Fortinet NSE6_OTS_AR-7.6 Mock Exam

Shared by Wooten on 17-06-2026

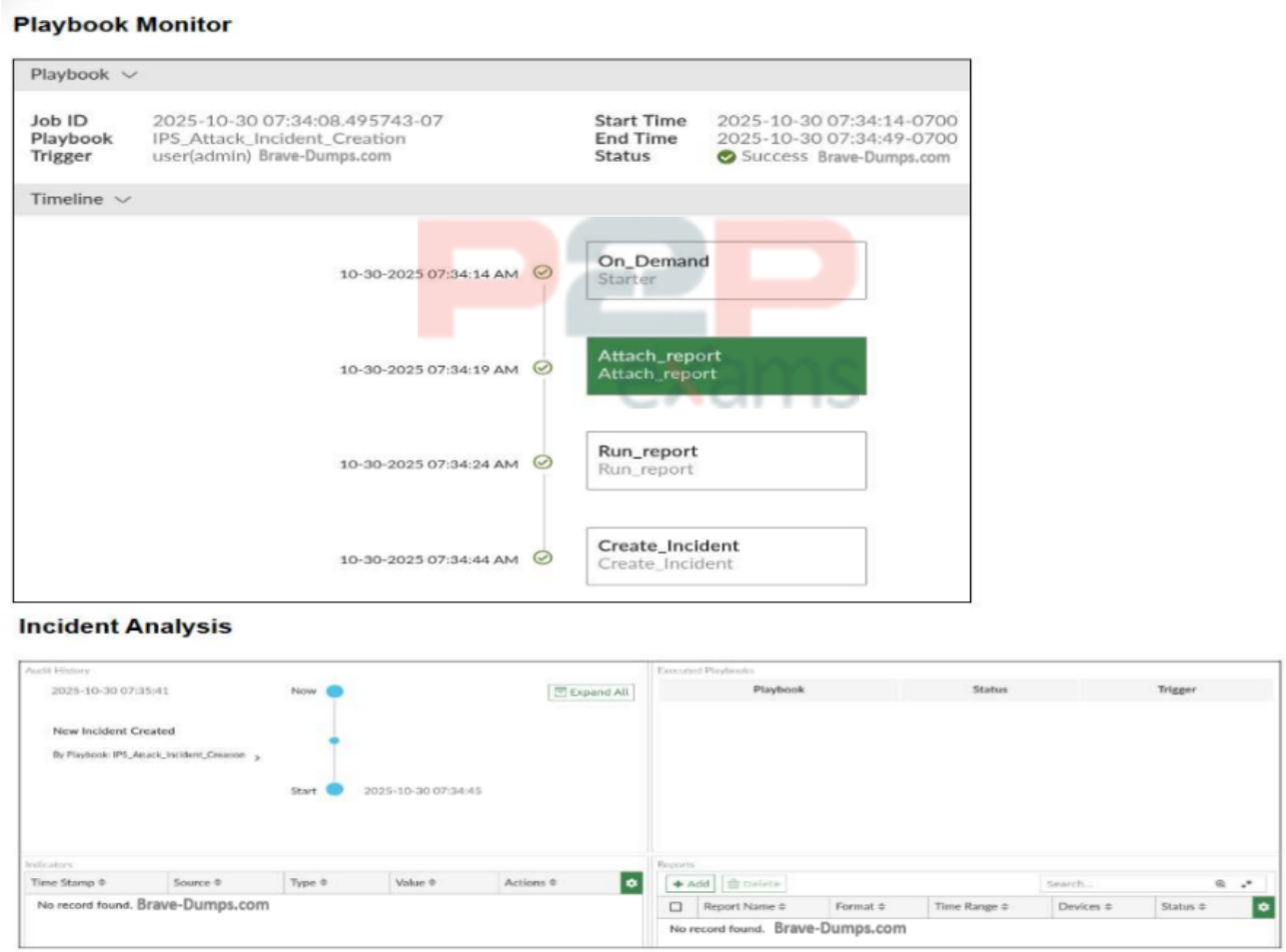
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibits.



The Playbook Monitor dashboard and the analysis of the corresponding incident analysis are shown. You created the playbook with the objective of automatically attaching the report to the incident that was created. Which two statements are correct? (Choose two answers)

Options:

A- You must wait for the report to be generated and attached to the incident.
B- Only the Create_Incident task was executed.
C- The tasks in the playbook must be reordered.
D- The playbook was triggered manually.

Answer:

C, D

Explanation:

The correct answers are C and D.

Option D is correct because the Playbook Monitor clearly shows the starter as On_Demand and the trigger as user(admin). The study guide states that ''ON_DEMAND: The playbook runs when an administrator manually starts it'' and also notes that to run it manually, you select the playbook and click Run. This exactly matches the exhibit, so the playbook was manually triggered.

Option C is also correct. The study guide explains that ''tasks run one after another'' and that ''if needed, the output of one task can be used by the tasks that follow it.'' It also gives an example where workflow logic matters, such as creating an incident and then attaching details to it. In the exhibit, the sequence shown is Attach_report, then Run_report, then Create_Incident, while the incident analysis shows no report attached. Since the report must exist and the incident must already be available before it can be attached properly, the task order is wrong and must be reordered.

Option B is incorrect because the monitor shows multiple tasks completed successfully, not only Create_Incident. Option A is not the best answer because the main problem demonstrated by the exhibits is not simply waiting time, but the incorrect workflow order. The playbook completed successfully, yet the report is still not attached, which indicates a design issue in the task sequence rather than just a delay.

Question 2

Question Type: MultipleChoice

What are two advantages provided by industrial Ethernet? (Choose two answers)

Options:

A- Encryption
B- Real-time control
C- Remote access
D- Determinism

Answer:

B, D

Explanation:

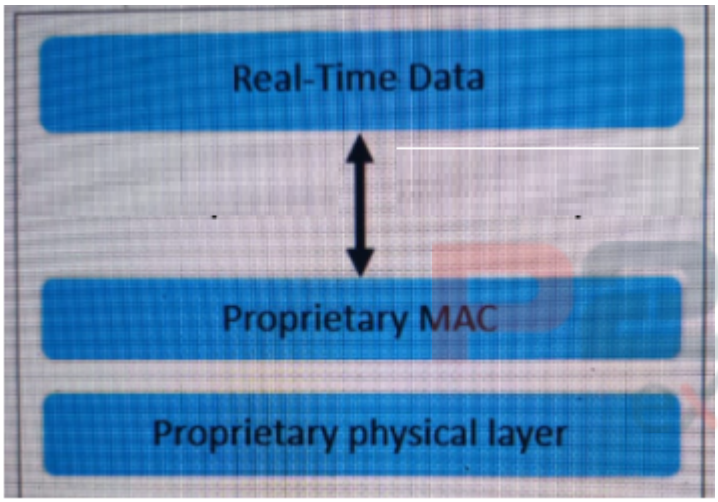
The correct answers are B. Real-time control and D. Determinism. The study guide defines industrial Ethernet as the ''use of Ethernet and TCP/IP as transport mechanisms for industrial protocols'' and states that it provides ''real-time control,'' ''low latency,'' and ''determinism (meaning reliable and predictable data delivery)'' in harsh environments. It further explains that industrial Ethernet ''provides deterministic communication between machine controllers, actuators, sensors, and other units.'' These statements directly confirm that the two key advantages are real-time control and determinism.

The other options are not supported by the study guide as core advantages of industrial Ethernet. Encryption is not listed as one of the benefits in this section, and remote access is discussed elsewhere in the OT architecture but not as a defining advantage of industrial Ethernet itself. The guide is explicit that the main benefits here are predictable delivery and real-time communication, which are essential in industrial control environments where timing and reliability matter.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



An industrial Ethernet protocol skipping layers 3 to 6 is shown. Which industrial Ethernet protocol is it? (Choose one answer)

Options:

A- POWERLINK

B- Ethernet over industrial protocol

C- Modbus
D- EtherCAT

Answer:

D

Explanation:

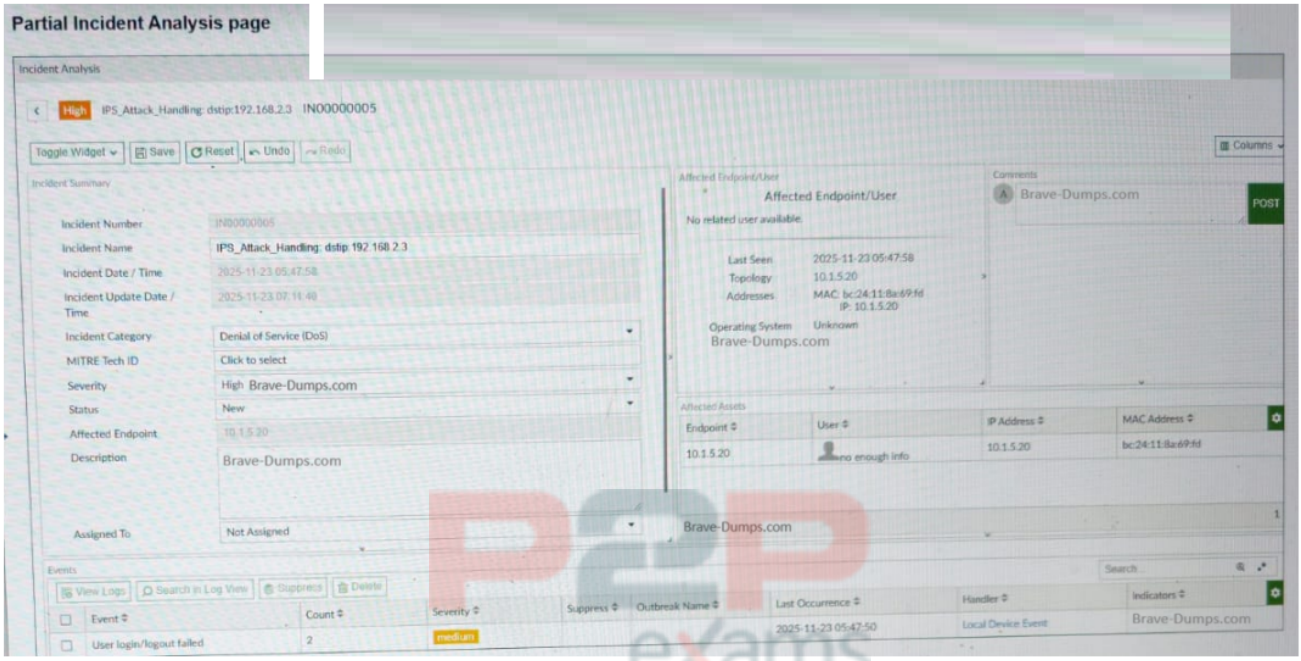
The correct answer is D. EtherCAT. The study guide explicitly states under the Ethernet/IP and EtherCAT section that ''EtherCAT is a protocol that offers real-time communication in a primary-secondary configuration'' and ''EtherCAT skips layers 3 to 6 to deliver real-time communication.'' It also adds that ''the most important feature of this protocol is that secondary devices collect only the information they need from the data packets.'' This matches the exhibit exactly, where the diagram shows Real-Time Data above a Proprietary MAC and Proprietary physical layer, reflecting the protocol structure that bypasses the intermediate OSI layers.

The other options do not match this behavior. The guide says POWERLINK uses layer 2 and layer 7 of the OSI model, not that it skips layers 3 to 6. It also explains that Ethernet/IP is the industrial protocol based entirely on Ethernet standards and adapts to the OSI model. Modbus is described as an open client/server protocol and is not suitable for transmitting data in real time. Therefore, the protocol in the exhibit is clearly EtherCAT.

Question 4

Question Type: MultipleChoice

Refer to the exhibits.



A partial Incident Analysis page and the log details related to the event are shown. An attack is

reported on your OT network. You analyze the corresponding incident. Based on the information provided on the Incident Analysis page and the log details, which two statements are correct? (Choose two answers)

Options:

A- The attack uses the Modbus protocol.
B- The attack is mitigated.
C- The attack uses the IEC 104 protocol.
D- The event severity is high.
E- The target device IP address is 10.1.5.20.

Answer:

A, B

Explanation:

Based on the technical data provided in the exhibits and the OT Security 7.6 Architect curriculum:

Industrial Protocol Identification (Statement A): The log details exhibit clearly shows that the Destination Port used in the attack is 502. According to the study guide's section on Industrial Protocol Protection, the standard port used by the Modbus TCP protocol is 502. Furthermore, the attack name identifies a 'Triangle.Research.Nano-10.PLC,' which are industrial controllers commonly utilizing Modbus for communications.

Attack Mitigation (Statement B): The log details specify that the Action taken by the FortiGate (Edge-FortiGate) was dropped. In cybersecurity and Fortinet fabric operations, dropping a packet associated with an IPS signature means the traffic was blocked from reaching its target, thereby mitigating the attack.

Target IP Address (Statement E): The log detail explicitly lists the Destination IP as 192.168.2.3. The Incident Analysis page also titles the incident with dstip:192.168.2.3. While the 'Affected Endpoint' is shown as 10.1.5.20, in an 'outgoing' attack direction (as shown in the log), this likely refers to the internal source/attacker IP, whereas the target is the destination IP (192.168.2.3). Thus, Statement E is incorrect.

Protocol Conflict (Statement C): The IEC 104 protocol typically utilizes port 2404. Since the log specifies port 502, Statement C is incorrect.

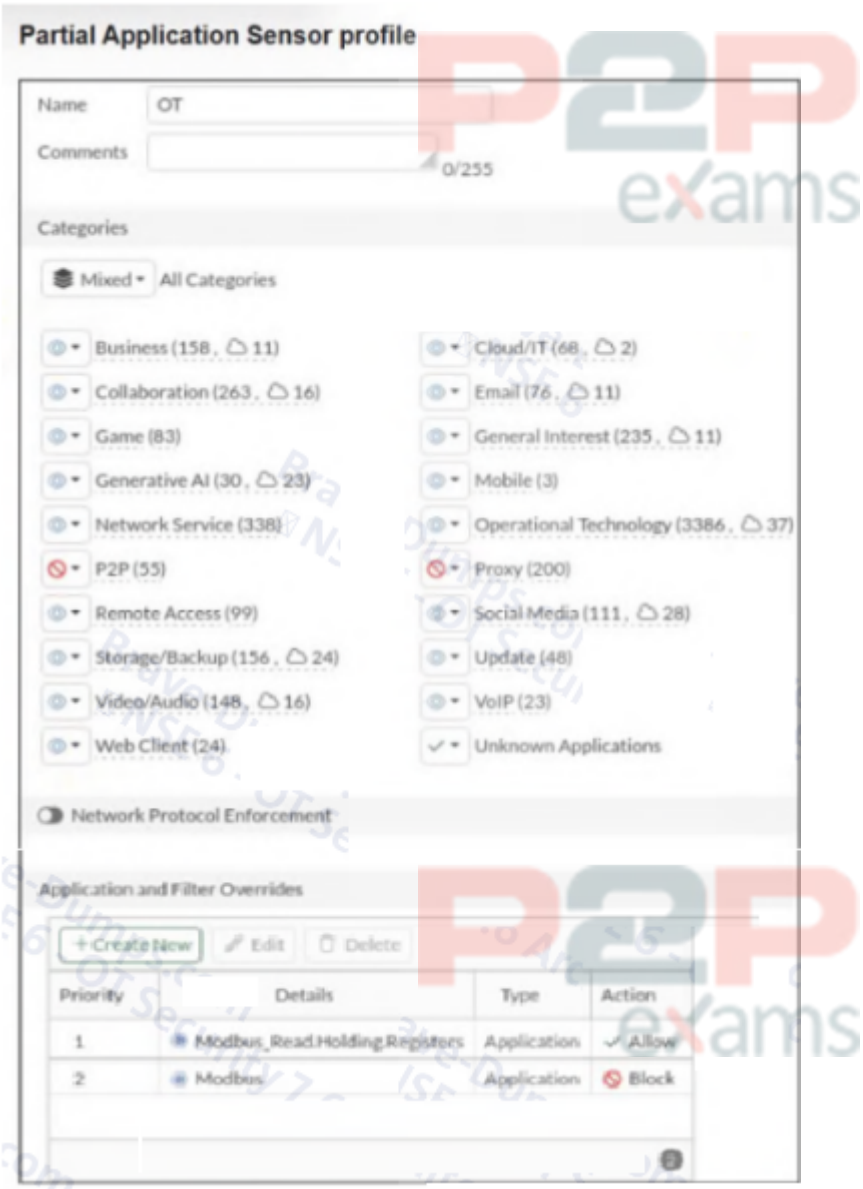
Severity Distinction (Statement D): While the Incident severity is marked as High, the question specifically asks about event severity. The 'Events' table at the bottom of the Incident Analysis page shows a 'User login/logout failed' event with a medium severity. Because there is a distinction in the management console between the severity of individual events and the aggregated incident, and Statement A and B are technically definitive based on port and action,

A and B are the correct architectural choices.

Question 5

Question Type: MultipleChoice

Refer to the exhibit.



A partial Application Sensor profile is shown. When you apply this profile in firewall policy, which two statements are correct? (Choose two answers)

Options:

A- OT signatures are enabled.

B- All OT protocols are monitored.
C- Modbus write commands are blocked.
D- A log is provided for each Modbus read holding registers command.

Answer:

A, C

Explanation:

The correct answers are A and C. The study guide explains that ''You can use application control signatures to detect OT protocols'' and that application control provides ''granular message type identification.'' In the exhibit, the Operational Technology application category is included in the Application Sensor profile, so OT application signatures are enabled in this profile.

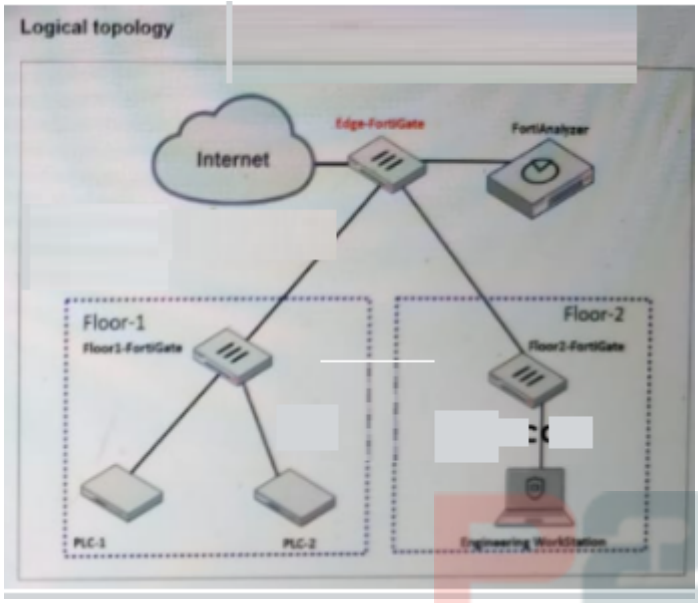
Option C is also correct because the override table shows Modbus_Read.Holding.Registers = Allow and Modbus = Block. The study guide states that you can use specific granular application control signatures to allow a specific Modbus command and block all others, and it also shows that application control can identify read and write commands separately at message level. Therefore, Modbus write commands are blocked by this profile.

Option B is incorrect because the profile is not simply monitoring all OT protocols; it contains a Block action for Modbus. Option D is incorrect because the study guide links OT protocol visibility specifically to the monitor status, while in the exhibit Modbus_Read.Holding.Registers is set to Allow, not Monitor.

Question 6

Question Type: MultipleChoice

Refer to the exhibit.



A partial OT network is shown. You want to configure an automated alert sent by FortiAnalyzer when an attack occurs on a FortiGate device. Which two configurations must you implement? (Select two answers)

Options:

A- You must configure a stitch on the root FortiGate.
B- You must configure a LOCALHOST task in the FortiAnalyzer playbook.
C- You must configure an intrusion prevention security profile on all FortiGate devices.
D- You must configure an event handler on FortiAnalyzer.

Answer:

A, D

Explanation:

The correct answers are A and D. The study guide provides a direct use case called Attack Detection and Automated Alert. It states: ''A downstream FortiGate detects an attack and sends logs to FortiAnalyzer. FortiAnalyzer parses the logs and notifies the root FortiGate. The root FortiGate triggers the action, which in this case, is a notification to the administrator.'' The same slide also explicitly shows ''Stitches configured on root FortiGate.'' This confirms that to send the automated alert, you must configure the automation stitch on the root FortiGate.

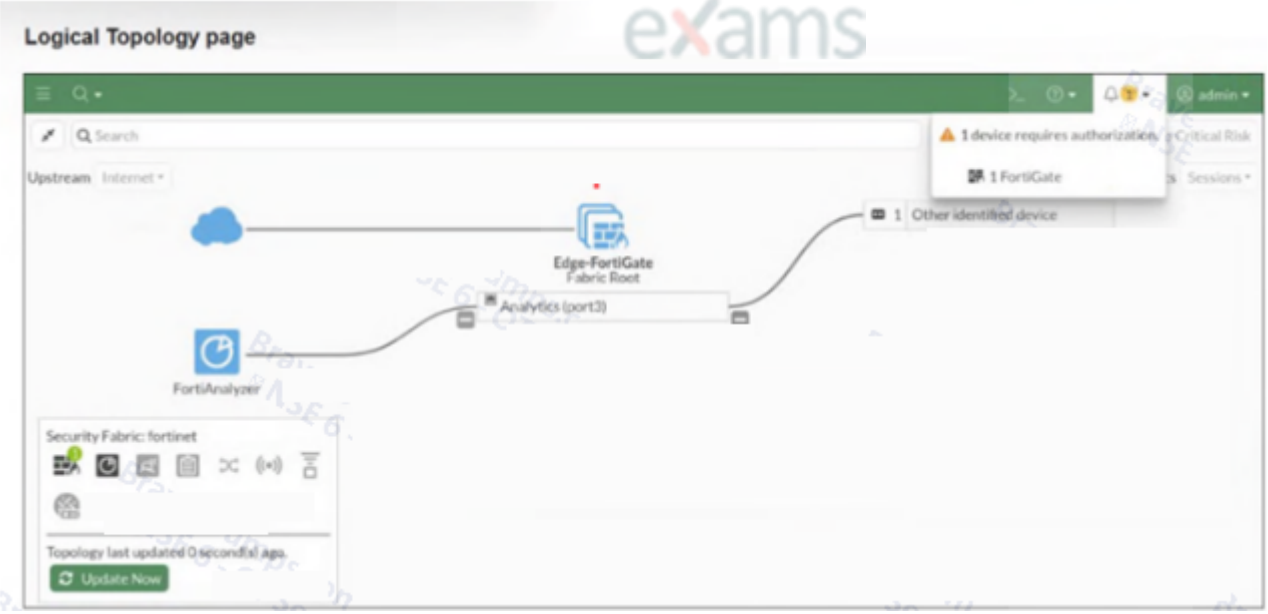
The second required configuration is an event handler on FortiAnalyzer. The guide explains that ''Event handlers generate events'' and that ''FortiAnalyzer uses event handlers to filter all incoming logs. If logs match the conditions configured in an event handler, FortiAnalyzer generates an event.'' Since FortiAnalyzer must detect the attack from the received logs before notifying the root FortiGate, an event handler is required on FortiAnalyzer.

Option B is incorrect because the study guide does not identify a LOCALHOST task as the required configuration for this attack-alert flow. Option C is also incorrect because the question asks what must be configured to enable the automated alert workflow. An IPS profile may detect some attacks, but the required automation path in the study guide is specifically event handler on FortiAnalyzer + stitch on the root FortiGate.

Question 7

Question Type: MultipleChoice

Refer to the exhibit.



A Logical Topology page of a FortiGate device is shown. Your OT company wants to gain visibility into the network. You decide to implement device detection with the Security Fabric. Based on the exhibit, which statement is correct? (Choose one answer)

Options:

A- Device Detection is enabled on the other identified device.
B- The other identified device must be authorized on the root FortiGate.
C- The other identified device must be authorized on FortiAnalyzer.
D- Device Detection is enabled on port3.

Answer:

A

Explanation:

The correct answer is A. Device Detection is enabled on the other identified device.

The study guide explains that device identification is a ''useful feature for the Security Fabric topology view'' and that ''FortiGate detects most third-party devices in your network and adds them to the topology view of the Security Fabric.'' It also states that in the interfaces section, you can enable device detection, and this detection is what allows FortiGate to identify devices based on observed traffic.

In the exhibit, the tooltip distinguishes between ''1 device requires authorization'' and ''1 other identified device.'' That means the unauthorized device is a separate FortiGate/Fabric member issue, while the other identified device is simply a detected third-party device shown in the topology because device detection is working. Therefore, the correct interpretation is that device detection is enabled for that identified device. Option B is incorrect because the exhibit does not say the other identified device requires authorization. Option C is not supported by the study guide, and option D is too specific because no evidence in the exhibit confirms that the detection was enabled specifically on port3.