

CompTIA.N10-009J.v2026-09-01.q248

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：	248
バージョン：	v2026-09-01
ページの閲覧量：	106
問題集の閲覧量：	3220
https://www.jpnsiken.com/shiken/CompTIA.N10-009J.v2026-09-01.q248.html	

質問: 1

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: [\(正解を表示します\)](#)

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.

質問: 2

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** ([コメントを发表する](#))

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: 3

ルータが 1 台しかない環境で、ネットワーク エンジニアが追加のハードウェアを購入せずに VLAN 間で通信できるようにするには、次のどれを使用しますか。

- A. サブインターフェース
- B. VXLAN
- C. レイヤー3スイッチ
- D. 仮想

正解: [A \(コメントを發表する\)](#)

A subinterface is a logical interface created on a single physical router interface that allows routing between VLANs (known as Router-on-a-Stick (ROAS)). This method is commonly used when only one physical router is available, allowing inter-VLAN communication without additional hardware.

*Why not the other options?

*VXLAN (B) - This is used for extending Layer 2 networks over a Layer 3 infrastructure, primarily in data centers. It does not directly enable inter-VLAN communication.

*Layer 3 switch (C) - A Layer 3 switch can route between VLANs, but the scenario states that purchasing additional hardware is not an option.

*VIR (D) - This is not a standard networking term in the context of VLAN communication.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 8: VLANs and Inter-VLAN Routing

質問: 4

ベンダーが提供する品質、可用性、責任などの要件を文書化したセットは次のどれですか。

- A. 覚書
- B. 終了
- C. EOS
- D. SLA

正解: [\(正解を表示します\)](#)

The correct answer is SLA (Service Level Agreement) because it is a formal, documented contract between a service provider and a customer that defines expected service standards.

According to CompTIA Network+ (N10-009) objectives under network operations and service management concepts, an SLA outlines measurable performance metrics such as uptime percentage, response time, throughput, support availability, escalation procedures, and responsibilities of both parties.

An SLA ensures accountability and establishes clear expectations for service delivery. For example, a vendor may guarantee 99.99% uptime, define maximum resolution times for incidents, and specify penalties or credits if performance targets are not met. SLAs are critical in cloud services, ISP agreements, managed services, and enterprise vendor contracts.

An MOU (Memorandum of Understanding) is a non-binding agreement outlining general terms between parties but does not define enforceable service metrics. EOL (End of Life) refers to when a product is no longer sold or supported. EOS (End of Support) indicates when a vendor stops providing updates or assistance for a product.

Therefore, an SLA is the correct document that defines vendor-delivered service requirements.

Top of Form

質問: 5

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ーを実装したいと考えています。技術者は次のテクノロジー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: **A** ([コメントを发表する](#))

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: **6**

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: **7**

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:
$$\text{MTBF} = \frac{\text{Total Operational Time}}{\text{Number of Failures}}$$
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:

$$\text{MTBF} = \frac{1000 \text{ hours}}{2} = 500 \text{ hours}$$
MTBF=1000 hours2=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: 8

ある企業は、短期間のダウンタイムを許容できる災害復旧サイトまたは重要でないアプリケーションを実装したいと考えています。この目標を達成するには、次のどのタイプのサイトを実装する必要がありますか？

A. ホット

B. 寒い

C. 暖かい

D. パッシブ

正解: ([正解を表示します](#))

A warm site is a compromise between a hot site and a cold site, providing a balance between cost and recovery time. It is partially equipped with the necessary hardware, software, and infrastructure, allowing for a quicker recovery compared to a cold site but at a lower cost than a hot site.

* Recovery Time: Warm sites can be operational within hours to a day, making them suitable for non- critical applications that can tolerate short downtimes.

* Cost-Effectiveness: Warm sites are more economical than hot sites as they do not require all systems to be fully operational at all times.

Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Discusses disaster recovery strategies and the different types of recovery sites.

* Cisco Networking Academy: Provides training on disaster recovery planning and site selection.

* Network+ Certification All-in-One Exam Guide: Explains the characteristics of hot, warm, and cold sites and their use cases in disaster recovery planning.

Warm sites offer a practical solution for maintaining business continuity for non-critical applications, balancing the need for availability with cost considerations.

質問: 9

ネットワーク技術者は、ネットワークのアクセス層で STP をサポートしていない新しいスイッチをインストールしています。

技術者は配電スイッチへの冗長接続を希望しています。技術者は次のうちどれを使用すべきでしょうか？

A. リンクアグリゲーション

B. サブインターフェース

C. スイッチ仮想インターフェース

D. 半二重接続

正解: ([正解を表示します](#))

Link aggregation(also known as port channeling or EtherChannel) allows multiple physical connections to act as one logical connection. This avoids loops that would typically be prevented by STP and provides redundancy and increased bandwidth. It's ideal when STP is not available or desirable.

Reference:Section 2.2 - Switching Technologies and Features - "Link Aggregation"

質問: 10

企業ネットワークのデータ帯域幅要件を削減するために使用するのに最適な VPN は次のどれですか？

- A. スプリットトンネル
- B. サイト間
- C. フルトンネルクライアント
- D. GREトンネル

正解: ([正解を表示します](#))

A split-tunnel VPN allows a device to route some traffic through the VPN (typically corporate traffic) while sending other traffic (like general internet browsing) directly over the local internet connection. This reduces the load on the corporate network because not all traffic is routed through the VPN tunnel.

Site-to-site VPNs are for permanent links between locations.

Full-tunnel VPNs route all traffic through the VPN, increasing the bandwidth usage on the corporate network.

GRE (Generic Routing Encapsulation) is a tunneling protocol that doesn't encrypt and doesn't reduce bandwidth usage by itself.

Reference:

CompTIA Network+ N10-009 Official Objectives: 3.3 - Given a scenario, configure and deploy common VPN technologies.

質問: 11

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: 12

ネットワークセキュリティ管理者は、安全なネットワークと社内ネットワーク間で送信されるデータの内容を監視する必要があります。このタスクを達成できる監視方法は、次のうちどれですか？

- A. ポートミラーリング
- B. フローデータ
- C. Syslogエントリ
- D. SNMPトラップ

正解: ([正解を表示します](#))

To monitor the contents of data (i.e., inspect the actual packets/frames and their payloads) moving between networks, the administrator should use port mirroring (also called SPAN on some platforms). Port mirroring copies traffic from one or more switch ports (or VLANs) to a designated monitoring port where a packet analyzer/IDS sensor can capture and inspect the traffic in detail. This aligns with Network+ (N10-009) security and monitoring concepts that distinguish between packet-level visibility and higher-level summaries or logs. If the requirement is explicitly to monitor "contents," you need a method that provides full packet capture capability, not just metadata.

Flow data (e.g., NetFlow) provides summarized metadata—who talked to whom, how much, ports, and timestamps—but not full payload contents. Syslog entries are device/application-generated logs and only show events a device chooses to report; they don't provide full data content visibility. SNMP traps are alerts about status changes (interfaces, thresholds, etc.) and similarly do not include traffic contents. Therefore, port mirroring is the correct monitoring method for inspecting data contents in transit.

質問: 13

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: **A** ([コメントを發表する](#))

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: 14

3 層階層モデルのボトムアップ アプローチにおけるコンポーネントの正しい順序は次のどれですか。

- A.** アクセス、配布、コア
- B.** コア、ルート、ディストリビューション
- C.** コア、スパイン、リーフ
- D.** アクセス、コア、ルーフ

正解: ([正解を表示します](#))

The three-tier hierarchical model in network design consists of three layers: access, distribution, and core. The access layer is where devices like PCs and printers connect to the network. The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer, which is responsible for high-speed data transfer and routing. This approach improves scalability and performance in larger networks. References: CompTIA Network+ Exam Objectives and official study guides.

質問: 15

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: 16

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.

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

質問: 17

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: 18

次のネットワーク トラフィック タイプのうち、ネットワーク上のすべてのノードに送信されるものはどれですか。

- A. ユニキャスト
- B. ブロードキャスト
- C. マルチキャスト
- D. エニーキャスト

正解: ([正解を表示します](#))

Comprehensive and Detailed Explanation (aligned to N10-009):

A broadcast message is delivered to all nodes in a broadcast domain (e.g., ARP requests).

A). Unicast is one-to-one.

C). Multicast is one-to-many but only to subscribed members.

D). Anycast is one-to-one-of-many, sending to the nearest node.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Traffic types: unicast, multicast, broadcast, anycast.

質問: 19

ネットワーク エンジニアは、リモート ブランチのルーターを含むネットワーク サービスを仮想化する必要があります。次のソリューションのうち、要件を満たすものはどれですか。

- A. NFV
- B. VRF
- C. VLAN
- D. VPC

正解: **A** ([コメントを发表する](#))

Network Functions Virtualization (NFV): NFV is a technology that virtualizes network services like routing, firewalls, and load balancers. It allows these services to run on virtual machines rather than requiring dedicated hardware. This is ideal for remote branch locations where deploying physical devices is costly and complex.

VRF (B): Virtual Routing and Forwarding is used for segmenting routing tables but does not virtualize services.

VLAN (C): Virtual Local Area Networks help segregate broadcast domains but are unrelated to virtualizing network functions.

VPC (D): Virtual Private Cloud is used for cloud computing but does not pertain to virtualizing network services.

Reference: CompTIA Network+ Official Study Guide, Domain 2.1 (Virtualization and Cloud Concepts).

質問: 20

ある企業のネットワークで、不審なネットワークトラフィックが大量に発生しています。セキュリティチームは、トラフィックが未知の外部IPアドレスから来ていることを発見しました。この脅威を軽減するための最も費用対効果の高い方法は、次のうちどれですか？

- A. ACL
- B. IDS
- C. NAT
- D. DoS prevention

正解: ([正解を表示します](#))

The correct answer is ACL (Access Control List). According to the CompTIA Network+ N10-009 objectives, ACLs are a fundamental and cost-effective method for controlling traffic flow at routers and firewalls. An ACL allows administrators to permit or deny traffic based on source IP address, destination IP address, protocol, or port number.

In this scenario, the suspicious traffic is identified as originating from a specific unknown foreign IP address.

The most direct and economical mitigation strategy is to configure an ACL rule that denies traffic from that specific IP address (or subnet) at the network perimeter. This approach leverages existing network infrastructure without requiring additional hardware or licensing costs.

An IDS (Intrusion Detection System) monitors and alerts on malicious activity but does not actively block traffic unless paired with IPS functionality, and it may involve additional cost and complexity. NAT is used for address translation and does not provide traffic filtering based on threat intelligence. DoS prevention solutions are typically more advanced, specialized, and costly, often intended for large-scale distributed denial-of-service attacks rather than blocking traffic from a single suspicious IP.

The Network+ objectives emphasize implementing layered security controls, starting with simple and effective measures. In this case, applying an ACL at the firewall or router is the most cost-efficient and immediate method to mitigate the identified threat.

質問: 21

ネットワーク管理者は、複数の場所に最近設置されたファイアウォールからのデータを監視する必要があります。管理者のニーズに最も適したソリューションは次のどれですか？

- A. IDS
- B. IPS
- C. SIEM
- D. SNMPv2

正解: ([正解を表示します](#))

SIEM (Security Information and Event Management) systems are used to aggregate and analyze log data from various sources, including firewalls, to detect potential security incidents and assist in regulatory compliance.

The document explains:

"SIEM solutions aggregate and analyze log and event data from multiple devices, including firewalls, across different locations. They help in real-time monitoring, incident response, and ensuring compliance with security policies."

質問: 22

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: A ([コメントを發表する](#))

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: 23

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。

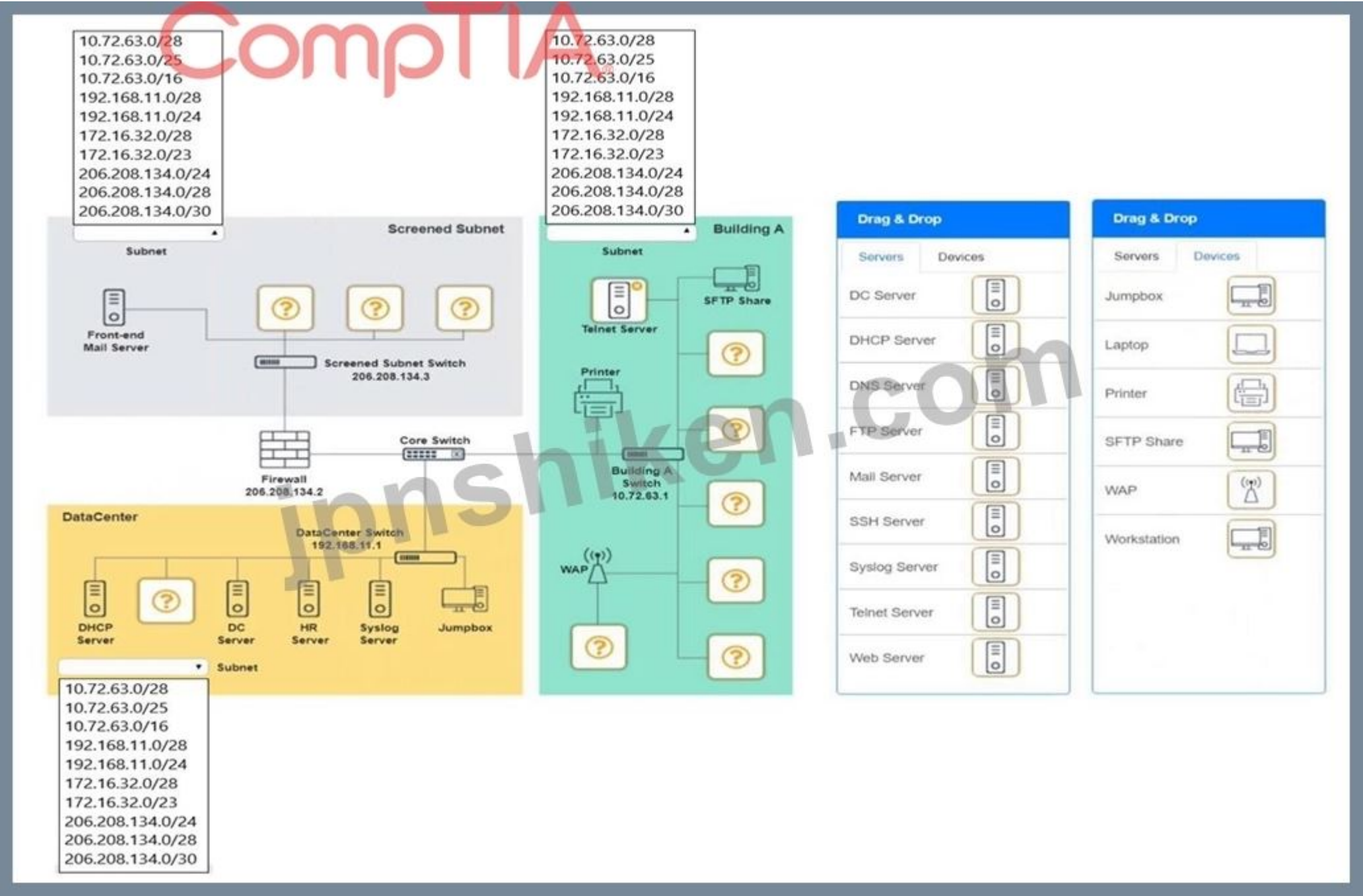
要件：

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。

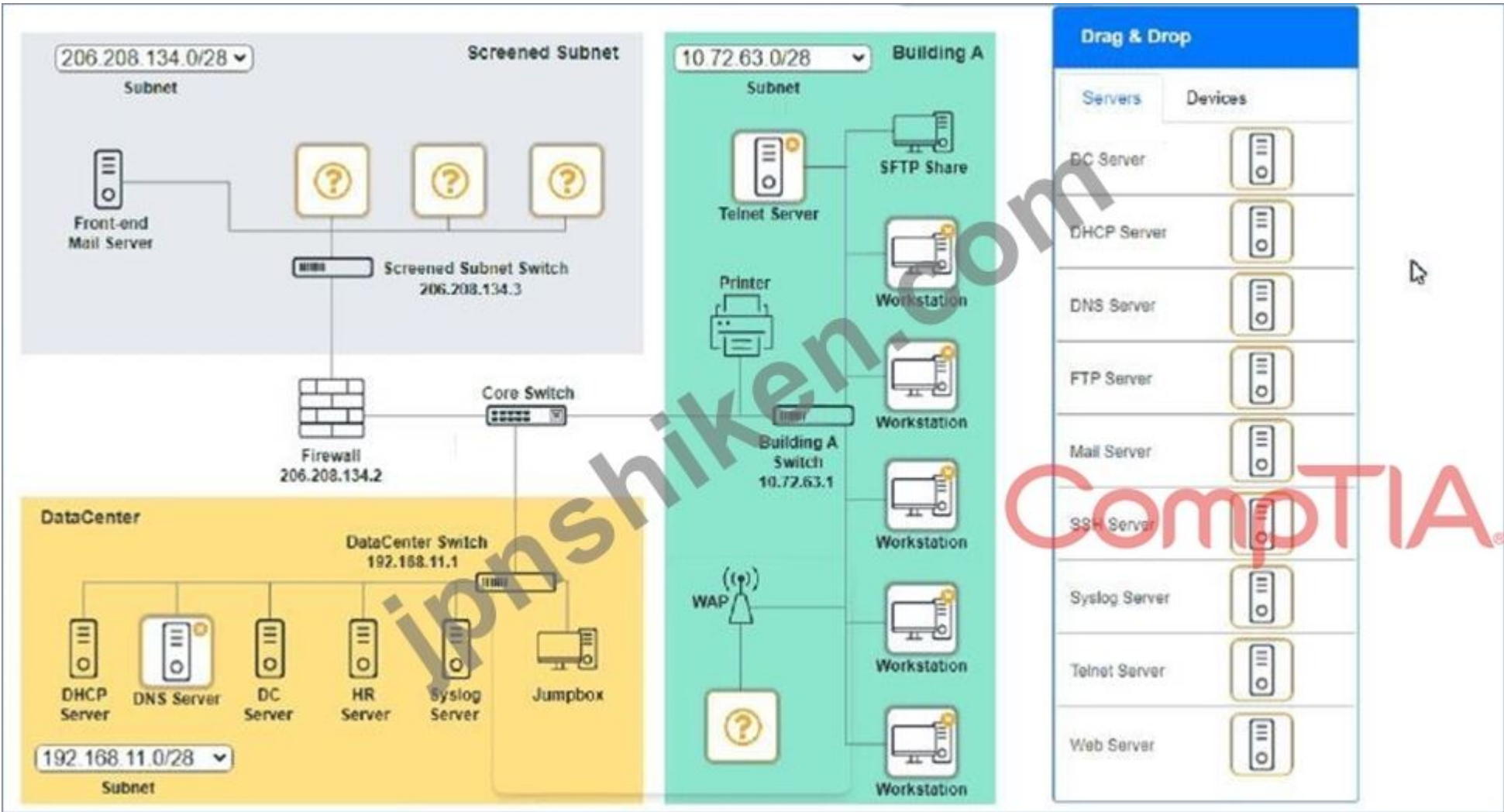
使用可能なオブジェクトは、ドラッグ アンド ドロップ メニューの [サーバー] タブと [デバイス] タブの両方にあります。

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。

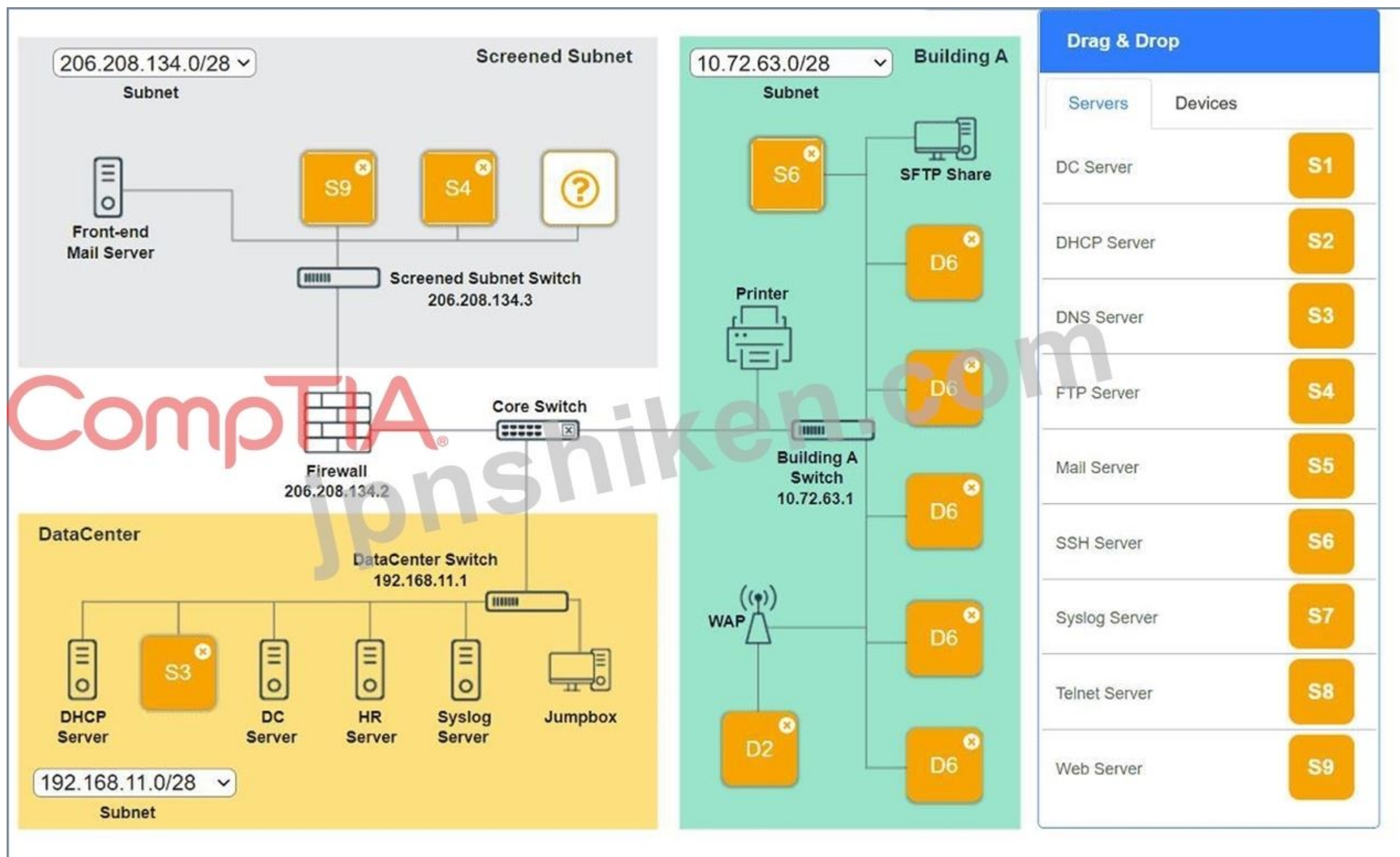


正解:
See explanation below.
Explanation:
Screened Subnet devices - Web server, FTP server

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: 24

安全な電子メールに使用されるポートは次のどれですか？

- A. 25
- B. 110
- C. 143
- D. 587

正解: **D** ([コメントを發表する](#))

Port 587 is used for secure email submission. This port is designated for message submission by mail clients to mail servers using the SMTP protocol, typically with STARTTLS for encryption.

Port 25: Traditionally used for SMTP relay, but not secure and often blocked by ISPs for outgoing mail due to spam concerns.

Port 110: Used for POP3 (Post Office Protocol version 3), not typically secured.

Port 143: Used for IMAP (Internet Message Access Protocol), which can be secured with STARTTLS or SSL/TLS.

Port 587: Specifically used for authenticated email submission (SMTP) with encryption, ensuring secure transmission of email from clients to servers.

Network References:

CompTIA Network+ N10-007 Official Certification Guide: Discusses email protocols and ports, including secure email transmission.

Cisco Networking Academy: Provides training on securing email communications and the use of appropriate ports.

Network+ Certification All-in-One Exam Guide: Explains email protocols, ports, and security considerations for email transmission.

質問: **25**

ネットワーク技術者は、SSID: business という会社の Wi-Fi ネットワークに新しいユーザーを接続しなければなりません。

接続しようとする、2つのネットワークが選択肢として表示されます: SSID: ビジネスとSSID:

myaccess。次の攻撃のうちどれが発生していますか？

A. パス上

B. ロードAP

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 attack occurs when an attacker creates a fraudulent AP with an SSID very similar (or identical) to the legitimate one. Users may accidentally connect, allowing the attacker to capture traffic and credentials.

A). On-path is the consequence of connecting to the evil twin, not the initial attack itself.

B). Rogue AP is any unauthorized access point, but the key here is the malicious mimicry of a legitimate SSID

- specifically an evil twin.

D). Tailgating is a physical social engineering attack, unrelated to Wi-Fi.

References (CompTIA Network+ N10-009):

Domain: Network Security - Wireless threats (rogue APs, evil twins).

質問: **26**

会社のビルのフロアにあるすべてのネットワーク ケーブルの中央終端ポイントを容易にするには、次のパネルのうちどれが最適ですか。

A. パッチ

B. UPS

C. 中質繊維板

D. ラック

正解: **A** ([コメントを發表する](#))

Reference: CompTIA Network+ Certification Exam Objectives - Network Installation section.

質問: **27**

次の攻撃のうち、ネットワーク内で IP アドレスの重複を引き起こす可能性が最も高いのはどれですか？

- A. 不正な DHCP サーバー
- B. DNS ポイズニング
- C. ソーシャルエンジニアリング
- D. サービス拒否

正解: ([正解を表示します](#))

* Definition of a Rogue DHCP Server:

* A rogue DHCP server is an unauthorized DHCP server on a network, which can assign IP addresses to devices without proper control, leading to IP address conflicts.

* Impact of a Rogue DHCP Server:

* IP Address Conflicts: Multiple devices may receive the same IP address from different DHCP servers, causing network connectivity issues.

* Network Disruption: Devices may be assigned incorrect network configuration settings, disrupting network services and connectivity.

* Comparison with Other Attacks:

* DNS poisoning: Alters DNS records to redirect traffic to malicious sites, but does not cause IP address conflicts.

* Social engineering: Involves manipulating individuals to gain unauthorized access or information, not directly related to IP address conflicts.

* Denial-of-service (DoS): Floods a network or service with excessive traffic to disrupt operations, but does not cause duplicate IP addresses.

* Prevention and Detection:

* Implement network access control measures to prevent unauthorized devices from acting as DHCP servers.

* Use DHCP snooping on switches to allow DHCP responses only from authorized DHCP servers.

References:

* CompTIA Network+ study materials on network security threats and mitigation techniques.

質問: 28

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: ([正解を表示します](#))

* 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 tracer.
- * 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:
 - * tracer 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: 29

会社のネットワークでは、ピーク時に大きな遅延とパケット損失が発生しています。ネットワーク監視ツールは、スイッチ上のトラフィックの増加を示しています。ネットワーク技術者がネットワークの輻輳を軽減し、パフォーマンスを向上させるために実装する必要があるのは次のうちどれですか。

- A. 負荷分散
- B. ポートミラーリング
- C. サービス品質
- D. スパニングツリープロトコル

正解: ([正解を表示します](#))

Quality of Service (QoS): This is a feature used in networking to prioritize certain types of traffic. By configuring QoS, network administrators can allocate higher bandwidth to time-sensitive applications like VoIP, video conferencing, or critical business applications during peak usage times. This helps to reduce latency and packet loss, which are often caused by congestion.

Load Balancing (A): While load balancing is useful in distributing traffic across multiple servers or paths, it does not address congestion on a single switch.

Port Mirroring (B): This is used for monitoring network traffic for troubleshooting and diagnostics but does not alleviate congestion.

Spanning Tree Protocol (D): STP prevents switching loops in redundant network topologies, but it is not designed to handle traffic prioritization or congestion issues.

Reference: CompTIA Network+ Official Study Guide, Domain 1.5 (Network Optimization), Domain 2.1 (Network Management).

質問: 30

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: **A** ([コメントを发表する](#))

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: 31

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.

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

質問: **32**

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.

質問: **33**

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
- D. 暖かい

正解: **B** ([コメントを發表する](#))

*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: 34

組織のアーキテクチャに OT デバイスを追加するときに、ネットワーク管理者は次のどれを設定する必要がありますか？

- A. ハニーネット
- B. 保存データの暗号化
- C. 時間ベースの認証
- D. ネットワークセグメンテーション

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: 35

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: 36

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

チャンネルグループ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

チャンネルグループ1モードアクティブ

インターフェースポートチャンネル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: 37

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。

Cable Test Results



Switch 1

Length : 16M

Port : GigabitEthernet0/5

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

PC2

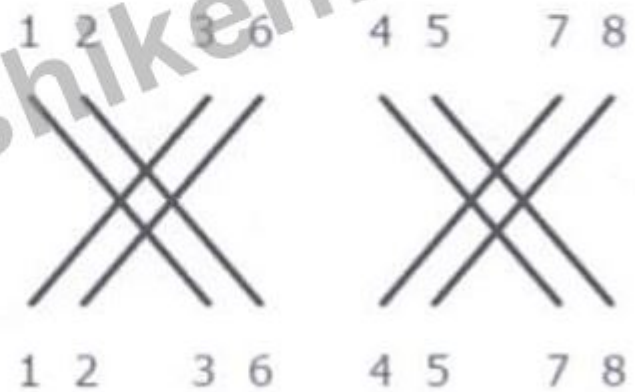
PC3

PC4

PC5

PC6

Connected to Switch 2



CompTIA

Cable Test Results



Switch 1

Length : 16M

Port : GigabitEthernet0/5

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

PC2

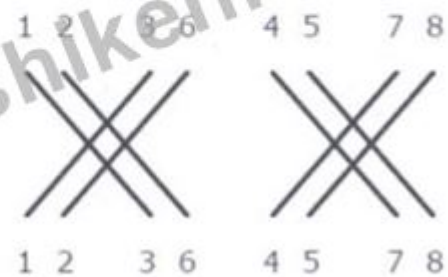
PC3

PC4

PC5

PC6

Connected to Switch 1



Cable Test Results



Switch 1

Length : 22M

Port : GigabitEthernet0/1

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

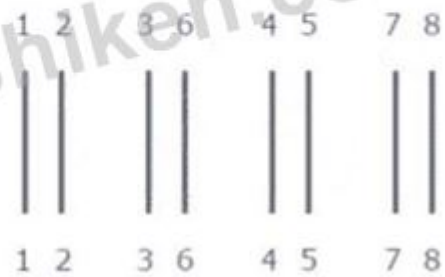
PC2

PC3

PC4

PC5

PC6



Cable Test Results



Switch 1

Length : 12M

Port : GigabitEthernet0/1

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

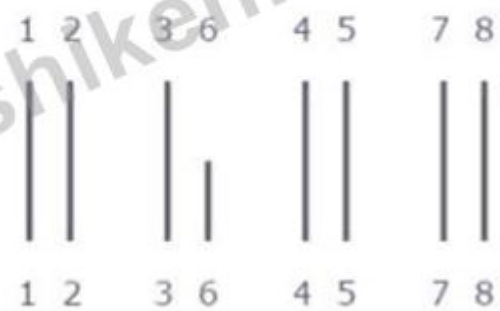
PC2

PC3

PC4

PC5

PC6



Cable Test Results



Switch 1

Length : 18M

Port : GigabitEthernet0/3

Switch 2

VLAN : VLAN 11

Speed : 1000 FDX

Server

PC1

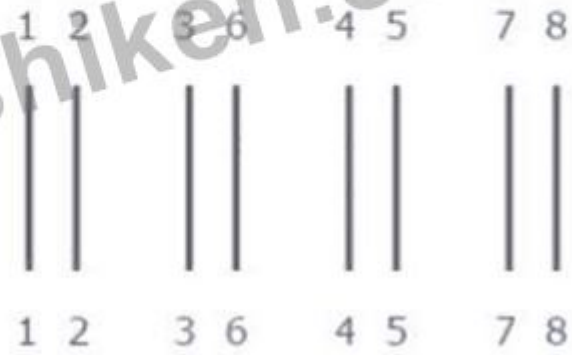
PC2

PC3

PC4

PC5

PC6



CompTIA

Cable Test Results

Switch 1

Switch 2

Server

PC1

PC2

PC3

PC4

PC5

PC6

Length : 33M Port : GigabitEthernet0/4

VLAN : VLAN 10 Speed : 1000 FDX

Cable Test Results

Switch 1

Switch 2

Server

PC1

PC2

PC3

PC4

PC5

PC6

Length : 90M Port : GigabitEthernet0/3

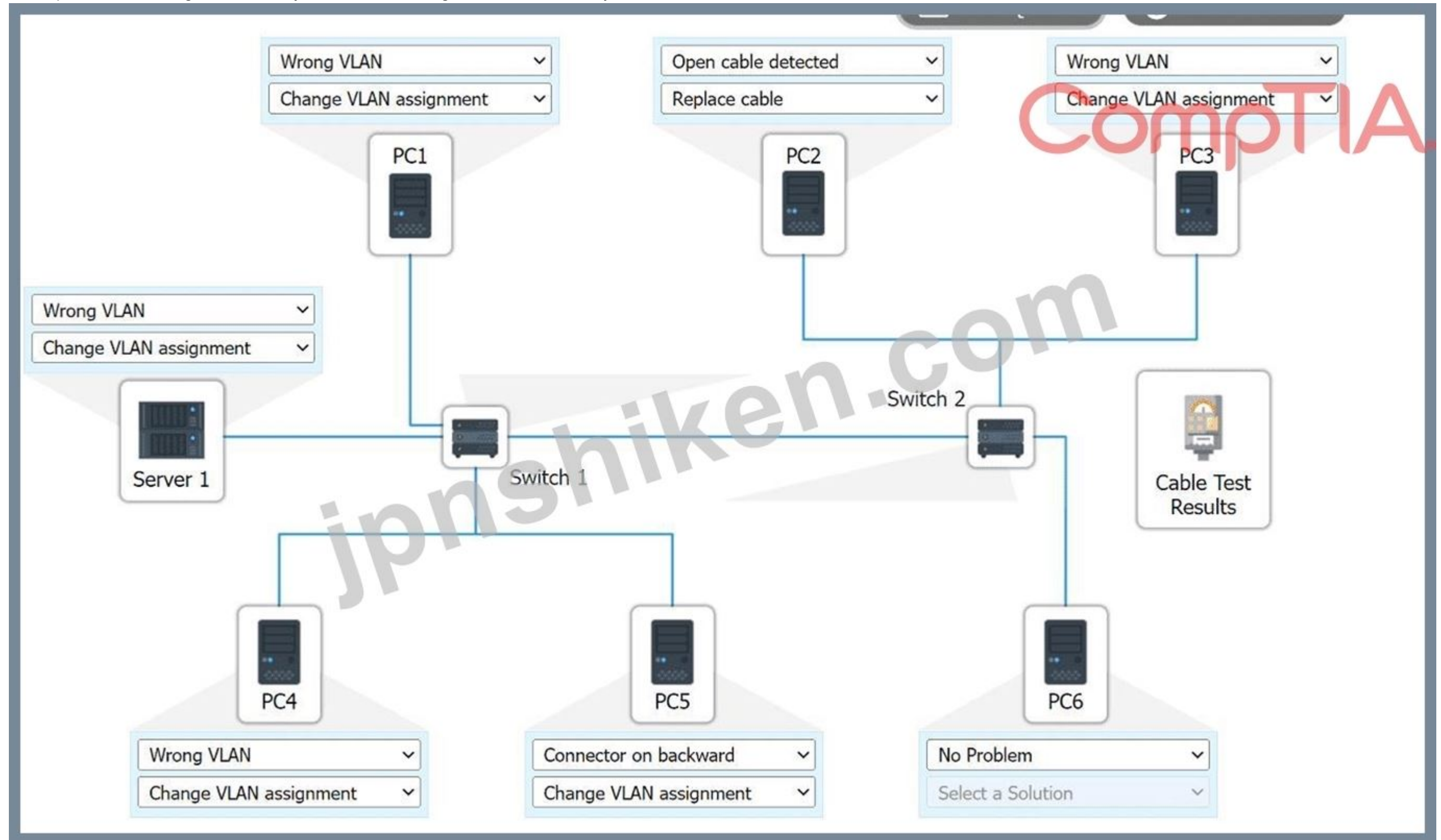
VLAN : VLAN 10 Speed : 1000 FDX

正解:

See the answer and solution below:

Explanation:

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



質問: 38

管理者は、顧客がアクセスできるオフィスのエリアに設置されるスイッチを設定しています。管理者が不明なデバイスがネットワークに接続するのを防ぐための最適な方法は、次のうちどれですか。

A. 南南東

- B. ACL
- C. 境界ネットワーク
- D. 802.1x

正解: ([正解を表示します](#))

802.1x is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. This ensures that only authorized devices can access the network, making it ideal for mitigating the risk of unknown devices connecting to the network, especially in accessible areas.

802.1x Authentication: Requires devices to authenticate using credentials (e.g., username and password, certificates) before gaining network access.

Access Control: Prevents unauthorized devices from connecting to the network, enhancing security in public or semi-public areas.

Implementation: Typically used in conjunction with a RADIUS server to manage authentication requests.

Network References:

CompTIA Network+ N10-007 Official Certification Guide: Covers 802.1x and its role in network security.

Cisco Networking Academy: Provides training on implementing 802.1x for secure network access control.

Network+ Certification All-in-One Exam Guide: Explains the benefits and configuration of 802.1x authentication in securing network access.

質問: 39

ユーザーからSaaSアプリケーションの遅延に関する報告がありました。この問題を解決するために技術者が調整すべき項目は次のうちどれですか？

- A. サーバーのハードウェア仕様
- B. 保存データの暗号化設定
- C. ネットワーク帯域幅と使用率
- D. 仮想マシン構成

正解: ([正解を表示します](#))

The correct answer is Network bandwidth and utilization because latency issues with a SaaS (Software as a Service) application are most commonly related to network performance constraints, not local server hardware or virtualization settings. According to CompTIA Network+ (N10-009) troubleshooting objectives, technicians should evaluate bandwidth capacity, throughput, congestion, packet loss, and overall utilization when diagnosing performance issues affecting cloud-based applications.

Since SaaS applications are hosted externally by a service provider, the organization typically does not control the underlying server hardware or virtual machine configurations (Options A and D). Therefore, adjusting internal server specifications would not resolve user-side latency.

Option B, data-at-rest encryption, applies to stored data security and does not impact real-time application responsiveness.

High network utilization, insufficient bandwidth, QoS misconfiguration, or WAN congestion can significantly increase latency. Technicians should review network monitoring tools, check interface statistics, analyze traffic patterns, and verify Quality of Service (QoS) policies to ensure SaaS traffic is prioritized appropriately.

Thus, optimizing bandwidth and reducing network congestion is the most appropriate corrective action.

質問: 40

会社の会計担当者が財務部門の共有フォルダしか閲覧できない場合、会社が実施する可能性が高いのは次のどれですか。

- A. 一般データ保護規則
- B. 最小権限のネットワークアクセス
- C. 利用規定
- D. エンドユーザー使用許諾契約

正解: ([正解を表示します](#))

Least privilege network access is a principle that restricts users' access rights to only what is necessary for them to perform their job functions. In this case, the accountant's access is limited to only the financial department's shared folders, ensuring that they cannot access other parts of the network unnecessarily. This reduces the risk of unauthorized access and potential data breaches. References: CompTIA Network+ Exam Objectives and official study guides.

質問: 41

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: 42

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: D ([コメントを发表する](#))

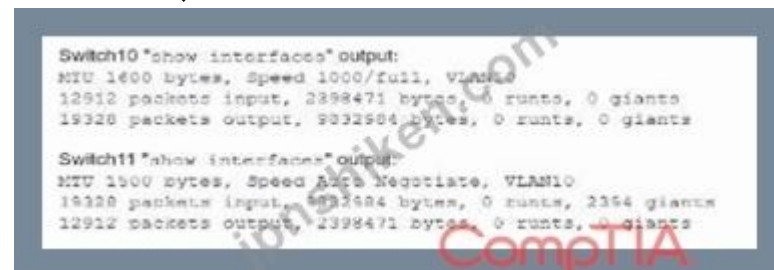
API gateways offer programmable control and real-time communication, commonly over HTTPS, which allows administrators to update and manage devices like access points remotely and efficiently.

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: 43

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. ポートのネイティブ VLAN を変更します。
- C. Switch10のMTU値を1500に変更します。
- D. 両方のスイッチで STP を設定します。

正解: ([正解を表示します](#))

質問: 44

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: ([正解を表示します](#))

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: 45

最近の侵害を受けて、クライアントは全体的なセキュリティを強化したいと考えています。次のうち、実装するのに最適なものはどれですか? (2 つ選択してください。)

- A. 最小権限のネットワークアクセス
- B. 動的在庫
- C. 集中ポリシー管理
- D. ゼロタッチプロビジョニング
- E. 構成ドリフト防止
- F. サブネット範囲の制限

正解: ([正解を表示します](#))

To increase overall security after a recent breach, implementing least privilege network access and central policy management are effective strategies.

* Least Privilege Network Access: This principle ensures that users and devices are granted only the access necessary to perform their functions, minimizing the potential for unauthorized access or breaches. By limiting permissions, the risk of an attacker gaining access to critical parts of the network is reduced.

* Central Policy Management: Centralized management of security policies allows for consistent and streamlined implementation of security measures across the entire network. This helps in quickly responding to security incidents, ensuring compliance with security protocols, and reducing the chances of misconfigurations.

Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Discusses network security principles, including least privilege and policy management.

* Cisco Networking Academy: Provides training on implementing security policies and access controls.

* Network+ Certification All-in-One Exam Guide: Covers strategies for enhancing network security and managing policies effectively.

質問: 46

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: ([正解を表示します](#))

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."

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

質問: **47**

ネットワークエンジニアは、内部ネットワークを公開インターネットから分離・隔離するために境界ネットワークを追加する必要があります。このタスクを達成するのに最適なセキュリティ防御ソリューションは次のどれですか？

A. 信頼ゾーン

B. URLフィルタリング

C. ACL

D. スクリーンドサブネット

正解: ([正解を表示します](#))

Ascreened subnet, also known as aDMZ (Demilitarized Zone), is a boundary network that separates an organization's internal network from external-facing systems. It is used to host public services like web or email servers while protecting internal systems from exposure.

Reference: Section 4.3 - Network Security Features, Defense Techniques, and Solutions - "Screened Subnet (DMZ)"

質問: **48**

技術者は5台の無線デバイスでネットワークを迅速に構築する必要があります。このタスクを完了するには、技術者は次のどのネットワークタイプを設定する必要がありますか？

A. アドホック

B. 背骨と葉

C. ポイントツーポイント

D. メッシュ

正解: ([正解を表示します](#))

The correct answer is Ad hoc because it allows wireless devices to communicate directly with one another without requiring a centralized access point or additional infrastructure. According to CompTIA Network+ (N10-009) objectives under wireless networking concepts, an ad hoc network (also known as an Independent Basic Service Set, or IBSS) enables peer-to-peer wireless communication.

This type of network is ideal for temporary or quick setups where only a small number of devices need to connect. In an ad hoc configuration, each device connects directly to others, making it simple and fast to deploy without requiring switches, routers, or wireless access points.

Spine and leaf (Option B) is a data center architecture designed for high scalability and redundancy, not small wireless setups. Point-to-point (Option C) refers to a direct connection between two devices only, which would not support five devices efficiently. Mesh (Option D) allows multiple nodes to interconnect and provide redundancy, but it is more complex and typically requires compatible infrastructure devices.

Therefore, for a quick setup with five wireless devices, an ad hoc network is the most appropriate choice.

質問: 49

データセンター管理者は、ストレージ環境におけるジャンボフレームの使用を検討しています。ストレージ環境でジャンボフレームを使用する最も適切な理由として、次のうちどれが適切でしょうか。

- A. デバイスのオーバーヘッドを削減するため
- B. STPの現在のルートスイッチを報告する
- C. ルーティングの収束を改善する
- D. ドライブのスループットを向上させる

正解: ([正解を表示します](#))

Jumbo frames are Ethernet frames with a payload greater than the standard 1,500 bytes. Using jumbo frames reduces the number of frames transmitted over the network, thereby reducing the overhead associated with frame headers and processing. The document explains:

"Jumbo frames are used in storage networks to reduce device overhead by lowering the number of frames required for data transfer, which can increase overall throughput and performance."

質問: 50

ある企業の最高情報セキュリティ責任者(CIO)は、セキュリティアナリストがインシデント調査中にイベントを相関分析できるよう、ログファイルを作成する際にサーバーとファイアウォールに正確なタイムスタンプを付与することを要求しています。次のうち、実装すべきものはどれですか？

- A. Syslogサーバー
- B. SMTP
- C. SNMP
- D. NTP

正解: ([正解を表示します](#))

NTP (Network Time Protocol) synchronizes clocks across network devices, ensuring accurate timestamps in logs. This is critical for correlating events across different systems during investigations.

- A). Syslog collects logs but relies on accurate timestamps already present.
- B). SMTP is an email protocol, unrelated to time synchronization.
- C). SNMP is for monitoring and management, not time.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Time synchronization (NTP), log correlation, security operations.

質問: 51

ネットワーク技術者は、取り付けるために丸くてねじるコネクタを備えたファイバー パッチ コードを要求しています。

このコネクタ タイプの正しい名前は次のどれですか？

- A. ST
- B. BNC

C. SC

D. LC

正解: **A** ([コメントを发表する](#))

The ST (Straight Tip) fiber connector is round with a bayonet twist-lock mechanism. It is older but still used in some fiber installations.

B). BNC is a coaxial connector.

C). SC (Subscriber Connector) is a square push-pull fiber connector.

D). LC (Lucent Connector) is a small form-factor fiber connector.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Fiber connectors (ST, SC, LC).

質問: **52**

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: ([正解を表示します](#))

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: **53**

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。

AP1 Configuration



https://ap1.setup.do

Basic Configuration

Access Point Name

IP Address /

Gateway

SSID

SSID Broadcast ☒ Yes ☐ No

Wireless

Mode

Channel

Wired

Speed ☐ Auto ☒ 100 ☐ 1000

Duplex ☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings ☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

AP3 Configuration



https://ap3.setup.do

Basic Configuration

Access Point Name

AP3

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B
G

Channel

1
2
3
4
5
6
7
8
9
10
11

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Security Settings

None WEP WPA WPA2 WPA2-Enterprise

Key or Passphrase

Reset to Default Save Close

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.

AP1 Configuration

https://ap1.setup.do

Basic Configuration

Access Point Name AP1

IP Address 192.168.1.32

Gateway 192.168.1.1

SSID CorpNet

SSID Broadcast ☒ Yes ☐ No

Wireless

Mode B

Channel 3

Wired

Speed ☐ Auto ☒ 100 ☐ 1000

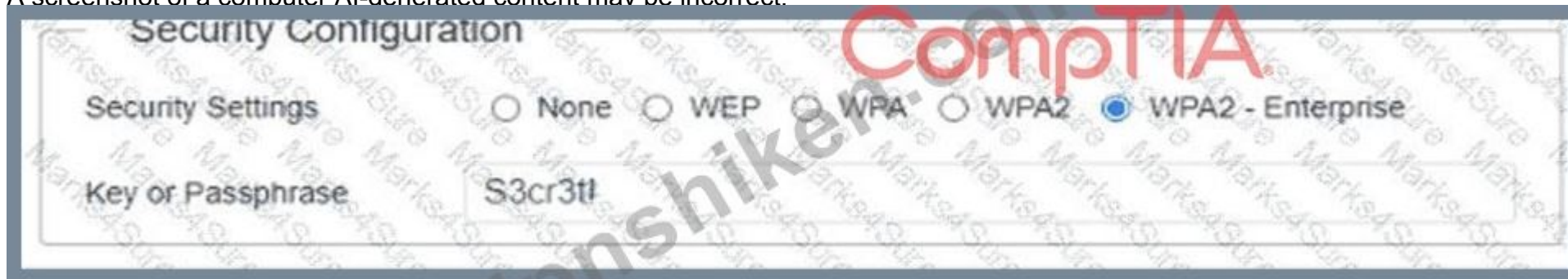
Duplex ☐ Auto ☐ Half ☒ Full

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.

AP1 Configuration

https://ap1.setup.do

IP Address

192.168.1.3

/

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

Yes

No

Wireless

Mode

G

Channel

3

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Reset to Default

Save

Close

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.

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name: AP3

IP Address: 192.168.1.96 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode: B

Channel: 9

Wired

Speed: ☐ Auto ☒ 100 ☐ 1000

Duplex: ☐ Auto ☐ Half ☒ Full

Security Configuration

Reset to Default Save Close

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

Security Configuration

Security Settings: ☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase: S3cr3t!

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

AP3 Configuration

https://ap3.setup.do

IP Address: 192.168.1.5 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode: G

Channel: 9

Wired

Speed: ☒ Auto ☐ 100 ☐ 1000

Duplex: ☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings: ☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase: S3cr3t!

Reset to Default Save Close

質問: 54

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: ([正解を表示します](#))

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: **55**

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の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** ([コメントを發表する](#))

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: **56**

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: **57**

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: **D** ([コメントを發表する](#))

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: **58**

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.

質問: **59**

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: **A** ([コメントを發表する](#))

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: **60**

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: 61

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NTPI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).

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

質問: 62

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: **C** ([コメントを发表する](#))

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: 63

ルーターが優先ルートを決定するために使用するものは次のどれですか？

A. 最短接頭辞一致

B. EIGRPから学習したルート

C. 最長接頭辞一致

D. OSPFから学習したルート

正解: **C** ([コメントを发表する](#))

Routers determine the best route to a destination using longest prefix match . This means the router chooses the route entry with the most specific matching network prefix for the destination IP address. For example, if a routing table contains 10.1.0.0/16 and 10.1.2.0/24 , a packet destined to 10.1.2.50 matches both entries, but the router prefers /24 because it is more specific (longer mask). Network+ (N10-009) routing fundamentals emphasize that route selection begins with prefix length specificity before considering other factors within the same prefix length (such as administrative distance and metric, depending on the platform).

"Shortest prefix match" is the opposite of correct behavior. "Routes learned from EIGRP" and "routes learned from OSPF" describe sources of routes, not the general selection rule routers use when multiple matching routes exist. Even if routes come from different protocols, the router still applies selection logic; the universal rule for matching destination networks is longest prefix match . Hence, option C is correct.

質問: 64

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ーが活用されていますか？

A. TLS

B. FHRP

C. SSL

D. PAT

正解: **D** ([コメントを发表する](#))

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: 65

ルーターがルート選択プロセスで最初に優先するものは次のどれですか？

- A. プレフィックス長
- B. メトリック
- C. 管理距離
- D. デフォルトルート

正解: ([正解を表示します](#))

In the router route selection process, the first priority is the longest prefix match, also known as prefix length.

According to CompTIA Network+ (N10-009) routing concepts, routers examine the destination IP address in the packet and compare it to entries in the routing table. When multiple routes exist, the router selects the route with the most specific match, meaning the route with the longest subnet mask (largest number of matching bits). For example, a /30 route is preferred over a /24, and a /24 is preferred over a /16 if all match the destination.

Only after the longest prefix match is determined do other factors come into play. Administrative distance (AD) is used to determine which routing source is more trustworthy when the same network is learned from different routing protocols (e.g., OSPF vs. RIP). Metric is then used within the same routing protocol to determine the best path (e.g., hop count, cost, bandwidth). A default route (0.0.0.0/0) is used only when no more specific match exists.

Therefore, prefix length is always evaluated first in route selection.

質問: 66

次のルーティング テクノロジーのうち、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: 67

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: D ([コメントを發表する](#))

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: 68

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: 69

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: 70

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: **A** ([コメントを發表する](#))

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: 71

ある企業が、すべてのデバイスがIPv6アドレスを使用する新しい社内ネットワークを構築しようとしています。この設定に最適なルーティングプロトコルは次のうちどれですか？

- A. EIGRP
- B. OSPFv3
- C. BGP4
- D. iBGP

正解: **B** ([コメントを發表する](#))

For an internal network using IPv6 , the best option listed is OSPFv3 , which is the OSPF version designed to support IPv6 routing. In Network+ (N10-009) routing objectives, OSPF is a common interior gateway protocol (IGP) used within an organization (an autonomous system) to exchange routes dynamically and converge efficiently. OSPFv3 maintains the link-state approach of OSPF while adding IPv6 support, making it a strong fit for enterprise internal routing where multiple routers and subnets need dynamic path calculation and fast convergence. BGP4 and iBGP are associated with BGP , primarily used for inter-domain routing on the internet and between large networks; while BGP can carry IPv6 (via MP-BGP), it is generally not the "best" default choice for a typical internal-only enterprise network unless there is a specific design reason. EIGRP can support IPv6 in some implementations, but Network+ typically emphasizes OSPF/OSPFv3 as the widely adopted, vendor-neutral IGP for IPv6 deployments. Given the options and the "best for this setup" wording, OSPFv3 is the most appropriate answer.

質問: 72

ネットワーク管理者は新しいスイッチを構成しており、割り当てられたデバイスのみがスイッチに接続できるようにしたいと考えています。管理者は次のどれを行う必要がありますか？

- A. ACL を設定します。
- B. キャプティ ブポータルを実装します。
- C. ポートセキュリティを有効にします。
- D. 不要なサービスを無効にします。

正解: ([正解を表示します](#))

Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

質問: 73

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. 複数の問題を個別に処理する
- B. 考えられる根本原因についての理論を作成する
- C. トップダウンアプローチを使用する
- D. アイデアを検証するためのテストを実施する

正解: ([正解を表示します](#))

質問: 74

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: 75

ユーザーは、リモート ファイル サーバーにアクセスできなくなったことをネットワーク管理者に通知します。ネットワーク管理者はサーバーに ping を実行し、現在のファイアウォール ルールがネットワーク ファイル共有へのアクセスをブロックしていないことを確認します。次のツールのうち、リモート ファイル サーバーで開いているポートを識別するのに役立つものはどれですか。

- A. 掘る
- B. Nmap
- C. トレース
- D. nslookup

正解: ([正解を表示します](#))

Nmap (Network Mapper) is a powerful network scanning tool used to discover hosts and services on a computer network. It can be used to identify which ports are open on a remote server, which can help diagnose access issues to services like a remote file server.

* Port Scanning: Nmap can perform comprehensive port scans to determine which ports are open and what services are running on those ports.

* Network Discovery: It provides detailed information about the host's operating system, service versions, and network configuration.

* Security Audits: Besides troubleshooting, Nmap is also used for security auditing and identifying potential vulnerabilities.

Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Covers network scanning tools and their uses.

* Nmap Documentation: Official documentation provides extensive details on how to use Nmap for port scanning and network diagnostics.

* Network+ Certification All-in-One Exam Guide: Discusses various network utilities, including Nmap, and their applications in network troubleshooting.

質問: 76

パブリック クラウド プロバイダーへの専用回線を持つことに最も関連しているのは次のうちどれですか。

- A. VPN
- B. 直接接続
- C. インターネットゲートウェイ
- D. プライベートクラウド

正解: ([正解を表示します](#))

Direct Connect is the option most closely associated with having a leased line to a public cloud provider, as defined in the CompTIA Network+ N10-009 objectives under cloud connectivity and WAN technologies.

Direct Connect (or equivalent services such as Azure ExpressRoute or Google Cloud Interconnect) provides a dedicated, private physical connection between an organization's on-premises network and a public cloud provider's infrastructure. This connection bypasses the public internet, offering consistent bandwidth, lower latency, improved performance, and enhanced security. A VPN uses encrypted tunnels over the public internet, which does not qualify as a leased line and is subject to internet congestion and variable performance. An internet gateway simply allows cloud resources to communicate with the public internet and does not imply a private or dedicated connection. A private cloud refers to a deployment model where cloud resources are dedicated to a single organization; it does not describe the connectivity method or the use of a leased circuit.

According to Network+ objectives, leased-line connectivity to cloud providers is commonly used by enterprises that require high availability, predictable throughput, regulatory compliance, or secure hybrid cloud architectures. Direct Connect is a foundational component of hybrid networking strategies, linking on- premises environments directly to public cloud services using provider-managed circuits.

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

質問: 77

ネットワーク管理者は、断続的なネットワーク接続に関する苦情を受けました。管理者は調査を行い、ネットワーク設計に潜在的なループシナリオが含まれていることを発見しました。管理者は次のうちどれを行うべきでしょうか？

- A. スパニングツリーを有効にする
- B. ポートセキュリティを構成する
- C. スイッチポートの速度制限を変更する
- D. 802.1Qタグ付けを強制する

正解: **A** ([コメントを发表する](#))

Spanning Tree Protocol (STP) is designed to detect and prevent Layer 2 loops by blocking redundant paths. If loops are possible in the design, enabling STP ensures network stability.

- B). Port security controls endpoint MAC addresses, not loops.
- C). Speed limits address bandwidth, not loop prevention.
- D). 802.1Q tagging allows VLAN separation but does not resolve loops.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Loop prevention, spanning tree, switch design.

質問: 78

ネットワーク管理者が評価を実施したところ、基準を満たしていないネットワークデバイスを発見しました。デバイスが遵守すべき一連のルールとして考えられる構成は次のうちどれですか？

- A. 生産
- B. バックアップ
- C. 候補
- D. ゴールデン

正解: ([正解を表示します](#))

The correct answer is golden configuration. This is a reference standard or baseline that defines the approved settings and rules devices should follow. Any deviation from the golden configuration indicates drift or misconfiguration that must be remediated.

- A). Production refers to the live environment but doesn't define a standard.
- B). Backup configurations are stored copies, not the standard rules.
- C). Candidate configuration is a proposed change being tested, not the final baseline.

By enforcing golden configurations, administrators ensure compliance, maintain security standards, and improve consistency across the enterprise.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Configuration standards, golden images/configs.

質問: 79

トラブルシューティング方法論の次の手順のうち、最近の変更についてログを確認する手順はどれですか？

- A. 問題を特定します。
- B. 調査結果と結果を文書化します。
- C. 原因を特定するために理論をテストします。
- D. 行動計画を立てます。

正解: ([正解を表示します](#))

Reference: CompTIA Network+ Certification Exam Objectives - Troubleshooting section.

質問: 80

ある会社が新しい IPS をインストールした後、ネットワークの速度が低下しています。ネットワーク管理者は問題のトラブルシューティングを行い、速度テストを実行します。さまざまなネットワークの場所からの結果は次のとおりです。

場所 スピード ダウン スピード アップ

ワイヤレス ラップトップ 4.8 Mbps 47.1 Mbps

有線デスクトップ 5.2 Mbps 49.3 Mbps

ファイアウォール 48.8 Mbps 49.5 Mbps

最も可能性の高い問題はどれですか？

- A. パケット損失
- B. ボトルネック
- C. チャネルの重複
- D. ネットワークの混雑

正解: ([正解を表示します](#))

Bottlenecking occurs when a device in the network (such as an IPS) cannot process traffic efficiently, resulting in a dramatic drop in throughput. The significant difference between the firewall's speed (48.8 Mbps down) and the end-user devices' speeds (4.8 - 5.2 Mbps down) indicates a bottleneck caused by the IPS.

*Why not the other options?

*Packet loss (A) - Would typically cause connection timeouts, not just slow speeds.

*Channel overlap (C) - Affects only wireless networks, but the wired desktop is also experiencing slow speeds.

*Network congestion (D) - Would show fluctuations in both upload and download speeds, but upload speeds remain unaffected.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 13: Network Performance Optimization

質問: 81

顧客が新しいUTMデバイスを購入し、開発チームにデバイスのデータレポート機能の一部を社内のカスタムサポートソフトウェアに統合するよう依頼しました。開発チームは、デバイスのデータを取得するために、以下のどの機能を使用すべきでしょうか？

A. API

B. SNMPv2c

C. SIEM

D. MIB

正解: [\(正解を表示します\)](#)

An API (Application Programming Interface) is the best choice when a development team needs to integrate a device's reporting data directly into custom software. In Network+ (N10-009) objectives, network operations commonly include device management, monitoring, and automation, and APIs are a key method for programmatic access to operational data (often via REST/HTTPS with structured formats like JSON). This enables the internal support application to pull dashboards, health metrics, events, configuration details, and reporting outputs in a controlled, developer-friendly way.

SNMPv2c is primarily used for network monitoring and polling counters/alerts, but it is less secure (community strings) and is not as flexible for modern application integration as an API. A MIB is not a data- access "feature" by itself; it's the schema/definitions SNMP uses to describe managed objects. A SIEM is a separate security analytics platform that collects and correlates logs/events-useful for security operations, but not the direct interface a custom support tool would typically call to retrieve device reporting data.

質問: 82

HTTPS を使用する際に転送中の暗号化を実装するために最もよく使用されるのは次のどれですか。

A. SSH

B. TLS

C. SCADA

D. RADIUS

正解: **B** ([コメントを发表する](#))

Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):

HTTPS is HTTP encapsulated in TLS (the successor to SSL), which provides confidentiality, integrity, and server authentication for web traffic.

* A. SSH secures remote shell and tunnels, not HTTPS.

* C. SCADA refers to industrial control systems, not a transport security protocol.

* D. RADIUS is an AAA protocol for authentication/authorization/accounting, not the web encryption layer.

References (CompTIA Network+ N10-009):

* Domain: Network Standards, Protocols, and Implementations - Web protocols (HTTP/HTTPS), TLS handshake and purpose, encryption in transit.

質問: 83

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: **84**

ゲスト ネットワークを使用する前に、管理者はユーザーに使用条件に同意することを要求します。この目的を達成するための最適な方法はどれですか。

- A. 事前共有キー
- B. 自律アクセスポイント
- C. キャプティブポータル
- D. WPA2 暗号化

正解: **C** ([コメントを发表する](#))

A captive portal is a web page that users must view and interact with before being granted access to a network. It is commonly used in guest networks to enforce terms of use agreements.

When a user connects to the network, they are redirected to this portal where they must accept the terms of use before proceeding. This method ensures that users are aware of and agree to the network's policies, making it the best choice for this scenario. References: CompTIA Network+ Exam Objectives and official study guides.

質問: **85**

顧客が隣接する建物間にファイバー接続を追加しています。技術者がマルチモード ケーブルをファイバー パッチ パネルに終端します。技術者がファイバー パッチ ケーブルを接続した後、インジケータ ライトが点灯しません。技術者がこの問題のトラブルシューティングを行うために最初に試すべきことは次のどれですか。

- A. 繊維を反転します。
- B. ファイバーを再終端します。
- C. ファイバーのサイズを確認します。
- D. ケーブル配線に目視による欠陥がないか検査します。

正解: ([正解を表示します](#))

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

質問: **86**

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.

質問: 87

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: ([正解を表示します](#))

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: 88

EOL と EOS の違いは次のどれですか？

- A. EOL により製品は廃止されますが、サポートは提供される場合があります。
- B. EOS は無料サポートをサブスクリプション モデルに置き換えます。
- C. EOS は物理的な製品にのみ適用されます。
- D. EOL でも保証サービスは引き続き保証されます。

正解: ([正解を表示します](#))

The correct answer is EOL discontinues the product but may offer support. According to CompTIA Network+ (N10-009) objectives related to lifecycle management and vendor support policies, End of Life (EOL) indicates that a product is no longer being manufactured or sold by the vendor. However, after EOL is declared, the vendor may continue to provide limited support, updates, or warranty services for a defined period.

In contrast, End of Support (EOS) means the vendor has stopped providing technical assistance, patches, firmware updates, and security fixes for the product. Once a product reaches EOS, organizations are responsible for maintaining it without vendor assistance, which can introduce operational and security risks.

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

Therefore, the key distinction is that EOL ends product sales, while EOS ends vendor support.

質問: 89

次の IP 送信タイプのうち、送信されるデータをすべて暗号化するものはどれですか？

- A. 超能力
- B. ああ
- C. GRE
- D. UDP
- E. TCP

正解: [\(正解を表示します\)](#)

Definition of ESP (Encapsulating Security Payload):

ESP is a part of the IPsec protocol suite used to provide confidentiality, integrity, and authenticity of data.

ESP encrypts the payload and optional ESP trailer, providing data confidentiality.

ESP Functionality:

ESP can encrypt the entire IP packet, ensuring that the data within the packet is secure from interception or eavesdropping. It also provides options for data integrity and authentication.

ESP operates in two modes: transport mode (encrypts only the payload of the IP packet) and tunnel mode (encrypts the entire IP packet).

Comparison with Other Protocols:

AH (Authentication Header): Provides data integrity and authentication but does not encrypt the payload.

GRE (Generic Routing Encapsulation): A tunneling protocol that does not provide encryption.

UDP (User Datagram Protocol) and TCP (Transmission Control Protocol): These are transport layer protocols that do not inherently provide encryption. Encryption must be provided by additional protocols like TLS/SSL.

Use Cases:

ESP is widely used in VPNs (Virtual Private Networks) to ensure secure communication over untrusted networks like the internet.

References:

CompTIA Network+ study materials on IPsec and encryption.

質問: 90

サイト間接続を提供する最も安全な方法はどれですか？

- A. VXLAN
- B. IKE
- C. GRE
- D. IPsec

正解: **D** ([コメントを發表する](#))

IPsec (Internet Protocol Security) is the most secure way to provide site-to-site connectivity. It provides robust security services, such as data integrity, authentication, and encryption, ensuring that data sent across the network is protected from interception and tampering. Unlike other options, IPsec operates at the network layer and can secure all traffic that crosses the IP network, making it the most comprehensive and secure choice for site-to-site VPNs.

References: CompTIA Network+ study materials and NIST Special Publication

800-77.

質問: 91

ネットワーク管理者は、サービスをオフサイト環境にフェイルオーバーする必要があります。このプロセスが完全に機能するまでには4週間かかります。これは、以下のDR(災害復旧)の概念のうちどれに当てはまりますか？

- A. ホットサイト
- B. コールドサイト

C. アクティブ・アクティブアプローチ

D. ウォームサイト

正解: ([正解を表示します](#))

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

質問: **92**

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** ([コメントを发表する](#))

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: **93**

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: **C** ([コメントを发表する](#))

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: 94

組織のユーザーから、建物の一部のエリアでワイヤレス ネットワークが機能していないという報告がありました。ネットワークを検索すると他のワイヤレス ネットワークの SSID は表示されるものの、組織のネットワークが表示されないという報告がありました。次のどれが最も原因として考えられますか。

A. 干渉またはチャネルの重複

B. 無線範囲が不十分です

C. ローミングの設定ミス

D. クライアントの分離の問題

正解: ([正解を表示します](#))

If the company's SSID is not visible in some areas while other networks are still visible, the most likely cause is insufficient wireless coverage. The wireless signal does not reach those areas, meaning additional access points or signal boosters may be required.

Breakdown of Options:

A). Interference or channel overlap - Would cause slow or unstable connections, but the SSID should still be visible.

B). Insufficient wireless coverage - # Correct answer. If the SSID is not appearing, the signal is too weak in that area.

C). Roaming misconfiguration - Would cause devices to stay on weaker APs instead of switching, but the SSID should still be visible.

D). Client disassociation issues - This would disconnect users, but they should still see the network.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.6: Explain wireless concepts and technologies.

質問: 95

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: ([正解を表示します](#))

* 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: 96

次のネットワーク トポロジのうち、ネットワーク内のすべてのノード間に直接接続が含まれるのはどれですか。

- A. メッシュ
- B. ハブアンドスポーク
- C. スター
- D. ポイントツーポイント

正解: **A** ([コメントを發表する](#))

In a mesh topology, every node is directly connected to every other node. This provides high redundancy and reliability, as there are multiple paths for data to travel between nodes. This topology is often used in networks where high availability is crucial. References: CompTIA Network+ study materials.

質問: 97

ある企業の最高情報セキュリティ責任者 (CIO) は、セキュリティアナリストがインシデント調査中にイベントを相関分析できるよう、ログファイルを作成する際にサーバーとファイアウォールに正確なタイムスタンプを付与することを要求しています。次のうち、実装すべきものはどれですか？

- A. Syslogサーバー
- B. SMTP
- C. NTP
- D. SNMP

正解: ([正解を表示します](#))

The correct solution is NTP (Network Time Protocol). Accurate timestamps across servers, firewalls, and network devices are critical for correlating logs during incident response. NTP synchronizes device clocks to a trusted time source, ensuring consistency across the network.

A). Syslog centralizes logs but does not synchronize time.

B). SMTP is email transfer, unrelated to time.

D). SNMP monitors devices but does not correct time discrepancies.

By implementing NTP, analysts can ensure that logs from different devices are time-aligned, which is essential for reconstructing attack timelines and detecting anomalies.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Time synchronization, NTP, log correlation.

質問: 98

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. ルーター 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: ([正解を表示します](#))

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.

質問: **99**

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: **100**

ネットワーク管理者は、150 人のユーザーを抱える新しいサイトのネットワークを構成しています。今後 1 年以内に、サイトのユーザー数は 10 人増加すると予想されます。各ユーザーには 2 つの IP アドレスが与えられます。1 つはコンピューター用、もう 1 つはネットワークに接続された電話用です。次のクラスフル IPv4 アドレス範囲のうち、ネットワークに最適なのはどれでしょうか。

- A. クラスD
- B. クラスB
- C. クラスA
- D. クラスC

正解: ([正解を表示します](#))

IPv4 addresses are divided into classes:

Class A: Supports 16,777,214 hosts (large enterprises).

Class B: Supports 65,534 hosts (medium to large networks).

Class C: Supports 254 hosts (small to medium networks).

Class D: Used for multicast, not for assigning IPs to hosts.

Step-by-step Calculation:

The network will have 150 users initially, with a projected growth of 10 users, totaling 160 users.

Each user has two devices, so $160 \times 2 = 320$ IP addresses needed.

A Class C subnet has 254 usable IPs by default, which is not sufficient.

A Class B subnet can support thousands of hosts, making it the most appropriate option.

Incorrect Options:

A:Class D: Reserved for multicast, not for host assignments.

C:Class A: Overkill for a network of this size.

D:Class C: Cannot support 320 hosts without subnetting, making Class B the best choice.

Reference:

CompTIA Network+ N10-009 Official Study Guide - Chapter on IP Addressing and Subnetting

質問: **101**

ネットワークエンジニアが新しいPoE対応無線APを設置しています。最初の5台のAPは正常に展開されましたが、6台目が起動に失敗しました。エンジニアが最初に調査すべき項目は次のうちどれですか？

- A. 信号強度
- B. デュプレックスの不一致
- C. 電力予算
- D. CRC

正解: ([正解を表示します](#))

When deploying multiple Power over Ethernet (PoE) devices, the switch's power budget can be exhausted. If the available wattage on the switch cannot supply the additional AP, it will fail to power on. This is the most likely cause when previous APs worked fine but a new one does not.

A). Signal strength affects wireless connectivity, not whether the AP powers up.

B). Duplex mismatch causes poor throughput, not power failure.

D). CRC errors point to cabling issues but do not prevent booting if no power is available.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - PoE power budget considerations, device startup issues.

質問: **102**

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

- A. /24
- B. /25
- C. /26
- D. /27

正解: **B** ([コメントを发表する](#))

The correct answer is /25, which is the appropriate subnet mask for dividing an existing Class C network into two equal subnets. According to the CompTIA Network+ N10-009 objectives, subnetting is a core networking concept used to improve network segmentation, performance, and security.

A Class C network uses a default subnet mask of /24 (255.255.255.0), which provides 256 total addresses (254 usable). To split this network into two sections, the administrator must borrow one host bit from the last octet. Borrowing one bit results in a /25 subnet mask (255.255.255.128). This creates two subnets, each with 128 total addresses (126 usable)-an ideal solution for separating two departments such as finance and marketing.

A /24 would not create any segmentation, as it represents the original single network. A /26 would create four subnets, and a /27 would create eight subnets, both of which exceed the requirement of only two sections and unnecessarily reduce the number of available host addresses per subnet.

The Network+ objectives emphasize selecting subnet masks based on organizational requirements, balancing the number of subnets with sufficient host capacity. In this scenario, /25 is the most efficient and correct choice.

質問: 103

ネットワーク技術者が最近購入した商用スイッチのセキュリティ強化を試みています。公開情報の利用を最も効果的に軽減できるセキュリティ強化手法はどれですか？

- A. デフォルトのパスワードの変更
- B. 受信SSH接続をブロックしています
- C. ネットワーク構成からゲートウェイを削除する
- D. スイッチへの物理的なアクセスを制限する

正解: ([正解を表示します](#))

Changing the default password is a fundamental step in device hardening, as default credentials are widely known and published online, posing a significant security risk if not updated. The document notes:

"Default passwords are often known by attackers and published on the internet. Changing them to unique, strong passwords is a critical first step in securing network devices against unauthorized access."

質問: 104

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: **105**

次のファイバー コネクタ タイプのうち、ネットワーク インターフェイス カードで使用される可能性が最も高いのはどれですか。

- A. LC
- B. SC
- C. ST
- D. MPO

正解: ([正解を表示します](#))

* Definition of Fiber Connector Types:

* LC (Lucent Connector): A small form-factor fiber optic connector with a push-pull latching mechanism, commonly used for high-density applications.

* SC (Subscriber Connector or Standard Connector): A larger form-factor connector with a push- pull latching mechanism, often used in datacom and telecom applications.

* ST (Straight Tip): A bayonet-style connector, typically used in multimode fiber optic networks.

* MPO (Multi-fiber Push On): A connector designed to support multiple fibers (typically 12 or 24 fibers), used in high-density cabling environments.

* Common Usage:

* LC Connectors: Due to their small size, LC connectors are widely used in network interface cards (NICs) and high-density environments such as data centers. They allow for more connections in a smaller space compared to SC and ST connectors.

* SC and ST Connectors: These are larger and more commonly used in patch panels and older fiber installations but are less suitable for high-density applications.

* MPO Connectors: Primarily used for trunk cables in data centers and high-density applications but not typically on individual network interface cards.

* Selection Criteria:

* The small form-factor and high-density capabilities of LC connectors make them the preferred choice for network interface cards, where space and connection density are critical considerations.

References:

* CompTIA Network+ study materials on fiber optics and connector types.

質問: **106**

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.

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

質問: **107**

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

ping -c 10 192.168.50.140

パケット: 送信 = 10、受信 = 5、損失 = 5 (50% 損失)

往復時間: 最小 = 3ms、最大 = 144ms、平均 = 42ms

スイッチの問題のトラブルシューティングを最小限の影響で継続するには、技術者は次のどれを実行する必要がありますか？

- A. トーニングとプローブを実行します。
- B. ケーブルを交換してください。
- C. 障害を視覚的に特定します。
- D. スイッチを再起動します。

正解: ([正解を表示します](#))

The ping results show intermittent connectivity (50% packet loss) with highly variable latency, which commonly indicates a Layer 1/Layer 2 problem (e.g., damaged cable pairs, bad patch-panel termination, failing switch port, duplex/negotiation issues, or excessive errors on the interface). Because the facility has incomplete documentation, the technician's first priority at the switch is to positively identify the correct switch port and cable path associated with the file server before making disruptive changes.

Using a tone generator and probe aligns with Network+ troubleshooting objectives that emphasize selecting the appropriate tool and following an efficient, structured process: identify the problem, establish a theory, test, and then implement the least disruptive fix. Toning/probing helps map the server's drop to the switch port (even through patch panels) so the technician can then check that specific interface for errors/discards, CRCs, speed/duplex negotiation status, and link stability-all without rebooting the switch or immediately replacing hardware. By contrast, restarting the switch is high-impact, and replacing a cable is a change best performed after the correct run/port is confirmed.

質問: **108**

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: 109

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: 110

IDF のコンセント容量を安全に拡張するための最も費用対効果の高い方法はどれですか？

- A. PDU
- B. サージプロテクター
- C. UPS
- D. 電源タップ

正解: [A \(コメントを发表する\)](#)

A Power Distribution Unit (PDU) provides multiple power outlets in a data center or IDF (Intermediate Distribution Frame), while offering features like surge protection, load balancing, and sometimes remote monitoring, making it a cost-effective and reliable solution. The document confirms:

"PDUs (Power Distribution Units) are a cost-effective way to expand outlet capacity in a structured cabling environment like an IDF. They ensure safe power delivery to networking equipment and often include monitoring features."

質問: 111

ネットワーク管理者は、オーディオおよびビデオのブロードキャスト用にマルチキャスト ネットワークを設定する必要があります。

次のネットワークのうち、このアプリケーションに最も適したものはどれでしょうか？

- A. 172.16.0.0/24
- B. 192.168.0.0/24
- C. 224.0.0.0/24
- D. 240.0.0.0/24

正解: [C \(コメントを发表する\)](#)

* Understanding Multicast:

* Multicast IP Address Range: The multicast address range is from 224.0.0.0 to 239.255.255.255, designated for multicast traffic.

* Multicast Applications:

* Use Case: Multicast is used for one-to-many or many-to-many communication, suitable for applications like audio and video broadcasting where the same data is sent to multiple recipients simultaneously.

* Appropriate Network Selection:

* 224.0.0.0/24 Network: This range is reserved for multicast addresses, making it the appropriate choice for setting up a multicast network.

* Comparison with Other Options:

* 172.16.0.0/24: Part of the private IP address space, used for private networks, not designated for multicast.

* 192.168.0.0/24: Another private IP address range, also not for multicast.

* 240.0.0.0/24: Reserved for future use, not suitable for multicast.

References:

* CompTIA Network+ study materials on IP address ranges and multicast.

質問: 112

攻撃者がエンドポイントのhostsファイルにアクセスし、変更しました。これにより、ユーザーは会社のホームページから不正なウェブサイトへリダイレクトされます。最も可能性が高いのは次のうちどれですか？

A. DNSスプーフィング

B. フィッシング

C. VLANホッピング

D. ARPポイズニング

正解: ([正解を表示します](#))

When the hosts file is altered, local name resolution is compromised, and domain queries are redirected to malicious IP addresses. This is a form of DNS spoofing/poisoning, where false mappings trick users into visiting fraudulent websites.

B). Phishing typically uses emails or messages to trick users, not local file modification.

C). VLAN hopping is a Layer 2 attack to gain unauthorized network access, unrelated to DNS.

D). ARP poisoning manipulates ARP tables on a LAN to reroute traffic, not name resolution.

References (CompTIA Network+ N10-009):

Domain: Network Security - DNS poisoning/spoofing, host file manipulation, endpoint attacks.

質問: 113

ネットワーク管理者は、システム イベントを相関させるために SIEM システムを実装したいと考えています。ネットワーク管理者は次のプロトコルのうちどれを検証する必要がありますか？

A. NTP

B. DNS

C. LDAP

D. DHCP

正解: ([正解を表示します](#))

* Role of NTP (Network Time Protocol):

* NTP is used to synchronize the clocks of network devices to a reference time source. Accurate time synchronization is critical for correlating events and logs from different systems.

* Importance for SIEM Systems:

* Event Correlation: SIEM (Security Information and Event Management) systems collect and analyze log data from various sources. Accurate timestamps are essential for correlating events across multiple systems.

* Time Consistency: Without synchronized time, it is challenging to piece together the sequence of events during an incident, making forensic analysis difficult.

* Comparison with Other Protocols:

* DNS (Domain Name System): Translates domain names to IP addresses but is not related to time synchronization.

* LDAP (Lightweight Directory Access Protocol): Used for directory services, such as user authentication and authorization.

* DHCP (Dynamic Host Configuration Protocol): Assigns IP addresses to devices on a network but does not handle time synchronization.

* Implementation:

* Ensure that all network devices, servers, and endpoints are synchronized using NTP. This can be achieved by configuring devices to use an NTP server, which could be a local server or an external time source.

References:

* CompTIA Network+ study materials on network protocols and SIEM systems.

質問: 114

最近、携帯電話リピーターを設置した後、携帯電話の接続に問題が発生しているとユーザーから報告されています。

ユーザーからは、携帯電話のバッテリー残量が急速に減っているという報告もあります。技術者は、この問題のトラブルシューティングを行うために、まず以下のどれを確認すべきでしょうか？

A. WPS設定

B. 信号強度

C. チャンネル周波数

D. 電力予算

正解: **B** ([コメントを發表する](#))

When signal strength is poor, mobile devices constantly boost their transmission power in an attempt to maintain a stable connection. This results in dropped calls/data and rapid battery drain.

Since a repeater was installed, misalignment or misconfiguration could be degrading the signal strength.

A). WPS applies to Wi-Fi, not cellular repeaters.

C). Channel frequency might matter for interference, but signal strength is the most direct cause of the described symptoms.

D). Power budget applies to PoE and wired devices, not mobile phones.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - Wireless/cellular troubleshooting, signal strength impact, user symptoms (battery drain, poor connectivity).

質問: 115

一連のポリシーを使用して、ユーザーの ID に基づいてネットワークへのアクセスを許可または拒否する NAC のタイプは次のどれですか。

A. Standard ACL

B. MAC filtering

C. 802.1X

D. SSO

正解: ([正解を表示します](#))

802.1X is a port-based Network Access Control (NAC) method that enforces authentication before allowing access to the network. It uses a RADIUS server for identity verification and policy enforcement, ensuring only authorized users/devices gain access.

A). Standard ACL filters traffic by IP, not identity.

B). MAC filtering controls devices by hardware address but can be spoofed.

D). SSO (Single Sign-On) provides user convenience across services, not network-level access control.

References (CompTIA Network+ N10-009):

Domain: Network Security - NAC, 802.1X authentication, identity-based access.

質問: 116

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: 117

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: 118

次の VPN 構成のうち、リモート ユーザーが企業ネットワーク経由でインターネット リソースにアクセスすることを強制するものはどれですか。

- A. クライアントレス
- B. サイト間
- C. SSE
- D. フルトンネル

正解: D ([コメントを发表する](#))

A full-tunnel VPN forces a remote user's traffic-including access to public internet resources-to traverse the corporate VPN tunnel and egress from the organization's network. This is commonly

required to ensure consistent enforcement of corporate security controls such as web filtering, IDS/IPS inspection, DLP policies, logging, and access control. In Network+ terms, full-tunnel VPNing routes the user's default gateway through the VPN, meaning both internal traffic (to corporate subnets) and external traffic (to internet destinations) is sent through the encrypted tunnel. By contrast, a split-tunnel VPN (not listed) would send only corporate-bound traffic through the VPN while allowing internet traffic to go directly out the user's local ISP-reducing corporate bandwidth usage but also reducing centralized inspection and control. Clientless VPN usually refers to browser-based access to specific internal applications without a full network tunnel for all traffic. Site-to-site VPN connects entire networks to each other (e.g., branch office to HQ) rather than an individual remote user. SSE (Security Service Edge) is a cloud security framework/service model, not the classic VPN configuration described in the question. Hence, full-tunnel is the correct answer.

質問: 119

内部サーバーへの攻撃は、隔離されたゲストネットワークに起因することが判明しました。この攻撃を最もよく表すのは次のどれですか？

- A. パス上
- B. DNSポイズニング
- C. VLANホッピング
- D. ARPスプーフィング

正解: **C** ([コメントを发表する](#))

The correct answer is VLAN hopping, which is a Layer 2 attack specifically associated with bypassing network segmentation controls. According to the CompTIA Network+ N10-009 objectives, VLANs are commonly used to isolate traffic between different network segments, such as separating a guest network from internal production systems. When an attack originates from an isolated guest network and successfully reaches an internal server, it strongly indicates a failure or exploitation of VLAN boundaries.

VLAN hopping occurs when an attacker gains access to traffic on another VLAN by exploiting misconfigured switch ports or trunking protocols. Common techniques include switch spoofing, where the attacker pretends to be a switch to negotiate a trunk link, and double-tagging, where two VLAN tags are inserted to trick switches into forwarding traffic across VLANs. The other options do not best fit this scenario. An on-path (man-in-the-middle) attack requires interception between two communicating hosts but does not inherently bypass VLAN isolation. DNS poisoning manipulates name resolution, not network segmentation. ARP spoofing affects local Layer 2 address resolution within the same broadcast domain and typically cannot cross VLAN boundaries.

The Network+ objectives emphasize proper VLAN configuration, disabling unused trunk ports, and implementing port security to prevent VLAN hopping attacks. In this case, VLAN hopping most accurately explains how a guest network could access internal servers.

質問: 120

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** ([コメントを发表する](#))

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: 121

ある会社では最近、一部のユーザーのワークスペースを再配置し、複数のユーザーを以前使用していたワークスペースに移動しました。ネットワーク管理者は、移動したすべてのユーザーに接続の問題が発生しているという報告を受け取りました。最も可能性の高い理由はどれですか？

A. ポートはエラーにより無効になっています。

B. ポートのネイティブ VLAN が正しくありません。

C. ポートに MDIX の問題が発生しています。

D. ポートはトランク ポートです。

正解: ([正解を表示します](#))

The most likely cause is that the switchports were previously configured for a different VLAN than the one the users' computers are on. If the native VLAN on the port doesn't match the end device's VLAN, communication fails.

* A. Ports are error-disabled: Would result in no link at all, not common across multiple ports unless a violation occurred.

* C. MDIX issue: Auto-MDIX eliminates most crossover problems on modern switches.

* D. Ports are trunk ports: While possible, typical user devices should be on access ports, but if the port is incorrectly trunked, it can cause similar issues. However, "incorrect VLAN" is more precise here.

#Reference:

CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.

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

質問: 122

ある企業が ISP から 40Gbps のブロードバンド接続サービスを購入しています。新しいサービスを利用するには、10G スイッチで次のどれを設定するのが最も適切でしょうか。

A. 802.1Q タグ付け

B. ジャンボフレーム

C. Half duplex

D. リンクアグリゲーション

正解: ([正解を表示します](#))

Since the switch supports only 10Gbps per port, achieving 40Gbps throughput requires link aggregation (LACP), which combines multiple 10Gbps links into one logical interface for higher bandwidth.

Breakdown of Options:

A). 802.1Q tagging - VLAN tagging helps segment traffic but does not increase throughput.

B). Jumbo frames - Jumbo frames reduce overhead but do not increase bandwidth.

C). Half duplex - Half duplex restricts communication, reducing performance instead of improving it.

D). Link aggregation - Correct answer. LACP combines multiple 10Gbps links to provide a 40Gbps connection.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.2: Compare and contrast network topologies and technologies.

IEEE 802.3ad: Link Aggregation Control Protocol (LACP)

質問: 123

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: **B** ([コメントを發表する](#))

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: 124

次のどれが、ボット ネットワークの一部となる侵害されたシステムを一般的に使用しますか?

A. 邪悪な双子の攻撃

B. DDoS攻撃

C. XMLインジェクション

D. ブルートフォースパスワード攻撃

正解: ([正解を表示します](#))

A DDoS (Distributed Denial of Service) attack is often launched from botnets - networks of compromised systems (bots or zombies) under the control of an attacker. These devices flood the target with traffic to disrupt services.

A: Evil twin attack is a wireless spoofing method.

C: XML injection targets web applications.

D: Brute-force attacks repeatedly guess passwords but don't involve a botnet by default.

Reference:

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

質問: **125**

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witch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)

質問: **126**

データ センター間でインターネット経由で安全な通信リンクを構成する必要があります。データ センターはさまざまな地域にあります。ネットワーク管理者が使用するのに最適なプロトコルは次のどれですか。

- A. DCI
- B. GO
- C. VXLAN
- D. IPSec

正解: ([正解を表示します](#))

IPSec (Internet Protocol Security) is the best choice for secure communication over the internet, as it provides encryption, authentication, and data integrity. It is widely used in VPNs and site-to-site secure tunnels.

Breakdown of Options:

- A). DCI (Data Center Interconnect) - A general term for linking data centers, but it doesn't specify a secure tunneling protocol.
- B). GRE (Generic Routing Encapsulation) - Encapsulates traffic but lacks encryption, making it less secure than IPSec.
- C). VXLAN (Virtual Extensible LAN) - Used for Layer 2 network overlays, not for securing communication over the internet.
- D). IPSec - # Correct answer. Provides encryption, authentication, and integrity for data over the internet.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.5: Implement secure remote access methods.

RFC 4301: Security Architecture for the Internet Protocol

質問: **127**

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のどの機能を設定する必要がありますか？

- A. QoS
- B. STP

正解: **A** ([コメントを發表する](#))

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: 128

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: 129

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: **D** ([コメントを发表する](#))

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: 130

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: 131

ある企業がスパムメールのせいで非承認リストに追加されました。ネットワーク管理者は、ワークステーションがマルウェアに感染していることを確認しました。管理者は根本原因を特定するために、以下のどのプロセスを使用しましたか？

- A. トラフィック分析
- B. 可用性監視
- C. ベースラインメトリック
- D. ネットワーク検出

正解: **A** ([コメントを發表する](#))

Traffic analysis involves monitoring and inspecting network traffic flows to detect unusual patterns, such as a workstation sending large volumes of outbound SMTP (spam). This process enables identification of malware as the root cause.

- B). Availability monitoring checks uptime but doesn't diagnose spam traffic.
- C). Baseline metrics show normal usage but don't pinpoint infected hosts.
- D). Network discovery identifies devices, not malicious traffic flows.

References (CompTIA Network+ N10-009):

Domain: Network Security - Traffic analysis, malware detection, identifying compromised hosts.

質問: 132

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: ([正解を表示します](#))

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: 133

ある中小企業が、自社のネットワークに静的ルーティングと動的ルーティングのどちらを採用するかを検討しています。成長を続けるネットワークにおいて、動的ルーティングを使用する最も適切な理由は次のうちどれですか？

- A. 手動で入力したルートを使用する場合に比べて設定が簡単です
- B. 追加のネットワークセキュリティ制御は必要ありません
- C. 強化されたネットワーク監視と可視性を備えています
- D. ネットワークトポロジの自動変更と更新が含まれます

正解: ([正解を表示します](#))

Dynamic routing is most beneficial in a growing/changing network because it can automatically learn, adapt, and update routes as the topology changes. In Network+ (N10-009) routing objectives, dynamic routing protocols exchange routing information between routers and recalculate paths when links go down, new networks are added, or metrics change. This reduces the operational burden and the risk of human error that increases as the environment scales. With dynamic routing, adding a new subnet or branch often requires far fewer manual updates because routers propagate new route information automatically, and convergence mechanisms help restore connectivity after failures.

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

質問: 134

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** ([コメントを發表する](#))

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: 135

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. 1つ
- B. 3つ
- C. 4つ
- D. 2つ

正解: ([正解を表示します](#))

質問: 136

あるメディア企業がグローバルストリーミングサービスを導入しています。現地の法律を遵守するために、各地域の拠点(Point of Presence)に以下のどれを適用すべきでしょうか？

- A. ACL
- B. ポートセキュリティ
- C. キー管理
- D. コンテンツフィルタリング

正解: **D** ([コメントを發表する](#))

For a global streaming service, different countries and regions often have specific legal requirements about what content can be accessed (for example, age restrictions, prohibited material,

censorship rules, or licensing constraints). To comply with these local laws at each regional point of presence (PoP), the company should implement content filtering. In Network+ security objectives, content filtering is a control used to allow, block, or restrict access to specific categories of content, URLs, applications, or media based on policy. Applied regionally, it supports geo-policy enforcement by ensuring that users served by a given PoP receive only content permitted in that jurisdiction. An ACL primarily controls network traffic flows (permit/deny based on IPs, ports, and protocols). While ACLs can help block certain services, they are not designed to classify and regulate streaming media content in a way that aligns with legal content rules. Port security is a switch feature to restrict which devices can connect to a port (MAC-based controls) and is unrelated to regional compliance for streamed media. Key management concerns encryption key handling and protects confidentiality/integrity, but it does not determine which content is allowed in a region. Therefore, regional content filtering is the best match for meeting local legal requirements.

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

質問: 137

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: A ([コメントを发表する](#))

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: 138

技術者が、企業サーバーに接続できないユーザーのラップトップのトラブルシューティングを行っています。

技術者は、この問題がルーティングに関連していると考えています。技術者は、問題を特定するために次のコマンドのどれを使用する必要がありますか？

- A. tcpdump
- B. 掘る
- C. トレース
- D. アルペジオ

正解: ([正解を表示します](#))

The tracert (Traceroute) command is used to determine the path packets take from the source to the destination. It helps in identifying routing issues by showing each hop the packets pass through, along with the time taken for each hop. This command can pinpoint where the connection is failing or experiencing delays, making it an essential tool for troubleshooting routing issues. References: CompTIA Network+ study materials and common network troubleshooting commands.

質問: 139

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: 140

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

A. キャプティブポータル

B. 利用規約

C. ネットワークアクセス制御

D. DNSフィルタリング

正解: ([正解を表示します](#))

A captive portal is designed to present terms, conditions, or usage rules to users and require them to acknowledge/accept those rules before granting network or internet access. In Network+ (N10-009) security and access control concepts, captive portals are commonly associated with guest wireless or public access scenarios, where users are redirected to a web page that displays acceptable-use language and requires a click- through acceptance (and sometimes authentication). This provides a technical enforcement point: users must actively accept the rules to proceed, which supports organizational policy compliance and creates a recordable control in many implementations.

An Acceptable Use Policy (AUP) is the document that defines the rules, but by itself it does not technically force a user to acknowledge them at the time of access. NAC controls who/what can connect and can enforce posture and segmentation, but it does not inherently ensure users "accept" usage rules unless paired with a portal workflow. DNS filtering blocks or allows domain access categories (malware, adult content, etc.), which enforces browsing restrictions but does not guarantee user acceptance of rules. Therefore, the best answer to ensure users accept the rules is captive portal.

質問: 141

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: ([正解を表示します](#))

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: **142**

VoIP通話中に、ユーザーは音声の不安定さに気づき、インシデントチケットをログに記録しました。ネットワーク管理者は、RTPパケットの到着に一貫性のない遅延があることに気付きました。ネットワーク管理者は、問題を特定するために、以下のどのトラブルシューティングツールを使用すべきでしょうか？

A. トナーとプローブ

B. プロトコルアナライザー

C. ケーブルテスター

D. スペクトラムリーダー

正解: ([正解を表示します](#))

Inconsistent arrival of RTP (Real-Time Protocol) packets indicates jitter or latency variation. A protocol analyzer (packet sniffer, e.g., Wireshark) can capture and analyze RTP streams, showing delay, jitter, and packet loss statistics.

A). Toner and probe locates cable runs, not packet analysis.

C). Cable tester checks wiring faults, not packet timing.

D). Spectrum reader is for identifying wireless interference, not analyzing RTP traffic.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - Protocol analyzers, VoIP troubleshooting, jitter analysis.

質問: **143**

証券取引所のブローカーのネットワークアーキテクトが、災害復旧 (DR) のための高可用性計画を実装しています。以下のアプローチのうち、最も適したものはどれでしょうか？

A. ウォームサイト

B. アクティブ-アクティブ

C. フルメッシュ

D. インバンド

正解: ([正解を表示します](#))

The correct answer is Active-active because a stock exchange broker requires extremely high availability, minimal downtime, and near-zero data loss. According to CompTIA Network+ (N10-009) objectives under high availability and disaster recovery concepts, an active-active configuration involves multiple systems or sites operating simultaneously and sharing the workload. If one system fails, the other continues processing traffic without service interruption.

This model provides the lowest Recovery Time Objective (RTO) and Recovery Point Objective (RPO), which is critical in financial trading environments where even seconds of downtime can result in major financial loss. Active-active architectures also support load balancing, redundancy, and continuous synchronization between systems.

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

Therefore, an active-active approach is the most suitable solution for mission-critical financial operations.

質問: 144

ユーザーがウェブサイトアクセスしようとしたのですが、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: [\(正解を表示します\)](#)

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: 145

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: **C** ([コメントを發表する](#))

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: 146

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: 147

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** ([コメントを发表する](#))

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: 148

ネットワーク管理者は、ネットワーク スイッチへの暗号化ログインのために次のポートのどれを有効にする必要がありますか？

- A. 22
- B. 23
- C. 80
- D. 123

正解: [\(正解を表示します\)](#)

Port 22 is used for Secure Shell (SSH), which enables encrypted remote login and command execution on network devices.

* Port 23 = Telnet (unencrypted)

* Port 80 = HTTP

* Port 123 = NTP

From Andrew Ramdayal's guide:

"SSH uses port 22 to provide secure command-line access to devices such as switches and routers. Unlike Telnet (port 23), SSH encrypts session traffic, making it the preferred method for remote administration."

質問: 149

コネクションレス通信上のトランスポート層で発生する伝送形式を最もよく表すものはどれですか？

- A. データグラム
- B. セグメント
- C. フレーム
- D. パケット

正解: **A** ([コメントを發表する](#))

At the transport layer, connectionless communication is typically handled using the User Datagram Protocol (UDP), which transmits data in units called datagrams. Unlike TCP, UDP does not establish a connection before sending data and does not guarantee delivery, making datagrams the correct term for the transmission format in this context. References: CompTIA Network+ Exam Objectives and official study guides.

質問: 150

ネットワーク管理者が外部の悪意のある行為者によるセキュリティ リスクを理解し、どの脅威を軽減すべきかの洞察を得るのに役立つのは次のうちどれですか。

- A. コンプライアンスベンチマーク
- B. CIA三位一体
- C. SAML
- D. ハニーポット

正解: **B** ([コメントを發表する](#))

The CIA triad (Confidentiality, Integrity, Availability) is a foundational security model used in Network+ (N10-009) to evaluate risk and guide prioritization of mitigations. By categorizing assets and threats based on how they could impact confidentiality (data exposure), integrity (unauthorized alteration), or availability (service disruption), administrators can better understand which attacks from external actors matter most to the business and which controls to apply first. For example, a public-facing portal might prioritize availability protections (DDoS mitigation, redundancy), while sensitive customer records demand strong confidentiality controls (encryption, access control), and financial systems require integrity controls (logging, validation, change control). This model helps translate "threats" into business impact , which is central to deciding what to mitigate. Compliance benchmarks support meeting regulatory/industry requirements, but they don't inherently provide a conceptual lens for analyzing external attacker impact across all systems. SAML is a federation

/authentication standard, not a risk model. A honeypot can provide insight into attacker behavior, but it doesn't broadly structure risk prioritization the way CIA does. Therefore, CIA triad is the best answer.

質問: 151

邪悪な双子が達成する目的は次のどれですか？

- A. DNSポイズニング
- B. ログイン資格情報
- C. ARPスプーフィング
- D. サービス拒否

正解: ([正解を表示します](#))

An evil twin attack is when an attacker sets up a rogue access point (AP) with the same SSID as a legitimate one to trick users into connecting. Once users connect, attackers often present fake login pages or capture unencrypted session data to steal login credentials.

- A). DNS poisoning manipulates DNS resolution but is not inherent to evil twin.
- C). ARP spoofing is a Layer 2 attack involving MAC/IP mapping manipulation.
- D). Denial of service can be a side effect but is not the primary objective of evil twin attacks.

The main purpose of an evil twin is credential theft, enabling further unauthorized access to networks or systems.

References (CompTIA Network+ N10-009):

Domain: Network Security - Wireless attacks, rogue APs, evil twins.

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

質問: 152

次のプロトコルのうち、ダイクストラのリンク ステート アルゴリズムを使用してルーティング テーブル内のルートを確認するものはどれですか。

- A. OSPF
- B. EIGRP
- C. BGP
- D. RIP

正解: ([正解を表示します](#))

OSPF (Open Shortest Path First) is a link-state routing protocol that uses the Dijkstra algorithm, also known as the shortest path first (SPF) algorithm, to determine the most efficient routes.

From Andrew Ramdayal's guide:

"OSPF is a link-state routing protocol that provides fast, efficient path selection using the shortest path first (SPF) algorithm."

質問: 153

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: 154

技術者が理論を確認するために実行する必要があるトラブルシューティング方法論の次のステップはどれですか？

A. 問題が重複しています。

B. 症状を特定します。

C. 情報を収集します。

D. 変更内容を決定します。

正解: ([正解を表示します](#))

To confirm a theory in the troubleshooting process, the technician should duplicate (replicate) the problem under controlled conditions. In the Network+ (N10-009) methodology, confirming a theory means validating that the suspected cause actually produces the observed symptoms. Replicating the issue helps ensure the technician is not chasing a coincidence, and it allows changes to be tested safely (for example, reproducing the issue with a specific user account, endpoint, cable, port, SSID, or configuration). If the problem can be duplicated, the technician can then try targeted actions to see whether the symptoms change in predictable ways-strengthening or disproving the hypothesis.

The other choices occur earlier as part of forming the theory. Identify the symptoms is an initial step to define the problem clearly. Gather information is part of the discovery phase-collect logs, error messages, topology details, and user observations. Determine any changes is also an early step used to correlate recent modifications (patches, new devices, config changes) with the onset of the issue. Those steps help create a theory; duplication helps confirm it before implementing a full fix.

質問: 155

組織が ID プロバイダーを活用して SaaS アプリケーション全体のアクセスを管理できるようにするには、次のうちどれを使用しますか？

A. PKI

B. SSO

C. TACACS+

D. 半径

正解: B ([コメントを发表する](#))

SSO (Single Sign-On) allows an organization to use an identity provider (IdP) to centrally manage authentication and access across multiple SaaS applications. In the Network+ (N10-009) objectives, identity and access management concepts include federated authentication, centralized account control, and reducing password sprawl. With SSO, users authenticate once to the IdP, and the IdP then provides assertions/tokens to SaaS services (commonly using federation standards such as SAML or OIDC in real environments). This improves security (fewer reused passwords, easier MFA enforcement), streamlines user experience, and simplifies administration (provisioning/deprovisioning from one place).

PKI supports certificates and encryption/signing, but it is not the core mechanism for managing access across many SaaS apps via an IdP. TACACS+ is typically used for device administration (AAA) on network equipment, and RADIUS commonly supports network access (802.1X, VPN) AAA-both are important AAA protocols but do not describe the SaaS-wide "one login across many apps" capability. Therefore, SSO is the best answer.

質問: 156

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: ([正解を表示します](#))

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: 157

接続の問題をトラブルシューティングする際に、初級ネットワーク管理者には、まずホストの TCP/IP スタックをテストするようという明確な指示が与えられます。ネットワーク管理者は、次のコマンドのどれを実行する必要がありますか？

- A. 127.0.0.1 にping
- B. 169.254.1.1 にping
- C. 172.16.1.1 にpingする
- D. 192.168.1.1 にpingを実行

正解: ([正解を表示します](#))

The loopback address 127.0.0.1 is used to test the TCP/IP stack of the local machine. Pinging this address confirms whether the local system's networking stack is functioning correctly.

質問: 158

ネットワーク管理者は、新しく設置したスイッチがネットワークに接続できないという問題のトラブルシューティングを試みています。管理者はスイッチにログオンし、インターフェース上で衝突が発生していることを確認しました。最も可能性の高い問題は次のうちどれですか？

- A. 速度が間違っています
- B. ジャンボフレームが有効
- C. VLANが正しくありません
- D. デュプレックス不一致

正解: ([正解を表示します](#))

The most likely issue is a duplex mismatch, which is a well-documented cause of collisions and poor network performance, as outlined in the CompTIA Network+ N10-009 troubleshooting objectives. A duplex mismatch occurs when one end of a network link is configured for full duplex while the other end is operating in half duplex. In half-duplex mode, devices must take turns transmitting and receiving data, which inherently allows for collisions. When paired with a full-duplex device which expects simultaneous send and receive, collisions and retransmissions occur frequently.

The presence of collisions on a switch interface is a key diagnostic clue. Modern Ethernet switches operating correctly in full duplex should not experience collisions at all. When collisions are observed, it almost always points to a duplex configuration issue, often caused by manual speed/duplex settings on one device and auto- negotiation on the other.

A wrong speed setting may prevent link establishment entirely or cause errors, but it does not typically result in collisions. Jumbo frames can cause packet drops or fragmentation issues, not collisions. An incorrect VLAN configuration affects logical segmentation and connectivity but operates at Layer 2 and does not generate collisions.

CompTIA Network+ emphasizes duplex mismatch as a classic and frequently tested troubleshooting scenario.

Correcting it-usually by enabling auto-negotiation on both ends-restores normal, collision-free communication.

質問: 159

隣接デバイスとの通信を確立するために自律システムを設定する必要があるルーティング プロトコルは次のどれですか。

- A. OSPF
- B. EIGRP
- C. FHRP
- D. 安らかに眠ってください

正解: ([正解を表示します](#))

EIGRP (Enhanced Interior Gateway Routing Protocol) is a Cisco proprietary advanced distance-vector routing protocol. While it operates within an Autonomous System (AS), it requires the AS number to be configured for routers to recognize each other as EIGRP neighbors.

OSPF (Open Shortest Path First) uses areas and routers must be in the same area to form adjacencies, but it doesn't require AS numbers in the same way.

FHRP (First Hop Redundancy Protocol) is not a routing protocol but a group of protocols (e.g., HSRP, VRRP) to ensure high availability at the default gateway level.

RIP (Routing Information Protocol) does not use autonomous system numbers.

Reference:

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

質問: 160

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. ルーター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: 161

次のどれが法律によって施行されますか？

- A. AUP
- B. GDPR
- C. 行動規範
- D. EULA

正解: **B** ([コメントを发表する](#))

GDPR (General Data Protection Regulation) is a legal framework enforced by the European Union to protect personal data and privacy. Unlike internal organizational policies such as AUPs or codes of conduct, GDPR is a legislated regulation, and organizations must comply or face legal consequences.

Reference:Section 4.1 - Basic Network Security Concepts - "GDPR and Compliance Regulations"

質問: 162

ネットワーク管理者は、国に基づいて企業ネットワークへのリモートアクセスを制限するために、ジオフェンシングポリシーを更新したいと考えています。管理者が最も活用する可能性のあるのは次のうちどれですか？

- A. MACフィルタリング
- B. 管理距離
- C. Bluetoothビーコン信号
- D. IPアドレスブロック

正解: ([正解を表示します](#))

The correct answer is IP address blocks because geofencing policies typically rely on public IP address ranges associated with specific geographic regions or countries. According to CompTIA Network+ (N10-009) security objectives, geofencing is a security control used to restrict or allow traffic based on geographic location. This is commonly implemented on firewalls, VPN concentrators, or security gateways by referencing databases that map IP address blocks to countries or regions.

When configuring geofencing, administrators create access control rules that permit or deny traffic from specific country-based IP ranges. This method is effective for limiting remote access to approved geographic locations and reducing exposure to international threat sources.

MAC filtering (Option A) is used within local networks and does not function over the internet for geographic control. Administrative distance (Option B) is a routing concept that determines route preference and has no relation to access control policies. Bluetooth beacon signals (Option C) are used for proximity-based services and indoor positioning, not for country-level remote access restrictions.

Therefore, leveraging IP address blocks is the correct approach for implementing geofencing controls.

質問: 163

ネットワーク技術者が新しい施設のLANを設計しています。会社は300台以上のデバイスがネットワークに接続されることを想定しています。次のうち、最も効率的なサブネットマスクはどれでしょうか？

- A. 255.255.0.0
- B. 255.255.192.0
- C. 255.255.254.0
- D. 255.255.255.254

正解: **C** ([コメントを发表する](#))

The requirement is to support over 300 hosts. The subnet mask 255.255.254.0 (or /23) provides 512 addresses, 510 of which are usable - ideal for around 300 devices.

* 255.255.0.0 (/16) provides too many addresses.

* 255.255.192.0 (/18) gives 16384 addresses - overkill.

* 255.255.255.254 is invalid for host assignments (only 2 addresses, 0 usable).

From Andrew Ramdayal's guide:

"To support 300 hosts, a /23 subnet (255.255.254.0) offers 510 usable addresses - the most efficient choice without excessive overhead."

質問: 164

外部からネットワークアプライアンスに安全にアクセスする最適な方法はどれですか？

- A. RDP
- B. テルネット
- C. FTPS
- D. SSH

正解: ([正解を表示します](#))

SSH (Secure Shell) is the best and most secure method for accessing a network appliance from an external location, according to the CompTIA Network+ N10-009 objectives related to secure management protocols and network security. SSH provides encrypted remote command-line access, ensuring that authentication credentials, commands, and session data are protected from interception, eavesdropping, and man-in-the-middle attacks.

Telnet is an insecure legacy protocol that transmits all data, including usernames and passwords, in cleartext, making it unsuitable for any external or untrusted network access. RDP is primarily used for graphical remote desktop access to Windows systems and is not commonly used for managing network appliances such as routers, switches, firewalls, or load balancers.

Additionally, RDP introduces a larger attack surface if exposed externally. FTPS is a secure file transfer protocol and is designed for transferring files, not for interactive device management or configuration.

The Network+ N10-009 exam emphasizes the use of secure administrative access methods, and SSH is the industry-standard protocol for managing network infrastructure devices. It supports strong encryption, key-based authentication, and secure tunneling, making it ideal for remote administration over untrusted networks such as the internet.

質問: 165

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: 166

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: ([正解を表示します](#))

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.

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

質問: **167**

技術者は、ネットワーク上で不正なコンテンツをダウンロードしていると報告されているコンピュータを特定する必要があります。技術者は次のどれを使用する必要がありますか？

- A. 異常アラート
- B. ポートミラーリング
- C. パフォーマンス監視
- D. パケットキャプチャ

正解: ([正解を表示します](#))

Packet Capture: This method captures and inspects network traffic to identify unauthorized downloads or malicious behavior. It provides detailed insight into the data being transmitted, making it the best tool for this scenario.

Anomaly alerts (A): Alerts may indicate unusual activity but do not provide detailed traffic analysis.

Port mirroring (B): Port mirroring can redirect traffic for analysis but requires a packet capture tool for deeper inspection.

Performance monitoring (C): Focuses on system performance metrics, not detailed traffic content.

Reference: CompTIA Network+ Official Study Guide, Domain 4.3 (Network Monitoring Tools).

質問: **168**

ISP は、事前設定されたモデムと 5 つのパブリック静的 IP アドレスを企業に提供しました。インターネットにアクセスするために、企業のファイアウォールで必要なのは次のどれですか? (2 つ選択してください)。

- A. NTP サーバー
- B. デフォルトゲートウェイ
- C. モデムのIPアドレス
- D. 1つの静的IPアドレス
- E. DNS サーバー
- F. DHCPサーバー

正解: ([正解を表示します](#))

To access the internet using static IPs, the firewall (or router) must be configured correctly:

B: Default gateway: This is essential because it tells the firewall where to send outbound traffic destined for outside the local network.

D: One static IP address: The firewall must be assigned one of the static IPs to communicate over the public internet.

The other options are not essential for basic internet connectivity in this context:

A: NTP server: Useful for time synchronization but not required for internet access.

C: The modem's IP address: Irrelevant unless doing modem-level configuration.

E: DNS servers: Important for name resolution but not for basic layer 3 connectivity.

F: DHCP server: Not used when static IPs are assigned.

Reference:

CompTIA Network+ N10-009 Official Objectives: 2.2 - Compare and contrast addressing technologies.

質問: 169

組織はネットワークの可視性を向上させたいと考えています。組織の要件は次のとおりです。

- * マルチベンダー/OS監視機能
- * リアルタイム収集
- * データの相関関係

次のどれがこれらの要件を満たしていますか？

- A. SNMP
- B. SIEM
- C. Nmap
- D. Syslog

正解: ([正解を表示します](#))

A Security Information and Event Management (SIEM) system collects, correlates, and analyzes logs from multiple sources in real-time, providing enhanced visibility across multivendor environments.

Breakdown of Options:

- A). SNMP - SNMP is used for network device monitoring, but it lacks real-time correlation across multiple vendors.
- B). SIEM - Correct answer. SIEM aggregates, analyzes, and correlates logs from multiple sources, providing real-time visibility.
- C). Nmap - Nmap is a network scanning tool used for mapping hosts and detecting open ports but does not provide log correlation.
- D). Syslog - Syslog collects logs but does not correlate or analyze them in real-time.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.3: Explain network security concepts.

NIST Special Publication 800-92: Guide to Computer Security Log Management

質問: 170

ネットワークエンジニアが新しいブランチネットワークにトンネルを追加します。トンネル内のすべてのデータが暗号化されることを保証するのは次のうちどれですか？

- A. ESP
- B. SSH
- C. GRE
- D. IKE

正解: ([正解を表示します](#))

ESP (Encapsulating Security Payload) is an IPsec protocol that provides encryption, integrity, and authentication for data inside a VPN tunnel. It ensures that all tunneled traffic is encrypted.

- B). SSH secures remote terminal sessions, not site-to-site VPN tunnels.
- C). GRE (Generic Routing Encapsulation) provides encapsulation but does not encrypt data.
- D). IKE (Internet Key Exchange) negotiates keys and establishes the IPsec tunnel but does not encrypt the payload itself.

References (CompTIA Network+ N10-009):

Domain: Network Security - VPN protocols, IPsec (AH vs. ESP), encryption in transit.

質問: 171

問題が特定された後、トラブルシューティング方法論の次のステップのうち、OSI モデルの各レベルをチェックする可能性が高いのはどれですか。

- A. 理論を確立する。
- B. ソリューションを実装します。
- C. 行動計画を作成します。

D. 機能を検証します。

正解: **A** ([コメントを發表する](#))

The CompTIA troubleshooting methodology includes steps like identifying the problem, establishing a theory of probable cause, testing the theory, creating a plan of action, implementing the solution, verifying functionality, and documenting findings. Establishing a theory involves analyzing the problem and considering possible causes, often by systematically checking each level of the OSI model (Physical, Data Link, Network, etc.) to pinpoint the root cause.

Why not Implement the solution? This step involves applying the fix, not analyzing the OSI model.

Why not Create a plan of action? This step focuses on planning the solution, not diagnosing the cause.

Why not Verify functionality? This step confirms the solution worked, not analyzing the OSI model.

Reference:CompTIA Network+ N10-009 Objective 5.2: Explain the troubleshooting methodology. The CompTIA Network+ Study Guide (e.g., Chapter 13: Network Troubleshooting) details the troubleshooting steps, noting that establishing a theory often involves using the OSI model to systematically identify the cause of network issues.

質問: **172**

ネットワーク エンジニアが新しいメール サーバーへの移行を実行しました。エンジニアは MX レコードを変更し、変更が正確であることを確認し、A レコードの IP アドレス経由で新しいメール サーバーにアクセスできることを確認しました。ただし、ユーザーはメールを受信できません。問題の発生を防ぐために、エンジニアは次のどれを実行する必要がありますか。

A. MX レコードと一致するように電子メール クライアントの構成を変更します。

B. MX レコードを変更する前に TTL レコードを減らします。

C. MX レコードを変更する前に DNS ゾーン転送を実行します。

D. IP アドレスの変更を反映するために NS レコードを更新します。

正解: ([正解を表示します](#))

Understanding TTL (Time to Live):

TTL is a value in a DNS record that tells how long that record should be cached by DNS servers and clients.

A higher TTL value means that the record will be cached longer, reducing the load on the DNS server but delaying the propagation of changes.

Impact of TTL on DNS Changes:

When an MX record change is made, it may take time for the change to propagate across all DNS servers due to the TTL setting. If the TTL is high, old DNS information might still be cached, leading to email being directed to the old server.

Best Practice Before Making DNS Changes:

To ensure that changes to DNS records propagate quickly, it is recommended to reduce the TTL value to a lower value (such as 300 seconds or 5 minutes) well in advance of making the changes. This ensures that any cached records will expire quickly, and the new records will be used sooner.

Verification of DNS Changes:

After reducing the TTL and making the change to the MX record, it is important to verify the propagation using tools like dig or nslookup.

Comparison with Other Options:

Change the email client configuration to match the MX record: Email clients generally do not need to match the MX record directly; they usually connect to a specific mail server specified in their settings.

Perform a DNS zone transfer prior to the MX record change: DNS zone transfers are used to replicate DNS records between DNS servers, but they are not related to the propagation of individual record changes.

Update the NS record to reflect the IP address change: NS records specify the DNS servers for a domain and are not related to MX record changes.

References:

CompTIA Network+ study materials and DNS best practices.

質問: **173**

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: **D** ([コメントを发表する](#))

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: **174**

重要なインフラストラクチャ スイッチのサポートが終了していると判断されました。セキュリティを確保するための最適な次のステップは次のうちどれですか。

- A. 最新のパッチとバグ修正を適用します。
- B. スイッチを廃止して交換します。
- C. 現在のファームウェアに問題がないことを確認します。
- D. スイッチをネットワークから分離します。

正解: ([正解を表示します](#))

* Understanding End-of-Support:

* End-of-Support Status: When a vendor declares a device as end-of-support, it means the device will no longer receive updates, patches, or technical support. This poses a security risk as new vulnerabilities will not be addressed.

* Risks of Keeping an End-of-Support Device:

* Security Vulnerabilities: Without updates, the switch becomes susceptible to new security threats.

* Compliance Issues: Many regulatory frameworks require that critical infrastructure be maintained with supported and secure hardware.

* Best Next Step - Replacement:

* Decommission and Replace: The most secure approach is to replace the end-of-support switch with a new, supported model. This ensures the infrastructure remains secure and compliant with current standards.

* Planning and Execution: Plan for the replacement by evaluating the network's needs, selecting a suitable replacement switch, and scheduling downtime for the hardware swap.

* Comparison with Other Options:

* Apply the Latest Patches: While helpful, this does not address future vulnerabilities since no further patches will be provided.

* Ensure the Current Firmware Has No Issues: This is only a temporary measure and does not mitigate future risks.

* Isolate the Switch from the Network: Isolating the switch may disrupt network operations and is not a viable long-term solution.

References:

* CompTIA Network+ study materials on network maintenance and security best practices.

質問: **175**

次のポートのうち、安全なプロトコルはどれですか？

- A. 20
- B. 23
- C. 443
- D. 445

正解: **C** ([コメントを発表する](#))

Port 443 is used by HTTPS (Hypertext Transfer Protocol Secure), a secure version of HTTP that uses SSL

/TLS to encrypt the communication between a client and server. This ensures confidentiality and integrity of data in transit. The document states:

"Port 443 is the default port for HTTPS, which secures HTTP traffic using SSL/TLS, providing encryption and secure identification of web servers."

質問: **176**

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: **177**

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. テルネット
- C. GUI
- D. API

正解: ([正解を表示します](#))

Comprehensive and Detailed Explanation (aligned to N10-009):

APIs (Application Programming Interfaces) allow automation tools and scripts to push configurations to network devices programmatically. Modern network automation platforms rely on APIs to ensure consistency and scalability.

A). RDP is remote desktop for Windows systems, not automation.

B). Telnet is insecure and manual.

C). GUI requires manual configuration, not automation.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Automation, orchestration, APIs in network management.

質問: **178**

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: 179

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	AAAAAA1111112	-83dBm	11
Home	AAAAAA1111113	-91dBm	11
Home	AAAAAA1111114	-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: [\(正解を表示します\)](#)

*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: 180

ネットワーク管理者は、ネットワークの可視性を高めるためにデバイス監視を実装することを計画しています。ソリューションが提供するセキュリティは、認証と暗号化です。次のどれがこれ

らの要件を満たしていますか？

- A. SIEM
- B. Syslog
- C. NetFlow
- D. SNMPv3

正解: ([正解を表示します](#))

SNMPv3 (Simple Network Management Protocol version 3) provides device monitoring with authentication and encryption. This enhances network visibility and security by ensuring that monitoring data is securely transmitted and access to network devices is authenticated.

Authentication: SNMPv3 includes robust mechanisms for authenticating users accessing network devices.

Encryption: It provides encryption to protect the integrity and confidentiality of the data being transmitted.

Network Management: SNMPv3 allows for detailed monitoring and management of network devices, ensuring better control and security.

Network References:

CompTIA Network+ N10-007 Official Certification Guide: Covers SNMP versions, their features, and security enhancements in SNMPv3.

Cisco Networking Academy: Provides training on implementing and securing SNMP for network management.

Network+ Certification All-in-One Exam Guide: Explains the benefits and security features of SNMPv3 for network monitoring.

質問: 181

変更諮問委員会に意思決定に必要な情報を提供するトラブルシューティング手順は次のどれですか。

- A. 問題を特定する
- B. 考えられる原因の理論を構築する
- C. 原因を特定するために理論をテストする
- D. 行動計画を立てる

正解: ([正解を表示します](#))

When dealing with troubleshooting and change management, the plan of action outlines the steps, risks, and mitigation strategies. A change advisory board (CAB) uses this documented plan to decide whether to approve the change.

A). Identify the problem is the first step in troubleshooting, not decision-making for CAB.

B). Develop a theory is diagnostic work, not planning.

C). Test the theory confirms causes but doesn't provide actionable planning information.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Change management, troubleshooting methodology, CAB processes.

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

質問: 182

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: **183**

次のどれが Web ベースの顧客ポータルの可用性に影響しますか？

A. MACフラッディング

B. ARPスプーフィング

C. DoS

D. 不正デバイス

正解: ([正解を表示します](#))

A DoS (Denial of Service) attack directly targets availability, one of the core security goals (CIA triad) emphasized in Network+ (N10-009) security objectives. A web-based customer portal depends on reachable services (web servers, load balancers, DNS, upstream bandwidth). In a DoS, an attacker attempts to overwhelm the portal or its supporting infrastructure-consuming bandwidth, exhausting server resources, or saturating state tables-so legitimate users cannot connect or experience severe degradation. This is the most direct and common scenario where "availability" is impacted for a public web service.

MAC flooding aims to overflow a switch's CAM table and can lead to traffic being broadcast out ports, which is more commonly associated with enabling sniffing or disruption within a local switched network segment- not typically the primary attack described for a web portal's availability. ARP spoofing is a local network man-in-the-middle/redirection technique affecting integrity/confidentiality and potentially availability for local hosts, but it is not the best match for a public portal availability impact. Rogue devices can introduce risk, but the option is broad and indirect; DoS is the clearest availability-focused threat.

質問: **184**

ネットワーク管理者は、分類されたサービスとアプリケーションの優先順位付けを行うために、ネットワークトラフィックを管理しています。ネットワーク管理者は次のどのテクノロジーを使用すべきでしょうか？

A. 負荷分散

B. 生存時間

C. サービス品質

D. コンテンツ配信ネットワーク

正解: **C** ([コメントを发表する](#))

Quality of Service (QoS) is used to prioritize certain types of traffic to ensure critical applications receive the bandwidth, low latency, and low jitter they need-especially during congestion.

Network+ objectives cover QoS concepts such as classification, marking, queuing, and policing/shaping to manage how traffic is handled on interfaces and across links. If the requirement is to prioritize "classified services and applications," QoS policies can match traffic using ports, protocols, DSCP markings, VLAN tags, or application identifiers and then place that traffic into higher-priority queues or reserve bandwidth for it. Load balancing distributes traffic across multiple servers/paths but does not inherently prioritize one class of traffic over another on congested links.

TTL (time to live) is an IP header field used to prevent routing loops and is unrelated to prioritization. A CDN improves content delivery and caching for distributed users, but it is not a traffic-prioritization mechanism within an organization's network. Therefore, QoS is the correct technology for prioritizing specific services and applications.

質問: **185**

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: **186**

ネットワーク管理者は、ユーザーがネットワーク上のリソースにアクセスできないという通知を受け取ります。ネットワーク管理者は、ユーザー 3 というラベルの付いたワークステーションへの物理接続をチェックし、イーサネットが正しく接続されていることを確認します。ただし、コンピューターでもスイッチでも、ネットワーク インターフェイスのインジケータ ライトが点滅しません。次のどれが最も可能性の高い原因ですか。

- A. スイッチに失敗しました。
- B. デフォルトゲートウェイが間違っています。
- C. ポートはシャットダウンされています。
- D. VLAN の割り当てが正しくありません。

正解: **C** ([コメントを发表する](#))

When a network interface's indicator lights are not blinking on either the computer or the switch, it suggests a physical layer issue. Here is the detailed reasoning:

Ethernet Properly Connected: The Ethernet cable is correctly connected, eliminating issues related to a loose or faulty cable.

No Indicator Lights: The absence of blinking indicator lights on both the computer and the switch typically points to the port being administratively shut down.

Switch Port Shut Down: In networking, a switch port can be administratively shut down, disabling it from passing any traffic. This state is configured by network administrators and can be verified and changed using the command-line interface (CLI) of the switch.

Command to Check and Enable Port:

```
bash
```

Copy code

```
Switch> enable
```

```
Switch# configure terminal
```

```
Switch(config)# interface [interface id]
```

```
Switch(config-if)# no shutdown
```

The command no shutdown re-enables the interface if it was previously disabled. This will restore the link and the indicator lights should start blinking, showing activity.

Basic Configuration Commands PDF, sections on interface configuration (e.g., shutdown, no shutdown).

質問: 187

追加のパスワードを必要とせずにユーザーが複数のリソースに対して認証できるようにするには、次のうちどれを使用しますか？

- A. SSO
- B. MFA
- C. SAML
- D. 半径

正解: ([正解を表示します](#))

The correct answer is SSO (Single Sign-On) because it enables a user to authenticate once and gain access to multiple systems or resources without being prompted to log in again. According to CompTIA Network+ (N10-009) security objectives, SSO improves usability and productivity while maintaining centralized authentication control. After the initial authentication, a trust relationship between systems allows the user to access additional applications seamlessly.

MFA (Multi-Factor Authentication) enhances security by requiring two or more authentication factors (something you know, have, or are), but it does not inherently provide access to multiple systems without repeated authentication events.

SAML (Security Assertion Markup Language) is an authentication and authorization protocol commonly used to implement SSO in web-based environments. While SAML supports SSO functionality, it is the underlying protocol rather than the access method itself.

RADIUS is a centralized authentication, authorization, and accounting (AAA) protocol used for network access control but does not specifically provide seamless multi-resource authentication without additional logins.

Therefore, SSO best describes authentication to multiple resources without requiring additional passwords.

質問: 188

ネットワーク管理者は、大学の DHCP サーバーの問題をトラブルシューティングしています。最近、キャンパスに学生が増えたため、ユーザーは IP アドレスを取得できません。管理者は、この問題に対処するために次のどれを実行する必要がありますか？

- A. IP ヘルパーを有効にします。
- B. サブネットマスクを変更します。
- C. スコープのサイズを大きくします。
- D. アドレスの除外。

正解: ([正解を表示します](#))

The issue is that more students have arrived on campus, meaning the available IP addresses are exhausted. To fix this, the administrator should increase the DHCP scope size to allow more devices to obtain IP addresses.

Breakdown of Options:

A: Enable IP helper - IP helper is used to forward DHCP requests across different subnets. However, the problem here is that the DHCP scope is full, not that requests are not reaching the server.

B: Change the subnet mask - The subnet mask determines the number of available hosts, but changing it without increasing the IP pool does not help.

C: Increase the scope size - Correct answer. Expanding the DHCP scope provides more IP addresses for assignment.

D: Add address exclusions - Exclusions reserve IP addresses, which would further reduce available addresses instead of solving the issue.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 2.4: Compare and contrast IP addressing schemes.

RFC 2131: Dynamic Host Configuration Protocol (DHCP)

質問: 189

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: C ([コメントを發表する](#))

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: 190

復旧戦略の一環として、ネットワーク管理者はデータ 損失が8時間を超えないようにする必要があります。次のDR指標のうち、この要件を説明するものはどれですか？

- A. RPO
- B. 平均所要時間
- C. RTO
- D. MTBF

正解: ([正解を表示します](#))

Recovery Point Objective (RPO) defines the maximum acceptable amount of data loss measured in time. If leadership states "no more than eight hours of data loss," they are describing how far back the organization is willing to roll data after an outage or disaster-meaning backups, replication, snapshots, or journaling must ensure recoverable data is no older than eight hours. In Network+ terms, this is a core availability and resiliency planning concept: you choose an RPO based on business impact, then implement backup frequency /replication strategy to meet it. By contrast, Recovery Time Objective (RTO) is about how quickly services must be restored (downtime duration), not how much data can be lost. MTTR (Mean Time to Repair/Recover) is an operational reliability metric describing typical time to restore a system, and MTBF (Mean Time Between Failures) indicates expected time between failures- neither directly states acceptable data loss.

Therefore, the metric matching "eight hours of data loss" is RPO.

質問: 191

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: A ([コメントを發表する](#))

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: **192**

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

A. ホットサイト

B. DCI

C. 直接接続

D. 能動的・受動的アプローチ

正解: **A** ([コメントを发表する](#))

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

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

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

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

Reference:

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

質問: **193**

ネットワーク管理者は、次の要件を満たすデバイス監視の方法を開発しています。

*ユーザーによる明示的な権限管理が可能

*変更の集中ログが含まれます

*広範囲にアクセスできるリモート管理を提供

*サービスアカウントのサポートを提供します

次のどれがこれらの要件を最も満たすでしょうか？

A. SNMP

B. API

C. SIEM

D. SSO

正解: ([正解を表示します](#))

*API (Application Programming Interface) enables secure and granular access control, remote management, and logging, making it ideal for network monitoring.

*SNMP (A) is mainly used for device monitoring but lacks centralized logging and user-based privilege control.

*SIEM (C) is a security monitoring tool focused on log collection, not device management.

*SSO (D) is related to authentication, not monitoring.

#Reference: CompTIA Network+ N10-009 Official Documentation - Network Monitoring & Management Technologies.

質問: **194**

次のどれが、リモート ボックスへの軽量かつプライベートな接続を提供できるでしょうか？

- A. サイト間VPN
- B. テルネット
- C. コンソール
- D. セキュアシェル

正解: ([正解を表示します](#))

Secure Shell (SSH) is a protocol used to securely access remote devices over an unsecured network. It provides encrypted command-line access and is a lightweight and secure method of remote administration.

- A). Site-to-site VPN connects entire networks, not just a single host.
- B). Telnet is not secure; it transmits data (including credentials) in plaintext.
- C). Console access is direct via serial cable, not remote.

Reference:

CompTIA Network+ N10-009 Official Objectives: 2.6 - Configure and troubleshoot remote access.

質問: **195**

次のネットワーク ケーブルのうち、保護被覆で光を反射するものはどれですか。

- A. ツインアクシャル
- 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](#))

Comprehensive and Detailed Explanation (aligned to N10-009):

Multimode fiber uses multiple paths (modes) of light that bounce off the cladding to travel through the fiber.

This is effective for shorter distances but more prone to dispersion.

- A). Twinaxial is copper, not fiber.
- B). Coaxial carries electrical signals, not light.
- C). Single-mode fiber uses a single light path directly through the core without bouncing.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Fiber optics: single-mode vs. multimode.

質問: **196**

あるユーザーから、社内ネットワークへの接続が断続的に途切れるという問題が発生していると報告がありました。このユーザーのネットワーク構成は以下のとおりです。

IPアドレス: 192.168.1.10

サブネットマスク: 255.255.255.0

デフォルトゲートウェイ: 192.168.1.254

ネットワーク スイッチには次の ARP テーブルが表示されます。

MAC address	IP address	Interface	VLAN
0c00.1134.0001	192.168.1.10	eth4	10
0c00.1983.210a	192.168.2.13	eth5	11
0c00.1298.d239	192.168.1.10	eth6	10
0c00.a291.c113	192.168.2.12	eth7	11
0c00.923b.2391	192.168.1.11	eth8	10
feff.2391.1022	192.168.1.254	eth1	10

ユーザーの接続問題の原因として最も考えられるのは次のどれですか？

- A. 間違ったVLANが割り当てられたポート
- B. スパニングツリー競合のあるスイッチ
- C. 手動でIPアドレスが設定された別のPC
- D. 重複するルートテーブルを持つルータ

正解: C ([コメントを发表する](#))

This scenario describes a duplicate IP address. The ARP table shows two different MAC addresses (0c00.

1134.0001 and 0c00.1298.d239) associated with the same IP address (192.168.1.10), which leads to ARP table conflicts and intermittent connectivity.

From Andrew Ramdayal's guide:

"Duplicate IP addresses occur when two devices on the same network are assigned the same IP address, causing network conflicts. Common issues include manual configuration errors or DHCP lease issues.

Resolution includes using IP management tools and avoiding overlaps in DHCP and static IP assignments."

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

質問: 197

ネットワーク管理者は、以前はローカルネットワーク上に存在していたが、現在はSaaSソリューションとしてホストされているネットワークリソースをリダイレクトする方法を作成する必要があります。このタスクを実行するには、次のどのレコードを使用する必要がありますか？

- A. TXT
- B. AAA
- C. PTR
- D. CNAME

正解: ([正解を表示します](#))

To redirect a network resource that has moved from a local network to a Software-as-a-Service (SaaS) solution, the network administrator needs to configure a DNS record that maps an alias to the new canonical name (hostname) of the SaaS provider's server. The CNAME (Canonical Name) record is used to alias one domain name to another, effectively redirecting requests to the new hostname without needing to update the IP address directly. This is ideal for SaaS solutions, where the provider's server hostname is used, and the IP address may change dynamically.

Why not TXT? A TXT record is used to store arbitrary text data, such as SPF records for email authentication or verification strings, not for redirecting resources.

Why not AAA? There is no such thing as an "AAA" record in DNS. This might be a typo for AAAA (IPv6 address record), but AAAA maps a hostname to an IPv6 address, not an alias.

Why not PTR? A PTR record is used for reverse DNS lookups (mapping an IP address to a hostname), not for redirecting a resource to a new hostname.

Reference:CompTIA Network+ N10-009 Objective 1.5: Compare and contrast common network services and ports. The CNAME record is discussed under DNS configuration in the CompTIA Network+ Certification Study Guide (e.g., Mike Meyers' CompTIA Network+ Guide, Chapter 7: TCP/IP Applications). The guide explains that CNAME records are used to create aliases for hostnames, particularly useful for redirecting services to external providers like SaaS solutions.

質問: 198

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: 199

ユーザーのデスクにはワークステーションと IP 電話があります。ユーザーはワークステーションでインターネットを閲覧できませんが、電話は機能します。次のどの構成が必要ですか？

- A. 音声VLAN
- ~~B. ネイティブVLAN~~
- ~~C. データVLAN~~
- D. トランクポート

正解: **C** ([コメントを發表する](#))

If the IP phone works but the workstation doesn't, it indicates that the Voice VLAN is functioning correctly, but the Data VLAN (C) is either misconfigured or missing. The workstation typically connects through the phone, which tags voice and data traffic separately using VLANs.

A: Voice VLAN is for the IP phone, which is already working.

B: Native VLAN is for untagged traffic on trunk ports, but doesn't control access directly.

D: Trunk port is more relevant to switch interconnections than individual workstation ports.

Reference:

CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.

質問: 200

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: **A** ([コメントを發表する](#))

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 $2^{(\text{host bits})} \# 2$ (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: 201

ある企業が IPv6 アドレスのみを利用した新しいネットワークを実装し、インターネットに接続する必要があります。
内部ネットワークがインターネット上のサーバーに接続するためには、次のうちどれを有効にする必要がありますか？

- A. MPLS
- B. NAT64
- C. GRE
- D. 静的ルーティング

正解: ([正解を表示します](#))

The correct answer is NAT64, which is required when an IPv6-only internal network needs to communicate with IPv4-based servers on the internet. According to the CompTIA Network+ N10-009 objectives, NAT64 is a translation technology that enables interoperability between IPv6 clients and IPv4 resources during the ongoing transition from IPv4 to IPv6.

Although IPv6 is widely deployed, a significant portion of internet services still operate exclusively on IPv4.

An IPv6-only host cannot natively communicate with an IPv4 server because the protocols use different addressing formats. NAT64 solves this problem by translating IPv6 packets into IPv4 packets and translating the responses back into IPv6, allowing seamless communication without requiring dual-stack configuration on internal hosts.

The other options do not address this requirement. MPLS is a WAN forwarding technology used by service providers and does not provide protocol translation. GRE is a tunneling protocol used to encapsulate traffic and does not enable IPv6-to-IPv4 communication. Static routing determines packet paths but does not resolve protocol incompatibility between IPv4 and IPv6.

The Network+ N10-009 exam places strong emphasis on IPv6 transition mechanisms, including NAT64, DNS64, and dual stack. In this scenario, NAT64 is the essential component that enables IPv6-only networks to access legacy IPv4 internet services.

質問: 202

次の OSI モデル層のうち、HTTP 情報の交換を管理するのはどれですか？

- A. セッション
- B. データリンク
- C. ネットワーク
- D. アプリケーション

正解: **D** ([コメントを发表する](#))

HTTP is an application-layer protocol, so the OSI layer that manages the exchange of HTTP information is Layer 7 (Application). In the Network+ (N10-009) objectives, the OSI model is used to map common protocols to the layers where they operate. HTTP defines how web clients and servers format and exchange requests and responses (methods like GET/POST, headers, status codes, and message bodies). Those behaviors are part of the application services provided to end-user software such as web browsers, APIs, and web servers.

While HTTP relies on lower layers to function (for example, TCP at the Transport layer for reliable delivery and IP at the Network layer for addressing and routing), the protocol logic and meaning of the web transactions exist at the Application layer. The distractors do not fit: the Network layer handles IP routing, the Data Link layer handles frames and MAC addressing on local links, and the Session layer is associated with session establishment/management concepts but is not where HTTP is categorized for Network+ mapping. Therefore, Application is the correct answer.

質問: 203

技術者は、デフォルト構成で新しい SD-WAN デバイスを実装しています。技術者は電子メールで URL を受け取り、新しいデバイスをインターネットに接続してインストールを完了します。
これは次のどれの例ですか？

- A. SASEデバイスのインストール
- B. ゼロタッチプロビジョニング
- C. コードとしてのインフラストラクチャ
- D. 構成管理

正解: ([正解を表示します](#))

This process describes Zero-touch provisioning (ZTP), where a device automatically pulls its configuration from a cloud controller or URL once connected to the internet. It's common in SD-WAN and modern network appliances.

A: SASE (Secure Access Service Edge) refers to cloud-delivered network security, not a provisioning method.

C: Infrastructure as code automates infrastructure deployment using code, but this scenario specifically fits ZTP.

D: Configuration management tracks and maintains system configurations but doesn't describe the installation process.

Reference:

CompTIA Network+ N10-009 Official Objectives: 4.3 - Explain remote access methods and automation.

質問: 204

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: 205

次のトラブルシューティング手順のうち、変更諮問委員会に意思決定に必要な情報を提供するものはどれですか？

- A. 問題を特定します。
- B. 考えられる原因の理論を構築します。
- C. 原因を特定するために理論をテストします。
- D. 行動計画を立てます。

正解: ([正解を表示します](#))

A Change Advisory Board (CAB) reviews and approves network changes. Before approval, they need a detailed action plan outlining the change, potential impacts, and mitigation strategies.

* A Plan of Action includes risk assessments, rollback procedures, and deployment steps, which are critical for decision-making.

? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Network Troubleshooting Methodologies

質問: 206

ある研究施設では、近い将来に世界的なネットワーク トラフィックが急増すると予想しています。オフィスには ISP からの 2.5Gbps ファイバー接続が装備されていますが、施設では現在 1Gbps 接続しか利用していません。ISP の接続速度を使用するには、次のどれを設定する必要がありますか。

- A. 802.1Q タグ付け
- B. ネットワークアドレス変換
- C. ポートデュプレックス
- D. リンクアグリゲーション

正解: ([正解を表示します](#))

Understanding Link Aggregation:

Definition: Link aggregation combines multiple network connections into a single logical link to increase bandwidth and provide redundancy.

Usage in High-Bandwidth Scenarios:

Combining Links: By aggregating multiple 1Gbps connections, the facility can utilize the full 2.5Gbps bandwidth provided by the ISP.

Benefits: Enhanced throughput, load balancing, and redundancy, ensuring better utilization of available bandwidth.

Comparison with Other Options:

802.1Q Tagging: Used for VLAN tagging, which does not affect the physical bandwidth utilization.

Network Address Translation (NAT): Used for IP address translation, not related to link speed or bandwidth aggregation.

Port Duplex: Refers to the mode of communication (full or half duplex) on a port, not the aggregation of bandwidth.

Implementation:

Configure link aggregation (often referred to as LACP - Link Aggregation Control Protocol) on network devices to combine multiple physical links into one logical link.

References:

CompTIA Network+ study materials on network configuration and link aggregation.

質問: 207

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

- A. SSID
- B. RSSI
- C. チャンネル番号
- D. BSSID

正解: ([正解を表示します](#))

To locate a specific access point (AP) , the most reliable identifier to view is the BSSID . In 802.11 networks, the BSSID is the radio interface identifier for the AP (typically the AP radio's MAC address).

Unlike an SSID, which can be shared across many APs in the same wireless network (especially in an enterprise deployment using the same SSID across multiple APs), the BSSID uniquely distinguishes one AP radio from another. This is critical during an 802.11ax (Wi-Fi 6) migration , where multiple APs may broadcast identical SSIDs and operate on the same channels in different areas.

While RSSI is useful for physically walking toward the strongest signal (a technique used in locating RF sources), RSSI alone does not confirm you are tracking the correct AP-only that you are near an RF transmitter. Channel number also does not uniquely identify the AP because multiple APs can share the same channel (and channels may overlap depending on band and width).

SSID similarly is not unique.

Therefore, viewing the BSSID on the analyzer (or Wi-Fi analyzer mode) allows the administrator to confirm the exact AP being measured and located.

質問: 208

リモート ユーザー向けの従来の VPN の代わりとして最もよく使用されるのは次のどれですか。

A. SD-WAN

B. SASE

C. サイト間VPN

D. リバースプロキシ

正解: **B** ([コメントを发表する](#))

A modern replacement for traditional remote-access VPN for users is SASE (Secure Access Service Edge) .

Network+ highlights trends in remote connectivity and security where organizations move away from backhauling all user traffic through a VPN concentrator and instead use cloud-delivered security and access controls closer to the user. SASE combines networking and security capabilities-commonly including ZTNA (Zero Trust Network Access) , secure web gateway (SWG), CASB, firewall-as-a-service (FWaaS), and centralized policy enforcement-so remote users can securely access applications without relying on a classic "connect to the corporate network first" VPN model.

SD-WAN primarily optimizes connectivity between sites and to cloud services, often for branch networks; it' s not typically the direct replacement for remote user VPN access. Site-to-site VPN connects networks (locations) and is not intended for individual remote users. A reverse proxy can publish specific internal web applications externally and provide some security functions, but it does not replace VPN broadly for remote user access to multiple internal resources the way SASE/Zero Trust access solutions do. Therefore, SASE is the best answer as the likely replacement for traditional remote-access VPN.

質問: 209

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** ([コメントを发表する](#))

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: 210

ある会社から、ファックスを送信しようとしても、ファックス機から発信音が聞こえなくなったという報告がありました。電話ケーブルの片側が損傷しています。技術者が交換すべきコネクタは次のうちどれですか。

A. F-type

B. RJ45

C. SC

D. RJ11

正解: ([正解を表示します](#))

Fax machines use analog phone lines, which are connected using RJ11 connectors. These are standard telephone connectors with 4 or 6 positions and are used for POTS (Plain Old Telephone Service) lines.

F-type is used for coaxial cables (e.g., TV and cable modems).

RJ45 is used for Ethernet network connections.

SC (Subscriber Connector) is used for fiber optic connections, not analog telephone lines.

Reference:

CompTIA Network+ N10-009 Official Objectives: 2.4 - Compare and contrast common network connectors.

質問: **211**

ネットワーク管理者は、192.168.1.0/24 を 2 つの均等な部分に分割する必要があります。管理者は次のどのサブネット マスクを使用する必要がありますか？

A. 255.255.0.0

B. 255.255.254.0

C. 255.255.255.0

D. 255.255.255.128

正解: **D** ([コメントを發表する](#))

* Understanding Subnetting:

* Original Network: 192.168.1.0/24 has a subnet mask of 255.255.255.0, which allows for 256 IP addresses (including network and broadcast addresses).

* Objective: Divide this network into two equal subnets.

* Calculating Subnet Mask:

* New Subnet Mask: To divide 192.168.1.0/24 into two equal halves, we need to borrow one bit from the host portion of the address, changing the subnet mask to 255.255.255.128 (/25).

* Subnet Breakdown:

* First Subnet: 192.168.1.0/25 (192.168.1.0 - 192.168.1.127)

* Second Subnet: 192.168.1.128/25 (192.168.1.128 - 192.168.1.255)

* Verification:

* Each subnet now has 128 IP addresses (126 usable IP addresses, excluding the network and broadcast addresses).

* Comparison with Other Options:

* 255.255.0.0 (/16): Provides a much larger network, not dividing the original /24 network.

* 255.255.254.0 (/23): Also creates a larger subnet, encompassing more than the original /24 network.

* 255.255.255.0 (/24): Maintains the original subnet size, not dividing it.

References:

* CompTIA Network+ study materials on subnetting and IP addressing.

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

質問: **212**

根本原因理論のテストに成功した後に実行する次のステップはどれですか？

A. 解決手順を決定します。

- B. ラボで問題を再現します。
- C. 承認のために理論を提示します。
- D. 問題に対する解決策を実装します。

正解: ([正解を表示します](#))

* Troubleshooting Methodology:

* Confirming the Root Cause: After testing and confirming the theory, the next logical step is to address the issue by implementing a solution.

* Implementation of the Solution:

* Resolve the Issue: Implement the identified solution to rectify the problem. This step involves making necessary changes to the network configuration, replacing faulty hardware, or applying software patches.

* Documentation: Document the solution and the steps taken to resolve the issue to provide a reference for future troubleshooting.

* Comparison with Other Steps:

* Determine Resolution Steps: This is part of the implementation process where specific actions are outlined, but the actual next step after testing is to implement those steps.

* Duplicate the Problem in a Lab: This step is typically done earlier in the troubleshooting process to understand the problem, not after confirming the root cause.

* Present the Theory for Approval: In some scenarios, presenting the theory might be necessary for major changes, but generally, once the root cause is confirmed, the solution should be implemented.

* Final Verification:

* After implementing the solution, it is important to verify that the issue is resolved and that normal operations are restored. This may involve monitoring the network and testing to ensure no further issues arise.

References:

* CompTIA Network+ study materials on troubleshooting methodologies and best practices.

質問: 213

ネットワーク管理者は各部門にセキュリティ ゾーンを実装しています。このタスクを実行するために管理者は次のどれを使用する必要がありますか？

- A. ACL
- B. ポートセキュリティ
- C. コンテンツフィルタリング
- D. NAC

正解: A ([コメントを発表する](#))

* Understanding ACLs:

* Access Control Lists (ACLs): A set of rules used to control network traffic and restrict access to network resources by filtering packets based on IP addresses, protocols, or ports.

* Implementing Security Zones:

* Defining Zones: ACLs can be used to create security zones by applying specific rules to different departments, ensuring that only authorized traffic is allowed between these zones.

* Control Traffic: ACLs control inbound and outbound traffic at network boundaries, enforcing security policies and preventing unauthorized access.

* Comparison with Other Options:

* Port Security: Limits the number of devices that can connect to a switch port, preventing MAC address flooding attacks, but not used for defining security zones.

* Content Filtering: Blocks or allows access to specific content based on predefined policies, typically used for web filtering rather than network segmentation.

* NAC (Network Access Control): Controls access to the network based on the security posture of devices but does not define security zones.

* Implementation Steps:

* Define ACL rules based on the requirements of each department.

* Apply these rules to the appropriate network interfaces or firewall policies to segment the network into security zones.

References:

* CompTIA Network+ study materials on network security and access control methods.

質問: 214

ネットワークエンジニアは、無線カバレッジを改善するためにAPを追加しました。しかし、ユーザーから接続が切断と再接続を繰り返すという報告が寄せられています。この問題の原因は次のどれでしょうか？

- A. スループット容量
- B. ローミングの設定ミス
- C. チャンネルの重複
- D. パケット損失

正解: ([正解を表示します](#))

Adding more access points can improve coverage, but it also increases the risk of co-channel interference if APs are configured on the same or overlapping channels. Channel overlap causes contention and interference, leading to retries, unstable performance, and symptoms that feel like frequent disconnect

/reconnect events-especially in dense deployments. Network+ (N10-009) wireless troubleshooting objectives highlight proper channel planning (non-overlapping channels, appropriate channel width) as critical when increasing AP density. If adjacent APs are competing on the same channel (or overlapping channels in

2.4 GHz), clients may experience poor signal-to-noise ratios and repeated reassociations as they struggle to maintain a stable link.

Roaming misconfiguration can cause sticky clients or poor handoffs, but the classic problem introduced immediately after "adding more APs" is interference from bad channel design.

Throughput capacity is about available bandwidth and airtime efficiency; it can make things slow, but it doesn't inherently cause repeated disconnect/reconnect loops like interference does.

Packet loss is a symptom that may occur due to interference, but the root cause in the options that best fits the scenario is channel overlap .

質問: 215

ハッシュが提供するものは次のどれですか？

- A. 否認防止
- B. 誠実さ
- C. 機密性
- D. 可用性

正解: B ([コメントを發表する](#))

The correct answer is Integrity because a hashing algorithm ensures that data has not been altered. According to CompTIA Network+ (N10-009) security objectives, hashing is a cryptographic process that takes input data of any size and produces a fixed-length output known as a hash value or digest. If even a single bit of the original data changes, the resulting hash value will be significantly different.

Hashing is commonly used to verify file integrity, validate message authenticity, and securely store passwords. For example, when downloading software, the vendor may publish a hash value so users can calculate the hash of the downloaded file and confirm it matches, ensuring the file was not tampered with.

Non-repudiation (Option A) typically requires digital signatures that combine hashing with asymmetric encryption to verify the sender's identity. Confidentiality (Option C) is achieved through encryption, which protects data from unauthorized access. Availability (Option D) refers to ensuring systems and data are accessible when needed and is not related to hashing functions.

Therefore, hashing primarily provides data integrity verification.

質問: 216

ネットワーク エンジニアは、拡張と冗長性のために新しいスイッチを設定し、既存のスイッチに接続します。ユーザーはすぐにネットワークへの接続を失います。ネットワーク エンジニアは、両方のスイッチから次のスパニング ツリー情報を記録します。

スイッチ1

港湾費用

1 前進 2

2 前進 2

スイッチ2

港湾費用

1 前進 2

2 前進 2

次のどれが問題を最もよく表していますか？

- A. ポートコストは等しくありません。
- B. ポートはリンク アグリゲーションを使用する必要があります。
- C. ルートブリッジを識別する必要があります。
- D. スイッチは RSTP 用に設定する必要があります。

正解: **C** ([コメントを发表する](#))

The issue is that no root bridge has been identified. In STP, a root bridge is necessary to manage redundant paths and avoid loops in the network. Without a root bridge, all switches will assume they can forward traffic, causing a network loop and connectivity problems.

質問: **217**

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](#))

An 802.11ac wireless bridge is the most practical solution to connect two nearby buildings without trenching or laying physical cable. It provides high-speed, point-to-point connectivity using directional antennas.

- * A. Multimode fiber is effective but expensive and typically limited to 500 meters or less.
- * C. Cat 6 copper is only rated for up to 100 meters - not viable for a street-wide distance.
- * D. Loopback adapter is 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: **218**

ユーザーからネットワークのパフォーマンスに関する問題が報告されます。ネットワーク管理者はブロードキャストストームが発生していることに気付きます。

この問題を軽減するために管理者が設定する必要があるプロトコルは次のどれですか？

- A. スパニングツリー
- B. 拡張内部ゲートウェイルーティングプロトコル (EIGRP)
- C. シスコ検出プロトコル (CDP)
- D. リンク層検出プロトコル (LLDP)
- E. ボーダーゲートウェイプロトコル (BGP)

正解: ([正解を表示します](#))

The correct answer is Spanning Tree because broadcast storms are typically caused by Layer 2 switching loops in Ethernet networks. According to the CompTIA Network+ (N10-009) objectives under switching concepts, the Spanning Tree Protocol (STP) is specifically designed to prevent loops in networks that have redundant switch connections.

In a Layer 2 environment, switches forward broadcast frames out all ports except the one on which they were received. If redundant paths exist without STP, frames can circulate indefinitely, creating a broadcast storm.

This results in excessive traffic, high CPU utilization on switches, MAC address table instability, and significant network performance degradation.

STP prevents this by logically blocking redundant paths while maintaining them as backups. If the active path fails, STP recalculates and activates a previously blocked path, preserving redundancy without loops.

The other options-EIGRP and BGP (routing protocols) and CDP and LLDP (device discovery protocols)- do not prevent Layer 2 loops.

Therefore, configuring Spanning Tree Protocol is the appropriate solution to mitigate broadcast storms.

質問: 219

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 ([コメントを發表する](#))

The most probable issue is with the transceiver 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: 220

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: 221

コストを削減し、モビリティを向上させるために、最高技術責任者 (CTO) は、組織とその関連会社にクラウド サービスを導入したいと考えています。ユーザーへの影響を軽減するために、CTO は主要なサービスをオンサイト データ センターから実行し、エンタープライズ サービスをクラウドで実行したいと考えています。次の展開モデルのうち、組織に最適なものはどれですか。

- A. パブリック
- B. ハイブリッド

C. SaaS

D. プライベート

正解: **B** ([コメントを發表する](#))

A hybrid cloud deployment model is the best choice for the CTO's requirements. It allows the organization to run key services from the on-site data center while leveraging the cloud for enterprise services. This approach provides flexibility, scalability, and cost savings, while also minimizing disruptions to users by keeping critical services local. The hybrid model integrates both private and public cloud environments, offering the benefits of both. References: CompTIA Network+ study materials and cloud computing principles.

質問: **222**

ネットワーク管理者は、組織のネットワークを外部の脅威から保護するためにファイアウォールを設定しています。

ファイアウォールを構成する際に管理者が最初に考慮すべき事項は次のどれですか？

A. 必要なポート、プロトコル、およびサービス

B. すべて拒否ルールの組み込み

C. VPNアクセス

D. 顧客向けサーバーからの発信アクセス

正解: ([正解を表示します](#))

When configuring a firewall, the first step is identifying which ports, protocols, and services are required for normal business operations. This ensures only legitimate traffic is allowed. After establishing the required rules, a default deny rule is added for security.

B). Deny all rule is important, but it should come after defining required rules.

C). VPN access is a service to configure, but only after determining baseline needs.

D). Outbound traffic policies are part of refinement, not the first consideration.

References (CompTIA Network+ N10-009):

Domain: Network Security - Firewall configuration, rule order, least privilege.

質問: **223**

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. 問題を特定する

B. ソリューションを実装する

C. 理論をテストする

D. 行動計画を作成する

正解: ([正解を表示します](#))

質問: **224**

ネットワーク技術者は、新しく入居したオフィスのアクセス スイッチに UTP パッチ パネルからパッチ コードを取り付ける必要があります。パッチ パネルには、ジャックを簡単に識別できるようにラベルが付いていません。

適切なパッチ パネル ポートを識別する最も簡単な方法を提供するツールは次のどれですか。

A. トナー

B. ラップトップ

C. ケーブルテスター

D. 視覚的障害検出装置

正解: ([正解を表示します](#))

A toner probe, often referred to as a toner and probe kit, is the easiest and most effective tool for identifying individual cables in a bundle, especially in situations where the patch panel is not labeled. The toner sends an audible tone through the cable, and the probe detects the tone at the other end, allowing the technician to quickly identify the correct cable.

- * **Functionality:** The toner generates a tone that travels along the cable. When the probe is placed near the correct cable, it detects the tone and emits a sound.

- * **Ease of Use:** Toner probes are straightforward to use, even in environments with many cables, making them ideal for identifying cables in unlabeled patch panels.

- * **Efficiency:** This method is much faster and more reliable than manual tracing, especially in complex setups.

Network References:

- * **CompTIA Network+ N10-007 Official Certification Guide:** Details tools used for cable identification and troubleshooting.

- * **Cisco Networking Academy:** Provides training on using toner probes and other cable testing tools.

- * **Network+ Certification All-in-One Exam Guide:** Explains the use of different tools for network cable identification and management.

質問: **225**

顧客が最近新しいオフィスに移転したのですが、一部の壁プレートが機能しておらず、ラベルも適切に貼られていないことに気付きました。IDF 内の適切な配線を識別するには、次のツールのうちどれが最適ですか？

A. トナーとプローブ

B. ケーブルテスター

C. 視覚的障害ロケター

D. ネットワークタップ

正解: ([正解を表示します](#))

A toner and probe tool, also known as a tone generator and probe, is used to trace and identify individual cables within a bundle or to locate the termination points of cables in wiring closets and patch panels. It generates a tone that can be picked up by the probe, helping technicians quickly and accurately identify and label wall plates and wiring. This is the best tool for identifying proper wiring in the Intermediate Distribution Frame (IDF). References: CompTIA Network+ Exam Objectives and official study guides.

質問: **226**

ネットワーク技術者が複数のVLANを備えたスイッチを実装します。クライアントが他のVLANのクライアントと通信できるようにするには、技術者は次のうちどれを設定する必要がありますか？

A. VPC

B. VXLAN

C. ACL

D. SVI

正解: ([正解を表示します](#))

To enable communication between VLANs , the technician must configure inter-VLAN routing . On a Layer 3 switch, this is commonly done by creating an SVI (Switched Virtual Interface) for each VLAN. An SVI provides a virtual Layer 3 interface with an IP address that acts as the default gateway for hosts in that VLAN. Once SVIs exist and routing is enabled, the switch can route traffic between VLAN subnets internally, allowing clients in different VLANs to communicate (subject to any security controls). This aligns with Network+ (N10-009) infrastructure objectives covering VLANs, Layer 2/Layer 3 switching, and the requirement for routing to cross broadcast domains.

ACLs can permit or deny inter-VLAN traffic, but they do not create the routing function by themselves.

VXLAN is an overlay tunneling technology used mainly in data centers to extend Layer 2 networks over Layer 3 fabrics, not the standard solution for basic VLAN-to-VLAN connectivity on a switch. VPC is not the required configuration element for inter-VLAN routing in this context. Therefore, configuring SVIs is the correct and most direct answer.

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

質問: **227**

通常、ユーザーは RDP を使用して、ホスト名 TS19 (10.0.100.19 を指す) を持つターミナル サーバーに接続します。

しかし、最近、ユーザーがTS19に接続できなくなっています。技術者が10.0.100.19にpingを打つと、到達不能エラーが発生します。最も可能性の高い原因は次のどれですか？

- A. ユーザーは間違ったサブネット上にいます。
- B. DHCP サーバーがリースを更新しました。
- C. IP アドレスは予約されていません。
- D. ホスト名が変更されました。

正解: ([正解を表示します](#))

If a ping to 10.0.100.19 is unreachable, the most likely issue is that users are on the wrong subnet and cannot communicate with the server.

Breakdown of Options:

- A). The users are on the wrong subnet. # Correct answer. If users are on a different subnet without proper routing, they won ' t reach the server.
- B). The DHCP server renewed the lease. - Would change the client's IP, but the server's static IP should remain unchanged.
- C). The IP address was not reserved. - DHCP reservations matter for dynamic IPs, but RDP servers typically have static IPs.
- D). The hostname was changed. - Would affect DNS resolution, but pinging the IP directly would still work.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 2.4: Explain subnetting concepts.

質問: **228**

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** ([コメントを發表する](#))

Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

質問: **229**

新しい無線アクセスポイントを設置した後、エンジニアがデバイスをテストしたところ、定格速度で動作していないことがわかりました。エンジニアは、この問題をトラブルシューティングするために、次のうちどれを行うべきでしょうか？ 2つ選択してください。）

- A. ネットワーク上の他のデバイスがボトルネックになっていないことを確認します。
- B. デバイスの最新のファームウェアをインストールします。
- C. アクセス ポイントの新しい VLAN を作成します。
- D. SSID が 16 文字を超えていないことを確認してください。
- E. AP を自律モードに設定します。

F. ワイヤレス LAN コントローラーをインストールします。

正解: ([正解を表示します](#))

Troubleshooting poor performance of a newly installed access point involves multiple steps. Checking for network bottlenecks and ensuring the device firmware is up to date are crucial first steps. The document confirms: "Network bottlenecks can severely limit the performance of even the fastest wireless access points, so it's essential to verify that no other devices are causing a slowdown. In addition, keeping firmware updated ensures optimal performance and security."

質問: 230

ヘルプデスクの技術者は、ユーザーがインターネットの URL にアクセスできないという報告を受け取ります。技術者が ping テストを実行すると、URL を使用するとサイトが失敗し、IP を使用するとサイトが成功することを発見しました。技術者が次に利用すべきツールは次のどれですか。

A. tcpdump

B. tracert

C. nmap

D. dig

正解: ([正解を表示します](#))

The issue is clearly related to DNS resolution, as IP-based connections succeed but domain name-based ones fail.

D). dig (Domain Information Groper) is a DNS lookup tool used to troubleshoot DNS problems by querying name servers directly.

Other tools are less relevant here:

A). tcpdump is a packet analyzer and is more advanced for deeper traffic analysis.

B). tracert is used to trace the route to a destination, not ideal for DNS issues.

C). nmap is a port scanner and network mapper, not for resolving DNS problems.

Reference:

CompTIA Network+ N10-009 Official Objectives: 5.1 - Given a scenario, use the appropriate network troubleshooting tools.

質問: 231

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 ([コメントを发表する](#))

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: 232

大規模な自然災害が会社の本社を襲い、甚大な被害とデータ損失が発生しました。会社は迅速な復旧と業務再開を必要としています。ネットワーク管理者が最初に行うべきことは何でしょうか？

- A. 損害評価を実施する
- B. コールドサイトに移行する
- C. 顧客に災害を通知する
- D. コミュニケーションプランを確立する

正解: ([正解を表示します](#))

In disaster recovery, the first step after an incident is to conduct a thorough damage assessment to understand the extent of the damage and determine the next appropriate steps. This allows for informed decision-making during the recovery process. The document says:

"The first step after a disaster is to conduct a damage assessment. This involves evaluating the extent of damage to equipment, infrastructure, and data, forming the foundation for recovery efforts and prioritizing response actions."

質問: 233

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: 234

最後のバックアップ以降に失われたデータの量を表すために使用される災害復旧メトリックは次のどれですか？

- A. 平均所要時間
- B. RTO
- C. RPO
- D. MTBF

正解: ([正解を表示します](#))

* Definition of RPO:

* Recovery Point Objective (RPO) is a disaster recovery metric that describes the maximum acceptable amount of data loss measured in time. It indicates the point in time to which data must be recovered to resume normal operations after a disaster.

* For example, if the RPO is set to 24 hours, then the business could tolerate losing up to 24 hours' worth of data in the event of a disruption.

* Why RPO is Important:

* RPO is critical for determining backup frequency and helps businesses decide how often they need to back up their data. A lower RPO means more frequent backups and less potential data loss.

* Comparison with Other Metrics:

* MTTR (Mean Time to Repair): Refers to the average time required to repair a system or component and return it to normal operation.

* RTO (Recovery Time Objective): The maximum acceptable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.

* MTBF (Mean Time Between Failures): The predicted elapsed time between inherent failures of a system during operation.

* How RPO is Used in Disaster Recovery:

* Organizations establish RPOs to ensure that they can recover data within a timeframe that is acceptable to business operations. This involves creating a backup plan that meets the RPO requirements.

References:

* CompTIA Network+ study materials and certification guides.

質問: 235

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API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. チャンネル幅の設定

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: **A** ([コメントを发表する](#))

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: 236

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

A. 22

B. 389

C. 445

D. 636

正解: **D** ([コメントを发表する](#))

LDAP (Lightweight Directory Access Protocol) uses port 389 for standard connections and port 636 for LDAP over SSL (LDAPS), which secures directory service communication.

Breakdown of Options:

A: 22 - SSH port, not used for directory services.

B: 389 - Used for LDAP, but not encrypted.

C: 445 - Used for SMB file sharing, not LDAP.

D: 636 - Correct answer. LDAPS (LDAP over SSL/TLS) secures directory authentication.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.1: Compare and contrast network protocols.

RFC 4511: Lightweight Directory Access Protocol (LDAP)

質問: 237

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: 238

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: 239

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 uses hot aisle/cold aisle ventilation, equipment is typically installed so that cool air enters from the cold aisle (front) and hot air is exhausted to the hot aisle (rear). This configuration maximizes cooling efficiency.

質問: **240**

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witch間にSTPケーブルを設置します
- C. スwitch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** ([コメントを发表する](#))

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: **241**

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witchを接続しています。これらのスウィッチは、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.

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

質問: **242** 管理者は、特定の日にインフラストラクチャ全体のトラフィックの最大の送信先を特定したいと考えています。管理者は次のうちどれを使用すべきでしょうか？

- A. SNMP
- B. パケットキャプチャ
- C. ネットフロー
- D. トレースルート

正解: ([正解を表示します](#))

NetFlow (and similar flow technologies like IPFIX/sFlow in concept) is used to collect traffic-flow metadata such as source/destination IPs, ports, protocols, interfaces, and byte/packet counts over time. In Network+ (N10-009) operations and monitoring objectives, flow data is ideal for identifying top talkers and top destinations across the network on a given day because it provides summarized, queryable information at scale without capturing every packet payload. An administrator can review reports to determine which destination IPs/hosts consumed the most bandwidth, which applications were most active, and what time ranges saw spikes-perfect for historical analysis.

SNMP is great for polling device counters (interface utilization, errors, CPU) but it does not natively tell you the "top destination" by conversation/flow without additional flow awareness. Packet capture can reveal exact conversations and payloads, but it is heavy, localized, and not efficient for infrastructure-wide daily top- destination reporting. traceroute maps the path to a destination and helps isolate routing/path issues; it does not provide usage statistics. Therefore, NetFlow is the best fit.

質問: **243**

特定のサブネットのルーティング テーブルを構築するときに優先されるルートのタイプは次のどれですか。

- A. 静的
- B. BGP
- C. OSPF
- D. デフォルト

正解: **A** ([コメントを发表する](#))

The correct answer is Static because static routes have a lower administrative distance (AD) than most dynamic routing protocols, giving them higher priority when a router selects routes for the same destination network. According to CompTIA Network+ (N10-009) routing objectives, administrative distance is used to determine the trustworthiness of a route source when multiple routing protocols provide a path to the same subnet. The lower the administrative distance, the more preferred the route.

By default, a static route has an administrative distance of 1, which is lower than OSPF (110) and BGP (20 for eBGP, 200 for iBGP). Because of this, when identical routes to a subnet exist from both static and dynamic sources, the router installs the static route in the routing table.

A default route (0.0.0.0/0) is only used when no more specific route exists and does not take precedence over specific static or dynamic routes.

Therefore, when building the routing table for a given subnet and comparing route sources, static routes take precedence due to their lower administrative distance.

質問: **244**

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フラッド
- B. DNSポイズニング
- C. VLANホッピング

D. ARPスプーフィング

正解: ([正解を表示します](#))

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: 245

次のクラウド サービス モデルのうち、データ センターをクラウドに移行する際に顧客による初期費用が最も高くなる可能性が高いのはどれですか。

A. サービスとしてのインフラストラクチャ

B. サービスとしてのソフトウェア

C. サービスとしてのプラットフォーム

D. サービスとしてのネットワーク

正解: ([正解を表示します](#))

Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

質問: 246

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: ([正解を表示します](#))

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: 247

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

A. AAAA

B. CNAME

C. MX

D. NS

正解: **D** ([コメントを發表する](#))

When an organization moves its DNS servers to new IP addresses, the NS (Name Server) records must be updated. The NS record defines which DNS servers are authoritative for a domain.

If these records still point to the old IP addresses, clients will continue to query the outdated servers, leading to connectivity issues.

Breakdown of Options:

- A). AAAA - This record maps a domain name to an IPv6 address. Since the issue is with DNS resolution, not IP versioning, this is incorrect.
- B). CNAME - A CNAME (Canonical Name) record is used for domain aliasing, not for defining authoritative name servers.
- C). MX - Mail Exchange (MX) records direct email traffic to the correct mail server, which does not impact general website accessibility.
- D). NS - Correct answer. NS records must be updated to reflect the new authoritative DNS servers.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.3: Explain the purpose and properties of DNS records.

RFC 1035: Domain Names - Implementation and Specification

質問: **248**

ある組織では、受信メールが信頼できるソースから送信されたことを確認したいと考えています。ソースを確認するために使用される DNS レコードは次のどれですか。

- A. テキスト
- B. AAAA
- C. CNAME
- D. MX

正解: ([正解を表示します](#))

A TXT record can be used to store SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) information, which help verify that an email has been sent from a trusted source.

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