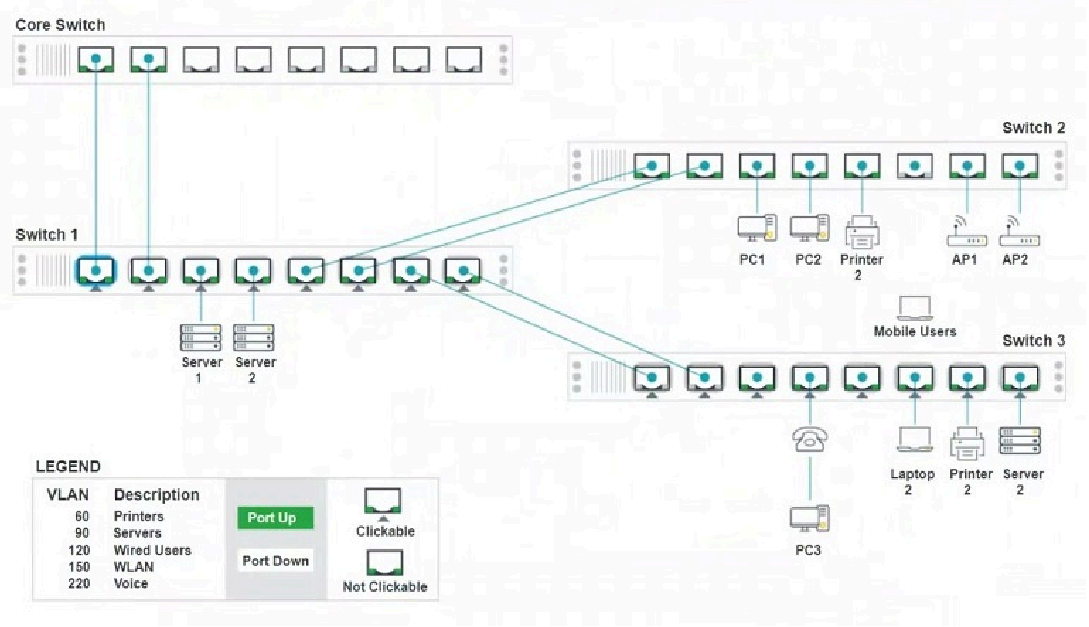
Question #1 *Topic 1*

SIMULATION -

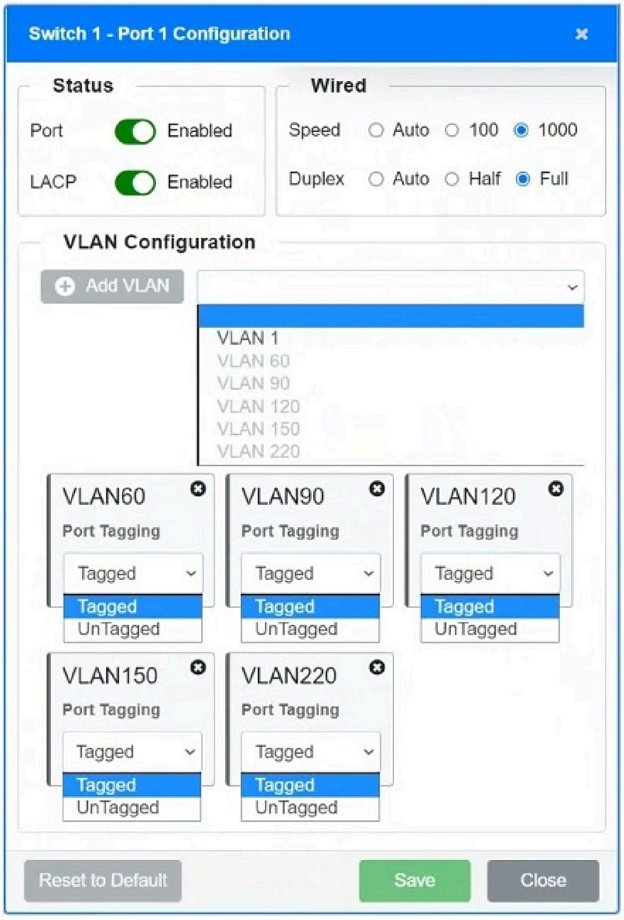
A network technician replaced an access layer switch and needs to reconfigure it to allow the connected devices to connect to the correct networks.

INSTRUCTIONS -

Click on the appropriate port(s) on Switch 1 and Switch 3 to verify or reconfigure the correct settings:
Ensure each device accesses only its correctly associated network.
Disable all unused switchports.
Require fault-tolerant connections between the switches.
Only make necessary changes to complete the above requirements.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



VLAN	Description
60	Printers
90	Servers
120	Wired Users
150	WLAN
220	Voice



Switch 1 - Port 1 Configuration

Status

Port: Enabled

LACP: Enabled

Wired

Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

VLAN Configuration

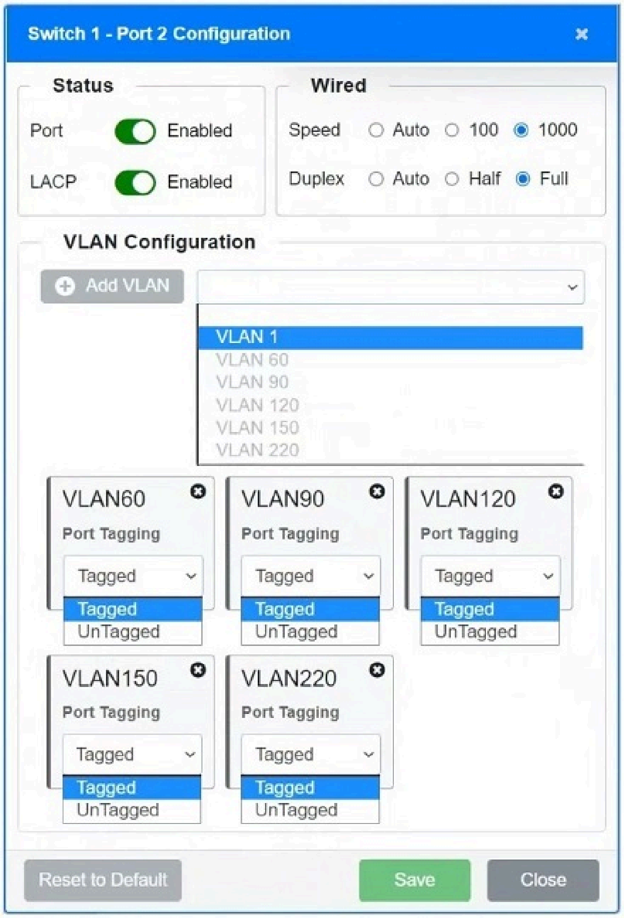
VLAN60 Port Tagging: Tagged

VLAN90 Port Tagging: Tagged

VLAN120 Port Tagging: Tagged

VLAN150 Port Tagging: Tagged

VLAN220 Port Tagging: Tagged



Switch 1 - Port 2 Configuration

Status

Port: Enabled

LACP: Enabled

Wired

Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

VLAN Configuration

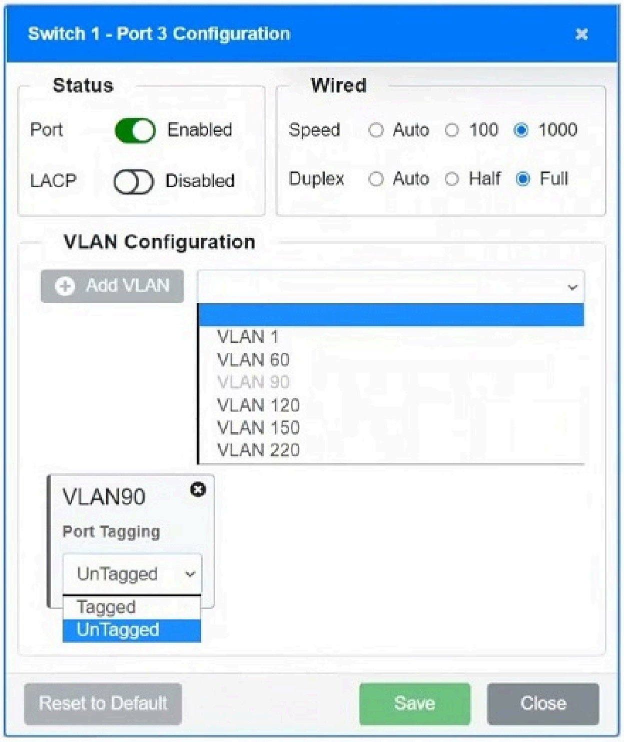
VLAN60 Port Tagging: Tagged

VLAN90 Port Tagging: Tagged

VLAN120 Port Tagging: Tagged

VLAN150 Port Tagging: Tagged

VLAN220 Port Tagging: Tagged



Switch 1 - Port 3 Configuration ×

Status

Port Enabled

LACP Disabled

Wired

Speed ○ Auto ○ 100 ● 1000

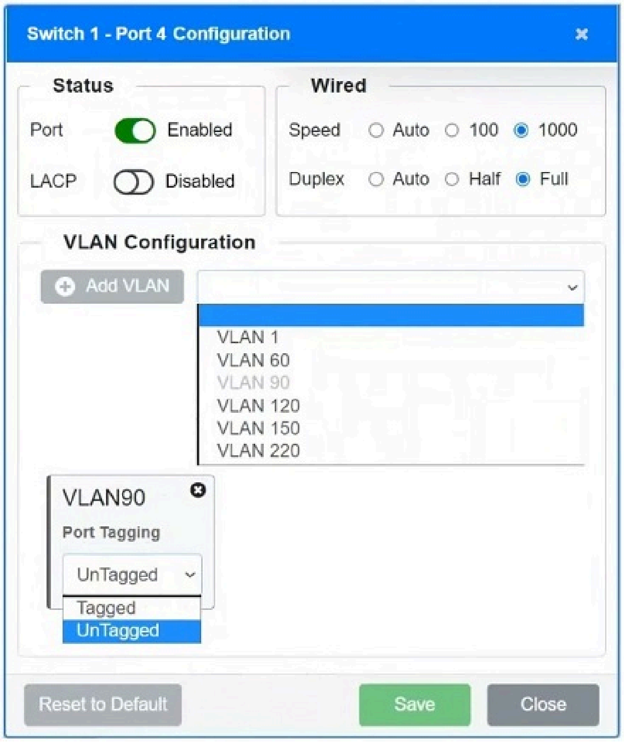
Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN90

Port Tagging

UnTagged



Switch 1 - Port 4 Configuration ×

Status

Port Enabled

LACP Disabled

Wired

Speed ○ Auto ○ 100 ● 1000

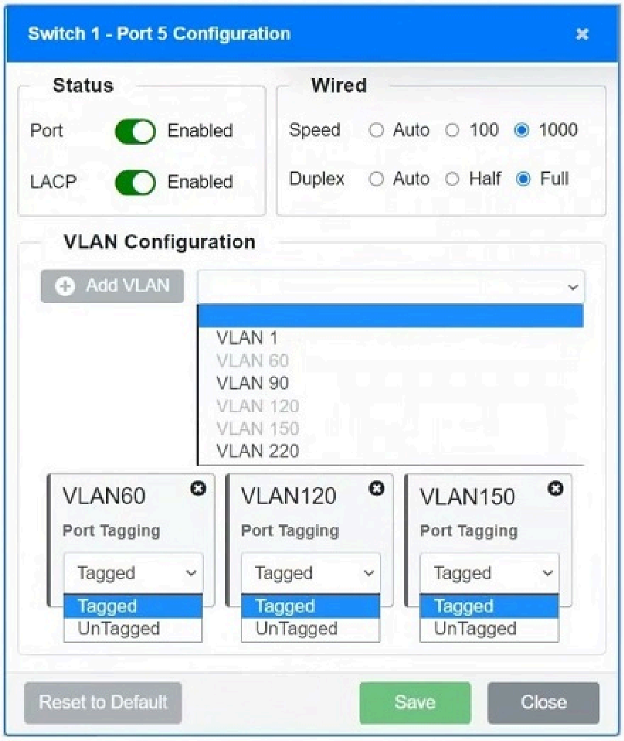
Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN90

Port Tagging

UnTagged



Switch 1 - Port 5 Configuration

Status

Port: Enabled

LACP: Enabled

Wired

Speed ○ Auto ○ 100 ● 1000

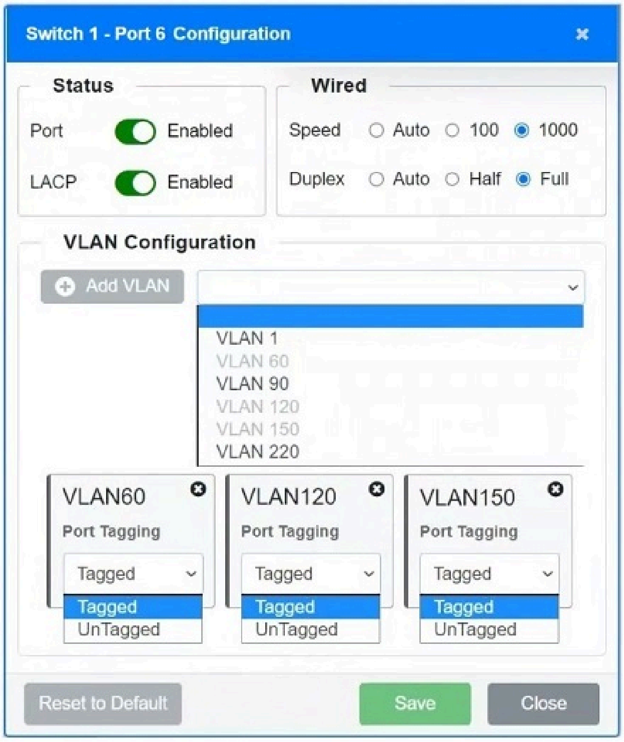
Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN60 — Port Tagging: Tagged

VLAN120 — Port Tagging: Tagged

VLAN150 — Port Tagging: Tagged



Switch 1 - Port 6 Configuration

Status

Port: Enabled

LACP: Enabled

Wired

Speed ○ Auto ○ 100 ● 1000

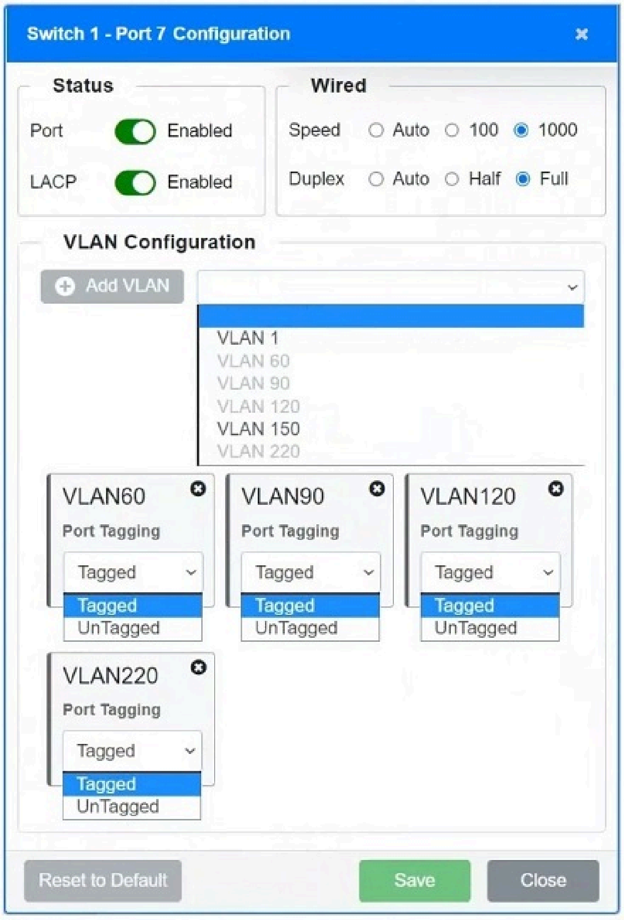
Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN60 — Port Tagging: Tagged

VLAN120 — Port Tagging: Tagged

VLAN150 — Port Tagging: Tagged


Switch 1 - Port 7 Configuration ×

Status

Port Enabled

LACP Enabled

Wired

Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

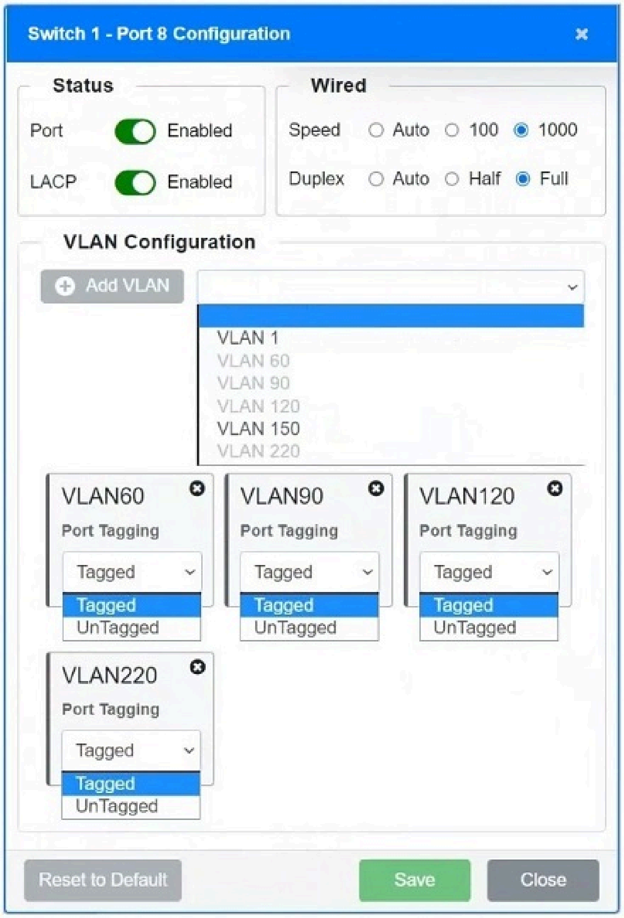
VLAN Configuration

VLAN60 Port Tagging: Tagged

VLAN90 Port Tagging: Tagged

VLAN120 Port Tagging: Tagged

VLAN220 Port Tagging: Tagged


Switch 1 - Port 8 Configuration ×

Status

Port Enabled

LACP Enabled

Wired

Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

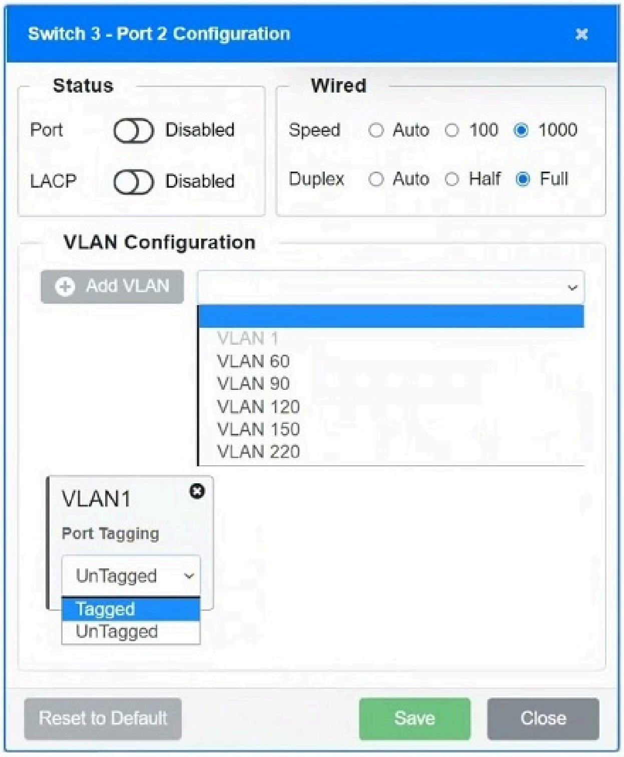
VLAN Configuration

VLAN60 Port Tagging: Tagged

VLAN90 Port Tagging: Tagged

VLAN120 Port Tagging: Tagged

VLAN220 Port Tagging: Tagged


Switch 3 - Port 2 Configuration

Status

Port ◯ Disabled

LACP ◯ Disabled

Wired

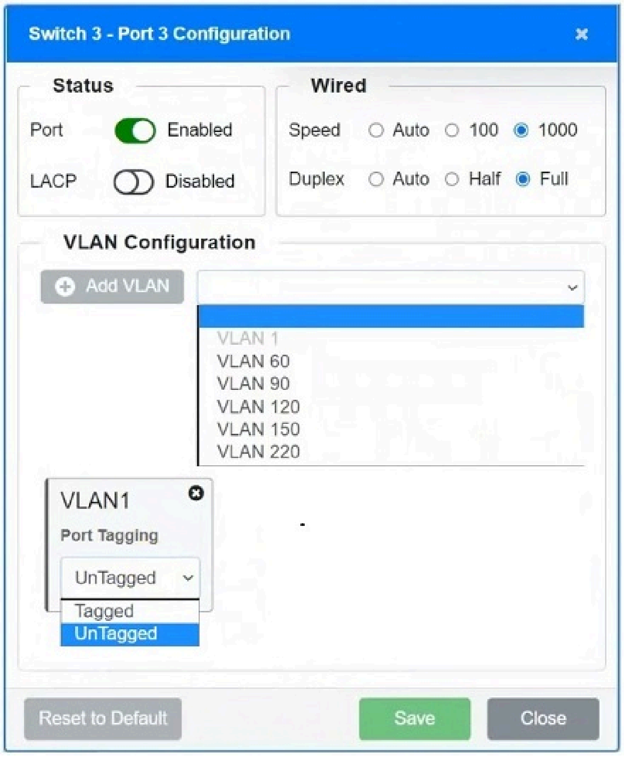
Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN1

Port Tagging: UnTagged


Switch 3 - Port 3 Configuration

Status

Port ● Enabled

LACP ◯ Disabled

Wired

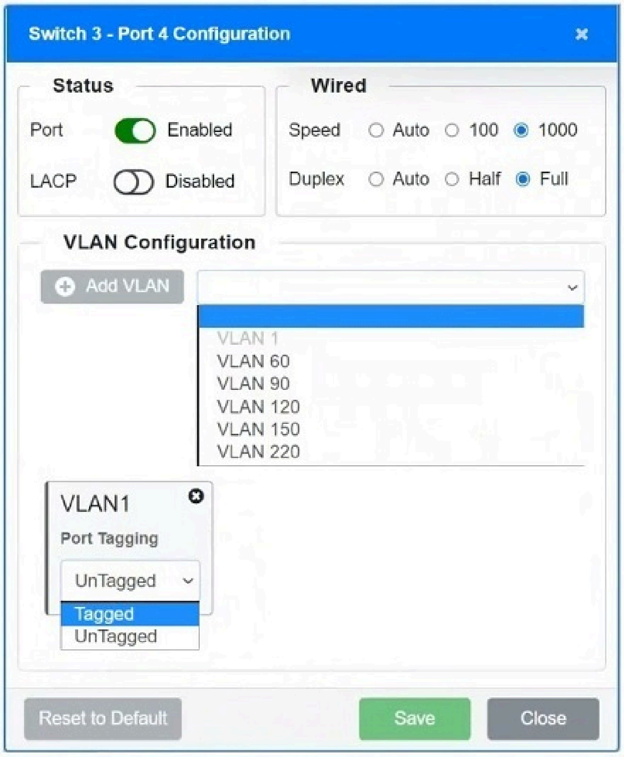
Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN1

Port Tagging: UnTagged



Switch 3 - Port 4 Configuration ×

Status

Port Enabled

LACP Disabled

Wired

Speed ○ Auto ○ 100 ● 1000

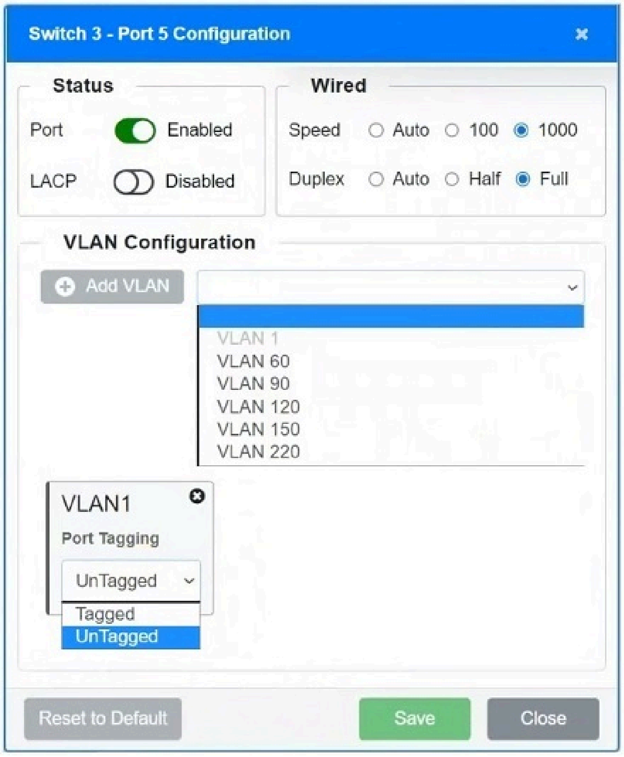
Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN1

Port Tagging

UnTagged



Switch 3 - Port 5 Configuration ×

Status

Port Enabled

LACP Disabled

Wired

Speed ○ Auto ○ 100 ● 1000

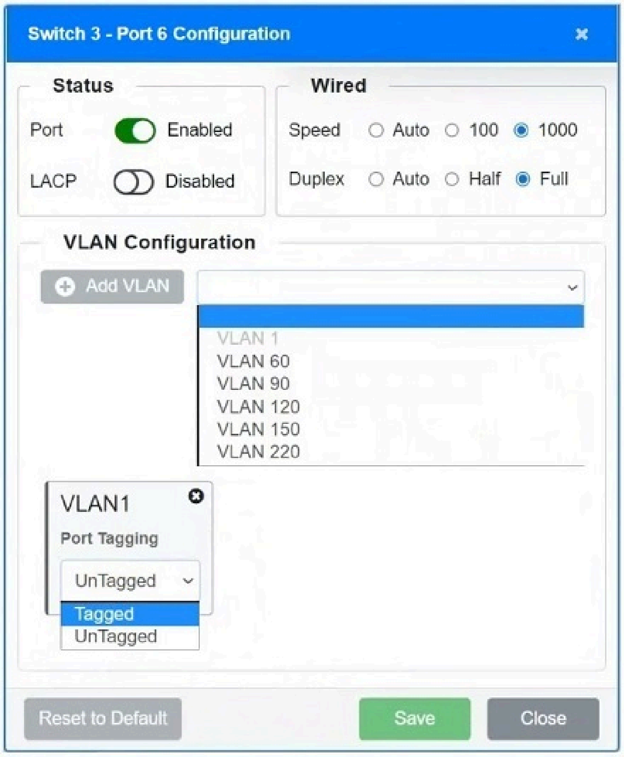
Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN1

Port Tagging

UnTagged



Switch 3 - Port 6 Configuration ×

Status

Port: Enabled

LACP: Disabled

Wired

Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

VLAN Configuration

Add VLAN

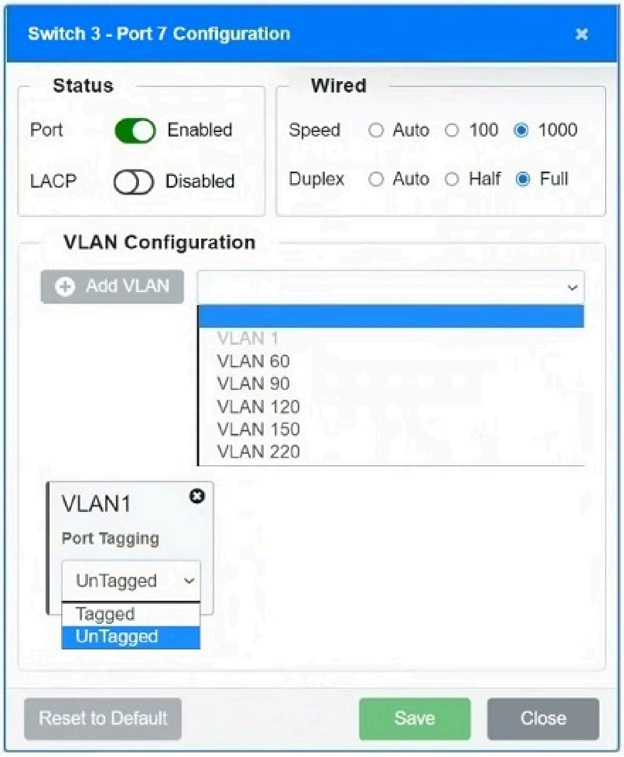
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220

VLAN1

Port Tagging: UnTagged

Tagged
UnTagged

Reset to Default | Save | Close



Switch 3 - Port 7 Configuration ×

Status

Port: Enabled

LACP: Disabled

Wired

Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

VLAN Configuration

Add VLAN

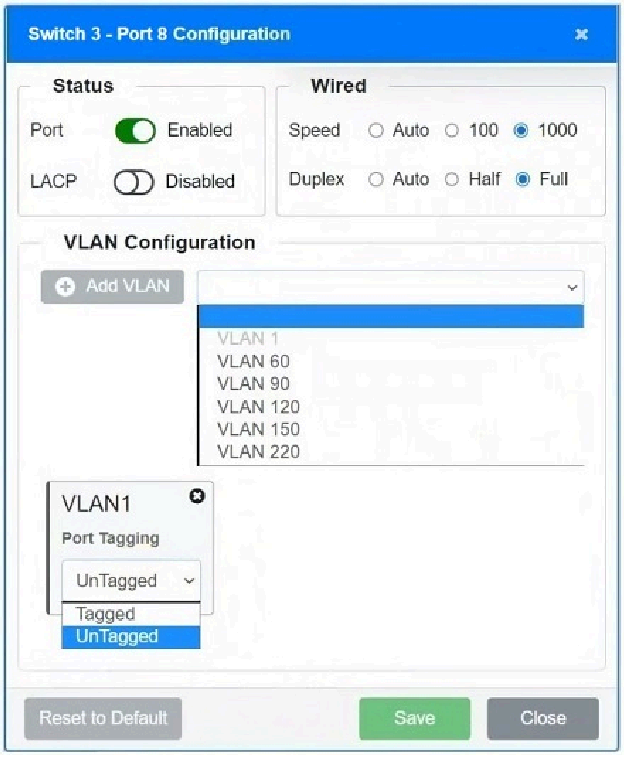
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220

VLAN1

Port Tagging: UnTagged

Tagged
UnTagged

Reset to Default | Save | Close



Switch 3 - Port 8 Configuration ×

Status

Port: Enabled

LACP: Disabled

Wired

Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN1

Port Tagging: UnTagged

Correct Answer:

Analysis and Configuration Recommendations:

Switch 1 Configurations:

- **Port 1 to Port 7**:
  - Ports should have VLANs set according to the devices they connect to. For instance, if a port is connecting to servers, only the VLAN for servers (e.g., VLAN 90) should be enabled and tagged if required.
  - Ensure unused VLANs are not active or set to untagged on these ports to prevent unauthorized network access.
- **Port 8**:
  - This port's configuration needs to align with the devices it connects to. Based on your first image, adjust the VLAN tagging accordingly. If it connects to printers, VLAN 60 should be tagged, and all other VLANs should be disabled or untagged.

Switch 3 Configurations:

- **Ports 2 to 8**:
  - The configurations here must also match the connected devices. For mobile user connections, only VLANs relevant to user access (like VLAN 150 for WLAN) should be enabled and set to tagged or untagged based on network policies.
  - Any VLAN not associated with the connected devices should be disabled to secure the network.

Fault Tolerant Connections:

- **Ensure redundancy**: If these switches are connected via multiple ports, configure Link Aggregation Control Protocol (LACP) if not already set up to provide redundancy and increased bandwidth.
- **Check duplex and speed settings**: Ensure that duplex settings are set to Auto to avoid duplex mismatch which can cause performance issues.

Disabling Unused Ports:

- Any port not connected or not planned to be used should be disabled to prevent unauthorized access or network breaches.

Final Checks:

- **Verify settings**: After configuration changes, verify all settings to ensure they adhere to network policies and the devices are performing as expected.
- **Documentation**: Update network documentation to reflect changes for future troubleshooting and audits.

airmancompsci Highly Voted 1 month, 1 week ago

After reviewing some outside notes and doing this on paper, I think the answer is this below. Correct me if anything may be wrong though:

SWITCH 1:
- The only thing that would need to be fixed here is to set all the Speed and Duplex values to auto.
- All LACP, tagging, and VLAN assignments look to be correct.

SWITCH 3:
- For all ports, set Speed and Duplex to auto (although I guess disabled ones don't matter as much).
- For all ports, remove from VLAN 1 (although, again, disabled ports might not matter as much).
- Port 1 and Port 2:
* Enable port
* Enable LACP
* Add following VLANS as TAGGED: 60, 90, 120, 220
- Port 3:
* Disable port
- Port 4:
* Add to VLAN 220 TAGGED
* Add to VLAN 120 untagged
- Port 5:
* Disable port
- Port 6:
* Add to VLAN 120 untagged
- Port 7:
* Add to VLAN 60 untagged
- Port 8:
* Add to VLAN 90 untagged

upvoted 6 times

⊟ **chrys** Highly Voted 👍 4 months ago

Old CCSI here. I'll have to post response in chunks. Wasn't able to respond in one post. First: Disable Core switchports 3 - 8, Switch 2 port 6, Switch 3 ports 3, 5

upvoted 5 times

⊟ **jaylom** 1 month, 3 weeks ago

On switch 3 port 4 both voice and wired user traffic are carried through on the same link, should that port be configured as a trunk link? since it needs to carry traffic from two different vlans?

upvoted 1 times

⊟ **chrys** 4 months ago

Unless scenario indicates a speed/duplex mismatch, leave all ports on all switches at Full / 1000 (IRL we would set these to auto/auto)

upvoted 4 times

⊟ **max12553** Most Recent 🕘 6 days, 17 hours ago

One half says to leave speeds at 1000, other side says to change to Auto.
Any tie breakers here?

upvoted 1 times

⊟ **Azizuddeen** 1 month, 1 week ago

Port enabled = connected devices
Port disabled = no devices
LACP enabled = if connected from switch to switch
untagged VLAN = devices connected (servers, pc, printer...)
tagged VLAN = if connected from switch to switch

Should be pretty straightforward with that info.

upvoted 4 times

⊟ **chrys** 4 months ago

Oh I screwed up. Should just be replying to myself, instead of posting new. OK, I'll redo. Sorry guys.

upvoted 3 times

⊟ **chrys** 4 months ago

For VLAN tagging, looks like on access-distribution trunk links, they only want VLANs that the access switches are using. Dist-core trunk links will need to carry all VLANs. You only tag VLANs on trunk links. Never on the ports endpoints are plugged into.

upvoted 3 times

MIXDBAG 3 months, 4 weeks ago

So basically, you leave Switch2 P3,4,5,7,8 and Switch3 P4,6,7,8 as untagged correct?

upvoted 6 times

chrys 4 months ago

LACP should be enabled on all the trunk ports: Core switchports 1, 2; Switch 1 ports 1, 2, 5, 6, 7, 8; Switch 2 ports 1, 2; Switch 3 ports 1, 2

upvoted 4 times

chrys 4 months ago

Looks like Switch 1 is a distribution layer switch with two servers hanging off of it

Switch 2 and 3 are access layer switches.

upvoted 2 times

chrys 4 months ago

Unless scenario indicates a speed/duplex mismatch, leave all ports on all switches at Full / 1000 (IRL we would set these to auto/auto)

upvoted 3 times

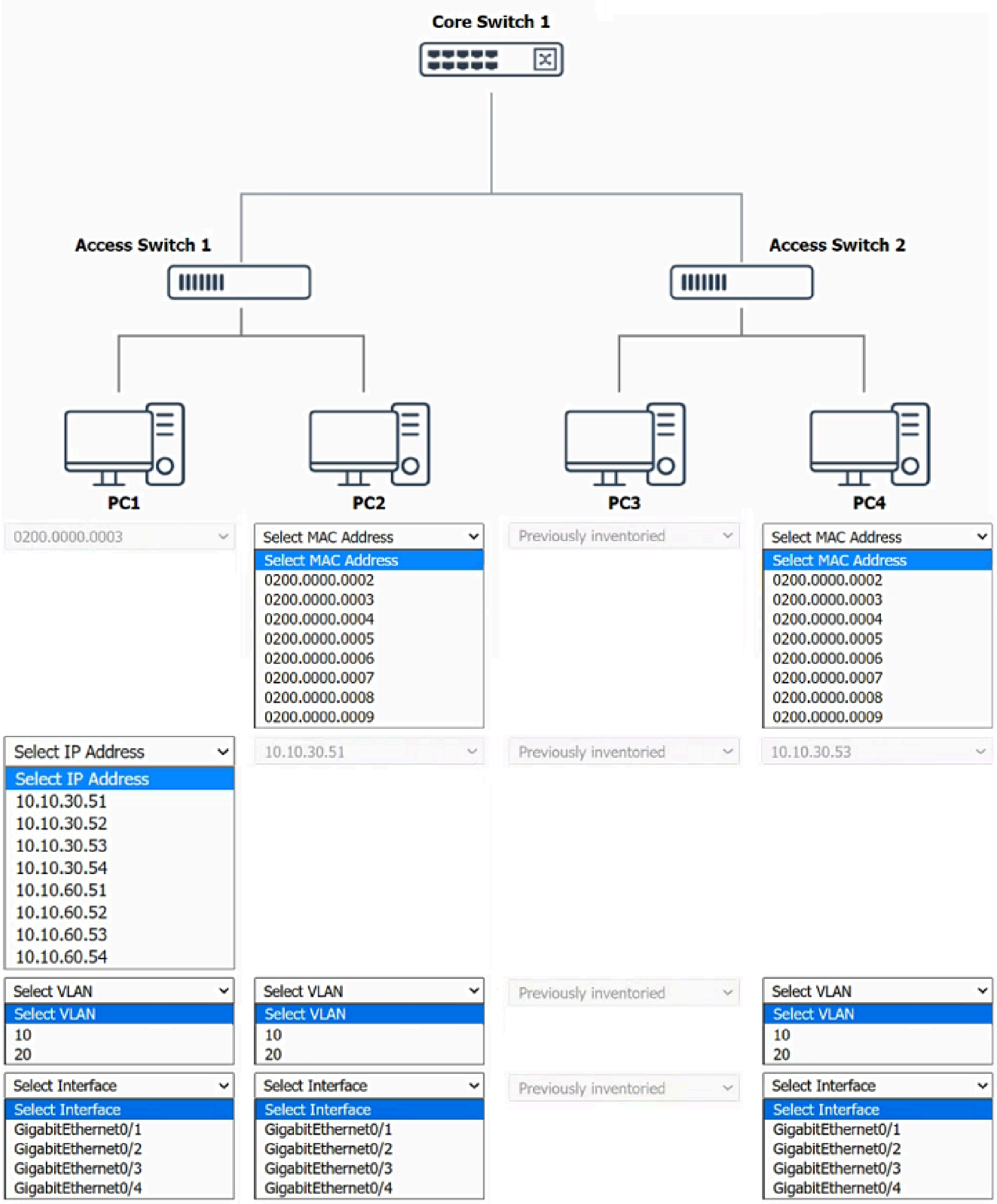
Question #2 *Topic 1*

SIMULATION -

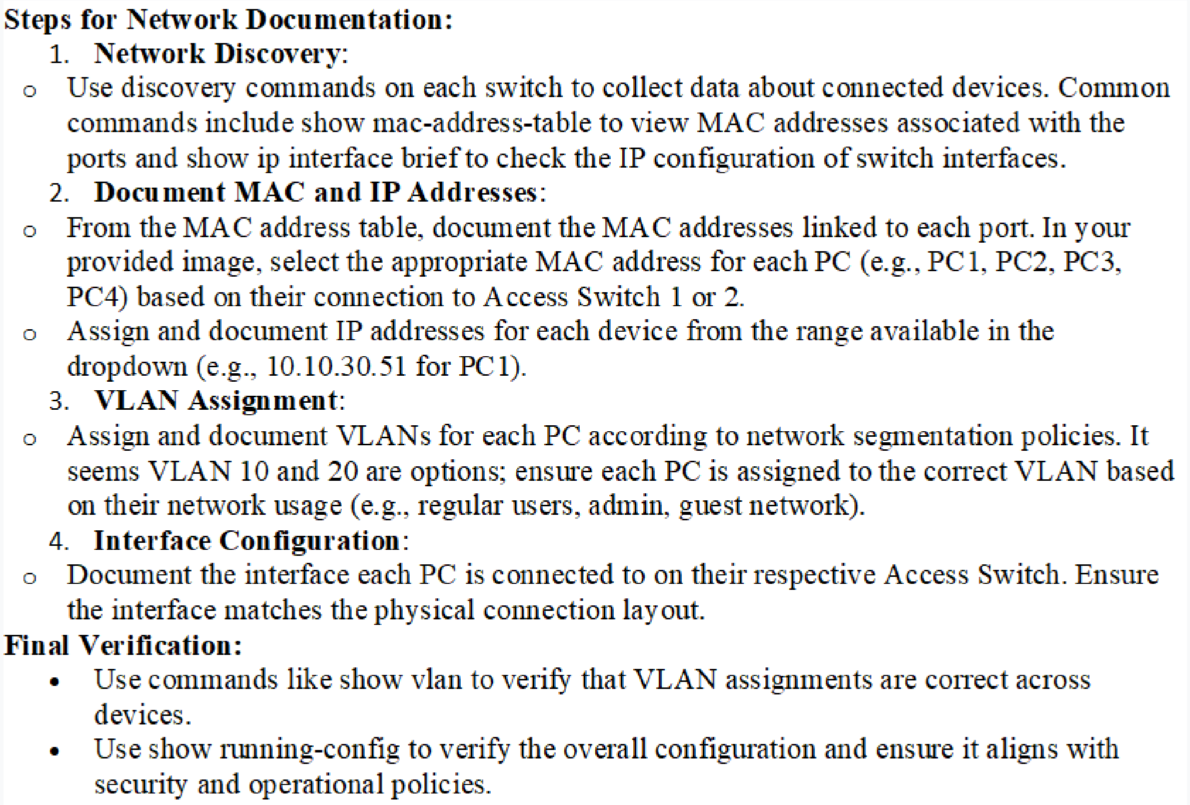
A network technician was recently onboarded to a company. A manager has tasked the technician with documenting the network and has provided the technician with partial information from previous documentation.

INSTRUCTIONS -

Click on each switch to perform a network discovery by entering commands into the terminal. Type help to view a list of available commands.
Fill in the missing information using the drop-down menus provided.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Correct Answer:



Steps for Network Documentation:

1. **Network Discovery**:
   - Use discovery commands on each switch to collect data about connected devices. Common commands include show mac-address-table to view MAC addresses associated with the ports and show ip interface brief to check the IP configuration of switch interfaces.
2. **Document MAC and IP Addresses**:
   - From the MAC address table, document the MAC addresses linked to each port. In your provided image, select the appropriate MAC address for each PC (e.g., PC1, PC2, PC3, PC4) based on their connection to Access Switch 1 or 2.
   - Assign and document IP addresses for each device from the range available in the dropdown (e.g., 10.10.30.51 for PC1).
3. **VLAN Assignment**:
   - Assign and document VLANs for each PC according to network segmentation policies. It seems VLAN 10 and 20 are options; ensure each PC is assigned to the correct VLAN based on their network usage (e.g., regular users, admin, guest network).
4. **Interface Configuration**:
   - Document the interface each PC is connected to on their respective Access Switch. Ensure the interface matches the physical connection layout.

Final Verification:

- Use commands like show vlan to verify that VLAN assignments are correct across devices.
- Use show running-config to verify the overall configuration and ensure it aligns with security and operational policies.

max12553 6 days, 17 hours ago

Type help or Type '?'

Look at the arp table and cross reference data?

show interfaces

show ip arp

show mac address-table

show mac-address-table

show vlan

upvoted 1 times

smella 1 week, 5 days ago

How are yall figuring out which PC is connected to what port, any time i have taken this there is 5+ connections to the access switch. Cant seem to figure out how to differentiate the others except the one core port

upvoted 1 times

Alex3790 2 weeks, 5 days ago

Passed my exam yesterday, this pbq was there with different IPs

upvoted 2 times

Azizuddeen 1 month, 1 week ago

type "help" in the core switch and you will receive the commands.

Ask and thy shall receive :)

upvoted 1 times

WTD34 3 months, 3 weeks ago

show mac-address table and show arp would be good, compare to the answers pregiven like PC1 and refer to the address table it pretty much tells you the answer to the questions

upvoted 2 times

chrys 4 months ago

Looks like I'll have to post response in sections.

upvoted 4 times

chrys 4 months ago

Huh. show mac-address-table is an old Cisco command. Surprised they haven't gone to show mac address-table. I suppose maybe they have super old switches in the scenario.

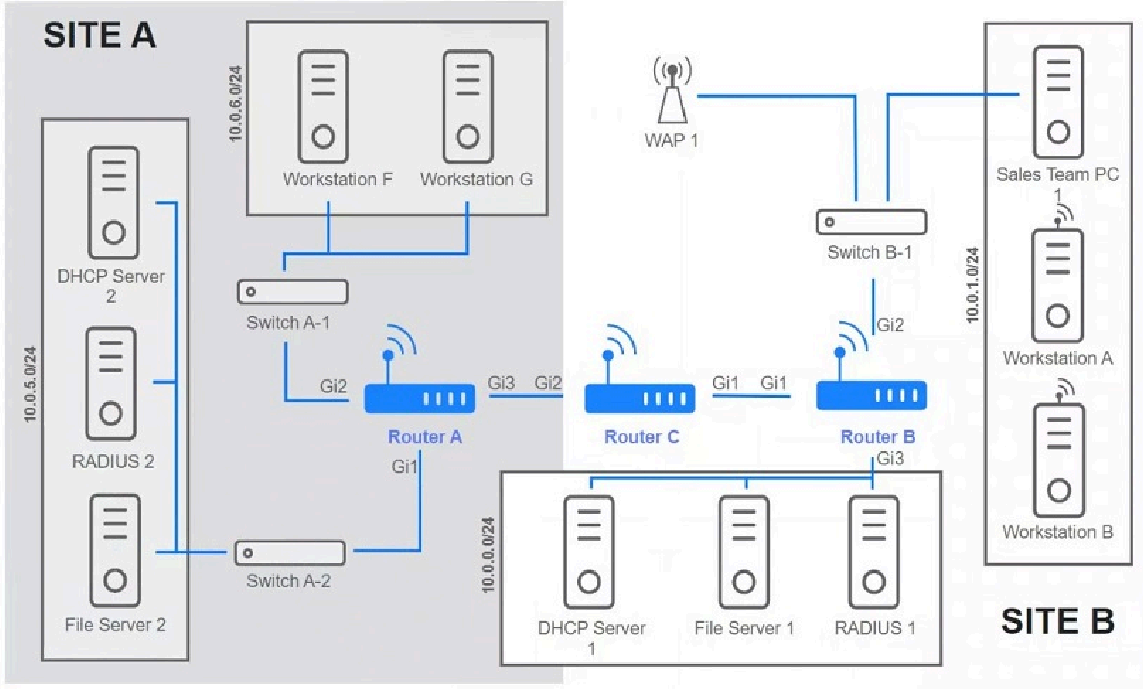
upvoted 1 times

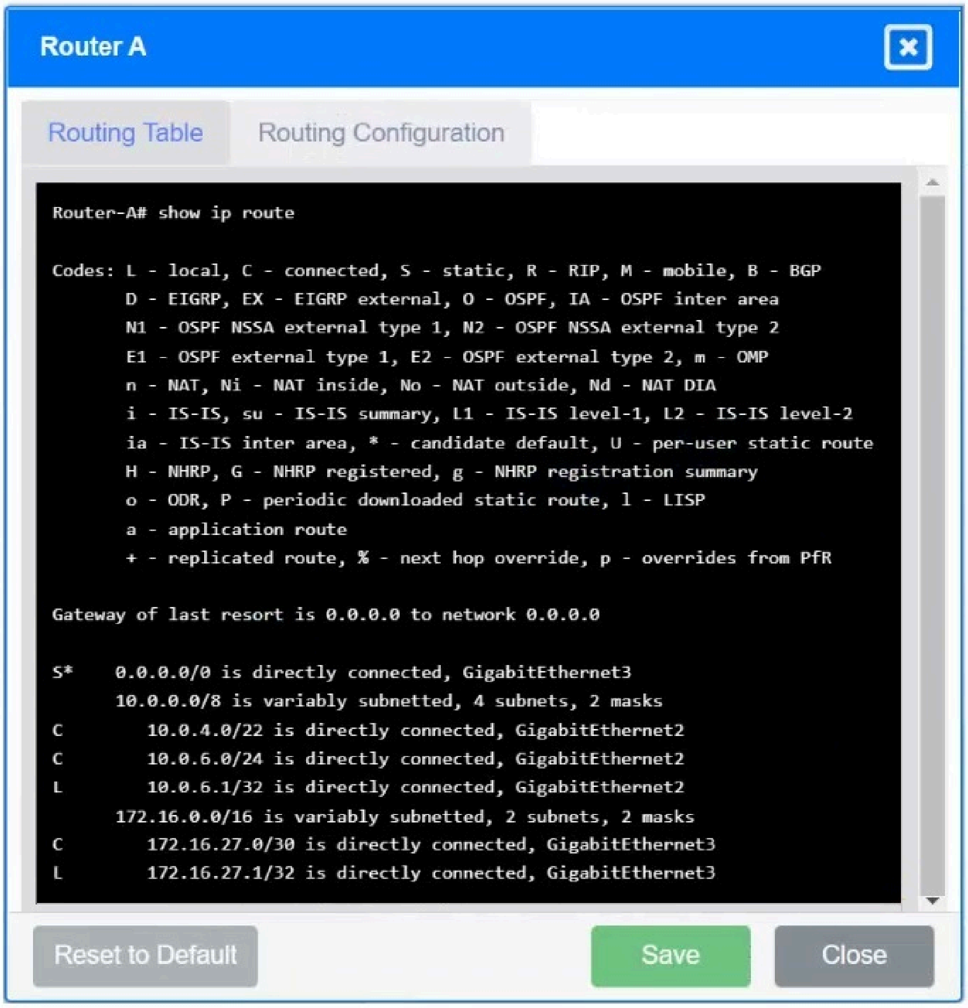
SIMULATION -

Users are unable to access files on their department share located on file server 2. The network administrator has been tasked with validating routing between networks hosting workstation A and file server 2.

INSTRUCTIONS -

Click on each router to review output, identify any issues, and configure the appropriate solution.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



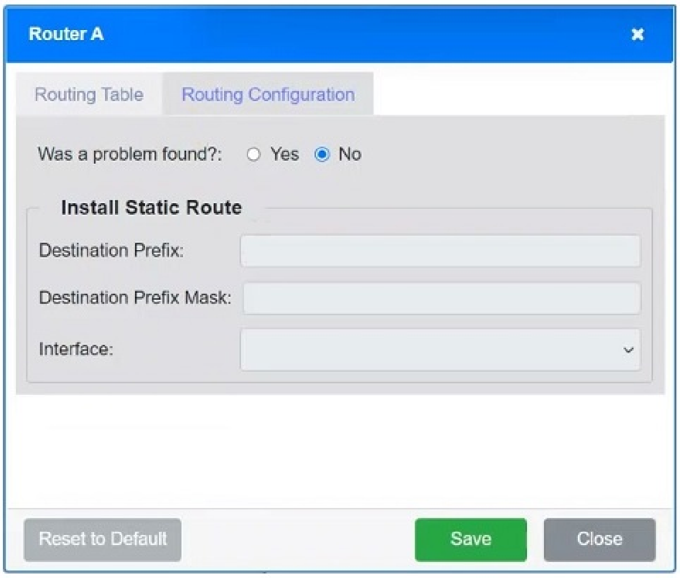


```
Router-A# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, GigabitEthernet3
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.4.0/22 is directly connected, GigabitEthernet2
C        10.0.6.0/24 is directly connected, GigabitEthernet2
L        10.0.6.1/32 is directly connected, GigabitEthernet2
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.0/30 is directly connected, GigabitEthernet3
L        172.16.27.1/32 is directly connected, GigabitEthernet3
```



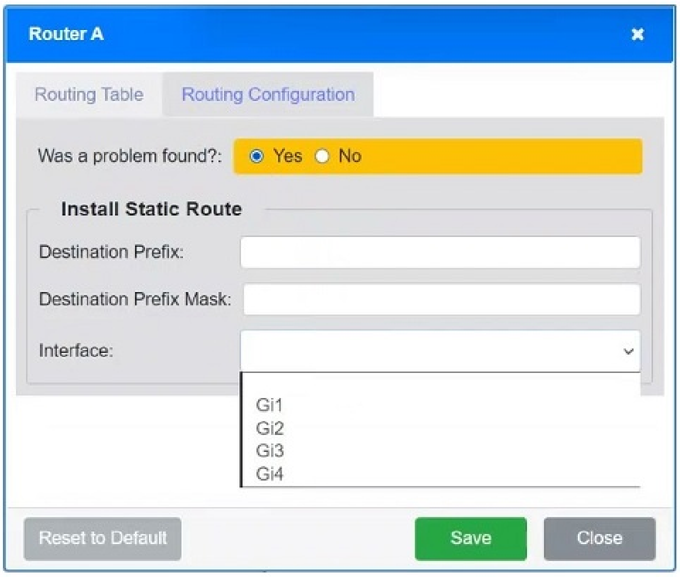
Was a problem found?: ○ Yes ● No

Install Static Route

Destination Prefix:

Destination Prefix Mask:

Interface:



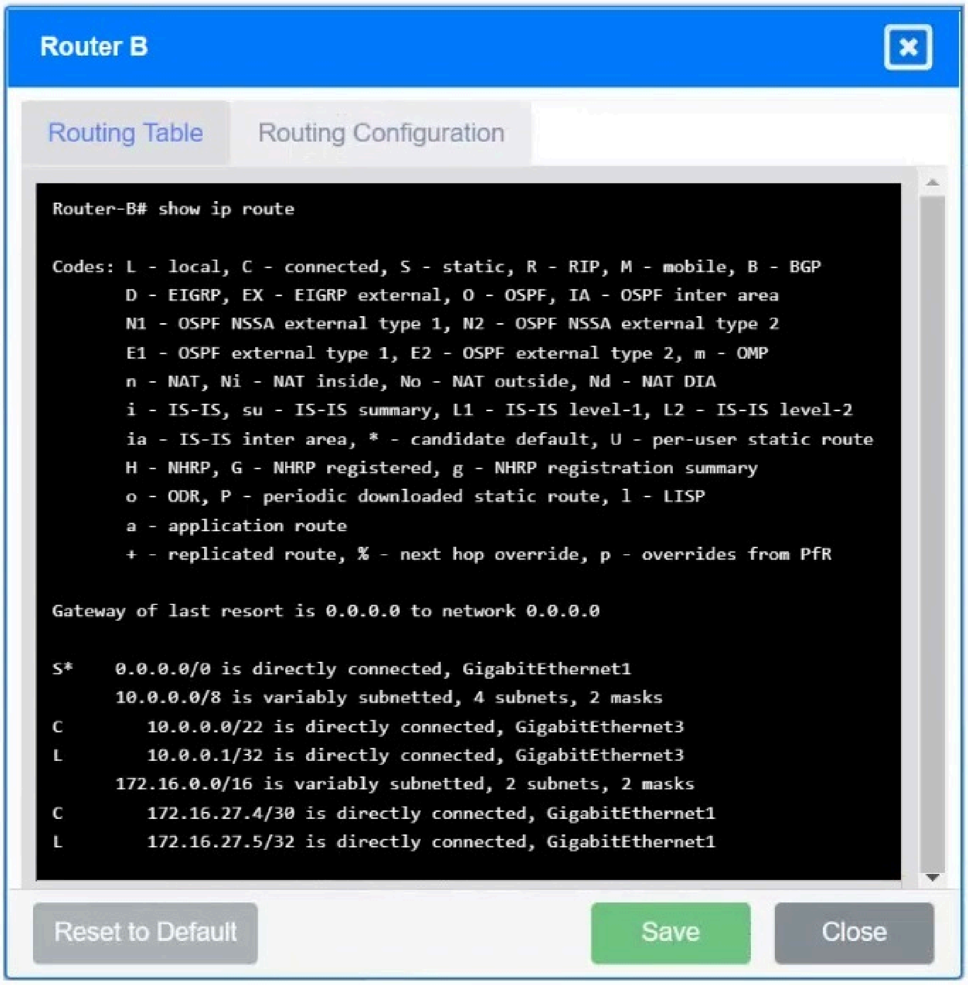
Was a problem found?: ● Yes ○ No

Install Static Route

Destination Prefix:

Destination Prefix Mask:

Interface:

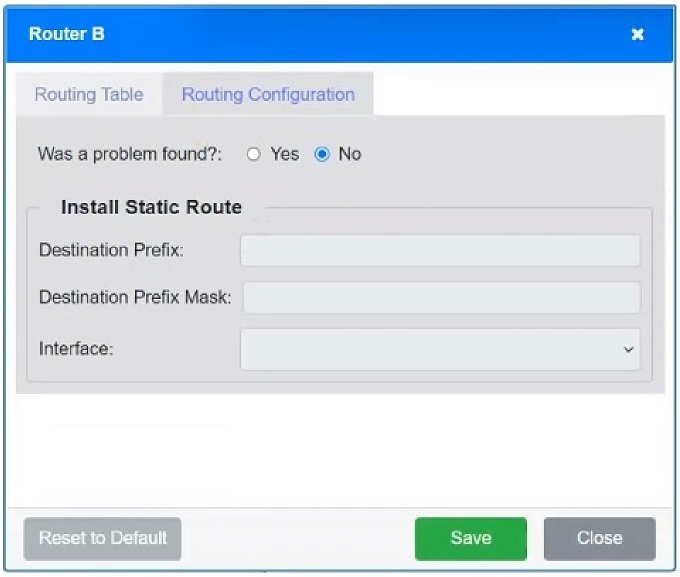


```
Router-B# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, GigabitEthernet1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/22 is directly connected, GigabitEthernet3
L        10.0.0.1/32 is directly connected, GigabitEthernet3
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.4/30 is directly connected, GigabitEthernet1
L        172.16.27.5/32 is directly connected, GigabitEthernet1
```



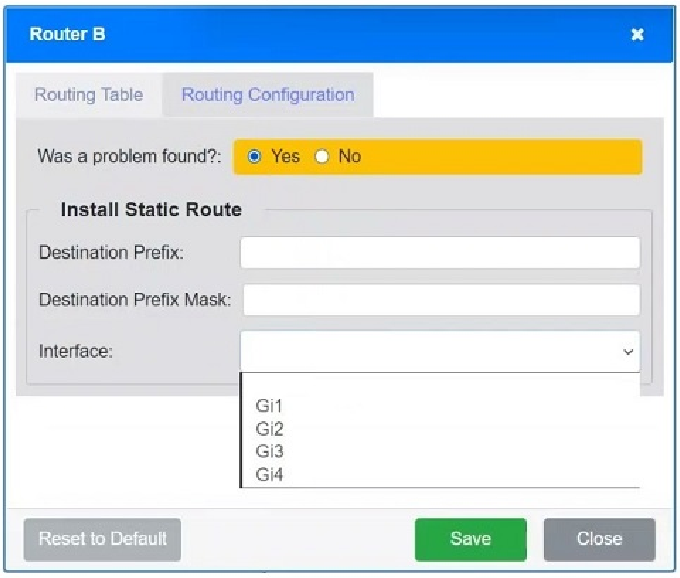
Was a problem found?: ○ Yes ● No

Install Static Route

Destination Prefix:

Destination Prefix Mask:

Interface:



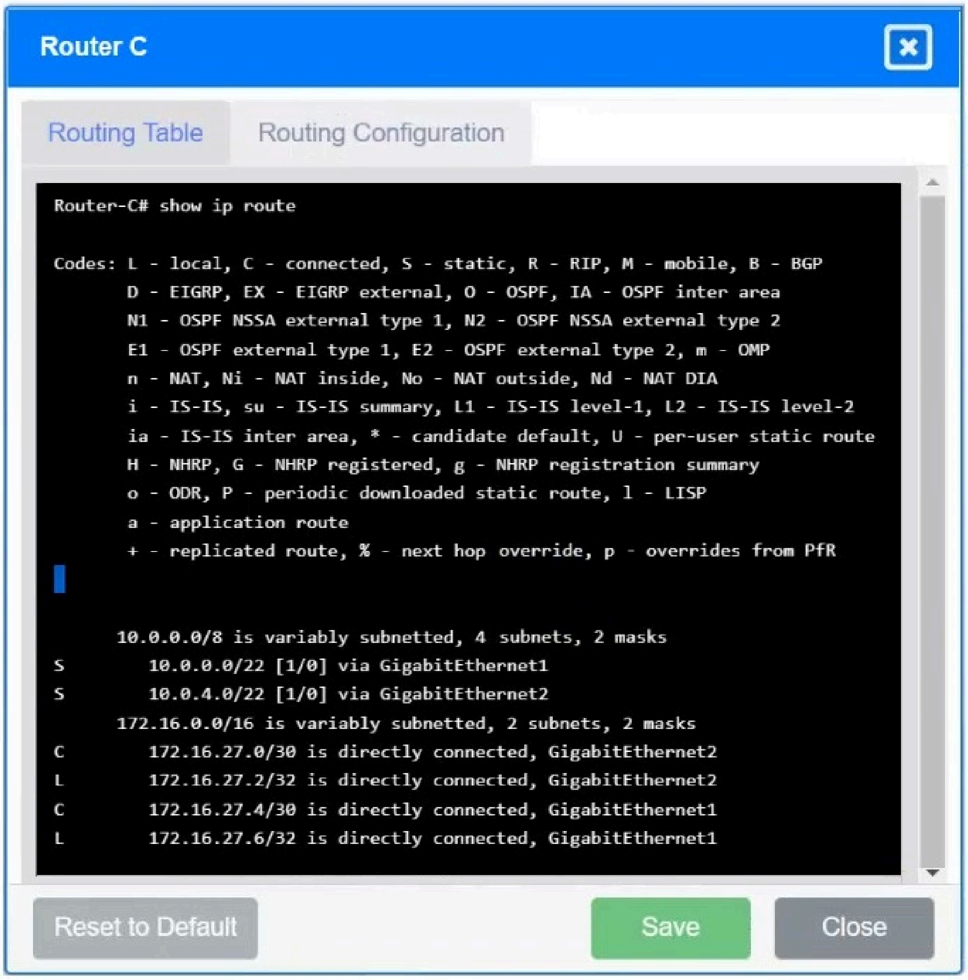
Was a problem found?: ● Yes ○ No

Install Static Route

Destination Prefix:

Destination Prefix Mask:

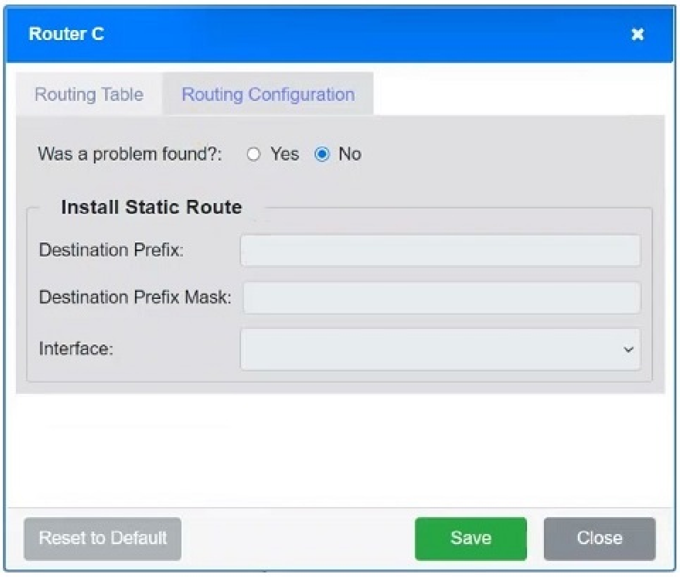
Interface:



```
Router-C# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR


      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S        10.0.0.0/22 [1/0] via GigabitEthernet1
S        10.0.4.0/22 [1/0] via GigabitEthernet2
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.0/30 is directly connected, GigabitEthernet2
L        172.16.27.2/32 is directly connected, GigabitEthernet2
C        172.16.27.4/30 is directly connected, GigabitEthernet1
L        172.16.27.6/32 is directly connected, GigabitEthernet1
```



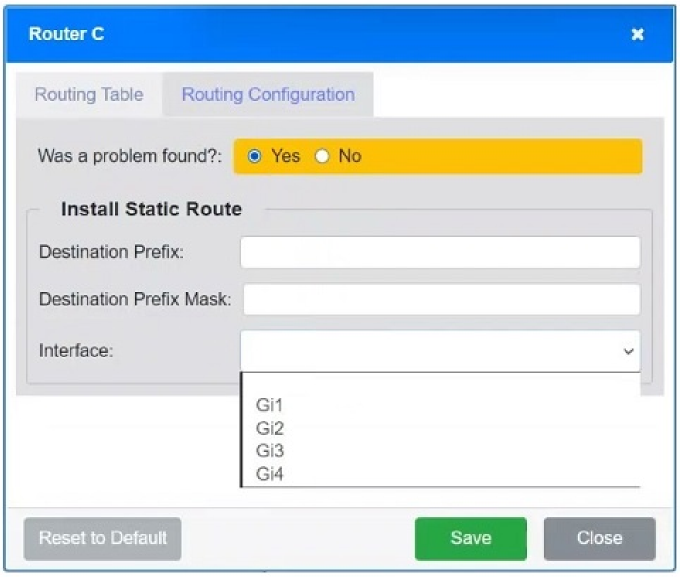
Was a problem found?: ○ Yes ● No

Install Static Route

Destination Prefix:

Destination Prefix Mask:

Interface:



Router C ✖

Was a problem found?: ● Yes ○ No

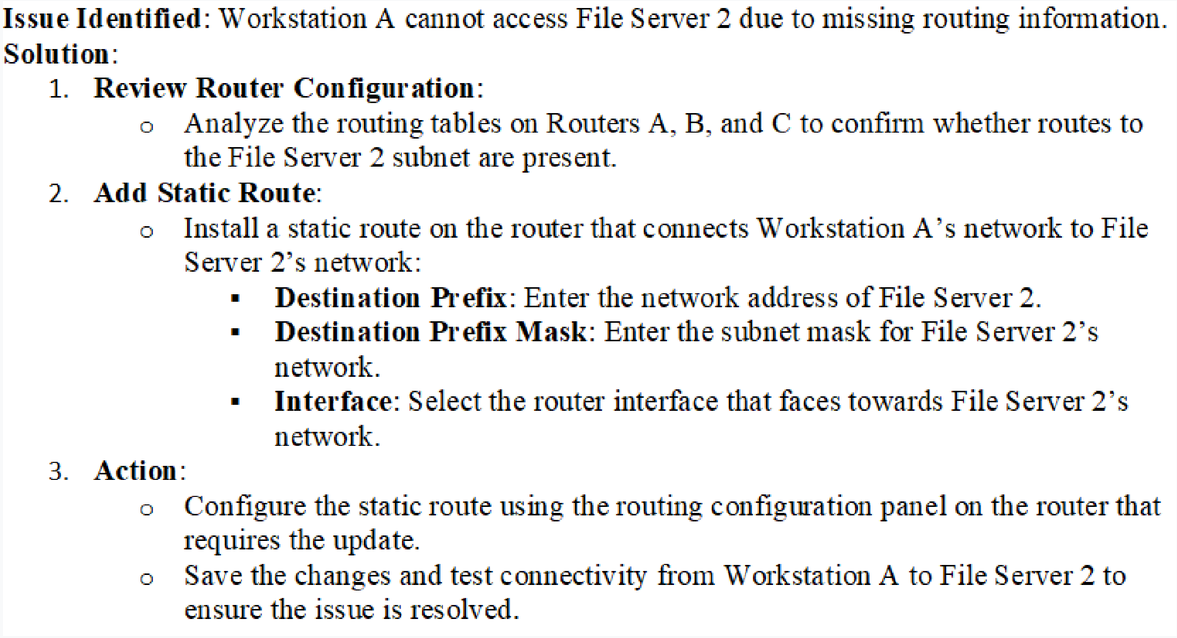
Install Static Route

Destination Prefix:

Destination Prefix Mask:

Interface:

Correct Answer:



Issue Identified: Workstation A cannot access File Server 2 due to missing routing information.

Solution:

1. **Review Router Configuration**:
   - Analyze the routing tables on Routers A, B, and C to confirm whether routes to the File Server 2 subnet are present.
2. **Add Static Route**:
   - Install a static route on the router that connects Workstation A's network to File Server 2's network:
     - **Destination Prefix**: Enter the network address of File Server 2.
     - **Destination Prefix Mask**: Enter the subnet mask for File Server 2's network.
     - **Interface**: Select the router interface that faces towards File Server 2's network.
3. **Action**:
   - Configure the static route using the routing configuration panel on the router that requires the update.
   - Save the changes and test connectivity from Workstation A to File Server 2 to ensure the issue is resolved.

⊟ **Azizuddeen** Highly Voted 1 month, 1 week ago

Router A:

Problem found: Yes

Destination Prefix: 10.0.5.0

Destination Mask: 255.255.255.0

Interface: Gi1

Router B:

Problem Found: Yes

Destination Prefix: 10.0.1.0

Destination Mask: 255.255.255.0

Interface: Gi2

Router B: nothing to do, all good

upvoted 7 times

⊟ **PatrickH** 2 weeks ago

This answer seems perfect. Router A is unaware of the 10.0.5.0/24 network and Router B is unaware of the 10.0.1.0/24 network. Both need to be added. Interfaces are correct. Good job

upvoted 1 times

⊟ **8d5b6f0** 3 weeks, 2 days ago

router B all good or router C?

upvoted 1 times

⊟ **tempuser1232** Most Recent 1 week ago

Can someone explain the answer to me please?

upvoted 1 times

⊟ **Alex3790** 2 weeks, 5 days ago

Passed my exam Yesterday, this was the first pbq but different IPs

upvoted 2 times

⊟ **mikazouk** 1 month, 3 weeks ago

Does anyone know the complete answer to the exercise?

upvoted 2 times

⊟ **TreyPar3** 3 months, 4 weeks ago

It seems as if Router B isnt detecting the Sub Network that Workstation A is within, (10.0.1.0/24), given the Information we have. So, a static route configuration to 10.0.1.0 on Gi2, might be need as well as the static route needed for the File 2 server and Router A.

Also I might be wrong, but Router C looks like it is having a duplicate IP issue between its Gi2 and Gi1, but I don't know how applying more static routes will solve that conundrum.

upvoted 1 times

⊟ **st1a** 3 months, 1 week ago

router A is missing the 10.0.5.0/24 network. I built this lab in packet tracer to verify.

router C is correct. It has static routes that include a larger address space to send to the correct interface.

router b has a default route sending it to the correct interface.

upvoted 1 times

⊟ **st1a** 3 months, 1 week ago

fixing my mistake. router b needs a default route for the 10.0.1.0 traffic on interface2. the default route on router b is for sending traffic outbound

upvoted 1 times

Question #4 *Topic 1*

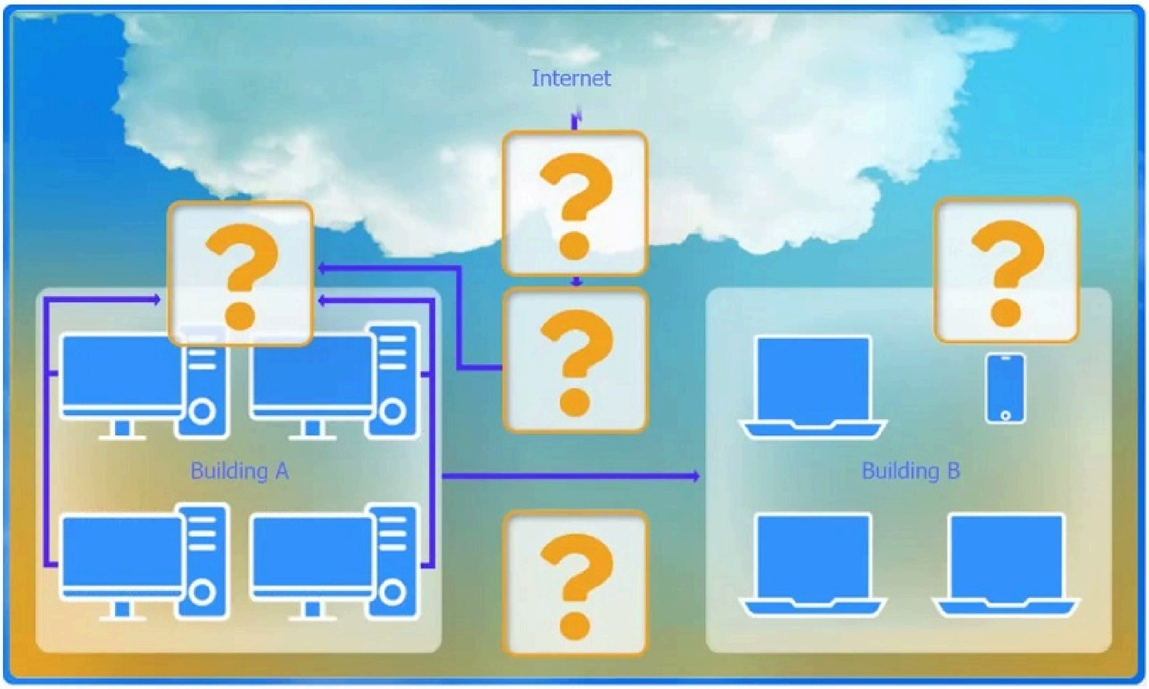
SIMULATION -

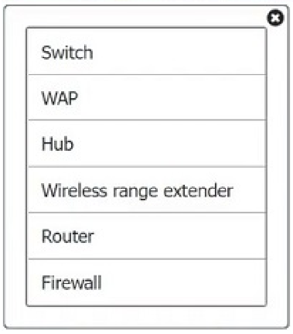
A network administrator has been tasked with configuring a network for a new corporate office. The office consists of two buildings, separated by 50 feet with no physical connectivity. The configuration must meet the following requirements:

Devices in both buildings should be able to access the Internet.
Security insists that all Internet traffic be inspected before entering the network.
Desktops should not see traffic destined for other devices.

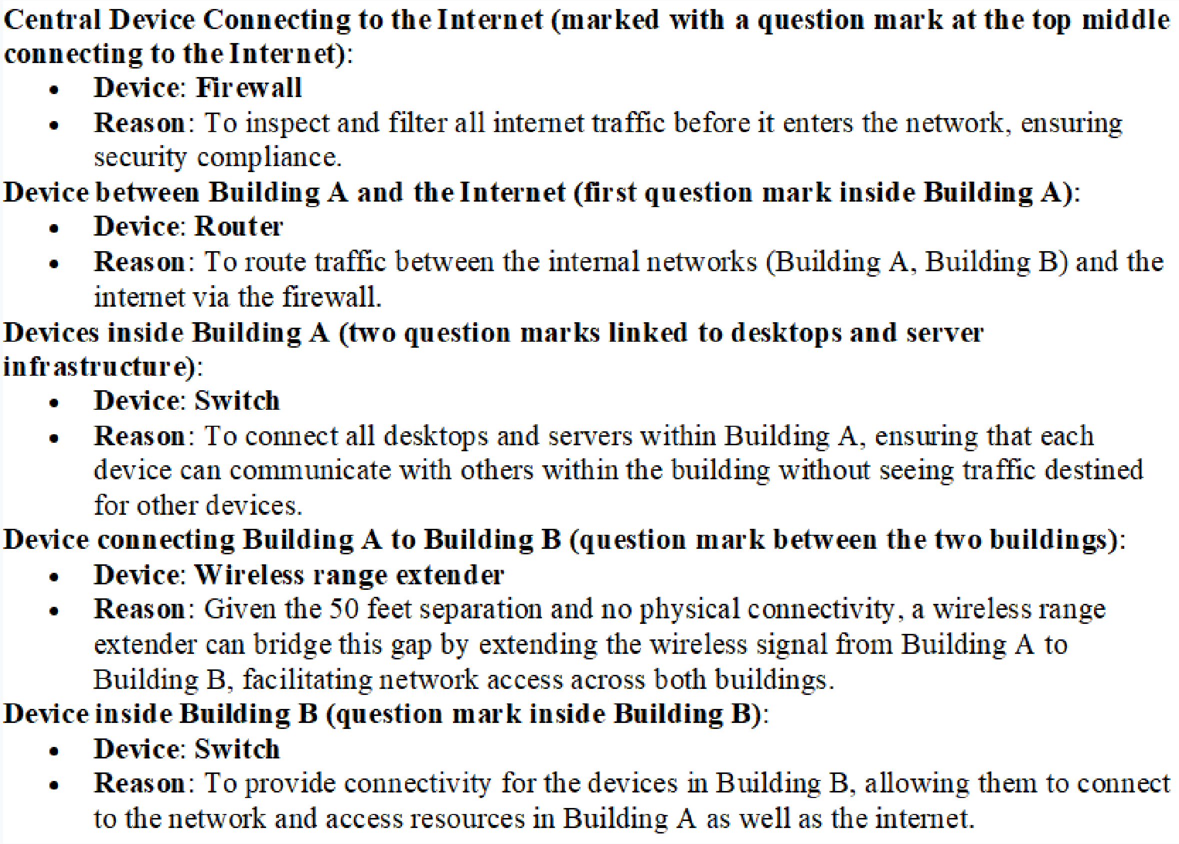
INSTRUCTIONS -

Select the appropriate network device for each location. If applicable, click on the magnifying glass next to any device which may require configuration updates and make any necessary changes.
Not all devices will be used, but all locations should be filled.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Correct Answer:



Central Device Connecting to the Internet (marked with a question mark at the top middle connecting to the Internet):

- **Device**: **Firewall**
- **Reason**: To inspect and filter all internet traffic before it enters the network, ensuring security compliance.

Device between Building A and the Internet (first question mark inside Building A):

- **Device**: **Router**
- **Reason**: To route traffic between the internal networks (Building A, Building B) and the internet via the firewall.

Devices inside Building A (two question marks linked to desktops and server infrastructure):

- **Device**: **Switch**
- **Reason**: To connect all desktops and servers within Building A, ensuring that each device can communicate with others within the building without seeing traffic destined for other devices.

Device connecting Building A to Building B (question mark between the two buildings):

- **Device**: **Wireless range extender**
- **Reason**: Given the 50 feet separation and no physical connectivity, a wireless range extender can bridge this gap by extending the wireless signal from Building A to Building B, facilitating network access across both buildings.

Device inside Building B (question mark inside Building B):

- **Device**: **Switch**
- **Reason**: To provide connectivity for the devices in Building B, allowing them to connect to the network and access resources in Building A as well as the internet.

⊟ **chrys** Highly Voted 4 months ago

You can't have a Wireless Range Extender without a WAP for it to connect to and repeat. The device at the bottom middle needs to be a WAP. Then the device in Bldg B can be a wireless range extender. It's ok since all Bldg B devices appear to be wireless capable (laptops, phone)

upvoted 8 times

⊟ **Hill87** 1 week, 2 days ago

Why not put the extender between buildings and the WAP inside?

upvoted 1 times

⊟ **temp_user_007** 3 months, 1 week ago

Agree. Also with "...two buildings, separated by 50 feet with no physical connectivity.", I think the WAP will be connected to building A's switch physically so it gets inbound internet connection from wired ethernet. Then put a wireless range extender in building B.

upvoted 1 times

⊟ **Michu07** 3 months ago

But will they be able to access the company's network resources with a wireless extender?

upvoted 2 times

⊟ **tempuser1232** Most Recent 1 week ago

Can someone explain the answer to me please?

upvoted 1 times

⊟ **Quezzo** 1 week, 1 day ago

Yo alex, help me out with the PBQs, if you don't mind.

upvoted 1 times

⊟ **Alex3790** 2 weeks, 5 days ago

Passed my exam Yesterday, this was the first PBQ firewall goes first and then the router, once you placed all, double click on repeater and change the Security to WPA2-Ent all others need to open and just click on save

upvoted 1 times

⊟ **UncleSmurf** 4 months, 2 weeks ago

- Building A: Switch
- Connection between Building A and the Internet: Router
- Connection to Internet: Firewall

- Connection to Building B: WAP or Wireless Range Extender
- Inside Building B: Switch (if wired) or use WAP

upvoted 1 times

Question #5 *Topic 1*

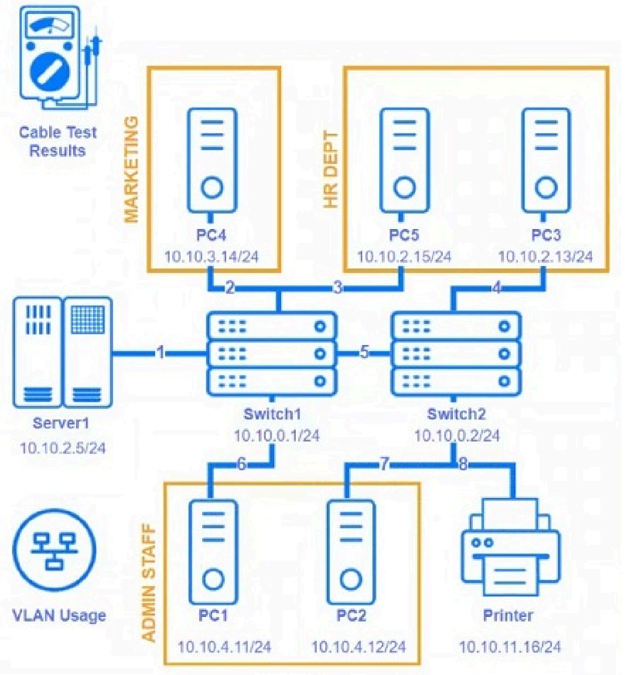
SIMULATION -

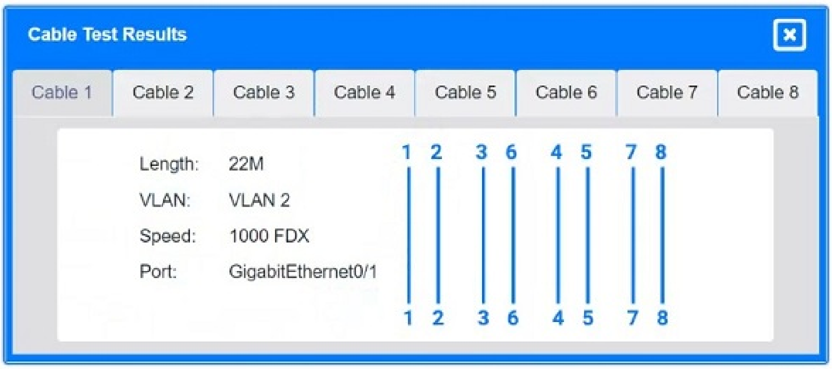
A network technician needs to resolve some issues with a customer's SOHO network. The customer reports that some of the devices are not connecting to the network, while others appear to work as intended.

INSTRUCTIONS -

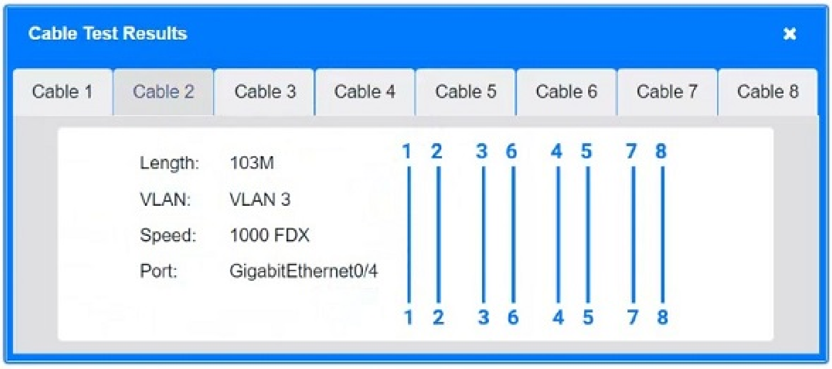
Troubleshoot all the network components and review the cable test results by clicking on each device and cable. Type help in each terminal to view a list of available commands.

Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

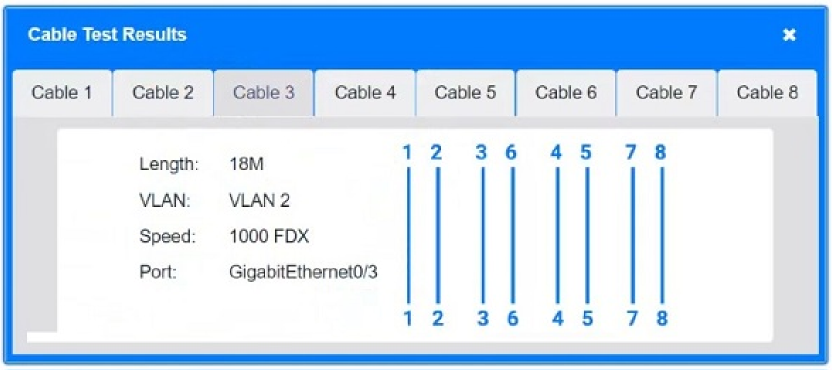



Cable Test Results

Length: 22M
VLAN: VLAN 2
Speed: 1000 FDX
Port: GigabitEthernet0/1


Cable Test Results

Length: 103M
VLAN: VLAN 3
Speed: 1000 FDX
Port: GigabitEthernet0/4

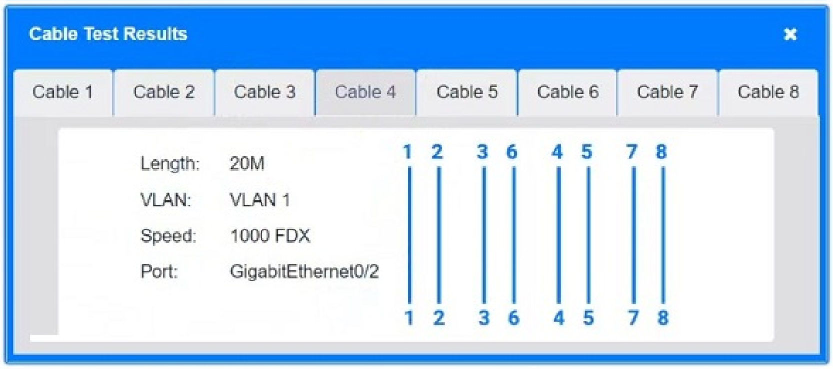


Length: 18M

VLAN: VLAN 2

Speed: 1000 FDX

Port: GigabitEthernet0/3

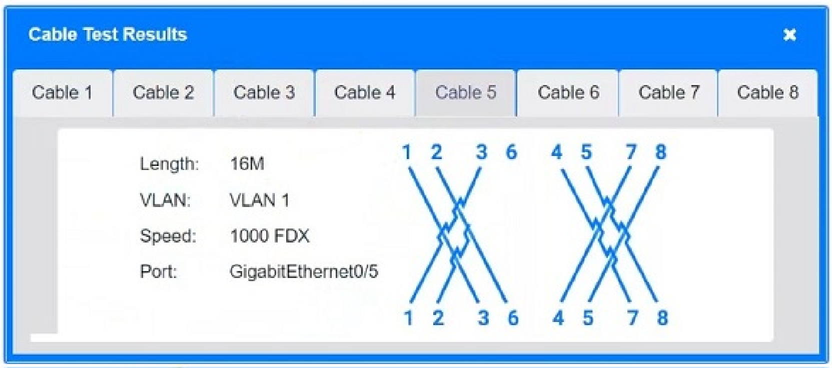


Length: 20M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/2

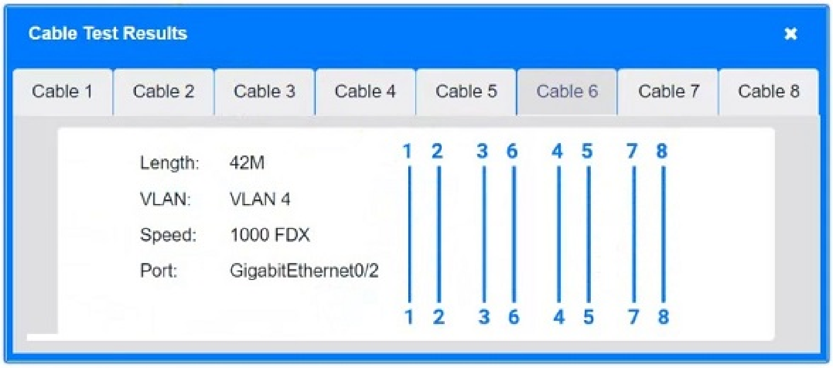


Length: 16M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/5

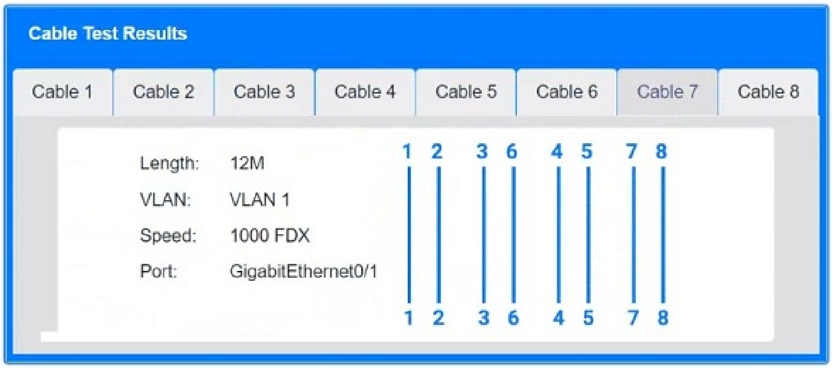


Length: 42M

VLAN: VLAN 4

Speed: 1000 FDX

Port: GigabitEthernet0/2

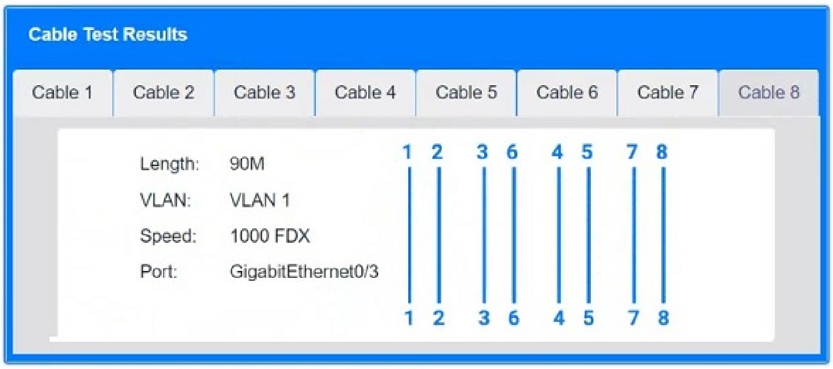


Length: 12M

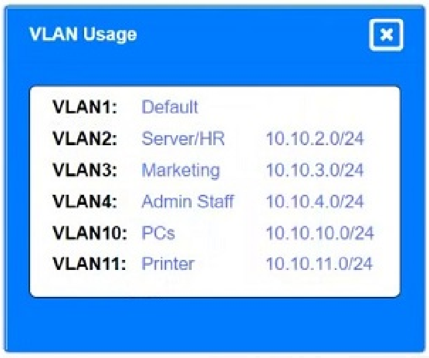
VLAN: VLAN 1

Speed: 1000 FDX

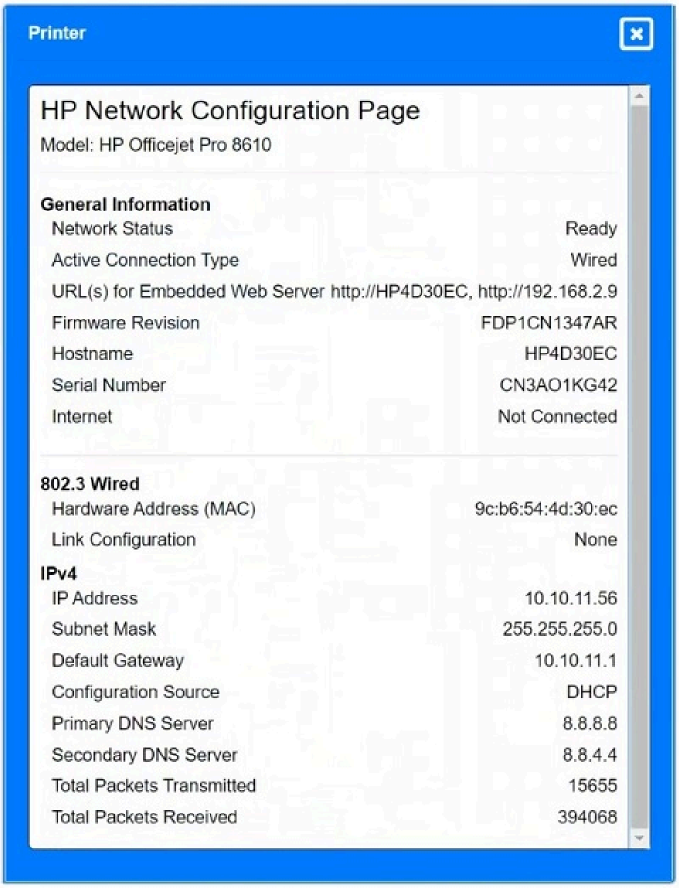
Port: GigabitEthernet0/1



Length:	90M
VLAN:	VLAN 1
Speed:	1000 FDX
Port:	GigabitEthernet0/3



VLAN1:	Default	
VLAN2:	Server/HR	10.10.2.0/24
VLAN3:	Marketing	10.10.3.0/24
VLAN4:	Admin Staff	10.10.4.0/24
VLAN10:	PCs	10.10.10.0/24
VLAN11:	Printer	10.10.11.0/24



HP Network Configuration Page

Model: HP Officejet Pro 8610

General Information

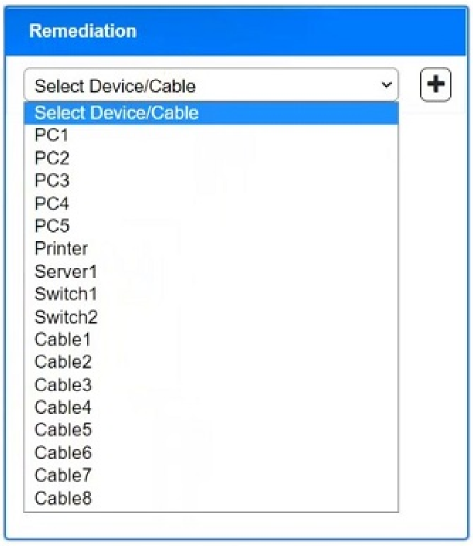
Network Status	Ready
Active Connection Type	Wired
URL(s) for Embedded Web Server	http://HP4D30EC, http://192.168.2.9
Firmware Revision	FDP1CN1347AR
Hostname	HP4D30EC
Serial Number	CN3AO1KG42
Internet	Not Connected

802.3 Wired

Hardware Address (MAC)	9c:b6:54:4d:30:ec
Link Configuration	None

IPv4

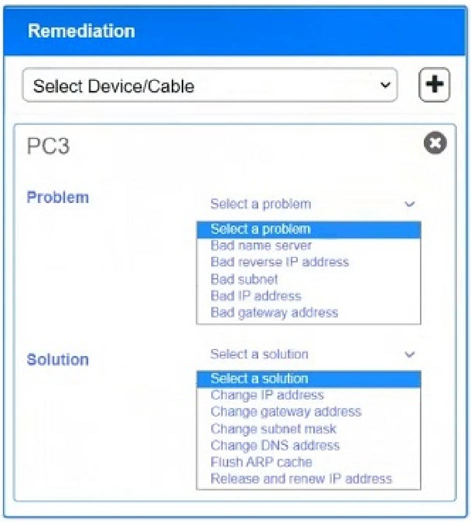
IP Address	10.10.11.56
Subnet Mask	255.255.255.0
Default Gateway	10.10.11.1
Configuration Source	DHCP
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4
Total Packets Transmitted	15655
Total Packets Received	394068



Remediation

Select Device/Cable

Select Device/Cable
PC1
PC2
PC3
PC4
PC5
Printer
Server1
Switch1
Switch2
Cable1
Cable2
Cable3
Cable4
Cable5
Cable6
Cable7
Cable8



Remediation

Select Device/Cable

PC3

Problem: Select a problem

Select a problem
Bad name server
Bad reverse IP address
Bad subnet
Bad IP address
Bad gateway address

Solution: Select a solution

Select a solution
Change IP address
Change gateway address
Change subnet mask
Change DNS address
Flush ARP cache
Release and renew IP address

Correct Answer:

Router and Firewall Configuration:

- Ensure that all routers are configured with correct static routes to facilitate proper network traffic routing between different VLANs and external networks.
- Install a firewall at the network's entry point to inspect and filter Internet traffic as required by the security policy.

Switch Configuration:

- Configure switches to ensure PCs in different VLANs do not see each other's traffic. Implement VLAN tagging on the switches to segregate traffic between the different departments as indicated.

Cable Test Results:

- Address any faulty cables as indicated by the test results. For example, any cable showing physical connection issues (crossed pairs, etc.) should be replaced.
- Ensure that cables are appropriately labeled and meet the length requirements to avoid potential transmission issues over long distances.

Device Specific Issues:

- For devices showing incorrect configuration details such as bad IP addresses, subnet masks, or DNS configurations, apply appropriate corrections. For instance, resetting IP configurations or updating DNS settings where mismatches are found.

Printer Configuration:

- Check the printer configuration to ensure it aligns with the network settings, particularly the IP address, subnet, and gateway to guarantee connectivity for all users needing access.

Overall Network Health:

- Continuously monitor the network for any emerging issues, perform regular updates to the firmware of network devices, and ensure compliance with the latest security standards to maintain network integrity and performance.

⊟ **PatrickH** 1 week, 5 days ago

We have 8 Cables we can click on. Cable 2 is too long, at 103 meters. Cable 5, which is a crossover cable, has a break.

All other cables are physically fine.

However there seems to be a few incorrect VLAN assignments

VLAN assignments

Cable 1 seems fine. Going from server to switch. VLAN 2 is correct.

Cable 2 Going from Marketing to Switch. VLAN 3 is correct

Cable 3. Going from HR to Switch. VLAN 2 is correct

Cable 4. Going from HR to Switch. VLAN is Wrong. Should be VLAN 2 for HR.

Cable 5. Going from Switch to Switch. VLAN 1 is correct

Cable 6. Going from Admin to Switch. VLAN 4 is correct

Cable 7. Going from Admin to Switch. VALN is Wrong. Should be VLAN 4 for Admin

Cable 8. Going from Printer to Switch, VLAN is wrong. Should be VLAN 11 for Printers

You can seemingly click on PC1 to PC 5. Maybe there's other problems, I just cannot see from here. Look at the IP addresses. Subnet masks, default gateways etc.. carefully. If you even can!

From what we can see all the IP addresses seem Ok.

upvoted 2 times

⊟ **CISUMPATR** 1 week, 6 days ago

Can someone provide a detailed answer

upvoted 1 times

⊟ **TLR87_** 2 weeks, 5 days ago

The Cable 5 between the switches...

Has to be Crossover from one side , not both of them

upvoted 1 times

⊟ **Fosterboi** 4 weeks ago

Can someone please explain what you see ?

upvoted 2 times

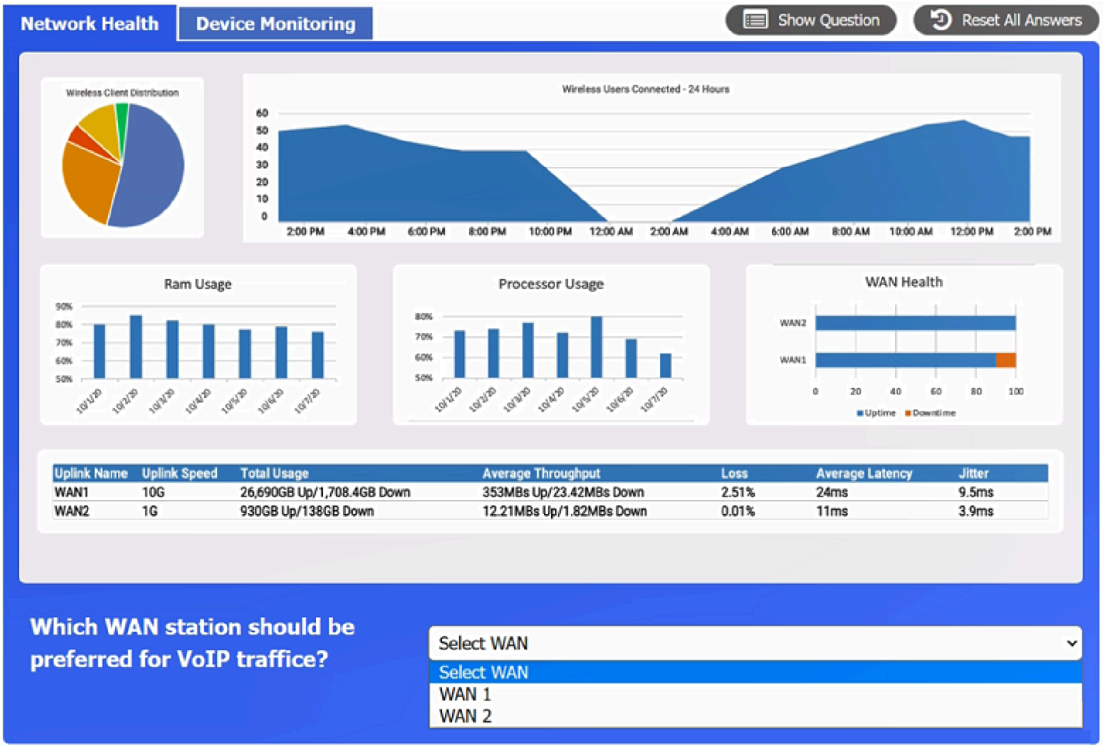
SIMULATION -

After a recent power outage, users are reporting performance issues accessing the application servers. Wireless users are also reporting intermittent Internet issues.

INSTRUCTIONS -

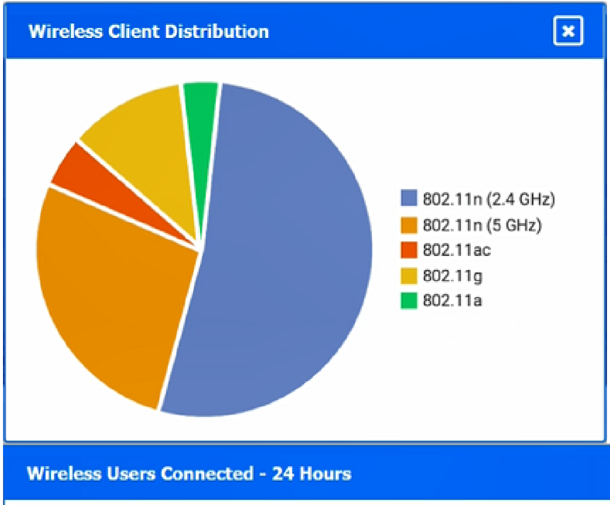
Click on each tab at the top of the screen. Select a widget to view information, then use the drop-down menus to answer the associated questions.

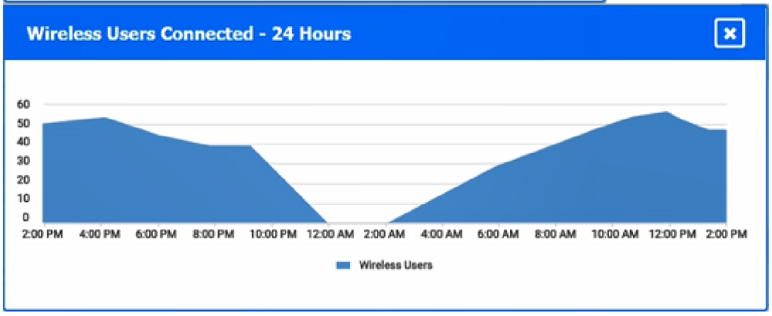
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

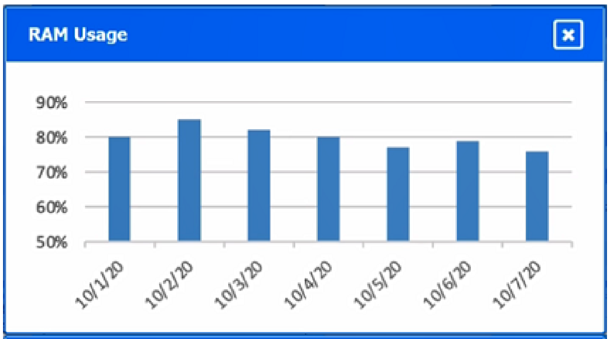


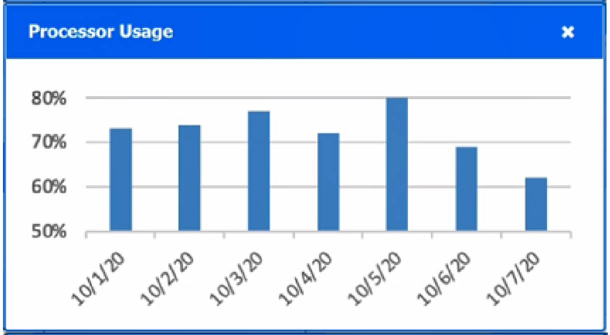
Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	Jitter
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9.5ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3.9ms

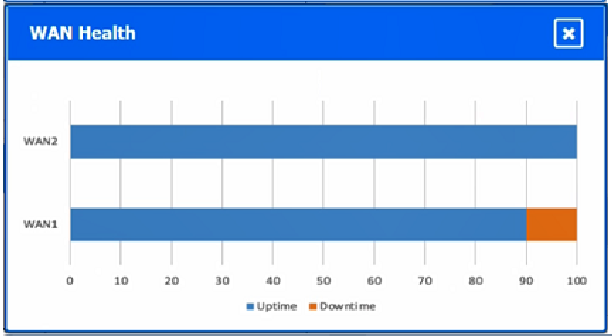
Which WAN station should be preferred for VoIP traffice?

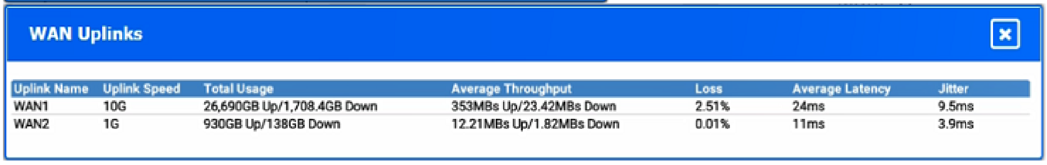




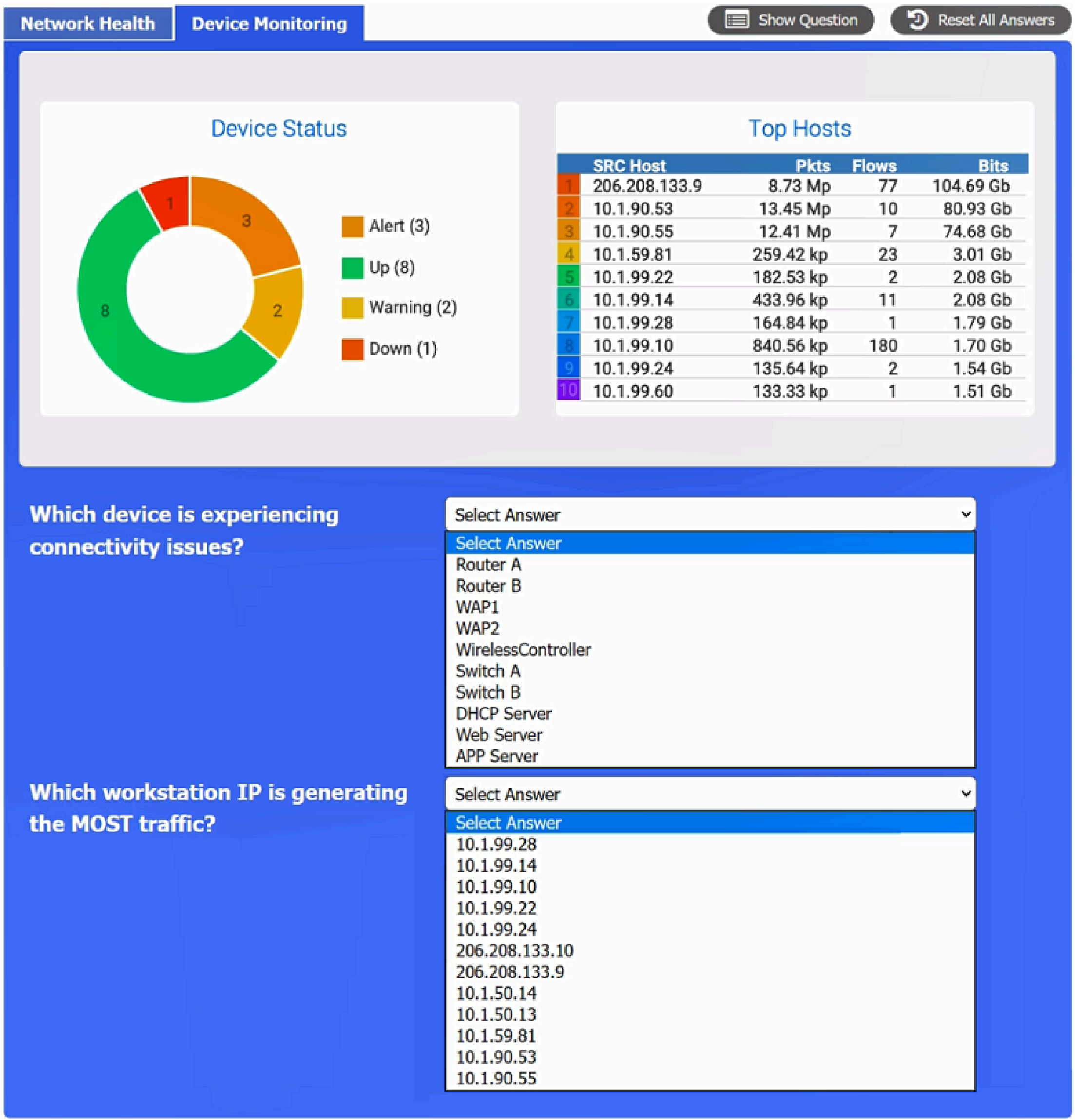








Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	Jitter
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9.5ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3.9ms



Device Status

🟧 Alert (3)
🟩 Up (8)
🟨 Warning (2)
🟥 Down (1)

Top Hosts

	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb
3	10.1.90.55	12.41 Mp	7	74.68 Gb
4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

Which device is experiencing connectivity issues?

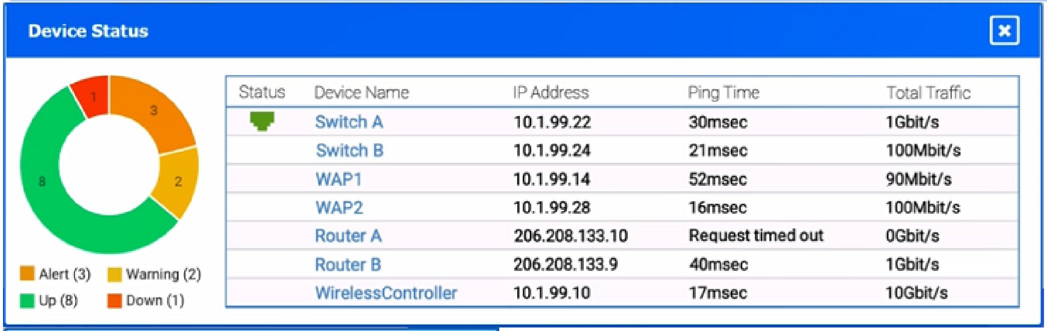
Select Answer

- Select Answer
- Router A
- Router B
- WAP1
- WAP2
- WirelessController
- Switch A
- Switch B
- DHCP Server
- Web Server
- APP Server

Which workstation IP is generating the MOST traffic?

Select Answer

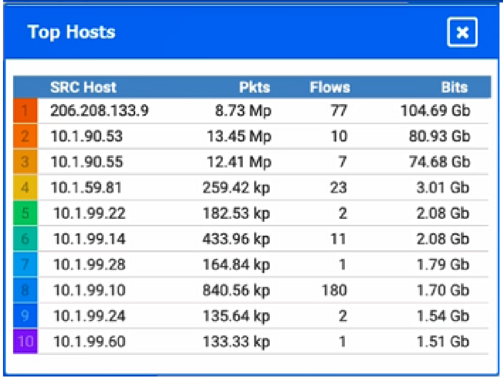
- Select Answer
- 10.1.99.28
- 10.1.99.14
- 10.1.99.10
- 10.1.99.22
- 10.1.99.24
- 206.208.133.10
- 206.208.133.9
- 10.1.50.14
- 10.1.50.13
- 10.1.59.81
- 10.1.90.53
- 10.1.90.55



Device Status

🟧 Alert (3) 🟨 Warning (2)
🟩 Up (8) 🟥 Down (1)

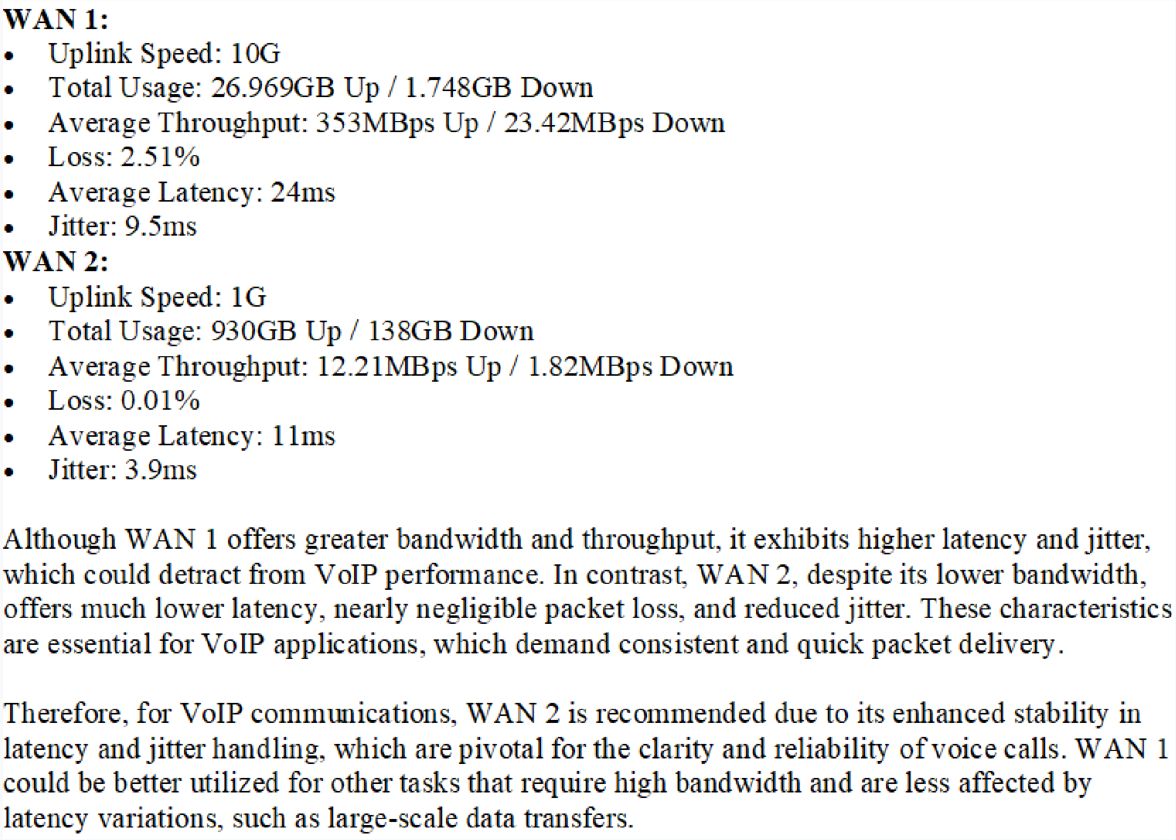
Status	Device Name	IP Address	Ping Time	Total Traffic
🖧	Switch A	10.1.99.22	30msec	1Gbit/s
	Switch B	10.1.99.24	21msec	100Mbit/s
	WAP1	10.1.99.14	52msec	90Mbit/s
	WAP2	10.1.99.28	16msec	100Mbit/s
	Router A	206.208.133.10	Request timed out	0Gbit/s
	Router B	206.208.133.9	40msec	1Gbit/s
	WirelessController	10.1.99.10	17msec	10Gbit/s



Top Hosts

	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb
3	10.1.90.55	12.41 Mp	7	74.68 Gb
4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

Correct Answer:



WAN 1:

- Uplink Speed: 10G
- Total Usage: 26.969GB Up / 1.748GB Down
- Average Throughput: 353MBps Up / 23.42MBps Down
- Loss: 2.51%
- Average Latency: 24ms
- Jitter: 9.5ms

WAN 2:

- Uplink Speed: 1G
- Total Usage: 930GB Up / 138GB Down
- Average Throughput: 12.21MBps Up / 1.82MBps Down
- Loss: 0.01%
- Average Latency: 11ms
- Jitter: 3.9ms

Although WAN 1 offers greater bandwidth and throughput, it exhibits higher latency and jitter, which could detract from VoIP performance. In contrast, WAN 2, despite its lower bandwidth, offers much lower latency, nearly negligible packet loss, and reduced jitter. These characteristics are essential for VoIP applications, which demand consistent and quick packet delivery.

Therefore, for VoIP communications, WAN 2 is recommended due to its enhanced stability in latency and jitter handling, which are pivotal for the clarity and reliability of voice calls. WAN 1 could be better utilized for other tasks that require high bandwidth and are less affected by latency variations, such as large-scale data transfers.

ojones888 Highly Voted 3 months, 3 weeks ago

The first answer is WAN 2. WAN 2 has better average throughput and less downtime which makes it better for VoIP traffic.

The second answer is Router A. Under ping time it says "request timed out" and total traffic is 0gbit/s. This means there is a connectivity issue.

The Third Answer is 206.208.133.9. This IP has 104.69gb of traffic making it the workstation with the most traffic.

upvoted 7 times

st1a 3 months, 1 week ago

3rd should be 10.1.90.53. the public ip belongs to a router interface, not workstation.

upvoted 15 times

Abx_01 Highly Voted 3 weeks ago

1. Which WAN station should be preferred for VoIP traffic? WAN2
2. Which device is experiencing connectivity issue? Router A (Ping test result)
3. Which workstation IP is generating most traffic? 10.1.90.53 (206.208.133.9 is a router not workstation)

upvoted 5 times

Azizuddeen Most Recent 1 month, 1 week ago

How do you determine what is a workstation?

upvoted 1 times

mo8888 1 month, 1 week ago

You do not need to determine it, it is the next busiest host after the router

upvoted 1 times

Question #7 *Topic 1*

Which of the following steps of the troubleshooting methodology would most likely include checking through each level of the OSI model after the problem has been identified?

A. Establish a theory.

B. Implement the solution.

C. Create a plan of action.

D. Verify functionality.

Correct Answer: *A*

Community vote distribution

A (62%) D (38%)

Community vote distribution

a484b2b Highly Voted 3 months, 4 weeks ago

I just passed N10-009 this past weekend, 11.9.24 using these questions. I studied the 159 questions and they were a lifesaver. I also got all 6 scenario questions, the first one was very complicated and I gave up and moved on. I saved the scenarios for last and they took 50 min to go through. Study all 159 questions the answers given. It's worth it. I got a 836 for my score even not doing well with a couple of the scenario questions!!

upvoted 17 times

Legacy_SOG 3 months, 3 weeks ago

Were the scenario based questions similar to the ones here?

upvoted 1 times

a484b2b 3 months, 2 weeks ago

exactly these questions

upvoted 5 times

Nyang2 Highly Voted 3 months, 3 weeks ago

https://www.comptia.org/blog/troubleshooting-methodology

1. Identify the problem
2. Establish a theory of probable cause ===> Answer : A
3. Test the theory to determine the cause
4. Establish a plan of action to resolve the problem and identify potential effects
5. Implement the solution or escalate as necessary
6. Verify full system functionality and, if applicable, implement preventive measures
7. Document findings, actions, outcomes and lessons learned

upvoted 9 times

93831b0 Most Recent 3 weeks, 6 days ago

Selected Answer: C

Here is my view on this one. Designing a methodical process to check each layer of the OSI model falls under "Create a plan of action." This step involves developing a thorough plan that includes troubleshooting each OSI layer to pinpoint the issue. You can look at it like drawing up a detailed blueprint for troubleshooting. You're outlining how you'll approach each layer if necessary.

upvoted 1 times

93831b0 2 weeks, 3 days ago

Changed my mind, A. establish a theory is the step where you try to determine the most likely cause of the identified problem. You use the information you've gathered to form a hypothesis about what's going wrong. Checking through each level of the OSI model is a common technique to systematically narrow down the possible causes and pinpoint the most probable one.

upvoted 1 times

PepeProblemas198753567 3 months ago

Selected Answer: A

The correct answer is A

(check Nyang2´s answer)

upvoted 2 times

lord_darth_vader 3 months ago

Selected Answer: A

A. Establish a theory

upvoted 2 times

b82faaf 3 months, 2 weeks ago

Selected Answer: A

A. Establish a theory

According to the CompTIA troubleshooting methodology, once the problem has been identified, the next step is to establish a theory of probable cause. This involves systematically analyzing the problem and narrowing down potential causes. Checking through each level of the OSI model is a common practice at this stage to identify where the issue might be occurring.

upvoted 2 times

Hayder81 3 months, 3 weeks ago

Establish a theory

chat gpt

upvoted 1 times

KD603 4 months ago

Selected Answer: A

The next step after identifying the problem is establishing a theory of probable cause which can include considering multiple approaches: top-to-bottom or bottom-to-top OSI model approaches. Verify functionality would include OSI model but only after implementing the solution which hasn't happened in this question

upvoted 3 times

ec80b38 4 months ago

The reason it is said to be A is because from comptias website under establish a theory "The steps in this phase are:

Questioning the obvious to identify the cause of the problem

Considering multiple approaches, including top-to-bottom or bottom-to-top for layered technologies (such as networks)"

upvoted 1 times

Dennizje 4 months, 1 week ago

Selected Answer: D

Correction, it's D

Verifying using the OSI model is explicitly mentioned in the troubleshooting methodology.

upvoted 4 times

Dennizje 4 months, 1 week ago

Selected Answer: A

Notice or identify problem, hypothesize possible cause, look for problem testing the possible cause, fix the problem, only then you verify the functionality.

upvoted 2 times

Dennizje 4 months, 1 week ago

Correction, it's D

Verifying using the OSI model is explicitly mentioned in the troubleshooting methodology.

upvoted 1 times

LilJuneBug 4 months, 1 week ago

is the answer not D?

upvoted 1 times

Intel_Geek 4 months, 2 weeks ago

Selected Answer: D

When verifying functionality after identifying a network problem, Checking each layer of the OSI model would be good to make sure the issue is fully resolved at every level of communication - please correct me if I am wrong

upvoted 1 times

chupapi_001 4 months, 2 weeks ago

Selected Answer: A

The correct answer is A: Establish a theory.

upvoted 3 times

LilJuneBug 4 months, 1 week ago

explain how?

upvoted 1 times

Question #8 *Topic 1*

While troubleshooting a VoIP handset connection, a technician's laptop is able to successfully connect to network resources using the same port. The technician needs to identify the port on the switch. Which of the following should the technician use to determine the switch and port?

A. LLDP

B. IKE

C. VLAN

D. netstat

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

⊟ **Intel_Geek** Highly Voted 4 months, 2 weeks ago

LLDP is the Link Layer Discovery Protocol, which is designed to discover neighboring network devices and their port details

IKE is used for establishing VPN connections, not related
VLAN logically separates network traffic, not related to identifying ports
netstat views network connections and statistics, not port information

upvoted 8 times

⊟ **khindinikorse** Most Recent 3 months, 2 weeks ago

Selected Answer: A

show lldp

upvoted 2 times

⊟ **chrys** 4 months ago

LLDP is perfect. IP phones don't necessarily support Cisco CDP, but they DO support LLDP. And you can configure both on your switch.

upvoted 1 times

⊟ **chupapi_001** 4 months, 2 weeks ago

Selected Answer: A

The correct answer is A: LLDP (Link Layer Discovery Protocol)

LLDP is specifically designed to help network devices advertise information about themselves and discover information about directly connected neighboring devices

upvoted 3 times

⊟ **nap61** 4 months, 2 weeks ago

Selected Answer: A

The Link Layer Discovery Protocol is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbours on a local area network based on IEEE 802
IKE - Internet Key Exchange - Not related to Switch
VLAN - Not related to identify Port in the switch
netstat - Identify logical ports in the computer/laptop, not in the switch

upvoted 3 times

Question #9 *Topic 1*

A network administrator needs to set up a file server to allow user access. The organization uses DHCP to assign IP addresses. Which of the following is the best solution for the administrator to set up?

A. A separate scope for the file server using a /32 subnet

B. A reservation for the server based on the MAC address

C. A static IP address within the DHCP IP range

D. A SLAAC for the server

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

BobbyCruz111 **Highly Voted 👍** 4 months ago

Selected Answer: B

DHCP Reservation: A DHCP reservation allows the administrator to assign a specific IP address to the file server based on its MAC address. This means that the file server will always receive the same IP address from the DHCP server, ensuring stable and predictable access for users while still utilizing DHCP for address management.

upvoted 7 times

chrys **Most Recent ⏲** 4 months ago

DHCP reservation is perfect. That way, if you change scope options, you don't have to go manually configuring it on all your servers.

upvoted 2 times

chupapi_001 4 months, 2 weeks ago

Selected Answer: B

The correct answer is B: A reservation for the server based on the MAC address.

upvoted 1 times

Question #10 *Topic 1*

Which of the following technologies are X.509 certificates most commonly associated with?

A. PKI

B. VLAN tagging

C. LDAP

D. MFA

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

Abx_01 3 weeks ago

Selected Answer: A

Public Key Infrastructure (PKI) is the set of technology and processes required to secure environments with high assurance to control access to systems

upvoted 1 times

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. public-key infrastructure (PKI)

The system for creating and distributing digital certificates issued by trusted third parties such as DigiCert, GoDaddy, or Sectigo.

upvoted 1 times

BobbyCruz111 4 months ago

Selected Answer: A

PKI is the answer
due to it using X509 certs

upvoted 4 times

chrys 4 months ago

Yep. PKI uses X.509 certs.

upvoted 1 times

chupapi_001 4 months, 2 weeks ago

Selected Answer: A

The correct answer is A: PKI (Public Key Infrastructure)

The other options are less suitable because:

VLAN tagging (B): This is a networking concept unrelated to certificate-based security
LDAP (C): While LDAP can use certificates, it's primarily a directory service protocol
MFA (D): While certificates can be used in MFA, they are just one of many possible authentication factors

upvoted 4 times

Question #11 *Topic 1*

A network administrator wants to implement an authentication process for temporary access to an organization's network. Which of the following technologies would facilitate this process?

A. Captive portal

B. Enterprise authentication

C. Ad hoc network

D. WPA3

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

chupapi_001 Highly Voted 4 months, 2 weeks ago

Selected Answer: A

The correct answer is A: Captive portal.

Captive portals are specifically designed for temporary access management.

The other options are less suitable because:

Enterprise authentication (B): This is more suited for permanent employees and requires complex setup
Ad hoc network (C): This refers to a temporary network structure, not an authentication method
WPA3 (D): This is an encryption standard for securing wireless networks, not specifically for managing temporary access
upvoted 7 times

HeatSquad77 Most Recent 2 months, 1 week ago

Selected Answer: A

A. captive portal

A Wi-Fi network implementation used in some public facilities that directs attempts to connect to the network to an internal Web page for that facility; generally used to force terms of service on users.
upvoted 2 times

favouralain 3 months, 2 weeks ago

Selected Answer: A

A captive portal is a web page that users see before accessing a public network. Users typically need to provide some form of authentication, such as logging in with temporary credentials, before they can access the network. This is particularly useful for temporary access as it can be used to enforce network access policies and gather user information.
upvoted 1 times

chrys 4 months ago

Captive portal is what we all do. It's easy, self-service, and you can log MAC addresses and user email addresses without any work on your part.
upvoted 1 times

Question #12 *Topic 1*

A user is unable to navigate to a website because the provided URL is not resolving to the correct IP address. Other users are able to navigate to the intended website without issue. Which of the following is most likely causing this issue?

A. Hosts file

B. Self-signed certificate

C. Nameserver record

D. IP helper

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. hosts file

The predecessor to DNS, a static text file that resides on a computer and is used to resolve DNS hostnames to IP addresses. Automatically mapped to a host’s DNS resolver cache in modern systems. The hosts file has no extension.

upvoted 4 times

chrys 4 months ago

Hosts file is checked before DNS. It's actually a fun and simple way to hack a system. I had to use it once to keep users from using a PC running an XRAY controller to get on Facebook and other social media sites. Quick 'n' dirty ;-)

upvoted 2 times

chupapi_001 4 months, 2 weeks ago

Selected Answer: A

The hosts file is a local system file that maps hostnames to IP addresses and can override normal DNS resolution
. When only one user is experiencing resolution issues while others can access the website normally, this strongly suggests a local configuration problem rather than a network-wide DNS issue.

upvoted 4 times

Question #13 *Topic 1*

A network administrator is planning to host a company application in the cloud, making the application available for all internal and third-party users. Which of the following concepts describes this arrangement?

A. Multitenancy

B. VPC

C. NFV

D. SaaS

Correct Answer: *D*

Community vote distribution

D (57%) A (43%)

Community vote distribution

⊟ **TheSplurge** Highly Voted 2 months ago

Selected Answer: A

While SaaS and Multitenancy have similar definitions SaaS would more so be the actual delivery of the model, or the accessing of the service while multitenancy describes the scenario of an admin hosting this application.

upvoted 7 times

⊟ **TheSplurge** 2 months ago

-From what I gathered from chat gpt

upvoted 3 times

⊟ **2fd1029** 2 months ago

Piss off with the ChatGPT answer. ChatGPT gets things wrong all the time and there's a chance you're screwing people over with your misinformation.

upvoted 7 times

⊟ **GEO2** Most Recent 1 month, 1 week ago

Selected Answer: A

Multitenancy is a cloud computing concept where a single instance of an application serves multiple users (tenants). In this case, the company application is hosted in the cloud and is available for both internal users and third-party users, meaning it supports multiple groups (or tenants) sharing the same application infrastructure while keeping their data isolated.

Why not the others?

D. SaaS (Software as a Service): While this application might be offered as a SaaS product, the question focuses on the arrangement where multiple users access the same hosted application, which aligns better with multitenancy.

Key Takeaway:
Multitenancy ensures efficient resource usage in cloud environments while securely serving multiple user groups or organizations.

upvoted 3 times

⊟ **jmcd2** 1 month, 3 weeks ago

Selected Answer: A

A.
third party users that means people outside the company. Multitenancy is the best answer.

upvoted 4 times

⊟ **kinkistyle** 1 month, 3 weeks ago

Selected Answer: D

SaaS. Multitenancy is like an apartment building where all the tenants live in the same building and share the same infrastructure but everybody is lives in their own locked apartments. SaaS is what the company is doing which is serving applications to users from the cloud.

upvoted 3 times

braveheart22 1 month, 3 weeks ago

Selected Answer: D

I'm super convinced with "lockjaw's" explanation, so from my point of view, I feel SaaS is the correct answer, so I will go with D.

upvoted 1 times

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. multitenancy

The ability to support multiple customers on the same infrastructure at the same time. Multitenancy enables customers with small computing needs to only pay for what they actually need in exchange for sharing the same infrastructure with other customers. Comes with the risk those customers will hog shared resources or compromise the infrastructure (by accident or on purpose).

upvoted 1 times

Lailo 2 months, 2 weeks ago

Selected Answer: A

A. Multitenancy. is the correct answer

upvoted 1 times

ba10f26 2 months, 3 weeks ago

Selected Answer: A

The correct answer is:
A. Multitenancy.

Multitenancy describes a cloud computing architecture where multiple users or organizations (tenants) share the same application or infrastructure while keeping their data and configurations separate. Hosting a company application in the cloud for internal and third-party users aligns with this concept, as the application serves multiple distinct user groups on a shared platform.

upvoted 2 times

> **lockjaw** 2 months, 1 week ago
>
> I see your point about multitenancy, which indeed involves multiple users or organizations sharing the same application or infrastructure while keeping their data separate. However, in the context of making an application available to all internal and third-party users, SaaS (Software as a Service) is the more accurate concept. SaaS specifically refers to delivering applications over the internet, allowing users to access them without managing the underlying infrastructure.
>
> Multitenancy is a characteristic of many SaaS applications, but SaaS itself describes the delivery model you're referring to.
>
> upvoted 1 times

Parshman 2 months, 3 weeks ago

Selected Answer: A

One resource pool with multiple tenants, so multi-tenancy would be the best answer.

upvoted 2 times

gregrhernandez07 2 months, 3 weeks ago

Selected Answer: A

Multitenancy.
Explanation:
Multitenancy refers to a cloud computing architecture where a single instance of an application serves multiple customers, with each customer's data kept separate and secure from the others. This is the most suitable description for the scenario given, as the administrator wants to make the application accessible to various users while maintaining data isolation.

upvoted 2 times

Nyang2 3 months, 1 week ago

Selected Answer: D

SaaS cannot service a company application.
So answer sould be A

upvoted 3 times

> **Nyang2** 3 months, 1 week ago
>
> Not D.
> A!
>
> upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

Multitenancy refers to a cloud architecture where multiple users (tenants) share the same application or resources while maintaining data and access separation. In this scenario, hosting the application in the cloud for both internal and third-party users aligns with the concept of multitenancy, as the same application instance will likely serve different groups of users.

upvoted 2 times

> **SuntzuLegacy** 3 months, 1 week ago
>
> D. SaaS (Software as a Service)
>
> Explanation:
>
> The key aspect of the question is that the company application is being hosted in the cloud and made available for internal and third-party users.
>
> upvoted 2 times

favouralain 3 months, 2 weeks ago

Selected Answer: D

SaaS is the best answer

upvoted 4 times

chrys 4 months ago

SaaS! One app, no pain.

upvoted 2 times

a01561f 4 months, 1 week ago

Software as a Service essentially making an App in the cloud

upvoted 1 times

Question #14 Topic 1

Which of the following should be used to obtain remote access to a network appliance that has failed to start up properly?

A. Crash cart

B. Jump box

C. Secure Shell

D. Out-of-band management

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

⊟ **chupapi_001** Highly Voted 4 months, 2 weeks ago

Selected Answer: D

The correct answer is D: Out-of-band management (OOB).

OOB management provides access to devices even when they are:

Powered down
Unresponsive
Without an operating system
Unable to start properly

Crash cart (A): Requires physical presence at the device location
Jump box (B): While related to OOB, it's just one component and requires a functioning network4
Secure Shell (C): Requires the device to be operational and the OS to be functioning

upvoted 10 times

⊟ **HeatSquad77** Most Recent 2 months, 1 week ago

Selected Answer: D

D. out-of-band management

Method to connect to and administer a managed device such as a switch or router that does not use a standard network-connected host as the administrative console. A computer connected to the console port of a switch is an example of out-of-band management

upvoted 1 times

⊟ **ba10f26** 2 months, 3 weeks ago

Selected Answer: D

The correct answer is:
D. Out-of-band management.

Out-of-band management allows administrators to access and manage network appliances remotely, even when the device has not started up properly or is not functioning on the primary network. It typically uses a dedicated management interface separate from the regular network traffic, enabling troubleshooting and configuration in such scenarios.

upvoted 1 times

Question #15 *Topic 1*

Which of the following attacks utilizes a network packet that contains multiple network tags?

A. MAC flooding

B. VLAN hopping

C. DNS spoofing

D. ARP poisoning

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: B

B. VLAN hopping

A Layer 2 attack that enables an attacker to access hosts on a VLAN the attacker is not a part of. Traditionally this attack used switch spoofing or double tagging.

upvoted 3 times

bg5850 3 months, 2 weeks ago

Selected Answer: B

Lets Goo Vlan Hop

upvoted 1 times

chrys 4 months ago

VLAN hopping, baby!

upvoted 1 times

chupapi_001 4 months, 2 weeks ago

Selected Answer: B

The correct answer is B: VLAN hopping

upvoted 1 times

Question #16 *Topic 1*

A network administrator is configuring a new switch and wants to connect two ports to the core switch to ensure redundancy. Which of the following configurations would meet this requirement?

A. Full duplex

B. 802.1Q tagging

C. Native VLAN

D. Link aggregation

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

chupapi_001 Highly Voted 4 months, 2 weeks ago

Selected Answer: D

The correct answer is D: Link aggregation.

upvoted 5 times

HeatSquad77 Most Recent 2 months, 1 week ago

Selected Answer: D

D. link aggregation

Connecting multiple NICs in tandem to increase bandwidth in smaller increments

upvoted 1 times

favouralain 3 months, 2 weeks ago

Selected Answer: D

Link aggregation is the combining of multiple network connections in parallel by any of several methods.

upvoted 1 times

Question #17 *Topic 1*

Which of the following ports is used for secure email?

A. 25

B. 110

C. 143

D. 587

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

Intel_Geek Highly Voted 👍 4 months, 2 weeks ago

Selected Answer: D

Port 25 is for SMTP, now considered insecure

Port 110 is associated with POP3 which retrieves emails but is only secure with additional encryption

Port 143 is associated with IMAP, without encryption

Port 587 is the secure version of SMTP and uses TLS encryption

upvoted 6 times

HeatSquad77 Most Recent 🕘 1 month, 4 weeks ago

Selected Answer: D

D. simple mail transfer protocol (SMTP)

Application protocol used to send mail between hosts on the Internet. Messages are sent between servers over TCP port 25 or submitted by a mail client over secure port TCP/587.

upvoted 1 times

chupapi_001 4 months, 2 weeks ago

Selected Answer: D

The correct answer is D: Port 587.

upvoted 4 times

Question #18 *Topic 1*

A client wants to increase overall security after a recent breach. Which of the following would be best to implement? (Choose two.)

A. Least privilege network access

B. Dynamic inventories

C. Central policy management

D. Zero-touch provisioning

E. Configuration drift prevention

F. Subnet range limits

Correct Answer: *AC*

Community vote distribution

AC (100%)

Community vote distribution

CISUMPATR 4 weeks ago

Selected Answer: AC

Definitely A and C

upvoted 1 times

kinkistyle 1 month, 3 weeks ago

Selected Answer: AC

Least privilege.

Central Policy Management which will make it easier to enforce security policies through the entire network

upvoted 1 times

Coburn 1 month, 3 weeks ago

Selected Answer: AE

A: Least privilege network access as that's an efficient way to reduce unnecessary permissions being used on the network, and reduces the likelihood of an inside threat or social engineer gaining elevated credentials.

E: Configuration drift prevention as that can mean configurations not matching or updated to the baseline or golden configuration, which should be the most secure within the organization.

upvoted 1 times

mmmpeanutbuttercrunch 2 months, 3 weeks ago

Selected Answer: AC

A: Least Privilege

C: Central Policy Management

These two answers best align with what the question is asking: "overall security". All other options are more specific than these two.

upvoted 2 times

Parshman 2 months, 3 weeks ago

Selected Answer: AE

A: Least privilege network access as that's an efficient way to reduce unnecessary permissions being used on the network, and reduces the likelihood of an inside threat or social engineer gaining elevated credentials.

E: Configuration drift prevention as that can mean configurations not matching or updated to the baseline or golden configuration, which should be the most secure within the organization.

upvoted 2 times

chupapi_001 4 months, 2 weeks ago

Selected Answer: AC

A. Least privilege network access

C. Central policy management

upvoted 3 times

Question #19 *Topic 1*

Which of the following is a cost-effective advantage of a split-tunnel VPN?

A. Web traffic is filtered through a web filler.

B. More bandwidth is required on the company's internet connection.

C. Monitoring detects insecure machines on the company's network.

D. Cloud-based traffic flows outside of the company's network.

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

chupapi_001 Highly Voted 4 months, 2 weeks ago

Selected Answer: D

The correct answer is D. Cloud-based traffic flows outside of the company's network.

Split-tunnel VPNs provide cost savings primarily because they reduce the bandwidth load on the company's network by allowing non-essential traffic to flow directly to the internet.

upvoted 8 times

kinkistyle Most Recent 1 month, 3 weeks ago

Selected Answer: D

D is the only answer that has anything to do with an advantage of Split Tunnel VPN's

upvoted 1 times

Parshman 2 months, 3 weeks ago

Selected Answer: D

I chose D because split tunnel VPNs only encrypt the critical traffic within the company's tunnel. The data that isn't encrypted is non-essential, allowing the company to save on overhead and resources by having to encrypt less data.

upvoted 2 times

Question #20 *Topic 1*

A network technician is troubleshooting a web application's poor performance. The office has two internet links that share the traffic load. Which of the following tools should the technician use to determine which link is being used for the web application?

A. netstat

B. nslookup

C. ping

D. tracert

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: D

D. tracert (also traceroute)

A command-line utility used to follow the path a packet takes between two hosts.

upvoted 1 times

chupapi_001 4 months, 2 weeks ago

Selected Answer: D

Tracert shows the exact route that packets take from source to destination, including all intermediate routers and network links

upvoted 4 times

Question #21 *Topic 1*

Which of the following attacks can cause users who are attempting to access a company website to be directed to an entirely different website?

A. DNS poisoning

B. Denial-of-service

C. Social engineering

D. ARP spoofing

Correct Answer: *A*

Community vote distribution

A (83%) D (17%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. DNS cache poisoning

Also known as DNS poisoning, an attack that adds or changes information in a DNS server's cache to point hostnames to incorrect IP addresses, under the attacker's control. When a client requests an IP address from this DNS server for a Web site, the poisoned server hands out an IP address of an attacker machine, not the legitimate site. When the client subsequently visits the attacker site, they become vulnerable to a number of threats including malware.

upvoted 2 times

ba10f26 2 months, 3 weeks ago

Selected Answer: A

The correct answer is:
A. DNS poisoning.

DNS poisoning (or DNS spoofing) involves corrupting the DNS cache or records to redirect users from a legitimate website to a fraudulent or malicious website. This type of attack can deceive users and potentially capture sensitive information.

upvoted 1 times

BobbyCruz111 4 months ago

Selected Answer: A

DNS Poisoning

upvoted 1 times

Dennizje 4 months, 1 week ago

Selected Answer: A

It is DNS poisoning, the DNS is generally what the user is clicking on in good faith.

upvoted 1 times

Intel_Geek 4 months, 2 weeks ago

Selected Answer: A

a

upvoted 3 times

Intel_Geek 4 months, 2 weeks ago

Selected Answer: D

DNS poisoning redirects your URL to a malicious website when trying to access a regular one,

upvoted 1 times

chupapi_001 4 months, 2 weeks ago

The correct answer is A. DNS poisoning

DNS poisoning is a type of cyber attack that specifically causes users to be redirected to malicious websites when they attempt to access legitimate ones.

upvoted 2 times

Question #22 *Topic 1*

As part of an attack, a threat actor purposefully overflows the content-addressable memory (CAM) table on a switch. Which of the following types of attacks is this scenario an example of?

A. ARP spoofing

B. Evil twin

C. MAC flooding

D. DNS poisoning

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

ba10f26 2 months, 3 weeks ago

Selected Answer: C

The correct answer is:

C. MAC flooding.

MAC flooding is an attack where a threat actor overwhelms a switch's content-addressable memory (CAM) table by sending numerous fake MAC addresses. This causes the switch to fail and behave like a hub, broadcasting traffic to all ports, which allows the attacker to potentially capture sensitive data through network traffic interception.

upvoted 1 times

chupapi_001 4 months, 2 weeks ago

Selected Answer: C

The correct answer is C. MAC flooding

MAC flooding is a type of network attack that specifically targets a switch's Content-Addressable Memory (CAM) table by overwhelming it with fake MAC addresses.

upvoted 3 times

Question #23 *Topic 1*

A company's office has publicly accessible meeting rooms equipped with network ports. A recent audit revealed that visitors were able to access the corporate network by plugging personal laptops into open network ports. Which of the following should the company implement to prevent this in the future?

A. URL filters

B. VPN

C. ACLs

D. NAC

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

kinkistyle 1 month, 3 weeks ago

Selected Answer: D

NAC is the right choice

upvoted 1 times

HeatSquad77 2 months, 1 week ago

Selected Answer: D

D. network access control (NAC)

Control over information, people, access, machines, and everything in between

upvoted 2 times

BobbyCruz111 4 months ago

Selected Answer: D

NAC - Network Access Control. Even though the users can still plug into the ports they will not be authenticated to be connected and use the network

upvoted 4 times

chupapi_001 4 months, 2 weeks ago

Selected Answer: D

The correct answer is D. NAC (Network Access Control)

upvoted 2 times

Question #24 *Topic 1*

A user notifies a network administrator about losing access to a remote file server. The network administrator is able to ping the server and verifies the current firewall rules do not block access to the network fileshare. Which of the following tools would help identify which ports are open on the remote file server?

A. dig

B. nmap

C. tracert

D. nslookup

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: B

B. network map

A highly detailed illustration of a network, down to the individual computers. A network map shows IP addresses, ports, protocols, and more.

upvoted 1 times

BobbyCruz111 4 months ago

Selected Answer: B

NMAP- It will allow for scanning of ports that are open. Great tool for listening and can be used for malicious purposes as well.

upvoted 2 times

chupapi_001 4 months, 2 weeks ago

Selected Answer: B

The correct answer is B. nmap

Nmap (Network Mapper) is the most appropriate tool for identifying open ports on the remote file server.

upvoted 1 times

Question #25 *Topic 1*

Which of the following technologies is the best choice to listen for requests and distribute user traffic across web servers?

A. Router

B. Switch

C. Firewall

D. Load balancer

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

⊟ **HeatSquad77** 2 months, 1 week ago

Selected Answer: D

D. load balancing

The process of taking several servers and making them look like a single server, spreading processing and supporting bandwidth needs.

upvoted 1 times

⊟ **BobbyCruz111** 4 months ago

Selected Answer: D

Load Balancer balances the load which it is listening for incoming requests and then distributes it evenly so that a single server does not crash due to excessive load.

upvoted 1 times

⊟ **chupapi_001** 4 months, 2 weeks ago

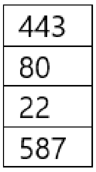
Selected Answer: D

the correct answer is D. Load balancer.

upvoted 2 times

Question #26 *Topic 1*

A company is hosting a secure server that requires all connections to the server to be encrypted. A junior administrator needs to harden the web server. The following ports on the web server are open:



443
80
22
587

Which of the following ports should be disabled?

A. 22

B. 80

C. 443

D. 587

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

kinkistyle 1 month, 3 weeks ago

Selected Answer: B

Only unsecure port is B

upvoted 1 times

jamjam8148 2 months, 2 weeks ago

Selected Answer: B

B is the only unsecured option (HTTP)

upvoted 1 times

BobbyCruz111 4 months ago

Port 80 is the unsecure port of HTTPS hence port 80 is HTTP. This port out of all the other ports are unsecure.

22- ssh secure

443- https secure

587- SMTPS Secure version of STMP

upvoted 2 times

Intel_Geek 4 months, 2 weeks ago

Selected Answer: B

Port 80 is an insecure hypertext transfer protocol

upvoted 1 times

Question #27 *Topic 1*

Which of the following is the next step to take after successfully testing a root cause theory?

A. Determine resolution steps.

B. Duplicate the problem in a lab.

C. Present the theory for approval.

D. Implement the solution to the problem.

Correct Answer: *A*

Community vote distribution

A (73%) D (27%)

Community vote distribution

FrostyBoi Highly Voted 4 months ago

Selected Answer: A

From CompTIA's website, the troubleshooting steps are as follows:

1.) Identify the problem

2.) Establish a theory of probable cause

3.) Test the theory to determine the cause

4.) Establish a plan of action to resolve the problem

5.) Implement the solution and escalate if necessary

6.) Verify full system functionality, and if possible implement preventative measures

7.) Document findings, actions, outcomes, and lessons learned.

With this in mind, A would be the correct answer, as it would be establishing a plan of action after testing the theory to determine the cause of the problem.

upvoted 12 times

kinkistyle Most Recent 1 month, 3 weeks ago

Selected Answer: A

After testing the theory comes establishing a plan of action, which is A.

upvoted 1 times

Coburn 1 month, 3 weeks ago

Selected Answer: D

After identifying the "root cause" in a root cause analysis, the next step is to develop and implement solutions that directly address the underlying cause to prevent the problem from recurring

upvoted 1 times

ba10f26 2 months, 3 weeks ago

Selected Answer: A

With the information provided from the CompTIA troubleshooting steps, the correct answer:

A. Determine resolution steps.

This step aligns with CompTIA's methodology: after testing the theory and determining the root cause, the next logical step is to establish a plan of action to resolve the problem, before implementing the solution. This ensures a clear, organized approach to addressing the issue.

upvoted 2 times

favouralain 3 months, 2 weeks ago

Selected Answer: A

Determine resolution steps. This involves figuring out the specific actions needed to fix the identified root cause of the problem. Once you have a clear plan of resolution, you can then proceed to implement the solution.

upvoted 2 times

BobbyCruz111 4 months ago

Selected Answer: A

Once the root cause theory has been successfully tested and confirmed, the next logical step is to determine the resolution steps. These steps involve identifying how to fix the problem, including creating a plan to address the issue, implementing the solution, and ensuring that the solution will effectively resolve the issue without causing new problems.

upvoted 2 times

BobbyCruz111 4 months ago

Explanation of the other options:
B. Duplicate the problem in a lab: This step is typically taken earlier in the troubleshooting process when you're trying to recreate the issue in a controlled environment to better understand its causes. After confirming the root cause theory, you don't need to duplicate the problem again; you're already at the point where you know what the issue is.

C. Present the theory for approval: While presenting the theory for approval might be important in some organizational settings (particularly for formal change management), it's not typically the next step after confirming the root cause. At this stage, you would already have the necessary buy-in to proceed with resolution steps.

D. Implement the solution to the problem: Implementing the solution is a crucial step, but it comes after determining the specific resolution steps. First, you need to decide on the best course of action, including testing and validating the solution, and then implement it in a controlled way.

upvoted 2 times

ojones888 4 months, 1 week ago

Selected Answer: D

After successfully testing a root cause theory and confirming it explains the issue, the next step is to implement the solution. This involves applying the fix based on the validated theory to resolve the problem.

The other options do not directly follow testing a confirmed root cause theory:

A. Determine resolution steps: This would occur before testing the solution.
B. Duplicate the problem in a lab: This is typically done earlier to diagnose or test hypotheses.
C. Present the theory for approval: This might be necessary in some cases, but the next logical step in troubleshooting is usually implementing the solution.

upvoted 4 times

chupapi_001 4 months, 1 week ago

Selected Answer: A

A. Determine resolution steps.

upvoted 1 times

Question #28 *Topic 1*

A network administrator is configuring a new switch and wants to ensure that only assigned devices can connect to the switch. Which of the following should the administrator do?

A. Configure ACLs.

B. Implement a captive portal.

C. Enable port security.

D. Disable unnecessary services.

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

⊟ **BobbyCruz111** Highly Voted 👍 4 months ago

Selected Answer: C

Port security is a feature available on most network switches that allows you to control which devices can connect to a particular switch port based on MAC addresses. By enabling port security, the network administrator can restrict each port to only allow a specific set of MAC addresses, ensuring that only authorized devices can connect. If an unauthorized device tries to connect, the switch can take actions such as shutting down the port, dropping the traffic, or sending an alert.

upvoted 6 times

⊟ **chupapi_001** Most Recent ⏲ 4 months, 1 week ago

Selected Answer: C

The correct answer is C. Enable port security.

upvoted 1 times

Question #29 *Topic 1*

A customer needs six usable IP addresses. Which of the following best meets this requirement?

A. 255.255.255.128

B. 255.255.255.192

C. 255.255.255.224

D. 255.255.255.240

Correct Answer: *D*

Community vote distribution

D (60%) C (40%)

Community vote distribution

kinkistyle 1 month, 3 weeks ago

Selected Answer: D

The ideal mask would be 255.255.255.248 which would give us exactly the right amount of usable addresses at 6, but the next best is D. with 14 usable address

upvoted 2 times

Philco 1 month, 3 weeks ago

Selected Answer: C

Since you need 6 IP addresses, the closest power of 2 that can accommodate that is 2^3 (which equals 8), meaning you need 3 host bits

upvoted 1 times

Philco 1 month, 1 week ago

sorry , 2nd thoughts I am wrong

the correct answer would have been 255.255.255.248

since it is not available --- the next best one is D

upvoted 1 times

Philco 1 month ago

Subnet Masks Avail.- IP's Networks Cidr
255.255.255.252 4-2 64 /30
255.255.255.248 8-2 32 /29
255.255.255.240 16-2 16 /28
255.255.255.224 32-2 8 /27
255.255.255.192 64-2 4 /26
255.255.255.128 128-2 2 /25
255.255.255.0 256-2 1 /24

upvoted 1 times

ba10f26 2 months, 3 weeks ago

Selected Answer: D

Correct Answer: D

255.255.255.240 provides 14 usable IP addresses, which is more than enough for the 6 usable IPs the customer needs.
This option is more efficient compared to 255.255.255.224, which provides 30 usable IPs and would waste a larger number of addresses.

upvoted 1 times

Powerserg28 2 months, 4 weeks ago

Selected Answer: D

255.255.255.240 = 11111111.1111111.1111111.11110000
Number of networks = 2^n; n = on bits (1); 2^4 = 16
Number of host = (2^n) - 2; n = off bits (0); (2^4) - 2 = 14

upvoted 3 times

S1vu 4 months ago

Selected Answer: D

255.255.255.240 (Option D) is the most efficient choice, as it provides 14 usable addresses, which meets the requirement without wasting too many additional addresses.

upvoted 1 times

S1vu 4 months ago

Correct answer is D (14 addresses), It is the closest to 6 usable IP addresses without wasting any additional addresses

upvoted 1 times

BobbyCruz111 4 months ago

Selected Answer: C

The subnet mask 255.255.255.224 (option C) provides 6 usable IP addresses, which is exactly what the customer needs.

255.255.255.240 (option D) provides 14 usable IPs, which is more than needed.
So, C. 255.255.255.224 is the best answer for 6 usable IP addresses.

upvoted 2 times

Army_Germ 3 months, 2 weeks ago

C provides 6 networks not usable addresses.

upvoted 1 times

ilikeyou 3 months, 3 weeks ago

Wrong-Option C /27 provides 30 usable hosts. However, /29 provides exactly 6 usable host addresses, which is not an option here. Therefore option D is correct.

upvoted 1 times

chupapi_001 4 months, 1 week ago

Selected Answer: D

Since the customer needs 6 usable IP addresses, we should choose the smallest subnet that can accommodate this requirement while minimizing wasted addresses. 255.255.255.240 provides 14 usable addresses, which is the closest match to the requirement of 6 addresses.

upvoted 1 times

Question #30 Topic 1

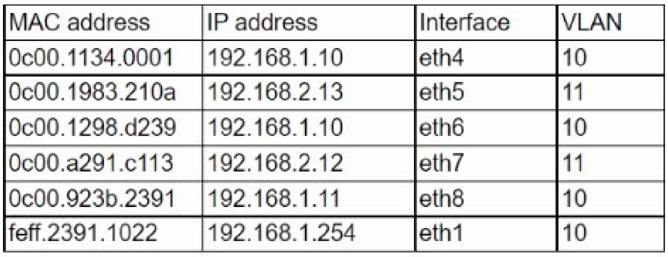
A user reports having intermittent connectivity issues to the company network. The network configuration for the user reveals the following:

IP address: 192.168.1.10 -

Subnet mask: 255.255.255.0 -

Default gateway: 192.168.1.254 -

The network switch shows the following ARP table:



MAC address	IP address	Interface	VLAN
0c00.1134.0001	192.168.1.10	eth4	10
0c00.1983.210a	192.168.2.13	eth5	11
0c00.1298.d239	192.168.1.10	eth6	10
0c00.a291.c113	192.168.2.12	eth7	11
0c00.923b.2391	192.168.1.11	eth8	10
feff.2391.1022	192.168.1.254	eth1	10

Which of the following is the most likely cause of the user's connection issues?

A. A port with incorrect VLAN assigned

B. A switch with spanning tree conflict

C. Another PC with manually configured IP

D. A router with overlapping route tables

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

chupapi_001 Highly Voted 4 months, 1 week ago

Selected Answer: C

The correct answer is C.

Another PC with manually configured IP. Looking at the ARP table provided in the image, we can identify the issue:

There are two devices with the same IP address (192.168.1.10):
One device with MAC address 0c:00.1134.0001 on eth4
Another device with MAC address 0c:00.1298.d239 on eth6
This is a clear case of an IP address conflict where:
Both devices are trying to use 192.168.1.10
Both are on VLAN 10
Different physical ports (eth4 and eth6)

upvoted 7 times

Question #31 *Topic 1*

Which of the following is created to illustrate the effectiveness of wireless networking coverage in a building?

A. Logical diagram

B. Layer 3 network diagram

C. Service-level agreement

D. Heat map

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

2fd1029 2 months ago

Selected Answer: D

A heat map would be used to determine this.

upvoted 1 times

chupapi_001 4 months, 1 week ago

Selected Answer: D

The correct answer is D. Heat map

upvoted 3 times

Question #32 *Topic 1*

Which of the following cloud deployment models is most commonly associated with multitenancy and is generally offered by a service provider?

A. Private

B. Community

C. Public

D. Hybrid

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

ba10f26 2 months, 3 weeks ago

Selected Answer: C

The correct answer is:

C. Public.

The public cloud deployment model is most commonly associated with multitenancy and is generally offered by a service provider. In this model, multiple organizations (tenants) share the same infrastructure and resources while keeping their data separate. Examples include cloud services like AWS, Microsoft Azure, and Google Cloud.

upvoted 3 times

chupapi_001 4 months, 1 week ago

Selected Answer: C

The correct answer is C. Public

upvoted 1 times

Question #33 *Topic 1*

A network administrator needs to create an SVI on a Layer 3-capable device to separate voice and data traffic. Which of the following best explains this use case?

A. A physical interface used for trunking logical ports

B. A physical interface used for management access

C. A logical interface used for the routing of VLANs

D. A logical interface used when the number of physical ports is insufficient

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

ba10f26 2 months, 3 weeks ago

Selected Answer: C

The correct answer is:

C. A logical interface used for the routing of VLANs.

A Switch Virtual Interface (SVI) is a logical interface configured on a Layer 3 switch to provide inter-VLAN routing. By creating an SVI, the network administrator can separate voice and data traffic into different VLANs and enable communication between them through the Layer 3 device.

upvoted 4 times

chupapi_001 4 months, 1 week ago

Selected Answer: C

The correct answer is C. A logical interface used for the routing of VLANs

upvoted 4 times

Question #34 *Topic 1*

A network administrator is performing a refresh of a wireless environment. As the APs are being placed, they overlap a little bit with each other. Which of the following 2.4GHz channels should be selected to ensure that they do not conflict?

A. 1, 3, 5

B. 1, 6, 11

C. 2, 6, 10

D. 3, 6, 9

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

chupapi_001 4 months, 1 week ago

Selected Answer: B

The correct answer is B. 1, 6, 11

upvoted 2 times

Question #35 *Topic 1*

Which of the following network cables involves bouncing light off of protective cladding?

A. Twinaxial

B. Coaxial

C. Single-mode

D. Multimode

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

penguin4121 1 week, 2 days ago

Selected Answer: D

SINGLE MODE!!! It has the peculiarity that inside of its core, data travels WITHOUT bouncing off of its walls which allows and maintains higher transfer speeds

upvoted 1 times

penguin4121 1 week, 2 days ago

EDIT, singlemode does not bounce while multi does, i answered D which is the right answer but said single... it is multi.

upvoted 1 times

FrozenCarrot 1 month, 1 week ago

Selected Answer: D

The correct answer is D. Multimode.

Explanation:

Multimode fiber optic cables use a larger core (typically 50 or 62.5 microns) that allows light signals to travel in multiple paths (modes). These signals bounce off the protective cladding (due to total internal reflection) as they propagate, which is a defining characteristic of multimode fibers. In contrast, single-mode fiber (C) has a much smaller core (9 microns) and uses a single, direct path for light with minimal reflection. Twinaxial (A) and Coaxial (B) cables transmit electrical signals, not light, and are unrelated to fiber optics.

Thus, multimode fiber explicitly relies on bouncing light off the cladding to transmit data.

upvoted 2 times

HeatSquad77 1 month, 3 weeks ago

Selected Answer: C

C. Single-mode.

In a single-mode fiber optic cable, light travels through a core with a very small diameter, and it bounces off the cladding (the protective layer surrounding the core) in a straight line. This design allows the light to travel long distances with minimal signal loss.

upvoted 2 times

chupapi_001 4 months, 1 week ago

Selected Answer: D

The correct answer is D. Multimode

upvoted 3 times

Question #36 *Topic 1*

Which of the following would allow a network administrator to analyze attacks coming from the internet without affecting latency?

A. IPS

B. IDS

C. Load balancer

D. Firewall

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: B

B. intrusion detection system (IDS)

An application (often running on a dedicated IDS box) that inspects incoming packets, looking for active intrusions. The difference between an IDS and an IPS is that an IPS can react to an attack by blocking traffic, while an IDS can only notify a person or device of the attack.

upvoted 1 times

ba10f26 2 months, 3 weeks ago

Selected Answer: B

The correct answer is:

B. IDS (Intrusion Detection System).

An IDS monitors network traffic and analyzes attacks without actively interfering with the traffic flow, ensuring it does not affect latency. It operates passively, alerting the administrator to potential threats without blocking or modifying the traffic.

upvoted 2 times

chupapi_001 4 months, 1 week ago

Selected Answer: B

The correct answer is B. IDS (Intrusion Detection System)

upvoted 1 times

Question #37 *Topic 1*

A technician is troubleshooting wireless connectivity near a break room. Whenever a user turns on the microwave, connectivity to the user's laptop is lost. Which of the following frequency bands is the laptop most likely using?

A. 2.4GHz

B. 5GHz

C. 6GHz

D. 900MHz

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 1 month, 3 weeks ago

Selected Answer: A

A. 2.4GHz.

Microwaves operate on the 2.4GHz frequency, which is the same frequency band commonly used by many Wi-Fi networks, particularly those that use 802.11b/g/n standards. When the microwave is turned on, it can cause interference with Wi-Fi signals in the 2.4GHz range, leading to connectivity issues.

upvoted 1 times

Legacy_SOG 3 months, 3 weeks ago

Selected Answer: A

The laptop is most likely using the **2.4 GHz frequency band**. Microwaves commonly operate on this frequency, which can cause interference with Wi-Fi signals. Switching to the 5 GHz band, if available, might help reduce this interference.

upvoted 4 times

Question #38 Topic 1

A network administrator needs to implement routing capabilities in a hypervisor. Which of the following should the administrator most likely implement?

A. VPC

B. Firewall

C. NFV

D. IaaS

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: C

C. network function virtualization (NFV)

A network architecture that applies infrastructure-as-code (IaC)-style automation and orchestration to network management.

upvoted 2 times

favouralain 3 months, 1 week ago

Selected Answer: C

NFC > Network function virtualization

upvoted 3 times

Hayder81 3 months, 2 weeks ago

C

NFV (Network Functions Virtualization).

upvoted 2 times

Question #39 *Topic 1*

A network technician needs to install patch cords from the UTP patch panel to the access switch for a newly occupied set of offices. The patch panel is not labeled for easy jack identification. Which of the following tools provides the easiest way to identify the appropriate patch panel port?

A. Toner

B. Laptop

C. Cable tester

D. Visual fault locator

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. toner

Generic term for two devices used together—a tone generator and a tone locator (probe)—to trace cables by sending an electrical signal along a wire at a particular frequency. The tone locator then emits a sound when it distinguishes that frequency. Also referred to as Fox and Hound

upvoted 4 times

favouralain 3 months, 1 week ago

Selected Answer: A

Toner is the easiest tool to identify the appropriate patch panel port

upvoted 2 times

escomgmt 4 months ago

A toner (also known as a tone generator and probe) is the easiest tool to use for identifying the appropriate patch panel port when the ports are not labeled. It works by sending a tone down the cable, which can be traced with the probe at the other end, helping the technician quickly identify the corresponding patch panel port.

upvoted 3 times

FrostyBoi 4 months ago

C, Cable tester. In this scenario a cable tester can verify the connectivity of one end of the cable, while you can test each of the ports of the patch panel to see where the connection is easily.

A Toner on the other hand (I think they are trying to refer to a tone generator probe?) Would not work as well, since you'd send a signal down a cable, and test for an already patched cable to be giving off the tone for the probe to read.

upvoted 1 times

Question #40 *Topic 1*

A network administrator received complaints of intermittent network connectivity issues. The administrator investigates and finds that the network design contains potential loop scenarios. Which of the following should the administrator do?

A. Enable spanning tree.

B. Configure port security.

C. Change switch port speed limits.

D. Enforce 802.1Q tagging.

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. Spanning Tree Protocol (STP)

A protocol that enables switches to detect and prevent switching loops automatically

upvoted 2 times

02fd592 2 months, 4 weeks ago

Selected Answer: A

Spanning tree protocol or STP is used to help prevent loops. When a loop is identified, all traffic is blocked from going in or out of the interface to prevent a loop.

upvoted 3 times

Question #41 *Topic 1*

Which of the following routing technologies uses a successor and a feasible successor?

A. IS-IS

B. OSPF

C. BGP

D. EIGRP

Correct Answer: *D*

LadyBirdArchitect 3 weeks ago

Selected Answer: D

D. EIGRP

In EIGRP, a successor is a primary route to a destination network, chosen based on having the best metric. The successor route is actively used to forward traffic to the destination network. If the successor becomes unavailable, EIGRP uses a backup route called a feasible successor.

upvoted 1 times

HeatSquad77 2 months, 1 week ago

Selected Answer: D

D. Enhanced Interior Gateway Routing Protocol (EIGRP)

Cisco's proprietary hybrid protocol that has elements of both distance vector and link state routing.

upvoted 1 times

TreyPar3 4 months ago

The routing technology that uses the concepts of a successor and a feasible successor is Enhanced Interior Gateway Routing Protocol (EIGRP). EIGRP is a Cisco-proprietary routing protocol that uses these terms in its Dual (Diffusing Update Algorithm) to ensure efficient and loop-free path selection.

upvoted 3 times

Question #42 *Topic 1*

Which of the following best describes what an organization would use port address translation for?

A. VLANs on the perimeter

B. Public address on the perimeter router

C. Non-routable address on the perimeter router

D. Servers on the perimeter

Correct Answer: *C*

Community vote distribution

C (75%) B (25%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: C

port address translation (PAT) The most commonly used form of network address translation, where the NAT uses the outgoing IP addresses and port numbers (collectively known as a socket) to map traffic from specific machines in the network.

upvoted 2 times

Legacy_SOG 3 months, 3 weeks ago

Selected Answer: C

C. Non-routable address on the perimeter router

Port Address Translation allows multiple devices on a local network to be mapped to a single public IP address with different port numbers. This is particularly useful for:
- **Non-routable address**: Providing access to devices with private, non-routable IP addresses (e.g., within a local network) via a single public IP address. This helps conserve public IP addresses and enables communication with external networks.

PAT is a form of Network Address Translation (NAT) that extends the concept by utilizing port numbers to distinguish between different devices using the same public IP address.

upvoted 3 times

st1a 4 months ago

Selected Answer: C

PAT is used for translating non routable to routable. It doesnt translate already routable public ip's

upvoted 1 times

TreyPar3 4 months ago

Selected Answer: B

The Correct is B. PAT utilizes public addresses, and they are routable.

upvoted 1 times

Question #43 *Topic 1*

A company is implementing a wireless solution in a high-density environment. Which of the following 802.11 standards is used when a company is concerned about device saturation and coverage?

A. 802.11ac

B. 802.11ax

C. 802.11g

D. 802.11n

Correct Answer: *B*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: B

B. 802.11ax

Wireless standard that brings improvements in high-density areas such as stadiums and conferences in comparison to previous standards. Marketed as both Wi-Fi 6 and Wi-Fi 6E. Wi-Fi 6 operates at the 2.4-GHz and 5-GHz bands, while Wi-Fi 6E operates at the 6-GHz band. 802.11ax offers a maximum throughput of up to 10 Gbps.

upvoted 1 times

jmcd2 2 months, 1 week ago

Selected Answer: B

802.11ax (Wi-Fi 6) is specifically designed to perform exceptionally well in high-density areas. Its features address the challenges posed by environments where many devices are competing for bandwidth, such as stadiums, airports, office buildings, and multi-tenant dwellings.

upvoted 1 times

ba10f26 2 months, 3 weeks ago

Selected Answer: B

The correct answer is:

B. 802.11ax

802.11ax (Wi-Fi 6) is designed to address challenges in high-density environments where many devices connect to the network. It improves device saturation and coverage by introducing advanced features such as:

OFDMA (Orthogonal Frequency Division Multiple Access): Allows multiple devices to share the same channel efficiently.
MU-MIMO (Multi-User Multiple Input Multiple Output): Supports simultaneous communication with multiple devices.
Target Wake Time (TWT): Improves power efficiency for connected devices.
Enhanced signal performance and reduced interference in both 2.4GHz and 5GHz bands.
This makes 802.11ax the most suitable standard for high-density environments

upvoted 3 times

Nateforreal 2 months, 3 weeks ago

Selected Answer: A

802.11ac (also known as Wi-Fi 5), as it utilizes the 5GHz band which offers more non-overlapping channels, allowing for better performance in dense environments with many connected devices.

upvoted 1 times

Question #44 | *Topic 1*

Which of the following network traffic types is sent to all nodes on the network?

A. Unicast

B. Broadcast

C. Multicast

D. Anycast

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

HeatSquad77 1 month, 3 weeks ago

Selected Answer: B

B. Broadcast.

Broadcast traffic is sent to all nodes on the network. When a device sends a broadcast message, it is delivered to every other device on the same network segment or broadcast domain.

upvoted 1 times

jmcd2 2 months, 2 weeks ago

Selected Answer: B

B. Broadcast
That sends it to all nodes

upvoted 1 times

favouralain 3 months, 1 week ago

Selected Answer: B

computer science refers to the type of network traffic that is sent to all nodes within a broadcast domain.

upvoted 1 times

Question #45 *Topic 1*

Which of the following cable types provides the highest possible transmission speed?

A. Plenum

B. Ethernet

C. Fiber-optic

D. DAC

Correct Answer: *C*

⊟ **HeatSquad77** 2 months, 1 week ago

Selected Answer: C

C. fiber-optic cable

A high-speed physical medium for transmitting data that uses light rather than electricity to transmit data and is made of high-purity glass fibers sealed within a flexible opaque tube. Much faster than conventional copper wire.

upvoted 1 times

Question #46 *Topic 1*

Which of the following layers of the OSI model is responsible for end-to-end encryption?

A. Presentation

B. Application

C. Session

D. Transport

Correct Answer: *A*

Community vote distribution

A (56%) B (22%) D (22%)

Community vote distribution

⊟ **ba10f26** Highly Voted 👍 2 months, 3 weeks ago

Selected Answer: A

The correct answer is:

A. Presentation

The Presentation layer (Layer 6) of the OSI model is responsible for functions like data formatting, translation, and encryption/decryption. End-to-end encryption is typically handled at this layer to ensure that data is securely encoded before being transmitted and properly decoded upon receipt.

upvoted 5 times

⊟ **lord_darth_vader** Most Recent ⊙ 3 months ago

Selected Answer: A

A. Presentation

upvoted 4 times

⊟ **GT256** 4 months ago

Selected Answer: B

This is my answer, but please correct me if I'm wrong.

True end-to-end encryption (E2EE) typically operates at the application layer (Layer 7) of the OSI model. This is because E2EE is designed to encrypt data from the time it leaves the sender's application until it is decrypted by the recipient's application, ensuring that it remains secure throughout its journey.

Application Layer (Layer 7): This is where E2EE protocols, such as Signal Protocol, OpenPGP, and various proprietary methods used in messaging apps, work. They ensure that the data is encrypted and decrypted only by the end-users' applications.

The transport layer (Layer 4), which includes protocols like TLS, does provide encryption, but it doesn't always maintain encryption throughout the entire path between sender and receiver, since data may be decrypted at intermediate points.

upvoted 2 times

⊟ **342d098** 4 months ago

Selected Answer: A

Presentation Layer responsible for end-to-end encryption

upvoted 4 times

⊟ **FrostyBoi** 4 months ago

Selected Answer: D

D, The transport layer is responsible for end-to-end encryption using protocols such as TLS.

upvoted 3 times

Question #47 *Topic 1*

A network security administrator needs to monitor the contents of data sent between a secure network and the rest of the company. Which of the following monitoring methods will accomplish this task?

A. Port mirroring

B. Flow data

C. Syslog entries

D. SNMP traps

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. port mirroring

The capability of many advanced switches to mirror data from any or all physical ports on a switch to a single physical port. Useful for any type of situation where an administrator needs to inspect packets coming to or from certain computers.

upvoted 1 times

ba10f26 2 months, 3 weeks ago

Selected Answer: A

The correct answer is:

A. Port mirroring

Port mirroring is a technique used on a network switch to duplicate (or "mirror") the traffic from one or more ports to another port where a monitoring device, such as a network analyzer or intrusion detection system, is connected. This allows the administrator to monitor the contents of data being sent between the secure network and the rest of the company.

upvoted 2 times

Hayder81 3 months, 2 weeks ago

Selected Answer: A

A. Port mirroring.

upvoted 2 times

Question #48 *Topic 1*

Which of the following does a full-tunnel VPN provide?

A. Lower bandwidth requirements

B. The ability to reset local computer passwords

C. Corporate inspection of all network traffic

D. Access to blocked sites

Correct Answer: *C*

nastness 2 weeks, 6 days ago

Selected Answer: D

I would think it can do both c & d. here is what google AI said A full-tunnel VPN does not provide corporate inspection of all network traffic, but it can provide access to blocked sites. So the correct answer is D.

upvoted 1 times

HeatSquad77 2 months ago

Selected Answer: C

C. Corporate inspection of all network traffic

Explanation:
A full-tunnel VPN routes all network traffic from the user's device through the VPN server, meaning all internet traffic (not just traffic destined for corporate resources) goes through the VPN. This allows the corporate network or the VPN provider to inspect and monitor all traffic, providing a higher level of security and control over the data.

upvoted 2 times

Question #49 *Topic 1*

Which of the following does a hash provide?

A. Non-repudiation

B. Integrity

C. Confidentiality

D. Availability

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: B

B. Integrity

The fixed-length value that a hash function computes from its input. Hashes have many important jobs in computing, but in networking they are primarily used for authentication and ensuring data integrity

upvoted 1 times

HeatSquad77 2 months, 2 weeks ago

Selected Answer: B

Integrity

upvoted 1 times

ba10f26 2 months, 3 weeks ago

Selected Answer: B

The correct answer is:

B. Integrity

A hash provides integrity by generating a fixed-length unique representation (hash value) of data. If the data is altered, even slightly, the hash value will change, allowing verification that the data has not been tampered with. Hashes do not provide confidentiality, non-repudiation, or availability.

upvoted 2 times

02fd592 2 months, 3 weeks ago

Selected Answer: B

B. Integrity

Hashes help verify integrity.

upvoted 1 times

Question #50 *Topic 1*

A company wants to implement a disaster recovery site for non-critical applications, which can tolerate a short period of downtime. Which of the following types of sites should the company implement to achieve this goal?

A. Hot

B. Cold

C. Warm

D. Passive

Correct Answer: *C*

Community vote distribution

C (86%) 14%

Community vote distribution

⊟ **HeatSquad77** 2 months, 1 week ago

Selected Answer: C

C. warm site

Facility with all of the physical resources, computers, and network infrastructure to recover from a primary site disaster. A warm site does not have current backup data and it may take a day or more to recover and install backups before business operations can recommence.

upvoted 1 times

⊟ **ba4cbc8** 3 months, 1 week ago

Selected Answer: C

Warm Sites are sites that include a small amount of downtime and have the services that can be started within a short time. Hot sites are available immediately as they constantly keep the same standards as the main workcenter. Cold sites typically require more extensive updates/personnel to go to the installation and take a slightly longer time than a warm site to become operational.

upvoted 3 times

⊟ **b82faaf** 3 months, 2 weeks ago

Selected Answer: B

Cold sites are cost-effective and suitable for non-critical applications that can tolerate a short period of downtime, making them ideal for this scenario.

upvoted 1 times

⊟ **b82faaf** 3 months, 1 week ago

I take this back. After checking more closely, especially considering the keywords " 'short' period of time", I believe the answer should be C. Warm

upvoted 3 times

⊟ **TreyPar3** 4 months ago

Selected Answer: C

C. Warm

Explanation:
A warm site is suitable for non-critical applications that can tolerate a short period of downtime. Warm sites typically have some infrastructure and equipment already in place, but they may need additional setup or data synchronization before they can be fully operational. This makes warm sites a balanced choice for companies that need faster recovery than a cold site but do not require the immediate availability of a hot site.

upvoted 4 times

⊟ **ojones888** 4 months ago

I agree. Hot site would have no down time. Cold site would have extended down time.

upvoted 1 times

Question #51 *Topic 1*

Which of the following is an XML-based security concept that works by passing sensitive information about users, such as log-in information and attributes, to providers?

A. IAM

B. MFA

C. RADIUS

D. SAML

Correct Answer: *D*

LilJuneBug Highly Voted 3 months, 3 weeks ago

SAML (Security Assertion Markup Language) is an open standard used for exchanging authentication and authorization data between different parties, primarily between an identity provider (IdP) and a service provider (SP). It is often used in Single Sign-On (SSO) systems to allow users to authenticate once and gain access to multiple applications or services without having to log in again.

upvoted 7 times

HeatSquad77 Most Recent 1 month, 3 weeks ago

Selected Answer: D

D. SAML.

SAML (Security Assertion Markup Language) is an XML-based security concept that allows the exchange of authentication and authorization data between parties, especially between identity providers and service providers. It is commonly used for single sign-on (SSO) solutions, where users' login information and attributes are securely passed to service providers.

upvoted 2 times

Question #52 *Topic 1*

Which of the following routing technologies uses unequal cost load balancing and port 88?

A. EIGRP

B. BGP

C. RIP

D. OSPF

Correct Answer: *A*

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. Enhanced Interior Gateway Routing Protocol (EIGRP)

Cisco's proprietary hybrid protocol that has elements of both distance vector and link state routing.

upvoted 2 times

ebcd6a1 2 months, 1 week ago

Selected Answer: A

EIGRP (Enhanced Interior Gateway Routing Protocol) is a Cisco proprietary routing protocol that supports unequal cost load balancing (UCLB) through its variance feature. With UCLB, EIGRP can send traffic over multiple routes, even if those routes have unequal costs (i.e., different metrics), as long as the variance multiplier is configured to allow for it.

In addition, EIGRP uses UDP port 88 for communication between routers.

upvoted 2 times

Question #53 *Topic 1*

A wireless network consultant is deploying a large number of WAPs and wants to centrally control them from one wireless LAN controller. Which of the following network types should the consultant employ?

A. Mesh

B. Infrastructure

C. Point-to-point

D. Ad hoc

Correct Answer: *B*

HeatSquad77 2 months, 1 week ago

Selected Answer: B

B. infrastructure mode

Mode in which wireless networks use one or more wireless access points to connect the wireless network nodes centrally. This configuration is similar to the star topology of a wired network.

upvoted 3 times

HeatSquad77 2 months, 2 weeks ago

Selected Answer: B

infrastructure

upvoted 1 times

Question #54 *Topic 1*

Which of the following network topologies involves sending all traffic through a single point?

A. Mesh

B. Hybrid

C. Hub-and-spoke

D. Point-to-point

Correct Answer: *C*

HeatSquad77 2 months, 2 weeks ago

Selected Answer: C

The spoke–hub distribution paradigm (also known as the hub-and-spoke system) is a form of transport topology optimization in which traffic planners organize routes as a series of "spokes" that connect outlying points to a central "hub".

upvoted 1 times

Question #55 *Topic 1*

Which of the following functions is used to prioritize network traffic based on the type of traffic?

A. QoS

B. VPN

C. CDN

D. TTL

Correct Answer: *A*

HeatSquad77 2 months, 2 weeks ago

Selected Answer: A

Quality of service

upvoted 1 times

Nateforreal 2 months, 2 weeks ago

Selected Answer: A

QoS allows network administrators to classify different types of traffic and assign priority levels to them, ensuring that critical applications receive preferential treatment over less important traffic.

upvoted 2 times

Question #56 Topic 1

Which of the following most likely determines the size of a rack for installation? (Choose two.)

A. KVM size

B. Switch depth

C. Hard drive size

D. Cooling fan speed

E. Outlet amperage

F. Server height

Correct Answer: *BF*

HeatSquad77 1 month, 3 weeks ago

Selected Answer: BF

B. Switch depth

F. Server height

Explanation:

Switch depth (B): The depth of network switches and other equipment that will be installed in the rack can impact the rack's depth to ensure everything fits properly.

Server height (F): Racks are often designed to accommodate specific server heights, typically measured in "rack units" (U). The height of the servers that will be installed in the rack is critical for determining the rack size.

upvoted 1 times

Question #57 *Topic 1*

A network administrator is planning to implement device monitoring to enhance network visibility. The security team requires that the solution provides authentication and encryption. Which of the following meets these requirements?

A. SIEM

B. Syslog

C. NetFlow

D. SNMPv3

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

HeatSquad77 2 months, 2 weeks ago

Selected Answer: D

SNMPv3

upvoted 1 times

efe498c 2 months, 4 weeks ago

Selected Answer: D

SNMPv3 provides authentication and encryption

upvoted 1 times

Question #58 *Topic 1*

A network administrator needs to change where the outside DNS records are hosted. Which of the following records should the administrator change at the registrar to accomplish this task?

A. NS

B. SOA

C. PTR

D. CNAME

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. name server

DNS servers that hold the actual name and IP DNS records in a kind of database called a zone.

upvoted 1 times

HeatSquad77 2 months, 2 weeks ago

Selected Answer: A

Name Server

upvoted 1 times

efe498c 2 months, 4 weeks ago

Selected Answer: A

NS is a name server what you would use for DNS. SOA is service orientated architecture. PTR is a pointer record which maps a domain name essentially opposite of A or AAAA (IP<Domain). CNAME is used to create an alias for a domain name, allowing multiple subdomains to point to the same sever without needing separate A records

upvoted 3 times

TheCrumbs 2 months, 4 weeks ago

Selected Answer: A

The correct answer is A. NS (Name Server).

To change where the outside DNS records are hosted, the network administrator needs to update the NS (Name Server) records at the domain registrar. NS records specify which DNS servers are authoritative for the domain. When the administrator updates the NS records, they are directing queries for the domain to the new DNS servers.

Here's what the other records do:

B. SOA (Start of Authority): The SOA record indicates the start of a zone and includes details like the primary DNS server and the email of the domain administrator. While important for DNS zone configuration, changing the hosting of DNS records typically requires updating the NS records, not the SOA record.

C. PTR (Pointer): PTR records are used for reverse DNS lookups, mapping an IP address to a domain name. They are not used to control where DNS records are hosted.

D. CNAME (Canonical Name): A CNAME record is used to alias one domain name to another. Changing DNS hosting typically involves modifying the NS records, not CNAME records.

Thus, to change the DNS hosting, the administrator should modify the NS records at the domain registrar.

upvoted 2 times

Question #59 *Topic 1*

A support agent receives a report that a remote user's wired devices are constantly disconnecting and have slow speeds. Upon inspection, the support agent sees that the user's coaxial modem has a signal power of -97dB. Which of the following should the support agent recommend to troubleshoot the issue?

A. Removing any splitters connected to the line

B. Switching the devices to wireless

C. Moving the devices closer to the modem

D. Lowering the network speed

Correct Answer: *A*

HeatSquad77 1 month, 3 weeks ago

Selected Answer: A

A. Removing any splitters connected to the line.

Explanation:

A signal power of -97dB is quite low for a coaxial connection, indicating that there is likely signal degradation or interference in the line. Splitters can weaken the signal, and removing any unnecessary splitters could help restore signal strength and improve the connection.

upvoted 1 times

Question #60 *Topic 1*

Which of the following does OSPF use to communicate routing updates?

A. Unicast

B. Anycast

C. Multicast

D. Broadcast

Correct Answer: *C*

Community vote distribution

C (50%) D (50%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: C

C. multicast

Method of sending a packet in which the sending computer sends it to a group of interested computers.

upvoted 2 times

ba10f26 2 months, 3 weeks ago

Selected Answer: C

The correct answer is:

C. Multicast

OSPF (Open Shortest Path First) uses multicast to communicate routing updates with other routers. Specifically, it sends updates to the following multicast addresses:

224.0.0.5: All OSPF routers
224.0.0.6: All OSPF designated routers (DRs)
Using multicast allows OSPF to efficiently share routing information only with routers that are configured to participate in the OSPF process, rather than broadcasting to all devices on the network.

upvoted 2 times

efe498c 2 months, 4 weeks ago

Selected Answer: C

The answer is OSPF uses multicast to communicate routing updates.

upvoted 1 times

lord_darth_vader 3 months ago

Selected Answer: D

Garrett says its D

upvoted 1 times

lord_darth_vader 3 months ago

FATAL ERROR! I apologize for the confusion here. Garrett said it was B not D.

upvoted 1 times

Question #61 *Topic 1*

A storage network requires reduced overhead and increased efficiency for the amount of data being sent. Which of the following should an engineer most likely configure to meet these requirements?

A. Link speed

B. Jumbo frames

C. QoS

D. 802.1q tagging

Correct Answer: *B*

LadyBirdArchitect 2 weeks, 5 days ago

Selected Answer: B

B. Jumbo frames

Jumbo frames can encapsulate more data in a single frame, reducing the number of frames required for a given amount of data. This results in lower overhead per byte and improved overall network efficiency.

upvoted 1 times

HeatSquad77 2 months, 1 week ago

Selected Answer: B

b. jumbo frames

Frames (usually 9000 bytes long—though technically anything over 1500 bytes qualifies) that make large data transfer easier and more efficient than using the standard frame size.

upvoted 2 times

Question #62 *Topic 1*

A security administrator is creating a new firewall object for a device with IP address 192.168.100.1/25. However, the firewall software only uses dotted decimal notation in configuration fields. Which of the following is the correct subnet mask to use?

A. 255.255.254.0

B. 255.255.255.1

C. 255.255.255.128

D. 255.255.255.192

Correct Answer: *C*

HeatSquad77 2 months, 2 weeks ago

Selected Answer: C

/25 in binary looks like this...11111111.11111111.11111111.10000000...if you count all the ones it adds up to 255.255.255.128

upvoted 2 times

Question #63 Topic 1

Which of the following disaster recovery metrics describes the average length of time a piece of equipment can be expected to operate normally?

A. RPO

B. RTO

C. MTTR

D. MTBF

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: D

D. mean time between failures (MTBF)

A factor typically applied to a hardware component that represents the manufacturer's best guess (based on historical data) regarding how much time will pass between major failures of that component

upvoted 1 times

Vealbrevity 3 months, 1 week ago

Selected Answer: D

The correct answer is:

D. MTBF (Mean Time Between Failures)

Explanation:
MTBF: This metric describes the average length of time a piece of equipment or system is expected to operate normally before a failure occurs. It is used to predict reliability and is critical in disaster recovery and maintenance planning.
Why not the others?
A. RPO (Recovery Point Objective): This measures the maximum amount of data that can be lost during a disruption, expressed in time. It focuses on data recovery.
B. RTO (Recovery Time Objective): This refers to the maximum allowable downtime after a disaster to restore normal operations.
C. MTTR (Mean Time to Repair): This measures the average time required to repair a failed piece of equipment or system and restore it to normal operation.

upvoted 2 times

Question #64 *Topic 1*

A network administrator logs on to a router and sees an interface with an IP address of 10.61.52.34 255.255.255.252. Which of the following best describes how this interface IP address is being used?

A. As a point-to-point connection

B. To connect to the internet

C. As a virtual address for redundancy

D. For out-of-band management

Correct Answer: *A*

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. Point to point

The IP address 10.61.52.34 with a subnet mask 255.255.255.252 corresponds to a very small subnet, which provides only 4 IP addresses in total. Specifically:

The network address: 10.61.52.32
Usable host addresses: 10.61.52.33 and 10.61.52.34
Broadcast address: 10.61.52.35
Since this subnet allows for only two usable IP addresses, it is commonly used for point-to-point connections, such as connecting two routers or devices directly. In a point-to-point link, each device in the connection typically gets one of the two available IP addresses
upvoted 4 times

Question #65 *Topic 1*

A network technician is troubleshooting a faulty NIC and tests the theory. Which of the following should the technician do next?

A. Develop a theory.

B. Establish a plan of action.

C. Implement the solution.

D. Document the findings.

Correct Answer: *B*

Nanox 1 month ago

Selected Answer: B

B. Establish plan of action. Thiis is step four in the Basic Network Troubleshooting Steps. CompTia States: "Once you've confirmed your theory about the causes of the network issues, you're in a position to solve them. Come up with a plan of action to address the problem. Sometimes your plan will include just one step. For example, restart the router. In other cases, your plan will be more complex and take longer, such as when you need to order a new part or roll a piece of software back to a previous version on multiple users' computers." Referances: https://www.comptia.org/content/guides/a-guide-to-network-troubleshooting

upvoted 1 times

HeatSquad77 2 months, 2 weeks ago

Selected Answer: B

next step is to establish a plan of action

upvoted 1 times

Question #66 Topic 1

A network administrator is configuring access points for installation in a dense environment where coverage is often overlapping. Which of the following channel widths should the administrator choose to help minimize interference in the 2.4GHz spectrum?

A. 11MHz

B. 20MHz

C. 40MHz

D. 80MHz

E. 160MHz

Correct Answer: *B*

HeatSquad77 2 months, 2 weeks ago

Selected Answer: B

20 MHz

upvoted 1 times

chrys 3 months, 4 weeks ago

20 MHz is absolutely correct. The wider the channel, the higher the risk that somewhere in its frequency range it will be hit with interference. Since 2.4 GHz is an especially crowded band, you want to avoid the risk of interference, even though it means that each mobile client will be stuck with less overall bandwidth for their connection

upvoted 4 times

Question #67 *Topic 1*

A network manager wants to view network traffic for devices connected to a switch. A network engineer connects an appliance to a free port on the switch and needs to configure the switch port connected to the appliance. Which of the following is the best option for the engineer to enable?

A. Trunking

B. Port mirroring

C. Full duplex

D. SNMP

Correct Answer: *B*

HeatSquad77 2 months, 1 week ago

Selected Answer: B

B. Port mirroring.

Explanation:
Port mirroring is a feature on network switches that allows network traffic from one or more ports to be copied (mirrored) to another port, where it can be monitored or analyzed by a network appliance (such as a network analyzer, IDS/IPS, or other monitoring device). In this scenario, the engineer needs to monitor network traffic for devices connected to a switch, which is exactly what port mirroring is designed for.

upvoted 1 times

Question #68 *Topic 1*

A network administrator is in the process of installing 35 PoE security cameras. After the administrator installed and tested the new cables, the administrator installed the cameras. However, a small number of the cameras do not work. Which of the following is the most likely reason?

A. Incorrect wiring standard

B. Power budget exceeded

C. Signal attenuation

D. Wrong voltage

Correct Answer: *B*

HeatSquad77 2 months, 2 weeks ago

Selected Answer: B

the network admin tested and verified that the cables are working. the cameras are new so they should not be having any hardware failures. correct answer is power budget has been exceeded

upvoted 2 times

Question #69 *Topic 1*

A network administrator is troubleshooting an application issue after a firewall change. The administrator has confirmed that the port and protocol are accessible to the user, but the application is still having issues. Which of the following tools allows the administrator to look at traffic on the application layer of the OSI model?

A. ifconfig

B. tcpdump

C. nslookup

D. traceroute

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

HeatSquad77 1 month, 3 weeks ago

Selected Answer: B

B. tcpdump.

Explanation:

tcpdump is a network packet analyzer that captures and displays packets from the network, allowing the administrator to look at traffic at various layers of the OSI model, including the application layer (Layer 7). By inspecting the packets in detail, the administrator can check the contents of the communication to troubleshoot the application issue.

upvoted 1 times

chrys 4 months ago

Selected Answer: B

B is correct. For example, you could see the contents of a DNS query and response, which are both at the Application Layer

upvoted 1 times

LilJuneBug 4 months, 1 week ago

B is correct

upvoted 1 times

Question #70 *Topic 1*

Which of the following ports should a network administrator enable for encrypted log-in to a network switch?

A. 22

B. 23

C. 80

D. 123

Correct Answer: *A*

HeatSquad77 2 months, 2 weeks ago

Selected Answer: A

Port 22 is the default port for the Secure Shell (SSH) protocol

upvoted 2 times

Question #71 *Topic 1*

Which of the following is used to stage copies of a website closer to geographically dispersed users?

A. VPN

B. CDN

C. SAN

D. SDN

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

SuntzuLegacy Highly Voted 👍 3 months, 1 week ago

Selected Answer: B

The correct answer is:

B. CDN (Content Delivery Network)

Explanation:
A Content Delivery Network (CDN) is used to stage copies of a website or its content closer to geographically dispersed users. It works by caching website resources (e.g., images, videos, scripts, and HTML pages) on servers located in various geographical locations. This reduces latency, improves load times, and enhances the user experience by delivering content from a server that is physically closer to the user.

upvoted 5 times

HeatSquad77 Most Recent 🕓 2 months, 1 week ago

Selected Answer: B

B. CDN (Content Delivery Network).

Explanation:
A Content Delivery Network (CDN) is a system of distributed servers that deliver web content, such as HTML pages, images, videos, and other resources, to users based on their geographic location. CDNs cache copies of the website’s content at multiple locations around the world (called edge servers). When a user accesses the website, the content is served from the closest server to reduce latency and improve load times.

upvoted 1 times

Question #72 *Topic 1*

Which of the following appliances provides users with an extended footprint that allows connections from multiple devices within a designated WLAN?

A. Router

B. Switch

C. Access point

D. Firewall

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: C

C. Access point.

Explanation:
An access point (AP) is a device that allows wireless devices to connect to a wired network via Wi-Fi, extending the footprint of a wireless local area network (WLAN). The AP serves as the bridge between the wired network and the wireless devices, and by placing multiple access points in different locations, you can extend the coverage area, allowing users to connect from various devices within that extended footprint

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: C

The correct answer is:

C. Access point

Explanation:
An access point (AP) is a networking device that allows multiple devices to connect to a wireless local area network (WLAN). It extends the network footprint by broadcasting a Wi-Fi signal, enabling devices like laptops, smartphones, and IoT devices to connect wirelessly within its coverage area.

upvoted 3 times

Question #73 *Topic 1*

An administrator is configuring a switch that will be placed in an area of the office that is accessible to customers. Which of the following is the best way for the administrator to mitigate unknown devices from connecting to the network?

A. SSE

B. ACL

C. Perimeter network

D. 802.1X

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

HeatSquad77 2 months, 2 weeks ago

Selected Answer: D

802.1x allows for devices to be authenticated to the network if its a known device based on its MAC address

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: D

The correct answer is:

D. 802.1X

Explanation:

802.1X is a network access control protocol that provides port-based authentication for devices attempting to connect to a network. It ensures that only authorized devices and users can access the network by requiring authentication before granting access. This is particularly useful for mitigating the risk of unknown devices connecting to a switch in a public or semi-public area.

upvoted 2 times

Question #74 Topic 1

Which of the following diagrams would most likely include specifications about fiber connector types?

A. Logical

B. Physical

C. Rack

D. Routing

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: B

B. physical network diagram

A document that shows all of the physical connections on a network. Cabling type, protocol, and speed are also listed for each connection.

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: B

The correct answer is:

B. Physical

Explanation:
A physical diagram represents the actual physical layout of a network, including the types of cables, connectors, and devices used. This type of diagram would most likely include details about fiber connector types (e.g., LC, SC, ST) because it specifies how network components are physically connected.

upvoted 3 times

Question #75 *Topic 1*

Which of the following is the most likely reason an insurance brokerage would enforce VPN usage?

A. To encrypt sensitive data in transit

B. To secure the endpoints

C. To maintain contractual agreements

D. To comply with data retention requirements

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. To encrypt sensitive data in transit.

Explanation:
An insurance brokerage handles a large amount of sensitive client data, such as personal information, financial records, and insurance details. Enforcing VPN usage is a key way to ensure that this sensitive data is encrypted when transmitted over the internet, especially when employees or agents need to access systems remotely.

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

The correct answer is:

A. To encrypt sensitive data in transit

Explanation:
An insurance brokerage is likely to handle a significant amount of sensitive data, such as personal identifiable information (PII), financial records, and health-related information. Using a VPN (Virtual Private Network) ensures that all data transmitted between endpoints (e.g., employee devices and company systems) is encrypted, protecting it from interception by unauthorized parties during transit, especially over untrusted networks like public Wi-Fi.

upvoted 3 times

Question #76 *Topic 1*

An organization moved its DNS servers to new IP addresses. After this move, customers are no longer able to access the organization's website. Which of the following DNS entries should be updated?

A. AAA

B. CNAME

C. MX

D. NS

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

SuntzuLegacy 3 months, 1 week ago

Selected Answer: D

The correct answer is:

D. NS (Name Server)

Explanation:
The NS (Name Server) record specifies which DNS servers are authoritative for a domain. If the organization has moved its DNS servers to new IP addresses, the NS records need to be updated to point to the new name servers. This ensures that DNS queries for the domain are directed to the correct authoritative servers.

upvoted 3 times

Question #77 *Topic 1*

Which of the following are environmental factors that should be considered when installing equipment in a building? (Choose two.)

A. Fire suppression system

B. UPS location

C. Humidity control

D. Power load

E. Floor construction type

F. Proximity to nearest MDF

Correct Answer: *AC*

Community vote distribution

AC (100%)

Community vote distribution

SuntzuLegacy 3 months, 1 week ago

Selected Answer: AC

The correct answers are:

A. Fire suppression system
C. Humidity control

Explanation:
A. Fire suppression system:
Ensuring the presence of an appropriate fire suppression system is crucial for protecting equipment in case of fire. Modern data centers and server rooms typically use non-water-based fire suppression systems (e.g., FM200 or CO2 systems) to avoid damaging sensitive electronics.

C. Humidity control:
Maintaining proper humidity levels is essential for preventing condensation (too high humidity) or static electricity (too low humidity), both of which can damage sensitive equipment. Humidity control is a critical environmental factor in equipment installations.

upvoted 2 times

FrostyBoi 4 months ago

Selected Answer: AC

Definitely A, and C. For environmental factors, preventing fire (wild fires or otherwise) and controlling humidity. The power load is not an environmental factor, but a cost factor.

upvoted 3 times

ojones888 4 months, 1 week ago

Selected Answer: AC

A. Fire suppression system
C. Humidity control

Explanation:
A. Fire suppression system: This is crucial for ensuring the safety of the equipment and personnel. A proper fire suppression system can help protect against potential fire hazards that could damage the equipment.

C. Humidity control: Maintaining appropriate humidity levels is essential for preventing damage to electronic equipment. Excess humidity can lead to corrosion, while low humidity can cause static electricity issues.

upvoted 4 times

Question #78 *Topic 1*

A customer lost the connection to the telephone system. The administration console is configured with multiple network interfaces and is connected to multiple switches. The network administrator troubleshoots and verifies the following:
The support team is able to connect remotely to the administration console.
Rebooting the switch shows solid link and activity lights even on unused ports.
Rebooting the telephone system does not bring the system back online.
The console is able to connect directly to individual modules successfully.
Which of the following is the most likely reason the customer lost the connection?

A. A switch failed.

B. The console software needs to be reinstalled.

C. The cables to the modules need to be replaced.

D. A module failed.

Correct Answer: *D*

ec_ 4 days, 20 hours ago
Selected Answer: A
A module failed. But the console can connect directly to individual modules, which implies they're working. So D is unlikely.

So the most likely answer is A. The switch failed. Even though they rebooted it, maybe the reboot didn't resolve the hardware issue, or there's a configuration problem. The solid lights on unused ports might indicate a malfunctioning switch. Since the telephone system didn't come back after reboot, and direct connections work, the problem is likely the switch handling the telephone system's traffic. The support team can access the admin console via another interface connected to a different switch, so that's why they can still connect remotely.
upvoted 1 times

085d557 3 weeks ago
Selected Answer: D
I would still go with D.
It's an astute observation. While solid link and activity lights on unused ports might seem unusual and could be interpreted as a potential switch failure, the fact that the support team can still connect remotely to the administration console suggests that the switch is likely still functioning correctly to some extent.

The presence of activity lights on unused ports could indicate a misconfiguration or another network issue, but given the symptoms described, a module failure within the telephone system still seems more plausible. The console's ability to connect directly to individual modules but not to bring the entire system online points towards an internal issue within the telephone system, potentially with one of the modules.
upvoted 2 times

93831b0 1 month ago
Selected Answer: A
When a network switch shows solid link and activity lights on all ports, including unused ones, after rebooting, it typically indicates that the switch is experiencing a broadcast storm or network loop. This screams switch failing !!!
upvoted 2 times

> **Big_Wes** 3 weeks, 6 days ago
> True, however "Rebooting the telephone system does not restore service" meaning it is an issue with the module if the switch is back online.
>
> D. Failed Module
> upvoted 2 times

blasgmz99 1 month, 1 week ago
Selected Answer: A
Direct connection to modules work, Link lights up on a port with no cable connection are indicative of a failing switch.
upvoted 2 times

HeatSquad77 2 months, 1 week ago
Selected Answer: D

The most likely reason the customer lost the connection is D. A module failed.

upvoted 1 times

Question #79 *Topic 1*

A systems administrator is configuring a new device to be added to the network. The administrator is planning to perform device hardening prior to connecting the device. Which of the following should the administrator do first?

A. Update the network ACLs.

B. Place the device in a screened subnet.

C. Enable content filtering.

D. Change the default admin passwords.

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

SuntzuLegacy 3 months, 1 week ago

Selected Answer: D

The correct answer is:
D. Change the default admin passwords.

Explanation:
Changing the default admin passwords is the most critical first step when performing device hardening. Default credentials are widely known and easily exploited by attackers. By changing these to strong, unique passwords, the administrator ensures that unauthorized access to the device is immediately mitigated.

upvoted 4 times

Question #80 *Topic 1*

A network administrator needs to connect two network closets that are 492ft (150m) away from each other. Which of the following cable types should the administrator install between the closets?

A. Single-mode fiber

B. Coaxial

C. DAC

D. STP

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

Abx_01 2 weeks, 5 days ago

Selected Answer: A

Fiber is good for long distance.
Direct Attach Copper (DAC) cable is ideal for short-range connections, typically up to 7 meters.

upvoted 1 times

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. Single-mode fiber.

Explanation:
To connect two network closets that are 492 feet (150 meters) apart, the key consideration is the distance and the type of cable that can effectively handle that distance without significant signal loss or degradation

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

The correct answer is:

A. Single-mode fiber

Explanation:
At a distance of 492 feet (150 meters), single-mode fiber is the best choice for connecting network closets. Single-mode fiber is designed for long-distance transmission and provides high bandwidth with minimal signal loss over distances far exceeding the 150 meters required in this scenario.

upvoted 3 times

Question #81 *Topic 1*

An IT manager needs to connect ten sites in a mesh network. Each needs to be secured with reduced provisioning time. Which of the following technologies will best meet this requirement?

A. SD-WAN

B. VXLAN

C. VPN

D. NFV

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. SD-WAN.

Explanation:
The IT manager needs to connect ten sites in a mesh network while ensuring security and reduced provisioning time

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

The correct answer is:

A. SD-WAN (Software-Defined Wide Area Networking)

Explanation:
SD-WAN is the best technology to meet the requirements of connecting multiple sites in a mesh network with enhanced security and reduced provisioning time. SD-WAN simplifies the deployment and management of a wide area network by using centralized control, automation, and intelligent routing to securely connect multiple sites.

upvoted 3 times

Question #82 *Topic 1*

Which of the following is most likely responsible for the security and handling of personal data in Europe?

A. GDPR

B. SCADA

C. SAML

D. PCI DSS

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

Big_Wes 3 weeks, 6 days ago

Selected Answer: A

A. GDPR.

upvoted 1 times

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. GDPR.

Explanation:
GDPR (General Data Protection Regulation) is the regulation most directly responsible for the security and handling of personal data in Europe

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

The correct answer is:

A. GDPR (General Data Protection Regulation)

Explanation:
The General Data Protection Regulation (GDPR) is the European Union's comprehensive data protection law. It governs the security, privacy, and handling of personal data for individuals within the EU. GDPR applies to any organization, regardless of location, that processes personal data of EU residents. It establishes strict requirements for data protection, transparency, and individual rights.

upvoted 1 times

Question #83 *Topic 1*

An organization has a security requirement that all network connections can be traced back to a user. A network administrator needs to identify a solution to implement on the wireless network. Which of the following is the best solution?

A. Implementing enterprise authentication

B. Requiring the use of PSKs

C. Configuring a captive portal for users

D. Enforcing wired equivalent protection

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

The correct answer is:

A. Implementing enterprise authentication

Explanation:
Enterprise authentication (e.g., using WPA3-Enterprise or WPA2-Enterprise) ensures that each network connection can be uniquely traced back to a user by requiring individual authentication credentials for each user. Typically, enterprise authentication uses an 802.1X authentication framework with a RADIUS server to authenticate users and devices. This provides a detailed audit trail, enabling the organization to trace activity back to specific users.

upvoted 2 times

b82faaf 3 months, 2 weeks ago

Selected Answer: A

A. Implementing enterprise authentication
Enterprise authentication using 802.1X and a RADIUS server is the most secure and effective solution to trace wireless network connections back to individual users, meeting the organization's security requirements.

upvoted 1 times

Question #84 *Topic 1*

A customer is adding fiber connectivity between adjacent buildings. A technician terminates the multimode cable to the fiber patch panel. After the technician connects the fiber patch cable, the indicator light does not tum on. Which of the following should a technician try first to troubleshoot this issue?

A. Reverse the fibers.

B. Reterminate the fibers.

C. Verify the fiber size.

D. Examine the cable runs for visual faults.

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. Reverse the fibers.

Explanation:
In fiber optics, multimode cables often use duplex connectors, and the transmit (Tx) and receive (Rx) fibers need to be properly aligned. If the indicator light does not turn on, it could be due to the Tx and Rx being mismatched. Reversing the fibers is the quickest and easiest troubleshooting step to verify this alignment issue before moving on to more complex checks like examining the cable or reterminating fibers.

upvoted 2 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

The correct answer is:

A. Reverse the fibers.

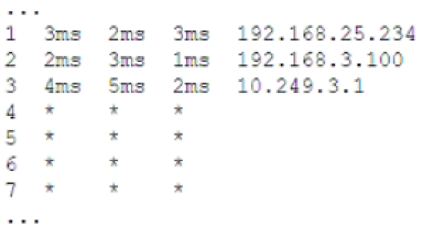
Explanation:
When terminating and connecting fiber cables, it's common to inadvertently reverse the transmit (Tx) and receive (Rx) fibers. In a fiber connection, one strand of the cable is used for transmitting data, while the other is used for receiving. If these strands are reversed, the devices cannot communicate, and the indicator light will not turn on.

Reversing the fibers is a quick and easy step to verify if the issue is due to Tx/Rx mismatching.

upvoted 2 times

Question #85 *Topic 1*

Users cannot connect to an internal website with an IP address 10.249.3.76. A network administrator runs a command and receives the following output:



```
...
1  3ms  2ms  3ms  192.168.25.234
2  2ms  3ms  1ms  192.168.3.100
3  4ms  5ms  2ms  10.249.3.1
4  *    *    *
5  *    *    *
6  *    *    *
7  *    *    *
...
```

Which of the following command-line tools is the network administrator using?

A. tracert

B. netstat

C. tcpdump

D. nmap

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

The correct answer is:
A. tracert

Explanation:
The output provided is from the tracert (on Windows) or traceroute (on Linux/Unix) command-line tool. This tool is used to trace the path packets take to reach a destination IP address or hostname. The output shows:

-A sequence of hops (routers) along the path.
-The response time for each hop.
-The IP addresses of the routers in the path.

In this case, the tool is showing the route to the destination 10.249.3.76, and it stops at 10.249.3.1, indicating a possible issue beyond this router.
upvoted 2 times

Question #86 *Topic 1*

After running a Cat 8 cable using passthrough plugs, an electrician notices that connected cables are experiencing a lot of cross talk. Which of the following troubleshooting steps should the electrician take first?

A. Inspect the connectors for any wires that are touching or exposed.

B. Restore default settings on the connected devices.

C. Terminate the connections again.

D. Check for radio frequency interference in the area.

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. Inspect the connectors for any wires that are touching or exposed.

Explanation:

Cat 8 cables are highly sensitive to proper termination due to their high-frequency performance requirements. Passthrough plugs can sometimes cause wires to touch or leave exposed conductors, leading to crosstalk. Inspecting the connectors for these issues is the quickest and least invasive first step in troubleshooting.

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

The correct answer is:

A. Inspect the connectors for any wires that are touching or exposed.

Explanation:

When experiencing cross-talk with a Cat 8 cable, one of the most common causes is improper termination, especially when using passthrough plugs. Improperly aligned or exposed wires can lead to signal interference and cross-talk. By visually inspecting the connectors, the electrician can identify if wires are incorrectly aligned, exposed, or not fully inserted into the connector.

upvoted 3 times

Question #87 *Topic 1*

A technician is troubleshooting a user's laptop that is unable to connect to a corporate server. The technician thinks the issue pertains to routing. Which of the following commands should the technician use to identify the issue?

A. tcpdump

B. dig

C. tracert

D. arp

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: C

C. tracert

Explanation:
The tracert (or traceroute on Linux/Mac) command is used to track the path that packets take from the source device to the destination server. It displays the route and the number of hops, helping identify where the connection may be failing, such as a misconfigured router or a broken link.

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: C

The correct answer is:

C. tracert

Explanation:
The tracert (on Windows) or traceroute (on Linux/Unix) command is used to trace the path packets take to reach a destination server. It identifies all the hops (routers) along the route and displays the time taken for each hop. This helps pinpoint where the routing issue might be occurring, such as a misconfigured router or a dead route.

upvoted 2 times

Question #88 *Topic 1*

After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect take to troubleshoot the issue?

A. Check to see if the end connections were wrapped in copper tape before terminating.

B. Use passthrough modular crimping plugs instead of traditional crimping plugs.

C. Connect the RX/TX wires to different pins.

D. Run a speed test on a device that can only achieve 100Mbps speeds.

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. Check to see if the end connections were wrapped in copper tape before terminating.

Explanation:
Cat 8 cables are designed for high-speed, high-frequency environments, and proper shielding is crucial to minimize interference. The shielding needs to be continuous, and ensuring that the end connections are wrapped in copper tape before termination helps maintain this shielding. If this step is overlooked, it can lead to higher interference and degraded performance.

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

The correct answer is:

A. Check to see if the end connections were wrapped in copper tape before terminating.

Explanation:
Cat 8 cables are designed for high-speed data transmission in data centers and have stringent requirements to minimize interference and maintain shielding integrity. One critical aspect of Cat 8 installation is ensuring that the shielding (often foil or braided) remains continuous and properly grounded, especially at termination points. Wrapping the end connections in copper tape before termination ensures proper contact with the keystone jack, maintaining the shield's effectiveness and minimizing interference.

upvoted 2 times

Question #89 *Topic 1*

A small business is deploying new phones, and some of the phones have full HD videoconferencing features. The Chief Information Officer is concerned that the network might not be able to handle the traffic if the traffic reaches a certain threshold. Which of the following can the network engineer configure to help ease these concerns?

A. A VLAN with 100Mbps speed limits

B. An IP helper to direct VoIP traffic

C. A smaller subnet mask

D. Full duplex on all user ports

Correct Answer: *A*

Community vote distribution

A (56%) B (33%) 11%

Community vote distribution

kinkistyle 1 month, 3 weeks ago

Selected Answer: A

The question is asking how to keep the network itself running under heavy load, not how to improve VoIP performance. In that case, the correct answer is to place limits on the bandwidth which is A

upvoted 3 times

Big_Wes 3 weeks, 6 days ago

This is correct. "Might not be able to handle the traffic" Concern = Bandwidth/Congestion
A. Solves Bandwidth and Congestion on the network
B. IP helpers are for DHCP Requests
C. Not even worth thought
D. ....

upvoted 1 times

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. A VLAN with 100Mbps speed limits.

Explanation:
Creating a VLAN specifically for the phones and configuring speed limits (such as 100Mbps) can help manage traffic and ensure that the network remains stable under high load conditions. VLANs segment traffic, which improves performance and reduces congestion by isolating specific types of traffic, such as VoIP and videoconferencing

upvoted 2 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

A is the most correct Answer.

upvoted 1 times

Hayder81 3 months, 1 week ago

Selected Answer: A

When deploying HD videoconferencing phones, Quality of Service (QoS) and traffic management become essential to ensure the network can handle increased traffic without degradation. Here's why a VLAN with traffic limits is the best solution

upvoted 2 times

KO443 3 months, 1 week ago

Selected Answer: A

C
Creating a VLAN with speed limits helps the network engineer manage HD videoconferencing traffic effectively, addressing the concern about

excessive network usage while maintaining overall network performance.
upvoted 2 times

⊟ **SuntzuLegacy** 3 months, 1 week ago

Selected Answer: B

The correct answer is:

B. An IP helper to direct VoIP traffic

Explanation:
Configuring an IP helper can assist in directing VoIP traffic to specific devices or servers (such as DHCP, TFTP, or call controllers) and ensure that network resources are properly allocated for VoIP operations. Additionally, implementing Quality of Service (QoS) in conjunction with IP helpers can prioritize VoIP traffic, which is sensitive to delays, jitter, and packet loss, ensuring that videoconferencing traffic does not degrade the overall network performance.
upvoted 1 times

⊟ **SuntzuLegacy** 3 months, 1 week ago

After extensive research A is the correct Answer. Its not D or B.
upvoted 1 times

⊟ **SuntzuLegacy** 3 months, 1 week ago

D is the correct answer.
upvoted 1 times

⊟ **favouralain** 3 months, 1 week ago

Selected Answer: D

D. Full duplex on all user ports. is the answer, because by configuring full duplex on all user ports, the network can handle more traffic efficiently, just like how super walkie-talkies make conversations smoother!
upvoted 1 times

⊟ **vandriel** 3 months, 2 weeks ago

Selected Answer: B

The speed limit for VOIP traffic makes no sense. B is correct as per chat gpt
upvoted 2 times

Question #90 *Topic 1*

A virtual machine has the following configuration:

IPv4 address: 169.254.10.10 -

Subnet mask: 255.255.0.0 -
The virtual machine can reach collocated systems but cannot reach external addresses on the internet. Which of the following is most likely the root cause?

A. The subnet mask is incorrect.

B. The DHCP server is offline.

C. The IP address is an RFC1918 private address.

D. The DNS server is unreachable.

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: B

B. The DHCP server is offline.

Explanation:
The IP address 169.254.x.x is an Automatic Private IP Addressing (APIPA) address, which is assigned when a device cannot obtain an IP address from a DHCP server. APIPA addresses allow communication within the same local subnet but cannot route traffic to external networks, such as the internet. This indicates that the DHCP server is offline or unreachable.

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: B

The correct answer is:

B. The DHCP server is offline.

Explanation:
The IP address 169.254.10.10 is a Link-Local Address, which is automatically assigned when a device cannot obtain an IP address from a DHCP server. These addresses (ranging from 169.254.0.0 to 169.254.255.255) are part of the Automatic Private IP Addressing (APIPA) scheme and are only valid for communication within the same local subnet. Devices with APIPA addresses cannot communicate with external networks, including the internet.

upvoted 2 times

Question #91 *Topic 1*

Which of the following is used to estimate the average life span of a device?

A. RPO

B. RTO

C. MTTR

D. MTBF

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: D

D. MTBF (Mean Time Between Failures).

Explanation:
MTBF is a metric used to estimate the average time a device operates before experiencing a failure. It is commonly used to predict the reliability and expected lifespan of a device or system.

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: D

The correct answer is:

D. MTBF (Mean Time Between Failures)

Explanation:
MTBF (Mean Time Between Failures) is a reliability metric that estimates the average life span of a device or system before a failure occurs. It is commonly used to predict the expected operational life of hardware components and helps organizations plan for maintenance and replacements.

upvoted 1 times

Question #92 Topic 1

Which of the following is the most secure way to provide site-to-site connectivity?

A. VXLAN

B. IKE

C. GRE

D. IPSec

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: D

D. IPSec (Internet Protocol Security).

Explanation:
IPSec is the most secure option for providing site-to-site connectivity. It offers strong encryption and authentication, ensuring that data transmitted between sites is protected against eavesdropping and tampering. It is widely used in VPNs to secure communication over untrusted networks like the Internet

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: D

The correct answer is:

D. IPSec (Internet Protocol Security)

Explanation:
IPSec is the most secure method for providing site-to-site connectivity. It provides strong encryption, authentication, and integrity to protect data as it travels between sites over an untrusted network like the internet. IPSec is often used to create secure VPN tunnels for site-to-site connections.

upvoted 1 times

Question #93 *Topic 1*

A network technician is terminating a cable to a fiber patch panel in the MDF. Which of the following connector types is most likely in use?

A. F-type

B. RJ11

C. BNC

D. SC

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: D

D. SC (Subscriber Connector).

Explanation:
SC connectors are commonly used for terminating fiber optic cables in data centers, MDFs (Main Distribution Frames), and other networking setups. They are push-pull connectors that provide secure connections and are widely used in fiber patch panels.

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: D

The correct answer is:

D. SC

Explanation:
SC (Subscriber Connector or Standard Connector) is one of the most common connector types used for terminating fiber optic cables in environments like a Main Distribution Frame (MDF). It is known for its snap-in/push-pull design, which provides a secure and reliable connection. SC connectors are widely used in patch panels, data centers, and enterprise networks.

upvoted 1 times

Question #94 *Topic 1*

A network administrator is connecting two Layer 2 switches in a network. These switches must transfer data in multiple networks. Which of the following would fulfill this requirement?

A. Jumbo frames

B. 802.1Q tagging

C. Native VLAN

D. Link aggregation

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: B

B. 802.1Q tagging

Explanation:
802.1Q tagging is the standard method used to enable VLAN (Virtual Local Area Network) tagging on a switch-to-switch link. This allows multiple VLANs to be transmitted over a single physical connection by tagging Ethernet frames with VLAN information. This is essential for transferring data across multiple networks between Layer 2 switches

upvoted 2 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: B

The correct answer is:

B. 802.1Q tagging

Explanation:
802.1Q tagging is a standard for VLAN tagging on Ethernet frames, which allows Layer 2 switches to transfer data for multiple VLANs across a single trunk link. When switches are connected using 802.1Q tagging, they can handle traffic from different VLANs by adding a VLAN tag to each Ethernet frame. This ensures that data for multiple networks (VLANs) is properly identified and routed across the trunk connection.

upvoted 3 times

Question #95 *Topic 1*

A network administrator wants users to be able to authenticate to the corporate network using a port-based authentication framework when accessing both wired and wireless devices. Which of the following is the best security feature to accomplish this task?

A. 802.1X

B. Access control list

C. Port security

D. MAC filtering

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. 802.1X

Explanation:
802.1X is a port-based network access control (PNAC) framework that provides authentication for devices trying to connect to the network, both wired and wireless. It uses an authentication server (typically RADIUS) to verify the identity of devices before granting them access, ensuring that only authorized users can connect to the network

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

The correct answer is:

A. 802.1X

Explanation:
802.1X is a port-based authentication framework that provides secure access control for devices connecting to a network, whether via wired or wireless connections. It works by authenticating users or devices before granting access to the network, using protocols like RADIUS (Remote Authentication Dial-In User Service). This ensures that only authorized users and devices can access the corporate network.

upvoted 1 times

Question #96 *Topic 1*

Which of the following is most closely associated with a dedicated link to a cloud environment and may not include encryption?

A. Direct Connect

B. Internet gateway

C. Captive portal

D. VPN

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: A

A. Direct Connect

Explanation:
Direct Connect is a service provided by cloud providers (such as AWS Direct Connect) that establishes a dedicated, private link between a company's on-premises network and the cloud environment. This connection is typically used for high-bandwidth, low-latency communication and may not include encryption by default, as the link itself is private and separate from the public internet.

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

The correct answer is:

A. Direct Connect

Explanation:
Direct Connect (or similar services, depending on the cloud provider) refers to a dedicated, private connection between an organization's on-premises network and a cloud environment. This connection does not go through the public internet and provides higher performance, lower latency, and more reliable bandwidth.

Since it is a private link, encryption is often not included by default, as the data does not traverse the public internet. However, encryption can be added if needed for additional security.

upvoted 1 times

Question #97 *Topic 1*

A systems administrator is investigating why users cannot reach a Linux web server with a browser but can ping the server IP. The server is online, the web server process is running, and the link to the switch is up. Which of the following commands should the administrator run on the server first?

A. traceroute

B. netstat

C. tcpdump

D. arp

Correct Answer: *B*

Community vote distribution

B (56%) C (44%)

Community vote distribution

ojones888 Highly Voted 3 months, 3 weeks ago

Selected Answer: C

C. tcpdump

Explanation:
Since users can ping the server but cannot access the web server via a browser, it suggests that the server's network interface is operational (because it responds to ICMP ping requests), but there may be an issue with the web server's network traffic or its ability to respond to HTTP requests.

tcpdump is a network packet analyzer that can capture and display packets on the network. Running tcpdump on the server will help the administrator observe if the server is receiving the HTTP requests (on port 80 for HTTP or port 443 for HTTPS) from users and whether the server is responding to those requests. This would be the first step to identify if the issue lies with the server not receiving or not responding to web traffic.

upvoted 5 times

Big_Wes 3 weeks, 6 days ago

Yes, but it asks which you should do FIRST. A simple netstat could verify this rather than looking through packets.

B. Netstat

upvoted 1 times

SuntzuLegacy Highly Voted 3 months, 1 week ago

Selected Answer: B

The correct answer is:
B. netstat

Explanation:
The netstat command is used to check the listening ports and active network connections on a system. Since the web server process is running and users can ping the server, the issue might be related to whether the web server is properly listening on the expected port (e.g., TCP port 80 for HTTP or TCP port 443 for HTTPS).

Running netstat (or its modern replacement, ss) can quickly verify if:

The web server is listening on the expected port.
The service is bound to the correct IP address or network interface.

upvoted 5 times

Nyang2 Most Recent 3 months, 1 week ago

Selected Answer: B

Check the netstat first.

Even if the demon is running, there is no port mapping or correcrt port number when checking netstat.

.

upvoted 3 times

Samuel1822 3 months, 1 week ago

Selected Answer: B

The netstat command helps verify if the server is listening on the correct port (e.g., 80 or 443 for HTTP/HTTPS)

upvoted 4 times

Question #98 *Topic 1*

Which of the following devices can operate in multiple layers of the OSI model?

A. Hub

B. Switch

C. Transceiver

D. Modem

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: B

B. Switch

Explanation:
A Switch can operate at multiple layers of the OSI model. Specifically:

A Layer 2 switch operates at the Data Link Layer, where it uses MAC addresses to forward frames within the same local network.
A Layer 3 switch (also known as a routing switch) can operate at the Network Layer, using IP addresses to perform routing functions between different networks.
This ability to function at both Layer 2 and Layer 3 allows switches to handle different types of network traffic and responsibilities.

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: B

The correct answer is:

B. Switch

Explanation:
A switch can operate at multiple layers of the OSI model, depending on its type:

Layer 2 (Data Link Layer):
Most switches are Layer 2 devices. They forward traffic based on MAC addresses and use a MAC address table to direct frames to the appropriate ports.

Layer 3 (Network Layer):
Layer 3 switches (often called multilayer switches) can perform routing functions, forwarding traffic based on IP addresses. These switches combine the functionality of traditional Layer 2 switches and routers, making them versatile in modern networks.

upvoted 1 times

Question #99 *Topic 1*

Before using a guest network, an administrator requires users to accept the terms of use. Which of the following is the best way to accomplish this goal?

A. Pre-shared key

B. Autonomous access point

C. Captive portal

D. WPA2 encryption

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: C

C. Captive portal

Explanation:
A captive portal is a web page that is presented to users when they first connect to a network, typically used in public Wi-Fi networks or guest networks. It forces users to accept the terms of use before granting full access to the internet or the network. This method is commonly used to ensure that users acknowledge and agree to the network's policies.

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: C

The correct answer is:
C. Captive portal

Explanation:
A captive portal is the best solution to require users to accept terms of use before accessing a guest network. A captive portal redirects users to a web page (often hosted by the network) where they must take specific actions, such as:

-Accepting terms and conditions.
-Entering credentials or payment information.
-Registering or completing other actions before gaining network access.

This is commonly used in public Wi-Fi networks, hotels, airports, and corporate guest networks.

upvoted 1 times

Question #100 *Topic 1*

A network administrator for a small office is adding a passive IDS to its network switch for the purpose of inspecting network traffic. Which of the following should the administrator use?

A. SNMP trap

B. Port mirroring

C. Syslog collection

D. API integration

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

HeatSquad77 2 months, 1 week ago

Selected Answer: B

B. Port mirroring

Explanation:
Port mirroring (also known as SPAN on Cisco devices) is the process of copying network traffic from one port (or a group of ports) on a switch to another port where a monitoring device, such as an Intrusion Detection System (IDS), can inspect the traffic. This is the best method for deploying a passive IDS because it allows the IDS to analyze network traffic without interfering with or disrupting the normal flow of data.

upvoted 1 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: B

The correct answer is:
B. Port mirroring

Explanation:
Port mirroring (also known as SPAN, Switched Port Analyzer) is the correct method for enabling a passive Intrusion Detection System (IDS) to inspect network traffic. Port mirroring copies all traffic from one or more switch ports or VLANs to a designated port where the IDS is connected. This allows the IDS to analyze the network traffic without interfering with the normal flow of data, fulfilling the requirement for passive monitoring.

upvoted 1 times

Question #101 *Topic 1*

Which of the following most likely requires the use of subinterfaces?

A. A router with only one available LAN port

B. A firewall performing deep packet inspection

C. A hub utilizing jumbo frames

D. A switch using Spanning Tree Protocol

Correct Answer: *A*

HeatSquad77 2 months ago

Selected Answer: A

A. A router with only one available LAN port

Explanation:

Subinterfaces are logical interfaces created on a single physical interface of a network device, such as a router. They are commonly used in scenarios where multiple VLANs or networks need to be configured on a single physical interface. Each subinterface is assigned its own VLAN ID and IP configuration.

upvoted 1 times

Nateforreal 2 months ago

Selected Answer: A

Google says a router , But can someone please correct if wrong?

upvoted 2 times

Question #102 *Topic 1*

A company receives a cease-and-desist order from its ISP regarding prohibited torrent activity. Which of the following should be implemented to comply with the cease-and-desist order?

A. MAC security

B. Content filtering

C. Screened subnet

D. Perimeter network

Correct Answer: *B*

HeatSquad77 2 months ago

Selected Answer: B

B. Content filtering

Explanation:
Content filtering allows an organization to block or restrict access to specific types of content, such as torrenting websites or peer-to-peer (P2P) file-sharing activities. By implementing content filtering, the company can ensure compliance with the ISP's cease-and-desist order by preventing users from accessing prohibited services or websites.

upvoted 1 times

Question #103 *Topic 1*

Which of the following requires network devices to be managed using a different set of IP addresses?

A. Console

B. Split tunnel

C. Jump box

D. Out of band

Correct Answer: *D*

HeatSquad77 2 months ago

Selected Answer: D

D. Out of band

Explanation:

Out-of-band (OOB) management requires a separate network or set of IP addresses to manage devices independently of the production network. This ensures that management traffic is isolated from regular network traffic, providing enhanced security and access even if the primary network is down.

upvoted 2 times

Question #104 *Topic 1*

A network administrator wants to configure a backup route in case the primary route fails. A dynamic routing protocol is not installed on the router. Which of the following routing features should the administrator choose to accomplish this task?

A. Neighbor adjacency

B. Link state flooding

C. Administrative distance

D. Hop count

Correct Answer: *C*

Big_Wes 3 weeks, 5 days ago

Selected Answer: C

it states "A dynamic protocol is not installed on the router", Hop count cannot manage backup routes without this.

C. Administrative Distance

upvoted 1 times

93831b0 1 month ago

Selected Answer: C

I'm a bit torn here. Both Hop Count and Administrative Distance seem relevant, but I need to think about the context. Since the routing protocol isn't dynamic, they might be using static routing or have administrative nodes set up certain rules based on hop counts. Therefore, choosing Administrative Distance could make sense as a way to configure backup routes by applying administrative criteria that include hop counts.
But then again, hop count is more of a metric used during route discovery and management rather than an administrative setting for backup routing. So, perhaps the correct answer is D. Hop Count if they're using static routing based on known network segments, or C. Administrative distance as an administrative rule that includes hop counts.
I'm still leaning towards C. Administrative distance because it allows applying administrative criteria like considering hop count when setting up backup routes.

upvoted 1 times

93831b0 2 weeks, 2 days ago

After some more research have also found that Hop count is a routing metric used by older distance-vector routing protocols like RIP. While hop count can influence routing decisions, it's not the primary mechanism for configuring a backup route, especially when static routes are involved.

upvoted 1 times

OldManJim 1 month, 1 week ago

Selected Answer: C

Administrator wants to CONFIGURE a route....

upvoted 1 times

b359e92 1 month, 1 week ago

Selected Answer: C

GPT
C. Administrative distance

Administrative Distance – It allows the router to prioritize a backup static route if the primary route fails.

upvoted 2 times

Chris_128 1 month, 3 weeks ago

Selected Answer: D

D. Hop count

Hop count is a routing feature.

Administrative distance is a configuration not a feature.

upvoted 4 times

⊟ **HeatSquad77** 2 months ago

Selected Answer: C

C. Administrative distance

Explanation:
Administrative distance (AD) is a value used by routers to prioritize routes when multiple routes to the same destination are available. By configuring static routes with different administrative distances, the network administrator can set one route as the primary (lower AD) and another as the backup (higher AD). If the primary route fails, the router will automatically switch to the backup route with the higher AD.

upvoted 2 times

Question #105 *Topic 1*

Which of the following steps of the troubleshooting methodology should a technician take to confirm a theory?

A. Duplicate the problem.

B. Identify the symptoms.

C. Gather information.

D. Determine any changes.

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

HeatSquad77 2 months ago

Selected Answer: A

A. Duplicate the problem.

Explanation:

To confirm a theory, a technician needs to reproduce the issue under similar conditions to ensure the identified cause matches the symptoms and behavior of the problem. Duplicating the problem helps validate the theory and provides evidence that the suspected cause is correct.

upvoted 1 times

GT256 3 months, 4 weeks ago

Selected Answer: A

I think "A" is correct. You're right though, all these choices are part of the information-gathering phase but the only choice that can allow you to directly confirm your theory is by "duplicating the problem" (again) after making some changes.

upvoted 2 times

ec80b38 4 months ago

This should be C but Correct me if im wrong under step three on the comptia website it is said this step is also part of the "information-gathering" phase

upvoted 1 times

MIXDBAG 3 months, 4 weeks ago

Duplicating the problem is what confirms the theory, the answer is A

upvoted 1 times

GT256 3 months, 4 weeks ago

I think "A" is correct. You're right though, all these choices are part of the information-gathering phase but the only choice that can allow you to directly confirm your theory is by "duplicating the problem" (again) after making some changes.

upvoted 1 times

Question #106 *Topic 1*

A network administrator is deploying a new switch and wants to make sure that the default priority value was set for a spanning tree. Which of the following values would the network administrator expect to see?

A. 4096

B. 8192

C. 32768

D. 36684

Correct Answer: *C*

Philco 1 month, 1 week ago

Selected Answer: C

The default priority value is derived by multiplying 8 by 4096.
priority value is typically configured in increments of 4096
default priority value for a spanning tree is 32768
In spanning tree protocol, a lower priority value indicates a higher priority, meaning a switch with a lower priority is more likely to be chosen as the root bridge.

upvoted 2 times

HeatSquad77 2 months ago

Selected Answer: C

C. 32768

Explanation:
In the Spanning Tree Protocol (STP), the default priority value for a switch is typically set to 32768. This value is combined with the VLAN ID to form the Bridge ID, which determines the root bridge in an STP topology.

upvoted 1 times

Question #107 *Topic 1*

A network administrator is configuring a wireless network with an ESSID. Which of the following is a user benefit of ESSID compared to SSID?

A. Stronger wireless connection

B. Roaming between access points

C. Advanced security

D. Increased throughput

Correct Answer: *B*

Philco 1 month, 1 week ago

Selected Answer: B

user benefit of ESSID compared to SSID is that it allows for seamless roaming between multiple access points within a network, meaning a user can move between different locations in a building while maintaining a constant connection to the same network name (ESSID), without needing to manually reconnect to a new access point (SSID); essentially providing uninterrupted connectivity across a larger area.

ESSID :

Represents the entire wireless network, including multiple access points, and ensures consistent network name across the whole network, enabling seamless roaming

SSID

Refers to the visible network name that users see and connect to on a single access point.

upvoted 1 times

HeatSquad77 2 months, 1 week ago

Selected Answer: B

The Extended Service Set Identification (ESSID) is an identifier for your wireless network.

upvoted 1 times

Question #108 *Topic 1*

A network administrator needs to connect two routers in a point-to-point configuration and conserve IP space. Which of the following subnets should the administrator use?

A. /24

B. /26

C. /28

D. /30

Correct Answer: *D*

HeatSquad77 2 months ago

Selected Answer: D

D. /30

Explanation:
A /30 subnet provides 4 IP addresses in total, with 2 usable IP addresses for hosts. This is ideal for a point-to-point link because only two IP addresses are needed (one for each router).

upvoted 1 times

Question #109 *Topic 1*

An attacker follows an employee through a badge-secured door before the door closes. Which of the following types of attacks is occurring?

A. Shoulder surfing

B. Tailgating

C. Phishing

D. On-path

Correct Answer: *B*

HeatSquad77 2 months, 1 week ago

Selected Answer: B

tailgating is following someone into a secure area without them knowing

upvoted 1 times

Question #110 *Topic 1*

A research facility is expecting to see an exponential increase in global network traffic in the near future. The offices are equipped with 2.5Gbps fiber connections from the ISP, but the facility is currently only utilizing 1Gbps connections. Which of the following would need to be configured in order to use the ISP's connection speed?

A. 802.1Q tagging

B. Network address translation

C. Port duplex

D. Link aggregation

Correct Answer: *D*

HeatSquad77 2 months, 1 week ago

Selected Answer: D

Link aggregation is a networking technique that combines multiple network connections into a single logical link

upvoted 2 times

Question #111 *Topic 1*

A VoIP phone is plugged in to a port but cannot receive calls. Which of the following needs to be done on the port to address the issue?

A. Trunk all VLANs on the port.

B. Configure the native VLAN.

C. Tag the traffic to voice VLAN.

D. Disable VLANs.

Correct Answer: *C*

HeatSquad77 2 months ago

Selected Answer: C

C. Tag the traffic to voice VLAN.

Explanation:

Voice VLANs are used to separate voice traffic from other types of traffic for better performance and Quality of Service (QoS).

upvoted 1 times

Question #112 *Topic 1*

Which of the following can support a jumbo frame?

A. Access point

B. Bridge

C. Hub

D. Switch

Correct Answer: *D*

HeatSquad77 2 months ago

Selected Answer: D

D. Switch

Explanation:

A jumbo frame is an Ethernet frame with a payload larger than the standard 1500 bytes, typically up to 9000 bytes. Jumbo frames are commonly used in environments requiring high throughput and reduced CPU overhead, such as data centers and storage networks

upvoted 1 times

Question #113 *Topic 1*

A network manager wants to implement a SIEM system to correlate system events. Which of the following protocols should the network manager verify?

A. NTP

B. DNS

C. LDAP

D. DHCP

Correct Answer: *A*

HeatSquad77 2 months ago

Selected Answer: A

A. NTP

Explanation:
A SIEM (Security Information and Event Management) system collects and correlates logs and events from multiple devices across a network. Accurate time synchronization is crucial to ensure that logs and events from different sources are correlated correctly.
NTP (Network Time Protocol) is used to synchronize the clocks of network devices, ensuring that timestamps in logs are consistent across the network.

upvoted 1 times

Question #114 *Topic 1*

A network engineer is designing a secure communication link between two sites. The entire data stream needs to remain confidential. Which of the following will achieve this goal?

A. GRE

B. IKE

C. ESP

D. AH

Correct Answer: *C*

HeatSquad77 2 months ago

Selected Answer: C

C. ESP

Explanation:
ESP (Encapsulating Security Payload) is a protocol used in IPSec to provide confidentiality, integrity, and authentication for data transmitted over a network. ESP encrypts the entire data payload, ensuring that the data stream remains confidential. This is the most suitable option for maintaining confidentiality in a secure communication link.

upvoted 1 times

02fd592 2 months, 2 weeks ago

Selected Answer: C

ESP (Encapsulating Security Payload): a protocol that encrypts and authenticates data packets in IPsec

upvoted 2 times

Question #115 *Topic 1*

Which of the following protocols has a default administrative distance value of 90?

A. RIP

B. EIGRP

C. OSPF

D. BGP

Correct Answer: *B*

HeatSquad77 2 months ago

Selected Answer: B

B. EIGRP

Explanation:
EIGRP (Enhanced Interior Gateway Routing Protocol) has a default administrative distance (AD) value of 90. This value is used to determine the trustworthiness of routes learned from different routing protocols. The lower the AD, the more preferred the route.

upvoted 1 times

Question #116 *Topic 1*

An office is experiencing intermittent connection issues. A network engineer identifies that the issue occurs whenever someone uses the fax machine that is connected to a switch. Which of the following should the engineer do first to resolve the issue?

A. Run a new Cat 5 line.

B. Enable 802.1Q tagging.

C. Change the MTU.

D. Configure a VLAN.

Correct Answer: *D*

Community vote distribution

A (100%)

Community vote distribution

ec_ 4 days, 18 hours ago

Selected Answer: D

Isolating the fax machine into a dedicated VLAN is the most effective first step to mitigate interference and stabilize the network. This approach directly addresses the correlation between fax usage and network disruption.

upvoted 1 times

HeatSquad77 2 months ago

Selected Answer: D

D. Configure a VLAN.

Explanation:
The issue described suggests that the fax machine, which is likely generating a high amount of traffic or interference, is causing disruption to other devices on the same network segment. In this case, placing the fax machine on a separate VLAN can help isolate it from other devices and prevent it from interfering with regular network traffic.

upvoted 2 times

jmcd2 2 months, 1 week ago

Selected Answer: D

D Configure a VLAN
The fax machine's network traffic could be causing interference or broadcast issues that disrupt other devices on the same network. By configuring a VLAN (Virtual Local Area Network), the engineer can isolate the traffic from the fax machine onto its own separate network segment, preventing it from affecting other devices.

upvoted 2 times

SuntzuLegacy 3 months, 1 week ago

Selected Answer: A

A run a new Cat 5 Line is correct.

upvoted 1 times

escomgmt 3 months, 3 weeks ago

A. Run a new Cat 5 line, Intermittent connection issues when a fax machine (often analog and potentially connected through a VoIP adapter or similar setup) is in use suggest possible interference or crosstalk on the current cable. Running a new, dedicated Cat 5 line for the fax machine would isolate it from the rest of the network traffic on the switch, reducing interference and connection problems. This is a straightforward approach to eliminate potential issues with shared cabling or interference.

upvoted 1 times

> **ojones888** 3 months, 3 weeks ago
>
> Running a new Cat 5 cable could potentially help if there is a physical connection issue, but it is unlikely to address the specific issue of intermittent connection problems caused by the fax machine. The problem seems more related to network configuration rather than the physical connection.

upvoted 5 times

Question #117 *Topic 1*

A network engineer receives a vendor alert regarding a vulnerability in a router CPU. Which of the following should the engineer do to resolve the issue?

A. Update the firmware.

B. Replace the system board.

C. Patch the OS.

D. Isolate the system.

Correct Answer: *A*

TTechman 6 days, 8 hours ago

Selected Answer: A

A. Update the firmware.

upvoted 1 times

Cpl_copenhagen 2 weeks, 2 days ago

Selected Answer: D

No need to speculate here. Anytime you discover vulnerability, you should isolate the system, patch the system, then bring it back into your network.

upvoted 1 times

TTechman 6 days, 8 hours ago

yes, however, the question doesn't ask what to do "first", just what should the engineer do. so update the firmware solves the issue. Isolate only mitigates until an update is applied. just my 2 cents.

upvoted 1 times

HeatSquad77 2 months ago

Selected Answer: A

A. Update the firmware.

Explanation:
A vulnerability in a router CPU is likely related to firmware or software running on the device that could be exploited by attackers. To resolve this, the network engineer should look for a firmware update from the vendor that addresses the vulnerability. Firmware updates often contain security patches or fixes for known vulnerabilities in hardware and software.

upvoted 2 times

Question #118 *Topic 1*

Which of the following fiber connector types is the most likely to be used on a network interface card?

A. LC

B. SC

C. ST

D. MPO

Correct Answer: *A*

HeatSquad77 2 months ago

Selected Answer: A

A. LC

Explanation:
The LC (Lucent Connector) is the most commonly used fiber connector type on network interface cards (NICs), especially for modern high-speed networks. LC connectors are smaller in size, making them more suitable for devices like network cards and switches where space is a consideration. Additionally, LC connectors are often used in single-mode and multimode fiber connections.

upvoted 1 times

Question #119 *Topic 1*

Which of the following connectors provides console access to a switch?

A. ST

B. RJ45

C. BNC

D. SFP

Correct Answer: *B*

HeatSquad77 2 months, 1 week ago

Selected Answer: B

RJ45 is the type of connection you'd use to manage the switch

upvoted 1 times