**UNIT IV 9 hours The Transport Layer: User datagram protocol; Transmission control protocol; TCP congestion control; Internet routing protocols (RIP,OSPF).**

**The Transport Layer in the OSI (Open Systems Interconnection)** model is responsible for ensuring reliable communication between processes running on different hosts. Two of the most prominent protocols operating at this layer are the User Datagram Protocol (UDP) and the Transmission Control Protocol (TCP). Additionally, TCP encompasses congestion control mechanisms to manage network congestion effectively. At the network layer, routing protocols like Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) play vital roles in determining the optimal paths for data packets to traverse the network.

**User Datagram Protocol (UDP):**

UDP is a connectionless protocol that provides a simple and unreliable communication service between devices on a network.

It is commonly used for applications where speed and efficiency are prioritized over reliability, such as real-time multimedia streaming, online gaming, DNS (Domain Name System), and DHCP (Dynamic Host Configuration Protocol).

**Transmission Control Protocol (TCP):**

TCP is a connection-oriented protocol that offers reliable and ordered delivery of data packets between devices.

It ensures that data packets are delivered without errors, in sequence, and without duplication.

TCP includes features like flow control, error detection, and retransmission of lost packets to guarantee reliable data transmission.

Common applications that rely on TCP include web browsing, email transfer (SMTP), file transfer (FTP), and remote terminal access (SSH).

**TCP Congestion Control:**

TCP congestion control mechanisms are designed to prevent network congestion and ensure fair sharing of network resources among competing connections.

Techniques such as slow start, congestion avoidance, fast retransmit, and fast recovery are employed to dynamically adjust the transmission rate based on network conditions.

These mechanisms help TCP to maintain high throughput while avoiding network congestion and packet loss.

**Internet Routing Protocols (RIP, OSPF):**

Routing protocols are responsible for dynamically discovering and maintaining routing tables, which are used to determine the best path for forwarding packets through a network.

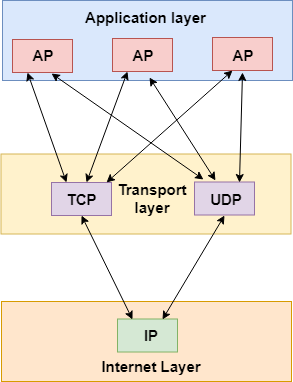
RIP (Routing Information Protocol) is a distance-vector routing protocol that uses hop count as the metric for path selection. It is suitable for small to medium-sized networks.

OSPF (Open Shortest Path First) is a link-state routing protocol that constructs a detailed topology map of the network. It calculates the shortest path to each destination based on metrics such as bandwidth and delay.

Both RIP and OSPF enable routers to exchange routing information and adapt to changes in network topology, ensuring efficient packet delivery across the network.

Transport Layer

* The transport layer is a 4th layer from the top.
* The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.
* The transport layer provides a logical communication between application processes running on different hosts. Although the application processes on different hosts are not physically connected, application processes use the logical communication provided by the transport layer to send the messages to each other.
* The transport layer protocols are implemented in the end systems but not in the network routers.
* A computer network provides more than one protocol to the network applications. For example, TCP and UDP are two transport layer protocols that provide a different set of services to the network layer.
* All transport layer protocols provide multiplexing/demultiplexing service. It also provides other services such as reliable data transfer, bandwidth guarantees, and delay guarantees.
* Each of the applications in the application layer has the ability to send a message by using TCP or UDP. The application communicates by using either of these two protocols. Both TCP and UDP will then communicate with the internet protocol in the internet layer. The applications can read and write to the transport layer. Therefore, we can say that communication is a two-way process.

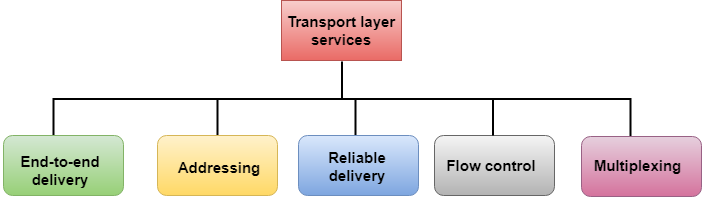


Services provided by the Transport Layer

The services provided by the transport layer are similar to those of the data link layer. The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks. The data link layer controls the physical layer while the transport layer controls all the lower layers.

**The services provided by the transport layer protocols can be divided into five categories:**

* End-to-end delivery
* Addressing
* Reliable delivery
* Flow control
* Multiplexing



End-to-end delivery:

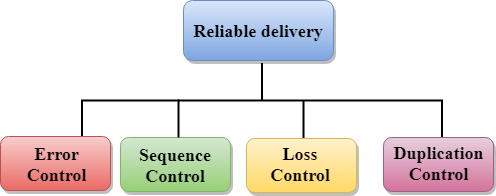
The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-end delivery of an entire message from a source to the destination.

Reliable delivery:

The transport layer provides reliability services by retransmitting the lost and damaged packets.

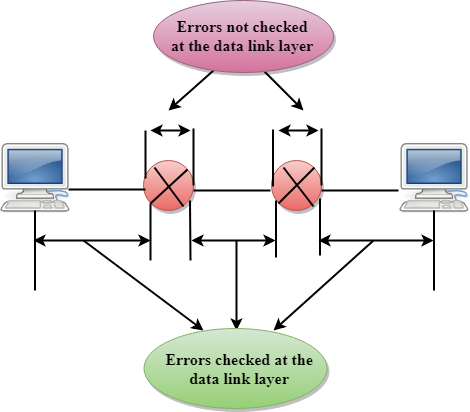
**The reliable delivery has four aspects:**

* Error control
* Sequence control
* Loss control
* Duplication control



**Error Control**

* The primary role of reliability is **Error Control**. In reality, no transmission will be 100 percent error-free delivery. Therefore, transport layer protocols are designed to provide error-free transmission.
* The data link layer also provides the error handling mechanism, but it ensures only node-to-node error-free delivery. However, node-to-node reliability does not ensure the end-to-end reliability.
* The data link layer checks for the error between each network. If an error is introduced inside one of the routers, then this error will not be caught by the data link layer. It only detects those errors that have been introduced between the beginning and end of the link. Therefore, the transport layer performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.



**Sequence Control**

* The second aspect of the reliability is sequence control which is implemented at the transport layer.
* On the sending end, the transport layer is responsible for ensuring that the packets received from the upper layers can be used by the lower layers. On the receiving end, it ensures that the various segments of a transmission can be correctly reassembled.

**Loss Control**

Loss Control is a third aspect of reliability. The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receiver?s transport layer to identify the missing segment.

**Duplication Control**

Duplication Control is the fourth aspect of reliability. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers are used to identify the lost packets; similarly, it allows the receiver to identify and discard duplicate segments.

Flow Control

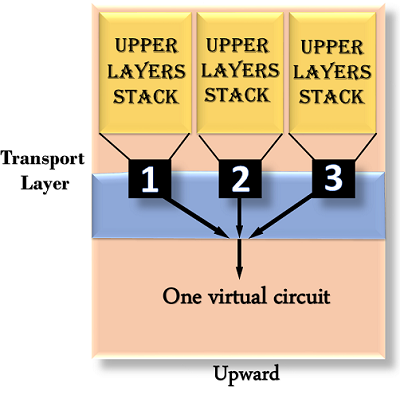
Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.

Multiplexing

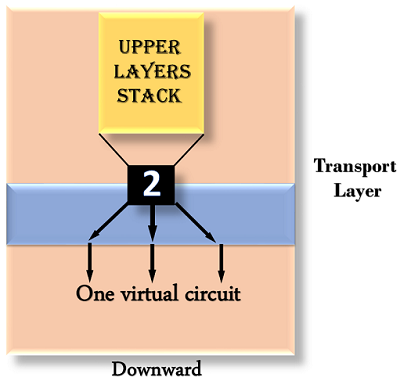
The transport layer uses the multiplexing to improve transmission efficiency.

**Multiplexing can occur in two ways:**

* **Upward multiplexing:** Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.

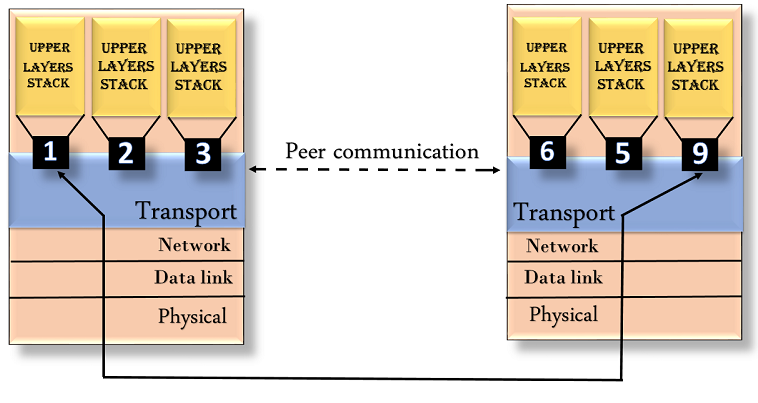


* **Downward multiplexing:** Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.



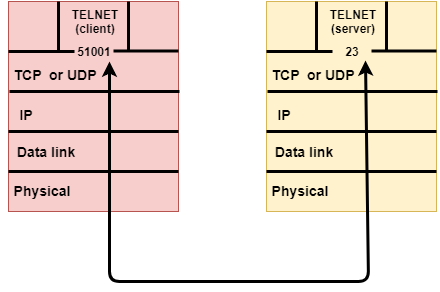
Addressing

* According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.
* The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.
* The transport layer protocols need to know which upper-layer protocols are communicating.



Transport Layer protocols

* The transport layer is represented by two protocols: TCP and UDP.
* The IP protocol in the network layer delivers a datagram from a source host to the destination host.
* Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process. When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.
* An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.
* Each port is defined by a positive integer address, and it is of 16 bits.

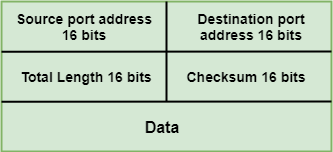


UDP

* UDP stands for **User Datagram Protocol**.
* UDP is a simple protocol and it provides nonsequenced transport functionality.
* UDP is a connectionless protocol.
* This type of protocol is used when reliability and security are less important than speed and size.
* UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
* The packet produced by the UDP protocol is known as a user datagram.

User Datagram Format

The user datagram has a 16-byte header which is shown below:



**Where,**

* **Source port address:** It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.
* **Destination port address:** It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
* **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.
* **Checksum:** The checksum is a 16-bit field which is used in error detection.

Disadvantages of UDP protocol

* UDP provides basic functions needed for the end-to-end delivery of a transmission.
* It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
* UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

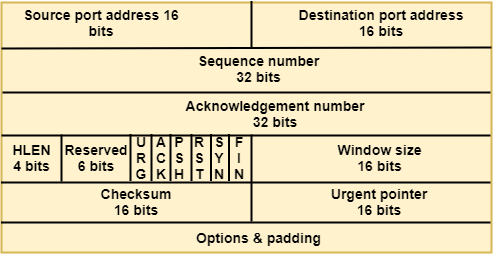
TCP

* TCP stands for Transmission Control Protocol.
* It provides full transport layer services to applications.
* It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

Features Of TCP protocol

* **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
* **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination.  
  The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.
* **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
* **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.
* **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
* **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:
  + Establish a connection between two TCPs.
  + Data is exchanged in both the directions.
  + The Connection is terminated.

TCP Segment Format



**Where,**

* **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
* **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
* **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
* **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
* **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
* **Reserved:** It is a six-bit field which is reserved for future use.
* **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

There are total six types of flags in control field:

* **URG:** The URG field indicates that the data in a segment is urgent.
* **ACK:** When ACK field is set, then it validates the acknowledgement number.
* **PSH:** The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.
* **RST:** The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers.
* **SYN:** The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation ( with the ACK bit set ), and confirmation acknowledgement.
* **FIN:** The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination confirmation.
  + **Window Size:** The window is a 16-bit field that defines the size of the window.
  + **Checksum:** The checksum is a 16-bit field used in error detection.
  + **Urgent pointer:** If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
  + **Options and padding:** It defines the optional fields that convey the additional information to the receiver.

Differences b/w TCP & UDP

|  |  |  |
| --- | --- | --- |
| **Basis for Comparison** | **TCP** | **UDP** |
| Definition | TCP establishes a virtual circuit before transmitting the data. | UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not. |
| Connection Type | It is a Connection-Oriented protocol | It is a Connectionless protocol |
| Speed | slow | high |
| Reliability | It is a reliable protocol. | It is an unreliable protocol. |
| Header size | 20 bytes | 8 bytes |
| acknowledgement | It waits for the acknowledgement of data and has the ability to resend the lost packets. | It neither takes the acknowledgement, nor it retransmits the damaged frame. |

# TCP Congestion Control

Prerequisites – [Basic Congestion control knowledge](https://www.geeksforgeeks.org/computer-networks-congestion-control/)

TCP congestion control is a method used by the TCP protocol to manage data flow over a network and prevent congestion. TCP uses a congestion window and congestion policy that avoids congestion. Previously, we assumed that only the receiver could dictate the sender’s window size. We ignored another entity here, the network. If the network cannot deliver the data as fast as it is created by the sender, it must tell the sender to slow down. In other words, in addition to the receiver, the network is a second entity that determines the size of the sender’s window

## Congestion Policy in TCP

1. **Slow Start Phase:** Starts slow increment is exponential to the threshold.
2. **Congestion Avoidance Phase:** After reaching the threshold increment is by 1.
3. **Congestion Detection Phase:** The sender goes back to the Slow start phase or the Congestion avoidance phase.

### Slow Start Phase

**Exponential increment**: In this phase after every RTT the congestion window size increments exponentially.

**Example:-** If the initial congestion window size is 1 segment, and the first segment is successfully acknowledged, the congestion window size becomes 2 segments. If the next transmission is also acknowledged, the congestion window size doubles to 4 segments. This exponential growth continues as long as all segments are successfully acknowledged.

Initially cwnd = 1

After 1 RTT, cwnd = 2^(1) = 2

2 RTT, cwnd = 2^(2) = 4

3 RTT, cwnd = 2^(3) = 8

### Congestion Avoidance Phase

**Additive increment:** This phase starts after the threshold value also denoted as ssthresh. The size of cwnd(congestion window) increases additive. After each RTT cwnd = cwnd + 1.

**Example:-** if the congestion window size is 20 segments and all 20 segments are successfully acknowledged within an RTT, the congestion window size would be increased to 21 segments in the next RTT. If all 21 segments are again successfully acknowledged, the congestion window size would be increased to 22 segments, and so on.

Initially cwnd = i

After 1 RTT, cwnd = i+1

2 RTT, cwnd = i+2

3 RTT, cwnd = i+3

### Congestion Detection Phase

**Multiplicative decrement:** If congestion occurs, the congestion window size is decreased. The only way a sender can guess that congestion has happened is the need to retransmit a segment. Retransmission is needed to recover a missing packet that is assumed to have been dropped by a router due to congestion. Retransmission can occur in one of two cases: when the RTO timer times out or when three duplicate ACKs are received.

**Case 1:** Retransmission due to Timeout – In this case, the congestion possibility is high.

(a) ssthresh is reduced to half of the current window size.

(b) set cwnd = 1

(c) start with the slow start phase again.

**Case 2:**Retransmission due to 3 Acknowledgement Duplicates – The congestion possibility is less.

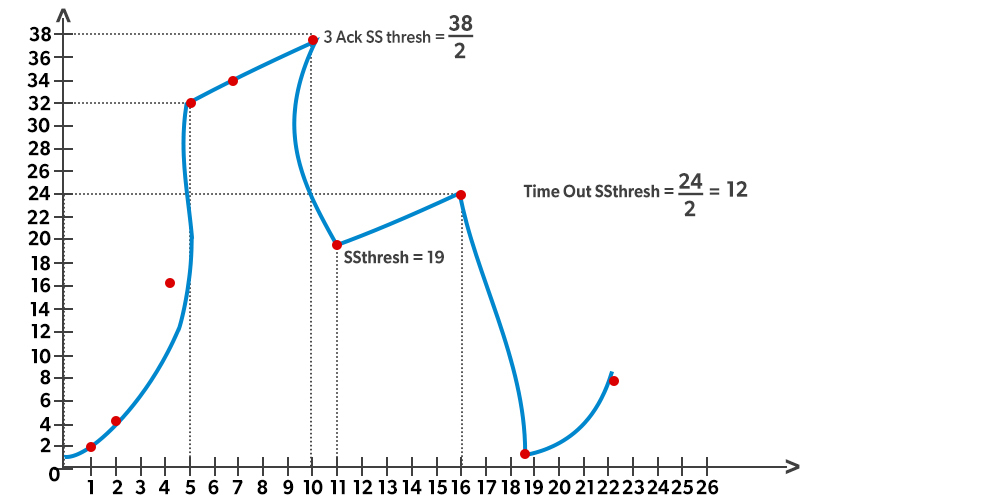
(a) ssthresh value reduces to half of the current window size.

(b) set cwnd= ssthresh

(c) start with congestion avoidance phase

#### Example

Assume a TCP protocol experiencing the behavior of slow start. At the 5th transmission round with a threshold (ssthresh) value of 32 goes into the congestion avoidance phase and continues till the 10th transmission. At the 10th transmission round, 3 duplicate ACKs are received by the receiver and entered into additive increase mode. Timeout occurs at the 16th transmission round. Plot the transmission round (time) vs congestion window size of TCP segments.



# Definition of Autonomous System (AS):

# An Autonomous System (AS) is a collection of IP networks and routers under the control of one or more network operators that presents a common, clearly defined routing policy to the internet. Autonomous Systems are a fundamental concept in the operation of the internet's global routing system. Each AS is identified by a unique Autonomous System Number (ASN), which is assigned by a regional internet registry (RIR). ASes use interior gateway protocols (IGPs) to exchange routing information internally and exterior gateway protocols (EGPs) to communicate with other ASes, enabling the global reachability of internet resources.

# Three Categories of Autonomous Systems:

# Single-Homed Autonomous System:

# A Single-Homed AS is connected to only one other AS.

# It typically represents small organizations or internet service providers (ISPs) with a single connection to an upstream provider for internet connectivity.

# Single-Homed ASes rely entirely on their connection to the upstream provider for internet access and do not have redundant links to other ASes.

# Multi-Homed Autonomous System:

# A Multi-Homed AS is connected to multiple other ASes.

# It has redundant connections to different upstream providers for internet connectivity, improving network reliability and performance.

# Multi-Homed ASes may also have peering relationships with other ASes for direct exchange of traffic, such as content delivery networks (CDNs) or large enterprises.

# Transit Autonomous System:

# A Transit AS serves as an intermediary for routing traffic between other ASes.

# It provides transit services by allowing traffic from one AS to traverse its network to reach another AS.

# Transit ASes typically have extensive network infrastructure and peering agreements with multiple other ASes, enabling them to efficiently route traffic across the internet.

# b) Explanation of RIP and OSPF:

# i) RIP (Routing Information Protocol):

# Routing Information Protocol (RIP) is one of the oldest distance vector routing protocols used in computer networks, particularly in smaller networks. Here's an explanation of its key features:

# Distance Vector Protocol: RIP operates based on the distance vector algorithm, where routers exchange routing tables with their neighboring routers at regular intervals. Each router advertises its entire routing table to its neighbors, containing information about reachable networks and associated hop counts.

# Hop Count Metric: RIP uses hop count as its metric for path selection. Each router increments the hop count when propagating routing information. Routes with lower hop counts are considered more favorable, and routers choose paths with the fewest hops to reach a destination.

# Periodic Updates: RIP routers periodically broadcast their entire routing tables to neighboring routers, even if there are no changes in the network topology. This can lead to increased network traffic and slower convergence, especially in larger networks.

# Split Horizon and Poison Reverse: RIP employs mechanisms like split horizon and poison reverse to prevent routing loops. Split horizon prevents a router from advertising routes back to the neighbor from which it learned them, while poison reverse advertises unreachable routes with infinite metric to inform neighbors about link failures.

# Limited Scalability: RIP's reliance on periodic updates and hop count as the metric limits its scalability and suitability for large networks. It may suffer from slow convergence and routing loops in complex topologies.

# ii) OSPF (Open Shortest Path First):

# Open Shortest Path First (OSPF) is a link-state routing protocol designed to overcome the limitations of distance vector protocols like RIP. Here's an explanation of its key features:

# Link-State Protocol: OSPF operates as a link-state protocol, where routers exchange information about the state of their directly connected links. Each router constructs a link-state database containing information about reachable networks and the cost (metric) associated with each link.

# Area Hierarchies: OSPF organizes networks into areas to improve scalability and reduce routing overhead. Routers within the same area share link-state information, and only summary information is exchanged between areas. This hierarchical structure helps minimize the impact of network changes on the entire OSPF domain.

# Shortest Path First (SPF) Algorithm: OSPF uses the Dijkstra algorithm to calculate the shortest path tree from each router to all destinations within the OSPF domain. This allows routers to select the most optimal paths based on link costs, resulting in efficient routing and faster convergence.

# Fast Convergence: OSPF achieves faster convergence compared to distance vector protocols by flooding link-state updates only when there are changes in network topology. Routers use the information in the link-state database to calculate new routes promptly in response to network changes.

# Scalability: OSPF is highly scalable and suitable for large and complex networks. Its hierarchical design, efficient use of link-state information, and support for route summarization contribute to its scalability and robustness in various network environments.

# RIP Protocol

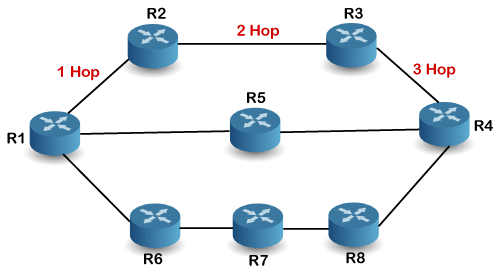
RIP stands for Routing Information Protocol. RIP is an intra-domain routing protocol used within an autonomous system. Here, intra-domain means routing the packets in a defined domain, for example, web browsing within an institutional area. To understand the RIP protocol, our main focus is to know the structure of the packet, how many fields it contains, and how these fields determine the routing table.

**Before understanding the structure of the packet, we first look at the following points:**

* RIP is based on the distance vector-based strategy, so we consider the entire structure as a graph where nodes are the routers, and the links are the networks.
* In a routing table, the first column is the destination, or we can say that it is a network address.
* The cost metric is the number of hops to reach the destination. The number of hops available in a network would be the cost. The hop count is the number of networks required to reach the destination.
* In RIP, infinity is defined as 16, which means that the RIP is useful for smaller networks or small autonomous systems. The maximum number of hops that RIP can contain is 15 hops, i.e., it should not have more than 15 hops as 16 is infinity.
* The next column contains the address of the router to which the packet is to be sent to reach the destination.

### How is hop count determined?

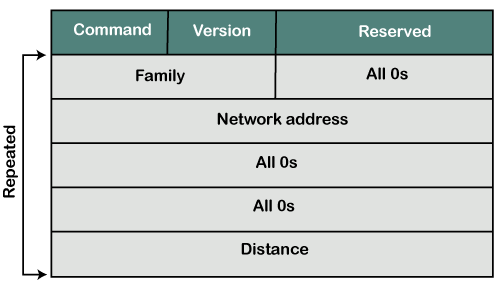
When the router sends the packet to the network segment, then it is counted as a single hop.



In the above figure, when the router 1 forwards the packet to the router 2 then it will count as 1 hop count. Similarly, when the router 2 forwards the packet to the router 3 then it will count as 2 hop count, and when the router 3 forwards the packet to router 4, it will count as 3 hop count. In the same way, [RIP](https://www.javatpoint.com/rip-full-form) can support maximum upto 15 hops, which means that the 16 routers can be configured in a RIP.

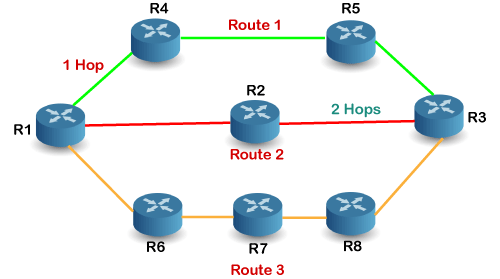
### RIP Message Format

Now, we look at the structure of the RIP message format. The message format is used to share information among different routers. The RIP contains the following fields in a message:



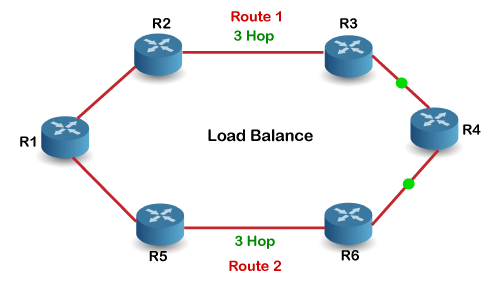
* Command: It is an 8-bit field that is used for request or reply. The value of the request is 1, and the value of the reply is 2.
* Version: Here, version means that which version of the protocol we are using. Suppose we are using the protocol of version1, then we put the 1 in this field.
* Reserved: This is a reserved field, so it is filled with zeroes.
* Family: It is a 16-bit field. As we are using the TCP/IP family, so we put 2 value in this field.
* Network Address: It is defined as 14 bytes field. If we use the IPv4 version, then we use 4 bytes, and the other 10 bytes are all zeroes.
* Distance: The distance field specifies the hop count, i.e., the number of hops used to reach the destination.

### How does the RIP work?



If there are 8 routers in a network where Router 1 wants to send the data to Router 3. If the network is configured with RIP, it will choose the route which has the least number of hops. There are three routes in the above network, i.e., Route 1, Route 2, and Route 3. The Route 2 contains the least number of hops, i.e., 2 where Route 1 contains 3 hops, and Route 3 contains 4 hops, so RIP will choose Route 2.

### Let's look at another example.

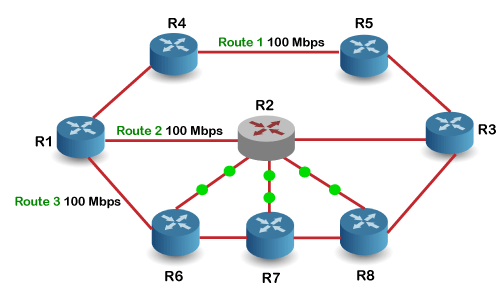


Suppose R1 wants to send the data to R4. There are two possible routes to send data from r1 to r2. As both the routes contain the same number of hops, i.e., 3, so RIP will send the data to both the routes simultaneously. This way, it manages the load balancing, and data reach the destination a bit faster.

### Disadvantages of RIP

**The following are the disadvantages of RIP:**

* In RIP, the route is chosen based on the hop count metric. If another route of better bandwidth is available, then that route would not be chosen. Let's understand this scenario through an example.



We can observe that Route 2 is chosen in the above figure as it has the least hop count. The Route 1 is free and data can be reached more faster; instead of this, data is sent to the Route 2 that makes the Route 2 slower due to the heavy traffic. This is one of the biggest disadvantages of RIP.

* The RIP is a classful routing protocol, so it does not support the VLSM (Variable Length Subnet Mask). The classful routing protocol is a protocol that does not include the subnet mask information in the routing updates.
* It broadcasts the routing updates to the entire network that creates a lot of traffic. In RIP, the routing table updates every 30 seconds. Whenever the updates occur, it sends the copy of the update to all the neighbors except the one that has caused the update. The sending of updates to all the neighbors creates a lot of traffic. This rule is known as a split-horizon rule.
* It faces a problem of Slow convergence. Whenever the router or link fails, then it often takes minutes to stabilize or take an alternative route; This problem is known as Slow convergence.
* RIP supports maximum 15 hops which means that the maximum 16 hops can be configured in a RIP
* The Administrative distance value is 120 (Ad value). If the Ad value is less, then the protocol is more reliable than the protocol with more Ad value.
* The RIP protocol has the highest Ad value, so it is not as reliable as the other routing protocols.

### How RIP updates its Routing table

The following timers are used to update the routing table:

* **RIP update timer : 30 sec**

The routers configured with RIP send their updates to all the neighboring routers every 30 seconds.

* **RIP Invalid timer : 180 sec**

The RIP invalid timer is 180 seconds, which means that if the router is disconnected from the network or some link goes down, then the neighbor router will wait for 180 seconds to take the update. If it does not receive the update within 180 seconds, then it will mark the particular route as not reachable.

* **RIP Flush timer : 240 sec**

The RIP flush timer is 240 second which is almost equal to 4 min means that if the router does not receive the update within 240 seconds then the neighbor route will remove that particular route from the routing table which is a very slow process as 4 minutes is a long time to wait.

### Advantages of RIP

**The following are the advantages of a RIP protocol:**

* It is easy to configure
* It has less complexity
* The CPU utilization is less.

**Significance of TCP Segment Fields:**

**i) Sequence Number:** The sequence number field in the TCP segment is crucial for maintaining the order of data transmission and ensuring reliable communication between the sender and the receiver.

Ordering: Each byte of data sent over a TCP connection is assigned a sequence number. These sequence numbers are used by the receiver to rearrange the segments in the correct order upon arrival. This ensures that the data is reconstructed in the same order as it was sent by the sender.

Detecting Loss and Duplication: Sequence numbers also allow the receiver to detect any lost or duplicated segments. By comparing the received sequence numbers with the expected sequence numbers, the receiver can identify missing segments or duplicates and request retransmissions if necessary.

Flow Control: Sequence numbers play a role in flow control mechanisms. They help the receiver indicate to the sender how much data it can accept by acknowledging segments up to a certain sequence number. This helps in preventing overwhelming the receiver with data it cannot process.

**ii) Acknowledgment Number:** The acknowledgment number field in the TCP segment is used by the receiver to inform the sender about the next sequence number it expects to receive.

Acknowledgment: When the receiver receives data segments successfully, it sends back an acknowledgment (ACK) containing the acknowledgment number indicating the next expected sequence number. This confirms to the sender that the data has been received successfully up to that point.

Acknowledgment for Cumulative Data: TCP uses cumulative acknowledgments, meaning that the acknowledgment number acknowledges receipt of all bytes up to, but not including, the indicated sequence number. This allows for efficient acknowledgment of data segments without needing to acknowledge each individual byte.

**Flow Control:** Similar to the sequence number, the acknowledgment number also plays a role in flow control. By indicating the next expected sequence number, the receiver effectively communicates to the sender the available buffer space for receiving more data.

iii) Window Size: The window size field in the TCP segment represents the size of the receive window, which is the amount of data, in bytes, that the sender can transmit before receiving an acknowledgment from the receiver.

Flow Control: The window size is essential for flow control, as it allows the sender to regulate the rate at which it sends data to match the receiver's ability to process it. A larger window size indicates that the receiver has more buffer space available for receiving data, allowing the sender to transmit more data without waiting for acknowledgments.

Dynamic Adjustment: TCP dynamically adjusts the window size during the connection to optimize throughput and prevent congestion. If the receiver's buffer space becomes limited, it can advertise a smaller window size to throttle the sender's transmission rate and avoid overwhelming the receiver.

Congestion Avoidance: By controlling the window size, TCP helps in congestion avoidance by ensuring that the sender does not flood the network with more data than the receiver or the network can handle. This helps maintain network stability and efficiency.