



- A. RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 22  
RouterB(config)# access-list 101 permit any any  
RouterB(config)# int g0/0/2  
RouterB(config-if)# ip access-group 101 in
- B. RouterB(config)# access-list 101 deny icmp 10.100.2.0 0.0.0.248 10.100.2.0 0.0.0.248  
RouterB(config)# access-list 101 permit any any  
RouterB(config)# int g0/0/2  
RouterB(config-if)# ip access-group 101 in
- C. RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 23  
RouterB(config)# access-list 101 permit any any  
RouterB(config)# int g0/0/2  
RouterB(config-if)# ip access-group 101 in
- D. RouterB(config)# access-list 101 permit tcp 10.100.2.0 0.0.0.252 10.100.3.0 0.0.0.255  
RouterB(config)# int g0/0/2  
RouterB(config-if)# ip access-group 101 in

**Correct Answer: C**

#### QUESTION 187

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

- A. Cisco Firepower and FireSIGHT
- B. Cisco Stealth watch system
- C. Advanced Malware Protection
- D. Cisco Web Security Appliance

**Correct Answer: B**

#### QUESTION 188

Which IPv4 packet field carries the QoS IP classification marking?

- A. ID
- B. TTL

- C. FCS
- D. ToS

**Correct Answer: D**

**Explanation:**

The classification is carried in the IP packet header, using 6 bits from the deprecated IP type of service (ToS) field to carry the classification (class) information. Classification can also be carried in the Layer 2 frame.

**QUESTION 189**

AN engineer is implementing MPLS OAM to monitor traffic within the MPLS domain. Which action must the engineer perform to prevent from being forwarded beyond the service provider domain when the LSP is down?

- A. Disable IP redirects only on outbound interfaces
- B. Implement the destination address for the LSP echo request packet in the 127.x.y.z/8 network
- C. Disable IP redirects on all ingress interfaces
- D. Configure a private IP address as the destination address of the headend router of Cisco MPLS TE.

**Correct Answer: C**

**QUESTION 190**

Refer to the exhibit. An administrator troubleshoots intermittent connectivity from internal hosts to an external public server. Some internal hosts can connect to the server while others receive an ICMP Host Unreachable message and these hosts change over time. What is the cause of this issue?

```
!Jun 28 19:14:59.462: %IPNAT-4-ADDR_ALLOC_FAILURE: Address allocation failed for 10.0.3.1,
pool NAT might be exhausted
!Jun 28 19:14:59.462: NAT: translation failed (A), dropping packet s=10.0.3.1 d=203.0.113.8

CPE# show ip nat translation
Pro Inside global   Inside local   Outside local   Outside global
---
tcp 198.51.100.5    10.0.1.1       203.0.113.8:23 203.0.113.8:23
---
tcp 198.51.100.5    10.0.1.1       203.0.113.8:23 203.0.113.8:23
---
tcp 198.51.100.6    10.0.2.1       203.0.113.8:23 203.0.113.8:23
---
tcp 198.51.100.6    10.0.2.1       203.0.113.8:23 203.0.113.8:23
---

CPE# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet0/1
Hits: 234 Misses: 0
CEF Translated packets: 234, CEF Punted packets: 7
Expired translations: 2
Dynamic mappings:
-- Inside Source
id: 11 access-list NAT pool NAT-relocat-4
pool NAT-id 1, netmask 255.255.255.0
start 198.51.100.5 end 198.51.100.6
type generic, total addresses 2, allocated 2 (100%), misses 7
nat-lsm statistics:
max entry, max allowed 0, used 0, missed 0
Outside global interfaces count: 1
```

- A. The translator does not use address overloading
- B. The NAT ACL does not match all internal hosts
- C. The NAT ACL and NAT pool share the same name
- D. The NAT pool netmask is excessively wide

**Correct Answer: B**

### QUESTION 191

Refer to the exhibit. An engineer must configure HSRP for VLAN 1000 on SW2. The secondary switch must immediately take over the role of active router if the interlink with the primary switch fails. Which command set completes this task?

```
SW2(config)# track 1000 interface gigabitEthernet 0/0 line-protocol
SW2(config-track)# exit
SW2(config)# interface vlan 1000
SW2(config-if)# ip address 10.23.87.3 255.255.255.0
```

- A. SW2(config-if)# standby version 2  
SW2(config-if)# standby 1000 ip 10.23.87.1  
SW2(config-if)# standby 1000 priority 95  
SW2(config-if)# standby 1000 preempt  
SW2(config-if)# standby 1000 track gigabitEthernet0/0
- B. SW2(config-if)# standby 1000 ip 10.23.87.1  
SW2(config-if)# standby 1000 priority 95  
SW2(config-if)# standby 1000 preempt  
SW2(config-if)# standby 1000 track 1000
- C. SW2(config-if)# standby version 2  
SW2(config-if)# standby 1000 ip 10.23.87.1  
SW2(config-if)# standby 1000 priority 95  
SW2(config-if)# standby 1000 preempt  
SW2(config-if)# standby 1000 track 1000
- D. SW2(config-if)# standby version 2  
SW2(config-if)# standby 1000 ip 10.23.87.1  
SW2(config-if)# standby 1000 priority 95  
SW2(config-if)# standby 1000 track 1000

**Correct Answer: C**

### QUESTION 192

Refer to the exhibit. Which command set must be added to permit and log all traffic that comes from 172.20.10.1 in interface GigabitEthernet0/1 without impacting the functionality of the access list?

```
Router#show access-lists
Extended IP access list 100
10 permit ip 192.168.0.0 0.0.255.255 any
20 permit ip 172.16.0.0 0.0.15.255 any
```

- Router(config)#no access-list 100 permit ip 172.16.0.0 0.0.15.255 any  
Router(config)#access-list 100 permit ip 172.16.0.0 0.0.15.255 any log  
Router(config)#interface GigabitEthernet0/1  
Router(config-if)#access-group 100 in
- Router(config)#access-list 100 seq 5 permit ip host 172.20.10.1 any log  
Router(config)#interface GigabitEthernet0/1  
Router(config-if)#access-group 100 in
- Router(config)#ip access-list extended 100  
Router(config-ext-nacl)#5 permit ip 172.20.10.0 0.0.0.255 any log  
Router(config)#interface GigabitEthernet0/1  
Router(config-if)#access-group 100 in
- Router(config)#access-list 100 permit ip host 172.20.10.1 any log  
Router(config)#interface GigabitEthernet0/1  
Router(config-if)#access-group 100 in

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Correct Answer: D**

**QUESTION 193**

In a Cisco Catalyst switch equipped with two supervisor modules an administrator must temporarily remove the active supervisor from the chassis to perform hardware maintenance on it. Which mechanism ensure that the active supervisor removal is not disruptive to the network operation?

- A. NSF/NSR
- B. SSO
- C. HSRP
- D. VRRP

**Correct Answer: B**

**QUESTION 194**

Why would an engineer use YANG?

- A. to transport data between a controller and a network device
- B. to access data using SNMP
- C. to model data for NETCONF
- D. to translate JSON into an equivalent XML syntax

**Correct Answer: C**

**QUESTION 195**

What is the calculation that is used to measure the radiated power of a signal after it has gone through the radio, antenna cable, and antenna?

- A. EIRP
- B. mW
- C. dBm
- D. dBi

**Correct Answer: A**

**QUESTION 196**

Which two mechanisms are available to secure NTP? (Choose two.)

- A. IP prefix list-based
- B. IPsec
- C. TACACS-based authentication
- D. IP access list-based
- E. Encrypted authentication

**Correct Answer: DE**

**QUESTION 197**

Which benefit is realized by implementing SSO?

[Download Full Version 350-401 Exam Dumps \(Updated in Feb/2023\)](#)

- A. IP first-hop redundancy
- B. communication between different nodes for cluster setup
- C. physical link redundancy
- D. minimal network downtime following an RP switchover

**Correct Answer: B**

**QUESTION 198**

Refer to the exhibit. What step resolves the authentication issue?

The first screenshot shows the output of the 'show control connections' command. It lists several connections with their public IP, private IP, local color, proxy state, and uptime. The connections are:

LINE	PROXY	PROXYPUBLIC IP	AM	AM PORT	PRIVATE IP	LOCAL COLOR	PROXY STATE	UPTIME	PROXY ID
vsmart	dtls	4.4.4.70	100	1	192.168.100.80	12446 default	No	up	
12446		10.10.20.70							
0:02:24:09		0							
vbond	dtls	0.0.0.0	0	0	192.168.100.81	12346 default	-	up	
12346		10.10.20.80							
0:02:24:10		0							
vmanage	dtls	4.4.4.90	100	0	192.168.100.82	12446 default			
12446		10.10.20.90							

The second screenshot shows a curl command being executed: curl -X POST https://192.168.100.80:8443/\_security/check. The output shows an error: 'Could not get any response'. Below the error, there are suggestions for why this might have happened, such as 'The server couldn't send a response' or 'Self-signed SSL certificates are being blocked'.

- A. use basic authentication
- B. change the port to 12446
- C. target 192 168 100 82 in the URI
- D. restart the vsmart host

**Correct Answer: C**

**Explanation:**

The first figure is the output of the "show control connections" command. From this figure we learned that the 192.168.100.82 so we need to connect to this IP address (not 192.168.100.80).

**QUESTION 199**

**DRAG DROP**

Drag and drop the virtual components from the left onto their descriptions on the right.

vNIC	zip file connecting a virtual machine configuration file and a virtual disk
OVA	file containing a virtual machine disk drive
VMDK	configuration file containing settings for a virtual machine such as guest OS
VIX	component of a virtual machine responsible for sending packets to the hypervisor

**Correct Answer:**