Network Layer: IPv4 Functions

Lecture 8 | CSE421 – Computer Networks

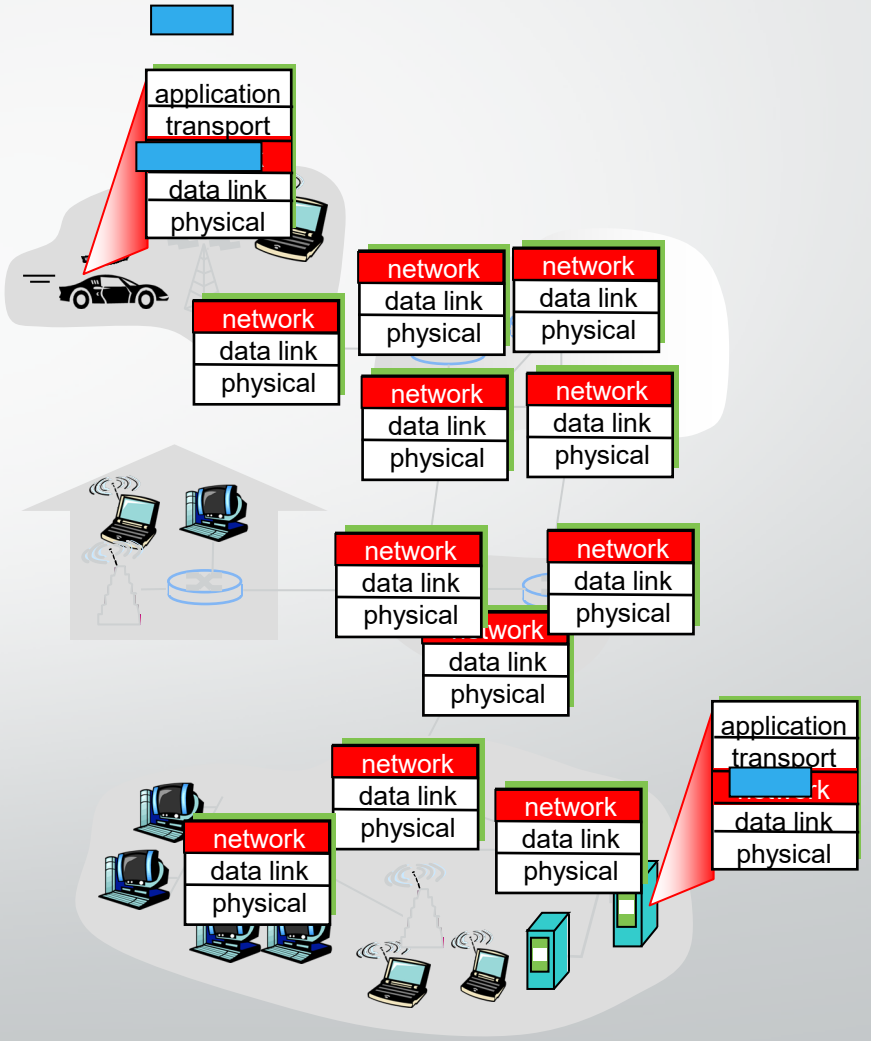
Department of Computer Science and Engineering
School of Data & Science

Objectives

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

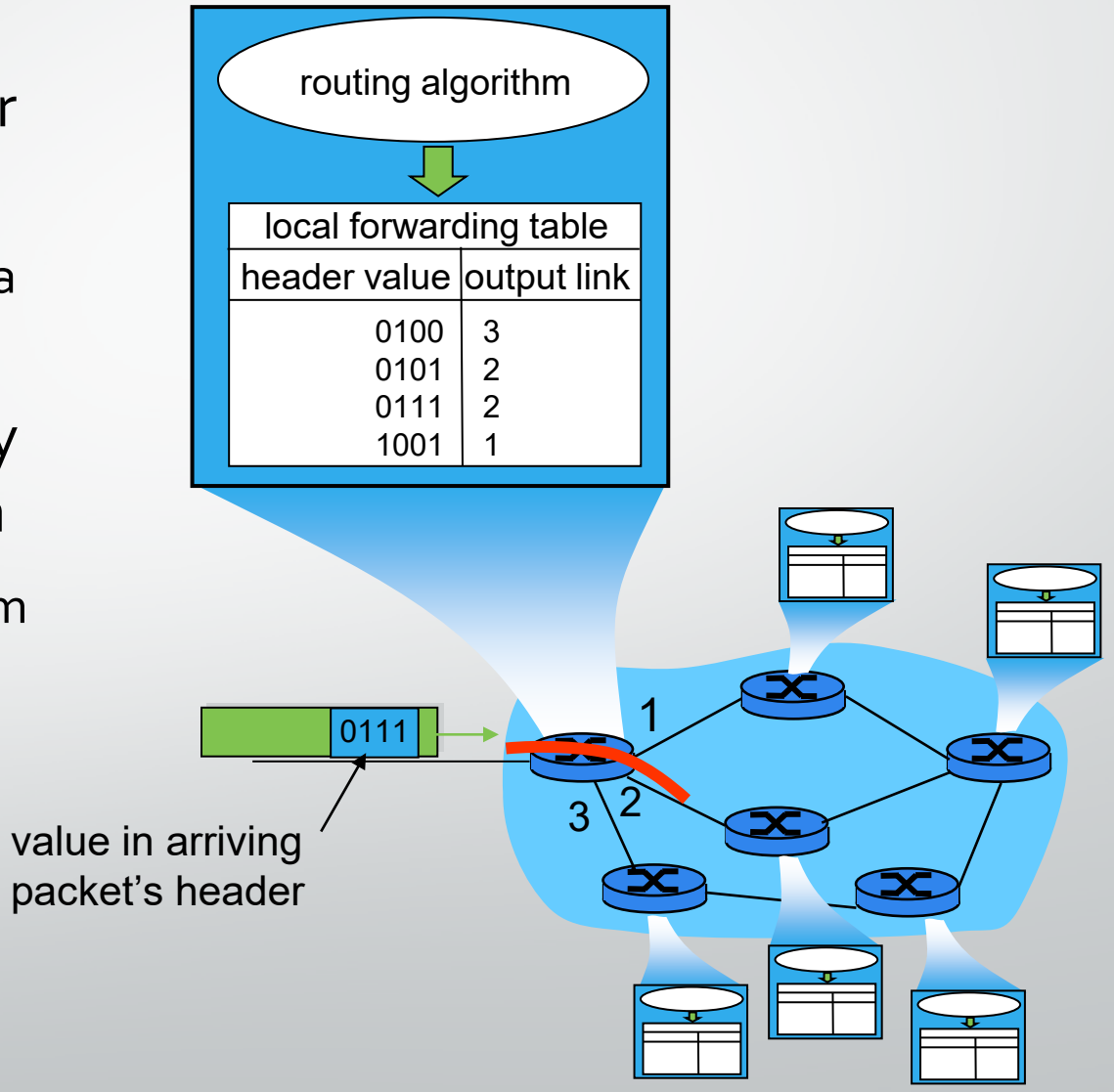
The Network Layer

- 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
  - Analogy: process of planning trip from source to dest
  - Has various routing algorithms



BRAC UNIVERSITY
Inspiring Excellence

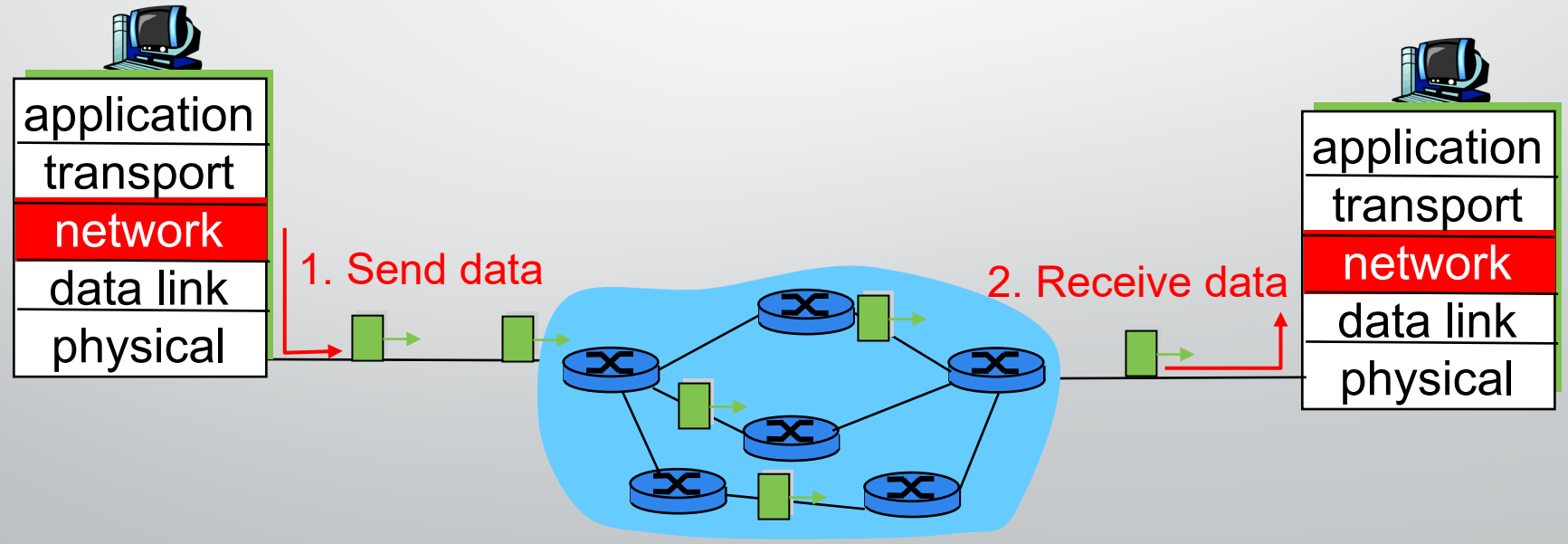
Virtual Circuits Datagram Network

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

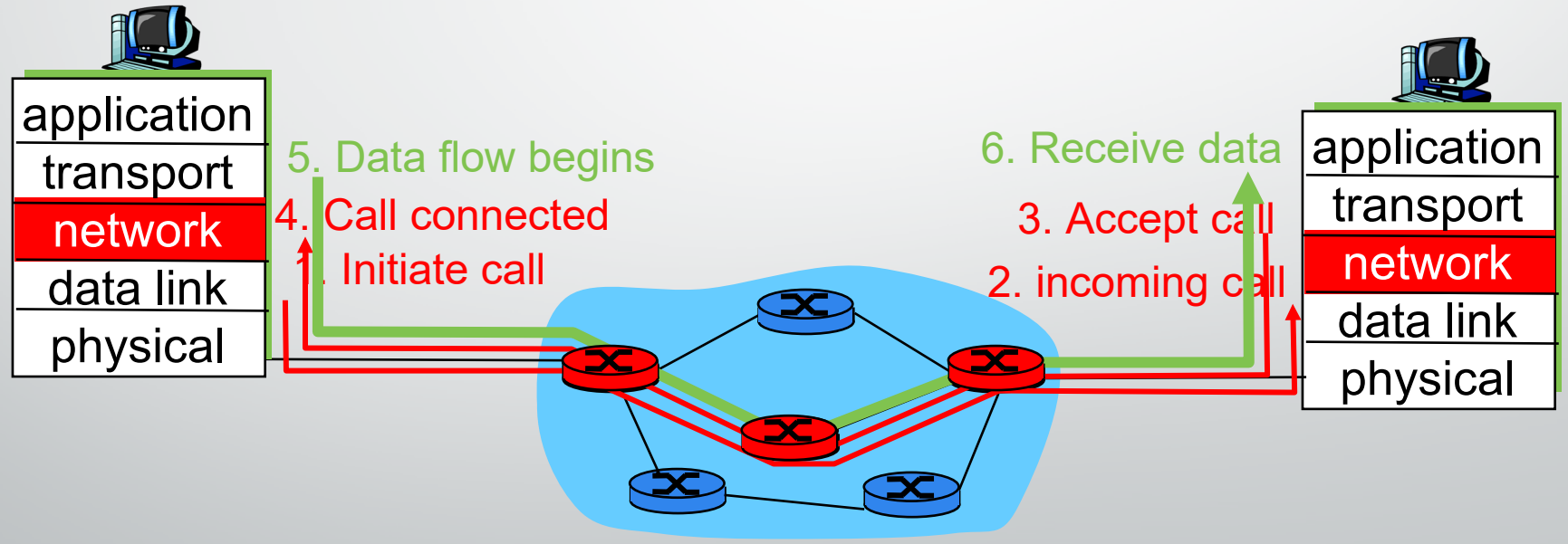
Datagram networks

- 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



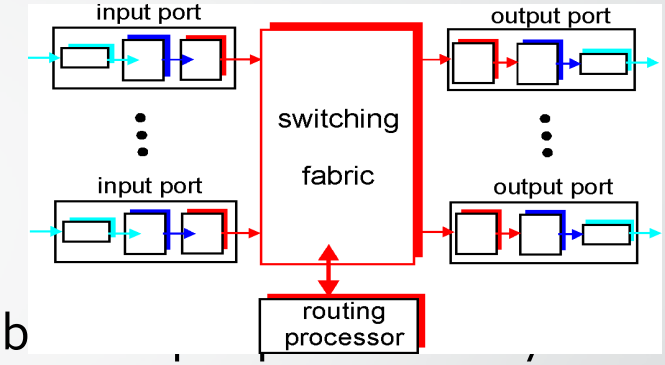
Virtual circuits: signaling protocols

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



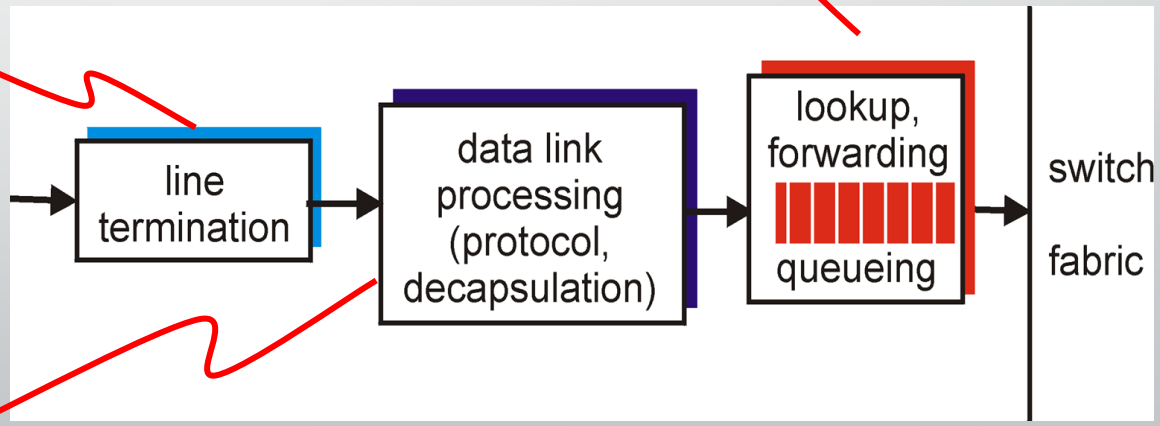
Functions of Router

- Run routing algorithms/protocol (RIP, OSPF, BGP)
- **Forwarding** datagrams from incoming to outgoing link
- **Decentralized switching:**
  - Given datagram dest., lookup output port using forwarding tab
  - **Goal:** complete input port processing at 'line speed'
  - **Queuing:** if datagrams arrive faster than forwarding rate into switch fabric



Physical layer:
bit-level reception

Data link layer:
e.g., Ethernet
see chapter 5

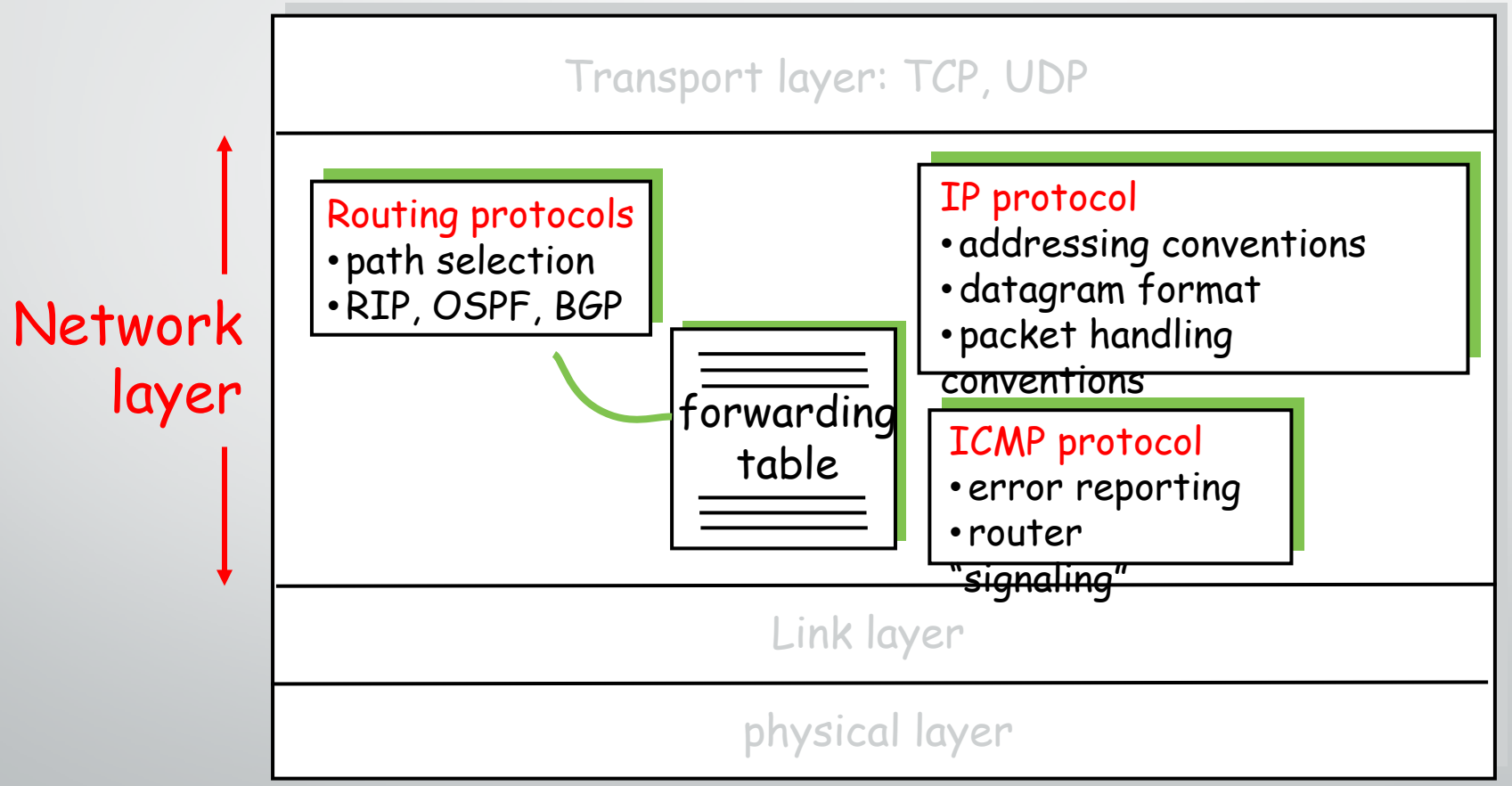


BRAC UNIVERSITY
Inspiring Excellence

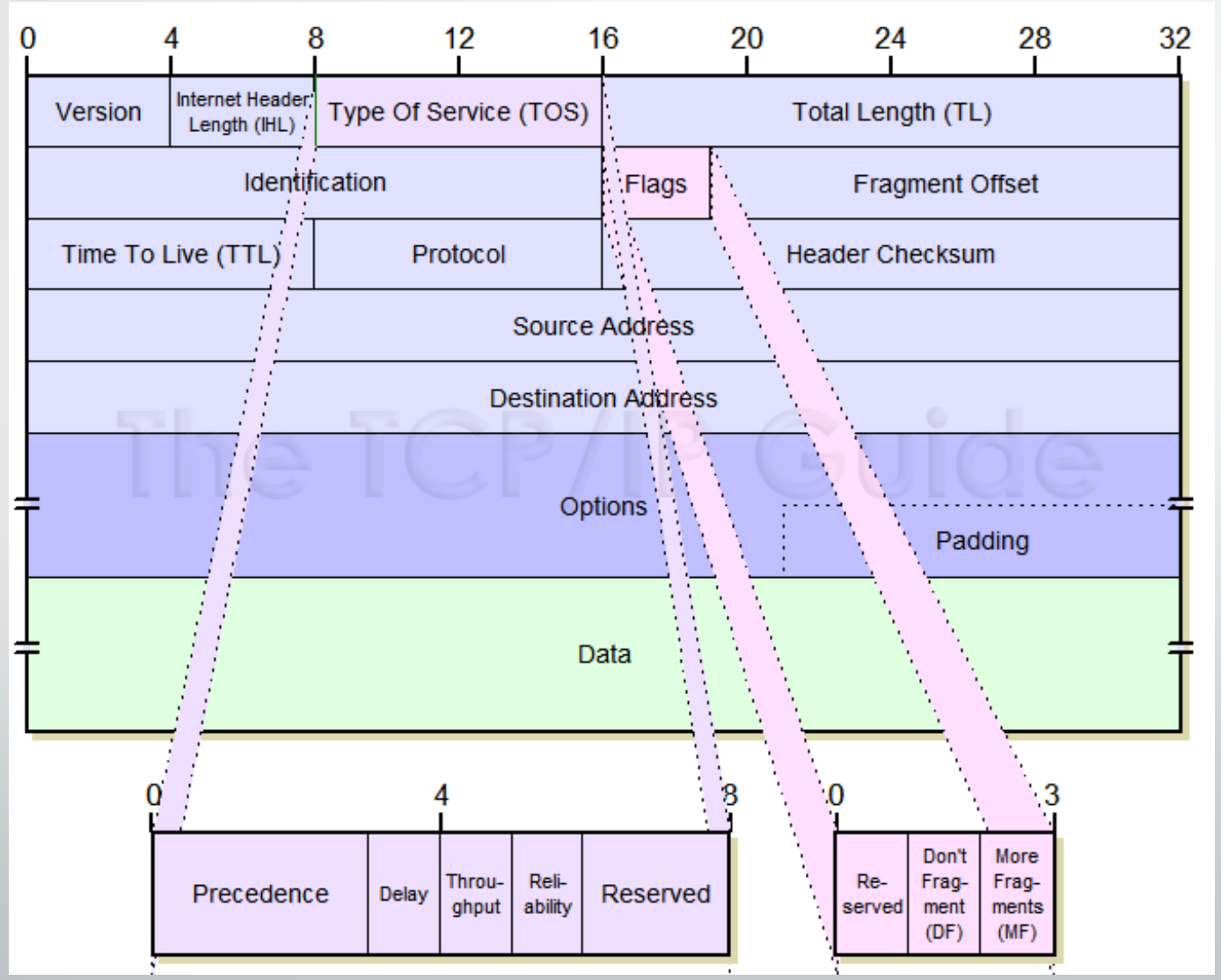
Internet Protocol

Internet Network Layer

- Host, router network layer functions:

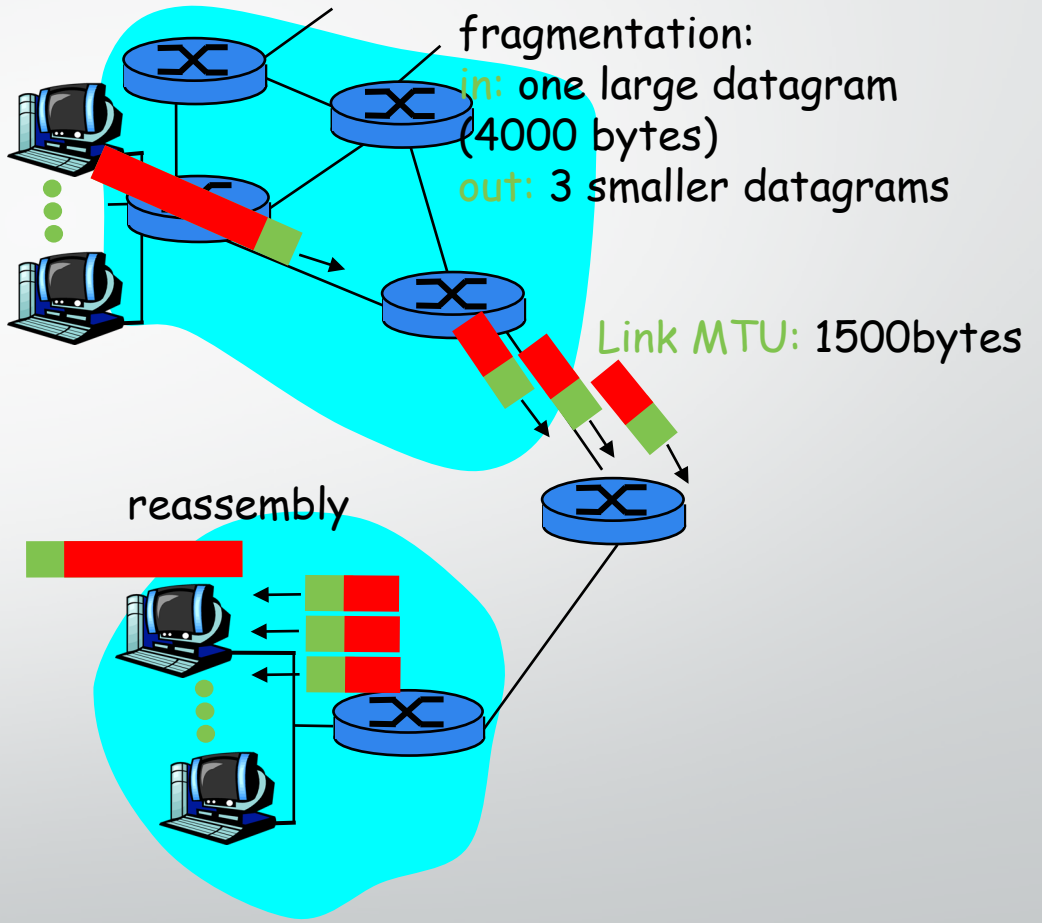


IPv4 Datagram Format



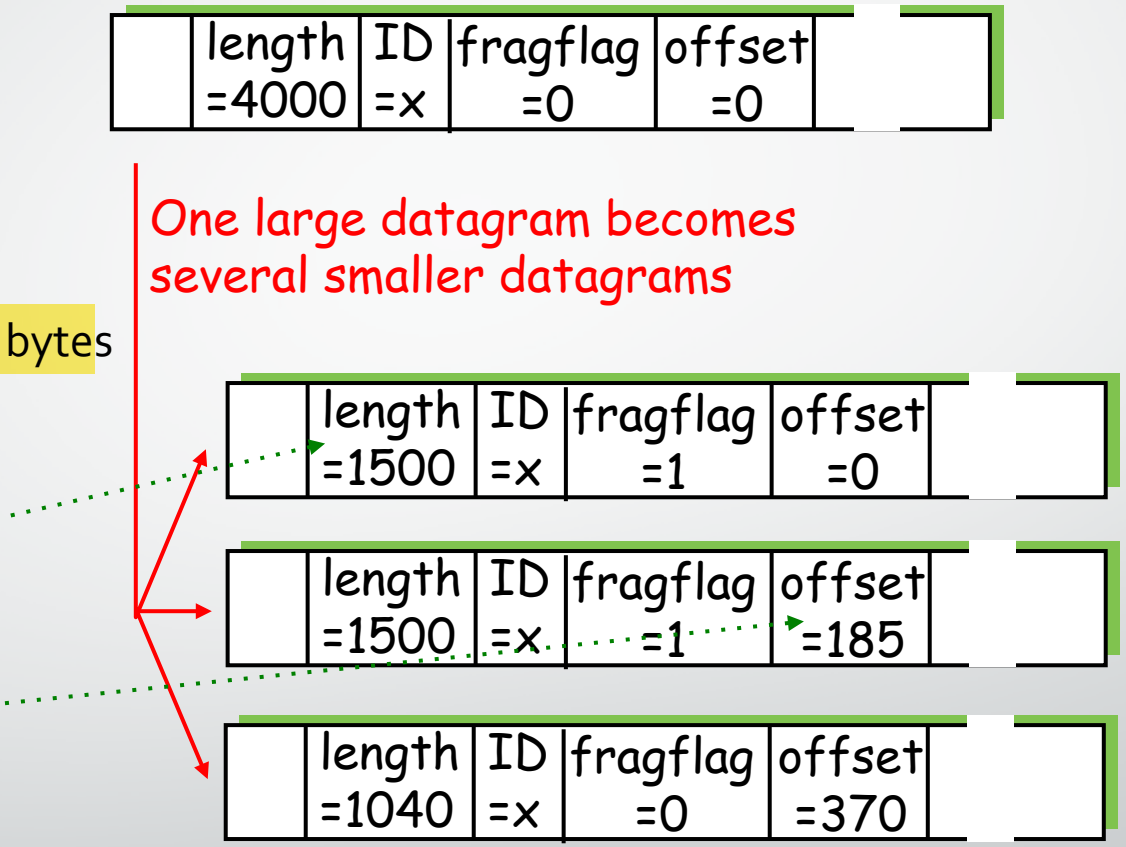
IP Fragmentation & Reassembly

- network links have **MTU (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



IP Fragmentation & Reassembly

BRAC UNIVERSITY
Inspiring Excellence

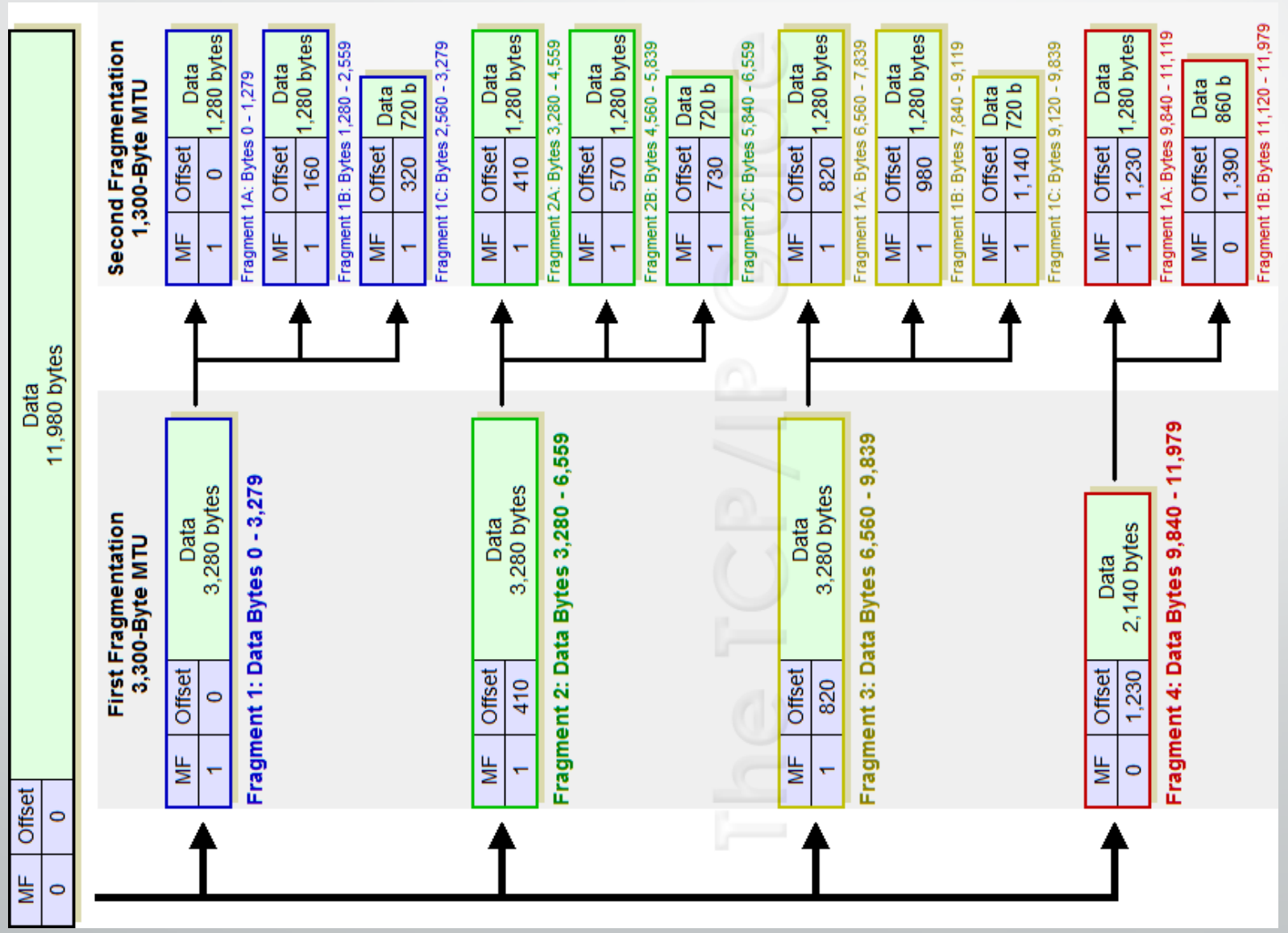
Original IP Datagram

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	Data Bytes	Fragment Offset
0-0	345	1500	0	1	0	0 -1479	0/8=0
0-1	345	1500	0	1	185	1480-2959	1480/8=185
0-2	345	1500	0	1	370	2960-4439	2960/8=370
0-3	345	700	0	0	555	4440-5119	4440/8=555

IP Fragmentation Example



BRAC UNIVERSITY
Inspiring Excellence

ICMP

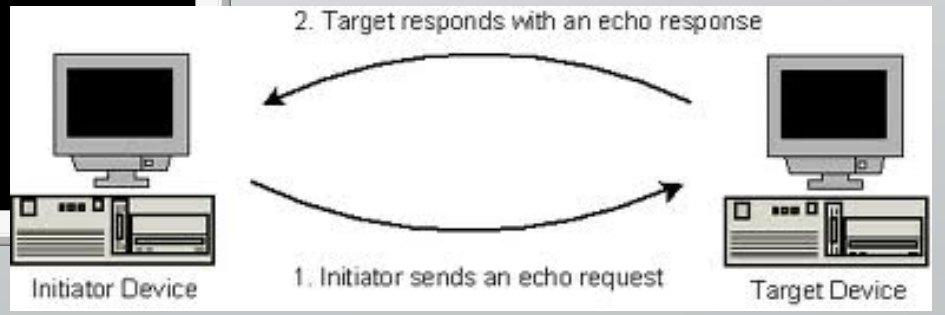
ICMP

- Also known as **Internet Control Message Protocol**
- It is chiefly 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
  - TRACEROUTE

Ping

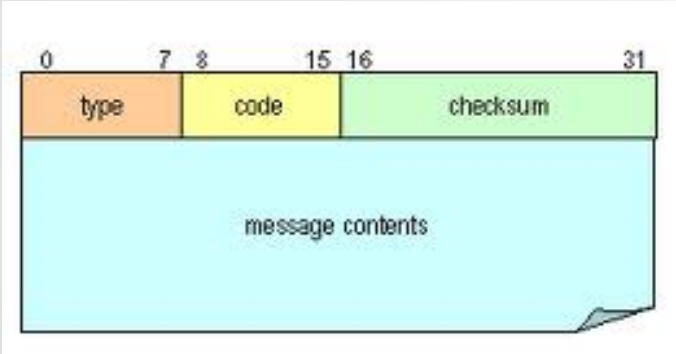
- Utility used to test the reachability of a host.
- Sends Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response.
- In the process it measures the time from transmission to reception (round-trip time) and records any packet loss.

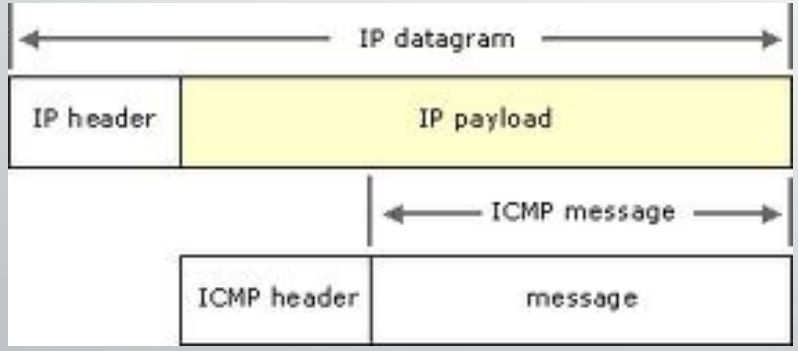
```
C:\Windows\system32\command.com
C:\USERS\LARRYP~1>ping www.pepperdine.edu

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

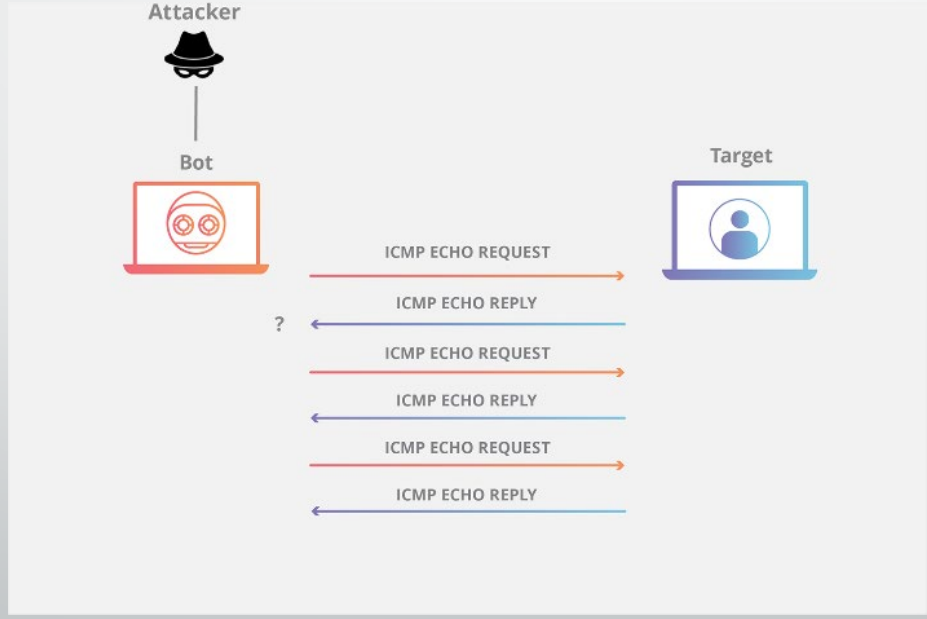




Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement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

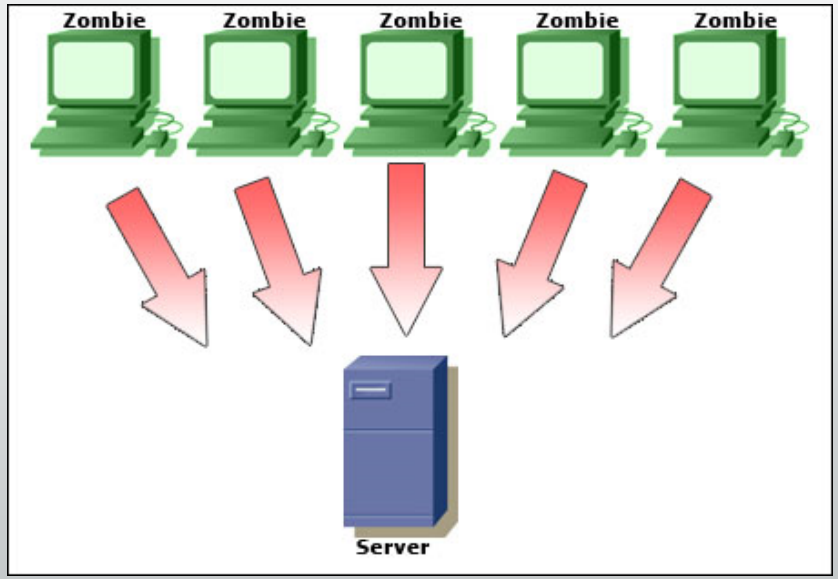
Ping Attacks

- 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.



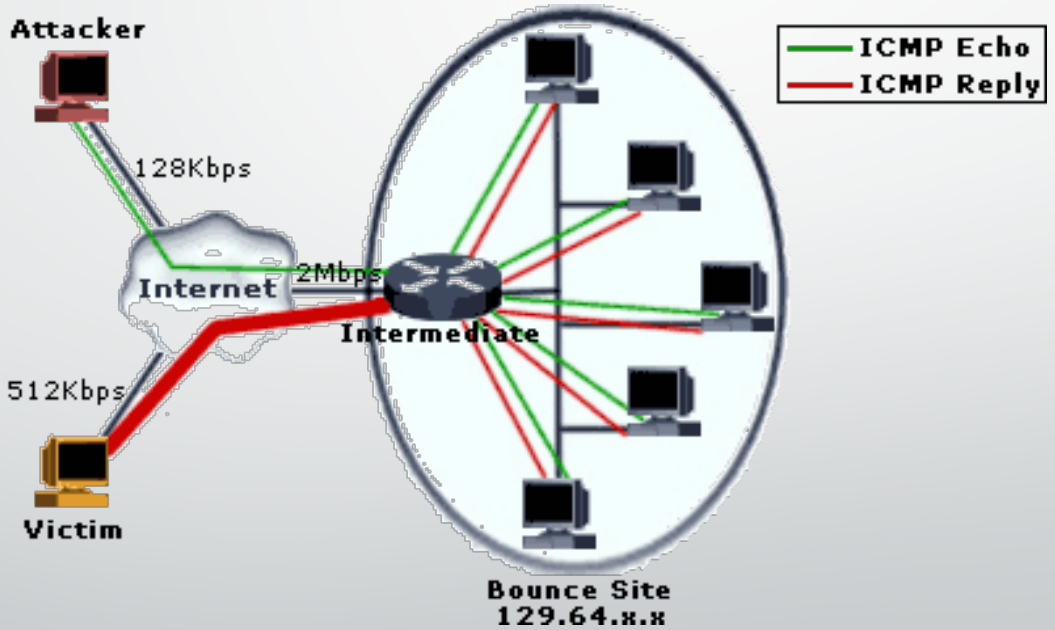
Ping Attacks

- 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 for attack. In this case the victim computers are called zombies.



Ping Attacks

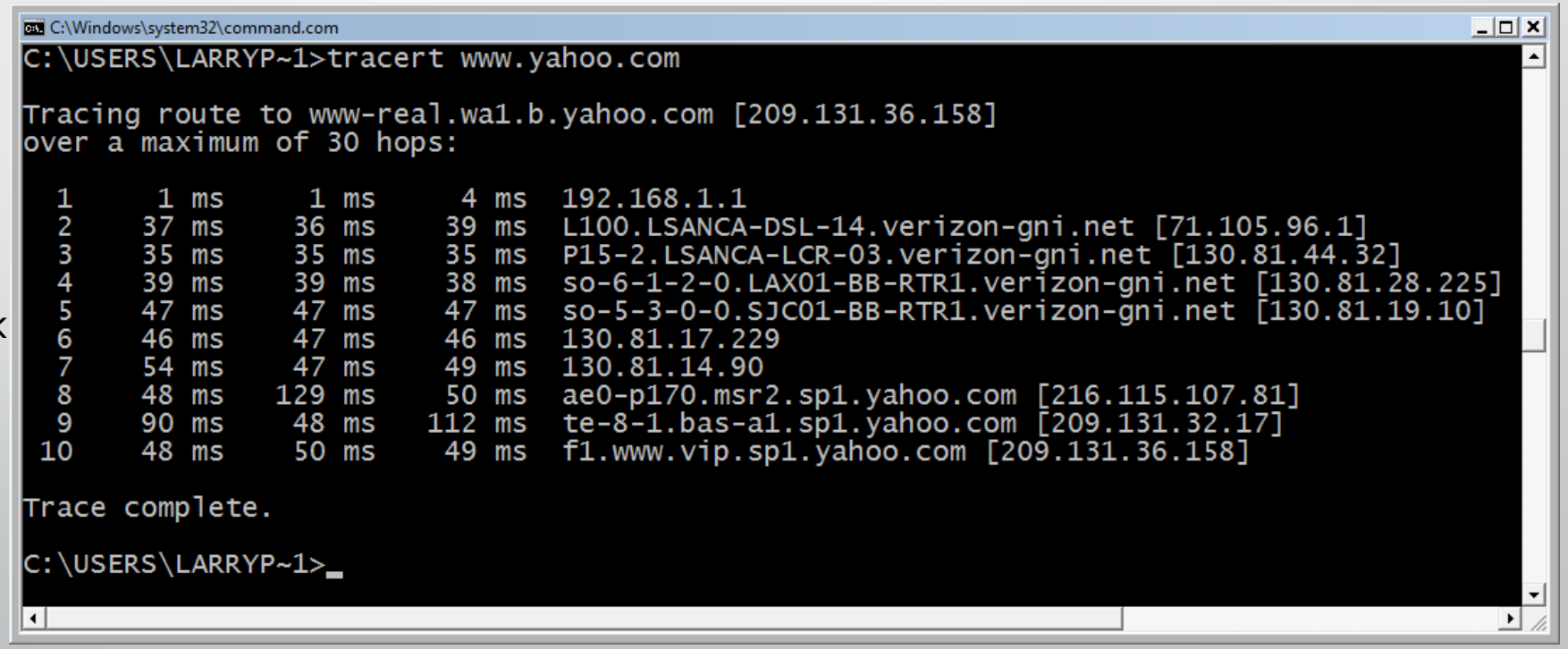
- ICMP DDOS attack – Packet magnification (or ICMP Smurf):
  - An attacker sends forged ICMP echo packets to vulnerable networks' broadcast addresses. All the systems on those networks send ICMP echo replies to the victim.



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 (trace)**
  - DOS: **tracert**

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



Traceroute: Another example

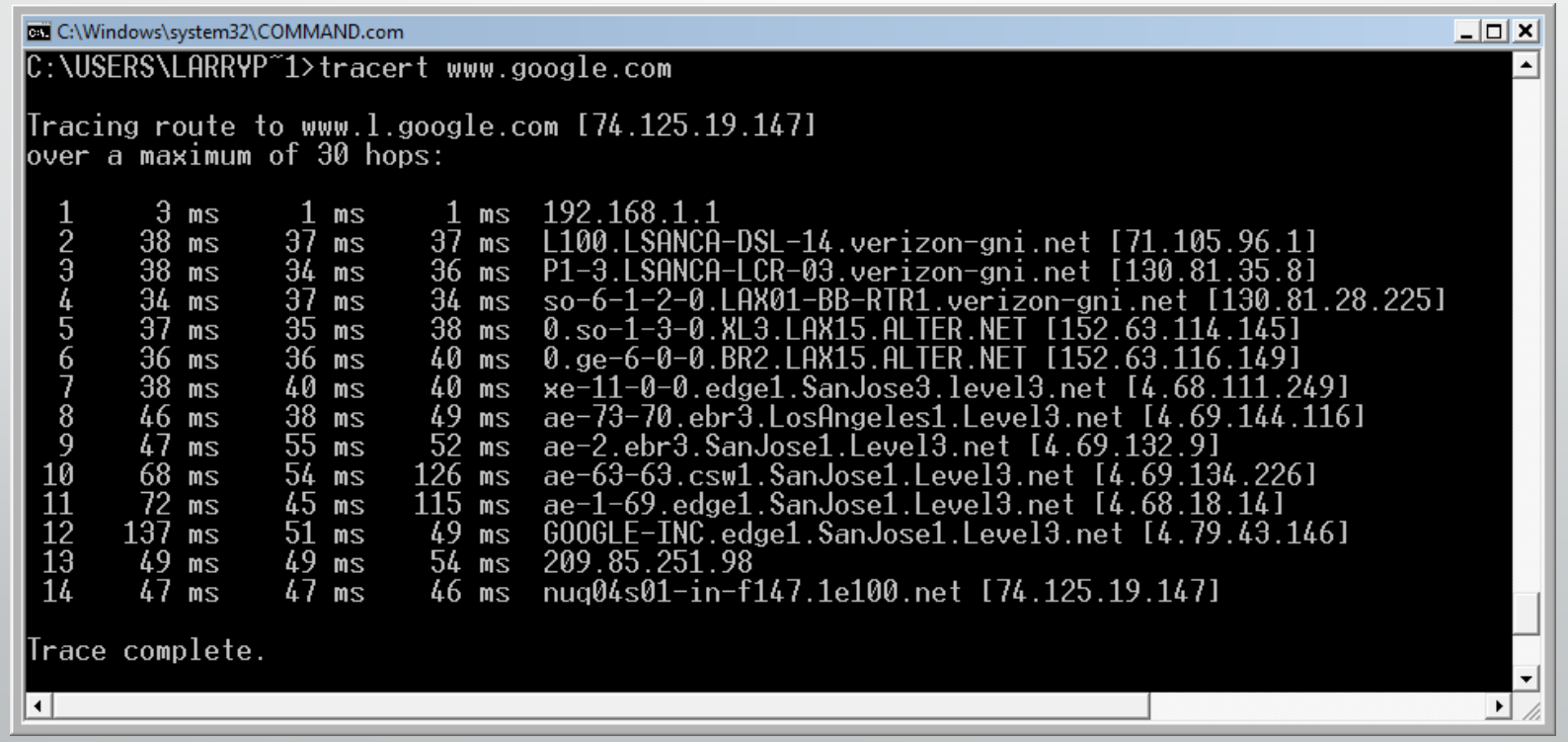
Hop 1: User LAN router

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

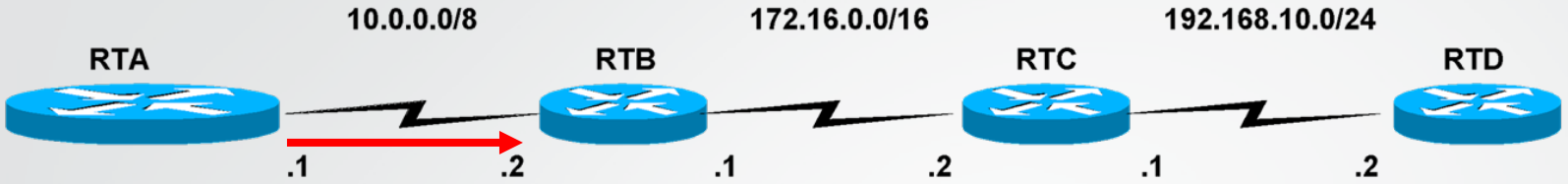
This message indicates that the router security settings keep it from revealing its identity or the router and connection are slow.

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

Traceroute

- Source sends series of UDP segments to dest
  - First has TTL =1
  - Second has TTL=2, etc.
  - Unlikely port number
- When nth datagram arrives to nth router:
  - Router discards datagram
  - And sends to source an ICMP message (type 11, code 0)
  - Message includes name of router& IP address
- When ICMP message arrives, source calculates RTT
- Traceroute does this 3 times
- **Stopping criterion**
  - UDP segment eventually arrives at destination host
  - Destination returns ICMP "port unreachable" packet (type 3, code 3)
    - When source gets this ICMP, it stops.

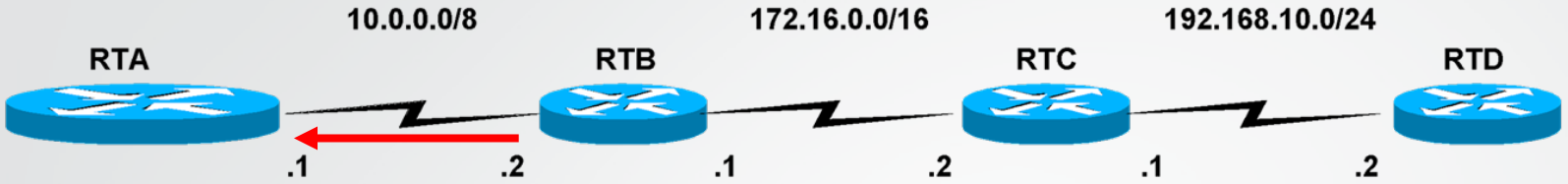
Traceroute



Layer 2 Header	Layer 3 Header	ICMP Message Echo Request (trace)		Layer 4 Header (UDP)	Layer 2 Trailer
*All layer 2 info	**Src. IP:** 10.0.0.1 **Dest. IP:** 192.168.10.2 **TTL =** 1	**Type:** 8 **Code:** 0	Other fields of ICMP Packet	**Dest. Port:** 35,000	FCS

- **How it works by fooling the routers & host!**
  - Trace uses ping (echo requests)
  - Traceroute sets the TTL (Time to Live) field, in the Layer 3 (IP) header, initially to "1".

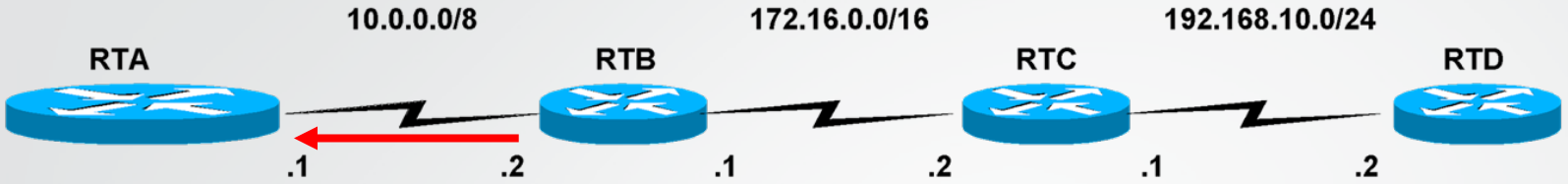
Traceroute



Layer 2 Header	Layer 3 Header	ICMP Message (Time Exceeded)		Layer 4 Header (UDP)	Layer 2 Trailer
*All layer 2 info	**Src. IP:** 10.0.0.2 **Dest. IP:** 10.0.0.1	**Type: 11** **Code:** 0	Other fields of ICMP Packet	-	FCS

- **RTB -** TTL:
  - When a router receives an IP Packet, it **decrements** the **TTL by 1**.
    - TTL '1' is decremented to '0'
  - If the TTL is 0, it will not forward the IP Packet, and send back to the source with an **ICMP "time exceeded"** message.

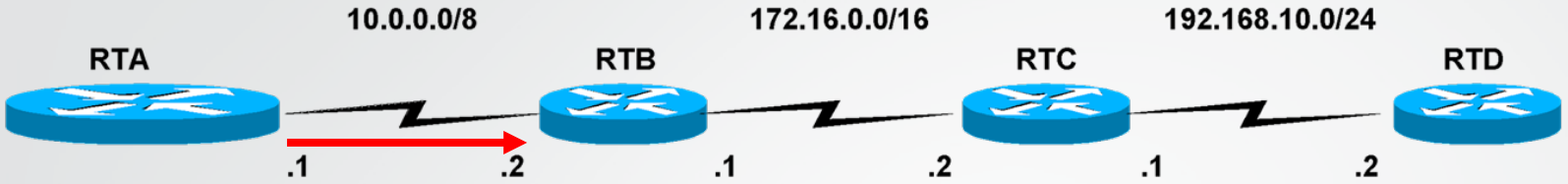
Traceroute



Layer 2 Header	Layer 3 Header	ICMP Message (Time Exceeded)		Layer 4 Header (UDP)	Layer 2 Trailer
*All layer 2 info	**Src. IP:** 10.0.0.2 **Dest. IP:** 10.0.0.1	**Type: 11** **Code:** 0	Other fields of ICMP Packet	-	FCS

- **RTA at this point**
  - The traceroute program of the sending host (RTA) will **use the source IP address** of this ICMP Time Exceeded packet to display the following at the first hop.
- **Output of RTA:** 1 10.0.0.2 4 msec 4 msec 4 msec

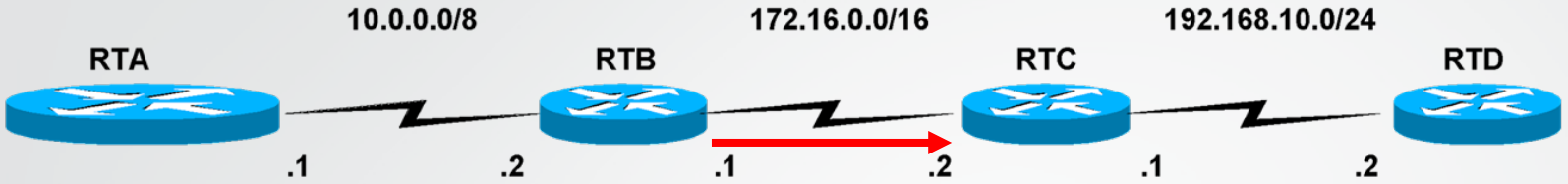
Traceroute



Layer 2 Header	Layer 3 Header	ICMP Message Echo Request (trace)		Layer 4 Header (UDP)	Layer 2 Trailer
*All layer 2 info	**Src. IP:** 10.0.0.1 **Dest. IP:** 192.168.10.2 **TTL = 2**	**Type:** 8 **Code:** 0	Other fields of ICMP Packet	**Dest. Port:** 35,000	FCS

- **RTA**
  - The traceroute program **increments the TTL by 1** (now 2) and **resends** the ICMP Echo Request packet.

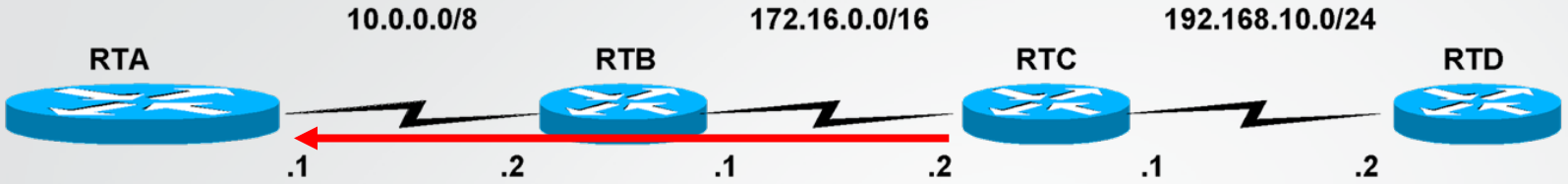
Traceroute



Layer 2 Header	Layer 3 Header	ICMP Message Echo Request (trace)		Layer 4 Header (UDP)	Layer 2 Trailer
*All layer 2 info	**Src. IP:** 10.0.0.1 **Dest. IP:** 192.168.10.2 **TTL = 1**	**Type:** 8 **Code:** 0	Other fields of ICMP Packet	**Dest. Port:** 35,000	FCS

- This time RTB **decrements** the TTL by 1 and it is **NOT** 0. (It is 1.)
- So it **looks up the destination IP** address in its routing table and forwards it on to the next router.

Traceroute

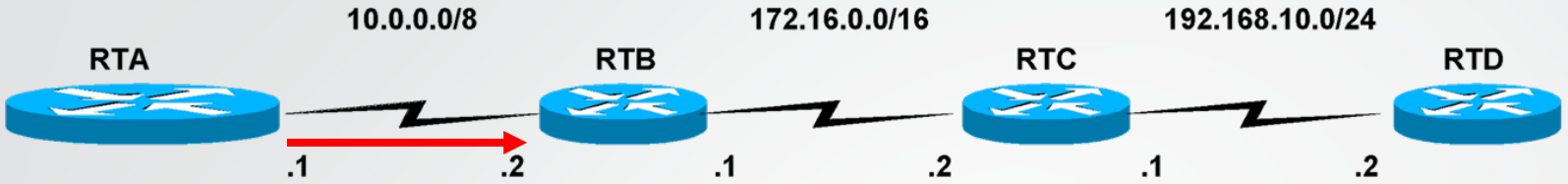


Layer 2 Header	Layer 3 Header	ICMP Message (Time Exceeded)		Layer 4 Header (UDP)	Layer 2 Trailer
*All layer 2 info	**Src. IP:** 172.16.0.2 **Dest. IP:** 10.0.0.1	**Type: 11** **Code:** 0	Other fields of ICMP Packet	-	FCS

- RTC **decrements** the TTL by 1 and it is 0.
  - RTC notices the TTL is 0 and **sends back the ICMP** Time Exceeded message back to the source.
  - RTC's IP header **includes its own IP** address (source IP) and the sending host's IP address (destination IP address of RTA).
  - The sending host, RTA, will use the source IP address of this ICMP Time Exceeded message to display at the second hop.

```
1 10.0.0.2 4 msec 4 msec 4 msec
2 172.16.0.2 20 msec 16 msec 16 msec
```

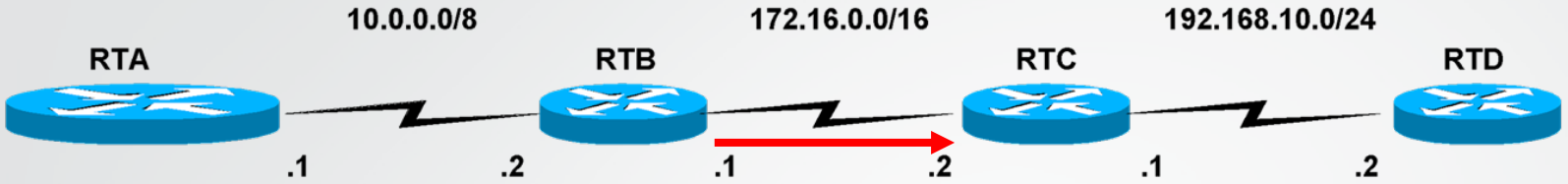
Traceroute



Layer 2 Header	Layer 3 Header	ICMP Message Echo Request (trace)		Layer 4 Header (UDP)	Layer 2 Trailer
*All layer 2 info	**Src. IP:** 10.0.0.1 **Dest. IP:** 192.168.10.2 **TTL = 3**	**Type:** 8 **Code:** 0	Other fields of ICMP Packet	**Dest. Port:** 35,000	FCS

- The sending host, RTA:
  - The traceroute program **increments** the TTL by 1 (now 3) and resends the Packet.

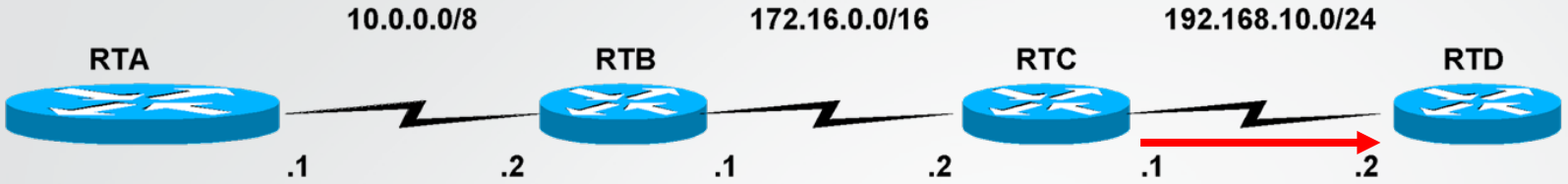
Traceroute



Layer 2 Header	Layer 3 Header	ICMP Message Echo Request (trace)		Layer 4 Header (UDP)	Layer 2 Trailer
*All layer 2 info	**Src. IP:** 10.0.0.1 **Dest. IP:** 192.168.10.2 **TTL = 2**	**Type:** 8 **Code:** 0	Other fields of ICMP Packet	**Dest. Port:** 35,000	FCS

- RTB
  - This time RTB **decrements** the TTL by 1 and it is NOT 0. (It is 2.)
  - So it looks up the destination IP address in its routing table and forwards it on to the next router.

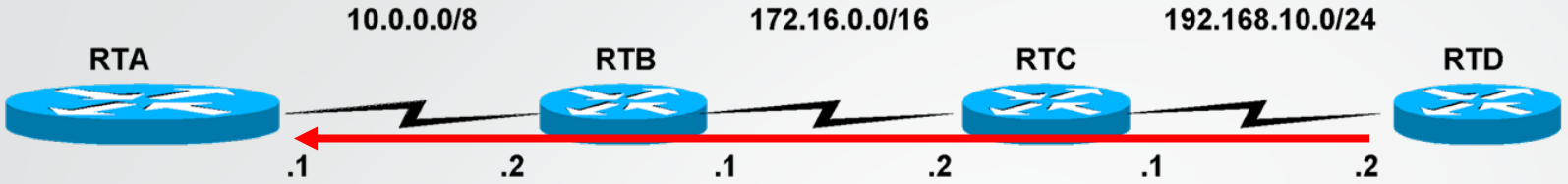
Traceroute



Layer 2 Header	Layer 3 Header	ICMP Message Echo Request (trace)		Layer 4 Header (UDP)	Layer 2 Trailer
*All layer 2 info	**Src. IP:** 10.0.0.1 **Dest. IP:** 192.168.10.2 **TTL = 1**	**Type:** 8 **Code:** 0	Other fields of ICMP Packet	**Dest. Port:** 35,000	FCS

- RTC
  - This time RTC **decrements** the TTL by 1 and it is NOT 0. (It is 1.)
  - So it looks up the destination IP address in its routing table and forwards it on to the next router.

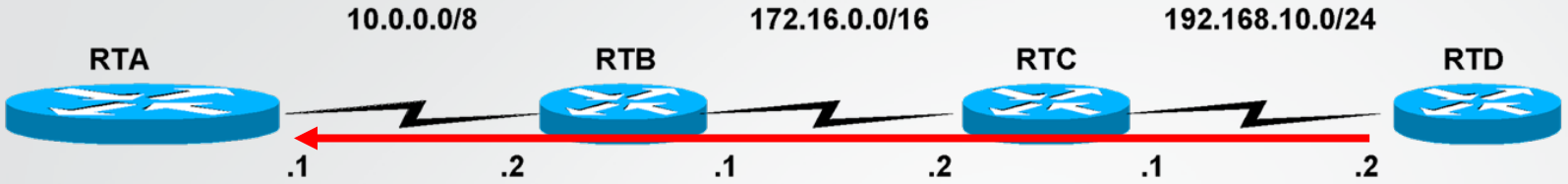
Traceroute



Layer 2 Header	Layer 3 Header	ICMP Message (Port Unreachable)		Layer 4 Header (UDP)	Layer 2 Trailer
*All layer 2 info	**Src. IP:** 192.168.10.2 **Dest. IP:** 10.0.0.1	**Type: 3 Code: 3**	Other fields of ICMP Packet	-	FCS

- RTD decrements the TTL by 1 and it is 0.
- However, RTD notices that the Destination IP Address of 192.168.0.2 is it's own interface.
- Since it does not need to forward the packet, the TTL of 0 has no affect.
- RTD sends the packet to the UDP process.
- UDP examines the unrecognizable port number of 35,000 and sends back an ICMP Port Unreachable message to the sender, RTA, using Type 3 and Code 3.

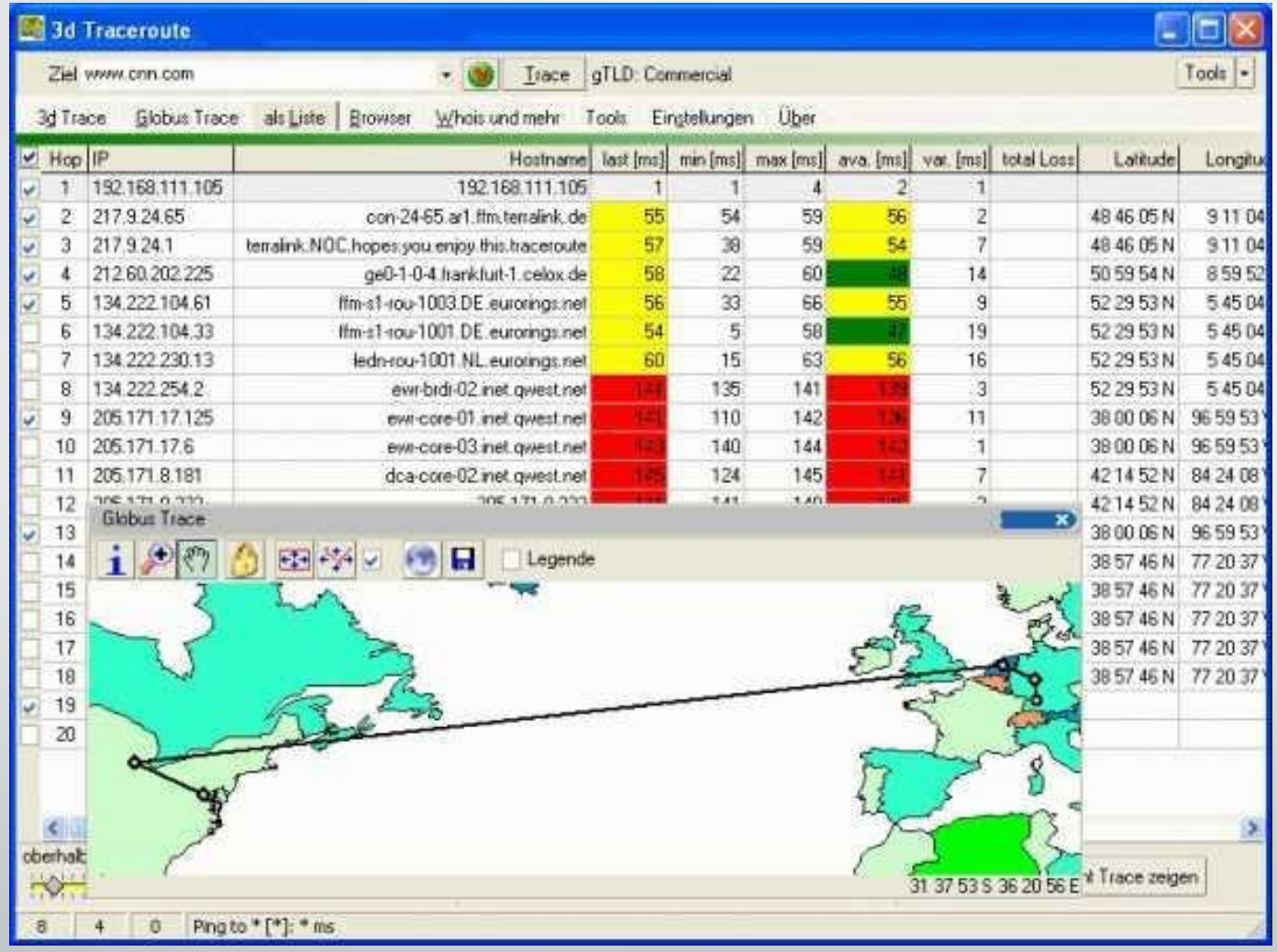
Traceroute



Layer 2 Header	Layer 3 Header	ICMP Message (Port Unreachable)		Layer 4 Header (UDP)	Layer 2 Trailer
*All layer 2 info	**Src. IP:** 192.168.10.2 **Dest. IP:** 10.0.0.1	**Type: 3 Code: 3**	Other fields of ICMP Packet	-	FCS

- Sending host, RTA
  - RTA **receives the ICMP Port Unreachable** message.
  - The traceroute program uses this information (Source IP Address) and displays the third hop.
  - The traceroute program also **recognizes** this Port Unreachable message as **meaning this is the destination it was tracing.**

3D Traceroute



BRAC UNIVERSITY
Inspiring Excellence

The End