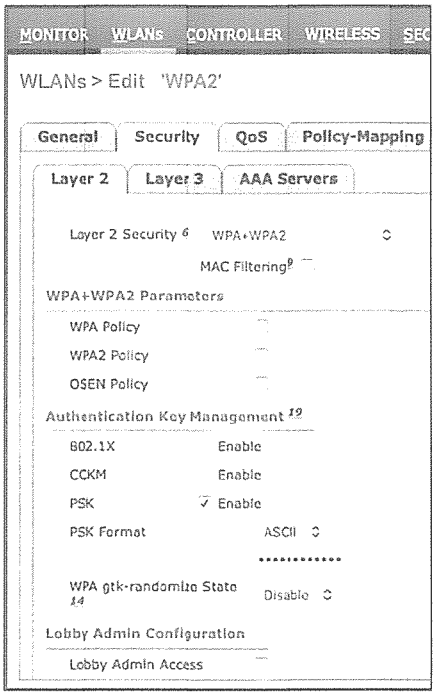
Part15

問題1　WPA2 PSK を使用して特定のクライアントのみが参加できるように WLAN を構成しています。プロセスを完了するには、どのアクションを実行しますか。(2つ選択)



A. 認証キー管理の CCKMを有効にする
B. 認証キー管理の 802.1Xを有効にする
C. WPA2 ポリシーを有効にする
D. OSEN ポリシーを有効にする
E. MAC フィルタリングを有効にする

答え　C,E
Layer 2 Security：WPA+WPA2
MAC Filtering：有効（許可するMACアドレスは別画面で設定する）
Authentication Key Management：PSK
PSK Format：ASCII または HEX
WPA gtk-randomize State（Group Temporal Key の生成に毎回ランダムな値を使うかどうか）：Enable/Disableはどちらでも。

問題2　JSON テキストの RFC 4627 デフォルト エンコーディングは何ですか。
A. UTF-8
B. GB18030
C. UCS-2

D. 16進数

答え A
＊JSONの文字コードはUTF-8が標準であり、推奨されている。

問題3 ["red", "one"]は、どのタイプの JSON データですか。
A. 数値
B. 配列
C. オブジェクト
D. 文字列

答え B
＊"key":"値"、オブジェクト{}、配列[]
＊正確にいうと、配列があって、その中にredやoneという文字列がある。

問題4 ブランチオフィスで新しいルーターを設定します。ルーターは、ブランチが本社と通信できるようにする上流の WAN ネットワークに接続されています。172.24.54.8 の中央タイムサーバーは、本社のファイアウォールの背後にあります。新しいルーターのソフトウェアクロックがタイムサーバーと同期するために、エンジニアはどのコマンドを設定しますか。
A. ntp client 172.24.54.8
B. ntp master 172.24.54.8
C. ntp peer 172.24.54.8
D. ntp server 172.24.54.8

答え D
＊ブランチ＝支社＝クライアント側はDのように設定します。親(本社)はBのように設定します。

問題5 インターネットへの接続が不安定です。インターフェイスの問題の原因は何ですか。

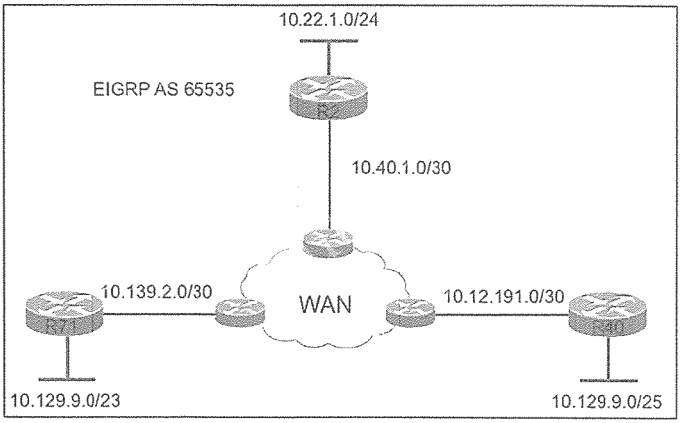
```
Router-WAN1#show interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CSR NIC, address is 5000.0001.0000 (bia 5000.0001.0000)
  Internet address is 192.168.0.0/31
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is NIC
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size /max)
  5 minute input rate 1000 bits/sec, 0 packets/sec
  5 minute output rate 2000 bits/sec, 1 packets/sec
```

0 packets input, 0 bytes, 0 no buffer
Received 110 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
100 input errors, 100 CRC, 100 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
260 packets output, 89070 bytes, 0 underruns
Output 0 broadcasts (0 IP multicasts)
0 output errors, **100 collisions**, 0 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
1 lost carrier, 0 no carrier, 0 pause output

A. ARPタイムアウトが有効になっているためブロードキャストパケットが拒否される
B. ブロードキャストストームにより受信バッファがいっぱいになる
C. 半二重ネゴシエーションによりフレームが破棄される
D. 64バイト未満の小さなフレームはサイズが小さいため拒否される

答え C
＊太字のエラー内容から、通信モードの不一致（相手が Half Duplex）、物理的なエラー（ケーブル破損、NIC故障など）が考えられます。
＊outputにエラーカウントが無いのは、自身の送信動作は制御できるため。

問題6　R2がネイバーから学習するルートはどれか。

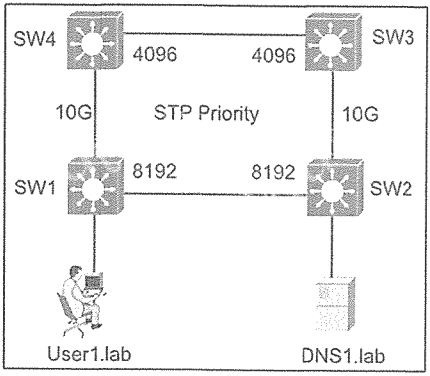


C.
10.129.9.0/23
10.40.1.0/30
10.12.191.0/30
10.129.9.0/25
D.
10.129.9.0/23
10.139.2.0/30

10.12.191.0/30
10.129.9.0/25

答え D
＊10.40.1.0/30 や 10.22.1.0/24 はローカルから学習されるため、除外します。

問題7　どのスイッチがルートブリッジとして選択されますか。



A. SW1: 0C:4A:82.:65:62:72
B. SW2: 0C:0A:A8:1A:3C:9D
C. SW3: 0C:0A:18:81:B3:19
D. SW4: 0C:0A:05:22:05:97

答え D
＊①プライオリティが小さい方→②同じならMACアドレスが小さい方

問題8　デバイスは、100.100.100.100 宛てのパケットをどのように処理しますか。

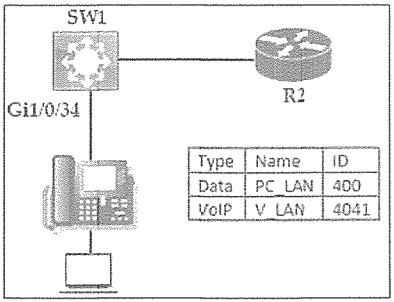
```
100.0.0.0/8 is variably subnetted, 4 subnets, 4 masks
...
R    100.0.0.0/8 [120/2] via 192.168.3.1, 00:00:13, Ethernet0/3
S    100.100.0.0/16 [1/0] via 192.168.4.1
D    100.100.100.0/24 [90/435200] via 192.168.2.1, 00:00:13, Ethernet0/2
O    100.100.100.100/32 [110/21] via 192.168.1.1, 00:05:57, Ethernet0/1
```

A. 動的ルートよりも静的ルートを常に優先します
　S 100.100.0.0/16 [1/0]
B. 最も低いメトリックのルートを選択します
　R 100.0.0.0/8 [120/2] via 192.168.3.1, 00:00:13, Ethernet0/3
C. 最も高いメトリックのルートを選択します
　D 100.100.100.0/24 [90/435200] via 192.168.2.1, 00:00:13, Ethernet0/2
D. 最も長い一致を持つルートを選択します
　O 100.100.100.100/32 [110/21] via 192.168.1.1, 00:05:57, Ethernet0/1

答え D

＊プレフィックス長が最も長いルートが選択されます。なお、/32はホストルートと呼ばれる。

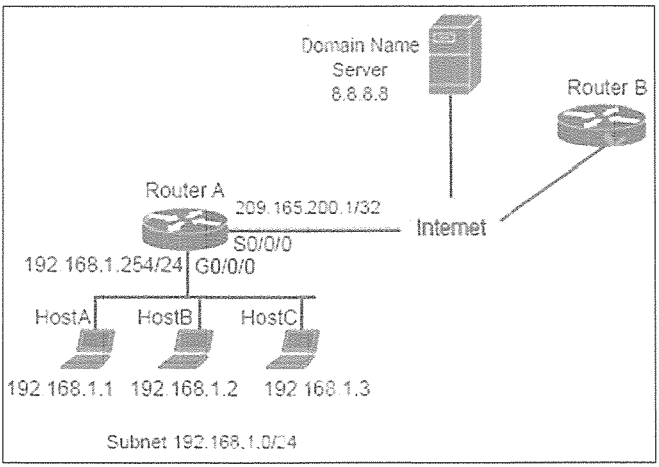
問題9　Gi 1/0/34 でネットワークサービスを有効にします。これを満たす構成はどれですか。

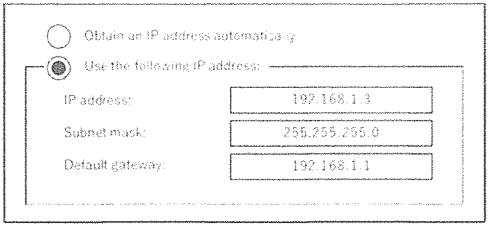


C.
```
interface Gi1/0/34
switchport mode trunk
switchport trunk allowed native vlan 400
switchport voice vlan 4041
```
D.
```
interface Gi1/0/34
switchport mode access
switchport access vlan 400
switchport voice vlan 4041
```

答え　D
＊この手の問題（データ+音声）はアクセスモードにします。

問題10　ホストC がインターネットに接続できない原因となっている構成パラメータはどれか。

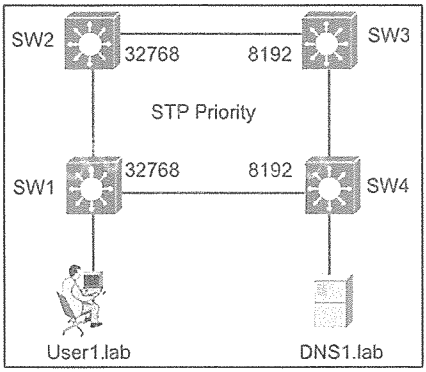




A. IPアドレスの割り当て
B. デフォルトゲートウェイ
C. IPネットワークマスク
D. 自動DNS

答え B
＊192.168.1.254 を指定するのが正しい

問題11　どのスイッチがルートブリッジとして選択されますか。



SW1 0C:0A:05:22:05:97
SW2 0C:4A:82:07:57:58
SW3 0C:0A:A8:1A:3C:9D
SW4 0C:0A:18:A1:B3:19

答え D
＊①プライオリティが小さい方→②同じならMACアドレスが小さい方。なお、16進数なので、アルファベットより数字の方が小さいと見なされます。

問題12　2.4GHzおよび5GHzで稼働するワイヤレスネットワークで、WPA2を使用したセキュアな事前共有キーベースのSSIDを作成しています。このプロセスを完了するために、エンジニアが実行しなければならない作業はなにか。(2つ選択)
A. 認証キー管理に802.1xオプションを選択する
B. WPA2 WPA3暗号化 に AES (CCMP128)オプションを選択する
C. 認証キー管理にAESオプションを選択する
D. 認証キー管理にPSKオプションを選択する

E. WPAポリシーオプションを選択する

答え B,D
＊「WPA2-PSK」に必要は設定は何か。問題1を参照。
＊"事前共有キー"とのこと、「pre shared Key」から、Dが選択できる。
＊WPA2-PSKの標準の暗号化はAESです。

問題13　ポートが近隣からのBPDUを受信せず、アドレスデータベースを更新せずに動作するRapid PVST+のポート状態はどれですか。
A. Listening
B. Forwarding
C. Disabled
D. Blocking

答え C
＊RSTPはDiscarding → Learning → Forwardingであるが、Disabled（完全に停止）という状態が存在する。問題文の「動作する」という言い方は良くない。

問題14　ファイアウォールで TCP 20 と 21 を許可している企業イントラネット上で、大きなファイルを転送する際に使用すべきプロトコルはどれか。
A. FTP
B. REST API
C. TFTP
D. SMTP

答え A
＊20転送、21制御

問題15　企業デバイスが企業ネットワークにログインできるようにするために実装されているパスワード認証以外の方法として最適なものはどれか。
A. デジタル証明書
B. マジックリンク
C. ワンタイムパスワード
D. 90日ごとの更新ポリシー

答え A
＊デジタル証明書はパスワードを使用せずに認証を行う方法です。企業ネットワークへのアクセス制御に広く使用されている認証方法です。

問題16　安全なパスワードポリシーを作成するのに役立つガイドラインはどれか。
A. パスワードマネージャーにパスワードを保存することをユーザーに禁止する
B. サービスアカウントで使用されるパスワードが期限切れにならないようにする
C. 単純な短いパスワードではなく、複雑で長いパスワードを要求する
D. パスワードの共有を非常に小さなグループに制限する

答え C

問題17　SSHアクセスだけを許可し、パスワードを隠すには、どのコマンドセットが必要ですか。

```
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#enable password test!2E
SW1(config)#line con 0
SW1(config-line)#password Labtest32!
SH1(config-line)#exit

SW1#(config)#line vty 0 15
SW1#(config-line)#password Labtest32!
```

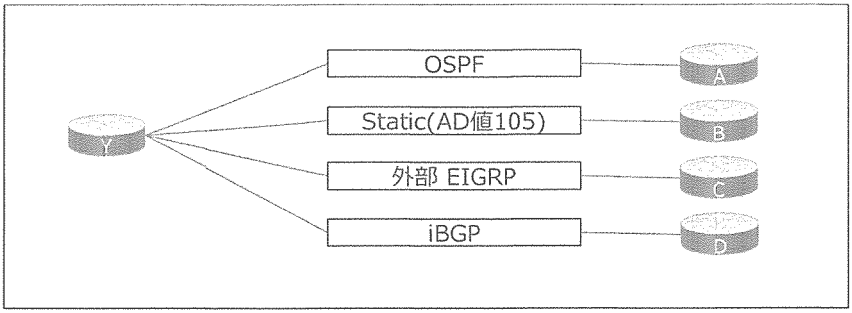
A.
```
SW1(config-line)#login local
SW1(config-line)#exit
SW1(config)#enable secret test!2E
```
B.
```
SW1(config-line)#transport input ssh
SW1(config-line)#exit
SW1(config)#service password-encryption
```
C.
```
SW1(config-line)#login local
SW1(config-line)#exit
```
D.
```
SW1(config-line)#exit
SW1(config)#aaa new-model
```

答え B
＊sshと書かれているのはBしかない。
＊transport input ssh：SSHのみが許可される
＊service password-encryption：設定済みのパスワードおよび今後設定するパスワードが平文で表示されなくなる

問題18　機械学習は侵入検知システムの有効性にどのように貢献するでしょうか。
A. セキュリティの権限レベルを割り当てる
B. セキュリティポリシーの更新を指示する
C. 古いソフトウェアを監視する
D. 侵入を示すパターンを識別する

答え D
＊侵入検知システムはIDSやIPSのこと
＊攻撃パターン（シグネチャ）を検知するだけでなく、"正常な動作ではないこと"や、複数動作の相関関係からも攻撃を検知します。

問題19　10.220.100.96/27の現在のルートが利用できなくなった場合、ルーターYは10.220.100.96/27へのトラフィックのルーティングにどのルーターを使用しますか。




```
Router-Y#show ip route
Gateway of last resort is not set

10.0.0.0/8 is variably subnetted
B 10.220.100.96/27 [20/0] via 10.224.1.3, 1w6d
```

A. ルーターA
B. ルーターB
C. ルーターC
D. ルーターD

答え B
＊現在のAD値は20である。21以上で、より小さいAD値が正解。
＊A.110、B.105、C.170、D.200

問題20　IPsec VPNの展開を計画する際に考慮すべきことは何か。
A. IPsecトランスポートモードでは、中間デバイスがパケットの最終宛先を確認できる
B. IPsecトンネルモードでは、IPペイロードのみが暗号化される
C. IPsecトランスポートモードでは、トンネルモードのGREトンネルのセキュリティが向上する
D. IPsecトランスポートモードでは、レイヤー4ヘッダーが暗号化されないため、パケットの完全な検査が可能になる

答え A
＊トランスポート：ペイロードのみ暗号化される。トンネル：ヘッダーもペイロードも暗号化される。

問題21　スプリットMACアーキテクチャでは、リアルタイム制御機能はどこで処理されるか。
A. 中央WLC
B. 個々のAP
C. 集中型クラウド管理プラットフォーム
D. クライアントデバイス

答え B
＊スプリットMACアーキテクチャとは、WLCとAPのアーキテクチャのこと。WLCは全体の制御(セキュリティなど)、APはリアルタイムなこと（暗号化/複合化やフレーム転送）。

問題22　802.11b/g/n/ax 2.4 GHz 周波数帯域のチャネルグループのうち、重複しないチャネルはどれか。
A. チャネル 1、6、10
B. チャネル 1、5、11
C. チャネル 1、6、11
D. チャネル 1、5、10

答え C
＊5の差が必要です。2,7,12でも正解。

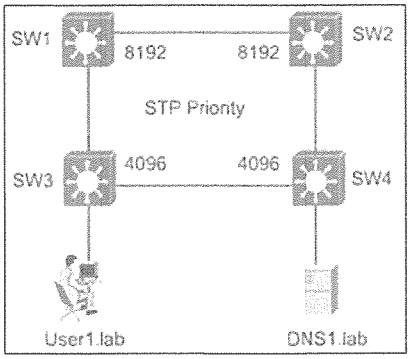
問題23　IPパケット全体をカプセル化するIPsecモードはどれか。
A. トンネル
B. トランスポート
C. SSL VPN
D. Q-in-Q

答え A
＊問20参照

問題24　WPA3が従来よりも高度なセキュリティを提供できる仕組みはどれか。
A. 自動デバイスペアリング
B. 共有鍵における特殊文字のサポート
C. 証明書ベースの認証
D. SAE パスワードベースの鍵交換

答え D
＊SAE（Simultaneous Authentication of Equals＝同等者の同時認証）は、毎回異なるセッション鍵を生成するという点でWPA2よりも優れています。WPA2では、ハンドシェイクをキャプチャされると、オフラインで攻撃可能であり、攻撃者はローカル環境で時間をかけて大量のパスワードを試せるという脆弱性がありました。

問題25　どのスイッチがルートブリッジに選ばれますか。



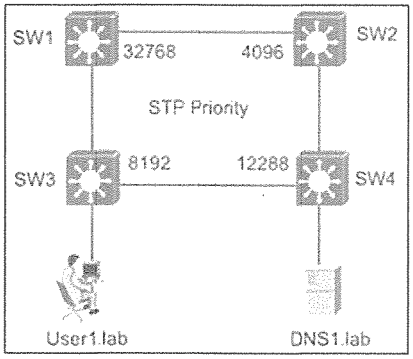
SW1　0c:b4:86:22:42:37
SW2　0c:0b:15:22:05:97

SW3　0c:0b:15:1a:3c:9d
SW4　0c:B0:18:A1:B3:19

A. SW1
B. SW2
C. SW3
D. SW4

答え C
＊①プライオリティが小さい方→②同じならMACアドレスが小さい方。なお、16進数なので、アルファベットより数字の方が小さいと見なされます。

問題26　どのスイッチがルートブリッジに選ばれますか。



SW1　0c:e4:85:71:03:80
SW2　0c:0e:1a:22:05:97
SW3　0c:e0:a1:1a:3c:9d
SW4　0c:00:18:a1:b3:19

A. SW1
B. SW2
C. SW3
D. SW4

答え B
＊①プライオリティが小さい方→②同じならMACアドレスが小さい方。

問題27　認証に成功するために、ユーザーが物理的な属性を提供する必要がある認証方法はどれですか。
A. 証明書
B. パスワード
C. 多要素
D. バイオメトリクス

答え D

＊"物理的な属性"が分かりづらい。

問題28　AES および事前共有キー Cisco123456 を使用した WPA2 暗号化用に WLAN を設定します。「Layer 2 Security」から[WPA+WPA2]を選択した後、どのタスクを実行しますか。(2つ選択)

A. 「Auth Key Mgmt」から[PSK]を選択し、「PSK Format」を[ASCII]に設定し、キーを入力する。
B. 「Auth Key Mgmt」から[CCKM]を選択し、[PSK Format]を[Hex]に設定し、キーを入力する。
C. 「PSK Format」から[ASCII]を選択し、キーを入力し、「Auth Key Mgmt」を空白のままにする。
D. WPA2 Policy、AES、TKIPチェックボックスを選択する。
E. WPA2 Policy、 AES チェックボックスを選択する。

答え A,E
＊A.問題文で"事前共有キー"とのこと、PSK（Pre-Shared Key）が正しい。
＊B.パスワードが"Cisco"であるため、HEX(16進数)では表現できません。
＊D.TKIPは非推奨です

問題29　Ansibleがネットワーク内のノードにモジュールをプッシュするために使用するプロトコルはどれですか。
A. SSH
B. Kerberos
C. SNMP
D. Telnet

答え A
＊Ansible で標準的に使われるのはSSHです。
＊B,C,Dはプッシュ（転送）とは関係ないプロトコル。

問題30　ドメイン名解決プロセスにおいて、反復DNSクエリはどの機能を果たしますか。
A. DNSクライアントとサーバー間の通信を自動的に暗号化する。
B. 正しい情報が見つかるまで、DNSクライアントが複数のDNSサーバーに問い合わせることを許可する。
C. スコープ内に設定されているすべてのルートDNSサーバーから直接情報を取得する。
D. 複数のDNSサーバーで同時にレコードを動的に更新する。

答え B
＊DNSの再帰や反復の理解。PC→ローカルDNSサーバは再帰、ローカルDNSサーバから先は反復で探してくれる。

問題31　制御プレーンやデータプレーン機能に関連するコントローラベースのネットワークと、従来のネットワークの違いは何ですか。
A. コントローラベースのネットワークはすべての重要な制御プレーン機能を集中管理し、従来のネットワークは制御プレーン機能を分散管理する。
B. 従来のネットワークは、すべての重要な制御プレーン機能を集中管理し、コントローラベースのネットワークは制御プレーン機能を分散管理する。
C. 従来のネットワークは重要なデータプレーン機能をすべて集中管理し、コントローラベースのネットワークはデータプレーン機能を分散管理する。

D. コントローラベースのネットワークがすべての重要なデータプレーン機能を集中管理し、従来のネットワークがデータプレーン機能を分散管理する。

答え A
＊SDNの理解。集中管理し＝SDNコントローラーで管理する。分散管理する＝各機器に設定をする。

問題32　IPsec VPNの実装時に考慮しなければならない要素はどれか。
A. IPsecトランスポートモードは、検査のためにレイヤ4ヘッダを暗号化せずに残す。
B. IPsecトランスポートモードは、トンネルモードよりもGREトンネルのセキュリティを向上させます。
C. IPsec トンネルモードでは、IP ペイロードだけが暗号化されます。
D. IPsec トンネルモードでは、元の IP データグラム全体が暗号化されます。

答え D
＊IPsecにはトランスポートモード（ホスト間、ペイロードのみ暗号化）とトンネルモード（拠点間、ヘッダもペイロードも暗号化）がある。類20,23

問題33　WLC のインバンド無線ネットワーク管理用のデフォルトインターフェースは何ですか。
A. マネジメント
B. 冗長ポート
C. サービスポート
D. アウトオブバンド

答え A
＊WLCの論理インターフェースの理解。管理者がWLC経由で各機器を設定するときに使用するポートは、マネジメントポート。

問題34　自動ライフサイクル管理にCisco DNA Centerを選択する理由は何ですか。
A. サービスを中断することなくアップグレードを実行するため
B. ネットワークにソフトウェアの冗長性を提供するため
C. パッチとアップデートを迅速かつ正確に展開するため
D. ネットワーク内のすべてのノードへの SSH アクセスを可能にするため

答え C
＊イメージを一括ダウンロード→展開スケジュール設定→自動配信・適用

問題35　IPsecサイト間VPNにおけるトンネルモードの主な機能は何ですか。(2つ選択)
A. オリジナルパケットのデータフィールドを認証する
B. データフィールドと完全なIPパケットを暗号化する
C. パケット内のデータフィールドのみを保護する
D. 元のパケットヘッダが見える状態で送信する
E. 新しいIPアドレスを持つ新しいIPsecヘッダを挿入します

答え B,E
＊E.全体を暗号化したうえで新たにヘッダを付ける。類20,23,32

問題36　AIはネットワークトラフィック分析にどのように貢献しますか。

A. トラフィックのルートマッピングを簡素化します
B. データパケットの配信速度を向上させます
C. 異常検出のためにパターンを分析します
D. ネットワークの脅威を排除します

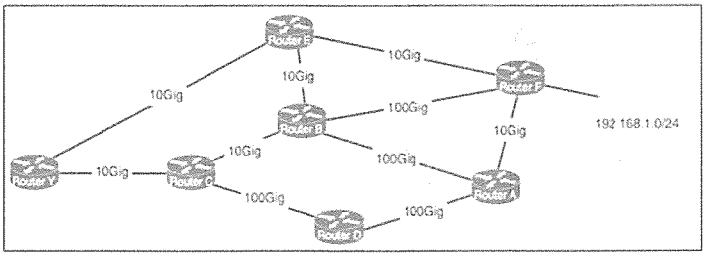
答え C
＊問18参照

問題37　純粋なIPsecで送信されるトラフィックのタイプはどれか。
A. 2つの異なるサイトにあるスイッチ間のスパニングツリー更新
B. リモートサイトのホストから本社のサーバーへのユニキャストメッセージ
C. 複数のリモートサイトの1つにあるMACアドレスを見つけようとするスイッチからのブロードキャストパケット

D. あるサイトのサーバーから別のサイトのホストへのマルチキャストトラフィック

答え B
＊IPsecは基本的に1:1（ユニキャスト）の通信を前提として設計されています。

問題38　すべてのルーターの基準帯域幅が100Gbの場合、ルーターYはネットワーク192.168.1.0/24に到達するためにどのパスを使用しますか。



A. C > D > A > F
B. E > B > F
C. E > F
D. C > D > A > B > F

答え D
＊帯域が大きいところを通せばよい。
＊計算方法としては100÷そこの帯域　→　Y～C[10]+C～D[1]+D～A[1]+A～B[1]+B～F[1]＝14

問題39　RSAの特徴は何ですか。
A. 双方が同一の鍵を持つ必要がある
B. 秘密鍵暗号化アルゴリズムである
C. 暗号化に共有鍵を使用する
D. 公開鍵暗号方式である

答え D
＊AESは共通鍵、RSAは秘密鍵/公開鍵

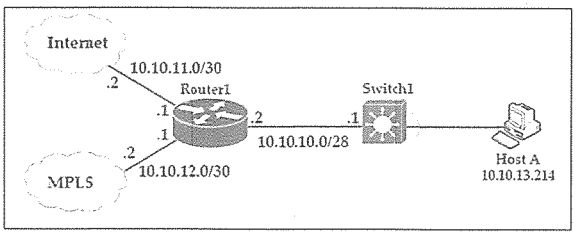
問題40　ネットワークにおけるコントロールプレーンの機能は何ですか。
A. ネットワークデバイスへのCLIアクセスを提供する
B. 他のルーターとトポロジー情報を交換する
C. フォワーディング情報ベースでイグレスインターフェースを検索する
D. 次のホップにトラフィックを転送する

答え B
＊SDNの理解。コントロールプレーン（経路作成）とデータプレーン（転送処理）の区別。

問題41　RESTリクエストのURI文字列の目的は何ですか。
A. リモートリソースの変更方法を指定するため
B. ターゲットサーバー上のリソースを識別するため
C. リクエストのデータコンテンツエンコーディングで応答するため
D. データまたはペイロードをリモートリソースに転送する

答え B
＊例：POST /api/users
＊RESTリクエストは、HTTPメソッド（GET、POSTなど）を使用してリソースを操作するリクエストのことです。この「/api/users」がURIです。データリソース（操作の対象）を指しています。

問題42　ルーター1がホストAに到達するために使用するルートのプレフィックス長は？




```
Router1#show ip route
Gateway of last resort is 10.10.11.2 to network 0.0.0.0

  209.165.200.0/27 is subnetted, 1 subnets
B    209.165.200.224 [20/0] via 10.10.12.2, 03:03:03
  209.165.201.0/27 is subnetted, 1 subnets
B    209.165.201.0 [20/0] via 10.10.12.2, 03:03:03
  209.165.202.0/27 is subnetted, 1 subnets
B    209.165.202.128 [20/0] via 10.10.12.2, 03:03:03
  10.0.0.0/8 is variably subnetted, 8 subnets, 4 masks
C    10.10.10.0/28 is directly connected, GigabitEthernet0/0
C    10.10.11.0/30 is directly connected, FastEthernet2/0
C    10.10.12.0/30 is directly connected, GigabitEthernet0/1
O    10.10.13.0/25 [110/2] via 10.10.10.1, 00:00:03, GigabitEthernet0/0
O    10.10.13.128/28 [110/2] via 10.10.10.1, 00:00:03, GigabitEthernet0/0
```

```
O    10.10.13.144/28 [110/2] via 10.10.10.1, 00:00:03, GigabitEthernet0/0
O    10.10.13.160/29 [110/2] via 10.10.10.1, 00:00:03, GigabitEthernet0/0
O    10.10.13.208/29 [110/2] via 10.10.10.1, 00:00:03, GigabitEthernet0/0
S*  0.0.0.0/0 [1/0] via 10.10.11.2
```

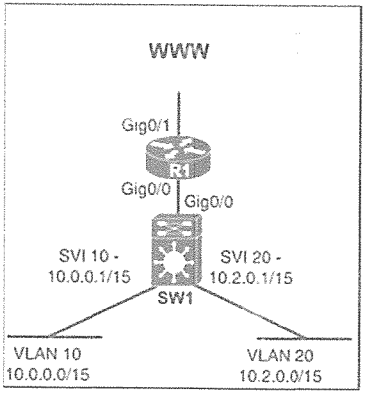
A. /25
B. /27
C. /28
D. /29

答え D
＊10.10.13.208/29 が使用されます。ロンゲストマッチ：①宛先がサブネットに含まれていること→②よりビットが一致していること

問題43　FlexConnectは、他のアーキテクチャに比べ、どのような条件で推奨されますか。
A. 複数のリモートオフィスへの接続待ち時間が300ミリ秒を超えると予想される場合
B. さまざまなリモートオフィスで高精度の位置情報サービスが必要な場合
C. 個々のWLCがない複数のリモートオフィスで集中管理が必要な場合
D. 各リモートオフィスがネットワーク管理のために独自のローカルWLCを必要とする場合

答え C
＊FlexConnectは、中央のワイヤレスLANコントローラ(WLC)からWAN経由でリモートサイトのアクセスポイント(AP)を管理できるようにする技術です。

問題44　SW1にVLAN間ルーティングが設定されている。クライアントAはVLAN 10のOSとしてLinuxを実行しており、デフォルトゲートウェイIPは10.0.0.1ですが、Windowsを実行しているVLAN 20のクライアントBにpingを送信できません。クライアントAが正しいIP設定を持っていることを確認するために、どのようなアクションを取らなければなりませんか。



A. ifconfigコマンドを実行し、IPとサブネットマスクが255.254.0.0の範囲内にあることを確認する
B. ipconfigコマンドを実行し、IPアドレスが10.0.0.1～10.0.255.254の範囲内にあることを確認する
C. ipconfigコマンドを実行し、デフォルトゲートウェイが10.0.0.1に使用されていることを確認する
D. ifconfigコマンドを実行し、サブネットマスクが255.255.128.0に設定されていることを確認する

答え A
＊Linuxでは「ifconfig」が正しい。/15は、255.254.0.0である。
＊ifconfigはネットワークインターフェースの設定状況を確認するためのコマンド。ちなみに、いまは、ip addr を使うことが推奨されている。

問題45　新しい管理者は、DNSサービスへのTCPアクセスも追加したいと考えています。このACLを効率的に更新する設定方法として、最も適切なものはどれですか？

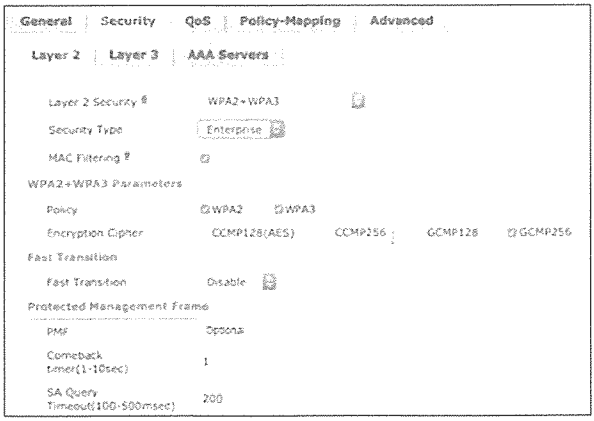
```
CPE# show ip access-list Services
...
Extended IP access list Services
  10 permit tcp 10.0.0.0 0.255.255.255 any eq www
  20 permit tcp 10.0.0.0 0.255.255.255 any eq 443
  30 permit udp 10.0.0.0 0.255.255.255 host 198.51.100.11 eq domain
  40 deny ip any any log
```

C.
```
no ip access-list extended Services
ip access-list extended Services
 permit udp 10.0.0.0 0.255.255.255 any eq 53
 permit tcp 10.0.0.0 0.255.255.255 host 198.51.100.11 eq domain
 deny ip any any log
```

D.
```
ip access-list extended Services
 35 permit tcp 10.0.0.0 0.255.255.255 host 198.51.100.11 eq domain
```

答え D
＊C.「no」で一度全部を削除してしまっているので、HTTPやHTTPSの設定が無くなってしまう。
＊D.40より若い番号（35）で設定していることもポイント。若い順に適用されるため。

問題46　Wi-Fi SSID「Office_WLan」にはレイヤー2セキュリティが設定されています。この構成によって何が決定されますか。



A. 強力な暗号化と認証を提供するガロアキャッシュアルゴリズムが設定されています。
B. x.509標準を使用して、NACとネットワーク・デバイス間で強力な相互認証が使用されています。
C. 既知のMACアドレスを持つ許可されたデバイスのみが、ネットワークに接続することを保証するセキュリティの追加レイヤーがある。
D. さまざまなレイヤー 2 およびレイヤー 3 攻撃から保護するために設定された堅牢なセキュリティ メカニズムがあります。

答え C
＊MAC Filtering にチェックが入っている

問題47　エンドホストに接続されたスイッチポートにPortFastを設定する理由は何ですか。(2つ選択)
A. ポートで学習する MAC アドレス数を 1 にする
B. トポロジ変更プロセスからポートの動作を保護する
C. ホストが起動すると、ポートが直ちにフォワーディング状態になるようにする
D. スパニングツリープロトコルの動作にポートが参加しないようにする
E. 別のスイッチまたはホストがポートを介して通信するのをブロックする

答え B,C　※D.STPには引き続き参加します

問題48　ユーザーは192.168.3.0/24上のデバイスには接続できますが、10.10.1.0/24上のユーザーには接続できません。接続性を確認する最初のステップは何ですか。

```
C:¥Users¥ADMIN>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
<...>
   Physical Address . . . . . : 04-42-1A-EE-AA-5E
   DHCP Enabled . . . . . : Yes
   Autoconfiguration Enabled. . . . . : Yes
```

```
Link-local IPv6 Address. . . . . : fe80::8a79:bcde:34dc:c11e35%(Preferred)
Ipv4 Address . . . . . : 192.168.3.20(Preferred)
Subnet Mask. . . . . : 255.255.255.0
Lease Obtained . . . . . : Thursday, 16 March 2023 6:25:01 AM
Lease Expires. . . . . : Sunday, 26 March 2023 16:17:26 PM
Default Gateway. . . . . : 192.168.3.1
DHCP Server. . . . . : 192.168.3.1
DHCPv6 IAID. . . . . : 201605658
DHCPv6 Client DUID . . . . . : 00-01-00-01-2A-3F-45-34-03-13-23-EE-AD-5E
DNS Servers. . . . . : 10.10.1.254
NetBIOS over Tcpip . . . . . : Enabled
```

A. インターネットに接続できるか
B. デフォルトゲートウェイに到達可能か
C. DNSサーバーに到達可能か

答え B
※他のネットワークと通信できないとのこと、デフォルトゲートウェイへの到達を確認します。

問題49　攻撃者がシステム管理者の平文のパスワードをスニッフィング（盗聴）できた場合の、パスワード攻撃を軽減する適切な解決策は何ですか。
A. 次世代ファイアウォールによって、ステートフルパケットインスペクションを維持する。
B. 2つの異なる認証ソースを使用する多要素認証
C. ACL を使用して、受信する Telnet セッションを「admin」アカウントに制限する。
D. 既知の攻撃ベクトルのブロックリストを持つIPS

答え B
※多要素認証：知識情報（パスワード）、所持情報（スマホ）、生体情報（指紋）　カッコは例

問題50　ネットワークエンジニアが、認証サーバーの設定とダイナミックインターフェイスの作成によって、新しい無線LANの実装を開始します。基本設定を完了するには、次に何を実行しますか。
A. 管理インターフェイスをインストールし、管理IPを追加します。
B. アクセスポイントの高可用性と冗長性を設定します。
C. 管理インターフェイスでTelnetとRADIUSアクセスを有効にする。
D. 新しい WLAN を作成し、ダイナミックインターフェイスをそれにバインドします。

答え D
※ダイナミックインターフェイスは、WLCにおいて、SSIDとVLANを動的にマッピングする仮想的なインターフェイスです。順序：インターフェイス作成 → WLAN作成 → インターフェイスをWLANにバインド

問題51　[TCP/UDP]ドラッグ＆ドロップ
答え
TCP
・ シーケンス番号を使用する
・ 確認応答パケットに依存する
・ データの完全性を保証する

UDP
・ リアルタイム・アプリケーションをサポート
・ トランスポート層でのコネクションレス
・ 最小限のエラーチェック

＊TCPは品質重視、UDPは速度重視
＊リアルタイム・アプリケーションとはNTP,SNMP,VoIPなどのこと

問題52　機械学習はネットワークセキュリティにどのような利点をもたらしますか。
A. リアルタイムの脅威検出を改善します
B. ファイアウォールのルール セットを管理します
C. パスワードの複雑さの要件を適用します
D. VPN アクセス権限を制御します

答え A
＊問18参照

問題53　インターネットにアクセスする前にユーザーに認証、登録、または利用規約への同意を強制するキャプティブポータルを提供するAP機能はどれですか。
A. ワンクリック
B. ホットスポット
C. 強化された Bluetooth
D. ホールホーム

答え B
＊ホットスポットとは"ワイヤレスでインターネットに接続するための場所（スポット）"という概念です。アクセスポイントはホットスポットを提供する機器（概念ではなく物理的なもの）です。

問題54　ワイヤレス アーキテクチャにおける「スプリット MAC」という用語は何を指しますか。
A. データリンク層機能を AP と WLC の間で分割する
B. データ転送機能から管理機能と制御機能を統合する
C. 同じ AP で 2.4 GHz 帯と 5 GHz 帯に異なる MAC アドレスを使用する
D. 2 つの AP を活用して制御トラフィックとデータ トラフィックを処理する

答え A
＊問21参照
＊リアルタイムタスク (プローブ応答、パケット バッファリング、フラグメンテーション、キューイングなど) は AP によって処理され、非リアルタイム タスク (関連付け/関連付け解除、分類、802.1x/EAP 認証など) は WLC によって処理されます。

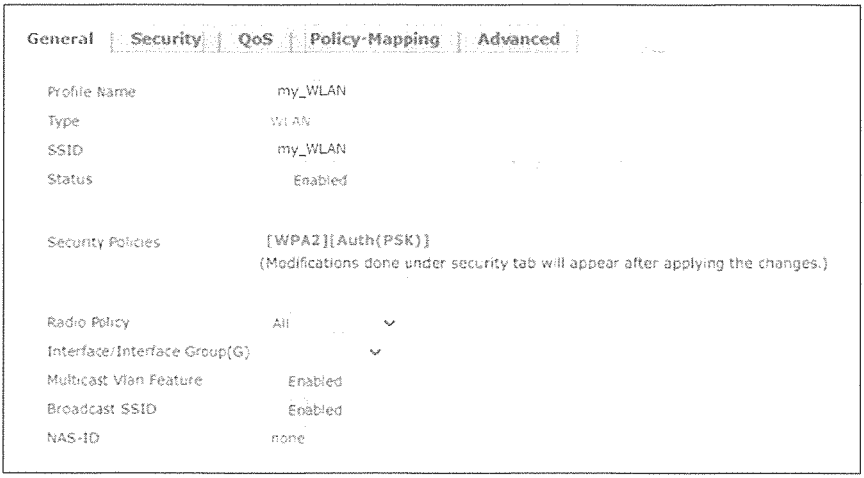
問題55　ソフトウェア定義ネットワークではどのプレーンが集中化されますか。
A. アプリケーション
B. サービス
C. 制御
D. データ

答え C
＊SDNはコントロールプレーン(判断)とデータプレーン(転送)を分離する

問題56　機械学習によって不正なネットワークアクセスの検出がどのように改善されますか。
A. 古いソフトウェアを監視します。
B. セキュリティ ポリシーの更新を指示します。
C. 侵入を示すパターンを識別します。
D. セキュリティ クリアランス レベルを割り当てます。

答え C
＊機械学習はデータを分析してパターンを見つけることで継続的に学習することで、マルフェアや脅威を検出します。類18,52,56

問題57　「My_WLAN」というWLANに接続するユーザーを、「Data」という別サブネットに接続させたいとき、管理者はどんな追加設定をしますか。



A. Broadcast SSIDを有効にし、Interface/Interface Group(G)のドロップダウンリストから「Data」を選択します。
B. ステータスを有効にし、Interface/Interface Group(G)のドロップダウンリストから「Data」を選択します。

C. ステータスを有効にし、NAS-IDを「Data」に設定します。
D. ステータスを有効にし、ブロードキャストSSIDを有効にします。

答え B
＊【余談】セキュリティポリシーは「Security」タブで設定しているため、この画面では設定できないようになっている。

問題58　RADIUSサーバーを使って全ユーザーとデバイスを認証したいが、すべての端末がdot1xに対応しているわけではありません。この要件を満たすには、どの設定を変更しますか。（2つ選択）

A. [レイヤ2] タブで［AutoConfig iPSK］を有効にします。
B. [AAAサーバー]タブで[認証サーバー]を選択します。
C. [レイヤ2] タブで［エンタープライズセキュリティ］タイプを設定します。
D. [レイヤ3] タブで［認証］を設定します。
E. [レイヤ2] タブで「WPA2ポリシー」を有効にします。

答え A,B
＊dot1x＝IEEE 802.1X認証のこと
＊A.iPSK（Identity PSK） は、ユーザーやデバイスごとに異なるPSK（事前共有キー）をRADIUSと連携して設定する方式。dot1xに対応していないデバイス向けにRADIUS連携を可能にする方法として有効。B.ここでRADIUSサーバーを指定する

問題59　自律型、クラウドベース、スプリットMACアーキテクチャのいずれかを決定しなければならない。アーキテクトが考慮すべきことはどれか。(2つ選択)
A. 軽量アクセスポイントは、スプリットMACアーキテクチャによってのみ使用される。
B. クラウドベースのアーキテクチャは、アクセスポイントとクライアント間の通信にCAPWAPプロトコルを独自に使用する。
C. 3つのアーキテクチャのそれぞれは、アクセスポイントを管理するためにWLCを使用する必要があります。
D. 3つのアーキテクチャはすべて、有線インフラストラクチャに接続されたワイヤレスデバイスを管理するためにアクセスポイントを使用します。

答え A,D
＊Aの説明：自律型はWLCなし、クラウドベースはWLCなし＋ブラウザ上のダッシュボードで管理できる、スプリットMACアーキテクチャはWLCを経由して処理する。
＊Dの説明：分かりにくい文章である。"スイッチ等の有線インフラストラクチャに接続するスマホやPCに無線を提供するためにアクセスポイントを使用します"と読み替える。

問題60　ポイント・ツー・マルチポイントのネットワーク・トポロジーにおいて、プライマリ・ハブとして機能するAPモードはどれか。
A. ブリッジ
B. SE-Connect
C. FlexConnect
D. ローカル

答え A
＊プライマリ・ハブ＝中央の親機。他のAPを束ねる役割をする。

問題61　ネットワークの自動化は、ネットワークのダウンタイムをどのように削減しますか？
A. ネットワーク管理者がネットワークの変更を実行した時に基づいてEメールを生成することができ、可視性が向上します。
B. 設定テンプレートとテストを実装に組み込むことができ、ネットワーク変更の成功率を高めます。
C. 一度に複数のデバイスで変更を並行して実施できるため、変更速度が向上する。
D. インテント・ベースのコンフィギュレーションを備えた自動化プラットフォームを使用することで、すべての変更が実施前に機能停止の可能性がないかチェックされる。

答え B

＊問題文の意味は「ダウンさせないようにするには？」です。
＊C.速さについては本問では関係ない。また、一度に平行して実行するのは逆にリスクである。

問題62　[ネットワーク・トポロジー]ドラッグ&ドロップ

答え：
・パケットを可能な限り高速にスイッチする：コア
・ルーティング,フィルタリング,WANアクセスを提供：ディストリビューション
・エンドユーザー接続：アクセス
・トップ・オブ・ラック：スパインリーフ

＊3層アーキテクチャは「コア＋ディストリビューション＋アクセス」であるが、トラフィックを徐々に集約するため、コア層側になるほど高性能で高価となる。
＊スパインリーフ：スパインは幹、リーフは葉の意味。スイッチがラックの最上段にあるので、Top Of Rackと呼ばれる。データセンターで利用されるアーキテクチャ。

問題63　SNMPトラップとSNMPポーリングの違いは何ですか。
A. SNMPトラップはネットワーク・デバイスでプッシュ・モデルを使用して開始され、SNMPポーリングはサーバーで開始されます。
B. SNMPトラップはプロアクティブ監視に使用され、SNMPポーリングはリアクティブ監視に使用されます。
C. SNMPトラップはネットワーク管理システムによって開始され、SNMP ポーリングはネットワーク・デバイスによって開始されます。
D. SNMPトラップはMIBを介して定期的な更新を送信し、SNMPポーリングはオンデマンドでデータを送信します。

答え A
＊SNMPトラップ：何かあれば機器が知らせる（Push）、SNMPポーリング：ネットワークを監視するサーバー（NMS）が機器たちを定期的に確認しにいく（引き出す＝Pull）

問題64　WPA3-SAEを使用したSSIDはワイヤレスクライアントによって使用されている間、どのような機能を持つか。
A. エアスニッフィング攻撃に対するネットワークセキュリティを低下させ、複雑なパスワードの使用を抑制します。
B. オフライン辞書攻撃に対するネットワークセキュリティを向上させ、時間のかかる総当たり攻撃を抑制します。

C. 中間者攻撃に対するネットワーク・セキュリティを高め、サービス拒否攻撃を抑制する。
D. オフライン辞書攻撃に対するネットワークセキュリティを低下させ、ネットワークへの容易なアクセスを促す。

答え B
＊問24参照。オフライン辞書攻撃とは、ハンドシェイク情報を盗聴して、オフラインで復号を試みること。

問題65　ネットワーク機器のヘルスモニタリングにおけるsyslogレベル7の役割は何ですか？
A. ネットワークデバイス上で見えるエラー状態に関する情報を提供します。
B. ネットワーク機器からの正常な操作メッセージを共有します。
C. デバイス上の様々なデバッグコマンドからの出力を送信します。

D. ネットワーク・アプライアンスの緊急事態について警告します。

答え C
＊レベル0～7の順に、緊急(Emergency)→警報(Alert)→重大(Critical)→エラー(Error)→警告(Warning)→通知(Notice)→情報(Information)→デバッグ(Debug)

問題66　小規模オフィスで無線の必要性が最小限で中央管理が不要な場合、どのアーキテクチャが最適ですか。
A. クラウドベースのアクセスポイント
B. スプリットMAC
C. 自律型アクセスポイント
D. メッシュネットワーク

答え C
＊自律型APは単体で動作するアクセスポイントで、WLCを必要としません。小規模環境でシンプルな構成を求める場合に適しています。

問題67　[TCP/UDP]ドラッグ&ドロップ

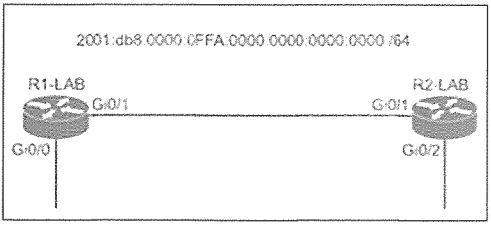
TCP
・データを特定の順序で送信します
・確立された接続が必要です
・ウェブブラウジングをサポートします
UDP
・ライブストリーミングに適しています
・再送信はサポートされていません
・パケット損失に耐性があります

＊類51

問題68　DNSにおける有効なIPv6アドレスレコードとは何ですか？
A. A
B. MX
C. AAAA
D. CNAME

答え C
＊アドレスレコードは、AかC。AはIPv4アドレス用、CはIPv6アドレス用。

問題69　R1-LAB と R2-LAB はリンクローカルアドレスで設定されています。R1-LAB の Gi0/0 に、IPv6 ネットワークでの自動アドレス割り当てを有効にするために、どのコマンドを適用しますか。



A. ipv6 address 2001:db8:0:0FFA::/64 eui-64
B. ipv6 address 2001:db8:0:0FFA::1/64
C. ipv6 address 2001:db8:1:0FFA:0::/64
D. ipv6 address 2001:db8:0:0FFA::/64 anycast

答え A
＊"自動アドレス割り当て"→EUI-64「::/64 eui-64」

問題70　アプリケーションがJSON形式のコンテンツを要求する場合、RESTリクエストに必ず含まなければならないヘッダーはどれですか？
A. Content-Type: application/json
B. Accept-Encoding: application/json
C. Accept: application/json
D. Accept-Language: application/json

答え C
＊【丸暗記】この一行がないと、サーバーは他の形式（例：XMLやHTML）で返すことがある

問題71　ネットワーク管理者がRFC 1918アドレス空間を実装する理由はなにか。
A. インターネット上のトラフィックをルーティングするため
B. ネットワーク上のホストの数を制限するため
C. 別のネットワークとアドレス空間を重複させるため
D. IPネットワーク設計の柔軟性を確保するため

答え D
＊RFC1918＝プライベートIPアドレス。アドレス枯渇対策、セキュリティ確保が主な理由。

問題72　AireOS GUIを使用する際、管理ページに同時にアクセスできるのは何人か。
A. 2
B. 5
C. 8
D. 9

答え B
＊【丸暗記】Cisco AireOS（旧WLCのオペレーティングシステム）では、GUI（Web管理画面）に同時にアクセスできるユーザー数は5人。

問題73　SSH管理アクセスの一番の目的は何ですか。
A. ユーザー名とドメイン名のみで管理アクセスを認証するため
B. HTTPS暗号化で保護されたパスワードを送信できるようにするため
C. DES 56ビットと3DES（168ビット）暗号化方式をサポートするため
D. 着信管理インターフェースへのセキュアなアクセスを可能にするため

答え D
＊SSHアクセスの目的→セキュアなアクセス

問題74　自動化は、データモデルをどのように活用して管理対象ネットワークの運用複雑性を軽減しますか。
A. 多くのインターフェースを持つデバイスに対する特定の要求への応答時間を短縮する
B. コントローラーがベンダーに依存しないようにする
C. トラフィックを分類し、洞察を提供する
D. SNMPやその他のポーリングツールを使用して監視を効率化する

答え B
＊ネットワーク自動化は、ベンダーに依存しない方法で構成やトポロジーを定義する。

問題75　ネットワーク運用における生成 AI の機能は何ですか？
A. 人工的なネットワーク構成を作成します
B. ネットワークのファームウェア更新を適用します
C. 使用されていないサービスを無効にします
D. 最適なデータストレージソリューションを計算します

答え A
＊生成AIは、ネットワーク環境における新しい構成の作成、プロセスの自動化、様々なシナリオのシミュレーションなどを行うことができます。

問題76　組織は新しいセキュリティポリシーを策定し、そのポリシーを印刷して全従業員に配布し、従業員がポリシーを確認し適用するように決定しました。この組織が実施しているセキュリティプログラムの要素はどれですか？
A. 資産の特定
B. ユーザートレーニング
C. 物理的アクセス制御
D. 脆弱性制御

答え B
＊【補足】ユーザートレーニングは定期的に実施することが望ましい。

問題77　WLCで利用される機能のうち、その配布システムポートを1つの802.3adグループに束ねることを可能にするものはどれですか？
A. QinQ
B. ISL
C. PAgP
D. LAG

答え D
＊802.3ad＝LACP (Link Aggregation Control Protocol)、"束ねる"→LAG

問題78　このJSONスキーマ内の「switch」という単語は何を表していますか？

```
1  [
2  {"IDS": "IPS22", "port":"te3/46"},
3  {"load balancer": "LB12", "port":"te6/38"},
4  {"switch": "SW18", "port":"ge2/41"},
5  ]
```

A. 配列
B. 値
C. キー
D. オブジェクト

答え C
＊"key":"値"、オブジェクト{}、配列[]

問題79　SSIDで使用される文字の最大長はどれですか？
A. 16
B. 32
C. 48
D. 64

答え B
＊【丸暗記】SSIDは最長32文字

問題80　次のうち、コンテナにおける仮想化を説明するものはどれですか？
A. ホストOSが異なるCPUメモリプロセスを制御するタイプのOS仮想化です。
B. 物理的なコンピュータをエミュレートし、物理マシン上で複数のマシンと多くのOSを実行可能にします。
C. 仮想マシンを互いに分離し、メモリ、プロセッサ、ストレージを計算用に割り当てます。
D. ゲストOSとハードウェアの仮想パーティションをOS用に含み、アプリケーションライブラリが必要です。

答え A
＊コンテナはホストOSのカーネルを共有し、ゲストOSを必要としません。BやCはVMの説明です。

問題81　ネットワーク管理者がHSRPを実装する理由はなぜですか。
A. ルーターの故障時にネットワークの冗長性を確保するため
B. Ciscoとサードパーティのルーターで設定可能なオープン標準プロトコルを使用するため
C. ネットワーク内のホストがトラフィックのロードバランシング時に同じデフォルトゲートウェイの仮想IPを使用できるようにするため
D. クライアントに複数のデフォルトゲートウェイIPを設定できるようにするため

答え A
＊HSRP（Hot Standby Router Protocol）：シスコ独自のデフォルトゲートウェイを冗長化するためのプロトコル。業界標準はVRRP (Virtual Router Redundancy Protocol)。

問題82　既存のPort-Channel1バンドルに新しいメンバーとして別の物理インターフェースを追加します。新しいインターフェースに設定する必要があるコマンドセットはどれですか？

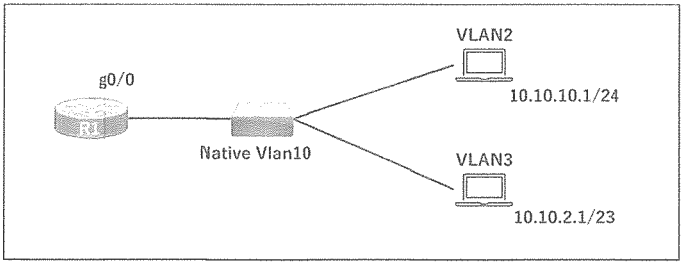
```
SW1#show etherchannel summary
Flags:   D - down        P - in port-channel
         I - stand-alone  s - suspended
         H - Hot-standby (LACP only)
         R - Layer3       S - Layer2
         U - in use       f - failed to allocate aggregator
         u - unsuitable for bundling
         w - waiting to be aggregated
         d - default port
         A - formed by auto LAG
Number of channel-groups in use: 1
Number of aggregators: 2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1 (RU)         LACP      Et0/0(P)    Et0/1(P)
```

A. switchport mode trunk
　channel-group 1 mode active
B. no switchport
　channel-group 1 mode active
C. no switchport
　channel-group 1 mode on
D. switchport
　switchport mode trunk

答え B
＊1番下の行（1）には、「RU」と記載があります。Flagsを見ると、Rは、Layer3であると記載されています。つまり、「no switchport」でL3モードにしてから追加します。LACPなので、active/passiveです。

問題83　スイッチとPCの設定は完了しています。VLAN 2とVLAN 3が相互に通信できるようにするには、どの設定を適用しますか。



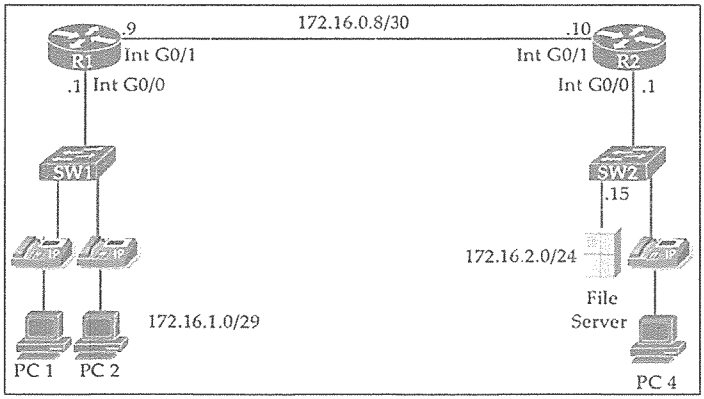
0

```
R1#show run
...
interface GigaEthernet0/0.2
 encapsulation dot1Q 2
 ip address 10.10.10.10 255.255.255.0
```

A. interface GigabitEthernet0/0
　ip address 10.10.2.10 255.255.252.0
B. interface GigabitEthernet0/0.3
　encapsulation dot1Q 10
　ip address 10.10.2.10 255.255.255.252
C. interface GigabitEthernet0/0.10
　encapsulation dot1Q 3
　ip address 10.10.2.10 255.255.254.0
D. interface GigabitEthernet0/0.3
　encapsulation dot1Q 3 native
　ip address 10.10.2.10 255.255.252.0

答え C
＊普通はBやD「0/0.3」のようにVLAN番号と合わせるので、イジワルな問題である。/23→.254でも解ける。

問題84　PC1が 172.16.2.0/24 に接続できません。どの設定変更が問題を解決しますか。




```
IPv4 Address. . . . . . . . . . . : 172.16.1.8(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.240
Default Gateway . . . . . . . . . : 172.16.1.1

DHCPv6 IAID . . . . . . . . . . . : 116155351
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-BE-0A-47-3C-15-AB-80-12-F6

DNS Servers . . . . . . . . . . . : 172.16.1.3,  172.16.1.4
```

A. IPアドレスを172.16.1.9に変更し、DNSサーバーを172.16.1.12のみに変更する。
B. IPアドレスを172.16.1.6に変更し、DNSサーバーを172.16.1.12と172.16.1.13に変更する。
C. IPアドレスを172.16.1.9に変更し、デフォルトゲートウェイを172.16.1.7に変更する。
D. IPアドレスを172.16.1.6に変更し、サブネットマスクを255.255.255.248に変更する。

答え D
＊図には/29（.248）、ターミナル画面には「.240」と記載があり差異がある。
＊図（/29＝.248）を正として、設定しなおします。/29にすると、有効IPは 172.16.1.1～6になるため、「.6」に変更することも問題ないです。