

問題 2

MIB	SNMP 経由で状態を問い合わせることができる、一意に識別可能なオブジェクトのコレクション
管理対象デバイス	SNMPによるネットワークノード制御
NMS	監視アプリケーションを実行し、ネットワークノードを制御するシステム
エージェント	デバイスとネットワークのデータをキャプチャして変換するSNMPコンポーネント

問題 8

ポリシング	パケットの最大レートを超えるたびに、パケットに特定のアクションを適用します。
マーキング	ToS値を設定してパケットをQoSグループに関連付ける
キューイング	利用可能な帯域幅が許す限りパケットを保持し、それらを分配することでトラフィックの混雑を軽減します
分類	特定の基準を使用してトラフィックをカテゴリに分類する全体的なプロセス

問題 10

エンドポイントはドメイン名の IP アドレスの要求を送信します。	ステップ1
DNS はルート DNS サーバーに要求を送信します。	ステップ2
DNS はドメイン DNS サーバーに要求を送信します。	ステップ3
DNS はドメイン DNS サーバーから応答を受信します。	ステップ4
DNS はエンドポイントに応答します。	ステップ5

問題 12

<code>ip host switch_1 192.168.0.1</code>	ホストテーブルにエントリを追加します
<code>ip domain-name</code>	DNSサーバーのFQDNを完了する
<code>show hosts</code>	アドレスマッピング情報を表示します
<code>ip domain-lookup</code>	ホストからIPアドレスへの変換を可能にする
<code>ip name-server</code>	DNSサーバーのIPアドレスを指定します

#### 問題 15

<code>ip domain lookup source-interface</code>	個々のインターフェースでDNSルックアップを有効にする
<code>ip dns server</code>	デバイス上のDNSサーバーを有効にする
<code>ip name-server</code>	検索サービスを提供するDNSサーバーを識別します
<code>ip domain list</code>	一連のドメイン名を指定します
<code>ip domain name</code>	修飾されていないホスト名に追加するデフォルトのドメインを指定します
<code>ip host</code>	IPアドレスをホスト名に静的にマッピングする

#### 問題 22

デフォルト以外のVLANを使用してネイティブVLANを構成する	802.1q 二重タグ付け VLAN ホッピング攻撃
DHCPスヌーピング機能を設定する	MACフラッド攻撃
802.1x認証プロトコルを構成する	中間者スプーフィング攻撃
ダイナミック トランキン グ プロトコルを無効にする	スイッチスプーフィングVLANホッピング攻撃

#### 問題 27

FTP サーバーなどのネットワークへのアクセスを許可します。	認証
ユーザーが実行できる CLI コマンドを制限します。	TACACS+ 経由でユーザー検証を実行します。
TACACS+ 経由でユーザー検証を実行します。	「あなたが誰であるか」を確認します。
各接続の継続時間を記録します。	認可
ユーザー アクセス レポートをサポートします。	FTP サーバーなどのネットワークへのアクセスを許可します。
「あなたが誰であるか」を確認します。	ユーザーが実行できる CLI コマンドを制限します。

問題 41

ユーザーごとに属性を割り当てます。	認証
ユーザーが実行できる CLI コマンドに到達します。	ログイン試行を許可し、導出します。
ログイン試行を許可し、導出します。	ローカル、PPP、RADIUS、TACACS+ オプションをサポートします。
ユーザーが消費したネットワーク リソースの量を記録します。	認可
ローカル、PPP、RADIUS、TACACS+ オプションをサポートします。	ユーザーごとに属性を割り当てます。
ユーザーが使用しているサービスを追跡します。	ユーザーが実行できる CLI コマンドに到達します。

問題 44

FTP サーバーなどのネットワーク資産へのアクセスを許可します。	Accounting
ユーザーが利用できるサービスを制限します。	各接続の継続時間を記録します。
TACACS+ 経由でユーザー検証を実行します。	ユーザー アクセス レポートをサポートします。
各接続の継続時間を記録します。	認可
ユーザー アクセス レポートをサポートします。	ユーザーが利用できるサービスを制限します。
「あなたが誰であるか」を確認します。	FTP サーバーなどのネットワーク資産へのアクセスを許可します。

問題 53

自動化をサポート	自動化をサポート
SDNコントローラとアプリケーションプレーン間の通信	SDNコントローラとアプリケーションプレーン間の通信
SDNコントローラとデータプレーン間の通信	システム間のデータ共有をサポート
システム間のデータ共有をサポート	RESTベースの要件をサポート
ネットワーク仮想化プロトコルをサポートします	
RESTベースの要件をサポート	
OpenFlowを使用してデータプレーンとコントロールプレーン間のインターフェースを構築します	

問題 60

Cisco Prime インフラストラクチャを活用する	従来のキャンバスデバイス管理
企業顧客の作業負担を軽減します	Cisco Prime インフラストラクチャを活用する
複雑なプロトコルを手動で設定する必要がある	SDA のサポートが不足している
SDA のサポートが不足している	複雑なプロトコルを手動で設定する必要がある
セキュリティ上の脅威を検出するアルゴリズムを使用する	Cisco DNA センター
ノースバウンド API を使用する	セキュリティ上の脅威を検出するアルゴリズムを使用する
	ノースバウンド API を使用する
	企業顧客の作業負担を軽減します

#### 問題 70

デフォルトではSSH経由でモジュールを実行します	デフォルトではSSH経由でモジュールを実行します
YAML言語を使用します	YAML言語を使用します
エージェントを使用してホストを管理する	設定をクライアントにプッシュする
設定をクライアントにプッシュする	エージェントなしで動作する
クライアントがサーバーから構成を取得する必要がある	
エージェントなしで動作する	

#### 問題 73

オーバーレイとアンダーレイの構成
ルーテッドアクセスの展開
STP展開
VLAN と HSRP の設定
VXLAN と LISP の設定
コンソール経由の設定

Cisco DNA センター
オーバーレイとアンダーレイの構成
ルーテッドアクセスの展開
VXLAN と LISP の設定
従来型
STP展開
VLAN と HSRP の設定
コンソール経由の設定

#### 問題 76

複数のツールとアプリケーションを使用して、さまざまな種類のデータを分析およびトラブルシューティングします。
デバイスごとにデバイス構成を管理します。
ネットワーク セキュリティと分析のための単一のインターフェイスを提供します。
セキュリティは、ファイアウォール、VPN、IPS を使用してネットワークの境界付近で管理されます。
複数のデバイスに一貫した構成を適用するための CLI テンプレートをサポートしています。
NetFlow を使用して潜在的なセキュリティ脅威を分析し、そのトラフィックに対して適切なアクションを実行します。

Cisco DNA Center デバイス管理
ネットワーク セキュリティと分析のための単一のインターフェイスを提供します。
複数のデバイスに一貫した構成を適用するための CLI テンプレートをサポートしています。
複数のツールとアプリケーションを使用して、さまざまな種類のデータを分析およびトラブルシューティングします。
従来のデバイス管理
デバイスごとにデバイス構成を管理します。
セキュリティは、ファイアウォール、VPN、IPS を使用してネットワークの境界付近で管理されます。
複数のツールとアプリケーションを使用して、さまざまな種類のデータを分析およびトラブルシューティングします。

#### 問題 80

エージェント	エージェント
エージェントレス	プッシュ
プロビジョン	プロビジョン
フル	エージェントレス
プッシュ	ポスト
ポスト	

問題 93

```
SW1(config)#interface range eth0/0-1
SW1(config-if-range)# channel-group 44 mode active
SW1(config-if-range)# interface port44
SW1(config-if)# switchport trunk encapsulation dot1q
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk naïve vlan 746
SW1(config-if)# no shut
SW1(config-if)# end
```

```
SW2(config)#interface range eth0/0-1
SW2(config-if-range)# channel-group 44 mode active
SW2(config-if-range)# interface port44
SW2(config-if)# switchport trunk encapsulation dot1q
SW2(config-if)# switchport mode trunk
SW2(config-if)# switchport trunk naïve vlan 746
SW2(config-if)# no shut
SW2(config-if)# end
```

This assumes that VLAN 746 is the MONITORING VLAN.

問題 95

### R3

```
config terminal
ip route 192.168.1.1 255.255.255.255 209.165.200.229
end
copy running start
```

### R2

```
config terminal
ip route 0.0.0.0 0.0.0.0 209.165.202.130
ipv6 route ::/0 2001:db8:abcd::2
end
copy running start
```

### 問題 104

NAT:

```
R2(config)# ip access list standard PUBNET
R2(config-std-nacl)# permit 10.2.3.3
R2(config-std-nacl)# permit 10.1.3.11
R2(config-std-nacl)# permit 192.168.3.1
R2(config-std-nacl)# exit
R2(config)# interface e0/1
R2(config-if)# ip nat inside
R2(config)# interface e0/0
R2(config-if)# ip nat outside
R2(config)# ip nat inside source list PUBNET interface e0/0 overload
```

NTP:

```
R1# clock set 00:00:00 jan 1 2019
R1(config)# ntp master 1
R2(config)# ntp server 10.1.3.1
```

DHCP:

```
R1(config)# ip dhcp pool NETPOOL
R1(dhcp-config)# network 10.1.3.0 255.255.255.0
R1(config)# exit
R1(config)# ip dhcp excluded-address 10.1. 3.1 10.1.3.10
```



```
R3(config)# interface e0/2
R3(config-if)# ip address dhcp
```

SSH:

```
R3(config)# username netadmin password N3t4ccess
R3(config)# line vty 0 4
R3(config-line)# login local
R3(config-line)# exit
R3(config)# ip domain-name cisco.com
R3(config)# crypto key generate rsa
```

## 問題 106

### Task 1

```
SW1(config)#vlan 12
SW1(config-vlan)#name Compute
SW1(config-vlan)#vlan 34
SW1(config-vlan)#name Telephony
```

```
SW2(config)#vlan 12
SW1(config-vlan)#name Compute
```

### Task 2

まず、「show vlan Brief」または「show vlan」を使用して利用可能な VLAN を確認し、「Available」の VLAN ID を取得します。この値の代わりに「available-vlan-id」を使用します。

```
SW2(config)#interface e0/1
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan available-vlan-id
```

### Task 3

```
SW1(config)#interface e0/0
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 12
```

```
SW2(config)#interface e0/0
```

```
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 12
```

#### Task 4

```
SW1(config)#interface e0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport voice vlan 34
SW1(config-if)#switchport access vlan 12
```

#### Task 5

```
SW2(config)#cdp run
SW2(config)#interface e0/1
SW2(config-if)#no cdp enable
```

#### 問題 110

```
R1
config terminal
ipv6 unicast-routing
inter eth0/1
ip addre 192.168.180.1 255.255.255.240
ipv6 addre 2001:db8:acca::1/64
no shut
end
copy running start
```

```
R2
config terminal
ipv6 unicast-routing
inter eth0/1
ip address 192.168.180.14 255.255.255.240
ipv6 address 2001:db8:acca::2/64
no shut
end
copy running start
```

#### 問題 111

Sw1

```
enable
config t
Vlan 303
Name FINANCE
Inter e0/1
Switchport access vlan 303
Wr mem
```

Sw2

```
Enable
config t
Vlan 202
Name MARKETING
Int e0/1
Switchport access vlan 202
Wr mem
```

Sw3

```
Enable
config t
Vlan 202
Name MARKETING
Vlan 303
Name FINANCE
Int e0/0
Switchport access vlan 202
Int e0/1
Switchport access vlan 303
Sw1
Int e0/1
Switchport allowed vlan 303
Sw2
Int e0/2
Switchport trunk allowed vlan 303
Sw3
Int e0/3
Switchport trunk allowed vlan 303
Switchport trunk allowed vlan 202, 303
```

Sw101

Config t

Username support password max2learn privilege 15

Line vty 0 4

Login local

Transport input telnet

Access-class 10

Access-list ENT-ACL permit icmp host 192.168.200.10 host 182.168.100.10

Access-list ENT-ACL deny icmp any any

Access-list ENT-ACL permit ip any any

Access-list 10 permit 192.168.200.10

Interface vlan 200

ip access-group ENT-ACL in

interface ethernet 0/0

switchport port-security

switchport port-security maximum 4

switchport port-security violation protect

switchport port-security mac-address sticky

wr mem

問題 113

Gw1:

Config t

Username wheel secret lock3path privilege 15

Line vty 0 4

Login local

Transport input telnet

Access-list CORP\_ACL permit tcp any any eq bootp

Access-list CORP\_ACL permit tcp any any eq https

Access-list CORP\_ACL deny ip any any log

Interface vlan 10

ip access-group CORP\_ACL in

wr mem

Sw1:

Config t

Interface vlan 10

ip dhcp snooping

ip dhcp snooping information

ip dhcp snooping verify mac-address

p dhcp relay information trusted

wr mem

## 問題 120

### Answer Area

ff00:af60:767d:9258:e688:c478:ec75:12

2000:6794:5699:e122:42e0:4236:085d:1

fe80:b680:8af8:7cc1:6df1:71e1:b8f3:7

fc00:a4d3:af37:cbc6:cdbd:b73d:5561:3

fc00:a4d3:af37:cbc6:cdbd:b73d:5561:3

fe80:b680:8af8:7cc1:6df1:71e1:b8f3:7

2000:6794:5699:e122:42e0:4236:085d:1

ff00:af60:767d:9258:e688:c478:ec75:12

## 問題 124

```

R2:
Conf t
Ip route 192.168.1.0 255.255.255.0 10.10.31.1
Ip route 172.20.20.128 255.255.255.128 e0/2
Ip route 172.20.20.128 255.255.255.128 e0/1

```

```

R1:
conf t
Ip route 0.0.0.0 0.0.0.0 10.10.13.3
Ip route 192.168.0.0 255.255.255.0 e0/1
Ip route 192.168.0.0 255.255.255.0 10.10.12.2 3

```

問題 133

単一の固体導体を含む	同軸
長距離のDWDM光システムに通常使用される	単一の固体導体を含む
重なり合う光パルスの歪みを除去する	電気および磁気干渉の影響を受ける
電気および磁気干渉の影響を受ける	単一モードファイバー
	長距離のDWDM光システムに通常使用される
	重なり合う光パルスの歪みを除去する

問題 138

単一の固体導体が含まれています	同軸
長距離にわたるDWDM光システムによく使用されます。	単一の固体導体が含まれています
単一波長の光を使用する	電子信号の形でデータを送信する
電子信号の形でデータを送信する	単一モードファイバー
	長距離にわたるDWDM光システムによく使用されます。
	単一波長の光を使用する

問題 139

小規模オフィスアプリケーションでよく使用されます
通常は内部データセンター接続に使用されます
長距離では減衰が増加する
シールド付きツイストペアとシールドなしツイストペアで構成されている

同軸
通常は内部データセンター接続に使用されます
長距離では減衰が増加する
マルチモードファイバー
小規模オフィスアプリケーションでよく使用されます
シールド付きツイストペアとシールドなしツイストペアで構成されている

問題 140

整合性をほとんど損なわずに長距離に最適です
簡単に壊れない
単一の固体導体が含まれています
コアを通過する際の光の反射は最小限である

シングルモードファイバー
整合性をほとんど損なわずに長距離に最適です
コアを通過する際の光の反射は最小限である
同軸
簡単に壊れない
単一の固体導体が含まれています

問題 141

光に単一の波長を使用します
長くなるほど歪む
最大100ギガビットのデータを送信しますが、距離が長くなると速度が低下します。
コアを通過する際の光の反射は最小限である

シングルモードファイバー
光に単一の波長を使用します
コアを通過する際の光の反射は最小限である
マルチモードファイバー
長くなるほど歪む
最大100ギガビットのデータを送信しますが、距離が長くなると速度が低下します。

問題 142

### Answer Area

2000:2eb8:3e5f:376c:da66:bf1d:d36a:1

fc00:1664:bc95:3c7a:c300:c468:3969:3

fe80:e6ab:b5f9:c358:ea58:0029:b4db:7

ff00:c279:edd5:99c4:b0de:fc11:4b12:12

### 問題 143

単一波長の光を使用する	シングルモードファイバー
シールド付きツイストペアとシールドなしツイストペアで構成されている	単一波長の光を使用する
導体、ベッド、シースを含む	コア径は9ミクロン
コア径は9ミクロン	同軸
	シールド付きツイストペアとシールドなしツイストペアで構成されている
	導体、ベッド、シースを含む

### 問題 144

### Answer Area

ff00:a648:6ad8:4591:80a2:75db:4b5f:12

2000:fda9:65b0:e8c0:1d84:6369:2daa:1

fe80:9885:e8c7:6f41:ac11:b954:cc04:7

fc00:6fd1:6158:034c:6144:eafe:8da6:3

fc00:6fd1:6158:034c:6144:eafe:8da6:3

fe80:9885:e8c7:6f41:ac11:b954:cc04:7

2000:fda9:65b0:e8c0:1d84:6369:2daa:1

ff00:a648:6ad8:4591:80a2:75db:4b5f:12

### 問題 145



整合性をほとんど失わずに長距離でも最適です
光に単一の波長を使用します
コア径は62.5または50ミクロンです
長距離にわたるDWDM光システムによく使用されます。

シングルモードファイバー
整合性をほとんど失わずに長距離でも最適です
光に単一の波長を使用します
マルチモードファイバー
コア径は62.5または50ミクロンです
長距離にわたるDWDM光システムによく使用されます。

#### 問題 153

##### Answer Area

ff00:0a7c:cf36:cd7c:6dad:44fa:c11c:12	2000:0962:6dee:8c78:93b8:c429:c78d:1
fe80:27bb:1ef9:6b3d:b347:686f:f3b7:7	fc00:9e81:2346:4929:7fec:34e9:7b8c:3
fc00:9e81:2346:4929:7fec:34e9:7b8c:3	fe80:27bb:1ef9:6b3d:b347:686f:f3b7:7
2000:0962:6dee:8c78:93b8:c429:c78d:1	ff00:0a7c:cf36:cd7c:6dad:44fa:c11c:12

#### 問題 154

複数の組織で同時に使用される可能性がある
パケットを単一のアドレスではなくグループアドレスに送信する
1対多の通信を提供する
アドレスの競合なしにサイトを結合できる

ユニークローカル
複数の組織で同時に使用される可能性がある
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
パケットを単一のアドレスではなくグループアドレスに送信する
1対多の通信を提供する

問題 155

複数の組織で同時に使用される可能性がある	ユニークローカル
単一のサブネットに接続されている	複数の組織で同時に使用される可能性がある
すべての IPv6 デバイスで必須	プライベート IPv4 アドレスに相当する
プライベート IPv4 アドレスに相当する	リンクローカルアドレス
	単一のサブネットに接続されている
	すべての IPv6 デバイスで必須

問題 164

DHCPサーバー	スヌーピングバインディングデータベース
スヌーピングバインディングデータベース	DHCPサーバー
スプリアスDHCPサーバー	信頼できる
信頼できる	スプリアスDHCPサーバー
信頼されていない	信頼されていない

問題 166

プライベート IPv4 アドレスに相当する	ユニークローカル
パケットを単一のアドレスではなくグループアドレスに送信する	プライベート IPv4 アドレスに相当する
グループにユニキャストソースが送信されている	アドレスの競合なしにサイトを結合できる
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
	パケットを単一のアドレスではなくグループアドレスに送信する
	グループにユニキャストソースが送信されている

問題 167

光に単一の波長を使用します	マルチモードファイバー
長くなるほど歪む	長くなるほど歪む
通常は内部データセンター接続に使用されます	通常は内部データセンター接続に使用されます
コアを通過する際の光の反射は最小限である	シングルモードファイバー
	光に単一の波長を使用します
	コアを通過する際の光の反射は最小限である

問題 171

Answer Area

2000:87aa:84ab: added9:5ac3:41a5:ef72:1	2000:87aa:84ab: added9:5ac3:41a5:ef72:1
fc00:c51f:922d:0c12:9c54:7644:28f5:3	fe80:ccc7:17f1:5d15:f611:5cea:ef92:7
fe80:ccc7:17f1:5d15:f611:5cea:ef92:7	ff00:520a:3e47:de13:fe6f:476e:5325:12
ff00:520a:3e47:de13:fe6f:476e:5325:12	fc00:c51f:922d:0c12:9c54:7644:28f5:3

問題 177

複数の波長の光を使用する	マルチモードファイバー
コア径は9ミクロン	複数の波長の光を使用する
長距離では減衰が増加する	長距離では減衰が増加する
単一波長の光を使用する	シングルモードファイバー
	コア径は9ミクロン
	単一波長の光を使用する

問題 179

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ます	エニーキャスト
送信元アドレスとして使用することはできません	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ません
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ます	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ます
1対多の通信を提供する	マルチキャスト
	送信元アドレスとして使用することはできません
	1対多の通信を提供する

問題 182

FTP サーバーなどのネットワーク資産へのアクセスを許可します。	アカウントティング
ユーザーが実行できる CLI コマンドを制限します。	各接続の継続時間を記録します。
TACACS+ 経由でユーザー検証を実行します。	ユーザー アクセス レポートをサポートします。
各接続の継続時間を記録します。	認可
ユーザー アクセス レポートをサポートします。	FTP サーバーなどのネットワーク資産へのアクセスを許可します。
「あなたが誰であるか」を確認します。	ユーザーが実行できる CLI コマンドを制限します。

問題 184

fe80:cc72:4b9e:445c:8179:0420:5988:7	2000:1092:a1e8:827d:527c:3ce7:9816:1
2000:1092:a1e8:827d:527c:3ce7:9816:1	fe80:cc72:4b9e:445c:8179:0420:5988:7
ff00:ec6c:dbb1:3e8b:6d46:bd27:a236:12	ff00:ec6c:dbb1:3e8b:6d46:bd27:a236:12
fc00:9860:653f:5146:8cb2:a27c:cb6f:3	fc00:9860:653f:5146:8cb2:a27c:cb6f:3

問題 186

### R1

```
conf terminal
interface Loopback0
ip address 10.10.1.1 255.255.255.255
!
interface Loopback1
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/0
no shut
ip address 10.10.12.1 255.255.255.0
ip ospf 1 area 0
duplex auto
!
interface Ethernet0/1
no shut
ip address 10.10.13.1 255.255.255.0
ip ospf 1 area 0
duplex auto
!
router ospf 1
router-id 10.10.12.1
network 10.10.1.1 0.0.0.0 area 0
network 192.168.1.0 0.0.0.255 area 0
!
copy run star
```

### R2

```
conf terminal
interface Loopback0
ip address 10.10.2.2 255.255.255.255
!
interface Loopback1
ip address 192.168.2.2 255.255.255.0
!
interface Ethernet0/0
no shut
ip address 10.10.12.2 255.255.255.0
ip ospf priority 255
ip ospf 1 area 0
duplex auto
!
interface Ethernet0/2
no shut
ip address 10.10.23.2 255.255.255.0
ip ospf priority 255
ip ospf 1 area 0
duplex auto
!
router ospf 1
network 10.10.2.2 0.0.0.0 area 0
network 192.168.2.0 0.0.0.255 area 0
!
copy runs start
```

---

### R3

```
conf ter
interface Loopback0
ip address 10.10.3.3 255.255.255.255
!
interface Loopback1
ip address 192.168.3.3 255.255.255.0
!
interface Ethernet0/1
no shut
ip address 10.10.13.3 255.255.255.0
ip ospf 1 area 0
duplex auto
!
interface Ethernet0/2
no shut
ip address 10.10.23.3 255.255.255.0
ip ospf 1 area 0
duplex auto
!
router ospf 1
network 10.10.3.3 0.0.0.0 area 0
network 192.168.3.0 0.0.0.255 area 0
!
copy run start
!
```

問題 187

複数のインターフェースに割り当てられている	エニーキャスト
送信元アドレスとして使用することはできません	複数のインターフェースに割り当てられている
非ホストデバイスによってのみ使用される	非ホストデバイスによってのみ使用される
1対多の通信を提供する	マルチキャスト
	送信元アドレスとして使用することはできません
	1対多の通信を提供する

問題 189

導体、ベッド、シースを含む	同軸
整合性をほとんど失わずに長距離でも最適です	導体、ベッド、シースを含む
小規模オフィスアプリケーションでよく使用されます	小規模オフィスアプリケーションでよく使用されます
単一波長の光を使用する	シングルモードファイバー
	整合性をほとんど失わずに長距離でも最適です
	単一波長の光を使用する

問題 196

グループにユニキャストソースが送信されている	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	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	アドレスの競合なしにサイトを結合できる
パケットを単一のアドレスではなくグループアドレスに送信する	マルチキャスト
	グループにユニキャストソースが送信されている
	パケットを単一のアドレスではなくグループアドレスに送信する

問題 199

データベース同期トラフィック	標準Webブラウジングトラフィック
標準Webブラウジングトラフィック	ビデオトラフィック
ビデオトラフィック	VoIPトラフィック
VoIPトラフィック	データベース同期トラフィック

問題 205

導体、ベッド、シースを含む	同軸
長距離にわたるDWDM光システムによく使用されます。	導体、ベッド、シースを含む
小規模オフィスアプリケーションでよく使用されます	小規模オフィスアプリケーションでよく使用されます
重なり合う光パルスによる歪みを排除	シングルモードファイバー
	長距離にわたるDWDM光システムによく使用されます。
	重なり合う光パルスによる歪みを排除



問題 207

DELETE	POST
GET	DELETE
PATCH	PUT
POST	PATCH
PUT	GET

問題 217

簡単にアクセスして安全な情報を入手することができます	同軸
長距離で最大40Gbit/sのデータ伝送が可能	簡単にアクセスして安全な情報を入手することができます
電気的および磁氣的干渉の影響を受ける	電気的および磁氣的干渉の影響を受ける
コアを通過する際の光の反射は最小限である	シングルモードファイバー
	長距離で最大40Gbit/sのデータ伝送が可能
	コアを通過する際の光の反射は最小限である

問題 222

アドレスの競合なしにサイトを結合できる	ユニークローカル
パケットを単一のアドレスではなくグループアドレスに送信する	アドレスの競合なしにサイトを結合できる
インターネット上でルーティングできない	インターネット上でルーティングできない
1対多の通信を提供する	マルチキャスト
	パケットを単一のアドレスではなくグループアドレスに送信する
	1対多の通信を提供する

#### 問題 223

	2000:6166:6ba9:cde4:d89e:4c4a:bdc8:1
	fe80:ae46:d315:41c8:4593:12dc:9827:7
	ff00:a8bb:b2a1:7490:4ef0:f603:109b:12
	fc00:382e:29e1:f7e2:1573:ff4f:04f9:3

#### 問題 227

1.

```
sw-2#conf t
```

```
sw-2(config)#vlan 20
```

```
sw-2(config-vlan)#aname SERVER1
```

```
sw-2(config-vlan)#exit
```

```
sw-2(config)#vlan 30
```

```
sw-2(config-vlan)#name SALES
```

```
sw-2(config-vlan)#exit
```

2.

```
sw-2(config)#interface ETH0/2
```

```
sw-2(config-if)#sw-1port mode access
```

```
sw-2(config-if)#sw-1port access vlan 20
sw-2(config-if)#no sh
sw-2(config-if)#exit
```

3

```
sw-2(config)#interface ETH0/3
sw-2(config-if)#sw-1port mode access
sw-2(config-if)#sw-1port access vlan 30
sw-2(config-if)#no sh
sw-2(config-if)#end
sw-2#wr
```

4.

```
sw-1#configure t
sw-1(config)#cdp run
sw-1(config)#interface fastEthernet 0/1
sw-1(config-if)#cdp enable
sw-1(config-if)#no sh
sw-1(config)#interface fastEthernet 0/2
sw-1(config-if)#no cdp enable
sw-1(config-if)#no sh
sw-1(config-if)#end
sw-1#wr
```

問題 230

R1:

```
Ip route 10.0.41.10 255.255.255.255 10.0.12.2  
Ip route 10.0.41.0 255.255.255.0 10.0.12.2 200  
Ip route 10.0.41.0 255.255.255.0 10.0.13.2
```

R2:

```
Ip route 0.0.0.0 0.0.0.0. 209.165.200.225
```

#### 問題 234

16 進数に変換し直し必要に応じて短縮すると、2 番目のサブネットのアドレスが得られます。

2001:DB8:0:4::/54 設定 まず、L3 スイッチを扱っていることに注意してください。

質問には、必要な構成がすべて適用されていると書かれていますが、実行中の構成をチェックして、これが実際に当てはまるかどうかを確認する必要があります。

1. IP ルーティングが有効であることを確認する
2. ipv6 が有効であることを確認する
3. スイッチポートが無効であることを確認する
4. ルーティング インターフェイスがシャットダウンされていないことを確認する

この例では、これらの構成が次のとおりであると仮定します。 \*適用されません\*。

まず、Sw101 を設定します Sw101:

```
SW101(config)#ip routing  
SW101(config)#ipv6 unicast-routing  
SW101(config)#interface e0/0  
SW101(config-if)#no switchport  
SW101(config-if)#ip address 172.16.16.1 255.255.240.0  
SW101(config-if)#ipv6 address 2001:DB8:0:4::/54 eui-64  
SW101(config-if)#no shutdown  
SW101(config-if)#do write memory
```

次に、SW102 を設定します:

```
SW102(config)#ip routing
SW102(config)#ipv6 unicast-routing
SW102(config)#interface e0/0
SW102(config-if)#no switchport
SW102(config-if)#ip address 172.16.31.254 255.255.240.0
SW102(config-if)#ipv6 address 2001:DB8:0:4::/54 eui-64
SW102(config-if)#no shutdown
SW102(config-if)#do write memory
```

問題 238

小規模オフィスアプリケーションでよく使用されます	同軸
長距離で最大40Gbit/sのデータ伝送が可能	小規模オフィスアプリケーションでよく使用されます
簡単に壊れない	簡単に壊れない
重なり合う光パルスによる歪みを排除	シングルモードファイバー
	長距離で最大40Gbit/sのデータ伝送が可能
	重なり合う光パルスによる歪みを排除

問題 240

	2000:4011:2a0d:d571:1976:4bab:adb7:1
	fe80:5db2:1f32:0ee4:32a3:855f:b0d5:7
	ff00:b823:1dc6:263b:ba6a:50f5:15b7:12
	fc00:e896:c4cd:422b:7660:59e5:dd00:3

問題 242

複数の組織で同時に使用される可能性がある	ユニークローカル
送信元アドレスとして使用することはできません	複数の組織で同時に使用される可能性がある
アドレスの競合なしにサイトを結合できる	アドレスの競合なしにサイトを結合できる
グループにユニキャストソースが送信されている	マルチキャスト
	送信元アドレスとして使用することはできません
	グループにユニキャストソースが送信されている

問題 268

R1:  
 config t  
 ip route 0.0.0.0 0.0.0.0 10.0.12.2  
 ip route 10.0.41.0 255.255.255.0 10.0.13.2

R2:  
  
 config t  
 ip route 0.0.0.0 0.0.0.0 209.165.200.225  
 ip route 10.0.41.10 255.255.255.255 10.0.24.2

問題 308

送信元アドレスとして使用されることはありません	マルチキャスト
アドレスの競合なしにサイトを結合できる	送信元アドレスとして使用されることはありません
インターネット上でルーティングできません	1対多の通信を提供する
1対多の通信を提供する	ユニークローカル
	アドレスの競合なしにサイトを結合できる
	インターネット上でルーティングできません

問題 310

Task 1. Configure SW-1 with VLAN 15 and label it exactly as OPS

```
SW-1(config)#vlan 15
SW-1(config-vlan)#name OPS
SW-1(config-vlan)#exit //To apply the VLAN configured
```

Task 2. Configure SW-2 with VLAN 66 and label it exactly as ENGINEERING

```
SW-2(config)#vlan 66
SW-2(config-vlan)#name ENGINEERING
SW-2(config-vlan)#exit //To apply the VLAN configured
```

Task 3. Configure the switch port connecting to PC1

```
SW-1(config)#int e0/1
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 15
SW-1(config-if)#no shut
```

Task 4. Configure the switch port connecting to PC2

```
SW-2(config)#int e0/1
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 66
SW-2(config-if)#no shut
```

Task 5. Configure the E0/2 connections on SW-1 and SW-2 for neighbor discovery using the vendor-neutral standard protocol and ensure that e0/0 on both switches uses the Cisco proprietary protocol

“neighbor discovery using the vendor-neutral standard protocol” means LLDP while “Cisco proprietary protocol” means CDP.

On both SW-1 and SW-2

```
SW-1(config)#lldp run
SW-2(config)#lldp run
```

```
SW-1(config)#int e0/0
SW-1(config-if) no lldp transmit
SW-1(config-if) no lldp recieve
SW-1(config-if) cdp enable
```

```
SW-2(config)#int e0/0
SW-2(config-if) no lldp transmit
SW-2(config-if) no lldp recieve
SW-2(config-if) cdp enable
```



Task 1. Configure SW-1 with VLAN 15 and label it exactly as OPS

```
SW-1(config)#vlan 35
SW-1(config-vlan)#name SALES
SW-1(config-vlan)#exit //To apply the VLAN configured
```

Task 2. Configure SW-2 with VLAN 66 and label it exactly as ENGINEERING

```
SW-2(config)#vlan 39
SW-2(config-vlan)#name MARKETING
SW-2(config-vlan)#exit //To apply the VLAN configured
```

Task 3. Configure the switch port connecting to PC1

```
SW-1(config)#int e0/2
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 35
SW-1(config-if)#no shut
```

Task 4. Configure the switch port connecting to PC2

```
SW-2(config)#int e0/2
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 39
SW-2(config-if)#no shut
```

Task 5. Configure SW-1 and SW-2 for universal neighbor discovery using the industry standard protocol and disable it on the interface connecting to PC1

“neighbor discovery using the vendor-neutral standard protocol” means LLDP while “Cisco proprietary protocol” means CDP.

On both SW-1 and SW-2

```
SW-1(config)#lldp run
SW-2(config)#lldp run
```

On SW-1

```
SW-1(config)#int e0/2
SW-1(config-if) no lldp transmit
SW-1(config-if) no lldp receive
```

プライベート IPv4 アドレスの対応	ユニークローカル
IPv4アドレスと同様にパブリックにルーティング可能	プライベート IPv4 アドレスの対応
一対一のコミュニケーションを可能にする	複数の組織で同時に使用される可能性がある
複数の組織で同時に使用される可能性がある	グローバルユニキャストアドレス
	IPv4アドレスと同様にパブリックにルーティング可能
	一対一のコミュニケーションを可能にする

問題 318

SW-1

Interface e0/0

Channel-group 12 mode active

Interface e0/1

Channel-group 12 mode active

Interface port-channel 12

Switchport trunk encapsulation dot1q

Switchport mode trunk

Switchport trunk native vlan 35

Interface e0/2

Switchport trunk native vlan 35

SW-2

Interface e0/0

Channel-group 12 mode passive

Interface e0/1

Channel-group 12 mode passive

Interface port-channel 12

Switchport trunk encapsulation dot1q

Switchport mode trunk

Switchport trunk native vlan 35

Interface e0/2

Switchport trunk native vlan 35

SW-3

Interface e0/0

Switchport trunk native vlan 35

Interface e0/1

Switchport trunk native vlan 35

簡単にアクセスして安全な情報を入手することができます
光のパルスを使って信号を送信する
電子信号の形でデータを送信する
コア、クラッド、コーティングを含む

同軸
簡単にアクセスして安全な情報を入手することができます
電子信号の形でデータを送信する
マルチモードファイバー
光のパルスを使って信号を送信する
コア、クラッド、コーティングを含む

問題 323

簡単にアクセスして安全な情報を入手することができます
長距離では減衰が増加する
シールド付きツイストペアとシールドなしツイストペアで構成されている
取り扱うと損傷しやすい

同軸
簡単にアクセスして安全な情報を入手することができます
シールド付きツイストペアとシールドなしツイストペアで構成されている
マルチモードファイバー
長距離では減衰が増加する
取り扱うと損傷しやすい

問題 324

IPv4アドレスと同様にパブリックにルーティング可能	グローバルユニキャストアドレス
パケットを単一のアドレスではなくグループアドレスに送信する	IPv4アドレスと同様にパブリックにルーティング可能
送信元アドレスとして使用されることはありません	インターネット経由でルーティングおよびアクセス可能
インターネット経由でルーティングおよびアクセス可能	マルチキャスト
	パケットを単一のアドレスではなくグループアドレスに送信する
	送信元アドレスとして使用されることはありません

問題 327

一元的な管理とセキュリティを提供します	アクセスポイント
イーサネットフレームをフォーマットし、宛先に転送する	オンプレミスまたはクラウドベースで使用
LWAPモード時に転送を決定する	IEEE 802.11とイーサネット規格の両方をサポート
オンプレミスまたはクラウドベースで使用	無線LANコントローラー
IEEE 802.11とイーサネット規格の両方をサポート	LWAPモード時に転送を決定する
	一元的な管理とセキュリティを提供します

問題 329

PoE実装用の導管を供給	同軸
長距離にわたるDWDM光システムに使用される	PoE実装用の導管を供給
簡単にアクセスして安全な情報を入手できる	簡単にアクセスして安全な情報を入手できる
コア径は9ミクロン	シングルモードファイバー
	長距離にわたるDWDM光システムに使用される
	コア径は9ミクロン

問題 334

2000:e2a1:a1ee:03ed:39a0:4f8e:9f02:1
fe80:efae:0b2a:56fe:4a87:147f:dc21:7
fc00:733d:b542:a948:d7fa:eeea:989a:3
ff00:3b64:fbca:171a:6140:6a35:1ea6:12

問題 336

電気的および磁氣的干渉の影響を受ける	同軸
移動中にクラッドとコアの間の屈折が増加する	電気的および磁氣的干渉の影響を受ける
簡単にアクセスして安全な情報を入手できる	簡単にアクセスして安全な情報を入手できる
光のパルスを使って信号を送信する	マルチモードファイバー
	移動中にクラッドとコアの間の屈折が増加する
	光のパルスを使って信号を送信する

問題 337

## SW-2

Config t

Interface e0/0

switchport mode trunk

switchport trunk encapsulation dot1q

switchport access vlan 10

switchport trunk native vlan 11

Interface e0/2

switchport mode trunk

switchport trunk encapsulation dot1q

channel-group 23 mode passive

Interface e0/3

switchport mode trunk

switchport trunk encapsulation dot1q

channel-group 23 mode passive

interface port-channel 23

switchport mode trunk

switchport trunk encapsulation dot1q

## SW-3

Config t

Interface e0/0

switchport mode trunk

switchport trunk encapsulation dot1q

switchport access vlan 10

switchport trunk native vlan 11

Interface e0/2

switchport mode trunk

switchport trunk encapsulation dot1q

channel-group 23 mode active

Interface e0/3

switchport mode trunk

switchport trunk encapsulation dot1q

channel-group 23 mode active

interface port-channel 23

switchport mode trunk

switchport trunk encapsulation dot1q



問題 341

IGPのネクストホップアドレスとして機能する	リンクローカルアドレス
グループにユニキャストソースが送信されている	IGPのネクストホップアドレスとして機能する
送信元アドレスとして使用されることはありません	単一のリンクに限定
単一のリンクに限定	マルチキャスト
	グループにユニキャストソースが送信されている
	送信元アドレスとして使用されることはありません

問題 344

	207.165.200.244/30
	192.168.2.0/24
	192.168.1.0/24
	172.16.2.0/24
207.165.200.248/30	

問題 347

```
SW101:
Sw101>en
Sw101#conf t
Sw101(config)#int g1/0/1
Sw101(config-if)#no switchport
Sw101(config-if)#ip add 172.16.16.1 255.255.240.0
Sw101(config-if)#ipv6 address 2001:db8:0:400::/54 eui-64
Sw101(config-if)#no shutdown
Sw101(config-if)#end
Sw101#wr
```

```
SW102:
Sw102>en
Sw102#conf t
Sw102(config)#int g1/0/1
Sw102(config-if)#no switchport
Sw102(config-if)#ip add 172.16.31.254 255.255.240.0
Sw102(config-if)#ipv6 address 2001:db8:0:400::/54 eui-64
Sw102(config-if)#no shutdown
Sw102(config-if)#end
Sw102#wr
```

2001:db8::/50 main prefix to get 16 subnets i need 4 bits binary  
2001:db8:000:00 0000 000000000000::/54 → First subnet  
2001:db8:000:00 0001 000000000000::/54 → second 2001:db8:0:400::/54  
2001:db8:000:00 0010 000000000000::/54 → third subnet  
2001:db8:000:00 0011 000000000000::/54 → fourth subnet

光のパルスを使って信号を送信する	同軸
信号がコアを通過する際に光の反射が最小限に抑えられる	導体、ベッド、シースを含む
導体、ベッド、シースを含む	シールド付きまたはシールドなしのツイストペアで構成されている
シールド付きまたはシールドなしのツイストペアで構成されている	シングルモードファイバー
	光のパルスを使って信号を送信する
	信号がコアを通過する際に光の反射が最小限に抑えられる

問題 353

パケットを単一のアドレスではなくグループアドレスに送信する	マルチキャスト
単一のリンクに限定	パケットを単一のアドレスではなくグループアドレスに送信する
1対多の通信を提供する	1対多の通信を提供する
IGPのネクストホップアドレスとして機能する	リンクローカルアドレス
	単一のリンクに限定
	IGPのネクストホップアドレスとして機能する

問題 361

シールド付きツイストペアとシールドなしツイストペアで構成されている	同軸
断熱ガラス繊維で構成されている	シールド付きツイストペアとシールドなしツイストペアで構成されている
電気的および磁氣的干渉の影響を受ける	電気的および磁氣的干渉の影響を受ける
単一波長の光を使用する	シングルモードファイバー
	断熱ガラス繊維で構成されている
	単一波長の光を使用する

問題 362

```

SW-1:
SW-1>en
SW-1# Config t
SW-1(config)# int e0/0
SW-1(config-if) # switchport trunk allowed vlan 5,6
SW-1(config)# int e0/1
SW-1(config-if) # switchport trunk allowed vlan 77
SW-1(config-if) # end
SW-1# wr mem

SW-2:
SW-2>en
SW-2# Config t
SW-2(config)# interface range eth0/0-1
SW-2(config-if) # channel-group 44 mode active
SW-2(config)# int e0/1
SW-2(config-if) # switchport trunk allowed vlan 77
SW-2(config-if) # end
SW-2# wr mem

SW-3>en
SW-3# Config t
SW-3(config)# interface range eth0/0-1
SW-3(config-if) # channel-group 34 mode active
SW-3(config)# interface port34
SW-3(config-if) # switchport trunk encapsulation dot1q
SW-3(config-if) # end
SW-3# wr mem

SW-4>en
SW-4# Config t
SW-4(config)# interface range eth0/0-1
SW-4(config-if) # channel-group 34 mode passive
SW-4(config)# interface port34
SW-4(config-if) # switchport trunk encapsulation dot1q
SW-4(config-if) # end
SW-4# wr mem

```

導体、ベッド、シースを含む
コア、クラッド、コーティングを含む
電気的および磁氣的干渉の影響を受ける
断熱ガラス繊維で構成されている

同軸
導体、ベッド、シースを含む
電気的および磁氣的干渉の影響を受ける
シングルモードファイバー
コア、クラッド、コーティングを含む
断熱ガラス繊維で構成されている

問題 377

プライベート IPv4 アドレスの対応
送信元アドレスとして使用されることはありません
1対多の通信を提供する
複数の組織で同時に使用される可能性がある

ユニークローカル
プライベート IPv4 アドレスの対応
複数の組織で同時に使用される可能性がある
マルチキャスト
送信元アドレスとして使用されることはありません
1対多の通信を提供する

問題 379

テンプレートを使用してQoS設定を実装する	アクセスポイント
Wi-Fi信号を強化する機能	Wi-Fi信号を強化する機能
PoE用の特別なアダプタが必要	ワークグループブリッジとして構成可能
デバイスグループ内のユーザー接続データを提供する	無線LANコントローラー
ワークグループブリッジとして構成可能	テンプレートを使用してQoS設定を実装する
	デバイスグループ内のユーザー接続データを提供する

問題 381

電気的および磁氣的干渉の影響を受ける	同軸
整合性をほとんど失わずに長距離でも最適です	電気的および磁氣的干渉の影響を受ける
シールド付きツイストペアとシールドなしツイストペアで構成されている	シールド付きツイストペアとシールドなしツイストペアで構成されている
光のパルスを使って信号を送信する	シングルモードファイバー
	整合性をほとんど失わずに長距離でも最適です
	光のパルスを使って信号を送信する

問題 386

```

SW103:
SW103>en
SW103#config t
SW103(config)# username devnet privilege 15 algorithm-type sha256 secret access8cli
SW103(config)# line vty 0 4
SW103(config-line)#login local
SW103(config-line)#transport input telnet
SW103(config-line)#end
SW103# wr

```

```

R1:
R1>en
R1#config t
R1(config)# ip access-list extended INTERNET_ACL
R1(config-ext-nacl)#permit tcp 172.16.0.0 0.0.255.255 any eq 443
R1(config-ext-nacl)#permit tcp 172.16.101.0 0.0.0.255 any eq telnet
R1(config-ext-nacl)#deny ip any any log
R1(config-ext-nacl)#end
R1#wr

```

```

SW101:
Sw101>en
Sw101#config t
Sw101(config)#ip dhcp snooping vlan 101
Sw101(config)#no ip dhcp snooping information option
Sw101(config)#ip dhcp snooping verify mac-address
Sw101(config)#end
Sw101#wr

```

#### 問題 388

IPv4アドレスと同様にパブリックにルーティング可能	グローバルユニキャストアドレス
1対多の通信を提供する	IPv4アドレスと同様にパブリックにルーティング可能
グループにユニキャストソースが送信されている	インターネット経由でルーティングおよびアクセス可能
インターネット経由でルーティングおよびアクセス可能	マルチキャスト
	1対多の通信を提供する
	グループにユニキャストソースが送信されている



## 問題 389

- To subnet 10.30.64.0/19 to meet the subnet requirements and maximize the number of hosts, you need to determine how many bits you need to borrow from the host portion of the address to create enough subnets for 64 sites. Since 64 is  $2^6$ , you need to borrow 6 bits, which means your new subnet mask will be /20 or 255.255.240.0. To find the second subnet, you need to add the value of the fifth bit (64) to the third octet of the network address (0), which gives you 10.30.64.0/20 as the second subnet. The first usable IP address in this subnet is 10.30.64.1, and the last usable IP address is 10.30.64.254.

- To assign the first usable IP address to e0/0 on Sw101, you need to enter the following commands on the device console:

```
Sw101#configure terminal
Sw101(config)#interface e0/0
Sw101(config-if)#ip address 10.30.64.1 255.255.240.0
Sw101(config-if)#no shutdown
Sw101(config-if)#end
```

- To assign the last usable IP address to e0/0 on Sw102, you need to enter the following commands on the device console:

```
Sw102#configure terminal
Sw102(config)#interface e0/0
Sw102(config-if)#ip address 10.30.64.254 255.255.240.0
Sw102(config-if)#no shutdown
Sw102(config-if)#end
```

- To subnet an IPv6 GUA to meet the subnet requirements and maximize the number of hosts, you need to determine how many bits you need to borrow from the interface identifier portion of the address to create enough subnets for 64 sites. Since 64 is  $2^6$ , you need to borrow 5 bits, which means your new prefix length will be /68 or ffff:ffff:ffff:ffff::/68 (assuming that your IPv6 GUA has a /64 prefix by default). To find the second subnet, you need to add the value of the fifth bit (64) to the fourth hextet of the network address (0000), which gives you xxxx:xxxx:xxxx:0020::/68 as the second subnet (where xxxx:xxxx:xxxx is your IPv6 GUA prefix). The first and last IPv6 addresses in this subnet are xxxx:xxxx:xxxx:0020::1 and xxxx:xxxx:xxxx:0027:ffff:ffff:ffff:ffff respectively.

- To assign an IPv6 GUA using a unique 64-bit interface identifier on e0/0 on Sw101, you need to enter the following commands on the device console (assuming that your IPv6 GUA prefix is 2001:db8::/64):

```
Sw101#configure terminal
Sw101(config)#interface e0/0
Sw101(config-if)#ipv6 address 2001:db8::20::1/68
Sw101(config-if)#no shutdown Sw101(config-if)#end
```

- To assign an IPv6 GUA using a unique 64-bit interface identifier on e0/0 on Sw102, you need to enter the following commands on the device console (assuming that your IPv6 GUA prefix is 2001:db8::/64):

```
Sw102#configure terminal
Sw102(config)#interface e0/0
Sw102(config-if)#ipv6 address 2001:db8::27::ffe/68
Sw102(config-if)#no shutdown Sw102(config-if)#end
```

## 問題 390

```
R1# config t
R1(config)# ipv6 route 2001:db8:41::/64 2001:db8:12::2
R1(config)# ipv6 route 2001:db8:41::/64 2001:db8:13::3 2
R1(config)#end
R1#wr
```

```
R2:
R2> en
R2# config t
R2(config)# ipv6 route 2001:db8:41::/64 2001:db8:24::4
R2(config)#end
R2#wr
```

```
R3:
R3> en
R3# config t
R3(config)# ipv6 route 2001:db8:41::/64 2001:db8:34::4
R3(config)#end
R3#wr
```

```
R4:
R4>en
R4# config t
R4(config)# ipv6 route 2001:db8:12::/64 2001:db8:24::2
R4(config)# ipv6 route 2001:db8:13::/64 2001:db8:34::3
R4(config)#end
4#wr
```

```
SW-1:
SW-1>en
SW-1# Config t
SW-1(config)# vlan 10
SW-1(config-vlan)# name Engineering
SW-1(config-vlan)#int f0/10
SW-1(config-if)#lldp transmit
SW-1(config-if)#lldp receive
SW-1(config-if)#int f0/1
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 10
SW-1(config-if)#switchport voice vlan 11
SW-1(config-if)#int f0/2
SW-1(config-if)#no cdp enable
SW-1(config-if)#end
SW-1#wr
```

```
SW-2:
SW-2>en
SW-2# Config t
SW-2(config)#int f0/10
SW-2(config-if)#lldp transmit
SW-2(config-if)#lldp receive
SW-2(config-if)#int f0/1
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 30
SW-2(config-if)#end
SW-2#wr
```

Task 1. Configure Sw1 and Sw2 with both VLANs, naming them according to the VLAN Name provided in the topology

```
SW-1(config)#vlan 77
SW-1(config-vlan)#name User_VLAN
SW-1(config-vlan)#exit
SW-1(config)#vlan 177
SW-1(config-vlan)#name Voice_VLAN
SW-1(config-vlan)#exit
```

```
SW-2(config)#vlan 77
SW-2(config-vlan)#name User_VLAN
SW-2(config-vlan)#exit
SW-2(config)#vlan 177
SW-2(config-vlan)#name Voice_VLAN
SW-2(config-vlan)#exit
```

Task 2. Configure the E0/1, E0/2, and E0/3 ports on both switches for both VLANs and ensure that Cisco IP phones and PCs pass traffic.

```
SW-1(config)#interface range E0/1-3
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 77
SW-1(config-if)#switchport voice vlan 177
```

```
SW-2(config)#interface range E0/1-3
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 77
SW-2(config-if)#switchport voice vlan 177
```

Task 3. Configure Sw1 and Sw2 to allow neighbor discovery via the vendor-neutral protocol on e0/0.

```
SW-1(config)#lldp run
SW-2(config)#lldp run
```

Step 1:

SW-1:

```
interface e0/0
  switchport mode trunk
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,12,22
interface e0/1
  switchport mode trunk
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,12,22
```

SW-2:

```
interface e0/0
  switchport mode trunk
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,12,22
interface e0/1
  switchport mode trunk
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,12,22
```

Step 2:

SW-1:

```
interface e0/2
  switchport mode trunk
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 12,22
```

Step 3:

SW-1:

```
interface range e0/0 - e0/1
  channel-group 1 mode active
```

SW-2:

```
interface range e0/0 - e0/1
  channel-group 1 mode active
```

問題 403

Task 1:

```
SW101(config)# username netops password ipsec4all
SW101(config)# service password-encryption
SW101(config)# line vty 0 4
SW101(config-line)# login local
SW101(config-line)# transport input telnet
SW101(config-line)# exit
SW101(config)# end
SW101# write memory
```

Task 2:

```
SW103(config)# ip access-list extended ENT_ACL
SW103(config-ext-acl)# permit icmp host 172.16.10.10 host 172.16.20.10
SW103(config-ext-acl)# deny icmp any any
SW103(config-ext-acl)# permit tcp host 172.16.10.10 host 172.16.30.2 eq telnet
SW103(config-ext-acl)# deny tcp any any eq telnet
SW103(config-ext-acl)# permit ip any any
SW103(config-ext-acl)# exit
SW103(config)# interface vlan 10
SW103(config-if)# ip access-group ENT_ACL in
SW103(config-if)# exit
SW103(config)# end
SW103# write memory
```

Task 3:

```
SW102(config)# interface Ethernet0/0
SW102(config-if)# switchport port-security
SW102(config-if)# switchport port-security maximum 2
SW102(config-if)# switchport port-security violation restrict
SW102(config-if)# exit
SW102(config)# end
SW102# write memory
```

問題 409

```
R2#conf t
R2(config)# ip access-list standard XLATE
R2(config-std-nacl)#permit 10.2.3.3
R2(config-std-nacl)#permit 192.168.3.1
R2(config-std-nacl)#permit 10.1.3.11
R2(config-std-nacl)#exit
R2(config)# interface G0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface G0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#ip nat pool test_pool 10.10.10.1 10.10.10.254 netmask 255.255.255.0
R2(config)#ip nat inside source list XLATE pool test_pool
R2(config)#exit
R2(config)#ntp server 10.1.2.1
R2#wr
```

```
R3(config)#interface G0/2
R3(config-if)#ip address dhcp
R3(config-if)#exit
```

```
R1#config t
R1(config)#ntp master 1
R1(config)#exit
R1#wr
```

```
R3(config)#ip domain name cisco.com
R3(config)#line vty 0 4
R3(config-line)#transport input ssh
R3(config-line)#login local
R3(config-line)#exit
R3(config)#username root password s3cret
R3(config)#crypto key generate rsa
R3(config)#exit
R3#wr
```

Task 1:

```
SW-1(config)# vlan 99
SW-1(config-vlan)# name FINANCIAL
SW-1(config-vlan)# exit
```

```
SW-2(config)# vlan 99
SW-2(config-vlan)# name FINANCIAL
SW-2(config-vlan)# exit
```

```
SW-3(config)# vlan 99
SW-3(config-vlan)# name FINANCIAL
SW-3(config-vlan)# exit
```

Task 2:

```
SW-1(config)# interface e0/2
SW-1(config-if)# switchport mode access
SW-1(config-if)# switchport access vlan 99
SW-1(config-if)# exit
```

```
SW-2(config)# interface e0/2
SW-2(config-if)# switchport mode access
SW-2(config-if)# switchport access vlan 99
SW-2(config-if)# exit
```

```
SW-3(config)# interface e0/2
SW-3(config-if)# switchport mode access
SW-3(config-if)# switchport access vlan 99
SW-3(config-if)# exit
```

Task 3:

```
SW-1(config)# cdp run
```

Task 4:

```
SW-1(config)# interface e0/2
SW-1(config-if)# no cdp enable
```



問題 413

Task 1:

R1:

```
interface e0/0  
ip address 10.0.12.5 255.255.255.254
```

R2:

```
interface e0/0  
ip address 10.0.12.6 255.255.255.254
```

Verification

To verify connectivity, ping between R1 and R2:

On R1:

```
ping 10.0.12.6
```

On R2:

```
ping 10.0.12.5
```

Task 2:

R1:

```
interface e0/0  
ipv6 address 2001:db8:12::1/126
```

R2:

```
interface e0/0  
ipv6 address 2001:db8:12::2/126
```

Verification:

R1:

```
ping 2001:db8:12::2
```

R2:

```
ping 2001:db8:12::1
```

問題 414

Task 1:

```
R5(config)# ip route 10.200.220.6 255.255.255.255 10.100.110.1
R1(config)# ip route 0.0.0.0 0.0.0.0 10.133.13.2
R5# traceroute 10.200.220.6
R5# ping 10.200.220.6
```

Task 2:

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.122.12.2 225
R2(config)# ip route 10.100.110.0 255.255.255.128 10.122.12.1
R1(config)# interface e0/1
R1(config-if)# shutdown
R5# traceroute 10.200.220.6
R5# ping 10.200.220.6
```

問題 421

Task 1:

```
Sw3(config)# username tech12 secret load1key
Sw3(config)# service password-encryption
Sw3(config)# line vty 0 4
Sw3(config-line)# login local
Sw3(config-line)# transport input telnet
Sw3(config-line)# exit
Sw3(config)# end
```

Task 2:

```
R1(config)# ip access-list extended ISP_ACL
R1(config-ext-acl)# deny ip 10.0.0.0 0.255.255.255 any
R1(config-ext-acl)# deny ip 172.16.0.0 0.255.255.255 any
R1(config-ext-acl)# permit ip any any
R1(config-ext-acl)# exit
R1(config)# interface e0/1
R1(config-if)# ip access-group ISP_ACL out
R1(config-if)# exit
```

Task 3:

```
Sw2(config)# ip arp inspection vlan 5
Sw2(config)# ip arp inspection validate dst-mac
Sw2(config)# ip arp inspection validate src-mac
Sw2(config)# ip arp inspection validate ip
```

Task 1:

Sw1:

```
interface e0/0
  switchport mode trunk
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 110,99
  switchport trunk native vlan 99
```

```
interface e0/1
  switchport mode trunk
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 110,99
  switchport trunk native vlan 99
```

Sw2:

```
interface e0/0
  switchport mode trunk
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 110,99
  switchport trunk native vlan 99
```

```
interface e0/1
  switchport mode trunk
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 110,99
  switchport trunk native vlan 99
```

Task 2:

Sw1:

```
interface range e0/0 - e0/1
  channel-group 1 mode active
interface Port-channel1
  no shutdown
```

Sw2:

```
interface range e0/0 - e0/1
  channel-group 1 mode active
interface Port-channel1
  no shutdown
```

問題 428

Task 1. Configure Sw1 and Sw2 with the VLAN naming as indicated.

```
SW-1(config)#vlan 77
SW-1(config-vlan)#name IT_User_VLAN
SW-1(config-vlan)#exit
SW-1(config)#vlan 88
SW-1(config-vlan)#name HR_User_VLAN
SW-1(config-vlan)#exit
SW-1(config)#vlan 177
SW-1(config-vlan)#name IT+Voice_VLAN
SW-1(config-vlan)#exit
SW-1(config)#vlan 188
SW-1(config-vlan)#name HR_User_VLAN
SW-1(config-vlan)#exit
```

```
SW-2(config)#vlan 77
SW-2(config-vlan)#name IT_User_VLAN
SW-2(config-vlan)#exit
SW-2(config)#vlan 88
SW-2(config-vlan)#name HR_User_VLAN
SW-2(config-vlan)#exit
SW-2(config)#vlan 177
SW-2(config-vlan)#name IT+Voice_VLAN
SW-2(config-vlan)#exit
SW-2(config)#vlan 188
SW-2(config-vlan)#name HR_User_VLAN
SW-2(config-vlan)#exit
```

Task 2. Assign the VLANs to the appropriate interfaces and set a non-trunking, non-tagged, single-VLAN for each interface according to the topology.

```
SW-1(config)#interface range E0/1-2
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 77
SW-1(config)#interface range E0/3
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 88
SW-1(config)#interface range E0/1
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 177
SW-1(config)#interface range E0/3
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 188
```

```
SW-2(config)#interface range E0/3
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 77
```

```
SW-2(config)#interface range E0/1
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 88
```

```
SW-2(config)#interface range E0/2
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 177
```

```
SW-2(config)#interface range E0/1
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 178
```

Task 3. Configure Sw1 and Sw2 to allow neighbor discovery via the vendor-neutral protocol on e0/0.

```
SW-1(config)#lldp run
SW-2(config)#lldp run
```

問題 429

```
R1# configure terminal
R1(config)# interface e0/1
R1(config-if)# ip address 10.0.22.1 255.255.255.252
R1(config-if)# exit
R1(config)# interface e0/2
R1(config-if)# ip address 10.0.33.1 255.255.255.252
R1(config-if)# exit
R1(config)# interface e0/0
R1(config-if)# ip address 10.0.233.1 255.255.255.240
R1(config-if)# exit
R1(config)# router ospf 33
R1(config-router)# router-id 10.0.22.1
```

```
R1(config-router)# interface e0/0
R1(config-if)# ip ospf 33 area 0
R1(config-if)# ip ospf priority 255
R1(config-if)# exit
```

```
R1(config-router)# interface e0/1
R1(config-if)# ip ospf 33 area 0
R1(config-if)# ip ospf priority 255
R1(config-if)# exit
```

```
R1(config-router)# interface e0/2
R1(config-if)# ip ospf 33 area 0
R1(config-if)# ip ospf priority 255
R1(config-if)# exit
```