テスト対策

OSPF

R1

1. すべてのルータで OSPF ルーティングプロセスを開始します。プロセス ID 10を使用します。

```
router ospf 10
```

2. router-id コマンドを使用して、すべてのルータの OSPF ID を次のように設定します。
   • R1: 1.1.1.1
   • R2: 2.2.2.2
   • R2: 3.3.3.3

```
router-id 1.1.1.1
```

3. すべてのルータで接続されているすべてのネットワークに対してOSPFルーティングをアクティブ化し、ルーティングプロセスを設定します。

```
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 209.165.201.0 0.0.0.3 area 0
```

4. すべてのルータでOSPF ネイバーに直接接続されていないすべてのインターフェイスをパッシブに設定します。

```
passive-interface g0/0/0
passive-interface g0/0/1
```

5. すべてのルータで参照帯域幅を1ギガビットに調整します。

```
auto-cost reference-bandwidth 1000
```

6. すべてのルータでhello タイムを 30 秒に設定します。

```
int s0/1/0
ip ospf hello-interval 30
```

R2

```
router ospf 10
router-id 2.2.2.2
network 192.168.3.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
network 209.165.201.0 0.0.0.3 area 0
network 209.165.101.0 0.0.0.3 area 0
passive-interface g0/0/0
passive-interface g0/0/1
auto-cost reference-bandwidth 1000
int s0/1/0
ip ospf hello-interval 30
int s0/1/1
ip ospf hello-interval 30
```

R3

```
router ospf 10
router-id 3.3.3.3
network 192.168.5.0 0.0.0.255 area 0
network 209.165.101.0 0.0.0.3 area 0
passive-interface g0/0/0
auto-cost reference-bandwidth 1000
int s0/1/1
ip ospf hello-interval 30
```

ACL

R3

1. R3で表1を実現するアクセスコントロールリスト「ACL_X」を作成します。※プロトコルに関係なく、他のすべてのトラフィックが許可されます

   ```
   ip access-list extended ACL_X
   deny tcp host 192.168.1.1 host 192.168.5.1 eq 80
   deny tcp host 192.168.3.1 host 192.168.5.1 eq 80
   deny icmp host 192.168.2.1 host 192.168.5.1
   deny icmp host 192.168.4.1 host 192.168.5.1
   permit ip any any !こいつ重要!
   ```

   eqは=
2. 「ACL_X」をR3の適切なインターフェイスと向きに適用します。

```
int s0/1/1 !基本的に入ってくるinterfaceを選択!
ip access-group ACL_X in
```

試しにpingコマンド(ICMP)やWebブラウザ(HTTP)を使ってパケットが到達するか確認する(重要)

NAT

1. R1のOSPF から 192.168.1.0/24 を削除します。

```
router ospf 10
no network 192.168.1.0 0.0.0.255 area 0
exit
```

2. R1で192.168.1.0 ネットワークと一致する ACL を作成します。

```
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface s0/1/0 overload
```

overloadはポートアドレス変換

3. R1でACL とインターフェイス S0/1/0 の間の NAT を設定し、ポートアドレス変換を使用します。

```
int g0/0/0
ip nat inside
int s0/1/0
ip nat outside
```

memo

- show run大事です。