

HCIE-Security 备考指南

DSVPN



HCIE 只是一个开始....

HCIE 仅是一个证书...懂得做人和处事比证书和技能更重要...

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security DSVPN 需要掌握的知识点.....	1
DSVPN 简介.....	1
DSVPN 基本概念和原理.....	3
建立 Spoke 与 Hub 之间的 MGRE 隧道.....	5
建立 Spoke 与 Spoke 之间的 MGRE 隧道（Normal 方式）.....	6
建立 Spoke 与 Spoke 之间的 MGRE 隧道（Shortcut 方式）.....	8
应用场景——基本场景.....	10
应用场景——Hub 主备份场景.....	11
应用场景——Hub 负载分担场景.....	12
应用场景——级联场景.....	13
使用限制及注意事项.....	14
配置分支.....	14
配置总部.....	19
配置级联总部.....	21
监控.....	23
配置隧道参数.....	24
配置路由参数.....	27
（可选）配置 IPSec 安全框架.....	30
维护 DSVPN.....	32
举例：配置 DSVPN 基本场景.....	33
故障处理——Spoke 与 Hub 建立静态 MGRE 隧道失败.....	42
现象描述.....	42
可能原因.....	42
处理步骤.....	42
故障处理——Spoke 与 Spoke 间建立动态 MGRE 隧道失败.....	42
现象描述.....	42
可能原因.....	42
处理步骤.....	42
HCIE-Security 模拟面试问题及面试建议.....	43

HCIE-Security DSVPN 需要掌握的知识点

- 掌握 DSVPN 各组成协议的原理；
- 理解 MGRE 的原理和作用；
- 掌握 NHRP 协议的协商过程；
- 掌握 DSVPN 的各种配置细节。

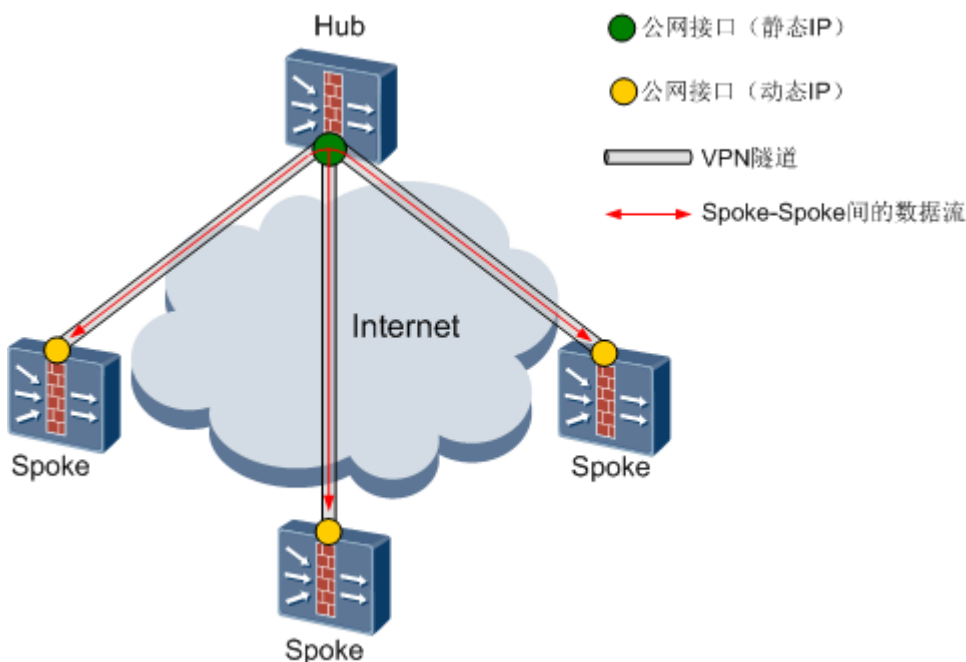
DSVPN 简介

介绍 DSVPN 技术的产生背景和基本概念。

越来越多的企业希望建立 VPN 网络将企业总部机构（Hub）与地理位置不同的多个分支机构（Spoke）相连，从而加强企业的通信安全，降低通信成本。当企业总部机构采用静态的公网地址接入 Internet，分支机构采用动态的公网地址接入 Internet 时，使用传统的 IPSec、GRE over IPSec 等技术构建 VPN 网络将存在一个问题，即分支与分支间无法直接通信，所有分支与分支间的通信数据只能由总部中转，如图 1 所示。

通过总部中转流量的办法来解决分支与分支间的通信问题只能是一个临时方案，并不能从根本上解决问题。这是因为，总部在中转分支间的通信流量时会消耗 Hub 的 CPU 及内存资源，造成资源紧张；另外，总部要对分支间的流量进行封装和解封装，会引入额外的网络延时。因此，如何在公网地址动态变化的分支之间建立 VPN 隧道，使分支与分支直接通信，进而减轻总部的通信负担成为了 VPN 技术中一个亟待解决的问题。

图 1 Hub-Spoke 组网方式下的 VPN 网络



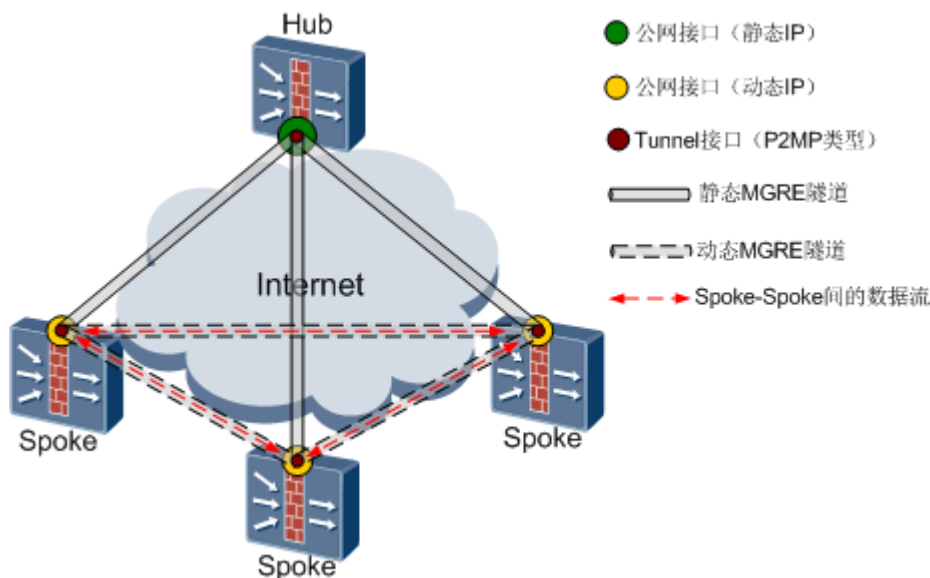
DSVPN (Dynamic Smart Virtual Private Network)，即动态智能 VPN，是一种在 Hub-Spoke 组网方式下，为公网地址动态变化的分支之间建立 VPN 隧道的解决方案。

DSVPN 通过 NHRP (Next Hop Resolution Protocol，下一跳地址解析协议) 协议动态收集、维护和发布分支节点的公网地址信息，解决了源分支无法获取目的分支公网地址的问题，从而在分支与分支之间建立 VPN 隧道。分支之间建立 VPN 隧道以后，分支之间的业务流量将不再经过总部 (Hub) 中转，从而减轻了总部的负担，也避免了网络延时。

为了在 VPN 隧道中能够传送组播报文 (如动态路由协议报文)，DSVPN 在网络节点之间采用 GRE 协议建立 VPN 隧道。但 DSVPN 对 GRE 隧道做了改进，它将传统 GRE 隧道点到点 (P2P) 类型的 Tunnel 接口扩展成了点到多点 (P2MP) 类型的 Tunnel 接口。通过改变接口类型，VPN 网关 (Hub 或 Spoke) 上只需要配置一个 Tunnel 接口便可与多个对端建立隧道，从而减少了配置 GRE 隧道的工作量。采用点到多点方式建立起来的 GRE 隧道被称为 MGRE (Multipoint Generic Routing Encapsulation) 隧道。另外，总部与分支建立 MGRE 隧道以后，新增分支或分支公网地址发生变化时，总部可以自动维护与分支机构之间的隧道关系，而不用调整总部的隧道配置，使得网络维护变得更智能化。

图 2 所示是一个采用 DSVPN 技术构建的 VPN 网络。在该网络中，当源 Spoke (隧道发起方) 需要向目的 Spoke (隧道响应方) 发送流量时，源 Spoke 将通过 NHRP 协议获取目的 Spoke 的公网地址，并与目的 Spoke 建立动态 MGRE 隧道。隧道建立完成后，Spoke 与 Spoke 之间的流量将通过新建的动态 MGRE 隧道直接发送给对方。并且网络节点间使用 MGRE 隧道以后，每个 VPN 网关上只需配置一个 Tunnel 接口 (P2MP 类型) 即可以与多个对端建立隧道，从而减少了配置隧道的工作量。

图 2 Hub-Spoke 组网方式下的 DSVPN 网络



DSVPN 基本概念和原理

介绍 DSVPN 的基本概念和原理。

NHRP 协议

NHRP (Next Hop Resolution Protocol) 即下一跳地址解析协议。在 DSVPN 中网络中, Spoke 利用 NHRP 协议获取对端 Spoke 的公网地址。其基本原理是源 Spoke (隧道发起方) 以到目的 Spoke (隧道响应方) 路由的下一跳地址为索引, 向目的 Spoke 发送 NHRP 地址解析请求, 目的 Spoke 收到该地址请求后将向源 Spoke 返回其公网地址。源 Spoke 获取到目的 Spoke 的公网地址后, 两者之间将建立动态的 MGRE 隧道。

NHRP 映射表

NHRP 映射表是有关 Tunnel 地址和公网地址的映射关系表。NHRP 映射表中的表项按照生成方式的不同, 分为静态表项和动态表项两种。

- 静态表项

静态表项是由网络管理员手工配置。例如, Spoke 需要与 Hub 建立 MGRE 隧道, 管理员就需要在 Spoke 上手工配置 Hub 的 Tunnel 地址和公网地址。

- 动态表项

动态表项是根据 NHRP 协议解析到对端地址, 然后自动更新到 NHRP 映射表中的表项。源 Spoke 获取到目的 Spoke 的公网地址后, 会把目的 Spoke 的 Tunnel 地址和公网地址存放到自己的 NHRP 映射表中。

DSVPN 的工作原理

DSVPN 建立 Spoke 与 Spoke 之间 MGRE 隧道的基本原理是: 所有 Spoke 都向 Hub 注册自己的 Tunnel 地址和公网地址, 并与 Hub 建立 MGRE 隧道。当 Spoke 与 Spoke 需要建立动态 MGRE 隧道时, 源 Spoke (隧道发起方) 将 NHRP 地址解析请求通过其与 Hub 间的隧道发送给 Hub, 然后 Hub 再将该地址解析请求通过 Hub 与目的 Spoke (隧道响应方) 间的 MGRE 隧道发送到目的 Spoke, 目的 Spoke 收到该地址解析请求后会将自己的公网地址告知源 Spoke, 并建立源 Spoke 与目的 Spoke 之间的动态 MGRE 隧道。因此, 可以将 DSVPN 建立 MGRE 隧道的过程分为以下两个阶段。

1. 建立 Spoke 与 Hub 之间的 MGRE 隧道。

Spoke 主动向 Hub 发送注册消息，告知 Hub 自己的公网地址。Hub 获取 Spoke 的公网地址后，刷新自己的 NHRP 映射表，从而与 Spoke 建立 MGRE 隧道。具体隧道建立过程请参见[建立 Spoke 与 Hub 之间的 MGRE 隧道](#)。

Spoke 与 Hub 之间的 MGRE 隧道建立完成后，Spoke 之间将按照 DSVPN 网络中部署的路由方案进行路由学习。DSVPN 网络支持两种路由部署方案：

- 分支节点相互学习路由

采用分支节点相互学习路由的方案时，Spoke 需要学习到所有对端的路由数据。这种情况下，Spoke 会消耗大量的 CPU 和内存资源，因而对其路由表容量和性能有较高的要求。而实际应用中，Spoke 的性能往往较低，能存放的路由数量有限。所以，该路由部署方案只适用于网络节点较少，路由信息量小的场景。

- 分支节点路由汇聚到总部

采用路由汇聚方案时，Spoke 只需存放到 Hub 路由。由于 Spoke 减少了自身的路由数量，所以适用于那些网络规模大，分支节点较多的场景。

DSVPN 在 Spoke 与 Hub 之间建立的 MGRE 隧道是一种静态隧道，无论 Spoke 与 Hub 间是否有流量经过，该隧道一直存在。

2. 建立 Spoke 与 Spoke 之间的 MGRE 隧道。

Spoke 与 Hub 之间的 MGRE 隧道建立完成后，Spoke 与 Spoke 之间将通过该隧道，发送 NHRP 地址解析请求给对方，获取对端的公网地址，并生成 NHRP 映射表。

两种不同的路由部署方案下，Spoke 学习到的路由信息也不同。于是，Spoke 与 Spoke 之间建立 MGRE 隧道的方式也按照路由部署方案的不同，分为了如下两种方式。

- Normal 方式

当 DSVPN 采用分支节点相互学习路由方案时，源 Spoke 可以学习到目的 Spoke 的 Tunnel 地址（在该路由部署方案下，目的 Spoke 的 Tunnel 地址等同于源 Spoke 到目的 Spoke 路由的下一跳地址），因此源 Spoke 将以目的 Spoke 的 Tunnel 地址为索引，查找其公网地址。具体隧道建立过程请参见[建立 Spoke 与 Spoke 之间的 MGRE 隧道（Normal 方式）](#)。

- Shortcut 方式

当 DSVPN 采用分支节点路由汇聚到总部时，所有 Spoke 的路由下一跳全部都是 Hub 的 Tunnel 地址。源 Spoke 无法学习到目的 Spoke 的 Tunnel 地址，因此，源 Spoke 只能以目的 Spoke 的私网网段查找其公网地址。具体隧道建立过程请参见[建立 Spoke 与 Spoke 之间的 MGRE 隧道（Shortcut 方式）](#)。

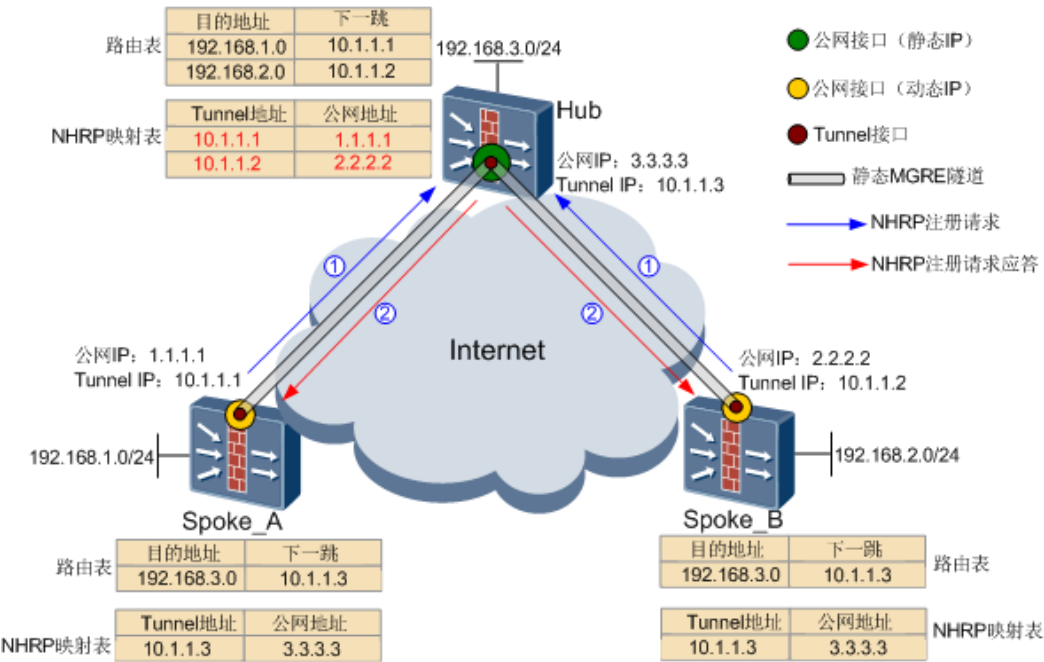
Spoke 与 Spoke 之间建立的 MGRE 隧道是一种动态隧道，当 Spoke 与 Spoke 间有流量通过时，隧道被自动创建；当一定周期内没有流量经过时，隧道将自动拆除。

建立 Spoke 与 Hub 之间的 MGRE 隧道

介绍 DSVPN 建立 Spoke 与 Hub 之间 MGRE 隧道的原理。

图 1 所示是 DSVPN 建立 Spoke 与 Hub 之间 MGRE 隧道的过程。

图 1 DSVPN 建立 Spoke 与 Hub 之间 MGRE 隧道的过程



Spoke 和 Hub 间建立 MGRE 隧道的过程如下：

1. Spoke 向 Hub 注册。

管理员在 Spoke 上手工配置 Hub 的 Tunnel 地址和公网地址以后，Spoke 将向 Hub 发送注册消息，注册消息中包含了 Spoke 节点的 Tunnel 地址和公网地址信息。

2. Hub 向 Spoke 返回注册应答消息。

Hub 从注册请求中提取 Spoke 的 Tunnel 地址和公网地址（见 Hub 的 NHRP 映射表中红色字体），并生成 NHRP 映射表，从而建立两者之间的 MGRE 隧道。

Spoke 与 Hub 之间建立 MGRE 隧道以后，Spoke 将按照网络中部署的路由方案学习路由。

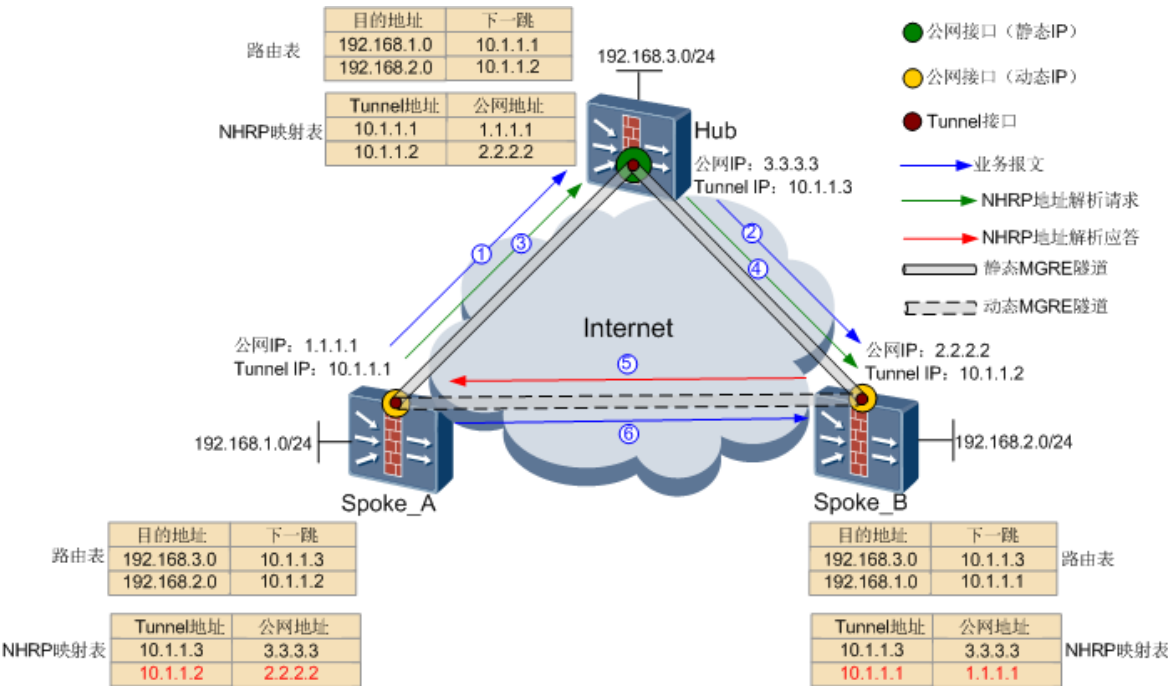
Hub 生成 Spoke 的动态 NHRP 映射表以后，该表项存在一段时间以后会老化。由于 Spoke 和 Hub 间的静态隧道需要永久存在，因此 Spoke 就需要定时向 Hub 发送注册消息，使 Hub 的 NHRP 映射表在老化时间到来前重新计时，确保分支与总部一直能够维持隧道关系。如果 Spoke 的公网地址发生变化，Spoke 会重新向总部注册。

建立 Spoke 与 Spoke 之间的 MGRE 隧道（Normal 方式）

当 DSVPN 网络中的路由部署方式为分支节点相互学习路由时，Spoke 与 Spoke 之间将采用 Normal 方式建立 MGRE 隧道。

图 1 所示是 DSVPN 采用 Normal 方式建立 Spoke 与 Spoke 之间 MGRE 隧道的工作原理。

图 1 Normal 方式建立 Spoke 与 Spoke 之间的 MGRE 隧道



路由学习完成后，Spoke_A 到 Spoke_B 的路由下一跳就是 Spoke_B 的 Tunnel 地址。Spoke_A 在与 Spoke_B 建立动态 MGRE 隧道时，将会按照 Spoke_B 的 Tunnel 地址来查找 Spoke_B 的公网地址。

当 Spoke_A 下的用户需要访问 Spoke_B 下的用户时，将触发 Spoke_A 与 Spoke_B 之间建立动态的 MGRE 隧道，隧道建立过程如下：

1. Spoke_A 将其下用户发送给 Spoke_B 的业务报文通过 Spoke_A 与 Hub 间的 MGRE 隧道发送给 Hub。

Spoke_A 收到其下用户的业务报文时，将按照路由表找到下一跳 10.1.1.2。然后再根据下一跳 10.1.1.2 来查找 NHRP 映射表。由于此时 Spoke_A 的 NHRP 映射表中还不存在 Spoke_B 的公网地址，因此 Spoke_A 会默认将该报文直接转发给 Hub。另外，Spoke_A 在 NHRP 映射表查找不到 Spoke_B 的公网时，将触发 NHRP 地址解析请求。

2. Hub 收到 Spoke_A 的业务报文以后，将此报文通过 Hub 与 Spoke_B 间的 MGRE 隧道转发给 Spoke_B。
3. Spoke_A 向 Hub 发送 NHRP 地址解析请求。

解析请求中包含了 Spoke_A 的 Tunnel 地址 10.1.1.1 和公网地址 1.1.1.1，还有需要解析的 Spoke_B 的 Tunnel 地址 10.1.1.2。

4. Hub 收到 Spoke_A 的地址解析请求后转发给 Spoke_B 处理。
5. Spoke_B 收到地址解析请求后，向 Spoke_A 返回应答消息。

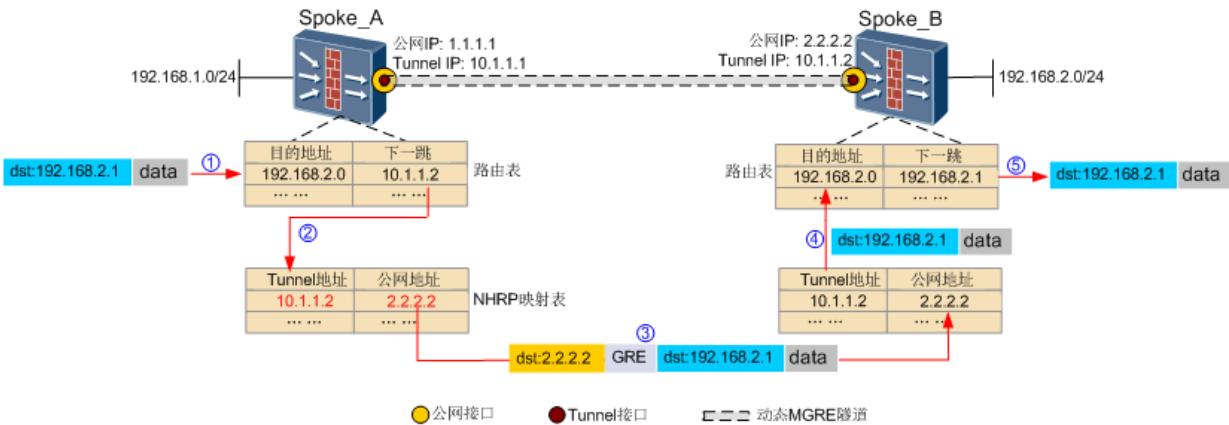
Spoke_B 首先从 NHRP 地址解析请求中提取 Spoke_A 的 Tunnel 地址和公网地址，并将该信息更新到自己的 NHRP 映射表中（见 Spoke_B 的 NHRP 映射表中红色字体）。同时，Spoke_B 生成 NHRP 地址解析应答消息返回给 Spoke_A，应答消息中包含 Spoke_B 的 Tunnel 地址 10.1.1.2 和公网地址 2.2.2.2。

6. Spoke_A 收到 Spoke_B 的 NHRP 地址解析应答报文后与 Spoke_B 建立动态 MGRE 隧道。

Spoke_A 收到 Spoke_B 的应答报文后，将从应答消息中提取 Spoke_B 的 Tunnel 地址 10.1.1.2 和公网地址 2.2.2.2，更新到自己的 NHRP 映射表（见 Spoke_A 的 NHRP 映射表中红色字体）。

Spoke_A 与 Spoke_B 的 MGRE 隧道建立好以后，当 Spoke_A 再次收到其下用户发送给 Spoke_B 的业务报文时，Spoke_A 将会通过新建的动态 MGRE 隧道传送此报文到 Spoke_B。下面以 Spoke_A 单向发送数据给 Spoke_B 为例，介绍动态 MGRE 隧道的封装过程。Spoke_B 返回给 Spoke_A 的反向报文封装过程同理。

图 2 MGRE 隧道报文封装过程



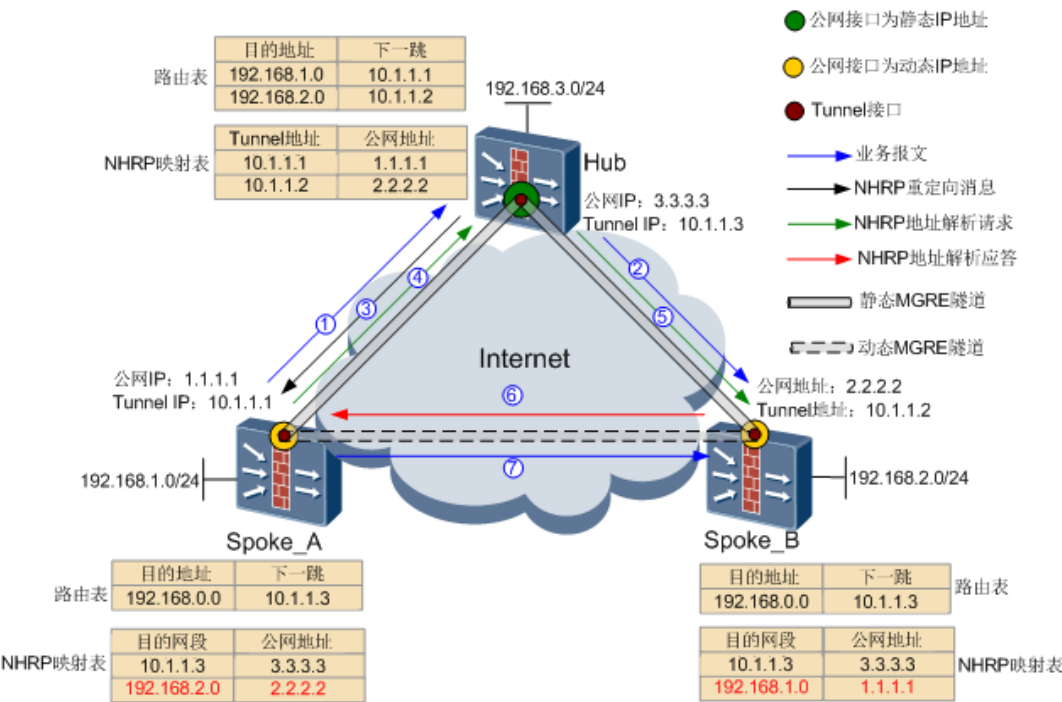
- a. Spoke_A 再次收到发往 Spoke_B 的业务报文以后，将按报文的目的地址 192.168.2.1 查找路由表找到去 Spoke_B 的路由下一跳 10.1.1.2。
- b. Spoke_A 以下一跳地址 10.1.1.2 为索引查找 NHRP 映射表，找到对端 Spoke_B 的公网地址 2.2.2.2。
- c. Spoke_A 以 GRE 协议作为报文头进行报文封装，封装后的目的地址为 2.2.2.2。
- d. Spoke_B 收到 Spoke_A 发送的封装报文后，按照 2.2.2.2 查找对应的 Tunnel 接口，并通过对应的 Tunnel 接口对报文解封装。
- e. 解封装后的报文将按照 Spoke_B 的路由表进行转发，发送给其下的用户。

建立 Spoke 与 Spoke 之间的 MGRE 隧道（Shortcut 方式）

当 DSVPN 网络中的路由部署方式为分支节点路由汇聚到总部时，Spoke 与 Spoke 之间将采用 Shortcut 方式建立 MGRE 隧道。

图 1 所示是 DSVPN 采用 Shortcut 方式建立 Spoke 与 Spoke 之间 MGRE 隧道的工作原理。

图 1 Shortcut 方式建立 Spoke 与 Spoke 之间的 MGRE 隧道



路由学习完成后，所有 Spoke 只有到 Hub 的路由。Spoke 只能通过业务报文要发送的目的地址来查找对端 Spoke 的公网地址。

当 Spoke_A 下的用户需要访问 Spoke_B 下的用户时，将触发 Spoke_A 与 Spoke_B 之间建立动态的 MGRE 隧道，隧道建立过程如下：

1. Spoke_A 将其下用户发送给 Spoke_B 的业务报文通过 Spoke_A 与 Hub 间的 MGRE 隧道发送给 Hub。

Spoke_A 收到其下用户的业务报文时，先根据报文的地址 192.168.2.0 查找 NHRP 映射表。此时，Spoke_A 的 NHRP 映射表中还不存在 Spoke_B 的公网地址。当 Spoke_A 通过目的地址 192.168.2.0 找不到 Spoke_B 的公网地址以后，Spoke_A 会再根据路由对应的下一跳 10.1.1.3 查找 NHRP 映射表。发现 10.1.1.3 在 NHRP 映射表中有对应的公网地址（即 Hub 的公网地址），于是 Spoke_A 将此报文发送至 Hub。

2. Hub 收到 Spoke_A 的业务报文以后，将此报文通过 Hub 与 Spoke_B 间的 MGRE 隧道转发给 Spoke_B。

如果 Hub 发现接收业务报文的 Tunnel 接口和发送业务的 Tunnel 接口属于同一个 NHRP 域以后，Hub 会向 Spoke_A 发送 NHRP 重定向消息。

3. Hub 向 Spoke_A 发送 NHRP 重定向消息。

Hub 通知 Spoke_A 发送 NHRP 地址解析请求，要求 Spoke_A 与 Spoke_B 建立隧道直接通信，后续业务报文就无需再经 Hub 中转。

4. Spoke_A 向 Hub 发送 NHRP 地址解析请求。

解析请求中包含了 Spoke_A 的私网网段 192.168.1.0 和公网地址 2.2.2.2，还有需要解析的私网网段 192.168.2.0。由于 Shortcut 方式下采用的是路由汇聚方案，因此 Spoke_A 无法学习到 Spoke_B 的 Tunnel 地址，只能通过 Spoke_B 的私网网段作为关键信息，获取 Spoke_B 的公网地址。

5. Hub 收到 Spoke_A 的地址解析请求后转发给 Spoke_B 处理。

6. Spoke_B 收到地址解析请求后，向 Spoke_A 返回应答消息。

Spoke_B 首先从 NHRP 地址解析请求中提取 Spoke_A 的私网网段和公网地址，并将该信息更新到自己的 NHRP 映射表中（见 Spoke_B 的 NHRP 映射表中红色字体）。同时，Spoke_B 生成 NHRP 地址解析应答消息返回给 Spoke_A，应答消息中包含 Spoke_B 的公网地址 2.2.2.2。

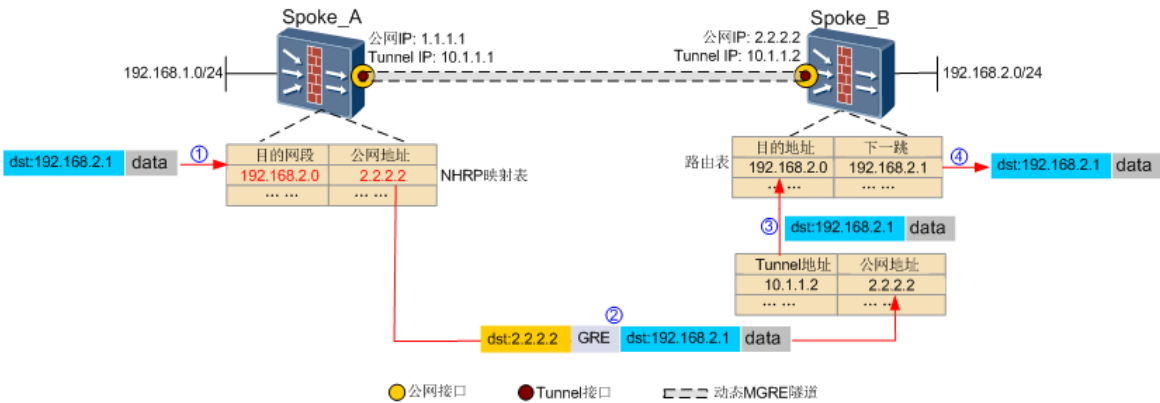
7. Spoke_A 收到 Spoke_B 的 NHRP 地址解析应答报文后与 Spoke_B 建立动态 MGRE 隧道。

Spoke_A 收到 Spoke_B 的应答报文后，将从应答消息中提取 Spoke_B 的私网网段和公网地址 2.2.2.2，更新到自己的 NHRP 映射表（见 Spoke_A 的 NHRP 映射表中红色字体）。

Spoke_A 与 Spoke_B 的 MGRE 隧道建立好以后，当 Spoke_A 再次收到其下用户发送给 Spoke_B 的业务报文时，Spoke_A 将会通过新建的动态 MGRE 隧道传送此报文到 Spoke_B。下面以 Spoke_A 单向发送数据给

Spoke_B 为例，详细介绍 MGRE 的封装原理。Spoke_B 返回给 Spoke_A 的反向报文封装过程同理。

图 2 MGRE 隧道报文封装过程



- Spoke_A 再次收到发往 Spoke_B 的业务报文以后，以该报文的网段 192.168.2.0 查找 NHRP 映射表，找到 Spoke_B 的公网地址 2.2.2.2。
- Spoke_A 以 GRE 协议作为报文头进行报文封装，封装后的目的地址为 2.2.2.2。
- Spoke_B 收到 Spoke_A 发送的封装报文后，按照 2.2.2.2 查找对应的 Tunnel 接口，并通过对应的 Tunnel 接口对报文解封装。
- 解封装后的报文将按照 Spoke_B 的路由表进行转发，发送给其下的用户。

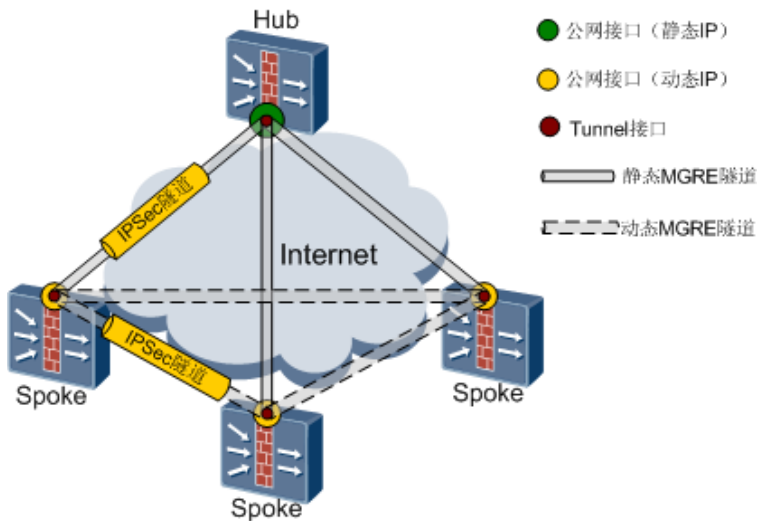
应用场景——基本场景

图 1 所示是 DSVPN 的典型组网，所有 Spoke 与 Hub 通过公网相连并建立 MGRE 隧道。

MGRE 隧道本身不具备安全加密功能，无法保证通信安全。当企业需要对总部和分支机构以及分支机构间传输的数据进行加密保护的时候，可以在部署 DSVPN 的同时绑定 IPSec 安全框架，以此达到安全通信的目的。

DSVPN 支持 NAT 穿越场景。当隧道的发起者（Spoke）和响应者（Spoke 或 Hub）之间存在 NAT 设备时，则隧道两端应开启 NAT 穿越功能。

图 1 DSVPN 的基本应用场景组网图



应用场景——Hub 主备备份场景

DSVPN 支持部署多台 Hub 设备，用以提高总部的可靠性。

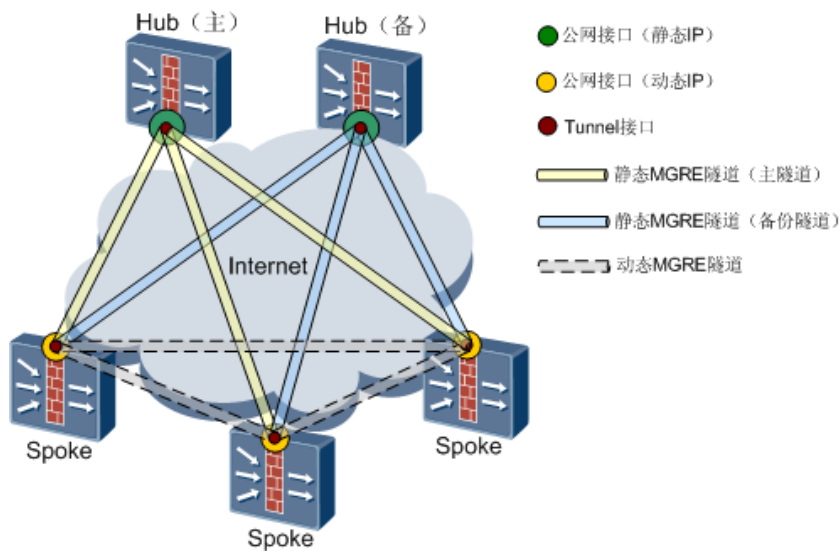
在基本应用场景中，所有的 Spoke 都与一台 Hub 相连。当该 Hub 出现故障时，Spoke 与 Spoke 间将无法建立隧道进行通信。通过在总部部署多台 Hub 设备，可以提升 DSVPN 网络的可靠性。

如图 1 所示，总部部署了两台 Hub 设备，两台 Hub 之间为主备关系。所有 Spoke 分别向主 Hub 和备 Hub 注册，并与主、备 Hub 建立 MGRE 隧道。

在主 Hub 和备 Hub 都运行正常的情况下，源 Spoke 和目的 Spoke 需要建立动态 MGRE 隧道时，受路由协议的控制，Spoke 到主 Hub 的路由优先级较高，因此源 Spoke 发出的 NHRP 协议报文将由主 MGRE 隧道发送到主 Hub，并由主 Hub 将此协议报文转发至目的 Spoke。当主 Hub 出现故障时，会导致 Spoke 到主 Hub 的路由优先级降低，源 Spoke 发出的 NHRP 协议报文将由备份隧道发送到备 Hub，并由备 Hub 转发协议报文至目的 Spoke。当主 Hub 从故障中恢复时，Spoke 又将进行隧道回切，重新将 NHRP 协议报文交由主 Hub 转发。

对于 Spoke 与 Spoke 之间已经建立动态 MGRE 隧道的情况下，Hub 设备运行正常与否不会对 Spoke 与 Spoke 之间的业务流量产生影响，因为 Spoke 与 Spoke 之间业务流量是直接通过动态 MGRE 隧道发送到对方。如果 Spoke 与 Spoke 之间的动态 MGRE 隧道由于长时间没有流量经过被拆除以后，Spoke 与 Spoke 再次需要建立 MGRE 隧道，那么 Spoke 就需要重新向 Hub 发送 NHRP 地址解析请求，此时 Spoke 将会根据路由优先级判断向哪个 Hub 发送 NHRP 地址解析请求。

图 1 Hub 备份场景组网图

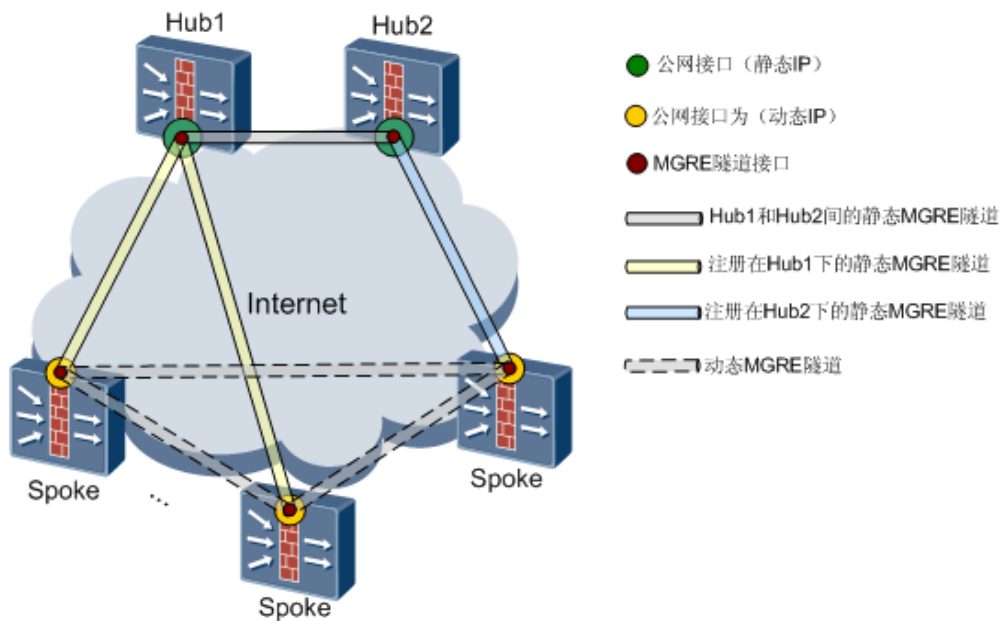


应用场景——Hub 负载分担场景

单台 Hub 设备受性能制约，其下所能连接的 Spoke 数量有限，当网络中 Spoke 节点较多时，总部需要部署多台 Hub 来提高总部的处理能力。

如图 1 所示，总部部署了两台 Hub 设备 Hub1 和 Hub2。由于 Spoke 节点较多，无法将所有的 Spoke 节点都注册到一台 Hub 设备上。因此，选择将一部分 Spoke 节点注册到 Hub1 下，另一部分 Spoke 节点注册到 Hub2 下。当 Hub1 下的 Spoke 需要与 Hub2 下的 Spoke 建立动态隧道时，Hub1 因为要转发 NHRP 地址解析请求给 Hub2，所以 Hub1 和 Hub2 之间需要建立静态 MGRE 隧道。源 Spoke 先将 NHRP 地址解析报文发送给 Hub1，Hub1 通过查找路由表和 NHRP 映射表以后将该报文通过 Hub1 与 Hub2 之间的静态 MGRE 隧道到达 Hub2，Hub2 再将该报文转发给目的 Spoke。通过该过程，两个不同 Hub 下的 Spoke 之间即可建立动态 MGRE 隧道。

图 1 Hub 负载分担场景组网图



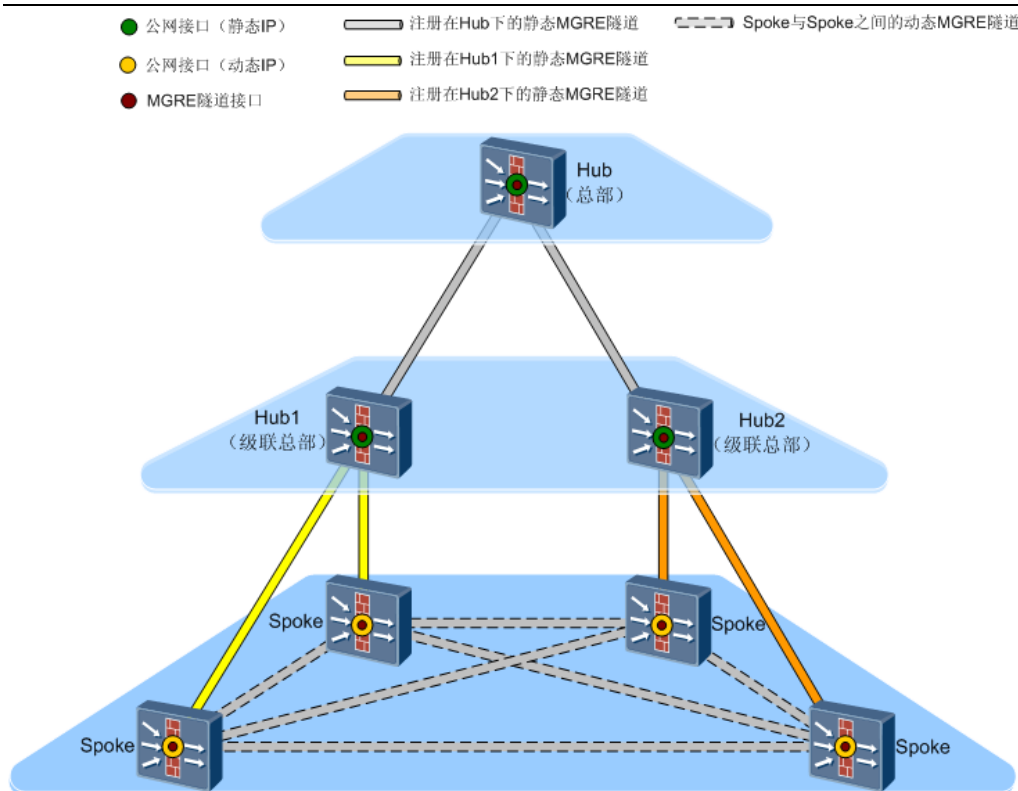
应用场景——级联场景

介绍设备同时充当 Spoke 和 Hub 两种角色时的应用场景。

图 1 所示是某企业的一个网络拓扑，该企业的办事机构存在层级关系。在此类有层级关系的网络中部署 DSVPN，一些中间节点将同时充当 Spoke 和 Hub 两种角色，这些同时充当 Spoke 和 Hub 角色的设备被称为级联总部。例如，Hub1 和 Hub2 即充当其下 Spoke 的总部，又充当 Hub（总部）的 Spoke 节点。

根据业务规划，一部分 Spoke 隶属于 Hub1；一部分 Spoke 隶属于 Hub2。当 Hub1 下的 Spoke 需要与 Hub2 下的 Spoke 建立动态 MGRE 隧道时，源 Spoke 将向 Hub1 发送 NHRP 地址解析请求，该地址解析请求经 Hub1 转发后最终到达 Hub（总部），Hub（总部）再将 NHRP 地址解析请求发送至 Hub2，并最终到达目的 Spoke，从而实现在级联场景下建立 Spoke 与 Spoke 之间的动态 MGRE 隧道。

图 1 Hub 级联场景组网图



使用限制及注意事项

配置 DSVPN 之前请先阅读使用限制和注意事项。

使用限制

- DSVPN 网络中只支持 2 种路由协议：静态路由、OSPF 路由协议。
- DSVPN 特性不支持双机热备。
- DSVPN 特性不支持虚拟系统。

注意事项

- 在同一个 DSVPN 网络中，所有 Tunnel 接口的 IP 地址应该配置为同一个网段。
- 在 MGRE 隧道中，一个 Tunnel 接口下只能引用一个 IPsec 安全框架。
- 在 DSVPN 部署了 IPsec 隧道时，快速刷新 NHRP 映射表会引发 IKE 邻居重协商等待，有可能造成业务中断，因此应避免频繁刷新 NHRP 映射表。

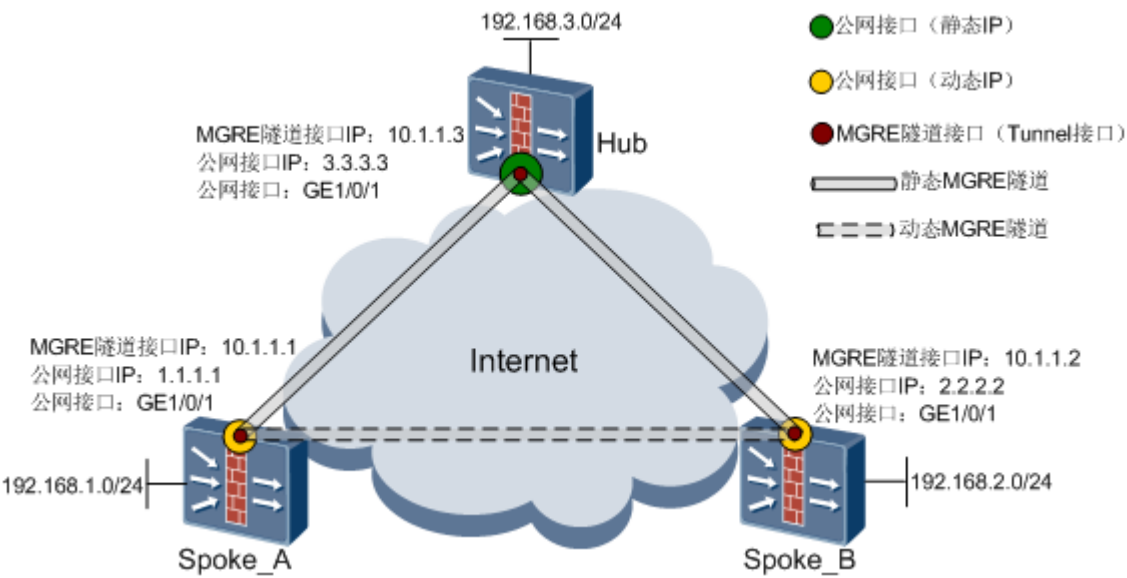
配置分支

介绍本设备在 DSVPN 中作为分支节点（Spoke）时的配置方法。

背景信息

图 1 所示是 DSVPN 的典型组网，图中标注了 MGRE 隧道接口、MGRE 隧道接口的 IP 地址、隧道类型以及各接口与隧道之间的关系，以作配置时的参考。

图 1 DSVPN 典型组网




操作步骤

1. 选择“网络 > DSVPN > DSVPN”。
2. 单击“DSVPN 列表”下的“新建”。
3. 在“场景”中选择“分支机构”。
4. 配置分支机构（Spoke）的基本信息。

参数	说明
策略名称	Spoke 节点上 MGRE 隧道接口的名称。在同一个 Spoke 上，MGRE 隧道接口的名称不能重复。
分支隧道 IP 地址	Spoke 节点上 MGRE 隧道接口的 IP 地址。如图 1 中的 10.1.1.1 和 10.1.1.2。
分支公网接口	Spoke 节点上的公网接口编号。
分支公网 IP 地址	Spoke 节点上公网接口的 IP 地址。如图 1 中的 1.1.1.1 和 2.2.2.2。
认证算法	<ul style="list-style-type: none">• NONE：表示采用明文方式传输认证字符串。• MD5：表示传输认证字符串时采用 MD5 算法进行加密。• SHA1：表示传输认证字符串时采用 SHA1 算法进行加密。 出于安全性考虑，推荐使用 SHA1 算法对认证字符串加密。

参数	说明
认证密钥	Hub 认证 Spoke 合法身份的字符串。 Spoke 向 Hub 注册时，Hub 通过认证密钥对 Spoke 进行身份认证。为了保证 Spoke 能够通过 Hub 的身份认证，双方的认证密钥必须配置一致。

5. 配置总部信息。分支需要向总部注册，并与总部建立静态 MGRE 隧道。因此，分支上需要手工配置总部的地址信息。

参数	说明
隧道 IP 地址	Hub 节点上 MGRE 隧道接口的 IP 地址。如图 1 中的 10.1.1.3。 在 Hub 备份场景中，Spoke 需要向多个 Hub 注册，单击  , 可以配置多个 Hub。
公网 IP 地址	Hub 节点上公网接口的 IP 地址。如图 1 中的 3.3.3.3。

6. 配置分支的路由信息。

参数	说明
路由协议	DSVPN 支持 OSPF 动态路由协议。 由于 OSPF 具备了适应范围广、路由收敛速度快、无自环等特点,因此在 DSVPN 中推荐部署 OSPF。
网络地址	指定加入 OSPF 区域的网段 IP。 分支需要将内网网段发布给其他分支，进行路由学习。所以，此处应输入各分支的内网网段。如图 1 中的 192.168.1.0 和 192.168.2.0。
路由学习方式	DSVPN 网络中支持两种路由部署方式： <ul style="list-style-type: none"> 分支节点相互学习路由 采用该路由部署方式，Spoke 与 Spoke 间将采用 Normal 方式建立动态 MGRE 隧道。 分支节点路由汇聚到总部 采用该路由部署方式，Spoke 与 Spoke 间将采用 Shortcut 方式建立动态 MGRE 隧道。 <p>当网络中的 Spoke 节点较少，Spoke 上需要存放的路由信息不多的情况下，可以选择“分支节点相互学习路由”的部署方案。当网络规模大，Spoke 节点较多时，请选择“分支节点路由汇聚到总部”的部署方案。</p> <p>说明： 同一 DSVPN 网络中，所有 Spoke、Hub 的路由学习方式必须一致，否则将导</p>

参数	说明
	致隧道建立失败。

7. 可选：配置 IPsec 信息。

MGRE 隧道本身不具备安全加密功能，无法保证通信安全。当企业需要对总部和分支机构以及分支机构间传输的数据进行加密保护的时候，可以在部署 DSVPN 的同时配置 IPsec 功能，以达到安全通信的目的。

a. 启用 IPsec 功能，并配置 IPsec 身份认证方式等参数。

参数	说明
IPsec 功能	开启 IPsec 功能。
认证方式	建立 IPsec 隧道时，隧道两端需要验证彼此身份。在 DSVPN 中，IPsec 支持两种身份认证方式：预共享密钥方式和证书方式。
预共享密钥	当“认证方式”选择“预共享密钥”时会出现本参数。在此填入双方管理员约定的密钥字符串。
证书	当“认证方式”选择“证书”时会出现本参数。在此选择本端的公钥证书。此证书中的部分信息将会在隧道建立过程中发给对端，供对端验证本端的合法性。同时也要求对端将其自身证书中的对应信息发给本端进行认证。上传证书的相关操作请参见 本地证书 。

b. 完成 IPsec 的高级配置。

启用 IPsec 功能以后，IPsec 的高级配置中会有缺省配置。你可以直接使用缺省配置，也可以根据实际需要修改缺省配置。

1. 配置 IKE 安全提议等协商参数。

参数	说明
IKE 版本	选择“v1”或“v2”来确定与对端进行 IKE 协商时所使用的协议版本，一般要求与对端保持一致。关于 IKE 不同版本的详细信息，请参见 IPsec 安全联盟 。同时选择两种版本表示可响应 v1 和 v2 两个版本的 IKE 请求，但是主动发起请求时只使用 v2 版本。
协商模式	选择 IKE 的协商模式。关于协商模式的详细信息，请参见 IKEv1 协商阶段 1 。 <ul style="list-style-type: none"> 自动：在响应协商时可接受主模式和野蛮模式，在发起协商时使用主模式。 主模式：强制使用主模式协商。主模式更安全。 野蛮模式：强制使用野蛮模式协商。野蛮模式更快速。
加密算法	选择保证数据不被窃取的加密算法。关于加密算法的详细信息，请参见 加密 。

参数	说明
认证算法	选择保证数据发送源可靠的认证算法。关于认证算法的详细信息，请参见 验证 。
完整性算法	当“IKE 版本”选择了“v2”时会出现本参数。 使用 IKEv2 版本时，选择保证数据不被篡改的完整性算法。关于完整性算法的详细信息，请参见 验证 。
DH 组	选择密钥交换方法。关于密钥交换方法的详细信息，请参见 密钥交换 。
SA 超时时间	为了保证隧道的安全，避免其在公网上存在过久，增加被攻击的风险，可以设定一个超时时间。当一定时间内隧道内没有流量可以自动拆除隧道，等后续有流量时再重新建立。

2. 配置 IPsec 安全提议等协商参数。

参数	说明
封装模式	选择 IPsec 的封装模式。关于封装模式的详细信息，请参见 封装模式 。 <ul style="list-style-type: none"> 自动：在响应协商时可接受隧道模式和传输模式，在发起协商时使用隧道模式。 隧道模式：只保护报文载荷部分，常用于 VPN 网关之间建立隧道。 传输模式：保护整个报文，常用于移动终端与 VPN 网关建立隧道。
安全协议	选择 IPsec 的安全协议。关于安全协议的详细信息，请参见 安全协议 。 <ul style="list-style-type: none"> AH：提供对整个报文的认证能力，但是不提供加密能力。 ESP：提供对报文载荷的加密和认证能力。 AH-ESP：提供对整个报文的加密和认证能力。
ESP 加密算法	当“安全协议”选择“ESP”或“AH-ESP”后会出现本参数。 选择保证数据不被窃取的加密算法。关于加密算法的详细信息，请参见 加密 。
ESP 认证算法	当“安全协议”选择“ESP”或“AH-ESP”后会出现本参数。 选择保证数据发送源可靠的认证算法。关于认证算法的详细信息，请参见 验证 。
AH 认证算法	当“安全协议”选择“AH”或“AH-ESP”后会出现本参数。 选择保证数据发送源可靠的认证算法。关于认证算法的详细信息，请参见 验证 。
PFS	选择密钥交换方法。关于密钥交换方法的详细信息，请参见 密钥交换 。 组号越大密钥越长，安全性越高。选择“NONE”表示不进行额外的密钥交换。
SA 超时	IPsec 隧道将在建立时间或者传输流量大小达到阈值时重新协商以保证安全性。 在“基于时间”中输入重协商间隔时间。在“基于流量”中输入流量阈值。 只要 IPsec 隧道建立后，满足其中任意一个条件，IPsec SA 就会开始重协商。 重协商不会导致当前隧道中断。

3. 配置 DPD 功能（对端状态检测）。

参数	说明
检测方式	<p>开启“DPD 状态检测”后，设备会自动发送 DPD 报文检测对端是否存活，以便及时拆除错误的隧道。</p> <p>可以有两种检测方式：</p> <ul style="list-style-type: none"> 周期性发送：“检测时间间隔”内未收到对端报文则发送一次 DPD 报文。 需要时才发送：“检测时间间隔”内未收到对端报文，且本端需要通信时发送一次 DPD 报文。 <p>对于使用 IKEv1 的隧道，此功能需要两端同时开启或关闭。在发送 DPD 报文后，在“重传时间间隔”内未收到回应报文，会被记录为一次失败时间。当连续发生五个失败事件后，则认为对端已经失效，设备会自动拆除隧道。</p> <p>对于使用 IKEv2 的隧道，此功能只需一端开启就可检测成功。发送 DPD 报文的间隔时间不按照“重传时间间隔”，而是以指数形式增长（发送 DPD 报文 1 后，隔 1 秒发报文 2，再隔 2 秒发报文 3，再隔 4 秒发报文 4，依次类推），一直到间隔 64 秒后发送报文 8。如果还收到回应报文，在报文 8 发送后的 128 秒时，隧道会被自动拆除。整个过程耗时约半个小时。</p>
检测时间间隔	输入“检测时间间隔”，单位为秒。
重传时间间隔	输入“重传时间间隔”，单位为秒。仅对 IKEv1 有效。

4. 配置 NAT 穿越功能。

参数	说明
NAT 穿越	<p>当两端之间存在 NAT 设备时，请选择此选项。</p> <p>开启 NAT 穿越功能后，设备会在普通 IPSec 报文基础上增加 UDP 头封装。当 IPSec 报文经过 NAT 设备时，NAT 设备会对该报文的外层 IP 头和增加的 UDP 报头进行地址和端口号转换。这样 NAT 设备对报文 IP 的转换就不会破坏原始 IPSec 报文的完整性，使其可以被对端网关正常接收。</p>

5. 单击“确定”。

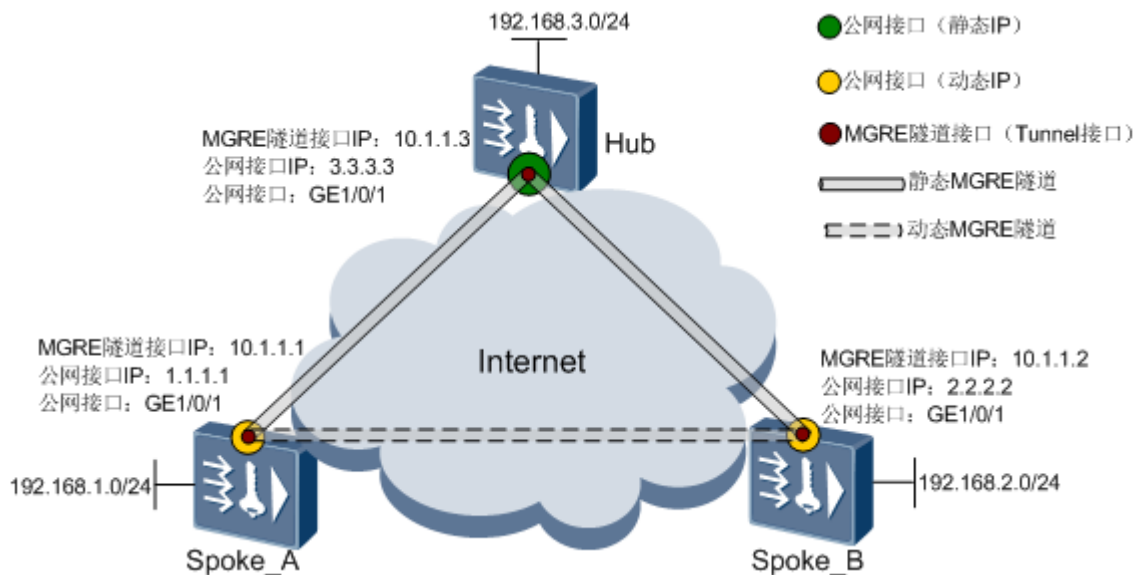
配置总部

介绍本设备在 DSVPN 中作为总部节点（Hub）时的配置方法。

背景信息

图 1 所示是 DSVPN 网络的典型组网，图中标注了 MGRE 隧道接口、MGRE 隧道接口的 IP 地址、隧道类型以及各接口与隧道之间的关系，以作配置时的参考。

图 1 DSVPN 典型组网



操作步骤

1. 选择“网络 > DSVPN > DSVPN”。
2. 单击“DSVPN 列表”下的“新建”。
3. 在“场景”中选择“总部”。
4. 配置总部节点（Hub）的基本信息。

参数	说明
策略名称	Hub 节点上 MGRE 隧道接口的名称。在同一个 Hub 上，MGRE 隧道接口的名称不能重复。
总部隧道 IP 地址	Hub 节点上 MGRE 隧道接口的 IP 地址。如图 1 中的 10.1.1.3。
总部公网接口	Hub 节点上的公网接口编号。
总部公网 IP 地址	Hub 节点上公网接口的 IP 地址。如图 1 中的 3.3.3.3。
认证算法	<ul style="list-style-type: none">• NONE：表示采用明文方式传输认证字符串。• MD5：表示传输认证字符串时采用 MD5 算法进行加密。• SHA1：表示传输认证字符串时采用 SHA1 算法进行加密。 出于安全性考虑，推荐使用 SHA1 算法对认证字符串加密。
认证密钥	Hub 认证 Spoke 合法身份的字符串。 Spoke 向 Hub 注册时，Hub 通过认证密钥对 Spoke 进行身份认证。为了保证 Spoke 能够通过 Hub 的身份认证，双方的认证密钥必须配置一致。

5. 配置总部的路由信息。

参数	说明
路由协议	DSVPN 只支持 OSPF 动态路由协议。

参数	说明
	由于 OSPF 具备了适应范围广、路由收敛速度快、无自环等特点,因此在 DSVPN 中推荐部署 OSPF。
网络地址	指定加入 OSPF 区域的网段 IP。 总部需要将内网网段发布给所有分支,进行路由学习。所以,此处应输入总部的内网网段。如图 1 中的 192.168.3.0。
路由学习方式	<p>DSVPN 网络中支持两种路由部署方式:</p> <ul style="list-style-type: none"> 分支节点相互学习路由 采用该路由部署方式, Spoke 与 Spoke 间将采用 Normal 方式建立动态 MGRE 隧道。 分支节点路由汇聚到总部 采用该路由部署方式, Spoke 与 Spoke 间将采用 Shortcut 方式建立动态 MGRE 隧道。 <p>当网络中的 Spoke 节点较少, Spoke 上需要存放的路由信息不多的情况下,可以选择“分支节点相互学习路由”的部署方案。当网络规模大, Spoke 节点较多时,请选择“分支节点路由汇聚到总部”的部署方案。</p> <p>说明: 同一 DSVPN 网络中,所有 Spoke、Hub 的路由学习方式必须一致,否则将导致隧道建立失败。</p>

6. 可选: 配置 IPsec 信息。详细参数解释请参见[配置 IPsec 信息](#)。

当企业需要对通信信息进行加密保护时,请配置 IPsec 相关信息。

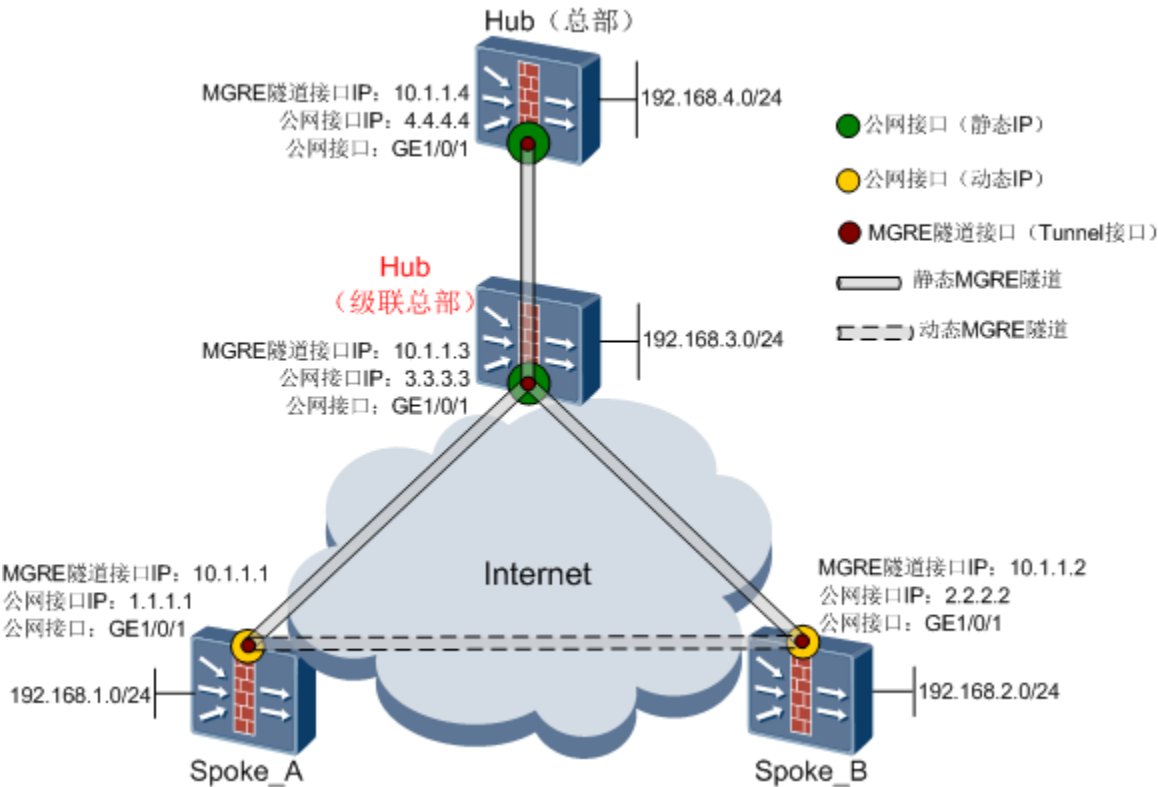
配置级联总部

介绍本设备在 DSVPN 中同时充当 Spoke 和 Hub (级联总部) 时的配置方法。

背景信息

图 1 所示是 DSVPN 的级联场景,图中标注了 MGRE 隧道接口、MGRE 隧道接口的 IP 地址、隧道类型以及各接口与隧道之间的关系,以作配置时的参考。级联总部和总部所不同的是,级联总部需要向上级总部注册,而总部不需要。

图 1 DSVPN 典型组网



操作步骤

1. 选择“网络 > DSVPN > DSVPN”。
2. 单击“DSVPN 列表”下的“新建”。
3. 在“场景”中选择“级联总部”。
4. 配置 Hub（级联总部）的基本信息。

参数	说明
策略名称	Hub（级联总部）节点上 MGRE 隧道接口的名称。在同一个 Hub（级联总部）上，MGRE 隧道接口的名称不能重复。
本端隧道 IP 地址	Hub（级联总部）节点上 MGRE 隧道接口的 IP 地址。如图 1 中的 10.1.1.3。
本端公网接口	Hub（级联总部）节点上的公网接口编号。
本端公网 IP 地址	Hub（级联总部）节点上公网接口的 IP 地址。如图 1 中的 3.3.3.3。
认证算法	<ul style="list-style-type: none">• NONE：表示采用明文方式传输认证字符串。• MD5：表示传输认证字符串时采用 MD5 算法进行加密。• SHA1：表示传输认证字符串时采用 SHA1 算法进行加密。 出于安全性考虑，推荐使用 SHA1 算法对认证字符串加密。
认证密钥	Hub（级联总部）认证 Spoke 合法身份的字符串。 由于 Hub（级联总部）要使用该密钥认证 Spoke 的身份，同时该密钥又要被 Hub（总部）认证。因此，Spoke、Hub（级联总部）、Hub（总部）三者的认

参数	说明
	证密钥必须配置一致。

5. 配置总部信息。Hub（级联总部）与 Hub（总部）建立静态 MGRE 隧道，下级 Hub 上需要手工配置上级 Hub 的地址信息。

参数	说明
隧道 IP 地址	Hub（总部）节点上 MGRE 隧道接口的 IP 地址。如 图 1 中的 10.1.1.4。
公网 IP 地址	Hub（总部）节点上公网接口的 IP 地址。如 图 1 中的 4.4.4.4。

6. 配置 Hub（级联总部）的路由信息。

参数	说明
路由协议	DSVPN 只支持 OSPF 动态路由协议。 由于 OSPF 具备了适应范围广、路由收敛速度快、无自环等特点，因此在 DSVPN 中推荐部署 OSPF。
网络地址	指定加入 OSPF 区域的网段 IP。 Hub（级联总部）需要将自身的内网网段发布给网络中的所有节点，进行路由学习。所以，此处应输入 Hub（级联总部）的内网网段。如 图 1 中的 192.168.4.0。
路由学习方式	DSVPN 网络中支持两种路由部署方式： <ul style="list-style-type: none"> 分支节点相互学习路由 采用该路由部署方式，Spoke 与 Spoke 间将采用 Normal 方式建立动态 MGRE 隧道。 分支节点路由汇聚到总部 采用该路由部署方式，Spoke 与 Spoke 间将采用 Shortcut 方式建立动态 MGRE 隧道。 <p>当网络中的 Spoke 节点较少，Spoke 上需要存放的路由信息不多的情况下，可以选择“分支节点相互学习路由”的部署方案。当网络规模大，Spoke 节点较多时，请选择“分支节点路由汇聚到总部”的部署方案。</p> <p>说明： 同一 DSVPN 网络中，所有 Spoke、Hub 的路由学习方式必须一致，否则将导致隧道建立失败。</p>

7. 可选：配置 IPsec 信息。详细参数解释请参见[配置 IPsec 信息](#)。

当企业需要对通信信息进行加密保护时，请配置 IPsec 相关信息。

监控

查看当前设备上建立的 MGRE 隧道相关信息。

1. 选择“网络 > DSVPN > 监控”。
2. 单击“刷新”，查看已建立的 MGRE 隧道信息如下。

参数	说明
设备名称	隧道两端的设备名称。如果隧道两端配置了设备名称，则此处显示将显示此名称；如果隧道两端未配置隧道名称，则此处显示隧道两端的 MGRE 隧道接口的 IP 地址。
设备序列号	设备的序列编号，用以唯一标识网络设备的身份。
设备身份	设备在 DSVPN 网络中所处的位置。设备可以是分支（Spoke）、总部（Hub）和级联总部。
私网 IP 地址	MGRE 隧道接口的 IP 地址。
公网 IP 地址	MGRE 隧道接口绑定的公网 IP 地址。
连接状态	隧道的连接状态。
最近一次建立时间	最近一次 MGRE 隧道的建立时间。
最近一次断开时间	最近一次 MGRE 隧道的断开时间。
断开原因	隧道的断开原因。

配置隧道参数

DSVPN 建立的是 MGRE 隧道。因此需要在 Spoke 和 Hub 上创建 Tunnel 接口，并改变 Tunnel 接口为点到多点类型。

在分支 Spoke 和总部 Hub 上需要分别进行如下配置。

配置 Spoke 节点的 MGRE 隧道参数

1. 配置 Tunnel 接口的类型为 P2MP。
 - a. `system-view`
 - b. `interface tunnel interface-number`
 - c. `tunnel-protocol gre p2mp`

2. 配置 Tunnel 接口的 IP 地址。

```
ip address ip-address { mask | mask-length }
```

3. 配置 Tunnel 接口的源地址。

```
source { vpn-instance vpn-instance-name source-ip-address | source-ip-address | interface-type interface-number | virtual-template vt-number }
```

4. 配置静态 NHRP 映射表项。

```
nhrp entry protocol-address nbma-address register
```

Spoke 需要向 Hub 注册，并与 Hub 建立静态 MGRE 隧道，因此需要手工指定 Hub 的 Tunnel 接口 IP 地址（*protocol-address*）和公网地址（*nbma-address*）。在主备备份场景中，Spoke 要分别向两个 Hub 注册，因此需要配置两条注册命令。一条命令的注册地址配置为主 Hub 的 Tunnel 地址和公网，另一条命令的注册地址为备 Hub 的 Tunnel 地址和公网。

5. 配置分支动态生成本地的组播成员列表。

```
nhrp entry multicast dynamic
```

在 DSVPN 网络中部署动态路由协议以后，分支节点需要与自身组播列表中的成员建立邻接关系，并学习彼此的路由信息。因此，在分支上需要配置动态生成组播成员列表功能。

6. 可选：配置 NHRP 协商的认证字符串。

```
nhrp authentication { md5 | plain | sha1 } authentication-string
```

 说明：

Spoke 和 Hub 上配置的认证字符串必须一致，隧道才能协商成功。

7. 可选：配置 NHRP 注册间隔。

```
nhrp registration interval interval
```

缺省情况下，分支节点向中心节点定时注册的时间间隔是 1800 秒。

8. 可选：配置允许覆盖冲突的 NHRP peer 表项。

```
nhrp registration no-unique
```

分支节点向总部发送 NHRP 注册消息，总部会生成动态的 NHRP 映射表项。当分支节点上的公网地址被修改以后，该分支节点将会重新向总部注册。如果分支节点设置了 **nhrp registration no-unique**，则总

部会在 NHRP 映射表中用该分支新的公网地址覆盖掉旧的公网地址；如果分支节点未设置 **nhrp registration no-unique**，则总部不覆盖。设置禁止覆盖的目的在于防止非法分支采用地址变更的办法覆盖合法分支的 NHRP 映射表项，从而带来安全隐患。在确认网络环境安全的前提下，也可以配置为允许覆盖，管理人员需根据实际的网络环境选择配置策略。

9. 可选：配置 MGRE 隧道建立方式为 Shortcut 方式。

[nhrp shortcut](#)

设备缺省使用 Normal 方式建立 MGRE 隧道。如果需要通过 Shortcut 方式建立 MGRE 隧道时，需要配置此命令。

配置 Hub 节点的 MGRE 隧道参数

1. 配置 Tunnel 接口的类型为 P2MP。
 - a. [system-view](#)
 - b. [interface tunnel](#) *interface-number*
 - c. [tunnel-protocol](#) gre p2mp

说明：

如果 Hub 是级联总部，则配置时还需要执行 [nhrp entry protocol-address nbma-address register](#) 命令向上级总部注册，如果 Hub 不是级联总部，则无需关注本命令。级联总部与总部的配置仅此差别，其余配置相同。

2. 配置 Tunnel 接口的 IP 地址。

[ip address](#) *ip-address* { *mask* | *mask-length* }

3. 配置 Tunnel 接口的源地址。

[source](#) { **vpn-instance** *vpn-instance-name* *source-ip-address* | *source-ip-address* | *interface-type* *interface-number* | **virtual-template** *vt-number* }

4. 配置总部动态生成本地的组播成员列表。

[nhrp entry multicast](#) dynamic

在 DSVPN 网络中部署动态路由协议以后，总部节点需要与自身组播列表中的成员建立邻接关系，并学习彼此的路由信息。因此，在总部上需要配置动态生成组播成员列表功能。

5. 可选：配置 NHRP 协商的认证字符串。

[nhrp authentication](#) { md5 | plain | sha1 } *authentication-string*

Spoke 向 Hub 注册时，Hub 通过认证字符串确认 Spoke 的身份。如果 Spoke 配置了认证字符串，则 Hub 也应配置相同的认证字符串。

6. 可选：配置 NHRP 域。

[nhrp network-id](#) *network-id*

DSVPN 网络支持域的划分，不同 NHRP 域互不相通，通过划分 NHRP 域可以控制 MGRE 隧道的建立范围。每一个 MGRE 接口都属于一个 NHRP 域，设备在转发 NHRP 报文时，会判断该报文出入接口的 NHRP 域 ID 是否相同，如果相同则转发；不同则丢弃。

7. 可选：配置 NHRP 重定向功能。

[nhrp redirect](#)

设备缺省使用 Normal 方式建立 MGRE 隧道，Normal 方式下无需配置 NHRP 重定向功能。如果需要通过 Shortcut 方式建立 MGRE 隧道时，需要配置此命令。

8. 可选：配置 NHRP 映射表的老化时间。

[nhrp entry holdtime second](#) *seconds*

缺省情况下，NHRP 映射表的老化时间是 7200 秒。

为了防止在分支注册消息到来前，总部的 NHRP 映射表先行老化，因此在配置时，分支向总部定时注册的间隔时间应该要短于总部的 NHRP 映射表老化时间。假如用户配置的注册间隔时间比 NHRP 映射的老化时间要长，则该注册时间将不会生效。这种情况下，设备会自动以 NHRP 映射表老化时间的 1/3 作为分支向总部注册的间隔时间。

配置路由参数

DSVPN 网络支持两种路由部署方案，一种是分支节点相互学习路由，另一种是分支节点路由汇聚到总部。采用不同的路由部署方案，DSVPN 建立 MGRE 隧道的过程不同。

DSVPN 的路由部署方案与隧道建立方式间的关系如下：

- 分支节点相互学习路由

在该路由部署方式下，Spoke 上将存放到 DSVPN 网络中所有对端的私网路由。Spoke 存放所有对端的私网路由数据，将消耗大量的 CPU 和内存资源来处理这些数据，因而对其路由表容量和性能有较高的要求。而实际应用中，出于费用的方面的考虑，Spoke 的性能往往较低，能存放的路由数量有限。所以，本方案只适用于网络节点较少，路由信息量小的场景。在该路由部署方案下，DSVPN 采用 Normal 方式建立 MGRE 隧道。

- 分支节点路由汇聚到总部

在该路由部署方式下，Spoke 只需要存放到 Hub 路由，路由下一跳指向 Hub 的 Tunnel 接口地址。由于 Spoke 减少了自身的路由数量，所以适用于网络规模大，分支节点较多的场景。在该路由部署方案下，DSVPN 采用 Shortcut 方式建立 MGRE 隧道。

DSVPN 部署路由时，可以部署静态路由和动态路由。其中，动态路由只支持 OSPF 协议。

分支节点相互学习路由

- 静态路由

1. 进入系统视图。

[system-view](#)

2. 配置静态路由。

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

当分支节点相互学习路由时，DSVPN 采用 Normal 方式建立 MGRE 隧道。Spoke 和 Hub 上的路由配置方法相同，*ip-address* 配置为对端节点（Spoke 或 Hub）的私网网段地址，*nexthop-address* 为对端节点的 Tunnel 接口 IP 地址。

- 动态路由

1. 进入系统视图。

[system-view](#)

2. 配置动态路由。

动态路由只支持 OSPF 协议，路由的配置方法如下表。

节点	OSPF
Spoke	<ol style="list-style-type: none"> a. 进入 OSPF 视图。 ospf [<i>process-id</i>] b. 进入 OSPF 区域视图。 area <i>area-id</i> c. 指定 Spoke 要发布的内网路由信息。 network <i>address wildcard-mask</i> d. 将 OSPF 网络类型配置成广播型。 <ol style="list-style-type: none"> 1. 进入 Spoke 的 Tunnel 接口视图。 interface tunnel <i>interface-number</i> 2. 配置 OSPF 的网络类型为广播型。 ospf network-type broadcast 3. 配置 Spoke 的接口在选举 DR 时的优先级为 0。 ospf dr-priority 0 <p>在广播类型的 OSPF 网络中，所有路由信息都要由网络中的 DR（Designated Router）广播到其他节点。网络中由哪个设备充当 DR，是根据各设备发布 OSPF 路由的接口优先级来决定，接口优先级高的设备就会被选举为 DR。在本场景中，Hub 需要向 Spoke 发布路由信息，因此需要将 Hub 选举为网络中的 DR。而缺省情况下，Spoke 和 Hub 上 Tunnel 接口对应优先级的值都为 1。通过本命令降低 Spoke 接口的优先级（本例设置为 0），当 Spoke 的优先级低于 Hub 以后，就可以确保 Hub 被选择为 DR。此处也可以采用提高 Hub 接口优先级的办法达到这个目的，效果是一样的。</p>
Hub	配置方法与 Spoke 相同。

分支节点路由汇聚到总部

- 静态路由

1. 进入系统视图。

[system-view](#)

2. 配置静态路由。

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

当分支节点路由汇聚到总部时，DSVPN 采用 Shortcut 方式建立 MGRE 隧道。Spoke 和 Hub 的静态路由配置如下：

- Spoke

`ip-address` 配置为 Hub 的私网网段地址，`nexthop-address` 为 Hub 节点的 Tunnel 接口 IP 地址。

- Hub

`ip-address` 配置为 Spoke 节点的私网网段地址，`nexthop-address` 为 Spoke 节点的 Tunnel 接口 IP 地址。

- 动态路由配置动态路由。

1. 进入系统视图。

`system-view`

2. 配置动态路由。

动态路由只支持 OSPF 协议，路由的配置方法如下表。

节点	OSPF
Spoke	<ol style="list-style-type: none">a. 进入 OSPF 进程视图。 <code>ospf [process-id]</code>b. 进入 OSPF 区域视图。 <code>area area-id</code>c. 指定 Spoke 要发布的内网路由信息。 <code>network address wildcard-mask</code>d. 将 OSPF 网络类型配置成 P2MP。<ol style="list-style-type: none">1. 进入 Spoke 的 Tunnel 接口视图。 <code>interface tunnel interface-number</code>2. 配置 OSPF 的网络类型为点到多点。 <code>ospf network-type p2mp</code>
Hub	配置方法与 Spoke 相同。

（可选）配置 IPsec 安全框架

当企业需要对总部和分支机构以及分支机构间传输的数据进行加密保护的时候，可以在部署 DSVPN 的同时绑定 IPsec 安全框架，实现分支间同时动态建立起 GRE 隧道和 IPsec 隧道。

前提条件

IPsec 安全框架中包含了建立 IPsec 隧道所需的 IKE 安全提议、IPsec 安全提议等协商参数，其作用与 IPsec 安全策略相同。由于 IPsec 安全框架是对所有路由到隧道接口的数据流进行 IPsec 保护，所以无需定义 ACL，较之于 IPsec 安全策略，IPsec 安全框架的配置更简单。在 DSVPN 中如果要应用 IPsec 安全框架，则需要提前在设备上准备以下数据：

- 创建 IKE 安全提议，配置步骤请参见[配置 IKE 安全提议](#)。
- 创建 IKE 对等体，配置步骤请参见[配置 IKE 对等体](#)。

被 IPsec 安全框架所引用的 IKE 对等体无需配置本端地址和对端地址。

- 创建 IPsec 安全提议，配置步骤请参见[配置 IPsec 安全提议](#)。

完成上述准备之后，请在分支 Spoke 和总部 Hub 上进行如下配置。

操作步骤

1. 进入系统视图。

[system-view](#)

2. 创建一个 IPsec 安全框架，并进入 IPsec 安全框架视图。

[ipsec profile](#) *profile-name*

3. 在 IPsec 安全框架下绑定 IKE 对等体。

[ike-peer](#) *peer-name*

4. 在 IPsec 安全框架下绑定 IPsec 安全提议。

[proposal](#) *proposal-name1* [*proposal-name2*]<1-5>

5. 返回系统视图。

[quit](#)

6. 进入 Tunnel 接口视图。

[interface tunnel](#) *interface-number*

7. 配置接口绑定 IPsec 安全框架。

[ipsec profile](#) *profile-name*

如果 Tunnel 接口下需要引用新的 IPsec 安全框架，需要先取消当前已引用的 IPsec 安全框架。

维护 DSVPN

配置完成后，可参考以下命令进行隧道验证和维护。如果验证通过，则您可正常使用隧道；如果验证不通过，请对照故障现象进行故障处理。

查看 DSVPN 网络中的 MGRE 隧道运行状况

通过查看 DSVPN 的配置信息以及 NHRP 协议报文的统计信息，了解 MGRE 隧道的运行情况。

在任意视图下执行如[表 1](#)所示的命令可查看 MGRE 运行状况。

表 1 查看 MGRE 隧道运行状况	
操作	命令
查看 NHRP 映射表	display nhrp entry [<i>ip protocol-address</i> interface tunnel <i>interface-number</i>]
查看 NHRP 协议报文的统计信息	display nhrp statistics [interface tunnel <i>interface-number</i>]
查看 IPsec 安全框架的信息	display ipsec profile [brief name <i>profile-name</i>]

清除 DSVPN 网络中的 MGRE 隧道相关信息

如果用户需要重新配置 MGRE 隧道，可以清除相关的 NHRP 映射表项，NHRP 映射表项清除后将造成业务中断。

如果 NHRP 协议的统计信息比较多不便于查看，可以清除 NHRP 协议报文统计信息。

在任意视图下执行如[表 2](#)所示的命令可清除 MGRE 隧道信息。

表 2 清除 MGRE 隧道相关信息

操作	命令
清除 NHRP 映射表中的动态表项	<code>reset nhrp entry [nbma-address interface tunnel interface-number]</code>
清除 NHRP 协议报文的统计信息	<code>reset nhrp statistics [interface tunnel interface-number]</code>

举例：配置 DSVPN 基本场景

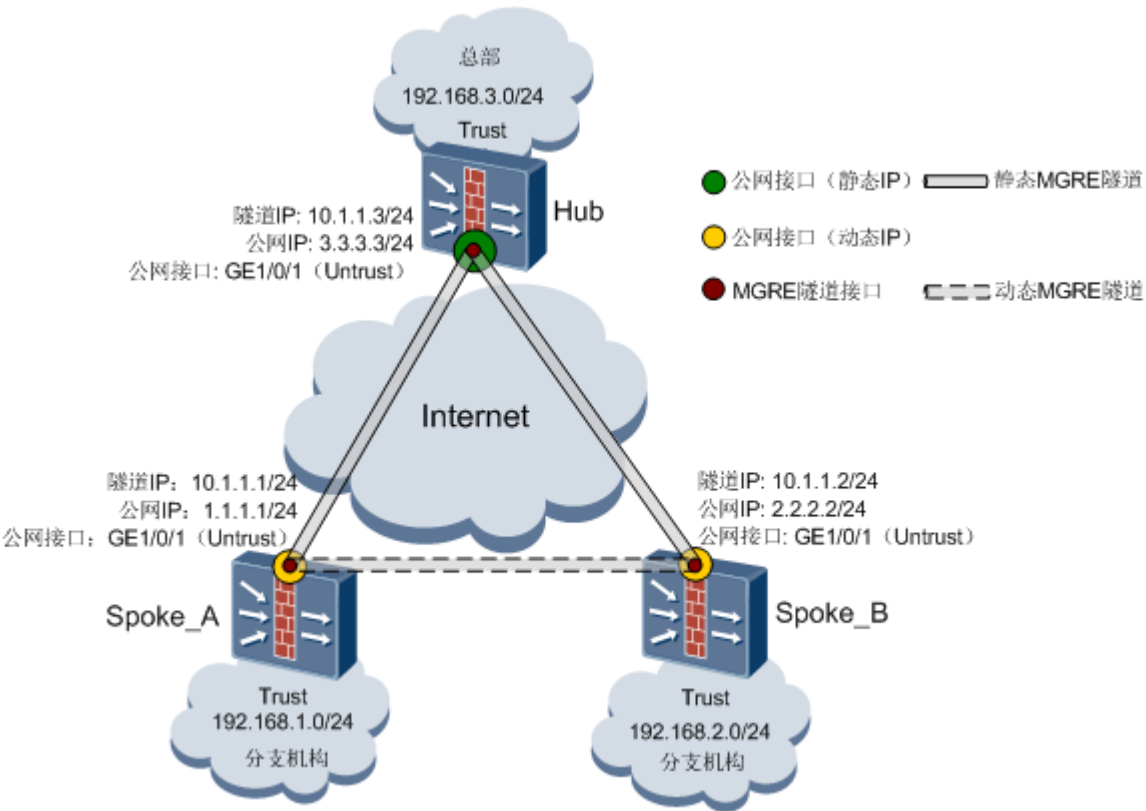
介绍基本应用场景下，DSVPN 的配置方法。

组网需求

图 1 所示，某企业有总部（Hub）和两个分支（Spoke_A 和 Spoke_B），分布在不同地域。Hub 的公网地址固定，Spoke 通过 DHCP 方式从运营商处获取动态的公网地址，Hub 和 Spoke 间的公网路由可达。

现在用户希望能够在分支（Spoke_A）与分支（Spoke_B）间直接建立 VPN 隧道，使各分支下的用户可通过隧道互相访问。

图 1 DSVPN 的典型组网



配置思路

对用户需求做如下分析：

1. 用户需要在公网地址动态变化的分支间直接建立 VPN 隧道，因此需要采用 DSVPN 技术建立隧道。
2. 考虑到网络中分支节点较少，因此在网络中部署 OSPF 路由协议，并采用全网络路由学习方案。



说明：

本举例中只列举了 2 个分支机构，仅为说明配置原理。当实际场景中分支节点较多时，可以选择使用路由汇聚方案。

操作步骤

1. 配置 Spoke_A 节点。

- a. 配置接口 IP 地址和安全区域，完成网络基本参数配置。

1. 选择“网络 > 接口”，单击 GE1/0/1 对应的 ，按如下参数配置。假设此处获取到的公网地址为 1.1.1.1。

安全区域	untrust
模式	路由
IPv4	
连接类型	DHCP

2. 单击“确定”。

- b. 配置安全策略中需要引用的地址段。

1. 选择“对象 > 地址 > 地址”，在“地址列表”中，单击“新建”，并配置地址的各项参数。

名称	source_address
IP 地址/范围或 MAC 地址	192.168.1.0/24

2. 单击“确定”。

- c. 配置安全策略。

1. 选择“策略 > 安全策略 > 安全策略”，单击“新建”，配置安全策略 policy_sec_gre_1 的各项参数，允许 GRE 协议报文通过域间安全策略。

名称	policy_sec_gre_1
源安全区域	local,untrust
目的安全区域	local,untrust
服务	gre
动作	允许

2. 单击“确定”。

3. 再新建一条名称为 policy_sec_gre_2 的安全策略，并配置安全策略的各项参数，保证业务流量的转发。

名称	policy_sec_gre_2
源安全区域	trust,untrust
目的安全区域	trust,untrust
源地址/地区	source_address
动作	允许

4. 单击“确定”。

d. 配置 DSVPN 参数。

1. 选择“网络 > DSVPN > DSVPN”。

2. 单击“新建”，选择“分支机构”。

3. 配置 Spoke_A 基本信息。认证密钥由网络管理员自行规划，隧道两端使用的认证密钥必须保持一致。本举例中使用的认证密钥为 Test!123。

1、基本配置

策略名称 *

分支隧道IP地址 *

分支公网接口 *

分支公网IP地址 *

认证密钥 *

4. 配置总部信息。

Spoke_A 需要向 Hub 注册，因此需要在 Spoke_A 上指定 Hub 的地址信息。

2. 总部信息

隧道IP地址

10.1.1.3

*

+

公网IP地址

3.3.3.3

*

5. 配置路由信息。

选择 DSVPN 中部署的路由协议以及路由的学习方式。

3. 路由配置

路由协议

☒ OSPF

网络地址

192.168.1.0/255.255.255.0

*一行一条记录，
输入格式为 “1.1.1.0/255.255.255.0”。

路由学习方式

☒ 分支节点相互学习路由

☐ 分支节点路由汇聚到总部


6. 单击“确定”。

2. 配置 Spoke_B 节点。

Spoke 节点的配置方法都相同，请参考 Spoke_A 的配置步骤，完成 Spoke_B 的配置。

3. 配置 Hub 节点。

a. 配置接口 IP 地址和安全区域，完成网络基本参数配置。

1. 选择“网络 > 接口”，单击 GE1/0/1 对应的，按如下参数配置。

安全区域	untrust
IPv4	
IP 地址	3.3.3.3/24

2. 单击“确定”。

b. 配置安全策略中需要引用的地址段。

1. 选择“对象 > 地址 > 地址”。在“地址列表”中，单击“新建”，并配置地址的各项参数。

名称	source_address
----	----------------

IP 地址/范围或 MAC 地址	192.168.3.0/24
------------------	----------------

2. 单击“确定”。

c. 配置安全策略。

1. 选择“策略 > 安全策略 > 安全策略”，单击“新建”。配置安全策略 policy_sec_gre_1 的各项参数，允许 GRE 协议报文通过域间安全策略。

名称	policy_sec_gre_1
源安全区域	local,untrust
目的安全区域	local,untrust
服务	gre
动作	允许

2. 单击“确定”。

3. 再新建一条名称为 policy_sec_gre_2 的安全策略，并配置安全策略的各项参数，保证业务流量的转发。

名称	policy_sec_gre_2
源安全区域	trust,untrust
目的安全区域	trust,untrust
源地址/地区	source_address
动作	允许

4. 单击“确定”。

d. 配置 DSVPN 参数。

1. 选择“网络 > DSVPN > DSVPN”。
2. 单击“新建”，选择“总部”。

3. 配置 Hub 的基本信息。认证密钥由网络管理员自行规划，只要保证隧道两端的认证密钥一致即可。本举例中使用的认证密钥为 Test!123。

1. Basic Configuration

Policy Name: Hub

HQ Tunnel IP Address: 10.1.1.3/24

HQ Public Interface: GE1/0/1(GE1/0/1)

HQ Public IP Address: 3.3.3.3

Authentication Key: Test!123

4. 配置路由信息。

选择 DSVPN 中部署的路由协议以及路由的学习方式。

路由配置

路由协议: ☒ OSPF

网络地址: 192.168.3.0/255.255.255.0

路由学习方式: ☒ 分支节点相互学习路由

☐ 分支节点路由汇聚到总部

*一行一条记录，输入格式为“1.1.1.0/255.255.255.0”。

5. 单击“确定”。

结果验证

- 配置完成后，使用 Spoke_A 下的用户 PC Ping Spoke_B 下的用户 PC，触发 Spoke 之间建立动态 MGRE 隧道。
- 在 Spoke_A 上，选择“网络 > DSVPN > DSVPN”。在 DSVPN 列表中可以看到名称为“Spoke_A”的记录，单击该条记录对应的“详情”，查看隧道建立情况。
- 如果隧道建立正常，则可以看到 Spoke_A 与 Hub、Spoke_B 建立的隧道连接状态为 UP。

设备名称	设备身份	私网 IP 地址	公网 IP 地址	连接状态
10.1.1.1	分支机构	10.1.1.1/255.255.255.255	1.1.1.1	up
10.1.1.3	总部	10.1.1.3/255.255.255.255	3.3.3.3	up
10.1.1.2	分支机构	10.1.1.2/255.255.255.255	2.2.2.2	up

配置脚本

- Spoke_A 的配置脚本

```
#
interface GigabitEthernet1/0/1
  dhcp client enable
#
interface Tunnel0
  alias Spoke_A
  ip address 10.1.1.1 255.255.255.0
  tunnel-protocol gre p2mp
  source GigabitEthernet1/0/1
  nhrp authentication plain %$$$Se0N~X[7S6P~!!=c\zg0Mzqh%$$$
  nhrp entry multicast dynamic
  nhrp entry 10.1.1.3 3.3.3.3 register
  ospf network-type broadcast
  ospf dr-priority 0
#
ospf 1
  area 0.0.0.0
    network 1.1.1.0 0.0.0.255
  area 0.0.0.1
    network 192.168.1.0 0.0.0.255
#
ip address-set source_address type object
  address 0 192.168.1.0 mask 24
#
security-policy
  rule name policy_sec_gre_1
    source-zone local
    source-zone untrust
    destination-zone local
    destination-zone untrust
    service gre
    action permit
  rule name policy_sec_gre_2
    source-zone trust
    source-zone untrust
    destination-zone trust
    destination-zone untrust
```

```
source-address address-set source_address
action permit
```

- Spoke_B 的配置脚本

```
#
interface GigabitEthernet1/0/1
  dhcp client enable
#
interface Tunnel0
  alias Spoke_B
  ip address 10.1.1.2 255.255.255.0
  tunnel-protocol gre p2mp
  source GigabitEthernet1/0/1
  nhrp authentication plain %$$$Se0N~X[7S6P~!!=c\zg0Mzqh%$$$
  nhrp entry multicast dynamic
  nhrp entry 10.1.1.3 3.3.3.3 register
  ospf network-type broadcast
  ospf dr-priority 0

#
ospf 1
  area 0.0.0.0
    network 1.1.1.0 0.0.0.255
  area 0.0.0.1
    network 192.168.2.0 0.0.0.255
#
ip address-set source_address type object
  address 0 192.168.2.0 mask 24
#
security-policy
  rule name policy_sec_gre_1
    source-zone local
    source-zone untrust
    destination-zone local
    destination-zone untrust
    service gre
    action permit
  rule name policy_sec_gre_2
    source-zone trust
    source-zone untrust
    destination-zone trust
    destination-zone untrust
```

```
source-address address-set source_address
action permit
```

- Hub 的配置脚本

```
#
interface GigabitEthernet1/0/1
 ip address 3.3.3.3 255.255.255.0
#
interface Tunnel0
 alias Hub
 ip address 10.1.1.3 255.255.255.0
 tunnel-protocol gre p2mp
 source GigabitEthernet1/0/1
 nhrp authentication plain %$$$Se0N~X[7S6P~!!=c\zg0Mzqh%$$$
 nhrp entry multicast dynamic
 ospf network-type broadcast
#
ospf 1
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
 area 0.0.0.1
  network 192.168.3.0 0.0.0.255
#
ip address-set source_address type object
 address 0 192.168.3.0 mask 24
#
security-policy
 rule name policy_sec_gre_1
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service gre
  action permit
 rule name policy_sec_gre_2
  source-zone trust
  source-zone untrust
  destination-zone trust
  destination-zone untrust
  source-address address-set source_address
  action permit
```

故障处理——Spoke 与 Hub 建立静态 MGRE 隧道失败

现象描述

在 Hub 上执行 [display nhrp entry](#) 查看 NHRP 映射表，发现没有动态生成 Spoke 的 NHRP 映射表项。

可能原因

- 网络层连通性、安全策略等基本配置问题。
- Spoke 和 Hub 上配置的认证密钥不一致。

处理步骤

1. 检查 Spoke、Hub 之间的公网路由是否可达，且安全策略是否配置正确，排除基本的网络问题。
2. 检查 Spoke、Hub 上配置的认证密钥是否相同。

请核对 Hub 和 Spoke 所使用的认证字密钥是否一致。如果不一致，请执行 [nhrp authentication](#) 命令修改配置。

故障处理——Spoke 与 Spoke 间建立动态 MGRE 隧道失败

现象描述

在源 Spoke 上执行 [display nhrp entry](#) 查看 NHRP 映射表，发现没有动态生成目的 Spoke 的 NHRP 映射表项。

可能原因

- 网络层连通性、安全策略等基本配置问题。
- 源 Spoke 和目的 Spoke 的隧道建立方式不一致。

处理步骤

1. 检查 Spoke、Hub 之间的公网路由是否可达，且安全策略是否配置正确，排除基本的网络问题。
2. 检查源 Spoke 和目的 Spoke 的隧道建立方式是否一致。

在源 Spoke 的 Tunnel 接口视图下执行 [display this](#) 命令。

```
[sysname-Tunnel0] display this
```

```
interface Tunnel0
alias spoke_A
ip address 10.1.1.1 255.255.255.0
tunnel-protocol gre p2mp
source 1.1.1.1
nhrp authentication plain %$$$J7h~Y.ZdQ7P`d3=e.KON3aX0%$$$
nhrp entry multicast dynamic
nhrp shortcut
nhrp entry 10.1.1.3 3.3.3.3 register
```

在目的 Spoke 的 Tunnel 接口视图下执行 [display this](#) 命令。

```
[sysname-Tunnel0] display this
interface Tunnel0
alias spoke_B
ip address 10.1.1.2 255.255.255.0
tunnel-protocol gre p2mp
source 2.2.2.2
nhrp authentication plain %$$$J7h~Y.ZdQ7P`d3=e.KON3aX0%$$$
nhrp entry multicast dynamic
nhrp entry 10.1.1.3 3.3.3.3 register
```

从以上显示信息可以看出，源 Spoke 采用的是 **Shortcut** 方式建立 MGRE 隧道，目的 Spoke 采用默认的 **Normal**（Normal 是缺省配置，因此回显信息中不显示）方式建立 MGRE 隧道。由于双方隧道建立方式不一致，因此动态隧道无法成功建立。请将源 Spoke 和目的 Spoke 的隧道建立方式改为一致。

HCIE-Security 模拟面试问题及面试建议

1. DSVPN 有哪些应用场景，请分别说明。
2. DSVPN 工作原理，请说明。