

# 100-105<sup>Q&As</sup>

Interconnecting Cisco Networking Devices Part 1 (ICND1)

## Pass Cisco 100-105 Exam with 100% Guarantee

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

https://www.geekcert.com/100-105.html

100% Passing Guarantee 100% Money Back Assurance

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

Instant Download After Purchase

100% Money Back Guarantee

- 😳 365 Days Free Update
- 800,000+ Satisfied Customers





#### **QUESTION 1**

Which IPv4 address type can reach each node on a network?

- A. unicast
- B. anycast
- C. broadcast
- D. multicast

Correct Answer: C

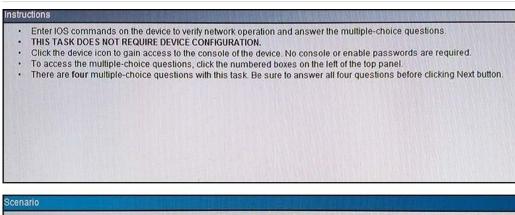
#### **QUESTION 2**



### https://www.geekcert.com/100-105.html

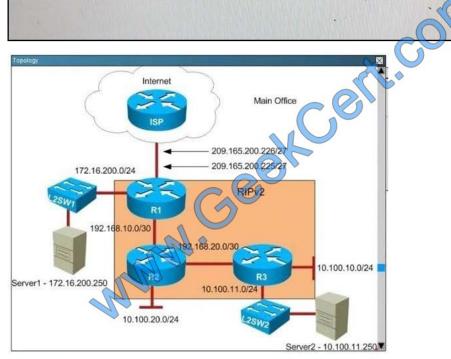
2021 Latest geekcert 100-105 PDF and VCE dumps Download

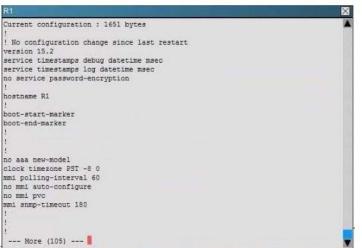
X



You are a junior network engineer for a financial company, and the main office network is experiencing network issues. Troubleshoot the network issues.

Router R1 connects the main office to the Internet, and routers R2 and R3 are internal routers. NAT is enabled on router R1. The routing protocol that is enabled between routers R1, R2, and R3 is RIPv2. R1 sends the default route into RIPv2 for the internal routers to forward Internet traffic to R1. You have console access on R1, R2, and R3 devices. Use only show commands to troubleshoot the issues.







RI	
	-
ip def no ipv6 def	
1	
multilink bundle-name authenticated	
redundancy !	
	-
More (79)	V
R1	×
interface Ethernet0/0 description ***Link to ISP***	
ip address 209.165.200.225 255.255.255.224 ip nat outside	
ip virtual-reassembly in	
interface Ethernet0/1	
<pre>description ***Link to Server1 segment*** ip address 172.16.200.1 255.255.0</pre>	
ip nat inside ip virtual-reassembly in	
interface Ethernet0/2	
description ***Link to R2*** ip address 192.168.10.1 255.255.255.252	
ip access-group R2LANBLOCK in ip nat inside	
ip virtual-reassembly in	
interface Ethernet0/3 no ip address	
ahutdown	
router rip	
version 2	
R1 ip ast inside source list LOCAL interface Ethernet0/0 overload ip route 0.0.0.0 0.0.0.0 209.165.200.226 ip access-list standard R2LANBLOCK deny 10.100.20.0 0.0.0.255 permit any ip access-list extended LOCAL permit ip host 127.0.0.1 any control-plane inte con 0 line con 0 line any 0 	177
ip nat inside source list LOCAL interface Ethernet0/0 overload	
ip route 0.0.0.0 0.0.0.0 209.165.200.226	•
ip access-list standard R2LANBLOCK deny 10.100.20.0 0.0.0.255	
permit any	
ip access-list extended LOCAL permit ip host 127.0.0.1 any	
control-plane	
(Sol)	
- AR	
line con 0	
logging symphronous line aux 0	
More (7)	×
RI	×
ip access-list extended LOCAL	
permit ip host 127.0.0.1 any	
! control-plane	
2 2	
! line con 0	
logging synchronous line aux 0	
line vty 0 4 login	
transport input all	
ntp server 209.165.200.226	
end	
RI#	
R2	$\times$
Building configuration	-
Current configuration : 1243 bytes !	
version 15.2 service timestamps debug datetime msec	
service timestamps log datetime msec no service password-encryption	
l hostname R2	
loot-start-marker	
bost-start-marker bost-end-marker	
: no aaa new-model	
clock timezone PST -8 0 mmi polling-interval 60	
no mmi auto-configure no mmi pvo	
mmi snmp-timeout 180	
1 More (92)	

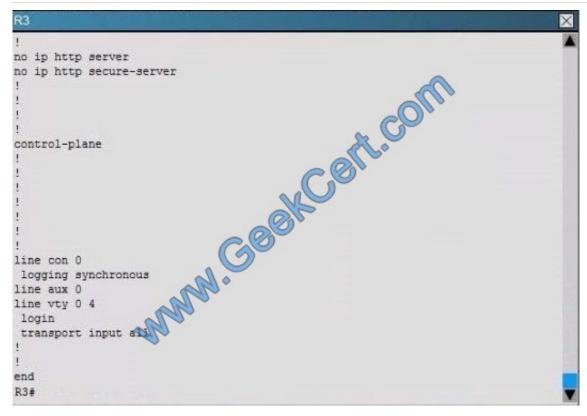


	×
version 15.2 service timestamps debug datetime msec	
service timestamps log datetime msec no service password-encryption	
! hostname R2	
! boot-start-marker	
boot-end-marker	
no aaa new-model clock timezone PST -8 0	
mmi polling-interval 60	
no mmi auto-configure no mmi pvc	
mmi snmp-timeout 180	
1	
1	
R2	X
1 Main 1	
1	
ip dhcp excluded-address 192.168.20.1	
ip dhcp pool DHCPASSIGNR3 network 10.10.10.0 255.255.255.252	
UEUWER 10110110.0 200.200.202	
ip cef no ipv6 cef	
! multilink bundle-name authenticated	
R2#	
R3	×
Lurrent configuration : 1115 bytes	
version 15.2 service timestamps debug datetime msec	
service timestamps log datetime msec no service password-encryption	
hostname R3	
boot-end-marker	
boot-end-marker	
boot-end-marker	
boot-end-marker i aas new-model clock timesone PST -6 0 mmi polling-interval 60	
boot-end-marker in aas new-model clock timesone PST -6 0 min polling-interval 60 no min auto-configure	
boot-end-marker 1 no aas new-model clock timesone PST -8 0 mmi polling-interval 60 no mmi auto-configure no	
boot-end-marker 1 no aas new-model clock timesone PST -6 0 mmi poling-interval 60 no mmi armo-timeour impo mi armo-timeour impo	
boot-end-marker i no aas new-model clock timesone PST -6 0 mmi poling-interval 60 no mmi pvo mmi anup-timeour impo i i	
boot-end-marker 10 aas new-model clock timescoe PST -6 0 mmi poling-interval 60 no smi supc-timeour iso mi smp-timeour iso 10 mmi supc-timeour iso 10 mmi supc-timeo	
R3 Current configuration : 1115 bytes ' version 15.2 service timestamps debug datetime mace service timestamps log datetime mace service timestamps dobug datetime mace service timestamps debug datetime mace service timestamps debug datetime mace bot-end-marker t t no ana new-model clock timestone P3T = 0 mm supportinguity mm supportinguity t t t t t t t t t t t t t	
	Y
	Y
i je cef mo iprof cef	•
t to off	•
: ; ip cef no ipv6 cef	
: ; ip cef no ipv6 cef	
lp cef no ipv6 cef multilink bundle-name authenticated	
lp cef no ipv6 cef multilink bundle-name authenticated	
lp off no ipv6 off f miltillik bundle-pame authenticated	
lp off no ipv6 off f millilik bundle-name authenticated	
lp off no ipv6 off f miltillik bundle-pame authenticated	
lp off no ipv6 off f millilik bundle-name authenticated	
ip oef no ipv6 oef millink bundle-name authenticated redundancy	
ip oef miltilink bundle-mame authenticated redundancy More (60)	
ip oef no ipv6 oef millink bundle-name authenticated redundancy	
<pre>ip cef ip cef imitian bundle-name authenticated i redundancy More (60) R3</pre>	
<pre>p cef no tpr6 cef redundancy More (60) R3</pre>	
<pre>ip oef in ipv6 oef initiality bundle-pame authenticated i redundancy More (60) R3 interface Loopback0 ip address 192.168.250.3 255.255.255 interface Ethernet0/0</pre>	
<pre>ip oef in ipv6 oef initiality bundle-pame authenticated i redundancy  More (60) R3 Interface Loopback0 Ip address 192.168.250.3 255.255.255 Interface Loopback0 Ip address 192.168.250.3 255.255.255.0</pre>	
<pre>ip oef no ipv6 oef miltilink bundle-name authenticated redundancy  More (60) R3 interface Loopback0 ip address 122.168.250.3 255.255.255 ipradress 122.168.250.3 255.255.255 interface Loopback0 ip address 122.168.250.3 255.255.255.0 interface Ethernet0/0 description ***Link to LAX*** interface Ethernet0/1</pre>	
<pre>p cef no tpr6 cef mltllink bundle-name authenticated redundancy  More (60) R3 interface Loopback0 interface Loopback0 interface Loopback0 interface Ecologback0 interface Ecologback0</pre>	
<pre>ip oef in ipv6 oef initial bundle-name authenticated if initial bundle-name auth</pre>	
<pre>ip oef in ipv6 oef imitilink bundle-name authenticated imitil</pre>	
<pre>point of point o</pre>	
<pre>ip off miltilik bundle-name authenticated  More (60) <b>K3</b> interface Loopback0 interface Loopback0 interface Loopback0 interface State 122.168.250.3 255.255.255. interface Ethernet0/0 description **Link to LM*** ip address loubloot.125.255.255.0 interface Ethernet0/1 description **Link to Server12 Segment*** ip address 10.0100.11.255.255.255.0 interface Ethernet0/2 description **Link to Server12 Segment*** ip address 10.100.11.1255.255.255.0 interface Ethernet0/2 description **Link to Server12 Segment*** ip address 10.100.11.1255.255.255.0 interface Ethernet0/3 no ip address</pre>	
<pre>ip off miltilik bundle-name authenticated  More (60) <b>K3</b> Interface Loopback0 interface Loopback0 interface Loopback0 interface States 192.168.250.3 255.255.255.255 interface Ethernet0/0 description **Link to LM*** ip address 10.100.101.255.255.255.0 interface Ethernet0/1 description **Link to Server12 Segment*** ip address 10.100.11.255.255.255.0 interface Ethernet0/2 interface Ethernet0/2 interface Ethernet0/2 interface Ethernet0/2 interface Ethernet0/3 no ip address 10.100.11.255.255.255.0 interface Ethernet0/3 no ip address 10.100.11.255.255.255.0</pre>	
<pre>ip off no ipv6 off miltilink bundle-pame authenticated  More (60) R3 Interface Loopback0 ip address 192.168.250.3 255.255.255.255 interface Lienet0/0 description ***Link to Lä*** ip address 10.100.10.1 255.255.255.0 interface Ethernet0/1 description ***Link to B2*** ip address adop interface Ethernet0/2 description ***Link to B2*** ip address adop interface Ethernet0/3 no ip address shutdown router rip version 2</pre>	Y X A
<pre>ip oef no ipv6 oef milcilink bundle-name authenticated redundancy redundancy interface Loopback0 ip address 192.168.250.3 255.255.255.255 interface Ethernet0/0 description **Link to LAM*** ip address 10.100.10.1 255.255.255.0 interface Ethernet0/1 description **Link to A2*** ip address 10.100.10.1 255.255.255.0 interface Ethernet0/2 description **Link to A2*** ip address 10.100.11.1 255.255.255.0 interface Ethernet0/2 description **Link to Server2 Segment*** ip address 10.100.11.1 255.255.255.0 interface Ethernet0/3 no ip address shutdown router rip</pre>	



X 23 description \*\*\*Link to Server2 Segment\*\*\* ip address 10.100.11.1 255.255.255.0 interface Ethernet0/3 no ip address shutdown router rip version 2 network 10.0.0.0 network 192.168.20.0 network 192.168.250.0 no auto-summary Kcert.com Ŧ ip forward-protocol nd 1 no ip http server no ip http secure-server control-plane 1 ş GO R3 network 192.168.250.0 no auto-summary ip forward-protocol nd no ip http server no ip http secure-server 1 control-plane ţ ! ţ 1 1 t line con 0 logging synchronous line aux 0 line vty 0 4 --- More (5) ----





Why application that are installed on PC\\'s in R2 LAN network 10.100.20.0/24 are unable to communicate with Server1?

A. A standard ACL statement that is configured on R1 is blocking the traffic sourced from Server1 network.

B. A standard ACL statement that is configured on R2 is blocking the traffic sourced from Server1 network.

C. A standard ACL statement that is configured on R2 is blocking the traffic sourced from R2 LAN network.

D. A standard ACL statement that is configured on R1 is blocking the traffic sourced from R2 LAN network.

Correct Answer: B

We should check if we can ping from R1 to Server 1 or not:

R1#ping 172.16.200.250 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.200.250, timeout is 2 seconds: !!!!!

The ping worked well so maybe R1 is good so we should check R2 first. We notice on R2 there is an access-list:



R2# show running-config
<output omitted=""></output>
interface Ethernet0/2
description Link to R1
ip address 192.168.102 255.255.255.252
ip access-group SERVER1BLOCK in
!
<output omitted=""></output>
ip access-list standard SERVERIBLOCK
deny 172.16.200.0 0.0.0.255
permit any

This access-list is applied to E0/2 interface with inbound direction. The purpose of this access-list is to block traffic with source IP address of 172.16.200.0/24 so it will block all traffic sent from Server 1 to us.

#### **QUESTION 3**

You ping a remote device by name from a router, and the router you are using immediately displays a new prompt. What are two possible reasons for the problem? (Choose two.)

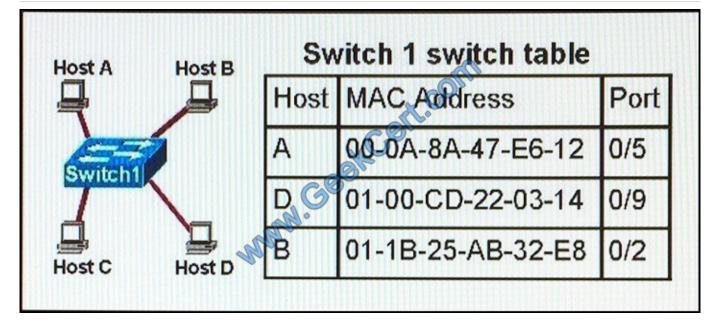
- A. The IP address of the remote device is listed in multiple ip host statements in the router configuration.
- B. The ACL on the router blocked the ping.
- C. The DNS server configuration on the router is missing.
- D. The DNS server is unreachable.
- E. The no ip domain-lookup command is configured on the router.

Correct Answer: CE

**QUESTION 4** 

### https://www.geekcert.com/100-105.html 2021 Latest geekcert 100-105 PDF and VCE dumps Download





Refer to the topology and switching table shown in the graphic. Host B sends a frame to Host C. Which option describes what the switch will do with the frame?

- A. send an ICMP Host Unreachable message to Host B
- B. return the frame to Host B
- C. drop the frame
- D. send the frame out all ports except port 0/2
- E. record the destination MAC address in the switching table and send the frame directly to Host C
- F. send an ARP request for Host C

Correct Answer: D

#### Explanation/Reference:

An Ethernet switch appears to use the same logic as a transparent bridge. However, the internal logic of the switch is optimized for performing the basic function of choosing when to forward and when to filter a frame. Just as with a transparent bridge, the basic logic of a LAN switch is as follows:

- Step 1 A frame is received.
- Step 2 If the destination is a broadcast or multicast, forward on all ports.

Step 3	If the destination is a unicast and the address is not in the address
	table, forward on all ports.

Step 4	If the destination is a unicast and the address is in the address
	table, forward the frame out the associated port, unless the MAC
	address is associated with the incoming port.



### **QUESTION 5**

Which statement is a Cisco best practice for switch port security?

- A. Vacant switch ports must be shut down.
- B. Empty ports must be enabled in VLAN 1.
- C. VLAN 1 must be configured as the native VLAN.
- D. Err-disabled ports must be configured to automatically re-enable.

Correct Answer: A

100-105 VCE Dumps

100-105 Practice Test

100-105 Study Guide



To Read the Whole Q&As, please purchase the Complete Version from Our website.

# Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

### https://www.geekcert.com/allproducts

### **Need Help**

Please provide as much detail as possible so we can best assist you. To update a previously submitted ticket:



#### **One Year Free Update**



Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.



To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days

**Money Back Guarantee** 

from the date of purchase



#### Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Any charges made through this site will appear as Global Simulators Limited. All trademarks are the property of their respective owners. Copyright © geekcert, All Rights Reserved.