600-210Q&As

Implementing Cisco Service Provider Mobility UMTS Networks

Pass Cisco 600-210 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/600-210.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which version of GTP supports piggybacking of GTP messages?

A. GTPv0

B. Gn-prime

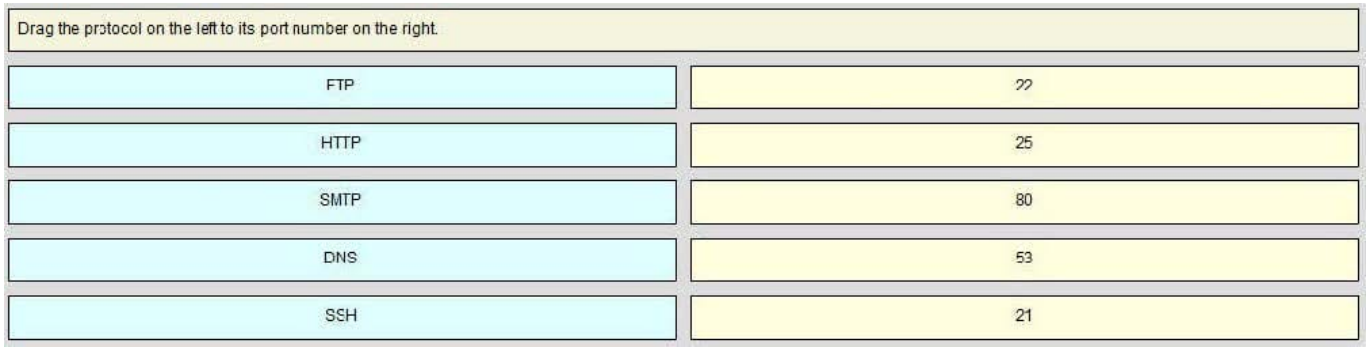
C. GTPv1

D. GTPv2

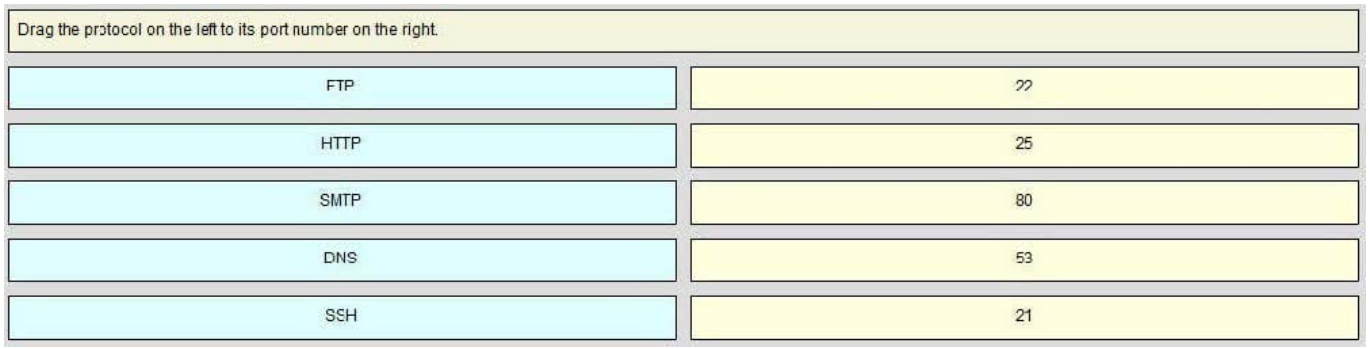
E. GTPv1-prime

Correct Answer: D

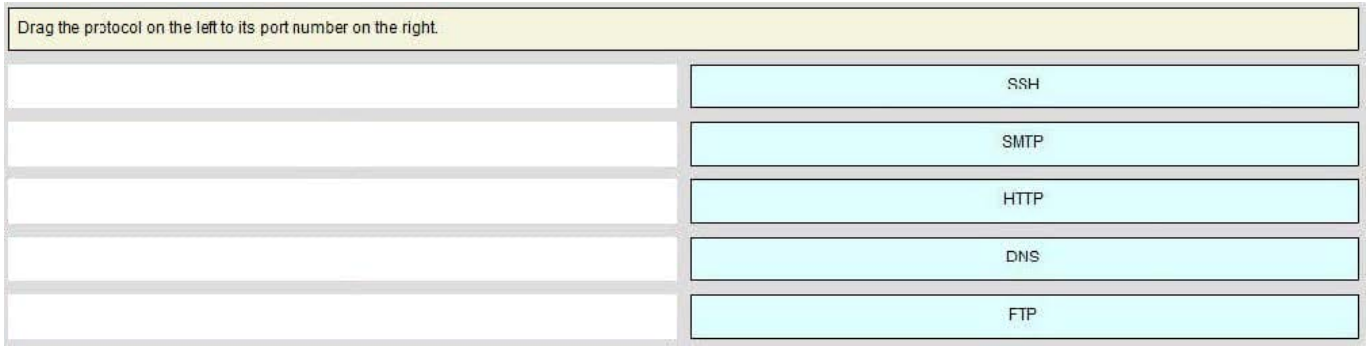
QUESTION 2



Select and Place:



Correct Answer:



QUESTION 3

Which option lists the contents of the flow label in a GTPv0 header?

A. IMSI and NSAPI

B. MSISDN and NSAPI

C. IMEI and NSAPI

D. IMSI and Transaction Identifier

E. IMEI and Transaction Identifier

Correct Answer: A

QUESTION 4

Which option describes how DNS snooping is used on the Cisco ASR 5000?

A. DNS snooping allows the Cisco ASR 5000 to snoop DNS query packets and compare against known DNS responses. If a match is found, the Cisco ASR 5000 replies to the query itself instead of forwarding the query to the destination DNS server.

B. DNS snooping allows the Cisco ASR 5000 to detect if a DNS response sent back to a subscriber is valid. If the response is invalid, the Cisco ASR 5000 drops the packet.

C. DNS snooping allows the Cisco ASR 5000 to enable set of dynamic IP rules to be installed based on the response to DNS queries sent by a subscriber that matches a configured domain rule definition. Dynamic IP rules are created for these IP entries within the same rule that has the domain name, which applies the same charging action to these dynamic rules.

D. DNS snooping allows the Cisco ASR 5000 to enable set of dynamic domain rules to be installed based on the response to DNS queries sent by a subscriber that matches a configured domain rule definition. Dynamic domain rules are created for the DNS responses within the same rule that has the domain name, which applies the same charging action to these dynamic rules.

Correct Answer: C

QUESTION 5

Which node is configured with a Network Mode of Operation value of 1 to be able to support combined attach and routing area update procedures?

A. RNC

B. GGSN

C. S4-SGSN

D. SIM

E. HLR

Correct Answer: A

QUESTION 6

During the network-initiated PDP activation procedure, which network entity provides the GGSN the address of the SGSN, which the subscriber is attached to?

A. AAA

B. OCS

C. PCRF

D. HLR

Correct Answer: D

QUESTION 7

Which two services does GPRS support? (Choose two.)

A. MMS

B. SMS

C. Video Calling

D. EMM

E. ESM

Correct Answer: AB

QUESTION 8

Which two options are functions of the Diameter base protocol? (Choose two.)

A. offline billing

B. policy control

C. transporting CDRs

D. streaming

E. retrieving PDP context information

Correct Answer: AB

QUESTION 9

Your company wants to limit bandwidth for Skype traffic. You have been tasked to configure Application Detection and Control using the Cisco ASR 5000 to detect Skype traffic for all subscribers. If Skype traffic is detected, limit the uplink and downlink data rate to 32 kb/s. Which required configuration is needed to complete this task?

A. active-charging service ACS_ACME p2p-detection protocol skype

ruledef skype_detection

p2p protocol = skype

exit

charging-action skype_rate_limit

content-id 1500

flow limit-for-bandwidth direction downlink peak-data-rate 32000 peak-burst- 8000 violate- action

discard

flow limit-for-bandwidth direction uplink peak-data-rate 32000 peak-burst- 8000 violate- action discard

rulebase acme_rulebase

action priority 1000 ruledef skype_detection charging-action skype_rate_limit

B. active-charging service ACS_ACME ruledef skype_detection p2p protocol = skype exit charging-action

skype_rate_limit content-id 1500 flow limit-for-bandwidth direction downlink peak-data-rate 16000 peak-burst- 8000 violate- action discard flow limit-for-bandwidth direction uplink peak-data-rate 16000 peak-burst- 8000 violate- action discard rulebase acme_rulebase action priority 32000 ruledef skype_detection charging-action skype_rate_limit

C. active-charging service ACS_ACME p2p-detection protocol skype ruledef skype_detection p2p protocol = skype flow limit-for-bandwidth direction downlink peak-data-rate 32000 peak-burst- 8000 violate- action discard flow limit-for-bandwidth direction uplink peak-data-rate 32000 peak-burst- 8000 violate- action discard exit rulebase acme_rulebase action priority 1000 ruledef skype_detection

D. active-charging service ACS_ACME p2p-detection protocol skype ruledef skype_detection p2p protocol = skype_traffic exit charging-action skype_rate_limit content-id 1500 flow limit-for-credit direction downlink peak-data-rate 32000 peak-burst- 8000 violate- action discard flow limit-for-credit direction uplink peak-data-rate 32000 peak-burst-8000 violate-action discard rulebase acme_rulebase action priority 1000 ruledef skype_detection charging-action skype_rate_limit

Correct Answer: A

QUESTION 10

Drag and arrange the steps on the left in the correct order on the right that indicates how DPC+ SSN based routing in SGSN is performed on the Cisco ASR 5000.

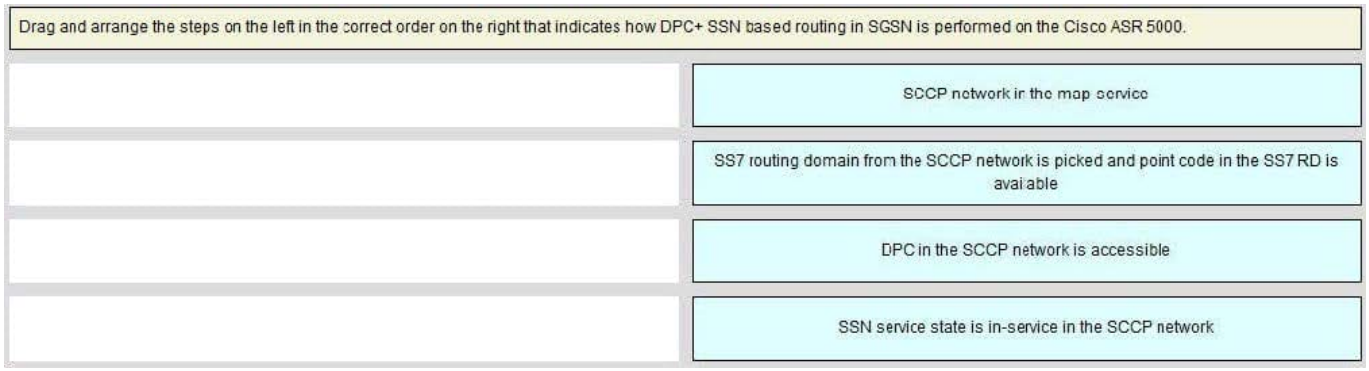
SS7 routing domain from the SCCP network is picked and point code in the SS7 RD is available	First
SCCP network in the map-service	Second
SSN service state is in-service in the SCCP network	Third
DPC in the SCCP network is accessible	Fourth

Select and Place:

Drag and arrange the steps on the left in the correct order on the right that indicates how DPC+ SSN based routing in SGSN is performed on the Cisco ASR 5000.

SS7 routing domain from the SCCP network is picked and point code in the SS7 RD is available	First
SCCP network in the map-service	Second
SSN service state is in-service in the SCCP network	Third
DPC in the SCCP network is accessible	Fourth

Correct Answer:



QUESTION 11

Which failure code is sent in the authentication reject message when a UE with USIM fails to receive the AUTN as part of the authentication and ciphering request from the SGSN?

A. GSM authentication unacceptable

B. MAC failure

C. SYNC failure

D. RAND failure

E. UMTS authentication unacceptable

Correct Answer: A

QUESTION 12

In which two ways does SGSN detect and know when GGSN has restarted? (Choose two.)

A. change in recovery value in echo response

B. change in recovery value in PDU notification request from GGSN to SGSN

C. change in recovery value in Update PDP Context Request from GGSN to SGSN

D. when the sequence number in a response message is different from that of the request message

E. when the TEID value in response in GTP header is different from that of the request message

Correct Answer: AC

QUESTION 13

Which option describes how a PDN connection context is identified at the PGW?

A. IMSI and EPS bearer ID

B. IMSI, EPS bearer ID, and interface type

C. IMSI, QoS, and EPS bearer ID

D. MSISDN, QoS, and interface type

Correct Answer: B

QUESTION 14

Which two options describe two reasons for deploying MPLS on GGSN? (Choose two.)

A. Ensure faster routing.

B. Replace RIP.

C. Allow overlapping IP addressing in different APNs.

D. Segregate corporate APN traffic.

E. Replace GRE tunnels.

Correct Answer: CD

QUESTION 15

Which description of a smurf attack is true?

A. A smurf attack is an attack in which small TCP packets are sent toward a server from thousands of subscribers, which causes the server network buffer to overflow and drop packets and results in a denial of service.

B. A smurf attack is an attack in which the attacker sends ICMP echo request packets using a spoofed source IP address destined to remote network broadcast addresses, which results in all recipients replying back to the spoofed source IP address in an attempt to cause a denial of service to the targeted spoofed IP address.

C. A smurf attack is an attack in which the attacker sends UDP echo packets using a spoofed source IP address destined to remote network broadcast addresses, which results in all recipients replying back to the spoofed source IP address in an attempt to cause a denial of service to the targeted spoofed IP address.

D. A smurf attack is an attack in which the attacker attempts to change the TCP MSS value to a small value for all TCP flows destined to the target device, which results in many small packets having to be processed by the target, which causes buffer overflows and denial of service.

Correct Answer: B