Jaringan Komputer

Pertemuan 6

Prodi Informatika

1

Outline

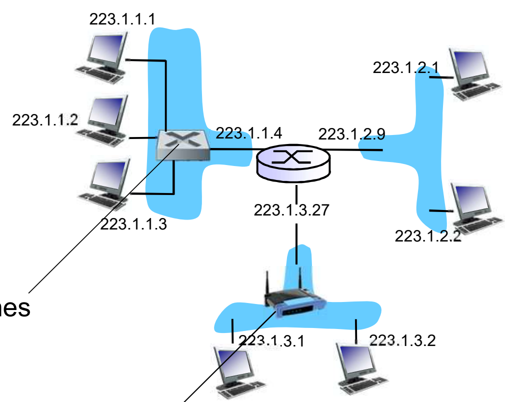
- Network Layer :
  - DHCP
  - Network Address Translation

Prodi Informatika

2

IP addressing: introduction

Q: how are interfaces actually connected?



A: wired Ethernet interfaces connected by Ethernet switches

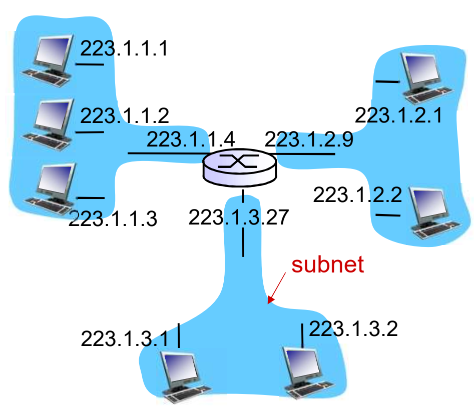
A: wireless WiFi interfaces connected by WiFi base station

Prodi Informatika

3

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

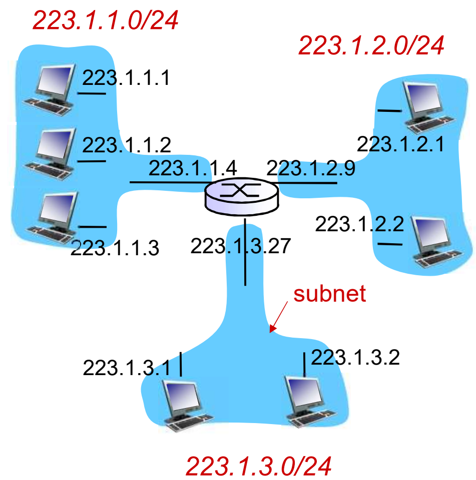
Prodi Informatika

4

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*



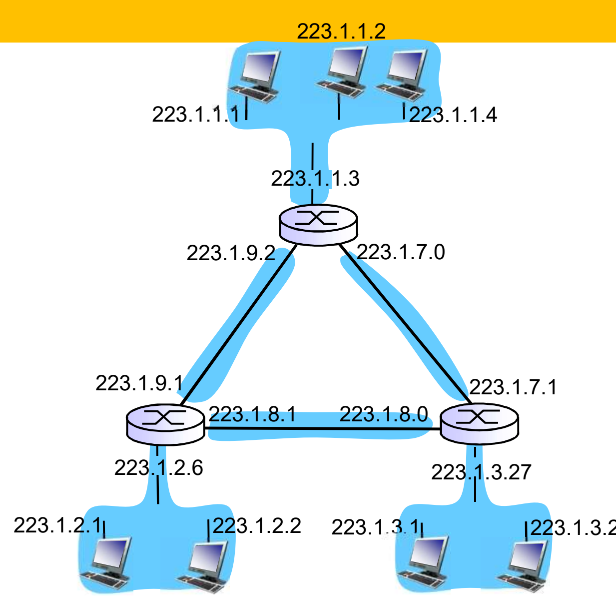
subnet mask: /24

Prodi Informatika

5

Subnets

how many?



Prodi Informatika

6

IP addressing: CIDR

CIDR: Classless InterDomain Routing

- Bagian dari subnet yang Panjang alamatnya bisa kita tentukan sendiri
- address format: a.b.c.d/x, dimana x adalah # bits dibagian alamat subnet

subnet part ←→ host part

11001000 00010111 00010000 00000000

200.23.16.0/23

Prodi Informatika

7

IP addresses: how to get one?

Q: How does a *host* get IP address?

- hard-coded by system admin in a file
  - Windows: control-panel->network->configuration->tcp/ip->properties
  - UNIX: /etc/rc.config
- DHCP: Dynamic Host Configuration Protocol: dynamically get address from as server
  - "plug-and-play"

Prodi Informatika

8

DHCP: Dynamic Host Configuration Protocol

goal: memungkinkan host untuk secara dinamis mendapatkan alamat IP-nya dari server jaringan ketika bergabung dengan jaringan

- dapat memperbarui sewa pada alamat yang digunakan
- memungkinkan penggunaan kembali alamat (hanya tahan alamat saat terhubung / "aktif")
- dukungan untuk pengguna seluler yang ingin bergabung dengan jaringan (lebih singkat)

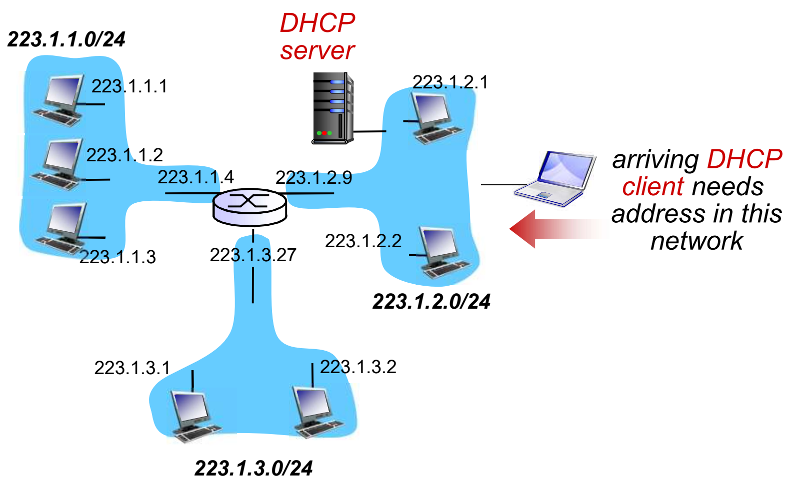
▪ *DHCP overview:*

- host broadcasts "DHCP discover" msg [optional]
- DHCP server responds with "DHCP offer" msg [optional]
- host requests IP address: "DHCP request" msg
- DHCP server sends address: "DHCP ack" msg

Prodi Informatika

9

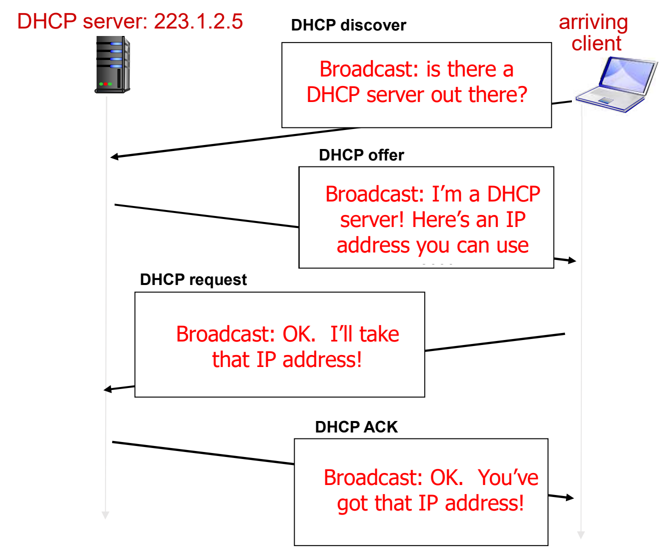
DHCP client-server scenario



Prodi Informatika

10

DHCP client-server scenario



Prodi Informatika

11

DHCP: more than IP addresses

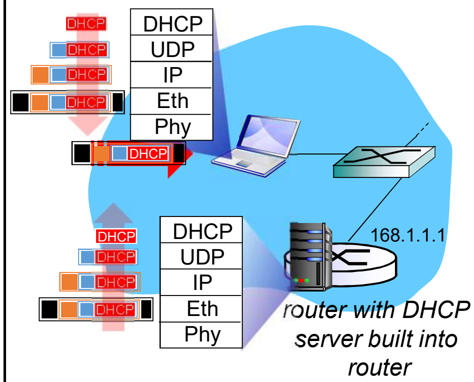
DHCP dapat mengembalikan lebih dari sekadar alamat IP yang dialokasikan pada subnet :

- alamat router *first-hop* untuk klien
- nama dan alamat IP dari server DNS
- mask jaringan (menunjukkan jaringan versus bagian host dari alamat)

Prodi Informatika

12

DHCP: example

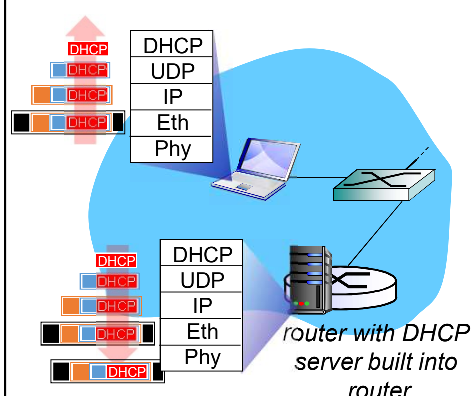


- menghubungkan laptop memerlukan alamat IP-nya, addr first-hop router, addr dari server DNS : use DHCP
- DHCP request dienkapsulasi ke UDP, diencapsulasi ke IP, di enkapsulasi ke 802.1 Ethernet
- Ethernet frame broadcast (dest: FFFFFFFFFFFF) di LAN, diterima di router yang menjalankan server DHCP
- Ethernet demuxed ke IP, UDP demuxed ke DHCP

Prodi Informatika

13

DHCP: example



- DCP server memformulasikan DHCP ACK berisi IP address client, IP address dari first-hop router untuk client, name & IP address DNS server
- encapsulation di DHCP server, frame diforward ke client, demuxing hingga DHCP di klien
- klien sekarang tahu alamat IP-nya, nama dan alamat IP server DNS, alamat IP router first-hop-nya

Prodi Informatika

14

DHCP: Wireshark output (home LAN)

request

Message type: **Boot Request (1)**
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) **DHCP Message Type = DHCP Request**
Option: (61) Client identifier
    Length: 7; Value: 010016D323688A;
    Hardware type: Ethernet
    Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Option: (t=50,l=4) Requested IP Address = 192.168.1.101
Option: (t=12,l=5) Host Name = "nomad"
Option: (55) Parameter Request List
    Length: 11; Value: 010F03062C2E2F1F21F92B
    1 = Subnet Mask; 15 = Domain Name
    3 = Router; 6 = Domain Name Server
    44 = NetBIOS over TCP/IP Name Server
    ……

reply

Message type: **Boot Reply (2)**
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.1.101 (192.168.1.101)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 192.168.1.1 (192.168.1.1)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=54,l=4) Server Identifier = 192.168.1.1
Option: (t=1,l=4) Subnet Mask = 255.255.255.0
Option: (t=3,l=4) Router = 192.168.1.1
Option: (6) Domain Name Server
    Length: 12; Value: 445747E2445749F244574092;
    IP Address: 68.87.71.226;
    IP Address: 68.87.73.242;
    IP Address: 68.87.64.146
Option: (t=15,l=20) Domain Name = "hsd1.ma.comcast.net."

Prodi Informatika

15

IP addresses: how to get one?

Q: how does *network* get subnet part of IP addr?

A: gets allocated portion of its provider ISP's address space

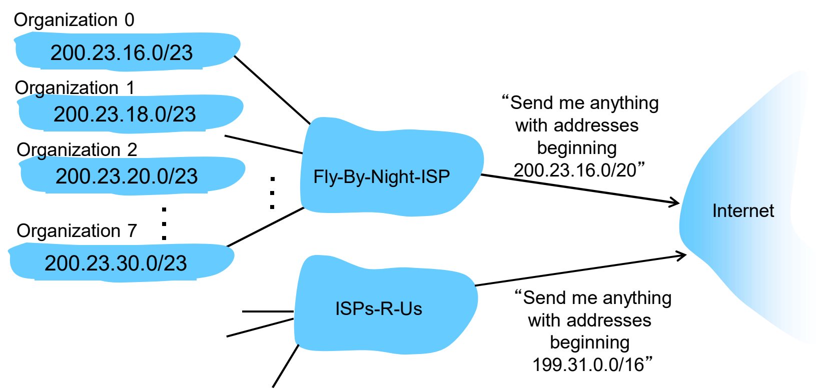
ISP's block	11001000 00010111 00010000	00000000	200.23.16.0/20
Organization 0	11001000 00010111 00010000	00000000	200.23.16.0/23
Organization 1	11001000 00010111 00010010	00000000	200.23.18.0/23
Organization 2	11001000 00010111 00010100	00000000	200.23.20.0/23
...	…..	….	….
Organization 7	11001000 00010111 00011110	00000000	200.23.30.0/23

Prodi Informatika

16

Hierarchical addressing: route aggregation

hierarchical addressing allows efficient advertisement of routing information:

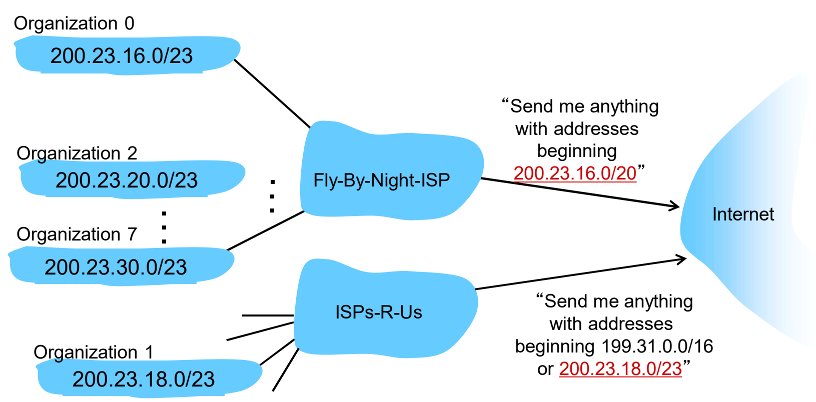


Prodi Informatika

17

Hierarchical addressing: more specific routes

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



Prodi Informatika

18

IP addressing: the last word...

Q: how does an ISP get block of addresses?

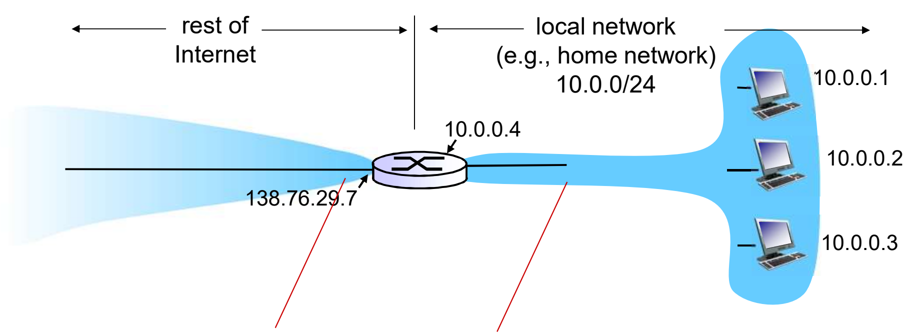
A: ICANN: Internet Corporation for Assigned Names and Numbers http://www.icann.org/

- allocates addresses
- manages DNS
- assigns domain names, resolves disputes

Prodi Informatika

19

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)

Prodi Informatika

20

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)

Prodi Informatika

21

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 #)

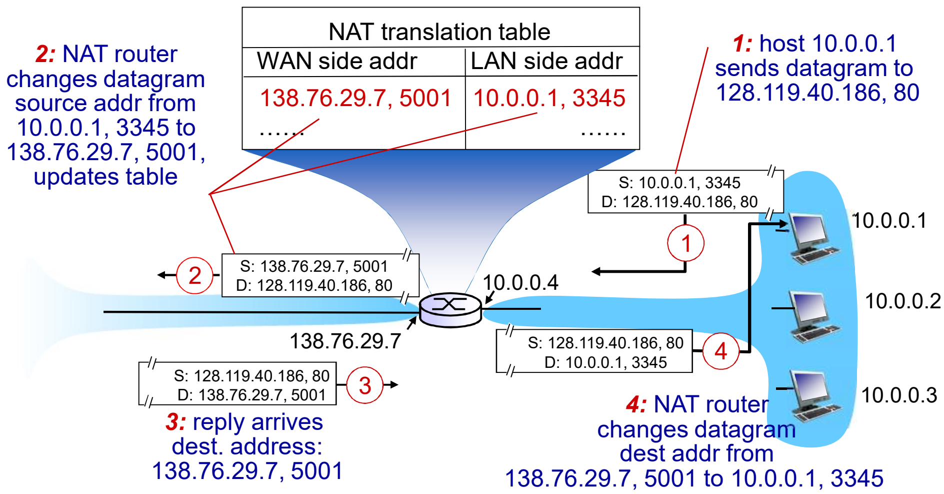
  . . . remote clients/servers will respond using (NAT IP address, new port #) as destination addr

- *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

Prodi Informatika

22

NAT: network address translation



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

Prodi Informatika

23

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 layer 3
  - address shortage should be solved by IPv6
  - violates end-to-end argument
    - ✓ NAT possibility must be taken into account by app designers, e.g., P2P applications
  - NAT traversal: what if client wants to connect to server behind NAT?

Prodi Informatika

24

IPv6: motivation

- *initial motivation:* 32-bit address space soon to be completely allocated.
- additional motivation:
  - header format helps speed processing/forwarding
  - header changes to facilitate QoS

IPv6 datagram format:

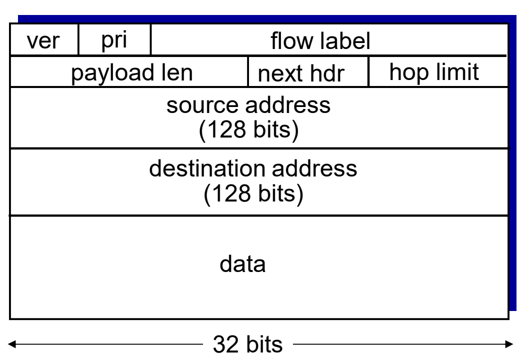
- fixed-length 40 byte header
- no fragmentation allowed

Prodi Informatika

25

IPv6 datagram format

priority: identify priority among datagrams in flow
flow Label: identify datagrams in same "flow."
(concept of "flow" not well defined).
next header: identify upper layer protocol for data



Prodi Informatika

26

Other changes from IPv4

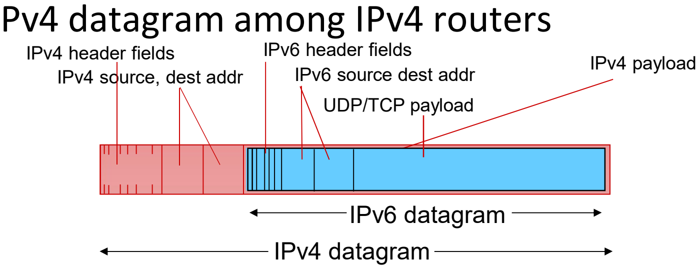
- *checksum*: removed entirely to reduce processing time at each hop
- *options:* allowed, but outside of header, indicated by "Next Header" field
- *ICMPv6:* new version of ICMP
  - additional message types, e.g. "Packet Too Big"
  - multicast group management functions

Prodi Informatika

27

Transition from IPv4 to IPv6

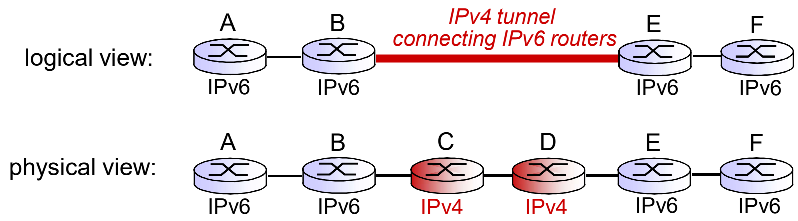
- not all routers can be upgraded simultaneously
  - no "flag days"
  - how will network operate with mixed IPv4 and IPv6 routers?
- *tunneling:* IPv6 datagram carried as *payload* in IPv4 datagram among IPv4 routers



Prodi Informatika

28

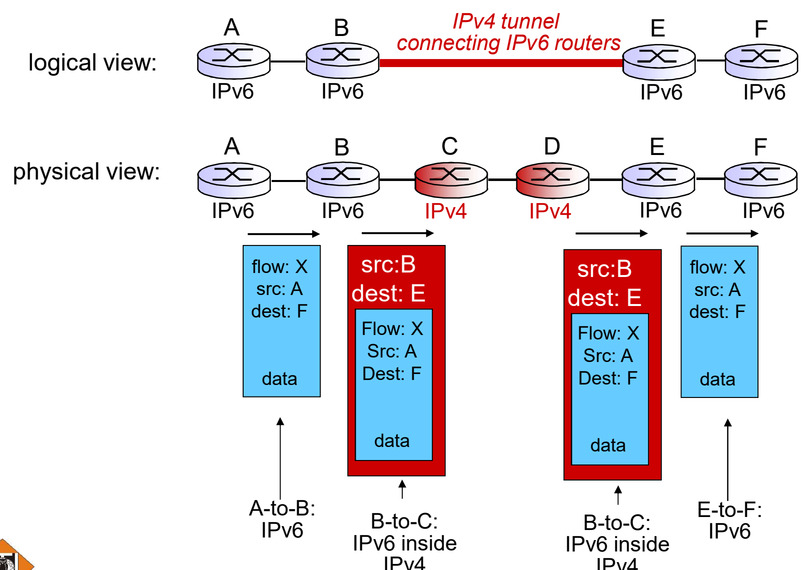
Tunneling



Prodi Informatika

29

Tunneling



Prodi Informatika

30

IPv6: adoption

- Google: 8% of clients access services via IPv6
- NIST: 1/3 of all US government domains are IPv6 capable

- *Long (long!) time for deployment, use*
  - 20 years and counting!
  - think of application-level changes in last 20 years: WWW, Facebook, streaming media, Skype, …
  - *Why?*

Prodi Informatika

31