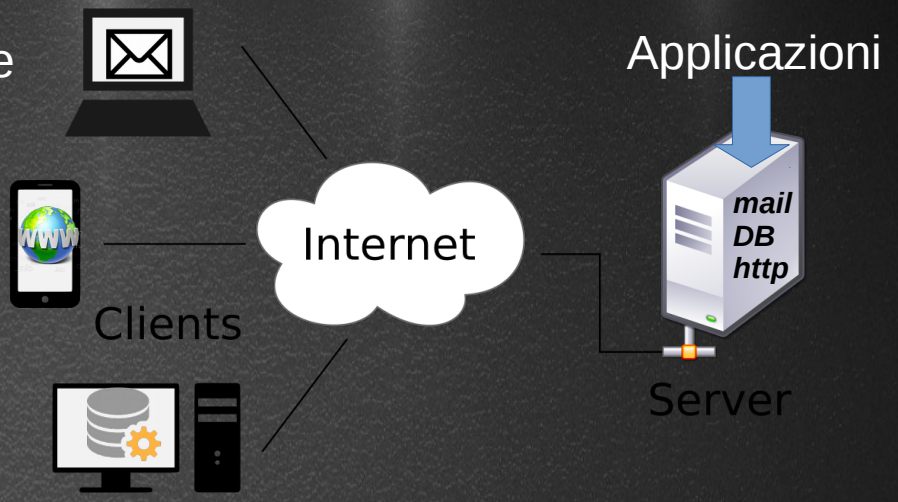
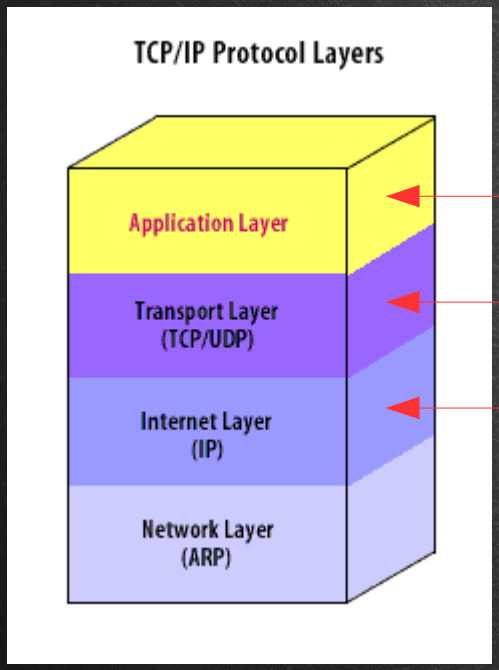
Inoltro pacchetti su rete

In una rete UN indirizzo IPv4 identifica UN host ma se sul quell'host girano più software server, come capiamo dall'indirizzo quale servizio il client richiede?





ID processo

TSAP → indica una applicazione in esecuzione su quel computer → NSAP + info supplementare → *numero di **PORTA***

Indirizzo IP (NSAP)

Esempio
62.149.140.202:80

Connetti all'host 62.149.140.202

Una volta connesso cerca il servizio in ascolto alla porta 80 → **Usa il server apache (PID 4271)**

Nota:
La porta non è un indirizzo fisico (esiste solo 1 porta fisica: NIC) ma un'astrazione logica, ovvero un parametro numerico usato dai sistemi di rete. Questo utilizza 16 bit, quindi va da 0 a 65535

Inoltro pacchetti su rete

Le prime 1024 porte, quindi da 0 a 1023 sono assegnate da IANA per importati servizi standard e sono note come “well know ports”, anche se non tutte sono assegnate e la porta 0 è riservata per a traffico di sicurezza/controllo

Servizio	Porta	Servizio	Porta
Ping	7	DNS	53
ftp	21	Web	80
Ssh	22	Pop3	110
telnet	23	Imap	143
smtp	25	UUCP	540

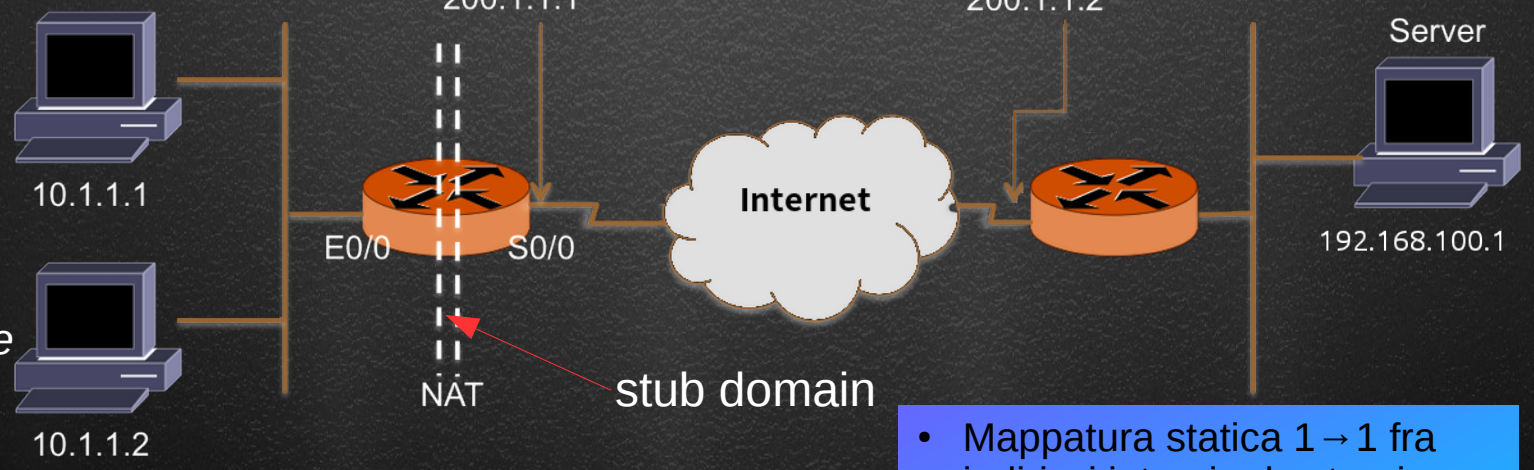
Le applicazioni possono usare LIBERAMENTE le porta da 1024 in su

TCP e UDP usano (normalmente) LA STESSA porta

Network Address Translation

D-NAT

Modifica l’indirizzo interno per la visualizzazione esterna della sorgente di connessione



S-NAT

Modifica l’indirizzo esterno per la redirezione verso particolari indirizzi (es.port-forwarding)

Local	Global
10.1.1.1:3212 10.1.1.1:3213 10.1.1.2:38913	200.1.1.1:3212 200.1.1.1:3213 200.1.1.1:38913

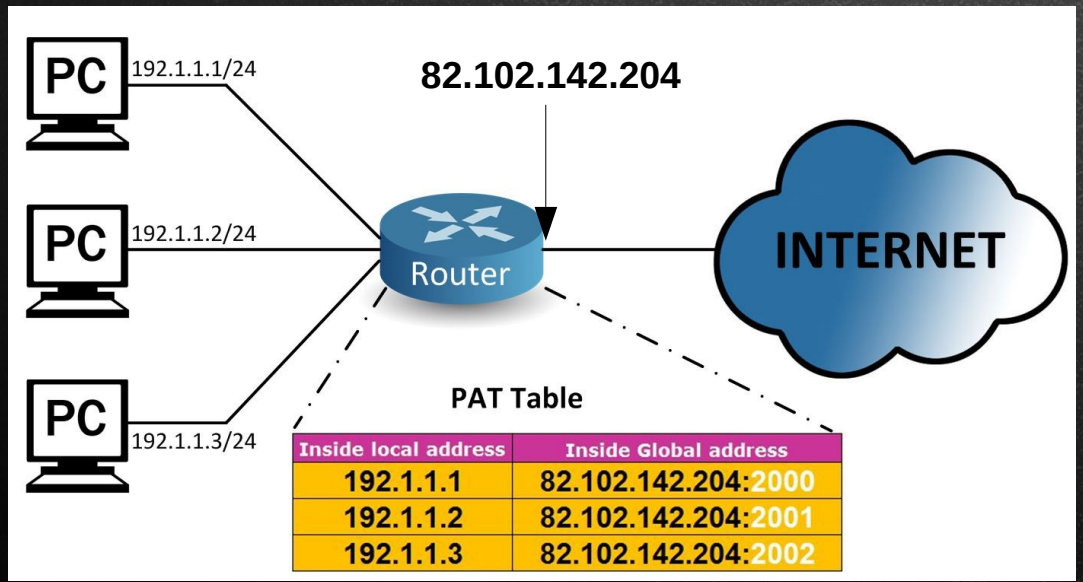
- Mappatura statica 1→1 fra indirizzi interni ed esterni
- Mappatura dinamica *(ip masquerading)* prevede più indirizzi locali con un solo indirizzo pubblico *(in figura)*

Inoltro pacchetti su rete

- Il NAT NON è un sistema di sicurezza (molto meglio firewall o proxy) ma solo un sistema di reindirizzamento, al contrario l'uso di NAT statico per esporre servizi all'esterno diminuisce i livelli di sicurezza di una rete. Lievemente più sicuro è il NAT dinamico perché la mappatura fra interno ed esterno viene creata solo al momento della richiesta di connessione
- L'uso del NAT favorisce l'abbattimento di costi per l'uso di indirizzi pubblici multipli
- Tale pratica è risultata molto utile per la problematica dell'esaurimento degli indirizzi IP ed alleggerisce le tabelle di routing
- L'uso del NAT non richiede riconfigurazioni di router o host

Port Address Translation

Oltre alla modifica dell'indirizzo IP nella trasmissione bidirezionale fra client e server, è possibile cambiare anche il numero di porta fra l'interno e l'esterno di una rete.

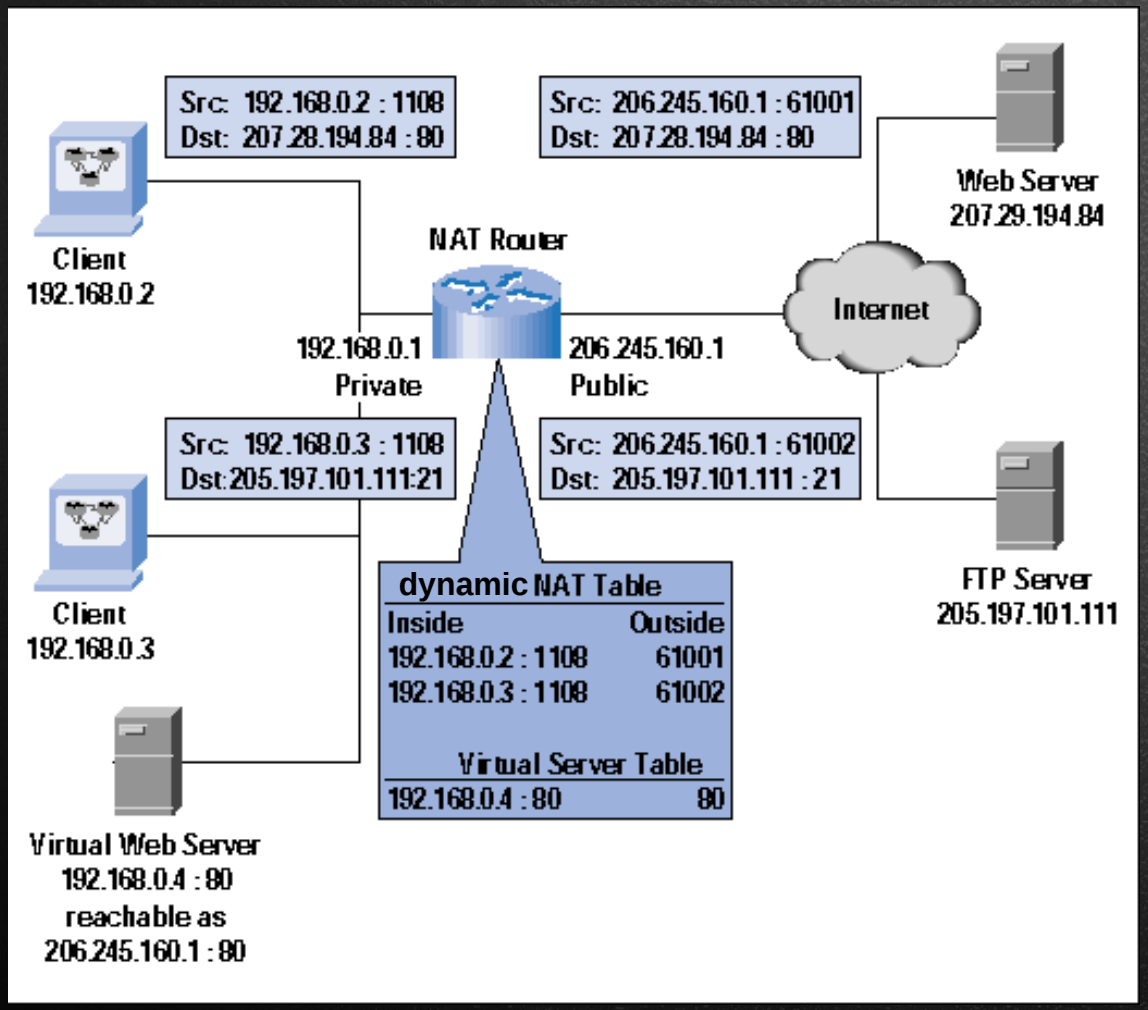


PAT statico

In questa maniera posso utilizzare l'unico indirizzo pubblico del router per smistare pacchetti ai diversi host interni alla rete, che ad esempio, possono fornire diversi servizi

Inoltro pacchetti su rete

L'IP masquerading prevede la possibilità di cambiare non solo l'indirizzo IP tramite NAT ma anche il numero di porta tramite PAT, in tal caso le porte usate dall'interno verso l'esterno saranno sempre superiori alla 1023 (rfc 2663).
Tale tecnica prende anche il nome di IP overloading o NAPT *(Network and Port Translation)*



La dynamic NAT table si riempe e si svuota continuamente con le richieste dei client interni verso l'esterno.
Quando la richiesta viene soddisfatta la entry viene cancellata e fa posto ad un'altra eventuale richiesta.

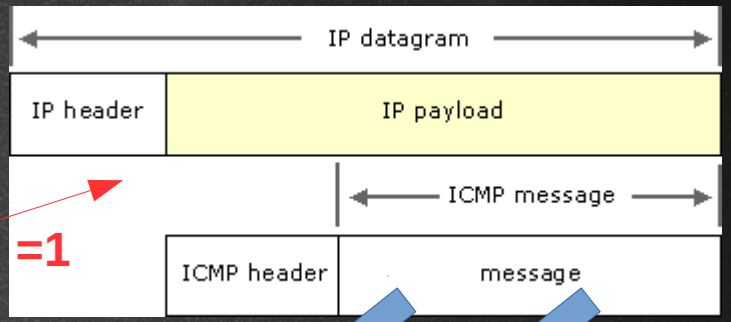
La virtual server table, invece, è STATICA ma è anch'essa da considerarsi parte del servizio PAT-NAT

Nota:
Ogni volta che un pacchetto attraversa un router viene incrementato un contatore (hop, *vedi TTL*), il next hop è l'indirizzo del prossimo router da attraversare

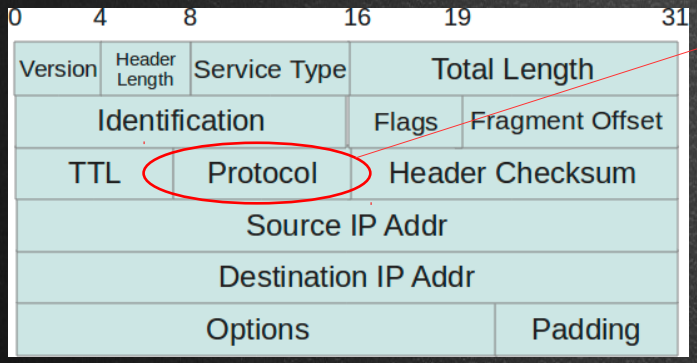
Inoltro pacchetti su rete

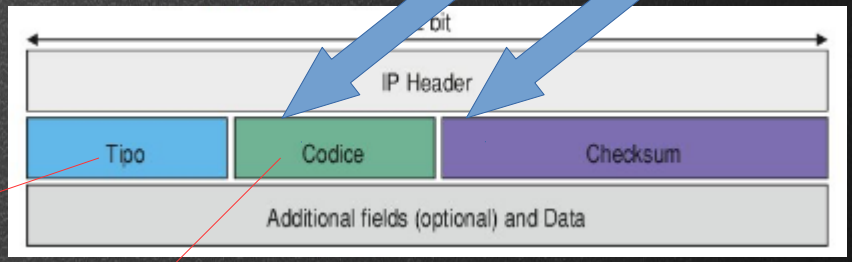
Internet Control Message Protocol

Il livello internet NON garantisce la consegna messaggi poiché connection-less, per capire se ci sono stati problemi nella consegna ci si affida all'ICMP (rfc792), che è incapsulato direttamente a livello internet nel payload del datagram.
ICMP segnala gli errori non provvede a correggere!



Header IP





Tipo	Descrizione	Tipo	Descrizione
0	Echo Reply	13	Timestamp Request
3	Destination Unreachable	14	Timestamp Reply
4	Source Quench	15	Information Request
5	Redirect (change a route)	16	Information Reply
8	Echo Request	17	Address Mask Request
11	Time Exceeded for a Datagram	18	Address Mask Reply
12	Parameter Problem for a Datagram		

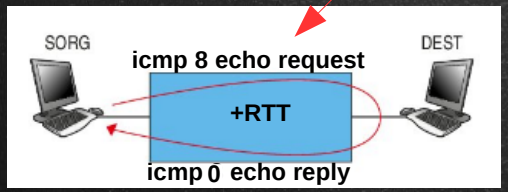
Tipo	Codice	Descrizione	RFC
3		DESTINATION UNREACHABLE	792
	0	Net Unreachable	792
	1	Host Unreachable	792
	2	Protocol Unreachable	792
	3	Port Unreachable	792
	4	Fragmentation Needed and Don't Fragment was Set	792
	5	Source Route Failed	1812
	6	Destination Network Unknown	1812
	7	Destination Host Unknown	1812
	8	Source Host Isolated	1812
	9	Communication with Destination Network is Administratively	1812
	10	Communication with Destination Host is Administratively	1812
	11	Destination Network Unreachable for Type of Service	1812
	12	Destination Host Unreachable for Type of Service	1812
	13	Communication Administratively Prohibited	1812

Inoltro pacchetti su rete

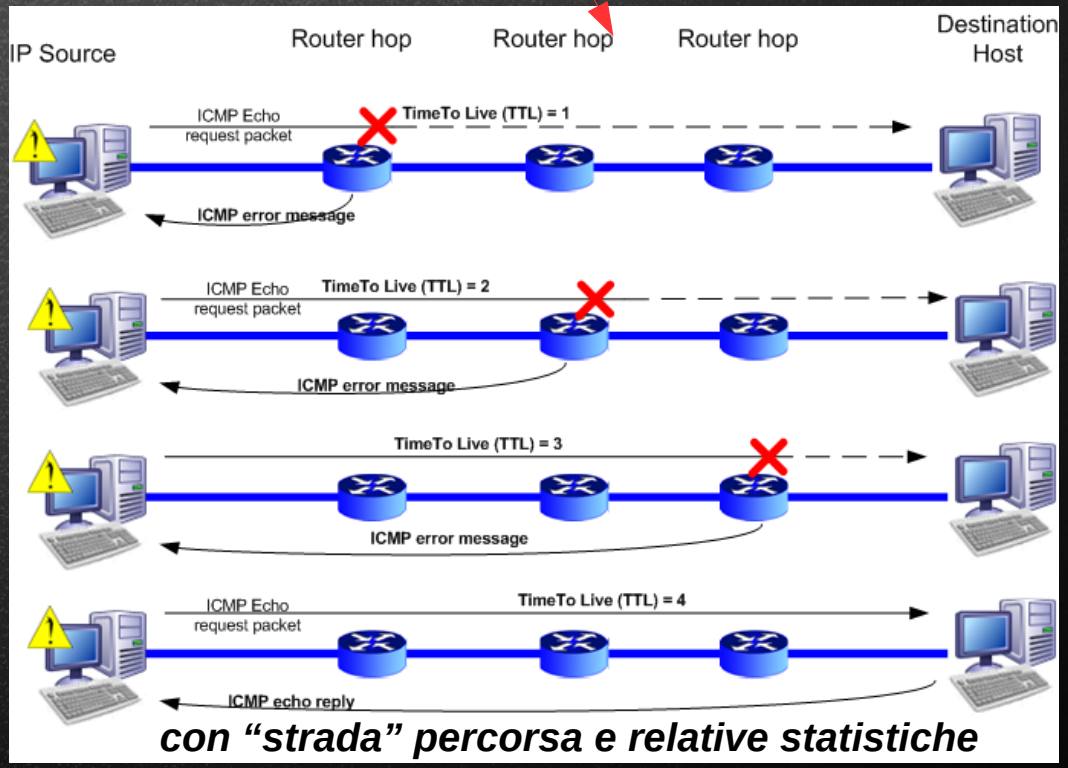
0-8	**Richiesta di eco e relativa risposta** (Echo Request/Reply): serve a determinare lo stato di una rete; viene inviato a qualsiasi indirizzo IP che deve restituire una risposta al trasmittente.
3	**Destinazione irraggiungibile** (Destination Unreachable): viene utilizzato da un router quando incontra problemi nel raggiungere la rete di destinazione specificata nell'indirizzo di destinazione IP.
4	**Rallentamento della sorgente** (Source Quence): viene utilizzato da un router se non possiede memoria sufficiente per accodare i datagrammi in arrivo.
5	**Reindirizzamento** (Redirect): viene inviato da un router all'host che ha spedito il datagramma indicandogli di scegliere un percorso migliore, cioè un altro router al quale indirizzare il messaggio: ricevendo il messaggio l'host può aggiornare la propria tabella di routing aggiungendo la riga che il router indica come parametro del messaggio (router alternativo).
11	**Superamento del tempo massimo di durata del datagramma** (Time Exceeded for a Datagram): viene inviato da un router quando scarta un datagramma giunto alla scadenza del tempo massimo di durata.
12	**Parametro inintelligibile** (Parameter Problem for a Datagram): questo è il messaggio di errore che viene inviato dall'host o dal router che incontra problemi nell'elaborare parte di un'intestazione IP.
13-14	**Registrazione del tempo e relativa risposta** (Timestamp Request/Reply): vengono utilizzate dai router e dagli host per determinare il ritardo con cui sono stati consegnati i dati.
15-16	**Richiesta di informazioni e relativa risposta** (Information Request/Reply): consentono a un host di identificare la rete alla quale è collegato.
17-18	**Richiesta di maschera di indirizzi e relativa risposta** (Address-Mask Request/Reply): vengono utilizzati da un host per ottenere la maschera di sottorete a cui appartiene.

I tipi di messaggio ICMP vengono sfruttati da alcune funzionalità del protocollo TCP/IP come ping o traceroute

*Sotto windows traceroute si chiama **tracert** per compatibilità storica con MS-DOS (7 caratteri)*



No ping se c'è ip masquerading



con "strada" percorsa e relative statistiche