

修订记录

本页不打印

课程编码	适用产品	产品版本	课程版本

作者/工号	时间	审核人/工号	新开发/优化





VRF基本概念及应用



前言

- 回顾前面学习的课程，您还记得几个名字中带“V”的协议或技术？这些协议或技术又有哪些特点或共同点？
- VRF（Virtual Routing and Forwarding，虚拟路由转发）技术通过在一台三层转发设备上创建多张路由表实现数据或业务的隔离，常用于MPLS VPN、防火墙等一些需要实现隔离的应用场景。
- 本课程将介绍VRF的基本概念及其基本配置方法。



目标

- 学完本课程后，您将能够：
 - 描述VRF的基本概念
 - 描述VRF的典型应用
 - 实现VRF的基本配置

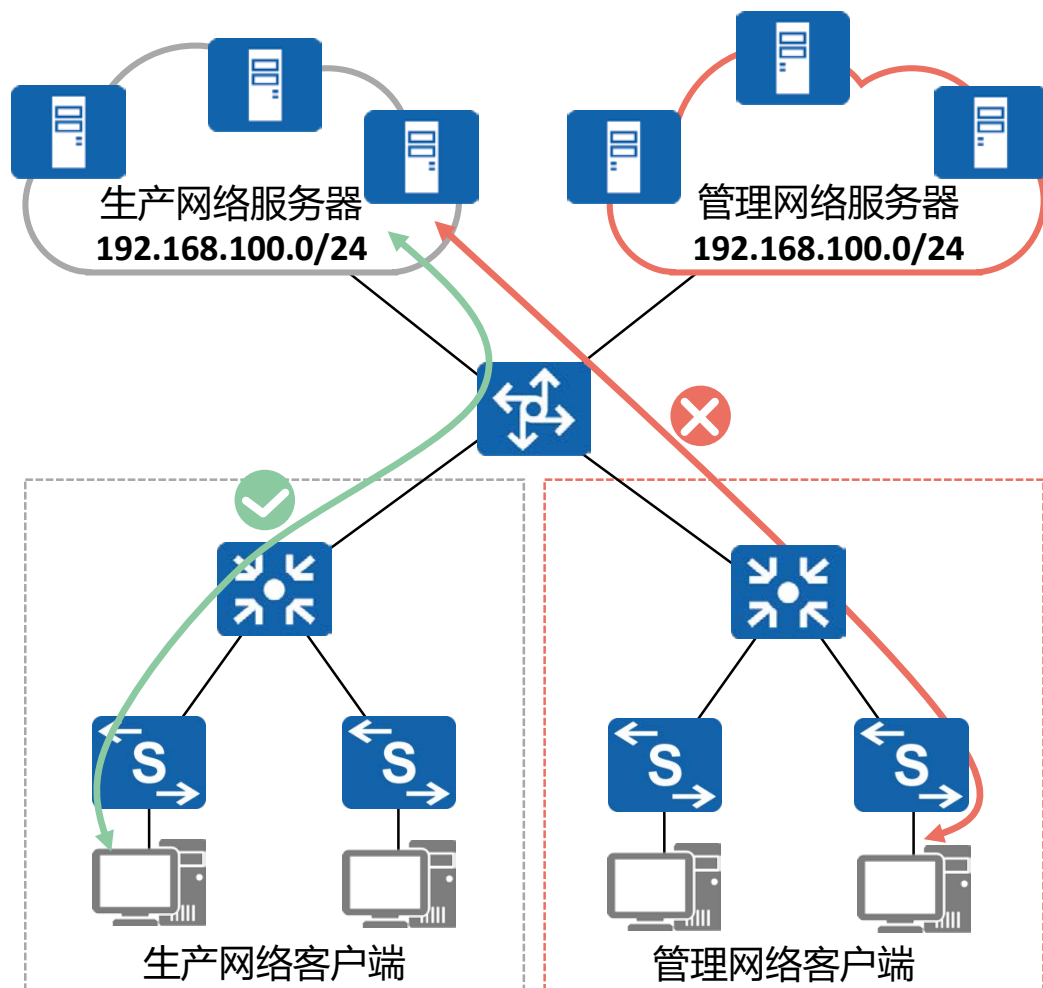


目录

1. VRF基本概念
2. VRF典型配置案例



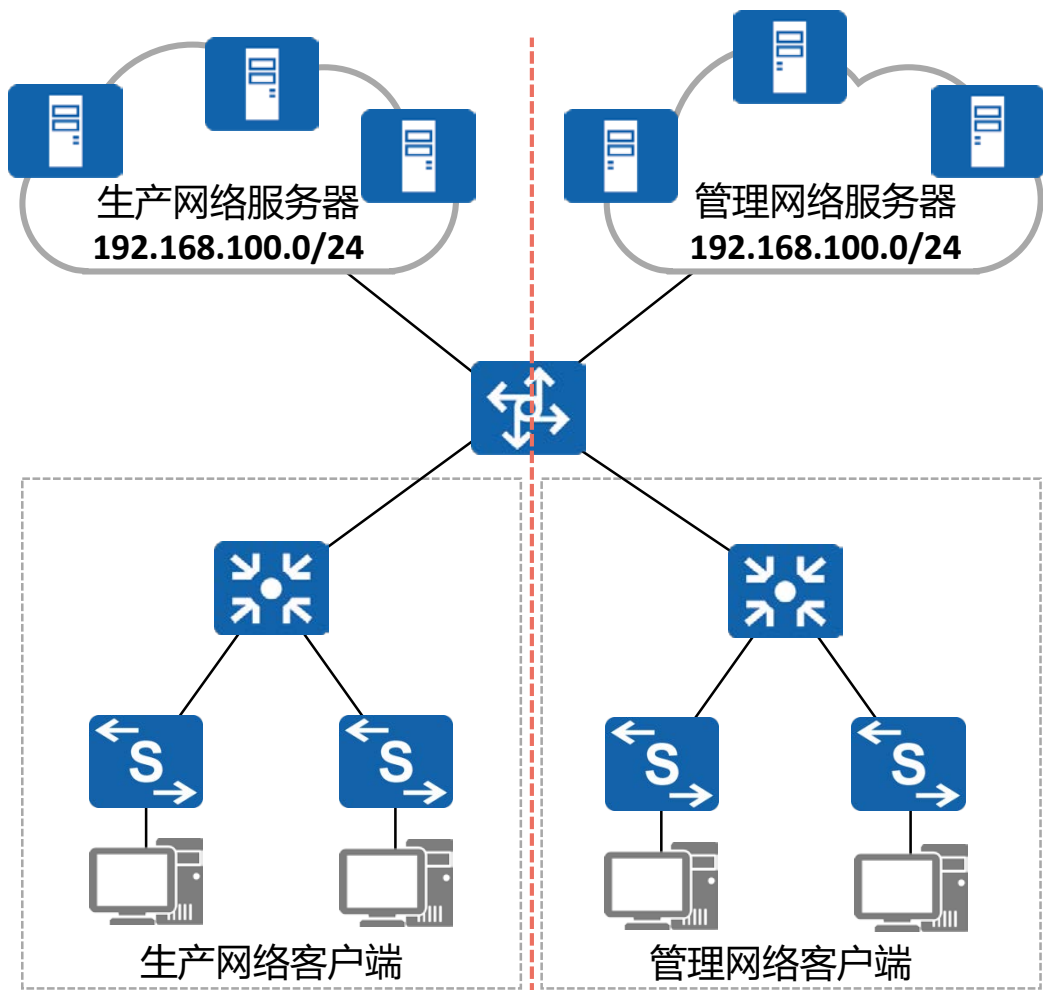
网络需求



- 某企业网络内有生产和管理两张网络，这两张网络独占接入和汇聚层交换机，共享核心交换机。
- 核心交换机上同时连接了生产网络和管理网络的服务器群，两个网段均为192.168.100.0/24网段。
- 需求：实现生产和管理网络内部的数据通信，同时隔离两张网络之间的通信。



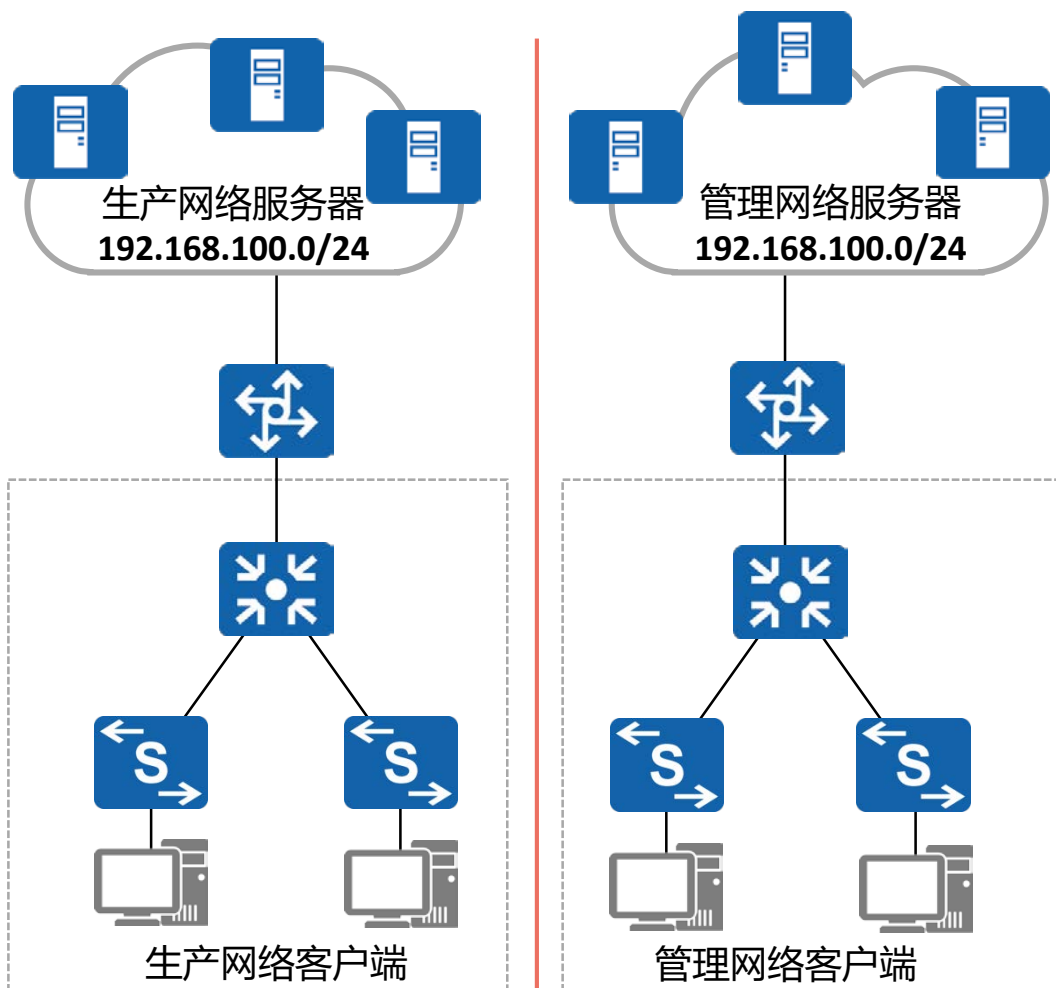
通过部署ACL实现



- 在核心交换机部署ACL，禁止生产和管理网络之间的互访流量。
- 缺陷：
 - 配置繁琐，拓展性差。
 - 无法解决两张网络使用重叠网段的问题，需要在部署时规避重叠网段。



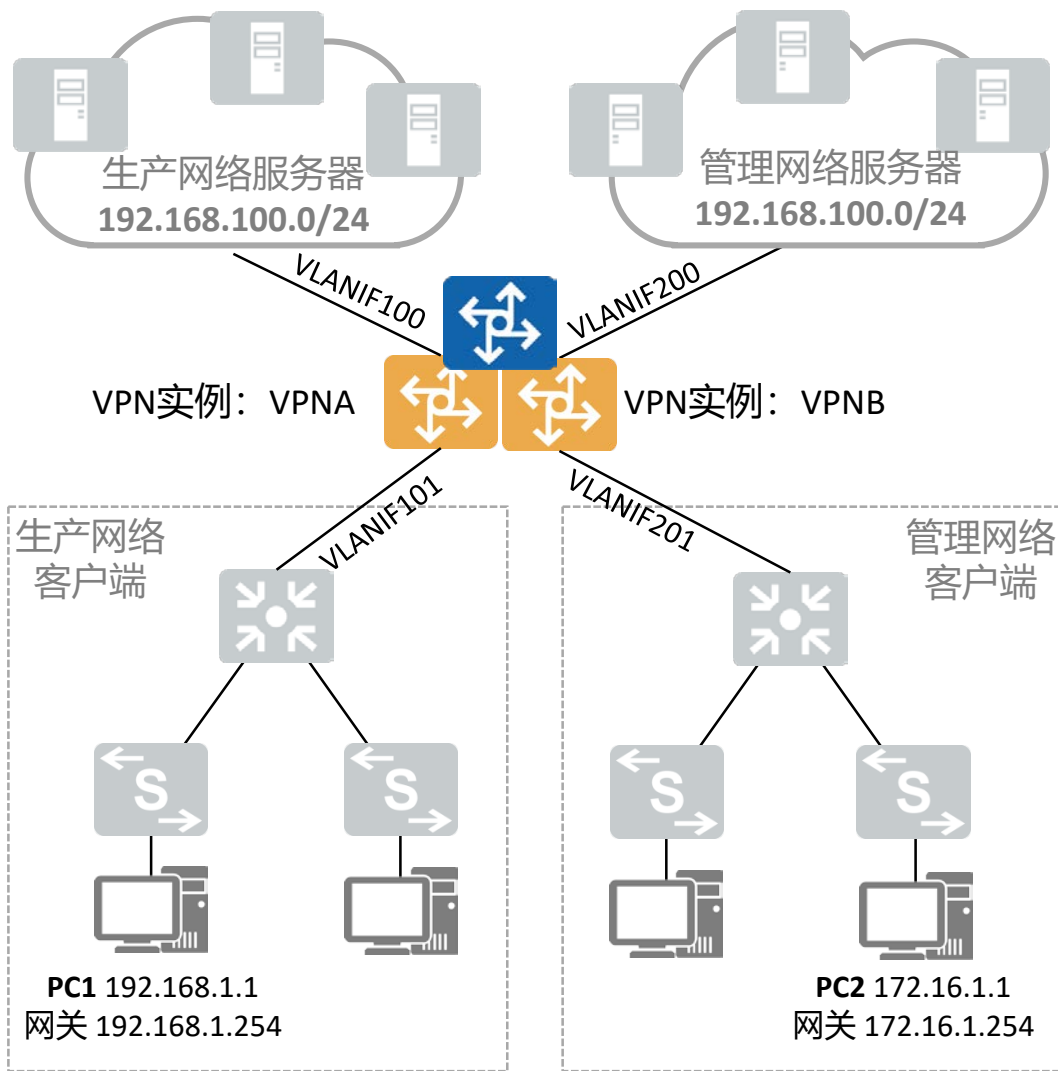
通过增加核心交换机实现



- 增加核心交换机，从物理上隔离两张网络。
- 缺陷：增加额外的设备成本投入。



通过VRF技术实现



- VRF又称VPN实例 (VPN Instance) , 是一种虚拟化技术。在物理设备上创建多个VPN实例, 每个VPN实例拥有**独立**的接口、路由表和路由协议进程等。

VPNA的路由表

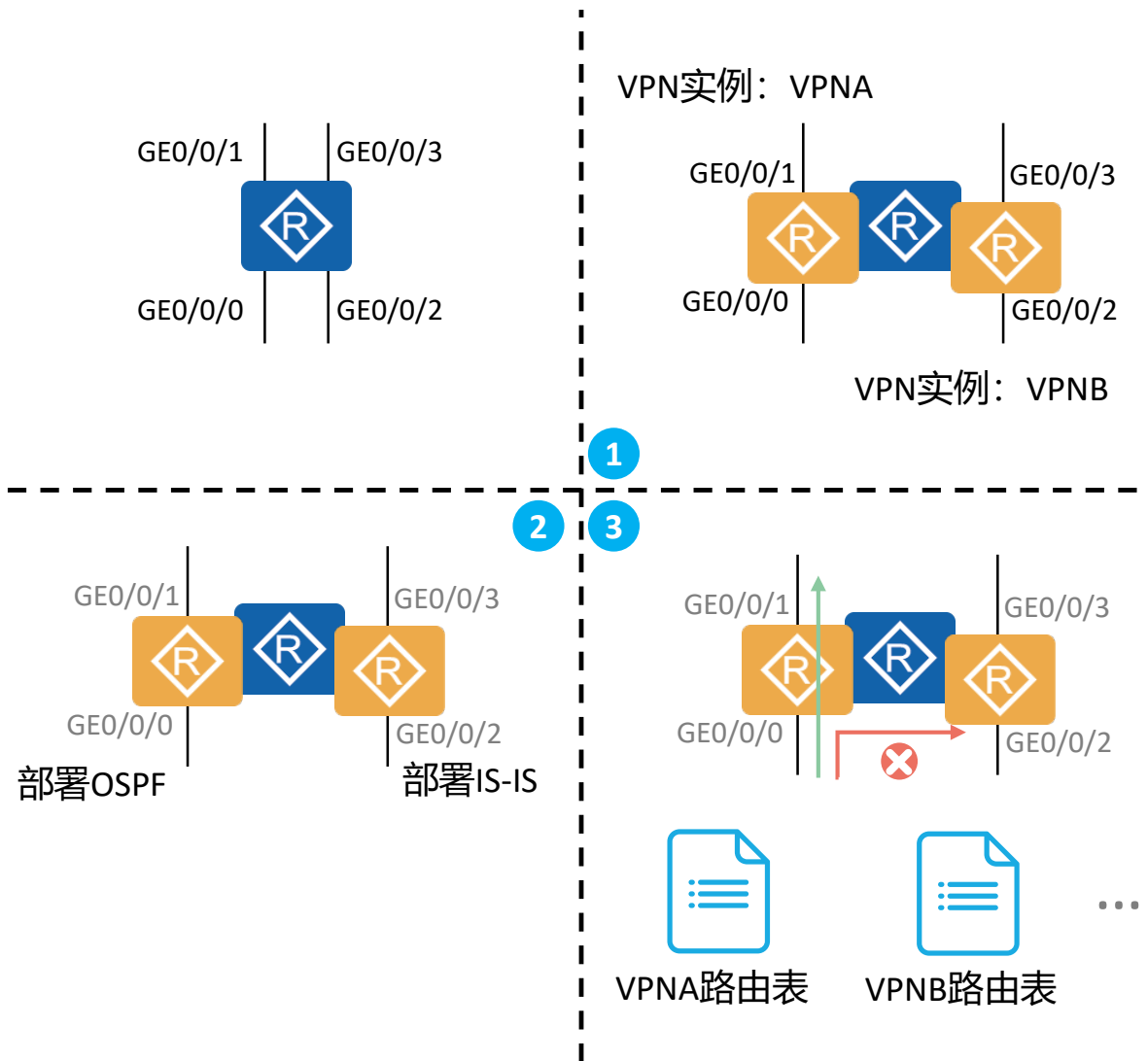
目的网段/掩码	协议	出接口	下一跳
192.168.100.0/24	OSPF	VLANIF100	192.168.100.1
192.168.1.0/24	OSPF	VLANIF101	192.168.101.1

VPNB的路由表

目的网段/掩码	协议	出接口	下一跳
192.168.100.0/24	OSPF	VLANIF200	192.168.100.1
172.16.1.0/24	Static	VLANIF201	192.168.201.1



VRF的实现过程



- VRF是对物理设备的一个逻辑划分，每个逻辑单元都被称为一个VPN实例，实例之间在路由层面是隔离的。VRF实现过程如下：

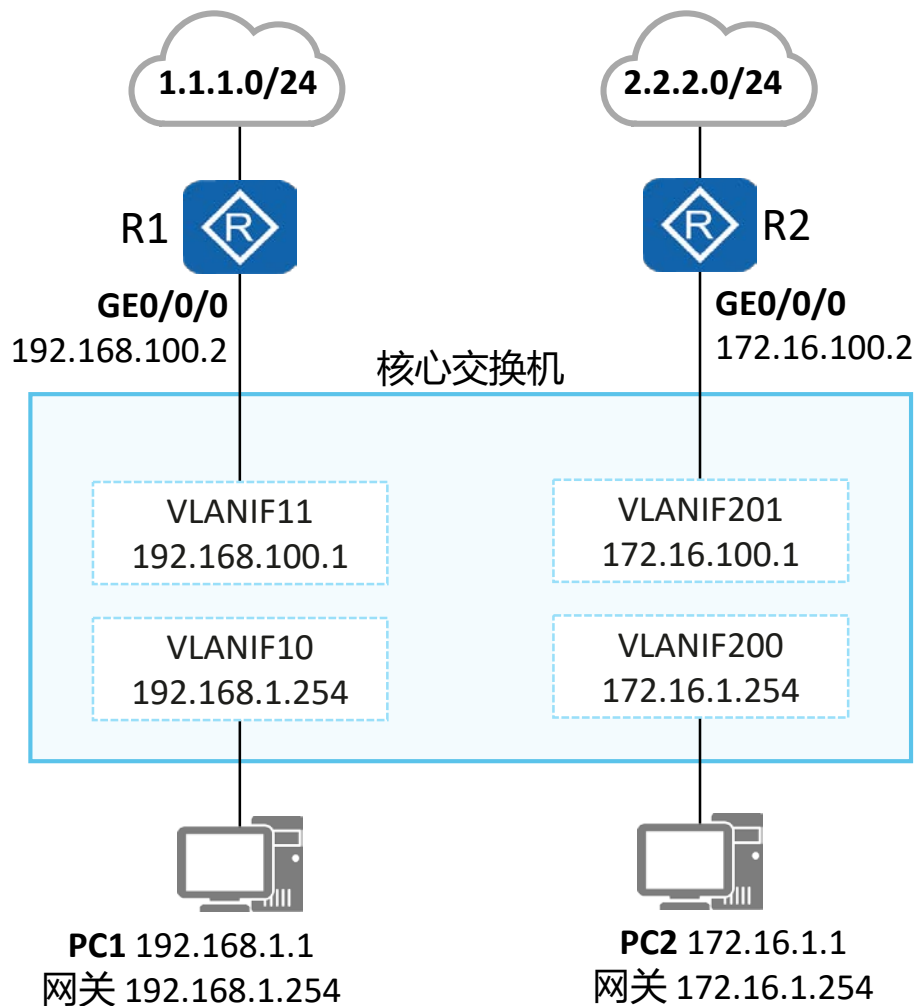
1. 创建实例，并将三层接口（可以是路由器的物理接口或者子接口，也可以是VLANIF接口）绑定到实例；
2. （可选）配置与实例绑定的路由协议或静态路由；
3. 基于与实例绑定的接口和路由协议等建立实例路由表并基于实例路由表转发数据，实现实例间隔离。

当前路由器上会有几张路由表呢？





举例：部署VRF前



核心交换机的路由表

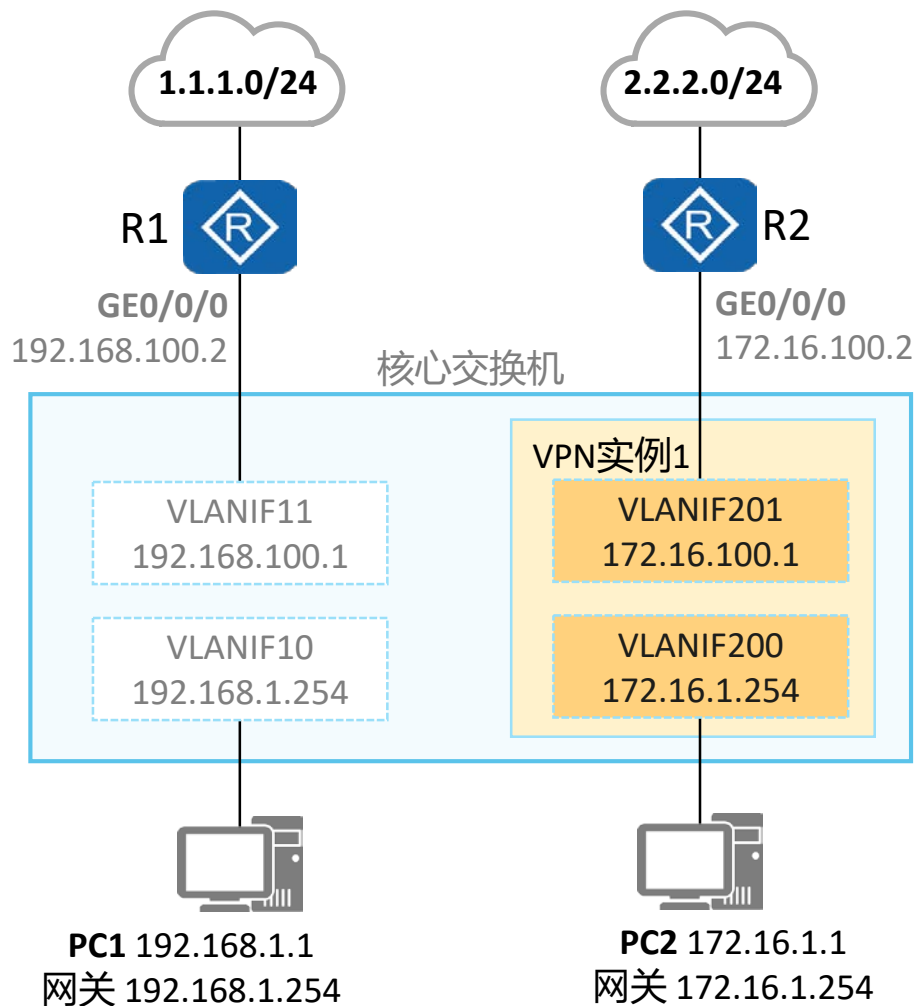
目的网络/掩码	协议	出接口	下一跳
192.168.1.0/24	Direct	VLANIF10	192.168.1.254
172.16.1.0/24	Direct	VLANIF200	172.16.1.254
192.168.100.0/24	Direct	VLANIF11	192.168.100.1
172.16.100.0/24	Direct	VLANIF201	172.16.100.1
1.1.1.0/24	Static	VLANIF11	192.168.100.2
2.2.2.0/24	Static	VLANIF201	172.16.100.2

背景： PC1、R1及R1所连的1.1.1.0/24网段属于业务网络。PC2、R2及R2所连的2.2.2.0/24网段属于管理网络。核心交换机上所有的直连路由，以及设备所发现的、到达远端网络的路由，均被存储在设备的路由表中（我们将该路由表称为全局路由表），业务及管理网络可以通过核心交换机实现互通。

需求： 通过配置实现业务与管理网络完全隔离。



举例：创建VPN实例



核心交换机的全局路由表
(根设备路由表)

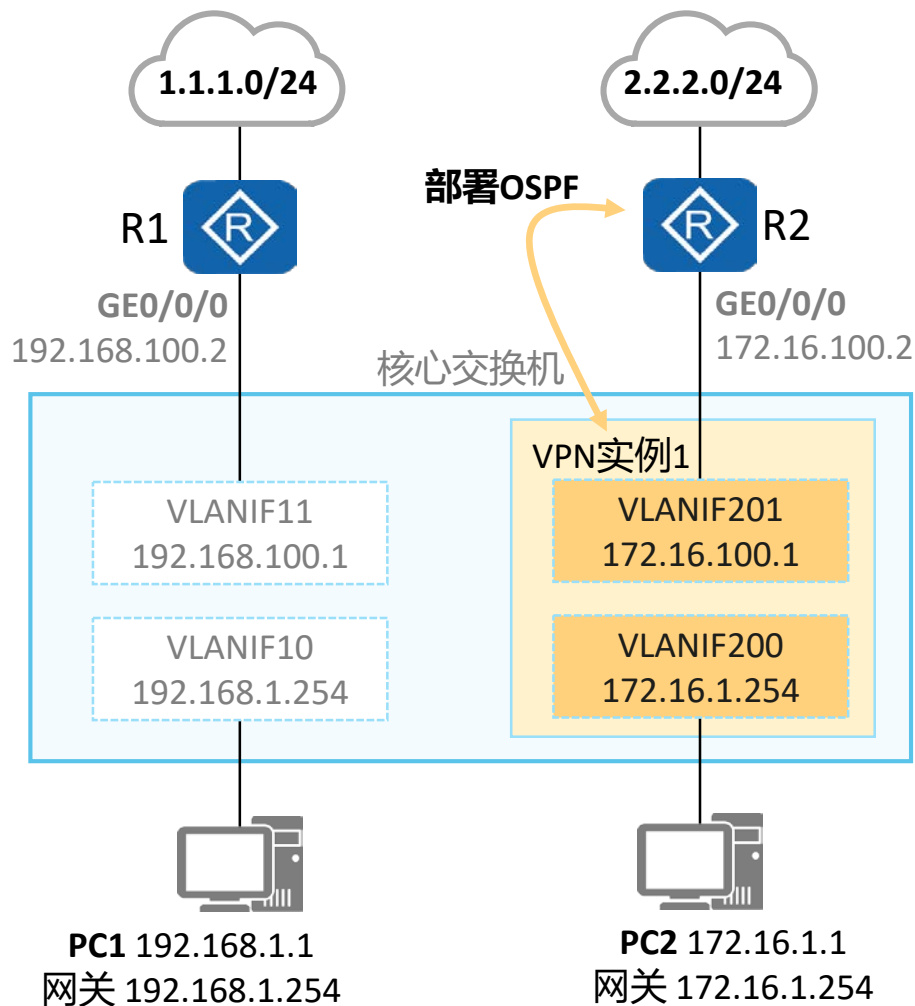
目的网络/掩码	协议	出接口	下一跳
192.168.1.0/24	Direct	VLANIF10	192.168.1.254
192.168.100.0/24	Direct	VLANIF11	192.168.100.1
1.1.1.0/24	Static	VLANIF11	192.168.100.2

核心交换机的VPN实例1路由表

目的网络/掩码	协议	出接口	下一跳
172.16.1.0/24	Direct	VLANIF200	172.16.1.254
172.16.100.0/24	Direct	VLANIF201	172.16.100.1



举例：部署动态路由协议



核心交换机的全局路由表
(根设备路由表)

目的网络/掩码	协议	出接口	下一跳
192.168.1.0/24	Direct	VLANIF10	192.168.1.254
192.168.100.0/24	Direct	VLANIF11	192.168.100.1
1.1.1.0/24	Static	VLANIF11	192.168.100.2

核心交换机的VPN实例1路由表

目的网络/掩码	协议	出接口	下一跳
172.16.1.0/24	Direct	VLANIF200	172.16.1.254
172.16.100.0/24	Direct	VLANIF201	172.16.100.1
2.2.2.0/24	OSPF	VLANIF201	172.16.100.2

在设备上可运行多种动态路由协议，或运行同一种动态路由协议的多个进程，关联到VPN实例的动态路由协议进程专为该实例服务，从该进程学习到的路由加载到VPN实例的路由表中。



常见应用场景

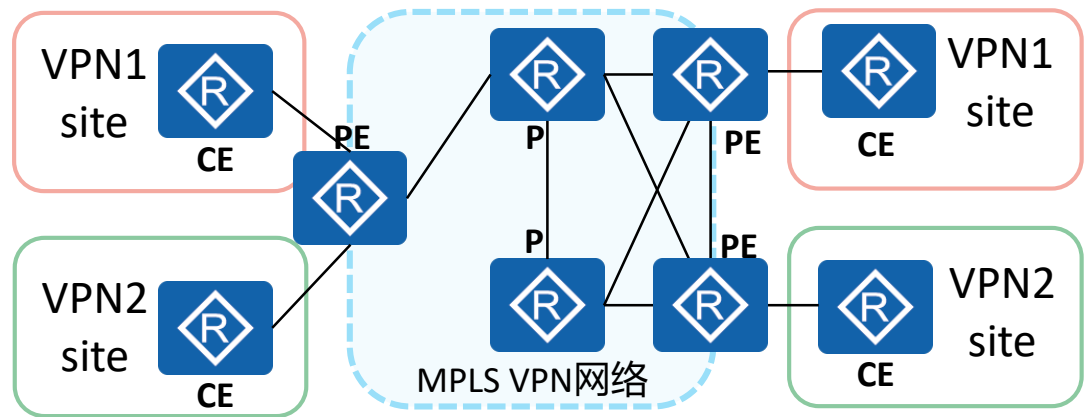
防火墙虚拟系统



虚拟系统（Virtual System）是在一台物理设备上划分出的多台相互独立的逻辑设备。虚拟系统主要具有以下特点：

- 资源虚拟化：每个虚拟系统都有独享的资源，包括接口、VLAN、策略和会话等。
- 路由虚拟化：每个虚拟系统都拥有各自的路由表，相互独立隔离。其中路由虚拟化依靠创建VPN实例来实现。

BGP/MPLS IP VPN



BGP/MPLS IP VPN是一种基于PE的L3VPN技术。它使用BGP在服务提供商骨干网上发布VPN路由，使用MPLS在服务提供商骨干网上转发VPN报文。

通过创建VPN实例的方式在PE上区别不同VPN的路由。



目录

1. VRF基本概念
- 2. VRF典型配置案例**



VRF基本配置命令 (1)

1. 创建VPN实例/进入VPN实例视图

```
[Huawei] ip vpn-instance vpn-instance-name
```

ip vpn-instance命令用来创建VPN实例，并进入VPN实例视图。缺省情况下，未配置VPN实例。

2. 使能VPN实例的IPv4类型的路由通告和数据转发功能

```
[Huawei-vpn-instance-InstanceName] ipv4-family
```

ipv4-family命令用来使能VPN实例的IPv4地址族，并进入VPN实例IPv4地址族视图。缺省情况下，未使能VPN实例的IPv4地址族。接口不能与未使能任何地址族的VPN实例绑定。

3. 将接口绑定到VPN实例

```
[Huawei-GigabitEthernet0/0/0] ip binding vpn-instance vpn-instance-name
```

ip binding vpn-instance命令用来将PE上的接口与VPN实例绑定。缺省情况下，接口不与任何VPN实例绑定，属于根实例。配置接口与VPN实例绑定后，或取消接口与VPN实例的绑定，都会清除该接口的IP地址、三层特性和IP相关的路由协议，如果需要应重新配置。



VRF基本配置命令 (2)

4. 向VPN实例的路由表中添加静态路由

```
[Huawei] ip route-static vpn-instance vpn-instance-name ip-address { mask | mask-length } { nexthop-address | interface-type interface-number }
```

5. 创建与VPN实例绑定的动态路由协议进程（以OSPF为例）

```
[Huawei] ospf [ process-id | router-id router-id ] vpn-instance vpn-instance-name
```

注：不同VPN实例之间的进程号不可重叠。

6. VPN实例维护命令

```
[Huawei] display ip routing-table vpn-instance vpn-instance-name
```

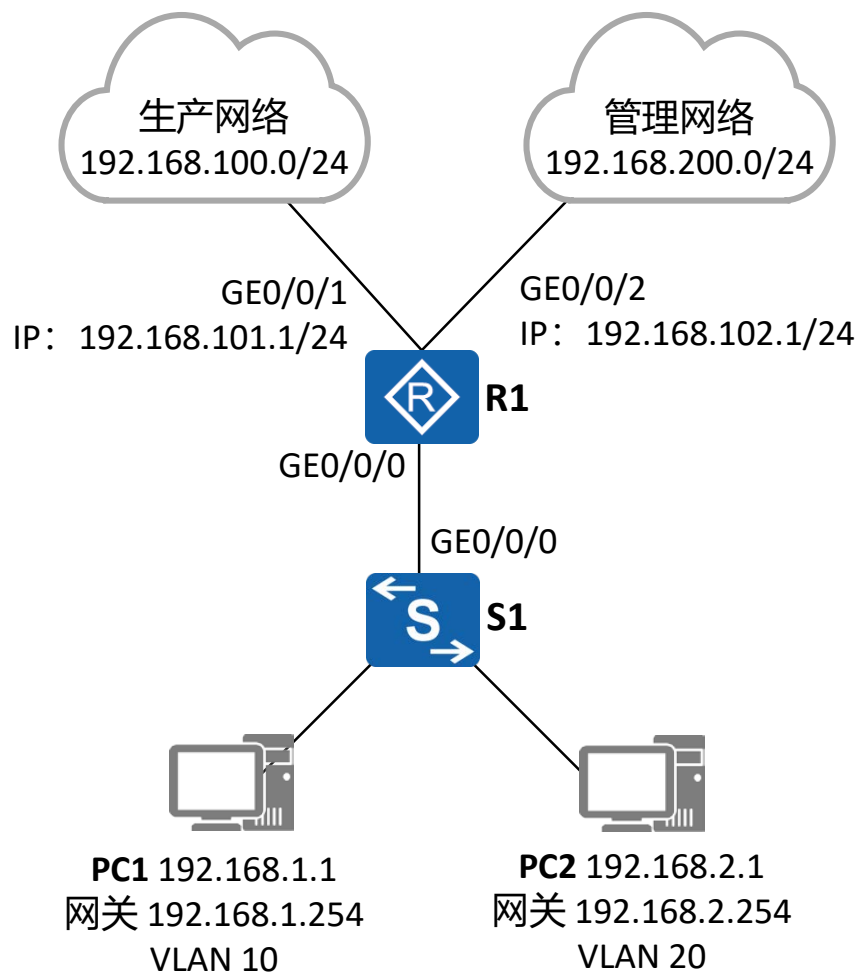
```
[Huawei] ping -vpn-instance vpn-instance-name host
```

```
[Huawei] tracert -vpn-instance vpn-instance-name host
```

注：如果执行ping时没有携带vpn-instance关键字及参数，则默认在根设备上执行ping操作，并且所产生的ICMP报文根据全局路由表进行转发。tracert操作同理。



配置案例 - 背景介绍与需求分析



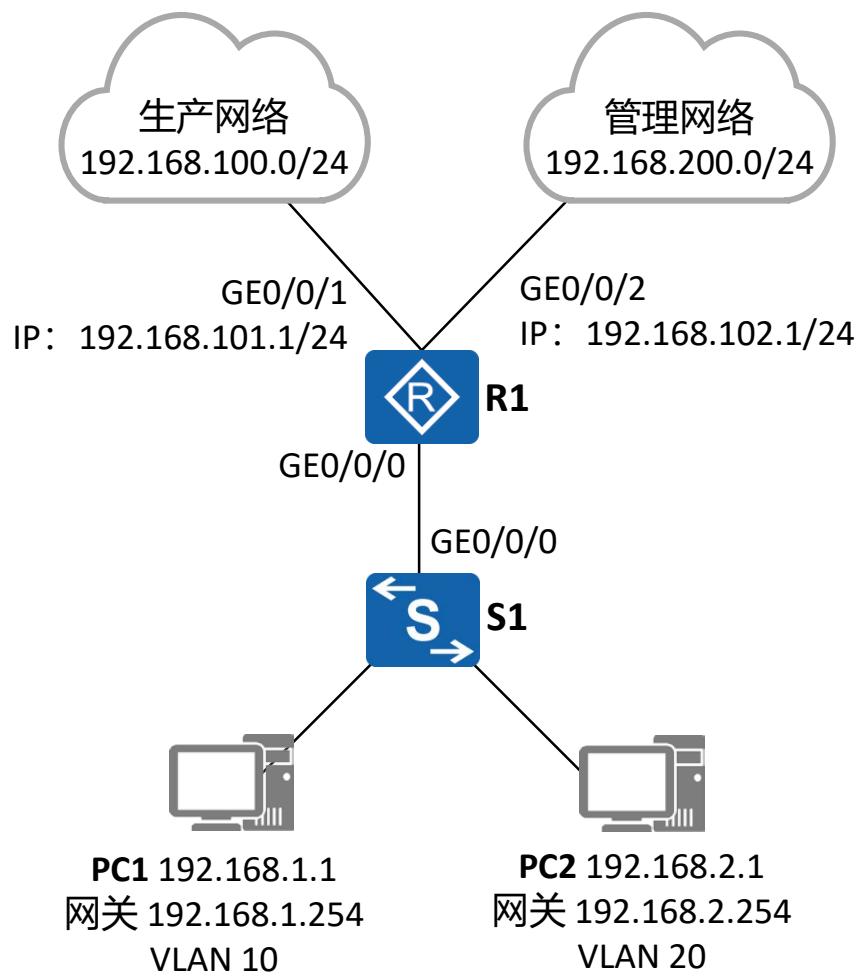
- **背景：**某企业内部有生产和管理两张网络，其拓扑简化如左图：
 - PC1属于生产网络，PC2属于管理网络，S1是这两台PC的接入交换机，将两台PC分别划入VLAN10和VLAN20。
 - R1上通过配置子接口作为PC1和PC2的网关。
- **需求：**将生产和管理网络隔离开来，并使用静态路由实现网络内部通信。

目的网络/掩码	协议	出接口	下一跳
192.168.100.0/24	Static	GE0/0/1	192.168.101.254
192.168.200.0/24	Static	GE0/0/2	192.168.102.254
192.168.1.0/24	Direct	GE0/0/0.1	192.168.1.254
192.168.2.0/24	Direct	GE0/0/0.1	192.168.2.254

R1未部署VRF前的路由表



配置案例 - 配置过程 (1)

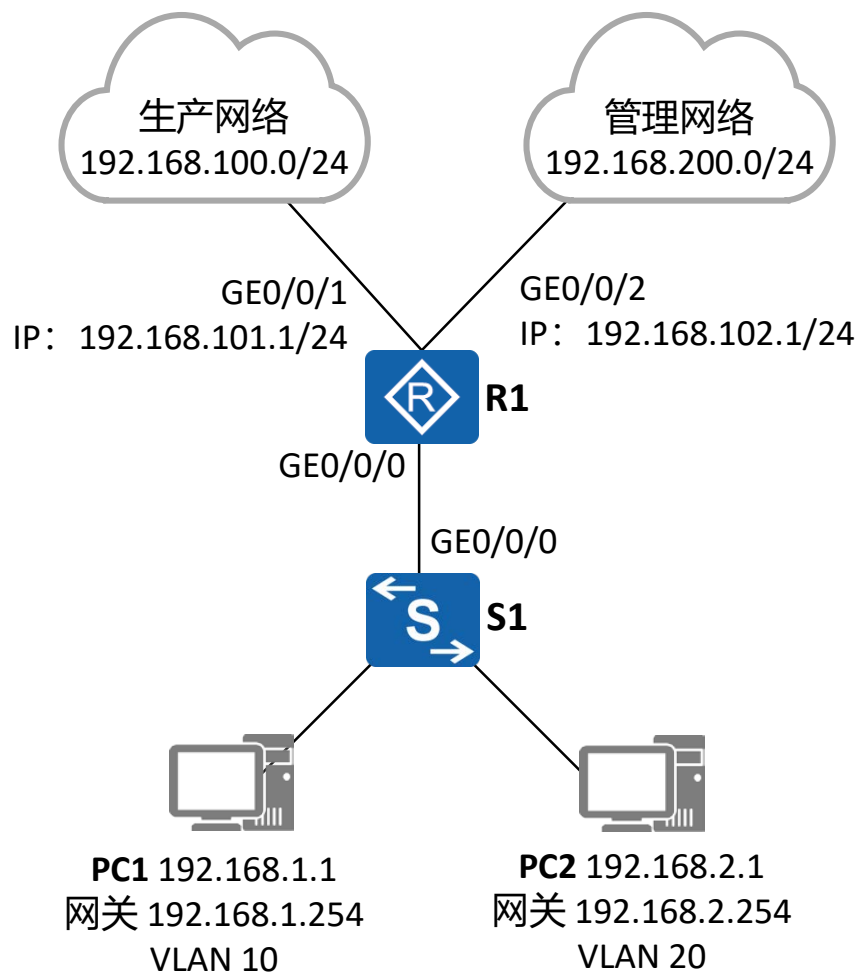


- 1、交换机上完成VLAN相关配置（略）
- 2、创建生产与管理网络的VPN实例，并使能IPv4地址族

```
[R1]ip vpn-instance production
[R1-vpn-instance-production]ipv4-family
[R1-vpn-instance-production-af-ipv4]quit
[R1-vpn-instance-production]quit
[R1]ip vpn-instance management
[R1-vpn-instance-management]ipv4-family
[R1-vpn-instance-management-af-ipv4]quit
[R1-vpn-instance-management]quit
```



配置案例 - 配置过程 (2)



3、将接口绑定到实例

```
[Huawei]interface GigabitEthernet 0/0/0.1
```

```
[Huawei-GigabitEthernet0/0/0.1]ip binding vpn-instance production
```

Info: All IPv4 related configurations on this interface are removed!

//接口绑定到实例后，接口下关于IP的配置将被清除，需要重新配置。

```
[Huawei-GigabitEthernet0/0/0.1]ip address 192.168.1.254 24
```

```
[Huawei-GigabitEthernet0/0/0.1]quit
```

```
[Huawei]interface GigabitEthernet 0/0/0.2
```

```
[Huawei-GigabitEthernet0/0/0.2]ip binding vpn-instance management
```

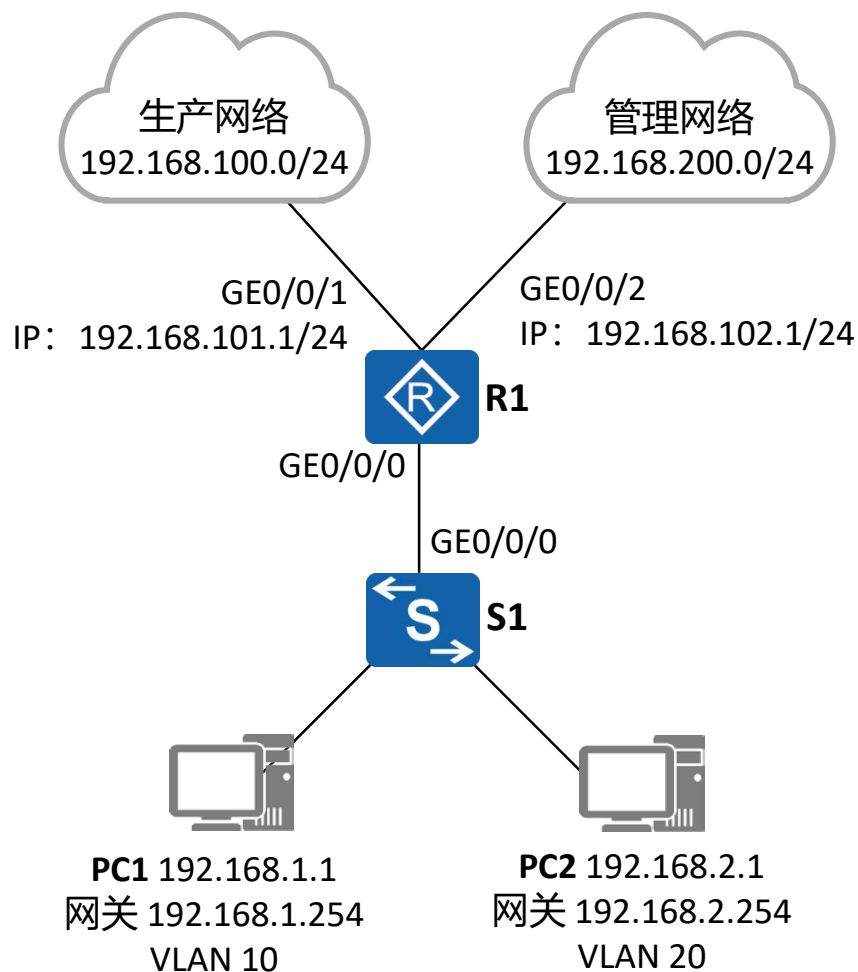
Info: All IPv4 related configurations on this interface are removed!

```
[Huawei-GigabitEthernet0/0/0.2]ip address 192.168.2.254 24
```

```
[Huawei-GigabitEthernet0/0/0.2]quit
```



配置案例 - 配置过程 (3)



4、往实例中添加静态路由

```
[R1]ip route-static vpn-instance production 192.168.100.0 24 192.168.101.254  
public  
[R1]ip route-static vpn-instance management 192.168.200.0 24  
192.168.102.254 public
```

5、检查配置

```
[R1] display ip routing-table vpn-instance production
```

Route Flags: R - relay, D - download to fib

Routing Tables: production

Destinations : 5 Routes : 5

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
192.168.100.0/24	Static	60	0	RD	192.168.101.254	GigabitEthernet0/0/1



思考题

1. （单选题）VRF技术可以实现（ ）的隔离。
 - A. 物理层
 - B. 网络层
 - C. 数据链路层
 - D. 应用层
2. （判断题）缺省情况下，华为数通产品上所有三层接口都属于根实例。
 - A. 正确
 - B. 错误



本章总结

- VRF技术实现了同一物理设备上不同网络之间的逻辑隔离，当在物理设备上部署多个VRF实例时，每一个VRF实例就相当于一个虚拟的网络设备。VRF实例之间的接口和路由天然隔离，当同一个物理设备连接到多个相同的网段时，也不用担心IP地址冲突的问题。
- VRF技术广泛应用于防火墙虚拟系统、BGP/MPLS IP VPN等多个场景中。

The background of the slide features a blue-tinted image of several business professionals in a modern office environment. They are standing on a highly reflective floor, and their silhouettes are clearly visible. The overall aesthetic is professional and corporate.

谢谢

www.huawei.com