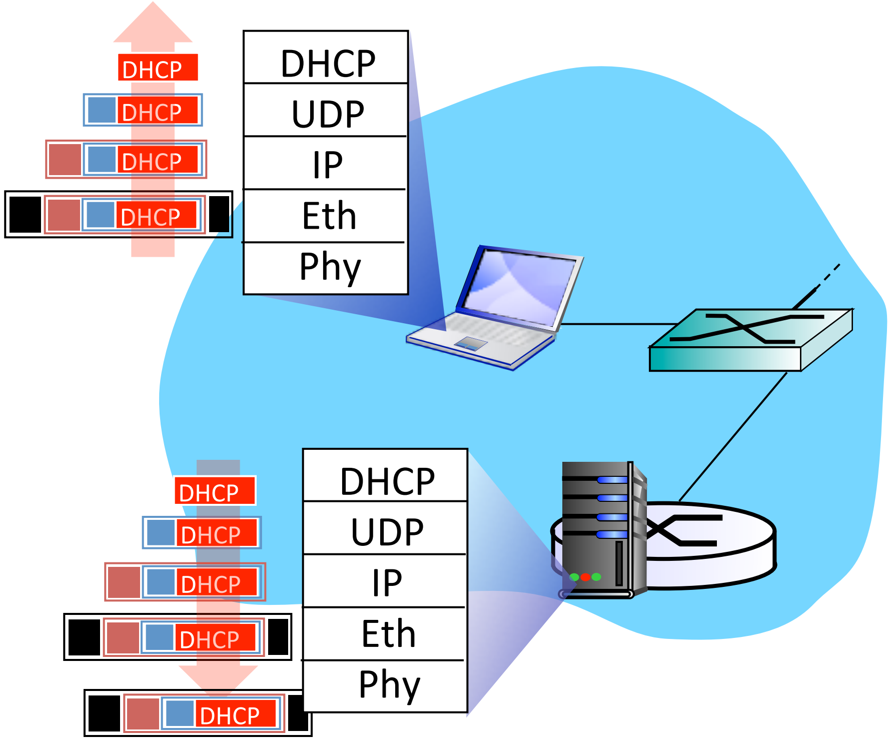
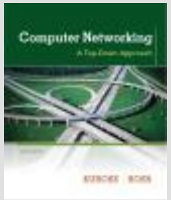
DHCP, ICMP, IPv6



Computer Networking: A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley



Chapter 4: outline

4.1 Introduction

4.2 Virtual circuit and datagram networks

4.3 What's inside a router

4.4 IP: Internet Protocol

- Datagram format
- IPv4 addressing
- Network Address Translation (NAT)
- DHCP
- ICMP
- IPv6
- IPsec

4.5 Routing algorithms

- Link state
- Distance vector
- Hierarchical routing

4.6 Routing in the Internet

- RIP
- OSPF
- BGP

4.7 Broadcast and multicast routing

IP addresses: How to get one?

Q: How does a *host* get IP address?

- Hard-coded by in a file:
  - Windows:
    - Control-panel -> Network -> Config -> TCP/IP -> Properties
  - Ubuntu:
    - /etc/network/interfaces
- DHCP: Dynamic Host Configuration Protocol
  - Dynamically get address from a server
  - Plug-and-play

DHCP protocol

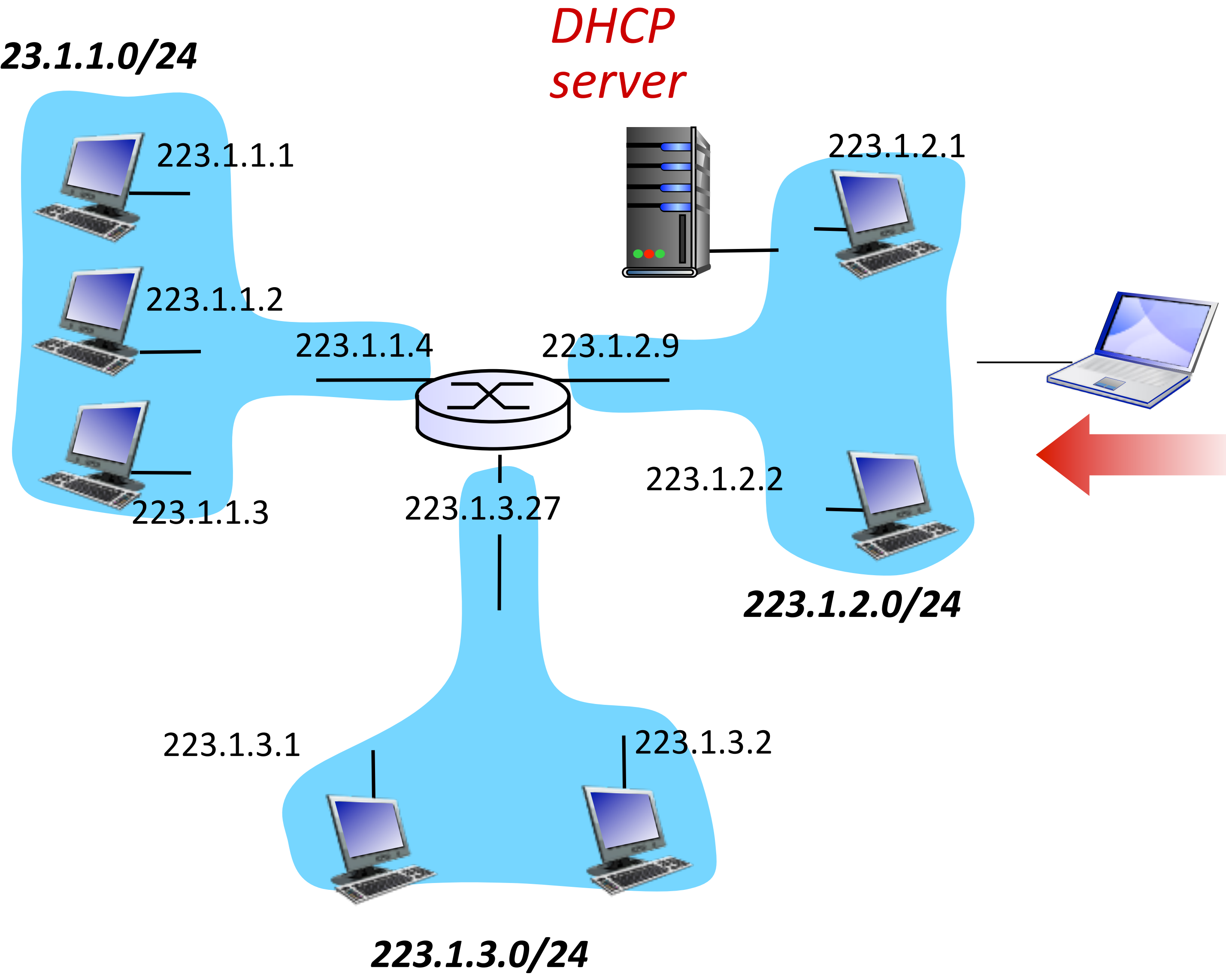
Goal: Host *dynamically* obtains IP from network

- Can renew its lease on address in use
- Allows reuse of addresses
  - Only hold address while connected
- Support for mobile users who want to join network

DHCP overview:

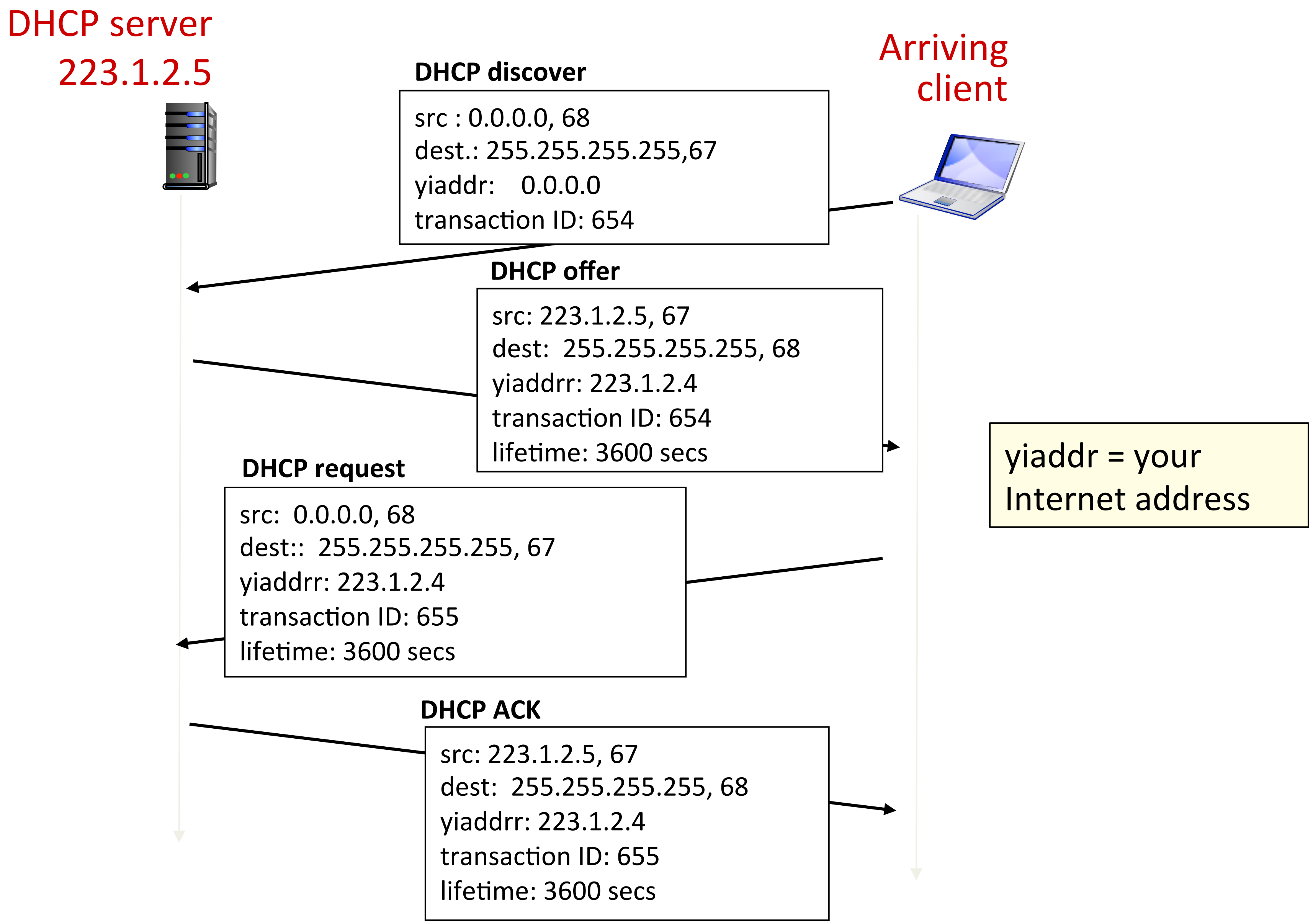
- Host broadcasts DHCP discover msg
- DHCP server responds with DHCP offer msg
- Host requests IP address: DHCP request msg
- DHCP server sends address: DHCP ACK msg

DHCP client-server scenario



Arriving *DHCP client* needs address in this network

DHCP client-server scenario



DHCP server
223.1.2.5

Arriving
client

DHCP discover

src : 0.0.0.0, 68
dest.: 255.255.255.255,67
yiaddr: 0.0.0.0
transaction ID: 654

DHCP offer

src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddrr: 223.1.2.4
transaction ID: 654
lifetime: 3600 secs

DHCP request

src: 0.0.0.0, 68
dest:: 255.255.255.255, 67
yiaddrr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

DHCP ACK

src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddrr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

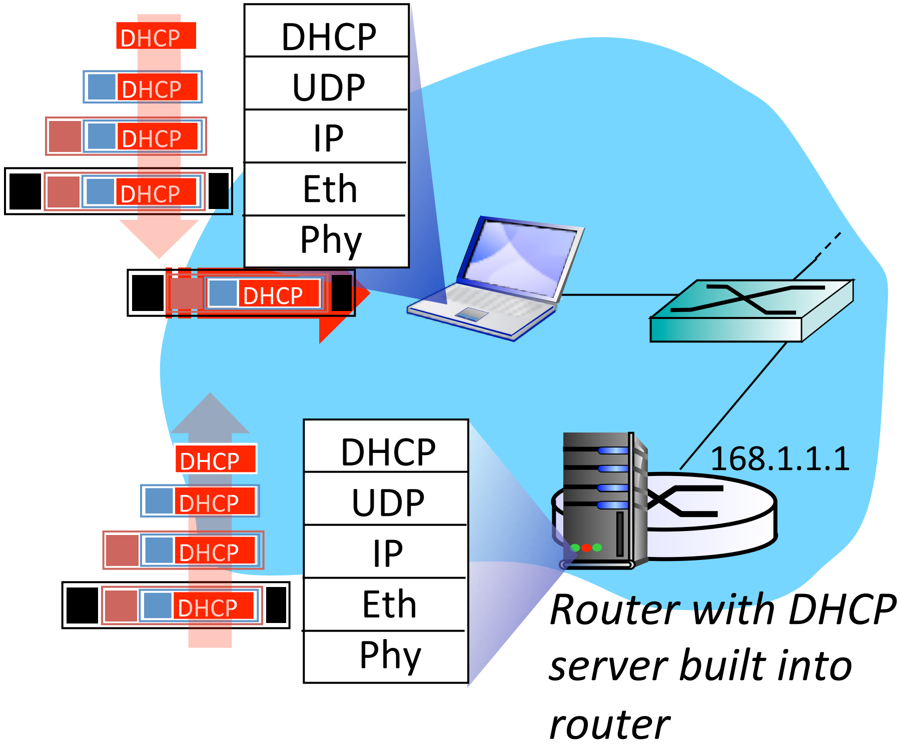
yiaddr = your Internet address

DHCP: More than IP addresses

DHCP can return more than just allocated IP address on subnet:

- Address of first-hop router for client
- Name and IP address of DNS sever
- Network mask
  - Indicating network versus host portion of address

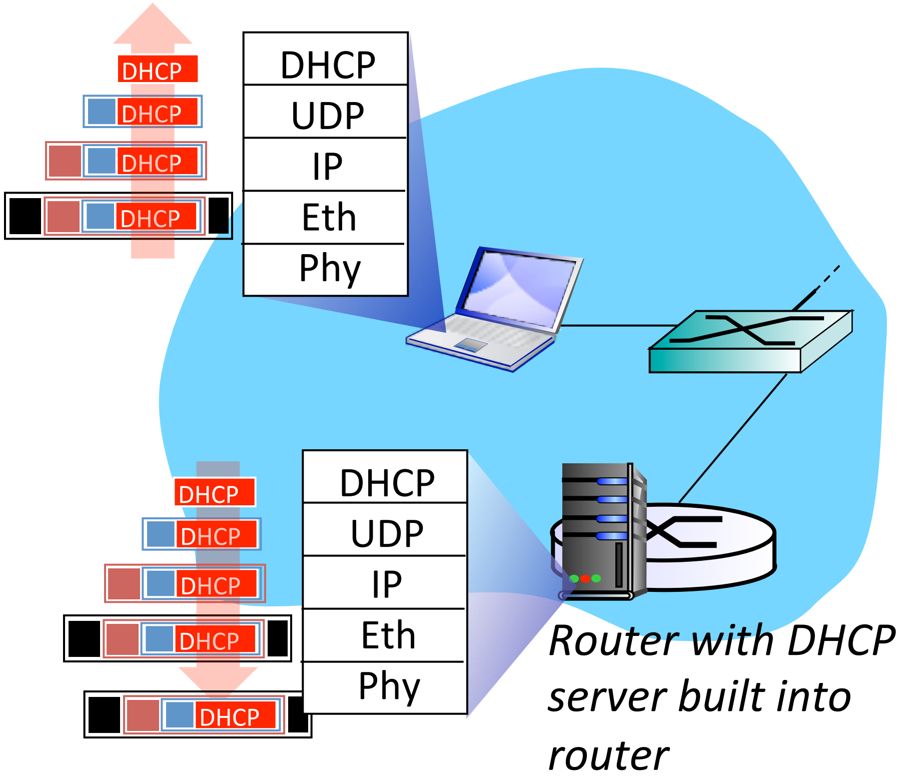
DHCP: example



Router with DHCP server built into router

- Connecting laptop needs IP address, address of first-hop router, address of DNS server: use DHCP
- DHCP request encapsulated in UDP, encapsulated in IP, encapsulated in Ethernet
- Ethernet frame broadcast (destination: FFFFFFFFFFFF) on LAN, received at router running DHCP server
- Ethernet demuxed to IP, UDP demuxed to DHCP

DHCP: example



- DCP server formulates DHCP ACK containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server

- Encapsulation of DHCP server, frame forwarded to client, demuxing up to DHCP at client

- Client now knows its IP address, name and IP address of DSN server, IP address of its first-hop router

DHCP: Wireshark trace

request

```
Message type: Boot Request (1)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP Request
Option: (61) Client identifier
    Length: 7; Value: 010016D323688A;
    Hardware type: Ethernet
    Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Option: (t=50,l=4) Requested IP Address = 192.168.1.101
Option: (t=12,l=5) Host Name = "nomad"
Option: (55) Parameter Request List
    Length: 11; Value: 010F03062C2E2F1F21F92B
    1 = Subnet Mask; 15 = Domain Name
    3 = Router; 6 = Domain Name Server
    44 = NetBIOS over TCP/IP Name Server
    ……
```

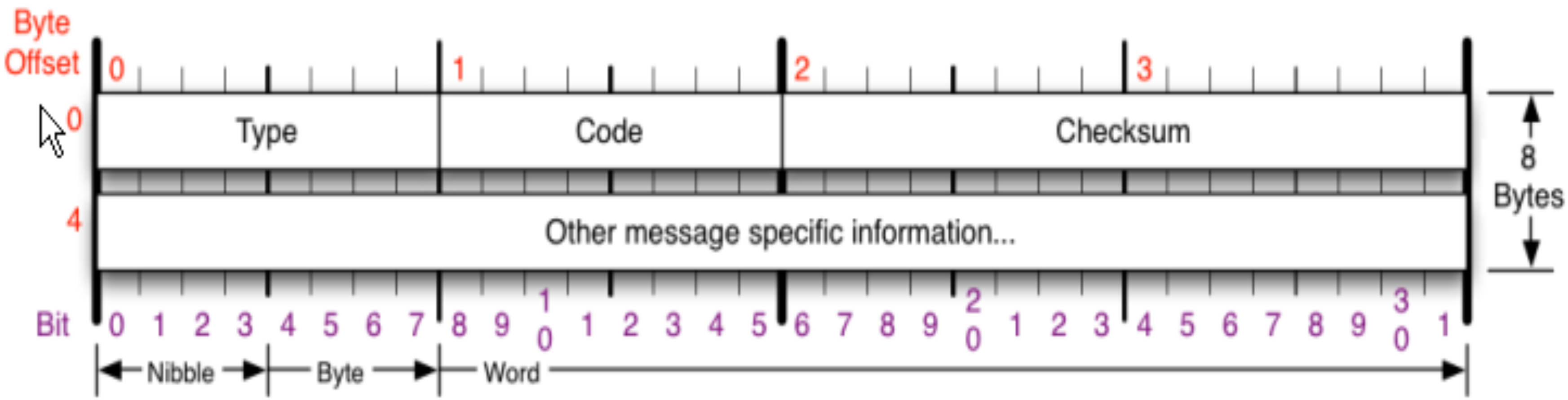
reply

```
Message type: Boot Reply (2)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.1.101 (192.168.1.101)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 192.168.1.1 (192.168.1.1)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=54,l=4) Server Identifier = 192.168.1.1
Option: (t=1,l=4) Subnet Mask = 255.255.255.0
Option: (t=3,l=4) Router = 192.168.1.1
Option: (6) Domain Name Server
    Length: 12; Value: 445747E2445749F244574092;
     IP Address: 68.87.71.226;
     IP Address: 68.87.73.242;
     IP Address: 68.87.64.146
Option: (t=15,l=20) Domain Name = "hsd1.ma.comcast.net."
```

Network error reporting

- Internet Control Message Protocol (ICMP)
  - Considered network layer
    - But ICMP carried inside IP datagram (like TCP/UDP)
  - Error messages sent back to host by routers
  - ICMP used by some user utilities:
    - traceroute
    - ping

ICMP



ICMP Message Types

Type	Code/Name
0	Echo Reply
3	Destination Unreachable
	0 Net Unreachable
	1 Host Unreachable
	2 Protocol Unreachable
	3 Port Unreachable
	4 Fragmentation required, and DF set
	5 Source Route Failed
	6 Destination Network Unknown
	7 Destination Host Unknown
	8 Source Host Isolated
	9 Network Administratively Prohibited
	10 Host Administratively Prohibited
	11 Network Unreachable for TOS
3	Destination Unreachable (continued)
	12 Host Unreachable for TOS
	13 Communication Administratively Prohibited
4	Source Quench
5	Redirect
	0 Redirect Datagram for the Network
	1 Redirect Datagram for the Host
	2 Redirect Datagram for the TOS & Network
	3 Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceded
	0 TTL Exceeded
	1 Fragment Reassembly Time Exceeded
12	Parameter Problem
	0 Pointer Problem
	1 Missing a Required Operand
	2 Bad Length
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

Checksum

Checksum of ICMP header

RFC 792

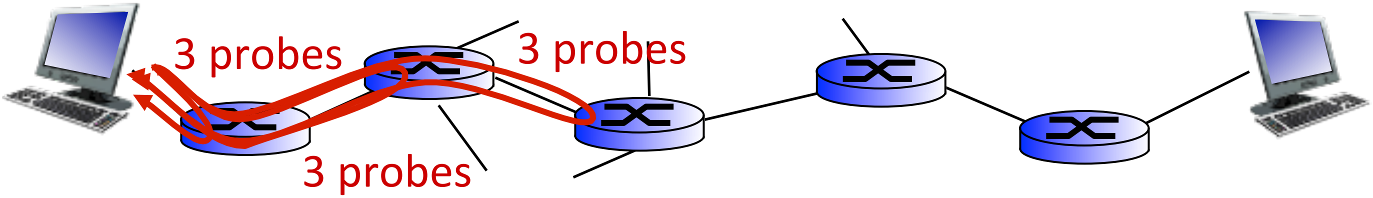
Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.

Traceroute and ICMP

- Source sends series of UDP segments to dest
  - First set has TTL =1
  - Second set has TTL=2, etc.
  - Unlikely port number
- When *n*th set of datagrams arrives to *n*th router:
  - Router discards datagrams
  - Sends source ICMP messages (type 11, code 0)
  - ICMP messages includes name of router & IP address
- When ICMP messages arrives, source records RTTs

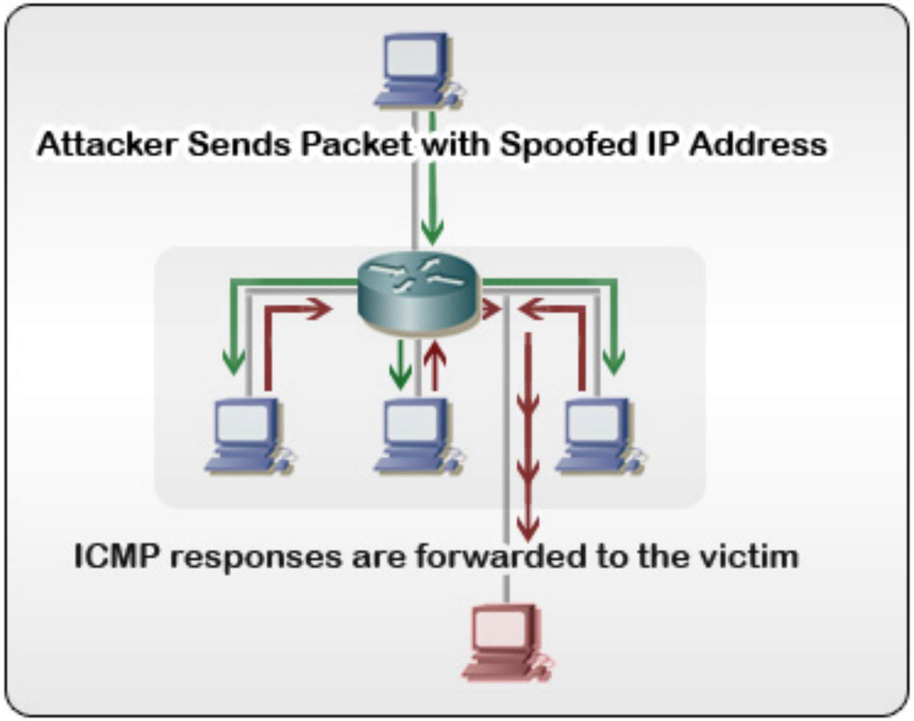
Stopping criteria:

- UDP segment eventually arrives at destination host
- Destination returns ICMP port unreachable message (type 3, code 3)
- Source stops



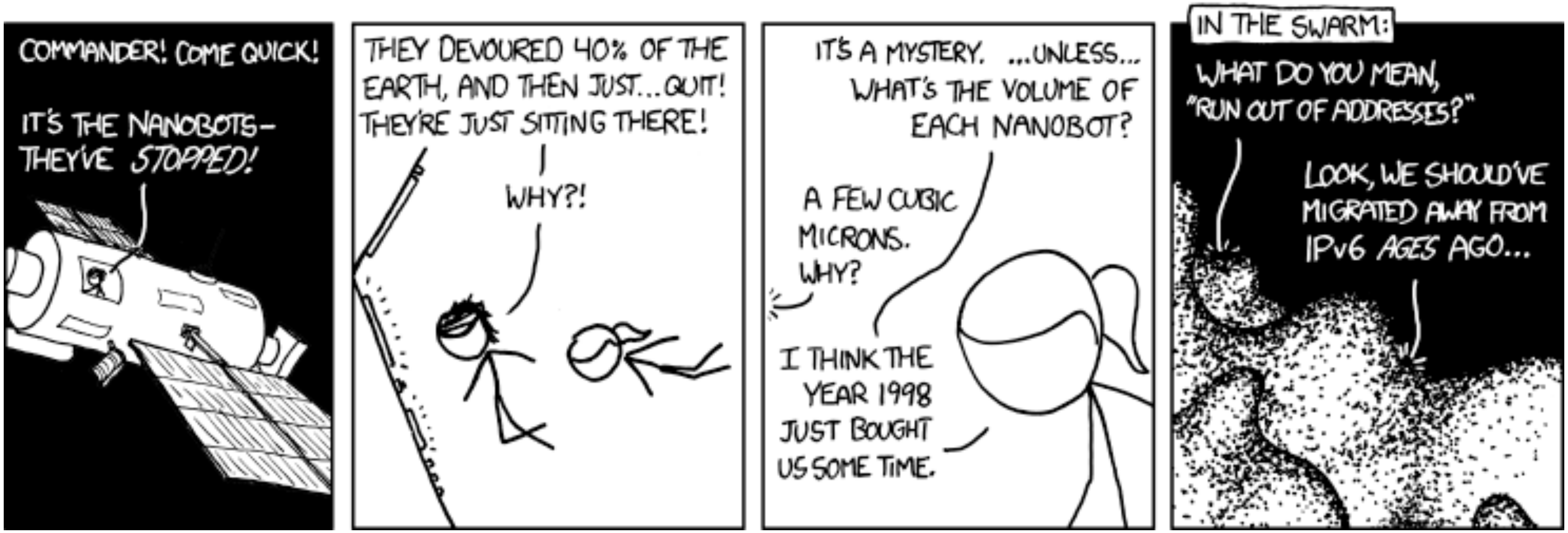
Smurf Attack

- Denial-of-Service attack
  - Attacker sends stream of ICMP echo requests
  - Sent to network broadcast address
  - Uses spoofed IP of victim
  - Generates large amounts of traffic on target network


Attacker Sends Packet with Spoofed IP Address
ICMP responses are forwarded to the victim

New and improved Internet Protocol

- Birth of IP version 6
  - Started looking at IPv4 exhaustion in 1991
  - Increase address size → new IP packet header
    - Thus new software for every Internet host/router
    - Might as well overhaul the whole thing
    - Draft standard in 1998


COMMANDER! COME QUICK!
IT'S THE NANOBOTS– THEY'VE STOPPED!
THEY DEVOURED 40% OF THE EARTH, AND THEN JUST...QUIT! THEY'RE JUST SITTING THERE!
WHY?!
IT'S A MYSTERY. ...UNLESS... WHAT'S THE VOLUME OF EACH NANOBOT?
A FEW CUBIC MICRONS. WHY?
I THINK THE YEAR 1998 JUST BOUGHT US SOME TIME.
IN THE SWARM:
WHAT DO YOU MEAN, "RUN OUT OF ADDRESSES?"
LOOK, WE SHOULD'VE MIGRATED AWAY FROM IPv6 AGES AGO...

http://xkcd.com/865/

IPv6 goals & features

1. Support billions of hosts
   - 2^{128} addresses ≈ 3 x 10^{38}
   - If entire planet covered with computers:
     - 7 x 10^{23} IPs/ m^2, pessimistic util. scenario: 1000 IPs / m^2
   - Address format: 8 groups of 4 hex digits

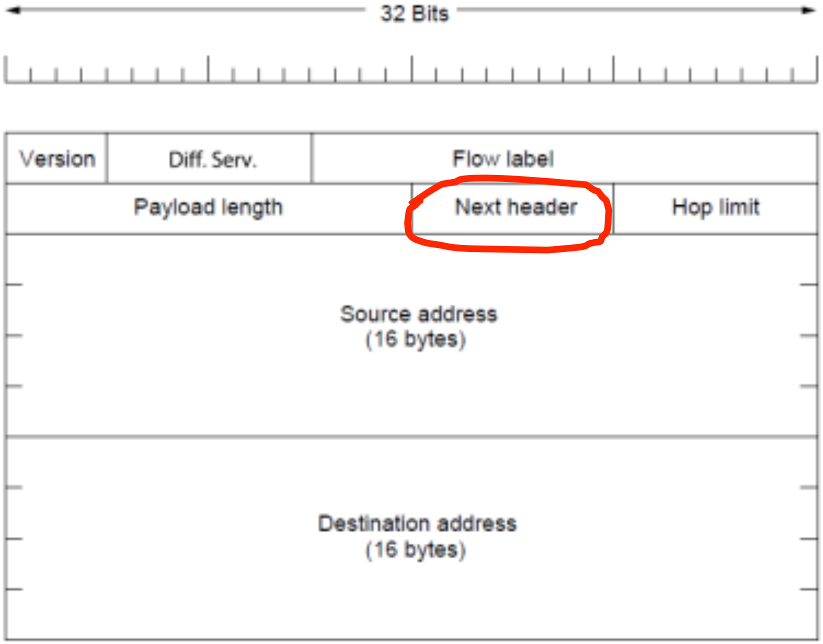
Full address	8000:0000:0000:0000:0123:4567:89AB:CDEF
Abbreviated	8000::0123:4567:89AB:CDEF
IPv4 mapped to IPv6	::FFFF:192.31.20.46

00...0 (128 bits)	Unspecified
00...1 (128 bits)	Loopback
1111 1111...	Multicast address
1111 1110 10...	Link-local unicast
Everything else	Global unicast addresses, 99% of the space

IPv6 goals & features

2. Simplify the protocol

- Allow routers to process packets faster
- Support gigabit/terabit routing
  - Predictable header size (40 bytes)
  - Removed little used fields
  - No checksum
- Allow future evolution
- Extension headers



32 Bits

Version

Diff. Serv.

Flow label

Payload length

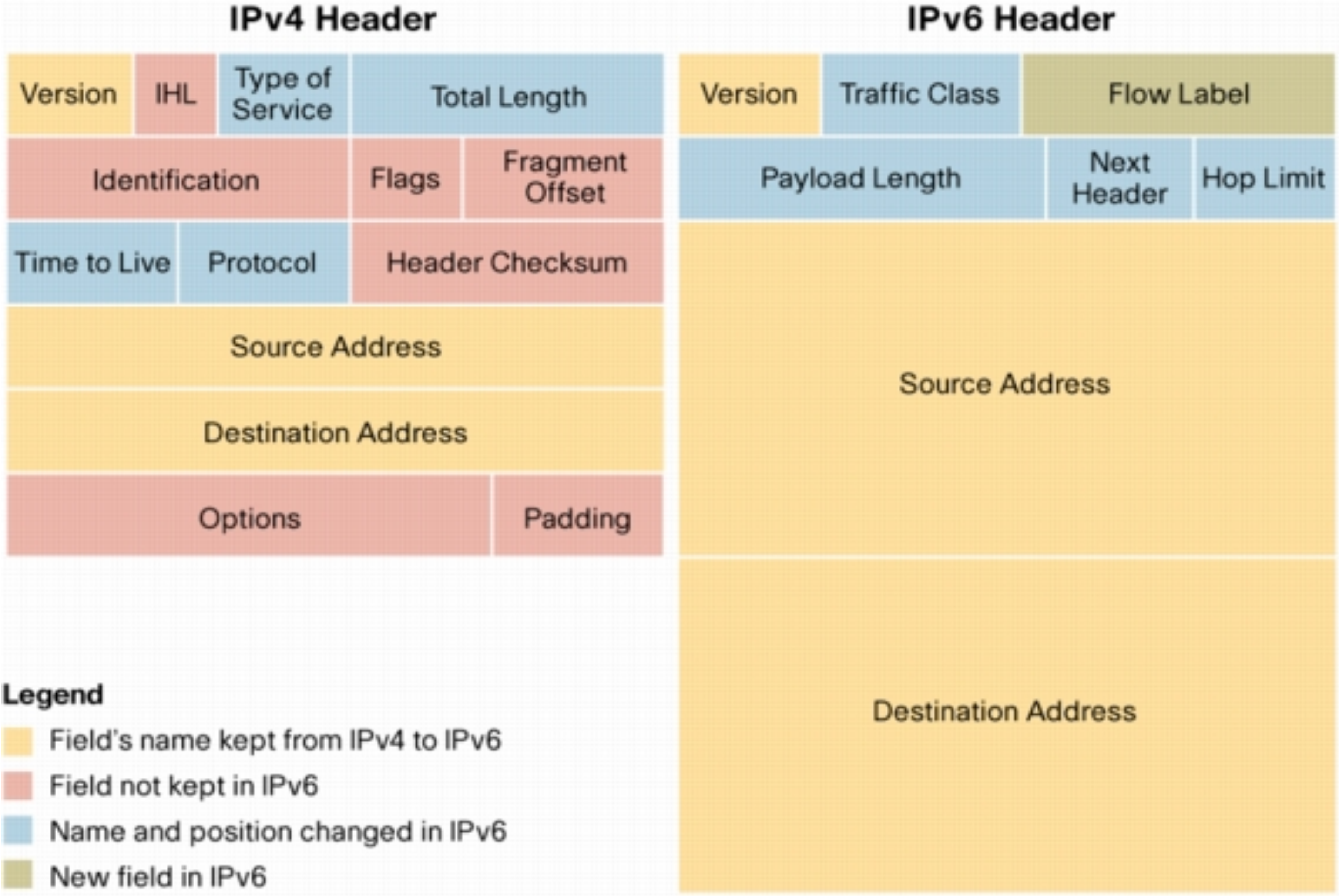
Next header

Hop limit

Source address
(16 bytes)

Destination address
(16 bytes)

IPv6 fixed 40-byte header.



IPv4 Header

Version	IHL	Type of Service	Total Length
Identification	Flags	Fragment Offset	
Time to Live	Protocol	Header Checksum	
Source Address			
Destination Address			
Options	Padding		

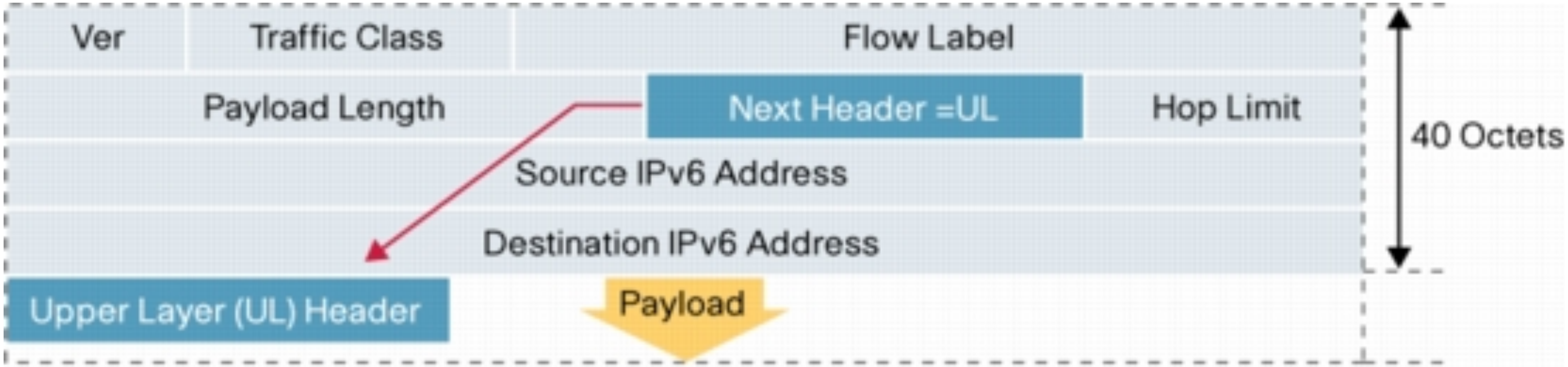
IPv6 Header

Version	Traffic Class	Flow Label
Payload Length	Next Header	Hop Limit
Source Address		
Destination Address		

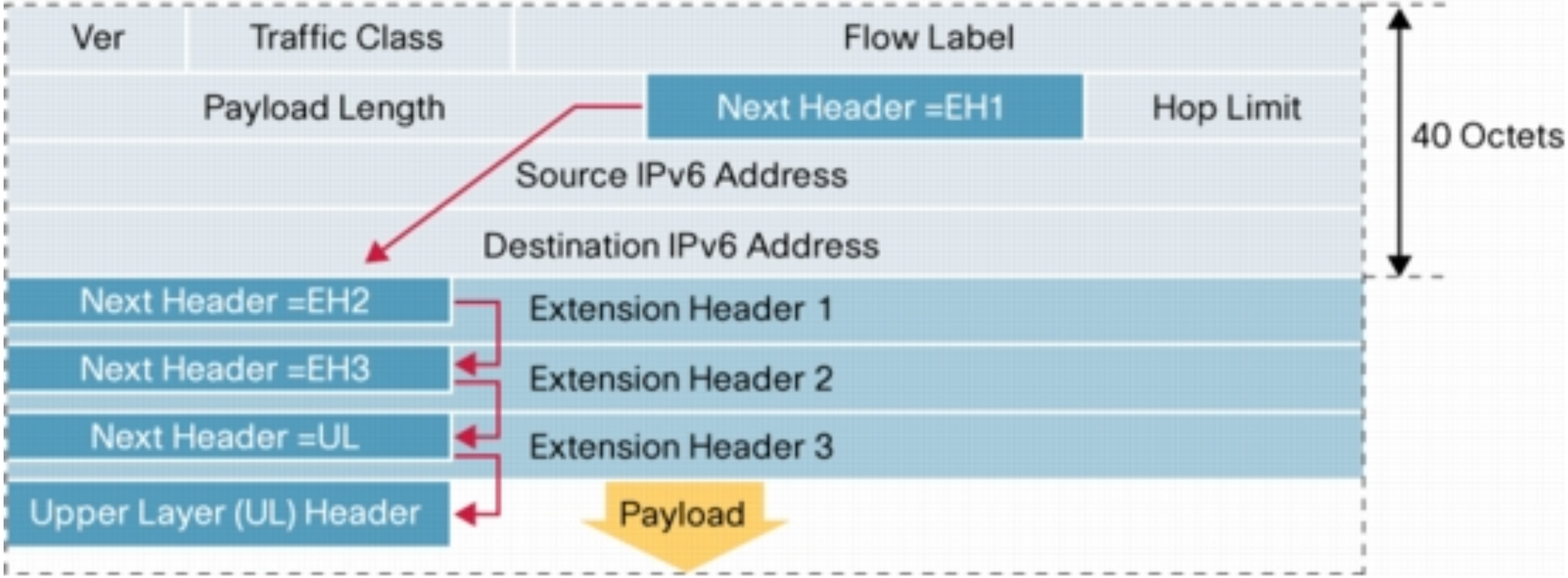
Legend

- 🟨 Field's name kept from IPv4 to IPv6
- 🟥 Field not kept in IPv6
- 🟦 Name and position changed in IPv6
- 🟫 New field in IPv6

http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html



Packet with Extension Header



http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

Extension headers

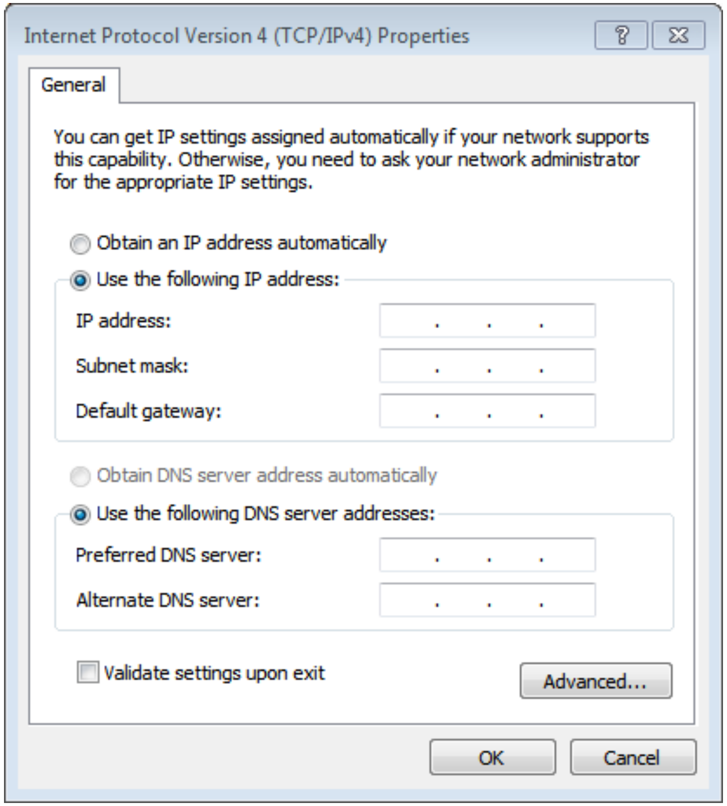
- Next header field
  - Allows chain of extension headers
  - Last one indicates payload protocol
    - e.g. 6 = TCP, 17 = UDP

Extension header	Description
Hop-by-hop options	Only extension that must be processed by all nodes. Support for datagrams exceeding 64 KB.
Destination options	Fields needed at destination host.
Routing	Lists one or more routers than must be visited on the way to destination. Similar to IPv4 loose source routing.
Fragmentation	Datagram identifier, fragment number, more fragments to follow. Must be done by source host, no fragmentation allowed in-route. IPv6 requires MTU path discovery.
Authentication	Receiver can verify who sent it.
Encrypted security payload	Allows payload to be encrypted so only receiver can read it.

IPv6 goals & features

3. Autoconfiguration of hosts

- – Guaranteed unique IPv6 addr: prefix + 48-bit MAC
- – Avoid users dealing with 16 bytes addresses


Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

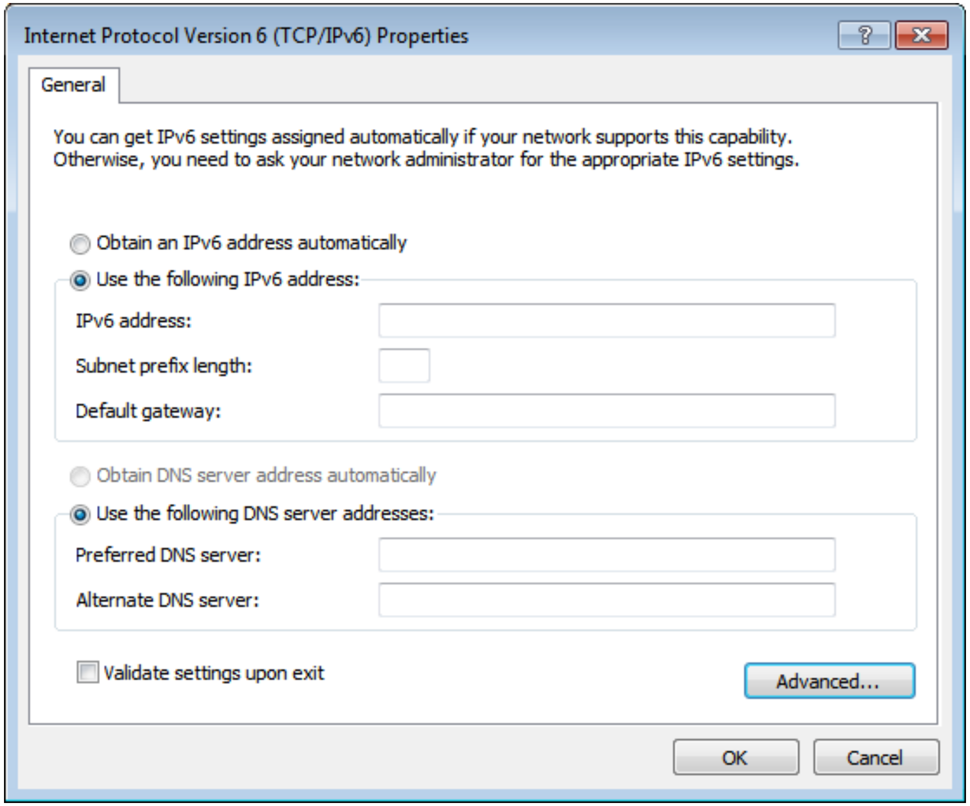
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

192.168.1.3


Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

○ Obtain an IPv6 address automatically

● Use the following IPv6 address:

IPv6 address:

Subnet prefix length:

Default gateway:

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:

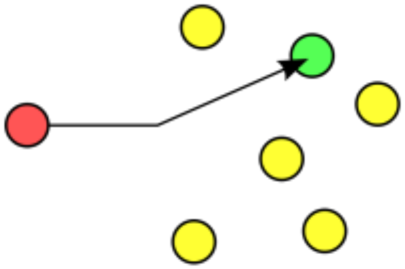
Alternate DNS server:

□ Validate settings upon exit

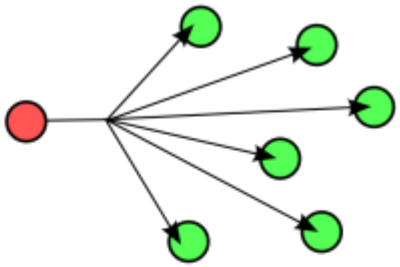
8000:0000:0000:0000:0123:4567:89AB:CDEF

IPv6 goals & features

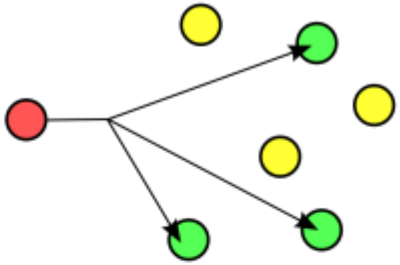
4. Multicast/multimedia
   - – Multicast a requirement, no longer optional
   - – IPv4 DiffServ field + new 20-bit traffic flow field
   - – Anycast, one address for a group of nodes
     - Delivery to only one node
     - Fault-tolerance, load balancing
     - Routing to closest node



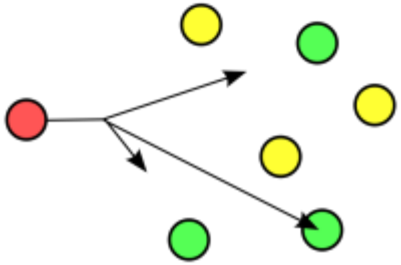
Unicast



Broadcast



Multicast



Anycast

IPv6 goals & features

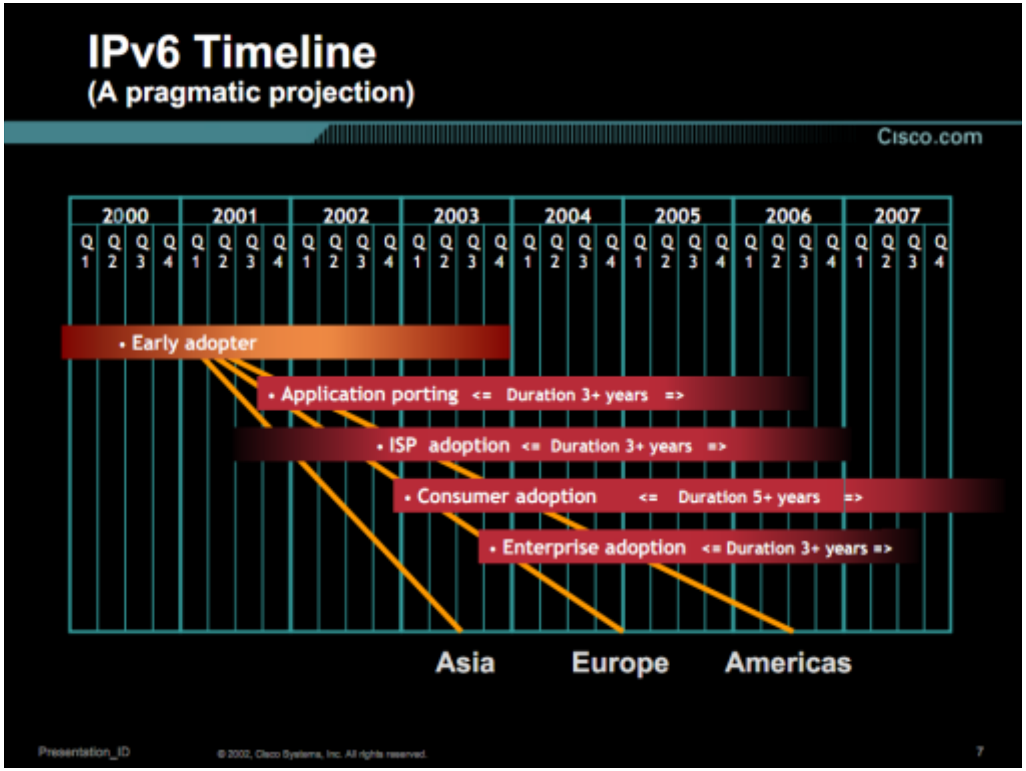
5. Improved security
   - IP security architecture (IPSec)
     - End-to-end security at the network layer
     - Must be in a IPv6 complaint node
     - An optional feature of an IPv4 node
   - Authentication header (AH)
     - Supports many different authentication techniques
     - Protects against attacks based on masquerading
   - Encapsulating security payload (ESP)
     - Integrity and confidentiality of datagram

IPv6 goals & features

6. Support for mobile hosts
   - Mobile clients likely to be majority of IPv6 hosts
   - Mobile IPv6 (RFC 3775)
   - Use IPv6 features:
     - Stateless autoconfiguration
     - Neighbor discovery
     - Extension headers such as routing header

IPv6 goals & features

7. Ease of deployment
   - Achilles heel of IPv6
     - Google 2008 estimate, < 1% of traffic
   - We can't have a "flag" day to switch over

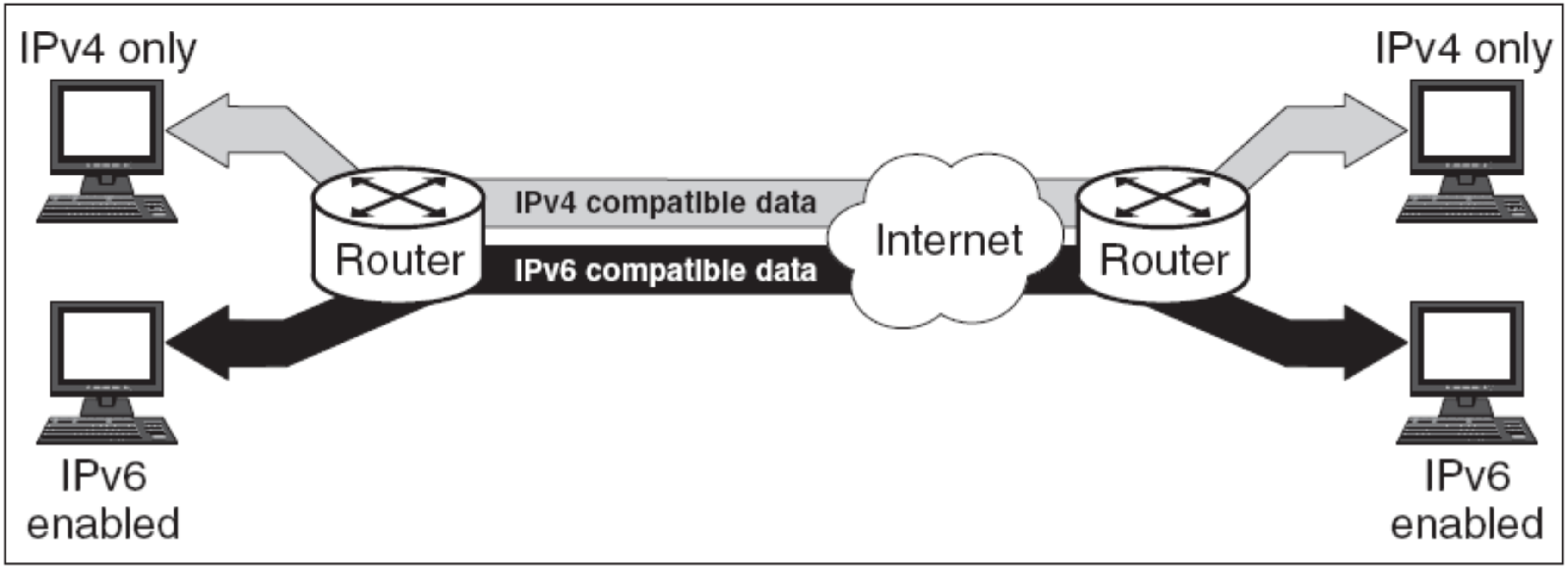


IPv6 Timeline

(A pragmatic projection)

Deploying IPv6

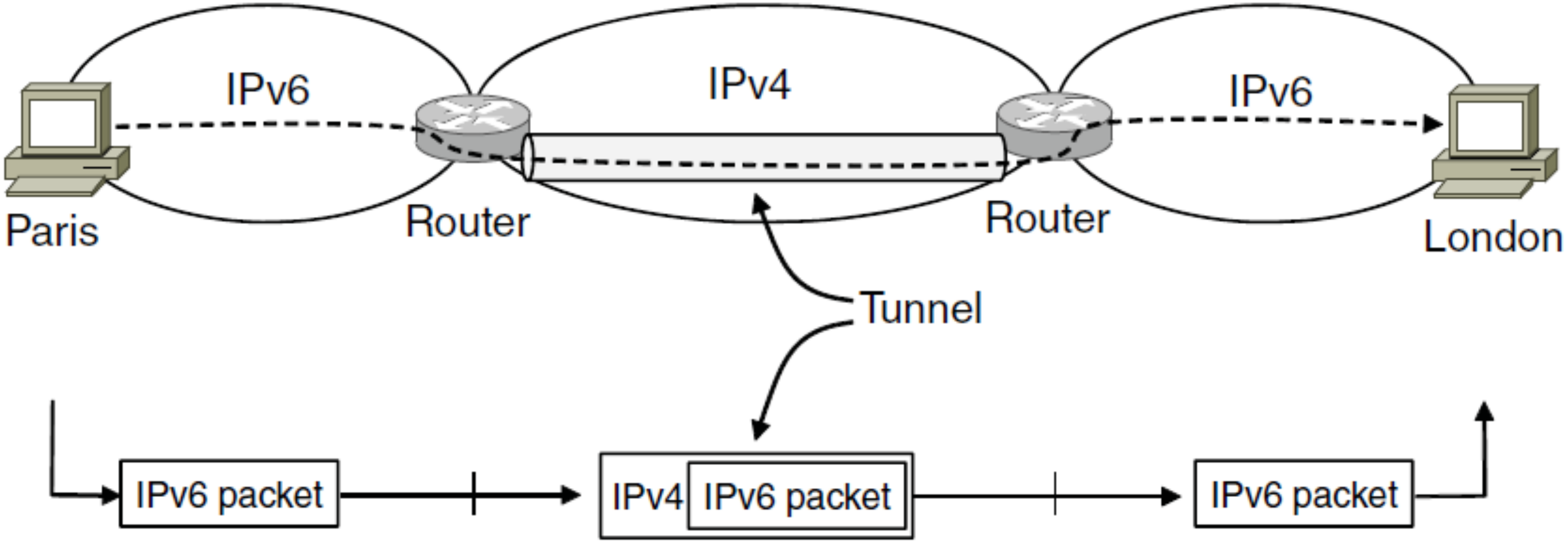
- Dual-stack operation
  - IPv6 nodes also run IPv4
    - Consult version field in header to decide
  - Supported by major OS's for a long time
  - Any IPv4-only node in path = loss of IPv6 info



Source: GAO.

Deploying IPv6

- Tunneling IPv6 over IPv4 networks
  - – Route IPv6 traffic over network segment that only understands IPv4



IPsec

- Internet Protocol
  - Designed in the 1970s by mutually trusting researchers, security not a major design concern
- IPsec
  - Connection-oriented security between two hosts
  - *Cryptographic agreement*, what algorithms/keys
  - *Encryption* of payload
  - *Data integrity*, payload not modified in transit
  - *Origin authentication*, source is the real source

Summary

- Getting an IP address
  - DHCP protocol
- Sending network info/error messages
  - ICMP protocol
- Dealing with IPv4 address scarcity
  - IPv6
- Security at the network-layer
  - IPsec