

OSPF 验证问题

今天一个朋友问我 OSPF 验证的问题，说 OSPF 的接口加密，区域加密和虚链路加密不清楚。

这里我就先简单的解答一下接着用实验验证结论。

1.OSPF 的接口加密。

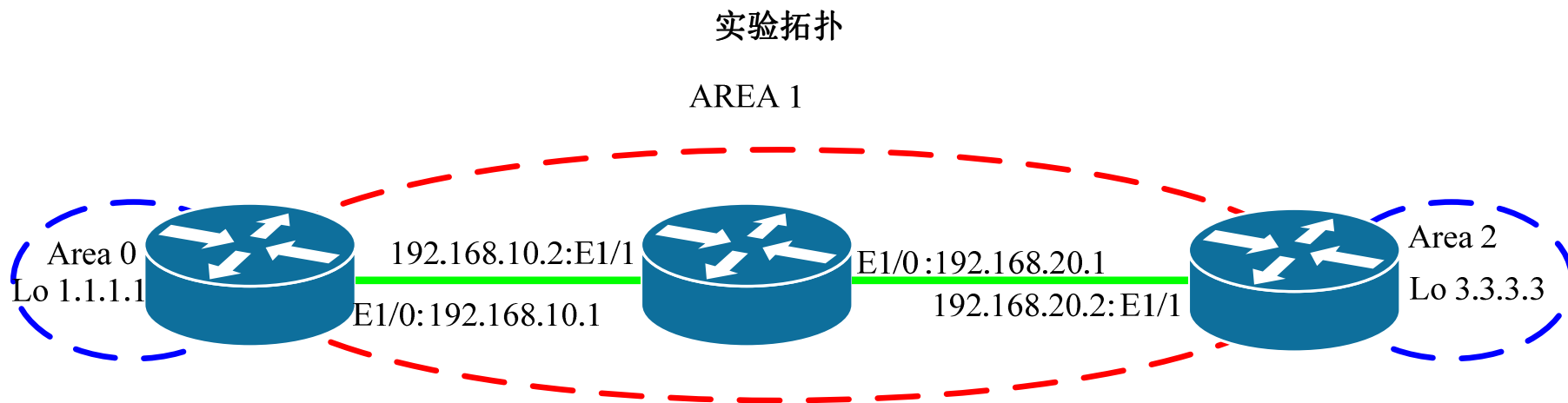
是指在运行 OSPF 网络中,两个路由器直连接口的验证。相当于本地的一种验证，跟其它接口没有关系，只是定位到具体的两个接口之间。但是如果接口上起了验证,就不需要在区域中配置验证了。

2.OSPF 的区域加密

是指在运行 OSPF 网络中，配置了区域加密,那么想加入该区域的设备必须启用区域加密。区域加密的所有的密钥和加密方式必须是统一的。

3.虚链路加密。

虚链路加密是区域加密的一种应用，可以看做是从外部接入到区域中需要进行的一种验证身份的方式。如果区域上已经建立了验证,链路这端就不需要进行验证。



1. 先配置 OSPF 路由。然后在一端启用加密，另一端不启用加密。观察效果

配置 OSPF~

R1

```
R1(config)#router ospf 100
```

```
R1(config-router)#router-id 1.1.1.1
```

```
R1(config-router)#net 1.1.1.1 0.0.0.0 area 0
```

```
R1(config-router)#net 192.168.10.1 0.0.0.0 area 1
```

R2

```
R2(config)#router ospf 100
```

```
R2(config-router)#router-id 2.2.2.2
```

```
R2(config-router)#net 2.2.2.2 0.0.0.0 area 1
```

```
R2(config-router)#net 192.168.10.2 0.0.0.0 area 1
```

R3

```
R3(config)#router ospf 100
```

```
R3(config-router)#router-id 3.3.3.3
```

```
R3(config-router)#net 3.3.3.3 0.0.0.0 area 2
```

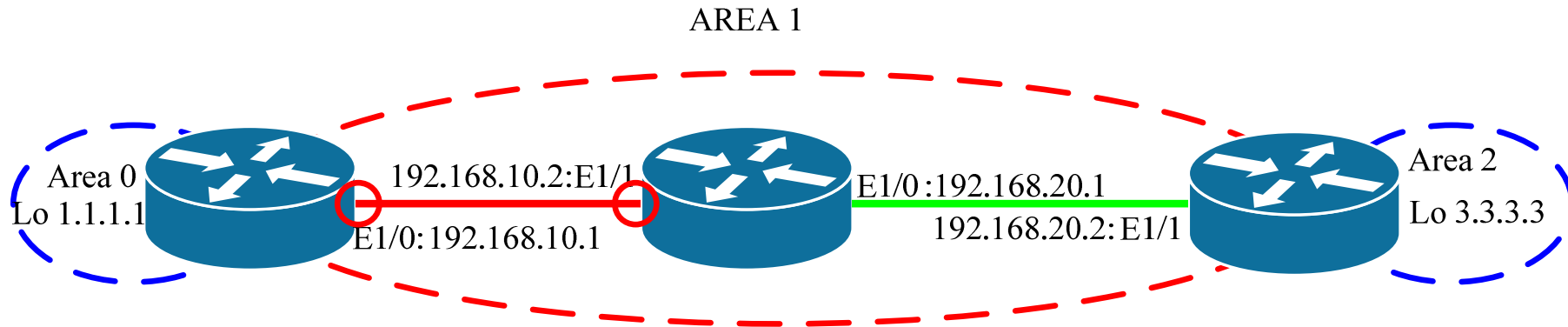
```
R3(config-router)#net 192.168.20.2 0.0.0.0 area 1
```

在 R2 上 show ip ospf nei 可以看到两个 OSPF 的邻居。证明 OSPF 已经正常运行了。

```
R2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	2WAY/DROTHER	00:00:33	192.168.20.2	Ethernet1/0
1.1.1.1	1	FULL/BDR	00:00:39	192.168.10.1	Ethernet1/1

下面将 R1 和 R2 之间的链路进行接口加密,看效果。



R1

```
R1(config)#int e1/0
```

```
R1(config-if)#ip ospf authentication message-digest
```

```
R1(config-if)#ip ospf message-digest-key 1 md5 cisco
```

当一端启用了验证加密的时候,与之直连的 OSPF 的邻居关系会 down 掉。因为 OSPF 的交互的报文会不匹配,无法建立邻居关系。

```
R2#  
*Mar  1 00:47:03.675: %OSPF-5-ADJCHG: Process 100, Nbr 1.1.1.1 on Ethernet1/1 from FULL to DOWN,  
Neighbor Down: Dead timer expired  
R2#
```

R2

```
R2(config)#int e1/1
```

```
R2(config-if)#ip ospf authentication message-digest
```

```
R2(config-if)#ip ospf message-digest-key 1 md5 cisco
```

这时候使用 `show ip ospf interface e1/1` 命令 可以看启用 OSPF 接口的信息，显示的是加密的，并调用了密钥。这时候两端接口使用的验证方式一样，密钥也一样，并且调用了密钥的 `Key id` ，那么就坐等 OSPF 的邻居关系的建立。

```
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 1.1.1.1 (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
Message digest authentication enabled
  Youngest key id is 1
```

当两端同时启用了验证加密,OSPF 邻居关系自然就起来了。因为两端交互报文相同。

```
R2(config-if)#
*Mar  1 00:47:54.327: %OSPF-5-ADJCHG: Process 100, Nbr 1.1.1.1 on Ethernet1/1 from LOADING to FULL, Loading Done
R2(config-if)#
```

然而在接口上启用加密是不影响区域内，其它运行 OSPF 设备的关系

```
R2#show ip ospf neighbor
```

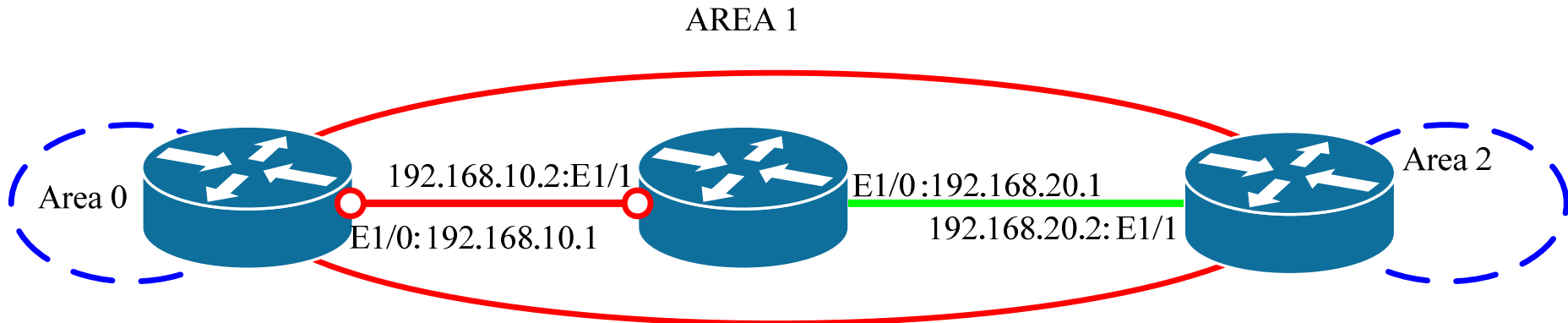
Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/DR	00:00:32	192.168.20.2	Ethernet1/0
1.1.1.1	1	FULL/BDR	00:00:38	192.168.10.1	Ethernet1/1

结论

OSPF 的接口加密。

是指在运行 OSPF 网络中,两个路由器直连接口的验证。相当于本地的一种验证,跟其它接口没有关系,只是定位到具体的两个接口之间。

2.在 R2 和 R3 之间配置 OSPF 的区域加密,观察如果配置的区域加密, R1 和 R2 的邻居关系有什么变化。



R2

```
R2(config)#router ospf 100
```

```
R2(config-router)#area 1 authentication message-digest
```

```
R2(config-if)#ip ospf message-digest-key 2 md5 111222
```

```
R2(config-router)#
*Mar 1 01:13:47.831: %OSPF-5-ADJCHG: Process 100, Nbr 3.3.3.3 on Ethernet1/0 from FULL to DOWN,
Neighbor Down: Dead timer expired
```

R3

```
R3(config)#router ospf 100
```

```
R3(config-router)#area 1 authentication message-digest
```

```
R3(config-if)#ip ospf message-digest-key 2 md5 111222
```

```
R2#  
*Mar  1 01:18:36.615: %OSPF-5-ADJCHG: Process 100, Nbr 3.3.3.3 on Ethernet1/0 from LOADING to FULL, Loading Done  
R2#
```

R1 上不启用 AREA 1 的验证也可以建立邻居关系。实际上合你们想的有些不一样吧。区域加密和链路加密同时启用时,链路加密是优先的。

```
R1#show run | se ospf
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
router ospf 100
router-id 1.1.1.1
log-adjacency-changes
network 1.1.1.1 0.0.0.0 area 0
network 192.168.10.1 0.0.0.0 area 1
R1#
```

R2 上 show ip ospf neighbor 查看 OSPF 邻居关系。

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	1	FULL/BDR	00:00:31	192.168.10.1	Ethernet1/1
3.3.3.3	1	FULL/BDR	00:00:37	192.168.20.2	Ethernet1/0

启用了区域加密后，只有 R3 断开的邻居关系，是因为 R1 和 R2 OSPF 的报文交互的时候已经使用的是验证的数据包文。那么当启用区域验证的时候。端口的验证在先，端口起来的，那么自然就需要区域验证了。也就是大家所说的端口验证的优先级要高于区域验证。如果端口有验证了，那么就不需要区域验证。

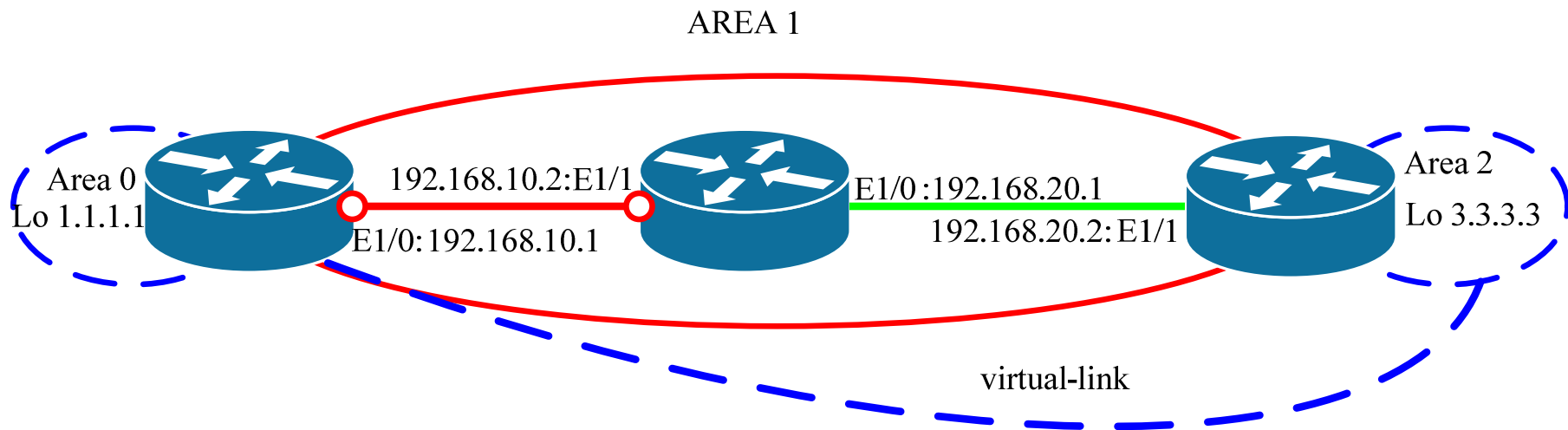
端口验证：是验证路由器对端设备的身份。也就是说只是点到点的认证。其它的不管。一般在边界路由上端口认证用的比较多。

区域验证：是接入到目的区域中，必须启用的验证，范围是整个区域。这要比端口验证的范围大的多。一般在核心路由上端口认证用的比较多。

2. 虚链路加密,下面解决一下虚链路加密的问题。如果虚链路加密是为了验证接入 OSPF 区域路由的身份。

创建虚链路是为了遵循所有非骨干区域的路由都要与骨干区域路由相连的原则。在以上拓扑中就是虚链路的一个典型应用。为了让 AREA 0 区域知道

AREA 2 的路由使用虚链路。穿越 AREA 1 进行加密验证。这里在 R1 上配置虚链路,并起了验证。密码为 cisco 验证类型为 MD5



配置:

```
R1(config)#router ospf 100
```

```
R1(config-router)#area 1 virtual-link 3.3.3.3 message-digest-key 3 md5 cisco
```

```
R3(config)#router ospf 100
```

```
R3(config-router)#area 1 virtual-link 1.1.1.1 message-digest-key 3 md5 cisco
```

同样我在 R3 上配置虚链路起验证。然后观察，发现虚链路已经建立成功。可以通过 `show ip ospf neighbor` 命令看到 OSPF 虚链路的状态。

```
R3#show ip ospf nei
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	0	FULL/ -	-	192.168.10.1	OSPF_VL1
2.2.2.2	1	FULL/DR	00:00:33	192.168.20.1	Ethernet1/1

接下来我验证一件事情，R1 上没有启用区域加密，但是虚链路起了加密。R3 上启用了区域加密，也启用了虚链路加密。要证明虚链路加密是基于区域的。实际上只要 R3 不用虚链路加密同样能够使 R1 和 R3 之间的虚链路建立成功即可。那就试了一下。把 R3 上的 虚链路加密的命令 NO 掉。观察一下效果。

```
R3(config-router)#
R3(config-router)#area 1 virtual-link 1.1.1.1 message-digest-key 3 md5 cisco
R3(config-router)#
*Mar  1 03:09:45.859: %OSPF-5-ADJCHG: Process 100, Nbr 1.1.1.1 on OSPF_VL5 from LOADING to FULL
Loading Done
R3(config-router)#no area 1 virtual-link 1.1.1.1 message-digest-key 3
R3(config-router)#do show run | se ospf
ip ospf message-digest-key 2 md5 cisco
router ospf 100
router-id 3.3.3.3
log-adjacency-changes
area 1 authentication message-digest
area 1 virtual-link 1.1.1.1
network 3.3.3.3 0.0.0.0 area 2
```

以上图示，正如所说的一样，只要 R3 不用虚链路加密同样能够使 R1 和 R3 之间的虚链路建立成功即可，是因为 R3 在区域上已经进行了加密验证。所以在建立虚链路的时候报文的加密格式是相同的，自然就能够通信。

Summary

1.OSPF 的接口加密。

是指在运行 OSPF 网络中,两个路由器直连接口的验证。相当于本地的一种验证,跟其它接口没有关系,只是定位到具体的两个接口之间。但是如果接口上起了验证,就不需要在区域中配置验证了。

2.OSPF 的区域加密

是指在运行 OSPF 网络中,配置了区域加密,那么想加入该区域的设备必须启用区域加密。区域加密的所有的密钥和加密方式必须是统一的。

3.虚链路加密。

虚链路加密是区域加密的一种应用,可以看做是从外部接入到区域中需要进行的一种验证身份的方式。如果区域上已经建立了验证,链路这端就不需要进行验证。

验证方式的区别

端口验证：是验证路由器对端设备的身份。也就是说只是点到点的认证。其它的不管。一般在边界路由上端口认证用的比较多。

区域验证：是接入到目的区域中，必须启用的验证，范围是整个区域。这要比端口验证的范围大的多。一般在核心路由上端口认证用的比较多

通过以上实验大家应该能够弄清楚 OSPF 几种加密类型的关系了吧。接口>区域>虚链路。也就是说虚链路基于区域。区域基于接口。

CCIE#27588

Paddy.Liu

2010-12-20