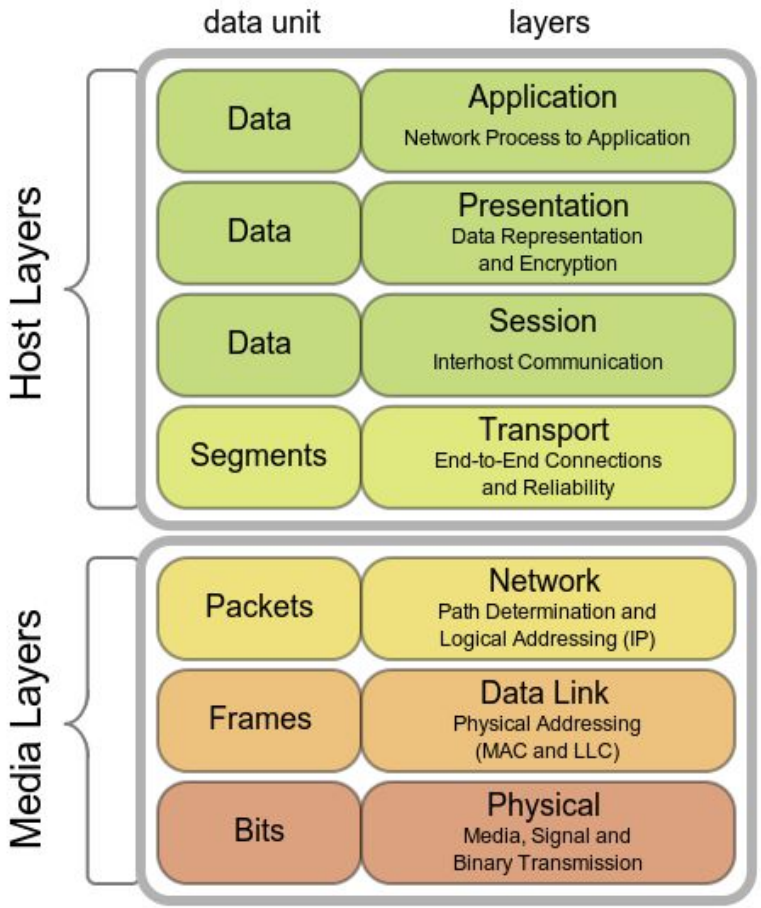
TCP / UDP

Primera introducció a la capa de transport. Capa 4 OSI.

Referències:

http://www.highteck.net/EN/Transport/OSI_Transport_Layer.html
https://www.practicalnetworking.net/series/
https://microchipdeveloper.com/networking:start
https://www.homenethowto.com/



- 7. **Aplicació**
- 6. **Presentació**
- 5. **Sessió**
- **4. Transport**
- 3. **Xarxa**
- 2. **Enllaç de dades**
- 1. **Físic**

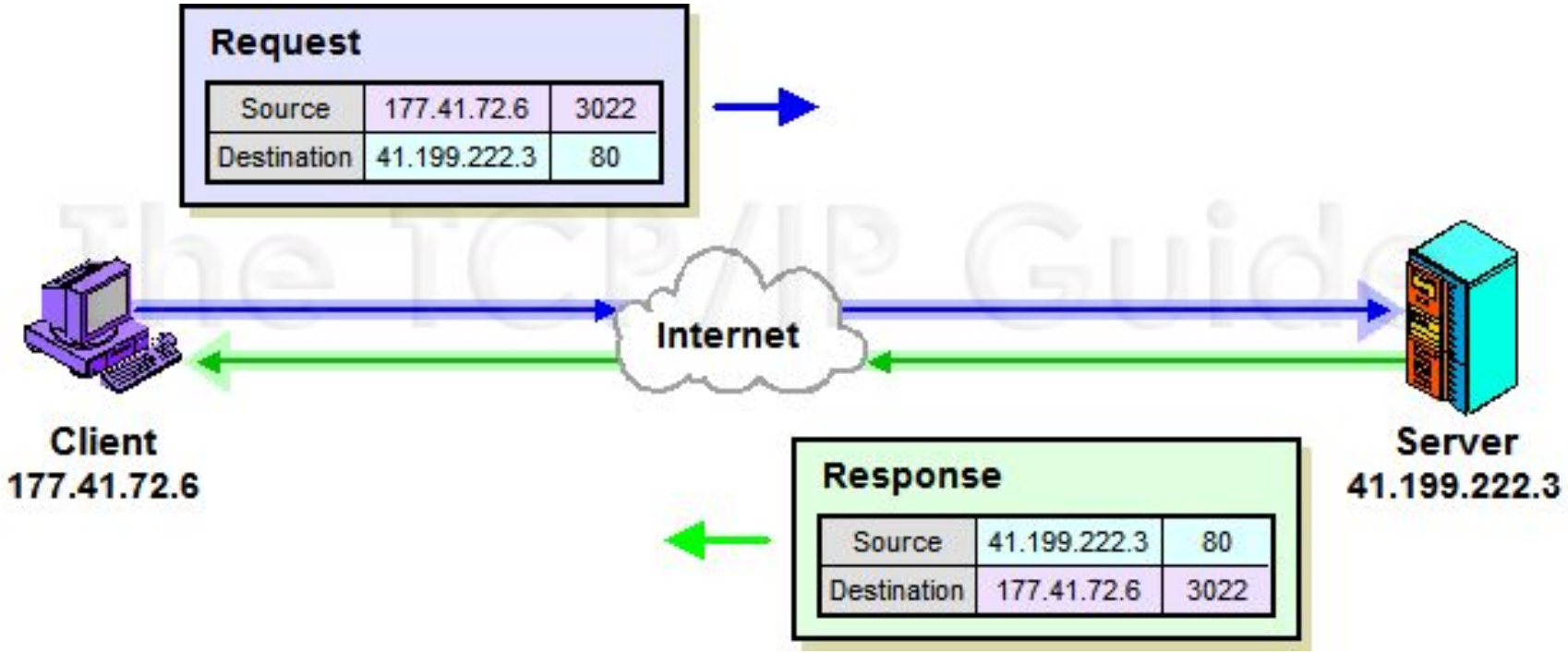
Funcionalitats de la capa de transport (OSI capa 4)

La capa de transport garanteix la transmissió de dades. A més, introdueix el concepte de **Port**. Un port **és un número** de 16 bits, per tant n'hi ha 2^{16} ports (65_536).

Els paquets en el nivell de transport es dirigeixen a un port d'una adreça IP, que apareix **en cada paquet**. Podem pensar en l'**adreça de transport** com la parella:

- L'**adreça IP** identifica el host de destí.
- El **port** és un identificador per vincular els missatges amb la interfície d'un **programari del host de destí**.

De la mateixa manera, el **remitent d'un paquet** de la capa de transport incorpora, a més de l'**adreça IP**, el **port** del programari remitent, per permetre la resposta.



Un exemple d'una petició Web http. El protocol ***http*** fa servir el ***port 80***.

Estat d'un port

En una comunicació es fa servir un port de l'emisor i un altre en el destí. Els ports tenen memòria intermèdia associada (*buffer*), tant per les dades rebudes com per les dades que s'envien.

Podem veure les comunicacions actives amb l'aplicatiu ***netstat***. Amb l'opció ***netstat -a*** veiem connexions TCP establertes i també els ports *oberts* (ports a l'aguait).

L'estat d'un port pot ser:

- **Obert**: Existeix una aplicació escoltant el port.
- **Tancat**: No n'hi ha cap aplicació escoltant.
- **Filtrat**: El tallafocs (*firewall*) no permet comunicacions fent servir aquest port.

Assignació dels ports

- ***Well Known Ports*** (Ports ben coneguts): Ports **fins el 1024**. Són serveis acordats que **gestiona el sistema operatiu**.
- ***Registered Ports*** (Ports registrats): Són ports que les fan servir diferents aplicacions; IANA manté una llista amb quin protocol fa servir cada port.
- ***Dynamic Ports / Private Ports***: Ports amb **número superior a *C000*** (hexadecimal). Ports que generalment s'assignen dinàmicament quan es crea la connexió.

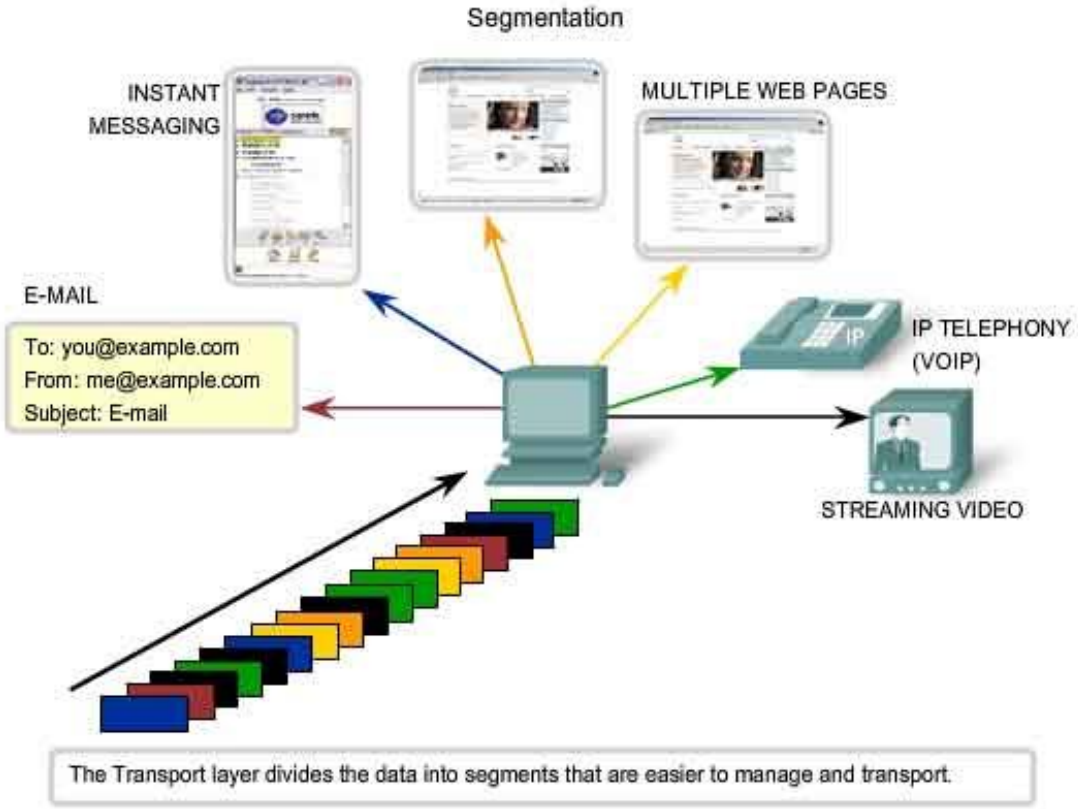
Els ports 25, 53, 80 i 443 són alguns dels ports més importants d'Internet, com podem veure més endavant en la llista.

Ports més freqüents

- **80 - HTTP** (*Hypertext Transfer Protocol*): Pàgines dels llocs Web.
- **443 - HTTPS** (*HTTP Secure*): Les pàgines dels llocs Web s'encripten i se autentiquen, garantint que provenen del servidor amb qui s'ha establert la connexió.
- **20, 21 - FTP** (*File Transfer Protocol*): Port 20 es fa servir per la transferència d'arxius, i el port 21 per les ordres i comandes.
- **67, 68 - DHCP** (Dynamic Host Configuration Protocol): Configuració automàtica: obtenir adreça IP, Gateway i servidor DNS. El port 67 correspon al servidor, i el 68 és el port del client. Fa servir missatges **UDP**.

Ports més freqüents (continuació)

- **23 - Telnet**: Connexió remota a un host en mode terminal.
- **22 - SSH** (*Secure Shell*): Connexió remota a un host en mode terminal, però incorpora encriptació i també transferència d'arxius.
- **25 - SMTP** (*Simple Mail Transfer Protocol*): Enviament de correu.
- **143 - IMAP** (*Internet Message Access Protocol*): Permet accedir al correu d'un servidor, sense haver de descarregar-lo (*correu Web*).
- **110 - POP3** (*Post Office Protocol Version 3*): Més antic que IMAP, protocol senzill que descarrega el correu del servidor i l'esborra.
- **53 - DNS** (Domain Name System): Servei de noms de domini. Fa servir **UDP**, però DNS també és capaç de funcionar per TCP, quan no pot fer-ho per UDP.
- **3389 - RDP** (*Remote Desktop Protocol*): Escriptori remot, només Windows.



Els **ports** actuen ***multiplexant*** el transport de dades de diferentes **aplicacions**.

És en les capes inferiors on els paquets IP i les trames *Ethernet* introdueixen la *multiplexació* que permet ***compartir el canal***. A més, les capes OSI superiors també poden afegir *multiplexació*; per exemple, podem obrir múltiples pàgines web simultàniament.

La **capa de transport** divideix les dades a transmetre en **paquets** (segments o *PDU*) que fa més fàcil la ***gestió d'errors***, i permet enviar les dades en ***paquets IP***, que s'envien en ***trames Ethernet***.

Per saber-ne més de consultar ports

L'aplicatiu **netstat** també ens pot informar quina aplicació fa servir el port (calen permisos d'administrador)

- En Windows: ***netstat -b***
- En Linux: ***netstat -p***

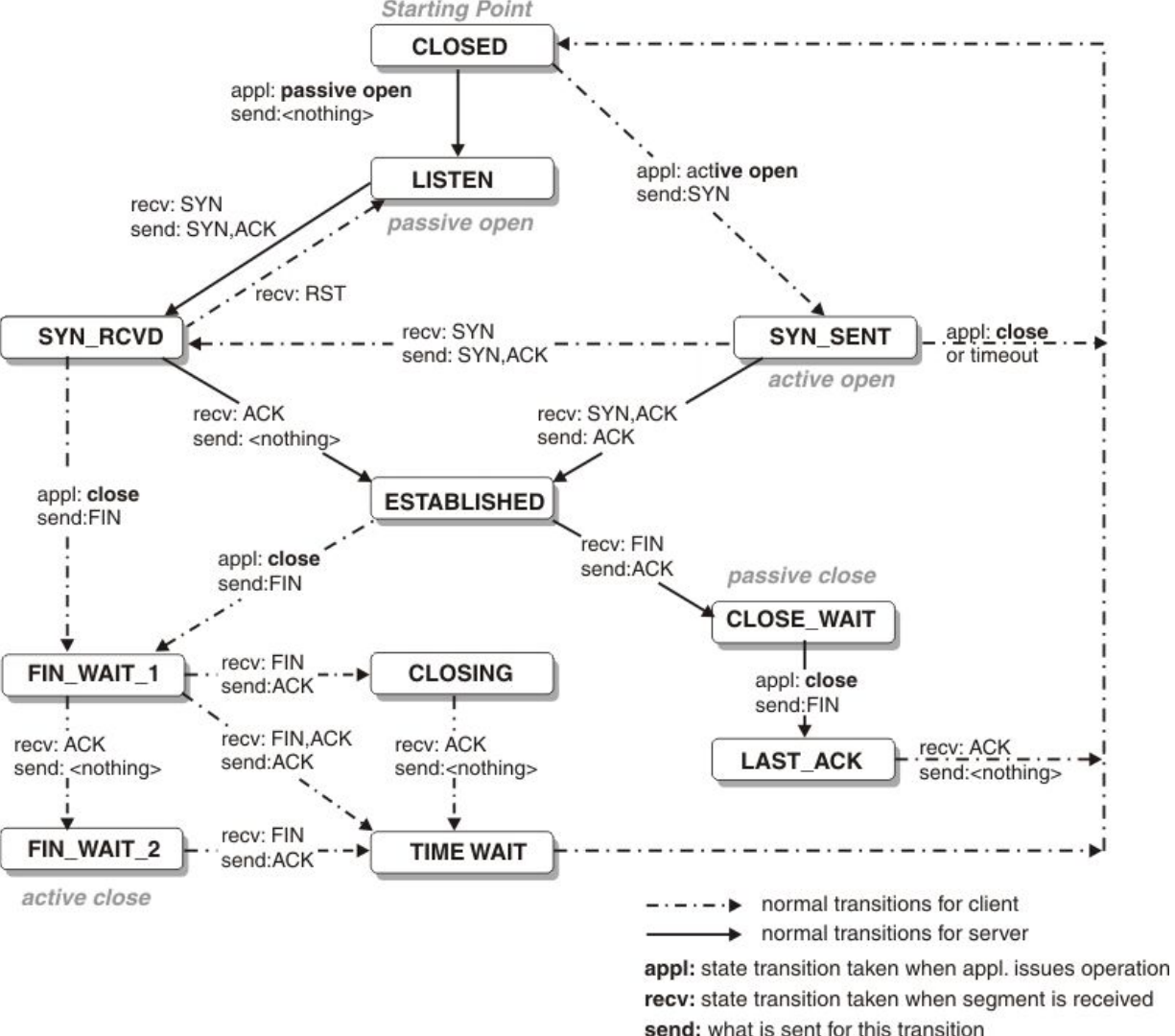
Es pot combinar amb l'opció -a

- En Windows: ***netstat -ab***
- En Linux: ***netstat -ap***

Per consultar l'estat dels ports, l'eina més coneguda per hackers i administradors de xarxa és **nmap**, que ens informa remotament de l'estat dels ports; així podem obtenir un informe de tota la xarxa, i detectar *vulnerabilitats* en qualsevol *host*.

TCP (*Transmission Control Protocol*)

- Orientat a la **connexió**:
  - Inicialment es produeix una **fase de connexió**, abans de la transferència de dades.
  - Una **fase de desconnexió** es produeix quan es finalitza:
    - Activament, amb una petició de desconnexió.
    - Pasivament, per time-out, si durant un temps no n'hi ha activitat.
- **Ordena i confirma** els paquets rebuts, **garantint que s'han rebut tots els paquets i en l'ordre correcte**.
- Inclou una **suma de control** (*checksum*) en cada paquet TCP, per garantir que les **dades de cada paquet s'han rebut sense errors**.

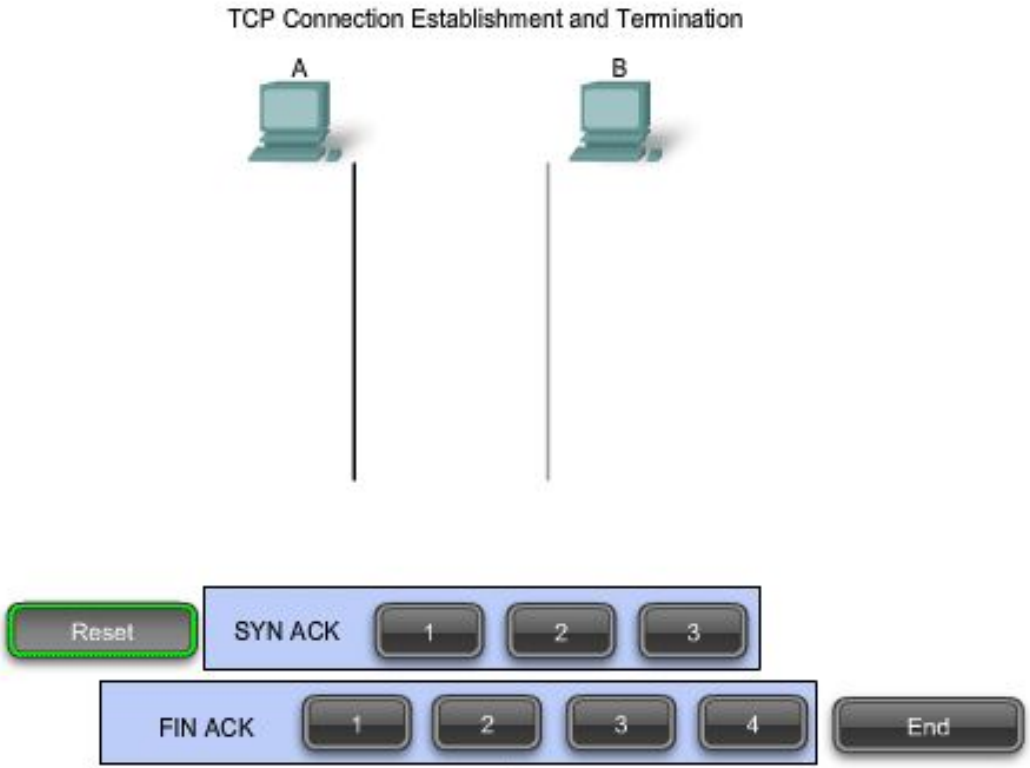


Per saber-ne més de les connexions TCP:

Estats d'una ***connexió***

TCP

La part esquerra del gràfic és qui rep la petició de connexió, que es troba *ESCOLTANT* (*LISTEN*), i la dreta qui emet la petició.



Per saber-ne més de les connexions TCP:

Missatges que s'intercanvien en les fases de ***connexió*** i ***desconnexió*** de **TCP**

Connexió en el nivell de capa física (nivell 1 OSI)

Les **xarxes telefòniques commutades** (***commutació de circuits***) proporcionen connexió entre dos punts (nivell físic) quan fem una trucada telefònica.

Es fan servir senyals de control per establir la connexió: **pulsos** (*obsolet*) o **tons**. Aquests senyals permeten que la connexió física s'estableixi punt a punt, fent servir mecanismes electrònics de commutació. Un **modem** faria servir aquests senyals per establir una connexió (*de nivell 1*) entre dos ordinadors o dues xarxes.

En canvi les connexions ***VoIP***, telefonia per Internet, com ara ***Skype***, i ara ja alguna companyia telefònica, fan servir **connexions** de ***nivell de transport*** (**TCP, OSI nivell 4**), o fins i tot de *nivell d'aplicació*, fent servir una xarxa de *commutació de paquets* (*Internet Protocol*).

Connexió en el nivell d'enllaç de dades (nivell 2 OSI)

Les connexions de nivell 2 s'anomenen ***Circuits Virtuals***

Per exemple, *Frame Relay* és una tecnologia que ofereix *Circuits Virtuals Permanents*, circuits predefinits que no cal establir i alliberar, en la capa d'enllaç de dades.

El concepte d'***Ethernet*** (CSMA/CD i CSMA/CA) és de medi compartit, són **protocols sense connexió**.

Connexió en el nivell de xarxa (nivell 3 OSI)

IP (***Internet Protocol***) és un protocol **sense connexió**.

La capa de xarxa pot admetre xarxes orientades a connexió o sense connexió (*recordem que la capa de xarxa interconnecta diferents xarxes*), però cada xarxa només pot ser d'un tipus.

Fiabilitat de la comunicació

Mecanismes de control d'errors de les capes inferiors:

- **Control de paritat** (*nivell físic, capa 1*)
- **CRC** (*Control de redundància cíclica*) valida les dades de les trames d'Ethernet (*capa d'enllaç de dades, capa 2*)

En la capa de transport s'afegeix un **Checksum** per a cada paquet.

A més a més, **TCP confirma els paquets**, de manera que els paquets que no arriben, o que arriben amb error, l'emissor els reenvia.

La connexió permet garantir el correcte ordre dels paquets, i que no s'ha perdut cap.

UDP (*User Datagram Protocol*)

- Protocol **sense connexió**.
- No ofereix garantia de que els paquets hagin estat entregats.
- No ofereix garantia en l'ordre en que paquets enviats seran rebuts.
- Senzillament, a les trames IP afegeix:
  - **Checksum** per garantir que en cada paquet les dades es reben sense errors.
  - Multiplexació d'aplicacions, fent servir **ports**.

És un protocol ***senzill***, amb menys sobrecàrrega que TCP.

És molt útil per missatges petits, de només un paquet, però cal considerar la situació que no arribi el paquet o arribi danyat. També es fa servir per *streaming* en temps real, perquè si un paquet no arriba es millor descartar-lo que esperar.

Els ports de capa 4 (*transport*) en la capa 3 (*xarxa*)

La capa 3 és capaç de fer la traducció d'adreces de xarxa (**NAT** *Network Address Translation*).

La principal finalitat és la **traducció d'adreces privades en adreces públiques**, amb dos objectius:

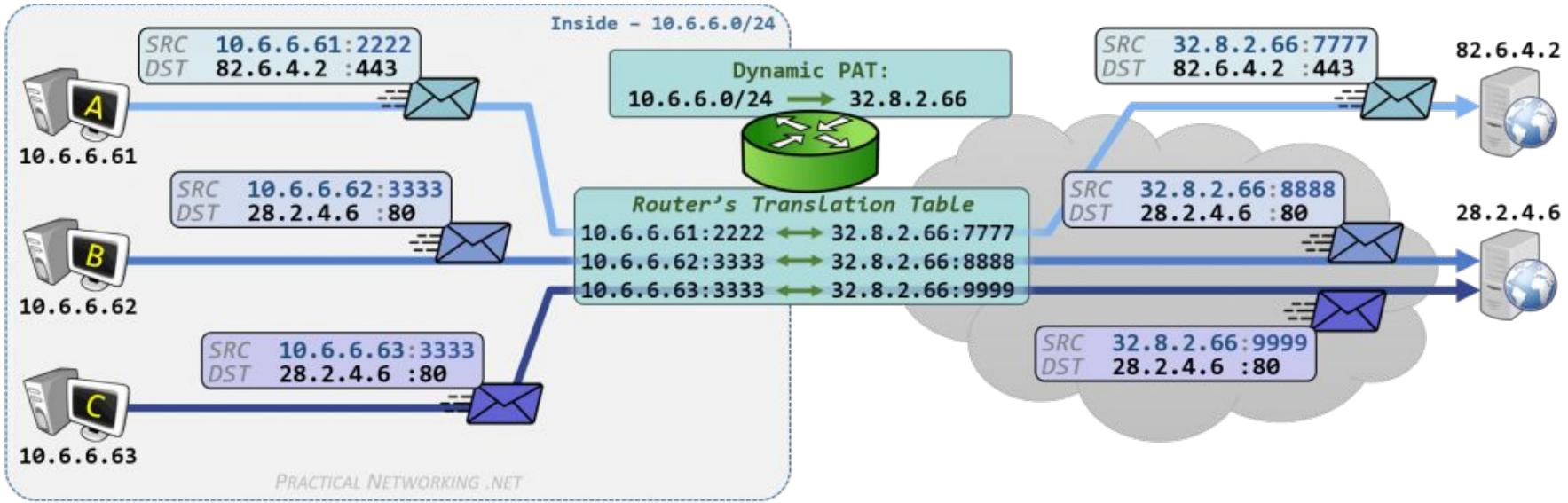
- Les adreces IP públiques són escases, i fent servir NAT podem ***compartir una adreça pública*** per a molts hosts d'una xarxa privada.
- ***Seguretat***: Si un host **no té adreça pública, no és accessible des de l'exterior**, quedant així amagada la xarxa privada darrera el servidor NAT.

Tipus de NAT

Tenim principalment dos tipus de **NAT**, i tots dos fan servir els ports de la capa de transport (TCP i UDP) :

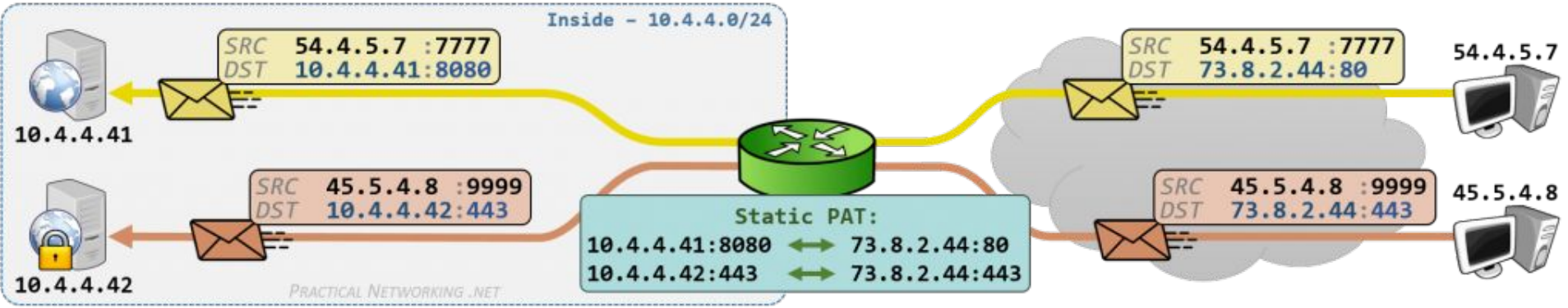
- **PAT** (*Port Address Translation*): Es fa servir per traduir l'**adreça d'origen**, convertint ***adreces IP privades en una adreça IP pública***.
  - De vegades també s'anomena ***IP masquerading***, o també ***dynamic PAT***.
- **DNAT** (*Destination Network Address Translation*): Es fa servir per traduir una **adreça de destí (servidor)** en una adreça privada, i permet tenir servidors especialitzats per a cada servei, compartint la mateixa adreça IP pública. Els servidors tindran adreces privades que amaguen l'accés a la resta de ports.
  - De vegades també s'anomena ***Port forwarding***, o també ***static PAT***.

PAT (també anomenat ***IP masquerading***, o també ***dynamic PAT***)



Moltes adreces privades comparteixen una mateixa adreça pública, fent servir un diferent port per a cada parella *adreça-port* mapejada.

DNAT (també anomenat ***Port forwarding***, o també ***static PAT***)



Es fa servir per mapejar en una **mateixa adreça** diferents **serveis oferts per diferents servidors**. Cada servei es correspon amb un port, i assignem una adreça local diferent per a cada port.

En la imatge d'exemple, un servidor HTTP (port 80) i un HTTPS (port 443).

Per saber-ne més:

UPnP port forward

Universal Plug&Play port forward (DNAT)