Exam Report: 10.4.9 Practice Questions

Date: 11/5/2019 5:18:20 pm
Time Spent: 15:01

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 36%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

What is the risk associated with smart technology used in networked devices such as smart refrigerators, environmental controls, or industrial equipment?

- They are not compatible with routing protocols, which causes a burden on network bandwidth.
- They are not physically secure, so they can be reconfigured by anyone who has access to them.
- They are vulnerable to exploits due to weaker security.
- They use redundant paths for fault tolerance that can cause message loops to develop on the network.

Explanation

Devices with embedded smart technology are not designed to be customized or directly configured by system administrators. For example, you cannot install anti-malware software on a smart TV. Because of this weaker security, smart technology devices are vulnerable to exploits and attacks.

References

LabSim for Network Pro, Section 10.4.
[netpro18v5_all_questions_en.exm *NP15_SCADA_SYSTEMS_04]

Question 2: Correct

Which protocol is well known for its use in the the home security and home automation industry, uses a mesh topology, makes devices act as repeaters, and has a low data transfer rate?

- 802.11 AC
- Z-Wave
- Ant+
- NFC

Explanation

The Z-Wave protocol is mostly used in the home security and automation market and uses only a mesh topology. Each device that is added acts as a repeater and increase the strength of the network. Z-Wave has a low data transfer rate.

Ant+ is can be used in a mesh topology, but is generally used to monitor sensor data. NFC is commonly used for mobile pay solutions and connections like blue tooth, but has to be several

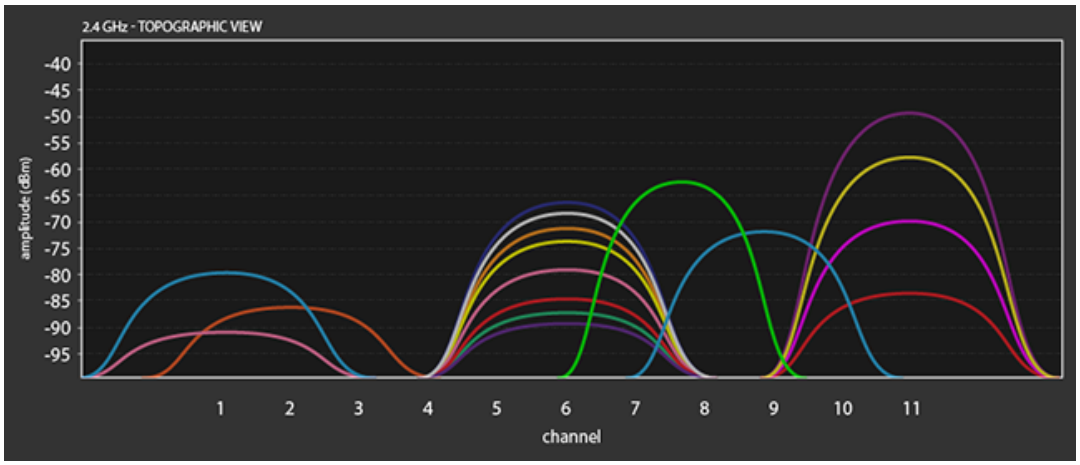
inches within another device to connect. 802.11 AC is a wireless networking standard that offers high-speed data transfer.

References

LabSim for Network Pro, Section 10.4.
[netpro18v5_all_questions_en.exm MCS11]

Question 3: Incorrect

This question includes an image to help you answer the question. Close



To optimize your network, you want to configure your wireless AP to use a channel that meets the following criteria:

- Non-overlapping
- Low utilization
- Low interference

You performed a spectrum analysis to identify 2.4 GHz wireless channel utilization, as shown in the exhibit. (To read the spectrum analysis, imagine a line coming down from the center of the highest point of each wave. For example, the four waves whose crests are over channel 11 belong to channel 11.)

Based on the results, which channel should you configure your wireless AP to use?

- Channel 3
- Channel 11
- Channel 1
- Channel 6
- ~~Channel 8~~

Explanation

You should use channel 1. Based on the results, the only channel that meets all the criteria is channel 1.

Channels 3 and 8 overlap. Channel 6 is heavily utilized and would cause issues. Channel 11 isn't used as much as channel 6, but the signal interference is much stronger.

References

LabSim for Network Pro, Section 10.4.
[netpro18v5_all_questions_en.exm *NP15_WIRELESS_NETWORK_DESIGN_01]

Question 4: Correct

Your wireless network consists of multiple 802.11n access points that are configured as follows:

- SSID (hidden): CorpNet
- Security: WPA2-PSK using AES
- Frequency: 5.7 GHz
- Bandwidth per channel: 20 MHz

This network is required to support an ever-increasing number of devices. To ensure there is sufficient capacity, you want to maximize the available network bandwidth.

What should you do?

- Upgrade to 802.11a access points.
- Switch to TKIP encryption.
- Double the bandwidth assigned per channel to 40 MHz.
- Implement antenna diversity.

Explanation

802.11n access points provide an option to allocate double the bandwidth per channel (increasing it to 40 MHz), which results in double the data rate.

The 802.11a standard only supports data rates up to 54 Mbps, which is much slower than 802.11n. Antenna diversity implements multiple antennas to combat multipath interference and improve the reliability of a wireless link; however, it does not increase throughput. TKIP is considered less secure than AES and does not increase the throughput of a wireless network.

References

LabSim for Network Pro, Section 10.4.
[netpro18v5_all_questions_en.exm MCS3]

Question 5: Incorrect

You are designing an update to your client's wireless network. The existing wireless network uses 802.11g equipment, which your client complains runs too slowly. She wants to upgrade the network to run at 150 Mbps or faster.

Due to budget constraints, your client wants to upgrade only the wireless access points in the network this year. Next year, she will upgrade the wireless NICs in the workstations. She has also indicated that the system must continue to function during the transition period.

Which 802.11 standard will work best in this situation?

- 802.11a
- ~~802.11b~~
- 802.11d
- 802.11n

Explanation

802.11n is the best choice for this client. 802.11a operates at a maximum speed of 54 Mbps. 802.11a isn't compatible with 802.11g network boards. 802.11b runs at only 11 Mbps.

802.11n access points are backwards compatible with 802.11g equipment and run at speeds of up to 600 Mbps. Using this type of access point will allow the wireless network to continue to function during the transition.

References

LabSim for Network Pro, Section 10.4.

[netpro18v5_all_questions_en.exm RT NP15_5.3-3]

Question 6: Correct

You are designing a wireless network for a client. Your client needs the network to support a data rate of at least 150 Mbps. In addition, the client already has a wireless telephone system installed that operates 2.4 GHz.

Which 802.11 standard will work best in this situation?

- 802.11a
- 802.11g
- 802.11n
- 802.11b

Explanation

802.11n is the best choice for this client.

802.11b and 802.11g both operate in the 2.4 GHz to 2.4835 GHz range, which will cause interference with the client's wireless phone system. 802.11a operates in the 5.725 GHz to 5.850 GHz frequency range. While this won't interfere with the phone system, its maximum speed is limited to 54 Mbps.

References

LabSim for Network Pro, Section 10.4.
[netpro18v5_all_questions_en.exm RT NP15_5.3-1]

Question 7: Incorrect

You are designing a wireless network for a client. Your client needs the network to support a data rate of at least 54 Mbps. In addition, the client already has a wireless telephone system installed that operates at 2.4 GHz.

Which 802.11 standards will work best in this situation? (Select two.)

- [ ] 802.11b
- [x] ~~802.11g~~
- [ ] 802.11a
- [ ] 802.11n
- [ ] 802.11d

Explanation

802.11a or 802.11n are the best choices for this client.

While both 802.11a and 802.11g each operate at 54 Mbps, 802.11g operates in the 2.4 GHz to 2.4835 GHz range—which will cause interference with the client's wireless phone system. 802.11a and 802.11n, on the other hand, operate in the 5.725 GHz to 5.850 GHz frequency range. This won't interfere with the phone system. 802.11n can operate at speeds up to 600 Mbps.

References

LabSim for Network Pro, Section 10.4.
[netpro18v5_all_questions_en.exm RT NP15_5.3-2]

Question 8: Incorrect

You have been hired to design a wireless network for a SOHO environment. You are currently in

the process of gathering network requirements from management.
Which of the following questions should you ask? (Select three.)

- [x] Is the size of the business expected to grow in the future?
- [x] How many devices will need to be supported?
- [x] ~~Are there microwaves or cordless phones that can cause interference?~~
- [ ] What type of data will be transmitted on the network?
- [ ] Where can network hardware be mounted in the building?

Explanation

The first thing you do when designing a wireless network is gather network requirements. Meet with all stakeholders and decision-makers to discuss the implementations and gather detailed information. For example, you should:

- Identify the intended use of the wireless network.
- Identify the location of wireless service areas.
- Anticipate the number of wireless devices that need to be supported in each area.
- Discuss future network needs so that you can plan for expansion.
- Discuss data encryption and network security requirements.

Mounting points or sources of interference should be considered in the network design phase, after all requirements have been gathered.

References

LabSim for Network Pro, Section 10.4.
[netpro18v5_all_questions_en.exm *NP15_WIRELESS_NETWORK_DESIGN]

Question 9: Incorrect

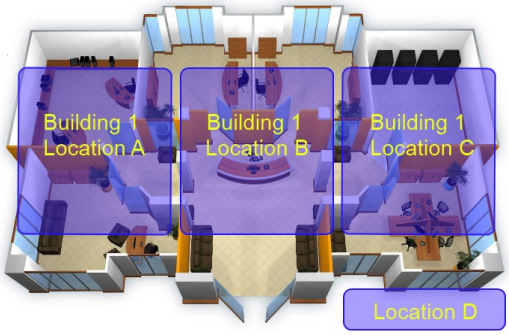
You are building a wireless network within and between two buildings. The buildings are separated by more than 3000 feet. The wireless network should meet the following requirements:

- Wireless data within Building 1 should be protected with the highest degree of security.
- Wireless data within Building 2 should be accessible and permitted by any wireless client.
- Wireless signals between Buildings 1 and 2 should be protected with the highest degree of security.
- Wireless signals within Buildings 1 and 2 should cover the whole structure, but not extend to the outside.

For each location on the image below, you need to select the following:

- Antenna option
- Security option

Drag the items from the list on the left to the location identifier on the right. Items may be used more than once. Not all items will be used.



Building 1 - Location A

✔ Right-facing directional antenna	WPA2 with CCMP

Building 1 - Location B

Omni-directional antenna	WPA2 with CCMP

Building 1 - Location C

✔ Left-facing directional antenna	WPA2 with CCMP

Building 1 - Location D

Right-facing high-gain directional antenna	WPA2 with CCMP

Building 2 - Location A

Omni-directional antenna	WEP with open authentication

Building 2 - Location B

Left-facing high-gain directional antenna	WPA2 with CCMP

Explanation

To answer this question correctly, you should choose the following:

Building 1 - Location A = Right-facing directional antenna, WPA2- CCMP
Building 1 - Location B = Omni-directional antenna, WPA2- CCMP
Building 1 - Location C = Left-facing directional antenna, WPA2- CCMP
Building 1 - Location D = Right-facing parabolic antenna, WPA2- CCMP
Building 2 - Location A = Omni-directional antenna, WEP with open authentication
Building 2 - Location B = Left-facing parabolic antenna, WPA2- CCMP

Be aware of the following types of antennas:

- Directional antenna:
  - Creates a narrow, focused signal in a particular direction.
  - Focuses the signal to provide greater signal strength, thus increasing the transmission distance.
  - Provides a stronger point-to-point connection, better equipping them to handle obstacles. A *parabolic* directional antenna is highly focused, sending and receiving signals in far greater distances than achieved with a typical directional antenna.
- Omni-directional antenna:
  - Disperses the RF wave in an equal 360-degree pattern.
  - Provides access to many clients in a radius.

Be aware of the following types of security:

- Wired Equivalent Privacy (WEP) is an optional component of the 802.11 specifications, but is easily broken. When using WEP, use open authentication.
- Wi-Fi Protected Access 2 (WPA2) resolves the weaknesses inherent in WEP. WPA2 uses counter mode with the CBC-MAC protocol (CCMP), also known as AES-CCMP. Note that WPA2 does not use TKIP.

References

LabSim for Network Pro, Section 10.4.

[netpro18v5_all_questions_en.exm PERF-BASED#2]

Question 10: Incorrect

What purposes does a wireless *site* survey fulfill? (Choose two.)

- [x] ~~To document existing infrared traffic in the 5.4 GHz spectrum.~~
- [ ] To identify the recommended 100 degree separation angle for alternating access points.
- [ ] To identify the coverage area and preferred placement of access points.
- [x] To identify existing or potential sources of interference.

Explanation

Wireless site surveys provide layout and design parameters for access point coverage and placement. Site surveys can also identify rogue access points and other forms of interference that reduce security and prevent the proper operation of authorized network devices.

Radio frequency spectrum and protocol analyzers are used to conduct the surveys.

References

LabSim for Network Pro, Section 10.4.
[netpro18v5_all_questions_en.exm SP02_2-6 [117]]

Question 11: Incorrect

Match each wireless term or concept on the left with its associated description on the right. Each term may be used more than once; not all descriptions have a matching term.

Compares the level of the Wi-Fi signal to the level of background radio signals.

Signal to noise ratio

Checks channel utilization and identifies sources of RF inference.

Spectrum analysis

Identifies how strong a radio signal is at the receiver.

Received signal level

Identifies the number of useful bits delivered from the sender to the receiver.

~~Spectrum analysis~~ (leave blank)

Causes multiple copies of the same radio signal to be received by the receiving antenna.

~~Device saturation~~ Bounce

Degrades wireless network performance.

~~Signal to noise ratio~~ Device saturation

Explanation

You should be familiar with the following wireless networking concepts and terms:

- *Bounce* can cause multiple copies (one from each path) of the same signal to be received by the receiving antenna.
- *Received Signal Level* (RSL) identifies how strong the radio signal is at the receiver. The closer you are to the transmitter, the stronger the RSL.
- *Signal to Noise Ratio* (SNR) compares the level of the wireless network signal (RSL) to the level of background noise.
- A *spectrum analysis* is used to check channel utilization and to identify sources of RF

inference at each location where you plan to deploy an access point.

- *Device saturation* occurs when the wireless network is fully utilized and can no longer support additional wireless clients. Adding more clients can severely degrade network performance.

References

LabSim for Network Pro, Section 10.4.
[netpro18v5_all_questions_en.exm RT NP15_4.3-1]