Version: 11.0

Question: 1

Which statement about RADIUS configuration distribution using Cisco Fabric Services on a Cisco Nexus 7000 Series Switch is true?

A. Cisco Fabric Services does not distribute the RADIUS server group configuration or server and global keys.
B. Enabling Cisco Fabric Services causes the existing RADIUS configuration on your Cisco NX-OS device to be immediately distributed.
C. When the RADIUS configuration is being simultaneously changed on more than one device in a Cisco Fabric Services region, the most recent changes will take precedence.
D. Only the Cisco NX-OS device with the lowest IP address in the Cisco Fabric Services region can lock the RADIUS configuration.

Answer: A

Explanation:
CFS does not distribute the RADIUS server group configuration or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.
Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_6-x/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_6-x_chapter_0101.html

Question: 2

By default it will take 10 seconds for authentication to fail due to an unresponsive RADIUS server before a Cisco Nexus series switch reverts to another RADIUS server or local authentication. What is one efficient way to improve the reaction time to a RADIUS server failure?

A. Decrease the global RADIUS retransmission count to 1.
B. Decrease the global RADIUS timeout interval to 5 seconds.
C. Configure the RADIUS retransmission count and timeout interval per server, versus globally.
D. Configure per server a test idle timer, along with a username and password.

Answer: D

Explanation:
You can monitor the availability of RADIUS servers. These parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval during which a RADIUS server receives no requests before the Nexus 5000 Series switch sends out a test packet. You can configure this option to test servers periodically. The test idle timer specifies the interval during which a RADIUS server receives no requests before the Nexus 5000 Series switch sends out a test packet. The

default idle timer value is 0 minutes. When the idle time interval is 0 minutes, the Nexus 5000 Series switch does not perform periodic RADIUS server monitoring.
Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_0_1a/CLIConfigurationGuide/sec_radius.html

Question: 3

Which statement explains why a Cisco UCS 6200 Fabric Interconnect that is configured in end-host mode is beneficial to the unified fabric network?

A. There is support for multiple (power of 2) uplinks.
B. Upstream Layer 2 disjoint networks will remain separated.
C. The 6200 can connect directly via vPC to a Layer 3 aggregation device.
D. STP is not required on the uplink ports from the 6200.

Answer: D

Explanation:
In Cisco Unified Computing System environments, two Ethernet switching modes determine the way that the fabric interconnects behave as switching devices between the servers and the network. In end-host mode, the fabric interconnects appear to the upstream devices as end hosts with multiple links. In end-host mode, the switch does not run Spanning Tree Protocol and avoids loops by following a set of rules for traffic forwarding. In switch mode, the switch runs Spanning Tree Protocol to avoid loops, and broadcast and multicast packets are handled in the traditional way.
Explanation:
http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-computing/whitepaper_c11-701962.html

Question: 4

Which two statements about Cisco Nexus 7000 line cards are true? (Choose two.)

A. M1, M2, and F1 cards are allowed in the same VDC.
B. M line cards are service-oriented and likely face the access layer and provide Layer 2 connectivity.
C. F line cards are performance-oriented and likely connect northbound to the core layer for Layer 3 connectivity.
D. M line cards support Layer 2, Layer 3, and Layer 4 with large forwarding tables and a rich feature set.
E. The F2 line card must reside in the admin VDC.

Answer: A, D

Explanation:
Cisco is introducing a new line card called as F3 Module which has rich feature set and offers high performance 40G/100G port density to the Nexus 7000 product family. Cisco also introduced a new feature in NX-OS 6.2(2) where the F2e line card can be in the same VDC as M1 or M2 Line Card. The

objective of this session is to cover detailed steps and methodology of migrating Nexus 7000 with VDC types prior to NX-OS 6.2 to the newer F3 or M/F2e VDC types. The session also covers the effect of VDC migration with commonly used Network features, firewall and load balancer services.
M-Series XL modules support larger forwarding tables. M-Series modules are frequently required at network core, peering, and aggregation points. When used with the F1-Series, the M-Series modules provide inter-VLAN services and form a pool of Layer 3 resources for the system.
Reference:
https://www.ciscolive2014.com/connect/sessionDetail.ww?SESSION_ID=2244
And http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/2-6/vmdctechwp.html

Question: 5

Which statement about the Layer 3 card on the Cisco Nexus 5500 Series Switch is true?

A. BGP support is not provided, but RIP, EIGRP, and OSPF support is provided.
B. Up to two 4-port cards are supported with up to 160 Gb/s of Layer 3 forwarding capability.
C. Up to 16 FEX connections are supported.
D. Port channels cannot be configured as Layer 3 interfaces.

Answer: C

Explanation:
From the Cisco NX-OS 5.1(3)N1(1) release and later releases, each Cisco Nexus 5500 Series device can manage and support up to 24 FEXs without Layer 3. With Layer 3, the number of FEXs supported per Cisco Nexus 5500 Series device is 8. With Enhanced vPC and a dual-homed FEX topology each FEX is managed by both Cisco Nexus 5000 Series devices. As a result, one pair of Cisco Nexus 5500 Series devices can support up to 24 FEXs and 16 FEXs for Layer 2 and Layer 3.
Reference:
http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mkt_ops_guides/513_n1_1/n5k_enhanced_vpc.html

Question: 6

Which statement about SNMP support on Cisco Nexus switches is true?

A. Cisco NX-OS only supports SNMP over IPv4.
B. Cisco NX-OS supports one instance of the SNMP per VDC.
C. SNMP is not VRF-aware.
D. SNMP requires the LAN_ENTERPRISE_SERVICES_PKG license.
E. Only users belonging to the network operator RBAC role can assign SNMP groups.

Answer: B

Explanation:
Cisco NX-OS supports one instance of the SNMP per virtual device context (VDC). By default, Cisco NX-OS

places you in the default VDC. SNMP supports multiple MIB module instances and maps them to logical network entities. SNMP is also VRF aware. You can configure SNMP to use a particular VRF to reach the SNMP notification host receiver. You can also configure SNMP to filter notifications to an SNMP host receiver based on the VRF where the notification occurred.
Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/system_management/configuration/guide/sm_nx_os_cg/sm_9snmp.html

Question: 7

Which GLBP load-balancing algorithm ensures that a client is always mapped to the same VMAC address?

A. vmac-weighted
B. dedicated-vmac-mode
C. shortest-path and weighting
D. host-dependent

Answer: D

Explanation:
Host dependent—GLBP uses the MAC address of the host to determine which virtual MAC address to direct the host to use. This algorithm guarantees that a host gets the same virtual MAC address if the number of virtual forwarders does not change.
Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/unicast/configuration/guide/l3_cli_nxos/l3_glbp.html

Question: 8

Which three items must be configured in the port profile client in Cisco UCS Manager? (Choose three.)

A. port profile
B. DVS
C. data center
D. folder
E. vCenter IP address
F. VM port group

Answer: B, C, D

Explanation:
After associating an ESX host to a DVS, you can migrate existing VMs from the vSwitch to the DVS, and you can create VMs to use the DVS instead of the vSwitch. With the hardware-based VN-Link implementation, when a VM uses the DVS, all VM traffic passes through the DVS and ASIC-based switching is performed by the fabric interconnect.

In Cisco UCS Manager, DVSes are organized in the following hierarchy:

```
vCenter
  Folder (optional)
    Datacenter
      Folder (required)
        DVS
```

At the top of the hierarchy is the vCenter, which represents a VMware vCenter instance. Each vCenter contains one or more datacenters, and optionally vCenter folders with which you can organize the datacenters. Each datacenter contains one or more required datacenter folders. Datacenter folders contain the DVSes.

Reference:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/gui/config/guide/1-3-1/b_UCSM_GUI_Configuration_Guide_1_3_1/UCSM_GUI_Configuration_Guide_1_3_1_chapter28.html

Question: 9

Refer to the command below. When configuring an SVS connection on the Cisco Nexus 5000 Series Switch, which device is being referenced as the remote IP address?

```
nexus5500-2(config-svs-conn)# remote ip address 10.10.1.15 port 80 vrf management
```

A. ESX or ESXi host
B. vCenter
C. vPC peer switch
D. Cisco IMC management

Answer: B

Explanation:

This command specifies the hostname or IP address for the vCenter Server. Optionally, specifies the port number and VRF.

Reference:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5500/sw/layer2/6x/b_5500_Layer2_Config_6x/b_5500_Layer2_Config_602N12_chapter_010000.html

Question: 10

On a Cisco Nexus 7000 Series router, which statement about HSRP and VRRP is true?

A. When VDCs are in use, only VRRP is supported.
B. HSRP and VRRP both use the same multicast IP address with different port numbers.
C. HSRP has shorter default hold and hello times.
D. The VRRP group IP address can be the same as the router-specific IP address.

Answer: D

Explanation:

VRRP allows for transparent failover at the first-hop IP router by configuring a group of routers to share a virtual IP address. VRRP selects a master router in that group to handle all packets for the virtual IP address. The remaining routers are in standby and take over if the master router fails.
Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/unicast/configuration/guide/l3_cli_nxos/l3_vrrp.html

Question: 11

Which protocol is the foundation for unified fabric as implemented in Cisco NX-OS?

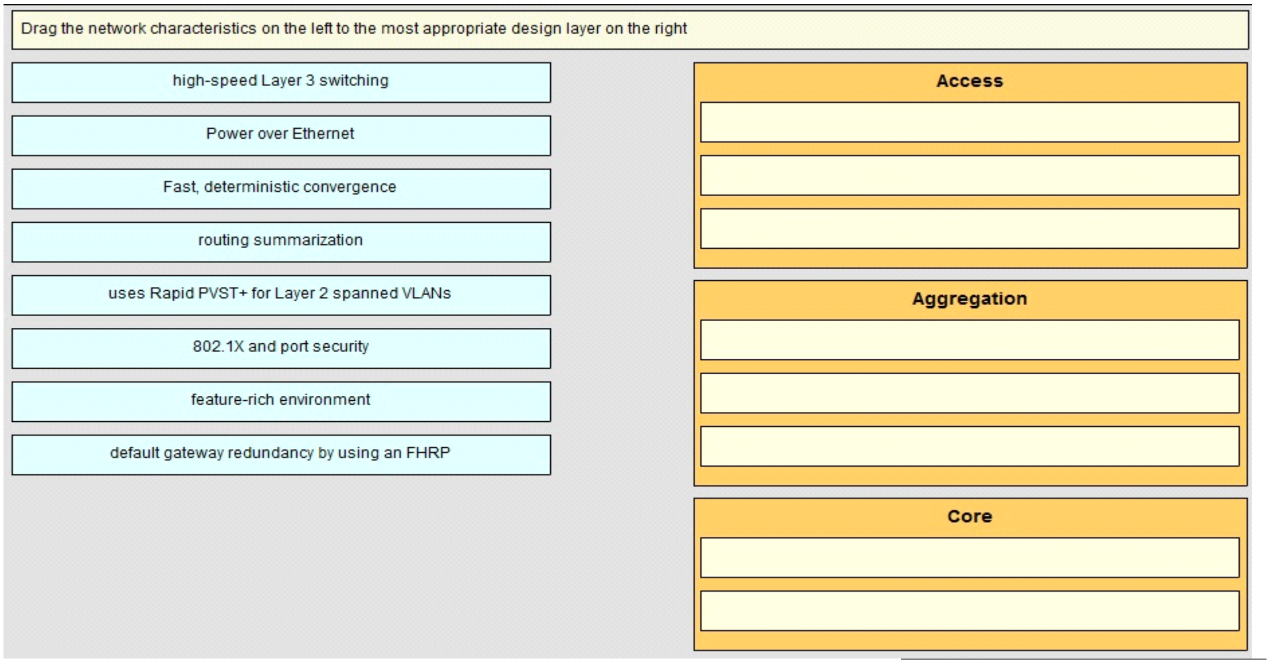
A. Fibre Channel
B. Data Center Bridging
C. Fibre Channel over Ethernet
D. N proxy virtualization
E. N Port identifier virtualization

Answer: C

Explanation:
Fibre Channel over Ethernet (FCoE) is one of the major components of a Unified Fabric. FCoE is a new technology developed by Cisco that is standardized in the Fibre Channel Backbone 5 (FC-BB-5) working group of Technical Committee T11 of the International Committee for Information Technology Standards (INCITS). Most large data centers have huge installed bases of Fibre Channel and want a technology that maintains the Fibre Channel model. FCoE assumes a lossless Ethernet, in which frames are never dropped (as in Fibre Channel) and that therefore does not use IP and TCP.
Reference:
http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/white_paper_c11-495142.html

Question: 12

DRAG DROP
Drag the network characteristics on the left to the most appropriate design layer on the right.



Drag the network characteristics on the left to the most appropriate design layer on the right

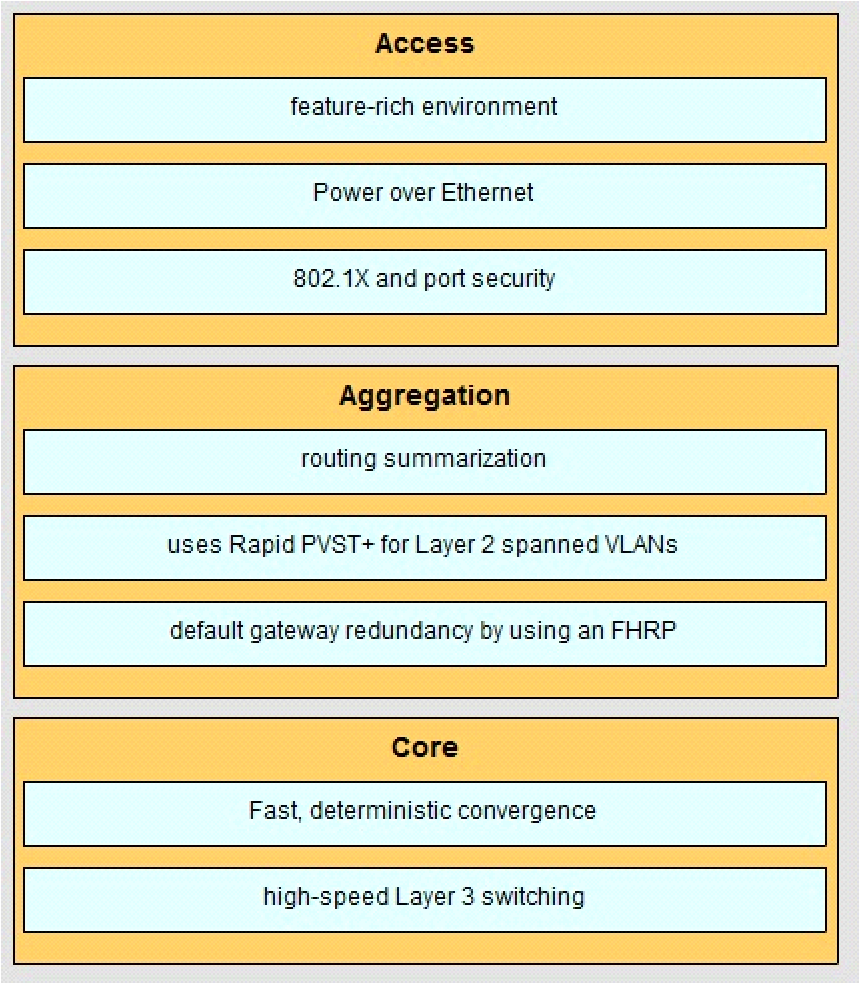
- high-speed Layer 3 switching
- Power over Ethernet
- Fast, deterministic convergence
- routing summarization
- uses Rapid PVST+ for Layer 2 spanned VLANs
- 802.1X and port security
- feature-rich environment
- default gateway redundancy by using an FHRP

Access

Aggregation

Core

Answer:



Access

- feature-rich environment
- Power over Ethernet
- 802.1X and port security

Aggregation

- routing summarization
- uses Rapid PVST+ for Layer 2 spanned VLANs
- default gateway redundancy by using an FHRP

Core

- Fast, deterministic convergence
- high-speed Layer 3 switching

Explanation:

The access layer is the first tier or edge of the campus. It is the place where end devices (PCs, printers, cameras, and the like) attach to the wired portion of the campus network. It is also the place where devices that extend the network out one more level are attached—IP phones and wireless access points (APs) being the prime two key examples of devices that extend the connectivity out one more layer from the actual campus access switch. The wide variety of possible types of devices that can connect and the various services and dynamic configuration mechanisms that are necessary, make the access layer one of the most feature-rich parts of the campus network.

You can enable an 802.1X port for port security by using the dot1x multiple-hosts interface configuration command. You must also configure port security on the port by using the switchport port-security interface configuration command. With the multiple-hosts mode enabled, 802.1X authenticates the port, and port security manages network access for all MAC addresses, including that of the client. You can then limit the number or group of clients that can access the network through an 802.1X multiple-host port.

Question: 13

Which statement about RBAC user roles on a Cisco Nexus switch is true?

A. If you belong to multiple roles, you can execute only the commands that are permitted by both roles (logical AND).
B. Access to a command takes priority over being denied access to a command.
C. The predefined roles can only be changed by the network administrator (superuser).
D. The default SAN administrator role restricts configuration to Fibre Channel interfaces.
E. On a Cisco Nexus 7000 Series Switch, roles are shared between VDCs.

Answer: B

Explanation:
If you belong to multiple roles, you can execute a combination of all the commands permitted by these roles. Access to a command takes priority over being denied access to a command. For example, suppose a user has RoleA, which denied access to the configuration commands. However, the users also have RoleB, which has access to the configuration commands. In this case, the users have access to the configuration commands.
Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLI ConfigurationGuide/sec_rbac.html

Question: 14

Which statement is true if password-strength checking is enabled?

A. Short, easy-to-decipher passwords will be rejected.
B. The strength of existing passwords will be checked.
C. Special characters, such as the dollar sign ($) or the percent sign (%), will not be allowed.
D. Passwords become case-sensitive.

Answer: A

Explanation:
If a password is trivial (such as a short, easy-to-decipher password), the cisco NX_OS software will reject your password configuration if password-strength checking is enabled. Be sure to configure a strong password. Passwords are case sensitive.
Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_7x_chapter_01000.pdf

Question: 15

When a local RBAC user account has the same name as a remote user account on an AAA server, what happens when a user with that name logs into a Cisco Nexus switch?

A. The user roles from the remote AAA user account are applied, not the configured local user roles.
B. All the roles are merged (logical OR).
C. The user roles from the local user account are applied, not the remote AAA user roles.
D. Only the roles that are defined on both accounts are merged (logical AND).

Answer: C

Explanation:
If you have a user account configured on the local Cisco NX-OS device that has the same name as a remote user account on an AAA server, the Cisco NX-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.
Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_rbac.html