



640-554^{Q&As}

Implementing Cisco IOS Network Security (IINS v2.0)

Pass Cisco 640-554 Exam with 100% Guarantee

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

<https://www.pass4lead.com/640-554.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

When a company puts a security policy in place, what is the effect on the company's business?

- A. minimizing risk
- B. minimizing total cost of ownership
- C. minimizing liability
- D. maximizing compliance

Correct Answer: A

QUESTION 2

You suspect that an attacker in your network has configured a rogue Layer 2 device to intercept traffic from multiple VLANs, which allows the attacker to capture potentially sensitive data. Which two methods will help to mitigate this type of activity? (Choose two.)

- A. Turn off all trunk ports and manually configure each VLAN as required on each port.
- B. Place unused active ports in an unused VLAN.
- C. Secure the native VLAN, VLAN 1, with encryption.
- D. Set the native VLAN on the trunk ports to an unused VLAN.
- E. Disable DTP on ports that require trunking.

Correct Answer: DE

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/layer2.html>

Layer 2 LAN Port Modes

Table 17-2 lists the Layer 2 LAN port modes and describes how they function on LAN ports.

switchport mode access

Puts the LAN port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The LAN port becomes a nontrunk port even if the neighboring LAN port does not agree to the change.

switchport mode dynamic desirable

Makes the LAN port actively attempt to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to trunk, desirable, or auto mode. This is the default mode for all LAN ports.

switchport mode dynamic auto

Makes the LAN port willing to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to trunk or desirable mode.



switchport mode trunk

Puts the LAN port into permanent trunking mode and negotiates to convert the link into a trunk link. The LAN port becomes a trunk port even if the neighboring port does not agree to the change.

switchport nonegotiate

Puts the LAN port into permanent trunking mode but prevents the port from generating DTP frames. You must configure the neighboring port manually as a trunk port to establish a trunk link.

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

Double Encapsulation Attack

When double-encapsulated 802.1Q packets are injected into the network from a device whose VLAN happens to be the native VLAN of a trunk, the VLAN identification of those packets cannot be preserved from end to end since the 802.1Q

trunk would always modify the packets by stripping their outer tag. After the external tag is removed, the internal tag permanently becomes the packet's only VLAN identifier. Therefore, by doubleencapsulating packets with two different tags,

traffic can be made to hop across VLANs.

This scenario is to be considered a misconfiguration, since the 802.1Q standard does not necessarily force the users to use the native VLAN in these cases. As a matter of fact, the proper configuration that should always be used is to clear

the native VLAN from all 802.1Q trunks (alternatively, setting them to 802.1q-all- tagged mode achieves the exact same result). In cases where the native VLAN cannot be cleared, then always pick an unused VLAN as native VLAN of all the

trunks; don't use this VLAN for any other purpose.

Protocols like STP, DTP, and UDLD (check out [3]) should be the only rightful users of the native VLAN and their traffic should be completely isolated from any data packets.

QUESTION 3

Which type of address translation should be used when a Cisco ASA is in transparent mode?

- A. Static NAT
- B. Dynamic NAT
- C. Overload
- D. Dynamic PAT

Correct Answer: A

QUESTION 4

What is the best way to prevent a VLAN hopping attack?

- A. Encapsulate trunk ports with IEEE 802.1Q.



- B. Physically secure data closets.
- C. Disable DTP negotiations.
- D. Enable BDPU guard.

Correct Answer: C

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml 802.1Q and ISL Tagging Attack Tagging attacks are malicious schemes that allow a user on a VLAN to get unauthorized access to another VLAN. For example, if a switch port were configured as DTP auto and were to receive a fake DTP packet, it might become a trunk port and it might start accepting traffic destined for any VLAN. Therefore, a malicious user could start communicating with other VLANs through that compromised port. Sometimes, even when simply receiving regular packets, a switch port may behave like a full-fledged trunk port (for example, accept packets for VLANs different from the native), even if it is not supposed to. This is commonly referred to as "VLAN leaking" (see [5] for a report on a similar issue).

QUESTION 5

Which two countermeasures can mitigate ARP spoofing attacks? (Choose two.)

- A. port security
- B. DHCP snooping
- C. IP source guard
- D. dynamic ARP inspection

Correct Answer: BD

[Latest 640-554 Dumps](#)

[640-554 PDF Dumps](#)

[640-554 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.pass4lead.com/allproducts>

Need Help

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

To update a previously submitted ticket:



 <p>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.</p>	 <p>Money Back Guarantee 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>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.</p>
---	---	--

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

All trademarks are the property of their respective owners.

Copyright © pass4lead, All Rights Reserved.