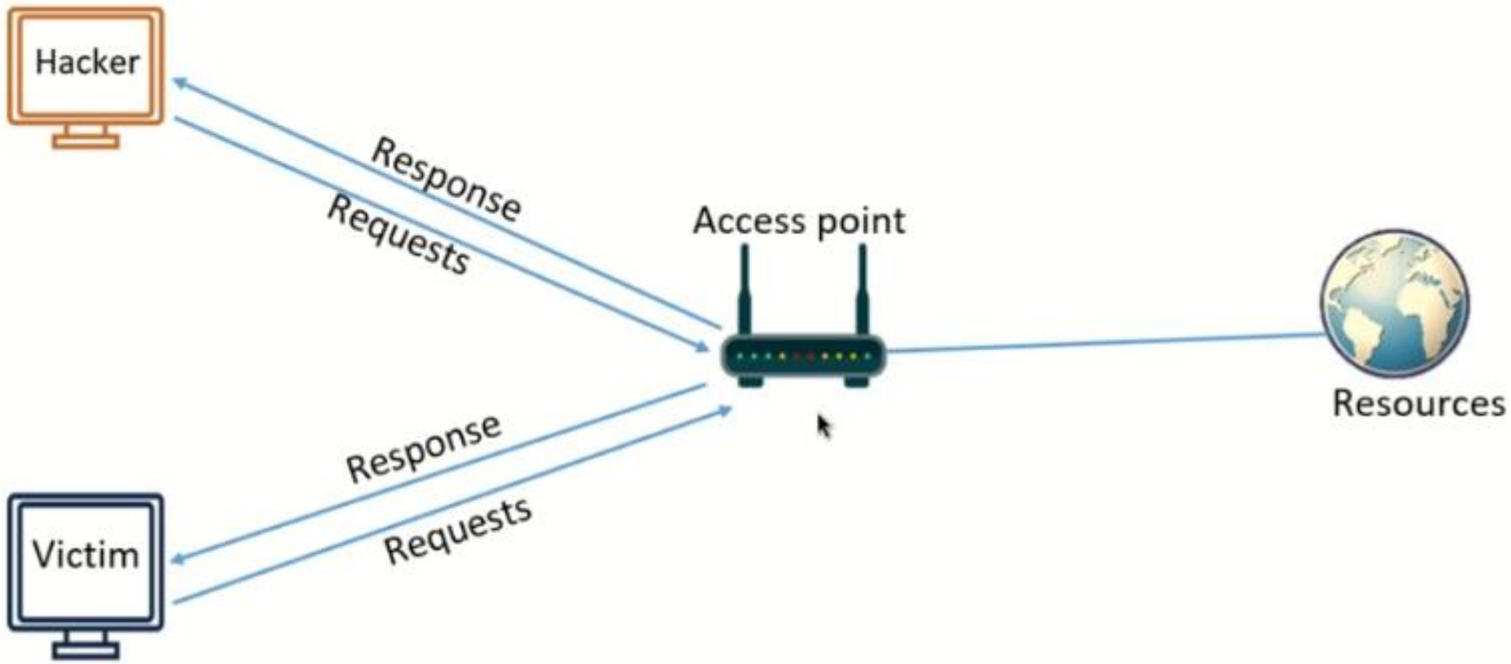
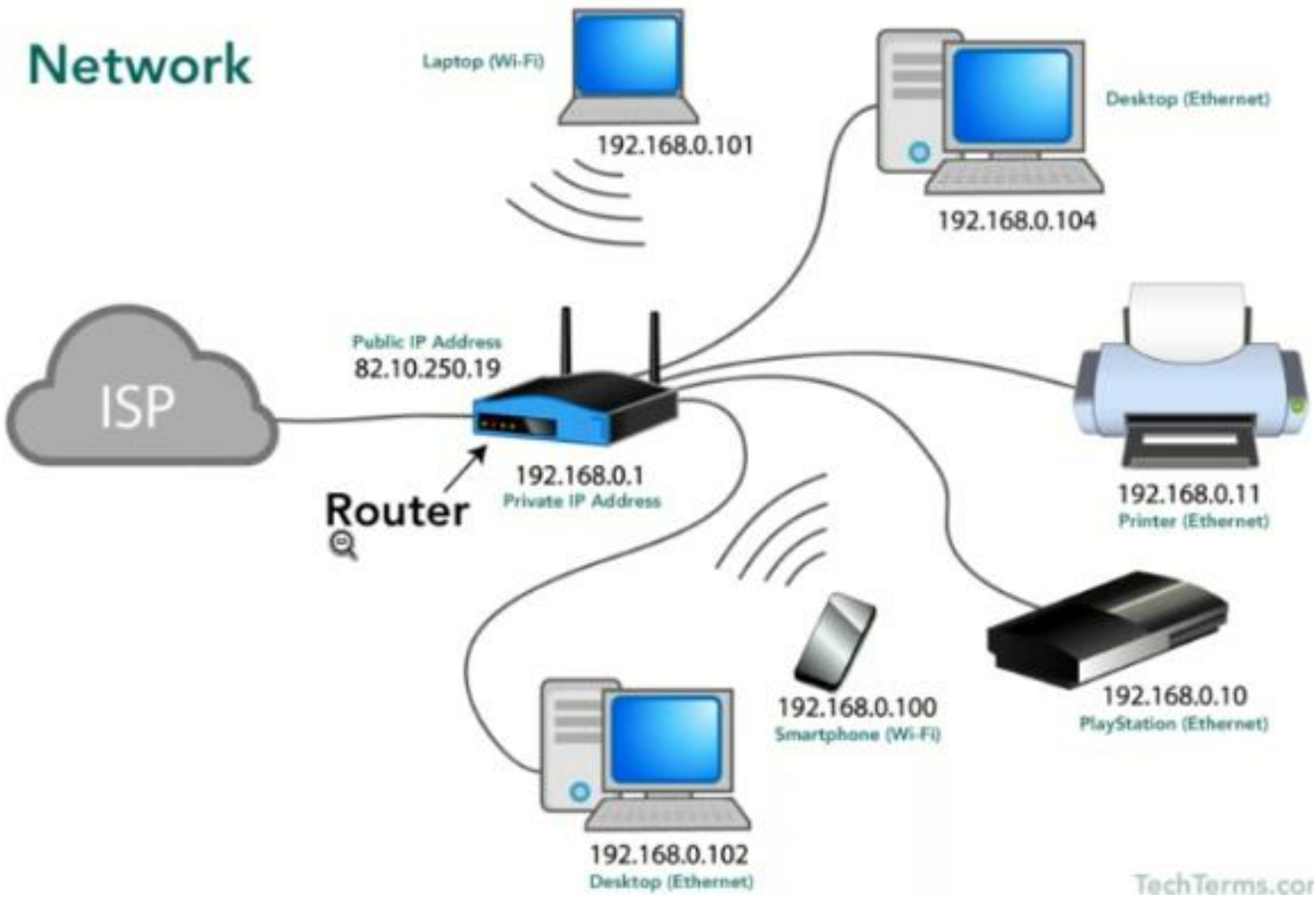
Networking Basic

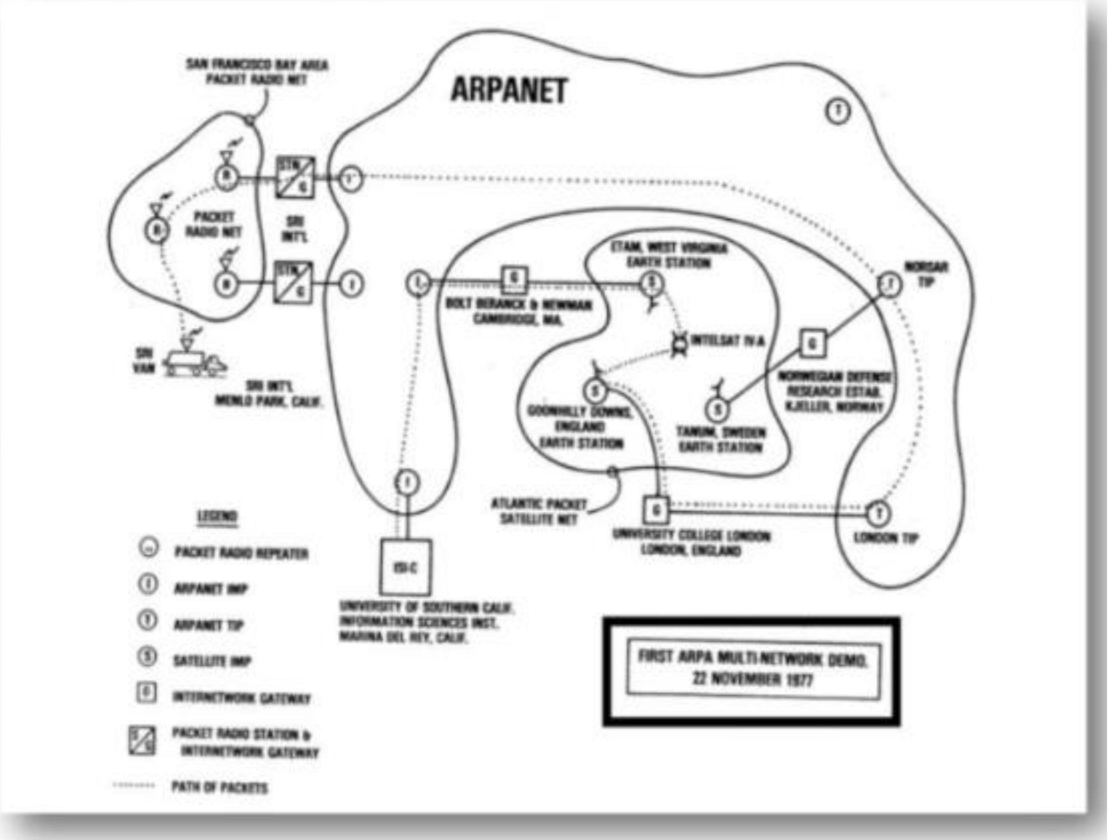

Hacker
Response
Requests
Access point
Resources
Response
Requests
Victim

Network


Laptop (Wi-Fi)
192.168.0.101
Desktop (Ethernet)
192.168.0.104
ISP
Public IP Address
82.10.250.19
192.168.0.1
Private IP Address
Router
192.168.0.11
Printer (Ethernet)
192.168.0.100
Smartphone (Wi-Fi)
192.168.0.10
PlayStation (Ethernet)
192.168.0.102
Desktop (Ethernet)

The Internet

The Internet	- interconnected computer networks. “Network of Networks”
1960s	- The origins of the Internet
ARPANET	- Backbone for interconnection of regional academic and military networks
4.1 Billion	- nearly 55% of the world population use the services of the Internet


ARPANET
SAN FRANCISCO BAY AREA PACKET RADIO NET
PACKET RADIO NET
SRI INT'L
STN
G
R
T
I
L
S
SRI VAN
SRI INT'L MENLO PARK, CALIF.
BOLT BERANEK & NEWMAN CAMBRIDGE, MA.
ETAM, WEST VIRGINIA EARTH STATION
INTELSAT IV-A
NORSAR TIP
NORWEGIAN DEFENSE RESEARCH ESTAB. KJELLER, NORWAY
GOONHILLY DOWNS, ENGLAND EARTH STATION
TANUM, SWEDEN EARTH STATION
ATLANTIC PACKET SATELLITE NET
UNIVERSITY COLLEGE LONDON LONDON, ENGLAND
LONDON TIP
ISI-C
UNIVERSITY OF SOUTHERN CALIF. INFORMATION SCIENCES INST. MARINA DEL REY, CALIF.
LEGEND
PACKET RADIO REPEATER
ARPANET IMP
ARPANET TIP
SATELLITE IMP
INTERNETWORK GATEWAY
PACKET RADIO STATION & INTERNETWORK GATEWAY
PATH OF PACKETS
FIRST ARPA MULTI-NETWORK DEMO, 22 NOVEMBER 1977

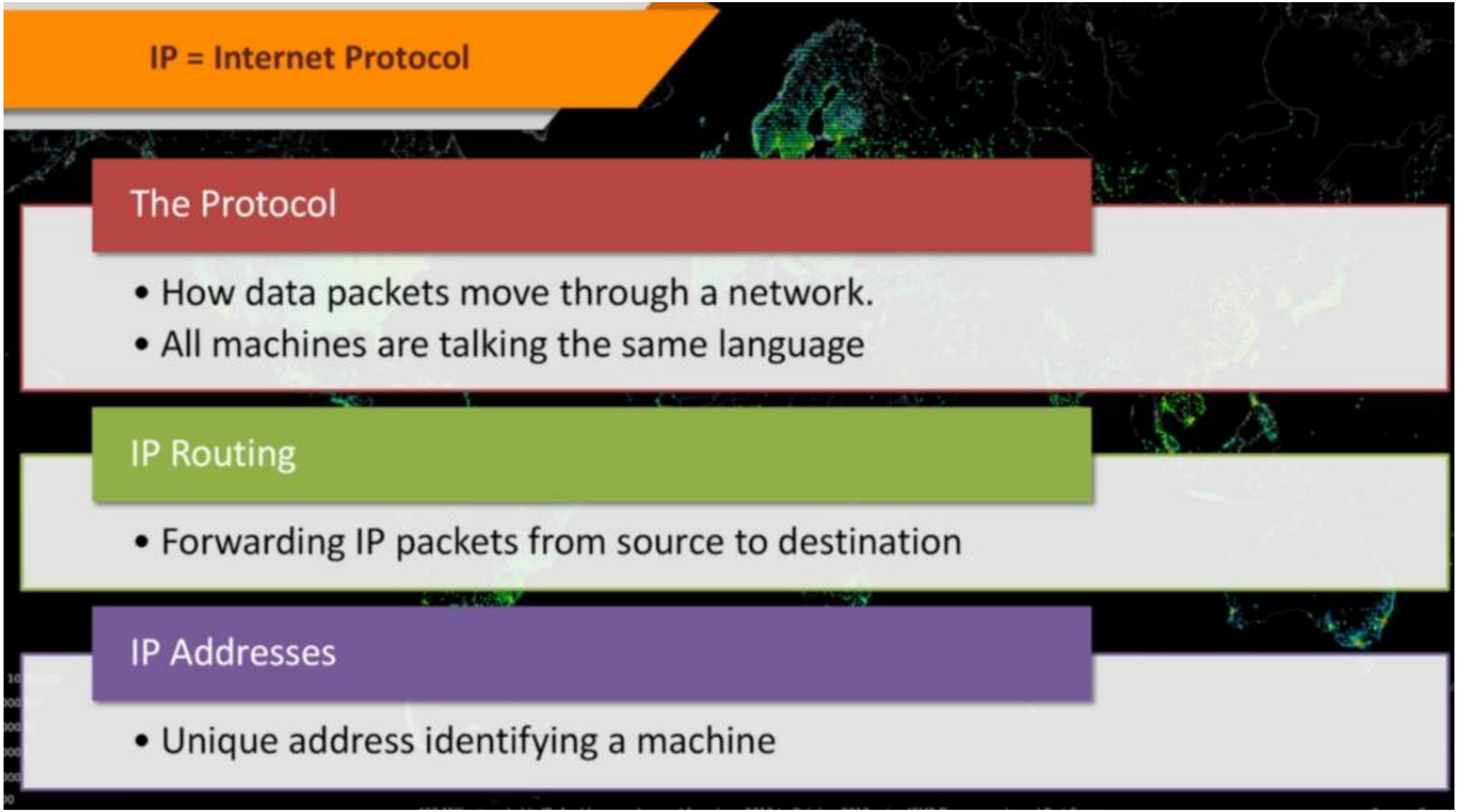
Communication Protocol

Set of rules

Standardisation

Right PC, right program

Protocols are to computers what language is to humans.



IP = Internet Protocol

The Protocol

- How data packets move through a network.
- All machines are talking the same language

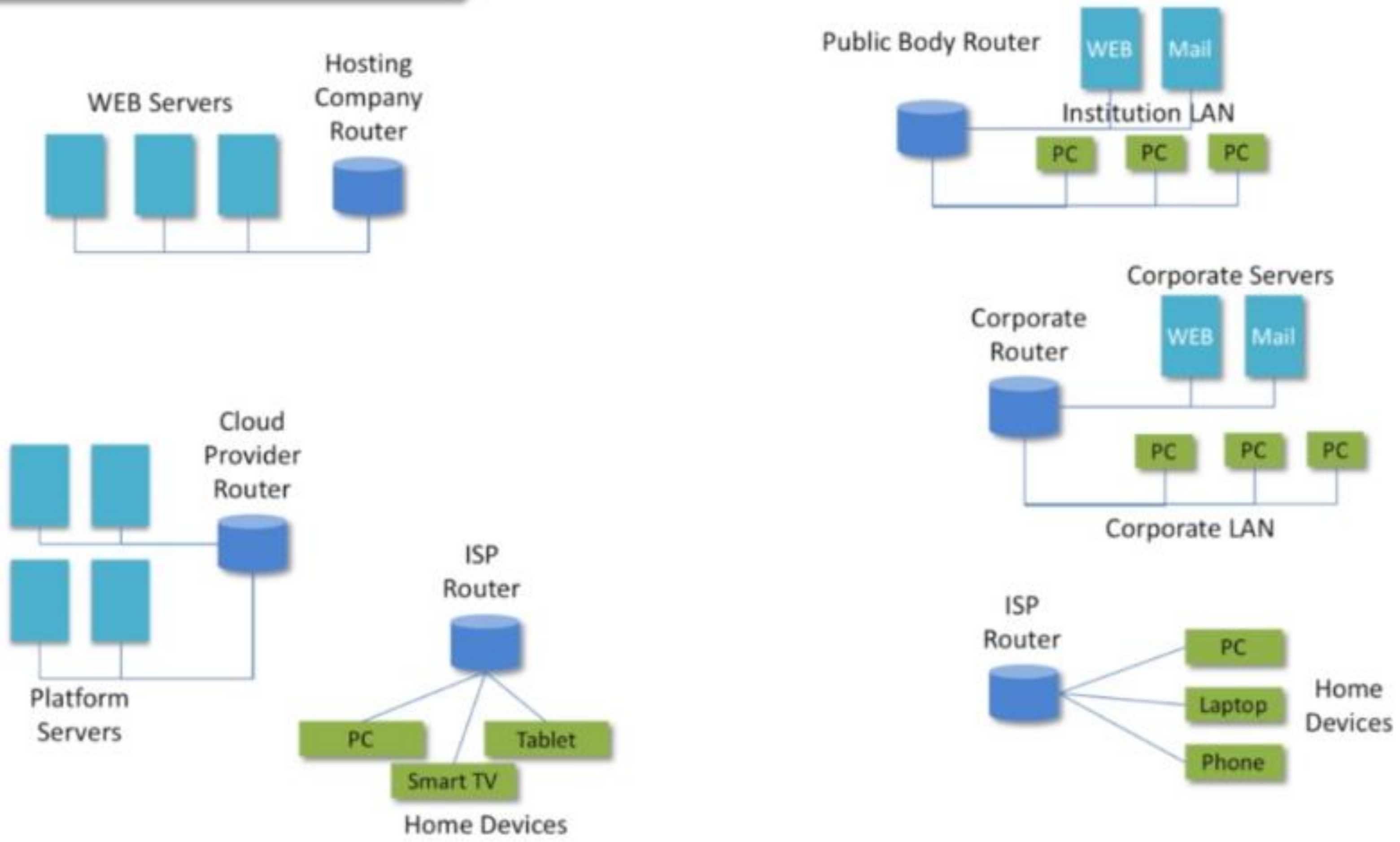
IP Routing

- Forwarding IP packets from source to destination

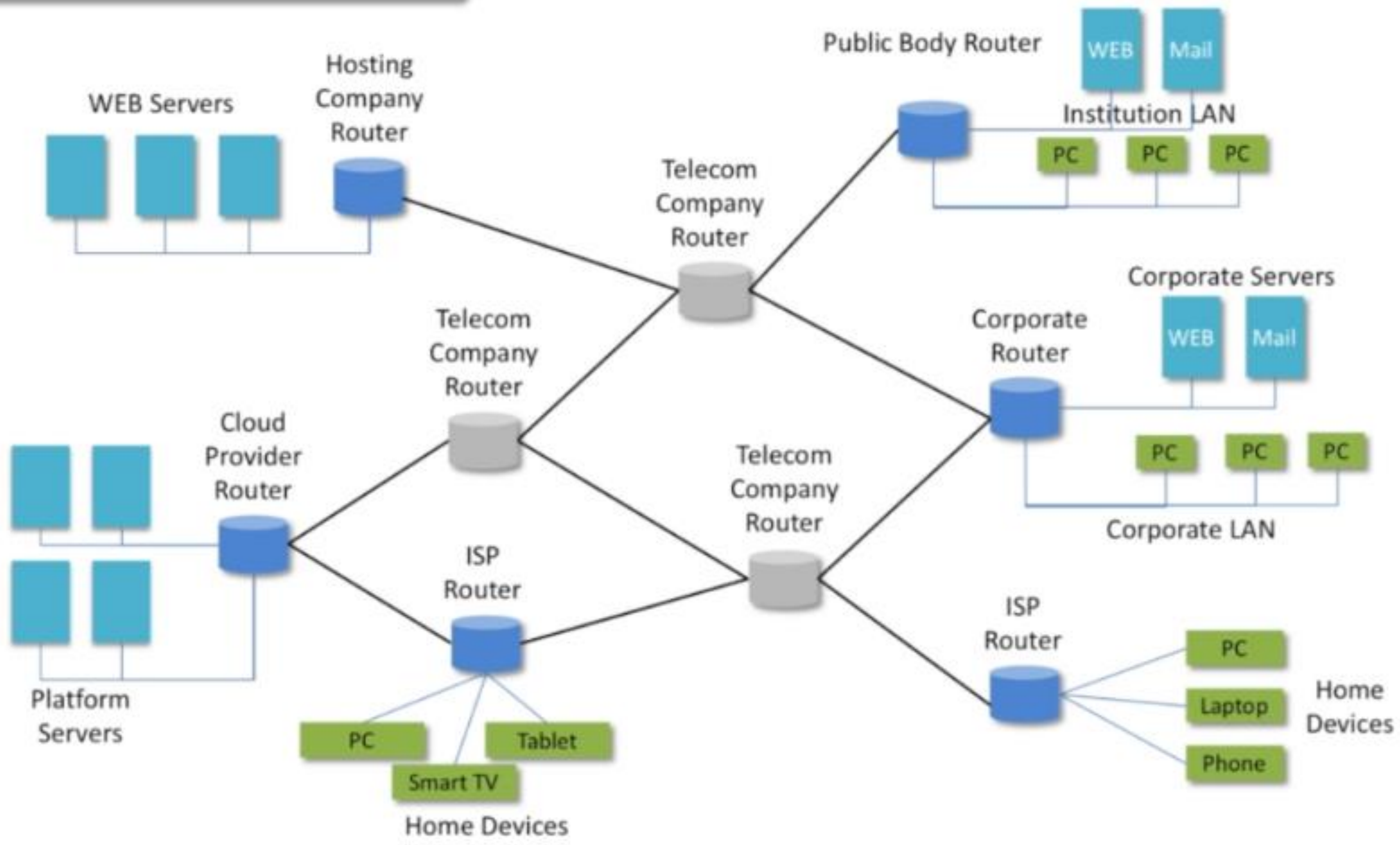
IP Addresses

- Unique address identifying a machine

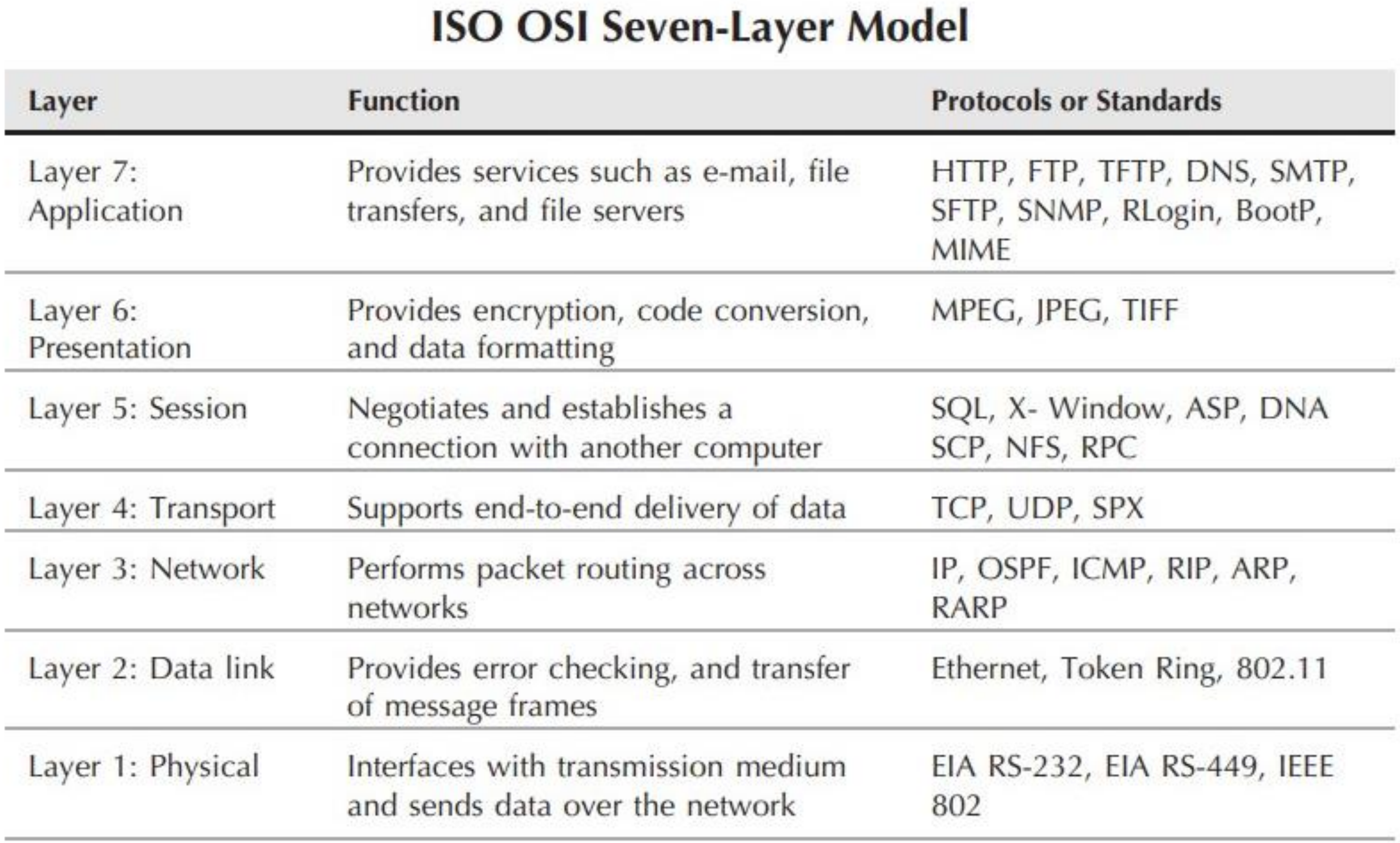
User, Companies and the Internet



User, Companies and the Internet



The Open Systems Interconnect Model

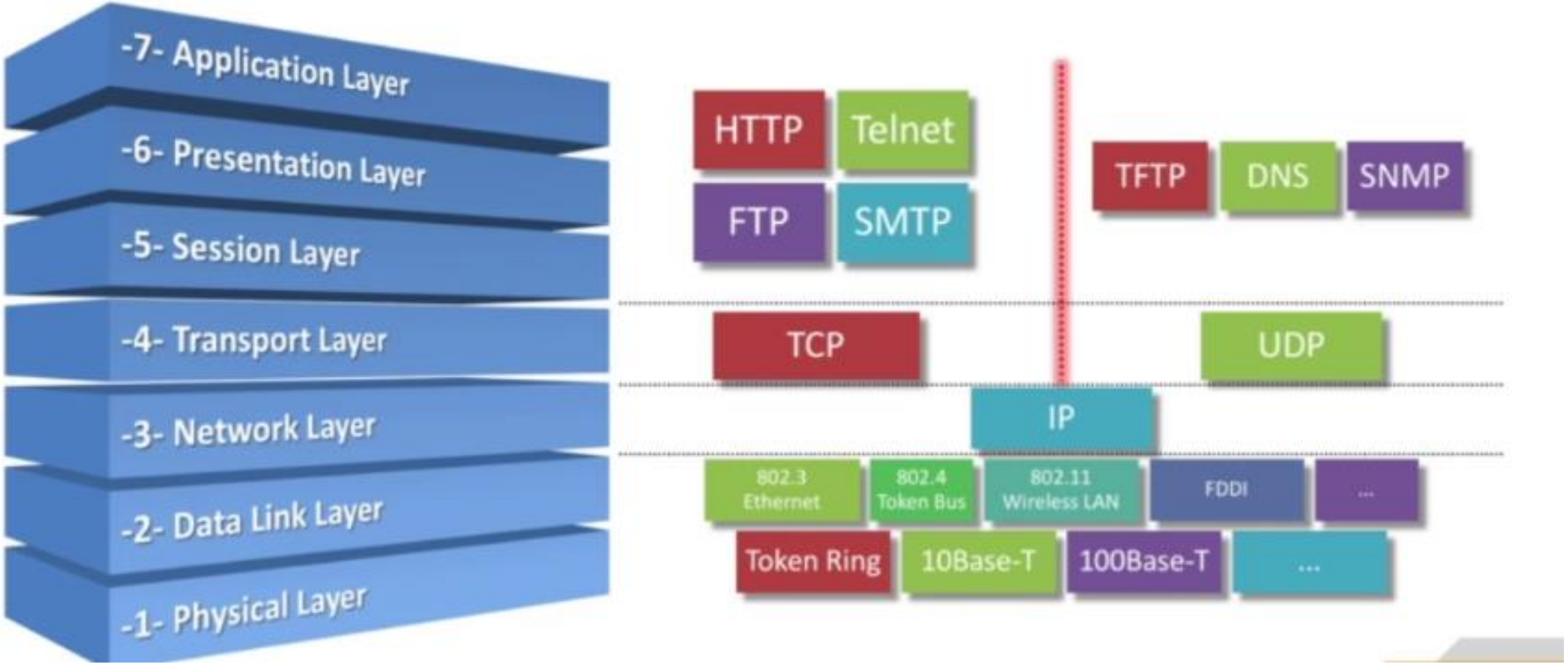


ISO OSI Seven-Layer Model

Layer	Function	Protocols or Standards
Layer 7: Application	Provides services such as e-mail, file transfers, and file servers	HTTP, FTP, TFTP, DNS, SMTP, SFTP, SNMP, RLogin, BootP, MIME
Layer 6: Presentation	Provides encryption, code conversion, and data formatting	MPEG, JPEG, TIFF
Layer 5: Session	Negotiates and establishes a connection with another computer	SQL, X- Window, ASP, DNA SCP, NFS, RPC
Layer 4: Transport	Supports end-to-end delivery of data	TCP, UDP, SPX
Layer 3: Network	Performs packet routing across networks	IP, OSPF, ICMP, RIP, ARP, RARP
Layer 2: Data link	Provides error checking, and transfer of message frames	Ethernet, Token Ring, 802.11
Layer 1: Physical	Interfaces with transmission medium and sends data over the network	EIA RS-232, EIA RS-449, IEEE 802

TCP/IP Basics

Layers and Protocols



-7- Application Layer

-6- Presentation Layer

-5- Session Layer

-4- Transport Layer

-3- Network Layer

-2- Data Link Layer

-1- Physical Layer

HTTP

Telnet

FTP

SMTP

TFTP

DNS

SNMP

TCP

UDP

IP

802.3 Ethernet

802.4 Token Bus

802.11 Wireless LAN

FDDI

...

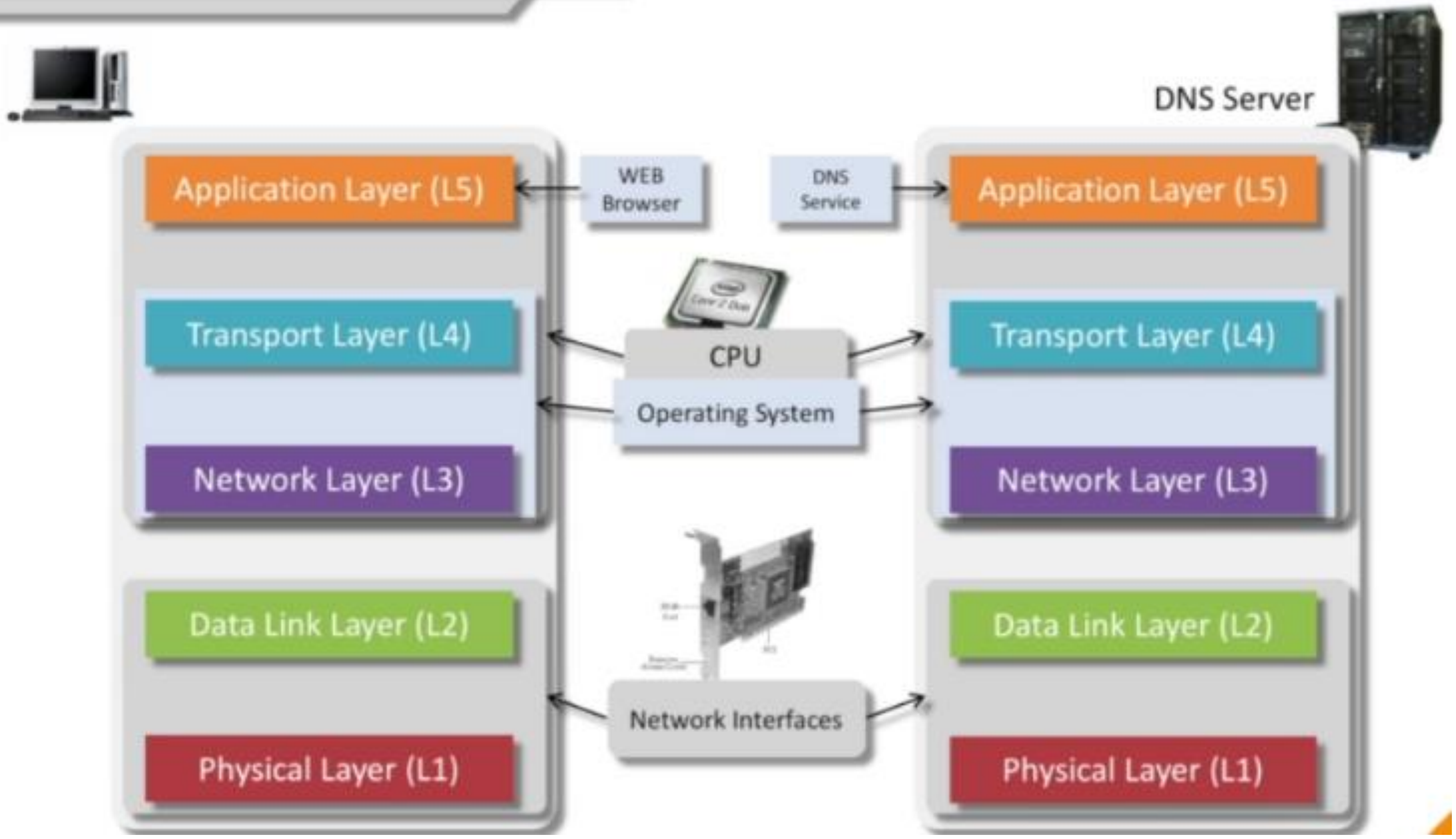
Token Ring

10Base-T

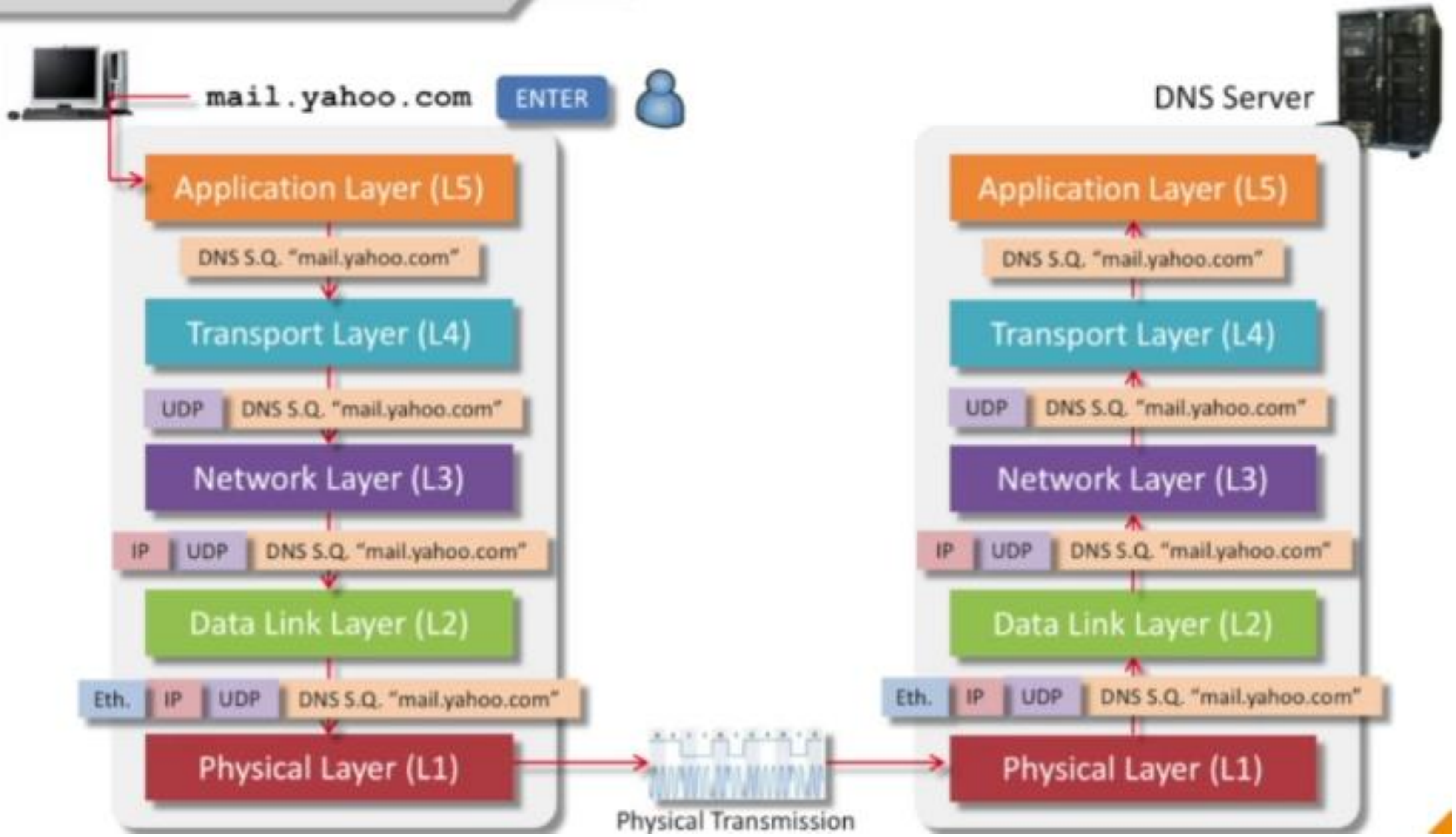
100Base-T

...

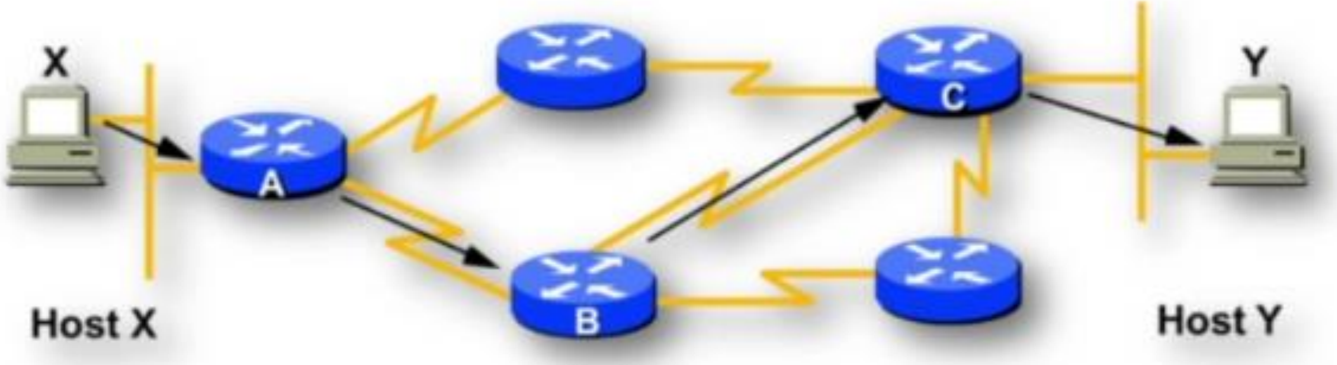
Example: DNS Query

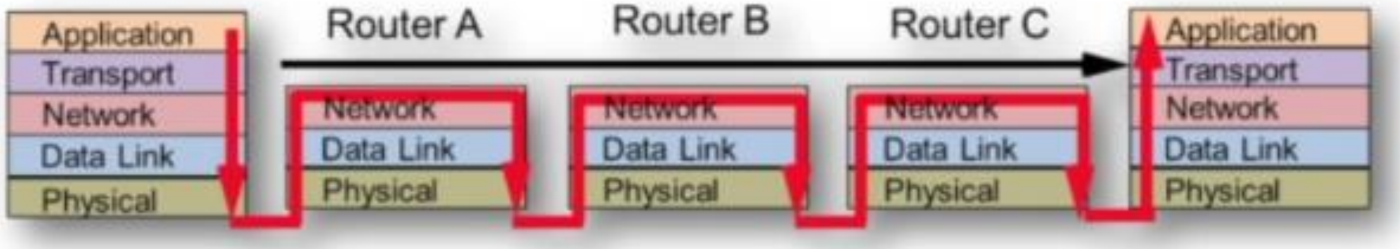


Example: DNS Query

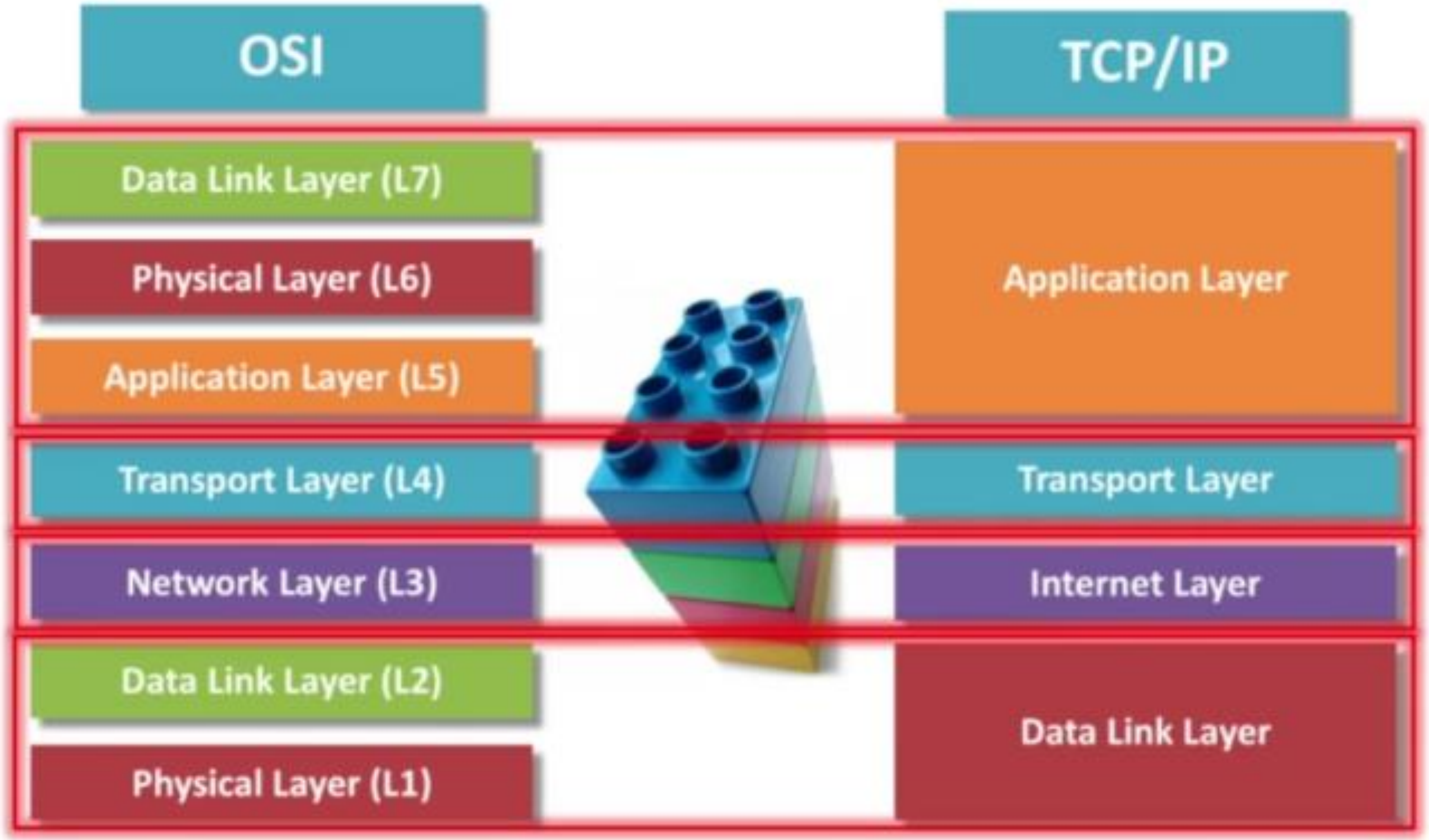


Communication with TCP/IP





Reference Models: OSI vs TCP/IP



OSI	TCP/IP
Data Link Layer (L7)	Application Layer
Physical Layer (L6)	
Application Layer (L5)	
Transport Layer (L4)	Transport Layer
Network Layer (L3)	Internet Layer
Data Link Layer (L2)	Data Link Layer
Physical Layer (L1)	

Every layer needs the service of lower layers to operate.

Layer 2: Data Link Layer

Main responsibility:

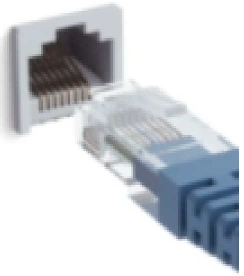
- Encoding bits into packets prior to transmission,
- And decoding the packets back into bits at the destination.

Other responsibilities:

- Logical link control
- Media access control
- Hardware addressing
- Error detection
- Handling and defining physical layer standards

Sub-layers

- Media Access Control (MAC) layer
- Logical Link Control (LLC) layer



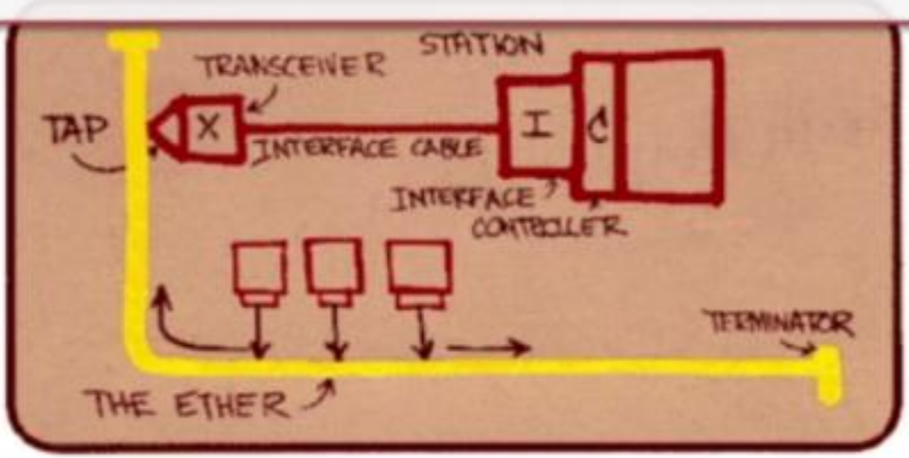
Standards of Data Link Layer

Address Resolution Protocol (**ARP**)	Link Access Procedures, D channel (**LAPD**)
ATM	Multiprotocol Label Switching (**MPLS**)
Cisco Discovery Protocol (**CDP**)	Nortel Discovery Protocol (**NDP**)
Controller Area Network (**CAN**)	Split multi-link trunking (**SMLT**)
Ethernet	Point-to-Point Protocol (**PPP**)
Fiber Distributed Data Interface (**FDDI**)	Serial Line Internet Protocol (**SLIP**) (obsolete)
Frame Relay	**Spanning Tree** Protocol
High-Level Data Link Control (**HDLC**)	**StarLan**
IEEE 802.2 (LLC functions to IEEE 802 MAC)	**Token ring**
IEEE 802.11 wireless LAN	Unidirectional Link Detection (**UDLD**)

Ethernet

Introduction

- Commercially introduced in 1980 and first standardised in 1983 as IEEE 802.3



Picture of the first Ethernet schematic, drawn by its inventor

Ethernet

Introduction

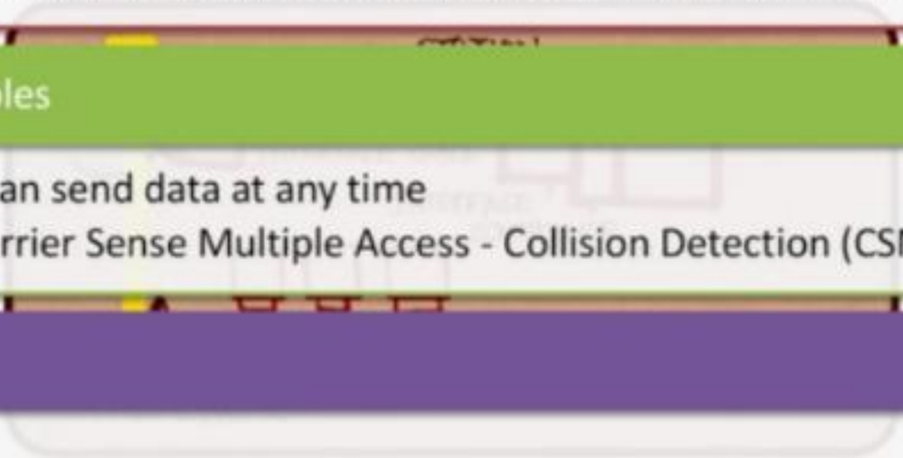
- Commercially introduced in 1980 and first standardised in 1983 as IEEE 802.3

Ethernet Design Principles

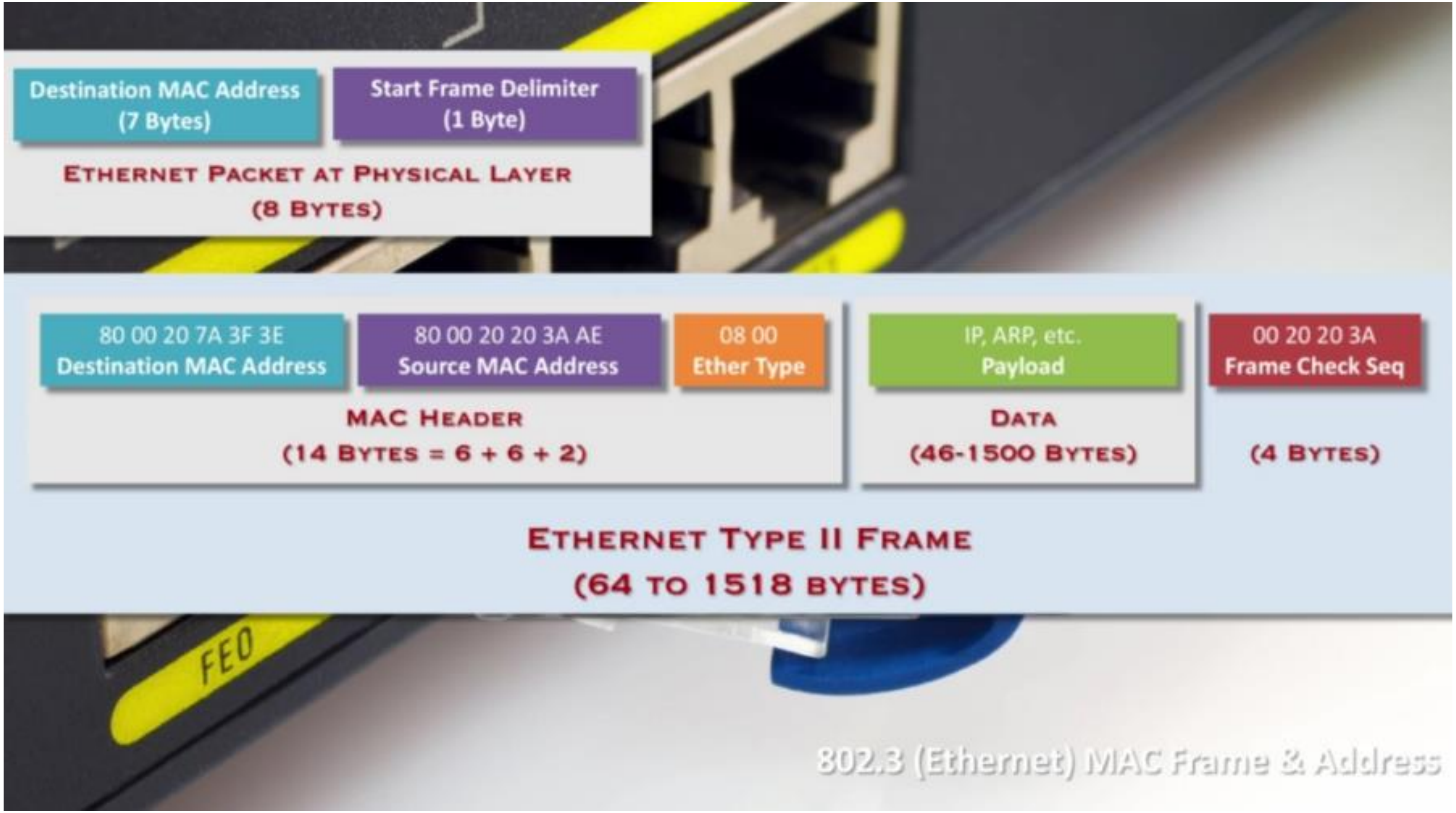
- Multiple computers can send data at any time
- Collision handling: Carrier Sense Multiple Access - Collision Detection (CSMA/CD)

Cable Types

- 10Base2, 10Base5
- 10BaseT, 100BaseT, 1000BaseT
- 10BaseF



Portion of the first Ethernet schematic, drawn by its inventor



Destination MAC Address
(7 Bytes)

Start Frame Delimiter
(1 Byte)

ETHERNET PACKET AT PHYSICAL LAYER
(8 BYTES)

80 00 20 7A 3F 3E
Destination MAC Address

80 00 20 20 3A AE
Source MAC Address

08 00
Ether Type

IP, ARP, etc.
Payload

00 20 20 3A
Frame Check Seq

MAC HEADER
(14 BYTES = 6 + 6 + 2)

DATA
(46-1500 BYTES)

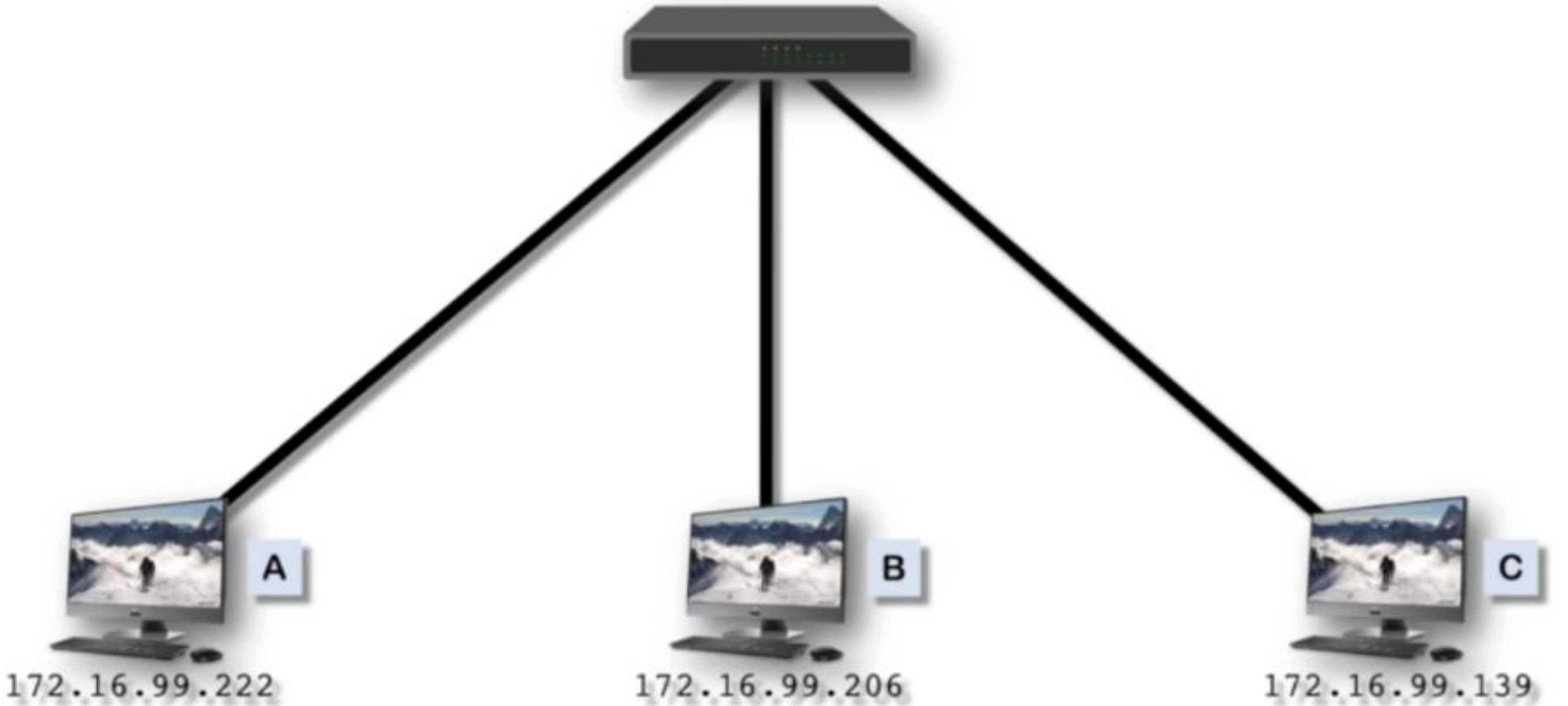
(4 BYTES)

ETHERNET TYPE II FRAME
(64 TO 1518 BYTES)

802.3 (Ethernet) MAC Frame & Address

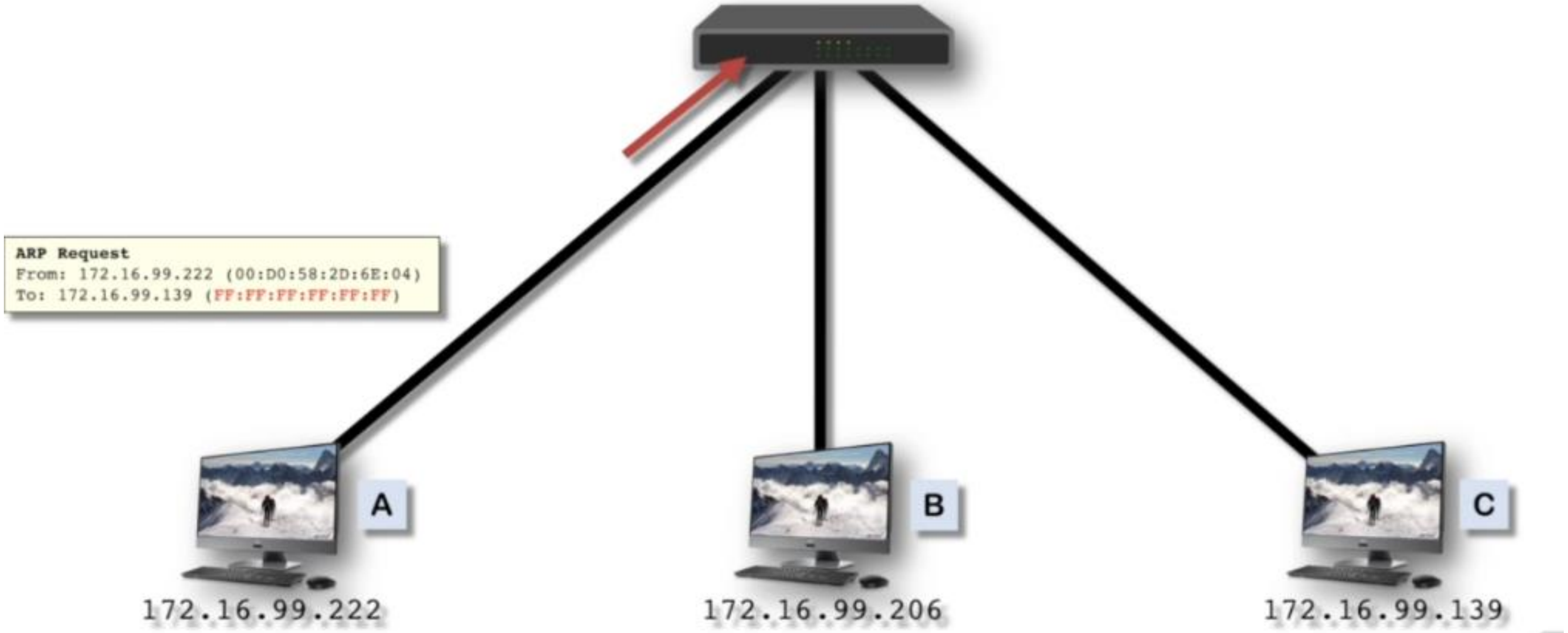
ARP - Address Resolution Protocol

ARP Mechanism



ARP - Address Resolution Protocol

ARP Mechanism

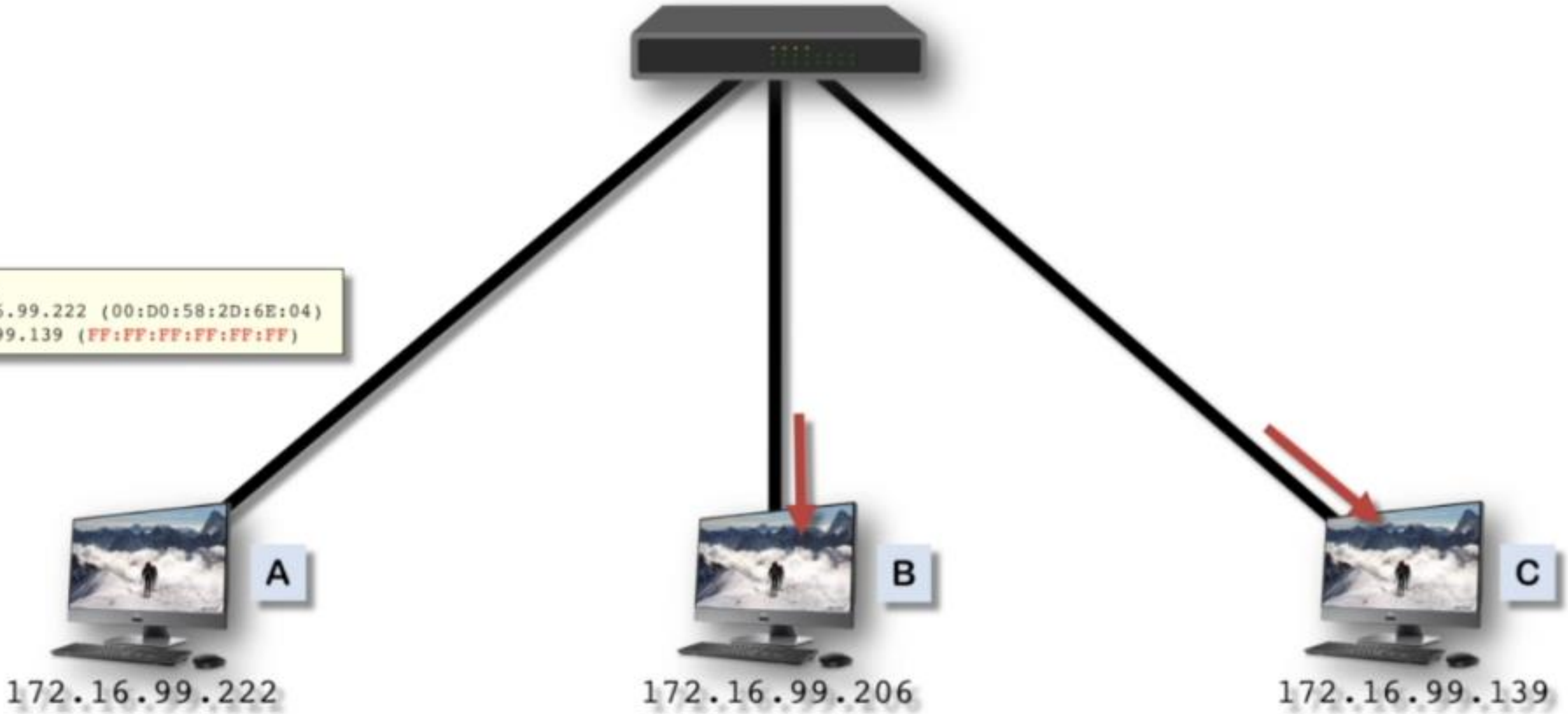


ARP Request
From: 172.16.99.222 (00:D0:58:2D:6E:04)
To: 172.16.99.139 (FF:FF:FF:FF:FF:FF)

ARP - Address Resolution Protocol

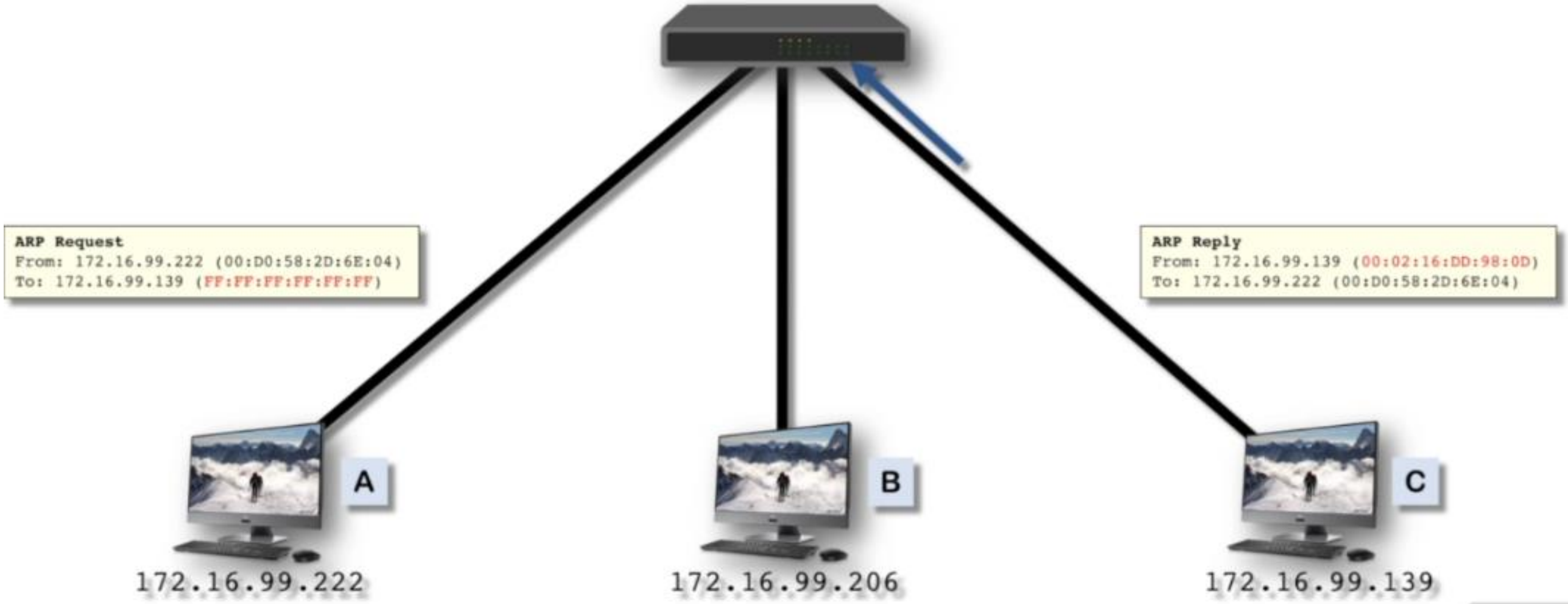
ARP Mechanism

```
ARP Request
From: 172.16.99.222 (00:D0:58:2D:6E:04)
To: 172.16.99.139 (FF:FF:FF:FF:FF:FF)
```



ARP - Address Resolution Protocol

ARP Mechanism

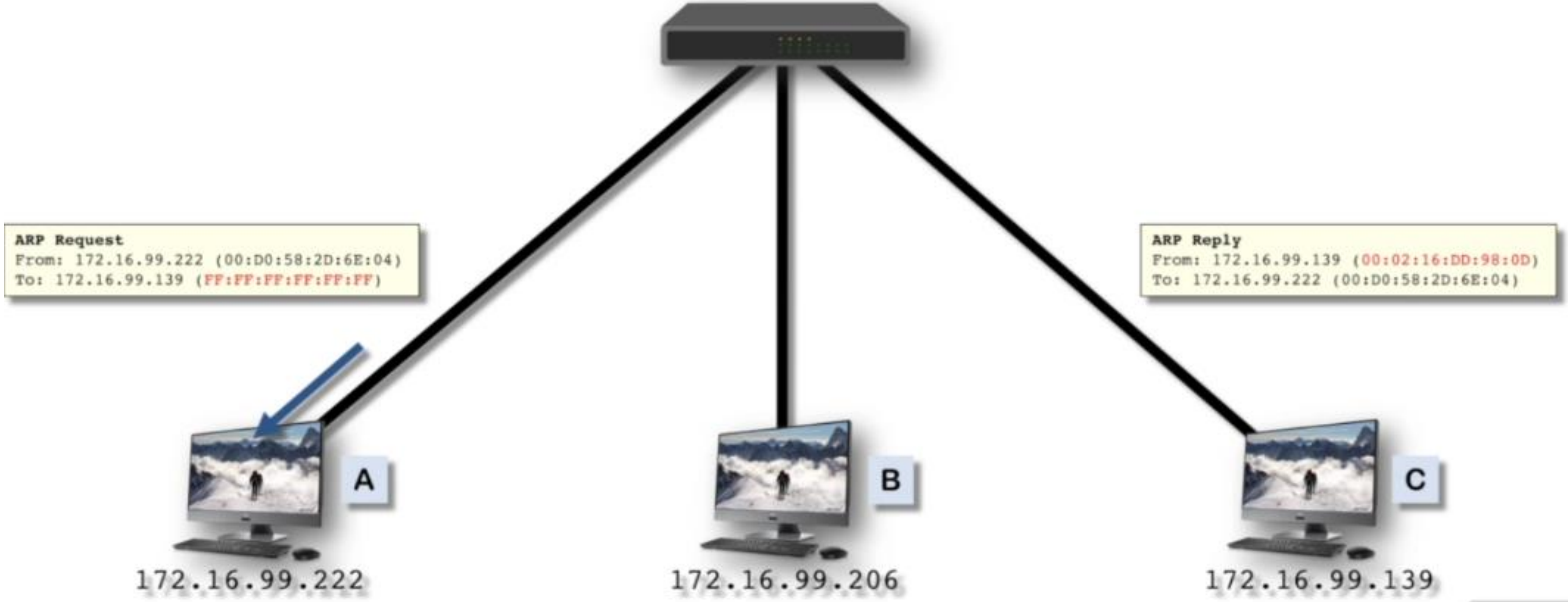


ARP Request
From: 172.16.99.222 (00:D0:58:2D:6E:04)
To: 172.16.99.139 (FF:FF:FF:FF:FF:FF)

ARP Reply
From: 172.16.99.139 (00:02:16:DD:98:0D)
To: 172.16.99.222 (00:D0:58:2D:6E:04)

ARP - Address Resolution Protocol

ARP Mechanism

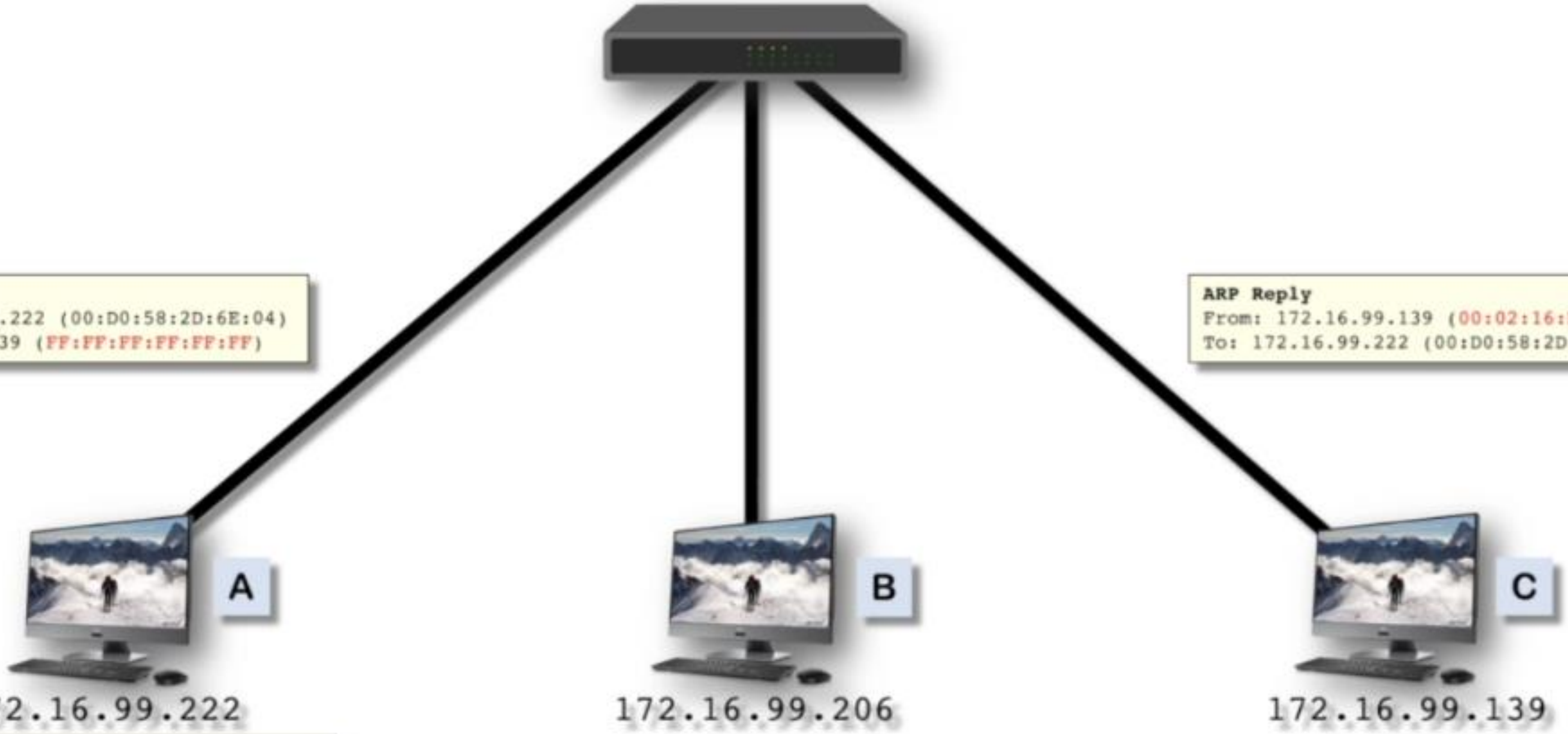


```
ARP Request
From: 172.16.99.222 (00:D0:58:2D:6E:04)
To: 172.16.99.139 (FF:FF:FF:FF:FF:FF)
```

```
ARP Reply
From: 172.16.99.139 (00:02:16:DD:98:0D)
To: 172.16.99.222 (00:D0:58:2D:6E:04)
```

ARP - Address Resolution Protocol

ARP Mechanism

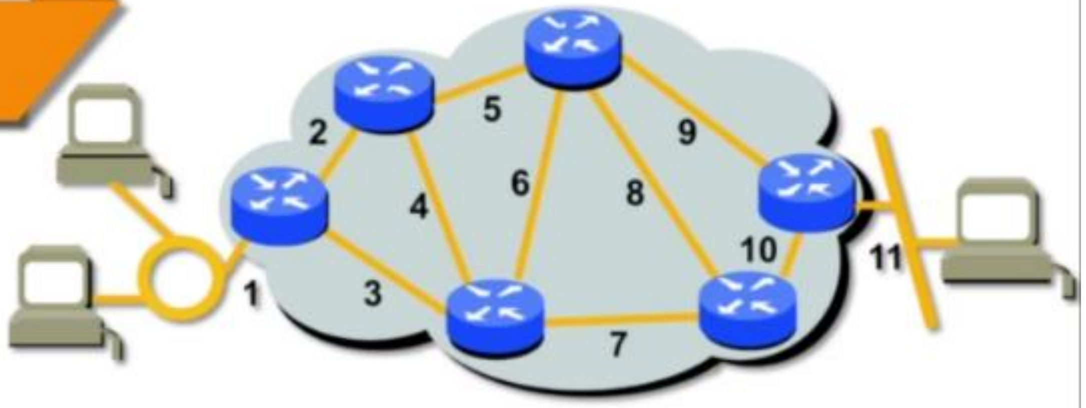


```
ARP Request
From: 172.16.99.222 (00:D0:58:2D:6E:04)
To: 172.16.99.139 (FF:FF:FF:FF:FF:FF)
```

```
ARP Reply
From: 172.16.99.139 (00:02:16:DD:98:0D)
To: 172.16.99.222 (00:D0:58:2D:6E:04)
```

```
ARP TABLE:
172.16.99.139 is (00:02:16:DD:98:0D)
```

L3 - Network Layer



Transferring the network packets from the source all the way to the destination

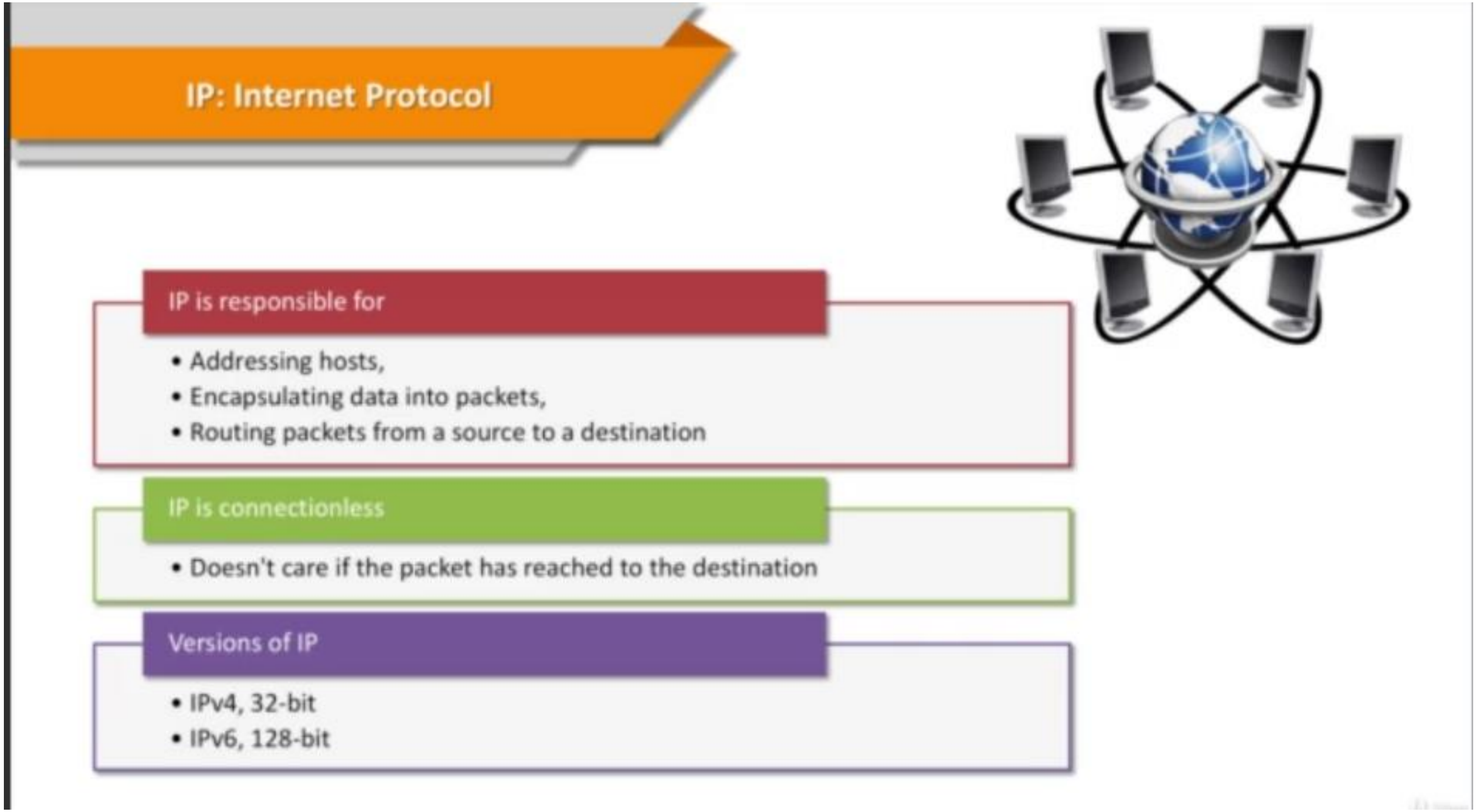
Responsible for packet forwarding including routing

Responds to service requests from the transport layer

Issues service requests to the data link layer

Functions:

- Connectionless communication
- Host addressing
- Message forwarding



IP: Internet Protocol

IP is responsible for

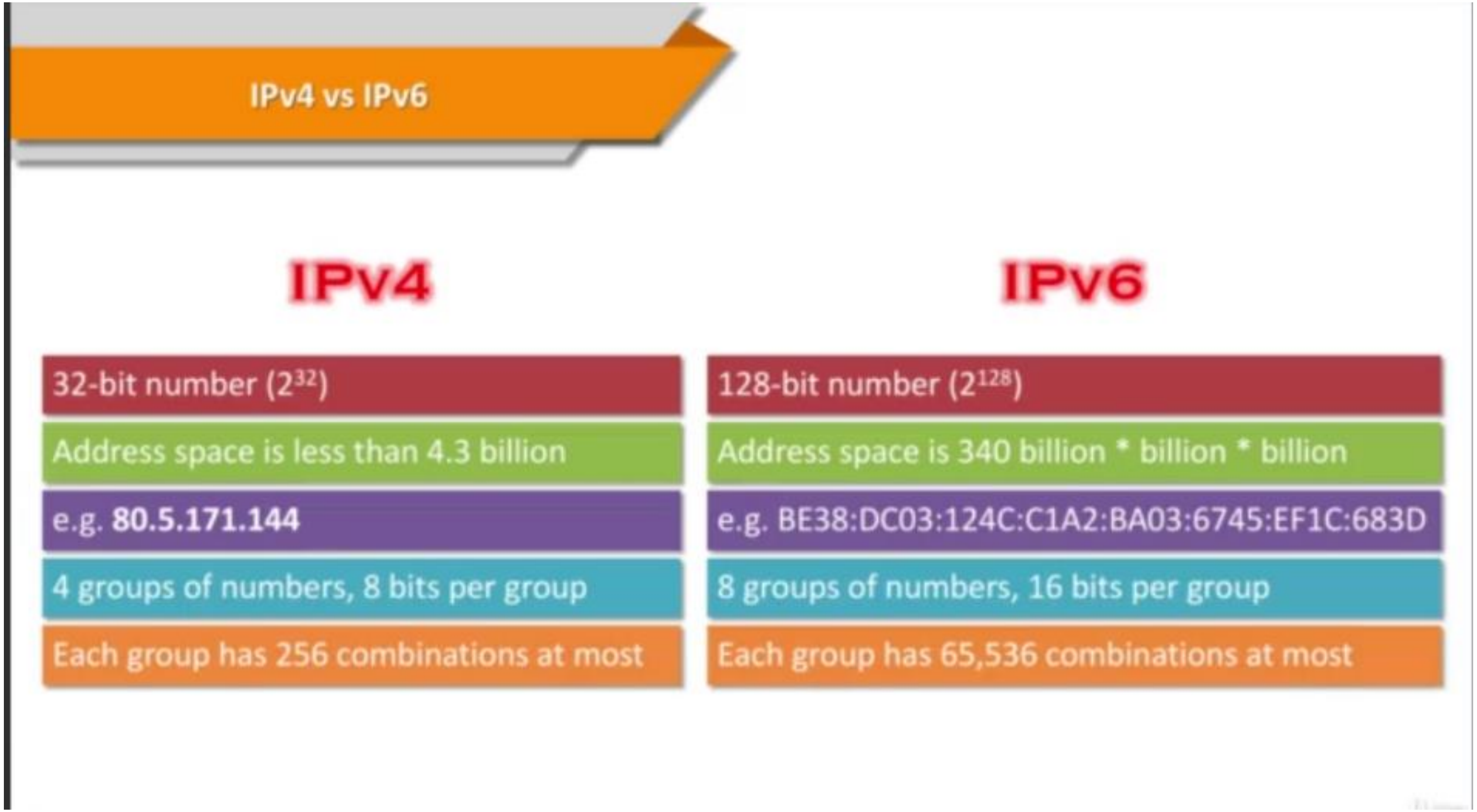
- Addressing hosts,
- Encapsulating data into packets,
- Routing packets from a source to a destination

IP is connectionless

- Doesn't care if the packet has reached to the destination

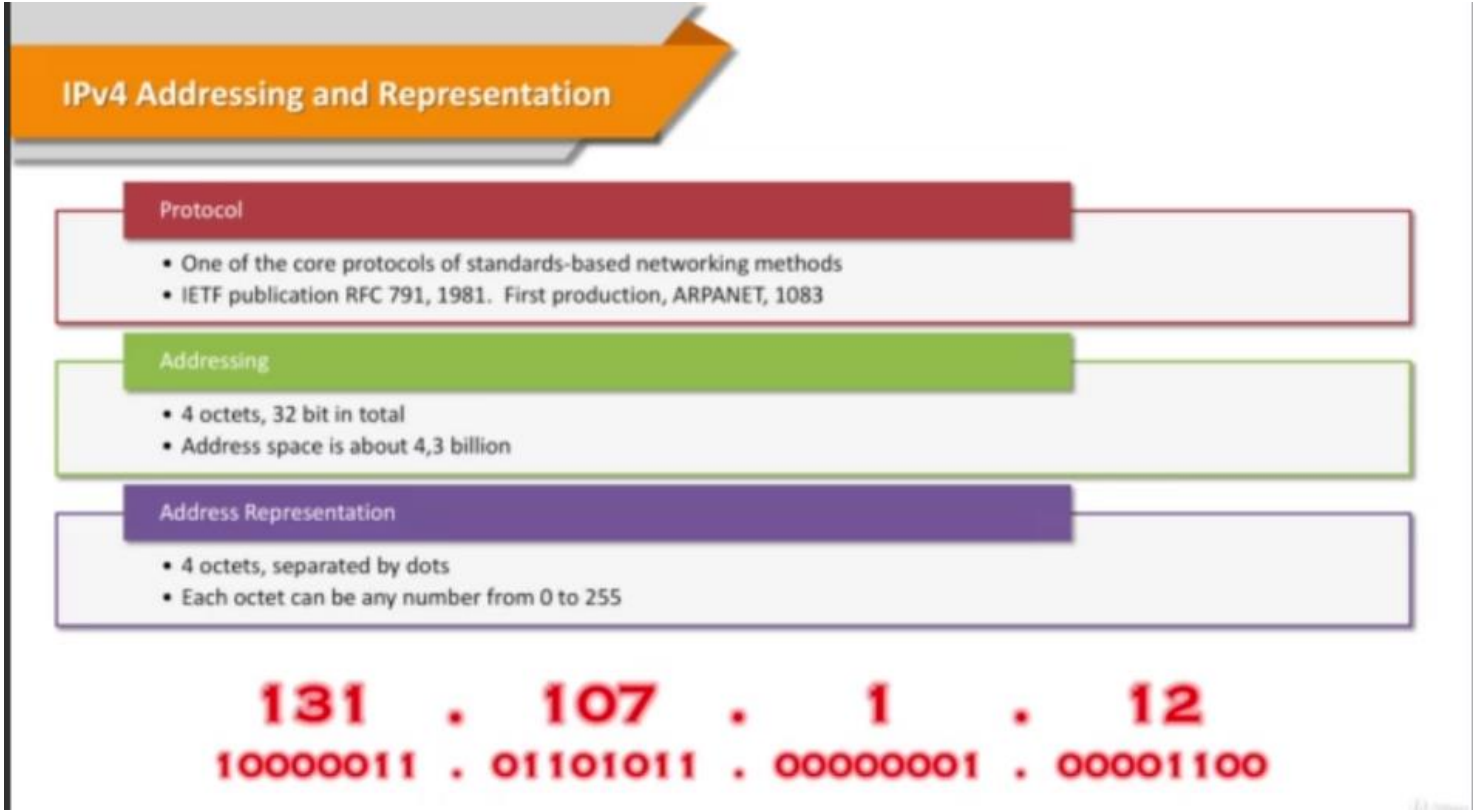
Versions of IP

- IPv4, 32-bit
- IPv6, 128-bit



IPv4 vs IPv6

IPv4	IPv6
32-bit number (2^{32})	128-bit number (2^{128})
Address space is less than 4.3 billion	Address space is 340 billion * billion * billion
e.g. **80.5.171.144**	e.g. BE38:DC03:124C:C1A2:BA03:6745:EF1C:683D
4 groups of numbers, 8 bits per group	8 groups of numbers, 16 bits per group
Each group has 256 combinations at most	Each group has 65,536 combinations at most



IPv4 Addressing and Representation

Protocol

- One of the core protocols of standards-based networking methods
- IETF publication RFC 791, 1981. First production, ARPANET, 1083

Addressing

- 4 octets, 32 bit in total
- Address space is about 4,3 billion

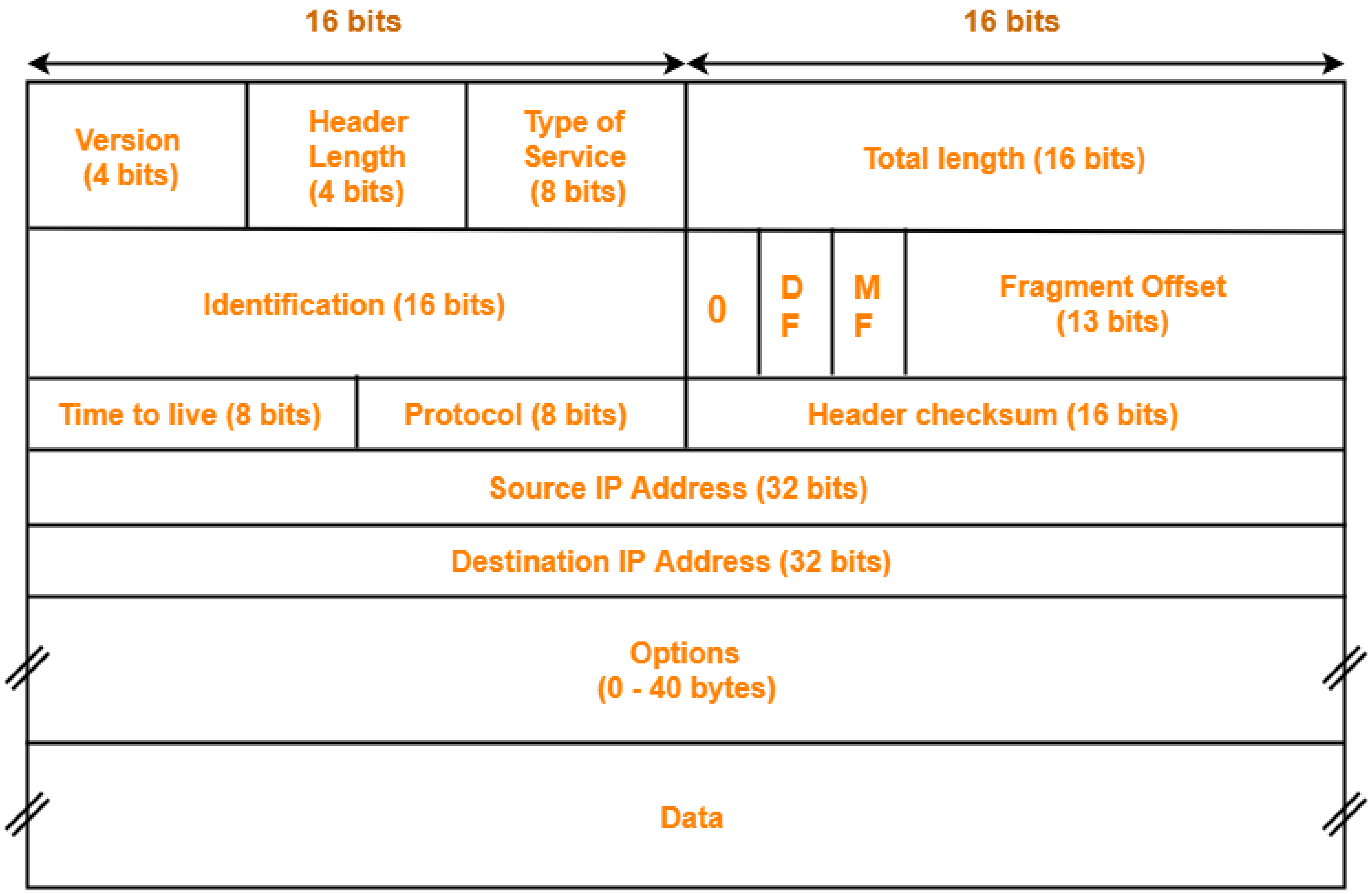
Address Representation

- 4 octets, separated by dots
- Each octet can be any number from 0 to 255

131 . 107 . 1 . 12

10000011 . 01101011 . 00000001 . 00001100

IP header



16 bits

16 bits

Version (4 bits)

Header Length (4 bits)

Type of Service (8 bits)

Total length (16 bits)

Identification (16 bits)

0

D F

M F

Fragment Offset (13 bits)

Time to live (8 bits)

Protocol (8 bits)

Header checksum (16 bits)

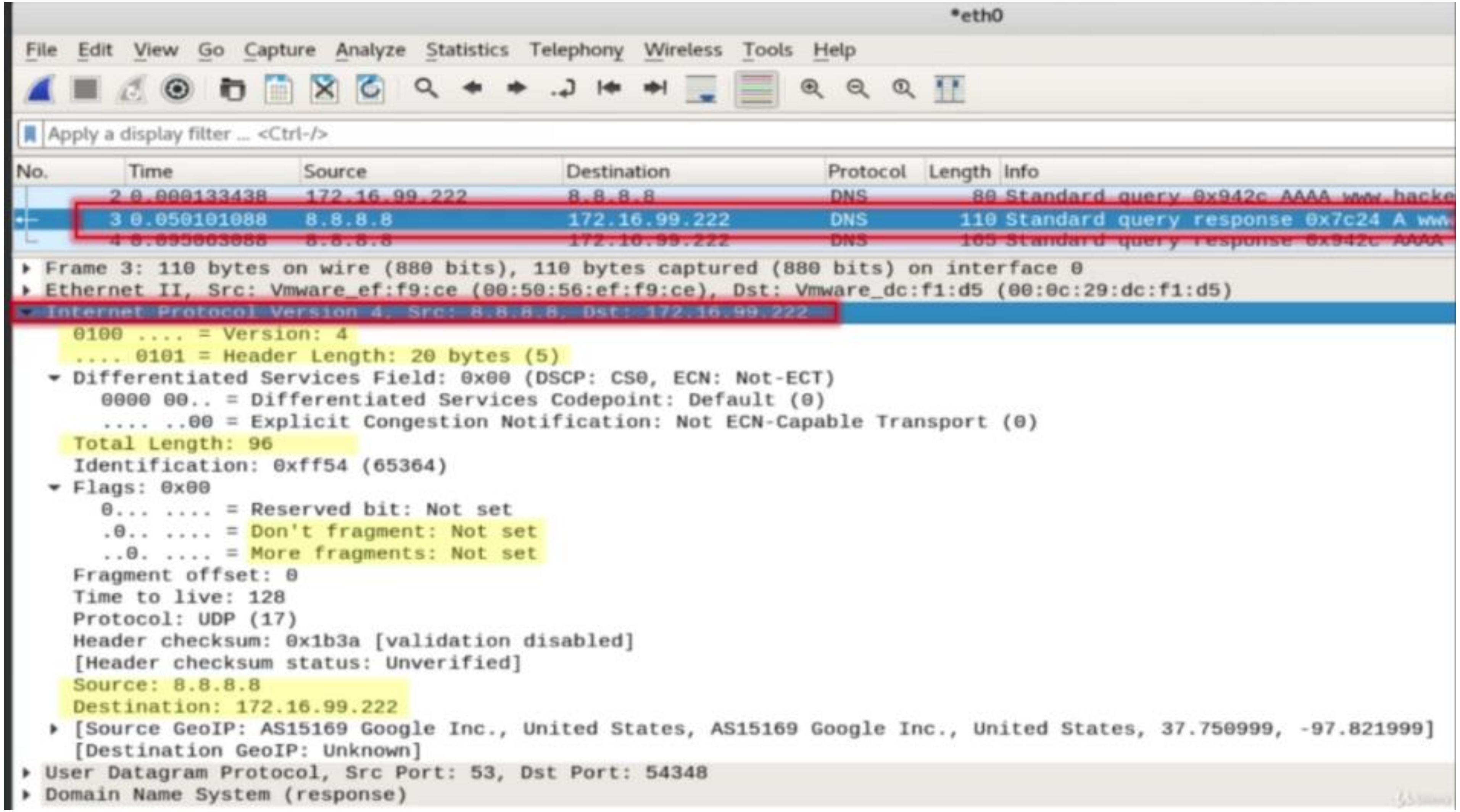
Source IP Address (32 bits)

Destination IP Address (32 bits)

Options (0 - 40 bytes)

Data

IPv4 Header

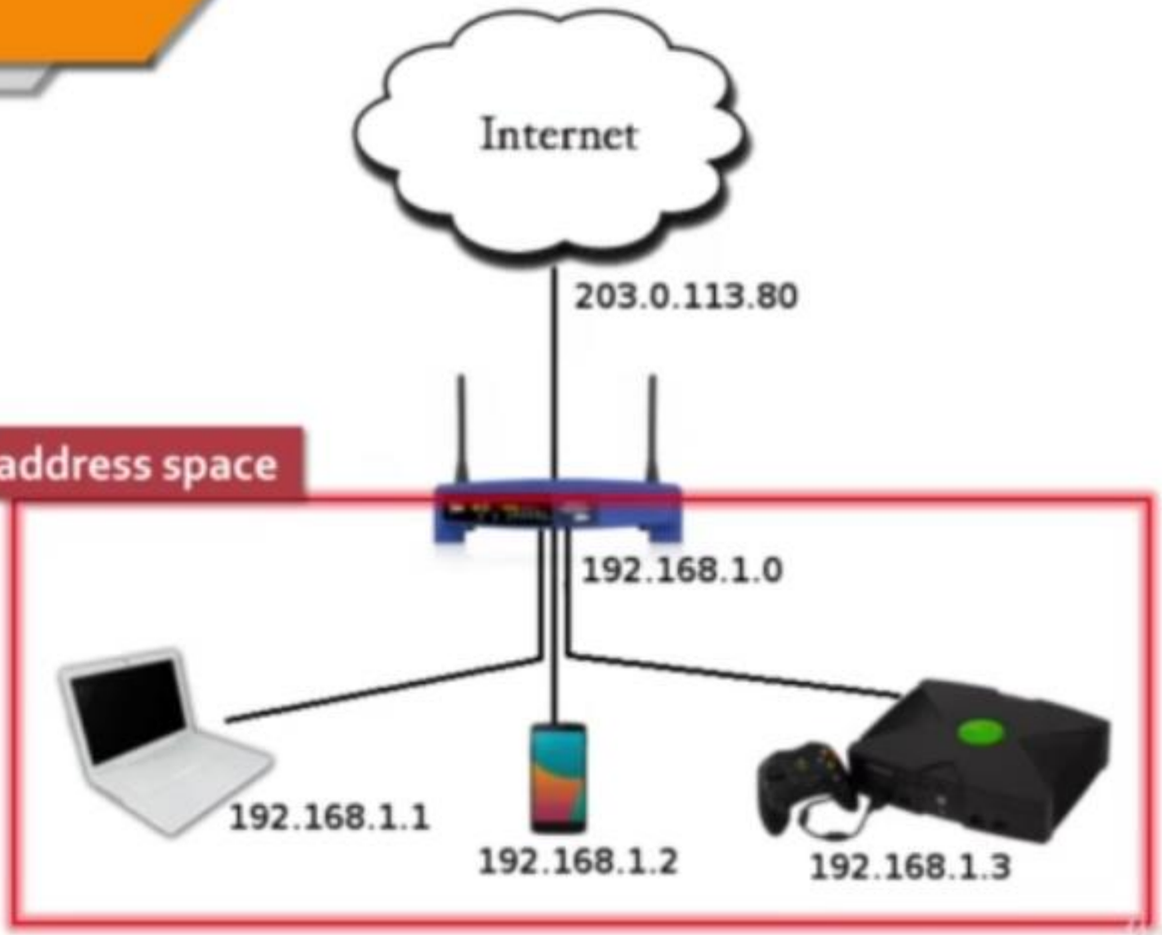

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

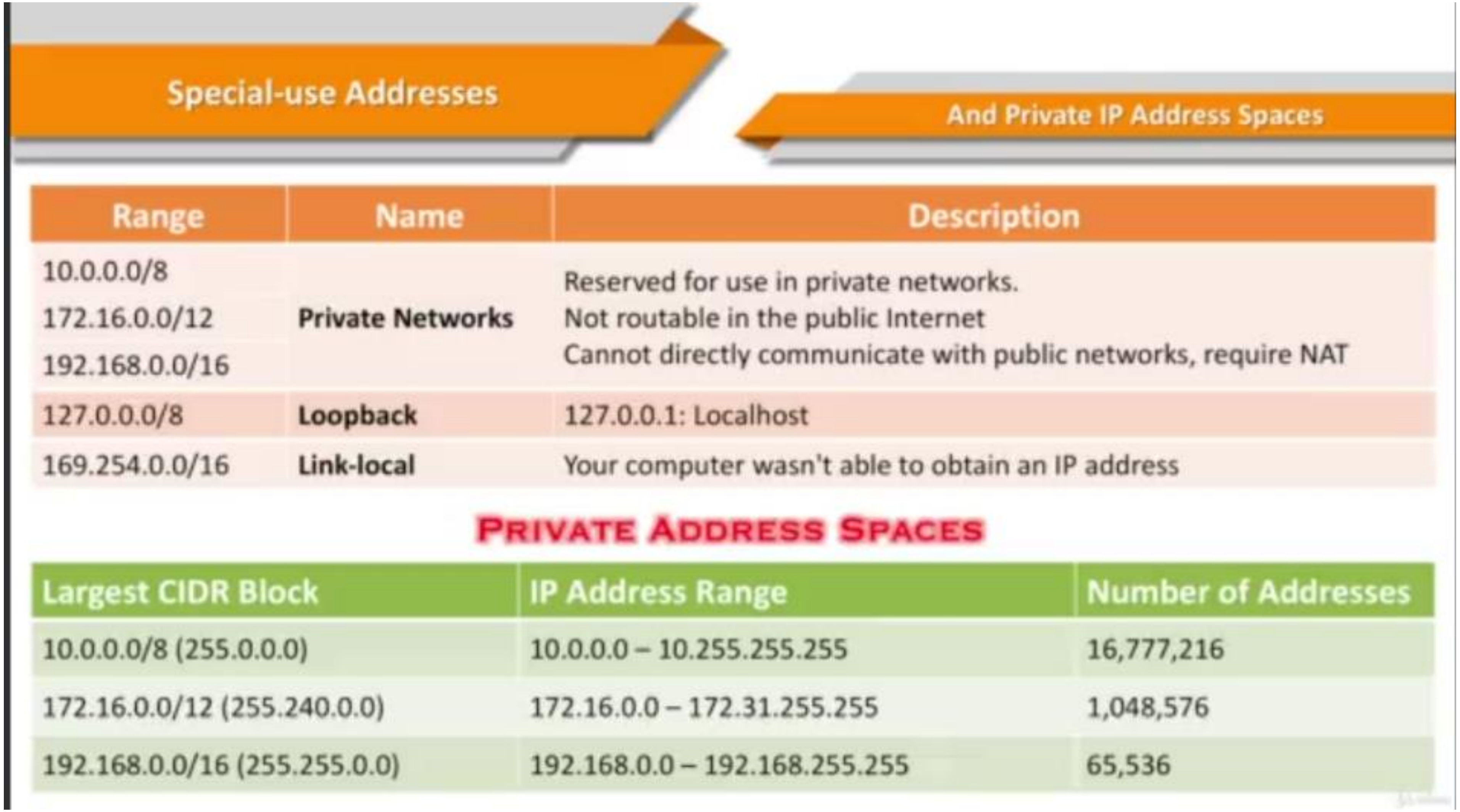
```
No.     Time          Source          Destination     Protocol Length Info
      2 0.000133438   172.16.99.222   8.8.8.8         DNS         80 Standard query 0x942c AAAA www.hacke
      3 0.050101088   8.8.8.8         172.16.99.222   DNS        110 Standard query response 0x7c24 A www
      4 0.095003088   8.8.8.8         172.16.99.222   DNS        105 Standard query response 0x942c AAAA
```

```
▸ Frame 3: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
▸ Ethernet II, Src: Vmware_ef:f9:ce (00:50:56:ef:f9:ce), Dst: Vmware_dc:f1:d5 (00:0c:29:dc:f1:d5)
▾ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.16.99.222
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 96
    Identification: 0xff54 (65364)
  ▾ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x1b3a [validation disabled]
    [Header checksum status: Unverified]
    Source: 8.8.8.8
    Destination: 172.16.99.222
  ▸ [Source GeoIP: AS15169 Google Inc., United States, AS15169 Google Inc., United States, 37.750999, -97.821999]
    [Destination GeoIP: Unknown]
▸ User Datagram Protocol, Src Port: 53, Dst Port: 54348
▸ Domain Name System (response)
```

Private Network

The network that uses **private IP address space**





Special-use Addresses

And Private IP Address Spaces

Range	Name	Description
10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	**Private Networks**	Reserved for use in private networks. Not routable in the public Internet Cannot directly communicate with public networks, require NAT
127.0.0.0/8	**Loopback**	127.0.0.1: Localhost
169.254.0.0/16	**Link-local**	Your computer wasn't able to obtain an IP address

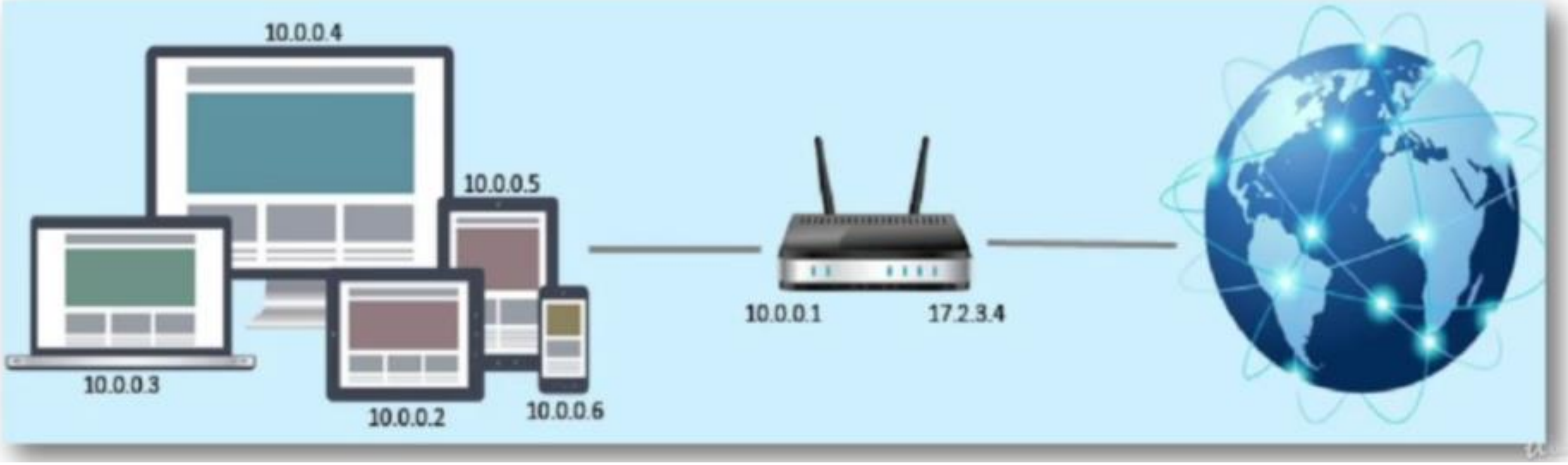
PRIVATE ADDRESS SPACES

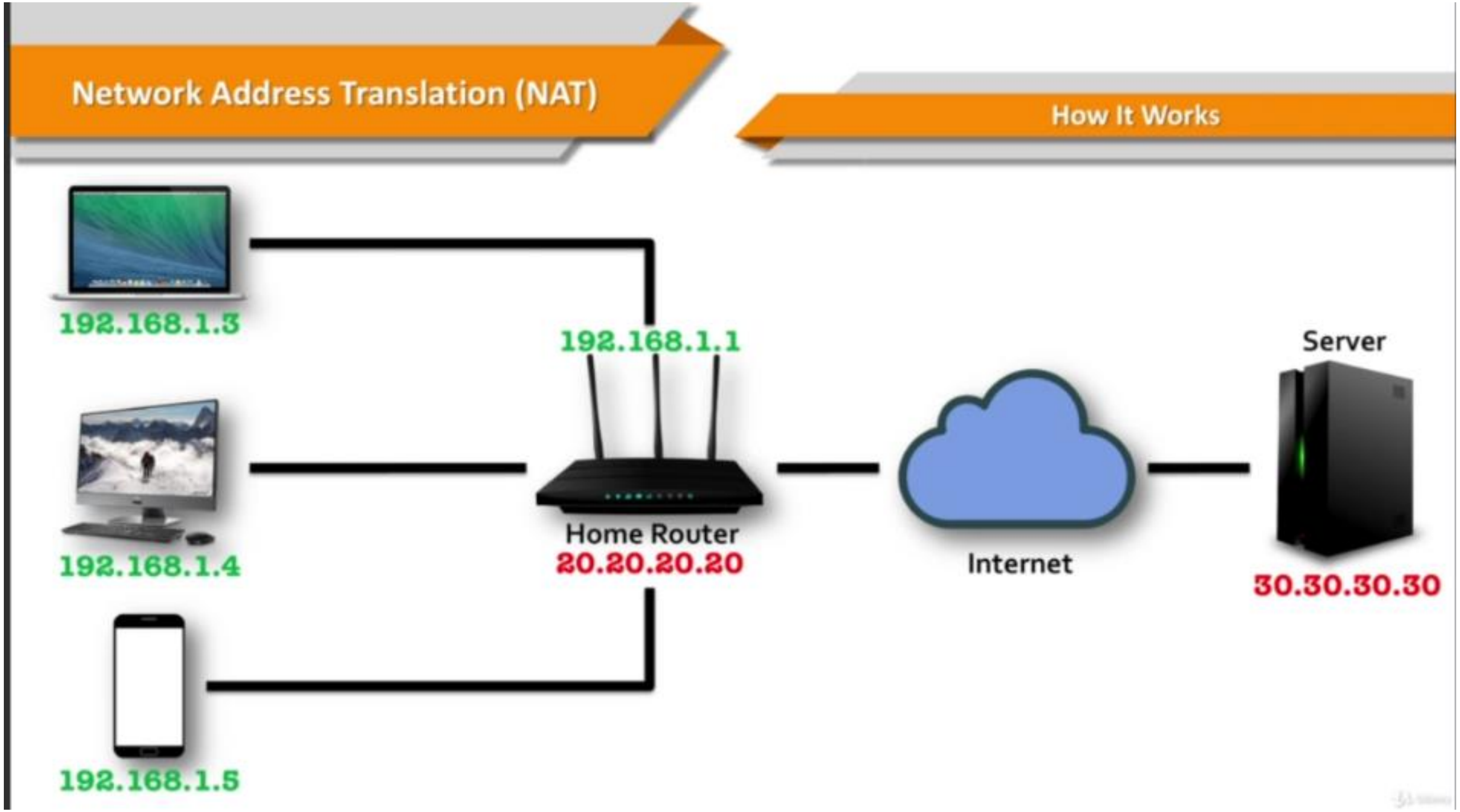
Largest CIDR Block	IP Address Range	Number of Addresses
10.0.0.0/8 (255.0.0.0)	10.0.0.0 – 10.255.255.255	16,777,216
172.16.0.0/12 (255.240.0.0)	172.16.0.0 – 172.31.255.255	1,048,576
192.168.0.0/16 (255.255.0.0)	192.168.0.0 – 192.168.255.255	65,536

Network Address Translation

Devices in a private network cannot talk to public IP addresses without NAT.

Hide an entire private network behind a single public IP address.





Network Address Translation (NAT)

How It Works

192.168.1.3

192.168.1.4

192.168.1.5

192.168.1.1

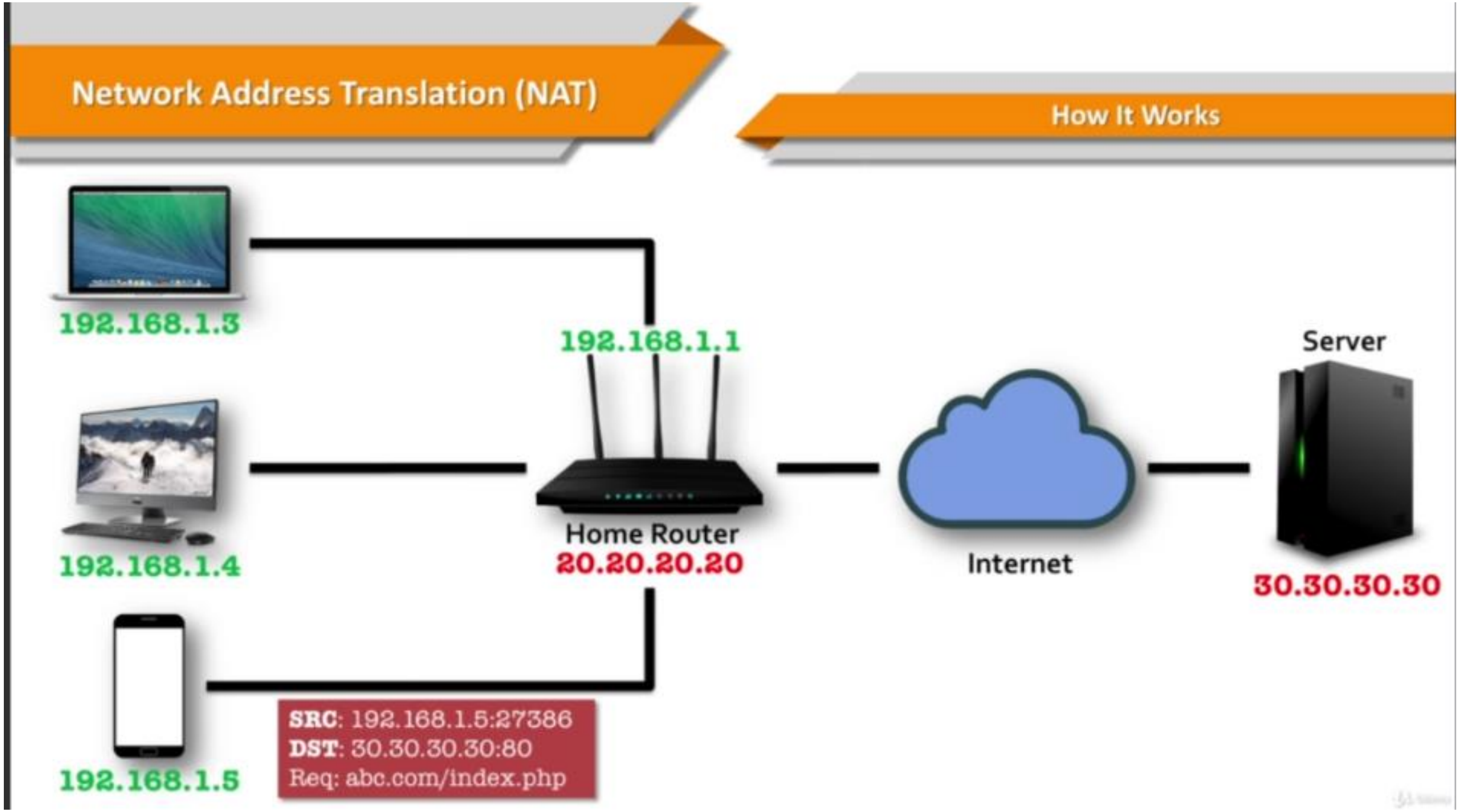
Home Router

20.20.20.20

Internet

Server

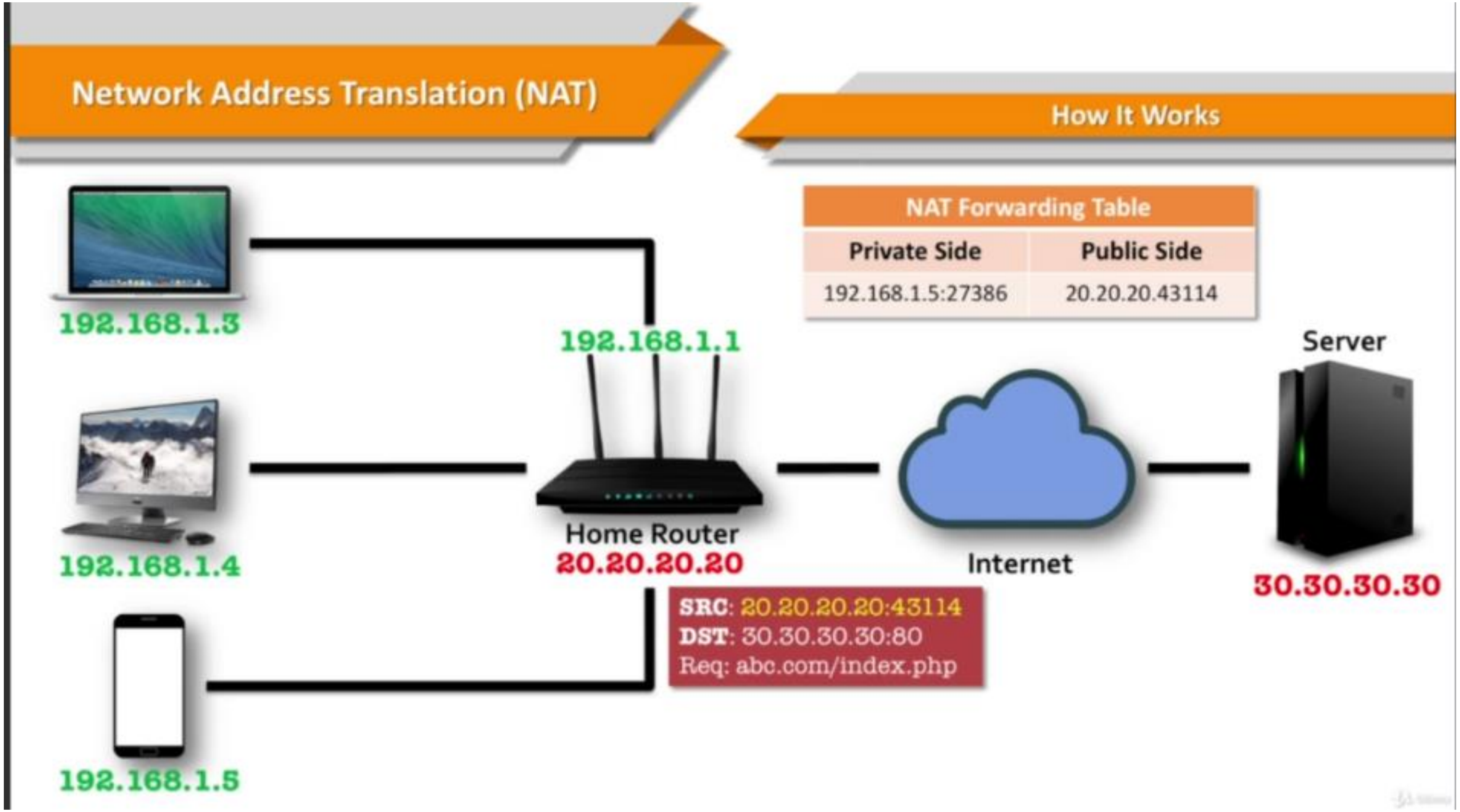
30.30.30.30



Network Address Translation (NAT)

How It Works

SRC: 192.168.1.5:27386
DST: 30.30.30.30:80
Req: abc.com/index.php

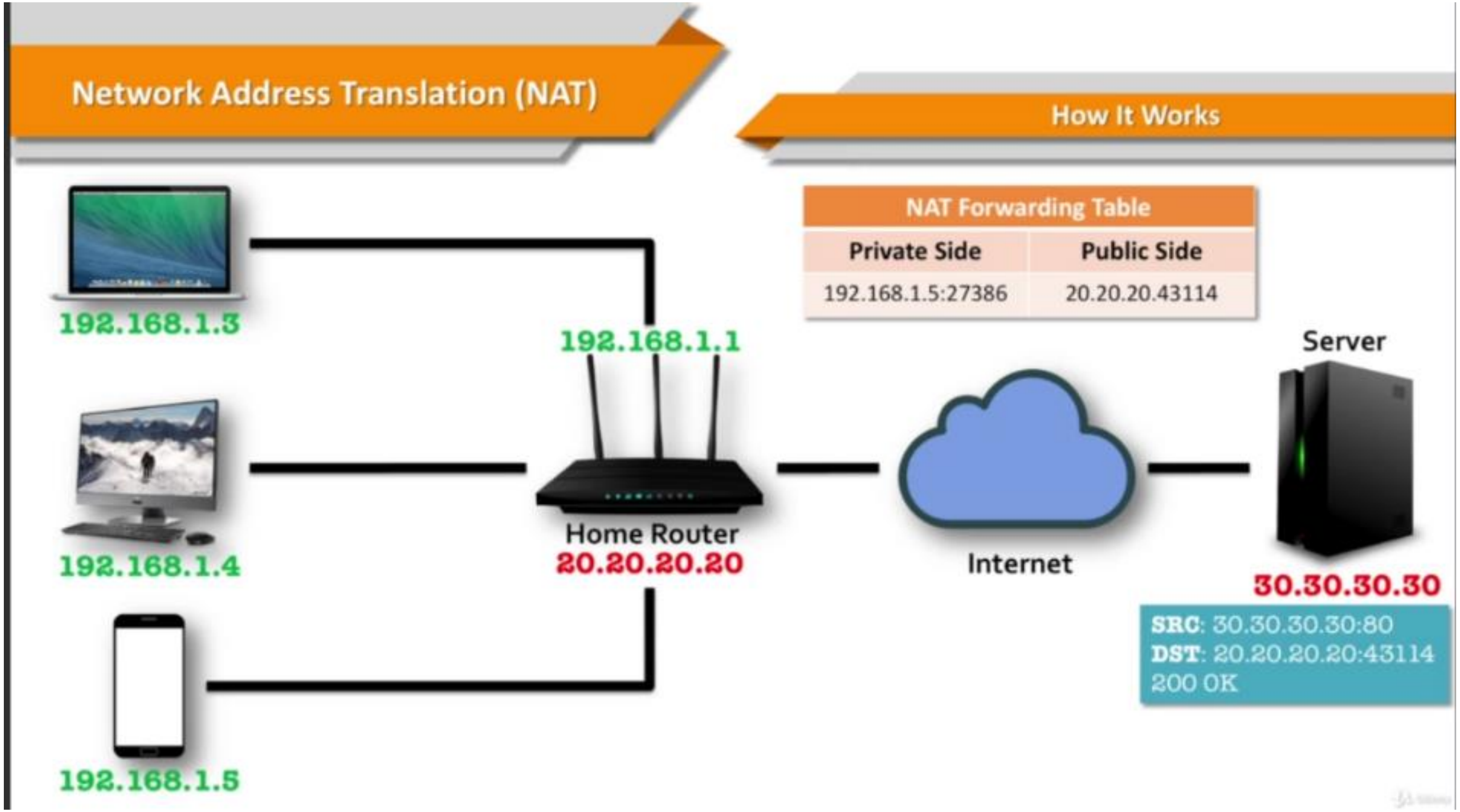


Network Address Translation (NAT)

How It Works

NAT Forwarding Table	
Private Side	**Public Side**
192.168.1.5:27386	20.20.20.43114

SRC: 20.20.20.20:43114
DST: 30.30.30.30:80
Req: abc.com/index.php

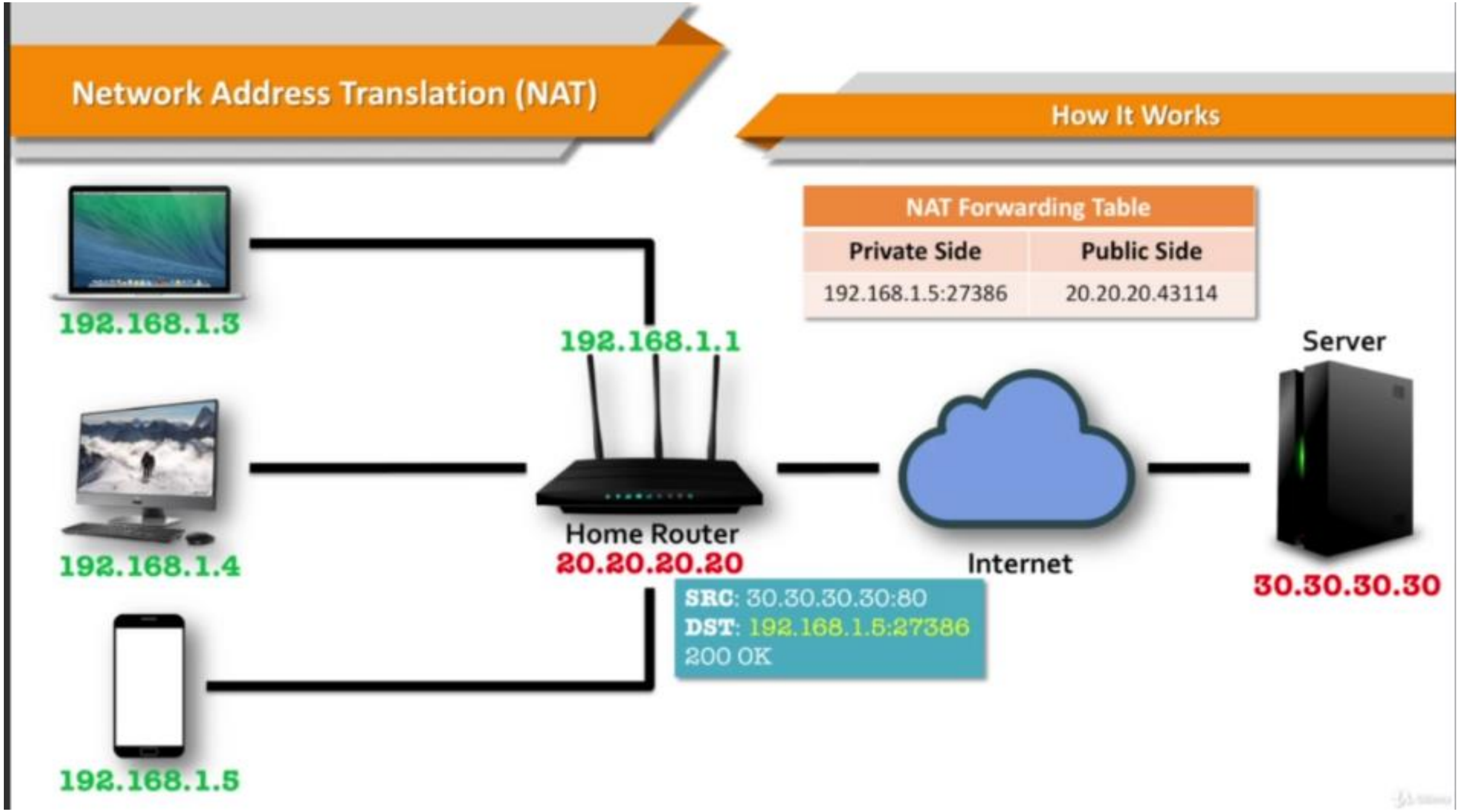


Network Address Translation (NAT)

How It Works

NAT Forwarding Table	
Private Side	Public Side
192.168.1.5:27386	20.20.20.43114

SRC: 30.30.30.30:80
DST: 20.20.20.20:43114
200 OK

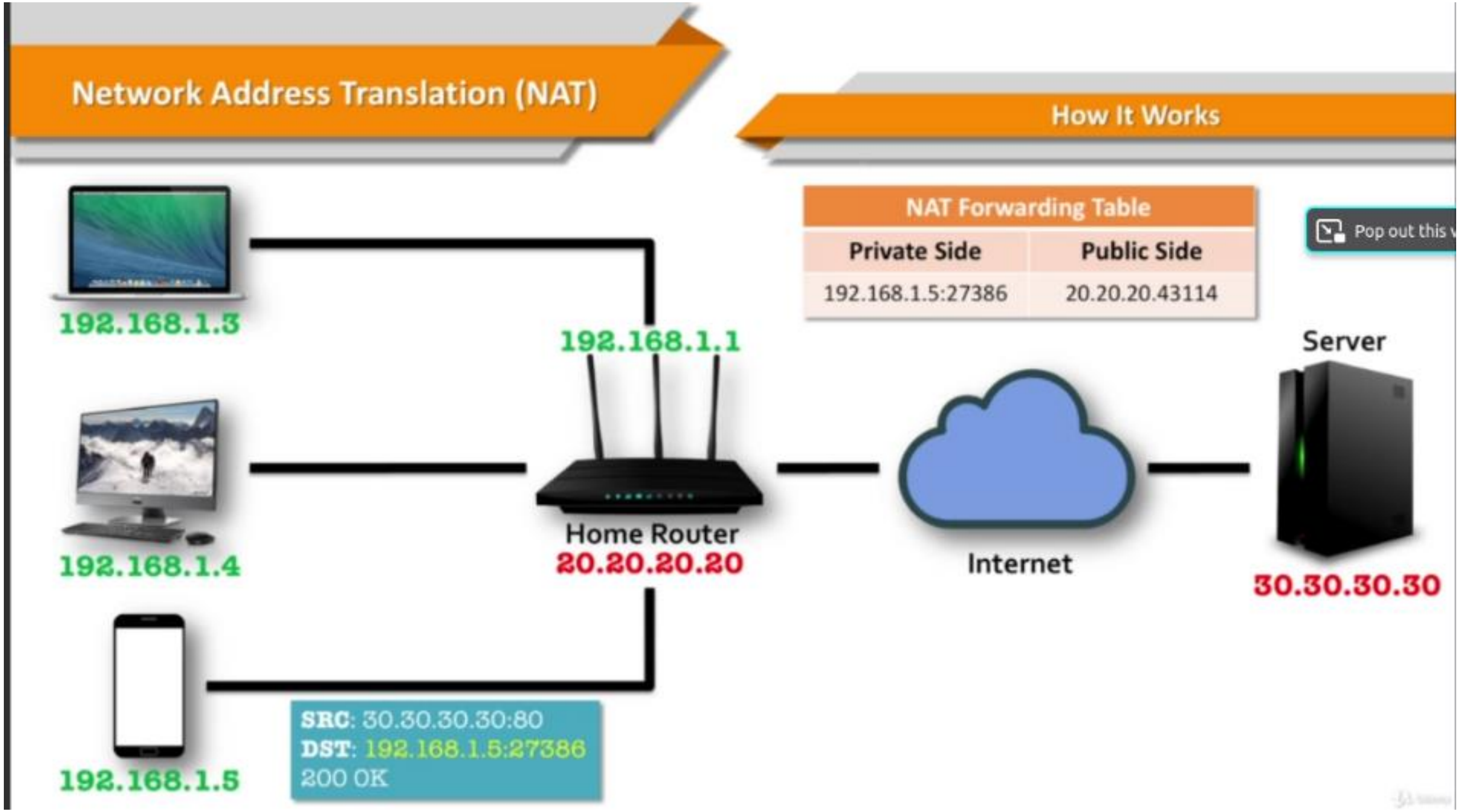


Network Address Translation (NAT)

How It Works

NAT Forwarding Table	
Private Side	**Public Side**
192.168.1.5:27386	20.20.20.43114

SRC: 30.30.30.30:80
DST: 192.168.1.5:27386
200 OK

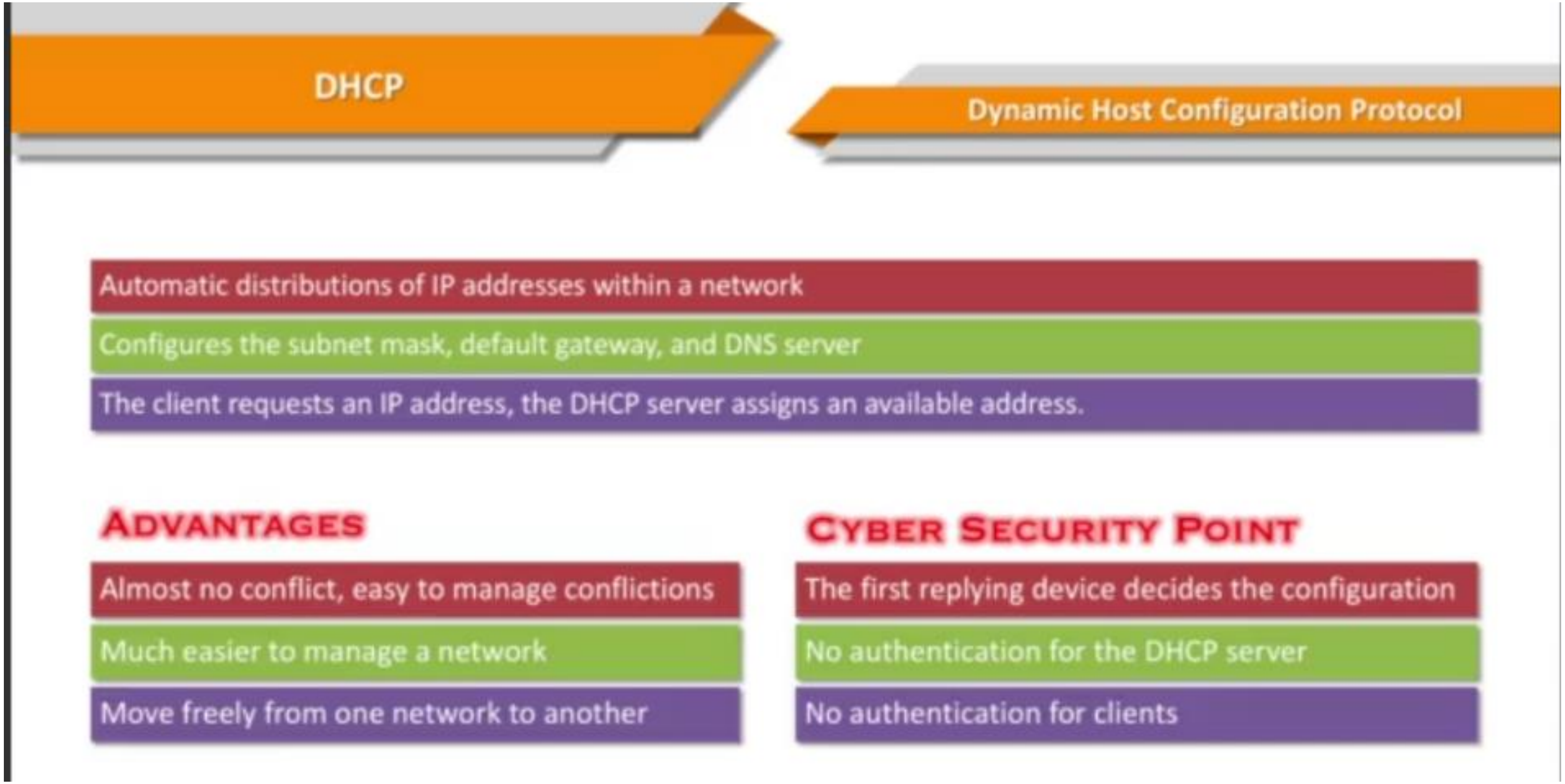


Network Address Translation (NAT)

How It Works

NAT Forwarding Table	
Private Side	**Public Side**
192.168.1.5:27386	20.20.20.43114

SRC: 30.30.30.30:80
DST: 192.168.1.5:27386
200 OK



DHCP

Dynamic Host Configuration Protocol

- Automatic distributions of IP addresses within a network
- Configures the subnet mask, default gateway, and DNS server
- The client requests an IP address, the DHCP server assigns an available address.

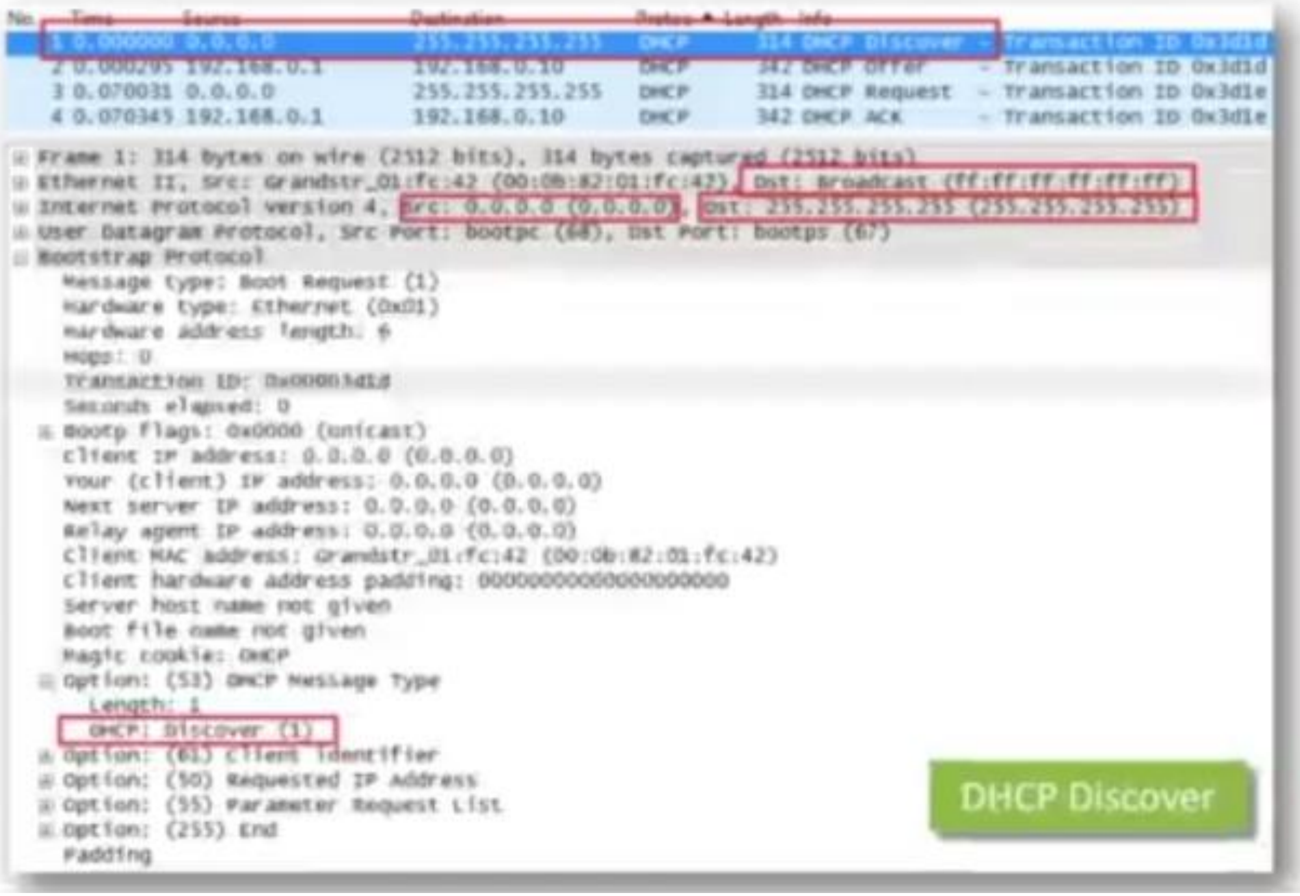
Advantages

- Almost no conflict, easy to manage conflictions
- Much easier to manage a network
- Move freely from one network to another

Cyber Security Point

- The first replying device decides the configuration
- No authentication for the DHCP server
- No authentication for clients

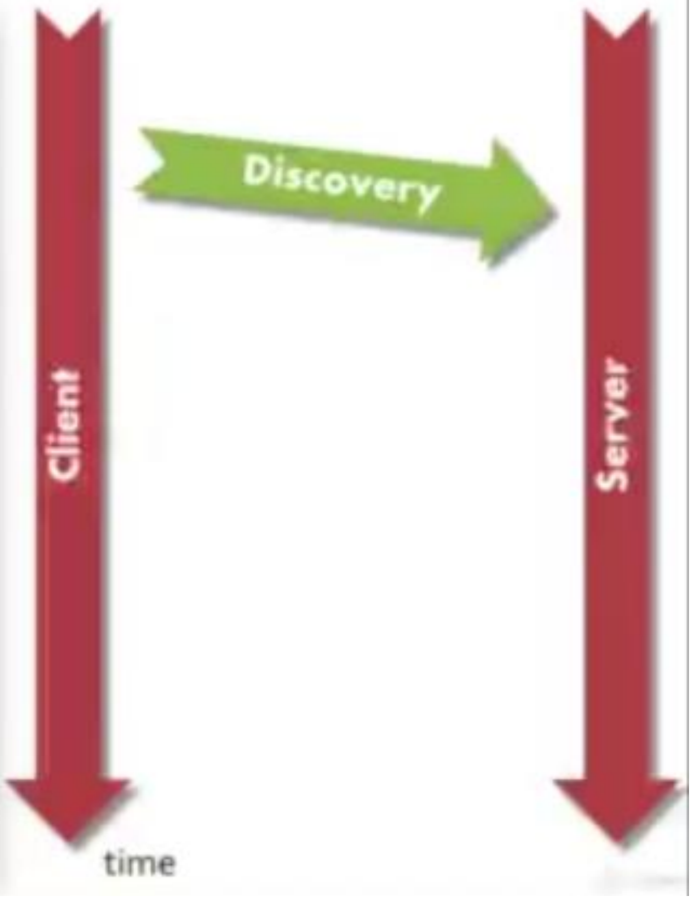
DHCP Mechanism



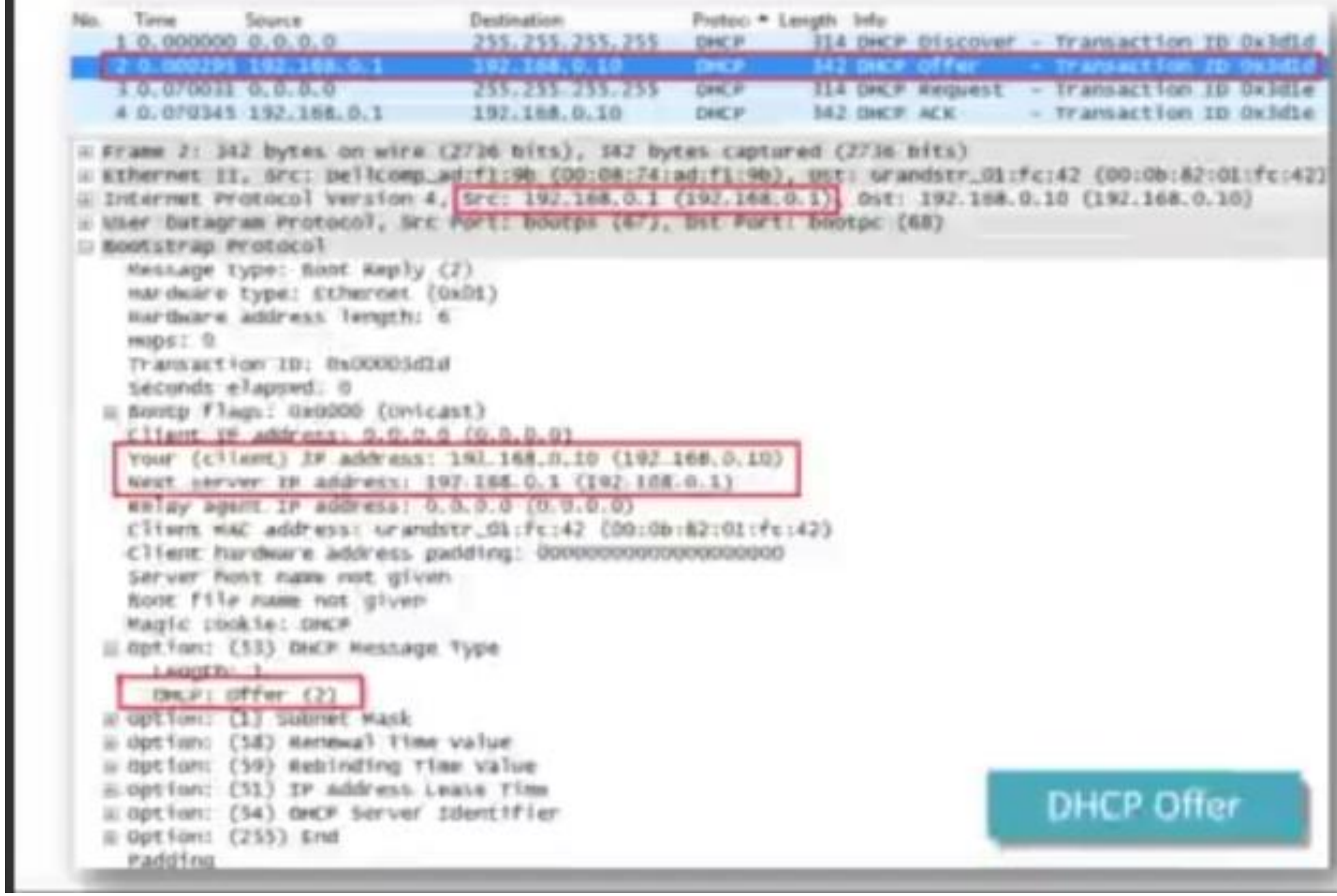
```
No. Time     Source        Destination      Protoc▲ Length Info
  1 0.000000 0.0.0.0       255.255.255.255  DHCP    314 DHCP Discover - Transaction ID 0x3d1d
  2 0.000295 192.168.0.1   192.168.0.10     DHCP    342 DHCP Offer    - Transaction ID 0x3d1d
  3 0.070031 0.0.0.0       255.255.255.255  DHCP    314 DHCP Request  - Transaction ID 0x3d1e
  4 0.070345 192.168.0.1   192.168.0.10     DHCP    342 DHCP ACK      - Transaction ID 0x3d1e

⊞ Frame 1: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
⊞ Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1d
    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: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊟ Option: (53) DHCP Message Type
      Length: 1
      DHCP: Discover (1)
  ⊞ Option: (61) Client identifier
  ⊞ Option: (50) Requested IP Address
  ⊞ Option: (55) Parameter Request List
  ⊞ Option: (255) End
    Padding
```

DHCP Discover



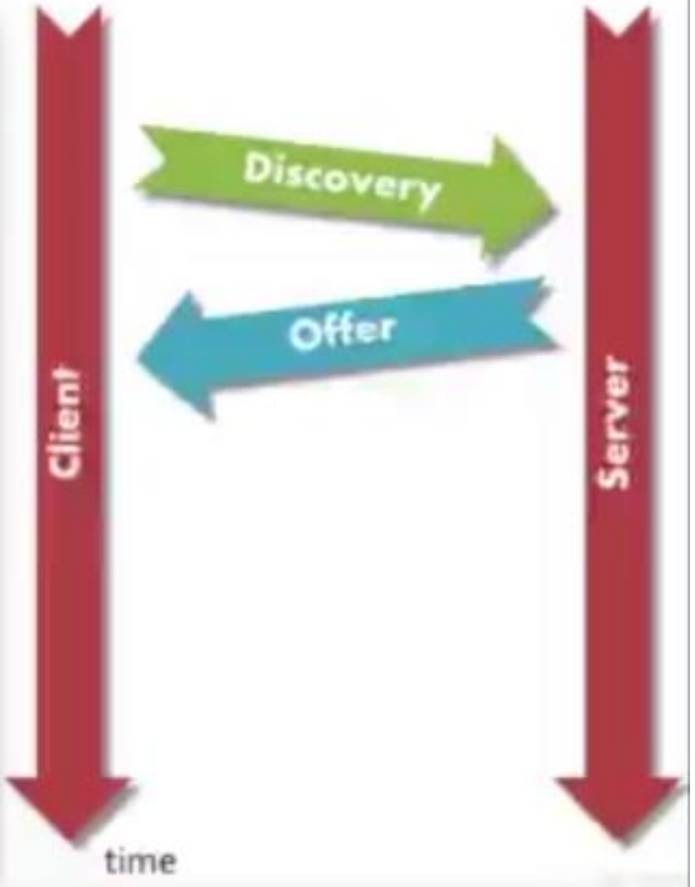
DHCP Mechanism



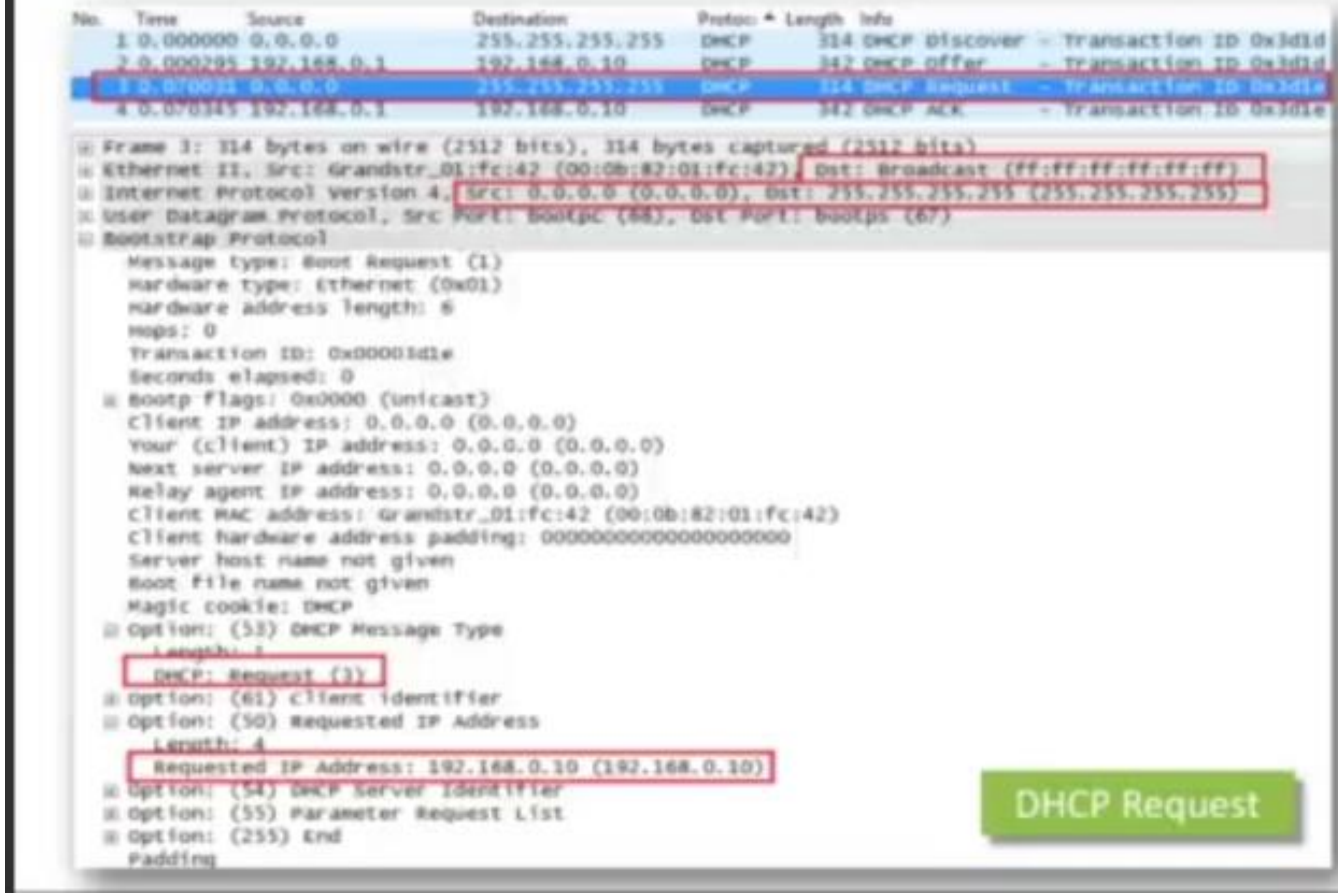
```
No.  Time      Source        Destination       Protoc ▲ Length Info
   1 0.000000 0.0.0.0       255.255.255.255   DHCP      314 DHCP Discover  - Transaction ID 0x3d1d
   2 0.000295 192.168.0.1   192.168.0.10      DHCP      342 DHCP Offer     - Transaction ID 0x3d1d
   3 0.070031 0.0.0.0       255.255.255.255   DHCP      314 DHCP Request   - Transaction ID 0x3d1e
   4 0.070345 192.168.0.1   192.168.0.10      DHCP      342 DHCP ACK       - Transaction ID 0x3d1e

⊞ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊞ Ethernet II, Src: Dellcomp_ad:f1:9b (00:08:74:ad:f1:9b), Dst: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
⊞ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.10 (192.168.0.10)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1d
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.0.10 (192.168.0.10)
    Next server IP address: 192.168.0.1 (192.168.0.1)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊟ Option: (53) DHCP Message Type
      Length: 1
      DHCP: Offer (2)
  ⊞ Option: (1) Subnet Mask
  ⊞ Option: (58) Renewal Time Value
  ⊞ Option: (59) Rebinding Time Value
  ⊞ Option: (51) IP Address Lease Time
  ⊞ Option: (54) DHCP Server Identifier
  ⊞ Option: (255) End
    Padding
```

DHCP Offer



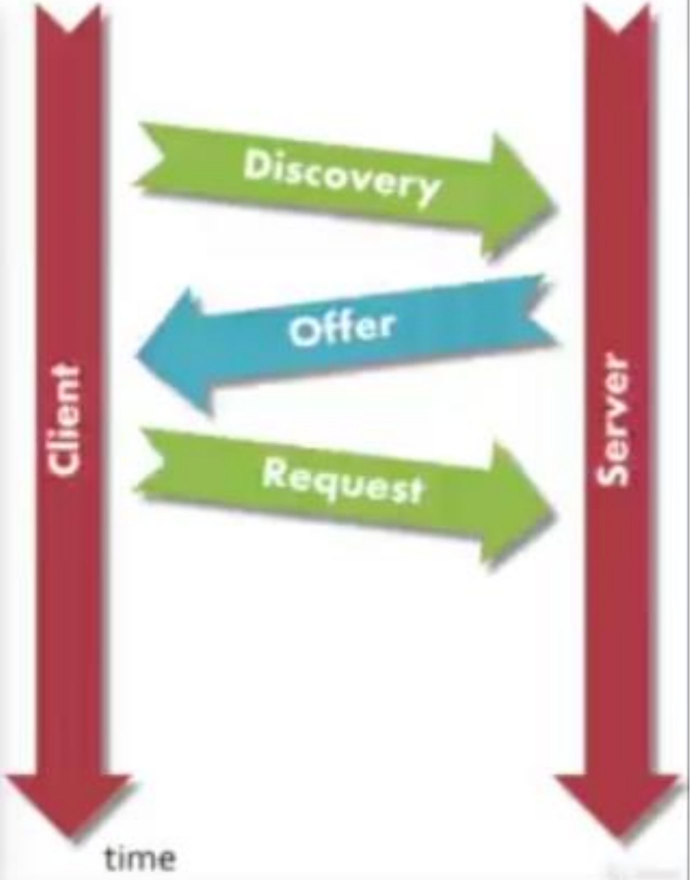
DHCP Mechanism



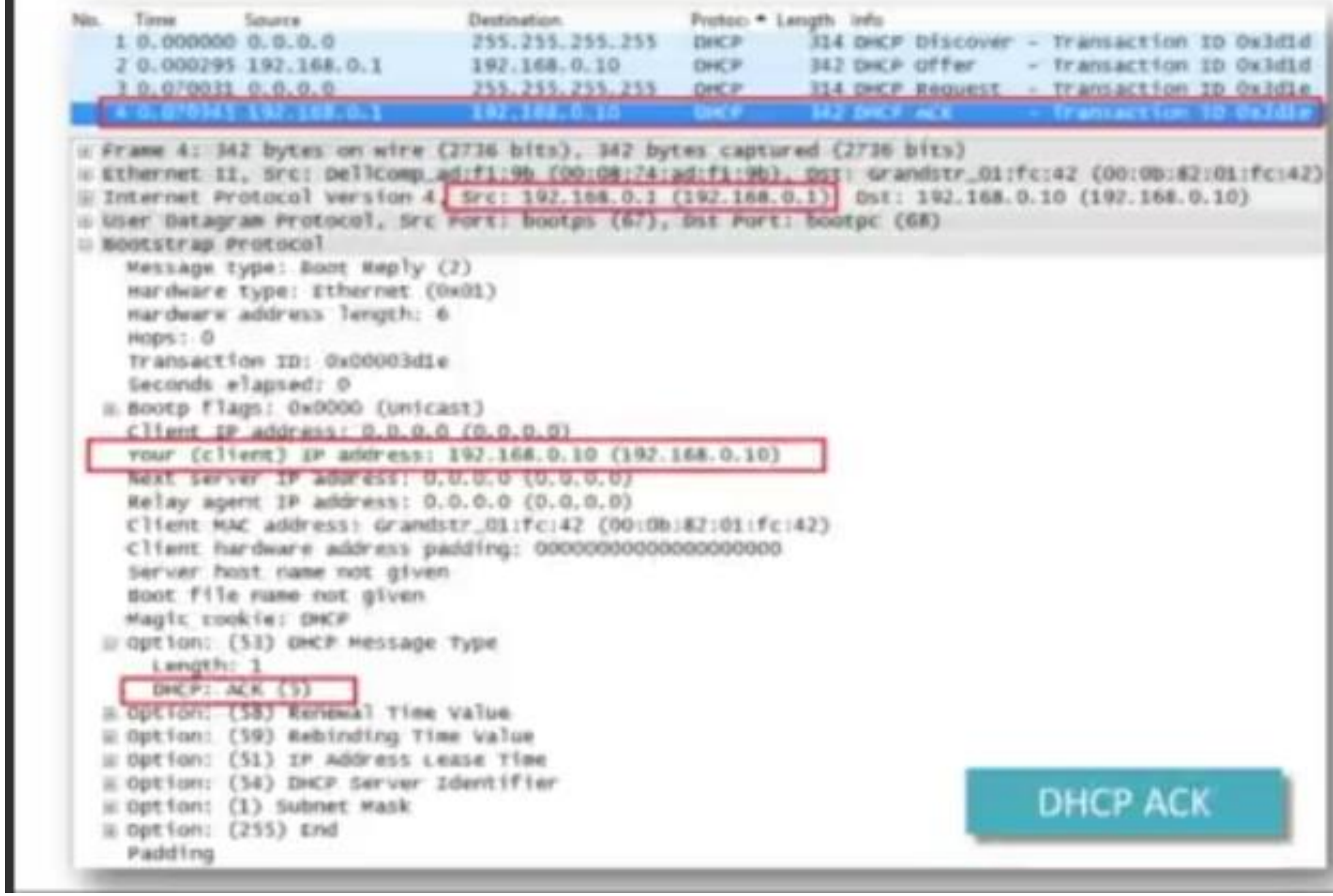
```
No.  Time       Source        Destination       Protoc ^ Length Info
   1 0.000000  0.0.0.0       255.255.255.255   DHCP      314 DHCP Discover - Transaction ID 0x3d1d
   2 0.000295  192.168.0.1   192.168.0.10      DHCP      342 DHCP Offer    - Transaction ID 0x3d1d
   3 0.070031  0.0.0.0       255.255.255.255   DHCP      314 DHCP Request  - Transaction ID 0x3d1e
   4 0.070345  192.168.0.1   192.168.0.10      DHCP      342 DHCP ACK      - Transaction ID 0x3d1e

⊞ Frame 3: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
⊞ Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1e
    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: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊟ Option: (53) DHCP Message Type
      Length: 1
      DHCP: Request (3)
  ⊞ Option: (61) Client identifier
  ⊟ Option: (50) Requested IP Address
      Length: 4
      Requested IP Address: 192.168.0.10 (192.168.0.10)
  ⊞ Option: (54) DHCP Server Identifier
  ⊞ Option: (55) Parameter Request List
  ⊞ Option: (255) End
    Padding
```

DHCP Request



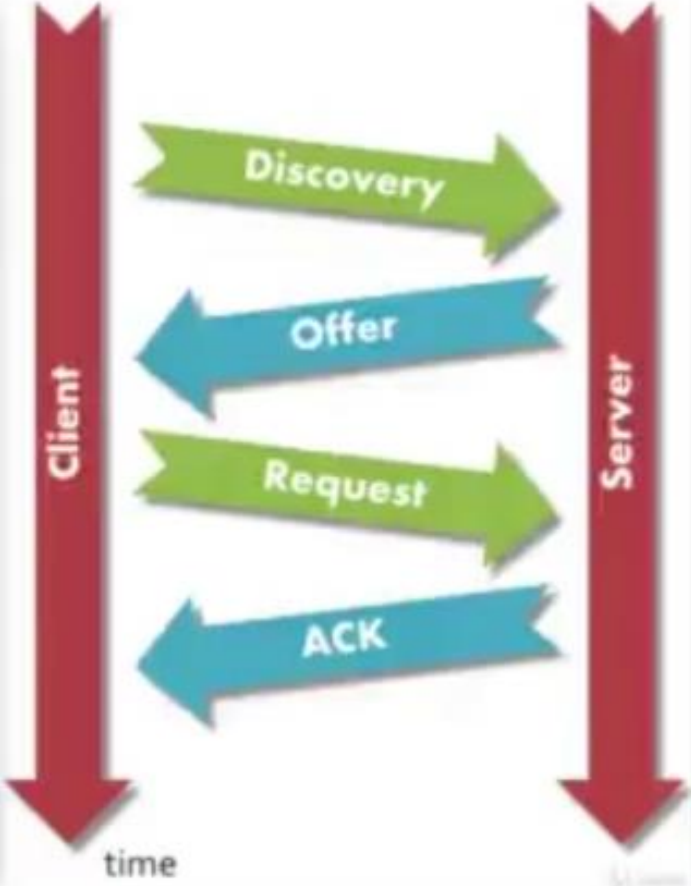
DHCP Mechanism

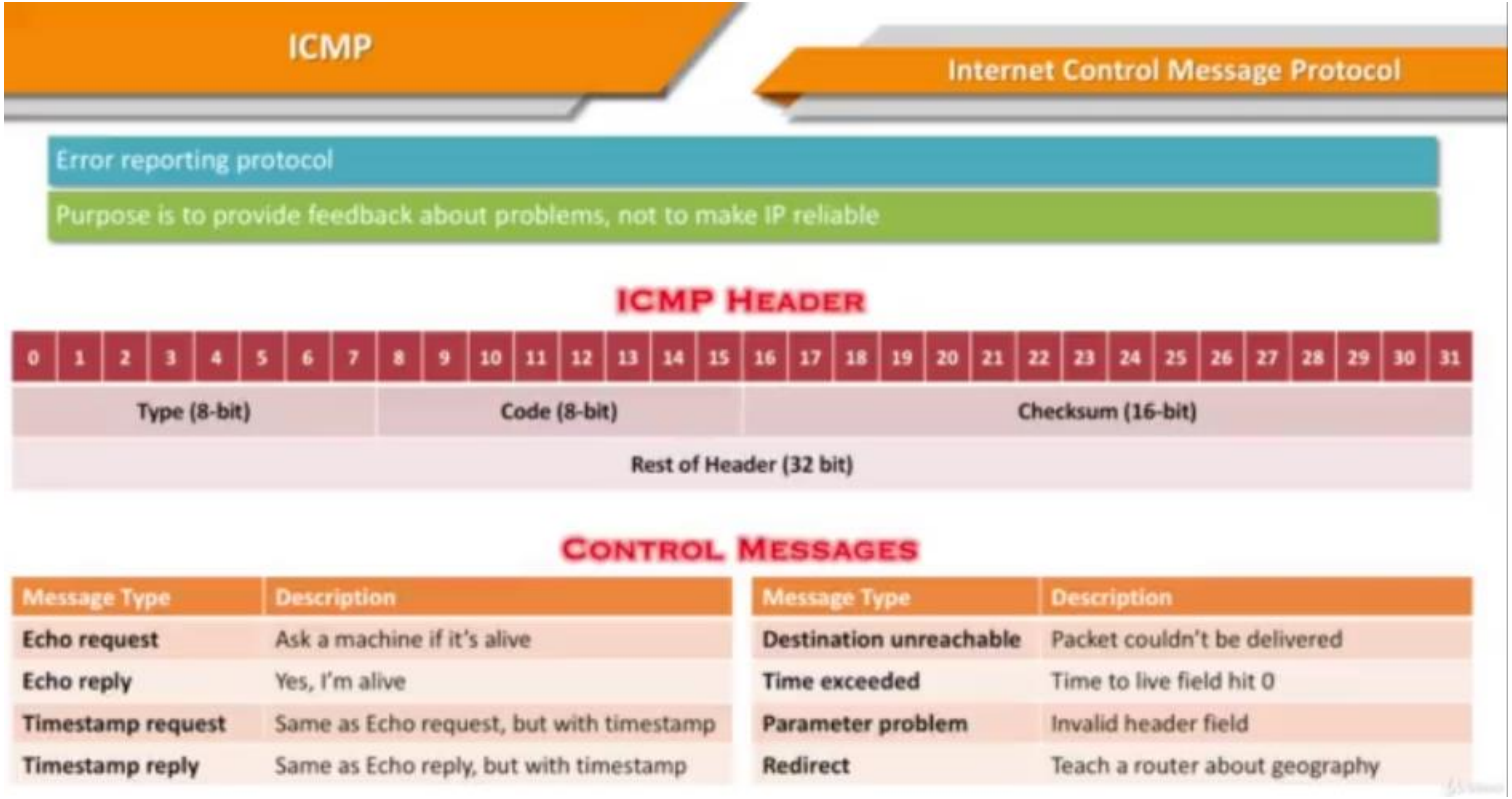


```
No.  Time      Source        Destination      Protoc ▾ Length Info
  1 0.000000  0.0.0.0       255.255.255.255  DHCP     314 DHCP Discover  - Transaction ID 0x3d1d
  2 0.000295  192.168.0.1   192.168.0.10     DHCP     342 DHCP Offer     - Transaction ID 0x3d1d
  3 0.070031  0.0.0.0       255.255.255.255  DHCP     314 DHCP Request   - Transaction ID 0x3d1e
  4 0.070345  192.168.0.1   192.168.0.10     DHCP     342 DHCP ACK       - Transaction ID 0x3d1e

⊞ Frame 4: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊞ Ethernet II, Src: DellComp_ad:f1:9b (00:08:74:ad:f1:9b), Dst: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
⊞ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.10 (192.168.0.10)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1e
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.0.10 (192.168.0.10)
    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: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊟ Option: (53) DHCP Message Type
      Length: 1
      DHCP: ACK (5)
  ⊞ Option: (58) Renewal Time Value
  ⊞ Option: (59) Rebinding Time Value
  ⊞ Option: (51) IP Address Lease Time
  ⊞ Option: (54) DHCP Server Identifier
  ⊞ Option: (1) Subnet Mask
  ⊞ Option: (255) End
    Padding
```

DHCP ACK





ICMP

Internet Control Message Protocol

Error reporting protocol

Purpose is to provide feedback about problems, not to make IP reliable

ICMP Header

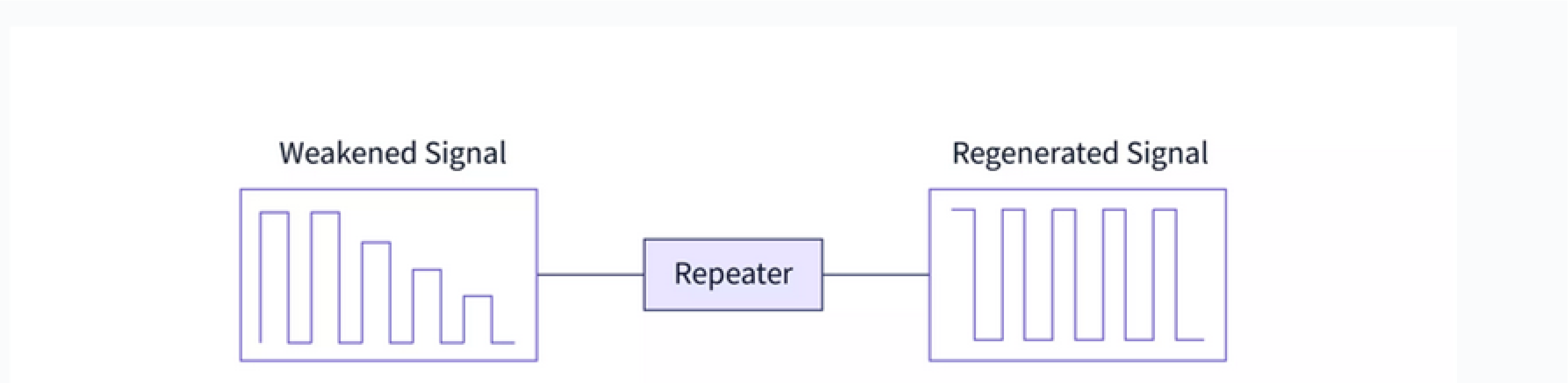
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type (8-bit)								Code (8-bit)								Checksum (16-bit)															
Rest of Header (32 bit)																															

Control Messages

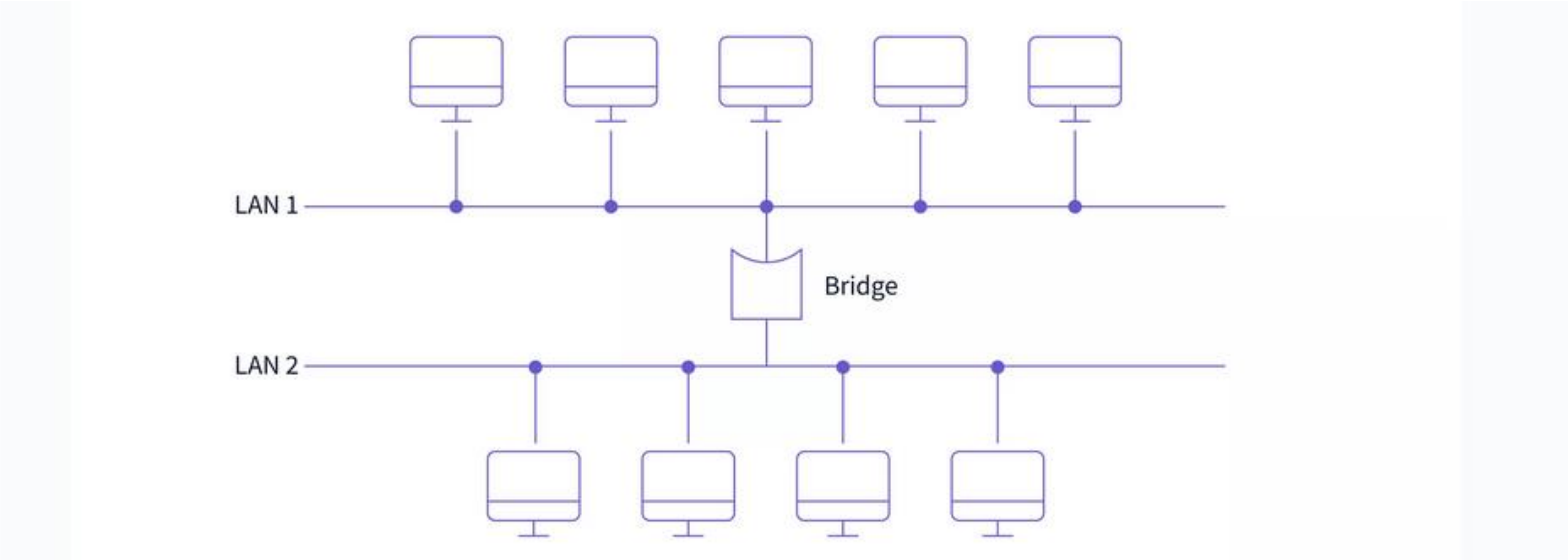
Message Type	Description
Echo request	Ask a machine if it's alive
Echo reply	Yes, I'm alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

Message Type	Description
Destination unreachable	Packet couldn't be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Redirect	Teach a router about geography

Repeater

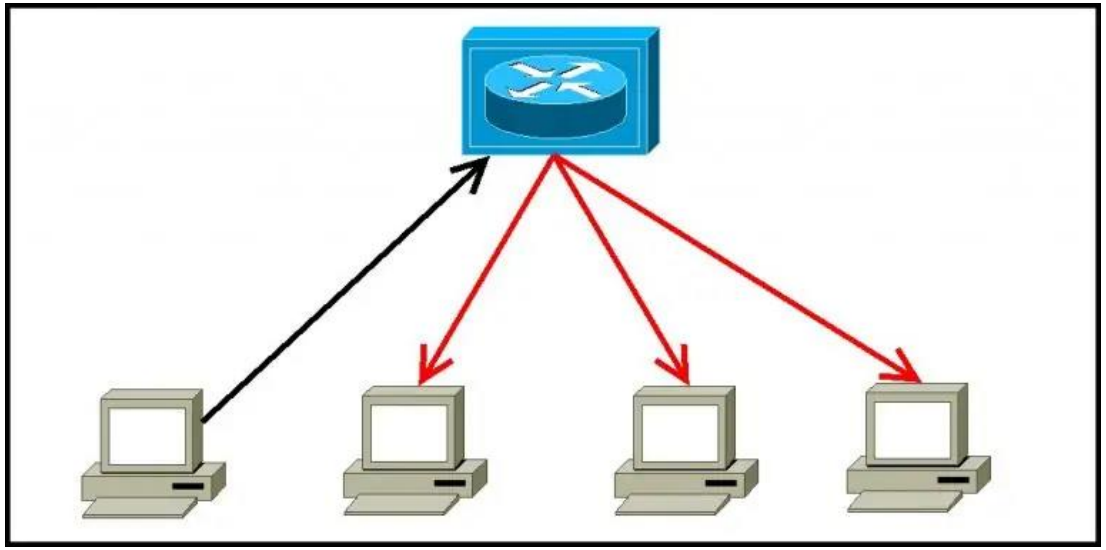


Bridge

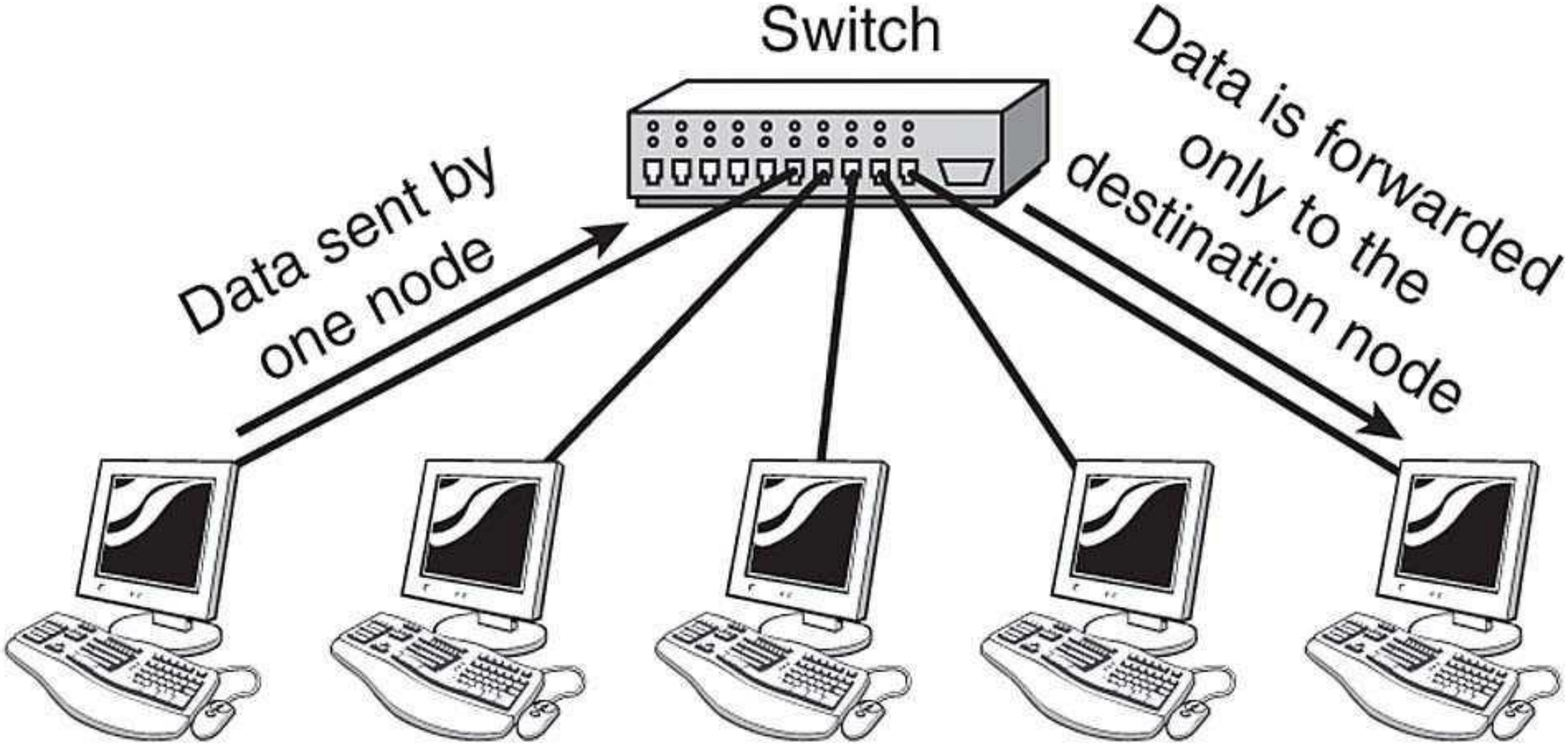


Hub

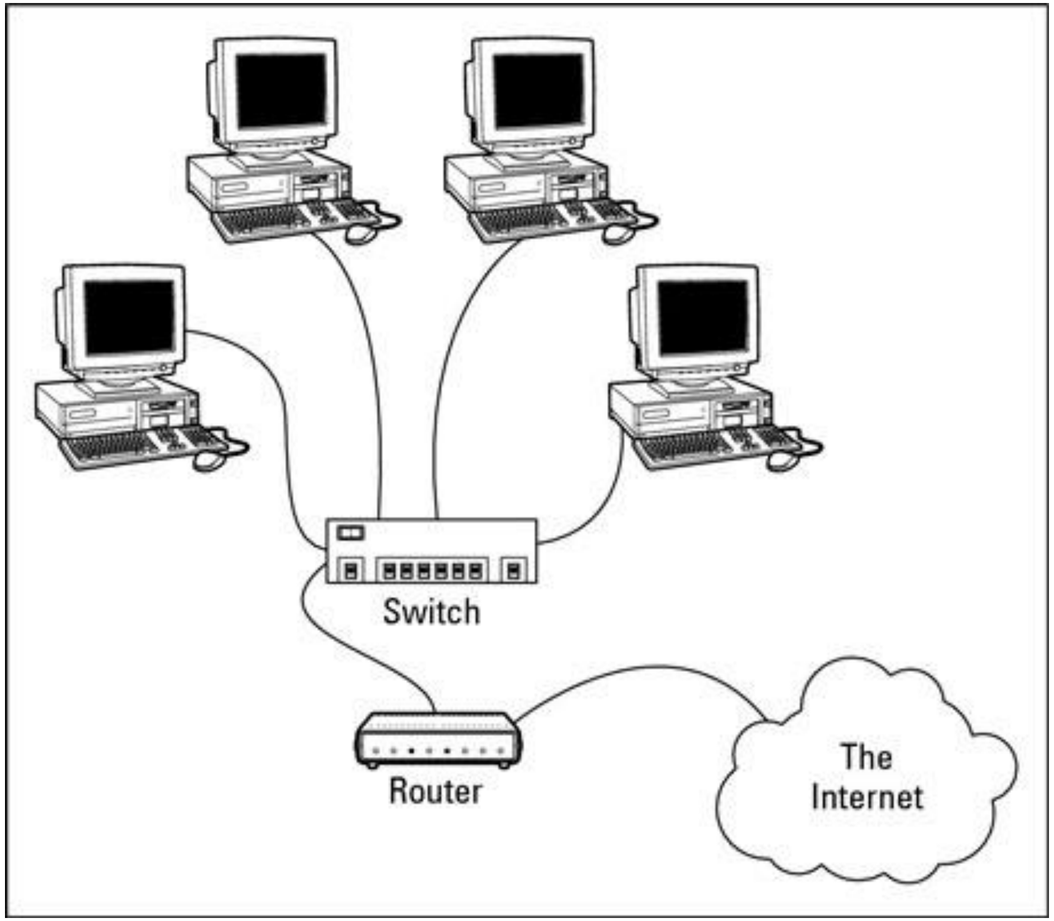
NETGEAR
Ethernet Hub
EN 104TP
Bay Networks
NETGEAR HUB EN104TP
Link
Rx
Pwr
Col
Normal / Uplink
1
2
3
4



Switch


Switch
Data sent by one node
Data is forwarded only to the destination node

Router

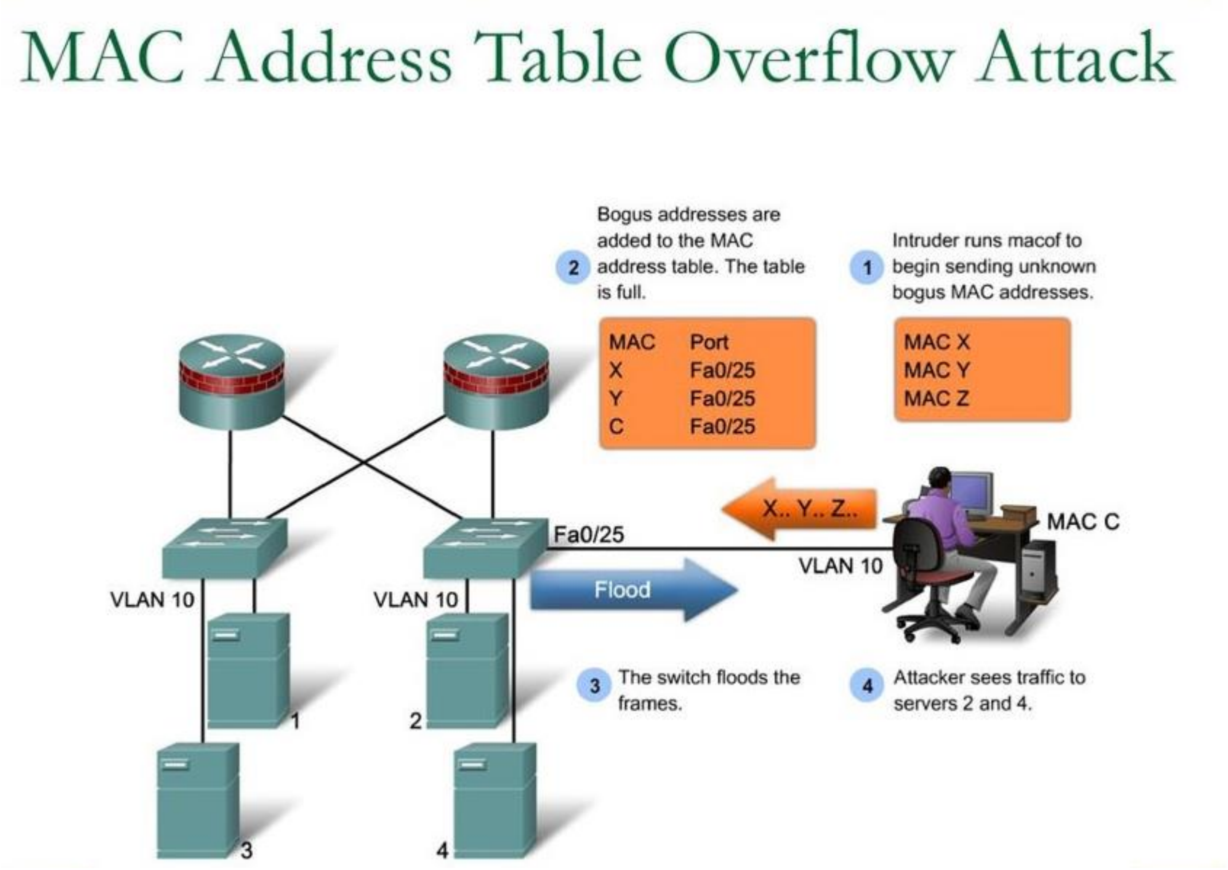


TCP/IP Vulnerability

- Physical layer
  - Fiber cable cuts
  - Wireless link jamming
  - Copper cable influenced by electromagnetic fields
  - Application of high voltage on copper wire

Data link layer

CAM table overflows



MAC Address Table Overflow Attack

1 Intruder runs macof to begin sending unknown bogus MAC addresses.

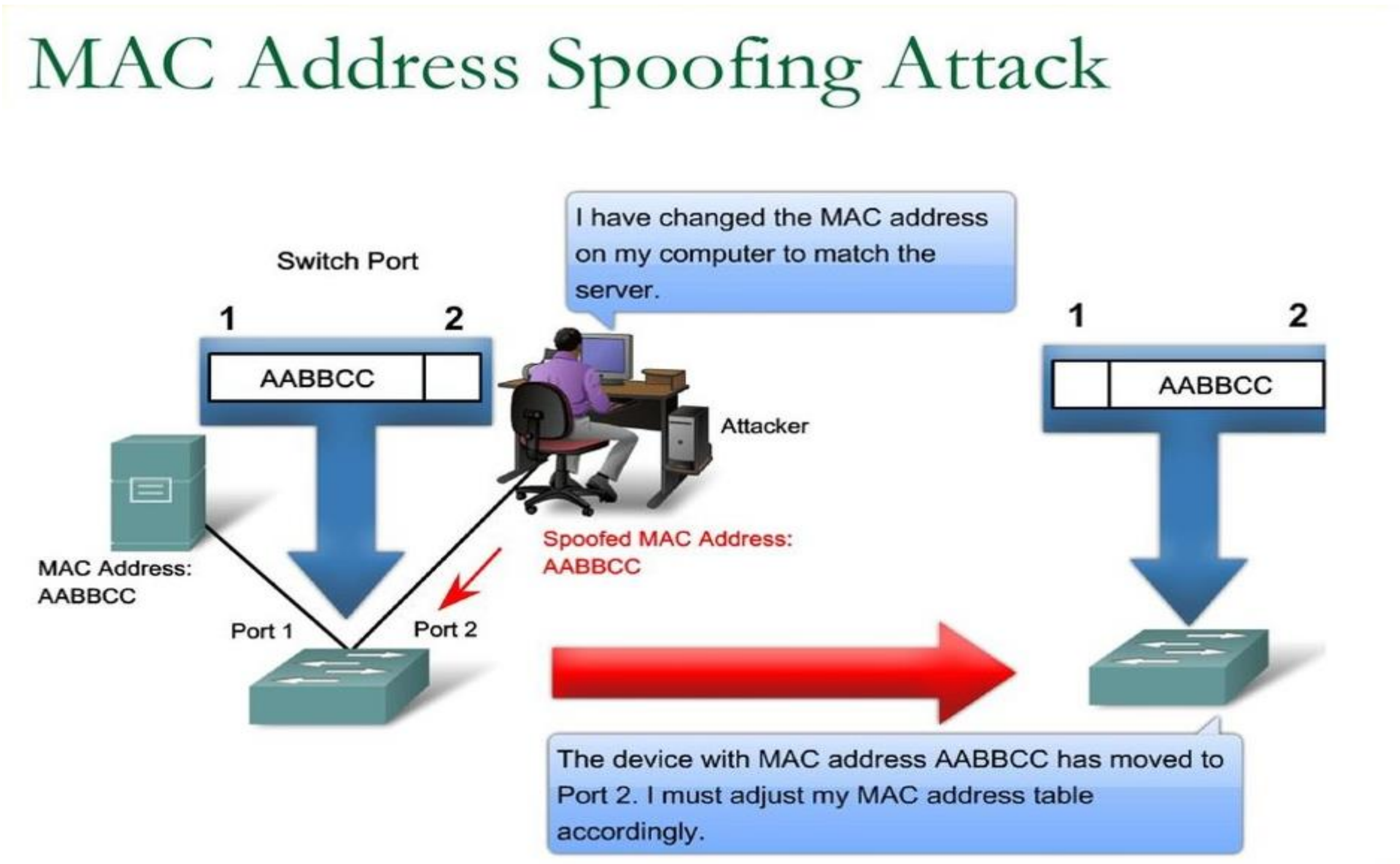
2 Bogus addresses are added to the MAC address table. The table is full.

MAC	Port
X	Fa0/25
Y	Fa0/25
C	Fa0/25

3 The switch floods the frames.

4 Attacker sees traffic to servers 2 and 4.

Data link layer

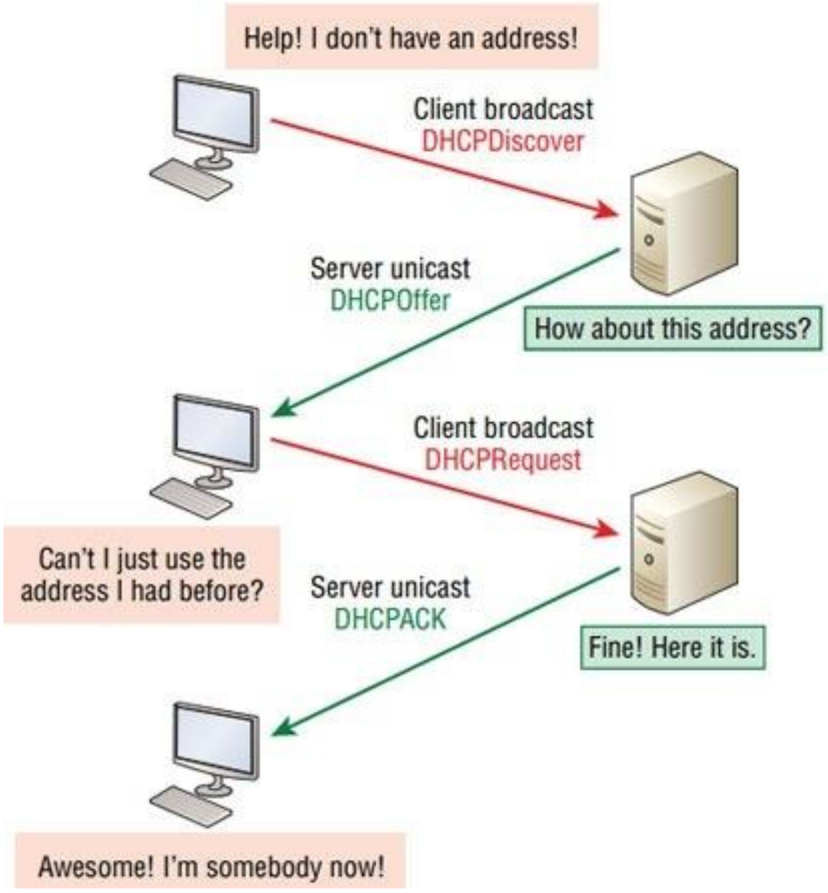


MAC Address Spoofing Attack

I have changed the MAC address on my computer to match the server.

The device with MAC address AABBCC has moved to Port 2. I must adjust my MAC address table accordingly.

Normal DHCP process



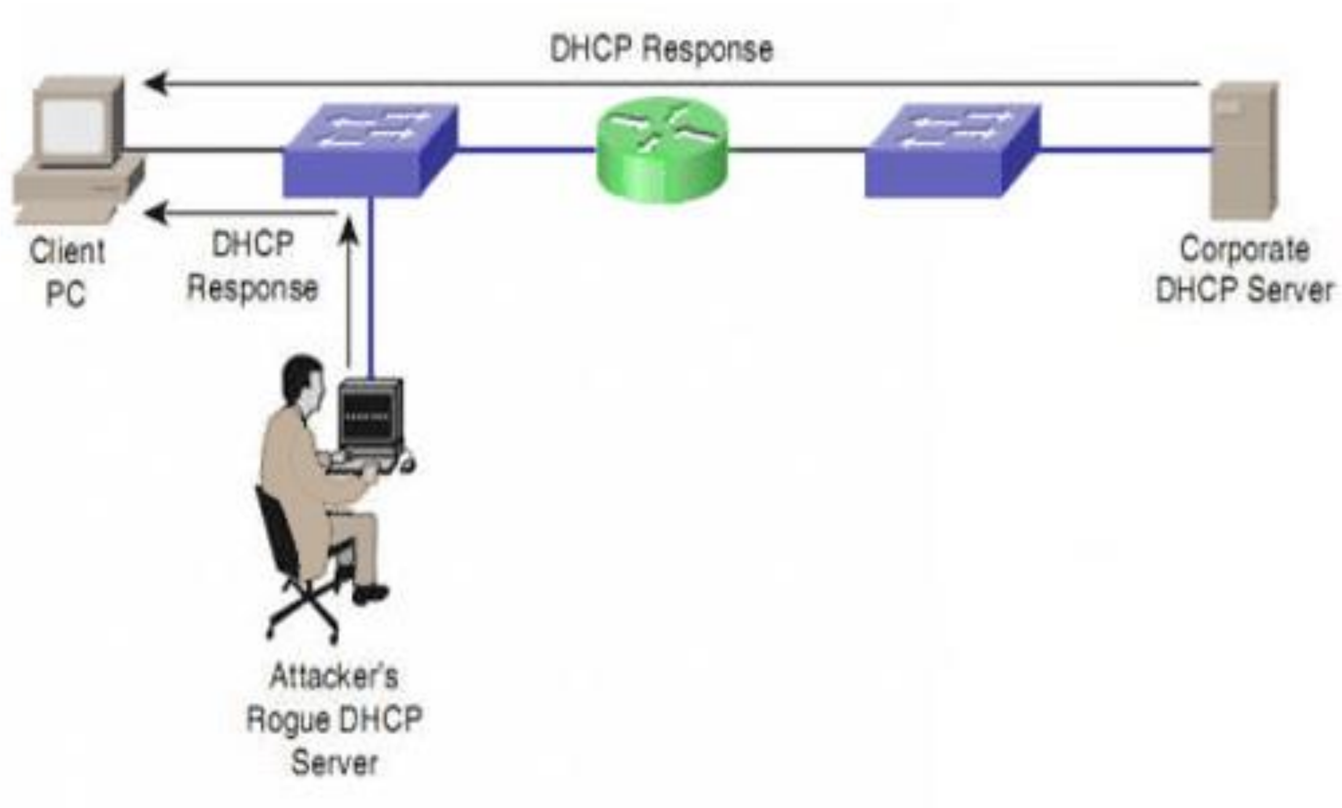
DHCP spoofing

The purpose behind this attack is to send a reply to the victim machine before the real DHCP does. In case we are able to successfully accomplish this, we are able to manipulate the following things:

1. The IP address of the victim
2. Default gateway

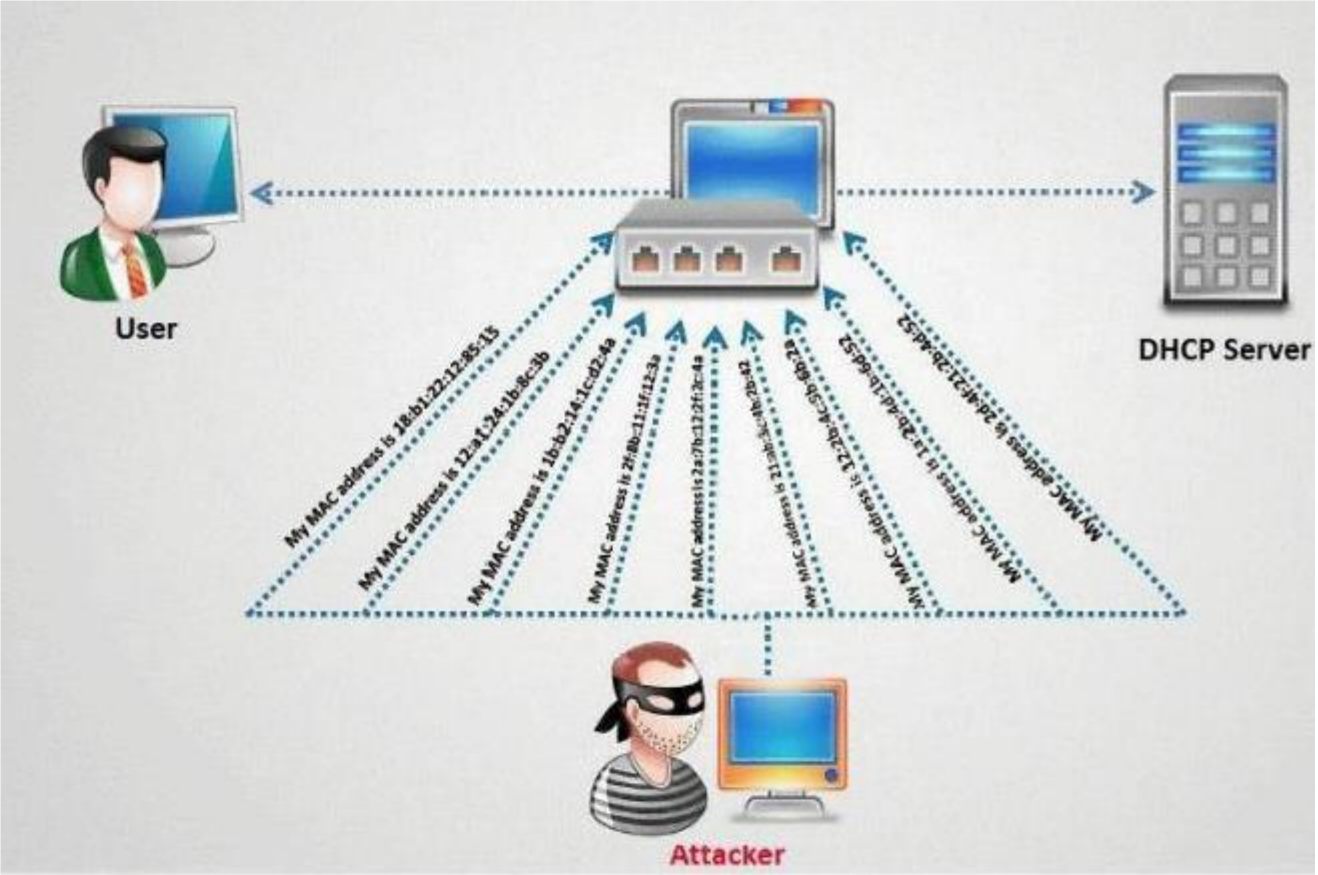
3. DNS address

link: https://latesthackingnews.com/2017/10/18/dhcp-spoofing/

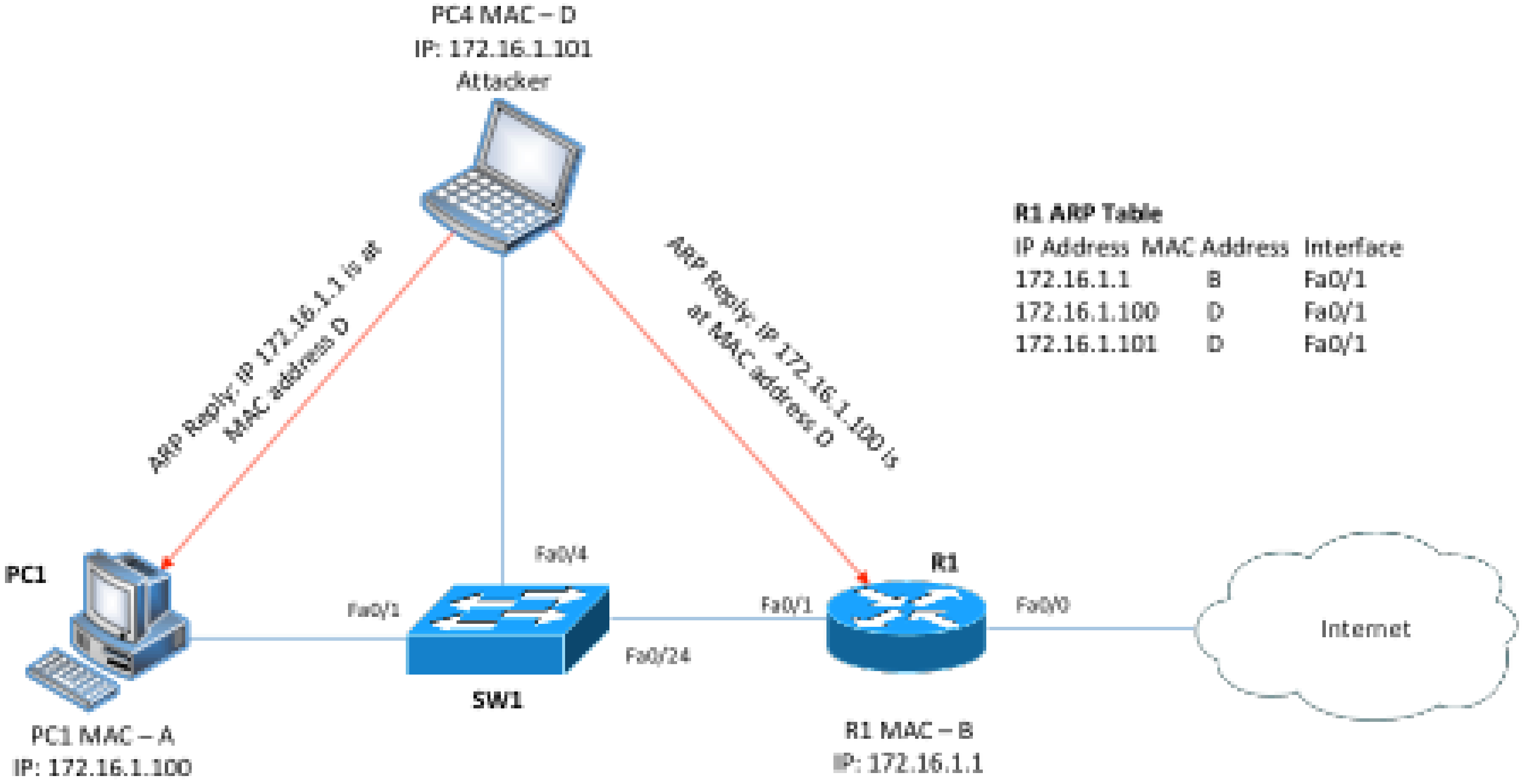


DHCP starvation

- A Modest attack vector DHCP Starvation attack happens when attacker sends large number of **DHCP request packets** with spoofed MAC Addresses.
- Multiple broadcast of Discover request allots the available IP addresses and exhausts the full range of IP addresses.
- So when a real user want to connect with the router, automatically the request will be denied because all the available **IP addresses were exhausted** by the attack.
- Simply we can say it leads to a **DOS attack** in router


User
DHCP Server
My MAC address is 18:b1:22:12:85:15
My MAC address is 12:a1:24:1b:8c:3b
My MAC address is 1b:b2:14:1c:d2:4a
My MAC address is 2f:8b:11:1f:12:3a
My MAC address is 2a:7b:12:2f:3c:4a
My MAC address is 21:ab:3c:4b:2b:42
My MAC address is 12:2b:4c:5b:6b:2a
My MAC address is 13:3b:4d:1b:6d:52
My MAC address is 2d:4f:21:2b:4d:52
Attacker

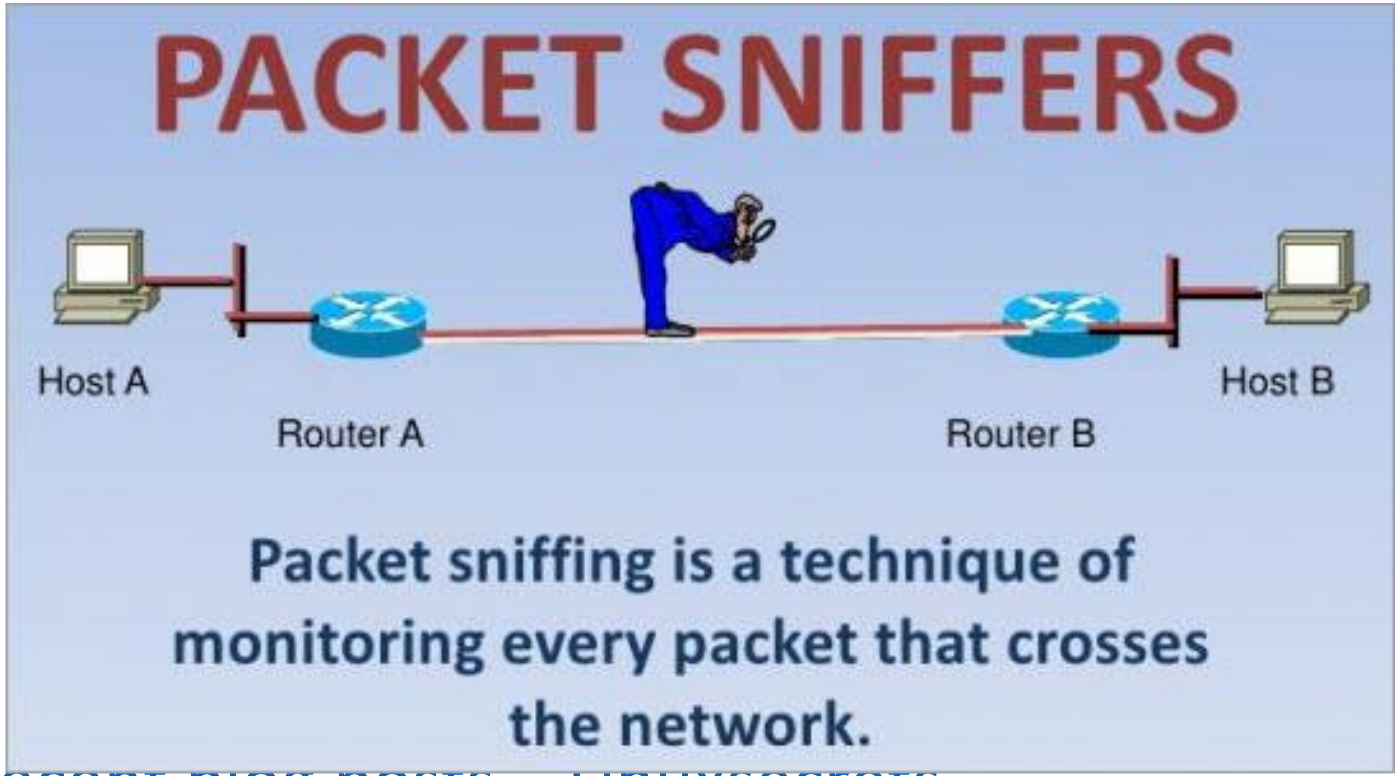
ARP Spoofing



R1 ARP Table

IP Address	MAC Address	Interface
172.16.1.1	B	Fa0/1
172.16.1.100	D	Fa0/1
172.16.1.101	D	Fa0/1

Network layer

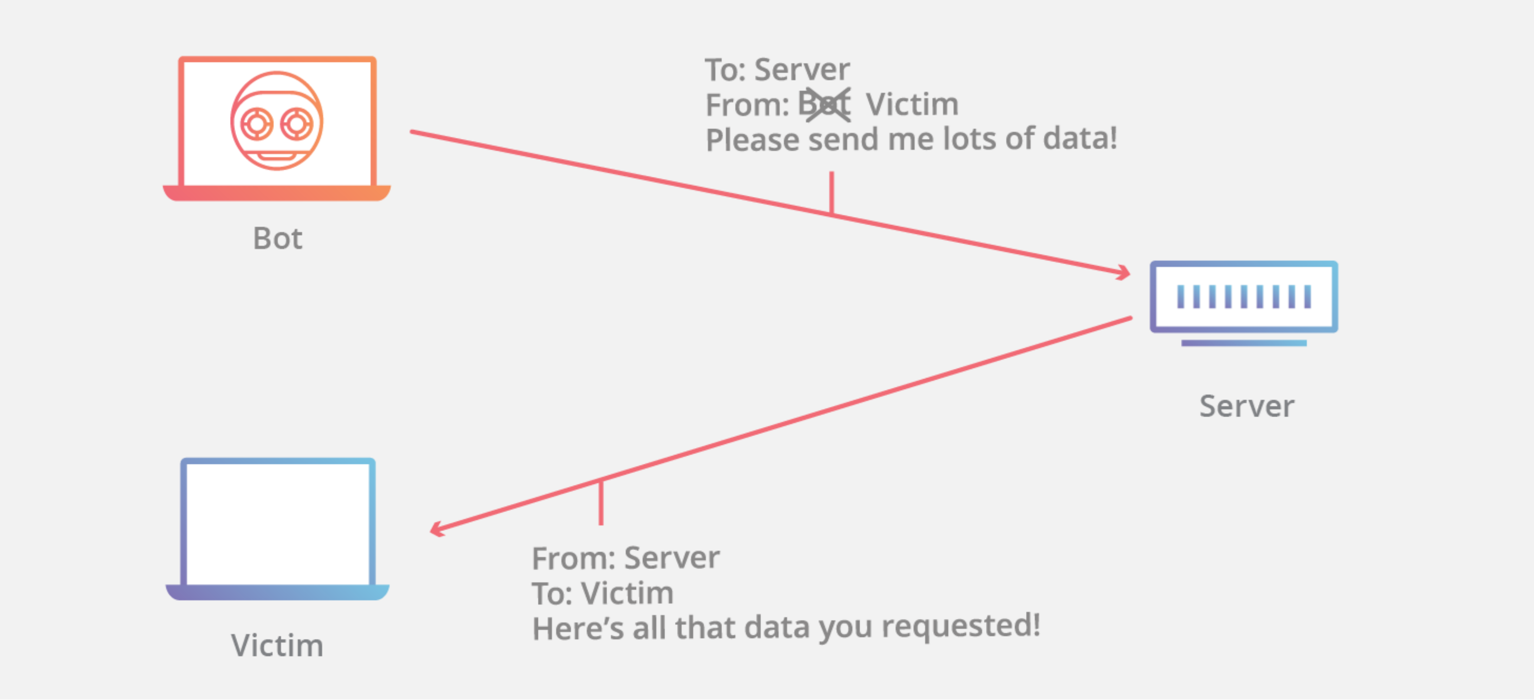


PACKET SNIFFERS

Packet sniffing is a technique of monitoring every packet that crosses the network.

Source-Recent blog posts – Linuxsecrets

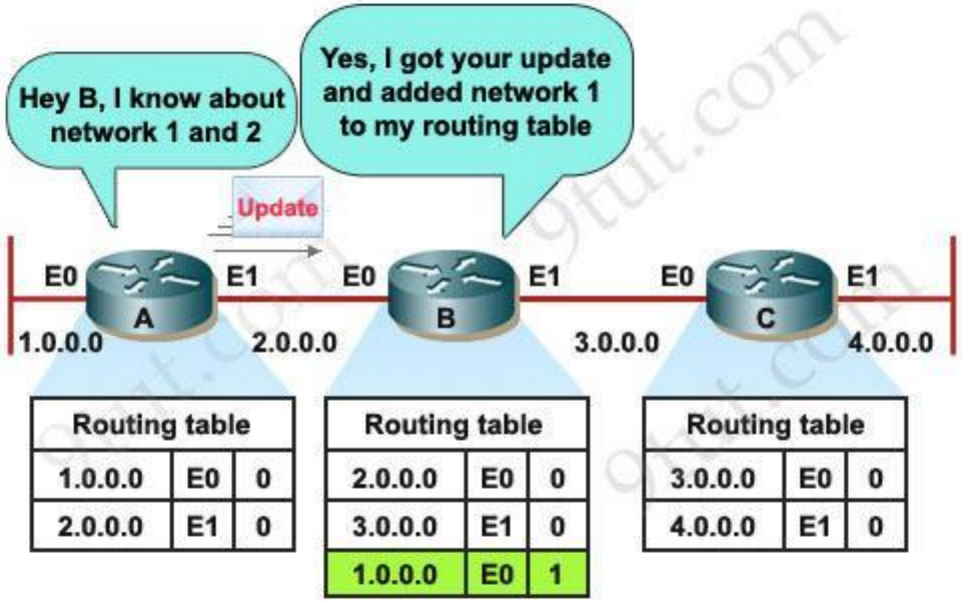
- IP spoofing



To: Server
From: ~~Bot~~ Victim
Please send me lots of data!

From: Server
To: Victim
Here’s all that data you requested!

- RIP Routing attack


Hey B, I know about network 1 and 2
Yes, I got your update and added network 1 to my routing table
Update
E0
E1
A
B
C
1.0.0.0
2.0.0.0
3.0.0.0
4.0.0.0

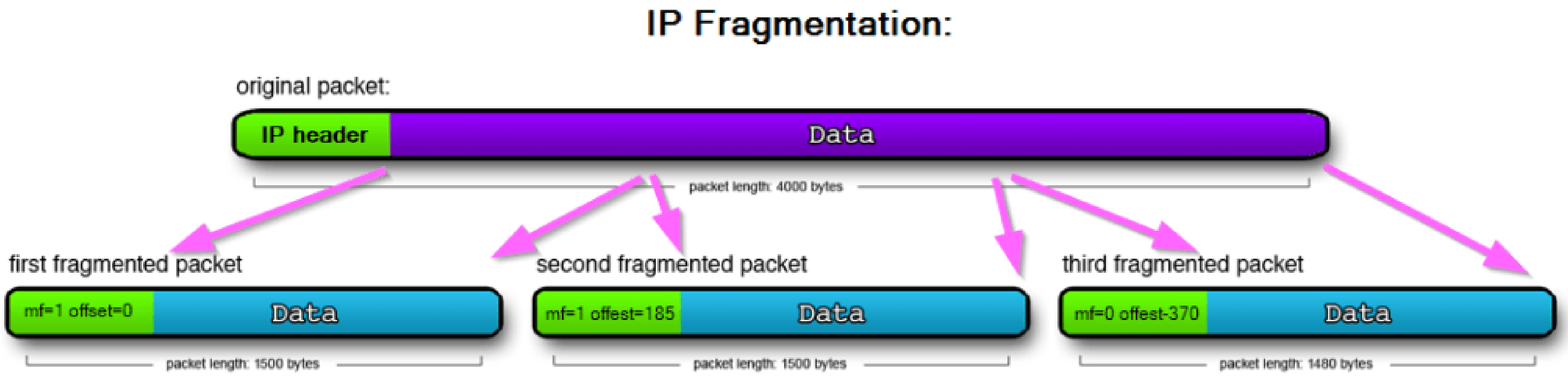
Routing table		
1.0.0.0	E0	0
2.0.0.0	E1	0

Routing table		
2.0.0.0	E0	0
3.0.0.0	E1	0
1.0.0.0	E0	1

Routing table		
3.0.0.0	E0	0
4.0.0.0	E1	0

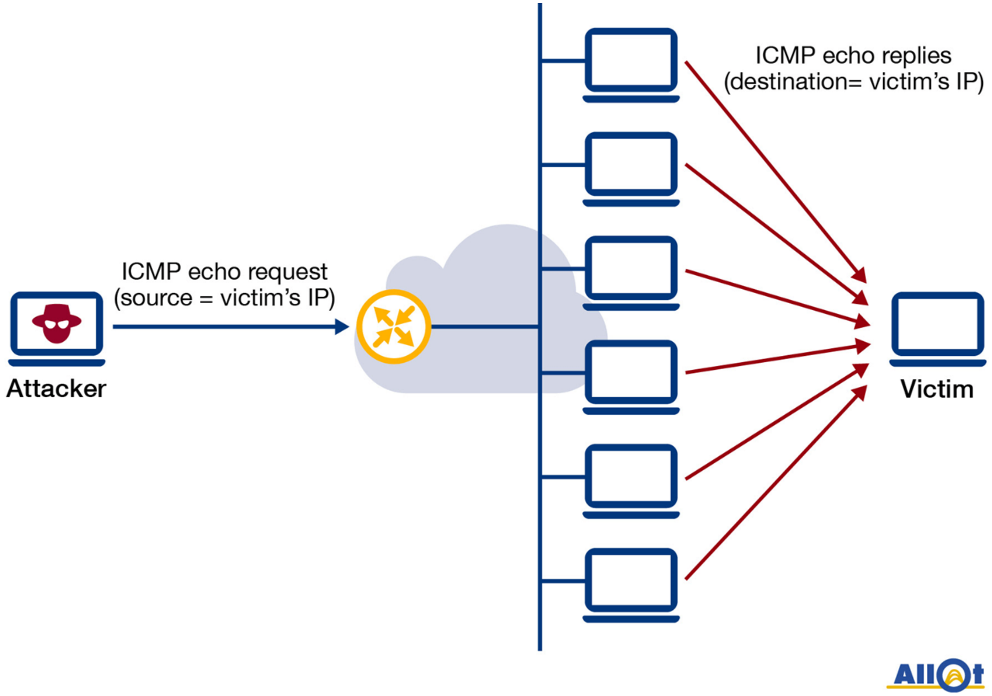
- Source-RIP (Routing Information Protocol) – Rahul Gupta (wordpress.com)

- Fragmentation attack



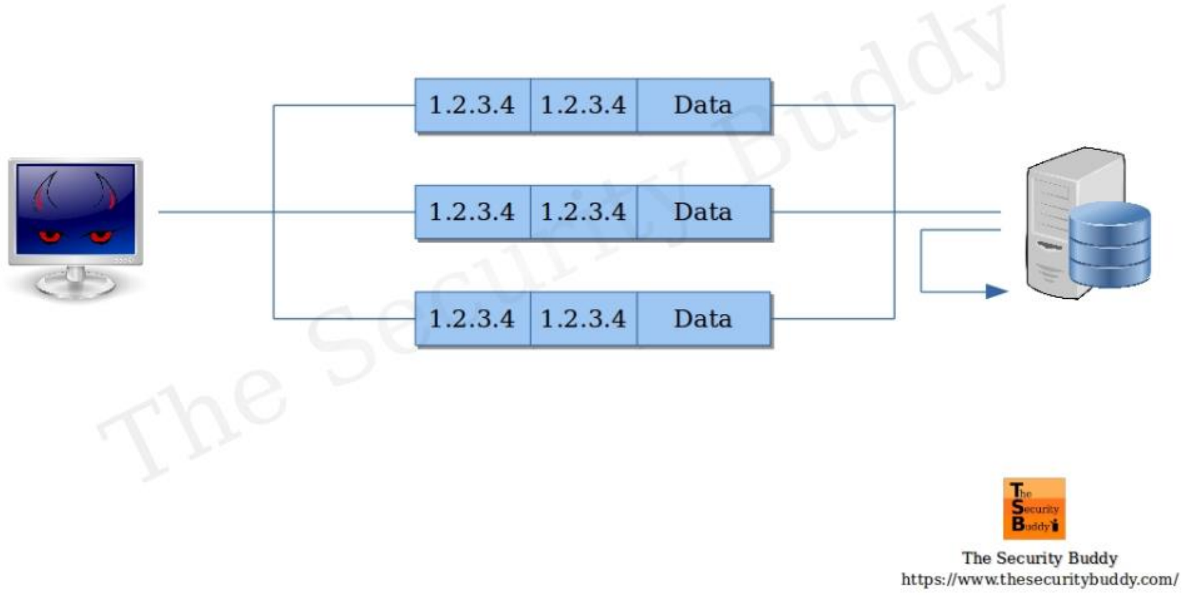
- Source-NetFlow Security: Detecting IP Fragmentation Exploits with Scrutinizer (plixer.com)

- ICMP attack

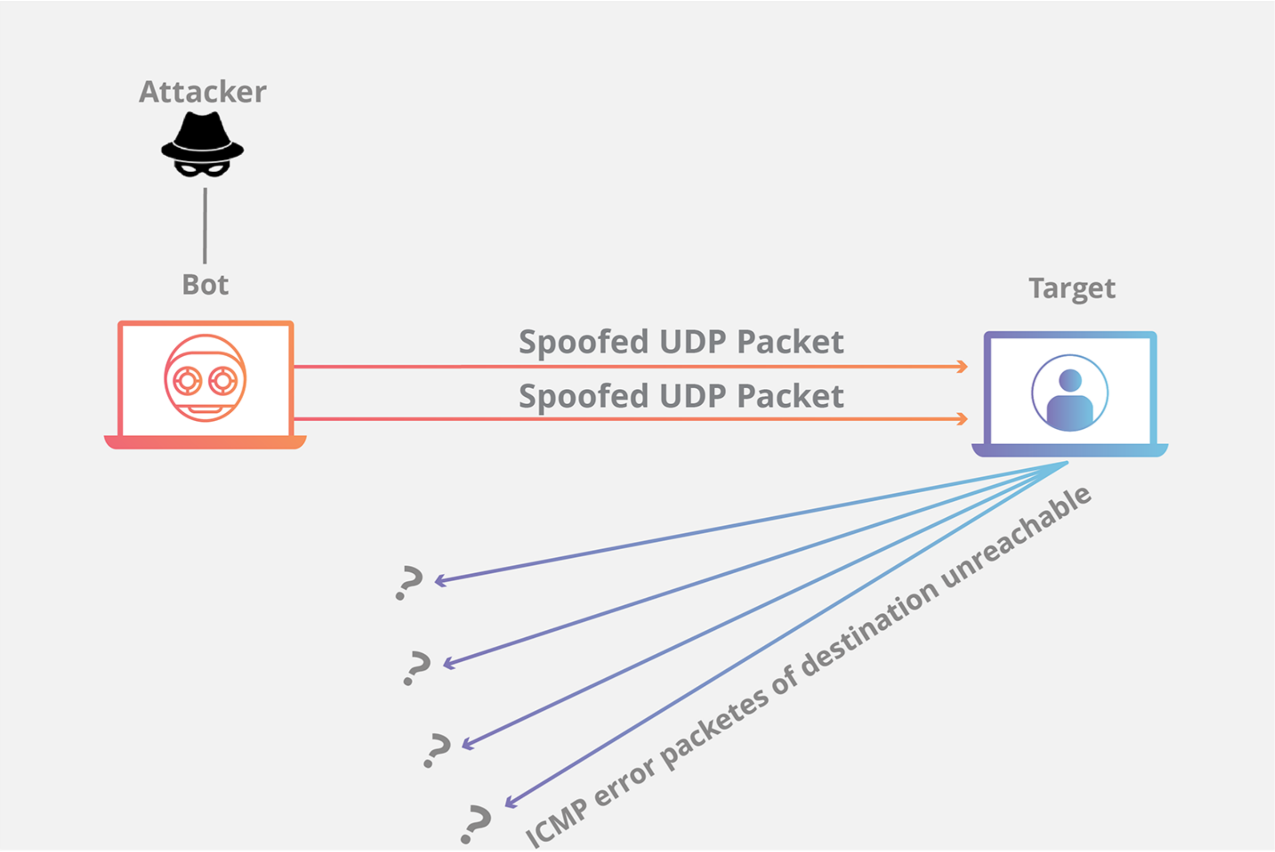

ICMP echo replies
(destination= victim's IP)
ICMP echo request
(source = victim's IP)
Attacker
Victim
Allot

Transport Layer

- TCP Land attack

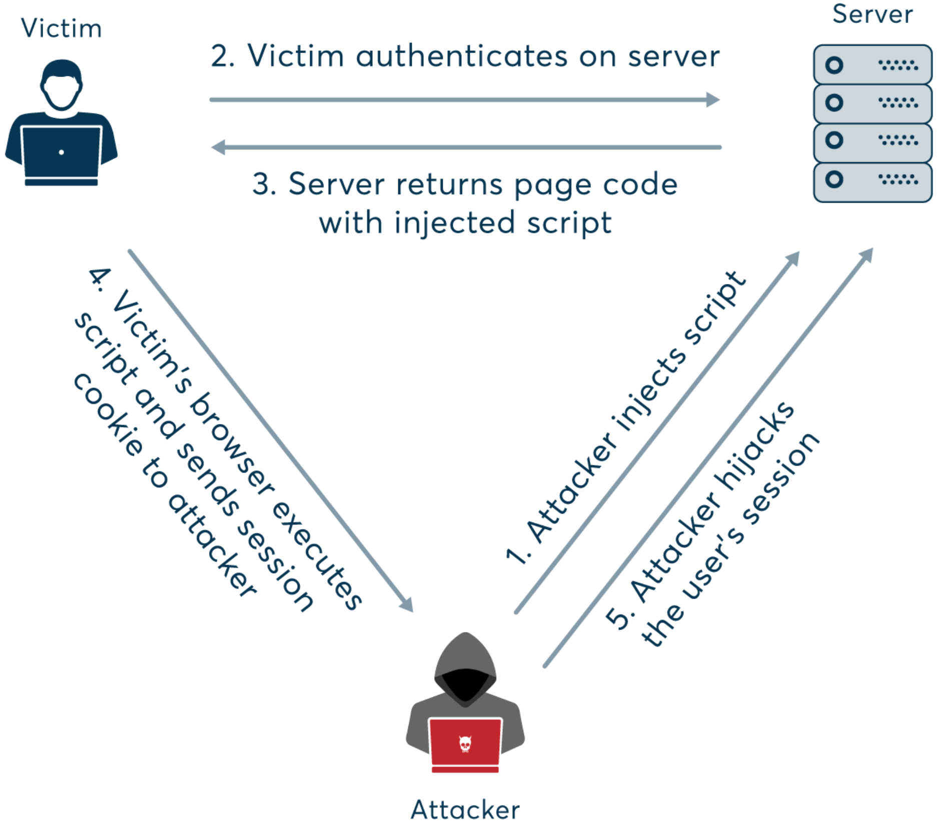


- UDP flooding attack

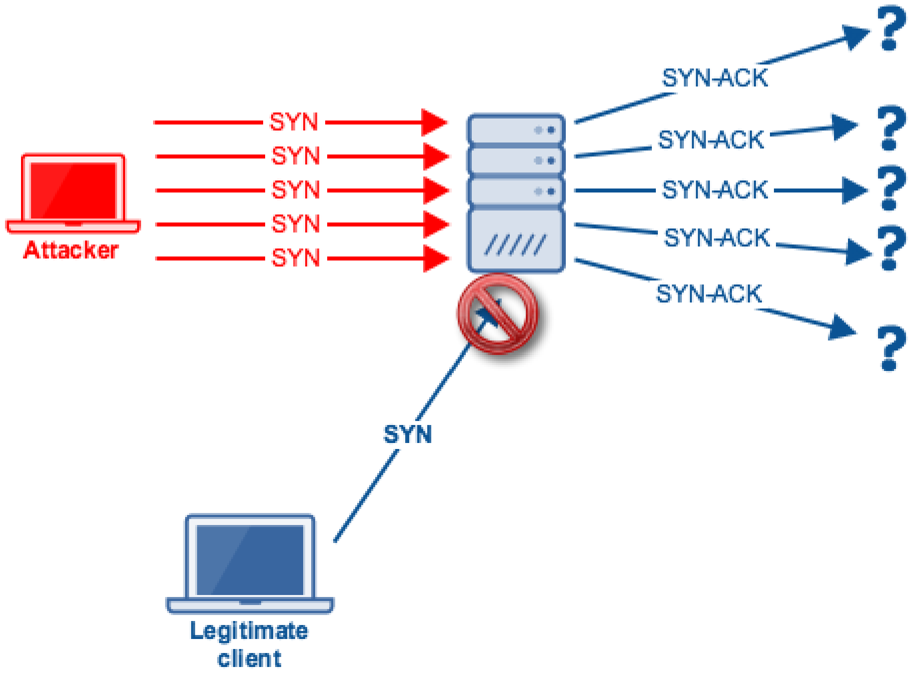


- TCP and UDP port scanning techniques

- Connection Hijacking


Victim
Server
2. Victim authenticates on server
3. Server returns page code with injected script
4. Victim's browser executes script and sends session cookie to attacker
1. Attacker injects script
5. Attacker hijacks the user's session
Attacker

- TCP SYN attack



Source-[These 6 DNS Attacks Threaten Your Business - Defence Intelligence Blog (defintel.com)]

Layer 5,6 and 7: security threats

- BIND Domain Name system
- Apache web server
- Version control system
- Mail transport system
- Simple network management protocol