Advanced Computer Networking (ACN)

IN2097 – WiSe 2019-2020

Prof. Dr.-Ing. Georg Carle

Sebastian Gallenmüller, Max Helm, Benedikt Jaeger, Patrick Sattler, Johannes Zirngibl

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich
50 years of Internet
October 29, 1969: First ARPANET Packets Sent

Important people for ARPANET: Paul Baran (RAND Corporation), Lawrence Roberts (MIT Lincoln Lab), Leonard Kleinrock (UCLA), Douglas Engelbart (SRI)

Excerpt from: https://en.wikipedia.org/wiki/History_of_the_Internet:
The first ARPANET link was established between the University of California, Los Angeles (UCLA) and the Stanford Research Institute at 22:30 hours on October 29, 1969.

"We set up a telephone connection between us and the guys at SRI ...", Kleinrock ... said in an interview: "We typed the L and we asked on the phone, "Do you see the L?"

"Yes, we see the L," came the response.

We typed the O, and we asked, "Do you see the O."

"Yes, we see the O."

Then we typed the G, and the system crashed ... Yet a revolution had begun" ....[46]
Chapter 3: Internet Protocol v4

Network layer

Internet addressing

ICMP

ARP

Routing

Bibliography
Network layer
Host or router network layer functions

- IP protocol
  - addressing conventions
  - datagram format
  - packet handling conventions
- Routing protocols
  - path selection
  - RIP, OSPF, BGP
- ICMP protocol
  - error reporting
  - router “signaling”
Internet addressing
IPv4 address exhaustion

IPv4 addresses are rare a resource nowadays

- **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

Various solutions proposed, the most notable one being **private addresses:**

- 10.0.0.0/8 - 24-bit block
- 172.16.0.0/12 - 20-bit block
- 192.168.0.0/16 - 16-bit block
Chapter 3: Internet Protocol v4

Network layer

Internet addressing

ICMP

ARP

Routing

Bibliography
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
Two classes of ICMP messages:

- Query messages
  - Only kind of ICMP messages that generate another ICMP message
- Error messages
  - Contain IP header and 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]

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

ICMP message types continued

- Cf. RFC 792 [3]

<table>
<thead>
<tr>
<th>type</th>
<th>code</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0</td>
<td>dest network unreachable</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>dest host unreachable</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>dest protocol unreachable</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>dest port unreachable</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>dest network unknown</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>dest host unknown</td>
</tr>
</tbody>
</table>

- 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 572 byte for the ICMP message (RFC 1812)
ICMP Ping

- Checks if host is reachable, alive
- Uses ICMP echo request/reply
- Copy packet data request reply

PING net.in.tum.de (131.159.15.24): 56 data bytes
64 bytes from 131.159.15.24: icmp_seq=0 ttl=63 time=4.033 ms
64 bytes from 131.159.15.24: icmp_seq=1 ttl=63 time=13.310 ms
64 bytes from 131.159.15.24: icmp_seq=2 ttl=63 time=58.955 ms
64 bytes from 131.159.15.24: icmp_seq=3 ttl=63 time=7.143 ms
^C
--- net.in.tum.de ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 4.033/20.860/58.955/22.246 ms

Listing 1: Sample output of ping
ICMP
Traceroute

- Allows to follow path taken by packet
- Send UDP/TCP/... packets with increasing TTL to (unlikely) port
- ICMP replies: ‘time exceeded’; last ICMP message: ‘port unreachable’

```bash
$ traceroute gaia.cs.umass.edu
1 scylla (131.159.20.11) 4.263 ms 2.531 ms 2.162 ms
2 nz-bb-net.informatik.tu-muenchen.de (131.159.252.149) 6.124 ms 15.174 ms 3.546 ms
3 nz-csr1-kw5-bb1.informatik.tu-muenchen.de (131.159.252.2) 2.925 ms 4.234 ms 3.033 ms
4 vl-3010.csr1-2wr.lrz.de (129.187.0.149) 5.082 ms 3.387 ms 4.694 ms
5 cr-gar1-be2-147.x-win.dfn.de (188.1.37.89) 3.254 ms 3.274 ms 2.967 ms
6 cr-fra2-hundredgige0-0-0-3x-win.dfn.de (188.1.144.253) 13.139 ms 12.260 ms 15.702 ms
7 dfn.mx1.fra.de.geant.net (62.40.124.217) 11.365 ms 11.716 ms 16.314 ms
8 ae1.mx1.gen.ch.geant.net (62.40.98.108) 19.889 ms 26.193 ms 19.661 ms
9 ae4.mx1.par.fr.geant.net (62.40.98.152) 28.465 ms 27.664 ms 29.365 ms
10 et-3-1-0102.rtsw.newy32aoa.net.internet2.edu (198.71.45.236) 104.199 ms 104.173 ms 109.925 ms
11 nox300gw1-i2-re.nox.org (192.5.89.221) 111.437 ms 110.232 ms 109.370 ms
12 umass-re-nox300gw1.nox.org (192.5.89.102) 113.755 ms 115.848 ms 110.634 ms
13 core1-rt-xe-0-0-0-gw.umass.edu (192.80.83.101) 118.469 ms 119.070 ms 114.279 ms
14 lgrc-rt-106-8-po-10.gw.umass.edu (128.119.0.233) 111.948 ms 111.992 ms 111.616 ms
15 128.119.3.32 (128.119.3.32) 112.194 ms 124.315 ms 111.624 ms
16 nscc1bbs1.cs.umass.edu (128.119.240.253) 114.384 ms 166.509 ms 113.220 ms
17 gaia.cs.umass.edu (128.119.245.12) 130.574 ms !Z 114.883 ms !Z 116.865 ms !Z
```

Listing 2: Sample output of traceroute
Acknowledgements

• Jim Kurose, University of Massachusetts, Amherst
• Keith Ross, Polytechnic Institute of NYC
• Olivier Bonaventure, University of Liege
• Srinivasan Keshav, University of Waterloo
ARP
Connecting Link and Network Layer

Application
Presentation
Session
Transport
Presentation
Session
Transport
Application
Presentation
Session
Transport
Application
Presentation
Session
Transport

Host A

Host B

Switch

Switch

Switch

Switch

Chapter 3: Internet Protocol v4 – ARP 3-28
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 → MAC
  - MAC → IPv4

Mapping from L3 host address to MAC address

- Needed to identify correct L2 adapter of L3

Address Resolution Protocol (ARP)

Mapping from MAC address to L3 address

- Reverse Address Resolution Protocol (RARP) (rarely used)
### ARP

**Addresses and names**

<table>
<thead>
<tr>
<th>Example</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC address</td>
<td>6C:40:08:BD:A5:B4</td>
</tr>
<tr>
<td>IP address</td>
<td>172.16.0.1</td>
</tr>
<tr>
<td>Host name</td>
<td><a href="http://www.ietf.org">www.ietf.org</a></td>
</tr>
</tbody>
</table>

**Diagram:**

```
host name [m to n] IP address [1 to 1] MAC address
```

**Notes:**
- DNS, 1 to 1
- ARP, m to n
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 Packet Format

<table>
<thead>
<tr>
<th>Offset</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 B</td>
<td>Hardware Type</td>
<td>Protocol Type</td>
</tr>
<tr>
<td>4 B</td>
<td>Hardware Addr. Length</td>
<td>Protocol Addr. Length</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operation</td>
</tr>
<tr>
<td>8 B</td>
<td></td>
<td>Sender Hardware Address (first 32 bit)</td>
</tr>
<tr>
<td>12 B</td>
<td>Sender Hardware Address (last 16 bit)</td>
<td>Sender Protocol Address (first 16 bit)</td>
</tr>
<tr>
<td>16 B</td>
<td>Sender Protocol Address (last 16 bit)</td>
<td>Target Hardware Address (first 16 bit)</td>
</tr>
<tr>
<td>20 B</td>
<td></td>
<td>Target Hardware Address (last 32 bit)</td>
</tr>
<tr>
<td>24 B</td>
<td></td>
<td>Target Protocol Address</td>
</tr>
</tbody>
</table>
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 48 byte MAC address
- sender hardware address (SHA)
- target hardware address (THA)

L3 network fields (protocol)

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

Operation Code

- 01: request
- 02: reply
- 03: reverse request
- 04: reverse reply (for RARP)
• **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

![Network Diagram](image)
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
When should a host send ARP requests?

- Before sending each IP packet?
  - No, each host/router maintains ARP table (IP address \rightarrow 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
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.
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

Bibliography
Routing
Routers vs. Switches

Both store-and-forward devices

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

Routers:

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

Switches:

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

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 creating a forwarding table

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

- Distributed routing protocol entities in routers talking amongst themselves

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
IP router: functional components

Routing protocol messages
forwarding table updates
forwarding table lookups
IP forwarding
Routing protocol messages
incoming IP datagrams
outgoing IP datagrams

Control Plane
Data Plane: per-packet processing
Routing functions include:

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

On commercial routers handled by a single general purpose processor, called routing processor

IP forwarding is per-packet processing

- On high-end commercial routers, IP forwarding is distributed (Most work is done on the interface cards)
Routing

Router architecture

Two key router functions

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