Network Address Translation
NAT & …

NAT, PAT, NAPT, IP masquerading
et cetera

un'introduzione

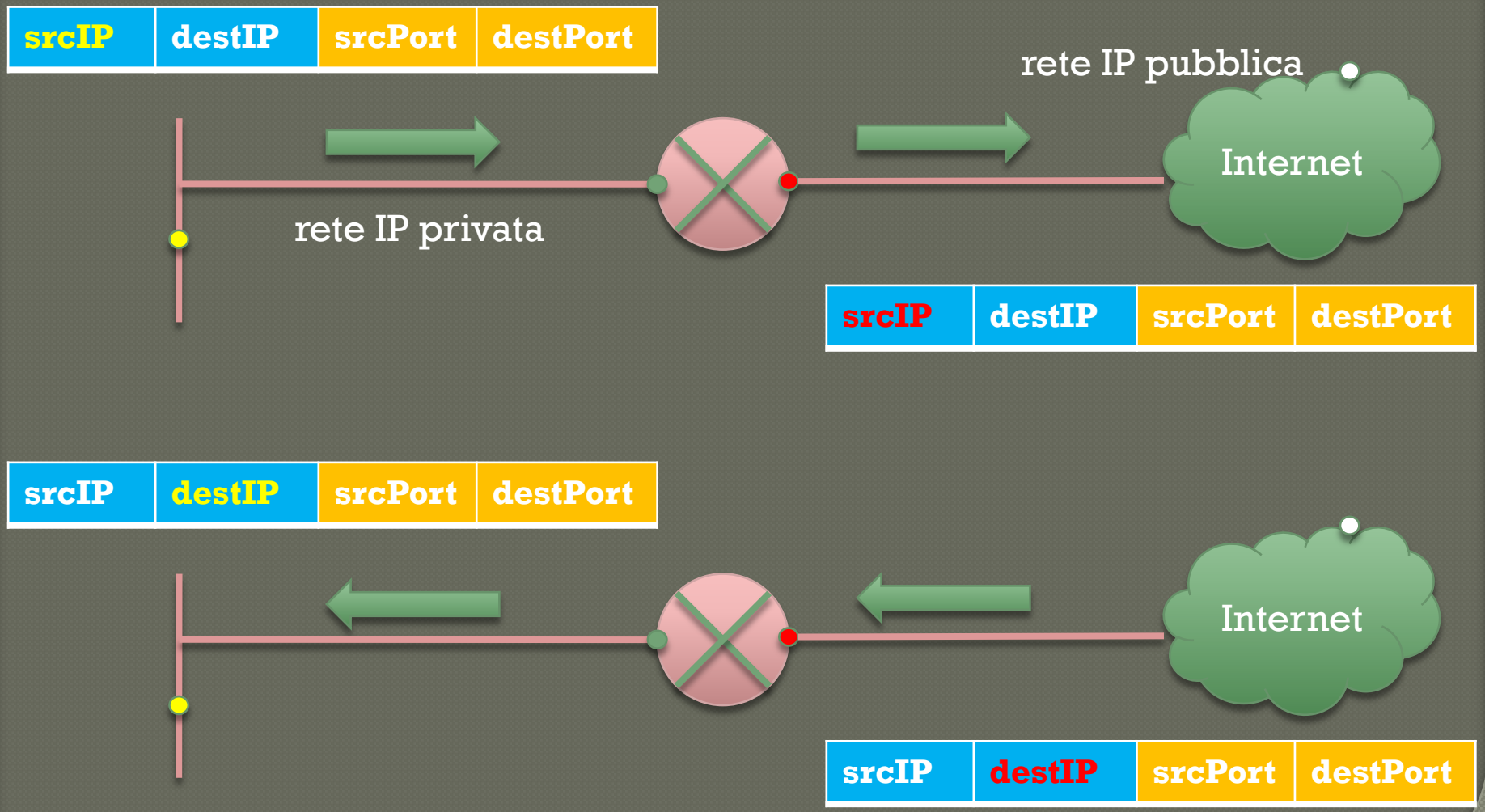
Introduction to NAT

- **Network Address Translation**
  - Non proprio vecchia; in uso in maniera intensiva dalla fine degli anni 90
  - Nata come tecnica per **mappare** indirizzi privati IPv4 in indirizzi pubblici IPv4, e viceversa
  - Limita il problema della penuria (shortage) di indirizzi IPv4; problema che NON si presenta con IPv6
  - Utilizza primariamente gli indirizzi IP per fare il lavoro, e secondariamente le porte TCP/UDP
  - Il tipo più comune è NAPT (Network Address Port Translation)
  - Per lavorare usa la **tabella NAT**
- Why NAT? (video)

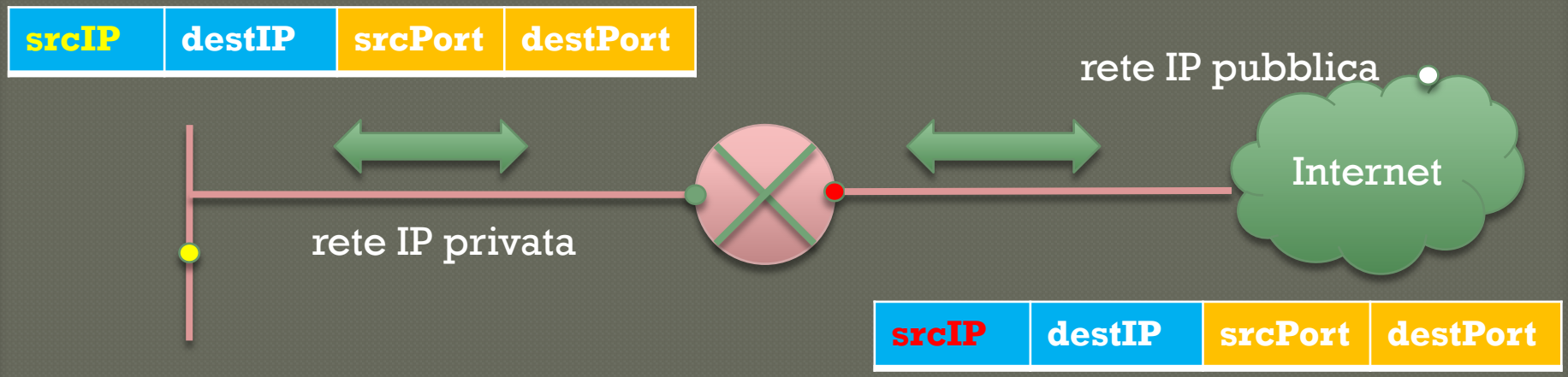
IP Private Networks

- Sono reti basate sul protocollo IP non direttamente connesse a Internet; p.e.: reti casalinghe, Small Office, ma anche reti di ISP!
- Gli indirizzi in tali reti sono liberamente assegnabili ma, se vuoi andare su Internet, devi evitare gli indirizzi **pubblici** e limitarti a configurare indirizzi **privati**,
- in questi range:
  - 10.0.0.0/8 → 10.255.255.255
  - 172.16.0.0 /12 → 172.31.255.255
  - 192.168.0.0/16 → 192.168.255.255
- Gli indirizzi IP privati non sono instradabili su Internet → vengono "droppati"

NAT schema di riferimento



NAT schema di riferimento



I pacchetti disegnati qui sopra si riferiscono al solo percorso di andata

tabella NAT

prot	inside local	inside global	outside local	outside global
	●	●		

La riga nella tabella qui sopra viene configurata nel router, a mano; è **statica** *e permanente.*
Per consultare la tabella NAT in IOS si usa il comando:
router(config)#**show ip nat translations**
→ Studieremo più avanti la struttura della tabella

NAT schema di riferimento

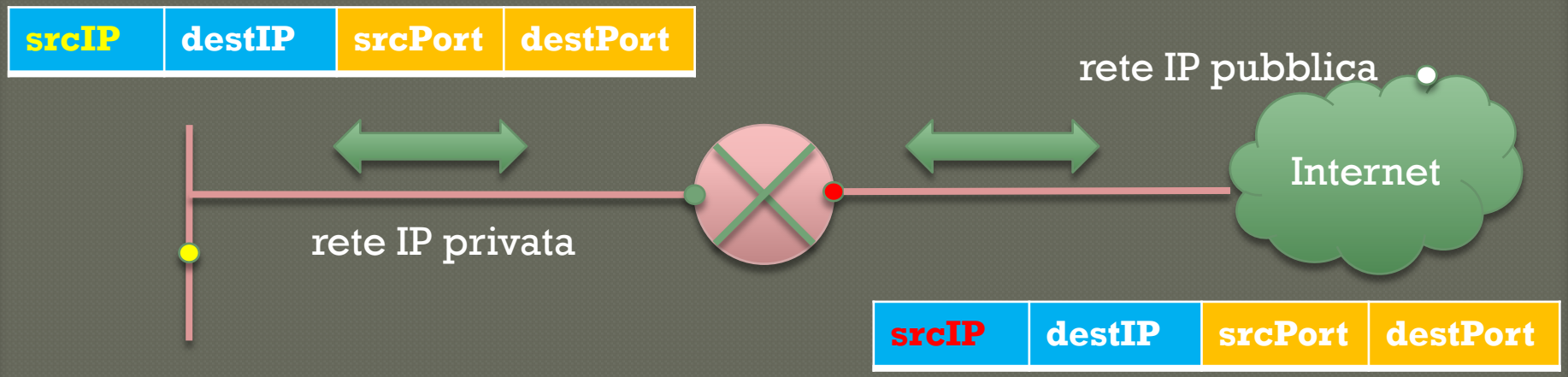


tabella NAT

prot	inside local	inside global	outside local	outside global

Per configurare la riga qui sopra nella tabella NAT ,in IOS si usa il comando:
router(config)#**ip nat inside source static**
per esempio:
router(config)#**ip nat inside source static 10.0.1.2 128.195.4.119**
La parola static ha il significato di configurazione scritta a mano dall'admin

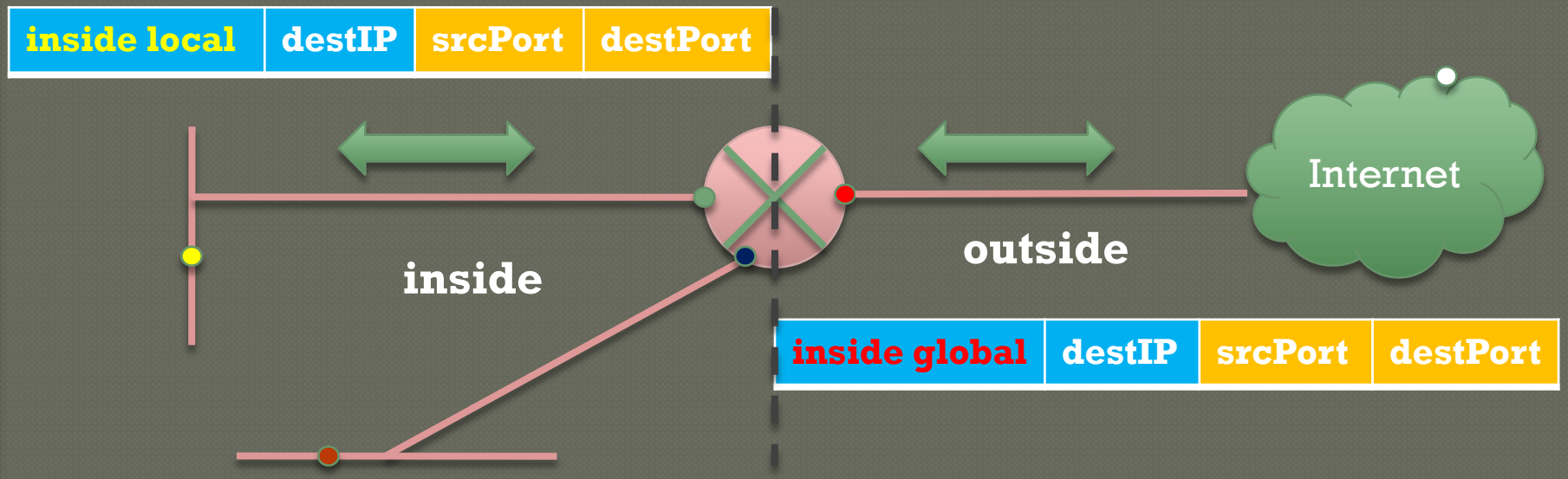
NAT: considerazioni sullo schema

Lo scenario visto nella slide precedenti suggerisce alcune puntualizzazioni:

- A cosa può servire configurare un NAT statico 1-a-1 ?
  - forse una piccola scuola elementare con una rete interna e un solo host che possa uscire su Internet; scenario poco diffuso
  - la **pubblicazione** di un server inside, che diventa accessibile da Internet; scenario molto diffuso
- Il router non pensa tanto a "IP privati" o "IP pubblici"; ragiona piuttosto con uno schema inside/outside
  - per esempio si usa NAT tra IP privati "casalinghi" e IP privati dell'ISP (basta operare un tracert sulla propria macchina windows di casa e vedere gli hop effettuati) *
  - quindi è fondamentale definire quali i/f appartengono alla parte inside e quali alla parte outside

* *È necessario utilizzare NAT nel caso descritto?*

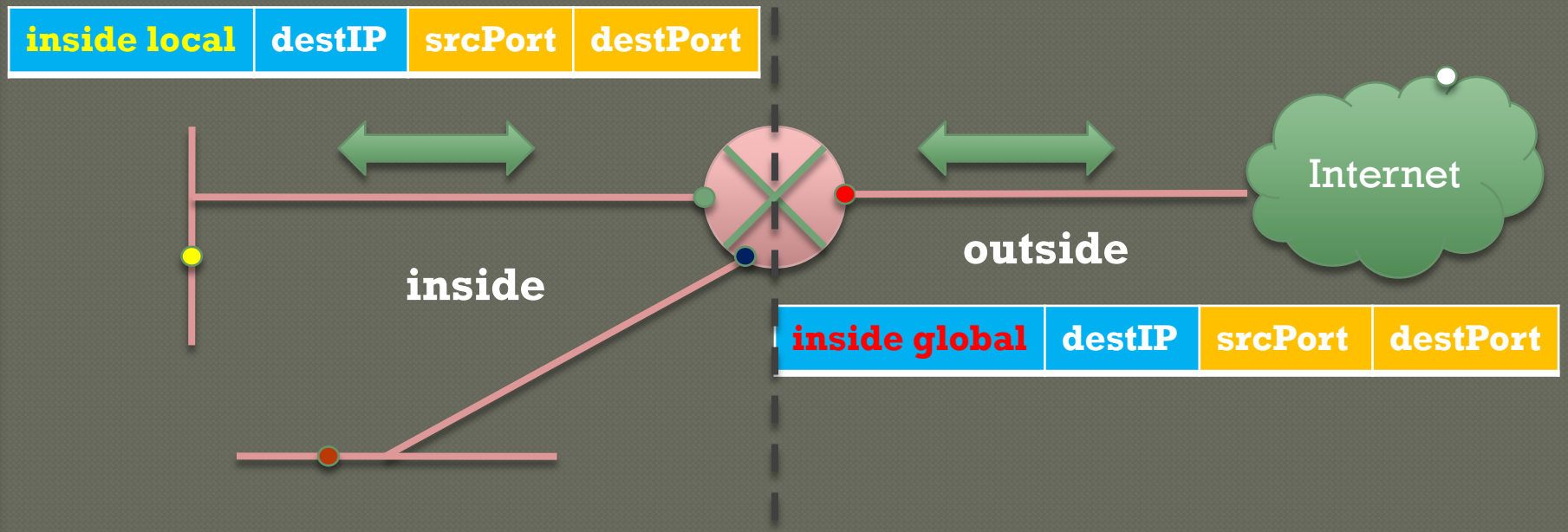
NAT: config i/f as inside/outside



Configurare le i/f del router per il NAT richiede la definizione del "lato", inside vs outside:

router(config)#**interface**
router(config-if)#**ip nat inside**
router(config)#**interface**
router(config-if)#**ip nat inside**
router(config)#**interface**
router(config-if)#**ip nat outside**

NAT: inside vs outside local vs global



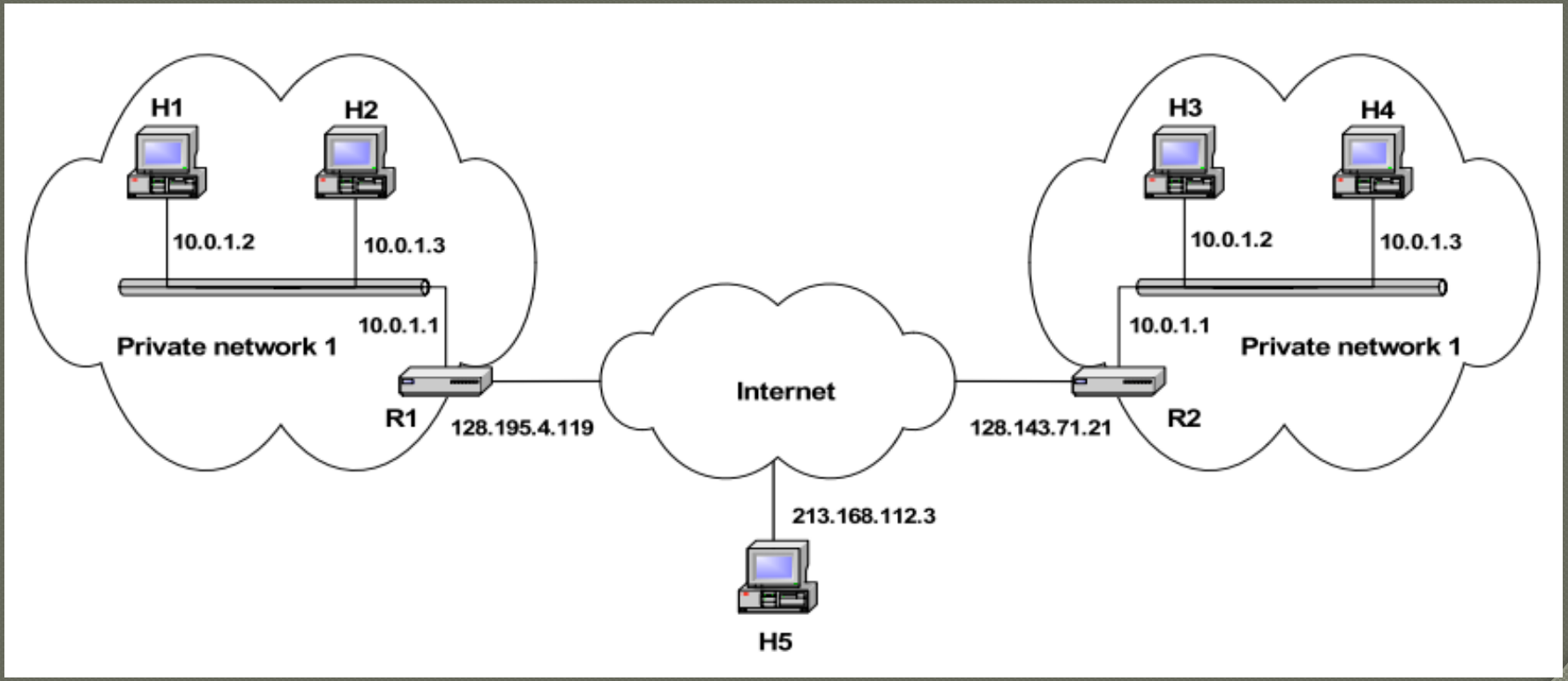
inside vs outside: la posizione fisica dell'host
local vs global: il punto di vista (l'indirizzo, come appare)
➔ inside global = ● l'indirizzo dell'host interno per come appare all'esterno

tabella NAT

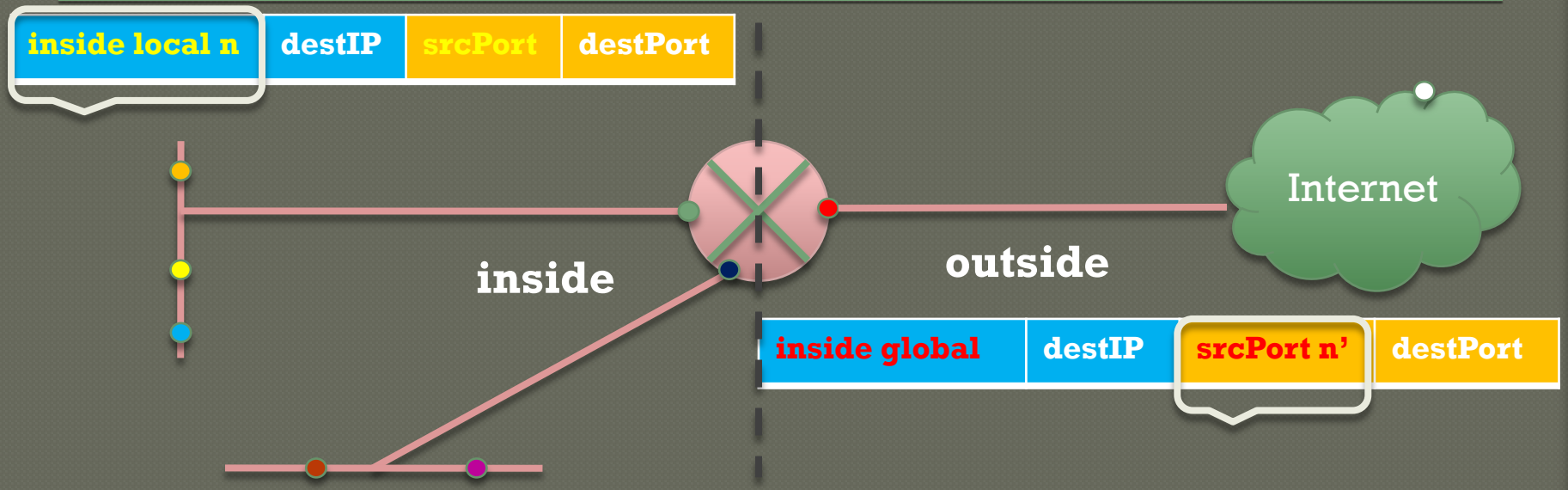
prot	inside local	inside global	outside local	outside global
	●	●		

NAT: Scenario principale

Scenario molto diffuso è quello di una rete privata in cui gli host devono avere la possibilità di accedere a Internet, come nell'esempio in figura.
La configurazione statica 1-a-1 vista precedentemente non funziona perché richiede un indirizzo IP pubblico per ogni host interno; 20 host interni→20 indirizzi pubblici…. E dove sarebbe il risparmio di indirizzi pubblici per cui NAT è stato ideato?

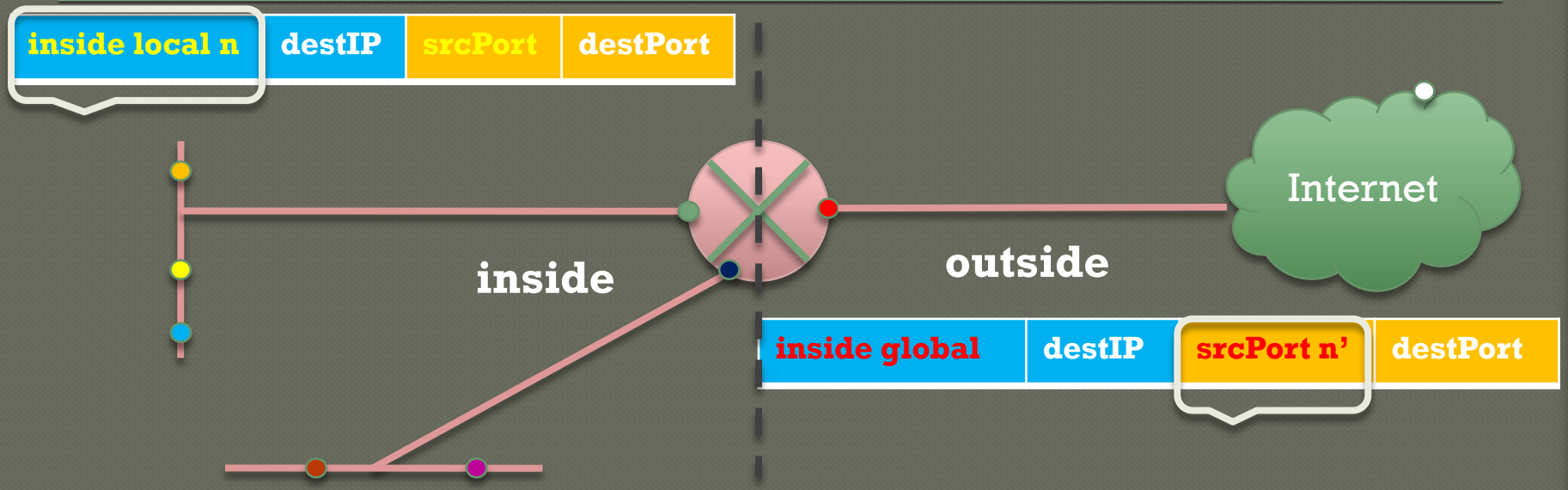


NAT: Scenario principale



- Tutti gli inside local si presentano esternamente come l'unico inside global e vengono differenziati, per il traffico di ritorno, attraverso la srcPort di uscita
- Si vede il gioco combinato di IP e porte; si parla di NAPT (o PAT o IP masquerade)
- IP e porta destination NON vengono alterate
- Per evitare conflitti la srcPort di uscita è cambiata sistematicamente da NAT
- *Come sarà il gioco al ritorno?*
- *Come indirizzerà il router il pacchetto alla corretta subnet?*

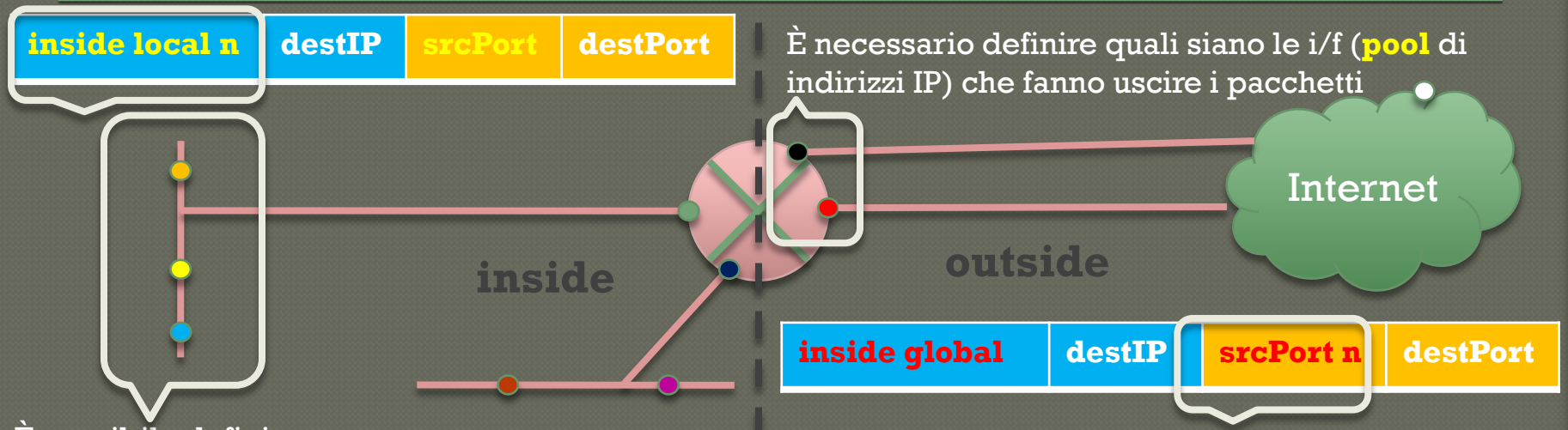
NAT: Scenario principale



La tabella NAT è inizialmente vuota; si riempie col traffico; il comando show ip nat translations fornisce per il primo pacchetto in uscita da ● :

prot	inside local	inside global	outside local	outside global
tcp	10.0.1.2:55000	128.195.4.119:22000	●:80	●:80

NAT: Scenario principale



È possibile definire quali siano gli host che possono accedere outside mediante una **ACL**

Il comando per configurare un **pool** di nome myPool è:
R(config)#ip nat pool myPool 128.195.4.119 128.195.4.120 255.255.255.0
I due indirizzi IP sono "da… a…"

Il comando per il NAPT dynamic è:
R(config)#ip nat inside source list 8 pool myPool

ACL = Access Control List
Il comando seguente configura la ACL con numero 8
R(config)#access-list 8 permit 10.0.0.0 0.0.0.255
definendo un gruppo di indirizzi con la wildcard (opposta alla SM), ai quali è consentito…

NAT vs PAT & Static vs Dynamic

- Video (video)
- Sintesi:

	static *impostato a mano, persistente*	**dynamic** *generato al momento del traffico*
NAT **L3**		
PAT **L3+L4**		

Cisco non usa i termini PAT o NAPT ma quasi sempre solo NAT intendendo tutte le possibili traduzioni; questa annotazione rimarca la sostanza del NAT, che è un meccanismo di sostituzione di indirizzi e porte negli header dei pacchetti nel passaggio attraverso il dispositivo che implementa il ANT

NAT vs PAT, Static vs Dynamic

Sintesi

	static *impostato a mano, persistente*	**dynamic** *generato al momento del traffico*
NAT **L3**	1 IP inside local ↔ 1 IP inside global	*senza overload:* N IP inside local ↔ N IP inside global**
PAT (NPAT) **L3+L4**	1 inside local IP+port° ↔ 1 inside global IP+port*	*con overload:* N IP inside local ↔ 1 IP+port inside global

° il PAT ''da solo'' non esiste ma puoi fare la traduzione, stabilito un IP, della porta (local ↔ global)

* con più config come questo si realizza il port forwarding

** ci devono essere N indirizzi inside nella ACL e stesso numero di indirizzi outside nel pool, altrimenti…

NAT vs PAT, Static vs Dynamic

Sintesi con comandi IOS, con scenari

	static *impostato a mano, persistente*	**dynamic** *generato al momento del traffico*
NAT **L3**	1 IP insi… global ip nat inside source static 10.0.1.2 128.195.4.119	*~~senza overload:~~* ~~N IP inside local ↔ N IP inside global~~ ~~ip nat inside source list 8 pool myPool~~
PAT (NPAT) **L3+L4**	…global IP + port ip nat inside source static tcp 10.0.1.2 8080 128.195.4.119 80	*con overload:* N IP inside … global ip nat inside source list 8 pool myPool overload *oppure* ip nat inside source list 8 interface typenum overload

pubblicare un server interno

pubblicare un server interno specificando la porta

Far uscire gli host interni su ISP o Internet

port forwarding

Altri scenari

Capito l'utilizzo tipico e più diffuso del NAT, esistono situazioni in cui si può operare una traduzione e che vengono bene per altri scopi

- Due subnet S1 e S2 connesse da un router; in S1 vengono ridefiniti gli indirizzi durante un weekend; in S2 non abbiamo ancora aggiornato i path verso S1; potremo implementare un NAT sul router che le collega
- NATtare IPv4 ↔ IPv6
- …

Problemi con NAT

NAT is cool but… presenta problemi; p.e.:

- creare connessioni diventa complicato
- Breaks end-to-end connectivity (grosso problema risolto con IPv6)
- Riscrive gli headers dei pacchetti
- … quindi ricalcola le checksum (costo computazionale, in termini di tempo)
- il tunneling diventa complicato

NAT & Cisco IOS…

provare i comandi:

- show ip nat statistics
- show ip nat translations verbose
- clear ip nat translations *
- clear ip nat statistics *
- debug ip nat

Types of NAT

- Full-cone NAT
  - Accepts data through any previously used port
- Address-restricted-cone NAT
  - Only accepts data through previously used ports if the source IP matches a system we've already sent to
- Port-restricted-cone NAT
  - Like the above, but uses source ports too
- Symmetric NAT
  - Mappings are unique to external hosts: a different public port is used for each external host

NAPT Operation

- Ogni dispositivo NAT (router, …) ha una NAT table
- Quando un pacchetto esce e subisce traslazione, si crea una nuova riga nella tabella, con un numero di porta arbitrario → l'header TCP/IP viene riscritto
- Per un pacchetto in arrrivo, il dispositivo NAT consulta la tabella, aggiorna gli header, instrada il pacchetto

Running Services behind a NAT

- You're behind a NAT, and you need an external host's packets to get to you
- Example: running a web host behind a NAT
- You can't necessarily send an outbound packet first to write the NAT table
- Major issue for games and P2P
- Solutions?
  - Port forwarding (manually adding tables to the address translation table)

NAT Punchthrough

- Two hosts behind NATs need a way to exchange data directly
- They know each other's IPs, but not each other's communication ports
- They both connect to a known server that exchanges the data for them
- They can now communicate
- Often used for multiplayer games

UPnP and IGD

- UPnP: Universal Plug and Play
  - Set of protocols for networked devices to perform discovery automatically
- IGD: Internet Gateway Device protocol
  - NAT protocol that can perform automatic port mapping
  - Allows a host inside a network to tell the router which public port it wants to use for communication
  - Also gives mechanisms for finding public IP address and checking existing port mappings
  - Games can rely on this protocol to configure NAT tables such that users can be mapped with known ports and communication can take place

STUN

- Old Name: Simple Traversal of UDP through NAT
- New Name: Session Traversal Utilities for NAT
- Protocol for NAT traversal
- Attempt to standardize NAT traversal by establishing NAT categories and methods for checking for/communicating with each

TURN

- Traversal Using Relays Around NAT
- Similar to earlier punchthrough algorithm
- A server sits between two hosts behind NATs
- The server relays data between the two hosts

ICE

- Interactive Connectivity Establishment
- Protocol that utilizes STUN and TURN to perform NAT punchthrough
- Used often in VoIP