

Internet Control Protocols

CSC 343-643



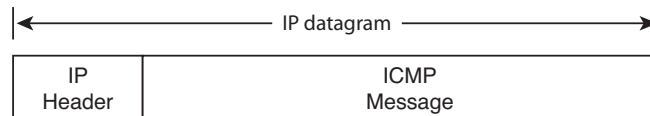
Fall 2013

Internet Control Message Protocols

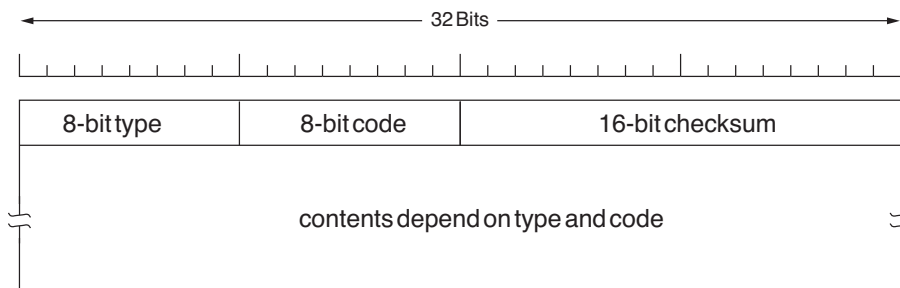
- In addition to IP, which is used for data transmission, there are several control protocols used in the network layer
 - Internet Control Message Protocol (ICMP)
 - Address Resolution Protocol (ARP)
 - Reverse Address Resolution Protocol (RARP)
 - Bootstrap Protocol (BOOTP)
 - Dynamic Host Configuration Protocol (DHCP)

Internet Control Message Protocol

- Operation of the Internet is monitored by routers
- If something unexpected occurs, event is reported to **ICMP** (Internet Control Message Protocol) RFC[792]
- ICMP messages are acted on by the IP layer or transport layer
 - Messages are either query or error oriented
- ICMP messages are transmitted within IP datagrams



- ICMP message format
 - First four bytes have the same format
 - **Type** field, identifies the ICMP message
 - **Code** field, helps specify the condition
 - **Checksum**, covers the ICMP message



ICMP Message Types

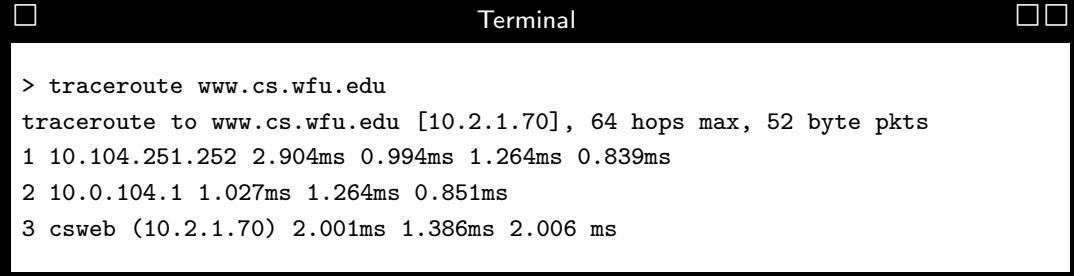
There are 15 different values for the ICMP type field, the following table lists a few, see RFC 792 for a complete list

Message Type	Description
Destination unreachable	Datagram could not be delivered
Time exceeded	TTL field reached 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach router about geography
Echo request	Ask machine if alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as echo reply, but with timestamp

- **Destination unreachable** (type = 3, code = 0 - 15)
 - Datagram was not delivered, the code identifies why
 - Example codes include
 - * If code = 0, network unreachable
 - * If code = 4, fragmentation needed, but DF set
- **Source quench** (type = 4, code = 0)
 - Was used to throttle source if congestion occurred
 - Rarely used now, since it tended to add more traffic ...
Is there congestion control in the Internet?
- **Echo request/reply** (type = 8/0, code = 0)
 - See if given destination is reachable and alive
 - ping program uses ICMP to determine if a host is alive

Tracing a Route

- A helpful program that is based on ICMP is traceroute
 - traceroute traces a route from one host to another
 - Shows the intermediate routers on the route
 - Windows version is tracert
 - Determines the route by sending a series of IP packets
 - Send a packet that has a TTL of one
 - Afterwards, send a packet that has a TTL of two
 - This repeats until a packet is sent that reaches the destination
- So how does this actually determine the route? How is ICMP actually involved?*

A terminal window titled "Terminal" with a black background and white text. It shows the command "traceroute www.cs.wfu.edu" and its output. The output displays three hops with IP addresses and round-trip times (RTT) for three packets per hop.

```
> traceroute www.cs.wfu.edu
traceroute to www.cs.wfu.edu [10.2.1.70], 64 hops max, 52 byte pkts
 1 10.104.251.252 2.904ms 0.994ms 1.264ms 0.839ms
 2 10.0.104.1 1.027ms 1.264ms 0.851ms
 3 csweb (10.2.1.70) 2.001ms 1.386ms 2.006 ms
```

- Output is the route hop followed by the round-trip times (RTT)
 - Three packets are sent per hop, each RTT is displayed
 - If no response for a hop, then *'s are printed
- traceroute has several command line options
 - The option -g allows loose source routing
 - The option -t allows you to alter the ToS bits

When ICMP Message is Never Generated

- An ICMP message should never be generated in response to

1. An ICMP *error* message

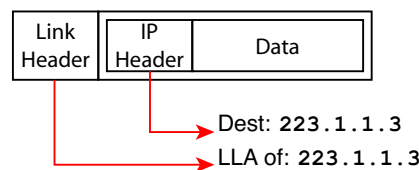
An ICMP message is sent in response to a query message, what is an example?

2. A datagram destined to an IP broadcast or multicast address
3. A datagram sent as a link-layer broadcast
4. A fragment other than the first
5. A datagram that does not identify a single host (includes zero address, loopback address, broadcast address, and multicast address)

What problems are we trying to avoid with these rules?

Layer 3 Addresses versus Layer 2 Addresses

- Sending IP datagrams requires knowledge of the link-layer address
 - The IP datagram is placed inside a link-layer frame then sent



- Hosts are attached to the network via an interface card
 - The interface card is a layer 1 and 2 device
 - Can only understand **LAN addresses** (also called **hardware address** or **MAC address**)

- For example, every Ethernet board has a 48-bit Ethernet address
 - In DOS run `winipcfg` to determine the Ethernet address
 - Card manufacturers given a *block* of Ethernet addresses
 - Assignments given in RFC 1700 or a more up-to-date at <http://standards.ieee.org/regauth/oui/oui.txt>

MAC addresses were used at Duke to reduce laptop theft, how?

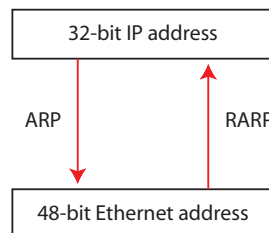
- Similar to IP, hardware address of all 1's is for broadcast

Who will receive such broadcasts?

How do IP addresses get mapped to data-link addresses?

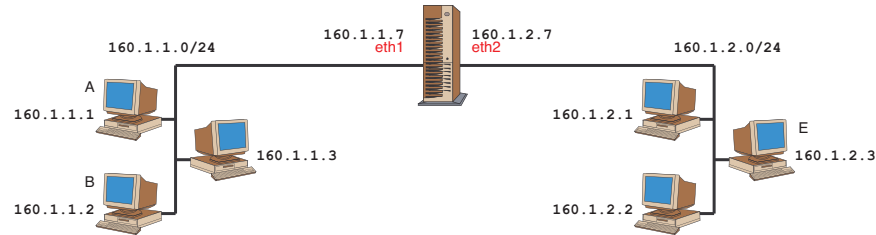
Address Resolution

- Address resolution - Mapping between two different address forms
 - IP addresses and data-link addresses
- Two different protocols in IP
 - Address Resolution Protocol (ARP)
 - Reverse Address Resolution Protocol (RARP)



ARP

- Dynamic mapping of IP address → hardware address [RFC 826]
- Assume A needs the hardware address of host B



- Host A broadcasts an ARP request
 - Ethernet address of all 1's is the broadcast address
 - Host asks *"Who owns IP address 160.1.1.2?"*
- Host B would reply with its hardware address

- ARP is intended for broadcast (shared medium) networks
 - Not needed for point-to-point links
- Would A ever send an ARP request for the MAC address of E?*

- **Proxy ARP**
 - Assume host A does send an ARP request for host E (routing table incomplete or wrong)
 - If router is set-up to respond with its hardware address to any address outside of subnet, then this is proxy ARP
- **Gratuitous ARP**
 - Host sends request for own IP address
 - Lets host determine if another host using same IP address

ARP Optimization

There are various ways to improve the efficiency of ARP

- ARP Tables
 - Keep an ARP table for most recently used IP addresses
 - Entries can time-out
- Hey, this *used to be* lots of fun...
 - When your laptop is first connected to the network, enter the DOS command, `arp -a`
 - Ping a *local* machine on the network
 - Issue the `arp` command again, should see hardware (physical) address for the machine
 - This may be a proxy ARP, how can you tell?*
 - Wait a few minutes and issue the `arp` command again

- Broadcast at boot-time
 - When a machine connects, broadcast its mapping (ARP reply)
 - All hosts on network (or subnet) will know the IP and hardware address of the new machine
 - This is a big problem at Wake Forest, why?*
 - Also called gratuitous ARP, *a great way to spread ARP poison...*

ARP Security

- ARP introduces security problems

How could this protocol be used to obtain important information from users?

- A common way around this security issue is to use **static ARP**
 - Permanent ARP table created, for example
`/sbin/arp -s IPaddress MACaddress`
 - *So what is ARPish about this solution...*

Reverse Address Resolution Protocol

- Dynamic mapping of hardware address → IP address [RFC 903]
- If a host does not have an IP address, sends RARP request
 - Broadcast message *“My hardware address is x , what is my IP address?”*
 - **RARP server** responds with the appropriate IP address

Again the broadcast address is a link-layer address of all 1's, what is the limitation of this?

Dynamic Host Configuration Protocol

Provides configuration parameters to Internet hosts [RFC 2131]

- DHCP consists of two components
 1. Mechanism for allocation of network addresses to hosts
 2. Delivering host-specific configuration parameters to hosts
- If a host does not have an IP address, sends DHCP request
 - Broadcast message *“Can I have an IP address?”*
 - **DHCP server** responds with the appropriate IP address

This smells like RARP? What is the difference?
- DHCP goes beyond RARP by providing
 - IP address leases
 - Additional network configuration information

DHCP Operation

1. Host connects to the network as sends DHCPDISCOVER
 - Request for IP address from DHCP server(s)

How does the host know the address of the DHCP server?
2. Server responds with DHCPOFFER
 - Contains IP address and configuration parameters
 - Contains the IP address lease time

What is the IP address of the host?
3. Host responds with DHCPREQUEST (may receive multiple offers)
 - Confirms the offer from the server

4. Server responds with DHCPACK
 - Configuration parameters (committed network address)
5. Once the host is done sends DHCPRELEASE to server
 - Relinquishing network address and cancelling remaining lease

DHCP is used for laptops on campus. As a result, is it possible to run a web-server (or any other type of server) as a host on these networks?

DHCP, BOOTP, and RARP FAQ

- DHCP is based on BOOTP (backwards compatible)
 - BOOTP was designed for manual pre-configuration of the host information in a server database
 - DHCP allows for dynamic allocation (leasing) of network addresses and configurations to newly attached hosts
- RARP is a protocol used by Sun that allows a computer to determine its IP number (done by DHCP or BOOTP)
 - RARP doesn't support other parameters and using it, a server can only serve a single LAN. DHCP and BOOTP are designed so they can be **routed**; thus serve multiple LANs
- *Can multiple DHCP servers exist on the same network?*
 - Yes, if each has a dynamic pool accessible to the same clients, then even if one server is down, one of those clients can lease an address from the other server.

- Without communication between the two servers to share their information on current leases, when one server is down, any client with a lease from it will not be able to renew their lease with the other server. Such communication is the purpose of the "server to server protocol".
- *Where does the error about a duplicate IP come from?*
 - A host is to verify it's lease during bootup. It seems that every host during bootup does not verify it's lease, it just takes the configuration it received before shutting down the last time. If in the mean time the lease expired and was offered to another host, this could cause a IP address conflict. One host acts upon the current lease offered by the DHCP server and the other host thinks it still leases the IP address. This is why some DHCP enabled clients can experience duplicate IP address on the network. **Always remember to release your IP address?**