

1. BGP (Border Gateway Protocol)

BGP is a **path-vector protocol** used to manage routing between Autonomous Systems (AS).

- **Message Types (Wireshark Analysis):**
 - **OPEN:** Used to establish the BGP session and negotiate capabilities (like 4-byte AS support).
 - **UPDATE:** The most critical message; it carries routing prefixes (NLRI) and their associated **Path Attributes**.
 - **KEEPALIVE:** Sent periodically (TCP port 179) to ensure the peer is still active.
 - **NOTIFICATION:** Sent when an error occurs, leading to immediate session closure.
- **Path Attributes & Selection:** BGP uses a specific order to choose the "best path":
 - **Weight (Cisco only):** Local to the router; highest is preferred.
 - **Local Preference:** Used within an AS to choose an exit point; **highest** is preferred.
 - **AS-PATH:** The list of ASes a route has crossed; **shortest** path is preferred.
 - **Origin:** How BGP learned the route (IGP < EGP < Incomplete).
 - **MED (Multi-Exit Discriminator):** Suggestion to an external AS for incoming traffic; **lowest** is preferred.

2. MPLS & L3VPNs

MPLS forwards packets using **labels** assigned to Forwarding Equivalence Classes (FECs), rather than full IP lookups in the core.

- **Label Operations:**
 - **PUSH:** Adding a label (at the Ingress PE).
 - **SWAP:** Replacing a label in the core (at P routers).
 - **POP:** Removing a label (at the Egress PE).
 - **PHP (Penultimate Hop Popping):** The router before the destination PE removes the outer label to reduce the destination's processing load.
- **VPN Structure:** L3VPNs use a **two-label stack**:
 - **Outer Label:** Used to reach the remote BGP Next-Hop (the Egress PE).
 - **Inner Label (VPN Label):** Identifies the specific **VRF** (Virtual Routing and Forwarding) or customer site.

3. VXLAN (The Overlay Concept)

VXLAN is a **MAC-in-UDP** encapsulation technology that extends Layer 2 segments over a Layer 3 underlay.

- **Wireshark Identifiers:** Look for **UDP Port 4789**.
- **VNI (VXLAN Network Identifier):** A 24-bit field in the VXLAN header that allows up to **16 million** unique segments (compared to 4096 for VLANs).
- **VTEP (VXLAN Tunnel Endpoint):** The device (usually a Leaf switch) that performs the encapsulation and decapsulation.
- **Control Plane:** While initial VXLAN used "Flood and Learn," modern deployments use **BGP EVPN** to exchange MAC and IP reachability information to reduce network flooding.

4. Quality of Service (QoS)

QoS ensures critical traffic (like voice or video) receives priority over "Best Effort" data.

- **IntServ (Integrated Services):** Uses **RSVP** signaling for per-flow resource reservation. It creates "soft states" in routers that must be periodically refreshed.
- **DiffServ (Differentiated Services):** More scalable; it aggregates traffic into classes.
 - **DSCP (Differentiated Services Code Point):** A 6-bit field in the IP header (TOS byte) used to mark packets.
 - **PHB (Per-Hop Behavior):** Includes **EF** (Expedited Forwarding for low delay/voice) and **AF** (Assured Forwarding with different drop precedences).
- **Tools:** **Token Buckets** are used for metering/policing to ensure traffic stays within agreed rates.

5. Content Distribution Networks (CDNs)

A CDN is a proactive network of **surrogate (edge) servers** that deliver content on behalf of an origin site to improve performance.

- **Request Routing:** The most common method is **DNS-based redirection**. When a client requests a URL, the CDN's DNS server provides the IP of a nearby edge server based on network conditions and the client's location.
- **Proactive vs. Reactive:** Unlike standard web caches (which are reactive and ISP-controlled), CDNs are **proactive** and controlled by the content provider.

6. Network Management & SNMP

Network management is structured around the **FCAPS** model: Fault, Configuration, Accounting, Performance, and Security.

- **SNMP (Simple Network Management Protocol):**
 - Uses a **Manager/Agent** paradigm where the manager polls the agent or the agent sends unsolicited **Traps**.
 - **MIB (Management Information Base):** A hierarchical database (modeled using the ISO Object Identifier tree) that defines what can be managed.
 - **Encoding:** Uses ASN.1 with **BER (Basic Encoding Rules)**, which follows a **TLV (Type, Length, Value)** format.
- **TMN (Telecommunications Management Network):** A more complex, object-oriented framework (often using **CMIP**) used by telecom operators to manage multi-layer networks.