Internetworking with TCP/IP

MCSC202

Course Content

- IPv4 addressing (Classful and Classless), Network Address Translation
- IPv6 addressing
- Network Layer Routing algorithm (e.g. distance-vector, link-state, Flooding, BGP, OSPF
- Transport layer (connection establishment, connection release, congestion control, TCP and UDP)
- Internet QoS (architecture, application requirement)
- Software Defined Networking (SDN, OpenFlow)
- Mobility and Mobile IP
- Any other topic (multicast routing, Network Management)

Reference Books:

- **Computer Networking: A Top-Down Approach**, by Ames Kurose, Keith Ross
- **Computer Networks - Andrew S Tanenbaum**
- Douglas E Comer, **Internetworking with TCP/IP Principles, Protocol, and Architecture**, Volume I, 6th Edition, Pearson Education, 2015.
- Research Publications

Marks Distribution for Internal Assessment

- Internal Assessment = 30
- Mid-term: 15
- Presentation/Project: 10
- Attendance: 5
- End-term Exam: 70

Expectations and Policies

- Regular attendance and active participation.
- Respect deadlines for Projects/Presentations.
- Mid-term (Syllabus) and Projects/Presentations guidelines.

- **Don't message/ WhatsApp me on my personal number**.
- Always email your issue to rkasana@cs.du.ac.in

Revision

Computer Networks

1. The Protocol Data Unit for the Application layer in the Internet Stack (or TCP/IP) is called

(A) Message.

(B) Datagram

(C) Segments

(D) Frame

1. The Protocol Data Unit for the Application layer in the Internet Stack (or TCP/IP) is called
(A) Message.
(B) Datagram
(C) Segments
(D) Frame

Answer: A (Message)

- For the Application, Presentation and Session layers, the PDU is the message.
- For the Transport layer, PDU is segment for TCP and a datagram for UDP
- For the Network layer, PDU is a packet
- For the Datalink layer, PDU is frames
- For physical layer, PDU is a stream of bits

2. Which of the following transport layer protocols is used to support electronic mail? [GATE CSE 2012]
(A) SMTP
(B) IP
(C) TCP
(D) UDP

2. Which of the following transport layer protocols is used to support electronic mail? [GATE CSE 2012]
(A) SMTP
(B) IP
(C) TCP
(D) UDP

Solution: (C)

Application	Application-Layer Protocol	Underlying Transport Protocol
Electronic mail	SMTP	TCP
Remote terminal access	Telnet	TCP
Web	HTTP	TCP
File transfer	FTP	TCP
Remote file server	NFS	Typically UDP
Streaming multimedia	typically proprietary	UDP or TCP
Internet telephony	typically proprietary	UDP or TCP
Network management	SNMP	Typically UDP
Routing protocol	RIP	Typically UDP
Name translation	DNS	Typically UDP

Figure 3.6 ♦ Popular Internet applications and their underlying transport protocols

Q.3: In the IPv4 addressing format, the number of networks allowed under Class C addresses is [GATE CSE 2012]

(A) 2^14

(B) 2^7

(C) 2^21

(D) 2^24

Q.3: In the IPv4 addressing format, the number of networks allowed under Class C addresses is [GATE CSE 2012]

(A) 2^14

(B) 2^7

(C) 2^21

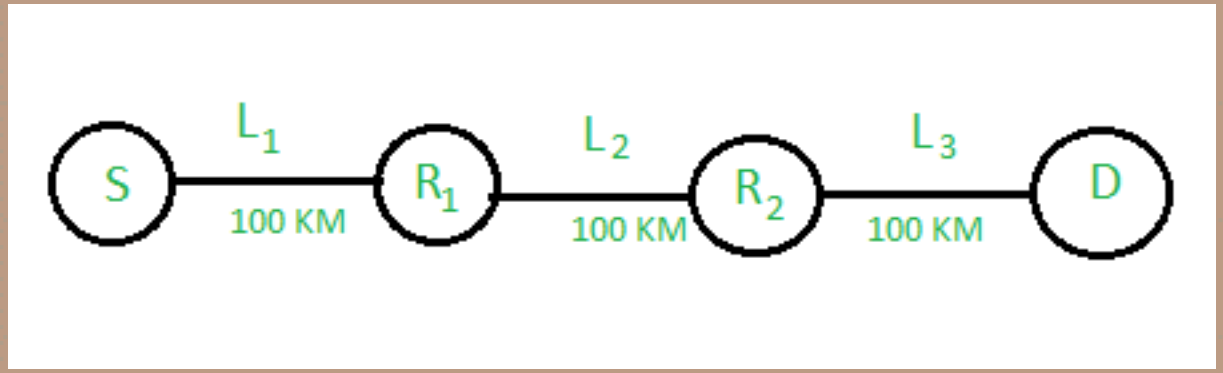
(D) 2^24

Solution: (C)
In class C, 8 bits are reserved for Host ID, and 24 bits are reserved for Network ID.
Out of these 24 Network ID bits, the leading 3 bits are fixed as 110.
So, the remaining 21 bits can be used for different networks.

Five Different Classes of IPv4 Addresses

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	**0**XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^{7}
Class B	128 – 191	**10**XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 – 223	**110**XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^{8}-2$	2^{21}
Class D (Multicast)	224 – 239	**1110**XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	**1111**XXXX	240.0.0.0-255.255.255.255			

Q.4: Consider a source computer (S) transmitting a file of size 106 bits to a destination computer (D) over a network of two routers (R1 and R2) and three links (L1, L2, and L3). L1 connects S to R1; L2 connects R1 to R2; and L3 connects R2 to D. Let each link be of length 100km. Assume signals travel over each link at a speed of 10^8 meters per second. Assume that the link bandwidth on each link is 1Mbps. Let the file be broken down into 1000 packets, each of size 1000 bits. Find the total sum of transmission and propagation delays in transmitting the file from S to D. [GATE CSE 2012]



(A) 1005ms

(B) 1010ms

(C) 3000ms

(D) 3003ms

Answer: 1005 msec

Propagation delay to travel from S to R1 = (Distance) / (Link Speed) = 10^5/10^8 = 1ms

Total prorogation delay to travel from S to D = 3*1 ms = 3ms

Total Transmission delay for 1 packet = 3 * (Number of Bits) / Bandwidth = 3*(1000/10^6) = 3ms.

The first packet will take 6ms to reach D.

While the first packet was reaching D, other packets must have been processed in parallel.

So D will receive the remaining packets 1 packet per 1 ms from R2.

So the remaining 999 packets will take 999 ms.

And total time will be 999 + 6 = 1005 ms

IP Addresses with Special meaning (0.0.0.0 - The Lowest Address)

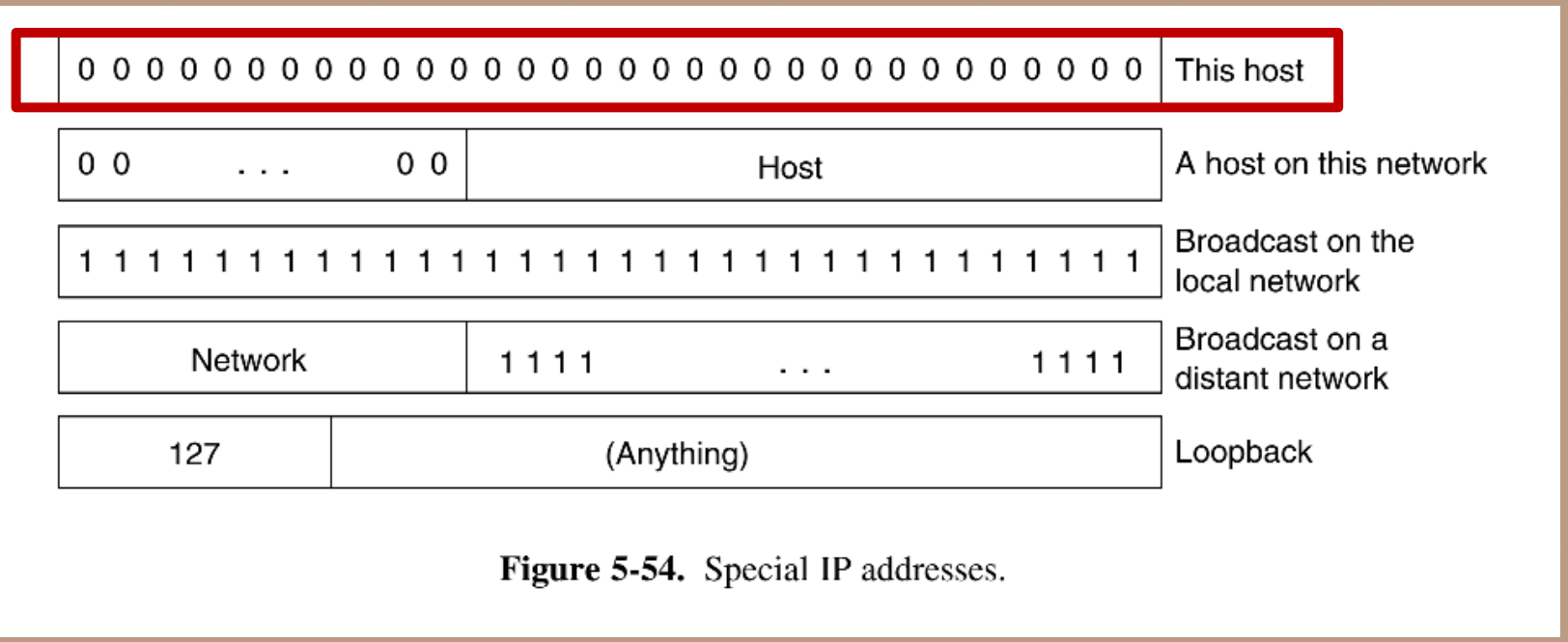


Figure 5-54. Special IP addresses.

- represents "this host" or "this network."
- Used by devices when they are booting up and do not yet have an assigned IP address.
- For example, a host can use 0.0.0.0 as a source address to indicate itself when it doesn't know its own IP address (like during DHCP discovery).

IP Addresses with Special meaning:

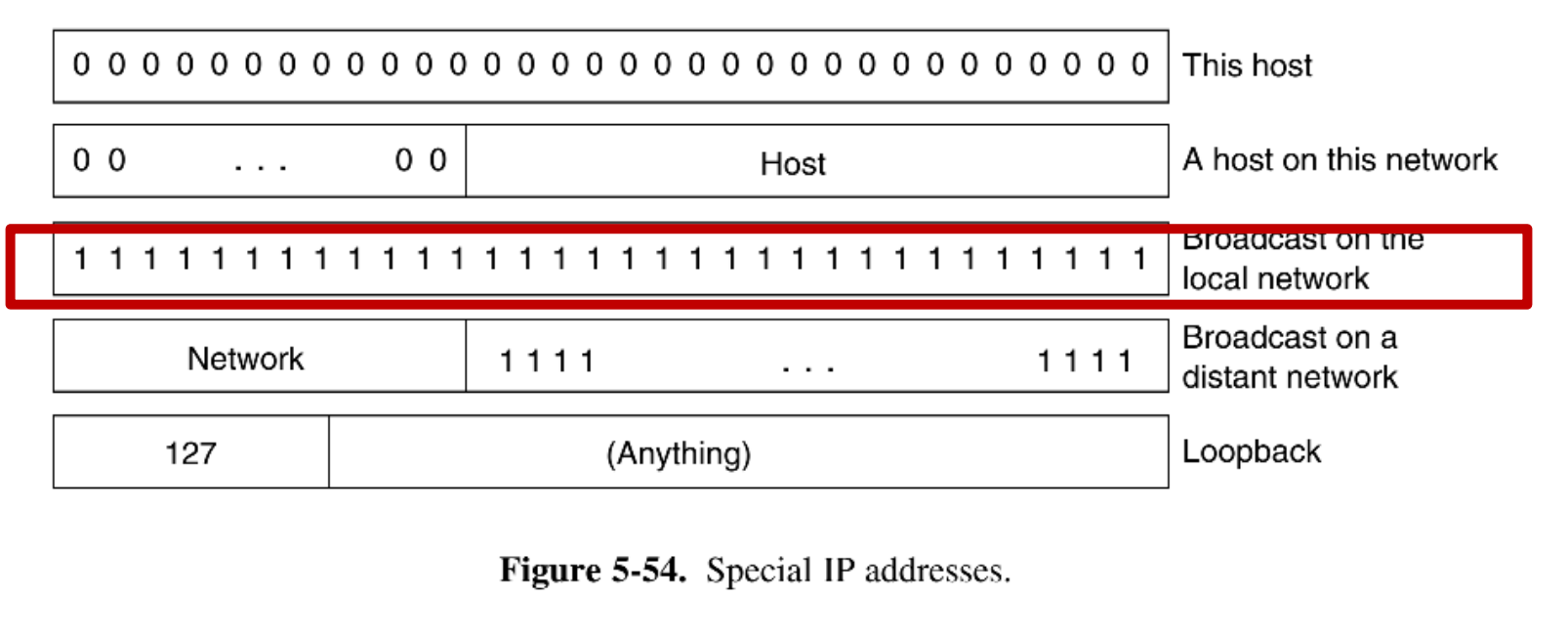


Figure 5-54. Special IP addresses.

IP addresses with 0 as the network number refer to the current network.

These addresses allow machines to refer to their own network without knowing its number

(but they have to know the network mask to know how many 0s to include).

uses the **subnet mask** to determine the **network portion** of its IP address and refers to the **current network** with **0.0.0.0**.

useful for situations like **default routing** or self-reference when communicating within the same network.

IP Addresses with Special meaning(255.255.255.255 - The Highest Address)

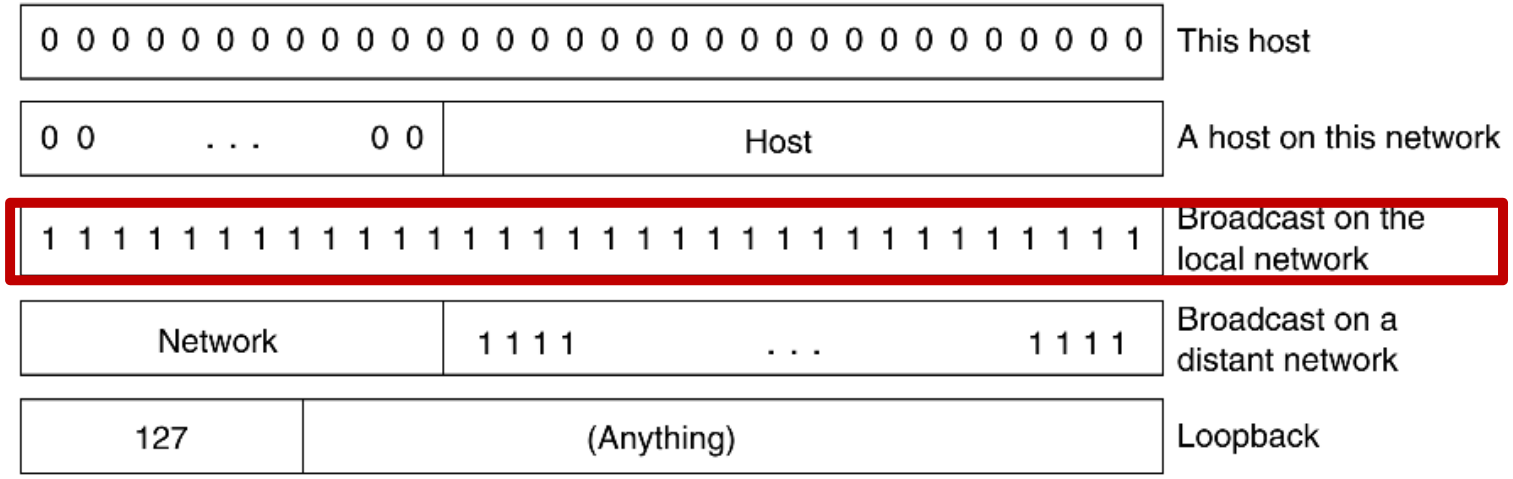


Figure 5-54. Special IP addresses.

- address is the limited broadcast address and is used to send data to all devices on the local network.
- does not leave the local network (LAN) because routers typically do not forward such packets.

IP Addresses with Special meaning:

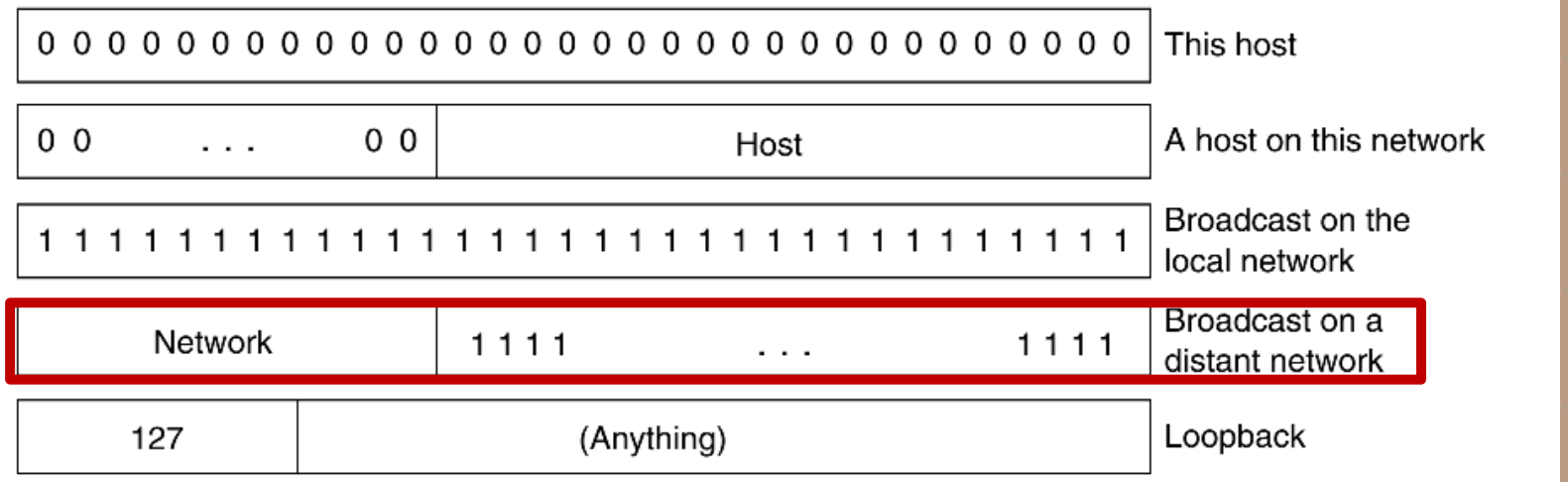


Figure 5-54. Special IP addresses.

- Addresses are used to send broadcast packets to all hosts on a specific remote network.
- Many network administrators disable this type of broadcast - it can be misused for malicious purposes (e.g. , broadcast storms and denial-of-service attacks) - causes congestion and degrading the network's performance.

IP Addresses with Special meaning: Loopback Addresses (127.x.x.x):

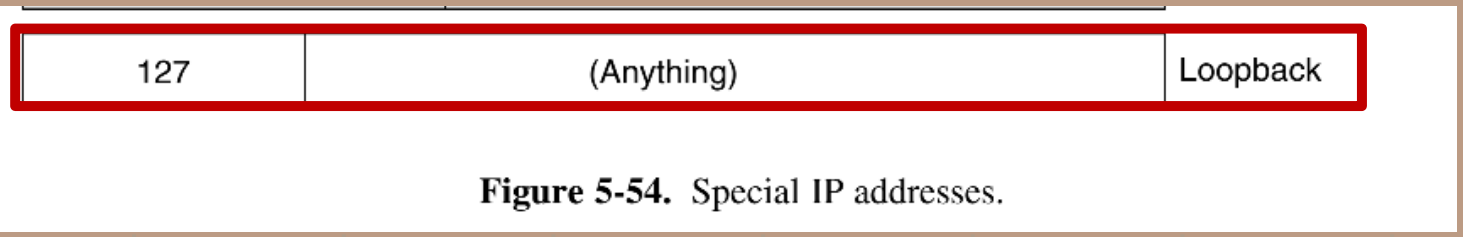


Figure 5-54. Special IP addresses.

1. Reserved for loopback testing, these addresses are used for internal communication within the host.
2. Packets sent to 127.X.X.X are not transmitted on the network wire.
3. These packets are processed internally and treated as if they were received from an external source.

IP Addresses with Special meaning: Loopback Addresses (127.x.x.x):

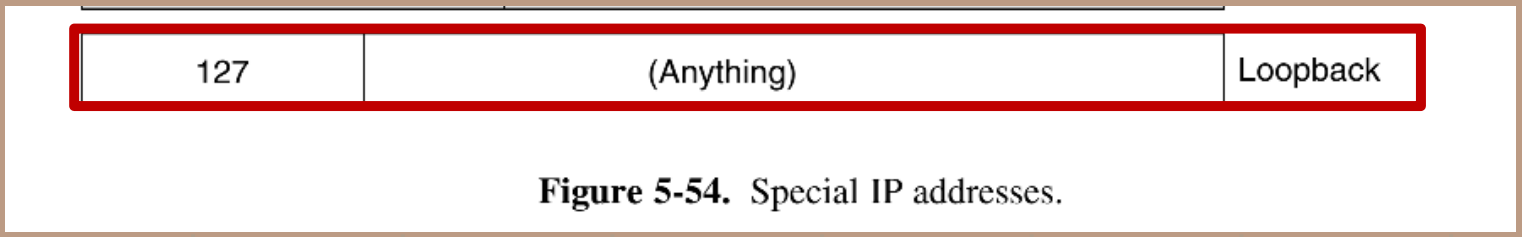


Figure 5-54. Special IP addresses.

- mock TCP/IP Client/Server on the same machine.
- The loopback IP addresses are always available. Hence, use the loopback IP addresses for TCP/IP troubleshooting purposes.
- Useful for testing network applications or configurations without needing an active network connection. For example, 127.0.0.1 is most commonly used to test local servers.

IP Addresses with Special meaning:

0.0.0.0: Temporary or undefined source address during boot or configuration.

255.255.255.255: Broadcast to all devices on the local network.

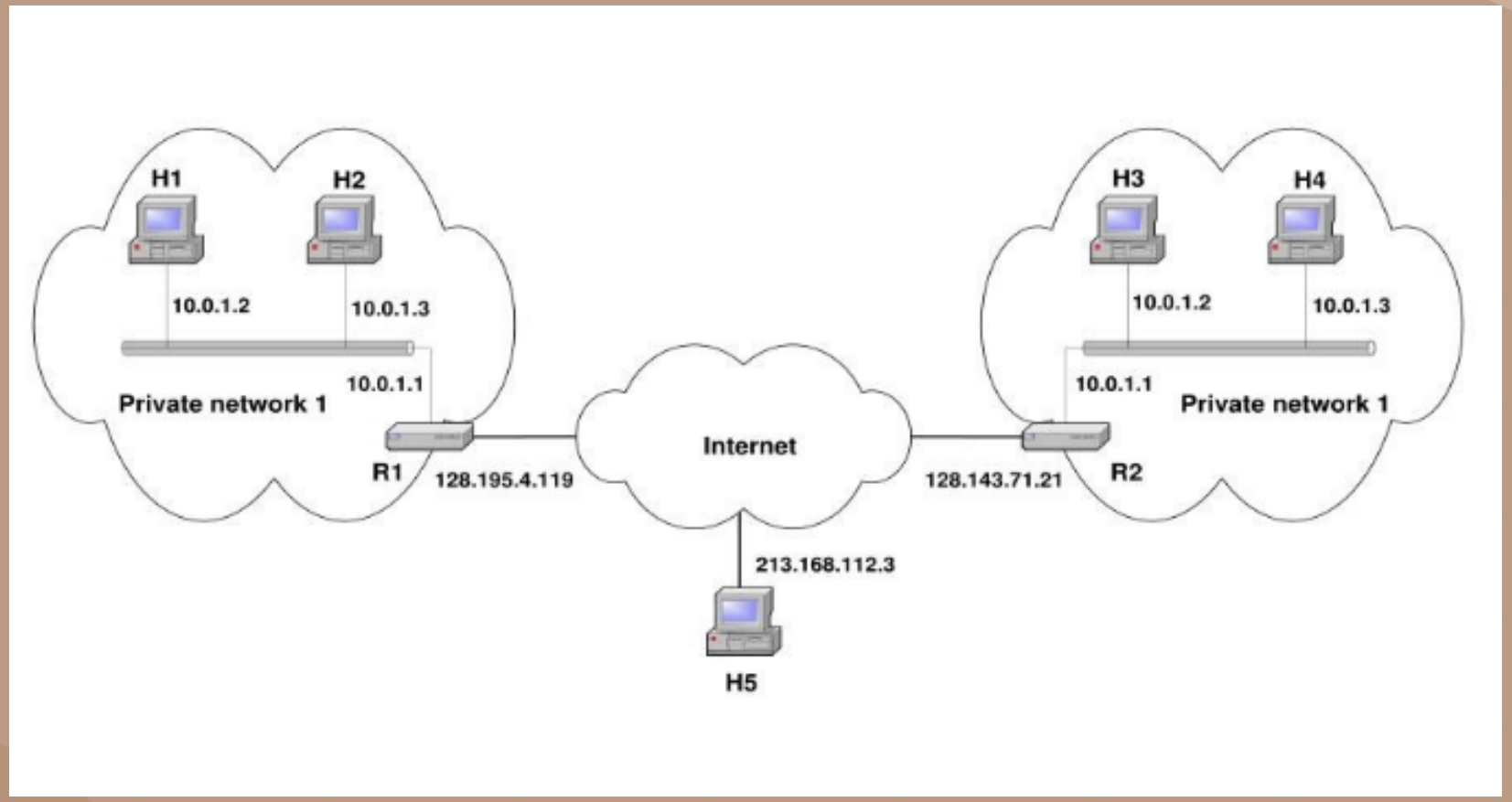
Directed Broadcast (<network>.255): Broadcasting to all devices on a specific remote network.

127.x.x.x: Loopback addresses for internal communication and testing.

Private Networks

- An IP network that is not directly connected to the network.
- IP addresses in a private network can be assigned arbitrarily.
- Not registered and not guaranteed to be globally unique.
- Generally, private networks use addresses from the following experimental address ranges (non-routable addresses):
- 10.0.0.0 – 10.255.255.255/8 (16,777,216 hosts (except for all 0s and all 1s))
- 172.16.0.0 to 172.31.255.255/12 (1,048,576 hosts)
- 192.168.0.0 to 192.168.255.255/16 (65,536 hosts)

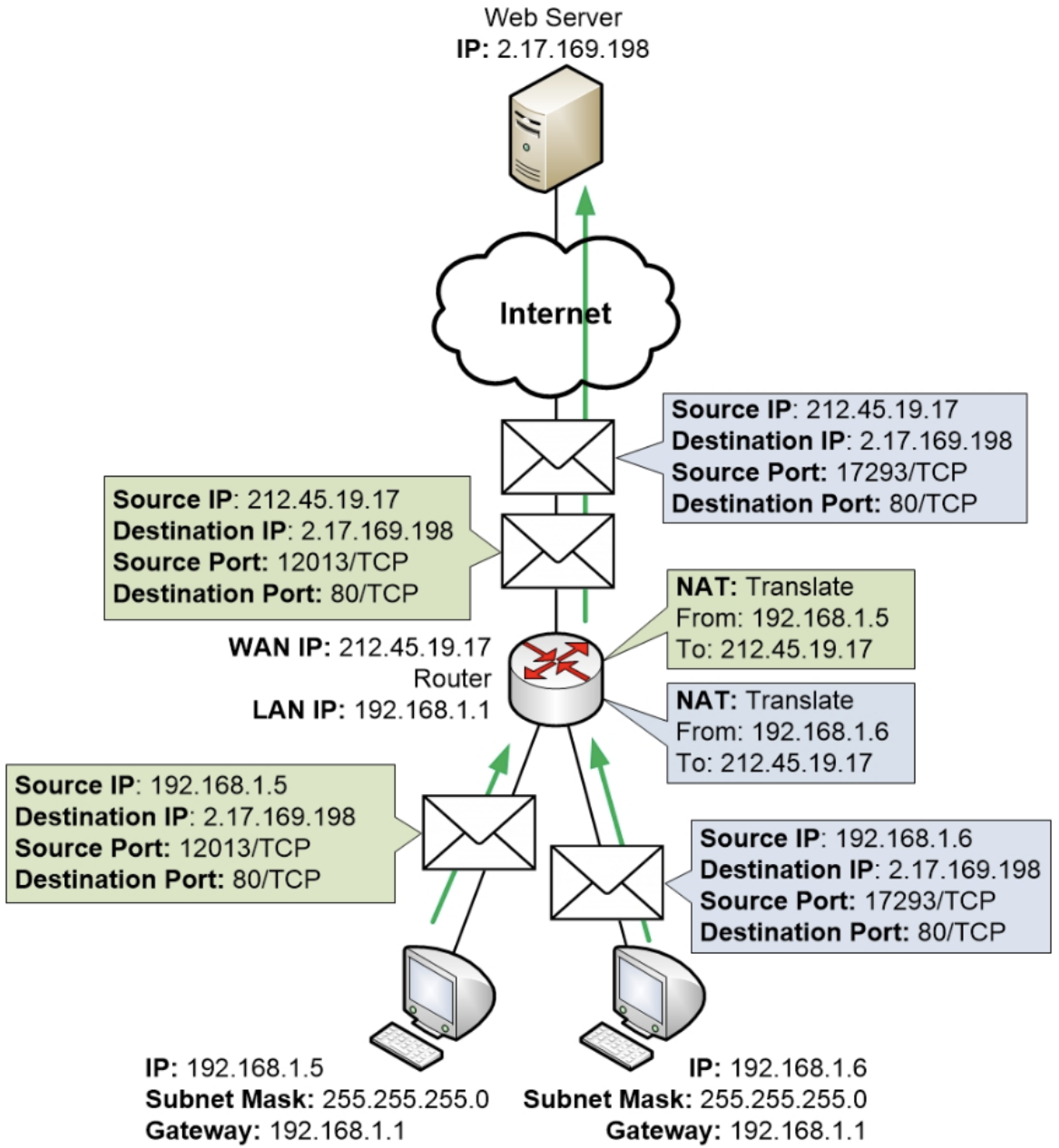
Network address translation



Network address translation

- NAT is a router function where IP addresses (and possibly port numbers) of IP datagrams are replaced at the boundary of a private network.
- NAT is a method that enables hosts on a private network to communicate with hosts on the Internet.
- NAT is run on routers that connect private networks to the public internet to replace an IP packet's IP address port pair with another IP address-port pair.

Netw


Web Server
IP: 2.17.169.198
Internet
Source IP: 212.45.19.17
Destination IP: 2.17.169.198
Source Port: 17293/TCP
Destination Port: 80/TCP
Source IP: 212.45.19.17
Destination IP: 2.17.169.198
Source Port: 12013/TCP
Destination Port: 80/TCP
NAT: Translate
From: 192.168.1.5
To: 212.45.19.17
WAN IP: 212.45.19.17
Router
LAN IP: 192.168.1.1
NAT: Translate
From: 192.168.1.6
To: 212.45.19.17
Source IP: 192.168.1.5
Destination IP: 2.17.169.198
Source Port: 12013/TCP
Destination Port: 80/TCP
Source IP: 192.168.1.6
Destination IP: 2.17.169.198
Source Port: 17293/TCP
Destination Port: 80/TCP
IP: 192.168.1.5
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
IP: 192.168.1.6
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1

From Source to NAT device

- Whenever an outgoing packet enters the NAT box, the 10.x.y.z source address is replaced by the customer's true IP address.
- the TCP Source port field is replaced by an index into the NAT box's 65,536-entry translation table.
- This table entry contains the original IP address and the original source port.
- Finally, both the IP and TCP header checksums are recomputed and inserted into the packet.
- It is necessary to replace the Source port because connections from machines 10.0.0.1 and 10.0.0.2 may both happen to use port 5000, for example, so the Source port alone is not enough to identify the sending process.

Source Computer	Source Computer's IP Address	Source Computer's Port	NAT Router's IP Address	NAT Router's Assigned Port Number
A	192.168.32.10	400	215.37.32.203	1
B	192.168.32.13	50	215.37.32.203	2
C	192.168.32.15	3750	215.37.32.203	3
D	192.168.32.18	206	215.37.32.203	4

From NAT to Source device

- When a packet arrives at the NAT box from the ISP, the Source port in the TCP header is extracted and used as an index into the NAT box's mapping table.
- From the entry located, the internal IP address and original TCP Source port are extracted and inserted into the packet.
- Then, both the IP and TCP checksums are recomputed and inserted into the packet.
- The packet is then passed to the customer router for normal delivery using the 10.x.y.z address.

Uses of NAT

- Pooling of IP addresses
- Supporting migration between ISPs
- IP Masquerading

Pooling of IP addresses

Scenario: A corporate network has many hosts but only a small number of public IP addresses

NAT solution:

- Corporate network is managed with a private address space
- NAT device, located at the boundary between the corporate network and the public Internet, manages a pool of public IP addresses
- When a host from the corporate network sends an IP datagram to a host in the public Internet, the NAT device picks a public IP address from the address pool, and binds this address to the private address of the host

Supporting migration between network service providers

Scenario: In CIDR, the IP addresses in a corporate network are obtained from the service provider.

Changing the service provider requires changing all IP addresses in the network.

NAT solution:

- Assign private addresses to the hosts of the corporate network
- NAT device has static address translation entries that bind the private address of a host to the public address.
- Migration to a new network service provider merely requires an update of the NAT device. The migration is not noticeable to the hosts on the network.

Note: The difference between the use of NAT and IP address pooling is that the mapping of public and private IP addresses is static.

IP Masquerading

- Also called: Network address and port translation (NAPT), port address translation (PAT).

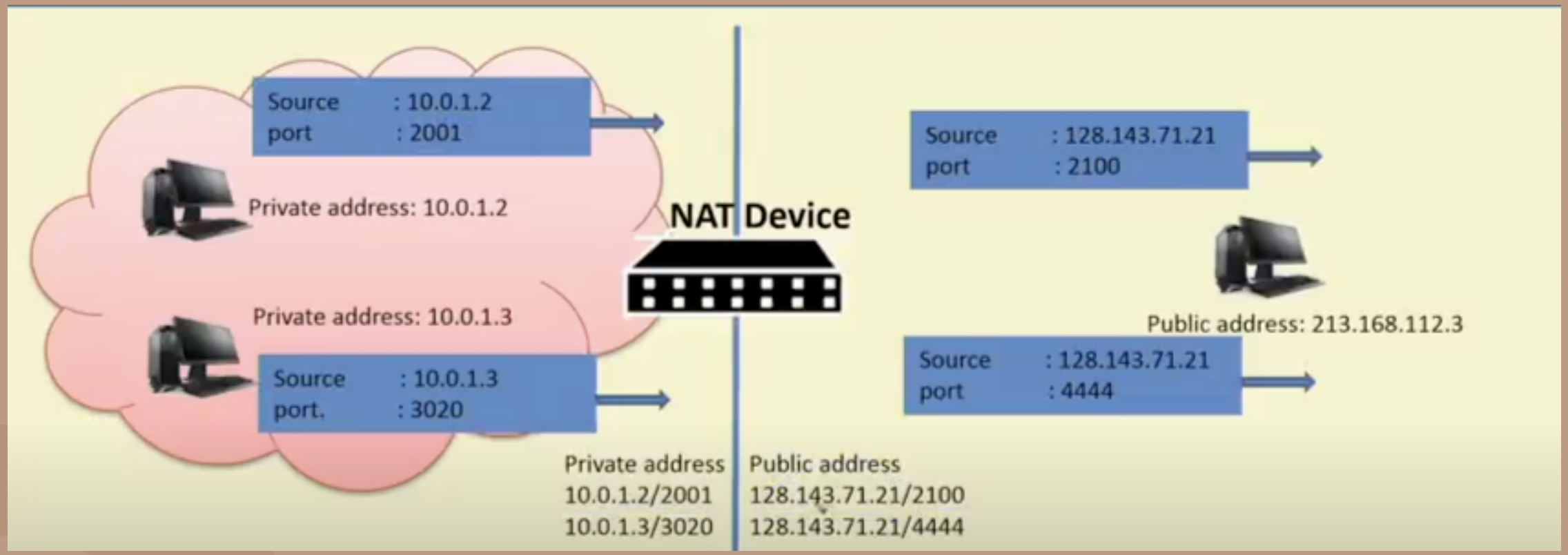
Scenario:

- Single public IP address is mapped to multiple hosts in a private network.

NAT solution:

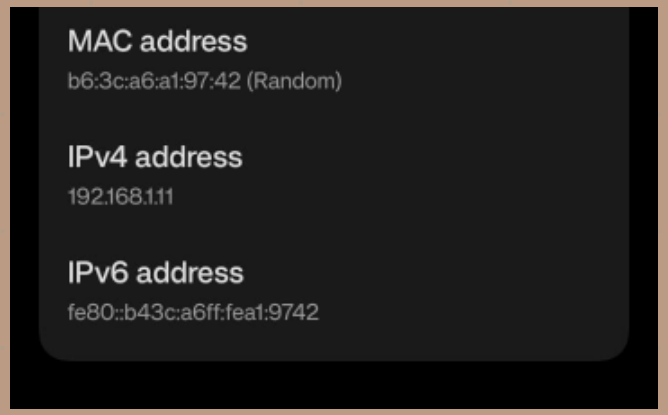
- Assign private addresses to the hosts of the corporate network
- NAT device modifies the port numbers for outgoing traffic

IP Masquerading

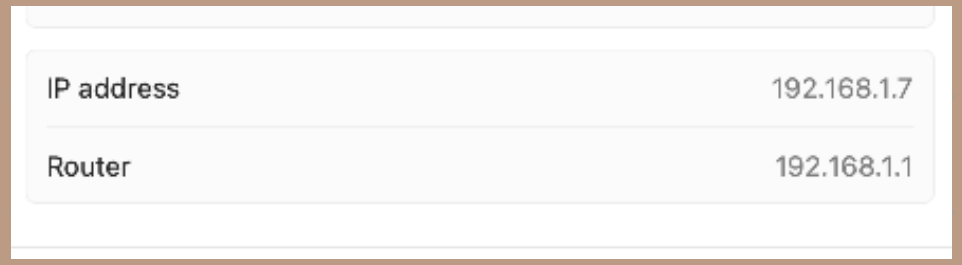


IP Masquerading

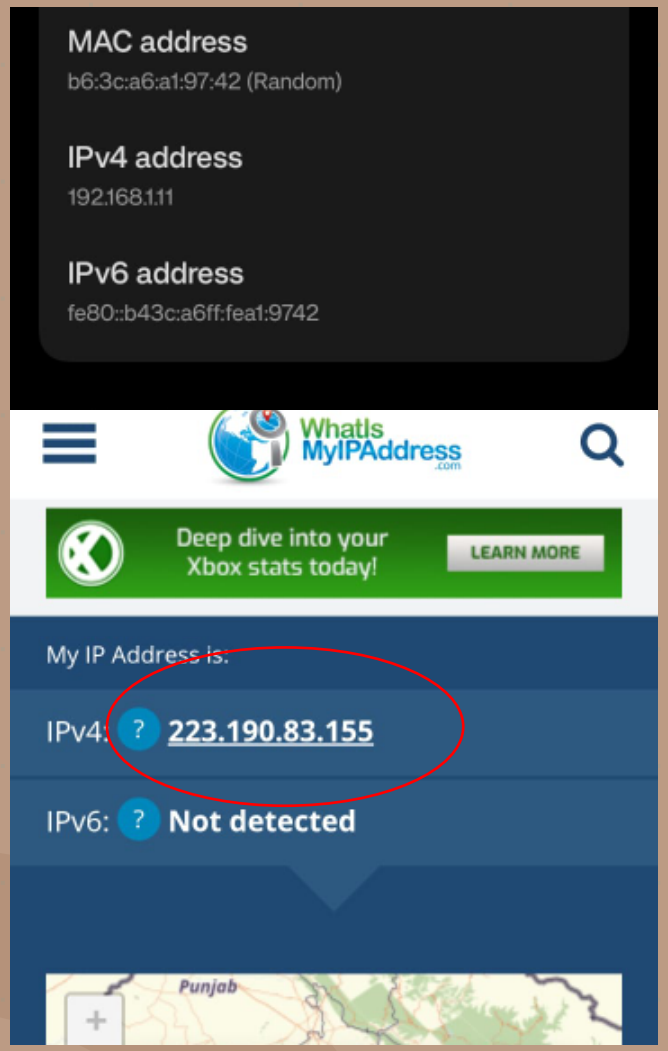
Private IP address of my Mobile Phone



Private IP address of My PC

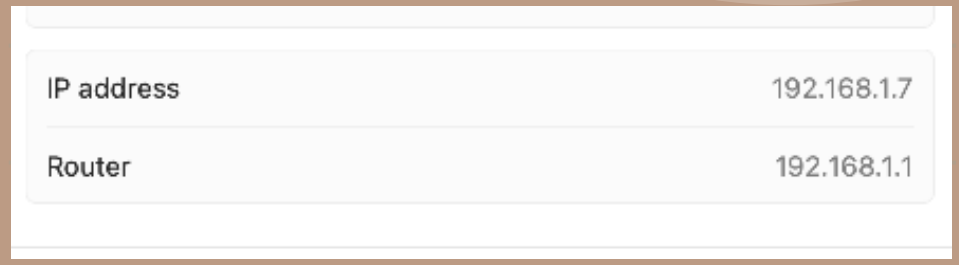


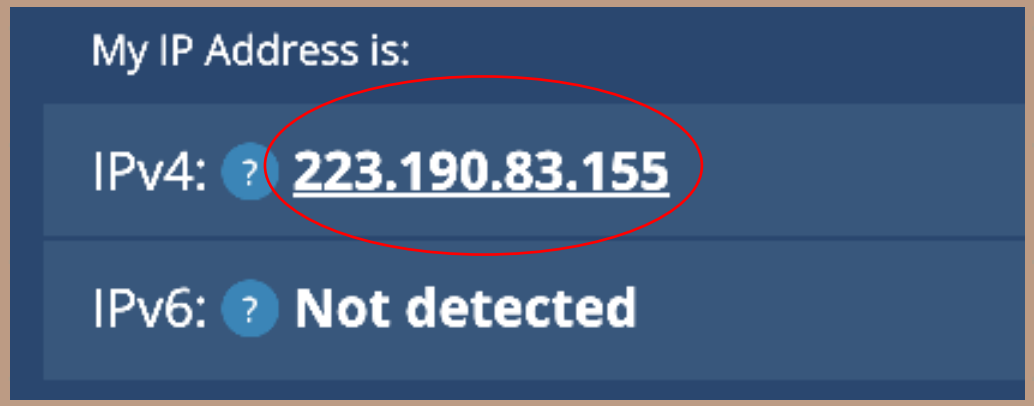
Private IP address of Mobile Phone



public IP address of Mobile Phone

Private IP address of My PC





Public IP address of my PC

Random MAC address:https://macadmin.fraserhess.com/2024/09/16/handling-mac-address-randomization-in-macos-15/

Some Objections to the NAT from the IP community

- violates the architectural model of IP, which states that every IP address uniquely identifies a single machine worldwide (the whole software structure of the Internet is Built on this fact)
- With NAT, thousands of machines may (and do) use address 10.0.0.1.

2nd Objections

- NAT breaks the end-to-end connectivity model of the Internet, which says that any host can send a packet to any other host at any time.
- Since the mapping in the NAT box is set up by outgoing packets, incoming packets cannot be accepted until after outgoing ones.
- In practice, this means that a home user with NAT can make TCP/IP connections to a remote Web server, but a remote user cannot make connections to a game server on the home network.
- Special configuration or NAT traversal techniques are needed to support this kind of situation

3rd Objection

- NAT changes the Internet from a connectionless network to a peculiar kind of connection-oriented network. The problem is that the NAT box must maintain information (i.e., the mapping) for each connection passing through it.
- Having the network maintain a connection state is a property of connection-oriented networks, not connectionless ones.
- If the NAT box crashes and its mapping table is lost, all its TCP connections are destroyed.
- In the absence of NAT, a router can crash and restart with no long-term effect on TCP connections.
- The sending process just times out within a few seconds and retransmits all unacknowledged packets.

4th Objection:

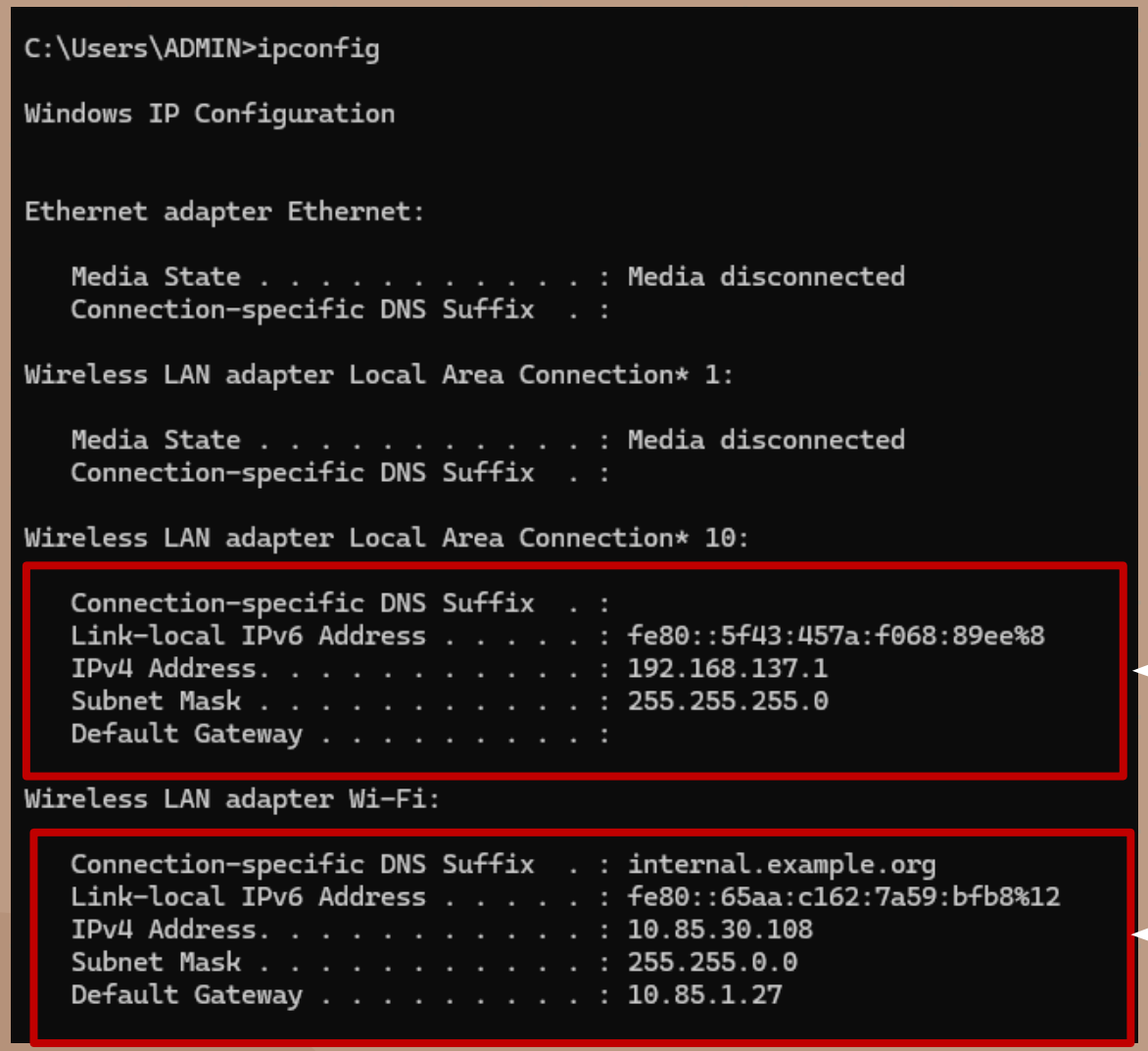
- NAT violates the most fundamental rule of protocol layering:
- *layer k may not make any assumptions about what layer k + 1 has put into the payload field.*
- basic principle: keep the layers independent.
- If TCP is later upgraded to TCP-2, with a different header layout (e.g. , 32-bit ports), NAT will fail.
- The whole idea of layered protocols is to ensure that changes in one layer do not require changes in other layers.
- NAT destroys this independence.

Objections (5^{th})

- some applications use multiple TCP/IP connections or UDP ports in prescribed ways. For example, FTP, the standard File Transfer Protocol, inserts IP addresses in the body of the packet for the receiver to extract and use.
- Since NAT knows nothing about these arrangements, it cannot rewrite the IP addresses or otherwise account for them.
- This lack of understanding means that FTP and other applications will fail in the presence of NAT unless special precautions are taken.
- It is often possible to patch NAT for these cases, but having to patch the code in the NAT box every time a new application comes along is not a good idea.

Summary: Network Address Translation(NAT)

- Despite the issues, NAT is widely used in practice, especially for home and small business networks, as the only expedient technique to deal with the IP address shortage.
- has become wrapped up with firewalls and privacy because it blocks unsolicited incoming packets by default.
- For this reason, it is unlikely to go away even when IPv6 is widely deployed



IP address: 192.168.137.1
Subnet Mask: 255.255.255.0

IP address: 10.185.30.108
Subnet Mask: 255.255.0.0

IP address: 192.168.137.1. **Subnet Mask**: 255.255.255.0

- It is a **private IP address** in the range 192.168.x.x - commonly used in home or small office networks.
- **IP Address**: 192.168.1.10 (Your device's local address).
- **Subnet Mask**: 255.255.255.0 (Defines the size of the network).
- **Broadcast Address**: 192.168.1.255 (Used for communication with all devices on the local network).

IP address: 10.185.30.108. **Subnet Mask**: 255.255.0.0

- Class A IP addressing, but the subnet mask is of Class B. Why?

4. A layer-4 firewall (a device that can look at all protocol headers up to the transport layer) CANNOT

(A) block HTTP traffic between 9:00 PM and 5:00 AM

(B) block all ICMP traffic

(C) stop incoming traffic from a specific IP address but allow outgoing traffic to the same IP

(D) block TCP traffic from a specific user on a specific IP address on a multi-user system during 9:00 PM and 5:00 AM

4. A layer-4 firewall (a device that can look at all protocol headers up to the transport layer) CANNOT

(A) block HTTP traffic between 9:00 PM and 5:00 AM

(B) block all ICMP traffic

(C) stop incoming traffic from a specific IP address but allow outgoing traffic to the same IP

(D) block TCP traffic from a specific user on a specific IP address on a multi-user system during 9:00 PM and 5:00 AM

Answer (A)

HTTP is an application layer protocol. Since the firewall is at layer 4, it cannot block HTTP data.

Q.5: Consider different activities related to email.

m1:Send an email from a mail client to the mail server

m2:Download an email from the mailbox server to a mail client

m3:Checking email in a web browser

Which is the applicable level protocol user in each activity?

(A) m1:HTTP, m2:SMTP, m3:POP

(B) m1:SMTP, m2:FTP, m3:HTTP

(C) m1:SMTP, m2:POP, m3:HTTP

(D) m1:POP, m2:SMTP, m3:IMAP

Q.5: Consider different activities related to email.

m1: Send an email from a mail client to the mail server

m2: Download an email from the mailbox server to a mail client

m3: Checking email in a web browser

Which is the applicable level protocol user in each activity?

(A) m1:HTTP, m2:SMTP, m3:POP

(B) m1:SMTP, m2:FTP, m3:HTTP

(C) m1:SMTP, m2:POP, m3:HTTP

(D) m1:POP, m2:SMTP, m3:IMAP

Answer (C)

Simple Mail Transfer Protocol (SMTP) is typically used by user clients for sending mails.

Post Office Protocol (POP) is used by clients for receiving mails.

Checking mails in web browser is a simple HTTP process.

Q.6: One of the header fields in an IP datagram is the Time to Live (TTL) field. Which of the following statements best explains the need for this field?

(A) It can be used to prioritize packets

(B) It can be used to reduce delays

(C) It can be used to optimize throughput

(D) It can be used to prevent packet looping

Q.6: One of the header fields in an IP datagram is the Time to Live (TTL) field. Which of the following statements best explains the need for this field?

(A) It can be used to prioritise packets

(B) It can be used to reduce delays

(C) It can be used to optimize throughput

(D) It can be used to prevent packet looping

Answer) (D)

Time to Live can be thought of as an upper bound on the time that an IP datagram can exist in the network.

The purpose of the TTL field is to avoid a situation in which an undeliverable datagram keeps circulating.

Q.7: Suppose computers A and B have IP addresses 10.105.1.113 and 10.105.1.91, respectively, and they both use the same netmask N. Which of the values of N given below should not be used if A and B should belong to the same network?

(A) 255.255.255.0

(B) 255.255.255.128

(C) 255.255.255.192

(D) 255.255.255.224

Q.7: Suppose computers A and B have IP addresses 10.105.1.113 and 10.105.1.91 respectively and they both use the same netmask N. Which of the values of N given below should not be used if A and B should belong to the same network?

(A) 255.255.255.0

(B) 255.255.255.128

(C) 255.255.255.192

(D) 255.255.255.224

Answer (D)

The last octets of IP addresses of A and B are 113 (01110001) and 91 (01011011).

The netmask in option (D) has the first three bits set in the last octet. If the netmask has the first 3 bits set, then these bits must be the same in A and B, but that is not the case. In simple words, we can say option (D) is not a valid netmask because doing binary ‘&’ of it with addresses of A and B doesn ' t give the same network address. It must be the same address as A and B , which are on the same network.

Q. You have been allocated a class A network address of **29.0.0.0**. You need to create at least 20 networks, and each network will support a maximum of 160 hosts. Would the following two subnet masks Work?

255.255.0.0 and or **255.255.255.0**

Solution:

Q. You have been allocated a class A network address of **29.0.0.0**. You need to create at least 20 networks, and each network will support a maximum of 160 hosts. Would the following two subnet masks Work? **255.255.0.0** and or **255.255.255.0**

Solution:

Yes both would work.

Mask **255.255.0.0** has 8 bits for the subnet and 16 bits for the host

8 bits would accommodate 2^8=256 subnets

16 bits would accommodate 2^{16}= over 64000 hosts

Mask 255.255.255.0 has 16 bits for the subnet and 8 bits of the host.

Have possible 2^8 -2 hosts =254 which is enough

Q. Subnet the Class C IP Address 195.1.1.0 So that you have 10 subnets, each with a maximum of 12 hosts on each subnet. List the Address on host 1 on subnet 0,1,2,3,10.

Solution:

Q. Subnet the Class C IP Address 195.1.1.0 So that you have 10 subnets, each with a maximum of 12 hosts on each subnet. List the Address on host 1 on subnet 0,1,2,3,10.

Solution:

Current mask= 255.255.255.0

Bits needs for 10 subnets =4 =2^4 =16 possible subnets

Bits needs for 12 hosts = 4 = 2^4 = 16-2=14 possible hosts.

So our mask in binary =**11110000**= **240** decimal

Final Mask =**255.255.255.240**

Hosts on Subnets 0,1,2,3,10

- Subnet 0 host 1 IP address = 195.1.1.1 **0000 0001**
- Subnet 1 host 1 IP address = 195.1.1.17 **0001 0001**
- Subnet 2 host 1 IP address = 195.1.1.33 **0010 0001**
- Subnet 3 host 1 IP address = 195.1.1.49 **0011 0001**
- Subnet 10 host 1 IP address = 195.1.1.161 **1010 0001**

Q. Your ISP has given you the address **223.5.14.6/29** to assign to your router's interface. They have also given you the default gateway address of **223.5.14.7**. After you have configured the address, the router is unable to ping any remote devices. What is preventing the router from pinging remote devices?

A. The default gateway is not an address on this subnet.

B. The default gateway is the broadcast address for this subnet.

C. The IP address is the broadcast address for this subnet.

D. The IP address is an invalid class D multicast address.

Correct Answer

B. The default gateway is the broadcast address for this subnet.

Explanation:

To resolve the issue described, we must first understand the addressing and subnetting based on the information provided:

IP Address Assigned: 223.5.14.6/29

Subnet Mask (/29): This subnet mask indicates that 29 bits are used for the network part, leaving 3 bits for the host part within the subnet. This means the subnet supports up to 23−2=623−2=6 usable host IP addresses.

Calculating the Subnet:

The subnet /29 means the subnet mask is 255.255.255.248.

To find the range, consider the last octet of the subnet mask (248): 256 - 248 = 8, which means each subnet increments by 8 in the last octet.

So, the subnet 223.5.14.0/29 covers addresses from 223.5.14.0 to 223.5.14.7.

Addresses in the Subnet:

Network Address: 223.5.14.0

Usable Addresses: 223.5.14.1 to 223.5.14.6

Broadcast Address: 223.5.14.7

Analysing the Problem:

The router's IP address given is 223.5.14.6, which falls within the usable range.

The default gateway address provided is 223.5.14.7, which is the broadcast address for the subnet.

Answer: The problem is that the default gateway is the broadcast address for this subnet. Routers or devices in a network cannot use the broadcast address as a gateway because it is reserved for broadcasting to all devices in the subnet. Thus, any packets intended for external networks sent to this gateway address would not be properly routed.

The forwarding table of a router is shown below.

Subnet Number	Subnet Mask	Interface ID
200.150.0.0	255.255.0.0	1
200.150.64.0	255.255.224.0	2
200.150.68.0	255.255.255.0	3
200.150.68.64	255.255.255.224	4
Default		0

A packet addressed to a destination address 200.150.68.118 arrives at the router. It will be forwarded to the interface with ID _____

The forwarding table of a router is shown below.

Subnet Number	Subnet Mask	Interface ID
200.150.0.0	255.255.0.0	1
200.150.64.0	255.255.224.0	2
200.150.68.0	255.255.255.0	3
200.150.68.64	255.255.255.224	4
Default		0

A packet addressed to a destination address 200.150.68.118 arrives at the router. It will be forwarded to the interface with ID _____.

As we know that when data packets arrived at the internal router, it will perform the following steps:
Find the first address/subnet id between the destination IP address and subnet mask using bitwise and operation.
after finding the first address 3 cases can be there:
If FA is matched with one subnet address then data is forwarded to the matched subnet address.
If FA is matched with more than one subnet address then data is forwarded to the interface corresponding to the largest subnet mask (maximum number of 1's)
If FA is not matched with anyone then the data packet is forwarded to the default interface.

(A): $200.150.68.118 \wedge 255.255.0.0$

$$\begin{array}{rrrr} 200.150.68.118 = 200 & 150 & 01000100 & 01110110 \\ \wedge\, 255.255.0.0 = 255 & 255 & 00000000 & 00000000 \\ \hline 200.150.0.0 = 200 & 150 & 00000000 & 00000000 \end{array}$$

$\therefore$ subnet id=$200.150.0.0$,matched

(B): $200.150.68.118 \wedge 255.255.224.0$

$$\begin{array}{rrrr} 200.150.68.118 = 200 & 150 & 01000100 & 01110110 \\ \wedge\, 255.255.224.0 = 255 & 255 & 11100000 & 00000000 \\ \hline 200.150.64.0 = 200 & 150 & 01000000 & 00000000 \end{array}$$

$\therefore$ subnet id=$200.150.64.0$,matched.

(C): $200.150.68.118 \wedge 255.255.255.0$

$$\begin{array}{rrrr} 200.150.68.118 = 200 & 150 & 01000100 & 01110110 \\ \wedge\, 255.255.255.0 = 255 & 255 & 11111111 & 00000000 \\ \hline 200.150.68.0 = 200 & 150 & 01000100 & 00000000 \end{array}$$

$\therefore$ subnet id=$200.150.68.0$,matched.

(D): $200.150.68.118 \wedge 255.255.255.224$

$$\begin{array}{rrrr} 200.150.68.118 = 200 & 150 & 01000100 & 01110110 \\ \wedge\, 255.255.255.224 = 255 & 255 & 11111111 & 11100000 \\ \hline 200.150.68.96 = 200 & 150 & 01000100 & 01100000 \end{array}$$

$\therefore$ subnet id=$200.150.68.96$ not matched.

Since more than one subnet address is matched the data packet is forwarded to the interface corresponding to the largest subnet mask (a subnet mask having the maximum number of 1's).

Here $255.255.255.0$ has the maximum number of 1's in binary representation among A, B, and C so the data packet is forwarded to the interface id 3.

the correct answer is 3

Classful vs Classless vs CIDR vs FLSM vs VLSM

https://www.practicalnetworking.net/stand-alone/classful-cidr-flsm-vlsm/

4. An Internet Service Provider(ISP) has the following chunk of CIDR-based IP addresses available with it: 245.248.128.0/20. The ISP wants to give half of this chunk of addresses to Organization A, and a quarter to Organization B while retaining the remaining with itself. Which of the following is a valid allocation of addresses to A and B? [GATE CSE 2012]

(A) 245.248.136.0/21 and 245.248.128.0/22

(B) 245.248.128.0/21 and 245.248.128.0/22

(C) 245.248.132.0/22 and 245.248.132.0/21

(D) 245.248.136.0/22 and 245.248.132.0/21

Solution: (A)

Since the routing prefix is 20, the ISP has 2^(32-20) or 2^12 addresses.

Out of these 2^12 addresses, half (or 2^11) addresses have to be given to organisation A, and a quarter (2^10) addresses have to be given to organisation B.

So, the routing prefix for organisation A will be 21. For B, it will be 22.

If we see all options given in the question, only options (A) and (B) are left as only these options have the same number of routing prefixes. Now, we need to choose from options (A) and (B).

To assign addresses to organisation A, ISP needs to take the first 20 bits from 245.248.128.0 and fix the 21st bit as 0 or 1. Similarly, the ISP needs to fix the 21st and 22nd bits for organization B.

If we take a closer look at options (A) and (B), we can see the 21st and 22nd bits for organization B are considered as 0 in both options. So 21st bit of organization A must be 1. Now take the first 20 bits from 245.248.128.0 and the 21st bit as 1, we get addresses for organization A as 245.248.136.0/21

Q.8: The address resolution protocol (ARP) is used for:

(a) Finding the IP address from the DNS

(b) Finding the IP address of the default gateway

(c) Finding the IP address that corresponds to a MAC address

(d) Finding the MAC address that corresponds to an IP address

Q.8: The address resolution protocol (ARP) is used for:

(a) Finding the IP address from the DNS

(b) Finding the IP address of the default gateway

(c) Finding the IP address that corresponds to a MAC address

(d) Finding the MAC address that corresponds to an IP address

Answer (d)

Address Resolution Protocol (ARP) is a request and reply protocol used to find a MAC address from an IP address.

Mapping Logical address to Physical address: ARP

Situation:

A host/router has a packet to send to another host or router. It knows its IP address.

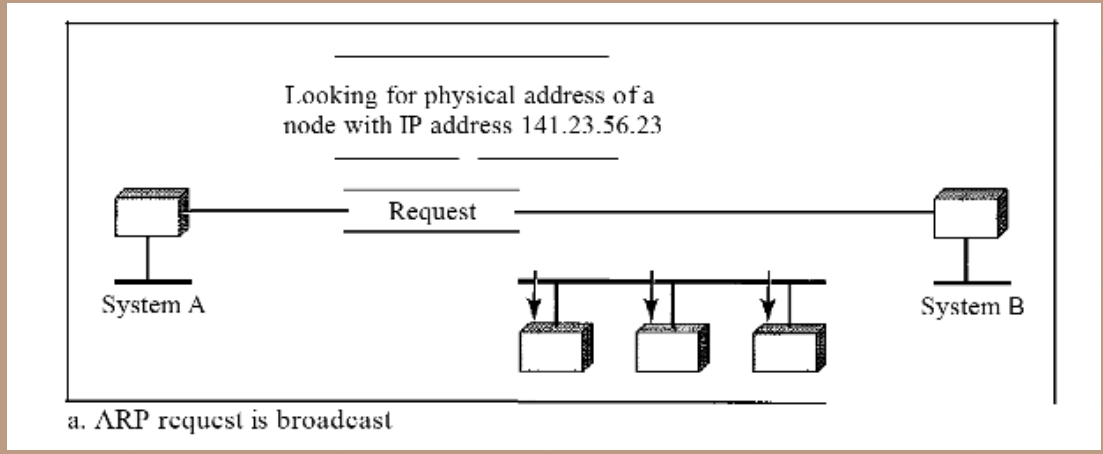
Sender machine needs to know the MAC address of the receiver because IP datagram must be encapsulated in a frame to be able to pass through the physical network.

Solution:

send an ARP query packet.

ARP packet includes the physical and IP addresses of the sender and the IP address of the receiver.

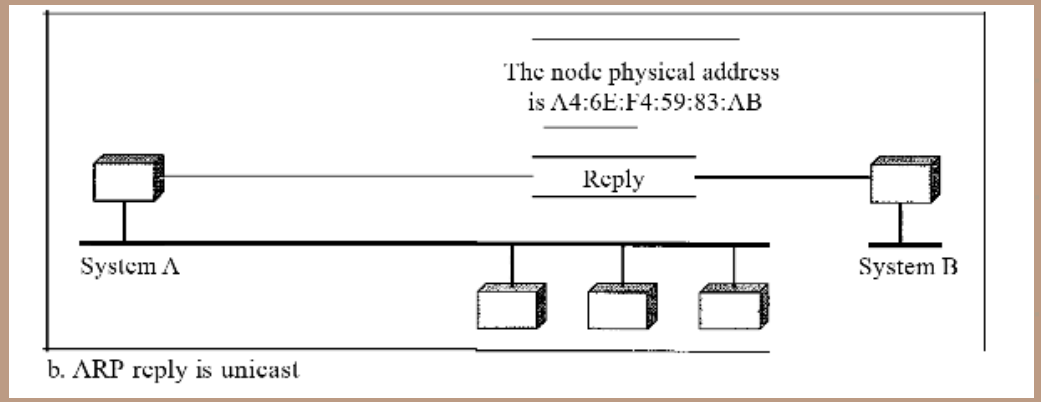
Because the sender does not know the physical address of the receiver, the query is broadcast over the network



a. ARP request is broadcast

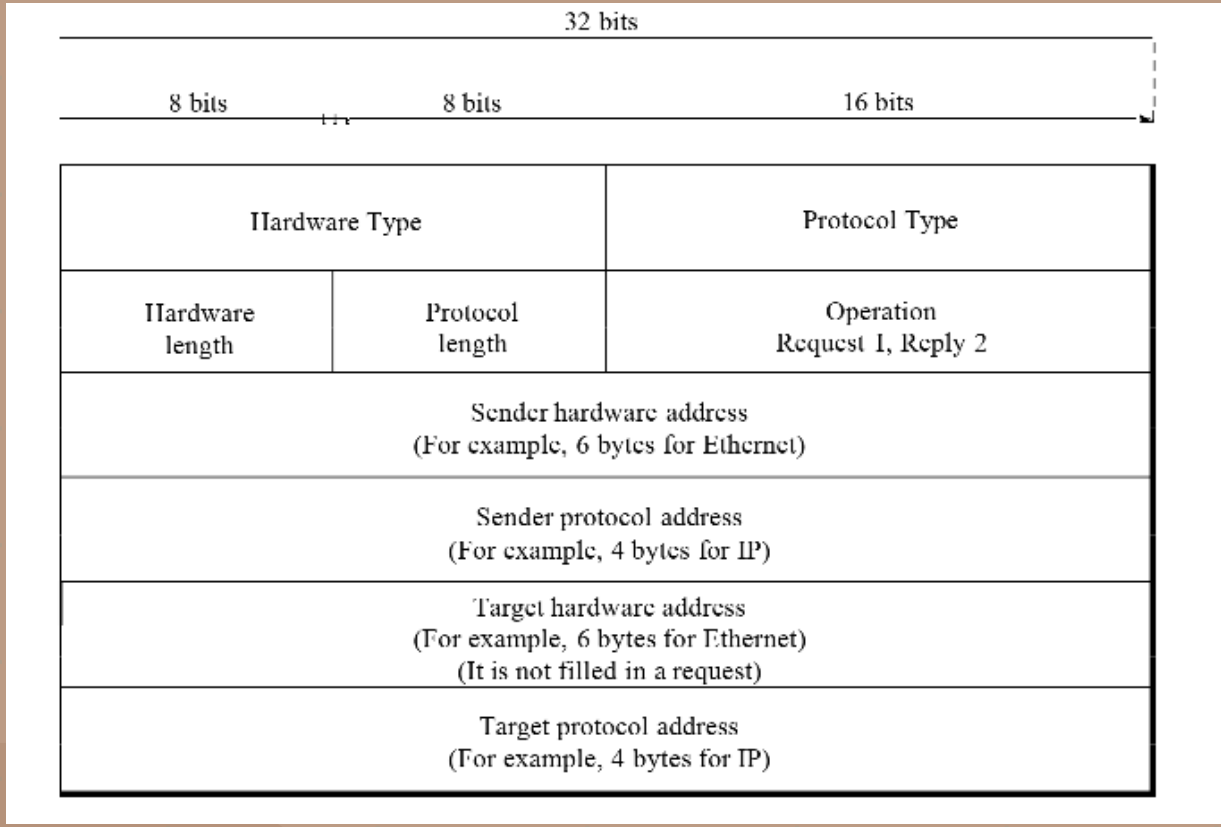
Mapping Logical address to Physical address: ARP

- Every host or router on the network receives - processes the ARP query packet
- only the intended recipient recognizes its IP address and sends back an ARP response packet.
- The response packet contains the recipient's IP and physical addresses.
- packet is unicast directly to the inquirer by using the physical address received in the query packet.



b. ARP reply is unicast

ARP Packet Format



Hardware type. 16-bit field defining the type of the network on which ARP is running. Ethernet is given type 1.

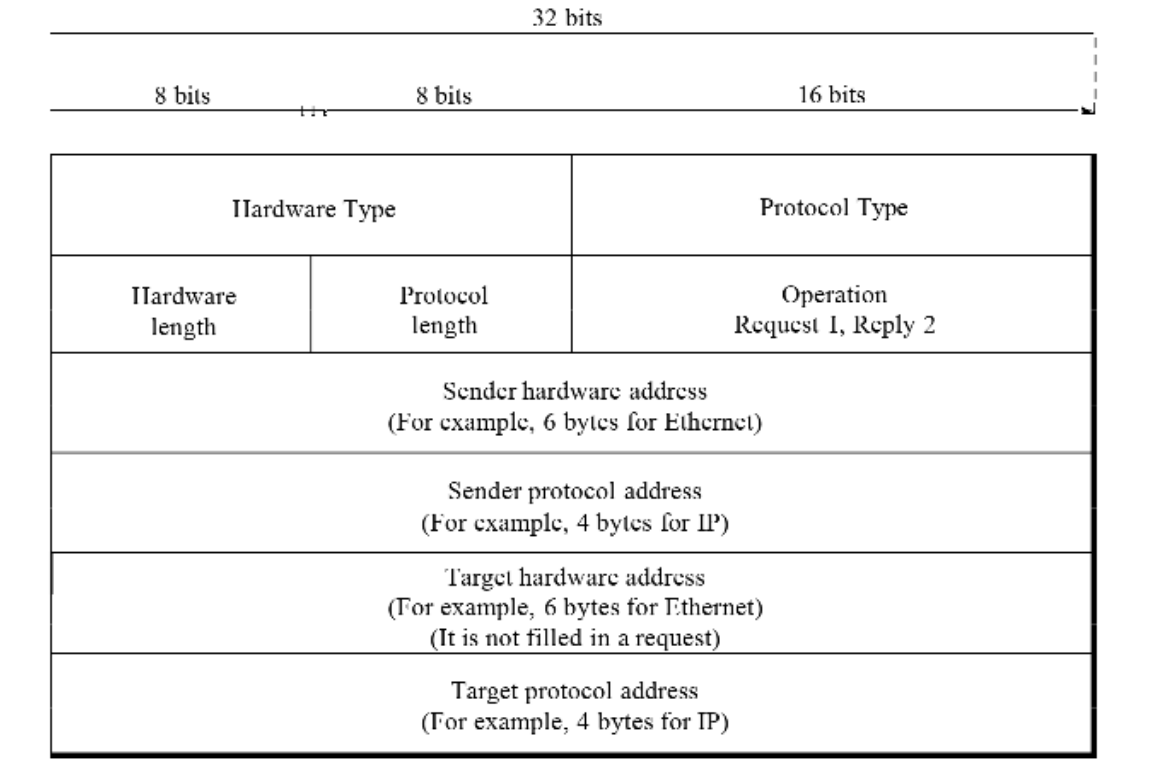
o **Protocol type.** 16-bit field defining the protocol. the value for IPv4 protocol is 0800 H.

o **Hardware length**. 8-bit field defining the length of the physical address in bytes. for Ethernet the value is 6.

o **Protocol length**. an 8-bit field defining the length of the logical address in bytes. for the IPv4 protocol the value is 4.

o **Operation.** a 16-bit field defining the type of packet. Two packet types are defined: ARP request (1) and ARP reply (2).

ARP Packet Format



o **Sender hardware address**. a variable-length field defining the physical address of the sender. for Ethernet this field is 6 bytes long.

o **Sender protocol address.** a variable-length field defining the logical (for example, IP) address of the sender. For IPv4 this field is 4 bytes long.

o **Target hardware address**. a variable-length field defining the physical address of the target. For example, for Ethernet this field is 6 bytes long. For an ARP request message, this field is all Os

o **Target protocol address**. a variable-length field defining the logical (for example, IP) address of the target. For the IPv4 protocol, this field is 4 bytes long.

ARP Layering

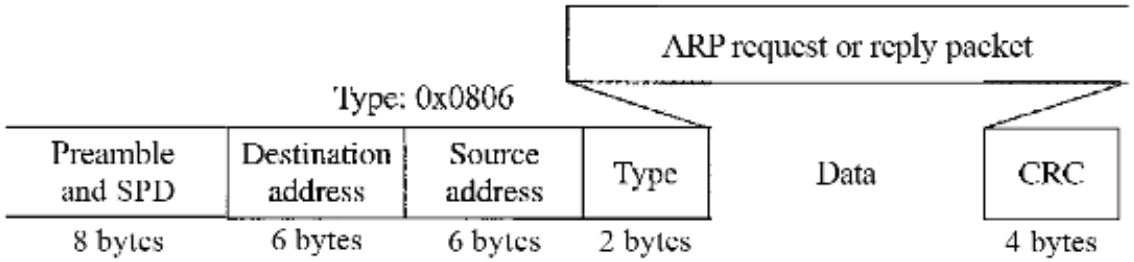
Layering [edit]

ARP's placement within the Internet protocol suite and the OSI model may be a matter of confusion or even of dispute. RFC 826 places it into the Link Layer and characterizes it as a tool to inquire about the "higher level layer", such as the Internet layer.[3] RFC 1122 also discusses ARP in its link layer section.[4] Richard Stevens places ARP in OSI's data link layer[5] while newer editions associate it with the network layer or introduce an intermediate OSI layer 2.5.[6]

Source: Wikipedia

An ARP packet is encapsulated directly into a data link frame (example: ethernet data link layer frame)

Figure 21.3 *Encapsulation of ARP packet*



Operation of ARP

Step 1: IP asks ARP to create an ARP request message.

Step 2: message is passed to the data link layer for encapsulation. Frame contains the physical address of the sender as the source address and the physical broadcast address as the destination address.

Step 3: Every host or router receives the frame. Because the frame contains a broadcast destination address. All machines except the one targeted drop the packet. The target machine recognizes its IP address.

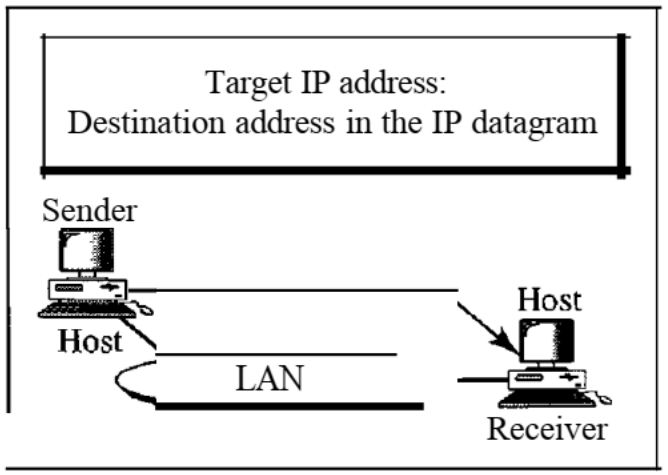
Operation of ARP

Step 4: The target machine replies with an ARP reply message that contains its physical address. The message is unicast.

Step 5: The sender receives the reply message. It now knows the physical address of the target machine.

Step 6: The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

Scenarios in which service of ARP are used

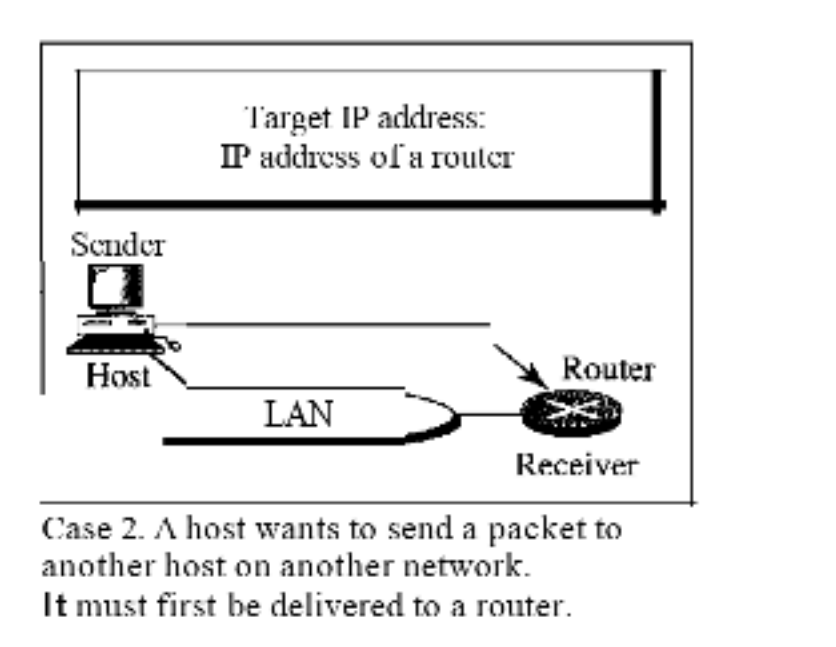


Case 1. A host has a packet to send to another host on the same network.

Scenario: The sender is a host and wants to send a packet to another host on the same network.

So, the logical address that must be mapped to a physical address is the destination IP address in the datagram header.

Scenarios in which service of ARP are used



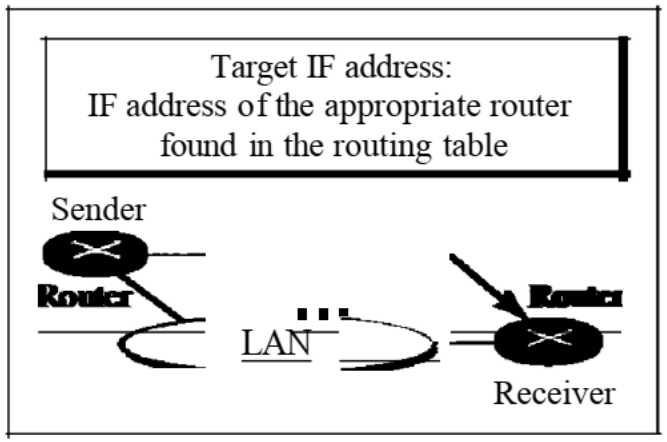
Case 2. A host wants to send a packet to another host on another network. It must first be delivered to a router.

Situation: The sender is a host and wants to send a packet to another host on another network.

How ARP is used:

- the host looks at its routing table and finds the IP address of the next hop (router) for this destination.
- If it does not have a routing table, it looks for the IP address of the default router.
- *The IP address of the router becomes the logical address that must be mapped to a physical address.*

Scenarios in which service of ARP are used



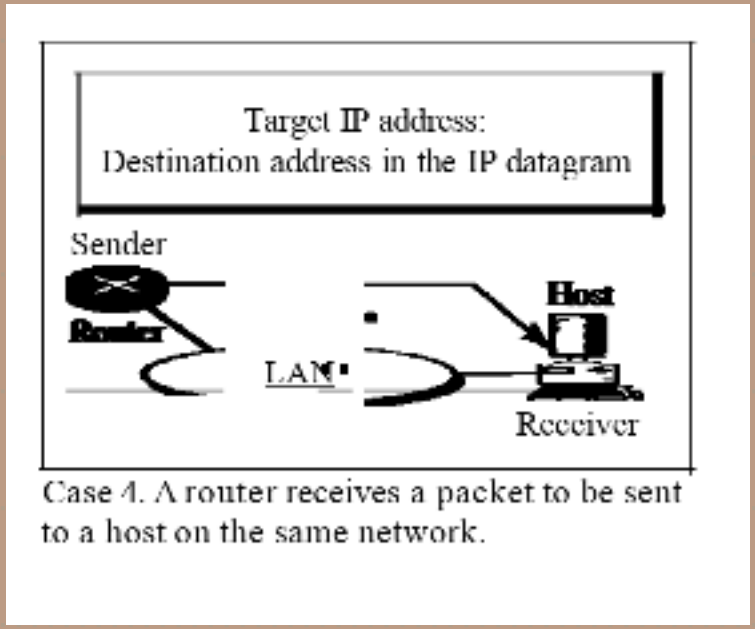
Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.

Scenario: The sender is a router that has received a datagram destined for a host on another network.

How ARP is used:

- It checks its routing table and finds the IP address of the next router.
- *The IP address of the next router becomes the logical address that must be mapped to a physical address.*

Scenarios in which service of ARP are used



Case 4. A router receives a packet to be sent to a host on the same network.

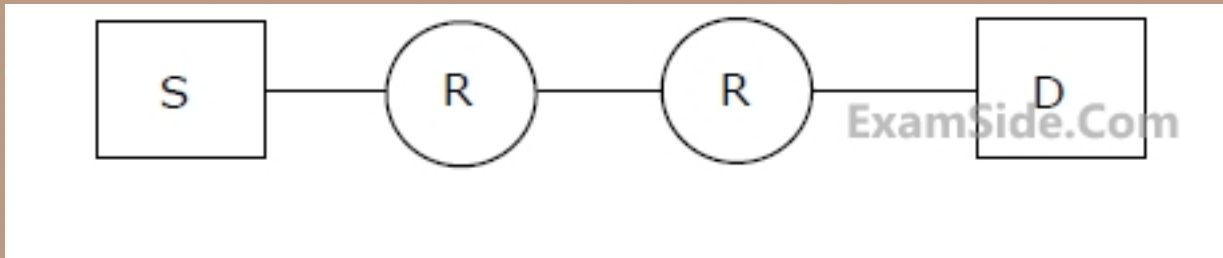
Scenario: The sender is a router that has received a datagram destined for a host on the same network.

How ARP is used:

- The destination IP address of the datagram becomes the logical address that must be mapped to a physical address.

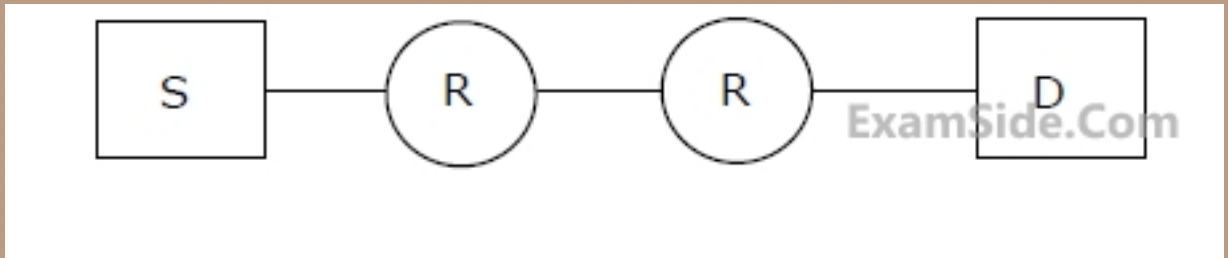
Q.9: Assume that source S and destination D are connected through two intermediate routers labeled R. Determine how many times each packet has to visit the network layer and the data link layer during transmission from S to D

1. Network layer - 4 times and Data link layer - 4 times
2. Network layer - 4 times and Data link layer - 3 times
3. Network layer - 4 times and Data link layer - 6 times
4. Network layer - 2 times and Data link layer - 6 times



Q.9: Assume that source S and destination D are connected through two intermediate routers labeled R. Determine how many times each packet has to visit the network layer and the data link layer during transmission from S to D

1. Network layer - 4 times and Data link layer - 4 times
2. Network layer - 4 times and Data link layer - 3 times
3. Network layer - 4 times and Data link layer - 6 times
4. Network layer - 2 times and Data link layer - 6 times



Answer: C

Q.10: Which one of the following is not a client-server application?

A) Internet chat

B) Web browsing

C) E-mail

D) Ping

Q.10: Which one of the following is not a client-server application?

A) Internet chat

B) Web browsing

C) E-mail

D) Ping

Q.10: Which one of the following is not a client-server application?

A) Internet chat

B) Web browsing

C) E-mail

D) Ping

Answer: D

Ping is the name of a standard software utility, used to test connectivity either between client-client or client-server.

Q. An organization is granted the block 130.56.0.0/16. The administrator creates 1024 subnets.

A. Find the subnet mask

B. Find the number of addresses in each subnet

C. Find the first and last address in subnet 1

D. Find the first and last address in subnet 1024.

Virtual Private Networks (VPN)

Virtual Private Networks (VPN)

How can an organisation that uses the global internet to connect its sites guarantee that all communication is kept private?

Answer: VPN

Basis Idea: "send datagrams across the global internet but encrypt the contents"

VPN = Virtual+ Private+ Network

Private: The use of encryption means that communication between any pair of computers remains concealed from outsiders.

Virtual: does not require dedicated leased circuits to connect one site to another.

Virtual Private Networks (VPN)

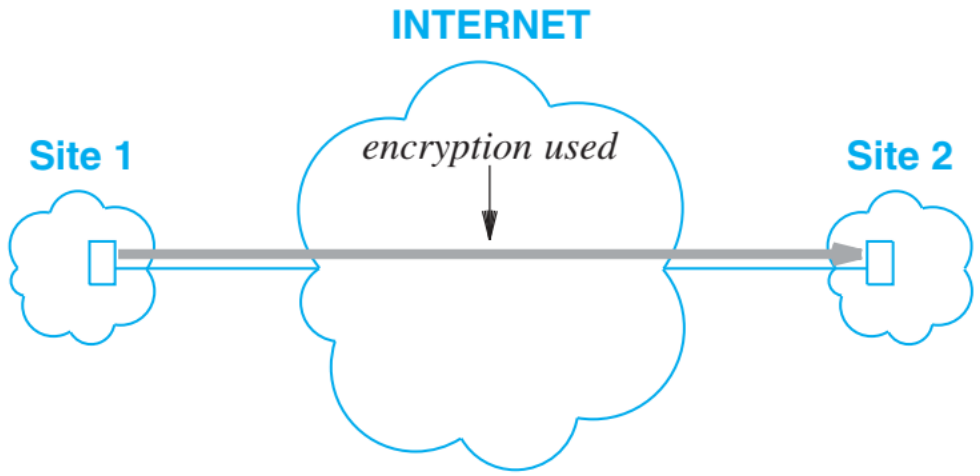


Figure 19.1 Illustration of a VPN that uses encryption when sending data across the global Internet between two routers at two sites of an organization.

Virtual Private Networks (VPN)

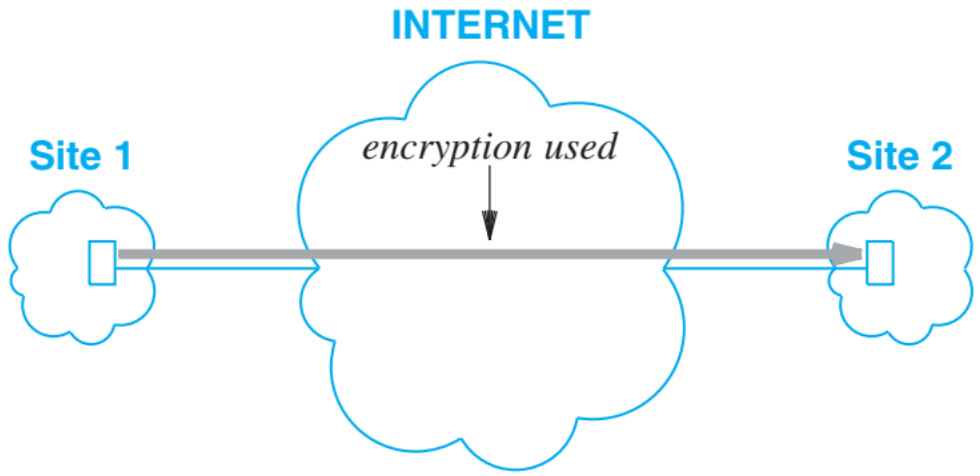


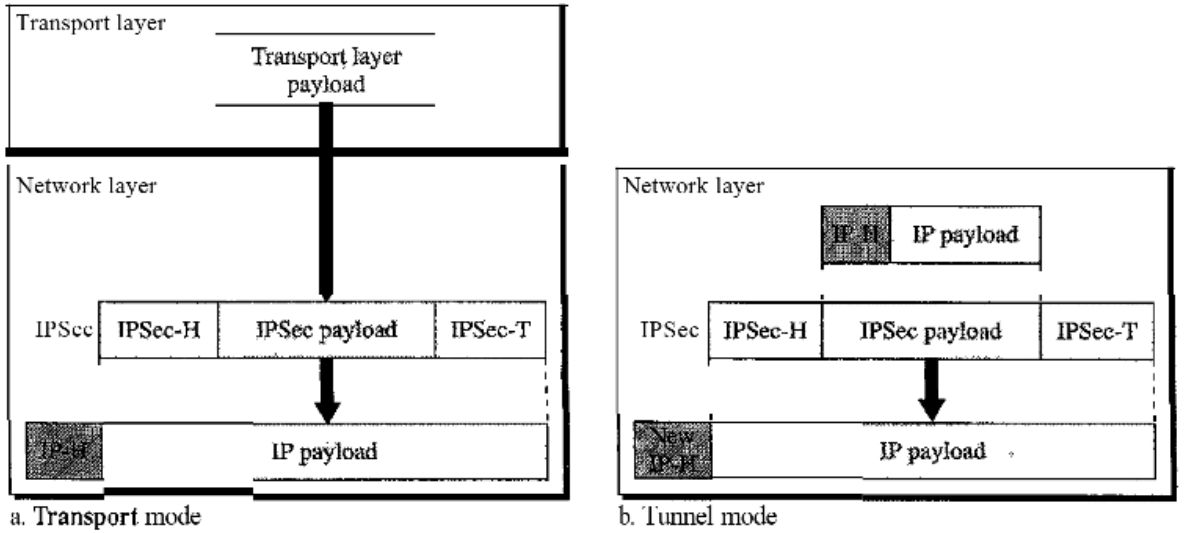
Figure 19.1 Illustration of a VPN that uses encryption when sending data across the global Internet between two routers at two sites of an organization.

VPN: Tunnelling

VPN encrypts all of the data sent to and from your device and routes it through an intermediary server that stands between you and the internet.
The encrypted connection between your device and the VPN server is often referred to as a “tunnel”.
No third parties, such as your ISP, government, or local IT administrator, can see the contents of your data or its destination while the VPN is active.

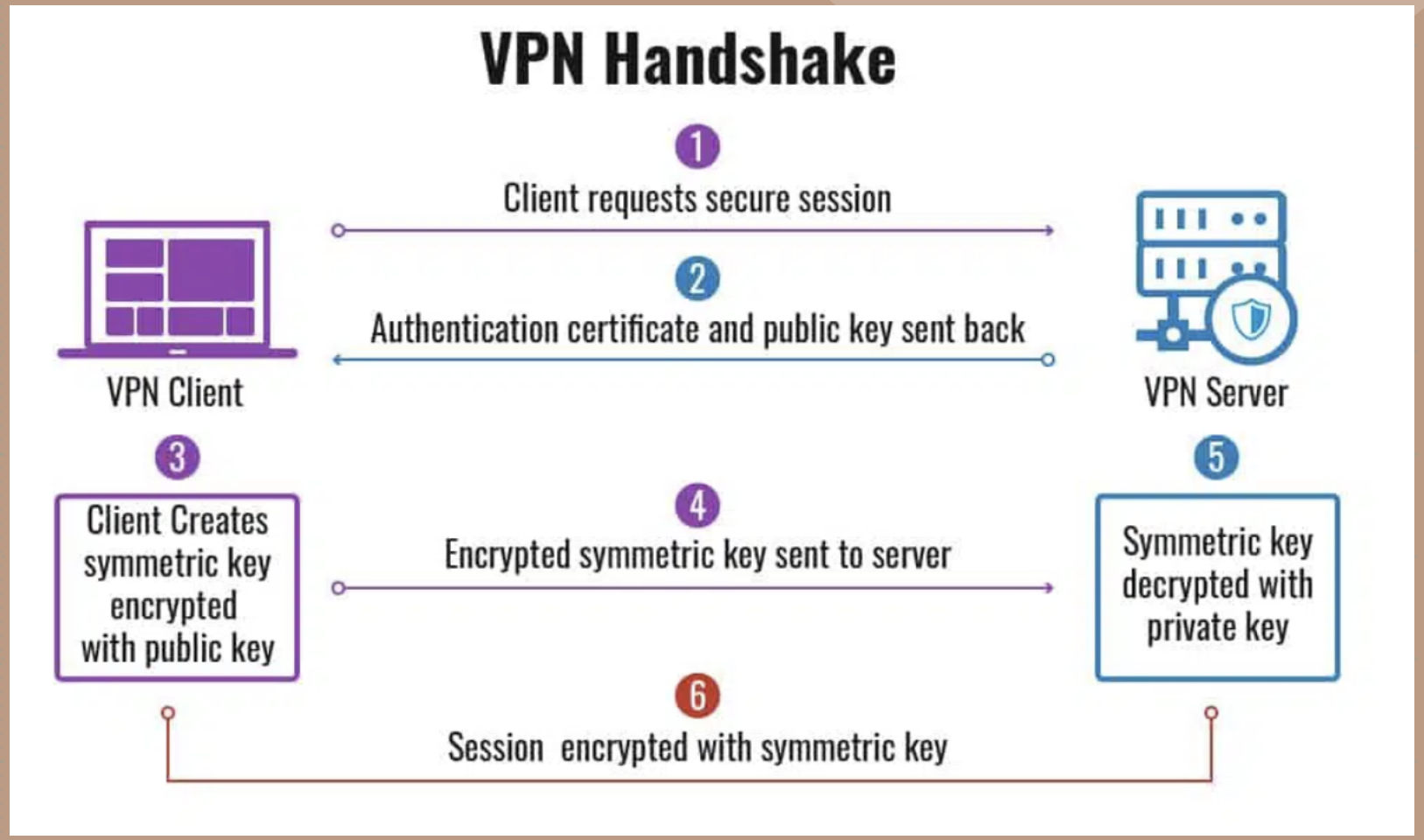
Most VPNs uses IP in IP tunneling

Figure 32.3 *Transport mode and tunnel modes of IPSec protocol*



VPN: Tunnelling

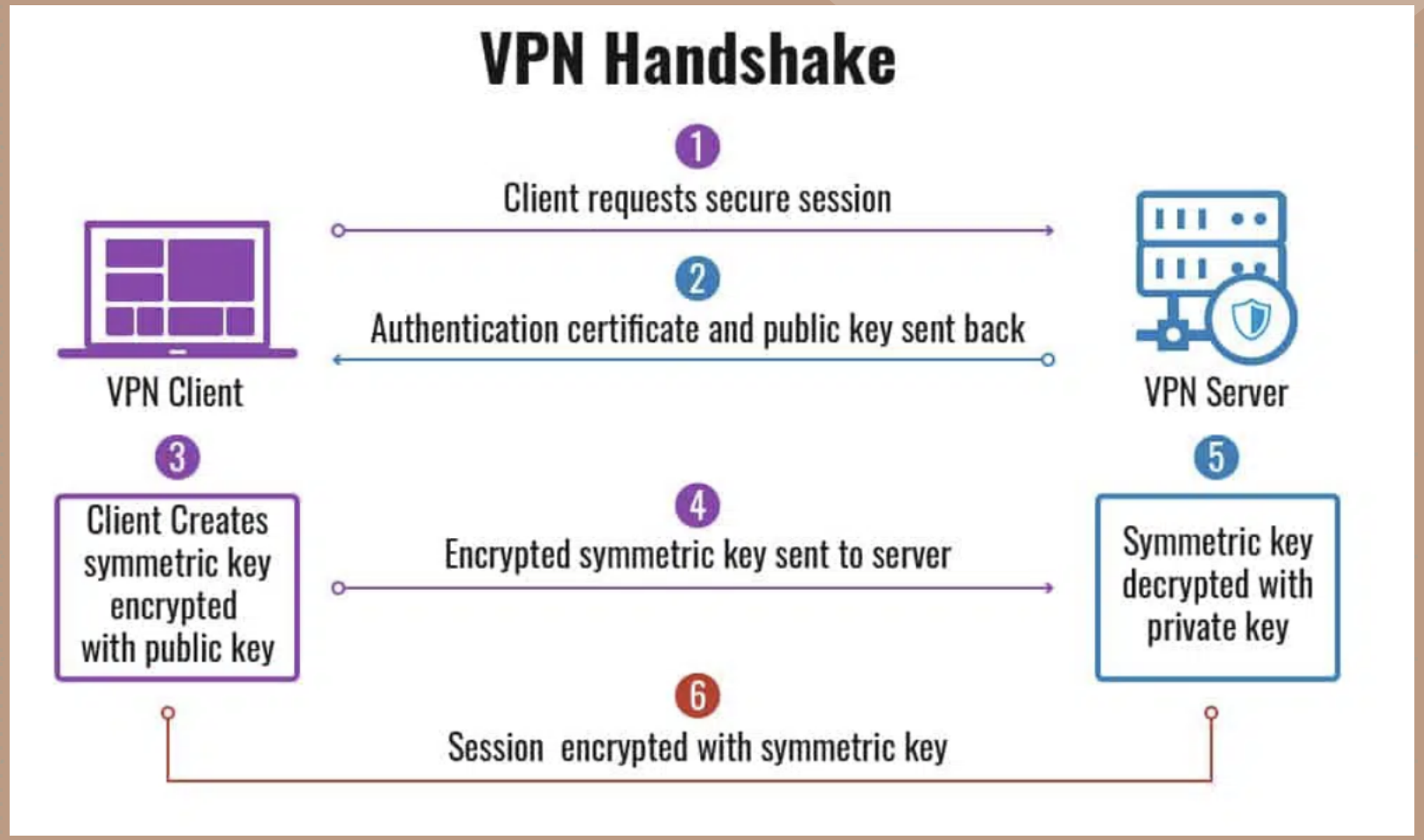
When you first connect to a VPN, your device and the VPN server perform a handshake and exchange encryption keys. This ensures that only the VPN server can decrypt data sent from your device and, conversely, only your device can decrypt data sent from the VPN server.



Source: https://www.comparitech.com/blog/vpn-privacy/vpn-tunneling/

VPN: Tunnelling

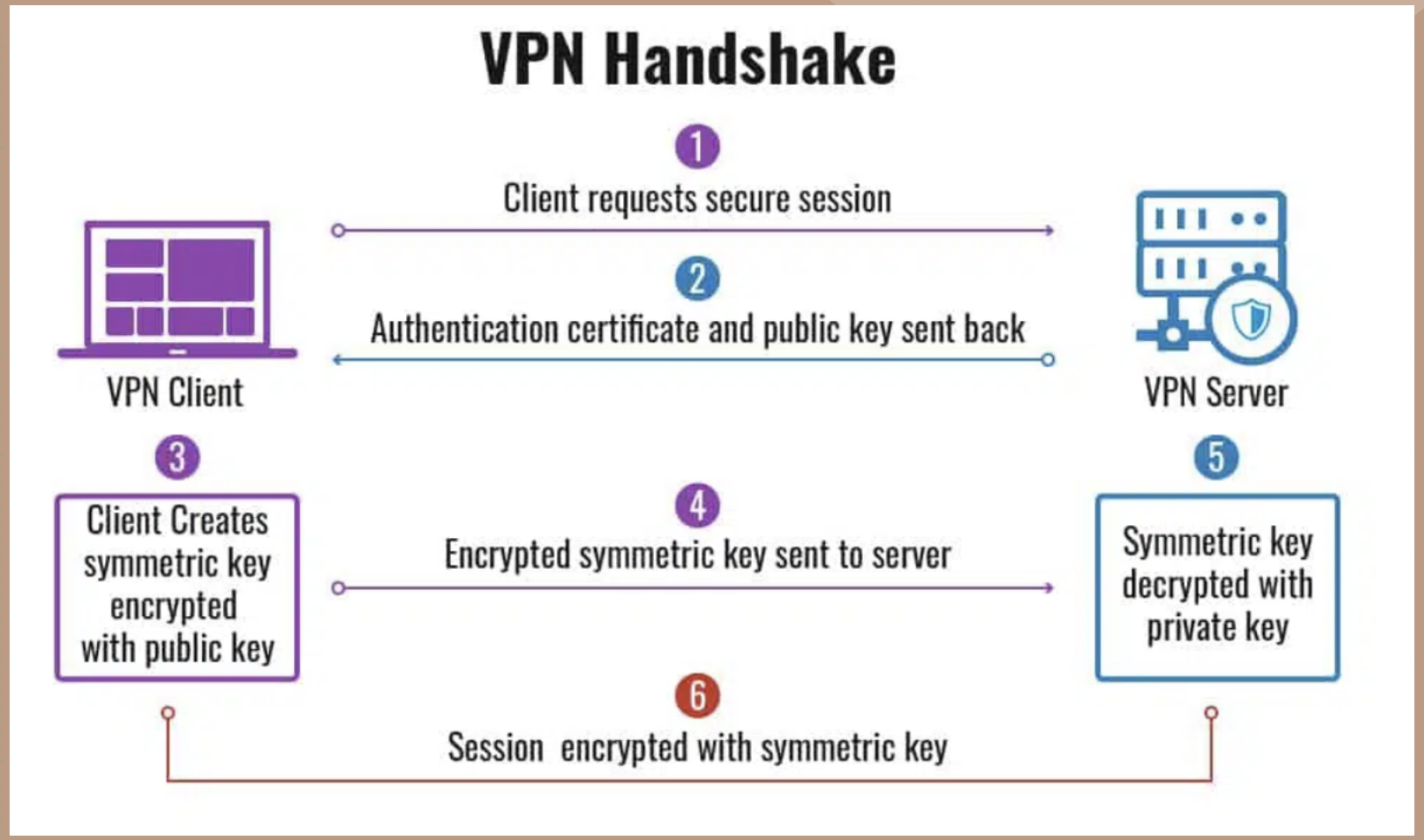
Once the connection is established, your device and the server can securely transmit data back and forth through the “tunnel”. Data is encrypted with the key before it ever leaves your device. When it reaches the VPN server, it is decrypted, then forwarded to the final destination—a website, app, streaming service, etc.



Source: https://www.comparitech.com/blog/vpn-privacy/vpn-tunneling/

VPN: Tunnelling

https://cybernews.com/what-is-vpn/



Source: https://www.comparitech.com/blog/vpn-privacy/vpn-tunneling/