Tik-110.350 Computer Networks

Lecture 2:
Internet Protocol

Contents

- Internet Protocol (IP)
  - Address and routing of datagrams
- Internet Control Message Protocol (ICMP)
- Classless Inter-Domain Routing (CIDR) and Network Address Translation (NAT)
- Address Resolution Protocol (ARP)
- Dynamic Host Configuration Protocol (DHCP)

Internet Protocol (IP)

Comer's
chapters 4, 7 and 8 (3rd and 4th ed.)

Repetition of IP

- Classfull addressing
  - Five classes of addresses
  - Addresses are divided to netid (identifies the network) and hostid (a host in the network)
- Address specifies a connection to a network, not a computer

Internet Control Message Protocol (ICMP)

Comer's
chapter 9 (3rd and 4th ed.)

Repetition of ICMP

- Internet Control Message Protocol (ICMP)
- Connectionless system is unreliable
- Control and error information
- Router to router or router to host
- ICMP works over IP

Structure of ICMP message

- ”Header” contains
  - type (8 bits)
  - code (8 bits)
  - checksum (16 bits)
- Error message contains the begining of the packet which was causing problems

Echo Request/Reply

TYPE (8 or 0)	CODE (0)	CHECKSUM
IDENTIFIER		SEQUENCE NUMBER
OPTIONAL DATA...		

- Ping program tests reachability of destination
- Traceroute traces the route to destination

Destination unreachable

TYPE (3)	CODE (0-12)	CHECKSUM
UNUSED		
INTERNET HEADER + FIRST 64 BITS OF DATAGRAM		

- code inidicates reason of unreachability, for example destination host unknown

Congestion

TYPE (4)	CODE (0)	CHECKSUM
UNUSED		
INTERNET HEADER + FIRST 64 BITS OF DATAGRAM		

- Datagrams cannot be delivered
  - A computer can send data too fast for the network
  - Single router is overloaded

Redirect

TYPE (5)	CODE (0-3)	CHECKSUM
ROUTER INTERNET ADDRESS		
INTERNET HEADER + FIRST 64 BITS OF DATAGRAM		

- Routers should know the correct route
- Redirect informs a sender that next time use the other route (not send to other router)

Other errors

- Detecting loops
  - Time-to-live (TTL) reaches zero
  - Time Exceeded ICMP message
  - code tells if the TTL reaches zero or if a fragment of the datagram has been lost
- Misformed IP packets
  - Parameter Problem message
  - Incorrect header checksum is not reported

Other uses of ICMP

- Clock synchronization
  - timestamp request/reply messages
- Subnet mask
  - address mask request/reply

Summary & References

- ICMP is used for error detection – not error correction
- Many kind of messages
- Some can be security risks

- Comer chapter 9

Subnetting and Supernetting

Comer's
chapter 10 (3rd and 4th ed.)

Techniques

- Transparent router scheme
- Proxy ARP
- Subnet addressing
- Point-to-point links
- CIDR

Subnetting

- Used locally in a network

- Fixed-length subnetting
- Variable-length subnetting
  - every subnetwork may have different subnet length

Subnet mask

11111111 11111111 11111111 11000000
11111111 11111111 00011000 01000000

- 1 = part of subnet prefix
- 0 = host identifier
- Binary notation
- Recommendation: use contiguous subnet masks

Subnet Mask Representation

- Dotted decimal representation or
- 3-tuple

  { <network #>, <subnet #>, <host #> }

  – For example, for B-class network with subnet mask 255.255.255.0: {-1, -1, 0}

  – For example, for network address 128.10: {128.10, -1, 0}

Subnet routing & broadcasting

- Routing algorithm and routing table must be modified
  – Normal routing is based on network address and next hop address
  – Now the subnet mask is also needed
- Broadcasting
  – even to several physical networks
  – to a specific subnet

Supernetting

- Running out of B-class networks
  - C-class network consist on only 254 hosts
  - Routing tables grow
  - How combine several C-class networks to act like one network?
  - How to give only few IP-addresses to a customer?
- Classless Inter-Domain Routing (CIDR)

Classless Inter-Domain Routing

- Contiguous IP network numbers can be advertised as a pair:
  - Network address of the first network
  - Number of contiguous networks
- Giving a part of a (C-class) network
- Block of addresses is power of two

Routing with CIDR

- Router cannot distinguish prefix and suffix
  - Lookups from routing table
  - Search by longest prefix (inefficient)
  - Usually hierarchical data structures are used

Summary

- Distribution of one large network
  - Subnetting and other technologies
- Classless addresses
  - Combining several network addresses
  - Using part of a network address space
  - CIDR

References

- Comer (note: more information in 4th ed. than in the 3rd ed.)
- Robert Hart: IP Sub-Networking Mini-Howto, March 1997 (GNU)
- RFC 950 - Internet Standard Subnetting procedure, August 1985

Network Address Translation (NAT)

Comer's

chapter 20 (4th ed.)

Concept of Private Internet

- Allow connection with everybody
- But hide the internal datagram transmission

- Routers/firewalls deny access of outsiders to private network
- Private network can use arbitrary IP addresses

Network Address Translation (NAT)

- IP-addresses can be mapped from one realm to another
- Transparent communication with external and private network
  - To hide private network
  - To hide invalid IP-addresses
- Works if application protocols does not use IP-addresses

NAT Translation Table

- Manual initialization
  - permanent mapping
- Outgoing datagrams
  - sent datagrams
  - most widely used
  - outsider cannot begin communication
- Incoming name lookups
  - modifications to DNS

Port-Mapped NAT

- Network Address Port Translation (NAPT)
- NAT table contains also port numbers
  - Private IP-address
  - Private port
  - NAT port
  - External IP-address
  - External port

Interaction with Other Protocols

- NAT and ICMP
  - Which ICMP messages are forwarded?
  - Echo request must be forwarded to correct host
  - Why? Destination unreachable
- NAT and applications
  - Does not work if application uses IP-addresses
  - or data in the packets must be changed

Summary & References

- Comer: “Network Address Translation technology provides transparent IP-level access to the Internet from a host with a private address.”
- Comer chapter 20
- RFC 2663 - IP Network Address Translator (NAT) Terminology and Considerations, August 1999

Address Resolution Protocol (ARP)

Comer's

chapter 5 (3rd and 4th ed.)

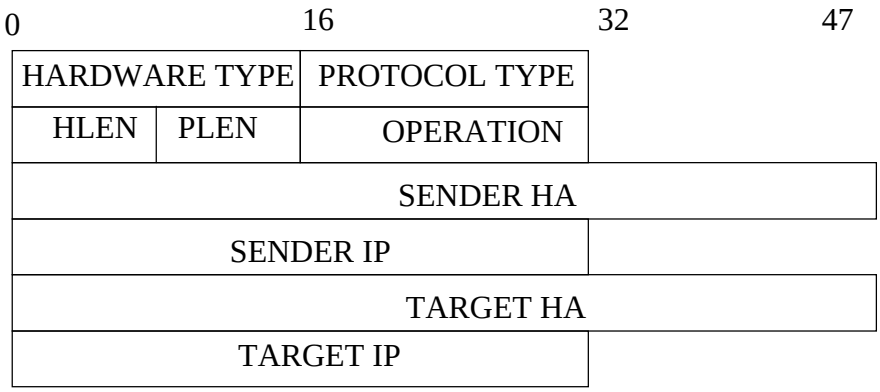
Repetition of ARP

- Address Resolution Problem
- Two kind of physical network addresses: small & flexible and long & fixed
- Address Resolution Protocol works in broadcast networks
- IP-address - hardware address pair is saved in ARP cache

Advantages and Disadvantages

- Advantages
  - Computers work independently
  - If the target does not response, it is down
  - No need for reliable transmission
- Disadvantage
  - Delay caused by cache

ARP Message Format



Sending an ARP Packet

- Check ARP cache
  - If physical address is known, send packet
- Send a broadcast request
  - Queue for outgoing packets
  - Retransmission if necessary
- Setting timer for ARP cache entries
  - If the destination goes offline or crashes

Handling of Incoming Packets

- Receiver
  - Response to the query if the physical address corresponds the machines physical address
  - Save addresses to cache
- Sender
  - Create cache entry / match with a cache entry
  - Handle additional queries of same address

Summary & References

- ARP is used to find out physical address of a machine that corresponds an IP-address
- ARP works in one physical network

- Comer
- RFC 826 - An Ethernet Address Resolution Protocol, November 1982

Dynamic Host Configuration Protocol (DHCP)

Comer's
chapter 23 (4th ed.)
chapter 21 (3rd ed.)

Purpose

- Physical network address
  - hardware dependent
- IP-address
  - independent of machine's hardware address
- How all kind of machines can find out their IP-addresses and other network settings?

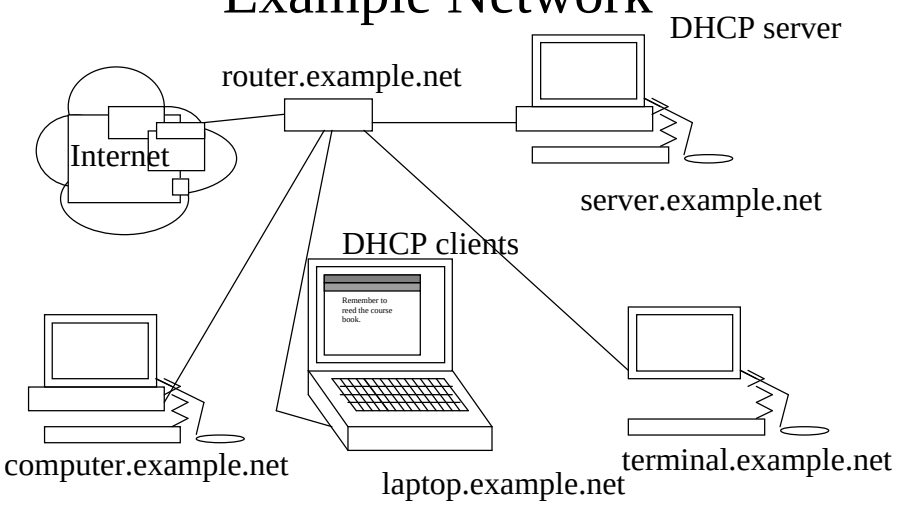
History: RARP

- Reverse Address Resolution Protocol (RARP)
- Machine without disk can find out its IP-address
- Based on ARP
- Main drawback: uses the physical network directly

History: BOOTstrap Protocol

- Application layer protocol
- Uses UDP and IP
  - before knowing machines own IP-address
  - on top of untrusted path
- Two phase protocol:
  - First get information about network
  - Then get memory image with other protocol, for example, TFTP

Example Network



DHCP

- Tree types of address assignment
  - Manual configuration
  - Automatic configuration
  - Dynamic configuration
- Example of configuration file with different kind of address assignment (next slide)

Example

```
option domain-name "example.net";
option domain-name-servers server.example.net;
option broadcast-address 10.0.1.255;
option routers router.example.net;

shared-network EXAMPLE {

  option subnet-mask 255.255.255.248;
  default-lease-time 120000;
  max-lease-time 720000;

  subnet 10.0.1.10 netmask 255.255.255.248 {
    range 10.0.1.11 10.0.1.12;
}
  host computer {
    hardware ethernet 00:01:5a:93:a7:e6;
    fixed-address computer.example.net;
  }
}
```

Dynamic Address Allocation

- Server leases an address
- A certain period of time (server/administrator decides)
- Leases can be renewed

Multiple Network Connections

- Computer that is connected to more than one network
  - Needs configuration information separately for all its interfaces
- Network may contain relay agents
  - Forwards requests to server
  - Several request from same computer may end up to same server.

State Machine of DHCP Client

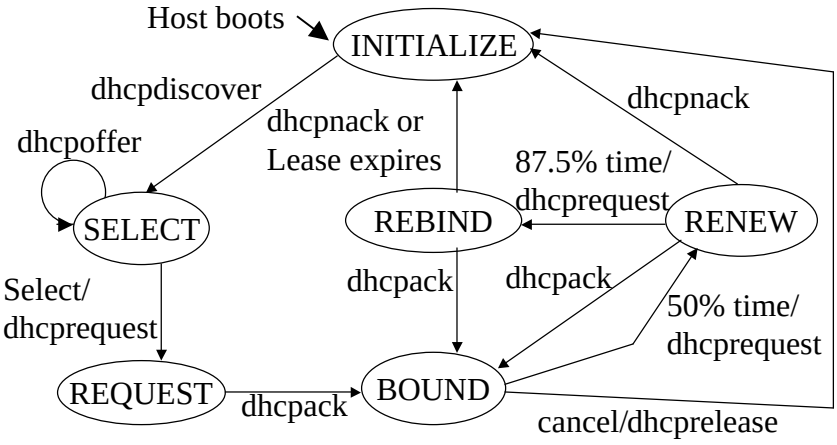


Fig. 23.4 in Comer

DHCP Message Format

0	8	16	24	31
OP	HTYPE	HLEN	HOPS	
TRANSACTION ID				
SECONDS		FLAGS		
CLIENT IP ADDRESS				
YOUR IP ADDRESS				
SERVER IP ADDRESS				
ROUTER IP ADDRESS				
CLIENT HARDWARE ADDRESS ...				
SERVER HOST NAME ...				
BOOT FILE NAME ...				
OPTIONS...				

Summary

- DHCP is used to distribute IP-addresses for computers and diskless terminals
  - Automatically or dynamically
- DHCP does not interact with DNS
  - Names must be handled separately

References

- Comer: chapters 6 and 23
- RFC 903 – A Reverse Address Resolution Protocol, 1984
- RFC 951 - Bootstrap Protocol (BOOTP), 1985
- RFC 1534 - Interoperation Between DHCP and BOOTP, 1993
- RFC 2131 – Dynamic Host Configuration Protocol, 1997
- RFC 2606 - Reserved Top Level DNS Names, 1999

Summary

- This lecture
  - Concludes the Internet Protocol facts
  - Handled many kind of address translations between layers and networks (from ARP to NAT)
  - Tells how IP-addresses can be distributed (from RARP to DHCP)