UNIT III

THE NETWORK LAYER

Border Gateway Protocol - BGP

BGP, or Border Gateway Protocol, is the routing protocol that connects networks on the internet, enabling data packets to find the most efficient path between them. It is an exterior gateway protocol used to exchange routing and reachability information between autonomous systems (AS), which are large networks like those managed by internet service providers (ISPs). BGP determines the best route for data by considering various path attributes, and its primary function is to make the large-scale routing of the internet possible.

- **Function:** BGP's main purpose is to exchange routing information to find the best path for data traveling across different networks on the internet.
- **Autonomous Systems (AS):** The internet is made up of many ASs, and BGP is the protocol used to manage routing between them.
- **Route selection:** Unlike some other protocols that simply find the shortest path, BGP is designed for the scale of the internet and can be configured to use more complex policies to choose the best route.
- **Connection:** BGP routers establish TCP connections over port 179 to communicate with each other and exchange routing data.
- **Internal vs. External:** BGP can be used for routing within an AS (iBGP) or between different ASs (eBGP).

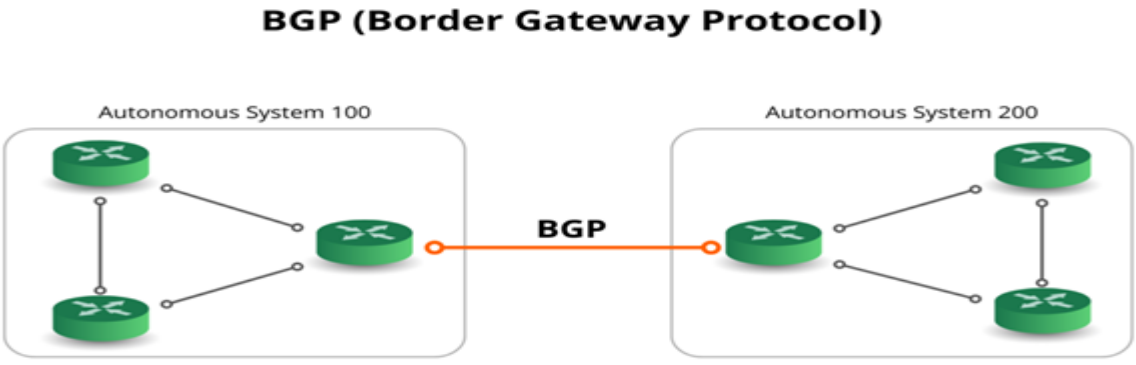
BGP's primary application in global internet routing is to exchange reachability information between different networks (Autonomous Systems, or AS) to determine the best paths for data to travel. Its key applications include connecting Internet Service Providers (ISPs) for public internet access, enabling multihomed organizations to ensure redundancy, and allowing Content Delivery Networks (CDNs) to optimize content delivery globally. It also supports complex use cases like traffic engineering, disaster recovery, and large-scale data center networking.

Core applications

- **Interconnecting ISPs**: BGP allows different ISPs to exchange routing information, which is the foundation for global internet connectivity, enabling users on one network to access resources on another.
- **Multihoming**: Organizations with multiple connections to different ISPs use BGP to manage their own internet traffic for high availability and load balancing. This ensures their network remains accessible even if one ISP connection fails.
- **Content Delivery Networks (CDNs)**: CDNs use BGP to efficiently distribute content to users by directing them to the nearest and fastest server location, optimizing performance and reducing latency.

Advanced applications

- **Traffic engineering**: Networks use BGP policies to influence traffic flow. This allows them to prioritize certain paths, avoid congested links, and manage costs by selecting specific routes through different ISPs or network links.
- **Disaster recovery**: By having multiple BGP-enabled connections, organizations can automatically reroute traffic away from an outage or a failing network, ensuring service continuity.
- **Large-scale data centers**: Within large data centers and cloud environments, BGP is used to manage complex, dynamic routing between servers and different network segments.
- **Security**: BGP helps in mitigating certain security threats, such as network-layer Distributed Denial of Service (DDoS) attacks, by filtering routes and controlling the flow of traffic.



OSPF in ISPs

OSPF

OSPF stands for **Open Shortest Path First**, a dynamic interior gateway protocol (IGP) used by routers to exchange routing information within an autonomous system (AS). It uses a link-state algorithm to create a map of the network topology, which allows each router to calculate the best path to all destinations using the Shortest Path First (SPF) algorithm. OSPF is known for its scalability and efficiency, especially in large networks, because it only sends updates when a change occurs, unlike protocols that send periodic updates.

How OSPF works

- **Link-state database:** Each router in an OSPF area maintains an identical link-state database, a complete map of the area's topology.
- **Link-state advertisements (LSAs):** Routers generate LSAs, which contain information about their neighbors and path costs, and flood them throughout the area.
- **Shortest Path First (SPF) algorithm:** Based on the link-state database, each router runs the SPF algorithm to calculate the shortest path to every other network in the area, with itself as the root of the tree.
- **Routing table population:** The calculated shortest paths are used to populate the router's IP routing table.

Key features

- **Dynamic:** Routers automatically learn about changes in the network, such as a link going down, and adjust their routing tables accordingly.
- **Efficient:** It only sends updates when a network change occurs, rather than at regular intervals, which conserves bandwidth.
- **Scalable:** OSPF is well-suited for large, complex networks by using a hierarchical design with OSPF areas.
- **Metric-based:** The cost, or metric, for calculating the best path is primarily based on bandwidth, though this can be overridden with manual configuration.

OSPF in ISPs

OSPF is used by Internet Service Providers (ISPs) as an **Interior Gateway Protocol (IGP)** for routing traffic within their own network (Autonomous System or AS). It is used alongside the exterior gateway protocol, BGP, which handles routing between different ISPs. OSPF is chosen for its scalability, fast convergence, and ability to divide large networks into hierarchical areas to manage routing complexity.

How OSPF works in an ISP network

- **Within the AS:** OSPF operates inside the ISP's network, which is a single AS. Routers use OSPF to discover each other, build a map of the network topology, and calculate the fastest path to every destination.
- **Link-state:** OSPF is a link-state protocol, meaning each router maintains a complete picture of the network. They do this by exchanging "link state advertisements" (LSAs) with other routers.
- **Dijkstra's algorithm:** Each router uses the link-state database to run Dijkstra's algorithm to calculate the shortest path to all other routers based on a "cost" metric, which can be based on factors like bandwidth or round-trip time.
- **Hierarchical areas:** To manage complexity, ISPs divide their large networks into areas. Area 0 is the "backbone" area, and all other areas must connect to it, either directly or indirectly. This limits the amount of routing information that each router needs to process.
- **Fast convergence:** When a link fails, OSPF routers quickly detect the change, flood the new topology information, and recalculate new paths, often within seconds.
- **BGP integration:** Outside of the ISP's network, BGP takes over for inter-domain routing. The ISP's OSPF network is connected to other networks via BGP.

Why ISPs use OSPF

- **Scalability:** Its hierarchical design with areas allows it to scale to handle the massive complexity of an ISP's internal network.
- **Fast convergence:** For a network that changes frequently (like a large ISP's), fast convergence is crucial to minimize disruption when a link fails or is added.
- **Efficiency:** By dividing the network into smaller areas, OSPF limits the routing overhead and keeps the routing tables manageable.
- **Flexibility:** The ability to assign costs to links allows for intelligent traffic engineering, such as load balancing across multiple links.

IPv6 in IoT

IPv6 is essential for the Internet of Things (IoT) due to its massive address space, which can uniquely identify a near-infinite number of devices, a necessity as the number of connected devices grows exponentially. Key benefits include built-in security features like IPsec, a simplified header format for efficient routing, and support for technologies like 6LoWPAN and RPL that enable low-power, resource-constrained devices to connect to the internet. These features allow for greater scalability, better security, and enhanced interoperability among IoT devices.

Advantages of IPv6 for IoT

- **Vast address space:** The 128-bit address format provides a virtually unlimited number of unique IP addresses, which is crucial for the billions of devices expected in IoT networks.
- **Simplified header:** IPv6 has a simpler header structure than IPv4, which reduces the processing time for routers and allows for more efficient data routing, especially important for the high volume of small data packets from IoT devices.
- **Enhanced security:** IPv6 includes built-in support for IPsec, a security protocol that provides authentication and encryption, helping to secure communications between devices.
- **Efficiency:** New fields like the Flow Label enable special handling for real-time traffic and can improve performance for applications like audio and video.
- **Interoperability:** IPv6 helps avoid the need for complex workarounds and gateways, allowing devices from different manufacturers to communicate more easily and preventing the formation of closed ecosystems.
- **Support for low-power devices:** Technologies like 6LoWPAN allow IPv6 to be used efficiently over low-power and low-bandwidth wireless networks, which is ideal for many IoT sensors and devices.

Supporting technologies and protocols

- **6LoWPAN:** A standard that enables IPv6 to work over low-power wireless networks, making it suitable for devices with limited power and bandwidth.
- **RPL (Routing Protocol for Low-Power and Lossy Networks):** A routing protocol designed specifically for the "lossy" networks common in IoT environments.
- **CoAP:** A constrained application protocol that works well with IPv6 and is designed for constrained devices.
- **DTLS:** A security standard that provides encryption and authentication for IoT devices.

- **LWM2M and SUIT:** Standards for device management in IoT, which rely on IPv6 for connectivity.

Challenges and considerations

- **Transition and investment:** Migrating from IPv4 to IPv6 requires significant investment in upgrading infrastructure, protocols, and device firmware.
- **Security vulnerabilities:** While IPv6 has built-in security features, a large number of connected devices also creates a larger attack surface. A lack of proper security implementation, such as using default credentials, can leave many IoT devices vulnerable despite using IPv6.
- **Device support:** Some older or low-cost IoT devices may lack native IPv6 support, requiring careful consideration during the planning and implementation phases.

Routers in enterprise edge networks

Enterprise networks are typically divided into the **Core**, **Distribution**, and **Access** layers. The **Enterprise Edge** is the part of the network that connects the internal enterprise network to the **outside world** — such as the Internet, WAN links, cloud services, partner networks, and remote sites.At this boundary, **routers play a critical role.**

What Are Enterprise Edge Routers?

Enterprise edge routers are specialized routers placed at the **perimeter of an organization's network**.
They manage communication between:

- Internal corporate network
- External networks (ISP, cloud, VPN, remote branches, partner networks)

They provide **routing, security, traffic control, and redundancy** at the network edge.

Functions of Enterprise Edge Routers

1. Border Routing

- Connect the enterprise network to ISPs or WAN providers.
- Handle external routing protocols like **BGP**.

2. IP Address Management

- Perform **NAT / PAT** to map private enterprise IPs to public IPs.
- Help conserve IPv4 addresses.

3. Security Enforcement

- First line of defense.
- Work with:
  - Firewalls
  - IDS/IPS
  - Access Control Lists (ACLs)
- Drop unwanted traffic and prevent attacks.

4. VPN & Remote Access Gateway

- Terminate **site-to-site VPNs** for branch offices.
- Provide **remote-user VPN** access.

5. QoS (Quality of Service)

- Prioritize critical business applications.
- Control bandwidth usage.

6. Traffic Filtering and Policy Enforcement

- Apply policies based on:
  - Source/destination IP
  - Application type
  - User group
  - Time of day

7. High Availability

- Support redundancy features:
  - HSRP / VRRP / GLBP
  - Dual-ISP connections
  - Link failover

8. Load Balancing

- Distribute traffic across multiple ISP links or WAN paths.

Types of Enterprise Edge Routers

1. **Branch Routers**
   – For remote office connections.
2. **WAN Edge Routers**
   – For MPLS, leased lines, VPN tunnels.
3. **Internet Edge Routers**
   – For direct Internet access.
4. **SD-WAN Routers**
   – Intelligent routing using software-defined policies.

Examples of enterprise edge routers

- **Cisco ASR 9922:** Designed for large-scale enterprises with high-performance requirements.
- **Cisco 4331:** A versatile router that can be used for various enterprise networking needs.
- **Cisco Catalyst IR8300 Rugged Series Router:** Built for industrial and harsh environments.

Dynamic Routing in Disaster Response Networks

Disaster Response Networks (DRNs) are temporary, rapidly deployable communication systems used during natural or man-made disasters such as floods, cyclones, earthquakes, or terrorist attacks.
In such situations, normal communication infrastructure (cell towers, cables, routers) may be damaged or unavailable.
To maintain reliable communication among rescue teams, medical units, drones, and command centers, **dynamic routing** is essential.
Dynamic routing automatically adjusts routing paths based on real-time network conditions, node mobility, and link availability.

Need for Dynamic Routing in Disaster Situations

In disaster environments, the network conditions change rapidly due to:

- High node mobility (rescue teams move frequently)
- Unpredictable link failures
- Limited energy resources for mobile devices
- Temporary, infrastructure-less network setups
- Varying traffic loads
- Unstable wireless channels

Static routing is ineffective in such conditions.
Dynamic routing ensures **continuous, adaptive, and reliable communication**, which is critical for life-saving operations.

Characteristics of Disaster Response Networks

- **Infrastructure-less:** No fixed towers or routers; relies on mobile ad hoc networks (MANETs).
- **Highly dynamic topology:** Nodes move unpredictably.
- **Multi-hop communication:** Data travels over many intermediate nodes.
- **Energy-constrained:** Devices like sensors and drones rely on batteries.
- **Emergency priority:** Real-time communication is crucial.

Role of Dynamic Routing

Dynamic routing protocols automatically:

a) Discover Routes Automatically

The protocol finds a path only when required, avoiding manual configuration.

b) Maintain and Repair Routes

When a link breaks due to movement or power failure, the network finds a new path instantly.

c) Support Multi-hop Communication

Ensures communication even when nodes are far apart.

d) Provide Fast Convergence

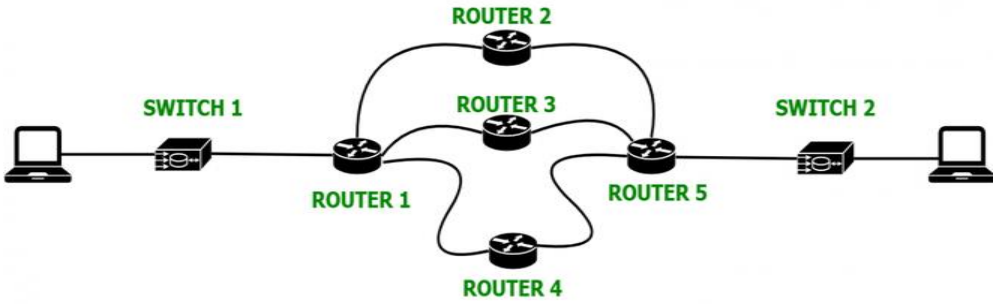
Updates and stabilizes routing tables quickly to avoid communication delays.

e) Reduce Control Overhead

Optimizes messages to save bandwidth and energy.

f) Improve Reliability

Ensures communication continuity even with unstable links.



Dynamic routing keeps all these nodes connected despite movement and link failures.

Dynamic Routing Protocols Used in DRNs

1. AODV (Ad hoc On-Demand Distance Vector)

- Reactive protocol (routes formed only when needed)
- Uses **Route Request (RREQ)** and **Route Reply (RREP)**
- Reduces unnecessary overhead
- Suitable for highly dynamic disaster networks

2. DSR (Dynamic Source Routing)

- Source keeps complete path information
- Good for small or medium networks
- Eliminates periodic updates

3. OLSR (Optimized Link State Routing)

- Proactive protocol (routes always available)
- Uses **Multi-Point Relays (MPRs)** to reduce flooding
- Suitable for medium to large DRNs

4. GPSR (Greedy Perimeter Stateless Routing)

- Geographic routing using GPS
- Suitable for drone-based rescue operations
- Uses node location instead of route tables

5. ZRP (Zone Routing Protocol)

- Hybrid protocol combining proactive + reactive features

- Reduces delays and overhead

Benefits of Dynamic Routing in Disaster Response

a) High Reliability

Automatically adapts to topology changes and ensures message delivery.

b) Faster Communication

Real-time adjustments provide low-latency communication for critical alerts.

c) Flexibility and Scalability

Easily handles new nodes and removal of failed nodes.

d) Efficient Resource Usage

Minimizes energy consumption by optimizing route selection.

e) Supports Heterogeneous Devices

Works across sensors, mobile phones, laptops, UAVs, and IoT devices.

Real-World Examples

- **Drones** delivering medical kits use GPSR routing.
- **Firefighters** deploy a mobile mesh network using AODV for search operations.
- **Ambulances and command centers** use OLSR-based MANETs for live communication.
- **Army relief operations** often utilize hybrid routing in rugged terrains.