

642-812

Cisco

BCMSN-Building Converged Cisco Multilayer Switched Networks

Visit: <http://www.pass4sureofficial.com/exams.asp?examcode=642-812>

Pass4sureofficial.com is a reputable IT certification examination guide, study guides and audio exam provider, we not only ensure that you pass your 642-812 exam in first attempt, but also you can get a high score to acquire Cisco certification.

If you use pass4sureofficial 642-812 Certification questions and answers, you will experience actual 642-812 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our Cisco exam prep covers over 95% of the questions and answers that may be appeared in your 642-812 exam. Every point from pass4sure 642-812 PDF, 642-812 review will help you take Cisco 642-812 exam much easier and become Cisco certified. All the Questions/Answers are taken from real exams.

Here's what you can expect from the Pass4sureOfficial Cisco 642-812 course:

- * Up-to-Date Cisco 642-812 questions taken from the real exam.
- * 100% correct Cisco 642-812 answers you simply can't find in other 642-812 courses.
- * All of our tests are easy to download. Your file will be saved as a 642-812 PDF.
- * Cisco 642-812 brain dump free content featuring the real 642-812 test questions.

Cisco 642-812 certification exam is of core importance both in your Professional life and Cisco certification path. With Cisco certification you can get a good job easily in the market and get on your path for success. Professionals who passed Cisco 642-812 exam training are an absolute favorite in the industry. You will pass Cisco 642-812 certification test and career opportunities will be open for you.



QUESTION: 1

Which two statements are true about a switched virtual interface (SVI)? (Choose two.)

- A. An SVI is created by entering the no switchport command in interface configuration mode.
- B. SVI is another name for a routed port.
- C. Multiple SVIs can be associated with a VLAN.
- D. An SVI is created for the default VLAN (VLAN1) to permit remote switch administration by default.
- E. An SVI provides a default gateway for a VLAN.

Answer: D,E

Explanation:

On a multilayer switch, you can also enable Layer 3 functionality for an entire VLAN on the switch. This allows a network address to be assigned to a logical interface—that of the VLAN itself. This is useful when the switch has many ports assigned to a common VLAN, and routing is needed in and out of that VLAN. The logical Layer 3 interface is known as an SVI. However, when it is configured, it uses the much more intuitive interface name `vlan vlan-id`, as if the VLAN itself is a physical interface. First, define or identify the VLAN interface, and then assign any Layer 3 functionality to it with the following configuration commands:

```
Switch(config)# interface vlan vlan-id
```

```
Switch(config-if)# ip address ip-address mask [secondary]
```

The VLAN must be defined and active on the switch before the SVI can be used. Make sure the new VLAN interface is also enabled with the `no shutdown` interface configuration command.

QUESTION: 2

Which three WLAN statements are true? (Choose three.)

- A. Another term for infrastructure mode is independent service set (IBSS).
- B. Ad hoc mode allows mobile clients to connect directly without an intermediate AP.
- C. The Aironet 1230 access point is an example of an access point that operates solely as a lightweight access point.
- D. A lightweight AP receives control and configuration from a WLAN controller to which it is associated.
- E. WLANs are designed to share the medium and can easily handle an increased demand of channel contention.
- F. A WLAN client that is operating in half-duplex mode will delay all clients in that WLAN.

Answer: B,D,F

Explanation:

The 802.11 standard specifies a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) transmit-recvie environment. Therefore, all 802.11 are half-duplex/simplex in nature .Lightweight access points first search for a WLAN controller using LWAPP in Layer 2 mode. Then the access point searches for a WLAN in Layer 3 mode. The control traffic between the access point and the controller is encapsulated with the LWAPP. The control traffic is encrypted via the Advanced Encryption Standard (AES). Lightweight APs need configuration and control information from a WLAN controller

Incorrect Answer:

A: Ad hoc mode: This mode is called Independent Basic Service Set (IBSS). Mobile clients connect directly without an intermediate access point.

QUESTION: 3

Refer to the exhibit. Based on the running configuration that is shown for interface FastEthernet0/2, what two conclusions can be deduced? (Choose two.)

<output truncated>

```
!
interface FastEthernet0/2
  switchport mode access
  switchport port-security
  switchport port-security maximum 6
  switchport port-security aging time 5
  switchport port-security aging static
  switchport port-security mac-address sticky
  switchport port-security mac-address 0000.0000.000b
  switchport port-security mac-address sticky 0000.0000.4141
  switchport port-security mac-address sticky 0000.0000.5050
  no ip address
```

<output truncated>

- A. Connecting a host with MAC address 0000.0000.4147 will move interface FastEthernet0/2 into error disabled state.
- B. The host with address 0000.0000.4141 is removed from the secure address list after 5 seconds of inactivity.
- C. The sticky secure MAC addresses are treated as static secure MAC addresses after the running configuration is saved to the startup configuration and the switch is restarted.
- D. Interface FastEthernet0/2 is a voice VLAN port.
- E. The host with address 0000.0000.000b is removed from the secure address list after 300 seconds.

Answer: C,E

Explanation:

The time aging_time keyword specifies the aging time for this port. Valid range for aging_time is from 0 to 1440 minutes. If the time is equal to 0, aging is disabled for this port. In this case, the aging time is set for 5 minutes, or 300 seconds. You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling sticky port security. To enable sticky port security, enter the switchport port-security mac-address sticky command. When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the running config file to the configuration file, the interface does not need to relearn these addresses when the switch restarts.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/25sg/configuration/guide/port_security.html

QUESTION: 4

Which three statements are correct with regard to the IEEE 802.1Q standard? (Choose three.)

- A. the packet is encapsulated with a 26 byte header and a 4 byte FCS
- B. the IEEE 802.1Q frame retains the original MAC destination address
- C. protocol uses point-to-point connectivity
- D. the IEEE 802.1Q frame format adds a 4 byte field to an Ethernet frame
- E. protocol uses point-to-multipoint connectivity
- F. the IEEE 802.1Q frame uses multicast destination of 0x01-00-0c-00-00

Answer: B,C,D

Explanation:

The IEEE 802.1Q protocol can also carry VLAN associations over trunk links. However, this frame identification method is standardized, allowing VLAN trunks to exist and operate between equipment from multiple vendors. In particular, the IEEE 802.1Q standard defines an architecture for VLAN use, services provided with VLANs, and protocols and algorithms used to provide VLAN services. Like Cisco ISL, IEEE 802.1Q can be used for VLAN identification with Ethernet trunks. Instead of encapsulating each frame with a VLAN ID header and trailer, 802.1Q embeds its tagging information within the Layer 2 frame. This method is referred to as single-

tagging or internal tagging .802.1Q also introduces the concept of a native VLAN on a trunk. Frames belonging to this VLAN are not encapsulated with any tagging information. In the event that an end station is connected to an 802.1Q trunk link, the end station can receive and understand only the native VLAN frames. This provides a simple way to offer full trunk encapsulation to the devices that can understand it, while giving normal access stations some inherent connectivity over the trunk.

QUESTION: 5

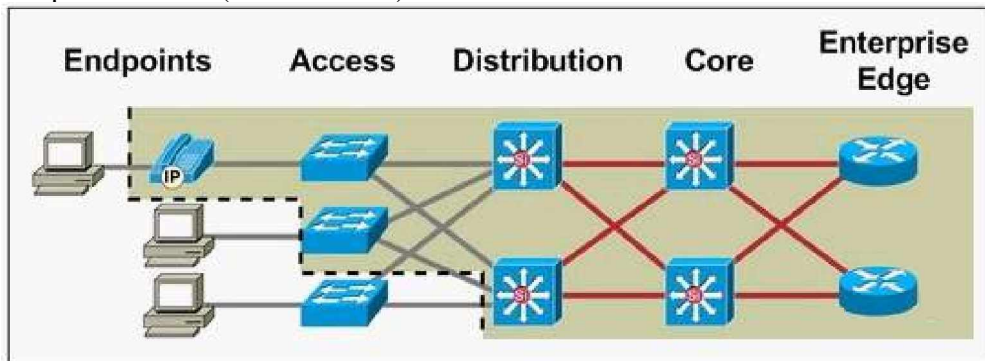
What does the auto qos voip cisco-phone command do?

- A. If a Cisco IP phone is attached and removed, the switch continues to trust the CoS values as long as the switch is not rebooted.
- B. If a Cisco IP phone is attached, the switch trusts the CoS.
- C. It turns on STP to see if a Cisco IP phone is attached.
- D. The switch assigns a CoS value of 5 to incoming packets.
- E. It disables the trust boundary feature because the switch knows a Cisco IP phone is attached.

Answer: B

QUESTION: 6

Refer to the exhibit. Which three statements are true about trust boundaries in the campus network? (Choose three.)



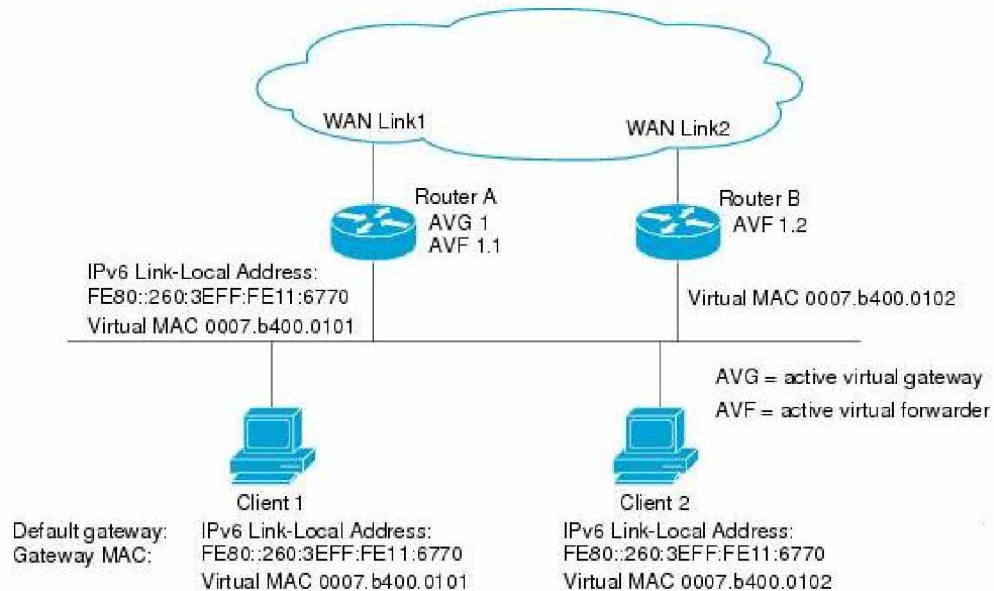
- A. Classification and marking occur using 802.1ab QoS bits before reaching the trust boundary.
- B. A device is trusted if it correctly declassifies packets.
- C. A device is trusted if it correctly classifies packets.
- D. Network trust boundaries are automatically configured in IOS version 12.3 and later.
- E. The outermost trusted devices represent the trust boundary.
- F. For scalability, classification should be done as close to the edge as possible.

Answer: C,E,F

QUESTION: 7

Refer to the exhibit.

Which three statements accurately describe this GLBP topology? (Choose three.)



- A. Router A is responsible for answering ARP requests sent to the virtual IP address.
- B. If Router A becomes unavailable, Router B will forward packets sent to the virtual MAC address of Router A.
- C. Router A alternately responds to ARP requests with different virtual MAC addresses.
- D. Router B will transition from blocking state to forwarding state when it becomes the AVG.
- E. If another router were added to this GLBP group, there would be two backup AVGs.
- F. Router B is in GLBP listen state.

Answer: A,B,C

QUESTION: 8

Which set of statements describes the correct order and process of a wireless client associating with a wireless access point?

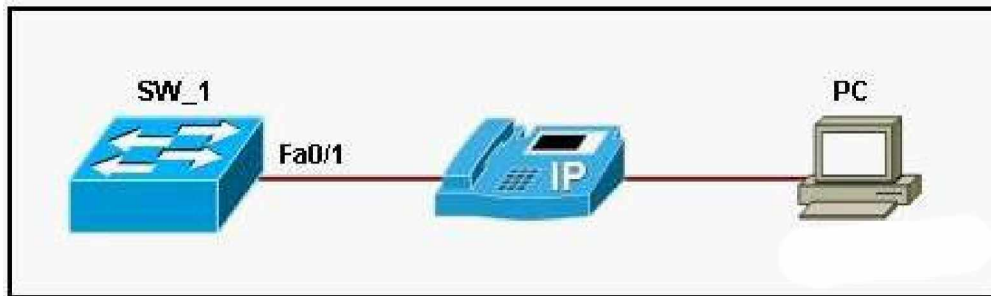
- A. 1. Client sends probe request.
2. Access point sends probe response.
3. Client initiates association.
4. Access point accepts association.
5. Access point adds client MAC address to association table.
- B. 1. Client sends probe request.
2. Access point sends probe response.
3. Access point initiates association.

4. Client accepts association.
 5. Access point adds client MAC address to association table.
- C.
1. Access point sends probe request .
 2. Client sends probe response.
 3. Client initiates association.
 4. Access point accepts association.
 5. Client adds access point MAC address to association table.
- D.
1. Access point sends probe request .
 2. Client sends probe response.
 3. Client initiates association.
 4. Access point accepts association.
 5. Access point adds client MAC address to association table.
- E.
1. Client sends probe request.
 2. Access point sends probe response.
 3. Client initiates association.
 4. Access point accepts association.
 5. Client adds access point MAC address to association table.

Answer: A

QUESTION: 9

Refer to the exhibit. Which statement is true when voice traffic is forwarded on the same VLAN used by the data traffic?



- A. The voice traffic cannot be forwarded to the distribution layer.
- B. The voice traffic cannot use 802.1p priority tagging.
- C. Port security cannot be enabled on the switch that is attached to the IP phone.
- D. Quality of service cannot be applied for the voice traffic.

Answer: B

Explanation:

You can configure a port connected to the Cisco IP Phone to send CDP packets to the phone to configure the way in which the phone sends voice traffic. The phone can carry voice traffic in 802.1Q frames for a specified voice VLAN with a Layer 2 CoS value. It

can use 802.1P priority tagging to give voice traffic a higher priority and forward all voice traffic through the native (access) VLAN. The IP phone can also send untagged voice traffic or use its own configuration to send voice traffic in the access VLAN. In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5). If the Cisco IP Phone and a device attached to the Cisco IP Phone are in the same VLAN, they must be in the same IP subnet. These conditions indicate that they are in the same VLAN:

-
They both use 802.1p or untagged frames.

-
The Cisco IP Phone uses 802.1p frames and the device uses untagged frames.

-
The Cisco IP Phone uses untagged frames and the device uses 802.1p frames.

-
The Cisco IP Phone uses 802.1Q frames and the voice VLAN is the same as the access VLAN.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps5206/products_configuration_guide_chapter09186a00801a64ea.html

QUESTION: 10

Refer to the exhibit. Based on the debug standby output in the exhibit, which HSRP statement is true?

```
DSW111(config)#interface vlan 11
DSW111(config-if)#no shut
*May 10 20:34:08.925: %SYS-5-CONFIG_I: Configured from console by console
*May 10 20:34:10.213: %LINK-3-UPDOWN: Interface Vlan11, changed state to up
*May 10 20:34:10.221: SB: V111 Interface up
*May 10 20:34:10.221: SB11: V111 Init: a/HSRP enabled
*May 10 20:34:10.221: SB11: V111 Init -> Listen
*May 10 20:34:11.213: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan11, changed state to up
*May 10 20:34:20.221: SB11: V111 Listen: c/Active timer expired (unknown)
*May 10 20:34:20.221: SB11: V111 Listen -> Speak
*May 10 20:34:20.221: SB11: V111 Hello out 10.10.10.111 Speak pri 100 ip 10.10.10.115
*May 10 20:34:28.905: SB11: V111 Hello out 10.10.10.111 Speak pri 100 ip 10.10.10.115
*May 10 20:34:30.221: SB11: V111 Speak: d/Standby timer expired (unknown)
*May 10 20:34:30.221: SB11: V111 Standby router is local
*May 10 20:34:30.221: SB11: V111 Speak -> Standby
*May 10 20:34:30.221: SB11: V111 Hello out 10.10.10.111 Standby pri 100 ip 10.10.10.115
*May 10 20:34:30.221: SB11: V111 Standby: c/Active timer expired (unknown)
*May 10 20:34:30.221: SB11: V111 Active router is local
*May 10 20:34:30.221: SB11: V111 Standby router is unknown, was local
*May 10 20:34:30.221: SB11: V111 Standby -> Active
*May 10 20:34:30.221: %STANDBY-6-STATECHANGE: Vlan11 Group 11 state Standby -> Active
*May 10 20:34:30.221: SB11: V111 Hello out 10.10.10.111 Active pri 100 ip 10.10.10.115
*May 10 20:34:33.085: SB11: V111 Hello out 10.10.10.111 Active pri 100 ip 10.10.10.115
```

A. DSW111 is the active router because it is the only HSRP-enabled router on that segment.

- B. DSW111 is the active router because the standby timer has been incorrectly configured.
- C. DSW111 is the active router because it has a lower priority on that VLAN.
- D. DSW111 is the active router because it has a lower IP address than the tying priority router on that VLAN.
- E. DSW111 is the active router and is advertising the virtual IP address 10.10.10.111 on VLAN 11.

Answer: A

QUESTION: 11

What is the default VTP advertisement for subset advertisements in Catalyst switches that are in server or client mode?

- A. 1 minute
- B. 10 seconds
- C. 5 seconds
- D. 5 minutes
- E. 30 seconds

Answer: D

Explanation:

Periodic (default is 5 minutes) VTP advertisements are sent out each trunk port with the multicast destination MAC address 01-00-0C-CC-CC-CC. VTP advertisements contain the following configuration information: VLAN IDs (ISL and 802.1Q) Emulated LAN names (ATM LANE) 802.10 SAID values (FDDI) VTP domain name VTP r VLAN configuration, including the maximum transmission unit (MTU) size for each VLAN Frame format

QUESTION: 12

What information can be drawn from the output presented in the following exhibit?

```
S# show spanning-tree inconsistentports
```

Name	Interface	Inconsistency
VLAN0001	FastEthernet3/1	Port Type Inconsistent
VLAN0001	FastEthernet3/2	Port Type Inconsistent
VLAN0002	FastEthernet3/1	Port Type Inconsistent
VLAN0002	FastEthernet3/2	Port Type Inconsistent
VLAN0003	FastEthernet3/1	Port Type Inconsistent
VLAN0003	FastEthernet3/2	Port Type Inconsistent
VLAN0004	FastEthernet3/1	Port Type Inconsistent
VLAN0004	FastEthernet3/2	Port Type Inconsistent
VLAN0005	FastEthernet3/1	Port Type Inconsistent
VLAN0005	FastEthernet3/2	Port Type Inconsistent

Number of inconsistent ports (segments) in the system : 10

- A. Interfaces FastEthernet3/1 and FastEthernet3/2 are candidates for becoming the STP root port, but neither can realize that role until BPDUs with a superior root bridge parameter are no longer received on at least one of the interfaces.
- B. Devices connected to interfaces FastEthernet3/1 and FastEthernet3/2 are sending BPDUs with a superior root bridge parameter and no traffic is forwarded across the ports. Once the inaccurate BPDUs have been stopped, the interfaces will need to be administratively shut down, and brought back up, to resume normal operation.
- C. Devices connected to interfaces FastEthernet3/1 and FastEthernet3/2 are sending BPDUs with a superior root bridge parameter and no traffic is forwarded across the ports. Once the inaccurate BPDUs have been stopped, the interfaces automatically recover and resume normal operation.
- D. Devices connected to interfaces FastEthernet3/1 and FastEthernet3/2 are sending BPDUs with a superior root bridge parameter, but traffic is still forwarded across the ports.

Answer: C

QUESTION: 13

Which two statements are true about best practices in VLAN design? (Choose two.)

- A. Routing should occur at the access layer if voice VLANs are utilized. Otherwise, routing should occur at the distribution layer.
- B. Routing should not be performed between VLANs located on separate switches.
- C. Routing should always be performed at the distribution layer.
- D. VLANs should be localized to a single switch unless voice VLANs are being utilized.
- E. VLANs should be localized to a switch.

Answer: C,E

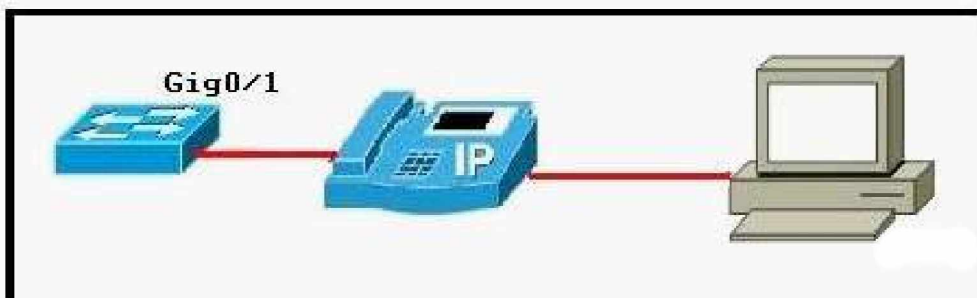
Explanation:

In the distribution layer, uplinks from all access layer devices are aggregated, or come together. The distribution layer switches must be capable of processing the total volume of traffic from all the connected devices. These switches should have a port density of high-speed links to support the collection of access layer switches. VLANs and broadcast domains converge at the distribution layer, requiring routing, filtering, and security. The switches at this layer must be capable of performing multilayer switching with high throughput. Only certain Catalyst switch models can provide multilayer switching; be sure to understand which ones can do this. A switched environment offers the technology to overcome flat network limitations. Switched networks can be subdivided into VLANs. By definition, a VLAN is a single broadcast domain. All devices connected to the VLAN receive broadcasts from other VLAN members. However, devices connected to a different VLAN will not receive those same broadcasts. (Naturally, VLAN members also receive unicast packets directed toward them from other VLAN members.) A VLAN consists of defined members communicating as a logical network segment. In contrast, a physical segment consists of devices that must be connected to a physical cable segment. A VLAN can have connected members located anywhere in the campus network, as long as VLAN connectivity is provided between all members. Layer 2 switches are configured with a VLAN mapping and provide the logical connectivity between the VLAN members.

QUESTION: 14

Refer to the exhibit.

Which two statements are true about the required switch configurations to support a voice VLAN? (Choose two.)



- A. CDP must be disabled on the switch port to prevent interference between CDP messages and voice traffic.
- B. Port security cannot be configured on a port that is configured for a voice vlan.
- C. Static secure MAC addresses should be configured on voice vlan ports to prevent access by devices other than IP phones.
- D. CDP must be enabled on the switch port to allow configuration information to be passed to the IP phone.
- E. Portfast must be enabled on the switch port.
- F. 802.1x authentication cannot be configured on a port configured for a voice vlan.

Answer: D,E

Pass4SureOfficial.com Lifetime Membership Features;

- Pass4SureOfficial Lifetime Membership Package includes over **2500** Exams.
- **All** exams Questions and Answers are included in package.
- **All** Audio Guides are included **free** in package.
- **All** Study Guides are included **free** in package.
- **Lifetime** login access.
- Unlimited download, no account expiry, no hidden charges, just one time \$99 payment.
- **Free updates** for Lifetime.
- **Free Download Access** to All new exams added in future.
- Accurate answers with explanations (If applicable).
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions, Answers and Study Guides are downloadable in **PDF** format.
- Audio Exams are downloadable in **MP3** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success **Guarantee**.
- **Fast**, helpful support 24x7.

View list of All exams (Q&A) downloads

<http://www.pass4sureofficial.com/allexams.asp>

View list of All Study Guides (SG) downloads

<http://www.pass4sureofficial.com/study-guides.asp>

View list of All Audio Exams (AE) downloads

<http://www.pass4sureofficial.com/audio-exams.asp>

Download All Exams Samples

<http://www.pass4sureofficial.com/samples.asp>

To purchase \$99 Lifetime Full Access Membership click here

<http://www.pass4sureofficial.com/purchase.asp>

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	SNIA	

