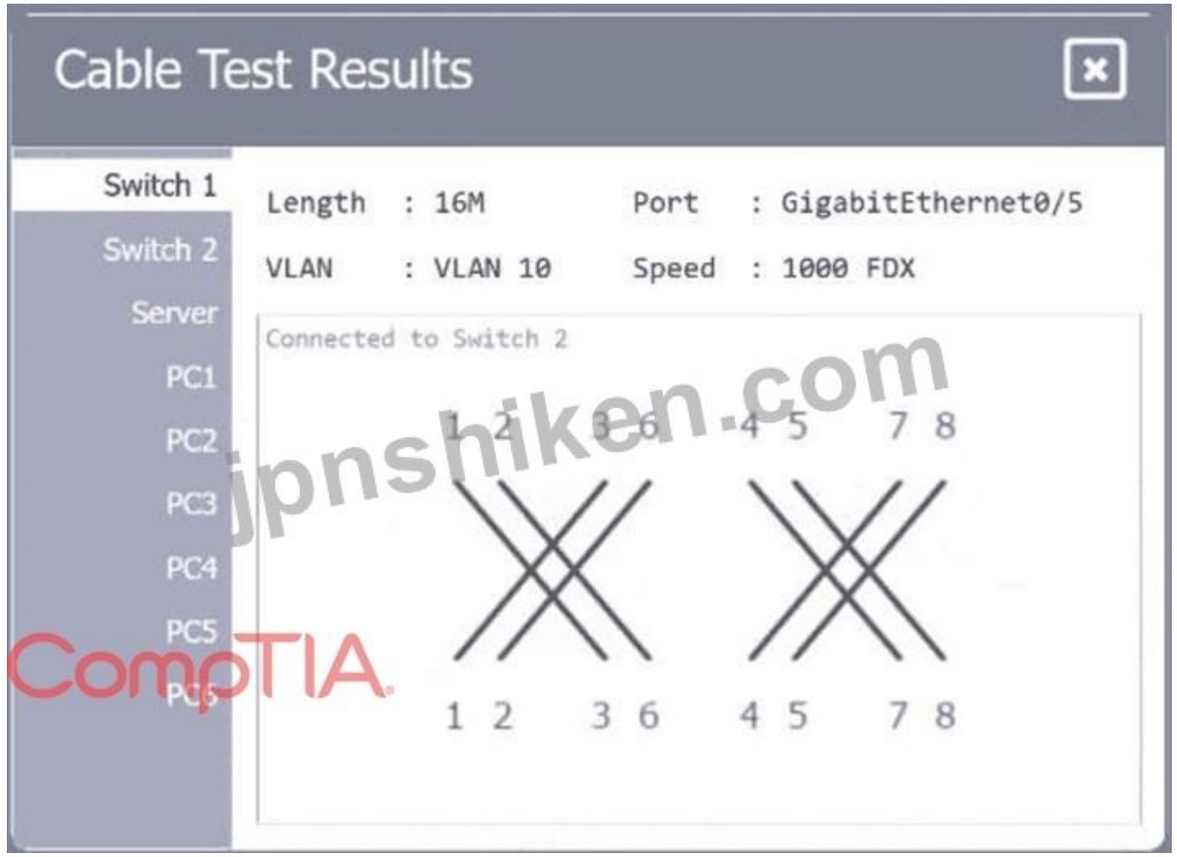
CompTIA.N10-009J.v2026-10-24.q226

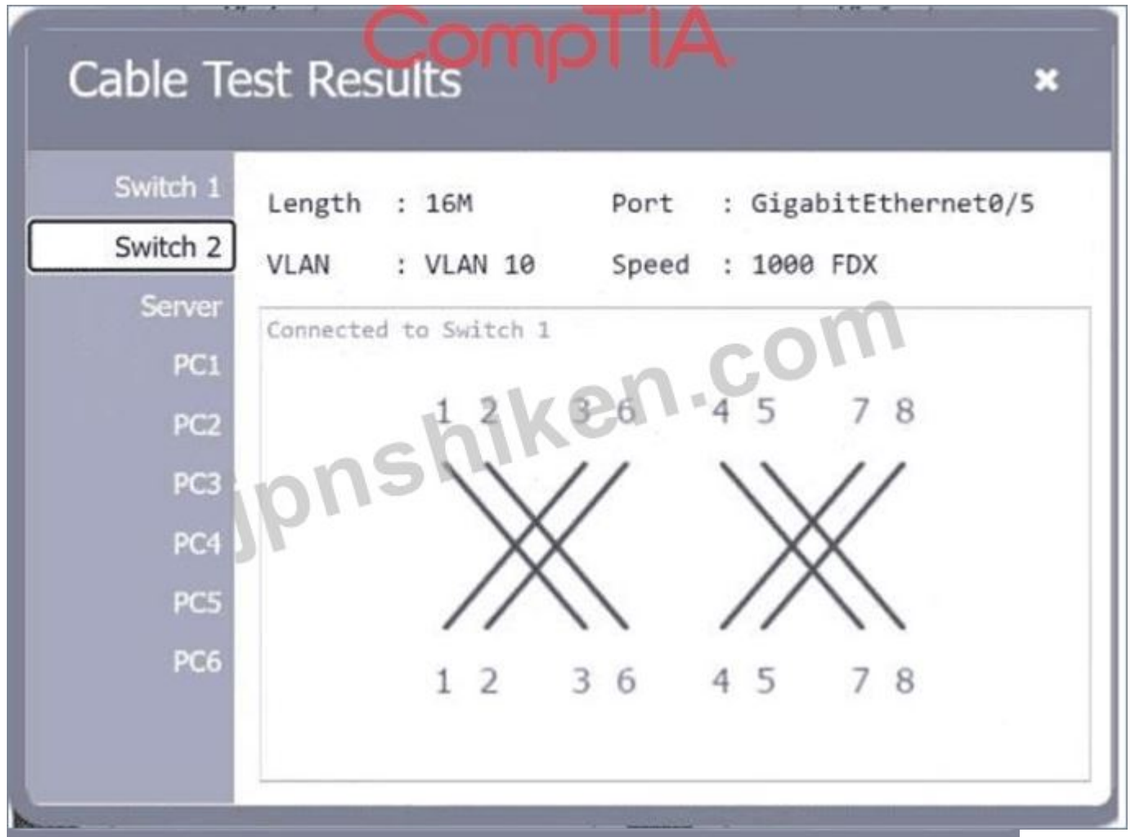
試験コード：	N10-009J
試験名称：	CompTIA Network+ Certification Exam (N10-009日本語版)
認証ベンダー：	CompTIA
無料問題の数：	226
バージョン：	v2026-10-24
ページの閲覧量：	102
問題集の閲覧量：	2300

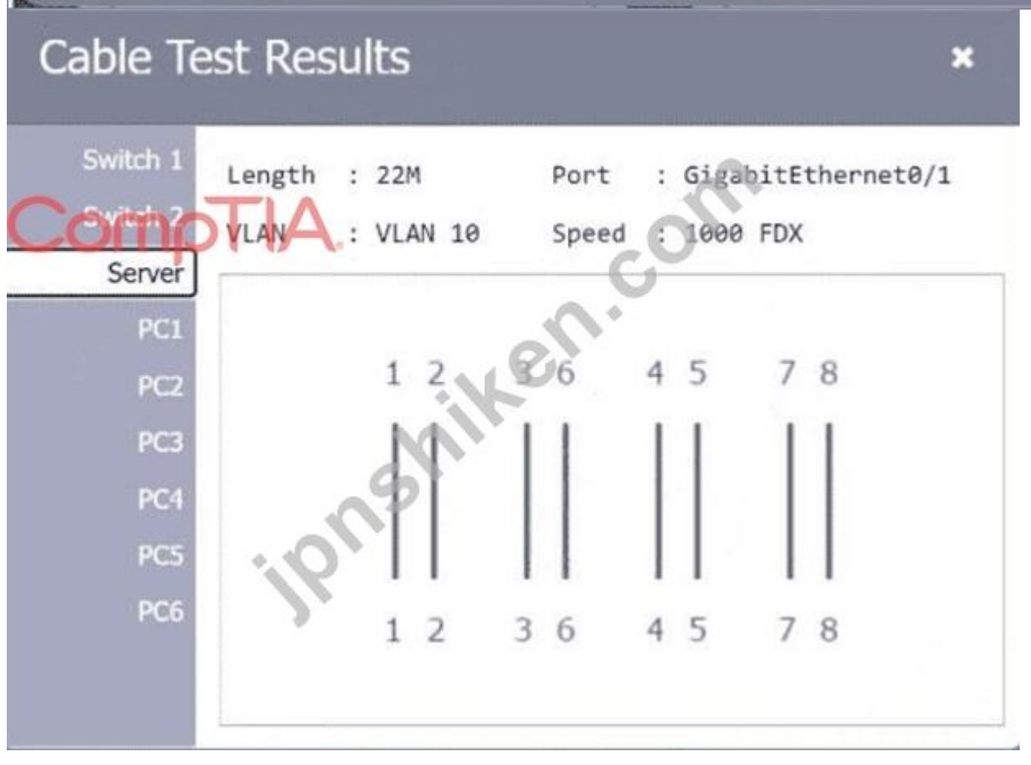
https://www.jpnshiken.com/shiken/CompTIA.N10-009J.v2026-10-24.q226.html

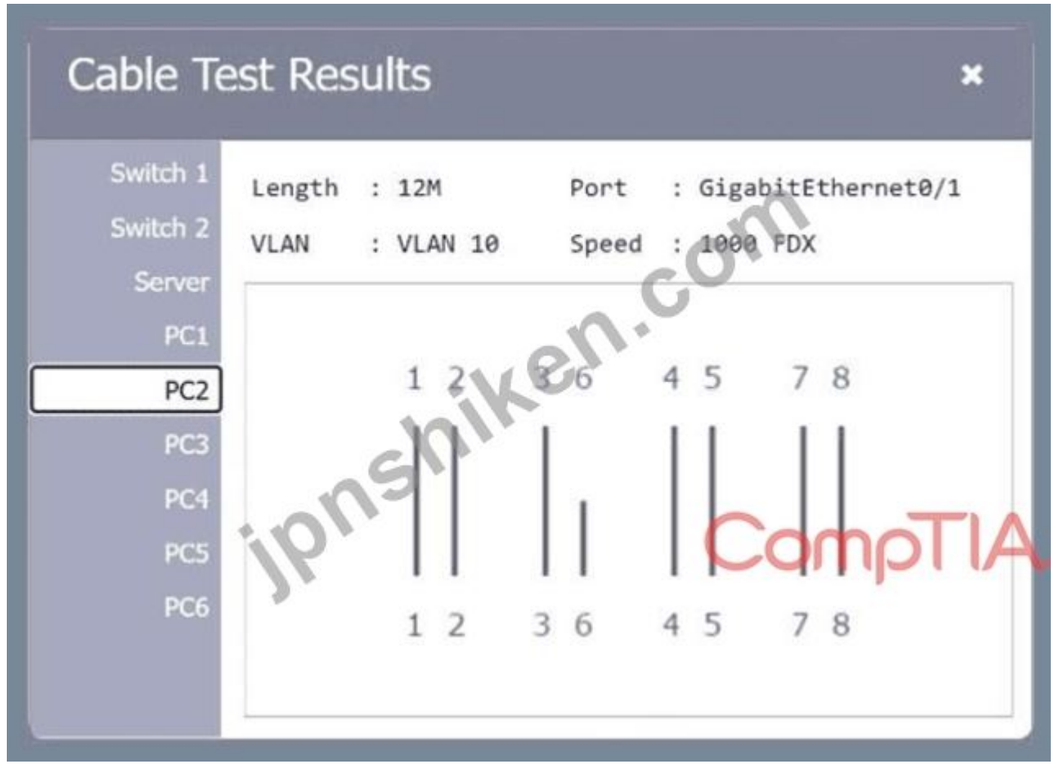
質問: **1**
ネットワーク技術者は、顧客のSOHOネットワークの問題を解決する必要があります。顧客から、一部のPCがネットワークに接続できない一方、他のPCは正常に動作しているようだという報告がありました。
説明書
すべてのネットワーク コンポーネントのトラブルシューティングを行います。
まずケーブル テストの結果を確認し、適切な PC、サーバー、およびレイヤー 2 スイッチをクリックして診断します。
問題のあるコンポーネントを特定し、それぞれの問題を修正するための解決策を提案します。
いつでもシミュレーションの初期状態に戻したい場合は、 「すべてリセット」ボタンをクリックしてください。



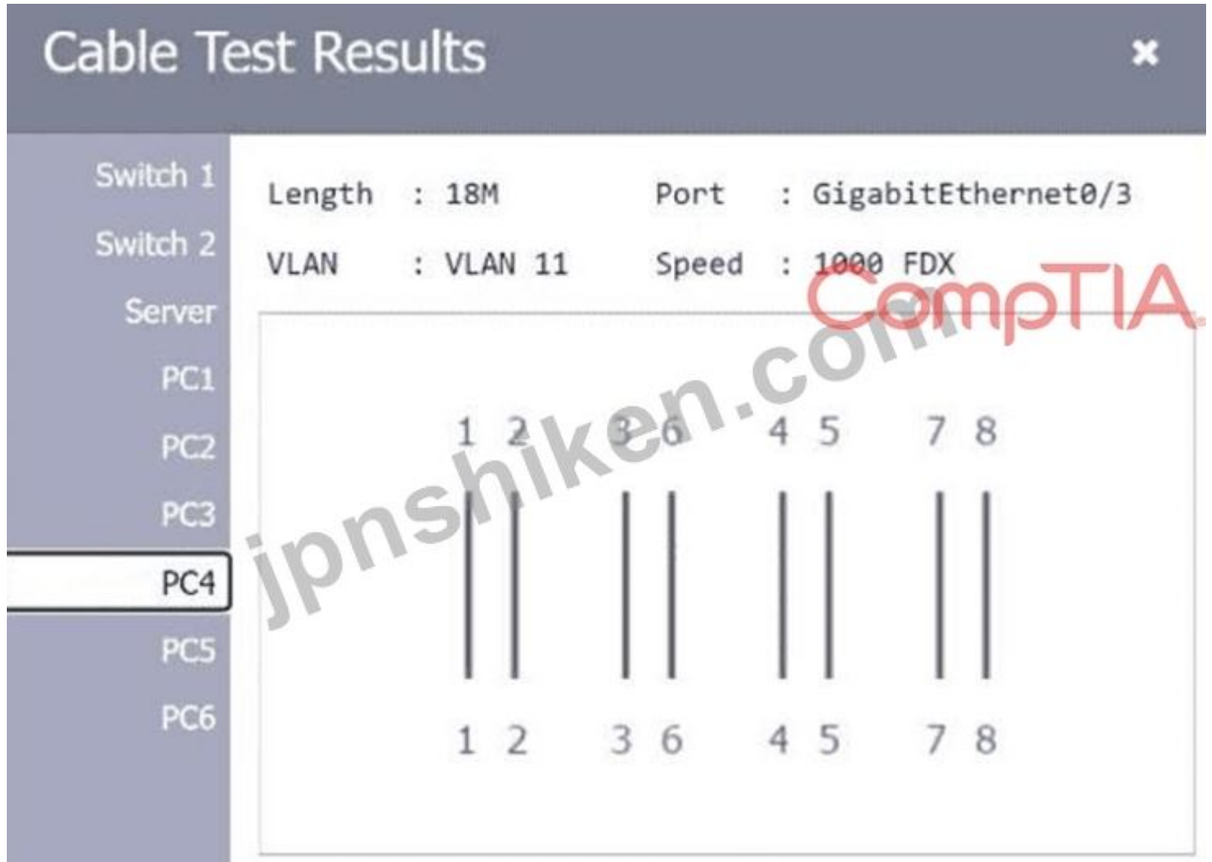
jpnshiken.com
CompTIA

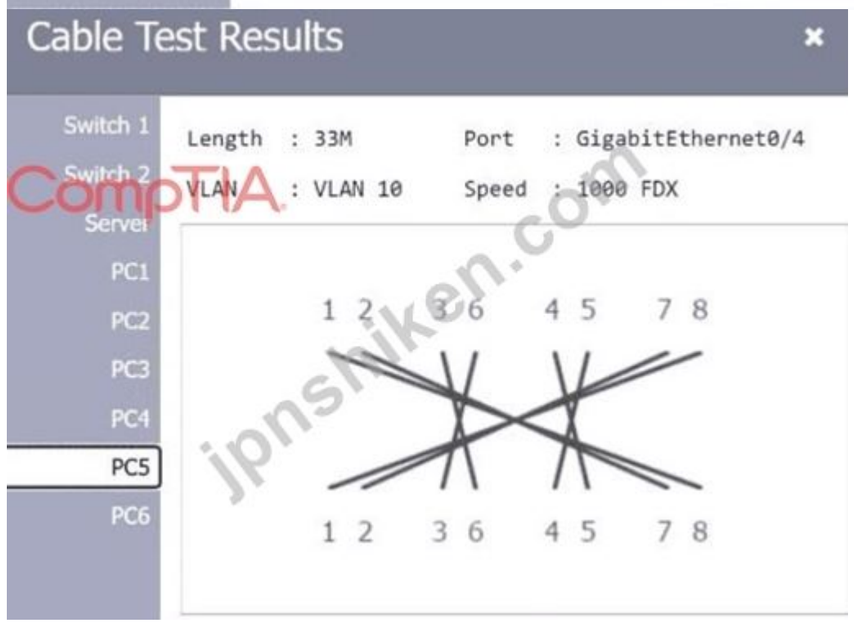

Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 16M
Port : GigabitEthernet0/5
VLAN : VLAN 10
Speed : 1000 FDX
Connected to Switch 1
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8


Cable Test Results
Switch 1
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 22M
Port : GigabitEthernet0/1
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

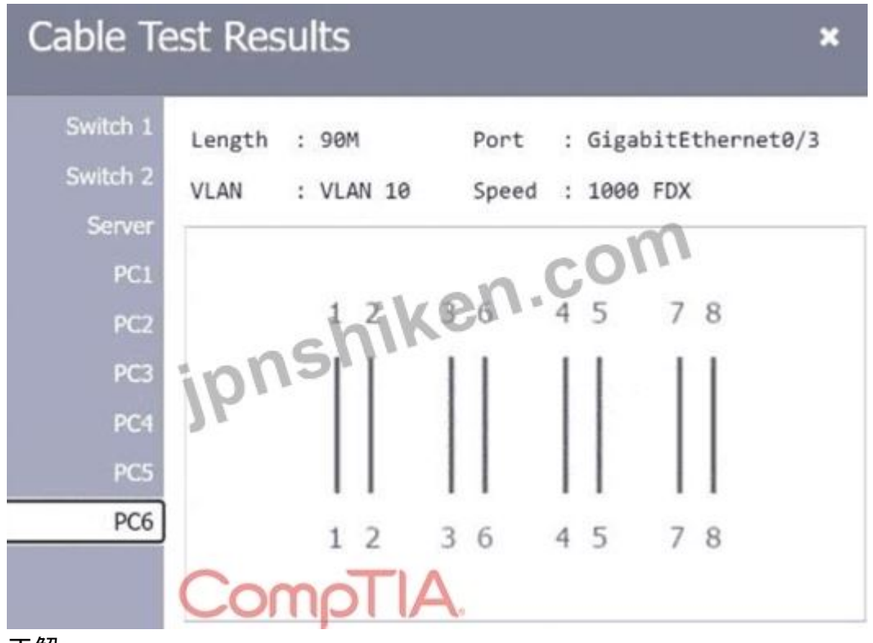


jpnshiken.com
CompTIA





CompTIA
jpnshiken.com

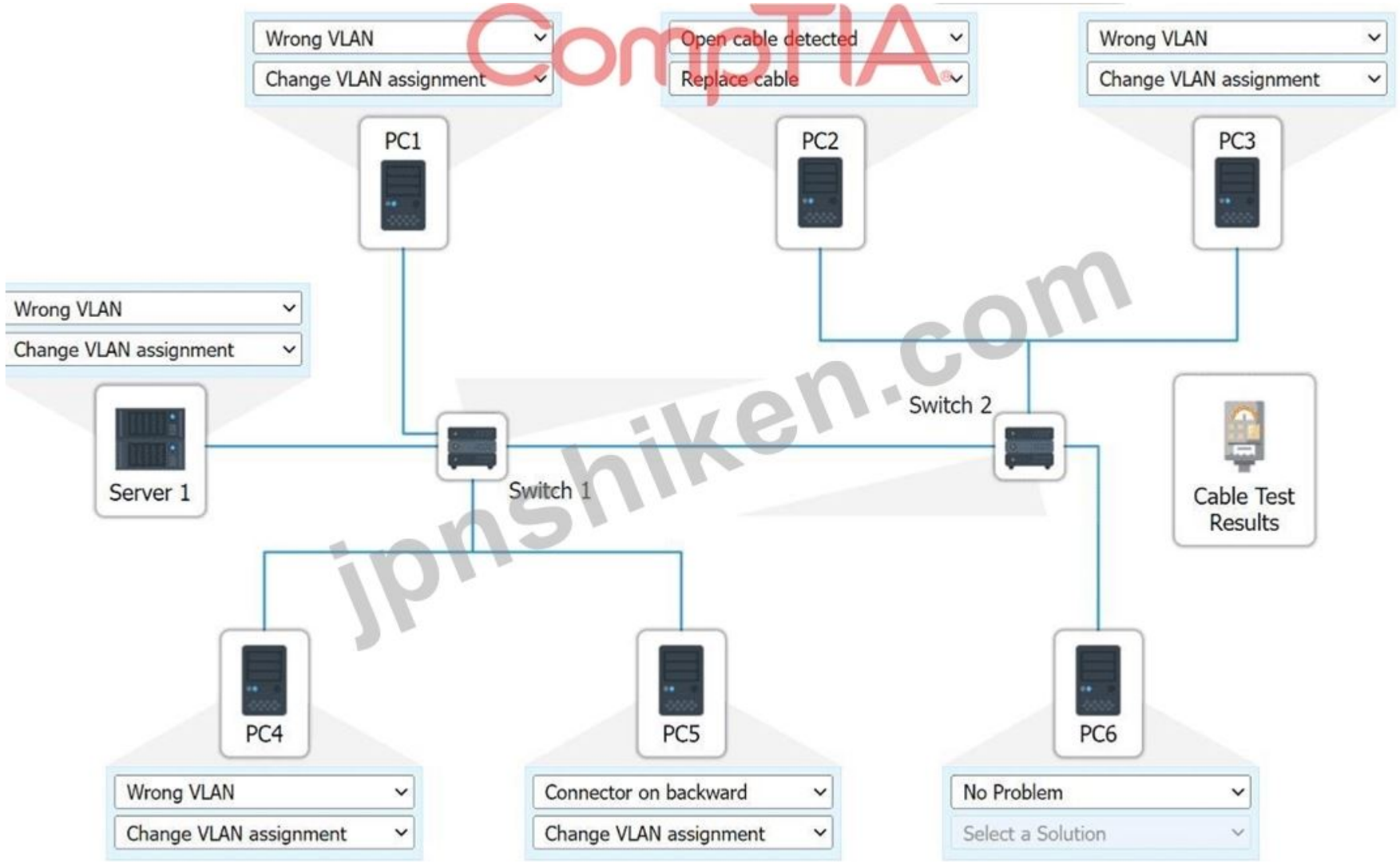


正解:

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: **2**
ネットワークエンジニアは、BYODデバイスが信頼できるワイヤレスネットワークに安全にアクセスできるようにする802.1Xアーキテクチャを実装したいと考えています。エンジニアが実装すべき項目は次のうちどれですか？
A. ACL
B. MACフィルタリング
C. ポートセキュリティ
D. NAC
正解: **(**正解を表示します**)**
For a secure 802.1X design that includes BYOD access to a trusted wireless network, the engineer should implement NAC (Network Access Control). In the Network+ (N10-009) objectives, 802.1X provides authentication (commonly via EAP to a RADIUS server), but NAC expands this by enforcing policy-based access decisions-such as device posture checks, user/device identity validation, and dynamic assignment to the appropriate VLAN/role. With BYOD, the organization often needs to confirm whether devices meet requirements (OS version, encryption, security software) and then grant the correct level of access (full, limited, or quarantine/remediation). NAC is the architecture that ties these controls together in a scalable way for wireless networks.

An ACL can restrict traffic after a device connects, but it doesn't perform authentication/posture assessment.
MAC filtering is weak because MAC addresses can be spoofed and it does not provide strong identity assurance. Port security is mainly a wired switch control (limiting MAC addresses per port) and is not the right control set for secure BYOD wireless access. NAC best matches the requirement of secure, policy- driven 802.1X BYOD access.

質問: **3**
ある企業が新しいサイトを開設しようとしていますが、そのサイトは、それぞれ 75 台のホストを収容できるサブネットに分割する必要があります。
次のうち最も効率的なサブネットはどれですか?
A. 192.168.13.0/25
B. 192.168.13.0/26
C. 192.168.13.0/27
D. 192.168.13.0/28
正解: **(**正解を表示します**)**
To support 75 hosts per subnet , you must choose a subnet size that provides at least 75 usable IP addresses.
In IPv4, usable hosts per subnet equals 2^(host bits) # 2 (subtracting network and broadcast). A /25 leaves 7 host bits (32-25 = 7), giving 2^7 # 2 = 128 # 2 = 126 usable hosts , which meets the requirement and is the smallest (most efficient) option listed that does so. A /26 leaves 6 host bits, giving 62 usable hosts , which is insufficient. A /27 gives 30 usable , and a /28 gives 14 usable , both far below 75. Network+ subnetting objectives emphasize selecting the smallest subnet that satisfies the host requirement to conserve address space while meeting growth and design constraints.
Therefore, 192.168.13.0/25 is the most efficient option that accommodates at least 75 hosts per subnet.

質問: **4**
ファイアウォールはポート 80 でトラフィックを受信し、ポート 88 で内部サーバーに転送します。次のどのテクノロジが活用されていますか?
A. TLS
B. FHRP
C. SSL
D. PAT
正解: **(**正解を表示します**)**
The correct answer is PAT (Port Address Translation). According to the CompTIA Network+ N10-009 objectives, PAT is a form of Network Address Translation (NAT) that allows multiple internal hosts- or services-to be mapped to a single public IP address using different port numbers. PAT can also translate destination port numbers, which is exactly what is occurring in this scenario.
In this case, the firewall receives incoming traffic on port 80 (commonly used for HTTP) and forwards it to an internal server listening on port 88. This process is often referred to as port forwarding, which is a practical implementation of PAT. The firewall rewrites the destination port and potentially the destination IP address so that external clients can access internal services without exposing internal addressing schemes.
The other options do not apply. TLS and SSL are encryption protocols used to secure data in transit; they do not perform port translation. FHRP (First Hop Redundancy Protocol), such as HSRP or VRRP, provides gateway redundancy and high availability, not traffic forwarding or port remapping.
The Network+ objectives emphasize understanding how firewalls and NAT technologies manipulate IP addresses and ports to enable secure access to internal resources. PAT is the technology that enables this functionality, making it the correct answer.

質問: **5**
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: **(**正解を表示します**)**
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: **6**
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: **(**正解を表示します**)**
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: **7**
ネットワーク管理者は新しいスイッチを導入しており、スパニング ツリーのデフォルトの優先度値が設定されていることを確認したいと考えています。ネットワーク管理者は次のどの値を確認する必要がありますか。
A. 4096
B. 8192
C. 32768
D. 36684
正解: **(**正解を表示します**)**
* Understanding Spanning Tree Protocol (STP):
* STP is used to prevent network loops in Ethernet networks by creating a spanning tree that selectively blocks some redundant paths.
* Default Priority Value:
* Bridge Priority: STP uses bridge priority to determine which switch becomes the root bridge. The default bridge priority value for most switches is 32768.
* Priority Range: The bridge priority can be set in increments of 4096, ranging from 0 to 61440.
* Configuration and Verification:
* When deploying a new switch, the network administrator can verify the bridge priority using commands such as show spanning-tree to ensure it is set to the default value of 32768.
* Comparison with Other Values:
* 4096 and 8192: Lower than the default priority, indicating these would be manually configured for higher preference.
* 36684: A non-standard value, likely a result of specific configuration changes.
References:
* CompTIA Network+ study materials on Spanning Tree Protocol and network configuration.

質問: **8**
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: **C (**コメントを発表する**)**
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: **9**
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: **10**
ネットワーク エンジニアは、HTTPS 経由でリアルタイムの可視性を維持しながら、AP をリモートで変更、更新、制御する必要があります。
これらのアクションを最も適切に許可するのは次のどれですか?
A. Webインターフェース
B. コマンドライン
C. SNMPコンソール
D. APIゲートウェイ

正解: (正解を表示します)
API gateways offer programmable control and real-time communication, commonly over HTTPS, which allows administrators to update and manage devices like access points remotely and efficiently.
From Andrew Ramdayal's guide:
"APIs enable automation and real-time interaction with network devices via secure interfaces, often using HTTPS for encrypted communication and control."

質問: **11**
ネットワーク管理者は接続の問題をトラブルシューティングしており、パケットが通過するパスを特定する必要があります。このタスクを実行するコマンドはどれですか？
A. netstat
B. traceroute
C. ping
D. nslookup
E. ipconfig
正解: (正解を表示します)
The correct answer is traceroute, which is the diagnostic command specifically designed to determine the path a packet takes across a network. According to the CompTIA Network+ N10-009 objectives, traceroute is a key network troubleshooting tool used to identify routing paths, hop counts, and points of latency or failure between a source and a destination.
Traceroute works by sending packets with incrementally increasing Time to Live (TTL) values. Each router along the path decrements the TTL by one, and when it reaches zero, the router returns an ICMP Time Exceeded message. This process allows the administrator to see each intermediate hop, its response time, and where packets may be delayed or dropped.
The other options do not fulfill this purpose. Ping only verifies basic connectivity and round-trip time but does not show the route taken. Netstat displays active connections, ports, and routing tables but does not trace packet paths. Nslookup is used to resolve DNS names to IP addresses, and ipconfig displays local network configuration information.
The Network+ objectives emphasize traceroute (or tracert on Windows systems) as the primary tool for diagnosing routing issues, asymmetric paths, and network congestion, making it the correct and most appropriate choice in this scenario.

質問: **12**
メール交換サーバー間でデータを転送するために使用されるポートは次のどれですか?
A. 21
B. 25
C. 53
D. 69
正解: (正解を表示します)
The correct answer is 25, which is the default port used by SMTP (Simple Mail Transfer Protocol) for communication between mail servers. According to CompTIA Network+ (N10-009) objectives under common port numbers and protocols, SMTP operates over TCP port 25 for server-to-server email transmission.
When an email is sent from one domain to another, the sending mail server queries DNS for the recipient domain's MX (Mail Exchange) record and then establishes an SMTP session over TCP port 25 to deliver the message. This port is specifically designated for mail relay between mail transfer agents (MTAs).
Port 21 is used for FTP (File Transfer Protocol), 53 is used for DNS (Domain Name System), and 69 is used for TFTP (Trivial File Transfer Protocol). None of these are responsible for transferring email between mail servers.
While SMTP can also use ports 587 (submission) and 465 (SMTPS) for client-to-server communication, port
25 remains the standard for mail server-to-mail server communication.
Therefore, TCP port 25 is the correct answer.

質問: **13**
攻撃者がネットワークのある部分からアクセスできないはずの別の部分に移動するには、次のうちどれが必要ですか?

A. MACフラッディング
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: **C** (コメントを発表する)
VLAN hopping allows an attacker to send traffic into another VLAN without authorization, often by impersonating a switch and negotiating a trunk link. This lets the attacker traverse into normally inaccessible VLANs.
A). MAC flooding disrupts switch operations but does not cross VLANs.
B). DNS poisoning corrupts name resolution.
D). ARP spoofing reroutes local traffic but doesn't grant VLAN traversal.
References (CompTIA Network+ N10-009):
Domain: Network Security - VLAN attacks, unauthorized lateral movement.

質問: **14**
次のツールのうち、ネットワーク ホストに到達可能かどうかを判断するために ICMP を使用するものはどれですか。
A. tcpdump
B. netstat
C. nslookup
D. ping
正解: (正解を表示します)
Ping sends ICMP Echo Request packets and waits for Echo Replies to verify host reachability and measure round-trip time.
A). tcpdump captures packets but does not test reachability.
B). netstat displays open ports and network sessions.
C). nslookup queries DNS servers for name resolution.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - ICMP operation, troubleshooting tools.

質問: **15**
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: **16**
サーバー管理者は、Webドメインの所有権を確認するために、会社のDNSサーバーにレコードを追加する必要があります。管理者はレコードの名前と値を知っています。管理者は、DNSサーバーにレコードを追加するために、次のどのレコードタイプを使用すべきでしょうか？
A. テキスト
B. A
C. PTR
D. CNAME
正解: **A (**コメントを発表する**)**
To verify ownership of a domain, providers commonly require adding a TXT record to DNS containing a specific validation token (a name/value pair). A TXT (text) record is designed to store arbitrary text data associated with a domain or hostname, which makes it ideal for domain verification workflows used by certificate authorities, email security (SPF/DKIM/DMARC-related entries), and third-party services that need proof of administrative control over DNS. This fits Network+ DNS objectives that cover common record types and their practical purposes in real deployments.
An A record maps a hostname to an IPv4 address and is used for name-to-address resolution, not ownership verification. A PTR record provides reverse DNS mapping (IP address to hostname) and is stored in reverse lookup zones, not typically used for validating web domain ownership. A CNAME record creates an alias from one hostname to another canonical hostname; while sometimes used in service integrations, the classic
"record name + token value" ownership verification is most directly and universally satisfied by a TXT record. Therefore, TXT is the correct choice given the requirement and the provided record name and value.

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 **608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
パスワードに加えて、MFA のためにユーザーに要求できるのは次のどれですか?
A. PIN
B. 好きな色
C. ハードトークン
D. 母親の旧姓
正解: **(**正解を表示します**)**
Multi-factor authentication (MFA) requires two or more different categories of authentication factors:
Something you know (password, PIN)
Something you have (smart card, hardware token)
Something you are (biometric)
The only valid second factor here is a hard token (e.g., a key fob generating one-time codes).
A). PIN is still "something you know," the same category as a password.

B). Favorite color is a weak knowledge-based factor, not a true second factor.
D). Mother's maiden name is also "something you know" and insecure.
References (CompTIA Network+ N10-009):
Domain: Network Security - Authentication methods, MFA factor categories.

質問: **18**
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: **19**
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: **20**
A systems administrator is looking for operating system information, running services, and network ports that are available on a server. Which of the following software tools should the administrator use to accomplish this task?
A. nslookup
B. nmap
C. traceroute
D. netstat
正解: **(**正解を表示します**)**
To identify a server's available network ports , running services , and often operating system details , the best tool listed is nmap . In the Network+ (N10-009) toolset, nmap is a standard utility used for network discovery and security assessment , including port scanning (which TCP/UDP ports are open), service enumeration (what application/service is listening on those ports), and service/version detection . With the appropriate scan options and permissions, nmap can also provide OS fingerprinting , which estimates the server's operating system by analyzing responses to crafted packets.
The other options do not meet all stated requirements. nslookup is used for DNS queries (name-to-IP and record lookups) and does not enumerate ports/services. traceroute (or tracert) maps the path packets take through the network to a destination and helps diagnose routing/latency issues, not services/ports. netstat shows local socket statistics on the host where it is executed (active connections, listening ports, and interface stats), but it does not reliably provide remote OS identification and is not a dedicated service/OS enumeration scanner like nmap.
Therefore, nmap is the correct tool to accomplish the task as described.

質問: **21**
複数の論理ネットワークを相互接続し、遅延を最小限に抑えながらそれらの間でデータ パケットを転送するのに最適なネットワーク アプライアンスは次のどれですか。
A. ファイアウォール
B. ルーター
C. レイヤー2スイッチ
D. ロードバランサー
正解: **B (**コメントを発表する**)**
The correct appliance is a router, which is specifically designed to interconnect multiple networks and forward packets based on IP addresses. Routers operate at Layer 3 (Network layer) of the OSI model and make intelligent forwarding decisions to ensure data reaches the correct destination network.
A). Firewall can also forward traffic, but its primary function is security, not routing efficiency.
C). Layer 2 switches connect devices within the same LAN but do not forward packets between different networks without routing capability.
D). Load balancers distribute traffic among servers but are not general-purpose routers.
Modern enterprise routers are optimized to minimize latency by using fast switching and hardware acceleration, making them ideal for interconnecting logical networks securely and efficiently.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Routers, Layer 3 devices, inter-network communication.

質問: **22**
ヨーロッパにおける個人データのセキュリティと取り扱いについて、最も責任があると思われるのは次のどれですか?
A. GDPR
B. SCADA
C. SAML
D. PCI DSS
正解: **A (**コメントを発表する**)**

* Definition of GDPR:
* General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.
* Scope and Objectives:
* GDPR aims to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
* It enforces rules about data protection, requiring companies to protect the personal data and privacy of EU citizens for transactions that occur within EU member states.
* Comparison with Other Options:
* SCADA (Supervisory Control and Data Acquisition): Refers to control systems used in industrial and infrastructure processes, not related to personal data protection.
* SAML (Security Assertion Markup Language): A standard for exchanging authentication and authorization data between parties, not specifically for personal data protection.
* PCI DSS (Payment Card Industry Data Security Standard): A set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment, not specific to personal data protection in Europe.
* Key Provisions:
* GDPR includes provisions for data processing, data subject rights, obligations of data controllers and processors, and penalties for non-compliance.
References:
* CompTIA Network+ study materials on regulatory and compliance standards.

質問**: 23**
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**: 24**
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
jpnshiken.com

CompTIA
jpnshiken.com

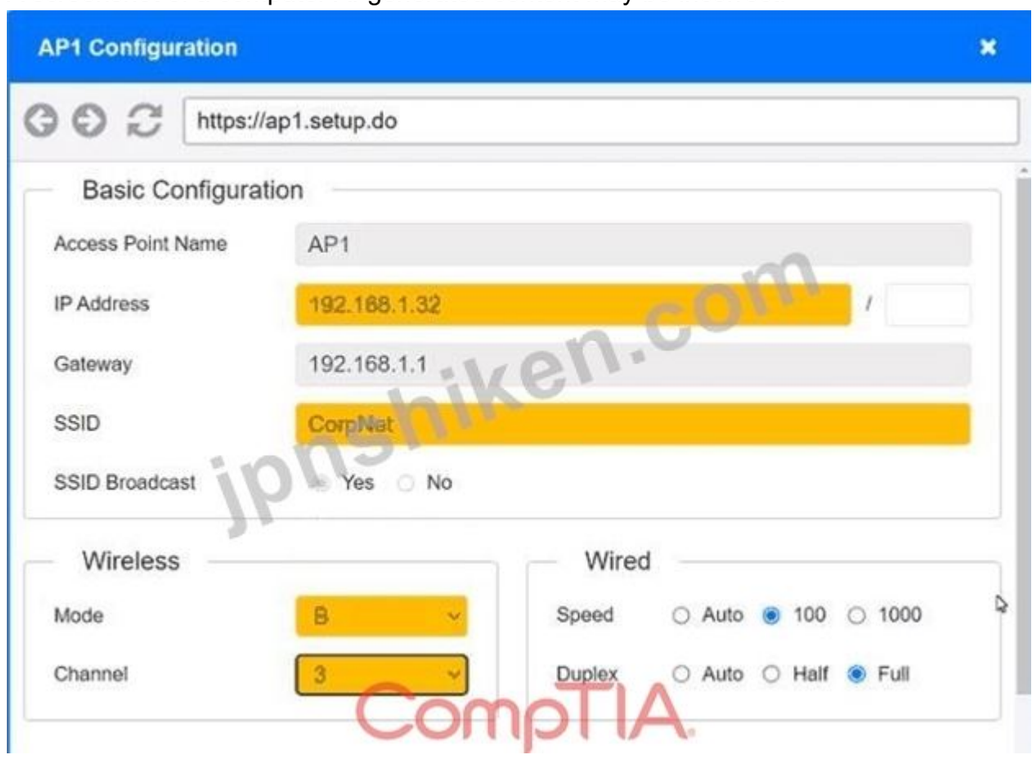
正解:

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.

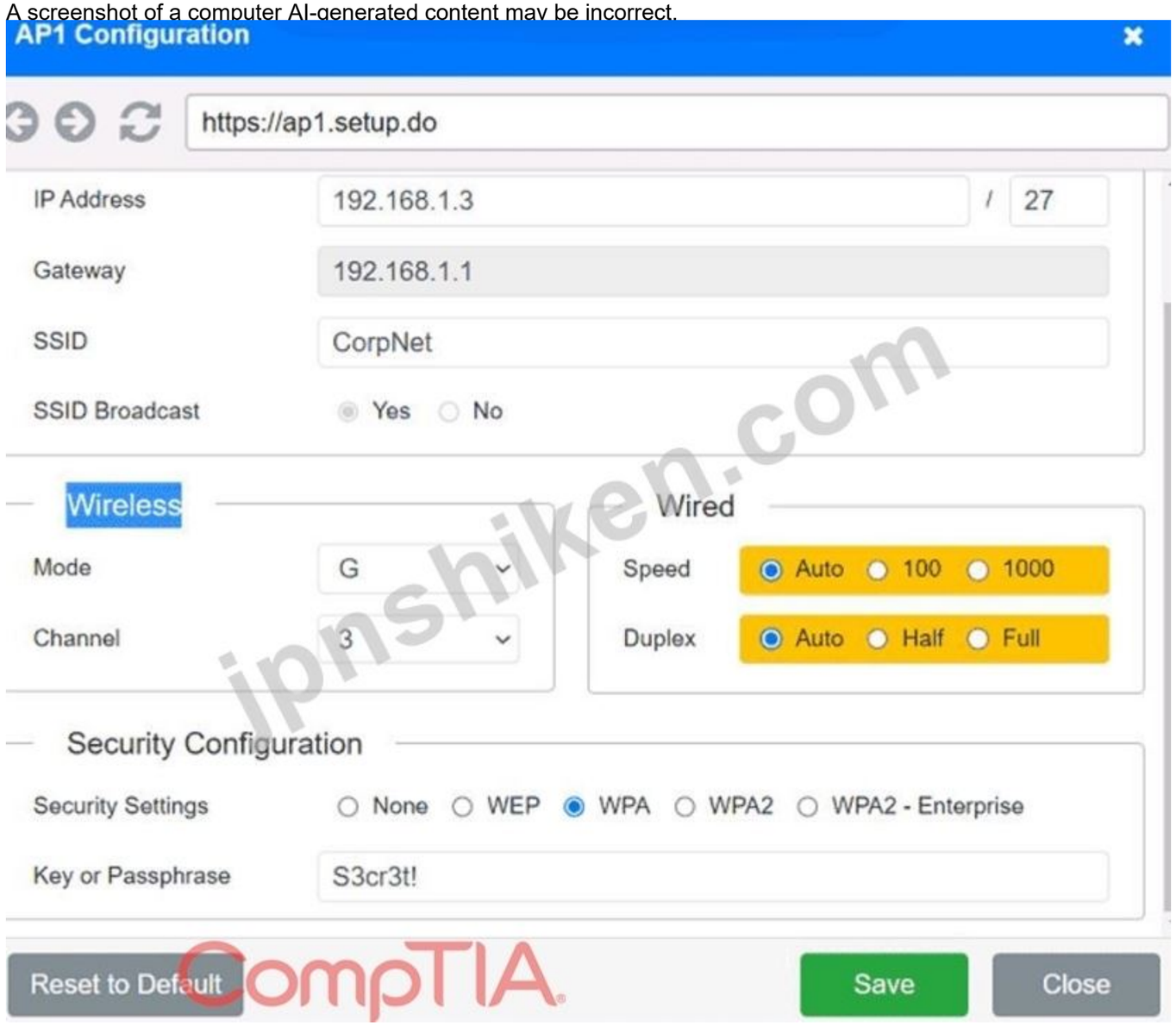
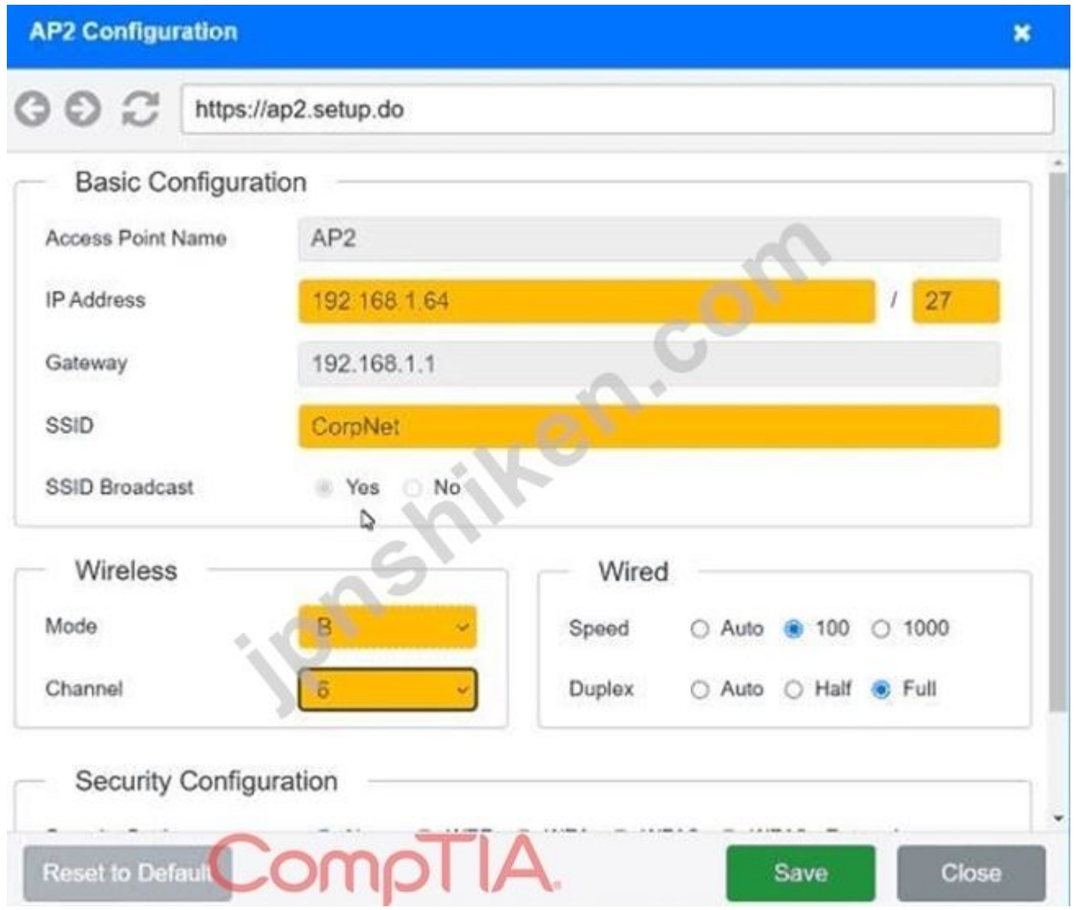


Exhibit 2 as follows

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.

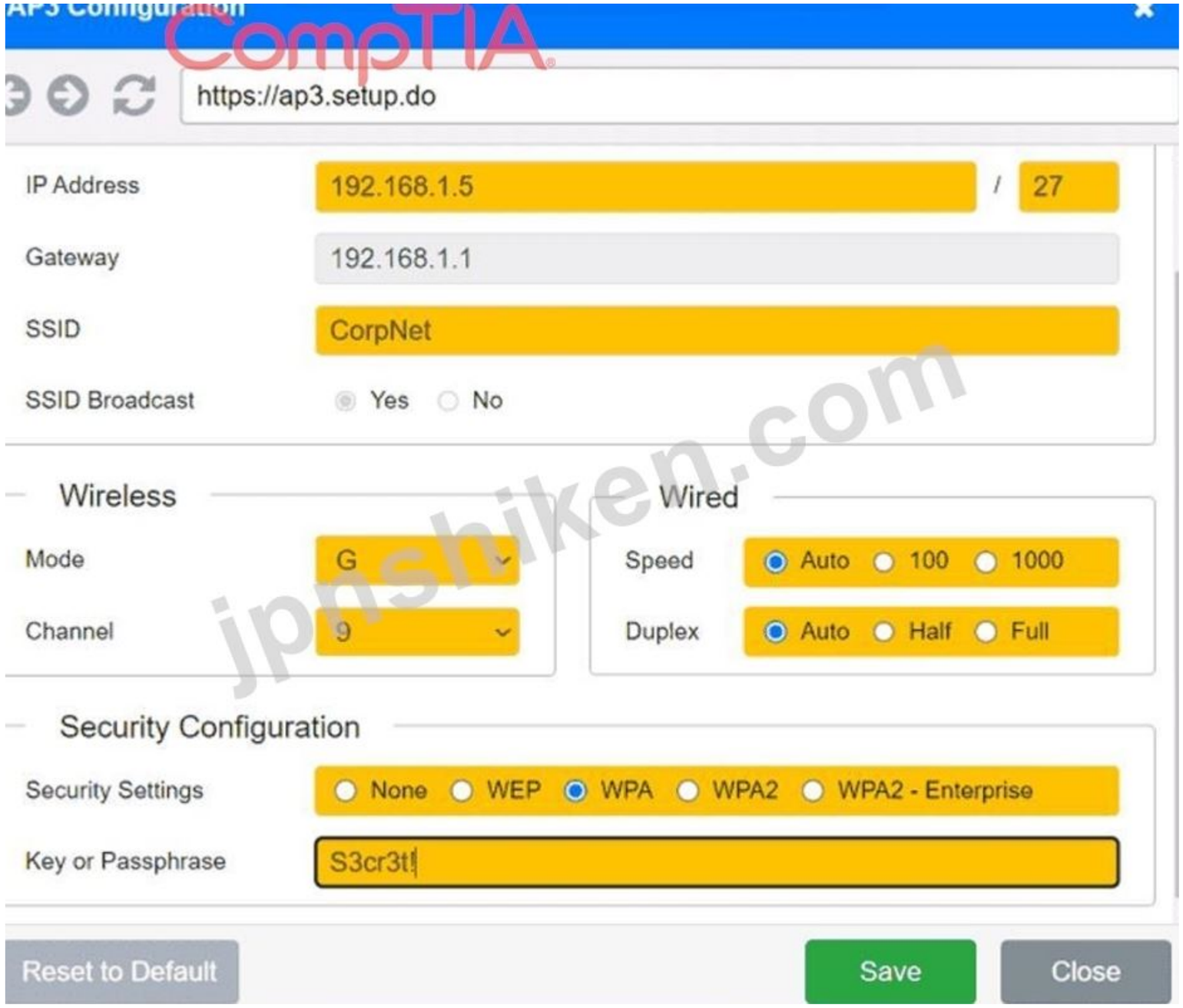
Exhibit 3 as follows

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.



CompTIA
ipnshiken.com

質問: **25**
正常に起動できなかったネットワークアプライアンスへのリモートアクセスを取得するには、次のどれを使用する必要がありますか?
A. クラッシュカート
B. ジャンプボックス
C. セキュア シェル (SSH)
D. 帯域外管理
正解: **(**正解を表示します**)**

If a network appliance fails to start, standard remote access methods like SSH won't work. Instead, Out-of- Band (OOB) management provides a dedicated access path (e.g., a console port or iDRAC/iLO), allowing administrators to troubleshoot devices even when the network is down.
Breakdown of Options:
A: Crash cart - A physical monitor/keyboard setup, not a remote solution.
B: Jump box - A hardened system used for secure remote access but requires the device to be operational.
C: Secure Shell (SSH) - Requires the device to be fully booted and network-connected.
D: Out-of-band management - # Correct answer. Provides independent access for troubleshooting failed network devices.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 4.3: Explain network device management concepts.

質問: 26
クラウド VM インスタンスでのアクセスを管理する機能を提供するのは次のどれですか?
A. セキュリティグループ
B. インターネットゲートウェイ
C. 直接接続
D. ネットワークACL
正解: (正解を表示します)
Security groups in cloud environments act as virtual firewalls for VM instances, controlling inbound and outbound traffic based on specified rules.
From Andrew Ramdayal's guide:
"Network security groups are used to control inbound and outbound traffic to cloud resources within a VPC.
They act as a virtual firewall for associated instances..."

質問: 27
経験の浅いネットワーク管理者が社内ネットワークの監査中に、長距離マイクロ波インターフェースの入力エラーが増加していることに気付きました。このエラー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. パラボラ信号の位置がずれています。
B. 全方向信号が妨害されています。
C. 全方向信号が十分に強くないため、正常に受信できません。
D. パラボリック信号は不適切なルーティング プロトコルを使用しています。
正解: (正解を表示します)
A misaligned parabolic antenna can cause a significant increase in input errors because the signal is not properly focused or directed towards the receiving antenna, resulting in poor reception and data corruption.
The document confirms:
"Misalignment of parabolic microwave antennas can lead to weak or incorrect signal reception, causing an increase in input errors and connectivity issues on the link."

質問: 28
次のコネクタのうち、単一の QSFP トランシーバーで複数の物理接続を可能にするものはどれですか。
A. RJ45
B. ST
C. LC
D. MPO

正解: **D** (コメントを発表する)
The MPO (Multi-fiber Push On) connector is designed to handle multiple fiber strands in a single connector, and it is commonly used with high-density transceivers like QSFP (Quad Small Form-factor Pluggable).
QSFP can support up to four channels (hence " quad "), and MPO connectors can interface multiple fibers (e.
g., 8, 12, 24), making them ideal for 40Gbps or 100Gbps deployments.
RJ45 (A) is used for Ethernet over copper.
ST (B) and LC (C) are single-fiber connectors - they don ' t support the multi-fiber needs of QSFP setups.
Therefore, MPO is the correct connector type for this use case.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 3.1: " Compare and contrast different types of connectors and transceivers. "

質問: **29**
組織が複数の内部デバイスを単一の外部向け IP アドレスにマッピングできるようにするには、次のうちどれを使用しますか?
A. NAT
B. BGP
C. OSPF
D. FHRP
正解: **A** (コメントを発表する)
NAT (Network Address Translation) allows multiple private IP addresses to share a single public IP when accessing the internet. This conserves public IPs and provides basic security by hiding internal addresses.
B). BGP is a routing protocol.
C). OSPF is a link-state IGP.
D). FHRP provides redundant gateways, not IP sharing.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - NAT, PAT, private-to-public IP mapping.

質問: **30**
ネットワークエンジニアは、コアスイッチ間の新しい接続を実装しています。エンジニアは以下の構成を導入します。
コア-SW01
VLAN 100
名前
インターフェース イーサネット 1/1
チャネルグループ1モードアクティブ
インターフェース イーサネット 1/2
チャネルグループ1モードアクティブ
インターフェースポートチャネル1
スイッチポートモードトランク
スイッチポートトランクでVLAN 100を許可する
コア-SW02
VLAN 100
名前
インターフェース イーサネット 1/1

スイッチポートモードトランク
スイッチポートトランクでVLAN 100を許可する
インターフェース イーサネット 1/2
スイッチポートモードトランク
スイッチポートトランクでVLAN 100を許可する
インターフェースポートチャネル1
スイッチポートモードトランク
スイッチポートトランクでVLAN 100を許可する
Core-SW01 ポートチャネル インターフェイスの状態は次のどれですか。
A. CRCエラーの増加
B. エラー無効
C. 管理上ダウン
D. 一時停止
正解: **(**正解を表示します**)**
On Core-SW01, the ports are configured with LACP (mode active) for link aggregation. On Core-SW02, the ports are configured as independent trunks, not as part of an LACP group. Because of this mismatch, LACP cannot form the bundle, and the aggregated ports on SW01 will go into a suspended state.
A). CRC errors suggest cabling or signal integrity issues, not config mismatch.
B). Error disabled occurs when a violation (like BPDU guard or port security) disables the port, not LACP mismatch.
C). Administratively down indicates a shutdown command, not the case here.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Port-channel/LACP configuration issues, interface states.

質問: **31**
2.4GHz ワイヤレス ネットワークを使用しているクライアントから、WAP を移動した後、オフィス全体でラップトップに断続的な問題が発生しているという報告がありました。これらの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. ネットワークは重複しないチャネルを使用します。
B. 信号が反射しすぎています。
C. ネットワークに過剰なノイズがあります。
D. オフィスに電子レンジがあります。
正解: **(**正解を表示します**)**
Microwaves are known to interfere with the 2.4GHz frequency, which is the same frequency used by many wireless networks. This can cause signal degradation and intermittent connectivity issues, especially if the WAP is placed near such devices.

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 **608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
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.

質問: **33**
ネットワーク管理者は、35 台の PoE セキュリティ カメラを設置中です。管理者は、新しいケーブルを設置してテストした後、カメラを設置しました。
ただし、少数のカメラは動作しません。主な原因は次のどれですか?
A. 配線規格が正しくありません
B. 電力予算を超過しました
C. 信号減衰
D. 電圧が間違っています
正解: **B (**コメントを発表する**)**
When installing multiple Power over Ethernet (PoE) devices like security cameras, it is crucial to ensure that the total power requirement does not exceed the power budget of the PoE switch. Each PoE switch has a maximum power capacity, and exceeding this capacity can cause some devices to fail to receive power.
* PoE Standards: PoE switches conform to standards such as IEEE 802.3af (PoE) and 802.3at (PoE+), each with specific power limits per port and total power capacity.
* Power Calculation: Adding up the power requirements of all connected PoE devices can help determine if the total power budget of the switch is exceeded.
* Symptoms: When the power budget is exceeded, some devices, typically those farthest from the switch or connected last, may not power up or function correctly.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Covers PoE standards and troubleshooting power issues.
* Cisco Networking Academy: Discusses PoE technologies, power budgeting, and managing PoE devices.
* Network+ Certification All-in-One Exam Guide: Provides information on PoE setup, including power budget considerations.

質問: **34**
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: **35**
ネットワーク エンジニアが、既存の VLAN に新しくインストールされたサーバーの接続のトラブルシューティングを行っています。
エンジニアは次の出力を確認します。
C:\> ipconfig
IPアドレス: 192.168.100.225
マスク: 255.255.255.224
ゲートウェイ: 192.168.100.254
ルータ# show ip route
C 192.168.100.0/24は直接接続されており、GigabitEthernet0/0
次のどれが問題を表していますか?
A. サーバーのサブネットマスクが正しくありません
B. ネットワーク上に重複したIPアドレスがあります
C. DHCPアドレスプールが枯渇しました
D. ルータにデフォルトルートがありません
正解: (正解を表示します)
The server's subnet mask is 255.255.255.224 (/27), which covers IPs from 192.168.100.224 to
192.168.100.255. However, the router only recognizes 192.168.100.0/24, indicating a mismatch between the server's subnet and the router's network.
Correct mask for the /24 network is 255.255.255.0, allowing 256 IPs from 192.168.100.0 to 192.168.100.255.
This mismatch would result in routing issues, especially with the gateway outside of the subnet range.
Reference:
CompTIA Network+ N10-009 Official Objectives: 5.2 - Given a scenario, troubleshoot common wired connectivity issues.

質問: **36**
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: **37**
OSI モデルの次の層のうち、ノード間の接続の確立、維持、終了を担当するのはどれですか。
A. 物理
B. ネットワーク
C. セッション
D. 輸送
正解: **(**正解を表示します**)**
TheSession Layer(Layer 5 of the OSI Model) is responsible for setting up, managing, and tearing down sessions between applications. It maintains dialog control and synchronizes data exchange between systems.
Reference:Section 1.1 - OSI Reference Model Concepts - "Layer 5 - Session"

質問: **38**
企業ネットワークとネットワーク管理インターフェースの間にセキュリティの層を追加するために実装できるのは次のどれですか?
A. ジャンプボックス
B. コンソールサーバー
C. APIインターフェース
D. インバンド管理
正解: **(**正解を表示します**)**
A jump box is a hardened, isolated system that provides secure access to critical infrastructure devices like routers and firewalls.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 4.3: Explain network security techniques.

質問: **39**
デバイスの平均寿命を推定するために使用されるのは次のどれですか?
A. RTO
B. RPO
C. MTBF
D. 平均所要時間
正解: **(**正解を表示します**)**
Understanding MTBF:
Mean Time Between Failures (MTBF): A reliability metric that estimates the average time between successive failures of a device or system.
Calculation and Importance:
Calculation: MTBF is calculated as the total operational time divided by the number of failures during that period.
Usage: Used by manufacturers and engineers to predict the lifespan and reliability of a device, helping in maintenance planning and lifecycle management.
Comparison with Other Metrics:
RTO (Recovery Time Objective): The maximum acceptable time to restore a system after a failure.
RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time.
MTTR (Mean Time to Repair): The average time required to repair a device or system and return it to operational status.
Application:
MTBF is crucial for planning maintenance schedules, spare parts inventory, and improving the overall reliability of systems.
References:

CompTIA Network+ study materials on reliability and maintenance metrics.

質問: **40**
ネットワークエンジニアが、ある企業を新しいISPに接続しました。8.8.8.8への簡単なpingテストは成功しました。しかし、ユーザーから、どのウェブサイトも極端に遅くなり、接続できない期間が続くという苦情が寄せられています。最も考えられる原因は次のどれですか？
A. デフォルトゲートウェイが正しくありません
B. VLAN不一致
C. サブネットマスクの設定
D. ISP IPアドレスが重複しています
正解: **D (**コメントを発表する**)**
If the business shares or duplicates the ISP-assigned public IP address, routing instability and conflicts will occur. Pinging a public IP like 8.8.8.8 may work (since ICMP can bypass certain conflicts), but browsing websites (which requires stable sessions and return traffic) will fail intermittently.
A). If the default gateway were incorrect, no external connectivity would work at all.
B). VLAN mismatch is an internal issue, not affecting ISP routing.
C). Subnet mask misconfiguration would prevent consistent routing but usually blocks ping too.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Internet connectivity issues, ISP IP conflicts.

質問: **41**
投資銀行が DR バックアップ ソリューションを探しています。次のうち、最もコスト効率の高いバックアップ サイトはどれですか?
A. ホット
B. 寒い
C. クラスター
D. 暖かい
正解: **(**正解を表示します**)**
*Cold sites are the most cost-effective disaster recovery (DR) option since they require the least infrastructure investment. They provide space and power but no pre-configured systems.
*Hot sites (A) are fully operational and very expensive.
*Warm sites (D) offer some pre-configured hardware but still require setup, making them more costly than cold sites.
*Clusters (C) are active failover systems, not DR sites.
#Reference: CompTIA Network+ N10-009 Official Documentation - Disaster Recovery & Business Continuity Planning.

質問: **42**
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: **43**
提供された URL が正しい IP アドレスに解決されないため、ユーザーは Web サイトに移動できません。
他のユーザーは問題なく目的の Web サイトに移動できます。この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. ホストファイル
B. 自己署名証明書
C. ネームサーバーレコード
D. IP ヘルパー ANS
正解: **A (**コメントを発表する**)**
* Role of the Hosts File:
* The hosts file is a local file on a computer that maps hostnames to IP addresses. It can be used to override DNS resolution by providing a static mapping of a hostname to an IP address.
* Common Issues with the Hosts File:
* If an incorrect IP address is mapped to a hostname in the hosts file, it can cause the computer to resolve the hostname to the wrong IP address. This can lead to navigation issues for specific websites while other users, relying on DNS, do not face the same problem.
* Why Other Options are Less Likely:
* Self-signed certificate: Relates to SSL/TLS and would cause a security warning, not a navigation failure.
* Nameserver record: Affects all users, not just one.
* IP helper: Used to forward DHCP requests and is unrelated to DNS resolution issues.
* Troubleshooting Steps:
* Check the hosts file on the affected user's computer (C:\Windows\System32\drivers\etc\hosts on Windows or /etc/hosts on Unix/Linux).
* Look for entries that map the problematic hostname to an incorrect IP address and correct or remove them.
References:
* CompTIA Network+ study materials and system administration documentation.

質問: **44**
ある刑事が、身元盗難事件を捜査しています。この事件では、RFID保護付き決済カードが発行され、その日のうちに不正利用されました。被害者がカードを使用したと主張する場所は、地元のコンビニエンスストアのみでした。刑事は、店舗に設置されたビデオカメラが、顧客の決済時に認証情報を確認できるような位置に配置されていることに気付きました。このソーシャルエンジニアリングの手法を最もよく説明しているのは次のうちどれですか？
A. 肩越しに覗き見る
B. なりすまし
C. ヴィッシング
D. テールゲーティング
正解: **(**正解を表示します**)**
Shoulder surfing is a social engineering attack where attackers observe someone's private information by looking over their shoulder or using tools like cameras to capture input.
From Andrew Ramdayal's guide:
"Shoulder surfing is the act of watching someone enter confidential information, such as PINs or passwords, often using direct line-of-sight or surveillance equipment."

質問: **45**
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."

質問: **46**
技術者が、オフィスビルの新しい別館で働くユーザーのコンピューターの問題をトラブルシューティングしています。ユーザーから、速度が遅く、接続が断続的であると報告されています。コンピューターは、Cat 6 ケーブルを介して 492 フィート (150 メートル) 離れた分散スイッチに接続されています。技術者は、この問題を解決するために次のどれを実施する必要がありますか。
A. コンピュータへの帯域幅の割り当てを増やします。
B. アクセス スイッチを別館に設置し、配布スイッチまでファイバーを配線します。
C. コンピューターから配布スイッチまで Cat 7 ケーブルを接続します。
D. コンピュータがジャンボ フレームをサポートできるようにします。
正解: **(**正解を表示します**)**
The maximum recommended length for Ethernet cable runs is 100 meters (328 feet). At 150 meters, the Cat 6 cable is too long, causing signal degradation and connectivity issues. Running fiber from the distribution switch to an access switch in the annex will allow for reliable connectivity over longer distances, as fiber can cover greater distances without signal loss. (Reference: CompTIA Network+ Study Guide, Chapter on Network Cable Standards)

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 **608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
ネットワーク管理者は、企業ネットワークにセキュリティ ゾーンを実装して、企業内の個人のみのアクセスを制御したいと考えています。次のセキュリティ ゾーンのうち、最適なソリューションはどれですか。
A. エクストラネット
B. 信頼できる
C. VPN
D. パブリック
正解: **(**正解を表示します**)**
Introduction to Security Zones:
Security zones are logical segments within a network designed to enforce security policies and control access.
They help in segregating and securing different parts of the network.
Types of Security Zones:
Trusted Zone: This is the most secure zone, typically used for internal corporate networks where only trusted users have access.
Extranet: This zone allows controlled access to external partners, vendors, or customers.
VPN (Virtual Private Network): While VPNs are used to create secure connections over the internet, they are not a security zone themselves.

Public Zone: This zone is the least secure and is typically used for public-facing services accessible by anyone.
Trusted Zone Implementation:
The trusted zone is configured to include internal corporate users and resources. Access controls, firewalls, and other security measures ensure that only authorized personnel can access this zone.
Internal network segments, such as the finance department, HR, and other critical functions, are usually placed in the trusted zone.
Example Configuration:
Firewall Rules: Set up rules to allow traffic only from internal IP addresses.
Access Control Lists (ACLs): Implement ACLs on routers and switches to restrict access based on IP addresses and other criteria.
Segmentation: Use VLANs and subnetting to segment and isolate the trusted zone from other zones.
Explanation of the Options:
A). Extranet: Suitable for external partners, not for internal-only access.
B). Trusted: The correct answer, as it provides controlled access to internal corporate users.
C). VPN: A method for secure remote access, not a security zone itself.
D). Public: Suitable for public access, not for internal corporate users.
Conclusion:
Implementing a trusted zone is the best solution for controlling access within a corporate network. It ensures that only trusted internal users can access sensitive resources, enhancing network security.
References:
CompTIA Network+ guide detailing security zones and their implementation in a corporate network (see page Ref 9 Basic Configuration Commands).

質問**: 48**
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**: 49**
ネットワークエンジニアがdigコマンドを使ってホスト名を照会したところ、有効なIPアドレスが返されました。しかし、同じIPアドレスをdigコマンドで照会すると、ホスト名が返されません。次のDNSレコードのうち、不足しているのはどれですか？
A. MX
B. CNAME
C. AAAA
D. PTR
正解**: (**正解を表示します**)**
This scenario describes a successful forward DNS lookup (hostname # IP address) but a failed reverse DNS lookup (IP address # hostname). Reverse lookups rely on a PTR (Pointer) record, which is stored in a reverse lookup zone (in-addr.arpa for IPv4, ip6.arpa for IPv6). If the engineer can resolve the hostname to an IP, that indicates an A record (or possibly AAAA for IPv6) exists and is

functioning. But when querying the IP directly and receiving no hostname, the most likely issue is that the reverse mapping is not configured- meaning the PTR record is missing.
An MX record is used for mail exchange routing, not hostname resolution. A CNAME provides an alias from one hostname to another and does not create reverse mappings. An AAAA record maps a hostname to an IPv6 address; it is not used for reverse lookups of an IP to a name. Network+ objectives emphasize understanding common DNS record types and the difference between forward and reverse resolution, making PTR the correct missing record here.

質問: **50**
ネットワーク管理者は、2 つの異なるサブネット上の 2 つのデバイス間の接続の問題をトラブルシューティングしています。
管理者は、両方のデバイスが同じサブネット上の他のデバイスに正常に ping できることを確認します。接続の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. デフォルトゲートウェイが正しくありません
B. イーサネットケーブルの故障
C. デュプレックス設定が間違っています
D. VLAN 不一致
正解: **(**正解を表示します**)**
When two devices on different subnets are unable to communicate, but can communicate with other devices on their own subnet, the issue is most often related to routing. Devices on different subnets require a default gateway to route traffic between networks.
If the default gateway is incorrectly configured, the device won't know how to reach other subnets.
Faulty cables (Option B) or duplex mismatches (Option C) would likely cause connectivity issues even within the local subnet, which is not the case here.
VLAN mismatches (Option D) are typically issues with switch port configurations and would likely cause total loss of connectivity, including within the same subnet.
So, the most probable and logical cause is an incorrect default gateway.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 2.4: "Compare and contrast routing technologies."

質問: **51**
ある会社では最近、オフィスのラップトップのほとんどを企業ネットワークにワイヤレスで接続するように変更しました。トラフィック量の多いマルウェア攻撃の後、ワイヤレス構成のため、イベントを特定のユーザーに絞り込むことが困難でした。
企業が取るべき行動は次のうちどれでしょうか?
A. ユーザーを 5GHz 周波数に制限します。
B. メッシュ ネットワークにアップグレードします。
C. PSK から Enterprise に移行します。
D. WPA2 暗号化を実装します。
正解: **C (**コメントを発表する**)**
Using Pre-Shared Key (PSK) authentication means that all users share the same Wi-Fi password, making it difficult to identify individual users when security incidents occur.
Migrating to WPA2-Enterprise (or WPA3-Enterprise) replaces PSK authentication with individual user credentials using 802.1X authentication and a RADIUS server. This allows the organization to:
Track and log specific user activity
Enforce per-user authentication policies
Improve network security
Breakdown of Options:
A). Restrict users to the 5GHz frequency - Improves performance but does not enhance user tracking or security.
B). Upgrade to a mesh network - A mesh network improves coverage, not security tracking.
C). Migrate from PSK to Enterprise - # Correct answer. WPA2-Enterprise or WPA3-Enterprise uses individual user authentication, allowing per-user tracking.
D). Implement WPA2 encryption - WPA2 is already widely used; it does not resolve the tracking issue.
Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.4: Given a scenario, implement wireless security measures.
IEEE 802.1X: Authentication framework for network access control

質問: **52**
ある会社の最高経営責任者 (CEO) が、さまざまな国を旅行するときに使用する新しい携帯電話を購入します。CEO は、SIM カードを使用して、電話で発信および着信ができる必要があります。CEO の携帯電話に必要な携帯電話技術は次のどれですか。
A. WDMA
B. CDMA
C. GSM
D. SLA
正解: **(**正解を表示します**)**
GSM (Global System for Mobile communications) is the international standard that uses SIM cards to authenticate and connect phones to the cellular network. GSM allows users to place and receive calls while traveling globally, provided they have a SIM card. CDMA, on the other hand, does not use SIM cards in the same way and is primarily used in the United States. (Reference: CompTIA Network+ Study Guide, Chapter on Network Fundamentals)

質問: **53**
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: **54**
セキュリティインシデントが発生した後、技術者が会社のデータが盗まれたことを明らかにしました。調査中に、ホストがスイッチを装っていたことが判明しました。発生した攻撃について最もよく説明されているのは次のうちどれですか？
A. VLANホッピング
B. 邪悪な双子
C. DNSポイズニング
D. ARPスプーフィング
正解: **A (**コメントを発表する**)**
VLAN hopping occurs when an attacker tricks a switch into believing the host is another switch by generating tagged frames or exploiting trunk negotiation (DTP). This allows the attacker to access traffic from multiple VLANs, potentially stealing sensitive data.

B). Evil twin is a rogue wireless AP attack, unrelated to switch impersonation.
C). DNS poisoning corrupts name resolution, not VLAN access.
D). ARP spoofing is a Layer 2 on-path attack, not masquerading as a switch.
References (CompTIA Network+ N10-009):
Domain: Network Security - VLAN hopping attacks, switch spoofing techniques.

質問: **55**
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: **56**
次のプロトコルのうち、デフォルトの管理距離値が 90 であるものはどれですか。
A. 安らかに眠ってください
B. EIGRP
C. OSPF
D. BGP
正解: **(**正解を表示します**)**
EIGRP (Enhanced Interior Gateway Routing Protocol) has a default administrative distance (AD) value of 90 for internal routes. The administrative distance is used to rate the trustworthiness of routing information received from different routing protocols. EIGRP, developed by Cisco, has an AD of 90, which is lower than that of RIP (120) and OSPF (110), making it more preferred if multiple protocols provide a route to the same destination.References: CompTIA Network+ study materials.

質問: **57**
標準ユーザーが 1 つのアカウントで複数のリソースにログインできるようにするには、次のうちどれを使用しますか?
A. 半径
B. MFA
C. TACACS+
D. SSO
正解: **D (**コメントを発表する**)**

Single Sign-On (SSO) enables a user to access multiple resources or applications with one set of credentials, improving usability and security. The document confirms:
"Single Sign-On (SSO) allows a user to authenticate once and gain access to multiple resources or applications without needing to log in again for each. It streamlines the login process and improves security by reducing the number of passwords that need to be managed."

質問: **58**
大企業のジュニア ネットワーク技術者は、サブネットあたり 14 個のホストを持つクラス C アドレスからネットワークを作成する必要があります。必要なホスト ビット数は、次のどれですか。
A. 3つ
B. 4つ
C. 2つ
D. 1つ
正解: **(**正解を表示します**)**

質問: **59**
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: **60**
次のどれが、出口インターフェースを決定するために最長プレフィックス一致を使用しますか?
A. ARPテーブル
B. MACアドレステーブル
C. ルーティングテーブル
D. Netstatテーブル
正解: **C (**コメントを発表する**)**
The longest prefix match is a routing concept used to find the most specific route to a destination IP address.
The routing table performs this calculation to determine the exit interface for a packet, ensuring the most accurate delivery. The document explains:
"Routers use the longest prefix match when searching the routing table to determine the best path for an IP packet. This ensures that the most specific (and thus optimal) route is chosen, based on the destination IP address."

質問: **61**
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: (正解を表示します)
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."

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 **608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
ファイアウォール管理者は、サーバーの内部 IP アドレスをパブリック用の外部 IP アドレスにマッピングしています。
この関数の名前は次のどれですか?
A. NAT
B. VIP
C. PAT
D. BGP
正解: (正解を表示します)
Network Address Translation (NAT) is a process that allows a device, typically a firewall or router, to map private IP addresses to public IP addresses. This enables internal network devices to communicate over the internet using a single or a limited number of public IP addresses.
Static NAT (One-to-One Mapping): Maps a single private IP address to a single public IP address, commonly used for servers that need to be accessible from the internet.
Dynamic NAT (Many-to-Many Mapping): Dynamically assigns a public IP from a pool to internal devices.
PAT (Port Address Translation): A type of NAT where multiple private IPs share a single public IP using different port numbers.
Incorrect Options:
B: VIP (Virtual IP Address): Used in load balancing and high-availability configurations, not for NAT.
C: PAT (Port Address Translation): A specific form of NAT, but the question refers to general NAT, making option A the best choice.
D: BGP (Border Gateway Protocol): A routing protocol used to exchange information between different networks, not related to NAT.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Network Address Translation (NAT)

質問: **63**
ネットワークコンサルタントは、イーサネットアップリンクを実行するか、内蔵の
WAP 上の 5GHz ツーポイント機能。コンサルタントがこの決定を下す際に役立つ最適な情報を提供するドキュメントは次のどれですか。
A. 物理図
B. サービスレベル契約
C. 論理図
D. サイト調査結果
正解: (正解を表示します)

質問: **64**
技術者は、ホット アイル/コールド アイル換気を実践しているデータ センターのラックに機器を設置することを計画しています。ラックに設置する際、機器の排気口は次のどの方向に向ける必要がありますか。
A. サイド
B. トップ
C. 前面
D. リア
正解: (正解を表示します)
In a data center that practices hot aisle/cold aisle ventilation, equipment should be installed so that the exhaust faces the rear of the rack. This setup ensures that hot air is expelled into the hot aisle, maintaining proper airflow and cooling efficiency.
* Hot Aisle/Cold Aisle Configuration: Equipment intake should face the cold aisle where cool air is supplied, and exhaust should face the hot aisle where hot air is expelled.
* Cooling Efficiency: Proper orientation of equipment helps maintain an efficient cooling environment by segregating hot and cold air, preventing overheating and improving energy efficiency.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses data center design principles, including hot aisle/cold aisle configurations.
* Cisco Data Center Design Guide: Provides best practices for data center layout and equipment installation.
* Network+ Certification All-in-One Exam Guide: Covers data center environmental controls and ventilation strategies.

質問: **65**
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: **66**
組織では、オンプレミスでホストされている電子メール サーバーからパートナーに暗号化された電子メール メッセージを送信する機能が必要です。組織は、ファイアウォール ルールを作成するときに標準のデフォルト ポートを使用することを好みます。要件を満たすには、次のどのポートを開く必要がありますか。
A. 110
B. 143
C. 587
D. 636
正解: (正解を表示します)

Port 587 is the standard default port for sending email (SMTP) with TLS encryption, which is used to secure email transmissions between mail servers or between clients and mail servers. Allowing traffic over port 587 enables secure email sending while maintaining standard protocol usage. (Reference: CompTIA Network+ Study Guide, Chapter on Ports and Protocols)

質問: **67**
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: **68**
3人の新入社員から、会社のリソースにアクセスできないものの、お互いのデバイスには接続できるという報告がありました。この問題を解決するために、最も変更が必要な項目は次のうちどれですか？
A. ゲートウェイ上のルーティングテーブル
B. ルーターのDNS設定
C. DHCPサーバ上のプール
D. ワークステーション上のファイアウォール
正解: **(**正解を表示します**)**
If the three new employees can communicate with each other's devices, that strongly suggests their local Layer 2/Layer 3 connectivity is working (same VLAN/subnet, switching is fine, and they have IP addressing that allows local communication). The fact that they cannot access company resources (often on other subnets, servers, or the internet via internal routing) points to a problem with how these new endpoints are being addressed or routed beyond their local segment.
The most likely shared root cause affecting only "new employees" is DHCP scope/pool configuration. If the DHCP pool is exhausted, mis-scoped, or handing out incorrect options (such as an incorrect default gateway, wrong subnet mask, or an address range tied to an isolated VLAN), users could still talk locally but fail to reach resources outside their subnet. Modifying the DHCP server pool (expanding the scope, correcting the scope network, or ensuring the correct options are assigned) would resolve this with minimal changes.
A gateway routing table issue would typically affect many users, not just three new ones. DNS misconfiguration on the router would more commonly cause name-resolution problems, not block all resource access (and wouldn't be isolated to only new employees). A workstation firewall would not usually prevent access to "company resources" in a way that consistently affects three new devices while still allowing peer connectivity.

質問: **69**
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: **A (**コメントを発表する**)**
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: **70**
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: **71**
ネットワーク管理者は、2 台のルーターをポイントツーポイント構成で接続し、IP スペースを節約する必要があります。管理者は次のどのサブネットを使用する必要がありますか?
A. 724
B. /26
C. /28
D. /30
正解: **(**正解を表示します**)**
Using a /30 subnet mask is the most efficient way to conserve IP space for a point-to-point connection between two routers. A /30 subnet provides four IP addresses, two of which can be assigned to the router interfaces, one for the network address, and one for the broadcast address. This makes it ideal for point-to- point links where only two usable IP addresses are needed.References: CompTIA Network+ study materials and subnetting principles.

質問: **72**
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: **73**
敵対者が悪魔の双子攻撃を実行する際に行うのは次のうちどれですか?
A. 正規のネットワークと同一のSSIDを持つAPを使用するようにユーザーを騙す
B. アドレス解決を操作してデバイスを悪意のあるエンドポイントに誘導する
C. 同一のMACアドレスを提示してネットワークリソースへの不正アクセスを取得する
D. 2つの正当なエンドポイント間で転送中のデータをキャプチャしてデータを盗む
正解: **(**正解を表示します**)**
An evil twin attack sets up a rogue AP with the same SSID as a legitimate wireless network, tricking users into connecting. Once connected, the attacker can intercept traffic or harvest credentials.
B). Describes ARP spoofing.
C). Describes MAC spoofing.
D). Describes on-path attacks, which may follow, but the evil twin method begins with SSID impersonation.
References (CompTIA Network+ N10-009):
Domain: Network Security - Wireless threats, rogue APs, evil twin.

質問: **74**
保存データに関する機密性の役割を最もよく説明しているのは次のどれですか?
A. 管理ネットワーク上の誰でもデータにアクセスできます。
B. 適切なトレーニングを受ければ、データにリモートでアクセスできます。
C. 特権アクセスが許可された後にデータにアクセスできます。
D. ハッシュを検証した後、データにアクセスできます。
正解: **C (**コメントを発表する**)**
Confidentiality with Data at Rest: Confidentiality is a core principle of data security, ensuring that data stored (at rest) is only accessible to authorized individuals. This protection is achieved through mechanisms such as encryption, access controls, and permissions.
Privileged Access: The statement "Data can be accessed after privileged access is granted" aligns with the confidentiality principle, as it restricts data access to users who have been granted specific permissions or roles. Only those with the appropriate credentials or permissions can access the data.
Incorrect Options:
A:"Data can be accessed by anyone on the administrative network." This violates the principle of confidentiality by allowing unrestricted access.
B:"Data can be accessed remotely with proper training." This focuses on remote access rather than restricting access based on privileges.
D:"Data can be accessed after verifying the hash." This option relates more to data integrity rather than confidentiality.
CompTIA Network+ materials on data security principles, particularly sections on confidentiality and access control mechanisms.

質問: **75**
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)
* Troubleshooting Methodology:
* Troubleshooting involves a systematic approach to diagnosing and resolving issues. It typically includes steps such as identifying symptoms, gathering information, formulating and testing theories, and implementing solutions.
* Confirming a Theory:
* Duplicate the Problem: To confirm a theory, the technician should reproduce the problem in a controlled environment. This helps verify that the identified cause actually leads to the observed issue.
* Verification: By duplicating the problem, the technician can observe the issue firsthand, validate the hypothesis, and rule out other potential causes.
* Comparison with Other Steps:
* Identify the Symptoms: Initial step to understand what the problem is, not specifically for confirming a theory.
* Gather Information: Involves collecting data and details about the issue, usually done before formulating a theory.
* Determine Any Changes: Involves checking for recent changes that could have caused the issue, a part of the information-gathering phase.
* Implementation:
* Use similar equipment or software in a test environment to recreate the issue.
* Observe the results to see if they match the original problem, thereby confirming the theory.
References:
* CompTIA Network+ study materials on troubleshooting methodologies and best practices.

質問: **76**
次のどれが送信元と宛先の間のトラフィックの傍受を可能にしますか?
A. 自己署名証明書
B. VLANホッピング
C. オンパス攻撃
D. フィッシング
正解: **C** (コメントを発表する)
An on-path attack (formerly known as a man-in-the-middle (MITM) attack) involves intercepting and potentially altering communications between two parties without their knowledge. This can be done via techniques like ARP poisoning, rogue access points, or SSL stripping.
Breakdown of Options:
A: Self-signed certificate - These are untrusted SSL certificates but do not intercept traffic.
B: VLAN hopping - VLAN hopping exploits VLAN misconfigurations but does not necessarily intercept communications.
C: On-path attack - Correct answer. This intercepts and modifies traffic between two endpoints.
D: Phishing - Phishing tricks users into revealing credentials rather than intercepting network traffic.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.2: Explain common security concepts.
NIST SP 800-115: Guide to Security Testing and Assessments

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 **608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
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: **(正解を表示します)**
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: **78**
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: **79**
次のコネクタ タイプのうち、Wi-Fi アンテナに最もよく関連付けられるのはどれですか?
A. BNC
B. SFP
C. MPO
D. RJ45
正解: **(正解を表示します)**
BNC (Bayonet Neill-Concelman) connectors are commonly used with coaxial cables in RF and wireless applications, including some older Wi-Fi antennas and specialized networking equipment. The document says:
"BNC (Bayonet Neill-Concelman) connectors are typically used with coaxial cables, especially in radio frequency (RF) and some Wi-Fi antenna applications, providing a secure and quick

connect/disconnect."

質問: **80**
ネットワーク エンジニアは、新しいサーバーのネットワーク設定を次のように構成します。
* IPアドレス = 192.163.1.15
* サブネットマスク = 255.255.255.0
* ゲートウェイ = 192.163.1.255
サーバーは同じサブネット上の他のホストに正常にアクセスできますが、異なるサブネット上のホストにはアクセスできません。次のうち、正しく構成されていない可能性が高いのはどれですか?
A. サブネットマスク
B. ゲートウェイ
C. デフォルトルート
D. IP アドレス
正解: (正解を表示します)
The default gateway for a network should be an IP address within the subnet, but not the broadcast address. In this case:
IP: 192.163.1.15
Subnet Mask: 255.255.255.0
This means the network range is: 192.163.1.0 - 192.163.1.255
192.163.1.255 is the broadcast address for this subnet, so it cannot be used as a gateway.
Hence, the device fails to communicate outside its subnet because it's trying to use a broadcast address as its gateway.
The issue is clearly with the gateway configuration.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 1.4: "Given a scenario, configure and deploy common Ethernet switching features."

質問: **81**
次のルーティング テクノロジのうち、パス選択に属性リストを使用するものはどれですか。
A. BGP
B. RIP
C. EIGRP
D. OSPF
正解: (正解を表示します)
BGP (Border Gateway Protocol) uses attributes like AS path, origin, and MED (multi-exit discriminator) to determine the best path among multiple available routes.
From Andrew Ramdayal's guide:
"BGP is the protocol underlying the global routing system of the internet. It is used for routing data between autonomous systems (ASes)... BGP uses a path vector mechanism and maintains a list of attributes for route selection."

質問: **82**
ネットワークエンジニアは、ネットワーク内でブルートフォース攻撃、DDoS攻撃、ポートスキャンが発生した場合、それらの検出結果を相関分析し、アラートを受信する必要があります。エンジニアが導入すべきネットワーク監視テクノロジーは次のうちどれですか？
A. パケットキャプチャ
B. SNMPv3
C. SIEM
D. Syslogコレクター

正解: **C** (コメントを発表する)
A SIEM (Security Information and Event Management) platform is built to collect, correlate, and alert on security-relevant events across many sources, which is exactly what's needed to identify patterns such as brute force attempts, port scanning, and DDoS indicators. In Network+ (N10-009) security operations concepts, correlation is key: a SIEM can ingest logs from firewalls, IDS/IPS, servers, authentication systems, endpoint agents, and network devices, then apply rules/analytics to detect suspicious behavior that might not be obvious from a single log source. It can also generate real-time alerts, dashboards, and incident timelines-helping the engineer respond quickly and prioritize threats.
Packet capture provides deep visibility into traffic but is not inherently designed for enterprise-wide correlation and alerting without significant additional tooling and expertise. SNMPv3 is used for secure device monitoring (status, counters, performance) rather than detecting coordinated attack patterns. A syslog collector centralizes logs but generally does not provide the same level of correlation, enrichment, and automated alerting capabilities as a SIEM. Therefore, SIEM is the best answer.

質問: **83**
ネットワーク管理者は、主要な機器の設置場所を超えてネットワークを拡張しようとしています。管理者が追加のネットワークスイッチを設置すべき場所は次のうちどれですか？
A. MDF
B. VPC
C. VXLAN
D. IDF
正解: (正解を表示します)
When extending a network beyond the primary equipment location, additional access/distribution switches are typically placed in an IDF (Intermediate Distribution Frame) . Network+ (N10-009) infrastructure objectives differentiate between the MDF and IDF : the MDF is the main, central wiring/equipment location (often where core switches, routers, WAN demarcation, and main cross-connects reside). As a building grows or spans multiple floors/areas, an IDF is used as a secondary wiring closet to reduce cable runs, provide local switching, and aggregate user access connections back to the MDF using backbone cabling (often fiber). This supports scalability, cable management, and performance by keeping horizontal runs within recommended distance limits.
VPC (Virtual Private Cloud) is a cloud networking construct, not a physical wiring location. VXLAN is an overlay tunneling technology used in virtualized/data center networks, not where you physically install switches. The question specifically references extending the network beyond the primary equipment location, which is a classic use case for deploying an IDF to host additional switches closer to endpoint areas while uplinking back to the MDF.

質問: **84**
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、ユーザーの通信速度を向上させ、チャネルの重複を減らす設定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: **D** (コメントを発表する)
Band steering allows wireless access points to automatically direct capable devices to the 5GHz band, which typically has higher throughput and less interference than the 2.4GHz band, improving performance. The document confirms:
"Band steering helps balance wireless client loads by steering dual-band capable devices to the 5GHz band, which offers higher speeds and less channel congestion than 2.4GHz."

質問: **85**
トラブルシューターが解決策を実装した直後に実行する必要がある手順は次のうちどれですか。
A. プロセス中に学んだ教訓を振り返ります。
B. 行動計画を立てます。
C. システムの全機能を検証します。

D. アクションと結果を文書化します。
正解: **(**正解を表示します**)**
After implementing the solution, the immediate next step is to verify full system functionality. This confirms that the problem has been resolved and helps ensure no new issues have been introduced.
From Andrew Ramdayal's guide:
"After the solution is implemented, test the system to ensure that it is fully operational, and the original problem has been resolved. Also, put in place any measures that could prevent the issue from recurring."

質問: **86**
リクエストをリッスンし、Web サーバー間でユーザー トラフィックを分散するには、次のテクノロジのうちどれが最適な選択肢でしょうか。
A. ルーター
B. スイッチ
C. ファイアウォール
D. ロードバランサー
正解: **(**正解を表示します**)**
A load balancer is designed to distribute user requests across multiple servers to ensure high availability and performance.
Breakdown of Options:
A: Router - Directs traffic between networks, not between web servers.
B: Switch - Works at Layer 2, does not distribute web traffic.
C: Firewall - Secures network traffic, but does not distribute load.
D: Load balancer - # Correct answer. Optimizes web traffic distribution across multiple servers.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.5: Explain load balancing and redundancy concepts.

質問: **87**
ネットワーク エンジニアは、Web サイトが IPv6 と互換性があるかどうかを確認するためにテストを行っています。Web サイトの IPv6 アドレスで ping を実行しようとしたところ、エンジニアは DNS が適切に設定されていないと判断しました。この問題を解決するために、ネットワーク エンジニアは次のどれを実行する必要がありますか。
A. PTR レコードを有効にします。
B. 既存の TXT レコードを更新します。
C. 新しい AAAA レコードを追加します。
D. セカンダリ NS レコードを設定します。
正解: **(**正解を表示します**)**
*AAAA records map domain names to IPv6 addresses, enabling proper resolution.
*PTR records (A) are for reverse DNS lookups.
*TXT records (B) store text-based information, not IP addresses.
*NS records (D) define authoritative name servers but don't directly affect IPv6 resolution.
#Reference: CompTIA Network+ N10-009 Official Documentation - DNS Configuration & IPv6.

質問: **88**
企業のクラウドやネットワークなどのリソースに、直接接続されているかのように安全にアクセスするために使用されるネットワーク アクセス方法は、次のうちどれですか。
A. ジャンプボックス/ホスト
B. セキュアシェル

C. クライアント対サイトVPN
D. GREトンネル
正解: **(**正解を表示します**)**
A client-to-site VPN (remote-access VPN) is designed to let an individual user securely connect into an organization's network over an untrusted network (like the internet) and access resources as if the user were locally connected . Network+ objectives emphasize VPNs as encrypted tunnels that provide confidentiality and integrity for traffic, commonly using technologies such as IPsec or SSL/TLS-based VPNs. With a client- to-site VPN, the user's device establishes a tunnel to the corporate VPN gateway, receives routes (and sometimes DNS settings), and can reach internal subnets and cloud resources according to policy.
A jump box/host is a hardened intermediate system used to access sensitive segments, but it does not make the user's device behave as if it is directly on the network; it provides controlled administrative access. SSH is a secure remote management protocol for connecting to a host's command line-useful for administration, not full network access to multiple internal resources. A GRE tunnel provides encapsulation but does not provide encryption by itself , so it is not inherently "securely access" unless combined with additional security (e.g., GRE over IPsec). Therefore, client-to-site VPN is the correct choice.

質問**: 89**
攻撃の一環として、脅威の攻撃者はスイッチ上のコンテンツ アドレス可能メモリ (CAM) テーブルを意図的にオーバーフローさせます。このシナリオは、次のどのタイプの攻撃の例ですか。
A. ARPスプーフィング
B. 邪悪な双子
C. MACフラッディング
D. DNS ポイズニング
正解**: C (**コメントを発表する**)**
* Definition of MAC Flooding:
* MAC flooding is an attack where a malicious actor sends numerous fake MAC addresses to a switch, overwhelming its CAM table. The CAM table stores MAC addresses and their associated ports for efficient traffic forwarding.
* Impact of MAC Flooding:
* CAM Table Overflow: When the CAM table is full, the switch cannot learn new MAC addresses and is forced to broadcast traffic to all ports, leading to a degraded network performance and potential data interception.
* Switch Behavior: The switch operates in a fail-open mode, treating the network as a hub, which can be exploited for eavesdropping on traffic.
* Comparison with Other Attacks:
* ARP Spoofing: Involves sending false ARP (Address Resolution Protocol) messages to associate the attacker's MAC address with the IP address of another device.
* Evil Twin: Involves creating a rogue wireless access point that mimics a legitimate one to intercept data.
* DNS Poisoning: Involves corrupting the DNS cache with false information to redirect traffic to malicious sites.
* Preventive Measures:
* Port Security: Configure port security on switches to limit the number of MAC addresses per port, preventing CAM table overflow.
* Network Segmentation: Use VLANs to segment network traffic and limit the impact of such attacks.
References:
* CompTIA Network+ study materials on network security threats and mitigation techniques.

質問**: 90**
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: **91**
ある組織が最近、新しいコンピュータをLANに接続しました。ユーザーはデフォルトゲートウェイにpingを実行できません。技術者が設定を調べたところ、自己割り当てIPアドレスが見つかりました。最も可能性の高い原因は次のどれですか？
A. DHCPサーバーが利用できません
B. RFC1918アドレスが使用されています
C. TCP/IPスタックが無効になっています
D. 静的IPが割り当てられています
正解: **A (**コメントを発表する**)**
When a host fails to obtain an IP address from a DHCP server, it assigns itself an APIPA (Automatic Private IP Addressing) address in the 169.254.x.x range, commonly described as a "self-assigned IP." This prevents communication outside the local link, including reaching the default gateway.
B). RFC1918 addresses are private ranges (10.x.x.x, 172.16-31.x.x, 192.168.x.x), but these are not self- assigned.
C). If the TCP/IP stack were disabled, the host wouldn't have any IP at all.
D). If a static IP were assigned, it would show a configured value, not self-assigned.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - IP addressing issues, DHCP failures, APIPA behavior.

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 **608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
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: **93**
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: **94**
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: **95**
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: **A (**コメントを発表する**)**
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: **96**
セキュリティ管理者が、IPアドレス192.168.100.1/25を持つデバイス用に新しいファイアウォールオブジェクトを作成しようとしています。しかし、ファイアウォールソフトウェアは設定フィールドでドット付き10進表記のみを使用しています。適切なサブネットマスクは次のうちどれですか？
A. 255.255.254.0
B. 255.255.255.1
C. 255.255.255.128
D. 255.255.255.192
正解: **(**正解を表示します**)**
A /25 subnet mask means 25 bits are reserved for the network portion, leaving 7 bits for host addresses. In dotted decimal, that is:
11111111.11111111.11111111.10000000
Decimal equivalent: 255.255.255.128
A). 255.255.254.0 corresponds to /23.
B). 255.255.255.1 is invalid as a subnet mask.
D). 255.255.255.192 corresponds to /26.
Thus, the correct subnet mask for a /25 network is 255.255.255.128.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Subnetting, CIDR notation, dotted decimal.

質問: **97**
ネットワークエンジニアは、WAN接続に使用する新しいルーターを受け取りました。ネットワークエンジニアが新しいルーターを接続すべきレイヤーを最もよく表しているのは次のうちどれですか？
A. Access
B. Core
C. Leaf
D. Spine
正解: **(正解を表示します)**
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
In a spine-leaf architecture, endpoints (including servers, firewalls, and WAN/edge routers) connect to leaf switches. Leaf switches then uplink to spine switches; spine switches do not have endpoints connected directly to them. Therefore, a WAN router (an external/edge device) should connect to the leaf layer-often specifically to a "border leaf" that handles external connectivity.
Why not B. Core or D. Spine? In spine-leaf, "core" isn't a formal layer, and spines are designed only to interconnect leafs, not to terminate endpoints.
Why not A. Access? "Access" is a term from the traditional three-tier model (access-distribution-core). In modern spine-leaf language, the analogous layer for endpoint attachment is the leaf.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Data center and campus architectures (spine-leaf vs. three-tier), roles of leaf/spine, WAN/edge connectivity points.

質問: **98**
次のどの VPN タイプが、Web ポータルを介してネットワーク リソースへの安全なリモート アクセスを提供しますか?
A. プロキシ
B. クライアントレス
C. サイト間
D. 直接接続
正解: **(正解を表示します)**
Clientless VPNsallow users to access network resources through asecure web portal using a browser, with no VPN software needed. This is ideal for occasional access to internal resources via HTTPS.
* A. Proxyis a gateway for accessing web content, not a VPN.
* C. Site-to-siteVPN connects entire networks, not individual users.
* D. Direct Connectusually refers to dedicated cloud connections, not VPNs.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 3.3 - Given a scenario, configure and deploy common VPN technologies.

質問: **99**
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: **100**
次のどの種類の標的型攻撃が、複数のコンピューターまたはボットを使用して同じリソースを繰り返し要求しますか?
A. パス上
B. DDoS
C. ARPスプーフィング
D. MACフラッディング
正解: **(正解を表示します)**
A Distributed Denial of Service (DDoS) attack leverages multiple computers or bots (botnet) to flood a target system with requests, overwhelming its resources and making it unavailable to legitimate users. This is a common tactic used by attackers to disrupt services. The document explains:
"A DDoS (Distributed Denial of Service) attack involves multiple computers (often called bots) simultaneously sending requests to a single resource, overwhelming the system and causing a denial of service to legitimate users."

質問: **101**
建物内に機器を設置する際に考慮すべき環境要因は次のどれですか? (2 つ選択してください)。
A. 消火システム
B. UPS の場所
C. 湿度制御
D. 電力負荷
E. 床構造タイプ
F. 最も近いMDFへの近さ
正解: **A (コメントを発表する)**
When installing equipment in a building, environmental factors are critical to ensure the safety and longevity of the equipment. A fire suppression system is essential to protect the equipment from fire hazards. Humidity control is crucial to prevent moisture-related damage, such as corrosion and short circuits, which can adversely affect electronic components. Both factors are vital for maintaining an optimal environment for networking equipment.References: CompTIA Network+ study materials.

質問: **102**
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: **(正解を表示します)**
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: **103**
ネットワーク管理者は新しいネットワーク検出ツールを設定しようとしていますが、業務に支障をきたすのではないかと懸念しています。管理者は次のスキャンタイプのうちどれを設定すべきでしょうか？
A. 認証済み
B. アドホック
C. 認証されていません
D. スケジュール済み
正解: **(**正解を表示します**)**
If the administrator is concerned a new discovery tool could disrupt operations, the safest option is to configure scheduled scans. Network+ (N10-009) operations guidance emphasizes minimizing impact by running potentially noisy tasks (discovery, vulnerability checks, inventory scans) during defined maintenance windows or off-peak hours. A scheduled scan allows controlled timing, predictable load, and easier coordination with change management, monitoring, and support teams. This reduces the risk of saturating links, overwhelming devices with queries, or triggering alerts during business-critical periods.
Ad hoc scanning is on-demand and may occur at any time, which increases the chance of disruption if run during peak usage. Authenticated versus unauthenticated describes whether the scanner uses credentials to log into systems for deeper visibility; that choice affects depth and accuracy, but it doesn't directly address when scanning occurs to reduce business impact. An authenticated scan can still be disruptive if run at the wrong time, and an unauthenticated scan can still generate significant traffic. Since the key concern is operational disruption, controlling scan timing via scheduled scans is the best mitigation.

質問: **104**
ユーザーが最近、ワークステーションをオフィス内の別の場所に移動しました。インターネットへのアクセスと印刷は可能ですが、サーバーリソースにアクセスできません。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. デフォルトゲートウェイが正しくありません
B. VLANの割り当てが間違っています
C. エラー無効ポート
D. IPアドレスが重複しています
正解: **B (**コメントを発表する**)**
If a workstation can access the internet and printers (likely in another VLAN) but not internal servers, the port was likely placed into the wrong VLAN after the move. VLAN assignment controls Layer 2 segmentation, restricting access to resources on different VLANs.
A). A wrong default gateway would prevent internet access.
C). An error-disabled port would block all connectivity.
D). A duplicate IP would cause general network issues, not just missing server access.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - VLAN misconfiguration, connectivity issues.

質問: **105**
仮想マシンの構成は次のとおりです。
- IPv4アドレス: 169.254.10.10
- サブネットマスク: 255.255.0.0
仮想マシンは共存するシステムにはアクセスできますが、インターネット上の外部アドレスにはアクセスできません。根本的な原因として最も可能性が高いのは次のどれですか?
A. サブネットマスクが正しくありません。

B. DHCP サーバーはオフラインです。
C. IP アドレスは RFC1918 プライベート アドレスです。
D. DNS サーバーにアクセスできません。
正解: **(**正解を表示します**)**
Understanding the 169.254.x.x Address:
An IPv4 address in the range of 169.254.x.x is an Automatic Private IP Addressing (APIPA) address, assigned when a DHCP server is unavailable.
DHCP Server Offline:
APIPA Assignment: When a device cannot obtain an IP address from a DHCP server, it assigns itself an APIPA address to enable local network communication. This allows communication with other devices on the same local subnet but not with external networks.
Resolution: Ensure the DHCP server is operational. Check for connectivity issues between the virtual machine and the DHCP server, and verify the DHCP server settings.
Comparison with Other Options:
The subnet mask is incorrect: The subnet mask 255.255.0.0 is appropriate for the 169.254.x.x range and does not prevent external access by itself.
The IP address is an RFC1918 private address: RFC1918 addresses are private IP ranges (10.x.x.x, 172.16.x.x-
172.31.x.x, 192.168.x.x) but 169.254.x.x is not one of them.
The DNS server is unreachable: While this could affect name resolution, it would not prevent the assignment of a non-APIPA address or local network communication.
Troubleshooting Steps:
Verify the DHCP server's status and connectivity.
Restart the DHCP service if necessary.
Renew the IP lease on the virtual machine using commands such as ipconfig /renew (Windows) or dhclient (Linux).
References:
CompTIA Network+ study materials on IP addressing and DHCP troubleshooting.

質問: **106**
ネットワーク エンジニアは、スイッチと LAN に接続されたルーターの間に新しい IDS を実装したいと考えています。エンジニアは、ゲートウェイのラインに IDS を配置することで遅延が発生することを望んでいません。エンジニアは、IDS がすべてのパケットを損失なく確認できるようにしたいと考えています。エンジニアが IDS を実装するのに最適な方法は、次のうちどれですか。
A. ネットワーク タップを使用します。
B. Nmap ソフトウェアを使用します。
C. プロトコル アナライザーを使用します。
D. ポートミラーを使用します。
正解: **D (**コメントを発表する**)**
Reference: CompTIA Network+ Certification Exam Objectives - Network Security 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　**608**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 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: **108**

ネットワークのセキュリティを確保するために、次の要件が満たされていることを確認する必要があります。

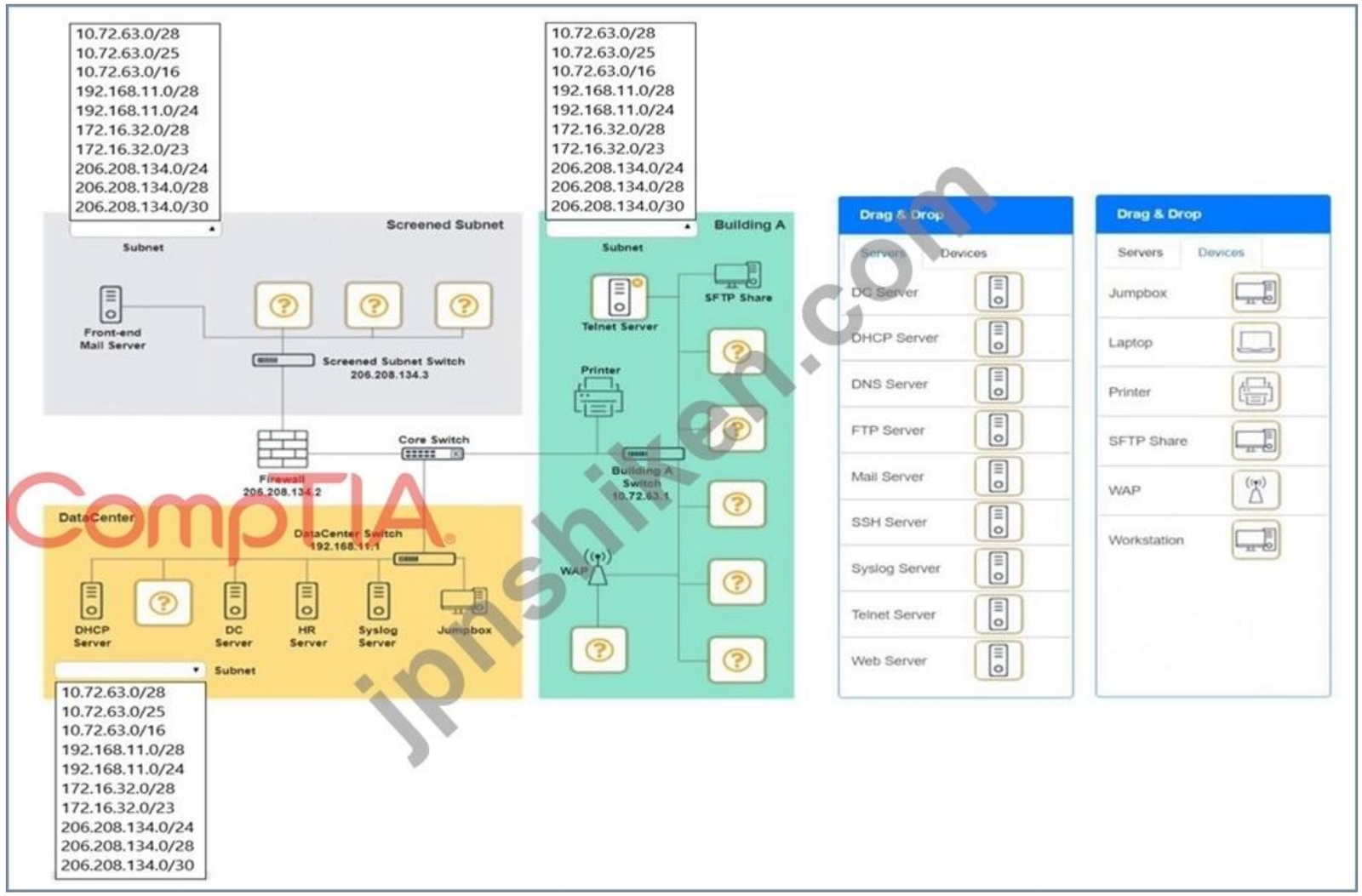
要件：

データセンター

ネットワークがサブネット化され、すべてのデバイスが適切に通信できるようになり、アドレス空間の使用を最小限に抑えます。IP アドレスとホスト名を正しく解決し、ポート 53 のトラフィックを処理する専用サーバーを用意します。ビルディング A ネットワークがサブネット化され、すべてのデバイスが適切に通信できるようになり、アドレス空間の使用を最小限に抑えます。5 人の追加のオフィス ユーザーをサポートするデバイスを用意します。モバイル ユーザーを追加します。Telnet サーバーをより安全なソリューションに置き換えます。スクリーン サブネット ネットワークがサブネット化され、すべてのデバイスが適切に通信できるようになり、アドレス空間の使用を最小限に抑えます。外部の 80/443 トラフィックを処理するサーバーを用意します。ポート 20/21 トラフィックを処理するサーバーを用意します。手順 オブジェクトを適切な場所にドラッグ アンド ドロップします。オブジェクトは複数回使用でき、すべてのプレースホルダーを埋める必要はありません。

使用可能なオブジェクトは、ドラッグ アンド ドロップ メニューの [サーバー] タブと [デバイス] タブの両方にあります。

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。



CompTIA
jpnshiken.com

正解:

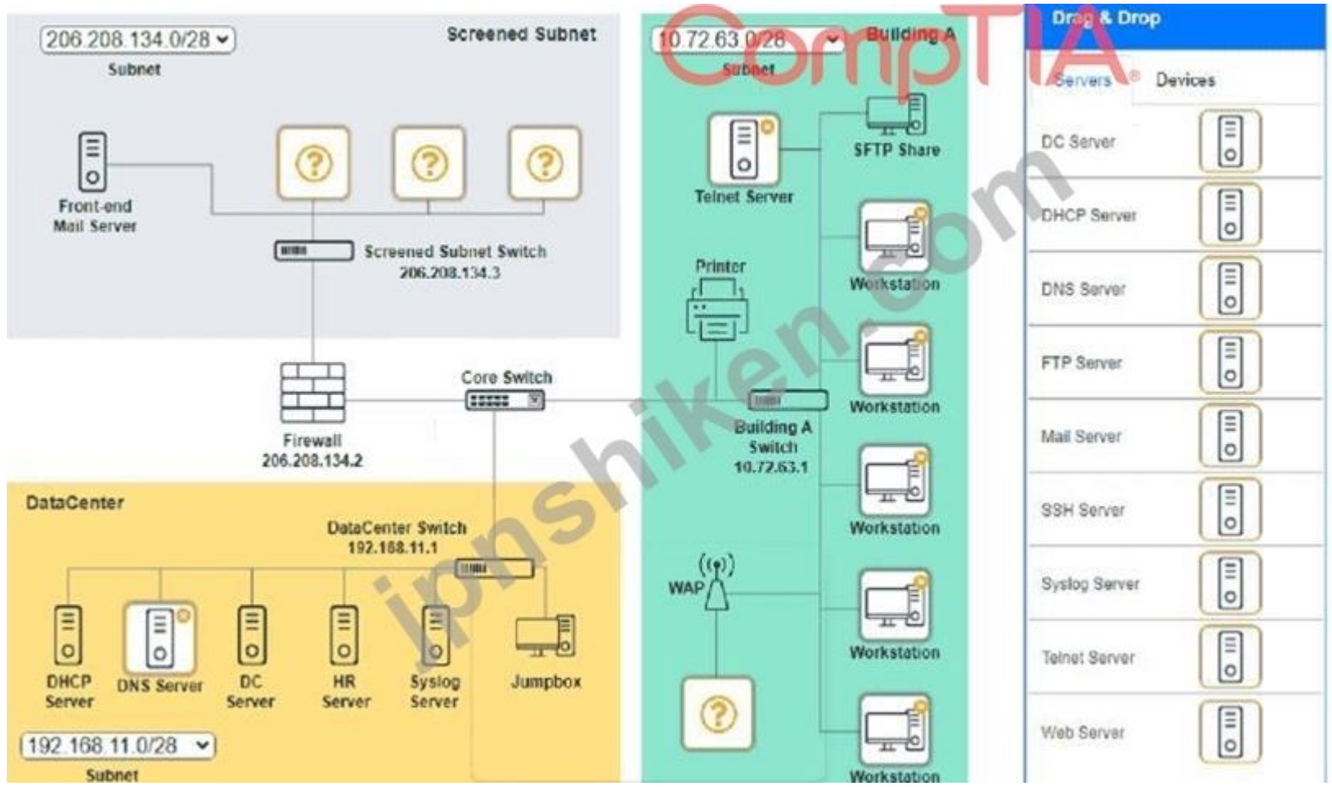
See explanation below.

Explanation:

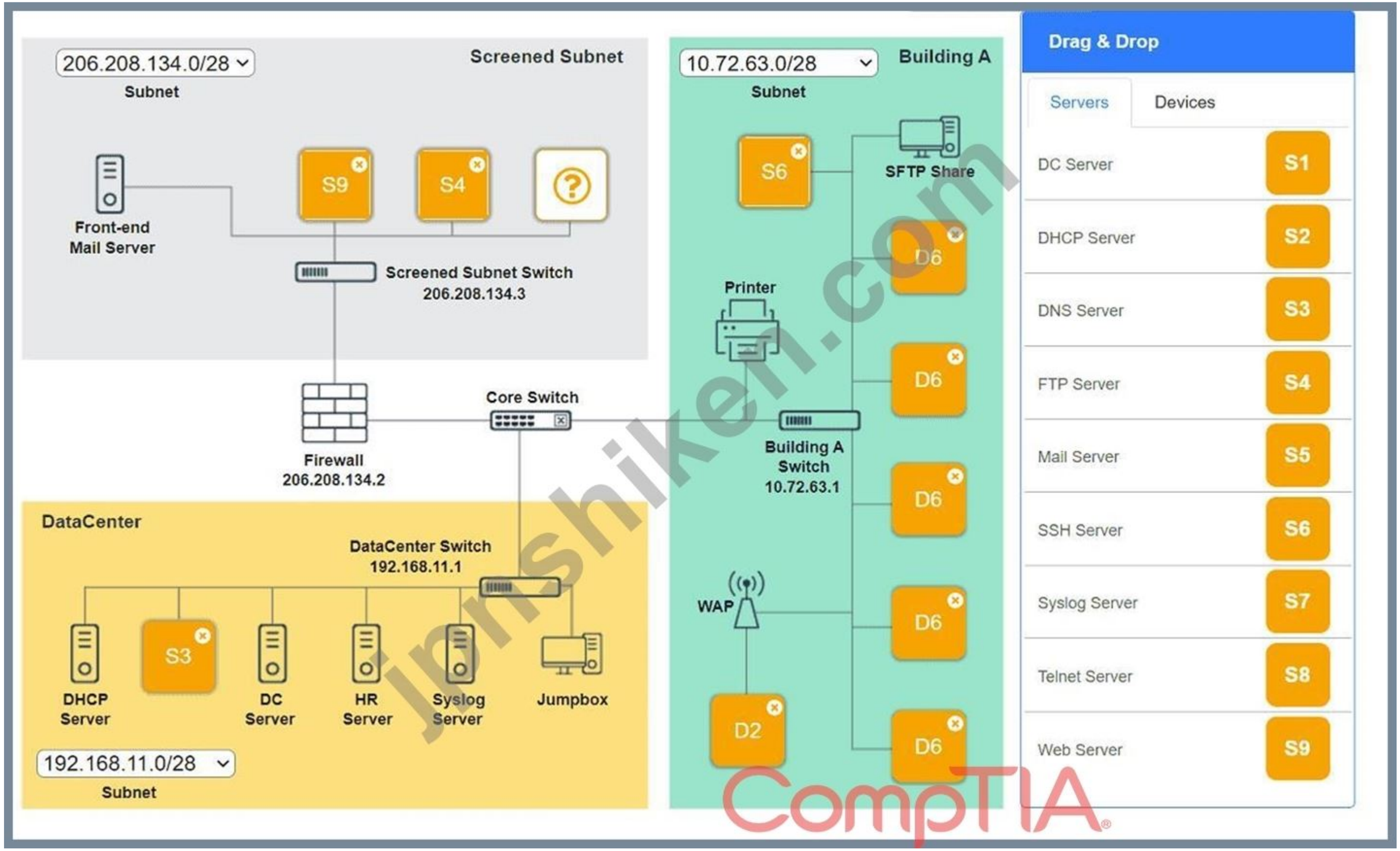
Screened Subnet devices - Web server, FTP server

Building A devices - SSH server top left, workstations on all 5 on the right, laptop on bottom left DataCenter devices - DNS server.

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: **109**

次の内部ルーティング プロトコルのうち、高速コンバージェンスとループフリーという特徴が最も優れているのはどれですか。

A. BGP

B. STP
C. OSPF
D. 安らかに眠ってください
正解: **(**正解を表示します**)**
The correct answer is OSPF (Open Shortest Path First). OSPF is a link-state routing protocol known for its fast convergence and use of the Dijkstra algorithm to calculate the shortest loop-free path. It efficiently scales to large enterprise networks and avoids routing loops by maintaining a complete topology map.
A). BGP is primarily an external routing protocol used between ISPs, not internal.
B). STP is not a routing protocol; it prevents loops at Layer 2.
D). RIP is an older distance-vector protocol with slower convergence and a maximum hop limit of 15.
OSPF's design makes it the preferred internal gateway protocol (IGP) for medium-to-large organizations requiring speed and loop-free reliability.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - IGPs, OSPF, routing protocols.

質問: **110**
ネットワーク管理者が最近、レイヤー 3 スイッチの設定を更新しました。更新後、特定のファイル サーバーにアクセスできなくなったとユーザーから報告がありました。最も考えられる原因は次のどれですか。
A. ACL が正しくありません
B. スイッチングループ
C. IPアドレスが重複しています
D. デフォルトルートが間違っています
正解: **(**正解を表示します**)**
*Since this issue occurred after a configuration change on a Layer 3 switch, the most likely cause is misconfigured ACLs (Access Control Lists).
*ACLs control which traffic is allowed or denied, so an incorrect ACL may be blocking access to the file server.
*Why not the other options?
*Switching loop (B): A switching loop occurs at Layer 2 (not Layer 3) and causes network-wide broadcast storms, not just loss of access to a file server.
*Duplicate IP addresses (C): This would cause connectivity issues for the devices with the conflict, but not necessarily prevent all users from accessing the file server.
*Wrong default route (D): The default route is used for traffic leaving the local network. If users are unable to access an internal file server, this is unlikely to be the issue.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 8: Network Access Control and ACLs

質問: **111**
建物内のワイヤレス ネットワーク カバレッジの有効性を説明するために作成されたものはどれですか。
A. 論理図
B. レイヤー3ネットワーク図
C. サービスレベル契約
D. ヒートマップ
正解: **D (**コメントを発表する**)**
* Definition of Heat Maps:
* A heat map is a graphical representation of data where individual values are represented by colors. In the context of wireless networking, a heat map shows the wireless signal strength in different areas of a building.
* Purpose of a Heat Map:

* Heat maps are used to illustrate the effectiveness of wireless networking coverage, identify dead zones, and optimize the placement of access points (APs) to ensure adequate coverage and performance.
* Comparison with Other Options:
* Logical Diagram: Represents the logical connections and relationships within the network.
* Layer 3 Network Diagram: Focuses on the routing and IP addressing within the network.
* Service-Level Agreement (SLA): A contract that specifies the expected service levels between a service provider and a customer.
* Creation and Use:
* Heat maps are created using specialized software or tools that measure wireless signal strength throughout the building. The data collected is then used to generate a visual map, guiding network administrators in optimizing wireless coverage.
References:
* CompTIA Network+ certification materials and wireless network planning guides.

質問: **112**
1 つのソースと、同じサービスを実行する複数のサーバー間でトラフィックを再配布するために使用されるのは次のどれですか。
A. ルーター
B. スイッチ
C. ファイアウォール
D. ロードバランサー
正解: **D (**コメントを発表する**)**
The correct answer is Load balancer because it is specifically designed to distribute incoming network traffic across multiple backend servers that provide the same application or service. According to CompTIA Network+ (N10-009) objectives under network infrastructure, load balancing improves performance, scalability, and high availability by preventing any single server from becoming overwhelmed.
A load balancer can operate at Layer 4 (transport layer, based on IP address and port) or Layer 7 (application layer, based on content such as HTTP headers or URLs). It uses various algorithms such as round-robin, least connections, or weighted distribution to efficiently allocate client requests among servers. If one server fails, the load balancer can redirect traffic to healthy servers, ensuring service continuity.
A router (Option A) forwards packets between different networks but does not distribute traffic among servers running the same application. A switch (Option B) forwards frames within a local network based on MAC addresses. A firewall (Option C) filters traffic based on security rules but does not perform traffic distribution for load-sharing purposes.
Therefore, a load balancer is the correct solution for redistributing traffic among multiple servers.

質問: **113**
ある会社のマーケティング チームが新しいアプリケーションを作成し、newapplication.comptia.org の DNS レコードを作成して、常に www.comptia.org と同じアドレスに解決したいと考えています。管理者は次のレコードのどれを使用する必要がありますか?
A. SOA
B. MX
C. CNAME
D. NS
正解: **(**正解を表示します**)**
A CNAME (Canonical Name) record is used in DNS to alias one domain name to another. This means that newapplication.comptia.org can be made to resolve to the same IP address as www.comptia.org by creating a CNAME record pointing newapplication.comptia.org to www.comptia.org. SOA (Start of Authority) is used for DNS zone information, MX (Mail Exchange) is for mail server records, and NS (Name Server) is for specifying authoritative DNS servers.
Reference:

The DNS section of the CompTIA Network+ materials describes the use of CNAME records for creating domain aliases.

質問: **114**
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: **A (**コメントを発表する**)**
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: **115**
次のどれが内部アプリケーションへの安全なリモート アクセスを許可しますか?
A. VPN
B. CDN
C. SAN
D. IDS
正解: **A (**コメントを発表する**)**
A Virtual Private Network (VPN) creates an encrypted connection between a remote user and an internal network, ensuring secure access to internal applications.
* VPNs use encryption protocols like IPSec and SSL/TLS to protect data during transmission.
* They are widely used for secure remote work, accessing company resources, and bypassing geographic restrictions.
* Option B (CDN - Content Delivery Network): Used for speeding up website content delivery, not for remote access security.
* Option C (SAN - Storage Area Network): Used for high-speed storage, unrelated to remote access.
* Option D (IDS - Intrusion Detection System): Monitors for malicious activities but does not provide secure access to applications.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Secure Remote Access Technologies

質問: **116**
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。

Router A

Routing Table | Routing Configuration

```
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, GigabitEthernet3
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.4.0/22 is directly connected, GigabitEthernet2
C        10.0.6.0/24 is directly connected, GigabitEthernet2
L        10.0.6.1/32 is directly connected, GigabitEthernet2
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.0/30 is directly connected, GigabitEthernet3
L        172.16.27.1/32 is directly connected, GigabitEthernet3
```

jpnshiken.com CompTIA

Reset to Default | Save | Close

Router C

Routing Table | Routing Configuration

```
Router-C# 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


      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S        10.0.0.0/22 [1/0] via GigabitEthernet1
S        10.0.4.0/22 [1/0] via GigabitEthernet2
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.0/30 is directly connected, GigabitEthernet2
L        172.16.27.2/32 is directly connected, GigabitEthernet2
C        172.16.27.4/30 is directly connected, GigabitEthernet1
L        172.16.27.6/32 is directly connected, GigabitEthernet1
```

Reset to Default | Save | Close

ComTIA shiken.com

jpnshiken.com
CompTIA

jpnshiken.com
CompTIA

正解:

See the solution in Explanation.

Explanation:

To validate routing between networks hosting Workstation A and File Server 2, follow these steps:

Review Routing Tables:

Check the routing tables of Router A, Router B, and Router C to identify any missing routes.

Identify Missing Routes:

Ensure that each router has routes to the networks on which Workstation A and File Server 2 are located.

Add Static Routes:

If a route is missing, add a static route to the relevant destination network via the correct interface.

Routing Table:

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, GigabitEthernet3

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

C 10.0.4.0/22 is directly connected, GigabitEthernet2

C 10.0.6.0/24 is directly connected, GigabitEthernet2

L 10.0.6.1/32 is directly connected, GigabitEthernet2
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.27.0/30 is directly connected, GigabitEthernet3
L 172.16.27.1/32 is directly connected, GigabitEthernet3
Routing Table:
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, GigabitEthernet1
L 10.0.0.1/32 is directly connected, GigabitEthernet1
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
Routing Table:
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S 10.0.0.0/22 [1/0] via GigabitEthernet1
S 10.0.4.0/22 [1/0] via GigabitEthernet2
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.27.0/30 is directly connected, GigabitEthernet2
L 172.16.27.2/32 is directly connected, GigabitEthernet2
C 172.16.27.4/30 is directly connected, GigabitEthernet1
L 172.16.27.6/32 is directly connected, GigabitEthernet1
Install Static Route to 10.0.0.0/22 via 172.16.27.1 (assuming Router C ' s IP is 172.16.27.1):
Destination Prefix: 10.0.0.0
Destination Prefix Mask: 255.255.252.0
Interface: GigabitEthernet3
Install Static Route to 10.0.4.0/22 via 172.16.27.5 (assuming Router C ' s IP is 172.16.27.5):
Destination Prefix: 10.0.4.0
Destination Prefix Mask: 255.255.252.0
Interface: GigabitEthernet1
Install Static Route to 10.0.6.0/24 via 172.16.27.2 (assuming Router A ' s IP is 172.16.27.2):
Destination Prefix: 10.0.6.0
Destination Prefix Mask: 255.255.255.0
Interface: GigabitEthernet2
Install Static Route to 10.0.0.0/22 via 172.16.27.1 (assuming Router B ' s IP is 172.16.27.1):
Destination Prefix: 10.0.0.0
Destination Prefix Mask: 255.255.252.0
Interface: GigabitEthernet1
Summary of Static Routes:
Router A:
ip route 10.0.0.0 255.255.252.0 GigabitEthernet3

Router B:
ip route 10.0.4.0 255.255.252.0 GigabitEthernet1
Router C:
ip route 10.0.6.0 255.255.255.0 GigabitEthernet2
ip route 10.0.0.0 255.255.252.0 GigabitEthernet1
These configurations ensure that each router knows the correct paths to reach Workstation A and File Server 2, resolving the connectivity issue.

質問**: 117**
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**: A (**コメントを発表する**)**
* 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**: 118**
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: **119**
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. Switch11 で自動ネゴシエーションを無効にします。
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. ポートのネイティブ VLAN を変更します。
正解: **(**正解を表示します**)**

質問: **120**
ネットワーク管理者は、すべてのネットワークポートで認証されたデバイスのみを許可するセキュリティ方式が使用されていることを確認する必要があります。ソリューションは以下の要件を満たす必要があります。
* なりすましの可能性が減少
* 集中管理ソリューション
* 監査可能なログ
この機能を提供するテクノロジは次のどれですか?
A. MACフィルタリング
B. ポートセキュリティ
C. ACL
D. 802.1X
正解: **(**正解を表示します**)**
802.1X provides port-based network access control that requires authentication before a switch port grants full network access. It uses a supplicant (client), an authenticator (switch/AP), and an authentication server (commonly RADIUS) to validate credentials or certificates. This directly supports the requirements: it reduces spoofing compared with MAC-based controls because authentication can be identity- and certificate-based rather than relying on easily forged MAC addresses; it is centrally managed through AAA infrastructure and policy (users/devices/groups); and it produces auditable logs via the authentication server and network devices, enabling accountability and investigation. Network+ security objectives emphasize AAA, NAC, and strong access controls for both wired and wireless networks. MAC filtering and basic port security rely largely on MAC addresses and are susceptible to spoofing; they also tend to be harder to manage at scale and provide weaker centralized auditing. ACLs control traffic flows but do not authenticate endpoints at the port level, so they cannot ensure "only authenticated devices" can connect. Therefore, 802.1X is the technology that best meets all stated requirements.

質問: **121**
次のケーブル タイプのうち、トランシーバーを必要とせずに QSFP ポートを使用できるのはどれですか。
A. マルチモード
B. ツインアクシャル
C. RG11
D. カテゴリー6
正解: **(**正解を表示します**)**
Twinaxial (Direct Attach Copper / DAC) cables can plug directly into QSFP ports without needing separate optical transceivers. They are cost-effective for short-distance, high-speed connections (commonly in data centers).
A). Multimode fiber requires SFP/QSFP transceivers to convert electrical signals to optical.
C). RG11 is coaxial cable for broadband/cable TV, not used in QSFP ports.
D). Category 6 is twisted-pair Ethernet cabling, not directly compatible with QSFP ports.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Cable types, QSFP, DAC (Twinaxial), transceiver requirements.

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 **608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
無線技術者は、ユーザー デバイスが利用可能な最適な周波数標準に自動的に移動できるようにするテクノロジを実装したいと考えています。技術者は次のテクノロジのどれを使用すべきでしょうか。
A. バンドステアリング
B. 無線LANコントローラ
C. 指向性アンテナ
D. 自律アクセスポイント
正解: **(**正解を表示します**)**
Band Steering: This technology enables wireless devices to connect to the most optimal frequency band (2.4 GHz or 5 GHz) by encouraging capable devices to switch to the less congested 5 GHz band. This improves overall network performance and prevents overcrowding on the 2.4 GHz band.
Wireless LAN controller (B): This manages multiple access points in a network but does not handle frequency optimization.
Directional antenna (C): This focuses the signal in a specific direction but does not affect frequency selection.
Autonomous access point (D): This operates independently but lacks advanced features like band steering.
Reference: CompTIA Network+ Official Study Guide, Domain 1.6 (Wireless Standards and Technologies).

質問: **123**
ネットワーク技術者が、サーバーとスイッチ間の接続に新しい6m（19.7フィート）のCat 6 UTPケーブルを設置しました。サーバーへの通信速度が低下し、NICの統計情報にはパケットのドロップとCRCエラーが表示されています。技術者は、エラーを軽減するために、以下のどのケーブルを代わりに使用する可能性が高いでしょうか？
A. 同軸ケーブル
B. 9.8フィート（3m）ケーブル
C. プレナムケーブル

D. STPケーブル
正解: **D (**コメントを発表する**)**
The errors described - dropped packets and CRC (Cyclic Redundancy Check) errors - often indicate electromagnetic interference (EMI) on unshielded twisted pair (UTP) cabling. The correct replacement is STP (Shielded Twisted Pair), which has shielding that protects signals from external interference, ensuring better reliability in noisy environments such as data centers or near heavy electrical equipment.
A). Coaxial is not used for modern Ethernet server-switch links.
B). Shorter UTP cable does not solve EMI issues.
C). Plenum cable refers to cable jacket type for fire safety, not electrical shielding.
STP cabling reduces interference and ensures reliable gigabit+ Ethernet connections between servers and switches.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Cabling issues, UTP vs. STP, EMI.

質問: **124**
ゴールデン構成を作成する最も適切な理由は次のうちどれですか?
A. 構成の一貫性を保つため
B. 設定ファイルのサイズを小さくする
C. 設定を暗号化してセキュリティを強化する
D. 各デバイスのバックアップ構成を設定するには
正解: **(**正解を表示します**)**
A golden configuration is a baseline configuration file that contains approved, standardized settings for network devices. The purpose is to ensure configuration consistency across the environment. This prevents misconfigurations, supports compliance with organizational or regulatory standards, and accelerates recovery if a device needs reconfiguration.
B). Reducing file size is not the goal of golden configs.
C). Golden configs can include security settings, but they are not inherently encrypted - they are simply a baseline template.
D). While configs can be backed up, golden configs are more about standardization, not device-specific backups.
By maintaining a golden configuration, administrators can quickly detect unauthorized changes (by comparing running configs against the golden file) and enforce consistency across devices. This improves network stability, reduces troubleshooting complexity, and enhances security posture.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Configuration management, golden images/configurations.

質問: **125**
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: **C (**コメントを発表する**)**
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: **126**
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: **127**
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: (正解を表示します)
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.

質問: **128**
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: **129**
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: **(**正解を表示します**)**
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: **130**
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: **131**
ネットワーク管理者は、オフィスエリアにワイヤレス ネットワークを導入しました。ユーザーが屋外パティオを訪れ、大きな添付ファイルのある電子メールをダウンロードしたり、トレーニング ビデオをストリーミングしたりしようとすると、バッファリングの問題が発生します。

最も可能性の高い原因は次のどれですか?
A. ネットワークの混雑
B. 無線干渉
C. 信号劣化
D. クライアントの切断
正解: (正解を表示します)
The most likely cause of buffering issues when moving outdoors is signal degradation. Wireless signals weaken as they travel through obstacles such as walls, glass, and air, leading to weaker connections and reduced data rates.
Breakdown of Options:
A). Network congestion - While congestion can slow down network speeds, it affects all users, not just those moving outdoors.
B). Wireless interference - Interference is possible but is more likely caused by other wireless signals rather than outdoor movement.
C). Signal degradation - Correct answer. Wireless signals weaken with distance and obstacles such as walls, reducing performance.
D). Client disassociation - Disassociation occurs when clients lose connection to the AP, but the question states that users experience buffering, indicating they are still connected but with a weak signal.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.6: Analyze wireless networking technologies.
IEEE 802.11 standards: Wi-Fi propagation characteristics

質問: **132**
IPS と IDS の主な違いは次のどれですか?
A. IPS はトラフィックに合わせてインストールする必要がありますが、IDS はそうする必要はありません。
B. IPS はシグネチャベースですが、IDS はシグネチャベースではありません。
C. IPS は IDS よりも誤検知の影響を受けにくくなります。
D. IPS では IDS よりも管理オーバーヘッドが少なくなります。
正解: (正解を表示します)
The key difference is that an Intrusion Prevention System (IPS) is installed in line with network traffic, allowing it to actively block threats. In contrast, an Intrusion Detection System (IDS) only monitors and alerts without actively blocking traffic.
Breakdown of Options:
A: An IPS needs to be installed in line with traffic and an IDS does not. # Correct answer. IPS actively prevents threats, while IDS only detects them.
B: An IPS is signature-based and an IDS is not. - False, both can use signature-based detection.
C: An IPS is less susceptible to false positives than an IDS. - False, both can produce false positives, depending on configurations.
D: An IPS requires less administrative overhead than an IDS. - False, IPS requires more administrative effort due to real-time blocking decisions.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.4: Explain network security devices.

質問: **133**
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: **134**
設置するラックのサイズを決定する要因として最も可能性が高いのはどれですか (2 つ選択してください)。
A. KVMのサイズ
B. スイッチの深さ
C. ハードドライブのサイズ
D. 冷却ファンの速度
E. コンセントのアンペア数
F. サーバーの高さ
正解: **B (**コメントを発表する**)**
Understanding Rack Size Determination:
The size of a rack for installation is determined by the dimensions of the equipment to be housed in it, primarily focusing on the depth and height of the devices.
Switch Depth:
Depth of Equipment: The depth of network switches and other rack-mounted devices directly influences the depth of the rack. If the equipment is deeper, a deeper rack is required to accommodate it.
Industry Standards: Most racks come in standard depths, but it is essential to match the depth of the rack to the deepest piece of equipment to ensure proper fit and airflow.
Server Height:
Height of Equipment: The height of servers and other devices is measured in rack units (U), where 1U equals
1.75 inches. The total height of all equipment determines the overall height requirement of the rack.
Rack Units: A rack's height is typically described in terms of the number of rack units it can accommodate, such as 42U, 48U, etc.
Why Other Options are Less Relevant:
KVM Size: While important for management, KVM (Keyboard, Video, Mouse) switches do not typically determine rack size.
Hard Drive Size: Individual hard drives are installed within servers or storage devices, not directly influencing rack dimensions.
Cooling Fan Speed: Fan speed affects cooling but not the physical size of the rack.
Outlet Amperage: Power requirements do not determine rack dimensions but rather the electrical infrastructure supporting the rack.
References:
CompTIA Network+ study materials on rack installation and equipment sizing.

質問: **135**
音声トラフィックに過度のジッタが発生しています。ネットワークエンジニアは通話パフォーマンスと明瞭度を改善したいと考えています。エンジニアは次のうちどの機能を設定する必要がありますか？
A. QoS
B. STP
正解: **A (**コメントを発表する**)**
Quality of Service (QoS) prioritizes delay-sensitive traffic such as VoIP by assigning higher priority in queues, reducing jitter, latency, and packet loss. Implementing QoS policies ensures stable and clear voice communication.
B). STP (Spanning Tree Protocol) prevents switching loops, but it does not address jitter or real-time traffic performance.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - QoS, traffic shaping, prioritization of voice/video.

質問: **136**

次のどれがリモート ユーザーがネットワークに接続することを可能にしますか?
A. コマンドラインインターフェース
B. APIゲートウェイ
C. クライアント対サイトVPN
D. ジャンプボックス
正解: **(**正解を表示します**)**
A Client-to-Site VPN allows a remote user to securely connect to a company's internal network, providing access as if they were physically on-site.

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 **608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **137**
攻撃者が悪意のある双子を設定した後に最も発生する可能性が高い攻撃の種類は次のどれですか?
A. パス上
B. DDoS
C. ARPスプーフィング
D. フィッシング
正解: **A (**コメントを発表する**)**
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
An evil twin is a malicious wireless access point that impersonates a legitimate SSID. Once victims connect, the attacker can intercept and manipulate traffic, performing an on-path (man-in-the-middle) attack- capturing credentials, injecting content, or downgrading encryption.
B). DDoS overwhelms services with traffic; it's not the typical follow-on from clients joining a rogue AP.
C). ARP spoofing is another way to become on-path on wired segments, but with an evil twin, the wireless association itself enables the on-path position.
D). Phishing is social engineering; while an evil twin could be used to present fake portals, the primary technical posture after connection is on-path.
References (CompTIA Network+ N10-009):
Domain: Network Security - Wireless threats (rogue APs/evil twins), traffic interception, on-path attacks.

質問: **138**
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: **(**正解を表示します**)**
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.

質問: **139**
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: **A (**コメントを発表する**)**
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: **140**
早朝、管理者は新しい DHCP サーバーをインストールします。午後、一部のユーザーからネットワークが停止していると報告がありました。次のどれが最も可能性の高い問題でしょうか。
A. 管理者が十分な IP アドレスをプロビジョニングしませんでした。
B. 管理者が誤ったデフォルトゲートウェイを設定しました。
C. 管理者が十分なルートをプロビジョニングしませんでした。
D. 管理者が十分な MAC アドレスをプロビジョニングしませんでした。
正解: **(**正解を表示します**)**
When a DHCP server is installed and not enough IP addresses are provisioned, users may start experiencing network outages once the available IP addresses are exhausted. DHCP servers assign IP addresses to devices on the network, and if the pool of addresses is too small, new devices or those renewing their lease may fail to obtain an IP address, resulting in network connectivity issues.References: CompTIA Network+ study materials.
質問: **141**
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: **142**
メイン施設の向かい側にある建物にネットワークを拡張するための最も適切なソリューションは次のどれですか?
A. マルチモードファイバー
B. 802.11ac ワイヤレス ブリッジ
C. Cat 6 銅線
D. ループバックアダプタ
正解: (正解を表示します)
An802.11ac wireless bridgeis the most practical solution to connect two nearby buildingswithout trenching or laying physical cable. It provides high-speed, point-to-point connectivity using directional antennas.
* A. Multimode fiberis effective but expensive and typically limited to 500 meters or less.
* C. Cat 6 copperis only rated for up to 100 meters - not viable for a street-wide distance.
* D. Loopback adapteris a troubleshooting tool, not for network extension.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 1.3 - Compare and contrast various network topologies, types, and technologies.

質問: **143**
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: (正解を表示します)
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: **144**
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: **145**
ネットワーク技術者が、100Mbpsのレイヤ2スイッチで構成される社内ネットワークを設定しています。技術者はスイッチ間のアップリンクのスループットを向上させたいと考えています。技術者はスイッチ間に複数の冗長リンクを接続します。技術者が設定すべき項目は次のうちどれですか？
A. スパニングツリープロトコル
B. スイッチ仮想インターフェース
C. ネイティブVLAN
D. ファーストホップ冗長プロトコル
正解: **(正解を表示します)**
When multiple redundant links exist between switches, Spanning Tree Protocol (STP) is required to prevent switching loops. STP blocks redundant paths but can allow aggregation if configured with protocols like LACP.
B). SVIs provide Layer 3 interfaces, not loop prevention.
C). Native VLAN defines the untagged VLAN but does not manage loops.
D). FHRP (VRRP, HSRP, GLBP) provides gateway redundancy, not switch uplink management.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - STP, redundancy, loop prevention.

質問: **146**
ある会社では、サーバーへのすべての接続を暗号化する必要があるセキュリティをホストしています。ジュニア管理者は、Web サーバーをハード化する必要があります。Web サーバー上の次のポート。Web サーバー上の次のポートが開いています。

443
80
22
587

次のポートのうちどれを無効にする必要がありますか?
A. 22
B. 80
C. 443
D. 587
正解: **B (コメントを発表する)**
For a web server that requires all connections to be encrypted, port 80 (HTTP) should be disabled. Port 80 is used for unencrypted web traffic, whereas port 443 is used for HTTPS, which provides encrypted communication.
Port 80 (HTTP): This port is used for unsecured web traffic. Disabling this port ensures that all web traffic must use HTTPS, which encrypts the data in transit.
Port 443 (HTTPS): This port is used for secure web traffic via SSL/TLS encryption. Keeping this port open ensures that secure connections can be made to the web server.
Other Ports:

Port 22: Used for SSH, providing secure remote access and file transfers.
Port 587: Used for secure email submission (SMTP) with encryption.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Discusses the roles and security implications of various ports and protocols.
Cisco Networking Academy: Provides training on secure web server configuration and port management.
Network+ Certification All-in-One Exam Guide: Covers port security and best practices for securing web servers.

質問: **147**
ファイアウォールに変更を加えた後、ユーザーは Web サーバーにアクセスできなくなりました。ネットワーク管理者は、Web サーバーのポート 80 と 443 が引き続きユーザーの IP 空間からアクセス可能であることを確認したいと考えています。
このテストを実行するのに最適なコマンドはどれですか?
A. 掘る
B. イフコンフィグ
C. nmap
D. ピン
正解: **(**正解を表示します**)**

質問: **148**
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: **(**正解を表示します**)**
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: **149**
クライアントとサーバー間でネットワーク ステータス メッセージを送信するために使用されるプロトコルは次のどれですか。
A. SSH
B. DHCP
C. NTP
D. SNMP
正解: **(**正解を表示します**)**
The correct answer is SNMP (Simple Network Management Protocol) because it is specifically designed to collect and transmit network management and status information between managed devices and management systems. According to CompTIA Network+ (N10-009) objectives, SNMP is used for monitoring and managing network devices such as routers, switches, servers, and printers.

SNMP operates using a manager-agent model. The SNMP manager (such as a network monitoring server) communicates with SNMP agents installed on network devices. Agents send traps and inform messages, which are unsolicited status alerts indicating events such as device failures, high CPU usage, or link outages.
The manager can also poll agents to retrieve performance metrics and configuration details stored in the Management Information Base (MIB).
SSH (Option A) is used for secure remote administration. DHCP (Option B) dynamically assigns IP addresses. NTP (Option C) synchronizes time between devices. None of these protocols are designed for network status monitoring and alert messaging.
Therefore, SNMP is the correct protocol for sending networking status messages between devices and management systems.
Bottom of Form

質問: **150**
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: **151**
インシデント発生後に最初に復旧する必要がある重要なシステムを特定する災害復旧 (DR) 計画の一部は次のどれですか。
A. RTO
B. SLA
C. MTBF
D. SIEM
正解: **(**正解を表示します**)**
RTO stands for Recovery Time Objective, which defines the maximum acceptable amount of time that a system, application, or function can be down after a failure or disaster. It helps prioritize which systems need to be recovered first based on their importance to business operations.
SLA (Service Level Agreement) refers to an agreement between a service provider and a customer regarding expected performance and availability, but it does not dictate recovery order.
MTBF (Mean Time Between Failures) is a measure of reliability and time between hardware or system failures.
SIEM (Security Information and Event Management) is a centralized tool for logging and alerting but not relevant to DR recovery prioritization.
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 **608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **152**
複数のサテライト オフィスと本社間の専用のプライベート接続を提供するために通常専用回線を使用するネットワーク アーキテクチャのタイプは次のどれですか。
A. メッシュ
B. ポイントツーポイント
C. ハブとスポーク
D. スター
正解: **(**正解を表示します**)**
The correct answer is hub-and-spoke. In this design, the head office serves as the hub, and all satellite or branch offices (the spokes) connect directly to the hub using leased lines or VPNs. Communication between spokes typically passes through the hub, which centralizes connectivity and simplifies management.
A). Mesh involves every site connecting to every other site, which is more redundant but costly.
B). Point-to-point describes a single dedicated link between two sites, not a multi-site topology.
D). Star is often used in LAN switching, with all devices connecting to a central switch, but it's not the WAN architecture typically used here.
Hub-and-spoke is a cost-effective WAN design, as fewer circuits are needed compared to full mesh. However, its main disadvantage is reliance on the hub site: if the hub goes down, inter-spoke communication fails.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - WAN topologies (hub-and-spoke, mesh, point-to-point).

質問: **153**
データ回復の目標を説明するものは次のどれですか?
A. MTBF
B. RPO
C. BCP
D. 平均所要時間
正解: **B (**コメントを発表する**)**
RPO (Recovery Point Objective) describes a data recovery goal by defining the maximum acceptable amount of data loss measured in time. For example, an RPO of 4 hours means the organization must be able to restore data to a point no more than four hours before the outage-so backups, replication, or snapshots must occur frequently enough to meet that target. In Network+ (N10-009) operations objectives, disaster recovery and business continuity concepts include understanding recovery metrics and how they influence backup strategies, replication design, and service resilience planning. RPO specifically answers: "How much data can we afford to lose?" By contrast, MTBF (Mean Time Between Failures) is a reliability metric describing how often failures occur. MTTR (Mean Time To Repair/Recover) measures how long it takes to restore a system after failure, which is more aligned with service restoration time rather than data loss. BCP (Business Continuity Plan) is the overall plan/process for keeping critical business functions running during disruptions; it is not a single data recovery metric. Therefore, RPO is the correct term for a data recovery goal.

質問: **154**
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: **155**
掃除機で損傷したケーブルの代わりに、新しく圧着された 26 フィート (8 メートル) の STP Cat 6 パッチ ケーブルが最近 1 つの部屋に設置されました。現在、その部屋のユーザーはネットワークに接続できません。ネットワーク技術者は、まず既存のケーブルをテストします。コア スイッチからフロアのアクセス スイッチまで伸びる 177 フィート (54 メートル) のケーブルは機能しており、アクセス スイッチからオフィスの壁のジャックまで伸びる 115 フィート (35 メートル) のケーブルも機能しています。ユーザーがネットワークに接続できない理由として最も可能性が高いのは次のどれですか。
A. UTP ケーブルと STP ケーブルが混在して使用されています。
B. パッチ ケーブルはプレナム定格ではありません。
C. ケーブル距離を超えています。
D. パッチ ケーブルのピン配置が正しくありません。
正解: (正解を表示します)
An incorrect pinout on the patch cable could prevent network connectivity due to mismatched wiring. Even if the cables are the correct length and type, a pinout issue can cause continuity problems and prevent data transmission. Proper crimping with the correct pinout is essential for network cables to function. (Reference:
CompTIA Network+ Study Guide, Chapter on Network Media and Topologies)

質問: **156**
ネットワーク管理者は、少なくとも次のIPアドレス範囲をサポートできるサブネットを展開する必要があります。
無駄なアドレスが最も少ない 260 台のデバイス。管理者は次のサブネットのどれを使用する必要がありますか?
A. 172.16.0.0/24
B. 172.25.2.0/23
C. 172.30.1.0/22
D. 172.33.0.0/21
正解: **B** (コメントを発表する)
To support at least 260 hosts, you need at least 512 total IP addresses (accounting for network/broadcast overhead).
/23 (255.255.254.0) gives 510 usable IPs, ideal for 260 devices with minimal waste.
/24 (255.255.255.0) gives only 254 usable - not enough.
/22 (1022 usable) and /21 (2046 usable) would work but result in significant address waste.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.1 - Given a scenario, configure and apply IP addressing schemes.

質問: **157**
技術者が会社の支社に新しいネットワークハードウェアを導入しようとしています。ブリッジの優先度を適切に設定する必要があります。技術者は次のうちどれを設定する必要がありますか？

A. スパニングツリープロトコル
B. ジャンボフレーム
C. 境界ネットワーク
D. ポートセキュリティ
正解: **(**正解を表示します**)**
Spanning Tree Protocol (STP) uses bridge priority values to determine the root bridge in a switched network topology. Correctly configuring bridge priority helps in maintaining a loop-free and efficient network. The document explains:
"Spanning Tree Protocol (STP) uses bridge priority values to determine which switch will be the root bridge, ensuring loop prevention and efficient path selection within the network."

質問: **158**
技術者は、重複しないチャネルで MIMO を利用するワイヤレス接続を設定する必要があります。
次のどれが最良の選択でしょうか?
A. 802.11a
B. 802.11b
C. 802.11g
D. 802.11n
正解: **D (**コメントを発表する**)**
The 802.11n standard supports MIMO (Multiple Input Multiple Output), which allows multiple antennas to increase data throughput and improve reliability. Additionally, it uses non-overlapping channels in the 5 GHz band (and optionally the 2.4 GHz band), making it a good choice for high-speed, interference-resistant wireless connections. (Reference: CompTIA Network+ Study Guide, Chapter on Wireless Technologies)

質問: **159**
次の災害復旧の概念のうち、総稼働時間を総ユニット数で割って計算されるものはどれですか?
A. 平均所要時間
B. MTBF
C. RPO
D. RTO
正解: **(**正解を表示します**)**
Introduction to Disaster Recovery Concepts:
Disaster recovery involves strategies and measures to ensure business continuity and data recovery in the event of a disaster.
Mean Time Between Failures (MTBF):
MTBF is a reliability metric used to predict the time between failures of a system during operation. It is calculated by dividing the total operational time by the number of failures.
Formula: MTBF=Total Operational TimeNumber of Failures\text{MTBF} = \frac{\text{Total Operational Time}}{\text{Number of Failures}}MTBF=Number of FailuresTotal Operational Time This metric helps in understanding the reliability and expected lifespan of systems and components.
Example Calculation:
If a server operates for 1000 hours and experiences 2 failures, the MTBF is:
MTBF=1000 hours2=500 hours\text{MTBF} = \frac{1000 \text{ hours}}{2} = 500 \text{ hours} MTBF=21000 hours=500 hours Explanation of the Options:
A: MTTR (Mean Time to Repair): The average time required to repair a system after a failure.
B: MTBF (Mean Time Between Failures): The correct answer, representing the average time between failures.
C: RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time.
D: RTO (Recovery Time Objective): The target time set for the recovery of IT and business activities after a disaster.

Conclusion:
MTBF is a crucial metric in disaster recovery and system reliability, helping organizations plan maintenance and predict system performance.
References:
CompTIA Network+ guide explaining MTBF, MTTR, RPO, and RTO concepts and their calculations (see page Ref 10 How to Use Cisco Packet Tracer).

質問: **160**
従業員からネットワークが遅いという報告を受けました。ネットワークエンジニアは、パフォーマンスの問題は上流ルーターにあると考えています。エンジニアは問題の場所を特定するために、以下のどのツールを使用すべきでしょうか？
A. nslookupとdig
B. Nmapとスピードテスター
C. tracert と ping
D. tcpdumpとプロトコルアナライザー
正解: **(**正解を表示します**)**
To determine where slowness is occurring-especially if an upstream router is suspected-the best tools are ping and tracert/traceroute. Network+ (N10-009) troubleshooting objectives emphasize using these to test connectivity, latency, and the path packets take through the network. Ping measures reachability and round- trip time; rising latency or packet loss can indicate congestion or a failing link/device. Tracert identifies each hop along the route and reports per-hop response times, helping pinpoint whether delays begin at a specific hop (for example, the default gateway, the upstream router, or a provider edge). This allows the engineer to localize the problem area and decide whether the issue is internal, at the upstream router, or beyond.
nslookup and dig are DNS tools; they diagnose name resolution, not general network slowness location.
Nmap focuses on scanning ports/hosts, and a "speed tester" measures throughput but does not locate the failing hop. tcpdump and protocol analyzer can reveal retransmissions, windowing, or application behavior, but they are not the fastest first-choice tools for locating an upstream routing/performance bottleneck across hops. Hence, tracert and ping are the correct pair.

質問: **161**
サーバー機器をラックに設置することで得られる最も可能性の高い利点は次のどれですか?
A. 簡素化されたトラブルシューティングプロセス
B. 消費電力の減少
C. ネットワークパフォーマンスの向上
D. 計算密度の向上
正解: **(**正解を表示します**)**
Installing server equipment in a rack increases compute density by allowing multiple servers to be organized efficiently in a vertical configuration, saving space while housing more devices in a smaller footprint. This is critical for data centers and businesses with high hardware demands.
Simplified troubleshooting process (A): While racks can aid in organizing equipment, this is a secondary benefit, not the primary purpose.
Decreased power consumption (B): Rack installation does not directly reduce power usage; equipment power consumption remains the same.
Improved network performance (C): Racking servers does not inherently improve network performance; that depends on network configurations.
Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (Rack Installations).

質問: **162**
異なる場所にある2つのネットワークスイッチが、10マイル（16km）離れた場所から光ファイバーケーブルで接続されています。パッチパネルとスイッチ間のデュプレックス光ファイバーパッチコードが誤って挟まれ、2つのスイッチ間の接続が切断されました。ネットワーク技術者は、断線したケーブルを新しいシングルモードパッチコードに交換しました。しかし、両スイッチ間の接続は依然としてダウンしており、リンクランプも消灯したままです。
技術者が最初に実行する必要があるアクションは次のうちどれですか?
A. スイッチ内の光ファイバトランシーバを交換します

B. スイッチにログインしてスイッチポートをシャットダウンし、再度有効にします
C. 新しいパッチコードの片端にある2つのファイバーコネクタを入れ替えます
D. シングルモード光ファイバーパッチコードをマルチモード光ファイバーパッチコードに交換します。
正解**: C (**コメントを発表する**)**
Fiber connections require Tx on one end to connect to Rx on the other end. If the patch cord is replaced and link lights remain off, the most common cause is that the connectors are reversed. Swapping (transposing) the connectors ensures proper transmit/receive alignment.
A). Replacing the transceiver may eventually be necessary, but only after verifying correct connections.
B). Restarting the switchport won't resolve a physical misconnection.
D). Using multimode fiber would be incorrect here, as the link was designed for single-mode (10 miles/16 km requires SMF).
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Fiber connectivity, Tx/Rx alignment, link light diagnostics.

質問**: 163**
ある中小企業は新しい電話機を導入しており、その一部の電話機にはフル HD ビデオ会議機能が搭載されています。
最高情報責任者 (CIO) は、トラフィックが特定のしきい値に達するとネットワークがトラフィックを処理できなくなる可能性があることを懸念しています。ネットワーク エンジニアは、これらの懸念を軽減するために次のどれを設定できますか。
A. 100Mbpsの速度制限を持つVLAN
B. VoIPトラフィックを誘導するIPヘルパー
C. より小さいサブネットマスク
D. すべてのユーザーポートで全二重
正解**: D (**コメントを発表する**)**
Full duplex mode allows devices to send and receive data simultaneously, improving network performance and reducing congestion, which is critical for VoIP and video conferencing.
Breakdown of Options:
A). A VLAN with 100Mbps speed limits - VLANs segment traffic but limiting speeds to 100Mbps would worsen video performance.
B). An IP helper to direct VoIP traffic - IP helper is used for DHCP relay, not for VoIP optimization.
C). A smaller subnet mask - A smaller subnet reduces IP address availability but does not improve network performance.
D). Full duplex on all user ports - Correct answer. Full duplex eliminates collisions, allowing better VoIP and video performance.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.2: Compare and contrast various networking devices.
IEEE 802.3: Ethernet Full Duplex Operation

質問**: 164**
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**: C (**コメントを発表する**)**
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: **165**
ネットワーク管理者は、ESSID を使用してワイヤレス ネットワークを構成しています。SSID と比較した場合の ESSID のユーザー メリットは次のどれですか。
A. より強力なワイヤレス接続
B. アクセスポイント間のローミング
C. 高度なセキュリティ
D. スループットの向上
正解: **(**正解を表示します**)**
An Extended Service Set Identifier (ESSID) allows multiple access points to share the same SSID, enabling seamless roaming for users. This means that users can move between different access points within the same ESSID without losing connection or having to reauthenticate. This provides a better user experience, especially in large environments such as office buildings or campuses.References: CompTIA Network+ study materials.

質問: **166**
会社がオフィスにフロアを追加した後、ネットワーク管理者はネットワークに新しい VLAN をインストールしました。ユーザーは新しい VLAN で IP アドレスを取得できませんが、既存の VLAN のポートは正常に動作しています。管理者は次のどの構成を更新する必要がありますか?
A. スコープサイズ
B. アドレス予約
C. リース時間
D. IP ヘルパー
正解: **(**正解を表示します**)**
When a new VLAN is created, it typically exists on a different subnet. If DHCP servers are on a different VLAN, the network needs an IP helper address to forward DHCP requests correctly. Without it, clients in the new VLAN won't receive an IP address.
Breakdown of Options:
A: Scope size - Increasing the DHCP scope would not resolve the issue if requests aren't reaching the server.
B: Address reservations - Reservations only assign specific addresses to devices; they do not fix DHCP communication issues.
C: Lease time - Changing the lease time does not impact DHCP functionality across VLANs.
D: IP helper - Correct answer. This forwards DHCP requests across VLANs to the DHCP server.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.4: Explain IP addressing technologies and subnetting.
RFC 1542: BOOTP (Bootstrap Protocol) relay agents

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 **608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **167**

次の接続方法のうち、ネットワーク エンジニアが環境全体のネットワーク デバイスの構成展開を自動化できるのはどれですか。
A. RDP
B. Telnet
C. SSH
D. GUI
正解: **(**正解を表示します**)**
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
SSH provides secure, scriptable remote access used by automation/orchestration tools (e.g., leveraging CLI, NETCONF over SSH, or Ansible modules) to push configurations at scale.
A). RDP is primarily for Windows GUI sessions and is not commonly used for network device automation.
B). Telnet can be scripted but is insecure (plaintext); modern best practice is to use SSH.
D). GUI access is typically manual and not ideal for scalable, repeatable automation.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Configuration management, automation/orchestration, secure management protocols (SSH vs. Telnet), change at scale.

質問: **168**
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: **169**
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: **170**
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: **171**
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: **172**
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**: 173**
スプリット トンネル VPN のコスト効率の面での利点は次のどれですか?
A. Web トラフィックは Web フィルターによってフィルター処理されます。
B. 会社のインターネット接続には、より多くの帯域幅が必要です。
C. 監視により、会社のネットワーク上の安全でないマシンが検出されます。
D. クラウドベースのトラフィックは会社のネットワーク外に流れます。
正解**: (**正解を表示します**)**
A split-tunnel VPN allows certain traffic (e.g., cloud-based services) to bypass the VPN and go directly to the Internet. This reduces the amount of traffic that needs to traverse the company ' s VPN and Internet connection, conserving bandwidth and reducing costs. It also means that not all traffic is subject to the same level of inspection or filtering, which can improve performance for cloud-based services.References:
CompTIA Network+ study materials.

質問**: 174**
ユーザーは、IP アドレス 10.249.3.76 の内部 Web サイトに接続できません。ネットワーク管理者がコマンドを実行すると、次の出力が表示されます。
1 3ミリ秒 2ミリ秒 3ミリ秒 192.168.25.234
2 2ミリ秒 3ミリ秒 1ミリ秒 192.168.3.100
3 4ミリ秒 5ミリ秒 2ミリ秒 10.249.3.1
4 *
5'
6 *
7 ?
ネットワーク管理者は、次のコマンドライン ツールのどれを使用していますか?

A. トレース
B. ネットスタット
C. tcpdump
D. nmap
正解**: A (**コメントを発表する**)**
* Understanding Tracert:
* tracert (Traceroute in Windows) is a command-line tool used to trace the path that packets take from the source to the destination. It records the route (the specific gateways at each hop) and measures transit delays of packets across an IP network.
* Output Analysis:
* The output shows a series of IP addresses with corresponding round-trip times (RTTs) in milliseconds.
* The asterisks (*) indicate that no response was received from those hops, which is typical for routers or firewalls that block ICMP packets used by tracert.
* Comparison with Other Tools:
* netstat: Displays network connections, routing tables, interface statistics, and more, but does not trace packet routes.
* tcpdump: Captures network packets for analysis, used for detailed network traffic inspection.
* nmap: A network scanning tool used to discover hosts and services on a network, not for tracing packet routes.
* Usage:
* tracert helps identify the path to a destination and locate points of failure or congestion in the network.
References:
* CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

質問**: 175**
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**: 176**
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: **177**
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: **178**
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: **179**
トラブルシューティング方法の最初のステップとして実行する必要があるアクションは次のどれですか。
A. アイデアを検証するためのテストを実施する
B. トップダウンアプローチを使用する
C. 複数の問題を個別に処理する
D. 考えられる根本原因についての理論を作成する
正解: **(**正解を表示します**)**

質問: **180**
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: **A (**コメントを発表する**)**
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: **181**
次のどれが PaaS 環境のユースケースですか?
A. モバイルアクセス
B. 電子商取引サイト
C. アプリケーション開発
D. クラウドネイティブソフトウェア
正解: **(**正解を表示します**)**
PaaS (Platform as a Service) is best suited for application development because it provides a managed platform that includes the runtime environment, development frameworks, middleware, databases (often), and build/deployment tooling. In a PaaS model, the cloud provider manages the underlying infrastructure (servers, storage, networking, OS patching, and often the application runtime), allowing developers to focus on writing code, testing, and releasing applications quickly. This aligns with Network+ cloud concepts where service models are compared by responsibility: PaaS reduces operational overhead for the customer and accelerates development through standardized environments and automation.
Mobile access is a use case for remote access solutions (VPN, zero trust access, MDM), not specifically PaaS. An e-commerce site could be hosted using many models (IaaS, PaaS, SaaS), so it's not the most specific match. Cloud-native software describes an architectural style (microservices, containers, managed services) and can be built using PaaS components, but it is broader than a single "use case" and is not as directly tied to the PaaS definition as application development is. Therefore, application development is the clearest and most accurate PaaS use case.

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　**608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **182**
保険仲介業者が VPN の使用を強制する理由として最も可能性が高いのは次のどれですか?

A. 転送中の機密データを暗号化する
B. エンドポイントを保護する
C. 契約上の合意を維持するため
D. データ保持要件に準拠するため
正解: **(**正解を表示します**)**
The most likely reason an insurance brokerage would enforce VPN usage is to encrypt sensitive data in transit. VPNs (Virtual Private Networks) create a secure tunnel between the user's device and the corporate network, ensuring that data is encrypted and protected from interception.
* Encryption: VPNs encrypt data, preventing unauthorized access and ensuring data privacy during transmission over public or unsecured networks.
* Data Protection: Essential for industries handling sensitive information, such as insurance brokerages, to protect customer data and comply with regulatory requirements.
* Security: Enhances overall network security by providing secure remote access for employees.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses the role of VPNs in securing data in transit.
* Cisco Networking Academy: Provides training on VPN technologies and their importance in data security.
* Network+ Certification All-in-One Exam Guide: Explains VPN usage and its benefits in protecting sensitive information.
質問**: 183**
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**: B (**コメントを発表する**)**
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**: 184**
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**: C (**コメントを発表する**)**
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: **185**
ネットワーク管理者が 2 つの施設間で永続的で安全な接続を確立するための最も費用対効果の高い方法はどれですか?
A. サイト間VPN
B. GREトンネル
C. VXLAN
D. 専用回線
正解: **(**正解を表示します**)**
A Site-to-site VPN (Virtual Private Network) is the most cost-effective solution for establishing a persistent, secure connection between two facilities. It uses the public internet to create an encrypted tunnel, leveraging existing internet connections without requiring expensive dedicated infrastructure. This makes it ideal for organizations looking to securely connect remote sites while minimizing costs.
Why not GRE tunnel? Generic Routing Encapsulation (GRE) tunnels encapsulate traffic but do not provide encryption natively, requiring additional protocols (e.g., IPsec) for security. This adds complexity and is less cost-effective than a site-to-site VPN, which integrates encryption.
Why not VXLAN? Virtual Extensible LAN (VXLAN) is used for overlay networks in data centers to extend Layer 2 networks, not for secure site-to-site connectivity.
Why not Dedicated line? A dedicated line (e.g., leased line or MPLS) provides high reliability but is significantly more expensive due to the need for dedicated infrastructure.
Reference:CompTIA Network+ N10-009 Objective 1.7: Explain the use cases for virtual private networks (VPNs) and tunneling protocols. The CompTIA Network+ Study Guide (e.g., Chapter 12: Network Security) explains that site-to-site VPNs are a cost-effective, secure method for connecting geographically separate networks over the internet.

質問: **186**
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: **(**正解を表示します**)**
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: **187**
組織内の複数のユーザーから、ビデオ会議中に接続の問題や遅延が発生したという報告がありました。ネットワーク管理者が tcpdump を実行すると、ネットワーク上の他の非ビデオ アプリケーションの再送信が増加していることが確認されました。次の症状のうち、ユーザーから報告された問題に当てはまるものはどれですか。
A. レイテンシー
B. パケット損失
C. ボトルネック
D. ジッター
正解: **(**正解を表示します**)**
Packet loss occurs when network packets fail to reach their destination, leading to disruptions in connectivity and performance issues. In this scenario:
Users report connectivity issues and lag during video meetings.
The administrator detects increased retransmissions in tcpdump, which is a strong indicator of lost packets that must be resent.
Video meetings are particularly sensitive to packet loss, leading to buffering, frozen screens, and dropped calls.
Latency (Option A) refers to delayed data transmission but does not necessarily cause retransmissions.
Bottlenecking (Option C) happens when a network component (e.g., router, switch) cannot handle the traffic load, but packet retransmissions are more directly related to packet loss.
Jitter (Option D) affects the consistency of packet arrival times, but the symptoms described here are more aligned with packet loss rather than timing variations.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Troubleshooting Connectivity Issues

質問: **188**
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: **189**
異なるネットワーク セグメントを接続し、許可されたトラフィックを特定のセグメント間で誘導するネットワーク アプライアンスの最適な例は次のうちどれですか。
A. ファイアウォール
B. IDS
C. 管理されていないスイッチ
D. (提供されていません)
正解: **(**正解を表示します**)**
A firewall is the best example of an appliance that can sit between network segments and permit or deny traffic flows based on security policy. In Network+ terms, firewalls enforce segmentation controls by applying rules that match on items such as source/destination IP, ports, protocols, and (with next-generation firewalls) even applications. This makes a firewall a common choice for directing allowed traffic between specific segments (for example, allowing users in a workstation VLAN to reach only certain ports on a server VLAN, while blocking everything else). This function is core to network security architecture and is frequently paired with concepts like network segmentation, ACL-style rule sets, and creating security zones.
An IDS (intrusion detection system) primarily monitors traffic and generates alerts on suspicious activity; it does not typically control or "direct allowed traffic" unless it is specifically an IPS (prevention)

with inline blocking. An unmanaged switch operates at Layer 2 and forwards frames within a broadcast domain; it does not provide policy-based filtering between security segments. Therefore, the correct answer is Firewall.

質問: **190**
126人のユーザーをサポートするために新しいネットワークを構築しています。次のCIDR範囲のうち、最も効率的にスペースを活用できるのはどれですか？
A. 10.2.2.0/23
B. 10.2.2.0/24
C. 10.2.2.0/25
D. 10.2.2.0/26
正解: **(**正解を表示します**)**
To support 126 users, the subnet must provide at least 126 usable host addresses. In IPv4 subnetting, usable hosts are calculated as: (2^(host bits)) # 2, subtracting the network and broadcast addresses.
A /25 leaves 7 host bits (because 32 # 25 = 7). That yields 2^7 = 128 total addresses, and 128 # 2 = 126 usable-an exact fit and therefore the most efficient option listed.
A /24 provides 256 total addresses and 254 usable, which would waste more addresses than necessary. A /23 provides 512 total addresses and 510 usable-far more waste. A /26 leaves 6 host bits, giving 64 total addresses and 62 usable, which is not enough for 126 users.
The 10.2.2.0 address is within the private 10.0.0.0/8 range, so it's appropriate for internal addressing.
Therefore, 10.2.2.0/25 is the correct CIDR range for efficiently supporting 126 hosts.

質問: **191**
ある大学が新しいキャンパス無線ネットワークを導入しています。ネットワーク管理者は、多数のデバイスと学生からの高帯域幅の要求に対応できるようにネットワークを構成する必要があります。このシナリオでは、管理者は次のワイヤレス テクノロジのどれを考慮する必要がありますか?
A. ブルートゥース
B. Wi-Fi 6E
C. 5G
D. LTE
正解: **(**正解を表示します**)**
Wi-Fi 6E is the best choice for high-density environments, such as a university campus. It:
Supports more devices with OFDMA (Orthogonal Frequency-Division Multiple Access) Uses the 6GHz band, reducing congestion Provides faster speeds and lower latency This makes Wi-Fi 6E ideal for large networks with high-bandwidth demands, like those in a university setting.
Breakdown of Options:
A). Bluetooth - Used for short-range, low-power connections, not large-scale wireless networks.
B). Wi-Fi 6E - # Correct answer. Designed for high-density environments, improving speed and efficiency.
C). 5G - Used for mobile networks, but not ideal for campus-wide local wireless infrastructure.
D). LTE - Used for cellular data, not for campus-wide Wi-Fi.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.6: Compare and contrast wireless networking technologies.
IEEE 802.11ax (Wi-Fi 6E): Enhancements for high-efficiency wireless networking

質問: **192**
ネットワーク管理者は最近、新しい AP でワイヤレス インフラストラクチャをアップグレードしました。ユーザーから、静止状態のときにワイヤレス接続が切断され、20 ～ 30 秒ごとに再接続されるとの報告がありました。ログを確認しているときに、管理者は AP がチャネルを変更していることに気付きました。

サービス中断の理由として最も可能性が高いのは次のどれですか?
A. チャネル干渉
B. ローミングの設定ミス
C. ネットワーク輻輳
D. 無線範囲が不十分です
正解: (正解を表示します)
If APs are changing channels frequently, it indicates automatic channel selection due to interference. This can cause temporary disconnections as the APs switch frequencies.
Breakdown of Options:
A: Channel interference - # Correct answer. APs change channels automatically to avoid interference, causing disconnections.
B: Roaming misconfiguration - Roaming only affects moving users, but users report issues while stationary.
C: Network congestion - Causes slow speeds, not frequent disconnects.
D: Insufficient wireless coverage - Would cause weak signals, but not channel switching issues.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.6: Explain wireless troubleshooting techniques.

質問: **193**
パブリック インターネット上のトラフィックをルーティングするために使用されるプロトコルは次のどれですか?
A. BGP
B. OSPF
C. EIGRP
D. RIP
正解: (正解を表示します)
Border Gateway Protocol (BGP) is the primary protocol used to route traffic on the public internet. It allows ISPs and large networks to exchange routing information, making it an Exterior Gateway Protocol (EGP).
Breakdown of Options:
A: BGP - Correct answer. Used for internet routing and exchanges routing information between ISPs.
B: OSPF - An Interior Gateway Protocol (IGP) used for routing within an autonomous system (not the public internet).
C: EIGRP - Cisco's proprietary IGP, used within private networks, not the public internet.
D: RIP - An older distance-vector protocol, not scalable for the internet.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.4: Explain routing technologies.
RFC 4271: Border Gateway Protocol 4 (BGP-4)

質問: **194**
ネットワーク管理者は、工業用倉庫内に無線アクセスポイント(AP)を設置しています。無線調査の結果、大量の電磁干渉が発生していることが判明しました。APをスイッチに接続する際に、管理者はどの種類のケーブルを使用すべきでしょうか?
A. UTP
B. STP
C. マルチモード
D. シングルモード
正解: (正解を表示します)

The correct answer is STP (Shielded Twisted Pair). According to the CompTIA Network+ N10-009 objectives, environments with high levels of electromagnetic interference (EMI)-such as industrial warehouses with heavy machinery, motors, and electrical equipment-require additional protection at the physical layer to maintain signal integrity.
STP cabling includes shielding around the twisted copper pairs that helps block external electromagnetic signals from interfering with data transmission. This shielding significantly reduces crosstalk and EMI, making STP far more suitable than UTP (Unshielded Twisted Pair) in electrically noisy environments. UTP lacks this shielding and is more prone to signal degradation under such conditions.
While fiber-optic cabling (multimode or single-mode) is completely immune to EMI, it is typically not used to directly connect wireless APs in most enterprise deployments. Wireless access points commonly rely on copper Ethernet connections to support Power over Ethernet (PoE), which supplies both data and electrical power over the same cable. Fiber does not natively support PoE, making it impractical for directly powering APs without additional equipment.
The Network+ objectives emphasize selecting appropriate cabling based on environmental factors and operational requirements. In this scenario, STP provides the optimal balance of EMI resistance, Ethernet compatibility, and PoE support, making it the best choice for connecting APs in an industrial warehouse.

質問: **195**
ネットワーク インストールにおける UPS と PDU の目的を最もよく表しているのは次のうちどれですか。
A. IDF内のデバイスの電圧要件をサポートするため
B. MDFの電力消費を管理する
C. 複数のデバイスを単一のネットワーク接続に接続する
D. MDFとIDFの温度を調節する
正解: **A (**コメントを発表する**)**
A UPS (Uninterruptible Power Supply) and PDU (Power Distribution Unit) are installed to provide reliable, properly distributed electrical power to network equipment-especially in wiring closets such as an IDF and in main equipment rooms. In Network+ (N10-009) infrastructure objectives, a UPS protects against power loss and instability by supplying battery-backed power during outages and often providing conditioning to reduce the impact of sags, spikes, and brief interruptions. A PDU then distributes that power to multiple devices in a rack (switches, routers, firewalls, AP controllers), often offering organized outlets and, in managed models, monitoring/control features.
Option A is the best match because it reflects the practical purpose: ensuring network devices receive appropriate and continuous power in distribution frames/closets. Option B is partially related, but "managing power consumption in the MDF" is too narrow and not as accurate as the broader function of providing backup and distribution power. Option C describes a network switch, not power equipment. Option D refers to HVAC/environmental controls, not UPS/PDU functionality. Hence, A is correct.

質問: **196**
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."

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 **608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **197**
ネットワーク スイッチを密閉されたエンクロージャ内に設置する場合、次の物理的な設置要因のうちどれが最も重要ですか。
A. 消火
B. 電力予算
C. 温度
D. 湿度
正解: **(**正解を表示します**)**
The correct answer is Temperature because a sealed enclosure restricts airflow, which can cause heat to accumulate rapidly. According to CompTIA Network+ (N10-009) objectives under physical installations and environmental factors, maintaining proper temperature control is critical for network equipment reliability and longevity.
Network switches generate heat during operation, particularly models with high port density or Power over Ethernet (PoE) capabilities. In a sealed enclosure without proper ventilation or cooling mechanisms, excessive heat buildup can lead to thermal throttling, unexpected shutdowns, hardware degradation, or permanent equipment failure. Manufacturers specify operating temperature ranges, and exceeding these limits significantly reduces device lifespan and performance.
While humidity (Option D) is important to prevent condensation and corrosion, temperature fluctuations pose a more immediate risk in a sealed environment. Power budget (Option B) is relevant when calculating PoE load capacity but does not directly address environmental installation conditions. Fire suppression (Option A) is important in data centers but is not the primary concern specific to a sealed enclosure scenario.
Therefore, ensuring proper temperature management is the most critical installation factor.

質問: **198**
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利用される可能性が高いのは次のどれですか?
A. SSH
B. TLS
C. SCADA
D. RADIUS
正解: **(**正解を表示します**)**
TLS (Transport Layer Security)is the protocol that providesencryption in transit for HTTPS. It ensures data is encrypted between the client (browser) and the web server, protecting it from interception or tampering.
* A. SSHis used for secure terminal access, not HTTPS.
* C. SCADArefers to control systems, not encryption protocols.
* D. RADIUSis an authentication protocol, not for encrypting HTTPS traffic.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 4.2 - Identify common security threats and vulnerabilities.
CompTIA Network+ N10-009 Official Objectives: 4.6 - Explain authentication and access controls.

質問: **199**
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: **B (**コメントを発表する**)**
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: **200**
次のネットワーク ケーブルのうち、保護被覆から光を反射するものはどれですか。
A. ツインアキシャル
B. 同軸
C. シングルモード
D. マルチモード
正解: **(**正解を表示します**)**
Multimode fiber optic cables involve the transmission of light signals that bounce off the core's cladding as they travel down the fiber. This characteristic differentiates it from single-mode fiber, where the light travels directly down the fiber without reflecting off the cladding.
Here are some detailed points about multimode fiber cables:
Construction: Multimode fibers have a larger core diameter, typically 50 or 62.5 microns, compared to single- mode fibers, which have a core diameter of about 9 microns.
Light Propagation: The larger core of multimode fiber allows multiple light modes to propagate. These modes travel at different angles, leading to reflections off the core-cladding boundary.
Distance and Bandwidth: Due to modal dispersion, where different light modes arrive at the receiver at different times, multimode fibers are suited for shorter distance applications compared to single-mode fibers.
Typical distances are up to 550 meters for 10 Gbps Ethernet using OM4 multimode fiber.
Applications: Multimode fibers are commonly used in LANs (Local Area Networks), data centers, and for shorter distance data transmission due to their cost-effectiveness and ease of installation.
Network References:
CompTIA Network+ N10-007 Official Certification Guide, which covers fiber optic technologies, including the differences between multimode and single-mode fibers.
Cisco Networking Academy: Provides training materials and reference guides on the properties of different fiber optic cables.
Fiber Optic Association (FOA): A professional society dedicated to fiber optics, offering extensive information and certification on fiber optic technologies.
Multimode fibers are specifically designed for short-range communication with higher data rates and are typically used in environments like data centers, where high bandwidth over shorter distances is crucial. The reflections off the cladding, inherent to multimode fiber, facilitate this high-capacity communication.

質問: **201**
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**: 202**
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**: (**正解を表示します**)**
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**: 203**
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**: (**正解を表示します**)**
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: **204**
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: **205**
ネットワーク エンジニアは、2 つのサイト間の安全な通信リンクを設計しています。データ ストリーム全体を機密に保つ必要があります。この目標を達成するには、次のどれが適していますか。
A. GRE
B. IKE
C. 超能力
D. ああ
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 designed to provide confidentiality, integrity, and authenticity of data by encrypting the payload and optional ESP trailer.
* Ensuring Confidentiality:
* Encryption: ESP encrypts the payload, ensuring that the data remains confidential during transmission. Only authorized parties with the correct decryption keys can access the data.
* Modes of Operation: ESP can operate in transport mode (encrypts only the payload) or tunnel mode (encrypts the entire IP packet), both providing strong encryption to secure data between sites.
* Comparison with Other Protocols:
* GRE (Generic Routing Encapsulation): A tunneling protocol that does not provide encryption or security features.
* IKE (Internet Key Exchange): A protocol used to set up a secure, authenticated communications channel, but it does not encrypt the data itself.
* AH (Authentication Header): Provides integrity and authentication for IP packets but does not encrypt the payload.
* Implementation:
* Use ESP as part of an IPsec VPN configuration to encrypt and secure communication between two sites. This involves setting up IPsec policies and ensuring both endpoints are configured to use ESP for data encryption.
References:

* CompTIA Network+ study materials on IPsec and secure communication protocols.

質問: **206**
ネットワーク管理者は、新しいIP電話の設定依頼に応答しています。データ トラフィックと音声トラフィックの優先順位を適切に設定するために、ネットワーク管理者は次のうちどれを行う必要がありますか？
A. 全二重を設定します。
B. QoS を変更します。
C. 802.1Q タグ付けを有効にします。
D. ネイティブVLANを変更します。
正解: **(**正解を表示します**)**
To ensure voice and data traffic are properly prioritized for an IP phone, the administrator should modify (configure) QoS. In Network+ (N10-009), QoS is the primary mechanism used to prioritize latency-sensitive traffic such as VoIP. By classifying and marking voice frames/packets (often using DSCP/CoS values) and applying priority queuing, the network ensures voice traffic experiences minimal delay and jitter even when links are congested. This is essential for call quality because voice is highly sensitive to variation in delivery time and packet loss.
802.1Q tagging is important for VLAN separation (and many IP phone deployments use a voice VLAN), but VLAN tagging alone does not guarantee prioritization; it separates traffic, while QoS provides preferential treatment. Full duplex can reduce collisions on Ethernet links, but it does not implement traffic prioritization policies. Changing the native VLAN is a trunking/security configuration detail and not the correct action to prioritize voice versus data. In practice, networks often use both a voice VLAN (802.1Q) and QoS, but for the explicit requirement of prioritization, QoS is the correct answer.

質問: **207**
最近、VXLAN を使用したデータ センター相互接続が実装されました。ネットワーク エンジニアは、相互接続のパフォーマンスの低下と断片化を観察しています。次のテクノロジのどれがこの問題を解決しますか。
A. 802.1Q タグ付け
B. スパニングツリー
C. リンクアグリゲーション
D. ジャンボフレーム
正解: **(**正解を表示します**)**
VXLAN (Virtual Extensible LAN) encapsulates Ethernet frames inside UDP packets, increasing packet size.
This can lead to fragmentation and performance degradation unless Jumbo Frames are enabled.
Breakdown of Options:
A: 802.1Q tagging - VLAN tagging enables segmentation but does not address fragmentation issues.
B: Spanning tree - STP prevents loops but does not improve performance for VXLAN traffic.
C: Link aggregation - LACP combines links for higher bandwidth but does not prevent fragmentation.
D: Jumbo frames - Correct answer. Enabling Jumbo Frames allows larger packet sizes, reducing fragmentation and improving VXLAN performance.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.3: Explain network performance concepts.
RFC 7348: VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks

質問: **208**
ネットワーク エンジニアが新しい VoIP のインストールを完了しようとしていますが、電話機が設定ファイルをダウンロードするための TFTP サーバーを見つけることができません。次の DHCP 機能のうち、電話機が TFTP サーバーに到達するのに役立つものはどれですか。
A. 除外
B. リース期間

C. オプション
D. スコープ
正解: **C (**コメントを発表する**)**
DHCP Options: DHCP options allow additional configuration parameters, such as the address of a TFTP server, to be provided to clients during the DHCP lease process. This is essential for VoIP phones to locate the server for configuration files.
Exclusions (A): Prevents certain IP addresses from being assigned by DHCP but does not direct devices to servers.
Lease time (B): Determines how long an IP address is assigned but does not impact TFTP settings.
Scope (D): Defines a range of IP addresses but does not include additional server information.
Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (DHCP Configuration).

質問: **209**
次のどれを使用すると、ユーザーはスタンドアロン ネットワーク上の分離されたデバイスに接続できますか?
A. ジャンプボックス
B. APIゲートウェイ
C. セキュア シェル (SSH)
D. クライアントレスVPN
正解: **(**正解を表示します**)**
A jump box is a hardened system that provides secure access to isolated or sensitive devices on a separate network.
Breakdown of Options:
A: Jump box - # Correct answer. Acts as a middle point for secure remote access.
B: API gateway - Used for managing API calls, not remote access to isolated devices.
C: Secure Shell (SSH) - Requires direct connectivity, which may not be available for an isolated device.
D: Clientless VPN - Allows web-based VPN access, but does not guarantee access to isolated devices.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.4: Implement secure remote access methods.

質問: **210**
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: **A (**コメントを発表する**)**
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: **211**
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.

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 **608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **212**
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."

質問: **213**
単一障害点に関する懸念から、ある企業はネットワークに WAN を追加することを決定しました。この企業は、現在の MPLS WAN に 2 番目の MPLS ベンダーを追加し、各サイトに WAN ルーターを追加で導入しました。両方の MPLS プロバイダーは WAN ネットワークで OSPF を使用し、EIGRP は内部で実行されています。新しい WAN が稼働する最初のサイトは成功しましたが、2 番目のサイトがアクティブになると、重大なネットワーク問題が発生します。WAN が不安定になる原因として最も可能性が高いのは次のどれですか。
A. 変更された CDP ネイバー
B. 非対称ルーティング
C. スイッチングループ
D. IP アドレスが正しくありません
正解: (正解を表示します)
Asymmetrical routing occurs when packets take different paths to and from the destination, leading to instability in network communication. The use of two different MPLS providers with OSPF can lead to this type of routing issue, especially if the paths aren't carefully configured and managed. This can cause unexpected routing behaviors and instability in a dual-WAN setup. (Reference: CompTIA Network+ Study Guide, Chapter on Network Routing)

質問: **214**
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: **215**
ユーザーがwww.abc.comにアクセスしようとしましたが、表示されるウェブサイトはwww.cba.comです。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 レコードを変更します。
B. PTRレコードを更新します。
C. NTP 設定を変更します。
D. TXTレコードを削除します。
正解: **(**正解を表示します**)**
The correct answer is Modify the CNAME record because a CNAME (Canonical Name) record maps one domain name (alias) to another domain name. If a user enters www.abc.com but is redirected to www.cba.
com, it is likely that the DNS configuration includes an incorrect CNAME entry pointing abc.com to cba.com.
Updating or correcting the CNAME record ensures the alias resolves to the intended host.
According to CompTIA Network+ (N10-009) objectives covering DNS record types, a CNAME record is used to alias one domain name to another, commonly for load balancing, CDN services, or website redirection.
A PTR record (Option B) is used for reverse DNS lookups (IP address to hostname) and does not control forward name resolution for websites. NTP settings (Option C) are used for time synchronization and have no impact on DNS resolution. A TXT record (Option D) stores descriptive text information (such as SPF, DKIM, or domain verification data) and does not affect website redirection.
Therefore, correcting the CNAME record resolves the issue and ensures users reach the correct website.

質問: **216**
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: **217**
ある企業は、ワークステーション上のソーシャル メディア プラットフォームと個人用クラウド ストレージへのユーザー アクセスを制限することで、データ損失防止を実装したいと考えています。これらの目標を達成するには、次のどのタイプのフィルタリングを導入する必要がありますか。
A. ポート
B. DNS
C. MAC
D. コンテンツ
正解: **(**正解を表示します**)**
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

質問: **218**
技術者は、会社の現在の規模、コンピューティング能力、およびストレージ能力に対応するクラウド サービス ソリューションを設計しています。次のクラウド展開モデルのどれがこれらの要件を満たしますか?
A. SaaS
B. PaaS
C. IaaS
D. IaC
正解: **(**正解を表示します**)**
Infrastructure as a Service (IaaS) provides scalable compute power, storage, and networking resources on demand. It is the best choice for a company that needs to customize its cloud solution based on size, compute capacity, and storage needs.
IaaS Benefits:
Provides virtual machines, storage, and networking resources.
Scalable based on company needs.

Reduces the need for physical infrastructure.
Incorrect Options:
A). SaaS (Software as a Service): Delivers software applications (e.g., Google Docs, Microsoft 365) but does not provide compute/storage infrastructure.
B). PaaS (Platform as a Service): Provides a development environment for application deployment but not full infrastructure control.
D). IaC (Infrastructure as Code): A methodology for automating infrastructure, not a cloud deployment model.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Cloud Computing Models

質問: **219**
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: **220**
次の動的ルーティング プロトコルのうち、インターネットで使用されているものはどれですか?
A. EIGRP
B. BGP
C. RIP
D. OSPF
正解: **(**正解を表示します**)**
BGP (Border Gateway Protocol) is the only dynamic routing protocol used across the internet. It's classified as an Exterior Gateway Protocol (EGP), responsible for routing between different autonomous systems (ASes).
A: EIGRP and D. OSPF are Interior Gateway Protocols (IGPs), used within organizations.
C: RIP is an outdated IGP with limited use, unsuitable for internet-scale routing.
Reference:

CompTIA Network+ N10-009 Official Objectives: 3.1 - Compare and contrast various routing technologies.

質問: **221**
ユーザーの自宅のメッシュワイヤレスネットワークで遅延の問題が発生しています。技術者は以下のことを行っています。
*速度テストを実行しました。
*デバイスを再起動しました。
*現場調査を実施しました。
*ワイヤレスパケットキャプチャを実行しました。
技術者は次の情報を確認します。

SSID	MAC	RSSI	Channel
Home	AAAAAA111112	-83dBm	11
Home	AAAAAA111113	-91dBm	11
Home	AAAAAA111114	-70dBm	11

技術者はパケットキャプチャでフレームが再送信されていることに気づきました。ユーザーのネットワーク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. SSIDは同じであってはなりません。
B. ネットワークの重複が多すぎます。
C. デバイスはメッシュ ネットワークと互換性がありません。
D. ノードの電力が不足しています。
正解: **B** (コメントを発表する)
*Too much overlap on the same channel (all devices on channel 11) causes interference, leading to retransmissions and high latency.
*Same SSIDs (A) are expected in mesh networks.
*Device compatibility (C) would show different symptoms.
*Node power (D) affects coverage, not congestion.
Reference: CompTIA Network+ N10-009 Official Documentation - Wireless Troubleshooting & Signal Interference.

質問: **222**
パブリック IP アドレス空間で 1 つの IP アドレスを共有する多くのシステムに最もよく関連するのは次のどれですか。
A. パット
B. NAT
C. VIP
D. NAT64
正解: **(**正解を表示します**)**
Port Address Translation (PAT) allows multiple internal devices to share a single public IP address by assigning each device a unique port number. This is the most common method used in environments where many systems need internet access but there are limited public IP addresses.

質問: **223**
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: **224**
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: **(**正解を表示します**)**
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: **225**
次のどれがオンパス攻撃の機会を提供しますか?
A. フィッシング
B. ゴミ漁り
C. 邪悪な双子
D. テールゲーティング

正解: (正解を表示します)
An evil twin is a rogue Wi-Fi access point that mimics a legitimate network. Attackers use it to intercept and manipulate traffic, making it an on-path (formerly MITM) attack opportunity.
Breakdown of Options:
A: Phishing - Tries to steal credentials through fake emails/websites but does not intercept network traffic.
B: Dumpster diving - Involves physical security breaches, not network interception.
C: Evil twin - # Correct answer. A rogue Wi-Fi AP impersonates a real network, allowing traffic interception.
D: Tailgating - Involves physical access security, not network interception.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.3: Explain common network security threats.

質問: **226**
ネットワーク管理者は、ルーターのインターフェイスを 10.0.0.95 255.255.255.240 として設定しました。管理者は、ルーターが IP 10.0.0.81/28 の Web サーバーにパケットをルーティングしていないことを発見しました。
次のどれが最も適切な説明でしょうか?
A. Web サーバーは別のサブネットにあります。
B. ルータ インターフェイスはブロードキャスト アドレスです。
C. IP アドレス空間はクラス A ネットワークです。
D. サブネットはプライベート アドレス空間内にあります。
正解: **B** (コメントを発表する)
Understanding Subnetting:
The subnet mask 255.255.255.240 (or /28) indicates that each subnet has 16 IP addresses (14 usable addresses, 1 network address, and 1 broadcast address).
Calculating the Subnet Range:
Subnet Calculation: For the IP address 10.0.0.95 with a /28 subnet mask:
Network address: 10.0.0.80
Usable IP range: 10.0.0.81 to 10.0.0.94
Broadcast address: 10.0.0.95
Router Interface Configuration:
Broadcast Address Issue: The IP address 10.0.0.95 is the broadcast address for the subnet 10.0.0.80/28.
Configuring a router interface with the broadcast address will cause routing issues as it is not a valid host address.
Comparison with Other Options:
The web server is in a different subnet: The web server (10.0.0.81) is within the same subnet range (10.0.0.80
/28).
The IP address space is a class A network: While 10.0.0.0 is a Class A network, this does not explain the routing issue caused by the broadcast address.
The subnet is in a private address space: The private address space designation (RFC 1918) does not impact the routing issue related to the broadcast address configuration.
Resolution:
Reconfigure the router interface with a valid host IP address within the usable range, such as 10.0.0.94.
References:
CompTIA Network+ study materials on subnetting and IP address configuration.

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　**608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

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　**608**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」