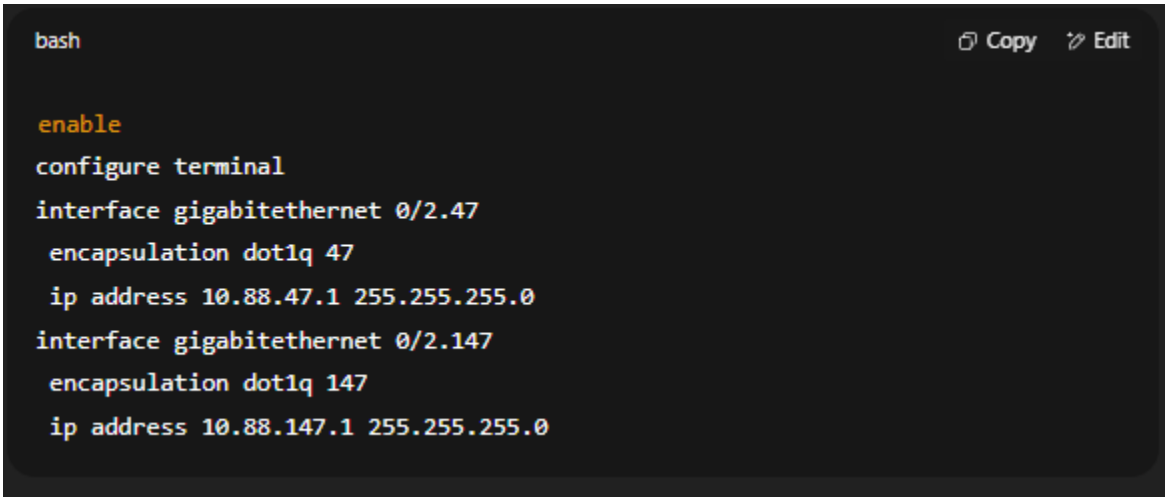

CompTIA N+ (N10-009) – Day 5
Chapter 7: IP Services

Default Gateways on Routers

- **Default Gateway** – Clients need a default gateway to send traffic outside their subnet. This is typically a routing-capable device such as a router or a Layer 3 (L3) switch.
- **Subinterfaces** – Allow multiple concurrent IP addresses to reside on a single router interface. Commonly used for routing between multiple VLANs.
    - A single physical interface can handle multiple VLANs by using VLAN tagging (802.1Q encapsulation).

Example Cisco Configuration:

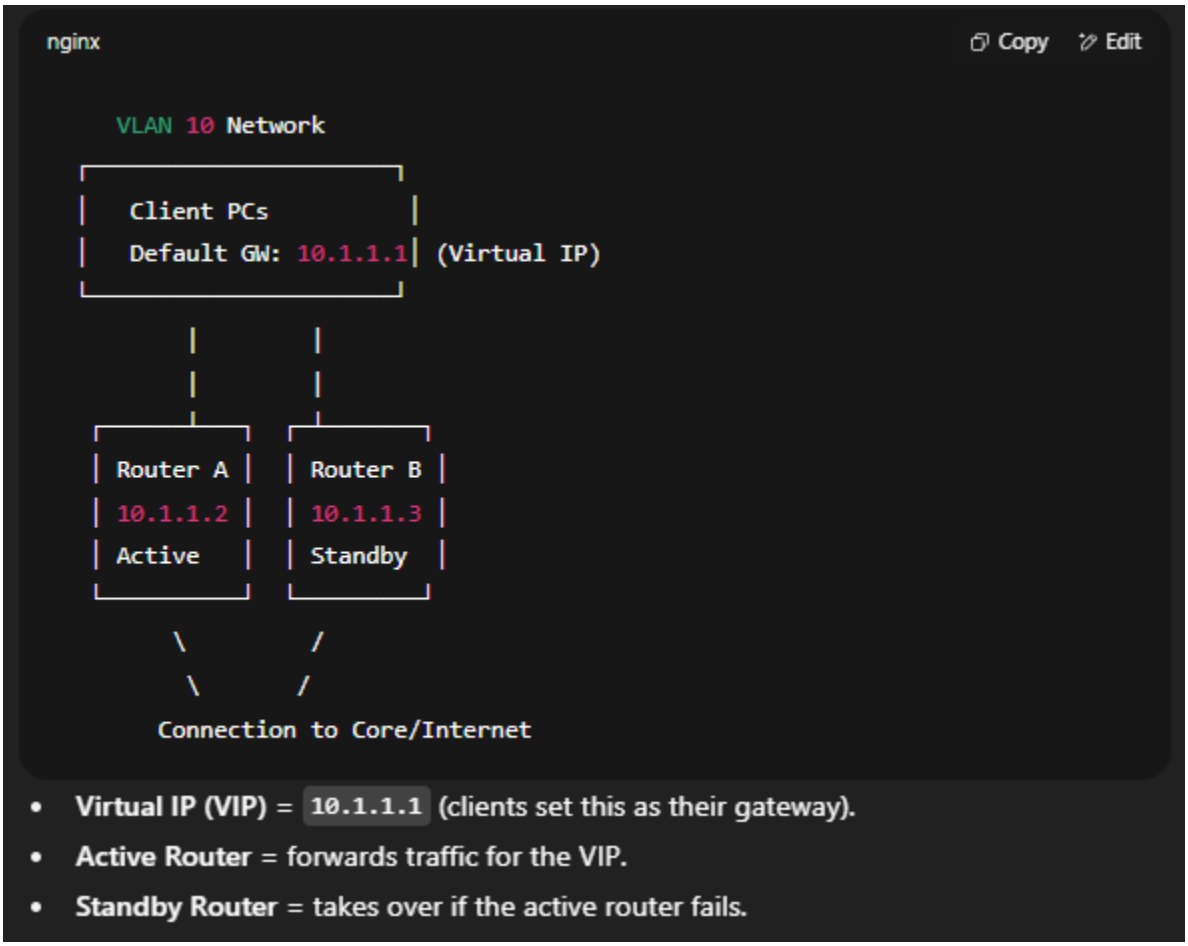


SVIs on L3 Switches

- An **SVI (Switched Virtual Interface)** is an interface on an L3 switch that is assigned an IP address.
- This allows the switch to route between VLANs without assigning an IP to each physical port.

VRRP and FHRPs

- **FHRP (First Hop Redundancy Protocol)** examples:
  - **VRRP (Virtual Router Redundancy Protocol)** – Vendor-neutral standard.
  - **HSRP (Hot Standby Router Protocol)** – Cisco proprietary.



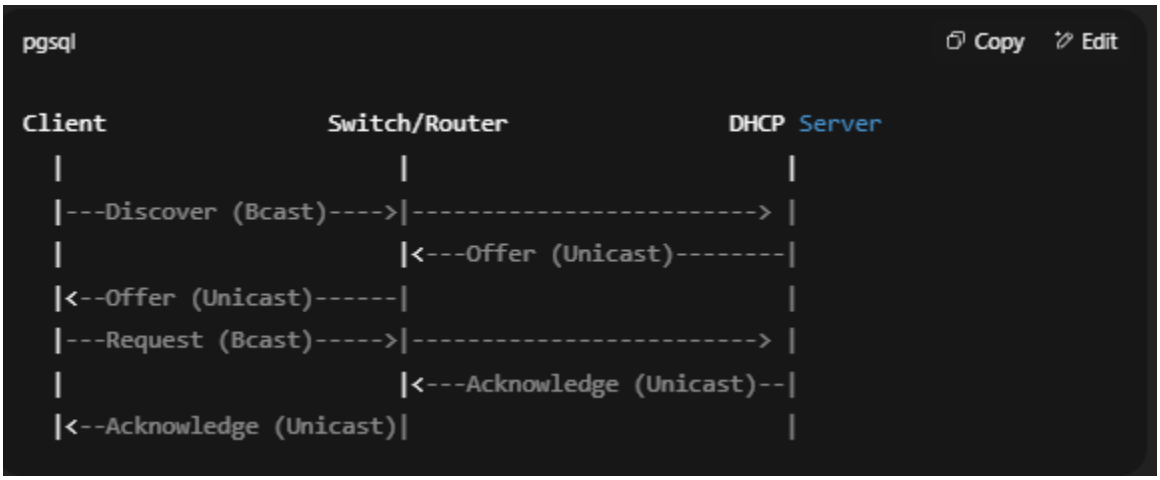
Key Points:

- Use a **Virtual IP (VIP)** address as the default gateway for clients.
- VIP is shared between two or more routers/switches for redundancy.
- Operates in **active-passive mode**: one device responds to the VIP and forwards traffic, the other(s) are on standby.

DHCP Configuration

DHCP Communication – DORA: *(HOLA, DORA!)*

1. **Discover** (Broadcast) – Client looks for a DHCP server.
2. **Offer** (Unicast) – Server offers an IP.
3. **Request** (Broadcast) – Client requests offered IP.
4. **Acknowledge** (Unicast) – Server confirms the lease.



IP host requirements:

- IP Address – Unique to the device.
- Subnet Mask – Defines the network.
- Default Gateway – Used to exit the local network.
- DNS IP – Resolves hostnames.

DHCP Scope – The range of IP addresses the server can lease in a subnet/VLAN/broadcast domain.

- **Exclusion range** – IP addresses set aside for statically assigned devices (servers, printers, etc.).

Static IPs, Duplicates, and Conflicts

- Duplicate IPs cause network connectivity issues.
- Most conflicts happen when a static IP is assigned inside the DHCP scope.
- **Fix:** Place static IPs outside the DHCP range or in the exclusion list.

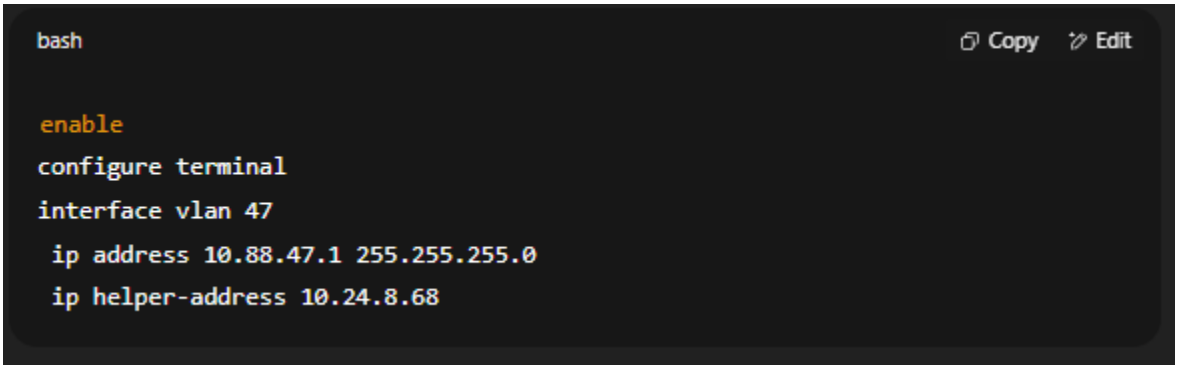
DHCP Options

- Provide additional information to clients.
    - Example: TFTP server IP (Option 66), Cisco-specific TFTP server IP (Option 150), DNS servers.

DHCP Relay Agent

- Needed when the DHCP server is not in the same subnet/VLAN/broadcast domain as the client.
- Forwards DHCP requests to the server across subnets.

Example Cisco Configuration:



DHCP Reservations

- Reserve a specific IP for a device's MAC address.
- Ensures the device always gets the same IP via DHCP.
- Common for printers, servers, and IoT devices.

APIPA & DHCP Exhaustion

- **APIPA (Automatic Private IP Addressing)**:
    - Address range: `169.254.0.0/16`.
    - Indicates the DHCP process failed.
    - May mean the DHCP pool is exhausted.

Solutions for Exhaustion:

- Reduce DHCP lease time.
- Increase the pool size (adjust subnet mask).

Rogue DHCP Servers

- Enable **on-path attacks** like DHCP spoofing (attacker gives fake gateway to capture traffic).
- Mitigation:
    - Enable **DHCP Snooping** – A switch security feature that allows DHCP messages only from trusted ports (trusted = uplink to the real DHCP server).

the missing definitions and explanations added:

Chapter 7: IP Services – The Domain Name System (DNS)

Overview

- **Purpose:** Translate human-readable hostnames (e.g., `www.example.com`) into IP addresses.
- **Protocol:** Uses **UDP port 53** for standard queries, **TCP port 53** for zone transfers.

DNS Zones

- **Zone:** An administrative segment of DNS containing records for part of the namespace.
- **Authoritative Name Server:** Stores and provides the official DNS records for the zone. Discoverable with `nslookup` or `dig`.
- **Primary DNS Server:** Holds the original, writable copy of the zone.
- **Secondary DNS Server:** Holds a read-only copy of the zone, synced via **zone transfers**.

SOA (Start of Authority) Record:

- Identifies the authoritative server for the zone.
- Contains:
    - Primary server name.
    - Contact email for the domain admin.
    - Serial number (increments when zone changes).
- Used by secondary servers to check if they need updates.

Zone Transfers:

- Updates secondary servers with data from the primary server.
- Uses the SOA serial number to validate freshness.

DNS Hierarchy

1. **Root** – . (root)
2. **Top-Level Domains (TLDs):** `.com`, `.org`, `.edu`, `.ca`, etc.
3. **Second-Level Domains:** `stormwindstudios`, `comptia`.
4. **Subdomains:** `.app`, `.www`.

Types of DNS Lookups

- **Forward Lookup:** Domain → IP address.
- **Reverse Lookup:** IP address → Domain name (via PTR records).
- **Recursive Lookup:** The DNS server performs all necessary queries on behalf of the client.
- **Iterative Lookup:** DNS server responds with the best info it has (may refer to another server).

DNS Cache: Stores recently resolved names (default 86,400s = 1 day). Clear with:

TTL (Time to Live): How long a record stays cached before expiring. Lower TTL speeds up propagation after changes.

Common DNS Record Types

- **A:** IPv4 address for an FQDN.
- **AAAA:** IPv6 address for an FQDN.
- **CNAME:** Canonical name (alias to another domain).
- **MX:** Mail Exchange – points to a mail server.
- **SOA:** Start of Authority – zone metadata.
- **PTR:** Pointer – reverse DNS mapping.
- **SRV:** Maps a service to hostname & port.
- **NS:** Name server for the domain.
- **TXT:** Text data (used for security):
    - **SPF:** Lists authorized mail servers.
    - **DKIM:** Stores public key for email signing.
    - **DMARC:** Policy for handling unverified email.

Hosts File

- Checked **before** DNS.
- Can be used maliciously (DNS hijacking).
- Path (Windows): `C:\\Windows\\System32\\Drivers\\etc\\hosts`
- Lookup order: **Hosts File → DNS Cache → DNS Server**

DNS Security Threats

DNS Spoofing/Poisoning:

- Attacker injects false DNS records to redirect traffic to malicious sites.

DNS Protocols

Protocol	Name	Port	Purpose
DNS	Domain Name Sys.	TCP/UDP 53	Standard name resolution.
DoH	DNS over HTTPS	TCP 443	Encrypt DNS in HTTPS traffic.
DoT	DNS over TLS	TCP 853	Encrypt DNS with TLS.

DNSSEC:

- DNS Security Extensions.
- Uses cryptographic signatures to validate DNS responses, preventing spoofing.

Chapter 8: Routing – Introduction

The Routing Table

- Shows all known network prefixes and the routes to reach them.
- Decision process: **Longest Match → Lowest Administrative Distance → Lowest Metric**.

Routing Sources

Source	AD	Metric	Operation	Communication
Connected	0	0	Directly connected network.	None
Static	1	0	Manually configured (`ip route ...`).	None
EIGRP	90/170	Bandwidth + Delay	Chooses best (successor) & backup (feasible successor) routes.	Multicast 224.0.0.10
OSPF	110	Cost (sum of interface costs)	Uses SPF (shortest path first) algorithm.	Multicast 224.0.0.5 & 224.0.0.6
BGP	20/200	Attributes (AS-path, Local-pref)	Internet routing (~900k routes aggregated to ~500k).	TCP 179 (unicast)
IS-IS	115	Cost (default 10 per link)	Often used internally in large networks.	L2 multicast 01:08:c2:00:00:14/15

Administrative Distance (AD)

- Lower = more trusted.
- If AD is equal, **use the metric**:
  - **Metric:** A value representing path preference based on protocol-specific criteria (e.g., bandwidth, delay, hop count).
  - Lower metric = preferred path.

Longest Match Rule

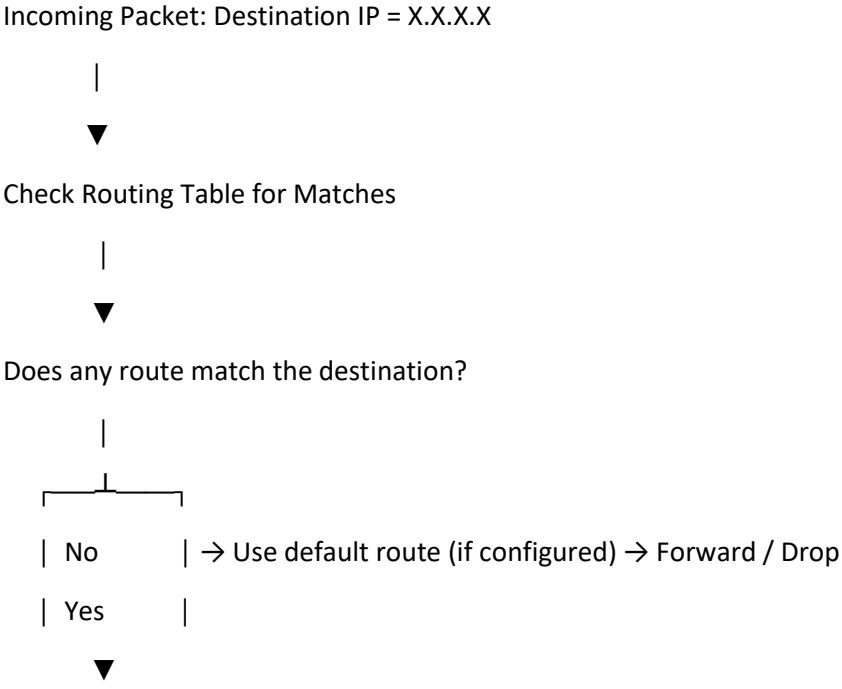
- The route with the most specific subnet mask matching the destination is chosen.
- Example: For traffic to `192.168.1.5`, `/29` will be chosen over `/24`.

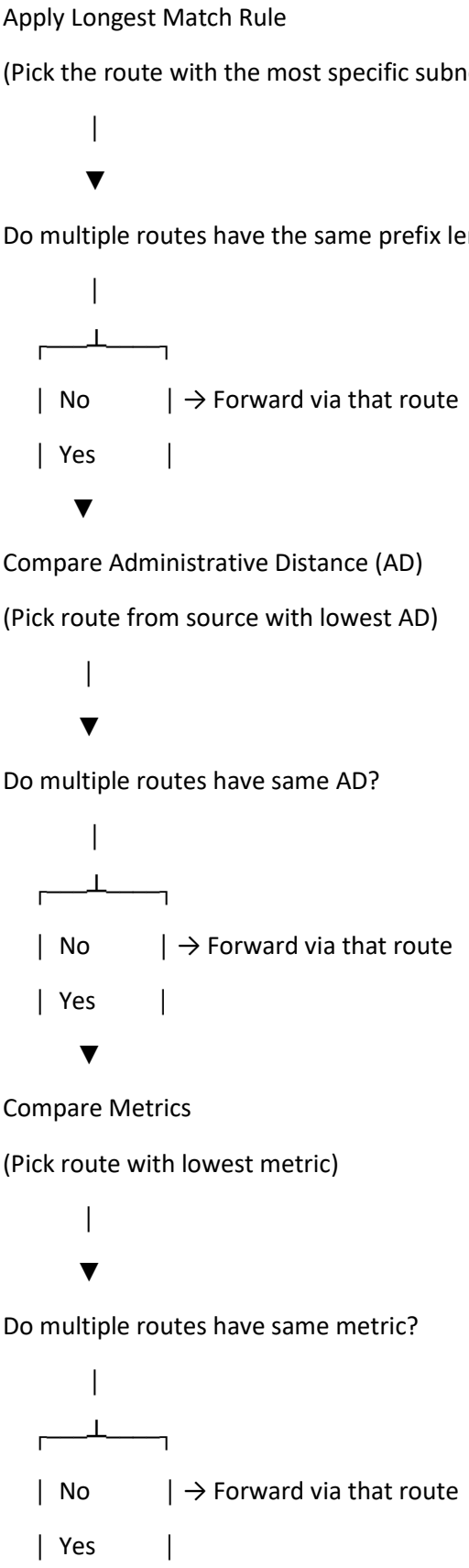
Diverse Paths & Longest Match Rule

- Using multiple ISPs means the router may have overlapping routes.
- Longest match rule ensures that local or more specific ISP routes are used before default routes.

Load Balancing & Longest Match Rule

- If two routes have the **same AD, same metric, and same prefix length**, the router may **load balance** traffic across both paths.



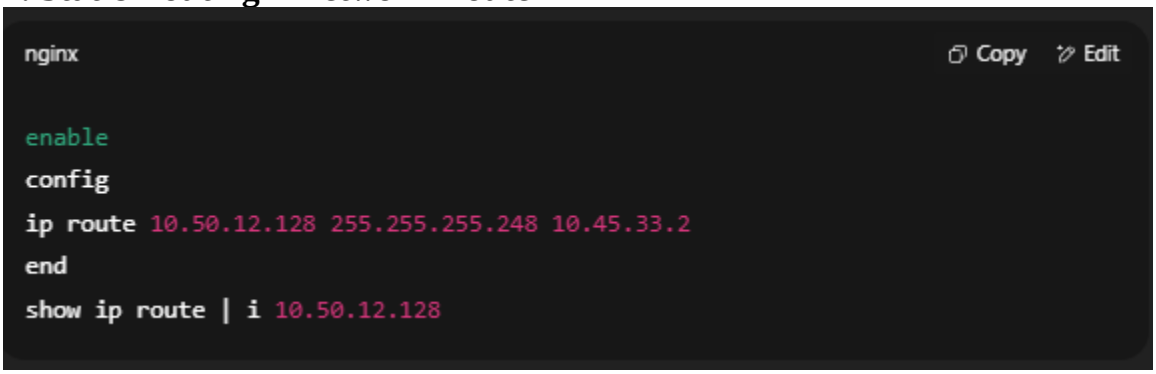

Apply Longest Match Rule
(Pick the route with the most specific subnet mask)
Do multiple routes have the same prefix length?
No
→ Forward via that route
Yes
Compare Administrative Distance (AD)
(Pick route from source with lowest AD)
Do multiple routes have same AD?
No
→ Forward via that route
Yes
Compare Metrics
(Pick route with lowest metric)
Do multiple routes have same metric?
No
→ Forward via that route
Yes

▼

Load Balance (Split traffic across available equal-cost paths)

Static Routing Types & What Enables Them

1. Static Routing – Network Route



- **What it is:**
  - A **network route** to a whole subnet.
  - Subnet mask (`/29` here) defines a block of addresses.
- **Enabled by:**
  - Manually adding a route in the router's config with `ip route [network] [mask] [next-hop]`.
  - This route becomes active if the next-hop IP is reachable.

---

2. Static Routing – Host Route

```nginx
enable
config
ip route 10.50.12.129 255.255.255.255 10.45.33.2
end
```

What it is:

- A **host route** — points to **one single IP** (`/32`).
- Often used for a specific device that's outside the normal routing logic.

- **Enabled by:**
  - Manually adding a route with a `255.255.255.255` mask.
  - Activated when next-hop is reachable.

---

3. Static Routing – Default Route

```nginx
enable
config
ip route 0.0.0.0 0.0.0.0 203.0.113.89
end
```

- **What it is:**
  - A **catch-all** route for any destination **not already in the routing table**.
  - Often called the "gateway of last resort."
- **Enabled by:**
  - Manually setting the `0.0.0.0 0.0.0.0` network and mask to point to the next-hop.

---

4. Static Routing – Floating Route

```nginx
enable
config
ip route 0.0.0.0 0.0.0.0 203.0.113.89
ip route 0.0.0.0 0.0.0.0 192.0.2.241 15
end
```

- **What it is:**
  - A **backup route** with a higher **Administrative Distance (AD)** than the primary route.
  - Only takes over if the primary route is removed from the table (e.g., link failure).
- **Enabled by:**
  - Adding a second static route to the same destination but with a **manual AD** (e.g., `15`).
  - AD must be **higher than the primary route's AD** but lower than unwanted alternatives.

Dynamic Routing Protocols

Consists of **EIGRP**, **OSPF**, **BGP**, and **IS-IS**.

Border Gateway Protocol (BGP)

Exam Note: Used BGP to advertise public prefixes (i.e., you have public IPs registered to you, and you wish to advertise them to your ISPs so they become reachable).

Routing Loops and TTL

- A data packet is repeatedly routed through the same routers.
- Commonly mitigated using **Time-To-Live (TTL)**.
- The IP header contains a TTL value.
- Each router hop reduces the value by **1**.
- Once the value reaches **0**, the packet is dropped.

Asymmetric Routing

- Outgoing packets take a different route than the returning incoming packets.
- Disruptive with **NAT**, **IPS**, **IDS**, and firewall services.