DUMPSBOSS.

Cisco Certified Support Technician (CCST) NetworkingExam

Cisco CCST-Networking

Version Demo

Total Demo Questions: 6

Total Premium Questions: 65

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Network Fundamentals	23
Topic 2, Network Access	9
Topic 3, IP Connectivity	16
Topic 4, IP Services	5
Topic 5, Security Fundamentals	11
Topic 6, Mix Questions	1
Total	65

QUESTION NO: 1

A help desk technician receives the four trouble tickets listed below. Which ticket should receive the highest priority and be addressed first?

A. Ticket 1: A user requests relocation of a printer to a different network jack in the same office. The jack must be patched and made active.

B. Ticket 2: An online webinar is taking place in the conference room. The video conferencing equipment lost internet access.

C. Ticket 3: A user reports that response time for a cloud-based application is slower than usual.

D. Ticket 4: Two users report that wireless access in the cafeteria has been down for the last hour.

ANSWER: B

Explanation:

“Ticket 2: An online webinar is taking place in the conference room. The video conferencing equipment lost internet access.” should receive the highest priority because it is an active, time-sensitive service interruption affecting a live business activity. The webinar is already underway, so loss of connectivity immediately prevents participants from communicating and can disrupt a meeting involving multiple attendees, including remote users. Help desk triage normally weighs both impact and urgency: this incident has high urgency because its resolution window is limited to the duration of the live event, and it has potentially broad impact because a conference-room collaboration service supports more than one person. Addressing the connectivity failure promptly can restore the service while the event is still occurring and minimize lost productivity, missed communications, and possible business or customer impact. Cisco’s support processes similarly use severity and business impact to prioritize incidents, with critical outages and major operational disruption receiving expedited attention. See Cisco’s Technical Assistance Center support information and its high-availability guidance for the importance of quickly restoring services that affect business operations.

QUESTION NO: 2 - (SIMULATION)

Move each protocol from the list on the left to its correct example on the right.

ANSWER: See the explanation for the answer

Explanation:

Match the protocols to the examples as follows:

DHCP → Assign the reserved IP address `10.10.10.200` to a web server at your company.
DNS → Perform a query to translate `companypro.net` to an IP address.
ICMP → Perform a ping to ensure that a server is responding to network connections.

DHCP provides IP address assignments (including reservations), DNS resolves names to IP addresses, and ping uses ICMP echo messages to test reachability.

QUESTION NO: 3 - (SIMULATION)

For each statement about bandwidth and throughput, select True or False.

Note: You will receive partial credit for each correct selection.

ANSWER: See the explanation for the answer

Explanation:

Selections:

Statement 1: True — Low bandwidth can cause congestion and queuing delays, increasing latency.
Statement 2: False — Latency does not reduce the link's available bandwidth; it can reduce effective performance/throughput.
Statement 3: True — Reducing latency can improve effective throughput, especially for protocols and applications affected by round-trip delay.

QUESTION NO: 4

Which two IPv6 addresses are link-local addresses? (Choose 2.)

A. fe80::25a:9cff:fe12:3456

B. febf::1

C. fd00::10

D. 2001:db8:20::1

E. ff02::1

ANSWER: A B

Explanation:

fe80::25a:9cff:fe12:3456 and **febf::1** are link-local IPv6 addresses. IPv6 link-local unicast addresses use the prefix `fe80::/10`, which includes addresses beginning with values from `fe80` through `febf`.

Link-local addresses are valid only on the local network segment and are commonly used for neighbor discovery and communication with the local default gateway. Addresses beginning with `fd` are unique local addresses, `2001:db8` is a documentation prefix, and addresses beginning with `ff` are multicast addresses.

QUESTION NO: 5

A support technician examines the front panel of a Cisco switch and sees 4 Ethernet cables connected in the first four ports. Ports 1, 2, and 3 have a green

LED. Port 4 has a blinking green light.

What is the state of the Port 4?

A. Link is up with cable malfunctions.

B. Link is up and not stable.

C. Link is up and active.

D. Link is up and there is no activity.

ANSWER: C

Explanation:

Link is up and active. A blinking green port-status LED indicates that the switch has successfully established an Ethernet link on that interface and that traffic is currently being transmitted or received. The physical connection is therefore operational, and the intermittent flashing represents frame activity over the link rather than merely the presence of a connected cable.

This LED behavior is useful during initial troubleshooting. It lets a support technician quickly distinguish an active connected device from a connected but idle device without first accessing the switch CLI or management interface. In the scenario, the blinking pattern on Port 4 shows that the attached endpoint is communicating through the switch. Exact LED behavior can differ slightly among Cisco switch families and according to the selected LED mode, so technicians should confirm the

model-specific hardware guide when working with a particular platform. However, in the standard port-status context used by this question, flashing green represents an operational link with network activity.

Cisco provides LED-status information in its Ethernet switch troubleshooting documentation and in the applicable Cisco switch installation guides.

QUESTION NO: 6

A 100 Mb/s Ethernet connection between a switch and an endpoint remains up, but users report very slow transfers. The switch interface shows an increasing number of late collisions and FCS errors. The endpoint is configured for half duplex, while the switch interface is configured for full duplex.

Which two statements explain the issue? (Choose 2.)

A. The link has a duplex mismatch.

B. The late collisions are consistent with a duplex mismatch.

C. The endpoint cannot reach its DNS server.

D. The switch is forwarding traffic between different VLANs.

E. The default gateway address is outside the endpoint subnet.

ANSWER: A B

Explanation:

The two ends of the Ethernet connection have a duplex mismatch. A half-duplex interface uses carrier sensing and collision detection, whereas a full-duplex interface can transmit and receive simultaneously. When the settings do not match, the link can remain operational while experiencing poor performance and frame errors.

Late collisions and FCS errors are common indicators of this condition. The link should be configured with matching speed and duplex settings, or both sides should use compatible auto-negotiation. A DNS or default-gateway issue would not produce physical-interface collision and FCS counters.