usfCS
UNIVERSITY of SAN FRANCISCO
department of computer science

CS 683
Computer Security and Privacy

EJ Jung

Announcements

- Step 1 of the lab is due on Tuesday, August 28
- Details at
  - http://www.cs.usfca.edu/~ejung/courses/683/assignments.html
- Readings
  - TCP/IP Illustrated, Volume 1: The Protocols, Second Edition
    - Chapter 2, Chapter 7

Extra credit opportunity

- Teach Internet Security at Tenderloin Technology Lab in St. Anthony's Foundation
- First-come first-served
- Replace 1 quiz of your choice (2~2.5%)
- Available dates:
  - One of September Wed 19th, Thur 20th, Mon 24th or Tues 25th, 10am-12noon
  - One of September Monday 17th or Tuesday the 18th, 2-4pm
  - More dates in October and November

Academic Honesty

- Use any sources that you can learn from
- Do NOT use any sources that you copy from
  - cite if you used a reference

- DO NOT CHEAT
  - 1st time: 0 and report to the Dean's office
  - 2nd time: F

usfCS
UNIVERSITY of SAN FRANCISCO
department of computer science

Today's goal: networking

- Half of you might know this already
  - 7 out of 14 have taken Computer Networks
  - fast forward or rewind as you see fit!
- TCP/IP model
  - Link layer/IP/TCP/application

What's the Internet: "nuts and bolts" view


PC


server


wireless laptop


cellular handheld

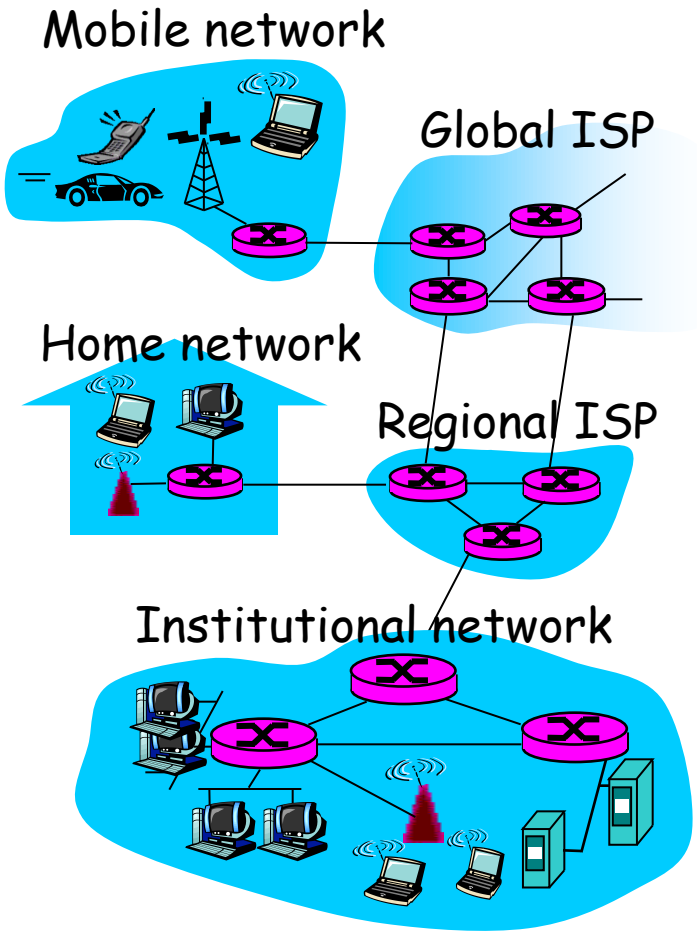
- millions of connected computing devices: *hosts = end systems*
  - running *network apps*
- *communication links*
  - fiber, copper, radio, satellite
  - transmission rate = *bandwidth*

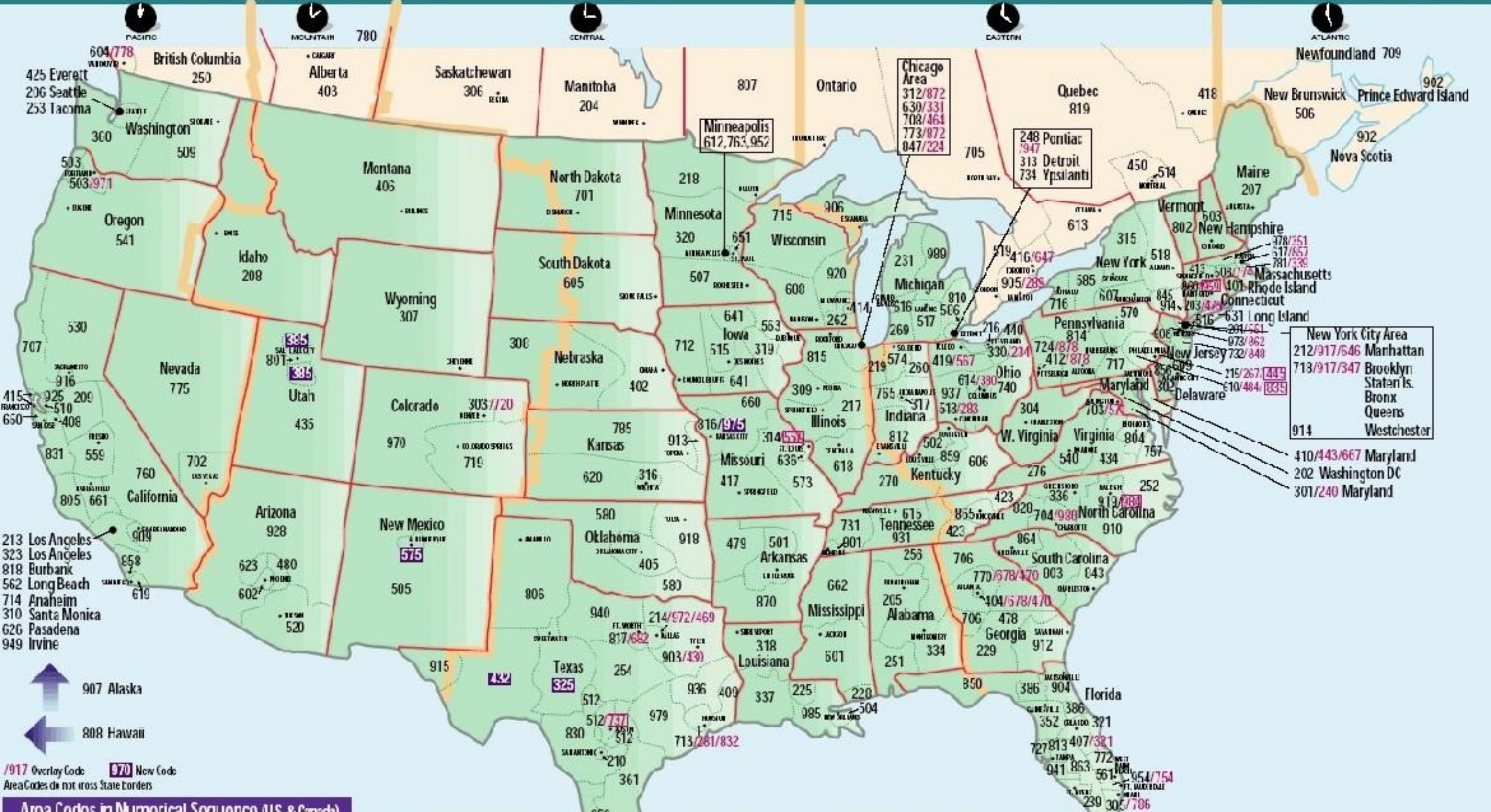

access points

wired links


router

- *routers:* forward packets (chunks of data)





/917 Overlay Code   970 New Code

AreaCodes do not cross State borders

Area Codes in Numerical Sequence (U.S. & Canada)

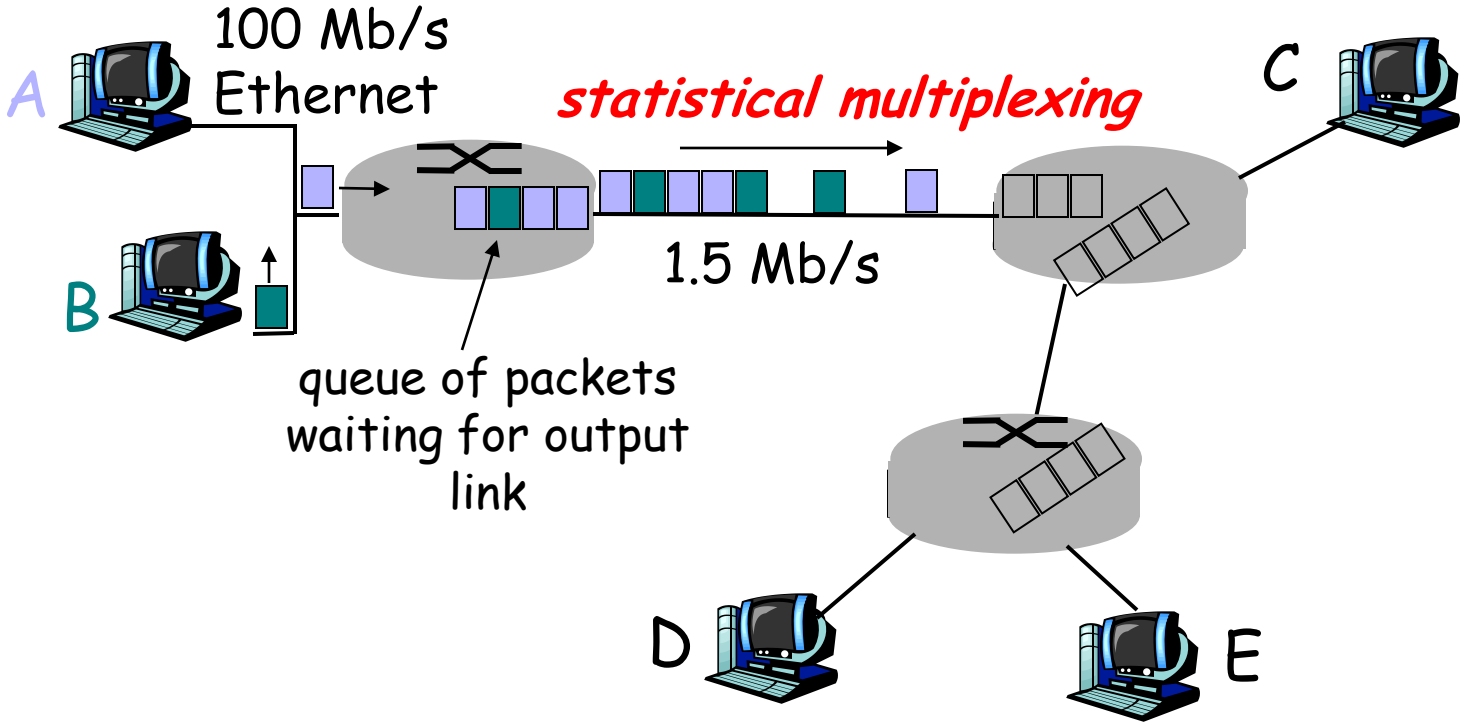
201 NJ	215 PA	248 MI	281 TX	312 IL	331 IL	401 RI	415 CA	445 PA	504 LA	518 NY	570 PA	606 KY	620 KS	662 MS	712 IA	734 MI	778 BC	808 HI	832 TX	863 FL	907 AK	925 CA	959 CT
202 DC	216 OH	250 BC	283 OH	313 MI	334 AL	402 NE	416 ON	450 PQ	505 NM	519 ON	571 VA	607 NY	623 AZ	667 MD	713 TX	737 TX	780 AB	810 MI	835 PA	864 SC	908 NJ	928 AZ	970 CO
203 CT	217 IL	251 AL	289 ON	314 MO	336 NC	403 AB	417 MO	464 IL	506 NB	520 AZ	573 MO	608 WI	626 CA	678 GA	714 CA	740 OH	781 MA	812 IN	843 SC	865 TN	909 CA	931 TN	971 OR
204 MB	218 MN	252 NC	301 MD	315 NY	337 LA	404 GA	418 PQ	469 TX	507 MN	530 CA	574 IN	609 NJ	630 IL	682 TX	715 WI	754 FL	785 KS	813 FL	845 NY	867 NT	910 NC	936 TX	972 TX
205 AL	219 IN	253 WA	302 DE	316 KS	339 MA	405 OK	419 OH	470 GA	508 MA	540 VA	575 NM	610 PA	631 NY	701 ND	716 NY	757 VA	786 FL	814 PA	847 IL	870 AR	912 GA	937 OH	973 NJ
206 WA	224 IL	254 TX	303 CO	317 IN	347 NY	406 MT	423 TN	475 CT	509 WA	541 OR	580 OK	612 MN	636 MO	702 NV	717 PA	760 CA	787 PR	815 IL	848 NJ	872 IL	913 KS	939 PR	975 MO
207 ME	225 LA	256 AL	304 WV	318 LA	351 MA	407 FL	425 WA	478 GA	510 CA	551 NJ	585 NY	613 ON	641 IA	703 VA	718 NY	763 MN	801 UT	816 MO	850 FL	878 PA	914 NY	940 TX	978 MA
208 ID	228 MS	260 IN	305 FL	319 IA	352 FL	408 CA	430 TX	479 AR	512 TX	557 MO	586 MI	614 OH	646 NY	704 NC	719 CO	765 IN	802 VT	817 TX	856 NJ	901 TN	915 TX	941 FL	979 TX
209 CA	229 GA	262 WI	306 SK	320 MN	360 WA	409 TX	432 TX	480 AZ	513 OH	559 CA	601 MS	615 TN	647 ON	705 ON	720 CO	770 GA	803 SC	818 CA	857 MA	902 NS	916 CA	947 MI	980 NC
210 TX	231 MI	267 PA	307 WY	321 FL	361 TX	410 MD	434 VA	484 PA	514 PQ	561 FL	602 AZ	616 MI	650 CA	706 GA	724 PA	772 FL	804 VA	819 PQ	858 CA	903 TX	917 NY	949 CA	984 NC
212 NY	234 OH	269 MI	308 NE	323 CA	380 OH	412 PA	435 UT	501 AR	515 IA	562 CA	603 NH	617 MA	651 MN	707 CA	727 FL	773 IL	805 CA	828 NC	859 KY	904 FL	918 OK	952 MN	985 LA
213 CA	239 FL	270 KY	309 IL	325 TX	385 UT	413 MA	440 OH	502 KY	516 NY	563 IA	604 BC	618 IL	660 MO	708 IL	731 TN	774 MA	806 TX	830 TX	860 CT	905 ON	919 NC	954 FL	989 MI
214 TX	240 MD	276 VA	310 CA	330 OH	386 FL	414 WI	443 MD	503 OR	517 MI	567 OH	605 SD	619 CA	661 CA	709 NF	732 NJ	775 NV	807 ON	831 CA	862 NJ	906 MI	920 WI	956 TX	

Caribbean & Other Islands

242	Bahamas	670	C.N.M.I.
246	Barbados	671	Guam
264	Anguilla	758	St.Lucia
268	Antigua/Barbuda	767	Dominica
284	B.V.I.	784	St.Vincent
340	U.S.V.I.	787/939	Puerto Rico
345	Cayman Islands	809	Dominican Republic
441	Bermuda	868	Trinidad & Tobago
473	Grenada	869	St.Kitts & Nevis
649	Turks & Caicos	876	Jamaica
664	Montserrat		

New Codes		Effective Dates	Old Codes
325	TX	4/5/03	915
432	TX	4/5/03	915
385	UT	3/30/03	801
575	NM	6/1/03	505
984	NC	TBD	919
975	MO	TBD	816
557	MO	TBD	314
445	PA	TBD	215,267
835	PA	TBD	610,484
475	CT	TBD	203
959	CT	TBD	860
737	TX	TBD	512

Packet Switching: Statistical Multiplexing

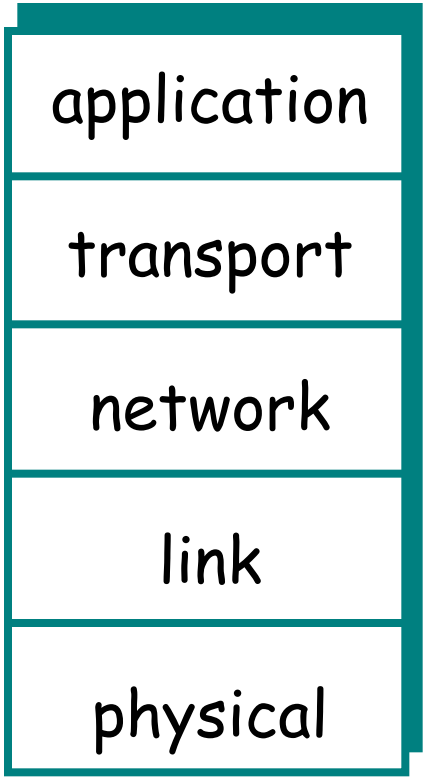


Sequence of A & B packets does not have fixed pattern, bandwidth shared on demand ➔ ***statistical multiplexing***.

TDM: each host gets same slot in revolving TDM frame.

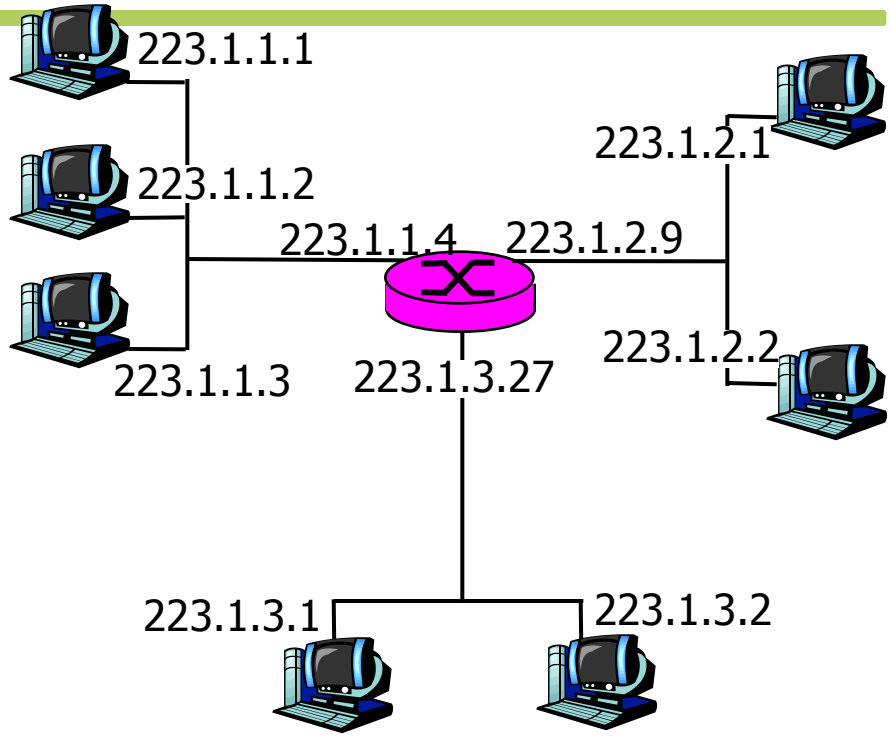
Internet protocol stack

- application: supporting network applications
  - FTP, SMTP, HTTP
- transport: process-process data transfer
  - TCP, UDP
- network: routing of datagrams from source to destination
  - IP, routing protocols
- link: data transfer between neighboring network elements
  - PPP, Ethernet
- physical: bits "on the wire"



IP Addressing: introduction

- IP address: 32-bit identifier for host, router *interface*
- *interface:* connection between host/router and physical link
  - router's typically have multiple interfaces
  - host typically has one interface
  - IP addresses associated with each interface

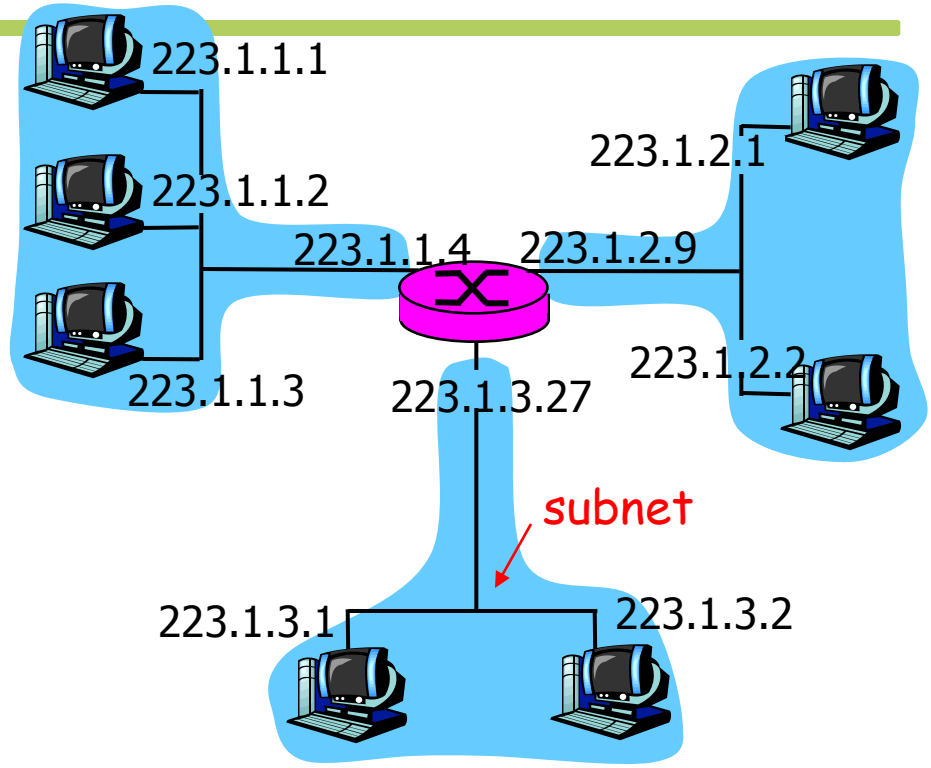


223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

Subnets

- IP address:
  - subnet part (high order bits)
  - host part (low order bits)
- *What's a subnet ?*
  - device interfaces with same subnet part of IP address
  - can physically reach each other without intervening router

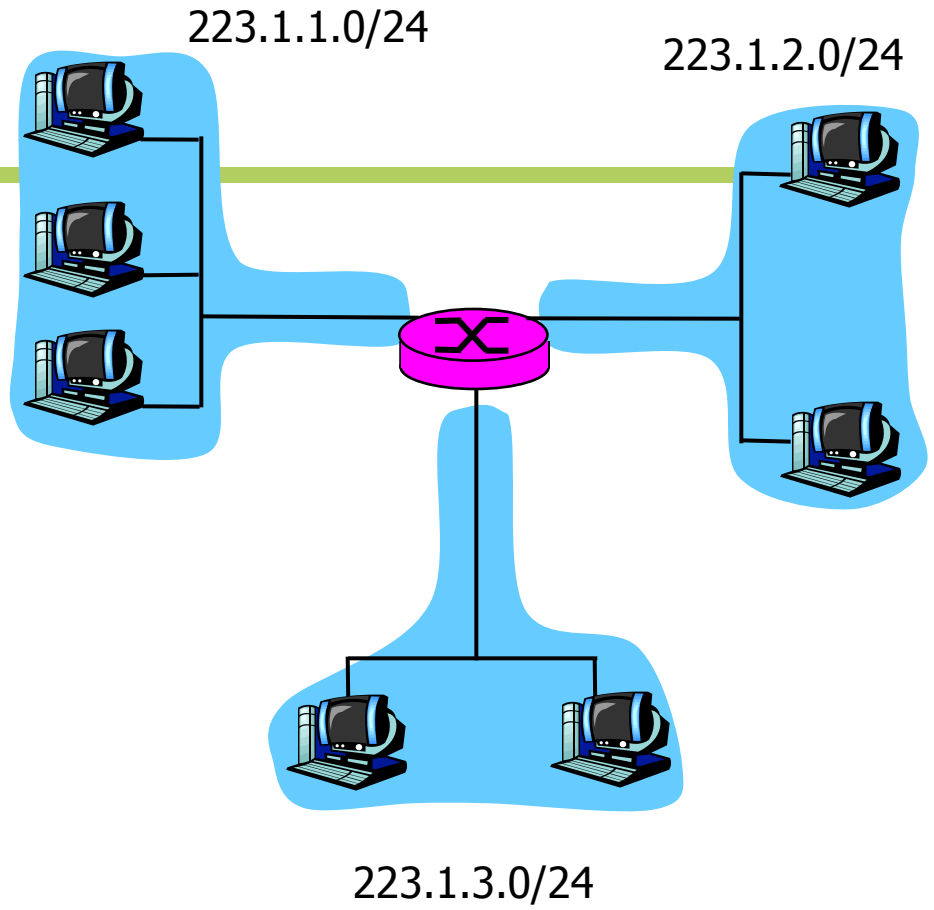


network consisting of 3 subnets

Subnets

Recipe

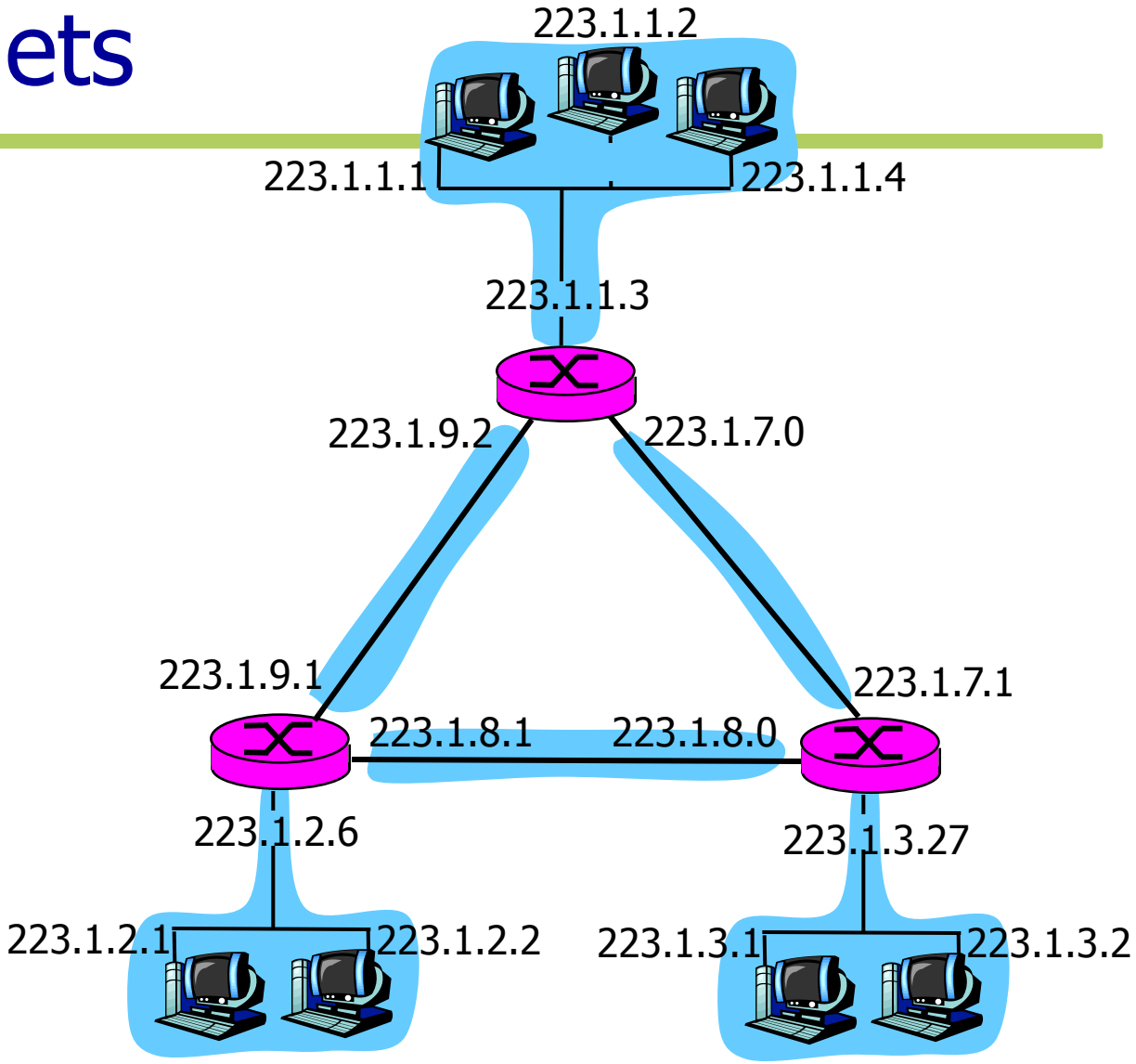
- To determine the subnets, detach each interface from its host or router, creating islands of isolated networks. Each isolated network is called a subnet.



Subnet mask: /24

Subnets

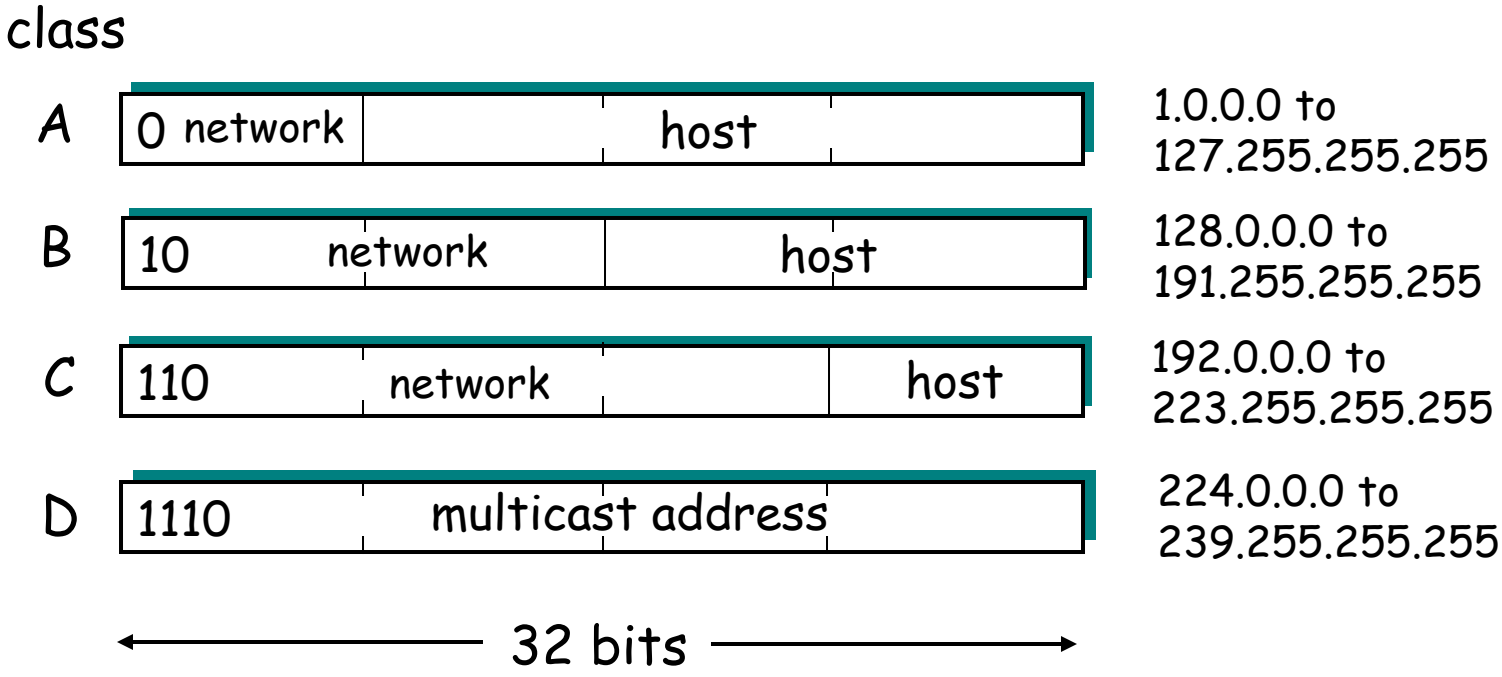
How many?



IP Addressing

given notion of "network", let's re-examine IP addresses:

"class-ful" addressing in the original IP design:



IP Addressing: CIDR

- (Static)classful addressing:
  - inefficient use of address space, address space exhaustion
    - e.g., a class A net allocated enough addresses for 16 million hosts, even if only 2K hosts in that network
  - not flexible for aggregation

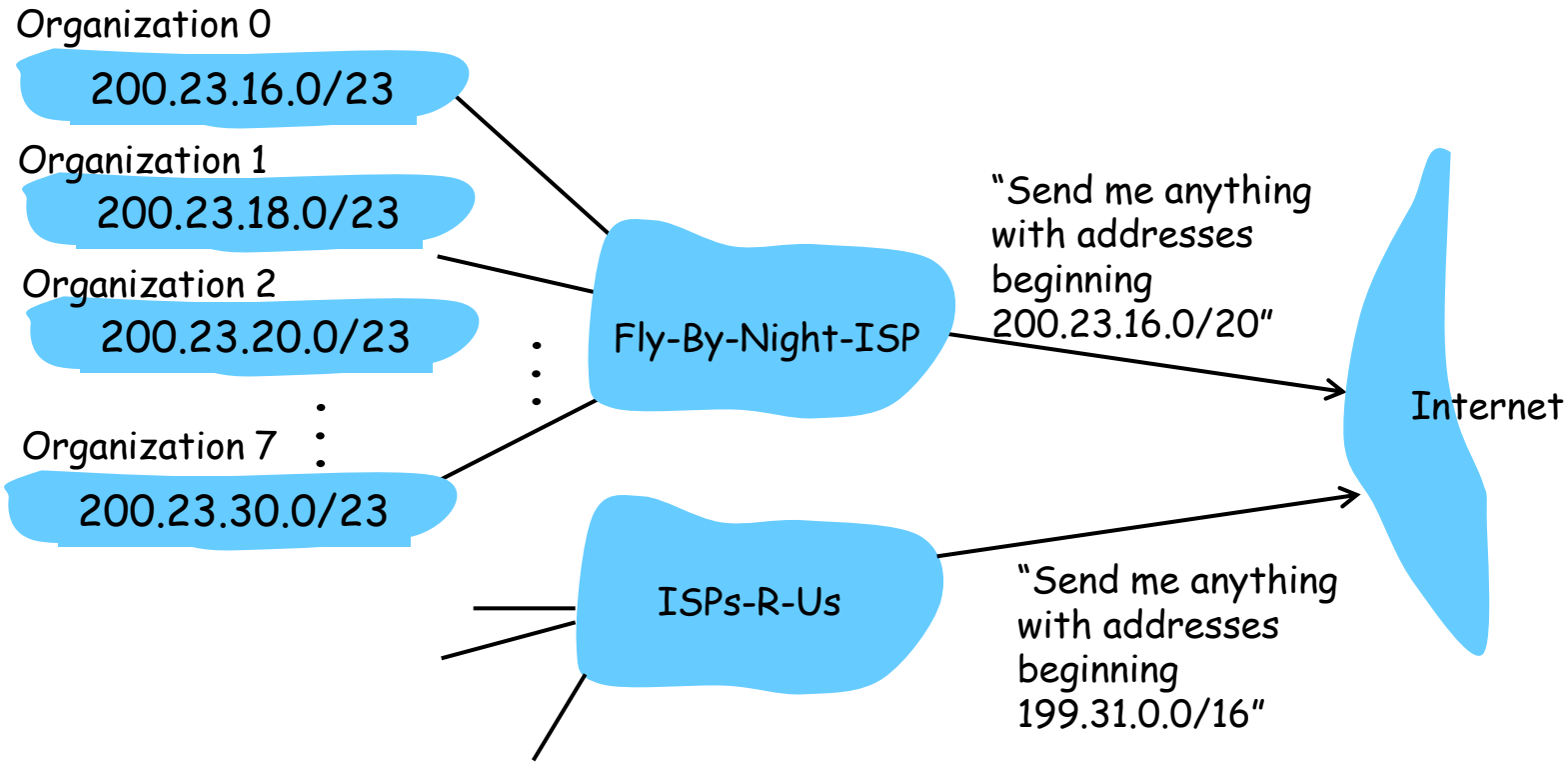
- CIDR: Classless InterDomain Routing
  - network portion of address of arbitrary length
  - address format: a.b.c.d/x, where x is # bits in network portion of address

200.23.16.0/23

Some systems use mask, instead of the /x format

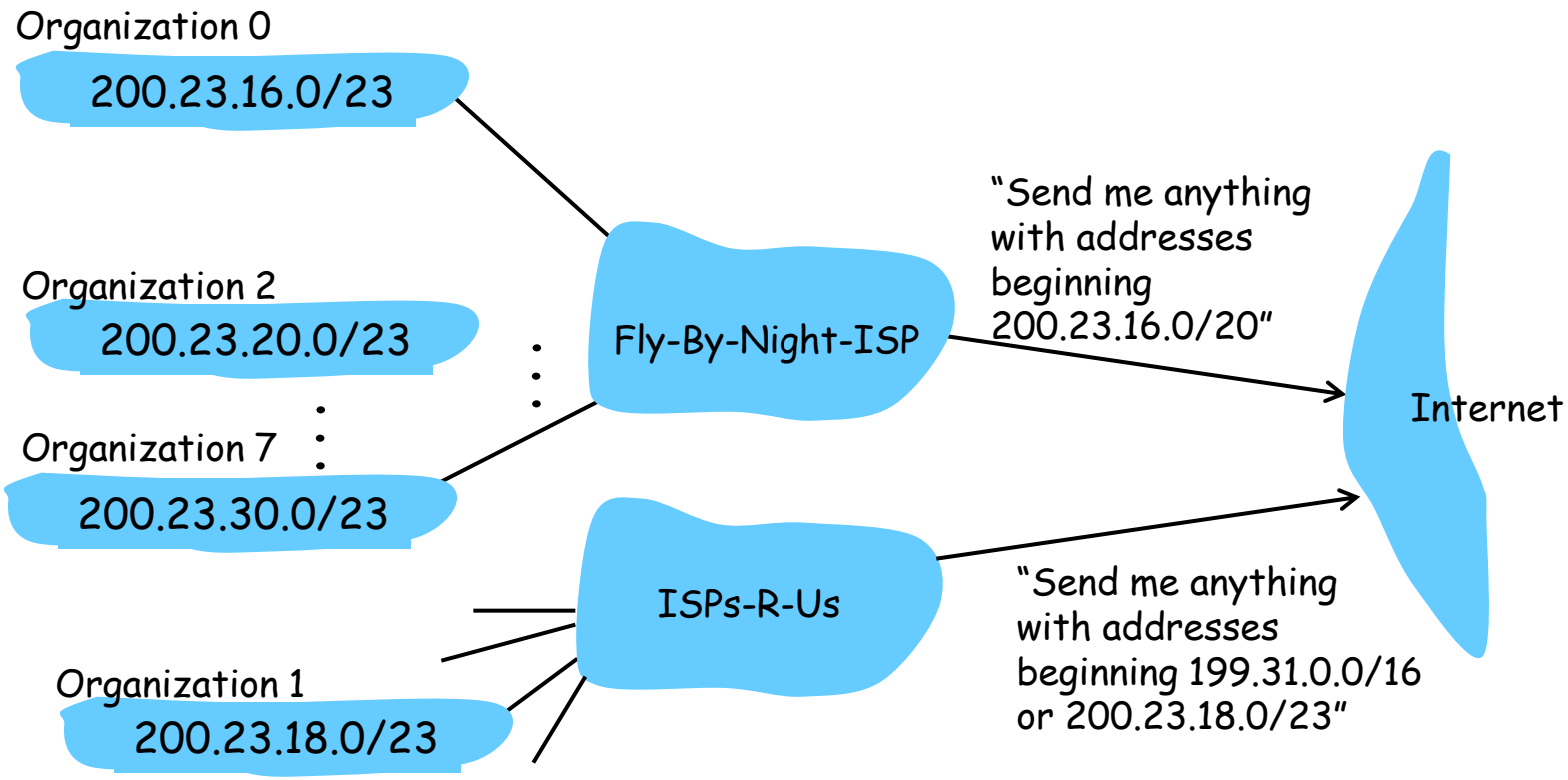
Hierarchical addressing: route aggregation

Hierarchical addressing allows efficient advertisement of routing information:

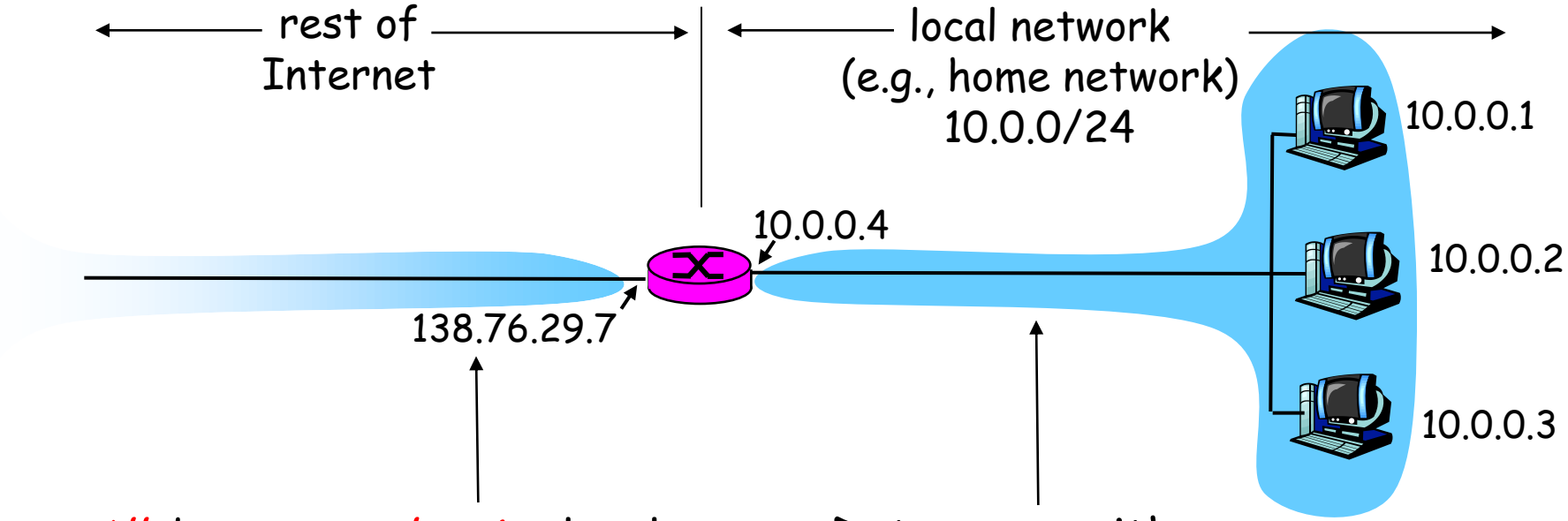


Hierarchical addressing: more specific routes

ISPs-R-Us has a more specific route to Organization 1



NAT: Network Address Translation



All datagrams *leaving* local network have same single source NAT IP address: 138.76.29.7, different source port numbers

Datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)

NAT: Network Address Translation

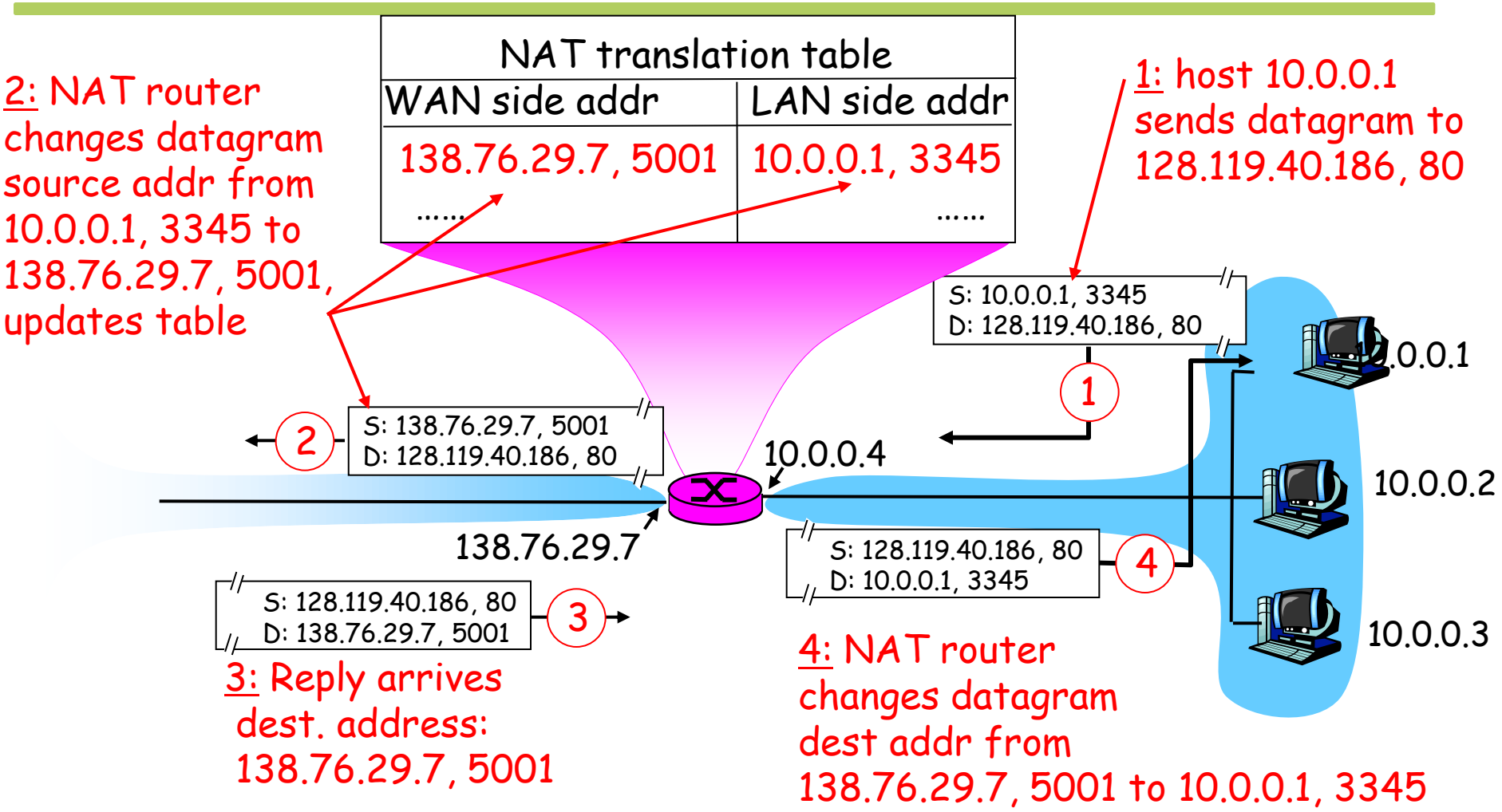
- Motivation: local network uses just one IP address as far as outside world is concerned:
  - range of addresses not needed from ISP: just one IP address for all devices
  - can change addresses of devices in local network without notifying outside world
  - can change ISP without changing addresses of devices in local network
  - devices inside local net not explicitly addressable, visible by outside world (a security plus).

NAT: Network Address Translation

Implementation: NAT router must:

- *outgoing datagrams: replace* (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)
  - . . . remote clients/servers will respond using (NAT IP address, new port #) as destination addr.
- *remember (in NAT translation table)* every (source IP address, port #) to (NAT IP address, new port #) translation pair
- *incoming datagrams: replace* (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table

NAT: Network Address Translation

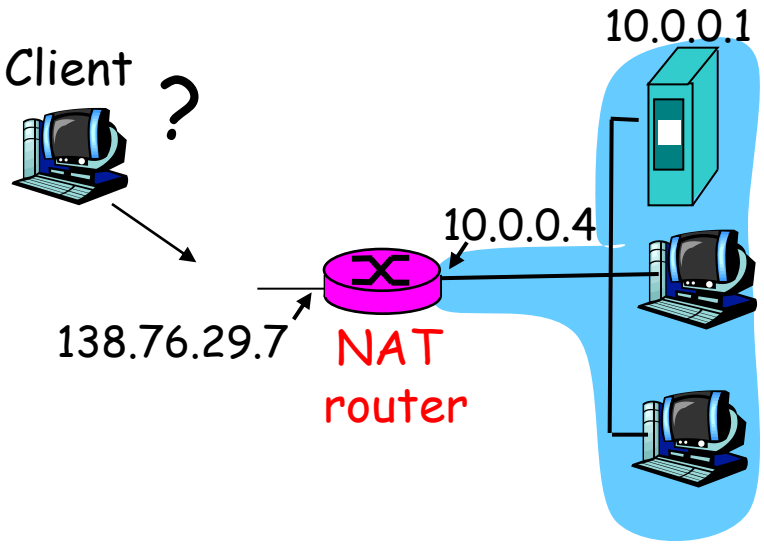


NAT: Network Address Translation

- 16-bit port-number field:
  - 60,000 simultaneous connections with a single LAN-side address!
- NAT is controversial:
  - routers should only process up to Network layer
  - violates end-to-end argument
    - NAT possibility must be taken into account by app designers, eg, P2P applications
  - address shortage should instead be solved by IPv6

NAT traversal problem

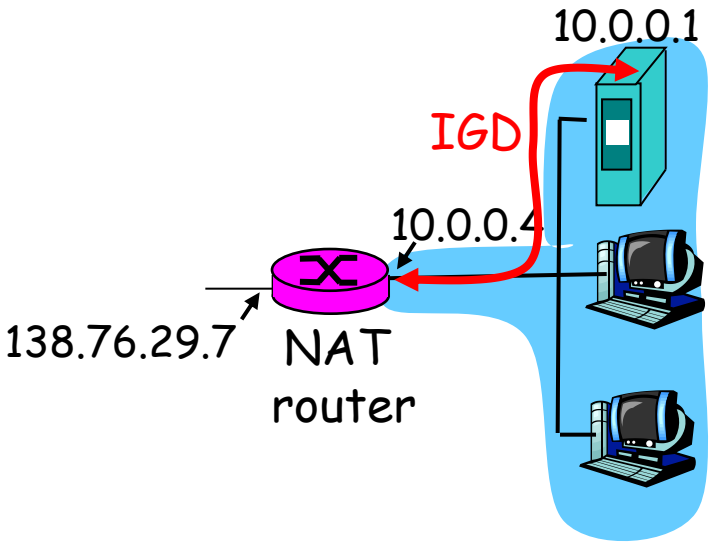
- client want to connect to server with address 10.0.0.1
  - server address 10.0.0.1 local to LAN (client can't use it as destination addr)
  - only one externally visible NATted address: 138.76.29.7
- solution 1: statically configure NAT to forward incoming connection requests at given port to server
  - e.g., (123.76.29.7, port 2500) always forwarded to 10.0.0.1 port 25000



NAT traversal problem

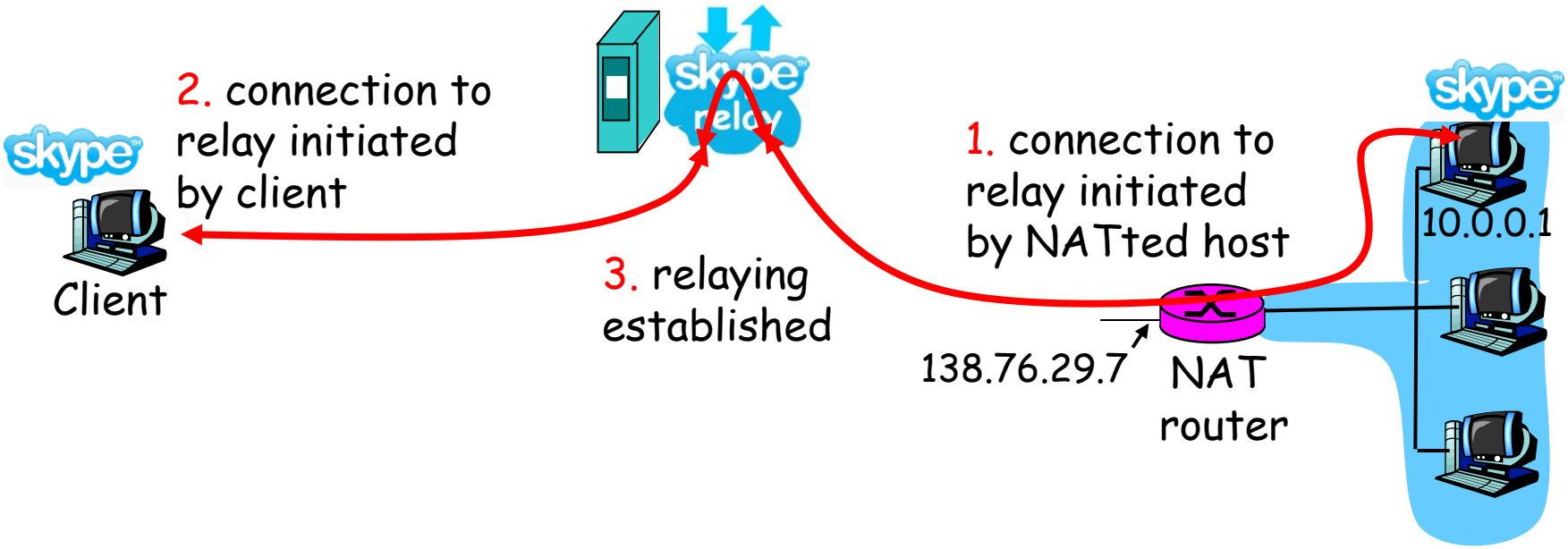
- solution 2: Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Allows NATted host to:
  - learn public IP address (138.76.29.7)
  - enumerate existing port mappings
  - add/remove port mappings (with lease times)

  i.e., automate static NAT port map configuration

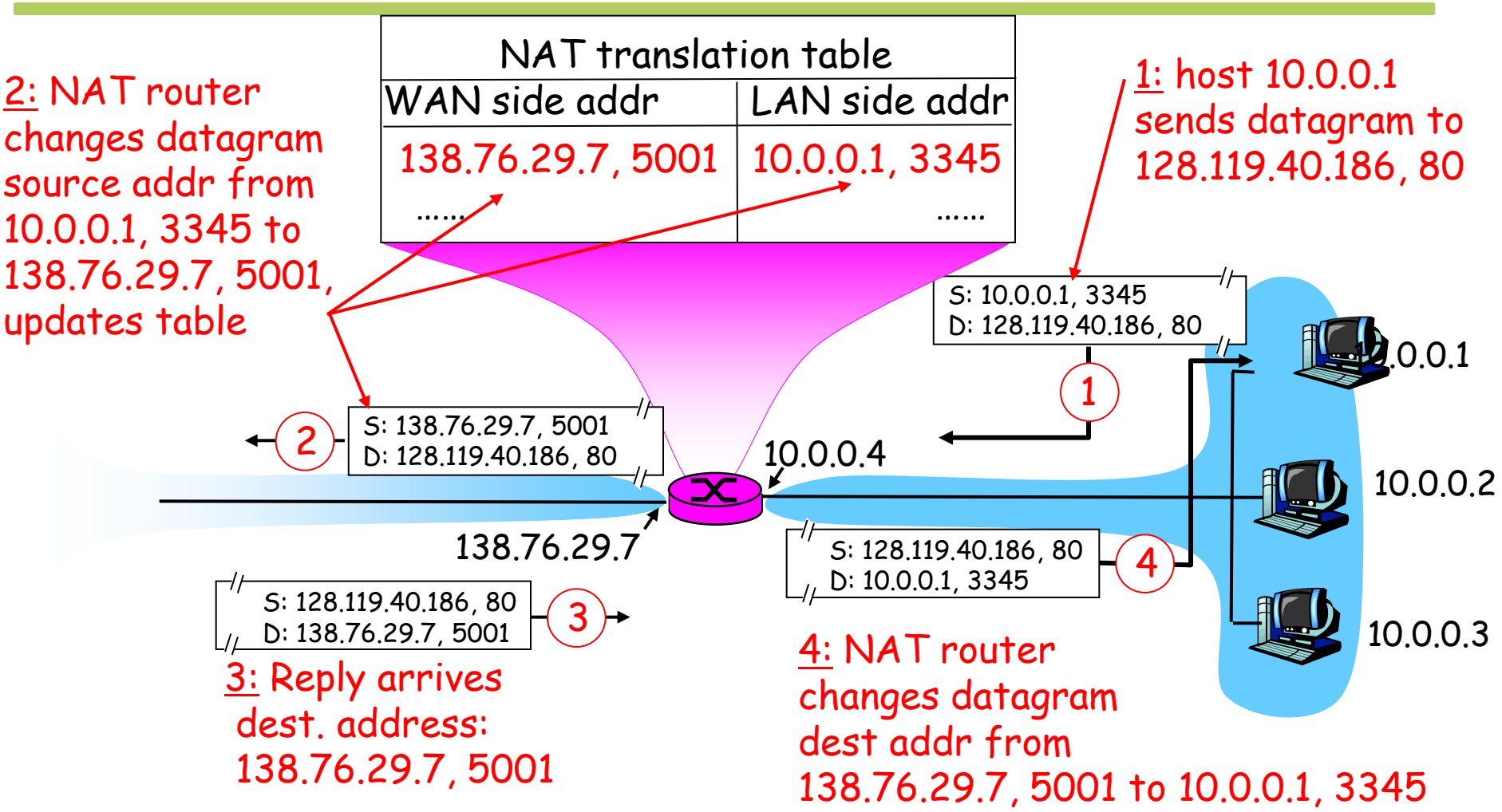


NAT traversal problem

- solution 3: relaying (used in Skype)
  - NATed server establishes connection to relay
  - External client connects to relay
  - relay bridges packets between to connections



NAT: Network Address Translation

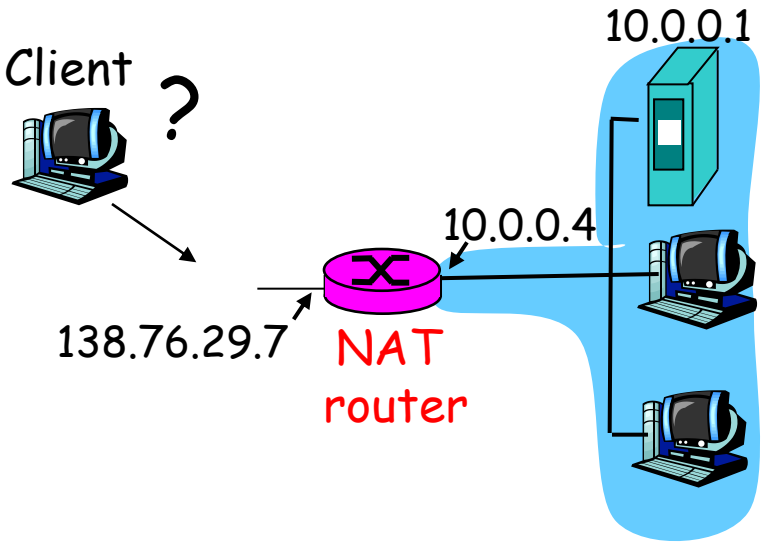


NAT: Network Address Translation

- 16-bit port-number field:
  - 60,000 simultaneous connections with a single LAN-side address!
- NAT is controversial:
  - routers should only process up to Network layer
  - violates end-to-end argument
    - NAT possibility must be taken into account by app designers, eg, P2P applications
  - address shortage should instead be solved by IPv6

NAT traversal problem

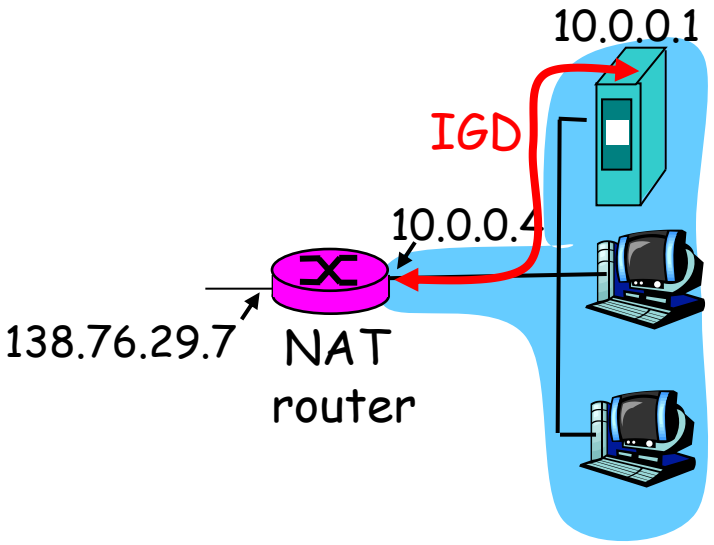
- client want to connect to server with address 10.0.0.1
  - server address 10.0.0.1 local to LAN (client can't use it as destination addr)
  - only one externally visible NATted address: 138.76.29.7
- solution 1: statically configure NAT to forward incoming connection requests at given port to server
  - e.g., (123.76.29.7, port 2500) always forwarded to 10.0.0.1 port 25000



NAT traversal problem

- solution 2: Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Allows NATted host to:
  - learn public IP address (138.76.29.7)
  - enumerate existing port mappings
  - add/remove port mappings (with lease times)

  i.e., automate static NAT port map configuration



NAT traversal problem

- solution 3: relaying (used in Skype)
  - NATed server establishes connection to relay
  - External client connects to relay
  - relay bridges packets between to connections