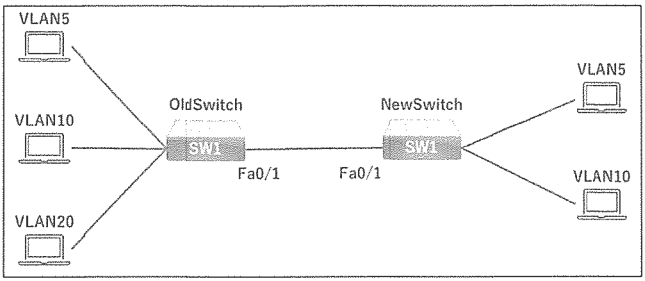
Part13

問1　新しい VLAN とスイッチがネットワークに追加されます。リモート エンジニアは OldSwitch を構成し、構成が次の要件を満たしていることを確認する必要があります。リンクの NewSwitch 側のどの構成がこれらの要件を満たしていますか。

・現在構成されている VLAN に対応する
・範囲を拡張して VLAN 20 を含める
・仮想 LAN の IEEE 標準サポートを可能にする




```
OldSwitch(config)#interface fastEthernet0/1
OldSwitch(config-if)#switchport mode trunk
OldSwitch(config-if)#switchport trunk allowed vlan 5,10
OldSwitch(config-if)#switchport trunk native vlan 15

NewSwitch(config)#interface fastEthernet0/1
NewSwitch(config-if)#switchport mode trunk
NewSwitch(config-if)#switchport trunk encapsulation isl
NewSwitch(config-if)#switchport trunk allowed vlan 5,10
NewSwitch(config-if)#switchport trunk native vlan 15
```

A.
no switchport trunk encapsulation isl
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 20
B.
switchport nonnegotiate
no switchport trunk allowed vlan 5,10
switchport trunk allowed vlan 5,10,15,20
C.
no switchport mode trunk
switchport trunk encapsulation isl
switchport mode access vlan 20
D.
switchport mode dynamic
channel-group 1 mode active
switchport trunk allowed vlan 5,10,15,20

答え: A
＊OldSwitchではVLAN5,10の設定がされています。カプセルタイプは記載がありませんが、おそらく802.1Q（dot1q、デフォルト）であると推測されます。NewSwitchはカプセルタイプがISLとなっております。ISLは802.1Qより古い規格のもので、この2つ同士ではトランクリンクは形成されません。解決方法として、AのようにISLを無効化し、 802.1Qで設定します。そして、不足しているVALN20を追加してあげます。

問2　[IPv6]ドラッグアンドドロップ

答え：
マルチキャスト
・単一のアドレスではなくグループアドレスにパケットを送信
・ユニキャストソースがグループに送信される
エニーキャスト
・非ホストデバイスによって排他的に使用される
・アドレスを持つ最も近いインターフェースにルーティングされる

＊IPv6アドレス：ユニキャスト（1対1）、マルチキャスト（1対多）、エニーキャスト（複数のデバイスが同じアドレスを持つ、最も近い1台にのみ送信される）。"ユニ（1台）キャストソースがグループ（複数）に送信される"、"非ホストデバイスによって排他的に使用される（PCではなく、例えばDNSサーバで実装される）"

問3　[IPv6]ドラッグアンドドロップ

答え：
グローバルユニキャストアドレス
・ルーティングプレフィックスの集約が可能
・インターネット経由でルーティングおよび到達可能
マルチキャスト
・1対多の通信を提供
・ユニキャストソースをグループに送信

＊グローバルユニキャストアドレスは、IPv4でいうところのグローバルIPアドレス。

問4　スイッチ上でフレームスイッチングはどのように機能しますか。
A. CDP を使用してフレームを隣接ポートに転送する
B. 既知の送信元 VLAN を含むフレームを変更する
C. 不明な宛先からのフレームを検査してドロップする
D. 既知の宛先を宛先ポートに転送する

答え: D
＊A.隣接情報を取得するためにCDPやLLDPを使用するが、フレーム転送のためではない。C.未知の宛先MACアドレスがきたら、基本的にはフラッディングします。

問5　個々のネットワーク エンドポイントを攻撃から保護するためのソリューションとして何が使用されていますか。
A. ルーター

B. ワイヤレス コントローラー
C. ウイルス対策ソフトウェア
D. Cisco DNA Center

答え: C
＊C以外は保護と関係がない

問6　SW1 と SW2 の間に LACP EtherChannel を構築します。show コマンドを実行しました。スイッチが LACP ポートチャネルの 2番目のメンバーを正常にバンドルするには、どのタスクを実行しますか。


```
SW1#show run interface fastEthernet0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 100,200,300
  channel-group 1 mode active

SW1#show run interface fastEthernet0/2
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  channel-group 1 mode active

SW2#show run interface fastEthernet 0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 100,200,300
  channel-group 1 mode active

SW2#show run interface fastEthernet 0/2
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 100,200,300
  channel-group 1 mode active
```

A. SW1のポートチャネル1に「switchport trunk allowed vlan 300」コマンドを設定します
B. SW1 のFa0/2 で「switchport trunk allowed vlan add 300」コマンドを設定します
C. SW2 のFa0/2 で「switchport trunk add vlan add 300」コマンドを設定します
D. SW1 のポートチャネル 1に「switchport trunk allowed vlan add 300」コマンドを設定します

答え: B
＊"2番目のメンバー"とは、Fa0/2を指す。
＊SW1のFa0/2だけ、VLAN300が足りていないという状況。
＊A.D.ポートチャネル1がうまく設定されていない（VLAN不一致でエラーになる）ので無効。

＊C.存在しないコマンド。

問7　REST ベースの API によって実行されるアクションに適した HTTP メソッドはどれですか。(2つ選択)
A. REMOVE
B. REDIRECT
C. POST
D. GET
E. POP

答え: C,D
＊POST,GET,DELETE,PUT

問8　ワイヤレス LAN コントローラとレイヤー 2 スイッチ間の接続冗長性、帯域幅の増加、負荷分散を実現するものは何ですか。
A. VLAN トランキング
B. トンネリング
C. ファーストホップ冗長性
D. リンクアグリゲーション

答え: D
＊業界標準はLACP、シスコ規格はPAgP

問9　[IPv6]ドラッグアンドドロップ

答え：
グローバルユニキャストアドレス
・1対1の通信を提供
・IPv4アドレスと同じようにパブリックにルーティング可能
ユニークローカル
・アドレス競合なしでサイトを結合できる
・プライベート IPv4 アドレスに相当する

＊アドレス競合なしでサイトを結合できる：IPv4のプライベートIPアドレスでは、複数のNWを結合しようとしたときに、10.～や172.～などアドレスの重複が起こることがある。その点、IPv6のユニークローカルは、一意なアドレスになる仕組みであるため、重複が起こらない。

問10　Cisco WLC で LAG 設定が更新された場合、変更が完了したらどの追加タスクを実行しますか。
A. WLCからすべてのMACアドレスをフラッシュする
B. WLC とアクセスポイントを再度関連付けます
C. WLC インターフェイスを再度有効にします
D. WLC を再起動します

答え: D
＊有効化/無効化/設定変更した場合、設定を反映させるにはコントローラの再起動が必須です。

問11　エッジ デバイスまたはアクセス回線に障害が発生した場合に、トラフィックが即座に、透過的に、自動的に回復することを保証する Cisco 独自のプロトコルはどれですか。
A. SLB
B. FHRP
C. VRRP
D. HSRP

答え: D
＊デフォルトゲートウェイを冗長化させるプロトコルとして、HSRP、VRRP、GLBPがあります。これらを総称として FHRP（ First Hop Redundancy Protocol ）と呼びますが、"シスコ独自"はHSRPやGLBPです。

問12　[IPv6]ドラッグアンドドロップ

答え：
グローバルユニキャストアドレス
・IPv4アドレスと同じようにパブリックにルーティング可能。
・1対1の通信が可能

リンクローカルアドレス
・ネクストホップアドレスとして機能する
・すべてのIPv6デバイスに必要

＊まず、外向け用／内向け用ということを理解します。リンクローカルは、自動で(勝手に)割り当てられます。同じNW内であれば、ネクストホップアドレスとして機能します。

問13　WPA3 に実装された拡張機能とは何ですか。
A. アクセス ポイントを識別するために PKI と RADIUS を採用する
B. 802.1x 認証と AES-128 暗号化を適用する
C. TKIP とパケットごとのキーイングを使用する
D. 認証解除攻撃と関連付け解除攻撃から防御する

答え: D
＊WPA3：SAE、前方秘匿性（解読防止）、PMF（管理フレーム）の暗号化。PMF（管理フレーム）の暗号化とは、Dの説明のとおりです。攻撃を受けると、APとの接続が遮断されたりしてしまいます。

問14　リンクローカル 全ノード IPv6 マルチキャスト アドレスとは何ですか。
A. ff02:0:0:0:0:0:0:1
B. 2004:31c:73d9:683e:255::
C. fffe:034:0dd:45d6:789e::
D. fe80:4433:034 :0dd::2

答え: A
＊FF02::1は同じリンク上の全てのノード、FF02::2は同じリンク上の全てのルータ。B.グローバル、C.存在しない、D,リンクローカルユニキャスト（1対1）

問15　2001:db8::/64 を EUI-64 IPv6 インターフェイス アドレスにした形式はどれですか。

```
GigabitEthernet1 is up, line protocol is up
Hardware is CSR vNIC, address is 5000.0004.0000 (bia 5000.0004.0000)
Internet address is 192.168.1.1/24
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, 1000Mb/s, link type is auto, media type is RJ45
```

A. 2001:db8::5000:0004:5678:0090/64
B. 2001:db8:4425:5400:77ff:fe07:/64
C. 2001:db8::5000:00ff:fe04:0000/64
D. 2001:db8::5200:00ff:fe04:0000/64

答え: D
＊EUI-64：MACアドレス（5000.0004.0000）の真ん中にFFFEを挿入し、7ビット目を反転させる。
5000 0004 0000→5000 00FF FE04 0000→5200 00FF FE04 0000　＊16進数
先頭の50「0101 0000」→7ビット目を反転「0101 0010」→52　＊2進数

問16　フルメッシュ トポロジの 2つの欠点は何ですか。(2つ選択)
A. サイト間で高い MTU が必要
B. 実装コストが高くなる
C. ポイントツーポイント通信が必要
D. 複雑な構成が必要
E. サイト間では BGP でのみ動作する

答え: B,D
＊フルメッシュ：すべてが接続されている状態。他のトポロジ（スター、メッシュ、スパイン＆リーフなど）も含め、絵で理解しておくと良い。

問17　[IPv6]ドラッグアンドドロップ

答え：
グローバルユニキャストアドレス
・1対1の通信を提供
・インターネット経由でルーティングおよび到達可能
リンクローカルアドレス
・単一のリンクに限定
・ネクストホップアドレスとして機能する

問18　スイッチ上で MAC 学習はどのように機能しますか。
A. キューイングせずにすべてのポートにフレームをブロードキャストする
B. 不明な送信元 MAC アドレスをアドレス テーブルに追加する
C. 新しいフレームを受信すると再送信要求を送信する
D. 宛先が不明なフレームをマルチキャスト グループに送信する

答え: B
＊スイッチは受信したフレームの送信元MACアドレスと受信ポートを関連付けてMACアドレステーブルに登録します。A.送信元にはフレームは送られない

問19　QoS でネットワーク トラフィックを分類する目的は何ですか。
A. クラスに応じてトラフィックを処理する
B. 特定の処理を受けるトラフィックの種類を識別する
C. パケットのクラス識別子をパケット ヘッダーの専用フィールドに書き込む
D. ネットワーク デバイスでトラフィック マッチング ルールを構成する

答え: B
＊Aと迷いますが、"分類する目的は？"なので処理することが目的ではない。

問20　プライベート IPv4 アドレスを使用する利点は何ですか。
A. 複数の企業が競合することなく同じアドレスを使用できる。
B. 企業ネットワークの外部から内部ホストに直接接続できる。
C. NATを使用せずにインターネットへの通信が可能。
D. すべての外部ホストにインターネットへの安全な通信が提供される。

答え: A
＊似た表現として「アドレスの枯渇対策」がある。その他、セキュリティ確保の観点もある。

問21　SDN ネットワーク内でコントロール プレーンとデータ プレーンを分離する利点は何ですか。
A. ネットワーク全体の複雑さを軽減する
B. データクエリをコントロールプレーンに制限する
C. コストを削減する
D. 仮想マシンの作成をデータプレーンにオフロードする

答え: A
＊"SDNコントローラとNW機器たち"という構成です。一元管理できる。

問22　[デバイス管理]ドラッグアンドドロップ

答え：
Cisco DNA Center
・オーバーレイおよびアンダーレイ構成
・ルーティングされたアクセスの展開
・VXLAN および LISP 構成
従来型
・STP 展開
・VLAN および HSRP 構成
・コンソール経由の構成

＊SDNトポロジと旧トポロジでの比較です。"ルーティングされた～"は、各スイッチまでL3レイヤーを用いるためSTPが不要であることを指しています。「オーバレイ,VXLAN,ポリシーベースで,柔軟に,一元管理,GUIで直感的に」あたりはSDNとお考えください。

問23　ファーストホップ冗長プロトコルが実装されるのはなぜですか。
A. デフォルトゲートウェイの障害から保護するため
B. ネットワーク内のループを防ぐため
C. 複数のスイッチを単一のユニットとして動作できるようにするため
D. マルチリンクセグメントの負荷分散を提供するため

答え：A
＊FHRPは、HSRP/VRRP/GLBPといったデフォゲ冗長化プロトコルの総称です。D.負荷分散もありますが、主な目的は障害対策です。

問24　どの WPA モードが PSK 認証を使用しますか。
A. ローカル
B. クライアント
C. エンタープライズ
D. パーソナル

答え：D
＊PSK認証とは一般家庭で用いられる事前共有PWのこと。"Pre-Shared Key"

問25　[AAA]ドラッグアンドドロップ

答え：
アカウンティング
・ユーザーがリモートサーバー上のネットワークにアクセスした時間の長さを記録します
・TACACS+を使用して、ネットワーク管理者が入力した設定コマンドを記録します
認可
・デバイスがユーザーまたはグループベースのアクセスを許可できるようにします
・ユーザーが実行できる CLI コマンドを制限します

＊AAA：認証(ログイン)、認可(権限付与)、アカウンティング(記録)。問24と異なり個人単位で設定されます。企業NW＝エンタープライズで用いられることが多いです。

問26　コラプスドコア アーキテクチャにおけるコア層とディストリビューション層の機能は何ですか。
A. ルーターはレイヤー3でIPv4とIPv6アドレスを使用する必要があります。
B. コアレイヤーとディストリビューションレイヤーは、フェイルオーバーを可能にするために、2つの異なるデバイス上に配置されます。
C. ルーターは、IPv6ネットワークのレイヤー2冗長化のためにHSRPをサポートすることができます。
D. ルーターは、単一デバイスまたは冗長ペア上で動作します。

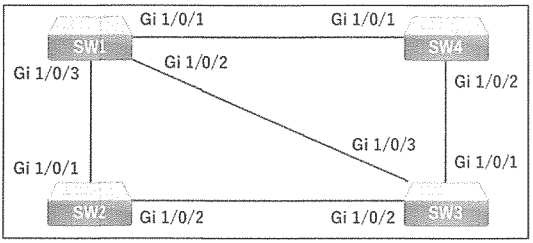
答え：D
＊コラプスドコア アーキテクチャとは2階層NWのこと。中小企業向けのNW構成です。大企業（大規模）NWであれば、コア層/ディストリビューション層/アクセス層という3階層NWになります。コラプスドコア（Collapsed Core＝崩壊したコア層）では、コア層がありません。厳密にはコア層とディストリビューション層が統合されています。このとき、コア層やディストリビューション層にあるルーターは1つ（または冗長構成で2つ）にまとめられるため、"単一デバイス"という表現がされています。

問27　[IPv6]ドラッグアンドドロップ

答え：
グローバル ユニキャスト　：3ffe:e54d:620:a87a::f00d
リンク ローカル ユニキャスト　：fe80::a00:23ff:feeb:89aa
マルチキャスト　：ff05::1:3
ユニーク ローカル　：fd6d:c83b:5cef:b6b2::1

＊鉄剣リンク（fe）、皆に知らせるファンファーレ（ff）、ユニークなフレンド（fd）

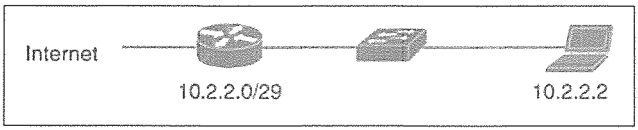
問28　どのスイッチがルートブリッジになりますか。



A. SW 1
　Bridge Priority – 32768
　mac-address 0fd7:9e:13:ab:82
B. SW 4
　Bridge Priority – 40960
　mac-address 05:d8:33:09:8f:89
C. SW3
　Bridge Priority – 32768
　mac-address 01:1c:6c:66:b7:70
D. SW2
　Bridge Priority – 40960
　mac-address 04:44:97:51:63:17

答え: C
＊ルートブリッジは優先度がMACアドレスが小さい方、OSPF(DR/BDR)はルータIDが大きい方。

問29　新しく設定された PC が、TCP ポート 80 を使用して www.cisco.com にインターネット接続できません。接続を機能させるには、どの設定を変更しますか。

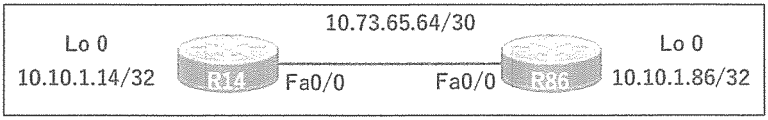


```
C:¥>ipconfig /all
Ethernet adapter Ethernet:
   Connection-specific DNS Suffix  . :
   Physical Address. . . . . . . . . . . : F8-75-A4-3B-AB-4F
   Link-local IPv6 Address . . . . . . . : fe80::644a:b01:3e5f:ae6%14(Preferred)
   IPv4 Address. . . . . . . . . . . . . : 10.2.2.2(Preferred)
   Subnet Mask . . . . . . . . . . . . . : 255.255.255.248
   Default Gateway . . . . . . . . . . . : 10.2.2.10
   DHCP Server . . . . . . . . . . . . . : 0.0.0.0
   DNS Servers . . . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . . . : Enabled
```

A. サブネットマスク
B. DNSサーバー
C. デフォルトゲートウェイ
D. DHCPサーバー

答え: C
＊デフォゲの設定が誤っている。10.2.2.0/29であれば、10.2.2.1～6 の範囲で設定可能。ただし、2はPCで使われているため不可。

問30　すべてのインターフェイスは、duplex auto および ip ospf network broadcast で設定されています。どの設定により、R14 と R86 が OSPFv2 隣接関係を形成し、ルータ間で OSPF 情報を交換するための中心点として機能できるようになりますか。



A.

```
R14#
interface FastEthernet0/0
ip address 10.73.65.65 255.255.255.252
ip ospf priority 0
ip mtu 1500

router ospf 10
router-id 10.10.1.14
network 10.10.1.14 0.0.0.0 area 0
network 10.73.65.64 0.0.0.3 area 0

R86#
interface FastEthernet0/0
ip address 10.73.65.66 255.255.255.252
ip mtu 1500

router ospf 10
```

```
router-id 10.10.1.86
network 10.10.1.86 0.0.0.0 area 0
network 10.73.65.64 0.0.0.3 area 0
```

B.

```
R14#
interface Loopback0
ip ospf 10 area 0

interface FastEthernet0/0
ip address 10.73.65.65 255.255.255.252
ip ospf priority 255
ip ospf 10 area 0
ip mtu 1500

router ospf 10
router-id 10.10.1.14

R86#
interface Loopback0
ip ospf 10 area 0

interface FastEthernet0/0
ip address 10.73.65.66 255.255.255.252
ip ospf 10 area 0
ip mtu 1500

router ospf 10
router-id 10.10.1.86
```

答え: B
＊"中心点として"とのこと、DRの設定のことを指している。プライオリティは255が最大であり、問題の意図として合っている。また、10.73.65.64/30 は、第4オクテッドは65，66どちらかになる。64はNWアドレス、67はブロードキャストアドレスであり使用不可。【実践】255と64,65を探す

問31　[ケーブル タイプ]ドラッグアンドドロップ

答え：
シングルモードファイバー:
・単一の光波長を使用
・コア径は9ミクロン
マルチモードファイバー:
・複数の光波長を使用
・長距離では減衰が増加する

＊光ケーブルのシングル（SMF）とマルチ（MMF）の違いです。シングルは細いトンネル（径）、マルチは複数の光信号を通すため太いトンネルが使用されます。マルチはコア径が太いため、距離が長くなるほど光信号（波長）が減衰します。

問32　10.200.0.2 経路のフローティングスタティックルートを設定します。
A. ip route 0.0.0.0 0.0.0.0 10.200.0.2 floating
B. ip route 0.0.0.0 0.0.0.0 10.200.0.2
C. ip route 0.0.0.0 0.0.0.0 10.200.0.2 10
D. ip route 0.0.0.0 0.0.0.0 10.200.0.2 1

答え: C
＊プライマリがダウンしたときにのサブ経路のこと。10はAD値。静的に登録したスタティックルートのADは1なので、2以上で設定するのが正しい。（AD値の小さい方が優先される＝大きい方はサブとなる）

問33　宛先ネットワークにトラフィックを送信するために使用されるインターフェースはどれですか。

```
D 10.87.161.30/27 [90/10331] via G0/17
D 10.87.161.30/27 [90/44594] via G0/8
O 10.87.161.30/27 [110/7820] via G0/24
O 10.87 161.30/27 [110/7879] via G0/1
```

A. G0/1
B. G0/8
C. G0/24
D. G0/17

答え: D
＊[AD値/メトリック]。AD値が小さい経路が優先される。同じときはメトリックが小さい経路。

問34　R1 は 172.16.1.4 /30 へのトラフィックをどのように処理しますか。

```
R1# show ip route
C    172.16.0.0/16 is directly connected, Loopback0
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O       172.16.1.3/32 [110/100] via 10.0.1.100, 00:39:08, Serial0
O       172.16.1.9/32 [110/5] via 172.16.1.50, 00:43:01, Gigabit Ethernet 0/0
D       172.16.1.4/30 [90/7445] via 172.16.9.5, 00:39:08, Gigabit Ethernet 0/0
                      [90/7445] via 172.16.4.4, 00:39:08, Gigabit Ethernet 0/4
```

A. 172.16.4.4経由ですべてのトラフィックを送信します。
B. 10.0.1経由ですべてのトラフィックを送信 100
C. 172.16.4.4をバックアップとして使用し、172.16.9.5経由のパスですべてのトラフィックを送信します。
D. 172.16.9.5と172.16.4.4経由のトラフィックを負荷分散します。

答え: D
＊[AD値/メトリック]が同じであるとき、負荷分散（ロードバランシング）します。

問35　[IPv6]ドラッグアンドドロップ

答え：
エニーキャスト
・同じネットワーク上の複数のデバイスに同時に割り当てられる
・アドレスを持つ最も近いインターフェースにルーティングされる
マルチキャスト
・送信元アドレスとして使用できない
・1対多の通信を提供する

＊【易】素直に回答できそう

問36　ワイヤレス ネットワークの SSID の特徴は何ですか。
A. 権限のないユーザーを防ぐためにポリシーを使用する
B. WLAN 上のアクセス ポイントを識別する
C. ユーザーにログイン ID を要求する
D. WLAN に名前を関連付ける

答え: D
＊予備知識）SSIDには、BSSIDとESSIDがあります。一般的にSSIDと言うときはESSIDを指しています。試験でも"ESSID"で出題されることがあります。

問37　この JSON スキーマ内の「port」という単語は何を表していますか。

```
1  [
2  {"IDS": "IPS_pittsburgh", "port":"te8/30"},
3  {"router": "R20", "port":"ge9/23"},
4  {"firewall": "FW42", "port":"fe3/24"},
5  ]
```

A. バリュー
B. 配列
C. キー
D. オブジェクト

答え: C
＊[]は配列、{}はオブジェクト、{“key” : “value”}

問38　[IPv6]ドラッグアンドドロップ

答え：
・グローバル ユニキャスト: 2000:1092 :a1e8:827d:527c:3ce7:9816:1
・リンク ローカル ユニキャスト: fe80:cc72:4b9e:445c:8179:0420:5988:7
・マルチキャスト: ff00:ec6c:dbb1:3e8b:6d46:bd27:a236:12
・ユニーク ローカル: fc00:9860:653f:5146:8cb2:a27c:cb6f:3

＊【丸暗記】IPv6のグローバルは2000で始まる、リンクローカルはfe80、マルチキャストはff、ユニークローカルはfcまたはfd。

問39　[ケーブル タイプ]ドラッグアンドドロップ

答え：
銅:
・導体、ベッド、シースを含みます
・通常は小規模オフィスの用途で使用されます
シングルモードファイバー:
・整合性の損失がほとんどなく、長距離に最適
・単一の光波長を使用

＊銅線（LANケーブル）と光ケーブルの比較。導体＝電流を通すもの＝ここでは銅線のこと。ベッドは絶縁体、シースは外皮を指す。

問40　この JSON スキーマ内の単語「ge3/36」は何を表していますか。

```
1 [
2 {"VPN concentrator": "VPN36", "interface":"ge3/36"},
3 {"load balancer": "LB33", "interface":"te7/10"},
4 {"switch": "SW31", "interface":"fe2/25"},
5 ]
```

A. 値
B. 配列
C. キー
D. オブジェクト

答え: A
＊"key":"値"、オブジェクト{}、配列[]

問41　[IPv6]ドラッグアンドドロップ

答え：
ユニークローカル
・インターネット上でルーティングできない
・アドレスの競合なしにサイトを結合できる
マルチキャスト
・ユニキャストのソースがグループに送られる
・単一のアドレスではなく,グループアドレスにパケットを送信する。

＊"アドレスの競合なしに"：ユニークローカルはIPv4のプライベートIPアドレスと言われることがあるが、仮に拠点Aと拠点Bで同じような172.16.x.x/24が存在したとしても、IPv6のユニークローカルアドレスは、重複しない仕組みになっている。"ユニキャストのソースが"：ユニキャストとは1:1の通信であるが、それが複数存在することでマルチキャスト（1:多）を実現しているということ。"グループアドレスに"：宛先をff～にして

問42　無線ネットワークにおける暗号化の特徴は何ですか。
A. 権限のないユーザーを防ぐためのポリシーを使用する
B. ネットワークを通過するデータの傍受を防止する
C. スパイウェアに対する保護を強化する
D. 電流を電波に変換する

答え: B
＊トラフィックを暗号化する理由：傍受＝盗聴の防止

問43　プライベート IPv4 アドレスの特徴は何ですか。
A. PCI 規制に準拠
B. 外部リソースにのみデータをストリーミングする内部ホストで使用される
C. インターネットの脅威に対する保護レベルが強化される
D. インターネット経由での安全な接続が可能

答え: C
＊アドレスの枯渇対策、セキュリティ強化（インターネットから直接参照されない）

問44　宛先ネットワークにトラフィックを送信するために使用されるインターフェースはどれですか。

```
D 10.214.247.237/28 [90/2170] via G0/12
D 10.214.247.237/28 [90/46985] via G0/19
O 10.214.247.237/28 [110/665] via G0/9
O 10.214.247.237/28 [110/3399] via G0/1
```

A. G0/12
B. G0/1
C. G0/9
D. G0/19

答え: A
＊[AD値/メトリック]。AD値が小さい経路が優先される。同じときはメトリックが小さい方。

問45　宛先ネットワークにトラフィックを送信するために使用されるインターフェースはどれですか。

```
O 10.139.120.253/29 [110/9443] via G0/20
O 10.139.120.253/29 [110/29560] via G0/16
R 10.139.120.253/29 [120/12] via G0/11
R 10.139120 253/29 [120/6] via G0/9
```

A. G0/11
B. G0/20
C. G0/9
D. G0/16

答え: B
＊[AD値/メトリック]。AD値が小さい経路が優先される。同じときはメトリックが小さい方。

問46　[ケーブルタイプ]ドラッグアンドドロップ

答え：
マルチモードファイバー
・長さが長くなると歪む
・通常はデータセンター内部の接続に使用されます
シングルモードファイバー

・コアを通過する際の光の反射が最小限に抑えられる
・単一の波長の光を使用する

＊問31参照　シングル：1人用道路で狭い、マルチ：太い道路で交通量も多い。

問47　ワイヤレス ネットワークの SSID の特徴は何ですか。
A. デフォルトでビーコン信号をブロードキャストして存在を知らせる
B. 権限のないユーザーを防ぐためのポリシーを使用する
C. 電流を電波に変換する
D. ユーザーにログイン ID の入力を求める

答え: A
＊ビーコンフレーム：SSIDや暗号化タイプを乗せたフレームのこと。APが一定の時間間隔でビーコンフレーム（信号）を発信している。

問48　P2P Blocking Action オプションは 無効になっています。キャンパス内をクライアントが移動するときに、各クライアントが割り当てられた IP アドレスを保持するための設定はどれですか？
A. P2P Blocking ActionオプションをForward-Up Streamに設定する
B. Static IP Tunneling オプションを有効にする
C. DHCP Addr. Assignment チェックボックスをオンにする
D. Coverage Hole Detection オプションを無効にする

答え: B
＊序文の「P2P～います。」は混乱するだけの不要な情報。問題文の「 IP アドレスを保持」から、「Static IP」が連想できる。

問49　[トランスポート層のプロトコル]ドラッグアンドドロップ

答え：
TCP
・パケットの配信を保証
・32 ビットのシーケンス番号を使用
・失われたパケットの再送信をサポート
UDP
・音声トラフィックに最適
・パケット内のオーバーヘッドが最小限
・必要なコンピュータリソースが少ない

＊TCP：信頼性優先、UDP：速度優先（音声、ビデオ電話、SNMP、NTPなど）
＊シーケンス番号とはパケットの完全性を検証するためのもの。TCPが連想される。

問50　企業が社内でネットワーク自動化を選択する理由は何ですか。
A. データサービスをより速く提供する
B. ネットワークのセグメンテーションを可能にする
C. スパニングツリーのループ回避を緩和する
D. きめ細かいQoSを実装する

答え: A
＊効率化、人的ミス防止、コストダウン。

問51　パケットの宛先は 172.16.32.8 です。優先するルートのサブネットマスクはどれですか。

```
router# show ip route
...
D       172.16.32.0/26 [90/25789217] via 10.0.0.1
R       172.16.32.0/24 [120/4] via 10.0.0.2
O       172.16.32.0/19 [110/229840] via 10.0.0.3
C       172.16.32.32/32 is directly connected, Loopback0
C       172.16.32.4/30 is directly connected, GigabitEthernet0/0
```

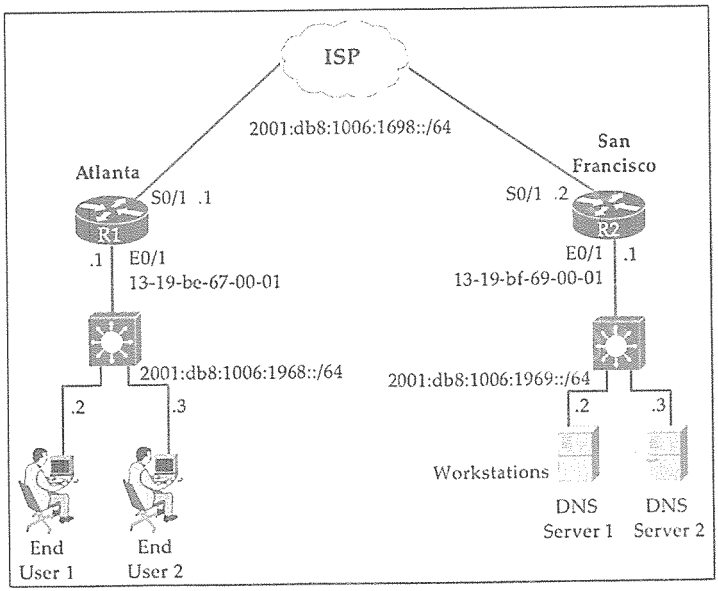
A. 255.255.224.0
B. 255.255.255.0
C. 255.255.255.192
D. 255.255.255.252

答え: C
＊8は4ビット必要です（1+2+4+8..から、3ビットだと7、4ビットだと15）。つまり32-4で/28が最適解です。showコマンドの中に/28はないため、/27、それがなければ/26、それがなければ/25..が正解になります。/26があるためこれが正解です。
＊【慣れ】/26は192（128+64）です。

問52　Cisco Unified Wireless Network アーキテクチャでアウトオブバンド管理を提供する WLC インターフェイスはどれですか。
A. ダイナミック
B. AP マネージャー
C. 仮想
D. サービスポート

答え: D
＊アウトオブバンド管理：通常時のデータトラフィックではない経路で行われるデバイス管理のこと。初期セットアップやトラブルシュート時に使用します。なお、通常のデータトラフィック経路での管理をインバンド管理といいます。

問53　R1の LAN セグメントの IPv6 アドレスをEUI-64 形式を使用して設定すると、どの IPv6 アドレスが生成されますか。



A. 2001:db8:1006:1968:4564:877F:FE99:1
B. 2001:db8:1006:1968:1119:BEFF:FE67:1
C. 2001:db8:1006:1968:1130:ABFF:FECC: 1
D. 2001:db8:1006:1968:12D8:BAFE:FF01:1

答え: B
＊【慣れ..】EUI形式：①NWアドレスのプレフィックス64ビット＋②EUI-64使用のMACアドレス64ビット。①は2001:db8:1006:1968です。②は、MACアドレスの真ん中にFFFEを挿入して7ビット目を反転させます。「13-19-be-67-00-01」→「13-19-be-FF-FE-67-00-01」→「11-19-be-ff-fe-67-00-01」（13：0001 0011→11：0001 0001）

問54　パケットの宛先がセキュリティ終端ポイントと異なる場合、どの IPsec 暗号化モードが適切ですか。
A. トンネル
B. メイン
C. アグレッシブ
D. トランスポート

答え: A
＊【難】"セキュリティ終端ポイントと異なる"とは、ホストA→VPNルータA→VPNルータB→ホストBを構成としたとき、ホストA→ホストBの通信を指しています（ホストA→VPNルータBではないということ）。経路にセキュリティ終端装置が存在していればトンネルモード。存在しなければトランスポートモード。

問55　VoIP などの低遅延を必要とするアプリケーションでは、なぜ UDP が TCP よりも適しているか。

A. UDPはすべてのパケットの配送を確実に保証し、TCPは高負荷時にパケットをドロップする。
B. TCPは効率的なパケット配送のために輻輳制御を使用し、UDPはパケット配送のためにフロー制御メカニズムを使用する。
C. UDPはパケットが順番に到着するようにシーケンスデータを使用し、TCPはパケットをランダムな順番で受信する機能を提供する。
D. TCPは受信したパケットごとに確認応答を送信し、UDPは確認応答なしで動作する。

答え: D
問49参照

問56　アプリケーションのパフォーマンスの問題、VoIP オーディオ品質の低下、ダウンロードの遅延が発生しています。問題の原因は何ですか。

```
Router# show interface FastEthernet0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 0017.59b2.7fb2 (bia 0017.59b2.7fb2) Internet address is
10.0.0.2/30
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:04, output 00:00:04, output hang sever
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1 Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 516000 bits/sec, 45 packets/sec
  5 minute output rate 516000 bits/sec, 46 packets/sec
    13282 packets input, 20075670 bytes
    Received 25 broadcasts, 0 runts, 0 giants, 0 throttles
    383 input errors, 383 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog
    0 input packets with dribble condition detected
    13438 packets output, 20084258 bytes, 0 underruns
    0 output errors, 831 collision, 5 interface resets
    11 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

A. QoS キューイング
B. インターフェース構成
C. ブロードキャスト ストーム
D. 過剰使用

答え: B

＊Half-duplex（半二重＝一方通行）に着目。対向がFull-duplex（全二重、二車線通行）であると考えられます。HalfとFullの通信はコリジョンの発生、スピードの低下など様々な問題が発生します。

問57　ルータOldR は、R2 とルートを交換する目的で、ネットワーク上の別のルータを置き換えています。エンジニアが最初の OSPF 設定を適用した後も、両方のデバイスでルートがまだ見つかりませんでした。ネイバー関係を有効にするために、clear IP ospf processコマンドを入力する前に、どのコマンドを発行しますか。

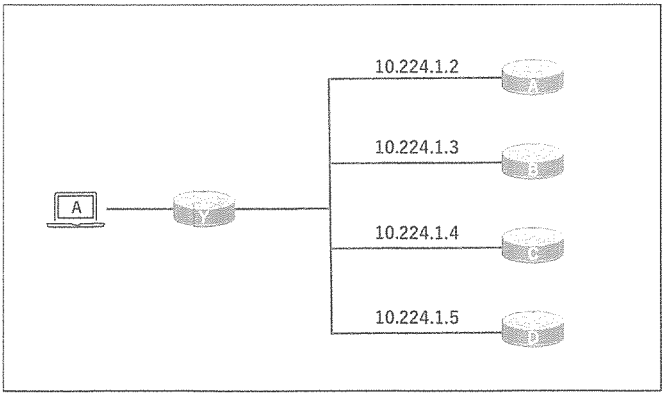
```
OldR#show ip ospf interface
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.1.2/24, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1 Transmit Delay is 1 sec,
State DROTHER, Priority 1
  Designated Router (ID) 192.168.1.1, Interface address 192.168.1.1
  Backup Designated Router (ID) 192.168.1.1, Interface address 192.168.1.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/1, flood queue length 0
  Neighbor Count is 1, Adjacent neighbor count is 2

R2#show ip ospf interface
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.1.1, Interface address 192.168.1.2
  Backup Designated Router (ID) 192.168.1.1, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 2/2, flood queue length 0
    Neighbor Count is 1, Adjacent neighbor count is 2
```

A. OldR(config)#router ospf 1
   OldR(config-router)#no router-id 192.168.1.1
B. OldR(config)#interface g0/0/0
   OldR(config-if)#ip ospf dead-interval 15
C. OldR(config)#interface g0/0/0
   OldR(config-if)#ip ospf hello-interval 15
D. OldR(config)#router ospf 1
   OldR(config-router)# network 192.168.1.0 255.255.255.0 area 2

答え: A
＊OldRとR2のルータIDが同じであり、エラーが発生しています。A.の実行によってOldRのルータIDは自身のインターフェースIPアドレスである192.168.1.2になるはずです。なお、clear IP ospf processコマンドを投入することで、OSPFプロセスがリセットされ、DR/BDRが再選出されます。

問58　PC A は 10.225.34.225 の別のデバイスと通信しています。ルータ Y はどのルータを経由してトラフィックをルーティングしますか。




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

10.0.0.0/8 is variably subnetted
B       10.0.0.0/8 [1/0] via 10.224.1.2
B       10.27.150.224/27 [20/0] via 10.224.1.3, 1w6d
S       10.128.0.0/9 [1/0] via 10.224.1.3
B       10.224.0.0/11 [20/0] via 10.224.1.5, 5d18h
B       10.224.0.0/15 [20/0] via 10.224.1.4, 5d18h
C       10.223.0.0/24 is directly connected, GigabitEthernet0/1
C       10.224.0.0/24 is directly connected, GigabitEthernet0/0
B       10.226.34.0/24 [20/0] via 10.224.1.5, 5d18h
```

A. ルータA
B. ルータB
C. ルータC
D. ルータD

答え: C
＊真ん中の「B」の2行が候補になりそう。BはBGP、正確にはeBGP（外部BGP）。
＊ロンゲストマッチ（よりサブネットが絞れている）の観点から、/15が正しい。
＊10.224.0.0/15 : 10.224.0.0 ～ 10.225.255.255

問59　すべてのクライアント トラフィックをワイヤレス コントローラ経由で転送するようにアクセスポイントを構成する必要があります。このタスクを実行するには、どのモードを有効にしますか。
A. ローカル
B. モニター
C. 自律
D. 不正検出

答え: A
＊【シンプル】APをローカルモードにします。

問60　STP のルートポートとは何ですか。
A. ルートブリッジに対する優先順位が最も高いポート
B. ルートブリッジが1つのLANセグメント上に正確に1つのポートを持つ場合にのみ選択されるポート
C. ルートブリッジに到達するためのコストが最も低いスイッチ上のポート
D. 別のスイッチ上の指定ポートにつながるルートスイッチ上のポート

答え: C
＊ルート、指定、非指定を図や要件で整理しましょう。
＊ざっくり、ルート(受取）、指定（送る）、非指定（受取重複回避）である。

問61　イーサネット フレームがスイッチ インターフェイス G0/1 に到着しましたが、宛先 MAC アドレスが MAC アドレス テーブルにありません。スイッチはフレームをどのように処理しますか。
A. ARPリクエストを送信し、宛先の特定を試みる。
B. 宛先をFFFF.FFFF.FFFFに更新する。
C. フレームをドロップし、送信ホストに通知する。
D. 残りのスイッチインタフェースからフレームをフラッディングします。

答え: D
＊G0/1以外にフラッディング

問62　どのような状況で、固有のローカル ユニキャスト サブネットではなく、グローバル ユニキャスト サブネットを実装しますか。
A. サブネットが組織内でのみ利用可能である必要がある場合
B. サブネットがルーティング可能である必要がない場合
C. サブネット上のアドレスがプライベート IPv4 アドレスと同等である必要がある場合
D. サブネットがインターネット経由でルーティング可能である必要がある場合

答え: D
＊グローバル＝外向け、ユニキャスト（1:1の通信）
＊つまり、どのようなときにプライベートIPではなく、グローバルIPを使うか？というシンプルな問題。

問63　IP ルーティング テーブルの内容を表示するために、route print コマンドの代わりに使用される Windows コマンドはどれですか。
A. netstat-n
B. ipconfig
C. ifconfig
D. netstat-r

答え: D
＊【難】network statistics、routing tableのこと

問64　Cisco OfficeExtend AP モードと FlexConnect AP モードの違いは何ですか。

A. FlexConnect では、AP に個人用 SSID を設定できますが、OfficeExtend では個人用 SSID はサポートされていません。
B. OfficeExtend は、WLC へのトラフィックの DTLS トンネリングをサポートしていません。FlexConnect は、DTLS を使用して WLC へのトラフィックをトンネリングします。
C. OfficeExtend は、すべてのトラフィックを WLC 経由でトンネリングし、FlexConnect は AP スイッチ ポートでクライアント トラフィックを終了します。
D. FlexConnect は、クライアント トラフィックを NAT するルータの背後に展開する必要があり、OfficeExtend はパブリック IP ソースを使用します。

答え: C
＊OEAP は全てのトラフィック（データ・管理）が WLC を経由します。FlexConnect（普通はLocal Switching モードを指す） は管理トラフィックは WLC を経由しますが、データトラフィックはWLC を経由しません。

問65　外部からのアクセスからサーバーを保護し、インターネット アクセスを制限しながら内部ユーザーのみのアクセスを許可するには、どのタイプの IPv4 アドレスをサーバーに割り当てる必要がありますか。
A. グローバルユニキャスト
B. パブリック
C. プライベート
D. マルチキャスト

答え: C
＊プライベートIPアドレスは外部と接点がない。外部IP→NAT→内部IP

問66　従来のネットワーク デバイスによって一般的に実行される機能はどれがソフトウェア定義コントローラーに置き換えられますか。
A. VPN リンク処理の暗号化と復号化
B. ルート テーブルの構築と転送テーブルの更新
C. NAT 操作中の送信元または宛先アドレスの変更
D. データリンク フレーム内のパケットのカプセル化とカプセル化解除

答え: B
＊SDN：「コントロールプレーン（制御）」と「データプレーン（転送）」の分離すること

問67　[ルーティング方法]ドラッグアンドドロップ

```
R1# show ip route | begin gateway
Gateway of last resort is not set
  172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
  172.16.1.0/24 is directly connected, FastEthernet0/0
  172.16.1.1/32 is directly connected, FastEthernet0/0
  172.16.2.0/24 [120/2] via 207.165.200.250, 00:00:25, Serial0/0/0
  192.168.1.0/24 [110/84437] via 207.165.200.254, 00:00:17, Serial0/0/1
  192.168.2.0/24 [90/3164437] via 207.165.200.254, 00:00:15, Serial0/0/1
  207.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
  207.165.200.244/30 [1/1] via 207.169.200.254, Serial0/0/1
  207.165.200.248/30 is directly connected, Serial0/0/0
  207.165.200.249/32 is directly connected, Serial0/0/0
```

207.165.200.252/30 is directly connected, Serial0/0/1
207.165.200.253/32 is directly connected, Serial0/0/1

答え：
・スタティック: 207.165.200.244/30
・EIGRP: 192.168.2.0/24
・OSPF: 192.168.1.0/24
・RIP: 172.16.2.0/24

＊[AD値/メトリック]のAD値の部分を見る。スタティックは1、EIGRPは90、OSPFは110、RIPは120

問68　サウスバウンド API の機能について説明しているものはどれですか。
A. 通信にはHTTPメッセージを使う。
B. コントローラとネットワークデバイス間の通信を可能にする。
C. コントローラから SDN アプリケーションに情報を伝える。
D. 管理プレーンと通信する。

答え: B
＊アプリケーション→ノースバンド→コントローラー→サウスバンド→エンドデバイス

問69　HSRP の 2つの目的は何ですか。(2つ選択)
A. 2台以上のルーターをグループ化し、1台の仮想ルーターとして動作させます
B. 冗長ゲートウェイを提供することで、ネットワークの可用性を向上させます
C. TCP/IPネットワーク内のホストにコンフィグレーション情報を渡します
D. ネットワーク上のホストが、デフォルトゲートウェイのないリモートサブネットに到達するのを助ける
E. ディスクレスクライアントがブート時にIPパラメータを自動設定するメカニズムを提供する

答え: AB
＊デフォルトゲートウェイを冗長化させるプロトコルとして、HSRP、VRRP、GLBPがあります。これらを総称として FHRP（ First Hop Redundancy Protocol ）と呼びます。HS＝ホット スワップと覚えておくと良い。

問70　新しい Cisco IOS ルータにアクセス リストを設定する必要があります。アクセス リストは、192.168.240.0/20 ネットワークからネットワーク 10.125.128.32/27 への HTTP トラフィックを拒否する必要がありますが、192.168.240.0/20 ネットワークが 10.0.0.0/8 ネットワークの残りの部分に到達できるようにする必要があります。エンジニアはどの設定を適用しますか。

Option A
```
ip access-list extended deny_outbound
 10 deny tcp 10.125.128.32 255.255.255.224 192.168.240.0 255.255.240.0 eq 443
 20 deny tcp 192.168.240.0 255.255.240.0 10.125.128.32 255.255.255.224 eq 443
 30 permit ip 192.168.240.0 255.255.240.0 10.0.0.0 255.0.0.0
```

Option B
```
ip access-list extended deny_outbound
  10 permit ip 192.168.240.0 255.255.240.0 10.0.0.0 255.0.0.0
  20 deny tcp 192.168.240.0 255.255.240.0 10.125.128.32 255.255.255.224 eq 443
  30 permit ip any any
```

```
Option C
ip access-list extended deny_outbound
 10 deny tcp 192.168.240.0 0.0.15.255 10.125.128.32 0.0.0.31 eq 80
 20 permit ip 192.168.240.0 0.0.15.255 10.0.0.0 0.255.255.255
 30 deny ip any any log

Option D
ip access-list extended deny_outbound
 10 deny tcp 192.168.240.0 0.0.15.255 any eq 80
 20 deny tcp 192.168.240.0 0.0.15.255 10.125.128.32 0.0.0.31 eq 80
 30 permit ip 192.168.240.0 0.0.15.255 10.0.0.0 0.255.255.255
```

答え: C
＊【難】色々な知識を問われています。①ワイルドカードが計算できること、②HTTPが80であると知っていること。（443はHTTPS）、③一番難しいのはdenyやpermitの設定方法。説明のされ方がバラバラなので、じっくり論理的に考える必要があります。オーソドックスな設定方法は、拒否を先に入れる→許可を入れる→最後にdeny any any。【実践】②からC,Dに絞ります。③から最後にdeny any anyがある方を検証します。

問71　DHCPプールが作成されました。プールは 192.168.20.0/24 を使用しており、DHCP クライアントのデフォルトゲートウェイとして、使用可能な最後から2番目の IP アドレスを使用する必要があります。
A. default-router 192.168.20.253
B. network 192.168.20.254 255.255.255.0 secondary
C. ip default-gateway 0.0.0.0 0.0.0.0 192.168.20.253
D. next-server 192.168.20.254

答え: A
＊デフォルトゲートウェイとなるIPアドレスを設定するコマンド。DHCPサーバーで設定する。

問72　ネットワークにおける SNMP の役割は何ですか。
A. プレゼンテーション層で動作する TCPを使用してネットワーク デバイスと機能を監視する
B. トランスポート層で動作する SSLを使用してネットワーク デバイスから直接データを収集する
C. アプリケーション層で動作する UDPを使用してネットワーク デバイスを監視および管理する
D. ネットワーク層で動作する SSHを使用してネットワーク デバイスからテレメトリと重要な情報を収集する

答え: C
＊"UDP","監視"で解答できる

問73　1 行目から 5 行目で終わる部分は何が表されますか。

```
1 [
2   {"switch": "3750", "port": "e2"},
3   {"router": "2951", "port": "e20"},
4   {"switch": "3750", "port": "e23"}
5 ]
```

A. object
B. key
C. value
D. array

答え: D
＊"key":"値"、オブジェクト{}、配列[]

問74　IPv6 リンクローカル アドレスとユニーク ローカル アドレスの違いは何ですか。
A. IPv6 リンクローカル アドレスのスコープは直接接続されたインターフェイスに制限されますが、IPv6 ユニーク ローカル アドレスは会社のサイトまたはネットワーク全体で使用されます。
B. IPv6リンクローカル アドレスのスコープはループバック アドレスに制限され、IPv6 ユニーク ローカル アドレスは直接接続されたインターフェイスに制限されます。
C. IPv6 リンクローカル アドレスのスコープはグローバルですが、IPv6 ユニーク ローカル アドレスのスコープはループバック アドレスに制限されます。
D. IPv6 リンクローカル アドレスのスコープは会社のサイトまたはネットワーク全体で使用できますが、IPv6 ユニーク ローカル アドレスはループバック アドレスに制限されます。

答え: A
＊リンクローカルは同じセグメント内で使用可能。ユニークローカルはIPv4でいうプライベートアドレスで、社内NW全体で使用可能。

問75　ネットワークに DHCP を実装する 2つの理由は何ですか。 (2つ選択)
A. ネットワークデバイス上の IP アドレスを手動で制御および構成する
B. クライアントの IP アドレス範囲を管理する管理時間を短縮する
C. ネットワークデバイスによる IP アドレスの使用時間を制御する
D. IP アドレスに到達するための最適なパスを動的に制御する
E. IP アドレスではなく名前で Web サイトにアクセスする

答え: B,C
＊A.DHCPの意味なし、D.ルーティング機能は無い、E.DNSのこと

問76　トラフィック・シェーピングとは何ですか。
A. パケットの QoS 属性を変更する
B. パケット内に QoS 属性を設定する
C. 過剰なトラフィックをキューに入れる
D. トラフィックをクラスに整理する

答え: C
＊"キューに入れる"＝送信速度を超えるトラフィックはバッファにキューイングされ、徐々に送信される（破棄しない）。ポリシング（破棄）との違いに注意。

問77　IPv6 マルチキャスト アドレスと IPv6 エニーキャスト アドレスの違いは何ですか。
A. IPv6 マルチキャスト アドレスはプレフィックス 2002:/15 を使用し、1 つの宛先に転送し、IPv6 エニーキャスト アドレスはプレフィックス ff00::/8 を使用し、グループ内の任意の宛先に転送します。

B. IPv6 マルチキャスト アドレスは IPv4 から IPv6 への移行に使用され、IPv6 エニーキャスト アドレスは IPv6 のみの環境でのアドレス集約に使用されます。 C. IPv6 マルチキャスト アドレスは
サブネット内の多数のインターフェイスに割り当てられますが、IPv6 エニーキャスト アドレスは、すべて IPv6 ルーターのグループ内の定義済みのノード グループに使用されます。
D. IPv6 マルチキャスト アドレスに送信されたパケットは、一度に 1 つ以上の宛先に配信されますが、IPv6 エニーキャスト アドレスに送信されたパケットは、そのアドレスに最も近いインターフェイスにルーティングされます。

答え: D
＊説明文のとおり。エニーキャストの使用例：東京、大阪、福岡に各1台ずつDNSサーバーを設置する。3台とも同じIPアドレスを設定する。埼玉にいるクライアントがDNSを呼び出すと、東京のサーバーが反応する。

問78　WPA3 の一部としてどのような機能強化が実装されましたか。
A. WEP とパケットごとのキーイングを改善する TKIP 暗号化
B. パーソナルモードにおける前方秘匿性とSAEの導入
C. 802.1x 認証と AES-128 暗号化
D. パーソナル モードでの AES-64、エンタープライズ モードでの AES-128

答え: B
＊SAEで鍵交換をすることにより、前方秘匿性が高まりました。前方秘匿性とは将来もし暗号鍵が漏れても、過去の通信内容が解読されないようになるということです。WPA2-PersonalではPSK（事前共有鍵）が使用されておりましたが、SAEはセッションごとに暗号鍵が異なります。

問79　軽量モードのワイヤレス AP の構成変更はどのように行われますか。
A. AP の管理 IP への SSH 接続
B. APの帯域外アドレスへの直接HTTPS接続
C. 親 WLC 経由の CAPWAP/LWAPP 接続
D. 親 WLC 経由の EoIP 接続

答え: C
＊CAPWAPやLWAPPは、WLCと軽量AP（集中管理型AP、Light Weight AP）の間で流れる制御用プロトコルのことです。

問80　接続されたサーバがアクティブになるとすぐにトラフィックをそのサーバに送信するには、スイッチ ポートでどの Rapid PVST・機能を設定しますか。
A. ループガード
B. BPDUガード
C. アップリンクファースト
D. ポートファースト

答え: D
＊通常のSTP/Rapid-PVSTでは、リスニング → ラーニング → フォワーディングという段階がありますが、PortFastはサーバが起動した直後から即座にネットワークトラフィックが流せるようになります。STPが不要なエンドホスト向けに使う設定です。

問81　Wi-Fi ではノイズはどのように定義されますか。

A. ローカル信号に干渉する他の Wi-Fi ネットワークからの信号
B. 目的の Wi-Fi 信号と干渉する Wi-Fi 信号との測定された差
C. ワイヤレス デバイスによって提供される信号対雑音比
D. 目的の信号を劣化させる Wi-Fi トラフィック以外の干渉

答え: D
＊ノイズ：Wi-Fi以外による悪影響（電子レンジなど）、干渉：他のWi-Fiによる悪影響

問82　LACP レイヤー 2 EtherChannel を設定するには、2つのスイッチにどのコマンド セットを適用しますか。

Option A

```
SW1(config)=interface range f0/13 -14
SW1(config-if-range)=channel-group 1 mode desirable
SW2(config)=interface range f0/13 -14
SW2(config-if-range)=channel-group 1 mode passive
```

Option B

```
SW1(config)=interface range f0/13 -14
SW1(config-if-range)=channel-group 1 mode on
SW2(config)=interface range f0/13 -14
SW2(config-if-range)=channel-group 1 mode passive
```

Option C

```
SW1(config)=interface range f0/13 -14
SW1(config-if-range)=channel-group 1 mode active
SW2(config)=interface range f0/13 -14
SW2(config-if-range)=channel-group 1 mode passive
```

Option D

```
SW1(config)=interface range f0/13 -14
SW1(config-if-range)=channel-group 1 mode auto
SW2(config)=interface range f0/13 -14
SW2(config-if-range)=channel-group 1 mode passive
```

答え: C
＊LACPは、active/activeまたはactive/passiveで成立します。なお、シスコ規格のPAgPは、desirable/desirableまたはauto/desirableで成立します。

問83　管理者は、203.0.113.0/24 ネットワーク内のホストからの管理接続のみを受け入れるように Cisco Catalyst スイッチを設定しています。スイッチを通過するその他のトラフィックは中断することなく通過する必要があります。エンジニアはどの 2つの設定をルータに適用しますか。 (2つ選択)
A. ip access-list extended Management
　permit tcp any range 22 23 203.0.113.0 0.0.0.255
B. line vty 0 15
　access-class Management in
C. ip access-list standard Management
　permit 203.0.113.0 255.255.255.0
D. interface range vlan 1 – 4094
　ip access-group Management out
E. ip access-list standard Management
　permit 203.0.113.0 0.0.0.255

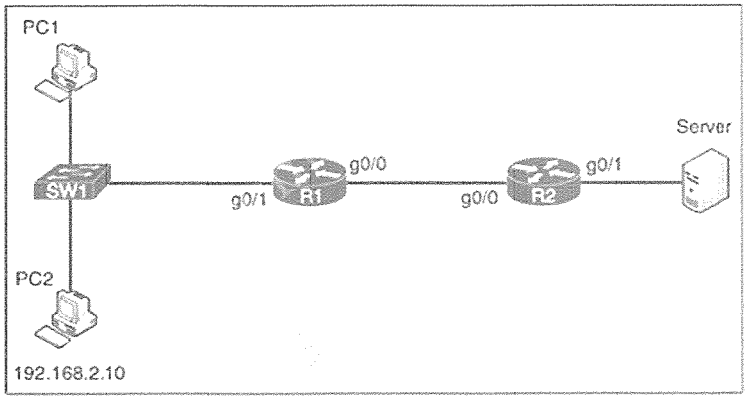
答え: B,E

＊"Management"はACLの名前です。B.Managementからの管理アクセスを許可する。E.ManagementのIPアドレス範囲（アクセス元）を設定する。C.ACLはワイルドカード表記なので注意。

問84　LAG の使用時に WLC 上のどのインターフェースが 1 つに制限されますか。
A. APマネージャ
B. 仮想
C. トランク
D. サービス

答え: A
＊「LAG を使うと、WLC のどの"論理インターフェース"が複数作れなくなるか？」という意味。複数のAPマネージャインターフェイスを束ねるということ。各論理インターフェースの役割を理解しておくと回答できる。A.AP用、B.ローミング用、C.無い、D.WLC管理用

問85　PC2 からファイル サーバーへの接続をブロックしながらも、PC2 が他のネットワーク ホストやデバイスに接続できるようにする必要があります。どの構成を使用しますか。



Option A

```
R1(config)#access-list 1 permit 192.168.2.10
R1(config)#access-list 1 deny any
R1(config)#interface g0/1
R1(config-if)#ip access-group 1 out
```

Option B

```
R2(config)#access-list 1 deny 192.168.2.10
R2(config)#access-list 1 permit any
R2(config)#interface g0/1
R2(config-if)#ip access-group 1 out
```

Option C

```
R2(config)#access-list 1 permit 192.168.2.10
R2(config)#access-list 1 deny 192.168.2.0 0.0.0.255
R2(config)#interface g0/1
R2(config)#ip access-group 1 in
```

Option D

```
R1(config)#access-list 1 deny 192.168.2.10
R1(config)#access-list 1 permit 192.168.2.0 0.0.0.255
R1(config)#interface g0/0
R1(config-if)#ip access-group 1 in
```

答え: B
＊PC2からのR2,g0/1,outを制限する。

問86　REST API は通信にどのプロトコルを使用しますか。
A. HTTP
B. STP
C. SNMP
D. SSH

答え: A
＊HTTPまたはHTTPSを使用します。メソッド（GETやPOSTなど）もHTTPと同様です。

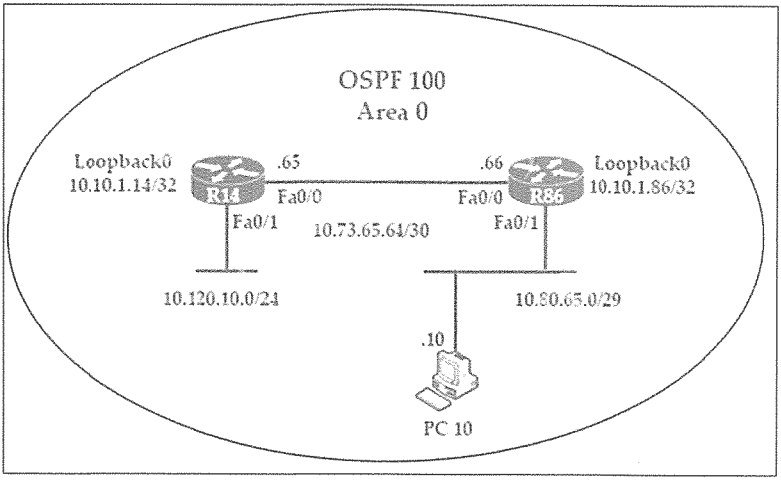
問87　企業ネットワーク上のファイアウォールの機能は何ですか。
A. 企業とISPの間の仲介装置として機能する。
B. インターネット上のホストへのデフォルトゲートウェイとして機能する。
C. ステートレス・インスペクションに基づいてトラフィックを処理する
D. イングレスとイグレスのトラフィックを許可したり拒否したりする

答え: D
＊イングレス（外部→内部の通信）、イグレス（内部→外部の通信）

問88　パケットの送信元および宛先 IP アドレス部分が暗号化されていないサイト間 VPN 接続からパケットが送信される場合、どの暗号化モードが使用されますか。
A. PPTP
B. セキュアシェル
C. トランスポート
D. PPPoE

答え: C
＊トランスポートモード：ペイロードのみを暗号化、トンネルモード：ヘッダ+ペイロードを暗号化

問89　ネットワーク 10.120.10.0/24 をインストールしました。このネットワークを OSPF ルーティング テーブルに追加するには、R14 ルータにどの設定を適用しますか。



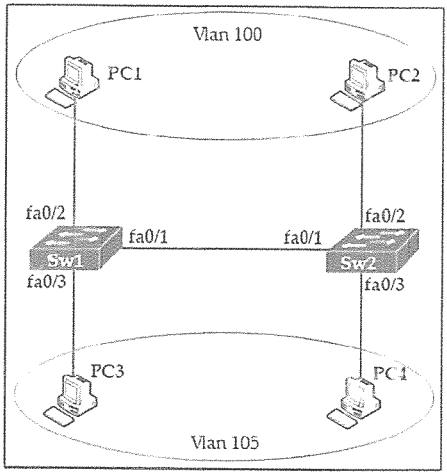
A. router ospf 100
　network 10.120.10.0 0.0.0.255 area 0
B. router ospf 100 area 0
　network 10.120.10.0 0.0.0.255
C. router ospf 120
　network 10.120.10.0 255.255.255.0 area 0
　ip route 10.120.10.0 255.255.255.0 fa0/1
D. router ospf 100
　network 10.120.10.0 255.255.255.0 area 0

答え: A
＊他は構文として誤りです。ワイルドカードである点も注意。

問90　データ プレーンによって提供される主要な機能は何ですか。
A. ルーティングの決定
B. ルーティングテーブルデータの交換
C. トラフィックを次のホップに転送
D. パケットの発信

答え: C
＊A,Bはコントロールプレーン

問91　2つの異なる VLAN からのトラフィックを通過させるように、SW1 と SW2 のインターフェイス fa0/1 を設定します。セキュリティ上の理由から、会社のポリシーではネイティブ VLAN をデフォルト以外の値に設定する必要があります。この要件を満たす設定はどれですか。



Option A

```
Switch(config-if)#switchport mode dynamic
Switch(config-if)#switchport access vlan 100,105
Switch(config-if)#switchport trunk native vlan 1
```

Option B

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport access vlan 100.105
Switch(config-if)#switchport trunk native vlan 3
```

Option C

```
Switch(config-if)#switchport mode trunk
Switch(config-if)# switch port trunk encapsulation isl
Switch(config-if)#switchport trunk allowed vlan 100,105
Switch(config-if)#s witch port trunk native vlan 1
```

Option D

```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan 100,105
Switch(config if)#switchport trunk native vlan 3
```

答え: D
＊SW間はトランクにする。ネイティブVLANはデフォルトが1なので、1以外にする。

問92　ネットワークに syslog を実装する場合、エンジニアは何を考慮しますか。
A. Syslogは、メッセージをトリガーしたソフトウェアまたはハードウェアコンポーネントを定義します。
B. デフォルトでは、すべてのメッセージレベルがsyslogサーバーに送信されます。
C. ロギングレベルは、特定のメッセージの重大度を定義します。
D. 16種類のロギングレベル（0～15）がある

答え: C
＊0緊急、1警報、2重大、3エラー、4警告、5通知、6情報、7デバック（キンさん法大へ。告白は通常で）

問93　これらの基準を使用してルータとスイッチを接続する場合、どのタイプのケーブルを使用しますか。
①ピン1と2は受信用、ピン3と6は送信用
②自動検出MDI-Xは利用できない
A. クロス
B. ロール
C. コンソール
D. ストレート

答え: A
＊ルータとスイッチなので、本来はストレートケーブルを使うのが正しい。
【悪問】ただし、①の説明から両端がMDIである前提であるため、MDIとMDIの接続となり、クロスケーブルが正解となる。
＊メモ
　MDIとMDI＝クロス、MDIとMDI-X＝ストレート、MDI-XとMDI-X＝クロス
　MDI：送信3,6、受信1,2　　MDI-X：送信1,2、受信3,6
＊なお、現代では「ストレートケーブル＋自動MDI-X」が主流である。②は「ストレートorクロスを正しく選択しないとリンクアップしないよ」ということを意味しています。

問94　ワイヤレスネットワーク用に新しい WLAN を設定します。これらの要件を満たすアクションはどれですか。(2つ選択)
・デュアルバンドクライアントは、5GHzに誘導される
・ワイヤレスクライアントは、返された RADIUS属性でVLAN 設定を適用できる

A. Client Band Select オプションを有効にする
B. Coverage Hole Detection オプションを有効にする
C. Alloe AAA Override オプションを有効にする
D. MFP Client Protection オプションを必須に設定する
E. Aironet IE オプションを有効にする

答え: A,C
＊A.2.4GHzと5GHzのうち、5GHzを優先させる。C.RADIUSなのでAAAを連想できるとよい。

問95　グローバル IPv6 アドレスと一意のローカル IPv6 アドレスの類似点は何ですか。
A. マルチキャスト IPv6 グループ タイプの一部である
B. グローバル インターネット上でルーティング可能である
C. 同じ組織によって割り当てられている
D. サブネット化に同じプロセスを使用する

答え: D
＊【奇問】どちらも/64のようにサブネット化することができます。

問96　SSIDの目的は何ですか。
A. モバイルデバイスが接続するワイヤレスネットワークを特定します。
B. ネットワーク・デバイスが接続されている有線ネットワークを識別します。
C. アプリケーションが接続する必要があるワイヤレスネットワークを識別します。
D. ユーザー・デバイスが接続されている有線ネットワークを識別します。

答え: A
＊Service Set Identifier、サービス セット識別子

問97　ネットワーク管理者は、従来管理されたネットワーク上でネットワークの整合性を維持しながら、どのようにメンテナンス コストを削減しますか。
A. ネットワークの問題を早期に警告するために、自動化されたネットワーク監視システムを導入する
B. ネットワークを積極的に管理するために、追加のネットワーク管理者を雇用する
C. 自動化を使用してネットワーク管理タスクを集中化する
D. 問題解決を確認する変更管理プロセスを自動化する

答え: C
＊【悪問】CにはAやDが含まれていると考える

問98　ネットワーク管理者はどのようにして軽量モードの AP を安全に管理しますか。
A. HTTPS 経由で WLC GUI を使用する
B. アウトオブバンド接続経由で CLI を使用する
C. SSH を使用した仮想インターフェイス経由で CLI を使用する
D. インバンド SSH 接続経由で AP GUI を使用する

答え: A
＊軽量APはWLCからアクセスする。

問99　組織がネットワーク パフォーマンスを検証し、問題をトラブルシューティングし、エージェントを使用して監視ツールとエンド デバイス間で通信する必要がある場合、どのプロトコルが実装されますか。
A. FTP
B. NTP
C. NFS
D. SNMP

答え: D
＊"エージェント"、"監視"という語句から、SNMPと判断できる。

問100　AAA 認証と認可の違いは何ですか。
A. 認証はユーザがアクセスするシステムプロセスを制御し、認可はユーザが開始する活動を記録する。
B. 認証はシステムにアクセスしようとするユーザーを識別し、認可はユーザーのパスワードを検証する。
C. 認証はシステムにアクセスしようとしているユーザを識別・検証し、認可はユーザが実行するタスクを制御する。
D. 認証はユーザ名とパスワードを検証し、認可は認証エージェントとユーザデータベース間の通信を処理する。

答え: C
＊Cのとおり。AAA（認証、認可、アカウンティング）

問101　どの syslog メッセージ ログレベルで、インターフェイスラインプロトコルのアップ/ダウン イベントが表示されますか。
A. 情報

B. アラート
C. デバッグ
D. 通知

答え: D
＊【難問】"インターフェイスラインプロトコルのアップ/ダウン"とは、ポートが有効/無効になることです。A.単なるお知らせであり対応しないことがほとんどです。それ以下のC.デバックは論外です。なんらかの対応が必要と考えると、BやDが考えられます。アラートはかなり深刻な状況ですから、消去法でDです。

問102　Cisco WLC に複数のディストリビューション システム ポートと 1 つの IP アドレスのみが設定されている場合に必要な標準はどれですか。
A. 802.3ad
B. 802.1q
C. 802.1d
D. 802.1af

答え: A
＊【丸暗記】LAGの規格は802.3adです。