PARTE 8

Elementi di Sicurezza Informatica per reti di calcolatori

Modulo 1 – VLAN e NAT

Meccanismi di sicurezza di rete: A quali livelli?

- Più si sale nello stack TCP/IP e più le funzioni di sicurezza potranno essere specifiche (es., è possibile identificare l'utente, i comandi, i dati) ed indipendenti dalle reti sottostanti. Soluzioni computazionalmente più onerose e quindi:
  - difficili da realizzare in reti ad alto traffico
  - soggette ad attacchi di tipo DoS (quanti ne subiscono?)
- Più si resta in basso nello stack e più sarà possibile "espellere" in fretta gli intrusi, ma le informazioni su cui basare le decisioni saranno più scarse (es., solo indirizzo MAC o IP, nessuna informazione sugli utenti, sui comandi e sulle applicazioni)

A quale livello è meglio introdurre meccanismi di sicurezza?

- Risposta ideale: a tutti i livelli!
- Paradigma di riferimento: **defense in depth**
- Deve essere declinato sulla base delle specifiche esigenze e dei vincoli (budget)

Segmentazione e segregazione

- Segmentazione: partizionare le risorse aziendali
  - Logiche e fisiche
  - Suddividere le reti in sottoreti, evitare *share di rete aperti*

- Segregazione: applicare controllo degli accessi
  - Definire politiche per accessi *cross-segment*
  - Applicare politiche mediante opportune tecnologie

Segmentare e segregare il traffico

- Virtual LAN (VLAN)
- Network Address Translation (NAT) e Port Address Translation (PAT)
- Firewall:
- Architetture sicure (DMZ)

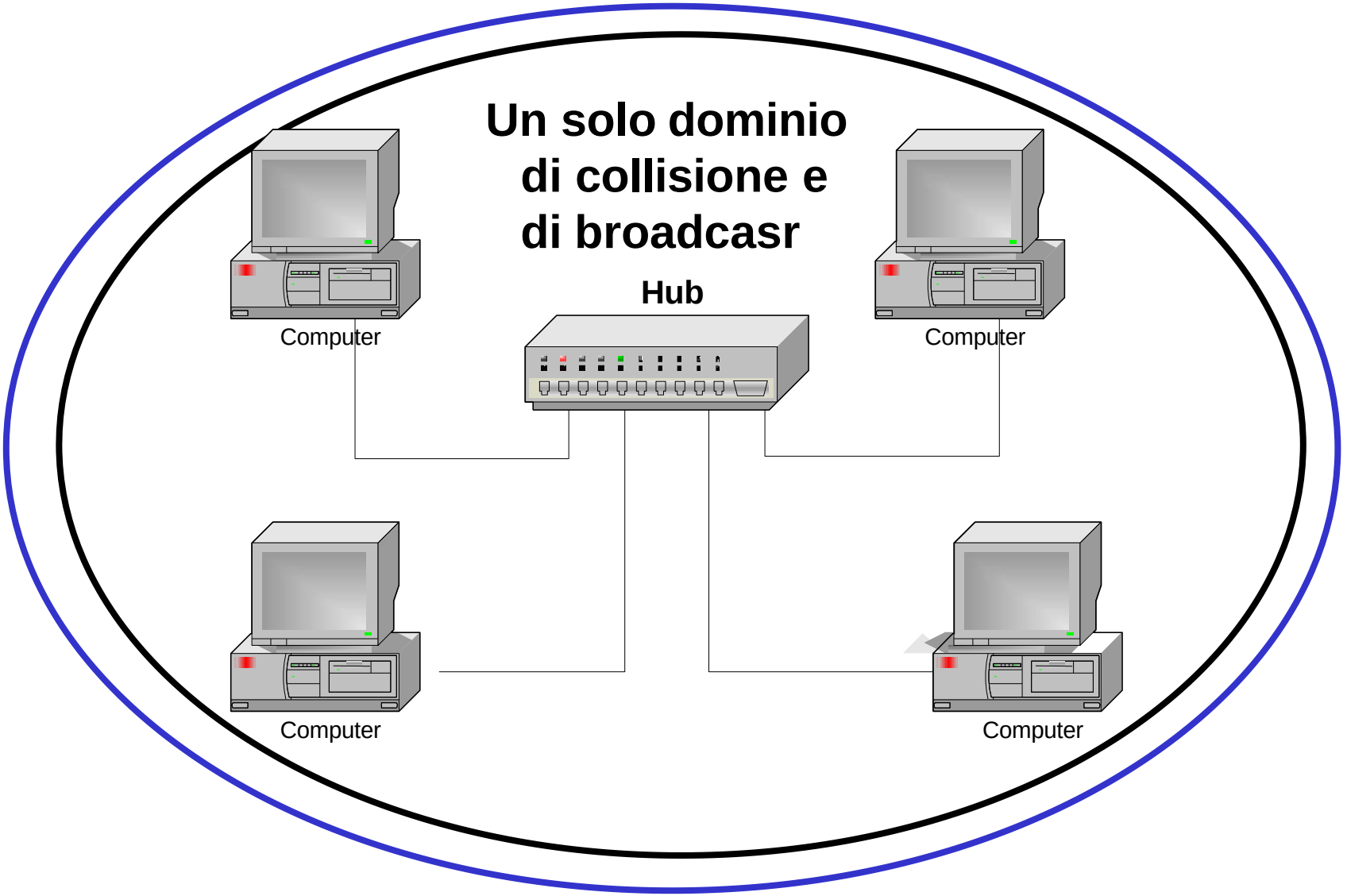
VLAN

LAN tradizionale

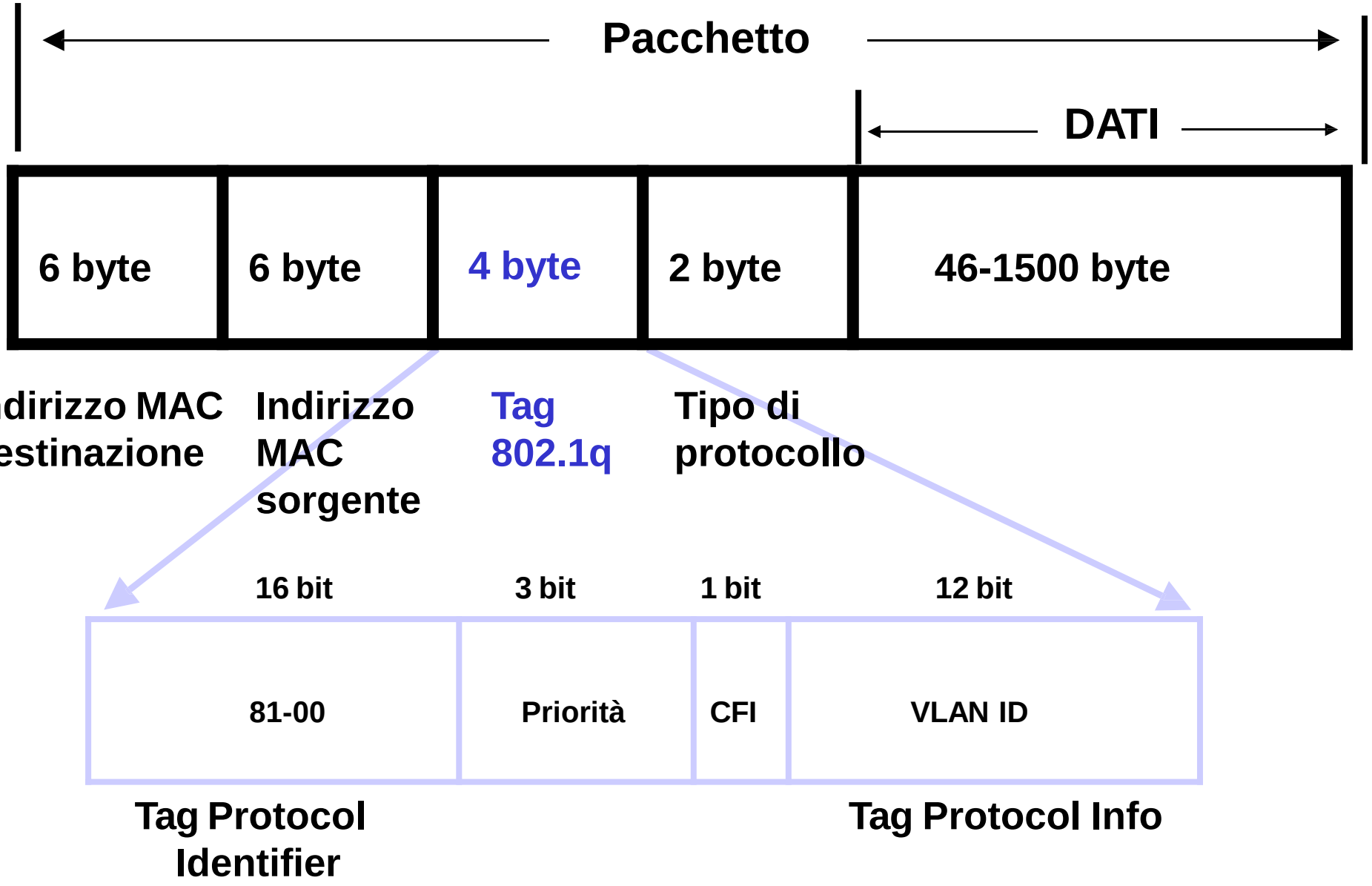
- Gli host sono aggregati “fisicamente” mediante dispositivi di rete, quali *hub*, *switch* e *router*

- *Hub*: non differenziano il dominio di collisione né il dominio di broadcast
- *Switch*: differenziano il dominio di collisione ma non il dominio di broadcast
- *Router*: differenziano sia il dominio di collisione sia il dominio di broadcast

Dominio di collisione: hub

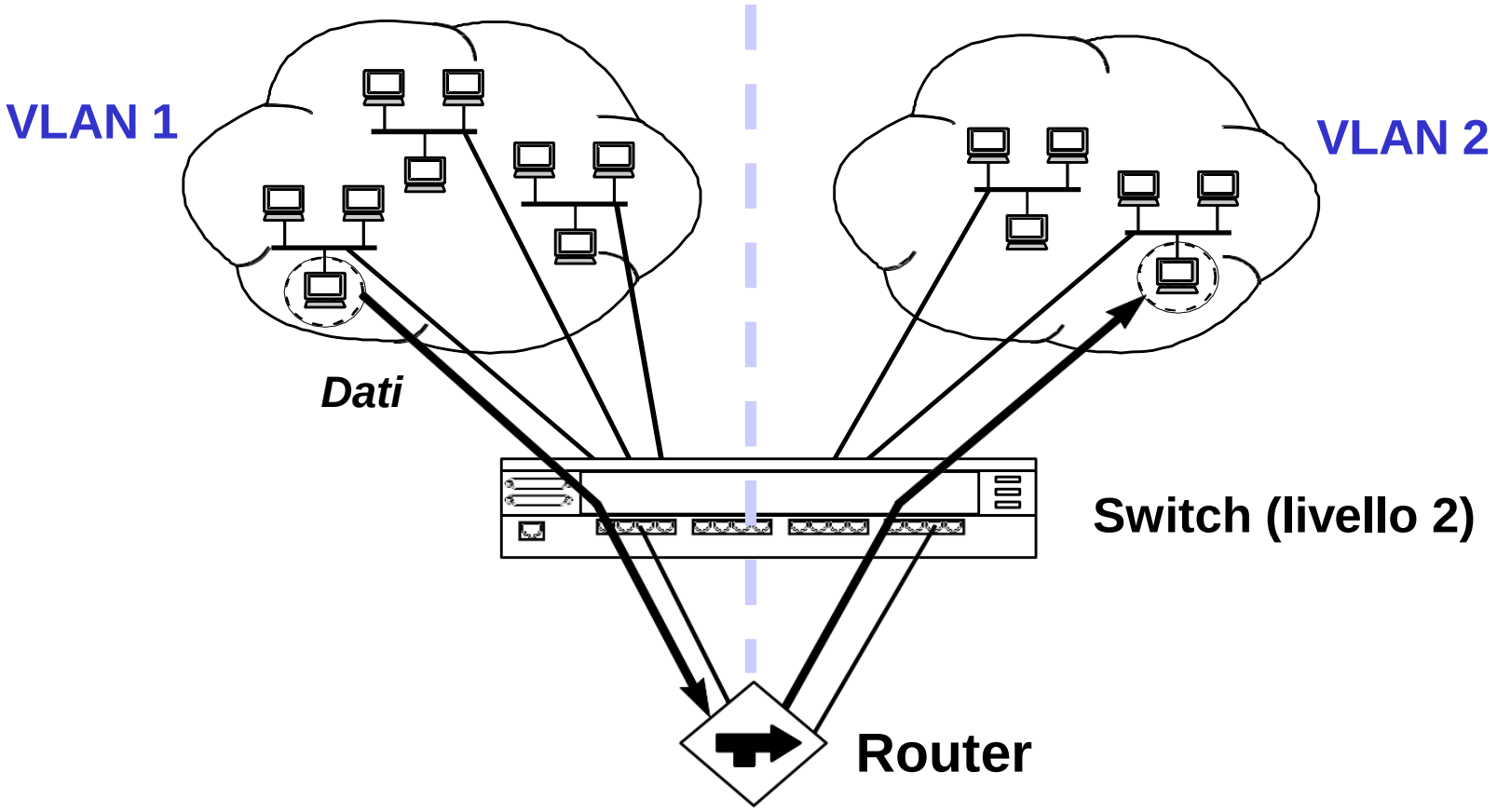


Frame tagging



VLAN e Router

- Poiché le VLAN definiscono domini di broadcast differenti, i router sono fondamentali per ricostruire un pacchetto con gli indirizzi MAC della VLAN di destinazione



NAT (PAT)

Reti semi-private

- Per molte organizzazioni è importante avere *reti semi-private* con tre categorie di host:
  - nessun accesso da/a host fuori “dall’organizzazione” (molti host)
  - accesso parziale (host che possono raggiungere l’esterno ma non sono raggiungibili dall’esterno)
  - accesso completo (pochi host, es. server Web)

Indirizzi non routable

- Poiché per molte organizzazioni non è necessario che tutti i loro indirizzi siano visibili globalmente, per evitare di sprecare indirizzi, la IANA ha definito delle *reti private*, ossia:
  - non uniche a livello mondiale (RFC 1918)
  - con indirizzi IANA privati (Non-Internet Routable IP Addresses)
  - gli indirizzi “non routable” si possono utilizzare senza richiedere autorizzazione, purché si garantisca che il traffico e gli indirizzi siano limitati alla rete interna

Indirizzi IP privati per Intranet

- In questo modo, un'organizzazione tipicamente ha la possibilità di progettare una rete che:
  - include host visibili da Internet (*host pubblici*)
  - altri host che non sono visibili (*host privati*)
- Gli *host privati* possono scambiare pacchetti:
  - solo con altri host privati all'interno della stessa rete senza intermediari
  - con host pubblici mediante:
    - **Application gateway (*proxy*) sugli host pubblici**
    - **Network Address Translation (NAT)**

Indirizzi per NAT

	Intervallo di indirizzi		
Classe A:	**[10.0.0.0 -10.255.255.255]**	**(10.0.0.0/8)**	**– 1 rete**
Classe B:	**[172.16.0.0 - 172.31.255.255]**	**(172.16.0.0/12)**	**– 16 reti**
Classe C:	**[192.168.0.0 - 192.168.255.255]**	**(192.168.0.0/12)**	**– 256 reti**

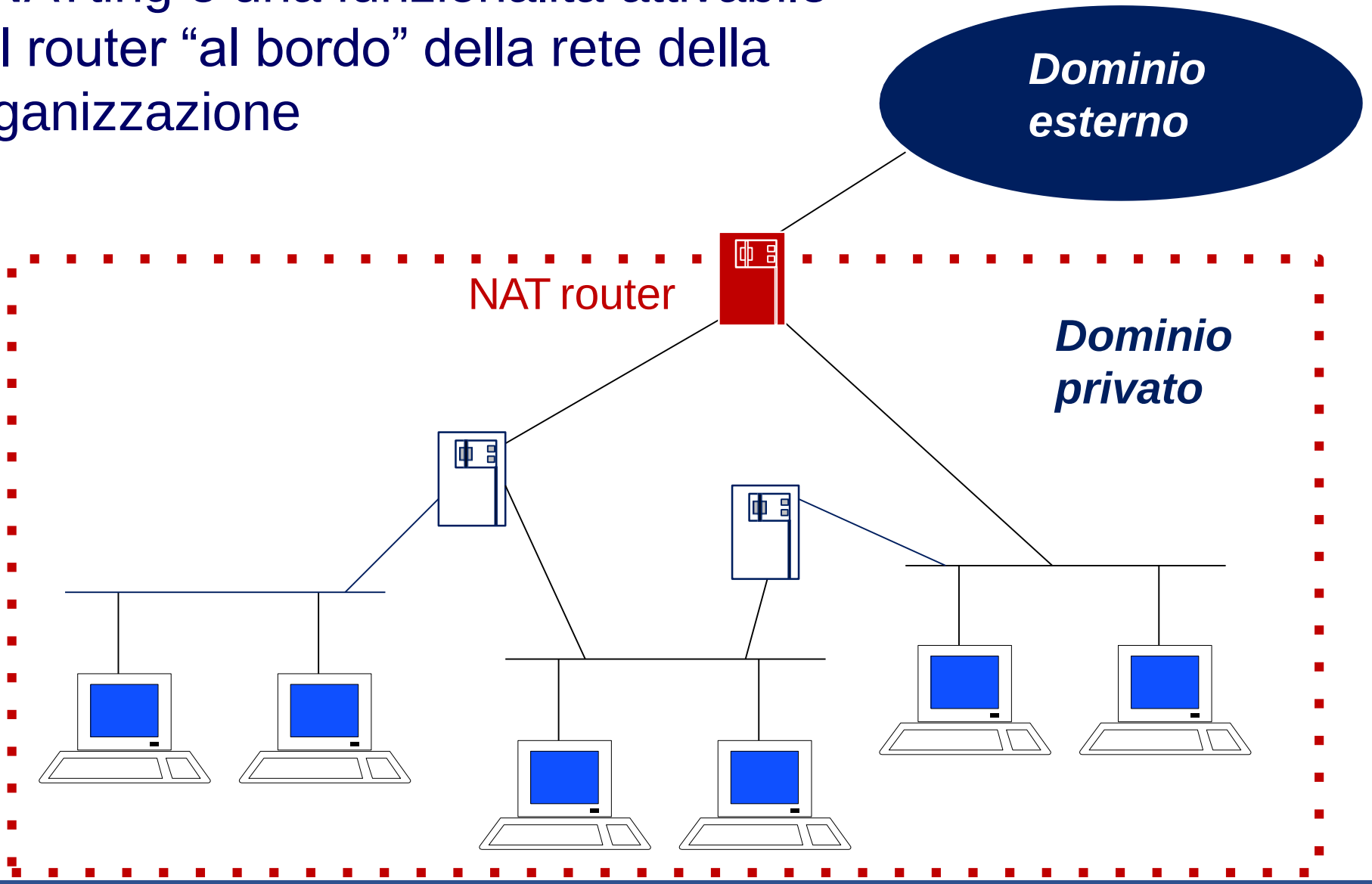
NAT router

- Il ***NAT router*** (un router con funzionalità di NATting) si interpone tra la rete locale di una organizzazione e Internet con i seguenti compiti:
  - Mappa gli indirizzi IP tra due domini (interno-esterno)

    indirizzi locali ←→ indirizzi IP globali
  - Garantisce la trasparenza del routing tra gli *end system*
  - "Moltiplica" le possibilità di interconnessioni di host di una organizzazione (nel caso in cui l'organizzazione abbia a disposizione un numero di indirizzi IP inferiore al numero di host)
  - Aumenta la sicurezza evitando di rendere visibili all'esterno alcuni computer di una organizzazione

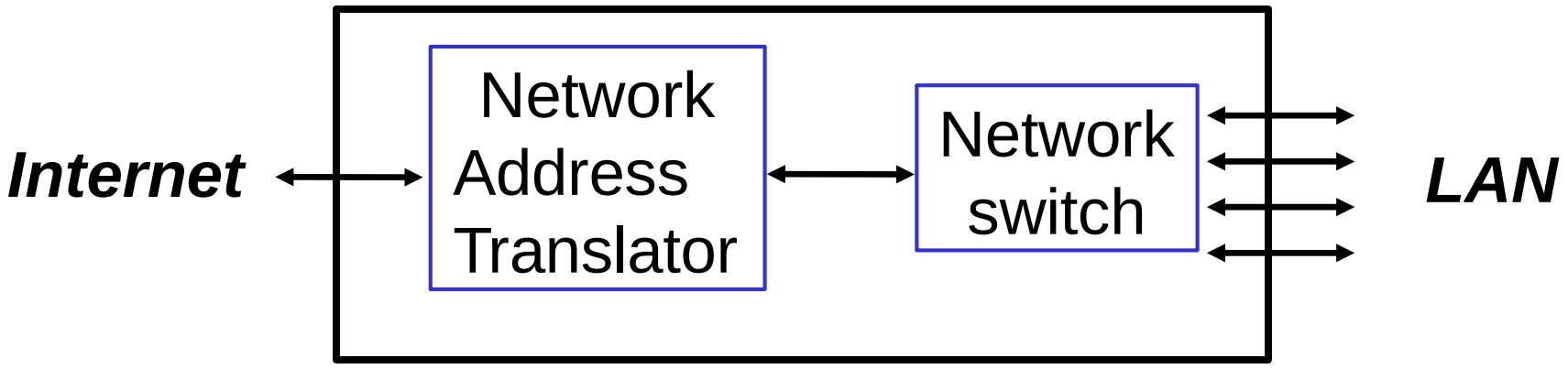
NATting per reti semi-private

Il NATting è una funzionalità attivabile sul router “al bordo” della rete della organizzazione

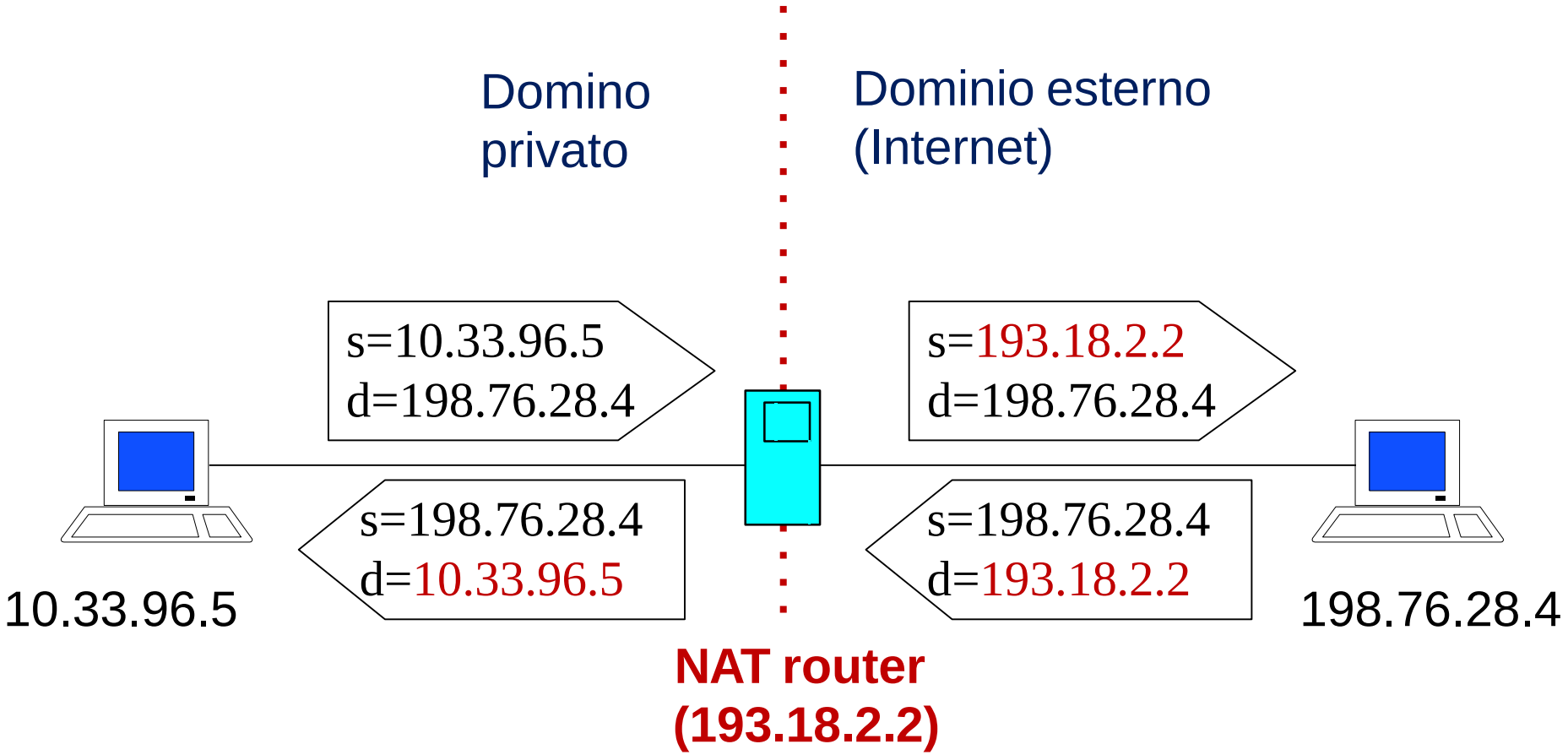


NAT router

In realtà, ha due funzionalità: *natting* e *switching*



Traduzione indirizzi - NAT



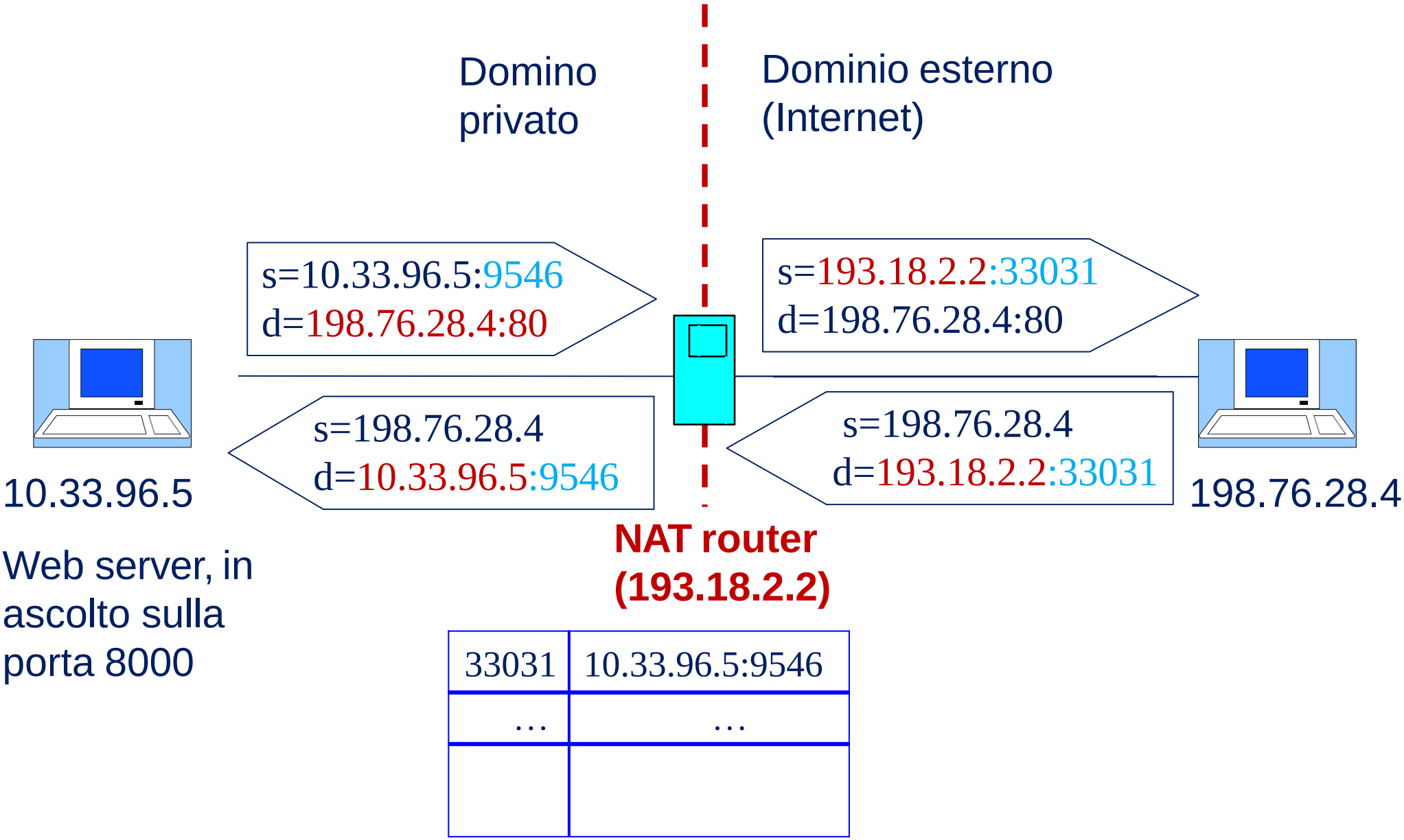
- Implementazione *software*: processo su un *dual-homed host*
- Implementazione *hardware*: a livello di router

Port Address Translation

- In una versione del NATting, è prevista la possibilità di "tradurre" non solo l'indirizzo IP sorgente, ma anche la porta sorgente ➔ **PAT**
- Molte operazioni NAT sono in realtà operazioni PAT per cui vi è confusione tra i termini
- Cisco, l'azienda leader dei router, usa il termine PAT

- Il PATting non crea particolari limitazioni di connessioni in quanto il NAT router ha un pool di circa 60000 numeri di porta disponibili

NAT/PAT, binding dinamico

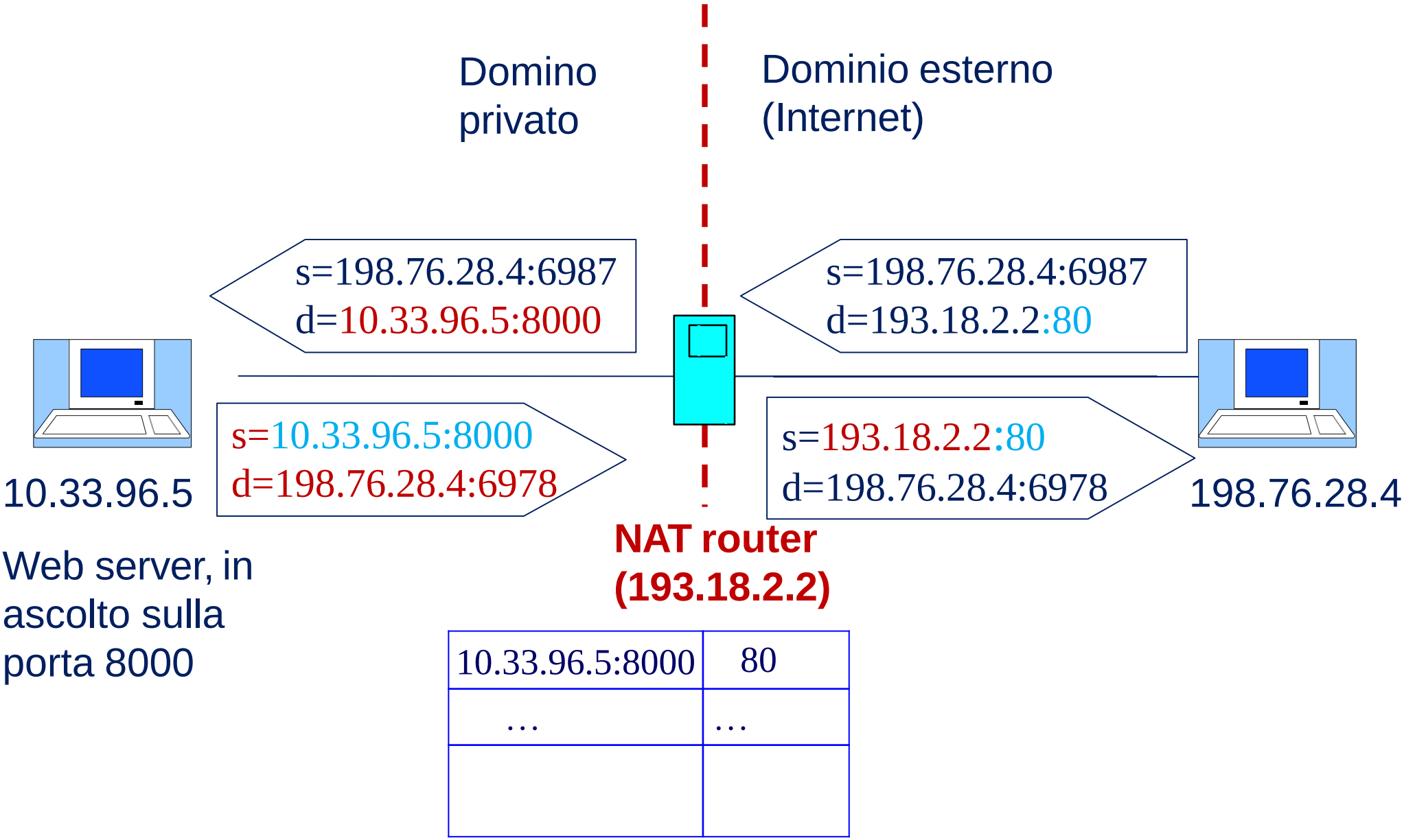


Binding degli indirizzi

Si gestisce una corrispondenza (*binding*) tra i due domini tramite una TABELLA di stato con le corrispondenze tra gli indirizzi e le porte originarie e i valori modificati:

- **binding statico**
  - la tabella viene configurata manualmente
- **binding dinamico**
  - la tabella viene calcolata dinamicamente
  - cambia nel tempo a seconda del traffico
  - ciascuna “sessione” ha una riga nella tabella
  - i numeri di porta degli hosti interni vengono mappati in numeri di porta presi da un pool del PAT router
  - la dimensione del pool determina il numero massimo di connessioni contemporanee a Internet, le altre vengono rifiutate dal router

NAT/PAT, binding statico



Natting: contro

Svantaggi

- Distrugge la semantica della comunicazione Internet *stateless* e *end-to-end* in quanto:
  - gli host interni non possono essere raggiunti direttamente dall'esterno
  - il NAT router mantiene uno "stato" sulla connessione
- La cosiddetta ***NAT box*** modifica i pacchetti al volo:
  - qualche volta questo richiede modifiche a livello di informazioni application e non solo header del datagramma IP (es., indirizzo IP nel protocollo FTP)
  - È necessario usare dei gateway NAT box a livello applicazione

Natting: pro

Vantaggi

- Distrugge la semantica della comunicazione *end-to-end,* che era uno dei fondamenti su cui è stata progettata Internet, in quanto gli host interni non possono essere raggiunti direttamente dall'esterno, ma tramite un elemento di controllo centralizzato

  → **Ottima soluzione per la SICUREZZA**

- Soluzione economica, relativamente facile e veloce
- Consente massima flessibilità nella gestione interna degli indirizzi (aggiunte, eliminazioni, modifiche) senza necessità di richiedere alcun permesso al proprio ISP né di comunicare ad altri eventuali modifiche