

Advanced Computer Networking (ACN)

IN2097 – WiSe 2026–2027

Prof. Dr.-Ing. Georg Carle, Dr. Sebastian Gallenmüller

Christian Dietze, Marcel Kempf, Lorenz Lehle

Chair of Network Architectures and Services
School of Computation, Information and Technology
Technical University of Munich

Internet Protocol v4

Network layer

Internet addressing

ICMP

ARP

Routing and Forwarding

Bibliography

Network layer

Internet addressing

ICMP

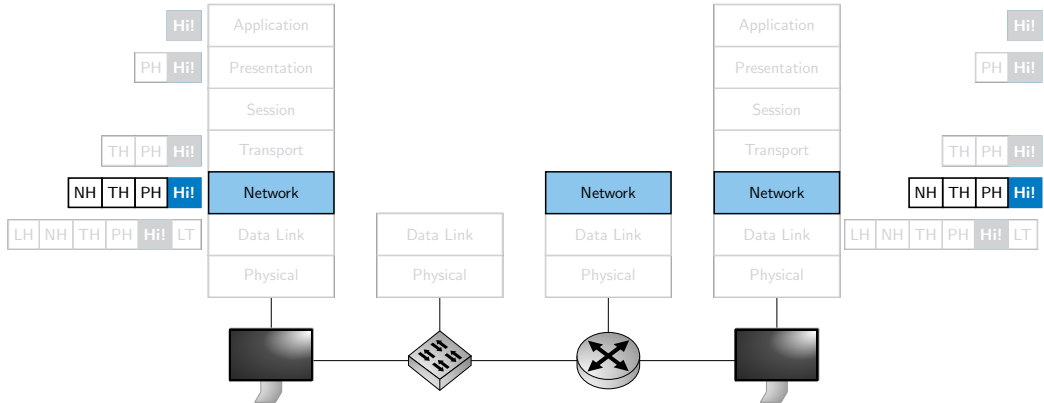
ARP

Routing and Forwarding

Bibliography

Network layer

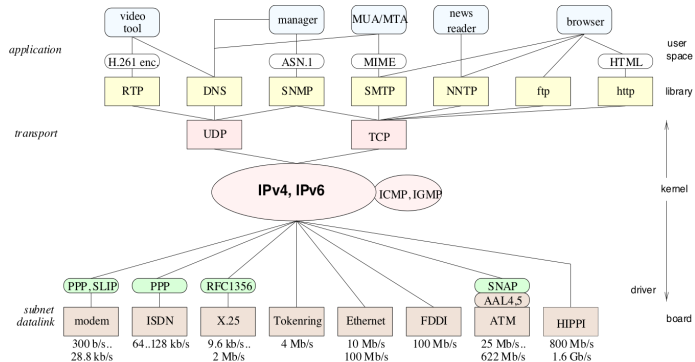
Protocol entities in hosts and routers



Network layer

IP protocol model

- Many application specific protocols over IP
- IP (with best effort service model) over many media specific LAN protocols
 - “Hourglass” model of IP
 - QoS support (RSVP, DiffServ) added to IP as an “afterthought”

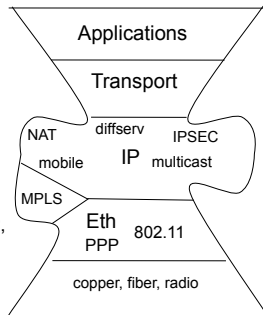


Network layer

IP protocol stack evolution

- Specific requirements and use cases did lead to the development of additional protocols
 - protocol implementation added to specific nodes
 - additional protocols not supported everywhere

- TLS, DTLS
- TCP, UDP, SCTP, DCCP
- BGP, OSPF, IS-IS, RIP, RIPng, VRRP, PIM, IGMP, MLD
- IPsec, IKE, EAP
- IPv4, IPv6, ICMP
- VLAN, GTP, IP in IP, GRE, L2TP, MPLS



Network layer

Network prefix and host number

- L3/IP service goal: forward IP datagrams to destination IP subnet/host/interface
- IP address has role of locator & identifier:
 - network part (network identifier & locator)
 - host part (host identifier)
- Each IP network (often called subnetwork or subnet) has an IP address:
 - IP address of a network = Host number is set to all zeros, e.g., 128.143.0.0
- IP routers are devices that forward IP datagrams between IP networks
- Delivery of an IP datagram proceeds in 2 steps:
 1. Use network prefix to deliver IP datagram to the right network
 2. Once the network is reached, use the host L3 address to deliver to the right interface

Network layer

Host or router network layer functions

- IP protocol
 - addressing conventions
 - datagram format
 - packet handling conventions
- ICMP protocol
 - error reporting
 - router “signaling”
- Routing protocols
 - path selection
 - RIP, OSPF, BGP

Network layer

IPv4 datagram [1]

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
0 B	Version				IHL				TOS								Total Length																			
4 B	Identification																Flags				Fragment Offset															
8 B	TTL								Protocol								Header Checksum																			
12 B	Source Address																																			
16 B	Destination Address																																			
20 B	Options / Padding (optional)																																			

Abbreviations:

- **IHL**: Internet Header Length
- **TOS**: Type Of Service
- **TTL**: Time To Live

Network layer

Internet addressing

ICMP

ARP

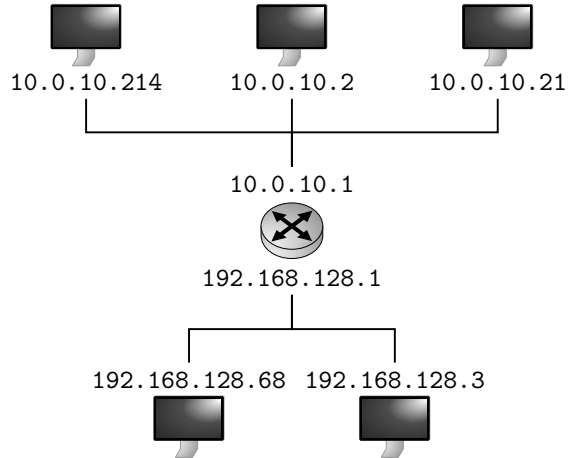
Routing and Forwarding

Bibliography

Internet addressing

IPv4 addressing

- **IP address:** 32-bit identifier for host, router interface
- **Address space:** 4.3 billion IPv4 addresses in theory
- **Interface:** connection between host/router and physical link
 - IP addresses associated with each interface

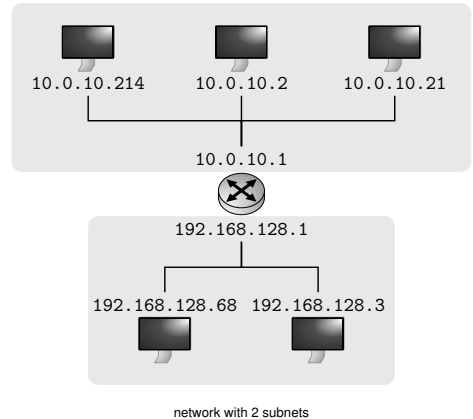


IP address **notation**: 4 numbers from 0 to 255 separated by dots

Internet addressing

Subnets

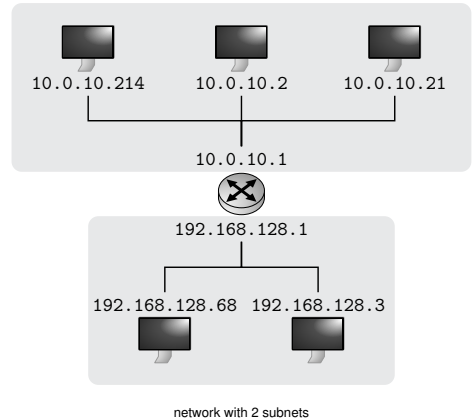
- What is a subnet?
 - device interfaces with same subnet part of IP address
 - can physically reach each other without intervening router



Internet addressing

Subnets

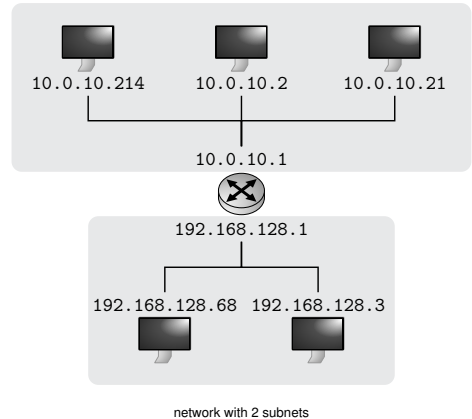
- What is a subnet?
 - device interfaces with same subnet part of IP address
 - can physically reach each other without intervening router
- How to determine?
 - Detach interfaces from host or router



Internet addressing

Subnets

- What is a subnet?
 - device interfaces with same subnet part of IP address
 - can physically reach each other without intervening router
- How to determine?
 - Detach interfaces from host or router
- Splitting IP addresses
 - **Network part**: Addressing the network
 - **Host part**: Addressing the interface of a host

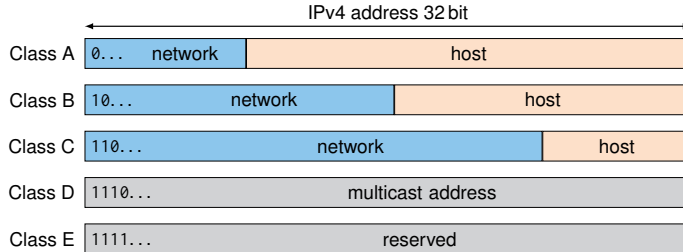


$$\begin{array}{rcl}
 & 192_{10}. & 168_{10}. \\
 = & 11000000_2.10101000_2.1_2 & 0000000_2.00000001_2 \\
 & \text{network part} & \text{host part}
 \end{array}$$

Internet addressing

Classful IP addresses (historic)

- Used from 1981 to 1993



class	start address		end address	network length	relative portion
A	0.0.0.0	to	127.255.255.255	8 bit	50.00 %
B	128.0.0.0	to	191.255.255.255	16 bit	25.00 %
C	192.0.0.0	to	223.255.255.255	24 bit	12.50 %
D	224.0.0.0	to	239.255.255.255	—	6.25 %
E	240.0.0.0	to	255.255.255.255	—	6.25 %

Internet addressing

Classless IP addresses (current)

- **CIDR:** Classless InterDomain Routing (introduced in 1993, RFC 1519)
- **Idea:** introduction of arbitrary subnet length
- **Address format:** a.b.c.d/x, where x corresponds to the number of bits in subnet portion of address
e.g., 192.168.128.1/17

Internet addressing

Classless IP addresses (current)

- **CIDR:** Classless InterDomain Routing (introduced in 1993, RFC 1519)
- **Idea:** introduction of arbitrary subnet length
- **Address format:** a.b.c.d/x, where x corresponds to the number of bits in subnet portion of address
e.g., 192.168.128.1/17

$$\begin{array}{ccccccc}
 & 192_{10} & . & 168_{10} & . & 128_{10} & . & 1_{10} & /17 \\
 = & 11000000_2 & . & 10101000_2 & . & 0000000_2 & . & 00000001_2 & \\
 & \text{network part} & & & & \text{host part} & & &
 \end{array}$$

Internet addressing

Example: CIDR

- How to calculate the network address for interface address 192.168.128.1 with a prefix length of 17 bits?
 - CIDR notation: 192.168.128.1/17
 - Dotted decimal notation: 192.168.128.1/255.255.128.0

host address ₁₀		192 ₁₀ .	168 ₁₀ .	128 ₁₀ .	1 ₁₀
host address ₂		11000000 ₂ .	10101000 ₂ .	10000000 ₂ .	00000001 ₂
network mask	&	11111111 ₂ .	11111111 ₂ .	10000000 ₂ .	00000000 ₂
<hr/>					
network address ₂		11000000 ₂ .	10101000 ₂ .	10000000 ₂ .	00000000 ₂
network address ₁₀		192 ₁₀ .	168 ₁₀ .	128 ₁₀ .	0 ₁₀

Internet addressing

Classful vs. CIDR

- Classful:



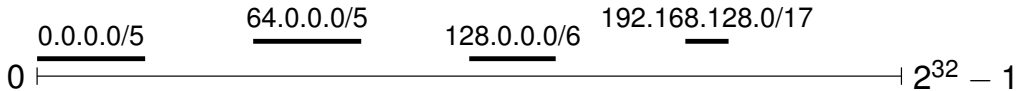
Internet addressing

Classful vs. CIDR

- Classful:



- CIDR:



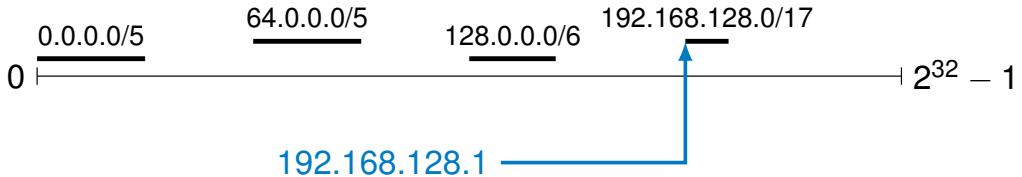
Internet addressing

Classful vs. CIDR

- Classful:

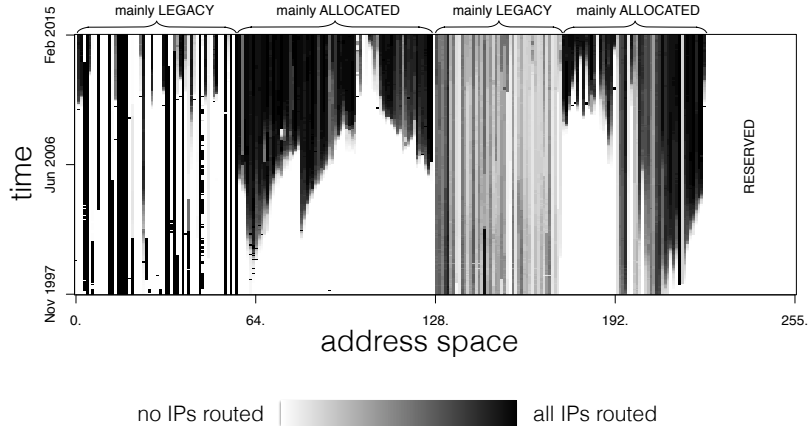


- CIDR:



Internet addressing

Current usage of IPv4 addresses¹



¹P. Richter et al., "A primer on ipv4 scarcity," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 2, pp. 21–31, 2015

Internet addressing

IPv4 address exhaustion

IPv4 addresses are a rare resource nowadays: price per IPv4 address on IP marketplaces is between 25 and 40 US-Dollar (2024)

- **Inefficiency of Classful Internet Routing:**
 - Class C (256 addresses) too small for small enterprises
 - Class B (65536 addresses) too small for large enterprises or universities
 - Class A (16 million addresses) too large
- **Rise of Internet-connected devices:** personal computers, mobile phones, Internet-of-Things, ...
- **Always-on devices:** Sharing of IPv4 addresses become less viable

Internet addressing

IPv4 address exhaustion

IPv4 addresses are a rare resource nowadays: price per IPv4 address on IP marketplaces is between 25 and 40 US-Dollar (2024)

- **Inefficiency of Classful Internet Routing:**
 - Class C (256 addresses) too small for small enterprises
 - Class B (65536 addresses) too small for large enterprises or universities
 - Class A (16 million addresses) too large
- **Rise of Internet-connected devices:** personal computers, mobile phones, Internet-of-Things, ...
- **Always-on devices:** Sharing of IPv4 addresses become less viable

Notable proposed solutions:

- **Private Addresses** in conjunction with network address translation (NAT)
 - 10.0.0.0/8 - 24-bit block
 - 172.16.0.0/12 - 20-bit block
 - 192.168.0.0/16 - 16-bit block
- **IPv4 shared address space** for carrier-grade NAT (CGN) deployments: 100.64.0.0/10
The ISPs use this prefix for the private network between the CPEs (customer-premises equipment) and core routers.

Network layer

Internet addressing

ICMP

ARP

Routing and Forwarding

Bibliography

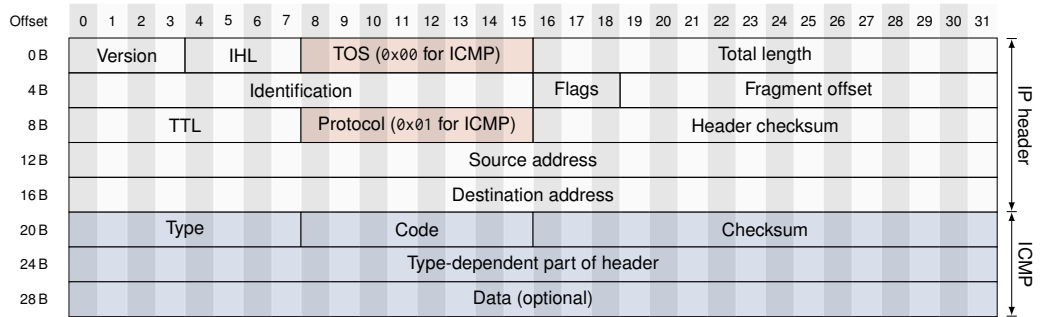
ICMP

Internet Control Message Protocol (ICMP)

- RFC 792 [3]
- Network control plane protocol “above” IP:
 - ICMP messages carried in IP datagrams
 - Can be considered part of the IP layer
- Communicates error messages and other conditions that require attention
- Error messages are acted on by either. . .
 - IP layer, or
 - TCP, or UDP
- Some ICMP messages cause error notifications to be returned to user processes

ICMP

ICMP message format



- 15 different types
- Some types use a code to further specify the condition

ICMP

ICMP message types

Two classes of ICMP messages:

- Query messages
 - Only kind of ICMP messages that generate another ICMP message
- Error messages
 - Contain IP header and at least first 8 bytes of datagram that caused the ICMP error to be generated.
 - Allows receiving ICMP module to associate the message with a particular protocol and process (port number)

ICMP

ICMP message types

- Cf. RFC 792 [3]

type	description
0	echo reply (ping)
3	destination unreachable (codes subsequent slide)
4	source quench (deprecated, RFC 6633)
5	redirect
8	echo request
9	router advertisement (MC, see RFC 1256)
10	router solicitation (MC, see RFC 1256)
11	time exceeded
12	parameter problem (bad IP header)
13	timestamp request
14	timestamp reply
15	info request
16	info reply
17	address mask request (see RFC 950)
18	address mask reply

ICMP

ICMP message types continued

- Cf. RFC 792 [3]

type	code	description
3	0	dest network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown

- **Historically:** ICMP content always contained IP header and first 8 bytes of IP payload that caused ICMP error message to be generated (RFC 792)
- **Today:** ICMP should contain as much data of the dropped message as possible up to a limit of 576 byte for the ICMP message (RFC 1812)

Network layer

Internet addressing

ICMP

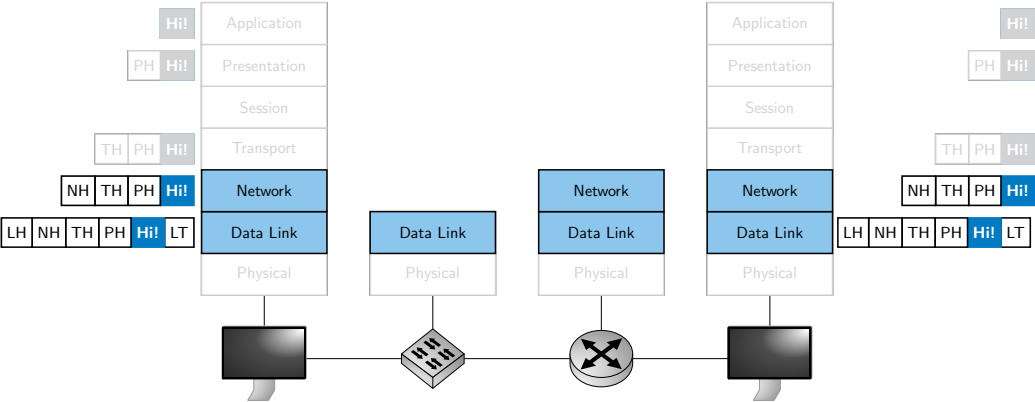
ARP

Routing and Forwarding

Bibliography

ARP

Connecting Link and Network Layer



ARP

MAC Addresses and IP Addresses

MAC (or LAN or physical or Ethernet) address

- L2 service: transmit frame from one interface to another physically-connected interface (same network) with specified destination address
- address length: 48 bit (for most LANs)
 - burned into network adapter ROM, or software settable
 - assumption: two hosts on the same LAN will not use the same Ethernet address

IP address: network-layer address

- L3 service: get datagram to destination IP subnet / host I/F
- L3 address: has role of locator & identifier (vs. HIP – Host Identity Protocol; LISP – Locator/ID Separator Protocol)
- address length: 32 bit (IPv4) or 128 bit (IPv6)
- address separated into:
 - network part (i.e. network identifier & locator)
 - host part (i.e. host identifier)

ARP

Address resolution

Mapping between addresses of different layers

- Examples:
 - IPv4 $\longrightarrow$ MAC
 - MAC $\longrightarrow$ IPv4

Mapping from L3 host address to MAC address

- Needed to identify correct L2 adapter of L3 address
- $\rightarrow$ Address Resolution Protocol (ARP)

Mapping from MAC address to L3 address

- $\rightarrow$ Reverse Address Resolution Protocol (RARP) (rarely used)

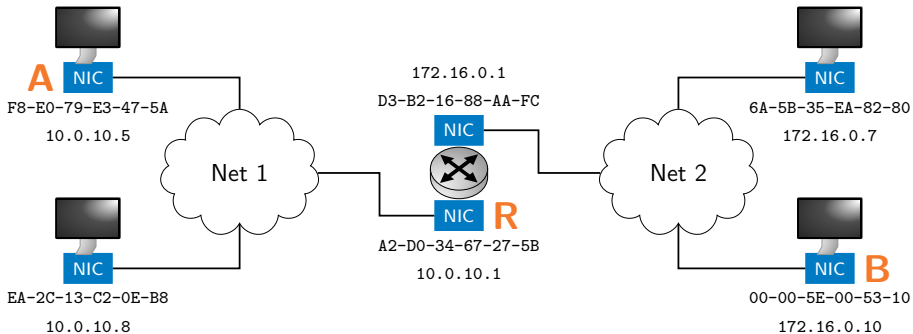
	Example	Organization
MAC address	6C:40:08:BD:A5:B4	flat, permanent
IP address	172.16.0.1	topological (mostly)
Host name	www.ietf.org	hierarchical



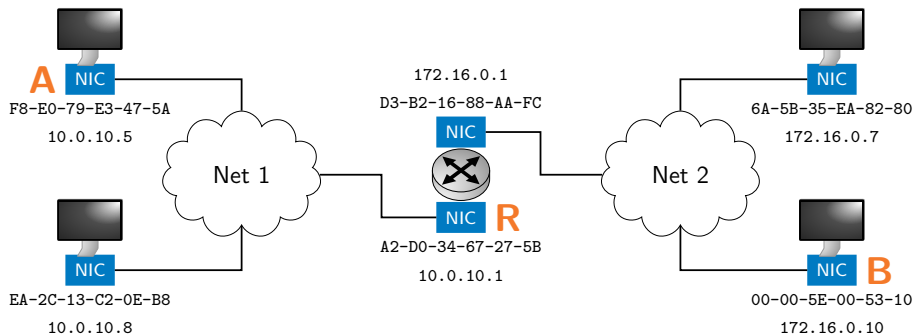
ARP

Addressing: routing to another LAN

- Example send datagram from **A** to **B** via **R** (assuming **A** knows **B**'s IP address)
- The router manages two ARP tables one for Net 1 and one for Net 2



- A creates IP datagram with source IP addr. A, destination IP addr. B
- A uses ARP to get R's MAC address of R's interface 10.0.10.1
- A creates link-layer frame with R's MAC address as destination, frame contains A-to-B IP datagram
- A's NIC sends frame
- R's NIC receives frame
- R extracts IP datagram from Ethernet frame, sees it is destined to B
- R uses ARP to get B's MAC address
- R creates frame containing A-to-B IP datagram, sends it to B



ARP

ARP protocol: same LAN (network)

- A wants to send datagram to R's interface 10.0.10.1, while R's MAC address is not in A's ARP table.
- A broadcasts ARP query packet, containing R's IP address
 - destination MAC address = FF-FF-FF-FF-FF-FF
 - all hosts on LAN receive ARP query
- When R receives ARP packet, it replies to A with its (R's) MAC address
 - frame sent to A's MAC address
- A caches IP-to-MAC address pair in its ARP table until information times out
 - soft state: information that times out (goes away) unless refreshed
- ARP is "plug-and-play":
 - nodes create their ARP tables without intervention from network administrator

ARP
ARP packet format

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0B	Hardware Type															Protocol Type																
4B	Hardware Addr. Length								Protocol Addr. Length								Operation															
8B	Sender Hardware Address (first 32 bit)																															
12B	Sender Hardware Address (last 16 bit)																Sender Protocol Address (first 16 bit)															
16B	Sender Protocol Address (last 16 bit)																Target Hardware Address (first 16 bit)															
20B	Target Hardware Address (last 32 bit)																															
24B	Target Protocol Address																															

ARP

ARP details

ARP supports different protocols at L2 and L3

- any network protocol over any LAN/MAC protocol
- type and address length fields specified in ARP PDUs

Reverse ARP (RARP) cf. RFC 903 (rarely used)

L2 MAC fields (hardware)

- hardware type: 6 = IEEE802 (with LLC/SNAP)
- address length: 6 for a 6 byte long MAC address
- sender hardware address (SHA)
- target hardware address (THA)

L3 network fields (protocol)

- protocol type: IP = 0800
- address length: 4 for 4 byte long IPv4 address
- sender protocol address (SPA)
- target protocol address (TPA)

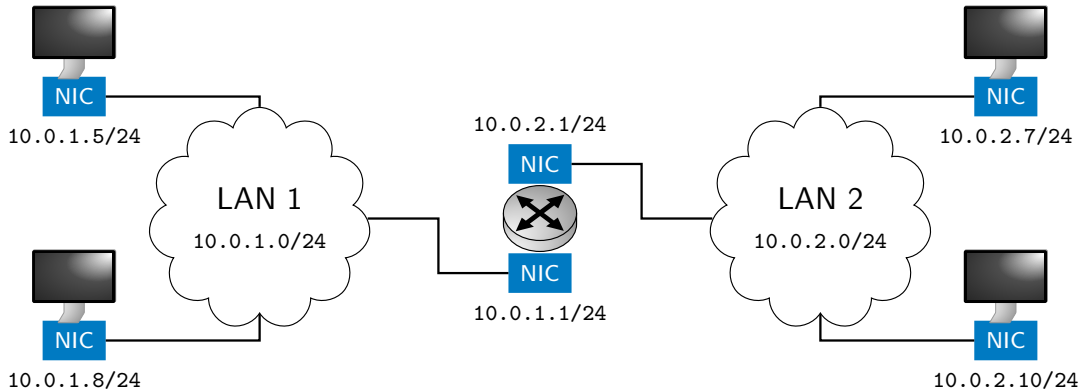
Operation Code

- 01: request
- 02: reply
- 03: reverse request
- 04: reverse reply (for RARP)
- cf. <http://www.iana.org/assignments/arp-parameters>

ARP

Proxy ARP

- **Proxy ARP:** Host or router responds to ARP Request that arrives from one of its connected networks for a host that is on another of its connected networks.
- RFC 925: Multi-LAN Address Resolution



ARP

Proxy ARP - possible uses

Transparent subnet gatewaying

- Two LANs sharing same IP subnet, connected via router
- cf. RFC 1027 – Using ARP to Implement Transparent Subnet Gateways

Host joining LAN via dialup link

- Dialup router employs Proxy ARP

Host joining LAN via VPN

- VPN server employs Proxy ARP

Host separated via firewall

- Firewall employs Proxy ARP

ARP

ARP optimizations

When should a host send ARP requests?

- Before sending each IP packet?
 - No, each host/router maintains ARP table (IP address $\longrightarrow$ MAC address mapping)
 - ARP request is only sent in case there is no entry for this IP address in the ARP table.

How to deal with hosts that change their addresses?

- Expiration timer is associated to each entry in the ARP table
 - ARP table entry is removed upon timer expiration
 - Some implementations send ARP request to revalidate before removing table entry
 - Some implementations remember when ARP table entries were used to avoid removing important entries

ARP

Things to know about ARP

What happens if an ARP request is made for a non-existing host?

- Several ARP requests are made with increasing time intervals between requests
- Eventually, ARP gives up

Gratuitous ARP Requests

- A host sends an ARP request for its own IP address
- Useful for detecting if an IP address has already been assigned.

ARP

Vulnerabilities of ARP

1. Since ARP does not authenticate requests or replies, ARP requests and replies can be forged
2. ARP is stateless: ARP replies can be sent without a corresponding ARP request
3. According to the ARP protocol specification, a node receiving an ARP packet (request or reply) must update its local ARP cache with the information in the sender fields. Updates also happen if the receiving node already has an entry for the IP address of the sender in its ARP cache. (This applies for ARP Request packets and for ARP Reply packets)

Typical exploitation of these vulnerabilities:

- A forged ARP request or reply can be used to update the ARP cache of a remote system with a forged entry ([ARP Poisoning](#))
- This can be used to redirect IP traffic from/to other hosts
- ARP poisoning & ARP spoofing also can be performed by hosts within a WPA2-protected WLAN

Network layer

Internet addressing

ICMP

ARP

Routing and Forwarding

Bibliography

Routing and Forwarding

Routers vs. Switches

Both store-and-forward devices

- routers: L3/network layer devices (examine network layer headers)
- switches: L2/link layer devices

Switches:

- maintain switching tables
- implement filtering, learning algorithms
- may implement spanning tree algorithm
- switch L2 frames based on switching table entries & destination MAC address

Routers:

- maintain forwarding tables
- implement routing protocols
- forward IP packets based on forwarding table entries & destination IP address

Routing and Forwarding

Forwarding: data plane

- Directing a data packet to an outgoing link
- Individual router using a forwarding table

Routing: control plane

- Computing the paths the packets will follow
- Individual router creates a forwarding table

Routing protocols (e.g., RIP, OSPF, BGP):

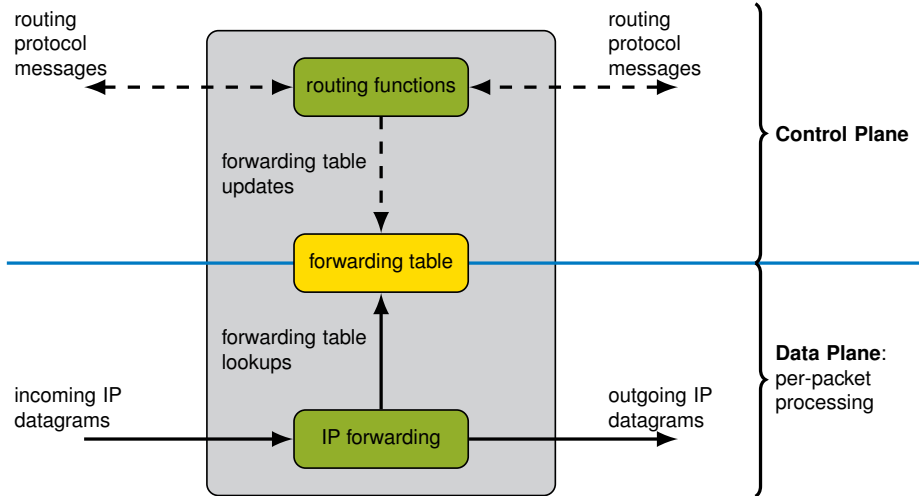
- Distributed routing protocol entities in routers talking amongst themselves (above IP)

Routing in Software Defined Networking (SDN):

- Router may receive forwarding and/or routing information via SDN control plane
- Control plane might not necessarily be inside the router

Routing and Forwarding

IP router: functional components



Routing and Forwarding

Router architecture

Routing functions include:

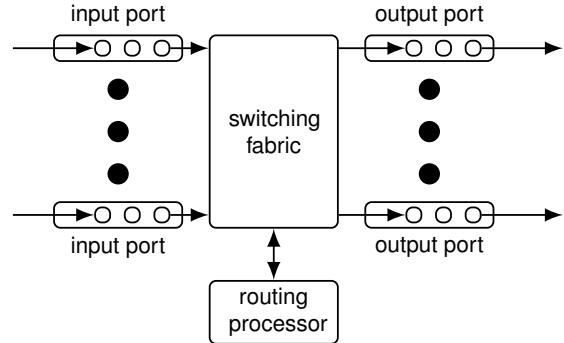
- route calculation
- execution of routing protocols
- maintenance of routing state
- maintenance of forwarding table

On (high-end) commercial routers:

- routing functions are handled by a single general purpose processor, called routing processor
- the per-packet processing and forwarding is distributed (Most work is done on the interface cards)

Two key router functions

- run routing algorithms/protocol (RIP, OSPF, BGP)
- forwarding datagrams from incoming to outgoing link



Network layer

Internet addressing

ICMP

ARP

Routing and Forwarding

Bibliography

- [1] DARPA, Internet Protocol, <https://tools.ietf.org/html/rfc791>, 1981.
- [2] P. Richter, M. Allman, R. Bush, and V. Paxson, “A primer on ipv4 scarcity,” *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 2, pp. 21–31, 2015.
- [3] J. Postel, Internet Control Message Protocol, <https://tools.ietf.org/html/rfc792>, 1981.

Internet Protocol v4

Acknowledgements

- Jim Kurose, University of Massachusetts, Amherst
- Keith Ross, Polytechnic Institute of NYC
- Olivier Bonaventure, University of Liege
- Srinivasan Keshav, University of Cambridge