解答・解説

A1. D

ネットワークアドレスとブロードキャストアドレスを求める方法はいくつかありますが、ここでは計算によって求める方法で解説します。

①計算対象となるオクテットに残っているホスト部のビット数だけ2の累乗計算をする

今回はサブネットマスクが255.255.255.240、つまり/28のため、ネットワーク部とホスト部の境界が第4オクテットにあることがわかります。第4オクテットのホスト部の残りのビット数が4のため、①で求められる値は$2^4 = 16$となります。

②対象オクテットの数字を①の計算結果で割り商を出す

求めるIPアドレスの第4オクテットの値147を16で割り商を出します。147÷16なので、商は9となります。

③①の結果と②で計算した商を掛け算した結果を計算対象オクテットの値とし、右のオクテットを0にするとネットワークアドレスとなる

①で求めた16と②で求めた9を掛けあわせると、16×9＝144となり、これがネットワークアドレスの第4オクテットの値となります。192.168.10.144/28がネットワークアドレスということが求められました。

④③の答えと①の答えを足して－1した結果を計算対象オクテットの値とし、右のオクテットを255にするブロードキャストアドレスとなる

この問題では問われていませんが、ブロードキャストアドレスも求めてみましょう。144＋16＝160となり、この値が連続する次のネットワークのネットワークアドレスの値となります。それより1つ手前までが該当ネットワーク内のIPアドレスとなりますので、160－1＝159から、ブロードキャストアドレスは192.168.10.159/28となります。

よって、**D**が正解となります。

A2. B

ダイナミックルーティングプロトコルでは、同じネットワークへの複数の経路を学習した場合、メトリックによって最適な経路を決定します。どのルーティングプロトコルでもメトリックが最小となる経路が最適な経路となります。OSPFでは10^8÷帯域幅（bps）で求められるコストの値をメトリックとして使用し、宛先ネットワークまでのコストの累計値が最も小さい値になるルートを最適経路として選択します。

A. EIGRPのメトリックについての記述になります。

C. OSPFではFastEthernetもGigabitEthernetもデフォルトのコストの値は1となります。それぞれ19や4といった値は、STPのデフォルトのパスコストの値のため誤りです。

D. RIPのメトリックについての記述になります。

よって、**B**が正解となります。

A3. C

コマンドの出力結果の3行目ネットワークタイプ（Network Type BROADCAST）と8行目の表示（Hello 10, Dead 40）から、デフォルトのHelloインターバルとDeadインターバルが使用されていることがわかります。

A. 出力結果の5行目の表示（State）から、このルータはDROTHERに選出されていることがわかります。

B. OSPFが有効化されていない場合は、show ip ospf interfaceコマンドを実行しても情報が一切出力されません。

D. 出力結果の3行目の表示（Network Type BROADCAST）から、このインターフェイスではOSPFネットワークのタイプがブロードキャストに設定されていることがわかります。

よって、**C**が正解となります。

A4. B, D

ワイヤレスLANコントローラではGUIを使用して設定を行うことができ、WLANを作成することでSSIDの作成や認証方法の設定が可能です。

SSIDを設定するには、GUI画面上部の［WLANs］を選択します。新たに作成する場合は、画面右上の［Create New］をメニュー選択している状態で［Go］を選択します。表示される次の画面で、「Profile name」と「SSID」に任意の文字列を入力して、最後に右上の［Apply］を選択します。

A, C. 事前共有鍵認証（PSK認証）におけるパスワードのフォーマット（PSK Format）を指定する場合に、ASCIIとHEXを選択することができます。

E. WLANを作成する際は、SSIDに紐づくダイナミックインターフェイスを指定します。ダイナミックインターフェイスを作成する際にVLAN IDを設定しますので誤りです。

よって、**B, D**が正解となります。

A5. A

この問題で設定しているデフォルトルートは、アドミニストレーティブディスタンス値を200に変更しています。ルーティングテーブルから確認できるOSPFのアドミニストレーティブディスタンス値は110のため、新しくデフォルトルートを設定したとしても、OSPFで学習した既存のデフォルトルートが優先されます。そのため、OSPFで学習した既存のデフォルトルートが削除されるまでは新しいデフォルトルートは反映されません。

よって、**A**が正解となります。

A6. C, D

JSONデータの形式は、メンバの値が数値の場合、引用符（'や"）なしで記述します。また、値が配列の場合は、［値1,値2,値3,...］のように記述します。

A, B. メンバはキーと値により構成されますが、キーと値の間は「:」（コロン）で区切ります。

よって、**C, D**が正解となります。

A7. C

IEEE802.1Qトランクリンクで異なるネイティブVLANを設定した場合、異なるネットワークのフレームがタグなしで送信されるので、ネットワーク構成に矛盾が生じる場合があります。今回の設定では、Switch1から送信されたVLAN10のフレームが、Switch2ではVLAN100のフレームと判断されてしまいます。そのため、Switch1のVLAN10の機器とSwitch2のVLAN100の機器が同一のネットワークとして扱われてしまうことになります。

A. 通信ができる・できないに関係なく、ネイティブVLANが異なっていたとしても、トランクリンクは形成されリンクがアップします。

B. ネイティブVLANが異なっていたとしても、ポートがerr-disableになることはありません。

D. 一般的にはあり得ませんが、Switch1配下のVLAN10の機器と、Switch2配下のVLAN100の機器に同じネットワークのIPアドレスが設定されていた場合、通信はできてしまいます。（ただし、ネットワークのIPアドレスに整合性が取れなくなってしまうため、そのような構成にすることはまずありません。）

よって、**C**が正解となります。

A8. C

図のようなCDPで収集した隣接機器の情報を表示するには、show cdp neighborsコマンドを実行します。これにより、隣接機器の名前や型番などを一覧で表示することができます。

A. show cdpコマンドは、CDPパケットの送信間隔やホールド時間、有効化されているCDPのバージョンを確認できるコマンドです。

B. show cdp interfaceコマンドは、インターフェイス単位でCDPが動作しているかどうかや、CDPパケットの送信間隔やホールド時間を確認できるコマンドです。

D. show cdp neighbors detailは、隣接機器のIPアドレスなどCDPで収集した詳細情報を表示するコマンドです。

よって、**C**が正解となります。

A9. A

多くのREST APIはHTTPやHTTPSを使用します。HTTPやHTTPSでは、リソースに対して実行したい操作を示すいくつかのメソッドを用意しています。

アプリケーションが必要としている主要な４つの基本機能を「CRUD]」といい、CRUDの「Create」に該当するHTTPのリクエストメソッドは「PUT」となります。

B. CRUDの「Read」に該当するHTTPのリクエストメソッドが「GET」になります。

C.「READ」というHTTPのリクエストメソッドは存在しません。

D. CRUDの「Delete」に該当するHTTPのリクエストメソッドが「DELETE」になります。

よって、**A**が正解となります。

A10. D

SNMPのセキュリティレベルは表のようになっています。

表　SNMPセキュリティモデルとSNMPセキュリティレベルの組み合わせ

モデル	レベル	認証	暗号化	意味
v1	noAuthNoPriv	コミュニティ名	なし	コミュニティ名を使用して認証を行う
v2c	noAuthNoPriv	コミュニティ名	なし	コミュニティ名を使用して認証を行う
v3	noAuthNoPriv	ユーザ名	なし	ユーザ名を使用して認証を行う
v3	authNoPriv	MD5またはSHA	なし	HMAC-MD5またはHMAC-SHAアルゴリズムに基づく認証を行う
v3	authPriv	MD5またはSHA	DES、AES	HMAC-MD5またはHMAC-SHAアルゴリズムに基づく認証を行い、データをDESかAESにより暗号化する

よって、**D**が正解となります。

A11. B

show lacp naighborコマンドでは、EtherChannelを形成している隣接機器の状態などを確認することができます。表示結果の「Flags」の欄に記載されているPから、Fa0/3とFa0/4と隣接する対向スイッチのポートがpassiveモードで設定されていることが読み取れます。LACPのモードにはactiveとpassiveがありますが、passiveモード同士ではEtherChannelを形成することができないため、自身がactiveモードであることがわかります。

よって、**B**が正解となります。

A12. C

IPv6アドレスのプレフィックス部分を手動で指定し、インターフェイスIDを自身のMACアドレスから自動生成してIPv6を割り当てるには、IPv6アドレスを設定する際にeui-64オプションを指定してコマンドを実行します。コマンドで指定するIPv6アドレスにはプレフィックス部分のみを入力することで、自動的にインターフェイスIDがEUI-64形式で付与されたIPv6アドレスが設定されます。

A. DHCPサーバによりIPv6アドレスを設定する方法です。プレフィックス部分もDHCPサーバから自動で付与されます。

B. SLAACでIPv6アドレスを設定する方法です。この場合もプレフィックス部は同一ネットワーク内のルータからRAメッセージで通知されるため、自身で指定しているわけではありません。

D. IPv6アドレスの設定時にlink-localオプションを付けると、リンクローカルユニキャストアドレスが設定されます。なお、リンクローカルユニキャストアドレスはFE80ではじまるアドレスのため、2001からはじまるアドレスを指定した場合はエラーとなり、コマンドが受け付けられません。

よって、**C**が正解となります。

A13. A

スイッチは、宛先MACアドレスが自身のMACアドレステーブルに登録されていないフレームを受信すると、通信をフラッディングします。書籍の第1章でフラッディングの動作は受信したポート以外のすべてのポートから送信すると説明しましたが（書籍P32参照）、VLANを作成している場合は、同一VLAN内に属する受信ポート以外のすべてのポートへと送信します。

よって、**A**が正解となります。

A14. B, E

show interfacesコマンドでは、インターフェイスの表示結果の下部から、入出力関連のエラー回数やエラーパケット数を確認することができます。late collisionの項目では、レイトコリジョンが発生した回数を確認することができます。レイトコリジョンはケーブルが長すぎたり、半二重全二重のミスマッチ、NICの不調などで発生します。

よって、**B, E**が正解となります。

A15. C

OSPFでは、リンクのレイヤ2プロトコルによってデフォルトのネットワークタイプが異なります。ネットワークタイプによってHelloインターバルやDeadインターバルの間隔が異なっていたり、DRとBDRの選出を行うかどうかなどの動作が異なります。

表　OSPFのネットワークのタイプ

タイプ	DRとBDRの選出	Helloパケットによるネイバーの自動検出	Hello/Deadインターバル	例
ブロードキャスト	○	○	10秒／40秒	イーサネット
NBMA（Non-Broadcast Multiple Access）	○	×	30秒／120秒	フレームリレー
ポイントツーマルチポイント	×	○	30秒／120秒	
ポイントツーマルチポイント（ノンブロードキャスト）	×	×	30秒／120秒	
ポイントツーポイント	×	○	10秒／40秒	PPP（第13章）

GigabitEthernetインターフェイスで接続した場合は、レイヤ2プロトコルがEthernetとなるため、デフォルトのネットワークタイプはブロードキャストとなります。

よって、**C**が正解となります。

A16. A, B

ルータにIPv6アドレスを設定すると、そのインターフェイスは自動でいくつかのマルチキャストグループに参加します。

表　マルチキャストグループ

アドレス	説明
FF02::1	リンクローカル内の全ノード宛のマルチキャストグループ
FF02::2	リンクローカル内の全ルータ宛のマルチキャストグループ
FF02::1:FFxx:xxxx	要請ノードマルチキャストアドレスのマルチキャストグループ。xx:xxxxはインターフェイスのIPv6アドレスの下から24ビットが入る

C. 全OSPFルータ宛のマルチキャストグループです。インターフェイスでIPv6のOSPFを有効化するとこのマルチキャストグループに参加します。
D. OSPFで選出されたDR・BDR宛のマルチキャストグループです。インターフェイスでIPv6のOSPFを有効化し、DRもしくはBDRに選出されるとこのマルチキャストグループに参加します。
E. 全RIPルータ宛のマルチキャストグループです。インターフェイスでIPv6のRIPを有効化すると、このマルチキャストグループに参加します。
なお、IPv6のダイナミックルーティングについてはCCNAの試験範囲外となります。
よって、**A, B**が正解となります。

A17.C

172.16.100.1宛のパケットは、ルーティングテーブル上の「O 172.16.100.0/24」に該当します。2つの経路が登録されているため、等コストロードバランシングの機能が働き、トラフィックを両経路に分散して送信します。
よって、**C**が正解となります。

A18.B

ワイヤレスLANコントローラにおいて設定できるACLの種類には、通常のACLのほか、CPU ACL、FlexConnect ACL、Layer2 ACLなどがあります。CPU ACLを設定することで、管理インターフェイス宛のパケットをフィルタリングすることができるため、ワイヤレスLANコントローラに接続してインバンド管理を行う機器を制限することなどが可能です。
よって、**B**が正解となります。

A19.C

従来のネットワーク構成では、それぞれの機器にデータプレーンとコントロールプレーンの機能が分散し、1つ1つの機器に接続して個別に設定を行う必要がありました。しかし、コントローラベースのネットワーク構成では、SDNコントローラにコントロールプレーンの機能が集約され、各機器ではデータプレーンのみが動作します。また、SDNコントローラにより各機器を集中管理・集中制御するため、ネットワークの管理効率も従来のネットワーク構成よりも向上します。
A. 従来のネットワークでは、各機器でデータプレーンとコントロールプレーンが動作します。述べられているのはコントローラベースのネットワーク構成の特徴のため誤りです。
B. 従来のネットワークでは、各機器にそれぞれ個別に設定を行います。この選択肢もコントローラベースのネットワーク構成の特徴のため誤りです。
D. コントローラベースのネットワーク構成では、SDNコントローラによる集中制御を行いますので誤りです。

よって、**C**が正解となります。

A20. D

JSONのデータ形式には様々な書式ルールがありますが、この問題では各選択肢の誤っている箇所を見ていきましょう。

A.「"キー ": 値」のペアで構成されているメンバに、さらにメンバが続く場合には「,」（カンマ）で区切らなくてはなりません。「;」（セミコロン）は誤りです。

B. メンバは「"キー ": 値」のペアで構成され、キーと値の間は「:」（コロン）で区切ります。「-」（ハイフン）は誤りです。

C.「"キー ": 値」のペアで構成されているメンバに、さらにメンバが続く場合には「,」（カンマ）で区切らなくてはなりません。「.」（ドット）は誤りです。

よって、**D**が正解となります。

A21. A, D

パケット受信時にルータでCRCチェックに失敗すると、show interfacesコマンドの「CRC」の項目の値が増加します。CRCチェックの失敗は、コリジョンが発生した場合や通信モードの不一致によって発生します。また、入力関連のエラー数の合算を表示する「input errors」の項目も同時に増加します。

B. runtsは、パケットの最小サイズを満たさないために破棄されたパケットです。この値は、通信モードの不一致やケーブルなどの接続関連のトラブルによって増加します。

C. giantsは、パケットの最大サイズを超えたために破棄されたパケットです。この値は、NIC が不良状態のときに増加します。

E. frameは、オクテット数が整数値となっていない不正なパケットです。

F. ignoredは、受信したデータがバッファ不足により破棄されたパケットです。この値は、ブロードキャストストームが発生した場合に増加します。

よって、**A, D**が正解となります。

A22. B

Cisco製のIP電話には、PCと接続するためのポートとスイッチに接続するためのポートの2つのLANポートがあり、PCからの通信はそのままIP電話を通過し、スイッチへと転送されます。また、IP電話からの通信にはVLANタグが付けられ、VLANタグ内のCoS値を設定することで、IP電話からの通信を優先するといったQoSの設定を行うことができます。そのため、PCとIP電話はそれぞれ異なるVLANに属する構成になります。

よって、**B**が正解となります。

A23. A

HSRPは、デフォルトゲートウェイとなるルータを冗長化する技術です。複数台のルータを用意してそのルータでスタンバイグループを形成し、仮想IPアドレスとMACアドレスを持った1台の仮想ルータとしてふるまうことで、冗長化を行うことができます。スタンバイグループ内からアクティブルータとスタンバイルータを選出して、アクティブルータに選出されたルータが実際のデフォルトゲートウェイとして動作し、ARP応答や通信の転送を行います。

B. GLBPの説明なので誤りです。HSRPではアクティブルータに選出されたルータのみが通信の転送を行うため、通信の負荷分散をすることはできません。

C. スタンバイルータはアクティブルータのバックアップとなるルータで、アクティブルータに障害が起きた際にその役割を引き継いで動作します。そのため、アクティブルータとスタンバイルータの両方が同時にデフォルトゲートウェイとして動作して負荷分散を行うことはありません。

D. HSRPのHelloパケットは、ICMPではなくUDPを使用しているため誤りです。

よって、**A**が正解となります。

A24. A

OSPFでは、default-information originateコマンドを実行することで、デフォルトルートを他のルータに配布することが可能です。また、originateの後ろにalwaysオプションを付けると、自身にデフォルトルートを設定していなくても、デフォルトルートを他のルータに配布することができます。この問題の構成では、Router1とRouter2の両方にデフォルトルートが必要となります。そのため、Router1に手動でデフォルトルートを作成します。その結果、Router2はRouter1からデフォルトルートが配布され、Router2にもデフォルトルートが作成されてインターネット方向とも通信が可能となります。

B. alwaysオプションを付けることで、Router2にデフォルトルートを配布することができますが、Router1にデフォルトルートが登録されていないため、インターネット方向への通信がRouter1で破棄されてしまい、通信を行うことができません。

C. Router2に手動でデフォルトルートを作成したとしても、Router1にデフォルトルートが作成されていないため、インターネット方向への通信がRouter1で破棄されてしまい、通信を行うことができません。

D. Router2でdefault-information originateコマンドを実行しても、Router1にもRouter2にもデフォルトルートは作成されませんので誤りです。

よって、**A**が正解となります。

A25. D

設定しようとしている10.53.12.35 255.255.255.252は、ブロードキャストアドレスに該当します。ブロードキャストアドレスは、ブロードキャストを使用する際に宛先として指定されるアドレスなので、端末やルータのインターフェイスなどに割り当てることはできません。「Bad mask ～」といったエラーメッセージは、何らかの理由で使用できないIPアドレスを設定しようとした際に表示されるメッセージになります。

よって、**D**が正解となります。

A26. C

NATによるアドレス変換テーブルのエントリを確認するには、show ip nat translationsコマンドを実行します。次の出力結果はスタティックNATによる変換が行われた際の例となります。

例　NATテーブルの確認

```
Router1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.0.2         192.168.0.10       ---                ---
```

A. NATによるアドレス変換の統計情報を表示するコマンドになります。

B. running-configでは設定したコマンドしか確認できないため、アドレス変換テーブルのエントリまでは確認することができません。

D. このコマンドでキャッシュに保存されたルーティングエントリを確認することができますが、CCNAの範囲外のコマンドとなります。

よって、**C**が正解となります。

A27. C

ネイティブVLANの機能はIEEE802.1Qを使用したトランクリンクにのみある機能で、ISLには存在しません。デフォルトではVLAN1となっていて、ネイティブVLANに割り当てられたVLANはタグを付加せずにそのまま送信をします。なお、コマンドでネイティブVLANを変更することも可能です。

A. IEEE802.1Qトランクリンクでは、デフォルトでネイティブVLANは有効となっています。セキュリティの問題から、ネイティブVLANでもタグを付けるようにすることができますが、その際はvlan dot1q tag nativeコマンドを実行する必要があります。

B. ネイティブVLANはデフォルトでVLAN1が割り当てられていますが、割り当てられたVLANはタグを付加せずに、そのまま送信するため誤りです。

D. ネイティブVLANはデフォルトでVLAN1が設定されていて、コマンドで変更

することが可能です。ランダムに決定されることはありません。
よって、**C**が正解となります。

A28. A, D

EtherChannelでは、L2ポートやL3ポート（L3スイッチの場合）をバンドル化することができます。L3ポートはルータのインターフェイスと同様の操作をすることができますので、ACLやIPアドレスの設定を行うことが可能です。ポートセキュリティやIEEE802.1Xの設定は行うことができないため、注意が必要です。
よって、**A, D**が正解となります。

A29. C, D

問題文のNAT変換テーブルは、通信を行う前からエントリが存在するため、スタティックNATを設定した際に作成される変換テーブルになります。スタティックNATは、1対1で変換するテーブルをあらかじめ作成しておく方法です。スタティックNATの設定を行うには、(config)#ip nat inside source static ＜内部ローカルアドレス＞＜内部グローバルアドレス＞コマンドを実行します。＜内部ローカルアドレス＞に変換対象となるローカルIPアドレスを指定し、＜内部グローバルアドレス＞に変換後のグローバルIPアドレスを指定します。
よって、**C, D**が正解となります。

A30. A, C, F

SDNコントローラを実装したコントローラベースのネットワークでは、SDNコントローラがコントロールプレーンの動作を担い、各ネットワーク機器上ではデータプレーンのみが動作します。データプレーンとコントロールプレーンの主な機能は、次のようになっています。

表　データプレーンとコントロールプレーンの主な機能

分類	機能
データプレーン	・ルーティングテーブルの検索 ・MACアドレステーブルの検索 ・パケットのカプセル化、非カプセル化 ・IEEE802.1Qタグの追加、削除 ・NAT変換 ・フィルタリング など
コントロールプレーン	・ルーティングテーブルの作成 ・MACアドレステーブルの作成 ・ARPによるアドレス解決 など

よって、**A, C, F**が正解となります。

A31. A, C, E

REST APIでサポートされているデータ形式には様々なものがありますが、JSON、XML、YAMLが代表的なものになります。他の選択肢は該当しません。
よって、**A, C, E**が正解となります。

A32. A, C, E

レイヤ3スイッチにはスイッチポート、ルーテッドポート、SVIの3つのポートが存在します。それぞれの役割について整理しておきましょう。

・スイッチポート

レイヤ2スイッチのポートと同様に、アクセスポートやトランクポートの設定を行う物理ポートです。レイヤ3スイッチの物理ポートはデフォルトでスイッチポートとして動作していますが、一度ルーテッドポートに変更したポートを再度スイッチポートに戻すには、該当ポートで(config-if)#switchportコマンドを実行します。

・ルーテッドポート

物理ポートをルータのインターフェイスとして動作させるポートです。IPアドレスの設定やACLの設定など、ルータのインターフェイスと同様の設定が可能になります。スイッチポートからルーテッドポートに切り替えて動作させるには、該当ポートで(config-if)#no switchportコマンドを実行します。

・SVI（Switch Virtual Interface）

スイッチ内部に存在する仮想インターフェイスで、各VLANに紐づく内部のスイッチと接続するルータのインターフェイスとして動作します。ルーテッドポートと同様に、IPアドレスの設定やACLの設定などが可能です。SVIを作成するには、(config)#interface vlan ＜VLAN番号＞コマンドを実行します。
よって、**A, C, E**が正解となります。

A33. B, E

ネットワークの自動化によりそれぞれの機器に対して都度設定を行うことなく、ネットワークの集中管理・集中制御が可能になります。その結果、運用や管理にかかる時間や人員を削減することができ、運用コストや管理コストを減少させることが可能になります。また、ネットワークの構成を変更する際にかかる時間も抑えることが可能です。
よって、**B, E**が正解となります。

A34. B

Cisco ACIで使用されるSDNコントローラの名称はAPICです。

A. Cisco DNA CenterはCisco SD-Accessで使用されるコントローラのため誤りです。
C,D. サウスバウンドAPIの名称のため誤りです。
よって、**B**が正解となります。

A35. B, D

大量の通信が届いたとき、送信されるパケットよりも受信するパケットが多くなってしまいキューにパケットがたまってしまいます。テールドロップとは、キューがいっぱいになると、以後到達するパケットはすべて優先順位に関係なく破棄することを指します。テールドロップの発生を回避するために、REDやWREDといった輻輳管理の仕組みがあります。WREDでは、キューがいっぱいになる前にパケットの優先順位を考慮しながら少しずつパケットを破棄することで、テールドロップの発生を回避しています。
よって、**B, D**が正解となります。

A36. C, D

RSTPではSTPの非指定ポートの役割を細分化し、代替ポートとバックアップポートという役割が新たに作られています。そのため、STPと比較するとポートの役割が3つから4つに増えています。ポートの状態（ステータス）はSTPでは5つの状態が定義されていますが、RSTPではSTPのディセーブルとブロッキングとリスニングがディスカーディングという役割に統一されているため、5つから3つに減っています。また、RSTPは通常のSTPで最大50秒ほどかかっていたコンバージェンスの時間を、数秒程度に短縮することができます。
よって、**C, D**が正解となります。

A37. A

PortFastなどが設定されているポートは、PCなどの端末と接続することが前提となっており、スイッチなどと接続するとブロードキャストストームが発生してしまう可能性があります。BPDUガードを設定すると、そのポートでBPDUを受信するとエラーディセーブル状態となり、強制シャットダウンすることでSTP環境を保護します。また、BPDUガードはグローバルコンフィギュレーションモードとインターフェイスモードで設定することができます。グローバルコンフィギュレーションモードでは(config)#spanning-tree portfast bpduguard defaultコマンドを実行することで、PortFastが設定されているポートすべてでBPDUガードを有効化することができます。インターフェイスモードでは、(config-if)#spanning-tree bpduguard enableコマンドによって、PortFastの設定の有無に関係なく対象インターフェイスでBPDUガードを有効化できます。
よって、**A**が正解となります。

A38. A, C

トラフィックの通信量を制限する方法には、ポリシングとシェーピングの2つがあります。シェーピングは設定値やCIRを超過した分は破棄せずにバッファに保持し、遅れて送信します。また、パケットを発信する際のアウトバウンド方向にのみ適用することが可能です。

B. しきい値を超えたパケットを再マーキングして送信することはありません。

D, E. ポリシングの説明になるため誤りです。

よって、**A, C**が正解となります。

A39. B, E

問題文の条件と作成されているACLを確認すると、Web通信とTELNET通信をブロックし、それ以外すべての通信を許可するにもかかわらず、ACLにはdenyの条件しか作成されていません。そのため、このACLの条件では暗黙のdenyにより、すべての通信がブロックされてしまいます。また、PC1からサーバ宛への通信であるにもかかわらず、ACLの送信元IPアドレスと宛先IPアドレスが逆になっています。そのため、条件を満たすようにするには、ACLの送信元IPアドレスと宛先IPアドレスを逆に書き換えたACLを作成し直す必要があります。

よって、**B, E**が正解となります。

A40. C

作成されている音声VLANは、show interface［＜インターフェイス＞］switchportコマンドで確認することができます。

例　スイッチポートの確認

```
Switch1#show interfaces FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
(省略)
```

表示結果の最下行の「Voice VLAN」の項目に、音声VLANが作成されている場合は該当するVLAN番号が記載されます。なお、他の選択肢のコマンドでは音声VLANを確認することはできません。

よって、**C**が正解となります。

A41. A

コマンドの表示結果を確認すると、両スイッチともPCと接続しているFa0/10はアクセスポートで接続し、VLAN10に所属していることがわかります。次にスイッチ間のFa0/1の設定を確認すると、どちらもトランクポートとして設定がされており、トランキングプロトコルもIEEE802.1Qとなっていて問題はありません。しかし、ネイティブVLANの設定を確認すると、Switch1ではVLAN1がネイティブVLANとなっていますが、Switch2ではVLAN10がネイティブVLANとなっています。両スイッチ間でネイティブVLANが異なっているため、PC間の通信は失敗してしまいます。
よって、**A**が正解となります。

A42. B

同じ宛先への経路を複数のルーティングプロトコルで学習した場合、アドミニストレーティブディスタンス値の最も小さいルーティングプロトコルで学習した経路がルーティングテーブルに登録されます。

表　デフォルトのアドミニストレーティブディスタンス値とコード

プロトコル	アドミニストレーティブディスタンス値	コード
接続されているネットワーク	0	C
スタティックルート	1	S
eBGP	20	B
EIGRP	90	D
OSPF	110	O
IS-IS	115	i
RIP	120	R
iBGP	200	B

この4つのルーティングプロトコルの中で、最もアドミニストレーティブディスタンス値が小さいルーティングプロトコルはEIGRPとなります。
よって、**B**が正解となります。

A43. B, E

REDやWREDはテールドロップの発生を回避するための機能で、キューが一杯になる前に少しずつパケットを破棄することで輻輳管理を行っています。REDはランダムに破棄するため、優先度の高いパケットが破棄される可能性がありますが、WREDはパケットの優先順位を考慮して優先度の低いパケットから破棄します。

よって、**B, E**が正解となります。

A44. D

ワイヤレスLANコントローラではQoSの設定を行うことができます。設定できるレベルは4段階で、IP電話などの音声通信を行うWLANではレベルをPlatinumという最高レベルに設定することが推奨されています。
よって、**D**が正解となります。

A45. B

ネットワーク上の機器などを一元管理し、CPUやメモリ使用率などのリソース情報などを収集できるプロトコルはSNMPになります。
A. IPアドレスからMACアドレスを解決するためのプロトコルです。
C. IPアドレスを自動で割り当てるためのプロトコルです。
D. メールを送信するためのプロトコルです。
よって、**B**が正解となります。

A46. A

表示結果を確認すると、VLAN100でダイナミックARPインスペクションが設定されていることが読み取れます。Fa0/1がVLAN100のアクセスポートに設定されているため、Fa0/1でもダイナミックARPインスペクションが有効化されています。デフォルトでは信頼できないポートとして動作し、信頼できるポートにするにはip arp inspection trustコマンドを実行する必要があるため、Fa0/1は信頼できないポートとして動作していることがわかります。ダイナミックARPインスペクションの信頼できないポートでは、DHCPスヌーピングバインディングデータベースや手動で作成した対応表を使ってARP通信のチェックを行い、一致しない場合はなりすまし通信として破棄します。
よって、**A**が正解となります。

A47. C

平文で保存されたパスワードを暗号化するには、グローバルコンフィギュレーションモードでservice password-encryptionコマンドを実行します。
A. イネーブルパスワードをMD5アルゴリズムによって暗号化して保存するコマンドですので、平文で保存されたパスワードを暗号化するわけではありません。
B. イネーブルパスワードを平文で保存するコマンドですので誤りです。
D. このようなコマンドはありません。ユーザアカウントのパスワードをMD5アルゴリズムによって暗号化するコマンドは、username ＜ユーザ名＞ secret ＜パスワード＞コマンドです。
よって、**C**が正解となります。

A48. A, C

構成管理ツールの代表的なものには、Ansible、Puppet、Chefがあります。それぞれの特徴を比較して覚えておきましょう。

表　Ansible、Puppet、Chefの特徴比較

ツール名	制御ファイル	構成ファイル書式	サーバ側待ち受けポート	プロトコル	アーキテクチャ	通信形態
Ansible	プレイブック	YAML形式	なし	SSH,NETCONF	エージェントレス	Push型
Puppet	マニフェスト	独自形式	TCP8140番	HTTP/HTTPS	エージェント	Pull型
Chef	レシピ、ランリスト	Ruby言語	TCP10002番	HTTP/HTTPS	エージェント	Pull型

B, D. Puppetの特徴についての説明になります。
E. Chefの特徴についての説明になります。
よって、**A, C**が正解となります。

A49. A

サイト間VPNを使用する場合にデータを暗号化してセキュリティを実装するには、IPsecを使用します。
よって、**A**が正解となります。

A50. C

NATは、プライベートIPアドレスである内部ローカルアドレスをグローバルIPアドレスである内部グローバルアドレスに変換し、インターネット接続などを可能にするアドレス変換技術になります。コマンドの表示結果から、内部グローバルアドレスを示す「Inside global」の欄に記載されているIPアドレスが、NAT変換後の送信元IPアドレスとなります。
よって、**C**が正解となります。

A51. B

スイッチは自身が保持しているMACアドレステーブルの情報に従い、通信を転送します。初期状態や再起動直後のスイッチでは、MACアドレステーブルに何も情報が登録されていませんが、スイッチはデータを転送しながらMACアドレスを学習し、MACアドレステーブルを動的に作成していきます。スイッチは通信を受信すると、その送信元MACアドレスと受信したポートを紐づけてMACアドレステーブルに登録をします。
A. 受信した通信の宛先MACアドレスと受信したポートを紐づけてMACアドレステーブルに登録することはないため誤りです。

C. スイッチは通信を転送する際、自身のMACアドレステーブルに宛先MACアドレスの情報がない場合、フラッディングを行います。通信を破棄することはありません。

D. スイッチがブロードキャストの通信を受信した際は、受信したポート以外のすべてのポートからフレームを転送します。受信したポートからは転送しないため誤りです。

よって、**B**が正解となります。

A52. D

logging console ＜レベル＞コマンドを実行すると、コンソール画面上に出力するログのレベルを指定することができます。＜レベル＞で指定したレベルよりも優先度が高いレベルのログだけが出力されます。そのため4を指定すると、「緊急」「警報」「重大」「エラー」「警告」の重大度が0～4までのログが画面に表示されます。

よって、**D**が正解となります。

A53. D

この問題の図にはIPアドレスが記載されていないため、ルーティングテーブルの表示内容からIPアドレスを読み取らなくてはなりません。ルーティングテーブルに表示される「L」のエントリはローカルルートといい、接続している自身のインターフェイスのIPアドレスが表示されます。その結果から、Router1のGi0/0が172.16.1.1/24、Gi0/1が172.16.10.1と、Router2のGi0/0が172.16.100.1/24、Gi0/1が172.16.10.2/24であることがわかります。通信を行うことができない原因はRouter1に172.16.100.0/24のネットワークへの経路情報が登録されていないことにあるため、ルーティングの設定を行う必要があります。選択肢のコマンドがすべてスタティックルートの設定であるため、ネクストホップであるRouter2のGi0/1、つまり172.16.10.2を指定したものが答えとなります。

よって、**D**が正解となります。

A54. C

ダイナミックARPインスペクションでは、ポートを信頼できるポートと信頼できないポートに分け、信頼できないポートでARP通信をチェックすることでARPスプーフィング攻撃を防ぐことができます。信頼できるポートではチェックを行いませんので、すべての通信が通過可能となります。

よって、**C**が正解となります。

A55. C, D

show spanning-treeコマンドの表示結果から、自スイッチとルートブリッジのブリッジIDや設定されているタイマー、自スイッチの各ポートの役割やその状態を確認することができます。それぞれの選択肢を見ていきましょう。

A. 自身がルートブリッジに選出されている場合は、「Cost」と「Port」が記載されず、「This bridge is the root」と記載されます。つまり、ルートブリッジではないため誤りです。

B. デフォルトのタイマーの秒数はHelloタイマー2秒、最大エージタイマー20秒、転送遅延タイマー15秒ですので誤りです。

C.「Spanning tree enabled protocol rstp」の表示から、RSTPが動作していることがわかります。

D.「Port」の項目では、ルートブリッジに最も近いインターフェイスが記載されます。つまり、Fa0/1がルートポートとなります。

E. 選択肢Dより、Fa0/1はルートポートのため指定ポートは誤りです。

よって、**C, D**が正解となります。

A56. C, E

OSPFはルータコンフィギュレーションモードでnetworkコマンドを実行するか、各インターフェイスでip ospf areaコマンドを実行することで有効化することができます。インターフェイスで実行する場合のコマンドは、ip ospf ＜プロセスID＞ area ＜エリアID＞コマンドとなります。

よって、**C, E**が正解となります。

A57. B, C

ルータのインターフェイスをDHCPクライアントとして設定するには、ip address dhcpコマンドを実行します。そのため、Router1のFa0/0ではこのコマンドを実行する必要があります。また、DHCPサーバが同一ネットワークに存在しない場合は、DHCP DISCOVERなどのブロードキャストがルータを越えて転送されないため、ネットワークの境界に位置するルータでリレーエージェントの設定を行う必要があります。リレーエージェントの設定はブロードキャストが着信するインターフェイスでip helper-addressコマンドを実行するため、Router2のFa0/0でこのコマンドを実行します。

よって、**B, C**が正解となります。

A58. B

光ファイバケーブルは、コアという芯をクラッドが同心円状に覆う構造となっています。データの転送には光信号が用いられ、その光信号がコア部分を反射しながら通過していきます。

よって、**B**が正解となります。

A59. A

ステートレスアドレス自動設定（SLAAC）では、RSメッセージやRAメッセージを使用して、同一ネットワーク内のルータから自身が属するネットワークのプレフィックス情報を取得します。そして、自身のMACアドレスから生成したEUI-64形式のインターフェイスIDを付加して、グローバルユニキャストアドレスを1つ生成・設定します。

よって、**A**が正解となります。

A60. B

ローカル認証に使用するユーザアカウントのパスワードを強力なアルゴリズムで暗号化するには、グローバルコンフィギュレーションモードでusername ＜ユーザ名＞ [privilege ＜特権レベル＞] algorithm-type ＜md5 | scrypt | sha256＞ secret ＜パスワード＞コマンドを実行します。algorithm-type ＜md5 | scrypt | sha256＞を省略すると、MD5アルゴリズムによって暗号化されます。また、VTY接続を有効化するので、VTYポートのラインコンフィギュレーションモードに移行する必要があります。

よって、**B**が正解となります。

A61. C

ルータはルーティングテーブルに経路が登録されていない場合、通信を転送せずに破棄してしまいます。デフォルトルートを設定することで、ルーティングテーブルに該当するエントリがないパケットはすべてデフォルトルートに向けて送信するようになります。デフォルトルートの設定はip route 0.0.0.0 0.0.0.0 ＜ネクストホップ | 出力インターフェイス＞コマンドで行います。

よって、**C**が正解となります。

A62. D

ワイヤレスLANコントローラを使用することで、集中管理型アクセスポイント（Lightweight AP）を一括で管理・設定を行うことができます。ワイヤレスLANコントローラと集中管理型アクセスポイントはCAPWAPなどを使用して両機器間でトンネルを形成するため、相互に通信ができるのであればどのスイッチに接続していても問題ありません。

よって、**D**が正解となります。

A63. B

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をやり取りするためのAPIです。反対にコントロールレイヤとインフラストラクチャレイヤ間をやり取りするためのAPIはサウスバウンドAPIと呼びます。

A. サウスバウンドAPIの説明のため誤りです。

C, D. ネットワーク機器はインフラストラクチャレイヤに該当し、コントローラはコントロールレイヤに該当します。どちらの選択肢もサウスバウンドAPIのため誤りです。

よって、**B**が正解となります。

A64. A

TCPはコネクション型のプロトコルで、データの送信をする前に相手と通信ができるかどうかを確認し、コネクションを確立してからデータを送信します。また、信頼性を確保するためにシーケンス番号による順序制御、確認応答による再送処理、ウィンドウサイズによるフロー制御などを行います。反対にUDPはこれらの処理を行わないため信頼性が低く、コネクションレス型のプロトコルとなります。

よって、**A**が正解となります。

A65. D, E

レイヤ3EtherChannelは、レイヤ3スイッチのルーテッドポートで行います。そのため、まず物理インターフェイスをno switchportコマンドでルーテッドポートに変更する必要があります。また、IPアドレスの設定はEtherChannelの設定を行った後に作成されたPort-channelインターフェイス上で行います。

よって、**D, E**が正解となります。

A66. A

HSRPでは、アクティブルータとスタンバイルータを選出します。この2つの役割はHSRPプライオリティを基準に選出されます。HSRPプライオリティが最も大きいルータがアクティブルータとなり、2番目に大きいルータがスタンバイルータとなります。プライオリティに差がない場合は、HSRPが動作しているインターフェイスのIPアドレスの大小を比較して、アクティブルータやスタンバイルータを選出します。

よって、**A**が正解となります。

A67. B

サブネットマスクが/30の場合、そのネットワークに属するIPアドレスの個数は22=4個となりますが、ネットワークアドレスとブロードキャストアドレスを除いた4－2=2個が実際にホストに割り当てることができるIPアドレスの数となります。同様に考え、/31の場合はIPアドレスの個数は21=2個となりますが、その2個はどちらもネットワークアドレスとブロードキャストアドレスとなるため、ホストに割り当てることができるIPアドレスは0個となってしまいます。/31や/32のネットワークにはホストとなる機器が存在できないため、最小のネットワークは/30となります。

よって、**B**が正解となります。

A68. C

仮想化により1台の物理サーバの上に複数の仮想マシンを作成することができ、それぞれの仮想マシンごとに異なるOSを動かして1台の物理サーバ上で複数台のサーバを運用することが可能になります。仮想化を行うことで、コンピュータが持つリソースを柔軟に仮想マシンに割り当てることができたり、仮想マシンの追加・削除が設定で簡単にできたりといったメリットがあります。

A. コンピュータのリソースをあらかじめ固定で割り当てることなく、可変で柔軟に割り当てたり変更したりすることができます。

B, D. 各仮想マシンは内部的に仮想NICを保持し、その仮想NICが仮想スイッチに接続している構成となり、その仮想スイッチを通して相互に通信することも可能です。

よって、**C**が正解となります。

A69. B

PoE（Power over Ethernet）とは、イーサネットケーブル上で電力を供給することができる技術です。PSEと呼ばれる給電機器からイーサネットケーブルを通してPDと呼ばれる受電機器へと電力が供給されます。電力供給と通信を1本のケーブルで同時に行うことができるということも大きな特徴です。PSEではポートに割り当てられた電力のしきい値を超えると自動でポートをシャットダウンし、エラーディセーブル状態にするという機能があるため、その機能によりPSE自身が電力不足に陥る事態を未然に防ぐことができます。

A. PSEが給電機器、PDが受電機器のため誤りです。

C. 給電機器であるPSEはコンセントなどから電源ケーブルを通じて電力供給を受けます。

D. 電力の供給とデータの転送を同時に行うことができるため誤りです。

よって、**B**が正解となります。

A70. A

IPv4アドレスでは、枯渇問題への対策としてプライベートIPアドレスとグローバルIPアドレスという役割の異なるIPアドレスが定義されています。プライベートIPアドレスは独立した異なるLANであれば重複してもよく、決められた範囲内で自由に設定することができます。

B. プライベートIPアドレスはインターネットでは使えないIPアドレスです。そのためインターネットに出る際はNATによるアドレスの変換を行う必要があります。

C, D. プライベートIPアドレスにこのような役割はありません。

よって、**A**が正解となります。

A71. ①B, F　②D, E　③A, C

Ansible、Puppet、Chefのそれぞれの特徴は以下のようになっています。Q48と同様に、それぞれの特徴を比較して覚えておきましょう。

表　Ansible、Puppet、Chefの特徴比較

ツール名	制御ファイル	構成ファイル書式	サーバ側待ち受けポート	プロトコル	アーキテクチャ	通信形態
Ansible	プレイブック	YAML形式	なし	SSH,NETCONF	エージェントレス	Push型
Puppet	マニフェスト	独自形式	TCP8140番	HTTP/HTTPS	エージェント	Pull型
Chef	レシピ、ランリスト	Ruby言語	TCP10002番	HTTP/HTTPS	エージェント	Pull型

A72. C

スパイン／リーフ型のネットワークでは、スパインスイッチとリーフスイッチという役割に分け、2階層型のネットワークとして構築します。エンドポイントの接続ポートを増やす場合はリーフスイッチを、帯域を増やす場合はスパインスイッチを増やすといったように、ネットワークの拡張をシンプルかつスムーズに行うことができるといった特徴があります。また、スパインスイッチ同士やリーフスイッチ同士は直接接続することないため、フルメッシュ構成とはなりません。エンドポイントの機器同士の通信の際は、リーフスイッチ→スパインスイッチ→リーフスイッチと通信が転送されるため、常に同一ホップ数となることも特徴の一つに挙げられます。

よって、**C**が正解となります。

A73. D

それぞれのルータの設定を確認すると、Router1のFa0/0ではMTUの値が変更され、1600となっています。Router2のFa0/0では設定がないため、デフォルトの1500となっています。OSPFでは両インターフェイスのMTUの値が異なっていると、完全な隣接関係を築くことができません。具体的にはFullステートに遷移せずにExstartもしくはExchangeステートから先に進まなくなります。その結果、ルーティングテーブルが形成できないなどといった障害が発生する可能性があります。

A. networkコマンドではワイルドカードマスクを使用し、有効化したいインターフェイスのIPアドレスが含まれるように指定します。192.168.1.1 0.0.0.0でIPアドレス192.168.1.1単体を指定していますが、実際にRouter1のFa0/0のIPアドレスが192.168.1.1なので問題ありません。

B. OSPFでは必ずバックボーンエリア（エリア0）を作成する必要があります。シングルエリア（1つのエリア）構成で設定する場合も同様のため、シングルエリア構成の場合は必ずエリア0となります。

C. Router2ではパッシブインターフェイスの設定がされていますが、指定されているインターフェイスがRouter1と接続しているFa0/0ではなくFa0/1のため、この場合は関係ありません。

よって、**D**が正解となります。

A74. C

この設問の条件から、PCからRouter1へのTELNETは禁止するが、それ以外の通信、つまりPCとRouter2との通信などは許可する必要があります。選択肢の宛先IPアドレスを確認するとすべてanyとなっているため、Router1のインターフェイスに設定してしまうと、Router2への通信も意図せずブロックされてしまいます。この場合、ACLをVTYポートに適用することで、その機器へのリモートアクセスのみを制御することが可能です。VTYポートにACLを適用するには、VTYのラインコンフィギュレーションモードへ移行し、access-classコマンドでACLを適用します。

A. この設定ではPCからRouter2へのTELNETもブロックされてしまいます。

B. この設定では暗黙のdenyによりすべての通信がブロックされてしまいます。

D. VTYポートにACLを適用する場合はip access-classコマンドではなくaccess-classコマンドとなります。

よって、**C**が正解となります。

A75. D

ポートセキュリティの違反時の動作モードにはprotect、restrict、shutdownの3種類があり、デフォルトのモードはshutdownになっています。transparentは

VTPのモードの一つです。
よって、**D**が正解となります。

A76. A, B

フローティングスタティックルートは、正常時にはダイナミックルーティングプロトコルを利用し、障害発生等でダイナミックルーティングによるルートの学習ができなくなった際にスタティックルートを使用する設定方法です。通常スタティックルートのアドミニストレーティブディスタンス値は1ですが、その値を大きくすることで優先度を下げ、ダイナミックルーティングの経路をプライマリルートとして使用し、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ことができます。
よって、**A, B**が正解となります。

A77. C

ディストリビューションシステムポートは、ワイヤレスLANコントローラを有線LANに接続する物理インターフェイスです。スイッチやアクセスポイントとのデータ転送を行うダイナミックインターフェイスや、ワイヤレスLANコントローラを操作・制御する管理インターフェイスといった論理ポートと接続します。
A. サービスポートは、ワイヤレスLANコントローラに管理アクセスするためのポートですが、LANケーブルを接続するポートです。コンソール接続を行うポートはコンソールポートになります。
B. 2台のワイヤレスLANコントローラを冗長ポートで接続することで冗長化することができますが、特別なケーブルではなくLANケーブルで接続します。
D. ダイナミックインターフェイスは、SSIDに紐づいたデータの送受信を行う論理ポートですが、SSIDに紐づいたVLANごとに異なるネットワークのIPアドレスを設定します。
よって、**C**が正解となります。

A78. C

図の設定では、アクセスポートやトランクポートの設定が同一インターフェイスにされていますが、最後の行にswitchport mode trunkコマンドが設定されているため、このインターフェイスはトランクポートとして動作していることがわかります。このような場合、switchport access vlan 10の設定は無視され、ネイティブVLANの設定、許可VLANの設定、トランキングプロトコルの設定のみが有効になります。したがってこのインターフェイスは、トランクポートとして動作し、ネイティブVLANがVLAN100として動作していることが読み取れます。
よって、**C**が正解となります。

A79. D

NTPサーバとして動作させるには、グローバルコンフィギュレーションモードでntp masterコマンドを実行します。NTPクライアントとして動作させるには、グローバルコンフィギュレーションモードでntp server ＜IPアドレス＞コマンドを実行し、＜IPアドレス＞に同期を取りたいNTPサーバのIPアドレスを指定します。ntp clientというコマンドは存在しません。

よって、**D**が正解となります。

A80. B, D, E

Cisco DNA Centerは、Cisco SD-Accessで使用されるSDNコントローラです。ノースバウンドAPIは、REST APIを、サウスバウンドAPIはTELNET、SSH、SNMP、NETCONF、RESTCONFといった複数のプロトコルをサポートしています。Cisco DNA Centerでは、スケーラブルグループによるアクセス制御が可能で、管理者がエンドポイントのユーザやデバイスをグループとして定義し、そのグループ単位で通信の許可や拒否のポリシーを適用することができます。管理者は適用する機器を考える必要がなく、Cisco DNA Centerにポリシーを指定するだけで完了するため、迅速かつ容易に設定することが可能です。また、SDNコントローラによるコントローラベースのネットワーク全体に当てはまることですが、SDNコントローラで集中管理・制御を行うため、従来のネットワークと比較して迅速にネットワークを管理・展開することが可能となっています。

よって、**B, D, E**が正解となります。

A81. A, E

ルータオンアスティックの構成でのVLAN間ルーティングでは、まずルータにサブインターフェイスを作成し、ルータ側にトランクの設定を行います。トランキングプロトコルと所属するVLANを指定するには、サブインターフェイスコンフィギュレーションモードでencapsulation ＜dot1q | isl＞ ＜VLAN番号＞コマンドを実行します。次に、サブインターフェイスのIPアドレスを設定します。所属するVLANと設定するIPアドレスが誤っていると通信ができません。また、物理インターフェイスをno shutdownコマンドで有効化する必要があるため、注意が必要です。

よって、**A, E**が正解となります。

A82. B

ブルートフォースアタック（総当たり攻撃）はパスワードを破る手法の一つで、パスワードに使用されている文字列を推測し、パスワードが解除できるまで考えられるパターンを試行し続ける攻撃手法です。

A. Dos攻撃やDDoS攻撃の説明になります。
C. フィッシングの説明になります。
D. ソーシャルエンジニアリング攻撃の説明になります。
よって、**B**が正解となります。

A83. C

/26の場合、2^6=64個のIPアドレスがあり、ホストに割り当てられるIPアドレスの数は64－2=62個となります。同様に考えると、/27の場合、ホストに割り当てられるIPアドレスの数は30個となります。よって、この3つのネットワークには/26を割り当てる必要があります。また、LAN内に割り当てるIPアドレスになるため、プライベートIPアドレスの範囲内のアドレスを割り当てなければなりません。
よって、**C**が正解となります。

A84. B, C, F

EIGRPはネイバーからアドバタイズされてきた情報などをもとに、宛先までのすべてのルートのメトリックを計算します。その結果から、最もメトリックが小さいものを最適なルート（サクセサ）とし、最適なルートがダウンした際の予備のルート（フィージブルサクセサ）を用意して切り替えられるようにしています。使用されるアルゴリズムはDUALで、ルーティングテーブル上の表記ではDUALの頭文字を取ったDが使われます。
よって、**B, C, F**が正解となります。

A85. B

通信の宛先IPアドレスがルーティングテーブル上の複数のエントリに該当していた場合、ルータはロンゲストマッチのルールに従って使用するエントリを決定します。設問のルーティングテーブルの場合、192.168.10.1宛の通信は3つのエントリすべてに該当するため、その中で最もプレフィックスが大きいOSPFで学習したエントリを選択します。
よって、**B**が正解となります。

A86. C

AAAの3つの機能の特徴を押さえておきましょう。

Authentication：認証
ネットワークサービスやリソースを利用する際、ユーザIDやパスワードなどの情報をもとに、アクセスが許可されたユーザなのかどうかなどの確認を行うこと。

Authorization：認可
認証により確認が行われたユーザがどういった機能を利用できるのかを決定し、アクセス制限をかけること。
Accounting：アカウンティング
ネットワーク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か、行動を監視して記録すること。
よって、**C**が正解となります。

A87. B

ネットワークを割り当てる場合に特に気を付けることは、「予想されるホストの数のIPアドレスを充分に確保できる大きさのネットワークを割り当てる」ことと「他のネットワークと重複していない範囲のネットワークを割り当てる」ことです。この問題では、28台の端末を接続するネットワークのため、/27より大きなネットワークにする必要があります。/28では、14個しかホストに割り当てることができるIPアドレスがないため不十分です。また、10.1.100.64/26を割り当ててしまうとIPアドレスの範囲が10.1.100.64～127となってしまい、Router3に接続している10.1.100.96/27のネットワークと重複してしまいます。
よって、**B**が正解となります。

A88. D

EUI-64形式によるインターフェイスIDの自動生成の手順は次の通りです。

①48ビットのMACアドレスを24ビットずつに分割する
②16ビットのFFFEを中央に挿入する
③先頭から7ビット目を反転する（0→1または1→0）
④最終的に16進数に戻すとインターフェイスIDになる

よって、**D**が正解となります。

A89. A, E

DHCPを使用することで、端末機器などに自動でIPアドレスを割り当てることができます。ネットワーク機器やサーバなどに手動で設定されたIPアドレスが誤ってDHCPによって割り当てられないように、指定したIPアドレスをプールから除外することもできます。除外するアドレスを指定するには、グローバルコンフィギュレーションモードでip dhcp excluded-addressコマンドを実行します。また、DHCPサーバから割り当てられたIPアドレスはリースによる一時的な貸し出しという形のため、リース期間が過ぎた場合は一度IPアドレスをDHCPサーバに

返却する仕組みとなっています（ただし、できるだけ長く同じIPアドレスを使用できるように、リース期限の半分が経過したタイミングでリースの更新要求を送る、といった仕組みもあります）。

B. DNSサーバのIPアドレスは、1つだけではなく複数設定することが可能です。

C. DHCPクライアントに対して、コンフリクトが発生したIPアドレスの情報が送られることはありません。

D. DHCPサーバから割り当てられたIPアドレスは、決められた期間貸し出すという仕組みのため、無条件で永続的に使用できるといったことはありません。

よって、**A, E**が正解となります。

A90. D

ワイヤレスLANコントローラではリンクアグリゲーション（Link Aggregation：LAG）の設定をすることで、物理ポートのディストリビューションシステムポートをバンドルし、EtherChannelを形成することができます。リンクアグリゲーション機能によって、帯域幅の向上や冗長化を実現できます。なお、ワイヤレスLANコントローラはLACPやPAgPのプロトコルをサポートしていないため、対向のスイッチのEtherChannelのモードはonで設定しなくてはなりません。

A. リンクアグリゲーションの機能は、サービスポートをバンドルするものではありません。

B. リンクアグリゲーションを有効化するには、［CONTROLLER］＞［General］タブ内の「LAG Mode on next reboot」の項目から行います。

C. リンクアグリゲーションの機能は、1つ以上のディストリビューションシステムポートが有効になっていれば有効となります。ただし、1ポートだけしかポートが動作していない場合は、帯域を増やすことはできません。

よって、**D**が正解となります。

A91. C

IPv6アドレスの中でIPv4アドレスのプライベートIPアドレスのようにLAN内のプライベートなネットワークで使用するアドレスは、ユニークローカルユニキャストアドレスです。

A. IPv4のグローバルIPアドレスに相当するアドレスで、インターネット上で一意となるアドレスです。

B. 同一サブネット上でのみ通信が可能なアドレスです。

D. 特定のサイト内でのみ利用可能なアドレスですが、現在は廃止されていて利用されていません。

よって、**C**が正解となります。

A92. C

音声VLANの設定は、ポートをアクセスポートとして設定し、通常のVLANと音声VLANの2つのVLANを割り当てます。PCが属するVLANは通常のアクセスポートに割り当てられたVLANを、IP電話が属するVLANは音声VLANとして割り当てられたVLANをそれぞれ使用することで、PCとIP電話の通信を分離してQoSを設定することができます。問題文の設定では音声VLANが50として設定されていますが、switchport access vlan ＜VLAN番号＞のコマンドが設定されていないため、アクセスポートのVLANはデフォルトの1となっていることが読み取れます。

よって、**C**が正解となります。

A93. C

EIGRPはDUALというアルゴリズムを使用してメトリックの計算を行います。帯域幅、遅延、信頼性、負荷、MTUの5つの値にK値という重みを掛けてメトリックを計算しています。

よって、**C**が正解となります。

A94. A, B

ダブルタギング攻撃は、ネイティブVLANを悪用した攻撃手法で、攻撃者がトランクリンクのネイティブVLANと同じVLANに属している場合に使用される方法です。ダブルタギング攻撃に対しては、VACLを適用して通信を制御する、スイッチのアクセスポートにVLAN1以外を割り当てる、ネイティブVLANを未使用のVLAN IDに設定する、ネイティブVLANでもタグが付くなどの設定をする、といったことで対策を行います。

よって、**A, B**が正解となります。

A95. A

隣接機器の情報を取得するプロトコルにはCDPやLLDPがありますが、CDPはCisco独自のプロトコルのため、隣接機器がCisco製品でなければ情報を取得することはできません。一方、LLDPを使用すれば、隣接機器が異なるベンダの製品でも情報を取得することができます。Cisco機器ではLLDPはデフォルトで無効となっているため、有効化するにはグローバルコンフィギュレーションモードでlldp runコマンドを実行します。実行すると、すべてのインターフェイスでLLDPが有効化されます。また、インターフェイスごとに個別に有効化する場合は、インターフェイスコンフィギュレーションモードでlldp transmitやlldp receiveコマンドを使用して、それぞれ送信または受信を有効化する必要があります。なお、lldp enableというコマンドは存在しません。

よって、**A**が正解となります。

A96. B

ACLの設定で、想定とは異なる動作をしている場合にはACLの条件やその記載順序、適用インターフェイスやインバウンド・アウトバウンドの向きなどを確認する必要があります。

A. ACLにpermitの条件を記載していない場合、すべての通信がブロックされます。そのため、想定よりも多くの通信がブロックされると考えられます。

B. ACLは条件が記載されたエントリを上から順番に処理していくため、上の行にあるほど優先されます。そのため、先頭行にすべての通信を許可する条件が記載されていると、それ以降にdenyによる拒否の条件を記載したとしても効果を発揮せず、本来ブロックされるべき通信もフィルタリングされずに転送されてしまいます。

C. ACLでは、ワイルドカードマスクを使ってIPアドレスの範囲を指定することができます。permitの条件に登録するワイルドカードマスクを誤って0.0.0.0に設定してしまうと、そのIPアドレス単体を許可する指定になるため、想定よりも多くの通信がブロックされると考えられます。

D. ACLをインターフェイスに適用する際に、番号の入力ミスなどで条件が何も記載されていないACLを適用してしまうと、暗黙のdenyによってすべてがブロックされます。そのため、想定よりも多くの通信がブロックされると考えられます。

よって、**B**が正解となります。

A97. B

WPA3は、WPA2で脆弱性が発見されたことにより、その対策を施して策定された最新のセキュリティ規格となります。WPA3ではSAE（Simultaneous Authentication of Equals）と呼ばれる高強度の認証機能が実装されています。

A. WPA2で採用されている暗号化方式です。

C. WPAで採用されている暗号化方式です。

D. WEPなどで採用されている暗号化アルゴリズムです。

よって、**B**が正解となります。

A98. B, D

3階層ネットワーク設計モデルはアクセス層・ディストリビューション層・コア層の3つの層で構成されています。それぞれの特徴は次の通りです。

アクセス層

ユーザが使用するPCなどの機器がネットワークに接続する層で、ポート密度の高いレイヤ2スイッチやスイッチングハブを使用する。

ディストリビューション層

アクセス層の各ネットワークを集約する層で、アクセス層の各スイッチに接続しているネットワークを相互接続する役割を持つ。ルータやレイヤ3スイッチなどを使

用し、ルーティングやACLなどによるパケットのフィルタリングを行う。

コア層

ディストリビューション層の機器が集約される層で、ネットワークの中心となる基幹部分（バックボーン）を構成する。より高速な通信が可能で高機能なハイエンドモデルのスイッチなどが配置される。

よって、**B, D**が正解となります。

A99. ①B, C, D　②A, E, F

TCP、UDPでよく利用されるプロトコルを押さえておきましょう。

表　TCPでよく利用するポート番号

ポート番号	サービス名	プロトコル	説明
20	ftp-data	FTP	FTPのデータ転送用
21	ftp	FTP	FTPのデータ制御用
22	ssh	SSH	セキュアなリモート接続を行う
23	telnet	TELNET	平文※1ベースのリモート接続を行う
25	smtp	SMTP	メールを送信する
80	http	HTTP	HTML文書などを公開する
443	https	HTTPS	HTML文書などをセキュアな通信で公開する

※1　平文とは、暗号化されていない情報（データ）を指します。

表　UDPでよく利用するポート番号

ポート番号	サービス名	プロトコル	説明
67	bootps	DHCP	DHCPサーバの送信用
68	bootpc	DHCP	DHCPクライアントの送信用
69	tftp	TFTP	認証を伴わないファイル転送を行う
123	ntp	NTP	時刻同期プロトコル
161,162	snmp	SNMP	各機器を一元管理する

A100. B, C, F

ワイヤレスLANコントローラのGUI設定で、Securityタブはさらに「Layer 2」、「Layer 3」、「AAA Servers」のタブに細分化されています。Layer 2タブでは、使用するワイヤレスLANのセキュリティ規格の設定を行うことができます。WPAやWPA2といったセキュリティ規格の選択や、認証方式（PSK認証やIEEE 802.1X認証など）の設定が可能です。

A. [Security]＞[Layer 3]タブで設定できる項目です。

D. [QoS]タブで設定できる項目です。

E. [WLANs]＞[General]タブで設定できる項目です。

よって、**B, C, F**が正解となります。

A101. B

STPの保護機能の代表的なものに、BPDUガードとルートガードがあります。これら2つの機能について押さえておきましょう。

BPDUガード

BPDUを受け取るべきでないポート（Portfastが設定されているようなポート）が、BPDUを受け取ることによるトラブルを防ぐ機能。BPDUガードが有効になっているポートは、BPDUを受け取ると、エラーディセーブル状態にして強制シャットダウンすることで既存のネットワークを保護する。BPDUガードはデフォルトで無効となっている。

ルートガード

既存の環境よりもブリッジプライオリティの小さいスイッチが勝手に接続された際に、既存のSTPトポロジが変更されてしまうのを防ぐ機能。ルートガードを設定しているポートにルートブリッジよりも上位のBPDUが送信されてくると、ポートをルート不整合という状態にして通信をブロックする。エラーディセーブル状態とは異なり、一度ルート不整合となっても上位のBPDUが送られてこなくなると解除され、通常通りの状態遷移を行う。ルートガードもデフォルトで無効となっている。

よって、**B**が正解となります。

A102. B

SDNを実装したネットワークでは、SDNコントローラにコントロールプレーンの機能が集約され、各機器ではデータプレーンのみが動作します。また、SDNコントローラにより各機器を集中管理・集中制御するため、ネットワークの管理効率も従来のネットワーク構成よりも向上します。

A, C. 従来のネットワーク構成の特徴ですので誤りです。

D. SDNコントローラに集約されるのはコントロールプレーンですので誤りです。

よって、**B**が正解となります。