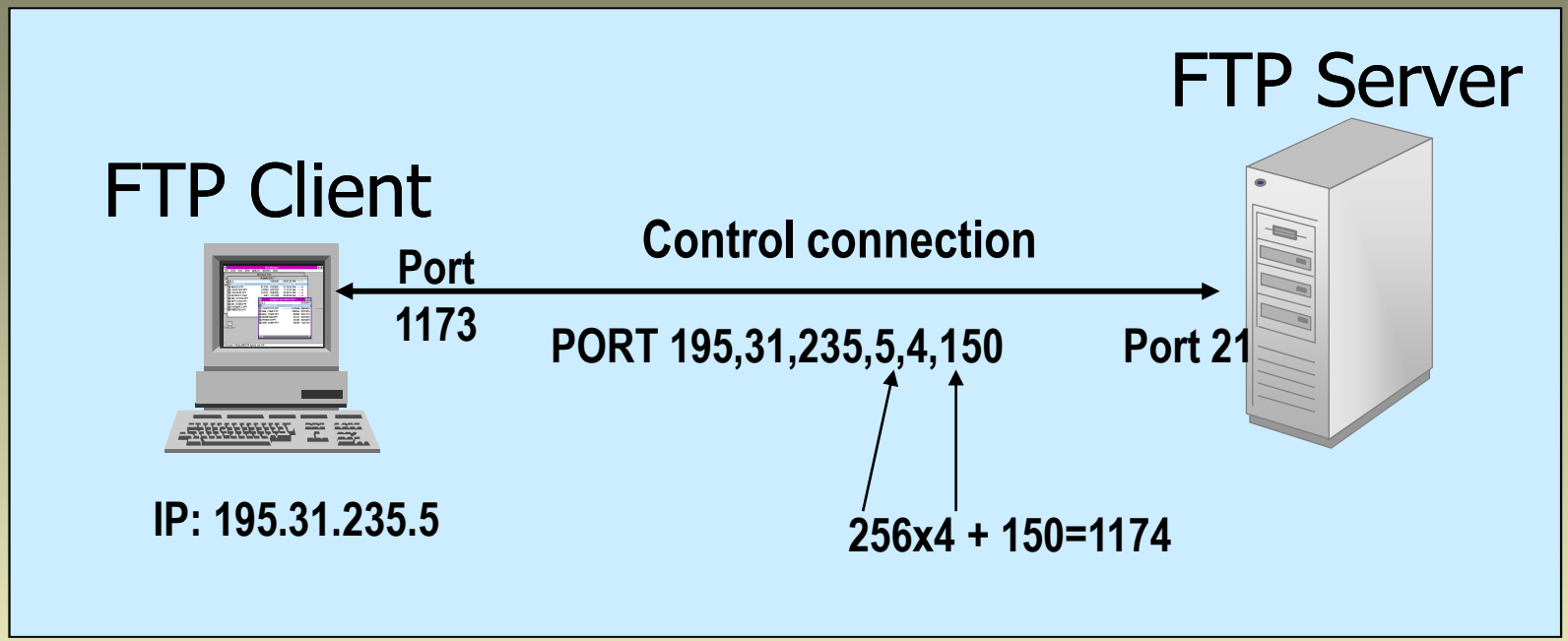
NAT: applicativi supportati

- **Gli applicativi supportati:**
  - **HTTP, TFTP, Telnet, NFS**
  - **ICMP, FTP, DNS**
- **Gli applicativi non supportati:**
  - **DHCP**
  - **SNMP**
  - **DNS zone transfers**
  - **IP multicast**
  - **Routing table updates**

FTP (File Transfer Protocol) – modalità attiva

- Il protocollo FTP si distingue dagli altri applicativi perchè utilizza due connessioni TCP per trasferire un file
  - una connessione di controllo
  - una connessione dati
- La ***connessione di controllo*** viene instaurata dal client utilizzando la porta di destinazione 21. Questa connessione rimane in piedi per tutto il tempo che il client comunica con il server ed e' utilizzata dal client per inviare i comandi e dal server per inviare le risposte
- La ***connessione dati*** viene creata ogni volta che un file e' trasferito tra il client ed il server. Questa connessione viene instaurata dal server utilizzando la porta sorgente 20 (FTP standard o PORT o modalità attiva)

FTP attivo: esempio (1)

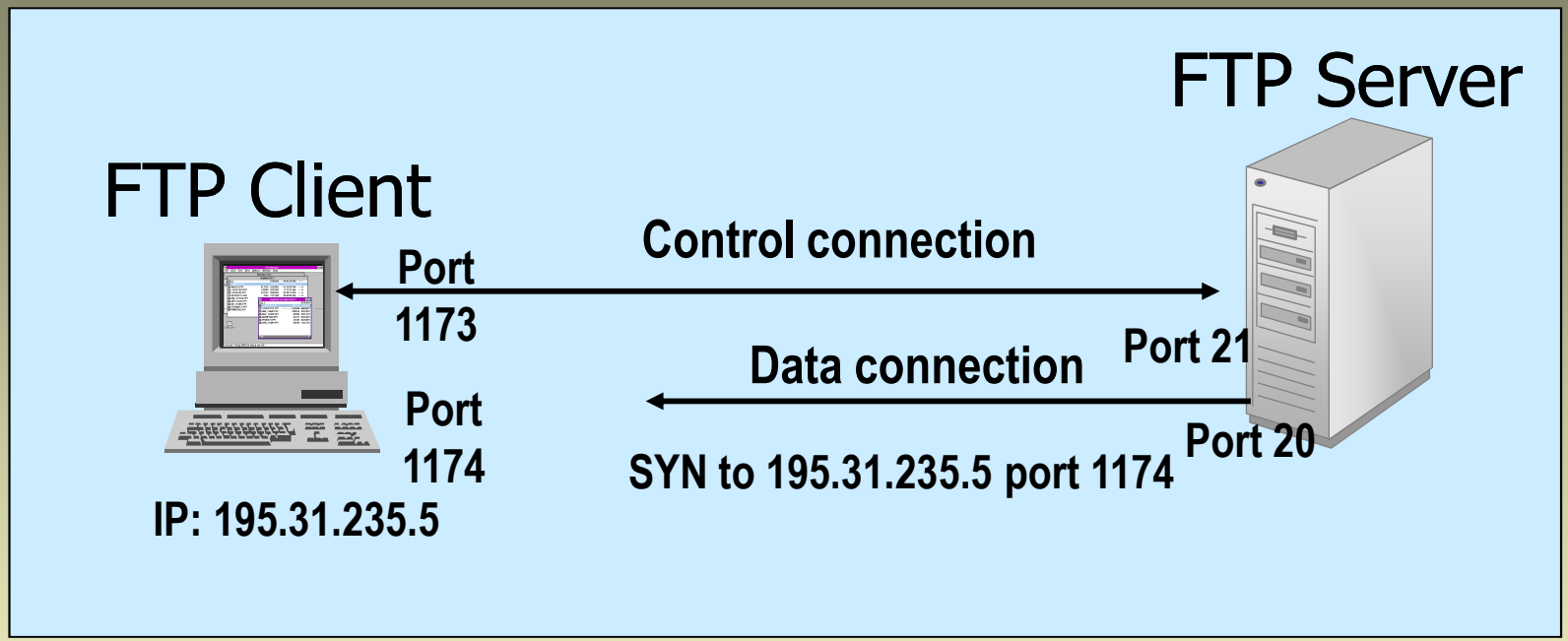


Il comando utilizzato dal client per creare una connessione dati e' PORT i cui argomenti sono sei numeri decimali in ASCII separati da virgole:

- i primi quattro numeri specificano l'indirizzo IP del client

- gli ultimi due numeri specificano la porta

FTP attivo: esempio (2)



Il server riceve il comando PORT ed apre una connessione TCP con il client utilizzando come porta sorgente la 20 e porta di destinazione quella specificata nel comando PORT

NAT e FTP

- Il comando PORT contiene un riferimento all'indirizzo IP, sebbene in formato ASCII, che deve essere tradotto
- Questa operazione può causare una modifica della lunghezza del pacchetto IP
- Se la nuova dimensione del pacchetto e' inferiore a quella originale, nel pacchetto vengono inseriti dei bit di riempimento per ricondurre la dimensione del pacchetto a quella originaria
- Se il pacchetto diventa più grande di quello originale, il numero di sequenza (TCP) deve essere modificato
- Una tabella speciale viene utilizzata per garantire la corretta traduzione dei numeri di ACK e SEQ

NAT e sicurezza

- Se i dati presenti nel pacchetto IP sono cifrati non e' possibile per il NAT effettuare le operazioni di traduzione all'interno del pacchetto
- In particolare, le checksum IP e TCP devono essere accessibili, e quindi le corrispondenti intestazioni non possono essere cifrate