350-401$^{\text{Q\&As}}$

Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) & CCIE Enterprise Infrastructure & CCIE Enterprise Wireless

Pass Cisco 350-401 Exam with 100% Guarantee

QUESTION 1

How does QoS traffic shaping alleviate network congestion?

A. It drops packets when traffic exceeds a certain bitrate.

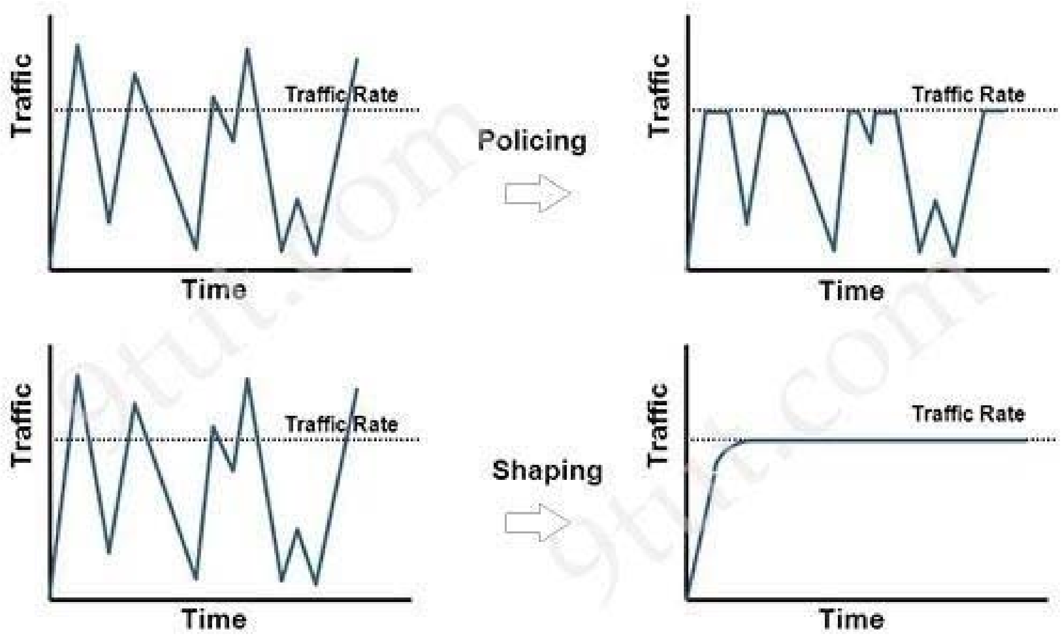
B. It buffers and queues packets above the committed rate.

C. It fragments large packets and queues them for delivery.

D. It drops packets randomly from lower priority queues.

Correct Answer: B

Traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time. The result of traffic shaping is a smoothed packet output rate.



Reference: https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html

QUESTION 2

Which component of the Cisco Cyber Threat Defense solution provides user and flow context analysis?

A. Cisco Firepower and FireSIGHT

B. Cisco Stealthwatch system

C. Advanced Malware Protection

D. Cisco Web Security Appliance

Correct Answer: B

The goal of the Cyber Threat Defense solution is to introduce a design and architecture that can help facilitate the discovery, containment, and remediation of threats once they have penetrated into the network interior. Cisco Cyber Threat Defense version 2.0 makes use of several solutions to accomplish its objectives:

* NetFlow and the Lancope StealthWatch System

1.

Broad visibility

2.

User and flow context analysis

3.

Network behavior and anomaly detection

4.

Incident response and network forensics

* Cisco FirePOWER and FireSIGHT

1.

Real-time threat management

2.

Deeper contextual visibility for threats bypassing the perimeters ?URL control

* Advanced Malware Protection (AMP)

1.

Endpoint control with AMP for Endpoints

2.

Malware control with AMP for networks and content

* Content Security Appliances and Services

1.

Cisco Web Security Appliance (WSA) and Cloud Web Security (CWS)

2.

Dynamic threat control for web traffic

3.

Outbound URL analysis and data transfer controls

4.

Detection of suspicious web activity

5.

Cisco Email Security Appliance (ESA)

6.

Dynamic threat control for email traffic

7.

Detection of suspicious email activity

* Cisco Identity Services Engine (ISE)

1.

User and device identity integration with Lancope StealthWatch

2.

Remediation policy actions using pxGrid

Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

QUESTION 3

Which router is elected the IGMP Querier when more than one router is in the same LAN segment?

A. The router with the shortest uptime

B. The router with the lowest IP address

C. The router with the highest IP address

D. The router with the longest uptime

Correct Answer: B

Query messages are used to elect the IGMP querier as follows: 1. When IGMPv2 devices start, they each multicast a general query message to the all-systems group address of 224.0.0.1 with their interface address in the source IP address

field of the message. 2. When an IGMPv2 device receives a general query message, the device compares the source IP address in the message with its own interface address. The device with the lowest IP address on the subnet is elected

the IGMP querier. 3. All devices (excluding the querier) start the query timer, which is reset whenever a general query message is received from the IGMP querier. If the query timer expires, it is assumed that the IGMP querier has gone down,

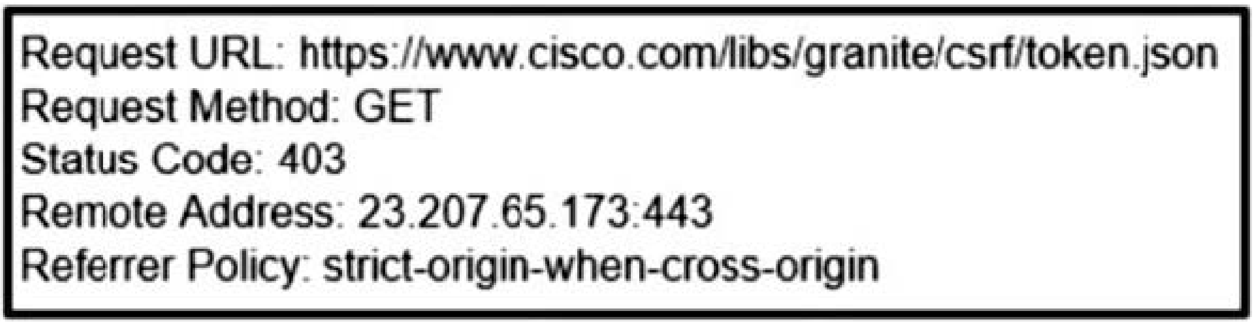
and the election process is performed again to elect a new IGMP querier.

Reference:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-2_2_e/multicast/configuration_guide/b_mc_1522e_3750x_3560x_cg/b_ipmc_3750x_3560x_chapte r_01000.html

QUESTION 4

Refer to the exhibit. Why was the response code generated?



Request URL: https://www.cisco.com/libs/granite/csrf/token.json
Request Method: GET
Status Code: 403
Remote Address: 23.207.65.173:443
Referrer Policy: strict-origin-when-cross-origin

A. The resource was unreachable.

B. Access was denied based on the user permissions.

C. Access was denied based on the credentials.

D. The resource is no longer available on the server.

Correct Answer: B

401 = Unauthorized (Bad credentials)

403 = Forbidden (Service refused, for insufficient permissions)

QUESTION 5

Which access control feature does MAB provide?

A. user access based on IP address

B. allows devices to bypass authenticate*

C. network access based on the physical address of a device

D. simultaneous user and device authentication

Correct Answer: C