



- Expert Verified, Online, **Free**.

Custom View Settings

Question #1003

Topic 1

How does Chef configuration management enforce a required device configuration?

- A. The Chef Infra Server uses its configured cookbook to push the required configuration to the remote device requesting updates.
- B. The installed agent on the device connects to the Chef Infra Server and pulls its required configuration from the cookbook.
- C. The Chef Infra Server uses its configured cookbook to alert each remote device when it is time for the device to pull a new configuration.
- D. The installed agent on the device queries the Chef Infra Server and the server responds by pushing the configuration from the cookbook.

Correct Answer: D

Community vote distribution

B (94%) 6%

 **sdmejia01** Highly Voted 3 months, 2 weeks ago

Selected Answer: B

I think the answer is B. The client pulls the configuration from the server. Check the Chef section here:
<https://study-ccna.com/configuration-management-tools-ansible-chef-puppet/>

upvoted 7 times

 **Bhrino** Most Recent 2 days ago

Selected Answer: B

chef is a pull
upvoted 1 times

 **Bhrino** 2 weeks, 4 days ago

Selected Answer: B

the answer is b because it is agentful and its a pull not a push
upvoted 1 times

 **Ciscoman021** 2 months, 2 weeks ago

Selected Answer: B

Chef configuration management enforces a required device configuration by using an installed agent on the device that connects to the Chef Infra Server and pulls the required configuration from the cookbook.

In Chef, a cookbook is a collection of recipes, attributes, templates, and other configuration files that define a desired configuration for a specific device or group of devices. The Chef Infra Server stores the cookbook, and the installed agent on each device periodically checks in with the server to see if there are any updates to the cookbook.

If an update is available, the agent pulls the updated cookbook from the server and applies the new configuration to the device. This process is known as "pull-based" configuration management, where the devices actively request updates from the server.

Therefore, option B, "The installed agent on the device connects to the Chef Infra Server and pulls its required configuration from the cookbook", is the correct answer.

upvoted 2 times

 **nawzat** 3 months ago

know which one is correct, please?
upvoted 1 times

 **Goena** 3 months, 3 weeks ago

Selected Answer: B

Sorry, the correct answer is B.
The device pulls the configuration from the cookbook.
upvoted 4 times

✉  **Goena** 3 months, 3 weeks ago

Selected Answer: A

Answer is A:

In Chef, Nodes are dynamically updated with the configurations in the Server. This is called Pull Configuration which means that we don't need to execute even a single command on the Chef server to push the configuration on the nodes, nodes will automatically update themselves with the configurations present in the Server.

upvoted 1 times

✉  **purenukeR** 1 month, 3 weeks ago

And how the server pushes the configuration ?

upvoted 1 times

Question #1004

Topic 1

What is the PUT method within HTTP?

- A. It replaces data at the destination.
- B. It is a nonidempotent operation.
- C. It is a read-only operation.
- D. It displays a web site.

Correct Answer: A

✉  **Bhrino** 2 weeks, 4 days ago

Replaces is synonymous to update in the CRUD model

Create
Read
Update
Delete

it matches up

upvoted 1 times

✉  **mageknight** 3 months, 2 weeks ago

put=update in restfull operation

upvoted 1 times

Question #1005

Topic 1

Which advantage does the network assurance capability of Cisco DNA Center provide over traditional campus management?

- A. Cisco DNA Center leverages YANG and NETCONF to assess the status of fabric and nonfabric devices, and traditional campus management uses CLI exclusively.
- B. Cisco DNA Center handles management tasks at the controller to reduce the load on infrastructure devices, and traditional campus management uses the data backbone.
- C. Cisco DNA Center automatically compares security postures among network devices, and traditional campus management needs manual comparisons.
- D. Cisco DNA Center correlates information from different management protocols to obtain insights, and traditional campus management requires manual analysis.

Correct Answer: A

Community vote distribution

D (100%)

 **sdmejia01** Highly Voted  3 months, 2 weeks ago

I would go with D.

<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-06-cisco-dna-assurance-technical-ebook-cte-en.pdf>

upvoted 9 times

 **oatmealturkey** 3 months, 2 weeks ago

I agree

upvoted 4 times

 **Ciscoman021** Highly Voted  2 months ago

Selected Answer: D

The correct answer is D. Cisco DNA Center correlates information from different management protocols to obtain insights, and traditional campus management requires manual analysis.

The network assurance capability of Cisco DNA Center provides an advantage over traditional campus management by automatically correlating information from different management protocols to obtain insights into the performance, health, and security of the network. This allows for quicker and more efficient troubleshooting and problem resolution.

upvoted 6 times

 **JY888** Most Recent  3 weeks, 4 days ago

Selected Answer: D

The advantage that the network assurance capability of Cisco DNA Center provides over traditional campus management is:

D. Cisco DNA Center correlates information from different management protocols to obtain insights, and traditional campus management requires manual analysis.

Explanation:

Network assurance refers to the process of proactively monitoring and optimizing network performance to ensure that applications and services are delivered reliably and efficiently. Cisco DNA Center provides advanced network assurance capabilities that go beyond the capabilities of traditional campus management systems.

upvoted 1 times

Question #1006

Topic 1

```
{  
    "myCar": {  
        "name": "thunder",  
        "wheels": ["good", "good", "pressureLow", "warning"],  
        "gasLight": false  
    },  
    "oldCar": {  
        "name": "sleepy",  
        "wheels": ["pressureLow", "pressureLow", "pressureLow", "pressureLow"],  
        "color": "rust"  
        "gasLight": true  
    },  
    "newCar": {  
        "name": "lightning",  
        "wheels": ["pressureLow", "good", "pressureLow", "good"],  
        "color": "blue"  
        "gasLight": true  
    }  
}
```

Refer to the exhibit. In which structure does the word “warning” directly reside?

- A. array
- B. object
- C. Boolean
- D. string

Correct Answer: B

Community vote distribution

A (100%)

 **ukguy** Highly Voted 3 months, 2 weeks ago

array is right answer
upvoted 10 times

 **Rynurr** Highly Voted 3 months, 2 weeks ago

Selected Answer: A
Definitely array, so "A" is the correct answer.
upvoted 8 times

 **Vikramaditya_J** Most Recent 3 weeks, 5 days ago

Selected Answer: A
Answer is A. Of course everything resides within an Object in JSON, but the question here asks about where does it “directly” reside, then the word “warning” clearly residing in an array, and not in object.
upvoted 2 times

 **DINVIS** 3 months ago

it's ARRAY
upvoted 2 times

 **gewe** 3 months, 2 weeks ago

why not array?
upvoted 4 times

Question #1007

Topic 1

What is the purpose of a southbound API in a controller-based networking architecture?

- A. facilitates communication between the controller and the applications
- B. allows application developers to interact with the network
- C. integrates a controller with other automation and orchestration tools
- D. facilitates communication between the controller and the networking hardware

Correct Answer: D

 **studying_1** 6 days, 10 hours ago

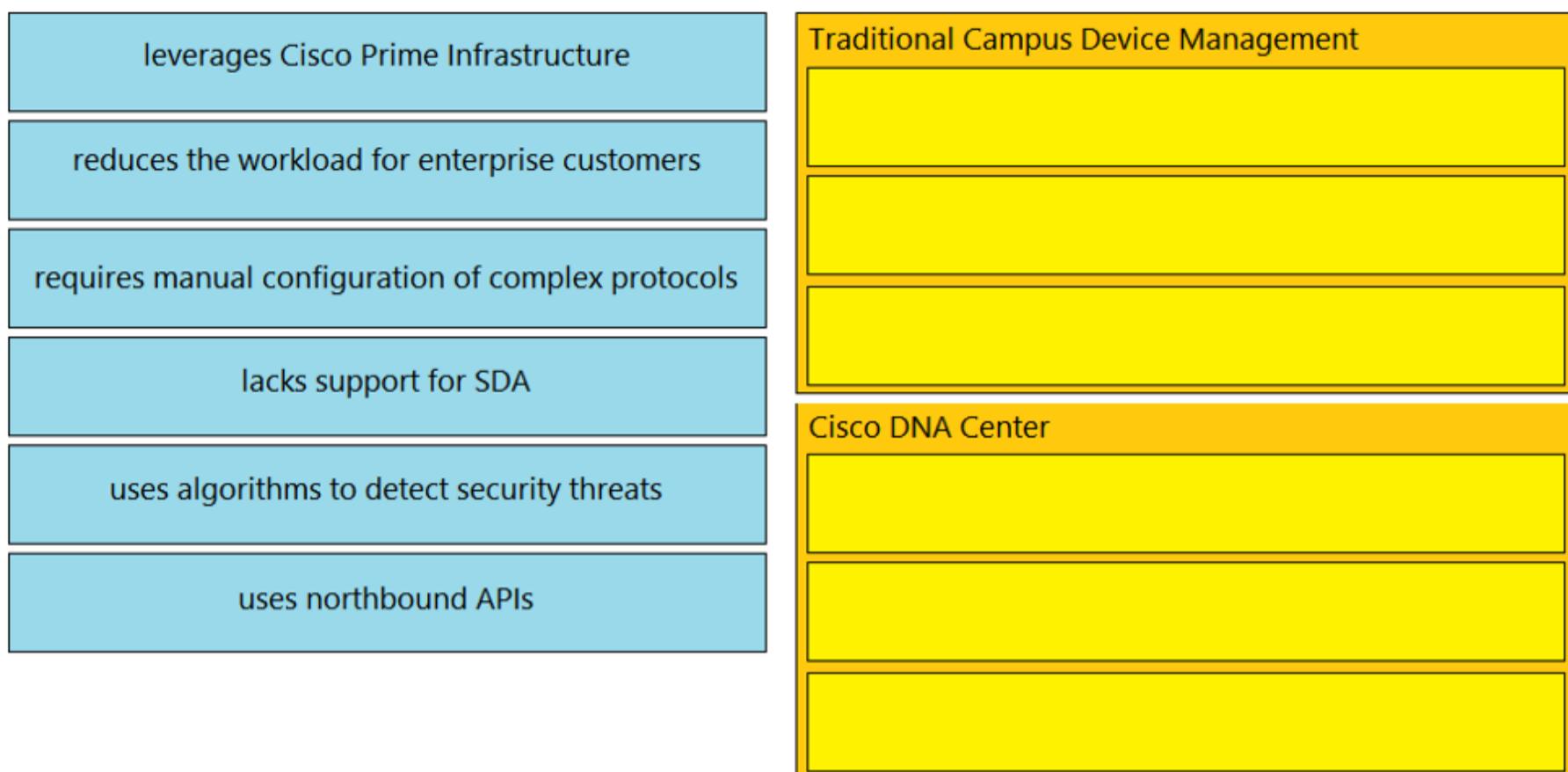
answer is correct

upvoted 2 times

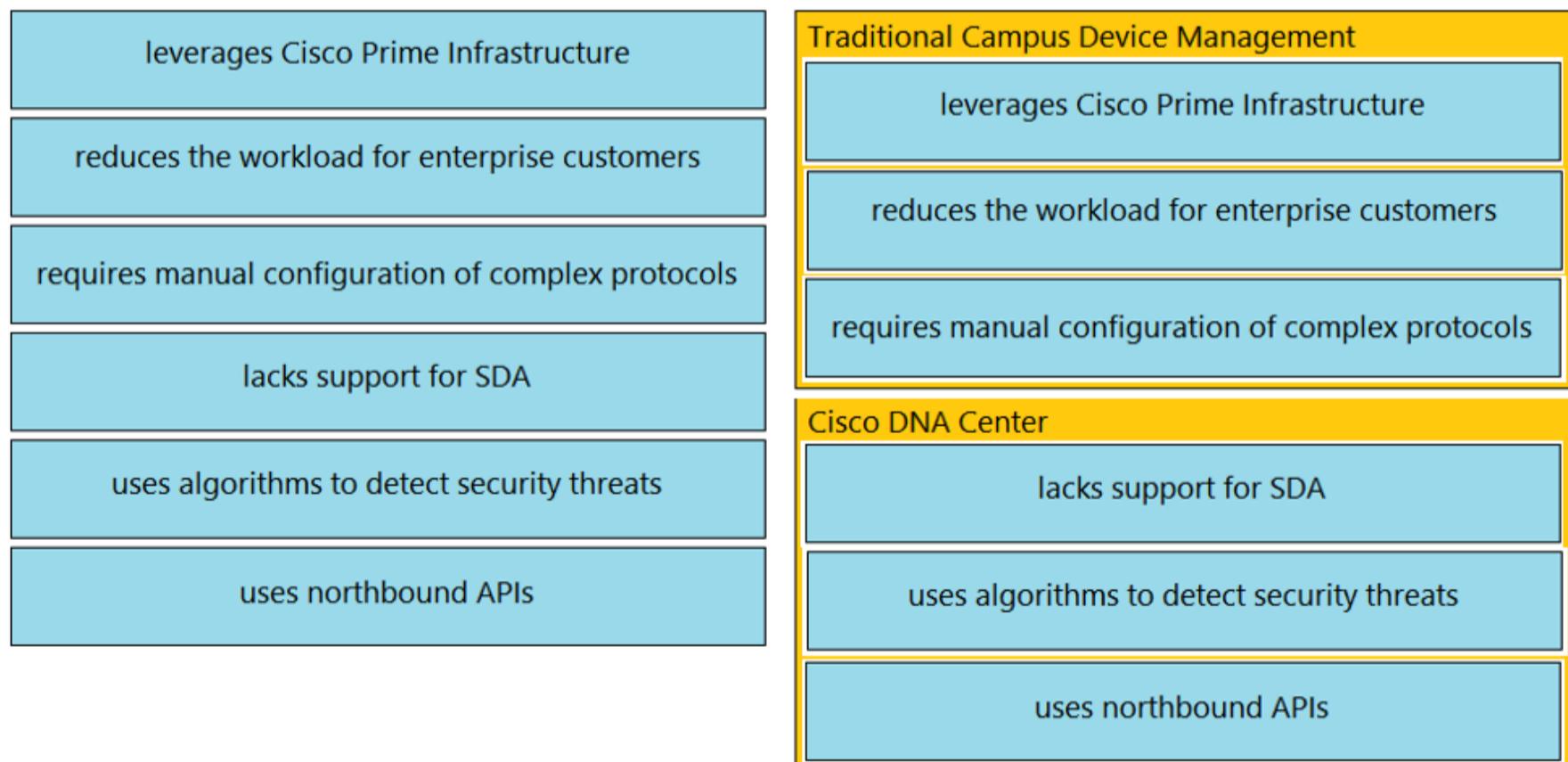
Question #1008

DRAG DROP

Drag and drop the statements about device management from the left onto the corresponding types on the right.



Correct Answer:



✉ **sdmejia01** Highly Voted 3 months, 2 weeks ago

I think reduce the workload for enterprise customers and Supports SDA should be switched. Correct me if I am wrong please.
upvoted 16 times

✉ **oatmealturkey** 3 months, 2 weeks ago

You are correct
<https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/index.html>
upvoted 4 times

✉ **HM01** Most Recent 4 days, 18 hours ago

A. REST (Representational State Transfer)
D. NETCONF (Network Configuration Protocol)

REST is a widely used architectural style for designing networked applications, and it is commonly used as a northbound API in SDN environments.

It provides a simple and lightweight approach for application developers to interact with the SDN controller.

NETCONF is a network management protocol that allows for the configuration and management of network devices. It is often used as a northbound API in SDN to provide a standardized interface for applications to configure and control network elements.

OpenFlow, SOAP, and OpFlex are not typically categorized as northbound APIs. OpenFlow is a southbound API that allows communication between the SDN controller and network switches. SOAP (Simple Object Access Protocol) is a protocol for exchanging structured information in web services and is not specific to SDN. OpFlex is a southbound protocol used in Cisco's Application Centric Infrastructure (ACI) and is not a widely adopted northbound API in the general SDN ecosystem.

upvoted 1 times

 **Dutch012** 2 months, 3 weeks ago

I think traditional:

- require.
- use
- lack

upvoted 1 times

 **ukguy** 3 months, 2 weeks ago

agreed

upvoted 1 times

Question #1009

Topic 1

Which two northbound APIs are found in a software-defined network? (Choose two.)

- A. REST
- B. OpenFlow
- C. SOAP
- D. NETCONF
- E. OpFlex

Correct Answer: AD

Community vote distribution

AC (93%)

7%

 **oatmealturkey** Highly Voted  3 months, 2 weeks ago

Selected Answer: AC

NETCONF is a Southbound API used to configure network devices.

<https://ipcisco.com/lesson/netconf-overview/#:~:text=NETCONF%20Protocol%20is%20used%20in,Plane%20and%20the%20Control%20Plane>.

upvoted 8 times

 **HM01** Most Recent  4 days, 18 hours ago

- A. REST (Representational State Transfer)
- D. NETCONF (Network Configuration Protocol)

REST is a widely used architectural style for designing networked applications, and it is commonly used as a northbound API in SDN environments. It provides a simple and lightweight approach for application developers to interact with the SDN controller.

NETCONF is a network management protocol that allows for the configuration and management of network devices. It is often used as a northbound API in SDN to provide a standardized interface for applications to configure and control network elements.

OpenFlow, SOAP, and OpFlex are not typically categorized as northbound APIs. OpenFlow is a southbound API that allows communication between the SDN controller and network switches. SOAP (Simple Object Access Protocol) is a protocol for exchanging structured information in web services and is not specific to SDN. OpFlex is a southbound protocol used in Cisco's Application Centric Infrastructure (ACI) and is not a widely adopted northbound API in the general SDN ecosystem.

upvoted 1 times

 **hamish88** 1 month, 2 weeks ago

Simple Object Access Protocol (SOAP) is considered an alternate technology to REST for API access.

upvoted 1 times

 **liviuml** 1 month, 2 weeks ago

Selected Answer: AC

SOAP is northbound

https://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.2/north_bound_api/developers/guide/websvc.html
Regards

upvoted 1 times

 **Leethy** 1 month, 4 weeks ago

Selected Answer: AD

- A. REST
- D. NETCONF

In a software-defined network (SDN), northbound APIs are used for communication between the SDN controller and higher-level applications or management systems. Two common northbound APIs are:

- A. REST (Representational State Transfer) - a lightweight, web-based API that uses standard HTTP methods for communication.
- D. NETCONF (Network Configuration Protocol) - an XML-based protocol used for managing network devices, including configuration, monitoring, and administration.

upvoted 1 times

 **Rynurr** 3 months, 2 weeks ago

Selected Answer: AC

Yeah, API and SOAP are correct answers.

upvoted 4 times

Question #1010

Topic 1

Which function generally performed by a traditional network device is replaced by a software-defined controller?

- A. building route tables and updating the forwarding table
- B. encapsulation and decapsulation of packets in a data-link frame
- C. changing the source or destination address during NAT operations
- D. encryption and decryption for VPN link processing

Correct Answer: D

Community vote distribution

A (100%)

 **oatmealturkey** Highly Voted  3 months, 2 weeks ago

Selected Answer: A

Answer is A, every other choice is a function of the data plane.

<https://www.ciscopress.com/articles/article.asp?p=2995354&seqNum=2>

upvoted 12 times

 **Bhrino** Most Recent  2 weeks, 4 days ago

Selected Answer: A

in most cases it really automates most things like making things that would take hours to do done either instantly or at least a fraction of the time
ie updating routing

upvoted 1 times

 **mrmanistheman** 3 weeks, 3 days ago

Selected Answer: A

Answer is A

upvoted 1 times

 **lucantonelli93** 3 months, 1 week ago

Selected Answer: A

The correct answer it's A

upvoted 4 times

 **Rynurr** 3 months, 1 week ago

Selected Answer: A

Looks like "A" is the correct answer

upvoted 4 times

 **mageknight** 3 months, 2 weeks ago

In some cases, both the data plane and control plane can be used to implement encryption and decryption for VPN link processing. Overall, the building of route tables and updating of forwarding tables are important functions in an SDN architecture, and are typically handled by the controller in the control plane. This allows for more efficient and flexible management of the network, and can enable a wide range of network automation and optimization techniques.

upvoted 3 times

 **sdmejia01** 3 months, 2 weeks ago

I think answer is D.

upvoted 1 times

Question #1011

Topic 1

What describes a northbound REST API for SDN?

- A. network-element-facing interface for GET, POST, PUT, and DELETE methods
- B. application-facing interface for SNMP GET requests
- C. application-facing interface for GET, POST, PUT, and DELETE methods
- D. network-element-facing interface for the control and data planes

Correct Answer: C

Question #1012

Topic 1

When is the PUT method used within HTTP?

- A. to update a DNS server
- B. when a nonidempotent operation is needed
- C. to display a web site
- D. when a read-only operation is required

Correct Answer: B

 oatmealturkey Highly Voted  3 months, 3 weeks ago

Selected Answer: A

Please correct.

"Standard REST methods are supported on the API, which includes POST, GET, PUT, and DELETE operations through HTTP. The PUT methods are idempotent, meaning that there is no additional effect if they are called more than once with the same input parameters. The GET method is nullipotent, meaning that it can be called zero or more times without making any changes (or that it is a read-only operation)."

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/aci_multi-site/sw/1x/rest_api_config/b_Cisco_ACI_Multi-Site_REST_Configuration_Guide/b_Cisco_ACI_Multi-Site_REST_Config_Guide_chapter_01.pdf
upvoted 7 times

 Ciscoman021 Most Recent  2 months, 2 weeks ago

Selected Answer: A

The PUT method is used within HTTP when a client wants to update an existing resource on the server. Therefore, the correct option is A: to update a resource on a server.

The PUT method is a part of the HTTP protocol that allows a client to update or replace a resource on the server with a new version. It is an idempotent operation, which means that making multiple identical requests has the same effect as making a single request.

The other options are incorrect:

- B. The PUT method is not used for non-idempotent operations; it is used for idempotent operations.
- C. The GET method is typically used to display a web site.
- D. The GET method is used for read-only operations, not the PUT method.

upvoted 3 times

 Rynurr 3 months, 1 week ago

Selected Answer: A

"B" is incorrect > NON-IDEMPOTENT: If an operation always causes a change in state, like POSTing the same message to a user over and over, resulting in a new message sent and stored in the database every time.

Must be "A".

upvoted 1 times

Question #1013

Topic 1

Which two HTTP methods are suitable for actions performed by REST-based APIs? (Choose two.)

- A. REMOVE
- B. REDIRECT
- C. POST
- D. GET
- E. POP

Correct Answer: CD

 **DINVIS** 3 months ago

right answers
upvoted 3 times

 **sdmejia01** 3 months, 2 weeks ago

Selected Answer: CD

C and D are correct!
upvoted 4 times

Question #1014

Topic 1

What is the advantage of separating the control plane from the data plane within an SDN network?

- A. limits data queries to the control plane
- B. reduces cost
- C. decreases overall network complexity
- D. offloads the creation of virtual machines to the data plane

Correct Answer: D

 **sdmejia01** Highly Voted  3 months, 2 weeks ago

I would go with C.
upvoted 10 times

 **Ciscoman021** Highly Voted  2 months, 2 weeks ago

Selected Answer: C

C is best answer.
Overall, separating the control plane from the data plane within an SDN network provides greater control, flexibility, scalability, and security, making it an ideal solution for large, complex, and dynamic networks.
upvoted 6 times

 **JY888** Most Recent  2 months, 4 weeks ago

Selected Answer: A

It reduces the cost form manpower with SDN period but that is not the question. It will minimize configuration but the network will still be complex. Virtual machines are going to be created from a management plane. Data is confined to the control plane and below. I vote A.
upvoted 2 times

 **Dutch012** 3 months ago

C seems the most logical answers
upvoted 3 times

 **Dutch012** 3 months ago

answer*
upvoted 1 times

 **mageknight** 3 months, 2 weeks ago

I would go with B
upvoted 3 times

 **ac891** 4 weeks ago

keep thinking ...
upvoted 1 times

Question #1015

Topic 1

```
{  
"Cisco Devices": [  
{  
"name": "ASA - Security Device",  
"name": "Cisco 1100 ASR Router",  
"name": "Cisco 6800 Switch"  
}  
]
```

Refer to the exhibit. What is missing from this output for it to be executed?

- A. double quotes (" ") around the "Cisco Devices" string
- B. exclamation point (!) at the beginning of each line
- C. square bracket ([) at the beginning
- D. curly braket ({) at the end

Correct Answer: D

 ac891 3 weeks, 2 days ago

easiest question without having a knowledge
upvoted 4 times

Question #1016

Topic 1

What is a function of a northbound API in an SDN environment?

- A. It relies on global provisioning and configuration.
- B. It upgrades software and restores files.
- C. It supports distributed processing for configuration.
- D. It provides orchestration and network automation services.

Correct Answer: D

 Goena  3 months, 1 week ago

Selected Answer: D

Answer D is correct:

Software-Defined Networking (SDN) – is a higher level of network orchestration. It was originally intended to separate the control-plane and data-plane to enable higher operational efficiency in networking layer devices through programmable forwarding tables (like via the OpenFlow protocol)
upvoted 5 times

Question #1017

Topic 1

What is an Ansible inventory?

- A. unit of Python code to be executed within Ansible
- B. file that defines the target devices upon which commands and tasks are executed
- C. device with Ansible installed that manages target devices
- D. collection of actions to perform on target devices, expressed in YAML format

Correct Answer: B

 **studying_1** 4 weeks ago

B is correct

upvoted 2 times

 **beerbisceps1** 2 months ago

B is correct

upvoted 2 times

 **zamkljo** 2 months ago

Selected Answer: B

for sure B

upvoted 2 times

 **bisiyemo1** 2 months, 4 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **bisiyemo1** 1 month, 1 week ago

Bis correct please

upvoted 2 times

 **ike110** 3 months, 1 week ago

Selected Answer: B

D can't be correct as that's PLAYBOOK

Inventory is where Ansible only stores hosts and groups of hosts, upon which commands/modules/tasks in a playbook operate

upvoted 3 times

 **UAE7** 3 months, 1 week ago

D is correct

upvoted 2 times

 **sang33** 3 months, 2 weeks ago

Selected Answer: D

Ansible uses YAML

upvoted 3 times

 **ike110** 3 months, 1 week ago

D is the answer for Ansible playbook

upvoted 3 times

Question #1018

DRAG DROP

Drag and drop the Ansible features from the left to the right. Not all features are used.

executes modules via SSH by default	feature
uses the YAML language	feature
uses agents to manage hosts	feature
pushes configurations to the client	feature
requires clients to pull configurations from the server	
operates without agents	

Correct Answer:

executes modules via SSH by default	executes modules via SSH by default
uses the YAML language	uses the YAML language
uses agents to manage hosts	pushes configurations to the client
pushes configurations to the client	operates without agents
requires clients to pull configurations from the server	
operates without agents	

 **Goena** Highly Voted 3 months, 1 week ago

Given answers are correct.

upvoted 5 times

Question #1019

Topic 1

What is a function of a northbound API?

- A. It relies on global provisioning and configuration.
- B. It upgrades software and restores files.
- C. It supports distributed processing for configuration.
- D. It provides a path between an SDN controller and network applications.

Correct Answer: A

 **sdmejia01** Highly Voted  3 months, 2 weeks ago

I would go with D.
upvoted 10 times

 **lucantonelli93** Highly Voted  3 months, 1 week ago

Selected Answer: D
For me it's D
upvoted 5 times

 **Bhrino** Most Recent  2 weeks, 4 days ago

Selected Answer: D
NBI allows communication between Controller and applications
SBI is the controller and data
upvoted 1 times

 **bisiyemo1** 1 month, 1 week ago

Selected Answer: D
D for sure
upvoted 2 times

 **beerbiseps1** 2 months ago

if it is not relying on global configuration in question 1016, how come it relies on global config in 1019?? The correct answer is D
upvoted 2 times

 **tal10** 3 months, 1 week ago

Selected Answer: D
d dddd
upvoted 4 times

 **Rynurr** 3 months, 1 week ago

Selected Answer: D
"D" for sure
upvoted 4 times

 **mageknight** 3 months, 2 weeks ago

the function of a northbound API is to provide a standard interface for higher-level network applications, services, and orchestration systems to interact with the SDN controller, enabling these applications to program the network and control network resources. It does not rely on global provisioning and configuration.
upvoted 2 times

Question #1020

Topic 1

```
{"apple": ["red", 1], "ripe": true}
```

Refer to the exhibit. What does apple represent within the JSON data?

- A. array
- B. object
- C. number
- D. string

Correct Answer: B

sdmejia01 Highly Voted 3 months, 2 weeks ago

apple represent a key which is not even in the answers.
upvoted 13 times

rogi2023 2 months ago

look at Q771 with comments. What is identified by the word apple - answer is key, But what represents the word apple - look the link <https://restfulapi.net/json-data-types/>
I would say, because it follows [] - so it is an array. Therefore answer A.
upvoted 1 times

rogi2023 2 months ago

and "ripe" represents Boolean
upvoted 2 times

mhayek 2 months, 4 weeks ago

100% agree
upvoted 1 times

oatmealturkey Highly Voted 3 months, 2 weeks ago

Selected Answer: D
The answer is D. string:
<https://restfulapi.net/json-data-types/>
upvoted 6 times

Bhrino Most Recent 2 weeks, 4 days ago

Selected Answer: D
anything thing in quotes are string which they could also be keys as well
upvoted 1 times

beerbiceps1 2 months ago

"" = string
upvoted 2 times

VictorCisco 2 months, 1 week ago

Selected Answer: A
It represents an array
upvoted 1 times

bisiyemo1 2 months, 4 weeks ago

Selected Answer: D
D is very correct
upvoted 1 times

bisiyemo1 2 months ago

A JSON string contains either an array of values, or an object (an associative array of name/value pairs). An array is surrounded by square brackets, [and] , and contains a comma-separated list of values. An object is surrounded by curly brackets, { and } , and contains a comma-separated list of name/value pairs.
upvoted 1 times

Dutch012 3 months ago

Selected Answer: A
Apple represents an array value, not a string, focus guys

upvoted 3 times

 **lucantonelli93** 3 months, 1 week ago

Selected Answer: D

It's D

upvoted 2 times

 **Rynurr** 3 months, 1 week ago

Selected Answer: D

That's string, so "D" is the correct answer.

upvoted 4 times

 **gewe** 3 months, 2 weeks ago

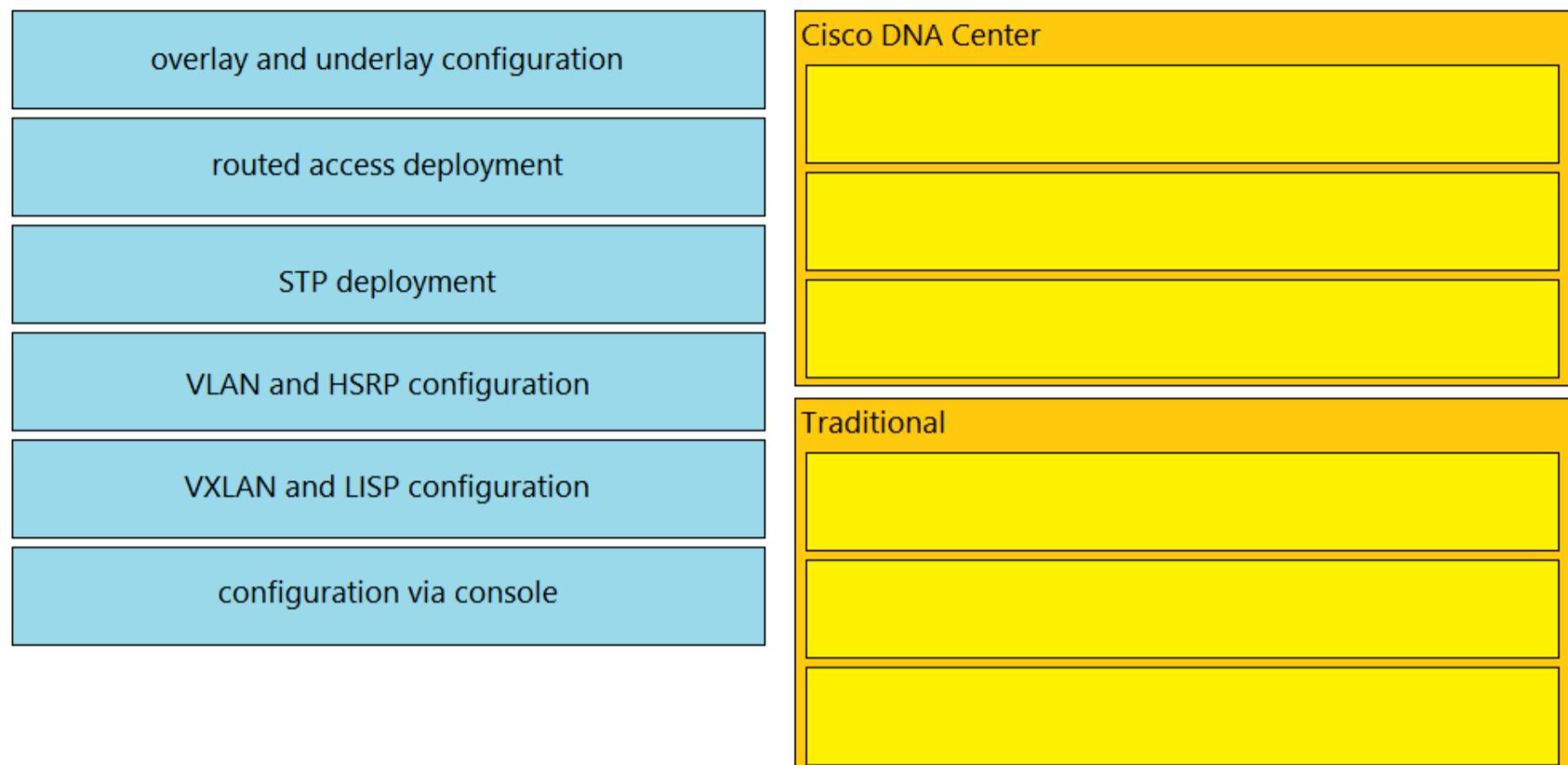
why not string<?

upvoted 3 times

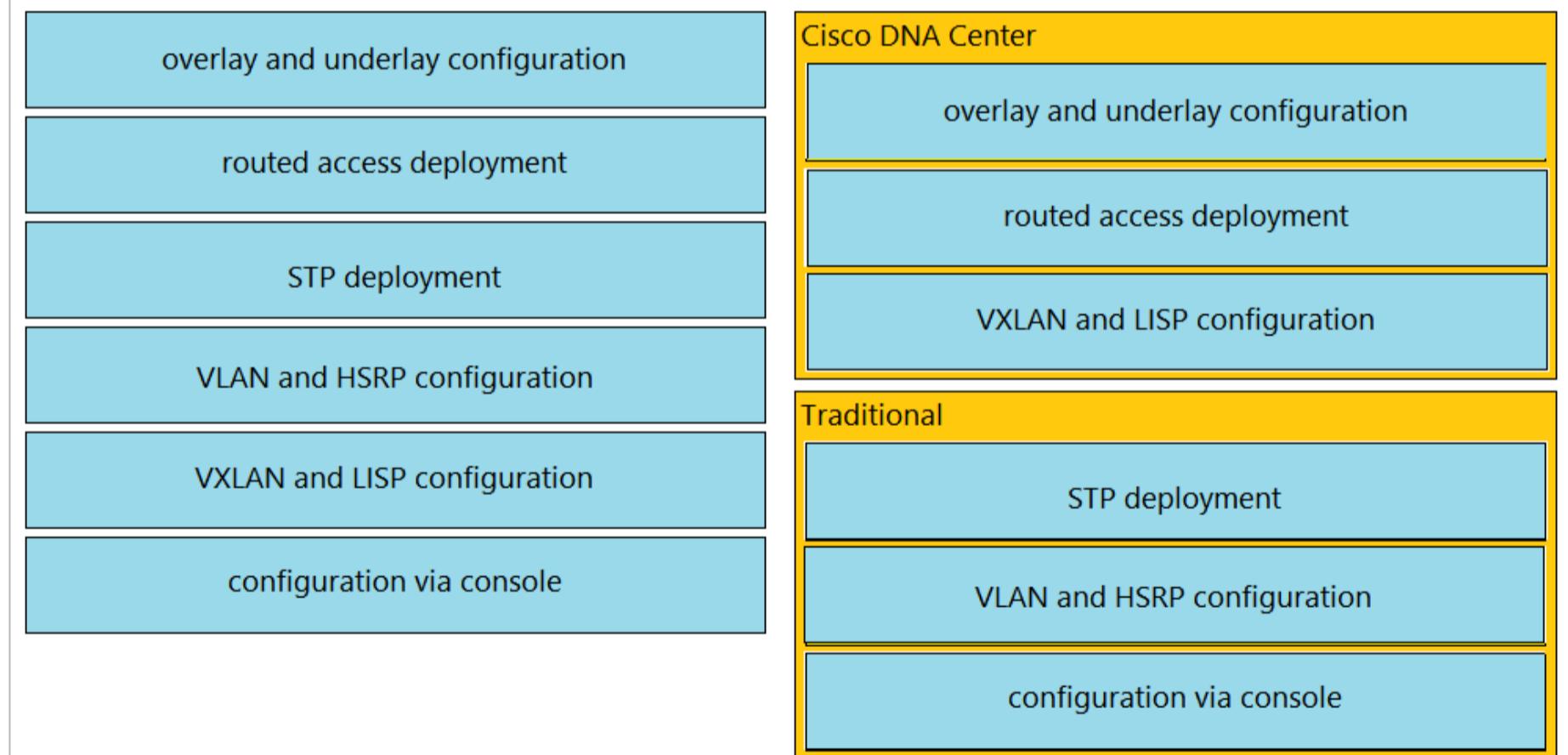
Question #1021

DRAG DROP

Drag and drop the use cases of device-management technologies from the left onto the corresponding types on the right.



Correct Answer:



RidzV 3 months ago

Correct answers
upvoted 4 times

Rydaz 4 weeks, 1 day ago

answers are wrong BIG TIME
DNA is VXLAN LSP
overlay underlay
config consol
Traditional is Routed Access
STP
VLan HSRP config
upvoted 1 times

studying_1 1 week, 2 days ago

Rydaz, in DNA all links between switches are routed ports, and stp is not needed to avoid loops, i guess given answer is correct
upvoted 1 times

ac891 2 weeks, 6 days ago
But traditional does have console, no ?
upvoted 1 times

Question #1022

Topic 1

Under the CRUD model, which two HTTP methods support the UPDATE operation? (Choose two.)

- A. PATCH
- B. DELETE
- C. GET
- D. POST
- E. PUT

Correct Answer: AE

Bhrino 2 weeks, 5 days ago
Selected Answer: AE
Create. Post
Read Get
Update Put,patch
Delete Delete
upvoted 1 times

UAE7 3 months, 1 week ago
answer is correct
upvoted 3 times

Question #1023

Topic 1

A network architect is considering whether to implement Cisco DNA Center to deploy devices on a new network. The organization is focused on reducing the time it currently takes to deploy devices in a traditional campus design. For which reason would Cisco DNA Center be more appropriate than traditional management options?

- A. Cisco DNA Center supports deployment with a single pane of glass.
- B. Cisco DNA Center provides zero-touch provisioning to third-party devices.
- C. Cisco DNA Center reduces the need for analytics on third-party access points and devices.
- D. Cisco DNA Center minimizes the level of syslog output when reporting on Cisco devices.

Correct Answer: A

  **JJY888**  2 months, 4 weeks ago

These questions are relying on knowledge of very minute details. Makes me not want to take the exam on principle.
upvoted 11 times

  **studying_1** 6 days, 9 hours ago

No, don't give up , you got this
upvoted 1 times

  **Tdawg1968** 1 week, 6 days ago

Welcome to the Cisco world. Got my first CCNA in 06 and it's been the same situation over all these years lol
upvoted 2 times

  **mageknight**  3 months, 2 weeks ago

The statement "Cisco DNA Center supports deployment with a single pane of glass" means that Cisco DNA Center provides a unified, centralized platform for managing and deploying network infrastructure. In other words, it offers a single point of access for managing all aspects of the network, such as network devices, applications, security policies, and network services.

The term "single pane of glass" is often used to describe a management tool that provides a unified view of multiple systems or components. In the context of network infrastructure, this means that instead of using separate tools to manage different parts of the network, such as switches, routers, wireless access points, and security appliances, network administrators can use Cisco DNA Center to manage them all from a single interface.

upvoted 11 times

Question #1024

DRAG DROP

Drag and drop the statements about device management from the left onto the corresponding device-management types on the right.

- It uses multiple tools and applications to analyze and troubleshoot different types of data.
- It manages device configurations on a per-device basis.
- It provides a single interface for network security and analytics.
- Security is managed near the perimeter of the network with firewalls, VPNs, and IPS.
- It supports CLI templates to apply a consistent configuration to multiple devices.
- It uses NetFlow to analyze potential security threats and take appropriate action on that traffic.

Cisco DNA Center Device Management

Traditional Device Management

Correct Answer:

- It uses multiple tools and applications to analyze and troubleshoot different types of data.
- It manages device configurations on a per-device basis.
- It provides a single interface for network security and analytics.
- Security is managed near the perimeter of the network with firewalls, VPNs, and IPS.
- It supports CLI templates to apply a consistent configuration to multiple devices.
- It uses NetFlow to analyze potential security threats and take appropriate action on that traffic.

Cisco DNA Center Device Management

It provides a single interface for network security and analytics.
It supports CLI templates to apply a consistent configuration to multiple devices.
It uses NetFlow to analyze potential security threats and take appropriate action on that traffic.

It manages device configurations on a per-device basis.
Security is managed near the perimeter of the network with firewalls, VPNs, and IPS.
It uses multiple tools and applications to analyze and troubleshoot different types of data.

✉  RidzV 3 months ago

I think Last answer for each section must be swapped.

Please correct me if I'm wrong.

upvoted 4 times

✉  fmaquino 1 month, 3 weeks ago

I agree. I would exchange the last of the Traditional with the first of DNA

upvoted 1 times

✉  ac891 4 weeks ago

But don't the DNA center use netflow ?

upvoted 3 times

✉  Rydaz 3 weeks, 5 days ago

they sure do, given answers are correct
upvoted 3 times

Question #1025

Topic 1

In a cloud-computing environment, what is rapid elasticity?

- A. control and monitoring or resource consumption by the tenant
- B. automatic adjustment of capacity based on need
- C. pooling resources in a multitenant model based on need
- D. self-service of computing resources by the tenant

Correct Answer: B

 **Goena** 3 months, 1 week ago

Selected Answer: B

Answer B is correct:

Rapid elasticity in cloud computing refers to the cloud's capability to scale quickly to meet demand. Consumers benefit from rapid elasticity because they can expand or reduce their resources how and when they would like.

upvoted 1 times

Question #1026

Topic 1

Which interface enables communication between a program on the controller and a program on the networking device?

- A. software virtual interface
- B. tunnel interface
- C. northbound interface
- D. southbound interface

Correct Answer: D

 **krzysiew** 2 weeks, 1 day ago

Selected Answer: D

The interface that enables communication between a program on the controller and a program on the networking device is typically referred to as a "southbound interface."

ChatGpt

upvoted 3 times

Question #1027

Topic 1

```
{  
    "Test_Questions" : [  
        "Automation",  
        "Configuration",  
    ],  
    "Test_Exam_Level" : [  
        "CCNA",  
        "CCNP",  
    ],  
    "Test_Response" : [  
        "Correct",  
        "Incorrect",  
    ]  
}
```

Refer to the exhibit. How many arrays are present in the JSON data?

- A. one
- B. three
- C. six
- D. nine

Correct Answer: B

✉  **jini4200** 2 months, 1 week ago

hey guys, why it's not six??

upvoted 1 times

✉  **beerbisceps1** 2 months ago

[] are used to wrap up arrays. therefore, 3

upvoted 3 times

Question #1028

DRAG DROP

Drag and drop the configuration management terms from the left onto the descriptions on the right. Not all terms are used.

agent	daemon that determines when the central authority has updates available
agentless	model in which the central server sends updates to nodes on an as-needed basis
provision	easy-to-manage deployment option that may lack scalability
pull	device hardware that runs without embedded management features
push	to automatically install or deploy a configuration or update
post	

Correct Answer:

agent	post
agentless	provision
provision	agentless
pull	pull
push	agent
post	

 **loco_desk** Highly Voted  2 months, 3 weeks ago

The correct order is

Agent
push
provision
agentless
post

upvoted 8 times

 **ac891** 3 weeks, 2 days ago

last one is pull
upvoted 1 times

 **bisiyemo1** 1 month, 1 week ago

This seems to be correct
upvoted 1 times

 **JY888** Most Recent  3 weeks, 4 days ago

My story and I am sticking to it: Agent
push
provision

agentless
pull

upvoted 1 times

✉ **iMo7ed** 1 month, 1 week ago

Agent - daemon that determines when the central authority has updates available
Push - model in which the central server sends updates to nodes on an as-needed basis
Provision - easy-to-manage deployment option that may lack scalability
Agentless - device hardware that runs without embedded management features
Pull - to automatically install or deploy a configuration or update

upvoted 2 times

✉ **jonathan126** 1 month, 1 week ago

daemon - Agent (e.g. puppet agent daemon)
central server - Push (e.g. ansible control node push configs to nodes)
easy-to-manage - Privison (not sure, I assume it means the provision of infrastructure without automation, which Ansible, Puppet and Chef have)
without embedded - agentless (e.g. Ansible)
automatically install - Pull (e.g. Puppet auto provision infrastructure from puppet master)

some source: <https://www.gspann.com/resources/blogs/puppet-vs-chef-vs-ansible/>

upvoted 1 times

✉ **Zortex** 2 months, 2 weeks ago

Agent - e (to automatically install or deploy a configuration or update)
Agentless - d (device hardware that runs without embedded management features)
Provision - c (easy to manage deployment option that may lack scalability)
Pull - b (model in which the central server sends updates to nodes on an as-needed basis)
Push - a (daemon that determines when central authority has updates available)

upvoted 1 times

✉ **JY888** 2 months, 4 weeks ago

I'm having a hard time finding the answers via Google. I hope I don't get this question.

upvoted 3 times

✉ **ike110** 3 months, 1 week ago

The following seems to be correct

agent
pull
push
agentless
provision

upvoted 2 times

✉ **Titan_intel** 3 months, 1 week ago

Can anyone confirm if this is correct?

upvoted 1 times

✉ **ike110** 3 months, 1 week ago

this is not correct

upvoted 4 times

Question #1029

Topic 1

Which interface type enables an application running on a client to send data over an IP network to a server?

- A. northbound interface
- B. application programming interface
- C. southbound interface
- D. Representational State Transfer application programming interface

Correct Answer: B

✉  **Friday_Night** 5 days, 20 hours ago

why not D - REST API ?

upvoted 1 times

✉  **JY888** 3 weeks, 4 days ago

Selected Answer: B

B again.

upvoted 1 times

✉  **Dutch012** 2 months, 3 weeks ago

I believe B

upvoted 1 times

✉  **bisiyemo1** 2 months, 3 weeks ago

Selected Answer: A

A is the correct answer

upvoted 1 times

✉  **JY888** 2 months, 4 weeks ago

Selected Answer: B

Correction.

upvoted 1 times

✉  **JY888** 2 months, 4 weeks ago

Selected Answer: A

API = Application Programmable Interface. Yes, it uses the Northbound interface but it is an API that is traveling over the Northbound.

upvoted 4 times

✉  **rmartin3444** 3 months ago

Shouldn't it be northbound?

upvoted 2 times

Question #1031

Topic 1

Which QoS feature drops traffic that exceeds the committed access rate?

- A. policing
- B. FIFO
- C. shaping
- D. weighted fair queuing

Correct Answer: A

 **studying_1** 6 days, 9 hours ago

Selected Answer: A

Answer is correct

upvoted 1 times

Question #1032

Topic 1

What does traffic shaping do?

- A. It queues excess traffic
- B. It sets QoS attributes within a packet
- C. It organizes traffic into classes
- D. It modifies the QoS attributes of a packet

Correct Answer: A

 **JY888** 3 weeks, 4 days ago

Selected Answer: A

How Does Traffic Shaping Work?

The first step in implementing an efficient traffic shaping system is categorizing the different kinds of traffic on the network.

For example, organizations may want to prioritize traffic to and from a key web application to ensure that no matter how busy the network gets, this important traffic is forwarded normally. What this means is that other kinds of traffic may be deprioritized. When this happens, the packets are simply held in a buffer until they can be forwarded without exceeding the total desired and configured rate.

Source: <https://www.f5.com/glossary/traffic-shaping#:~:text=Traffic%20shaping%20is%20a%20powerful,attacks%20from%20overwhelming%20network%20resources>.

upvoted 1 times

 **shiv3003** 1 month, 2 weeks ago

C is the answer

upvoted 1 times

 **ac891** 4 weeks ago

Thats QoS

upvoted 1 times

 **Goena** 3 months, 1 week ago

Selected Answer: A

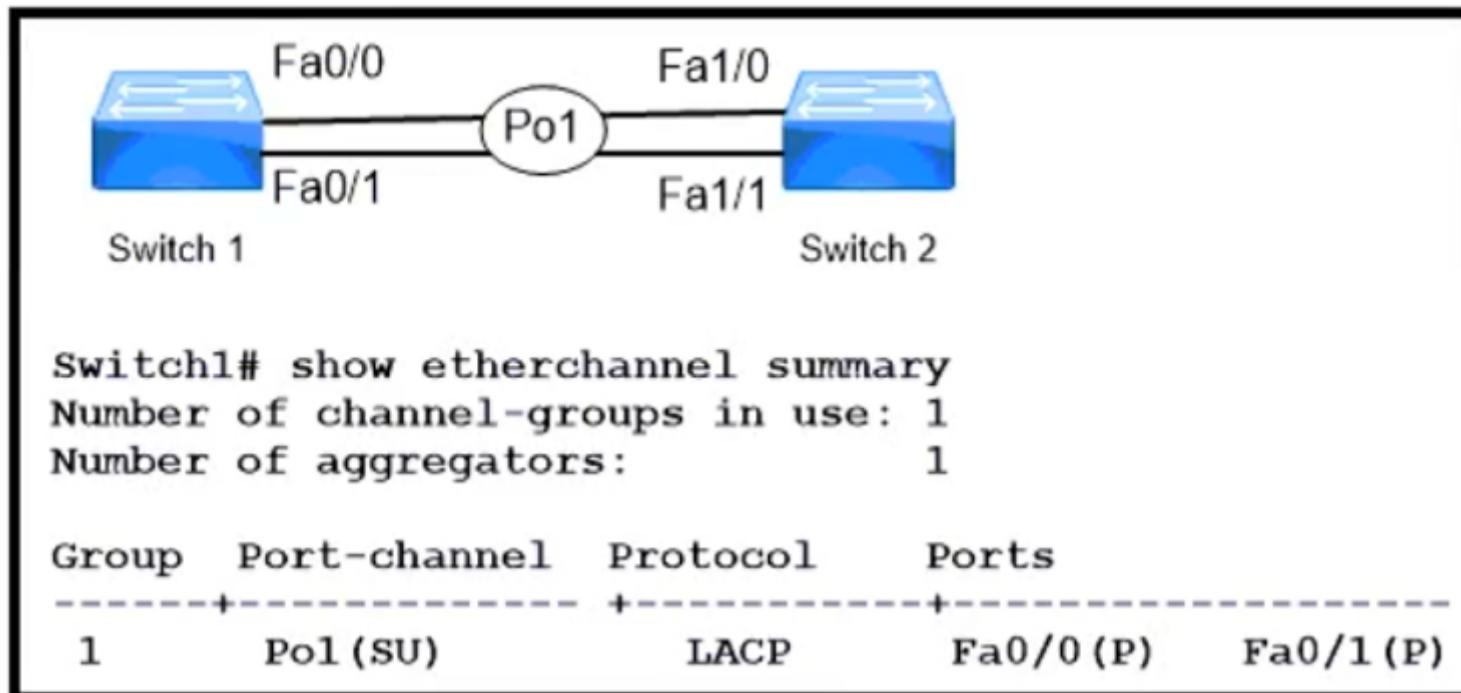
A is correct:

Traffic policing and traffic shaping have the following differences: Traffic policing directly discards packets with rates that are greater than the traffic policing rate. Traffic shaping, however, buffers packets with rates that are greater than the traffic shaping rate and sends the buffered packets at an even rate.

upvoted 4 times

Question #1033

Topic 1



Refer to the exhibit. A Cisco engineer is asked to update the configuration on switch 1 so that the EtherChannel stays up when one of the links fails. Which configuration meets this requirement?

- A. Switch1(config) # interface Fa0/0
Switch1(config-if) # lacp port-priority 100
Switch1(config) # interface Fa0/1
Switch1(config-if) # lacp port-priority 200
- B. Switch1(config) # interface port-channel 1
Switch1(config-if) # port-channel min-links 1
- C. Switch1(config) # interface Fa0/0
Switch1(config-if) # lacp port-priority 200
Switch1(config) # interface Fa0/1
Switch1(config-if) # lacp port-priority 100
- D. Switch1(config) # interface port-channel 1
Switch1(config-if) # lacp max-bundle 1

Correct Answer: B

ike110 3 months, 1 week ago

min-links command specifies the minimum number of interfaces that the configuration mode LAG requires to be active. If there are fewer ports than specified by this command, the port channel interface does not become active.

upvoted 4 times

Question #1034

Topic 1

Which two protocols are supported on service-port interfaces? (Choose two.)

- A. Telnet
- B. SCP
- C. TACACS+
- D. SSH
- E. RADIUS

Correct Answer: AD

 **Goena** 3 months, 1 week ago

Selected Answer: AD

Correct

upvoted 4 times

Question #1035

Topic 1

What is the benefit of using private IPv4 addressing?

- A. to enable secure connectivity over the Internet
- B. to shield internal network devices from external access
- C. to provide reliable connectivity between like devices
- D. to be routable over an external network

Correct Answer: B

 **studying_1** 6 days, 9 hours ago

correct

upvoted 1 times

Question #1036

Topic 1

Two switches have been implemented and all interfaces are at the default configuration level. A trunk link must be implemented between two switches with these requirements:

- using an industry-standard trunking protocol
- permitting VLANs 1-10 and denying other VLANs

How must the interconnecting ports be configured?

- A. switchport mode dynamic
channel-protocol lacp
switchport trunk allowed vlans 1-10
- B. switchport mode trunk
switchport trunk allowed vlans 1-10
switchport trunk native vlan 11
- C. switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk allowed vlans 1-10
- D. switchport mode dynamic desirable
channel-group 1 mode desirable
switchport trunk encapsulation isl
switchport trunk allowed vlan except 11-4094

Correct Answer: C

 **molly_zheng** 3 weeks ago

Selected Answer: C

correct

upvoted 2 times

 **RidzV** 3 months ago

Correct answer

upvoted 3 times

Question #1037

Topic 1

```
TenGigabitEthernet0/0/0 is up, line protocol is up
  Hardware is BUILT-IN-2T+6X1GE, address is 74a0.2f7a.0123 (bia 74a0.2f7a.0123)
  Description: Uplink
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 10000Mbps, link type is force-up, media type is unknown media type
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:05:40, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 6160000 bits/sec, 1113 packets/sec
  5 minute output rate 11213000 bits/sec, 1553 packets/sec
    12662416065 packets input, 12607032232894 bytes, 0 no buffer
    Received 14117163 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 26271385 multicast, 0 pause input
    7907779058 packets output, 5073750426832 bytes, 0 underruns
    0 output errors, 8662416065 collisions, 1 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions
```

Refer to the exhibit. Traffic that is flowing over interface TenGigabitEthernet0/0/0 experiences slow transfer speeds. What is the cause of this issue?

- A. speed conflict
- B. queuing drops
- C. duplex incompatibility
- D. heavy traffic congestion

Correct Answer: C

 RidzV Highly Voted 3 months ago

Duplex incompatibility can cause high number of collisions
upvoted 6 times

 JJY888 Most Recent 3 weeks, 4 days ago

Selected Answer: C
According to OCG and Boson practice exams, collisions are duplex incompatibility.
upvoted 4 times

 Simon_1103 1 month, 2 weeks ago

Selected Answer: D
Based on the information provided, the cause of the slow transfer speeds is most likely heavy traffic congestion. The output of the "show interface" command indicates that the interface is operating at full duplex with a speed of 10000Mbps, which rules out speed conflict and duplex incompatibility as potential causes. The input and output rates shown in the command output are both relatively high, indicating that there is a significant amount of traffic flowing through the interface. Additionally, there are no indications of queuing drops or other errors that could suggest a different cause. Therefore, it is most likely that the slow transfer speeds are due to congestion on the interface.
upvoted 2 times

 ac891 2 weeks, 6 days ago

heavy traffic is shown by tx rx load
upvoted 2 times

Question #1038

Topic 1

Which two host addresses are reserved for private use within an enterprise network? (Choose two.)

- A. 10.172.76.200
- B. 12.17.1.20
- C. 172.15.2.250
- D. 172.31.255.100
- E. 192.169.32.10

Correct Answer: AC

 ahmt Highly Voted 3 months, 3 weeks ago

Selected Answer: AD

Address ranges to be used by private networks are:

Class A: 10.0.0.0 to 10.255.255.255

Class B: 172.16.0.0 to 172.31.255.255

Class C: 192.168.0.0 to 192.168.255.255

upvoted 12 times

 rAlexandre Highly Voted 3 months, 2 weeks ago

Selected Answer: AD

Class B IP addresses. Configurations range from 172.16.0.0 to 172.31.255.255

upvoted 7 times

 Bhrino Most Recent 2 weeks, 5 days ago

Selected Answer: AC

just have to memorize private ipv4 ranges here

upvoted 1 times

 Bhrino 2 weeks, 5 days ago

i meant A and d!

upvoted 1 times

 bisiyemo1 2 months, 3 weeks ago

Selected Answer: AD

AD is the correct answer

upvoted 2 times

 tal10 3 months, 1 week ago

Selected Answer: AD

definitiv

upvoted 1 times

 lucantonelli93 3 months, 1 week ago

Selected Answer: AD

The correct answers it's AD

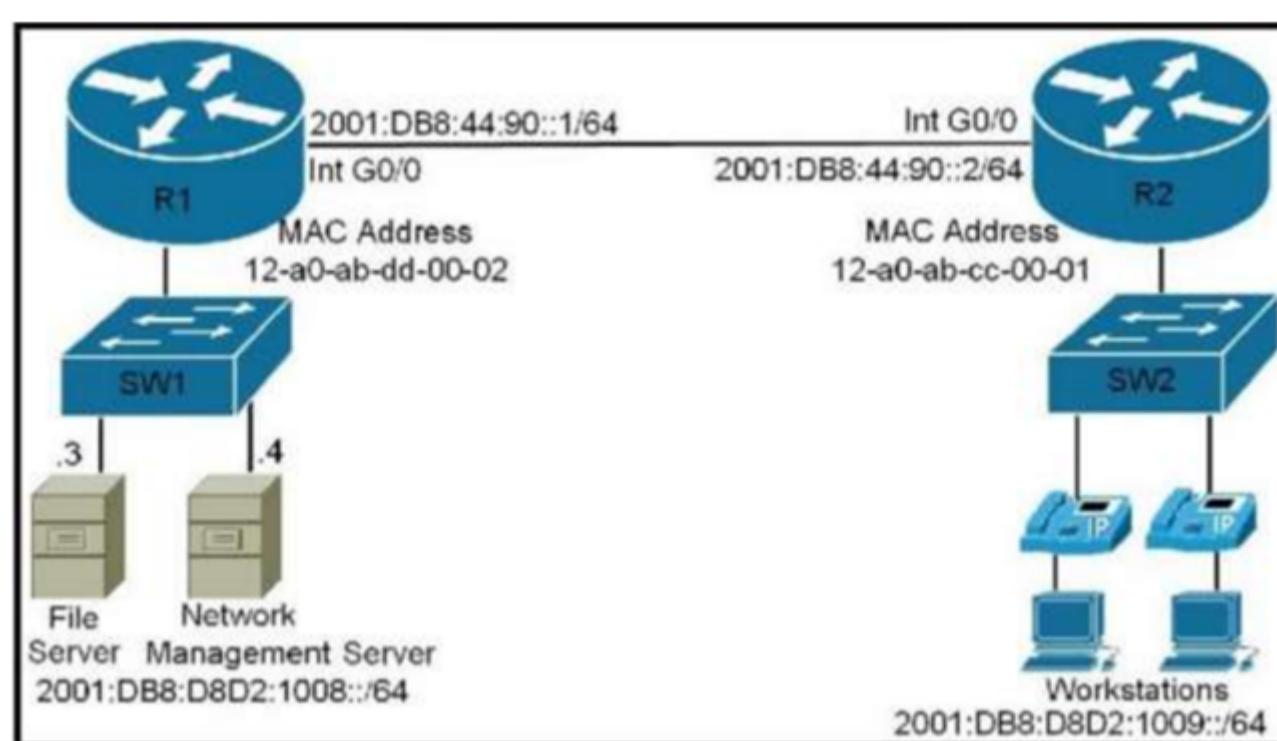
upvoted 1 times

 Rynurr 3 months, 1 week ago

Selected Answer: AD

Yeah, must be "AD"

upvoted 1 times



Refer to the exhibit. The IPv6 address for the LAN segment on router R2 must be configured using the EUI-64 format. Which address must be used?

- A. ipv6 address 2001:DB8:D8D2:1009:10A0:ABFF:FECC:1 eui-64
- B. ipv6 address 2001:DB8:D8D2:1009:1230:ABFF:FECC:1 eui-64
- C. ipv6 address 2001:DB8:D8D2:1009:4347:31FF:FF47:0 eui-64
- D. ipv6 address 2001:DB8:D8D2:1009:12A0:AB34:FFCC:1 eui-64

Correct Answer: A

audid 3 months, 1 week ago

Can someone explain please
upvoted 1 times

UAE7 3 months, 1 week ago

- classic EUI-64 --> just splits the mac and insert FFFE
- modified EUI-64 (that now is the standard)--> splits the mac address, insert FFFE and inverts the 7th bit
upvoted 6 times

Stichy007 3 months, 1 week ago

you insert fffe in the center of the mac address then invert the 7th bit. if its a 1 it becomes 0 and vice versa. there 12 be comes 10. 0001 0010
becomes 0001 000
upvoted 4 times

Question #1040

Topic 1

What are two reasons to configure PortFast on a switch port attached to an end host? (Choose two.)

- A. to block another switch or host from communicating through the port
- B. to enable the port to enter the forwarding state immediately when the host boots up
- C. to prevent the port from participating in Spanning Tree Protocol operations
- D. to protect the operation of the port from topology change processes
- E. to limit the number of MAC addresses learned on the port to 1

Correct Answer: BD

 ac891 3 weeks, 2 days ago

Selected Answer: BD

Though PortFast is enabled the port still participates in STP

https://www.arubanetworks.com/techdocs/ArubaOS_80_Web_Help/Content/ArubaFrameStyles/Network_Parameters/Portfast%20and%20BPDU%20Guard.htm

upvoted 2 times

 liviuml 1 month, 3 weeks ago

B & D are correct.

Port Fast still participate in STP ops.

https://www.arubanetworks.com/techdocs/ArubaOS_64_Web_Help/Content/ArubaFrameStyles/Branch%20Office/PortFast%20and%20BPDU%20Guard.htm

upvoted 4 times

 Leethy 1 month, 4 weeks ago

Selected Answer: BC

B. to enable the port to enter the forwarding state immediately when the host boots up

C. to prevent the port from participating in Spanning Tree Protocol operations

PortFast is a feature that allows a switch port to bypass the normal STP (Spanning Tree Protocol) listening and learning states and immediately transition to the forwarding state. This is beneficial when the port is connected to an end host, as it reduces the time it takes for the host to start sending and receiving data. Configuring PortFast on a switch port attached to an end host serves two purposes: enabling the port to enter the forwarding state immediately when the host boots up (B), and preventing the port from participating in Spanning Tree Protocol operations (C).

upvoted 1 times

 bisiyemo1 2 months, 3 weeks ago

Selected Answer: BD

BD are correct.

What are two features of PortFast?

Portfast does two things for us: Interfaces with portfast enabled that come up will go to forwarding mode immediately, the interface will skip the listening and learning state. A switch will never generate a topology change notification for an interface that has portfast enabled.

upvoted 3 times

 bisiyemo1 2 months, 3 weeks ago

<https://networklessons.com/switching/cisco-portfast-configuration#:~:text=Portfast%20does%20two%20things%20for%20us%3A&text=Interfaces%20with%20portfast%20enabled%20that,the%20listening%20and%20learning%20state.&text=A%20switch%20will%20never%20generate,interface%20that%20has%20portfast%20enabled.>

upvoted 1 times

 RidzV 3 months ago

Selected Answer: BC

Faster convergence can be achieved by skipping STP operations state.

upvoted 3 times

 Dutch012 3 months ago

I believe B & C are correct

upvoted 3 times

Question #1041

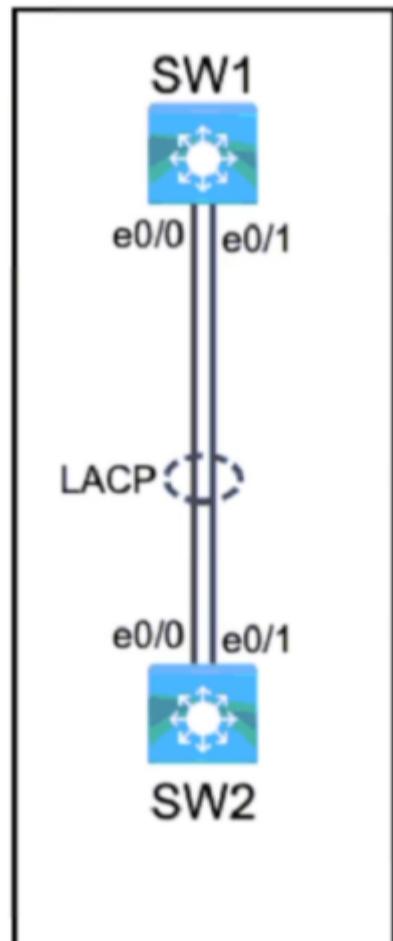
SIMULATION

Guidelines

This is a lab item in which tasks will be performed on virtual devices

- Refer to the Tasks tab to view the tasks for this lab item.
- Refer to the Topology tab to access the device console(s) and perform the tasks
- Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window
- All necessary preconfigurations have been applied
- Do not change the enable password or hostname for any device
- Save your configurations to NVRAM before moving to the next item
- Click Next at the bottom of the screen to submit this lab and move to the next question
- When Next is clicked the lab closes and cannot be reopened

Topology



Tasks

Physical connectivity is implemented between the two Layer 2 switches, and the network connectivity between them must be configured.

1. Configure an LACP EtherChannel and number it as 44; configure it between switches SW1 and SW2 using interfaces Ethemet0/0 and Ethernet0/1 on both sides. The LACP mode must match on both ends.
2. Configure the EtherChannel as a trunk link.
3. Configure the trunk link with 802.1q tags.
4. Configure VLAN 'MONITORING' as the untagged VLAN of the EtherChannel.

```
SW1(config)#interface range eth0/0-1
SW1(config-if-range)# channel-group 44 mode active
SW1(config-if-range)# interface port44
SW1(config-if)# switchport trunk encapsulation dot1q
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk native vlan 746
SW1(config-if)# no shutdown
SW1(config-if)# end
```

Correct Answer:

```
SW2(config)#interface range eth0/0-1
SW2(config-if-range)# channel-group 44 mode active
SW2(config-if-range)# interface port44
SW2(config-if)# switchport trunk encapsulation dot1q
SW2(config-if)# switchport mode trunk
SW2(config-if)# switchport trunk native vlan 746
SW2(config-if)# no shutdown
SW2(config-if)# end
```

This assumes that VLAN 746 is the MONITORING VLAN.

✉ **Wes_60** 2 months ago

There is a lot of things wrong with this. First before you create an etherchannel you have to shutdown the ports you going to create it on. Second when you go into the etherchannel interface to create the trunk you have to type the command interface port-channel 44. Lastly you have to you have issue the no shutdown command on the interface ranges on both switches at the end to bring them back up.

upvoted 2 times

✉ **ac891** 4 weeks ago

I just tried on my lab:

1. No need to shutdown.
- The command will be rejected only if the interfaces is L2 instead of L3. So the "no switchport" command on interfaces will do the work.
2. You can go to "interface port-channel 44" with just "interface port44"

upvoted 1 times

✉ **Rydaz** 4 weeks, 1 day ago

no shutdown is only for routers not switches

upvoted 1 times

✉ **Titan_intel** 3 months, 1 week ago

Not sure about this one. Does anyone have any insight?

upvoted 1 times

✉ **yuz1227** 2 months, 4 weeks ago

this seems legit.. alough.. i would create the portchannel 44 interface with all the configuration required.. then apply it to the interface range with the channel-group command

upvoted 1 times

Question #1042

Topic 1

A network administrator wants the syslog server to filter incoming messages into different files based on their importance. Which filtering criteria must be used?

- A. message body
- B. level
- C. facility
- D. process ID

Correct Answer: *B*

 krzysiew 1 month ago

question 961 says
What is the purpose of configuring different levels of syslog for different devices on the network?
I think the answer level is correct
upvoted 2 times

 UAE7 3 months, 1 week ago

since question asks to filter messages based on importance, I think severity level is the answer
upvoted 4 times

 mageknight 3 months, 2 weeks ago

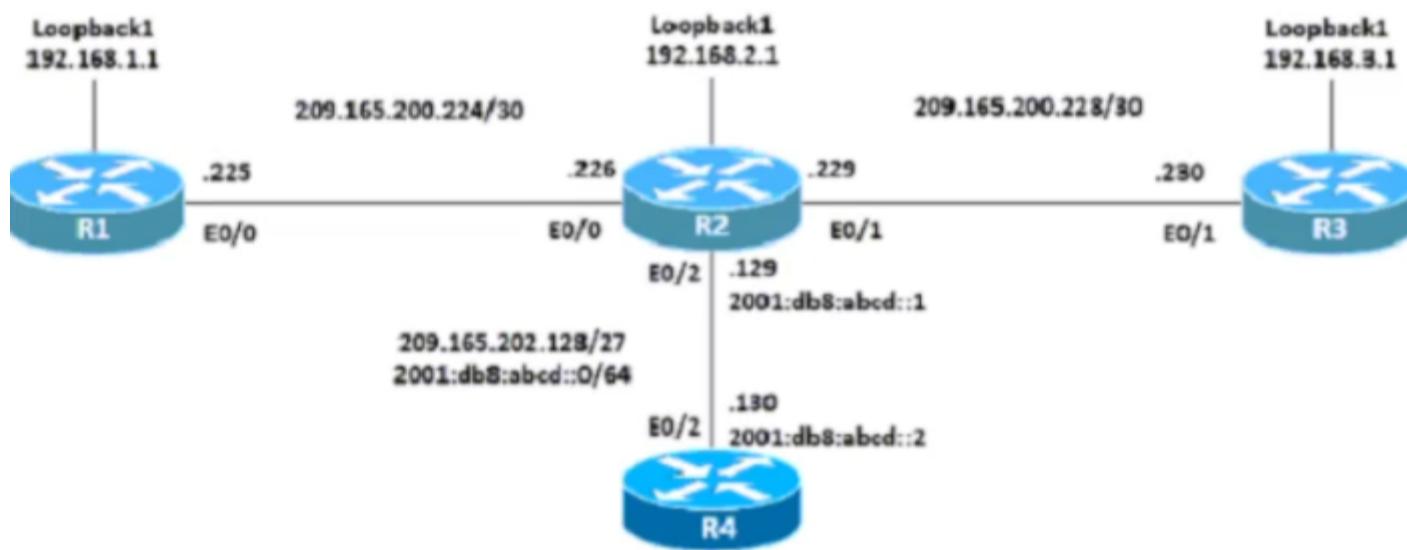
Facility code: Syslog messages have a facility code that indicates the type of process or application that generated the message. The facility code ranges from 0 to 23, and different facilities are used to indicate different types of messages. The network administrator can configure the syslog server to filter messages based on their facility code, so that messages generated by a specific process or application are stored in a specific file.
upvoted 2 times

Question #1043

SIMULATION**Guidelines**

This is a lab item in which tasks will be performed on virtual devices

- Refer to the Tasks tab to view the tasks for this lab item.
- Refer to the Topology tab to access the device console(s) and perform the tasks
- Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window
- All necessary preconfigurations have been applied
- Do not change the enable password or hostname for any device
- Save your configurations to NVRAM before moving to the next item
- Click Next at the bottom of the screen to submit this lab and move to the next question
- When Next is clicked, the lab closes and cannot be reopened

Topology**Tasks**

Connectivity between four routers has been established. IP connectivity must be configured in the order presented to complete the implementation. No dynamic routing protocols are included.

1. Configure static routing using host routes to establish connectivity from router R3 to the router R1 Loopback address using the source IP of 209.165.200.230.
2. Configure an IPv4 default route on router R2 destined for router R4.
3. Configure an IPv6 default router on router R2 destined for router R4.

R3

```
config terminal  
ip route 192.168.1.1 255.255.255.255 209.165.200.229  
end  
copy running start
```

Correct Answer:R2

```
config terminal  
ip route 0.0.0.0 0.0.0.0 209.165.202.130  
ipv6 route ::/0 2001:db8:abcd::2  
end  
copy running start
```

✉ **Mariachi** Highly Voted 2 months, 1 week ago

solution provided is not complete; R1 needs a route back to R3, otherwise connectivity is not established!

upvoted 5 times

✉ **VicM** 2 weeks, 5 days ago

Read the question well guys, it is sometime tricky. it says establish connectivity from router R3 to the router R1 not between R3 and R1 ;)

upvoted 1 times

✉ **ac891** 3 weeks, 2 days ago

actually, if cisco asks you to check ping, then you add back route if needed. if they did not ask, don be smart as*, they will fail you.

upvoted 1 times

✉ **rogi2023** 1 month, 2 weeks ago

Very good point. So folks check the successful ping or Routing table before you proceed. In worst scenario we have to create 4x static routes 2 to get there a 2 back. :-)

upvoted 3 times

✉ **studying_1** 4 days, 17 hours ago

only need one back, it's for the interface, not the loopback, one is enougha

upvoted 1 times

✉ **sany11** Most Recent 1 month, 1 week ago

1.- on R3

config terminal

ip route 192.168.1.1 255.255.255.255 209.165.200.229

end

copy running start

2.- on R2

config terminal

ip route 0.0.0.0 0.0.0.0 209.165.202.130

end

copy running start

3.- on R2

config terminal

ipv6 route ::/0 2001:db8:abcd::2

end

copy running start

upvoted 1 times

✉ **ac891** 2 weeks, 6 days ago

should there be a reverse route also ?

upvoted 1 times

✉ **itemba36** 1 month, 2 weeks ago

I agree with Mariachi and rogi2023 opinion.

For R3 e0/1 to ping to R1 loopback interface, then return back to R3,
we need to config as follows:

On R3, ip route 192.168.1.1 255.255.255.255 209.165.200.229
On R2, ip route 192.168.1.1 255.255.255.255 209.165.200.225
On R1, ip route 209.165.200.230 255.255.255.255 209.165.200.226
upvoted 2 times

 **Rydaz** 3 weeks, 5 days ago

on R1, why not use the loopback address on your route like u did with R2 and R3?
use the loopback of R3 which is 192.168.3.1
upvoted 1 times

Question #1044

Topic 1

Which interface or port on the WLC is the default for in-band device administration and communications between the controller and access points?

- A. console port
- B. management interface
- C. virtual interface
- D. service port

Correct Answer: B

 **Goena** 3 months ago

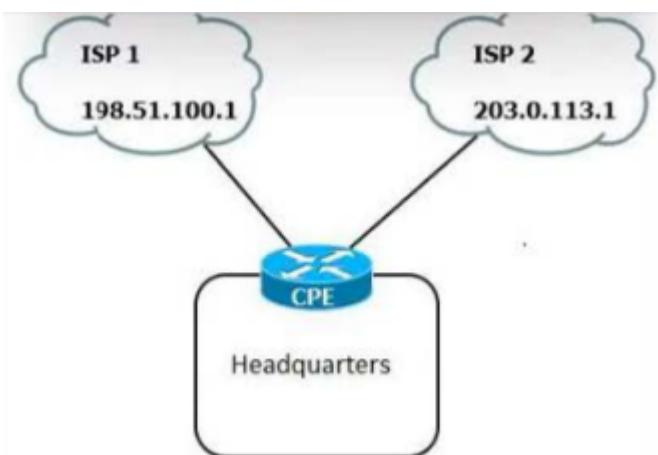
Selected Answer: B

B is correct:

The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers. It is also used for communications between the controller and access points, for all CAPWAP or intercontroller mobility messaging and tunneling traffic.

upvoted 3 times

Question #1045



Refer to the exhibit. A network administrator configures the CPE to provide internet access to the company headquarters. Traffic must be load-balanced via ISP1 and ISP2 to ensure redundancy.

Which two command sets must be configured on the CPE router? (Choose two.)

- A. ip route 0.0.0.0 0.0.0.0 198.51.100.1 255
ip route 0.0.0.0 0.0.0.0 203.0.113.1 255
ip route 128.0.0.0 128.0.0.0 203.0.113.1
- B. ip route 0.0.0.0 128.0.0.0 198.51.100.1
ip route 128.0.0.0 128.0.0.0 203.0.113.1
ip route 0.0.0.0 0.0.0.0 198.51.100.1
ip route 0.0.0.0 0.0.0.0 203.0.113.1
- C. ip route 0.0.0.0 0.0.0.0 198.51.100.1
ip route 0.0.0.0 0.0.0.0 203.0.113.1
- D. ip route 0.0.0.0 128.0.0.0 198.51.100.1
ip route 128.0.0.0 128.0.0.0 203.0.113.1
- E. ip route 0.0.0.0 0.0.0.0 198.51.100.1
ip route 0.0.0.0 0.0.0.0 203.0.113.1 2

Correct Answer: C

sdmejia01 Highly Voted 3 months, 2 weeks ago

I think it shouldn't be 2 answers. Answer C would work as intended in the question.
upvoted 6 times

Rydaz Most Recent 4 weeks, 1 day ago

C and D
upvoted 1 times

goldenoliver 1 month, 1 week ago

B and C right
upvoted 1 times

bisiyemo1 2 months, 3 weeks ago

A may be the second choice but C is sure
upvoted 1 times

tippy1000 3 months, 2 weeks ago

The 255 at the end of a is suspect
upvoted 1 times

mageknight 3 months, 2 weeks ago

may be A and C i think
upvoted 2 times

RaselAhmedIT 3 months, 2 weeks ago

What about the other one?
upvoted 2 times

oatmealturkey 3 months, 2 weeks ago

But you have to choose two :(

upvoted 3 times

Question #1046

Topic 1

```
SW1#show etherchannel
Channel-group listing:
-----
Group: 2
-----
Group state = L2
Ports: 1 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol: PAGP
```

Refer to the exhibit. A network engineer updates the existing configuration on interface fastethernet1/1 switch SW1. It must establish an EtherChannel by using the same group designation with another vendor switch. Which configuration must be performed to complete the process?

- A. interface port-channel 2
channel-group 2 mode desirable
- B. interface fastethernet 1/1
channel-group 2 mode on
- C. interface fastethernet 1/1
channel-group 2 mode active
- D. interface port-channel 2
channel-group 2 mode auto

Correct Answer: A

 **rAlexandre** Highly Voted 3 months, 2 weeks ago

Selected Answer: C

C is the right answer in order to change to LACP for multi vendor compatibility
upvoted 9 times

 **j1mlawton** Highly Voted 3 months, 2 weeks ago

Selected Answer: C

C is correct LACP must be used
upvoted 7 times

 **rubzal** 6 days, 21 hours ago

PAGP mentioned in the exhibit
upvoted 1 times

 **shiv3003** Most Recent 1 month, 2 weeks ago

i go for A
upvoted 1 times

 **Leethy** 1 month, 4 weeks ago

Selected Answer: B

B. interface fastethernet 1/1 channel-group 2 mode on

To establish an EtherChannel with another vendor switch, the configuration should be set to "mode on" for the interface. This means that the EtherChannel will be formed without using any specific negotiation protocol like PAgP (Cisco proprietary) or LACP (IEEE standard). The command for this would be:

interface fastethernet 1/1 channel-group 2 mode on
upvoted 2 times

 **ac891** 4 weeks ago

Configure Cross-Stack EtherChannel Without PAgP or LACP
-> channel-group 1 mode on
or
Configure Cross-Stack EtherChannel with LACP
-> channel-group 1 mode active/passive

I would go for C
upvoted 1 times

 **Leethy** 1 month, 4 weeks ago

B. interface fastethernet 1/1 channel-group 2 mode on

To establish an EtherChannel with another vendor switch, the configuration should be set to "mode on" for the interface. This means that the EtherChannel will be formed without using any specific negotiation protocol like PAgP (Cisco proprietary) or LACP (IEEE standard). The command for this would be:

interface fastethernet 1/1 channel-group 2 mode on
 upvoted 2 times

 **janekk** 3 months ago

Why not B?
mode on
 upvoted 2 times

 **lucantonelli93** 3 months, 1 week ago

Selected Answer: C
The correct answer it's C
 upvoted 1 times

 **lucantonelli93** 3 months, 1 week ago

The correct answer it's C
 upvoted 1 times

 **Rynurr** 3 months, 1 week ago

Selected Answer: C
"C" for sure
 upvoted 1 times

Question #1047

Topic 1

Which two characteristics are representative of virtual machines (VMs)? (Choose two.)

- A. multiple VMs operate on the same underlying hardware
- B. Each VM's operating system depends on its hypervisor
- C. A VM on a hypervisor is automatically interconnected to other VMs
- D. A VM on an individual hypervisor shares resources equally
- E. Each VM runs independently of any other VM in the same hypervisor

Correct Answer: AE

 **RidzV** 3 months ago

Correct answer
 upvoted 2 times

Question #1048

Topic 1

What is the recommended switch load-balancing mode for Cisco WLCs?

- A. source-destination IP address
- B. destination IP address
- C. destination MAC address
- D. source-destination MAC address

Correct Answer: A

✉️  **mageknight** Highly Voted 3 months, 2 weeks ago

When using EtherChannel with Cisco WLCs, the recommended load-balancing mode is the source-destination IP address mode. This mode distributes traffic based on the source and destination IP addresses, which ensures that all traffic between a specific client and the WLC is sent over the same physical link. This is important for maintaining client connectivity and optimizing network performance, as it helps to minimize latency, packet loss, and other network issues.

upvoted 10 times

Question #1049

Topic 1

What must be considered when using 802.11a?

- A. It is chosen over 802.11b when a lower-cost solution is necessary
- B. It is susceptible to interference from 2.4 GHz devices such as microwave ovens
- C. It is compatible with 802.11b- and 802.11g-compliant wireless devices
- D. It is used in place of 802.11b/g when many nonoverlapping channels are required

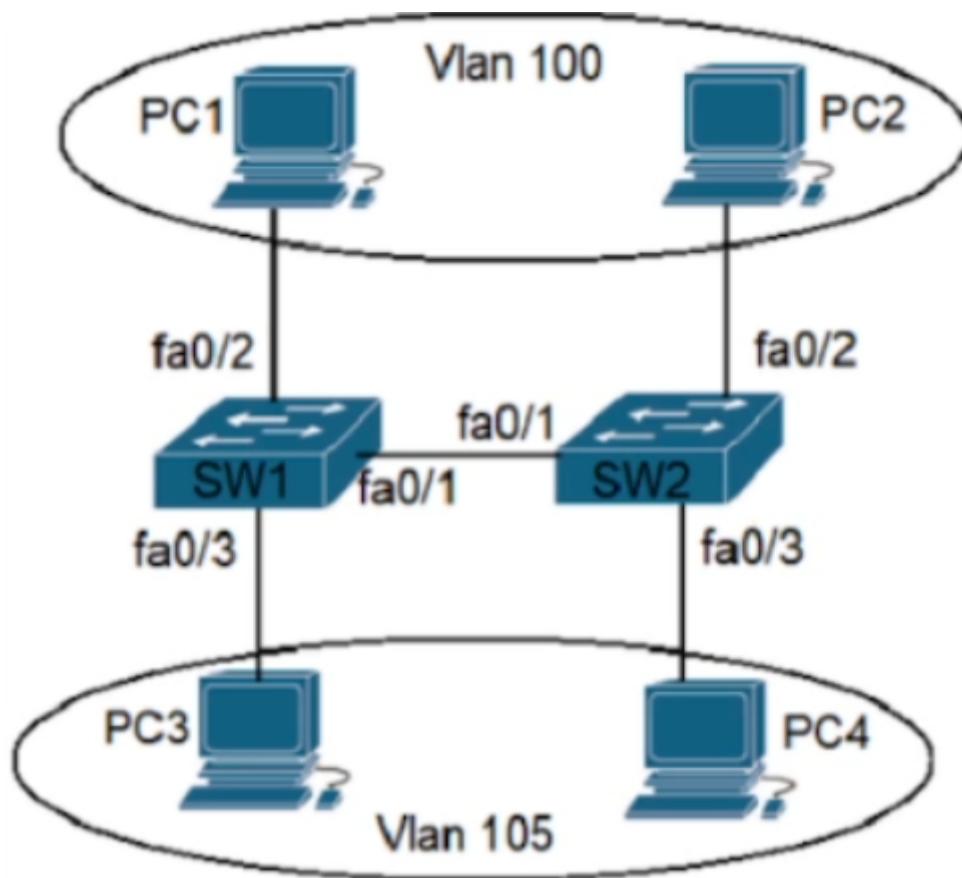
Correct Answer: D

✉️  **ike110** Highly Voted 3 months, 1 week ago

802.11a is a 5GHz standard

upvoted 6 times

Question #1050



Refer to the exhibit. An engineer configures interface fa0/1 on SW1 and SW2 to pass traffic from two different VLANs. For security reasons, company policy requires the native VLAN to be set to a nondefault value. Which configuration meets this requirement?

A. Switch(config-if)#switchport mode trunk

```
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan 100,105
Switch(config-if)#switchport trunk native vlan 3
```

B. Switch(config-if)#switchport mode trunk

```
Switch(config-if)#switchport trunk encapsulation isl
Switch(config-if)#switchport trunk allowed vlan 100,105
Switch(config-if)#switchport trunk native vlan 1
```

C. Switch(config-if)#switchport mode dynamic

```
Switch(config-if)#switchport access vlan 100,105
Switch(config-if)#switchport trunk native vlan 1
```

D. Switch(config-if)#switchport mode access

```
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport access vlan 100,105
Switch(config-if)#switchport trunk native vlan 3
```

Correct Answer: A

ac891 3 weeks, 2 days ago

IMO this is correct

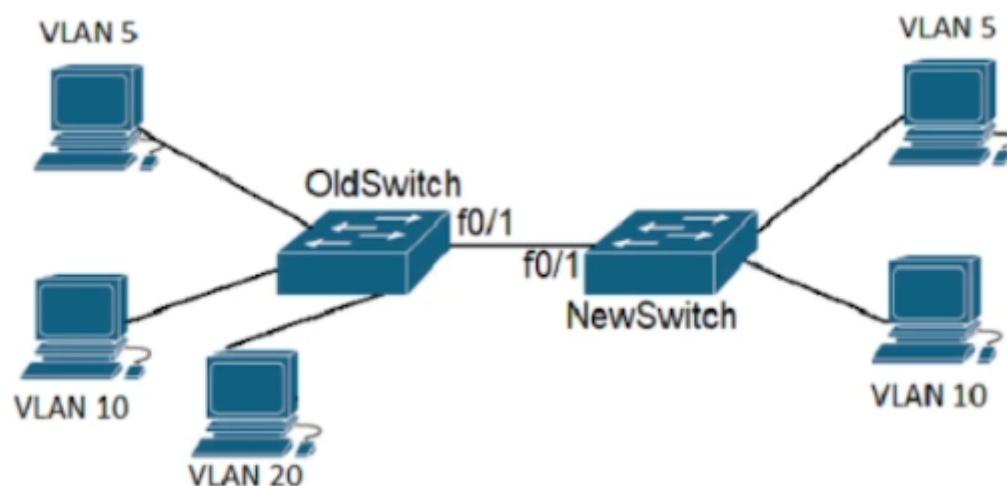
upvoted 3 times

studying_1 1 week, 1 day ago

Yes, it is, B & C wrong, because native vlan is 1 but the requirement is to use a nondefault vlan (not vlan1), and C configuration is wrong, but just by looking at the native vlan1 can exclude both, D is wrong because it should be trunk not access(access allows only one vlan)

upvoted 1 times

Question #1051



```

OldSwitch(config)#interface fastEthernet 0/1
OldSwitch(config-if)#switchport mode trunk
OldSwitch(config-if)#switchport trunk allowed vlan 5,10
OldSwitch(config-if)#switchport trunk native vlan 15
**output suppressed**

NewSwitch(config)#interface fastEthernet 0/1
NewSwitch(config-if)#switchport mode trunk
NewSwitch(config-if)#switchport trunk encapsulation isl
NewSwitch(config-if)#switchport trunk allowed vlan 5,10
NewSwitch(config-if)#switchport trunk native vlan 15

```

Refer to the exhibit A new VLAN and switch are added to the network. A remote engineer configures OldSwitch and must ensure that the configuration meets these requirements:

- accommodates current configured VLANs
- expands the range to include VLAN 20
- allows for IEEE standard support for virtual LANs

Which configuration on the NewSwitch side of the link meets these requirements?

- A. switch port mode dynamic
channel group 1 mode active
switchport trunk allowed vlan 5,10,15, 20
- B. no switchport mode trunk
switchport trunk encapsulation isl
switchport mode access vlan 20
- C. switchport nonegotiate
no switchport trunk allowed vlan 5,10
switchport trunk allowed vlan 5,10,15,20
- D. no switchport trunk encapsulation isl
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 20

Correct Answer: D

Friday_Night 4 days, 19 hours ago

I don't understand, we must configure the OLD SW right? but the new sw is in ISL encapsulation and letter D has the command [no trunk encapsulation ISL]. Unless the question is wrong and they meant to configure the new sw.

upvoted 1 times

krzysiew 1 month, 3 weeks ago

Selected Answer: D

answer is correct

upvoted 3 times

UAE7 3 months, 1 week ago

answer is correct

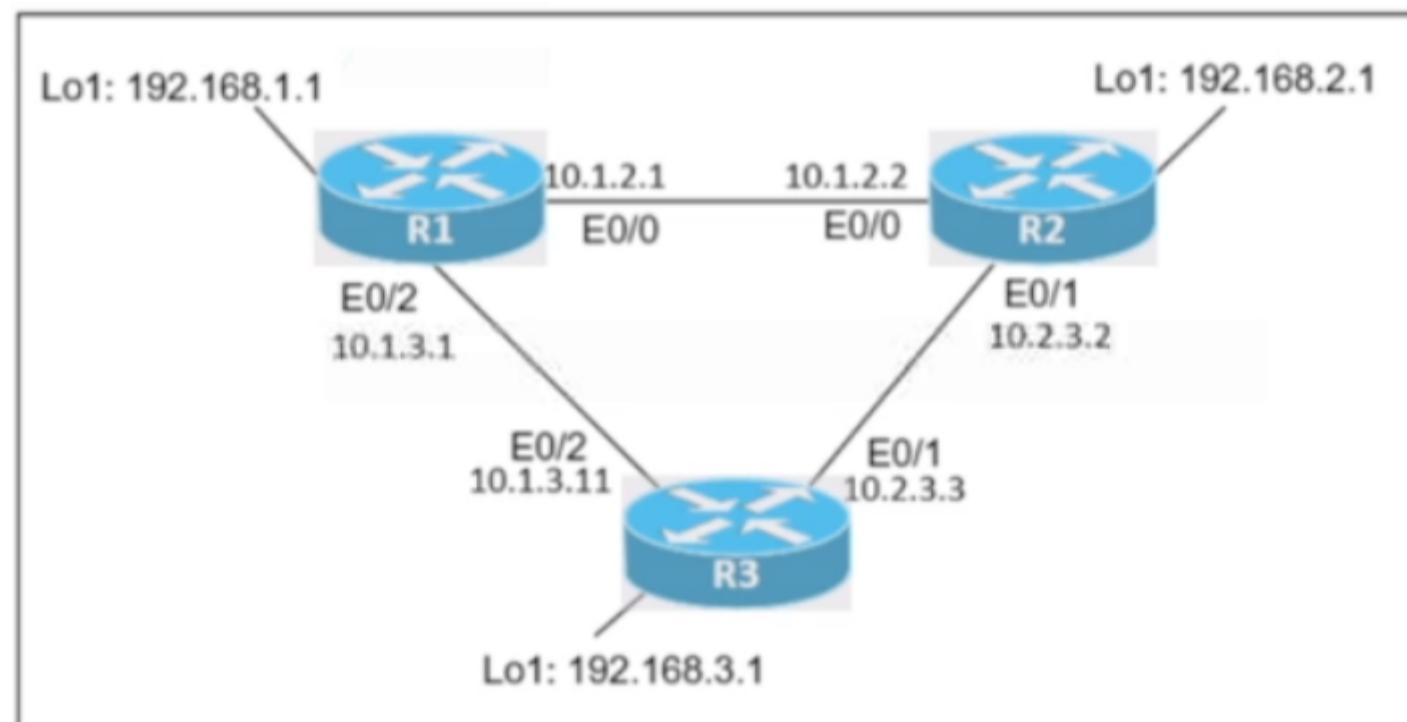
upvoted 4 times

Question #1052

SIMULATION**Guidelines**

This is a lab item in which tasks will be performed on virtual devices.

- Refer to the Tasks tab to view the tasks for this lab item.
- Refer to the Topology tab to access the device console(s) and perform the tasks.
- Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
- All necessary preconfigurations have been applied.
- Do not change the enable password or hostname for any device.
- Save your configurations to NVRAM before moving to the next item.
- Click Next at the bottom of the screen to submit this lab and move to the next question.
- When Next is clicked, the lab closes and cannot be reopened.

Topology**Tasks**

Connectivity between three routers has been established, and IP services must be configured in the order presented to complete the implementation. Tasks assigned include configuration of NAT, NTP, DHCP, and SSH services.

1. All traffic sent from R3 to the R1 Loopback address must be configured for NAT on R2. All source addresses must be translated from R3 to the IP address of Ethernet0/0 on R2, while using only a standard access list named PUBNET. To verify, a ping must be successful to the R1 Loopback address sourced from R3. Do not use NVI NAT configuration.
2. Configure R1 as an NTP server and R2 as a client, not as a peer, using the IP address of the R1 Ethernet0/2 interface. Set the clock on the NTP server for midnight on May 1, 2018.
3. Configure R1 as a DHCP server for the network 10.1.3.0/24 in a pool named NETPOOL. Using a single command, exclude addresses 1 - 10 from the range. Interface Ethernet0/2 on R3 must be issued the IP address of 10.1.3.11 via DHCP.
4. Configure SSH connectivity from R1 to R3, while excluding access via other remote connection protocols. Access for user netadmin and password N3t4cccess must be set on router R3 using RSA and 1024 bits. Verify connectivity using an SSH session from router R1 using a destination address of 10.1.3.11. Do NOT modify console.

```
conf t
```

```
R1(config)#ntp master 1
```

```
R2(config)#ntp server 10.1.2.1
```

```
Exit
```

```
R1#clock set 00:00:00 jan 1 2019
```

```
ip dhcp pool TEST
```

Correct Answer: network 10.1.3.0 255.255.255.0

```
ip dhcp excluded-address 10.1.3.1 10.1.3.10
```

```
R3(config)#int e0/2
```

```
ip address dhcp
```

```
no shut
```

```
crypto key generate RSA 1024
```

```
Copy run start
```

 **Goena** Highly Voted 2 months, 2 weeks ago

NAT:

```
R2(config)# ip access list standard PUBNET
```

```
R2(config-std-nacl)# permit 10.2.3.3
```

```
R2(config-std-nacl)# permit 10.1.3.11
```

```
R2(config-std-nacl)# permit 192.168.3.1
```

```
R2(config-std-nacl)# exit
```

```
R2(config)# interface e0/1
```

```
R2(config-if)# ip nat inside
```

```
R2(config)# interface e0/0
```

```
R2(config-if)# ip nat outside
```

```
R2(config)# ip nat inside source list PUBNET interface e0/0 overload
```

NTP:

```
R1# clock set 00:00:00 jan 1 2019
```

```
R1(config)# ntp master 1
```

```
R2(config)# ntp server 10.1.3.1
```

DHCP:

```
R1(config)# ip dhcp pool NETPOOL
```

```
R1(dhcp-config)# network 10.1.3.0 255.255.255.0
```

```
R1(config)# exit
```

```
R1(config)# ip dhcp excluded-address 10.1.3.1 10.1.3.10
```

```
R3(config)# interface e0/2
```

```
R3(config-if)# ip address dhcp
```

SSH:

```
R3(config)# username netadmin password N3t4ccess
```

```
R3(config)# line vty 0 4
```

```
R3(config-line)# login local
```

```
R3(config-line)# exit
```

```
R3(config)# ip domain-name cisco.com
```

```
R3(config)# crypto key generate rsa
```

upvoted 10 times

 **Friday_Night** 4 days, 15 hours ago

why use jan 1 2019 when it stated that clock must be May 1, 2018 ?

upvoted 1 times

 **rogi2023** 2 months ago

in ssh config missing "transport input ssh" (while excluding access via other remote connection protocols)

upvoted 4 times

 **Goena** Most Recent 2 months, 2 weeks ago

Is it nat to the loopback that is asked?

And how do you configure to a loopback?

upvoted 1 times

 **Goena** 2 months, 2 weeks ago

The configuration of NAT is missing.

upvoted 1 times

Question #1053

Topic 1

```
SW1# show etherchannel summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3       S - Layer2
      U - in use       f - failed to allocate aggregator
      M - not in use, minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port
      A - formed by Auto LAG
```

Number of channel-groups in use: 1

Number of aggregators: 1

Group	Port-channel	Protocol	Ports
1	Po1(RU)	LACP	Eto/0(P) Eto/1(P)

Refer to the exhibit. A network engineer is adding another physical interface as a new member to the existing Port-Channel1 bundle. Which command set must be configured on the new interface to complete the process?

- A. no switchport
channel group 1 mode active
- B. no switchport
channel-group 1 mode on
- C. switchport mode trunk
channel-group 1 mode active
- D. switchport
switchport mode trunk

Correct Answer: A

 **sdmejia01** Highly Voted 3 months, 2 weeks ago

The configuration shows is a layer 3 port channel, hence you need to use the command no switchport.

upvoted 5 times

 **Bhrino** Most Recent 2 weeks, 5 days ago

Selected Answer: A

because it says "R" we know its a layer three port channel meaning we need the no swtchport command and this is a Lacp so it would us active / passive

upvoted 1 times

 **gewe** 3 months, 2 weeks ago

its layer 3

upvoted 4 times

 **j1mlawton** 3 months, 2 weeks ago

Why not C?

upvoted 1 times

 **oatmealturkey** 3 months, 2 weeks ago

(RU) means Layer 3 & in use, so need to make it a layer 3 interface which is done with "no switchport"

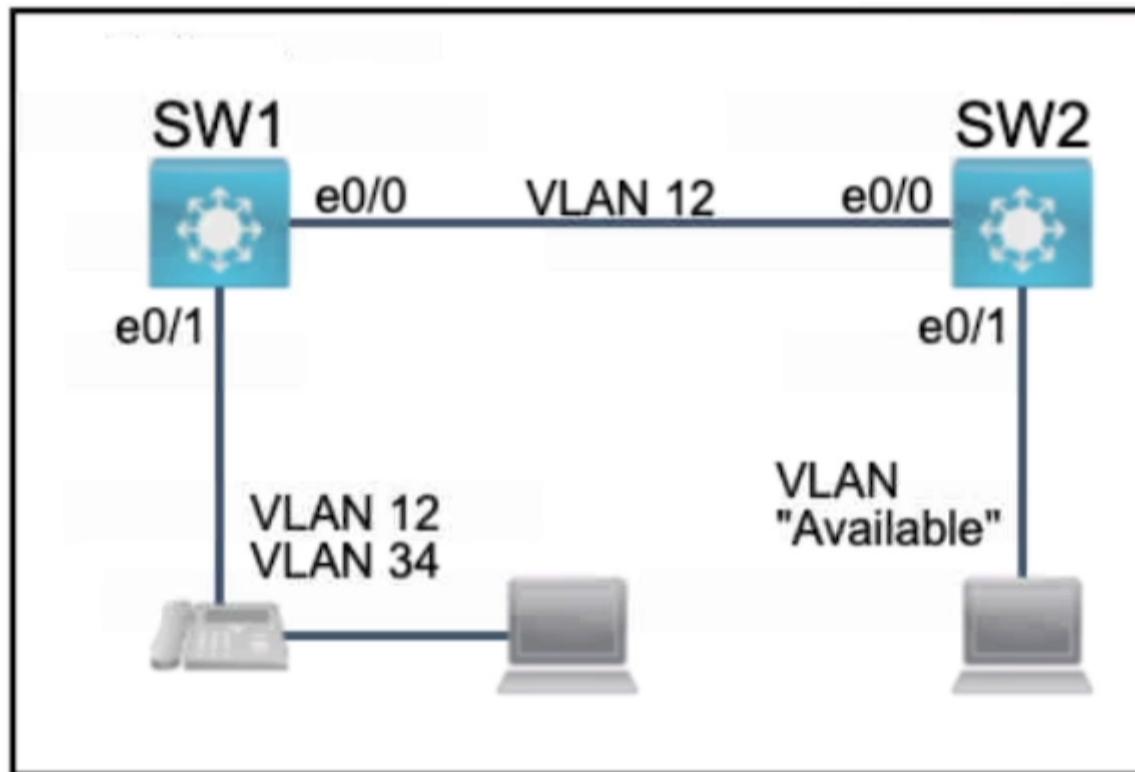
upvoted 5 times

Question #1054

SIMULATION**Guidelines**

This is a lab item in which tasks will be performed on virtual devices.

- Refer to the Tasks tab to view the tasks for this lab item.
- Refer to the Topology tab to access the device console(s) and perform the tasks.
- Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
- All necessary preconfigurations have been applied.
- Do not change the enable password or hostname for any device.
- Save your configurations to NVRAM before moving to the next item.
- Click Next at the bottom of the screen to submit this lab and move to the next question.
- When Next is clicked, the lab closes and cannot be reopened.

Topology**Tasks**

All physical cabling between the two switches is installed. Configure the network connectivity between the switches using the designated VLANs and interfaces.

1. Configure VLAN 12 named Compute and VLAN 34 named Telephony where required for each task.
2. Configure Ethernet0/1 on SW2 to use the existing VLAN named Available.
3. Configure the connection between the switches using access ports.
4. Configure Ethernet0/1 on SW1 using data and voice VLANs.
5. Configure Ethernet0/1 on SW2 so that the Cisco proprietary neighbor discovery protocol is turned off for the designated interface only.

SW1

```

enable
conf t
vlan 100
name Compute
vlan 200
name Telephony
int e0/1
switchport voice vlan 200
switchport access vlan 100
int e0/0
switchport mode access
wr mem

```

Correct Answer:**SW2**

```

Vlan 99
Name Available
Int e0/1
Switchport access vlan 99
wr mem

```

 **Mariachi** Highly Voted 2 months, 1 week ago

Solution is incomplete:

task 3: configuring the port into access mode, without assigning a vlan is just ... incomplete
 sw mode acc
 sw acc vl 12

task 5:
 no cdp enable (under the e0/1 interface)
 upvoted 7 times

 **rogi2023** Highly Voted 1 month, 2 weeks ago

```

sw1:
task#1:
vlan 12 name Compute
vlan 34 name Telephony
#3:
int e0/0
sw mo acc
sw acc vl 12 (the same on sw2)

#4 int e0/1
sw mo acc
sw acc vl 34
sw voice vl 12

```

#5 on SW2:
 sh vlan to see "Available #) and if its allready assignet to int, if not:
 int e0/1
 sw mo acc
 sw acc vl "#Available"
 no cdp enable

on allsw wr mem
 upvoted 6 times

 **itemba36** 1 month, 2 weeks ago

Hi rogi2023,
 For Task 4, the data vlan should be vlan 12 (named Compute), the voice vlan should be vlan 34 (named Telephony), so the e0/1 configuration should be modified as follow:
 int e0/1
 switchport mode access
 switchport access vlan 12
 switchport voice vlan 34
 upvoted 5 times

 **studying_1** Most Recent 4 days, 11 hours ago

wanted to add we need to configure vlan 100 on sw2 also, and the connection between the two switches given the diagram and please correct me if i'm wrong, on both switches:
 sw mode access
 sw access vlan 100

upvoted 1 times

 **Keba889** 1 month, 1 week ago

Correct, itemba36...Thanks!

upvoted 1 times

Question #1055

Topic 1

```
*AMD P2 FE-5-COLL: AMDP2/FE 0/0/[DEC], Excessive collisions, TDR=[DEC], TRC=[DEC]
*DEC21140-5-COLL: [chars] excessive collisions
*TLLACC-5-COLL: Unit [DEC], excessive collisions. TDR=[DEC]
*LANCE-5-COLL: Unit [DEC], excessive collisions. TDR=[DEC]
*PQUICC-5-COLL: Unit [DEC], excessive collisions. Retry limit [DEC] exceeded
*PQUICC_ETHER-5-COLL: Unit [DEC], excessive collisions. Retry limit [DEC] exceeded
```

Refer to the exhibit. What is occurring on this switch?

- A. Frames are dropped after 16 failed transmission attempts
- B. The internal transmit buffer is overloaded
- C. A high number of frames smaller than 64 bytes are received
- D. An excessive number of frames greater than 1518 bytes are received

Correct Answer: A

 **zamkijo** 2 months ago

Selected Answer: A

If the interface receives 16 consecutive collisions during frame transmission, then it gives up and the frame is dropped. This collision type is called Excessive Collision.

upvoted 3 times

 **Rynurr** 3 months, 1 week ago

Selected Answer: A

The retransmission algorithm helps to ensure that the packets do not retransmit at the same time. However, if the two devices retry at nearly the same time, packets can collide again; the process repeats until either the packets finally pass onto the network without collisions, or 16 consecutive collisions occur and the packets are discarded.

upvoted 4 times

 **oatmealturkey** 3 months, 2 weeks ago

Selected Answer: C

The exhibit indicates that collisions are occurring. Collisions result in runts (frames lower than 64 bytes). Therefore the correct answer is C. There is nothing in the exhibit to indicate that frames are dropped after 16 failed transmission attempts, only that there are a lot of collisions happening.

upvoted 1 times

 **oatmealturkey** 3 months, 2 weeks ago

I see here that the maximum number of retries in the backoff algorithm is set to 16, so A may be the right answer
<https://www.cisco.com/c/en/us/support/docs/interfaces-modules/port-adapters/12768-eth-collisions.html>

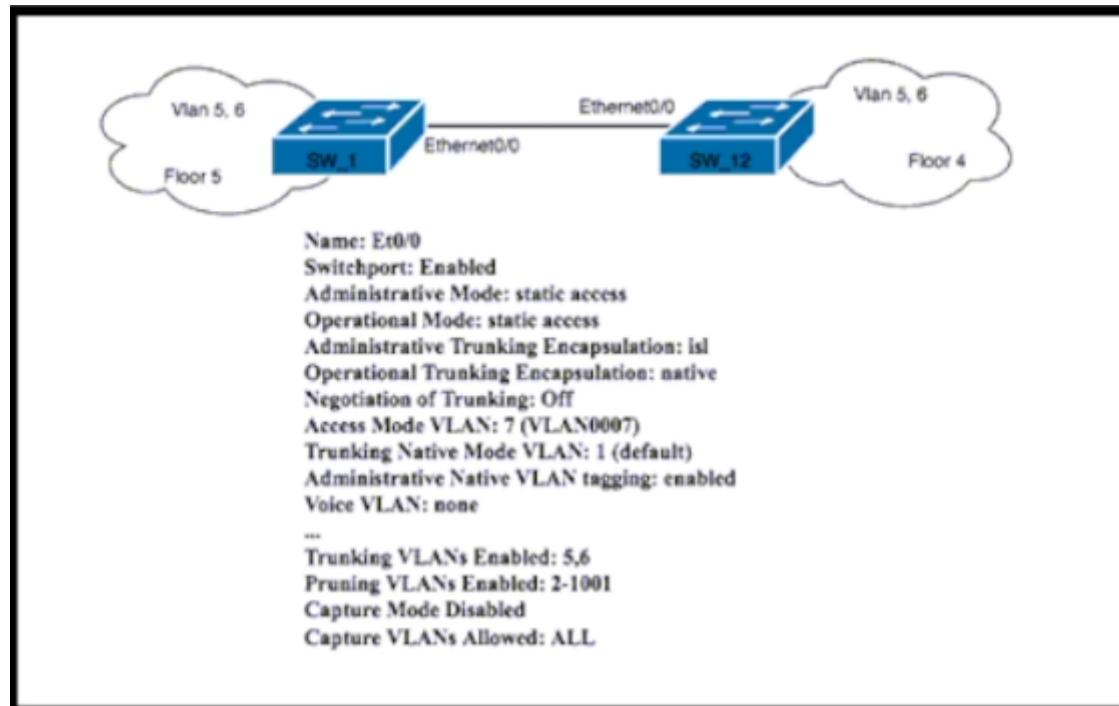
upvoted 2 times

 **oatmealturkey** 3 months, 2 weeks ago

A is definitely correct, my bad

upvoted 3 times

Question #1056



Refer to the exhibit SW_1 and SW_12 represent two companies that are merging. They use separate network vendors. The VLANs on both sides have been migrated to share IP subnets. Which command sequence must be issued on both sides to join the two companies and pass all VLANs between the companies?

- A. switchport mode trunk
switchport trunk encapsulation dot1q
- B. switchport mode trunk
switchport trunk allowed vlan all
switchport dot1q ethertype 0800
- C. switchport mode dynamic desirable
switchport trunk allowed vlan all
switchport trunk native vlan 7
- D. switchport dynamic auto
switchport nonegotiate

Correct Answer: C

✉ **rAlexandre** Highly Voted 3 months, 2 weeks ago

Selected Answer: A

I think the purpose is to change the encapsulation to dot1q because isl is a Cisco proprietary protocol
upvoted 11 times

✉ **oatmealturkey** 3 months, 2 weeks ago

Correct and dynamic desirable mode is only for DTP which is also Cisco proprietary
upvoted 5 times

✉ **bisiyemo1** Most Recent 2 months, 3 weeks ago

Selected Answer: A

A is sure
upvoted 4 times

✉ **Rynurr** 3 months, 1 week ago

Selected Answer: A

Need to set trunk and encapsulation dot1q, so "A" is the correct answer.
upvoted 4 times

Question #1057

Topic 1

An engineer is configuring a switch port that is connected to a VoIP handset. Which command must the engineer configure to enable port security with a manually assigned MAC address of abcd.abcd.abcd on voice VLAN 4?

- A. switchport port-security mac-address abcd.abcd.abcd vlan 4
- B. switchport port-security mac-address abcd.abcd.abcd vlan voice
- C. switchport port-security mac-address abcd.abcd.abcd
- D. switchport port-security mac-address sticky abcd.abcd.abcd vlan 4

Correct Answer: C

✉  **Dutch012** Highly Voted  3 months ago

final question yay!
upvoted 8 times

✉  **ac891** 3 weeks, 2 days ago

not for us ... :)
upvoted 5 times

✉  **Leethy** Highly Voted  1 month, 4 weeks ago

C. switchport port-security mac-address abcd.abcd.abcd

To enable port security with a manually assigned MAC address, the engineer would use the "switchport port-security mac-address abcd.abcd.abcd" command. This command sets the allowed MAC address for the port. The VLAN assignment for the VoIP handset is separate and not included in the port-security command.

upvoted 6 times

✉  **ac891** Most Recent  4 weeks ago

PTK-HOS-SRV-SW-L4-11(config-if)#switchport port-security mac-address ?
H.H.H 48 bit mac address
sticky Configure dynamic secure addresses as sticky

I go for C
upvoted 1 times

✉  **Rydaz** 4 weeks, 1 day ago

all wrong ending should be vlan voice 4,
and no sticky before the mac address, if B had 4 at the end it would be good
upvoted 1 times

✉  **Rydaz** 4 weeks, 1 day ago

my bad, C is right
upvoted 1 times

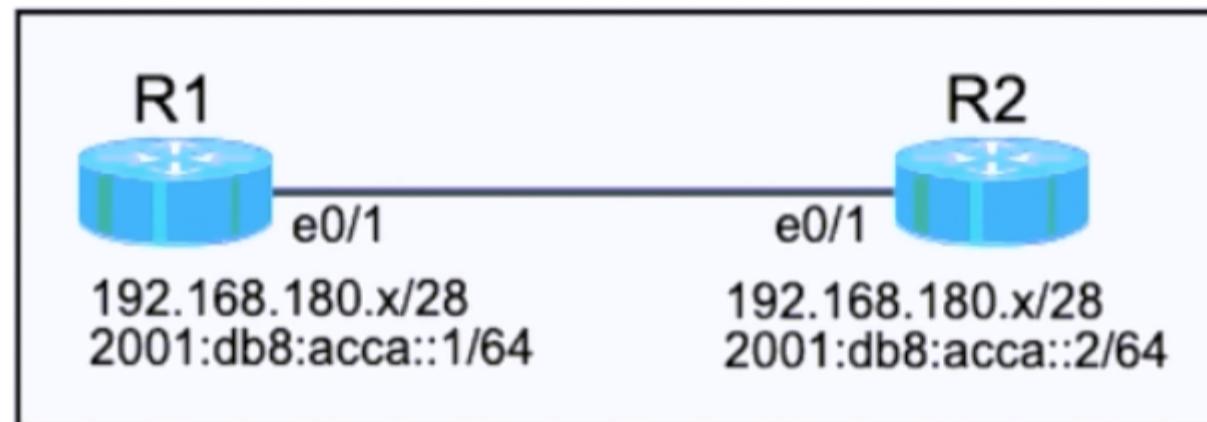
Question #1058

Topic 1

SIMULATION**Guidelines**

This is a lab item in which tasks will be performed on virtual devices

- Refer to the Tasks tab to view the tasks for this lab item.
- Refer to the Topology tab to access the device console(s) and perform the tasks.
- Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
- All necessary preconfigurations have been applied.
- Do not change the enable password or hostname for any device.
- Save your configurations to NVRAM before moving to the next item.
- Click Next at the bottom of the screen to submit this lab and move to the next question.
- When Next is clicked the lab closes and cannot be reopened.

Topology**Tasks**

Configure IPv4 and IPv6 connectivity between two routers. For IPv4, use a /28 network from the 192.168.180.0/24 private range. For IPv6, use the first /64 subnet from the 2001:0db8:acca:/48 subnet.

1. Using Ethernet0/1 on routers R1 and R2, configure the next usable /28 from the 192.168.180.0/24 range. The network 192.168.180.0/28 is unavailable.
2. For the IPv4 /28 subnet, router R1 must be configured with the first usable host address.
3. For the IPv4 /28 subnet, router R2 must be configured with the last usable host address.
4. For the IPv6 /64 subnet, configure the routers with the IP addressing provided from the topology.
5. A ping must work between the routers on the IPv4 and IPv6 address ranges.



```
R1
config terminal
ipv6 unicast-routing
inter eth0/1
ip addre 192.168.180.1 255.255.255.240
ipv6 addre 2001:db8:acca::1/64
no shut
end
copy running start
```

Correct Answer:

```
R2
config terminal
ipv6 unicast-routing
inter eth0/1
ip address 192.168.180.14 255.255.255.240
ipv6 address 2001:db8:acca::2/64
no shut
end
copy running start
```

✉ **rogij2023** Highly Voted 1 month, 3 weeks ago

Hey, read carefully: "The network 192.168.180.0/28 is unavailable." so the next /28 subnet is 192.168.180.16/28 therefore first IP is .17 and last usable is .30.

upvoted 7 times

✉ **dozer86** 1 month, 2 weeks ago

correct net 192.168.180.0/28 is unavailable.

upvoted 3 times

✉ **ac891** Most Recent 4 weeks ago

subnet is not available: 192.168.180.0/28

so the next /28 subnet is 192.168.180.16/28 therefore first IP is .17 and last usable is .30

on R1
config terminal
ipv6 unicast-routing
inter eth0/1

```
ip address 192.168.180.17 255.255.255.240
ipv6 addre 2001:db8:acca::1/64
not shut
end
copy running start

on R2
config terminal
ipv6 unicast-routing
inter eth0/1
ip address 192.168.1.30 255.255.255.240
ipv6 address 2001:db8:acca::2/64
not shut
end
copy running start
upvoted 2 times
```

✉ **VicM** 2 weeks, 5 days ago

For the IPv4 /28 subnet, router R2 must be configured with the last usable host address i.e 46 ;)
upvoted 1 times

✉ **studying_1** 5 days, 13 hours ago

no its /28 you're mistaken, from 16-31, it's 30
upvoted 1 times

✉ **VicM** 1 month ago

```
subnet is 192.168.180.16/28
on R1
config terminal
ipv6 unicast-routing
inter eth0/1
ip address 192.168.180.17 255.255.255.240
ipv6 addre 2001:db8:aaaa::1/64
not shut
end
copy running start
```

subnet is 192.168.180.32/28 use last usable IP i.e 46

```
on R2
config terminal
ipv6 unicast-routing
inter eth0/1
ip address 192.168.1.46 255.255.255.240
ipv6 address 2001:db8:aaaa::2/64
not shut
end
copy running start
upvoted 1 times
```

✉ **studying_1** 5 days, 13 hours ago

it's /28, 0-15 not available. 16-31, last ip address is 30
upvoted 1 times

✉ **RashidOzil** 1 month ago

Thank you firstly, I have question regarding the ipv6 why it changed from cc to aa (2001:db8:aaaa::2/64)?
upvoted 1 times

✉ **studying_1** 4 weeks ago

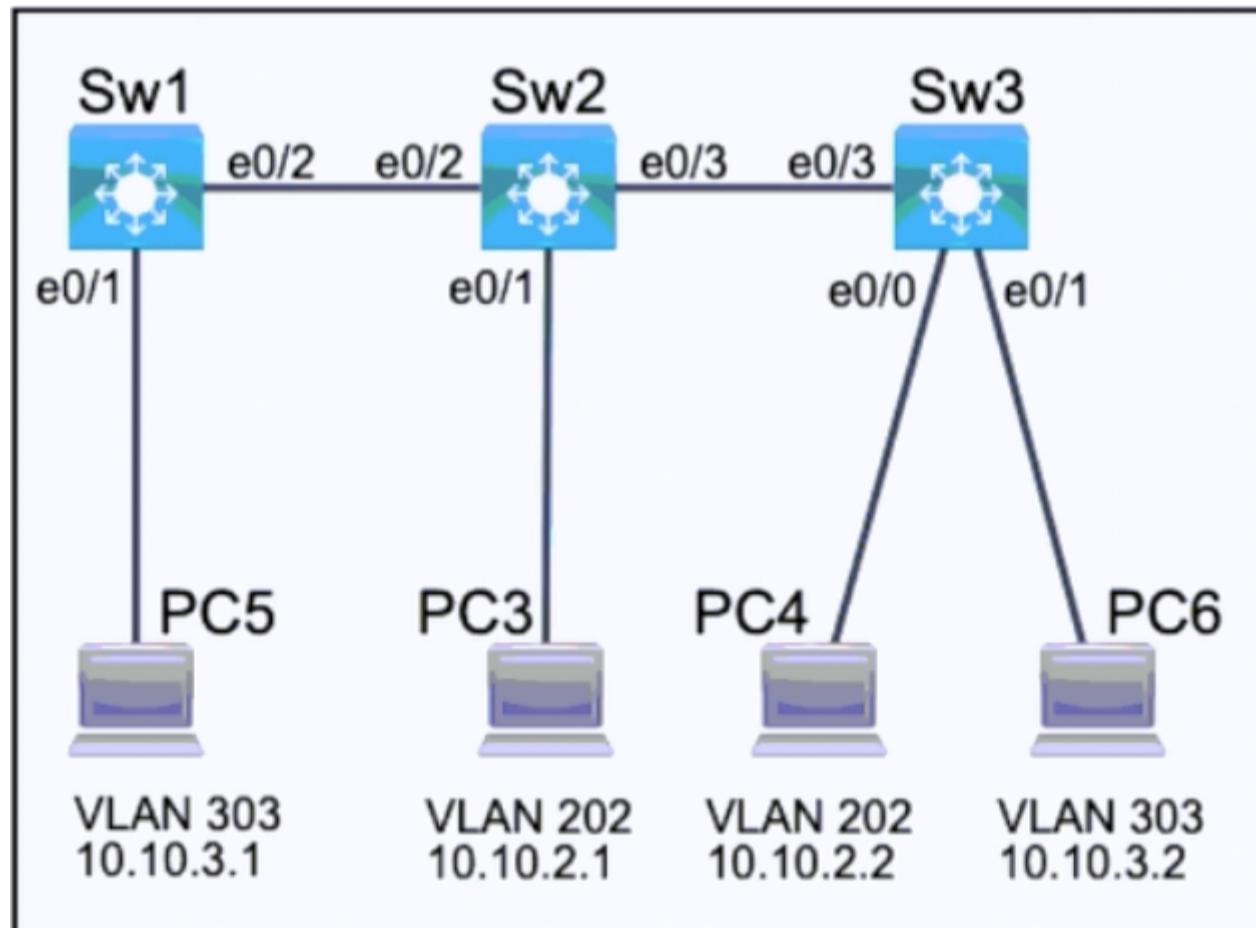
it shouldn't change, it's a typo
upvoted 2 times

Question #1059

SIMULATION**Guidelines**

This is a lab item in which tasks will be performed on virtual devices

- Refer to the Tasks tab to view the tasks for this lab item.
- Refer to the Topology tab to access the device console(s) and perform the tasks.
- Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
- All necessary preconfigurations have been applied.
- Do not change the enable password or hostname for any device.
- Save your configurations to NVRAM before moving to the next item.
- Click Next at the bottom of the screen to submit this lab and move to the next question.
- When Next is clicked the lab closes and cannot be reopened.

Topology**Tasks**

Three switches must be configured for Layer 2 connectivity. The company requires only the designated VLANs to be configured on their respective switches and permitted across any links between switches for security purposes. Do not modify or delete VTP configurations.

The network needs two user-defined VLANs configured:

VLAN 202: MARKETING

VLAN 303: FINANCE

1. Configure the VLANs on the designated switches and assign them as access ports to the interfaces connected to the PCs.
2. Configure the e0/2 interfaces on Sw1 and Sw2 as 802.1q trunks with only the required VLANs permitted.
3. Configure the e0/3 interfaces on Sw2 and Sw3 as 802.1q trunks with only the required VLANs permitted.

```
SW1 SW2 SW3

SW1>[REDACTED]
```

```
SW1 SW2 SW3

SW2>[REDACTED] ⌂ >- ✎
```

```
SW1 SW2 SW3

SW3>[REDACTED]
```

Sw1

```

enable
config t
Vlan 303
Name FINANCE
Int e0/1
Switchport access vlan 303
Wr mem

```

Sw2

```

Enable
config t
Vlan 202
Name MARKETING
Int e0/1
Switchport access vlan 202
Wr mem

```

Sw3**Correct Answer:**

```

Enable
config t
Vlan 202
Name MARKETING
Vlan 303
Name FINANCE
Int e0/0
Switchport access vlan 202
Int e0/1
Switchport access vlan 303
Sw1
Int e0/1
Switchport allowed vlan 303
Sw2
Int e0/2
Switchport trunk allowed vlan 303
Sw3
Int e0/3
Switchport trunk allowed vlan 303
Switchport trunk allowed vlan 202, 303

```

 **KraZd** 2 weeks, 6 days ago

ANSWER IS INCORRECT

upvoted 1 times

 **KraZd** 2 weeks, 6 days ago

Since the request states the three switches must be configured for Layer 2 connectivity we need to ensure that intra VLAN connectivity exists meaning PC5 & PC6 should be able to ping each other as well as PC3 & PC4

upvoted 1 times

 **KraZd** 2 weeks, 6 days ago

SW1:

The only VLAN that will need to traverse the link between SW1 & SW2 is VLAN 210 because that is the only VLAN with assigned hosts upstream from SW2. So only VLAN 210 is needed on SW1

upvoted 1 times

 **KraZd** 2 weeks, 6 days ago

SW2:

Since VLANS 110 & 210 will need to traverse the link between SW2 & SW3 both VLANS will need to be configured on SW2 or else VLAN 210 will be automatically pruned from the trunk resulting in a loss of communication between PC5 & PC6

upvoted 1 times

 **KraZd** 2 weeks, 6 days ago

SW3:

Switch 3 has hosts in both VLANS so both VLANS will need to be configured on it.

upvoted 1 times

 **KraZd** 2 weeks, 6 days ago

SW1:

Since the requirement is only for L2 connectivity and there are no hosts in VLAN 210 off of SW1 only VLAN 110 will need to traverse the link between Switch 1 & Switch 2

upvoted 1 times

 **KraZd** 2 weeks, 6 days ago

SW1:

Since the requirement is only for L2 connectivity and there are no hosts in VLAN 210 off of SW1 only VLAN 110 will need to traverse the link between Switch 1 & Switch 2

upvoted 1 times

✉ **KraZd** 2 weeks, 6 days ago

SW2:

Since Switch 2 has no connected hosts in VLAN 210 the only way to prevent VLAN 210 from being pruned from the trunk is to create the L2 VLAN on Switch 2 before allowing it on the link. DON'T FORGET THE CONFIGURATION FOR VLAN 210!

upvoted 1 times

✉ **KraZd** 2 weeks, 6 days ago

For requirement 3. Configure the e0/3 interfaces on Sw2 and Sw3 as 802.1q trunks with only the required VLANs permitted

Since Switch 3 has hosts in both VLAN 110 & VLAN 210 and the requirement is for L2 connectivity both VLANS will need to traverse the link between SW2 & SW3.

upvoted 1 times

✉ **itemba36** 1 month, 2 weeks ago

I think we should config both vlan 202 and 303 on all three switches.

On S1, S2, and S3, we should add VLAN 202 and 303 into their vlan databases.

That is to say, to config

vlan 303 name FINANCE, and vlan 202 name MARKETING on all three switches.

upvoted 1 times

✉ **rogi2023** 1 month, 3 weeks ago

I think on all trunk interfaces should be allowed vlans 202, 303

upvoted 1 times

✉ **jonathan126** 1 month, 2 weeks ago

Since there is no need for inter-vlan routing (see the question) and no IP configuration is also required, there is no need to allow vlan 202 on the connection between Sw1 and Sw2. I think the command that is missing on the answer would be:

Sw2

int e0/3

switchport trunk allowed vlan 202,303

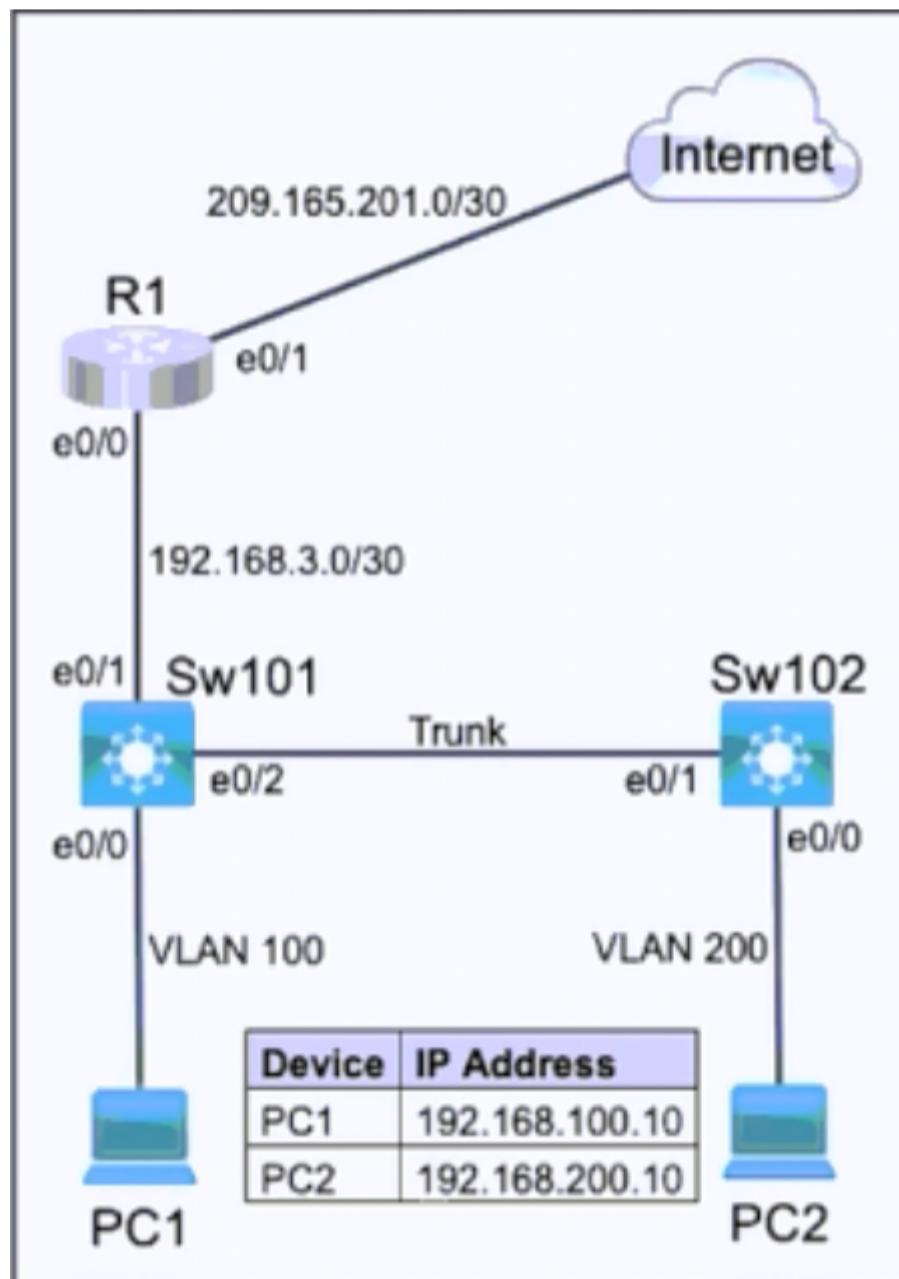
upvoted 2 times

Question #1060

SIMULATION**Guidelines**

This is a lab item in which tasks will be performed on virtual devices

- Refer to the Tasks tab to view the tasks for this lab item.
- Refer to the Topology tab to access the device console(s) and perform the tasks.
- Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
- All necessary preconfigurations have been applied.
- Do not change the enable password or hostname for any device.
- Save your configurations to NVRAM before moving to the next item.
- Click Next at the bottom of the screen to submit this lab and move to the next question.
- When Next is clicked the lab closes and cannot be reopened.

Topology**Tasks**

Refer to the topology. All physical cabling is in place. Configure a local user account, a Named ACL (NACL), and security.

Task 1

-

Configure a local account on Sw101 with telnet access only on virtual ports 0-4. Use the following information:

- Username: support
- Password: max2learn
- Privilege level: Exec mode

Task 2

-

Configure and apply a single NACL on Sw101 using the following:

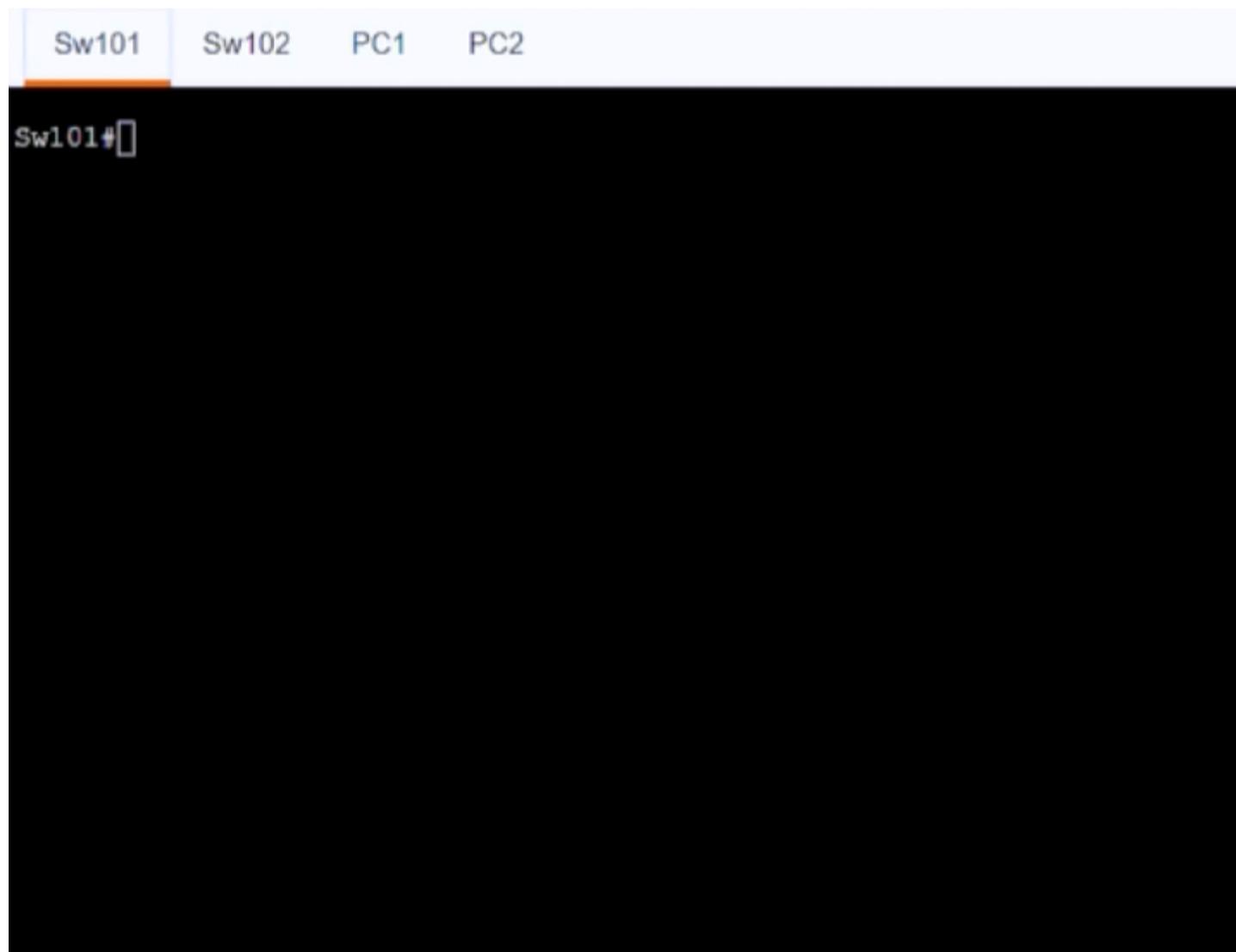
- Name: ENT_ACL
- Restrict only PC2 on VLAN 200 from pinging PC1
- Allow only PC2 on VLAN 200 to telnet to Sw101
- Prevent all other devices from telnetting from VLAN 200
- Allow all other network traffic from VLAN 200

Task 3

-

Configure security on interface Ethernet 0/0 of Sw102:

- Set the maximum number of secure MAC addresses to four.
- Drop packets with unknown source addresses until the number of secure MAC addresses drops below the configured maximum value. No notification action is required.
- Allow secure MAC addresses to be learned dynamically.



Sw101 Sw102 PC1 PC2

```
Sw102#sh vlan br

VLAN Name                               Status    Ports
---- --                                     ----
1   default                                active    Et0/2, Et0/3
200  VLAN0200                             active    Et0/0
1002 fddi-default                         act/unsup
1003 token-ring-default                   act/unsup
1004 fddinet-default                      act/unsup
1005 trnet-default                        act/unsup
Sw102#
```

Sw101 Sw102 PC1 PC2

```
PC1#[]
```

Sw101 Sw102 PC1 PC2

```
PC2#[]
```

Sw101

```
Config t
Username support password max2learn privilege 15
Line vty 0 4
Login local
Transport input telnet
Access-class 10

Access-list ENT-ACL permit icmp host 192.168.200.10 host 182.168.100.10
Access-list ENT-ACL deny icmp any any
Access-list ENT-ACL permit ip any any
```

Correct Answer:

```
Access-list 10 permit 192.168.200.10
```

```
Interface vlan 200
ip access-group ENT-ACL in
```

```
interface ethernet 0/0
switchport port-security
switchport port-security maximum 4
switchport port-security violation protect
switchport port-security mac-address sticky
```

```
wr mem
```

 **rogi2023** 1 month, 2 weeks ago

the given solution with errors:

Task1+2 is for sw101:

```
username support pass max2learn privi 15
line vt 0 4
```

login local

transport input telnet

Task2 says apply a SINGLE NACL, so therefore not another ACL on line vt 0 4 as suggested in solution

```
access-list ENT-ACL deny icmp host 192.168.200.10 host 192.168.100.10
```

```
access-list ENT-ACL permit tcp host 192.168.200.10 any eq 23
```

```
access-list ENT-ACL deny tcp any any eq 23
```

```
access-list ENT-ACL permit ip any any
```

interface Vlan 200

```
ip access-group ENT_ACL in
```

task3 for Sw102: (the provided solutions is correct)

interf e0/0

sw port-sec

sw port-sec max 4

sw port-sec violation protect

sw port-sec mac-address sticky

wr mem

upvoted 2 times

 **jonathan126** 1 month, 2 weeks ago

How about this? Question requires EXEC mode, priv 15 is privilege EXEC mode, dynamic mac addr is enabled by default, the provided answer is for sticky mac addr on dynamic learned addr.

Task 1

```
username support password max2learn
```

line vty 0 4

login local

transport input telnet

Task 2

```
ip access-list extended ENT_ACL
```

```
deny icmp host 192.168.200.10 192.168.100.10
```

```
permit tcp host 192.168.200.10 any eq 23
```

```
deny tcp any any eq 23
```

```
permit ip any any
```

int vlan 200

```
ip access-group ENT_ACL in
```

Task 3

int e0/0

switchport port-security

switchport port-security maximum 4

switchport port-security violation protect

upvoted 2 times

 **4aynick** 1 week, 3 days ago

username support priv 15 password max2learn
upvoted 1 times

 **ac891** 3 weeks, 2 days ago

They asked for named ACL not extendedthere is a difference
upvoted 1 times

 **studying_1** 6 days, 9 hours ago

you need to use protocols and port numbers, it only works when you use extended ACLs
upvoted 1 times

 **ac891** 4 weeks ago

They should be more clear in those questions:
Router> - User EXEC mode
Router# - Privileged EXEC mode
upvoted 1 times

Question #1061

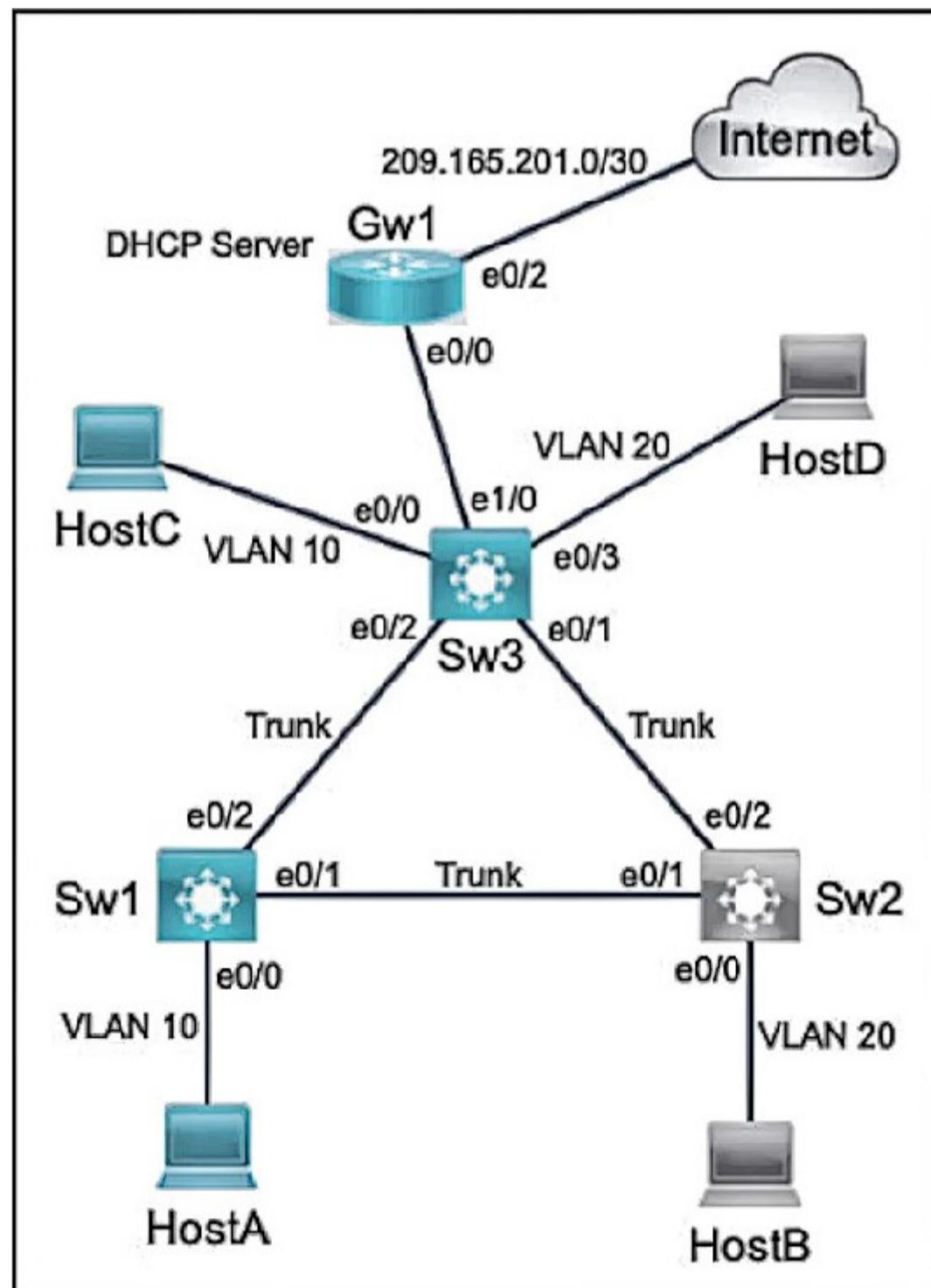
SIMULATION

Guidelines

This is a lab item in which tasks will be performed on virtual devices:

- Refer to the Tasks tab to view the tasks for this lab item.
- Refer to the Topology tab to access the device console(s) and perform the tasks.
- Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
- All necessary preconfigurations have been applied.
- Do not change the enable password or hostname for any device.
- Save your configurations to NVRAM before moving to the next item.
- Click Next at the bottom of the screen to submit this lab and move to the next question.
- When Next is clicked the lab closes and cannot be reopened.

Topology



Tasks

Refer to the topology. All physical cabling is in place. Configure local users accounts, modify the Named ACL (NACL), and configure DHCP Snooping. The current contents of the NACL must remain intact.

Task 1

-

Configure a local account on Gw1 with telnet access only on virtual ports 0-4. Use the following information:

- Username: wheel
- Password: lock3path
- Algorithm type: Scrypt
- Privilege level: Exec mode

Task 2

-

Configure and apply a NACL on Gw1 to control network traffic from VLAN 10:

- Name: CORP_ACL
- Allow BOOTP and HTTPS
- Restrict all other traffic and log the ingress interface, source MAC address, the packet's source and destination IP addresses, and ports

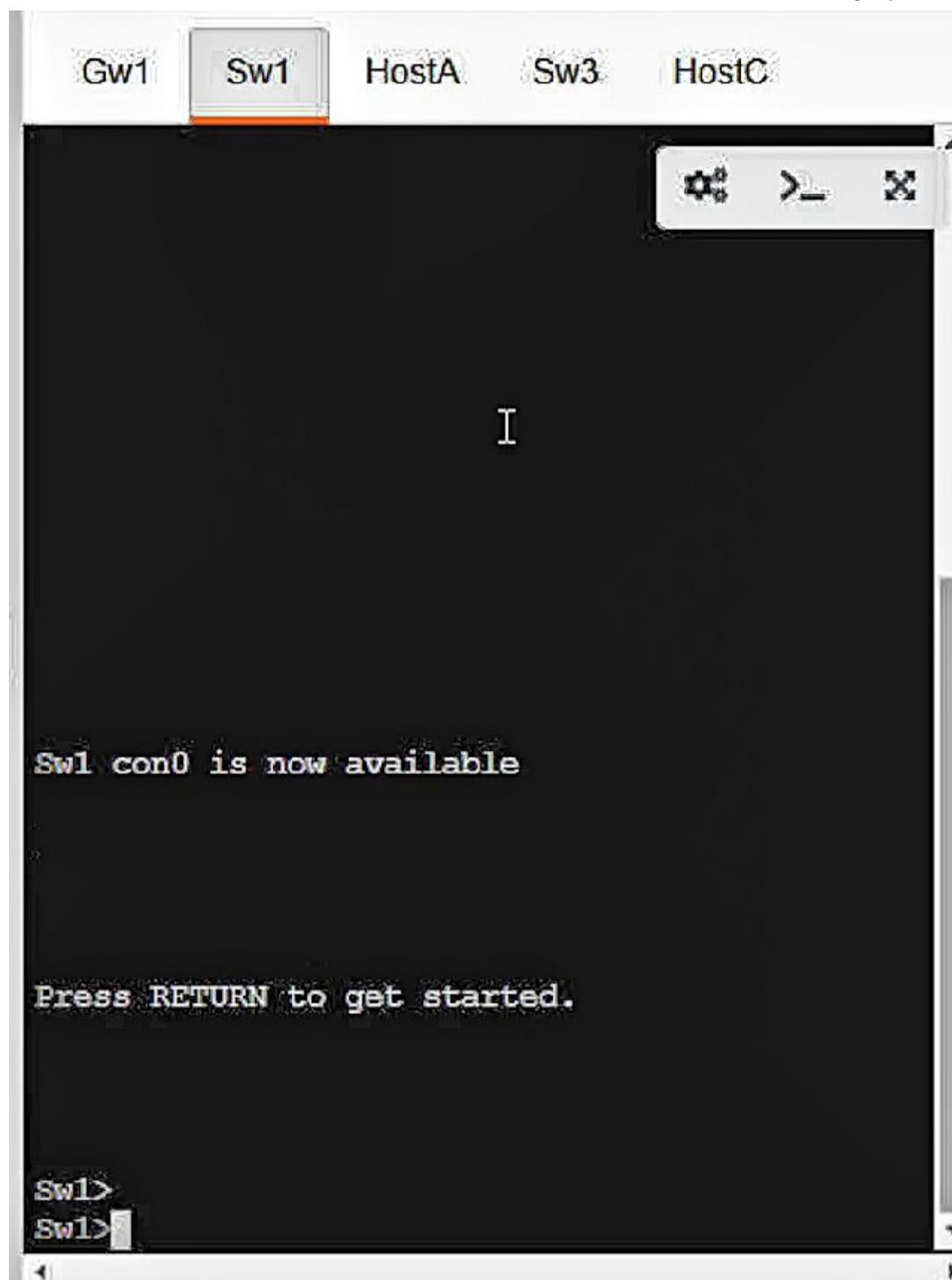
Task 3

-

Configure Sw1:

- Enable DNCP Snooping for VLAN 10
- Disable DHCP Option-82 data insertion
- Enable DHCP Snooping MAC address verification
- Enable trusted interfaces

The image shows a screenshot of a Cisco Network Simulator interface. At the top, there is a horizontal menu bar with five items: "Gw1", "Sw1", "HostA", "Sw3", and "HostC". The "Gw1" item is highlighted with a gray background and a white border. Below the menu, there is a large black terminal window. In the top-left corner of the terminal window, the text "Gw1>" is visible, followed by a small rectangular input field. The rest of the terminal window is completely blank, indicating no output or command entry. The entire interface is contained within a white frame.



Gw1:

```
Config t
Username wheel secret lock3path privilege 15
Line vty 0 4
Login local
Transport input telnet

Access-list CORP_ACL permit tcp any any eq bootp
Access-list CORP_ACL permit tcp any any eq https
Access-list CORP_ACL deny ip any any log
```

Interface vlan 10

Correct Answer: ip access-group CORP_ACL in

wr mem

Sw1:

```
Config t
Interface vlan 10
ip dhcp snooping
ip dhcp snooping information
ip dhcp snooping verify mac-address
p dhcp relay information trusted
```

wr mem

rogij2023 Highly Voted 1 month, 2 weeks ago

checking on GNS3 with IOS 15.2

GW1:

```
R1(config)#username wheel privilege 15 algorithm-type scrypt secret lock3path
line vty 0 4
login local
transport input telnet
```

```
task2 on GW1: bootp = udp; https = tcp
access-list CORP_ACL permit udp any any eq bootp (67,68)
access-list CORP_ACL permit tcp any any eq https (443)
access-list CORP_ACL deny ip any any log
```

on the router Gw1 find the gateway-subinterface for Vlan10 (router on the stick) and apply ACL
Gw1(config-subif)#ip access-group CORP_ACL in

task3 on Sw1: (not so sure, correct me if I am wrong pls)
Sw1(config)#ip dhcp snooping vlan 10
Sw1(config)#ip dhcp snooping verify mac-address
Sw1(config)#no ip dhcp snooping information option
Sw1(config)interface e0/2
Sw1(config-if)#ip dhcp snooping trust
upvoted 5 times

 **rogi2023** 1 month, 2 weeks ago

just adding also intf e0/1 for ip dhcp snooping trust. :-) In case the STP changes.
upvoted 3 times

 **studying_1** 3 weeks, 1 day ago

rogi only one thing, ip dhcp snooping needs to commands, dynamic arp only one command
ip dhcp snooping
ip dhcp snooping vlan 10
upvoted 3 times

 **studying_1** 3 weeks, 1 day ago

two* typo
upvoted 1 times

 **Peter_panda** 1 month, 2 weeks ago

Thank you, good job! Only one observation regarding the NACL: the task asks specifically to control traffic from VLAN10. It is possible that they expect us to permit traffic sourced by IPs from VLAN10 range instead of "any", i.e. access-list CORP_ACL permit udp 192.168.10.0 0.0.0.255 any eq bootp (VLAN10 ip addressing should be discovered on-the-job with show ip int brief)

upvoted 2 times

 **rogi2023** 1 month, 2 weeks ago

I expect that link Gw1-Sw3 is a trunk => Gw1 is R on the stick. Finding the correct sub-if in config will mean addressing the Gateway for the Vlan10 subnet. Therefore all source IPs on the Gateway are from VLAN 10 so wildcard "any" works just fine.
upvoted 2 times

Question #1062

Topic 1

What is represented by the word "LB20" within this JSON schema?

```
1 [
2 {"load balancer": "LB20", "interface": "te4/3"},
3 {"firewall": "FW49", "interface": "ge4/14"},
4 {"IDS": "IPS_frankfurt", "interface": "e9/7"}
5 ]
```

- A. value
- B. array
- C. object
- D. key

Correct Answer: A

Question #1063

Topic 1

What is represented beginning with line 1 and ending with line 5 within this JSON schema?

```
1 [
2 {"firewall": "FW24", "interface": "fe1/34"},  
3 {"switch": "SWseattle", "interface": "ge8/21"},  
4 {"IDS": "IPSsydney", "interface": "te2/43"}  
5 ]
```

- A. key
- B. object
- C. array
- D. value

Correct Answer: D

 **saoETo** Highly Voted 1 month, 3 weeks ago

Selected Answer: C

C. array
upvoted 9 times

 **fmaquino** Highly Voted 1 month, 3 weeks ago

Selected Answer: C

doesn't sqr brackets represent a array?
Correct me if I'm wrong
upvoted 7 times

 **DaimonANCC** 1 month, 3 weeks ago

i think to ARRAY
upvoted 5 times

 **Tdawg1968** Most Recent 1 week, 5 days ago

The previous question was an example of a value...
upvoted 1 times

 **Bhrino** 2 weeks, 6 days ago

]" or "[" = array
"{" or "}" = object
key : value
any thing in double quotes are strings
upvoted 1 times

 **mrmanistheman** 3 weeks, 2 days ago

Selected Answer: C
Answer is definitely C - Array
upvoted 1 times

 **bisiyemo1** 1 month, 1 week ago

Selected Answer: C
C for sure
upvoted 2 times

Question #1064

Topic 1

What is represented by the word "IDS" within this JSON schema?

1 [
2 {"firewall": "FW_portland", "port": "e2/5"},
3 {"IDS": "IPS31", "port": "ge0/28"},
4 {"load balancer": "LB48", "port": "fe0/43"}
5]

- A. object
- B. value
- C. array
- D. key

Correct Answer: D

Question #1065

Topic 1

What is represented in line 4 within this JSON schema?

1 [
2 {"switch": "SWbarcelona", "interface": "ge1/40"},
3 {"firewall": "FWamsterdam", "interface": "fe21"},
4 {"router": "R_frankfurt", "interface": "te8/30"}
5]

- A. object
- B. array
- C. key
- D. value

Correct Answer: A

Question #1066

Topic 1

What is represented by the word "port" within this JSON schema?

1 [
2 {"router": "R_pittsburgh", "port": "te6/21"},
3 {"VPN concentrator": "VPN47", "port": "e6/37"},
4 {"firewall": "FW28", "port": "ge7/42"}
5]

- A. key
- B. value
- C. array
- D. object

Correct Answer: A

 **Leethy** 1 month, 4 weeks ago

A. key

Within this JSON schema, the word "port" is a key within the objects represented by the curly braces {}. Each object in the schema has two key-value pairs, where "port" is one of the keys.

upvoted 3 times

Question #1067

Topic 1

What provides connection redundancy, increased bandwidth, and load sharing between a wireless LAN controller and a Layer 2 switch?

- A. first hop redundancy
- B. VLAN trunking
- C. tunneling
- D. link aggregation

Correct Answer: D

 **studying_1** 6 days, 9 hours ago

correct

upvoted 1 times

Question #1068

DRAG DROP

Drag and drop the IPv6 address from the left onto the type on the right.

Answer Area

ff00:af60:767d:9258:e688:c478:ec75:12

Global Unicast

fe80:b680:8af8:7cc1:6df1:71e1:b8f3:7

Unique Local

fc00:a4d3:af37:cbc6:cdbd:b73d:5561:3

Link-Local Unicast

2000:6794:5699:e122:42e0:4236:085d:1

Multicast

Correct Answer:**Answer Area**

ff00:af60:767d:9258:e688:c478:ec75:12

2000:6794:5699:e122:42e0:4236:085d:1

fe80:b680:8af8:7cc1:6df1:71e1:b8f3:7

fc00:a4d3:af37:cbc6:cdbd:b73d:5561:3

fc00:a4d3:af37:cbc6:cdbd:b73d:5561:3

fe80:b680:8af8:7cc1:6df1:71e1:b8f3:7

2000:6794:5699:e122:42e0:4236:085d:1

ff00:af60:767d:9258:e688:c478:ec75:12

 **Swiz005** Highly Voted  1 month, 2 weeks ago

Answers are correct

upvoted 7 times

Question #1069

Topic 1

Which interface is used to send traffic to the destination network?

- D 10.10.20.64/27 [90/6881] via F0/12
- D 10.10.20.64/27 [90/43618] via F0/5
- R 10.10.20.64/27 [120/7] via F0/9
- R 10.10.20.64/27 [120/3] via F0/6

- A. F0/5
- B. F0/6
- C. F0/12
- D. F0/9

Correct Answer: C

 **studying_1** 4 weeks ago

Selected Answer: C

Answer is correct
upvoted 2 times

Question #1070

Topic 1

What is the purpose of an SSID?

- A. It identifies an individual access point on a WLAN.
- B. It differentiates traffic entering access points.
- C. It provides network security.
- D. It identifies a WLAN.

Correct Answer: D

Question #1071

Topic 1

Which two types of attack are categorized as social engineering? (Choose two.)

- A. phoning
- B. malvertising
- C. probing
- D. pharming
- E. phishing

Correct Answer: DE

 **Bhrino** 2 weeks, 6 days ago

Selected Answer: DE

kennie is correct i believe they would have specifically called it Wishing

upvoted 1 times

 **kennie0** 3 weeks ago

Selected Answer: DE

correct answer is DE. There's nothing like phoning. Its rather called Vishing.

upvoted 1 times

 **JJY888** 3 weeks, 3 days ago

Selected Answer: AE

The two types of attack that are categorized as social engineering are E. phishing and A. phoning.

Phishing is a type of attack that involves sending fraudulent emails or messages that appear to come from a trusted source, with the goal of tricking the recipient into providing sensitive information or clicking on a malicious link.

Phoning, also known as "vishing", is a social engineering attack that involves calling a victim on the phone and using various tactics to convince them to provide sensitive information or perform a specific action.

Malvertising, probing, and pharming are not considered social engineering attacks. Malvertising is a type of attack where malicious advertisements are used to spread malware. Probing refers to the act of scanning a network or system for vulnerabilities or weaknesses. Pharming is a type of attack where a victim is redirected to a fake website in order to steal their personal information.

upvoted 1 times

 **studying_1** 2 weeks, 4 days ago

check volume 2 page 80, it is there in the table, answer is correct, phishing and pharming

upvoted 1 times

 **studying_1** 1 month, 1 week ago

Answer is correct. DE, Pharming is like phishing in that it is a threat that tricks users into divulging private information, but instead of relying on email as the attack vector, pharming uses malicious code executed on the victim's device to redirect to an attacker-controlled website. Because pharming runs code on the victim's computer, the attacker does not rely on the targeted user clicking a link or replying to an email. Instead, the malicious code directs the targeted user to the attacker's website, eliminating the extra step of a user clicking a link.

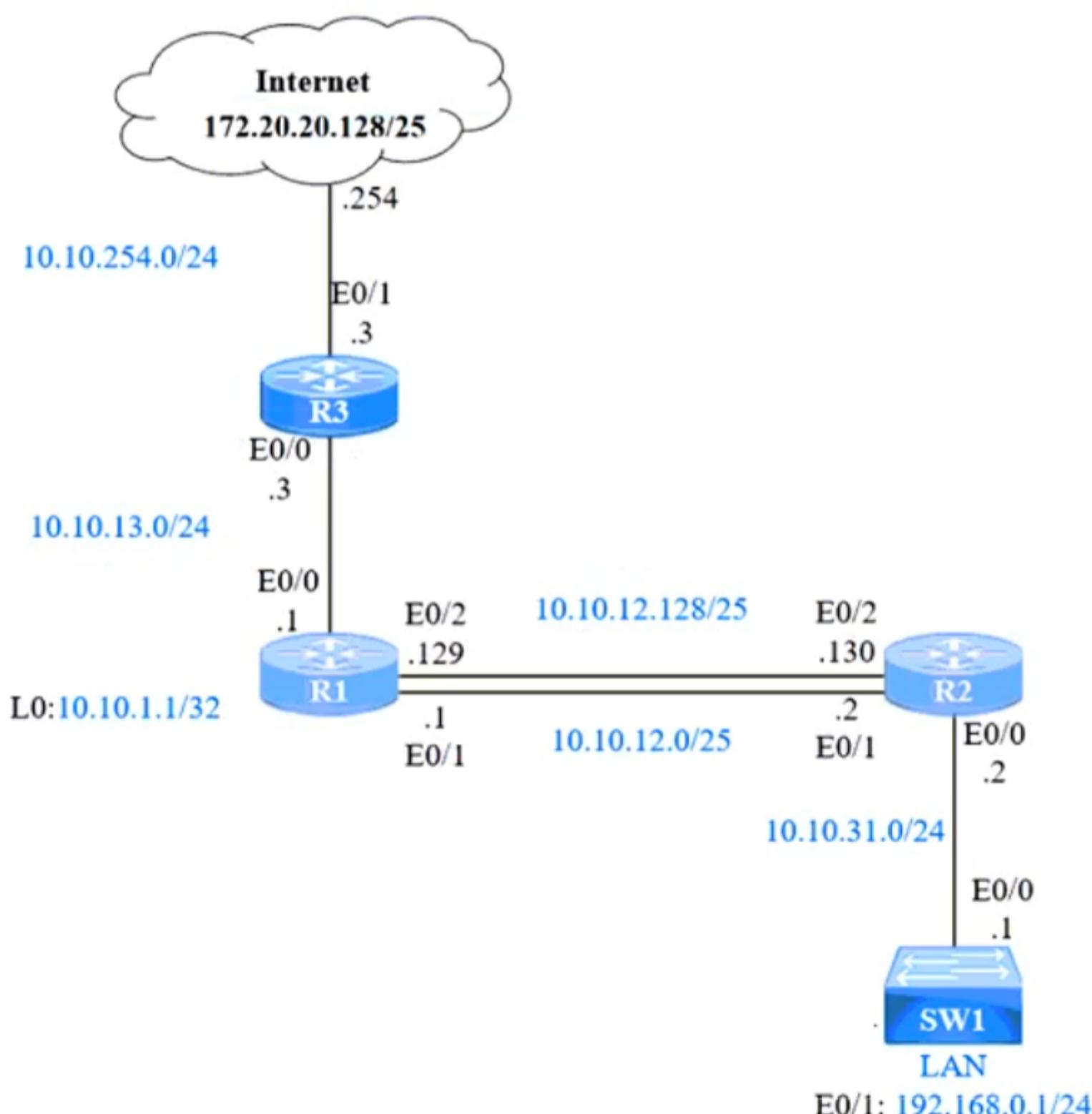
upvoted 2 times

Question #1072

SIMULATION**Guidelines**

This is a lab item in which tasks will be performed on virtual devices

- Refer to the Tasks tab to view the tasks for this lab item.
- Refer to the Topology tab to access the device console(s) and perform the tasks.
- Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
- All necessary preconfigurations have been applied.
- Do not change the enable password or hostname for any device.
- Save your configurations to NVRAM before moving to the next item.
- Click Next at the bottom of the screen to submit this lab and move to the next question.
- When Next is clicked the lab closes and cannot be reopened.

Topology

Tasks

-

IP connectivity and OSPF are preconfigured on all devices where necessary. Do not make any changes to the IP addressing or OSPF. The company policy uses connected interfaces and next hops when configuring static routes except for load balancing or redundancy without floating static. Connectivity must be established between subnet 172.20.20.128/25 on the Internet and the LAN at 192.168.0.0/24 connected to SW1:

1. Configure reachability to the switch SW1 LAN subnet in router R2.
2. Configure default reachability to the Internet subnet in router R1.
3. Configure a single static route in router R2 to reach to the Internet subnet considering both redundant links between routers R1 and R2. A default route is NOT allowed in router R2.
4. Configure a static route in router R1 toward the switch SW1 LAN subnet where the primary link must be through Ethernet0/1, and the backup link must be through Ethernet0/2 using a floating route. Use the minimal administrative distance value when required.



The image shows a terminal window interface. At the top, there are two labels: "R1" and "R2". Below them is a black terminal window with a white border. Inside the terminal window, the text "R1>" is displayed in white, indicating the current router prompt. The rest of the terminal window is blank, suggesting it is ready for input or has no output displayed.

```
R2:  
Conft  
Ip route 192.168.1.0 255.255.255.0 10.10.31.1  
Ip route 172.20.20.128 255.255.255.128 e0/2  
Ip route 172.20.20.128 255.255.255.128 e0/1
```

Correct Answer:

```
R1:  
conf t  
Ip route 0.0.0.0 0.0.0.0 10.10.13.3  
Ip route 192.168.0.0 255.255.255.0 e0/1  
Ip route 192.168.0.0 255.255.255.0 10.10.12.2 3
```

 **rogi2023** Highly Voted 1 month, 2 weeks ago

1@R2:
ip route 192.168.0.0 255.255.255.0 10.10.31.1

2@R1:
ip route 0.0.0.0 0.0.0.0 10.10.13.3

3@R2 the key is just a SINGLE static route, so I will check the ospf if both links are involved between R1<->R2 and learn the subnet 10.10.13.0/24; if yes then:
ip route 172.20.20.128 255.255.255.128 10.10.13.1

4@R1:
ip route 192.168.0.0 255.255.255.0 10.10.12.2
ip route 192.168.0.0 255.255.255.0 10.10.13.0 2

wr mem @ all R
upvoted 7 times

 **ac891** 3 weeks, 2 days ago

regarding task3, how could you route to 10.10.13.1 while it is not your next hop
upvoted 1 times

 **Peter_panda** 1 month, 2 weeks ago

Excellent point regarding task #3!
upvoted 4 times

 **Keba889** Most Recent 1 month, 1 week ago

shouldn't the 2nd route for 4@R1 be: ip route 192.168.0.0 225.255.255.0 10.10.12.130 2
.12 in ip address is missing) Thanks
upvoted 3 times

 **studying_1** 1 month, 1 week ago

Yes, AD should be 2 not 3
upvoted 1 times

Question #1073

Topic 1

What describes the functionality of southbound APIs?

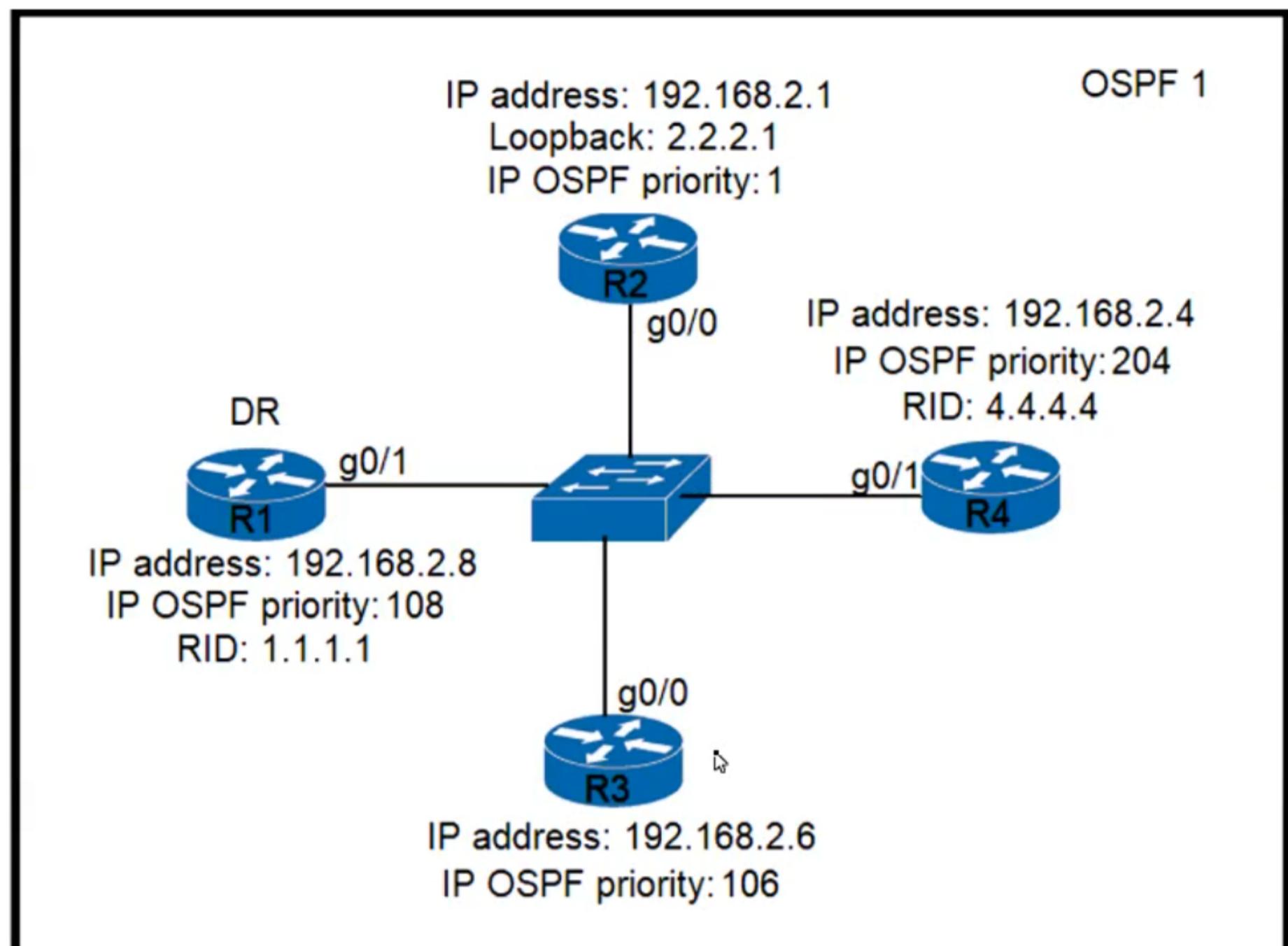
- A. They enable communication between the controller and the network device.
- B. They communicate with the management plane.
- C. They use HTTP messages to communicate.
- D. They convey information from the controller to the SDN applications.

Correct Answer: A

 **studying_1** 1 week, 1 day ago

Selected Answer: A

Answer is correct
upvoted 2 times



Refer to the exhibit. A network engineer is verifying the settings on a new OSPF network. All OSPF configurations use the default values unless otherwise indicated. Which router does the engineer expect will be elected as the DR when all devices boot up simultaneously?

- A. R1
- B. R2
- C. R3
- D. R4

Correct Answer: D

Mizuchan 1 week, 6 days ago

DR Election Criteria: The DR election process follows specific criteria:

The router with the highest priority becomes the DR. If multiple routers have the same highest priority, the router with the highest Router ID (RID) is elected as the DR.

The router with the second-highest priority becomes the BDR. If multiple routers have the same second-highest priority, the router with the highest RID is elected as the BDR.

upvoted 2 times

Bhrino 3 weeks ago

regarding ospf the highest ip priority becomes the dr

upvoted 1 times

Question #1075

Topic 1

Which command must be entered so that the default gateway is automatically distributed when DHCP is configured on a router?

- A. dns-server
- B. default-router
- C. ip helper-address
- D. default-gateway

Correct Answer: *B*

 **DaimonANCC** 2 weeks, 5 days ago

correct

upvoted 2 times

Question #1076

Topic 1

What are two functions of a firewall within an enterprise? (Choose two.)

- A. It enables traffic filtering based on URLs.
- B. It serves as an endpoint for a site-to-site VPN in standalone mode.
- C. It provides support as an endpoint for a remote access VPN in multiple context mode.
- D. It offers Layer 2 services between hosts.
- E. It enables wireless devices to connect to the network.

Correct Answer: BC

✉  **Leethy** Highly Voted 1 month, 4 weeks ago

- A. It enables traffic filtering based on URLs.
- B. It serves as an endpoint for a site-to-site VPN in standalone mode.

A firewall within an enterprise has multiple functions, including traffic filtering based on URLs (A) and serving as an endpoint for a site-to-site VPN in standalone mode (B). Firewalls help protect the network by inspecting and controlling incoming and outgoing traffic based on predetermined security rules. They can also establish secure connections between networks through VPNs.

upvoted 5 times

✉  **pikos1** Most Recent 1 week, 4 days ago

NGFW can filter based on URLs, but standard FW can't.
Standard FW can filter based domain, but no on URL.
upvoted 1 times

✉  **studying_1** 1 week, 1 day ago

right, the NGFW filters based on application
upvoted 1 times

✉  **Mizuchan** 1 week, 6 days ago

Selected Answer: AB

A. Traffic Filtering based on URLs: A firewall can be configured to filter network traffic based on Uniform Resource Locators (URLs) or website addresses. This feature allows organizations to enforce web access policies by blocking or allowing specific URLs or categories of websites.

B. Endpoint for Site-to-Site VPN in Standalone Mode: A firewall can act as an endpoint for a site-to-site Virtual Private Network (VPN) connection. In this mode, the firewall establishes secure communication tunnels between different locations or networks, ensuring the confidentiality and integrity of data transmitted over the VPN.

upvoted 1 times

✉  **jonathan126** 1 month, 1 week ago

I think C is also correct:

"This document describes how to configure Remote Access (RA) Virtual Private Network (VPN) on Cisco Adaptive Security Appliance (ASA) firewall in Multiple Context (MC) mode using the CLI. It shows the Cisco ASA in multiple context mode supported/unsupported features and licensing requirement with respect to RA VPN."

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-firewalls/200353-ASA-Multi-Context-Mode-Remote-Access-A.html>

upvoted 2 times

✉  **studying_1** 3 weeks, 6 days ago

I agree, I think it is C & E
upvoted 1 times

✉  **studying_1** 3 weeks, 6 days ago

i guess it is A and C,
functions of firewall
Controlling and blocking access. Firewalls can be used for controlling and blocking access to certain websites and online services to prevent unauthorized use. For example, an organization can use a firewall to block access to objectionable websites to ensure employees comply with company policies when browsing the internet.
Secure remote access. Firewalls can be used to grant secure remote access to a network through a virtual private network (VPN) or other secure remote access technology.
upvoted 1 times

✉  **bisiyemo1** 1 month, 1 week ago

Selected Answer: AB

A and B for sure
upvoted 2 times

Question #1077

Topic 1

What is the maximum number of concurrent Telnet sessions that a Cisco WLC supports?

- A. 3
- B. 5
- C. 6
- D. 15

Correct Answer: B

 **Joshrzo01** 1 week, 1 day ago

Correct https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/wireless/controller/8-1/configuration-guide/b_cg81/b_cg81_chapter_011.html.xml#:~:text=The%20valid%20range%20is%200,Telnet%2FSSH%20sessions%20are%20disallowed.

upvoted 1 times

 **4aynick** 1 week, 3 days ago

default, vty 0 4 for telnet, 5 15 for ssh
0,1,2,3,4 = 5 sessions in same time can be used for telnet

upvoted 1 times

 **JY888** 3 weeks, 3 days ago

Selected Answer: B

ChatGPT says 5 but sometimes ChatGPT is wrong.

upvoted 2 times

Question #1078

Topic 1

Which 802.11 management frame type is sent when a client roams between access points on the same SSID?

- A. Reassociation Request
- B. Authentication Request
- C. Association Request
- D. Probe Request

Correct Answer: A

 **studying_1** 1 week, 1 day ago

Answer is correct

upvoted 1 times

Question #1079

What is a functionality of the control plane in the network?

- A. It looks up an egress interface in the forwarding information base.
- B. It forwards traffic to the next hop.
- C. It exchanges topology information with other routers.
- D. It provides CLI access to the network device.

Correct Answer: C

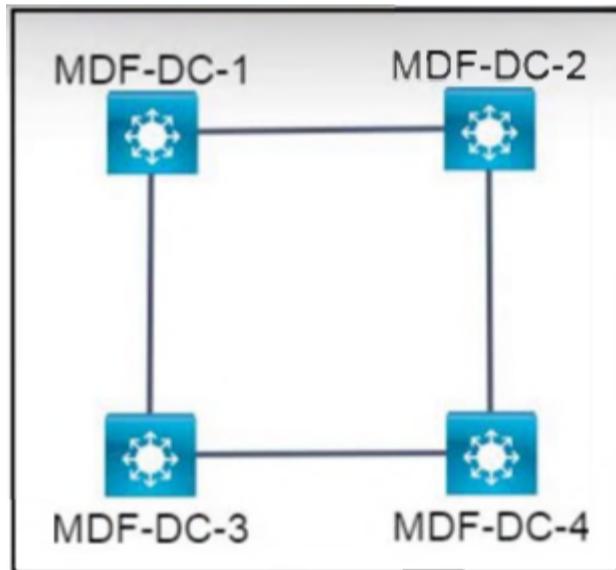
 **Bhrino** 3 weeks ago

Selected Answer: C

this also has some weirdly worded answer choices but C probably most correct. because this manages routing information so exchanging information in this case could be right

upvoted 2 times

Question #1080



Refer to the exhibit. All switches are configured with the default STP priorities. During the STP elections, which switch becomes the root bridge if all interfaces are in the same VLAN?

- A. MDF-DC-1: 0d:E0:43:96:02:30
- B. MDF-DC-2: 0d:0E:18:1B:05:97
- C. MDF-DC-4: 0d:E0:19:A1:B3:19
- D. MDF-DC-3: 0d:0E:18:2A:3C:9D

Correct Answer: B

 **sany11** Highly Voted  1 month, 1 week ago

Right ans

upvoted 5 times

 **Biggeorge123** Most Recent  3 weeks, 3 days ago

wait, shouldn't it be C? i thought the switch with the lowest IP address becomes the root bridge in this scenario?

upvoted 1 times

 **studying_1** 3 weeks, 1 day ago

yes, B has the lowest MAC address, check again, answer is correct

upvoted 2 times

Question #1081

DRAG DROP

Drag and drop the characteristic from the left onto the cable type on the right.

Answer Area

contains a single solid conductor

is typically used for DWDM optical systems spanning long distances

eliminates distortion from overlapping light pulses

is affected by electrical and magnetic interference

copper

single-mode fiber

Correct Answer:

Answer Area

contains a single solid conductor

is typically used for DWDM optical systems spanning long distances

eliminates distortion from overlapping light pulses

is affected by electrical and magnetic interference

copper

contains a single solid conductor

is affected by electrical and magnetic interference

single-mode fiber

is typically used for DWDM optical systems spanning long distances

eliminates distortion from overlapping light pulses

  **4aynick** 1 week, 3 days ago

correct without chatgpt)

upvoted 2 times

  **ac891** 3 weeks, 2 days ago

Correct according to chatgpt, but sometimes chatgpt is wrong :)

upvoted 2 times

Question #1082

Topic 1

What is represented by the word "VPN11" within this JSON schema?

```
1 [  
2 {"VPN concentrator": "VPN11", "port": "fe7/12"},  
3 {"router": "Radmin", "port": "e5/1"},  
4 {"switch": "SWbangkok", "port": "ge6/6"}  
5 ]
```

- A. key
- B. array
- C. object
- D. value

Correct Answer: D

 **Tdawg1968** 1 week, 4 days ago

I meant question 1084

upvoted 1 times

 **Tdawg1968** 1 week, 4 days ago

Contradicts question 1089. Shouldn't this be a key?

upvoted 1 times

 **studying_1** 1 week, 1 day ago

answer is correct, it is a value, if it is before ":" it's a (key), if after ":" it's a (value)

upvoted 2 times

Question #1083

Topic 1

Which port type supports the spanning-tree portfast command without additional configuration?

- A. Layer 3 main interfaces
- B. Layer 3 subinterfaces
- C. trunk ports
- D. access ports

Correct Answer: D

 **studying_1** 4 days, 21 hours ago

correct

upvoted 1 times

Question #1084

Topic 1

What is represented by the word "R29" within this JSON schema?

```
1 [  
2 {"firewall": "FW15", "interface": "e8/33"},  
3 {"switch": "SW_chicago", "interface": "ge5/26"},  
4 {"router": "R29", "interface": "fe4/25"}  
5 ]
```

- A. array
- B. key
- C. object
- D. value

Correct Answer: D

✉️  **sany11** 1 month, 1 week ago

Right ans
upvoted 4 times

Question #1085

Topic 1

What is represented in line 2 within this JSON schema?

```
1 [  
2 {"switch": "SW16", "interface": "fe3/43"},  
3 {"load balancer": "LBmiami", "interface": "e0/1"},  
4 {"firewall": "FWboston", "interface": "ge6/12"}  
5 ]
```

- A. object
- B. value
- C. key
- D. array

Correct Answer: A

✉️  **Bhrino** 3 weeks ago

Selected Answer: A
objects are show in {} curly brackets
upvoted 2 times

Question #1086

DRAG DROP

Drag and drop the characteristic from the left onto the cable type on the right.

Answer Area

contains a single solid conductor

is typically used for DWDM optical systems spanning long distances

uses a single wavelength of light

transmits data in the form of electronic signals

copper

single-mode fiber

Correct Answer:

Answer Area

contains a single solid conductor

is typically used for DWDM optical systems spanning long distances

uses a single wavelength of light

transmits data in the form of electronic signals

copper

contains a single solid conductor

transmits data in the form of electronic signals

single-mode fiber

is typically used for DWDM optical systems spanning long distances

uses a single wavelength of light

 **studying_1** 1 week, 1 day ago

Answer is correct

upvoted 2 times

Question #1087

DRAG DROP

Drag and drop the characteristic from the left onto the cable type on the right.

Answer Area

is typically used in small office applications

is typically used for internal datacenter connectivity

has increased attenuation over long distances

is comprised of shielded and unshielded twisted pairs

copper

multimode fiber

Correct Answer:

Answer Area

is typically used in small office applications

is typically used for internal datacenter connectivity

has increased attenuation over long distances

is comprised of shielded and unshielded twisted pairs

copper

is typically used in small office applications

is comprised of shielded and unshielded twisted pairs

multimode fiber

is typically used for internal datacenter connectivity

has increased attenuation over long distances

 **4aynick** 1 week, 3 days ago

correct

upvoted 2 times

Question #1088

DRAG DROP

Drag and drop the characteristic from the left onto the cable type on the right.

Answer Area

is ideal longer distances with little loss of integrity

is not easily broken

contains a single solid conductor

has minimal light reflection as it travels down the core

single-mode fiber

copper

Correct Answer:

Answer Area

is ideal longer distances with little loss of integrity

is not easily broken

contains a single solid conductor

has minimal light reflection as it travels down the core

single-mode fiber

is ideal longer distances with little loss of integrity

has minimal light reflection as it travels down the core

copper

is not easily broken

contains a single solid conductor

Question #1089

Topic 1

DRAG DROP

Drag and drop the characteristic from the left onto the cable type on the right.

Answer Area

uses a single wavelength on light

becomes distorted at longer lengths

transmits data up to 100 Gbits which degrades over distance

has minimal light reflection as it travels down the core

single-mode fiber

multimode fiber

Correct Answer:

Answer Area

uses a single wavelength on light

becomes distorted at longer lengths

transmits data up to 100 Gbits which degrades over distance

has minimal light reflection as it travels down the core

single-mode fiber

uses a single wavelength on light

has minimal light reflection as it travels down the core

multimode fiber

becomes distorted at longer lengths

transmits data up to 100 Gbits which degrades over distance

Question #1090

DRAG DROP

Drag and drop the IPv6 address from the left onto the type on the right.

Answer Area

ff00:c279:edd5:99c4:b0de:fc11:4b12:12

Global Unicast

fe80:e6ab:b5f9:c358:ea58:0029:b4db:7

Unique Local

fc00:1664:bc95:3c7a:c300:c468:3969:3

Link-Local Unicast

2000:2eb8:3e5f:376c:da66:bf1d:d36a:1

Multicast

Correct Answer:**Answer Area**

2000:2eb8:3e5f:376c:da66:bf1d:d36a:1

fc00:1664:bc95:3c7a:c300:c468:3969:3

fe80:e6ab:b5f9:c358:ea58:0029:b4db:7

ff00:c279:edd5:99c4:b0de:fc11:4b12:12

Question #1091

DRAG DROP

Drag and drop the characteristic from the left onto the cable type on the right.

Answer Area

uses a single wavelength of light

is comprised of shielded and unshielded twisted pairs

contains a conductor, bedding, and sheathing

has a core diameter of 9 microns

single-mode fiber

copper

Correct Answer:

Answer Area

uses a single wavelength of light

is comprised of shielded and unshielded twisted pairs

contains a conductor, bedding, and sheathing

has a core diameter of 9 microns

single-mode fiber

uses a single wavelength of light

has a core diameter of 9 microns

copper

is comprised of shielded and unshielded twisted pairs

contains a conductor, bedding, and sheathing

Question #1092

DRAG DROP

Drag and drop the IPv6 address from the left onto the type on the right.

Answer Area

ff00:a648:6ad8:4591:80a2:75db:4b5f:12

Global Unicast

fe80:9885:e8c7:6f41:ac11:b954:cc04:7

Unique Local

fc00:6fd1:6158:034c:6144:eafe:8da6:3

Link-Local Unicast

2000:fda9:65b0:e8c0:1d84:6369:2daa:1

Multicast

Correct Answer:**Answer Area**

ff00:a648:6ad8:4591:80a2:75db:4b5f:12

2000:fda9:65b0:e8c0:1d84:6369:2daa:1

fe80:9885:e8c7:6f41:ac11:b954:cc04:7

fc00:6fd1:6158:034c:6144:eafe:8da6:3

fc00:6fd1:6158:034c:6144:eafe:8da6:3

fe80:9885:e8c7:6f41:ac11:b954:cc04:7

2000:fda9:65b0:e8c0:1d84:6369:2daa:1

ff00:a648:6ad8:4591:80a2:75db:4b5f:12

Question #1093

DRAG DROP

Drag and drop the characteristic from the left onto the cable type on the right.

Answer Area

is ideal over longer distances with little loss of integrity

uses a single wavelength on light

has a core diameter of either 62.5 or 50 microns

is typically used for DWDM optical systems spanning long distances

single-mode fiber

multimode fiber

Correct Answer:

Answer Area

is ideal over longer distances with little loss of integrity

uses a single wavelength on light

has a core diameter of either 62.5 or 50 microns

is typically used for DWDM optical systems spanning long distances

single-mode fiber

is ideal over longer distances with little loss of integrity

uses a single wavelength on light

multimode fiber

is typically used for DWDM optical systems spanning long distances

has a core diameter of either 62.5 or 50 microns

jonathan126 1 month, 2 weeks ago

I think the answer should be:

single mode

- long distance

- DWDM

-> "WDM and DWDM use single-mode fiber to carry multiple lightwaves of differing frequencies.", see link https://www.cisco.com/c/dam/global/de_at/assets/docs/dwdm.pdf

multimode

- single wavelength

- core diameter 62.5 or 50 microns

-> "Typical cores sizes are 50 microns and 62.5 microns and a typical operating wavelength for multi-mode fiber is 850nm.", see link <https://blogs.cisco.com/sp/fiberopticspt2singlumultifiber>

-> "Most of Cisco's multimode transceivers are single-wavelength devices operating at 850 nm", see link <https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/diff-om4-om5-multimode-fiber-wp.html>

upvoted 2 times

hamish88 1 month, 2 weeks ago

Single mode: DWDM, Single wavelength, and long distance.

Multimode: Core diameter between 60 and 62.5.

I can't say if the question is incorrect, but in the exam, I would drop DWDM under multimode if I had no other choices.

upvoted 1 times

SamSerious365 1 month, 3 weeks ago

I think we should switch answers "Use a single wavelength on light" and "is used for DWDM"

upvoted 2 times

Question #1094

Topic 1

What is a characteristic of private IPv4 addressing?

- A. is used without allocation from a regional internet authority
- B. is used when traffic on the subnet must traverse a site-to-site VPN to an outside organization
- C. reduces the forwarding table on network routers
- D. provides unlimited address ranges

Correct Answer: A **studying_1** 1 week, 1 day ago

correct

upvoted 2 times

Question #1095

Topic 1

Which interface condition is occurring in this output?

```
R16# show interface fa0/0
FastEthernet0/0 is up, line protocol is up
Hardware is DEC21140, address is ca02.7788.0000 (bia ca02.7788.0000)
Description: sanfrancisco_subnet
Internet address is 10.32.102.2/30
MTU 1397 bytes, BW 100000 Kbit/sec, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (60 sec)
Full-duplex, 100 Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:01, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/300/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/300 (size/max)
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
7331 packets input, 7101162 bytes
Received 267 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
3927 packets output, 1440403 bytes, 0 underruns
0 output errors, 0 collisions, 0 Interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

- A. bad NIC
- B. high throughput
- C. queueing
- D. broadcast storm

Correct Answer: C

 **JY888** 3 weeks, 3 days ago

Selected Answer: C

There are no issues so I guess C is correct.

upvoted 2 times

 **studying_1** 1 week, 1 day ago

I agree, looking at the amount of input packets vs the amount of output packets, idk for sure lol

upvoted 1 times

 **Peter_panda** 1 month ago

Selected Answer: A

By exclusion, I would say the NIC is bad

upvoted 1 times

 **studying_1** 1 week, 1 day ago

the amount of input packets is double the amount of output packets, doesn't that mean it's queuing? i guess the answer is correct

upvoted 1 times

Question #1096

Topic 1

What is a characteristic of private IPv4 addressing?

- A. is used when the ISP requires the new subnet to be advertised to the internet for web services
- B. provides unlimited address ranges
- C. is used when the network has multiple endpoint listeners
- D. alleviates the shortage of IPv4 addresses

Correct Answer: D **studying_1** 1 week, 1 day ago

correct

upvoted 1 times

Question #1097

Topic 1

What is a characteristic of private IPv4 addressing?

- A. is used when traffic on the subnet must traverse a site-to-site VPN to an outside organization
- B. allows endpoints to communicate across public network boundaries
- C. is used on hosts that communicate only with other internal hosts
- D. reduces network complexity

Correct Answer: C **studying_1** 1 week, 1 day ago

correct

upvoted 2 times

Question #1098

Topic 1

What is a characteristic of private IPv4 addressing?

- A. traverses the internet when an outbound ACL is applied
- B. alleviates the shortage of IPv4 addresses
- C. is used when the ISP requires the new subnet to be advertised to the internet for web services
- D. enables secure connectivity over the internet

Correct Answer: B **studying_1** 1 week, 1 day ago

correct

upvoted 1 times

Question #1099

Topic 1

Which interface condition is occurring in this output?

```
R43# show interface fa0/0
FastEthernet0/0 is up, line protocol is up
Hardware is DEC21140, address is ca02.7788.0000 (bia ca02.7788.0000)
Description: munich_subnet
Internet address is 10.32.102.2/30
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
reliability 255/255, txload 255/255, rxload 255/255
Encapsulation ARPA, loopback not set
Keepalive set (60 sec)
Full-duplex, 100 Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:01, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/300/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/300 (size/max)
30 second input rate 200234873 bits/sec, 0 packets/sec
30 second output rate 233830309 bits/sec, 0 packets/sec
7331 packets input, 7101162 bytes
Received 267 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
3927 packets output, 1440403 bytes, 0 underruns
0 output errors, 0 collisions, 0 Interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

- A. broadcast storm
- B. duplex mismatch
- C. high throughput
- D. queueing

Correct Answer: D

 **Mizuchan** 1 week, 6 days ago

Selected Answer: C

RX and TX 255/255
upvoted 1 times

 **Bhrino** 3 weeks ago

Selected Answer: C

The answer is C due to high input and out put and
high Rx/tx loads
upvoted 2 times

 **Peter_panda** 1 month ago

Selected Answer: A

High bandwidth usage, but zero packets in the last 30 seconds, it seems that the traffic is comprised of L2 broadcasts
upvoted 1 times

 **ac891** 3 weeks, 2 days ago

Where do you see high bandwidth when you have 100/full speed ... ?
upvoted 1 times

 **Rydaz** 4 weeks, 1 day ago

I would go with C, high throughput
upvoted 2 times

Question #1100

Topic 1

What is a characteristic of private IPv4 addressing?

- A. is used when the ISP requires the new subnet to be advertised to the internet for web services
- B. allows multiple companies to use the same addresses without conflict
- C. is used on the external interface of a firewall
- D. allows endpoints to communicate across public network boundaries

Correct Answer: B

Question #1101

Topic 1

DRAG DROP

Drag and drop the IPv6 address from the left onto the type on the right.

Answer Area

ff00:0a7c:cf36:cd7c:6dad:44fa:c11c:12
fe80:27bb:1ef9:6b3d:b347:686f:f3b7:7
fc00:9e81:2346:4929:7fec:34e9:7b8c:3
2000:0962:6dee:8c78:93b8:c429:c78d:1

Global Unicast
Unique Local
Link-Local Unicast
Multicast

Correct Answer:**Answer Area**

ff00:0a7c:cf36:cd7c:6dad:44fa:c11c:12
fe80:27bb:1ef9:6b3d:b347:686f:f3b7:7
fc00:9e81:2346:4929:7fec:34e9:7b8c:3
2000:0962:6dee:8c78:93b8:c429:c78d:1

2000:0962:6dee:8c78:93b8:c429:c78d:1
fc00:9e81:2346:4929:7fec:34e9:7b8c:3
fe80:27bb:1ef9:6b3d:b347:686f:f3b7:7
ff00:0a7c:cf36:cd7c:6dad:44fa:c11c:12

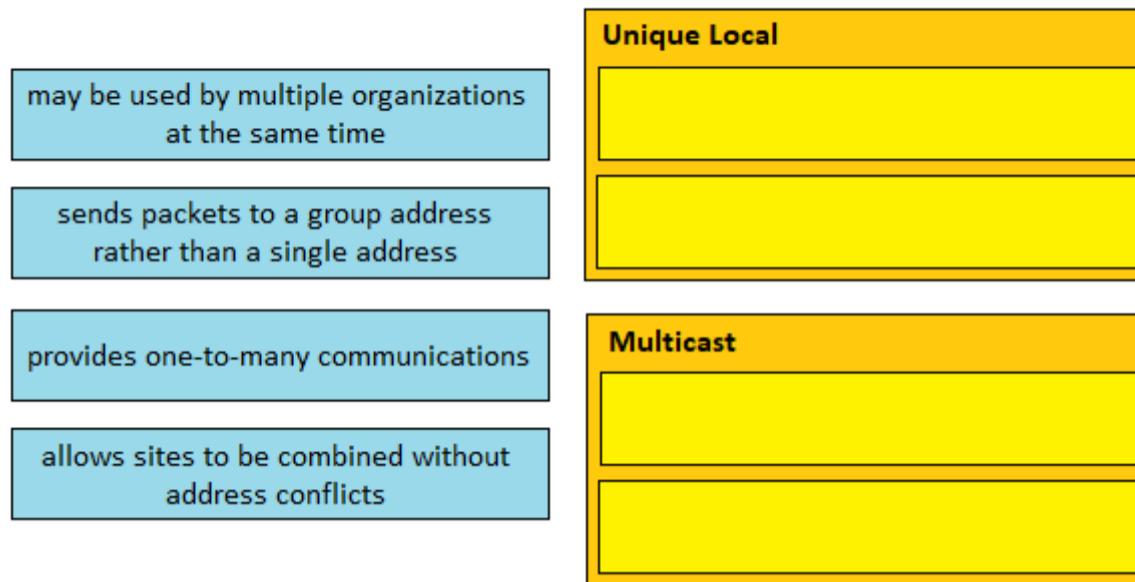
Question #1102

Topic 1

DRAG DROP

Drag and drop the characteristic from the left onto the IPv6 address type on the right.

Answer Area



Answer Area

Correct Answer:

- may be used by multiple organizations at the same time
- sends packets to a group address rather than a single address
- provides one-to-many communications
- allows sites to be combined without address conflicts

- | IPv6 Address Type | Characteristics |
|-------------------|---|
| Unique Local | may be used by multiple organizations at the same time
allows sites to be combined without address conflicts |
| Multicast | sends packets to a group address rather than a single address
provides one-to-many communications |

 **studying_1** 1 week, 1 day ago

Answers are correct

upvoted 2 times

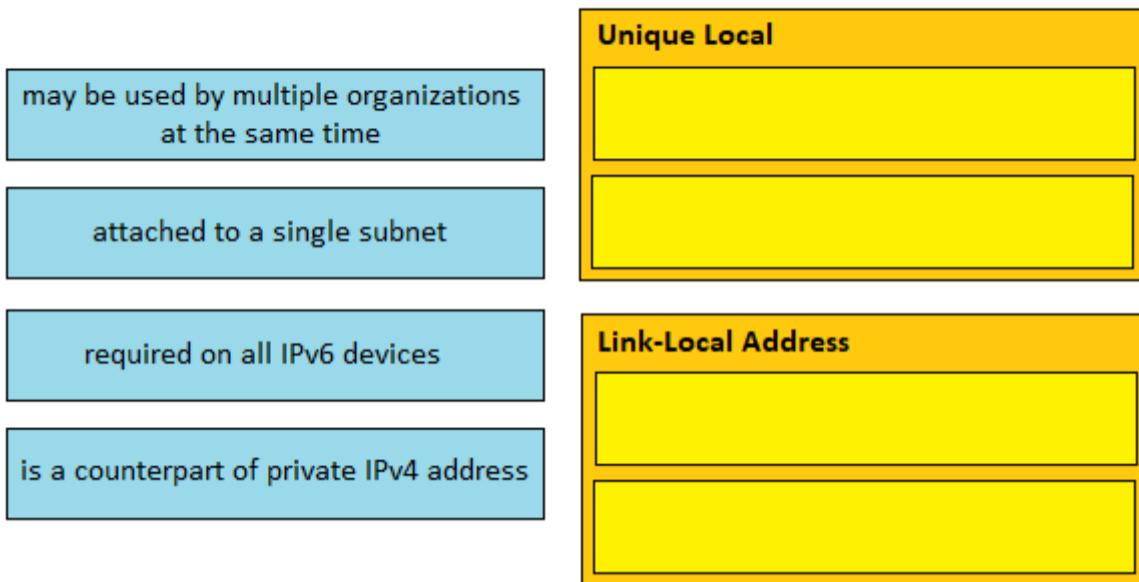
Question #1103

Topic 1

DRAG DROP

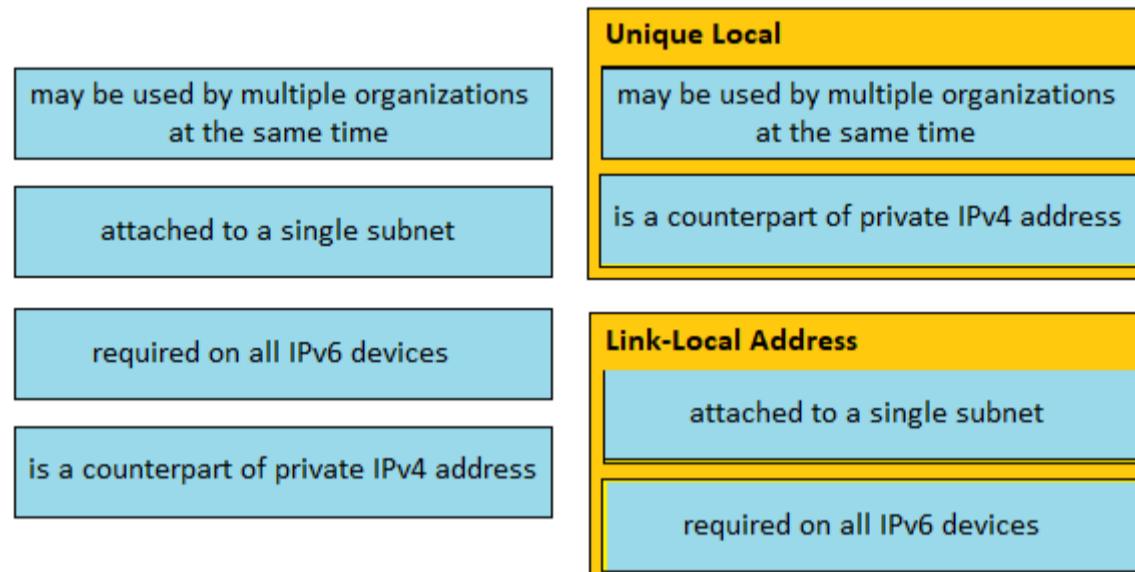
Drag and drop the characteristic from the left onto the IPv6 address type on the right.

Answer Area



Answer Area

Correct Answer:

 **Bhrino** 3 weeks ago

answers are correct

upvoted 2 times

Question #1104

What is a characteristic of an SSID in wireless networks?

- A. identifies an access point on a WLAN
- B. uses the password to connect to an access point
- C. uses policies to prevent unauthorized users
- D. uses a case-sensitive text string

Correct Answer: D

 **studying_1** 1 week, 1 day ago

Selected Answer: D

Answer is D

upvoted 1 times

 **studying_1** 1 week, 1 day ago

Selected Answer: A

D is correct

upvoted 1 times

 **studying_1** 1 week, 1 day ago

sorry voted wrong, answer is D

upvoted 1 times

 **Bhrino** 3 weeks ago

Selected Answer: D

The answer could be A or D because while it does help with security it not specific defining characteristic of it. Really I go with D because that more of a characteristic

upvoted 1 times

 **ac891** 3 weeks, 2 days ago

Selected Answer: C

B,D,A = Wrong

upvoted 1 times

Question #1105

What is a characteristic of private IPv4 addressing?

- A. reduces network complexity
- B. is used on hosts that communicate only with other internal hosts
- C. simplifies the addressing in the network
- D. reduces network maintenance costs

Correct Answer: B

Question #1106

What is a characteristic of encryption in wireless networks?

- A. identifies an access point on a WLAN
- B. uses the password to connect to an access point
- C. uses integrity checks to identify forgery attacks in the frame
- D. uses authentication protocols to secure a network

Correct Answer: D

 **Bhrino** 3 weeks ago

Selected Answer: C

While I don't like the wording of any of these answers C sounds more right. It really used to stop people from intercepting messages sent over a wireless network. In a way it keeps the integrity of the message

upvoted 1 times

 **ac891** 3 weeks, 2 days ago

Selected Answer: D

Encryption can also be used to verify the identity of the communicating parties by requiring the use of authentication protocols, such as WPA2-PSK or EAP-TLS, to establish a secure connection.

upvoted 1 times

 **ac891** 3 weeks, 2 days ago

<https://www.geeksforgeeks.org/wireless-encryption-methods-in-cisco/>

upvoted 1 times

 **studying_1** 1 week, 1 day ago

Answer is C, its encryption, D is about authentication

upvoted 1 times

 **JY888** 3 weeks, 3 days ago

Selected Answer: C

C. uses integrity checks to identify forgery attacks in the frame.

Encryption in wireless networks is a security mechanism used to protect data transmitted over wireless networks from unauthorized access. Encryption involves converting plain text into cipher text using a cryptographic algorithm and a key. The encrypted data is then transmitted over the wireless network and can only be decrypted by authorized recipients who possess the key. One of the features of encryption is the use of integrity checks to identify forgery attacks in the frame, ensuring that the data has not been tampered with during transmission.

upvoted 4 times

Question #1107

What is a characteristic of private IPv4 addressing?

- A. simplifies the addressing in the network
- B. complies with PCI regulations
- C. reduces the forwarding table on network routers
- D. is used on hosts that communicate only with other internal hosts

Correct Answer: D

 **Bhrino** 3 weeks ago

Selected Answer: D

D is almost an exact purpose of Private addresses

upvoted 2 times

Question #1108

Topic 1

What is a characteristic of an SSID in wireless networks?

- A. eliminates network piggybacking
- B. prompts a user for a login ID
- C. broadcasts a beacon signal to announce its presence by default
- D. must include a combination of letters and numbers

Correct Answer: C

 **studying_1** 6 days, 9 hours ago

Selected Answer: C

correct, SSID broadcast a beacon message periodically & stations listen for these messages from the AP, & it's called passive scanning, active scanning probe request & probe response

upvoted 1 times

Question #1109

Topic 1

What is a characteristic of encryption in wireless networks?

- A. provides increased protection against spyware
- B. prompts a user for a login ID
- C. uses ciphers to detect and prevent zero-day network attacks
- D. prevents the interception of data as it transits a network

Correct Answer: D

 **Bhrino** 3 weeks ago

while some can argue for A. D is more correct because while wireless networks are easier to use and connect to that makes it open for people to intercept the message and view. really Id say D is the primary purpose of this.

upvoted 1 times

Question #1110

Topic 1

What is a characteristic of an SSID in wireless networks?

- A. intercepts data threats before they attack a network
- B. encodes connections at the sending and receiving ends
- C. broadcasts a beacon signal to announce its presence by default
- D. identifies an access point on a WLAN

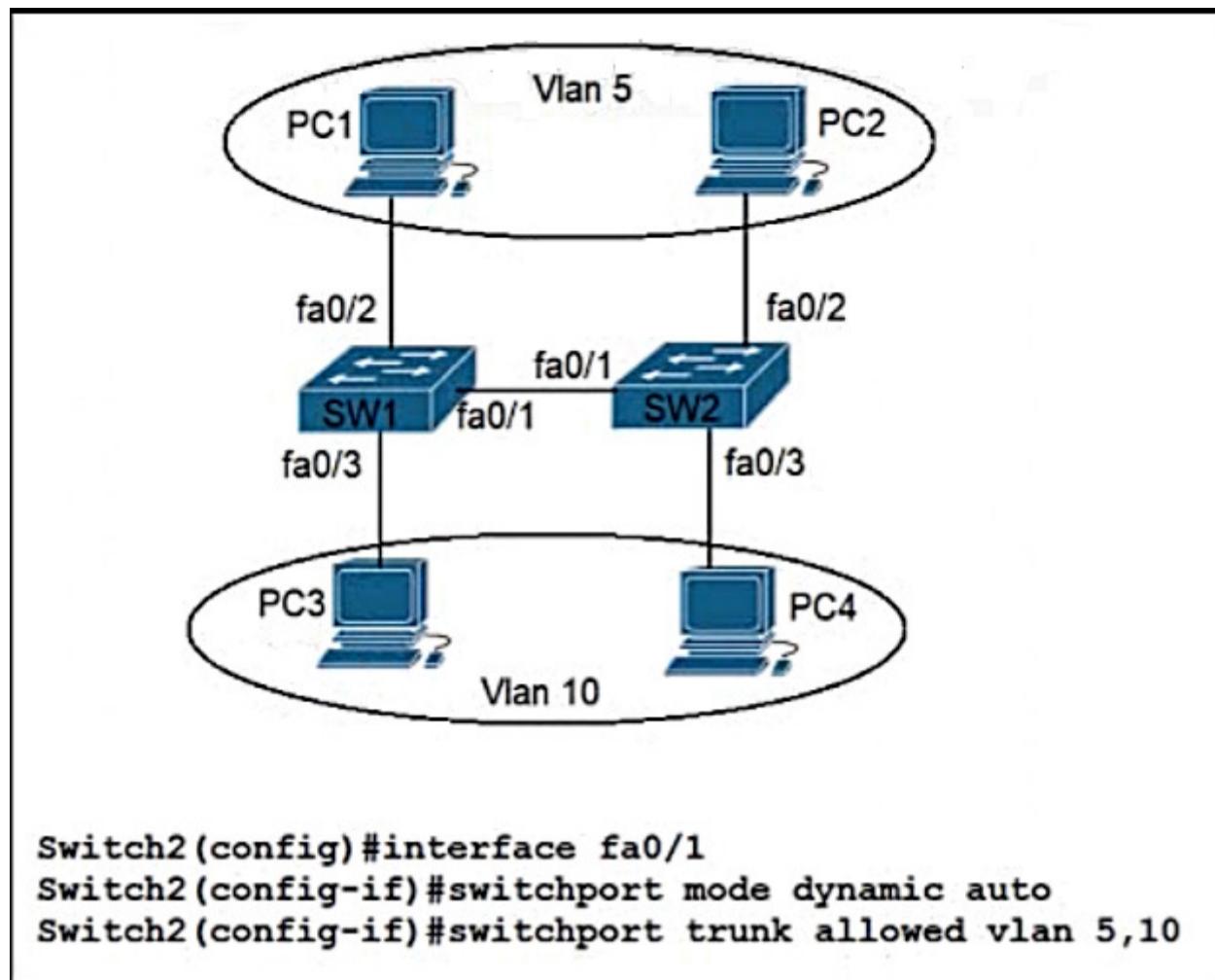
Correct Answer: C

 **Bhrino** 3 weeks ago

answer is correct

upvoted 1 times

Question #1111



Refer to the exhibit. SW2 is replaced because of a hardware failure. A network engineer starts to configure SW2 by copying the fa0/1 interface configuration from SW1. Which command must be configured on the fa0/1 interface of SW2 to enable PC1 to connect to PC2?

- A. switchport mode trunk
- B. switchport trunk native vlan 10
- C. switchport mode access
- D. switchport trunk allowed remove 10

Correct Answer: A

Bhrino 3 weeks ago

Selected Answer: A

have to tell the switch that the specific interface is a trunk port ie A
upvoted 2 times

Question #1112

Topic 1

DRAG DROP

Drag and drop the DHCP snooping terms from the left onto the descriptions on the right.

Answer Area

DHCP server	list of hosts on the network that are unknown to the administrative domain
snooping binding database	network component that propagates IP addresses to hosts on the network
spurious DHCP server	internal device under the control of the network administrator
trusted	unknown DHCP server within an administrative domain
untrusted	default state of all interfaces

Answer Area

Correct Answer:

DHCP server	snooping binding database
snooping binding database	DHCP server
spurious DHCP server	trusted
trusted	spurious DHCP server
untrusted	untrusted

 **blablablabla123** 2 weeks, 5 days ago

can anyone post the solution?

upvoted 1 times

 **Bhrino** 3 weeks ago

answers are right

upvoted 2 times

 **bisiyemo1** 4 weeks ago

The answers are correct

upvoted 3 times

Question #1113

Topic 1

What is a characteristic of private IPv4 addressing?

- A. composed of up to 65,536 available addresses
- B. issued by IANA in conjunction with an autonomous system number
- C. used without tracking or registration
- D. traverse the Internet when an outbound ACL is applied

Correct Answer: C

 **Bhrino** 3 weeks ago

Selected Answer: C

because private ips are private people don't have to register to get them so its c
upvoted 2 times

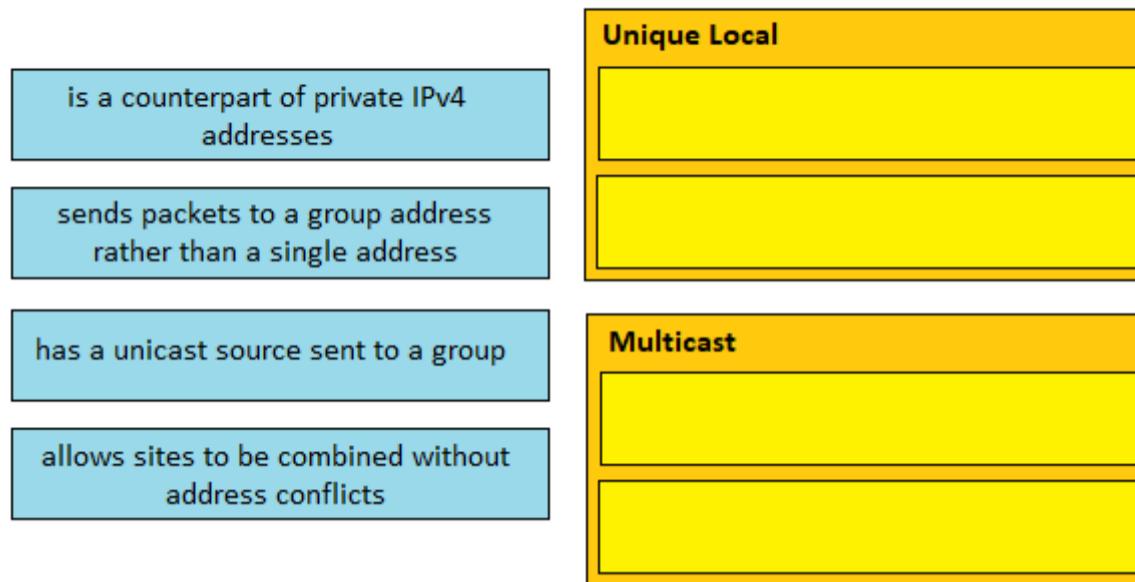
Question #1114

Topic 1

DRAG DROP

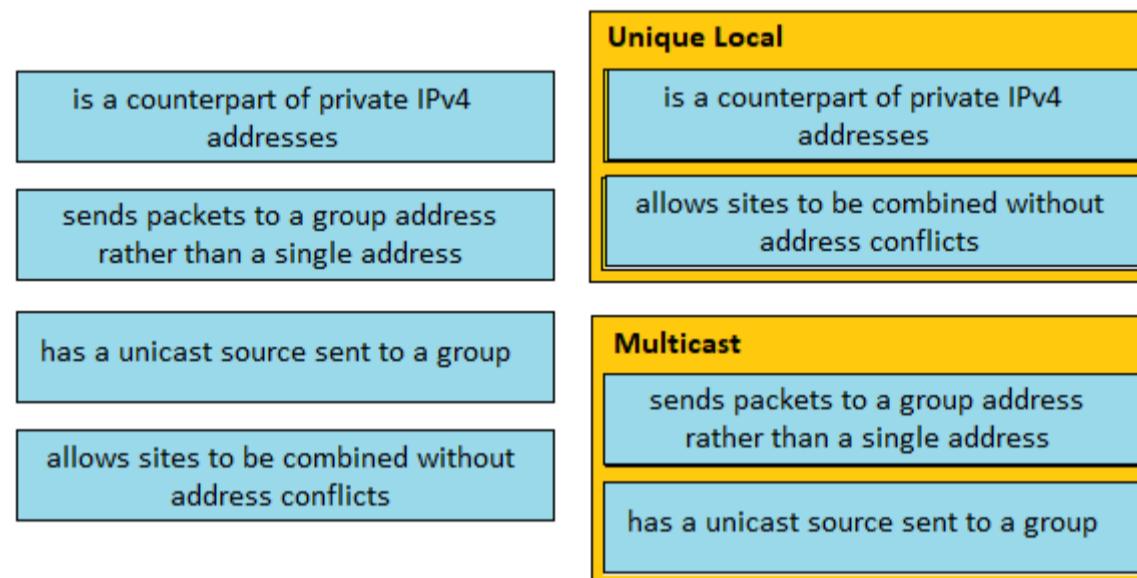
Drag and drop the characteristic from the left onto the IPv6 address type on the right.

Answer Area



Answer Area

Correct Answer:



 **Bhrino** 3 weeks ago

Answer is correct Ip v6 (unicast address) = Ip v4 (private addresses) meaning there will be no problems with overlapping ips with different networks

upvoted 1 times

Question #1115

DRAG DROP

Drag and drop the characteristic from the left onto the cable type on the right.

Answer Area

uses a single wavelength on light

becomes distorted at longer lengths

is typically used for internal datacenter connectivity

has minimal light reflection as it travels down the core

multimode fiber**single-mode fiber****Correct Answer:**

uses a single wavelength on light

becomes distorted at longer lengths

is typically used for internal datacenter connectivity

has minimal light reflection as it travels down the core

multimode fiber

is typically used for internal datacenter connectivity

becomes distorted at longer lengths

single-mode fiber

uses a single wavelength on light

has minimal light reflection as it travels down the core

 **Bhrino** 3 weeks ago

answer is correct a single mode goes further because its one light and doesn't get reflected or distorted while with multimode while cheaper with the extra lights after a certain range can get weaker

upvoted 2 times

Question #1116

How does MAC learning function on a switch?

- A. broadcasts frames to all ports without queueing
- B. sends an ARP request to locate unknown destinations
- C. adds unknown source MAC addresses to the address table
- D. sends a retransmission request when a new frame is received

Correct Answer: C

 **Bhrino** 3 weeks ago

Selected Answer: C

The answer is c because when a switch receives PDUs it examines the mac address to see if its already in its table and if its not it then adds it to its own table this process is called mac address learning

upvoted 1 times

Question #1117

Topic 1

Which interface condition is occurring in this output?

```
R45# show interface fa0/0
FastEthernet0/0 is up, line protocol is up
Hardware is DEC21140, address is ca02.7788.0000 (bia ca02.7788.0000)
Description: atlanta_subnet
Internet address is 10.32.102.2/30
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
reliability 255/255, txload 255/255, rxload 255/255
Encapsulation ARPA, loopback not set
Keepalive set (60 sec)
Full-duplex, 100 Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:01, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/300/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/300 (size/max)
30 second input rate 234712855 bits/sec, 0 packets/sec
30 second output rate 228528957 bits/sec, 0 packets/sec
7331 packets input, 7101162 bytes
Received 267 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
3927 packets output, 1440403 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

- A. broadcast storm
- B. collisions
- C. high throughput
- D. duplex mismatch

Correct Answer: C

 **Bhrino** 3 weeks ago

Selected Answer: C

it is C because not only is the rxload and txload maxed there are no input errors and the input and out rates are high
upvoted 1 times

 **ac891** 3 weeks, 2 days ago

Selected Answer: C

Notice the txload/rxload
upvoted 2 times

Question #1118

Topic 1

What is a characteristic of an SSID in wireless networks?

- A. converts electrical current to radio waves
- B. uses policies to prevent unauthorized users
- C. broadcasts a beacon signal to announce its presence by default
- D. prompts a user for a login ID

Correct Answer: C

 **Bhrino** 3 weeks ago

honestly all of the other choices besides c doesn't make sense to me and ssids tell people which one they are connecting to
upvoted 2 times

Question #1119

Topic 1

DRAG DROP

Drag and drop the IPv6 address from the left onto the type on the right.

Answer Area

2000:87aa:84ab:fdd9:5ac3:41a5:ef72:1

Global Unicast

fc00:c51f:922d:0c12:9c54:7644:28f5:3

Link-Local Unicast

fe80:ccc7:17f1:5d15:f611:5cea:ef92:7

Multicast

ff00:520a:3e47:de13:fe6f:476e:5325:12

Unique Local

Answer Area

2000:87aa:84ab:fdd9:5ac3:41a5:ef72:1

2000:87aa:84ab:fdd9:5ac3:41a5:ef72:1

fc00:c51f:922d:0c12:9c54:7644:28f5:3

fe80:ccc7:17f1:5d15:f611:5cea:ef92:7

fe80:ccc7:17f1:5d15:f611:5cea:ef92:7

ff00:520a:3e47:de13:fe6f:476e:5325:12

ff00:520a:3e47:de13:fe6f:476e:5325:12

fc00:c51f:922d:0c12:9c54:7644:28f5:3

Correct Answer:

 **Bhrino** 3 weeks ago

give answer is correct

ff = multi

2000 = global

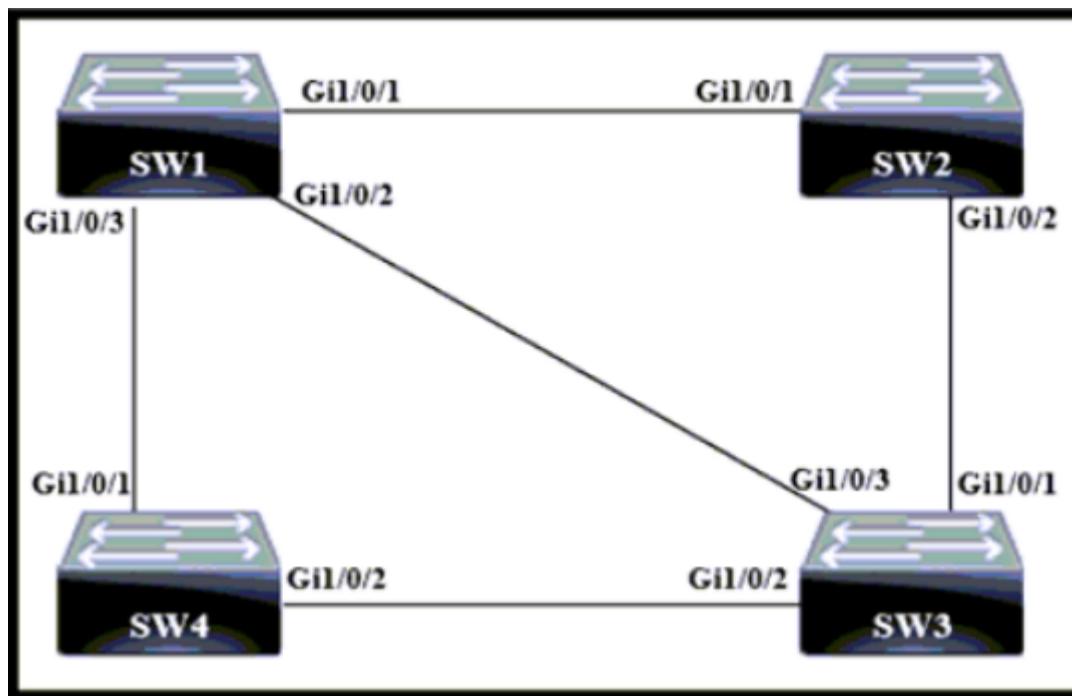
fc /fd = unique local

fe8 = link local

upvoted 2 times

Question #1120

Topic 1



Refer to the exhibit. Which switch becomes the root bridge?

A. SW3 -

Bridge Priority - 57344 -

mac-address 0b:bb:e0:96:a3:86

B. SW2 -

Bridge Priority - 57344 -

mac-address 00:b6:c5:17:8e:89

C. SW1 -

Bridge Priority - 28672 -

mac-address 0c:d4:e9:1d:3c:24

D. SW4 -

Bridge Priority - 28672 -

mac-address 0b:09:23:33:b8:91

Correct Answer: D

 **Bhrino** 3 weeks ago

The answer is D because this switch has the lowest priority and mac address

upvoted 2 times

Question #1121

Topic 1

Which interface is used to send traffic to the destination network?

- O 10.139.120.253.29 [110/9443] via G0/20
- O 10.139.120.253.29 [110/29560] via G0/16
- R 10.139.120.253.29 [120/12] via G0/11
- R 10.139.120.253.29 [120/6] via G0/9

- A. G0/9
- B. G0/20
- C. G0/16
- D. G0/11

Correct Answer: B **Bhrino** 3 weeks ago**Selected Answer:** B

The answer is because it has the lowest ad and metric

upvoted 2 times

Question #1122

Topic 1

What is represented by the word "fe5/42" within this JSON schema?

```
1 [
2 {"load balancer": "LB_milwaukee", "port": "fe5/42"},
3 {"VPN concentrator": "VPNadmin", "port": "e1/39"},
4 {"firewall": "FW_chicago", "port": "te3/42"},
5 ]
```

- A. array
- B. object
- C. value
- D. key

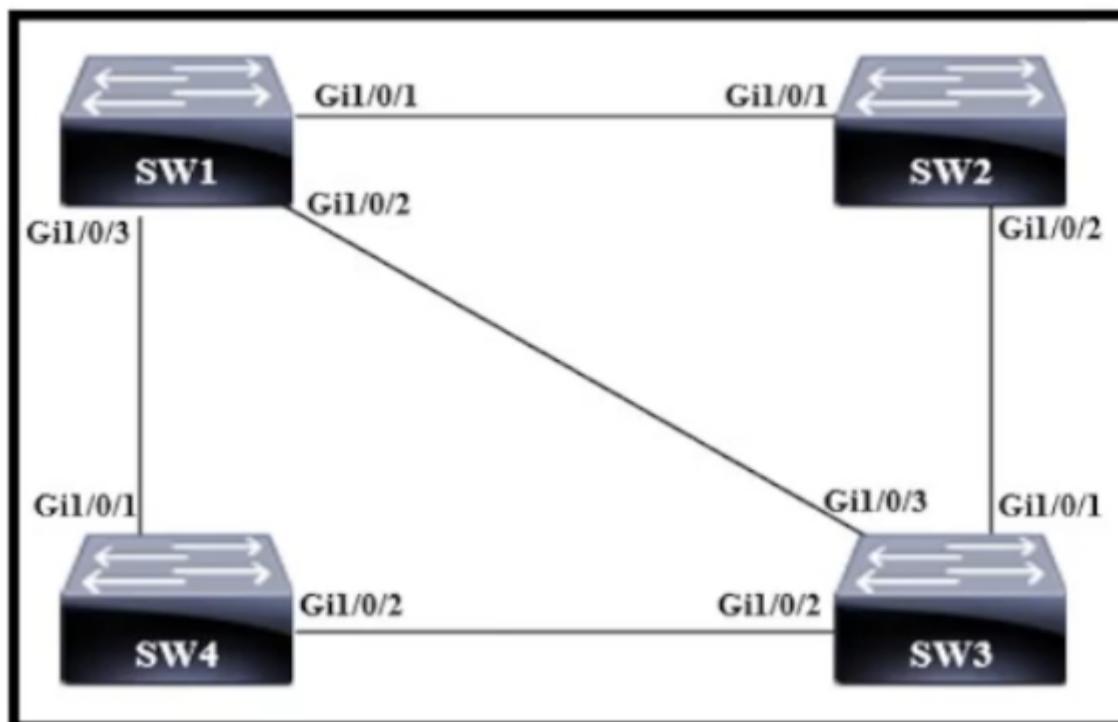
Correct Answer: C **Bhrino** 3 weeks ago**Selected Answer:** C

The answer is c because in this array this is specifically asking about a key : value pair. In this instance it would also be considered a string

upvoted 2 times

Question #1123

Topic 1



Refer to the exhibit. Which switch becomes the root bridge?

A. SW 1 -

Bridge Priority - 32768 -

mac-address 0f:d7:9e:13:ab:82

B. SW 2 -

Bridge Priority - 40960 -

mac-address 05:d8:33:09:8f:89

C. SW 3 -

Bridge Priority - 32768 -

mac-address 01:1c:6c:66:b7:70

D. SW 4 -

Bridge Priority - 40960 -

mac-address 04:44:97:51:63:17

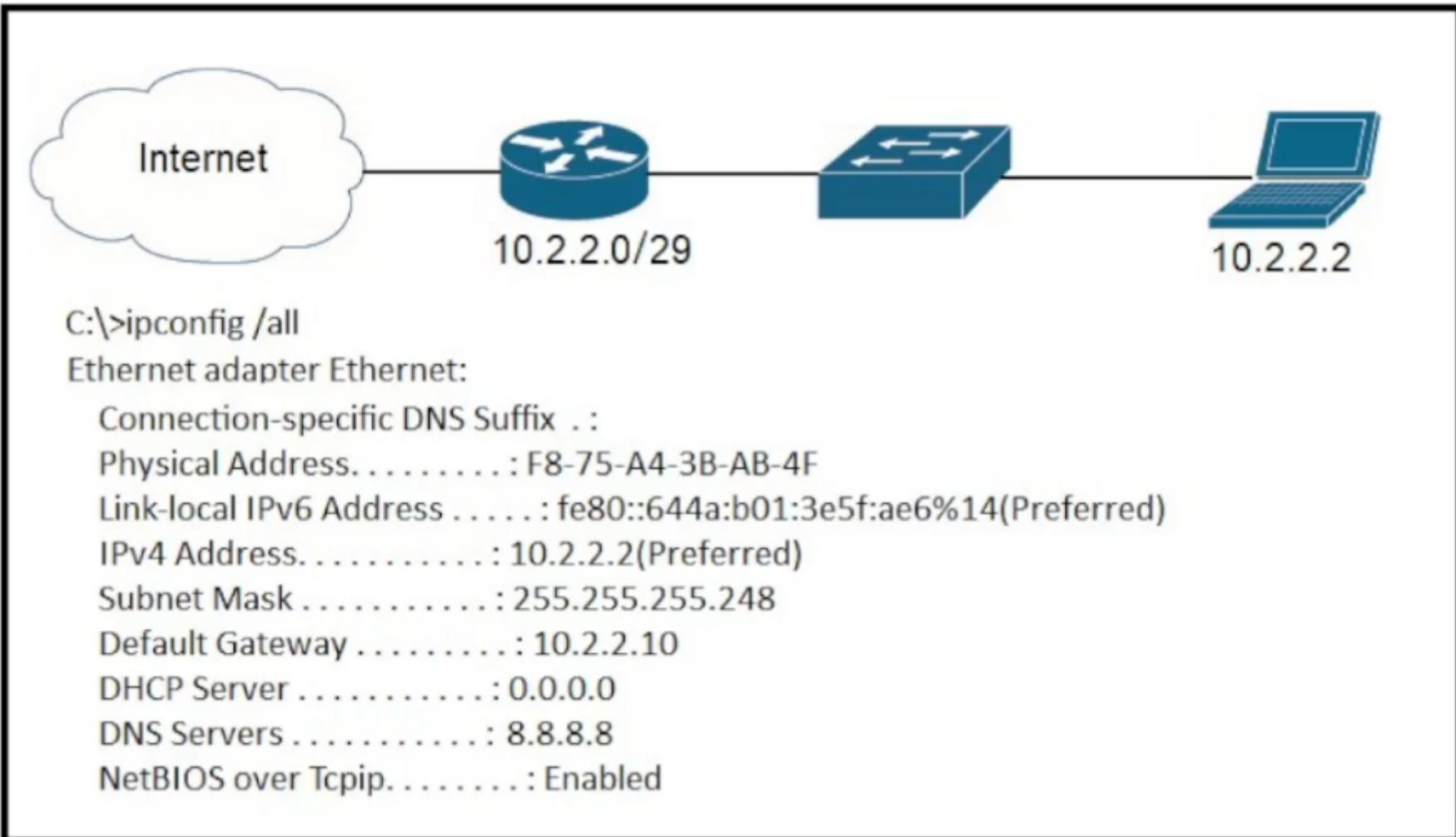
Correct Answer: C

 **studying_1** 5 days, 13 hours ago

Selected Answer: C

Answer is correct, lowest priority, and lowest MAC address
upvoted 2 times

Question #1124



Refer to the exhibit. A newly configured PC fails to connect to the internet by using TCP port 80 to www.cisco.com. Which setting must be modified for the connection to work?

- A. Subnet Mask
- B. DNS Servers
- C. Default Gateway
- D. DHCP Servers

Correct Answer: C

studying_1 5 days, 13 hours ago

Selected Answer: C

answer is correct, 10.2.2.0/29, 10.2.2.0 - 10.2.2.7, the current config is 10.2.2.10, which is out of range, and needs to be changed
upvoted 1 times

Question #1125

Topic 1

DRAG DROP

Drag and drop the characteristic from the left onto the cable type on the right.

uses multiple wavelengths of light	multimode fiber
has a core diameter of 9 microns	
has increased attenuation over long distances	
uses a single wavelength of light	single-mode fiber

Correct Answer:

uses multiple wavelengths of light	multimode fiber
has a core diameter of 9 microns	uses multiple wavelengths of light
has increased attenuation over long distances	has increased attenuation over long distances
uses a single wavelength of light	single-mode fiber

Question #1126

Topic 1

How does frame switching function on a switch?

- A. rewrites the source and destination MAC address
 - B. forwards frames to a neighbor port using CDP
 - C. forwards known destinations to the destination port
 - D. is disabled by default on all interfaces and VLANs

Correct Answer: C

Question #1127

DRAG DROP

Drag and drop the characteristic from the left onto the IPv6 address type on the right.

is assigned to multiple devices on the same network simultaneously

cannot be used as a source address

is routed to the nearest interface that has the address

provides one-to-many communications

Anycast

Multicast

Correct Answer:

is assigned to multiple devices on the same network simultaneously

cannot be used as a source address

is routed to the nearest interface that has the address

provides one-to-many communications

Anycast

is routed to the nearest interface that has the address

cannot be used as a source address

Multicast

is assigned to multiple devices on the same network simultaneously

provides one-to-many communications

 **studying_1** 5 days, 12 hours ago

given answer is not correct,

anycast : assigned to multiple devices, & routed to the nearest interface

multicast: cant be used as a source address and provides communication one to many

upvoted 3 times

Question #1128

Topic 1

What is a characteristic of an SSID in wireless networks?

- A. uses policies to prevent unauthorized users
- B. identifies an access point on a WLAN
- C. prompts a user for a login ID
- D. associates a name to a WLAN

Correct Answer: D

Question #1129

Topic 1

What is represented by the word "port" within this JSON schema?

```
1 [  
2 {"IDS": "IPS_pittsburgh", "port": "te8/30"},  
3 {"router": "R20", "port": "ge9/23"},  
4 {"firewall": "FW42", "port": "fe3/24"},  
5 ]
```

- A. value
- B. array
- C. key
- D. object

Correct Answer: C

Question #1130

Topic 1

DRAG DROP

Drag and drop the statements about AAA services from the left to the corresponding AAA services on the right. Not all options are used.

It grants access to network assets, such as FTP servers.

Accounting

It restricts the CLI commands that a user is able to perform.

Authorization

It performs user validation via TACACS+.

It records the duration of each connection.

It supports User Access Reporting.

It verifies "who you are".

Correct Answer:

It grants access to network assets, such as FTP servers.

Accounting

It restricts the CLI commands that a user is able to perform.

It records the duration of each connection.

It performs user validation via TACACS+.

It supports User Access Reporting.

It records the duration of each connection.

It grants access to network assets, such as FTP servers.

It supports User Access Reporting.

It restricts the CLI commands that a user is able to perform.

It verifies "who you are".

Question #1131

Topic 1

Which interface condition is occurring in this output?

```
R7# show interface fa0/0
FastEthernet0/0 is up, line protocol is up
Hardware is DEC21140, address is ca02.7788.0000 (bia ca02.7788.0000)
Description: admin_subnet
Internet address is 10.32.102.2/30
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (60 sec)
Half-duplex, 100 Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:01, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/300/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/300 (size/max)
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
7331 packets input, 7101162 bytes
Received 267 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
3927 packets output, 1440403 bytes, 0 underruns
0 output errors, 119 collisions, 0 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

- A. collisions
- B. broadcast storm
- C. duplex mismatch
- D. queueing

Correct Answer: C

 **studying_1** 5 days, 12 hours ago

Selected Answer: C

there are 119 collisions, caused by duplex mismatch, which can be seen on the half duplex side(if one side is configured half duplex and the other one full duplex)

upvoted 1 times

Question #1132

DRAG DROP

Drag and drop the IPv6 address from the left onto the type on the right.

fe80:cc72:4b9e:445c:8179:0420:5988:7

Global Unicast

2000:1092:a1e8:827d:527c:3ce7:9816:1

Link-Local Unicast

ff00:ec6c:dbb1:3e8b:6d46:bd27:a236:12

Multicast

fc00:9860:653f:5146:8cb2:a27c:cb6f:3

Unique Local

Correct Answer:

fe80:cc72:4b9e:445c:8179:0420:5988:7

2000:1092:a1e8:827d:527c:3ce7:9816:1

2000:1092:a1e8:827d:527c:3ce7:9816:1

fe80:cc72:4b9e:445c:8179:0420:5988:7

ff00:ec6c:dbb1:3e8b:6d46:bd27:a236:12

ff00:ec6c:dbb1:3e8b:6d46:bd27:a236:12

fc00:9860:653f:5146:8cb2:a27c:cb6f:3

fc00:9860:653f:5146:8cb2:a27c:cb6f:3

 **studying_1** 5 days, 12 hours ago

answer is correct, and LAST QUESTION YAASS, maybe there will be update lol
upvoted 2 times