Free Questions for CCST-Networking by ebraindumps

Shared by Abbott on 27-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which device protects the network by permitting or denying traffic based on IP address, port number, or application?

Options:

A- Firewall

B- Access point

C- VPN gateway

D- Intrusion detection system

Answer:

A

Explanation:

Firewall: A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It permits or denies traffic based on IP addresses, port numbers, or applications.

Access Point: This is a device that allows wireless devices to connect to a wired network using Wi-Fi. It does not perform traffic filtering based on IP, port, or application.

VPN Gateway: This device allows for secure connections between networks over the internet, but it is not primarily used for traffic filtering based on IP, port, or application.

Intrusion Detection System (IDS): This device monitors network traffic for suspicious activity and policy violations, but it does not actively permit or deny traffic.

Understanding Firewalls: Firewall Basics

Question 2

Question Type: **MultipleChoice**

Which address is included in the 192.168.200.0/24 network?

Options:

A- 192.168.199.13

B- 192.168.200.13

C- 192.168.201.13

D- 192.168.1.13

Answer:

B

Explanation:

* 192.168.200.0/24 Network: This subnet includes all addresses from 192.168.200.0 to 192.168.200.255. The /24 indicates a subnet mask of 255.255.255.0, which allows for 256 addresses.

* 192.168.199.13: This address is in the 192.168.199.0/24 subnet, not the 192.168.200.0/24 subnet.

* 192.168.200.13: This address is within the 192.168.200.0/24 subnet.

* 192.168.201.13: This address is in the 192.168.201.0/24 subnet, not the 192.168.200.0/24 subnet.

* 192.168.1.13: This address is in the 192.168.1.0/24 subnet, not the 192.168.200.0/24 subnet.

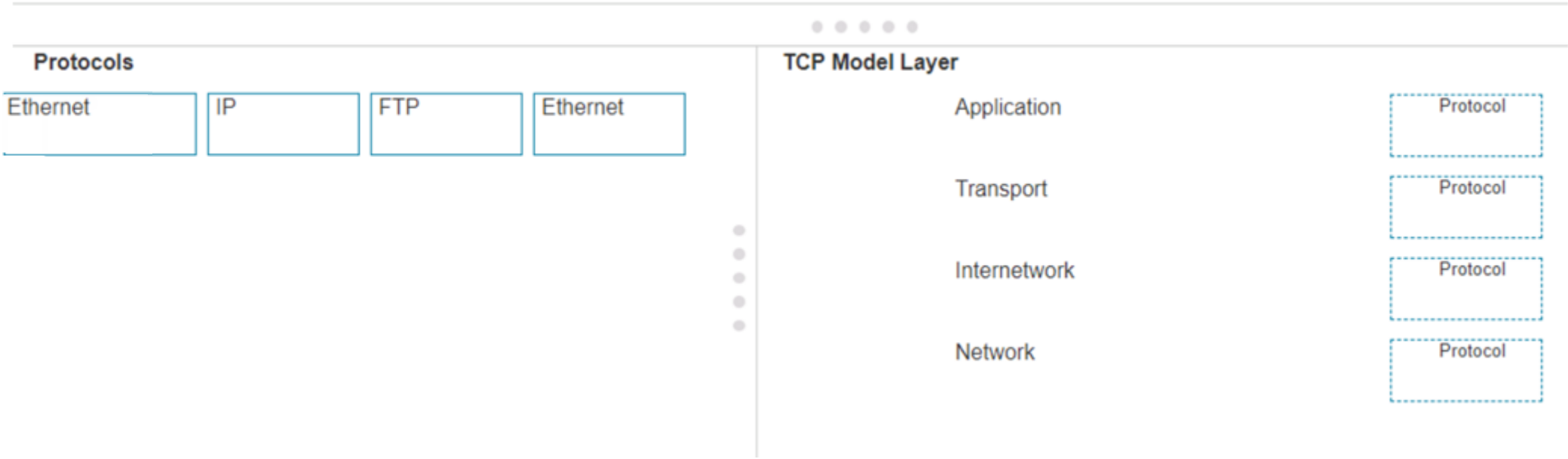
* Subnetting Guide: Subnetting Basics

Question 3

Question Type: DragDrop

Move each protocol from the list on the left to the correct TCP/IP model layer on the right.

Note: You will receive partial credit for each correct match.



Explanation:

TCP/IP Model Overview: Cisco TCP/IP Model

Understanding the TCP/IP Model: TCP/IP Layers

Question 4

Question Type: **Hotspot**

You plan to use a network firewall to protect computers at a small office.

For each statement about firewalls, select True or False.

Note: You will receive partial credit for each correct selection.

	True	Fals
A firewall can direct all web traffic to a specific IP address.	○	○
A firewall can block traffic to specific ports on internal computers.	○	○
A firewall can prevent specific apps from running on a computer.	○	○

An

Explanation:

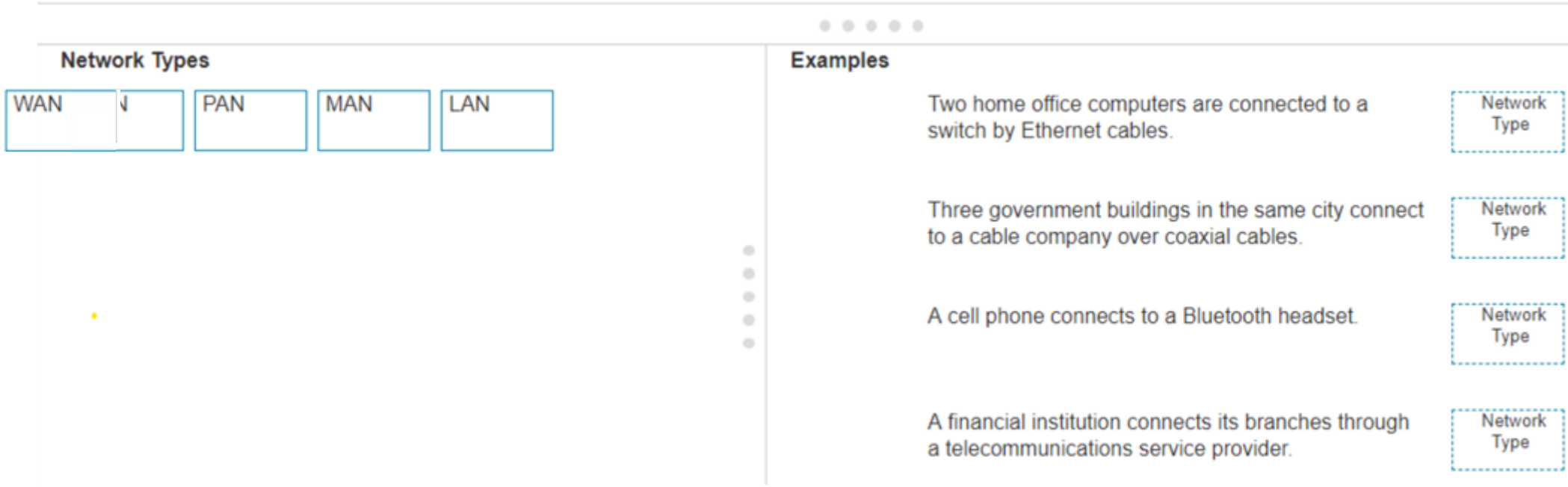
Understanding Firewalls: Firewall Capabilities

Network Security Best Practices: Network Security Guide

Question 5

Question Type: DragDrop

Move each network type from the list on the left to the correct example on the right.



Explanation:

Network Types Overview: Cisco Networking Basics

Understanding Different Network Types: Network Types Guide

Question 6

Question Type: **MultipleChoice**

Which two pieces of information should you include when you initially create a support ticket? (Choose 2.)

Options:

A- A detailed description of the fault

B- Details about the computers connected to the network

C- A description of the conditions when the fault occurs

D- The actions taken to resolve the fault

E- The description of the top-down fault-finding procedure

Answer:

A, C

Explanation:

Statement A: 'A detailed description of the fault.' This is essential for support staff to understand the nature of the problem and begin troubleshooting effectively.

Statement C: 'A description of the conditions when the fault occurs.' This helps in reproducing the issue and identifying patterns that might indicate the cause of the fault.

Statement B: 'Details about the computers connected to the network.' While useful, this is not as immediately critical as understanding the fault itself and the conditions under which it occurs.

Statement D: 'The actions taken to resolve the fault.' This is important but typically follows the initial report.

Statement E: 'The description of the top-down fault-finding procedure.' This is more of a troubleshooting methodology than information typically included in an initial support ticket.

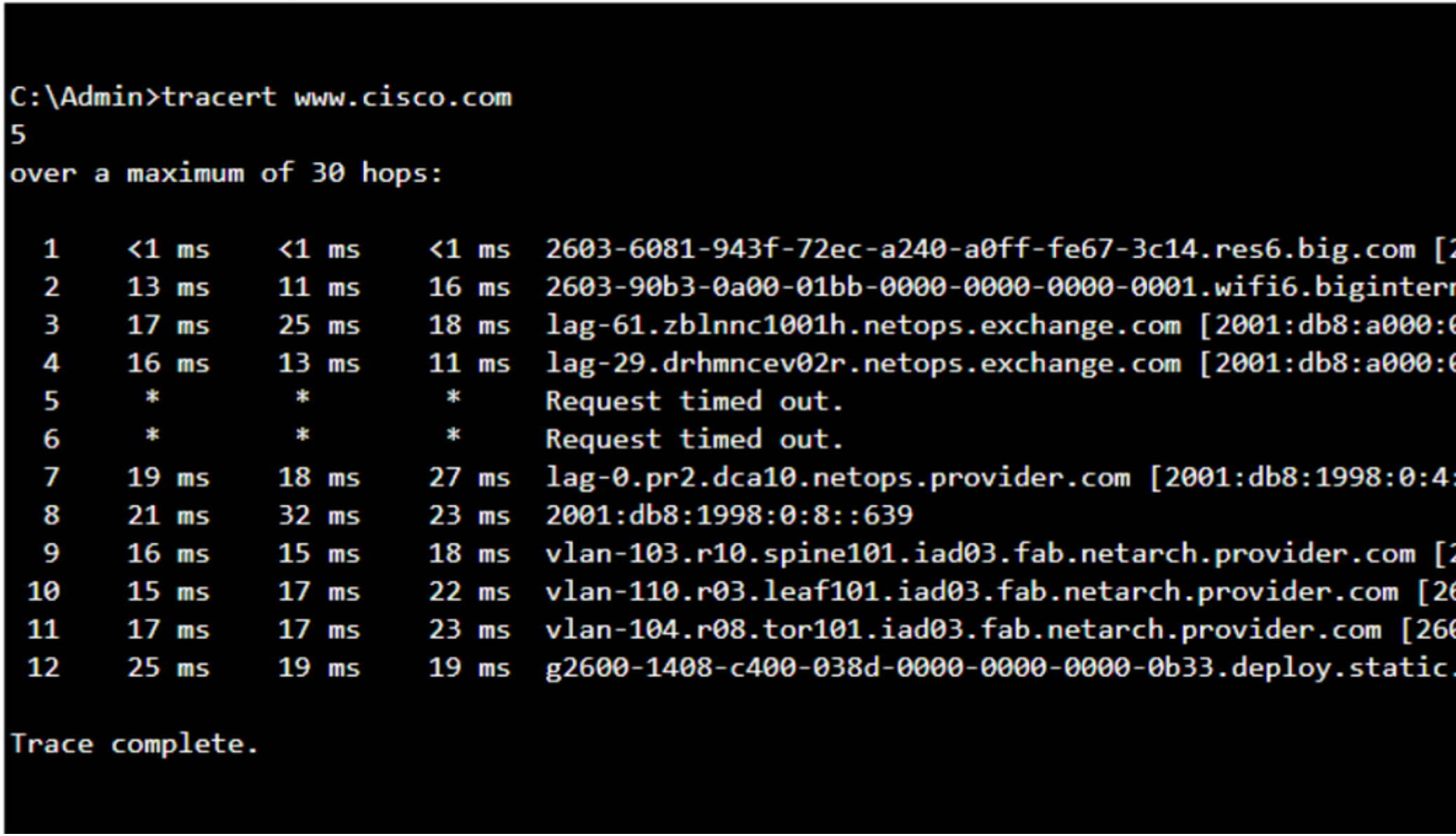
Best Practices for Submitting Support Tickets: Support Ticket Guidelines

Question 7

Question Type: **MultipleChoice**

Examine the following output:

Examine the following command output:



```
C:\Admin>tracert www.cisco.com
5
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  2603-6081-943f-72ec-a240-a0ff-fe67-3c14.res6.big.com [
  2    13 ms    11 ms    16 ms  2603-90b3-0a00-01bb-0000-0000-0000-0001.wifi6.biginter
  3    17 ms    25 ms    18 ms  lag-61.zblnnc1001h.netops.exchange.com [2001:db8:a000:
  4    16 ms    13 ms    11 ms  lag-29.drhmncev02r.netops.exchange.com [2001:db8:a000:
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    19 ms    18 ms    27 ms  lag-0.pr2.dca10.netops.provider.com [2001:db8:1998:0:4
  8    21 ms    32 ms    23 ms  2001:db8:1998:0:8::639
  9    16 ms    15 ms    18 ms  vlan-103.r10.spine101.iad03.fab.netarch.provider.com [
 10    15 ms    17 ms    22 ms  vlan-110.r03.leaf101.iad03.fab.netarch.provider.com [2
 11    17 ms    17 ms    23 ms  vlan-104.r08.tor101.iad03.fab.netarch.provider.com [26
 12    25 ms    19 ms    19 ms  g2600-1408-c400-038d-0000-0000-0000-0b33.deploy.static

Trace complete.
```

Which two conclusions can you make from the output of the tracert command? (Choose 2.)

Note: You will receive partial credit for each correct answer.

Options:

A- The trace successfully reached the www.cisco.com server.

B- The trace failed after the fourth hop.

C- The IPv6 address associated with the www.cisco.com server is 2600:1408: c400: 38d: : b33.

D- The routers at hops 5 and 6 are offline.

E- The device sending the trace has IPv6 address 2600:1408:c400:38d :: b33.

Answer:

A, C

Explanation:

* Statement A: 'The trace successfully reached the www.cisco.com server.' This is true as indicated by the 'Trace complete' message at the end, showing that the trace has reached its destination.

* Statement C: 'The IPv6 address associated with the www.cisco.com server is 2600:1408:c400:38d::b33.' This is true because the final hop in the trace, which is the destination, has this IPv6 address.

* Statement B: 'The trace failed after the fourth hop.' This is incorrect as the trace continues beyond the fourth hop, despite some intermediate timeouts.

* Statement D: 'The routers at hops 5 and 6 are offline.' This is not necessarily true. The routers might be configured to not respond to traceroute requests.

* Statement E: 'The device sending the trace has IPv6 address 2600:1408:c400:38d::b33.' This is incorrect; this address belongs to the destination server, not the sender.

* Understanding Traceroute: Traceroute Guide

Question 8

Question Type: **DragDrop**

Move each cloud computing service model from the list on the left to the correct example on the right

Note: You will receive partial credit for each correct answer.

Explanation:

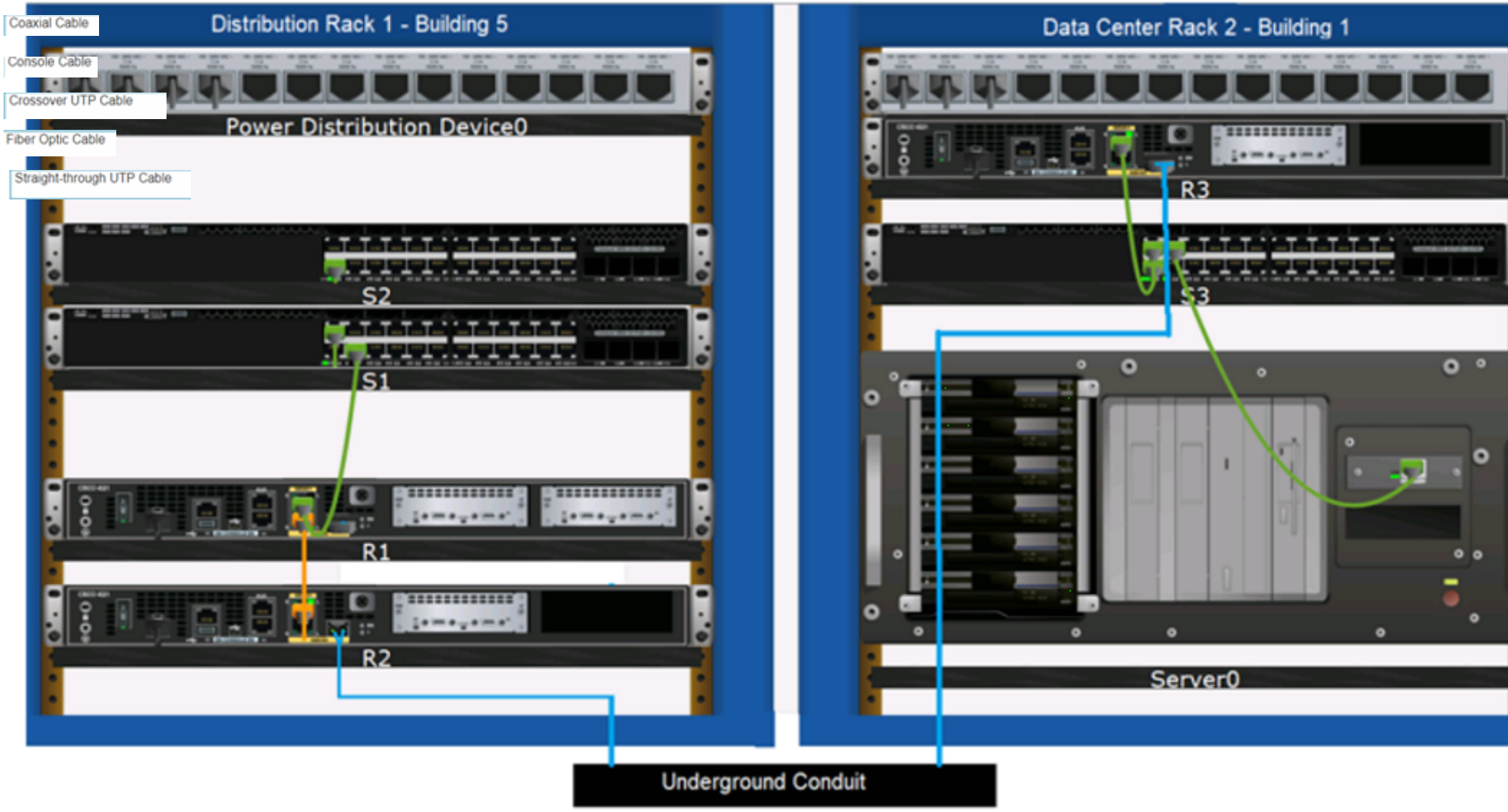
Cloud Service Models: Understanding IaaS, PaaS, SaaS

NIST Definition of Cloud Computing: NIST Cloud Computing

Question 9

Question Type: **DragDrop**

Examine the connections shown in the following image. Move the cable types on the right to the appropriate connection description on the left. You may


Coaxial Cable
Console Cable
Crossover UTP Cable
Fiber Optic Cable
Straight-through UTP Cable
Distribution Rack 1 - Building 5
Power Distribution Device0
S2
S1
R1
R2
Data Center Rack 2 - Building 1
R3
S3
Server0
Underground Conduit

Explanation:

Network Cable Types and Uses: Cisco Network Cables

Understanding Ethernet Cabling: Ethernet Cable Guide