JN0-649 Training Course

Enterprise Routing and Switching Professional (JNCIP-ENT)

Structured Learning & Certification Preparation

Table of Contents

Introduction

The Enterprise Routing and Switching Professional (JNCIP-ENT) certification, designated by exam code JN0-649, is designed to validate a professional's ability to implement, troubleshoot, and manage complex enterprise routing and switching technologies. It represents a significant benchmark for networking specialists, confirming their mastery of advanced routing protocols and switching configurations within a modern enterprise environment. As network architectures evolve to support higher density and greater automation, this certification ensures that practitioners possess the technical depth required to maintain high-availability infrastructures.

About This Training / Certification

This certification assesses advanced competencies in the configuration and management of enterprise-level networking components. Positioned as a professional-level credential, it serves as an intermediate to advanced milestone in a networking career path, typically following the acquisition of specialist-level knowledge. The certification focuses on the practical application of theoretical networking concepts, moving beyond basic connectivity to address sophisticated traffic engineering, policy implementation, and system resiliency. It is an essential component for those seeking to demonstrate their readiness for high-level architectural and operational roles.

What We Offer (AAAdemy)

AAAdemy provides structured training resources designed to support certification preparation and skill development across a wide range of IT domains. Our learning materials are built around clear knowledge structures, practical study guidance, and exam-oriented practice to help learners progress with confidence.

We offer well-organized knowledge explanations that break down complex topics into clear, understandable sections aligned with official exam objectives and real-world skill requirements. Each topic is designed to support both conceptual understanding and practical application.

Our study plans and learning guidance help learners follow a logical progression, focusing on key concepts, common pitfalls, and effective preparation strategies. This approach enables learners to study efficiently while maintaining a clear view of their learning goals.

To reinforce understanding, AAAdemy also provides practice questions and exam-focused insights that reflect typical certification scenarios. These resources are intended to help learners evaluate their readiness and strengthen their confidence before taking an exam.

All content is designed for flexible, self-paced learning, allowing individuals to study independently or alongside their existing professional or academic commitments.

Knowledge Overview

The knowledge scope for this certification is divided into critical domains that reflect the complexities of modern enterprise environments. Candidates are expected to demonstrate a profound conceptual understanding of the following areas:

- **Interior Gateway Protocols (IGPs):** Advanced implementation and troubleshooting of OSPF and IS-IS, focusing on multi-area operations and path selection.
- **Border Gateway Protocol (BGP):** Comprehension of BGP attributes, routing policies, and the integration of external and internal routing domains.
- **IP Multicast:** Principles of efficient data distribution, including PIM-SM and IGMP, to support one-to-many communications.
- **Ethernet Switching and Spanning Tree:** Deep expertise in Layer 2 loop prevention, VLAN management, and high-availability protocols.
- **Layer 2 Authentication and Access Control:** Implementation of security frameworks, such as 802.1X, to manage and secure network access points.
- **IP Telephony Features:** Integration and optimization of network infrastructure to support Voice over IP (VoIP) and specialized telephony requirements.
- **Class of Service (CoS):** Advanced traffic prioritization, queuing, and congestion management to ensure quality for critical applications.
- **EVPN:** Understanding Ethernet VPN concepts for scalable Layer 2 and Layer 3 connectivity across modern data center and enterprise fabrics.

Detailed Knowledge Explanation

1. JN0-649 BGP

The Border Gateway Protocol (BGP) is the indispensable engine of the modern internet and large-scale enterprise edges. While Interior Gateway Protocols (IGPs) like OSPF prioritize rapid convergence and internal topology visibility, BGP is a path-vector protocol engineered for stability, scalability, and granular policy control between distinct Autonomous Systems (ASes). For the JNCIS-ENT professional, mastering BGP’s path-selection logic and its nuanced loop-prevention mechanisms is essential for designing resilient multi-homed architectures and inter-domain connectivity.

1. BGP Overview

BGP differentiates itself from IGPs through its scope and transport reliability. By operating over **TCP port 179**, BGP leverages a connection-oriented protocol to ensure the reliable exchange of massive routing tables—often exceeding 900,000 prefixes in the global DFZ—without the instability of frequent link-state SPF recalculations.

1.1 Protocol Type

BGP is a **path vector protocol**. Its primary role is to manage reachability between Autonomous Systems by tracking the **AS_PATH** attribute. Unlike distance-vector protocols that only see a neighbor's "distance," BGP sees the entire list of ASes a route has traversed, allowing for sophisticated loop detection and policy-based path manipulation.

1.2 Key Concepts

BGP behavior is dictated by the relationship between peers.

1.2.1 eBGP vs. iBGP

- **eBGP (External BGP):** Peers in different ASes. In Junos, eBGP has a default **TTL of 1**, requiring peers to be directly connected unless `multihop` is configured.
- **iBGP (Internal BGP):** Peers within the same AS. To prevent loops, iBGP utilizes the **"no iBGP-to-iBGP advertisement" rule**: a router will not forward a route learned from one iBGP peer to another. This necessitates a **full-mesh** topology or scaling mechanisms like route reflectors.

1.2.2 BGP Attributes

BGP evaluates attributes in a deterministic hierarchy:

- **Well-Known Mandatory: AS_PATH** (loop detection), **NEXT_HOP** (IP reachability), and **ORIGIN** (source of the route).
- **Optional Transitive: Community** (tagging for policy application) and **Aggregator** (identifying the router that performed summarization).

1.2.3 Routing Policies

BGP is fundamentally a "policy-based" protocol. Junos uses powerful import and export policies to manipulate attributes (like Local Preference) or filter specific prefixes. This allows an AS to act as a transit network or a stub, depending on business requirements.

2. Scaling with BGP

Scaling iBGP requires moving beyond the n(n-1)/2 complexity of a full mesh.

2.1 Route Reflectors

Route Reflectors (RRs) use a hub-and-spoke logic. An RR reflects routes learned from its **clients** to all other clients and non-clients, effectively bypassing the iBGP split-horizon rule within a cluster.

2.2 Confederations

Confederations divide a large AS into smaller sub-ASes. To external peers, the network appears as a single AS, but internally, sub-ASes use eBGP-like rules to simplify the internal mesh.

3. BGP Path Selection

Junos follows a strict, deterministic sequence to select the "best path."

3.1 Decision Process

1. **Local Preference:** Highest is preferred (controls outbound traffic).
2. **AS_PATH:** Shortest (fewer hops) is preferred.
3. **MED (Multi-Exit Discriminator):** Lowest is preferred (influences inbound traffic from neighbors).
4. **eBGP vs. iBGP:** eBGP routes are preferred over iBGP.
5. **Router ID:** Lowest Router ID is the tie-breaker.

3.2 BGP Communities

Communities are 32-bit tags. Predefined types include:

- **NO_EXPORT:** Do not advertise to eBGP peers.
- **NO_ADVERTISE:** Do not advertise to any peer.

4. Configurations

4.1 Basic eBGP Configuration

```
set protocols bgp group external-peers type external
set protocols bgp group external-peers peer-as 65002
set protocols bgp group external-peers neighbor 192.168.1.2
```

4.2 Route Reflector Setup

On the RR, designate the client:

```
set protocols bgp group internal-clients cluster 1.1.1.1
set protocols bgp group internal-clients neighbor 10.0.0.2 cluster-client
```

5. Advanced BGP Configurations

5.1 Advanced Policies

5.1.1 Filtering Prefixes

```
set policy-options policy-statement reject-bogon term 1 from route-filter 192.168.0.0/16 orlonger
set policy-options policy-statement reject-bogon term 1 then reject
```

5.1.2 AS-Path Prepending

set policy-options policy-statement prepend-as term 1 then as-path-prepend "65001 65001"

5.1.3 Adjusting Local Preference

set policy-options policy-statement set-local-pref term 1 then local-preference 200

5.2 Route Aggregation

set routing-options aggregate route 10.0.0.0/8

6. Troubleshooting BGP Connections

6.1 Common Issues

- **Session Not Established:** Check for **TCP 179** blockages or AS mismatches.
- **Routes Not Received:** Check import policies or verify if the route exists in the BGP table.
- **AS-Path Loops:** Routes are rejected if the local AS is in the received AS_PATH.

6.2 Debugging Tools

- `show bgp summary`: Check if the state is **Established**. If it says **Active**, the router is actively trying to connect but failing (common for config errors).
- `show route protocol bgp`: View the BGP table.
- `show bgp neighbor`: Detailed logs for specific peers.

7. Real-World BGP Use Cases

- **Multi-Homed Connections:** Connecting to two ISPs for redundancy.
- **Traffic Engineering:** Using MED to prefer one entry point over another.
- **DDoS Mitigation:** Using **blackhole** routing to drop malicious traffic at the ISP edge.

8. BGP Administrative Distance (Route Preference)

In Junos, lower preference is better.

- **BGP (iBGP and eBGP):** 170.
- **OSPF Internal:** 10.
- **OSPF External:** 150.
- **Connected:** 0 | **Static:** 5.

9. BGP Loop Prevention Mechanism

- **eBGP:** Uses **AS_PATH**. Routes containing the local AS are rejected.
- **iBGP:** Uses the **"no iBGP-to-iBGP advertisement" rule**.

10. BGP Multipath (Add-Path)

Junos supports **ECMP** for BGP by allowing multiple equal-cost paths in the forwarding table.

set protocols bgp group <name> multipath

11. BGP for IPv6 Routing

To support IPv6, the `inet6 unicast` address family must be declared.

set protocols bgp group ipv6-peers family inet6 unicast

12. BGP Practice Question

Q1: Which BGP attribute is used to determine the origin of a route and can have values such as IGP, EGP, or Incomplete?
A. NEXT_HOP
B. LOCAL_PREFERENCE
C. COMMUNITY
D. ORIGIN

Q2: In BGP path selection, which attribute is considered **first** when evaluating multiple routes to the same destination?
A. LOCAL_PREFERENCE
B. AS_PATH
C. MED
D. NEXT_HOP

Q3: Which BGP feature reduces the need for a full-mesh iBGP topology?
A. MED
B. BGP Confederation
C. Route Reflector
D. Aggregator

Q4: Which BGP community prevents a route from being advertised outside the local AS?
A. BLACKHOLE
B. LOCAL_AS
C. NO_ADVERTISE
D. NO_EXPORT

Q5: In which situation is BGP AS-path prepending typically used?
A. To make a route less attractive for inbound traffic
B. To enforce MED values across different ASes
C. To prevent BGP route loops within the same AS
D. To reduce the size of the routing table

Q6: What command is used in Junos to configure a router as a BGP route reflector?
A. set protocols bgp cluster-id
B. set routing-options reflector enable
C. set protocols bgp group internal cluster <cluster-id>
D. set bgp reflector internal

Q7: Which BGP attribute is used to influence routing between autonomous systems and prefers the lowest value?
A. LOCAL_PREFERENCE
B. AS_PATH
C. COMMUNITY
D. MED

Q8: What is the default TTL (Time-to-Live) value for eBGP sessions?
A. 64
B. 1
C. 128
D. 255

Q9: Which BGP attribute is mandatory and helps in loop prevention by listing all ASes a route has passed through?
A. NEXT_HOP
B. ORIGIN
C. AS_PATH
D. LOCAL_PREFERENCE

Q10: What does the following Junos command achieve?

```
set policy-options policy-statement prefer-local term 1 then local-preference 200
```

A. Sets the local preference to 200 for matching routes
B. Discards all prefixes below a certain local preference
C. Accepts routes only if local preference is 200
D. Rejects routes from AS 200

---

2. JN0-649 Class of Service (CoS)

Class of Service (CoS) is a strategic necessity for managing finite bandwidth and ensuring that latency-sensitive applications—like VoIP and real-time video—remain functional during congestion. Without CoS, the network operates on a "best-effort" basis, which can be catastrophic for business-critical data.

1. Overview of Class of Service (CoS)

1.1 Purpose of CoS

CoS prioritizes traffic to mitigate the impact of jitter and latency. It ensures that voice traffic receives preferential treatment over a large background file transfer.

2. Core Concepts of CoS

2.1 Classification

The process of identifying traffic.

- **DSCP:** 6-bit IP header field (e.g., DSCP 46/EF).
- **802.1p:** 3-bit Ethernet header field (0-7).
- **IP Precedence:** Older 3-bit ToS field method.

2.2 Scheduling

Determines egress priority.

- **Strict Priority:** The queue is always served first.
- **Weighted Round Robin (WRR):** Bandwidth is allocated proportionally.

2.3 Shaping vs. Policing

- **Policing (Ingress):** Enforces a **hard rate limit**. Excess traffic is **dropped or re-marked**.
- **Shaping (Egress):** Smooths bursts by **buffering** packets and sending them later.

3. Configurations

3.1 Defining Classifiers

```
set class-of-service classifiers dscp voice-class import default
set class-of-service interfaces ge-0/0/0 unit 0 classifiers dscp voice-class
```

3.2 Configuring Schedulers

```
set class-of-service schedulers voice-sched transmit-rate percent 30
set class-of-service schedulers voice-sched priority strict-high
set class-of-service scheduler-maps corp-map forwarding-class voice scheduler voice-sched
set class-of-service interfaces ge-0/0/1 scheduler-map corp-map
```

4. Practical Example

In a converged network, **Voice** is mapped to `strict-high` priority, **Video** receives a guaranteed 20% bandwidth via WRR, and **Data** is shaped at the egress to 50% of link speed.

5. Monitoring and Troubleshooting CoS

5.1 Monitoring CoS

- `show interfaces queue ge-0/0/0`: Check for drops in specific forwarding classes.
- `show class-of-service classifier`: Verify mapping.

5.2 Troubleshooting CoS

- **Symptom:** Voice latency. **Cause:** Misclassification or lack of `strict-high` priority.
- **Symptom:** Policing drops. **Cause:** Threshold set lower than burst traffic.

6. Real-World Use Cases

- **Enterprise:** VoIP quality.
- **Service Provider:** Enforcing SLAs for premium customers.

7. Best Practices

Start with **NetFlow** traffic analysis to identify critical flows before applying policies.

8. Relationship Between CoS and QoS

Clarification Statement: CoS is typically used to mark traffic at Layer 2 (e.g., 802.1p), while QoS is a broader framework encompassing traffic classification, scheduling, policing, and shaping at Layers 3–7.

9. Hybrid Scheduling – Low Latency Queuing (LLQ)

LLQ integrates strict priority with weighted scheduling to ensure low latency for real-time traffic while preserving fairness for other classes.

10. Monitoring Tools

Use **SNMP, NetFlow, Telemetry,** and **Juniper HealthBot** for long-term CoS validation.

11. Class of service (CoS) Practice Question

Q1: Which field in an IP header is commonly used to classify packets for CoS purposes?
A. IP Precedence
B. VLAN ID
C. DSCP (Differentiated Services Code Point)
D. TCP Port Number

Q2: In Junos, which CoS mechanism ensures that excess traffic is queued rather than dropped, smoothing out traffic bursts?
A. Policing
B. Traffic Marking

C. Shaping
D. Rewriting

Q3: What is the primary difference between strict priority scheduling and Weighted Round Robin (WRR)?
A. WRR is only used on Layer 3 routers
B. Strict priority always services high-priority queues first, while WRR allocates bandwidth based on weights
C. WRR does not support DSCP
D. Strict priority can only be used for voice traffic

Q4: Which of the following is a classification method that uses MAC address or protocol type?
A. ACL-based classification
B. Shaping
C. Policing
D. Scheduler mapping

Q5: What is the purpose of defining a scheduler in a CoS policy?
A. To control how bandwidth is allocated across queues
B. To determine how incoming packets are filtered
C. To assign IP addresses based on priority
D. To tag packets with VLAN IDs

Q6: Which CoS mechanism is most appropriate when you want to **drop** excess traffic instead of buffering it?
A. Rewriting
B. Policing
C. Scheduling
D. Forwarding

Q7: What is one reason to use DSCP-based classification over 802.1p in a CoS environment?
A. 802.1p is supported on all network devices
B. DSCP has fewer marking values
C. DSCP is used only in VLAN headers
D. DSCP works at Layer 3, making it effective across IP networks

Q8: What is the purpose of a scheduler map in Junos CoS configuration?
A. To classify traffic into default classes
B. To route packets to multiple destinations
C. To link forwarding classes to specific scheduler profiles
D. To rewrite traffic priority levels

Q9: Which of the following would most likely result in voice traffic being delayed in a congested network?
A. Voice traffic is placed in a low-priority queue
B. Traffic is classified using DSCP EF
C. Voice VLAN is assigned to the interface
D. Strict priority scheduling is used

Q10: What command would you use to verify queue utilization and dropped packets on an interface in Junos?
A. show interfaces queue ge-0/0/1

B. show dscp-map
C. show class-of-service schedulers
D. show interfaces statistics

---

3. JN0-649 EVPN

EVPN modernizes Layer 2 extension by using **MP-BGP (AFI 25, SAFI 70)** as the control plane. This replaces the inefficient flood-and-learn method of traditional VPLS with control-plane MAC learning.

1. Overview of EVPN

1.1 Purpose

EVPN provides **MAC mobility**, **multi-tenancy**, and **all-active multi-homing** over a Layer 3 underlay (IP or MPLS).

2. Core Concepts

2.1 Route Types

- **Type 1 (EAD):** Ethernet Auto-Discovery; used for aliasing and split-horizon.
- **Type 2 (MAC/IP):** Propagates host MAC/IP bindings.
- **Type 3 (Inclusive Multicast):** Manages BUM traffic replication.
- **Type 4 (Ethernet Segment):** Critical for **Designated Forwarder (DF) election**. DF is selected based on **ESI, Router ID, and Priority** to prevent BUM duplication.
- **Type 5 (IP Prefix):** Propagates /24 or /32 IP subnets for L3 forwarding.

2.2 VXLAN (Virtual Extensible LAN)

VXLAN encapsulates L2 frames into UDP. **VTEPs** use a 24-bit **VNI** to identify up to 16 million unique segments.

3. Configurations

set protocols evpn encapsulation vxlan
set protocols evpn extended-vni-list all
set vlans v1001 vxlan vni 1001

4. Troubleshooting EVPN

- `show evpn database`: Verify MAC learning.
- `show evpn instance`: Check VNI/ESI status.

5. Advanced EVPN Features

- **Multi-Homing (ESI):** Uses an **ESI** to connect a device to multiple VTEPs.
- **ARP/ND Suppression:** Type 2 routes allow VTEPs to respond locally to ARP requests, significantly reducing core BUM traffic.

6. Anycast Gateway via IRB

All VTEPs share the same gateway IP and MAC on an **IRB** interface, allowing seamless host mobility across the fabric.

7. EVPN Practice Question

Q1: What is the primary purpose of EVPN Type 3 route advertisements?
A. Carry MAC and IP address mapping
B. Signal multihoming Ethernet segment availability
C. Propagate IP prefixes in Layer 3 EVPN
D. Enable efficient replication of broadcast and multicast traffic across VXLAN

Q2: What component of VXLAN is responsible for identifying a specific Layer 2 segment?
A. Ethernet Segment Identifier (ESI)
B. VTEP Router ID
C. VXLAN Network Identifier (VNI)
D. BGP Route Distinguisher

Q3: What is the role of a VTEP in an EVPN-VXLAN deployment?
A. Encapsulate and decapsulate Ethernet frames into VXLAN packets
B. Perform BGP route reflection
C. Filter multicast routes
D. Control Layer 1 hardware forwarding

Q4: Which EVPN route type is used to advertise MAC/IP bindings learned from a local CE device?
A. Type 2
B. Type 4
C. Type 3
D. Type 5

Q5: What is the main function of the Designated Forwarder (DF) in an EVPN multihoming environment?
A. Synchronize VNI to VLAN mappings
B. Assign the bridge domain identifier
C. Determine loopback IPs for BGP sessions
D. Ensure only one VTEP forwards BUM traffic on a segment

Q6: Which route type in EVPN is primarily used to identify Ethernet Segments in multihomed environments?
A. Type 2
B. Type 1

C. Type 3
D. Type 5

Q7: What problem does ARP suppression in EVPN primarily solve?
A. Authentication of BGP routes
B. Excessive multicast group formation
C. Reduction of unnecessary broadcast traffic in the fabric
D. IP address assignment for VTEPs

Q8: In an EVPN deployment, what is a valid use case for Route Target (RT)?
A. Loopback IP assignment for VTEPs
B. Defining import/export policies between EVPN instances
C. Assigning MAC addresses to bridge domains
D. Identifying Ethernet segments

Q9: What does Anycast Gateway (IRB interface) achieve in an EVPN-VXLAN architecture?
A. Allows VXLAN tunnels to bypass the underlay network
B. Prevents all broadcast traffic in a segment
C. Ensures hosts use a consistent default gateway across VTEPs
D. Disables BUM replication to remote VTEPs

Q10: Which benefit is most associated with EVPN Type 5 routes?
A. Broadcasting MAC/IP bindings to all VTEPs
B. Preventing loops through DF election
C. Advertising IP prefixes for inter-subnet routing
D. Synchronizing Ethernet Segment Identifiers across VTEPs

---

4. JN0-649 Ethernet Switching and Spanning Tree

1. Ethernet Switching Overview

1.1 Core Concepts

- **MAC Table:** Built via "flood, learn, and forward."
- **VLANs:** Segment broadcast domains.
- **Trunking (802.1Q):** The **Native VLAN** is the single VLAN whose traffic is transmitted **untagged** (Default: VLAN 1).

1.2 Advanced Features

- **Private VLANs:** Includes **Promiscuous** (talks to all), **Isolated** (talks only to Promiscuous), and **Community** ports.
- **Q-in-Q:** Double-tagging for service provider transparency.

2. Spanning Tree Protocols (STP)

2.1 STP Variants

- **RSTP:** Rapid convergence.
- **MSTP:** Groups VLANs into 2-3 instances for CPU efficiency.

2.2 Key Concepts

- **Root Bridge:** Elected based on the **lowest Bridge ID (Priority + MAC address)**.
- **RSTP States:** Legacy "Blocking" and "Listening" are merged into **Discarding**.

2.3 Optimizations

- **BPDU Guard:** Disables a port if a BPDU is received (host ports).

set protocols rstp interface ge-0/0/10 edge
set protocols rstp interface ge-0/0/10 bpdu-guard

3. Ethernet Switching and Spanning Tree Practice Question

Q1: What does a switch do when it receives a frame with a destination MAC address that is not in its MAC address table?
A. Sends an ARP request for the destination
B. Floods it out all ports except the incoming port
C. Drops the frame silently
D. Forwards it only to the uplink port

Q2: What is the maximum number of VLANs supported with the standard 802.1Q tagging?
A. 4096
B. 1024
C. 4094
D. 65535

Q3: In Junos, which command enables RSTP on an interface?
A. set spanning-tree interface ge-0/0/1
B. set protocols rstp interface ge-0/0/1
C. set ethernet-switching rstp interface ge-0/0/1
D. set protocols stp interface ge-0/0/1

Q4: What is the role of a “Designated Port” in Spanning Tree Protocol?
A. It connects to the Root Bridge only

B. It remains in a blocking state to prevent loops
C. It forwards traffic away from the Root Bridge on a segment
D. It receives BPDUs from downstream switches

Q5: Which feature protects the Spanning Tree topology by disabling a port if any BPDU is received?
A. BPDU Guard
B. PortFast
C. Loop Protect
D. Root Guard

Q6: What happens when two switches have the same bridge priority during a root bridge election?
A. The port with the lowest cost is used to break the tie
B. The switch with the lowest MAC address becomes root
C. The switch with the highest MAC address becomes root
D. The election fails and STP disables all ports

Q7: Which STP variant allows multiple VLANs to share a single spanning tree instance?
A. VLAN Spanning Tree Protocol (VSTP)
B. Rapid Spanning Tree Protocol (RSTP)
C. Multiple Spanning Tree Protocol (MSTP)
D. Per VLAN Spanning Tree Plus (PVST+)

Q8: What is the default bridge priority value used in STP?
A. 4096
B. 0
C. 65535
D. 32768

Q9: Which port role in RSTP replaces the “blocking” state from the original STP?
A. Backup Port
B. Root Port
C. Alternate Port
D. Discarding Port

Q10: Which feature allows customer VLAN tags to be encapsulated within a provider VLAN tag?
A. 802.1ad (Q-in-Q) Tunneling
B. VLAN Aggregation
C. Private VLAN
D. STP Filtering

---

5. JN0-649 IP Multicast

1. IP Multicast Overview

1.1 Addressing

- **IPv4:** 224.0.0.0/4. (224.0.0.x is Link-Local and **never forwarded**).
- **IPv6:** FF00::/8.

2. Reverse Path Forwarding (RPF)

The RPF check ensures multicast traffic arrives on the interface used to reach the **source**. If the check fails, the traffic is dropped.

3. Protocols

- **IGMP:** v1 (Join), v2 (Leave), v3 (Source Filtering).
- **MLD:** The IPv6 successor to IGMP, utilizing **ICMPv6**.
- **PIM-SM:** Uses a **Rendezvous Point (RP)**.
- **RP Methods:** Junos supports **Static RP, Auto-RP, and BSR**. BSR is the standards-based dynamic election method.

4. Configurations

set protocols pim interface all sparse-mode
set protocols pim rp static address 1.1.1.1

5. IP Multicast Practice Question

Q1: Which of the following IP address ranges is used for IPv4 administratively scoped multicast traffic?
A. 225.0.0.0 – 231.255.255.255
B. 232.0.0.0 – 232.255.255.255
C. 224.0.0.0 – 224.0.0.255
D. 239.0.0.0 – 239.255.255.255

Q2: Which version of IGMP introduced support for source-specific multicast filtering?
A. IGMPv1
B. IGMPv2
C. IGMPv3
D. IGMP-lite

Q3: What is the purpose of the Reverse Path Forwarding (RPF) check in multicast routing?
A. To find the shortest path from source to receiver
B. To prevent multicast packets from looping
C. To select the highest bandwidth interface
D. To ensure lowest latency delivery

Q4: In PIM Sparse Mode, what is the role of the Rendezvous Point (RP)?
A. It stores group membership databases
B. It replicates multicast traffic to IGMP queriers
C. It serves as a shared tree root for multicast group joins
D. It forwards multicast traffic to non-IP-capable devices

Q5: What is the multicast group-to-source notation used in source-specific multicast?
A. (*, G)
B. (G, S)
C. (S, *)
D. (S, G)

Q6: Which PIM mode does not require a Rendezvous Point (RP)?
A. PIM Dense Mode
B. PIM Sparse Mode
C. PIM Bidir
D. PIM Source-Specific Multicast (SSM)

Q7: Which command would you use to verify current multicast group memberships on a Junos device?
A. show pim neighbors
B. show route protocol multicast
C. show igmp group
D. show pim rp mapping

Q8: Which of the following multicast addresses is considered **link-local** and is not forwarded by routers?
A. 224.1.1.1
B. 239.1.1.1
C. 232.0.0.1
D. 224.0.0.5

Q9: What does a static RPF route configuration help prevent?
A. Misrouted multicast traffic due to asymmetric unicast paths
B. Loopback interface flapping
C. PIM DR election issues
D. BGP neighbor session resets

Q10: In Junos, which command configures a PIM-SM RP address?
A. set interfaces pim rp-address 192.0.2.1
B. set protocols pim ssm range 232.0.0.0/8
C. set protocols igmp rp-address 192.0.2.1
D. set protocols pim rp 192.0.2.1

---

6. JN0-649 IP Telephony Features

1. Key Concepts

- **Voice VLAN:** Isolates voice for QoS.
- **PoE:** 802.3af (15.4W) / 802.3at (30W).
- **PoE Priority: Critical, High, and Low**. Critical devices (phones) remain powered during budget shortages.
- **LLDP-MED:** Unlike generic LLDP, MED auto-negotiates **Voice VLAN and QoS parameters** for endpoints.

2. VoIP Thresholds

- **Latency:** ≤ 150ms | **Jitter:** ≤ 30ms | **Packet Loss:** ≤ 1%.

3. IP Telephony Features Practice Question

Q1: What is the primary purpose of a Voice VLAN in IP Telephony deployments?
A. To provide backup power to IP phones
B. To separate and prioritize voice traffic from data traffic
C. To authenticate voice calls using SIP
D. To enforce encryption policies for RTP streams

Q2: Which IEEE standard defines Power over Ethernet (PoE+) that supports up to 30 watts per port?
A. 802.3at
B. 802.1p
C. 802.1X
D. 802.3u

Q3: What function does LLDP-MED provide in a VoIP-enabled network?
A. Encrypts all SIP signaling traffic
B. Assigns private IP addresses to phones
C. Automatically communicates network policies to VoIP devices
D. Distributes call logs to centralized storage

Q4: Which of the following DSCP values is typically used for voice traffic in a QoS-enabled network?
A. 24 (CS3)
B. 8 (CS1)
C. 34 (AF41)
D. 46 (EF)

Q5: What would be the result of a misconfigured Voice VLAN on an access port?
A. The port will shut down automatically
B. The phone will receive an IP but be unable to register
C. The phone may not join the correct VLAN, causing call quality or connectivity issues
D. The IP phone will receive a duplicate IP address

Q6: Which command in Junos enables PoE on a specific interface?
A. set poe interface ge-0/0/1
B. set protocols poe ge-0/0/1
C. set interfaces ge-0/0/1 poe power-on
D. set interfaces ge-0/0/1 power enable

Q7: Which LLDP-MED attribute allows a switch to advertise the Voice VLAN ID to a connected IP phone?
A. Power Management TLV
B. Device Location TLV
C. End-of-Life TLV
D. Network Policy TLV

Q8: What is the primary purpose of enabling QoS in an IP Telephony environment?
A. To conserve bandwidth by compressing voice packets
B. To limit data access for voice users
C. To prioritize voice traffic and ensure call quality
D. To authenticate SIP users before registration

Q9: Which command would help verify whether LLDP-MED is correctly advertising the Voice VLAN?
A. show vlans
B. show lldp interface
C. show poe interface
D. show interfaces terse

Q10: If an IP phone does not power on when connected to a switch, what is a likely cause?
A. LLDP is disabled on the phone
B. The wrong subnet was configured
C. The switch does not support SIP
D. The switch PoE budget is exhausted

---

7. JN0-649 Interior Gateway Protocols (IGPs)

1. Open Shortest Path First (OSPF)

- **LSAs:** Type 1 (Router), Type 2 (Network/DR), Type 3 (Summary), Type 5 (External).
- **OSPFv3:** Configured **directly on interfaces** and uses **IPsec** for security.
- **Adjacencies:** Must match timers, Area ID, and MTU. **MTU mismatches** commonly prevent neighbors from reaching the 'Full' state.

2. IS-IS

- **L2 Link-State:** Uses CLNS and NSAP addresses.

- **Metrics:** Standard metrics only support values up to 63. **Wide metrics** are required for values > 63K.
- **DIS:** The IS-IS equivalent of OSPF's DR.

3. Redistribution Best Practices

In Junos, redistribution is always policy-controlled. You must define a `policy-statement` and apply it as an `export` to the protocol.

4. Interior Gateway Protocols (IGPs) Practice Question

Q1: Which OSPF LSA type is generated by an ABR to advertise networks from one area to another?
A. Type 5 – External LSA
B. Type 3 – Summary LSA
C. Type 1 – Router LSA
D. Type 2 – Network LSA

Q2: In OSPF, what is the function of the Designated Router (DR) on broadcast networks?
A. It encrypts OSPF hello packets for secure transmission.
B. It generates Type 3 LSAs for inter-area routing.
C. It reduces LSA flooding by acting as the central point of exchange on the segment.
D. It provides backup routes in case of SPF calculation failures.

Q3: Which OSPF area type blocks both Type 3 and Type 5 LSAs?
A. Totally Stubby Area
B. Stub area
C. Backbone area
D. Not-So-Stubby Area (NSSA)

Q4: What is required for two OSPF routers to form an adjacency?
A. Static default routes configured between them
B. Use of point-to-multipoint network type
C. Same MAC address and different router IDs
D. Matching area ID, Hello and Dead intervals, and authentication settings

Q5: Which of the following best describes a Type 5 LSA in OSPF?
A. Summarizes routes between areas
B. Generated by the DR to describe broadcast networks
C. Describes a router’s interfaces and links within an area
D. Advertises external routes imported into the OSPF domain

Q6: In IS-IS, what is the purpose of the System ID within the NSAP address?
A. It uniquely identifies the router within the area
B. It identifies the area to which the router belongs
C. It designates the routing protocol to use
D. It determines whether the router is a DIS

Q7: Which OSPF network type requires manual neighbor configuration and does not support multicast?
A. Broadcast
B. Virtual link
C. Non-Broadcast Multi-Access (NBMA)
D. Point-to-Point

Q8: What metric does IS-IS use by default to calculate the best path?
A. Delay and reliability
B. Cost, with a default value of 10
C. Bandwidth-based metric
D. Administrative distance

Q9: What is the primary difference between OSPF and IS-IS in terms of transport layer usage?
A. OSPF uses IP as its transport, while IS-IS runs directly on Layer 2 (CLNS)
B. Both use GRE as an encapsulation mechanism
C. OSPF runs on Layer 4, while IS-IS runs on Layer 7
D. OSPF uses TCP while IS-IS uses UDP

Q10: Which command enables OSPF MD5 authentication on interface ge-0/0/1 in Junos?
A. set interfaces ge-0/0/1 ospf authentication md5 key 1 secret-key
B. set ospf md5-authentication key 1 ge-0/0/1
C. set protocols ospf interface ge-0/0/1 md5-authentication on
D. set security ospf-authentication md5 ge-0/0/1

---

8. JN0-649 Layer 2 Authentication and Access Control

1. 802.1X (Port-Based Access Control)

Involves the **Supplicant** (device), **Authenticator** (switch), and **RADIUS server**.

2. Unauthorized Traffic Handling

Certification Trap: By default, 802.1X blocks **all** traffic—including **DHCP, ARP, and Ping**—until authentication is successful.

3. Fallback

If authentication fails and no **Guest VLAN** is defined, the port remains unauthorized and blocks all traffic.

4. Configuration

set protocols dot1x authenticator interface ge-0/0/0.0 supplicant multiple
set radius-server 10.0.0.5 secret "juniper123"

5. Layer 2 Authentication and Access Control Practice Question

Q1: In an 802.1X authentication setup, which device acts as the intermediary between the supplicant and the authentication server?
A. Firewall
B. RADIUS server
C. Authenticator (switch or access point)
D. DHCP relay agent

Q2: What happens to a device that fails 802.1X authentication when a Guest VLAN is configured?
A. It retries authentication until success
B. It is permanently blocked from accessing the network
C. It is placed into a VLAN with full access to the network
D. It is assigned to the Guest VLAN with limited access

Q3: Which protocol is used by 802.1X to carry authentication messages between the supplicant and authenticator?
A. RADIUS
B. EAP (Extensible Authentication Protocol)
C. HTTP
D. SNMP

Q4: Which of the following is a key limitation of MAC authentication compared to 802.1X?
A. It does not work with RADIUS
B. It requires a supplicant agent
C. MAC addresses can be spoofed
D. It is more difficult to configure

Q5: Which command in Junos verifies the operational status of 802.1X on an interface?
A. show dot1x interface
B. show access radius-server
C. show log messages
D. show configuration interfaces

Q6: Which of the following describes the function of a RADIUS server in 802.1X authentication?
A. Provides IP addresses to authenticated devices
B. Routes traffic for guest VLAN users
C. Validates user credentials and enforces access policies
D. Stores MAC address tables for access switches

Q7: What is the role of the supplicant in an 802.1X setup?
A. Acts as a backup authentication server
B. Manages VLAN assignments

C. Authorizes guest access through firewall
D. Requests access and provides credentials

Q8: Which RADIUS attribute is used to assign a VLAN to an authenticated user?
A. Class
B. Tunnel-Private-Group-ID
C. NAS-Port-Type
D. Framed-IP-Address

Q9: What is a common reason for devices experiencing intermittent delays during 802.1X authentication?
A. High latency between the switch and RADIUS server
B. Invalid VLAN tagging on the trunk
C. Incorrect duplex settings on the access port
D. Expired DHCP lease on the device

Q10: What is the purpose of configuring a backup RADIUS server in a Layer 2 access control environment?
A. To ensure authentication still works if the primary server fails
B. To provide secondary DHCP for guest VLANs
C. To balance load between routers
D. To handle MAC address filtering

Learning Path & Study Advice

Achieving professional-level proficiency requires a disciplined progression from fundamental networking principles to applied architectural logic. Candidates should begin by reinforcing their understanding of core routing and switching behaviors before transitioning into the nuances of protocol interaction and fabric-based technologies like EVPN. Study efforts should prioritize concept clarity, particularly how different protocols interact within a single converged network. It is recommended to approach preparation through a combination of theoretical review and practical scenario analysis, focusing on how specific configurations impact traffic flow and network stability. Strengthening the ability to diagnose complex configuration misalignments and understanding the underlying logic of protocol behavior is more effective than memorizing command syntax.

Who This PDF Is For

This document is intended for experienced networking professionals, including network engineers, system administrators, and technical consultants responsible for maintaining enterprise-scale infrastructure. It is best suited for individuals who have established a strong foundation in routing and switching and are looking to formalize their expertise at a professional level. Recommended candidates typically possess several years of hands-on experience in production environments and a thorough understanding of multi-protocol networking. This overview serves as a structural guide for anyone seeking to align their professional development with industry-standard enterprise networking competencies.

Call To Action

This document provides an overview of structured learning and certification preparation approaches. For learners seeking clear knowledge organization, guided study planning, and exam-focused practice resources, AAAdemy offers a comprehensive platform to support independent and effective learning.

Explore additional training materials, study guidance, and practice resources at:

https://www.aaademy.com/JNCIP-ENT/JN0-649.html

Online Flashcards (Quizlet):

https://quizlet.com/user/AAAdemy/folders/jn0-649-enterprise-routing-and-switching-professional-jncip?i=6zfa5t&x=1xqt

Attachment : Answers by Knowledge Point

Interior Gateway Protocols (IGPs) Practice Question
A1: Answer: B
Explanation: Type 3 LSAs are Summary LSAs generated by Area Border Routers (ABRs) to advertise network prefixes from one area into another. This facilitates inter-area routing within an OSPF autonomous system.

A2: Answer: C
Explanation: The DR is elected on multi-access networks (like Ethernet) to reduce LSA flooding. All routers form adjacencies with the DR, which then disseminates LSAs to all other routers in that segment.

A3: Answer: A
Explanation: A Totally Stubby Area blocks both external LSAs (Type 5) and inter-area summary LSAs (Type 3), only allowing a default route to be injected, reducing routing table size.

A4: Answer: D
Explanation: For two OSPF routers to become neighbors and form an adjacency, several parameters must match: Area ID, Hello interval, Dead interval, and authentication configuration. Differences in these settings will prevent adjacency.

A5: Answer: D
Explanation: Type 5 LSAs are External LSAs generated by Autonomous System Boundary Routers (ASBRs) to advertise external routes into the OSPF domain, such as those learned from BGP or static configurations.

A6: Answer: A
Explanation: The System ID is a unique identifier for a router within an IS-IS area. It's part of the NSAP address and ensures each router is uniquely recognized in the IS-IS routing domain.

A7: Answer: C
Explanation: NBMA networks, such as Frame Relay, do not support multicast by default. OSPF must be manually configured with neighbors for adjacency formation in NBMA environments.

A8: Answer: B
Explanation: IS-IS uses a simple "cost" metric, which is administratively assigned. The default value is typically 10, and it determines the best path for routing decisions.

A9: Answer: A
Explanation: OSPF is an IP-based protocol (Layer 3) and uses IP for transport. In contrast, IS-IS operates directly on Layer 2 using CLNS (Connectionless Network Service), making it protocol-independent.

A10: Answer: A
Explanation: Junos uses the command `set interfaces ge-0/0/1 ospf authentication md5 key 1 secret-key` to enable MD5 authentication on the specified interface. This secures OSPF communication on that link.

BGP Practice Question
A1: Answer: D
Explanation: The ORIGIN attribute in BGP indicates the source of the route. It can have values IGP (route originated within an AS), EGP (route from EGP protocol), or Incomplete (route redistributed from another source).

A2: Answer: A
Explanation: LOCAL_PREFERENCE is the first attribute considered in the BGP best-path selection process. The route with the highest Local Preference is preferred.

A3: Answer: C
Explanation: Route Reflectors allow iBGP routers to avoid full mesh by reflecting routes to other routers, simplifying scalability in large AS deployments.

A4: Answer: D
Explanation: The NO_EXPORT community tag instructs routers not to advertise the route to eBGP peers outside the local AS.

A5: Answer: A
Explanation: AS-path prepending is used to artificially lengthen the AS_PATH attribute, making a route appear longer and thus less preferred by other BGP routers for inbound traffic.

A6: Answer: C
Explanation: In Junos, the route reflector is configured by setting the cluster ID under the internal BGP group using `set protocols bgp group <name> cluster <id>`.

A7: Answer: D
Explanation: MED (Multi-Exit Discriminator) is used to influence the preferred path into an AS when multiple entry points exist. Lower MED values are preferred.

A8: Answer: B
Explanation: By default, eBGP sessions in most implementations, including Junos, use a TTL of 1 to enforce single-hop connectivity between peers.

A9: Answer: C
Explanation: AS_PATH is a well-known mandatory attribute used in loop prevention and path selection. It records the list of ASes a route has traversed.

A10: Answer: A
Explanation: This policy configuration sets the local preference of the matched route to 200, influencing BGP path selection in favor of this route within the AS.

IP Multicast Practice Question
A1: Answer: D
Explanation: The address range 239.0.0.0 – 239.255.255.255 is reserved for administratively scoped multicast traffic, typically used within private domains.

A2: Answer: C
Explanation: IGMPv3 introduced the ability for hosts to specify source filters, enabling Source-Specific Multicast (SSM) by indicating which source(s) they want to receive traffic from.

A3: Answer: B
Explanation: RPF ensures that multicast packets are accepted only if they arrive on the interface that the router would use to reach the source, which prevents loops and duplicate traffic.

A4: Answer: C
Explanation: In PIM-SM, the RP acts as the root of the shared tree (*,G). Sources initially register with the RP, and receivers join the tree via the RP until shortest path trees (SPT) are built.

A5: Answer: D
Explanation: In source-specific multicast (SSM), the notation (S, G) is used, where S represents the source address and G is the multicast group.

A6: Answer: D
Explanation: PIM-SSM eliminates the need for a Rendezvous Point because receivers know the source address in advance and join source-specific trees directly.

A7: Answer: C
Explanation: The command `show igmp group` displays multicast group memberships learned via IGMP on a router's interfaces.

A8: Answer: D
Explanation: 224.0.0.0/24 is the link-local multicast range. Packets in this range are not forwarded by routers. 224.0.0.5 is used by OSPF to send hello packets to all OSPF routers.

A9: Answer: A
Explanation: A static RPF route can override the default unicast route to ensure multicast RPF checks use the correct source interface, especially in networks with asymmetric routing.

A10: Answer: B
Explanation: In Junos, the RP (Rendezvous Point) for PIM-SM is configured using the command `set protocols pim rp <IP address>`.

Ethernet Switching and Spanning Tree Practice Question
A1: Answer: B
Explanation: When a switch doesn't know the destination MAC address, it floods the frame out of all ports except the one it was received on. This allows the destination to receive the frame and the MAC to be learned.

A2: Answer: C
Explanation: The 802.1Q VLAN tag contains a 12-bit VLAN ID field, which supports up to 4096 VLANs. VLAN IDs 0 and 4095 are reserved, leaving 1–4094 usable.

A3: Answer: B
Explanation: In Junos OS, Rapid Spanning Tree Protocol (RSTP) is enabled on an interface with the command `set protocols rstp interface <interface-name>`.

A4: Answer: C
Explanation: A Designated Port is the forwarding port on a segment that is responsible for sending traffic away from the Root Bridge toward other switches.

A5: Answer: A
Explanation: BPDU Guard disables a port if it receives a BPDU, which helps prevent rogue switches or misconfigured devices from affecting the spanning tree topology.

A6: Answer: B
Explanation: If two switches have the same bridge priority, the one with the lower MAC address wins the election and becomes the Root Bridge.

A7: Answer: C
Explanation: MSTP (Multiple Spanning Tree Protocol) allows grouping of VLANs into instances to reduce the number of STP processes, improving scalability and resource efficiency.

A8: Answer: D
Explanation: The default bridge priority in STP is 32768. Lowering this value increases the chance that the switch becomes the Root Bridge.

A9: Answer: D
Explanation: In RSTP, the “discarding” state replaces both “blocking” and “listening” states from traditional STP, simplifying the state machine.

A10: Answer: A
Explanation: Q-in-Q (802.1ad) Tunneling adds a second VLAN tag, allowing service providers to encapsulate customer VLAN traffic within their own VLAN infrastructure.

Layer 2 Authentication and Access Control Practice Question
A1: Answer: C
Explanation: The authenticator is typically a Layer 2 switch or wireless access point that controls access to the network and relays EAP messages between the supplicant and the authentication server (usually a RADIUS server).

A2: Answer: D
Explanation: If a device fails authentication and a Guest VLAN is configured, it is placed in that VLAN, which typically provides limited access (e.g., to the internet) but no access to internal resources.

A3: Answer: B
Explanation: 802.1X uses EAP to exchange authentication messages between the supplicant and the authenticator. The authenticator encapsulates these messages into RADIUS packets to communicate with the server.

A4: Answer: C
Explanation: MAC authentication is less secure than 802.1X because MAC addresses can be easily spoofed. However, it is useful for devices that cannot run supplicant software.

A5: Answer: A
Explanation: `show dot1x interface` provides detailed status information about 802.1X authentication on a specific interface, including the state and authentication result.

A6: Answer: C
Explanation: The RADIUS server is responsible for validating the credentials provided by the supplicant and for communicating access control decisions back to the authenticator.

A7: Answer: D
Explanation: The supplicant is the client device (e.g., PC, phone) that requests access to the network and submits authentication credentials to the authenticator.

A8: Answer: B
Explanation: Tunnel-Private-Group-ID is the RADIUS attribute used to specify the VLAN ID for dynamic VLAN assignment based on the user or device profile.

A9: Answer: A
Explanation: Delays in 802.1X authentication are often caused by high latency or congestion between the authenticator and the RADIUS server, which slows the authentication exchange.

A10: Answer: A
Explanation: A backup RADIUS server ensures that authentication requests can still be processed in case the primary RADIUS server is unreachable, maintaining access availability.

IP Telephony Features Practice Question
A1: Answer: B
Explanation: Voice VLANs are used to separate voice traffic from regular data traffic, allowing the application of QoS policies to ensure minimal delay, jitter, and packet loss for VoIP.

A2: Answer: A
Explanation: IEEE 802.3at, also known as PoE+, supports up to 30W per port, allowing more powerful devices like video phones to be powered over Ethernet.

A3: Answer: C
Explanation: LLDP-MED is an extension of LLDP that enables switches to advertise policies like VLAN IDs, QoS settings, and other parameters to VoIP endpoints.

A4: Answer: D
Explanation: DSCP 46 (Expedited Forwarding - EF) is commonly used to mark voice traffic because it ensures low latency and high priority in QoS policies.

A5: Answer: C
Explanation: If a Voice VLAN is not correctly configured, the IP phone may fail to receive the correct VLAN settings and fall into the default VLAN, which may not provide proper QoS or reach the call server.

A6: Answer: A
Explanation: The correct command to enable PoE on an interface in Junos is `set poe interface <interface-name>`.

A7: Answer: D
Explanation: The Network Policy TLV (Type-Length-Value) is used in LLDP-MED to advertise VLAN ID, priority, and DSCP values to media devices such as IP phones.

A8: Answer: C
Explanation: QoS ensures voice traffic is prioritized over other types, reducing latency, jitter, and packet loss, thereby maintaining call quality during congestion.

A9: Answer: B
Explanation: `show lldp interface` displays the LLDP and LLDP-MED advertisement status on an interface, including VLAN and QoS policies being sent to the device.

A10: Answer: D
Explanation: If the total PoE budget of a switch is used up, additional devices may not receive power. This can be verified using `show poe controller` or similar commands.

Class of service (CoS) Practice Question
A1: Answer: C
Explanation: The DSCP field is a 6-bit value in the IP header used to mark and classify packets into different traffic classes for CoS/QoS treatment.

A2: Answer: C
Explanation: Shaping buffers and delays excess traffic instead of dropping it, allowing it to be sent later at a controlled rate. It helps avoid burst-induced congestion.

A3: Answer: B
Explanation: Strict Priority gives absolute preference to high-priority queues, while WRR allows fair distribution of bandwidth based on configured weights.

A4: Answer: A
Explanation: ACL-based classification allows traffic to be classified based on source/destination IP, MAC addresses, port numbers, or protocol types.

A5: Answer: A
Explanation: A scheduler determines how each forwarding class is treated when traffic exits an interface. It defines the priority and rate for traffic queues.

A6: Answer: B
Explanation: Policing enforces rate limits by dropping or remarking packets that exceed configured thresholds, unlike shaping, which buffers the traffic.

A7: Answer: D
Explanation: DSCP operates at Layer 3 and can be preserved across routers, making it more versatile than 802.1p, which is Layer 2 and only valid on a single segment.

A8: Answer: C
Explanation: Scheduler maps are used to bind forwarding classes to their respective schedulers, determining how different traffic types are treated on output.

A9: Answer: A
Explanation: Placing voice traffic in a low-priority queue during congestion will delay its transmission, resulting in latency and poor call quality.

A10: Answer: A
Explanation: The `show interfaces queue` command provides visibility into the CoS queue statistics, including packet counts, drops, and usage per queue.

EVPN Practice Question
A1: Answer: D
Explanation: Type 3 EVPN routes are used for Inclusive Multicast Ethernet Tag (IMET) advertisements. They support BUM (Broadcast, Unknown Unicast, and Multicast) traffic delivery by enabling efficient multicast replication across the EVPN fabric.

A2: Answer: C
Explanation: The VXLAN Network Identifier (VNI) is a 24-bit field used to identify and separate Layer 2 segments in a VXLAN-based overlay network.

A3: Answer: A
Explanation: A VXLAN Tunnel Endpoint (VTEP) encapsulates Layer 2 Ethernet frames into VXLAN over UDP and also decapsulates them on the receiving side.

A4: Answer: A
Explanation: Type 2 routes are used to carry MAC address and optional IP information, allowing remote VTEPs to learn and reach hosts connected to another site.

A5: Answer: D
Explanation: In EVPN multihoming, the DF is elected to forward BUM (Broadcast, Unknown Unicast, and Multicast) traffic to prevent loops caused by multiple VTEPs forwarding simultaneously.

A6: Answer: B
Explanation: Type 1 routes advertise Ethernet Auto-Discovery (EAD) information, allowing VTEPs to identify which Ethernet segments they share, which is critical in multihoming scenarios.

A7: Answer: C
Explanation: ARP suppression allows a VTEP to respond to ARP requests on behalf of remote endpoints, minimizing the need to flood broadcast ARP traffic across the VXLAN fabric.

A8: Answer: B
Explanation: Route Targets (RTs) are BGP extended community attributes used to control which routes are imported or exported between EVPN routing instances, facilitating multi-tenant segmentation.

A9: Answer: C
Explanation: An Anycast Gateway allows multiple VTEPs to present the same MAC and IP address for a default gateway, enabling optimal local routing for connected hosts.

A10: Answer: C
Explanation: Type 5 routes are used in EVPN to advertise IP prefixes, which enables L3 routing services across EVPN instances — especially useful for L3VPN-like behavior in data centers.