Introduction to Routing in Internet

Internet basics

IPv4 and ICMP

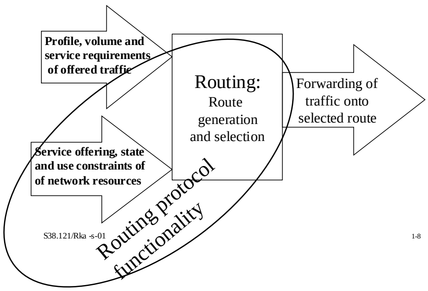
Internet Addressing

ARP - Address Resolution Protocol

Routing Information (Distance Vector) Protocol Principles

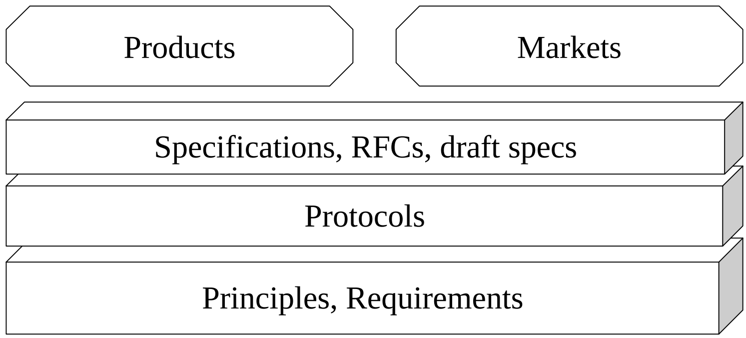
Internet routing is based on routing protocols that collect the input data

Routing process



- No off-line route planning, off-line only dimensioning.
- Routing is fully automated.
- Routing is divided to interior and exterior.
  - This course will concentrate only on Interior routing.
  - S38.191 will talk about exterior routing

Levels of analysis - we deal with principles, protocols and specifications



Internet Architecture Principles
End-to-end principle

by Dave Clark

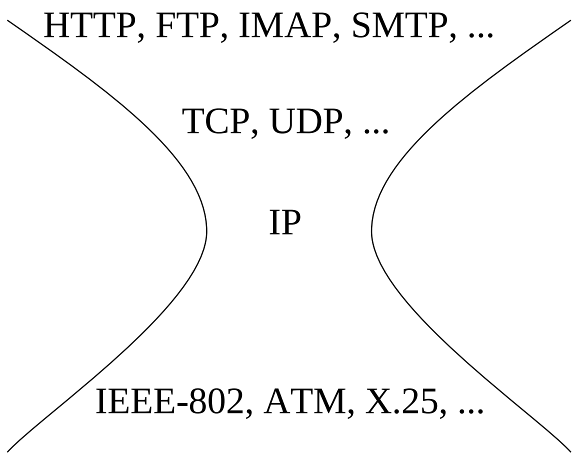
- All control in end stations
  - e.g. error and flow control
- The network can not be trusted
- User must in any case check for errors -> network control redundant
- More reliable transport works for IP
- No state information/connection in the network
  - packets routed independently
- Same principle as in distributed systems

Internet Architecture Principles
IP over everything

- Interconnection based on IP overlay over all kinds of networks
  - framing or encapsulation
  - address resolution
    - IP-address to network address for each transport technology
  - unique IP-address
- Interconnection based on translation:
  - e.g. signalling interworking - inperfect mapping
  - IPv4 to IPv6 mapping!

by Vinston Cerf

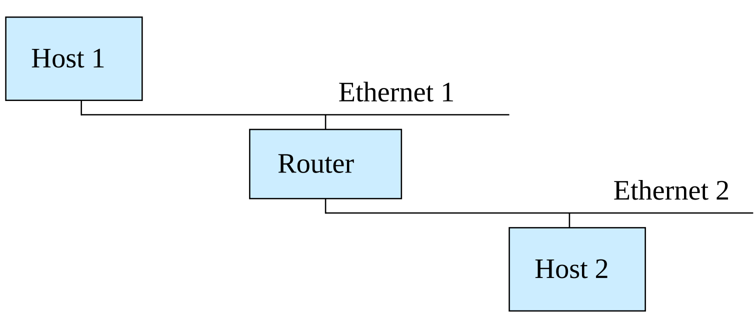
Internet Architecture Principles
IP over everything



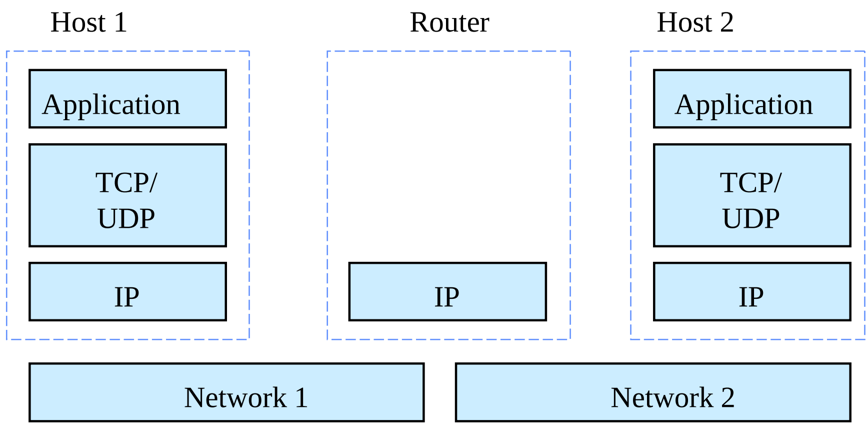
Internet Architecture Principles
Connectivity is its own reward

- The value of a network increases in proportion to the square of the number of nodes on the network (Robert Metcalf's law)
- Be liberal with what you receive, conservative with what you send
  - try to make your best to understand what you receive
  - maximum adherance to standard when sending
- Snowballing effect keeps all interested in connectivity thus keeps adhering to standards

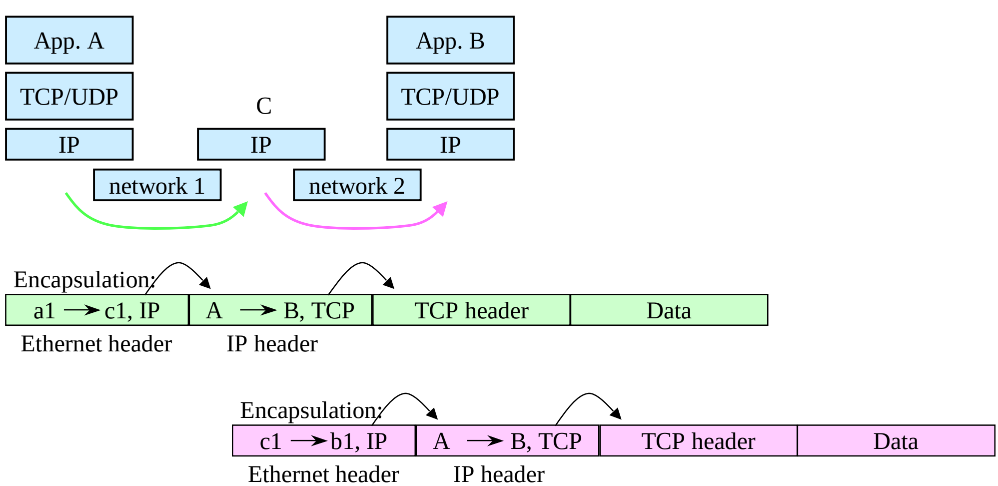
By connecting Ethernet segments with routers the traffic of the segments can be separated



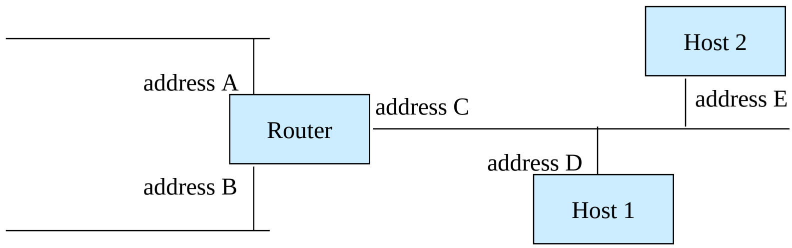
Internet layer model - hosts and routers



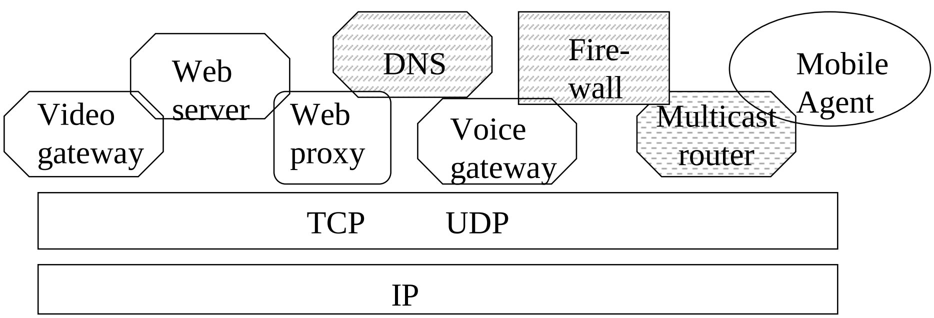
Message forwarding in Internet layers



The IP address defines the interface

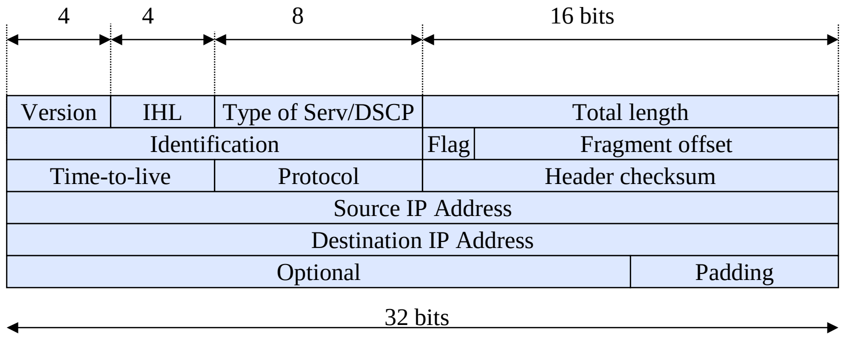


Internet architecture includes a set of Service level components on top of TCP/IP



In this course we may touch some of these but only in their relation to routing.

IPv4 packet header



We assume that the sender knows its own IP address, if not self configuration protocols such as *RARP, BOOTP, DHCP* - *dynamic host conf. protocol* are used

DSCP - DiffServ Code Point, IHL - IP header length

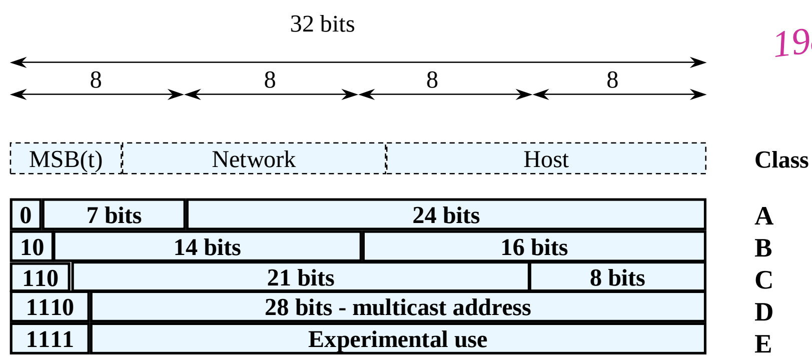
IP version	IP version number. Current version is 4
IHL	Internet header length. Expressed as number of 32 –bit words
Type of Service/ DSCP	TOS contains 3MSBits: packet priority + service type. DSCP – is proposed use for Differentiated Services
Total length of the packet	Expressed as nrof octets in the payload and in the header
Identifikation, Flags and Offset	Are used when large packets are fragmented when underlaying network has maximum packet length.
TTL	Time-to-live. The value is decremented with an integer representing the quality of the network on each router a path of the packet. Packet is deleted when TTL reaches

Protocol	Protocol, that the receiving host should use to process the datapacket, e.g. TCP
Checksum	Header checksum. Calculated as 16 bit one’s complement sum
Source Address	IP address of the sender of the packet.
Destination Address	IP address of the destination host
Options	Used for special types of information or “tricks”. One packet can carry many option fields

IPv4 address formats

- Originally two-level (network, host) hierarchy

1981



IPv4 address formats

1984

- A new level for easier network administration

Network	Subnet	Host

- Examples:

Mask	IP address	Network	Subnet	Host
0xFFFF0000	10.27.32.100	A: 10	27	32.100
0xFFFFFE00	136.27.33.100	B: 136.27	16 (32)	1.100
	136.27.34.141	136.27	17(34)	0.141
0xFFFFFFC0	193.27.32.197	C: 193.27.32	3(192)	5

High order bits:
0 ..... 0 - 127. --> A-class
10.... 128. - 191. --> B-class
110...192. - 223. --> C-class

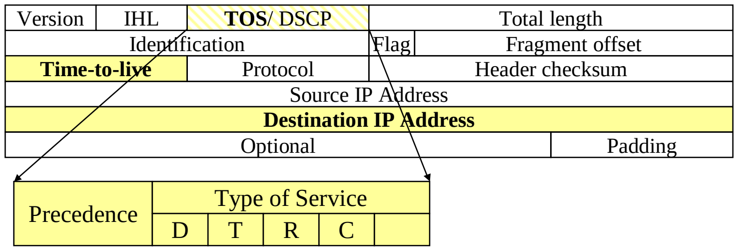
Without right zeroes (and with right zeroes)

Later updated by CIDR

Special addresses

- Unknown network replaced by 0
  - Only in source address
  - 0.0.0.0 = ”this host in this network”
  - 0.X.Y.Z = ”host X.Y.Z in this network”
- Broadcast address 255.255.255.255
  - All host in the local network
- Broadcast addresses A.255.255.255, B.B.255.255, C.C.C.255
  - All hosts in a specified network
- Loopback-address 127.X.X.X (usually 127.0.0.1)
  - Internal in one host
- Multicast-osoitteet

Destination Address and the TTL are used for Routing



TOS = ***route selection criteria: D - minimization of delay or***
T - maximization of bandwidth or
R - maximization of reliability or
C - minimization of cost

This Schema was never widely adopted!

priority - highest value --> must be served first in the queue.

Options: for example: source routing. Used very seldom because routers tend to serve packets with options last.

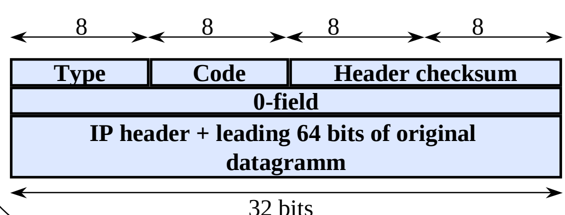
Source routing

- Implemented with the ”source routing” option
  - Loose source routing (type 131)
    - The packet is sent to the next address in the list using normal routing.
  - Strict source routing (type 137)
    - The packet is sent to the next address in the list. If there is no direct link to the address, the packet is destroyed.
- Not often used

ICMP - Internet Control Message Protocol gives feedback to the sender about the network state

- Gives feedback about the network operation
- All hosts and routers must support ICMP.
  - (To battle Denial of Service Attacks not always a good idea).
- ICMP packet is sent backwards if e.g.
  - the receiver is unreachable
  - router deletes a packet
  - TTL = 0
- If ICMP message is deleted, a new one is not generated to avoid the snowballing effect.

ICMP messages



Type=0 - Echo reply
- ***3 - destination unreachable***
- 4 - (source quench)
- ***5 - Redirect***
- 8 - Echo
- ***9 - Router advertisement***
- ***10 - Router solicitation***
- ***11 - Time exceeded***
- 12 - Parameter problem
- 13 - Timestamp
- 14 - Timestamp reply
- 15 - Information request
- 16 - Information reply

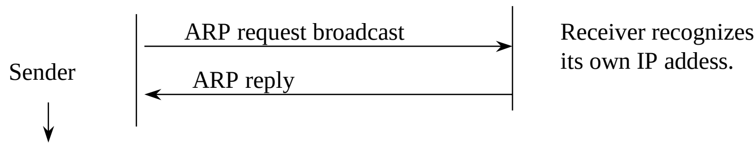
(4 - source quench=“slow down” has been dropped from recommendations)

Code =
- **0 - net unreachable**
- **1 - host unreachable**
- **2 - protocol unreachable**
- **3 - port unreachable**
- 4 - fragmentation needed and DF set
- **5 - source route failed**

ARP - Address resolution protocol (RFC-826) maps IP to the underlaying protocol.

Sender works like this:

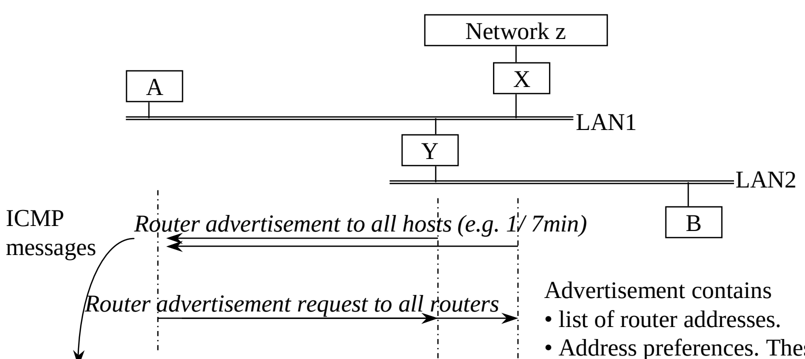
1. Compare masked values of own and destination IP addresses to find out whether the destination is in the same sub-network. If =, destination is in the same sub-network, if not the packet must be sent to a router.
2. Find media address (MAC address) of the next hop.



Store in local address cache

Each network technology requires its own ARP adaptation. Adaptation is easy if the network supports broadcast or multicast.
E.g. ATM requires a special ARP - server.

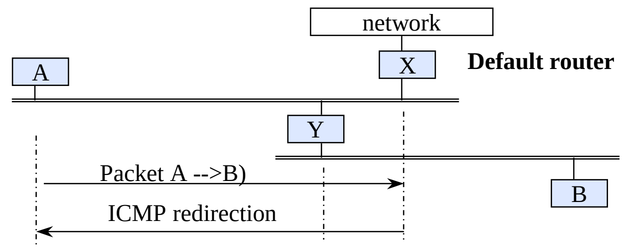
A network may have many routers, closest to destination must be found



Advertisement contains
- list of router addresses.
- Address preferences. These mark default, designated,etc. router or router address
- validity period (e.g. 30 min)

- *Pick advertisement from own sub-network*
- *Default router preference is highest.*

Router can send redirection packet to hint to a better route towards a destination



8	8	8	8
Type = 5	**Code**	**Header checksum**	
IP address --> router=Y			
IP header + 64 bits of original datagramm			

32 bittiä

Code:
0 - redirection for the network
1 - redirection for the destination
2 - Redir for TOS and network
4 - Redir for TOS and host

Redirect is a slow mechanism. Hot-standby addressing is an improvement

- Virtual router redundancy protocol (RFC 2338 - 4/98)
  - a router may have a virtual IP address
  - a router can take the IP and MAC addresses of a failed router (in the same segment)
  - After recovery routers negotiate about address assignments
  - Clients are configured with a static (virtual) router address
  - Cisco and DEC have equivalent proprietary protocols
- Host can listen to RIP or OSPF
  - not recommended but used sometimes anyway

Host must have feedback from the first router to avoid sending to a “black hole”

Feedback may be

- TCP acknowledgements
- Router advertisements
- ARP-replies
- ICMP echo reply

Between routers, routing protocols provide similar feedback and help in detecting failed router neighbors.

DNS - Domain Name Service

- Why DNS?
  - Easier to remember names than addresses
  - The address may change, the name is the same
  - Several addresses per host
- Name → address
- DNS does not affect routing

Routing in the Internet

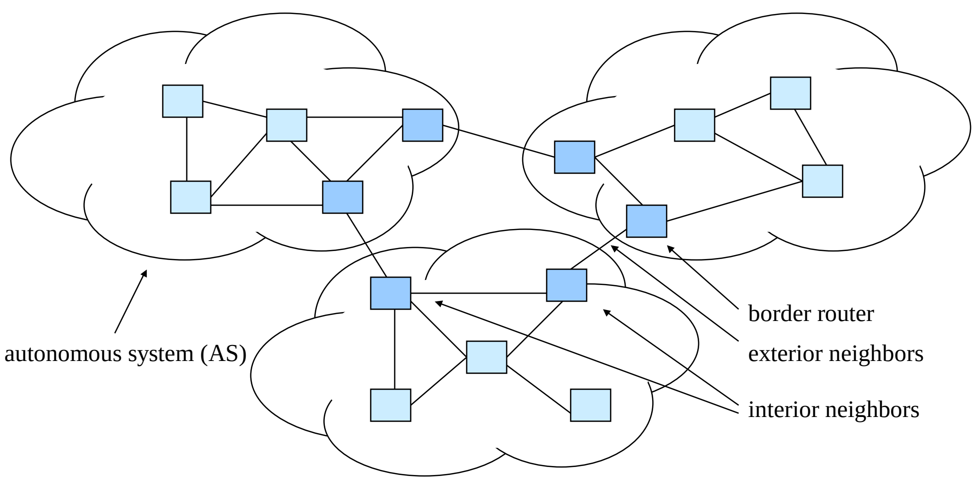
Routing can be static or dynamic

- Static routing is based on manually configured routing tables.
  – Static routing is used when e.g. two peer providers do not trust each other or
  – To connect an organization to a Service Provider with a single connection
  – Static routing is difficult to maintain
- Dynamic routing is based on routing protocols which create and maintain the routing tables automatically
  – examples of routing protocols are RIP, OSPF, BGP...
  – E.g. to connect an organization with multiple links to the Internet

Internet routing is based on routing protocols, which collect information

- No off-line route planning
- Only dimensioning is made off-line
- Routing itself is completely automatic
- The routers communicate with a routing protocol
- The routing algorithm finds the shortest (cheapest) route to every destination

Routing is divided into interior and exterior



In this couse we only deal with interior routing

Routing is divided into interior and exterior

- Autonomous system, AS
  - Networks operated by a single organization and having a common routing strategy
- Border router
  - At least one neighbor belongs to another autonomous system

Routing is divided into interior and exterior

- Interior routing protocols
  - Routing Information Protocol (RIP)
  - Open Shortest Path First (OSPF)
  - IGRP
  - IS-IS
- Exterior routing protocols
  - External Gateway Protocol (EGP)
  - Border Gateway Protocol version 4 (BGP-4)

Routing algorithms

- Distance vector
  - Distance vectors are sent, until the state of the network is stable
  - The routers cooperate to generate the routes
- Link state
  - Topology databases are sent periodically
  - Every router generates the routes independently of the other routers

Properties of the routing algorithms

Distance vector	Link state
+ Simple and lightweight	- Complex and heavy
- Slow convergence	+ Fast convergence
- Only one route per destination	+ Several routes per destination
- Only one metric	+ Supports different metrics