

Livello Collegamento

Ethernet

Switch

VLAN

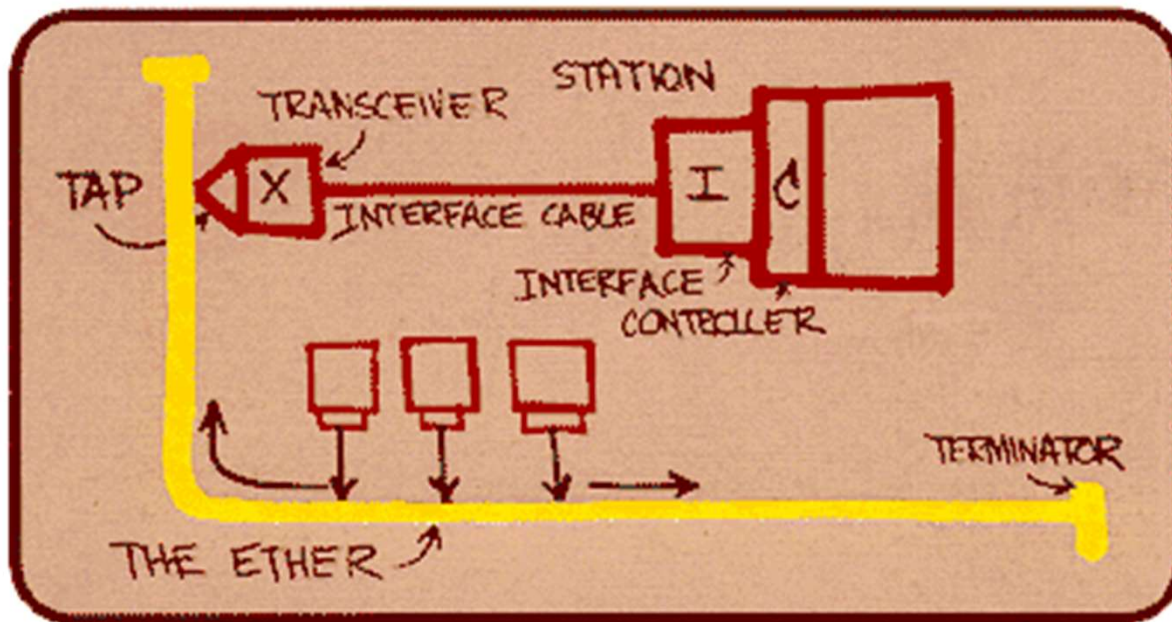
Reti di Calcolatori

Federica Paganelli

Ethernet

Detiene una posizione dominante nel mercato delle LAN cablate.

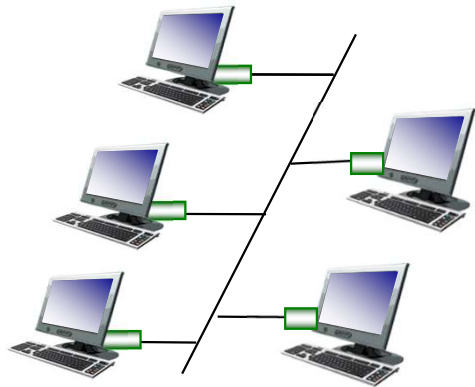
- È stata la prima LAN ad alta velocità con vasta diffusione.
- Più semplice e meno costosa di token ring, FDDI e ATM.
- Sempre al passo dei tempi con il tasso trasmissivo (10 Mbps, 100Mbps, 1 Gbps, 10 Gbps, 40 Gbps...).



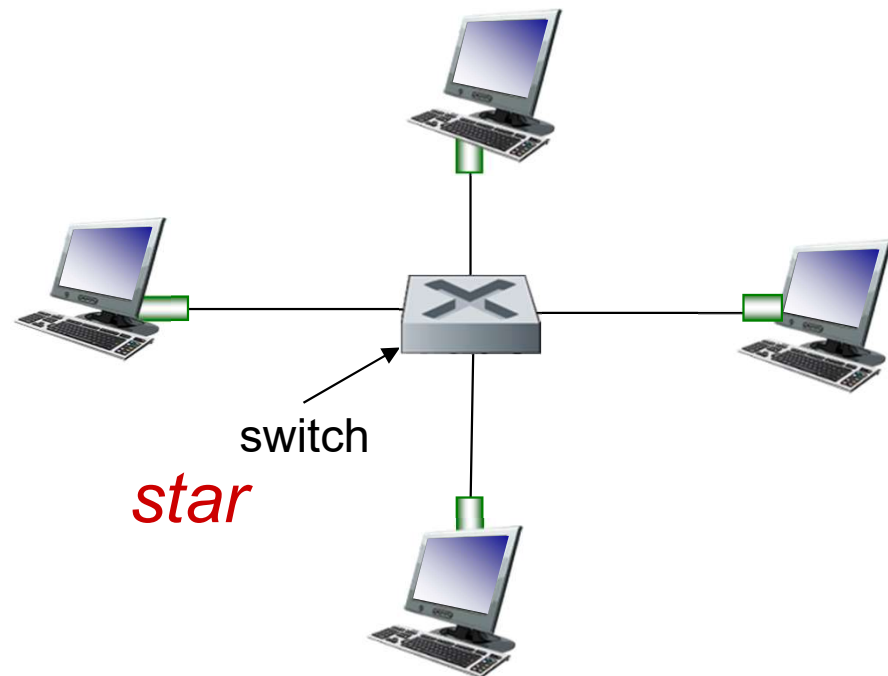
Il progetto originale di Bob Metcalfe che portò allo standard Ethernet nella metà degli anni '70

Topologia fisica

- La topologia a bus era diffusa fino alla metà degli anni 90.
- Quasi tutte le odierne reti LAN Ethernet sono progettate con topologia a stella.
- Al centro della stella è collocato uno *switch*.



bus: coaxial cable



Struttura dei pacchetti Ethernet

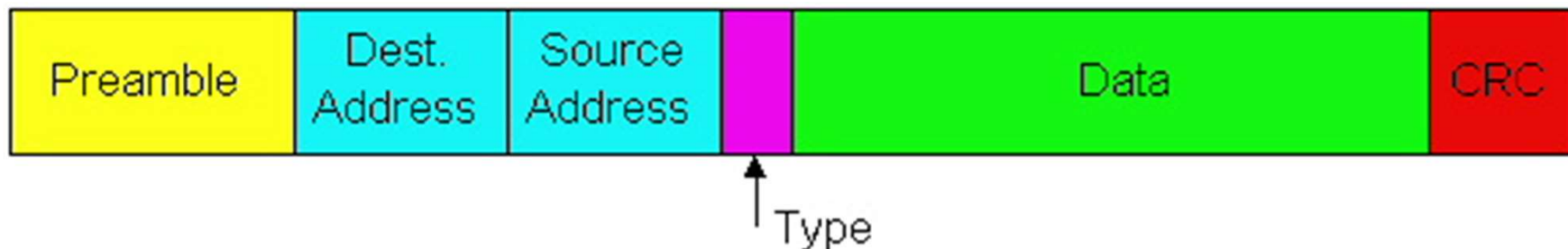
- L'adattatore trasmittente incapsula i datagrammi IP in un pacchetto Ethernet



- **Preambolo:**
 - I pacchetti Ethernet iniziano con un campo di otto byte: sette hanno i bit 10101010 e l'ultimo è 10101011.
 - Servono per “attivare” gli adattatori dei riceventi e sincronizzare i loro orologi con quello del trasmittente.
- **Dati:**
 - L'unità massima di trasferimento MTU varia da 46 byte ad un max di 1500 byte. Se il datagramma è più grande allora deve essere frammentato. Se il campo dati è più piccolo il campo dati deve essere riempito (stuffed)

Struttura dei pacchetti Ethernet

- **Indirizzo di destinazione:** 6 byte
- Quando un adattatore riceve un pacchetto con indirizzo di destinazione corrispondente al proprio indirizzo MAC o l'indirizzo broadcast (es.: un pacchetto ARP), trasferisce il contenuto del campo dati del pacchetto al livello di rete.
- I pacchetti con altri indirizzi MAC vengono ignorati.
- **Indirizzo sorgente:** 6 byte. Indirizzo dell'adattatore (scheda di rete) che trasmette il frame
- **Campo tipo (2 byte):** consente a Ethernet di supportare vari protocolli di rete (i.e., IP, ARP) (in gergo questa è la funzione di “multiplexare” i protocolli).
- **Controllo CRC:** consente all'adattatore ricevente di rilevare la presenza di un errore nei bit del pacchetto.

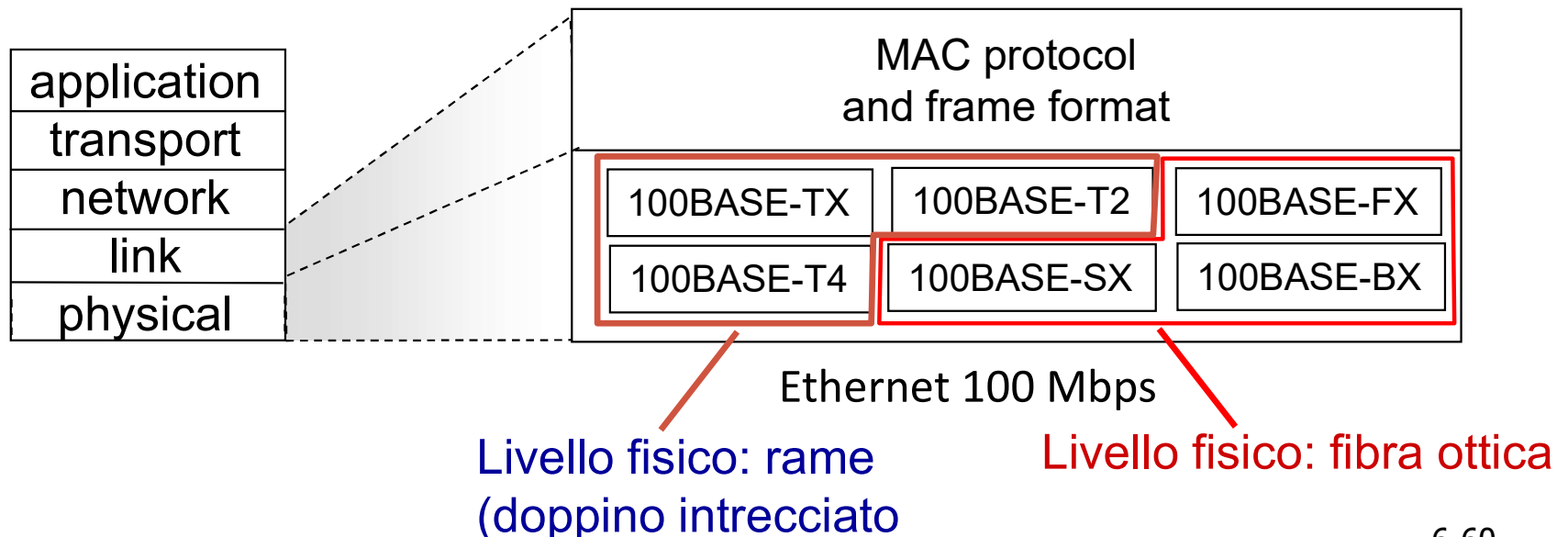


Ethernet: non affidabile, senza connessione

- *connectionless*: no handshaking tra nodo mittente e destinatario
- *unreliable: nodo* in ricezione non invia ack or nack al nodo mittente
 - I dati nei frame eliminati (dropped) sono recuperati solo se il trasferimento dati affidabile è implementato ai livelli superiori (e.g., TCP),
 - Protocollo MAC in LAN broadcast : *CSMA/CD con binary backoff*

802.3 Ethernet standards: link & physical layers

- *molti* standard Ethernet diversi
 - protocollo MAC e formato frame in comune
 - Differenti velocità: 2 Mbps, 10 Mbps, 100 Mbps, 1Gbps, 10 Gbps, 40 Gbps (ma anche 100G e superiori)
 - Mezzo fisico: fibra, cavo coassiale, doppino intrecciato



Evoluzione di Ethernet

Ethernet 10 Mbps

- primi standard 10BASE-2 e 10BASE-5 su due tipi di cavi coassiali, ciascuno limitato a una lunghezza di 500 metri.
- Segmenti più lunghi si possono ottenere usando un repeater (ripetitore)
- CSMA/CD

Fast Ethernet

- 100 Mbps
- 100 metri di distanza su doppino e a parecchi chilometri su fibra
- Usare un commutatore (switch) a livello link, dotato di buffer. Switch al centro della stella, tutti i nodi collegati ai rami della stella → **no collisioni**

Gigabit Ethernet (802.3z)

- 1000 Mbps = 1 Gbps
- Mantiene invariata lunghezza min/max frame

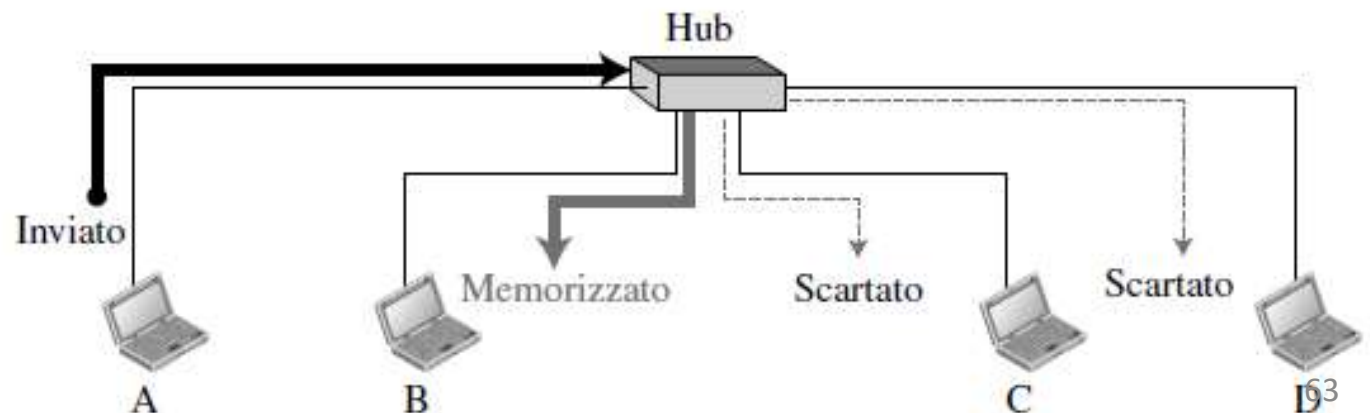
40/100 Gigabit Ethernet (802.3b..)

- Estende tecnologia, velocità trasferimento, distanza max copertura
- 40 Gbps: data centers
- 100 Gbps internet backbones

Dispositivi di interconnessione

Repeater e Hub

- Repeater
 - operano solo a livello fisico
 - Rigenerano il segnale che ricevono
 - in passato usati per collegare segmenti di Ethernet con topologia a bus
- Hub
 - repeater multi-porta
- Repeater e hub non hanno capacità di filtraggio

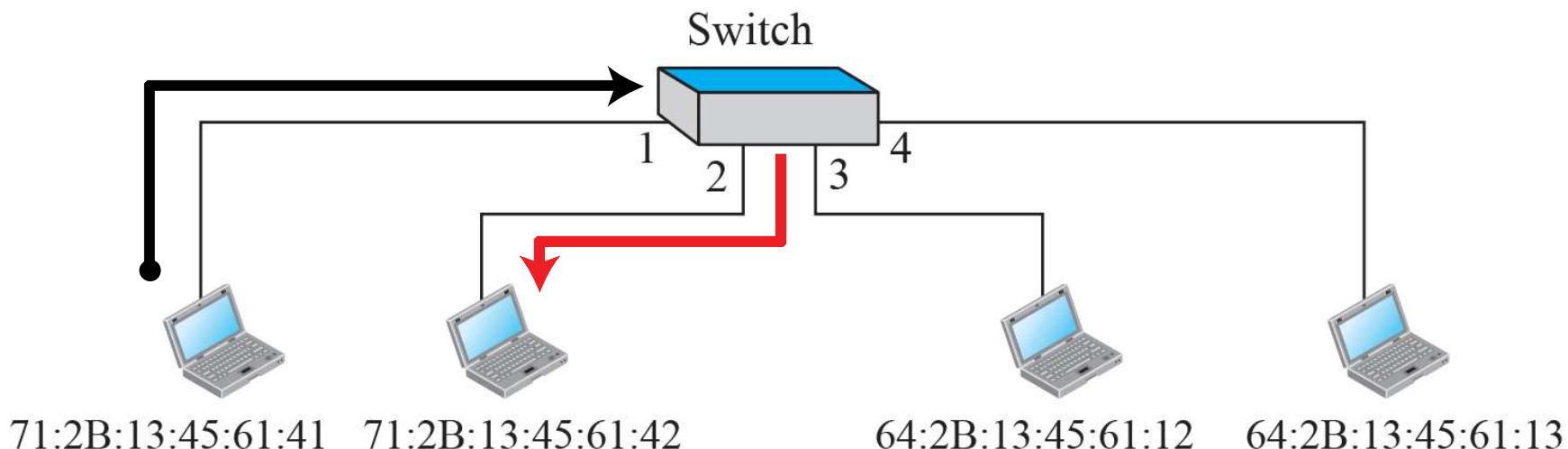


Switch di livello link

- Operano
 - Sia a livello fisico: rigenerando segnale
 - Sia a livello link: verificando indirizzi MAC contenuti in frame
- Dispositivi store and forward (buffer)
- Non modificano indirizzi MAC in intestazione frame
- Hanno una tabella che usano per filtraggio

Tabella di commutazione

Indirizzo	Porta
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3
64:2B:13:45:61:13	4

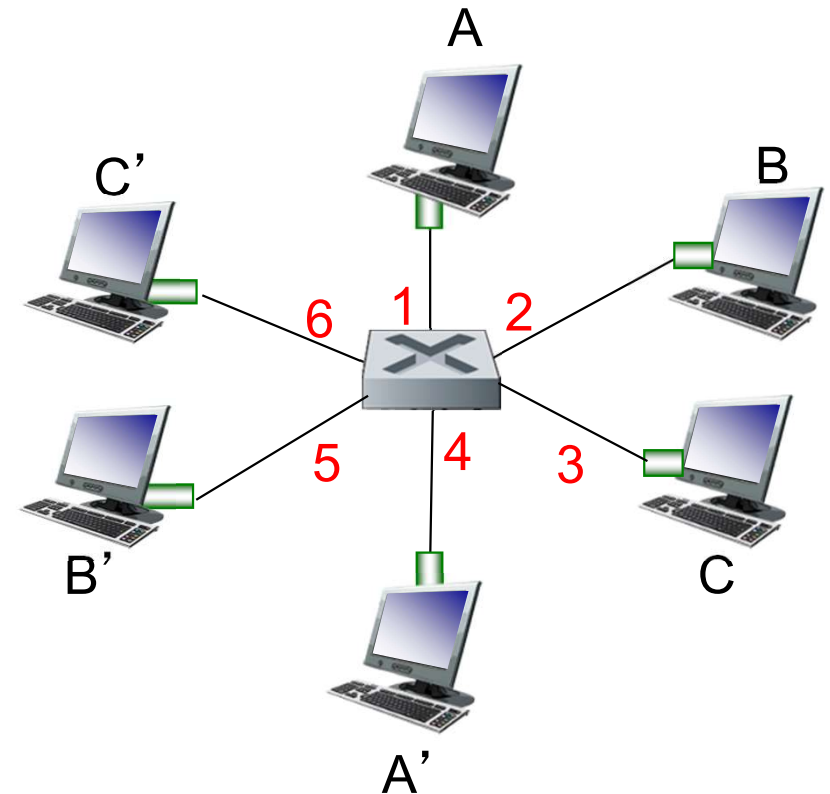


Ethernet switch

- **link-layer device: ruolo attivo**
 - Store and forward di frame Ethernet
 - Esamina gli indirizzi MAC dei frame in arrivo, inoltra in modo selettivo i frame su uno o più collegamenti
- ***transparente***
 - Gli host non sono a conoscenza della presenza degli switch
- ***plug-and-play, self-learning***
 - Gli switch non devono essere configurati

Switch: trasmissioni *multiple* simultanee

- Gli host hanno connessioni dedicate verso lo switch
- Gli switch bufferizzano i pacchetti
- no collisions; full duplex
 - Ogni link ha il suo proprio dominio di collisione
- *switching*: A-to-A' and B-to-B' possono trasmettere simultaneamente, senza collisioni



*switch with six interfaces
(1,2,3,4,5,6)*

Switch con auto-apprendimento

Costruzione graduale della tabella

Indirizzo	Porta
-----------	-------

a. Originale

Indirizzo	Porta
71:2B:13:45:61:41	1

b. Dopo che A invia un frame a D

Indirizzo	Porta
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4

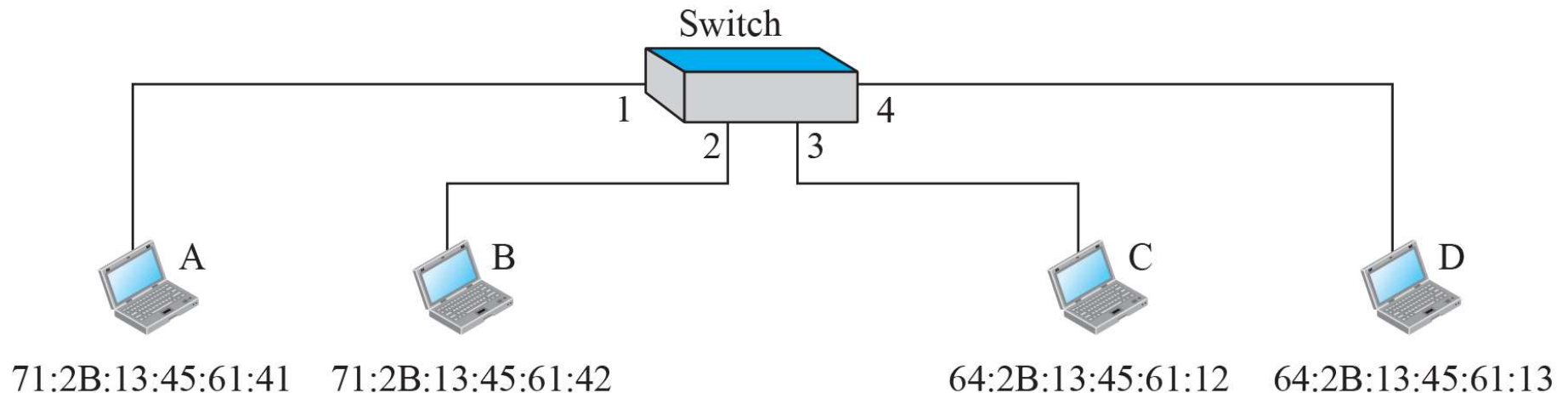
c. Dopo che D invia un frame a B

Indirizzo	Porta
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2

d. Dopo che B invia un frame ad A

Indirizzo	Porta
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3

e. Dopo che C invia un frame a D



Switch: frame filtering/forwarding

when frame received at switch:

1. record incoming link, MAC address of sending host
2. index switch table using MAC destination address

3. if entry found for destination

then {

if destination on segment from which frame arrived

then drop frame

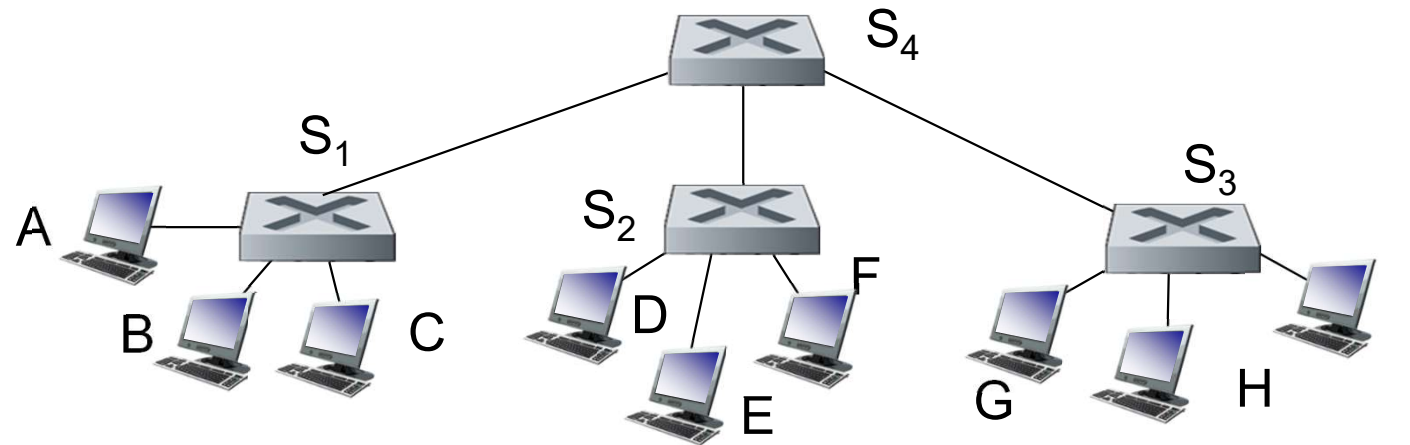
else forward frame on interface indicated by entry

}

else flood /* forward on all interfaces except arriving
interface */

Interconnecting switches

Più switch ad autoapprendimento possono essere collegati:

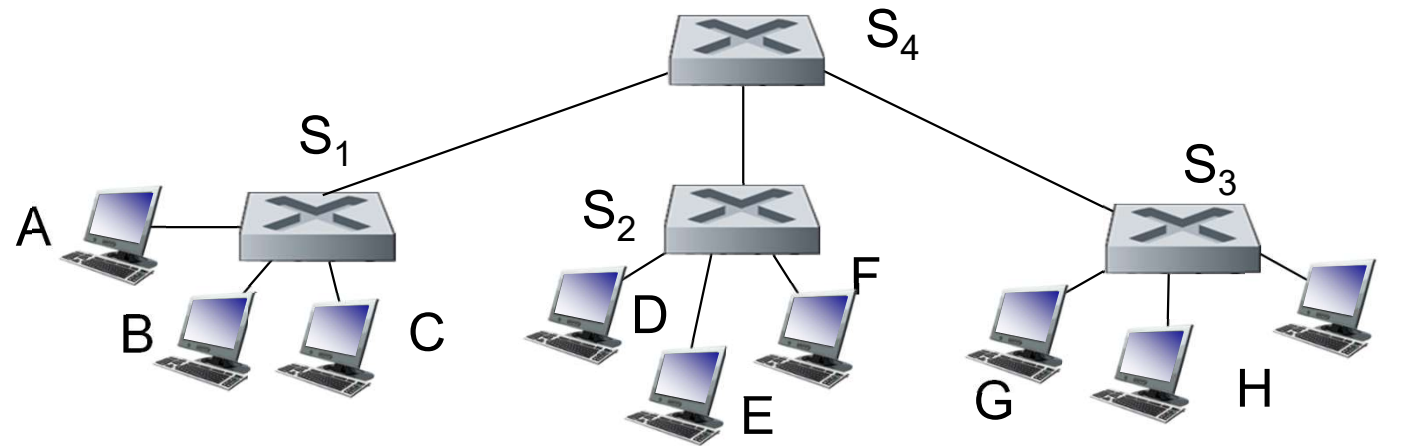


Q: A invia un frame a G – come fa S_1 ad apprendere che il frame destinato a G deve passare da S_4 e S_3 ?

- **A:** self learning! (esattamente come nel caso dello switch singolo!)

Self-learning multi-switch example

C invia un frame a I, I risponde a C

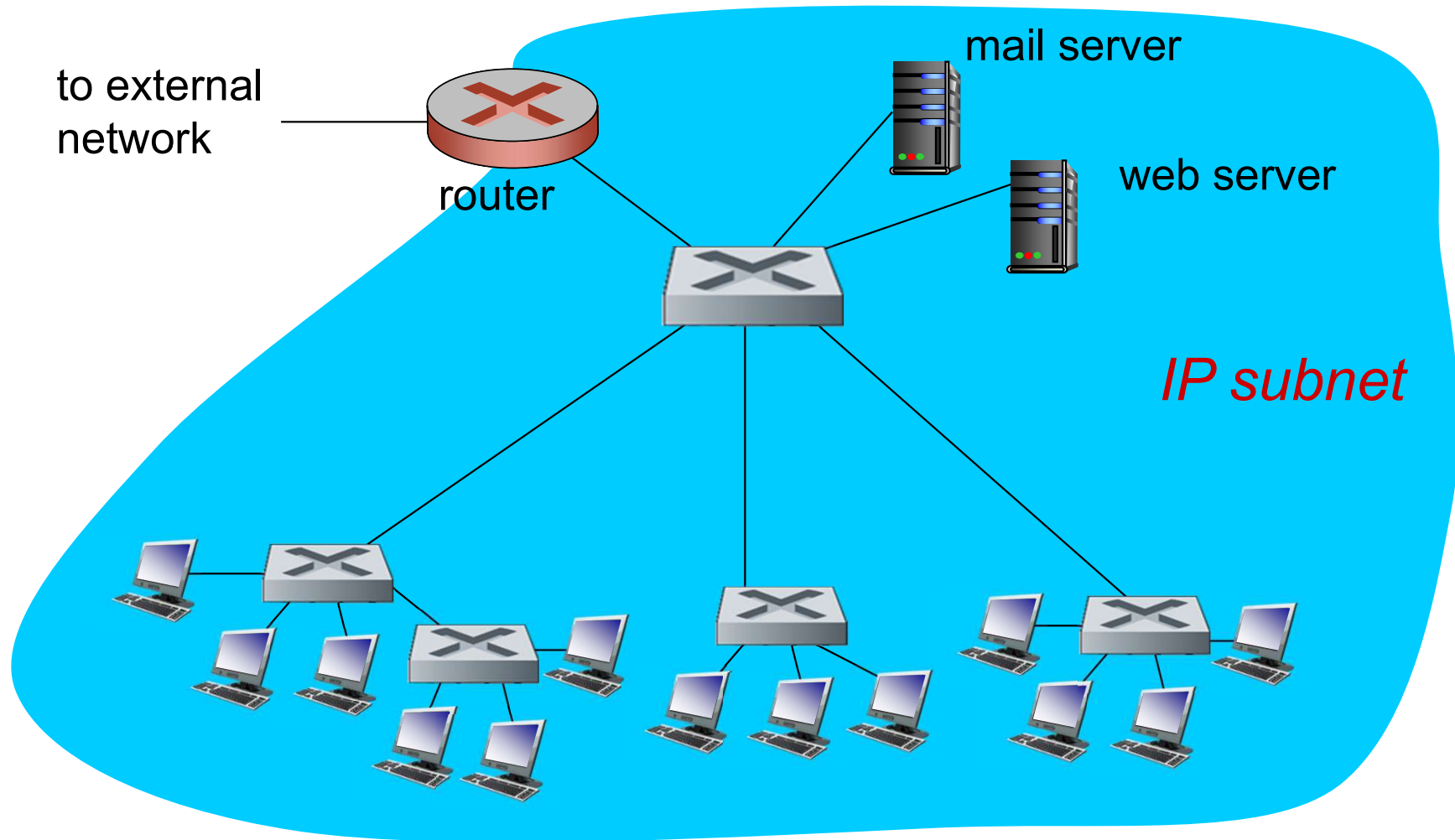


- Q: indicare le tabelle in S₁, S₂, S₃, S₄

Router

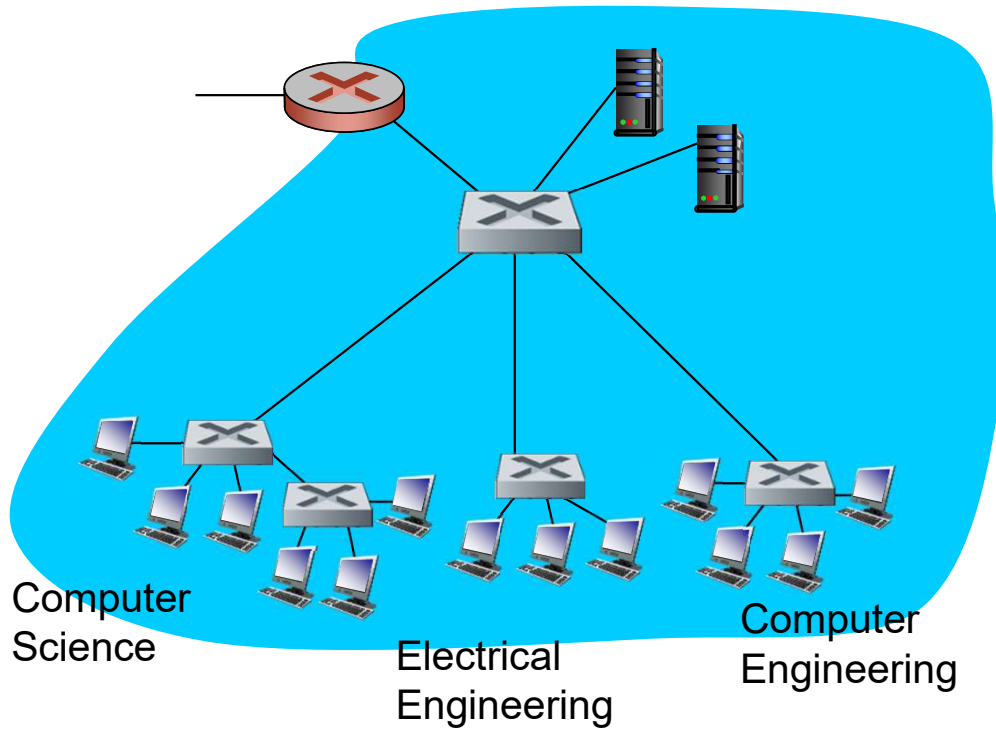
- Operano
 - Sia a livello fisico: rigenerando segnale
 - Sia a livello link: verificando indirizzi MAC contenuti in frame
 - Sia a livello network: verificando indirizzi IP
- Router \neq repeater e switch/hub
 1. Router hanno 1 indirizzo MAC e 1 indirizzo IP per ogni loro interfaccia
 2. Operano solo sui frame il cui indirizzo destinazione (link) è l'indirizzo (link) dell'interfaccia su cui arrivano
 3. Cambiano indirizzi link contenuti nei frame che inoltrano

Institutional network



VLAN

VLANs: motivation



consider:

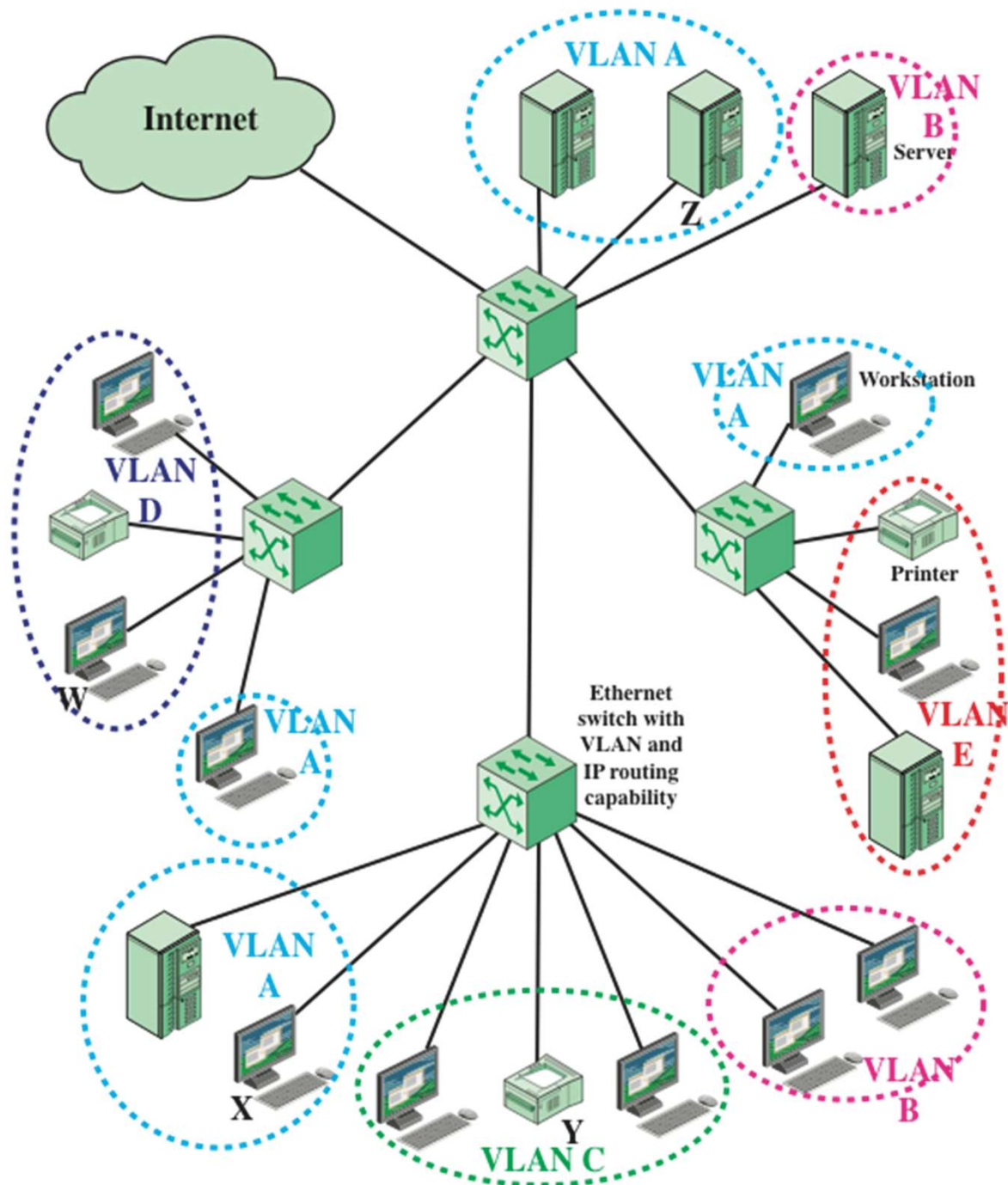
- single broadcast domain:
 - all layer-2 broadcast traffic (ARP, DHCP, unknown location of destination MAC address) must cross entire LAN
 - security/privacy, efficiency issues

Broadcast domain

- The total collection of devices that receive broadcast frames from each other is referred to as a **broadcast domain**.
- In molte situazioni, un frame di broadcast viene utilizzato per uno scopo, come la gestione della rete o la trasmissione di qualche tipo di avviso, con un'importanza relativamente locale.
- Se un frame broadcast contiene informazioni utili solo a un particolare reparto, la capacità di trasmissione viene sprecata sulle altre porzioni della LAN e sugli altri switch.

VLAN

- Una rete locale virtuale (VLAN) è un sottogruppo logico all'interno di una LAN creato dal software anziché spostando e separando fisicamente i dispositivi
- Riunisce le stazioni utente e i dispositivi di rete in un **unico dominio di broadcast, indipendentemente dal segmento fisico della LAN** a cui sono collegati, consentendo al traffico di fluire in modo più efficiente all'interno di popolazioni di interesse reciproco
- Gli host all'interno di una VLAN comunicano tra loro come se fossero tutti (e nessun altro) connessi allo switch
- La VLAN logica è implementata negli switch e funziona a livello MAC
- tali switch permette di definire più reti locali virtuali su una certa infrastruttura fisica
- Poiché l'obiettivo è isolare il traffico all'interno della VLAN, per collegarsi da una VLAN all'altra è necessario un router o uno switch a 3 livelli



- Le VLAN consentono a qualsiasi gruppo di essere fisicamente disperso in tutta l'azienda, pur mantenendo la propria identità di gruppo.
- Una trasmissione dalla stazione di lavoro X al server Z avviene all'interno della stessa VLAN.
- Un frame MAC broadcast da X viene trasmesso a tutti i dispositivi in tutte le porzioni della stessa VLAN.
- Ma una trasmissione da X alla stampante Y passa da una VLAN a un'altra. Di conseguenza, per spostare il pacchetto IP da X a Y è necessaria una logica di router a livello IP.
- lo switch determina se il frame MAC in arrivo è destinato a un altro dispositivo della stessa VLAN. In caso contrario, lo switch instrada il pacchetto a livello IP.

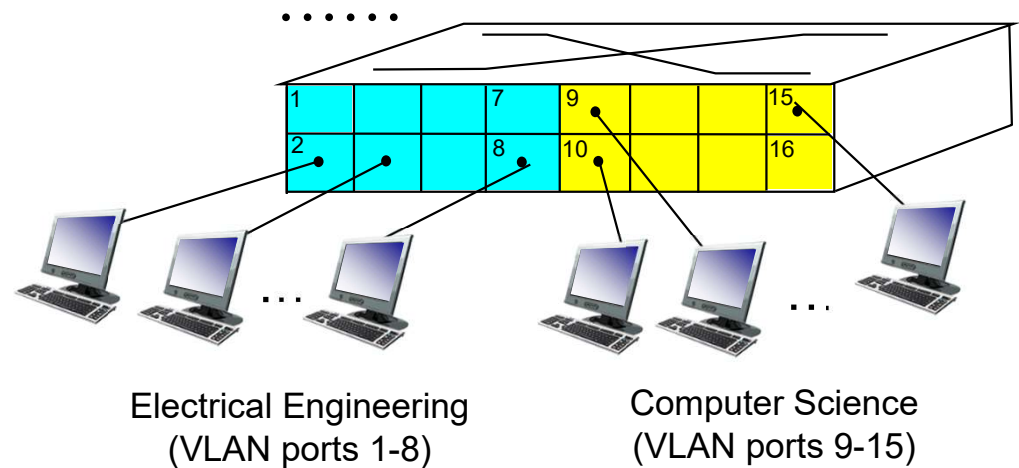
Figure 9.3 A VLAN Configuration

VLANs

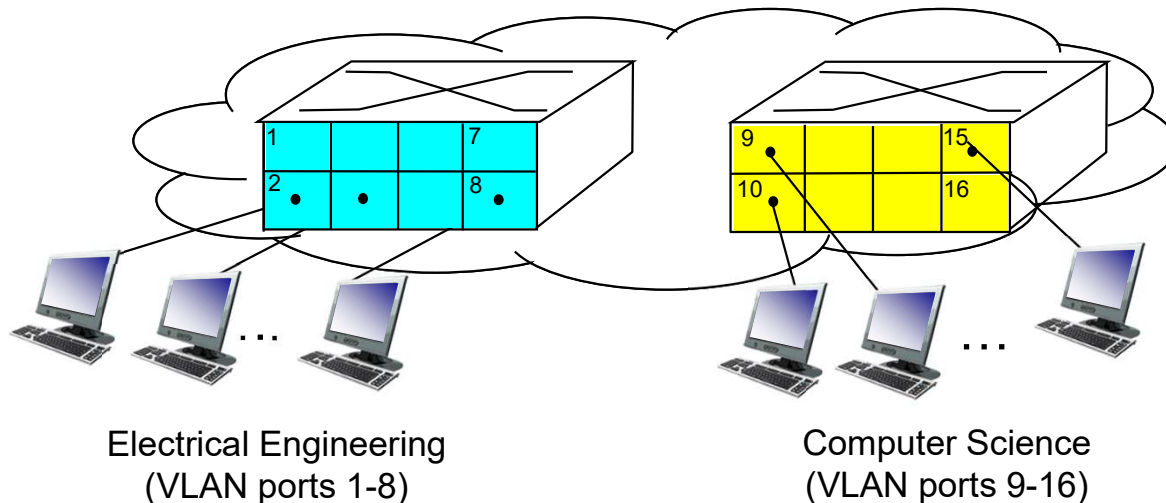
Virtual Local Area Network

switch(es) supporting VLAN capabilities can be configured to define multiple *virtual* LANS over single physical LAN infrastructure.


port-based VLAN: switch ports grouped (by switch management software) so that *single* physical switch

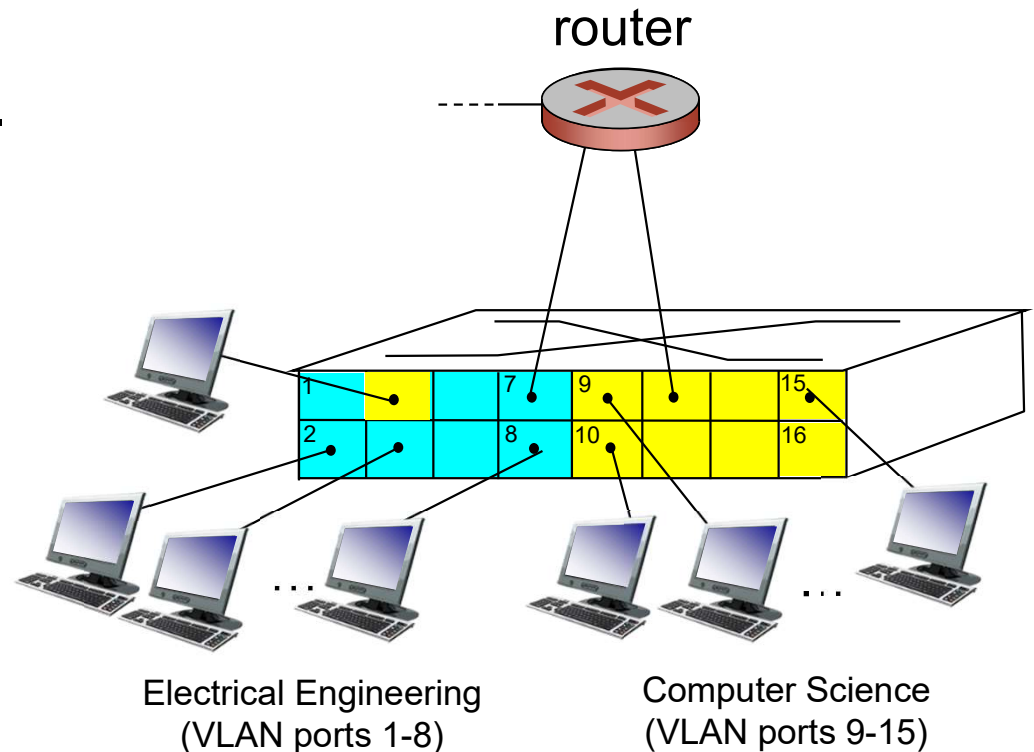


... operates as **multiple** virtual switches

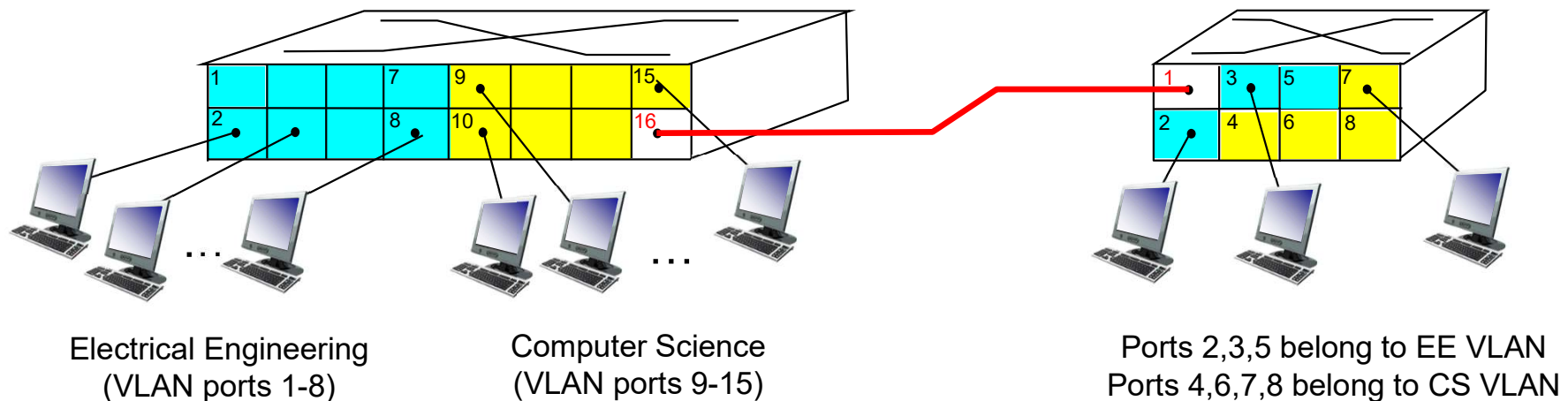


Port-based VLAN

- **traffic isolation:** frames to/from ports 1-8 can *only* reach ports 1-8
 - can also define VLAN based on MAC addresses of endpoints, rather than switch port
 - **dynamic membership:** ports can be dynamically assigned among VLANs
 - **forwarding between VLANs:** done via routing (just as with separate switches)
 - in practice vendors sell combined switches plus routers
- 

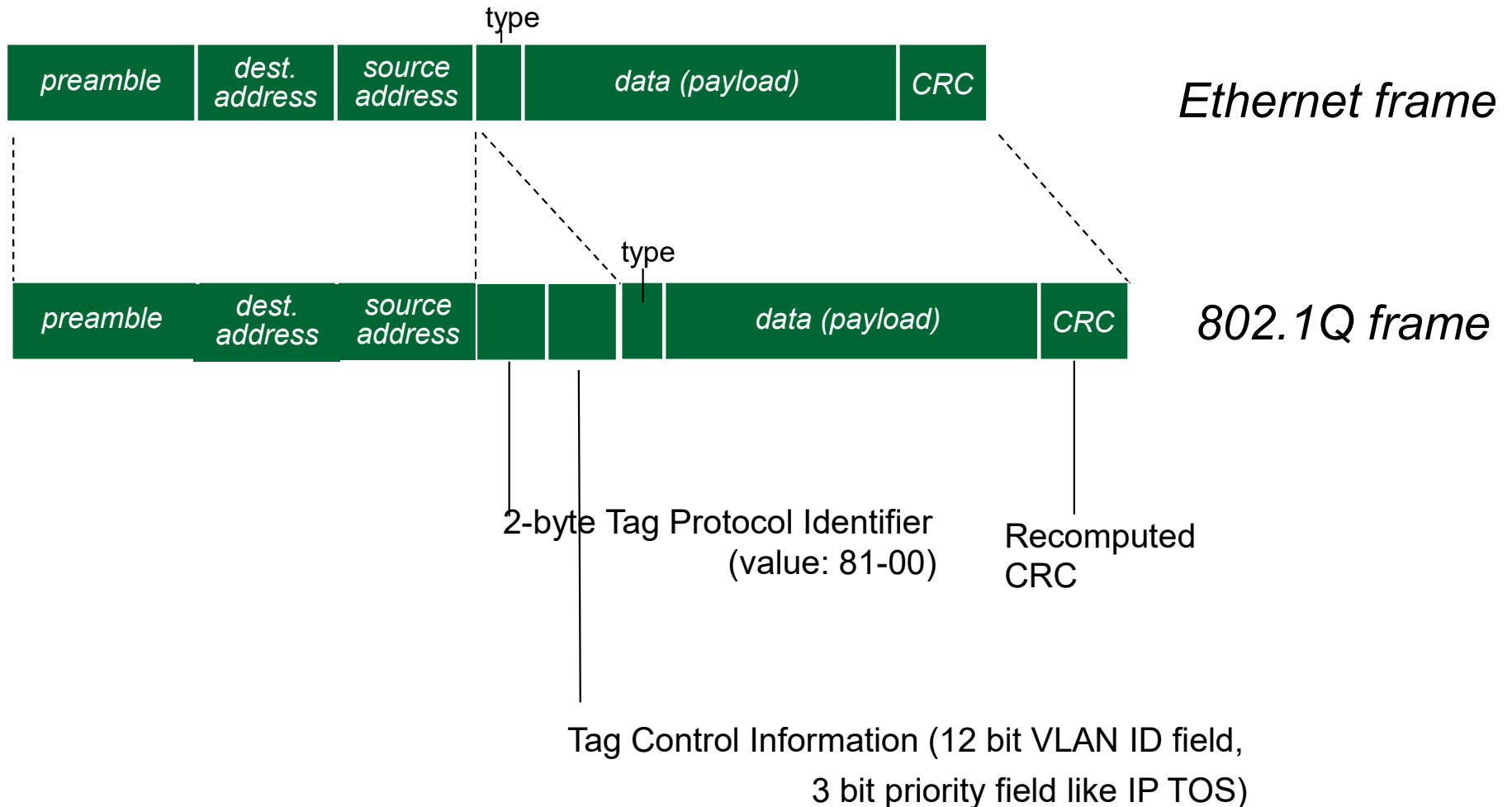


VLANs spanning multiple switches

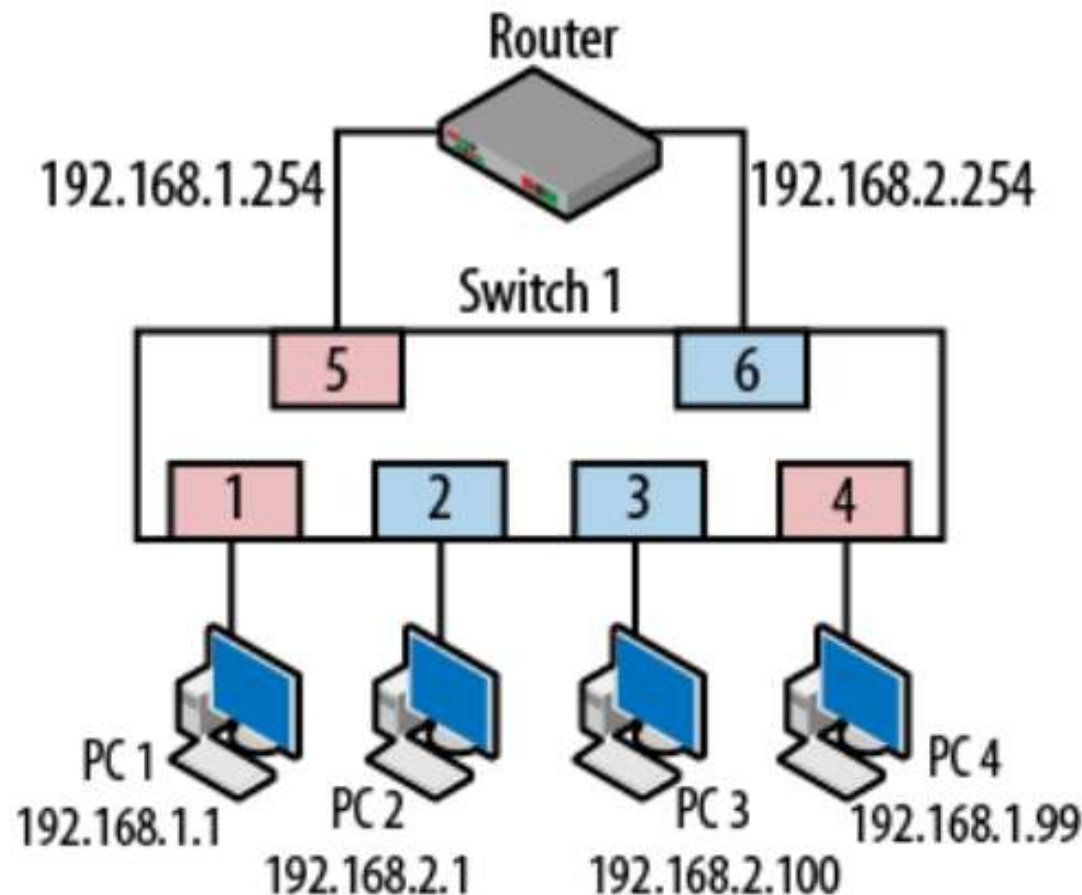


- **trunk port:** carries frames between VLANs defined over multiple physical switches
 - frames forwarded within VLAN between switches can't be vanilla 802.1 frames (must carry VLAN ID info)
 - 802.1q protocol adds/removed additional header fields for frames forwarded between trunk ports

802.1Q VLAN frame format



VLAN and subnets

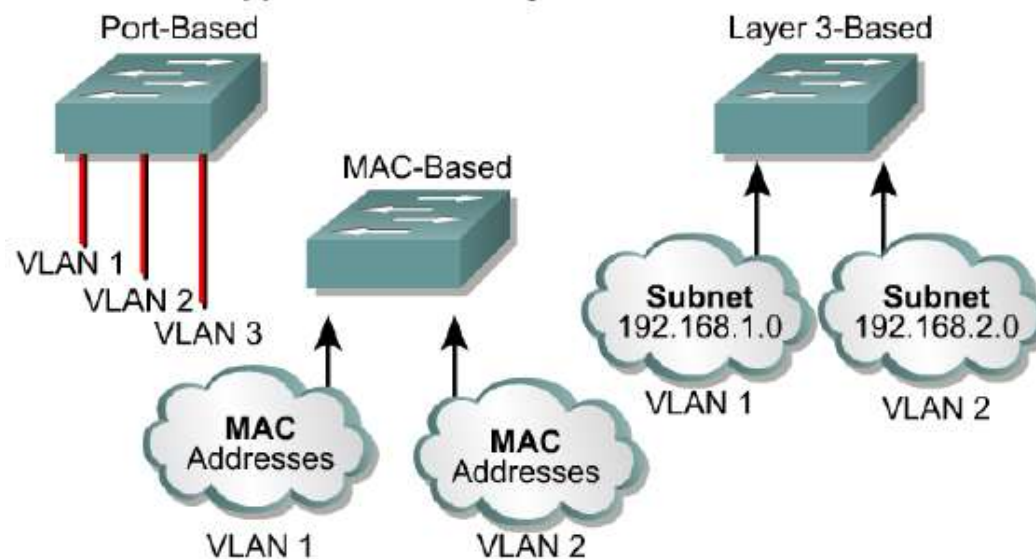


- PC1 and PC4 can communicate directly with each other
- but must use the router to get to PC2 and PC3.
- Frames issued on red VLAN 1 will not be seen by nodes on blue VLAN 2

The recommendation is to have: 1 VLAN = 1 IP subnet = 1 Broadcast Domain

Altri modi per definire VLAN

- Abbiamo visto port-based VLAN, ci sono altri criteri possibili, tra cui:
- VLAN basate sull'indirizzo MAC
 - il gestore di rete specifica un insieme di indirizzi MAC che appartengono a ciascuna VLAN; quando un dispositivo viene collegato a una porta, la porta viene associata alla VLAN appropriata sulla base dell'indirizzo MAC del dispositivo.
- VLAN definite sulla base dei protocolli a livello di rete (per esempio, IPv4, IPv6)

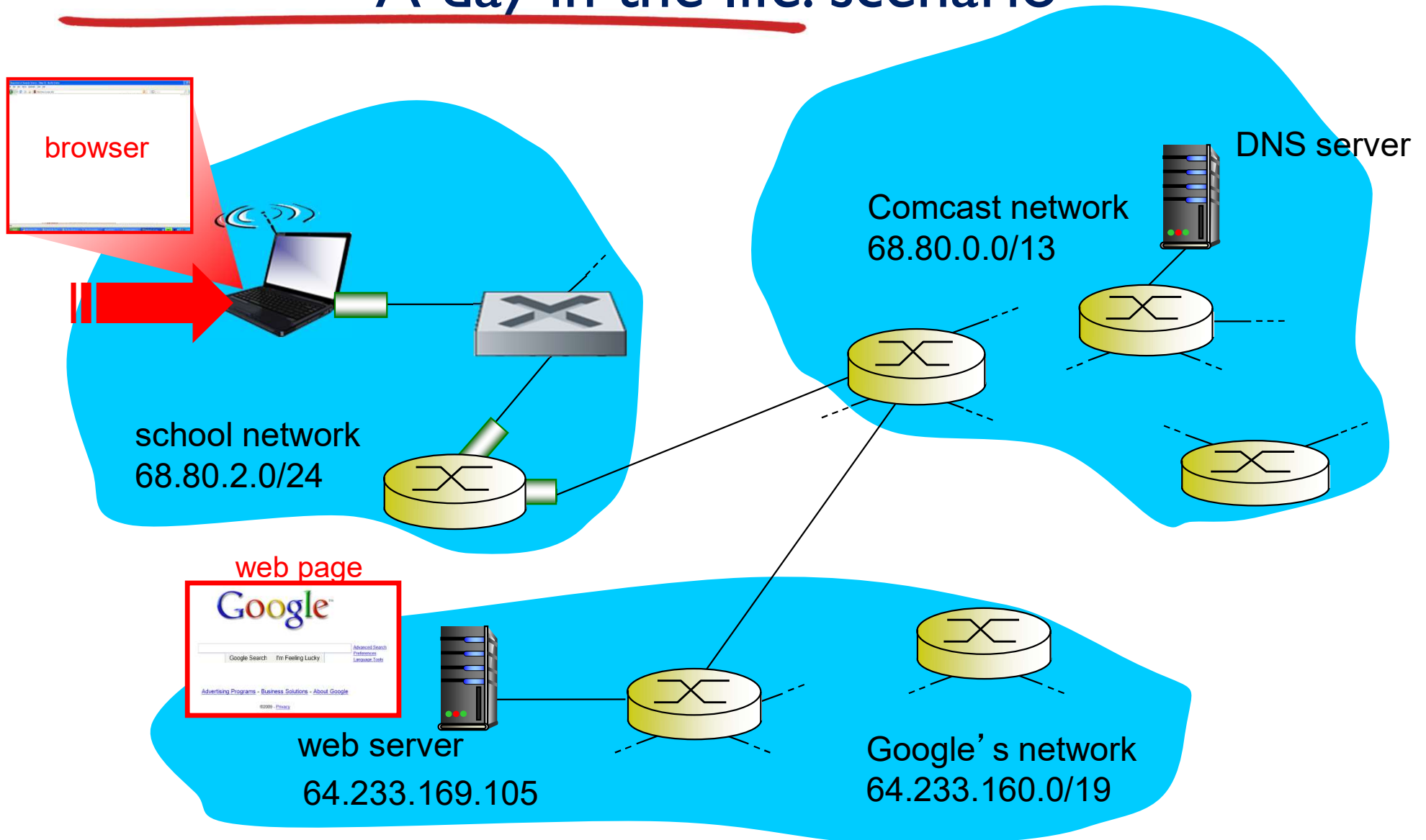


Synthesis: a day in the life of a web request

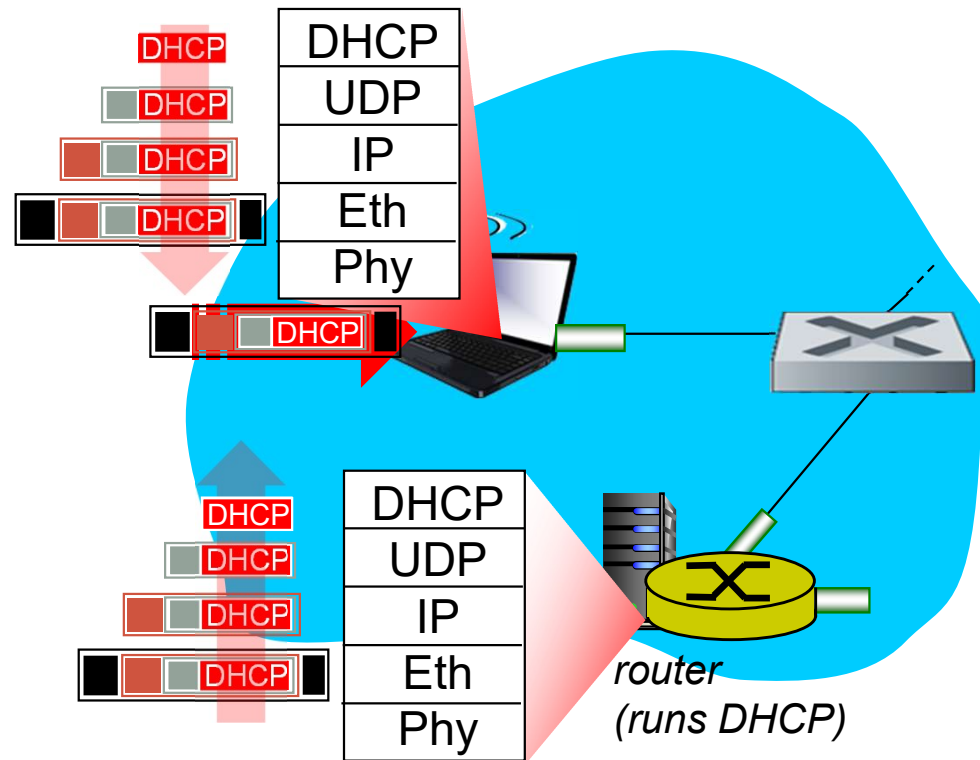
Synthesis: a day in the life of a web request

- journey down protocol stack complete!
 - application, transport, network, link
- putting-it-all-together: synthesis!
 - *goal*: identify, review, understand protocols (at all layers) involved in seemingly simple scenario: requesting www page
 - *scenario*: student attaches laptop to campus network, requests/receives www.google.com

A day in the life: scenario

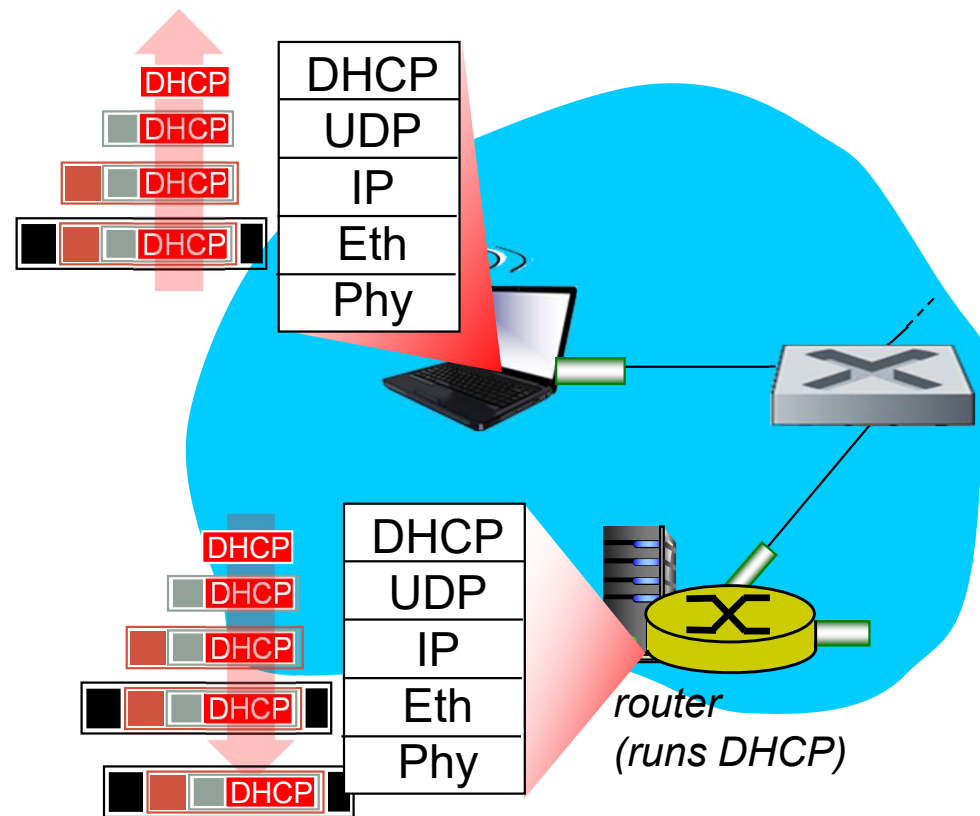


A day in the life... connecting to the Internet



- connecting laptop needs to get its own IP address, addr of first-hop router, addr of DNS server: use **DHCP**
- DHCP request **encapsulated** in **UDP**, encapsulated in **IP**, encapsulated in **802.3 Ethernet**
- Ethernet frame **broadcast** (dest: FFFFFFFFFFFFFFFF) on LAN, received at router running **DHCP** server
- Ethernet **demuxed** to IP demuxed, UDP demuxed to DHCP

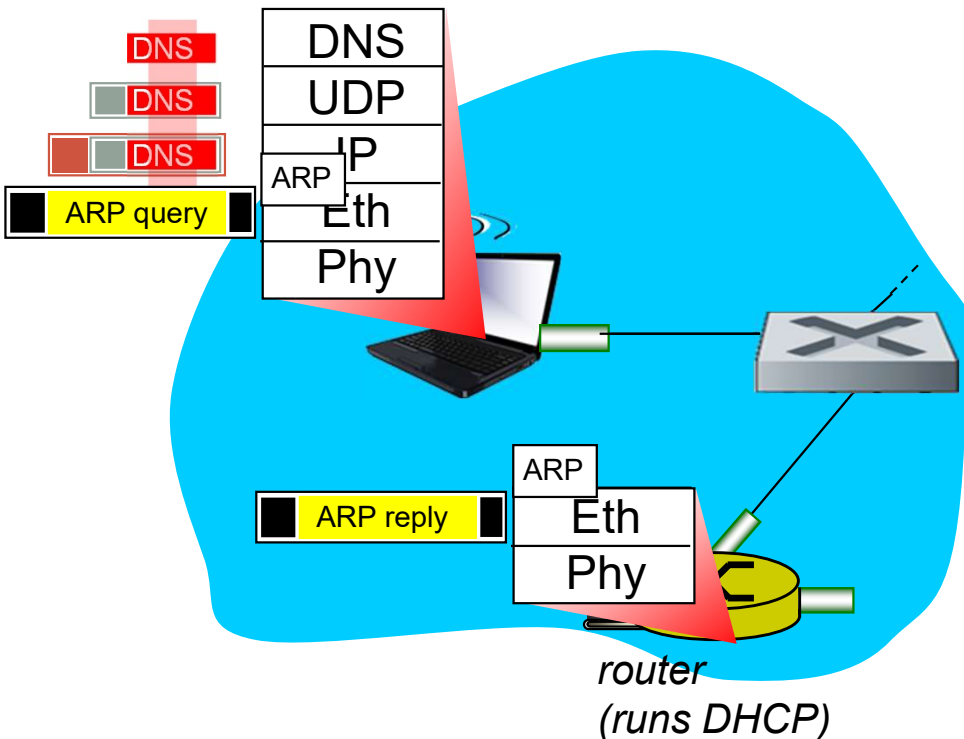
A day in the life... connecting to the Internet



- DHCP server formulates **DHCP ACK** containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server
 - encapsulation at DHCP server, frame forwarded (**switch learning**) through LAN, demultiplexing at client
 - DHCP client receives DHCP ACK reply

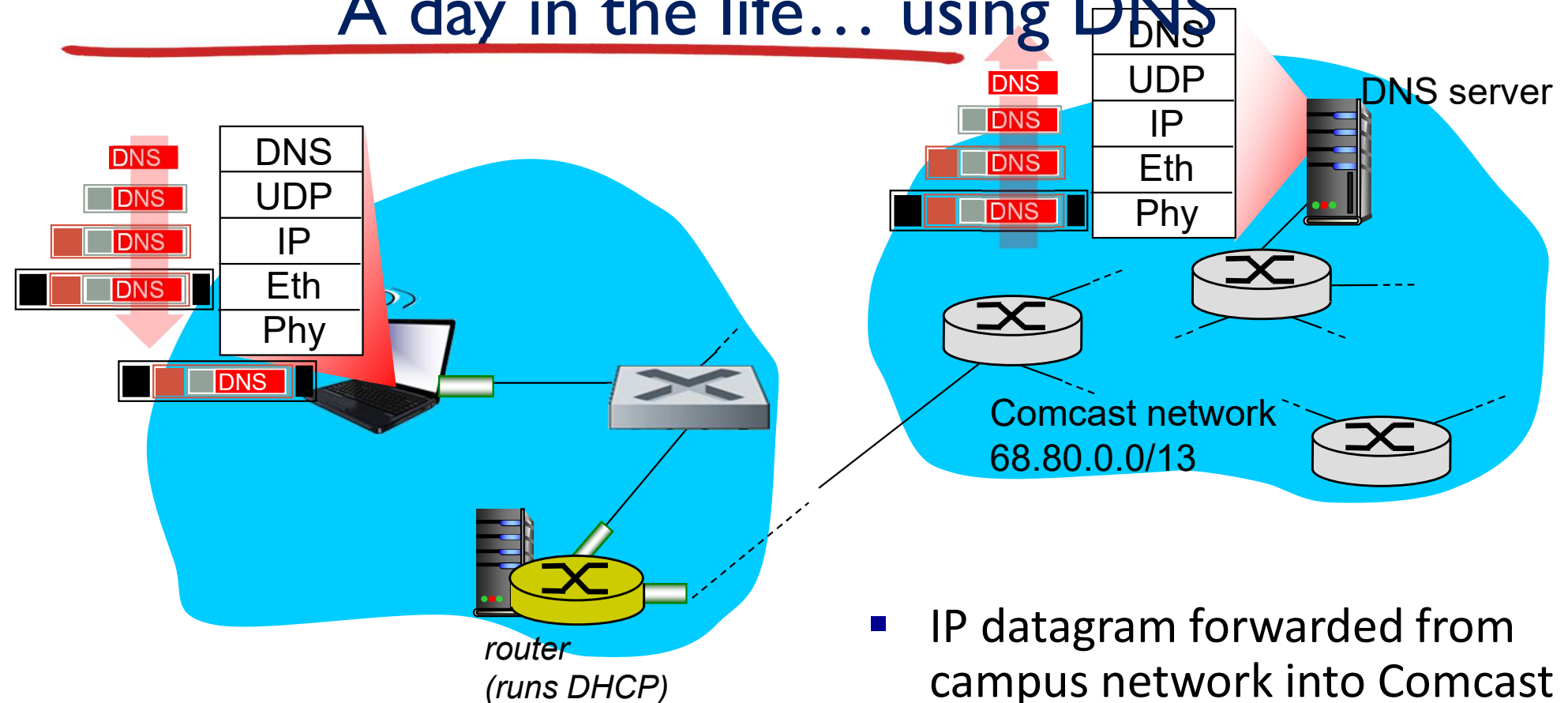
Client now has IP address, knows name & addr of DNS server, IP address of its first-hop router

A day in the life... ARP (before DNS, before HTTP)



- before sending *HTTP* request, need IP address of `www.google.com`:
DNS
- DNS query created, encapsulated in UDP, encapsulated in IP, encapsulated in Eth. To send frame to router, need MAC address of router interface: *ARP*
- *ARP query* broadcast, received by router, which replies with *ARP reply* giving MAC address of router interface
- client now knows MAC address of first hop router, so can now send frame containing DNS query

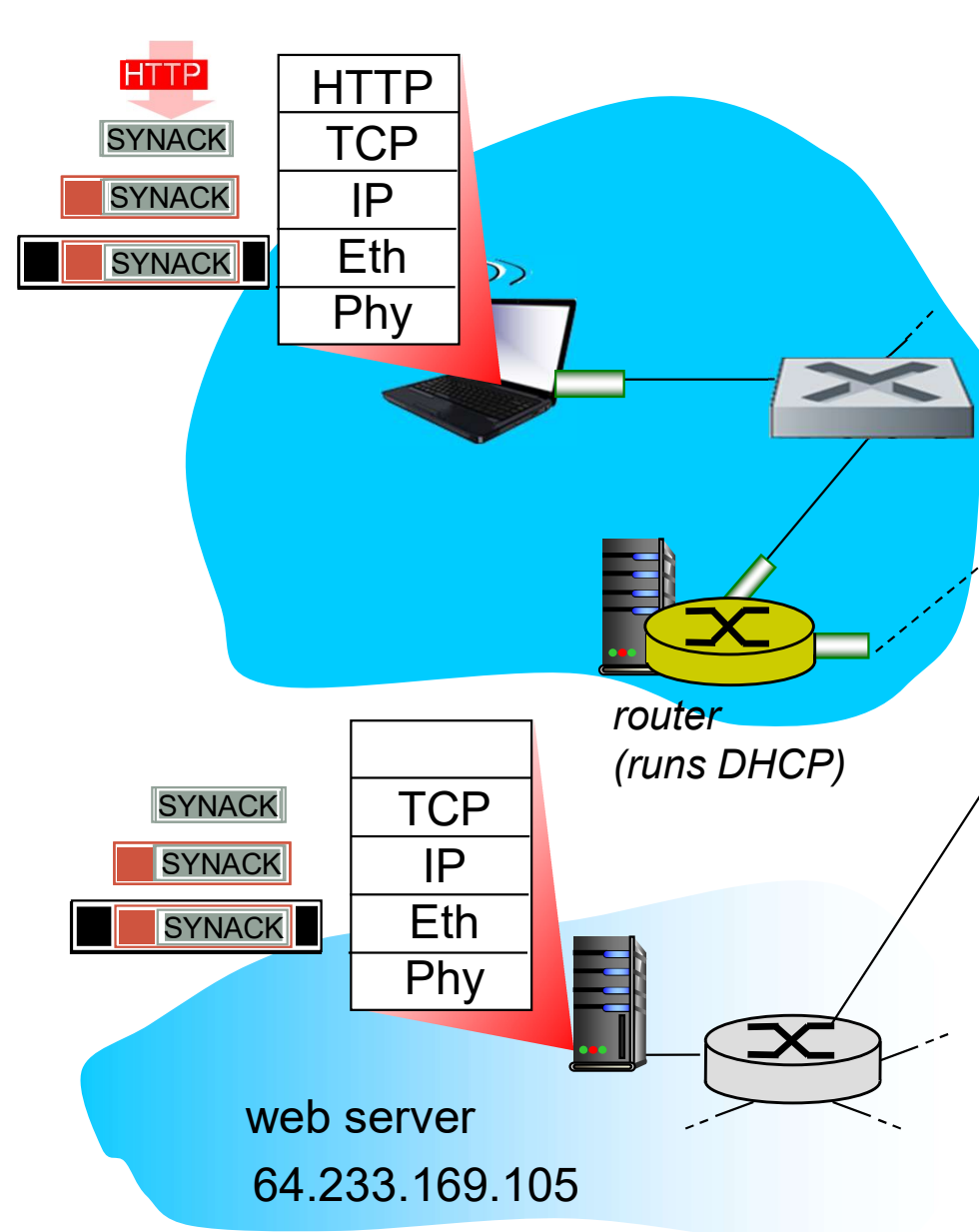
A day in the life... using DNS



- IP datagram containing DNS query forwarded via LAN switch from client to 1st hop router

- IP datagram forwarded from campus network into Comcast network, routed (tables created by **RIP**, **OSPF**, **IS-IS** and/or **BGP** routing protocols) to DNS server
- demuxed to DNS server
- DNS server replies to client with IP address of www.google.com

A day in the life...TCP connection carrying HTTP



- to send HTTP request, client first opens **TCP socket** to web server
- TCP **SYN segment** (step 1 in 3-way handshake) inter-domain routed to web server
- web server responds with **TCP SYNACK** (step 2 in 3-way handshake)
- TCP **connection established!**

A day in the life... HTTP request/reply

- web page **finally (!!!)** displayed

