CompTIA.N10-009J.v2026-09-22.q217

試験コード：	N10-009J
試験名称：	CompTIA Network+ Certification Exam (N10-009日本語版)
認証ベンダー：	CompTIA
無料問題の数：	217
バージョン：	v2026-09-22
ページの閲覧量：	109
問題集の閲覧量：	2842

https://www.jpnshiken.com/shiken/CompTIA.N10-009J.v2026-09-22.q217.html

質問: **1**
ネットワーク上の機密情報を最も直接的に保護するものは次のどれですか?
A. 転送中のデータの暗号化
B. 最小権限の原則
C. ロールベースのアクセス制御
D. 多要素認証
正解: **(**正解を表示します**)**
The option that most directly secures sensitive information on the network is data-in-transit encryption. This ensures that data packets are unreadable to attackers who intercept them while moving across the network.
Protocols such as TLS, HTTPS, IPsec, and SSH protect confidentiality and integrity of sensitive information.
B). Principle of least privilege (PoLP) secures access control but does not directly protect data in motion.
C). Role-based access control (RBAC) enforces permissions but again does not secure the data while transmitted.
D). Multifactor authentication (MFA) strengthens identity verification but does not directly protect the data itself once transmitted.
Thus, while all options contribute to overall security, encryption of data-in-transit most directly addresses protection of sensitive information on the network.
References (CompTIA Network+ N10-009):
Domain: Network Security - Encryption methods, confidentiality, data-in-transit protection.

質問: **2**
ネットワーク技術者が、マーケティング部門のユーザーのために経理部門のフロアにコンピュータを設置しました。ユーザーから、マーケティング部門の共有ドライブにはアクセスできないが、インターネットにはアクセスできるという報告がありました。この問題の原因として最も可能性が高いのは次のうちどれですか。
A. スイッチポートのデュプレックスが一致しません
B. ゲートウェイ設定が正しく構成されていません
C. VLANの割り当てが正しくありません
D. SVI が間違った IP アドレスに割り当てられています
正解: **C (**コメントを発表する**)**
The user's inability to access the marketing department's shared drives, despite having internet access, suggests a network segmentation issue. The most likely cause is an incorrect VLAN assignment. The computer is physically located on the accounting department floor, and the switchport is likely configured for the accounting VLAN, not the marketing VLAN. VLANs segment network traffic, and if the computer is in the wrong VLAN, it cannot communicate with the marketing department's resources.
Why not Mismatched switchport duplex? Duplex mismatches cause performance issues (e.g., packet loss) but not specific access denials to shared drives.
Why not Misconfigured gateway settings? Incorrect gateway settings would prevent internet access, which the user has.

Why not SVI is assigned to the wrong IP address? A Switch Virtual Interface (SVI) with an incorrect IP address affects inter-VLAN routing, but this would likely impact multiple users, not just one.
Reference:CompTIA Network+ N10-009 Objective 2.2: Explain the purpose of network segmentation and VLAN configuration. The CompTIA Network+ Study Guide (e.g., Chapter 6: Switching) explains that VLANs isolate traffic, and incorrect VLAN assignments prevent access to resources on other VLANs.

質問**: 3**
一連のポリシーを使用して、ユーザーの ID に基づいてネットワークへのアクセスを許可または拒否する NAC のタイプは次のどれですか。
A. Standard ACL
B. MAC filtering
C. 802.1X
D. SSO
正解**: (**正解を表示します**)**
802.1X is a port-based Network Access Control (NAC) method that enforces authentication before allowing access to the network. It uses a RADIUS server for identity verification and policy enforcement, ensuring only authorized users/devices gain access.
A). Standard ACL filters traffic by IP, not identity.
B). MAC filtering controls devices by hardware address but can be spoofed.
D). SSO (Single Sign-On) provides user convenience across services, not network-level access control.
References (CompTIA Network+ N10-009):
Domain: Network Security - NAC, 802.1X authentication, identity-based access.

質問**: 4**
VoIP ハンドセット接続のトラブルシューティング中に、技術者のラップトップは同じポートを使用してネットワーク リソースに正常に接続できます。技術者はスイッチ上のポートを識別する必要があります。技術者はスイッチとポートを特定するために次のどれを使用する必要がありますか?
A. LLDP
B. IKE
C. VLAN
D. ネットスタット
正解**: (**正解を表示します**)**
Link Layer Discovery Protocol (LLDP) is a network protocol used for discovering devices and their capabilities on a local area network, primarily at the data link layer (Layer 2). It helps in identifying the connected switch and the specific port to which a device is connected. When troubleshooting a VoIP handset connection, the technician can use LLDP to determine the exact switch and port where the handset is connected. This protocol is widely used in network management to facilitate the discovery of network topology and simplify troubleshooting.
Other options such as IKE (Internet Key Exchange), VLAN (Virtual LAN), and netstat (network statistics) are not suitable for identifying the switch and port information. IKE is used in setting up secure IPsec connections, VLAN is used for segmenting networks, and netstat provides information about active connections and listening ports on a host but not for discovering switch port details.
Reference: CompTIA Network+ Certification Exam Objectives - Network Troubleshooting and Tools section.

質問**: 5**
次のどれが回避、受容、緩和、移転と関連していますか?
A. リスク

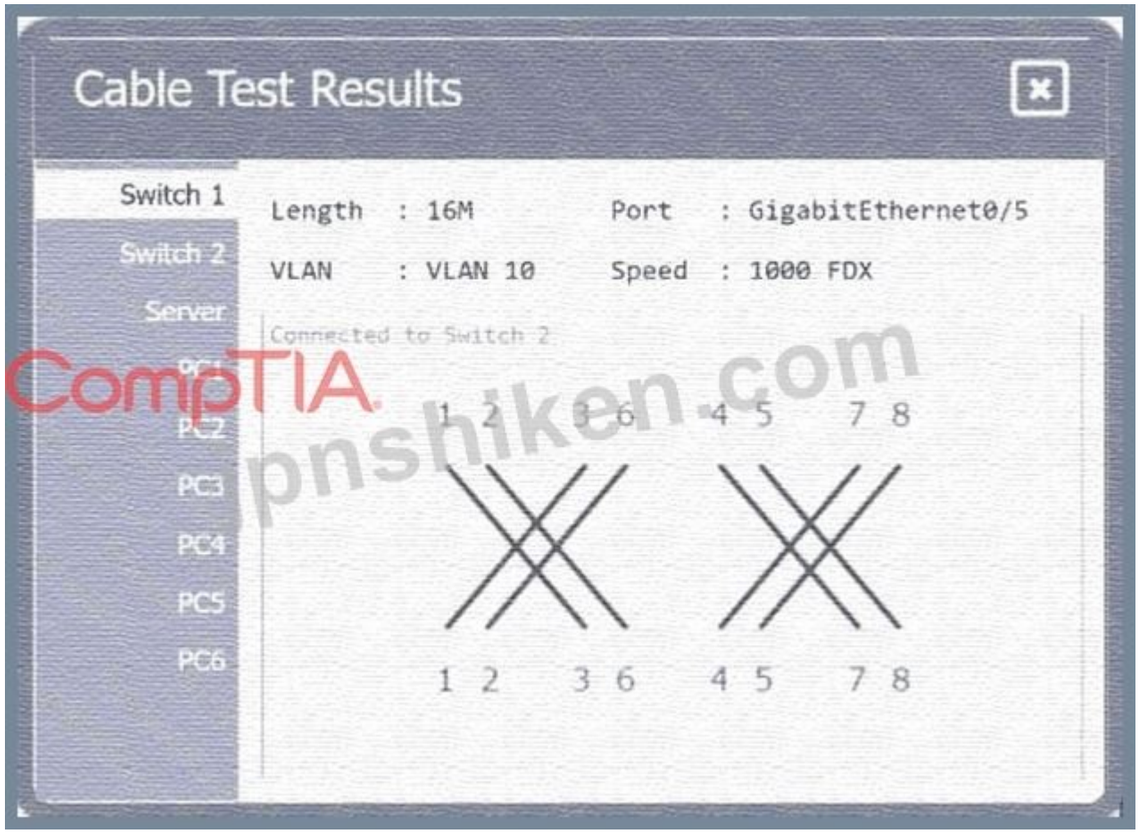
B. エクスプロイト
C. 脅威
D. 脆弱性
正解: **(**正解を表示します**)**
These four terms-avoidance, acceptance, mitigation, and transfer-are strategies used in risk management.
From Andrew Ramdayal's guide:
"Risk in security refers to the potential for loss, damage, or destruction of assets or data due to a threat exploiting a vulnerability. Risk management strategies include avoidance, acceptance, mitigation, and transfer."

質問: **6**
ネットワーク管理者は、新しく設置したスイッチがネットワークに接続できないという問題のトラブルシューティングを試みています。管理者はスイッチにログオンし、インターフェース上で衝突が発生していることを確認しました。最も可能性の高い問題は次のうちどれですか？
A. 速度が間違っています
B. ジャンボフレームが有効
C. VLANが正しくありません
D. デュプレックス不一致
正解: **(**正解を表示します**)**
The most likely issue is a duplex mismatch, which is a well-documented cause of collisions and poor network performance, as outlined in the CompTIA Network+ N10-009 troubleshooting objectives. A duplex mismatch occurs when one end of a network link is configured for full duplex while the other end is operating in half duplex. In half-duplex mode, devices must take turns transmitting and receiving data, which inherently allows for collisions. When paired with a full-duplex device-which expects simultaneous send and receive-collisions and retransmissions occur frequently.
The presence of collisions on a switch interface is a key diagnostic clue. Modern Ethernet switches operating correctly in full duplex should not experience collisions at all. When collisions are observed, it almost always points to a duplex configuration issue, often caused by manual speed/duplex settings on one device and auto- negotiation on the other.
A wrong speed setting may prevent link establishment entirely or cause errors, but it does not typically result in collisions. Jumbo frames can cause packet drops or fragmentation issues, not collisions. An incorrect VLAN configuration affects logical segmentation and connectivity but operates at Layer 2 and does not generate collisions.
CompTIA Network+ emphasizes duplex mismatch as a classic and frequently tested troubleshooting scenario.
Correcting it-usually by enabling auto-negotiation on both ends-restores normal, collision-free communication.

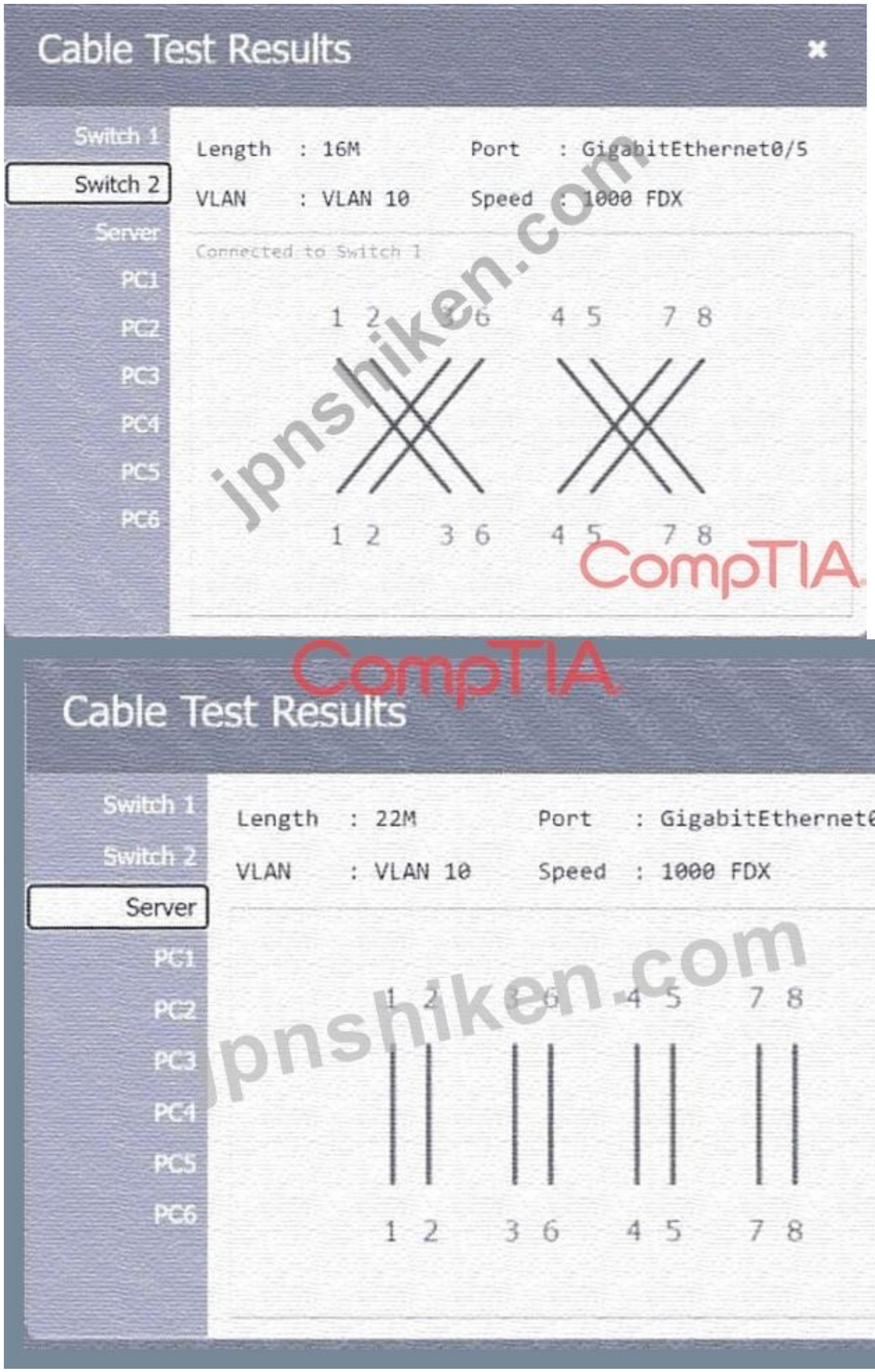
質問: **7**
ネットワーク管理者が最近、自律型無線APを設定し、comptiaspeedtester.comでスループットテストを実施しました。結果は75Mbpsでした。他のAPに接続すると、500Mbpsに達しました。この差の理由として最も可能性が高いのは次のうちどれですか？
A. チャネル幅の設定
B. DNSサーバーの問題
C. 認証失敗
D. DHCP設定が正しくありません
正解: **(**正解を表示します**)**
The channel width (20 MHz vs. 40 MHz vs. 80 MHz) directly impacts Wi-Fi throughput. If the AP is configured with a narrow channel width (e.g., 20 MHz), maximum data rates will be significantly lower than other APs using wider channels (e.g., 80 MHz). This matches the scenario where one AP achieves only ~75 Mbps, while others reach 500 Mbps.
B). DNS issues affect name resolution, not raw throughput.
C). Authentication failure would prevent connection, not reduce throughput.

D). DHCP issues would prevent obtaining an IP, not cause slower speeds.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Wireless throughput issues, channel width configuration.

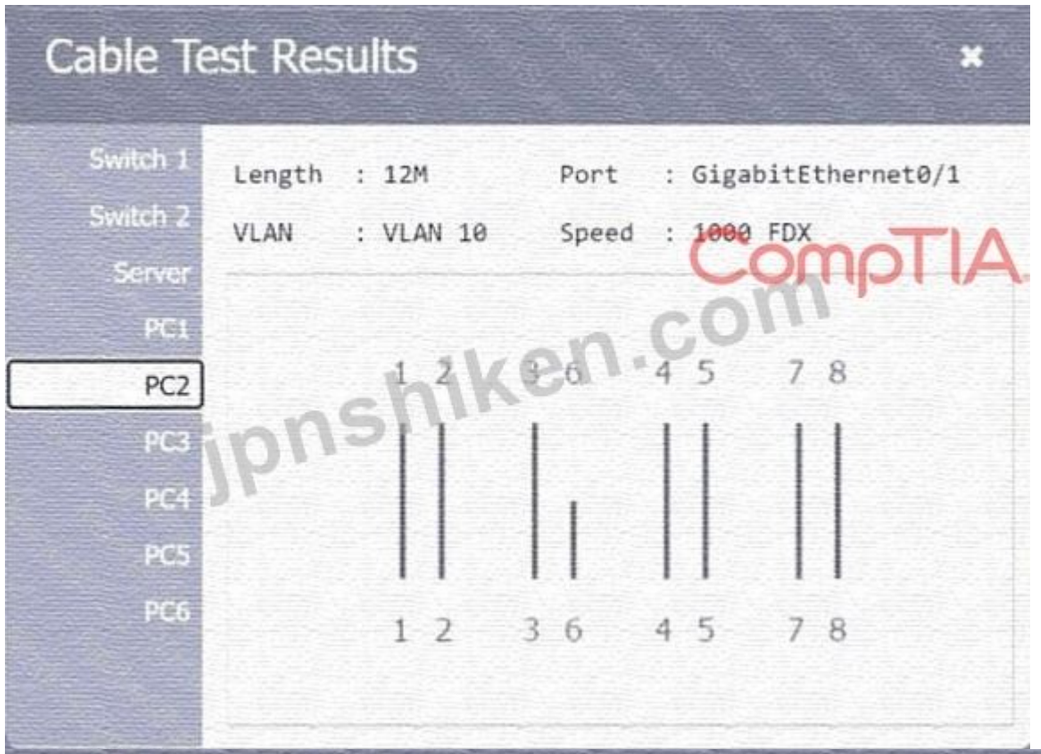
質問: **8**
ネットワーク技術者は、顧客のSOHOネットワークの問題を解決する必要があります。顧客から、一部のPCがネットワークに接続できない一方、他のPCは正常に動作しているようだという報告がありました。
説明書
すべてのネットワーク コンポーネントのトラブルシューティングを行います。
まずケーブル テストの結果を確認し、適切な PC、サーバー、およびレイヤー 2 スイッチをクリックして診断します。
問題のあるコンポーネントを特定し、それぞれの問題を修正するための解決策を提案します。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。

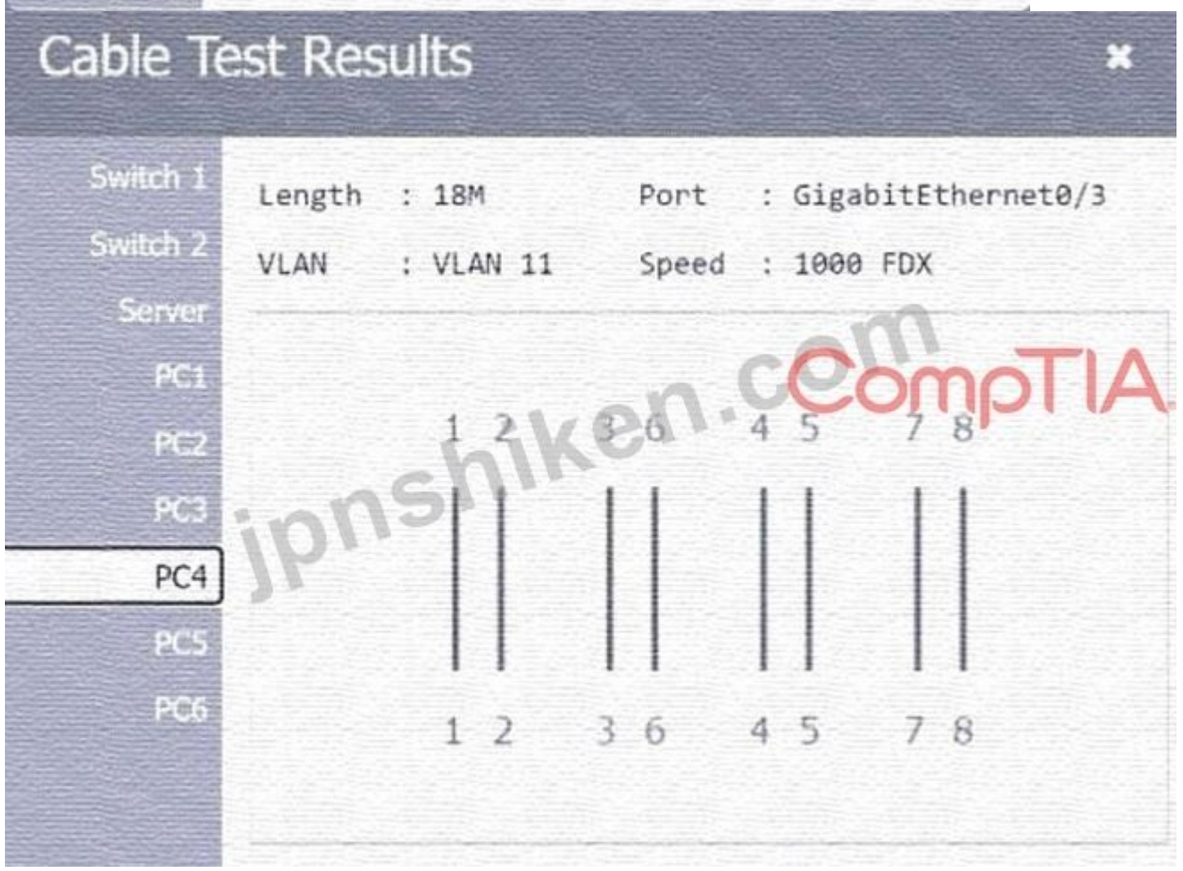


CompTIA
pnshiken.com

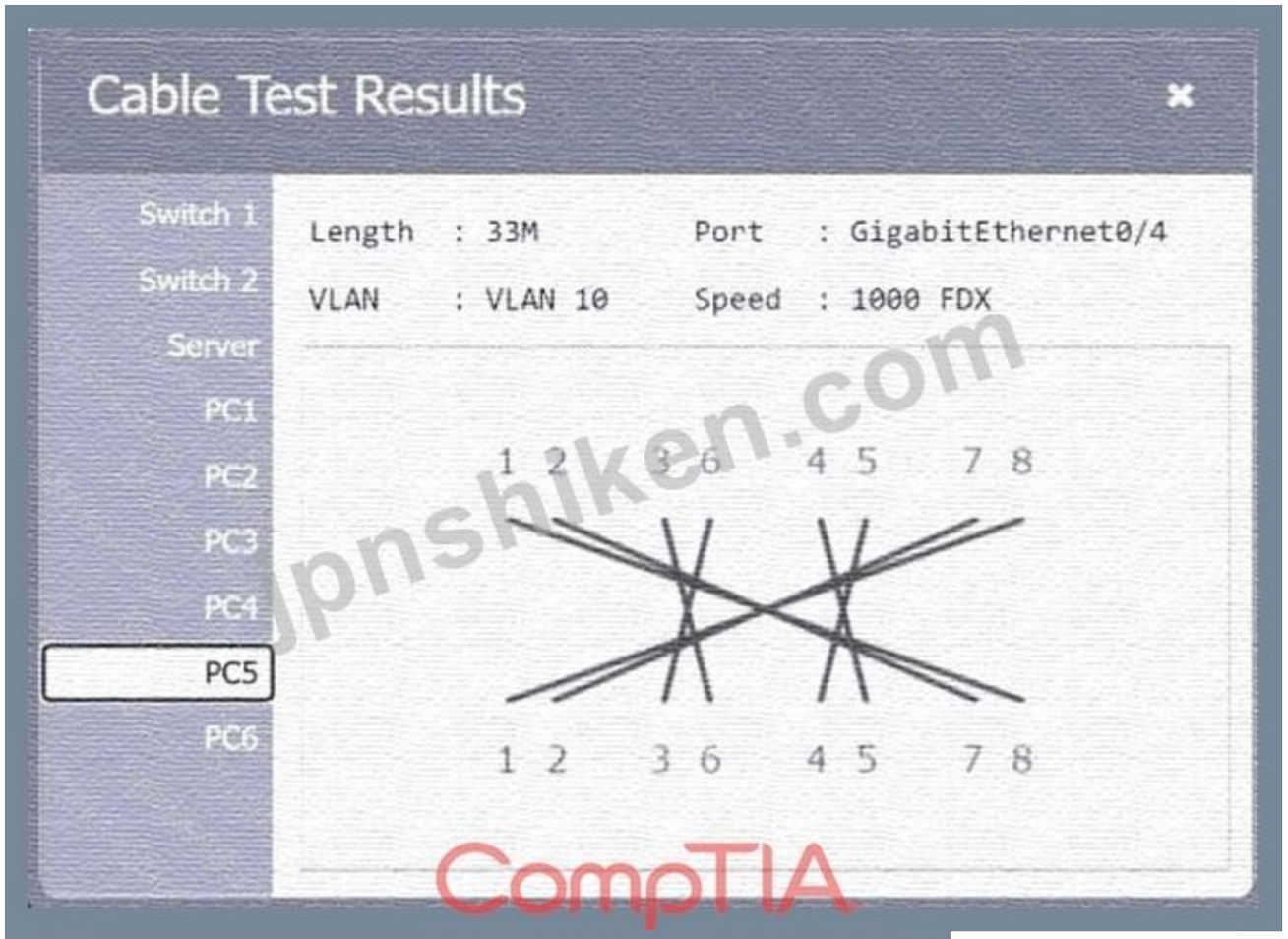


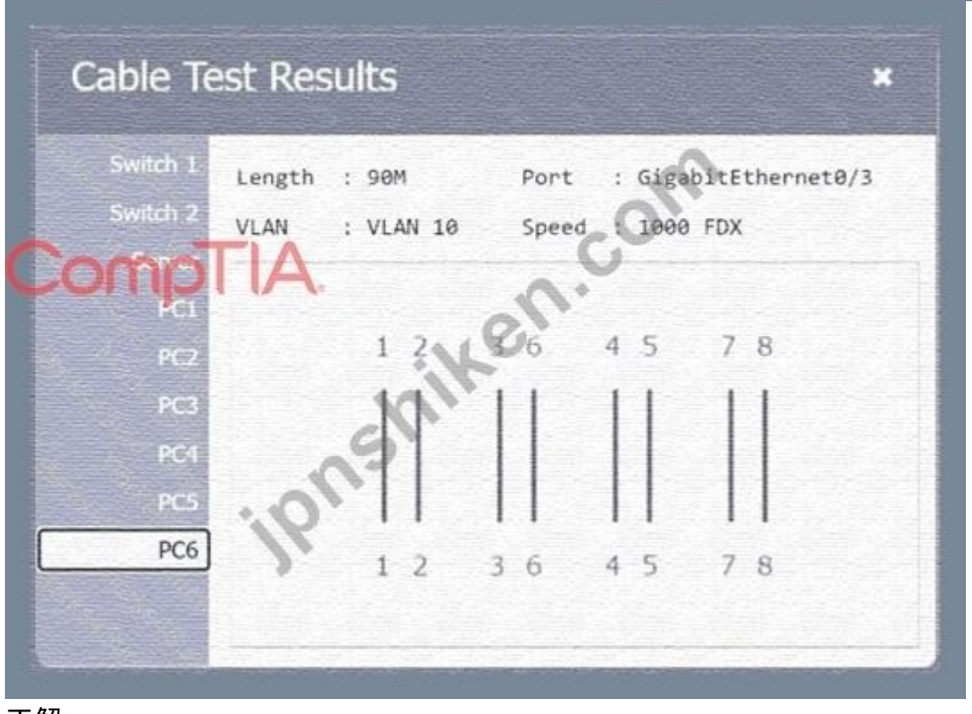
CompTIA
jpnshiken.com





jpnshiken.com
CompTIA





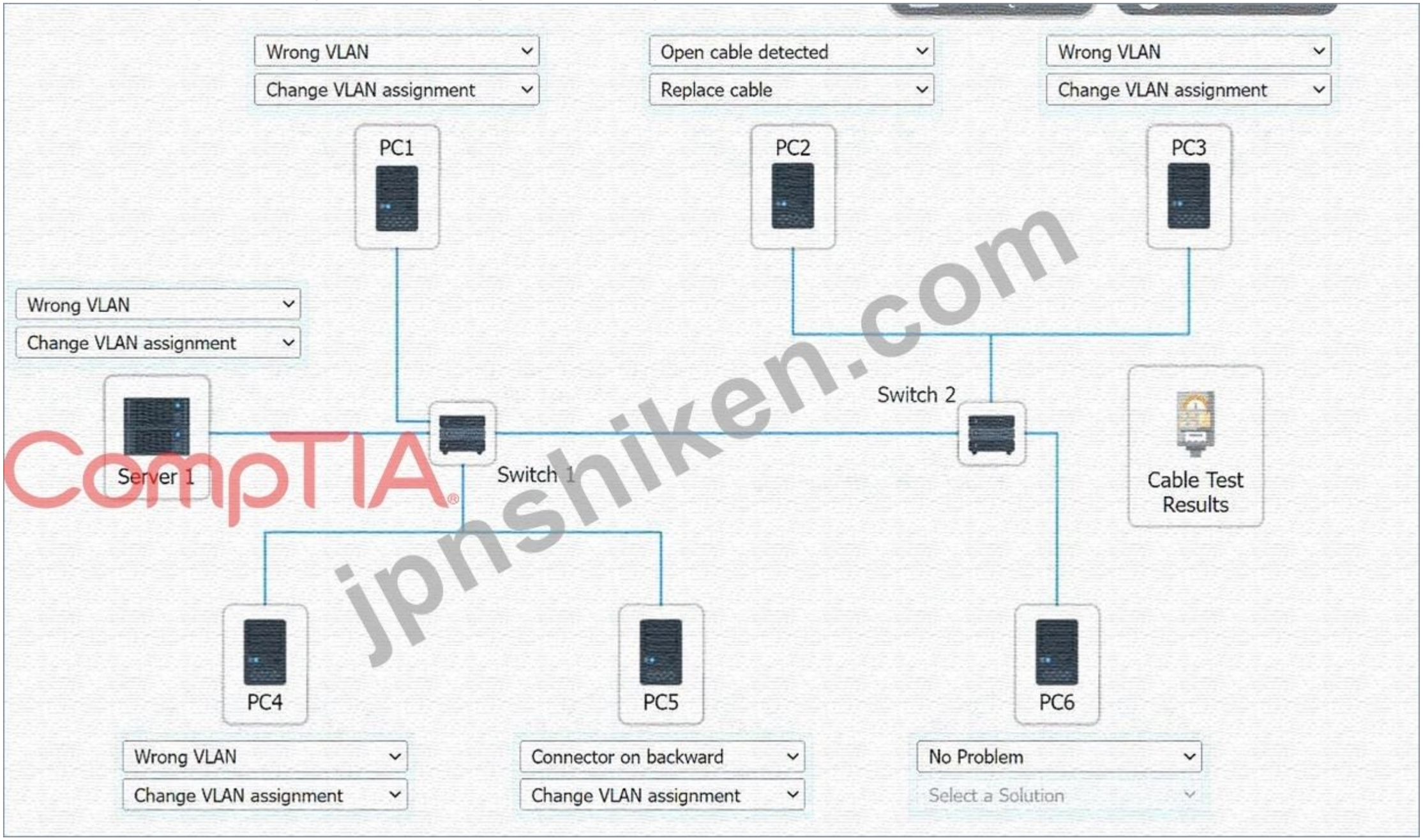
jpnshiken.com
CompTIA

正解:

See the answer and solution below:

Explanation:

A computer network diagram with many boxes and text AI-generated content may be incorrect.



CompTIA
jpnshiken.com

質問: **9**

ネットワーク管理者は、インターネットへのアクセスをフィルタリングするソリューションを実装する必要があります。管理者が実装する可能性が高いソリューションは次のどれですか？

A. ルーター

B. クラウドゲートウェイ

C. プロキシ

D. 侵入検知システム

正解: (正解を表示します)
A proxy server can filter internet access by controlling which websites or services users can reach. It enforces content policies and can provide caching and monitoring.
A). A router directs traffic but doesn't filter internet sites by itself.
B). A cloud gateway could also filter, but the most direct answer is proxy.
D). An IDS detects suspicious activity but doesn't filter browsing access.
References (CompTIA Network+ N10-009):
Domain: Network Security - Proxy servers, filtering, access control.

質問: **10**
ある企業が、1Gbpsのバックボーン、新しいアクセスポイント、そして全従業員向けの新しいタブレットを導入し、無線インフラをアップグレードしました。しかし、IT部門は、以前のタブレットと比べて速度が向上していないことに気づきました。以下のネットワーク情報に基づいて、パフォーマンスの問題の最も可能性の高い原因はどれでしょうか？
A. AP 4 にはデバイスが接続されていません。
B. デバイスが多すぎて混雑が発生しています。
C. APに正しいVLAN割り当てがありません。
D. スイッチの帯域幅がボトルネックになっています。
正解: (正解を表示します)
The most likely answer is D. Switch bandwidth is creating a bottleneck . Even though the company upgraded the wireless environment with newer access points and new tablets, wireless performance still depends on the capacity of the wired network that the APs connect back to. If multiple APs are sending traffic through a shared switch uplink or limited switch bandwidth, that wired segment can become the choke point, preventing users from seeing the benefit of the newer wireless equipment.
This kind of issue shows up often when organizations focus on upgrading the wireless edge but do not account for the aggregate traffic load feeding into the switching infrastructure. Faster wireless standards can increase the amount of traffic that reaches the switch, but if the switching path cannot handle that volume efficiently, end-user throughput will still feel unchanged.
The other options are less convincing. One AP having no connected devices does not explain why speeds on active clients are not improved. VLAN assignment problems would more likely cause access or segmentation issues rather than a general performance ceiling. Device congestion can hurt performance, but the information given points more strongly to the wired backhaul as the limiting factor.
In this scenario, the wireless upgrade is being held back by the switching side of the network, making switch bandwidth bottleneck the best answer.

質問: **11**
EOL と EOS の違いは次のどれですか?
A. EOL により製品は廃止されますが、サポートは提供される場合があります。
B. EOS は無料サポートをサブスクリプション モデルに置き換えます。
C. EOS は物理的な製品にのみ適用されます。
D. EOL でも保証サービスは引き続き保証されます。
正解: (正解を表示します)
The correct answer is EOL discontinues the product but may offer support. According to CompTIA Network+ (N10-009) objectives related to lifecycle management and vendor support policies, End of Life (EOL) indicates that a product is no longer being manufactured or sold by the vendor. However, after EOL is declared, the vendor may continue to provide limited support, updates, or warranty services for a defined period.
In contrast, End of Support (EOS) means the vendor has stopped providing technical assistance, patches, firmware updates, and security fixes for the product. Once a product reaches EOS, organizations are responsible for maintaining it without vendor assistance, which can introduce operational and security risks.

Option B is incorrect because EOS does not typically convert support into a subscription model-it signifies the termination of support. Option C is incorrect because EOS applies to both hardware and software products. Option D is incorrect because warranty terms depend on vendor policy and are not guaranteed after EOL status.
Therefore, the key distinction is that EOL ends product sales, while EOS ends vendor support.

質問: **12**
次のトラブルシューティング手順のうち、変更諮問委員会に意思決定に必要な情報を提供するものはどれですか?
A. 問題を特定します。
B. 考えられる原因の理論を構築します。
C. 原因を特定するために理論をテストします。
D. 行動計画を立てます。
正解: **D (**コメントを発表する**)**
A Change Advisory Board (CAB) reviews and approves network changes. Before approval, they need a detailed action plan outlining the change, potential impacts, and mitigation strategies.
* A Plan of Action includes risk assessments, rollback procedures, and deployment steps, which are critical for decision-making.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Network Troubleshooting Methodologies

質問: **13**
次の OSI モデル層のうち、データ転送にコネクションレス プロトコルを利用できるのはどれですか?
A. 物理
B. ネットワーク
C. トランスポート
D. アプリケーション
正解: **(**正解を表示します**)**
The Network layer (Layer 3 of the OSI model) can utilize the connectionless protocol IP (Internet Protocol) to send data packets independently without establishing a connection. This approach is typical for protocols like IP, which provide best-effort delivery rather than guaranteed delivery. The document explains:
"The OSI Network Layer is responsible for logical addressing and routing, and it can utilize connectionless protocols like IP to send packets without requiring a session setup. This layer does not guarantee packet delivery, relying on higher layers for error detection or correction if needed."

質問: **14**
ネットワーク管理者は、ネットワークへの侵入を試みている脅威アクターを隔離し、特定できるソリューションを必要としています。攻撃の種類を特定するために、管理者が実装すべき対策は次のうちどれですか？
A. MFA
B. スクリーンドサブネット
C. キャプティブポータル
D. ハニーポット
正解: **D (**コメントを発表する**)**
A honeypot is specifically designed to attract, isolate, and observe malicious activity so defenders can learn how an attacker is operating and determine attack techniques. In the context of Network+ (N10-009) security objectives, honeypots (and broader deception technologies) are defensive controls used to detect reconnaissance and exploitation attempts by presenting a decoy system or service that appears legitimate.

Because a honeypot should not receive normal production traffic, any interaction is suspicious, making it valuable for identifying threat actors, collecting indicators of compromise, and analyzing the attacker's tools, commands, and behavior patterns. This supports the goal of understanding the type of attack used (for example, credential stuffing, exploitation attempts, lateral movement probes) while keeping the attacker away from real assets.
MFA strengthens authentication but does not provide a controlled environment to observe attacker techniques.
A screened subnet (DMZ) is for segmentation of public-facing services and reducing exposure of internal systems, but it is not primarily used to "bait" and analyze attackers. A captive portal enforces user acknowledgement/authentication for network access; it is not a deception/analysis system. Therefore, honeypot is the best match.

質問: **15**
邪悪な双子が達成する目的は次のどれですか?
A. DNSポイズニング
B. ログイン資格情報
C. ARPスプーフィング
D. サービス拒否
正解: **(**正解を表示します**)**
An evil twin attack is when an attacker sets up a rogue access point (AP) with the same SSID as a legitimate one to trick users into connecting. Once users connect, attackers often present fake login pages or capture unencrypted session data to steal login credentials.
A). DNS poisoning manipulates DNS resolution but is not inherent to evil twin.
C). ARP spoofing is a Layer 2 attack involving MAC/IP mapping manipulation.
D). Denial of service can be a side effect but is not the primary objective of evil twin attacks.
The main purpose of an evil twin is credential theft, enabling further unauthorized access to networks or systems.
References (CompTIA Network+ N10-009):
Domain: Network Security - Wireless attacks, rogue APs, evil twins.

質問: **16**
ネットワーク アーキテクトは、公共安全車両に信頼性の高いサービスを提供するために、ワイヤレス フィールド ネットワークを構築する必要があります。次のネットワークの種類のどれが最適なソリューションでしょうか。
A. メッシュ
B. アドホック
C. ポイントツーポイント
D. インフラストラクチャ
正解: **A (**コメントを発表する**)**
A mesh network is the best solution for providing reliable wireless service to public safety vehicles. In a mesh network, each node (vehicle) can connect to multiple other nodes, providing multiple paths for data to travel.
This enhances reliability and redundancy, ensuring continuous connectivity even if one or more nodes fail.
Mesh networks are highly resilient and are well-suited for dynamic and mobile environments such as public safety operations.References: CompTIA Network+ study materials.

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu **792**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
ヘルプデスクの技術者は、ユーザーがインターネットの URL にアクセスできないという報告を受け取ります。技術者が ping テストを実行すると、URL を使用するとサイトが失敗し、IP を使用するとサイトが成功することを発見しました。技術者が次に利用すべきツールは次のどれですか。
A. tcpdump
B. tracert
C. nmap
D. dig
正解: **(**正解を表示します**)**
The issue is clearly related to DNS resolution, as IP-based connections succeed but domain name-based ones fail.
D). dig (Domain Information Groper) is a DNS lookup tool used to troubleshoot DNS problems by querying name servers directly.
Other tools are less relevant here:
A). tcpdump is a packet analyzer and is more advanced for deeper traffic analysis.
B). tracert is used to trace the route to a destination, not ideal for DNS issues.
C). nmap is a port scanner and network mapper, not for resolving DNS problems.
Reference:
CompTIA Network+ N10-009 Official Objectives: 5.1 - Given a scenario, use the appropriate network troubleshooting tools.

質問: **18**
ネットワーク エンジニアは、リモート ブランチのルーターを含むネットワーク サービスを仮想化する必要があります。次のソリューションのうち、要件を満たすものはどれですか。
A. NFV
B. VRF
C. VLAN
D. VPC
正解: **A (**コメントを発表する**)**
Network Functions Virtualization (NFV): NFV is a technology that virtualizes network services like routing, firewalls, and load balancers. It allows these services to run on virtual machines rather than requiring dedicated hardware. This is ideal for remote branch locations where deploying physical devices is costly and complex.
VRF (B): Virtual Routing and Forwarding is used for segmenting routing tables but does not virtualize services.
VLAN (C): Virtual Local Area Networks help segregate broadcast domains but are unrelated to virtualizing network functions.
VPC (D): Virtual Private Cloud is used for cloud computing but does not pertain to virtualizing network services.
Reference: CompTIA Network+ Official Study Guide, Domain 2.1 (Virtualization and Cloud Concepts).

質問: **19**
DNS ポイズニング攻撃の特徴を最もよく表しているのは次のうちどれですか?
A. DNS アドレス レコードは DNS サーバー上で編集および変更されます。
B. 攻撃者は、正規のサーバーの代わりに悪意のある DNS サーバーを設定します。

C. DNS クライアント要求が傍受され、誤った応答が返されます。
D. 偽の DNS レコードが DNS サーバーのキャッシュに挿入されます。
正解: **(**正解を表示します**)**
DNS poisoning (also commonly called DNS cache poisoning) is characterized by inserting fraudulent DNS data into a resolver's cache so that subsequent queries return incorrect IP mappings. Option D describes this precisely: false DNS records are injected into a DNS server's cache, causing users to be redirected to attacker- controlled destinations even when they request a legitimate hostname. This aligns with Network+ security objectives covering common network attacks targeting name resolution and trust relationships. Editing authoritative DNS records on a DNS server (A) implies direct compromise or unauthorized administrative change, which is a different scenario than cache poisoning. Setting up a malicious DNS server in place of a legitimate server (B) is closer to DNS hijacking or rogue DNS configuration rather than cache poisoning.
Intercepting client requests and returning false responses (C) describes man-in-the-middle style spoofing on the wire; while related, the defining "poisoning" trait is the persistence created by corrupting the cache so the bad answer continues to be served. For defensive relevance in Network+ scope, cache poisoning highlights the importance of DNS security controls such as source port randomization, transaction ID entropy, and DNSSEC validation where applicable.

質問: **20**
ネットワーク アクセス制御にエンタープライズ認証を使用できるようにする標準は次のどれですか。
A. 802.1Q
B. 802.1X
C. 802.3bt
D. 802.11h
正解: **(**正解を表示します**)**
Comprehensive and Detailed Explanation (aligned to N10-009):
802.1X provides port-based Network Access Control (NAC), requiring authentication (often through RADIUS) before granting access. This is the standard for enterprise authentication on both wired and wireless networks.
A). 802.1Q defines VLAN trunking.
C). 802.3bt defines higher-power PoE.
D). 802.11h deals with spectrum management in wireless.
References (CompTIA Network+ N10-009):
Domain: Network Security - NAC, 802.1X authentication.

質問: **21**
ある中小企業が、自社のネットワークに静的ルーティングと動的ルーティングのどちらを採用するかを検討しています。成長を続けるネットワークにおいて、動的ルーティングを使用する最も適切な理由は次のうちどれですか？
A. 手動で入力したルートを使用する場合に比べて設定が簡単です
B. 追加のネットワークセキュリティ制御は必要ありません
C. 強化されたネットワーク監視と可視性を備えています
D. ネットワークトポロジの自動変更と更新が含まれます
正解: **(**正解を表示します**)**
Dynamic routing is most beneficial in a growing/changing network because it can automatically learn, adapt, and update routes as the topology changes. In Network+ (N10-009) routing objectives, dynamic routing protocols exchange routing information between routers and recalculate paths when links go down, new networks are added, or metrics change. This reduces the operational burden and the risk of human error that increases as the environment scales. With dynamic routing, adding a new subnet or branch often requires far fewer manual updates because routers propagate new route information automatically, and convergence mechanisms help restore connectivity after failures.

Option A can be partly true in large environments, but the core "best reason" emphasized for dynamic routing is the automatic adaptation to topology changes. Option B is incorrect- dynamic routing may introduce additional security considerations (route filtering, authentication, neighbor control). Option C is not a defining advantage; monitoring visibility depends on tools/telemetry rather than routing type. Therefore, the strongest and most correct reason is automatic changes and updates in network topology.

質問: **22**
ある会社では、特定のグループに参加しているすべてのコンピューターで再生できるビデオ ストリーミング ソリューションを実装していますが、ルーターの ACL によってトラフィックがブロックされています。ACL で許可される最も適切な IP アドレスは次のどれですか。
A. 127.0.0.1
B. 172.17.1.1
C. 224.0.0.1
D. 240.0.0.1
正解: **(**正解を表示します**)**
224.0.0.1 is a multicast address that allows packets to be sent to all hosts within a multicast group. Since video streaming often uses multicast to efficiently distribute data to multiple clients without unnecessary duplication, this is the correct answer.
*Why not the other options?
*127.0.0.1 (A) - This is the loopback address used for internal device testing, not for multicast traffic.
*172.17.1.1 (B) - This is a private unicast address, meaning it can only send packets to one specific host.
*240.0.0.1 (D) - This falls within the reserved experimental IP address range and is not used for multicast.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 7: IP Addressing and Subnetting

質問: **23**
C社はA社とB社を買収する。C社はこれら3社のネットワークを統合し、1つのクラスBネットワークにする必要がある。さらに、各社のネットワーク容量を20%増加させる必要がある。C社はまた、A社とB社それぞれに存在する未知のセキュリティ脆弱性に対応するため、両社をセグメント化する必要がある。
説明書：
C社の要件を満たす適切なサブネット範囲を選択してください。

Company	Current number of devices	Current subnet range	New subnet range
A	32	192.168.10.1/27	Select 192.168.10.0/22 10.0.8.0/26 192.168.10.0/27 10.0.1.0/21 192.168.10.0/26 10.0.0.1/17 **10.0.0.1/18** 192.168.1.0/23 192.168.1.0/22 10.0.1.0/22 10.0.8.0/27
B	100	192.168.1.1/22	Select 192.168.10.0/27 10.0.1.0/22 192.168.1.0/23 10.0.0.1/17 **192.168.1.0/22** 10.0.8.0/27 10.0.8.0/26 10.0.0.1/18 192.168.10.0/26 192.168.10.0/22 10.0.1.0/21
C	10,000	10.0.0.1/8	Select 192.168.10.0/27 10.0.1.0/22 192.168.1.0/23 10.0.0.1/17 **192.168.1.0/22** 10.0.8.0/27 10.0.8.0/26 10.0.0.1/18 192.168.10.0/26 192.168.10.0/22 10.0.1.0/21

CompTIA
jpnshiken.com

正解:

Company	Current number of devices	Current subnet range	New subnet range
A	32	192.168.10.1/27	Select
B	100	192.168.1.1/22	Select
C	10,000	10.0.0.1/8	Select

CompTIA

jpnshiken.com

Explanation:
A = 192.168.10.0/26
B = 192.168.1.0/23
C = 10.0.0.1/18
Using the choices shown in the screenshot, the best-fit subnet selections are based on host growth requirements first, then segmentation .
For Company A , the current device count is 32 . With 20% growth , that becomes about 39 devices . A /27 only supports 30 usable hosts , so it is too small. A /26 supports 62 usable hosts , so 192.168.10.0/26 is the correct choice.
For Company B , the current device count is 100 . With 20% growth , that becomes 120 devices . The smallest correct subnet would normally be a /25 with 126 usable hosts , but that option is not shown. From the available choices, 192.168.1.0/23 is the smallest subnet that still supports more than 120 hosts, so that is the best answer.
For Company C , the current device count is 10,000 . With 20% growth , it needs space for 12,000 hosts . A
/18 provides 16,382 usable hosts , while a /19 is not available and a /21 or /22 would be far too small.
Therefore, 10.0.0.1/18 is the correct selection.
One important note: the dropdown choices shown do not actually let all three companies be placed into a single true Class B network block. So these answers are the best valid selections from the provided options .

質問: **24**
ネットワーク技術者が故障したNICを搭載したPCで作業しています。ホストはセキュアポートを備えたスイッチに接続されています。接続ケーブルをテストし、正常なNICを使用しても、ホストはネットワークに接続できません。接続問題の原因は次のどれですか？
A. 新しいカードのMACアドレス
B. BPDUガード設定
C. リンクアグリゲーション設定
D. PoE電力バジェット
正解: **A (**コメントを発表する**)**
If a switch has port security enabled (such as sticky MAC or a configured allowed MAC), the port will only allow the original NIC's MAC address. When a new NIC with a different MAC address is installed, the port rejects traffic, preventing network connectivity.
B). BPDU guard protects against rogue switches, not end hosts.
C). Link aggregation applies when bundling multiple uplinks, not a single PC connection.
D). PoE budget applies to powered devices like APs, not PCs.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Port security, MAC address filtering, switch security features.

質問: **25**
ある企業では最近、顧客向けアプリケーションの一つに障害が発生しました。根本原因はネットワークルーターの過剰利用でしたが、最高技術責任者（CTO）は、顧客からの報告があるまでサポートスタッフがこの問題に気付いていなかったことを懸念しています。今後この問題に対処するための最良の方法は、次のうちどれでしょうか？
A. パケットキャプチャ
B. SNMP
C. Syslogコレクター
D. 見る
正解: **(**正解を表示します**)**

The best answer is SNMP (Simple Network Management Protocol). SNMP enables monitoring of network devices (routers, switches, firewalls, servers) and provides performance data such as CPU usage, bandwidth utilization, and interface status. In this scenario, if SNMP monitoring had been in place, administrators would have received alerts that the router was overutilized before customers noticed outages.
A). Packet capture (e.g., Wireshark) is useful for deep troubleshooting but is reactive, not proactive, and not scalable for continuous monitoring.
C). Syslog collects log messages but generally does not provide proactive resource utilization metrics. It is complementary but not the best fit for this problem.
D). SIEM aggregates logs and security events for analysis, but the primary requirement here is performance and availability monitoring.
By implementing SNMP monitoring (and potentially integrating it with a network monitoring tool such as Nagios, PRTG, or SolarWinds), the organization can track utilization trends, set thresholds, and automatically generate alerts, thereby preventing downtime from going unnoticed.
References (CompTIA Network+ N10-009):
Domain: Network Operations - SNMP monitoring, proactive network performance management.

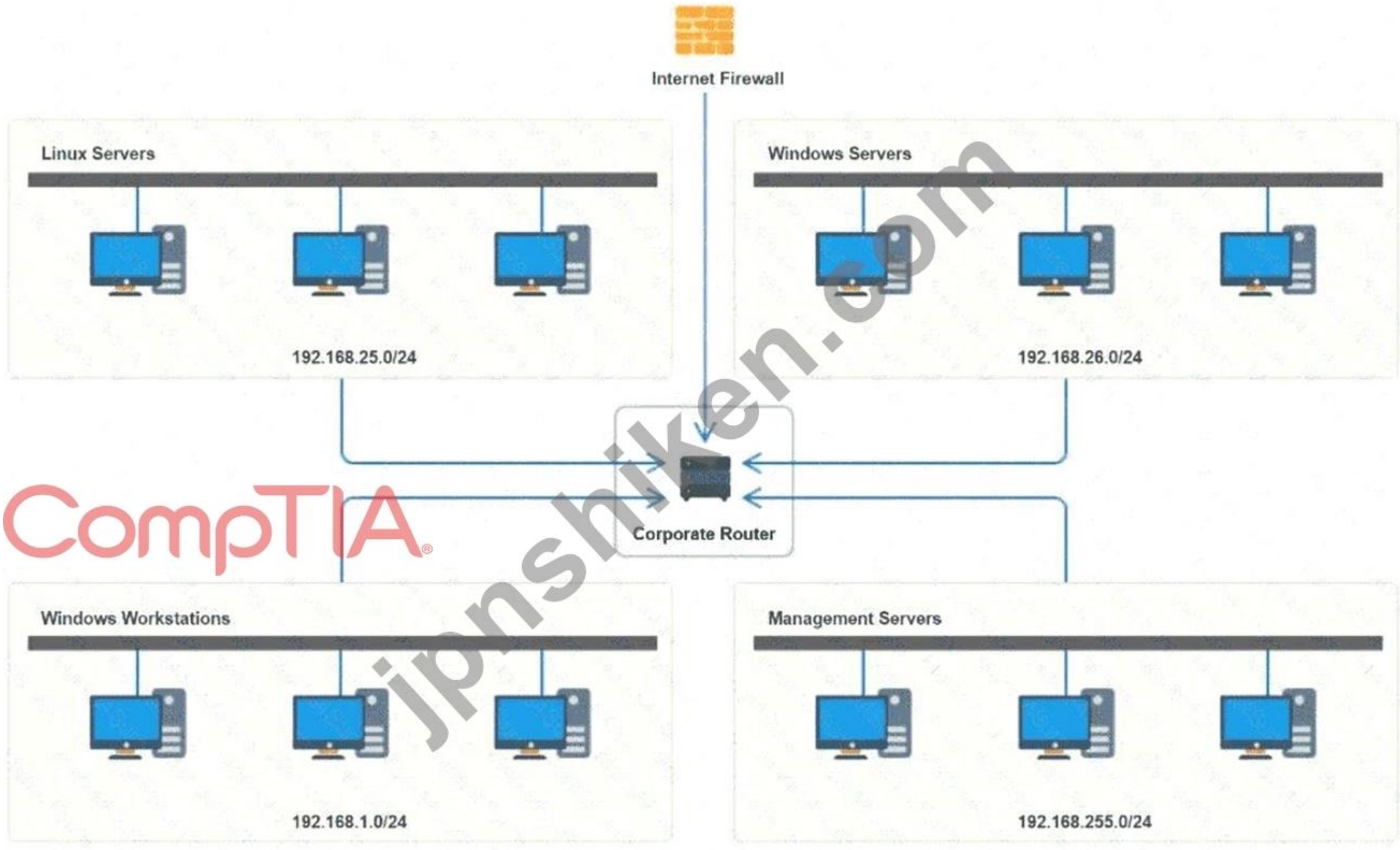
質問: **26**
ネットワーク エンジニアは、同じ市内の 2 つの建物を接続するためのケーブルを注文する必要があります。ネットワーク エンジニアは次のメディア タイプのうちどれを使用する必要がありますか。
A. Coaxial
B. Twinaxial
C. Single-mode fiber
D. Cat 5
正解: **(**正解を表示します**)**
Single-mode fiber is best suited for long-distance communication, often exceeding 10 km (6.2 miles). It's immune to EMI and offers high bandwidth - making it the ideal choice for connecting buildings across a city.
Coaxial (A) and Twinaxial (B) are used for shorter distances and specific use cases (e.g., storage or legacy systems).
Cat 5 (D) is limited to 100 meters and is not suitable for city-level interconnects.
For long-distance, high-speed, and reliable communication between buildings, Single-mode fiber is the professional choice.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 3.4: "Summarize the properties and purposes of physical network topologies and network types."

質問: **27**
次のどれが、単一のクラウド アカウント内でのコンピューティング リソースのセグメント化に最も関連していますか?
A. ネットワーク セキュリティ グループ
B. aaS
C. VPC
D. ハイブリッドクラウド
正解: **(**正解を表示します**)**
Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

質問: **28**
ユーザーがノートパソコンのログイン失敗に関するエスカレーションチケットを送信しました。ユーザーはノートパソコンに表示される時刻が正しくないと主張しています。管理者は、この問題はNTPに関連していると考えています。管理者は次に、以下のどれを行うべきでしょうか？
A. 行動計画を作成する
B. ソリューションを実装する

C. 問題を特定する
D. 理論をテストする
正解: **C (**コメントを発表する**)**
The first step of troubleshooting is always to identify the problem, which includes verifying the symptoms (incorrect time), asking the user clarifying questions, and checking system logs. Only after confirming the problem can the administrator proceed to form a theory and plan.
A). Plan of action is later.
B). Implement solution comes after testing a theory.
D). Test the theory requires a defined problem first.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Troubleshooting methodology (Identify # Theory # Test # Plan # Implement # Verify # Document).

質問**: 29**
ルータに次の ACL を実装することが求められています。
1. 管理ネットワークから他のすべてのローカルネットワークセグメントへの、最も一般的に使用される安全なリモートアクセステクノロジを許可する
2. ユーザー サブネットが、Linux および Windows Server セグメントで最も一般的に使用されるリモート アクセス テクノロジを使用できないことを確認します。
3. 特に許可されていないトラフィックを禁止します。
説明書
ドロップダウンを使用してACLを完了します
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。



CompTIA
jpnshiken.com

正解:

See the answer and solution below.

Explanation:

A screenshot of a computer screen AI-generated content may be incorrect.

Router Access Control List

Rule	Source	Destination	Protocol	Service	Action
1	192.168.255.0	192.168.26.0	TCP	SSH	Allow
2	192.168.255.0	192.168.25.0	TCP	SSH	Allow
3	192.168.255.0	192.168.1.0	TCP	SSH	Allow
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0	Any	TCP	RDP	Deny
7	192.168.1.0	Any	TCP	VNC	Deny
8	192.168.1.0	Any	Any	Any	Allow
9	Any	Any	Any	Any	Deny

lpnshiken.com
CompTIA

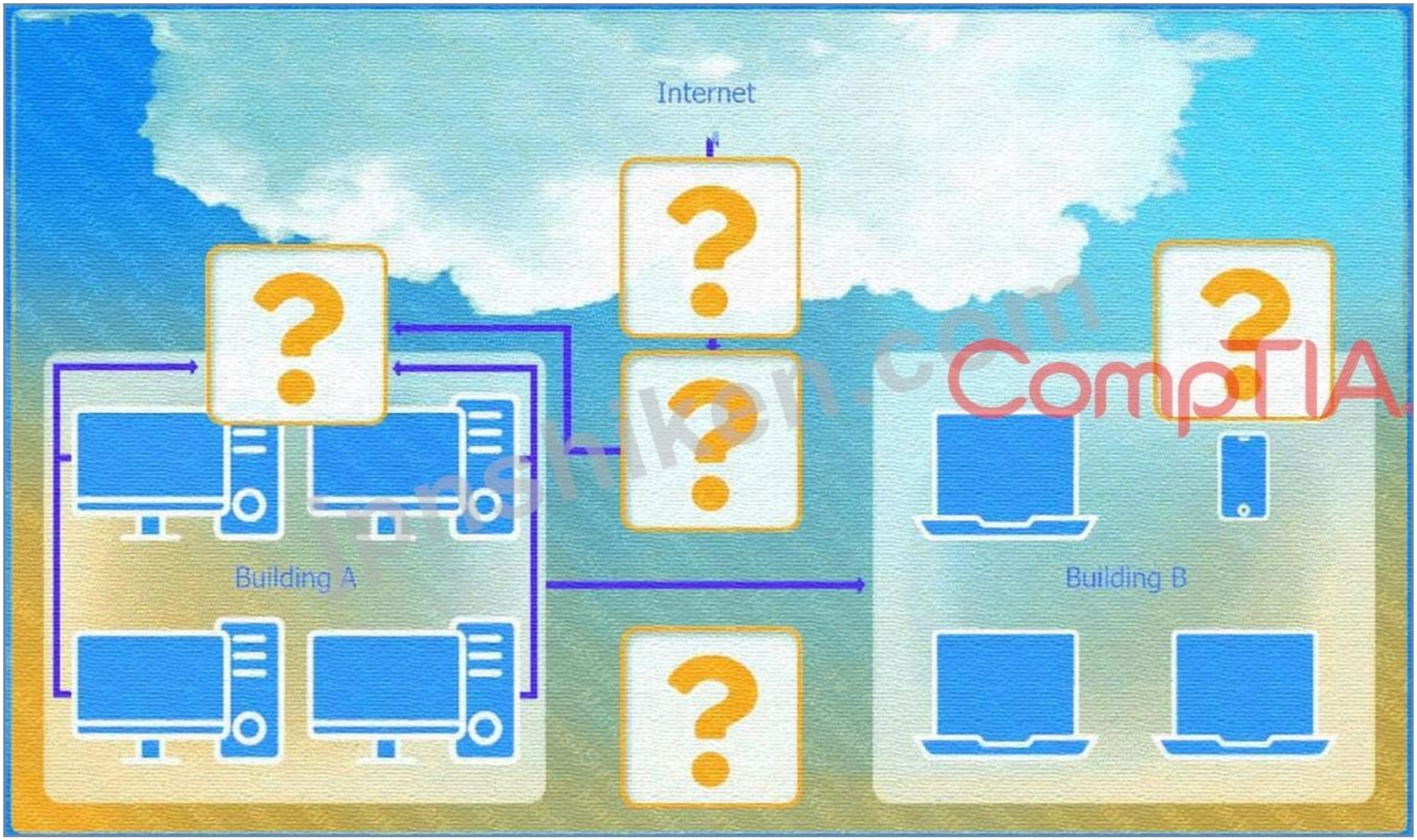
質問: **30**
技術者が、企業サーバーに接続できないユーザーのラップトップのトラブルシューティングを行っています。
技術者は、この問題がルーティングに関連していると考えています。技術者は、問題を特定するために次のコマンドのどれを使用する必要がありますか?
A. tcpdump
B. 掘る
C. トレース
D. アルペジオ
正解: (正解を表示します)
The tracert (Traceroute) command is used to determine the path packets take from the source to the destination. It helps in identifying routing issues by showing each hop the packets pass through, along with the time taken for each hop. This command can pinpoint where the connection is failing or experiencing delays, making it an essential tool for troubleshooting routing issues.References: CompTIA Network+ study materials and common network troubleshooting commands.

質問: **31**
内部サーバーへの攻撃は、隔離されたゲストネットワークに起因することが判明しました。この攻撃を最もよく表すのは次のどれですか？
A. パス上
B. DNSポイズニング
C. VLANホッピング
D. ARPスプーフィング
正解: (正解を表示します)

The correct answer is VLAN hopping, which is a Layer 2 attack specifically associated with bypassing network segmentation controls. According to the CompTIA Network+ N10-009 objectives, VLANs are commonly used to isolate traffic between different network segments, such as separating a guest network from internal production systems. When an attack originates from an isolated guest network and successfully reaches an internal server, it strongly indicates a failure or exploitation of VLAN boundaries.
VLAN hopping occurs when an attacker gains access to traffic on another VLAN by exploiting misconfigured switch ports or trunking protocols. Common techniques include switch spoofing, where the attacker pretends to be a switch to negotiate a trunk link, and double-tagging, where two VLAN tags are inserted to trick switches into forwarding traffic across VLANs.
The other options do not best fit this scenario. An on-path (man-in-the-middle) attack requires interception between two communicating hosts but does not inherently bypass VLAN isolation. DNS poisoning manipulates name resolution, not network segmentation. ARP spoofing affects local Layer 2 address resolution within the same broadcast domain and typically cannot cross VLAN boundaries.
The Network+ objectives emphasize proper VLAN configuration, disabling unused trunk ports, and implementing port security to prevent VLAN hopping attacks. In this case, VLAN hopping most accurately explains how a guest network could access internal servers.

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu **792**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 32
ネットワーク管理者は、新しい企業オフィスのネットワーク構成を任されました。オフィスは2つの建物で構成されており、それぞれ50フィート(約15メートル)離れていますが、物理的な接続はありません。構成は以下の要件を満たす必要があります。
両方の建物のデバイスは
インターネットにアクセスできます。
セキュリティは、すべてのインターネットトラフィックを
入場前に検査を受ける
ネットワーク。
デスクトップではトラフィックは表示されない
他のデバイス向け。
説明書
各拠点に適切なネットワークデバイスを選択してください。該当する場合は、設定の更新が必要なデバイスの横にある虫眼鏡アイコンをクリックし、必要な変更を加えてください。
すべてのデバイスが使用されるわけではありませんが、すべての場所を入力する必要があります。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。


Internet
Building A
Building B

CompTIA

- Hub
- Switch
- WAP
- Firewall
- Router
- Wireless range extender

jpnshiken.com

CompTIA

Wireless range extender settings

Basic Configuration

Access Point Name	WAP extender
Gateway	192.168.0.1
SSID	CORP
SSID Broadcast	Yes No

Wireless

Mode	
Channel	

Wired

Speed	Auto 100 1000
Duplex	Auto Half Full

Security Configuration

Security Settings	None WEP WPA WPA2 WPA2 - Enterprise
Key or Passphrase	N@En71$90*Ha

Reset to Default | Save | Close

jpnshiken.com



jpnshiken.com
CompTIA

正解:

See the step by step complete solution below.

Explanation:

Devices in both buildings should be able to access the Internet.

Security insists that all Internet traffic be inspected before entering the network.

Desktops should not see traffic destined for other devices.

Here is the corrected layout with explanation:

Building A:

Switch: Correctly placed to connect all desktops.

Firewall: Correctly placed to inspect all incoming and outgoing traffic.

Building B:

Switch: Not needed. Instead, place a Wireless Access Point (WAP) to provide wireless connectivity for laptops and mobile devices.

Between Buildings:

Wireless Range Extender: Correctly placed to provide connectivity between the buildings wirelessly.

Connection to the Internet:

Router: Correctly placed to connect to the Internet and route traffic between the buildings and the Internet.

Firewall: The firewall should be placed between the router and the internal network to inspect all traffic before it enters the network.

Corrected Setup:

Top-left (Building A): Switch

Bottom-left (Building A): Firewall (inspect traffic before it enters the network) Top-middle (Internet connection): Router Bottom-middle (between buildings): Wireless Range Extender Top-right (Building B): Wireless Access Point (WAP) In this corrected setup, the WAP in Building B will connect wirelessly to the Wireless Range Extender, which is connected to the Router. The Router is connected to the Firewall to ensure all traffic is inspected before it enters the network.

Configuration for Wireless Range Extender:

SSID: CORP

Security Settings: WPA2 or WPA2 - Enterprise

Key or Passphrase: [Enter a strong passphrase]

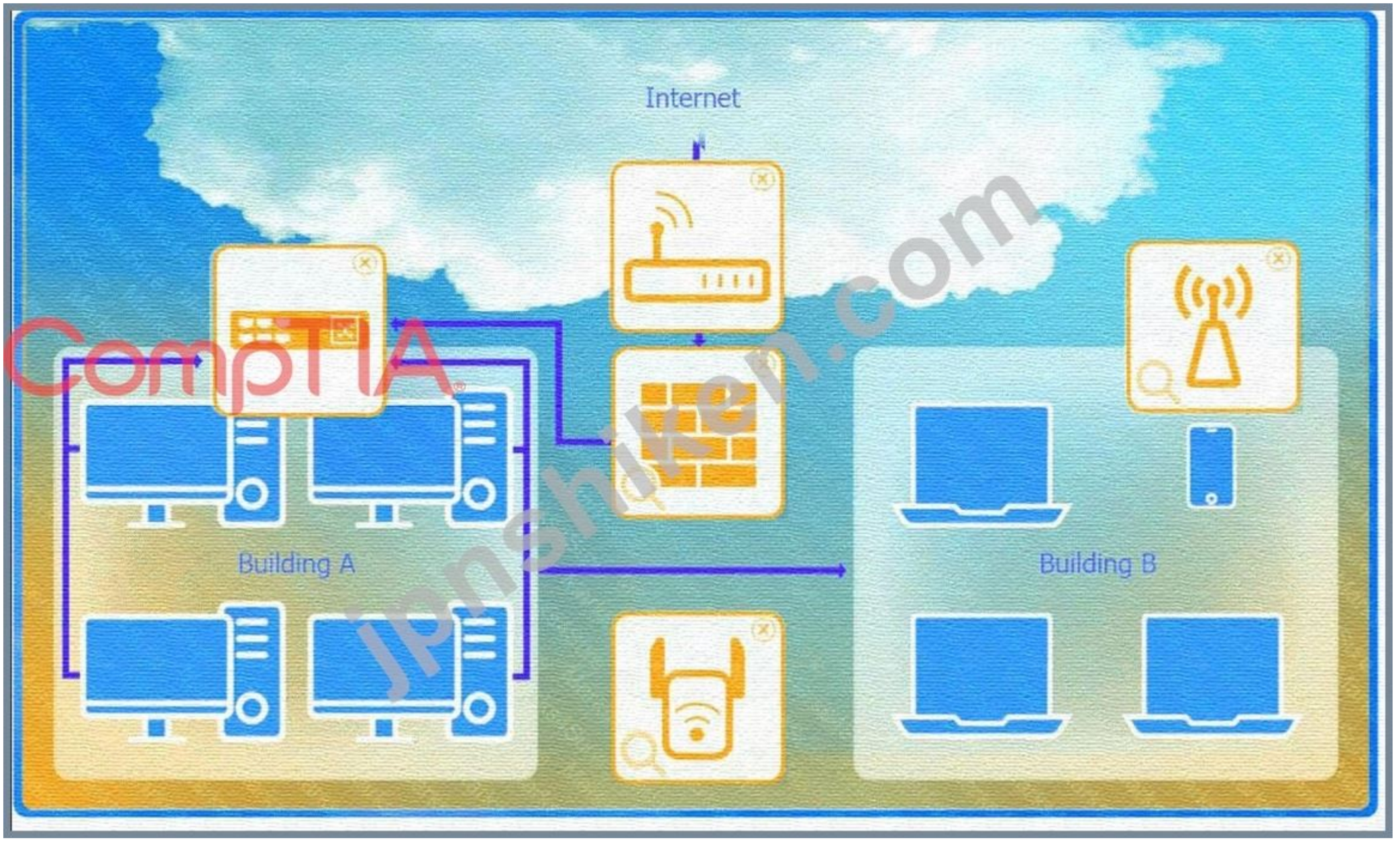
Mode: [Set based on your network plan]

Channel: [Set based on your network plan]

Speed: Auto

Duplex: Auto

With these settings, both buildings will have secure access to the Internet, and all traffic will be inspected by the firewall before entering the network. Desktops and other devices will not see traffic intended for others, maintaining the required security and privacy.



To configure the wireless range extender for security, follow these steps:

SSID (Service Set Identifier):

Ensure the SSID is set to " CORP " as shown in the exhibit.

Security Settings:

WPA2 or WPA2 - Enterprise: Choose one of these options for stronger security. WPA2-Enterprise provides more robust security with centralized authentication, which is ideal for a corporate environment.

Key or Passphrase:

If you select WPA2, enter a strong passphrase in the " Key or Passphrase " field.

If you select WPA2 - Enterprise, you will need to configure additional settings for authentication servers, such as RADIUS, which is not shown in the exhibit.

Wireless Mode and Channel:

Set the appropriate mode and channel based on your network design and the environment to avoid interference. These settings are not specified in the exhibit, so set them according to your network plan.

Wired Speed and Duplex:
Set the speed to " Auto " unless you have specific requirements for 100 or 1000 Mbps.
Set the duplex to " Auto " unless you need to specify half or full duplex based on your network equipment.
Save Configuration:
After making the necessary changes, click the " Save " button to apply the settings.
Here is how the configuration should look after adjustments:
SSID: CORP
Security Settings: WPA2 or WPA2 - Enterprise
Key or Passphrase: [Enter a strong passphrase]
Mode: [Set based on your network plan]
Channel: [Set based on your network plan]
Speed: Auto
Duplex: Auto
Once these settings are configured, your wireless range extender will provide secure connectivity for devices in both buildings.
Firewall setting to to ensure complete compliance with the requirements and best security practices, consider the following adjustments and additions:
DNS Rule: This rule allows DNS traffic from the internal network to any destination, which is fine.
HTTPS Outbound: This rule allows HTTPS traffic from the internal network (assuming 192.169.0.1/24 is a typo and should be 192.168.0.1/24) to any destination, which is also good for secure web browsing.
Management: This rule allows SSH access to the firewall for management purposes, which is necessary for administrative tasks.
HTTPS Inbound: This rule denies inbound HTTPS traffic to the internal network, which is good unless you have a web server that needs to be accessible from the internet.
HTTP Inbound: This rule denies inbound HTTP traffic to the internal network, which is correct for security purposes.
Suggested Additional Settings:
Permit General Outbound Traffic: Allow general outbound traffic for web access, email, etc.
Block All Other Traffic: Ensure that all other traffic is blocked to prevent unauthorized access.
Firewall Configuration Adjustments:
Correct the Network Typo:
Ensure that the subnet 192.169.0.1/24 is corrected to 192.168.0.1/24.
Permit General Outbound Traffic:
Rule Name: General Outbound
Source: 192.168.0.1/24
Destination: ANY
Service: ANY
Action: PERMIT
Deny All Other Traffic:
Rule Name: Block All
Source: ANY
Destination: ANY
Service: ANY
Action: DENY
Here is how your updated firewall settings should look:
Rule Name

Source
Destination
Service
Action
DNS Rule
192.168.0.1/24
ANY
DNS
PERMIT
HTTPS Outbound
192.168.0.1/24
ANY
HTTPS
PERMIT
Management
ANY
192.168.0.1/24
SSH
PERMIT
HTTPS Inbound
ANY
192.168.0.1/24
HTTPS
DENY
HTTP Inbound
ANY
192.168.0.1/24
HTTP
DENY
General Outbound
192.168.0.1/24
ANY
ANY
PERMIT
Block All
ANY
ANY
ANY
DENY
These settings ensure that:
Internal devices can access DNS and HTTPS services externally.

Management access via SSH is permitted.
Inbound HTTP and HTTPS traffic is denied unless otherwise specified.
General outbound traffic is allowed.
All other traffic is blocked by default, ensuring a secure environment.
Make sure to save the settings after making these adjustments.

質問: **33**
新しい無線アクセスポイントを設置した後、エンジニアがデバイスをテストしたところ、定格速度で動作していないことがわかりました。エンジニアは、この問題をトラブルシューティングするために、次のうちどれを行うべきでしょうか？ 2つ選択してください。）
A. ネットワーク上の他のデバイスがボトルネックになっていないことを確認します。
B. デバイスの最新のファームウェアをインストールします。
C. アクセス ポイントの新しい VLAN を作成します。
D. SSID が 16 文字を超えていないことを確認してください。
E. AP を自律モードに設定します。
F. ワイヤレス LAN コントローラーをインストールします。
正解: **(**正解を表示します**)**
Troubleshooting poor performance of a newly installed access point involves multiple steps. Checking for network bottlenecks and ensuring the device firmware is up to date are crucial first steps. The document confirms:"Network bottlenecks can severely limit the performance of even the fastest wireless access points, so it's essential to verify that no other devices are causing a slowdown. In addition, keeping firmware updated ensures optimal performance and security."

質問: **34**
ネットワーク管理者は、プライマリ ルートに障害が発生した場合に備えてバックアップ ルートを設定したいと考えています。ルータには動的ルーティング プロトコルがインストールされていません。管理者はこのタスクを実行するために、次のルーティング機能のどれを選択する必要がありますか。
A. 隣接関係
B. リンクステートフラッディング
C. 管理距離
D. ホップ数
正解: **(**正解を表示します**)**
Introduction to Administrative Distance
Administrative distance (AD) is a value used by routers to rank routes from different routing protocols. AD represents the trustworthiness of the source of the route. Lower AD values are more preferred. If a router has multiple routes to a destination from different sources, it will choose the route with the lowest AD.
Static Routes and Backup Routes
When a dynamic routing protocol is not used, static routes can be employed. Static routes are manually configured routes. To ensure a backup route, multiple static routes to the same destination can be configured with different AD values.
Configuring Static Routes with Administrative Distance
The primary route is configured with a lower AD value, making it the preferred route. The backup route is configured with a higher AD value. In the event of the primary route failure, the router will then use the backup route.
Example Configuration:
plaintext
Copy code

ip route 192.168.1.0 255.255.255.0 10.0.0.1 1
ip route 192.168.1.0 255.255.255.0 10.0.0.2 10
In the above example, 192.168.1.0/24 is the destination network.
10.0.0.1 is the next-hop IP address for the primary route with an AD of 1.
10.0.0.2 is the next-hop IP address for the backup route with an AD of 10.
Verification:
After configuration, use the show ip route command to verify that the primary route is in use and the backup route is listed as a candidate for use if the primary route fails.
References:
CompTIA Network+ guide explains the concept of administrative distance and its use in static routing configuration (see page Ref 9 Basic Configuration Commands).

質問: **35**
DHCPネットワーク上に新しいコンピュータ群を導入する際、ネットワーク管理者は新しいコンピュータがインターネットに接続できないことに気づきました。以下のうち、最も可能性の高い原因はどれでしょうか？
A. デフォルトゲートウェイが正しくありません
B. アドレスプール枯渇
C. 重複するIPアドレス
D. サブネットマスクが正しくありません
正解: **(**正解を表示します**)**
The best answer is B. Address pool exhaustion . The key detail is that this started happening while deploying a new fleet of computers on a DHCP network . That strongly suggests the number of available leases in the DHCP scope has been used up. When no more addresses are available, new devices cannot obtain valid network settings and will fail to connect properly.
This is a common issue when many systems are added at once. Existing devices may already be consuming most or all of the available leases, and the new clients are left without an address assignment. Without a valid IP configuration from DHCP, the computers will not be able to reach the local network or the internet in the normal way.
The other choices are possible network problems in general, but they are less likely in this exact scenario. An incorrect default gateway or incorrect subnet mask would more often reflect a bad DHCP option or a misconfiguration affecting many clients in a different way. A duplicate IP address can affect connectivity, but it does not naturally match the clue about many new devices being added at once on a DHCP scope.
When a question combines DHCP, many new clients, and sudden inability for new systems to connect, address pool exhaustion is the most likely cause.

質問: **36**
ノートパソコンのユーザーが会社のイントラネットサイトにアクセスしようとした際にエラーが発生しました。技術者がipconfig /allを実行したところ、以下の結果が得られました。
自動構成IPv4アドレス :169.254.0.5(推奨)
サブネットマスク . . . . . : 255.255.0.0
デフォルトゲートウェイ . . . . . :
DHCPサーバー . . . . . :
以下のうち、問題の原因として最も可能性が高いのはどれですか？
A. DHCPリース期間が短い
B. IISサーバーの不具合
C. アドレスプール枯渇
D. IDSの設定ミス
正解: **(**正解を表示します**)**

The correct answer is C. Address pool exhaustion . The laptop has assigned itself an address in the 169.254.
x.x range, which is an APIPA address. That happens when the device is configured to use DHCP but cannot successfully obtain an address lease from a DHCP server. The missing default gateway and DHCP server entries support that conclusion.
Among the choices, the most likely reason is that the DHCP scope has run out of available addresses .
When the pool is exhausted, new clients cannot receive a valid IP configuration and fall back to an automatic private address. As a result, the laptop will not be able to reach internal company resources like the intranet because it is not properly configured for the network.
The other answers do not fit the evidence. A short DHCP lease duration may cause more frequent renewals, but it does not directly explain the self-assigned APIPA address. An IIS server malfunction would affect the web service itself, not the client's local IP configuration. An IDS misconfiguration also would not normally result in a 169.254 address on the host.
The output clearly indicates a DHCP assignment failure, and from the options provided, address pool exhaustion is the best match.

質問: **37**
ネットワークエンジニアが新しいPoE対応無線APを設置しています。最初の5台のAPは正常に展開されましたが、6台目が起動に失敗しました。エンジニアが最初に調査すべき項目は次のうちどれですか？
A. 信号強度
B. デュプレックスの不一致
C. 電力予算
D. CRC
正解: **(**正解を表示します**)**
When deploying multiple Power over Ethernet (PoE) devices, the switch's power budget can be exhausted. If the available wattage on the switch cannot supply the additional AP, it will fail to power on. This is the most likely cause when previous APs worked fine but a new one does not.
A). Signal strength affects wireless connectivity, not whether the AP powers up.
B). Duplex mismatch causes poor throughput, not power failure.
D). CRC errors point to cabling issues but do not prevent booting if no power is available.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - PoE power budget considerations, device startup issues.

質問: **38**
IT 部門は、新しく採用された従業員に対し、会社がノートパソコンを提供できるまで個人用のノートパソコンを使用するように求めます。この状況に最も当てはまるポリシーは次のうちどれですか?
A. 今
B. BYOD
C. DLP
D. AUP
正解: **B (**コメントを発表する**)**
BYOD (Bring Your Own Device) policies define rules for using personal devices on the company network.
Since the new employee is using a personal laptop, this policy applies.
Breakdown of Options:
A). IAM (Identity and Access Management) - Governs user permissions, not device policies.
B). BYOD (Bring Your Own Device) - # Correct answer. Covers using personal devices for work.
C). DLP (Data Loss Prevention) - Focuses on preventing sensitive data leaks, not device usage policies.
D). AUP (Acceptable Use Policy) - Covers internet and system usage, but not personal device rules.

Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.6: Explain security policies and best practices.

質問: **39**
ある会社のVoIP電話の接続が途切れ途切れになっています。上級ネットワークエンジニアが音声VLANの導入を推奨しています。設定すべき項目は次のうちどれですか？
A. 802.1Qタグ付け
B. ジャンボフレーム
C. ネイティブVLAN
D. リンクアグリゲーション
正解: **(**正解を表示します**)**
Voice VLANs rely on 802.1Q tagging to separate voice traffic from data traffic on the same physical link.
This separation allows QoS policies to prioritize VoIP, reducing jitter and packet loss.
B). Jumbo frames improve throughput for large data transfers, not voice.
C). Native VLAN is the untagged VLAN, not specifically for voice.
D). Link aggregation bundles links for bandwidth/redundancy, not QoS.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - VLANs, voice VLANs, 802.1Q tagging, QoS.

質問: **40**
ある企業は、短期間のダウンタイムを許容できる災害復旧サイトまたは重要でないアプリケーションを実装したいと考えています。この目標を達成するには、次のどのタイプのサイトを実装する必要がありますか?
A. ホット
B. 寒い
C. 暖かい
D. パッシブ
正解: **(**正解を表示します**)**
A warm site is a compromise between a hot site and a cold site, providing a balance between cost and recovery time. It is partially equipped with the necessary hardware, software, and infrastructure, allowing for a quicker recovery compared to a cold site but at a lower cost than a hot site.
* Recovery Time: Warm sites can be operational within hours to a day, making them suitable for non- critical applications that can tolerate short downtimes.
* Cost-Effectiveness: Warm sites are more economical than hot sites as they do not require all systems to be fully operational at all times.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses disaster recovery strategies and the different types of recovery sites.
* Cisco Networking Academy: Provides training on disaster recovery planning and site selection.
* Network+ Certification All-in-One Exam Guide: Explains the characteristics of hot, warm, and cold sites and their use cases in disaster recovery planning.
Warm sites offer a practical solution for maintaining business continuity for non-critical applications, balancing the need for availability with cost considerations.

質問: **41**
次の攻撃のうち、複数のネットワーク タグを含むネットワーク パケットを利用するものはどれですか。
A. MACフラッディング
B. VLANホッピング

C. DNSスプーフィング
D. ARP ポイズニング
正解: **(**正解を表示します**)**
VLAN hopping is an attack where an attacker crafts packets with multiple VLAN tags, allowing them to traverse VLAN boundaries improperly. This can result in gaining unauthorized access to network segments that are supposed to be isolated. The other options do not involve the use of multiple network tags. MAC flooding aims to overwhelm a switch's MAC address table, DNS spoofing involves forging DNS responses, and ARP poisoning involves sending fake ARP messages.
Reference:
According to the CompTIA Network+ course materials, VLAN hopping exploits the tagging mechanism in network packets to gain unauthorized access.

質問: **42**
ネットワーク技術者は、SSID: business という会社の Wi-Fi ネットワークに新しいユーザーを接続しなければなりません。
接続しようとすると、2つのネットワークが選択肢として表示されます: SSID: ビジネスとSSID:
myaccess。次の攻撃のうちどれが発生していますか？
A. パス上
B. ローグAP
C. 邪悪な双子
D. テールゲーティング
正解: **C (**コメントを発表する**)**
An evil twin attack occurs when an attacker creates a fraudulent AP with an SSID very similar (or identical) to the legitimate one. Users may accidentally connect, allowing the attacker to capture traffic and credentials.
A). On-path is the consequence of connecting to the evil twin, not the initial attack itself.
B). Rogue AP is any unauthorized access point, but the key here is the malicious mimicry of a legitimate SSID
- specifically an evil twin.
D). Tailgating is a physical social engineering attack, unrelated to Wi-Fi.
References (CompTIA Network+ N10-009):
Domain: Network Security - Wireless threats (rogue APs, evil twins).

質問: **43**
ネットワーク管理者は、クライアント デバイスが同じサブネット上で直接通信できないようにすることで、ネットワーク セキュリティを強化したいと考えています。次のテクノロジのうち、どれを実装する必要がありますか。
A. ACL
B. トランキング
C. ポートセキュリティ
D. プライベートVLAN
正解: **D (**コメントを発表する**)**
Private VLANs (PVLANs) are used to segment devices on the same subnet and switch so they cannot communicate with each other, while still accessing a shared resource like a router or gateway. This is often used in shared hosting or DMZ environments.
A). ACLs (Access Control Lists) control traffic between networks, not within the same VLAN.
B). Trunking carries multiple VLANs between switches but does not isolate devices.
C). Port security limits MAC addresses per port but doesn't isolate communication between ports.

Reference:
CompTIA Network+ N10-009 Official Objectives: 3.4 - Compare and contrast access control methods.

質問: **44**
技術者は、デフォルト構成で新しい SD-WAN デバイスを実装しています。技術者は電子メールで URL を受け取り、新しいデバイスをインターネットに接続してインストールを完了します。
これは次のどれの例ですか?
A. SASEデバイスのインストール
B. ゼロタッチプロビジョニング
C. コードとしてのインフラストラクチャ
D. 構成管理
正解: **(**正解を表示します**)**
This process describes Zero-touch provisioning (ZTP), where a device automatically pulls its configuration from a cloud controller or URL once connected to the internet. It's common in SD-WAN and modern network appliances.
A: SASE (Secure Access Service Edge) refers to cloud-delivered network security, not a provisioning method.
C: Infrastructure as code automates infrastructure deployment using code, but this scenario specifically fits ZTP.
D: Configuration management tracks and maintains system configurations but doesn't describe the installation process.
Reference:
CompTIA Network+ N10-009 Official Objectives: 4.3 - Explain remote access methods and automation.

質問: **45**
ネットワーク管理者は、ユーザーがネットワーク上のリソースにアクセスできないという通知を受け取ります。ネットワーク管理者は、ユーザー 3 というラベルの付いたワークステーションへの物理接続をチェックし、イーサネットが正しく接続されていることを確認します。ただし、コンピューターでもスイッチでも、ネットワーク インターフェイスのインジケータ ライトが点滅しません。次のどれが最も可能性の高い原因ですか。
A. スイッチに失敗しました。
B. デフォルトゲートウェイが間違っています。
C. ポートはシャットダウンされています。
D. VLAN の割り当てが正しくありません。
正解: **(**正解を表示します**)**
When a network interface's indicator lights are not blinking on either the computer or the switch, it suggests a physical layer issue. Here is the detailed reasoning:
Ethernet Properly Connected: The Ethernet cable is correctly connected, eliminating issues related to a loose or faulty cable.
No Indicator Lights: The absence of blinking indicator lights on both the computer and the switch typically points to the port being administratively shut down.
Switch Port Shut Down: In networking, a switch port can be administratively shut down, disabling it from passing any traffic. This state is configured by network administrators and can be verified and changed using the command-line interface (CLI) of the switch.
Command to Check and Enable Port:
bash
Copy code
Switch> enable
Switch# configure terminal
Switch(config)# interface [interface id]

Switch(config-if)# no shutdown
The command no shutdown re-enables the interface if it was previously disabled. This will restore the link and the indicator lights should start blinking, showing activity.
Basic Configuration Commands PDF, sections on interface configuration (e.g., shutdown, no shutdown).

質問: **46**
ネットワークエンジニアが、224.7.8.99宛てのトラフィックを確認しました。このトラフィックの種類を最も適切に表しているのは次のうちどれですか？
A. 放送
B. ユニキャスト
C. マルチキャスト
D. エニーキャスト
正解: **(**正解を表示します**)**
The answer is C. Multicast . The address 224.7.8.99 falls within the IPv4 Class D range, which is 224.0.0.0 through 239.255.255.255 . That range is reserved for multicast traffic.
Multicast is used when one sender needs to deliver traffic to a specific group of receivers rather than to every device on the network or to just one destination.
That is what separates it from the other choices. Broadcast is intended for all hosts on the local broadcast domain. Unicast is one-to-one communication, where a single source sends traffic to one specific destination.
Anycast is typically associated with sending traffic to the nearest or best member of a group that shares the same address, not to a multicast group address in the 224.0.0.0/4 range.
From a Network+ point of view, this is a basic address-recognition question. Once you recognize that the destination begins with 224 , the answer should immediately point to multicast. Protocols and streaming applications often use multicast when they need efficient delivery to multiple interested hosts without flooding every device. So in this case, the traffic type is clearly multicast .

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu **792**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
サイト間接続を提供する最も安全な方法はどれですか?
A. VXLAN
B. IKE
C. GRE
D. IPsec
正解: **(**正解を表示します**)**
IPsec (Internet Protocol Security) is the most secure way to provide site-to-site connectivity. It provides robust security services, such as data integrity, authentication, and encryption, ensuring that data sent across the network is protected from interception and tampering. Unlike other options, IPsec operates at the network layer and can secure all traffic that crosses the IP network, making it the most comprehensive and secure choice for site-to-site VPNs.References: CompTIA Network+ study materials and NIST Special Publication 800-77.

質問: **48**
管理者が、Webサーバーとデータベースサーバー間のレイヤー3通信の問題をトラブルシューティングしています。管理者は以下の情報を発見しました。
デバイス

IP
サブネット
ゲートウェイ
ファイアウォール
192.168.1.1
255.255.255.0
1.2.3.4
ウェブサーバー
192.168.1.50
255.255.255.0
192.168.1.1
データベースサーバー
192.168.1.201
255.255.255.128
192.168.1.1
次のうち、コミュニケーションの問題を解決するものはどれですか？
A. データベースサーバーのサブネットを255.255.255.0に変更します
B. ファイアウォールのサブネットを 255.255.255.128 に変更します
C. データベースサーバーのデフォルトゲートウェイを1.2.3.4に変更します
D. データベースサーバーのIPアドレスを192.168.1.150に変更します
E. ファイアウォールのゲートウェイを192.168.1.1に変更します
正解: (正解を表示します)
The problem is a subnet mismatch . The web server is using 255.255.255.0 , which places it in the 192.168.1.0/24 network. The database server is using 255.255.255.128 , which places 192.168.1.201 in the 192.168.1.128/25 network. So even though both addresses begin with 192.168.1, the two systems are not treating the network boundaries the same way.
That creates a Layer 3 communication issue because one host may believe the other device is local while the other host may treat traffic differently based on its smaller subnet. In a normal server segment like this, both systems should agree on the same mask if they are intended to be on the same network.
Changing the database server's subnet mask to 255.255.255.0 fixes that inconsistency immediately. Then both servers and the firewall interface are using the same local network definition, and traffic can be handled properly.
The other options do not solve the real issue. Changing the firewall to /25 would break consistency for the rest of the segment. Pointing the database server to 1.2.3.4 is incorrect because that is outside the local subnet and appears to be an upstream route. Changing the IP to 192.168.1.150 still leaves the wrong mask in place. The clean fix is A .

質問: **49**
ネットワーク管理者は、有線デバイスと無線デバイスの両方にアクセスするときに、ユーザーがポートベースの認証フレームワークを使用して企業ネットワークに認証できるようにしたいと考えています。このタスクを実行するのに最適なセキュリティ機能はどれですか。
A. 802.1X
B. アクセス制御リスト
C. ポートセキュリティ
D. MACフィルタリング
正解: (正解を表示します)

802.1X is a port-based network access control (PNAC) protocol that provides an authentication mechanism to devices wishing to connect to a LAN or WLAN. It is widely used for secure network access, ensuring that only authenticated devices can access the network, whether they are connecting via wired or wireless means.
802.1X works in conjunction with an authentication server, such as RADIUS, to validate the credentials of devices trying to connect.References: CompTIA Network+ study materials.

質問: **50**
ネットワークエンジニアは、リモートオフィスにアクセスポイントを設置し、無線LANコントローラに通信を返さないようにする必要があります。このタスクを実行するために、エンジニアは次のどの設置方法を使用する必要がありますか？
A. 軽量
B. 自律型
C. メッシュ
D. アドホック
正解: **(**正解を表示します**)**
Autonomous access points operate independently without needing to communicate with a central wireless LAN controller. This is ideal for remote deployments.
From Andrew Ramdayal's guide:
"Autonomous access points are stand-alone devices that manage their own configurations and operations.
They do not require a WLC and are ideal for small or remote office deployments."

質問: **51**
開発者は、ランタイム環境、開発ツール、データベースを必要とするモバイルアプリケーションを開発したいと考えています。開発者はセキュリティパッチやアップデートの責任を負いません。これらの要件を満たすモデルは次のうちどれですか？
A. サービスとしてのコンテナ
B. サービスとしてのインフラストラクチャ
C. サービスとしてのプラットフォーム
D. サービスとしてのソフトウェア
正解: **C (**コメントを発表する**)**
The correct answer is Platform as a Service (PaaS). PaaS provides developers with a ready-to-use platform that includes runtime environments, developer tools, middleware, and database services. Developers can focus on writing code while the provider handles security patches, updates, and infrastructure management.
A). CaaS (Containers as a Service) focuses on deploying and managing containerized applications, not providing full developer platforms.
B). IaaS delivers virtual machines, storage, and networking, but administrators must install and maintain the OS, middleware, and updates.
D). SaaS provides end-user applications (e.g., email, CRM), not platforms for development.
By using PaaS, the developers can build applications quickly and cost-effectively without worrying about underlying infrastructure or system maintenance.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Cloud service models (IaaS, PaaS, SaaS, CaaS).

質問: **52**
オフィス内のすべての従業員間で単一の IP アドレスを共有するために、企業が実装する必要があるのは次のうちどれですか。
A. STP
B. BGP
C. PAT
D. VXLAN

正解: **C** (コメントを発表する)
PAT (Port Address Translation) allows multiple devices on a local network to share a single public IP address when accessing the internet. It translates the private IP addresses to a single public IP with different port numbers for each session. The document states:
"PAT (Port Address Translation) allows multiple devices on a LAN to share a single public IP address by assigning unique port numbers to each session, enabling internet connectivity for all devices."

質問: **53**
次の攻撃のうち、企業の Web サイトにアクセスしようとしているユーザーをまったく別の Web サイトに誘導する可能性のあるものはどれですか。
A. DNS ポイズニング
B. サービス拒否
C. ソーシャルエンジニアリング
D. ARPスプーフィング
正解: (正解を表示します)
Network segmentation involves dividing a network into smaller segments or subnets. This is particularly important when integrating OT (Operational Technology) devices to ensure that these devices are isolated from other parts of the network. Segmentation helps protect the OT devices from potential threats and minimizes the impact of any security incidents. It also helps manage traffic and improves overall network performance.References: CompTIA Network+ study materials.

質問: **54**
ネットワークラックには、デュアル電源を備えたサーバー4台とスイッチ4台が設置されています。ラックにはインテリジェントPDUが1台だけ設置されています。2台目のPDUを追加する理由は次のうちどれですか？
A. 電源冗長性
B. PSU監視に失敗しました
C. サージ保護
D. 電力節約
正解: (正解を表示します)
The correct answer is Power redundancy because the devices in the rack are equipped with dual power supplies, which are specifically designed to support redundant power sources. According to CompTIA Network+ (N10-009) objectives under high availability and physical infrastructure concepts, redundancy is a key strategy to eliminate single points of failure.
If only one PDU (Power Distribution Unit) is installed, both power supplies from each device may ultimately rely on the same power source. This creates a single point of failure-if the PDU fails or loses upstream power, all connected equipment will shut down despite having dual power supplies.
By installing a second PDU connected to a separate power circuit (and ideally a separate UPS or power feed), each power supply in the servers and switches can connect to different PDUs. If one PDU fails, the other continues delivering power, ensuring uninterrupted operation.
Option B (Failed PSU monitoring) is not the primary reason for adding another PDU. Option C (Surge protection) can be provided by a single PDU. Option D (Electricity conservation) is unrelated to redundancy design.
Therefore, adding a second PDU provides true power redundancy.

質問: **55**
データ センターで火災が発生した後、ケーブルが交換されました。その後すぐに、管理者はネットワークの問題に気付きました。ネットワークの問題の原因として最も可能性が高いのは次のうちどれですか (2 つ選択してください)。
A. スイッチの電圧が正しくありません。
B. 火災後、HVAC システムが完全に機能していることは確認されませんでした。

C. 機器がオンラインに戻る前に VLAN データベースが削除されませんでした。
D. RJ45 ケーブルがシールドなしケーブルに交換されました。
E. 新しい終端に間違ったトランシーバー タイプが使用されました。
F. 新しい RJ45 ケーブルは、古いものよりも上位のカテゴリです。
正解: **(**正解を表示します**)**
* Unshielded cables (D) are more prone to interference and may not be suitable for certain environments, especially after a fire where interference could be heightened.
* Using the wrong transceiver (E) for new terminations can lead to compatibility issues, causing network failures.

質問: **56**
UDP を使用しているときに、転送中にパケットが失われた場合に何が起こるかを説明しているのは次のうちどれですか。
A. データリンク層はエラーを認識し、パケットを再送信します。
B. IP は TTL フィールドを使用してパケット ホップを追跡し、必要に応じてパケットを再送信します。
C. 送信者が UDP 確認応答を受信しない場合、パケットは再送信されます。
D. 一部のアプリケーションは損失を認識し、必要に応じてパケットの再送信を開始します。
正解: **(**正解を表示します**)**
UDP (User Datagram Protocol) is a connectionless protocol that does not provide built-in mechanisms for error detection, retransmission, or acknowledgments. If a UDP packet is lost in transit, the protocol itself does not handle retransmission. However, some applications using UDP (e.g., TFTP or custom streaming protocols) may implement their own mechanisms to detect packet loss and request retransmission if needed.
Why not A? The data link layer (Layer 2) handles frame-level errors within a single network segment, not end- to-end packet loss across networks.
Why not B? The IP TTL (Time to Live) field prevents routing loops by decrementing with each hop, but IP does not handle retransmission.
Why not C? UDP does not use acknowledgments, so the sender does not expect or receive them.
Reference:CompTIA Network+ N10-009 Objective 1.4: Explain the characteristics of network topologies and protocols. The CompTIA Network+ Study Guide (e.g., Chapter 4: Network Protocols) explains that UDP is a
"fire-and-forget" protocol, and any retransmission logic must be handled by the application layer.

質問: **57**
ある医療クリニックでは、最近、既存のルーターにゲスト用のワイヤレス ネットワークを設定しました。それ以来、ゲストがスピーカー システムの音楽を変更しています。不正アクセスを防ぐために、クリニックが実行すべきアクションは次のうちどれですか (2 つ選択)。
A. スマート デバイスを独自のネットワーク セグメントに分離します。
B. ゲストによる変更を防ぐために IPS を構成します。
C. ネットワークに新しい AP をインストールします。
D. 誰が変更を行ったかを記録する syslog サーバーを設定します。
E. デフォルトの資格情報を変更します。
F. ワイヤレス ルーターで GRE を設定します。
正解: **(**正解を表示します**)**
*A: Isolate smart devices to their own network segment: Network segmentation using VLANs or separate SSIDs ensures that smart devices (like speakers) are not on the same network as guests, preventing unauthorized control.
*E: Change the default credentials: Many IoT devices (e.g., smart speakers) come with default usernames and passwords. If these are not changed, unauthorized users can easily take control.
*Why not the other options?

*B: Configure IPS: IPS (Intrusion Prevention System) detects threats but cannot block specific guest actions on an IoT device.
*C: Install a new AP: A new access point does not solve the unauthorized control issue.
*D: Set up a syslog server: Helps with logging, but does not prevent unauthorized access.
*F: Configure GRE: Generic Routing Encapsulation (GRE) is used for VPN tunneling, which is irrelevant in this case.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 11: Network Security

質問: **58**
次のアプライアンスのうち、指定された WLAN 内の複数のデバイスからの接続を可能にする拡張フットプリントをユーザーに提供するものはどれですか?
A. ルーター
B. スイッチ
C. アクセスポイント
D. ファイアウォール
正解: **(**正解を表示します**)**
An access point (AP) provides users with an extended footprint that allows connections from multiple devices within a designated Wireless Local Area Network (WLAN).
* Router: Typically used to connect different networks, not specifically for extending wireless coverage.
* Switch: Used to connect devices within a wired network, not for providing wireless access.
* Access Point (AP): Extends wireless network coverage, allowing multiple wireless devices to connect to the network.
* Firewall: Primarily used for network security, controlling incoming and outgoing traffic based on security rules, not for providing wireless connectivity.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Explains the roles and functions of network appliances, including access points.
* Cisco Networking Academy: Provides training on deploying and managing wireless networks with access points.
* Network+ Certification All-in-One Exam Guide: Covers network devices and their roles in creating and managing networks.

質問: **59**
ネットワーク管理者は、ネットワークに新しく追加されたワークステーションからリモートサーバーへのpingが実行できません。ワークステーションの127.0.0.1へのpingが失敗しています。管理者は、問題を診断するために、以下のどれを実行する必要がありますか？
A. NIC インターフェースのステータスを確認します。
B. ネットワークが混雑していないことを確認します。
C. ルータがパケットをドロップしていないことを確認します。
D. DNS が正しく解決されていることを確認します。
正解: **(**正解を表示します**)**
The failure of a ping to 127.0.0.1 (the loopback address) indicates a problem with the workstation's TCP/IP stack or network interface card (NIC). Since 127.0.0.1 is a local address, the issue is not related to the network, router, or DNS. The first step in diagnosing this issue is to verify the NIC interface status to ensure the network adapter is functioning and properly configured.
Why not Verify the network is not congested? Network congestion affects external connectivity, not the loopback address.
Why not Verify the router is not dropping packets? Router issues are irrelevant since the loopback ping fails locally.
Why not Verify that DNS is resolving correctly? DNS resolution is not involved in pinging 127.0.0.1, which uses a direct IP address.
Reference:CompTIA Network+ N10-009 Objective 5.2: Explain the troubleshooting methodology. The CompTIA Network+ Study Guide (e.g., Chapter 13: Network Troubleshooting) emphasizes that a failed loopback ping indicates a local TCP/IP stack or NIC issue, and checking the NIC status is the first diagnostic step.

質問: **60**
次のコネクタのうち、スイッチへのコンソール アクセスを提供するものはどれですか?
A. ST
B. RJ45
C. BNC
D. SFP
正解: **(**正解を表示します**)**
Console Access:
Purpose: Console access to a switch allows administrators to configure and manage the device directly. This is typically done using a terminal emulator program on a computer.
RJ45 Connector:
Common Use: The RJ45 connector is widely used for Ethernet cables and also for console connections to network devices like switches and routers.
Console Cables: Console cables often have an RJ45 connector on one end (for the switch) and a DB9 serial connector on the other end (for the computer).
Comparison with Other Connectors:
ST (Straight Tip): A fiber optic connector used for networking, not for console access.
BNC (Bayonet Neill-Concelman): A connector used for coaxial cable, typically in older network setups and not for console access.
SFP (Small Form-factor Pluggable): A modular transceiver used for network interfaces, not for console access.
Practical Application:
Connection Process: Connect the RJ45 end of the console cable to the console port of the switch. Connect the DB9 end (or USB via adapter) to the computer. Use a terminal emulator (e.g., PuTTY, Tera Term) to access the switch's command-line interface (CLI).
References:
CompTIA Network+ study materials on network devices and connectors.

質問: **61**
ネットワーク インフラストラクチャ デバイスのインタラクティブで安全なリモート管理を可能にするのは次のどれですか。
A. SSH
B. VNC
C. RDP
D. SNMP
正解: **(**正解を表示します**)**
SSH (Secure Shell) is a cryptographic network protocol that enables secure remote management and operation of network devices, including routers and switches. SSH encrypts traffic, making it more secure than alternatives like Telnet, which sends data in plaintext. The document states:
"SSH (Secure Shell) is the recommended protocol for secure, interactive remote management of network devices. It provides a secure channel over an unsecured network by encrypting the traffic between the administrator's workstation and the managed device."

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu **792**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
クライアントが SFTP サーバーにアクセスするときに使用されるネットワーク ポートは次のどれですか?
A. 22
B. 80
C. 443
D. 3389
正解: **(**正解を表示します**)**
SFTP (Secure File Transfer Protocol) operates over port 22, using SSH (Secure Shell) encryption for secure file transfers.
Breakdown of Options:
A: 22 - Correct answer. SFTP runs over SSH (port 22) for secure file transfers.
B: 80 - Used for HTTP, not SFTP.
C: 443 - Used for HTTPS (secure web traffic).
D: 3389 - Used for RDP (Remote Desktop Protocol).
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.1: Compare and contrast network protocols.
RFC 4253: SSH Transport Layer Protocol

質問: **63**
一部の従業員から、セッションが頻繁に切断される、バッファリングが繰り返される、パフォーマンスが低下するなどの問題が報告されています。以下の情報に基づいて、
* 従業員は複数のテナントが入居するオフィスビルに勤務しています。
* Wi-Fiは2.4GHz帯を使用します。
* ユーザーからの無線信号の範囲は-50～-65dBmです。
* WPA2が使用されます。
以下のうち、問題の原因として最も可能性が高いのはどれですか？
A. チャネルの重複
B. ワイヤレスカバレッジが不十分です
C. APアンテナタイプ
D. 暗号化方式が古くなっています
正解: **A (**コメントを発表する**)**
The correct answer is A. Channel overlap . The signal strength numbers given, -50 to -65 dBm , are generally strong enough for normal client connectivity, so this does not point to weak coverage. The bigger clue is that the environment is a multitenant office building and the wireless network is using 2.4 GHz .
That band is well known for congestion and overlapping channels, especially where many nearby businesses or tenants have their own access points.
In the 2.4 GHz range, there are only a few non-overlapping channels commonly used. When many APs operate close together on overlapping channels, clients can experience interference, retransmissions, poor throughput, buffering, and connection instability. Those symptoms fit the scenario very well.
The other options are less convincing. Insufficient wireless coverage does not line up with the reported signal levels. AP antenna type could matter in some designs, but there is nothing in the question pointing to a directional or placement issue. WPA2 is not the cause of the performance symptoms here; while it is older than WPA3, it does not normally create repeated buffering and disconnections in this way.
This is really a wireless interference question, and in a crowded 2.4 GHz building, channel overlap is the most likely reason.

質問: **64**

フルトンネル VPN は次のどれを提供しますか?
A. 帯域幅要件が低い
B. ローカルコンピュータのパスワードをリセットする機能
C. すべてのネットワークトラフィックの企業検査
D. ブロックされたサイトへのアクセス
正解: (正解を表示します)
A full-tunnel VPN routes all of a user's network traffic through the corporate network. This means that the organization can inspect all network traffic for security and compliance purposes, as all data is tunneled through the VPN, allowing for comprehensive monitoring and inspection.References: CompTIA Network+ study materials.

質問: **65**
ネットワーク技術者が、Web アプリケーションのパフォーマンス低下のトラブルシューティングを行っています。オフィスには、トラフィック負荷を共有する 2 つのインターネットリンクがあります。技術者は、Web アプリケーションに使用されているリンクを判断するために、次のどのツールを使用する必要がありますか。
A. ネットスタット
B. nslookup
C. ピン
D. トレース
正解: (正解を表示します)
* Understanding Tracert:
* Traceroute Tool: tracert (Windows) or traceroute (Linux) is a network diagnostic tool used to trace the path that packets take from a source to a destination. It lists all the intermediate routers the packets traverse.
* Determining Traffic Path:
* Path Identification: By running tracert to the web application's destination IP address, the technician can identify which route the traffic is taking and thereby determine which internet link is being used.
* Load Balancing Insight: If the office uses load balancing for its internet links, tracert can help verify which link is currently handling the traffic for the web application.
* Comparison with Other Tools:
* netstat: Displays network connections, routing tables, interface statistics, and more, but does not trace the path of packets.
* nslookup: Used for querying DNS to obtain domain name or IP address mapping, not for tracing packet routes.
* ping: Tests connectivity and measures round-trip time but does not provide path information.
* Implementation:
* Open a command prompt or terminal.
* Execute tracert [destination IP] to trace the route.
* Analyze the output to determine the path and the link being used.
References:
* CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

質問: **66**
機器を設置するときに、設置者は左舷側の排気口を次のどの方向に向ける必要がありますか?
A. パッチパネル
B. イスラエル国防軍の前線
C. 暖かい通路

D. 管理コンソール
正解: **(**正解を表示します**)**
In data centers, hot aisle/cold aisle configurations are used to manage airflow and cooling efficiency. Port-side exhausts should be oriented towards the warm aisle to expel hot air and maintain optimal cooling. The document clarifies:
"Equipment with port-side exhausts should be oriented towards the warm aisle to ensure that hot air is properly directed away from the cold air intake areas. This alignment supports effective cooling in data center environments."

質問: **67**
ある企業が、ビデオ監視録画で、権限のない人物が自社の安全な施設に不正なアクセス ポイントを設置したことを発見しました。権限のない人物がこれを行うことを許可したのは、次のどれですか。
A. 邪悪な双子
B. ハニートラップ
C. ウォードライビング
D. テールゲーティング
正解: **D (**コメントを発表する**)**
Tailgating is a physical security breach where someone follows an authorized person into a restricted area without proper credentials. Once inside, the attacker can install rogue devices like unauthorized APs.
A: Evil twin is a wireless attack where an attacker sets up a fake AP.
B: Honeytrap is used to attract attackers for analysis.
C: Wardriving involves scanning for unsecured Wi-Fi networks while driving, not physical intrusion.
Reference:
CompTIA Network+ N10-009 Official Objectives: 4.2 - Identify common security threats and vulnerabilities.

質問: **68**
次のどれがジャンボ フレームをサポートできますか?
A. アクセスポイント
B. ブリッジ
C. ハブ
D. スイッチ
正解: **(**正解を表示します**)**
* Definition of Jumbo Frames:
* Jumbo frames are Ethernet frames with more than 1500 bytes of payload, typically up to 9000 bytes. They are used to improve network performance by reducing the overhead caused by smaller frames.
* Why Switches Support Jumbo Frames:
* Switches are network devices designed to manage data packets and can be configured to support jumbo frames. This capability enhances throughput and efficiency, particularly in high- performance networks and data centers.
* Incompatibility of Other Devices:
* Access Point: Primarily handles wireless communications and does not typically support jumbo frames.
* Bridge: Connects different network segments but usually operates at standard Ethernet frame sizes.
* Hub: A simple network device that transmits packets to all ports without distinguishing between devices, incapable of handling jumbo frames.
* Practical Application:

* Enabling jumbo frames on switches helps in environments where large data transfers are common, such as in storage area networks (SANs) or large-scale virtualized environments.
References:
* CompTIA Network+ course materials and networking hardware documentation.

質問**: 69**
シミュレーション
オフィスに無線ネットワークを構築するという課題があります。ネットワークは3台のアクセスポイントと1台のスイッチで構成されます。ネットワークは以下の要件を満たす必要があります。
SSID は、S3cr3t のキーを使用して CorpNet として設定する必要があります。
無線信号は互いに干渉し合ってはならない
アクセス ポイントとスイッチが接続されているサブネットは、最大 30 台のデバイスのみをサポートする必要があります。アクセス ポイントは、TKIP クライアントを最大速度でのみサポートするように設定する必要があります。手順: ワイヤレス デバイスをクリックしてその情報を確認し、アクセス ポイントの設定を特定の要件に合わせて調整します。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。



CompTIA
ipnshiken.com

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name: AP3

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast: • Yes ○ No

Wireless

Mode:
- B
- G

Channel:
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11

Wired

Speed: ○ Auto • 100 ○ 1000

Duplex: ○ Auto ○ Half • Full

Security Configuration

Security Settings: • None ○ WEP ○ WPA ○ WPA2 ○ WPA2 - Enterprise

Key or Passphrase:

Reset to Default | Save | Close

jpnshiken.com
CompTIA

正解:
See explanation below.
Explanation:
On the first exhibit, the layout should be as follows
A screenshot of a computer AI-generated content may be incorrect.



A screenshot of a computer AI-generated content may be incorrect.



A screenshot of a computer AI-generated content may be incorrect.
A screenshot of a computer AI-generated content may be incorrect.



A screenshot of a computer AI-generated content may be incorrect.

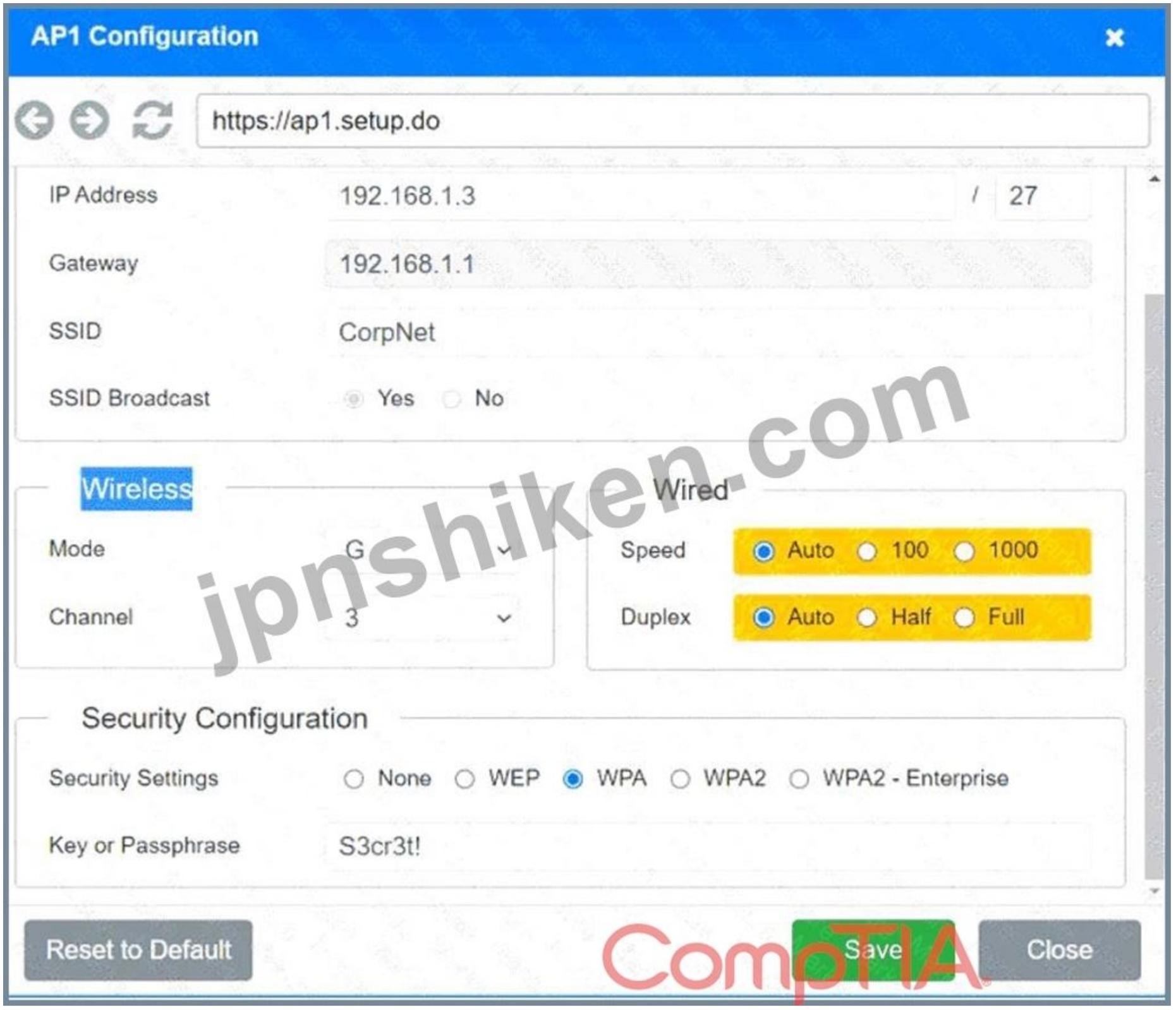
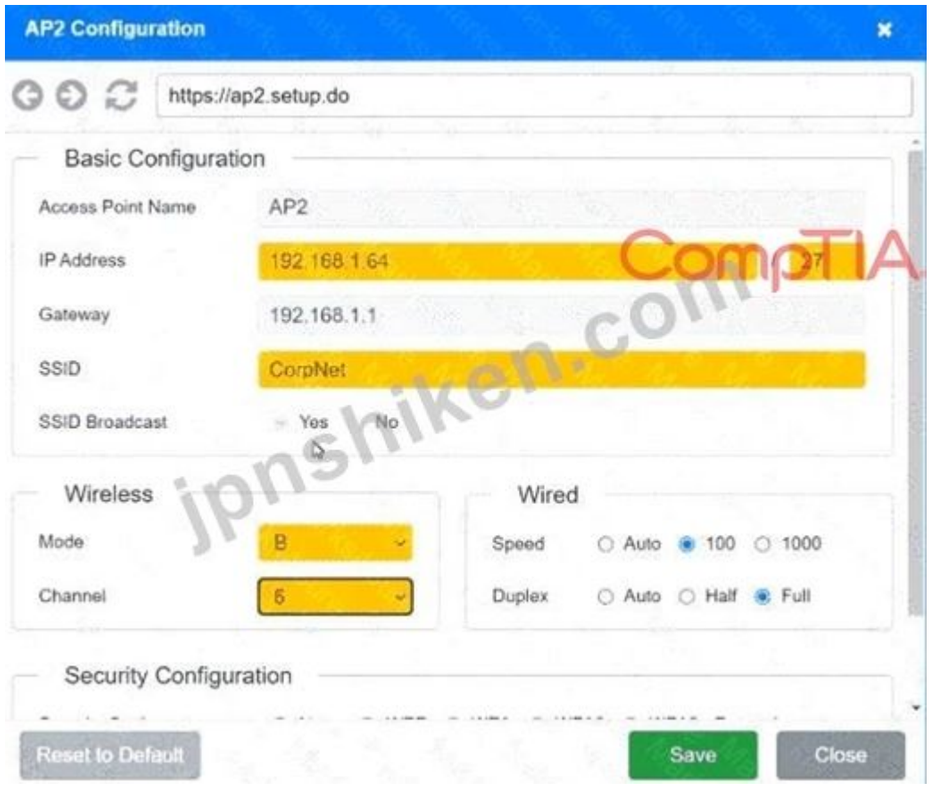


Exhibit 2 as follows

Access Point Name AP2

A screenshot of a computer AI-generated content may be incorrect.



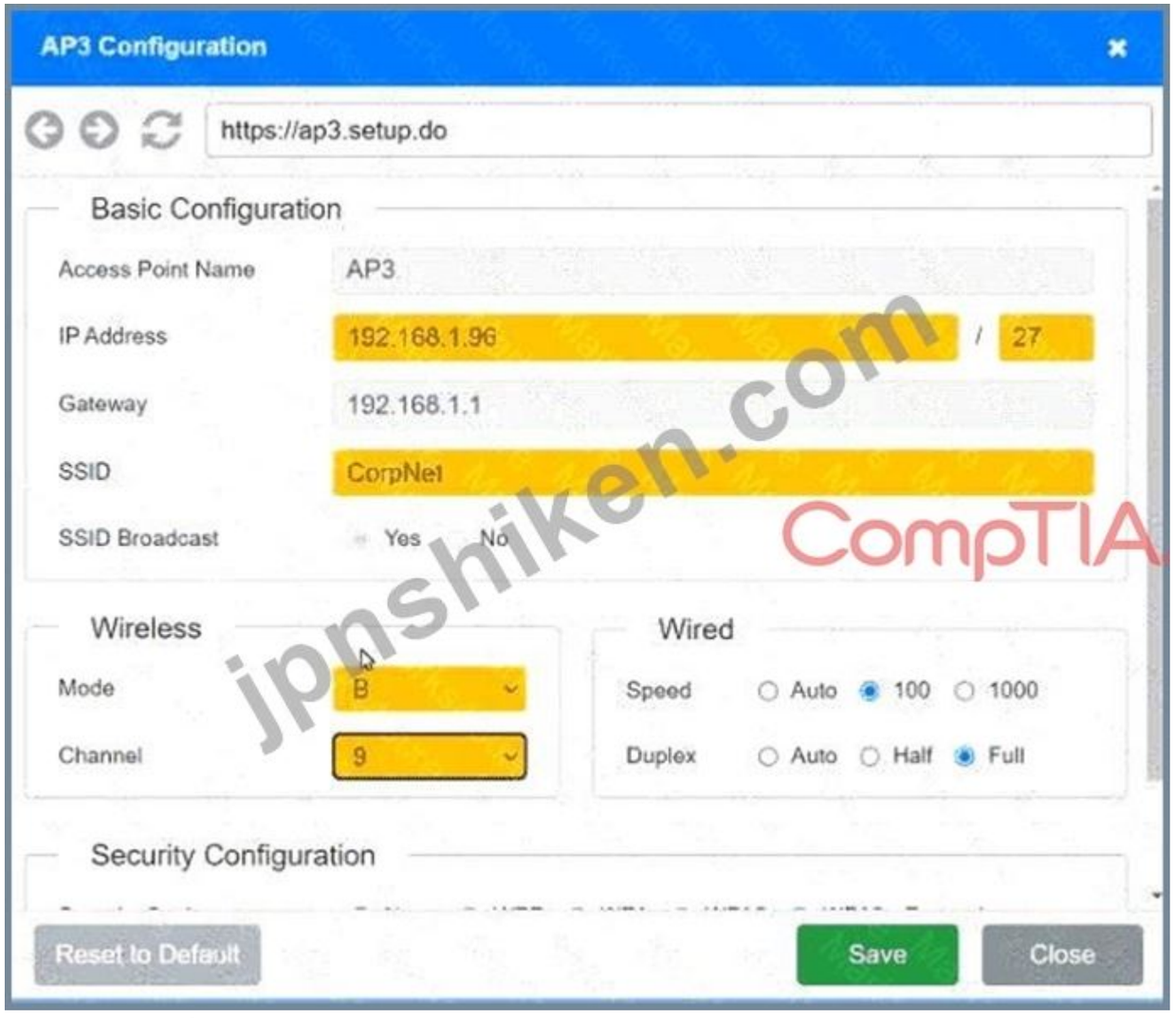
A screenshot of a computer AI-generated content may be incorrect.

A screenshot of a computer AI-generated content may be incorrect.

Exhibit 3 as follows

Access Point Name AP3

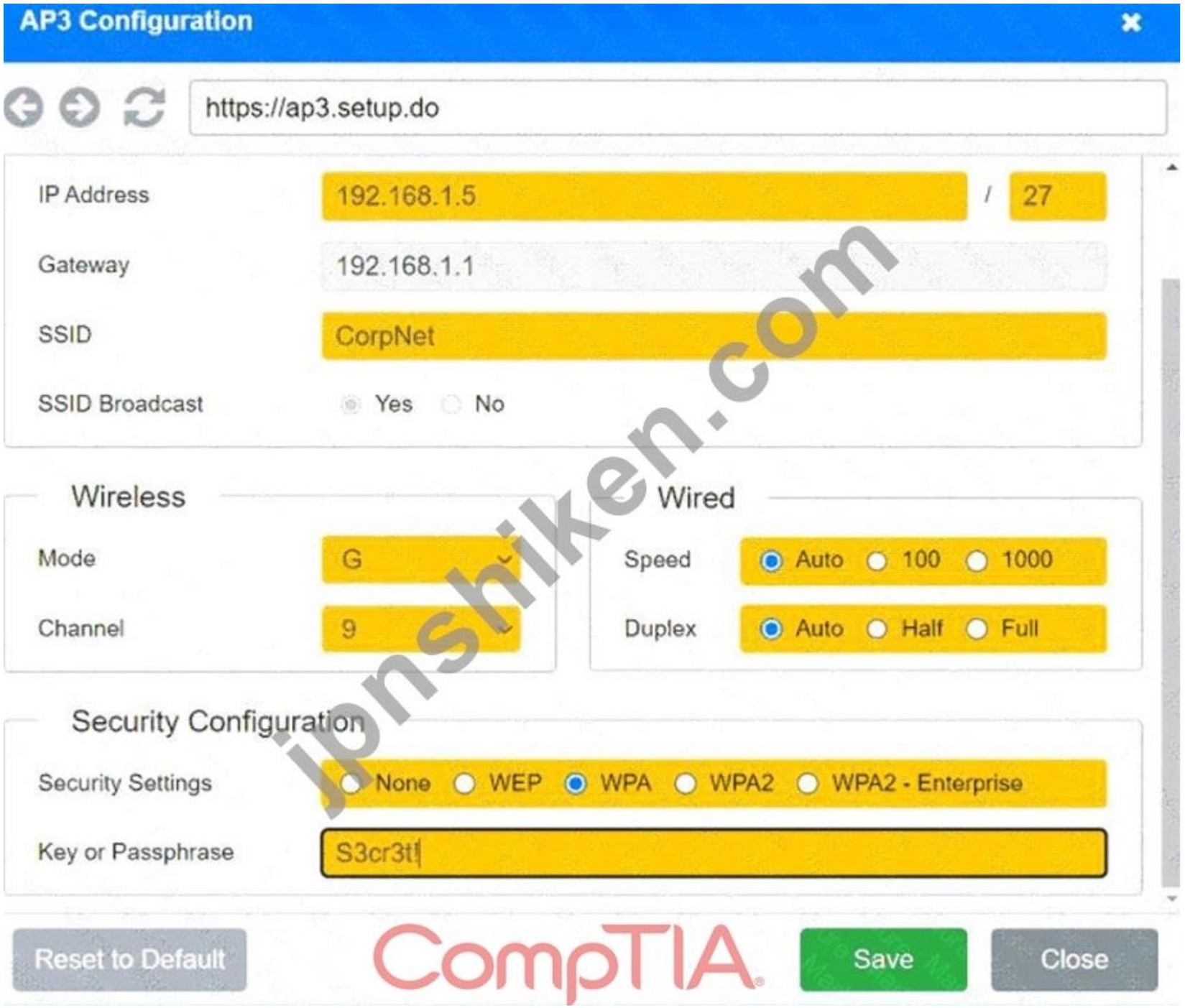
A screenshot of a computer AI-generated content may be incorrect.



A screenshot of a computer AI-generated content may be incorrect.



A screenshot of a computer AI-generated content may be incorrect.



質問: **70**

ある顧客が財務部門とマーケティング部門を分離したいと考えています。ネットワーク管理者は、既存のクラスCネットワークを2つのセクションに分割し、すべてのデバイスのアドレスを適切に再設定することを提案しています。ネットワーク管理者は、次のどのサブネットマスクを使用すべきでしょうか？

A. /24

B. /25

C. /26

D. /27

正解: **(**正解を表示します**)**
The correct answer is /25, which is the appropriate subnet mask for dividing an existing Class C network into two equal subnets. According to the CompTIA Network+ N10-009 objectives, subnetting is a core networking concept used to improve network segmentation, performance, and security.
A Class C network uses a default subnet mask of /24 (255.255.255.0), which provides 256 total addresses (254 usable). To split this network into two sections, the administrator must borrow one host bit from the last octet. Borrowing one bit results in a /25 subnet mask (255.255.255.128). This creates two subnets, each with
128 total addresses (126 usable)-an ideal solution for separating two departments such as finance and marketing.
A /24 would not create any segmentation, as it represents the original single network. A /26 would create four subnets, and a /27 would create eight subnets, both of which exceed the requirement of only two sections and unnecessarily reduce the number of available host addresses per subnet.
The Network+ objectives emphasize selecting subnet masks based on organizational requirements, balancing the number of subnets with sufficient host capacity. In this scenario, /25 is the most efficient and correct choice.

質問: **71**
会社のネットワークでは、ピーク時に大きな遅延とパケット損失が発生しています。ネットワーク監視ツールは、スイッチ上のトラフィックの増加を示しています。ネットワーク技術者がネットワークの輻輳を軽減し、パフォーマンスを向上させるために実装する必要があるのは次のうちどれですか。
A. 負荷分散
B. ポートミラーリング
C. サービス品質
D. スパニングツリープロトコル
正解: **C (**コメントを発表する**)**
Quality of Service (QoS): This is a feature used in networking to prioritize certain types of traffic. By configuring QoS, network administrators can allocate higher bandwidth to time-sensitive applications like VoIP, video conferencing, or critical business applications during peak usage times. This helps to reduce latency and packet loss, which are often caused by congestion.
Load Balancing (A): While load balancing is useful in distributing traffic across multiple servers or paths, it does not address congestion on a single switch.
Port Mirroring (B): This is used for monitoring network traffic for troubleshooting and diagnostics but does not alleviate congestion.
Spanning Tree Protocol (D): STP prevents switching loops in redundant network topologies, but it is not designed to handle traffic prioritization or congestion issues.
Reference: CompTIA Network+ Official Study Guide, Domain 1.5 (Network Optimization), Domain 2.1 (Network Management).

質問: **72**
証券取引所のブローカーのネットワークアーキテクトが、災害復旧（DR）のための高可用性計画を実装しています。以下のアプローチのうち、最も適したものはどれでしょうか？
A. ウォームサイト
B. アクティブアクティブ
C. フルメッシュ
D. インバンド
正解: **(**正解を表示します**)**
The correct answer is Active-active because a stock exchange broker requires extremely high availability, minimal downtime, and near-zero data loss. According to CompTIA Network + (N10-009) objectives under high availability and disaster recovery concepts, an active-active configuration involves multiple systems or sites operating simultaneously and sharing the workload. If one system fails, the other continues processing traffic without service interruption.
This model provides the lowest Recovery Time Objective (RTO) and Recovery Point Objective (RPO), which is critical in financial trading environments where even seconds of downtime can result in major financial loss. Active-active architectures also support load balancing, redundancy, and continuous synchronization between systems.

A warm site (Option A) contains preconfigured hardware but may require data restoration and configuration before becoming fully operational, resulting in some downtime. A full mesh (Option C) is a network topology design and does not specifically address disaster recovery at the service level. In-band (Option D) refers to management traffic sharing the production network and is unrelated to DR strategy.
Therefore, an active-active approach is the most suitable solution for mission-critical financial operations.

質問: **73**
ネットワークエンジニアは、内部ネットワークを公開インターネットから分離 隔離するために境界ネットワークを追加する必要があります。このタスクを達成するのに最適なセキュリティ防御ソリューションは次のどれですか？
A. 信頼ゾーン
B. URLフィルタリング
C. ACL
D. スクリーンドサブネット
正解: **(**正解を表示します**)**
Ascreened subnet, also known as aDMZ (Demilitarized Zone), is aboundary networkthat separates an organization's internal network from external-facing systems. It is used to host public services like web or email servers while protecting internal systems from exposure.
Reference:Section 4.3 - Network Security Features, Defense Techniques, and Solutions - "Screened Subnet (DMZ)"

質問: **74**
ネットワーク管理者は2つのスイッチを接続し、2つの接続リンクを使用します。次の構成のうち、レイヤ2ループを防ぐのはどれですか？
A. 802.1Qタグ付け
B. 全二重
C. リンクアグリゲーション
D. QoS
正解: **(**正解を表示します**)**
Link aggregation (also known as port trunking or EtherChannel) combines multiple network connections in parallel to increase throughput and provide redundancy. When two switches are connected with multiple links without any additional configuration, a Layer 2 loop may occur. Link aggregation prevents these loops by treating the multiple connections as a single logical link, using a protocol such as LACP (Link Aggregation Control Protocol).
From Andrew Ramdayal's guide:
"Link aggregation allows you to combine multiple network connections to increase the bandwidth and provide redundancy. It helps prevent Layer 2 loops when connecting switches with multiple links by making them operate as a single logical interface."

質問: **75**
根本原因理論のテストに成功した後に実行する次のステップはどれですか?
A. 解決手順を決定します。
B. ラボで問題を再現します。
C. 承認のために理論を提示します。
D. 問題に対する解決策を実装します。
正解: **(**正解を表示します**)**
* Troubleshooting Methodology:
* Confirming the Root Cause: After testing and confirming the theory, the next logical step is to address the issue by implementing a solution.

* Implementation of the Solution:
* Resolve the Issue: Implement the identified solution to rectify the problem. This step involves making necessary changes to the network configuration, replacing faulty hardware, or applying software patches.
* Documentation: Document the solution and the steps taken to resolve the issue to provide a reference for future troubleshooting.
* Comparison with Other Steps:
* Determine Resolution Steps: This is part of the implementation process where specific actions are outlined, but the actual next step after testing is to implement those steps.
* Duplicate the Problem in a Lab: This step is typically done earlier in the troubleshooting process to understand the problem, not after confirming the root cause.
* Present the Theory for Approval: In some scenarios, presenting the theory might be necessary for major changes, but generally, once the root cause is confirmed, the solution should be implemented.
* Final Verification:
* After implementing the solution, it is important to verify that the issue is resolved and that normal operations are restored. This may involve monitoring the network and testing to ensure no further issues arise.
References:
* CompTIA Network+ study materials on troubleshooting methodologies and best practices.

質問**: 76**
IT部門は、ネットワークセキュリティを向上させるためにSIEMソリューションの導入を検討しています。同部門は、SIEMシステムが会社のすべてのコアデバイスからのログを取り込んで分析できることを確認したいと考えています。SIEMソリューションを選択する際に最も重要な考慮事項は次のうちどれですか？
A. 管理が簡単
B. コスト
C. 互換性
D. 機能
正解**: C (**コメントを発表する**)**
The correct answer is C. Compatibility . A SIEM is only effective if it can successfully collect, normalize, and analyze data from the systems the organization relies on. Since the question specifically says the department wants the SIEM to ingest and analyze logs from all core devices , the most important factor is whether the SIEM is compatible with those devices, their log formats, and their supported methods of exporting events.
This includes support for common logging methods such as syslog , SNMP traps, API integrations, agent- based collection, and vendor-specific event formats. Even a SIEM with excellent features will not deliver value if it cannot properly receive and interpret logs from firewalls, routers, switches, servers, and security appliances already in use.
The other choices matter, but they come after compatibility. Ease of management is helpful for daily operations. Cost is always a practical concern. Features can improve visibility and automation. However, none of those benefits matter much if the SIEM cannot integrate with the organization's actual environment.
For Network+ exam purposes, when log ingestion across many device types is the requirement, the top selection criterion is compatibility . Without that foundation, correlation, alerting, and security analysis will be incomplete.

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu **792**問、３０%ディスカウント、特別な割引コード**: JPNshiken**」

質問**: 77**
電子メール サービスをホストするための最もコスト効率の高い方法は次のうちどれですか。

A. PaaS
B. IaaS
C. VPC
D. SaaS
正解: **(**正解を表示します**)**
The correct answer is SaaS (Software as a Service). According to the CompTIA Network+ N10-009 objectives, SaaS is the most cost-efficient cloud model for hosting common business applications such as email, collaboration tools, and productivity suites. With SaaS, the cloud provider manages all infrastructure, operating systems, application software, security updates, and maintenance, significantly reducing administrative overhead and operational costs.
Email services are a prime example of workloads that benefit from SaaS solutions such as Microsoft 365 or Google Workspace. Organizations pay a subscription-based fee, typically per user, and avoid expenses related to server hardware, licensing, patching, backups, redundancy, and disaster recovery. This makes SaaS far more economical than deploying and maintaining email servers internally or in lower-level cloud models.
IaaS requires the organization to manage virtual machines, operating systems, email server software, and security configurations, which increases both cost and complexity. PaaS simplifies application development but is not designed for hosting ready-made services like email platforms. A VPC (Virtual Private Cloud) is a networking construct, not a service model, and does not inherently provide email hosting functionality.
The Network+ objectives emphasize selecting cloud service models based on cost, management responsibility, and operational efficiency. For standardized services like email, SaaS offers the lowest total cost of ownership and the least administrative burden, making it the best and most cost-effective choice.

質問: **78**
ピーク時間帯にクラウドベースのアプリケーションに接続する際に、ユーザーが大きな遅延を経験しています。ネットワークを調査したところ、帯域幅が過度に使用されていることがわかりました。さらに分析を進めると、アプリケーションを使用しているユーザーは常時少数であることが分かりました。この問題に対する最も費用対効果の高い解決策はどれでしょうか？
A. アプリケーションにアクセスできるユーザーの数を制限します。
B. クラウド サービス プロバイダーへの Direct Connect 接続をリースします。
C. アプリケーション トラフィックの優先順位を設定するために QoS を実装します。
D. CDN を使用してアプリケーションにサービスを提供します。
正解: **C (**コメントを発表する**)**
Quality of Service (QoS)is the best cost-effective solution. It prioritizes traffic based on application criticality.
If the bandwidth is limited and only a few users are affected, prioritizing that application traffic can improve performance without needing costly bandwidth upgrades or direct connections.
Reference:Section 1.2 - Networking Appliances, Applications, and Functions - "Quality of Service (QoS)"

質問: **79**
ネットワーク管理者は、Telnetプロトコルを使用して、ネットワーク上のネットワークデバイスを管理しています。
192.168.1.0/24 サブネット。デバイスを最も適切に識別するために管理者が使用すべきツールは次のどれですか?
A. dig
B. nmap
C. tracert
D. telnet
正解: **(**正解を表示します**)**

nmap(Network Mapper) is the best tool in this scenario. It can scan the 192.168.1.0/24 subnet to discoverlive hosts, open ports (like Telnet on port 23), and device types. It's ideal for mapping and auditing the network.
* A. digis a DNS lookup tool; not useful for identifying hosts on a subnet.
* C. tracertshows the path packets take to a destination, not for host discovery.
* D. telnetis the protocol being used, not a tool for scanning or identifying devices.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 5.1 - Given a scenario, use the appropriate network troubleshooting tools.

質問: **80**
3 つのアクセス ポイントには、天井を通るイーサネットがあります。アクセス ポイントの 1 つはインターネットに接続できません。次のツールのうちどれが問題を特定するのに役立ちますか?
A. ネットワークタップ
B. ケーブルテスター
C. 視覚的障害ロケーター
D. トナーとプローブ
正解: **(**正解を表示します**)**
A cable tester is a tool that can help identify issues with the physical cabling, such as breaks or improper terminations, which may prevent the access point from reaching the internet.

質問: **81**
あるネットワーク技術者が最近、ある会社に入社しました。マネージャーは技術者にネットワークの文書化を依頼し、以前の文書から部分的な情報を提供しました。
説明書：
各スイッチをクリックし、ターミナルにコマンドを入力してネットワーク検出を実行します。不足している情報は、表示されるドロップダウンメニューを使用して入力してください。



CompTIA.
jpnshiken.com



CompTIA
jpnshiken.com

正解:

See the Explanation for detailed information on this simulation.

Explanation:

(Note: Ips will be change on each simulation task, so we have given example answer for the understanding) To perform a network discovery by entering commands into the terminal, you can use the following steps:

Click on each switch to open its terminal window.

Enter the command show ip interface brief to display the IP addresses and statuses of the switch interfaces.

Enter the command show vlan brief to display the VLAN configurations and assignments of the switch interfaces.

Enter the command show cdp neighbors to display the information about the neighboring devices that are connected to the switch.

Fill in the missing information in the diagram using the drop-down menus provided.

Here is an example of how to fill in the missing information for Core Switch 1:

The IP address of Core Switch 1 is 192.168.1.1.
The VLAN configuration of Core Switch 1 is VLAN 1: 192.168.1.0/24, VLAN 2: 192.168.2.0/24, VLAN 3: 192.168.3.0/24.
The neighboring devices of Core Switch 1 are Access Switch 1 and Access Switch 2.
The interfaces that connect Core Switch 1 to Access Switch 1 are GigabitEthernet0/1 and GigabitEthernet0/2.
The interfaces that connect Core Switch 1 to Access Switch 2 are GigabitEthernet0/3 and GigabitEthernet0/4.
You can use the same steps to fill in the missing information for Access Switch 1 and Access Switch 2.

質問: **82**
ユーザーが会社の資格情報を使用してワイヤレス ネットワークに認証できるようにするには、次のどれを設定する必要がありますか?
A. SSO
B. SAML
C. MFA
D. 半径
正解: **(**正解を表示します**)**
RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. RADIUS is often used to manage access to wireless networks, enabling users to authenticate with their company credentials, ensuring secure access to the network.References: CompTIA Network+ study materials.

質問: **83**
予防措置を講じた後、トラブルシューティング方法論で次に実行する手順はどれですか?
A. ソリューションを実装します。
B. システム機能を検証します。
C. 行動計画を立てます。
D. 原因を特定するために理論をテストします。
正解: **(**正解を表示します**)**
After implementing a solution and putting preventive measures in place, the next step is to verify that the system is functioning correctly. This ensures that the issue has been fully resolved.

質問: **84**
ネットワーク管理者は、ある部門を新しいネットワーク セグメントに接続する必要があります。別のネットワークにある DHCP サーバーを使用する必要があります。管理者がこのタスクを完了するには、次のどれを使用できますか。
A. IP ヘルパー
B. 予約
C. 除外
D. スコープ
正解: **(**正解を表示します**)**
An IP Helper (IP Helper Address) allows DHCP requests to pass through routers and reach a DHCP server on another network.
* DHCP broadcasts are not forwarded across routers by default, so an IP Helper Address is needed to relay the request.
* This is crucial for large networks where a single DHCP server serves multiple subnets.

* Option B (Reservation): Ensures a specific IP address is assigned to a MAC address but does not relay DHCP across networks.
* Option C (Exclusion): Prevents specific IP addresses from being assigned, but does not help with DHCP relay.
* Option D (Scope): Defines the range of IP addresses available for DHCP clients but does not assist in cross-network communication.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: DHCP and IP Addressing

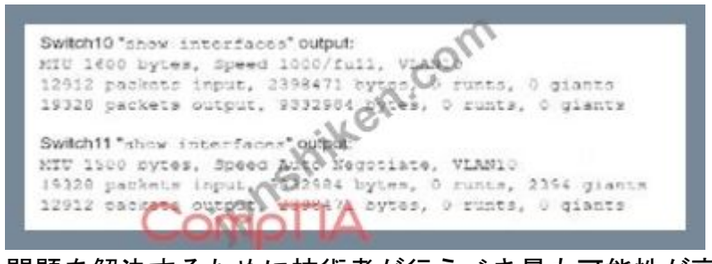
質問: **85**
従業員が誤って顧客のデータを削除した場合、次のどれが違反になりますか?
A. 誠実さ
B. 機密保持
C. 脆弱性
D. 可用性
正解: **D (**コメントを発表する**)**
Availability refers to ensuring that data is accessible when needed. If a customer's data is accidentally deleted, it impacts availability, as the data can no longer be accessed.

質問: **86**
ネットワークエンジニアが新しいブランチネットワークにトンネルを追加します。トンネル内のすべてのデータが暗号化されることを保証するのは次のうちどれですか？
A. ESP
B. SSH
C. GRE
D. IKE
正解: **A (**コメントを発表する**)**
ESP (Encapsulating Security Payload) is an IPsec protocol that provides encryption, integrity, and authentication for data inside a VPN tunnel. It ensures that all tunneled traffic is encrypted.
B). SSH secures remote terminal sessions, not site-to-site VPN tunnels.
C). GRE (Generic Routing Encapsulation) provides encapsulation but does not encrypt data.
D). IKE (Internet Key Exchange) negotiates keys and establishes the IPsec tunnel but does not encrypt the payload itself.
References (CompTIA Network+ N10-009):
Domain: Network Security - VPN protocols, IPsec (AH vs. ESP), encryption in transit.

質問: **87**
政府機関が国コードに基づいてウェブサイトをブロックできる技術を導入したいと考えています。この要件を満たす最も適切な方法は次のうちどれですか？
A. URLフィルタリング
B. コンテンツフィルタリング
C. DNSポイズニング
D. MACフィルタリング
正解: **(**正解を表示します**)**
URL filtering can block access to websites based on their domain or country code TLDs (e.g., .cn, .ru). This is the correct method to block by location identifiers in URLs.
B). Content filtering blocks based on keywords or categories within websites, not country code.
C). DNS poisoning is an attack, not a control mechanism.
D). MAC filtering restricts devices, not websites.

References (CompTIA Network+ N10-009):
Domain: Network Security - Filtering technologies, URL vs content filtering.

質問: **88**
ネットワーク技術者がネットワーク遅延のトラブルシューティングを行っており、2 つのネットワーク スイッチ (Switch10 と Switch11) で問題が発生していることが判明しました。報告された症状には、ビデオ パフォーマンスの低下とファイルのコピーの遅さが含まれています。次の情報が示されています。



問題を解決するために技術者が行うべき最も可能性が高いのは次のうちどれですか?
A. ポートのネイティブ VLAN を変更します。
B. Switch10のMTU値を1500に変更します。
C. 両方のスイッチで STP を設定します。
D. Switch11 で自動ネゴシエーションを無効にします。
正解: **(**正解を表示します**)**

質問: **89**
新しいバックアップシステムでは、毎晩新しいSANにファイルをコピーするのに時間がかかりすぎます。ネットワーク管理者は、バックアップ時間を短縮するために、ネットワークとデバイスに簡単な変更を加えます。ネットワーク管理者は次のうちどれを変更しますか？
A. QoS
B. SDN
C. MTU
D. VXLAN
E. TTL
正解: **(**正解を表示します**)**
Increasing the MTU (Maximum Transmission Unit) size allows larger frames to be transmitted, reducing overhead and improving throughput - especially for large file transfers like backups.
A). QoS prioritizes traffic but doesn't reduce backup times directly.
B). SDN is a network management model, not a parameter change.
D). VXLAN encapsulates VLANs, not relevant to backup speeds.
E). TTL is for packet lifetime, not throughput.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - MTU, jumbo frames, performance tuning.

質問: **90**
大規模施設のインフラストラクチャに関する資料が不十分なため、LAN上のIPアドレス192.168.50.140のファイルサーバーにアクセスできないという問題が報告されました。pingコマンドの結果は次のとおりです。
ping -c 10 192.168.50.140

パケット: 送信 = 10、受信 = 5、損失 = 5 (50% 損失)
往復時間: 最小 = 3ms、最大 = 144ms、平均 = 42ms
スイッチの問題のトラブルシューティングを最小限の影響で継続するには、技術者は次のどれを実行する必要がありますか?
A. トーニングとプローブを実行します。
B. ケーブルを交換してください。
C. 障害を視覚的に特定します。
D. スイッチを再起動します。
正解: **(**正解を表示します**)**
The ping results show intermittent connectivity (50% packet loss) with highly variable latency, which commonly indicates a Layer 1/Layer 2 problem (e.g., damaged cable pairs, bad patch-panel termination, failing switch port, duplex/negotiation issues, or excessive errors on the interface). Because the facility has incomplete documentation, the technician's first priority at the switch is to positively identify the correct switch port and cable path associated with the file server before making disruptive changes.
Using a tone generator and probe aligns with Network+ troubleshooting objectives that emphasize selecting the appropriate tool and following an efficient, structured process: identify the problem, establish a theory, test, and then implement the least disruptive fix. Toning/probing helps map the server's drop to the switch port (even through patch panels) so the technician can then check that specific interface for errors/discards, CRCs, speed/duplex negotiation status, and link stability-all without rebooting the switch or immediately replacing hardware.
By contrast, restarting the switch is high-impact, and replacing a cable is a change best performed after the correct run/port is confirmed.

質問: **91**
次のどれが BGP を使用する最も適切な理由を表していますか?
A. LAN内のループを防ぐ
B. 再収束時間の改善
C. 別のISPとルーターの更新を交換する
D. レイヤ3スイッチとのルートの共有
正解: **(**正解を表示します**)**
BGP (Border Gateway Protocol) is used for routing data between different ISPs, making it essential for the functioning of the internet. Its primary use is for exchanging routing information between autonomous systems, especially different ISPs. Preventing loops within a LAN is handled by protocols like Spanning Tree Protocol (STP), while improving reconvergence times and sharing routes with a Layer 3 switch are functions of other protocols or internal mechanisms.
Reference:
The CompTIA Network+ training emphasizes BGP's role in the exchange of routing information across different ISPs and autonomous systems.

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu **792**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
ユーザーからネットワークの遅延に関する報告が寄せられています。ネットワークエンジニアは次のように指摘しています。
唯一の変更点は新しいネットワークスイッチであったことが確認された
すべてのユーザーが遅延を経験していることを確認します

問題は、新しいスイッチのブリッジ ID が低いために発生したネットワーク ループであると考えられます。トラブルシューティング方法の次のステップを説明するのは次のうちどれですか。
A. 問題を特定します。
B. 理論をテストします。
C. ソリューションを実装します。
D. システムの全機能を検証します。
正解: **B (**コメントを発表する**)**
The correct answer is Test the theory, which aligns directly with the CompTIA Network+ N10-009 troubleshooting methodology. According to the official troubleshooting steps, once a problem has been identified and relevant information gathered, the next step is to establish a theory of probable cause and then test that theory to determine whether it is valid.
In this scenario, the engineer has already completed the problem identification phase by confirming that all users are experiencing latency and correlating the issue with the installation of a new switch. The engineer has also formed a theory: that a network loop caused by the lower bridge ID of the new switch may be impacting Spanning Tree Protocol (STP), resulting in congestion and latency. Because this theory has already been developed, the next logical and required step is to test the theory-for example, by reviewing STP states, temporarily disabling ports, or adjusting bridge priorities.
Implementing a solution would be premature without validating the theory, and verifying full system functionality occurs only after a fix has been applied. The Network+ objectives stress following a structured methodology to avoid unnecessary changes and minimize network disruption. Testing the theory ensures accuracy before corrective action is taken, reducing risk and downtime.

質問: **93**
ルータが 1 台しかない環境で、ネットワーク エンジニアが追加のハードウェアを購入せずに VLAN 間で通信できるようにするには、次のどれを使用しますか。
A. サブインターフェース
B. VXLAN
C. レイヤー3スイッチ
D. 仮想
正解: **(**正解を表示します**)**
A subinterface is a logical interface created on a single physical router interface that allows routing between VLANs (known as Router-on-a-Stick (ROAS)). This method is commonly used when only one physical router is available, allowing inter-VLAN communication without additional hardware.
*Why not the other options?
*VXLAN (B) - This is used for extending Layer 2 networks over a Layer 3 infrastructure, primarily in data centers. It does not directly enable inter-VLAN communication.
*Layer 3 switch (C) - A Layer 3 switch can route between VLANs, but the scenario states that purchasing additional hardware is not an option.
*VIR (D) - This is not a standard networking term in the context of VLAN communication.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 8: VLANs and Inter-VLAN Routing

質問: **94**
ネットワーク管理者は、顧客を新しいサーバーに誘導するために外部 DNS を変更しました。管理者は、新しいサーバーの構成をテストするために、次のどのツールを使用する必要がありますか?
A. ping
B. tracert
C. tcpdump
D. nslookup

正解: (正解を表示します)
*nslookup allows querying DNS records to verify if the new server is correctly resolving domain names.
*ping (A) tests basic connectivity, not DNS configuration.
*tracert (B) shows network path latency but doesn't test DNS.
*tcpdump (C) captures packets but isn't ideal for DNS verification.
#Reference: CompTIA Network+ N10-009 Official Documentation - DNS Testing Tools.

質問: **95**
次のどれがスプリットトンネル VPN の例ですか?
A. ユーザーのインターネット接続を通じて、パブリック リソースのみにアクセスします。
B. 暗号化されたリソースには、別のトンネルを介してアクセスします。
C. すべての企業リソースとパブリック リソースは、オンサイト サーバーへのルーティングを通じてアクセスされます。
D. ACL は、さまざまな接続を介したネットワーク トラフィックのバランスを取るために使用されます。
正解: (正解を表示します)
In a split-tunnel VPN, only corporate traffic is sent through the VPN tunnel, while public internet traffic goes directly through the user's local ISP. This reduces bandwidth use on the corporate VPN concentrator and improves performance for non-work traffic.
B). Separate tunnels for encrypted traffic describes multi-tunnel VPNs, not split tunneling.
C). All traffic routed through on-site servers is a full-tunnel VPN, not split-tunnel.
D). ACLs balancing traffic relates to routing or load balancing, not VPN split tunneling.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - VPN types, split vs. full tunnel, remote access.

質問: **96**
ファイルを安全に転送するには、次のどのプロトコル ポートを使用する必要がありますか?
A. 22
B. 69
C. 80
D. 3389
正解: (正解を表示します)
Port 22 is used for SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol), which encrypt file transfers using SSH (Secure Shell). This ensures data is transmitted securely over the network.
*Why not the other options?
*Port 69 (B) - TFTP (Trivial File Transfer Protocol): Transfers files but is not secure (no encryption).
*Port 80 (C) - HTTP: Used for web traffic, not for file transfer.
*Port 3389 (D) - RDP (Remote Desktop Protocol): Used for remote desktop access, not file transfer.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 5: Network Protocols and Ports

質問: **97**

ユーザーがウェブサイトにアクセスしようとしましたが、意図したサイトではなくvmw.cba.comが表示されます。正しいウェブサイトにアクセスするには、次のうちどれを実行する必要がありますか？
A. CNAMEレコードを変更する
B. PTRレコードを更新する
C. NTP設定を変更する
D. TXTレコードを削除する
正解: **A (**コメントを発表する**)**
A CNAME (Canonical Name) record maps an alias to the correct fully qualified domain name (FQDN). If a user is redirected to the wrong hostname, correcting or updating the CNAME ensures the alias points to the proper domain.
B). PTR record maps IP to hostname (reverse DNS), not forward website resolution.
C). NTP relates to time sync, irrelevant to DNS resolution.
D). TXT record stores metadata like SPF or DKIM info, not used for hostname aliasing.
References (CompTIA Network+ N10-009):
Domain: Network Standards, Protocols, and Implementations - DNS record types (A, AAAA, CNAME, PTR, TXT).

質問: **98**
ネットワーク管理者は、大規模ネットワークアーキテクチャ内の小規模なプライベートネットワーク上に、45台の個別のホストを含むサブネットを作成しています。このネットワークにネットワークアドレスを割り当てる際に、最も効率的なネットワークアドレスの使用方法は次のうちどれですか？
A. 10.0.50.128/25
B. 10.7.142.128/27
C. 10.152.4.192/26
D. 10.192.1.64/28
正解: **C (**コメントを発表する**)**
For 45 hosts, the minimum subnet size must allow at least 46 usable addresses (1 each for network and broadcast addresses).
A /26 subnet provides 64 addresses, 62 usable - suitable.
A /27 subnet gives only 30 usable - insufficient.
A /25 offers 126 usable - more than needed.
A /28 provides just 14 - too small.
So, the most efficient subnet with minimal wastage is /26.
From Andrew Ramdayal's guide:
"When designing subnets, always choose the smallest subnet mask that still accommodates all hosts. A /26 provides 62 usable host addresses, suitable for networks with about 50 hosts."

質問: **99**
エッジ サーバーを使用して地理的に分散された方法でコンテンツを保存し、クライアントに配信するために使用されるのは次のどれですか。
A. Load balancer
B. CDN
C. DNS server
D. SAN
正解: **(**正解を表示します**)**

A Content Delivery Network (CDN) stores cached versions of content in edge locations to deliver data faster and more reliably to users based on geographical proximity.
From Andrew Ramdayal's guide:
"CDNs distribute content to multiple, geographically dispersed servers. This enhances performance and reliability for end-users by reducing latency and load times."

質問**: 100**
ある研究施設では、近い将来に世界的なネットワーク トラフィックが急増すると予想しています。オフィスには ISP からの 2.5Gbps ファイバー接続が装備されていますが、施設では現在 1Gbps 接続しか利用していません。ISP の接続速度を使用するには、次のどれを設定する必要がありますか。
A. 802.1Q タグ付け
B. ネットワークアドレス変換
C. ポートデュプレックス
D. リンクアグリゲーション
正解**: (**正解を表示します**)**
Understanding Link Aggregation:
Definition: Link aggregation combines multiple network connections into a single logical link to increase bandwidth and provide redundancy.
Usage in High-Bandwidth Scenarios:
Combining Links: By aggregating multiple 1Gbps connections, the facility can utilize the full 2.5Gbps bandwidth provided by the ISP.
Benefits: Enhanced throughput, load balancing, and redundancy, ensuring better utilization of available bandwidth.
Comparison with Other Options:
802.1Q Tagging: Used for VLAN tagging, which does not affect the physical bandwidth utilization.
Network Address Translation (NAT): Used for IP address translation, not related to link speed or bandwidth aggregation.
Port Duplex: Refers to the mode of communication (full or half duplex) on a port, not the aggregation of bandwidth.
Implementation:
Configure link aggregation (often referred to as LACP - Link Aggregation Control Protocol) on network devices to combine multiple physical links into one logical link.
References:
CompTIA Network+ study materials on network configuration and link aggregation.

質問**: 101**
ネットワーク管理者は、150 人のユーザーを抱える新しいサイトのネットワークを構成しています。今後 1 年以内に、サイトのユーザー数は 10 人増加すると予想されます。各ユーザーには 2 つの IP アドレスが与えられます。1 つはコンピューター用、もう 1 つはネットワークに接続された電話用です。次のクラスフル IPv4 アドレス範囲のうち、ネットワークに最適なのはどれでしょうか。
A. クラスD
B. クラスB
C. クラスA
D. クラスC
正解**: (**正解を表示します**)**
IPv4 addresses are divided into classes:
Class A: Supports 16,777,214 hosts (large enterprises).
Class B: Supports 65,534 hosts (medium to large networks).
Class C: Supports 254 hosts (small to medium networks).
Class D: Used for multicast, not for assigning IPs to hosts.

Step-by-step Calculation:
The network will have 150 users initially, with a projected growth of 10 users, totaling 160 users.
Each user has two devices, so 160 × 2 = 320 IP addresses needed.
A Class C subnet has 254 usable IPs by default, which is not sufficient.
A Class B subnet can support thousands of hosts, making it the most appropriate option.
Incorrect Options:
A:Class D: Reserved for multicast, not for host assignments.
C:Class A: Overkill for a network of this size.
D:Class C: Cannot support 320 hosts without subnetting, making Class B the best choice.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on IP Addressing and Subnetting

質問: **102**
データセンター管理者は、ストレージ環境におけるジャンボフレームの使用を検討しています。ストレージ環境でジャンボフレームを使用する最も適切な理由として、次のうちどれが適切でしょうか。
A. デバイスのオーバーヘッドを削減するため
B. STPの現在のルートスイッチを報告する
C. ルーティングの収束を改善する
D. ドライブのスループットを向上させる
正解: **(正解を表示します)**
Jumbo frames are Ethernet frames with a payload greater than the standard 1,500 bytes. Using jumbo frames reduces the number of frames transmitted over the network, thereby reducing the overhead associated with frame headers and processing. The document explains:
"Jumbo frames are used in storage networks to reduce device overhead by lowering the number of frames required for data transfer, which can increase overall throughput and performance."

質問: **103**
ネットワーク技術者が新しい施設のLANを設計しています。会社は300台以上のデバイスがネットワークに接続されることを想定しています。次のうち、最も効率的なサブネットマスクはどれでしょうか？
A. 255.255.0.0
B. 255.255.192.0
C. 255.255.254.0
D. 255.255.255.254
正解: **(正解を表示します)**
The requirement is to support over 300 hosts. The subnet mask 255.255.254.0 (or /23) provides 512 addresses, 510 of which are usable - ideal for around 300 devices.
* 255.255.0.0 (/16) provides too many addresses.
* 255.255.192.0 (/18) gives 16384 addresses - overkill.
* 255.255.255.254 is invalid for host assignments (only 2 addresses, 0 usable).
From Andrew Ramdayal's guide:
"To support 300 hosts, a /23 subnet (255.255.254.0) offers 510 usable addresses - the most efficient choice without excessive overhead."

質問: **104**

ネットワーク エンジニアが顧客のために新しい VoIP ネットワークを設定しています。現在のネットワークは、コンピューターとサーバーのみにセグメント化されています。新しいネットワークでは追加のスイッチ ポートは使用できません。
ネットワークを正しく構成するためにエンジニアが行う必要があるのは次のどれですか? (2 つ選択してください)。
A. ネットワーク翻訳定義を変更する
B. 802.1Qを有効にする
C. ルーティングプロトコルを実装する
D. 音声VLANを設定する
E. DNSを再設定する
F. 境界ネットワークにデバイスを配置する
正解: **(**正解を表示します**)**
To support VoIP on the same physical ports used by computers:
B: Enable 802.1Q: This standard supports VLAN tagging, allowing voice and data traffic to share the same port using separate VLANs.
D: Set up voice VLANs: Separating voice traffic into its own VLAN improves QoS and manageability.
Other options are not directly related to configuring VoIP over existing ports:
A: Network translation definitions (NAT) are unrelated to switch-level VLAN configuration.
C: Routing protocols are not necessary at the switch level for VLAN setup.
E: DNS is not required for the switch or VLAN setup.
F: Perimeter network (DMZ) is used for public-facing servers, not VoIP VLANs.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.
CompTIA Network+ N10-009 Official Objectives: 3.6 - Explain the characteristics of network topologies and types.

質問: **105**
ネットワーク技術者が MDF 内のファイバー パッチ パネルへのケーブルを終端しています。次のコネクタ タイプのうち、最もよく使用されるのはどれですか。
A. F-type
B. RJ11
C. BNC
D. SC
正解: **(**正解を表示します**)**
In a fiber patch panel, the SC (Subscriber Connector or Standard Connector) is commonly used because of its push-pull design and reliability in enterprise environments.
Breakdown of Options:
A: F-type - Used for coaxial cables (e.g., cable TV), not fiber.
B: RJ11 - Used for telephone lines, not fiber.
C: BNC - Used for coaxial connections, not fiber.
D: SC - # Correct answer. A standard fiber optic connector used in patch panels.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.1: Compare and contrast physical network connectors.

質問: **106**
次のポートのうち、ディレクトリ サービスへの安全な接続を作成するのはどれですか?

A. 22
B. 389
C. 445
D. 636
正解: **D** (コメントを発表する)
LDAP (Lightweight Directory Access Protocol) uses port 389 for standard connections and port 636 for LDAP over SSL (LDAPS), which secures directory service communication.
Breakdown of Options:
A: 22 - SSH port, not used for directory services.
B: 389 - Used for LDAP, but not encrypted.
C: 445 - Used for SMB file sharing, not LDAP.
D: 636 - Correct answer. LDAPS (LDAP over SSL/TLS) secures directory authentication.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.1: Compare and contrast network protocols.
RFC 4511: Lightweight Directory Access Protocol (LDAP)

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu
792問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **107**
ネットワーク管理者は、断続的なネットワーク接続に関する苦情を受けました。管理者は調査を行い、ネットワーク設計に潜在的なループシナリオが含まれていることを発見しました。管理者は次のうちどれを行うべきでしょうか？
A. スパニングツリーを有効にする
B. ポートセキュリティを構成する
C. スイッチポートの速度制限を変更する
D. 802.1Qタグ付けを強制する
正解: **A** (コメントを発表する)
Spanning Tree Protocol (STP) is designed to detect and prevent Layer 2 loops by blocking redundant paths. If loops are possible in the design, enabling STP ensures network stability.
B). Port security controls endpoint MAC addresses, not loops.
C). Speed limits address bandwidth, not loop prevention.
D). 802.1Q tagging allows VLAN separation but does not resolve loops.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Loop prevention, spanning tree, switch design.

質問: **108**
ネットワーク技術者は、取り付けるために丸くてねじるコネクタを備えたファイバー パッチ コードを要求しています。
このコネクタ タイプの正しい名前は次のどれですか?
A. ST

B. BNC
C. SC
D. LC
正解: **(**正解を表示します**)**
The ST (Straight Tip) fiber connector is round with a bayonet twist-lock mechanism. It is older but still used in some fiber installations.
B). BNC is a coaxial connector.
C). SC (Subscriber Connector) is a square push-pull fiber connector.
D). LC (Lucent Connector) is a small form-factor fiber connector.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Fiber connectors (ST, SC, LC).

質問: **109**
ネットワーク技術者は、ネットワークの容量を増やすために新しいスイッチを追加しようとしています。技術者は2つのスイッチを1本のケーブルで接続しました。複数のホストを新しいスイッチに移動しましたが、どのホストもネットワークまたはインターネットにアクセスできません。この問題を解決するために、技術者は次のうちどれを行うべきでしょうか？
A. 接続ポートをトランクポートとして設定します
B. スイッチ間にSTPケーブルを設置します
C. スイッチのPoE予算を増やす
D. アップリンクポートにリンクアグリゲーションを設定する
正解: **(**正解を表示します**)**
The correct solution is to configure the connecting ports as trunk ports. When connecting switches, the uplink ports must be configured to carry traffic for multiple VLANs (trunking), not just a single access VLAN.
Without trunking, VLAN tags may be dropped, and traffic from hosts will not reach the rest of the network or internet.
B). STP cables is a misnomer - STP refers to Spanning Tree Protocol or Shielded Twisted Pair cables, neither of which solves this logical configuration issue.
C). PoE budget is irrelevant because switches and hosts in this context don't require PoE.
D). Link aggregation (LACP, EtherChannel) is for increasing bandwidth/redundancy across multiple links, not required with a single cable.
By enabling trunking on the uplink ports, the switches can pass VLAN-tagged traffic, ensuring hosts connected to the new switch have access to the same resources as those on the existing switch.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - VLAN trunking, inter-switch connectivity.

質問: **110**
ネットワークセキュリティ管理者は、安全なネットワークと社内ネットワーク間で送信されるデータの内容を監視する必要があります。このタスクを達成できる監視方法は、次のうちどれですか？
A. ポートミラーリング
B. フローデータ
C. Syslogエントリ
D. SNMPトラップ
正解: **A (**コメントを発表する**)**

To monitor the contents of data (i.e., inspect the actual packets/frames and their payloads) moving between networks, the administrator should use port mirroring (also called SPAN on some platforms). Port mirroring copies traffic from one or more switch ports (or VLANs) to a designated monitoring port where a packet analyzer/IDS sensor can capture and inspect the traffic in detail. This aligns with Network+ (N10-009) security and monitoring concepts that distinguish between packet-level visibility and higher-level summaries or logs. If the requirement is explicitly to monitor "contents," you need a method that provides full packet capture capability, not just metadata.
Flow data (e.g., NetFlow) provides summarized metadata-who talked to whom, how much, ports, and timestamps-but not full payload contents. Syslog entries are device/application-generated logs and only show events a device chooses to report; they don't provide full data content visibility. SNMP traps are alerts about status changes (interfaces, thresholds, etc.) and similarly do not include traffic contents. Therefore, port mirroring is the correct monitoring method for inspecting data contents in transit.

質問**: 111**
次のデバイスのうち、OSI モデルのデータ リンク層で主に機能し、光ファイバー ケーブルをネットワーク インターフェイスに接続するために使用されるものはどれですか。
A. SC
B. DAC
C. SFPトランシーバー
D. ツインアクシャルケーブル
正解**: (**正解を表示します**)**
An SFP (Small Form-factor Pluggable) transceiver is a modular device that provides the interface between fiber-optic or copper cabling and the networking equipment (e.g., switch or router). It operates primarily at Layer 2 (Data Link), converting optical or electrical signals into frames usable by the network device.
A). SC is a fiber connector type, not the transceiver.
B). DAC (Direct Attach Copper) is a passive copper cable assembly with fixed transceivers, not a general- purpose module.
D). Twinaxial cable is a copper medium, not an interface device.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Transceivers (SFP, GBIC, QSFP), fiber connectivity, OSI model mapping.

質問**: 112**
ネットワーク管理者は、会社のウェブサイトへの受信トラフィックをHTTPSのみに制限し、インターネットからのその他の受信トラフィックをすべて拒否したいと考えています。この目的を達成するのに最適な方法は次のうちどれですか？
A. エッジファイアウォールのACL
B. アクセススイッチのポートセキュリティ
C. Webゲートウェイでのコンテンツフィルタリング
D. 送信プロキシでのURLフィルタリング
正解**: (**正解を表示します**)**
AnAccess Control List (ACL)configured on theedge firewallis the correct and most effective solution to filter inbound traffic. The administrator can allow TCP port 443 (HTTPS) and deny all other traffic. This is a classic firewall configuration for securing public-facing servers.
Reference:Section 4.3 - Network Security Features, Defense Techniques, and Solutions - "ACLs (Access Control Lists)"

質問**: 113**
次のどれを使用すると、ネットワーク管理者は待ち時間に影響を与えずにインターネットからの攻撃を分析できますか?
A. IPS
B. IDS
C. ロードバランサー

D. ファイアウォール
正解: **(**正解を表示します**)**
An Intrusion Detection System (IDS) monitors and analyzes traffic to detect suspicious activity but does not sit in the traffic path, meaning it doesn't affect latency. In contrast, an IPS is in-line and can introduce delay.
From Andrew Ramdayal's guide:
"IDS monitors and alerts on malicious activity but does not block traffic, making it suitable for environments where low latency is critical."

質問: **114**
ユーザーは Web ブラウザ経由で企業の VPN に接続し、TLS を使用して社内財務システムにアクセスし、タイムカードを入力できます。VPN の使用方法を最もよく表しているのはどれですか。
A. クライアントレス
B. クライアントからサイトへ
C. フルトンネル
D. サイト間
正解: **A (**コメントを発表する**)**
Reference: CompTIA Network+ Certification Exam Objectives - Remote Access Methods section.

質問: **115**
次のどれが Web ベースの顧客ポータルの可用性に影響しますか?
A. MACフラッディング
B. ARPスプーフィング
C. DoS
D. 不正デバイス
正解: **C (**コメントを発表する**)**
A DoS (Denial of Service) attack directly targets availability, one of the core security goals (CIA triad) emphasized in Network+ (N10-009) security objectives. A web-based customer portal depends on reachable services (web servers, load balancers, DNS, upstream bandwidth). In a DoS, an attacker attempts to overwhelm the portal or its supporting infrastructure-consuming bandwidth, exhausting server resources, or saturating state tables-so legitimate users cannot connect or experience severe degradation. This is the most direct and common scenario where "availability" is impacted for a public web service.
MAC flooding aims to overflow a switch's CAM table and can lead to traffic being broadcast out ports, which is more commonly associated with enabling sniffing or disruption within a local switched network segment- not typically the primary attack described for a web portal's availability. ARP spoofing is a local network man-in-the-middle/redirection technique affecting integrity/confidentiality and potentially availability for local hosts, but it is not the best match for a public portal availability impact. Rogue devices can introduce risk, but the option is broad and indirect; DoS is the clearest availability-focused threat.

質問: **116**
ネットワーク管理者は、802.11axデバイスの移行を完了するために、スペクトラムアナライザを使用して特定のAPの位置を特定する必要があります。APの位置を特定するために、アナライザに表示される情報は次のどれですか？
A. SSID
B. RSSI
C. チャンネル番号
D. BSSID

正解: **(**正解を表示します**)**
To locate a specific access point (AP), the most reliable identifier to view is the BSSID. In 802.11 networks, the BSSID is the radio interface identifier for the AP (typically the AP radio's MAC address). Unlike an SSID, which can be shared across many APs in the same wireless network (especially in an enterprise deployment using the same SSID across multiple APs), the BSSID uniquely distinguishes one AP radio from another. This is critical during an 802.11ax (Wi-Fi 6) migration, where multiple APs may broadcast identical SSIDs and operate on the same channels in different areas.
While RSSI is useful for physically walking toward the strongest signal (a technique used in locating RF sources), RSSI alone does not confirm you are tracking the correct AP-only that you are near an RF transmitter. Channel number also does not uniquely identify the AP because multiple APs can share the same channel (and channels may overlap depending on band and width). SSID similarly is not unique. Therefore, viewing the BSSID on the analyzer (or Wi-Fi analyzer mode) allows the administrator to confirm the exact AP being measured and located.

質問: **117**
ネットワーク管理者は、国に基づいて企業ネットワークへのリモートアクセスを制限するために、ジオフェンシングポリシーを更新したいと考えています。管理者が最も活用する可能性のあるのは次のうちどれですか？
A. MACフィルタリング
B. 管理距離
C. Bluetoothビーコン信号
D. IPアドレスブロック
正解: **D (**コメントを発表する**)**
The correct answer is IP address blocks because geofencing policies typically rely on public IP address ranges associated with specific geographic regions or countries. According to CompTIA Network+ (N10-009) security objectives, geofencing is a security control used to restrict or allow traffic based on geographic location. This is commonly implemented on firewalls, VPN concentrators, or security gateways by referencing databases that map IP address blocks to countries or regions.
When configuring geofencing, administrators create access control rules that permit or deny traffic from specific country-based IP ranges. This method is effective for limiting remote access to approved geographic locations and reducing exposure to international threat sources.
MAC filtering (Option A) is used within local networks and does not function over the internet for geographic control. Administrative distance (Option B) is a routing concept that determines route preference and has no relation to access control policies. Bluetooth beacon signals (Option C) are used for proximity-based services and indoor positioning, not for country-level remote access restrictions.
Therefore, leveraging IP address blocks is the correct approach for implementing geofencing controls.

質問: **118**
ある会社が同じビルの別のフロアに拡張しています。ネットワーク エンジニアは、既存のスタックと同じ VLAN を使用して新しいスイッチを構成します。ネットワーク エンジニアが新しいスイッチを既存のスタックに接続すると、すべてのユーザーの接続が失われます。最も可能性の高い理由はどれですか。
A. 新しいスイッチでは未使用のポートが無効になっています
B. 新しいスイッチにはデフォルトゲートウェイがありません
C. 新しいスイッチはアクセスポートに接続されています
D. 新しいスイッチはスパニングツリーループ内にあります
正解: **(**正解を表示します**)**
This describes a Spanning Tree Protocol (STP) loop. If STP isn't correctly configured or a redundant link is added without STP protection, it causes broadcast storms and network outages.
A). Unused ports disabled would not affect the entire network.
B). Missing default gateway on a switch doesn't cause total network loss.

**C. Connecting a switch to an access port can cause VLAN mismatches, but not total connectivity loss unless a loop forms.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.6 - Explain the characteristics of network topologies and types.

質問: **119**
一連のポリシーを使用して、ユーザーの ID に基づいてネットワークへのアクセスを許可または拒否する NAC のタイプは次のどれですか。
A. Standard ACL
B. MAC filtering
C. 802.1X
D. SSO
正解: **(正解を表示します)**
The correct answer is 802.1X, which is an identity-based Network Access Control (NAC) framework emphasized in the CompTIA Network+ N10-009 objectives under network security and access control. 802.1 X uses a policy-driven authentication process to determine whether a user or device is allowed network access based on verified credentials, such as usernames, passwords, or digital certificates.
802.1X operates using three main components: the supplicant (the client requesting access), the authenticator (the network device such as a switch or wireless access point), and the authentication server (typically a RADIUS server). Once the user's identity is authenticated, predefined policies determine the level of access granted-full access, limited access, or denial. This makes 802.1X a cornerstone of zero trust and enterprise- grade NAC implementations.
A standard ACL controls traffic based on IP addresses and ports, not user identity. MAC filtering allows or denies access based on device MAC addresses, which can be easily spoofed and does not verify user identity.
SSO (Single Sign-On) simplifies authentication across multiple systems but does not control network-layer access.
Network+ highlights 802.1X as a secure, scalable solution for enforcing identity-based network access policies in both wired and wireless environments.

質問: **120**
顧客は、インターネットからのページ全体のダウンロード回数を減らすために、よく使用するコンテンツをキャッシュしたいと考えています。ネットワーク管理者は、次のうちどれを推奨すべきでしょうか？
A. プロキシサーバー
B. ロードバランサー
C. オープンリレー
D. コードリポジトリ
正解: **(正解を表示します)**
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
A proxy server (specifically a caching HTTP/HTTPS proxy) stores frequently accessed web objects and serves them locally to clients, reducing external bandwidth consumption and improving response times.
B). Load balancer distributes traffic across servers but does not inherently cache internet content.
C). Open relay is a misconfigured mail server that permits unauthorized relaying-this is a security issue, not a caching solution.
D). Code repository (e.g., for source control) isn't related to web content caching.
References (CompTIA Network+ N10-009):
Domain: Network Standards, Protocols, and Implementations - Application-layer services (HTTP/HTTPS), proxies and caching behavior, performance optimization.

質問: **121**
停電時にデバイスの電源をオンにしておくための最適な方法はどれですか?

A. UPS
B. 電力負荷
C. PDU
D. 電圧
正解: (正解を表示します)
A UPS (Uninterruptible Power Supply) provides backup power to devices during a power outage, allowing for continuous operation and protecting against sudden shutdowns that could cause data loss or equipment damage. The document confirms:
"A UPS (Uninterruptible Power Supply) is essential for maintaining power to critical devices during an outage, protecting data and ensuring continuous operation until power is restored or a safe shutdown can be performed."

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu **792**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
攻撃者がエンドポイントのhostsファイルにアクセスし、変更しました。これにより、ユーザーは会社のホームページから不正なウェブサイトにリダイレクトされます。最も可能性が高いのは次のうちどれですか？
A. DNSスプーフィング
B. フィッシング
C. VLANホッピング
D. ARPポイズニング
正解: (正解を表示します)
When the hosts file is altered, local name resolution is compromised, and domain queries are redirected to malicious IP addresses. This is a form of DNS spoofing/poisoning, where false mappings trick users into visiting fraudulent websites.
B). Phishing typically uses emails or messages to trick users, not local file modification.
C). VLAN hopping is a Layer 2 attack to gain unauthorized network access, unrelated to DNS.
D). ARP poisoning manipulates ARP tables on a LAN to reroute traffic, not name resolution.
References (CompTIA Network+ N10-009):
Domain: Network Security - DNS poisoning/spoofing, host file manipulation, endpoint attacks.

質問: **123**
ネットワーク管理者は、外部 DNS レコードがホストされている場所を変更する必要があります。このタスクを実行するために、管理者がレジストラに変更する必要があるレコードは次のどれですか。
A. NS
B. SOA
C. PTR
D. CNAME
正解: (正解を表示します)

To change where the outside DNS records are hosted, the network administrator needs to update the NS (Name Server) records at the domain registrar. NS records specify the authoritative name servers for a domain, directing where DNS queries should be sent.
NS (Name Server) Records: These records indicate the servers that are authoritative for a domain. Changing the NS records at the registrar points DNS resolution to the new hosting provider.
SOA (Start of Authority): Contains administrative information about the domain, including the primary name server.
PTR (Pointer) Records: Used for reverse DNS lookups, mapping IP addresses to domain names.
CNAME (Canonical Name) Records: Used to alias one domain name to another, not relevant for changing DNS hosting.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Discusses DNS records, their purposes, and how to manage them.
Cisco Networking Academy: Provides training on DNS management and the role of different DNS record types.
Network+ Certification All-in-One Exam Guide: Explains DNS records and their configuration for domain management.

質問: **124**
ネットワーク管理者はユーザーからチケットを受け取りました。ユーザーから、どのウェブサイトにもアクセスできないという報告があり、コンピューター上のすべての問題を確認済みだと言われました。管理者が最初に取るべき対応は次のうちどれですか？
A. 分割して統治する。
B. 考えられる原因の理論を確立する。
C. ユーザーに質問します。
D. 調査結果を文書化します。
正解: (正解を表示します)
The correct answer is Question the user because the first step in the CompTIA Network+ (N10-009) troubleshooting methodology is to identify the problem. Identifying the problem involves gathering information, asking clarifying questions, determining if anything has changed, and establishing the scope of the issue.
Even though the user states they have "checked everything," the administrator should not assume that all relevant troubleshooting steps were properly performed. The technician must ask specific questions such as:
Are other users affected? Is the issue limited to certain websites? Are there any error messages? When did the issue start? Were there recent updates or configuration changes?
Only after gathering sufficient information should the administrator move to the next steps, such as establishing a theory of probable cause (Option B) or using divide-and-conquer methods (Option A).
Documentation (Option D) occurs after resolving and verifying the issue.
Therefore, questioning the user to clearly define and scope the problem is the correct first action according to the structured troubleshooting process.

質問: **125**
ネットワーク管理者は、サービスをオフサイト環境にフェールオーバーする必要があります。このプロセスが完全に機能するまでには 4 週間かかります。これは、次の DR (災害復旧) の概念のどれを表していますか。
A. ホットサイト
B. 温かいサイト
C. コールドサイト
D. アクティブ･アクティブアプローチ
正解: (正解を表示します)
A cold site is a backup facility that provides infrastructure (such as power, cooling, and space) but does not have active IT resources installed. When a disaster occurs, IT teams must bring in and configure all necessary hardware and software before services can resume. This process can take weeks or longer-which matches the scenario described.

*Why not the other options?
*Hot site (A) - A hot site is a fully operational backup facility with up-to-date data and pre-configured hardware, allowing almost instant failover (minutes to hours).
*Warm site (B) - A warm site has pre-installed hardware and some software/configurations, but it requires some setup before becoming fully operational (hours to a few days).
*Active-active approach (D) - This means that multiple sites run simultaneously with load balancing, ensuring no downtime in case of a failure.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 15: Business Continuity and Disaster Recovery

質問: **126**
最近のセキュリティ意識向上を目的としたフィッシング攻撃を受け、サイバーセキュリティチームは、ユーザーが潜在的に悪意のあるウェブサイトにアクセスする際には、追加のセキュリティ対策を講じる必要があると判断しました。この懸念に対処するには、以下のセキュリティ対策のうちどれが最適ですか？
A. DNS フィルタリングを実装します。
B. HTTPS のみを許可するように ACL を更新します。
C. 新しい IPS ハードウェアを構成します。
D. 802.1X セキュリティ機能を展開します。
正解: **(**正解を表示します**)**
DNS filtering blocks access to known malicious websites by comparing domain requests against a list of allowed or blocked URLs. It is an effective defense against phishing and other web-based attacks.
From Andrew Ramdayal's guide:
"URL filtering restricts access to specific websites or web content by comparing URLs against a predefined list of allowed or blocked sites...commonly used to prevent users from accessing malicious sites."

質問: **127**
ネットワーク技術者がアクセス ポートの設定を調べているときに、複数の VLAN が設定されていることに気付きました。ポートの設定方法を最もよく表しているのは次のうちどれですか。
A. 音声VLANの場合
B. VLANが多すぎる
C. デフォルトのVLANの場合
D. ネイティブVLANの場合
正解: **A (**コメントを発表する**)**
It is common for an access port to have both a voice VLAN and a data VLAN. A voice VLAN separates voice traffic from regular data traffic, ensuring better quality and security for voice communications.

質問: **128**
ネットワーク エンジニアが組織内のすべての SNMP 管理を担当しています。エンジニアはプレーンテキスト データを使用しない SNMP バージョンを使用する必要があります。この要件をサポートする SNMP の最小バージョンは次のどれですか。
A. v1
B. v2c
C. v2u
D. v3
正解: **(**正解を表示します**)**

SNMPv3 is the version of the Simple Network Management Protocol that introduces security enhancements, including message integrity, authentication, and encryption. Unlike previous versions (v1 and v2c), SNMPv3 supports encrypted communication, ensuring that data is not transmitted in plaintext. This provides confidentiality and protects against eavesdropping and unauthorized access.References: CompTIA Network+ study materials.

質問: **129**
顧客からヘルプデスクに電話があり、リソースにアクセスできなくなったと報告がありました。ネットワーク変更前はリソースは利用可能でした。技術者が報告を確認し調査したところ、新しい論理レイアウトによってタグ付けが使用され、ネットワークがセグメント化されていることが分かりました。接続を復旧するために、以下のアプライアンスのうち、最も確認が必要なものはどれでしょうか？
A. アクセスポイント
B. ファイアウォール
C. スイッチ
D. ロードバランサー
正解: **(**正解を表示します**)**
The correct answer is Switch because the question references a new logical layout segmenting the network using tagging, which indicates VLAN (Virtual Local Area Network) configuration. VLAN tagging (IEEE
802.1Q) is performed on switches to logically separate broadcast domains within the same physical infrastructure.
According to CompTIA Network+ (N10-009) objectives under switching technologies, VLANs are used to improve security, reduce broadcast traffic, and logically segment network traffic. When VLAN tagging is misconfigured-such as incorrect trunk ports, access port assignments, or mismatched VLAN IDs-devices may lose connectivity to required network resources.
Since the issue began after changes involving tagging, the most likely cause is an incorrect switch configuration, such as improper VLAN assignments or trunking settings.
An access point (Option A) may use VLANs for SSID segmentation, but core tagging configuration is handled at the switch. A firewall (Option B) filters traffic but does not control VLAN tagging at Layer 2 in typical deployments. A load balancer (Option D) distributes traffic among servers and is unrelated to VLAN segmentation.
Therefore, reviewing the switch configuration is the appropriate action to restore connectivity.

質問: **130**
ネットワーク管理者は、MDFからサーバールームへマルチモードファイバーケーブルを接続する必要があります。管理者はケーブルをスイッチ2に接続しましたが、リンクランプが点灯しません。管理者はファイバーをテストし、問題がないことを確認しました。スイッチ1の正常なポートへの接続は成功しましたが、スイッチ2では接続が機能しません。管理者は次に、次のうちどの点を確認する必要がありますか？
A. 繊維長
B. トランシーバーモデル
C. コネクタタイプ
D. ポート速度
正解: **(**正解を表示します**)**
The most probable issue is with thetransceiver model. Not all transceivers are compatible with multimode fiber, and the specific type (e.g., SFP, SFP+) and its wavelength must match the fiber cable type. If a port works on one switch but not the other with the same cable, this is a strong indicator of incompatible or faulty transceiver hardware.
Reference:Section 1.5 - Transmission Media and Transceivers - "Transceivers and Compatibility"

質問: **131**
ネットワーク管理者は、ユーザーがインターネットの利用ルールに同意していることを確認する必要があります。管理者がこのタスクを達成するために役立つのは次のうちどれですか。

A. キャプティブポータル
B. 利用規約
C. ネットワークアクセス制御
D. DNSフィルタリング
正解: (正解を表示します)
A captive portal is designed to present terms, conditions, or usage rules to users and require them to acknowledge/accept those rules before granting network or internet access. In Network+ (N10-009) security and access control concepts, captive portals are commonly associated with guest wireless or public access scenarios, where users are redirected to a web page that displays acceptable-use language and requires a click- through acceptance (and sometimes authentication). This provides a technical enforcement point: users must actively accept the rules to proceed, which supports organizational policy compliance and creates a recordable control in many implementations.
An Acceptable Use Policy (AUP) is the document that defines the rules, but by itself it does not technically force a user to acknowledge them at the time of access. NAC controls who/what can connect and can enforce posture and segmentation, but it does not inherently ensure users "accept" usage rules unless paired with a portal workflow. DNS filtering blocks or allows domain access categories (malware, adult content, etc.), which enforces browsing restrictions but does not guarantee user acceptance of rules. Therefore, the best answer to ensure users accept the rules is captive portal.

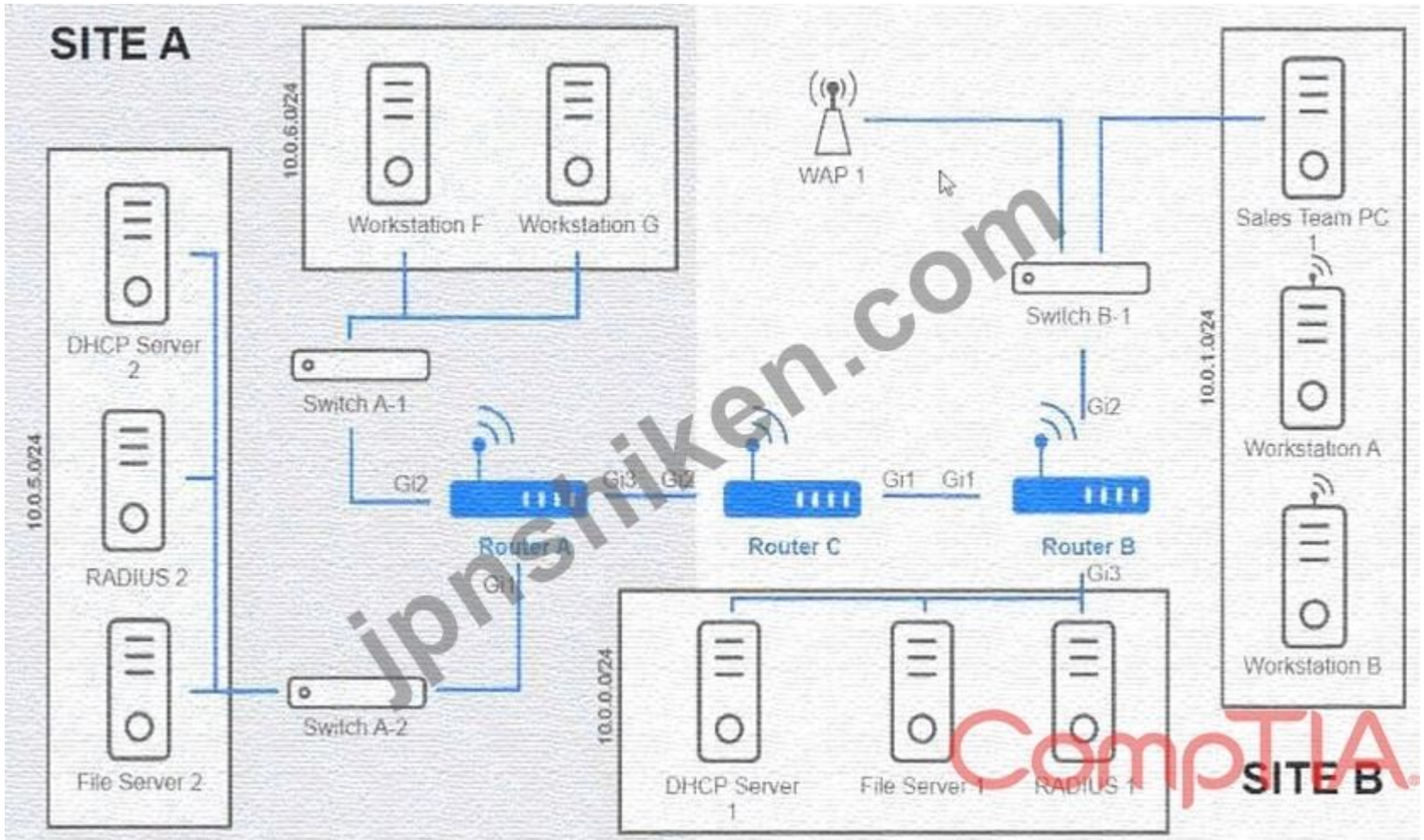
質問: **132**
ネットワーク管理者は冗長性を確保するために2台の新しいファイアウォールを設置し、冗長なインターネット接続を実装する必要があります。管理者は次のルーティング技術のうちどれを最も使用する可能性が高いでしょうか？
A. EIGRP
B. RIPv2
C. OSPF
D. BGP
正解: (正解を表示します)
The answer is D. BGP . When a company wants a redundant internet connection , especially across more than one external path or provider, Border Gateway Protocol (BGP) is the routing technology most commonly associated with that design. BGP is used between autonomous systems and is the standard protocol for making routing decisions across the internet or between an organization and one or more ISPs.
The other options are interior routing protocols. EIGRP , RIPv2 , and OSPF are generally used inside an organization to exchange routes within a private network environment. They are not the normal answer when the question specifically says internet connection redundancy . That wording points outward, beyond the internal LAN or campus routing domain.
In practical terms, BGP gives administrators a way to influence path selection, advertise network prefixes, and maintain reachability if one outside connection fails. That is why it appears in questions involving multihoming, ISP failover, or resilient edge connectivity. Since the scenario mentions redundant firewalls and a need for a redundant internet connection, the best match is the routing technology designed for external route exchange. For Network+, that technology is BGP .

質問: **133**
顧客が隣接する建物間にファイバー接続を追加しています。技術者がマルチモード ケーブルをファイバー パッチ パネルに終端します。技術者がファイバー パッチ ケーブルを接続した後、インジケータ ライトが点灯しません。技術者がこの問題のトラブルシューティングを行うために最初に試すべきことは次のどれですか。
A. 繊維を反転します。
B. ファイバーを再終端します。
C. ファイバーのサイズを確認します。
D. ケーブル配線に目視による欠陥がないか検査します。
正解: (正解を表示します)

When working with fiber optic cables, one common issue is that the transmit (TX) and receive (RX) fibers might be reversed. The first step in troubleshooting should be to reverse the fibers at one end to ensure they are correctly aligned (TX to RX and RX to TX). This is a simple and quick step to rule out a common issue before moving on to more complex troubleshooting.References: CompTIA Network+ study materials.

質問: **134**
ネットワーク管理者が評価を実施したところ、基準を満たしていないネットワークデバイスを発見しました。デバイスが遵守すべき一連のルールとして考えられる構成は次のうちどれですか？
A. 生産
B. バックアップ
C. 候補
D. ゴールデン
正解: **D (**コメントを発表する**)**
The correct answer is golden configuration. This is a reference standard or baseline that defines the approved settings and rules devices should follow. Any deviation from the golden configuration indicates drift or misconfiguration that must be remediated.
A). Production refers to the live environment but doesn't define a standard.
B). Backup configurations are stored copies, not the standard rules.
C). Candidate configuration is a proposed change being tested, not the final baseline.
By enforcing golden configurations, administrators ensure compliance, maintain security standards, and improve consistency across the enterprise.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Configuration standards, golden images/configs.

質問: **135**
ユーザーは、ファイル サーバー 2 にある部門共有上のファイルにアクセスできません。ネットワーク管理者は、ワークステーション A とファイル サーバー 2 をホストするネットワーク間のルーティングを検証する任務を負っています。
説明書
各ルータをクリックして出力を確認し、問題を特定し、適切なソリューションを構成します。いつでもトライシミュレーションの初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。



Routing Table Routing Configuration

```
Router-B# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, GigabitEthernet1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/22 is directly connected, GigabitEthernet3
L        10.0.0.1/32 is directly connected, GigabitEthernet3
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.4/30 is directly connected, GigabitEthernet1
L        172.16.27.5/32 is directly connected, GigabitEthernet1
```

jpnshiken.com
CompTIA

正解:

See the solution configuration below in Explanation.

Explanation:

A screenshot of a computer AI-generated content may be incorrect.



A screenshot of a computer AI-generated content may be incorrect.

A screenshot of a computer AI-generated content may be incorrect.



jpnshiken.com
CompTIA

質問: **136**

ネットワーク アーキテクトはオフプレミスのコンピューティング ファシリティを実装しており、大規模な停止によって運用が影響を受けないようにする必要があります。アーキテクトは次のどれを考慮する必要がありますか。

A. ホットサイト

B. DCI

C. 直接接続

D. 能動的 -受動的アプローチ

正解: **A** (コメントを発表する)

A hot site is a fully operational backup facility with hardware, network, and data synchronization already in place. It allows for immediate failover in the event of a disaster, minimizing downtime.

B: DCI (Data Center Interconnect) connects data centers but doesn't guarantee availability unless built redundantly.

C: Direct Connect refers to a private link to cloud providers, not disaster recovery.

D: Active-passive can help with failover but may involve delay unless combined with hot site principles.

Reference:

CompTIA Network+ N10-009 Official Objectives: 4.4 - Summarize business continuity and disaster recovery concepts.

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu **792**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **137**
次のクラウド展開モデルのうち、マルチテナントと最も一般的に関連し、サービス プロバイダーによって一般的に提供されるものはどれですか。
A. プライベート
B. コミュニティ
C. パブリック
D. ハイブリッド
正解: **(**正解を表示します**)**
The correct answer is public cloud. In public cloud models, a provider (such as AWS, Azure, or Google Cloud) hosts infrastructure and services that are shared across multiple customers, known as multitenancy.
Each tenant is logically isolated, but physical infrastructure is shared, allowing providers to achieve economies of scale.
A). Private cloud is dedicated to one organization, not multitenant.
B). Community cloud is shared among organizations with common interests, but it's less common than public multitenancy.
D). Hybrid cloud combines private and public but does not define tenancy alone.
Public cloud services are the most cost-effective and scalable because they spread costs across many customers, but they require strong security and isolation to protect tenants.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Cloud models, multitenancy, public vs private.

質問: **138**
ネットワーク管理者は、次の要件を満たすデバイス監視の方法を開発しています。
*ユーザーによる明示的な権限管理が可能
*変更の集中ログが含まれます
*広範囲にアクセスできるリモート管理を提供
*サービスアカウントのサポートを提供します
次のどれがこれらの要件を最も満たすでしょうか?
A. SNMP
B. API
C. SIEM
D. SSO
正解: **(**正解を表示します**)**
*API (Application Programming Interface) enables secure and granular access control, remote management, and logging, making it ideal for network monitoring.
*SNMP (A) is mainly used for device monitoring but lacks centralized logging and user-based privilege control.
*SIEM (C) is a security monitoring tool focused on log collection, not device management.
*SSO (D) is related to authentication, not monitoring.
#Reference: CompTIA Network+ N10-009 Official Documentation - Network Monitoring & Management Technologies.

質問: **139**

ネットワーク管理者は、2.4GHz 帯の産業機器への干渉に気づきました。この問題を最も緩和できると思われるテクノロジは次のうちどれですか (2 つ選択してください)。
A. メッシュネットワーク
B. 5GHz周波数
C. 全方向性アンテナ
D. 重複しないチャネル
E. キャプティブポータル
F. アドホックネットワーク
正解: **(**正解を表示します**)**
* Understanding 2.4GHz Interference:
* The 2.4GHz frequency range is commonly used by many devices, including Wi-Fi, Bluetooth, and various industrial equipment. This can lead to interference and degraded performance.
* Mitigation Strategies:
* 5GHz Frequency:
* The 5GHz frequency band offers more channels and less interference compared to the 2.4 GHz band. Devices operating on 5GHz are less likely to encounter interference from other devices, including industrial equipment.
* Non-overlapping Channels:
* In the 2.4GHz band, using non-overlapping channels (such as channels 1, 6, and 11) can help reduce interference. Non-overlapping channels do not interfere with each other, providing clearer communication paths for Wi-Fi signals.
* Why Other Options are Less Effective:
* Mesh Network: While useful for extending network coverage, a mesh network does not inherently address interference issues.
* Omnidirectional Antenna: This type of antenna broadcasts signals in all directions but does not mitigate interference.
* Captive Portal: A web page that users must view and interact with before accessing a network, unrelated to frequency interference.
* Ad Hoc Network: A decentralized wireless network that does not address interference issues directly.
* Implementation:
* Switch Wi-Fi devices to the 5GHz band if supported by the network infrastructure and client devices.
* Configure Wi-Fi access points to use non-overlapping channels within the 2.4GHz band to minimize interference.
References:
* CompTIA Network+ study materials on wireless networking and interference mitigation.

質問**: 140**
次の攻撃のうち、スイッチにすべてのトラフィックをすべてのポートから送信させるのはどれですか?
A. ARPポイズニング
B. 邪悪な双子
C. MACフラッディング
D. DNSスプーフィング
正解**: C (**コメントを発表する**)**
MAC flooding overwhelms a switch's CAM (Content Addressable Memory) table by sending a flood of frames with spoofed MAC addresses. Once the CAM table overflows, the switch cannot learn legitimate MAC addresses and defaults to flooding all frames out all ports, effectively turning it into a hub. This allows an attacker to capture traffic not originally destined for their port.
A). ARP poisoning corrupts ARP tables to redirect traffic but does not overflow the CAM table.
B). Evil twin is a wireless rogue AP attack, unrelated to switch behavior.

D). DNS spoofing redirects domain queries, not Layer 2 switching.
References (CompTIA Network+ N10-009):
Domain: Network Security - Switch security, CAM table attacks, MAC flooding.

質問: **141**
ある会社が最近、大量の帯域幅を使用するビデオ会議システムを導入しました。ユーザーから、インターネット速度が遅くなり、ネットワーク パフォーマンスが全体的に低下しているとの報告が寄せられています。ネットワーク パフォーマンスの問題の原因として最も可能性が高いのは次のうちどれですか (2 つ選択)。
A. DNS の設定ミス
B. ネットワークセキュリティが不十分
C. マルウェアまたはウイルス
D. 古いソフトウェア
E. QoS設定が正しくありません
F. ネットワーク輻輳
正解: **E,F (**コメントを発表する**)**
When high-bandwidth services like videoconferencing are introduced, two primary factors may degrade performance:
Incorrect QoS Settings (E):QoS (Quality of Service) is used to prioritize traffic. If not configured correctly, critical services like video may not get the necessary bandwidth and prioritization.
Network Congestion (F):Video services consume large amounts of data. If the network doesn't have sufficient bandwidth or is not segmented properly, congestion will slow down all services.
DNS misconfiguration (A) would affect name resolution, not bandwidth.
Malware (C) could degrade performance, but is not tied to the described scenario.
Outdated software (D) may affect performance in some cases, but not directly linked to network congestion in this case.
Inadequate network security (B) isn't likely to cause general slowness related to video traffic.
So, the most likely culprits are E. Incorrect QoS settings and F. Network congestion.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 2.5: "Explain common performance concepts and issues."

質問: **142**
ネットワークエンジニアがipconfigを実行し、デフォルトゲートウェイが0.0.0.0であることに気づきました。使用されているアドレスの種類は次のどれですか？
A. アピール
B. マルチキャスト
C. クラスC
D. 実験的
正解: **(**正解を表示します**)**
APIPA (Automatic Private IP Addressing) assigns an IP address in the range 169.254.x.x when a DHCP server cannot be contacted, and it sets the default gateway to 0.0.0.0 because APIPA is designed only for local communication within the same subnet. The document states:
"APIPA allows for automatic, ad hoc network communication within a single subnet when a DHCP server is not available. In this state, the default gateway is typically set to 0.0.0.0 because APIPA does not provide routing to other networks."

質問: **143**

最高情報責任者（CIO）は、プライマリサイトに障害が発生した後にのみ実行され、最新のバックアップをインポートするとすぐにオンラインに戻れるDRソリューションを望んでいます。次のDRサイトソリューションのうち、これらの要件を満たすものはどれですか？
A. 冷たい
B. 暖かい
C. アクティブ
D. ホット
正解: **B (**コメントを発表する**)**
Comprehensive and Detailed Explanation (aligned to N10-009):
A warm site is partially configured with necessary infrastructure and systems, but it requires recent backups to be restored before becoming fully operational. This provides a balance between cost and recovery time.
A). Cold site has only power and space, requiring full setup, which takes too long.
C). Active (active-active) runs simultaneously with the primary site, not only during failure.
D). Hot site is fully operational at all times and can take over immediately, but it's more expensive.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Disaster recovery sites (cold, warm, hot, active).

質問: **144**
顧客が新しいUTMデバイスを購入し、開発チームにデバイスのデータレポート機能の一部を社内のカスタムサポートソフトウェアに統合するよう依頼しました。開発チームは、デバイスのデータを取得するために、以下のどの機能を使用すべきでしょうか？
A. API
B. SNMPv2c
C. SIEM
D. MIB
正解: **(**正解を表示します**)**
An API (Application Programming Interface) is the best choice when a development team needs to integrate a device's reporting data directly into custom software. In Network+ (N10-009) objectives, network operations commonly include device management, monitoring, and automation, and APIs are a key method for programmatic access to operational data (often via REST/HTTPS with structured formats like JSON). This enables the internal support application to pull dashboards, health metrics, events, configuration details, and reporting outputs in a controlled, developer-friendly way.
SNMPv2c is primarily used for network monitoring and polling counters/alerts, but it is less secure (community strings) and is not as flexible for modern application integration as an API. A MIB is not a data- access "feature" by itself; it's the schema/definitions SNMP uses to describe managed objects. A SIEM is a separate security analytics platform that collects and correlates logs/events-useful for security operations, but not the direct interface a custom support tool would typically call to retrieve device reporting data.

質問: **145**
会社のセキュリティポリシーでは、リモート従業員の社内ノートパソコンからのすべてのネットワークトラフィックに会社のVPNを使用することが義務付けられています。このシナリオに最も適したネットワークアクセス方法は、次のうちどれですか？
A. クライアントレスVPN
B. フルトンネル
C. サイト間トンネル
D. スプリットトンネル
正解: **B (**コメントを発表する**)**

The correct answer is Full-tunnel because the policy requires all network traffic from remote corporate laptops to pass through the company's VPN. In a full-tunnel VPN configuration, once the VPN connection is established, all traffic-including internet-bound traffic-is routed through the corporate network before reaching its destination. This ensures centralized monitoring, content filtering, logging, and enforcement of security controls such as IDS/IPS and firewalls.
According to CompTIA Network+ (N10-009) security objectives, full-tunnel VPNs enhance security by preventing users from directly accessing the internet from their local connection, thereby reducing exposure to local network threats (e.g., public Wi-Fi attacks).
A split-tunnel VPN (Option D) allows users to access the internet directly while only sending corporate- bound traffic through the VPN, which does not meet the "all traffic" requirement.
A site-to-site tunnel (Option C) connects entire networks rather than individual remote users. A clientless VPN (Option A) typically provides web-based access without a full network tunnel and does not necessarily route all traffic.
Therefore, full-tunnel best matches the policy requirement.

質問: **146**
ネットワーク技術者が最近購入した商用スイッチのセキュリティ強化を試みています。公開情報の利用を最も効果的に軽減できるセキュリティ強化手法はどれですか？
A. デフォルトのパスワードの変更
B. 受信SSH接続をブロックしています
C. ネットワーク構成からゲートウェイを削除する
D. スイッチへの物理的なアクセスを制限する
正解: **(**正解を表示します**)**
Changing the default password is a fundamental step in device hardening, as default credentials are widely known and published online, posing a significant security risk if not updated. The document notes:
"Default passwords are often known by attackers and published on the internet. Changing them to unique, strong passwords is a critical first step in securing network devices against unauthorized access."

質問: **147**
管理者は、企業ネットワークで使用するために SNMP サーバーをセットアップしており、MIB 内にデバイス ID を作成する必要があります。MIB の機能について説明しているのは次のうちどれですか。
A. DHCPリレーデバイス
B. ポリシー適用ポイント
C. イベント変換の定義ファイル
D. ネットワーク アクセス コントローラ
正解: **(**正解を表示します**)**
* MIB (Management Information Base): A MIB is a database used for managing the entities in a communication network. The MIB is used by Simple Network Management Protocol (SNMP) to translate events into a readable format, enabling network administrators to manage and monitor network devices effectively.
* Function of MIB: MIBs contain definitions and information about all objects that can be managed on a network using SNMP. These objects are defined using a hierarchical namespace containing object identifiers (OIDs).
CompTIA Network+ materials discussing SNMP and MIB functionality.

質問: **148**
コネクションレス通信上のトランスポート層で発生する伝送形式を最もよく表すものはどれですか?
A. データグラム
B. セグメント

C. フレーム
D. パケット
正解: **A (**コメントを発表する**)**
At the transport layer, connectionless communication is typically handled using the User Datagram Protocol (UDP), which transmits data in units called datagrams. Unlike TCP, UDP does not establish a connection before sending data and does not guarantee delivery, making datagrams the correct term for the transmission format in this context. References: CompTIA Network+ Exam Objectives and official study guides.

質問: **149**
企業ネットワークのデータ帯域幅要件を削減するために使用するのに最適な VPN は次のどれですか?
A. スプリットトンネル
B. サイト間
C. フルトンネルクライアント
D. GREトンネル
正解: **A (**コメントを発表する**)**
A split-tunnel VPN allows a device to route some traffic through the VPN (typically corporate traffic) while sending other traffic (like general internet browsing) directly over the local internet connection. This reduces the load on the corporate network because not all traffic is routed through the VPN tunnel.
Site-to-site VPNs are for permanent links between locations.
Full-tunnel VPNs route all traffic through the VPN, increasing the bandwidth usage on the corporate network.
GRE (Generic Routing Encapsulation) is a tunneling protocol that doesn't encrypt and doesn't reduce bandwidth usage by itself.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.3 - Given a scenario, configure and deploy common VPN technologies.

質問: **150**
疑いを持たない攻撃者を誘い込み、攻撃者の活動を調査するために使用されるデバイスのグループを最もよく表すものはどれですか?
A. ジオフェンシング
B. ハニーネット
C. ジャンプボックス
D. スクリーンされたサブネット
正解: **(**正解を表示します**)**
A honeynet is a network of honeypots designed to attract and study attackers. Honeypots are decoy systems set up to lure cyber attackers and analyze their activities. A honeynet, being a collection of these systems, provides a broader view of attack methods and patterns, helping organizations improve their security measures. References: CompTIA Network+ Exam Objectives and official study guides.

質問: **151**
営業時間外にヘルプデスクに電話があり、デバイス上のファイルにアクセスできず、壁紙が変更されたと報告されました。ネットワーク管理者はこの問題は単発的なインシデントだと考えましたが、セキュリティアナリストはランサムウェア攻撃の可能性があると考えています。以下のトラブルシューティング手順のうち、最初に実行すべきものはどれですか？
A. 問題を特定します。
B. 理論を確立する。
C. 調査結果を文書化します。
D. 行動計画を作成します。

正解: **(**正解を表示します**)**
The correct answer is Identify the problem, which is always the first step in the CompTIA Network+ N10-009 troubleshooting methodology. Before forming theories, creating action plans, or documenting outcomes, technicians must clearly understand what is happening, who is affected, and what symptoms are present.
In this scenario, the symptoms-inaccessible files and a changed wallpaper-are serious and potentially indicative of a security incident such as ransomware. However, at this stage, there is disagreement between the network administrator and the security analyst regarding the nature of the issue. That reinforces the need to begin with problem identification, which includes gathering information, determining the scope of impact, identifying recent changes, and assessing whether the incident is isolated or widespread.
Establishing a theory comes after the problem has been clearly defined. Creating a plan of action and documenting findings occur later in the process, once the issue has been confirmed and remediation steps are determined. Jumping ahead without properly identifying the problem could result in delayed containment or an incorrect response-especially critical in potential security incidents.
The Network+ objectives emphasize following the structured troubleshooting process precisely to reduce risk, prevent escalation, and ensure accurate resolution-particularly when malware or ransomware may be involved.

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu **792**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **152**
ネットワーク管理者は、会社のサーバーが利用可能であることを確認するためにサーバーを監視しています。管理者はこのタスクに次のどれを使用する必要がありますか?
A. パケットキャプチャ
B. データ使用量レポート
C. SNMPトラップ
D. 構成監視
正解: **C (**コメントを発表する**)**
To monitor server availability, SNMP traps are the best choice. SNMP (Simple Network Management Protocol) allows devices to send alerts (traps) when certain conditions are met, such as server downtime or high resource usage.
Breakdown of Options:
A). Packet capture - Capturing packets provides insights into network traffic but does not actively monitor server availability.
B). Data usage reports - These analyze network traffic consumption but do not indicate whether a server is available or not.
C). SNMP traps - Correct answer. SNMP traps notify administrators of server issues in real time.
D). Configuration monitoring - This tracks configuration changes rather than availability.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.3: Explain network monitoring concepts.
RFC 1157: Simple Network Management Protocol (SNMP)

質問: **153**
HTTPS を使用する際に転送中の暗号化を実装するために最もよく使用されるのは次のどれですか。
A. SSH
B. TLS
C. SCADA

D. RADIUS
正解: **B (**コメントを発表する**)**
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
HTTPS is HTTP encapsulated in TLS (the successor to SSL), which provides confidentiality, integrity, and server authentication for web traffic.
* A. SSH secures remote shell and tunnels, not HTTPS.
* C. SCADA refers to industrial control systems, not a transport security protocol.
* D. RADIUS is an AAA protocol for authentication/authorization/accounting, not the web encryption layer.
References (CompTIA Network+ N10-009):
* Domain: Network Standards, Protocols, and Implementations - Web protocols (HTTP/HTTPS), TLS handshake and purpose, encryption in transit.

質問: **154**
ネットワーク管理者は、パフォーマンスを向上させるためにサーバーのアップグレードを実行し、新しい NIC をインストールしました。アップグレード後、ユーザーはサーバーにアクセスできなくなりました。最も考えられる理由は次のどれですか。
A. PoE 電力予算を超えました。
B. TX/RXが転置されました。
C. ポート セキュリティ違反が発生しました。
D. 間違ったケーブルタイプがインストールされました。
正解: **(**正解を表示します**)**
When a network administrator installs a new Network Interface Card (NIC) and users are unable to reach the server, one of the common issues is the use of an incorrect cable type. Network cables must match the specifications required by the NIC and the network infrastructure (e.g., Cat5e, Cat6 for Ethernet).
NIC Compatibility: The new NIC might require a specific type of cable to function properly. Using a cable not rated for the NIC's required speeds or capabilities can result in connectivity issues.
Cable Standards: Different NICs and network devices might need different cabling standards (straight-through vs. crossover cables, or specific fiber optic types).
Connection Types: Ensuring that the cable connectors are appropriate for the NIC ports (e.g., RJ45 for Ethernet, LC connectors for fiber optics).
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Discusses network cabling standards and NIC specifications.
Cisco Networking Academy: Provides insights into cabling and NIC configurations for optimal network performance.
Network+ Certification All-in-One Exam Guide: Offers comprehensive details on troubleshooting network connectivity issues, including cabling problems.

質問: **155**
顧客がヘルプデスクに電話をかけ、インターネット接続の問題を報告しました。顧客はローカルデータベースサーバーにアクセスできます。技術者が現場に赴き、設定を確認します。ユーザーの問題の原因は次のどれですか?
A. DNSが正しくありません
B. 到達できないゲートウェイ
C. ルートブリッジに障害が発生しました
D. アップストリームルーティングが不十分
正解: **(**正解を表示します**)**
The customer can access local resources (a database server), which means local networking is working.
However, the inability to reach the internet suggests an issue with the default gateway. If the default gateway is unreachable, packets will not be routed outside the local network.
Breakdown of Options:

A: Incorrect DNS - DNS issues would cause problems resolving domain names, but the user should still be able to access external resources via IP addresses.
B: Unreachable gateway - # Correct answer. If the default gateway is incorrect or unreachable, the device cannot route traffic to the internet.
C: Failed root bridge - STP (Spanning Tree Protocol) failures cause switching issues, but the user can still access local devices, meaning STP is not the problem.
D: Poor upstream routing - Would affect the entire network, not just one user.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.3: Explain network routing concepts.

質問: **156**
ネットワーク管理者が新しいネットワークハードウェアを導入しました。ネットワーク監視サーバーの設定中に、サーバーは認証はできましたが、ハードウェアの具体的な状態を特定できませんでした。管理者は、この問題を解決するために、次のうちどの方法を実行する可能性がありますか？
A. パブリックコミュニティ文字列を使用する
B. 適切なMIBをインポートする
C. スイッチポートアナライザーをセットアップしてトラフィックを転送する
D. SNMPv3プライバシーを設定する
正解: **(**正解を表示します**)**
MIBs (Management Information Bases) define the variables and objects that SNMP can query on a device. If the monitoring server authenticates but cannot interpret the data, it likely lacks the correct MIB for that vendor or model. Importing the proper MIB allows the monitoring server to correctly display device status and metrics.
A). Using a public community string is insecure and not related to missing MIBs.
C). Switchport analyzer (SPAN) captures traffic for packet analysis, not SNMP monitoring.
D). SNMPv3 privacy adds encryption but doesn't fix missing MIB interpretation.
References (CompTIA Network+ N10-009):
Domain: Network Operations - SNMP, MIBs, network monitoring systems.

質問: **157**
他の DR サイトと比較して、コールド DR サイトを維持することの最大の利点は次のどれですか。
A. 冗長性
B. 在庫状況
C. セキュリティ
D. コスト
正解: **(**正解を表示します**)**
Acold disaster recovery (DR) siteis a backup facility equipped withminimal infrastructure, often lacking active systems or real-time data replication. Itsgreatest advantage is cost-efficiency. Cold sites aremuch cheaperto maintain than warm or hot sites, which require continuous synchronization and operational readiness. They are used when low cost is more important than recovery speed.
Reference:Section 3.3 - Disaster Recovery Concepts - "Cold, Warm, and Hot Sites Comparison"

質問: **158**
ネットワーク管理者は、カバレッジが重複することが多い密集した環境に設置するアクセス ポイントを構成しています。2.4GHz スペクトルの干渉を最小限に抑えるために、管理者は次のどのチャネル幅を選択する必要がありますか。
A. 11MHz
B. 20MHz

C. 40MHz
D. 80MHz
E. 160MHz
正解: (正解を表示します)
Reference: CompTIA Network+ Certification Exam Objectives - Wireless Networks section.

質問: **159**
次のファイバー コネクタ タイプのうち、ネットワーク インターフェイス カードで使用される可能性が最も高いのはどれですか。
A. LC
B. SC
C. ST
D. MPO
正解: (正解を表示します)
* Definition of Fiber Connector Types:
* LC (Lucent Connector): A small form-factor fiber optic connector with a push-pull latching mechanism, commonly used for high-density applications.
* SC (Subscriber Connector or Standard Connector): A larger form-factor connector with a push- pull latching mechanism, often used in datacom and telecom applications.
* ST (Straight Tip): A bayonet-style connector, typically used in multimode fiber optic networks.
* MPO (Multi-fiber Push On): A connector designed to support multiple fibers (typically 12 or 24 fibers), used in high-density cabling environments.
* Common Usage:
* LC Connectors: Due to their small size, LC connectors are widely used in network interface cards (NICs) and high-density environments such as data centers. They allow for more connections in a smaller space compared to SC and ST connectors.
* SC and ST Connectors: These are larger and more commonly used in patch panels and older fiber installations but are less suitable for high-density applications.
* MPO Connectors: Primarily used for trunk cables in data centers and high-density applications but not typically on individual network interface cards.
* Selection Criteria:
* The small form-factor and high-density capabilities of LC connectors make them the preferred choice for network interface cards, where space and connection density are critical considerations.
References:
* CompTIA Network+ study materials on fiber optics and connector types.

質問: **160**
ネットワーク技術者は、別の問題に取り組んでいるときに新しいチケットを受け取ります。新しいチケットは業務運営にとって重要です。技術者は、どのチケットを最初に完了するかを判断するために、次のどのドキュメントを参照する必要がありますか?
A. NDA
B. AUP
C. サービスレベル保証
D. 覚書
正解: (正解を表示します)
AnSLA (Service Level Agreement)defines performance expectations, includingresponse time, prioritization, and resolution timefor services and support issues. It helps the technician determine which task hashigher priority based on business impact.
* A. NDA (Non-Disclosure Agreement)relates to confidentiality, not task prioritization.
* B. AUP (Acceptable Use Policy)defines user behavior, not issue handling.

* D. MOU (Memorandum of Understanding)outlines informal agreements and doesn't define ticket priorities.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 4.1 - Compare and contrast common documentation types.

質問: **161**
サイト間 VPN の最適な使用例は次のうちどれですか?
A. 信頼できないネットワークを介したアクセスのセキュリティ保護
B. 保存データの暗号化
C. 2つの内部サブネット間のトラフィックのフィルタリング
D. 会社のリソースを含む公開アプリケーションのホスティング
正解: **(**正解を表示します**)**
A site-to-site VPN is used to securely connect two networks over an untrusted network, most commonly the public internet. In Network+ (N10-009) objectives, VPNs are described as providing confidentiality and integrity for data in transit by creating an encrypted tunnel between sites (for example, headquarters and a branch office). This allows systems at both locations to communicate as if on the same private WAN, while preventing eavesdropping or tampering by intermediate networks. Typical implementations use IPsec tunneling and rely on negotiated encryption/authentication parameters to protect traffic end-to-end between VPN gateways.
Encrypting data at rest refers to storage encryption (disk/database), not VPN tunneling. Filtering traffic between two internal subnets is usually handled by ACLs, firewalls, or segmentation controls, not a site-to- site VPN. Hosting public-facing applications is a DMZ / reverse proxy / WAF design concern; a VPN is not the primary control for exposing public services (and generally you would not require the public to use a VPN to reach a public website). Therefore, securing site connectivity across an untrusted network is the best match.

質問: **162**
ログイン情報や属性など、ユーザーに関する機密情報をプロバイダーに渡すことによって機能する XML ベースのセキュリティ概念は次のどれですか。
A. 今すぐ
B. MFA
C. 半径
D. SAML
正解: **D (**コメントを発表する**)**
The correct answer is SAML (Security Assertion Markup Language). SAML is an XML-based standard used for single sign-on (SSO) and identity federation. It allows identity providers (IdPs) to share authentication and authorization data with service providers (SPs), passing secure tokens containing user attributes and credentials.
A). IAM (Identity and Access Management) is the broader framework, not specifically XML-based.
B). MFA enforces multiple factors for authentication but does not involve XML assertions.
C). RADIUS is an AAA protocol, but it uses UDP, not XML assertions.
SAML is widely used in federated identity systems, enabling secure authentication across different domains and applications without requiring multiple credentials.
References (CompTIA Network+ N10-009):
Domain: Network Security - Authentication methods, SAML, SSO.

質問: **163**
ネットワーク インターンがスイッチを接続した後、建物内の多数のユーザーの接続が失われました。
最も考えられる根本原因は次のどれですか?
A. VTP更新
B. ポートセキュリティの問題
C. LLDPの設定ミス

D. ネイティブVLANの不一致
正解: **D (**コメントを発表する**)**
When a switch is improperly connected to a network, it can cause widespread connectivity issues, especially if there's a misconfiguration in VLAN settings. A Native VLAN mismatch occurs when two switches connected via a trunk link have different native VLANs configured for untagged traffic. This can cause traffic to be sent to the wrong VLAN or dropped, resulting in connectivity loss for users.
Scenario Analysis: The intern likely connected the switch without ensuring that the trunk port's native VLAN matched the existing network configuration. This is a common issue in Cisco-based networks when trunk links are misconfigured.
Why not VTP update? VLAN Trunking Protocol (VTP) updates propagate VLAN configurations across switches. While a VTP misconfiguration could cause issues, it's less likely to immediately disrupt connectivity for many users unless the VTP server deleted critical VLANs, which is not implied here.
Why not Port security issue? Port security restricts access based on MAC addresses, typically affecting individual ports, not causing widespread outages.
Why not LLDP misconfiguration? Link Layer Discovery Protocol (LLDP) is used for device discovery, and misconfiguration is unlikely to cause a broad loss of connectivity.
Reference:CompTIA Network+ N10-009 Objective 2.2: Explain the purpose of network segmentation and VLAN configuration. The CompTIA Network+ Study Guide (e.g., Chapter 6: Switching) discusses VLAN trunking and the importance of matching native VLANs on trunk links to prevent connectivity issues. Native VLAN mismatches are highlighted as a common cause of network disruptions.

質問: **164**
ネットワーク管理者は、新しいコンピュータとアクセス ポイントを接続するために新しいケーブルを設置します。機器を導入した後、管理者はいくつかのデバイスが正しく接続されていないことに気付きました。管理者はデバイスを別のポートに移動しましたが、問題は解決しませんでした。管理者が次に確認する必要があるのは次のうちどれですか。
A. 電力予算
B. デバイス要件
C. ポートステータス
D. ケーブル終端
正解: **(**正解を表示します**)**
*Cable termination issues (e.g., improper crimping, loose connectors) can cause connectivity failures.
*Power budget (A) applies to PoE devices, not general cabling issues.
*Device requirements (B) relate to software/hardware compatibility, not wiring faults.
*Port status (C) would help if the issue was switch-related, but since moving devices didn't help, it's likely a cabling issue.
#Reference: CompTIA Network+ N10-009 Official Documentation - Cabling & Physical Layer Troubleshooting.

質問: **165**
組織には、すべてのネットワーク接続をユーザーまで追跡できるというセキュリティ要件があります。ネットワーク管理者は、ワイヤレス ネットワークに実装するソリューションを特定する必要があります。
次のどれが最善の解決策でしょうか?
A. エンタープライズ認証の実装
B. PSKの使用を要求する
C. ユーザー向けキャプティブポータルの設定
D. 有線と同等の保護の実施
正解: **(**正解を表示します**)**
Enterprise authentication (such as WPA2-Enterprise) utilizes unique credentials for each user, typically integrating with an authentication server like RADIUS. This allows for tracking and logging user activity, ensuring that all connections can be traced back to individual users. PSKs (Pre-Shared Keys) are shared among users and do not provide individual

accountability. Captive portals can identify users but are less secure than enterprise authentication, and Wired Equivalent Privacy (WEP) is outdated and not recommended for security purposes.
Reference:
CompTIA Network+ materials highlight enterprise authentication methods as the preferred solution for secure and accountable wireless network access.

質問: **166**
会社のビルのフロアにあるすべてのネットワーク ケーブルの中央終端ポイントを容易にするには、次のパネルのうちどれが最適ですか。
A. パッチ
B. UPS
C. 中質繊維板
D. ラック
正解: (正解を表示します)
Reference: CompTIA Network+ Certification Exam Objectives - Network Installation section.

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu **792**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **167**
ネットワーク セキュリティに最適なデバイス強化手法は次のどれですか? (2 つ選択してください)。
A. 未使用のポートを無効にする
B. 不正なデバイスの定期的なスキャンの実行
C. システムログの異常監視
D. SSOなどの論理セキュリティを有効にする
E. デフォルトのパスワードの変更
F. 最小権限の概念が確実に実施されるようにする
正解: (正解を表示します)
Disabling unused ports prevents unauthorized access and reduces the attack surface by ensuring that no inactive or unmonitored entry points are available for exploitation. Changing default passwords is critical for security because default credentials are widely known and can easily be exploited by attackers. These techniques are fundamental steps in hardening devices against unauthorized access and ensuring network security. References: CompTIA Network+ Exam Objectives and official study guides.

質問: **168**
ネットワークエンジニアは、需要の変化に応じてリソース割り当てを自動的に調整するようにアプリケーションサーバーを構成します。このサーバーは新しいアプリケーションをホストしますが、需要は予測できません。このシナリオは、以下のどの概念を示していますか？
A. スケーラビリティ
B. サービスとしてのソフトウェア
C. ハイブリッドクラウド
D. 弾力性

正解: **D (**コメントを発表する**)**
Elasticity is the ability of a system (often in cloud environments) to automatically scale resources up or down in real time based on demand.
A). Scalability means the ability to grow over time but not necessarily dynamically.
B). SaaS is a service model, not a resource-allocation concept.
C). Hybrid cloud is a deployment model, not a performance behavior.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Cloud computing, elasticity vs. scalability.

質問: **169**
ネットワークエンジニアが新しいリモートオフィスにスイッチを導入しています。スイッチにはホスト名とSTP優先度が事前に設定されています。以下の表に基づきます。
Switch Name
Priority
core-sw01
24576
access-sw01
28672
distribution-sw01
32768
access-sw02
36864
次のスイッチのうちどれがルート ブリッジになりますか?
A. core-sw01
B. access-sw01
C. distribution-sw01
D. access-sw02
正解: **(**正解を表示します**)**
The switch with the lowest STP priority becomes the root bridge.In the given table, core-sw01 has the lowest priority value of 24576. Therefore, it will be elected as the root bridge in the Spanning Tree Protocol topology.
Reference:Section 2.2 - Switching Technologies and Features - "Spanning Tree Protocol (STP)"

質問: **170**
ネットワーク管理者は、データセンター間で複数の接続が使用されるコアスイッチを設定する必要があります。以下の要件が与えられています。
耐障害性と冗長性
* ベンダー間の相互運用性
* 帯域幅の増加
* コスト効率
* 管理の簡素化
管理者は以下のうちどれを設定する必要がありますか？
A. スパニングツリー
B. インターフェース速度は最大10Gbps
C. リンク集約

D. ジャンボフレーム
正解: (正解を表示します)
The best answer is C. Link aggregation . The requirements point directly to combining multiple physical links into one logical connection. Link aggregation provides higher total bandwidth , supports redundancy if one member link fails, and simplifies administration because the bundle is managed as a single logical interface instead of several separate ones.
Another important clue is vendor interoperability . Standards-based link aggregation, such as LACP , is designed to work across different vendors when supported properly. That makes it a strong match for inter- data-center switch environments where equipment may not all come from the same manufacturer.
The other choices do not satisfy the full requirement list. Spanning tree helps prevent loops, but it can block redundant links instead of actively using them for extra bandwidth. Setting interface speeds to 10GB increases speed per port, but it does not by itself provide the logical bundling, simplified management, or redundancy benefits described. Jumbo frames can improve efficiency for some traffic types, but they are not the right answer for bandwidth aggregation and resilient uplinks.
Because the question asks for a solution that improves throughput, keeps redundancy, remains cost effective, and is easier to manage, link aggregation is the strongest fit.

質問: **171**
ネットワークエンジニアがIPアドレス192.168.123.232を持つNICを設定しています。このアドレスは次のうちどのクラスの例ですか？
A. クラスA
B. クラスB
C. クラスC
D. クラスD
正解: (正解を表示します)
The IPv4 address 192.168.123.232 falls within the Class C range under classful addressing. In classful terms, Class C addresses have a first octet from 192 to 223, which makes any address starting with 192.x.x.x a Class C address. Network+ (N10-009) networking concepts cover IPv4 addressing fundamentals and commonly reference class ranges as foundational knowledge, even though modern networks primarily use CIDR (classless) subnetting rather than strict classful boundaries.
This address is also within a well-known private IPv4 block: 192.168.0.0/16 (RFC1918 private addressing), which is frequently used for internal networks and NIC configurations where addresses are not routable on the public internet.
To eliminate the distractors: Class A uses first octet 1-126, Class B uses 128-191, and Class D (224-239) is reserved for multicast. Since the first octet here is 192, it maps to Class C, making option C correct.

質問: **172**
最近のセキュリティ評価中に、評価者は組織のヘルプデスクのふりをしてユーザーの資格情報を取得しようとしました。評価者は次のどの攻撃を使用していますか?
A. ソーシャルエンジニアリング
B. テールゲーティング
C. 肩越しに覗き見る
D. スミッシング
E. 邪悪な双子
正解: (正解を表示します)
This is a classic example ofsocial engineering, where an attacker manipulates individuals into giving up confidential information, such as credentials, by pretending to be someone trustworthy (like help desk staff).
* B. Tailgatinginvolves physical access without authentication.
* C. Shoulder surfingis spying over someone's shoulder to steal info.
* D. Smishingis phishing via SMS.
* E. Evil twininvolves a rogue Wi-Fi access point impersonating a legitimate one.
#Reference:

CompTIA Network+ N10-009 Official Objectives: 4.2 - Identify common security threats and vulnerabilities.

質問: **173**
従業員が新しいノートパソコンを購入し、無線ネットワークの使用時にパフォーマンスが遅いと報告しました。スイッチのファームウェアは前夜に更新されました。ネットワーク管理者がスイッチにログインすると、その従業員のスイッチインターフェースに以下の統計情報が表示されました。
98469パケット入力、1681937バイト、バッファなし0
1548 のブロードキャスト 25285 のマルチキャスト）を受信
65335 ランツ、0 ジャイアント、0 スロットル
入力エラー 11546 件、CRC 5 件、フレーム 0 件、オーバーラン 0 件、無視 0 件
ドリブル状態が検出された入力パケット数: 0
22781 パケット出力、858040 バイト、アンダーラン 0 件
出力エラー 0 件、衝突 89920 件、インターフェース リセット 0 件
0のバブル、0の遅い衝突、0の延期
キャリア紛失0、キャリアなし0
出力バッファ障害 0 件、スワップアウトされた出力バッファ 0 件
問題の原因として最も可能性が高いのは次のどれですか?
A. 壁のジャックからのパッチコードに障害があります。
B. スイッチポートの帯域幅を増やす必要があります。
C. スイッチでマルチキャストが正しく設定されていません。
D. NIC は半二重に設定されています。
正解: **D** (コメントを発表する)
A large number of collisions and input errors typically indicates a duplex mismatch, such as when one device is set to full duplex and the other to half duplex. This leads to communication issues and poor performance.
The document explains:
"Collisions and input errors are clear signs of duplex mismatches... typically caused when one device operates in half duplex while the other is in full duplex, causing performance and connectivity issues."

質問: **174**
ネットワーク管理者は、IPアドレスの無駄を最小限に抑えながら、新オフィス用のVLANを準備しています。新オフィスには約800台のワークステーションが設置される予定です。以下のネットワーク構成のうち、要件を満たすものはどれですか？
A. 10.0.100.0/22
B. 172.16.8.0/23
C. 172.16.15.0/20
D. 192.168.4.0/21
正解: (正解を表示します)
To support about 800 workstations with minimal IP waste, you choose the smallest subnet that provides at least 800 usable host addresses. In IPv4, usable hosts per subnet are calculated as 2^(host bits) # 2 (subtracting network and broadcast addresses). A /22 leaves 10 host bits (32 # 22 = 10), providing 2^10 # 2 =
1024 # 2 = 1022 usable addresses-enough for 800 devices with relatively low waste.
Check the other options: /23 leaves 9 host bits, giving 2^9 # 2 = 512 # 2 = 510 usable addresses, which is not enough. A /21 provides 2^11 # 2 = 2048 # 2 = 2046 usable addresses-enough, but wastes more than /22. A

/20 provides 2^12 # 2 = 4096 # 2 = 4094 usable addresses-much more waste.
Therefore, 10.0.100.0/22 is the best choice that meets the workstation requirement while minimizing unused addresses.

質問: **175**
セキュリティ監査中に、コンサルティング会社はドキュメントと実際の環境の間に不一致があることに気付きました。変更を行った人物と変更内容を記録できるのは、次のうちどれですか？
A. ネットワークアクセス制御
B. 構成監視
C. ゼロトラスト
D. Syslog
正解: **B (**コメントを発表する**)**
Configuration monitoring and management tools (often part of network management systems) maintain version-controlled records of device configurations, track changes, and log who made them. This provides accountability and supports compliance audits.
A). Network access control (NAC) manages endpoint access policies but does not track device config changes.
C). Zero Trust is a security framework requiring strict identity verification, not a configuration tracking tool.
D). Syslog collects system logs, but without a config monitoring system, it does not directly compare documentation to device state.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Change management, configuration management, auditing.

質問: **176**
ネットワーク管理者は、無線アクセスポイントをアップグレードし、デバイスの互換性に基づいて、ユーザーに高速化とチャネルの重複の低減を実現する構成を実装したいと考えています。この目標を達成するには、次のうちどれが適切でしょうか。
A. 802.1X
B. MIMO
C. ESSID
D. バンドステアリング
正解: **(**正解を表示します**)**
The best solution here is band steering. Band steering allows modern wireless access points to automatically direct dual-band capable clients toward the 5 GHz band instead of the crowded 2.4 GHz band. The 5 GHz band has more available non-overlapping channels and can provide faster speeds with less interference, especially in dense environments. Devices that only support 2.4 GHz will remain on that band, while compatible devices enjoy the improved performance of 5 GHz.
A). 802.1X is a port-based network access control method for authentication. While important for security, it does not affect wireless channel utilization or client throughput.
B). MIMO (Multiple Input, Multiple Output) is a technology that improves throughput by using multiple antennas to send/receive simultaneously, but it does not actively steer clients between frequency bands.
C). ESSID (Extended Service Set Identifier) is just the network name for a set of APs in the same WLAN; it has no role in optimizing performance by band.
By implementing band steering, administrators reduce channel overlap on the 2.4 GHz band, improve spectral efficiency, and provide higher performance to capable devices, directly meeting the requirements described in the scenario.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Wireless optimization, band steering, dual-band client management.

質問: **177**

ネットワーク エンジニアが新しい建物でワイヤレス インストールを完了しています。すべてのクライアントがサポートされている最速のネットワークに自動的に接続できることが要件です。この要件を最もよくサポートしているのは次のどれですか。
A. バンドステアリングを有効にする
B. 5GHz SSID を無効にする
C. キャプティブポータルの追加
D. MACフィルタリングの設定
正解: **A** (コメントを発表する)
Band steering is a feature in wireless networks that encourages dual-band capable devices to connect to the 5GHz band instead of the 2.4GHz band.
Why Band Steering?
The 5GHz band supports higher speeds and less interference compared to 2.4GHz.
If a device supports both bands, the access point (AP) can "steer" it to connect to 5GHz instead of 2.4GHz.
This helps ensure users always connect to the fastest available network.
Incorrect Options:
B). Disabling the 5GHz SSID: Would force devices onto 2.4GHz, which is slower and more congested.
C). Adding a Captive Portal: Used for guest authentication, not for speed optimization.
D). Configuring MAC Filtering: Used for security, not for optimizing network speed.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Wireless Technologies and Optimization

質問: **178**
ネットワーク アナリストが企業環境にワイヤレス ネットワークをインストールしています。従業員は、ドメイン ID と資格情報を使用して認証し、WLAN に接続する必要があります。要件を満たすために、アナリストは AP で次のどのアクションを実行する必要がありますか。
A. MAC セキュリティを有効にします。
B. ユーザーごとに PSK を生成します。
C. WPS を実装します。
D. WPA3 プロトコルを設定します。
正解: **D** (コメントを発表する)
WPA3-Enterprise provides strong security and supports authentication using domain identities through a RADIUS server and 802.1X authentication. This is the best choice for a corporate environment requiring user- based authentication.
WPA3-Enterprise Benefits:
Uses 802.1X with EAP (Extensible Authentication Protocol) to authenticate users via a directory service (e.g., Active Directory).
Eliminates shared passwords (PSK) for authentication.
Provides strong encryption and resistance to brute-force attacks.
Incorrect Options:
A). Enable MAC Security:
MAC filtering is not secure because MAC addresses can be spoofed.
B). Generate a PSK for Each User:
Pre-shared keys (PSK) are used in WPA-Personal, not in an enterprise setting.
Does not scale well in corporate environments.

C). Implement WPS:
Wi-Fi Protected Setup (WPS) is a vulnerable security method meant for home users.
Not suitable for enterprise authentication.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Wireless Security and Authentication

質問**: 179**
ストレージ ネットワークでは、送信されるデータ量に対するオーバーヘッドの削減と効率の向上が必要です。エンジニアがこれらの要件を満たすために構成する必要があるのは次のうちどれですか。
A. リンク速度
B. ジャンボフレーム
C. QoS
D. 802.1q タグ付け
正解**: (**正解を表示します**)**
Jumbo frames are Ethernet frames with a payload greater than the standard maximum transmission unit (MTU) of 1500 bytes. Configuring jumbo frames can reduce overhead and increase efficiency in storage networks by allowing more data to be sent in each frame, thus reducing the number of frames needed to transmit the same amount of data.
Reduced Overhead: By sending larger frames, the relative overhead for headers and acknowledgments is reduced.
Increased Efficiency: Larger frames mean fewer packets to process, leading to better utilization of network bandwidth and improved performance in high-throughput environments like storage networks.
Configuration: Requires support from all devices in the network path, including switches and network interface cards (NICs).
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Explains jumbo frames and their benefits in reducing network overhead.
Cisco Networking Academy: Provides training on network optimization techniques, including the use of jumbo frames.
Network+ Certification All-in-One Exam Guide: Covers advanced Ethernet features, including jumbo frames and their configuration for improved network performance.

質問**: 180**
ある企業が高密度環境でワイヤレス ソリューションを実装しています。企業がデバイスの飽和と集中化を懸念している場合、次の 802.11 標準のどれが使用されますか?
A. 802.11ac
B. 802.11ax
C. 802.11g
D. 802.11n
正解**: (**正解を表示します**)**
802.11ax, also known as Wi-Fi 6, is designed for high-density environments and improves device saturation and coverage compared to previous standards.
802.11ac: While it offers high throughput, it is not optimized for high-density environments as effectively as
802.11ax.
802.11ax (Wi-Fi 6): Introduces features like OFDMA, MU-MIMO, and BSS Coloring, which enhance performance in crowded environments, reduce latency, and increase the number of devices that can be connected simultaneously.
802.11g and 802.11n: Older standards that do not offer the same level of efficiency or support for high device density as 802.11ax.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Covers the 802.11 standards and their capabilities.
Cisco Networking Academy: Provides training on Wi-Fi technologies and best practices for high-density deployments.

Network+ Certification All-in-One Exam Guide: Discusses the various 802.11 standards and their applications in different environments.

質問: **181**
ネットワーク管理者は、SNMP を介してスイッチのリンク状態が変化したときに自動的にアラートが送信されるようにしたいと考えています。次の SNMP テクノロジーのうち、このアラートを実現できるのはどれですか？
A. トラップ
B. オブジェクト識別子
C. 文字列
D. MIB
正解: **(**正解を表示します**)**
The right answer is A. Trap . In SNMP, a trap is an unsolicited notification sent from a managed device to the management system when a significant event happens. A switch detecting that an interface has gone up or down is a textbook example of the kind of event that can trigger this kind of message.
That is different from normal SNMP polling, where the monitoring server asks the device for status information on a schedule. With a trap, the device does not wait to be asked. It sends the alert immediately, which makes it useful for link failures, threshold violations, and other time-sensitive conditions.
The other choices are related to SNMP, but not in the same way. An object identifier (OID) points to a specific managed value. A string is commonly associated with SNMP community information in older versions. A MIB is the structured database of manageable objects. None of those are the actual alerting mechanism.
Because the question asks for an automatic alert when link status changes, the feature being described is clearly an SNMP trap .

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu **792**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **182**
次のどれが実装時にセキュリティ機能も提供できますか?
A. NAT
B. BGP
C. FHRP
D. EIGRP
正解: **(**正解を表示します**)**
NAT (Network Address Translation) helps hide internal IP addresses from external networks, adding a layer of security by preventing direct access to internal systems from the outside.

質問: **183**
ネットワーク管理者は、一部のスイッチ ポートに予想よりも多くのエラーが発生していると判断しました。管理者は、これらのポートに関連付けられているケーブル配線をトレースします。エラーの原因として最も可能性が高いのは次のどれですか。
A. ipconfig
B. トレース
C. アルペジオ

D. nmap
正解: (正解を表示します)

質問: **184**
ジュニアネットワーク管理者が、会社のドメイン登録業者を装った番号からテキストメッセージを受け取ります。
管理者は騙されてグローバル管理者の資格情報を提供してしまいます。次のどの攻撃が行われていますか？
A. DNSポイズニング
B. ARPスプーフィング
C. ヴィッシング
D. スミッシング
正解: (正解を表示します)
Smishing (SMS phishing) occurs when attackers send fraudulent text messages pretending to be a trusted source, tricking the victim into giving up sensitive credentials. Since this came via text message, it qualifies as smishing.
A). DNS poisoning corrupts name resolution.
B). ARP spoofing manipulates MAC-to-IP mappings.
C). Vishing is phishing via voice calls, not text.
References (CompTIA Network+ N10-009):
Domain: Network Security - Social engineering, phishing types (smishing, vishing, spear phishing).

質問: **185**
次の IP 送信タイプのうち、送信されるデータをすべて暗号化するものはどれですか?
A. 超能力
B. あぁ
C. GRE
D. UDP
E. TCP
正解: (正解を表示します)
Definition of ESP (Encapsulating Security Payload):
ESP is a part of the IPsec protocol suite used to provide confidentiality, integrity, and authenticity of data.
ESP encrypts the payload and optional ESP trailer, providing data confidentiality.
ESP Functionality:
ESP can encrypt the entire IP packet, ensuring that the data within the packet is secure from interception or eavesdropping. It also provides options for data integrity and authentication.
ESP operates in two modes: transport mode (encrypts only the payload of the IP packet) and tunnel mode (encrypts the entire IP packet).
Comparison with Other Protocols:
AH (Authentication Header): Provides data integrity and authentication but does not encrypt the payload.
GRE (Generic Routing Encapsulation): A tunneling protocol that does not provide encryption.
UDP (User Datagram Protocol) and TCP (Transmission Control Protocol): These are transport layer protocols that do not inherently provide encryption. Encryption must be provided by additional protocols like TLS/SSL.
Use Cases:
ESP is widely used in VPNs (Virtual Private Networks) to ensure secure communication over untrusted networks like the internet.

References:
CompTIA Network+ study materials on IPsec and encryption.

質問: **186**
ネットワークエンジニアが、IPv4とIPv6の両方のルーティングをサポートする必要がある社内ネットワークを設計しています。次のルーティングプロトコルのうち、IPv4とIPv6の両方をサポートできるのはどれですか？
A. OSPFv3
B. RIPv2
C. BGP
D. EIGRP
正解: **D (**コメントを発表する**)**
EIGRP(Enhanced Interior Gateway Routing Protocol) supports bothIPv4 and IPv6. While OSPFv3 is specific to IPv6 and RIPv2 only supports IPv4, EIGRP was extended to handle dual-stack environments efficiently.
Reference:Section 2.1 - Characteristics of Routing Technologies - "EIGRP"

質問: **187**
あるユーザーが営業時間外にヘルプデスクに電話をかけ、デバイス上のファイルにアクセスできず、壁紙が変更されたと訴えました。ネットワーク管理者はこの問題は単発的なインシデントだと考えていますが、セキュリティアナリストはランサムウェア攻撃の可能性があると考えています。以下のトラブルシューティング手順のうち、最初に実行すべきものはどれですか？
A. 問題を特定する
B. 理論を確立する
C. 発見事項を文書化する
D. 行動計画を作成する
正解: **A (**コメントを発表する**)**
The first step in any troubleshooting process is to identify the problem. This includes gathering information from the user, reviewing logs, and observing the symptoms. In this case, identifying the scope and nature of the issue (e.g., signs of ransomware) is critical before forming any theories or plans.
From Andrew Ramdayal's guide:
"The troubleshooting methodology begins with identifying the problem. This step involves questioning users, identifying user changes, and determining the symptoms."

質問: **188**
ある組織は、無線ネットワークを用いた効果的なカバレッジの確保に苦慮しています。組織は、施設内のどこにいても継続的な接続を可能にするソリューションを導入したいと考えています。最適なカバレッジを確保するために、ネットワーク管理者は次のうちどれを提案すべきでしょうか？
A. 追加のアドホックアクセスポイントの実装
B. ユーザー接続用のイーサネットドロップを増やす
C. 建物内にメッシュネットワークを展開する
D. Wi-Fiの現在の周波数を変更する
正解: **(**正解を表示します**)**
The correct answer is deploying a mesh network. A mesh wireless network uses multiple interconnected access points that automatically route traffic through the best available path. This ensures seamless coverage throughout a facility, even when users move between APs. Mesh APs can extend coverage without requiring each AP to be directly wired, making them ideal for large or hard-to-wire environments.

A). Ad hoc access points are peer-to-peer connections and cannot provide enterprise-grade continuous coverage.
B). Ethernet drops provide wired connectivity but do not solve wireless coverage issues.
D). Changing the frequency (from 2.4 GHz to 5 GHz or vice versa) may reduce interference but will not guarantee building-wide seamless connectivity.
Mesh networks are particularly effective in environments with roaming devices (smartphones, tablets, handheld scanners) and ensure that there are no dead spots, thereby delivering continuous wireless access.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Wireless architectures, mesh networking, seamless connectivity.

質問**: 189**
ネットワーク技術者が複数のVLANを備えたスイッチを実装します。クライアントが他のVLANのクライアントと通信できるようにするには、技術者は次のうちどれを設定する必要がありますか？
A. VPC
B. VXLAN
C. ACL
D. SVI
正解**: (**正解を表示します**)**
To enable communication between VLANs, the technician must configure inter-VLAN routing. On a Layer 3 switch, this is commonly done by creating an SVI (Switched Virtual Interface) for each VLAN. An SVI provides a virtual Layer 3 interface with an IP address that acts as the default gateway for hosts in that VLAN.
Once SVIs exist and routing is enabled, the switch can route traffic between VLAN subnets internally, allowing clients in different VLANs to communicate (subject to any security controls). This aligns with Network+ (N10-009) infrastructure objectives covering VLANs, Layer 2/Layer 3 switching, and the requirement for routing to cross broadcast domains.
ACLs can permit or deny inter-VLAN traffic, but they do not create the routing function by themselves.
VXLAN is an overlay tunneling technology used mainly in data centers to extend Layer 2 networks over Layer 3 fabrics, not the standard solution for basic VLAN-to-VLAN connectivity on a switch. VPC is not the required configuration element for inter-VLAN routing in this context. Therefore, configuring SVIs is the correct and most direct answer.

質問**: 190**
次のプロトコルのうち、TCP ポート 443 に一般的に関連付けられているものはどれですか。
A. Telnet
B. SMTP
C. HTTPS
D. SNMP
正解**: C (**コメントを発表する**)**
TCP port 443 is reserved for HTTPS (Hypertext Transfer Protocol Secure), which uses TLS encryption to secure web traffic. It is the standard port for encrypted web communications.
A). Telnet uses TCP port 23.
B). SMTP commonly uses TCP ports 25, 465, or 587.
D). SNMP typically uses UDP ports 161 (queries) and 162 (traps).
References (CompTIA Network+ N10-009):
Domain: Network Standards, Protocols, and Implementations - Common ports and services.

質問**: 191**
サポート エージェントは、リモート ユーザーの有線デバイスが頻繁に切断され、速度が遅いという報告を受け取ります。調査の結果、サポート エージェントは、ユーザーの同軸モデムの信号電力が -97 dB であることを確認しました。

A. 回線に接続されているスプリッターを削除する
B. デバイスをワイヤレスに切り替える
C. デバイスを現代のものに近づける
D. ネットワーク速度を下げる
正解: (正解を表示します)
A signal power of -97dB indicates a very weak signal, which can cause connectivity issues and slow speeds.
Splitters on a coaxial line can degrade the signal quality further, so removing them can help improve the signal strength and overall connection quality.
* Signal Quality: Splitters can reduce the signal strength by dividing the signal among multiple lines, which can be detrimental when the signal is already weak.
* Direct Connection: Ensuring a direct connection from the modem to the incoming line can maximize signal quality and reduce potential points of failure.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses troubleshooting connectivity issues and the impact of signal strength on network performance.
* Cisco Networking Academy: Provides insights on maintaining optimal signal quality in network setups.
* Network+ Certification All-in-One Exam Guide: Covers common network issues, including those related to signal degradation and ways to mitigate them.

質問: **192**
ある会社が新しい IPS をインストールした後、ネットワークの速度が低下しています。ネットワーク管理者は問題のトラブルシューティングを行い、速度テストを実行します。さまざまなネットワークの場所からの結果は次のとおりです。
場所スピードダウンスピードアップ
ワイヤレス ラップトップ4.8 Mbps47.1 Mbps
有線デスクトップ5.2 Mbps49.3 Mbps
ファイアウォール48.8 Mbps49.5 Mbps
最も可能性の高い問題はどれですか?
A. パケット損失
B. ボトルネック
C. チャネルの重複
D. ネットワークの混雑
正解: (正解を表示します)
Bottlenecking occurs when a device in the network (such as an IPS) cannot process traffic efficiently, resulting in a dramatic drop in throughput. The significant difference between the firewall's speed (48.8 Mbps down) and the end-user devices' speeds (4.8 - 5.2 Mbps down) indicates a bottleneck caused by the IPS.
*Why not the other options?
*Packet loss (A) - Would typically cause connection timeouts, not just slow speeds.
*Channel overlap (C) - Affects only wireless networks, but the wired desktop is also experiencing slow speeds.
*Network congestion (D) - Would show fluctuations in both upload and download speeds, but upload speeds remain unaffected.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 13: Network Performance Optimization

質問: **193**
ある組織が DNS サーバーを新しい IP アドレスに移動しました。この移動後、顧客は組織の Web サイトにアクセスできなくなります。次の DNS エントリのうち、更新する必要があるのはどれですか。
A. AAAA

B. CNAME
C. MX
D. NS
正解: (正解を表示します)
When an organization moves its DNS servers to new IP addresses, the NS (Name Server) records must be updated. The NS record defines which DNS servers are authoritative for a domain. Ifthese records still point to the old IP addresses, clients will continue to query the outdated servers, leading to connectivity issues.
Breakdown of Options:
A). AAAA - This record maps a domain name to an IPv6 address. Since the issue is with DNS resolution, not IP versioning, this is incorrect.
B). CNAME - A CNAME (Canonical Name) record is used for domain aliasing, not for defining authoritative name servers.
C). MX - Mail Exchange (MX) records direct email traffic to the correct mail server, which does not impact general website accessibility.
D). NS - Correct answer. NS records must be updated to reflect the new authoritative DNS servers.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.3: Explain the purpose and properties of DNS records.
RFC 1035: Domain Names - Implementation and Specification

質問: **194**
ネットワークエンジニアは、無線カバレッジを改善するためにAPを追加しました。しかし、ユーザーから接続が切断と再接続を繰り返すという報告が寄せられています。この問題の原因は次のどれでしょうか？
A. スループット容量
B. ローミングの設定ミス
C. チャネルの重複
D. パケット損失
正解: (正解を表示します)
Adding more access points can improve coverage, but it also increases the risk of co-channel interference if APs are configured on the same or overlapping channels. Channel overlap causes contention and interference, leading to retries, unstable performance, and symptoms that feel like frequent disconnect/reconnect events- especially in dense deployments. Network+ (N10-009) wireless troubleshooting objectives highlight proper channel planning (non-overlapping channels, appropriate channel width) as critical when increasing AP density. If adjacent APs are competing on the same channel (or overlapping channels in 2.4 GHz), clients may experience poor signal-to-noise ratios and repeated reassociations as they struggle to maintain a stable link.
Roaming misconfiguration can cause sticky clients or poor handoffs, but the classic problem introduced immediately after "adding more APs" is interference from bad channel design. Throughput capacity is about available bandwidth and airtime efficiency; it can make things slow, but it doesn't inherently cause repeated disconnect/reconnect loops like interference does. Packet loss is a symptom that may occur due to interference, but the root cause in the options that best fits the scenario is channel overlap.

質問: **195**
ネットワーク管理者は、ネットワーク内の 2 つのレイヤー 2 スイッチを接続しています。これらのスイッチは、複数のネットワークでデータを転送する必要があります。次のどれがこの要件を満たしますか。
A. ジャンボフレーム
B. 802.1Q タグ付け
C. ネイティブVLAN
D. リンクアグリゲーション
正解: (正解を表示します)

802.1Q tagging, also known as VLAN tagging, is used to identify VLANs on a trunk link between switches.
This allows the switches to transfer data for multiple VLANs (or networks) over a single physical connection.
This method ensures that traffic from different VLANs is properly separated and managed across the network.
References: CompTIA Network+ study materials.

質問**: 196**
次のどれが法律によって施行されますか?
A. AUP
B. GDPR
C. 行動規範
D. EULA
正解**: B (**コメントを発表する**)**
GDPR (General Data Protection Regulation)is alegal frameworkenforced by the European Union to protect personal data and privacy. Unlike internal organizational policies such as AUPs or codes of conduct, GDPR is alegislated regulation, and organizations must comply or face legal consequences.
Reference:Section 4.1 - Basic Network Security Concepts - "GDPR and Compliance Regulations"

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu
792問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問**: 197**
ユーザーは、リモート ファイル サーバーにアクセスできなくなったことをネットワーク管理者に通知します。ネットワーク管理者はサーバーに ping を実行し、現在のファイア ウォール ルールがネットワーク ファイル共有へのアクセスをブロックしていないことを確認します。次のツールのうち、リモート ファイル サーバーで開いているポートを識別するのに役立つものはどれですか。
A. 掘る
B. Nmap
C. トレース
D. nslookup
正解**: (**正解を表示します**)**
Nmap (Network Mapper) is a powerful network scanning tool used to discover hosts and services on a computer network. It can be used to identify which ports are open on a remote server, which can help diagnose access issues to services like a remote file server.
* Port Scanning: Nmap can perform comprehensive port scans to determine which ports are open and what services are running on those ports.
* Network Discovery: It provides detailed information about the host's operating system, service versions, and network configuration.
* Security Audits: Besides troubleshooting, Nmap is also used for security auditing and identifying potential vulnerabilities.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Covers network scanning tools and their uses.
* Nmap Documentation: Official documentation provides extensive details on how to use Nmap for port scanning and network diagnostics.
* Network+ Certification All-in-One Exam Guide: Discusses various network utilities, including Nmap, and their applications in network troubleshooting.

質問: **198**
ある企業は、一般公開されている会議室のネットワークジャックから一般人が会社のサーバーにアクセスできることを懸念しています。この脆弱性を軽減する最善の方法は次のうちどれですか？
A. 信頼ゾーンを作成します。
B. 使用されていないサービスを無効にします。
C. MAC フィルタリングを使用します。
D. 802.1X を実装します。
正解: **(**正解を表示します**)**
The best mitigation is implementing 802.1X, which provides port-based Network Access Control (NAC).
With 802.1X enabled on access switch ports, a device plugged into a wall jack cannot gain normal network access until it successfully authenticates using credentials/certificates via an authentication server (commonly RADIUS). This directly addresses the threat of unauthorized users plugging into publicly accessible conference room jacks, because the switch keeps the port in an unauthenticated state (or places it into a restricted/guest VLAN) until authentication succeeds. This aligns with Network+ security objectives that emphasize controlling access at the edge, enforcing authentication, and reducing the risk of rogue or unmanaged devices on internal networks.
MAC filtering is weaker because MAC addresses can be spoofed and managing allow-lists at scale is error- prone. Creating a trusted zone is vague and does not prevent initial port access; segmentation helps limit blast radius but doesn't enforce authentication at the jack. Disabling unused services is a general hardening practice, but it does not stop someone from connecting physically to an active switch port and attempting access. 802.1X is purpose-built for this exact scenario.

質問: **199**
次のデバイスのうち、OSI モデルの複数のレイヤーで動作できるのはどれですか?
A. ハブ
B. スイッチ
C. トランシーバー
D. モデム
正解: **(**正解を表示します**)**
* Understanding Switches:
* Layer 2 (Data Link Layer): Traditional switches operate primarily at Layer 2, where they use MAC addresses to forward frames within a local network.
* Layer 3 (Network Layer): Layer 3 switches, also known as multilayer switches, can perform routing functions using IP addresses to forward packets between different networks.
* Capabilities of Multilayer Switches:
* VLANs and Inter-VLAN Routing: Multilayer switches can handle VLAN (Virtual Local Area Network) configurations and perform inter-VLAN routing, enabling communication between different VLANs.
* Routing Protocols: They can run routing protocols like OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) to manage traffic between networks.
* Comparison with Other Devices:
* Hub: Operates only at Layer 1 (Physical Layer) and simply repeats incoming signals to all ports.
* Transceiver: Also operates at Layer 1, converting electrical signals to optical signals and vice versa.
* Modem: Primarily operates at Layer 1 and Layer 2, modulating and demodulating signals for transmission over different types of media.
* Practical Application:
* Multilayer switches are commonly used in enterprise networks to optimize performance and manage complex routing and switching requirements within a single device.
References:
* CompTIA Network+ study materials on network devices and the OSI model.

質問: **200**
ネットワーク管理者は、音声トラフィックとデータ トラフィックを分離するために、レイヤー 3 対応デバイス上に SVI を作成する必要があります。このユース ケースを最もよく説明するのは次のどれですか。
A. 論理ポートをトランキングするために使用される物理インターフェース
B. 管理アクセスに使用される物理インターフェース
C. VLANのルーティングに使用される論理インターフェース
D. 物理ポート数が不足している場合に使用される論理インターフェース。
正解: **(**正解を表示します**)**
An SVI (Switched Virtual Interface) is a logical interface on a Layer 3-capable switch used to route traffic between VLANs. This is particularly useful in environments where voice and data traffic need to be separated, as each type of traffic can be assigned to different VLANs and routed accordingly.
* SVI (Switched Virtual Interface): A virtual interface created on a switch for inter-VLAN routing.
* VLAN Routing: Enables the routing of traffic between VLANs on a Layer 3 switch, allowing for logical separation of different types of traffic, such as voice and data.
* Use Case: Commonly used in scenarios where efficient and segmented traffic management is required, such as in VoIP implementations.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses VLANs, SVIs, and their applications in network segmentation and routing.
* Cisco Networking Academy: Provides training on VLAN configuration and inter-VLAN routing using SVIs.
* Network+ Certification All-in-One Exam Guide: Covers network segmentation techniques, including the use of SVIs for VLAN routing.

質問: **201**
管理者は、顧客がアクセスできるオフィスのエリアに設置されるスイッチを設定しています。管理者が不明なデバイスがネットワークに接続するのを防ぐための最適な方法は、次のうちどれですか。
A. 南南東
B. ACL
C. 境界ネットワーク
D. 802.1x
正解: **D (**コメントを発表する**)**
802.1x is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. This ensures that only authorized devices can access the network, making it ideal for mitigating the risk of unknown devices connecting to the network, especially in accessible areas.
802.1x Authentication: Requires devices to authenticate using credentials (e.g., username and password, certificates) before gaining network access.
Access Control: Prevents unauthorized devices from connecting to the network, enhancing security in public or semi-public areas.
Implementation: Typically used in conjunction with a RADIUS server to manage authentication requests.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Covers 802.1x and its role in network security.
Cisco Networking Academy: Provides training on implementing 802.1x for secure network access control.
Network+ Certification All-in-One Exam Guide: Explains the benefits and configuration of 802.1x authentication in securing network access.

質問: **202**
小規模オフィスに新しい 6E ワイヤレス ルーターを設置した後、技術者は一部のワイヤレス デバイスが定格速度を達成できないことに気付きました。
技術者が問題を解決するために確認すべき項目は次のうちどれですか? (2 つ選択)

A. 気象現象
B. 干渉レベル
C. 電圧源の要件
D. クライアントデバイスの互換性
E. バックエンドケーブル配線
F. 処理能力
正解: (正解を表示します)

質問: **203**
ネットワークエンジニアが公共オフィスのネットワークポートを設定しています。セキュリティ強化のため、エンジニアは認証後にのみネットワーク接続を許可するポートを設定したいと考えています。エンジニアは次のセキュリティ機能のうちどれを使用すべきでしょうか？
A. ポートセキュリティ
B. 802.1X
C. MACフィルタリング
D. アクセス制御リスト
正解: (正解を表示します)
802.1X provides port-based Network Access Control (NAC). Ports remain in a blocked state until a device authenticates (usually with RADIUS). This is ideal for public or semi-public areas where ports should not be
"always on."
A). Port security restricts by MAC addresses but does not authenticate users.
C). MAC filtering is easily spoofed and weaker than 802.1X.
D). ACLs filter traffic but do not enforce port-based authentication.
References (CompTIA Network+ N10-009):
Domain: Network Security - NAC, 802.1X authentication, port-based security.

質問: **204**
次のレイヤ 1 デバイスのうち、SFP 対応スイッチ上の光ファイバ接続の終端を担当するものはどれですか。
A. トランシーバー
B. モデム
C. イーサネット NIC
D. リピーター
正解: (正解を表示します)
A transceiver is the correct answer because it is the Layer 1 (Physical Layer) component that physically terminates and converts fiber-optic signals on an SFP-capable switch. In CompTIA Network+ N10-009 objectives, transceivers-such as SFP, SFP+, QSFP, and QSFP+ modules-are explicitly identified as physical interface components that handle signal transmission and reception. These modules convert electrical signals from the switch into optical signals for fiber cabling (and vice versa), enabling communication over different media types and distances.
A modem is also a Layer 1 device, but its purpose is to modulate and demodulate signals for WAN technologies such as DSL or cable-it does not terminate fiber connections on switches. An Ethernet NIC provides network access for end devices like computers and servers and typically terminates copper Ethernet, not modular fiber interfaces on switches. A repeater regenerates and amplifies signals to extend cable distances but does not provide fiber termination or media conversion at a switch port.

According to Network+ standards, SFP transceivers are essential for flexible network design, allowing administrators to select appropriate fiber types (single-mode or multi-mode), wavelengths, and distances while remaining compliant with physical layer requirements.

質問: **205**
クラウドVMインスタンスへのアクセスを管理する機能を提供するものはどれですか？
A. インターネットゲートウェイ
B. 直接接続
C. ネットワークACL
D. セキュリティグループ
正解: **D (**コメントを発表する**)**

質問: **206**
顧客が最近新しいオフィスに移転したのですが、一部の壁プレートが機能しておらず、ラベルも適切に貼られていないことに気付きました。IDF 内の適切な配線を識別するには、次のツールのうちどれが最適ですか?
A. トナーとプローブ
B. ケーブルテスター
C. 視覚的障害ロケーター
D. ネットワークタップ
正解: **A (**コメントを発表する**)**
A toner and probe tool, also known as a tone generator and probe, is used to trace and identify individual cables within a bundle or to locate the termination points of cables in wiring closets and patch panels. It generates a tone that can be picked up by the probe, helping technicians quickly and accurately identify and label wall plates and wiring. This is the best tool for identifying proper wiring in the Intermediate Distribution Frame (IDF). References: CompTIA Network+ Exam Objectives and official study guides.

質問: **207**
次のどれがクラウド環境への専用リンクに最も密接に関連し、暗号化を含まない可能性がありますか?
A. 直接接続
B. インターネットゲートウェイ
C. キャプティブポータル
D. VPN
正解: **(**正解を表示します**)**
Direct Connect refers to a dedicated network connection between an on-premises network and a cloud service provider (such as AWS Direct Connect). This link bypasses the public internet, providing a more reliable and higher-bandwidth connection. It may not inherently include encryption because it relies on the security measures of the dedicated physical connection itself. In contrast, other options like VPN typically involve encryption as they traverse the public internet.
Reference:
CompTIA Network+ full course material indicates that Direct Connect type services offer dedicated, private connections which might not include encryption due to the dedicated and secure nature of the link itself.

質問: **208**
OSI モデルの次のレイヤーのうち、エンドツーエンドの暗号化を担当するのはどれですか?
A. プレゼンテーション

B. アプリケーション
C. セッション
D. 輸送
正解: (正解を表示します)
The correct answer is Presentation, which is Layer 6 of the OSI model. According to the CompTIA Network+ N10-009 objectives, the Presentation layer is responsible for data formatting, compression, and encryption, ensuring that data sent from the application layer of one system can be properly interpreted by the receiving system.
End-to-end encryption refers to encrypting data before transmission and decrypting it only at the final destination, preventing intermediaries from accessing the plaintext data. In the OSI model, this encryption and decryption function is logically placed at the Presentation layer, which sits between the Application and Session layers. This layer transforms data into a standardized format and applies security mechanisms such as encryption algorithms.
While modern implementations like TLS/SSL often operate across multiple layers in real-world networking stacks, the Network+ exam adheres to the conceptual OSI model when testing knowledge. From an OSI perspective, encryption is explicitly associated with the Presentation layer.
The Application layer provides network services to end-user applications, the Session layer manages session establishment and teardown, and the Transport layer focuses on segmentation, flow control, and reliability.
None of these layers are primarily responsible for encryption within the OSI framework.
CompTIA emphasizes understanding these conceptual responsibilities, making Presentation the correct and expected answer.

質問: **209**
技術者が理論を確認するために実行する必要があるトラブルシューティング方法論の次のステップはどれですか?
A. 問題が重複しています。
B. 症状を特定します。
C. 情報を収集します。
D. 変更内容を決定します。
正解: (正解を表示します)
To confirm a theory in the troubleshooting process, the technician should duplicate (replicate) the problem under controlled conditions. In the Network+ (N10-009) methodology, confirming a theory means validating that the suspected cause actually produces the observed symptoms. Replicating the issue helps ensure the technician is not chasing a coincidence, and it allows changes to be tested safely (for example, reproducing the issue with a specific user account, endpoint, cable, port, SSID, or configuration). If the problem can be duplicated, the technician can then try targeted actions to see whether the symptoms change in predictable ways-strengthening or disproving the hypothesis.
The other choices occur earlier as part of forming the theory. Identify the symptoms is an initial step to define the problem clearly. Gather information is part of the discovery phase-collect logs, error messages, topology details, and user observations. Determine any changes is also an early step used to correlate recent modifications (patches, new devices, config changes) with the onset of the issue. Those steps help create a theory; duplication helps confirm it before implementing a full fix.

質問: **210**
ネットワーク管理者は、ネットワークに 255 個の使用可能な IP アドレスを追加する必要があります。現在 /24 が使用されています。次のプレフィックスのどれがこのニーズを満たしますか?
A. /23
B. /25
C. /29
D. /32
正解: (正解を表示します)
A /23 subnet provides 512 total addresses, of which 510 are usable (subtracting 2 for network and broadcast addresses). This would satisfy the need for 255 additional addresses.

質問: **211**
IT マネージャーは、メッシュ ネットワークで 10 個のサイトを接続する必要があります。各サイトは、プロビジョニング時間を短縮して保護する必要があります。次のテクノロジのうち、この要件を最もよく満たすものはどれですか。
A. SD-WAN
B. VXLAN
C. VPN
D. NFV
正解: **(**正解を表示します**)**
* Definition of SD-WAN:
* Software-Defined Wide Area Network (SD-WAN) is a technology that simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism. It allows for centralized management and enhanced security.
* Benefits of SD-WAN:
* Reduced Provisioning Time: SD-WAN enables quick and easy deployment of new sites with centralized control and automation.
* Security: Incorporates advanced security features such as encryption, secure tunneling, and integrated firewalls.
* Scalability: Easily scales to accommodate additional sites and bandwidth requirements.
* Comparison with Other Technologies:
* VXLAN (Virtual Extensible LAN): Primarily used for network virtualization within data centers.
* VPN (Virtual Private Network): Provides secure connections but does not offer the centralized management and provisioning efficiency of SD-WAN.
* NFV (Network Functions Virtualization): Virtualizes network services but does not specifically address WAN management and provisioning.
* Implementation:
* SD-WAN solutions are implemented by deploying edge devices at each site and connecting them to a central controller. This allows for dynamic routing, traffic management, and security policy enforcement.
References:
* CompTIA Network+ course materials and networking solution guides.

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu **792**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **212**
ネットワーク管理者は、分類されたサービスとアプリケーションの優先順位付けを行うために、ネットワークトラフィックを管理しています。ネットワーク管理者は次のどのテクノロジーを使用すべきでしょうか？
A. 負荷分散
B. 生存時間
C. サービス品質
D. コンテンツ配信ネットワーク
正解: **(**正解を表示します**)**

Quality of Service (QoS) is used to prioritize certain types of traffic to ensure critical applications receive the bandwidth, low latency, and low jitter they need-especially during congestion. Network+ objectives cover QoS concepts such as classification, marking, queuing, and policing/shaping to manage how traffic is handled on interfaces and across links. If the requirement is to prioritize "classified services and applications," QoS policies can match traffic using ports, protocols, DSCP markings, VLAN tags, or application identifiers and then place that traffic into higher-priority queues or reserve bandwidth for it. Load balancing distributes traffic across multiple servers/paths but does not inherently prioritize one class of traffic over another on congested links. TTL (time to live) is an IP header field used to prevent routing loops and is unrelated to prioritization. A CDN improves content delivery and caching for distributed users, but it is not a traffic-prioritization mechanism within an organization's network. Therefore, QoS is the correct technology for prioritizing specific services and applications.

質問: **213**
X.509 証明書が最も一般的に関連付けられているテクノロジは次のどれですか。
A. PKI
B. VLAN tagging
C. LDAP
D. MFA
正解: **(**正解を表示します**)**
X).509 certificates are most commonly associated with Public Key Infrastructure (PKI). These certificates are used for a variety of security functions, including digital signatures, encryption, and authentication.
PKI: X.509 certificates are a fundamental component of PKI, used to manage encryption keys and authenticate users and devices.
Digital Certificates: They are used to establish secure communications over networks, such as SSL/TLS for websites and secure email communication.
Authentication and Encryption: X.509 certificates provide the means to securely exchange keys and verify identities in various applications, ensuring data integrity and confidentiality.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Covers PKI and the role of X.509 certificates in network security.
Cisco Networking Academy: Provides training on PKI, certificates, and secure communications.
Network+ Certification All-in-One Exam Guide: Explains PKI, X.509 certificates, and their applications in securing network communications.

質問: **214**
システム管理者は、2台のノートパソコンをWi-Fi経由でプリンタに接続する必要があります。オフィスにはアクセスポイントがなく、購入することもできません。この要件を満たす最適な無線ネットワークの種類は次のうちどれですか？
A. メッシュ
B. インフラストラクチャ
C. この
D. ポイントツーポイント
正解: **(**正解を表示します**)**
Comprehensive and Detailed Explanation (aligned to N10-009):
An ad hoc wireless network allows devices to connect directly to each other without an access point. This is suitable for small, temporary setups like two laptops and a printer.
A). Mesh requires multiple nodes forming a larger distributed network.
B). Infrastructure requires an AP, which is not available here.
D). Point-to-point is typically for long-distance wireless links between two fixed endpoints.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Wireless network types: infrastructure, ad hoc, mesh.

質問: **215**
ある企業で、管理されていないスイッチをネットワークに接続したユーザーに関連するインシデントが発生しました。
資産インベントリを実施せずに同様のインシデントを回避するために、企業が実装する必要があるテクノロジは次のどれですか?
A. スクリーンサブネット
B. 802.1X
C. MACフィルタリング
D. ポートセキュリティ
正解: **(正解を表示します)**
Port security is a Layer 2 security feature that restricts the number of devices connecting to a network switch port. It helps prevent unauthorized devices, such as an unmanaged switch, from being connected to the network.
How Port Security Works:
Limits the number of MAC addresses that can connect to a port.
Can shut down or restrict the port if an unauthorized device is detected.
Prevents users from plugging in unauthorized networking equipment (e.g., unmanaged switches, hubs).
Incorrect Options:
A: Screened Subnet: A screened subnet (DMZ) is used for isolating external-facing servers, not for controlling unauthorized network connections.
B: 802.1X: Provides authentication for devices but requires a RADIUS server, which is a more complex solution than port security.
C: MAC Filtering: Controls which MAC addresses can connect but is difficult to manage and can be spoofed.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Network Security Controls

質問: **216**
会社の本社と支店を安全に接続するには、次のどれを実装する必要がありますか?
A. スプリットトンネルVPN
B. クライアントレスVPN
C. フルトンネルVPN
D. サイト間VPN
正解: **D (コメントを発表する)**
Site-to-Site VPN: A site-to-site VPN is used to securely connect two networks, such as a company's headquarters and a branch location, over the internet. This type of VPN creates a secure tunnel for data transmission, ensuring confidentiality and integrity.
Split-tunnel VPN (A): Allows some traffic to bypass the VPN tunnel, which may not secure all communications.
Clientless VPN (B): Used for individual users to access the network without VPN client software.
Full-tunnel VPN (C): Typically used for individual user traffic rather than connecting two networks.
Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (Secure Network Connections).

質問: **217**
パススルー プラグを使用して Cat 8 ケーブルを配線した後、電気技師は接続されたケーブルでクロストークが頻繁に発生していることに気付きました。電気技師が最初に実行する必要があるトラブルシューティング手順は次のうちどれですか。
A. コネクタに接触または露出しているワイヤがないか検査します。
B. 接続されているデバイスのデフォルト設定を復元します。

C. 接続を再度終了します。
D. エリア内の無線周波数干渉を確認します。
正解: **A** (コメントを発表する)
Cross talk can often be caused by improper termination of cables. The first step in troubleshooting should be to inspect the connectors for any wires that might be touching or exposed. Ensuring that all wires are correctly seated and that no conductors are exposed can help reduce or eliminate cross talk. This step should be taken before attempting to re-terminate the connections or check for other sources of interference.References:
CompTIA Network+ study materials.

有効的な**N10-009J**問題集はJPNTest.com提供され、**N10-009J**試験に合格することに役に立ちます！JPNTest.comは今最新**N10-009J**試験問題集を提供します。JPNTest.com N10-009J試験問題集はもう更新されました。ここで**N10-009J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/N10-009J-mondaishu **792**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」