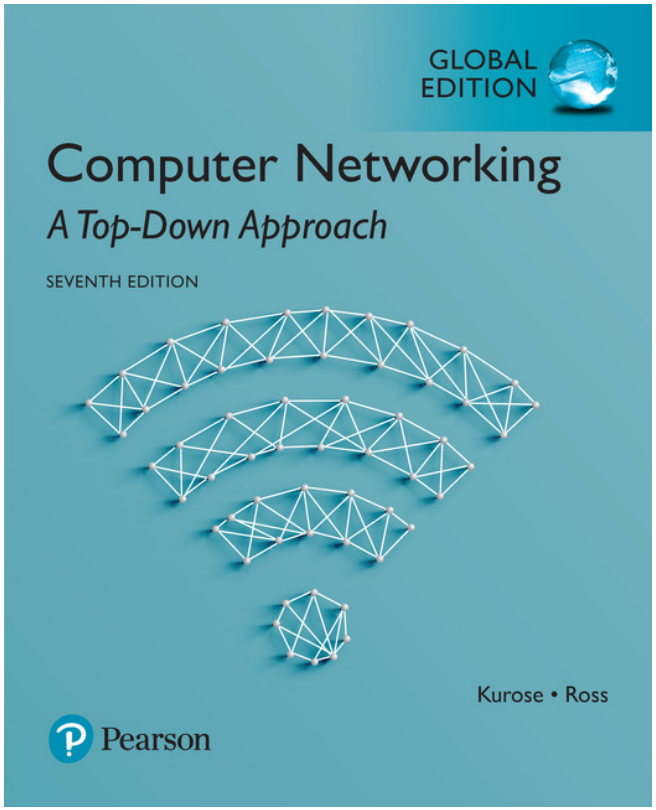
Chapter 6
Lotura Geruza eta LANak



Computer Networking: A Top Down Approach

7th Edition, Global Edition
Jim Kurose, Keith Ross
Pearson
April 2016

A note on the use of these Powerpoint slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

Chapter 6: Lotura geruza eta LANak

Helburuak:

- Lotura geruzak ezartzen dituen zerbitzuak ulertzea:
  - Akatsen detekzioa eta zuzenketa
  - Broadcast kanal baten erabilpena: atxipen anitzak
  - Lotura geruzaren helbideen esleipena
  - LAN, local area networks: Ethernet, VLANs
- Lotura geruzarako teknologia desberdin ulertzea

Link layer, LANs: outline

6.1 Sarrera, zerbitzuak

6.2 Akats detekzioa, zuzenketa

6.3 Atzipen anitzeko protokoloak, multiple access protocols

6.4 LAN-ak

- Helbideen esleipena, ARP
- Ethernet
- switches
- VLANS

6.5 Loturen birtualizazioa: MPLS

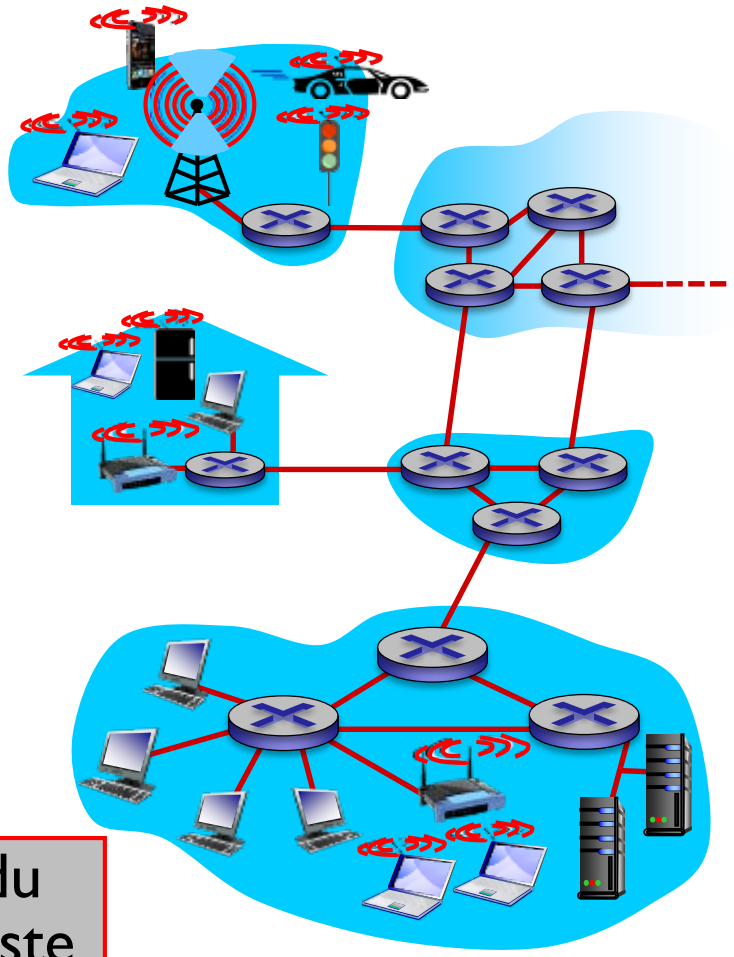
6.6 data center networking

6.7 a day in the life of a web request

Link layer: sarrera

terminologia:

- hosts eta routers: nodoak
- Komunikazio bidean, komunikazio nodoak batzen dituzten komunikazio kanalak: link, medioa
  - Hari bidezko loturak
  - Haririk gabeko loturak
  - LAN-ak
- 2. geruzako paketea: frame/trama, datagrama kapsulatzen du

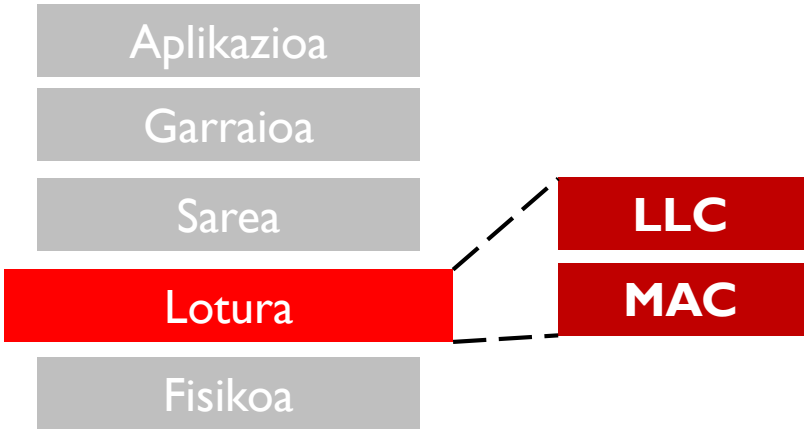


Lotura geruzak datagrama garraiatzen du nodo batetik *fisikoki ondoan* dagoen beste Batera, *link*, kanal bat erabiliz

Link layer: sarrera

Oinarrizko bi zerbitzu:

- Goiko geruzek bide fisikora duten bidea ziurtatzen du
- Link, medioen bidez datuak nola garraiatzen diren kontrolatzen du. Hau egiteko *link-ekiko atziþen kontrola* eta *akatsen antzemate teknikak* erabiltzen dira



***LLC-** Logical Link Control:*

Komunikazioa goiko geruzekin ahalbidetzen du

***MAC** - Media Access Control:*

Datu bitarrak zer host-era bideratuko den partekatutako medio batean erabakitzen duen protokoloa

Link layer: testuingurua

- Datagrama garraiatzen da medio desberdin gainean eta protokolo desberdinak erabilita:
  - e.g., Ethernet lehen loturan, frame relay tarteko nodoetan, 802.11 azkenean
- Lotura protokolo bakoitzak zerbitzu desberdinak inplementatzen ditu

transportation analogy:

- trip from Princeton to Lausanne
  - limo: Princeton to JFK
  - plane: JFK to Geneva
  - train: Geneva to Lausanne
- tourist = datagram
- transport segment = communication link
- transportation mode = link layer protocol
- travel agent = routing algorithm

Link layer zerbitzuak

Eskeinitako zerbitzuak (denak ez dira beharrezkoak)

- *framing, link access:*
  - Datagrama frame/trama batean kapsulatzen du, goiburua gehituz
  - Atzipen kanalera, partekatutako medio badago
  - "MAC" helbideak erabiltzen dira trametan iturria eta helmuga identifikatzeko
    - EZ dira IP helbideak!
- *Garraio fidagarria ondoko nodoen artean*
  - Garraio mailan ere ziurtatzen zen!
  - Sarritan erabiltzen da akats gutxiko medio-etan (fiber, some twisted pair)
  - Haririk gabeko loturetan: Akats ratio handiago
    - *Q:* Zergatik eskatzen da fidagarritasuna lotura mailan eta garraio mailan?

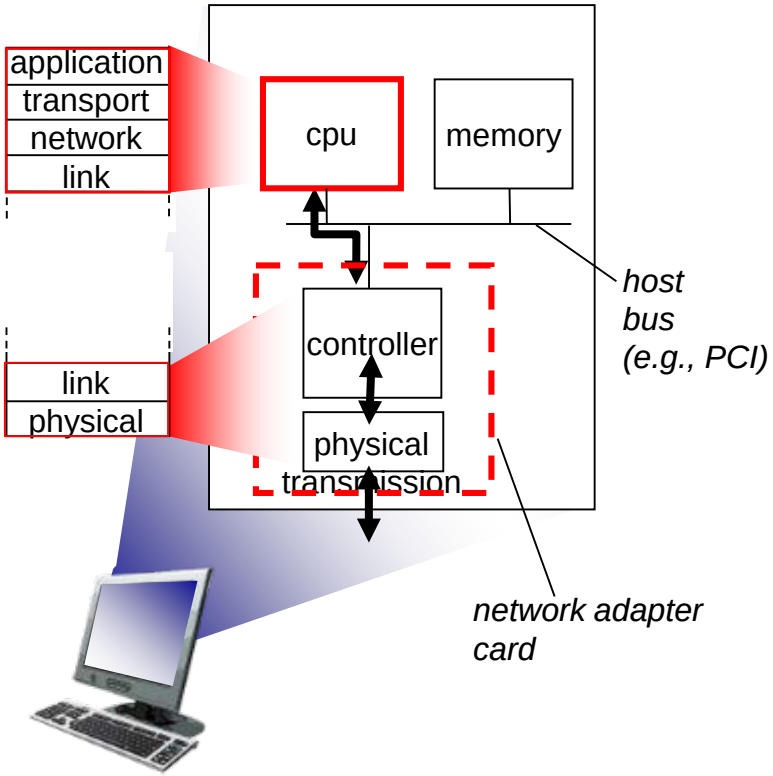
Link layer zerbitzuak (gehiago)

- *Fluxu kontrola:*
  - Elkarren ondoko nodoen arteko bidalketa abiaduraren kontrola
- *Akats antzemate:*
  - Seinalearen gutxipena edo zarata.
  - Jasotzaileak akatsak detektatzen ditu:
    - Igorleari abisatzen dio edo trama baztertzen du
- *Akats zuzenketa:*
  - Jasotzaileak bit-akatsak antzematen eta zuzentzen ditu, berbidalketa eskatu barik
- *Half-duplex eta full-duplex*
  - half duplex-ekin, bi aldetako nodoek informazioa bidal dezakete, baina ez aldiberean

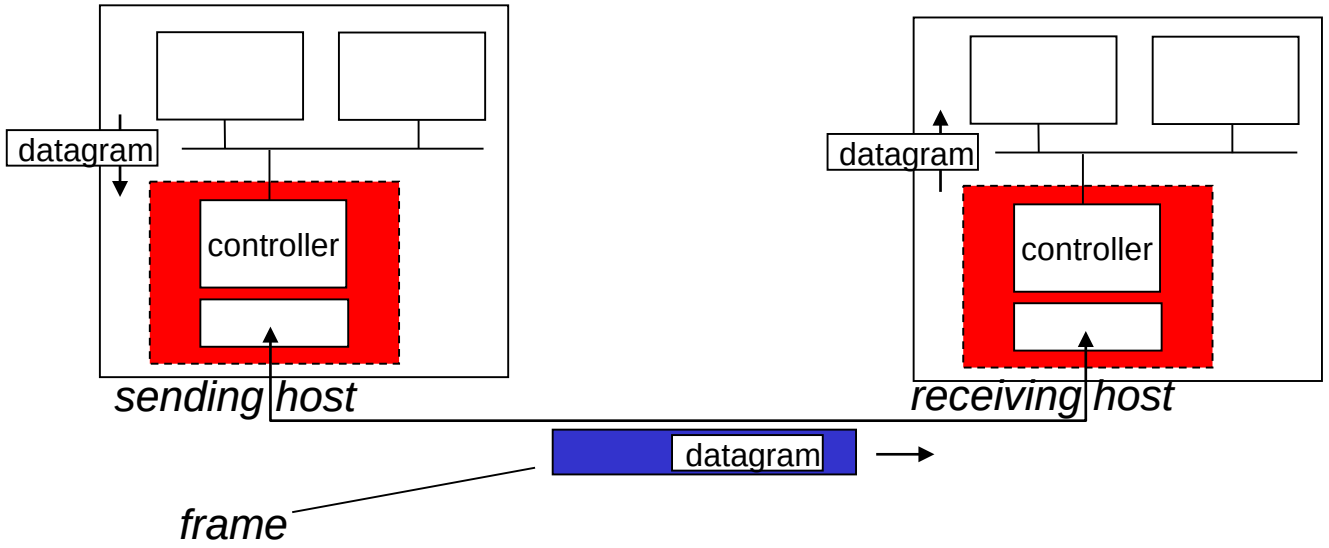
Funtzio gehienak ekipoen hardwarean inplementatzen dira

Non inplementatzen da lotura geruza?

- Host guztietan
- Adaptadorean inplementatzen da (aka *Network Interface Card* NIC) edo txip batean
  - Ethernet card, 802.11 card; Ethernet chipset
  - implements link, physical layer
- Host-aren sistemaren busetan gehituta
- hardware, software eta firmware nahasketa



Komunikazioa



- Igorleak:
  - Datagrama trametan kapsulatzen du
  - error checking bits, rdt, flow control, etc gehitzen du.
- Jasotzaileak
  - akatsak, rdt, flow control, etc. gainbegiratzen ditu
  - Datagramak ateratzen ditu eta jasotzaileren goiko geruzara pasatzen ditu

Link layer, LANs: outline

6.1 Sarrera, zerbitzuak

6.2 Akats detekzioa, zuzenketa

6.3 Atzipen anitzeko protokoloak, multiple access protocols

6.4 LAN-ak

- Helbideen esleipena, ARP
- Ethernet
- switches
- VLANS

6.5 Loturen birtualizazioa: MPLS

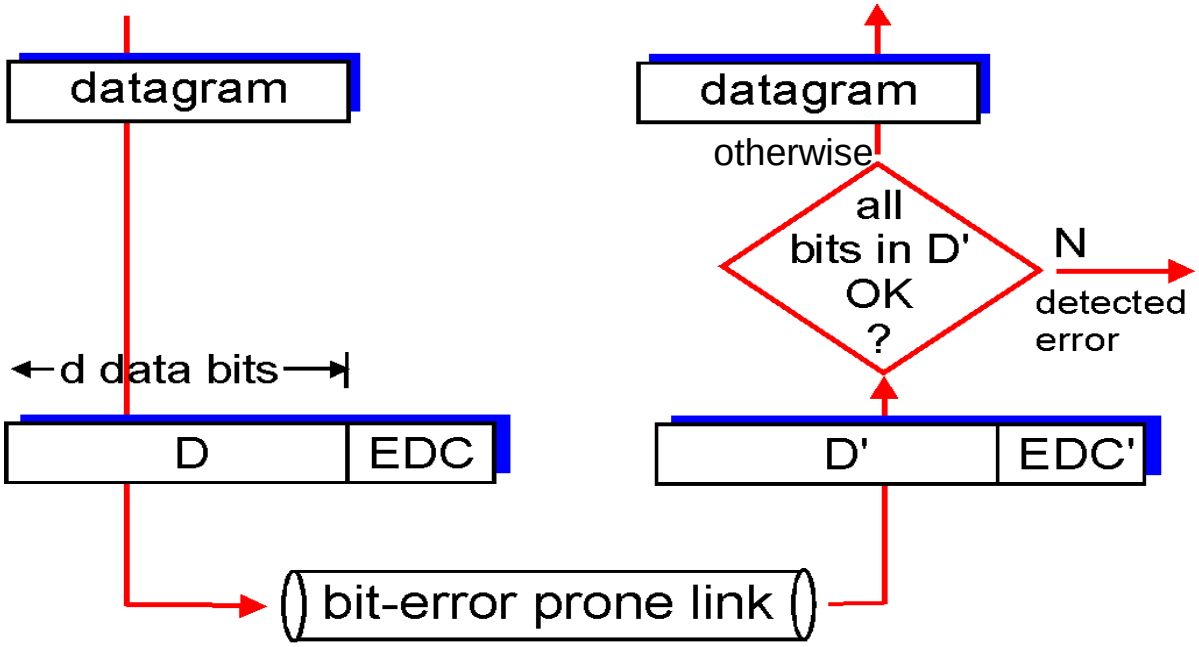
6.6 data center networking

6.7 a day in the life of a web request

Akats antzemate

EDC= Error Detection and Correction bits (redundancy)
D = Data protected by error checking, may include header fields

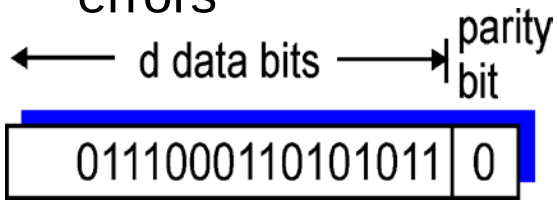
- Akats detekzioa ez da erabat (% 100) fidagarria!
  - protokoloak akats batsuk gal ditzake, oso gutxitan
  - EDC eremu luzeagoek antzemate eta zuzenketa errazten ditu



Paritatearen kudeaketa

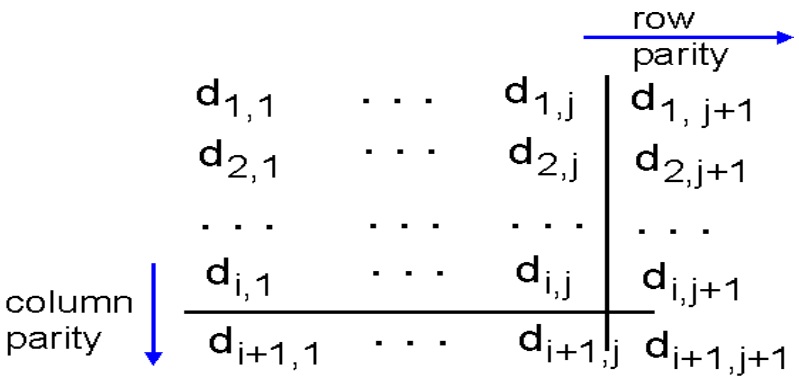
Bit bakarreko paritatea:

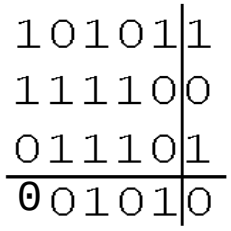
- detect single bit errors



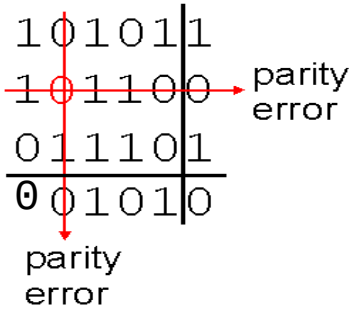
Bi dimentsiotako bit paritatea:

- detect and correct single bit errors





no errors



correctable single bit error

* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

Internet checksum (review)

Helburua: "Akatsak" antzematea (e.g., flipped bits) garraiatutako paketeetan (oharra: **garraio** mailan erabiltzen da). Software bidez inplementatzen da eta arina izan behar du

Igorlea:

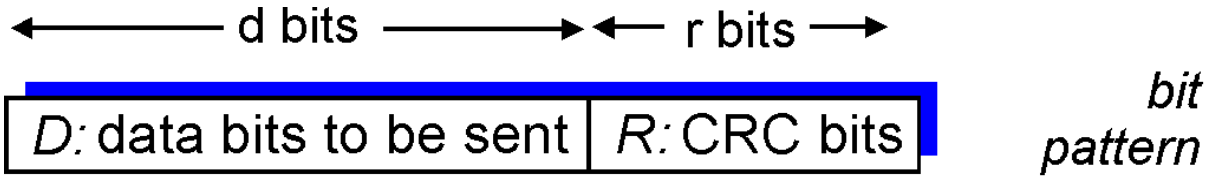
- Segmentuaren informazioa baieztatzen da 16 bit-eko eremu batean
- checksum: segmentuaren informazioaren batuketa (1's complement sum)
- Igorleak, checksumaren balioa dagokion eremuan jartzen du (UDP, TCP)

Jasotzaileak:

- Jasotako segmentuaren checksuma kalkulatzen du
- Checksum eremuan agertzen denarekin alderatzen du. Berdinak dira?
  - EZ - Akatsa
  - BAI – Ez da akatsik detektatu. *Baina egon litezke*

Cyclic redundancy check

- Normalean hardware bidez
- Aurrekoa baino teknika sendoago
- Informazioa, D zenbaki bitarra, polinomio bezala hartzen da
- igorleak eta jasotzaileak r+1 biteko patroi aukeratzen dute (generator), G (estandarretan definituta)
- Helburua: aukeratu r CRC bits, R, non
  - <D,R> exactly divisible by G (bitarrez) (hondarrik ez)
  - Jasotzaileak G ezagutzen du, zatiketa egiten du <D,R> zati G. Ondarra zero ez bada: AKATSA!
  - r+1 erratutako bit-ak baino txikiago diren akatsak antzematen ditu
- Erabilera zabala (Ethernet, 802.11 WiFi, ATM)



$D * 2^r \quad \text{XOR} \quad R$ — *mathematical formula*

CRC adibidea

want:

$D \cdot 2^r$ XOR R = nG

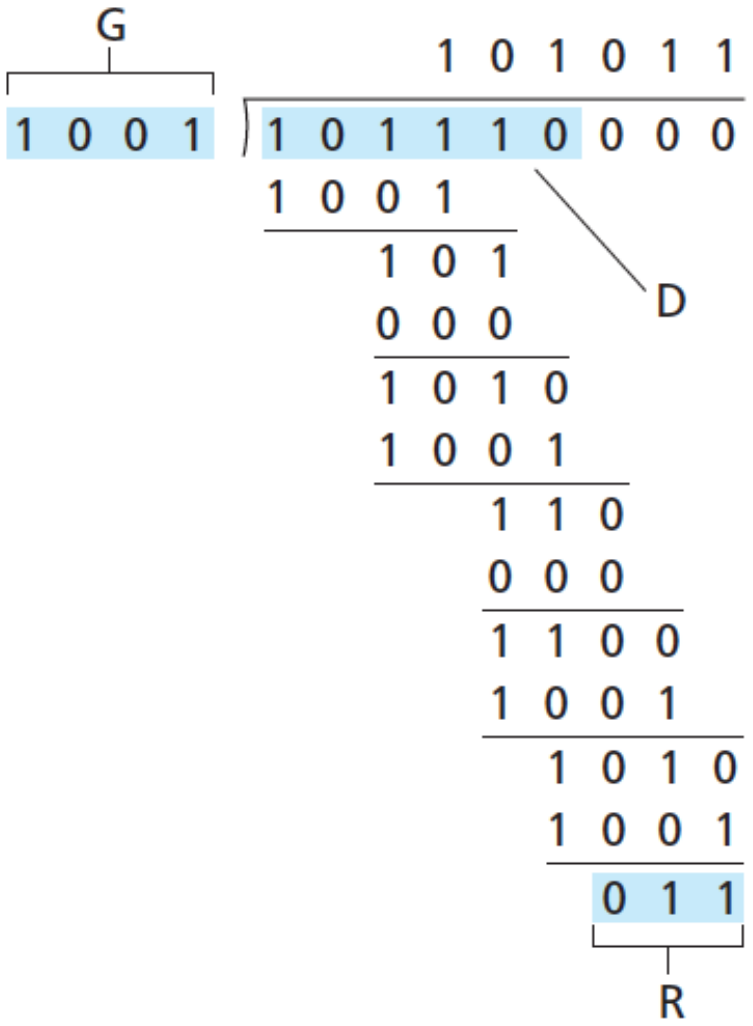
equivalently:

$D \cdot 2^r$ = nG XOR R

equivalently:

if we divide $D \cdot 2^r$ by G, want remainder R to satisfy:

$$R = remainder\left[\frac{D \cdot 2^r}{G}\right]$$



* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

Link layer, LANs: outline

6.1 Sarrera, zerbitzuak

6.2 Akats detekzioa, zuzenketa

6.3 Atzipen anitzeko protokoloak, multiple access protocols

6.4 LAN-ak

- Helbideen esleipena, ARP
- Ethernet
- switches
- VLANS

6.5 Loturen birtualizazioa: MPLS

6.6 data center networking

6.7 a day in the life of a web request

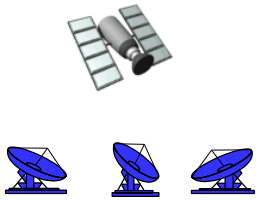
Atzipen anitzeko linkak, protokoloak

Bi motako “links”:

- point-to-point
  - PPP for dial-up access
  - point-to-point link swicht eta host artean
- *broadcast (shared wire or medium)*
  - old-fashioned Ethernet: partekatutako haria
  - upstream HFC
  - 802.11 wireless LAN

shared wire (e.g., cabled Ethernet)

shared RF (e.g., 802.11 WiFi)



shared RF (satellite)

humans at a cocktail party (shared air, acoustical)

Atzipen anitzeko protokoloak

- Erabiltzaile guztien artean partekatutako kanal bakarra
- Bi transmisio edo gehiago batera -> Interferentziak
  - *Collision/Talka* nodoak seinale bat baino gehiago jasotzen duenean

multiple access protocol

- Kanala nola erabiltzen den agintzen duen algoritmo banandua erabiltzen da. Ad: nodo batek noiz bidal dezakeen informazioa
- Kanalaren egoerari buruzko informazioa kanalean igortzen da
  - Ez dago kanpoko beste kanalik informazioa bidalketa koordinatzeko

Atzipen anitzeko protokolo ideala

Emanda: broadcast kanala, R bps abiadura duena (rate)

Bilatzen da:

1. Nodo batek informazioa igorri nahi duenean, R ratioan bidal dezake
2. M nodoek informazioa igorri nahi dutenean, bakoitzak R/M abiaduran bidal dezake
3. Erabat deszentralizatuta:
   - Kode berezirik gabe transmisioak kudeatzeko
   - Erlojuen sinkronizaziorik gabe
4. Erreza

MAC protocols: taxonomy

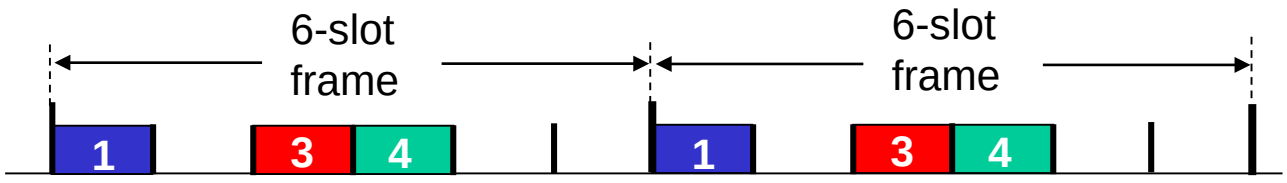
Hiru mota nagusi:

- *Kanalaren banaketa*
  - Kanala **zati** txikiagoetan banatzen da (time slots, frequency, code)
  - **Zatia**k nodoei esleitzen zaizkie
- *Ausazko atziþena*
  - Kanala ez da banatzen, talkak onartzen dira
  - Kolisioen kudeaketa eta berreskurapena tratatu behar da
- *"Txandak hartu"*
  - Nodoek txandak hartzen dituzte, baina gehiago bidali behar dutenek txanda luzeagoak hartuko dituzte

Kanalaren banaketa: TDMA

TDMA: Time Division Multiple Access

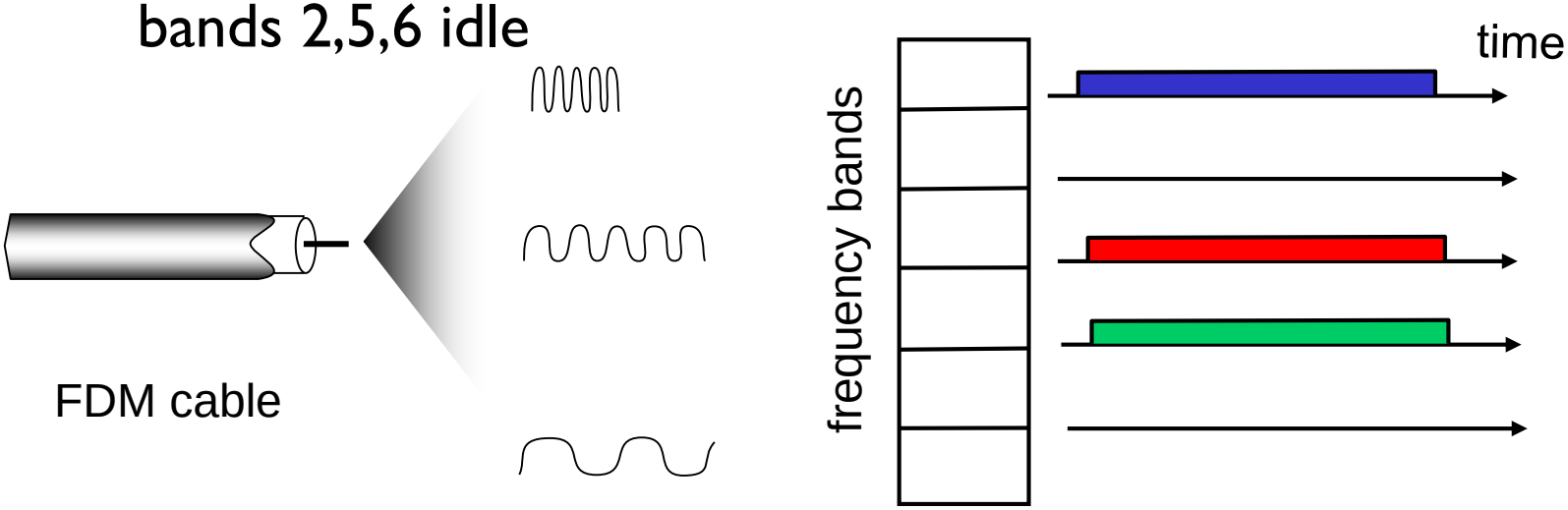
- Txandaka atzitzen da kanala
- Transmisio bakoitzak aurredefinitutako luzera batekoa
- Erabiltzen ez diren txandak, hutsik dihoazte
- example: 6-station LAN, 1,3,4 have packets to send, slots 2,5,6 idle



Kanalaren banaketa: FDMA

FDMA: Frequency Division Multiple Access

- Kanalaren espektroa maiztasun banda desberdinetan banatzen da
- Igorle bakoitzak, maiztasun tarte bat esleituta dauka
- Igorleak erabiltzen ez duenean, maiztasun tarte hori hutsik geratzen da
- example: 6-station LAN, 1,3,4 have packet to send, frequency bands 2,5,6 idle



Ausazko atzipena

- Nodoak pakete bat bidali behar duenean
  - Kanal osoa erabiltzen du informazioa transmititzeko, R ratioan.
  - *a priori*, ez dago nodoen arteko koordinaziorik
- Bi nodo batera igortzen dutenean → "collision/talka"
- random access MAC protocol honakoak espezifikatzen ditu:
  - Talkak nola detektatu
  - Nola berreskuratu informazioa kolisioak eta gero (e.g., via delayed retransmissions)
- Random access MAC protocols:
  - slotted ALOHA
  - ALOHA
  - CSMA, CSMA/CD, CSMA/CA

Slotted ALOHA

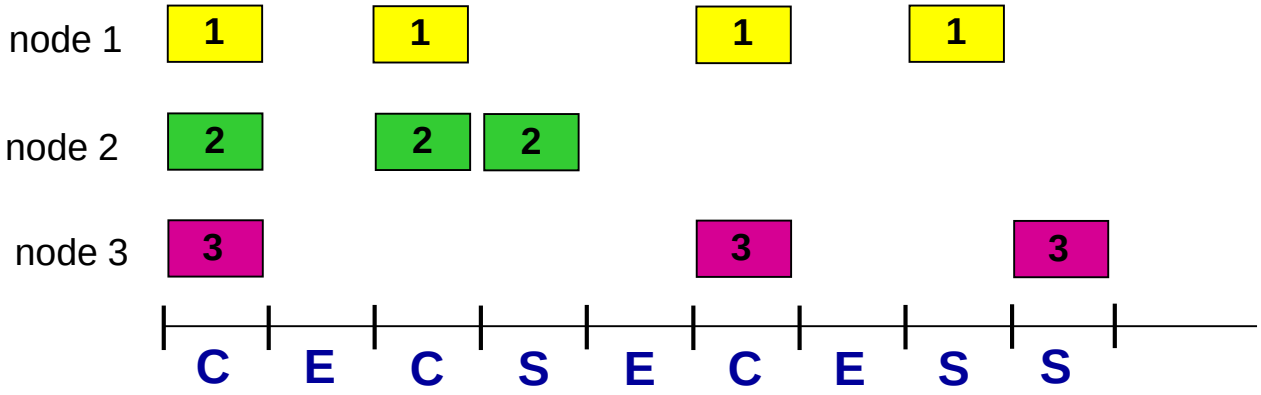
Onartzen da:

- Tamaina bereko tramak
- Denbora tarte berdinak (**slot**) transmisiorako (denbora tarte batean trama bat bidaltzen da)
- Nodoek transmititzen dute tarteen hasieran bakarrik
- Nodoak sinkronizatuta daude
- Talka gertatzen denean, nodo guztiek detektatzen dute

Operazioa:

- Nodo batek informazioa igorri behar duenean, hurrengo **slotean** igortzen du
  - *Talkarik ez badago:* Trama ondo transmititu da. Nodoak trama berria igor dezake hurrengo slotean
  - *Talka badago:* debora bat pasa eta gero, nodoak trama igorriko du berriz

Slotted ALOHA



Pros:

- Nodo bakarra dagoenean, kanal osoa eten gabe erabil dezake
- Deszentralizatuta: Sloten hasiera baino ez da sinkronizatu behar
- erraza

Cons:

- Talkak, galdutako slotak
- Ez erabilitako slotak
- Nodoek talka detektatu behar dute trama baten igortze denboran
- Erlojuaren sinkronizazioa

Slotted ALOHA: efficiency

efficiency: long-run fraction of successful slots (many nodes, all with many frames to send)

- *suppose:* N nodes with many frames to send, each transmits in slot with probability p
- prob that given node has success in a slot $= p(1-p)^{N-1}$
- prob that *any* node has a success $= Np(1-p)^{N-1}$

- max efficiency: find p^* that maximizes $Np(1-p)^{N-1}$
- for many nodes, take limit of $Np^*(1-p^*)^{N-1}$ as N goes to infinity, gives:

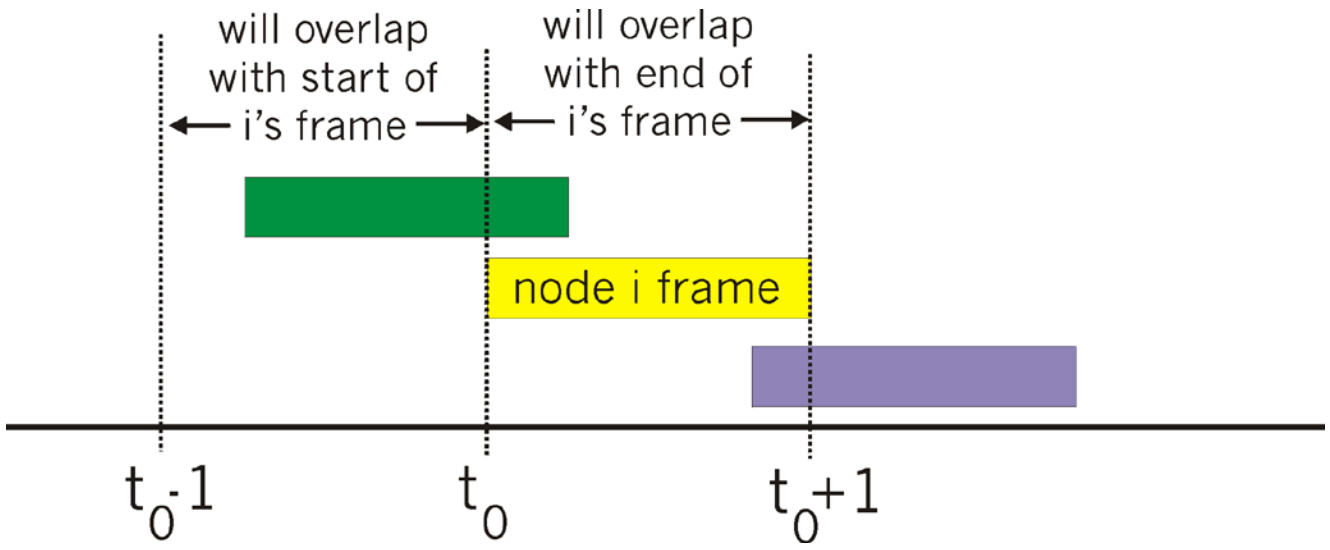
max efficiency $= 1/e = .37$

at best: channel used for useful transmissions 37% of time!

!

Pure (unslotted) ALOHA

- unslotted Aloha: Errazago, Sinkronizaziorik gabe
- Trama heltzen denean
  - Berehala transmititzen da
- Honek, talkak sortzeko aukera handitzen du:
  - t_0 unean bidalitako tramak talka egiten du $[t_0-1, t_0+1]$ tartean bidalitakoekin



Pure ALOHA efficiency

P(success by given node) = P(node transmits) ·
P(no other node transmits in $[t_0\text{-}1,t_0]$ ·
P(no other node transmits in $[t_0\text{-}1,t_0]$

$= p \cdot (1\text{-}p)^{N-1} \cdot (1\text{-}p)^{N-1}$

$= p \cdot (1\text{-}p)^{2(N-1)}$

… choosing optimum p and then letting $n \rightarrow \infty$

$= 1/(2e) = .18$

even *worse* than slotted Aloha!

CSMA (carrier sense multiple access)

CSMA: listen before transmit:

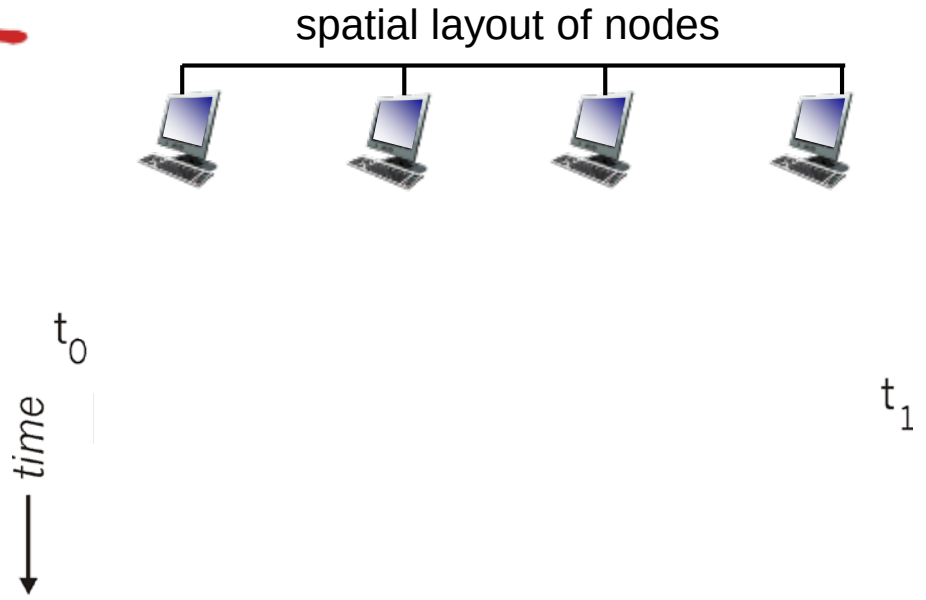
Kanala utzik badago: trama igorri

- Kanala okupatuta dagoenean, atzeratu transmisioa

- human analogy: don't interrupt others!

CSMA collisions

- Talkak gerta daitezke: hedapen atzerapena nodoek ezin dutela besteen transmisioaren hasiera
- Talka: Paketea bidaltzeko erabili den denbora guztia galtzen da
  - distance & propagation delay play role in in determining collision probability



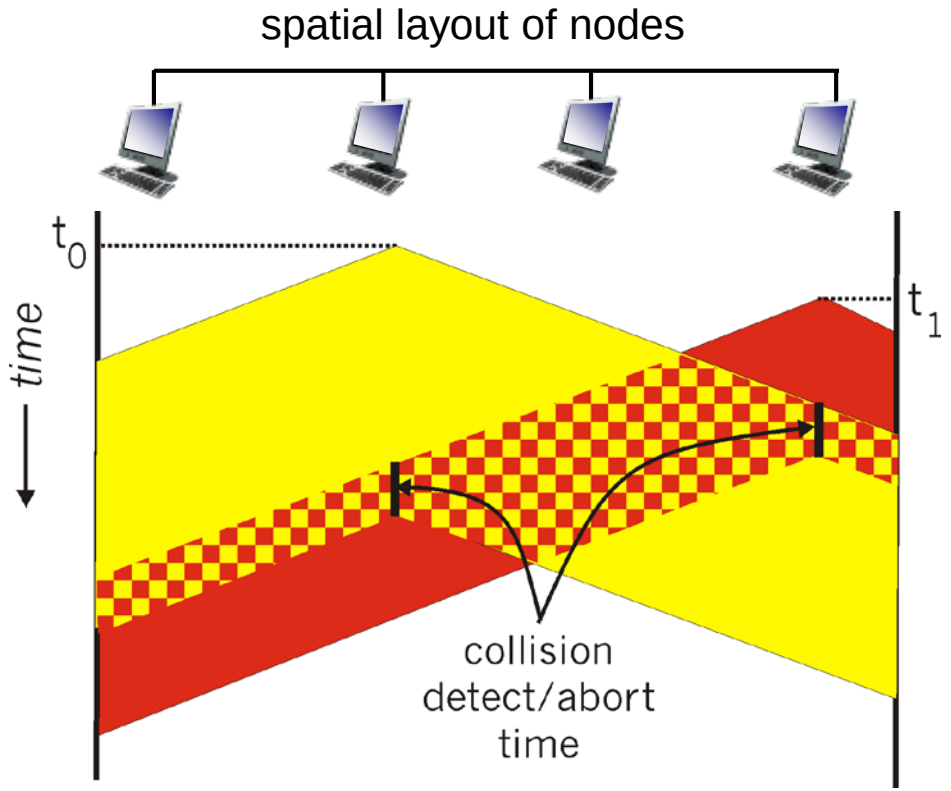
CSMA/CD (collision detection)

CSMA/CD: carrier sensing, deferral as in CSMA

- Talkak denbora tarte txikian detektatzen dira
- Talka izan duten tramen igorpena berehala geratzen da. Kanala garbiago mantentzen da

- Talken detekzioa:
  - Erraza haritutako LANetan: seinaleen indarra neur daiteke, igorritako eta jasotako seinaleak aldera daitezke
  - Haririk gabeko LANetan (wireless): seinale lokalaren indarrak, jasotako seinalearen indarra, gainditzen du, estaltzen du
- human analogy: the polite conversationalist

CSMA/CD (collision detection)



Ethernet CSMA/CD algorithm

1. NIC (txartelak) datagrama jasotzen du sare geruzatik, trama sortzen du
2. NIC-ak kanala utzik ikusten badu, tramaren transmisioari ekiten dio. NIC-ak kanala okupatuta ikusten badu, kanala utzik egon arte itxarotean du
3. NIC-ak trama osoa igortzen badu, talkak detektatu barik, trama transmitituta dago
4. NIC-ak beste transmisioa detektatzen badu igortzen duen bitartean, igorpena eteten du eta **jam** seinalea bidaltzen du
5. Igorpena eten eta gero, NIC-ak *binary (exponential) backoff batean* sartzen da:
   - after *m*th collision, NIC chooses *K* at random from $\{0,1,2, \ldots, 2^m-1\}$. NIC waits $K \cdot 512$ bit times, returns to Step 2
   - longer backoff interval with more collisions

CSMA/CD efficiency

- t_{prop} = max prop delay between 2 nodes in LAN
- t_{trans} = time to transmit max-size frame

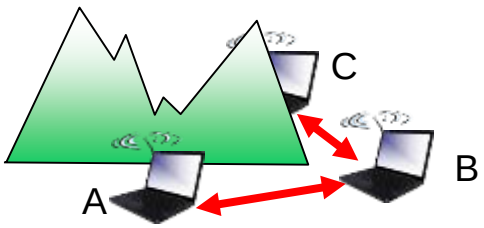
$$efficiency = \frac{1}{1 + 5t_{prop}/t_{trans}}$$

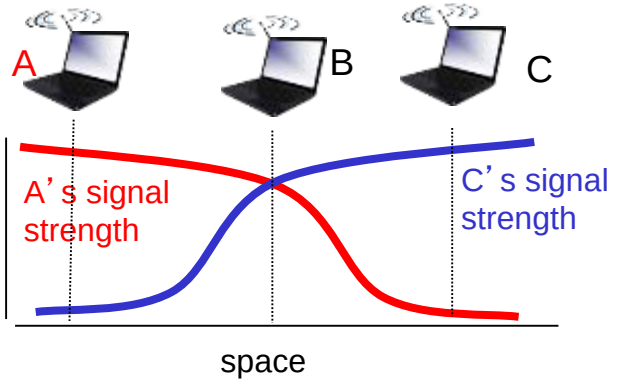
- efficiency goes to 1
  - as t_{prop} goes to 0
  - as t_{trans} goes to infinity
- better performance than ALOHA: and simple, cheap, decentralized!

CSMA/CA (collision avoidance)

Haririk gabeko sareek, dituzten berezitasunak direla eta, erronka berriak aurkezten dituzte:

- Seinalea arinago indargabetzen da distantziarekin. Zailagoa da talkak detektatzea
- Transmisioen irismena mugatua da (metro batzuk):

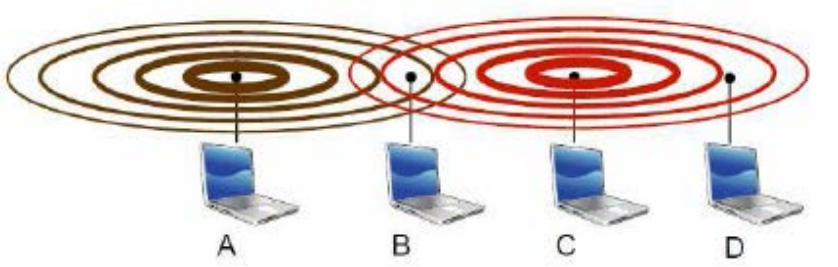




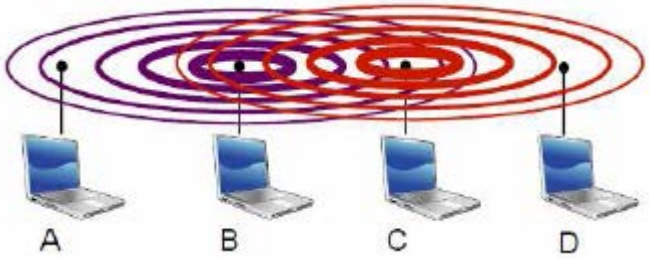
CSMA/CA (collision avoidance)

Bi arazo:

- Terminal ezkutua:
  - A-k ez du C ikusten baina talkak egon daitezke B-ri transmititu nahi diotenean



- Terminal ikusgai:
  - B eta C-ren artean talka dago azkenak D-ri zerbait bidali nahi dionean, baina informazioa ondo heltzen zaio D-ri



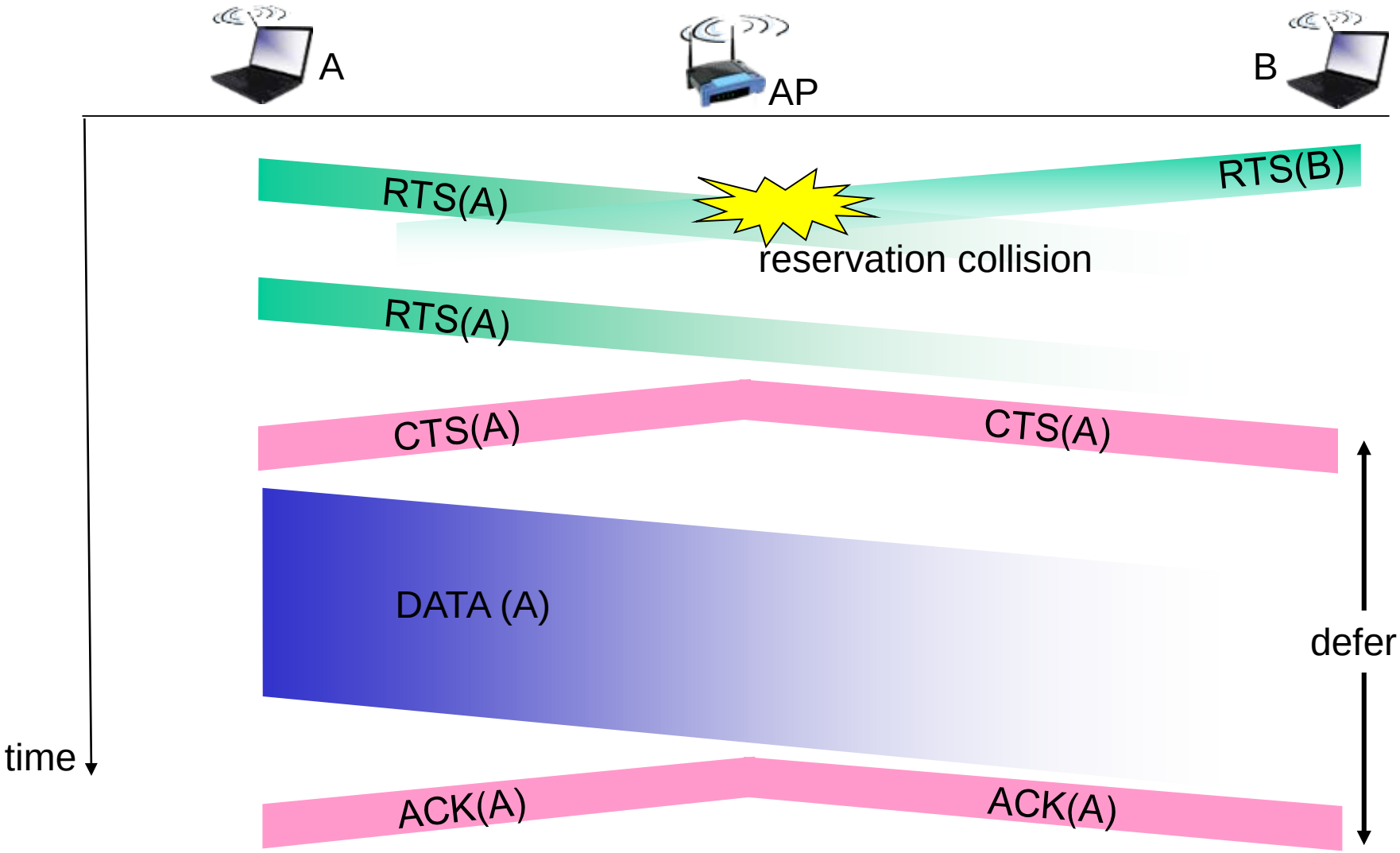
CSMA/CA (collision avoidance)

CSMA/CA talkak ekiditeko diseinatu zen:

- Igorleak ez du informazioa medioan jartzen nahi duenean.
- Igorleak igortzeko txanda "eskatu" eta "eskuratzen" du transmisioa arazorik gabe gauza dadin
- Igorleak, informazioa bidali aurretik, Bidaltzeko eskaera txiki bat bidaltzen dio jasotzaileari (request-to-send, RTS) CSMA erabiliz
  - RTS eskaeretan talkak gerta daitezke (baina txikiak dira, 30 byte)
- Jasotzaileak broadcast-en, clear-to-send (CTS), erantzuten dio igorleari, transmisio abisua emanez horren barrutian dauden guztiei
- Igorleak transmititzen du eta beste guztiek itxaroten dute
- Transmisioa bukatzen denean, jasotzaileak ACK bidaltzen du, medioa askatuz

Talkak erabat ekiditen dira, RTS eskaera txikiak bidalita

Collision Avoidance: RTS-CTS exchange



RTS: Request-To-Send

CTS: Clear-To-Send

"Taking turns" MAC protokoloak

Kanalaren banaketa MAC protokoloak:

- Igorpen karga handia dagoenean, era eraginkor eta egokian banatzen dute kanala
- Karga txikia dagoenean, era EZ eraginkorrean banatzen du kanala: banda zabaleraren 1/N erabiltzen da nodo bakar batek igortzen duenean!

Random access MAC protokoloak

- Karga handia ez denean, eraginkorra: nodo bakar batek igortzen duenean, kanal osoa erabil dezake
- Karga handia dagoenean: collision overhead

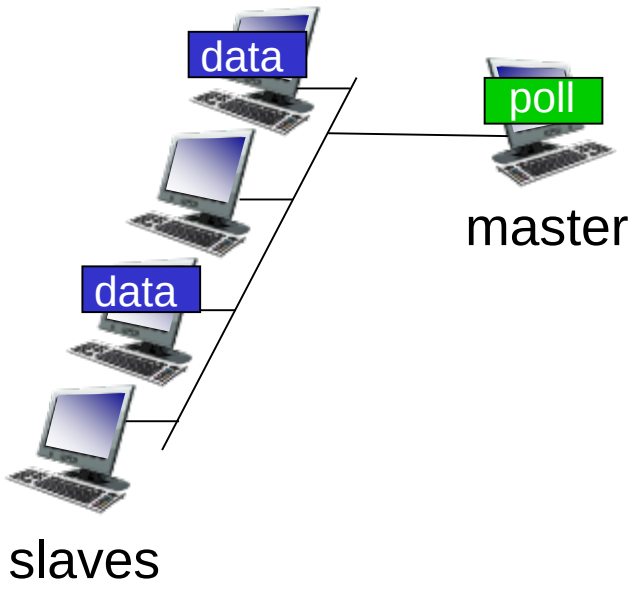
"taking turns" protokoloak

Bi munduen onena!

"Taking turns" MAC protocols

polling:

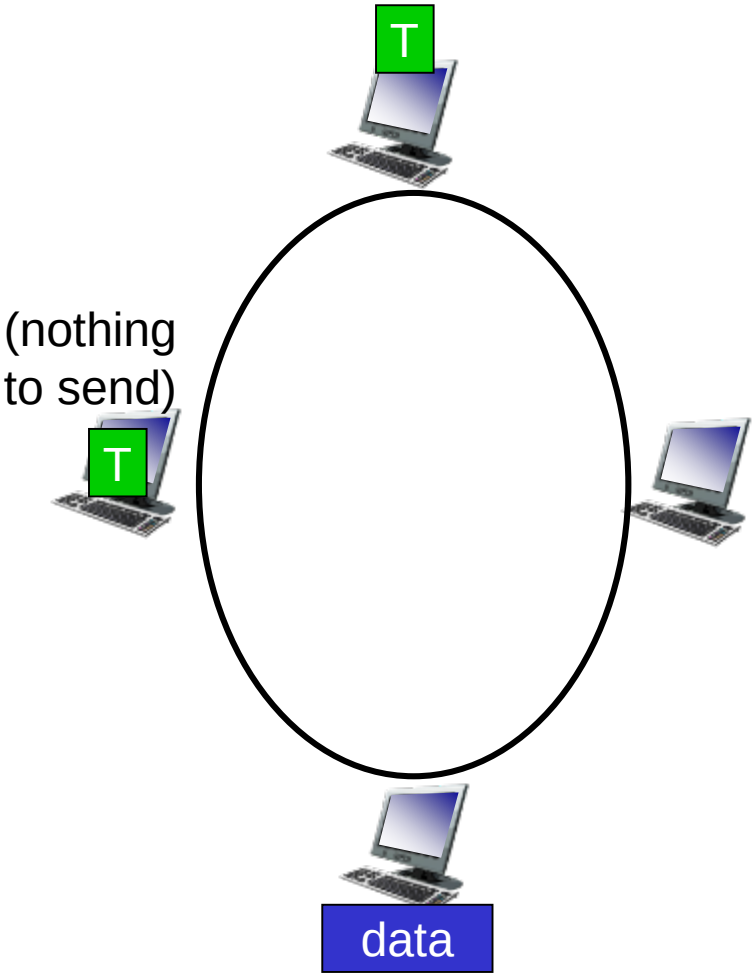
- master node "invites" slave nodes to transmit in turn
- typically used with "dumb" slave devices
- concerns:
  - polling overhead
  - latency
  - single point of failure (master)



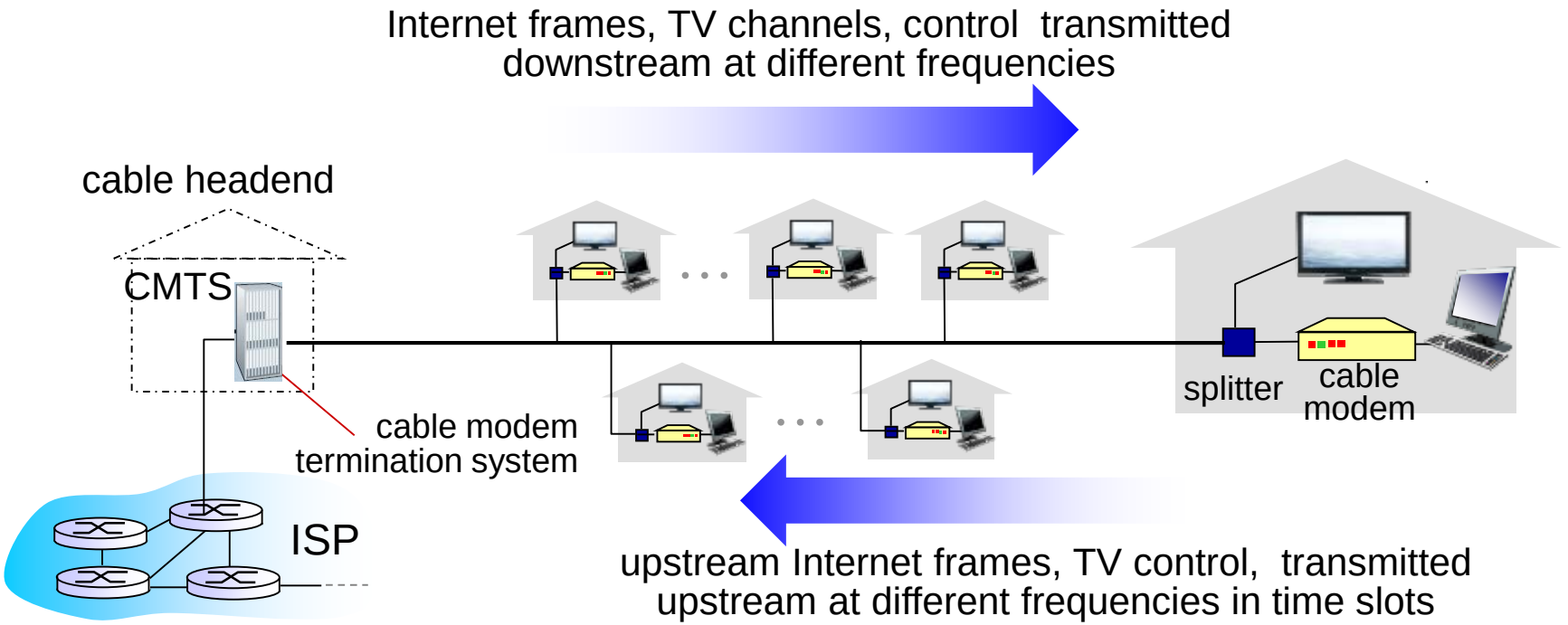
"Taking turns" MAC protocols

token passing:

- control *token* passed from one node to next sequentially.
- token message
- concerns:
  - token overhead
  - latency
  - single point of failure (token)

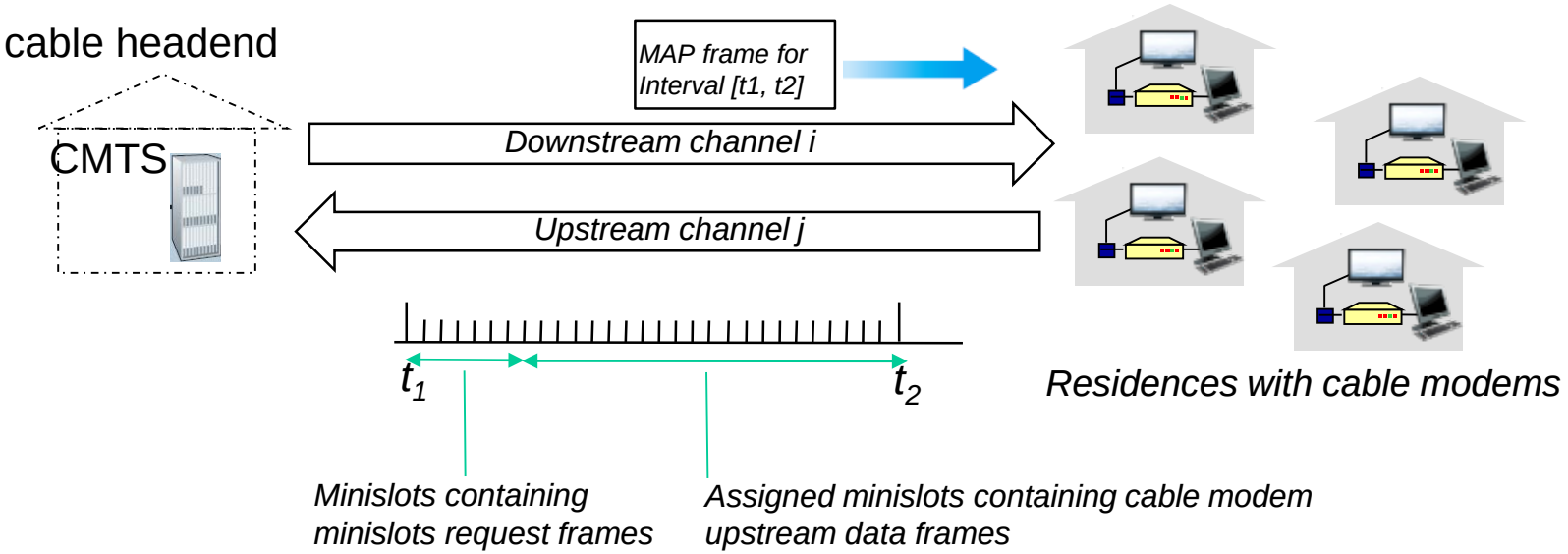


Cable access network



- multiple 40Mbps downstream (broadcast) channels
  - single CMTS transmits into channels
- multiple 30 Mbps upstream channels
  - multiple access: all users contend for certain upstream channel time slots (others assigned)

Cable access network



DOCSIS: data over cable service interface spec

- FDM over upstream, downstream frequency channels
- TDM upstream: some slots assigned, some have contention
  - downstream MAP frame: assigns upstream slots
  - request for upstream slots (and data) transmitted random access (binary backoff) in selected slots

Summary of MAC protocols

- *channel partitioning,* by time, frequency or code
  - Time Division, Frequency Division
- *random access* (dynamic),
  - ALOHA, S-ALOHA, CSMA, CSMA/CD
  - carrier sensing: easy in some technologies (wire), hard in others (wireless)
  - CSMA/CD (**C**ollission **D**etection) used in old Ethernet
  - CSMA/CA (**C**ollission **A**voidance) used in 802.11
- *taking turns*
  - polling from central site, token passing
  - Bluetooth, FDDI, token ring

Link layer, LANs: outline

6.1 Sarrera, zerbitzuak

6.2 Akats detekzioa, zuzenketa

6.3 Atzipen anitzeko protokoloak, multiple access protocols

6.4 LAN-ak

- Helbideen esleipena, ARP
- Ethernet
- switches
- VLANS

6.5 Loturen birtualizazioa: MPLS

6.6 data center networking

6.7 a day in the life of a web request

MAC helbideak eta ARP

- 32-bit-eko IP helbideak:
  - *network-layer* address for interface
  - 3. geruzan erabilita (sare geruza) bideraketarako
- MAC (edo LAN edo fisikoa edo Ethernet) helbidea:
  - Erabilera: *Lokalean erabilita, trama bat bidaltzeko fisikoki konektatuta dauden interfazeen artean (biak azpisare berean).*
  - 48 bit-eko MAC helbideak (LAN gehienetan) txartelaren (NICaren) ROM-ean ezarrita. Batzuetan posiblea da software bidez aldatzea
  - e.g.: 1a:2f:bb:76:09:ad

hexadecimal (base 16) notation
(each "numeral" represents 4 bits)

Hasierako 24 bit: ekoizlea

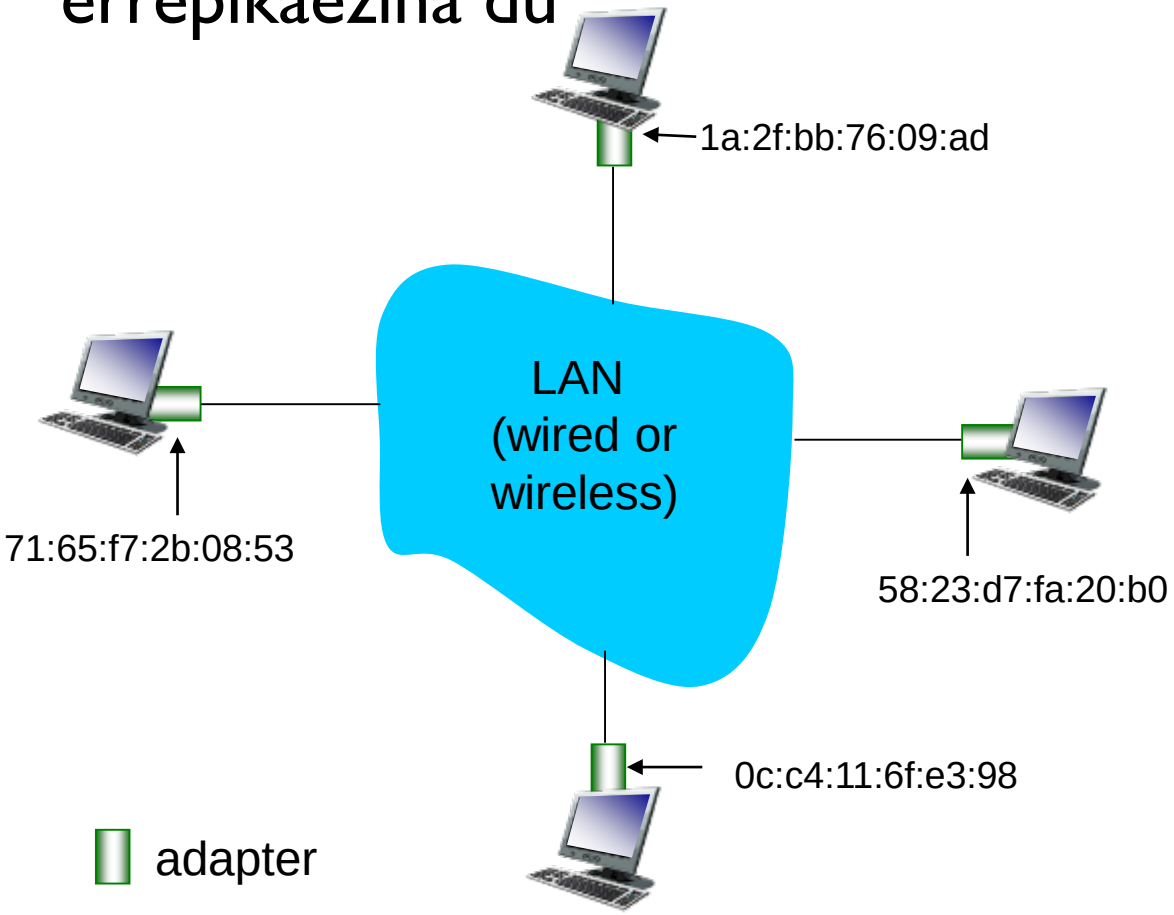
1a:2f:bb

Bukaerako 24 bit: identifikatzailea

76:09:ad

LAN helbideak eta ARP

LAN-eko txatel bakoitzak, *LAN* helbide propio eta errepikaezina du

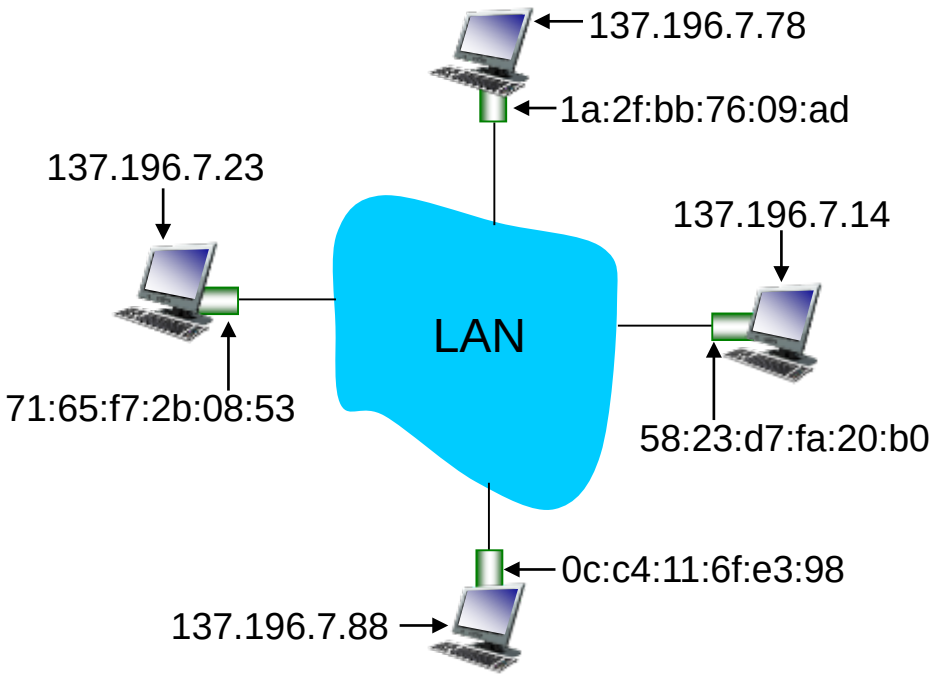


LAN helbideak (gehiago)

- IEEEk kudeatzen du MAC helbideen esleipena
- Ekoizleek MAC tarte bat erosten du helbide errepikatuak ez daudela ziurtatzeko
- analogia:
  - MAC helbidea: NAN-a bezala
  - IP helbidea: posta helbidea bezala
- MAC helbidea → eramangarritasuna ziurtatzen du
  - Sare txartela ekipo desberdinetan jar daiteke, LAN desberdinetan egon arren
- IP helbidea: hierarkiakoa, EZ eramangarria
  - Helbidea azpisarearen menpe dago

ARP: Address Resolution Protocol

Galdera: Nola jakin interfaze baten MAC helbidea IP helbidea ezagutzen denean?



ARP taula: LANeko IP nodo bakoitzak (host, router) taula dauka

- IP/MAC helbide mapa LAN nodo batzuentzat:

  < IP address; MAC address; TTL>
- TTL (Time To Live): mapa bizirik iraungo duen denbora berregin arte (normalean 20 min)

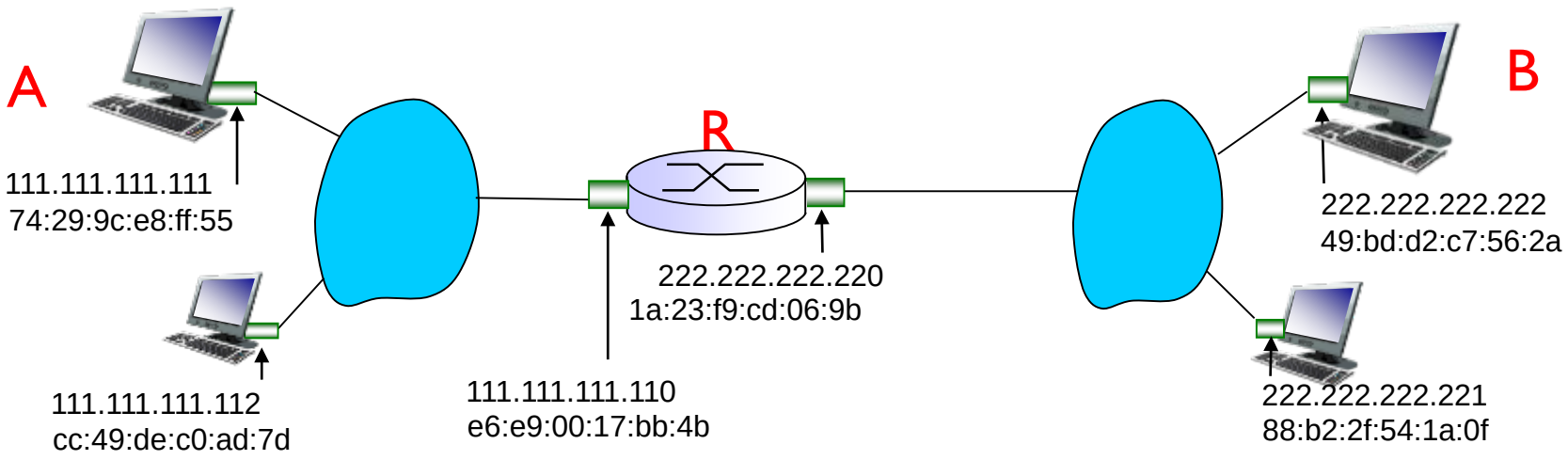
ARP protokoloa: LAN berean

- A-k B-ri datagrama bat bidali nahi dio
  - B-ren MAC helbidea ez dago Aren ARP taulan.
- A-k B-ren IP helbidea duen ARP eskaera bidaltzen du broadcast-en
  - destination MAC address = ff:ff:ff:ff:ff:ff
  - all nodes on LAN receive ARP query
- B-k ARP paketea jasotzen du, eta A- erantzuten dio bere (B-ren) MAC helbidea emanez
  - Trama bidaltzen dio A-ren MAC helbideari (unicast)
- A katxean gordetzen du (saves) IP-to-MAC helbide bikotea horren ARP taulan informazioa zaharkitu arte (times out)
  - soft state: Zaharkitzen den informazioa galtzen da (berritzen ez bada)
- ARP is "plug-and-play":
  - nodoek ARP taulak sortzen dituzte *sare kudeatzaileak ezan esan gabe*

Addressing: Beste LAN batera bideratuz

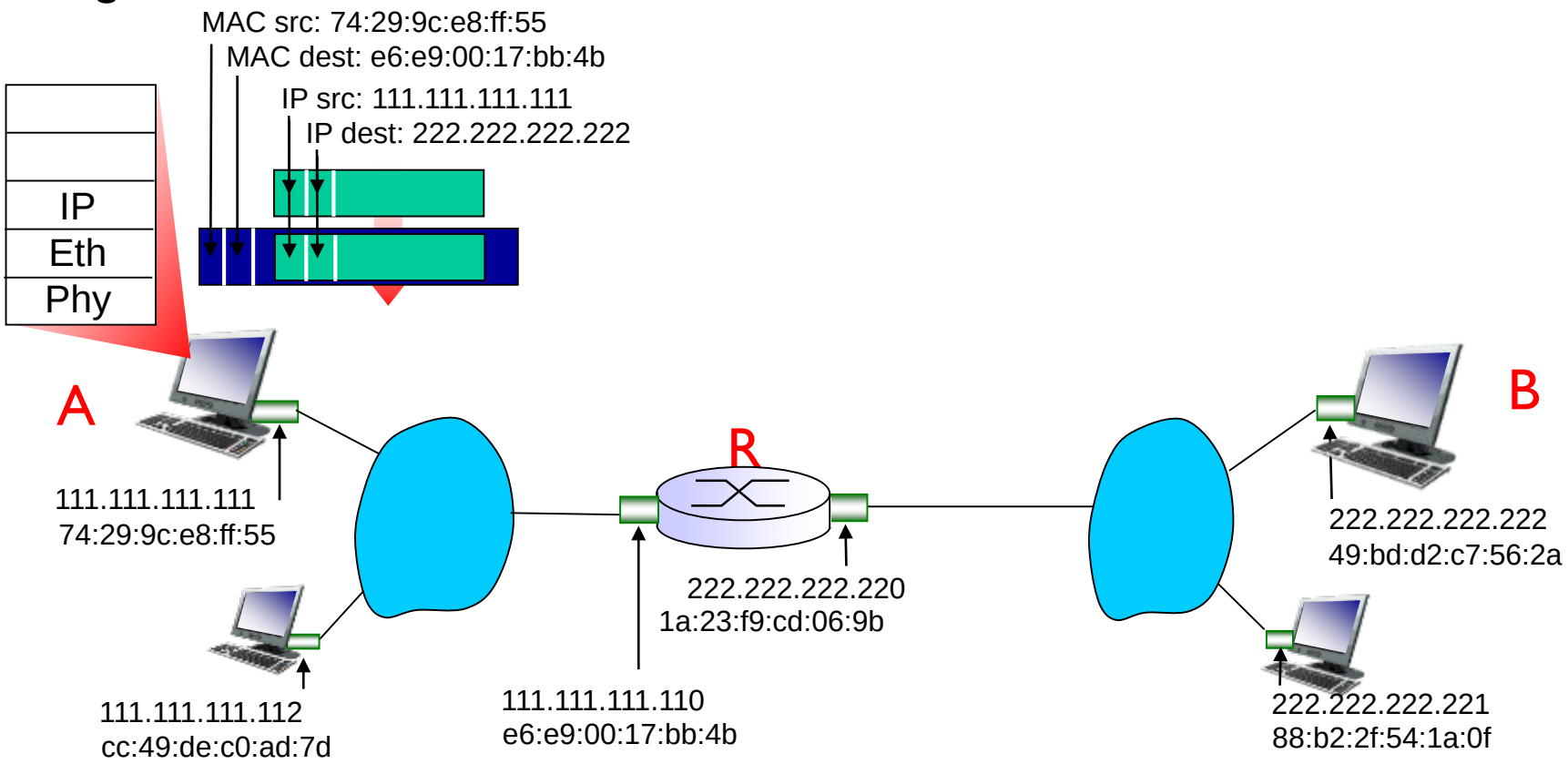
walkthrough: Bidali datagrama bat A-tik B-ra, R bidez

- Helbideak – IP (datagrama) eta MAC (trama)
- A-k B-ren IP-a ezagutzen du
- A-k, B-ra heltzeko lehen jausiaren (R-router) IP helbidea ezagutzen du (nola?)
- A-k R-ren MAC helbidea ezagutzen du (nola?)



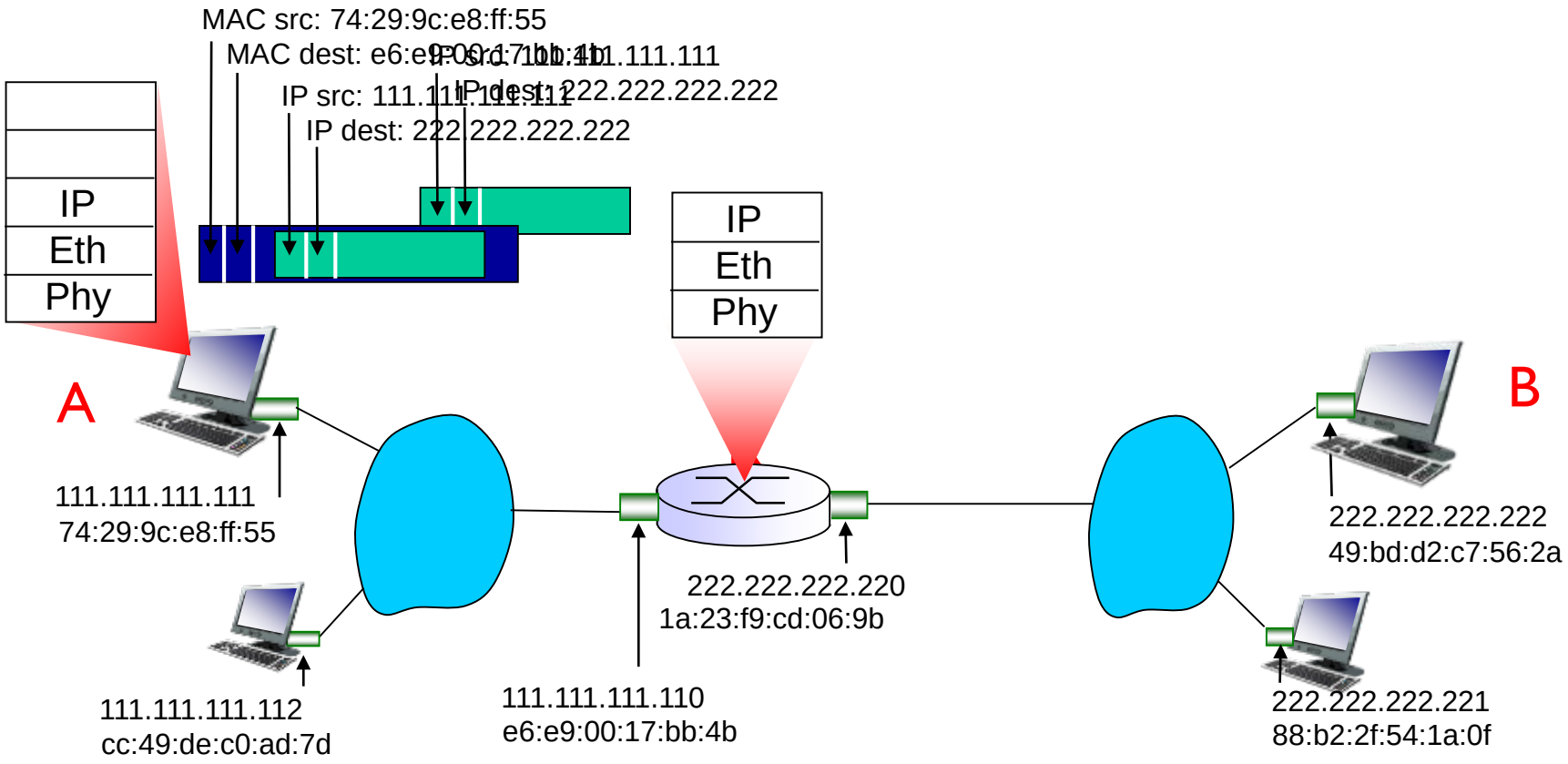
Addressing: Beste LAN batera bideratuz

- A-k IP datagrama sortzen du, igorle A, eta helmugaren B IP helbideekin, gero
- A-k lotura mailako trama sortzen du R-ren MAC helbidearekin (jasotzailearen helbidea). Trama honen barnean A-tik B-ra doan datagrama dago



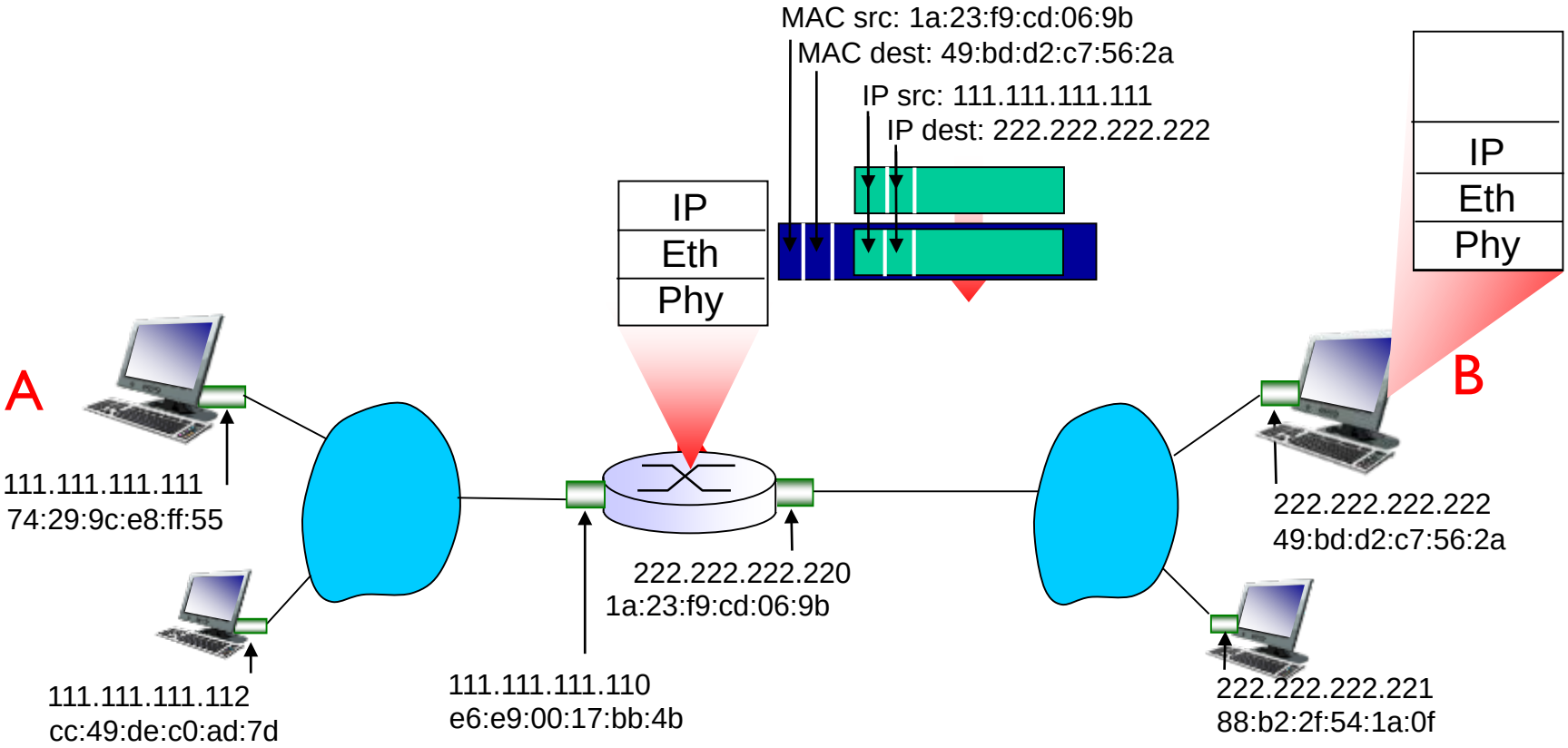
Addressing: Beste LAN batera bideratuz

- A-k trama bidaltzen dio R-ri
- R-ek trama jasotzen du, datagrama sare mailan aztertzen da, IP



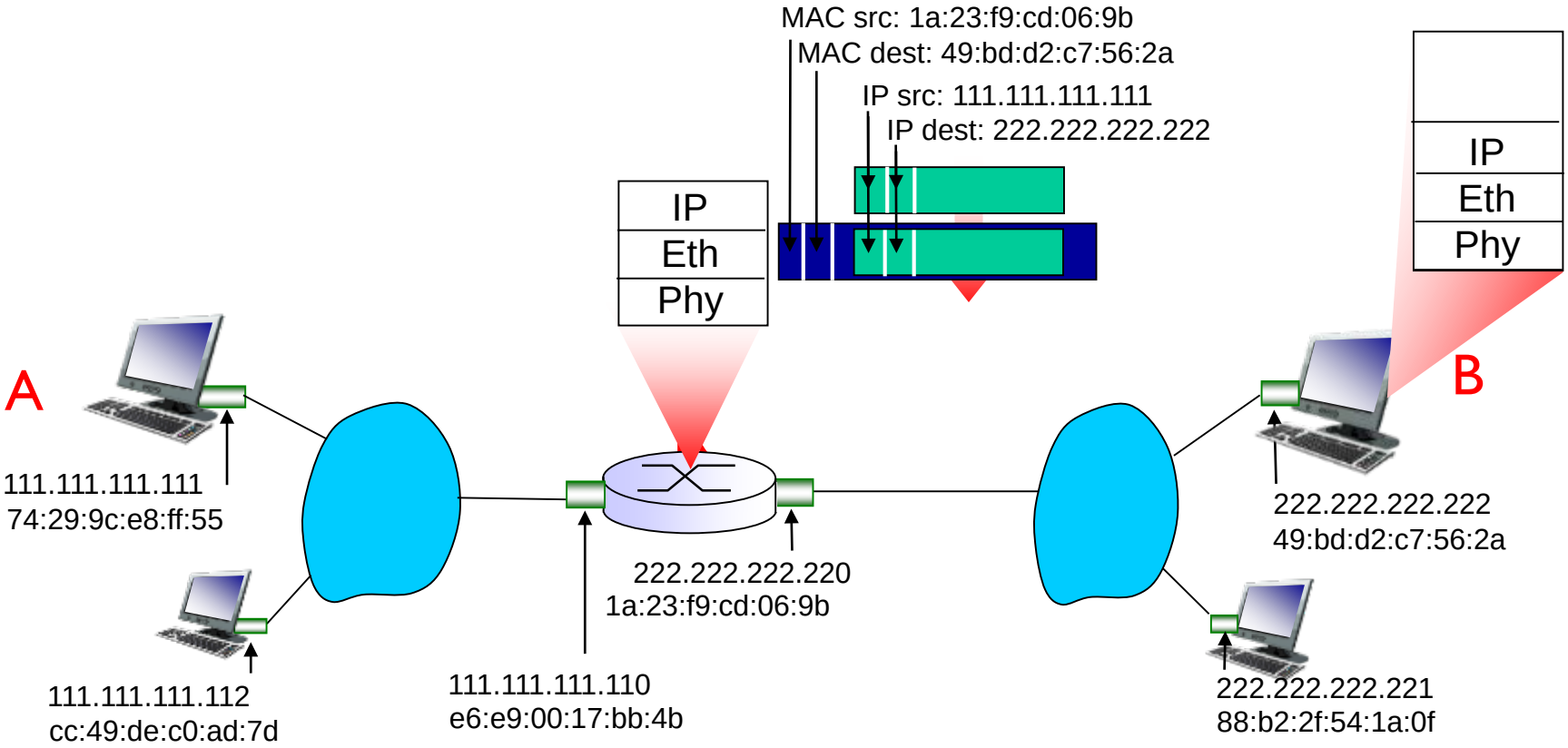
Addressing: Beste LAN batera bideratuz

- R-k B-rantz bideratzen du A iturria eta B helmuga duen datagrama, hau egiteko
- R-k lotura maileko trama bat sortzen du B-ren MAC helbidearekin (helmuga). Tramak A-to-B IP datagrama du barnean



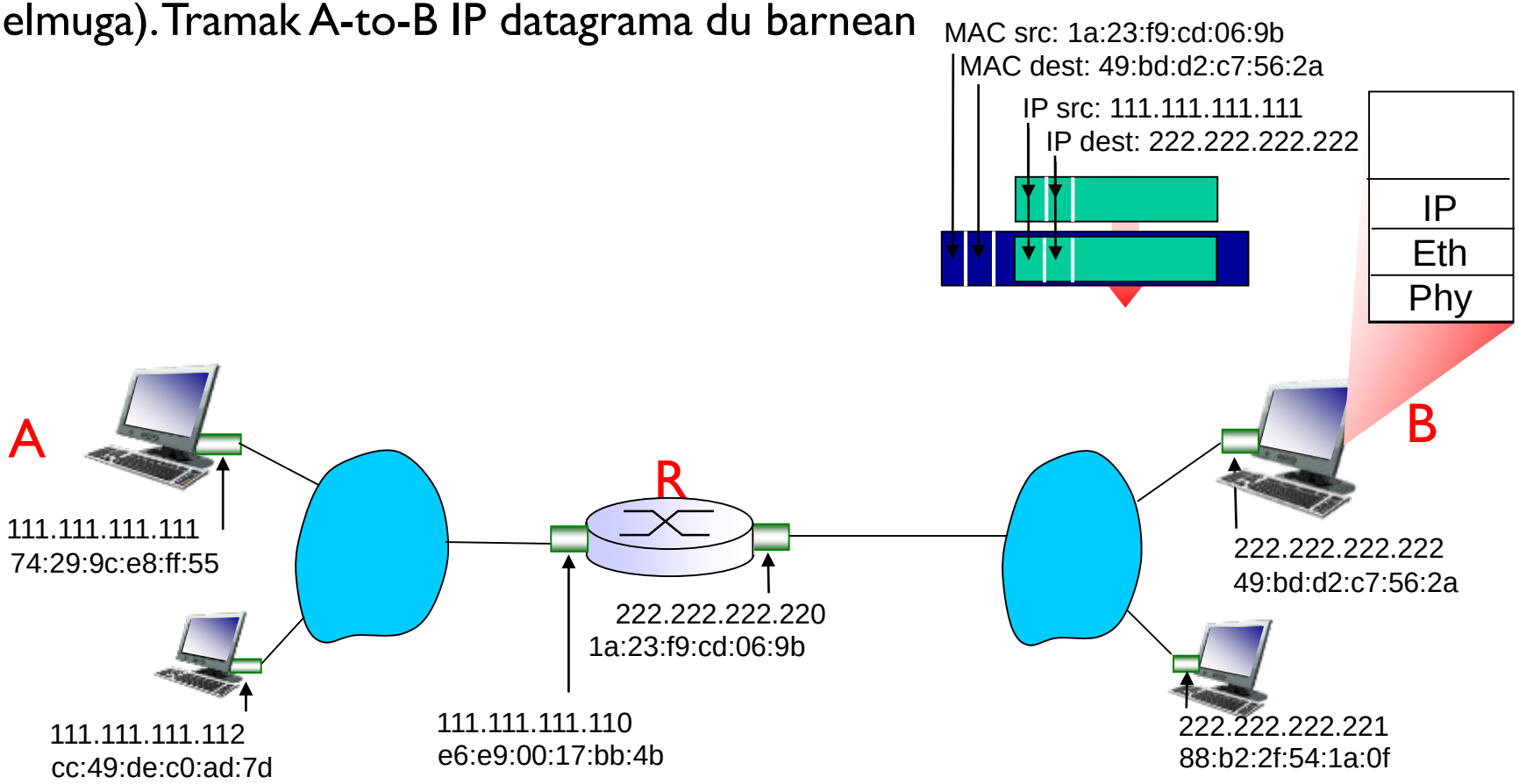
Addressing: Beste LAN batera bideratuz

- R-k B-rantz bideratzen du A iturria eta B helmuga duen datagrama, hau egiteko
- R-k lotura maileko trama bat sortzen du B-ren MAC helbidearekin (helmuga). Tramak A-to-B IP datagrama du barnean



Addressing: Beste LAN batera bideratuz

- R-k B-rantz bideratzen du A iturria eta B helmuga duen datagrama, hau egiteko
- R-k lotura maileko trama bat sortzen du B-ren MAC helbidearekin (helmuga). Tramak A-to-B IP datagrama du barnean



* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

Link layer, LANs: outline

6.1 Sarrera, zerbitzuak

6.2 Akats detekzioa, zuzenketa

6.3 Atzipen anitzeko protokoloak, multiple access protocols

6.4 LAN-ak

- Helbideen esleipena, ARP
- Ethernet
- switches
- VLANS

6.5 Loturen birtualizazioa: MPLS

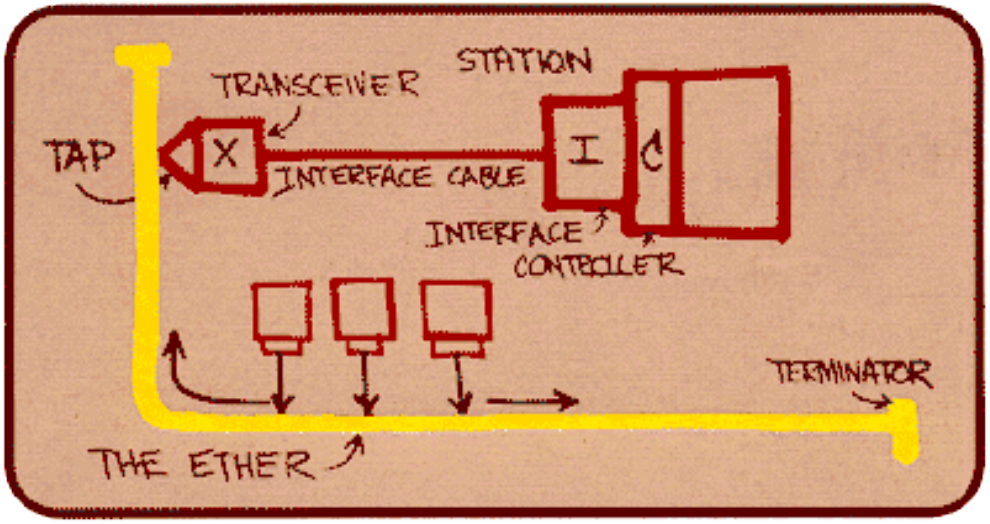
6.6 data center networking

6.7 a day in the life of a web request

Ethernet (IEEE 802.3)

LAN teknologia nagusia:

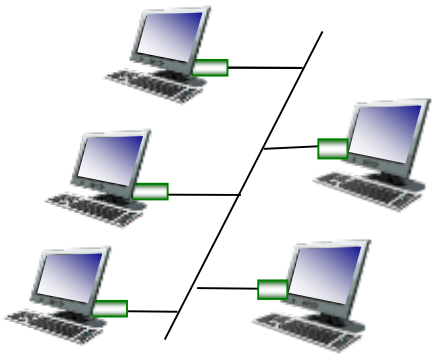
- Txip bakarra, abiadura desberdinak (e.g., Broadcom BCM5761)
- Era orokorrean erabilitako lehen LAN teknologia
- Erreza, merkea
- Abiadura lasterketa: 10 Mbps – 10 Gbps …



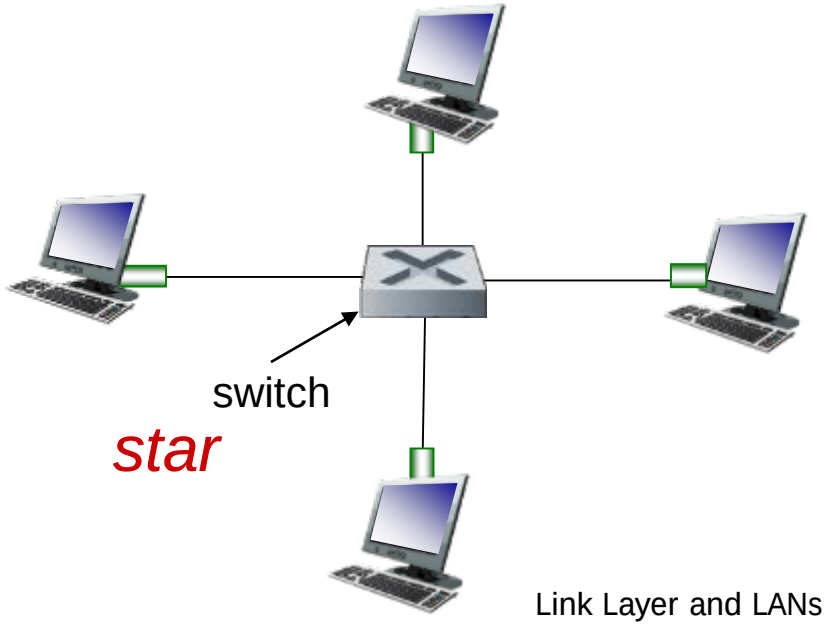
Metcalfe's Ethernet sketch

Ethernet: Topologia Fisikoa

- *bus:* ohikoa 90. hamarkadaren erdia arte
  - Nodo guztiak TALKA domeinu berean (nodo desberdinen tramen arteko talkak suerta daitezke)
- *star:* gaur egun
  - *switch* aktiboa erdian
  - Host bakoitzak Ethernet protokolo banandua exekutatzen du (EZ dago nodoen arteko talkak)



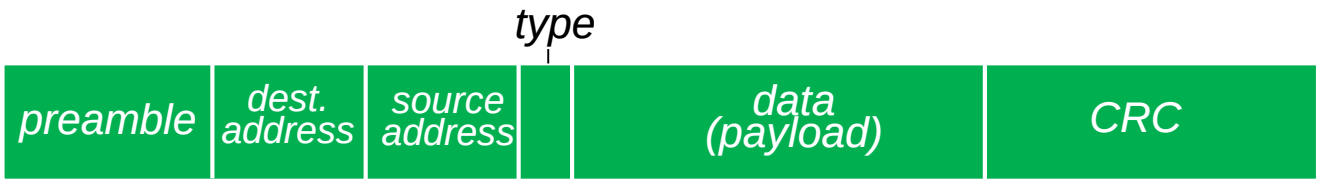
bus: coaxial cable



star

Ethernet-aren tramaren estruktura

Igorlearen txartelak IP datagrama (edo beste sare mailako paketea) Ethernet trama batean kapsulatzen du



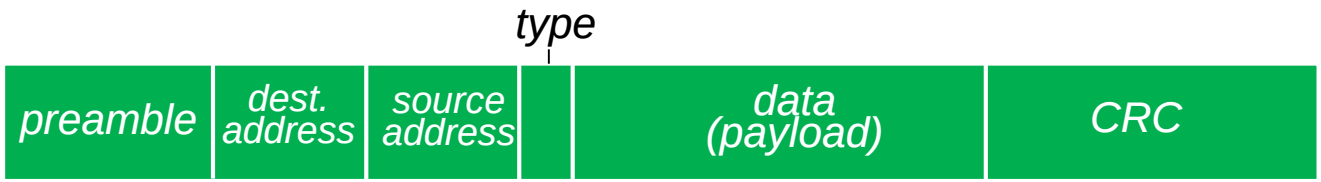
preamble:

- 7 bytes with pattern 10101010 followed by one byte with pattern 10101011
- used to synchronize receiver, sender clock rates

Zergatik ez dugu WhireShark-en ikusten?

Ethernet frame structure (more)

- *addresses:* 6 byte-eko igorle eta helmugaren MAC helbideak
  - Adaptadoreak (Txartelak) horren MAC helbidearekin bat egiten duen trama jasotzen badu, (edo broadcast, ad ARP paketea) trama barnean dagoen informazioa sare mailara pasatzen du
  - Bestela, trama baztertzen du
- *type:* goiko geruzaren adierazlea (mostly IP but others possible, e.g., Novell IPX, AppleTalk)
- *CRC:* cyclic redundancy check at receiver
  - Akatsik topatuz gero: trama baztertzen da

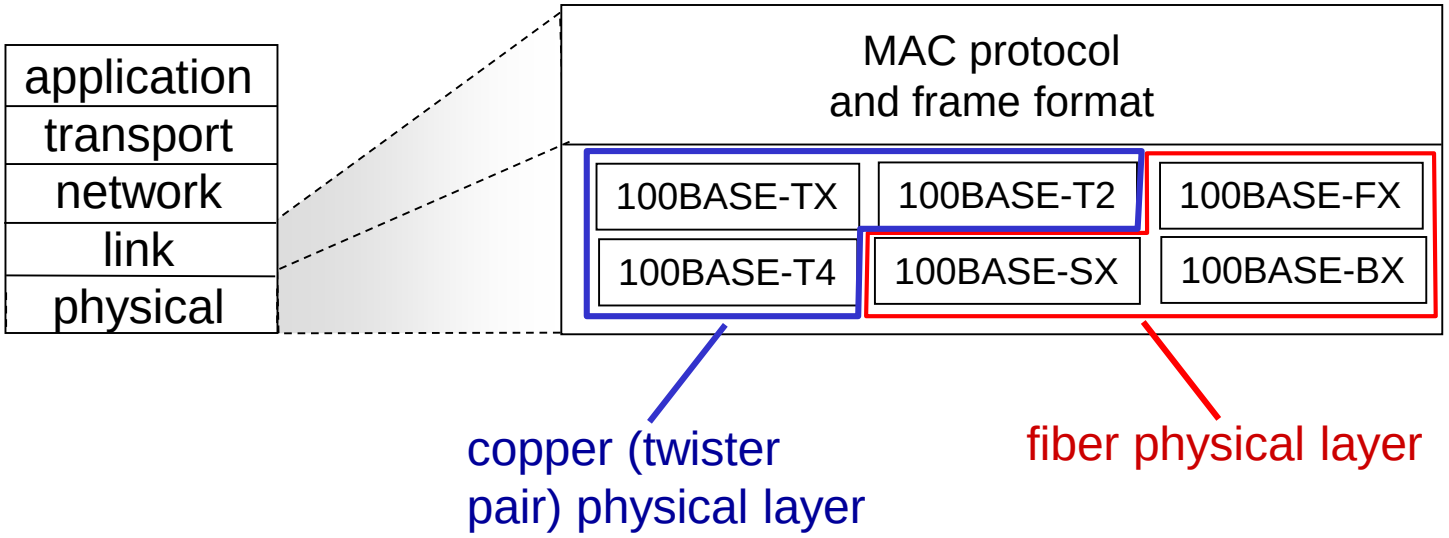


Ethernet: Ez Fidagarria, Konexiorik gabe

- *Konexiorik gabe:* Agurrik igorle eta helmugako NIC-en artean
- *Ez fidagarria:* Trama jasotzen duen NIC-ak ez du ACK edo NACK-rik bidaltzen trama igorri duen NIC-ri
  - Baztertutako trametan dagoen informazioa berrezkuratzen da rdt (reliable data transfer) portokolo erabiltzen bada goiko maietan (Ad, TCP), bestela, galtzen da
- Ethernetaren MAC protokoloa: unslotted *CSMA/CD with binary backoff*

802.3 Ethernet estandar: link & physical layers

- Ethernet-eko estandar desberdinak
  - amankomuneko trama formatua eta MAC protokoloa
  - Abiadura desberdinak: 2 Mbps, 10 Mbps, 100 Mbps, 1Gbps, 10 Gbps, 40 Gbps…
  - Medio fisiko desberdinak: zuntza, haria



Link layer, LANs: outline

6.1 Sarrera, zerbitzuak

6.2 Akats detekzioa, zuzenketa

6.3 Atzipen anitzeko protokoloak, multiple access protocols

6.4 LAN-ak

- Helbideen esleipena, ARP
- Ethernet
- switches
- VLANS

6.5 Loturen birtualizazioa: MPLS

6.6 data center networking

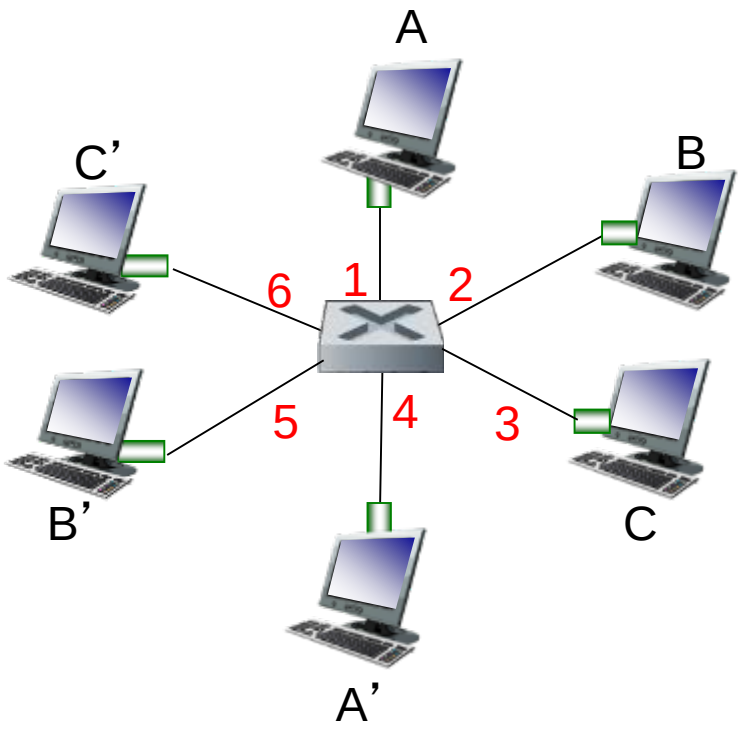
6.7 a day in the life of a web request

Ethernet switch

- Lotura mailako gailua: rol *aktiboa informazio trukaketan*
  - Ethernet tramak gorde eta bideratzen ditu
  - Heltzen diren tramen MAC helbideak aztertzen ditu, era selektiboan bideratu behar diren tramak aukeratzen ditu eta irteerako lin batera edo gehiagora bideratzen ditu. CSMA/CD erabiltzen du
- *gardena*
  - Host-ek ez dituzte switch-ak ikusten
- *plug-and-play, self-learning*
  - Ez dira konfiguratu behar

Switch: *multiple* simultaneous transmissions

- Hosts-ek konexio zuzena eta dedikatua dute switch-arekin
- Switchek buferrak erabiltzen dituzte tramen trataeran
- Ethernet protokoloa erabiltzen da link bakoitzean, baina ez dago talkarik; full duplex
  - link bakoitza da beraren talka domeinua
- *switching:* A-to-A' eta B-to-B' batera transmiti daitezke talkarik gabe



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

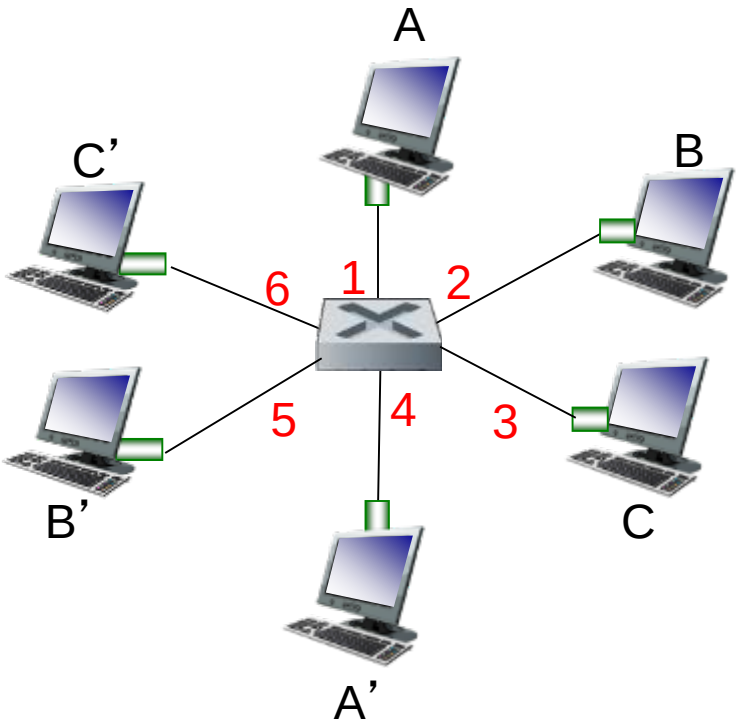
Switch forwarding table

Q: how does switch know A' reachable via interface 4, B' reachable via interface 5?

- A: Switch bakoitzak switch taula dauka sarrera bakoitzean:
  - (Host-aren MAC helbidea, host atzitzeko interfaze, denboraren sigilua)
  - Bideraketa taula modukoa!

Q: Nola sortzen dira sarrerak taulan? Nola mantentzen dira?

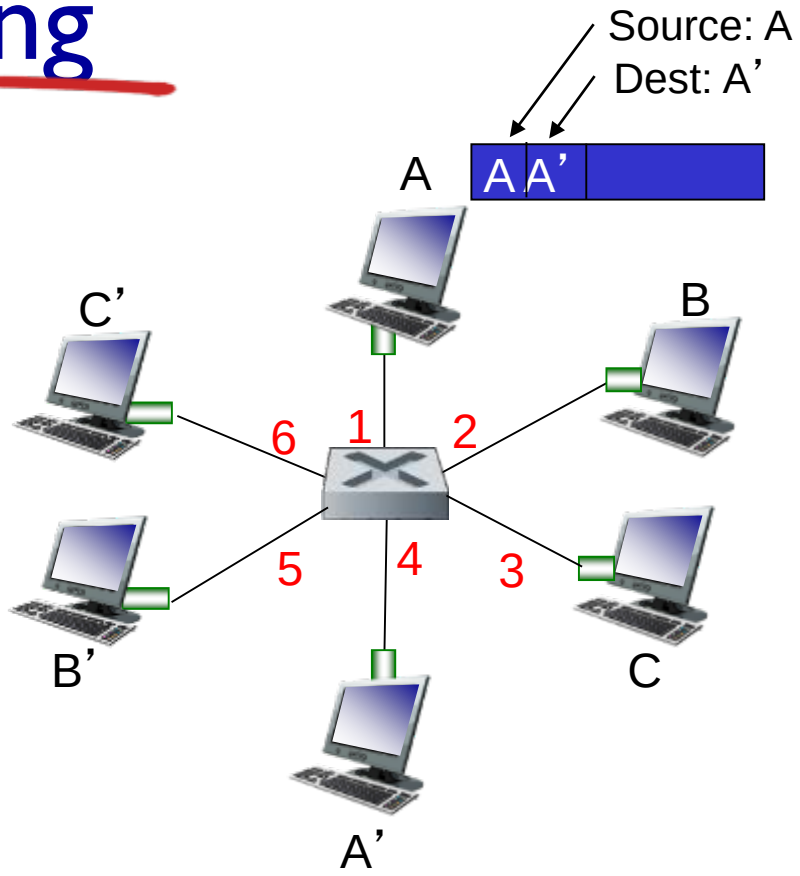
- Bideraketa protokoloaren modukoa?



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

Switch: self-learning

- Switch-ak *ikasten* du zein hostera hel daiteke interfaze desberdinen bidez
  - Trama jasotzen denean, switch-ak igorlearen kokapena "ikasten" du: incoming LAN segment
  - sender/location bikotea switch table-an gordetzen dira



MAC addr	interface	TTL
A	*1*	*60*

Switch table (initially empty)

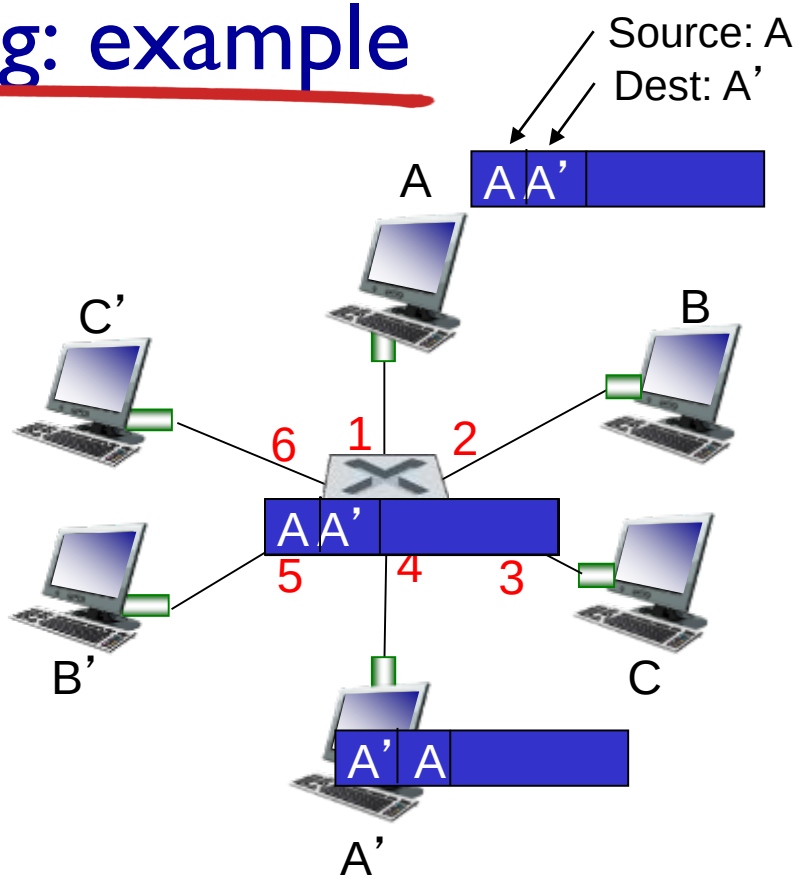
Switch: frame filtering/forwarding

Switch-ak trama jasotzen duenean:

1. Datorren link-a gorde, igorlearen MAC helbidea
2. Switch taula indexatu helmugaren MAC helbidea erabiliz
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 */

Self-learning, forwarding: example

- Tramaren helmuga, A', Non?: Ezezaguna: *flood*
- Helmuga A, ezaguna: Dagokion linkari bidali

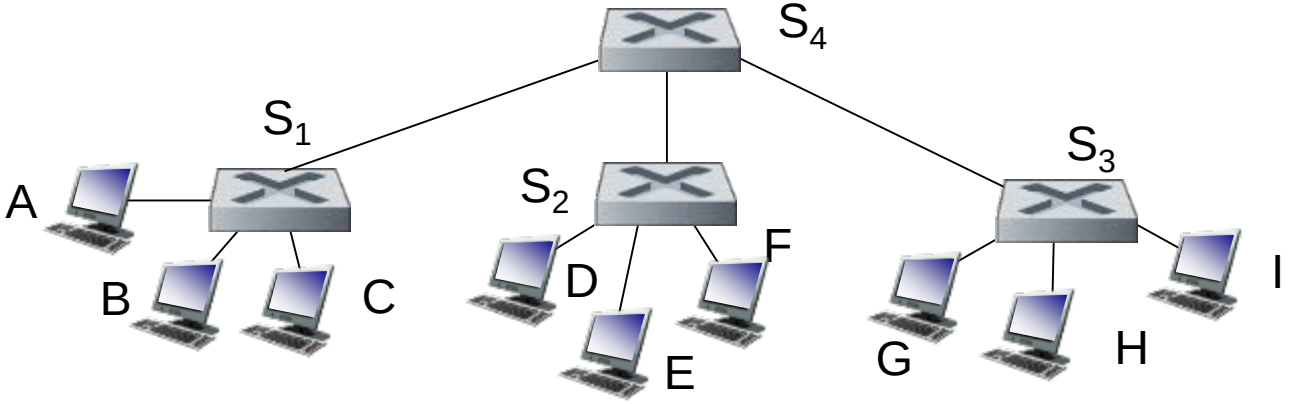


MAC addr	interface	TTL
A	*1*	*60*
A'	*4*	*60*

switch table (initially empty)

Interconnecting switches

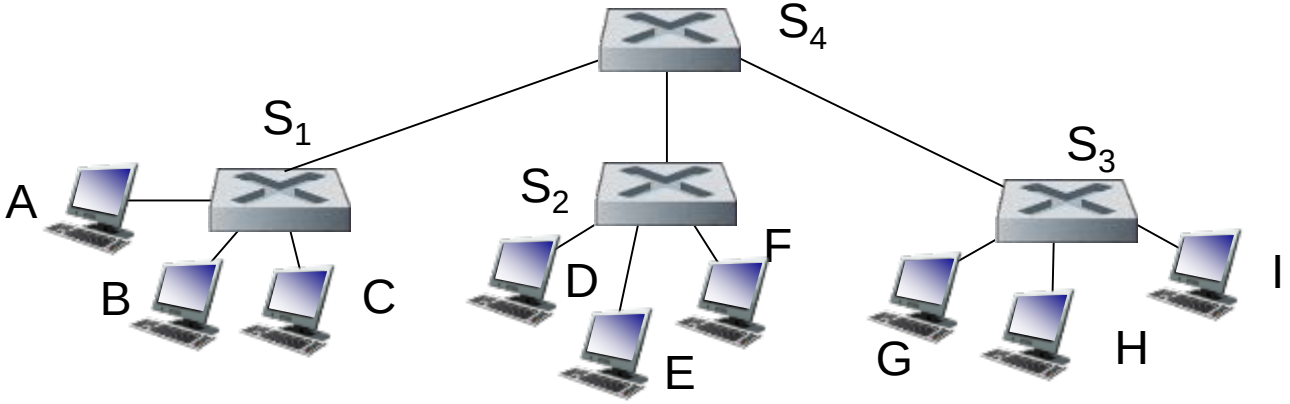
self-learning switche-ak elkarrekin konekta daitezke:



Q: A-tik G-ra bidaltzen. Nola daki S_1-ek nodik bidali behar duen trama G-ra heltzeko S_4 and S_3 zeharkatuz?
A: self learning! (Switch bakarren kasuan bezala lan egiten du!)

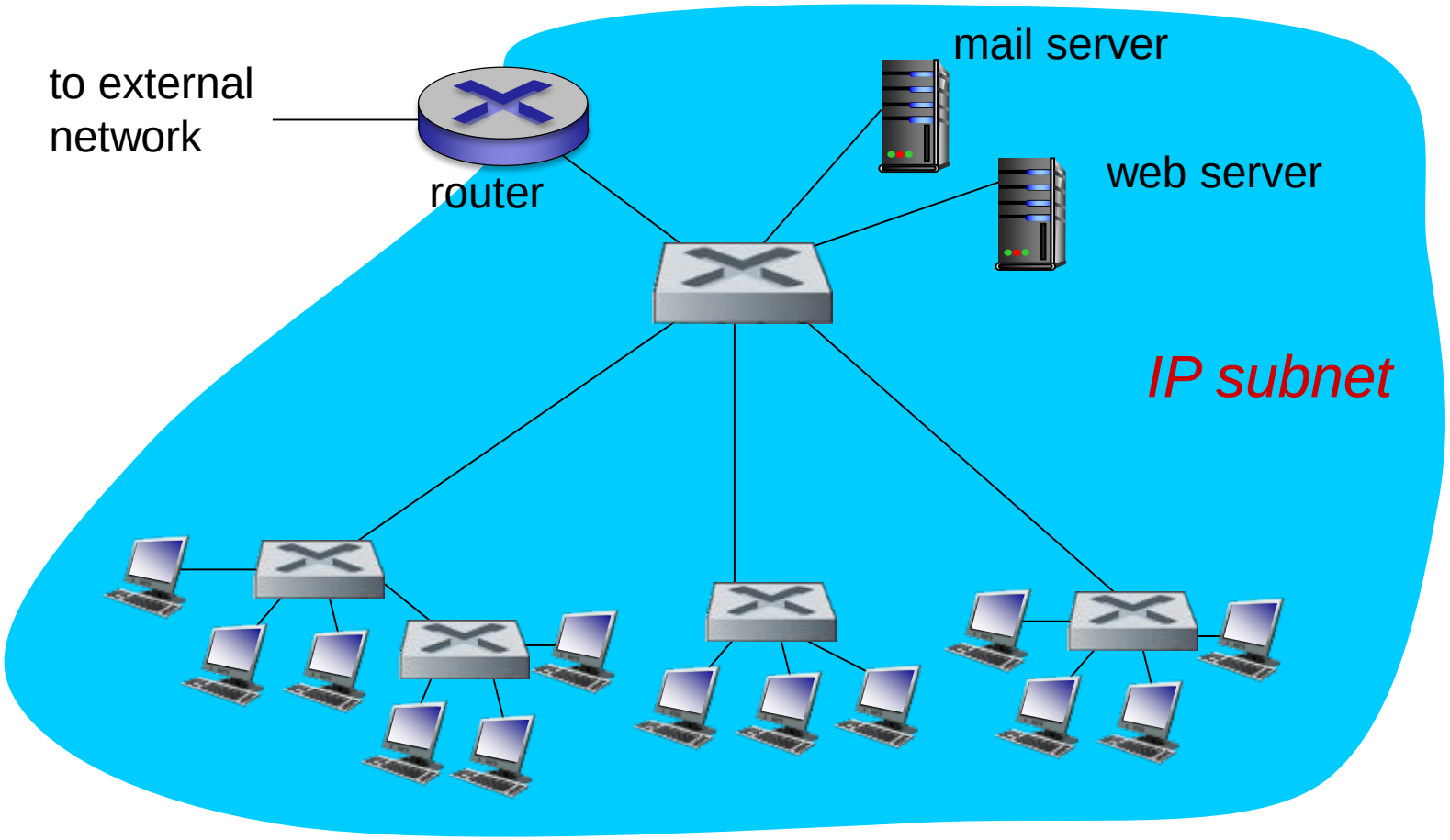
Self-learning multi-switch example

Demagun C-k frame bat bidaltzen diola I-ri eta I-k C-ri erantzuten diola



- Q: Erakutsi trukaketa taulak eta paketeen berbideraketa S_1, S_2, S_3, eta S_4-ean

Institutional network



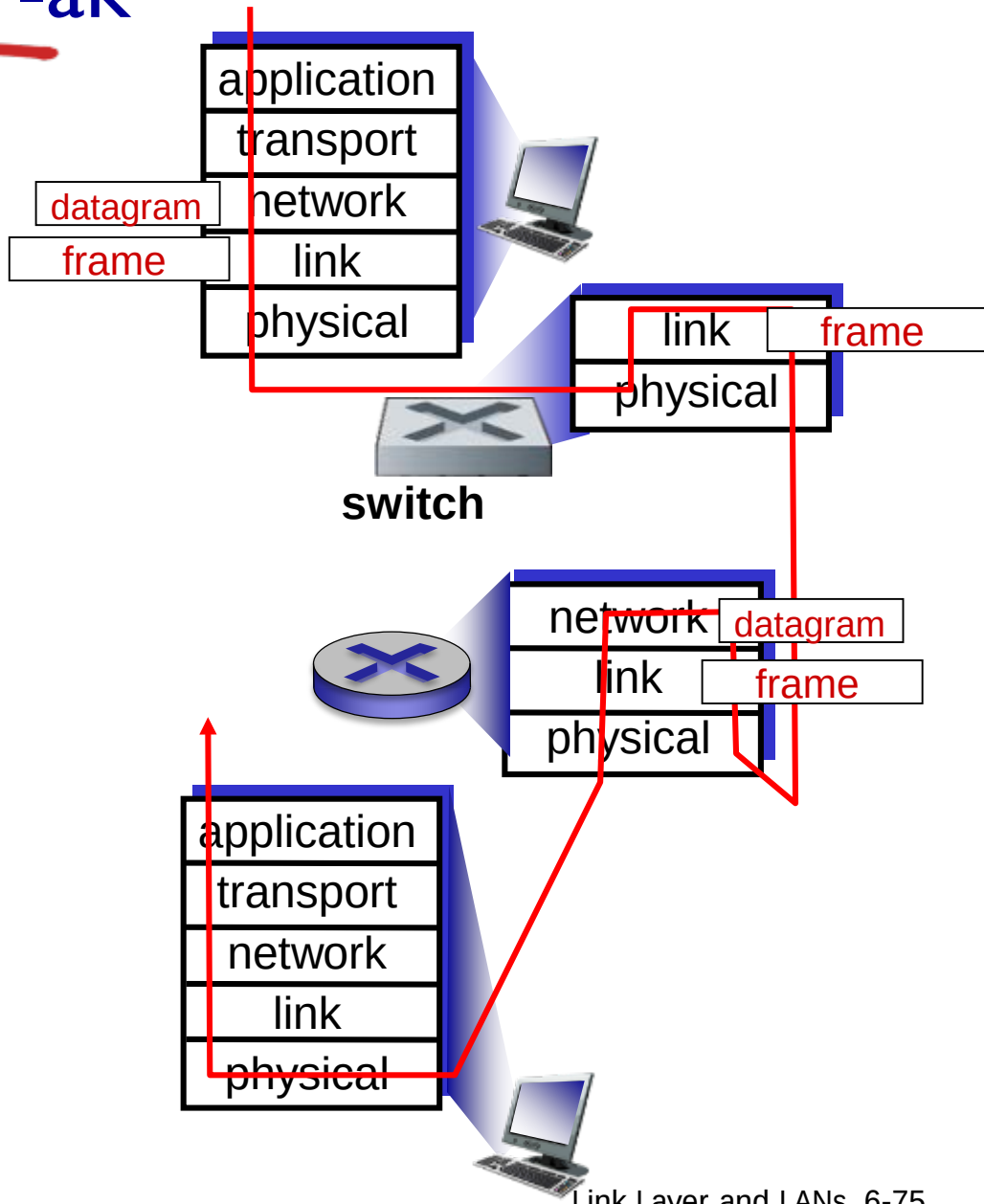
Switch-ak vs. Router-ak

Biak dira store-and-forward (gorde eta bideratu):

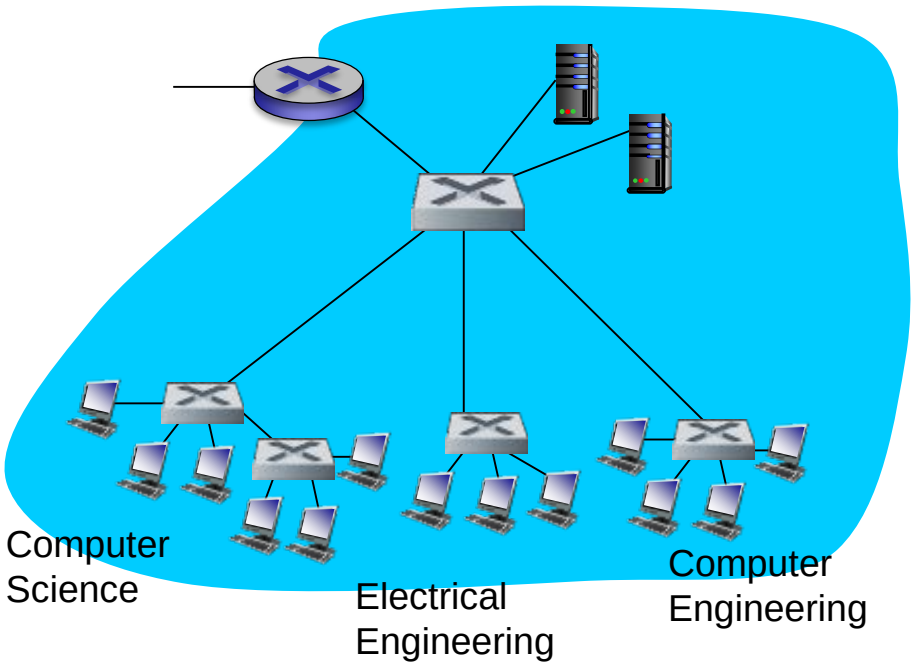
- *Router-ak:* sare mailako gailuak (sare mailako goiburuak aztertzen ditu)
- *switches*: lotura mailako gailuak (lotura mailako goiburuak aztertzen ditu)

Biek daukate bideraketa taulak:

- *Router-ak:* taulak eratzen ditu bideratze algoritmoak erabilita, IP helbideak
- *switches:* bideratze taula eratzen dute administratzailearen laguntzarik gabe, self-learning, MAC helbideak



VLANs: motivation



consider:

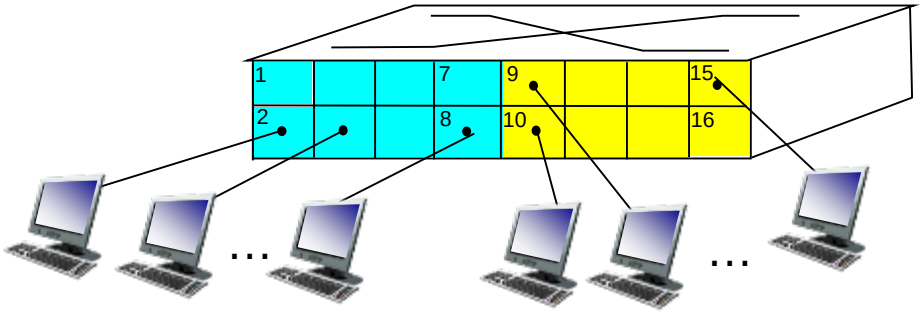
- CS user moves office to EE, but wants connect to CS switch?
- single broadcast domain:
  - all layer-2 broadcast traffic (ARP, DHCP, unknown location of destination MAC address) must cross entire LAN
  - security/privacy, efficiency issues

VLANs

Virtual Local Area Network

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

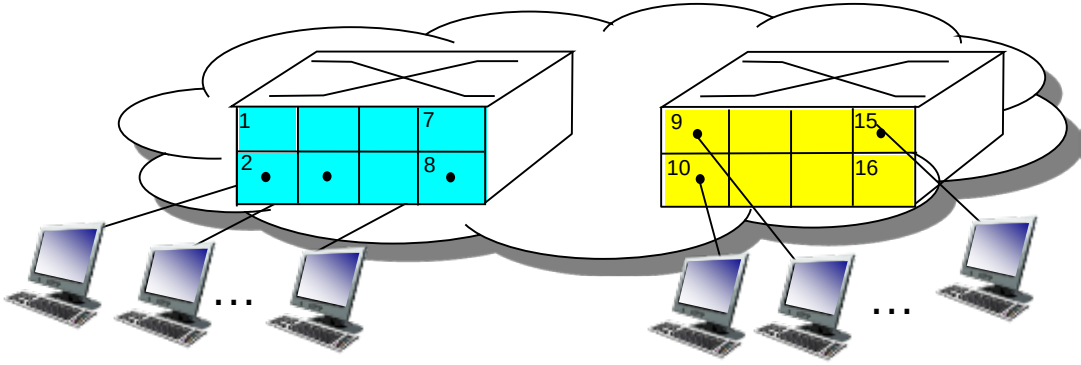
port-based VLAN: switch ports grouped (by switch management software) so that *single* physical switch ……



Electrical Engineering (VLAN ports 1-8)

Computer Science (VLAN ports 9-15)

… operates as multiple virtual switches

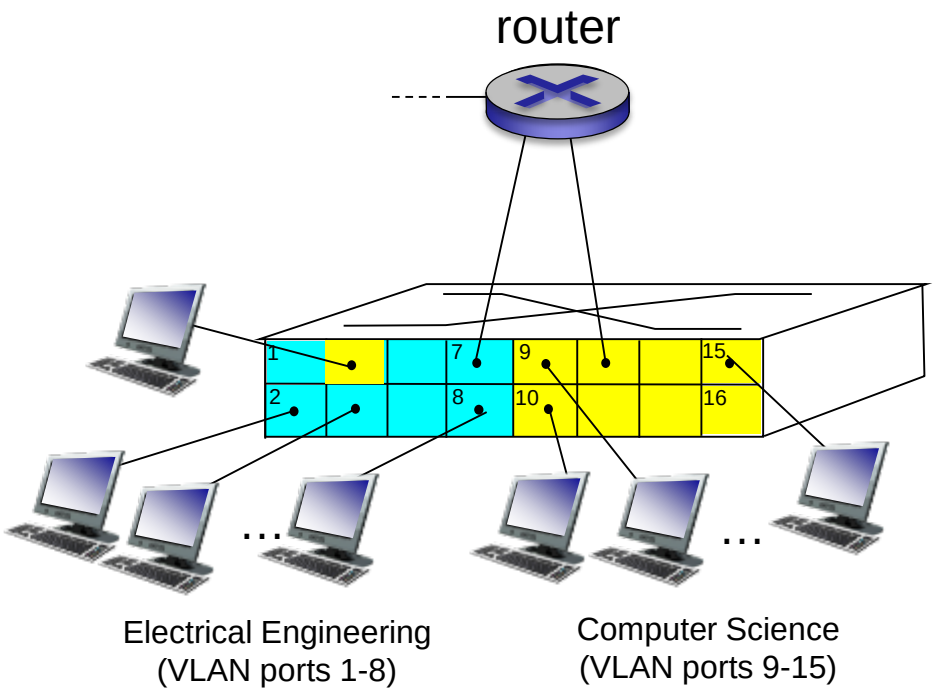


Electrical Engineering (VLAN ports 1-8)

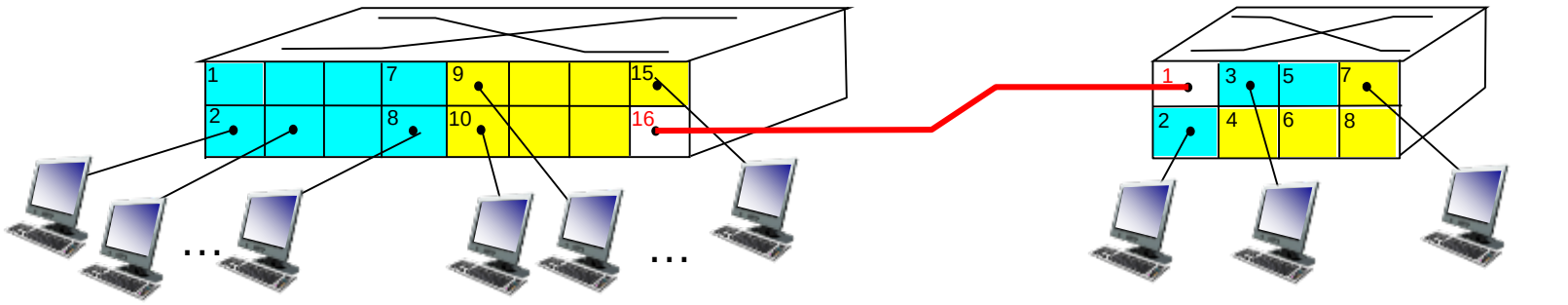
Computer Science (VLAN ports 9-16)

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

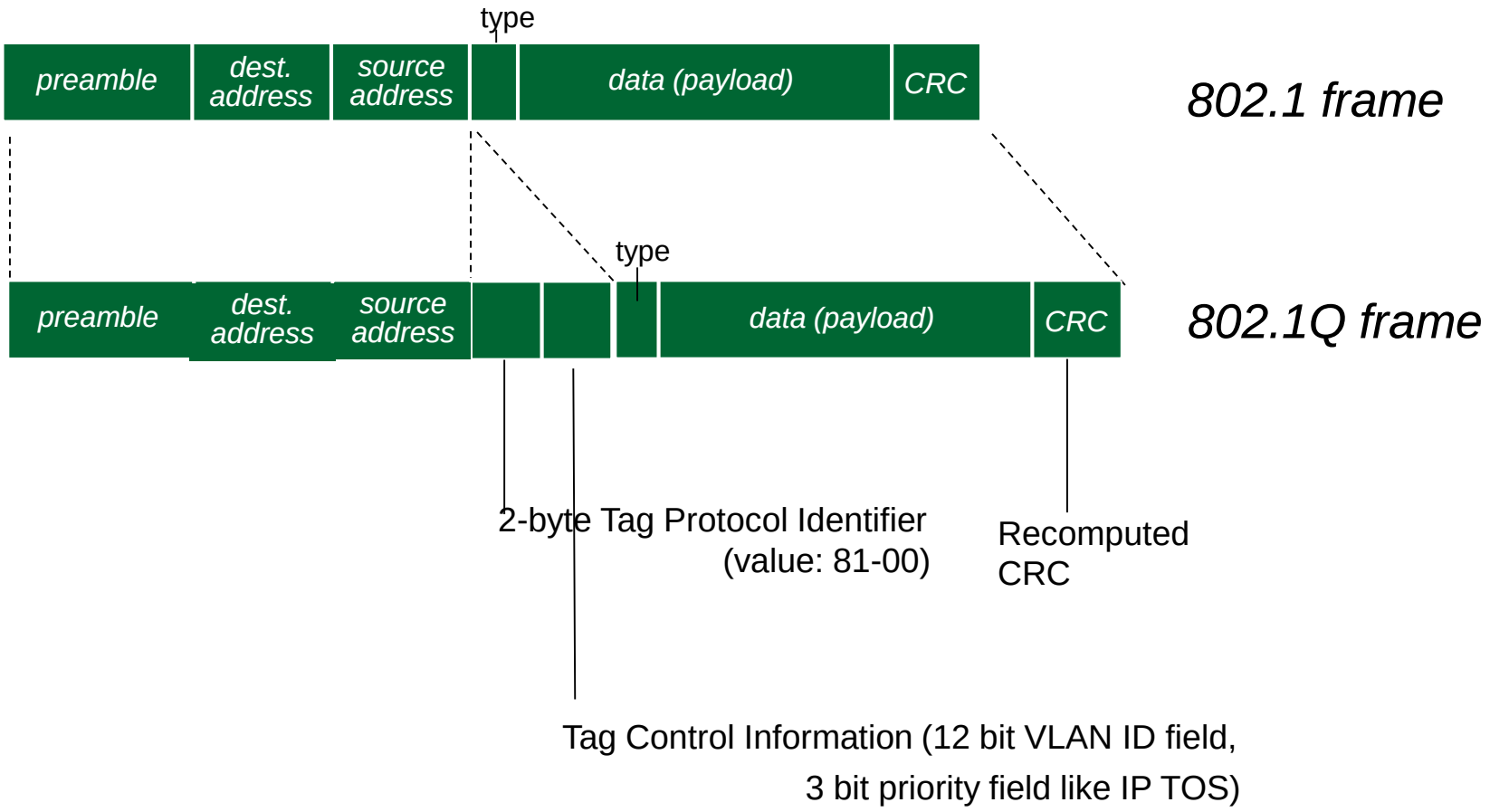


VLANS spanning multiple switches



- *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



Link layer, LANs: outline

6.1 Sarrera, zerbitzuak

6.2 Akats detekzioa, zuzenketa

6.3 Atzipen anitzeko protokoloak, multiple access protocols

6.4 LAN-ak

- Helbideen esleipena, ARP
- Ethernet
- switches
- VLANS

6.5 Loturen birtualizazioa: MPLS (Bukaeran)

6.6 data center networking (Bukaeran)

6.7 a day in the life of a web request

Link layer, LANs: outline

6.1 Sarrera, zerbitzuak

6.2 Akats detekzioa, zuzenketa

6.3 Atzipen anitzeko protokoloak, multiple access protocols

6.4 LAN-ak

- Helbideen esleipena, ARP
- Ethernet
- switches
- VLANS

6.5 Loturen birtualizazioa: MPLS (Bukaeran)

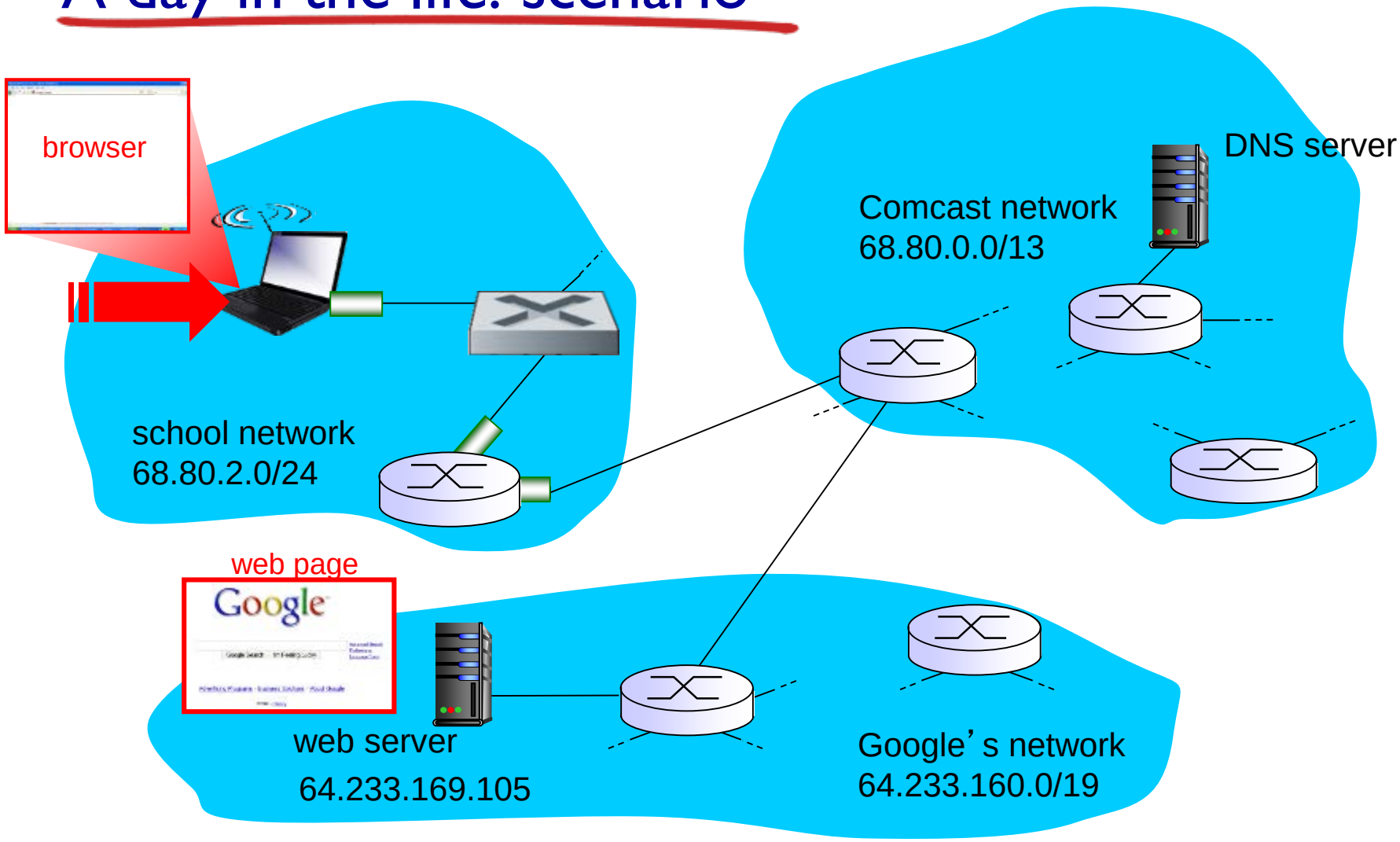
6.6 data center networking (Bukaeran)

6.7 a day in the life of a web request

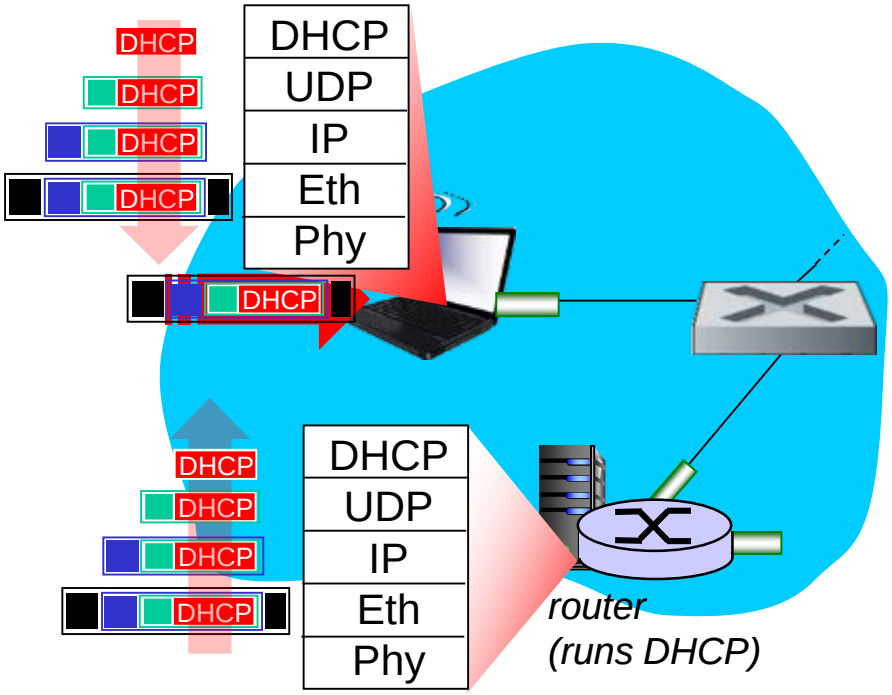
Synthesis: a day in the life of a web request

- Beherantzako bidea bukatu da!
  - aplikazioa, garraioa, sarea, lotura
- Dena batera jarriko dugu: sintesis!
  - *Helburua:* adibide sinple batean agertzen diren geruza guztien protokoloak identifikatu, birpasatu eta ulertu, *Jokalekua:* konexioa www.google.com –era, unibertsitateko wifi sarearen bidez

A day in the life: scenario



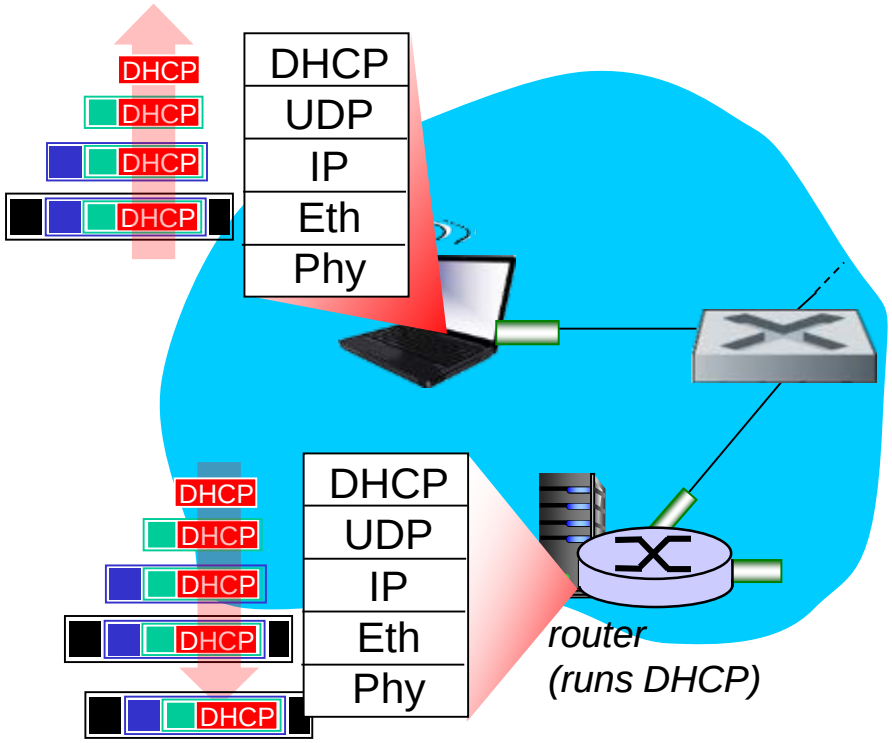
A day in the life… connecting to the Internet



- Konektatzen den eramangarriak horren IP h lortu behar du. Horretarako, Gateway-aren helbidea eta DNS zerbitzariaren helbideak behar dira : *DHCP erabiltzen da*

- DHCP eskaera, UDP-n kapsulatuta, IP-n kapsulatuta, 802.3 Ethernet-ean kapsulatuta
- Ethernet tramaren broadcast (dest: ff:ff:ff:ff:ff:ff) sare lokalean (LAN), DHCP zerbitzaria hartzen duen routerrak jasotzen du
- Ethernet demuxed to IP demuxed, UDP demuxed to DHCP

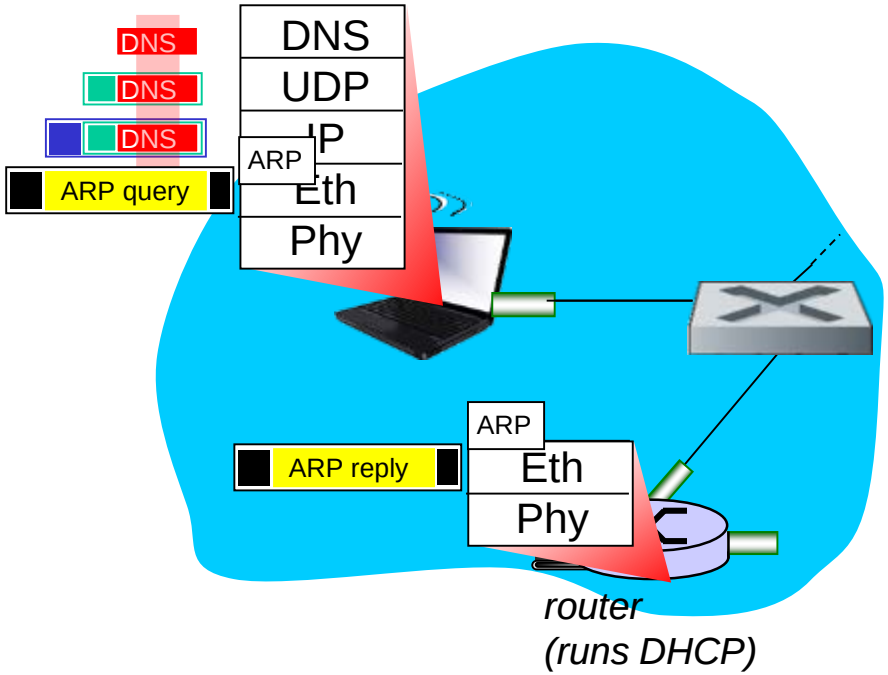
A day in the life… connecting to the Internet



- DHCP zerbitzariak *DHCP ACK* sortzen du, non bezeroaren IP helbidea, Gateway-aren IP helbidea eta DNS zerbitzariaren izen eta helbidea dauden
- Kapsulaketa DHCP zerbitzarian, frame/trama bideratuta (switch learning) LAN zehar, bezeroak demultiplexatzen du
- DHCP bezeroak DHCP ACK erantzuna jasotzen du

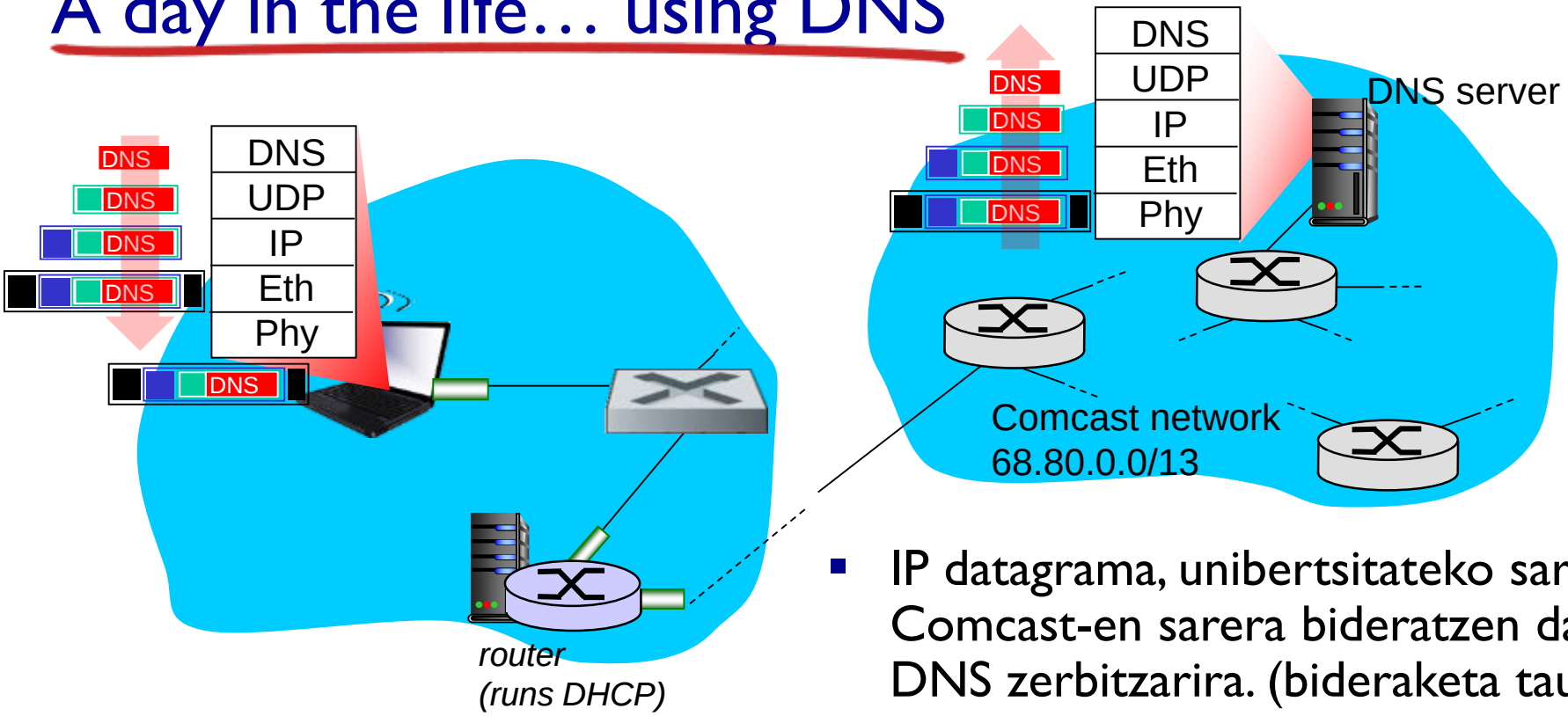
Orain bezeroak IP helbidea du, DNS zerbitzariaren izen eta helbideak ezagutzen ditu baita beraren Gateway-aren IP helbidea (router - lehen jauzia)

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



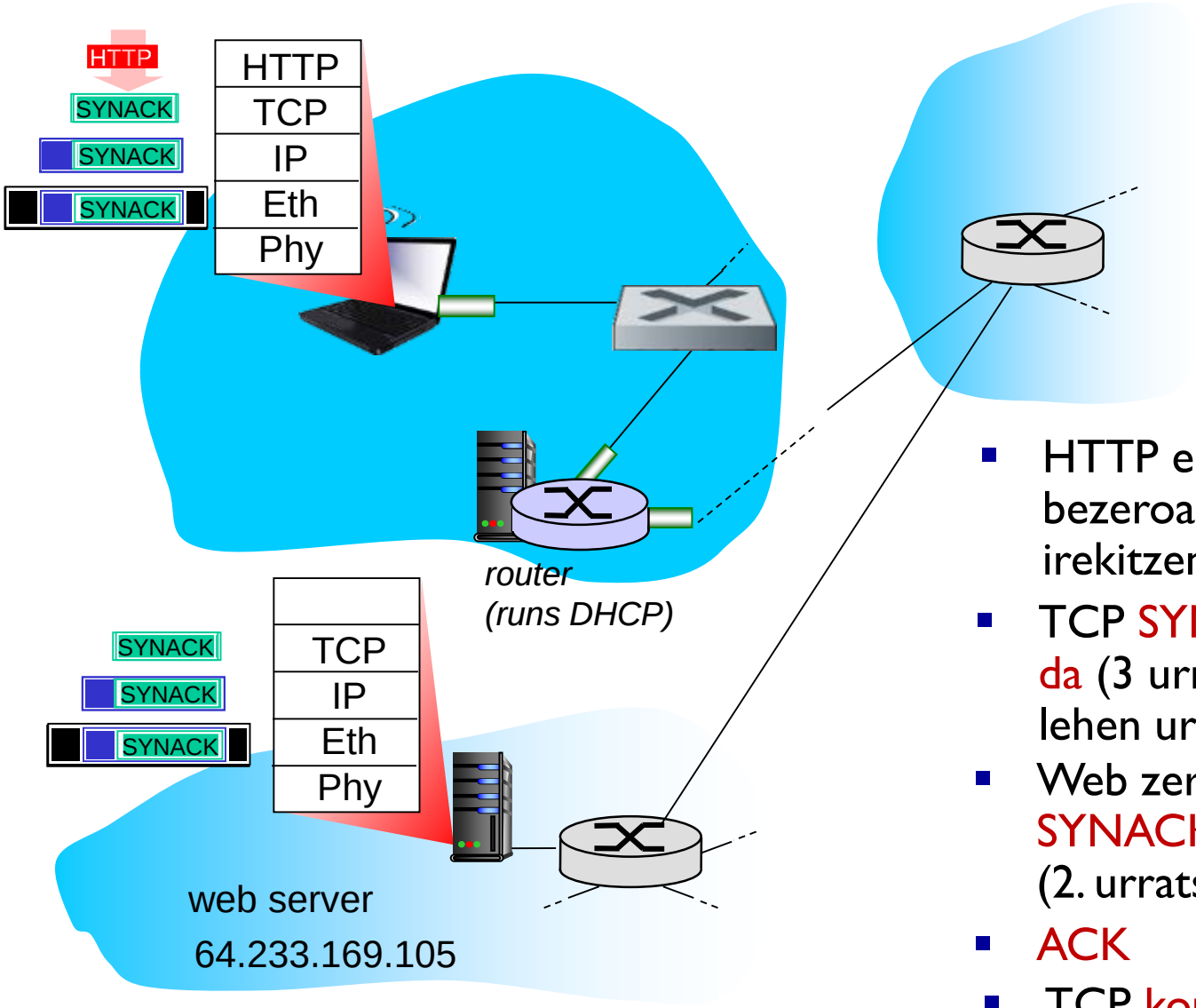
- *HTTP* eskaera bidali aurretik, www.google.com zerbitzariaren IP helbidea behar da: DNS
- DNS eskaera sortzen da, UDP-n kapsulatuta, IP-n kapsulatuta, Eth.-n kapsulatuta. Trama router-era bidaltzeko, router-aren MAC helbidea behar da: ARP
- ARP eskaera broadcast-en, router-ek jasotzen du, eta ARP reply batekin erantzuten du, non router-aren interfazearen MAC helbidea dagoen
- Orain, bezeroak lehen jauziko router-aren (Gateway-aren) MAC helbidea ezagutzen du eta DNS eskaera duen trama bidal dezake

A day in the life… using DNS



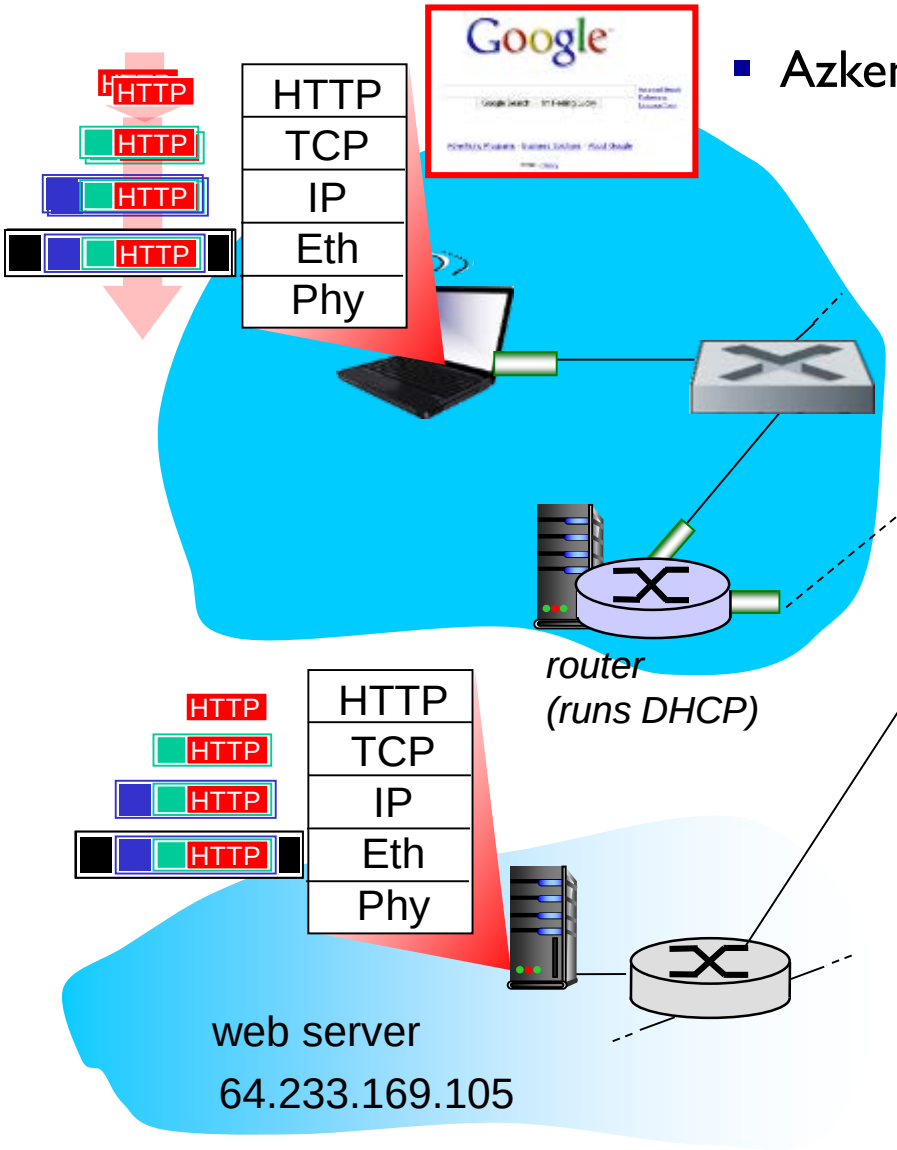
- DNS eskaera duen IP datagrama LAN-aren switch bidez bideratzen da Gateway-ra
- IP datagrama, unibertsitateko saretik Comcast-en sarera bideratzen da, DNS zerbitzarira. (bideraketa taulalk RIP, OSPF, IS-IS edota BGP bideraketa protokoloak erabilita sortzen dira)
- demuxed to DNS zerbitzaria
- DNS zerbitzariak bezeroari erantzuten dio www.google.com-en IP helbidea emanez

A day in the life…TCP connection carrying HTTP



- HTTP eskaera bidaltzeko, bezeroak TCP socket irekitzen du web zerbitzarira
- TCP SYN segmentua bidaltzen da (3 urratseko agurraren lehen urratsa) web zerbitzarira
- Web zerbitzariak TCP SYNACK-ekin erantzuten du (2. urratsa)
- ACK
- TCP konexioa ezarrita!

A day in the life… HTTP request/reply



- Azkenean(!!!) web orria ikusten da

- HTTP eskaera TCP segmentu batean bidaltzen da
- HTTP eskaera duen IP datagrama www.google.com-era bideratzen da
- Web zerbitzariak, HTTP reply prestatzen du (non eskatutako web orria dagoen)
- HTTP erantzuna (TCP barnean) duen IP datagrama bezeroari bidaltzen zaio

Chapter 6: Summary

- principles behind data link layer services:
  - error detection, correction
  - sharing a broadcast channel: multiple access
  - link layer addressing
- instantiation and implementation of various link layer technologies
  - Ethernet
  - switched LANS, VLANs
  - virtualized networks as a link layer: MPLS
- synthesis: a day in the life of a web request

Chapter 6: let's take a breath

- journey down protocol stack *complete* (except PHY)
- solid understanding of networking principles, practice
- ….. could stop here …. but *lots* of interesting topics!
  - wireless
  - multimedia
  - security

Link layer, LANs: outline

6.1 introduction, services

6.2 error detection, correction

6.3 multiple access protocols

6.4 LANs

- addressing, ARP
- Ethernet
- switches
- VLANS

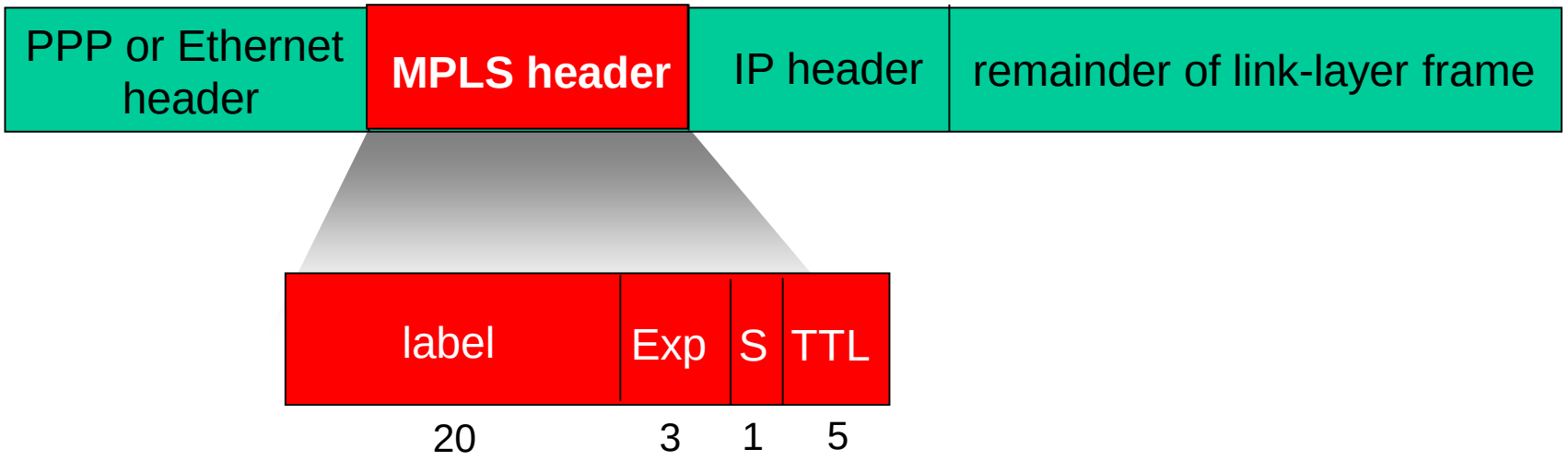
6.5 link virtualization: MPLS

6.6 data center networking

6.7 a day in the life of a web request

Multiprotocol label switching (MPLS)

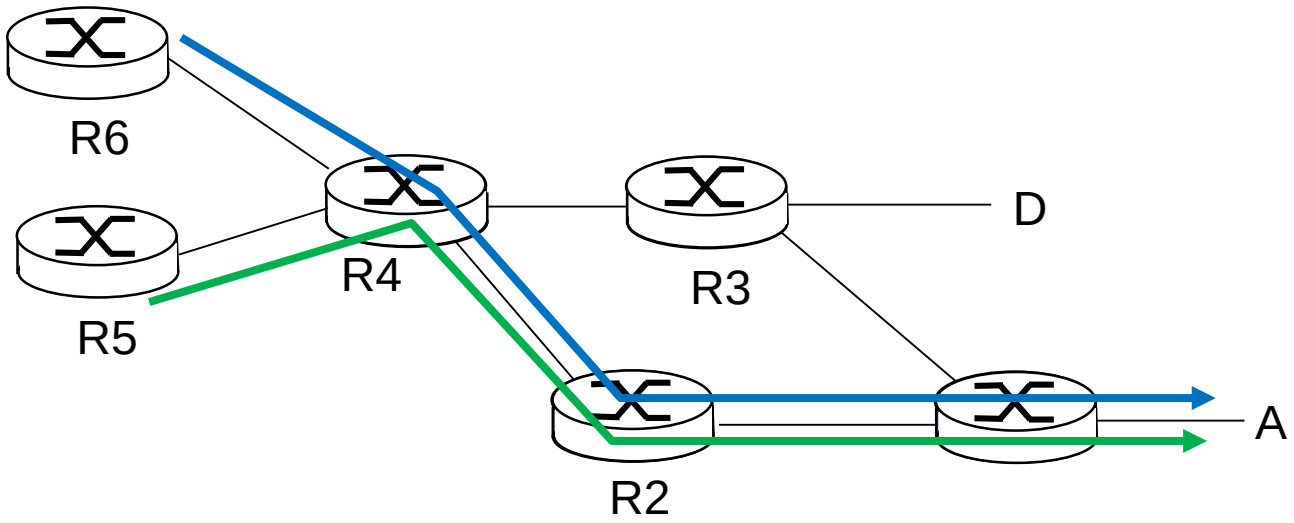
- initial goal: high-speed IP forwarding using fixed length label (instead of IP address)
  - fast lookup using fixed length identifier (rather than shortest prefix matching)
  - borrowing ideas from Virtual Circuit (VC) approach
  - but IP datagram still keeps IP address!



MPLS capable routers

- a.k.a. label-switched router
- forward packets to outgoing interface based only on label value (*don't inspect IP address*)
  - MPLS forwarding table distinct from IP forwarding tables
- *flexibility:* MPLS forwarding decisions can *differ* from those of IP
  - use destination *and* source addresses to route flows to same destination differently (traffic engineering)
  - re-route flows quickly if link fails: pre-computed backup paths (useful for VoIP)

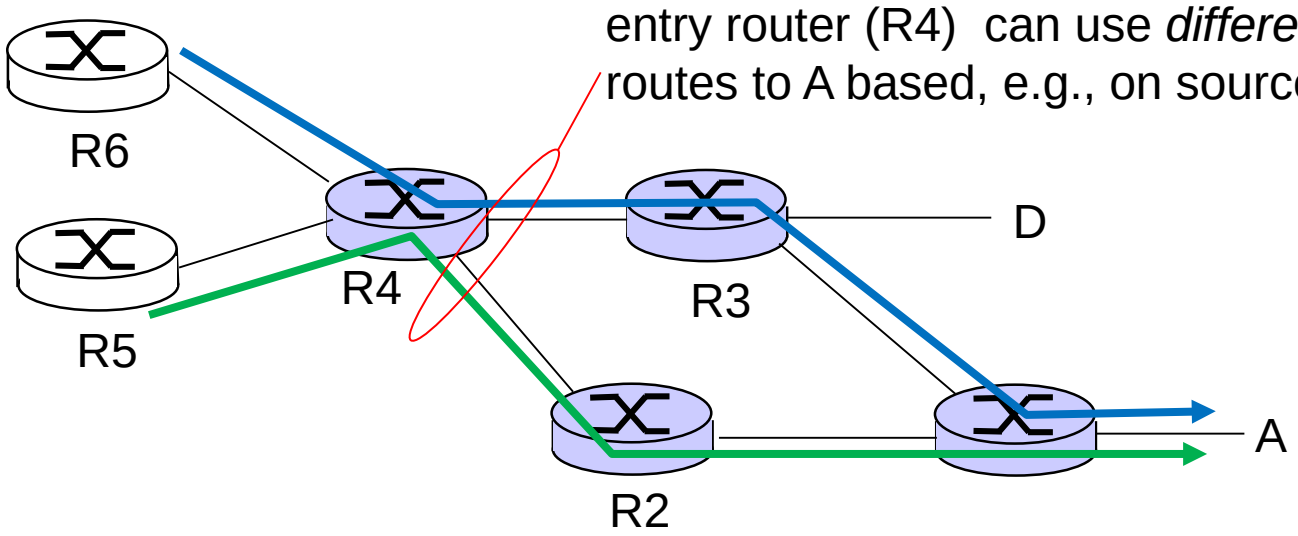
MPLS versus IP paths



- *IP routing: path to destination determined by destination address alone*

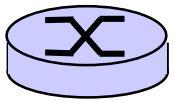

IP router

MPLS versus IP paths



- *IP routing: path to destination determined by destination address alone*
- *MPLS routing:* path to destination can be based on source *and* destination address
  - *fast reroute:* precompute backup routes in case of link failure

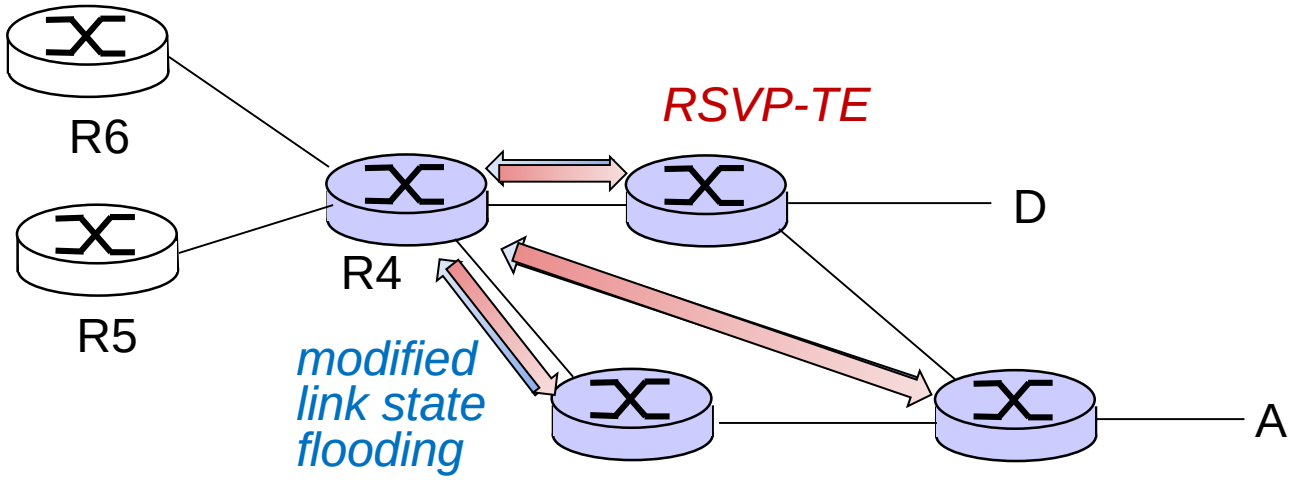
IP-only router



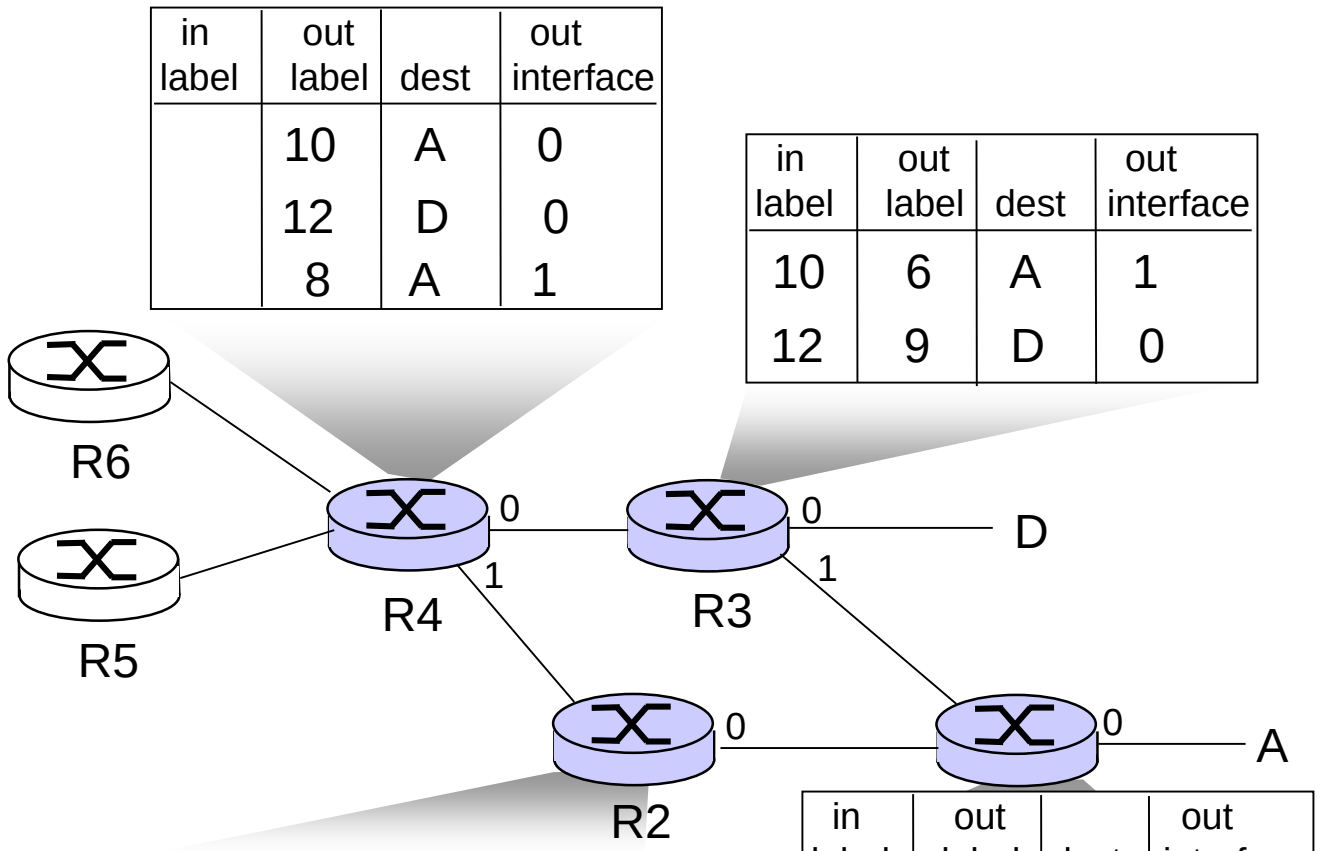
MPLS and IP router

MPLS signaling

- modify OSPF, IS-IS link-state flooding protocols to carry info used by MPLS routing,
  - e.g., link bandwidth, amount of "reserved" link bandwidth
- *entry MPLS router uses RSVP-TE signaling protocol to set up MPLS forwarding at downstream routers*



MPLS forwarding tables



Link layer, LANs: outline

6.1 introduction, services

6.2 error detection, correction

6.3 multiple access protocols

6.4 LANs

- addressing, ARP
- Ethernet
- switches
- VLANS

6.5 link virtualization: MPLS

6.6 data center networking

6.7 a day in the life of a web request

Data center networks

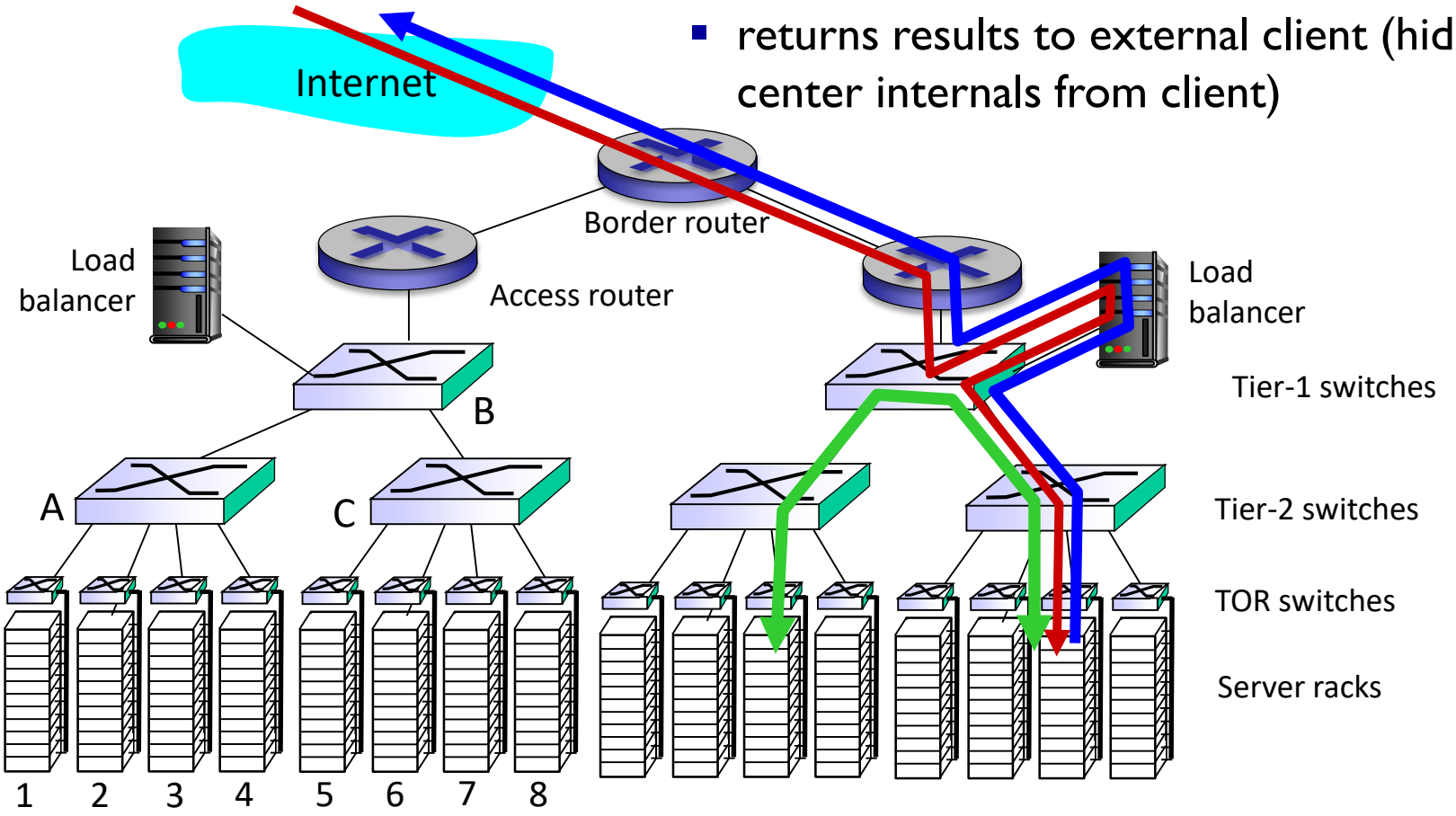
- 10's to 100's of thousands of hosts, often closely coupled, in close proximity:
  - e-business (e.g. Amazon)
  - content-servers (e.g., YouTube, Akamai, Apple, Microsoft)
  - search engines, data mining (e.g., Google)
- challenges:
  - multiple applications, each serving massive numbers of clients
  - managing/balancing load, avoiding processing, networking, data bottlenecks

Inside a 40-ft Microsoft container, Chicago data center

Data center networks

load balancer: application-layer routing

- receives external client requests
- directs workload within data center
- returns results to external client (hiding data center internals from client)



Data center networks

- rich interconnection among switches, racks:
  - increased throughput between racks (multiple routing paths possible)
  - increased reliability via redundancy