INTERNETWORKING

Internetworking is combined of 2 words, inter and networking which implies an association between totally different nodes or segments. This connection area unit is established through intercessor devices akin to routers or gateway. The first term for associate degree internetwork was catenet. This interconnection is often among or between public, private, commercial, industrial, or governmental networks. Thus, associate degree internetwork could be an assortment of individual networks, connected by intermediate networking devices, that function as one giant network. Internetworking refers to the trade, products, and procedures that meet the challenge of making and administering internet works.

To enable communication, every individual network node or phase is designed with a similar protocol or communication logic, that is Transfer Control Protocol (TCP) or Internet Protocol (IP). Once a network communicates with another network having constant communication procedures, it's called Internetworking. Internetworking was designed to resolve the matter of delivering a packet of information through many links.

There is a minute difference between extending the network and Internetworking. Merely exploitation of either a switch or a hub to attach 2 local area networks is an extension of LAN whereas connecting them via the router is an associate degree example of Internetworking. Internetworking is enforced in Layer three (Network Layer) of the OSI-ISO model. The foremost notable example of internetworking is the Internet.

There is chiefly 3 units of Internetworking:

1. Extranet
2. Intranet
3. Internet

Intranets and extranets might or might not have connections to the net. If there is a connection to the net, the computer network or extranet area unit is usually shielded from being accessed from the net if it is not authorized. The net isn't thought-about to be a section of the computer network or extranet, though it should function as a portal for access to parts of the associate degree extranet.

1. **Extranet –** It's a network of the internetwork that's restricted in scope to one organization or entity however that additionally has restricted connections to the networks of one or a lot of different sometimes, however not essential. It's the very lowest level of Internetworking, usually enforced in an exceedingly personal area. Associate degree extranet may additionally be classified as a Man, WAN, or different form of network however it cannot encompass one local area network i.e. it should have a minimum of one reference to associate degree external network.
2. **Intranet –** This associate degree computer network could be a set of interconnected networks, which exploits the Internet Protocol and uses IP-based tools akin to web browsers and FTP tools, that are underneath the management of one body entity. That body entity closes the computer network to the remainder of the planet and permits solely specific users. Most typically, this network is the internal network of a corporation or

different enterprise. An outsized computer network can usually have its own internet server to supply users with browsable data.

3. **Internet –** A selected Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and personal networks based mostly upon the Advanced analysis comes Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense additionally home to the World Wide Web (WWW) and cited as the 'Internet' to differentiate from all different generic Internetworks. Participants within the web, or their service suppliers, use IP Addresses obtained from address registries that manage assignments.

Internetworking has evolved as an answer to a few key problems: isolated LANs, duplication of resources, and an absence of network management. Isolated LANs created transmission problems between totally different offices or departments. Duplication of resources meant that constant hardware and code had to be provided to every workplace or department, as did a separate support employee. This lack of network management meant that no centralized methodology of managing and troubleshooting networks existed.

One more form of the interconnection of networks usually happens among enterprises at the Link Layer of the networking model, i.e. at the hardware-centric layer below the amount of the TCP/IP logical interfaces. Such interconnection is accomplished through network bridges and network switches. This can be typically incorrectly termed internetworking, however, the ensuing system is just a bigger, single subnetwork, and no internetworking protocol, akin to web Protocol, is needed to traverse these devices.

However, one electronic network is also reborn into associate degree internetwork by dividing the network into phases and logically dividing the segment traffic with routers. The Internet Protocol is meant to supply an associate degree unreliable packet service across the network. The design avoids intermediate network components maintaining any state of the network. Instead, this task is allotted to the endpoints of every communication session. To transfer information correctly, applications should utilize associate degree applicable Transport Layer protocol, akin to Transmission management Protocol (TCP), that provides a reliable stream. Some applications use a less complicated, connection-less transport protocol, User Datagram Protocol (UDP), for tasks that don't need reliable delivery of information or that need period of time service, akin to video streaming or voice chat.

Internetwork Addressing –

Internetwork addresses establish devices severally or as members of a bunch. Addressing schemes differ based on the protocol family and therefore the OSI layer. Three kinds of internetwork addresses area units are ordinarily used: data-link layer addresses, Media Access control (MAC) addresses, and network-layer addresses.

1. **Data Link Layer addresses:** A data-link layer address unambiguously identifies every physical network association of a network device. Data-link addresses typically area units

cited as physical or hardware addresses. Data-link addresses sometimes exist among a flat address area and have a pre-established and usually fastened relationship to a selected device. End systems usually have just one physical network association, and therefore have just one data-link address. Routers and different internetworking devices usually have multiple physical network connections and so eventually have multiple data-link addresses.

2. **MAC Addresses:** Media Access management (MAC) addresses encompass a set of data-link layer addresses. MAC addresses establish network entities in LANs that implement the IEEE MAC addresses of the data-link layer. MAC addresses different area units distinctively for every local area network interface. MAC addresses are forty-eight bits long and are expressed in form of twelve hexadecimal digits. The primary half dozen hexadecimal digits, which are usually administered by the IEEE, establish the manufacturer or merchant and therefore comprise the Organizational Unique Identifier (OUI). The last half dozen positional notation digits comprise the interface serial variety or another price administered by the particular merchant. MAC addresses are typically area units referred to as burned-in addresses (BIAs) as a result of being burned into read-only memory(ROM) and are traced into random-access memory (RAM) once the interface card initializes.
3. **Network-Layer Addresses:** Network addresses sometimes exist among a gradable address area and typically area units referred to as virtual or logical addresses. the connection between a network address and a tool is logical and unfixed, it usually relies either on physical network characteristics or on groupings that don't have any physical basis. finish systems need one network-layer address for every network-layer protocol they support. Routers and different Internetworking devices need one network-layer address per physical network association for every network-layer protocol supported.

Challenges to Internetworking –

Implementing useful internetwork isn't at any certainty. There are several challenging fields, particularly in the areas of dependableness, connectivity, network management, and adaptability, and each and every space is essential in establishing associate degree economical and effective internetwork. A few of them are:-

- The initial challenge lies when we are trying to connect numerous systems to support communication between disparate technologies. For example, Totally different sites might use different kinds of media, or they could operate at variable speeds.
- Another essential thought is reliable service that should be maintained in an internetwork. Individual users and whole organizations depend upon consistent, reliable access to network resources.
- Network management should give centralized support associate degree troubleshooting capabilities on the internetwork. Configuration, security, performance, and different problems should be adequately addressed for the internetwork to perform swimmingly.
- Flexibility, the ultimate concern, is important for network enlargement and new applications and services, among different factors.

Advantages:

Increased connectivity: Internetworking enables devices on different networks to communicate with each other, which increases connectivity and enables new applications and services.
Resource sharing: Internetworking allows devices to share resources across networks, such as printers, servers, and storage devices. This can reduce costs and improve efficiency by allowing multiple devices to share resources.
Improved scalability: Internetworking allows networks to be expanded and scaled as needed to accommodate growing numbers of devices and users.
Improved collaboration: Internetworking enables teams and individuals to collaborate and work together more effectively, regardless of their physical location.
Access to remote resources: Internetworking allows users to access resources and services that are physically located on remote networks, improving accessibility and flexibility.
Disadvantages:
Security risks: Internetworking can create security vulnerabilities and increase the risk of cyberattacks and data breaches. Connecting multiple networks together increases the number of entry points for attackers, making it more difficult to secure the entire system.
Complexity: Internetworking can be complex and requires specialized knowledge and expertise to set up and maintain. This can increase costs and create additional maintenance overhead.
Performance issues: Internetworking can lead to performance issues, particularly if networks are not properly optimized and configured. This can result in slow response times and poor network performance.
Compatibility issues: Internetworking can lead to compatibility issues, particularly if different networks are using different protocols or technologies. This can make it difficult to integrate different systems and may require additional resources to resolve.
Management overhead: Internetworking can create additional management overhead, particularly if multiple networks are involved. This can increase costs and require additional resources to manage effectively.

QUALITY OF SERVICE(QoS)

Quality of service (QoS) is the use of mechanisms or technologies that work on a network to control traffic and ensure the performance of critical applications with limited network capacity. It enables organizations to adjust their overall **network traffic** by prioritizing specific high-performance applications.

QoS is typically applied to networks that carry traffic for resource-intensive systems. Common services for which it is required include internet protocol television (IPTV), online gaming, streaming media, videoconferencing, video on demand (VOD), and Voice over IP (VoIP).

Using QoS in networking, organizations have the ability to optimize the performance of multiple applications on their network and gain visibility into the bit rate, delay, jitter, and packet rate of their network. This ensures they can engineer the traffic on their network and change the way that packets are routed to the internet or other networks to avoid transmission delay. This also ensures that the

organization achieves the expected service quality for applications and delivers expected user experiences.

As per the QoS meaning, the key goal is to enable networks and organizations to prioritize traffic, which includes offering dedicated bandwidth, controlled jitter, and lower **latency**. The technologies used to ensure this are vital to enhancing the performance of business applications, **wide-area networks (WANs)**, and service provider networks.

e packet loss, latency and jitter on a network.

Advantages of QoS

The deployment of QoS is crucial for businesses that want to ensure the availability of their business-critical applications. It is vital for delivering differentiated bandwidth and ensuring data transmission takes place without interrupting traffic flow or causing packet losses. Major advantages of deploying QoS include:

Unlimited application prioritization: QoS guarantees that businesses' most mission-critical applications will always have priority and the necessary resources to achieve high performance.

Better resource management: QoS enables administrators to better manage the organization's internet resources. This also reduces costs and the need for investments in link expansions.

Enhanced user experience: The end goal of QoS is to guarantee the high performance of critical applications, which boils down to delivering optimal user experience. Employees enjoy high performance on their high-bandwidth applications, which enables them to be more effective and get their job done more quickly.

Point-to-point traffic management: Managing a network is vital however traffic is delivered, be it end to end, node to node, or point to point. The latter enables organizations to deliver customer packets in order from one point to the next over the internet without suffering any packet loss.

Packet loss prevention: Packet loss can occur when packets of data are dropped in transit between networks. This can often be caused by a failure or inefficiency, network congestion, a faulty router, loose connection, or poor signal. QoS avoids the potential of packet loss by prioritizing bandwidth of high-performance applications.

Latency reduction: Latency is the time it takes for a network request to go from the sender to the receiver and for the receiver to process it. This is typically affected by routers taking longer to analyze information and storage delays caused by intermediate switches and bridges. QoS

enables organizations to reduce latency, or speed up the process of a network request, by prioritizing their critical application.

CONGESTION ALGORITHM

Congestion algorithms are used to manage network congestion by controlling the amount of data sent into the network. A congestion algorithm is a set of rules, processes, and techniques used to manage and control network congestion, ensuring efficient and reliable data transmission. The primary purpose of congestion algorithms is to prevent or mitigate network congestion, which occurs when the network capacity is exceeded by the volume of incoming traffic.

Key Functions:

Congestion algorithms perform the following key functions:

1. Network Monitoring: Continuously monitor network traffic and performance metrics.

2. Congestion Detection: Detect congestion based on predefined thresholds or metrics.

3. Traffic Control: Implement traffic control mechanisms, such as rate limiting, packet dropping, or queuing.

4. Resource Allocation: Allocate network resources, such as bandwidth or buffer space, to manage congestion.

5. Feedback Mechanisms: Provide feedback to senders or receivers to adjust their transmission rates or behavior.

Types of Congestion Algorithms:

1. Open-Loop Congestion Control: Prevents congestion by controlling the amount of data sent into the network.

2. Closed-Loop Congestion Control: Detects congestion and adjusts the transmission rate accordingly.

Congestion Algorithms:

1. TCP Tahoe: A simple, open-loop congestion control algorithm.

2. TCP Reno: A closed-loop congestion control algorithm that detects congestion and adjusts the transmission rate.

3. TCP Vegas: A closed-loop congestion control algorithm that detects congestion by measuring the delay.

4. TCP NewReno: An improved version of TCP Reno that handles multiple packet losses.

5. BIC (Binary Increase Control): A closed-loop congestion control algorithm that adjusts the transmission rate based on the network congestion level.

6. CUBIC (CUBIC TCP): A closed-loop congestion control algorithm that adjusts the transmission rate based on the network congestion level.

7. DCTCP (Data Center TCP): A closed-loop congestion control algorithm designed for data center networks.

Congestion Algorithm Metrics:

1. Throughput: Measures the amount of data transmitted per unit time.

2. Delay: Measures the time taken for data to travel from sender to receiver.

3. Packet Loss: Measures the number of packets lost during transmission.

4. Jitter: Measures the variation in packet delay.

5. Network Utilization: Measures the percentage of network resources used.

Congestion Algorithm Challenges

1. Scalability: Managing congestion in large-scale networks.

2. Fairness: Ensuring fair allocation of network resources.

3. Responsiveness: Responding quickly to changes in network congestion.

4. Network Heterogeneity: Managing congestion in networks with diverse characteristics.

Real-World Applications

1. Internet Service Providers (ISPs): Managing congestion in ISP networks.

2. Data Centers: Managing congestion in data center networks.

3. Cloud Computing: Managing congestion in cloud computing environments.

4. Online Gaming: Managing congestion in online gaming applications.

Congestion Algorithm Optimization Techniques

1. Active Queue Management (AQM): Proactively manages packet queues to prevent congestion.

2. Explicit Congestion Notification (ECN): Explicitly notifies senders of congestion.

3. Rate Limiting: Limits the transmission rate to prevent congestion.

4. Traffic Shaping: Shapes traffic to prevent congestion.

5. Packet Scheduling: Schedules packets to prevent congestion.

Congestion Algorithm Implementation

1. Network Devices: Implement congestion algorithms on network devices such as routers and switches.

2. Operating Systems: Implement congestion algorithms in operating systems to manage network traffic.

3. Applications: Implement congestion algorithms in applications to manage network traffic.

ROUTING ALGORITHM

Routing algorithms are used to determine the best path for forwarding packets between nodes in a computer network. Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Types of Routing Algorithms:

1**. Static Routing**: Routing decisions are made based on preconfigured routing tables.

2. **Dynamic Routing**: Routing decisions are made based on real-time network conditions.
3**. Adaptive Routing**: Routing decisions are made based on network conditions and traffic patterns.

Routing Algorithm Techniques:

1. Shortest Path Routing: Finds the shortest path between source and destination.
2. Minimum Hop Routing: Finds the path with the minimum number of hops.
3. Maximum Flow Routing: Finds the path that maximizes the flow of traffic.
4. Minimum Delay Routing: Finds the path with the minimum delay.

Routing Algorithm Protocols:

1. RIP (Routing Information Protocol): A distance-vector routing protocol.
2. OSPF (Open Shortest Path First): A link-state routing protocol.
3. BGP (Border Gateway Protocol): A path-vector routing protocol.
4. EIGRP (Enhanced Interior Gateway Routing Protocol): A hybrid routing protocol.

Routing Algorithm Applications:

1. Internet Routing: Routing packets across the internet.
2. Intranet Routing: Routing packets within an organization's network.
3. Wireless Networking: Routing packets in wireless networks.
4. Network Virtualization: Routing packets in virtualized networks.

Routing Algorithm Challenges:

1. Scalability: Managing routing tables in large-scale networks.
2. Convergence: Ensuring routing protocols converge quickly.
3. Security: Protecting routing protocols from security threats.
4. Network Dynamics: Adapting to changes in network topology and traffic.

Routing Algorithm Optimization Techniques:

1. Route Optimization: Optimizing routes to reduce latency and improve throughput.
2. Traffic Engineering: Optimizing traffic flow to reduce congestion.
3. Quality of Service (QoS): Ensuring guaranteed performance for critical applications.
4. Network Planning: Planning network topology and capacity to meet future demands.

Types of Routing Algorithms

1. Static Routing: Routing decisions are made based on preconfigured routing tables. Static routing is simple and easy to implement, but it's not suitable for large-scale networks or networks with frequent topology changes.

2. Dynamic Routing: Routing decisions are made based on real-time network conditions. Dynamic routing is more flexible and adaptable than static routing, but it's also more complex and requires more computational resources.
3. Adaptive Routing: Routing decisions are made based on network conditions and traffic patterns. Adaptive routing is a type of dynamic routing that can adjust to changes in network conditions and traffic patterns.

Routing Algorithm Metrics

1. Hop Count: The number of nodes a packet passes through. A lower hop count indicates a shorter path.
2. Delay: The time taken for a packet to travel from source to destination. A lower delay indicates a faster path.
3. Throughput: The amount of data transmitted per unit time. A higher throughput indicates a faster path.
4. Packet Loss: The number of packets lost during transmission. A lower packet loss indicates a more reliable path.
5. Jitter: The variation in packet delay. A lower jitter indicates a more consistent path.

Algorithm Techniques

1**. Shortest Path Routing**: Finds the shortest path between source and destination. Shortest path routing is simple and efficient, but it may not always find the optimal path.
2**. Minimum Hop Routing**: Finds the path with the minimum number of hops. Minimum hop routing is simple and efficient, but it may not always find the optimal path.
3. **Maximum Flow Routing**: Finds the path that maximizes the flow of traffic. Maximum flow routing is more complex and requires more computational resources, but it can find the optimal path.
4. **Minimum Delay Routing**: Finds the path with the minimum delay. Minimum delay routing is more complex and requires more computational resources, but it can find the optimal path.

Routing Algorithm Protocols

1. **RIP (Routing Information Protocol**): A distance-vector routing protocol that uses hop count as the routing metric. RIP is simple and easy to implement, but it's not suitable for large-scale networks.
2. **OSPF (Open Shortest Path First**): A link-state routing protocol that uses shortest path as the routing metric. OSPF is more complex and requires more computational resources, but it's suitable for large-scale networks.
3. **BGP (Border Gateway Protocol**): A path-vector routing protocol that uses maximum flow as the routing metric. BGP is more complex and requires more computational resources, but it's suitable for large-scale networks.
4**. EIGRP (Enhanced Interior Gateway Routing Protocol**): A hybrid routing protocol that uses a combination of distance-vector and link-state routing. EIGRP is more complex and requires more computational resources, but it's suitable for large-scale networks.

Routing Algorithm Applications

1. **Internet Routing**: Routing packets across the internet. Internet routing requires scalable and efficient routing algorithms that can handle large amounts of traffic.
2. **Intranet Routing**: Routing packets within an organization's network. Intranet routing requires secure and efficient routing algorithms that can handle sensitive data.
3. **Wireless Networking**: Routing packets in wireless networks. Wireless networking requires routing algorithms that can handle mobility and interference.
4. **Network Virtualization**: Routing packets in virtualized networks. Network virtualization requires routing algorithms that can handle virtual machines and virtual networks.

Routing Algorithm Challenges

1. Scalability: Managing routing tables in large-scale networks. Scalability requires efficient routing algorithms that can handle large amounts of traffic.
2. Convergence: Ensuring routing protocols converge quickly. Convergence requires efficient routing algorithms that can handle topology changes.
3. Security: Protecting routing protocols from security threats. Security requires secure routing algorithms that can handle sensitive data.
4. Network Dynamics: Adapting to changes in network topology and traffic. Network dynamics require adaptive routing algorithms that can handle mobility and interference.

Routing Algorithm Optimization Techniques

1. Route Optimization: Optimizing routes to reduce latency and improve throughput. Route optimization requires efficient routing algorithms that can handle large amounts of traffic.
2. Traffic Engineering: Optimizing traffic flow to reduce congestion. Traffic engineering requires efficient routing algorithms that can handle large amounts of traffic.
3. Quality of Service (QoS): Ensuring guaranteed performance for critical applications. QoS requires efficient routing algorithms that can handle sensitive data.
4. Network Planning: Planning network topology and capacity to meet future demands. Network planning requires efficient routing algorithms that can handle large amounts of traffic.