



# 351-018<sup>Q&As</sup>

CCIE Security written

## Pass Cisco 351-018 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/351-018.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 three attributes may be configured as part of the Common Tasks panel of an authorization profile in the Cisco ISE solution? (Choose three.)

- A. VLAN
- B. voice VLAN
- C. dACL name
- D. voice domain permission
- E. SGT

Correct Answer: ACD

### QUESTION 2

Refer to the exhibit.

1 0.000000 10.0.0.2 192.168.232.129 TCP 1024 > ftp [SYN Seq=4288200122 Win=16384 Len=0 MSS=138...

Frame 1 [62 bytes on wire (496 bits), 62 bytes captured (500 bits) on interface 0]

Ethernet II, Src: Intel\_cb:7d:01 (00:aa:00:cb:7d:01), Dst: Vmware\_9f:2e:84 (00:0c:29:9f:2e:84)

Internet Protocol, Src: 10.0.0.2 (10.0.0.2), Dst: 192.168.232.129 (192.168.232.129)

Transmission Control Protocol, Src Port: 1024 (1024), Dst Port: ftp (21), Seq: 4288200122, Len: 0

Source port: 1024 (1024)

Destination port: ftp (21)

[Stream index: 0]

Sequence number: 4288200122

Header length: 28 bytes

Flags: 0x02 (SYN)

Window size: 16384

Checksum: 0xd1db [correct]

Options: (8 bytes)

Maximum segment size: 1380 bytes

NOP

NOP

NOP

NOP

0000 00 0c 29 9f 2e 84 00 aa 00 cb 7d 01 08 00 45 00 ..).....}...E.

0010 00 3c 07 28 40 00 80 06 40 74 0a 00 00 02 c0 a8 .0.(@...@t.....

0020 e8 81 04 00 00 15 ff 98 bd ba 03 00 00 00 70 02 .....p.

0030 40 0c d1 db 00 00 02 04 05 64 01 01 01 01 @.....d....

Which statement is true?

- A. This packet decoder is using relative TCP sequence numbering?.



- B. This TCP client is proposing the use of TCP window scaling?.
- C. This packet represents an active FTP data session?.
- D. This packet contains no TCP payload.

Correct Answer: D

### QUESTION 3

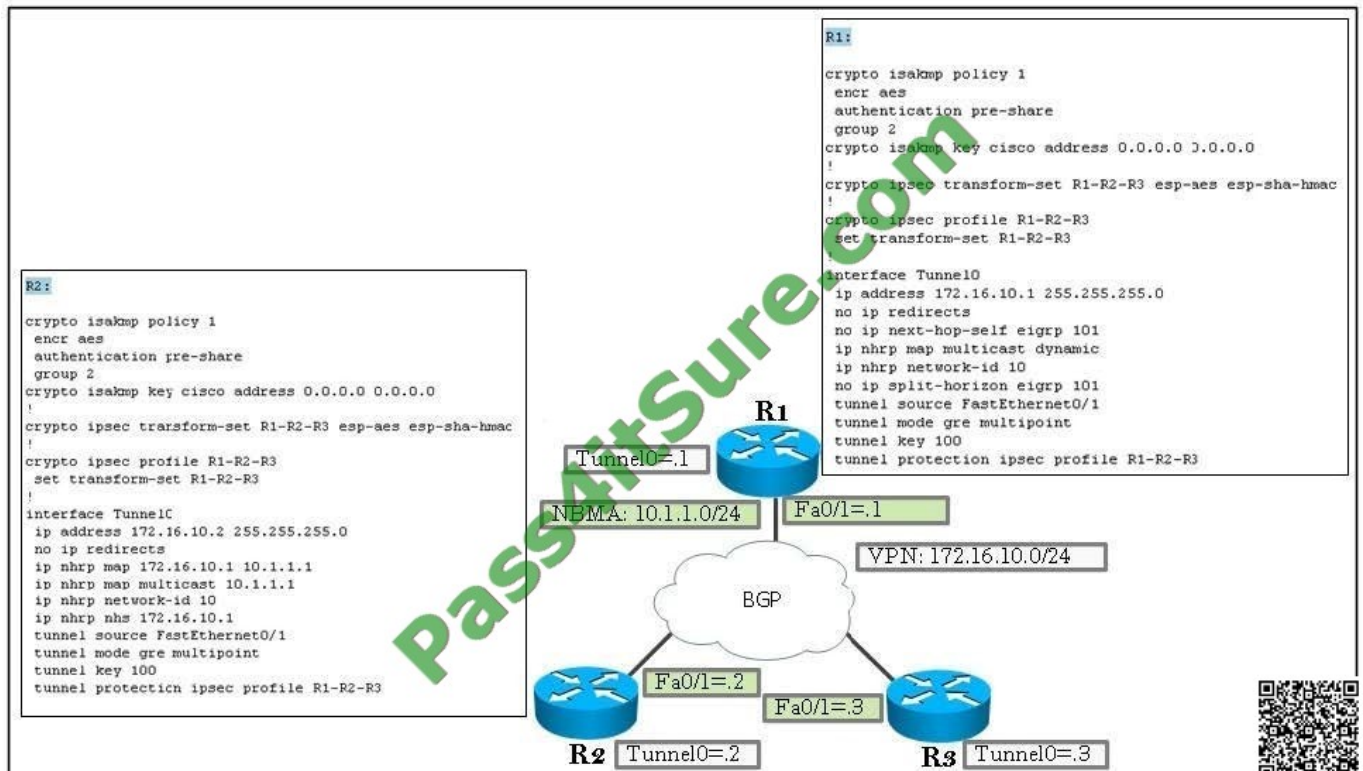
Which three statements about VXLANs are true? (Choose three.)

- A. It requires that IP protocol 8472 be opened to allow traffic through a firewall.
- B. Layer 2 frames are encapsulated in IP, using a VXLAN ID to identify the source VM.
- C. A VXLAN gateway maps VXLAN IDs to VLAN IDs.
- D. IGMP join messages are sent by new VMs to determine the VXLAN multicast IP.
- E. A VXLAN ID is a 32-bit value.

Correct Answer: BCD

### QUESTION 4

Refer to the exhibit.





Which statement about the exhibit is true?

- A. The tunnel configuration is incomplete and the DMVPN session will fail between R1 and R2.
- B. IPsec phase-2 will fail to negotiate due to a mismatch in parameters.
- C. A DMVPN session will establish between R1 and R2 provided that the BGP and EIGRP configurations are correct.
- D. A DMVPN session will establish between R1 and R2 provided that the BGP configuration is correct.
- E. A DMVPN session will fail to establish because R2 is missing the ISAKMP peer address.

Correct Answer: C

---

#### QUESTION 5

Which current RFC made RFCs 2409, 2407, and 2408 obsolete?

- A. RFC 4306
- B. RFC 2401
- C. RFC 5996
- D. RFC 4301
- E. RFC 1825

Correct Answer: C

---

#### QUESTION 6

What functionality is provided by DNSSEC?

- A. origin authentication of DNS data
- B. data confidentiality of DNS queries and answers
- C. access restriction of DNS zone transfers
- D. storage of the certificate records in a DNS zone file

Correct Answer: A

---

#### QUESTION 7

If ISE is not Layer 2 adjacent to the Wireless LAN Controller, which two options should be configured on the Wireless LAN Controller to profile wireless endpoints accurately? (Choose two.)

- A. Configure the Call Station ID Type to be: "IP Address".



- B. Configure the Call Station ID Type to be: "System MAC Address".
- C. Configure the Call Station ID Type to be: "MAC and IP Address".
- D. Enable DHCP Proxy.
- E. Disable DHCP Proxy.

Correct Answer: BE

---

#### QUESTION 8

What is the purpose of the BGP TTL security check?

- A. The BGP TTL security check is used for iBGP session.
- B. The BGP TTL security check protects against CPU utilization-based attacks.
- C. The BGP TTL security check checks for a TTL value in packet header of less than or equal to for successful peering.
- D. The BGP TTL security check authenticates a peer.
- E. The BGP TTL security check protects against routing table corruption.

Correct Answer: B

---

#### QUESTION 9

Which two EAP methods may be susceptible to offline dictionary attacks? (Choose two.)

- A. EAP-MD5
- B. LEAP
- C. PEAP with MS-CHAPv2
- D. EAP-FAST

Correct Answer: AB

---

#### QUESTION 10

Which statement about SMTP is true?

- A. SMTP uses UDP port 25.
- B. The POP protocol is used by the SMTP client to manage stored mail.
- C. The IMAP protocol is used by the SMTP client to retrieve and manage stored email.
- D. The mail delivery agent in the SMTP architecture is responsible for DNS lookup.



E. SMTP uses TCP port 20.

Correct Answer: C

---

#### QUESTION 11

Which mode of operation must be enabled on CSM to support roles such as Network Administrator, Approver, Network Operator, and Help Desk?

- A. Deployment Mode
- B. Activity Mode
- C. Workflow Mode
- D. User Roles Mode
- E. Administration Mode
- F. Network Mode

Correct Answer: C

---

#### QUESTION 12

You have been asked to configure a Cisco ASA appliance in multiple mode with these settings:

- A. You need two customer contexts, named contextA and contextB.
- B. Allocate interfaces G0/0 and G0/1 to contextA.
- C. Allocate interfaces G0/0 and G0/2 to contextB.
- D. The physical interface name for G0/1 within contextA should be "inside".
- E. All other context interfaces must be viewable via their physical interface names.

If the admin context is already defined and all interfaces are enabled, which command set will complete this configuration?

- A. context contextA config-url disk0:/contextA.cfg allocate-interface GigabitEthernet0/0 visible allocate-interface GigabitEthernet0/1 inside context contextB config-url disk0:/contextB.cfg allocate-interface GigabitEthernet0/0 visible allocate-interface GigabitEthernet0/2 visible
- B. context contexta config-url disk0:/contextA.cfg allocate-interface GigabitEthernet0/0 visible allocate-interface GigabitEthernet0/1 inside context contextb config-url disk0:/contextB.cfg allocate-interface GigabitEthernet0/0 visible allocate-interface GigabitEthernet0/2 visible
- C. context contextA config-url disk0:/contextA.cfg allocate-interface GigabitEthernet0/0 invisible allocate-interface GigabitEthernet0/1 inside context contextB config-url disk0:/contextB.cfg allocate-interface GigabitEthernet0/0 invisible allocate-interface GigabitEthernet0/2 invisible
- D. context contextA config-url disk0:/contextA.cfg allocate-interface GigabitEthernet0/0 allocate-interface



GigabitEthernet0/1 inside context contextB config-url disk0:/contextB.cfg allocate-interface GigabitEthernet0/0 allocate-interface GigabitEthernet0/2

E. context contextA config-url disk0:/contextA.cfg allocate-interface GigabitEthernet0/0 visible allocate-interface GigabitEthernet0/1 inside context contextB config-url disk0:/contextB.cfg allocate-interface GigabitEthernet0/1 visible allocate-interface GigabitEthernet0/2 visible

Correct Answer: A

---

### QUESTION 13

Which four types of VPN natively provide encryption of user traffic? (Choose four.)

- A. MPLS
- B. IPsec
- C. L2TPv3
- D. SSL
- E. VPLS
- F. AToM
- G. GETVPN
- H. Microsoft PPTP

Correct Answer: BDGH

---

### QUESTION 14

Refer to the exhibit.



```
Client:
```

```
|  
|  
(inside)  
ZBFW  
(outside)  
|  
|
```

```
Server
```

```
zone security inside  
zone security outside
```

```
interface inside  
  zone-member security inside
```

```
interface outside  
  zone-member security outside
```

```
class-map type inspect match-all HTTP_CMAP  
  match protocol HTTP  
class-map type inspect match-all TCP_CMAP  
  match protocol TCP
```

```
policy-map type inspect IN-OUT_PMAP  
  class type inspect TCP_CMAP  
  inspect  
  class type inspect HTTP_CMAP  
  pass  
  class class-default  
  drop
```

```
zone-pair IN-OUT_ZP source inside destination outside  
  service-policy type inspect IN-OUT_PMAP
```

With the client protected by the firewall, an HTTP connection from the client to the server on TCP port 80 will be subject to which action?

A. inspection action by the HTTP\_CMAP





- B. inspection action by the TCP\_CMAP
- C. drop action by the default class
- D. inspection action by both the HTTP\_CMAP and TCP\_CMAP
- E. pass action by the HTTP\_CMAP
- F. drop action due to class-map misclassification

Correct Answer: B

---

#### QUESTION 15

Which algorithm is used to generate the IKEv2 session key?

- A. Diffie-Hellman
- B. Rivest, Shamir, and Adleman
- C. Secure Hash Algorithm
- D. Rivest Cipher 4

Correct Answer: A

---

#### QUESTION 16

Which option represents IPv6 address ff02::1?

- A. PIM routers.
- B. RIP routers.
- C. all nodes on the local network.
- D. NTP.

Correct Answer: C

---

#### QUESTION 17

Which transport mechanism is used between a RADIUS authenticator and a RADIUS authentication server?

- A. UDP, with only the password in the Access-Request packet encrypted
- B. UDP, with the whole packet body encrypted
- C. TCP, with only the password in the Access-Request packet encrypted
- D. EAPOL, with TLS encrypting the entire packet



E. UDP RADIUS encapsulated in the EAP mode enforced by the authentication server.

Correct Answer: A

---

#### QUESTION 18

What transport protocol and port are used by GDOI for its IKE sessions that are established between the group members and the key server?

- A. UDP port 848
- B. TCP port 848
- C. ESP port 51
- D. SSL port 443
- E. UDP port 4500

Correct Answer: A

---

#### QUESTION 19

Which three statements are true about DES? (Choose three.)

- A. A 56-bit key is used to encrypt 56-bit blocks of plaintext.
- B. A 56-bit key is used to encrypt 64-bit blocks of plaintext.
- C. Each block of plaintext is processed through 16 rounds of identical operations.
- D. Each block of plaintext is processed through 64 rounds of identical operations.
- E. ECB, CBC, and CFB are modes of DES.
- F. Each Block of plaintext is processed through 8 rounds of identical operations.
- G. CTR, CBC, and OFB are modes of DES.

Correct Answer: BCE

---

#### QUESTION 20

Beacons, probe request, and association request frames are associated with which category?

- A. management
- B. control
- C. data



D. request

Correct Answer: A

---

#### QUESTION 21

Which three Cisco security product features assist in preventing TCP-based man-in-the-middle attacks? (Choose three.)

- A. Cisco ASA TCP initial sequence number randomization?
- B. Cisco ASA TCP sliding-window conformance validation?
- C. Cisco IPS TCP stream reassembly?
- D. Cisco IOS TCP maximum segment size adjustment?

Correct Answer: ABC

---

#### QUESTION 22

Which three statements are true about PIM-SM operations? (Choose three.)

- A. PIM-SM supports RP configuration using static RP, Auto-RP, or BSR.
- B. PIM-SM uses a shared tree that is rooted at the multicast source.
- C. Different RPs can be configured for different multicast groups to increase RP scalability.
- D. Candidate RPs and RP mapping agents are configured to enable Auto-RP.
- E. PIM-SM uses the implicit join model.

Correct Answer: ACD

---

#### QUESTION 23

Which three traffic conditions can be matched when configuring single rate, dual token bucket traffic policing on Cisco routers? (Choose three.)

- A. conform
- B. normal
- C. violate
- D. peak
- E. exceed
- F. average



Correct Answer: ACE

#### QUESTION 24

Which IPS module can be installed on the Cisco ASA 5520 appliance?

- A. IPS-AIM
- B. AIP-SSM
- C. AIP-SSC
- D. NME-IPS-K9
- E. IDSM-2

Correct Answer: B

#### QUESTION 25

Refer to the exhibit.

```
regex domainlist1 "\.facebook\.com"  
regex domainlist2 "\.youtube\.com"  
regex domainlist3 "\.twitter\.com"
```

```
class-map type regex match-any DomainBlockList  
match regex domainlist1  
match regex domainlist3
```

```
class-map type inspect http match all BlockDomainsClass  
match request header host regex class DomainBlockList
```

```
policy-map type inspect http http_inspection_policy  
parameters  
protocol-violation action drop-connection  
class BlockDomainsClass  
reset og
```

```
policy-map inside-policy  
class httptraffic  
inspect http http_inspection_policy
```

```
service-policy inside-policy interface inside
```





What will be the default action?

- A. HTTP traffic to the Facebook, Youtube, and Twitter websites will be dropped.
- B. HTTP traffic to the Facebook and Youtube websites will be dropped.
- C. HTTP traffic to the Youtube and Twitter websites will be dropped.
- D. HTTP traffic to the Facebook and Twitter websites will be dropped.

Correct Answer: D

---

#### QUESTION 26

According to OWASP guidelines, what is the recommended method to prevent cross-site request forgery?

- A. Allow only POST requests.
- B. Mark all cookies as HTTP only.
- C. Use per-session challenge tokens in links within your web application.
- D. Always use the "secure" attribute for cookies.
- E. Require strong passwords.

Correct Answer: C

---

#### QUESTION 27

Which two statements about the DH group are true? (Choose two.)

- A. The DH group is used to provide data authentication.
- B. The DH group is negotiated in IPsec phase-1.
- C. The DH group is used to provide data confidentiality.
- D. The DH group is used to establish a shared key over an unsecured medium.
- E. The DH group is negotiated in IPsec phase-2.

Correct Answer: BD

---

#### QUESTION 28

Which option explains the passive scan technique that is used by wireless clients to discover available wireless networks?

- A. listening for access point beacons that contain available wireless networks



- B. sending a null probe request
- C. sending a null association request
- D. listening for access point probe response frames that contain available wireless networks

Correct Answer: A

### QUESTION 29

Which option describes the main purpose of EIGRP authentication?

- A. to authenticate peers
- B. to allow faster convergence
- C. to provide redundancy
- D. to avoid routing table corruption

Correct Answer: D

### QUESTION 30

Refer to the exhibit.

```

R2:
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set R1-R2-R3 esp-aes esp-sha-hmac
!
crypto ipsec profile R1-R2-R3
  set transform-set R1-R2-R3
!
interface Tunnel0
  ip address 172.16.10.2 255.255.255.0
  no ip redirects
  ip nhrp map 172.16.10.1 10.1.1.1
  ip nhrp map multicast 10.1.1.1
  ip nhrp network-id 10
  ip nhrp nhs 172.16.10.1
  tunnel source FastEthernet0/1
  tunnel mode gre multipoint
  tunnel key 100
  tunnel protection ipsec profile R1-R2-R3
            
```

```

R1:
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set R1-R2-R3 esp-aes esp-sha-hmac
!
crypto ipsec profile R1-R2-R3
  set transform-set R1-R2-R3
!
interface Tunnel0
  ip address 172.16.10.1 255.255.255.0
  no ip redirects
  no ip next-hop-self eigrp 101
  ip nhrp map multicast dynamic
  ip nhrp network-id 10
  no ip split-horizon eigrp 101
  tunnel source FastEthernet0/0
  tunnel mode gre multipoint
  tunnel key 100
  tunnel protection ipsec profile R1-R2-R3
            
```

What is the reason for the failure of the DMVPN session between R1 and R2?



- A. tunnel mode mismatch
- B. IPsec phase-1 configuration is missing peer address on R2
- C. IPsec phase-1 policy mismatch
- D. IPsec phase-2 policy mismatch
- E. incorrect tunnel source interface on R1

Correct Answer: E

---

### QUESTION 31

Regarding VSAs, which statement is true?

- A. VSAs may be implemented on any RADIUS server.
- B. VSAs are proprietary, and therefore may only be used on the RADIUS server of that vendor. For example, a Cisco VSA may only be used on a Cisco RADIUS server, such as ACS or ISE.
- C. VSAs do not apply to RADIUS; they are a TACACS attribute.
- D. Each VSA is defined in an RFC and is considered to be a standard.

Correct Answer: A

---

### QUESTION 32

Which multicast capability is not supported by the Cisco ASA appliance?

- A. ASA configured as a rendezvous point
- B. sending multicast traffic across a VPN tunnel
- C. NAT of multicast traffic
- D. IGMP forwarding (stub) mode

Correct Answer: B

---

### QUESTION 33

Refer to the exhibit.



```
NHRP: Receive Registration Request via Tunnel0 vrf 0, packet : 92
(F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
shtl: 4(NSAP), sstl: 0(NSAP)
pktsz: 92 extoff: 52
(M) flags: "unique nat ", reqid: 65584
src NBMA: 69.1.1.2
src protocol: 192.168.10.2, dst protocol: 192.168.10.1
(C-1) code: no error(0)
prefix: 32, mtu: 17912, hd_time: 7200
addr_len: 3(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
%DUAL-5-NBRCHANGE: EIGRP-IPv4 101: Neighbor 192.168.10.2 (Tunnel0) is up: new adje
```



Which two statements correctly describe the debug output that is shown in the exhibit? (Choose two.)

- A. The request is from NHS to NNC.
- B. The request is from NHC to NHS.
- C. 69.1.1.2 is the local non-routable address.
- D. 192.168.10.2 is the remote NBMA address.
- E. 192.168.10.1 is the local VPN address.
- F. This debug output represents a failed NHRP request.

Correct Answer: BE

#### QUESTION 34

Which two statements about the SHA-1 algorithm are true? (Choose two)

- A. The SHA-1 algorithm is considered secure because it always produces a unique hash for the same message.
- B. The SHA-1 algorithm takes input message of any length and produces 160-bit hash output.
- C. The SHA-1 algorithm is considered secure because it is possible to find a message from its hash.
- D. The purpose of the SHA-1 algorithm is to provide data confidentiality.
- E. The purpose of the SHA-1 algorithm is to provide data authenticity.

Correct Answer: BE

#### QUESTION 35

Which three features describe DTLS protocol? (Choose three.)

- A. DTLS handshake does not support reordering or manage loss packets.
- B. DTLS provides enhanced security, as compared to TLS.





- C. DTLS provides block cipher encryption and decryption services.
- D. DTLS is designed to prevent man-in-the-middle attacks, message tampering, and message forgery.
- E. DTLS is used by application layer protocols that use UDP as a transport mechanism.
- F. DTLS does not support replay detection.

Correct Answer: CDE

### QUESTION 36

Refer to the exhibit.

```
regex App_regex_1
"[uU][nN][iI][oO][nN]([%2[0bB]][+])([aA][L][L]([%2[0bB]][+]))?
[sS][eE][L][eE][cC][tT]"
regex App_regex_2 "[Ss][Ee][Ll][Ee][Cc][Tt](%2[0bB][+])[\r\x00-
\x19\x7f-\xff]+(%2[0bB][+])[Ff][Rr][Oo][Mm](%2[0bB][+])"
!
class-map WebServers
  match port tcp eq www
class-map type inspect http match-any App-map
  match request body regex App_regex_1
  match request body regex App_regex_2
!
policy-map type inspect http drop-Protocol
  parameters
    body-match-maximum 3000
class App-map
  drop-connection log
policy-map protocol-traffic
  class WebServers
    inspect http drop-Protocol
!
service-policy protocol-traffic interface outside
```



What type of attack is being mitigated on the Cisco ASA appliance?

- A. HTTPS certificate man-in-the-middle attack
- B. HTTP distributed denial of service attack



- C. HTTP Shockwave Flash exploit
- D. HTTP SQL injection attack

Correct Answer: D

#### QUESTION 37

Which statement about DHCP snooping is true?

- A. The dynamic ARP inspection feature must be enabled for DHCP snooping to work.
- B. DHCP snooping is enabled on a per-VLAN basis.
- C. DHCP snooping builds a binding database using information that is extracted from intercepted ARP requests.
- D. DHCP snooping is enabled on a per-port basis.
- E. DHCP snooping is does not rate-limit DHCP traffic from trusted ports.

Correct Answer: B

#### QUESTION 38

Refer to the exhibit.

```
ISAKMP (62): processing SA payload. message ID = 0
ISAKMP (62): Checking ISAKMP transform 1 against priority 10 policy
                encryption DES-CBC
                hash SHA
                default group 1
                auth pre-share
ISAKMP (62): atts are acceptable. Next payload is 0
ISAKMP (62): SA is doing pre-shared key authentication
ISAKMP (62): processing KE payload. message ID = 0
ISAKMP (62): processing NONCE payload. message ID = 0
ISAKMP (62): SKEYID state generated
ISAKMP (62): processing vendor id payload
ISAKMP (62): speaking to another Cisco IOS box!
ISAKMP: reserved not zero on ID payload!
%CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 172.16.100.201
failed its sanity check or is malformed
```



Which message of the ISAKMP exchange is failing?

- A. main mode 1
- B. main mode 3
- C. aggressive mode 1
- D. main mode 5



E. aggressive mode 2

Correct Answer: B

---

#### QUESTION 39

In an 802.11 WLAN, which option is the Layer 2 identifier of a basic service set, and also is typically the MAC address of the radio of the access point?

- A. BSSID
- B. SSID
- C. VBSSID
- D. MBSSID

Correct Answer: A

---

#### QUESTION 40

Which statement regarding TFTP is not true?

- A. Communication is initiated over UDP port 69.
- B. Files are transferred using a secondary data channel.
- C. Data is transferred using fixed-size blocks.
- D. TFTP authentication information is sent in clear text.
- E. TFTP is often utilized by operating system boot loader procedures.
- F. The TFTP protocol is implemented by a wide variety of operating systems and network devices.

Correct Answer: D

[Latest 351-018 Dumps](#)

[351-018 VCE Dumps](#)

[351-018 Exam Questions](#)



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.pass4itsure.com/allproducts>

## Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <p><b>One Year Free Update</b> 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.</p>	 <p><b>Money Back Guarantee</b> To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p><b>Security &amp; Privacy</b> We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © pass4itsure, All Rights Reserved.