Network Layer: IPv4 Functions

Lecture 7 | CSE421 – Computer Networks

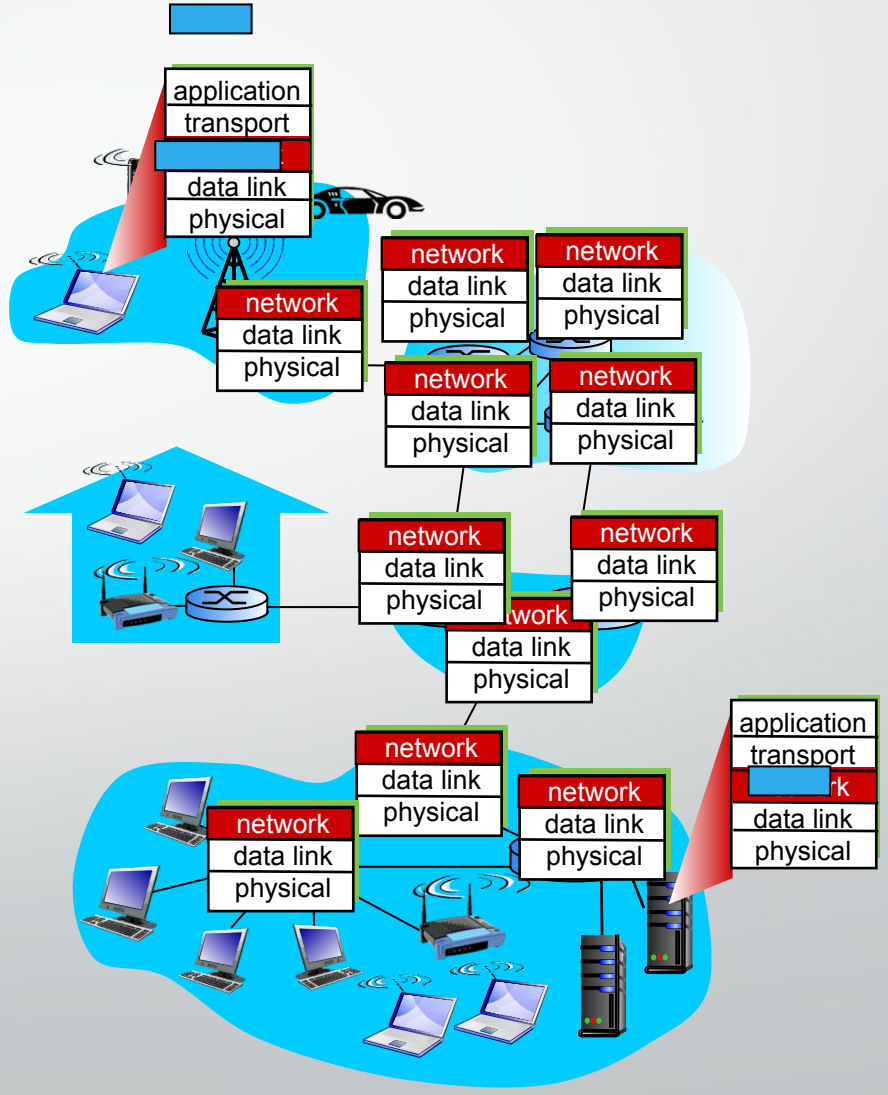
Department of Computer Science and Engineering
School of Data & Science

Objectives

- Short overview of the Network Layer
- Packet Switching: Virtual Circuits & Datagram Networks
- IP Fragmentation & Reassembly
- ICMP
  - Ping
  - Traceroute

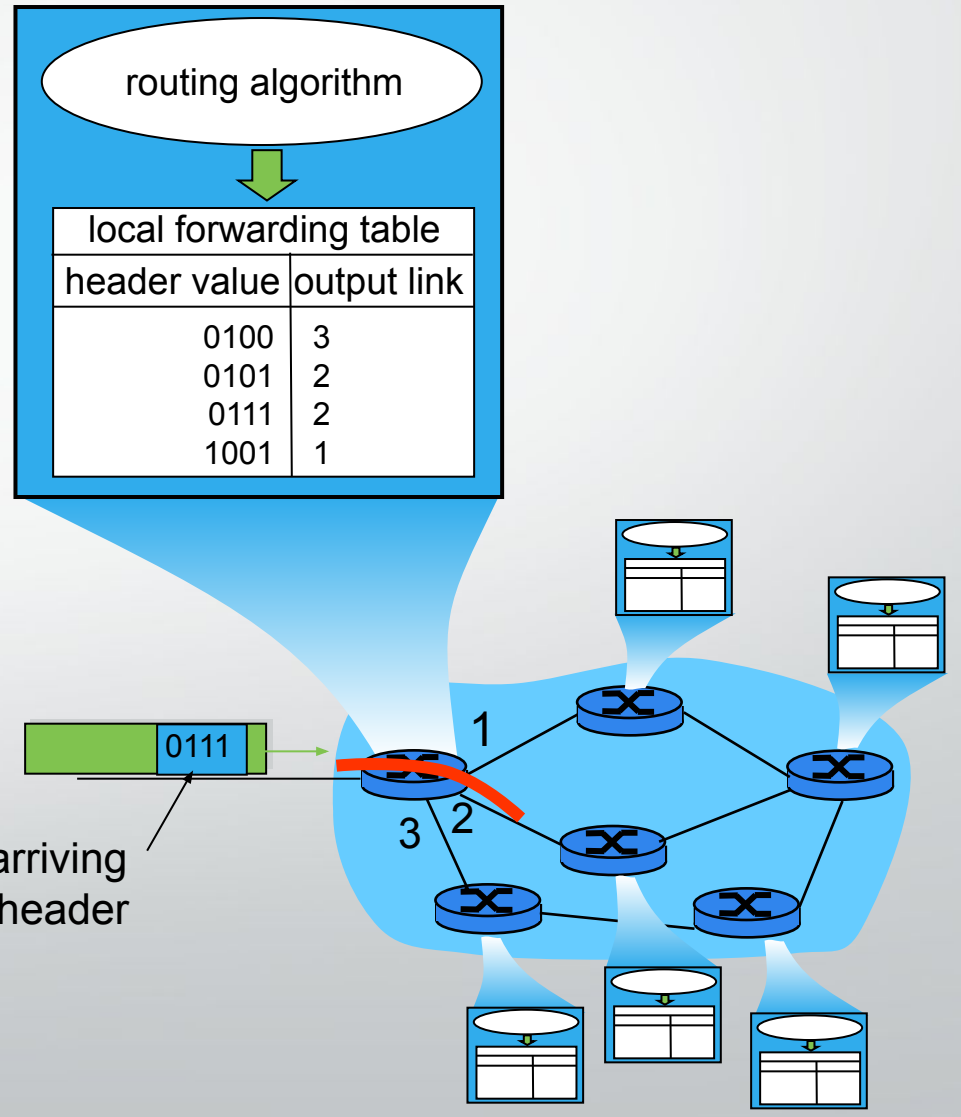
The Network Layer

- Transport segment from sending to receiving host
- On sending side encapsulates segments into packets
- Network layer protocols in every host, router
- Router examines header fields in all IP packets passing through it
- On receiving side, delivers segments to transport layer



Functions of Network Layer

- **Forwarding:** move packets from router's input to appropriate router output
  - Analogy: process of getting through a single interchange
- **Routing:** determine route taken by packets from source to destination
  - The algorithms that calculate the paths are referred to as routing algorithms.
  - Analogy: process of planning trip from source to destination
  - Has various routing algorithms



BRAC UNIVERSITY
Inspiring Excellence

Packet Switching:

Virtual Circuits

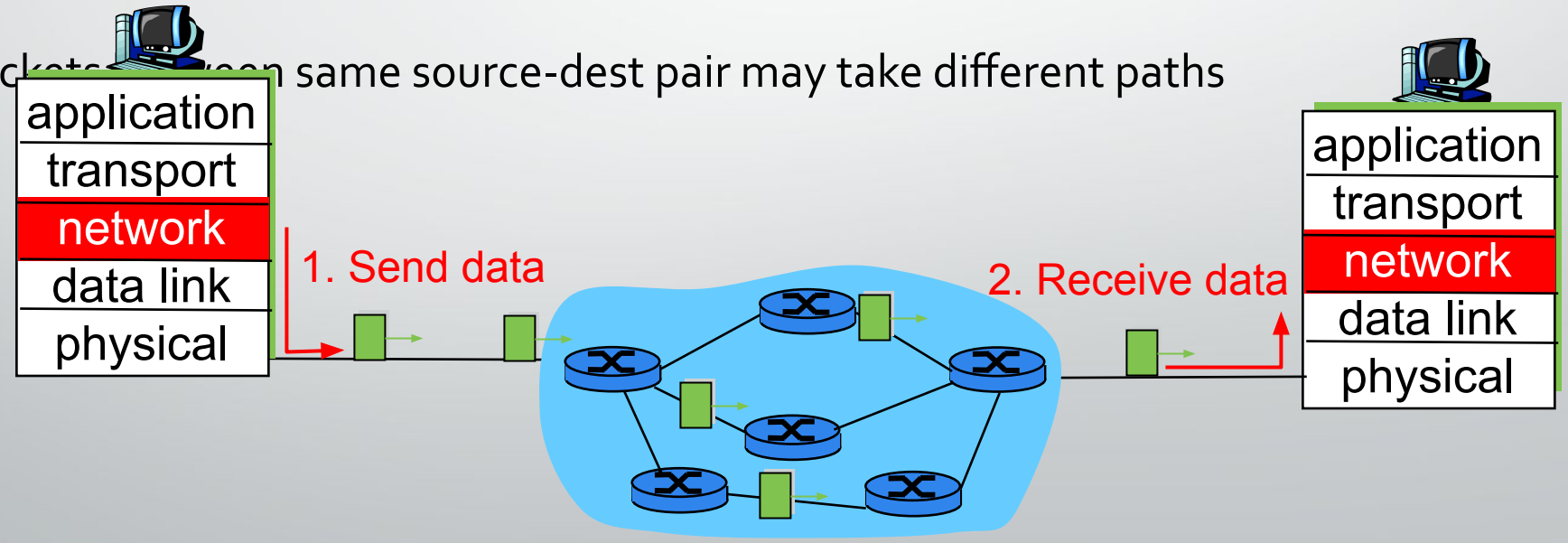
Datagram Network

Connection and Connection-less service

- Datagram network => network-layer connectionless service
- VC network => network-layer connection service
  - analogous to the transport-layer services, but:
  - **service:** host-to-host
  - **no choice:** network provides one or the other
  - **implementation:** in network core

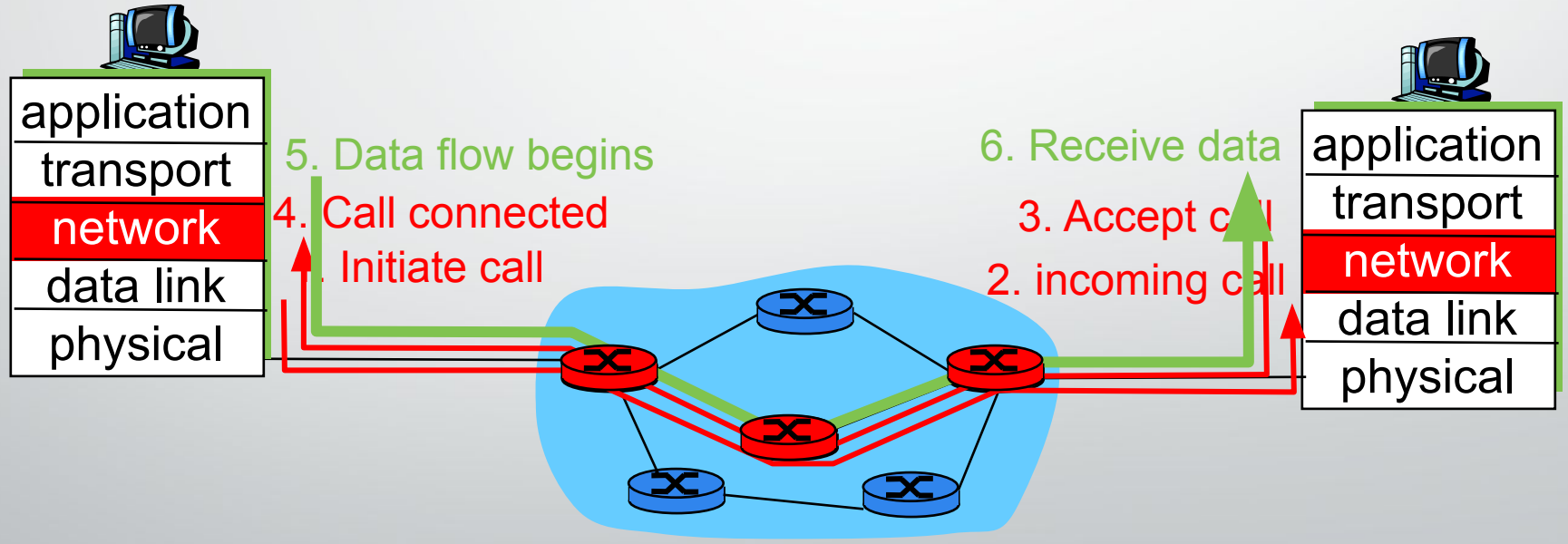
Datagram networks

- No call setup at network layer
- Routers: no state about end-to-end connections
  - no network-level concept of "connection"
- Packets forwarded using destination host address
  - packets between same source-dest pair may take different paths

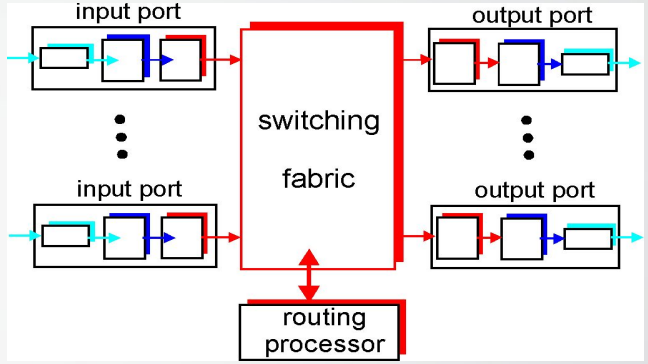


Virtual Circuits: Signaling Protocols

- Used to setup, maintain teardown VC
- Used in ATM, frame-relay, X.25
- Not used in today's Internet



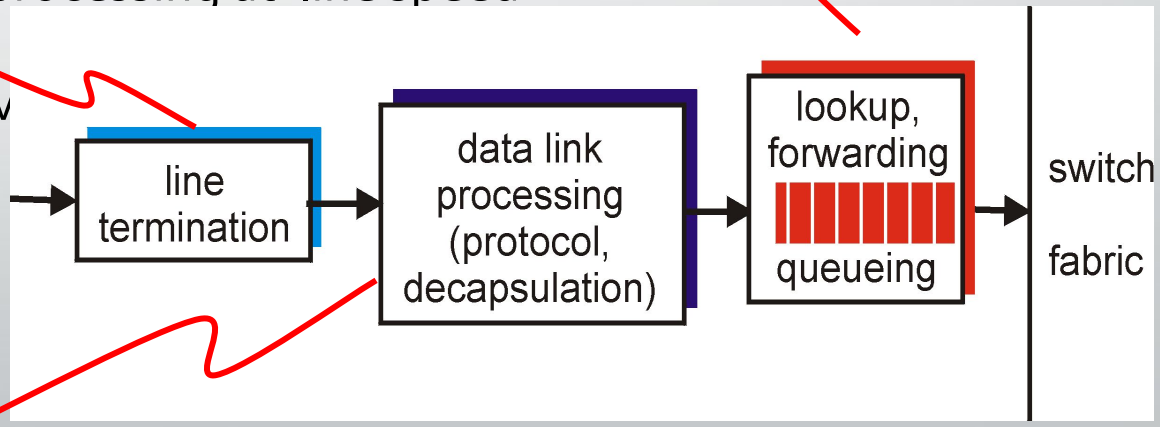
Functions of a Router



- Run routing algorithms/protocol (RIP, OSPF, BGP)
- **Forwarding** datagrams from incoming to outgoing link
- **Decentralized switching:**
  - Given datagram dest., lookup output port using forwarding table in input port memory
  - **Goal:** complete input port processing at 'line speed'
  - **Queuing:** if datagrams arriv

Physical layer:
bit-level reception

Data link layer:
e.g., Ethernet

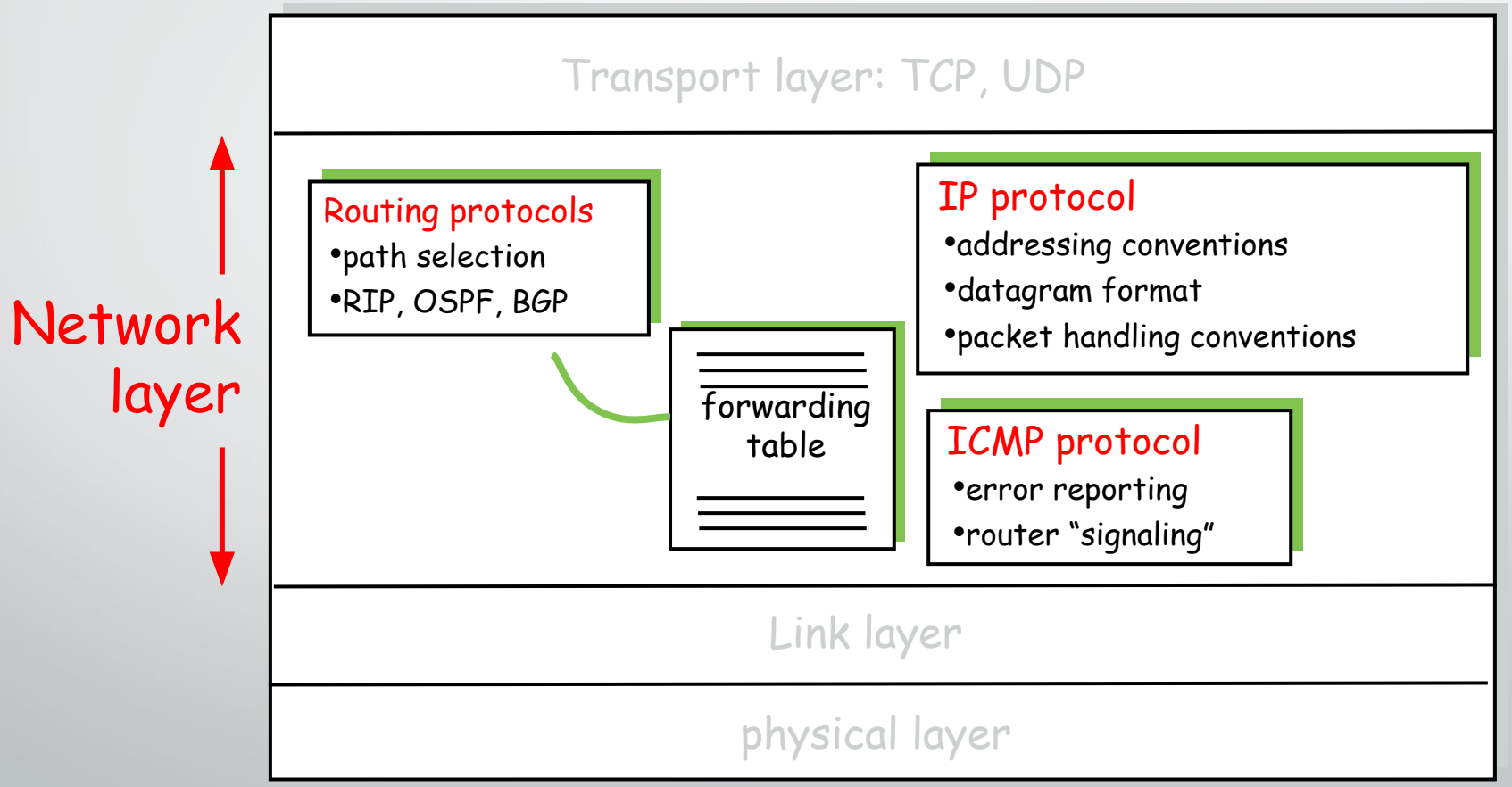


BRAC UNIVERSITY
Inspiring Excellence

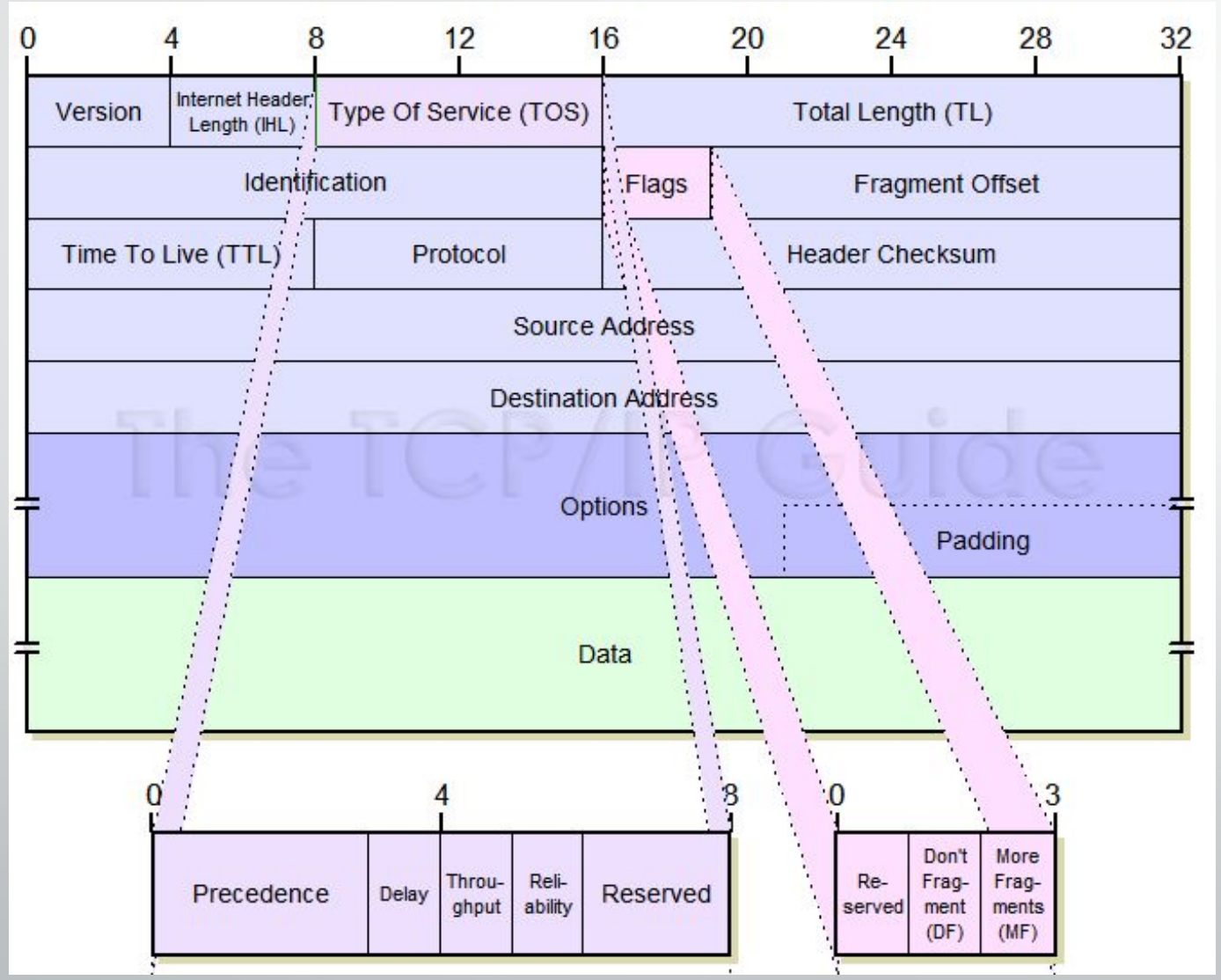
Internet Protocol

Internet Network Layer

- Host, router network layer functions:



IPv4 Datagram Format

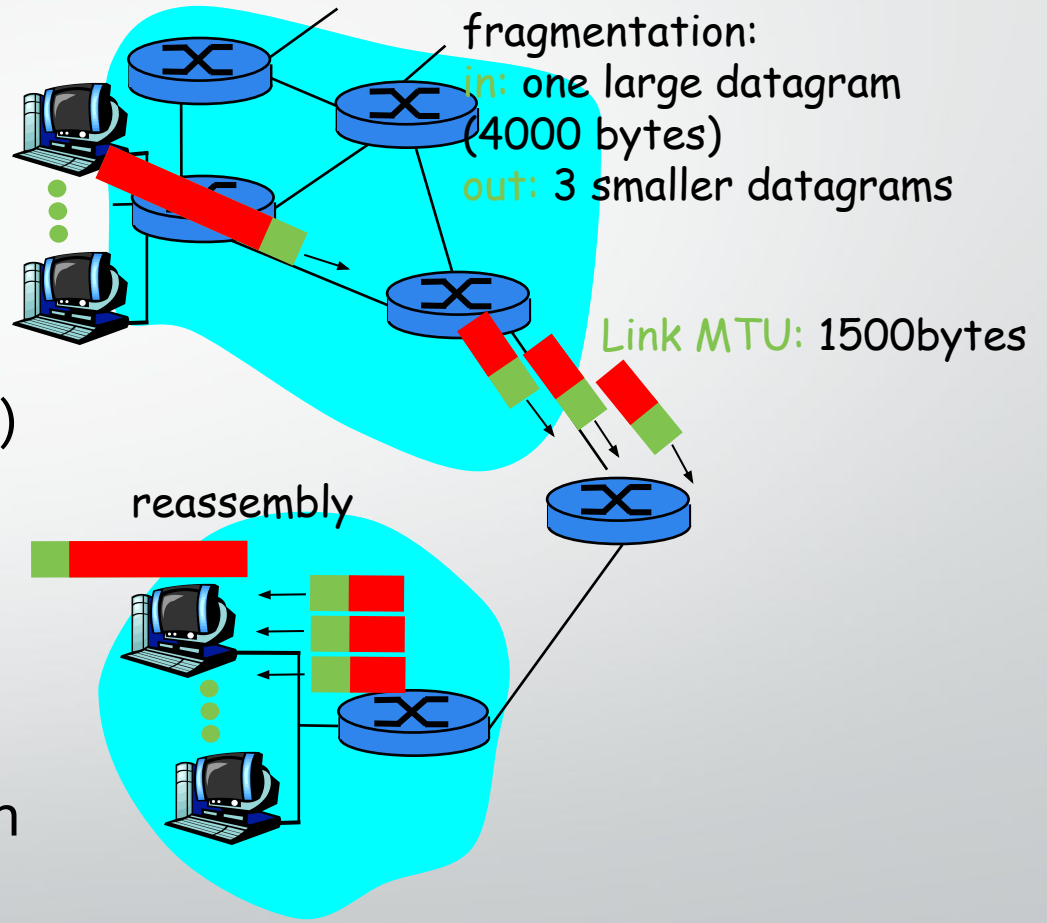


The size of an IP datagram:

- The minimum size is 20 bytes (if you have no data)
- The maximum size is 65,535 bytes

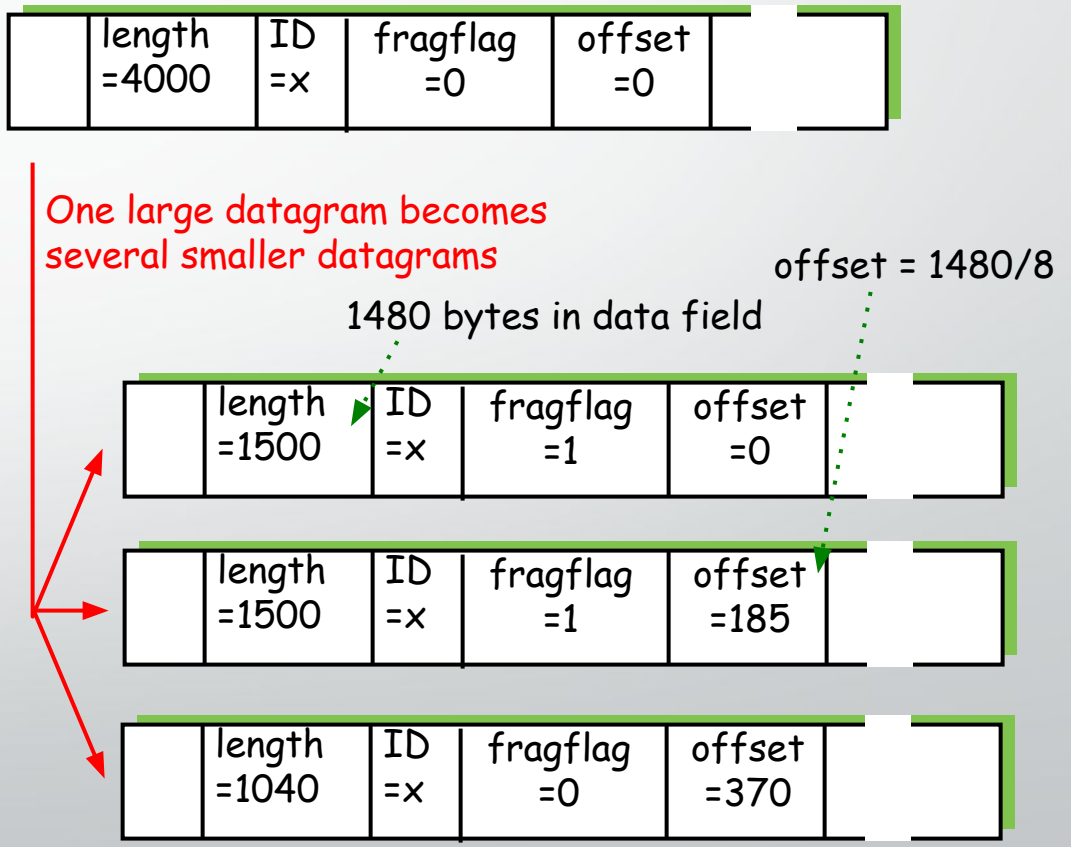
IP Fragmentation & Reassembly

- Network links have **MTU (max. transmission unit - max. transfer size)** - largest possible link-level frame.
  - different link types, different MTUs
- Large IP datagram divided ("fragmented") within net
  - one datagram becomes several datagrams
  - "reassembled" only at final destination
  - IP header bits used to identify, order related fragments



IP Fragmentation & Reassembly

- Example:
  - 4000 Bytes of datagram
  - MTU = 1500 Bytes
    - Header + Data
    - Header size is usually 20 bytes
      - It can differ
  - Offset:
    - The value of the offset is measured in units of 8 bytes.
    - This is done because the length of the offset field is only 13 bits long and cannot represent a sequence of bytes greater than 8191.
    - This forces hosts or routers that fragment datagrams to choose the size of each fragment so that the first byte number is divisible by 8.



IP Fragmentation & Reassembly

BRAC UNIVERSITY
Inspiring Excellence

MTU=20(H)+1480(D)
5140=20(H)+5120(D)
5120-1480=3640 (1st)
3640-1480=2160 (2nd)
2160-1480=680 (3rd)

680+20=700

Original IP Datagram

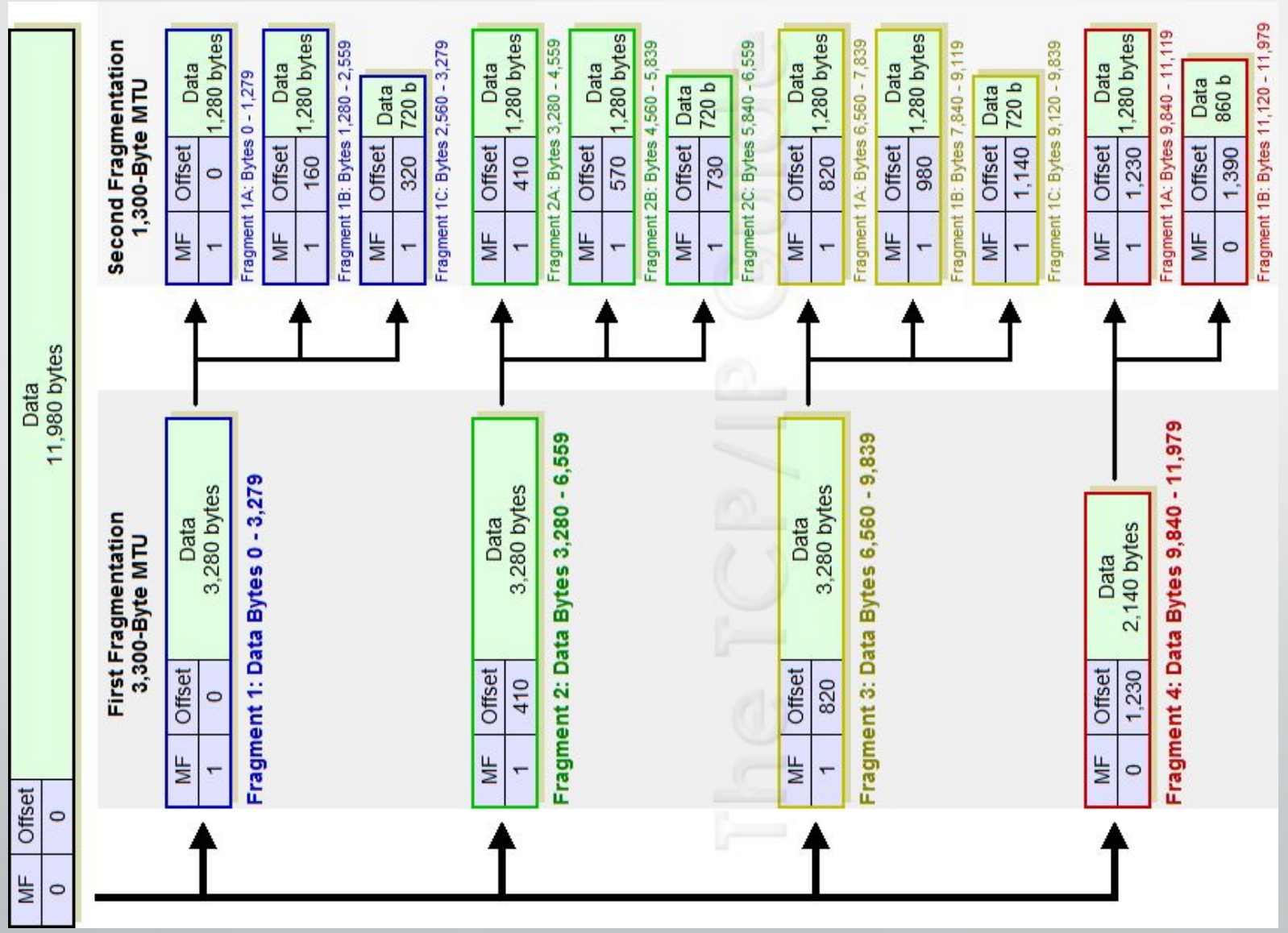
Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0	345	5140	0	0	0

IP Fragments (Ethernet)

Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0-0	345	1500	0	1	0
0-1	345	1500	0	1	185
0-2	345	1500	0	1	370
0-3	345	700	0	0	555

Data Bytes	Fragment Offset
0 -1479	0/8=0
1480-2959	1480/8=185
2960-4439	2960/8=370
4440-5119	4440/8=555

IP Fragmentation Example



BRAC UNIVERSITY
Inspiring Excellence

ICMP

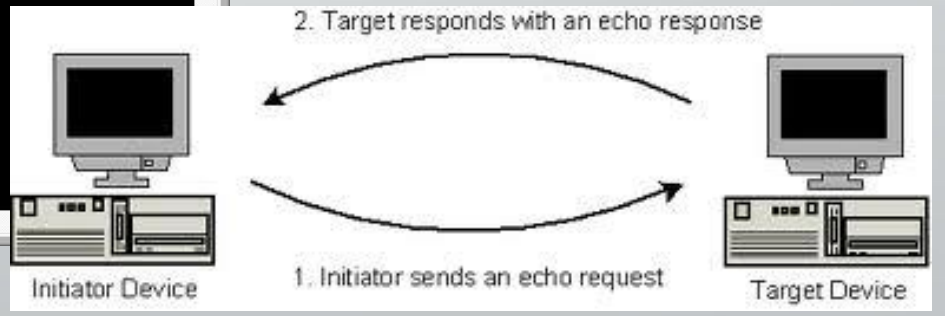
ICMP

- Also known as **Internet Control Message Protocol**
- It is mainly used by the **operating systems** in **IP** network management and administration.
- Used for
  - errors in the underlying communications of network applications
  - availability of remote hosts
  - network congestion
- It does not carry application data, but rather information about the status of the network itself.
- Example of ICMP in practice
  - PING

Ping

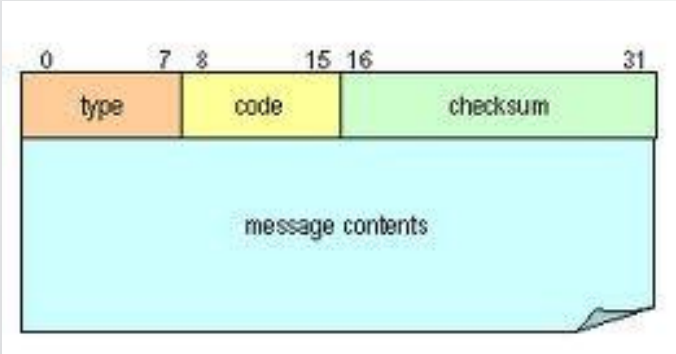
- Utility used to test the reachability of a host.
- Sends Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response.
- In the process it measures the time from transmission to reception

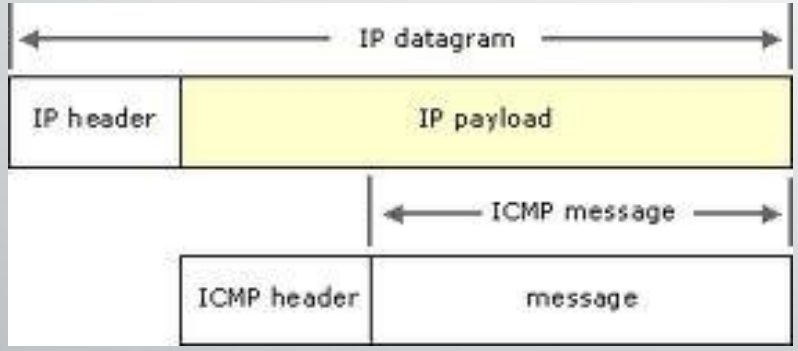
```
C:\Windows\system32\command.com
C:\USERS\LARRYP~1>ping www.pepperdine.edu

Pinging www.pepperdine.edu [137.159.8.186] with 32 bytes of data:
Reply from 137.159.8.186: bytes=32 time=37ms TTL=114
Reply from 137.159.8.186: bytes=32 time=38ms TTL=114
Reply from 137.159.8.186: bytes=32 time=36ms TTL=114
Reply from 137.159.8.186: bytes=32 time=38ms TTL=114

Ping statistics for 137.159.8.186:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 38ms, Average = 37ms

C:\USERS\LARRYP~1>
```



ICMP Message

- ICMP message: type, code plus first 8 bytes of IP datagram causing error

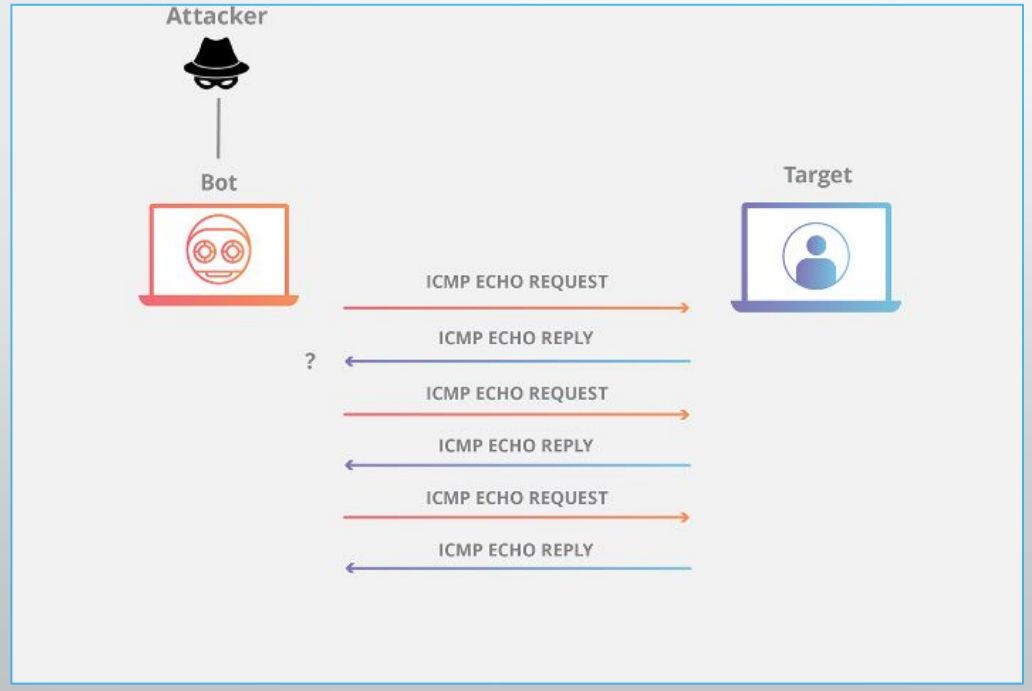




Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

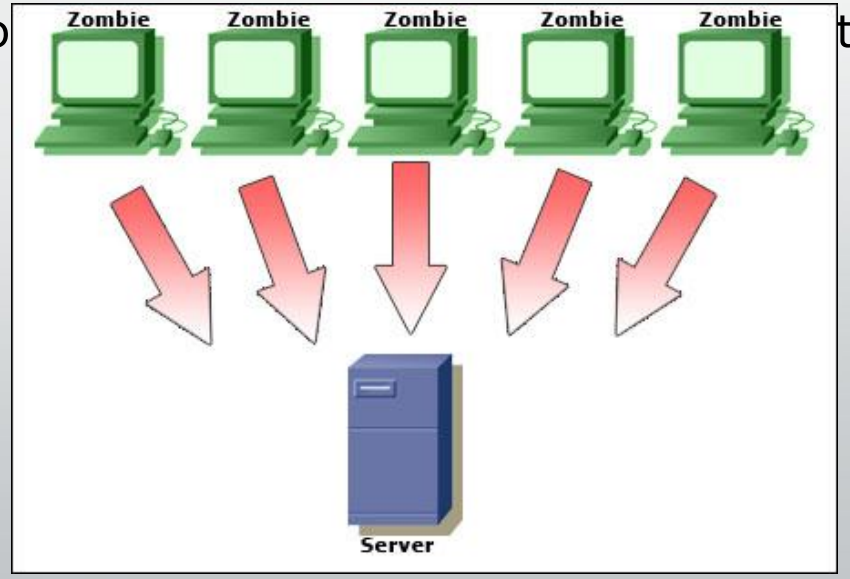
Ping Attacks

- ICMP PING flood attack /DOS Attack :
  - It uses the ICMP echo command to flood large amounts of data packets to the victim's computer in an attempt to overload it.
  - Another type of DOS Attack : Deny to give service by replying with false message.



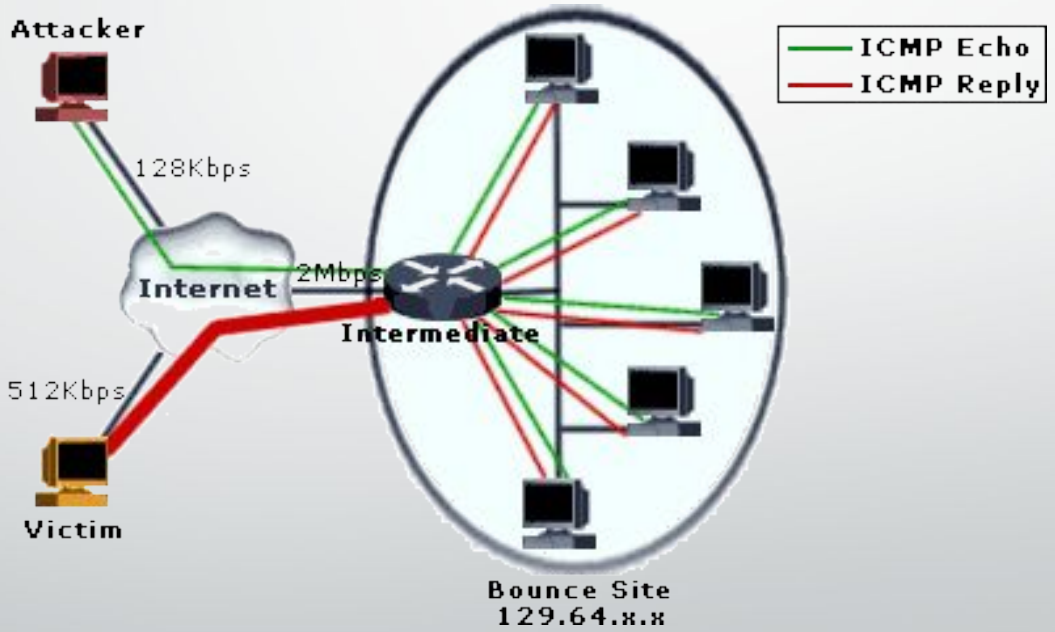
Ping Attacks

- ICMP DDOS attack – Zombie Attack:
  - Much like the ping flood method, only multiple computers are being used.
  - In this instance, the computers that are being used may or may not be aware of the fact that they are attacking a website or network.
  - Trojans and viruses commonly give the hacker control of a computer, and thus, the ability to use them fo ters are called zombies.



Ping Attacks

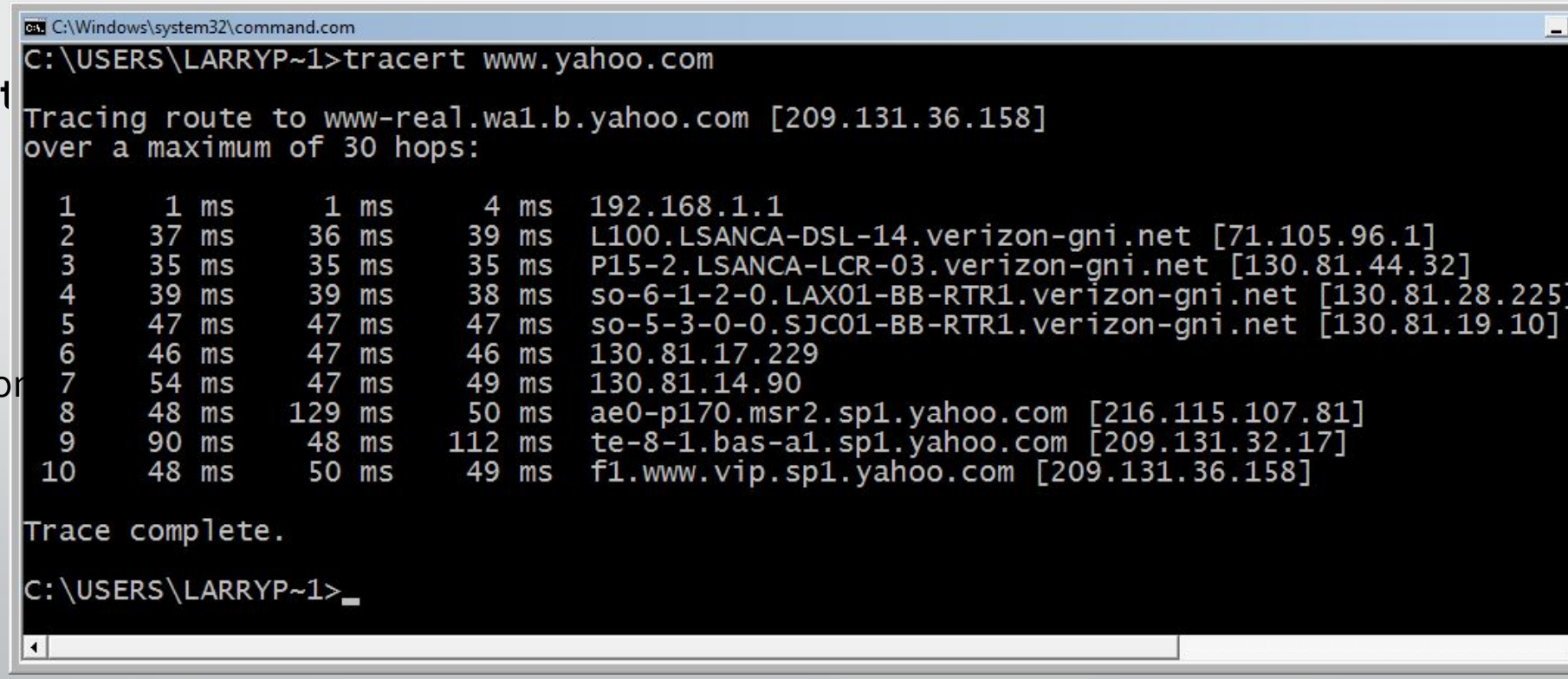
- ICMP DDOS attack – Packet magnification (or ICMP Smurf):
  - An attacker sends forged ICMP echo packets to vulnerable networks' broadcast addresses. All the systems on those networks send ICMP echo replies to the victim.



Traceroute

- Tool used to trace path from source to destination host.
- The IP address and domain name (if there is one) of each router is returned to the client.
- Commands:
  - Unix: **traceroute**
  - Cisco IOS: **traceroute (t**
  - DOS: **tracert**

Hop 1: User LAN router
Hops 2-7: Verizon (ISP) networ
Hops 8-10: the Yahoo LAN



Traceroute: Another example

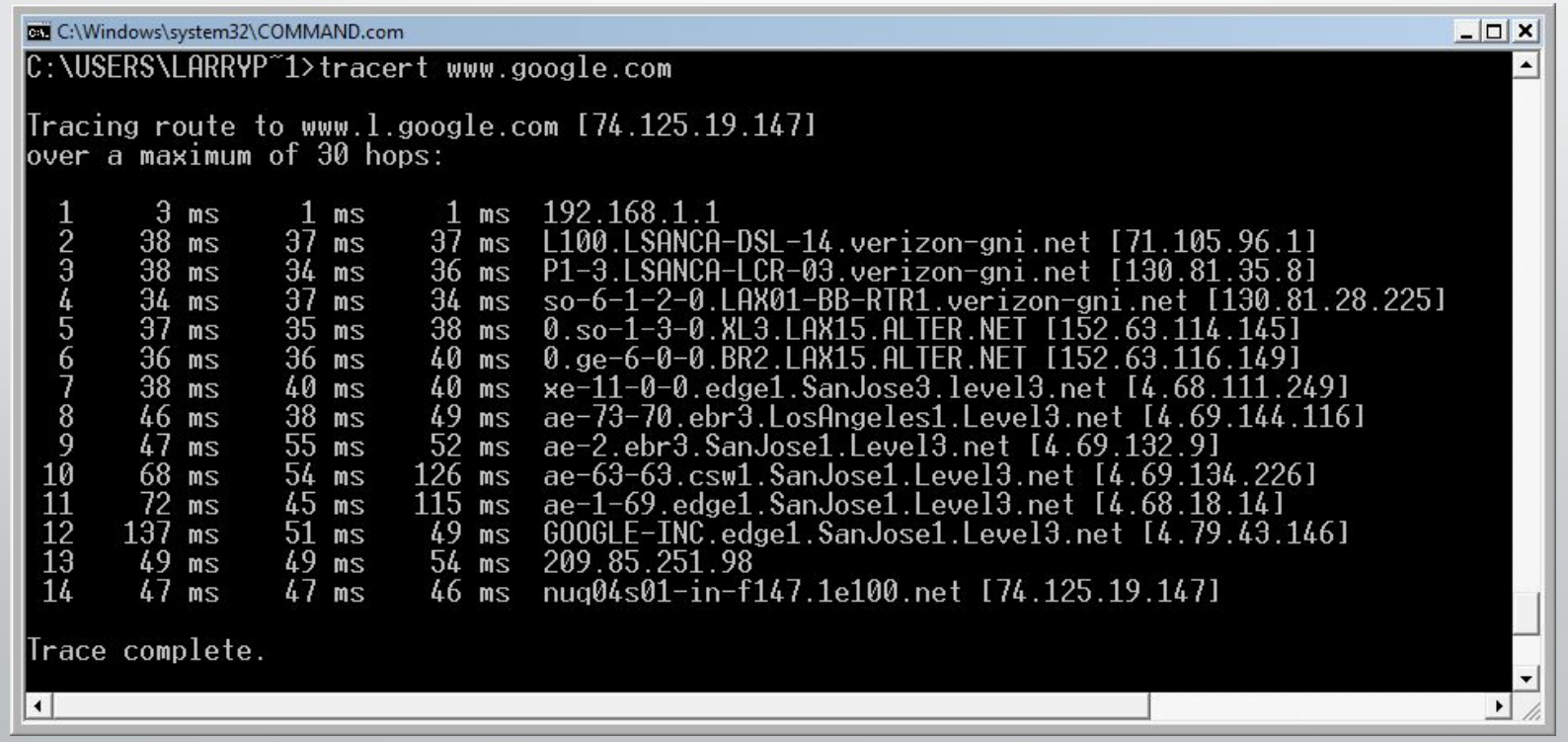
Hop 1: User LAN router

Hops 2-4: Verizon network (a backbone ISP)

Hops 5-6: Alternet (a backbone ISP)

Hops 7-11: Level 3 (a backbone ISP)

Hops 12-14: the Google LAN



Traceroute: Request Timed Out

This message indicates that the router security settings keep it from revealing its identity or the router and connection are slow.

```
*     *     *     Request timed out.
```

BRAC UNIVERSITY
Inspiring Excellence

The End