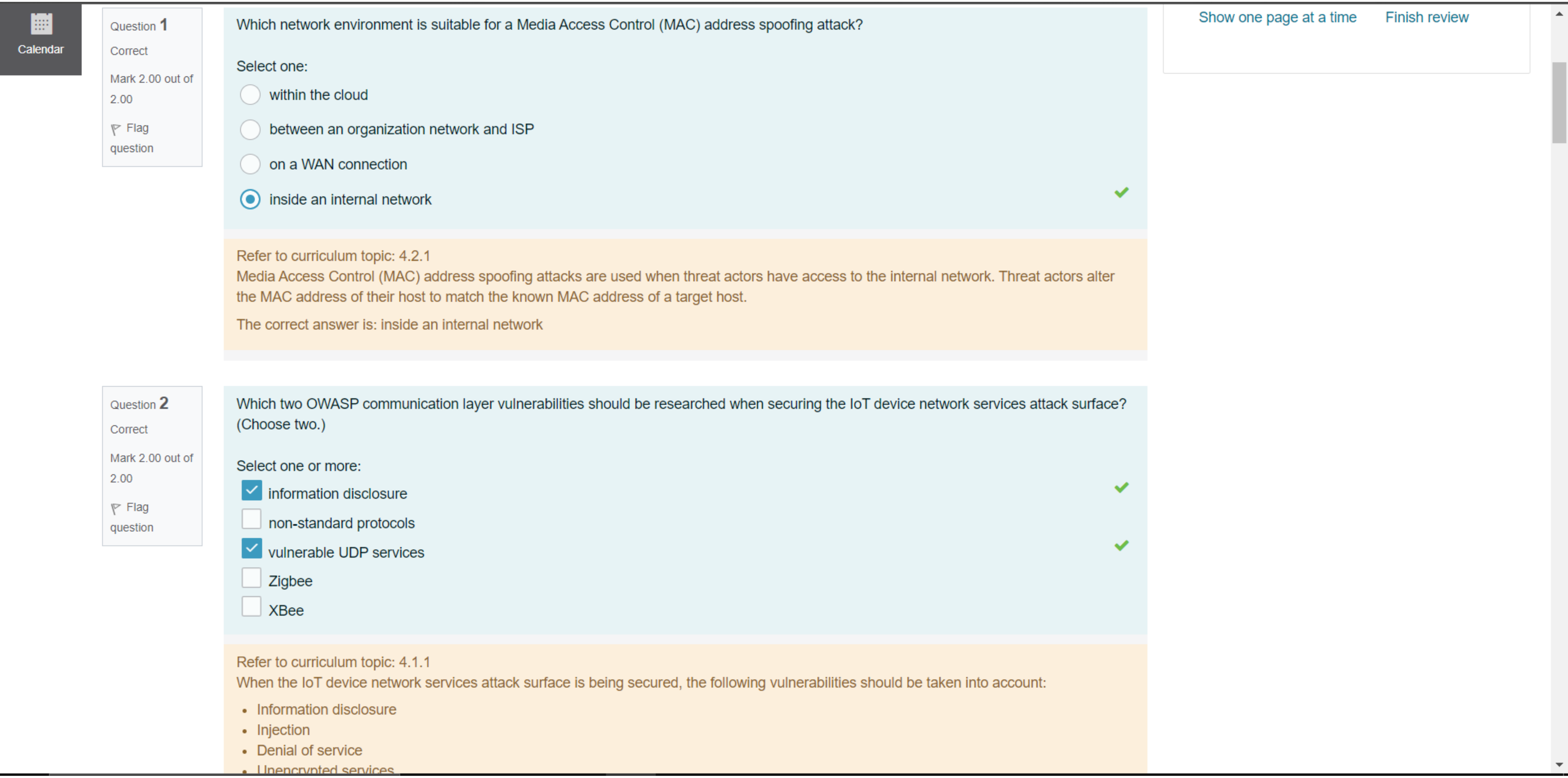


Question **1**

Correct

Mark 2.00 out of 2.00

Flag question

Which network environment is suitable for a Media Access Control (MAC) address spoofing attack?

Select one:

○ within the cloud

○ between an organization network and ISP

○ on a WAN connection

● inside an internal network ✓

Refer to curriculum topic: 4.2.1
Media Access Control (MAC) address spoofing attacks are used when threat actors have access to the internal network. Threat actors alter the MAC address of their host to match the known MAC address of a target host.

The correct answer is: inside an internal network

Question **2**

Correct

Mark 2.00 out of 2.00

Flag question

Which two OWASP communication layer vulnerabilities should be researched when securing the IoT device network services attack surface? (Choose two.)

Select one or more:

☑ information disclosure ✓

□ non-standard protocols

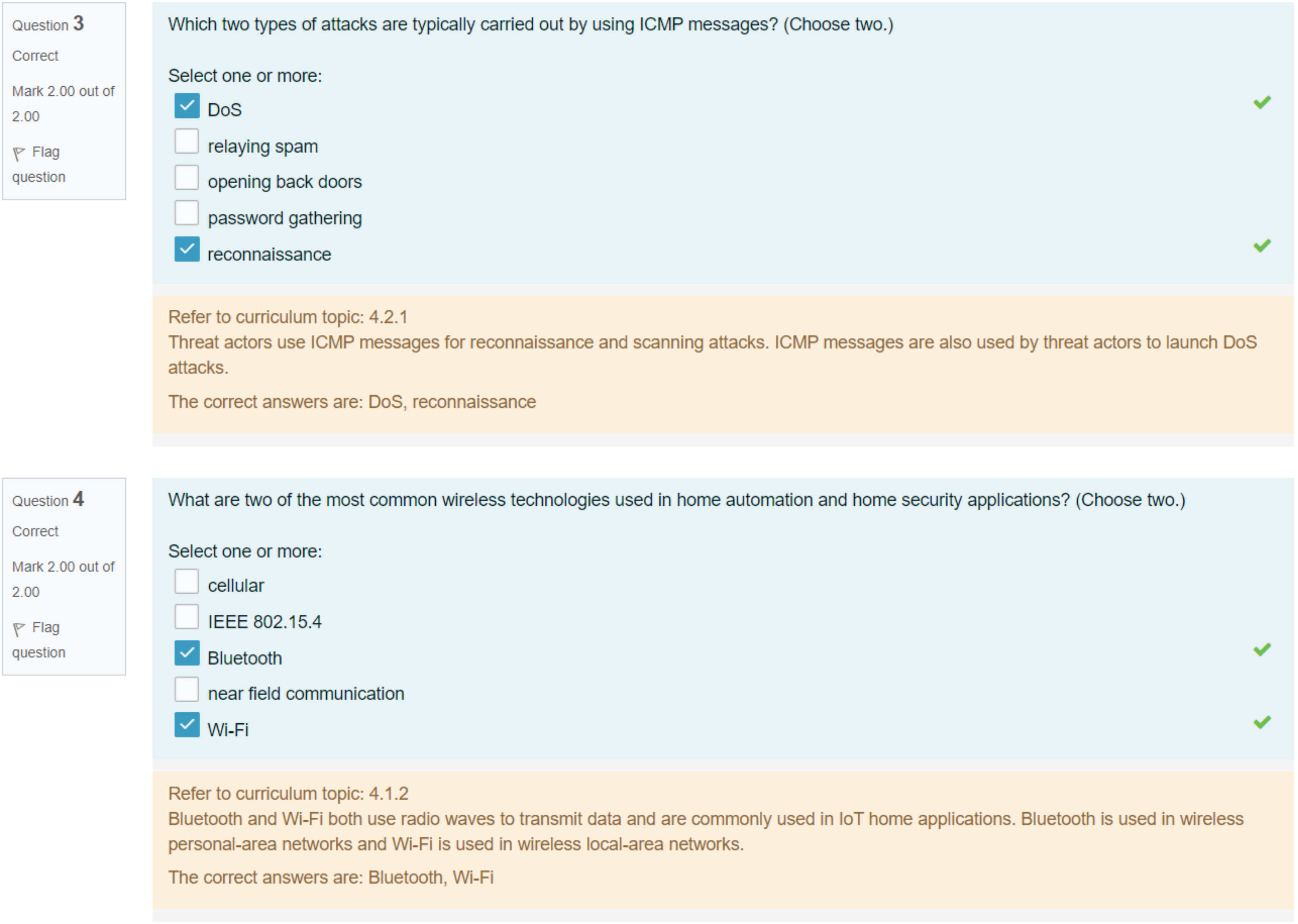
☑ vulnerable UDP services ✓

□ Zigbee

□ XBee

Refer to curriculum topic: 4.1.1
When the IoT device network services attack surface is being secured, the following vulnerabilities should be taken into account:

- Information disclosure
- Injection
- Denial of service
- Unencrypted services



Question 3

Correct

Mark 2.00 out of 2.00

Flag question

Which two types of attacks are typically carried out by using ICMP messages? (Choose two.)

Select one or more:

☑ DoS ✓

□ relaying spam

□ opening back doors

□ password gathering

☑ reconnaissance ✓

Refer to curriculum topic: 4.2.1
Threat actors use ICMP messages for reconnaissance and scanning attacks. ICMP messages are also used by threat actors to launch DoS attacks.

The correct answers are: DoS, reconnaissance

Question 4

Correct

Mark 2.00 out of 2.00

Flag question

What are two of the most common wireless technologies used in home automation and home security applications? (Choose two.)

Select one or more:

□ cellular

□ IEEE 802.15.4

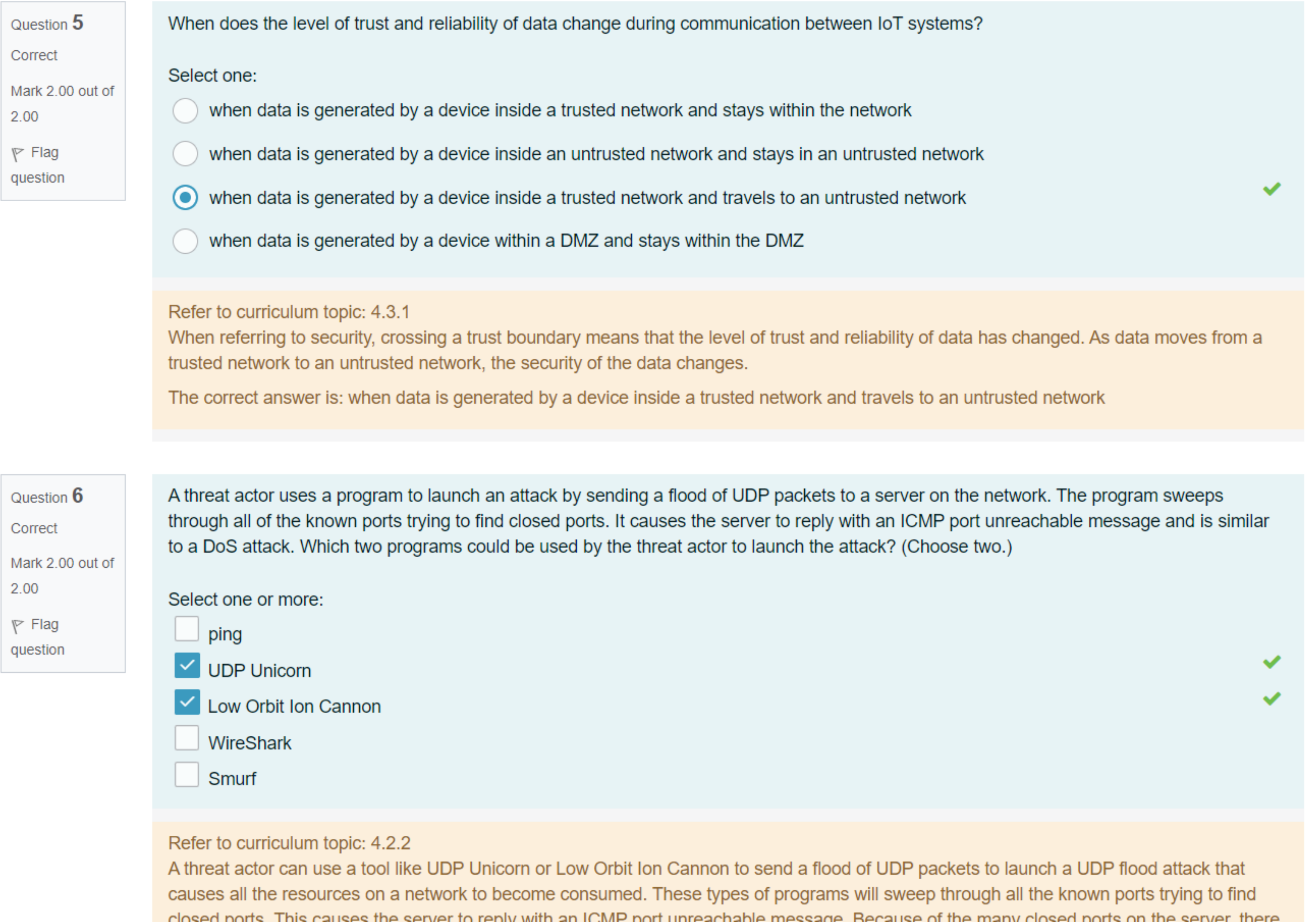
☑ Bluetooth ✓

□ near field communication

☑ Wi-Fi ✓

Refer to curriculum topic: 4.1.2
Bluetooth and Wi-Fi both use radio waves to transmit data and are commonly used in IoT home applications. Bluetooth is used in wireless personal-area networks and Wi-Fi is used in wireless local-area networks.

The correct answers are: Bluetooth, Wi-Fi



Question 5

Correct

Mark 2.00 out of 2.00

Flag question

When does the level of trust and reliability of data change during communication between IoT systems?

Select one:

○ when data is generated by a device inside a trusted network and stays within the network

○ when data is generated by a device inside an untrusted network and stays in an untrusted network

● when data is generated by a device inside a trusted network and travels to an untrusted network ✓

○ when data is generated by a device within a DMZ and stays within the DMZ

Refer to curriculum topic: 4.3.1
When referring to security, crossing a trust boundary means that the level of trust and reliability of data has changed. As data moves from a trusted network to an untrusted network, the security of the data changes.

The correct answer is: when data is generated by a device inside a trusted network and travels to an untrusted network

Question 6

Correct

Mark 2.00 out of 2.00

Flag question

A threat actor uses a program to launch an attack by sending a flood of UDP packets to a server on the network. The program sweeps through all of the known ports trying to find closed ports. It causes the server to reply with an ICMP port unreachable message and is similar to a DoS attack. Which two programs could be used by the threat actor to launch the attack? (Choose two.)

Select one or more:

□ ping

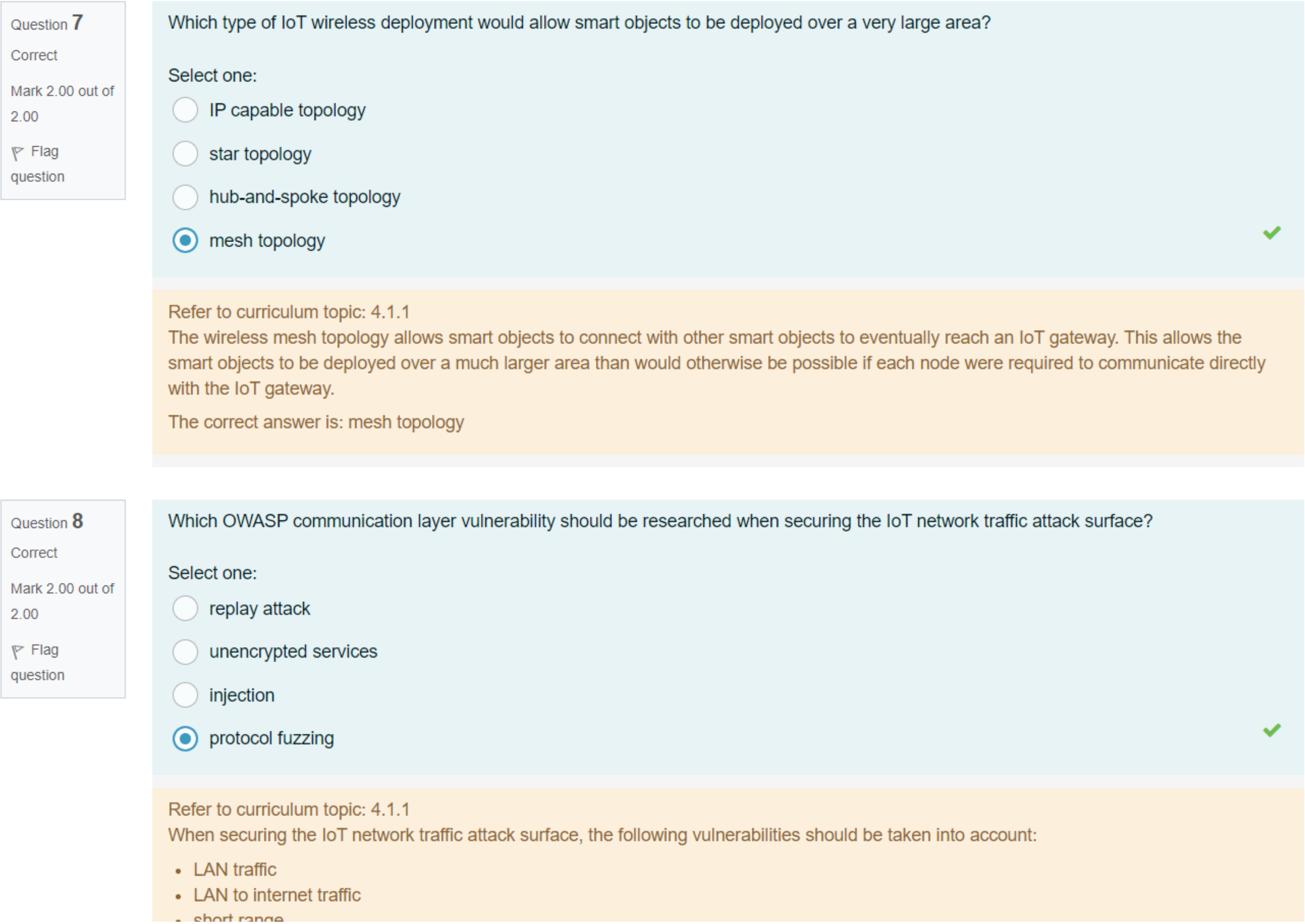
☑ UDP Unicorn ✓

☑ Low Orbit Ion Cannon ✓

□ WireShark

□ Smurf

Refer to curriculum topic: 4.2.2
A threat actor can use a tool like UDP Unicorn or Low Orbit Ion Cannon to send a flood of UDP packets to launch a UDP flood attack that causes all the resources on a network to become consumed. These types of programs will sweep through all the known ports trying to find closed ports. This causes the server to reply with an ICMP port unreachable message. Because of the many closed ports on the server, there



Question 7
Correct
Mark 2.00 out of 2.00
Flag question

Which type of IoT wireless deployment would allow smart objects to be deployed over a very large area?

Select one:

○ IP capable topology

○ star topology

○ hub-and-spoke topology

● mesh topology ✓

Refer to curriculum topic: 4.1.1
The wireless mesh topology allows smart objects to connect with other smart objects to eventually reach an IoT gateway. This allows the smart objects to be deployed over a much larger area than would otherwise be possible if each node were required to communicate directly with the IoT gateway.

The correct answer is: mesh topology

Question 8
Correct
Mark 2.00 out of 2.00
Flag question

Which OWASP communication layer vulnerability should be researched when securing the IoT network traffic attack surface?

Select one:

○ replay attack

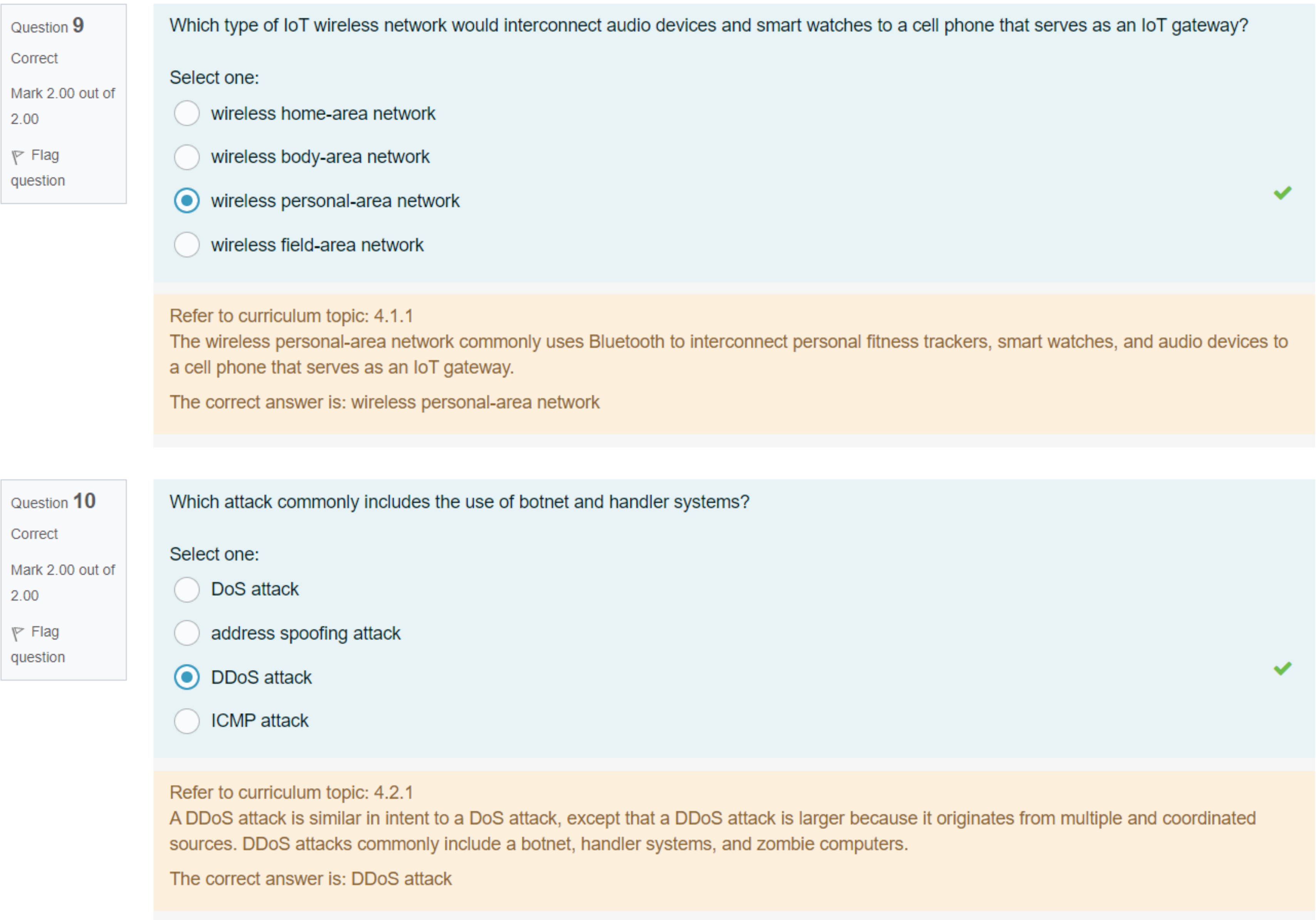
○ unencrypted services

○ injection

● protocol fuzzing ✓

Refer to curriculum topic: 4.1.1
When securing the IoT network traffic attack surface, the following vulnerabilities should be taken into account:

- LAN traffic
- LAN to internet traffic
- short range



Question 9

Correct

Mark 2.00 out of 2.00

Flag question

Which type of IoT wireless network would interconnect audio devices and smart watches to a cell phone that serves as an IoT gateway?

Select one:

○ wireless home-area network

○ wireless body-area network

● wireless personal-area network ✓

○ wireless field-area network

Refer to curriculum topic: 4.1.1
The wireless personal-area network commonly uses Bluetooth to interconnect personal fitness trackers, smart watches, and audio devices to a cell phone that serves as an IoT gateway.

The correct answer is: wireless personal-area network

Question 10

Correct

Mark 2.00 out of 2.00

Flag question

Which attack commonly includes the use of botnet and handler systems?

Select one:

○ DoS attack

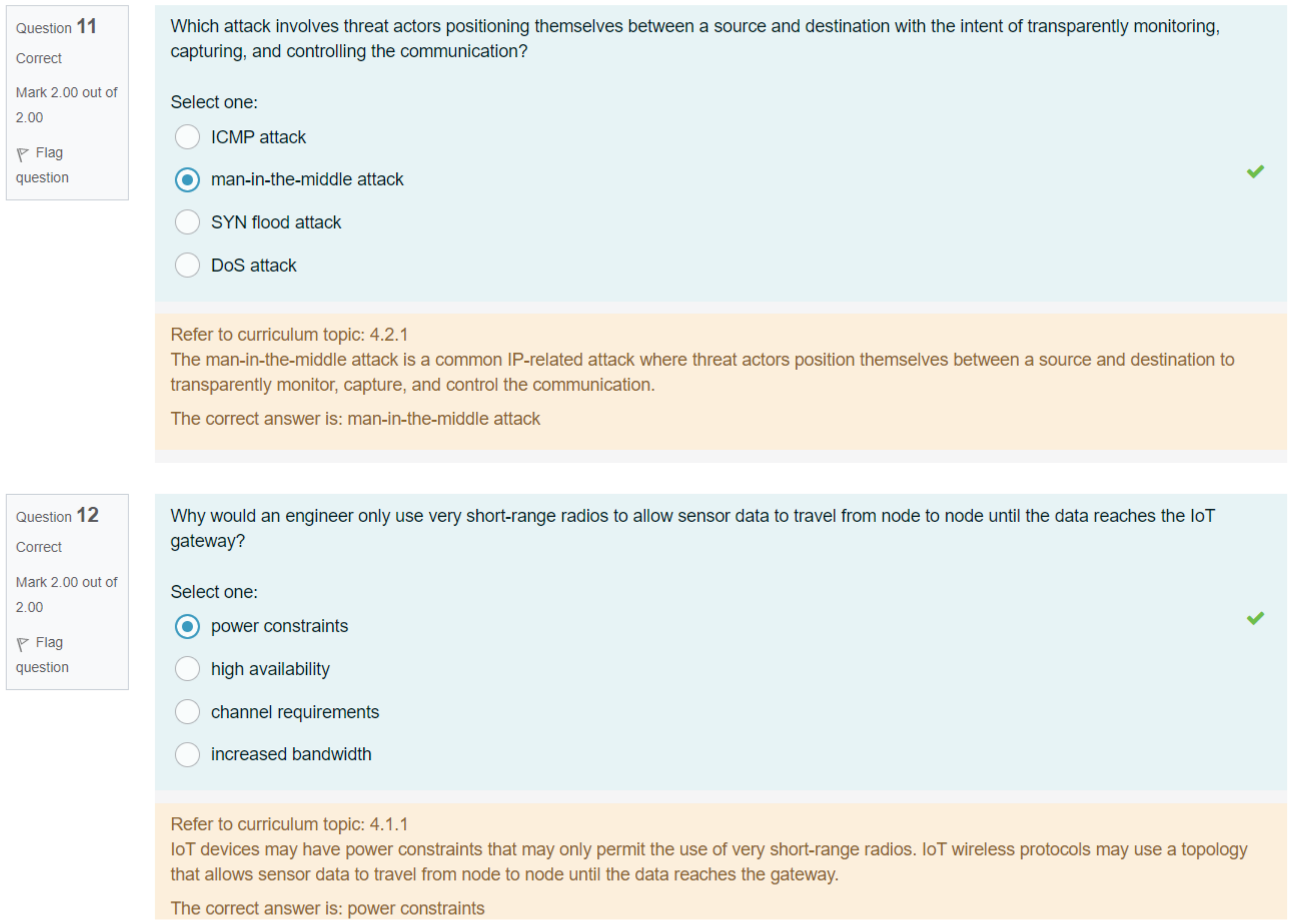
○ address spoofing attack

● DDoS attack ✓

○ ICMP attack

Refer to curriculum topic: 4.2.1
A DDoS attack is similar in intent to a DoS attack, except that a DDoS attack is larger because it originates from multiple and coordinated sources. DDoS attacks commonly include a botnet, handler systems, and zombie computers.

The correct answer is: DDoS attack



Question 11

Correct

Mark 2.00 out of 2.00

Flag question

Which attack involves threat actors positioning themselves between a source and destination with the intent of transparently monitoring, capturing, and controlling the communication?

Select one:

○ ICMP attack

● man-in-the-middle attack ✓

○ SYN flood attack

○ DoS attack

Refer to curriculum topic: 4.2.1
The man-in-the-middle attack is a common IP-related attack where threat actors position themselves between a source and destination to transparently monitor, capture, and control the communication.

The correct answer is: man-in-the-middle attack

Question 12

Correct

Mark 2.00 out of 2.00

Flag question

Why would an engineer only use very short-range radios to allow sensor data to travel from node to node until the data reaches the IoT gateway?

Select one:

● power constraints ✓

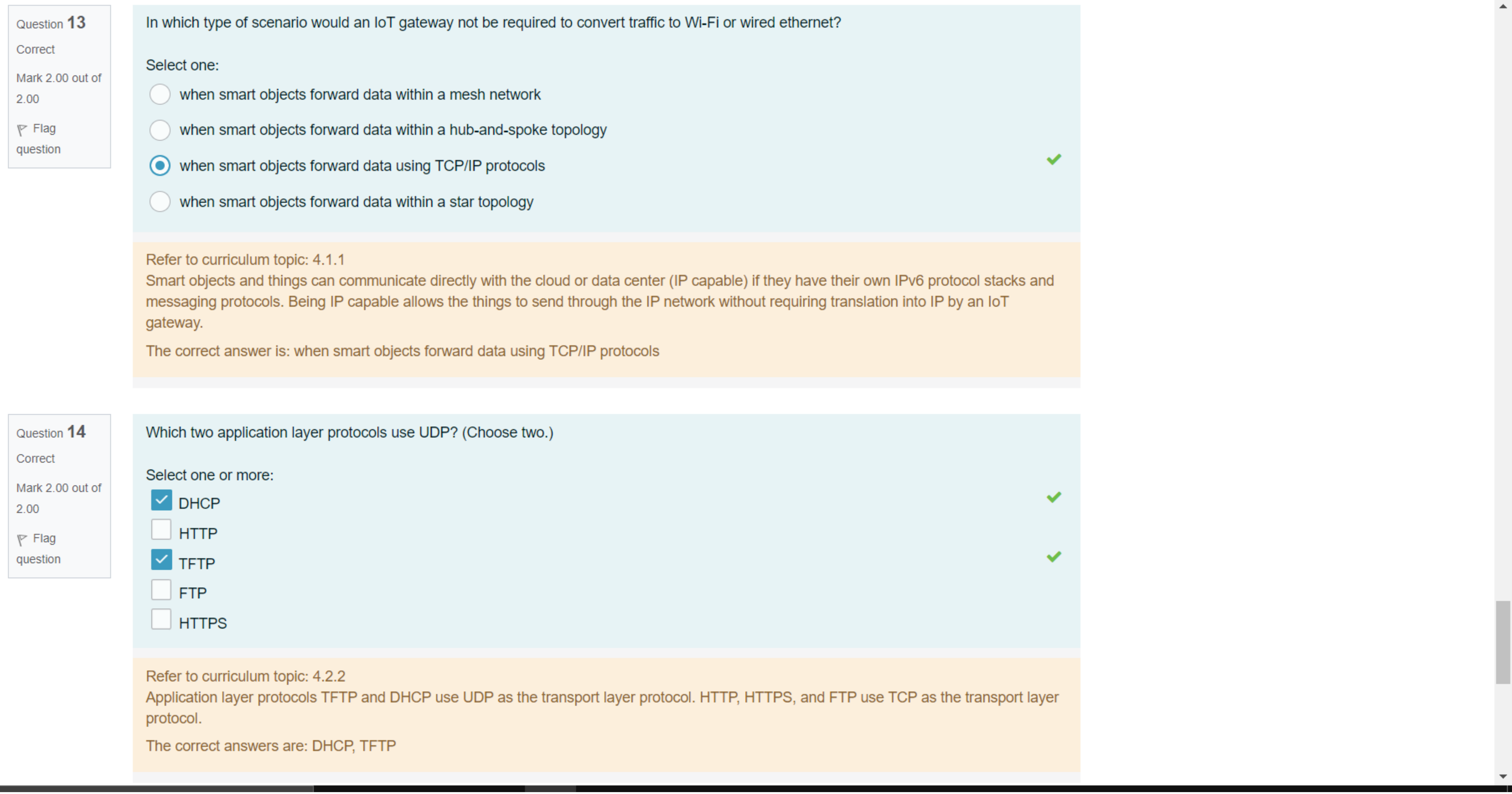
○ high availability

○ channel requirements

○ increased bandwidth

Refer to curriculum topic: 4.1.1
IoT devices may have power constraints that may only permit the use of very short-range radios. IoT wireless protocols may use a topology that allows sensor data to travel from node to node until the data reaches the gateway.

The correct answer is: power constraints



Question **13**

Correct

Mark 2.00 out of 2.00

Flag question

In which type of scenario would an IoT gateway not be required to convert traffic to Wi-Fi or wired ethernet?

Select one:

○ when smart objects forward data within a mesh network

○ when smart objects forward data within a hub-and-spoke topology

● when smart objects forward data using TCP/IP protocols ✓

○ when smart objects forward data within a star topology

Refer to curriculum topic: 4.1.1
Smart objects and things can communicate directly with the cloud or data center (IP capable) if they have their own IPv6 protocol stacks and messaging protocols. Being IP capable allows the things to send through the IP network without requiring translation into IP by an IoT gateway.

The correct answer is: when smart objects forward data using TCP/IP protocols

Question **14**

Correct

Mark 2.00 out of 2.00

Flag question

Which two application layer protocols use UDP? (Choose two.)

Select one or more:

☑ DHCP ✓

□ HTTP

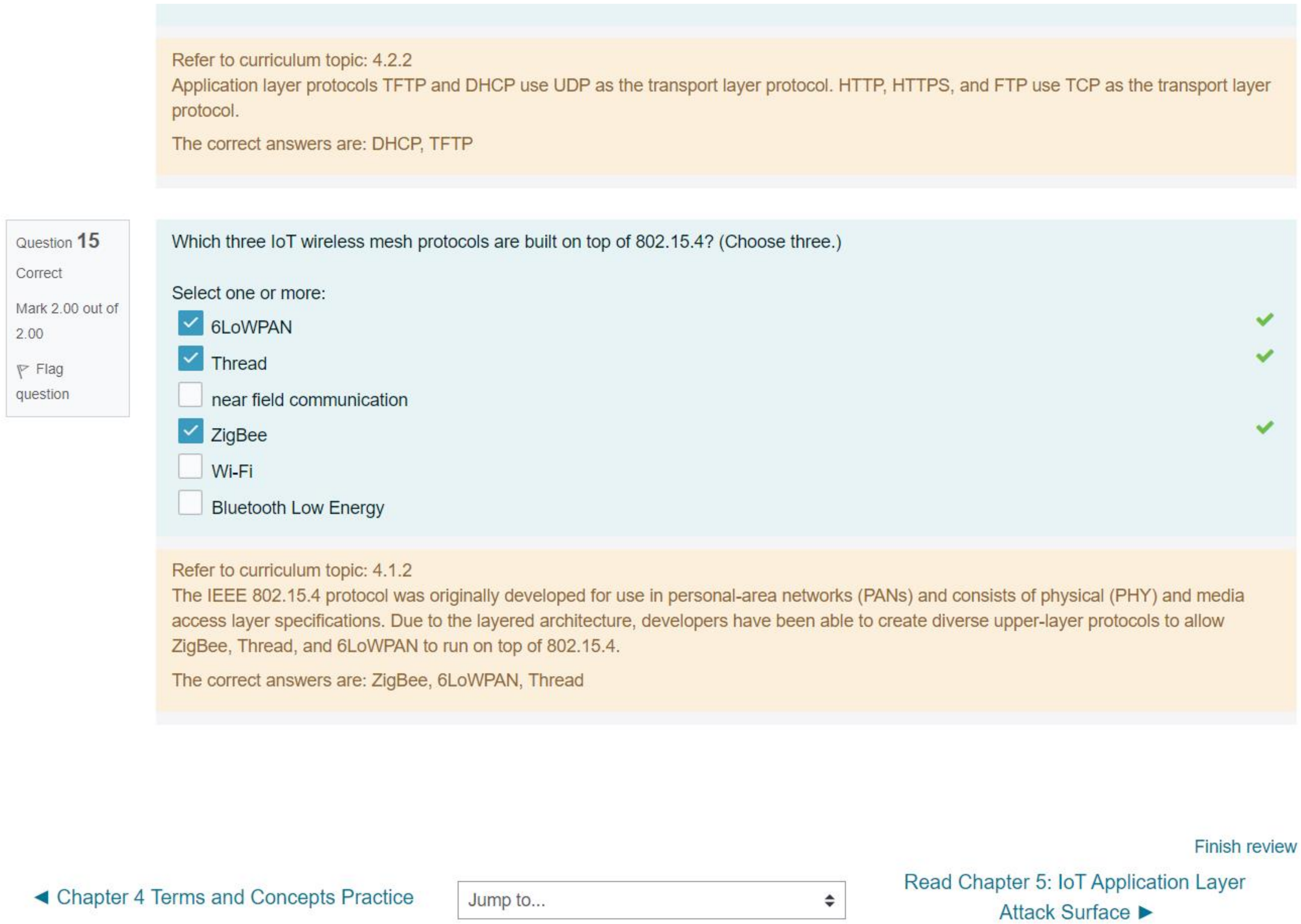
☑ TFTP ✓

□ FTP

□ HTTPS

Refer to curriculum topic: 4.2.2
Application layer protocols TFTP and DHCP use UDP as the transport layer protocol. HTTP, HTTPS, and FTP use TCP as the transport layer protocol.

The correct answers are: DHCP, TFTP



Refer to curriculum topic: 4.2.2
Application layer protocols TFTP and DHCP use UDP as the transport layer protocol. HTTP, HTTPS, and FTP use TCP as the transport layer protocol.

The correct answers are: DHCP, TFTP

Question **15**

Correct

Mark 2.00 out of 2.00

Flag question

Which three IoT wireless mesh protocols are built on top of 802.15.4? (Choose three.)

Select one or more:

- ☑ 6LoWPAN ✓
- ☑ Thread ✓
- ☐ near field communication
- ☑ ZigBee ✓
- ☐ Wi-Fi
- ☐ Bluetooth Low Energy

Refer to curriculum topic: 4.1.2
The IEEE 802.15.4 protocol was originally developed for use in personal-area networks (PANs) and consists of physical (PHY) and media access layer specifications. Due to the layered architecture, developers have been able to create diverse upper-layer protocols to allow ZigBee, Thread, and 6LoWPAN to run on top of 802.15.4.

The correct answers are: ZigBee, 6LoWPAN, Thread

Finish review

◄ Chapter 4 Terms and Concepts Practice

Jump to...

Read Chapter 5: IoT Application Layer Attack Surface ►