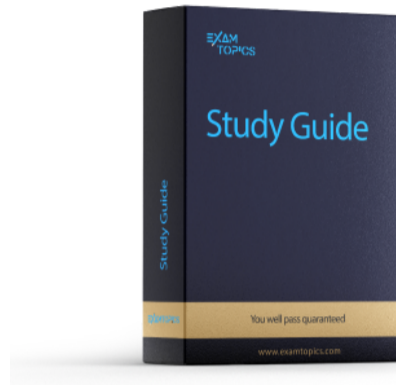


Prepare for your 200-301 exam with additional products



Study Guide

1969 PDF Pages

\$19.99

Buy Now

[Custom View Settings](#)

Question #1002

Topic 1

Which benefit does Cisco DNA Center provide over traditional campus management?

- A. Cisco DNA Center automates HTTPS for secure web access, and traditional campus management uses HTTP.
- B. Cisco DNA Center leverages SNMPv3 for encrypted management, and traditional campus management uses SNMPv2.
- C. Cisco DNA Center leverages APIs, and traditional campus management requires manual data gathering.
- D. Cisco DNA Center automates SSH access for encrypted entry, and SSH is absent from traditional campus management.

Correct Answer: C

Community vote distribution

C (100%)

[Removed] 2 months, 1 week ago

Selected Answer: C

C. Cisco DNA Center leverages APIs, and traditional campus management requires manual data gathering.
upvoted 1 times

Ciscoman021 5 months, 2 weeks ago

Selected Answer: C

Cisco DNA Center provides the benefit of leveraging APIs (Application Programming Interfaces) over traditional campus management which requires manual data gathering.
upvoted 3 times

Goena 7 months ago

Selected Answer: C

Ansewer C is correct
upvoted 4 times

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 (95%)

5%

 **sdmejia01** Highly Voted 6 months, 3 weeks ago

Selected Answer: B

I think the answer is B. The client pulls the configuration from the server. Check the Cheft section here:
<https://study-ccna.com/configuration-management-tools-ansible-chef-puppet/>
 upvoted 8 times

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

Selected Answer: B

The most accurate answer is B. Although D is also partially correct but the "word" push isn't generally a feature of Chef, instead Chef client, installed on a node, queries to the infra server for any configuration updates and if there's any update available, the client pulls it from the server. So option B is more appropriate here.
 upvoted 1 times

 **NetworkGeek00** 1 month, 1 week ago

Selected Answer: B

Answer is B,
 upvoted 1 times

 **binayD** 1 month, 1 week ago

Chef uses pull method to update configurations .That means the nodes will be pulling the config from the server (Chef has the capability to Push but it requires an external agent) I wondered for few seconds but since there is no mention of an external agent due to this I will conclude the default behaviour of the Chef config tool so the answer is B .
 upvoted 1 times

 **Bhrino** 3 months, 1 week ago

Selected Answer: B

chef is a pull
 upvoted 1 times

 **Bhrino** 3 months, 4 weeks ago

Selected Answer: B

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

 **Ciscoman021** 5 months, 3 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** 6 months, 1 week ago

know which one is correct, please?
 upvoted 1 times

🗨️ 👤 **Goena** 7 months ago

Selected Answer: B

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

🗨️ 👤 **Goena** 7 months 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** 5 months 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** 3 months, 4 weeks ago

Replaces is synonymous to update in the CRUD model

Create
Read
Update
Delete

it matches up
upvoted 3 times

🗨️ 👤 **mageknight** 6 months, 3 weeks ago

put=update in restfull operation
upvoted 2 times

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 6 months, 3 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 12 times

  **oatmealturkey** 6 months, 3 weeks ago

I agree

upvoted 5 times

  **Ciscoman021** Highly Voted 5 months, 2 weeks 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 8 times

  **JJY888** Most Recent 4 months 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 4 times

```

{
  "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 6 months, 3 weeks ago

array is right answer
upvoted 13 times

Rynurr Highly Voted 6 months, 3 weeks ago

Selected Answer: A

Definitely array, so "A" is the correct answer.
upvoted 9 times

COMPLUST Most Recent 6 days, 11 hours ago

?? it is not A?
upvoted 1 times

4aynick 3 months, 1 week ago

it is may be string inside array
upvoted 1 times

4aynick 3 months, 1 week ago

"" is string
[] - array
{ } - object
"key": "value" (variable type string)
upvoted 1 times

4aynick 3 months, 1 week ago

but question "In which structure" it is string in array structure
Correct is ARRAY 101%
upvoted 2 times

Vikramaditya_J 4 months, 1 week 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 3 times

DINVIS 6 months, 2 weeks ago

it's ARRAY

upvoted 2 times

  **gewe** 6 months, 4 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

Community vote distribution

D (100%)

  **Yannik123** 1 month, 2 weeks ago

Selected Answer: D

D is correct.
upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: D

D. facilitates communication between the controller and the networking hardware
upvoted 1 times

  **studying_1** 3 months, 2 weeks ago

answer is correct
upvoted 3 times

DRAG DROP

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

leverages Cisco Prime Infrastructure	Traditional Campus Device Management
reduces the workload for enterprise customers	
requires manual configuration of complex protocols	
lacks support for SDA	
uses algorithms to detect security threats	Cisco DNA Center
uses northbound APIs	

Correct Answer:

leverages Cisco Prime Infrastructure	Traditional Campus Device Management
reduces the workload for enterprise customers	leverages Cisco Prime Infrastructure
requires manual configuration of complex protocols	reduces the workload for enterprise customers
lacks support for SDA	requires manual configuration of complex protocols
uses algorithms to detect security threats	Cisco DNA Center
uses northbound APIs	lacks support for SDA
	uses algorithms to detect security threats
	uses northbound APIs

sdmejia01 Highly Voted 6 months, 3 weeks ago

I think reduce the workload for enterprise customers and Supports SDA should be switched. Correct me if I am wrong please.
upvoted 20 times

oatmealturkey 6 months, 3 weeks ago

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



lennylopes Most Recent 2 weeks ago

Traditional Campus Device Management:
- Leverages Cisco Prime Infrastructure
- Lacks support for SDA
- Requires manual configuration of complex protocols

Cisco DNA Center:

- Uses algorithms to detect security threats
- Uses Northbound APIs
- Reduces the workload for enterprise customers

upvoted 2 times

  **HM01** 3 months, 2 weeks 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** 6 months, 1 week ago

I think traditional:

- require.
- use
- lack

upvoted 3 times

  **ukguy** 6 months, 3 weeks ago

agreed

upvoted 1 times

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 (74%)

AD (26%)

  **oatmealturkey** Highly Voted 6 months, 3 weeks ago

Selected Answer: AC

NETCONF is a Southbound API used to configure network devices.

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

upvoted 8 times

  **Rynurr** Highly Voted 6 months, 3 weeks ago

Selected Answer: AC

Yeah, API and SOAP are correct answers.

upvoted 5 times

  **Yannik123** Most Recent 1 month, 1 week ago

Selected Answer: AD

NETCONF can be used as an Southbound AND Northbound API and SOAP is not an typically API for SDN

upvoted 1 times

  **poopie69** 1 month, 2 weeks ago

Selected Answer: AD

A. REST (Representational State Transfer):

REST is a widely used architectural style for creating web services, making it a popular choice for Northbound APIs in software-defined networks. It uses standard HTTP methods (GET, POST, PUT, DELETE) to communicate and transfer data between applications. REST APIs are known for their simplicity, scalability, and flexibility.

D. NETCONF (Network Configuration Protocol):

NETCONF is a network management protocol used for configuring and managing network devices in a software-defined network. It provides a programmatic interface for accessing and modifying device configurations, allowing centralized control and management of network devices. NETCONF uses XML-based messages over secure transport protocols for communication.

upvoted 2 times

  **HM01** 3 months, 2 weeks 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 2 times

  **hamish88** 4 months, 4 weeks ago

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

upvoted 1 times

  **liviuml** 5 months ago


Selected Answer: AC

SOAP is northbound

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

Regards

upvoted 1 times

 **Leethy** 5 months, 1 week 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 2 times

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  6 months, 3 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 14 times

  **lucantonelli93** Highly Voted  6 months, 3 weeks ago

Selected Answer: A

The correct answer it's A
upvoted 5 times

  **Bhrino** Most Recent  3 months, 4 weeks 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 2 times

  **mrmanistheman** 4 months ago

Selected Answer: A

Answer is A
upvoted 2 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: A

Looks like "A" is the correct answer
upvoted 5 times

  **mageknight** 6 months, 3 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** 6 months, 3 weeks ago

I think answer is D.
upvoted 1 times

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

Community vote distribution

C (100%)

 **Yannik123** 1 month, 2 weeks ago

Selected Answer: C

C is Correct

upvoted 1 times

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

Community vote distribution

A (94%)

6%

 **oatmealturkey** Highly Voted 7 months 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 8 times

 **raptuz** Most Recent 1 month ago

Selected Answer: B

The correct answer is B. when a nonidempotent operation is needed.

The PUT method in HTTP is used to update or create a resource on the server. It is typically used for idempotent operations, meaning that making the same request multiple times should have the same result as making it once. However, it's important to note that the PUT method is used for updating resources, not read-only operations or displaying web pages. Option A is incorrect because updating a DNS server typically involves administrative actions and may use different protocols. Option C is incorrect because displaying a web page is a read operation and would usually involve the GET method. Option D is incorrect because the PUT method is not used for read-only operations.

upvoted 1 times

 **Vikramaditya_J** 1 month, 1 week ago

Selected Answer: A

The PUT method in HTTP (Hypertext Transfer Protocol) is used to update a resource on the server. Non-idempotent methods are those that can have different outcomes when called multiple times with the same input parameters. Examples of non-idempotent methods include POST, PATCH, and non-idempotent PUT requests. Common non-idempotent methods: POST, PATCH, CONNECT. PUT isn't a non-idempotent methods.

upvoted 1 times

 **Ciscoman021** 5 months, 3 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 4 times

 **Rynurr** 6 months, 3 weeks 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 2 times

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

Community vote distribution

CD (100%)

 **sdmejia01** Highly Voted  6 months, 3 weeks ago

Selected Answer: CD

C and D are correct!

upvoted 5 times

 **DINVIS** Most Recent  6 months, 2 weeks ago

right answers

upvoted 4 times

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*

Community vote distribution

C (82%)

A (18%)

  **sdmejia01** Highly Voted 6 months, 3 weeks ago

I would go with C.
upvoted 12 times

  **Ciscoman021** Highly Voted 5 months, 3 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 7 times

  **kat1969** Most Recent 1 week, 3 days ago

In cloud computing, the control plane is the layer that handles tasks like creating and distributing routing policies. For instance, in Amazon Web Services (AWS), the control plane supplies administrative APIs for CRUD operations. A few examples of control plane tasks include creating S3 buckets and launching EC2 instances.
upvoted 1 times

  **Cynthia2023** 1 month, 1 week ago

Selected Answer: C

The advantage of separating the control plane from the data plane is that it reduces overall network complexity. This separation allows for centralized control and management of the network through a controller, making it easier to manage and configure the network. By centralizing control, administrators can make changes to network policies and configurations without needing to touch individual network devices. This simplifies network management and reduces the risk of misconfigurations and inconsistencies that can occur when managing individual devices separately.
upvoted 1 times

  **[Removed]** 2 months, 1 week ago


Selected Answer: C

C. decreases overall network complexity
upvoted 1 times

  **JJY888** 6 months, 1 week 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** 6 months, 1 week ago

C seems the most logical answers
upvoted 3 times

  **Dutch012** 6 months, 1 week ago

answer*
upvoted 1 times

  **mageknight** 6 months, 3 weeks ago

I would go with B
upvoted 4 times

  **ac891** 4 months, 1 week ago


keep thinking ...
upvoted 1 times


```
{
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

 **ac89l** Highly Voted 4 months ago
easiest question without having a knowledge
upvoted 6 times

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

Community vote distribution

D (100%)

 **Goena** Highly Voted 6 months, 2 weeks 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 6 times

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

Community vote distribution

B (54%)

D (46%)

 **NetworkGeek00** 1 month, 1 week ago

Selected Answer: B

Answer is B. use to define the target devices (ssh enabled) and it can write in .ini and .yaml formats.
upvoted 1 times

 **_mva** 1 month, 1 week ago

Inventory means devices. The inventory file is a listing of managed devices, so B is the answer.
upvoted 2 times

 **Yannik123** 1 month, 1 week ago

Selected Answer: D

The Inventory is an file where all managed Nodes are registered
upvoted 1 times


 **Yannik123** 1 month, 1 week ago

I hit the wrong selection box the correct answer is B!
upvoted 1 times

 **4Lucky711** 1 month, 2 weeks ago

Selected Answer: B

B is correct
<https://www.examttopics.com/discussions/cisco/view/80892-exam-200-301-topic-1-question-779-discussion/>
upvoted 1 times

 **Eallam** 2 months, 1 week ago

Selected Answer: D


check this question i779, this is the even the same words, so its D
upvoted 1 times

 **studying_1** 4 months, 1 week ago

B is correct
upvoted 2 times

 **beerbiceps1** 5 months, 1 week ago

B is correct
upvoted 2 times

 **zamkljo** 5 months, 2 weeks ago

Selected Answer: B

for sure B
upvoted 2 times


 **bisiyemo1** 6 months, 1 week ago

Selected Answer: D

D is correct
upvoted 1 times

 **bisiyemo1** 4 months, 3 weeks ago

Bis correct please
upvoted 2 times

 **ike110** 6 months, 2 weeks 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** 6 months, 2 weeks ago

D is correct
upvoted 2 times

  **sang33** 6 months, 3 weeks ago

Selected Answer: D

Ansible uses YAML
upvoted 3 times

  **ike110** 6 months, 2 weeks ago

D is the answer for Ansible playbook
upvoted 5 times

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 6 months, 2 weeks ago

Given answers are correct.

upvoted 9 times

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

Community vote distribution

D (100%)

  **sdmejia01** Highly Voted 6 months, 3 weeks ago

I would go with D.
upvoted 10 times

  **lucantonelli93** Highly Voted 6 months, 3 weeks ago

Selected Answer: D

For me it's D
upvoted 6 times

  **Bhrino** Most Recent 3 months, 4 weeks ago

Selected Answer: D

NBI allows communication between Controller and applications
SBI is the controller and data
upvoted 2 times

  **bisiyemo1** 4 months, 3 weeks ago

Selected Answer: D

D for sure
upvoted 3 times



  **beerbiceps1** 5 months, 1 week 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** 6 months, 3 weeks ago

Selected Answer: D

d dddd
upvoted 4 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: D

"D" for sure
upvoted 4 times

  **mageknight** 6 months, 3 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

```
{"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

Community vote distribution

D (68%)

A (24%)

8%

sdmejia01 Highly Voted 6 months, 3 weeks ago
apple represent a key which is not even in the answers.
upvoted 15 times

rogi2023 5 months, 2 weeks 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 2 times

rogi2023 5 months, 2 weeks ago
and "ripe" represents Boolean
upvoted 3 times

mhayek 6 months, 1 week ago
100% agree
upvoted 1 times

oatmealturkey Highly Voted 6 months, 3 weeks ago
Selected Answer: D
The answer is D. string:
<https://restfulapi.net/json-data-types/>
upvoted 7 times

Dunedrifter 2 months, 3 weeks ago
Nice. Thanks
upvoted 1 times

shaney67 Most Recent 2 weeks, 1 day ago
B. object

In the given JSON data, the key "apple" represents an object. An object in JSON consists of key-value pairs where the keys are strings and the values can be strings, numbers, booleans, arrays, or nested objects. In this case, the key "apple" is associated with an array containing the values "red" and 1, and the key "ripe" is associated with the boolean value "true."
upvoted 1 times

Yinx 3 weeks ago
Selected Answer: A
"apple" is the key of a object, but the value of "apple" is an array. So answer is A.
upvoted 1 times

raptuz 1 month ago
Selected Answer: A
"apple" is the key of an array, so A is the answer
upvoted 1 times

Stevens0103 1 month, 1 week ago
Selected Answer: B
An object in JSON consists of key-value pairs, where the keys are strings and the values can be various data types, including strings, numbers, arrays, and other objects.

The key "apple" is associated with the value ["red", 1], which is an array containing two elements: the string "red" and the number 1. The key "ripe" is associated with the value true, which is a boolean data type.



Since "apple" is a key within the JSON data structure and is associated with a value that includes multiple elements (an array), it represents an object.

upvoted 2 times

  **ananinamia** 2 weeks, 3 days ago

finally a dev

upvoted 1 times

  **Kerrera** 1 month, 3 weeks ago

Selected Answer: D

String inside an object, is a name/value - key concept

upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: D

Answer D

In JSON, the data known as an object is one or more key/value pairs enclosed in braces { }. The syntax for a JSON object includes:

Keys must be strings within double quotation marks " ".



Values must be a valid JSON data type (string, number, array, Boolean, null, or another object).

Keys and values are separated by a colon.

Multiple key/value pairs within an object are separated by commas.


Whitespace is not significant.

upvoted 1 times

  **Shabeth** 2 months, 2 weeks ago

D. String

upvoted 1 times

  **Bhrino** 3 months, 4 weeks ago

Selected Answer: D

anything thing in quotes are string which they could also be keys as well

upvoted 1 times

  **beerbiceps1** 5 months, 1 week ago

"" = string

upvoted 2 times

  **VictorCisco** 5 months, 2 weeks ago

Selected Answer: A

It represents an array

upvoted 1 times

  **bisiyemo1** 6 months, 1 week ago

Selected Answer: D

D is very correct

upvoted 1 times

  **bisiyemo1** 5 months, 1 week 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** 6 months, 1 week ago

Selected Answer: A

Apple represents an array value, not a string, focus guys


upvoted 3 times

  **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: D

It's D

upvoted 2 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: D

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

upvoted 4 times

  **gewe** 6 months, 4 weeks ago

why not string<?

upvoted 3 times

DRAG DROP

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

overlay and underlay configuration	Cisco DNA Center
routed access deployment	
STP deployment	
VLAN and HSRP configuration	Traditional
VXLAN and LISP configuration	
configuration via console	

Correct Answer:

overlay and underlay configuration	Cisco DNA Center
routed access deployment	
STP deployment	
VLAN and HSRP configuration	Traditional
VXLAN and LISP configuration	
configuration via console	

RidzV Highly Voted 6 months, 1 week ago

Correct answers
upvoted 6 times

Rydaz 4 months, 1 week 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 3 months, 2 weeks 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 2 times

  **ac89l** 4 months ago

But traditional does have console, no ?
upvoted 2 times

  **perri88** 3 months ago

yes of course
upvoted 2 times

  **Dunedrifter** Most Recent 2 months, 3 weeks ago

Correct!
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

Community vote distribution

AE (100%)



  **UAE7** Highly Voted 6 months, 2 weeks ago

answer is correct
upvoted 5 times

  **[Removed]** Most Recent 2 months, 2 weeks ago

Selected Answer: AE

A. PATCH
E. PUT
upvoted 1 times

  **Bhrino** 3 months, 4 weeks ago

Selected Answer: AE

Create. Post
Read Get
Update Put,patch
Delete Delete
upvoted 3 times

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

  **mageknight** Highly Voted 6 months, 3 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 16 times

  **JJY888** Highly Voted 6 months, 1 week ago

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

upvoted 12 times

  **LeonardoMcCabrio** 3 months, 1 week ago

Brother this question has a so stupid answer, no way to forget it! You got this!!

upvoted 1 times

  **studying_1** 3 months, 2 weeks ago

No, don't give up , you got this

upvoted 1 times

  **Tdawg1968** 3 months, 3 weeks 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 3 times

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.	Cisco DNA Center Device Management
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.	Traditional Device Management
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.	

Correct Answer:

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

RidzV Highly Voted 6 months, 1 week ago
I think Last answer for each section must be swapped.
Please correct me if I'm wrong.
upvoted 6 times

Secsoft 1 month, 2 weeks ago
The answers are correct. In traditional, there are a lot of configurations to be done manually which requires more number of tools and application whereas Cisco DNA provides a more unified and streamlined approach to network management and troubleshooting.
upvoted 4 times

fmaquino 5 months, 1 week ago
I agree. I would exchange the last of the Traditional with the first of DNA
upvoted 4 times

🗨️ 👤 **ac89l** 4 months, 1 week ago

But don't the DNA center use netflow ?
upvoted 4 times

🗨️ 👤 **Rydaz** 4 months, 1 week ago

they sure do, given answers are correct
upvoted 9 times

🗨️ 👤 **MoHTimo** Most Recent 1 month, 1 week ago

given answer is correct, netflow is for the southbound
upvoted 2 times

Question #1025

Topic 1

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

- A. control and monitoring of 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

Community vote distribution

B (100%)

🗨️ 👤 **Goena** 6 months, 2 weeks 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 2 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

Community vote distribution

D (100%)

🗨️ 👤 **krzysiew** 3 months, 3 weeks 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

```
{
  "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

- Danthemann** 1 month ago
more of an eye exam than anything
upvoted 2 times
- jini4200** 5 months, 2 weeks ago
hey guys, why it's not six??
upvoted 1 times
- beerbiceps1** 5 months, 1 week ago
[] are used to wrap up arrays. therefore, 3
upvoted 6 times

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 6 months, 1 week ago

The correct order is

- Agent
- push
- provision
- agentless
- post

upvoted 8 times

ac891 4 months ago

last one is pull
upvoted 1 times

bisiyemo1 4 months, 3 weeks ago

This seems to be correct
upvoted 1 times

Nwanna1 Most Recent 2 weeks ago

+ easy-to-manage deployment option that may lack scalability: agent + device hardware that runs without embedded management features:
agentless + to automatically install or deploy a configuration or update: pull + daemon that determines when the central authority has updates

available: provision + model in which the central server sends updates to nodes on an as-needed basis: push =====
New Questions (added on 31st-Dec-2022) =====

upvoted 1 times

  **Nwana1** 2 weeks ago

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

upvoted 1 times

  **Stevens0103** 1 month, 1 week ago

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

<https://gayatrisajith.medium.com/beginner-fundamentals-push-pull-configuration-management-tools-85eff1b41447>

upvoted 2 times

  **Stevens0103** 1 month, 1 week ago

<https://developer.cisco.com/docs/nx-os/#!agent-less-management>
<https://developer.cisco.com/docs/nx-os/#!agent-based-management>

upvoted 1 times

  **Stevens0103** 1 month, 1 week ago



https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/telemetry/70x/b-telemetry-cg-ncs5500-70x/b-telemetry-cg-ncs5500-70x_chapter_01.html

upvoted 1 times

  **JJY888** 4 months ago

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

upvoted 4 times

  **iMo7ed** 4 months, 2 weeks 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 3 times

  **jonathan126** 4 months, 3 weeks ago

daemon - Agent (e.g. puppet agent daemon)
central server - Push (e.g. ansible control node push configs to nodes)
easy-to-manage - Provision (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 3 times

  **Zortex** 5 months, 3 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

  **JJY888** 6 months, 1 week ago

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

upvoted 4 times


  **ike110** 6 months, 2 weeks ago

The following seems to be correct

agent
pull
push



agentless
provision

upvoted 2 times

  **Titan_intel** 6 months, 2 weeks ago

Can anyone confirm if this is correct?

upvoted 1 times

  **ike110** 6 months, 2 weeks ago

this is not correct

upvoted 4 times

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

Community vote distribution

B (58%)

A (42%)

 **JJY888** Highly Voted 6 months, 1 week 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 5 times

 **NetworkGeek00** Most Recent 1 month, 1 week ago

Selected Answer: B

API, answer is B
upvoted 1 times

 **paolino555** 1 month, 3 weeks ago

Selected Answer: B

Not "SDN" or "Controller" in question... so API
upvoted 2 times

 **paolino555** 1 month, 3 weeks ago


Selected Answer: B

correct!
upvoted 1 times

 **[Removed]** 2 months, 2 weeks ago

Selected Answer: A

A - Northbound interface
upvoted 2 times

 **Dunedrifter** 2 months, 3 weeks ago

Selected Answer: B

The correct answer is B. application programming interface (API).

An application programming interface (API) is a set of rules and protocols that allows different software applications to communicate and interact with each other. In the context of sending data over an IP network from a client to a server, an API provides the necessary methods and functions for the client application to establish a connection, format and send the data packets, and communicate with the server.

While northbound and southbound interfaces are also valid terms used in networking, they typically refer to the interfaces used in network management and communication between different layers of a network architecture. The Representational State Transfer (REST) API is a specific type of API that uses HTTP protocols and follows the principles of RESTful architecture for creating web services, but it is not the only type of API that enables data transfer over an IP network.

upvoted 3 times

 **Bingchengchen236** 2 months, 4 weeks ago

IT should be B, guys
upvoted 2 times

 **Friday_Night** 3 months, 2 weeks ago

why not D - REST API ?
upvoted 2 times

 **JJY888** 4 months ago

Selected Answer: B

B again.
upvoted 2 times



 **Dutch012** 6 months, 1 week ago

I believe B
upvoted 2 times

  **bisiyemo1** 6 months, 1 week ago

Selected Answer: A

A is the correct answer
upvoted 1 times

  **JJY888** 6 months, 1 week ago

Selected Answer: B

Correction.
upvoted 2 times

  **rmartin3444** 6 months, 1 week 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

Community vote distribution

A (100%)

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: A

A. policing
upvoted 1 times

  **studying_1** 3 months, 2 weeks ago

Selected Answer: A

Answer is correct
upvoted 2 times

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

Community vote distribution

A (100%)

 **Goena** Highly Voted 6 months, 2 weeks 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 5 times

 **[Removed]** Most Recent 2 months, 1 week ago

Selected Answer: A

A. It queues excess traffic

upvoted 1 times

 **JJY888** 4 months 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 2 times

 **shiv3003** 4 months, 3 weeks ago

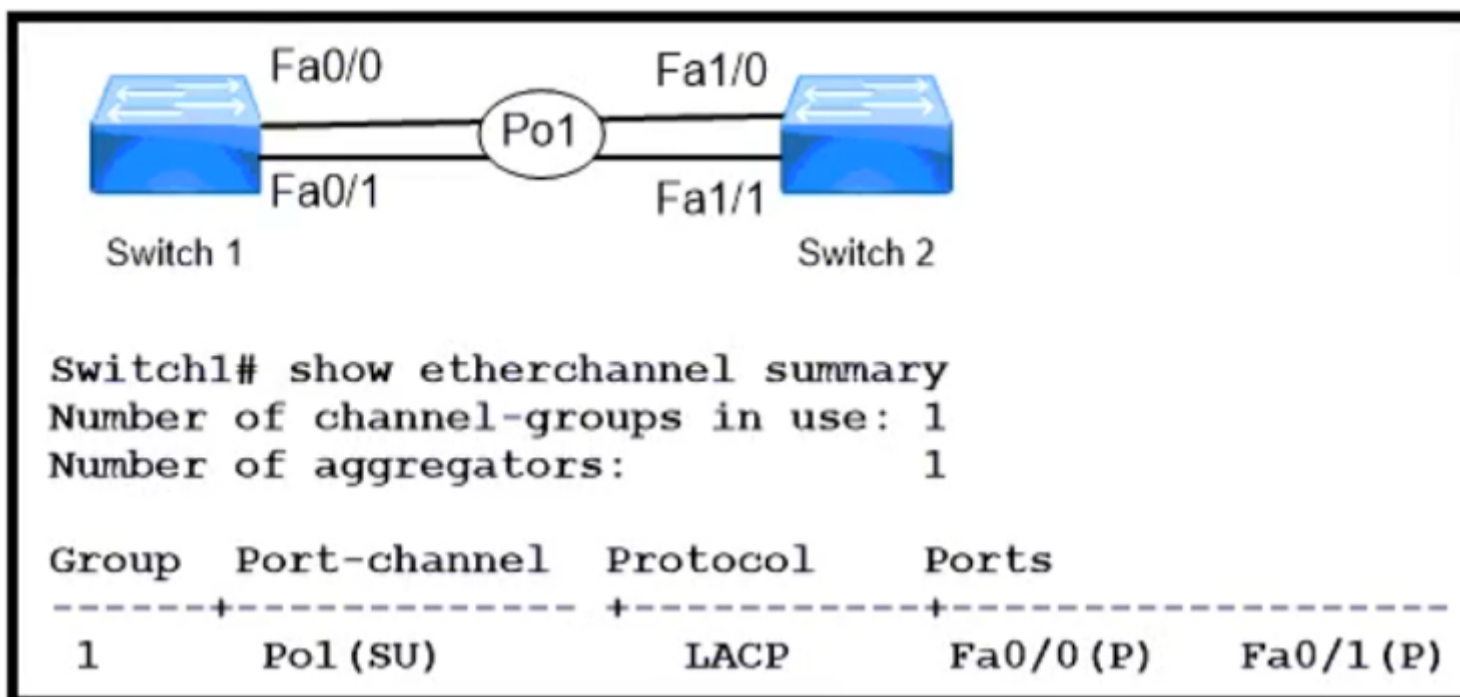
C is the answer

upvoted 1 times

 **ac89l** 4 months, 1 week ago

Thats QoS

upvoted 2 times



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

Community vote distribution

B (100%)

ike110 Highly Voted 6 months, 2 weeks 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 9 times

Vikramaditya_J Most Recent 1 month, 1 week ago

Selected Answer: B

The command "port-channel min-links 1" sets the minimum number of operational links required for the port-channel interface to be considered up. In this case, it sets the minimum number of operational links to 1, which means that if at least one physical link in the port-channel is up and functioning, the port-channel interface will also be up. If all the physical links in the port-channel go down, the port-channel interface will go down as well.

The port-channel min-links command is particularly useful for ensuring that the EtherChannel remains operational even if some of its member links fail. Setting the minimum number of links to 1 helps maintain connectivity in scenarios where not all physical links are available due to hardware issues, cable problems, or other temporary failures.

upvoted 1 times

perri88 3 months ago

does anyone know why?

upvoted 1 times



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

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

Correct Answer: AD

Community vote distribution

AD (100%)

  **no_blink404** 2 months, 2 weeks ago

Selected Answer: AD

A&D

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-6/configuration-guide/b_cg76/b_cg76_chapter_011110.pdf

upvoted 2 times

  **Goena** 6 months, 2 weeks ago

Selected Answer: AD

Correct

upvoted 4 times


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

Community vote distribution

B (100%)

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: B

B. to shield internal network devices from external access

upvoted 1 times

  **studying_1** 3 months, 2 weeks ago

correct

upvoted 2 times

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

Community vote distribution

C (100%)

  **shaney67** 1 week, 5 days ago

```
SW1(config)# interface range Ethernet0/0 - 1
SW1(config-if-range)# channel-group 44 mode active
SW1(config-if-range)# exit
```

```
SW2(config)# interface range Ethernet0/0 - 1
SW2(config-if-range)# channel-group 44 mode active
SW2(config-if-range)# exit
```

```
SW1(config)# interface Port-Channel44
SW1(config-if)# switchport mode trunk
SW1(config-if)# exit
```


```
SW2(config)# interface Port-Channel44
SW2(config-if)# switchport mode trunk
SW2(config-if)# exit
```

```
SW1(config)# interface Port-Channel44
SW1(config-if)# switchport trunk encapsulation dot1q
SW1(config-if)# exit
```

```
SW2(config)# interface Port-Channel44
SW2(config-if)# switchport trunk encapsulation dot1q
SW2(config-if)# exit
```

```
SW1(config)# interface Port-Channel44
SW1(config-if)# switchport trunk native vlan MONITORING
SW1(config-if)# exit
```

```
SW2(config)# interface Port-Channel44
SW2(config-if)# switchport trunk native vlan MONITORING
SW2(config-if)# exit
upvoted 1 times
```

  **[Removed]** 2 months, 1 week ago


Selected Answer: C

C.
switchport mode trunk
switchport trunk encapsulation dot1q <--using an industry-standard trunking protocol
switchport trunk allowed vlans 1-10 <-- permitting VLANs 1-10 and denying other VLANs
upvoted 2 times

 **molly_zheng** 4 months ago

Selected Answer: C

correct
upvoted 4 times

 **RidzV** 6 months, 1 week ago

Correct answer
upvoted 3 times


```

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

Community vote distribution

C (83%)

D (17%)

 **RidzV** Highly Voted 6 months, 1 week ago

Duplex incompatibility can cause high number of collisions
upvoted 9 times

 **JJY888** Highly Voted 4 months ago

Selected Answer: C

According to OCG and Boson practice exams, collisions are duplex incompatibility.
upvoted 6 times

 **Cynthia2023** Most Recent 1 month, 2 weeks ago

Selected Answer: C

output shows that there are 8662416065 collisions on the interface, which could be a likely reason for slow transfer speeds.

Answer: (C). a duplex incompatibility

"txload 1/255" means that the transmitted traffic load is 1/255th of the total bandwidth capacity.

"rxload 1/255" means that the received traffic load is 1/255th of the total bandwidth capacity.

"txload" and "rxload," a value of 1/255 indicates that there is very low traffic congestion.

upvoted 3 times

 **[Removed]** 2 months, 2 weeks ago

Selected Answer: C

C. duplex incompatibility

upvoted 1 times

  **Simon_1103** 4 months, 3 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

  **ac89l** 4 months ago

heavy traffic is shown by tx rx load

upvoted 5 times

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

Community vote distribution

AD (97%)

 **ahmt** Highly Voted 7 months ago

Selected Answer: AD

Address ranges to be use 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 17 times

 **rAlexandre** Highly Voted 7 months ago

Selected Answer: AD

Class B IP addresses. Configurations range from 172.16.0.0 to 172.31.255.255

upvoted 7 times

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

Selected Answer: AD

The two host addresses reserved for private use within an enterprise network are:

A. 10.172.76.200

D. 172.31.255.100

In IPv4 addressing, private IP address ranges are reserved for use within private networks. These addresses are not routable on the public internet. The private IP address ranges are as follows:

10.0.0.0 to 10.255.255.255 (10.0.0.0/8) - Addresses starting with 10.x.x are part of the private IP address range.

172.16.0.0 to 172.31.255.255 (172.16.0.0/12) - Addresses starting with 172.16.x.x to 172.31.x.x are part of the private IP address range.

192.168.0.0 to 192.168.255.255 (192.168.0.0/16) - Addresses starting with 192.168.x.x are part of the private IP address range.

From the given options, addresses A (10.172.76.200) and D (172.31.255.100) fall within the private IP address ranges mentioned above and are reserved for private use within an enterprise network.

upvoted 1 times

 **LeonardoMeCabrio** 3 months, 1 week ago

Selected Answer: AD

AD is the correct!


upvoted 1 times

 **Bhrino** 3 months, 4 weeks ago

Selected Answer: AC

just have to memorize private ipv4 ranges here

upvoted 1 times

 **Bhrino** 3 months, 4 weeks ago

i meant A and d!

upvoted 1 times

 **bisiyemo1** 6 months, 1 week ago

Selected Answer: AD

AD is the correct answer

upvoted 2 times

 **tal10** 6 months, 2 weeks ago

Selected Answer: AD

definitiv



upvoted 1 times

  **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: AD

The correct answers it's AD

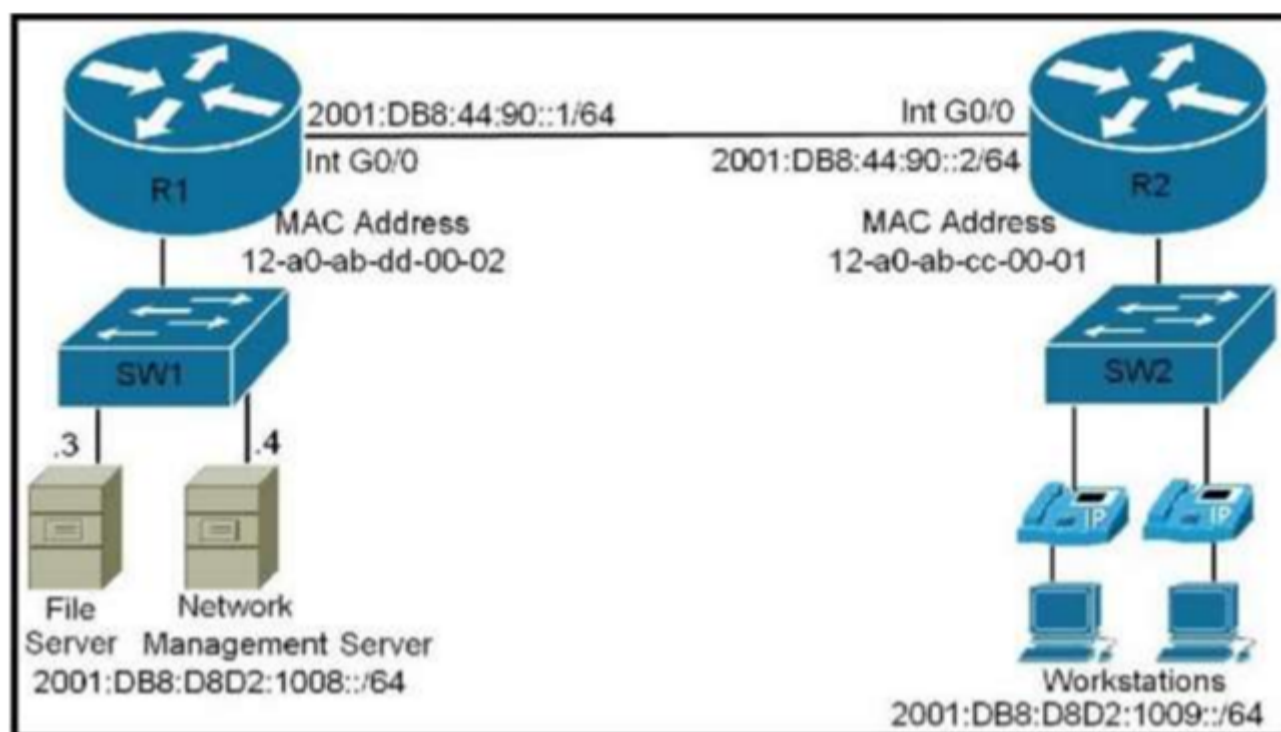
upvoted 1 times

  **Rynurr** 6 months, 3 weeks 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

Community vote distribution

A (100%)

no_blink404 2 months, 2 weeks ago

Selected Answer: A

Answer A is deffo correct

upvoted 2 times

audid 6 months, 3 weeks ago

Can someone explain please

upvoted 1 times

UAE7 6 months, 2 weeks 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 7 times

Stichy007 6 months, 3 weeks 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

ananiamia 2 weeks, 3 days ago

your 12 is 18 so your mind is correct but your math is weak!

upvoted 1 times

ananiamia 2 weeks, 3 days ago

I mean math is wrong

upvoted 1 times

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*

Community vote distribution

BD (53%)

BC (47%)

 **liviuml** Highly Voted 5 months 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 6 times

 **Yinx** Most Recent 3 weeks ago

Selected Answer: BD

The port onder PortFast is participating in STP.

upvoted 1 times

 **rijosh** 1 month ago

Selected Answer: BC

Answer is B and C

upvoted 1 times


 **ac89l** 4 months 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 3 times

 **Leethy** 5 months, 1 week 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 3 times

 **bisiyemo1** 6 months, 1 week 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 4 times

 **bisiyemo1** 6 months, 1 week ago

<https://networklessons.com/switching/cisco-portfast-configuration#:~:text=Portfast%20does%20two%20things%20for%20us%3A&text=Interfaces%20with%20portfast%20enabled%20that,the%20li>


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

upvoted 1 times

 **learntstuff** 1 month, 3 weeks ago

I thought BC at first then I found above link and I was wrong. It's BD.

upvoted 1 times

 **RidzV** 6 months, 1 week ago

Selected Answer: BC

Faster convergence can be achieved by skipping STP operations state.

upvoted 3 times

 **Dutch012** 6 months, 1 week ago

I believe B & C are correct

upvoted 3 times

SIMULATION

-

Guidelines

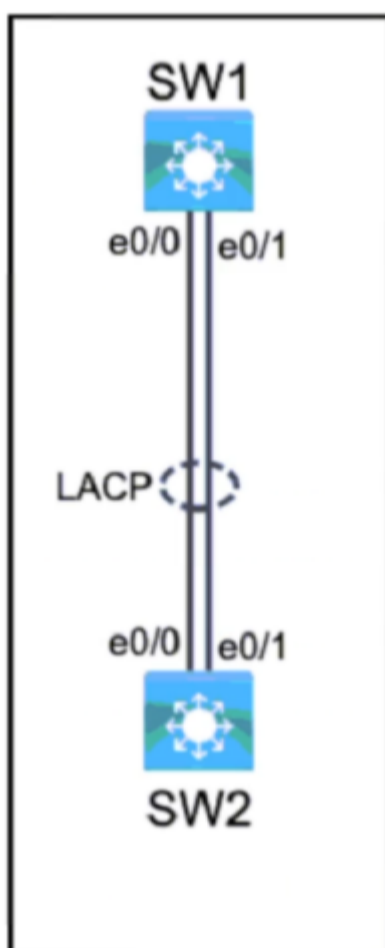
-

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 Ethernet0/0 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 shut
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 shut
SW2(config-if)# end
```

This assumes that VLAN 746 is the MONITORING VLAN.

  **Wes_60** Highly Voted 5 months, 2 weeks 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 5 times

  **ac891** 4 months, 1 week 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

  **[Removed]** 2 months, 2 weeks ago

Shutdown while configuring etherchannel is a best practice though

upvoted 2 times

  **Rydaz** 4 months, 1 week ago

no shutdown is only for routers not switches

upvoted 1 times

  **andrizo** 2 weeks, 4 days ago

we use it when resetting ports on switches.

upvoted 1 times

  **4Lucky711** Most Recent 1 month, 3 weeks ago

I'm a beginner, but I might do this....

```
<SW1>
```

```
en
```

```
conf t
```

```
int range e0/0-1
```

```
shutdown
```

```
channel-group 44 mode active
```

```
int port-channel 44
```

```
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
```

```
no shutdown
```

```
end
```

```
copy running-config startup-config
```

```
-----
```

```
<SW2>
```

```
en
```

```
conf t
```

```
int range e0/0-1
```

```
shutdown
```

```
channel-group 44 mode active
```

```
switchport trunk native vlan MONITORING
```

```
no shutdown
```

end
copy running-config startup-config
upvoted 1 times

🗨️ 👤 **4Lucky711** 1 month, 2 weeks ago

Sorry, "switchport trunk native vlan MONITORING" is a wrong command.
This vlan MONITORING must have an ID needed to create it.
upvoted 1 times

🗨️ 👤 **Brocolee** 1 month, 3 weeks ago

If S1 is 'Active', then S2 must be 'Passive' right? no?
upvoted 1 times

🗨️ 👤 **Shri_Fcb10** 1 month, 3 weeks ago

The question is asking to keep LACP mode same on both side, hence you have to keep it active on both side. There won't be an issue with running LACP active/active, As a matter of fact, when you connect Nexus 2ks to 5ks or 7ks active/active should be configured.
upvoted 1 times

🗨️ 👤 **LeonardoMcCabrio** 3 months ago

```
S1
interface range eth0/0-1
shut
channel-group 44 mode active
no shut

interface port-channel 44
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk native vlan 746
```

```
S2
interface range eth0/0-1
shut
channel-group 44 mode active
no shut
```

```
interface port-channel 44
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk native vlan 746
upvoted 3 times
```

🗨️ 👤 **Titan_intel** 6 months, 2 weeks ago

Not sure about this one. Does anyone have any insight?
upvoted 1 times

🗨️ 👤 **yuz1227** 6 months, 1 week ago

this seems legit.. although.. 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 2 times

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

Community vote distribution

B (100%)

  **UAE7** Highly Voted 6 months, 2 weeks ago

since question asks to filter messages based on importance, I think severity level is the answer
upvoted 5 times

  **[Removed]** Most Recent 2 months, 1 week ago

Selected Answer: B

"based on their importance"
B. level
upvoted 2 times

  **krzysiew** 4 months, 1 week 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 3 times

  **mageknight** 6 months, 3 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 3 times

SIMULATION

-

Guidelines

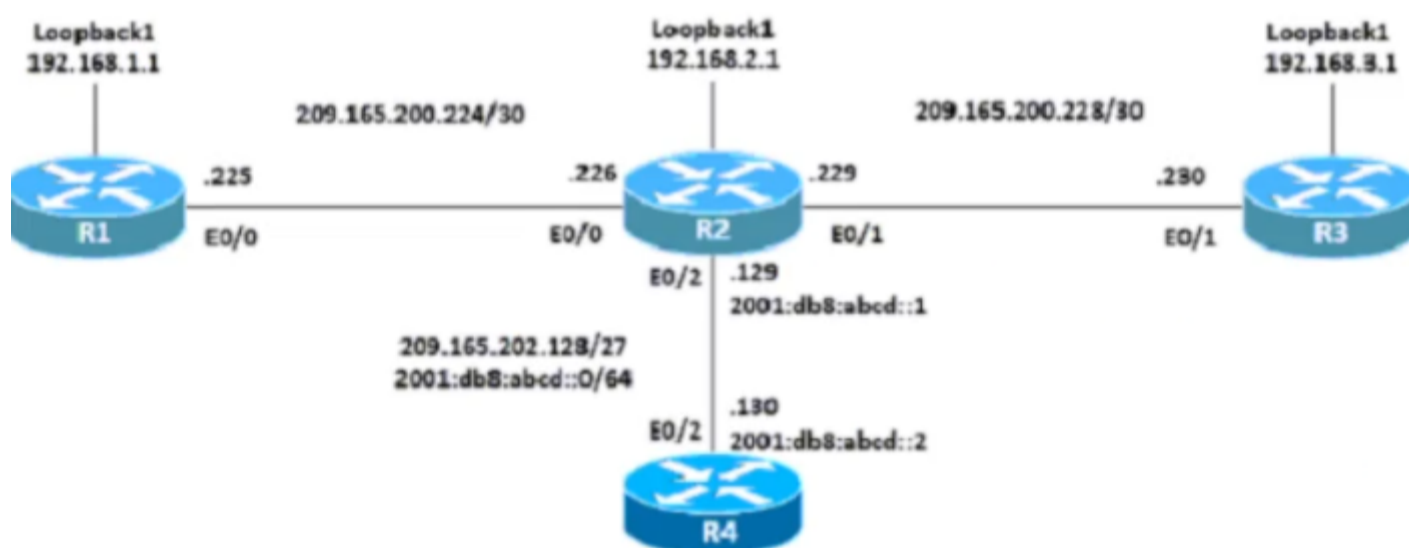
-

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 5 months, 3 weeks ago

solution provided is not complete; R1 needs a route back to R3, otherwise connectivity is not established!
upvoted 5 times

 **VicM** 3 months, 4 weeks 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

 **[Removed]** 2 months, 2 weeks ago

Do you mean only from router R3 to the router R1 and nothing from R1 to R3?
upvoted 1 times

 **ac89l** 4 months 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 4 times

 **rogi2023** 4 months, 4 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** 3 months, 2 weeks ago

only need one back, it's for the interface, not the loopback, one is enougha
upvoted 1 times

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


"using the source IP of 209.165.200.230"

```
---
R3(config)# ip route 192.168.1.1 e0/1
R3(config)# exit
R3# wr
---
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.202.130
R2(config)# ipv6 route ::/0 2001:db8:abcd::2
R2(config)# exit
R2# wr
```

upvoted 1 times

 **dropspablo** 2 weeks, 5 days ago


correcting (lacked MASK)
R3(config)# ip route 192.168.1.1 255.255.255.255 e0/1
Asked to use source interface e0/1
upvoted 1 times

 **Toto86** 2 months, 1 week ago

```
R3
ip route 192.168.1.1 255.255.255.255 e0/1
```

```
R2
ip route 0.0.0.0 0.0.0.0 209.165.202.130
ipv6 route ::/0 2001:db8:abcd::2
```

upvoted 1 times

 **sany11** 4 months, 3 weeks 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 2 times

  **Shri_Fcb10** 1 month, 3 weeks ago

the question says to use source IP address 209.165.200.230

upvoted 1 times

  **ac89l** 4 months ago

should there be a reverse route also ?

upvoted 1 times

  **itemba36** 4 months, 3 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 4 times

  **Secsoft** 2 weeks, 2 days ago

It has been clearly mentioned, you must use the source ip of 209.165.200.230. Do you guys have any idea about it?

upvoted 1 times

  **jhmint** 2 weeks, 5 days ago

I agree the only thing I will change is the last line. 209.165.200.230 should be 209.165.200.228. This way you are referencing the network rather than the port ID on RT3



I was able to ping RT3 to RT1 using the below:

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 209.165.200.228 255.255.255.255 209.165.200.226

upvoted 1 times

  **Rydaz** 4 months, 1 week 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 4 times

  **VarDav** 3 weeks, 4 days ago

I think that's a bad idea. You'll need another route on R2 so that it knows where the loopback of R3 is located. Why make it more difficult than it needs to be.

upvoted 1 times


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

Community vote distribution

B (100%)

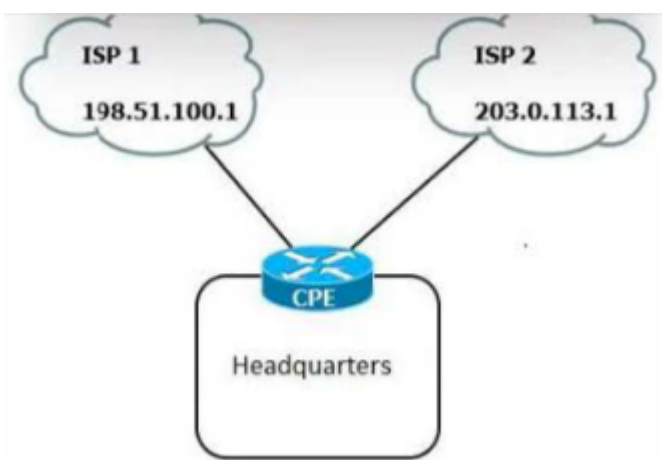
 **Goena** 6 months, 2 weeks ago

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 4 times



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

Community vote distribution

B (100%)

sdmejia01 Highly Voted 6 months, 3 weeks ago

I think it shouldn't be 2 answers. Answer C would work as intended in the question.
upvoted 11 times

xbololi Highly Voted 2 months ago

Helpful reminder, if you didn't understand what the heck is this;
Answer B is equal to C+D soooo
Just memorize this and you will answer this sh!t question at exam without any problem. You welcome.
upvoted 6 times

Stevens0103 Most Recent 1 month, 1 week ago

Selected Answer: B

The goal is to load-balance traffic between the two ISPs while ensuring redundancy. To achieve this, we need to divide the entire IP address space into two halves and send each half to a different ISP. This is typically done using a technique called "BGP Dual-Homed" setup, where the company headquarters announces two routes: one for the first half of the IP address space (0.0.0.0/1) to ISP1, and the other for the second half (128.0.0.0/1) to ISP2.

Option B: Two default routes are configured for each ISP. The first half of the IP address space (0.0.0.0/1) goes to ISP1, and the second half (128.0.0.0/1) goes to ISP2.

upvoted 2 times

Stevens0103 1 month, 1 week ago

Selected Answer: D

Option D: This option also divides the IP address space between the two ISPs using the /1 subnet mask.

Both of these options provide load-balancing and redundancy, ensuring that traffic is distributed across both ISPs.

upvoted 1 times

- 🗨️ 👤 **shaney67** 1 month, 2 weeks ago
C and E
upvoted 1 times
- 🗨️ 👤 **Shabeth** 2 months, 3 weeks ago
ill go with B and C
upvoted 1 times
- 🗨️ 👤 **Shabeth** 2 months, 3 weeks ago
cannot be A- AD of 255 is considered unreachable
upvoted 1 times
- 🗨️ 👤 **Rydaz** 4 months, 1 week ago
C and D
upvoted 1 times
- 🗨️ 👤 **goldenoliver** 4 months, 3 weeks ago
B and C right
upvoted 1 times
- 🗨️ 👤 **bisiyemo1** 6 months, 1 week ago
A may be the second choice but C is sure
upvoted 1 times
- 🗨️ 👤 **tippy1000** 6 months, 3 weeks ago
The 255 at the end of a is suspect
upvoted 1 times
- 🗨️ 👤 **mageknight** 6 months, 3 weeks ago
may be A and C i think
upvoted 2 times
- 🗨️ 👤 **RaselAhmedIT** 6 months, 4 weeks ago
What about the other one?
upvoted 2 times
- 🗨️ 👤 **oatmealturkey** 7 months ago
But you have to choose two :(
upvoted 3 times

```

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

Community vote distribution

C (90%)

10%

 **rAlexandre** Highly Voted 7 months ago

Selected Answer: C

C is the right awnser in order to change to LACP for multi vendor compatibility
upvoted 14 times

 **j1mlawton** Highly Voted 7 months ago

Selected Answer: C

C is correct LACP must be used
upvoted 8 times

 **rubzal** 3 months, 2 weeks ago

PAGP mentioned in the exhibit
upvoted 3 times

 **[Removed]** 2 months, 2 weeks ago

It must be changed to LACP
upvoted 2 times

 **Techpro30** Most Recent 2 weeks, 6 days ago

This is why I got out of cisco administration. After 25 years they could never have 1 standard...

There are three options for configuring an EtherChannel:

PAGP: A Cisco proprietary protocol

LACP: An IEEE standard

Manual: Bundle multiple physical interfaces without any protocol

PAGP has two modes:

Auto mode: The interface can respond to PAGP packet negotiation but will never start one on its own.

Desirable mode: The interface actively attempts a negotiating state for PAGP packet negotiation.

LACP has two modes:

Active: The interface actively sends LACP packets in its attempt to form an LACP connection.

Passive: The interface can respond to LACP negotiation but will never initiate on its own.

upvoted 1 times

 **Shabeth** 2 months, 3 weeks ago



Selected Answer: C

C is correct

upvoted 1 times

 **shiv3003** 4 months, 3 weeks ago

i go for A
upvoted 1 times

  **Leethy** 5 months, 1 week 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 3 times

  **Vikramaditya_J** 1 month, 1 week ago



When using the "mode on" configuration, the EtherChannel will be created "only" when another interface group is in EtherChannel "on" mode. However, one major drawback of using manually configured "On" EtherChannel Mode is that any layer one device like media converter or modem between two Etherchannel devices will not be able to diagnose link failure and keep on sending the traffic while PAgP/LACP configured devices will detect the failure and respond to it. The question also doesn't speak anything about such requirements. CCNA isn't an expert level exam and it doesn't ask such complicated questions. Answer is only B.

upvoted 1 times

  **ac89l** 4 months, 1 week 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 2 times

  **Leethy** 5 months, 1 week 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** 6 months, 2 weeks ago

Why not B?
mode on
upvoted 4 times



  **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: C

The correct answer it's C
upvoted 2 times

  **lucantonelli93** 6 months, 3 weeks ago

The correct answer it's C
upvoted 2 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: C

"C" for sure
upvoted 2 times

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

- A. multiple VMs operate on the same underlying hardware
- B. Each VMs 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

Community vote distribution

AE (100%)

  **Yannik123** 1 month ago



Selected Answer: AE

Answer is correct
upvoted 2 times

  **[Removed]** 2 months, 1 week ago

Selected Answer: AE

A. multiple VMs operate on the same underlying hardware
E. Each VM runs independently of any other VM in the same hypervisor
upvoted 1 times

  **RidzV** 6 months, 1 week ago

Correct answer
upvoted 3 times

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 6 months, 3 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 12 times

 **shaney67** Most Recent 2 weeks ago

D. source-destination MAC address

Explanation: For Cisco Wireless LAN Controllers (WLCs), the recommended switch load-balancing mode is typically the "source-destination MAC address" mode. This mode considers both the source MAC address (the client device) and the destination MAC address (the access point) to make load-balancing decisions. This helps distribute client traffic across access points while maintaining session continuity for individual client devices.

upvoted 1 times

 **dropspablo** 1 month, 4 weeks ago

Answer correct : https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-6/b_Cisco_Wireless_LAN_Controller_Configuration_Best_Practices.html#:~:text=%E2%80%9Csource%2Ddestination%20IP%E2%80%9D%20as%20the%20typically%20recommended%20option

upvoted 1 times

What must be considered when using 802.11a?

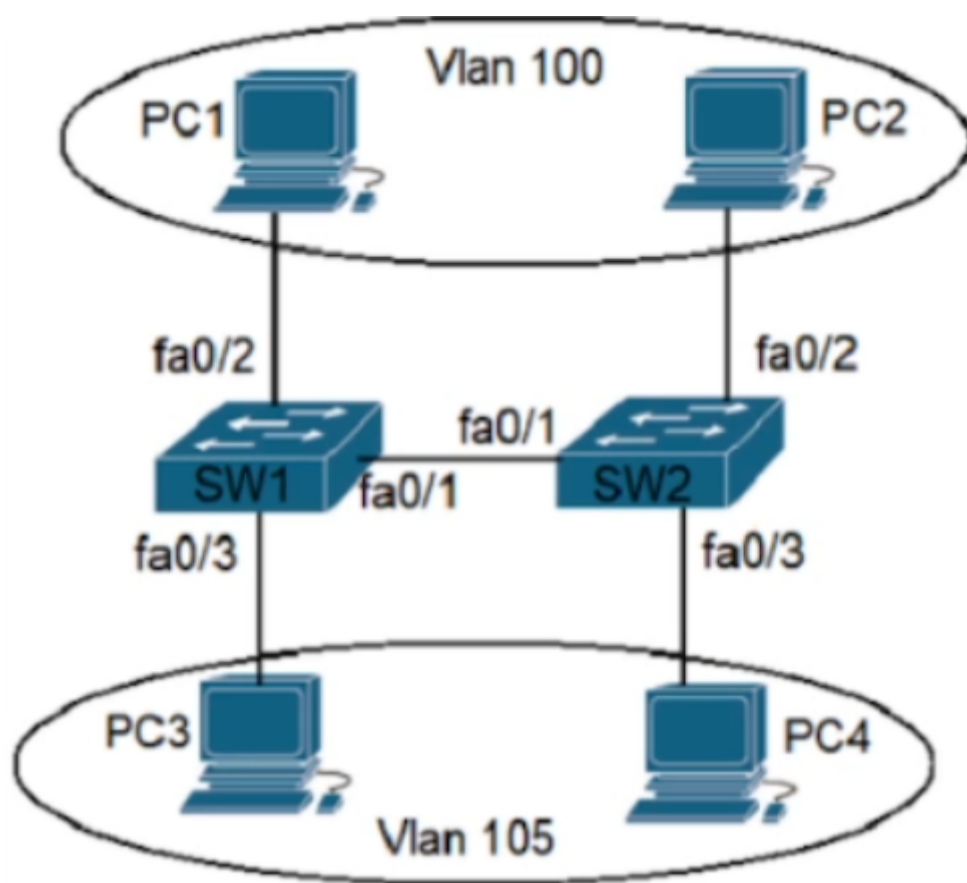
- A. It is chosen over 802.11b when a lower-cost solution is necessary
- B. It is susceptible to interference from 2.4 GHz devices such as microwave ovens
- C. It is compatible with 802.11b- and 802.11g-compliant wireless devices
- D. It is used in place of 802.11b/g when many nonoverlapping channels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

Correct Answer: D

 **ike110** Highly Voted 6 months, 2 weeks ago

802.11.a is a 5GHz standard

upvoted 6 times



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

ccnk 2 months, 3 weeks ago

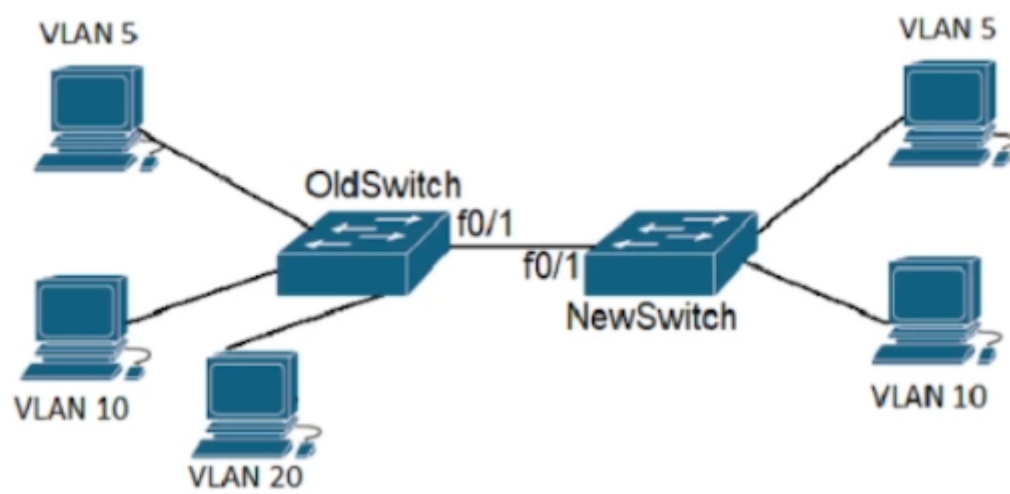
A is correct
upvoted 1 times

ac89l 4 months ago

IMO this is correct
upvoted 3 times

studying_1 3 months, 2 weeks 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 2 times



```
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

Community vote distribution

D (100%)

Friday_Night 3 months, 2 weeks 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 4 times

[Removed] 2 months, 2 weeks ago

The engineer must be bored lol

upvoted 1 times

  **Trains** 2 months, 4 weeks ago

I don't like the wording either, but after it lists the requirements, it asks us for the commands to configure the new switch
upvoted 1 times

  **krzysiew** 5 months, 1 week ago

Selected Answer: D

answer is correct
upvoted 3 times

  **UAE7** 6 months, 2 weeks ago

answer is correct
upvoted 4 times

SIMULATION

-

Guidelines

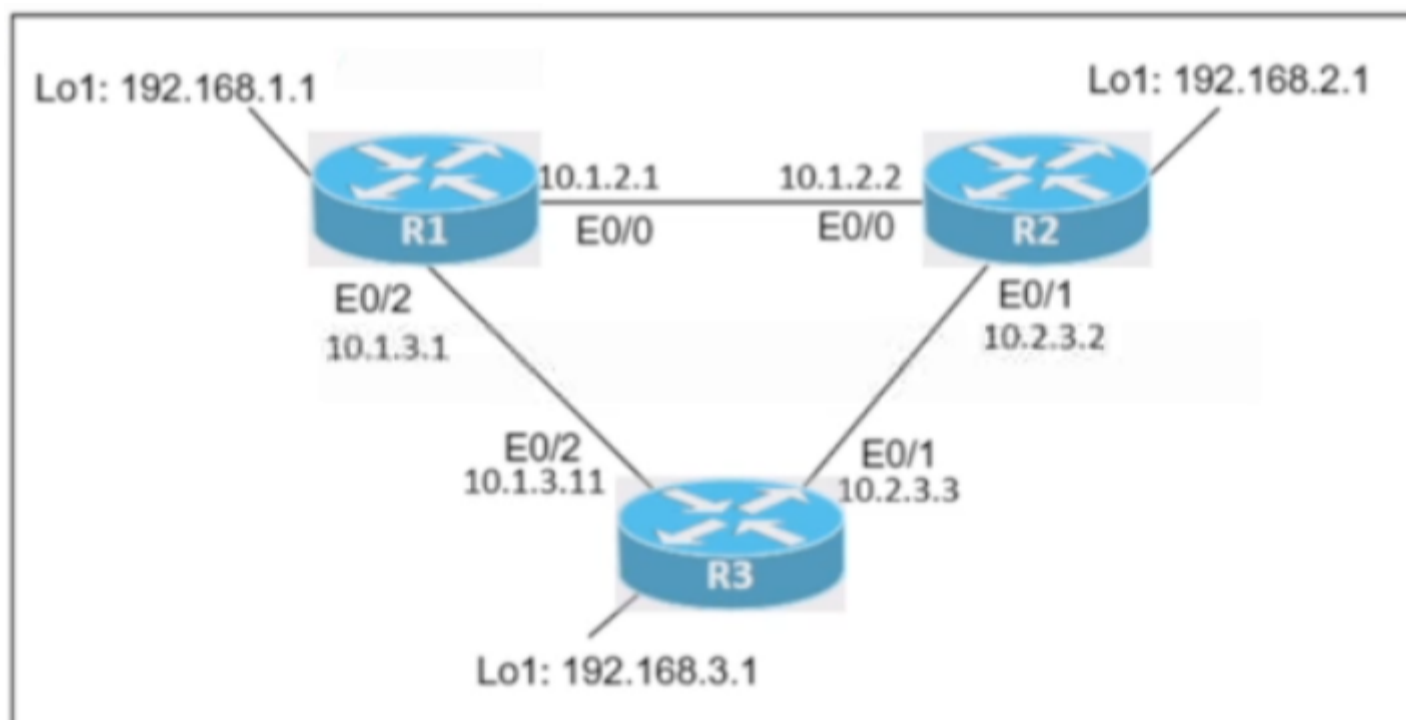
-

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 N3t4ccess 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 6 months 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 14 times

 **Shabeth** 2 months, 3 weeks ago

overload is for PAT, but the task said NAT, i am confused

upvoted 1 times

 **Shri_Fcb10** 1 month, 3 weeks ago


yes because the question is asking to translate all source IP add from R3 to the IP add of e0/0 of R2. So we are mapping multiple source addresses to a single IP address hence PAT is required

upvoted 3 times

 **Friday_Night** 3 months, 2 weeks ago

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

upvoted 3 times

 **rogi2023** 5 months, 2 weeks ago

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

upvoted 7 times

 **Secsoft** Most Recent 2 weeks, 3 days ago

In NAT, To verify, a ping must be successful to the R1 Loopback address sourced from R3. How can we achieve this by NAT configuration?

upvoted 1 times

 **dropspablo** 1 month ago

```
1- NAT
R2(config)# ip access-list standard PUBNET
R2(config-std-nacl)# permit 192.168.3.1 0.0.0.0
R2(config-std-nacl)# permit host 10.2.3.3
R2(config-std-nacl)# permit 10.1.3.11
(you can use both ways)
R2(config-std-nacl)# exit
R2(config)# ip nat inside source PUBNET interface ethernet0/0 overload
R2(config)#int e0/1
R2(config-if)#ip nat inside
R2(config-if)#interface e0/0
R2(config-if)#ip nat outside
#end
R3# ping 192.168.1.1 (to R1 Loopback1)
R2# show ip nat translations
2- NTP
R1(config)# ntp master
R1(config)# clock set 00:00:00 mai 1 2018
R1# do show clock
-
R2(config)# ntp server 10.1.3.1
R2# do show ntp associations
```

upvoted 1 times

 **dropspablo** 1 month ago

```
3- DHCP
R1(config)# ip dhcp pool NETPOOL
R1(dhcp-config)# network 10.1.3.0 255.255.255.0
R1(dhcp-config)# exit
R1(config)# ip dhcp excluded-address 10.1.3.1 10.1.3.10
R1# do show ip dhcp pool
-
R3(config)# interface ethernet0/2
R3(config-if)# ip address dhcp
R3# do show ip interface brief
4- SSH
R3(config)# username netadmin password N3t4ccess
R3(config)# ip domain-name cisco.com
R3(config)# crypto key generate rsa |1024|
R3(config)# access-list 10 permit 10.1.3.1
R3(config)# line vty 0 15
R3(config-line)# login local
R3(config-line)# transport input ssh
R3(config-line)# access-class 10 in
R3(config-line)# end
R1# ssh -l netadmin 10.1.3.11
```

upvoted 1 times

 **dropspablo** 1 month ago

Attention (* Do not change the enable password or hostname for any device.)

upvoted 1 times

 **dropspablo** 1 month ago

Correcting, access list in the vty lines (there are three):

```
R3(config)#access-list 10 permit 10.1.3.1
R3(config)#access-list 10 permit 192.168.1.1
R3(config)#access-list 10 permit 10.1.2.1
```

upvoted 1 times

 **dropspablo** 1 month ago

Attention - (1. All traffic sent from R3 to the R1 Loopback address must be configured for NAT on R2.) Check with "#show ip route", if the route from R3 to R1 Loopback goes through R2. If not, we must configure a static route on R3: R3(config)# ip route 192.168.1.1 255.255.255.255 10.2.3.2

upvoted 2 times

 **Toto86** 2 months, 1 week ago

Implementing DHCP like task 3 is not a part of CCNA 200-301. It was part of CCNA ICND1 100-105. CCNA 200-301 Official Cert Guide, Volume 2 Appendix D page 6

upvoted 1 times

 **[Removed]** 2 months, 2 weeks ago

I'm confused about the NAT part, i don't understand what they want exactly but here's my answer for the rest of the configuration :

NTP :

R1 :

enable

clock set 00:00:00 1 may 2018

configure terminal

ntp master 1

end

copy running-config startup-config

R2 :

enable

configure terminal

ntp server 10.1.3.1

end

copy running-config startup-config

DHCP :

R1 :

enable

configure terminal

ip dhcp excluded-address 10.1.3.1 10.1.3.10

ip dhcp pool NETPOOL

network 10.1.3.0 255.255.255.0

end

copy running-config startup-config

R3 :

enable

configure terminal

interface e0/2

ip address dhcp

end

copy running-config startup-config

SSH :

R3 :

enable

configure terminal

username netadmin secret N3t4ccess

ip domain-name ccna-lab.com

crypto key generate rsa general-keys modulus 1024

line vty 0 15

login local

transport input ssh

end

upvoted 3 times

  **Goena** 6 months ago

Is it nat to the loopback that is asked?

And how do you configure to a loopback?

upvoted 1 times

  **Goena** 6 months ago

The configuration of NAT is missing.

upvoted 1 times

```
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	Et0/0 (P) Et0/1 (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

Community vote distribution

A (100%)

 **sdmejia01** Highly Voted 6 months, 3 weeks ago

The configuration shows is a layer 3 port channel, hence you need to use the command no switchport.
upvoted 9 times

 **gewe** Highly Voted 6 months, 4 weeks ago

its layer 3
upvoted 5 times

 **Bhrino** Most Recent 3 months, 4 weeks 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 2 times

 **j1mlawton** 7 months ago

Why not C?
upvoted 1 times

 **oatmealturkey** 6 months, 4 weeks ago

(RU) means Layer 3 & in use, so need to make it a layer 3 interface which is done with "no switchport"
upvoted 7 times

SIMULATION

-

Guidelines

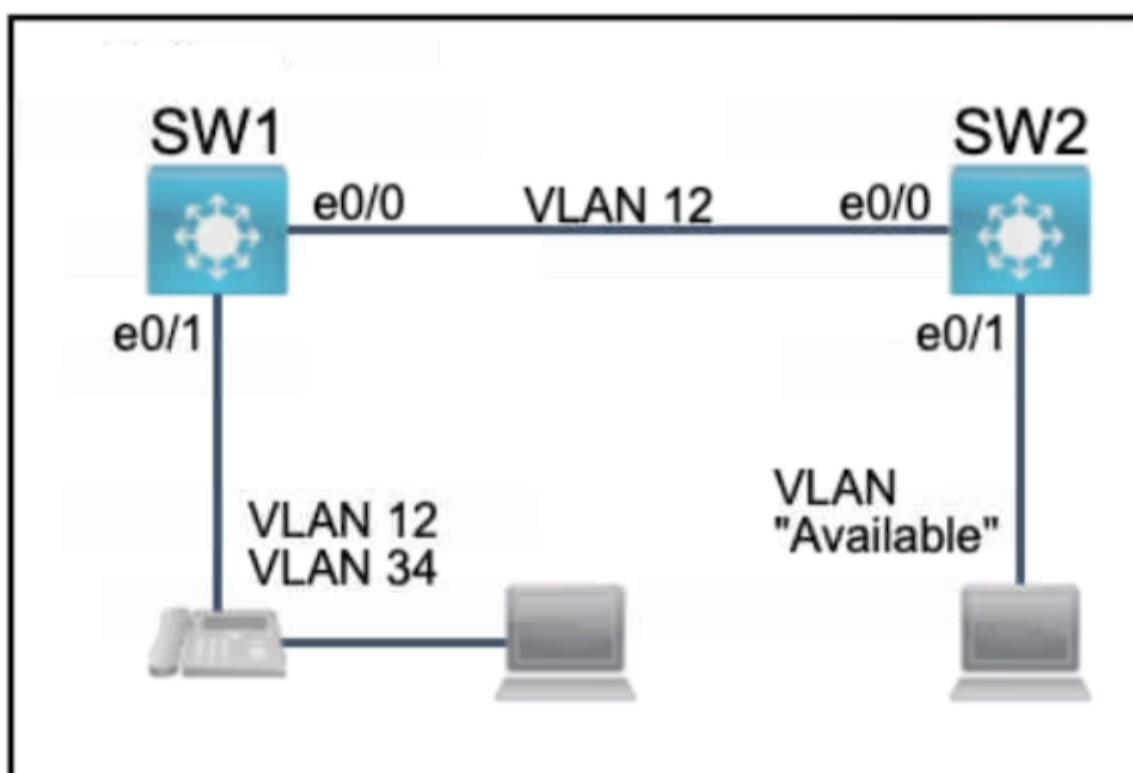
-

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
```

  **rogi2023** Highly Voted 4 months, 4 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 8 times
```

  **itemba36** 4 months, 3 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 14 times

  **Mariachi** Highly Voted 5 months, 3 weeks 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

  **Cynthia2023** Most Recent 1 month, 2 weeks ago

SW1 Configuration

```
enable
conf t
```

```
vlan 12
name Computer

vlan 34
name Telephony

int e0/1
switchport mode access
switchport access vlan 12
switchport voice vlan 34
no shutdown

int e0/0
switchport mode access
switchport access vlan 12
no shutdown

end
wr
```

```
# SW2 Configuration
enable
conf t
```

```
vlan 12
name Computer
```

```
vlan 34
name Telephony
```

```
int e0/1
switchport mode access
switchport access vlan Available
no cdp enable
no shutdown
```

```
int e0/0
switchport mode access
switchport access vlan 12
no shutdown
```

```
end
wr
```

upvoted 1 times

  **4Lucky711** 1 month, 3 weeks ago

I'm a beginner and I'm not sure the answer....

```
SW1:
en
conf t
vlan 12
name Compute
```

```
vlan 34
name Telephony
```

```
int e0/0
switchport mode access
switchport access vlan 12
```

```
int e0/1
switchport mode access
switchport access vlan 12
switchport voice vlan 34
end
copy running-config startup-config
-----
```

```
SW2:
en
conf t
int e0/1
switchport mode access
switchport access vlan Available
no cdp enable
end
copy running-config startup-config
```

upvoted 1 times

  **no_blink404** 2 months ago

No expert, but this is what I got:

```
SW1)
vlan 12
name Compute
vlan 34
name Telephony
```

```
int e0/0
switchport mode access
switchport access vlan 12
```

```
int e0/1
switchport mode access
switchport access vlan 12
switchport voice vlan 34
copy run start
```

```
SW2)
int e0/1
switchport mode access
switchport access vlan Available
no cdp enable
copy run start
upvoted 1 times
```

  **studying_1** 3 months, 2 weeks 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 3 times
```

  **Keba889** 4 months, 2 weeks ago

Correct, itemba36...Thanks!
upvoted 3 times

```

%AMDP2_FE-5-COLL: AMDP2/FE 0/0/[DEC], Excessive collisions, TDR=[DEC], TRC=[DEC]
%DEC21140-5-COLL: [chars] excessive collisions
%IIACC-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

Community vote distribution

A (89%)


11%

 **zamkljo** 5 months, 2 weeks 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 4 times

 **Rynurr** 6 months, 3 weeks 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** 7 months 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** 7 months ago

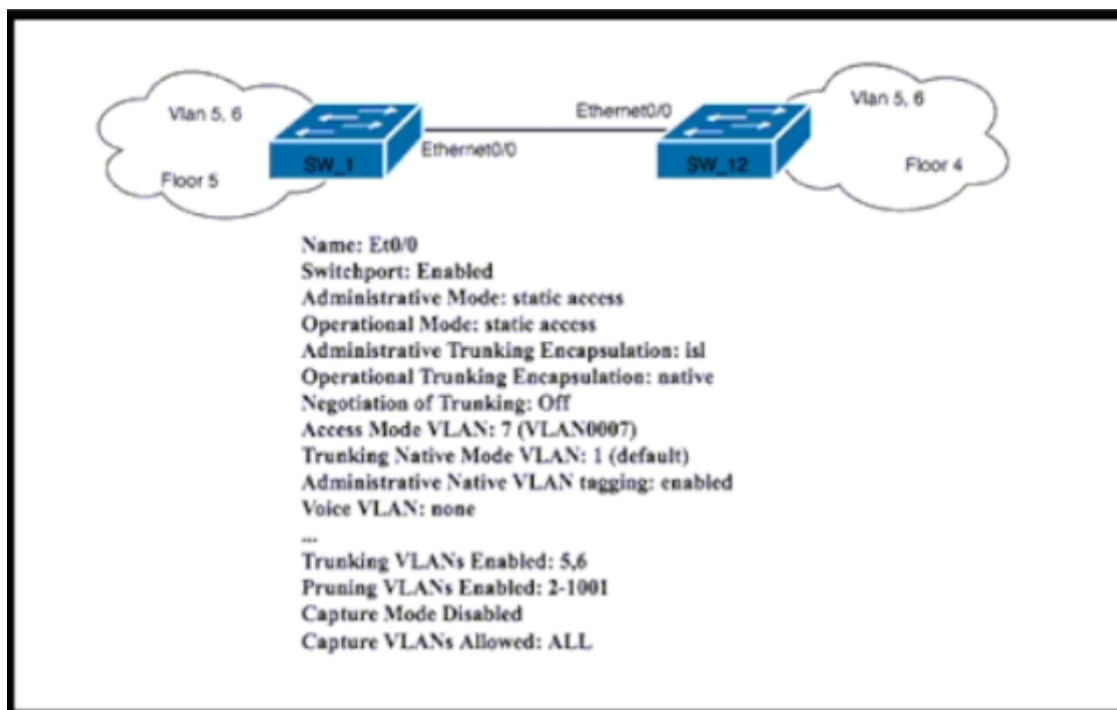
I see here that the maximum number of retries in the backoff algorithm is set to 16, so A may be the right answer <https://www.cisco.com/c/en/us/support/docs/interfaces-modules/port-adapters/12768-eth-collisions.html>

upvoted 3 times

 **oatmealturkey** 7 months ago

A is definitely correct, my bad

upvoted 6 times



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

Community vote distribution

A (100%)

rAlexandre Highly Voted 7 months ago

Selected Answer: A

I think the purpose is to change the encapsulation to dot1q because isl is a Cisco proprietary protocol
upvoted 13 times

oatmealturkey 6 months, 4 weeks ago

Correct and dynamic desirable mode is only for DTP which is also Cisco proprietary
upvoted 6 times

bisiyemo1 Highly Voted 6 months, 1 week ago

Selected Answer: A

A is sure
upvoted 5 times

Cynthia2023 Most Recent 1 month ago

Selected Answer: A

The command "switchport dot1q ethertype 0800" is not required in this context and doesn't play a role in joining VLANs between two switches. The "switchport dot1q ethertype" command is used to specify a particular EtherType to be used for tagging VLANs. The default EtherType for 802.1Q tagging is 0x8100, which is used to indicate that the frame carries VLAN information. The value 0800 corresponds to the EtherType for IPv4.
upvoted 1 times

Rynurr 6 months, 3 weeks ago

Selected Answer: A

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

upvoted 5 times

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

Community vote distribution

A (100%)

 **Leethy** Highly Voted 5 months, 1 week 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 9 times

 **Dutch012** Highly Voted 6 months, 1 week ago

final question yay!

upvoted 9 times

 **perri88** 3 months ago

1138 questions as of today

upvoted 3 times

 **ac89l** 4 months ago

not for us ... :)


upvoted 6 times

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

Selected Answer: A

C. Error, only MAC address specified without VLAN or port security enabled

upvoted 1 times

 **Eallam** 2 months, 1 week ago

Selected Answer: A

A is correct the command is

switchport port-security [mac-address mac-address [vlan {vlan-id | {access | voice}}]]

Example:

Switch(config-if)# switchport port-security mac-address 00:A0:C7:12:C9:25 vlan 3 voice

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_011111.html#ID437

and since in the question it stated vlan 4 and you can have multiple Voice Vlans , A is more accurate than B

upvoted 1 times

 **nostal** 2 months, 2 weeks ago

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-3/configuration_guide/sec/b_173_sec_9300_cg/port_security.html

switchport port-security mac-address sticky [mac-address | vlan {vlan-id | {access | voice}}]



Example:

Device(config-if)# switchport port-security mac-address sticky 00:A0:C7:12:C9:25 vlan voice

upvoted 1 times



 **nostal** 2 months, 2 weeks ago

B is correct, tested with a lab. C is for data vlan,
upvoted 1 times



  **ac89l** 4 months, 1 week 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 months, 1 week 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 2 times

  **Rydaz** 4 months, 1 week ago

my bad, C is right
upvoted 2 times

SIMULATION

-

Guidelines

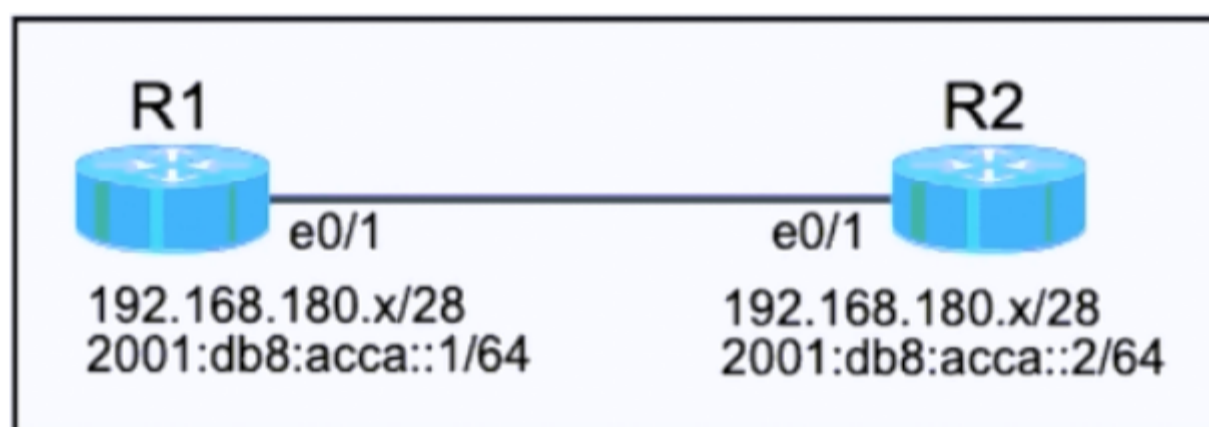
-

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 R2
R1#
```

```
R1 R2
R2#
```

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

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
```

rogi2023 Highly Voted 5 months 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 19 times

dozer86 4 months, 4 weeks ago

correct net 192.168.180.0/28 is unavailable.

upvoted 5 times

ac89l Highly Voted 4 months, 1 week 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 7 times
```

  **VicM** 4 months 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** 3 months, 2 weeks ago

no its /28 you're mistaken, from 16-31, it's 30
upvoted 6 times

  **raptuz** Most Recent 4 weeks ago

why enable ipv6 unicast-routing? is not required to enable ipv6 routing in the question
upvoted 1 times

  **Paul1111** 2 weeks, 1 day ago

It is required to enable ipv6 globally on a device
upvoted 1 times

  **VicM** 4 months, 2 weeks 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** 3 months, 2 weeks ago

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

  **RashidOzil** 4 months, 1 week 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 months, 1 week ago

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

SIMULATION

-

Guidelines

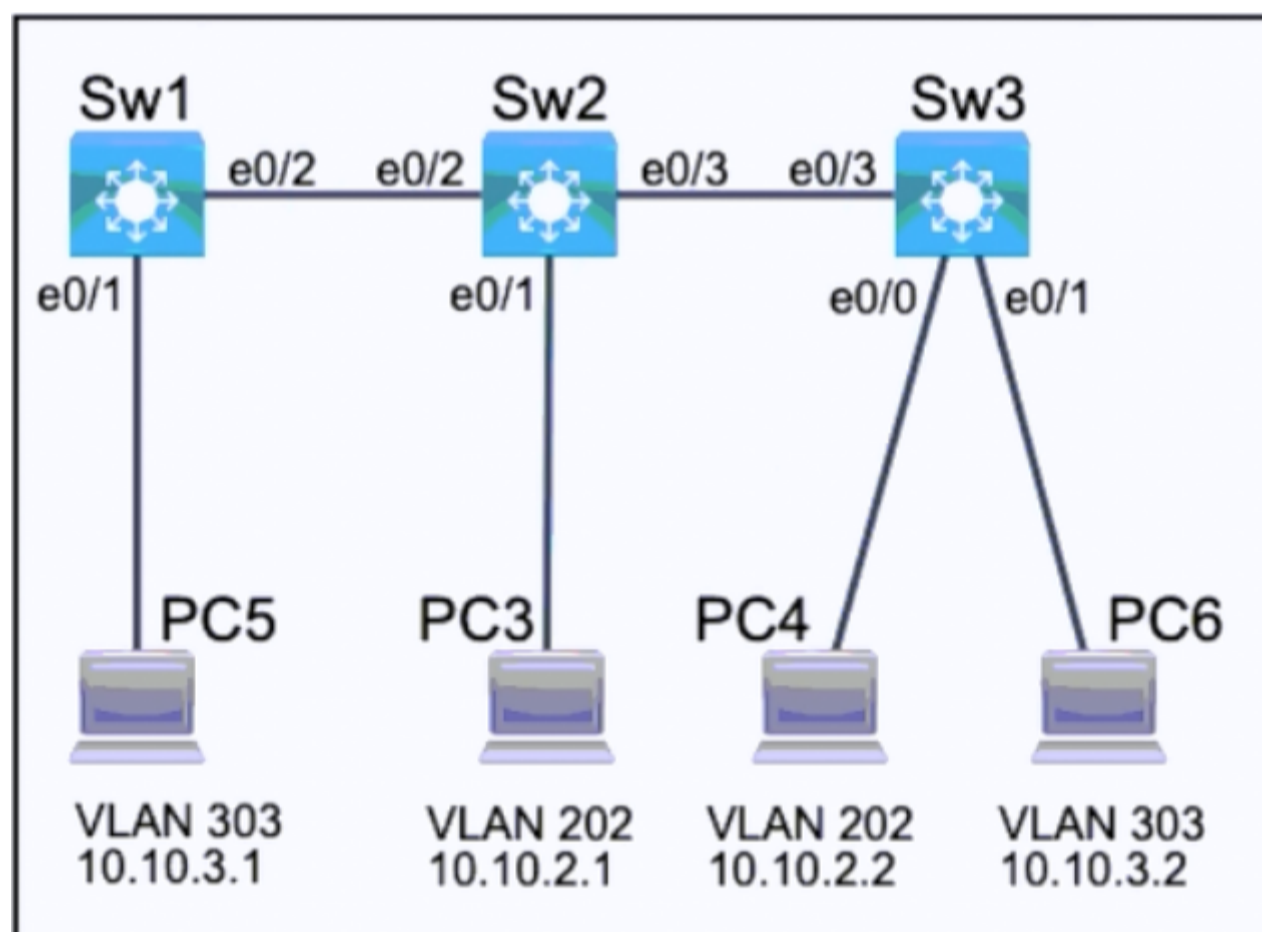
-

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>
```

```
SW1 SW2 SW3
SW2>
```

```
SW1 SW2 SW3
SW3>
```

```
Sw1

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

```
Sw2

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

Correct Answer:

```
Sw3

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
```

  **itemba36** Highly Voted 4 months, 3 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 5 times

  **[Removed]** Most Recent 2 months, 2 weeks ago

Here's my answer :

SW1

```
enable
configure terminal
```

```
vlan 303
name FINANCE
```

```
interface e0/1
switchport mode access
switchport access vlan 303
```

```
interface e0/2
switchport mode trunk
switchport trunk allowed vlan 303
```

```
end
copy running-config startup-config
```

SW2

```
enable
configure terminal
```

```
vlan 202
```

```
name MARKETING
vlan 303
name FINANCE
```

```
interface e0/1
switchport mode access
switchport access vlan 202
```

```
interface e0/2
switchport mode trunk
switchport trunk allowed vlan 303
```

```
interface e0/3
switchport mode trunk
switchport trunk allowed vlan 202,303
```

```
end
copy running-config startup-config
```

SW3

```
enable
configure terminal
```

```
vlan 202
name MARKETING
vlan 303
name FINANCE
```

```
interface e0/0
switchport mode access
switchport access vlan 202
```

```
interface e0/1
switchport mode access
switchport access vlan 303
```

```
interface e0/3
switchport mode trunk
switchport trunk allowed vlan 202,203
```

```
end
copy running-config startup-config
upvoted 3 times
```

 **Dunedrifter** 2 months, 3 weeks ago

**I tested this in cisco Packet tracer

SW1: create only vlan 303
create access port in vlan 303
only allow vlan 303 in the trunk towards SW2

SW2: create both 202 and 303 vlans
only allow vlan 303 in the trunk towards SW1
allow both vlans in the trunk towards SW3
Create access port in vlan 202

SW3: create both 202 and 303 vlans
allow both 202 and 303 vlans in the trunk towards SW2
assign access ports to their respective vlans.

Done! You have achieved layer 2 connectivity!!
upvoted 4 times

 **Shabeth** 2 months, 3 weeks ago

I am not sure about my answer, can someone pls check
SW1;

```
en
conf t
vlan 303
name Finance
```

```
int e0/1
switchport mode access
switchport access vlan 303
```

```
int e0/2
switchport mode trunk
switchport trunk allowed vlan 202,303
```

```
SW2:
en
conf t
vlan 202
name marketing

int e0/1
switchport mode access
switchport access vlan 202

int e0/2
switchport mode trunk
switchport trunk allowed vlan 203, 303
```

```
SW3:
en
conf t
vlan 303
name FINANCE
vlan 202
name MARKETING
```

```
int e0/0
switchport mode access
switchport access vlan 202
```

```
int e0/3
switchport mode trunk
switchport trunk allowed vlan 202, 203
```

```
int e0/1
switchport mode access
switchport access vlan 303
```

```
int e0/3
switchport mode trunk
switchport trunk allowed vlan 202,303
upvoted 1 times
```

  **no_blink404** 3 months ago

I am no expert but this is what I got:

```
SW1):
```

```
vlan 303
name FINANCE
vlan 202
name MARKETING
```

```
int e0/1
switchport mode access
switchport access vlan 303
```

```
int e0/2
switchport mode trunk
switchport encapsulation dot1q
switchport trunk allowed vlan 303, 202
```

```
SW2):
```

```
vlan 303
name FINANCE
vlan 202
name MARKETING
```

```
int e0/1
switchport mode access
switchport access vlan 202
```

```
int e0/2
switchport mode trunk
switchport encapsulation dot1q
switchport trunk allowed vlan 303, 202
```

```
int e0/3
switchport mode trunk
switchport encapsulation dot1q
switchport access vlan 303, 202
```

SW3):

```
vlan 303
name FINANCE
vlan 202
name MARKETING
```

```
int e0/0
switchport mode access
switchport access vlan 202
```

```
int e0/1
switchport mode access
switchport access vlan 303
```

```
int e0/3
switchport mode trunk
switchport encapsulation dot1q
switchport trunk allowed vlan 303, 202
upvoted 3 times
```

  **Secsoft** 1 month, 3 weeks ago

What does this command mean? (switchport access vlan 303, 202) in interface e0/3 of SW2.
upvoted 1 times

  **KraZd** 4 months ago

ANSWER IS INCORRECT
upvoted 2 times

  **KraZd** 4 months 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** 4 months 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 2 times

  **KraZd** 4 months ago

SW2:
Since VLANS 110 & 210 will need to traverse the linke 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 2 times

  **KraZd** 4 months ago

SW3:
Switch 3 has hosts in both VLANS so both VLANS will need to be configured on it.
upvoted 1 times

  **KraZd** 4 months 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** 4 months 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** 4 months 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** 4 months 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

  **rogi2023** 5 months ago

I think on all trunk interfaces should be allowed vlans 202, 303
upvoted 3 times

  **jonathan126** 4 months, 3 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 3 times

SIMULATION

-

Guidelines

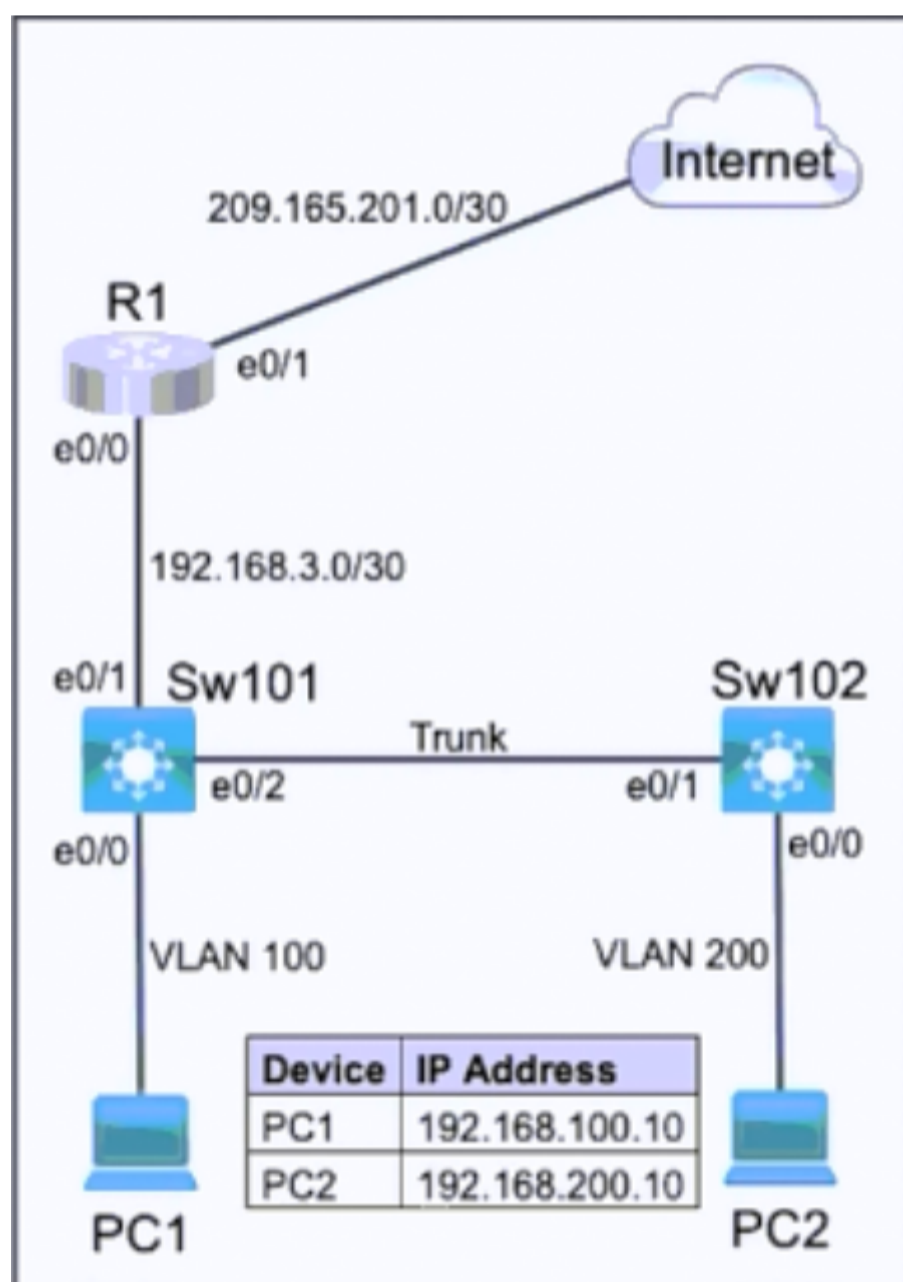
-

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:

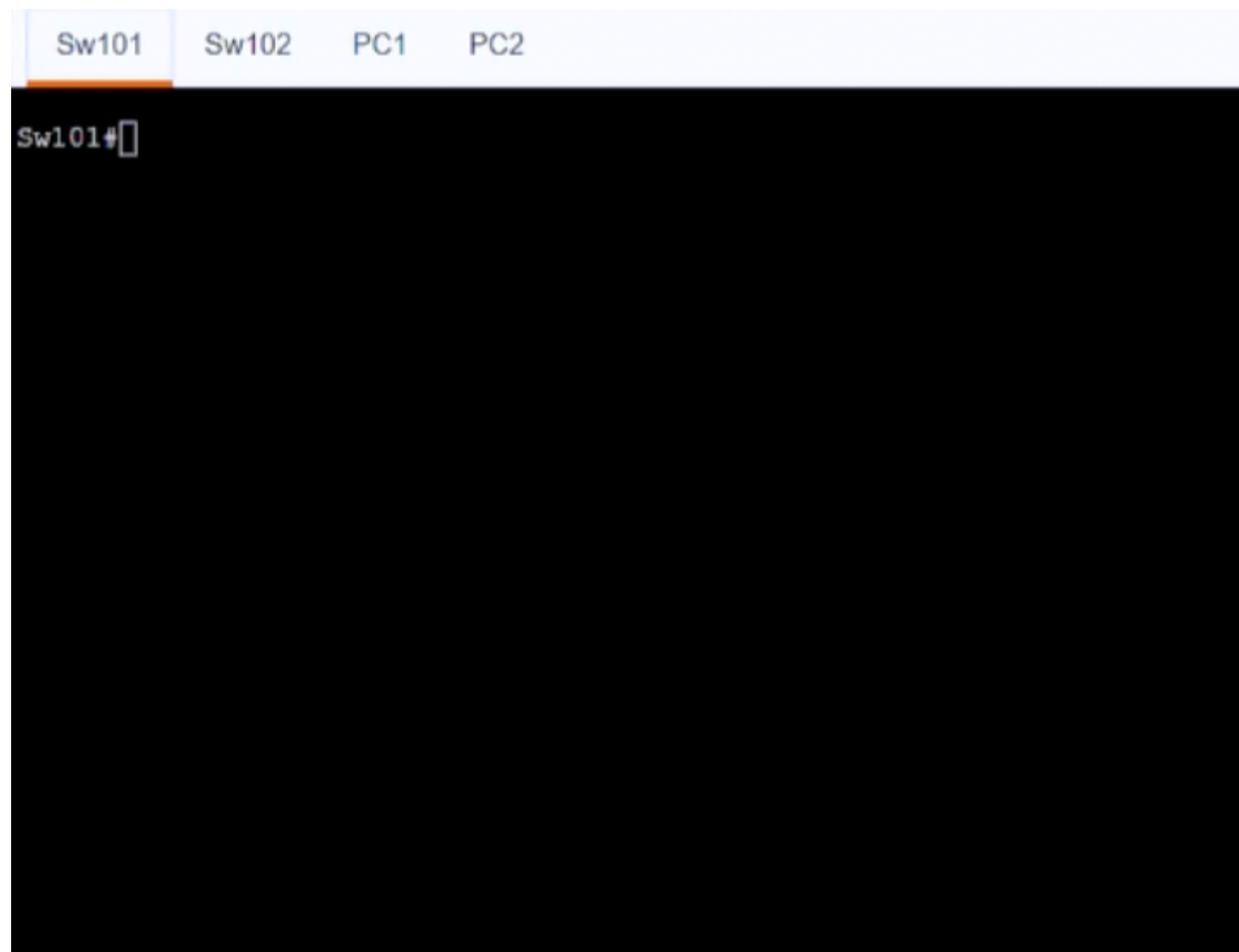
- Name: ENT_ACL
- Restrict only PC2 on VLAN 200 from pinging PC1
- Allow only PC2 on VLAN 200 to telnet to Sw101
- Prevent all other devices from telnetting from VLAN 200
- Allow all other network traffic from VLAN 200

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** 5 months 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 sugested 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** 4 months, 3 weeks ago

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

upvoted 6 times

 **4aynick** 3 months, 2 weeks ago



username support priv 15 password max2learn
upvoted 3 times

  **ac89l** 4 months ago

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

  **studying_1** 3 months, 2 weeks ago

you need to use protocols and port numbers, it only works when you use extended ACLs
upvoted 5 times

  **ac89l** 4 months, 1 week ago

They should be more clear in those questions:

Router> - User EXEC mode

Router# - Privileged EXEC mode

upvoted 3 times

SIMULATION

-

Guidelines

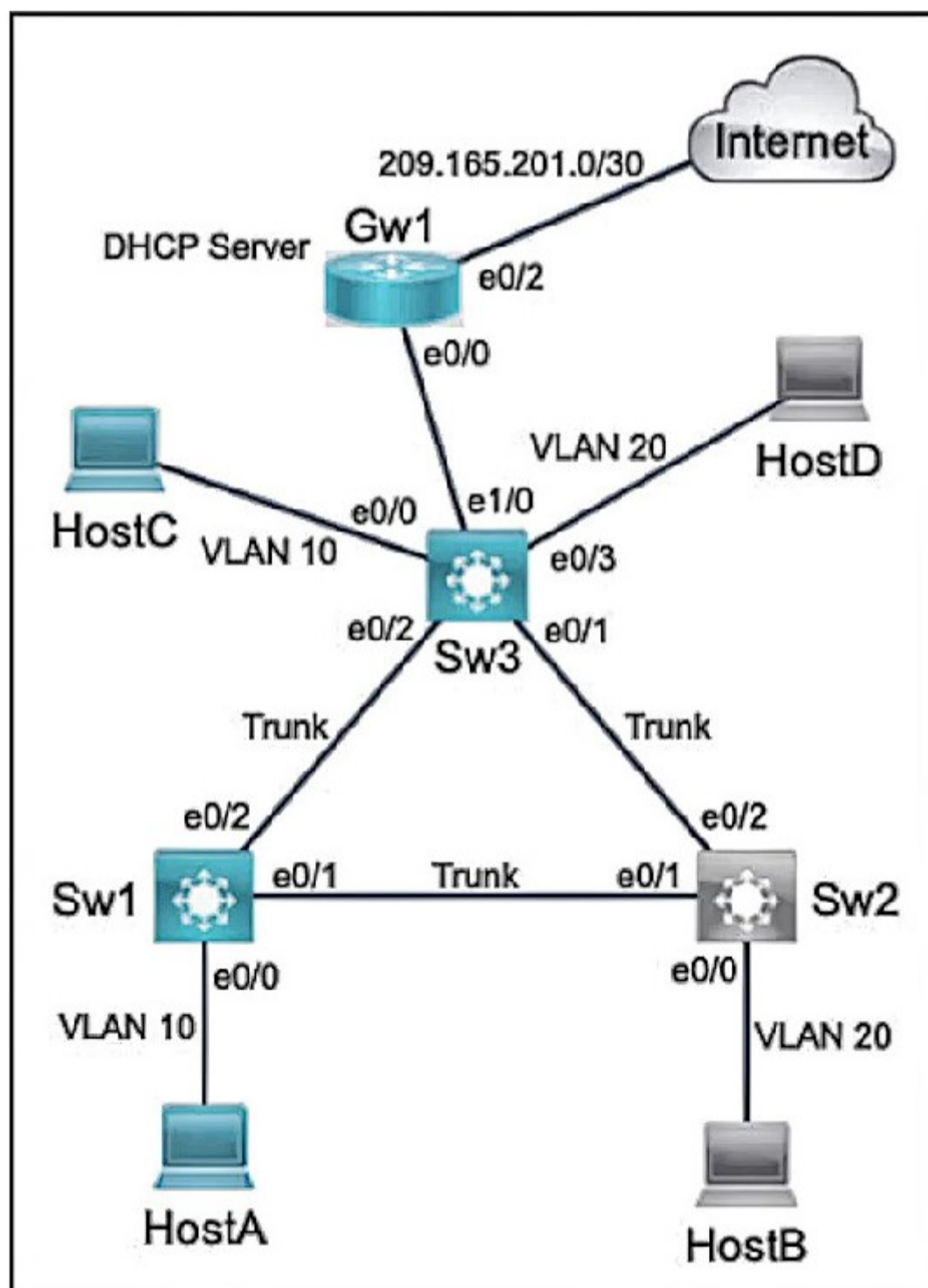
-

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

Gw1

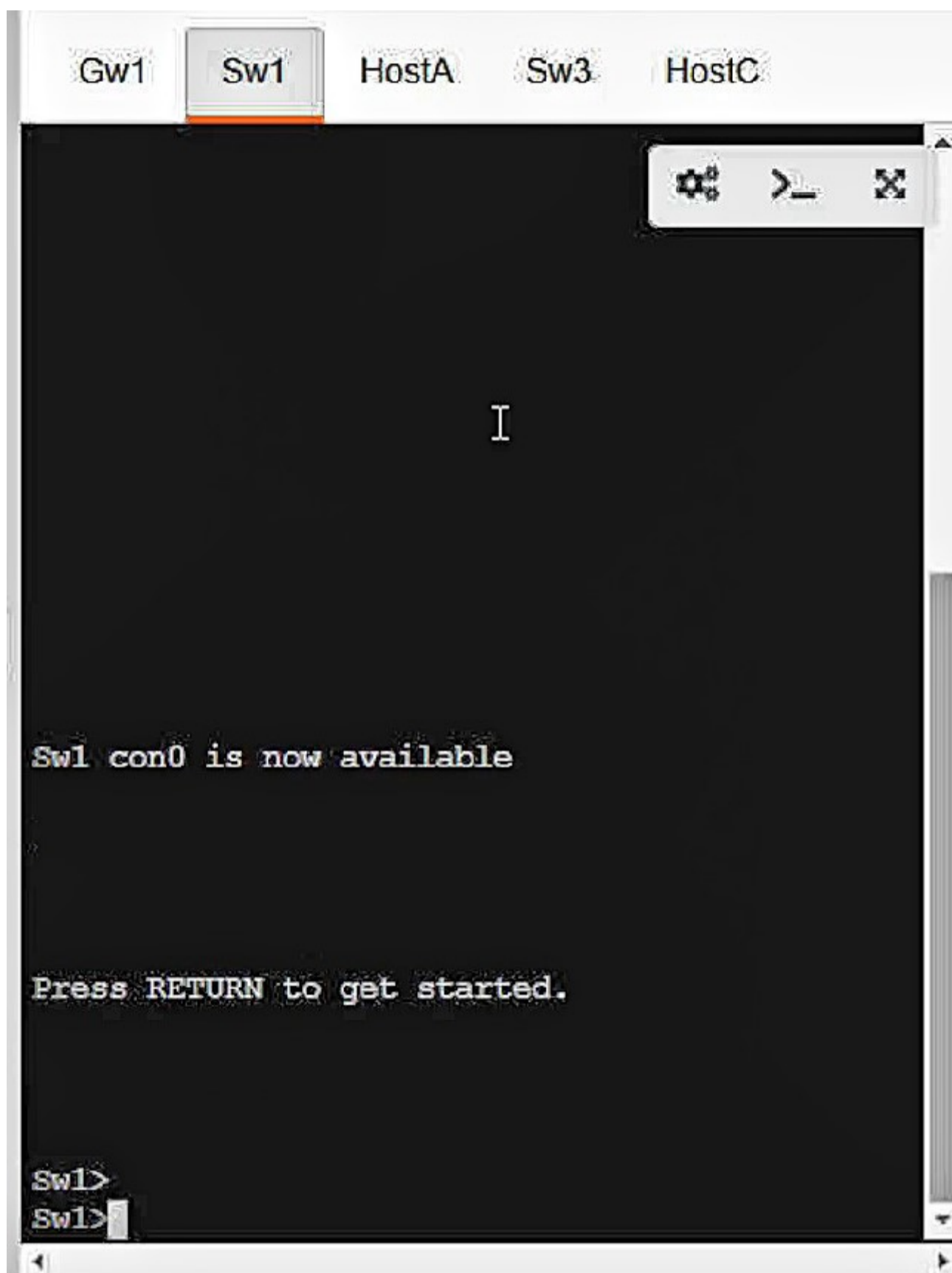
Sw1

HostA

Sw3

HostC

Gw1>



```
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
ip access-group CORP_ACL in


Correct Answer:

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
```

 **rogi2023** Highly Voted 5 months 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 7 times
```

  **Shri_Fcb10** 1 month, 3 weeks ago

Guys how come this ACL is working as standard ACL does not support filtering of packets., so therefore we should be using extended ACL as far as I know.

upvoted 1 times

  **rogi2023** 4 months, 4 weeks ago

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

upvoted 3 times

  **studying_1** 4 months 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 4 times

  **studying_1** 4 months ago

two* typo

upvoted 1 times

  **Peter_panda** 4 months, 4 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 3 times

  **rogi2023** 4 months, 4 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 4 times

  **Nwanna1** Most Recent 1 week, 3 days ago

For the Algorithm: scrypt

On GW1

```
username wheel privilege 15 algorithm-type scrypt secret lock3path
```

```
line vty 0 4
```

```
transport input telnet
```

```
login local
```

upvoted 1 times

  **Nwanna1** 1 week, 3 days ago

For TASK 2

```
ip access-list extended CORP_ACL
```

```
permit udp any any eq bootpc
```

```
permit udp any any eq bootps
```

```
permit tcp 10.10.10.0 0.0.0.255 any eq 443 //there is no "https" keyword so we have to use the port number
```

```
deny ip 10.10.10.0 0.0.0.255 any log-input
```

```
interface e0/0 ip access-group CORP_ACL in //confirm the interface
```

NOTE:

1. any any was used for bootpc and bootps since both used broadcast.

2. The "log-input" logs the following information:

a. ingress interface

b. source MAC address

c. source IP address

d. destination IP address

e. source port

f. destination port.

upvoted 1 times

🗄️ 👤 **Techpro30** 3 weeks ago

```
Router(config)#ip access-list extended CORP_ACL
Router(config-ext-nacl)#
upvoted 1 times
```

🗄️ 👤 **Techpro30** 1 month ago

```
Router(config)#ip access-list extended Corp_ACL
upvoted 1 times
```

🗄️ 👤 **dropspablo** 1 month ago

```
Gw1
configure terminal
username wheel privilege 15 algorithm-type scrypt secret lock3path
line vty 0 4
login local
transport input telnet
exit
-
do show access-list CORP_ACL
(CORP_ACL - modify or create?)
ip access-list extended CORP_ACL
no 10(?)
13(?) permit udp any any bootps (or 67)
14(?) permit udp any any bootpc (or 68)
15(?) permit tcp any any 443
deny ip any any log
exit
do show ip interface brief
do show interface e0/0.10 (confirm Vlan ID 10)
interface e0/0.10
ip access-group CORP_ACL in
do wr
-
Sw1
configure terminal
ip dhcp snooping
ip dhcp snooping vlan 10
no ip dhcp snooping information option
ip dhcp snooping verify mac-address
interface range e0/1 - 2
ip dhcp snooping trust
do wr
upvoted 1 times
```

🗄️ 👤 **dropspablo** 1 week, 4 days ago

```
JUST FIXING FORGOTTEN "EQ" COMMAND:
ip access-list extended CORP_ACL
permit udp any any eq bootps (67)
permit udp any any eq bootpc (68)
permit tcp any any eq 443
deny ip any any log
upvoted 1 times
```

🗄️ 👤 **[Removed]** 2 months, 1 week ago

This can't be CCNA 200-301. Some commands (algorithm-type scrypt, information option...) are nowhere on Cisco Netacad so if this is a lab during the exam, how are we supposed to know we need to learn these commands ?

🗄️ 👤 **Shri_Fcb10** 1 month, 3 weeks ago

Yeah I too felt like that, Because I didn't see in any course where the instructor show about this algo and also it doesn't work on packet tracer

🗄️ 👤 **Toto86** 2 months, 1 week ago

The commands algorithm-type scrypt and snooping information option are listed in CCNA 200-301 Official Cert Guide, Volume 2. Page 94 and page 152

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

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 5 months ago

Selected Answer: C

C. array
upvoted 11 times

 **fmaquino** Highly Voted 5 months, 1 week ago

Selected Answer: C

doesn't sqr brackets represent a array?
Correct me if I'm wrong
upvoted 9 times

 **DaimonANCC** 5 months, 1 week ago

i think to ARRAY
upvoted 6 times

 **Shabeth** Most Recent 2 months, 3 weeks ago

Selected Answer: C

C. Array
upvoted 2 times

 **Tdawg1968** 3 months, 3 weeks ago

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

 **Bhrino** 4 months ago

"]" or "[" = array
"{ " or "}" = object
key : value
any thing in double quotes are strings
upvoted 3 times

 **mrmanistheman** 4 months ago

Selected Answer: C

Answer is definitely C - Array
upvoted 2 times

 **bisiyemo1** 4 months, 3 weeks ago

Selected Answer: C

C for sure
upvoted 3 times

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

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

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** Highly Voted 5 months, 1 week 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 5 times

 **Stevens0103** Most Recent 1 month, 1 week ago

Selected Answer: A

"port" is used as a key to associate each device (router, VPN concentrator, firewall) with a specific port identifier. Therefore, "port" represents a key that labels the associated port value (te6/21, e6/37, ge7/42) within each object.

upvoted 1 times

 **1amconfused** 2 months, 4 weeks ago

Selected Answer: B

Isn't it value? {Key:Value}

upvoted 1 times

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

 **[Removed]** 2 months, 2 weeks ago

Selected Answer: D

Link aggregation provides all this

upvoted 1 times

 **studying_1** 3 months, 2 weeks ago

correct

upvoted 3 times

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 5 months ago

Answers are correct
upvoted 11 times

 **[Removed]** Most Recent 2 months, 1 week ago

Given answers are correct.
upvoted 1 times

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** Highly Voted 4 months, 1 week ago

Selected Answer: C

Answer is correct
upvoted 5 times

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

  **andrizo** 2 weeks, 4 days ago

Based on repeat questions, I agree with the answer.
upvoted 1 times

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

MoHTimo 1 month, 1 week ago

Selected Answer: AE

a and e is correct b/c phoning is the same as vishing
upvoted 1 times

andrizo 2 weeks, 4 days ago

Phoning is not the name of any attack, but phishing and pharming are.
upvoted 1 times

Stevens0103 1 month, 1 week ago

Selected Answer: DE

Phishing is a common social engineering technique that threat actors use to send emails that appear to be from a legitimate organization (such as a bank). The goal is to get the victim to submit personal or sensitive information such as usernames, passwords, account information, financial information, and more. The email could also attempt to trick the recipient into installing malware on their device.

Variations of phishing attacks include:

- Spear phishing
- Whaling
- Pharming
- Watering hole
- Vishing
- Smishing

<https://contenthub.netacad.com/legacy/CyberOps/1.1/en/index.html#6.2.2.7>
upvoted 1 times

[Removed] 2 months, 2 weeks ago

Selected Answer: DE

D. pharming
E. phishing
upvoted 1 times

Bhrino 4 months ago

Selected Answer: DE

kennie is correct i believe they would have specifically called it Wishing
upvoted 1 times

kennie0 4 months ago

Selected Answer: DE

correct answer is DE. There's nothing like phoning. Its rather called Vishing.
upvoted 1 times

JJY888 4 months 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** 3 months, 4 weeks ago

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

  **studying_1** 4 months, 2 weeks 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

SIMULATION

-

Guidelines

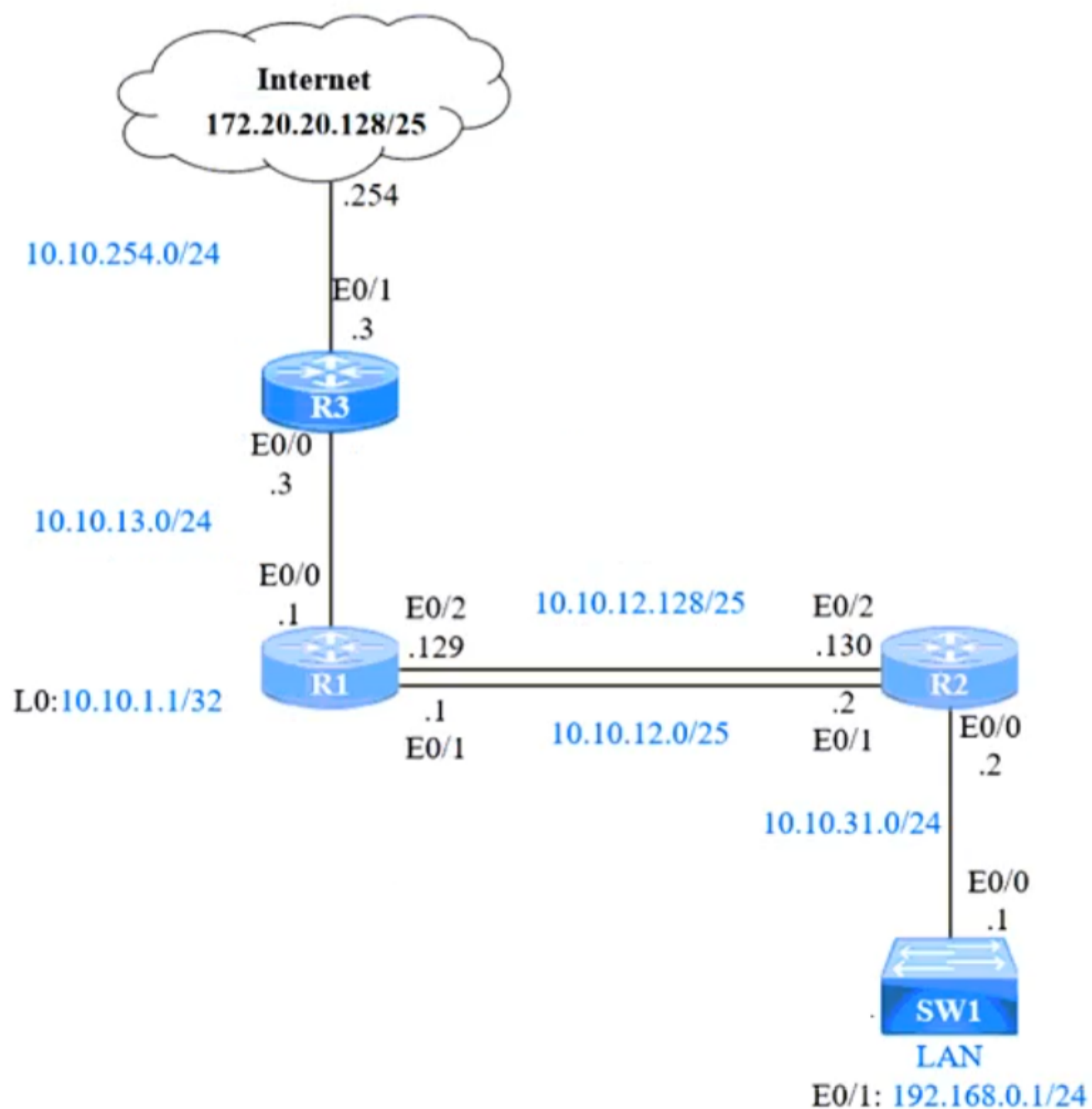
-

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.



```
R2:
Conf t
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 5 months 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 10.10.130 2
```

wr mem @ all R
upvoted 9 times

 **Secsoft** 3 weeks, 6 days ago

I think, for step 3 we need to configure the ether channel first between R1 and R2 then need to apply the static route.
upvoted 1 times

 **Chichi69** 2 months, 3 weeks ago

Hi Rogi, In step 3 we have been asked to configure a single static route but consider both redundant links. How do we consider both redundant links with a single route?
upvoted 1 times

 **ac89l** 4 months ago

regarding task3, how could you route to 10.10.13.1 while it is not your next hop
upvoted 2 times

 **spazzix** 3 weeks, 1 day ago

This is actually a really good packet tracer exercise. So long as the router has awareness to its next hop (in this case it needs to be explicit since a default route isn't allowed), it doesn't have to be a directly connected route. If I have two routes to A and then I set a route to B with next hop A, I will load balance traffic across my two A routes in order to get to B.
In this case, whatever route configuration R2 has to get to 10.10.13.1, it will use to get to 172.20.20.128 via 10.10.13.1
e.g. if traffic to a destination of 10.10.13.1 would be load balanced across e0/2 & e0/1, it will be load balanced to a destination of 172.20.20.128
upvoted 1 times

 **spazzix** 3 weeks, 1 day ago

and similarly, if the setup is such that e0/1 is the primary route and e0/2 is a floating route, then traffic to 172.20.20.128 will only go via e0/1 unless it goes down
upvoted 1 times

 **MDubYa913** 2 months, 1 week ago

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]. <<< I believe this indicates configuring the secondary floating static route.
upvoted 1 times

 **Peter_panda** 4 months, 4 weeks ago

Excellent point regarding task #3!
upvoted 4 times

 **im82** Highly Voted 2 months ago

Hi,
I passed my exam yesterday. more than 80% of the questions are present here. I had 103 questions.
Good luck everyone.
upvoted 7 times

 **kat1969** 1 week, 2 days ago

were the consensus answers correct?
upvoted 1 times

🗨️ 👤 **SudipSen** Most Recent 2 weeks, 6 days ago

Anyone tried this lab in packet tracer ? I tried from scratch. I understood well all the answers but I am unable to configure the SW1 properly ..
upvoted 1 times

🗨️ 👤 **Cynthia2023** 1 month, 2 weeks ago

what I wrote is below.

#Task 1

#R2

```
ip route 192.168.0.0 255.255.255.0 10.10.31.1
```

#Task 2

#R1

```
ip route 0.0.0.0 0.0.0.0 10.10.13.3
```

#Task 3

#R2

```
ip route 172.20.20.128 255.255.255.128 10.10.12.1
```

```
ip route 172.20.20.128 255.255.255.128 10.10.12.129 2
```

#Task 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 10.10.12.130 2
```

The solution to task 3, configure a single static route while considering redundant links, we can use a floating static route. A floating static route is a backup route that has a higher administrative distance than the primary route. It's how we can configure a single static route with redundancy using a floating static route on router R2.

upvoted 1 times

🗨️ 👤 **some0n3** 2 months ago

about task 3: I think we should use the L0 on R1 as the next hop when configuring the single static route on R2.

upvoted 3 times

🗨️ 👤 **[Removed]** 2 months, 2 weeks ago

At step 3, don't we need to configure two static routes (one per link)? I'm just wondering

upvoted 1 times

🗨️ 👤 **no_blink404** 3 months ago

I am no means an expert, but this would be my answer:

R2)

```
ip route 192.168.0.0 255.255.255.0 10.10.31.1 #STEP 1#
```

```
ip route 172.20.20.128 255.255.255.128 10.10.12.1 #STEP 3#
```

```
copy run start
```

R1)

```
ip route 0.0.0.0 0.0.0.0 10.10.13.3 #STEP 2#
```

```
ip route 192.168.0.0 255.255.255.0 e0/1 #STEP 4#
```

```
ip route 192.168.0.0 255.255.255.0 10.10.12.130 2 #STEP 4#
```

```
copy run start
```

upvoted 6 times

🗨️ 👤 **HM01** 2 months, 1 week ago

Router#1 step 4 can be done like this. correct me if i'm wrong

```
Router(config)#ip route 192.168.0.0 255.255.255.0 10.10.12.2
```

```
Router(config)#ip route 192.168.0.0 255.255.255.0 10.10.12.130 2
```

upvoted 2 times

🗨️ 👤 **Shabeth** 2 months, 3 weeks ago

correct

upvoted 1 times

🗨️ 👤 **Chichi69** 2 months, 3 weeks ago

Correct. Step 3 the next hop is 10.10.12.1

upvoted 1 times

🗨️ 👤 **Keba889** 4 months, 2 weeks 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 4 times

🗨️ 👤 **studying_1** 4 months, 2 weeks ago

Yes, AD should be 2 not 3

upvoted 1 times

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

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: A

This is correct

A. They enable communication between the controller and the network device.

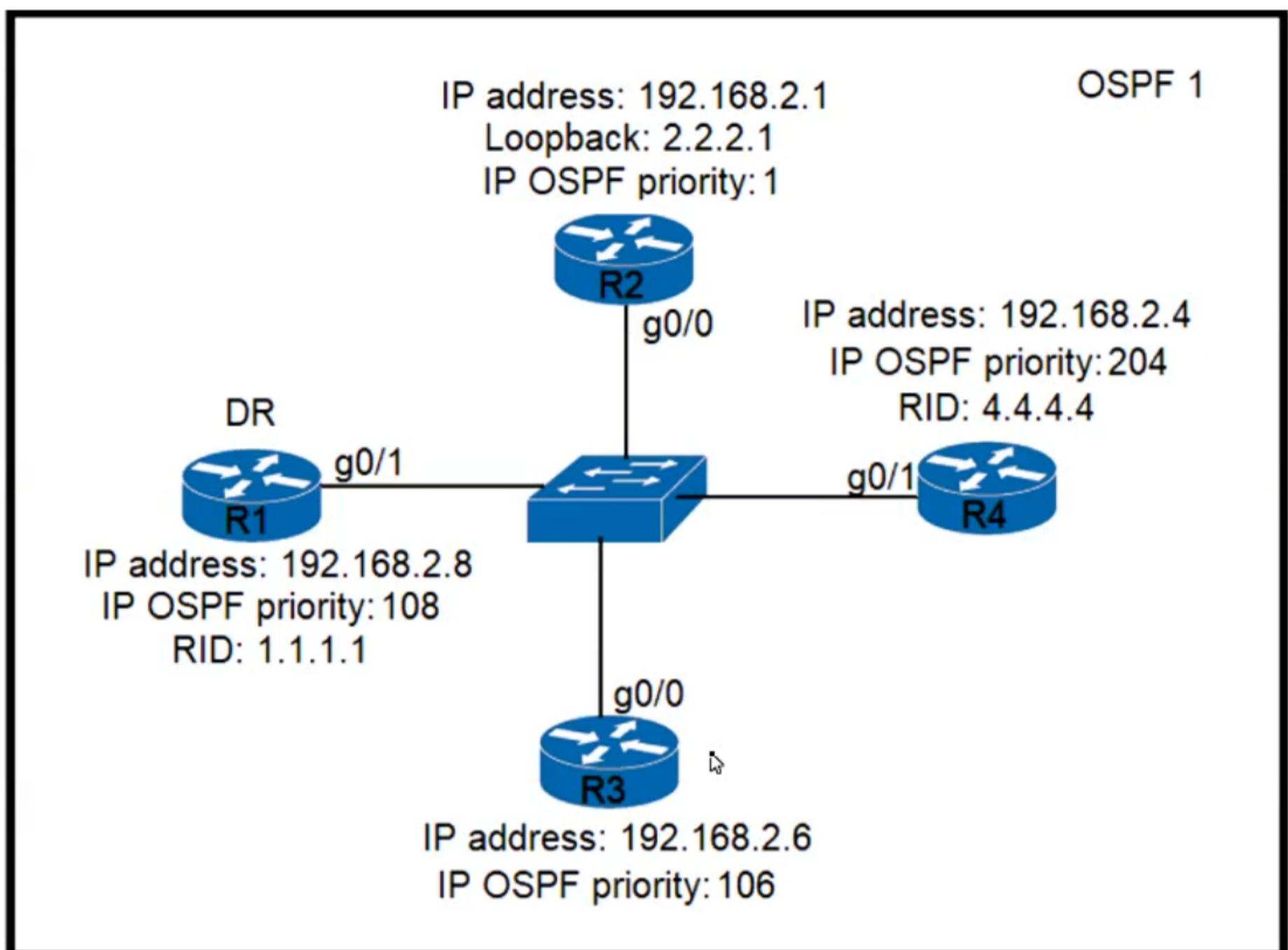
upvoted 1 times

  **studying_1** 3 months, 2 weeks 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 Highly Voted 3 months, 3 weeks 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 5 times

Yannik123 Most Recent 1 week, 3 days ago

Selected Answer: D

D is correct the OPSF Prio is the highest of all four routers.

upvoted 1 times

[Removed] 2 months, 2 weeks ago

Selected Answer: D

R4 has the highest priority therefore, it will be elected as the DR.

upvoted 1 times

Bhrino 4 months ago

regarding ospf the highest ip priority becomes the dr
upvoted 2 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

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: B

B. default-router
upvoted 2 times

  **DaimonANCC** 3 months, 4 weeks ago

correct
upvoted 4 times

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 5 months, 1 week 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 6 times

 **NetworkGeek00** Most Recent 1 month, 1 week ago

Selected Answer: AC

this is so confusing. i think it is A and C. about the B yeah its partially correct but A and C are more accurate.

upvoted 1 times

 **Stevens0103** 1 month, 1 week ago

Multiple context mode does not support the following features:

- Dynamic routing protocols

Security contexts support only static routes. You cannot enable OSPF or RIP in multiple context mode.

- VPN

- Multicast

https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/contexts.html

upvoted 2 times

 **Stevens0103** 3 weeks, 4 days ago

"Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management. Some features are not supported, including VPN and dynamic routing protocols."

https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/mode_contexts.html#92503

upvoted 1 times

 **dropspablo** 1 month, 4 weeks ago

Selected Answer: AC

"From what I understand, the firewall can have Multi-Context mode, in which it is virtualized in separate instances to be used in different domains of the company. This allows independent configurations, such as URI filters, NAT, remote access VPN and even configurations site-to-site VPN separated by context (instance). In addition, the firewall in Standalone mode, which is a normal and independent firewall (not divided into virtual instances), is also capable of offering site-to-site VPN feature -site as an endpoint to another firewall or router. So option B is wrong as it mentions that the firewall offers site-to-site VPN only in Standalone mode, when in fact, in both Multi-Context and Standalone mode, it is possible to configure the firewall as an endpoint for a site-to-site VPN. The correct statement would be: 'it serves as an endpoint for a site-to-site VPN in standalone mode or in Multi-Context mode'."

upvoted 1 times

 **Stevens0103** 1 month, 1 week ago

Unsupported Features

Multiple context mode does not support the following features:

- Dynamic routing protocols



Security contexts support only static routes. You cannot enable OSPF or RIP in multiple context mode.

- VPN

- Multicast

https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/contexts.html

upvoted 1 times

  **pikos1** 3 months, 3 weeks 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** 3 months, 2 weeks ago

right, the NGFW filters based on application

upvoted 1 times

  **Mizuchan** 3 months, 3 weeks 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** 4 months, 3 weeks 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 3 times

  **studying_1** 4 months, 1 week ago

I agree, i think it is C & E

upvoted 1 times

  **studying_1** 4 months, 1 week 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** 4 months, 3 weeks ago

Selected Answer: AB

A and B for sure

upvoted 2 times

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

 **Yannik123** 2 weeks, 3 days ago

Selected Answer: B

B is correct: The valid range is 0 to 5 sessions and the default value is 5 sessions. A value of zero indicates that Telnet/SSH sessions are disallowed.
upvoted 1 times

 **Joshrzo01** 3 months, 2 weeks 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 2 times

 **4aynick** 3 months, 2 weeks 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

 **JJY888** 4 months ago


Selected Answer: B

ChatGPT says 5 but sometimes ChatGPT is wrong.
upvoted 2 times

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

 **[Removed]** 2 months, 2 weeks ago

Selected Answer: A

A. Reassociation Request

In WLAN network, reassociation request frame is used by mobile stations in the following scenarios:

- Moving from one basic service area to the other service area in the same extended service area.
- leaving the wifi network coverage area and comes back to the same area again

upvoted 1 times

 **studying_1** 3 months, 2 weeks ago

Answer is correct
upvoted 2 times

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.

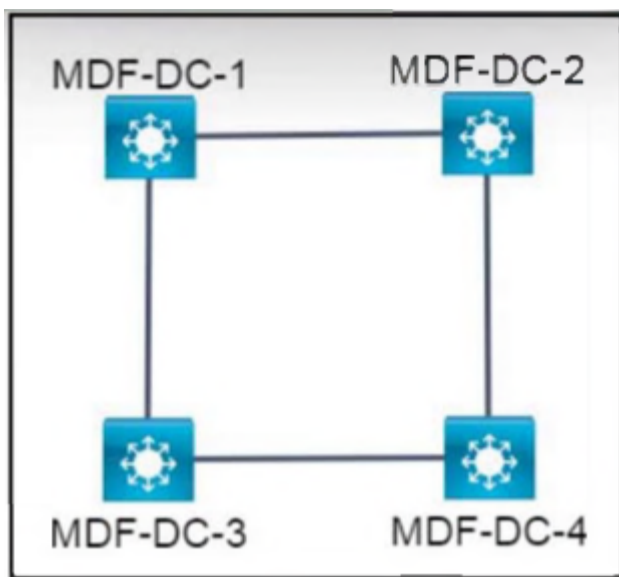
Correct Answer: C

  **Bhrino** 4 months ago

Selected Answer: C

this is 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 3 times



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 4 months, 3 weeks ago

Right ans
upvoted 7 times

Biggeorge123 Most Recent 4 months 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

[Removed] 2 months, 1 week ago

B is 0d:0E
C is 0d:E0

0 is lower than E therefore the correct answer is B
upvoted 1 times

studying_1 4 months ago

yes, B has the lowest MAC address, check again, answer is correct
upvoted 3 times

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** 3 months, 2 weeks ago
 correct without chatgpt)
 upvoted 4 times
- 🗨 **ac89l** 4 months ago
 Correct according to chatgpt, but sometimes chatgpt is wrong :)
 upvoted 4 times
- 🗨 **[Removed]** 2 months, 2 weeks ago
 I'm not ChatGPT but i confirm that given answers are correct :)
 upvoted 3 times

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** 3 months, 3 weeks ago

I meant question 1084
upvoted 1 times

  **Tdawg1968** 3 months, 3 weeks ago

Contradicts question 1089. Shouldn't this be a key?
upvoted 1 times

  **studying_1** 3 months, 2 weeks ago

answer is correct, it is a value, if it is before ":" it's a (key), if after ":" it's a (value)
upvoted 4 times

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

🗨️ **mda2h** 1 month, 1 week ago

Selected Answer: D

Access ports
upvoted 1 times

🗨️ **alfredshw** 1 month, 3 weeks ago

Selected Answer: A

A. Correct, layer 3 do not need STP
B. Wrong, portfast doesn't support trunk
C Wrong, same as B
D Wrong, portfast only support on access port so you still need to enable it.
upvoted 1 times

🗨️ **[Removed]** 2 months, 2 weeks ago

Selected Answer: D

Access ports
upvoted 1 times

🗨️ **studying_1** 3 months, 2 weeks ago

correct
upvoted 2 times

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** **Highly Voted** 4 months, 3 weeks ago



Right ans
upvoted 6 times

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** Highly Voted 4 months ago

Selected Answer: A

objects are show in {} curly brackets
upvoted 6 times

  **[Removed]** Most Recent 2 months, 2 weeks ago

Selected Answer: A

A. object
upvoted 1 times

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

- 🗨 **[Removed]** 2 months, 2 weeks ago
 Given answers are correct
 upvoted 1 times
- 🗨 **studying_1** 3 months, 2 weeks ago
 Answer is correct
 upvoted 3 times

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** Highly Voted 3 months, 2 weeks ago
correct
upvoted 5 times
- mda2h** Most Recent 1 month, 1 week ago
correct
upvoted 3 times

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

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

 **mda2h** 1 month, 1 week ago
correct
upvoted 3 times

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

 **BarkingSpider** 1 month, 2 weeks ago

this question appears 6 different times in this dump, so pretty safe to say you'll see this one on your exam.

upvoted 1 times

 **StingVN** 2 months, 2 weeks ago

Unique local: fc-fd

Link local: fe

Multicast: ff

Global unicast: 2000

upvoted 2 times

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

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

 **StingVN** 2 months, 2 weeks ago

Unique local: FC

Link Local: FE

Multicast: FF

Global Unicast: 2000

upvoted 3 times

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 Highly Voted 4 months, 3 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/fiberopticspt2singlemultifiber>
 - > "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 5 times

mda2h 1 month, 1 week ago

Given answer is correct.
Incredible how some can read but read wrong!

False, DWDM is multi-mode:

page 21 chapter 2
https://www.cisco.com/c/dam/global/de_at/assets/docs/dwdm.pdf

upvoted 1 times

  **mda2h** Most Recent 1 month, 1 week ago

Correct

<https://www.ciena.com/insights/what-is/What-Is-WDM.html>

upvoted 1 times



  **hamish88** 4 months, 3 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 3 times

  **[Removed]** 2 months, 1 week ago

I think you're right, i would say the question itself is wrong.

Here's what i found :

- In contrast to multimode, single-mode fibre cable has only one mode of propagation: a single wavelength of light in the fibre core

- Simply explained, DWDM technology is based on the combination and transmission of multiple optical signals, with dedicated wavelengths simultaneously using the same fiber cable. This means that DWDM uses single mode fiber to carry multiple light waves of different frequencies.

upvoted 2 times

  **SamSerious365** 5 months ago

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

upvoted 2 times

  **mda2h** 1 month, 1 week ago

This is false DWDM systems pack multiple wave-lengths

upvoted 1 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

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: A

A. is used without allocation from a regional internet authority

upvoted 2 times

  **studying_1** 3 months, 2 weeks ago

correct

upvoted 2 times

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

 **dropspablo** 1 month, 3 weeks ago

By ChatGPT:

Based on the provided output, the condition of interface that is occurring is:

C. queueing

The output shows information related to the interface's queuing strategy, including the input queue size, output queue size, and input/output rates. It also mentions that the queuing strategy is "fifo," which stands for "First In, First Out." This means that packets are processed in the order they arrive, and the interface is not experiencing any drops in the output queue (Output queue: 0/300).

upvoted 1 times

 **dropspablo** 1 month, 3 weeks ago

The other options are not supported by the information given in the output:

- A. "bad NIC" (Network Interface Card) is not mentioned or implied in the output.
- B. "high throughput" is not explicitly mentioned in the output. It only shows the bandwidth (BW) of the interface, but the current throughput is reported as 0 bits/sec for both input and output.
- D. "broadcast storm" is not mentioned in the output. There is a line showing "Received 267 broadcasts (0 IP multicasts)," which indicates the number of broadcast packets received, but it doesn't suggest a broadcast storm.

upvoted 1 times

 **JJY888** 4 months ago

Selected Answer: C

There are no issues so I guess C is correct.

upvoted 4 times

 **studying_1** 3 months, 2 weeks ago

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

upvoted 2 times

 **Peter_panda** 4 months, 2 weeks ago

Selected Answer: A

By exclusion, I would say the NIC is bad
upvoted 2 times

  **studying_1** 3 months, 2 weeks 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 4 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

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: D

D. alleviates the shortage of IPv4 addresses
upvoted 1 times

  **studying_1** 3 months, 2 weeks 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

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: C

C. is used on hosts that communicate only with other internal hosts
upvoted 1 times


  **studying_1** 3 months, 2 weeks ago

correct
upvoted 2 times

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

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: B

Answer B is correct
upvoted 1 times

  **NeoSam999** 2 months, 2 weeks ago

Selected Answer: B

B is correct
upvoted 2 times

  **studying_1** 3 months, 2 weeks ago

correct
upvoted 2 times

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 runs, 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

 **shaney67** 2 days, 1 hour ago

Went with high throughput, was tempted with queueing but dont see anything in the queue for input or output
upvoted 1 times

 **Shri_Fcb10** 1 month, 3 weeks ago

Why is D not right? The input packet is more than Output packet. I saw a question above on this same page where people have voted for queuing and in there too the input packet was more than output packet
upvoted 1 times

 **NetworkGeek00** 1 month, 1 week ago

both C and D are correct. but C is more accurate in this questions. because of the Rx and Tx values and the rates.
upvoted 2 times

 **dropspablo** 1 month, 3 weeks ago

C. high performance (high throughput)

The values "txload 255/255, rxload 255/255", indicate that the interface has "high throughput", operating close to or at the limit of its data transmission and reception capacity.

Also:

The output shows high rates of traffic on the interface, with an incoming rate of 200234873 bits/sec and an outgoing rate of 233830309 bits/sec for the last 30 seconds. This indicates that the interface is handling a significant amount of data, resulting in high throughput.

upvoted 1 times

 **NeoSam999** 2 months, 2 weeks ago

C is correct
Please look at Rx and Tx loads
upvoted 2 times

 **Mizuchan** 3 months, 3 weeks ago

Selected Answer: C

RX and TX 255/255

upvoted 4 times

  **Bhrino** 4 months ago

Selected Answer: C

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

upvoted 4 times

  **Peter_panda** 4 months, 2 weeks 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

  **ac89l** 4 months ago

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

upvoted 1 times

  **Rydaz** 4 months, 1 week 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

  **NeoSam999** 2 months, 2 weeks ago

B is correct

This is possible because private IP addresses are not globally unique or routable on the public internet. Instead, they are intended for use within private networks, offering a level of address reuse and allowing multiple entities to have overlapping address spaces without interfering with each other.

upvoted 2 times

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	Global Unicast
fe80:27bb:1ef9:6b3d:b347:686f:f3b7:7	Unique Local
fc00:9e81:2346:4929:7fec:34e9:7b8c:3	Link-Local Unicast
2000:0962:6dee:8c78:93b8:c429:c78d:1	Multicast

Answer Area**Correct Answer:**

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

 **NeoSam999** 2 months, 2 weeks ago

Answers are correct.

Global Unicast Address: 2000::/3 (2000 to 3FFF)

Link-Local Address: FE80::/10.

Unique Local Address: FC00::/7 or FD00::/8.

Multicast addresses: FF00::/8.

upvoted 2 times

DRAG DROP

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

Answer Area

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

Answer Area

Correct Answer:

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

[Removed] 2 months, 2 weeks ago
Given answers are correct.
upvoted 3 times

studying_1 3 months, 2 weeks ago
Answers are correct
upvoted 3 times

DRAG DROP

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

Answer Area

may be used by multiple organizations at the same time	Unique Local [] []
attached to a single subnet	
required on all IPv6 devices	Link-Local Address [] []
is a counterpart of private IPv4 address	

Answer Area

Correct Answer:

may be used by multiple organizations at the same time	Unique Local may be used by multiple organizations at the same time is a counterpart of private IPv4 address
attached to a single subnet	
required on all IPv6 devices	Link-Local Address attached to a single subnet required on all IPv6 devices
is a counterpart of private IPv4 address	

Bhrino Highly Voted 4 months ago
answers are correct
upvoted 6 times

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

🗨️ **4Lucky711** 1 month, 2 weeks ago

The SSID can consist of up to 32 alphanumeric, case-sensitive, characters.
So D is correct!

A is incorrect. --> It should be --> It "uniquely" identifies an access point in a WLAN
upvoted 1 times

🗨️ **NeoSam999** 2 months, 2 weeks ago

Selected Answer: D

D is correct
upvoted 1 times

🗨️ **Dunedrifter** 2 months, 3 weeks ago

Selected Answer: D

Answer is D
upvoted 1 times

🗨️ **studying_1** 3 months, 2 weeks ago

Selected Answer: D

Answer is D
upvoted 2 times

🗨️ **studying_1** 3 months, 2 weeks ago

Selected Answer: A

D is correct
upvoted 1 times

🗨️ **studying_1** 3 months, 2 weeks ago

sorry voted wrong, answer is D
upvoted 1 times

🗨️ **Bhrino** 4 months 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

🗨️ **ac89l** 4 months ago

Selected Answer: C

B,D,A = Wrong
upvoted 1 times

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

 **NeoSam999** 2 months, 2 weeks ago

Selected Answer: B

B is correct

The correct characteristic of private IPv4 addressing is that it is used on hosts that communicate only with other internal hosts. Private IPv4 addressing refers to the allocation of IP addresses from specific ranges reserved for use within private networks.

upvoted 1 times

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

  **olofinluajoshua** 1 week ago

Similar answer from ChatGPT & Bard:

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

Explanation: Encryption in wireless networks not only secures data by encoding it but also includes integrity checks to detect any unauthorized alterations or forgery of the data during transmission. This helps ensure the data's integrity and authenticity.

The other options are not accurate descriptions of encryption in wireless networks:

A. Identifying an access point is the role of an SSID, not encryption.

B. Using a password for connection is related to authentication, not encryption.

D. Authentication protocols are separate from encryption, although both are important security aspects in wireless networks. Encryption focuses on data confidentiality, while authentication verifies the identity of users or devices trying to connect to the network.

upvoted 1 times

  **4Lucky711** 1 month, 2 weeks ago

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

D. uses authentication protocols to secure a network --> WPA, WPA2, WPA3...

ChatGPT:

The statement "uses integrity checks to identify forgery attacks in the frame" is incorrect because using integrity checks to identify forgery attacks is not a characteristic of encryption in wireless networks. Integrity checks are used to verify whether data has been altered or corrupted during transmission and are typically implemented by certain protocols or security mechanisms like IPsec. In wireless networks, encryption is primarily used to ensure data confidentiality, not integrity.

WPA, WPA2, and WPA3 are encryption features in wireless networks. These protocols all use authentication and encryption to secure the wireless network, ensuring that only authorized users can connect and access the network. The encryption functionality prevents unauthorized users from eavesdropping on network communications, safeguarding users' personal information and data security.

upvoted 2 times

  **andrizo** 2 weeks, 6 days ago

Well can't argue with chatgpt.

upvoted 1 times

  **4Lucky711** 1 month, 2 weeks ago

So I think D is correct.

upvoted 2 times

  **Shri_Fcb10** 1 month, 3 weeks ago

Selected Answer: D

D is correct. Wireless encryption uses authentication protocols to secure your wireless network

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

upvoted 2 times

  **sam225555** 2 months ago

Selected Answer: C

CC is correct

upvoted 1 times

  **NeoSam999** 2 months, 2 weeks ago


Selected Answer: C

C is correct

The correct characteristic of encryption in wireless networks is that it uses integrity checks to identify forgery attacks in the frame. Encryption is the

process of encoding data to make it unreadable to unauthorized parties. In the context of wireless networks, encryption is used to secure the communication between devices and access points.

upvoted 1 times

 **perri88** 3 months ago

Selected Answer: D

I think it's D : Wireless encryption uses authentication protocols to secure your wireless network. A password or network key is required when a user or device attempts to connect.

upvoted 2 times

 **Bhrino** 4 months 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

 **ac89l** 4 months 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

 **ac89l** 4 months ago

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

upvoted 1 times

 **studying_1** 3 months, 2 weeks ago

Answer is C, its encryption, D is about authentication

upvoted 3 times

 **JJY888** 4 months 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

Topic 1

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

 **NeoSam999** 2 months, 2 weeks ago

D is correct

The correct characteristic of private IPv4 addressing is that it is used on hosts that communicate only with other internal hosts. Private IPv4 addressing refers to the allocation of IP addresses from a specific range of reserved IP address blocks that are designated for use within private networks.

upvoted 2 times

 **Bhrino** 4 months ago

Selected Answer: D

D is almost an exact purpose of Private addresses

upvoted 4 times

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

  **NeoSam999** 2 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

  **studying_1** 3 months, 2 weeks 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 2 times

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

 **learntstuff** 1 month, 3 weeks ago

This is a terrible question. Encryption doesn't prevent interception, it prevents people reading what is being sent. Which in turn is technically an increase in protect against spyware. All I am saying in this pointless comment is this question sucks. On a positive note, I hope no one gets this question on the exam and you all pass. Peace out!

upvoted 3 times

 **Stevens0103** 1 month, 1 week ago

"Encryption is the process of converting or scrambling data and information into an unreadable, encoded version that can only be read with authorized access. Encryption is a widely used security tool that can prevent the interception of sensitive data, either while stored in files or while in transit across networks."

<https://www.cisco.com/c/en/us/products/security/encryption-explained.html>

upvoted 2 times

 **NeoSam999** 2 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **Dunedrifter** 2 months, 3 weeks ago


Selected Answer: D

D. prevents the interception of data as it transits a network.

Encryption in wireless networks plays a crucial role in preventing unauthorized access to sensitive information by encrypting the data as it travels between devices over the network. This encryption ensures that even if the data is intercepted by an unauthorized party, it remains unreadable and protected. Therefore, option D accurately describes a characteristic of encryption in wireless networks.

Option A is not directly related to encryption but rather pertains to protection against spyware, which is a separate security concern. Option B refers to user authentication rather than encryption. Option C mentions the use of ciphers to detect and prevent zero-day network attacks, which is not a specific characteristic of encryption in wireless networks.

upvoted 1 times

 **Bingchengchen236** 2 months, 4 weeks ago

choose C

upvoted 1 times

 **Bhrino** 4 months 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 2 times

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

  **andrizo** 2 weeks, 6 days ago

Selected Answer: C

This question has appeared several times, and C is the only consistent answer.
upvoted 1 times

  **4Lucky711** 1 month, 2 weeks ago

Selected Answer: C

D is incorrect. --> It should be --> identifies a "unique" access point on a WLAN

The Service Set Identifier (SSID) is a "unique" identifier or a network name that wireless clients can connect to or share among all devices in a wireless network.

<https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5305-wireless-access-points-frequently-asked-questions.html#SSID>

upvoted 2 times

  **Stevens0103** 1 month, 1 week ago

You're absolutely right! SSID is an 'identifier'! It's not a machine like an AP, which does generate signals.



The answer is D.

upvoted 1 times

  **Stevens0103** 1 month, 1 week ago

I admit that I was wrong cause APs can be named the same. That leaves only one choice that I reluctantly agree to. Poorly worded question.

upvoted 1 times

  **Kerrera** 1 month, 2 weeks ago

Selected Answer: C

AP advertises the wireless network with a Service Set Identifier (SSID) and the AP group identifies the SSID

upvoted 1 times

  **Stevens0103** 1 month, 1 week ago

So, it's AP that generates the signals, not SSID, isn't it?

The answer is D.

upvoted 1 times

  **Stevens0103** 1 month, 1 week ago

I admit that I was wrong cause APs can be named the same. That leaves only one choice that I reluctantly agree to. Poorly worded question.

upvoted 1 times

  **dropspablo** 1 month, 3 weeks ago

Selected Answer: C

C. broadcasts a beacon signal to announce its presence by default

upvoted 1 times

  **Stevens0103** 1 month, 1 week ago

A string does not generate signals, a machine like AP does.


The answer is D.

upvoted 1 times

  **Stevens0103** 1 month, 1 week ago

I admit that I was wrong cause APs can be named the same. That leaves only one choice that I reluctantly agree to. Poorly worded question.

upvoted 1 times

  **Titiano** 2 months, 1 week ago

in question 1108 the answer is:

emits a beacon signal to announce its presence by default

Why wouldn't the same answer as in question 1108 be valid for this question?


upvoted 2 times

  **NeoSam999** 2 months, 2 weeks ago

Selected Answer: D

D is correct.

upvoted 1 times

  **Dunedrifter** 2 months, 3 weeks ago

Selected Answer: D

D. identifies an access point on a WLAN.

An SSID (Service Set Identifier) is a unique identifier that is assigned to an access point (AP) in a wireless network. It serves as the name of the wireless network and allows devices to identify and connect to a specific access point within the WLAN. Therefore, option D accurately describes a characteristic of an SSID in wireless networks.

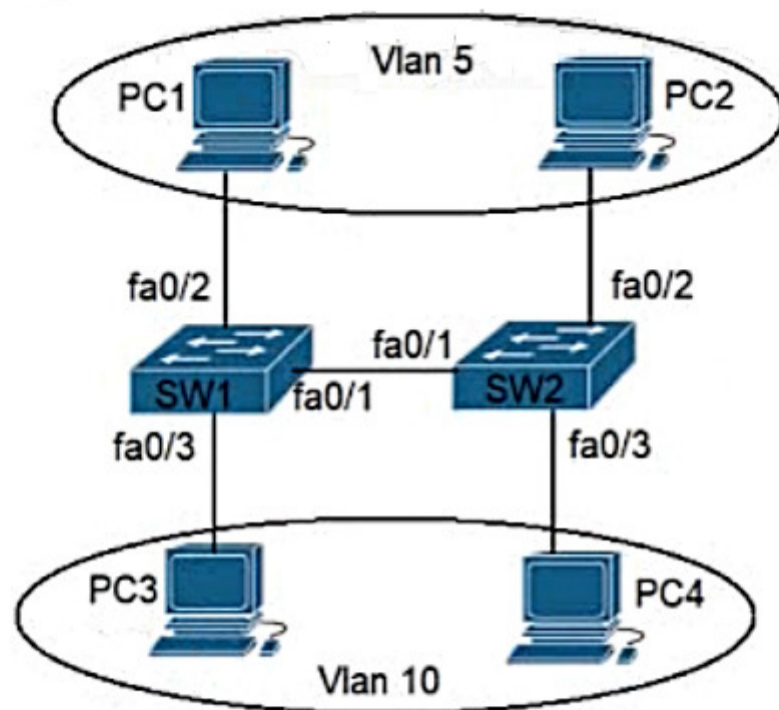
Option A refers to data threat interception, which is not specifically related to the SSID. Option B mentions the encoding of connections, which is more related to encryption rather than the SSID itself. Option C states that the SSID broadcasts a beacon signal to announce its presence by default, which is indeed a characteristic of an SSID in wireless networks. However, the more specific and accurate characteristic is that it identifies an access point on a WLAN. ~~chatgpt

upvoted 2 times

  **Bhrino** 4 months ago

answer is correct

upvoted 1 times



```
Switch2(config)#interface fa0/1
Switch2(config-if)#switchport mode dynamic auto
Switch2(config-if)#switchport trunk allowed vlan 5,10
```

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 Highly Voted 4 months ago

Selected Answer: A

have to tell the switch that the specific interface is a trunk port ie A
upvoted 5 times

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

bisiyemo1 Highly Voted 4 months, 1 week ago

The answers are correct
upvoted 7 times

blablalbla123 Most Recent 4 months ago

can anyone post the solution?
upvoted 1 times

Bhrino 4 months ago

answers are right
upvoted 4 times

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** Highly Voted 4 months ago

Selected Answer: C

because private ips are private people don't have to register to get them so its c
upvoted 7 times

DRAG DROP

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

Answer Area

is a counterpart of private IPv4 addresses	Unique Local
sends packets to a group address rather than a single address	
has a unicast source sent to a group	Multicast
allows sites to be combined without address conflicts	

Answer Area

Correct Answer:

is a counterpart of private IPv4 addresses	Unique Local
sends packets to a group address rather than a single address	allows sites to be combined without address conflicts
has a unicast source sent to a group	Multicast
allows sites to be combined without address conflicts	sends packets to a group address rather than a single address
	has a unicast source sent to a group

Bhrino 4 months ago

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

upvoted 3 times

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	multimode fiber
becomes distorted at longer lengths	
is typically used for internal datacenter connectivity	single-mode fiber
has minimal light reflection as it travels down the core	

Correct Answer:

uses a single wavelength on light	multimode fiber
becomes distorted at longer lengths	is typically used for internal datacenter connectivity
is typically used for internal datacenter connectivity	becomes distorted at longer lengths
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

Bhrino Highly Voted 4 months 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 6 times

[Removed] Most Recent 2 months, 2 weeks ago

Provided answers are correct
upvoted 2 times

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** Highly Voted 4 months 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 6 times

 **Cynthia2023** Most Recent 1 month, 2 weeks ago

Selected Answer: C

The answer is correct
upvoted 1 times

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** 4 months 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 4 times

 **ac89l** 4 months ago

Selected Answer: C

Notice the txload/rxload
upvoted 3 times

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

 **andrizo** 2 weeks, 6 days ago

Selected Answer: C

I don't think it's B because SSID isn't for authentication, just identification.

upvoted 1 times

 **VarDav** 3 weeks, 4 days ago

Selected Answer: C

It's C. Look at 1110.

upvoted 1 times

 **Stevens0103** 1 month, 1 week ago

Selected Answer: B

Again, APs generate signals, SSIDs don't.

"This document describes how to configure authorization policies in Cisco Identity Services Engine (ISE) to distinguish between different service set identifiers (SSIDs)."

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115734-ise-policies-ssid-00.html>

upvoted 1 times

 **Stevens0103** 1 month, 1 week ago

Since SSID can be used with or without policies, option C. seems to become the only possible answer to the question, which I reluctantly agree to.

upvoted 1 times

 **Bhrino** 4 months 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 3 times

 **[Removed]** 2 months, 1 week ago

Exactly

upvoted 1 times

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**Correct Answer:**

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

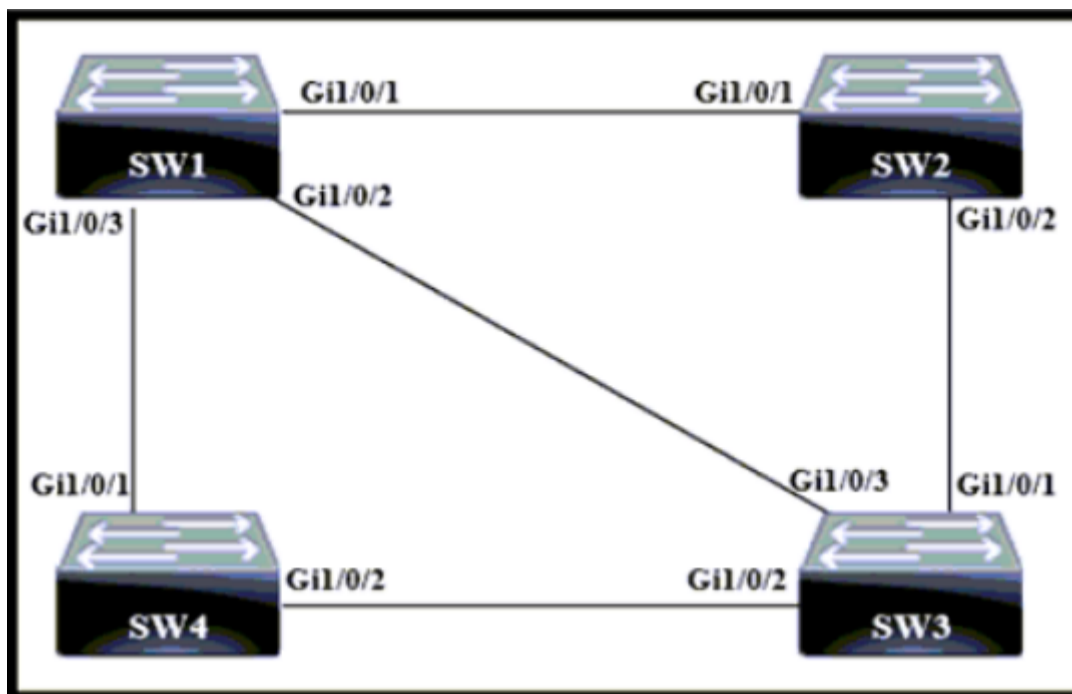
 **Bhrino** Highly Voted 4 months ago

give answer is correct

ff = multi
 2000 = global
 fc /fd = unique local
 fe8 = link local
 upvoted 8 times

 **[Removed]** Most Recent 2 months, 1 week ago

Given answers are correct
 upvoted 1 times



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 Highly Voted 4 months ago

The answer is D because this switch has the lowest priority and mac address
upvoted 7 times

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** Highly Voted 4 months ago

Selected Answer: B

The answer is because it has the lowest ad and metric
upvoted 6 times

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

Selected Answer: B

Select the answer with lowest Administrative distance when comparing two different routing protocols. Select the lowest metric when comparing two routes learned from same routing protocols.
upvoted 5 times

 **Yannik123** Most Recent 1 day, 16 hours ago

Selected Answer: B


Given answer is correct. Lowest AD an Metric = Winning Route
upvoted 1 times

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** Highly Voted 4 months ago

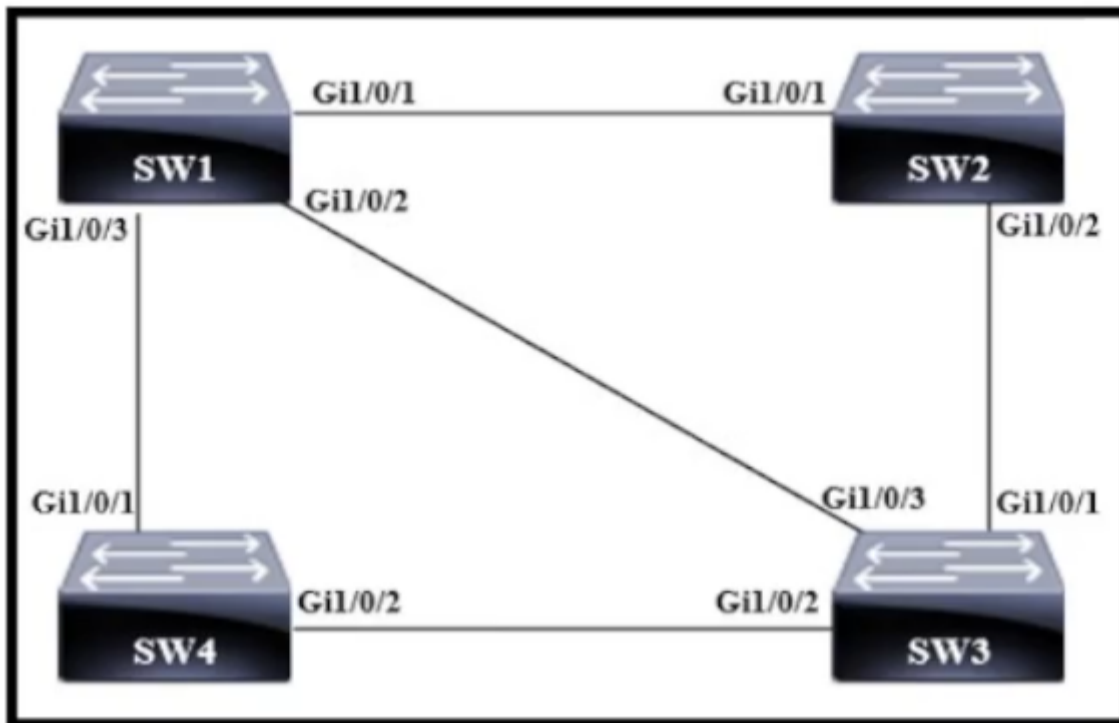
Selected Answer: C

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 5 times

 **[Removed]** Most Recent 2 months, 1 week ago

Selected Answer: C

C. value
"key": "value"
{ } = object
[] = array
upvoted 2 times



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 Highly Voted 3 months, 2 weeks ago

Selected Answer: C

Answer is correct, lowest priority, and lowest MAC address
upvoted 10 times

[Removed] 2 months, 2 weeks ago

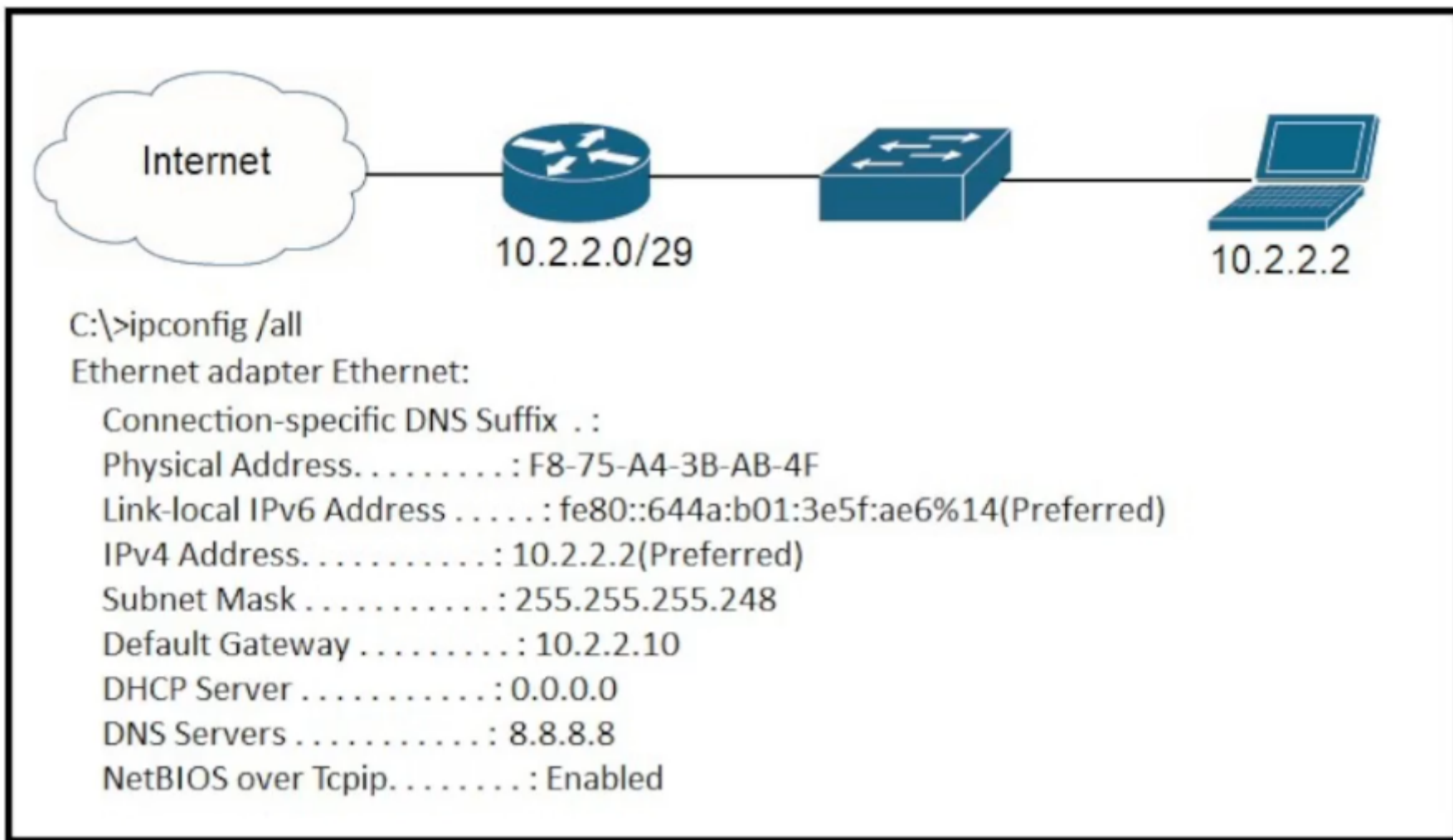
Exactly
upvoted 1 times

[Removed] Most Recent 2 months, 2 weeks ago

Selected Answer: C

C. SW 3 -

Bridge Priority - 32768 -
mac-address 01:1c:6c:66:b7:70
upvoted 1 times



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 Highly Voted 3 months, 2 weeks 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 7 times

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
	has a core diameter of 9 microns
	uses a single wavelength of light

 **learntstuff** 1 month, 3 weeks ago

Answer is Correct
upvoted 2 times

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

 **NeoSam999** 2 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 3 times

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	Anycast
cannot be used as a source address	
is routed to the nearest interface that has the address	Multicast
provides one-to-many communications	

Correct Answer:

is assigned to multiple devices on the same network simultaneously	Anycast
cannot be used as a source address	
is routed to the nearest interface that has the address	Multicast
provides one-to-many communications	

studying_1 Highly Voted 3 months, 2 weeks 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 20 times

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

 **NeoSam999** 2 months, 2 weeks ago

Selected Answer: D

D is the correct answer.

SSID (Service Set Identifier) is a unique name that is assigned to a wireless network .

upvoted 2 times

 **Stevens0103** 1 month, 1 week ago

SSID (Service Set Identifier) is a unique name that is assigned to the AP.

A WLAN's name is assigned by the network administrator and can be different from the APs connected to it.

upvoted 1 times

 **Stevens0103** 1 month, 1 week ago

"The SSID is a unique identifier that 'wireless network devices' use to establish and maintain wireless connectivity."

<https://www.cisco.com/c/en/us/support/docs/interfaces-modules/security-modules-routers-switches/116586-config-ap-00.html>

upvoted 1 times

 **Stevens0103** 1 month, 1 week ago

I admit that I was wrong cause APs can be named the same. That leaves option D. the only choice that I reluctantly agree to. Poorly worded question.

upvoted 2 times

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

 **NeoSam999** 2 months, 2 weeks ago

Selected Answer: C

It is a key-value pair where the key is "port," and the associated value is "te8/30."

upvoted 3 times

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 <div style="background-color: #fff9c4; height: 20px; margin-bottom: 5px;"></div> <div style="background-color: #fff9c4; height: 20px; margin-bottom: 5px;"></div>
It restricts the CLI commands that a user is able to perform.	
It performs user validation via TACACS+.	Authorization <div style="background-color: #fff9c4; height: 20px; margin-bottom: 5px;"></div> <div style="background-color: #fff9c4; height: 20px; margin-bottom: 5px;"></div>
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 <div style="background-color: #e0f7fa; padding: 5px; margin-bottom: 5px;">It records the duration of each connection.</div> <div style="background-color: #e0f7fa; padding: 5px; margin-bottom: 5px;">It supports User Access Reporting.</div>
It restricts the CLI commands that a user is able to perform.	
It performs user validation via TACACS+.	Authorization <div style="background-color: #e0f7fa; padding: 5px; margin-bottom: 5px;">It grants access to network assets, such as FTP servers.</div> <div style="background-color: #e0f7fa; padding: 5px; margin-bottom: 5px;">It restricts the CLI commands that a user is able to perform.</div>
It records the duration of each connection.	
It supports User Access Reporting.	
It verifies "who you are".	

 **learntstuff** 1 month, 3 weeks ago

Answer is Correct
upvoted 2 times

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

  **dropspablo** 1 month, 3 weeks ago

ChatGPT

Based on the provided output, it appears that option C. "duplex mismatch" is occurring in the interface condition. The line "Half-duplex, 100 Mb/s, 100BaseTX/FX" indicates that the interface is set to half-duplex mode, but the interface is also capable of 100 Mb/s speed. This is a mismatch between the duplex settings on both ends of the link, which can lead to various performance and connectivity issues.

upvoted 1 times

  **dropspablo** 1 month, 3 weeks ago


Disregard my answer above as interface speed doesn't matter in this case. In fact, a possible duplex mismatch is shown due to 119 collisions, and because the interface is in Half-duplex mode, it would receive collisions. In this case, the other side would not count the collisions, as it would be full-duplex where it transmits and receives simultaneously.

upvoted 1 times

  **Stussy** 3 months, 1 week ago

A or C is was i meant to say, sorry

upvoted 1 times

  **Stussy** 3 months, 1 week ago

Could be A or D in my opinion. But im just going to suppose its asking "why".

upvoted 1 times

  **studying_1** 3 months, 2 weeks 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 4 times

 **dropspablo** 1 month, 3 weeks ago

I agree

upvoted 1 times

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

 **Dadits** 1 month, 3 weeks ago

Just finished them i think i have to remake the questons at least 2 times to have a clear view of it!anyone took the test recently?If yes did you found similar questions?

upvoted 1 times

 **no_blink404** 2 months, 2 weeks ago

Hey you! Congrats on reaching the last question as of July 1st 2023 :D

upvoted 2 times

 **[Removed]** 2 months, 1 week ago

Hey! The last question is 1138 :)

upvoted 1 times

 **MadKisa** 2 months, 2 weeks ago

Everyone's talking about labs on examtopics, but i cant find any, any help?

upvoted 1 times

 **mda2h** 1 month, 1 week ago


Check questions 1000 to 1100

upvoted 1 times

 **StingVN** 2 months, 2 weeks ago

thanks god im finish. its just like forever.
Good luck everyone in your future exams.
Love you all.

upvoted 3 times

 **nawzat** 2 months, 3 weeks ago

Answer is correct

upvoted 4 times

 **john1247** 3 months ago

I'm unemployed, but it took me a month to finish 1132 questions. Is CCNA a hazing?

upvoted 2 times

  **studying_1** 2 months, 4 weeks ago

sorry to hear that, i hope you find a job soon & pass the exam and get the certificate

upvoted 3 times

  **Trains** 2 months, 4 weeks ago



Not sure what you mean by a hazing, but it gets faster the more you know. I did this in 2 days (while on a full time job) after a few months of study, but if I did it at the start it would've taken way longer. Just keep practicing. It'll be rough but it def gets easier

upvoted 2 times

  **studying_1** 3 months, 2 weeks ago

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

upvoted 2 times

  **Dunedrifter** 2 months, 3 weeks ago

I'm doing it in reverse lol. Just finished my first page. ;)

upvoted 1 times

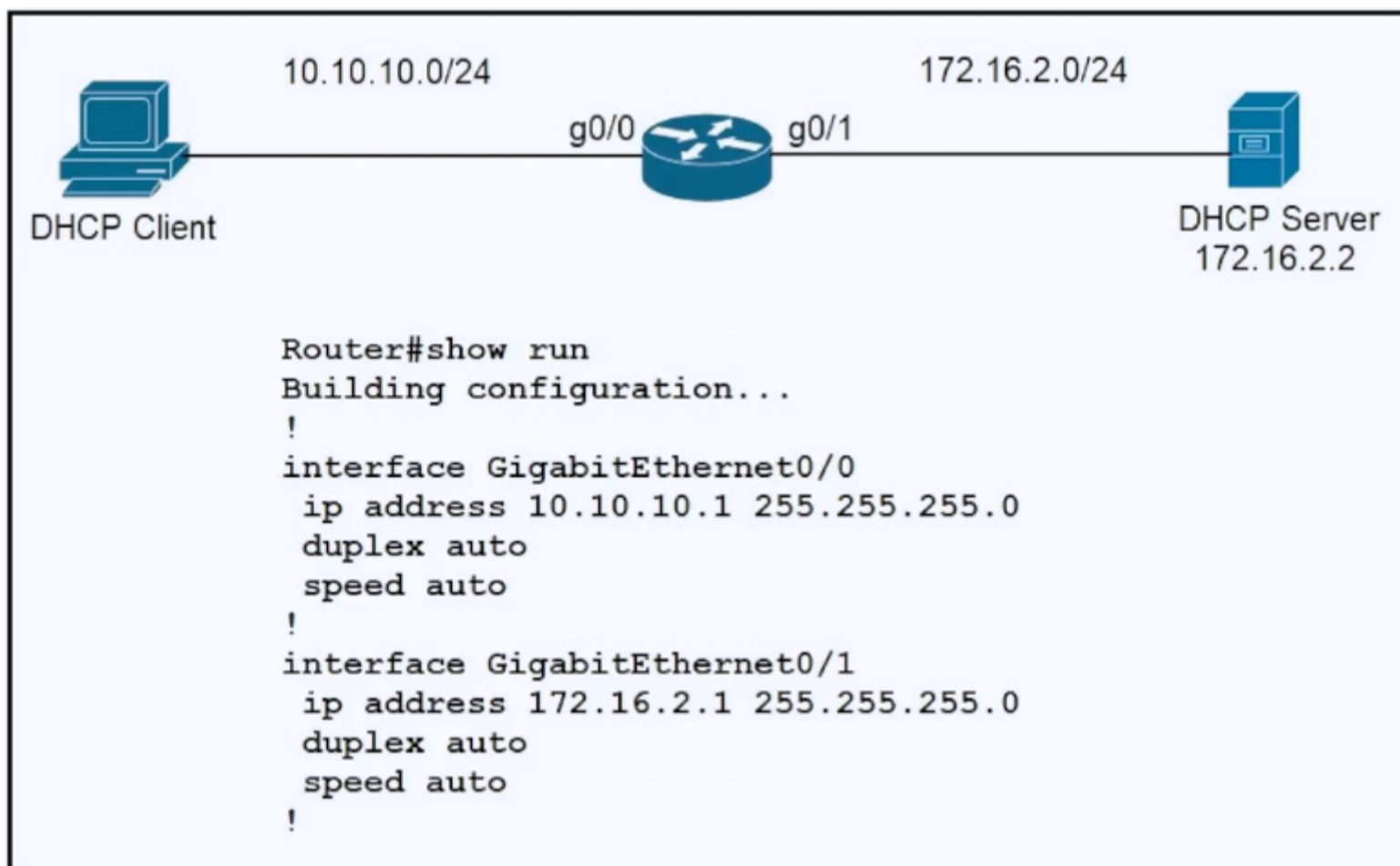
  **ananinamia** 2 weeks, 3 days ago

lol and lol

upvoted 1 times

Question #1133

Topic 1



Refer to the exhibit. An engineer is configuring a new router on the network and applied this configuration. Which additional configuration allows the PC to obtain its IP address from a DHCP server?

- A. Configure the ip helper-address 172.16.2.2 command under interface Gi0/0.
- B. Configure the ip dhcp relay information command under interface Gi0/1
- C. Configure the ip address dhcp command under interface Gi0/0
- D. Configure the ip dhcp smart-relay command globally on the router.

Correct Answer: A

SIMULATION

-

Guidelines

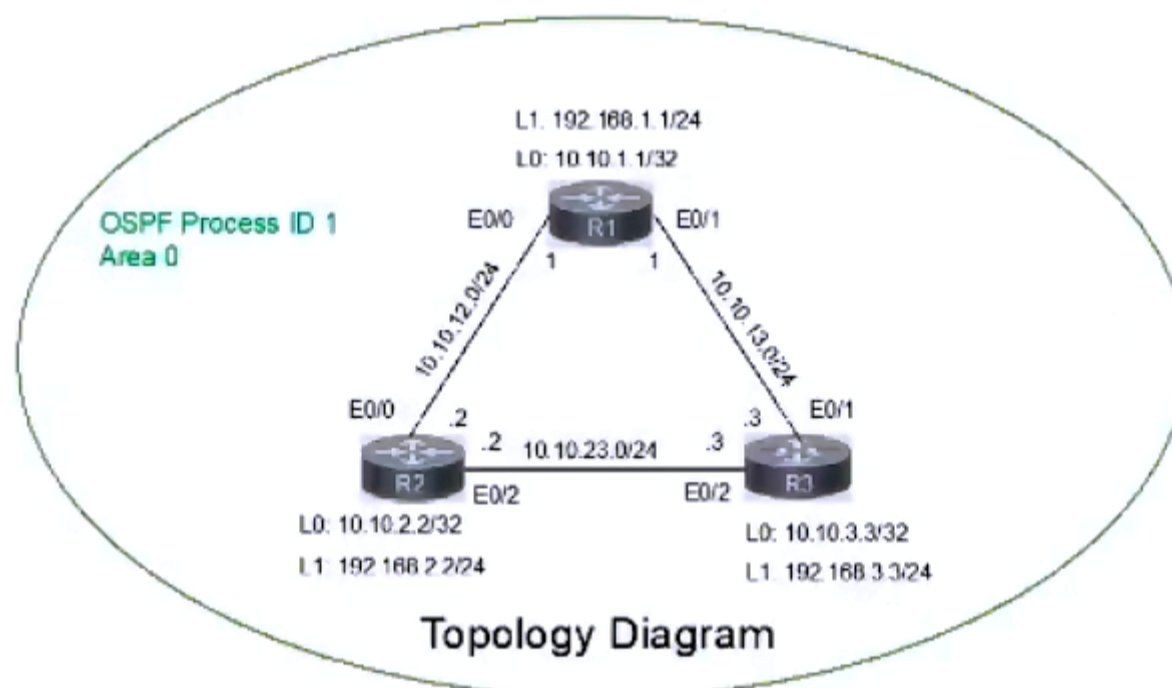
-

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 between the three routers is configured. OSPF adjacencies must be established.

1. Configure R1 and R2 Router IDs using the interface IP addresses from the link that is shared between them.
2. Configure the R2 links with a max value facing R1 and R3. R2 must become the DR. R1 and R3 links facing R2 must remain with the default OSPF configuration for DR election. Verify the configuration after clearing the OSPF process.
3. Using a host wildcard mask, configure all three routers to advertise their respective Loopback1 networks.

4. Configure the link between R1 and R3 to disable their ability to add other OSPF routers.



R1

```
conf terminal
interface Loopback0
ip address 10.10.1.1 255.255.255.255
!
interface Loopback1
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/0
no shut
ip address 10.10.12.1 255.255.255.0
ip ospf 1 area 0
duplex auto
!
interface Ethernet0/1
no shut
ip address 10.10.13.1 255.255.255.0
ip ospf 1 area 0
duplex auto
!
router ospf 1
router-id 10.10.12.1
network 10.10.1.1 0.0.0.0 area 0
network 192.168.1.0 0.0.0.255 area 0
!
copy run star
```

R2

```
conf terminal
interface Loopback0
ip address 10.10.2.2 255.255.255.255
!
interface Loopback1
ip address 192.168.2.2 255.255.255.0
!
interface Ethernet0/0
no shut
ip address 10.10.12.2 255.255.255.0
ip ospf priority 255
ip ospf 1 area 0
duplex auto
!
interface Ethernet0/2
no shut
ip address 10.10.23.2 255.255.255.0
ip ospf priority 255
ip ospf 1 area 0
duplex auto
!
router ospf 1
network 10.10.2.2 0.0.0.0 area 0
network 192.168.2.0 0.0.0.255 area 0
!
copy runs start
```

Correct Answer:

R3

```
conf ter
interface Loopback0
ip address 10.10.3.3 255.255.255.255
!
interface Loopback1
ip address 192.168.3.3 255.255.255.0
!
interface Ethernet0/1
no shut
ip address 10.10.13.3 255.255.255.0
ip ospf 1 area 0
```

```
ip ospf 1 area 0
duplex auto
!
interface Ethernet0/2
no shut
ip address 10.10.23.3 255.255.255.0
ip ospf 1 area 0
duplex auto
!
router ospf 1
network 10.10.3.3 0.0.0.0 area 0
network 192.168.3.0 0.0.0.255 area 0
!
copy run start
!
```

 **kappi91** 1 week, 4 days ago

Can somebody give me some feedback:

Step 1 -----

```
R1
router ospf 1
router-id 10.10.12.1
```

```
R2
router ospf 1
router-id 10.10.12.2
```

Step 2 -----

```
int e0/0
ip ospf priority 255
int e0/2
ip ospf priority 255
exit
clear ip ospf process
show ip ospf neighbors
```

Step 3 -----

```
r1
router ospf 1
network 10.10.1.1 0.0.0.0 area 0
```

```
r2
router ospf 1
network 10.10.1.2 0.0.0.0 area 0
```

```
r3
router ospf 1
network 10.10.1.3 0.0.0.0 area 0
```

Step 4 -----

```
r1
int e0/1
ip ospf network point-to-point
```

```
r3
int e0/1
ip ospf network point-to-point
upvoted 1 times
```


DRAG DROP

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

Answer Area

- is assigned to more than one interface
- cannot be used as a source address
- is used exclusively by a non-host device
- provides one-to-many communications

Anycast

[Empty box]

[Empty box]

Multicast

[Empty box]

[Empty box]

Correct Answer:

Answer Area

Anycast

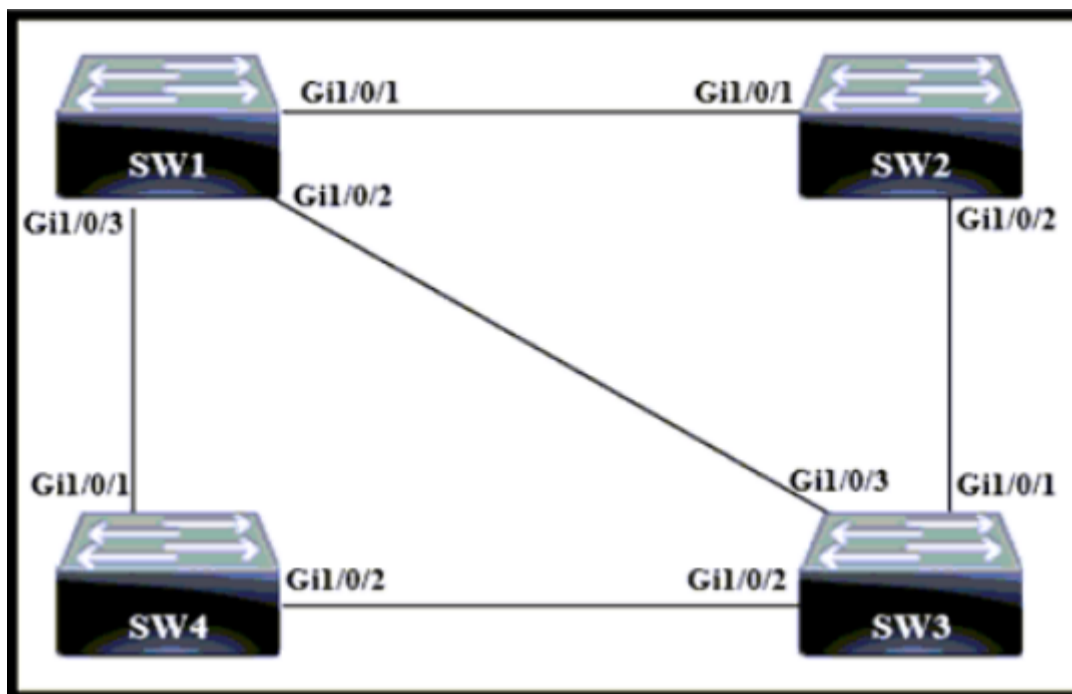
- is assigned to more than one interface
- is used exclusively by a non-host device

Multicast

- provides one-to-many communications
- cannot be used as a source address

 **shaney67** 6 days, 1 hour ago

I think this may be wrong? i dont think multicast or anycast can be used as a source address?
upvoted 1 times



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

A. SW4 -

Bridge Priority - 8192 -
mac-address 05:4a:f7:06:33:22

B. SW2 -

Bridge Priority - 8192 -
mac-address 05:52:bd:0c:be:69

C. SW3 -

Bridge Priority - 61440 -
mac-address 06:15:2e:7f:20:58

D. SW4 -

Bridge Priority - 61440 -
mac-address 0a:e5:03:a6:6e:37

Correct Answer: A

DRAG DROP

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

Answer Area

- contains a conductor, bedding, and sheathing
- is ideal over longer distances with little loss of integrity
- is typically used in small office applications
- uses a single wavelength of light

copper

single mode fiber

Correct Answer:

Answer Area

copper

uses a single wavelength of light

is ideal over longer distances with little loss of integrity

single mode fiber

contains a conductor, bedding, and sheathing

is typically used in small office applications

- Cisco3900** 1 week, 2 days ago
Both Copper and fiber answers need to be flipped to be correct.
upvoted 2 times
- shaney67** 1 week, 3 days ago
This has been answered back to front
upvoted 1 times

What is a characteristic of encryption in wireless networks?

- A. provides increased protection against spyware
- B. uses policies to prevent unauthorized users
- C. converts electrical current to radio waves
- D. prevents the interception of data as it transits a network

Correct Answer: D

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

- D 10.214.247.237.28 [90/2170] via G0/12
- D 10.214.247.237.28 [90/46985] via G0/19
- O 10.214.247.237.28 [110/665] via G0/9
- O 10.214.247.237.28 [110/3399] via G0/1

- A. G0/9
- B. G0/12
- C. G0/19
- D. G0/1

Correct Answer: B

Which IPsec encryption mode is appropriate when the destination of a packet differs from the security termination point?

- A. transport
- B. main
- C. aggressive
- D. tunnel

Correct Answer: D

A network administrator is evaluating network security in the aftermath of an attempted ARP spoofing attack. If Port-channel1 is the uplink interface of the access-layer switch toward the distribution-layer switch, which two configurations must the administrator configure on the access-layer switch to provide adequate protection? (Choose two.)

- A. ip dhcp snooping vlan 1-4094
!
interface Port-channel1
switchport protected
switchport port-security maximum 1
- B. ip dhcp snooping vlan 1-4094
ip dhcp snooping
!
interface Port-channel1
ip dhcp snooping trust
- C. ip dhcp snooping
!
interface Port-channel1
switchport port-security maximum 1
switchport port-security
- D. ip arp inspection trust
!
interface Port-channel1
switchport port-security maximum 4094
switchport port-security
ip verify source mac-check
- E. ip arp inspection vlan 1-4094
!
interface Port-channel1
ip arp inspection trust

Correct Answer: DE

Which type of hypervisor operates without an underlying OS to host virtual machines?

- A. Type 1
- B. Type 2
- C. Type 3
- D. Type 12

Correct Answer: A

What is a characteristic of an SSID in wireless networks?

- A. converts electrical current to radio waves
- B. associates a name to a WLAN
- C. uses a 4-way handshake for authentication
- D. provides increased protection against spyware

Correct Answer: B

DRAG DROP

-

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

has a unicast source sent to a group	Unique Local <div style="border: 1px solid black; height: 20px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; height: 20px;"></div>
is unable to route on the internet	
allows sites to be combined without address conflicts	Multicast <div style="border: 1px solid black; height: 20px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; height: 20px;"></div>
sends packets to a group address rather than a single address	

Correct Answer:

Unique Local <div style="border: 1px solid black; padding: 5px; text-align: center;">is unable to route on the internet</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">allows sites to be combined without address conflicts</div>
Multicast <div style="border: 1px solid black; padding: 5px; text-align: center;">has a unicast source sent to a group</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">sends packets to a group address rather than a single address</div>

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

```
D 10.148.172.22.27 [90/10259] via G0/24
D 10.148.172.22.27 [90/47955] via G0/10
R 10.148.172.22.27 [120/14] via G0/5
R 10.148.172.22.27 [120/1] via G0/1
```

- A. G0/10
- B. G0/24
- C. G0/5
- D. G0/1

Correct Answer: B

What is a characteristic of private IPv4 addressing?

- A. enables secure connectivity over the internet
- B. complies with PCI regulations
- C. provides an added level of protection against internet threats
- D. is used on internal hosts that stream data solely to external resources

Correct Answer: C

DRAG DROP

-

Drag and drop the traffic types from the left onto the QoS delivery mechanisms on the right.

Answer Area

database synchronization traffic

best effort

standard Web browsing traffic

policing

video traffic

priority queue

VoIP traffic

shaping

Answer Area**Correct Answer:**

standard Web browsing traffic

video traffic

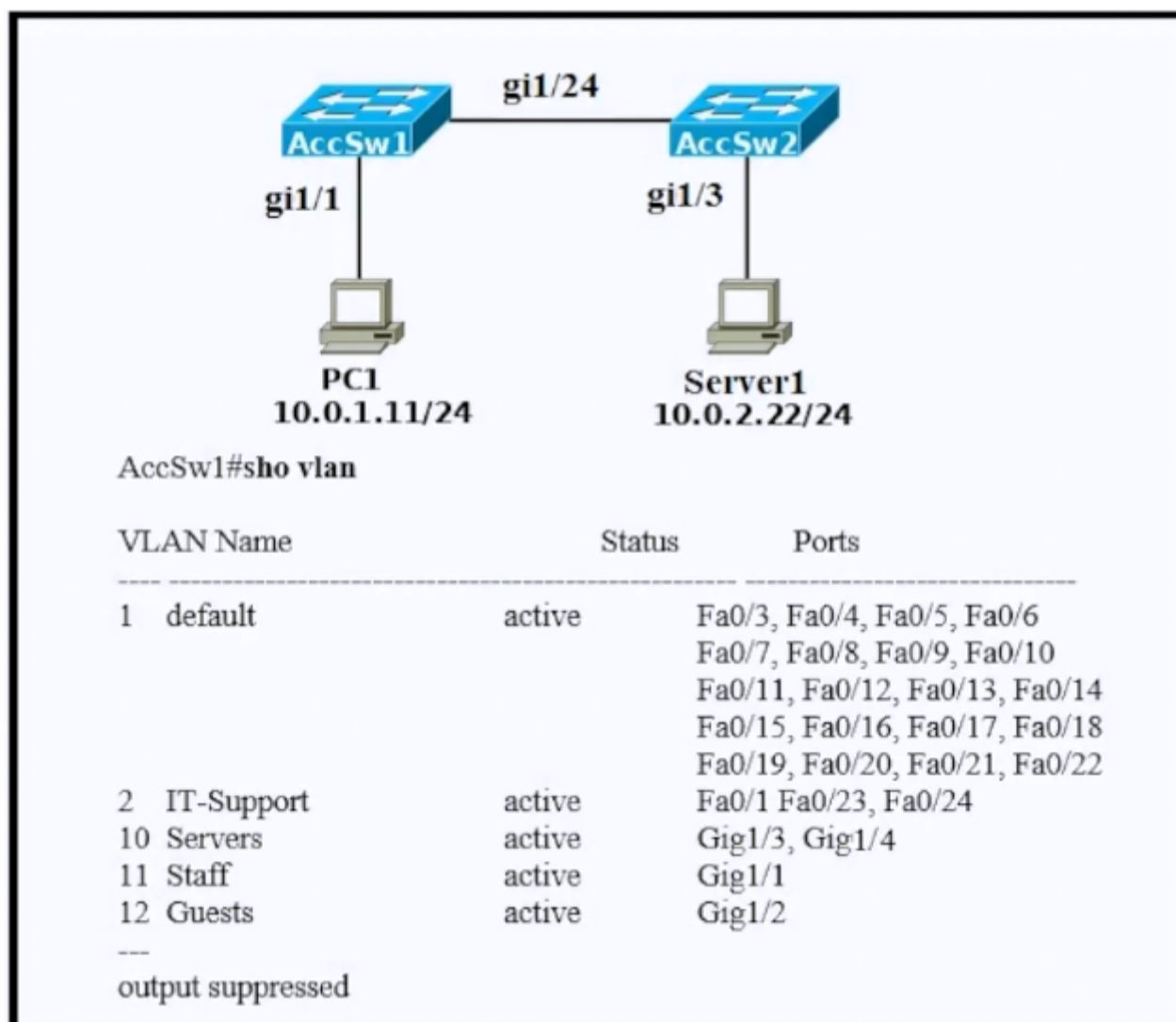
database synchronization traffic

VoIP traffic

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. is used on hosts that communicate only with other internal hosts


Correct Answer: D



Refer to the exhibit. The engineer configured the VLANs on the new AccSw2 switch. A router-on-a-stick is connected to both switches. How must the ports be configured on AccSw2 to establish full connectivity between the two switches and for Server1?

- A. interface GigabitEthernet1/1
switchport access vlan 11
!
interface GigabitEthernet1/24
switchport mode trunk
switchport trunk allowed vlan 10,11
- B. interface GigabitEthernet1/3
switchport mode access
switchport access vlan 10
!
interface GigabitEthernet1/24
switchport mode trunk
switchport trunk allowed vlan 2,10
- C. interface GigabitEthernet1/3
switchport mode access
switchport access vlan 10
!
interface GigabitEthernet1/24
switchport mode trunk
- D. interface GigabitEthernet1/1
switchport mode access
switchport access vlan 11
!
interface GigabitEthernet1/24
switchport mode trunk

Correct Answer: C

 **kat1969** 18 hours, 24 minutes ago

We don't know what VLAN the PC belongs to. So, if we restrict the VLANS that might create an issue.
upvoted 1 times

 **Cisco3900** 1 week, 2 days ago

Correct me if I'm wrong, but I think it's B.
upvoted 3 times

Question #1150

Topic 1

How does frame switching function on a switch?

- A. floods unknown destinations to all ports except the receiving port
- B. modifies frames that contain a known source VLAN
- C. rewrites the source and destination MAC address
- D. buffers and forwards frames with less than 5 CRCs

Correct Answer: A

Question #1151

Topic 1

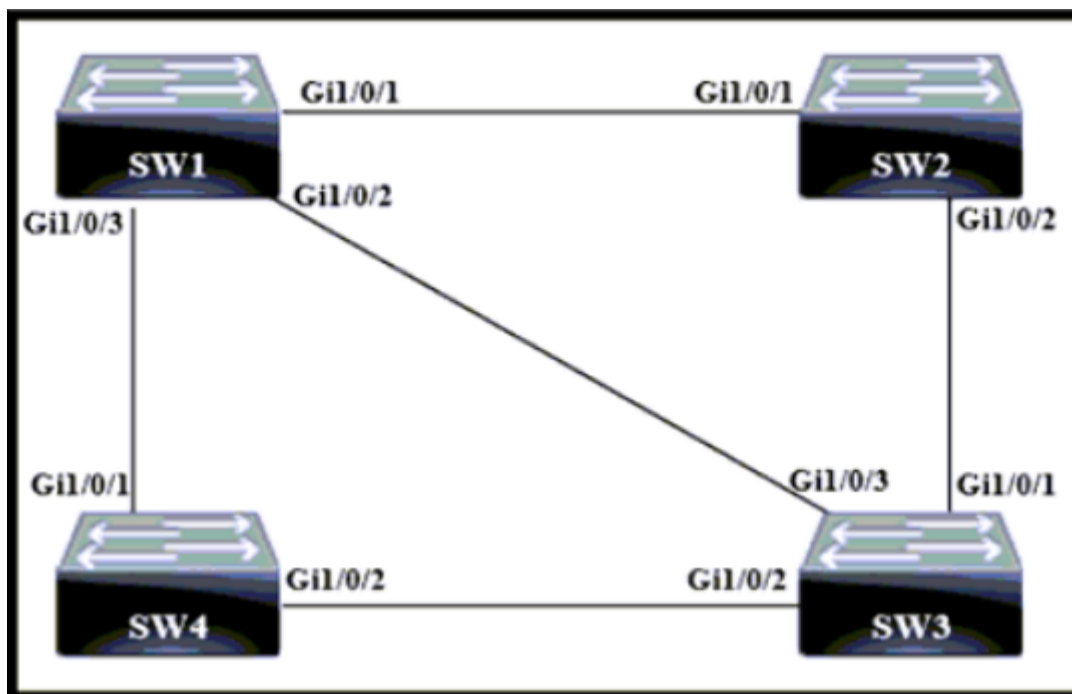
Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix  :  
Description . . . . . : Intel(R) Dual Band Wireless-AC 7265  
Physical Address. . . . . : C8-21-58-B4-D3-E0  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . : Yes  
Link-local IPv6 Address . . . . : fe80::45a1:b3fa:2f37:bf37%2 (Preferred)  
IPv4 Address. . . . . : 192.168.25.103 (Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Lease Obtained. . . . . : June 11, 2019 10:21:31 AM  
Lease Expires . . . . . : June 12, 2019 10:21:36 AM  
Default Gateway . . . . . : 192.168.25.1  
DHCP Server . . . . . : 192.168.25.100  
DHCPv6 IAID . . . . . : 46670168  
DHCPv6 Client DUID. . . . . : 00-01-00-01-20-FF-05-55-3C-52-82-33-D3-84  
DNS Servers . . . . . : 192.168.25.254  
                          192.168.25.254
```

Refer to the exhibit. Which address will the client contact to renew their IP address when the current lease expires?

- A. 192.168.25.103
- B. 192.168.25.1
- C. 192.168.25.100
- D. 192.168.25.254

Correct Answer: C



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

A. SW4 -

Bridge Priority - 8192 -
mac-address 05:0f:e8:ed:b2:98

B. SW2 -

Bridge Priority - 8192 -
mac-address 00:ac:f0:9b:dc:72

C. SW3 -

Bridge Priority - 16384 -
mac-address 0e:6c:e4:b1:8a:57

D. SW4 -

Bridge Priority - 16384 -
mac-address 0a:45:22:26:29:77

Correct Answer: B

DRAG DROP

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

Answer Area

contains a conductor, bedding, and sheathing	copper
is typically used for DWDM optical systems spanning long distances	
is typically used in small office applications	single-mode fiber
eliminates distortion from overlapping light pulses	

Correct Answer:

Answer Area

contains a conductor, bedding, and sheathing	copper
is typically used in small office applications	
is typically used for DWDM optical systems spanning long distances	single-mode fiber
eliminates distortion from overlapping light pulses	

How is a configuration change made to a wireless AP in lightweight mode?

- A. SSH connection to the management IP of the AP
- B. CAPWAP/LWAPP connection via the parent WLC
- C. EoIP connection via the parent WLC
- D. HTTPS connection directly to the out-of-band address of the AP

Correct Answer: B

DRAG DROP

-

Drag and drop the HTTP verbs from the left onto the API operations on the right.

Answer Area

DELETE	creates a subordinate resource under the specified URI
GET	erases a specific resource
PATCH	fully replaces the current version of a specific resource with new content from the payload
POST	partially modifies a specific resource
PUT	requests specific information about a resource

Correct Answer:**Answer Area**

POST
DELETE
PUT
PATCH
GET

Which plane is centralized in software-defined networking?

- A. application
- B. services
- C. data
- D. control

Correct Answer: D

What is a service that is provided by a wireless controller?

- A. It mitigates threats from the internet.
- B. It manages interference in a dense network.
- C. It provides Layer 3 routing between wired and wireless devices.
- D. It issues IP addresses to wired devices.

Correct Answer: B

When more than one AP-Manager interface is provisioned on a wireless LAN controller, how is the request handled by the AP?

- A. The discovery response from the AP to the AP-Manager interface disables the WLAN port.
- B. The AP join request fails and must be configured statically on the AP-Manager interface.
- C. The AP-Manager with the fewest number of APs is used by the AP to join.
- D. The first AP-Manager interface to respond is chosen by the AP.

Correct Answer: C

What is represented in line 2 within this JSON schema?

```
1 [  
2 {"load balancer": "LB48", "port": "e0/27"},  
3 {"firewall": "FW49", "port": "ge2/37"},  
4 {"router": "R_paris", "port": "te6/6"},  
5 ]
```

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

Correct Answer: A

How does MAC learning function on a switch?

- A. protects against denial of service attacks
- B. sends frames with unknown destinations to a multicast group
- C. adds unknown source MAC addresses to the address table
- D. sends a retransmission request when a new frame is received

Correct Answer: C

What is represented by the word "ge3/36" within this JSON schema?

```
1 [  
2 {"VPN concentrator": "VPN36", "interface": "ge3/36"},  
3 {"load balancer": "LB33", "interface": "te7/10"},  
4 {"switch": "SW31", "interface": "fe2/25"},  
5 ]
```

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

Correct Answer: A



Which SNMP message type is reliable and precedes an acknowledgment response from the SNMP manager?

- A. Get
- B. Inform
- C. Traps
- D. Set

Correct Answer: B

  **Cisco3900** 1 week, 2 days ago

Correct me if I'm wrong, but I think it's trap
upvoted 1 times

  **kat1969** 18 hours, 31 minutes ago

nformRequest –

It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to send trap message continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn't provide.

upvoted 1 times