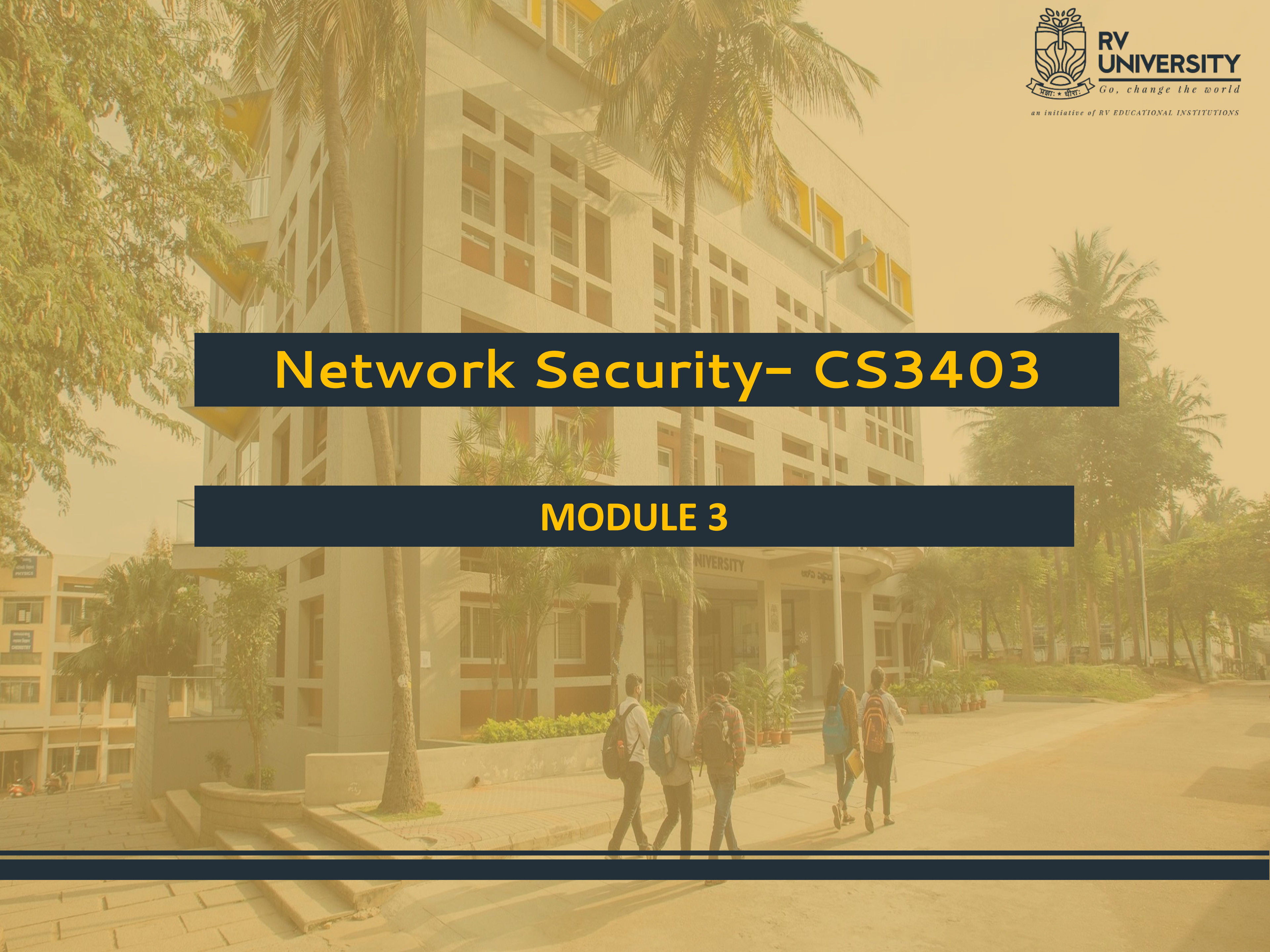


RV UNIVERSITY

Go, change the world

an initiative of RV EDUCATIONAL INSTITUTIONS

Network Security- CS3403

MODULE 3

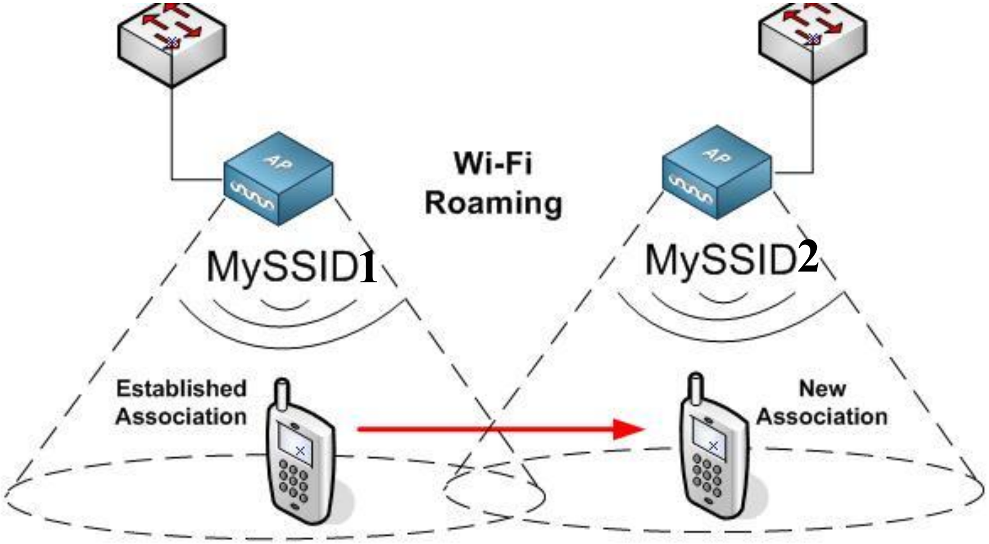
Network Security- CS3403

MODULE 3

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

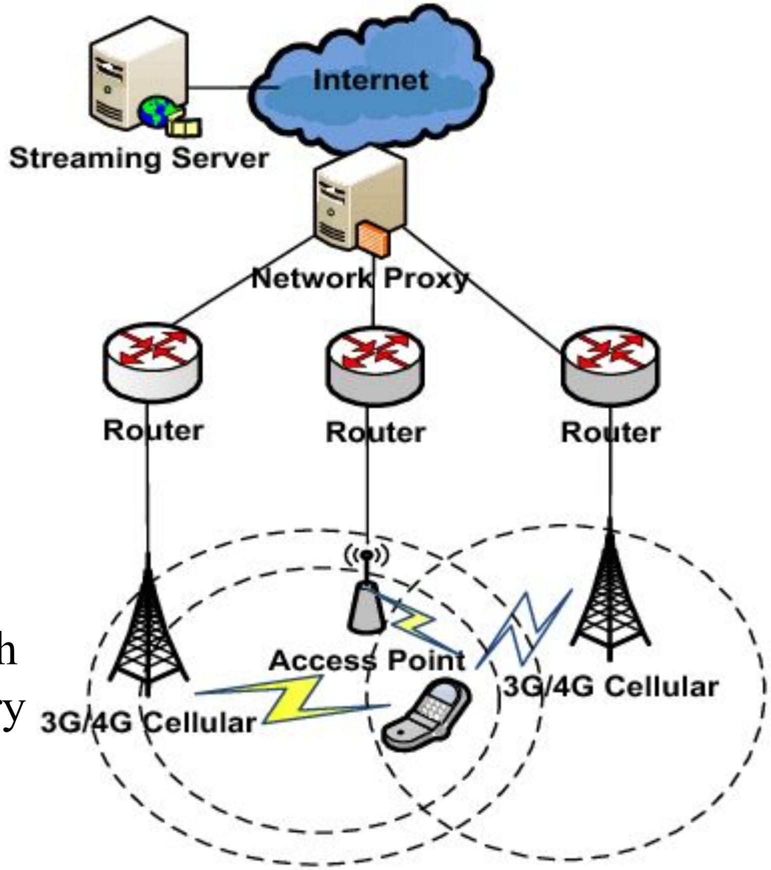
Mobile IP

Roaming Mobile Devices on Internet



Mobile devices moving from
one hotspot to another.

Mobile devices moving from
one BTS to another in 3G/4G Networks.



Note: It is not that only mobile devices transit through different networks, even laptops are also not stationary like desktops. In the college, your laptops connect to different WiFi routers on different subnets as you move across buildings or departments.

BTS: Base Transceiver Station

Routing among Mobile Devices

- It is very obvious that mobile devices present some challenges for the Internet architecture.
- The Internet was designed in an era when computers were large, immobile devices
- While the Internet's designers probably had some notion that mobile devices might appear in the future, it's fair to assume it was not a top priority to accommodate them.
- Today, of course, mobile computers are everywhere, notably in the forms of laptops and IP-enabled mobile phones, and increasingly in other forms such as sensors and IoT devices.
- Let us now look at some of the challenges posed by mobile devices connecting to Internet and some of the current approaches to accommodating them.

Mobile Devices on Internet

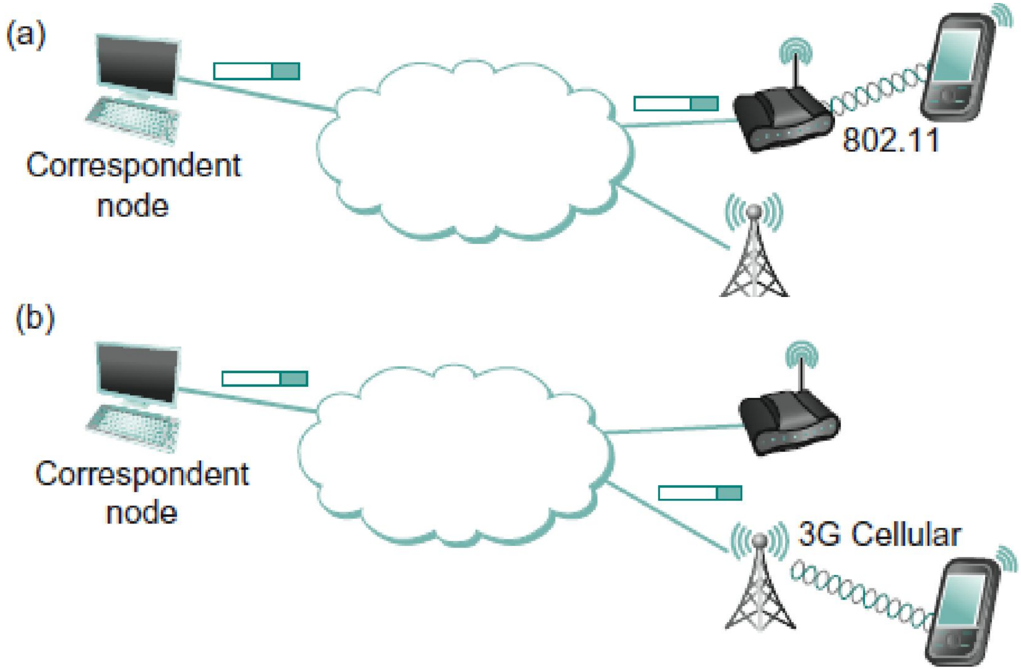
- Common ways mobile devices connect to Internet are:

1. Through cellular data networks (like 4G/5G) used for Internet access, VoIP calls, video calls, media streaming, etc.
2. Connecting through wireless hotspots (WiFi), Internet cafes, airport, or home supported by service providers.

- What do the mobiles devices need to communicate over Internet?
- A **unique IP address** for a mobile device to be recognized and for other hosts and routers on Internet to be in touch continuously with the mobile device, while it moves from one network to the other.
  - Scenario, while you are on a Skype call from the mobile, move from one hotspot to another or switch from WiFi to 3G network, without affecting the Skype call.

Connecting to a Hotspot and Moving Across …contd.

- Consequently, in the absence of some other mechanism, packets would continue to be sent to the address where the mobile device used to be, not where it is now.
- As the mobile node moves from an 802.11 network to a cellular network, somehow packets from the **correspondent node** need to find their way to the new network and then on to the mobile node.



- Assuming that there is some way to redirect packets, another important concern is:
  - To prevent some attacker **impersonating** the device and redirecting the packets meant for the device.

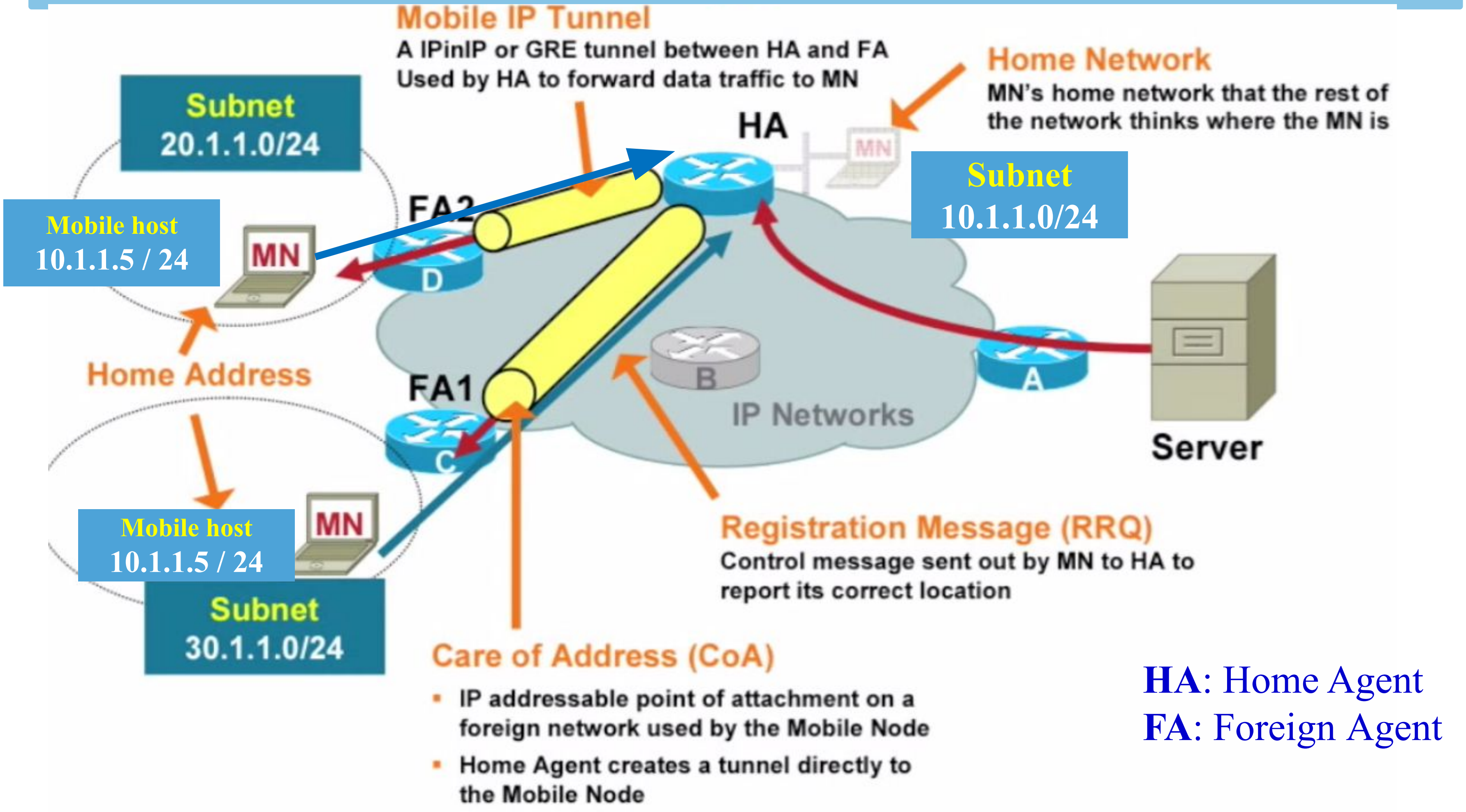
Impersonate: Pretend to be (another person) for entertainment or fraud

Mobility and Security are to be taken care of.

Correspondent node: The device which is having communication with a mobile device.

IP Tunneling (IP-in-IP)

IP Tunneling to Mobile Hosts



Mobile IP Tunnel

A IPinIP or GRE tunnel between HA and FA
Used by HA to forward data traffic to MN

Home Network

MN's home network that the rest of the network thinks where the MN is

Home Address

Registration Message (RRQ)

Control message sent out by MN to HA to report its correct location

Care of Address (CoA)

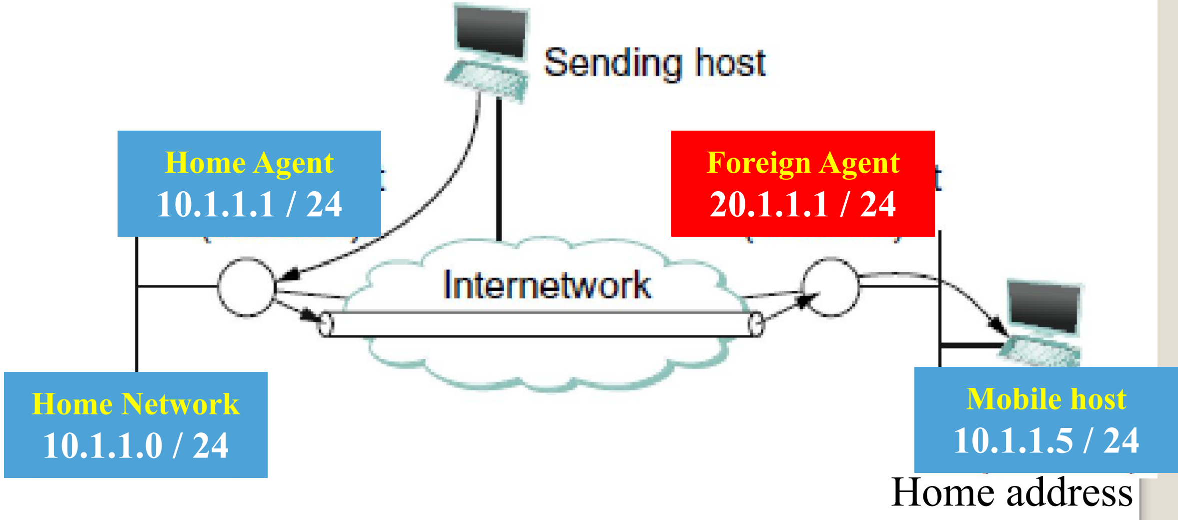
- IP addressable point of attachment on a foreign network used by the Mobile Node
- Home Agent creates a tunnel directly to the Mobile Node

HA: Home Agent
FA: Foreign Agent

GRE: Generic Routing Encapsulation (**GRE** is a **tunneling** protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links or point-to-multipoint links over an Internet Protocol network

Mobile Hosts and Home Address

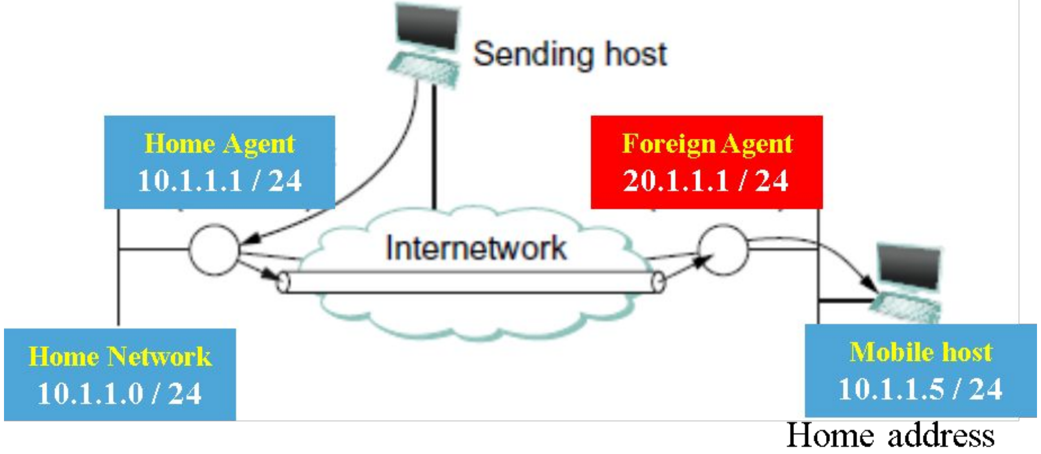
- The **mobile host** is assumed to have a permanent IP (10.1.1.5), called its **home address**, which has a network prefix equal to that of its **home network**.



- This is the address that will be used by other hosts when they initially send packets to the mobile host;
- Because it does not change, it can be used by long-lived applications (TCP connections, voice/video calls, etc.) as the host roams.
- We can think of this as the long-lived identifier of the host.
- When the **host moves** to a new **foreign network** away **from** its **home network**, it registers with the foreign agent by providing its home network details along with home agent's address.

Mobile Host on Foreign Network

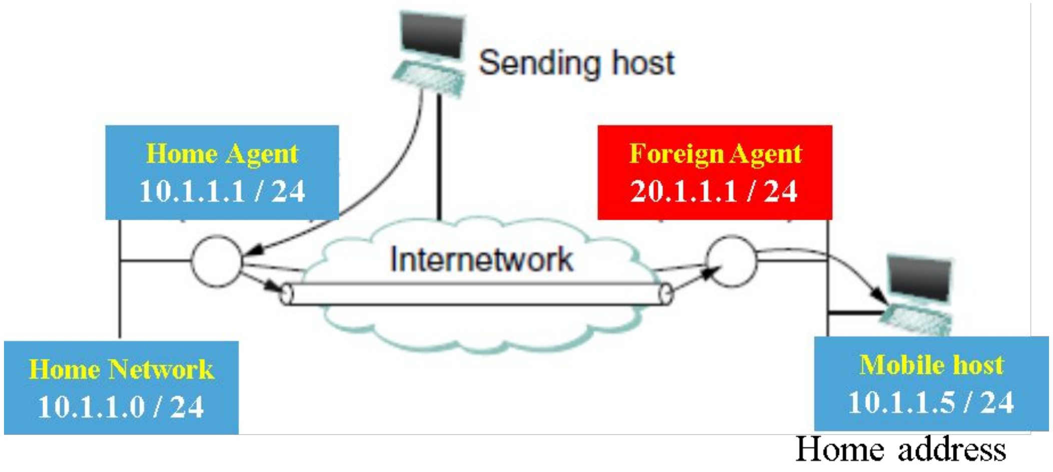
- It is important to note that the mobile host does not lose its permanent home address while it is on the foreign network.



- This home address is critical to its ability to sustain communications as it moves.
- While the routers in the core of the Internet remain unchanged, mobility support does require some new functionality in the routers in the home networks (**home agents)** of the mobile node and also the routers of the foreign networks (**Foreign agents**).
- This change is required for them to re-route the packets that arrive at the home agent to the mobile node in the foreign network through its current foreign agent.

Home Agents and Foreign Agents

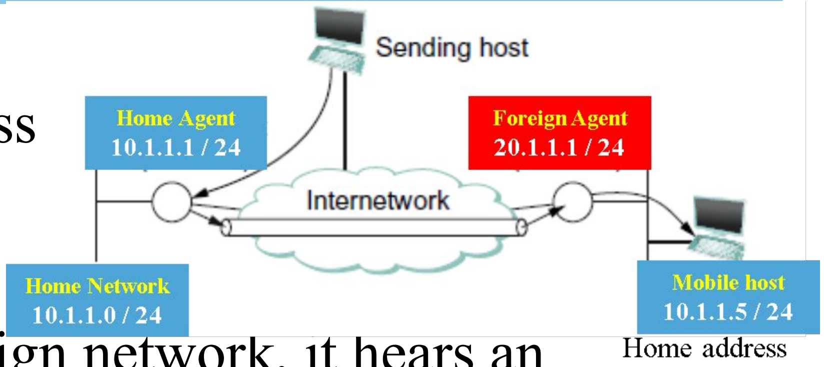
- **Home agent** is located on the home network of the mobile host.
- A second router with enhanced functionality is the **foreign agent** in the foreign network.



- Foreign agent is located on a network to which the mobile node attaches itself when it is away from its home network.
- Both home and foreign agents periodically announce their presence on the networks to which they are attached using agent advertisement messages.
- A mobile node may also solicit an advertisement when it attaches to a new network.

Steps taken by Mobile Host

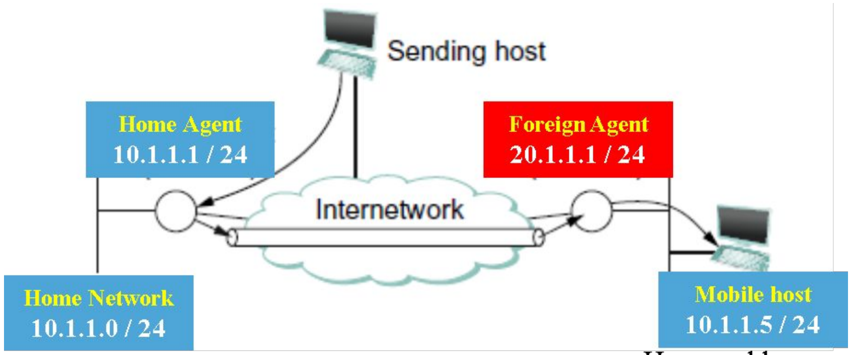
- The advertisement by the home agent enables a mobile host to learn the address (**10.1.1.1**) of its home agent before it leaves its home network.



- When the mobile host attaches to a foreign network, it hears an advertisement from a foreign agent and registers with the agent, providing the address of its home agent and its own IP address in its home network.
- The foreign agent then contacts the home agent, providing a **care-of address (its own address)** on behalf of the mobile device to its home agent.
  - This is the IP address (**12.1.1.1**) of the foreign agent.
- Since mobile host has a fixed home address, any device that tries to send a packet to the mobile host will always send it with a destination address equal to the home address of that node.
- Normal IP forwarding will cause that packet to arrive at the home network of the mobile node on which the **home agent** is part of (gateway).

Three Parts of Delivering Pkts to Mobile Host

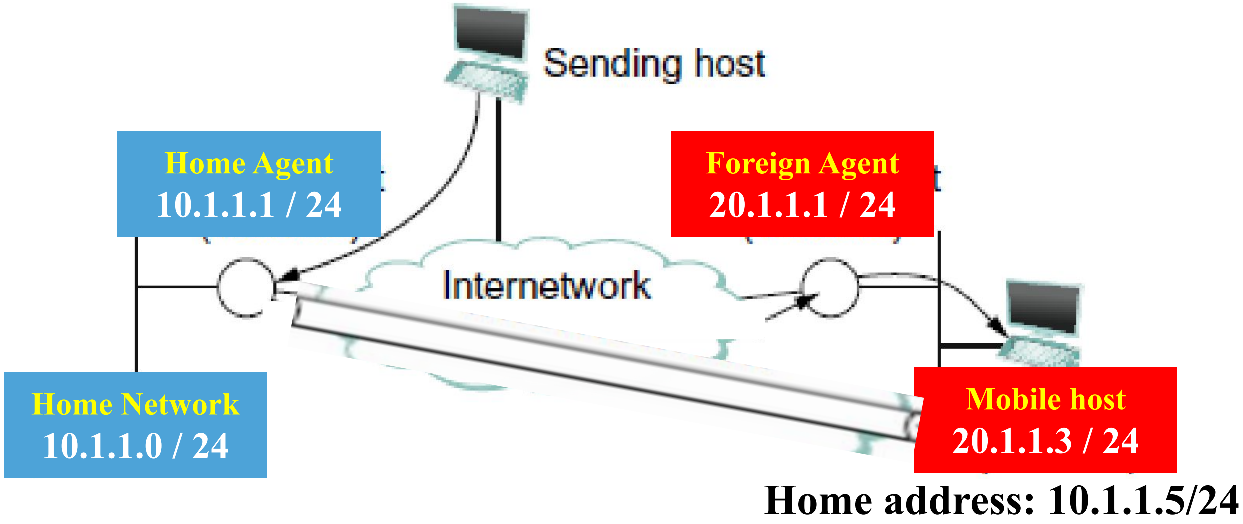
- Thus, we can divide the problem of delivering the packet to the mobile node into three parts:



Home address

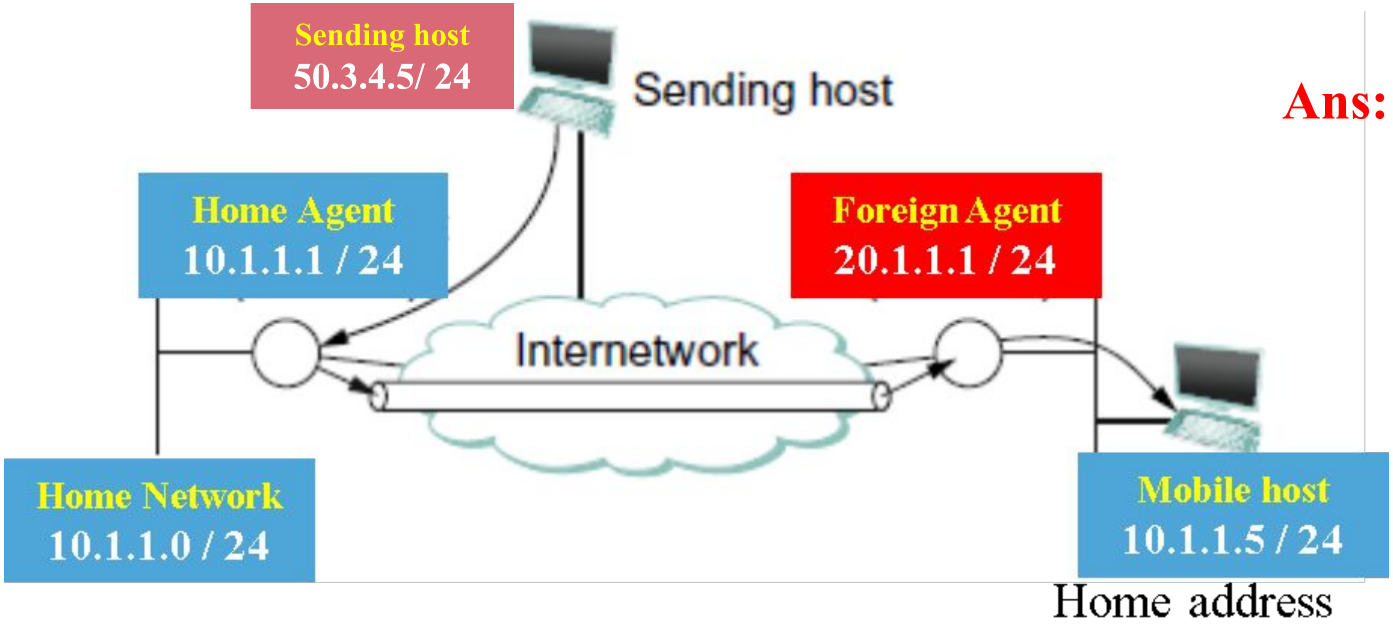
1. How does the home agent intercept a packet that is destined for the mobile node?
   - The home agent is the default gateway of the home network and thus it must receive all the packets that are destined to the mobile node.
2. How does the home agent then deliver the packet to the foreign agent?
   - Since it has learnt about the current **care-of-address** of the mobile node, it prepares another IP packet to be delivered to foreign agent, by packing the original IP packet of mobile node and sends it out. – **IP Tunnelling**
3. How does the foreign agent deliver the packet to the mobile node?
   - The foreign agent is the default gateway of the foreign network and thus it must receive all the packets that are destined to the **foreign agent (FA)** and because of the mobile node's registration with it, FA can now deliver the original IP packet sent by the home agent by unpacking it and deliver it through the datalink layer (MAC address of mobile node) of the foreign

Co-located Care-of-address



- **Another scenario** is where the mobile host gets a new IP address (**20.1.1.3**) in its current foreign network through DHCP.
- Here, the **mobile host** informs its **home agent** about its current **co-located care-of-address** in its current foreign network.
- In this case the **co-located care-of-address** is used by the Home Agent to forward the traffic destined to the mobile host directly.

Quiz 1: Mobile host from a Foreign Network



Sending host
50.3.4.5/ 24

Sending host

Home Agent
10.1.1.1 / 24

Foreign Agent
20.1.1.1 / 24

Internetwork

Home Network
10.1.1.0 / 24

Mobile host
10.1.1.5 / 24

Home address

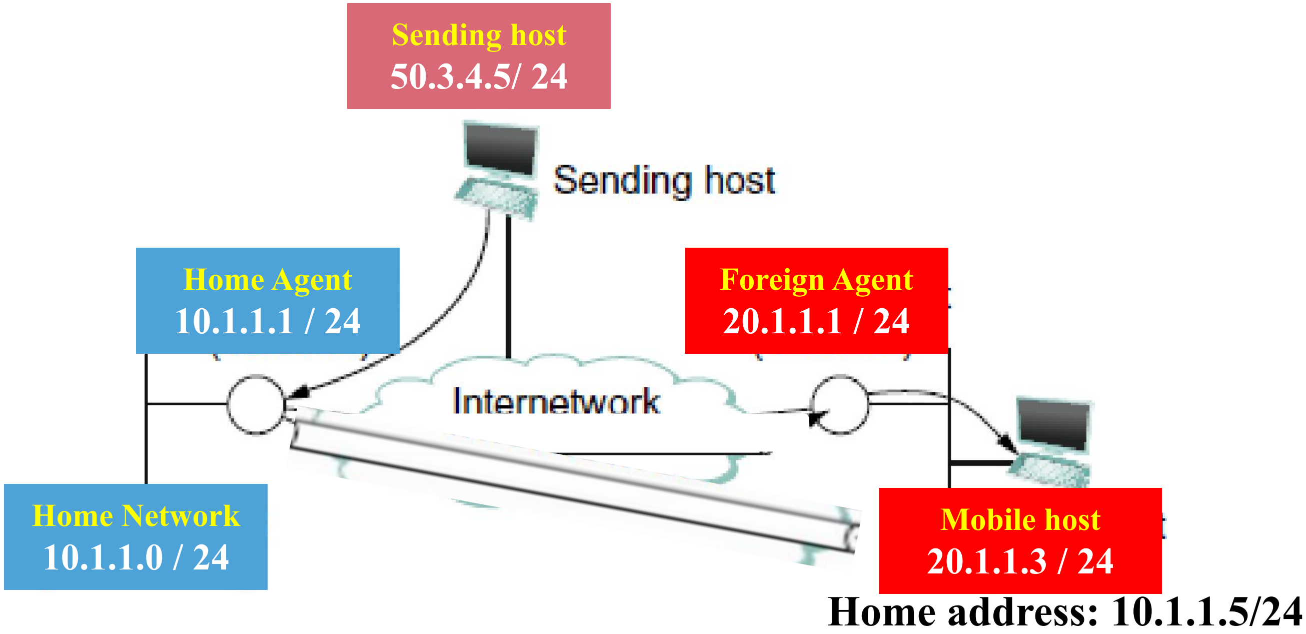
Ans: C

- When the mobile host from the current foreign network sends a packet to the sending host, the **Source IP** and **Destination IP** fields respectively would be:

A. Src: 10.1.1.5 and Dest: 20.1.1.1
B. Src: 10.1.1.5 and Dest: 10.1.1.1
C. Src 10.1.1.5 and Dest: 50.3.4.5
D. None of the given options is correct.

Note: The packets from the mobile node do not go through the home Agent, they go straight to the sending host. No IP tunneling is required. IP tunneling is only required to receive packets from the sending host by the mobile node.

Quiz 2: Sending host to a mobile node in a Foreign Network with a co-located care-of-address



Ans: B

- When the sending host sends a packet to the mobile node, the **Source IP** and **Destination IP** fields respectively would be:

A. Src: 50.3.4.5 and Dest: 20.1.1.3

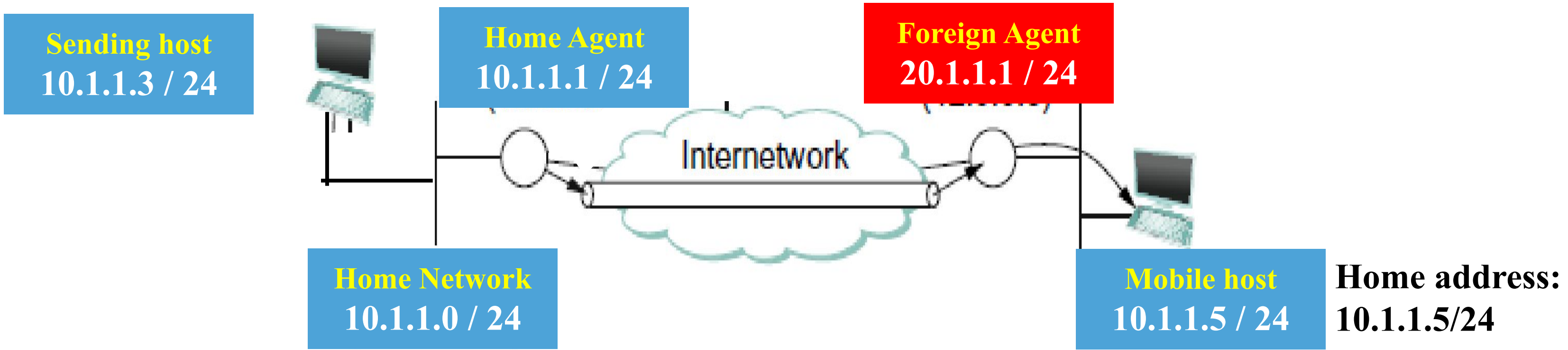
B. Src: 50.3.4.5 and Dest: 10.1.1.5

C. Src 50.3.4.5 and Dest: 10.1.1.1

D. Src 50.3.4.5 and Dest: 20.1.1.1.

Note: Even if the mobile node has been assigned A new IP address in its foreign network, the Sending host is not aware of it is current location, tt continues to send the packets to its original Home address. It is intercepted by the HA and IP tunneling is done directly to the Mobile node to its co-located care-of-address.

Proxy ARP: Sending Hosts in the Home Network



Sending host 10.1.1.3 / 24

Home Agent 10.1.1.1 / 24

Foreign Agent 20.1.1.1 / 24

Home Network 10.1.1.0 / 24

Mobile host 10.1.1.5 / 24

Home address: 10.1.1.5/24

- If the sending host is also on the home network and trying to contact the mobile host, then the packets from it would never reach the mobile host, since the mobile host is not currently in the home network.
- To address this problem, the home agent actually impersonates the mobile node, using a technique called **proxy ARP**.
- It works same as ARP except that the home agent inserts the MAC address of its own, in its ARP response, impersonating the mobile node.
- So, the packets from the sending host first reaches the home agent:
  - which takes care of tunneling it to the mobile node through its current care-of-address of foreign agent or directly to the co-located care-of-address, which the sending host needn't be aware of.

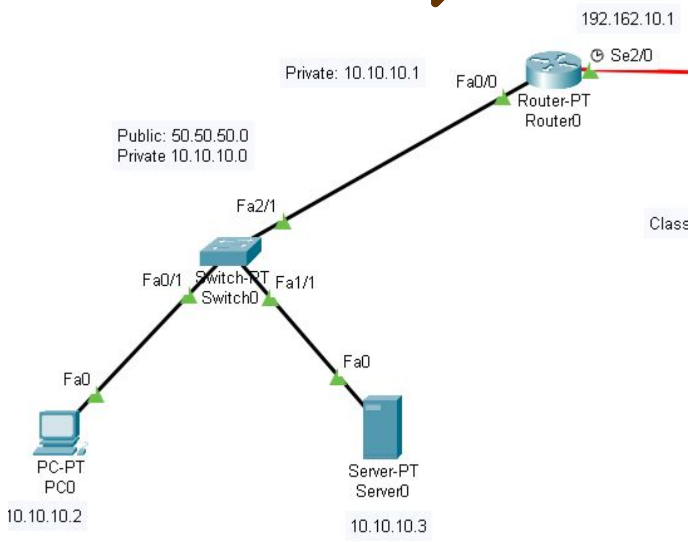
Network Address Translation (NAT)

NAT: An Introduction

- NAT is essentially a mechanism for allowing the same sets of IP addresses (Private IPs) to be reused in different parts of the Internet
- The primary motivation for the creation of NAT was the limited and diminishing availability of IP address space.
- NAT was introduced to solve two problems: **address depletion** and **concerns regarding the scalability of routing**.
  - Reduced number of globally routable Public IP addresses in the Internet
- It also protects the hosts within private network by not exposing their private IP addresses (**security**)

NAT: How it Works

Private IP
Src IP: 10.10.10.2 ⇨ **Public IP**
Src IP: 50.50.50.2



4. NAT is configured in the router which is interfacing a private NW with the Public NW
5. Source IP address of every IP pkt going out is replaced with a public IP and checksum of the IP header recalculated.
6. Src IP is again replaced with its own private IP addr on incoming packets before delivering it to the respective hosts.

1. NAT modifies IP addresses in packet headers while they are sent out of a private network to public network (Internet).
2. The **Private source IP addresses** of the hosts are **replaced** with **Public IP addresses**
3. It allows multiple devices on a private network to share a single or a limited set of public IP addresses to access the Internet.

NAT: Three Types

- **Static (one-to-one):**
  - Maps one private IP to one public IP.
  - Useful for servers that need to be publicly accessible.
  - IP translation remains fixed.

Q1:Is there any saving of IP addresses here?

ANS: NO

- **Dynamic (many-to-many):**
  - Uses a pool of public IPs and maps internal private IPs dynamically.
  - The router assigns an available public IP whenever a device needs access.
  - Normally the available public IP addresses are much lower than no. of Private hosts using them.

Q2:Which pool of IPs is likely to be more in numbers?

ANS: Private Pool of IPs

- **Port-based (many-to-one):**
  - Also called NAT Overload.
  - Multiple private IPs share a single public IP.
  - Uses different port numbers for each connection.

Q3:Can the same Public IP be sent out by different applications?

ANS: Yes

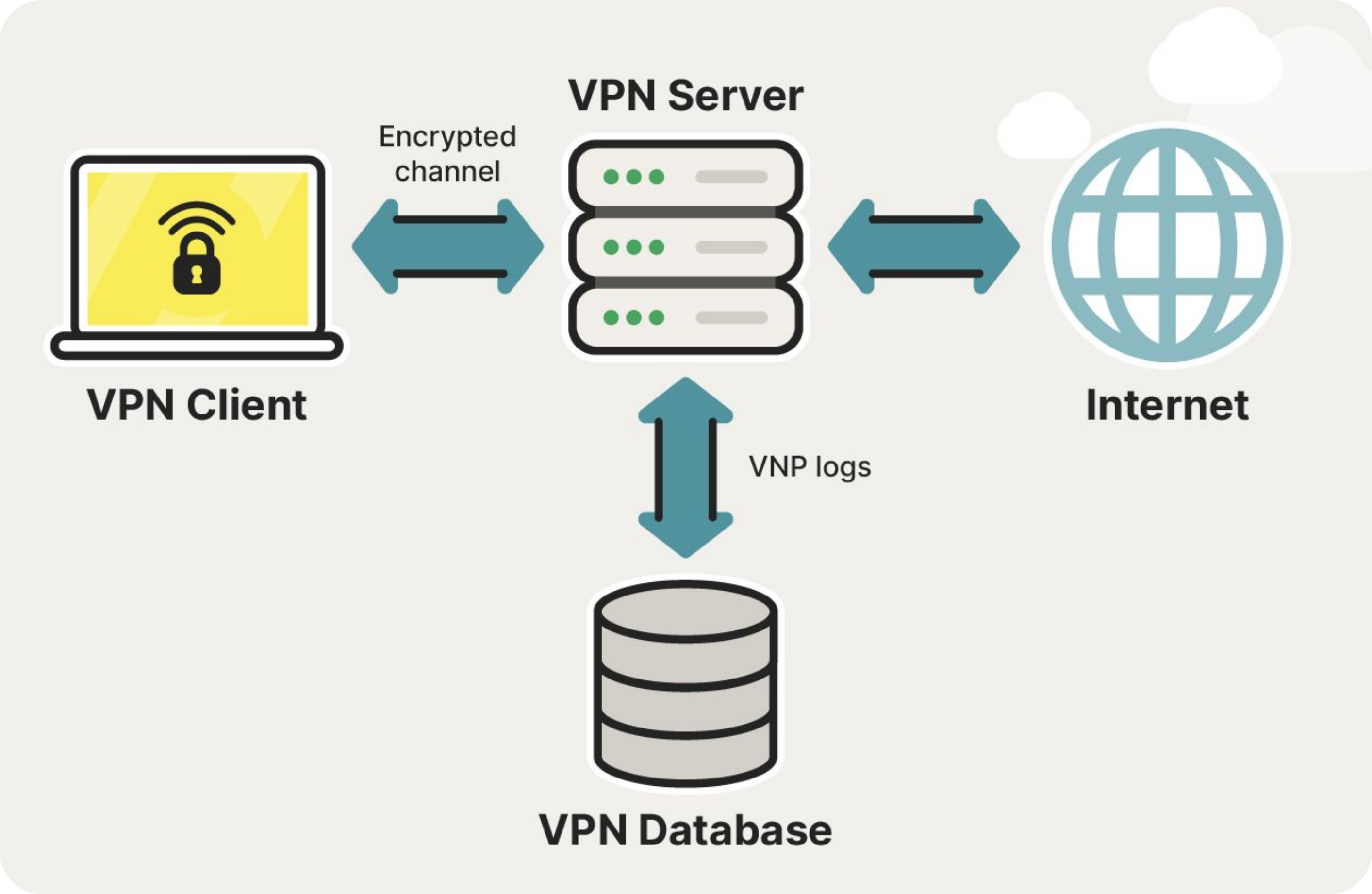
NAT: Drawbacks

- Offering Internet-accessible services from the private side of a NAT requires special configuration because privately addressed systems are not directly reachable from the Internet
- For a NAT to work properly, every packet in both directions of a connection or association must pass through the same NAT (router).
- NATs require connection state on a per-association (or per-connection) basis and must **operate across multiple protocol layers**, unlike conventional routers.
- NAT poses problems for some application protocols (File Transfer Protocol), because it sends IP addressing information inside the application-layer payload.
  - FTP uses two connections (control and data) before transferring data
  - FTP shares the IP address and port number for the data transfer through control connection (as application payload)

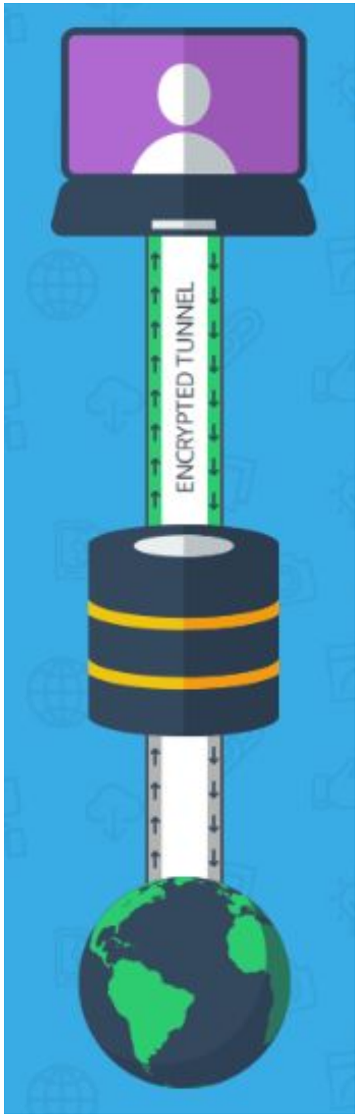
RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

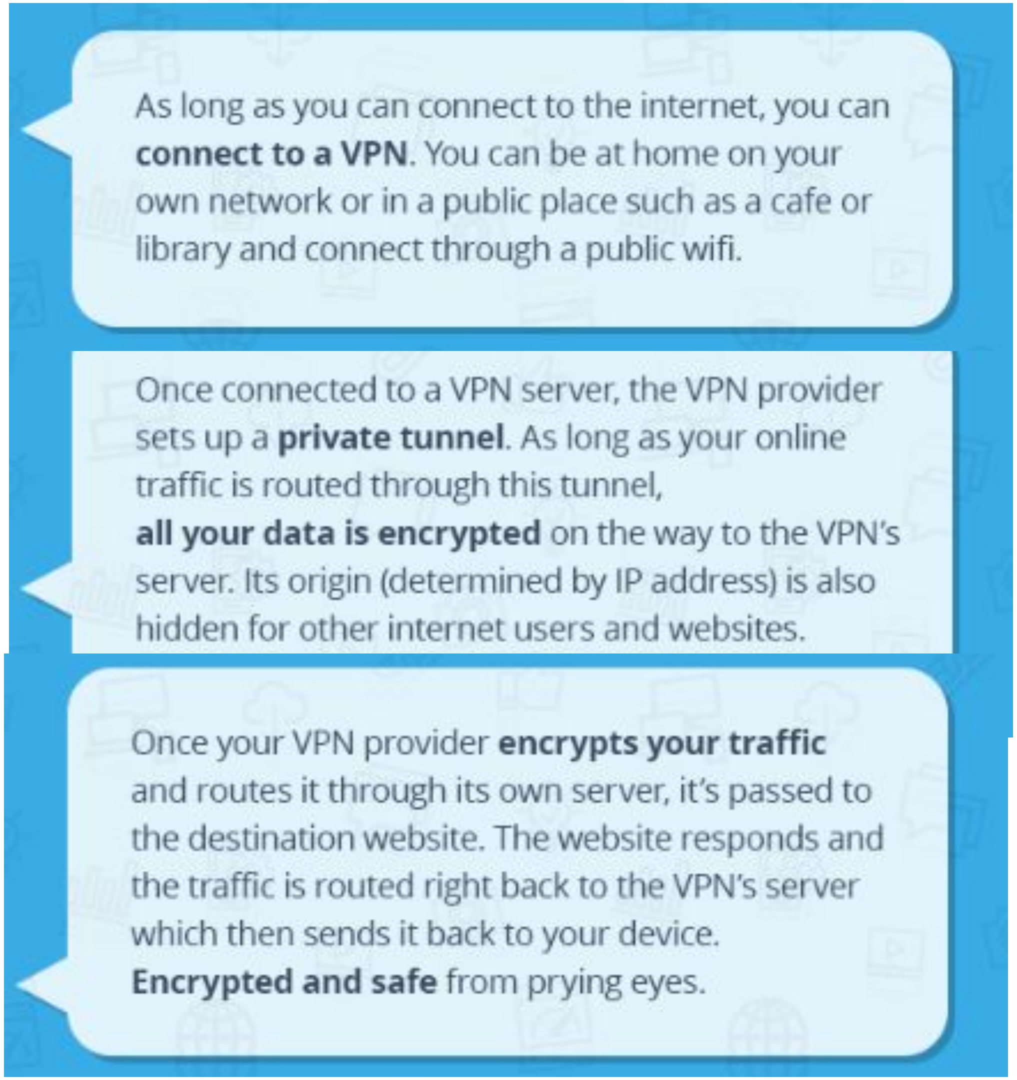
VPN

Connecting through VPN Server



VPN: Explained





As long as you can connect to the internet, you can **connect to a VPN**. You can be at home on your own network or in a public place such as a cafe or library and connect through a public wifi.

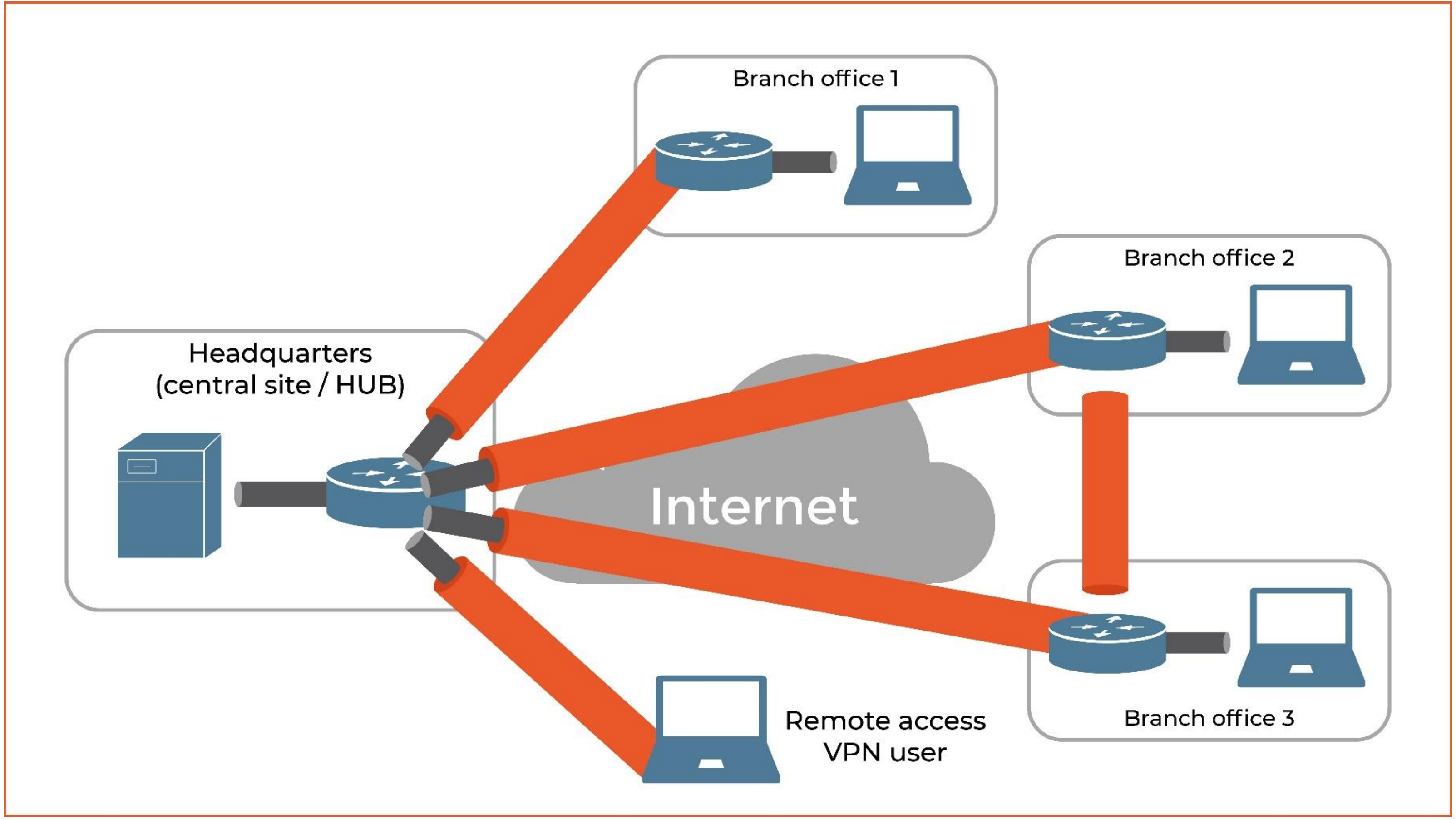
Once connected to a VPN server, the VPN provider sets up a **private tunnel**. As long as your online traffic is routed through this tunnel,
all your data is encrypted on the way to the VPN's server. Its origin (determined by IP address) is also hidden for other internet users and websites.

Once your VPN provider **encrypts your traffic** and routes it through its own server, it's passed to the destination website. The website responds and the traffic is routed right back to the VPN's server which then sends it back to your device.
Encrypted and safe from prying eyes.

Password
+ token

VPN for Connecting Branch Offices

Ref: Lab 8 Implementation of VPN using CISCO Packet Tracer.



Note: Once a VPN tunnel is successfully established, it acts like a virtual pipe through which IP packets flow both ways

Quiz 5: VPN

- Which of the following is a commonly used VPN protocol that supports encryption and runs at Layer 3 of the OSI model?

A. FTP

B. HTTP

C. IPSec

D. None of the above.

ANS: C

Note:

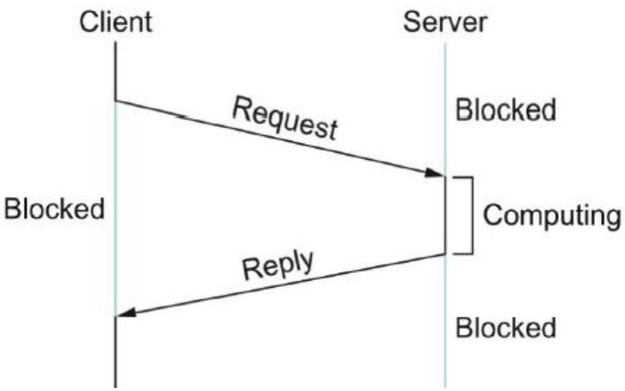
IPSec is a widely used **VPN** protocol that works at the Network Layer (Layer 3) of the OSI model and provides encryption, authentication, and integrity.

Remote Procedure Call (RPC)

RPC: Remote Procedure Call

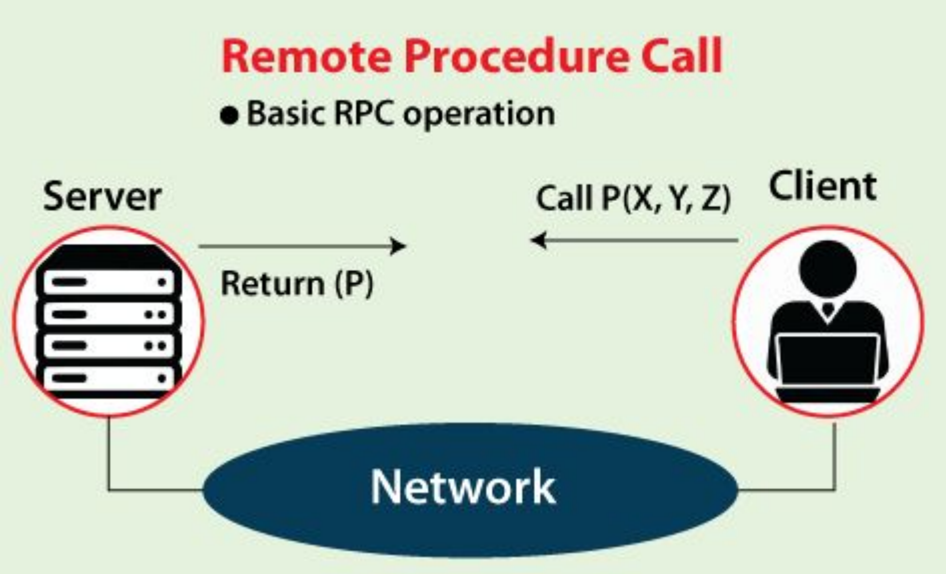
- **RPC** follows **request/reply message transaction**.

1. A client sends a request message to a server.
2. The server responds with a reply message.
3. The client blocking (suspending execution) to wait for the reply.



- **RPC** is not a protocol; it is a mechanism for structuring **distributed systems**.
- Here, an application program makes a call into a procedure without regard for whether it is local or remote and blocks until the call returns.
- When the procedures being called are actually, methods of remote objects in an object-oriented language, RPC is known as **Remote Method Invocation (RMI).**

RPC: Problems



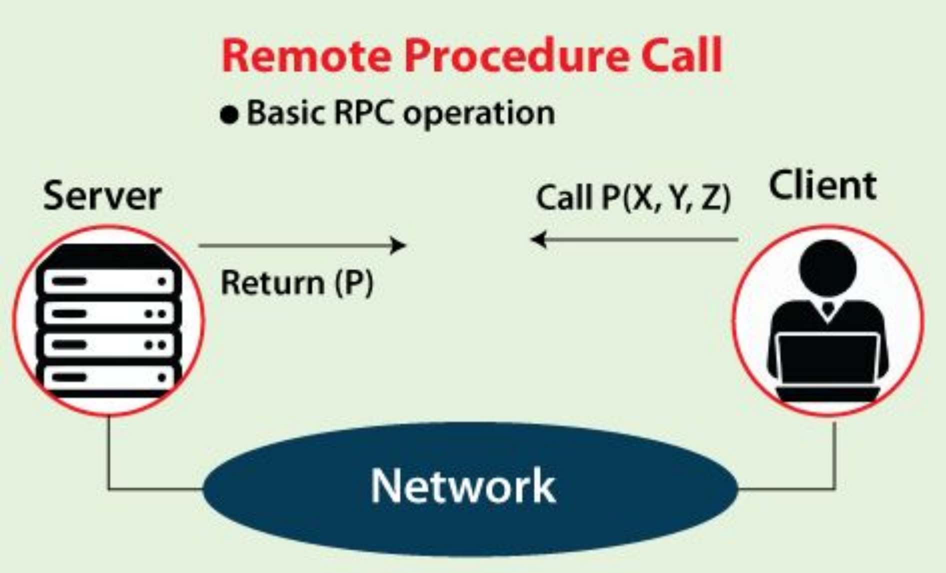
- Calling a procedure to be executed over a network is lot more different from calling it within a computer.
- The **two main problems** are:

1. Network can limit message sizes and also it has a tendency to lose or reorder messages sent over it.
2. The computers on which the calling and called processes run may have significantly different architectures and data representation formats, etc.

RPC: Major Components

- A complete **RPC mechanism** involves **two major components**

1. A protocol to manage the messages sent between the client and the server to deal with the potentially undesirable properties of the underlying network.

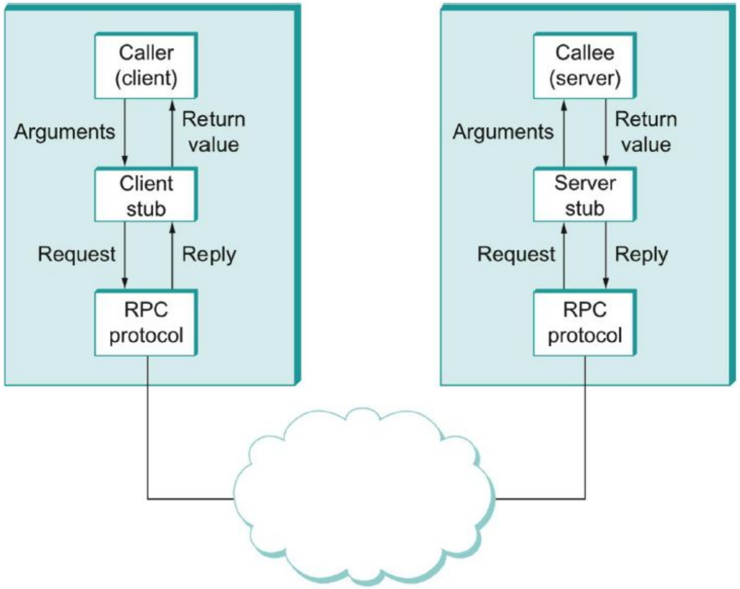


2. Programming language and compiler that support packaging **arguments** to the method into a request message on the client machine and then translates the message back into the arguments on the server machine before running.
3. Likewise, it handles the **return value** from the method on the client side (this piece of the RPC mechanism is usually called a **stub compiler**).

RPC Mechanism

RPC Mechanism

- The client calls a local stub for the procedure, passing it the arguments required by the procedure.
- This stub hides the fact that the procedure is remote by translating the arguments into a request message and then invoking an RPC protocol to send the request message to the server machine.

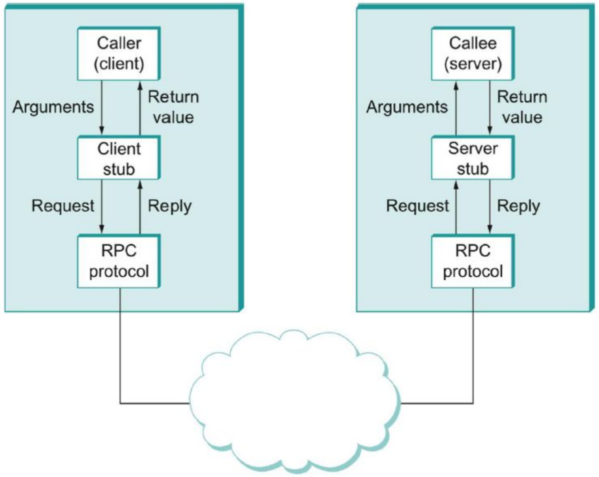


- At the server, the RPC protocol delivers the request message to the server stub, which translates it into the arguments to the procedure and then calls the local procedure.
- After the server procedure completes; it returns in a reply message that it hands off to the RPC protocol for transmission back to the client.
- The RPC protocol on the client passes this message up to the client stub, which translates it into a return value that it returns to the client program.

RPC Protocol

RPC Protocol

- RPC protocol, sometimes referred to as a **request/reply protocol**, that transmits messages between client and server.
- The term RPC refers to a type of protocol rather than a specific standard like TCP, so specific RPC protocols vary in the functions they perform.



- **Two functions** that must be performed by any **RPC protocol** are:
  - Provide a **name space** for uniquely identifying the procedure to be called
  - **Match** each reply message to the corresponding request message
- Especially in systems with multiple outstanding requests, concurrent clients, asynchronous messaging.
- It is essential for correct sequencing of responses, retransmissions or retries and avoiding mismatches in multi-threaded or multi-client environments

RPC: Key Features

- **Transparency**: The remote function appears local to the caller.
- **Stubs**: Automatically generated code that handles network communication.
- **Protocol-agnostic**: Can run over TCP, UDP, HTTP, or other transports.
- **Synchronous or Asynchronous**: RPC can block until the result is received, or it can work non-blocking in async mode.
- **Stateless or Stateful**: Depending on the implementation.

RPC: Use cases - Info

1. Microservices Communication

- Frameworks like **gRPC** (Google RPC) use Protocol Buffers and HTTP/2 to enable fast, efficient service-to-service communication in cloud-native systems.

2. Distributed Systems

- RPC is the foundation for communication between nodes in distributed file systems, clustered databases, and cloud platforms.

3. Client-Server Applications

- Traditional client-server apps (especially in enterprise) use RPC for calling functions on backend systems from a UI or client.

4. OS-level RPC (ONC RPC)

- Used in **NFS (Network File System)**, **NIS**, and other UNIX services.

5. Web & Mobile Apps

- RPC-style APIs (like **JSON-RPC**, **XML-RPC**) offer simple ways to call backend procedures over HTTP.

6. Game Networking

- Multiplayer games use RPC-like calls to sync actions between clients and servers in real time.

RPC: Quiz 1 to 2

Quiz 1: RPC

- Which of the following is a potential drawback of using RPC in a networked environment?

A. Increased complexity in error handling due to network failures
B. Limited support for multiple programming languages
C. Inability to scale beyond a single network segment
D. Requirement for specialized hardware to handle remote calls

ANS: A

Quiz 2: RPC

- In the context of RPC, what is the role of a 'stub’?

A. It serves as a placeholder for unimplemented functions

B. It translates requests and responses between client and server

C. It manages memory allocation for remote procedures

D. It establishes the physical connection between client and server

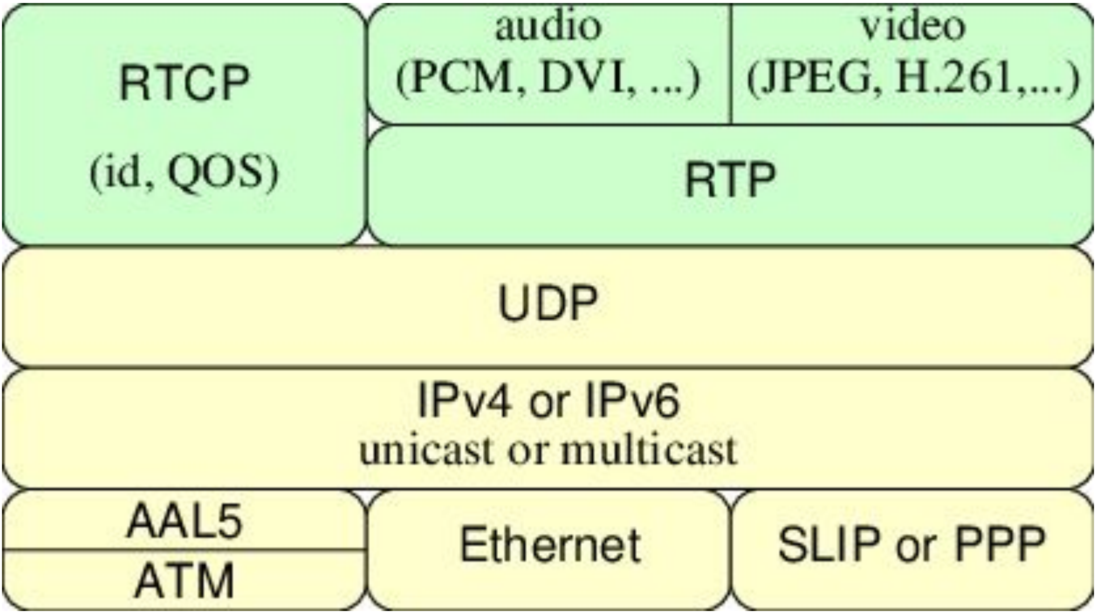
ANS: B

Real-Time Transport Protocol (RTP)

RTP: Introduction

- **RTP** is a protocol used for delivering real-time data,
  - Audio, Video, Sensor data, Interactive media (VoIP, video conferencing)
- It was standardized by the IETF in RFC 3550 and is often used alongside **RTCP** (Real-time Control Protocol)
- **RTP** itself **does not provide reliability**. It's intentionally lightweight to support **low-latency delivery**.

- It works only over **UDP** for a low-latency delivery
- RTP is designed primarily for speed, not reliability.
- RTP uses the demultiplexing function support of UDP using its port numbers.



RTCP (id, QOS)

audio (PCM, DVI, ...)

video (JPEG, H.261,...)

RTP

UDP

IPv4 or IPv6
unicast or multicast

AAL5
ATM

Ethernet

SLIP or PPP

RTP: Explained

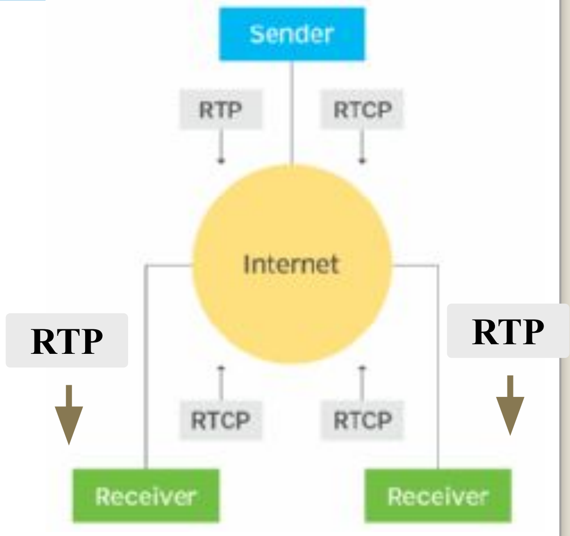
- Designed to handle time-sensitive data like audio, video, and sensor streams.
- It provides continuous, time-aligned delivery.
- RTP includes a sequence number field to detect packet loss and to maintain correct order of playback
  - Receivers buffer the data before playing back to avoid **jitter**
- Each packet includes a **timestamp** to synchronize the media streams (both audio and video). Timestamps are based on **sampling clock**.
- RTP includes a **payload type** field to notify the receiver the codec used (e.g., G.711, Opus, H.264) for the media stream
- RTP supports both **unicast** and **multicast** delivery.
  - Multicast for conferences or broadcasts and unicast for one-to-one communication like VoIP

Jitter: Variation in the time taken by the data packets to travel across a network

Real-time Transport Control Protocol (RTCP)

RTCP: Explained

- **RTCP** is the control protocol that works hand-in-hand with RTP to monitor transmission quality and help synchronize media streams
- **RTP** handles sending the actual **media data** over the network
- **RTCP** handles **reporting, feedback, and synchronization**.



- The following RTCP packets are send periodically (every few seconds)

1. **Sender reports (SR)** from RTP senders used for stream synchronization and throughput monitoring
2. **Receiver reports (RR)** sent by the RTP receivers that includes packet loss, jitter, round-trip time, to help the sender to adapt sending rates
3. **Source description (SDES)** shares sender identity useful in the multi-party conference calls.
4. **Bye** indicates a source is leaving (e.g., user disconnects)

RTP and RTCP: Quiz 1 to 3

Quiz 1: RTP

- Which transport layer protocol is typically used by RTP?

ANS: B

A. TCP

B. UDP

C. IP

D. ICMP

Note:
RTP prefers UDP due to its low-latency, connectionless nature — essential for real-time communication.

Quiz 2: RTCP

- What does RTCP provide in an RTP-based session?

A. Encryption for media

B. Routing of RTP packets

C. Feedback on media delivery quality

D. Compression of RTP data

ANS: C

Quiz 3: RTCP types

- Which of the following RTCP packet types is used to report packet loss, jitter, and delay?

A. SR

B. RR

C. SDR

D. Bye

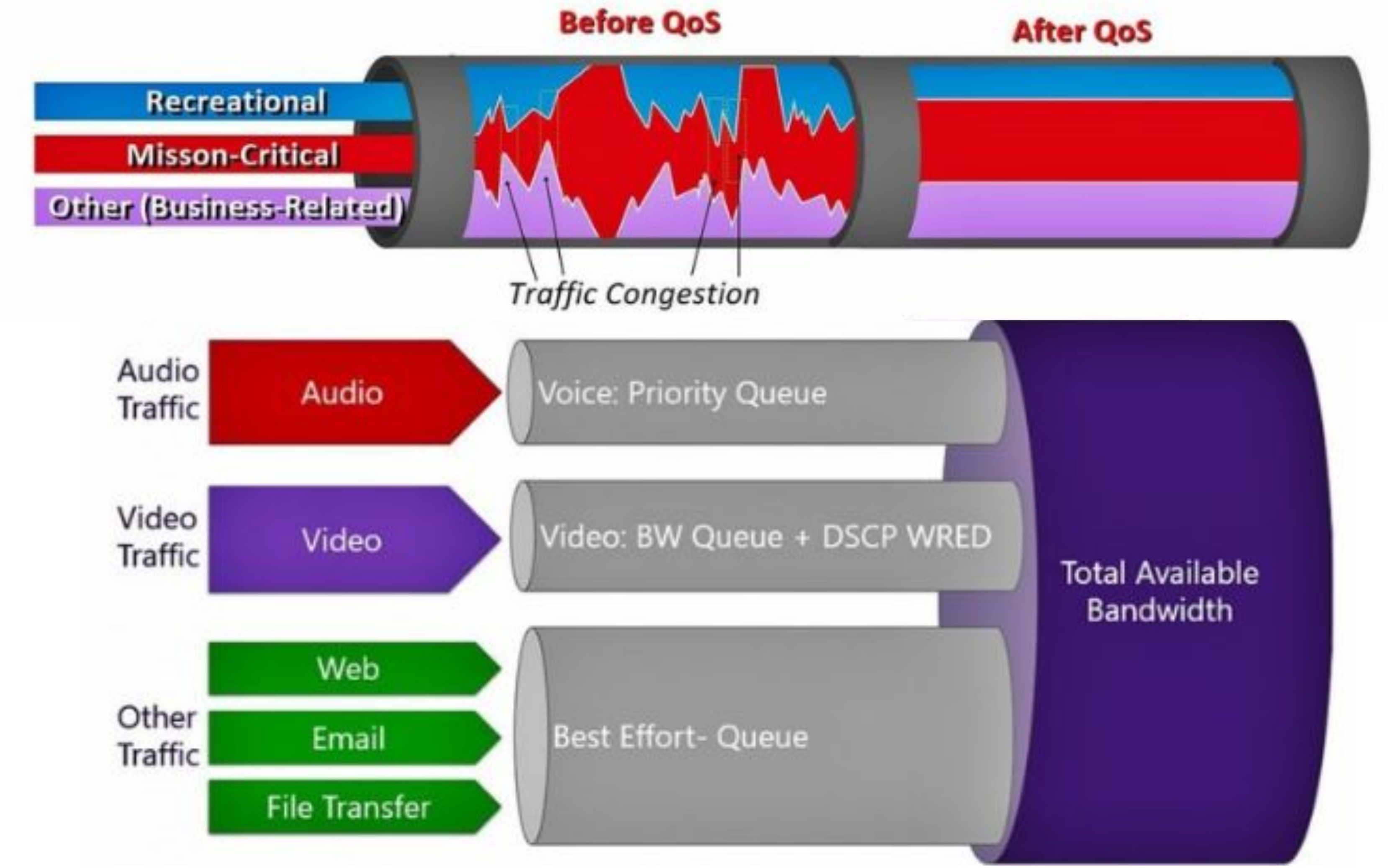
ANS: B

Quality of Service (QoS)

What is QoS?

Source:

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS



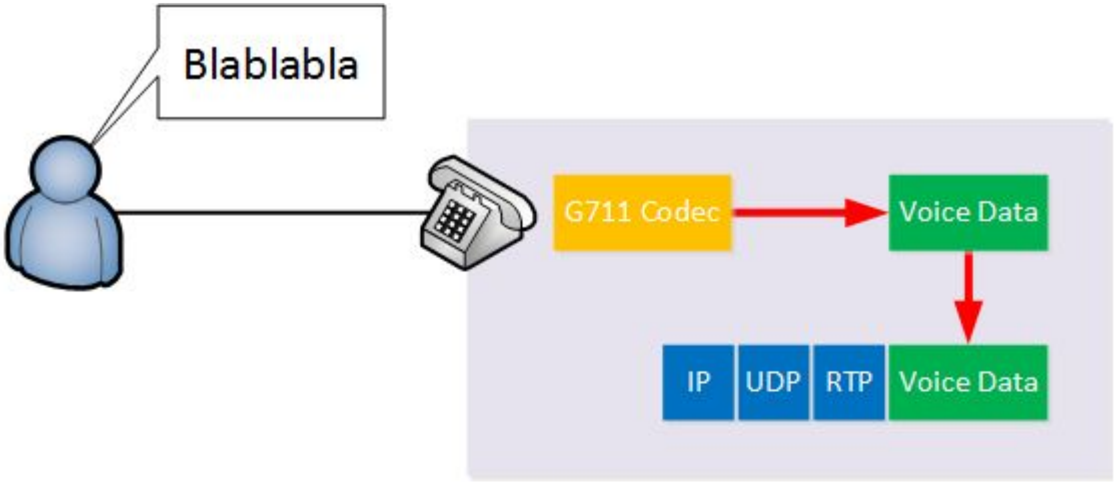
QoS: Introduction

- Quality of Service (QoS) refers to a set of technologies and techniques that help networks **prioritize important traffic**, control delay, reduce packet loss, and improve overall application performance.
- QoS ensures that critical applications get the network resources they need, even during congestion.
- Congestion can happen when network links are oversubscribed.
- Real-time applications (like VoIP) degrade significantly if packets are delayed or lost.
- Different types of traffic have different network requirements:
  - **Voice** needs low latency and low **jitter**.
  - **Video** needs high bandwidth and some tolerance for jitter.
  - **Email** or web browsing is tolerant to delays, but not to loss.

Jitter: Variation in delay

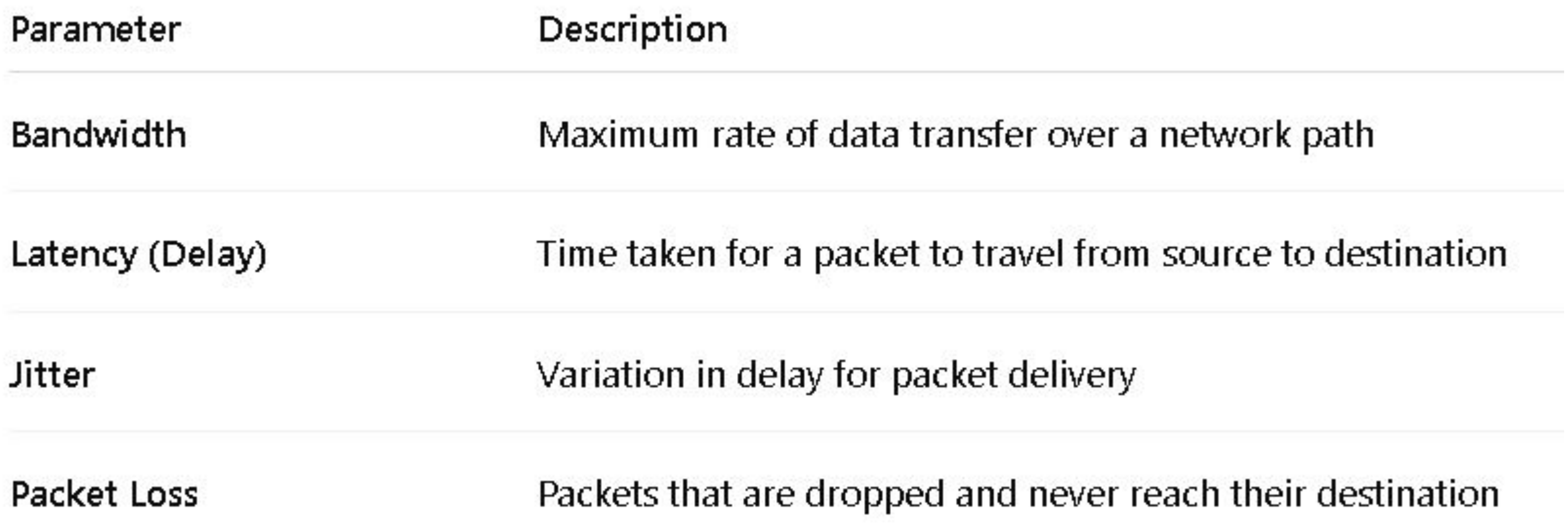
Example: Voice Data Processing

Source



- Codec processes the analog sound and converts it into a digital signal.
- The analog sound is digitized for a certain time period which is usually 20 ms.
- With the G711 codec, each 20 ms of audio is 160 bytes of data.
- The IP phone will then create a new IP packet with an UDP and RTP (Realtime Transport Protocol) headers, adds the voice data to it and forwards the IP packet to the destination.

QoS Parameters



Parameter	Description
Bandwidth	Maximum rate of data transfer over a network path
Latency (Delay)	Time taken for a packet to travel from source to destination
Jitter	Variation in delay for packet delivery
Packet Loss	Packets that are dropped and never reach their destination

QoS tries to optimize these metrics according to application needs.

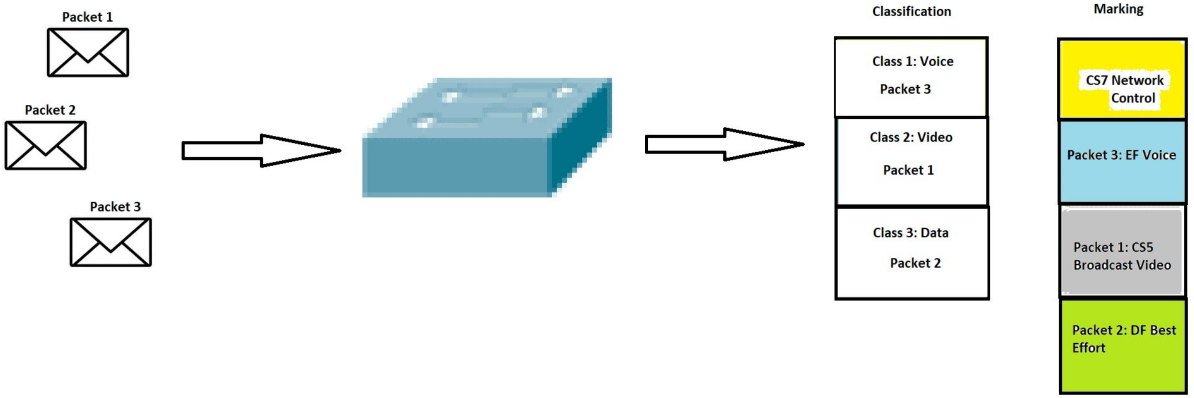
RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

QoS Tools

QoS Tools

- Some of the QoS tools are:
  A. Classification and Marking,
  B. Queuing and Scheduling,
  C. Congestion Management.
  D. Policing and Traffic Shaping

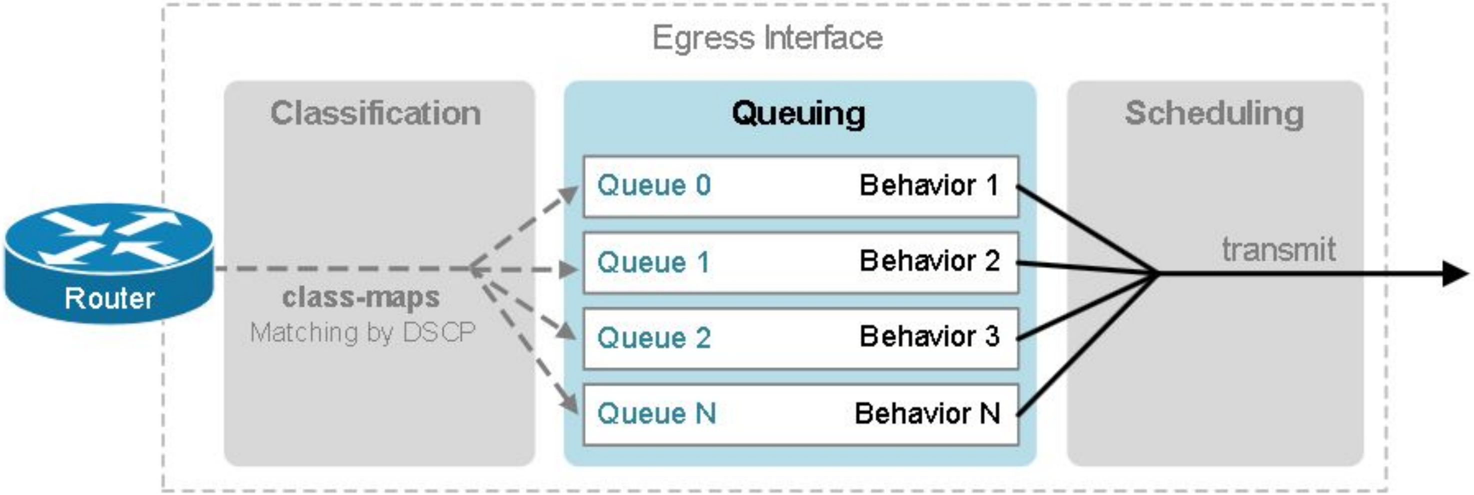
A. Classification and Marking



a) Classification and Marking

- **Classification**: Identifying and separating traffic into categories.
- **Marking**: Tagging packets based on priority levels.
- Common fields used:
  - **IP Precedence** (older)
  - **DSCP** (Differentiated Services Code Point) in IP header
  - **802.1p** tags for Ethernet frames

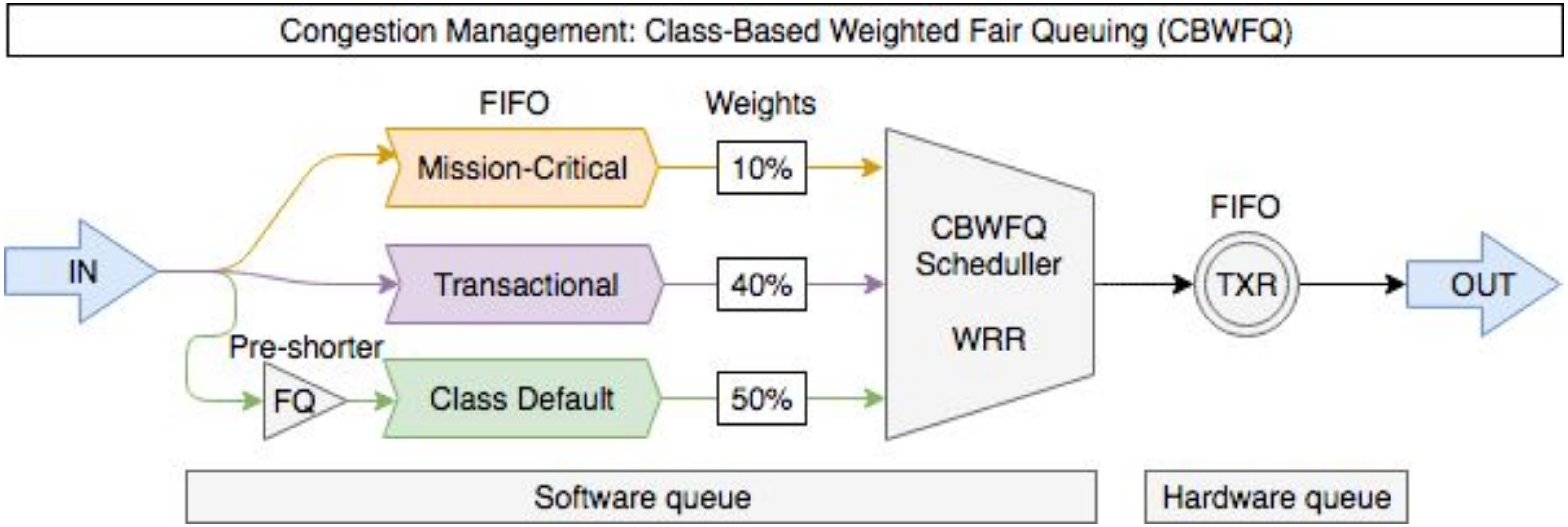
B. Queuing and Scheduling



b) Queuing and Scheduling

- Packets are placed into **queues** based on their classification.
- **Scheduling algorithms** determine the order in which packets are transmitted:
    - **First-In-First-Out (FIFO)** (default but not QoS-friendly)
    - **Priority Queuing (PQ)**: Highest priority queues first
    - **Weighted Fair Queuing (WFQ)**: Fair bandwidth division based on weights
    - **Class-Based Weighted Fair Queuing (CBWFQ)**: More flexible control

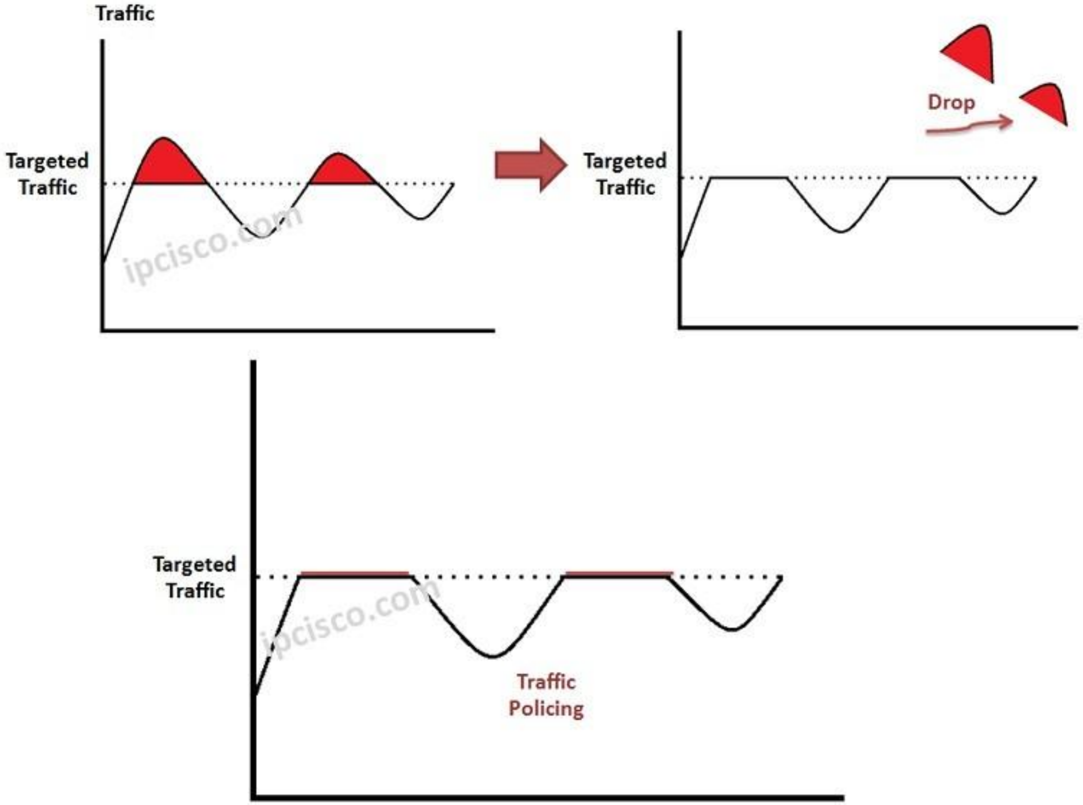
C. Congestion Management



c) Congestion Management

- Techniques to **control** or **avoid** congestion:
  - **Tail Drop**: Simply drops packets when queue is full (causes TCP global synchronization problems)
  - **Random Early Detection** (**RED**): Proactively drops packets to avoid full queues

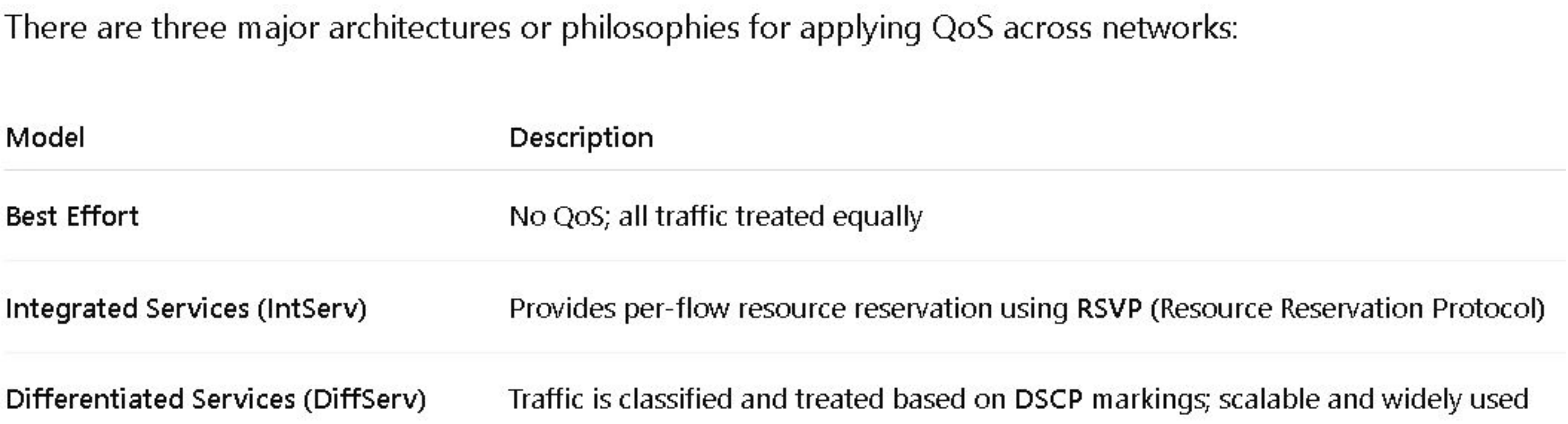
D. Policing and Traffic Shaping



d) Policing and Shaping

- **Policing**: Enforces a bandwidth limit by dropping or remarking packets exceeding the rate.
- **Shaping**: Buffers excess traffic and sends it at a controlled rate.

QoS Models



There are three major architectures or philosophies for applying QoS across networks:

Model	Description
Best Effort	No QoS; all traffic treated equally
Integrated Services (IntServ)	Provides per-flow resource reservation using **RSVP** (Resource Reservation Protocol)
Differentiated Services (DiffServ)	Traffic is classified and treated based on **DSCP** markings; scalable and widely used

DiffServ is the dominant model used in most enterprise and service provider networks.