

CCNP ENCOR(350-401) シミュレーション

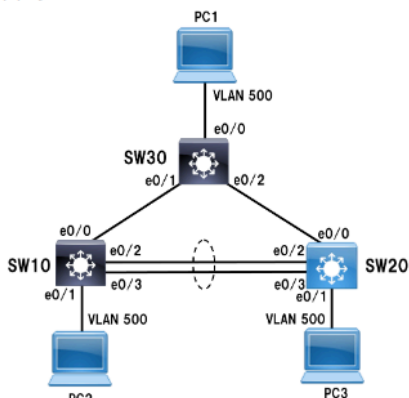
①Rapid PVST+ and LACP Sim

◆タスク

運用チームは、新しいサイトのネットワークデバイスの構成を開始しました。
これらの目標を達成するには、構成を完了します。

1. SW20 で Rapid PVST+ を設定します。
 2. SW20 と SW30 の間のトランクは動作していません。問題のトラブルシューティングを行い、PC3 がリンク経由で PC1 (10.10.100.10) に ping できることを確認します。
 3. SW10 と SW20 の間の LACP ポート チャネルは動作していません。問題をトラブルシューティングし、PC3 がポート チャネル経由で PC2 (10.10.100.20) に ping できることを確認します。
- 注: SW10 または SW30 にはアクセスできません。これらの問題は、SW20 のみに変更を加えて解決します。すべてのトランク上のトラフィックは、アクティブな VLAN のみに制限される必要があります。

◆トポロジ



◆SW20初期config

```
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree pathcost method long
!
interface Port-channel10
switchport mode access
!
interface Ethernet0/0
switchport mode access
!
```

```

interface Ethernet0/1
 switchport access vlan 500
 switchport mode access
 spanning-tree portfast edge
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 10 mode active
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 10 mode active
!
interface Vlan1
 ip address 10.10.1.20 255.255.255.0

```

◆ソリューション

このラボでは、スイッチ20にのみアクセス可能です。

タスク 1. SW20 で Rapid PVST+ を設定します。

```

SW20#conf t
SW20(config)#spanning-tree mode rapid-pvst

```

タスク 2. SW20とSW30の間のトランクが動作していません。問題のトラブルシューティングを行い、PC3 がリンク経由で PC1 (10.10.100.10) にpingできることを確認します。

SW20 で「show run」コマンドを使用すると、インターフェイス E0/0 がアクセス モードとして設定されていることがわかります。これをトランク モードに変更し、VLAN 500 のみを許可する必要があります(すべてのトランク上のトラフィックをアクティブな VLAN のみに制限する必要がある」という要求に従って)

```

SW20(config)#interface e0/0
SW20(config-if)#switchport trunk encapsulation dot1q
SW20(config-if)#switchport mode trunk
SW20(config-if)#switchport trunk allowed vlan 500

```

検証：
PC3#ping 10.10.100.10
!!!!

タスク 3. SW10 と SW20 の間の LACP ポート チャンネルが動作していません。問題をトラブルシューティングし、PC3 がポート チャンネル経由で PC2 (10.10.100.20) に ping できることを確認します。SW20 で「show run」コマンドを使用すると、ポート チャンネル 10 がその物理メンバー インターフェイス E0/2 および E0/3 と一致しないことがわかります。したがって、このポートチャンネルの設定を変更する必要があります。

注: ポートチャンネル番号は異なる場合があるため、注意深く確認してください。

```

SW20(config)#int Po10
SW20(config-if)#switchport trunk encapsulation dot1q
SW20(config-if)#switchport mode trunk
SW20(config-if)#switchport trunk allowed vlan 500

```

注:上記のインターフェイスポートチャンネル10でコマンド「switchport trunk allowed vlan 500」を発行すると、このコマンドは物理メンバーインターフェイス E0/2 および E0/3 にも自動的に適用されます。

◆検証：

SW20 で「show etherchannel summary」コマンドを使用して、問題が解決され、ポートチャンネルが SU (レイヤ 2/アップ) 状態になっているかどうかを確認します。

```

SW20#show etherchannel summary
--省略--
Number of channel-groups in use: 1
Number of aggregators:          1
Group Port-channel Protocol Ports
-----+-----+-----+-----
10   Po10(SU)    LACP    Et0/2(P)  Et0/3(P)

```

注: それでもエラーが表示される場合は、インターフェイスポートチャンネル10と E0/2、E0/3 の間の設定を確認してください。インターフェイス ポートチャンネル 10 が起動できるように、それらの間の設定は同じである必要があります

(channel-group 10 mode active)コマンドを除く)。

Interface Port-channel10 switchport trunk allowed vlan 500 switchport trunk encapsulation dot1q switchport mode trunk	Interface Ethernet0/2 switchport trunk allowed vlan 500 switchport trunk encapsulation dot1q switchport mode trunk channel-group 10 mode active
Interface Ethernet0/3 switchport trunk allowed vlan 500 switchport trunk encapsulation dot1q switchport mode trunk channel-group 10 mode active	

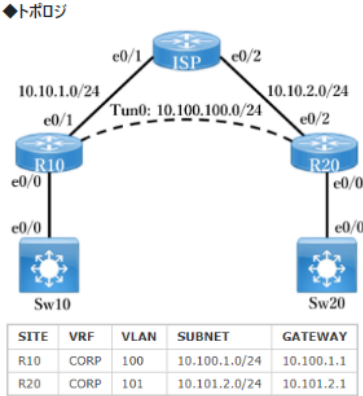
PC3#ping 10.10.100.20
!!!!

◆設定の保存
SW20#copy running-config startup-config

②VRF Configuration Sim

◆タスク
運用チームは、新しいサイトのネットワーク デバイスの構成を開始しました。R10 と R20 は、CORP VRF で事前構成されています。R10 は R20 にネットワーク接続されています。次の目標を達成するために構成を完了します。

1. Tunnel0 を使用して、R10 と R20 間の CORP VRF を拡張します。
- (オプション) 2. 事前構成済みのプロファイルを使用して Tunnel0 を保護します。
3. R10 と R20 でスタティック ルーティングを構成して、CORP VRF に属する VLAN 100 と VLAN 101 のユーザーが相互に通信できるようにします。Tunnel0 は、CORP VRF のトラフィックをルーティングするために使用される唯一のインターフェイスである必要があります。



◆初期config

<pre> R10 hostname R10 ! vrf definition CORP description Enable ipv4 for VRF CORP with below commands: address-family ipv4 exit-address-family ! interface e0/0 no shut interface e0/0.100 encapsulation dot1Q 100 vrf forwarding CORP ip address 10.100.1.1 255.255.255.0 ! interface e0/1 ip address 10.10.1.1 255.255.255.0 ip ospf 100 area 0.0.0.0 no shut ! router ospf 100 router-id 10.10.10.10 ! crypto isakmp policy 10 encr aes hash md5 authentication pre-share group 2 crypto isakmp key cisco address 10.10.2.1 ! crypto ipsec transform-set MYSET esp-aes esp-md5- hmac mode tunnel ! crypto ipsec profile MyProfile set transform-set MYSET ! interface tunnel0 vrf forwarding CORP ip address 10.100.100.1 255.255.255.0 tunnel source Ethernet0/1 no shut </pre>	<pre> R20 hostname R20 ! vrf definition CORP description Enable ipv4 for VRF CORP with below commands: address-family ipv4 exit-address-family ! interface e0/0 no shut interface e0/0.101 encapsulation dot1Q 101 vrf forwarding CORP ip address 10.101.2.1 255.255.255.0 ! interface e0/2 ip address 10.10.2.1 255.255.255.0 ip ospf 100 area 0.0.0.0 no shut ! router ospf 100 router-id 20.20.20.20 ! crypto isakmp policy 10 encr aes hash md5 authentication pre-share group 2 crypto isakmp key cisco address 10.10.1.1 ! crypto ipsec transform-set MYSET esp-aes esp-md5- hmac mode tunnel ! crypto ipsec profile MyProfile set transform-set MYSET ! interface tunnel0 vrf forwarding CORP ip address 10.100.100.2 255.255.255.0 tunnel source Ethernet0/2 no shut </pre>
<pre> ISP hostname ISP interface e0/1 ip address 10.10.1.2 255.255.255.0 ip ospf 100 area 0.0.0.0 no shut interface e0/2 ip address 10.10.2.2 255.255.255.0 ip ospf 100 area 0.0.0.0 no shut ! router ospf 100 router-id 1.1.1.1 </pre>	<pre> SW10 hostname Sw10 vlan 100 exit ! interface e0/0 switchport trunk encapsulation dot1q switchport mode trunk no shut ! interface e0/1 switchport mode access switchport access vlan 100 no shut </pre>

```
SW20
hostname Sw20
vlan 101
exit
!
interface e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
no shut
!
interface e0/1
switchport mode access
switchport access vlan 101
no shut
```

◆ソリューション

タスク 1. Tunnel0 を使用して、R10 と R20 の間で CORP VRF を拡張します。

まず、これらの 2 つのルータで「show ip interface brief」コマンドを使用して、R10 の e0/1 と R20 の e0/2 の IP アドレスを確認する必要があります。
それぞれ 10.10.1.1 と 10.10.2.1 であるとしています。これらを「tunnel destination ...」コマンドで使します。

R10で：

```
interface Tunnel 0
tunnel source Ethernet0/1 //初期設定に入っていない場合は入力
tunnel destination 10.10.2.1
vrf forwarding CORP //初期設定に入っていない場合は入力
「% Interface Tunnel0 IPv4 disabled and address(es) removed due to disabling VRF CORP」というメッセージが表示されますが、これはIPアドレスを再割り当てる必要がある事を意味しますので、その場合は以下を入力します
ip address 10.100.100.1 255.255.255.0
```

R20で：

```
interface Tunnel 0
tunnel source Ethernet0/2
tunnel destination 10.10.1.1
vrf forwarding CORP
ip address 10.100.100.2 255.255.255.0
```

トンネル インターフェイスでは、vrf forwarding コマンド (旧コマンドは「ip vrf forwarding」)を使用して、その特定のルーティング テーブルにトンネル インターフェイスを配置します。

「tunnel source ...」コマンドは初期設定で入力されていますが、念のためソリューションで再入力します。「vrf forwarding CORP」および「ip address 10.100.100.1 255.255.255.0」コマンドも同様です。

上記の「vrf forwarding CORP」コマンドを適用すると、IP アドレスが削除されるため、再度入力する必要があります (R10 の場合は「ip address 10.100.100.1 255.255.255.0」コマンドを使用)。

◆検証

R10:

```
R10#ping vrf CORP 10.100.100.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.100.2, timeout is 2 seconds:
!!!!
```

(オプション) タスク 2.事前設定されたプロファイルを使用して Tunnel0 を保護します。

注: このタスクは存在する場合と存在しない場合がありますので、慎重に確認してください。

タスク 2 では、「show run」コマンドを使用して事前設定されたプロファイルを見つける必要があります。「MyProfile」という名前だとします。このプロファイルを Tunnel 0 に適用します。

R10で：

```
interface Tunnel 0
tunnel protection ipsec profile MyProfile
```

R20で：

```
interface Tunnel 0
tunnel protection ipsec profile MyProfile
```

タスク 3. CORP VRF に属する VLAN 100 および VLAN 101 のユーザーが相互に通信できるように、R10 および R20 でスタティック ルーティングを設定します。

CORP VRF のトラフィックをルーティングするために使用するインターフェイスは、Tunnel0 のみにする必要があります。

スタティック ルート:

R10で:

```
R10(config)#ip route vrf CORP 10.101.2.0 255.255.255.0 Tunnel0
```

R20で:

```
R20(config)#ip route vrf CORP 10.100.1.0 255.255.255.0 Tunnel0
```

◆検証

R10:

```
R10#ping vrf CORP 10.101.2.1 source e0/0.100
!!!!
```

R20:

```
R20#ping vrf CORP 10.100.1.1 source e0/0.101
!!!!
```

◆configの保存

R10#, R20#copy running-config startup-config

③OSPF DR BDR Sim

◆検証

```
R3#show ip ospf neighbor
```

```
Neighbor ID Pri State Dead Time Address Interface
10.2.203.2 0 FULL/BDR 00:00:35 10.2.203.2 Ethernet 0/0
```

タスク 2. DR/BDR の選択に参加しないように R10 を設定します。このタスクを実行するために、インターフェイス設定で `ip ospf network point-to-point` コマンドを使用しないでください。

R10 が DR/BDR 選択に参加しないようにするには、そのインターフェイスを OSPF 優先度 0 で設定します。

```
R10(config)#int e0/0
```

```
R10(config-if)#ip ospf priority 0
```

◆検証

「show ip ospf neighbors」コマンドを使用して R2 上の R10 の OSPF 状態を確認すると、R10 の OSPF 状態が「DROTHER」であることがわかります。

```
R2#show ip ospf nei
```

```
Neighbor ID Pri State Dead Time Address Interface
10.0.3.1 1 FULL/BDR 00:00:37 10.0.2.1 Ethernet0/0
10.1.102.10 0 FULL/DROTHER 00:00:36 10.1.102.10 Ethernet0/1
```

◆コンフィグの保存

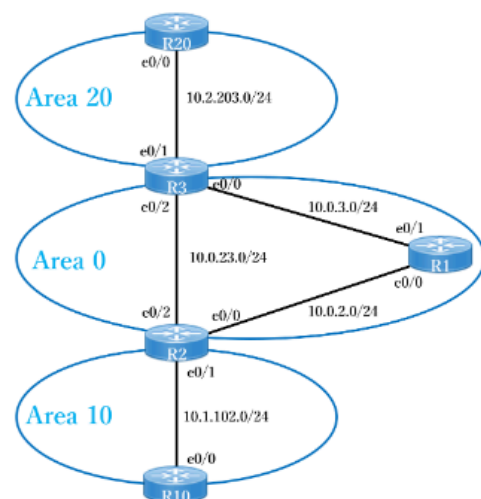
```
R3, R10# copy running-config startup-config
```

◆タスク

OSPF はすべてのデバイスで部分的に構成されています。次の結果を達成するには、構成を完了します。

1. R20 が常に BDR として指定されるように R3 を設定します。
2. DR/BDR の選択に参加しないように R10 を設定します。このタスクを実行するために、インターフェイス設定で `ip ospf network point-to-point` コマンドを使用しないでください。

◆トポロジ



◆ソリューション

タスク 1. R20 が常に BDR として指定されるように R3 を構成します。

OSPF プライオリティ値が最も高い DR になるように R3 を設定するため、確実に R20 が BDR を取得します。

```
R3(config)#interface e0/1
```

```
R3(config-if)#ip ospf priority 255
```

選択がリセットされていることを確認してください。R3 が DR になるように、R20 (R3 ではない) の OSPF プロセスをクリアする必要があることに注意してください。

```
R20#clear ip ospf process
```

```
Reset all OSPF processes? [no]: y
```

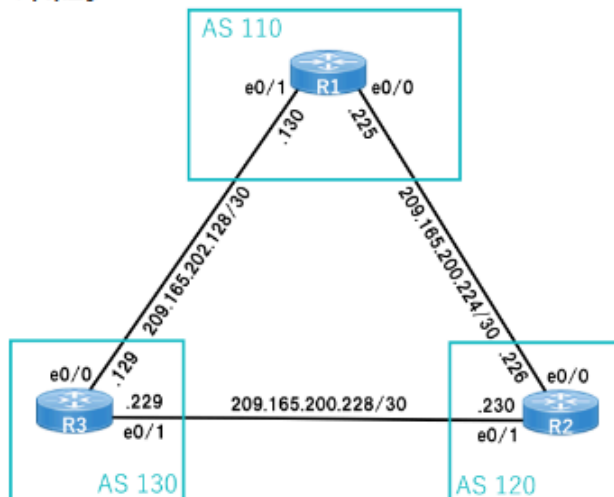
④eBGP Neighbor Sim

◆タスク

これらの結果を達成するには、トポロジに従って R3 を構成します。

1. ルーター ID にループバック 0 を使用して eBGP を設定します。これを行うために address-family コマンドを使用しないでください。
2. R3 のループバック 100 およびループバック 200 ネットワークを AS110 および AS120 にアドバタイズします。

◆トポロジ



初期コンフィグ

```
R1:
hostname R1
interface e0/0
ip address 209.165.200.225 255.255.255.252
no shut
!
interface e0/1
ip address 209.165.202.130 255.255.255.252
no shut
interface lo0
ip address 1.1.1.1 255.255.255.255
!
router bgp 110
bgp router-id 1.1.1.1
neighbor 209.165.200.226 remote-as 120
neighbor 209.165.202.129 remote-as 130
!
address-family ipv4
neighbor 209.165.200.226 activate
neighbor 209.165.202.129 activate
exit-address-family
```

```
R2:
hostname R2
interface e0/0
ip address 209.165.200.226 255.255.255.252
no shut
!
interface e0/1
ip address 209.165.200.230 255.255.255.252
no shut
interface lo0
ip address 2.2.2.2 255.255.255.255
!
router bgp 120
bgp router-id 2.2.2.2
neighbor 209.165.200.225 remote-as 110
neighbor 209.165.200.229 remote-as 130
!
address-family ipv4
neighbor 209.165.200.225 activate
neighbor 209.165.200.229 activate
exit-address-family
```

```

R3:
hostname R3
interface e0/0
 ip address 209.165.202.129 255.255.255.252
 no shut
!
interface e0/1
 ip address 209.165.200.229 255.255.255.252
 no shut
interface lo0
 ip address 3.3.3.3 255.255.255.255
interface lo100
 ip address 209.165.203.1 255.255.255.255
interface lo200
 ip address 200.200.203.2 255.255.255.255

```

◆ソリューション

注: このシムにはいくつかのバリエーションがあります。R3 の代わりに R2 を構成する必要がある場合があります。AS 番号も異なる場合がありますので、注意して確認してください。

タスク 1. ルーター ID にループバック 0 を使用して eBGP を設定します。これを行うために address-family コマンドを使用しないでください。

「show ip int brief」コマンドで Loopback0 インターフェースの IP アドレスを確認してください。この場合は 3.3.3.3 であるとしています。

```

R3:
router bgp 130
 bgp router-id 3.3.3.3
 neighbor 209.165.202.130 remote-as 110
 neighbor 209.165.200.230 remote-as 120

```

タスク 2. R3 のループバック 100 およびループバック 200 ネットワークを AS110 および AS120 にアドバタイズします。

Lo100 (209.165.203.1/32) および Lo200 (200.200.203.2/32) インターフェースの IP アドレスとサブネット マスクを注意深く確認し、以下の「network」コマンドと一致するようにしてください。この場合、Lo100 と Lo200 IP のサブネット マスクが両方とも /32 であると仮定します。

```

R3:
router bgp 130
 network 209.165.203.1 mask 255.255.255.255
 network 200.200.203.2 mask 255.255.255.255

```

検証:

「show ip route bgp」(または「show ip route」または「show ip bgp」) コマンドを使用して、R1、R2 のルーティングテーブルに R3 の Lo100 および Lo200 インターフェイスの IP アドレスがあるかどうかを確認します。

```

R1#show ip bgp summary
--output omitted--
Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
209.165.200.226 4        120     6      6      3    0  0:00:02:37    2
209.165.202.129 4        130     6      6      3    0  0:00:02:23    2

```

-> 「State/PfxRcd」フィールドに数字がある場合は、BGP 関係が確立されています。

```

R1#show ip route bgp
--output omitted--
 200.200.203.0/32 is subnetted, 1 subnets
B    200.200.203.2 [20/0] via 209.165.202.129, 00:02:15
 209.165.203.0/32 is subnetted, 1 subnets
B    209.165.203.1 [20/0] via 209.165.202.129, 00:02:15

```

◆設定の保存

```

R3#copy running-config startup-config

```

⑤ OSPF & Prefix-list Sim

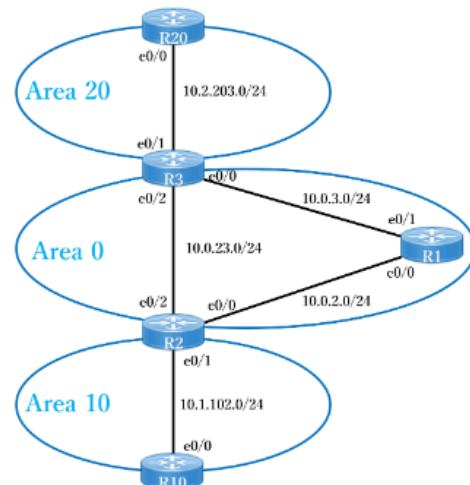
◆タスク

OSPF が部分的に構成されています。次の目標を達成するには、ABR ルーターで OSPF 構成を完了します。

1. R1 ループバック 0 のルートはエリア 10 にアドバタイズされるべきではありません。タスクを完了するには、部分的に設定されたプレフィックス リストを使用します。このタスクを実行するために、ルータの OSPF 設定セクションで area 0 コマンドを使用しないでください。

2. R20 ループバック 0 のルートは、エリア 20 の外にアドバタイズされるべきではありません。このタスクを実行するには、部分的に設定されたプレフィックス リストを使用します。このタスクを実行するために、ルータの OSPF 設定セクションで area 0 コマンドを使用しないでください。

◆トポロジ



◆R2 初期config

```
interface Loopback0
ip address 10.0.1.2 255.255.255.0
!
interface Ethernet0/0
ip address 10.0.2.2 255.255.255.0
!
interface Ethernet0/1
ip address 10.1.102.2 255.255.255.0
!
interface Ethernet0/2
ip address 10.0.23.2 255.255.255.0
!
router ospf 1
router-id 10.0.1.2
network 10.0.1.0 0.0.0.255 area 0
network 10.0.2.0 0.0.0.255 area 0
network 10.0.23.0 0.0.0.255 area 0
network 10.1.102.0 0.0.0.255 area 10
!
ip prefix-list deny_R1_Lo0 seq 2 permit 0.0.0.0/0 le 32
```

◆ソリューション

OSPF エリア フィルタリングに関する簡単な概要：

コマンド「area area-number filter-list prefix ... in」：プレフィックスがこのエリアに入らないようにします。

コマンド「area area-number filter-list prefix ... out」：ABR が接続されている他のエリアがプレフィックスを受信できないようにします。

注：IP アドレス、プレフィックス リスト名は異なる場合があるため、注意深く確認してください。

◆タスク 1. タスク 1. R1 ループバック 0 のルートは、エリア 10 にアドバタイズされません。タスクを実行するには、部分的に構成されたプレフィックス リストを使用します。タスクを実行するには、ルータ OSPF 構成セクションの area 0 コマンドを使用しないでください。

まず、R2 で「show run」コマンドを使用して、構成されたプレフィックス リストの名前を取得します。その名前が「deny_R1_Lo0」であるとしています。また、R1 で「show ip interface Brief」コマンドを使用して、R1 のループバック 0 の IP アドレスを見つけます。R1 の Lo0 IP アドレスが 1.1.1.1/32 であるとしています。

「deny_R1_Lo0」プレフィックス リストの初期構成は「ip prefix-list deny_R1_Lo0 seq 2 permit 0.0.0.0/0 le 32」であるため、R1 のループバック 0 のみを拒否するには、1 つのステートメントを先頭に追加するだけで済みます。

R2 :
R2(config)#ip prefix-list deny_R1_Lo0 seq 1 deny 1.1.1.1/32

受信方向のエリア フィルタリングを適用すると「area area-number filter-list prefix ... in」コマンドを使用）、ABR はこのエリアに入るプレフィックスをフィルタリングします。たとえば、エリア 10 に入ることから R1 の Loopback0 を除外したい場合は、R2 で次のコマンドを使用できます。

R2(config)#router ospf 1
R2(config-router)#area 10 filter-list prefix deny_R1_Lo0 in

検証 :
R10#ping 1.1.1.1
..... (失敗)
または、R10 で「show ip Route」コマンドを使用して、1.1.1.1 が R10 ルーティング テーブルに存在しないことを確認できます。

◆タスク 2. R20 ループバック 0 のルートはエリア 20 の外にアドバタイズされるべきではありません。このタスクを実行するには、部分的に設定されたプレフィックス リストを使用します。このタスクを実行するために、ルータの OSPF 設定セクションで area 0 コマンドを使用しないでください。

まず、R3 で「show run」コマンドを使用して、設定されたプレフィックス リストの名前を取得します。その名前が「deny_R20_Lo0」であるとしています。また、R20 で「show ip int Brief」コマンドを使用して、R20 の Loopback0 の IP アドレスを見つけます。R20 の Lo0 IP アドレスが 20.20.20.20/32 であるとしています。

「deny_R20_Lo0」プレフィックス リストには、「R3(config)#ip prefix-list deny_R20_Lo0 permit 0.0.0.0/0 le 32」という 1 つのステートメントがあることに注意してください。したがって、R20 の Loopback0 のみを拒否するには、このステートメントを先頭に追加するだけで済みます。

R3(config)#ip prefix-list deny_R20_Lo0 seq 1 deny 20.20.20.20/32

エリアフィルタリングのアウトバウンド方向を適用すると「area area-number filter-list prefix ... outbound」コマンドを使用）、ABR は他のエリアがこのプレフィックスを受信できないようにします。そのため、次のコマンドを使用する必要があります。

R3(config)#router ospf 1
R3(config-router)#area 20 filter-list prefix deny_R20_Lo0 out

検証 :
R2#ping 20.20.20.20
..... (失敗)

設定を保存 :
R2#, R3#copy running-config startup-config

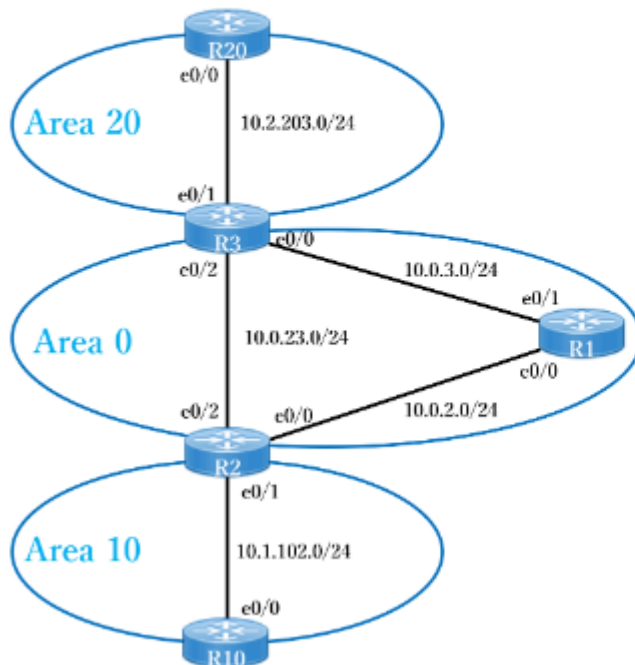
⑥ OSPF DR & Summarization Sim

◆タスク

OSPF はすべてのデバイスで部分的に構成されています。これらの目標を達成するには、構成を完了します。

1. R2 が常にエリア 10 の DR になるように設定します。ルーター ID は変更しないでください。
2. R2 で 1 つのコマンドを設定して、エリア 10 のルートを 1 つのルートに集約します。

◆トポロジ



R2 初期コンフィグ

```
interface Loopback0
ip address 10.0.1.2 255.255.255.0
!
interface Ethernet0/0
ip address 10.0.2.2 255.255.255.0
!
interface Ethernet0/1
ip address 10.1.102.2 255.255.255.0
!
router ospf 10
router-id 10.0.1.2
network 10.0.1.0 0.0.0.0.255 area 0
network 10.0.2.0 0.0.0.0.255 area 0
network 10.0.23.0 0.0.0.0.255 area 0
network 10.1.102.0 0.0.0.0.255 area 10
!
ip prefix-list deny_R1_Lo0 seq 2 permit 0.0.0.0/0 le 32
```

◆ソリューション

タスク 1. R2 が常にエリア 10 の DR になるように設定します。ルーター ID は変更しないでください。

```
R2(config)#int e0/1
R2(config-if)#ip ospf priority 255
```

選択がリセットされていることを確認してください。R2 が DR になれるように、R10 (R2 ではない) の OSPF プロセスをクリアする必要があることに注意してください。

```
R10#clear ip ospf process
Reset all OSPF processes? [no]: y
```

検証：
R10#show ip ospf neighbor

```
Neighbor ID Pri State Dead Time Address Interface
10.1.102.2 0 FULL/DR 00:00:35 10.2.203.2 Ethernet 0/0
```

タスク 2. R2 で 1 つのコマンドを設定して、エリア 10 のルートを 1 つのルートに要約します。

「show run」または「show ip ospf」コマンドで R2 の OSPF プロセス ID を確認します。OSPF プロセス ID が 10 であると仮定すると、この OSPF プロセス ID の下に要約されます。

注: このタスクを解決するための R10 構成がまだないため、推測する必要があります。

エリア 10 の下には 10.1.102.0/24 のネットワークが 1 つだけあるため、R10 にはループバックインターフェイスがあり、それらは OSPF にアダプタイズされていると考えられるため、それらをすべて要約する必要があります。R10 では、「show run」を使用して、これらのループバックインターフェイスの IP アドレスを確認し、それらが OSPF にアダプタイズされているかどうかを確認する必要があります（「network 10.1.x.x 0.0.x.x」コマンド経由）。

すべてのループバックインターフェイスのすべての IP アドレスが 10.1.x.x の範囲内にあると仮定します。それらをすべて 10.1.0.0/16 に要約しても安全です。

```
R2(config)#router ospf 10
R2(config-router)#area 10 range 10.1.0.0 255.255.0.0
```

検証：
R3 で「show ip route」（または「show ip route ospf」）コマンドを使用して、エリア 10 のすべてのルートが 1 つのルートに集約されているかどうかを確認します。

◆設定の保存

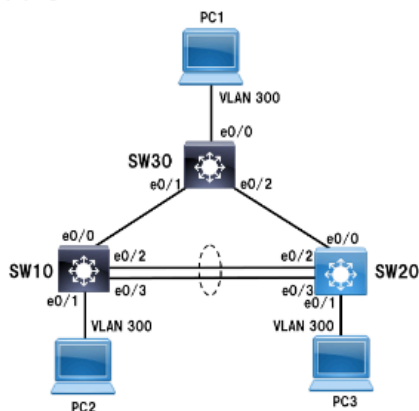
```
R2#copy running-config startup-config
```

⑦ Trunk UDLD & LACP Sim

◆タスク

1. SW10 と SW30 の間のトランクは動作していません。問題のトラブルシューティングを行い、PC2 がリンク経由で PC1 (10.10.100.10) に ping できることを確認します。
 2. SW10 インターフェイス E0/0 を積極的な単方向リンク検出用に設定します。
 3. SW10 と SW20 の間の LACP ポートチャネルは動作していません。問題のトラブルシューティングを行い、PC2 がポートチャネル経由で PC3 (10.10.100.30) に ping できることを確認します。
 - (オプション) 4. リンクステータスが UP に移行した直後にパケット転送が開始されるように、SW10 でインターフェイス e0/1 を設定します。
- 注: SW20 または SW30 にはアクセスできません。これらの問題は、SW10 のみに変更を加えて解決します。すべてのトランク上のトラフィックは、アクティブな VLAN のみに制限される必要があります。

◆トポロジ



```

Sw10 初期Config
interface Port-channel10
switchport trunk allowed vlan 1,300
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/0
switchport mode access
!
interface Ethernet0/1
switchport access vlan 300
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Vlan1
ip address 10.10.1.10 255.255.255.0

```

◆ソリューション

注: 一部のパラメータ (ポートチャネル番号など) が異なる場合があるため、設定を注意深く確認してください。

タスク 1. SW10 と SW30 の間のトランクが動作していません。問題のトラブルシューティングを行い、PC2 がリンク経由で PC1 (10.10.100.10) に ping できることを確認します。

SW10 で「show run」コマンドを使用すると、インターフェイス e0/0 がアクセスモードで設定されていることがわかり、それをトランクポートに変更する必要があります。

```

SW10(config)#interface e0/0
SW10(config-if)#switchport trunk encapsulation dot1q
SW10(config-if)#switchport mode trunk

```

検証:

PC2 を開き、PC1 に ping を実行してみます。

```
PC2>ping 10.10.100.10
```

```
!!!!
```

-> ping が成功しました。

タスク 2. SW10 インターフェイス E0/0 をアグレッシブな単方向リンク検出用に設定します。

```

SW10(config)#interface e0/0
SW10(config-if)#udld port aggressive

```

タスク 3. SW10 と SW20 の間の LACP ポートチャネルが動作していません。問題のトラブルシューティングを行い、PC2 がポートチャネル経由で PC3 (10.10.100.30) に ping できることを確認します。

上記の「show run」出力から、ポートチャネル 10 が最初に設定されていることがわかりました。そのため、このチャネルグループに E0/2 と E0/3 を割り当てるだけで済みます。

```

SW10(config)#interface range e0/2 - 3
SW10(config-if)#switchport trunk encapsulation dot1q
SW10(config-if)#switchport trunk allowed vlan 1,300
SW10(config-if)#channel-group 10 mode active

```

注: LACP を設定する前に「switchport trunk encapsulation dot1q」コマンドと「switchport trunk allowed vlan 1,300」コマンドを設定しない場合 (上記の「channel-group 10 mode active」コマンドを使用)、次のエラーが表示されます。

```
%EC-5-CANNOT_BUNDLE2: Et0/2 is not compatible with Po10 and will be suspended (trunk encap of Et0/2 is auto, Po10 is dot1q)
```

```
%EC-5-CANNOT_BUNDLE2: Et0/3 is not compatible with Po10 and will be suspended (trunk encap of Et0/3 is auto, Po10 is dot1q)
```

このエラーの原因は、e0/2 と e0/3 をグループ化する前に Po10 が作成されるため、物理インターフェイスが Po10 と互換性があることを確認する必要があります。

検証:

PC2 を開き、PC1 に ping を実行してみます。

```
PC2>ping 10.10.100.30
```

```
!!!!
```

-> ping が成功しました。

(オプション) タスク 4. リンクステートが UP に移行した直後にパケット転送が開始されるように、SW10 でインターフェイス e0/1 を設定します。

Portfast 機能により、スイッチポートは即座にスリーピング ツリー フォワーディング ステートに入り、リスニング ステートとラーニング ステートをバイパスするため、SW10 の E0/1 でこの機能を有効にする必要があります。

```

SW10(config)#interface e0/1
SW10(config-if)#spanning-tree portfast

```

◆設定の保存

```
SW10#copy running-config startup-config
```

⑧ OSPF DR BDR Sim 2

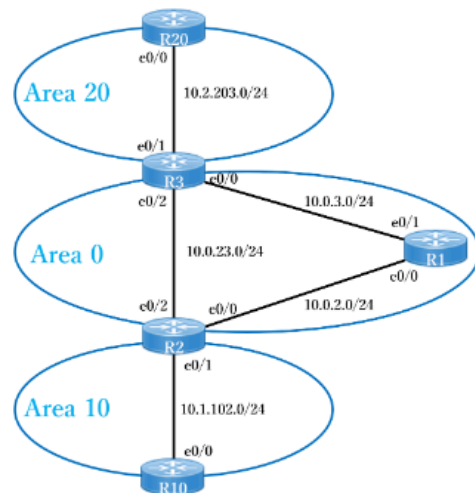
◆タスク

OSPF が部分的に構成されています。これらの目標を達成するには、OSPF 構成を完了します。

1. エリア 20 の DR/BDR 選択プロセスに参加しないように R3 と R20 を設定します。

2. R10 が常にエリア 10 の DR になるように設定します。ルーター ID は変更しないでください。

◆トポロジ



◆ソリューション

タスク 1. エリア 20 の DR/BDR 選択プロセスに参加しないように R3 と R20 を設定します。

エリア 20 にはルーターが 2 台しかいないため、それらのルーターで「ip ospf priority 0」コマンドを使用すると（DR/BDR 選択プロセスに参加しないように）、OSPF パケットを処理する DR/BDR がいないため、OSPF プロセスが失敗する可能性があります。より良い解決策は、OSPF ネットワークタイプをポイントツーポイントに設定することです。

R3 :

```
R3(config)#interface e0/1
```

```
R3(config-if)#ip ospf network point-to-point
```

R20 :

```
R20(config)#interface e0/0
```

```
R20(config-if)#ip ospf network point-to-point
```

両方のルーターで選択がリセットされていることを確認します。

```
R3#,R20#clear ip ospf process
Reset all OSPF processes? [no]: y
```

◆検証

```
R3#show ip ospf neighbor
Neighbor ID  Pri  State      Dead Time  Address      Interface
...
10.2.1.1      0  FULL/-    00:00:10  10.2.203.20  Ethernet0/1
```

注: ネイバーを識別するには、「アドレス」フィールドをチェックする必要があります (「ネイバー ID」フィールドではルータが明確に示されていないため)。上記の出力では、10.2.203.20 の「アドレス」フィールドから、これが R20 であることがわかります。

タスク 2. R10 が常にエリア 10 の DR になるように設定します。ルーター ID は変更しないでください。

```
R10 を、OSPF 優先度の値が最も高い DR になるように設定できます。
R10(config)#interface e0/0
R10(config-if)#ip ospf priority 255
```

R2 と R10 で選択がリセットされていることを確認します。

```
R2#,R10#clear ip ospf process
Reset all OSPF processes? [no]: y
```

◆検証

R2 で「show ip ospf neighbors」コマンドを使用すると、R10 (「アドレス」フィールドが 10.1.102.10) が「DR」状態を示していることがわかります。

◆コンフィグの保存

```
R3#,R10#, R20#copy running-config startup-config
```

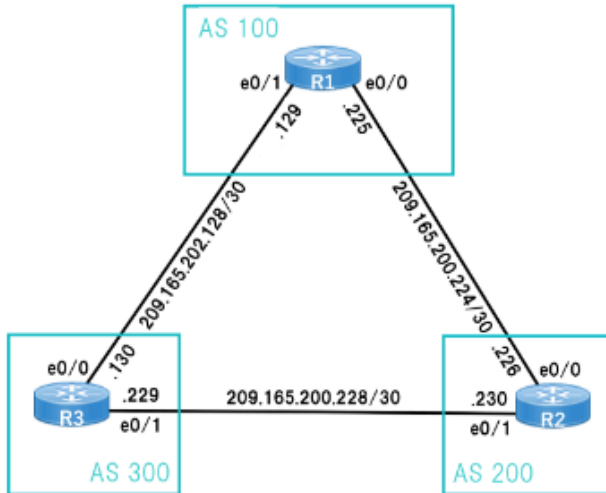
⑨eBGP Neighbor Sim 2

◆タスク

eBGP は R2 と R3 で設定されます。これらのタスクを完了するように R1 を構成します

1. address-family コマンドを使用して、トポロジに従って eBGP を設定します。ルーター ID には Loopback0 を使用します。
2. R1 のループバック 0、1、および 2 ネットワークを AS 200 および AS 300 にアドバタイズします。

◆トポロジ



R1初期コンフィグ

```
interface loopback0
ip address 10.1.1.100 255.255.255.255
!
interface loopback1
ip address 209.165.201.1 255.255.255.248
!
interface loopback2
ip address 209.165.201.9 255.255.255.248
!
interface Ethernet0/0
ip address 209.165.200.225 255.255.255.252
!
interface Ethernet0/1
ip address 209.165.202.129 255.255.255.252
```

※注: IP アドレス、サブネット マスク、BGP AS 番号は異なる場合があるため、注意深く確認してください。

◆ソリューション

タスク 1. address-family コマンドを使用して、トポロジに従って eBGP を設定します。ルーター ID には Loopback0 を使用します。
Loopback0 インターフェースの IP アドレスは「show ip int Brief」または「show run」コマンドで確認してください。この場合は 10.1.1.100 であるとして。

R1 で：

```
router bgp 100 //BGP AS番号は100ではない可能性があるので、注意深く確認下さい
bgp router-id 10.1.1.100
neighbor 209.165.200.226 remote-as 200
neighbor 209.165.202.130 remote-as 300
address-family ipv4
neighbor 209.165.200.226 activate
neighbor 209.165.202.130 activate
```

タスク 2. R1 のループバック 0、1、および 2 ネットワークを AS 200 および AS 300 にアドバタイズします。

R1 で：

注：タスク 1 からまだ「address-family ipv4」モードであると仮定します。

BGP では、各インターフェイスに設定されている正確なサブネット マスクを使用してネットワークをアドバタイズする必要があります。

したがって、ループバック 1 では「209.165.201.0 mask 255.255.255.248」、ループバック 2 では「209.165.201.8 mask 255.255.255.248」となる必要があります。

R1 で、次のコマンドを入力します (タスク 1 の「address-family ipv4」モードで)。

```
network 10.1.1.100 mask 255.255.255.255
network 209.165.201.0 mask 255.255.255.248
network 209.165.201.8 mask 255.255.255.248
```

◆検証

R1 では、「show ip bgp summary」コマンドを使用して、eBGP ネイバー関係が確立されているかどうかを確認できます。

```
R1#show ip bgp summary
--output omitted--

Neighbor      V      AS  MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
209.165.200.226 4      200      13      13        4    0    0 00:00:26        0
209.165.202.130 4      300      13      13        4    0    0 00:00:35        0
```

「State/PfxRcd」フィールドに数字 (この場合は「0」) があることがわかります。これは、eBGP ネイバー関係が確立されたことを意味します。

注：R2 と R3 は R1 にネットワークをアドバタイズしないため、ここでは受信したプレフィックス (PfxRcd) は 0 になります。

また、R2 または R3 で「show ip bgp」コマンドを使用して、R1 上の 3 つのネットワークがこのルータにアドバタイズされているかどうかを確認します。

R2 または R3:

```
R2#show ip bgp
--省略--

Network        Next Hop        Metric LocPrf Weight Path
* 10.1.1.100/32  209.165.200.229      0      0 300 100 i
*>
* 209.165.201.0/29 209.165.200.229      0      0 300 100 i
*>
* 209.165.201.8/29 209.165.200.225      0      0 100 i
*>
* 209.165.201.8/29 209.165.200.229      0      0 300 100 i
*>
* 209.165.200.225 209.165.200.225      0      0 100 i
```

◆設定の保存

R1#copy running-config startup-config

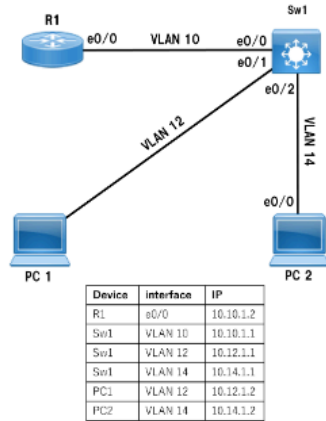
⑩NetFlow Sim

◆タスク

運用チームは、いくつかの監視アクティビティの構成を開始しました。以下のタスクの構成を完了します。

1. R1 で Flexible NetFlow フロー エクスポートの設定を完了し、UDP ポート 2055 を使用してコレクタにデータを送信します。
2. Sw1 でスイッチ ポート アナライザを設定し、セッション番号 11 を使用して PC1 との間のすべての通信をインターフェイス E1/1 にミラーリングします。
3. R1 上で事前設定された IP SLA 動作をスケジュールして、すぐに実行を開始し、無期限に実行します。

◆トポロジ



◆ソリューション

注: すべてのパラメータ (ポート、IP アドレス、セッション番号、IP SLA 番号など) は異なる場合があるため、注意深く確認してください。

タスク 1. R1 で Flexible NetFlow フロー エクスポートの設定を完了し、UDP ポート 2055 を使用してコレクタにデータを送信します。

「show run」コマンドを使用して、Flow Exporter が存在するかどうかを確認する必要があります。

存在しない場合は、任意の名前を定義できます。ここでの Flow Exporter の名前を「MyFlowExporter」とします。

NetFlow コレクタの IP アドレスがわかりません。Sw1 にアクセスできる場合は、「show run」コマンドを使用して、Sw1 が見つかるかどうかを確認します。ここでの NetFlow コレクタは、IP アドレス 10.14.1.2 の PC2 であるとして、以下の「destination」コマンドで使います。

```
R1:
flow exporter MyFlowExporter
destination 10.14.1.2
transport udp 2055
export-protocol netflow-v9
```

タスク 2. Sw1 でスイッチ ポート アナライザを設定し、セッション番号 11 を使用して PC1 との間のすべての通信をインターフェイス E1/1 にミラーリングします。

PC1 はスイッチのインターフェイス e0/1 上にあるため、このインターフェイスを監視します。

```
Sw1:
monitor session 11 source interface e0/1 both
monitor session 11 destination interface e1/1
```

タスク 3. R1 上で事前設定された IP SLA 動作をスケジュールして、すぐに実行を開始し、無期限に実行します。

まず、「show run」コマンドで事前設定された IP SLA 番号を確認する必要があります。

```
R1#show run
...
ip sla 5
...
```

見つかった IP SLA 番号が 5 であるとして、次のコマンドでこの番号を使用します。

```
R1:
R1(config)#ip sla schedule 5 life forever start-time now
```

◆設定の保存

```
R1#,Sw1#copy running-config startup-config
```

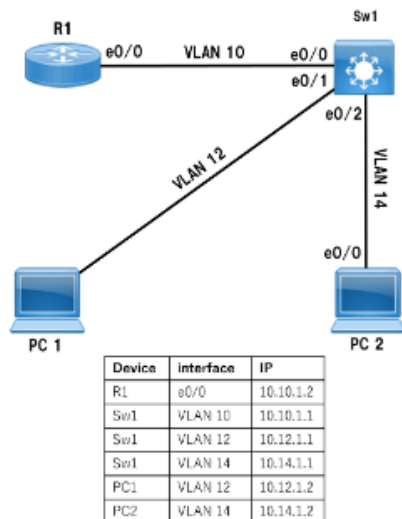
⑪ NetFlow Sim 2

◆タスク

運用チームは、いくつかの監視アクティビティの構成を開始しました。以下のタスクの構成を完了します。

1. 事前設定されたフロー モニタを使用して、R1 E0/0 で両方向の Flexible NetFlow を有効にします。
2. Sw1 でスイッチ ポート アナライザを設定し、セッション番号 12 を使用してすべての VLAN 12 トラフィックをインターフェイス E1/3 にミラーリングします。
3. R1 で基本的な IP SLA ICMP エコー動作を設定し、300 秒ごとに PC1 に ping を実行します。

◆トポロジ



◆R1の初期Config

```
flow exporter Export-R1Flow
destination 10.10.1.10
source Loopback0
transport udp 2055
!
flow monitor Monitor-R1Flow
exporter Export-R1Flow
cache timeout inactive 30
cache timeout active 300
record netflow ipv4 original-input
!
interface loopback0
ip address 1.1.1.1 255.255.255.255
```

```
interface Ethernet0/0
ip address 10.10.1.2 255.255.255.0
ip ospf network point-to-point
!
router ospf 10
router-id 1.1.1.1
network 1.1.1.1 0.0.0.0 area 0
network 10.10.1.0 0.0.0.255 area 0
```

◆ソリューション

注: すべてのパラメータ (ポート、IP アドレス、セッション番号、IP SLA 番号など) は異なる場合があるため、注意深く確認してください。

タスク 1. 事前設定されたフロー モニタを使用して、R1 E0/0 で両方向の Flexible NetFlow を有効にします。

```
R1:
R1(config)#interface e0/0
R1(config-if)# ip flow monitor Monitor-R1Flow input
R1(config-if)# ip flow monitor Monitor-R1Flow output
```

タスク 2. Sw1 でスイッチ ポート アナライザを設定し、セッション番号 12 を使用してすべての VLAN 12 トラフィックをインターフェイス E1/3 にミラーリングします。

```
Sw1:
Sw1(config)#monitor session 12 source vlan 12 both
Sw1(config)#monitor session 12 destination interface e1/3
```

検証:

```
SW1#show monitor session 12
```

タスク 3. R1 で基本的な IP SLA ICMP エコー動作を設定し、300 秒ごとに PC1 に ping を送信します。
PC1のIPアドレスは10.12.1.2です。

```
R1:
R1(config)# ip sla 1
R1(config-ip-sla)# icmp-echo 10.12.1.2 source-interface Ethernet0/0
R1(config-ip-sla-echo)#frequency 300
R1(config-ip-sla-echo)#exit
R1(config)# ip sla schedule 1 life forever start-time now
```

◆検証

「show ip sla summary」コマンドを使用して、この IP SLA のステータスを確認できます。

```
R1# show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
ID      Type      Destination      Stats      Return      Last
      (ms)      Code           Run
-----
*1      icmp-echo  10.12.1.2      RTT=2      OK          4 seconds ago
```

◆設定の保存

```
R1#,SW1#copy running-config startup-config
```

⑫ OSPF Advertised & Summarized Sim

◆タスク

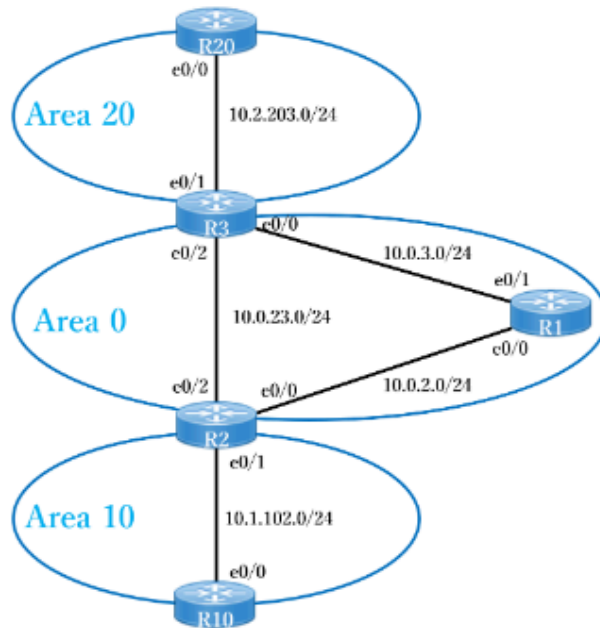
OSPF が部分的に構成されています。これらの目標を達成するには、OSPF 構成を完了します。

1. すべてのネットワークがアドバタイズされるように、トポロジに従ってルーター R1 で OSPF を構成します。

このタスクを実行するために、「router ospf」設定セクションの下にある network ステートメントを使用しないでください。

2. ABR ルーター上で 1 つのコマンドを設定して、1 つのサマリー ルートのみがエリア 0 にアドバタイズされるようにします。

◆トポロジ



◆R1初期config

```
interface loopback0
ip address 10.0.1.1 255.255.255.0
!
interface Ethernet0/0
ip address 10.0.2.1 255.255.255.0
!
interface Ethernet0/1
ip address 10.0.3.1 255.255.255.0
```

◆ソリューション

タスク 1. すべてのネットワークがアドバタイズされるように、トポロジに従ってルーター R1 で OSPF を構成します。
このタスクを実行するために、「router ospf」設定セクションの下にある network ステートメントを使用しないでください。

まず、R1 で「show run」コマンドを使用して、OSPF 関連の構成が設定されているかどうかを確認する必要があります。
そうでない場合は、任意の OSPF プロセス ID を選択できます。ここでは、OSPF プロセス ID 1 を使用します。
※タスクをよく読んでください。他の OSPF エリアを使用して他のルータを設定するよう求められる場合があります

```
R1(config)#router ospf 1
R1(config-router)#exit
R1(config)#interface loopback0
R1(config-if)#ip ospf 1 area 0
R1(config-if)#interface ethernet0/0
R1(config-if)#ip ospf 1 area 0
R1(config-if)#interface ethernet0/1
R1(config-if)#ip ospf 1 area 0
```

◆検証

「show ip ospf interface brief」コマンドで確認すると、ここにすべてのインターフェイス（Loopback0、E0/0、E0/1）が表示されます。
これは、OSPF がこれらのインターフェイスで有効になっていることを意味します。

R1#show ip ospf interface brief							
Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Lo0	1	0	10.0.1.1/24	1	LOOP	0/0	
Et0/1	1	0	10.0.3.1/24	10	BDR	1/1	
Et0/0	1	0	10.0.2.1/24	10	BDR	1/1	

また、「show ip route ospf」コマンドを使用して、R1 が学習した OSPF ルートを確認できるようになりました。

R1#show ip route ospf							
--省略--							
10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks							
O	10.0.23.0/24	[110/20]	via 10.0.3.3, 00:00:09, Ethernet0/1				
			[110/20] via 10.0.2.2, 00:00:09, Ethernet0/0				
O IA	10.1.102.0/24	[110/20]	via 10.0.2.2, 00:00:09, Ethernet0/0				
O IA	10.2.203.0/24	[110/20]	via 10.0.3.3, 00:00:09, Ethernet0/1				

タスク 2. ABR ルーター上で 1 つのコマンドを設定し、サマリー ルートが 1 つだけエリア 0 にアドバタイズされるようにします。

トポロジには R2 と R3 という 2 つの ABR ルーターがあるため、両方を設定する必要があります。
R2 および R3 で「show run」コマンドを使用して、各インターフェイスに設定されている OSPF プロセス ID、IP アドレス、およびサブネット マスクをチェックし、それらすべてを 1 つのサマリールートに要約できることを確認する必要があります。

- + R2 と R3 の両方の OSPF プロセス ID は「1」です「router ospf 1」の行を確認してください
- + R2 のすべてのインターフェイスは 10.1.0.0/16 サブネットに属します
- + R3 のすべてのインターフェイスは 10.2.0.0/16 サブネットに属します

R2で：
R2(config)#router ospf 1
R2(config-router)#area 10 range 10.1.0.0 255.255.0.0

R3で：
R3(config)#router ospf 1
R3(config-router)#area 20 range 10.2.0.0 255.255.0.0

◆検証

R1 で「show ip Route」(または「show ip Route ospf」) コマンドを使用して、10.1.x.x からのルートが 1 つだけ、および 10.2.x.x からのルートが 1 つだけ存在するかどうかを確認します。

R1#show ip route ospf							
--output omitted--							
10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks							
O	10.0.23.0/24	[110/20]	via 10.0.3.3, 00:03:28, Ethernet0/1				
			[110/20] via 10.0.2.2, 00:03:28, Ethernet0/0				
O IA	10.1.0.0/16	[110/20]	via 10.0.2.2, 00:00:27, Ethernet0/0				
O IA	10.2.0.0/16	[110/20]	via 10.0.3.3, 00:00:08, Ethernet0/1				

◆設定の保存

R1#,R2#,R3# copy running-config startup-config

⑬Access-list & CoPP Sim

EIGRPはすべてのルータに事前設定されています。これらのタスクを完了するには、R10とR20を構成します。

◆タスク

タスク1.EIGRPルートがR20およびR30から受信されるように、R10上の既存のACLを変更します。

–この変更では、EIGRPルートのみが通過できるようにする必要があります。

–このタスクを実行するためにR10から構成を削除しないでください。

タスク2.R20でCoPPを設定して、次の結果を実現します。

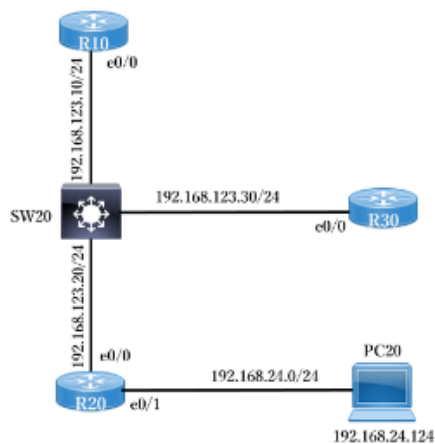
–192.168.24.0/24からのICMPトラフィックを許可します。*

–トラフィックを8,000bpsに制限します。

–追加のパケットを破棄します。

*注:このSIMには別のバージョンがあり、上記のタスク2でICMPではなくSSHを許可する必要があるため、要件を注意深く確認してください。

◆トポロジ



◆R10初期config

```
interface loopback0
ip address 192.168.1.0 255.255.255.255
interface e0/0
ip address 192.168.123.10 255.255.255.0
ip access-group 150 in
!
router eigrp 10
network 192.168.1.10 0.0.0.0
network 192.168.123.0
```

```
access-list 150 permit tcp any any
access-list 150 permit udp any any
access-list 150 permit icmp any any
access-list 150 deny ip any any
```

注: ACL 番号、IP アドレス、EIGRP AS 番号は異なる場合があるため、注意深く確認してください。

◆ソリューション

タスク 1. EIGRP ルートが R20 および R30 から受信されるように、R10 上の既存の ACL を変更します。
(変更では EIGRP ルートの通過のみが許可されます。R10 から設定は削除しないでください)

まず、R10 で「show ip eigrp neighbors」コマンドを使用して、R10 に EIGRP ネイバーがあるかどうかを確認する必要があります。

```
R10#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(10)
(E Empty)
```

-> ACL 150 が EIGRP プロトコルをブロックしているため、現在 R10 には EIGRP ネイバーがありません。
EIGRP プロトコルは TCP、UDP、または ICMP ではないため、フィルタリングされて除外されることに注意してください。

R10 では、「show ip access-list 150」コマンドを使用して ACL 150 のシーケンス番号を確認できます。

```
R10#show ip access-list 150
Extended IP access list 150
 10 permit tcp any any
 20 permit udp any any
 30 permit icmp any any
 40 deny ip any any (186 matches)
```

この ACL は R10 での EIGRP の受信をブロックしているため、シーケンス 40 より前にすべての EIGRP 関連パケットを許可する必要があります。
(他のパケットを「すべて拒否」します) この場合、シーケンス 5 を使用します。

```
R10:
R10(config)#ip access-list extended 150
R10(config-ext-nacl)#5 permit eigrp any any
```

次に、R10 で EIGRP ネイバーを再度確認します。

```
R10#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(10)
H   Address           Interface           Hold Uptime   SRTT   RTO   Q   Seq
                               (sec)          (ms)          Cnt  Num
1   192.168.123.20      Et0/0              12 00:02:11   10    100   0    9
0   192.168.123.30      Et0/0              14 00:02:14   10    100   0   10
```

-> R20 (192.168.123.20) と R30 (192.168.123.30) は R10 EIGRP ネイバーになりました。

タスク 2. これらの結果を達成するために R20 で CoPP を設定します (192.168.24.0/24 からの ICMP トラフィックを許可、トラフィックを 8,000 bps に制限、追加のパケットを破棄)

R20:

```
access-list 100 permit icmp 192.168.24.0 0.0.0.255 any
!
class-map CoPP_ICMP
 match access-group 100
!
policy-map CHECK_ICMP
 class CoPP_ICMP
  police 8000
   conform-action transmit
  exceed-action drop
!
control-plane
 service-policy input CHECK_ICMP
```

*バージョン 2: 192.168.24.0/24 からの SSH トラフィックを許可します (ICMP ではありません)
上記のアクセスリスト 100 を次のように変更するだけです。

```
access-list 100 permit tcp 192.168.24.0 0.0.0.255 any eq 22
```

PC20 では、約 100 パケットで R20 に ping を実行して、いくつかのパケットがドロップされることを確認できます。

```
PC20#ping 192.168.24.20 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.24.20, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 93 percent (93/100), round-trip min/avg/max = 1/1/1 ms
```

```
R20#show policy-map control-plane
Control Plane

Service-policy input: CHECK_ICMP

Class-map: CoPP_ICMP (match-all)
  436 packets, 49704 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: access-group 100
  police:
    cir 8000 bps, bc 1500 bytes
      conformed 405 packets, 46170 bytes; actions:
        transmit
      exceeded 31 packets, 3534 bytes; actions:
        drop
    conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)
  208 packets, 15749 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any
```

```
R10, R20#copy running-config startup-config
```

◆タスク

タスク1.Sw20は、LACPを使用してSw10との802.1トランキングEtherChannelのネゴシエーションを積極的に試行していますが、チャネルは機能していません。Sw10の問題を解決します。
タスク2.スパンニングツリー設定を変更して、Sw10が常にVLAN10およびVLAN30のルートになるようにします。

```
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel10
!
interface Ethernet0/0
 switchport access vlan 20
 switchport mode access
!
interface Ethernet0/1
 switchport access vlan 20
 switchport mode access
!
interface Ethernet0/2
 switchport access vlan 20
 switchport mode access
!
```

```
interface Ethernet0/3
switchport access vlan 10
switchport mode access
!
interface Ethernet1/0
switchport access vlan 20
switchport mode access
!
interface Vlan10
ip address 10.100.10.10 255.255.255.0
!
interface Vlan20
ip address 10.100.20.10 255.255.255.0
!
ip ssh server algorithm encryption aes128—ctr aes192—ctr aes256—ctr
ip ssh client algorithm encryption aes128-ctr aes192—ctr aes256-ctr
```

◆ソリューション

タスク1.Sw20は、LACPを使用してSw10との802.1トランキンクEtherChannelのネゴシエーションを積極的に試行していますが、チャネルは機能していません。Sw10の問題を解決します。
注: ポートチャネル番号は異なる場合があるため、注意深く確認してください。

e0/0-2にポートチャネルを作成するときに競合しないようにするには、最初にインターフェイスポートチャネル11を無効にする必要があります。

```
Sw10で：
no interface po11 //disable interface Port-channel 11
interface range e0/0 - 2
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 11 mode active
```

次のように、ポートチャネル 11 が起動しているという通知が表示されます。

*Apr 9 07:09:39.202: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel11, changed state to up

◆検証

インターフェイスポートチャネル11は、「show interfaces trunk」コマンドでトランクポートになりました。

```
Sw10# show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/3	on	802.1q	trunking	1
Et1/0	on	802.1q	trunking	1
Po11	on	802.1q	trunking	1

タスク2.スパンニングツリー設定を変更して、Sw10が常にVLAN10およびVLAN30のルートになるようにします。

```
Sw10(config)#spanning-tree vlan 10,30 root primary
```

◆検証

「show spanning-tree vlan 10,30」を使用して、Sw10 がルートブリッジになるかどうかを確認します。

```
Sw10#show spanning-tree vlan 10,30
```

VLAN0010

Spanning tree enabled protocol ieee

Root ID Priority 24586

Address aabb.cc00.1000

This bridge is the root

--省略--

VLAN0030

Spanning tree enabled protocol ieee

Root ID Priority 24606

Address aabb.cc00.1000

This bridge is the root

--省略--

◆configの保存

```
Sw10#copy running-config startup-config
```

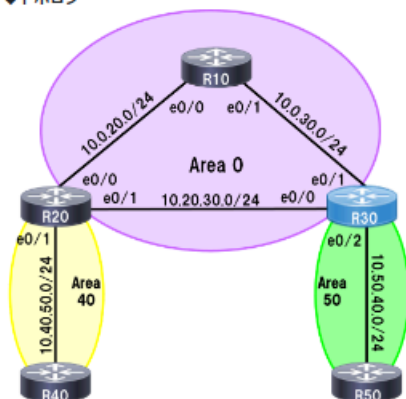
⑮ OSPF Summarization Sim

◆タスク

※R30のみにアクセスする

1. プロセスID100を使用してOSPFを設定します。ルーターIDにはLo0を使用します。「network」コマンドを使用してすべてのネットワークをアドバタイズします。
2. エリア50の集約ルート/18を作成します(LSAタイプ3のみをエリア0にフラッディングする必要があります)

◆トポロジ



注:ここでのIPアドレスはデモンストレーションのみを目的としています。試験では必ず異なりますので、概念をよく理解してください。
他のパラメータ(OSPFプロセス、集約ルート/18)も異なる場合があります。

◆R30初期config

```
interface loopback0
ip address 10.30.30.30 255.255.255.255
interface ethernet0/0
ip address 10.20.30.30 255.255.255.0
interface ethernet0/1
ip address 10.0.30.30 255.255.255.0
interface ethernet0/2
ip address 10.50.40.30 255.255.255.0
(OSPFのconfigは見当たりませんでした)
```

タスク1. プロセスID100を使用してOSPFを設定します。ルーターIDにはLo0を使用します。「network」コマンドを使用してすべてのネットワークをアドバタイズします。

R30で :

```
router ospf 100
router-id 10.30.30.30
network 10.30.30.30 0.0.0.0 area 0
network 10.20.30.0 0.0.0.255 area 0
network 10.0.30.0 0.0.0.255 area 0
network 10.50.40.0 0.0.0.255 area 50
```

タスク2. エリア50の集約ルート/18を作成します(LSAタイプ3のみをエリア0にフラッディングする必要があります)
要約されたルート(プレフィックスが/18となる)なので、サブネットマスクは255.255.192.0である必要があります。
※サブネット10.50.40.0/24は10.50.0.0/18(40<64として)に要約されます

R30で :

```
router ospf 100
area 50 range 10.50.0.0 255.255.192.0
```

◆configの保存

```
R30#copy running-config startup-config
```

⑩ OSPF Summarization Sim 2

OSPFは、R20を除くすべてのデバイスで事前設定されています。これらのタスクを完了するには、R20を構成します。

◆タスク

タスク1.次の要件を使用して、トポロジに従ってOSPFを構成します。

+プロセスID20を使用します。

+ルーターIDにはLoopback0を使用します。

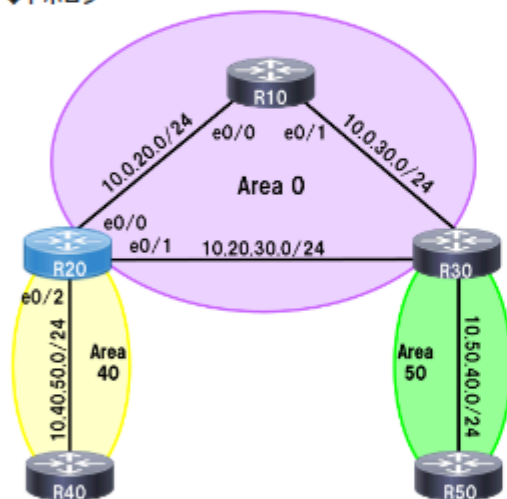
+すべてのネットワークをOSPFにアドバタイズします。

—このタスクを実行するために、OSPFプロセスでネットワークステートメントを使用しないでください。

タスク2.エリア40の/18サマリールートを設定します。

+タイプ3LSAのみをエリア0にアドバタイズします。

◆トポロジ



◆R20初期config

```
interface loopback0
ip address 20.20.20.20 255.255.255.255
interface e0/0
ip address 10.0.20.20 255.255.255.0
interface e0/1
ip address 10.20.30.20 255.255.255.0
interface e0/2
ip address 10.40.50.20 255.255.255.0
(OSPFの設定は見当たりませんでした)
```

◆ソリューション

タスク1.次の要件を使用して、トポロジに従ってOSPFを構成します。

+プロセスID20を使用します。

+ルーターIDにはLoopback0を使用します。

+すべてのネットワークをOSPFにアドバタイズします。

—このタスクを実行するために、OSPFプロセスでネットワークステートメントを使用しないでください。

まず、「show run」または「show ip interface brief」を使用して、R20のループバック0のIPアドレスを見つける必要があります。仮に20.20.20.20だとします。

R20で：

```
router ospf 20
router-id 20.20.20.20
```

「network」コマンドを使用せずにR20のすべてのネットワークをOSPFにアドバタイズするには、各インターフェイスでOSPFを有効にする必要があります。

R20で：

```
interface loopback0
ip ospf 20 area 0
interface e0/0
ip ospf 20 area 0
interface e0/1
ip ospf 20 area 0
interface e0/2
ip ospf 20 area 40
```

タスク2.エリア40の/18サマリールートを設定します。

+タイプ3LSAのみをエリア0にアドバタイズします。

R20で：

```
router ospf 20
area 40 range 10.40.0.0 255.255.192.0
```

◆configの保存

```
R30#copy running-config startup-config
```

⑪ VRF Configuration Sim 2

◆タスク

同僚が新しいネットワークの構成を開始しました。R11のすべての構成が完了し、R11とR22間の通信が機能しています。以下のタスクについて、R22 構成を完了してください。

タスク1

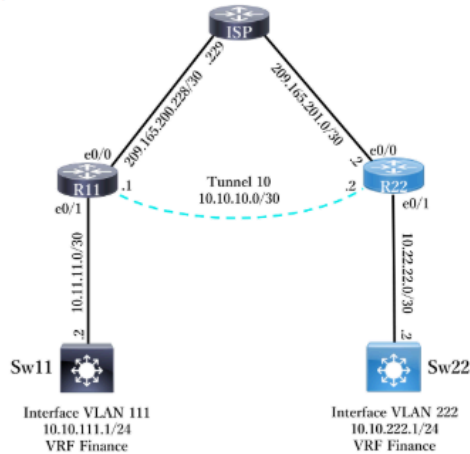
トンネル10を使用して、R11とR22の間にFinance VRFを拡張します。

タスク2

R22でFinance VRF構成を完了し、VLAN 111とVLAN 222間のトラフィックがトンネル10のみを使用するようにスタティックルーティングを構成します。

注: Sw22を使用してトラフィックフローを検証できます。

◆トポロジ



R22 Initial Config (use "show run" to get)

```
interface Loopback0
ip address 10.2.2.2 255.255.255.255
interface Ethernet0/0
ip address 209.165.201.2 255.255.255.252
no shut
interface Ethernet0/1
ip address 10.22.22.1 255.255.255.252
no shut
!
router bgp 3
neighbor 209.165.201.1 remote-as 2
address-family ipv4
neighbor 209.165.201.1 activate
network 209.165.201.0 mask 255.255.255.252
!
```

Sw22 Initial Config

```
vlan 222
!
interface Ethernet0/0
no switchport
ip address 10.22.22.2 255.255.255.252
interface Vlan222
ip address 10.10.22.1 255.255.255.0
no shut
!
interface Ethernet0/3 //to make interface VLAN 222 up
switchport mode access
switchport access vlan 222
!
ip route 0.0.0.0 0.0.0.0 10.22.22.1
```

注: 上記の構成は参考用です。異なる場合もありますので、概念を把握してください。

タスク1. トンネル10を使用して、R11とR22の間でFinance VRFを拡張します。

VRF Financeを作成し、それにインターフェイストンネル10を割り当てる必要があります。

R22の場合:

```
R22(config)#ip vrf Finance
R22(config-vrf)#rd 100:1 //任意の数値を使用することも、このコマンドを無視することもできます
R22(config-vrf)#exit
R22(config)#interface Tunnel10
R22(config-if)#vrf forwarding Finance //古い IOS バージョンでは、代わりに「ip vrf forwarding Finance」が必要です
R22(config-if)#ip address 10.10.10.2 255.255.255.252
R22(config-if)#tunnel source e0/0
R22(config-if)#tunnel destination 209.165.200.230
R22(config-if)#no shut
R22(config-if)#exit
R22(config)#exit
```

◆検証

R22#ping vrf Finance 10.10.10.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:

!!!! ->成功

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

タスク2. R22でFinance VRF構成を完了し、VLAN 111とVLAN 222間のトラフィックがトンネル10のみを使用するようにスタティックルーティングを構成します。

VRF FinanceをSw22に拡張するには、R22のe0/0インターフェイスをVRF Financeにも割り当てる必要があります。

R22の場合:

R22(config)#interface e0/1

R22(config-if)#vrf forwarding Finance

//次の通知が表示されます。[% Interface Ethernet0/1 IPv4 disabled and address(es) removed due to enabling VRF Finance.]

R22(config-if)#ip address 10.22.22.1 255.255.255.252 //IPアドレスを再割り当てする

R22で静的ルーティングを設定します。

R22(config)#ip route vrf Finance 10.10.111.0 255.255.255.0 tunnel10

R22(config)#ip route vrf Finance 10.10.222.0 255.255.255.0 10.22.22.2

◆検証

Sw22では、ソースVLAN 222を使用してSw11のインターフェイスVLAN 111にpingを実行してテストできます。

Sw22#ping 10.10.111.1 source vlan 222

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.111.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.222.1

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

◆設定を保存

R22#, SW22#copy running-config startup-config