

Internet Protocol Addressing



SI-E Workshop
AfNOG

Purpose of an IP address

- Unique Identification of:
 - Source
 - How would the recipient know where the message came from?
 - How would you know who hacked into your network (network/data security)
 - Destination
 - How would you send data to other network
- Network Independent Format
 - IP over anything

Purpose of an IP Address

Identifies a machine's connection to a network

- Uniquely assigned in a hierarchical format
 - IANA (Internet Assigned Number Authority)
 - IANA to RIRs (AfrINIC, ARIN, RIPE NCC, APNIC, LACNIC)
 - RIR to ISPs and large organisations
 - ISP or company IT department to end users
- IPv4 uses unique 32-bit addresses
- IPv6 uses unique 128-bit addresses

Basic Structure of an IPv4 Address

- 32 bit number (4 octet number):
(e.g. 133.27.162.125)
- Decimal Representation:

133	27	162	125
-----	----	-----	-----

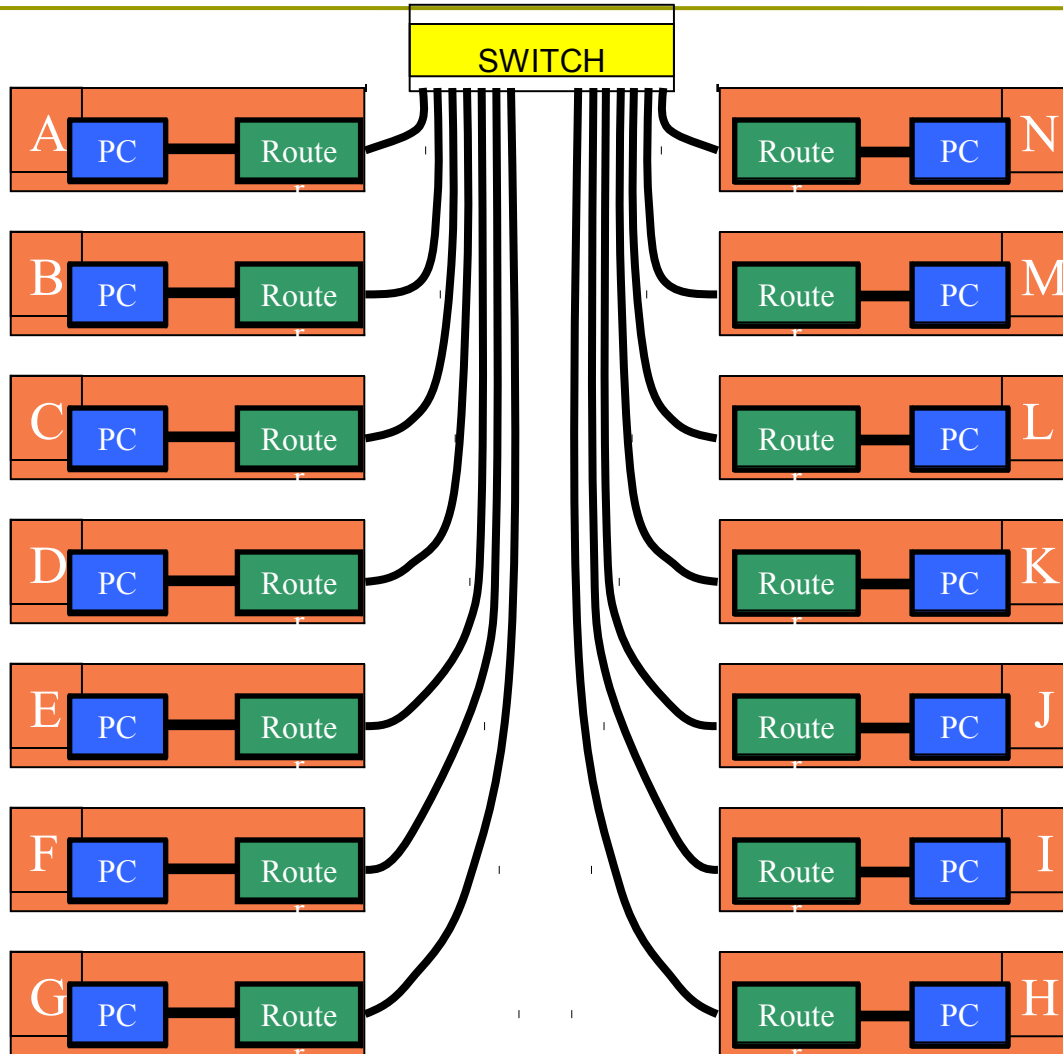
- Binary Representation:

10000101	00011011	10100010	01111101
----------	----------	----------	----------

- Hexadecimal Representation:

85	1B	A2	7D
----	----	----	----

Address Exercise



Address Exercise

- ❑ Construct an IP address for your router's connection to the backbone network.
- ❑ 196.200.220.x
- ❑ x = 1 for row A, 2 for row B, etc.
- ❑ Write it in decimal form as well as binary form.

Addressing in Internetworks

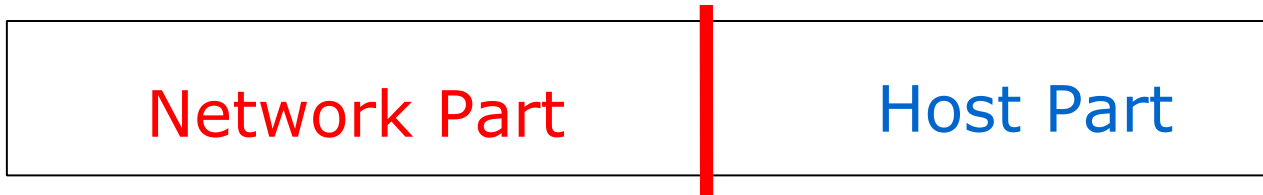
- The problem we have
 - More than one physical network
 - Different Locations
 - Larger number of hosts/computer systems
 - Need a way of numbering them all
- We use a structured numbering system
 - Hosts that are connected to the same physical network may have “similar” IP addresses

Network part and Host part

- Remember IPv4 address is 32 bits
- Divide it into a “network part” and “host part”
 - “network part” of the address identifies which network in the internetwork (e.g. the Internet)
 - “host part” identifies host on that network
 - Hosts or routers connected to the same link-layer network will have IP addresses with the same network part, but different host part.
 - Host part contains enough bits to address all hosts on that subnet; e.g. 8 bits allows 256 addresses

Dividing an address

- Hierarchical Division in IP Address:
 - Network Part (or Prefix) – high order bits (left)
 - describes which physical network
 - Host Part – low order bits (right)
 - describes which host on that network



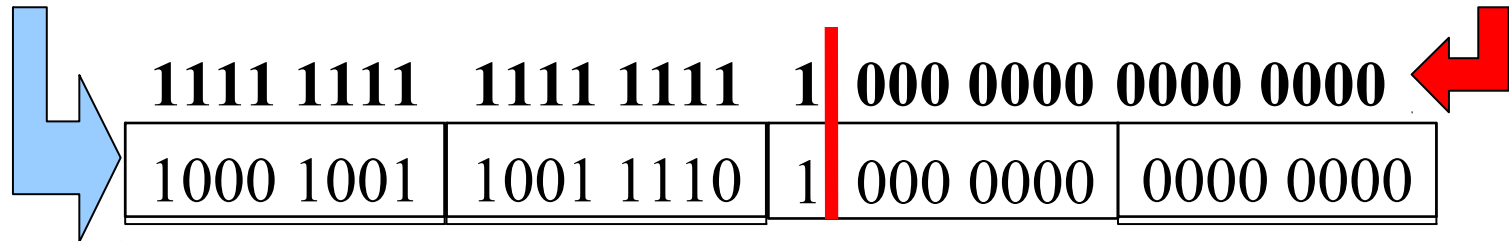
- Boundary can be anywhere
 - Boundaries are chosen according to number of hosts required

Network Masks

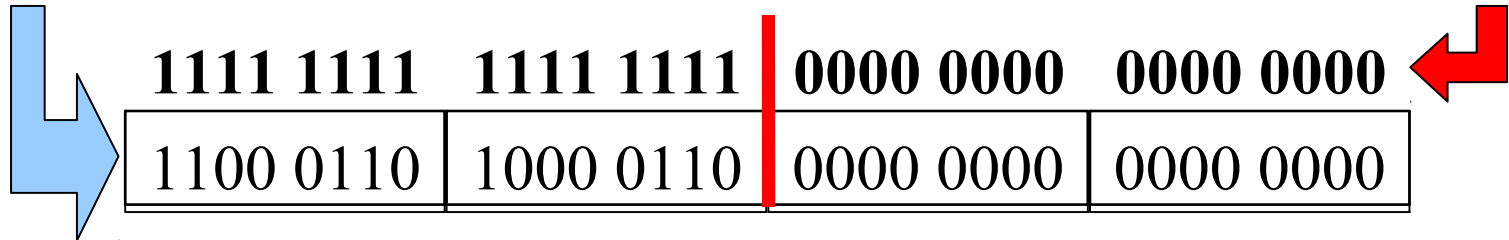
- “Network Masks” help define which bits describe the Network Part and which for the Host Part
- Different Representations:
 - decimal dot notation: 255.255.224.0
 - binary: 11111111 11111111 11100000 00000000
 - hexadecimal: 0xFFFFE000
 - number of network bits: /19
 - count the 1's in the binary representation
- Above examples all mean the same: 19 bits for the Network Part and 13 bits for the Host Part

Example Prefixes

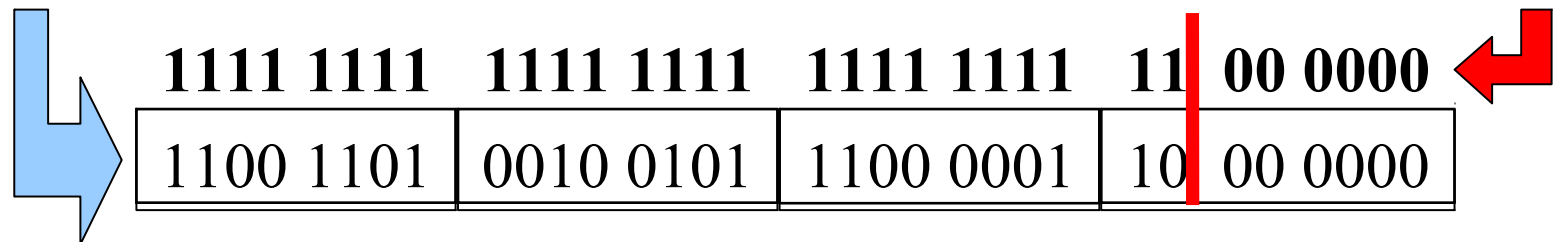
- 137.158.128.0/17 (netmask 255.255.128.0)



- 198.134.0.0/16 (netmask 255.255.0.0)



- 205.37.193.128/26 (netmask 255.255.255.192)



Special Addresses

- All 0's in host part: Represents Network
 - e.g. 193.0.5.0/24
 - e.g. 138.37.64.0/18
- All 1's in host part: Broadcast
 - e.g. 193.0.0.255 (prefix 193.0.0.0/24)
 - e.g. 138.37.127.255 (prefix 138.37.64.0/18)
- 127.0.0.0/8: Loopback address (127.0.0.1)
- 0.0.0.0: For various special purposes

Ancient History:

- A classful network naturally “implied” a prefix-length or netmask:
 - Class A: prefix length /8 (netmask 255.0.0.0)
 - Class B: prefix length /16 (netmask 255.255.0.0)
 - Class C: prefix length /24 (netmask 255.255.255.0)
- Modern (classless) routed networks rather have explicit prefix-lengths or netmasks.
 - So ideally you can't just look at an IP address and tell what its prefix-length or netmask should be.
 - Protocol configurations in this case also need explicit netmask or prefix length.

Post-1994 era of classless addressing

- ❑ Class A, Class B, Class C terminology and restrictions are now of historical interest only
 - Obsolete since 1994
- ❑ Internet routing and address management today is classless
- ❑ **CIDR = Classless Inter-Domain Routing**
 - Routing does not assume that former class A, B, C addresses imply prefix lengths of /8, /16, /24
- ❑ **VLSM = Variable-Length Subnet Masks**
 - Routing does not assume that all subnets are the same size

Classless addressing example

- An ISP gets a large block of addresses
 - e.g., a /16 prefix, or 65536 separate addresses
- Assign smaller blocks to customers
 - e.g., a /24 prefix (256 addresses) to one customer, and a /28 prefix (16 addresses) to another customer (and some space left over for other customers)
- An organisation that gets a /24 prefix from their ISP divides it into smaller blocks
 - e.g. a /27 prefix (32 addresses) for one department, and a /28 prefix (16 addresses) for another department (and some space left over for other internal networks)

Classless addressing exercise

- Consider the address block 133.27.162.0/24
- Allocate 5 separate /28 blocks, one /27 block, and one /30 block
- What are the IP addresses of each block allocated above?
 - In prefix length notation
 - Netmasks in decimal
 - IP address ranges
- What blocks are still available (not yet allocated)?
- How big is the largest available block?

Configuring interfaces – *ifconfig*

- `ifconfig interface [address_family] address [params]`
 - interface: network interface, e.g., eth0 or bge0
 - options: up, down, netmask mask
 - address: IP address

- Examples:
 - `ifconfig bge0 inet 192.168.2.2; ifconfig bge1 192.168.3.1`
 - `ifconfig eth0 inet 172.16.1.1/24`
 - `ifconfig bge0 192.168.2.2 netmask 255.255.255.0`
 - `ifconfig bge0 inet6 2001:db8:bdbd::123 prefixlen 48 alias`

IPv6 Addressing



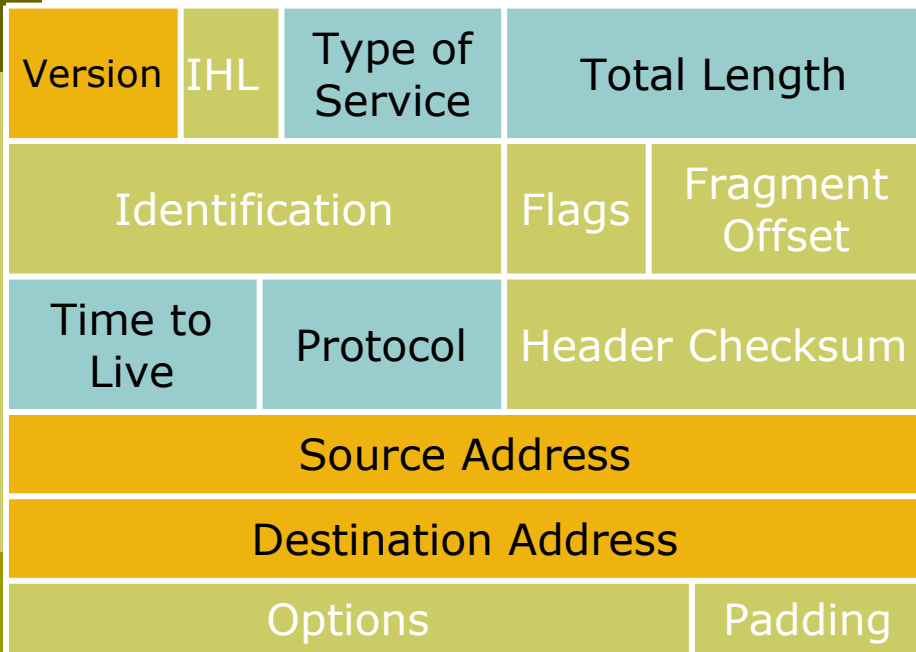
IP Addresses Continues

IP version 6

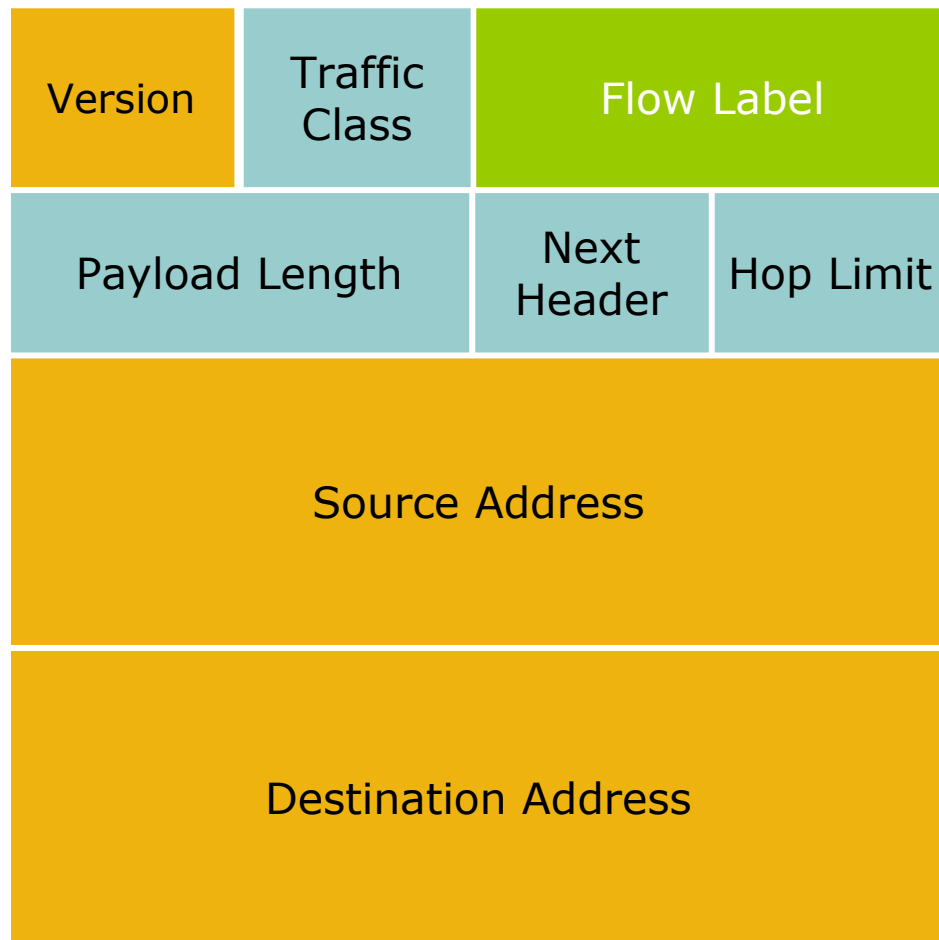
- IPv6 designed as successor to IPv4
 - Expanded address space
 - Address **length** quadrupled to 16 bytes (128 bits)
 - Header Format Simplification
 - Fixed length, optional headers are daisy-chained
 - No checksum at the IP network layer
 - No hop-by-hop fragmentation
 - Path MTU discovery
 - 64 bits aligned fields in the header
 - Authentication and Privacy Capabilities
 - IPsec is mandated
 - No more broadcast

IPv4 and IPv6 Header Comparison

IPv4 Header



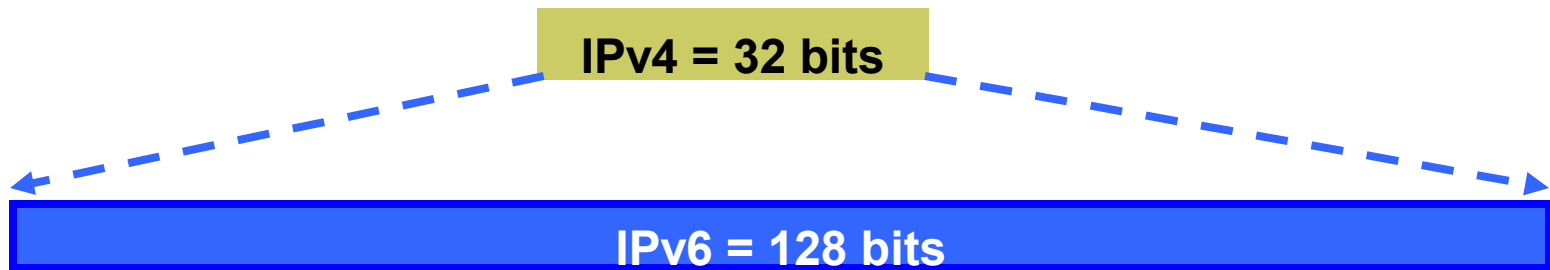
IPv6 Header



Legend


- Field's name kept from IPv4 to IPv6
- Fields not kept in IPv6
- Name and position changed in IPv6
- New field in IPv6

Larger Address Space



- IPv4
 - 32 bits
 - = 4,294,967,296 possible addressable devices
- IPv6
 - 128 bits: 4 times the size in bits
 - = 3.4×10^{38} possible addressable devices
 - = 340,282,366,920,938,463,463,374,607,431,768,211,456
 - $\sim 5 \times 10^{28}$ addresses per person on the planet

IPv6 Address Representation

- 16 bit fields in case insensitive colon hexadecimal representation
 - 2031:0000:130F:0000:0000:09C0:876A:130B
- Leading zeros in a field are optional:
 - 2031:0:130F:0:0:9C0:876A:130B
- Successive fields of 0 represented as ::, but only once in an address:
 - 2031:0:130F::9C0:876A:130B ← is ok
 - 2031::130F::9C0:876A:130B is NOT ok (two "::")
- 0:0:0:0:0:0:0:1 → ::1 (loopback address)
- 0:0:0:0:0:0:0:0 → :: (unspecified address)

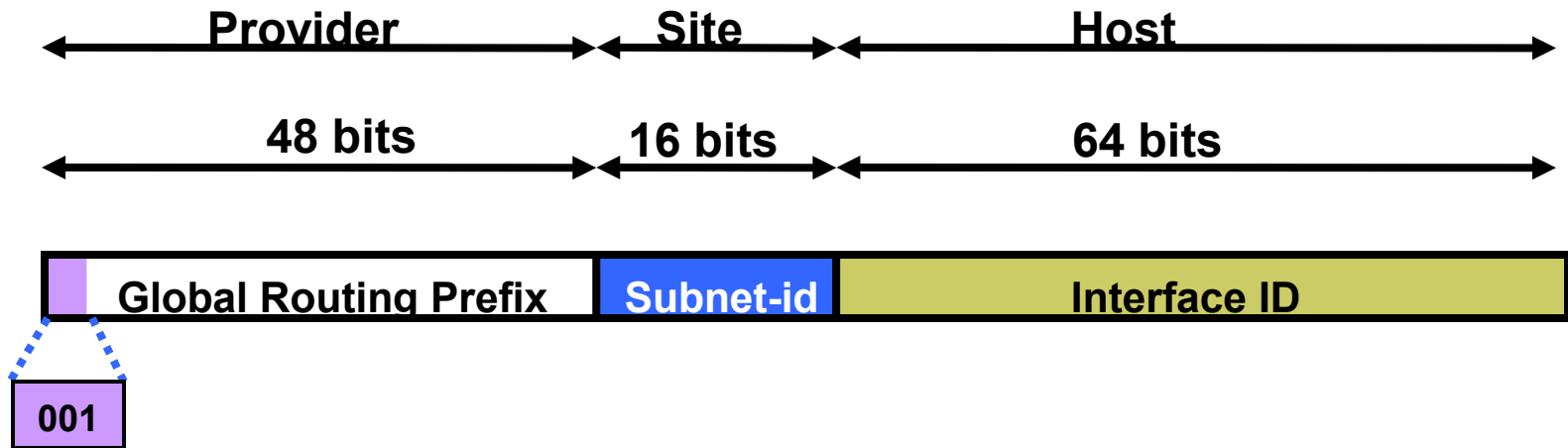
IPv6 Address Representation

- In a URL, it is enclosed in brackets (RFC3986)
 - [http://\[2001:db8:4f3a::206:ae14\]:8080/index.html](http://[2001:db8:4f3a::206:ae14]:8080/index.html)
 - Complicated for typical users
 - This is done mostly for diagnostic purposes
 - Use fully qualified domain names (FQDN) instead of this
- Prefix Representation
 - Representation of prefix is same as for IPv4 CIDR
 - Address and then prefix length, with slash separator
 - IPv4 address:
 - 198.10.0.0/16
 - IPv6 address:
 - 2001:db8:1200::/40

IPv6 Addressing

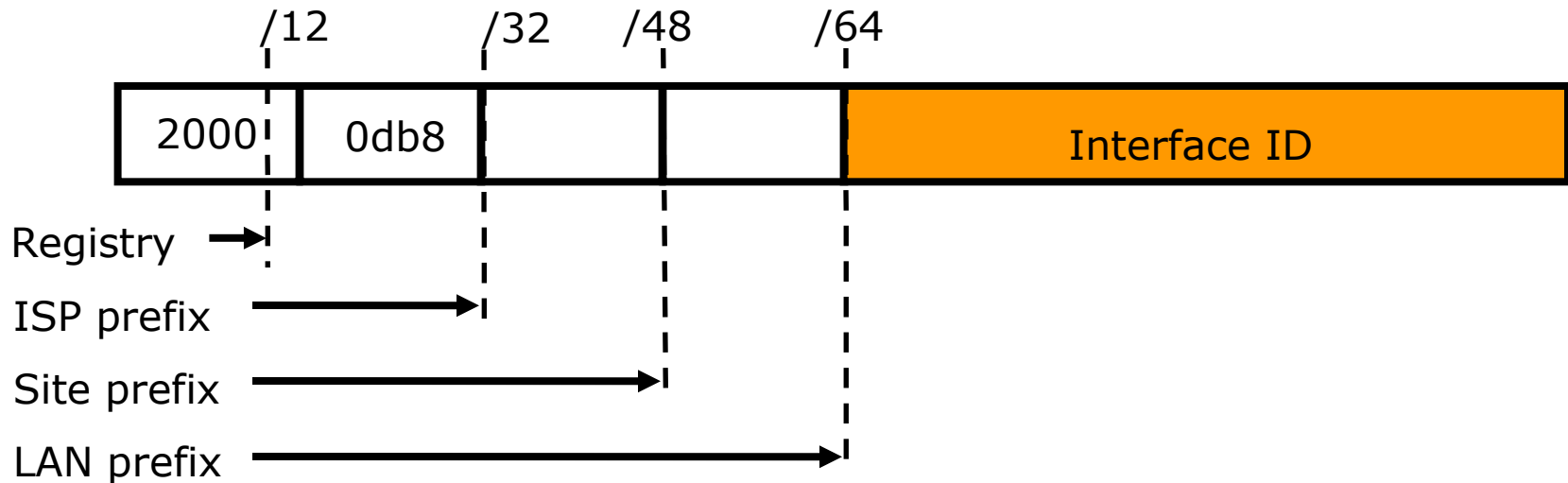
Type	Binary	Hex
Unspecified	0000...0000	::/128
Loopback	0000...0001	::1/128
Global Unicast Address	001.	2000::/3
Link Local Unicast Address	1111 1110 10...	FE80::/10
Unique Local Unicast Address	1111 1100 ... 1111 1101 ...	FC00::/7
Multicast Address	1111 1111 ...	FF00::/8

IPv6 Global Unicast Addresses



- IPv6 Global Unicast addresses are:
 - Addresses for generic use of IPv6
 - Hierarchical structure intended to simplify aggregation

IPv6 Address Allocation



□ The allocation process is:

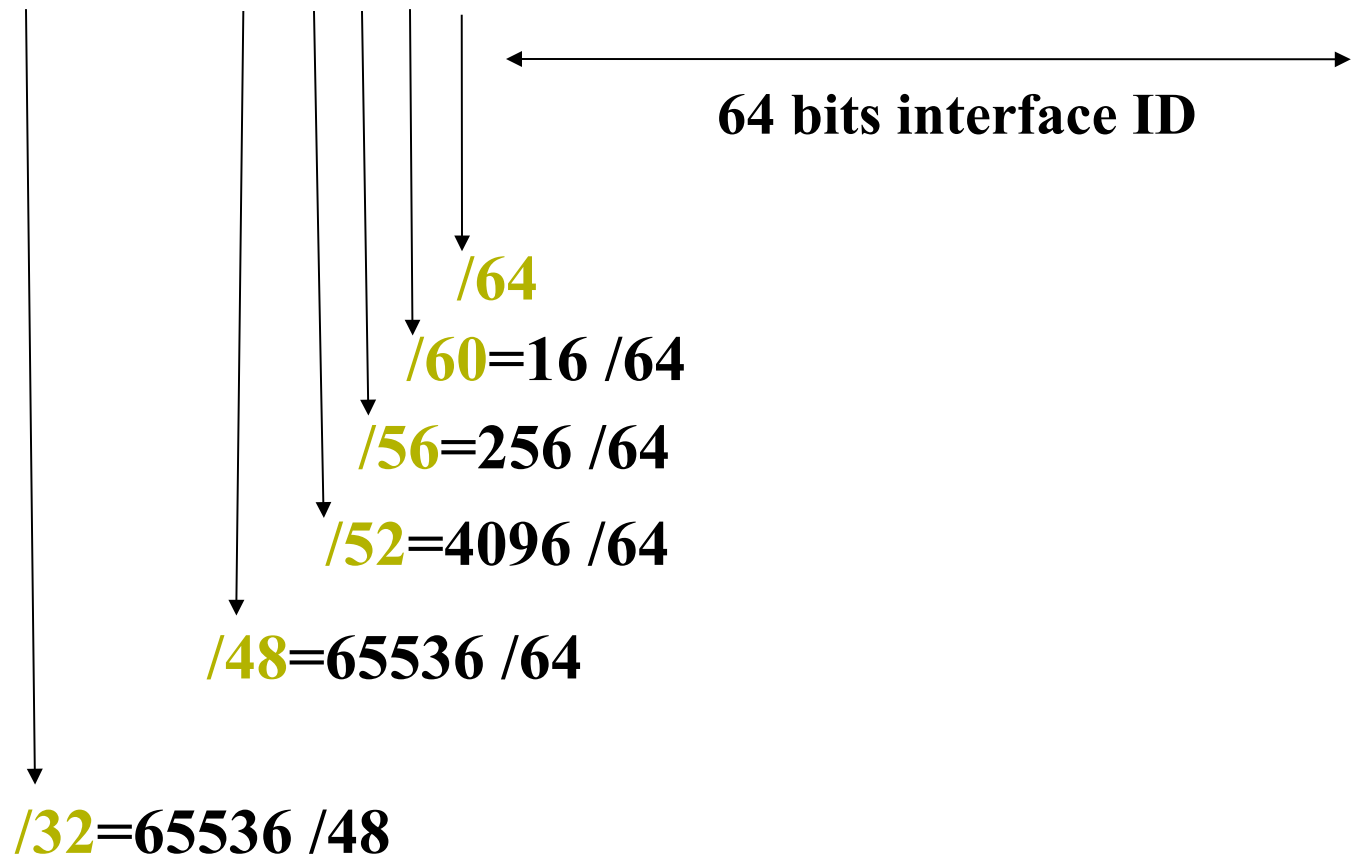
- The IANA is allocating out of 2000:::/3 for initial IPv6 unicast use
- Each registry gets a /12 prefix from the IANA
- Registry allocates a /32 prefix (or larger) to an IPv6 ISP
- ISPs usually allocate a /48 prefix to each end customer

IPv6 Addressing Scope

- 64 bits used for the interface ID
 - Possibility of 2^{64} hosts on one network LAN
 - Arrangement to accommodate MAC addresses within the IPv6 address
- 16 bits used for the end site
 - Possibility of 2^{16} networks at each end-site
 - 65536 subnets

IPV6 Subnetting

2001:0db8:0000:0000:0000:0000:0000:0000



Nibble (4 bits) Concept

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	a
11	1011	b
12	1100	c
13	1101	d
14	1110	e
15	1111	f

Summary

- Vast address space
- Hexadecimal addressing
- Distinct addressing hierarchy between ISPs, end-sites, and LANs
 - ISPs are typically allocated /32s or bigger
 - End customers are typically assigned /48s
 - LANs have /64s
- Other IPv6 features discussed later



The need for Packet Forwarding

- ❑ Many small networks can be interconnected to make a larger internetwork
- ❑ A device on one network cannot send a packet directly to a device on another network
- ❑ The packet has to be forwarded from one network to another, through intermediate nodes, until it reaches its destination
- ❑ The intermediate nodes are called “routers”

An IP Router

- ❑ A device with more than one link-layer interface (breaks broadcast domains)
- ❑ Different IP addresses (from different subnets) on different interfaces
- ❑ Receives packets on one interface, and forwards them (usually out of another interface) to get them one hop closer to their destination
- ❑ Maintains forwarding tables and routing information base

IP router - action for each packet

- ❑ Packet is received on one interface (ingress)
- ❑ Checks whether the destination address is the router itself – if so, pass it to higher TCP/IP stack layers
- ❑ Decrement TTL (time to live) and discard packet if it reaches zero (0). TTL value is a single octet and maximum is 255.
- ❑ Look up the destination IP address in the forwarding table.
- ❑ Destination could be on a directly attached link, or through another directly connected or remote router.

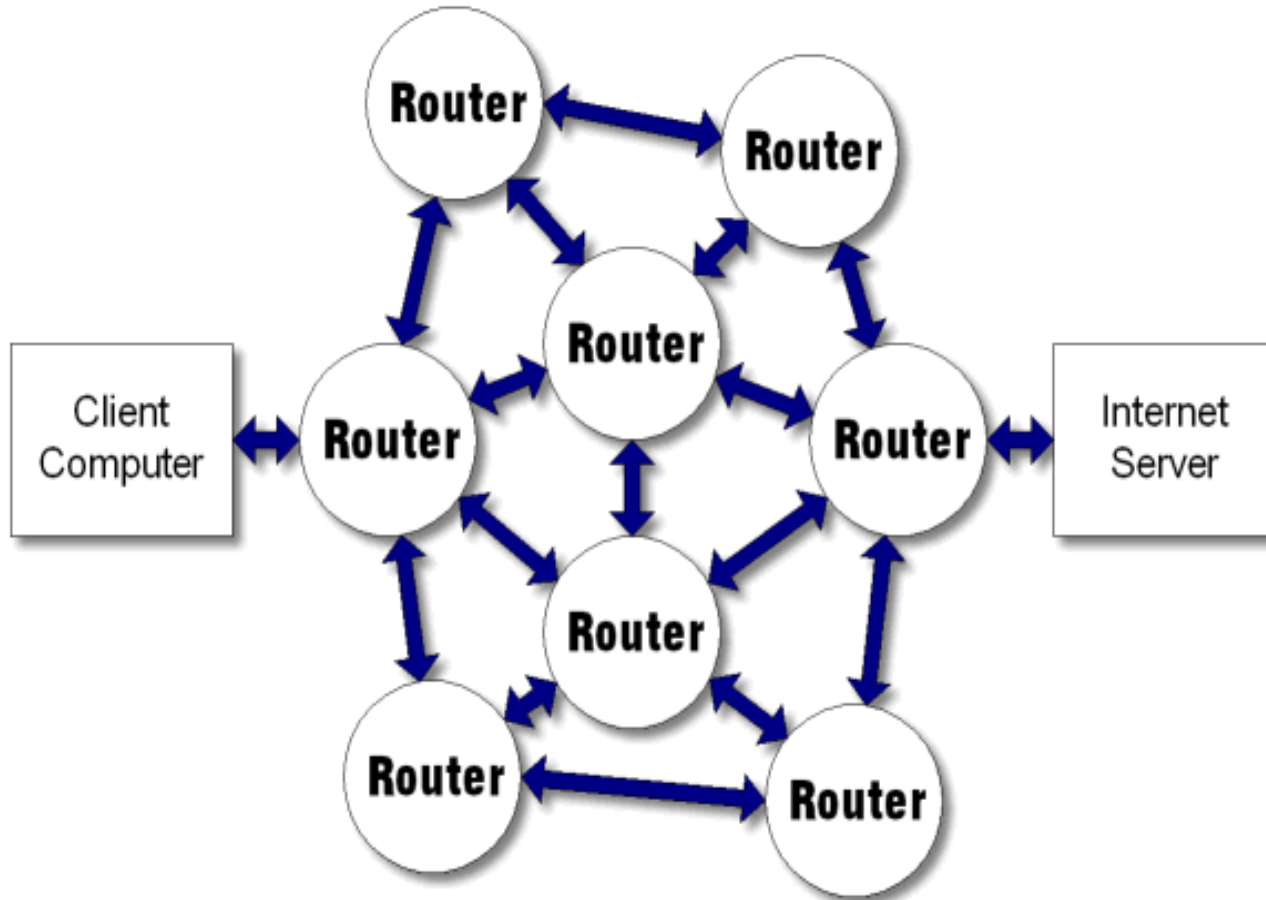
Forwarding vs. Routing

- Forwarding: moving packets between ingress and egress interfaces
 - Depends on the forwarding table
 - Information is in the packet
- Routing: process of building routing maps and giving directions
 - One or more routing protocols
 - Procedures (algorithms) to convert routing info to forwarding table.
- (Much more later ...)

Forwarding is hop by hop

- ❑ Each router makes an independent decision, based on its own forwarding table
- ❑ Different routers have different forwarding tables and make different decisions
- ❑ Routers talk routing protocols to each other, to help update routing information and forwarding tables

Hop by Hop Forwarding



Router Functions

- Determine optimum routing paths through a network
 - Lowest delay means shortest path
 - Highest reliability
- Move packets through the network
 - Determine and determine destination address in packet
 - Makes a decision on which port to forward the packet through
 - Decision is based on the Routing Table
- Interconnected Routers exchange routing tables in order to maintain a clear picture/map of the network
- In a large network, the routing table updates can consume a lot of resource (cpu, memory, bandwidth)
 - a protocol for route updates is required

Forwarding table structure

- ❑ Not every IP address on the Internet is listed otherwise the routing/forwarding table would be huge.
- ❑ Instead, the forwarding table contains ip prefixes (networks or subnetwork)
 - "If the first /n bits in the routing table matches this entry, send the datagram that way"
 - If more than one prefix matches, the longest prefix wins (more specific routes)
- ❑ 0.0.0.0/0 is "default route" - matches anything, but only if no other prefix matches.

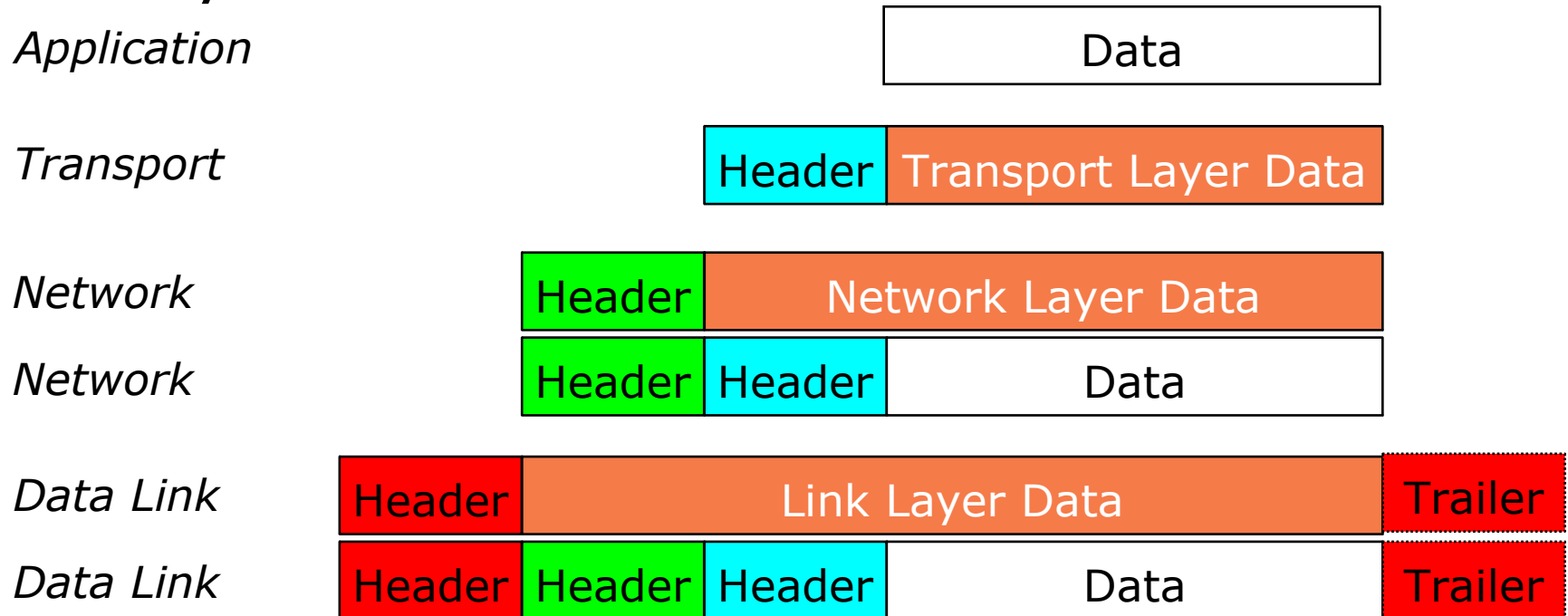
ARP



Continuation

Encapsulation Reminder

- Lower layers add headers (and sometimes trailers) to data from higher layers



Ethernet Essentials

- ❑ Ethernet is a broadcast medium
- ❑ Structure of Ethernet frame:

Preamble	Dest	Source	Length	Type	Data	CRC
----------	------	--------	--------	------	------	-----

- ❑ Entire IP packet makes data part of Ethernet frame
- ❑ Delivery mechanism (CSMA/CD)
 - back off and try again when collision is detected

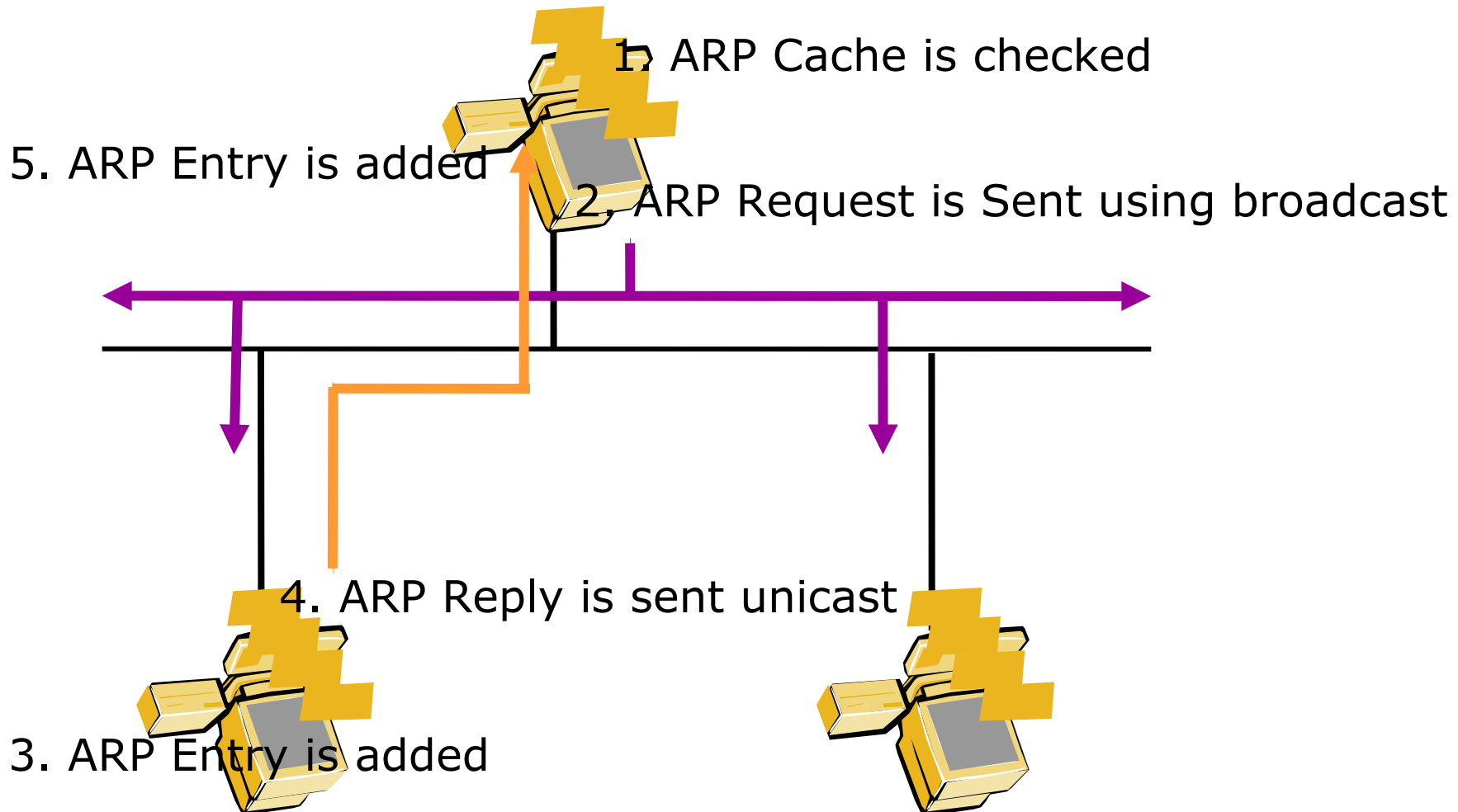
Ethernet/IP Address Resolution

- Internet Address
 - Unique worldwide (excepting private nets)
 - Independent of Physical Network technology
- Ethernet Address
 - Unique worldwide (excepting errors)
 - Ethernet Only
- Need to map from higher layer to lower (i.e. IP to Ethernet, using ARP)

Address Resolution Protocol

- ARP is only used in IPv4
 - ND (Neighbor Discovery) replaces ARP in IPv6
- Check ARP cache for matching IP address
- If not found, broadcast packet with IP address to every host on Ethernet
- “Owner” of the IP address responds
- Response cached in ARP table for future use
- Old cache entries removed by timeout

ARP Procedure



ARP Table

IP address	Interface	Hardware address	Age (secs)
192.168.0.2	Gi0/1	08-00-20-08-70-54	3
192.168.0.65	Gi0/1	05-02-20-08-88-33	120
192.168.1.34	Gi0/2	07-01-20-08-73-22	43

Types of ARP Messages

□ ARP request

- Who is IP addr X.X.X.X tell IP addr Y.Y.Y.Y

□ ARP reply

- IP addr X.X.X.X is Ethernet Address
hh:hh:hh:hh:hh:hh
- An ARP announcement is not intended to solicit a reply; instead it updates any cached entries in the ARP tables of other hosts that receive the packet.

Thank you

Any questions?