Question 1

What is an important feature of the PHP scripting language?

Options:

A- It only works on Linux systems

B- It only works embedded in web applications

C- It only works from the command line

D- It works in web applications and at the command line

Answer:

D

Explanation:

PHP's Cross-Platform Nature:PHP originated for server-side web development, but also has a command-line interface (CLI) enabling its use for scripts and automation tasks.

Other Options:

Somelanguages are OS-specific (but less frequent with modern scripting languages) .

Many languages work in weborcommand line, notbothlike PHP.

References:

PHP (Introduction):Overviews mentioning its dual role in server-side web applications and as a general-purpose scripting language.
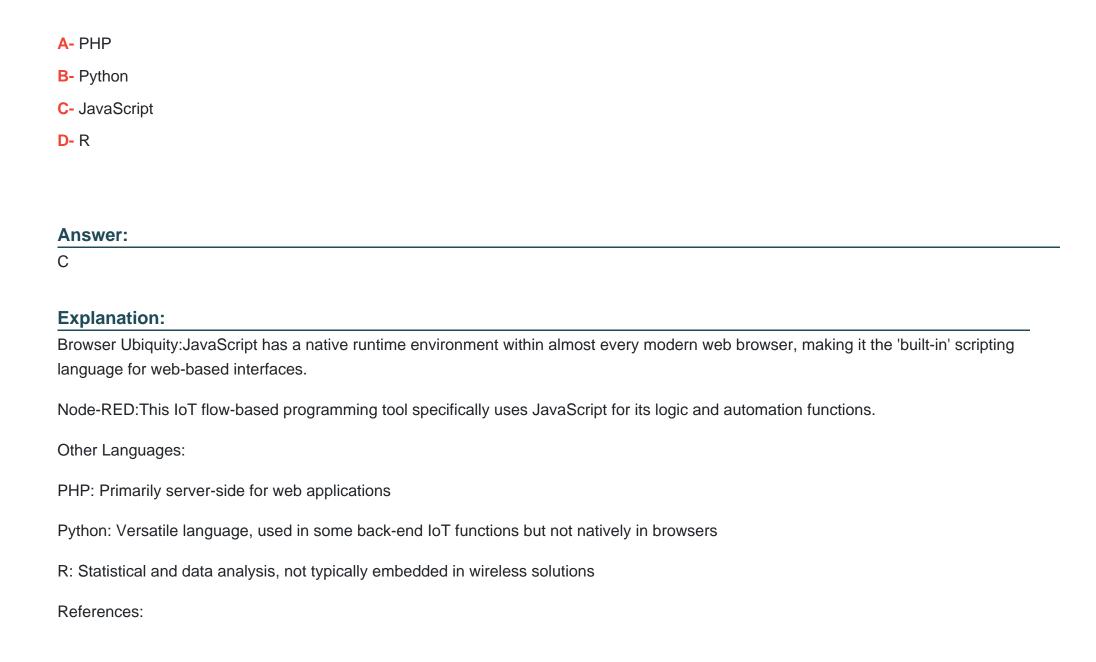
PHP CLI:Documentation on the command-line interface for PHP.

Question 2

Question Type: MultipleChoice

What scripting language works natively inside of nearly all modern Web browsers and may also be used for automation within some wireless solutions, such as Node-RED?

Options:

A- PHP

B- Python

C- JavaScript

D- R

Answer:

C

Explanation:

Browser Ubiquity:JavaScript has a native runtime environment within almost every modern web browser, making it the 'built-in' scripting language for web-based interfaces.

Node-RED:This IoT flow-based programming tool specifically uses JavaScript for its logic and automation functions.

Other Languages:

PHP: Primarily server-side for web applications

Python: Versatile language, used in some back-end IoT functions but not natively in browsers

R: Statistical and data analysis, not typically embedded in wireless solutions

References:

JavaScript (Browser Compatibility):Documentation of its near-universal support

Node-RED (Programming Model):Descriptions of how it uses JavaScript for node logic.

Question 3

Among these choices, what is the most common reason administrators use scripting during the deployment of a wireless solution?

Options:

A- To provide time for playing solitaire

B- To reduce configuration errors

C- To increase the signal strength of the resulting wireless links

D- To enhance the capabilities of the resulting solution

Answer:

B

Explanation:

Automation for Consistency:Scripts eliminate the potential for human error during repetitive configuration tasks on multiple devices. This ensures uniformity across the wireless solution.

Speed and Efficiency:Scripts can be much faster than manual configuration, particularly in large deployments.

Other Benefits:While scriptsmightaid signal strength (e.g., optimizing settings) or enhance solution capabilities, their core value in configuration is reducing errors.

References:

Network Automation:Benefits of using scripts for configuration management.

Configuration Management Best Practices:Emphasize the importance of consistency and repeatability.

Question 4

Question Type: MultipleChoice

In a wireless link, as the signal strength decreases, what else may decrease?

Options:

A- Noise

B- Interference

C- Latency

D- Transmission speeds

Answer:

D

Explanation:

Signal Strength and Data Rate:In wireless links, weaker signal strength often directly correlates to reduced transmission speeds. Modern wireless technologies use adaptive modulation and coding, sacrificing speed for reliability when signals become weaker.

Noise and Interference:While thesecanimpact performance, they don't inherently decrease simply because signal strength drops.

Latency:Latency can be affected by poor signal, but its primary drivers are distance and network congestion.

References:

Wireless Signal Strength vs. Speed:Articles explaining the relationship and how adaptive modulation works.

Modulation and Coding Schemes (MCS):Technical descriptions of how Wi-Fi and other wireless technologies adjust speeds based on signal quality.

Question 5

You must ensure proper security controls are in place for a wireless solution. The solution allows for the use of groups to grant access to resources and capabilities. What is the term used to describe a situation where an individual is granted more access than required because of inclusion in a group?

Options:

A- Improper delegation

B- Privilege escalation

C- Privilege creep

D- Improper grouping

Answer:

C

Explanation:

Privilege Creep Defined:Gradual accumulation of excessive permissions over time, often due to users changing roles or access needs not being adjusted accordingly.

Other Terms:

Privilege Escalation: A malicious act of obtaining higher-than-authorized access.

Improper Delegation/Grouping: Faulty permission assignment, but not the gradual accretion aspect.

References:

Principle of Least Privilege:Security best practice emphasizing the need to minimize access to only what's necessary.

Access Control Models:Discussions of how privilege creep can violate security principles.

Question 6

Question Type: **MultipleChoice**

You have been asked to locate an intermittent RF interference source. What tool will assist best in locating the generating device?

Options:

A- NMAP

B- WinPCAP

C- Spectrum analyzer

D- Protocol analyzer

Answer:

C

Explanation:

isualizing RF Interference:Spectrum analyzers display radio frequencies across a range, showing signal strength and potential interference sources. This is crucial for identifying non-Wi-Fi devices that might be disrupting your wireless solution.

Other Tools Have Limitations:

NMAP: Network mapper, focused on discovering devices, not RF analysis

WinPCAP: Packet capture software, helpful but doesn't directly display the RF spectrum.

Protocol Analyzer: Analyzes network traffic, but won't pinpoint physical layer interference.

References:

Spectrum Analyzers:How they work and common use cases in RF troubleshooting.

Wireless Interference Types:Resources that discuss non-Wi-Fi interference sources (microwaves, cordless phones, etc.)

Question 7

What provides the security (encryption) in an HTTPS connection?

Options:

A- IPSec

B- SNMPv3

C- SSL/TLS

D- SSH

Answer:

C

Explanation:

SSL/TLS Secures Web Traffic:HTTPS builds upon HTTP, adding the encryption provided by Secure Sockets Layer (SSL) or its successor, Transport Layer Security (TLS).

Other Protocols Have Different Purposes:

IPSec: Secures IP traffic at a network level, can be used alongside TLS.

SNMPv3: Management protocol, offers security features, but not the primary mechanism in HTTPS.

SSH: Secure remote shell, unrelated to web data encryption.

References:

TLS (and SSL):References of their role in HTTPS and how they provide encryption for web communication.

HTTPS Overview:Materials showing how TLS fits into the overall HTTPS architecture.

Question 8

Question Type: MultipleChoice

You have implemented a wireless mesh network. All mesh nodes are properly configured for participation in the same mesh network. Several of the mesh nodes are unable to connect to other mesh nodes. What action may provide a solution to this problem?

Options:

A- Place the faulty mesh nodes in their own mesh network

B- Move the faulty mesh nodes to provide for better signal strength

C- Change the output power settings only on the faulty mesh nodes

D- Change the security settings on the faulty mesh nodes

Answer:

B

Explanation:

Mesh Connectivity Depends on Signal:Mesh nodes relay data for each other. Weak signal strength between nodes can disrupt connectivity throughout the network.

Troubleshooting Signal Issues:Physically relocating affected nodes can improve their ability to form stable connections with other nodes in the mesh.

Why Other Options May Not Help:

Separate Mesh: Splits the network, not solving the root connectivity issue

Output Power: May help marginally, but significant improvement is typically achieved through repositioning.

Security Settings: Unlikely to cause connectivity issues between properly configured nodes in the same mesh.

References:

Wireless Mesh Network Troubleshooting:Guides addressing signal strength and coverage concerns.

RF Site Survey Tools:Resources on software that can help visualize signal strength and aid in node placement.

Question 9

What advantage is provided by using an NTP server within a wireless solution architecture?

Options:

A- It provides for semi-automatic IP addressing in wireless sensor networks

B- It ensures security through AES encryption

C- It ensures uniform, synchronized time among devices

D- It provides for name resolution for older network devices

Answer:

C

Explanation:

Importance of Time Sync in IoT:Coordinated actions, accurate data analysis, and event logging in wireless IoT solutions often rely on devices having a shared time reference.

NTP's Role:Network Time Protocol (NTP) enables devices to synchronize their clocks against a reliable time source (NTP server), ensuring consistency across the network.

Why Other Options Don't Fit:

IP Addressing: Usually handled by DHCP, not NTP.

Encryption: SSL/TLS secure data in transit, not related to timekeeping.

Name Resolution: Purpose of DNS, not NTP.

References:

Network Time Protocol (NTP):How it works and its importance in distributed systems.

IoT Time Synchronization Challenges:Articles highlighting the need for accuracy in sensor networks and similar use cases.

Question 10

What is an important acceptance agreement to achieve in the final customer meeting for a wireless IoT deployment?

Options:

A- Stakeholder acceptance

B- Support for wearable IoT solutions

C- Scope definition

D- Power supply provisioning

Answer:

A

Explanation:

Successful Deployment Depends on Buy-In:A final customer meeting signifies the handover phase. Achieving stakeholder agreement ensures everyone impacted by the solution has a voice and feels their concerns are addressed.

Sign-Off and Formal Acceptance:Stakeholders often need to formally 'sign-off' on a project's completion, indicating satisfaction and readiness for operational use.

Other Options: While Important, Not the Primary Goal:

Scope definition typically happens much earlier

Solutions may or may not include wearables

Power supply should already be planned

References:

Project Management Methodologies:Emphasis on stakeholder involvement & acceptance criteria.

ITIL (Change Management):Materials on getting approval before a system goes live.

Question 11

What is the most important consideration when deciding whether to implement a wired or wireless solution?

Options:

A- The distance between nodes

B- The availability of PoE

C- The applications being used

D- Business and system requirements

Answer:

D

Explanation:

Requirements Drive Decisions:The decision between wired or wireless must align with the solution's overall purpose, performance targets, and operational constraints.

Key Considerations:

Reliability:Does the application require guaranteed connectivity? (Wired may be favored).

Installation Cost:Can extensive cabling be done, or is it prohibitively expensive? (Wireless may be favored).

Flexibility and Scalability:Is node placement likely to change in the future? (Wireless may be favored).

Other Factors are Important, But Secondary:Distance, PoE availability, specific applications all matter, but they are assessedwithin the contextof the overarching business needs.

References:

Wireless vs. Wired Network Design:Comparisons of pros and cons, highlighting how use cases guide the choice.

IoT Solution Planning:Materials on defining requirementsbeforeselecting technology.

Question 12

Question Type: **MultipleChoice**

You are troubleshooting a problem with a wireless solution that uses MQTT where the IoT end devices are not reporting to the MQTT server/broker. At what Layer of the OSI Model should troubleshooting begin when using a bottom-up method?

Options:

A- Layer 1

B- Layer 4

C- Layer 5

D- Layer 6

Answer:

A

Explanation:

Bottom-Up Troubleshooting:The OSI model provides a structured diagnostic approach. Starting at Layer 1 ensures basic physical connectivity issues are ruled out first.

MQTT Relies on IP:MQTT operates at a higher layer of the OSI model, relying on TCP/IP (Layers 4 and 3) for communication. Problems at the physical layer will disrupt everything built upon it.

Checking the Fundamentals:Before investigating complex application issues (MQTT), verify cables, link lights, Wi-Fi signal strength, etc.

References:

OSI Model:Descriptions of the seven layers, emphasizing the foundation provided by Layer 1 (Physical).

Network Troubleshooting Guides:Resources that outline common Layer 1 problems and their symptoms.