解答・解説

A1. B

QoS(Quality of Service)とは、ネットワークを介して提供しているサービスの品質を保つための技術です。QoSを実現するためのアーキテクチャとして、以下の3つがあります。

- **ベストエフォート**

  パケットの優先順位などは考慮せず、先にきたものを先に出すという処理を行います。

- **IntServ**

  RSVPを使用してフローが必要とする帯域をあらかじめ確保しておくアーキテクチャです。

- **DiffServ**

  各ルータやスイッチごとにパケットの優先順位に基づいて区別して転送処理を行うアーキテクチャです 。イーサネットフレームの優先度を表すCoSやIPパケットの優先度を表すDSCPやIP Precedenceを利用します。

  よって、**B**が正解となります。

A2. B

ファーストホップルータ（ユーザのPCから見たデフォルトゲートウェイ）に障害が発生したとしても 、冗長化したルータに処理を切り替え、接続を維持することができるプロトコルの総称をFHRPといいます。Cisco独自のHSRPやGLBP、標準化されているVRRPなどがこれにあたります。HSRPでは、仮想IPアドレスを使用して複数のルータでこの仮想IPアドレスを共有することで、障害が発生したとしてもユーザからは障害を意識させることなく処理するルータを切り替えることができます。このような透過的なフェイルオーバーが可能となります。なお、フェイルオーバーとは障害が発生した際に冗長化された経路や機能に切り替える機能を指します。

A. STPはスイッチで構成されたネットワークで、冗長パスがある場合に発生する可能性があるレイヤ2のループを防ぐためのプロトコルです。

C. DNSはドメイン名からIPアドレスを解決する際に用いられるプロトコルです。

D. EtherChannelは複数の物理インターフェイスをバンドルして帯域幅を増やすことができる技術です 。

よって、**B**が正解となります。

A3. ①A, C, D, F　②B, E

OSPFで隣接関係を構築する際は、エリアID、サブネットマスク、Helloインターバル、Deadインターバルなどを一致させる必要があります。また、IPアドレス、ルータIDは重複がないように一意な値で設定する必要があります。
なお、プロセスIDは、複数のOSPFのプロセスを1台のルータ内で識別する際に必要になるものであるため、複数のルータ間で隣接関係を構築する際には一致させる必要も、一意な値である必要もありません。

A4.　D

サブネットマスク/30は、第4オクテットが11111100となるため、255.255.255.252となります。**B**の255.255.255.240の場合、第4オクテットが11110000となり、/28となるため誤りです。また、**A, C**は、ブロードキャストアドレスになるため 、機器に設定できません。
よって、**D**が正解となります。

A5.　A, E

ルータやスイッチでSSHを有効にするには、以下の手順で設定を行う必要があります。

①ホスト名を設定する
②ドメイン名を設定する
③RSA暗号鍵を生成する
④ユーザアカウントを作成する
⑤ローカル認証を設定する
⑥SSHの接続許可を設定する
⑦SSHのバージョンを設定する

ホスト名はデフォルトでRouterやSwitchとなっていますが、これらデフォルトのホスト名では③で行うRSA鍵の生成ができません。また、⑥の設定でTELNETを無効にすることでセキュリティを高めることができますが、必須の設定ではありません。コンソールパスワードの設定も同様にSSHを有効化するうえで必要ありません。補足として、SSHを使用するには、IOSイメージが暗号化に対応している必要があります。対応しているかどうかはIOSがK9（crypto）イメージであるかでどうかで判断できます 。

```
Router#show version
Cisco IOS Software, C181X Software (C181X-ADVENTERPRISEK9-M), Version
15.1(4)M7, RELEASE SOFTWARE (fc2)
```

よって、**A, E**が正解となります。

A6.　D

「enable password」「enable secret」の2つのコマンドを同時に設定すると、「secret」で入力したパスワードが優先されます。

よって、**D**が正解となります。

A7.　D

DTP（Dynamic Trunking Protocol）は、Cisco独自のプロトコルで、スイッチのポートを自動的にネゴシエートして「アクセスポート」か「トランクポート」にするかを決定します。

dynamic desirableは、DTPフレームを送信してネゴシエートを行い、相手がこれに応じた場合、トランクポートとして動作します。そうでなければアクセスポートとなります。

dynamic autoは、DTPフレームを送信しません。相手側からネゴシエートがあれば、応答フレームを送信してトランクポートとなります。

よって、**D**が正解となります。

A8.　A

PortFastの設定されているポートでは、端末やネットワーク機器などを接続した際やスイッチを再起動した場合、すぐにフォワーディング状態のポートとなります。その場合、リスニングやラーニングといったスパニングツリーの状態遷移を行いません。

他の選択肢は、spanning-tree portfastコマンドを実行した際の動作には該当しません。

よって、**A**が正解となります。

A9.　A, B

EtherChannelでは、ネゴシエーションすることでEtherChannelを動的に形成させることが可能となっています。具体的には、

「PAgP（Port Aggregation Protocol）」と「LACP（Link Aggregation Control Protocol）」を用います。

LACP（Link Aggregation Control Protocol）は、「IEEE802.3ad」で定義されている業界標準プロトコルです。他ベンダー機器との接続に適しています。LACPには、「active」と「passive」の2モードがあります。activeは、LACPパケットを送信して相手とのネゴシエーションを開始し、passiveは、相手からネゴシエーションを受信すると応答しますが、自身からはネゴシエーションを始めません。よって、**A, B**が正解となります。

A10. D

トランスポート層では、ノード間のデータ伝送における信頼性の提供、およびアプリケーション間でセッションを開始するうえで必要なポート番号の割り当てについて規定しています。

シーケンス番号は、送るデータそれぞれに付ける番号で、届いたデータの並べ替えや重複チェックに使われます。

MACアドレスは、データリンク層において、1つのネットワーク回線上で直接接続されている機器同士が通信する際の通信方式で使用されます。

プロトコル番号は、IPヘッダ内で使われているデータ部分のプロトコルを示す識別番号です。

よって、**D**が正解となります。

A11. A, C, D

IPv6アドレスは、「ユニキャストアドレス」「マルチキャストアドレス」「エニーキャストアドレス」の大きく3つに分類されます。

なお、IPv4で利用されていた「ブロードキャスト」は、IPv6では廃止されています。

よって、**A, C, D**が正解となります。

A12. A

DRやBDRの選出は、OSPFのプライオリティ値が同一であった場合には、ルータIDによって判断されます。ルータIDは32ビットの値で、IPアドレスと同じように表します。ルータIDは、以下のような順番で決定します。

①「router-id」コマンドを使用して設定したルータID

②有効なループバックインターフェイスの中で一番大きなIPアドレス

③有効な物理インターフェイスの中で一番大きなIPアドレス

今回のshow ip interface briefの出力結果からは、①のルータIDが確認できません。したがって、Loopback0に設定されている10.1.2.1がルータIDとして使用されます。

よって、**A**が正解となります。

A13. B, D

DHCPスヌーピングは、スイッチの各ポートを 「信頼できるポート」または「信頼できないポート」に定義することで、DHCPサーバのなりすましによる攻撃を防ぎます。

また、DHCPスヌーピングの設定をすると、スイッチのポートは、デフォルトで信頼できないポートになります。したがって、正規のDHCPサーバが接続されるポートは信頼できるポートに設定する必要があります。

よって、**B, D**が正解となります。

A14. A

フローティングスタティックルートとは、ダイナミックルーティングで経路情報が得られなくなったときに 、スタティックルートをバックアップルートとして使用する方法です。

通常はダイナミックルーティングを使用する場合 、バックアップルートとしてスタティックルートを設定し 、アドミニストレーティブディスタンス値にダイナミックルーティングより大きな値を指定します 。そうすると、正常時にはダイナミックルーティングのルートがプライマリルートとして採用されますが、障害が発生した際には代わりに、スタティックルートが採用されます。

よって、**A**が正解となります。

A15. D

Cisco ACI（Cisco Application Centric Infrastructure）は、CiscoによるデータセンターSDNの実装で、コントローラとしてAPIC（Application Policy Infrastructure Controller）を使用します。なお、その他の選択肢の概要は次の通りです。

A. Cisco APIC-EM（APIC-Enterprise Module）は、Ciscoによる企業向けのSDNコントローラです。

B. OpenFlowはサウスバウンドAPIに該当するプロトコルです。

C. Cisco DNA Centerは、Ciscoによる企業内ネットワーク向けのCisco SD-Access（Cisco Software-Defined Access）のコントローラです。

よって、**D**が正解となります。

A16. B

複数の異なるルーティングプロトコルで同じ宛先への経路を学習した場合、AD値（アドミニストレーティブディスタンス値）が最も低いルーティングプロトコルの経路が使用されます。

なお、経路選択の際の基準はルーティングプロトコルによって決まっており、「メトリック」といわれます。RIPでは「ホップカウント（ルータをまたぐ回数）」です。また、EIGRPでは、交換したルート情報からDUAL（Diffusing Update ALgorithm）によって最適ルートを決定しています。

よって、**B**が正解となります。

A17. C

この問題のケースではAD値が、EIGRPが90、OSPFが110のため、EIGRPのルートが優先されます。**A, D**はともにEIGRPとOSPFのAD値ではないため、誤りです。なお、AD値120はRIP、AD値20はBGP（外部）の値となります。

よって、**C**が正解となります。

A18. D

ルータが「10.0.2.195」宛のパケットを受信した場合、ルーティングテーブルのエントリのうち、OSPFで学習している10.0.2.128/25とEIGRPで学習している10.0.2.192/29の2つが該当します。その場合、ロンゲストマッチ（最長一致）のルールに従ってパケットを転送します。

ロンゲストマッチとは、転送するための宛先ネットワークがルーティングテーブルに複数ある場合に、宛先ネットワークのネットワーク部のビットが最も長く一致するルートがパケットの転送先として選択されるルールとなります。そのため、EIGRPで学習している10.0.2.192/29の経路が選択されます。

また、ルーティングテーブル上では、サブネットマスクの後ろに表記される[ ]内/の手前の値がAD値、後ろの値がメトリックを示しています。

よって、メトリックが3072の**D**が正解となります。

A19. A, B

Layer2タブを開いた後、Radiusサーバでの認証ではなく、WPAおよびWPA2対応のWLAN端末がPSKを使用して認証を行う場合は、Layer2 Security選択プルダウンで「WPA+WPA2」を選択します。さらにAuthentication Key Management選択ボックスから「PSK」を選択、最後に「Apply」を選択して完了となります。

よって、**A, B**が正解となります。

A20. A, C

R3で、インターフェイスFa0/0をプライマリルートとして使用して、R1のLo1インターフェイスに到達できるよう設定するには、まずスタティックルートをR1 (192.168.21.1)に向けて設定します。プライマリルートなので、アドミニストレーティブディスタンスをデフォルトにしておきます（選択肢A）。また、R1とR3の間のリンクがダウンしたとき、R2経由でR1のLo1インターフェイスに到達できるようにも設定する場合には、R2のネクストホップアドレス（192.168.22.2）を指定して、管理ディスタンスを選択肢**A**よりも大きくする必要があります。

よって、**A, C**が正解となります。

A21. D

有線ケーブルを使用せずに電波を使用するワイヤレスLANでは、2.4GHz帯と5GHz帯の電波が利用され、様々な規格が存在します。IEEE802.11b/g規格では、2.4GHz帯を複数のチャネルという単位に分けて使用しますが、各チャネルの周波数が重複するため、すべてのチャネルを同時使用することができません。したがって、電波干渉しないようにチャネルの間隔を空ける必要があります。

無線の技術は改良が続けられており、IEEE802.11nやIEEE802.11acといった規格では、MIMOやチャネルボンディングなどの技術により高速化が図られています。無線の通信方式は、アクセスポイントを介するインフラストラクチャモードと、介さないアドホックモードがあります。

よって、**D**が正解となります。

A22. B, C

多要素認証は、異なる種類の情報を組み合わせて認証を行う方式です。特に異なる2要素を組み合わせて行うものを2要素認証と呼びます。例えば、銀行のATM操作ではパスワードの入力以外にキャッシュカード（あるいは通帳）の挿入が求められます。キャッシュカードは実体のある所持情報に分類されるもので、パスワードはユーザが脳内に記憶しておくべきものなので、実体のない知識情報に分類されます。今回の選択肢では、知識要素はIDとパスワードとなります。なお、「顔」や「虹彩」は生体要素と呼ばれます。

よって、**B, C**が正解となります。

A23. A

「DR(Designated Router)」と「BDR(Backup Designated Router)」の選出は、最初のネイバーを確立する過程 「Down State」→「Init State」→「Two-way State」の後に、Helloパケット内に含まれるプライオリティ値やルータIDを比較してセグメントごとに行われます。DRとBDRに選出されなかったルータは、「DROther」と呼ばれ、DROtherは、DRとBDRとだけ「Full State」となり、LSAを送信するようになります。

よって、**A**が正解となります。

A24. A, D

WPA2は、暗号化方式にCCMP（Counter Mode-CBC MAC Protocol）を採用し、AES暗号化アルゴリズムを採用することで強度なセキュリティを実装しています。なお、**B**のTKIP（Temporal Key Integrity Protocol）はWPAの暗号化方式、**C**のPSKは認証方式となるため誤りです。

よって、**A, D**が正解となります。

A25. D

どの選択肢も名前付き拡張ACLで設定されています。アクセスリストは、上の行から検索が行われ当てはまると検索はストップします。そのため、記述順序を間違えると意図しない結果となりますので注意が必要です。
また、アクセスリストは、複数行設定することができますが、必ず最後の行に「暗黙のdeny」（すべての通信を拒否）が自動で入ります。つまり、上の行で許可されていない通信は、必ず最後の行に引っかかって拒否となります。これは許可忘れよりも拒否忘れのほうが危険な状態になるからです。暗黙のdenyの回避をするためには、名前付き拡張ACLの場合(config-ext-nacl)#permit ip any anyを最後に設定します。
なお、選択肢**A, B**はpermit ip any anyを最初に設定しているため、すべての通信が許可されてしまいます。**C**はACLに許可する条件がないため、PC01だけではなくすべての通信が拒否されてしまいます。
よって、**D**が正解となります。

A26. ①B, E, F　　②A, C, D

FTP（File Transfer Protocol）はファイル転送に使用するプロトコルです。FTPは以下の特徴を持ちます。

- TCPを使用
- TCPポート20番と21番を使用
- 認証の機能を持つ

一方TFTP（Trivial File Transfer Protocol）は、FTPの簡易版です。TFTPは以下の特徴を持ちます。

- UDPを使用
- UDPポート69番を使用する
- 認証の機能を持たない

A27. B

192.168.228.144/21（255.255.248.0）のネットワークアドレスは、192.168.224.0となります。
ブロードキャストアドレスは 、192.168.231.255になるため、使用できるアドレスは、192.168.224.1-192.168.231.254となります。
よって、**B**が正解となります。

A28. 1. C　　2. B　　3. F　　4. A　　5. E

ルータやスイッチ上で設定するパスワードに関するコマンドの問題です。特権EXECモードに移行する際に問いかけるパスワードは、

enable secretコマンドで暗号化したパスワードを設定することができます。それ以外のコマンドで設定したパスワードを暗号化する場合は、service password-encryptionコマンドを実行します。なお、モデム経由でログインするパスワードを設定するには 、AUXポートにパスワードを設定する必要があります。

A29. B

構成管理ツールには、「Ansible」「Puppet」「Chef」の3つがあります。PuppetやChefの場合、エージェント側ではHTTPまたはHTTPSのプロトコルで構成管理サーバから情報を取得して、自身の設定を行います（PULL型）。一方Ansibleは、SSHやNETCONFのプロトコルを使って機器に接続して設定を行います（PUSH型）。

なお、**D**の「Ruby」はプログラミング言語で、Chefで使用される「クックブック」「レシピ」と呼ばれるファイルに記述する際に使用するものです。

よって、**B**が正解となります。

A30. ①B, E　　②A, C, D

「DHCP（Dynamic Host Configuration Protocol）」は、コンピュータがネットワークに接続するために必要なネットワーク情報（IPアドレス、サブネットマスク、デフォルトゲートウェイ等）をクライアントに自動で割り当てるためのプロトコルです。DHCPサーバ側は、クライアントに配布されるネットワーク情報を保持しています。

DNS（Domain Name System）とは、ドメイン名とIPアドレスを紐付けるシステムです 。その際、DNSサーバ側は、ホスト名やドメイン名と紐付けられたIPアドレスのリストを保持しています。

A31. ①A, B　　②C, F　　③D, E

セキュリティを実現させるには、「AAA」という考え方が重要となります。AAAは、セキュリティの重要な機能である以下の3つの頭文字をとったものです。

▪Authentication（認証）

ユーザID、パスワードなどをもとに許可されているユーザなのかどうかの検証・識別を行うことです。

▪Authorization（認可）

認証が許可されたユーザが、どのような機能を利用することができるかの制限を行うことです。

▪Accounting（アカウンティング）

サービスやリソースを利用しているユーザがいつログインしてどのようなことを行っているのかを監視・記録することです 。

A32. A

DRは「代表ルータ」、BDRは「バックアップ代表ルータ」を指し、DRでもBDRでもないその他のルータはDROtherと呼ばれます。マルチアクセスネットワークでは、同一ネットワーク内のすべてのルータ同士が完全な隣接関係を構築するのではなく、DRとBDRとだけ完全な隣接関係を構築します。DROtherはネットワークに変更があるとDRとBDRにLSUを送信し、DRから全体にそれを送信します。これにより、個々のルータが情報交換を行うよりもトラフィック量が減らせるというメリットがあります。なお、その他の選択肢の概要は次の通りです。

B. OSPFが動作するルータがダウンするとネイバー関係が解消されるため、そのルータが保持していた情報はDRやBDRからも削除されてしまいます。その際にルーティングテーブルの再構築が行われるため誤りです。

C. DRやBDRが選出されることによって等コストロードバランシングが可能になっているわけではないので、誤りです。

D. OSPFはアップデートの際にマルチキャストを用いているため 、誤りです。

よって、**A**が正解となります。

A33. C, D

コントローラと各ネットワーク機器がデータをやり取りするためのインターフェイスをサウスバウンドAPIといいます。その際、OpenFlow、NETCONF、OpFlexが使用されます。

なお、選択肢**A**のCisco APIC-EM（APIC-Enterprise Module）はCiscoによる企業向けのSDNコントローラです。また、**B**のRESTAPIはノースバウンドAPIです。

よって、**C, D**が正解となります。

A34. C

SDNの実装であるCisco ACIでは、従来の3階層モデルに代わり、スパイン／リーフ型のトポロジを採用しています。スパイン／リーフ型トポロジの特徴は以下の通りです。

- 各リーフスイッチは 、すべてのスパインスイッチに接続する（ ＝各スパインスイッチは 、すべてのリーフスイッチに接続する）
- リーフスイッチは相互に接続できない
- スパインスイッチは相互に接続できない
- エンドポイント（サーバ等）はリーフスイッチにのみ接続する

よって、**C**が正解となります。

A35. A, E

サウスバウンドAPIとノースバウンドAPIは、SDNのアーキテクチャにおいて各レイヤ間のやり取りを行うためのAPIです。
SDNとは、ソフトウェアによりネットワークを管理制御するための新しい概念と、それに基づいたネットワークを構成するための技術のことです。SDNでは、実際に経路の計算やファイアウォールの設定などを行うアプリケーションが該当するアプリケーションレイヤ、ネットワーク上の各機器を制御するSDNコントローラが該当するコントロールレイヤ、パケットの転送処理を行う機器が該当するインフラストラクチャレイヤの3つのレイヤで構成されます。
サウスバウンドAPIは、コントロールレイヤとインフラストラクチャレイヤ間のやり取りを行うためのAPIで、ノースバウンドAPIはアプリケーションレイヤとコントロールレイヤ間でのやり取りを行うためのAPIです。
よって、**A, E**が正解となります。

A36. E, F

CDPとLLDPは、ともに隣接する機器の情報を取得することができるレイヤ2プロトコルです。物理的に接続している機器のみ、情報を取得することができます。たとえ同一ネットワーク内であっても、2つ以上先に接続されている機器の情報は取得することができません。
CDPはCisco独自のプロトコルのため、隣接する機器がCisco製であれば情報を取得することができます。LLDPは標準化されているプロトコルのため、隣接する機器がCisco製でなくても情報を取得することができます。なお、CDPでは隣接機器のMACアドレスは取得することができません。
よって、**E, F**が正解となります。

A37. D

SDNの実装において、インフラストラクチャ層（各ネットワーク機器）のエッジデバイスとコントローラ間で通信する際は、サウスバウンドAPIが使用されます。
なお、ノースバウンドAPIはアプリケーションレイヤとコントロールレイヤがデータをやり取りするためのインターフェイスです 。またアンダーレイとオーバーレイは 、Cisco SD-Accessのインフラストラクチャ層での「SD-Accessファブリック」の構成です。
よって、**D**が正解となります。

A38. E

DHCPクライアントはDHCP DISCOVERやDHCP REQUESTをDHCPサーバへと送信しますが、これらのメッセージはブロードキャストで送信されるため、ルータを越えた異なるネットワークへと送信することができません。DHCPサーバが異なるネットワークに配置されている場合、DHCPクライアントからのメッセージを適切に届けるために、ルータにDHCPリレーエージェントの設定を行う必要があります。DHCPリレーエージェントの設定はDHCP DISCOVERやDHCP REQUESTを受信するインターフェイスで設定を行う必要があるため、今回の場合はFa0/1でip helper-addressコマンドに続いてサーバのIPアドレスを指定して設定します 。

A. 設定しているインターフェイスが誤っています 。

B, C. DHCPリレーエージェントの設定にACLやNATの設定は必要ありません。

D. 今回の場合ルータに直接接続しているネットワーク上にDHCPサーバが配置されているため、ルーティングの設定を行わなくても通信をすることができるため誤りです。

よって、**E**が正解となります。

A39. B, D

WPA2は、WPAの後に策定されました。暗号化方式にCCMP（Counter Mode-CBC MAC Protocol）を採用し、AES暗号化アルゴリズムを採用することで、WPAよりもセキュリティレベルが強度なセキュリティを実装しています。また、WPA2パーソナルではPSK認証を行い、WPA2エンタープライズではIEEE802.1X認証を行います。

よって、**B, D**が正解となります。

A40. C

MPLS（Multi-Protocol Label Switching）は、IPアドレスによって経路を選択する方法ではなく、レイヤ2ヘッダとレイヤ3ヘッダの間にMPLSヘッダを挿入し、そのヘッダ内に格納されている値（ラベル）で経路選択を行うパケット転送技術です。MPLSヘッダのサイズは4byteでIPヘッダよりも軽量なため、ルータにかかる負荷も少なく、より高速にパケットを転送することが可能です。MPLSの技術はIP-VPN網で広く利用されています。従来では、レイヤ2ヘッダとレイヤ3ヘッダの中間にラベルが挿入されるため、レイヤ2とレイヤ3間で動作するプロトコルでしたが、現在では、他の層の間で動作させることもできます。なお、その他の選択肢の概要は次の通りです。

A. IP-VPNは通信事業者が提供する閉じられたIPネットワークを利用したVPNです。

B. IPsecはVPNなどで利用されるセキュリティプロトコルです。

D. SSLはリモートアクセスVPNなどで利用されるセキュリティプロトコルです 。

よって、**C**が正解となります。

A41. D

特定のマルチキャストグループに属している相手に対して通信する際は 、マルチキャストアドレスを使用します 。マルチキャスト用のアドレスは、224.0.0.0 ～ 239.255.255.255です。

なお、選択肢**A**と**B**は、マルチキャスト用のアドレスではありません 。また**C**はループバックアドレスとなります 。

よって、**D**が正解となります。

A42. D

PCのIPアドレスは192.168.10.20のため、ルーティングテーブルより、通るルートはOSPFで学習した192.168.10.16/28のルートであることがわかります。

A. デフォルトルートは当てはまる情報がルーティングテーブル上に存在しない場合に選択される経路なので、この場合は当てはまりません。

B. ホストルートまたはローカルルートは、そのルータのインターフェイスに設定されたIPアドレスを示す経路情報であるため、この場合は当てはまりません。

C.フローティングスタティックルートは、スタティックルートにルーティングプロトコルに設定されたAD値よりも大きな値を設定しておくことで、予備の経路を設定するものになります。フローティングスタティックルートは設定したとしてもルーティングテーブルには反映されないため、当てはまりません。

よって、**D**が正解となります。

A43. B, C, E

show interfaces trunkコマンドで、スイッチ上でトランクポートになっているインターフェイスを一覧表示することができます。Mode欄に表示されているonは、手動でトランクポートに設定したということを表しています。Encapsulation欄にはカプセル化タイプが表示されます。Native vlan欄には各ポートに設定されているネイティブVLANが表示されます。

A. Port欄に表示されているポートがトランクポートとして動作しています。Fa0/1からFa0/5までのように、複数のポートを示しているわけではありません。

D. Vlan allowed and active in management domain欄に表示されているVLANが、現在アクティブになっているVLANです。VLAN1,10,20,30となっているので誤りです。

F. Native vlan欄に表示されているVLANが、そのポートで設定されているネイティブVLANです。デフォルトのネイティブVLANはVLAN1なので、Fa0/5ではネイティブVLANは変更されていません。

よって、**B, C, E**が正解となります。

A44. D

一般的なクラウドサービスには、大きく分けて以下の3つの種類があります。

- SaaS（Software as a Service）
- PaaS（Platform as a Service）
- IaaS（Infrastructure as a Service）

IaaSは、物理サーバ、ネットワーク、インフラ部分だけが提供されるサービスです。独自のオペレーティングシステムや開発環境を使

用したい場合はIaaSを選ぶことになります。

よって、**D**が正解となります。

A45. C

FHRP(First Hop Redundancy Protocol)で使用される仮想MACアドレスは、以下の通りです。

- VRRPの仮想MACアドレス「0000.5E00.01XX」
- HSRPの仮想MACアドレス「0000.0C07.ACXX」（version1）
- HSRPの仮想MACアドレス「0000.0C9F. FXXX」（version2）
- GLBPの仮想MACアドレス「0007.B40X.XXYY」

よって、**C**が正解となります。

A46. C, E

QoSのアーキテクチャには「ベストエフォート」「IntServ」「DiffServ」の3つのアーキテクチャがあります。ベストエフォートでは、パケットの優先順位などは考慮せず、先に来たものを先に出すという処理を行います。

IntServは、RSVPを使用してフローが必要とする帯域をあらかじめ確保しておくアーキテクチャです。対象となるアプリケーションが増えてくると、帯域確保用のRSVP自体の負荷が高くなってくるという欠点があります。

DiffServは、各ルータやスイッチごとにパケットの優先順位に基づいて区別して転送処理を行うアーキテクチャです。イーサネットフレームの優先度を表すCoSや、IPパケットの優先度を表すDSCPやIP Precedenceを利用します。またホップごとの動作を決めたPHBに応じて、トラフィックが処理されます。PHBにはRFCで規定されたものがあり、音声パケットは優先度の高いDSCP46のEFというPHBに分類されます。

よって、**C, E**が正解となります。

A47. A

ワイヤレスLANコントローラ（WLC）を使用すれば、集中管理型アクセスポイント（Lightweight AP）には設定を行わず、WLCで設定を行いますので、各アクセスポイントには個別に設定する必要がなくなります。なお、ワイヤレスLANコントローラは多くのアクセスポイントを導入するような中・大規模ネットワークに適しています。

よって、**A**が正解となります。

A48. A

経路選択の際の基準は、ルーティングプロトコルによって決まっており、「メトリック」といわれます。OSPFでは帯域幅をもとに計算される「コスト」が該当します。また、RIPでは「ホップ数」（ルータをまたぐ回数）が判断基準となります。なお、「アドミニストレーティブディスタンス値」は、複数の異なるルーティングプロトコルで同じ宛先への経路を学習した場合の優先順位の決定に使用されます。

よって、**A**が正解となります。

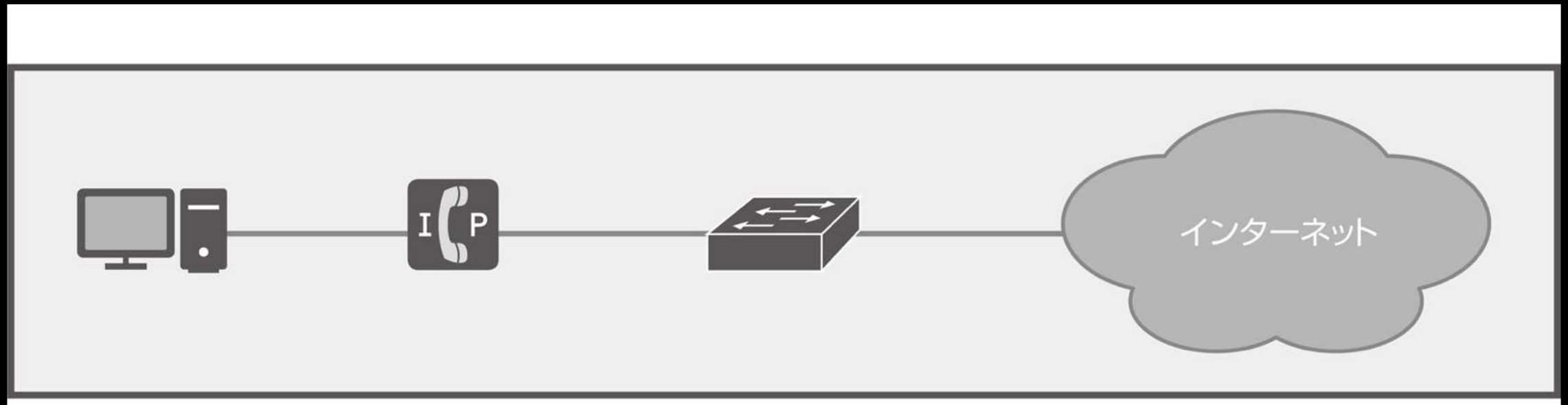
A49. B, D

VLANを実装することにより、スイッチ上で論理的にネットワークを分割することができます。その結果、ブロードキャストドメインが分割できるため、ブロードキャストのトラフィックが必要以上に送信されなくなり、ブロードキャストトラフィックの軽減が可能です。また、セキュリティの向上や、物理的な配置に依存しないネットワークが構築できるといったメリットもあります。なお、異なるVLAN間の通信を行うにはルータなどのL3の機器を用いてルーティングの設定を行う必要があります。

よって、**B, D**が正解となります。

A50. B

Cisco製のIP電話は、PCと接続するポートとスイッチと接続するポートの2つのポートを持ちます。そのため、IP電話を配置する場合は以下のような構成とすることができます。



ただ、同一のケーブル上を、「PCから送信されるHTTPなどの通信のデータ」と、「IP電話から送信される音声データ」が通過するため、音質に悪影響を与えるおそれがあります。（ノイズや音声の遅延など）。そのため、音声データを優先的に相手に届けることができるように、音声VLANを設定することができます。

スイッチでは、「通常のデータを送受信するためのVLAN」と、「音声データを送受信するためのVLAN」という形で2つのVLANを作成し、音声データはVLANタグを付けて通信します。VLANタグを使用しますが、設定上はアクセスポートの設定で、通信することが可能となっています。

なお、IP電話側ではVLANの設定などは必要なく、スイッチからのCDPによってVLAN番号を教えてもらう形となります。そのため、CDPは有効にしておく必要があります。

よって、**B**が正解となります。