Internet Protocol (IP)

ELEC-C7420 Basic Principles in Networking

Aalto University
School of Electrical
Engineering

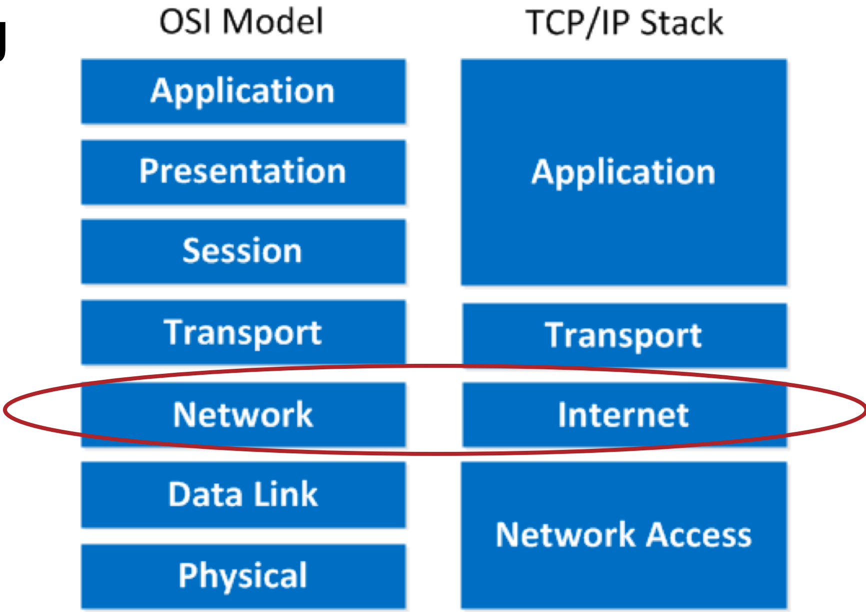
Yu Xiao

25.01.2022

Learning Outcomes

After this lecture, you should be able to

- **Understand IP addressing and subnetting**
- **Describe the process of IP Routing**



End-to-end delivery using addresses

What is an IP address?

IP Addresses

- An IP address identifies a host or network interface on a network, and provides the location of the host in the network

- Each device that wants to communicate with other devices on a TCP/IP network needs to have an IP address configured

%ifconfig

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 98:01:a7:90:7d:db
        inet6 fe80::9a01:a7ff:fe90:7ddb%en0 prefixlen 64 scopeid 0x4
        inet 130.233.101.149 netmask 0xfffffe00 broadcast 130.233.101.255
        nd6 options=1<PERFORMNUD>
        media: autoselect
        status: active

en7: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=4<VLAN_MTU>
        ether 00:1f:5b:fe:c0:2f
        inet6 fe80::21f:5bff:fefe:c02f%en7 prefixlen 64 optimistic scopeid 0xb
        nd6 options=1<PERFORMNUD>
        media: autoselect (100baseTX <full-duplex,flow-control>)
        status: active
```

In contrast to MAC address, an IP address is a logical address. It can be configured manually or obtained from a DHCP (Dynamic Host Configuration Protocol) server

DHCP is an application layer protocol. It dynamically assigns an IP address and other network configuration parameters to each device on a network so they can comm. with other IP networks.

IPv4 Addresses

- **An IPv4 address consists of 4 octets (32 bits)**

[octet] . [octet] . [octet] . [octet]

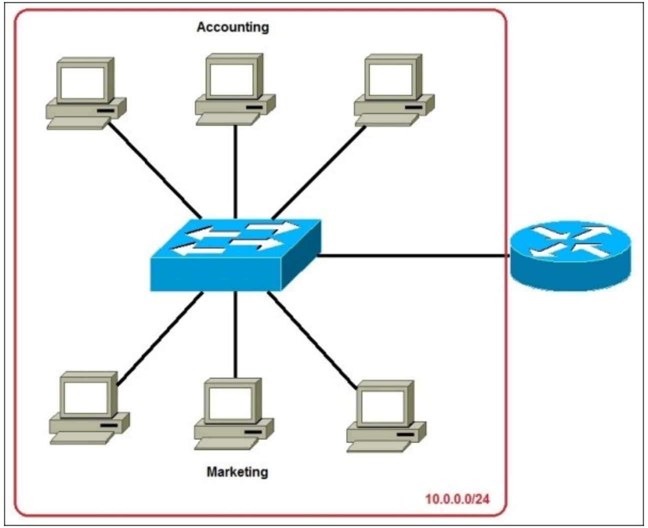
1000 1000.1110 0011.1110 1101.0110 1000 → 136.227.237.104

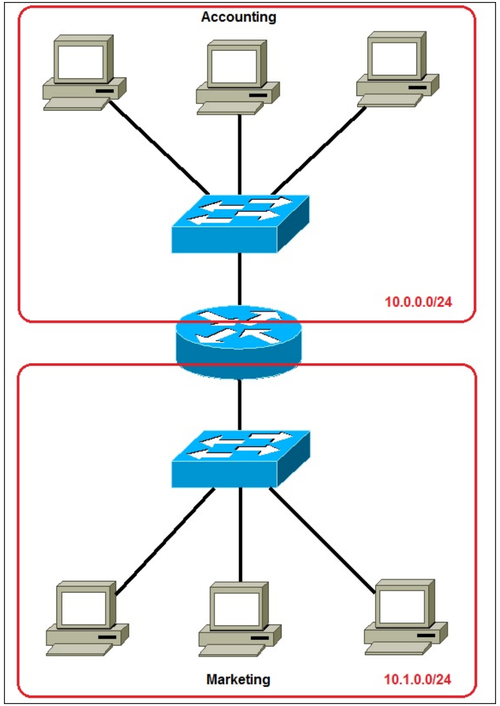
- Each number can be 0 to 255

#IPv4 addresses in the world?

Subnetting

- **Subnetting**: dividing a network into two or more smaller networks.





Aalto University
School of Electrical
Engineering

Source: https://study-ccna.com/subnetting-explained/

- **Purposes of subnetting**
  - Reducing the size of the broadcast domain
  - Increasing routing efficiency
  - Enhancing the security of the network

IPv4 Subnet Mask

- An IP address is divided into two parts: network and host parts.
- Subnet mask is used for determining the network part and the host part of an IP address.
- **A subnet mask consists of 32 bits. The 1s in the subnet mask represent a network part, the 0s a host part.**
- A subnet mask must always be a series of 1s followed by a series of 0s. E.g. 255.255.0.0, 255.0.0.0.

Given an IP address 10.0.0.1 and subnet mask 255.0.0.0, how to calculate the network number and the range of addresses in the network?

1) Convert the IP address to binary
2) Use AND operation to calculate the network number

```
00001010.00000000.00000000.00000001 = 10.0.0.1
11111111.00000000.00000000.00000000 = 255.0.0.0
-----------------------------------------------
00001010.00000000.00000000.00000000 = 10.0.0.0
```

The range of addresses in this network is 10.0.0.0 – 10.255.255.255

Special Addresses

- **IPv4 loopback address: 127.0.0.1**

The loopback interface has no hardware associated with it, and it is not physically connected to a network.

```
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet6 ::1 prefixlen 128
        inet 127.0.0.1 netmask 0xff000000
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=1<PERFORMNUD>
```

- **Broadcast addresses**
  - The broadcast address for a network has all host bits on.
  - For example, for the network 192.168.30.0 255.255.255.0, what would be the broadcast address?
  - What can 255.255.255.255 be used for?

Classes of IP addresses

- The value of the first octet determines the class.
- IP addresses from Class A, B and C can be used for host addresses.
- Class D for multicast and Class E for experimental purposes

Class	First octet value	Subnet mask	No. addresses per network
A	0 - 127	8	16 777 216 (2^{24})
B	128 - 191	16	65536 (2^{16})
C	192 - 223	24	256(2^{8})
D	224 - 239	-	-
E	240 - 255	-	-

Classless Inter-Domain Routing (CIDR)

- Introduced in 1993 by IETF (Internet Engineering Task Force)
- CIDR is based on **variable-length subnet masking (VLSM)** to allow allocation and routing based on arbitrary-length prefixes

Prefix

192.0.1.0/24 prefix length is 24.

32-24=8 bits are left for host addresses

10.0.0.0/8 32-8=24bits are left for host addresses

Exercise

IP address: 136.227.237.104/27

What is the subnet mask?

255.255.255.224

- **The number of usable IP addresses** can be calculated from the following formula:

2 to the power of host bits – 2

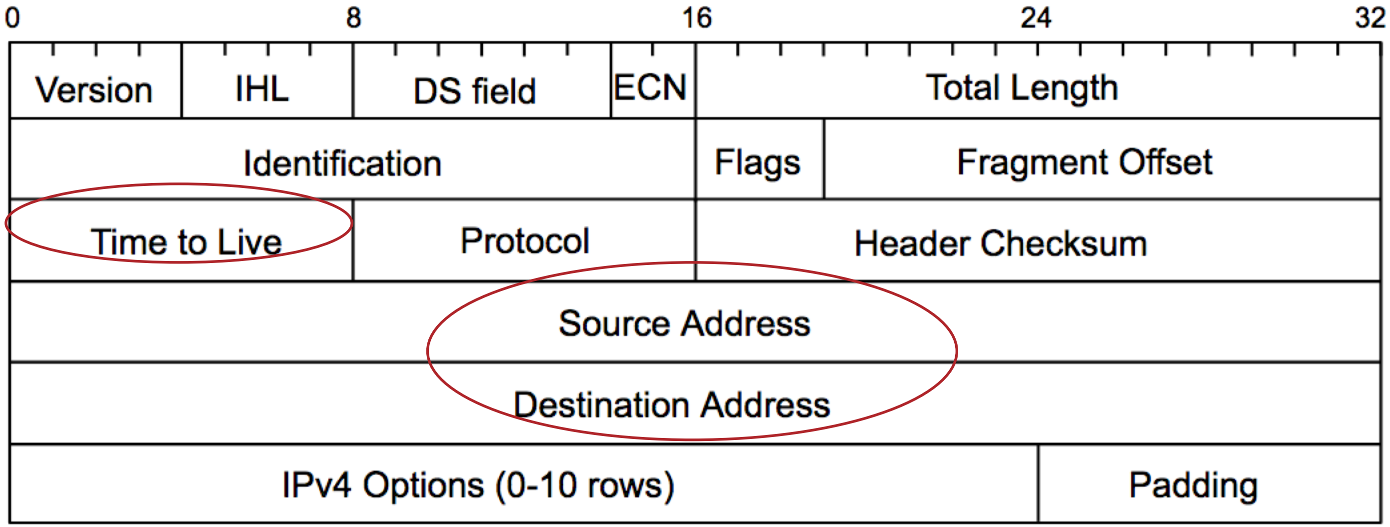
The first and the last address are the network address and the broadcast address, respectively. All other addresses inside the range could be assigned to Internet hosts.

If a company needs 12 public IP address, something like 190.5.1.1/k, what should be the value of k?

Private Addresses

- **Private addresses are IPv4 addresses intended only for site internal use**
- **Reserved private IPv4 network ranges**
    - 10.0.0.0/8
    - 172.16.0.0/12
    - 192.168.0.0/16

IPv4 Header



- **Time-to-Live (TTL):** decremented by 1 at each router; if it reaches 0, packet is discarded.

IPv4 Header

- **Time-to-Live (TTL):** decremented by 1 at each router; if it reaches 0, packet is discarded.
- **Protocol:** identifies the content of the packet body
  - 1: an ICMP packet
  - 4: an encapsulated IPv4 packet
  - 6: a TCP packet
  - 17: a UDP packet
  - 41: an encapsulated IPv6 packet
  - 50: an encapsulating security payload

IPv6 addresses

- **IPv6 address consists of 16 octets (128 bits). IPv6 separates pairs of octets with a colon.**

[octet] [octet] : [octet] [octet] :::::: [octet] [octet]

For example, fedc:13:1654:310:fedc:bc37:61:3210

- If an address contains a long run of 0's, "::" should be used to represent many blocks of 0000
- It is possible to embed an IPv4 address in IPv6 address

For example, ::ffff:147.126.65.141

First 80 0-bits

Scope of IPv6 addresses

- The scope of a unicast address is either **global**, meaning it is intended to be globally routable, or **link-local**, meaning that it will only work with directly connected neighbors
- E.g. the loopback address ::1 **(127 0-bits followed by 1 1-bit)** is considered to have link-local scope
- **Link-local** addresses begin with the 64-bit link-local prefix consisting of the ten bits 1111 1110 10 followed by 54 more zero bits; that is, **fe80::/64**.

Predefined and Reserved Scopes

Scope values

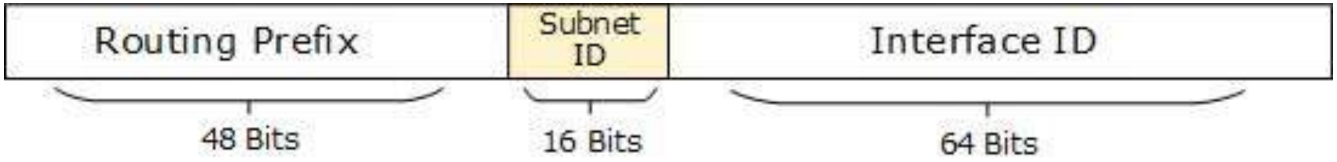
Value	Scope name	Notes
0x0	*reserved*	
0x1	interface-local	Interface-local scope spans only a single interface on a node, and is useful only for loopback transmission of multicast.
0x2	link-local	Link-local scope spans the same topological region as the corresponding unicast scope.
0x3	realm-local	Realm-local scope is defined as larger than link-local, automatically determined by network topology and must not be larger than the following scopes.[13]
0x4	admin-local	Admin-local scope is the smallest scope that must be administratively configured, i.e., not automatically derived from physical connectivity or other, non-multicast-related configuration.
0x5	site-local	Site-local scope is intended to span a single site belonging to an organisation.
0x8	organization-local	Organization-local scope is intended to span all sites belonging to a single organization.
0xe	global	Global scope spans all reachable nodes on the internet - it is unbounded.
0xf	*reserved*	

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 98:01:a7:90:7d:db
        inet6 fe80::9a01:a7ff:fe90:7ddb%en0 prefixlen 64 scopeid 0x4
        inet 192.168.0.154 netmask 0xffffff00 broadcast 192.168.0.255
        nd6 options=1<PERFORMNUD>
        media: autoselect
        status: active
```


Source: wikipedia

IPv6 Interface Identifier

- Most IPv6 addresses can be divided into a **64-bit network prefix** and a 64-bit “host” portion. These host-portion bits are known officially as the **interface identifier.**

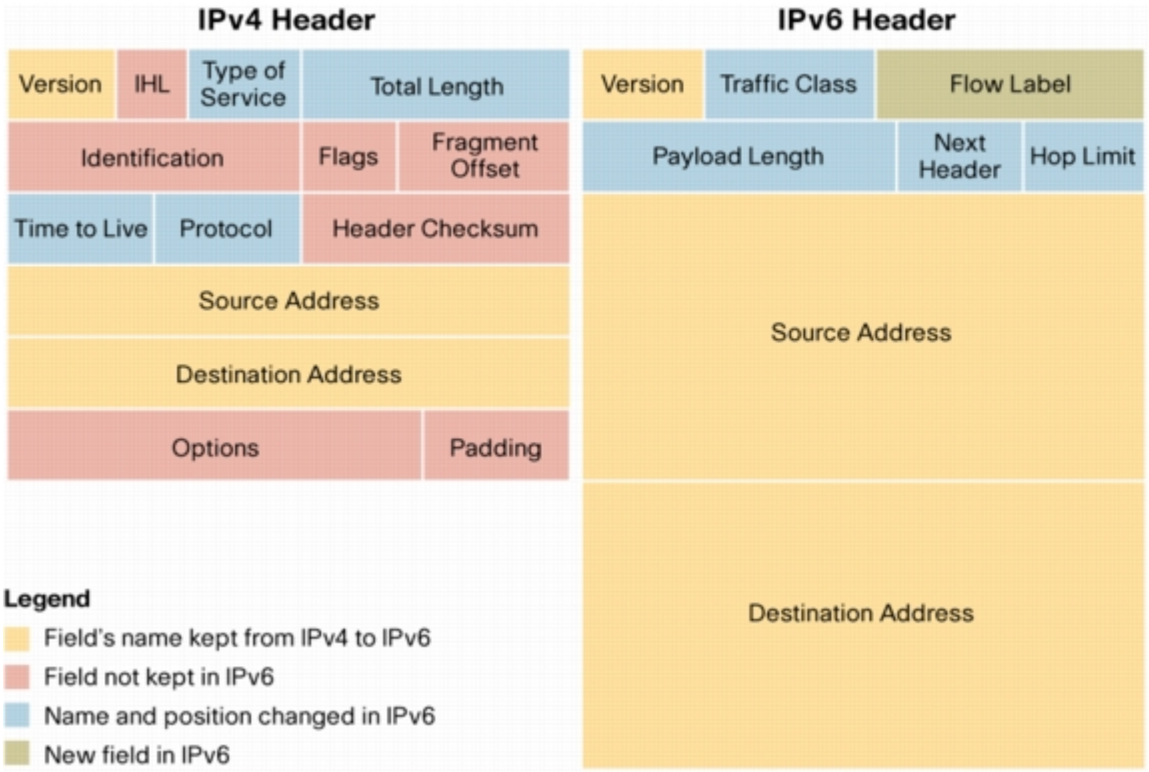


AnyCast

IPv6 has introduced Anycast mode of packet routing. In this mode, multiple interfaces over the Internet are assigned same Anycast IP address. Routers, while routing, send the packet to the nearest destination.

IPv6 does not support broadcast

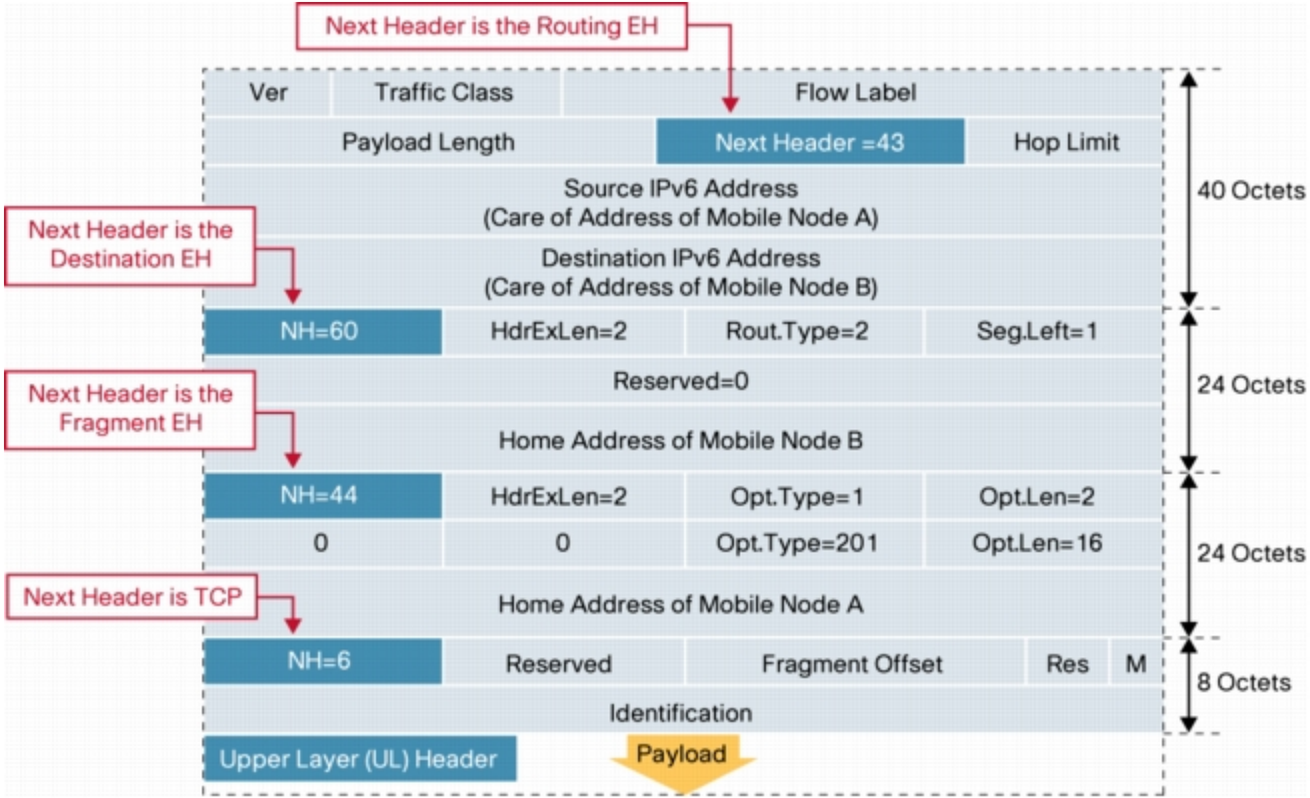
IPv4 vs. IPv6 Header



In IPv6, the main header remains fixed in size (40 bytes) while customized extension headers are added as needed.

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

IPv6 Packet with Extension Headers



What is IP Routing?

IP routing is the process of sending packets from a host on one network to another host on a different remote network. This process is usually done by **routers**.

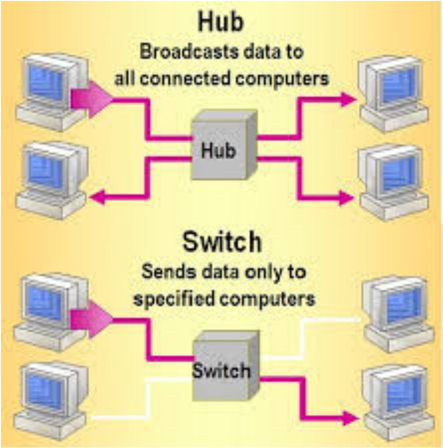
Hubs vs. Switches

Hubs

- Every station that is attached can see the traffic sent between all the other computers
- Use CSMA/CD to schedule transmission

Switches

- Traffic is forwarded only to the ports where it is destined.
- Multiple frames can be sent simultaneously by different stations



Source: hinditechy.com

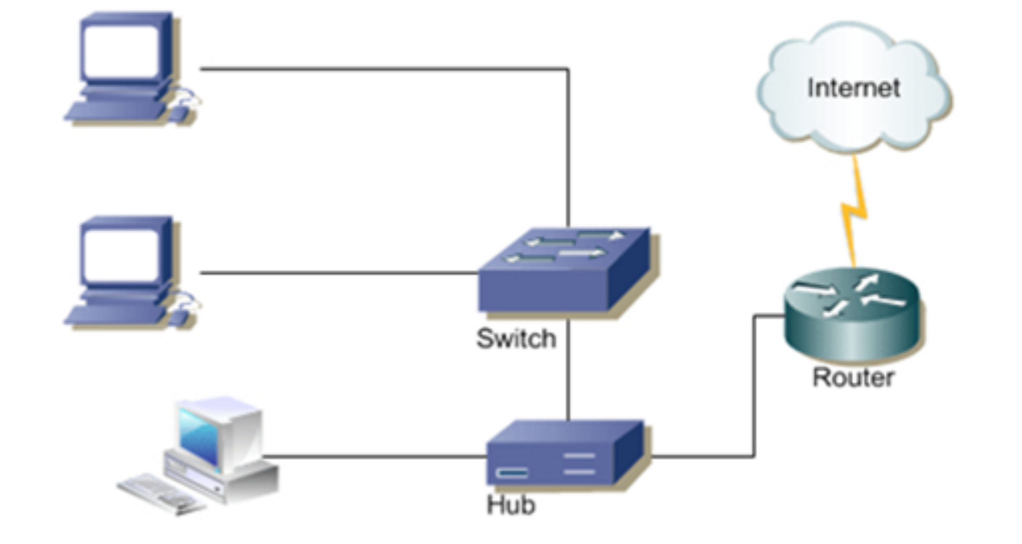
5 Ports

Aalto University
School of Electrical
Engineering

Router vs. Switch

A router connects different networks like two LANs, two WAN's or LAN and WAN.

The main purpose of the router is to determine the smallest and best path for a packet to reach the destination.



Source: http://www.fiberopticshare.com/

IP Routing

- **Routers examine the destination IP address of a packet , determine the next-hop address, and forward the packet.**
- Routers use routing tables to determine a next hop address to which the packet should be forwarded.

%traceroute www.google.com

```
traceroute to www.google.com (216.58.211.4), 64 hops max, 52 byte packets
 1  192.168.0.1 (192.168.0.1)  2.432 ms  2.260 ms  2.153 ms
 2  10.15.10.1 (10.15.10.1)  2.636 ms  3.159 ms  2.944 ms
 3  172.25.93.169 (172.25.93.169)  4.035 ms  3.821 ms  4.186 ms
 4  193.229.29.205 (193.229.29.205)  5.917 ms  4.645 ms  3.966 ms
 5  213.192.186.77 (213.192.186.77)  4.081 ms  3.849 ms  4.971 ms
 6  213.192.184.74 (213.192.184.74)  10.161 ms  9.918 ms  9.752 ms
 7  213.192.185.93 (213.192.185.93)  10.180 ms  9.620 ms  10.216 ms
 8  108.170.253.161 (108.170.253.161)  10.817 ms  11.786 ms
    108.170.253.177 (108.170.253.177)  11.988 ms
 9  209.85.241.225 (209.85.241.225)  11.249 ms  10.444 ms  11.538 ms
10  arn09s20-in-f4.1e100.net (216.58.211.4)  10.170 ms  10.850 ms  10.021 ms
```

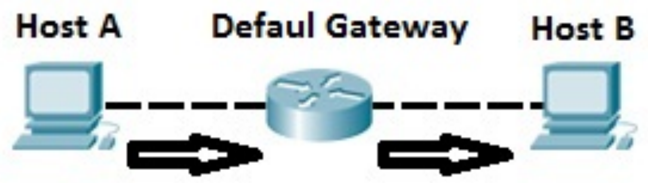
Routing Table

- Each router maintains a routing table and stores it in RAM.
- Each routing table consists of the following entries:
  - **network destination and subnet mask** – specifies a range of IP addresses.
  - **remote router** – IP address of the router used to reach that network.
  - **outgoing interface** – outgoing interface the packet should go out to reach the destination network.

All nodes on the internet have these routing tables, and this is how IP packets are routed to reach their destination.

Default Gateway

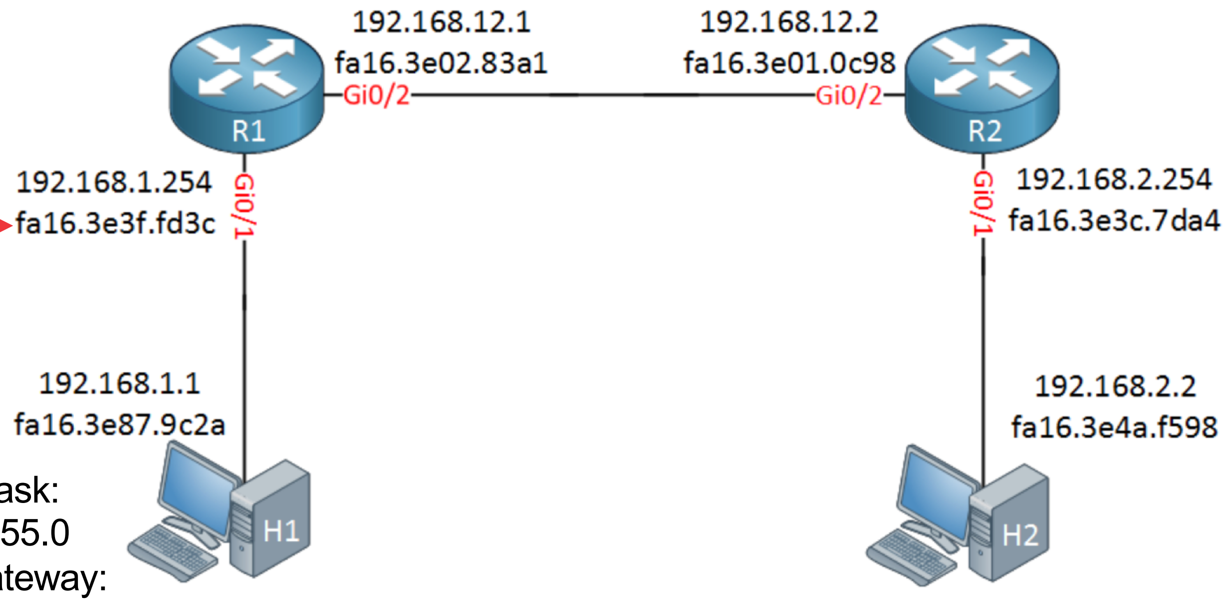
- A default gateway is used when a host doesn't have a route entry for the specific remote network and doesn't know how to reach that network.
- **Hosts can be configured to send all packets destined to remote networks to a default gateway**, which has a route to reach that network.



%netstat –rn

```
Routing tables

Internet:
Destination        Gateway            Flags        Refs      Use   Netif Expire
default            192.168.0.1        UGSc          243        0     en0
127                127.0.0.1          UCS             1        0     lo0
127.0.0.1          127.0.0.1          UH             53 38517336     lo0
169.254            link#4             UCS             1        0     en0
192.168.0          link#4             UCS             2        0     en0
192.168.0.1/32     link#4             UCS             2        0     en0
192.168.0.1        40:b0:76:2b:b5:10  UHLWIir       244       47     en0   1171
192.168.0.154/32   link#4             UCS             2        0     en0
192.168.0.154      98:1:a7:90:7d:db   UHLWIi          5      114     lo0
192.168.0.255      link#4             UHLWbI          1       33     en0
224.0.0            link#4             UmCS            2        0     en0
224.0.0.251        1:0:5e:0:0:fb      UHmLWI          1        0     en0
255.255.255.255/32 link#4             UCS             1        0     en0

Internet6:
Destination                             Gateway                         Flags         Netif Expire
::1                                     ::1                             UHL             lo0
fe80::%lo0/64                           fe80::1%lo0                     UcI             lo0
fe80::1%lo0                             link#1                          UHLI            lo0
fe80::%en0/64                           link#4                          UCI             en0
fe80::9a01:a7ff:fe90:7ddb%en0           98:1:a7:90:7d:db                UHLI            lo0
fe80::%awdl0/64                         link#9                          UCI           awdl0
fe80::58ea:cfff:fe72:4d29%awdl0         5a:ea:cf:72:4d:29               UHLI            lo0
ff01::%lo0/32                           ::1                             UmCI            lo0
ff01::%en0/32                           link#4                          UmCI            en0
ff01::%awdl0/32                         link#9                          UmCI          awdl0
ff02::%lo0/32                           ::1                             UmCI            lo0
ff02::%en0/32                           link#4                          UmCI            en0
ff02::%awdl0/32                         link#9                          UmCI          awdl0
```

Example

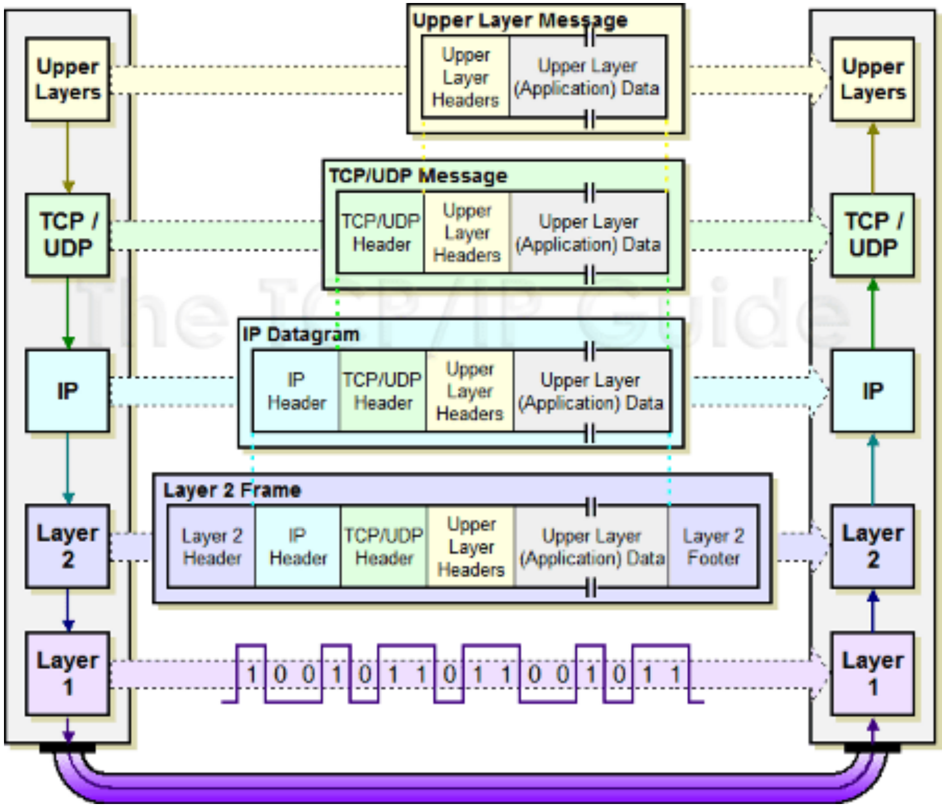


MAC address

Subnet mask:
255.255.255.0
Default gateway:
192.168.1.254

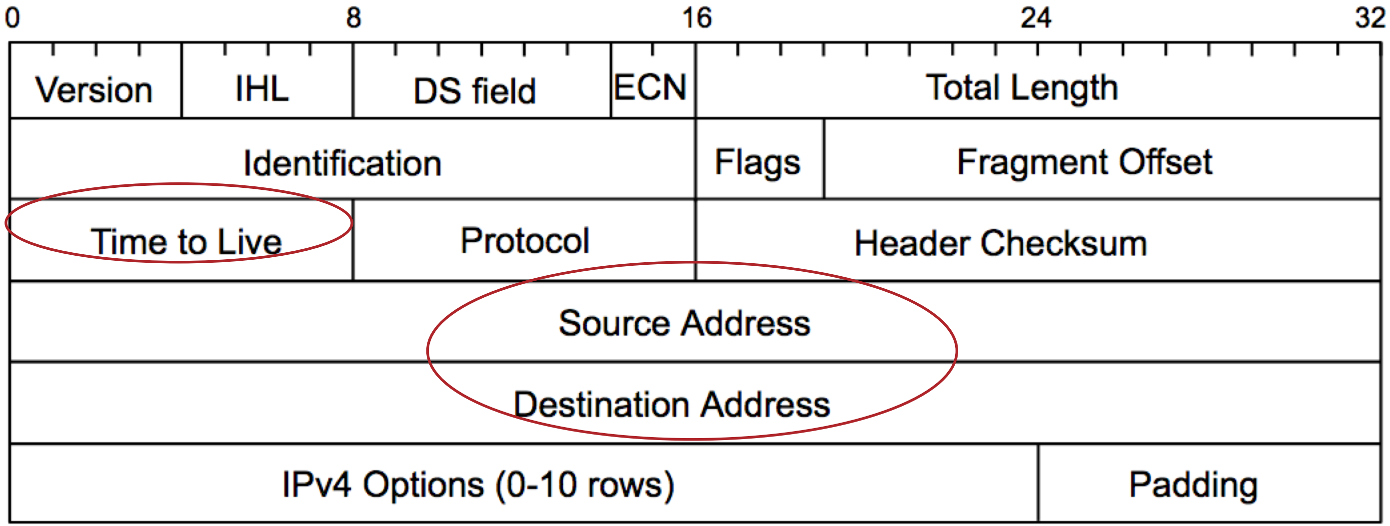
Source: https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/ip-routing-explained

Aalto University
School of Electrical
Engineering



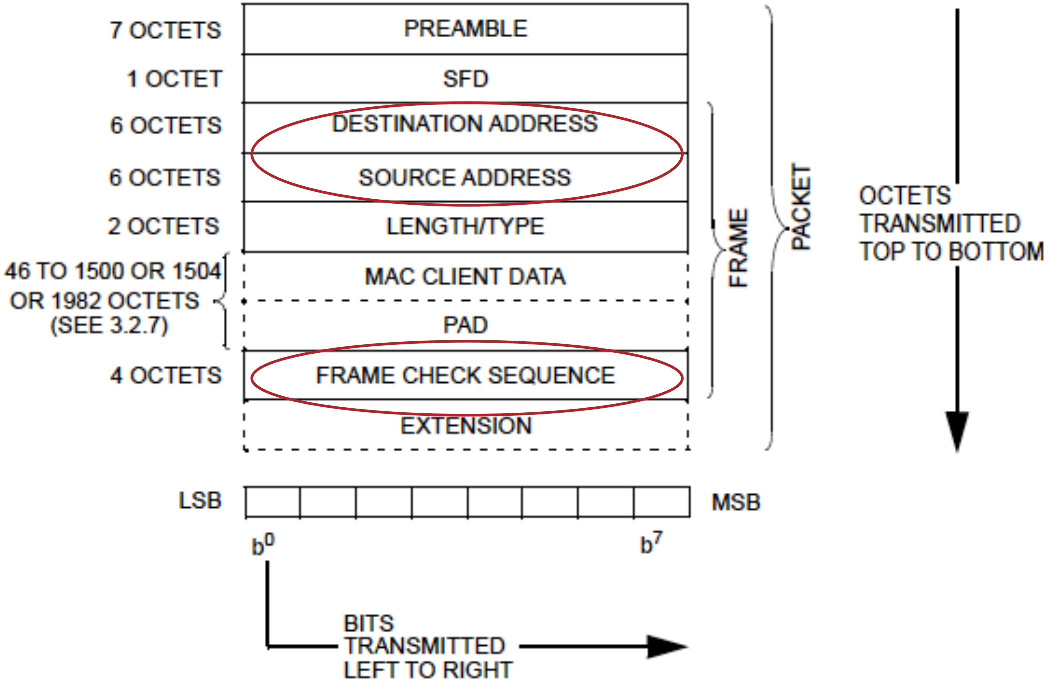
Aalto University
School of Electrical
Engineering

IPv4 Header



- **Time-to-Live (TTL):** decremented by 1 at each router; if it reaches 0, packet is discarded.

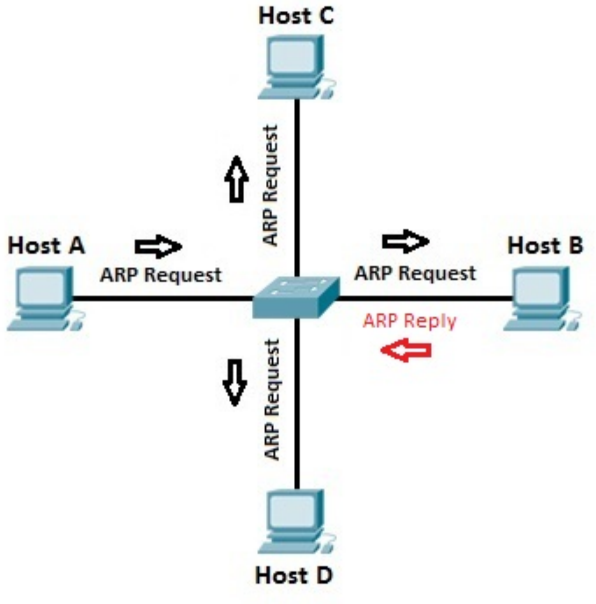
Ethernet Frame



Source: IEEE 802.3-2018

Address Resolution Protocol (ARP)

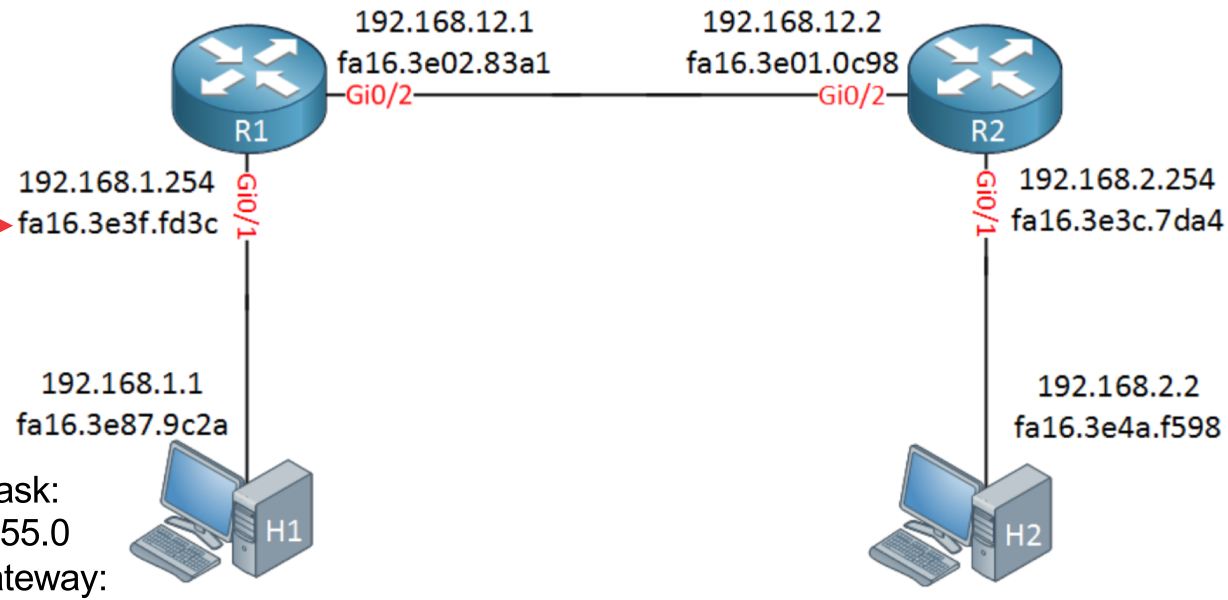
- **Data Link Layer**
- **Translate IP addresses into MAC addresses**
- It is communicated within the boundaries of a single network, never routed across internetworking nodes
- ARP requests are sent to broadcast addresses



ARP caches

- All operating systems maintain ARP caches that are checked before sending an ARP request message.
- The addresses will stay in the cache for a couple of minutes.
- Command line %arp -a

Example



MAC address

Subnet mask:
255.255.255.0
Default gateway:
192.168.1.254

Source: https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/ip-routing-explained

Process of IP Routing

H1:

1) **Create an IP packet** with its own IP address (192.168.1.1) as the source, and H2 (192.168.2.2) as the destination
2) **Check if the destination is local or remote** (e.g. check own IP, subnet mask, destination IP)
3) Build an Ethernet frame, enter its own source MAC address, and **check the destination MAC address of the default gateway**
4) Send an ARP request if MAC address is not known. After that, form an Ethernet frame that carries an IP packet and send it to R1

```
C:\Users\H1>arp -a

Interface: 192.168.1.1 --- 0x4
  Internet Address      Physical Address      Type
  192.168.1.254         fa-16-3e-3f-fd-3c     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Process of IP Routing

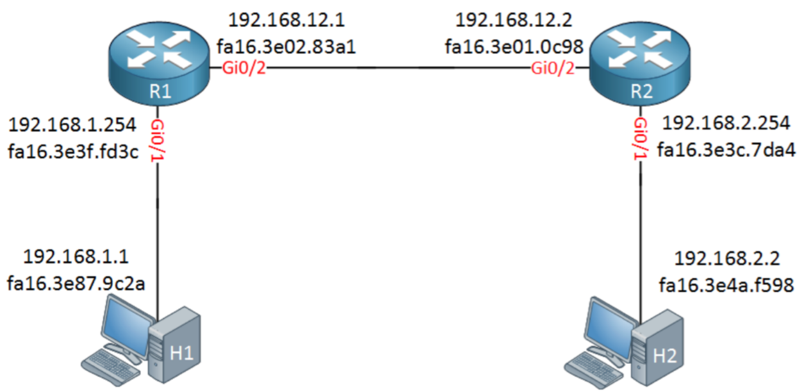
R1:

1) **Check if FCS (Frame Check Sequence) of the Ethernet frame is correct or not. If FCS is incorrect, the frame is dropped.**
2) **If FCS is correct, check if the destination MAC address is**
   - The address of the interface of the router, or
   - A broadcast address of the subnet that the router interface is connected to, or
   - A multicast address that the router listens to
3) **If MAC address matches in previous step, de-encapsulate the IP packet out of the Ethernet frame**

Process of IP Routing – R1 (cont.)

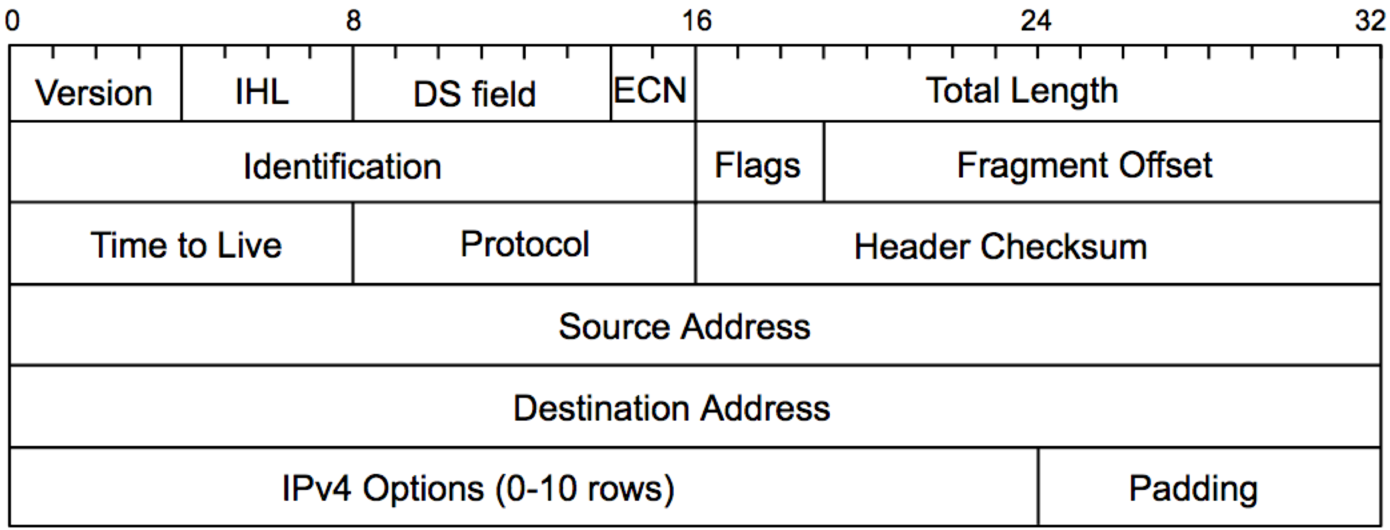
4) Check if the header checksum of the IP packet is correct. If not, drop the IP packet.

5) Check its routing table to see if there is a match for the destination IP address




```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/1
L        192.168.1.254/32 is directly connected, GigabitEthernet0/1
S     192.168.2.0/24 [1/0] via 192.168.12.2
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, GigabitEthernet0/2
L        192.168.12.1/32 is directly connected, GigabitEthernet0/2
```

IPv4 Header


0
8
16
24
32
Version
IHL
DS field
ECN
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
IPv4 Options (0-10 rows)
Padding

Process of IP Routing – R1 (cont.)

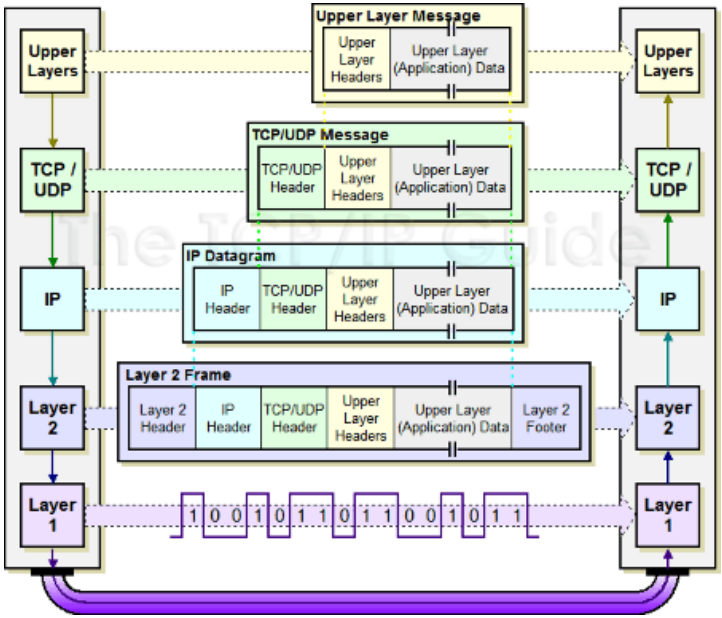
6) Decrease the TTL field by one and recalculate the header checksum

7) Check its ARP table to see if there is an entry for 192.168.12.2. If not, send an ARP request.

```
R1#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1             58  fa16.3e87.9c2a  ARPA
GigabitEthernet0/1
Internet  192.168.1.254            -  fa16.3e3f.fd3c  ARPA
GigabitEthernet0/1
Internet  192.168.12.1             -  fa16.3e02.83a1  ARPA
GigabitEthernet0/2
Internet  192.168.12.2            95  fa16.3e01.0c98  ARPA
GigabitEthernet0/2
```

Process of IP Routing – R1 (cont.)

8) Build a new Ethernet frame with its own MAC address of Gi0/2 as source and R2 as the destination. Encapsulate the IP packet into the new Ethernet frame.



Source: https://buildingautomationmonthly.com/what-is-the-tcp-ip-stack/

Process of IP Routing – R2

This Ethernet frame makes it to R2. Like R1 it will first do this:

- Check the FCS of the Ethernet frame.
- De-encapsulates the IP packet, discard the frame.
- Check the IP header checksum.
- Check the destination IP address.

```
R2#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.2.2            121  fa16.3e4a.f598  ARPA
GigabitEthernet0/1
Internet  192.168.2.254            -  fa16.3e3c.7da4  ARPA
GigabitEthernet0/1
Internet  192.168.12.1           111  fa16.3e02.83a1  ARPA
GigabitEthernet0/2
Internet  192.168.12.2             -  fa16.3e01.0c98  ARPA
GigabitEthernet0/2
```

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

S     192.168.1.0/24 [1/0] via 192.168.12.1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/1
L        192.168.2.254/32 is directly connected, GigabitEthernet0/1
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, GigabitEthernet0/2
L        192.168.12.2/32 is directly connected, GigabitEthernet0/2
```

Process of IP Routing – H2

H2 receives the Ethernet frame and will:

- Check the FCS
- Find its own MAC address as the destination MAC address.
- De-encapsulates the IP packet from the frame.
- Finds its own IP address as the destination in the IP packet.

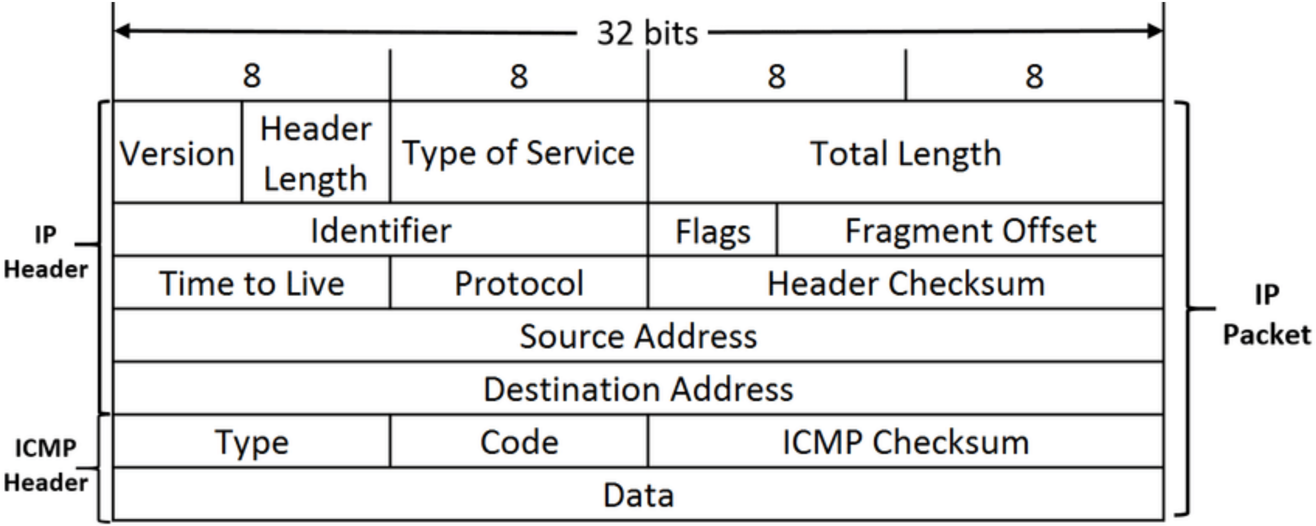
Which actions could be taken by a router if a specific match is not made to a route in the routing table?

a) The packet will be discarded
b) The packet will be sent back to the source
c) The packet will be flooded out all interfaces
d) Neighbouring routers are polled to find the best path
e) The packet will be forwarded to a default route if one is present

Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP)

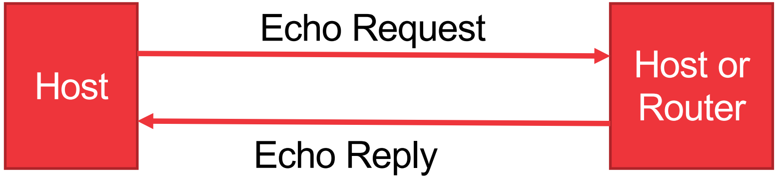
- **Used by network tools like Ping and Traceroute**
- **Host-to-host protocol, used for sending IP layer error and status messages**



- **ICMP parameters: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml**

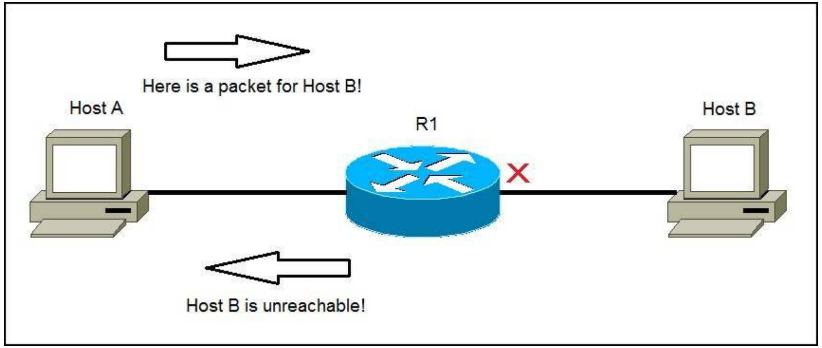
```
Type    Name
----    -------------------------
  0     Echo Reply                              (used by "ping")
                 Codes
            0  No Code
  1     Unassigned
  2     Unassigned
  3     Destination Unreachable
        Codes
            0  Net Unreachable
            1  Host Unreachable
            2  Protocol Unreachable
            3  Port Unreachable
            4  Fragmentation Needed and Don't Fragment was Set
            5  Source Route Failed
            6  Destination Network Unknown
            7  Destination Host Unknown
            8  Source Host Isolated
            9  Communication with Destination Network is
               Administratively Prohibited
           10  Communication with Destination Host is
               Administratively Prohibited
           11  Destination Network Unreachable for Type of Service
           12  Destination Host Unreachable for Type of Service
           13  Communication Administratively Prohibited

                                    14  Host Precedence Violation

                                    15  Precedence cutoff in effect


  4     Source Quench
        Codes
            0  No Code
```

ICMP Messages



Host A will start the ping utility that will send **ICMP Echo Request** packets to Server. If Server is reachable, it will respond with **ICMP Echo Reply** packets.

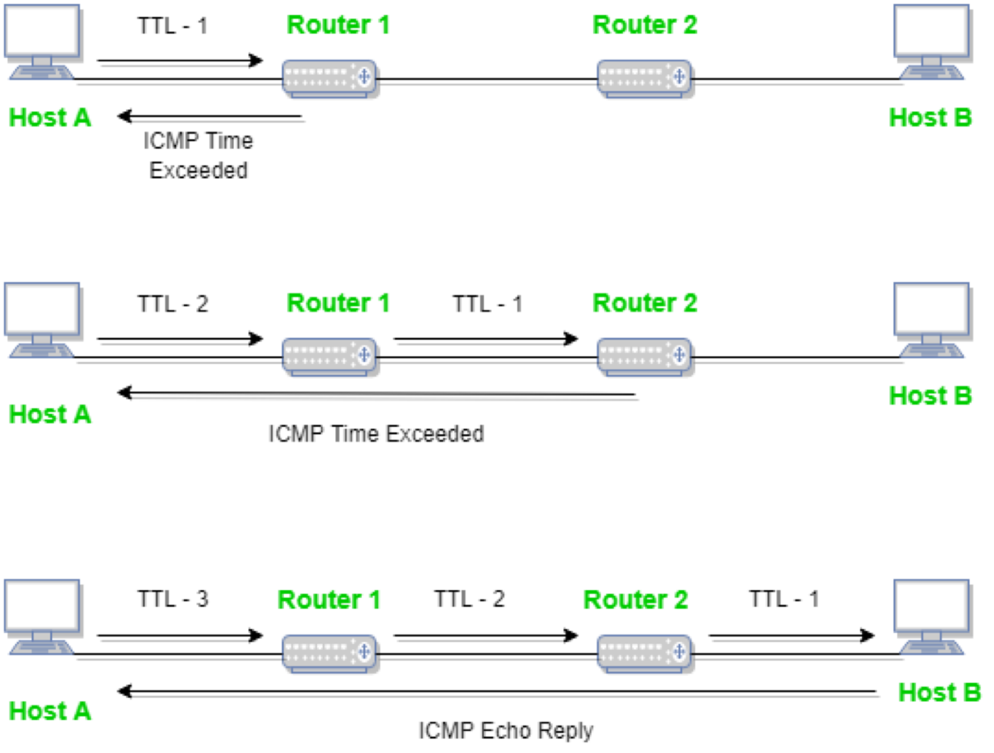
ICMP Messages



Host A sends a packet to Host B. Because the Host B is down, the router will send an **ICMP Destination host unreachable** message to Host A, informing it that the destination host is unreachable

Source: https://study-ccna.com/icmp-internet-control-message-protocol/

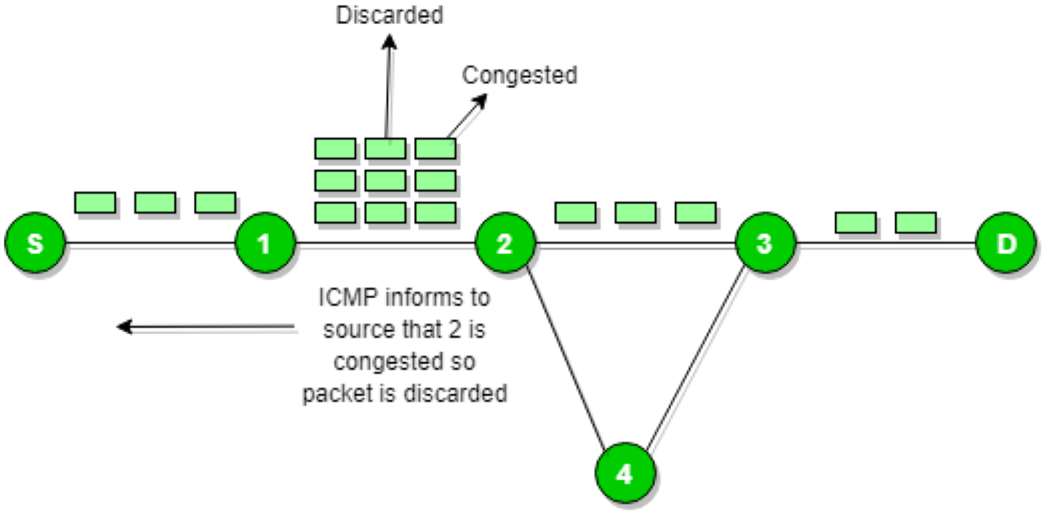
ICMP Time Exceeded Messages



Source: https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/

ICMP Source Quench Message

When receiving host detects that rate of sending packets to it is too fast, it sends the source quench message to the source to slow the pace down.



Source: https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/

Reading Task

Chapter 9, 11