目 录

1 ADVPN

1.1 ADVPN简介

ADVPN（Auto Discovery Virtual Private Network，自动发现虚拟专用网络）是一种基于 VAM（VPN Address Management，VPN 地址管理）协议的动态 VPN 技术。VAM 协议负责收集、维护和分发动态变化的公网地址等信息，采用 Client/Server 模型。ADVPN 网络中的节点（称为 ADVPN 节点）作为 VAM Client。当公网地址变化时，VAM Client 将当前公网地址注册到 VAM Server。ADVPN 节点通过 VAM 协议从 VAM Server 获取另一端 ADVPN 节点的当前公网地址，从而实现在两个节点之间动态建立跨越 IP 核心网络的 ADVPN 隧道。

在企业网各分支机构使用动态地址接入公网的情况下，可以利用 ADVPN 在各分支机构间建立 VPN。

1.1.1 ADVPN组网结构

ADVPN 通过 ADVPN 域区分不同的 VPN 网络，ADVPN 域由域 ID 来标识。属于同一个 VPN 的 VAM Client 需要规划到相同的 ADVPN 域中，且一个 VAM Client 只能属于一个 ADVPN 域；VAM Server 可以同时为多个 ADVPN 域服务，管理多个 ADVPN 域的 VAM Client。

ADVPN 节点分为如下两类：

- Hub：ADVPN 网络的中心设备。它是路由信息交换的中心。
- Spoke：ADVPN 网络的分支设备，通常是企业分支机构的网关。该节点不会转发收到的其它 ADVPN 节点的数据。

根据数据转发方式的不同，ADVPN 组网结构分为如下两种：

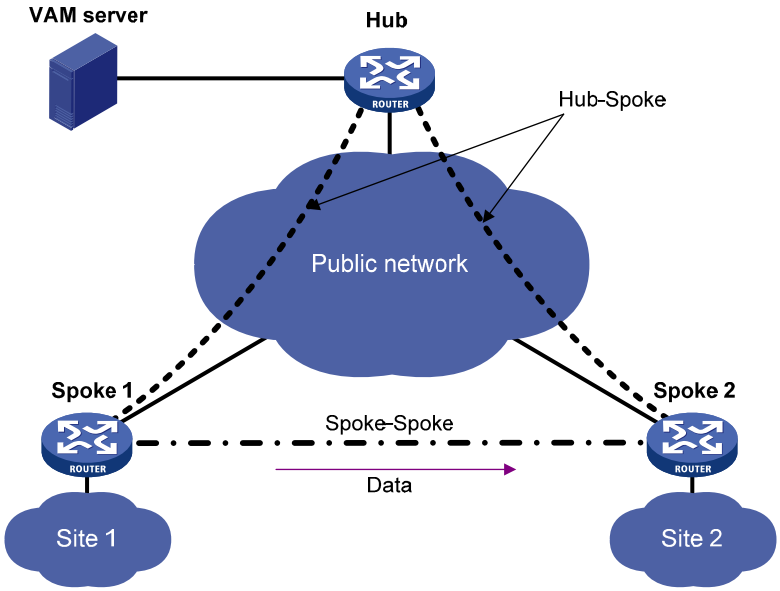
- Full-Mesh（全互联）网络：Spoke 和 Spoke 之间可以建立隧道直接通信。
- Hub-Spoke 网络：Spoke 之间不能建立隧道直接通信，只能通过 Hub 转发数据。

当一个 ADVPN 域中的 ADVPN 节点数目较多时，由于某些原因（如动态路由协议邻居数限制等），Hub 无法管理全部的 ADVPN 节点。此时，可以将 ADVPN 网络划分为多个 Hub 组，每个 Hub 组中包含一个或多个 Hub，及一部分 Spoke 节点，以减轻 Hub 节点的负担。

1. Full-Mesh网络

如 图 1-1 所示，在Full-Mesh网络中，Spoke向VAM Server注册后获得Spoke所属ADVPN域所在Hub组中Hub的信息，并与Hub建立永久的ADVPN隧道。当两个Spoke之间有数据报文交互时，Spoke从VAM Server获取对端Spoke的公网地址，并在Spoke之间直接建立隧道。Spoke之间的隧道是动态的，当在一段时间（Spoke-Spoke隧道空闲超时时间）内没有数据报文交互时，则删除该隧道。

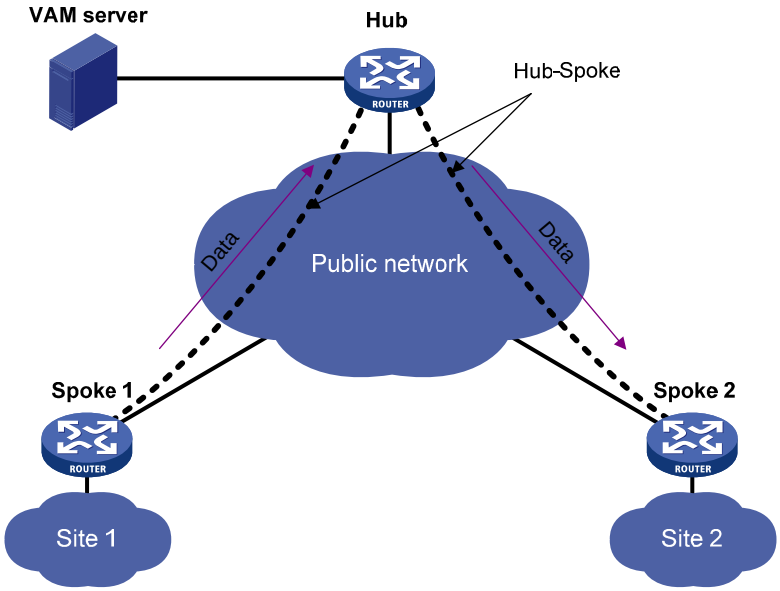
图1-1 Full-Mesh 网络示意图



2. Hub-Spoke网络

如 图 1-2 所示，在Hub-Spoke网络中，Spoke向VAM Server注册后获得Spoke所属ADVPN域所在Hub组中Hub的信息，并与Hub建立永久的ADVPN隧道。两个Spoke之间有数据报文交互时，该报文通过Hub转发，不会在Spoke之间建立隧道。Hub既作为路由信息交换的中心，又作为数据转发的中心。

图1-2 Hub-Spoke 网络示意图



3. 划分多个Hub组网络

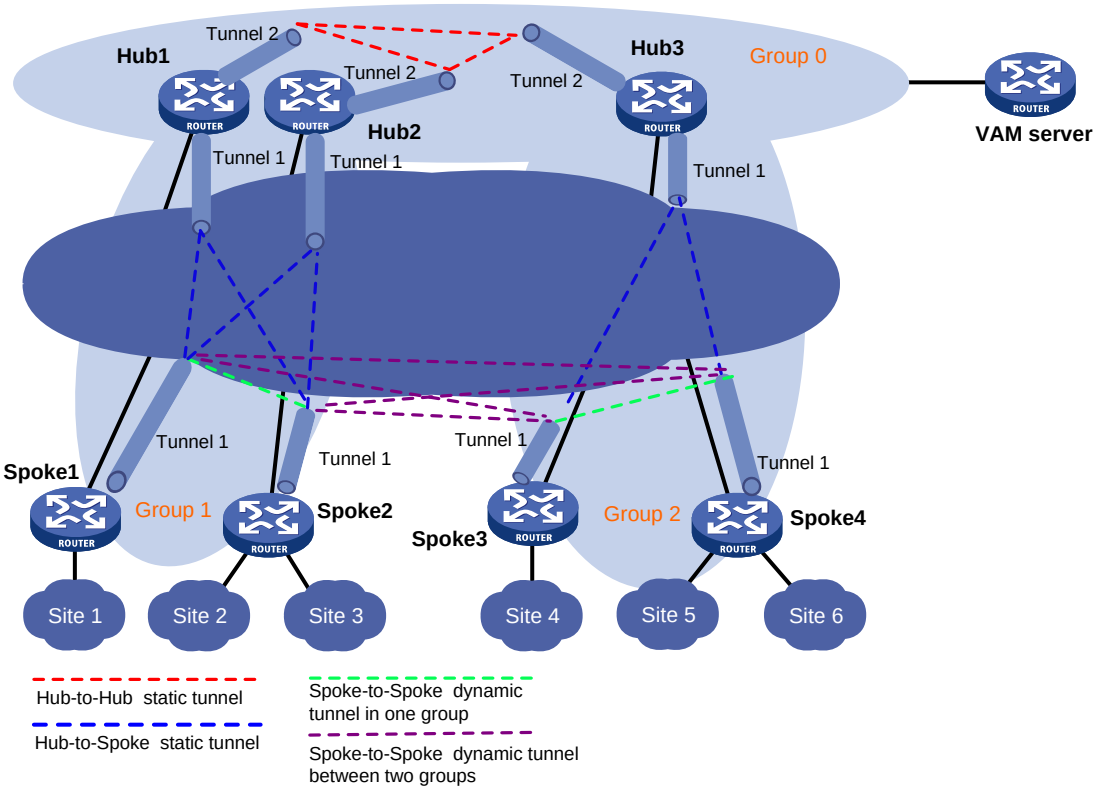
如 图 1-3 所示，划分多个Hub组网络中，Hub组的划分方式为：

- 所有 Hub 必须属于同一个 Hub 组，该 Hub 组作为骨干区域。骨干区域采用 Full-Mesh 组网，即 Hub 向 VAM Server 注册后获得骨干区域中所有 Hub 的信息，并在每两个 Hub 之间都建立永久的 ADVPN 隧道。
- 将 Spoke 部署到除骨干区域外的其他 Hub 组中。这些 Hub 组内至少有 1 个 Hub，可以使用 Full-Mesh 组网也可以使用 Hub-Spoke 组网。Spoke 向 VAM Server 注册后获得 Spoke 所属 ADVPN 域所在 Hub 组中 Hub 的信息，并与 Hub 建立永久的 ADVPN 隧道。一个 Hub 组内的 Spoke 只与本组的 Hub 建立 ADVPN 隧道，不与其他 Hub 组的 Hub 建立 ADVPN 隧道。

同一个 Hub 组内，隧道建立方式和数据转发方式由其组网方式决定。不同 Hub 组间，数据需要通过本组的 Hub 转发到目的组的 Hub，再由目的组 Hub 转发到对应的 Spoke。

为了减少 Hub 跨组转发数据时的压力，可以允许不同组的 Spoke 直接建立隧道，但该隧道是动态的，当在一段时间（Spoke-Spoke 隧道空闲超时时间）内没有数据报文交互时，则删除该隧道。

图1-3 划分多个 Hub 组网络示意图



1.1.2 ADVPN工作机制

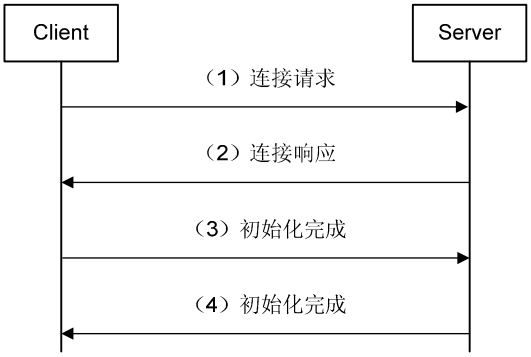
ADVPN 对 VAM Server 和 VAM Client 的地址具有一定要求：

- VAM Server 只需要具有公网地址，且该公网地址必须静态配置，不能动态变化。
- VAM Client 需要具有公网地址和私网地址。公网地址是 VAM Client 连接 IP 核心网络的接口的地址，既可以静态配置也可以动态获取。私网地址是 ADVPN 隧道接口的地址，必须静态配置。在同一个 ADVPN 域内，同一个 Hub 组内的 VAM Client 的私网地址应该属于同一个网段。

ADVPN 的关键是通过 VAM Client 的私网地址获取动态变化的公网地址，以便建立 ADVPN 隧道、转发报文。ADVPN 的工作过程分为连接初始化、注册、隧道建立、路由学习和报文转发四个阶段，下面对这四个阶段做简单说明。

1. 连接初始化阶段

图1-4 连接初始化流程图



如 图 1-4 所示，连接初始化阶段用来协商完整性验证、加密算法及密钥，其过程为：

(1) Client 通过连接请求报文将自己支持的完整性验证算法、加密算法等发送给 Server。

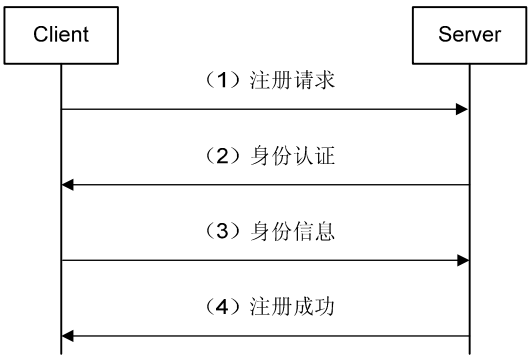
(2) Server 按照优先级从高到低的顺序从自己支持的算法列表中依次选择算法，与 Client 发送的算法列表进行匹配。如果存在相同的算法，则 Server 通过连接响应报文将该算法发送给 Client；如果不存在相同的算法，则算法协商失败，断开连接。

(3) 如果协商结果为不对 VAM 协议报文进行加密或认证（Server 上配置不需要加密或认证），则 Server 和 Client 不必生成加密密钥或完整性验证密钥。否则，Server 和 Client 都根据预共享密钥生成加密密钥和完整性验证密钥。

(4) Client 和 Server 分别利用生成的加密密钥和完整性验证密钥对初始化完成报文进行保护，并发送给对端。如果对端能够正确解密和验证该报文，则算法、密钥协商成功，后续的 VAM 协议报文都通过协商的算法和密钥进行保护。否则，协商失败，断开连接。

2. 注册阶段

图1-5 注册流程图



如 图 1-5 所示，注册阶段的具体过程为：

(1) Client 向 Server 发送注册请求报文，注册请求报文中包括 Client 的公网地址、私网地址、连接的私网网段等信息。

(2) Server 收到注册请求报文后，根据配置决定是否对该 Client 进行身份认证。如果配置为不认证，则直接注册 Client 信息并向 Client 发送注册成功响应；如果配置为认证，Server 向 Client 回应身份认证请求，并指明需要的认证方法。VAM 支持 PAP 和 CHAP 两种认证方式。

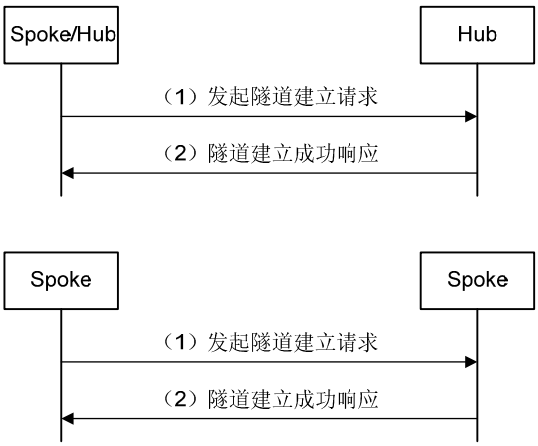
(3) Client 向 Server 提交自己的身份信息。

(4) Server 通过 AAA 对 Client 进行认证和计费。认证和计费成功后，Server 向 Client 发送注册成功响应报文，注册成功报文中携带 Server 下发给 Client 的 Hub 信息。

3. 隧道建立阶段

Spoke要和Hub建立永久隧道，一个Spoke可以和任意多个Hub建立永久隧道。如果在一个ADVPN域中有多个Hub，则Hub之间需要建立永久隧道。具体隧道建立流程如 图 1-6 所示。

图1-6 隧道建立流程图



(1) 发起隧道建立请求

- Hub-Spoke 隧道：Spoke 收到 Server 下发的 Hub 信息后，检查与这些 Hub 之间是否存在隧道。如果隧道不存在，则向 Hub 发送隧道建立请求报文。
- Hub-Hub 隧道：Hub 收到 Server 下发的已注册成功的 Hub 信息后，检查与这些 Hub 之间是否存在隧道。如果隧道不存在，则向其发送隧道建立请求报文。
- Spoke-Spoke 隧道：在 Full-Mesh 组网中，Spoke 收到某个数据报文后，若没有查到相应的能够转发该报文的隧道，则会向 Server 发送地址解析请求，根据得到的地址解析响应向对端 Spoke 发起隧道建立请求。

(2) 隧道对端收到隧道建立请求后，保存隧道信息，并向请求发起方发送隧道建立成功响应报文。

4. 路由学习和报文转发阶段

ADVPN 节点可以通过以下两种方式学习私网路由：

- 通过静态或动态路由协议学习：ADVPN 网络连接的各个私网及 ADVPN 隧道接口上都需要配置静态路由或动态路由协议，实现私网路由的连通。ADVPN 隧道建立以后，路由协议通过隧道进行邻居发现、路由更新，并建立路由表。ADVPN 隧道可以看作是私网中的一条普通链路，负责连接不同的私网网段。完成私网路由的学习后，Spoke 接收到它连接的私网用户访问其他私网的报文时，查找路由表找到私网下一跳的地址。Spoke 通过 VAM Server 查询私网下一

跳对应的公网地址，并将该公网地址作为隧道的目的地址对报文进行封装。封装后的报文通过 ADVPN 隧道发送给对端。

- 向 VAM Server 注册和查询私网网段：ADVPN 节点将本地连接的私网网段信息注册到 VAM Server。Spoke 接收到它连接的私网用户访问其他私网的报文时，将报文的目的地址发送给 VAM Server，通过 VAM Server 查询连接该目的地址所在私网网段的 ADVPN 节点的信息（包括 ADVPN 节点的公网和私网地址），并在本地生成到达该私网网段的路由，路由下一跳为该 ADVPN 节点。完成查询后，Spoke 将查询到的 ADVPN 节点的公网地址作为隧道的目的地址对报文进行封装。封装后的报文通过 ADVPN 隧道发送给对端。

在 ADVPN 网络中，如果同时使用了上述两种私网路由学习方式，则 Spoke 接收到它连接的私网用户访问其他私网的报文时，会同时将私网路由的下一跳地址和报文的目的地址发送给 VAM Server，VAM Server 优先根据目的地址进行查询，即优先采用向 VAM Server 注册和查询私网网段方式。如果同时通过上述两种方式学习到了到达同一私网网段的路由，则优先选择路由优先级小的路由转发报文。

说明

- 路由协议只在 Hub 和 Spoke 以及各 Hub 之间进行交互，在 Spoke 与 Spoke 之间不直接交换路由信息。
- ADVPN 组网采用的是 Full-Mesh 网络还是 Hub-Spoke 网络，由路由决定。如果学习到的路由下一跳是对端 Spoke，则为 Full-Mesh 网络；如果学习到的路由下一跳是 Hub，则为 Hub-Spoke 网络。

1.1.3 ADVPN对NAT的支持

当隧道发起方在 NAT 网关后侧时，则可以建立穿越 NAT 的 Spoke-Spoke 隧道；如果隧道接收方在 NAT 网关后侧，则数据包要由 Hub 转发，直到接收方发起隧道建立请求。如果双方都在 NAT 网关后侧，则它们都无法与对方建立隧道，所有的数据包都只能从 Hub 转发。

如果 NAT 网关采用 Endpoint-Independent Mapping（不关心对端地址和端口转换模式），隧道接收方在 NAT 网关后侧时，也可以建立穿越 NAT 的 Spoke-Spoke 隧道。

1.2 ADVPN配置任务简介

搭建 ADVPN 网络时，一般先配置 VAM Server，然后配置 Hub 设备，最后配置 Spoke 设备。

表1-1 ADVPN 配置任务简介

配置任务		说明	详细配置
VAM Server端的配置	配置AAA	可选	1.3
	配置VAM Server	必选	1.4
VAM Client端的配置	配置VAM Client	必选	1.5
	配置ADVPN隧道	必选	1.6
	配置路由	必选	1.7

配置任务		说明	详细配置
	配置IPsec保护ADVPN隧道报文	可选	1.8

1.3 配置AAA

VAM Server 可以根据需要使用 AAA 对接入到 ADVPN 域的 VAM Client 进行身份认证，只有通过身份认证的 VAM Client 才可以接入到 ADVPN 域。

VAM Server 端 AAA 的具体配置请参见“安全配置指导”中的“AAA”。

1.4 配置VAM Server

1.4.1 VAM Server配置任务简介

表1-2 VAM Server 配置任务简介

配置任务	说明	详细配置
创建ADVPN域	必选	1.4.2
启动VAM Server功能	必选	1.4.3
配置VAM Server的预共享密钥	必选	1.4.4
配置Hub组	必选	1.4.5
配置VAM Server的监听端口号	可选	1.4.6
配置VAM协议报文的安全参数	可选	1.4.7
配置对VAM Client的身份认证方式	可选	1.4.8
配置Keepalive报文参数	可选	1.4.9
配置请求报文重传参数	可选	1.4.10

1.4.2 创建ADVPN域

创建 ADVPN 域时必须指定一个唯一的 ID。进入已经创建的 ADVPN 域时，不需要指定 ID。

表1-3 创建 ADVPN 域

操作	命令	说明
进入系统视图	**system-view**	-
创建ADVPN域，并进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	缺省情况下，设备上不存在任何ADVPN域

1.4.3 启动VAM Server功能

该配置用来启动服务器端 ADVPN 域的 VAM Server 功能。

表1-4 启动 VAM Server 功能

操作		命令	说明
进入系统视图		**system-view**	-
启动VAM Server功能	启动所有或指定ADVPN域的VAM Server功能	**vam server enable** [**advpn-domain** *domain-name*]	二者选其一 缺省情况下，VAM Server功能处于关闭状态
	启动指定ADVPN域的VAM Server功能	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	
		server enable	

1.4.4 配置VAM Server的预共享密钥

预共享密钥用于生成加密/完整性验证的密钥：

- 在连接初始化阶段预共享密钥用来生成验证和加密连接请求、连接响应报文的初始密钥。
- 如果选择对后续的报文进行加密和验证，则预共享密钥还用来生成验证和加密后续报文的连接密钥。

同一个 ADVPN 域内的 VAM Server 和 VAM Client 上配置的预共享密钥必须一致。VAM Client/VAM Server 通过报文解密、完整性验证是否成功，可以判断二者的预共享密钥是否相同，从而实现对 VAM Server/VAM Client 的身份认证。

表1-5 配置 VAM Server 的预共享密钥

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
配置VAM Server的预共享密钥	**pre-shared-key** { **cipher** *cipher-string* | **simple** *simple-string* }	缺省情况下，未配置VAM Server的预共享密钥

1.4.5 配置Hub组

在大规模组网情况下，将 ADVPN 域划分为多个 Hub 组可以方便管理。创建 Hub 组后，可以按照 Spoke 的私网地址网段或地址范围，将 Spoke 划分到不同的 Hub 组中，并为每个 Hub 组指定一个或多个 Hub。

当 VAM Client 向 VAM Server 注册时，根据 VAM Client 的私网地址将 VAM Client 划分到对应的 ADVPN 域 Hub 组中：

(1) 根据 Hub 组名称字典序依次匹配各 Hub 组内配置的 Hub 私网地址。

(2) 如果匹配上，则 VAM Client 为 Hub，并被划分到该 Hub 组；如果 VAM Client 不是 Hub，再根据 Hub 组名称字典序依次匹配各 Hub 组内配置的 Spoke 私网地址范围。

(3) 如果匹配上，则VAM Client为Spoke，并被划分到该Hub组；否则，VAM Client既不是Hub也不是Spoke，注册失败。

VAM Server只向VAM Client下发其所属的Hub组内的Hub信息。VAM Client只与本Hub组内的Hub建立永久ADVPN隧道。

1. 创建Hub组

表1-6 创建 Hub 组

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
创建Hub组，并进入Hub组视图	**hub-group** *group-name*	缺省情况下，不存在Hub组

2. 配置Hub组内的Hub私网地址

每个Hub组必须至少配置一个Hub私网地址。

表1-7 配置 Hub

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
进入Hub组视图	**hub-group** *group-name*	-
配置Hub的私网地址	**hub private-address** *private-ip-address* [**public-address** { *public-ip-address* | *public-ipv6-address* } [**advpn-port** *port-number*]]	二者选其一 缺省情况下，Hub组内没有配置Hub私网地址
	hub ipv6 private-address *private-ipv6-address* [**public-address** { *public-ip-address* | *public-ipv6-address* } [**advpn-port** *port-number*]]	

3. 配置Hub组内的Spoke私网地址范围

每个Hub组可以配置多个Spoke的IPv4和IPv6私网地址范围，将按照地址从低到高的顺序排列。

表1-8 配置 Spoke 的地址范围

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
进入Hub组视图	**hub-group** *group-name*	-
配置Spoke的私网地址范围	**spoke private-address** { **network** *ip-address* { *mask-length* | *mask* } | **range** *start-address end-address* }	二者选其一 缺省情况下，Hub组内没有配置

操作	命令	说明
	spoke ipv6 private-address { **network** *prefix prefix-length* | **range** *start-ipv6-address end-ipv6-address* }	Spoke的私网地址范围

4. 配置跨Hub组建立Spoke-Spoke直连隧道的规则

如果配置了跨 Hub 组建立 Spoke-Spoke 直连隧道的规则，则在 Hub 上线后，VAM Server 将指定的规则下发到 Hub。在 Hub 转发私网数据报文的同时，会将数据报文与收到的规则进行匹配。如果匹配成功，Hub 向发送该数据报文的 Spoke 发送重定向报文。Spoke 收到重定向报文后，将被重定向的数据报文的目的地址发送给 VAM Server，向 VAM Server 查询连接该目的地址所在私网网段的 Spoke 节点的信息，并与该 Spoke 建立直连隧道。

跨 Hub 组 Spoke-Spoke 直连隧道建立前，数据报文仍由 Hub 进行转发。直连隧道建立后，数据报文将直接发送到直连路由下一跳所对应的 Spoke，而不再经过 Hub 中转。

表1-9 配置跨 Hub 组建立 Spoke-Spoke 直连隧道的规则

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
进入Hub组视图	**hub-group** *group-name*	-
配置跨Hub组建立Spoke-Spoke直连隧道的规则	**shortcut interest** { **acl** { *acl-number* | **name** *acl-name* } | **all** }	二者选其一 缺省情况下，没有配置跨Hub组建立Spoke-Spoke直连隧道的规则，不允许跨Hub组建立Spoke-Spoke直连隧道
	shortcut ipv6 interest { **acl** { *ipv6-acl-number* | **name** *ipv6-acl-name* } | **all** }	

1.4.6 配置VAM Server的监听端口号

VAM Server 的监听端口号与 VAM Client 上指定的 VAM Server 的端口号必须一致。

表1-10 配置监听端口号

操作	命令	说明
进入系统视图	**system-view**	-
配置VAM Server的监听端口号	**vam server listen-port** *port-number*	缺省情况下，VAM Server的监听端口号为18000

1.4.7 配置VAM协议报文的安全参数

该配置用来设置 VAM 协议报文的验证、加密算法。VAM Server 根据配置的报文完整性验证、加密算法以及优先级与 VAM Client 发送的算法列表进行协商，协商后的算法分别作为两端协议报文的完整性验证算法和加密算法。

需要注意的是：

- VAM Server 与 VAM Client 固定使用 SHA-1 验证算法和 AES-CBC-128 加密算法对连接初始化请求和响应报文进行完整性验证和加密；使用协商出来的验证算法和加密算法对其他 VAM 协议报文进行完整性验证和加密。
- 验证/加密算法在配置中的出现顺序决定其使用优先级。配置中越靠前的验证/加密算法，其优先级越高。
- 修改验证/加密算法对已经注册的 VAM Client 没有影响，新注册的 VAM Client 将采用修改后的算法进行协商。

表1-11 配置 VAM 协议报文的安全参数

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
配置VAM协议报文的验证算法	**authentication-algorithm** { **aes-xcbc-mac** | **md5** | **none** | **sha-1** | **sha-256** } *	缺省情况下，VAM协议报文的验证算法为SHA-1
配置VAM协议报文的加密算法	**encryption-algorithm** { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **des-cbc** | **none** } *	缺省情况下，按照优先级由高到低依次使用AES-CBC-256、AES-CBC-192、AES-CBC-128、AES-CTR-256、AES-CTR-192、AES-CTR-128、3DES-CBC、DES-CBC算法

1.4.8 配置对VAM Client的身份认证方式

该配置用来设置 VAM Server 对 VAM Client 的认证方式。目前，只支持 PAP 和 CHAP 两种身份验证方式。

需要注意的是：

- 如果配置时指定的认证 ISP 域不存在，则 VAM Server 对 VAM Client 的身份认证会失败。
- 修改认证方式对已经注册的 VAM Client 没有影响，新注册的 VAM Client 将按照修改后的认证方式进行身份认证。

表1-12 配置对 VAM Client 的身份认证方式

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
配置VAM Server对VAM Client的身份认证方式	**authentication-method** { **none** | { **chap** | **pap** } [**domain** *isp-name*] }	缺省情况下，VAM Server使用CHAP方式，对VAM Client进行身份认证，认证使用的ISP域为用户配置的系统默认域

1.4.9 配置Keepalive报文参数

VAM Client 和 VAM Server 之间通过 Keepalive 报文保持联系。该配置用来设置 VAM Client 发送 Keepalive 报文的时间间隔和重发次数。当 VAM Client 注册成功后，VAM Server 会将配置的参数在注册响应中下发给 VAM Client，同一个 ADVPN 域中所有 VAM Client 的 Keepalive 报文参数都是相同的。

VAM Client 按照 VAM Server 指定的时间间隔向 VAM Server 发送 Keepalive 报文，VAM Server 收到 Keepalive 报文后回复响应报文。当 Keepalive 报文的重发次数达到指定的值仍没有收到 VAM Server 的响应时，VAM Client 认为与 VAM Server 的连接中断，不再发送 Keepalive 报文。当 VAM Server 在时间间隔×重发次数的时间内没有收到 VAM Client 的 Keepalive 报文，则认为与 VAM Client 的连接中断，会删除该 VAM Client 的信息并将其下线。

需要注意的是：

- 如果 VAM Server 改变 Keepalive 报文参数，则修改后的参数只对新注册的 VAM Client 生效，已经注册的 VAM Client 不受影响。
- 如果 VAM Server 与 VAM Client 间存在配置了动态 NAT 的设备，则 Keepalive 报文的发送时间间隔应小于 NAT 表项的老化时间，从而保证 NAT 表项不会老化。

表1-13 配置 Keepalive 报文参数

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
配置VAM Client向VAM Server发送Keepalive报文的时间间隔和重试次数	**keepalive interval** *time-interval* **retry** *retry-times*	缺省情况下，VAM Client发送Keepalive报文的时间间隔为180秒，重试次数是3次

1.4.10 配置请求报文重传参数

VAM Server 向 VAM Client 发送请求报文后，如果在指定的时间间隔内没有收到响应报文，VAM Server 将重新发送该请求报文，直到收到响应报文或者 VAM Client Keepalive 超时（即 VAM Server 在 Keepalive 报文发送时间间隔×重发次数的时间内没有收到 VAM Client 的 Keepalive 报文）为止。

表1-14 配置报文重传参数

操作	命令	说明
进入系统视图	**system-view**	-
进入ADVPN域视图	**vam server advpn-domain** *domain-name* [**id** *domain-id*]	-
配置VAM Server重发请求报文的时间间隔	**retry interval** *time-interval*	缺省情况下，VAM Server重发请求报文的时间间隔为5秒

1.5 配置VAM Client

1.5.1 VAM Client配置任务简介

表1-15 VAM Client 配置任务简介

配置任务	说明	详细配置
创建VAM Client	必选	1.5.2
启动VAM Client功能	必选	1.5.3
配置VAM Server的地址	必选	1.5.4
配置VAM Client所属的ADVPN域	必选	1.5.5
配置VAM Client的预共享密钥	必选	1.5.6
配置请求报文重传参数	可选	1.5.7
配置VAM Client连接超时的静默时间	可选	1.5.8
配置认证用户名和密码	可选	1.5.9

1.5.2 创建VAM Client

表1-16 创建 VAM Client

操作	命令	说明
进入系统视图	**system-view**	-
创建VAM Client，并进入VAM Client视图	**vam client name** *client-name*	缺省情况下，没有配置VAM Client

1.5.3 启动VAM Client功能

表1-17 启动 VAM Client 功能

操作		命令	说明
进入系统视图		**system-view**	-
启动VAM Client功能	启动所有或指定VAM Client的VAM Client功能	**vam client enable** [**name** *client-name*]	二者选其一 缺省情况下，VAM Client的VAM Client功能处于关闭状态
	启动指定VAM Client的VAM Client功能	**vam client name** *client-name*	
		client enable	

1.5.4 配置VAM Server的地址

可以为一个 VAM Client 配置两个 VAM Server，一个主 VAM Server，一个备 VAM Server。VAM Client 会同时向主 VAM Server 和备 VAM Server 进行注册，如果都注册成功，VAM Client 会优先使用先注册成功的 VAM Server 向其下发的信息。当该 VAM Server 故障时，VAM Client 再使用另外一个 VAM Server 下发的信息。

需要注意的是：

- 如果主 VAM Server 和备 VAM Server 的地址相同（配置了相同的地址或通过域名解析到相同的地址），则只有主 VAM Server 有效。
- VAM Client 上指定的 VAM Server 端口号，必须和 VAM Server 上配置的监听端口号一致。

表1-18 配置 VAM Server 的地址

操作	命令	说明
进入系统视图	**system-view**	-
进入VAM Client视图	**vam client name** *client-name*	-
配置主VAM Server的地址	**server primary** { **ip-address** *ip-address* | **ipv6-address** *ipv6-address* | **name** *host-name* } [**port** *port-number*]	缺省情况下，没有配置主VAM Server的地址
（可选）配置备VAM Server的地址	**server secondary** { **ip-address** *ip-address* | **ipv6-address** *ipv6-address* | **name** *host-name* } [**port** *port-number*]	缺省情况下，没有配置备VAM Server的地址

1.5.5 配置VAM Client所属的ADVPN域

表1-19 配置 VAM Client 所属的 ADVPN 域

操作	命令	说明
进入系统视图	**system-view**	-
进入VAM Client视图	**vam client name** *client-name*	-
配置VAM Client所属的ADVPN域	**advpn-domain** *domain-name*	缺省情况下，VAM Client不属于任何ADVPN域

1.5.6 配置VAM Client的预共享密钥

预共享密钥用于生成加密/完整性验证的密钥：

- 在连接初始化阶段预共享密钥用来生成验证和加密连接请求、连接响应报文的初始密钥。
- 如果选择对后续的报文进行加密和验证，则预共享密钥还用来生成验证和加密后续报文的连接密钥。

同一个 ADVPN 域内的 VAM Client 和 VAM Server 上配置的预共享密钥必须一致。VAM Client/VAM Server 通过报文解密、完整性验证是否成功，可以判断二者的预共享密钥是否相同，从而实现对 VAM Server/VAM Client 的身份认证。

表1-20 配置 VAM Client 的预共享密钥

操作	命令	说明
进入系统视图	**system-view**	-
进入VAM Client视图	**vam client name** *client-name*	-
配置VAM Client的预共享密钥	**pre-shared-key** { **cipher** *cipher-string* | **simple** *simple-string* }	缺省情况下，无预共享密钥

1.5.7 配置请求报文重传参数

VAM Client 向 VAM Server 发送请求报文后，如果在指定的时间间隔内没有收到响应报文，VAM Client 将重新发送请求报文。如果重新发送请求报文的次数超过指定的重发次数，则 VAM Client 认为 VAM Server 不可达。

需要注意的是：

- 私网注册请求报文和节点信息更新请求报文不受重发次数的限制，将会按照指定的时间间隔一直发送，直至 VAM Client 下线。
- VAM Client 发送 Keepalive 报文的时间间隔和重发次数由 VAM Server 的配置决定。

表1-21 配置 VAM 协议报文重传参数

操作	命令	说明
进入系统视图	**system-view**	-
进入VAM Client视图	**vam client name** *client-name*	-
配置VAM协议报文重传参数	**retry interval** *time-interval* **count** *retry-times*	缺省情况下，VAM协议报文重发间隔时间为5秒，重传次数为3次

1.5.8 配置VAM Client连接超时的静默时间

VAM Client 在与 VAM Server 连接超时后，会进入静默状态，此时 VAM Client 不处理任何报文。当静默时间到达后，VAM Client 将重新发起连接请求。

表1-22 配置 VAM Client 连接超时的静默时间

操作	命令	说明
进入系统视图	**system-view**	-
进入VAM Client视图	**vam client name** *client-name*	-
配置VAM Client连接超时的静默时间	**dumb-time** *time-interval*	缺省情况下，VAM Client连接超时的静默时间为120秒

1.5.9 配置认证用户名和密码

配置 VAM Client 的用户名和密码，用于向 VAM Server 进行身份认证。

表1-23 配置认证用户和密码

操作	命令	说明
进入系统视图	**system-view**	-
进入VAM Client视图	**vam client name** *client-name*	-
配置认证用户名和密码	**user** *username* **password** { **cipher** *cipher-string* | **simple** *simple-string* }	缺省情况下，没有配置认证用户名和密码

1.6 配置ADVPN隧道

关于 Tunnel 接口的详细介绍，请参见“三层技术-IP 业务配置指导”中的“隧道”。关于 **interface tunnel**、**source** 和 **tunnel dfbit enable** 命令以及 Tunnel 接口下更多配置命令的详细介绍，请参见“三层技术-IP 业务命令参考”中的“隧道”。

表1-24 配置 ADVPN 隧道

操作	命令	说明
进入系统视图	**system-view**	-
创建ADVPN隧道类型的Tunnel接口，并进入Tunnel接口视图	**interface tunnel** *number* [**mode advpn** { **gre** | **udp** } [**ipv6**]]	缺省情况下，设备上不存在任何Tunnel接口 在隧道的两端应配置相同的隧道模式，否则可能造成报文传输失败
配置Tunnel接口的私网地址	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	二者至少选其一 缺省情况下，Tunnel接口上没有配置私网地址 在同一个Hub组中，所有Tunnel接口的地址应该配置为同一个网段
	ipv6 address *ipv6-address prefix-length*	
配置ADVPN隧道的源端地址或源接口	**source** { *ip-address* | *interface-type interface-number* }	缺省情况下，没有配置ADVPN隧道的源端地址和源接口 如果设置的是源端地址，则该地址将作为封装后隧道报文的源地址；如果设置的是源接口，则该接口的地址将作为封装后隧道报文的源地址
（可选）设置封装后隧道报文的DF（Don’t Fragment，不分片）标志	**tunnel dfbit enable**	缺省情况下，未设置隧道报文的不分片标志，即转发隧道报文时允许分片
（可选）配置ADVPN报文的源UDP端口号	**advpn source-port** *port-number*	缺省情况下，ADVPN报文的源UDP端口号为18001 本命令只有在UDP封装模式的ADVPN隧道类型的Tunnel接口下才能配置 如果Tunnel接口下执行**vam client**命令时指定了**compatible**参数，则该Tunnel接口配置的源端口号必须和其他Tunnel接口不同

操作	命令	说明
配置Tunnel接口绑定的VAM Client	**vam client** *client-name* [**compatible advpn0**]	缺省情况下，Tunnel隧道接口没有绑定任何VAM Client 一个VAM Client只能与一个IPv4 ADVPN类型的Tunnel接口绑定 一个VAM Client只能与一个IPv6 ADVPN隧道类型的Tunnel接口绑定
	vam ipv6 client *client-name*	
（可选）配置ADVPN隧道的私网信息	**advpn network** *ip-address* { *mask-length* | *mask* } [**preference** *preference-value*]	缺省情况下，没有配置ADVPN隧道的私网信息 私网路由的优先级建议高于其他动态路由协议，低于静态路由
	advpn ipv6 network *prefix prefix-length* [**preference** *preference-value*]	
（可选）配置ADVPN隧道的Keepalive报文发送周期及最大发送次数	**keepalive interval** *time-interval* **retry** *retry-times*	缺省情况下，ADVPN隧道的Keepalive报文发送周期为180秒，最大发送次数为3次 在同一个ADVPN域中，所有Tunnel接口的Keepalive报文发送周期及最大发送次数必须一致
（可选）配置Spoke-Spoke类型ADVPN隧道的空闲超时时间	**advpn session idle-time** *time-interval*	缺省情况下，Spoke-Spoke类型ADVPN隧道的空闲超时时间为600秒 修改此参数，已经建立的Spoke-Spoke类型ADVPN隧道会使用修改后的参数值重新开始计时
（可选）配置ADVPN隧道建立失败的静默时间	**advpn session dumb-time** *time-interval*	缺省情况下，ADVPN隧道建立失败的静默时间为120秒 修改此参数后，已经建立的ADPVN隧道不会改变静默时间，之后建立的ADPVN隧道会使用修改后的静默时间

说明

如果设备上配置了多个使用 GRE 封装的 ADVPN 隧道接口，且隧道的源端地址或源接口相同时，不同 GRE 封装的 ADVPN 隧道接口的 GRE Key 必须不同。关于 GRE Key 的详细介绍请参见“三层技术-IP 业务配置指导”中的“GRE”。

1.7 配置路由

ADVPN 客户端 IPv4 私网支持的路由协议为 OSPF、RIP 和 BGP：

- 采用 OSPF 路由协议时，如果是 Full-Mesh 网络，OSPF 接口的网络类型需要配置为 **broadcast**；如果是 Hub-Spoke 网络，OSPF 接口的网络类型需要配置为 **p2mp**。OSPF 的具体配置请参见“三层技术-IP 路由配置指导”中的“OSPF”。

- 采用 RIP 路由协议时，如果是 Full-Mesh 网络，可以使用 RIP-1 或 RIP-2 广播方式；如果是 Hub-Spoke 网络，需要使用 RIP-2 组播方式，并且关闭水平分割功能。RIP 的具体配置请参见“三层技术-IP 路由配置指导”中的“RIP”。
- 采用 BGP 路由协议时，如果是 Full-Mesh 网络，需要通过路由策略等配置，保证一端 Spoke 学习到的到达对端私网路由的下一跳为对端 Spoke 的地址（EBGP 不支持 Full-Mesh 网络）；如果是 Hub-Spoke 网络，需要通过路由策略等配置，保证一端 Spoke 学习到的到达对端私网路由的下一跳为 Hub 的地址。BGP 和路由策略的具体配置请参见“三层技术-IP 路由配置指导”中的“BGP”和“路由策略”。

ADVPN 客户端 IPv6 私网支持的路由协议为 OSPFv3、RIPng 和 IPv6 BGP：

- 采用 OSPFv3 路由协议时，如果是 Full-Mesh 网络，OSPFv3 接口的网络类型需要配置为 **broadcast**；如果是 Hub-Spoke 网络，OSPFv3 接口的网络类型需要配置为 **p2mp**。OSPFv3 的具体配置请参见“三层技术-IP 路由配置指导”中的“OSPFv3”
- 采用 RIPng 路由协议时，只支持 Full-Mesh 网络。RIPng 的具体配置请参见“三层技术-IP 路由配置指导”中的“RIPng”
- 采用 IPv6 BGP 路由协议时，如果是 Full-Mesh 网络，需要通过路由策略等配置，保证一端 Spoke 学习到的到达对端私网路由的下一跳为对端 Spoke 的地址（EBGP 不支持 Full-Mesh 网络）；如果是 Hub-Spoke 网络，需要通过路由策略等配置，保证一端 Spoke 学习到的到达对端私网路由的下一跳为 Hub 的地址。IPv6 BGP 和路由策略的具体配置请参见“三层技术-IP 路由配置指导”中的“BGP”和“路由策略”。

1.8 配置IPsec保护ADVPN隧道报文

设备支持用 IPsec 安全框架来保护 ADVPN 隧道数据报文和控制报文的传递，其基本配置思路如下：

(1) 配置 IPsec 安全提议：指定安全协议、认证算法和加密算法、封装模式等。

(2) 配置 IKE 协商方式的 IPsec 安全框架。

(3) 在 ADVPN 隧道接口上应用 IKE 协商方式的 IPsec 安全框架。

详细配置请参见“安全配置指导”中的“IPsec”。

1.9 ADVPN显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 ADVPN 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除相应的统计信息。

表1-25 ADVPN 显示和维护

操作	命令
显示注册到VAM Server上的VAM Client的IPv4私网地址和公网地址映射信息	**display vam server address-map** [**advpn-domain** *domain-name* [**private-address** *private-ip-address*]] [**verbose**]
显示注册到VAM Server上的VAM Client的IPv6私网地址和公网地址映射信息	**display vam server ipv6 address-map** [**advpn-domain** *domain-name* [**private-address** *private-ipv6-address*]] [**verbose**]

操作	命令
显示注册到VAM Server上的VAM Client的IPv4私网信息	**display vam server private-network** [**advpn-domain** *domain-name* [**private-address** *private-ip-address*]]
显示注册到VAM Server上的VAM Client的IPv6私网信息	**display vam server ipv6 private-network** [**advpn-domain** *domain-name* [**private-address** *private-ipv6-address*]]
显示VAM Server上ADVPN域的统计信息	**display vam server statistics** [**advpn-domain** *domain-name*]
显示VAM Client的状态机信息	**display vam client fsm** [**name** *client-name*]
显示VAM Client的统计信息	**display vam client statistics** [**name** *client-name*]
显示VAM Client收到的VAM Server下发的跨Hub组建立IPv4 Spoke-Spoke直连隧道的规则	**display vam client shortcut interest** [**name** *client-name*]
显示VAM Client收到的VAM Server下发的跨Hub组建立IPv6 Spoke-Spoke直连隧道的规则	**display vam client shortcut ipv6 interest** [**name** *client-name*]
显示IPv4 ADVPN隧道的信息	**display advpn session** [**interface tunnel** *number* [**private-address** *private-ip-address*]] [**verbose**]
显示IPv6 ADVPN隧道的信息	**display advpn ipv6 session** [**interface tunnel** *number* [**private-address** *private-ipv6-address*]] [**verbose**]
清除注册到VAM Server上的IPv4私网地址和公网地址映射信息	**reset vam server address-map** [**advpn-domain** *domain-name* [**private-address** *private-ip-address*]]
清除注册到VAM Server上的IPv6私网地址和公网地址映射信息	**reset vam server ipv6 address-map** [**advpn-domain** *domain-name* [**private-address** *private-ipv6-address*]]
清除VAM Server上ADVPN域的统计信息	**reset vam server statistics** [**advpn-domain** *domain-name*]
重置VAM Client的状态机	**reset vam client** [**ipv6**] **fsm** [**name** *client-name*]
清除VAM Client的统计信息	**reset vam client statistics** [**name** *client-name*]
删除IPv4 ADVPN隧道	**reset advpn session statistics** [**interface tunnel** *number* [**private-address** *private-ip-address*]]
删除IPv6 ADVPN隧道	**reset advpn ipv6 session statistics** [**interface tunnel** *number* [**private-address** *private-ipv6-address*]]
清除IPv4 ADVPN隧道的统计信息	**reset advpn session statistics** [**interface tunnel** *number* [**private-address** *private-ip-address*]]
清除IPv6 ADVPN隧道的统计信息	**reset advpn ipv6 session statistics** [**interface tunnel** *number* [**private-address** *private-ipv6-address*]]

1.10 ADVPN典型配置举例

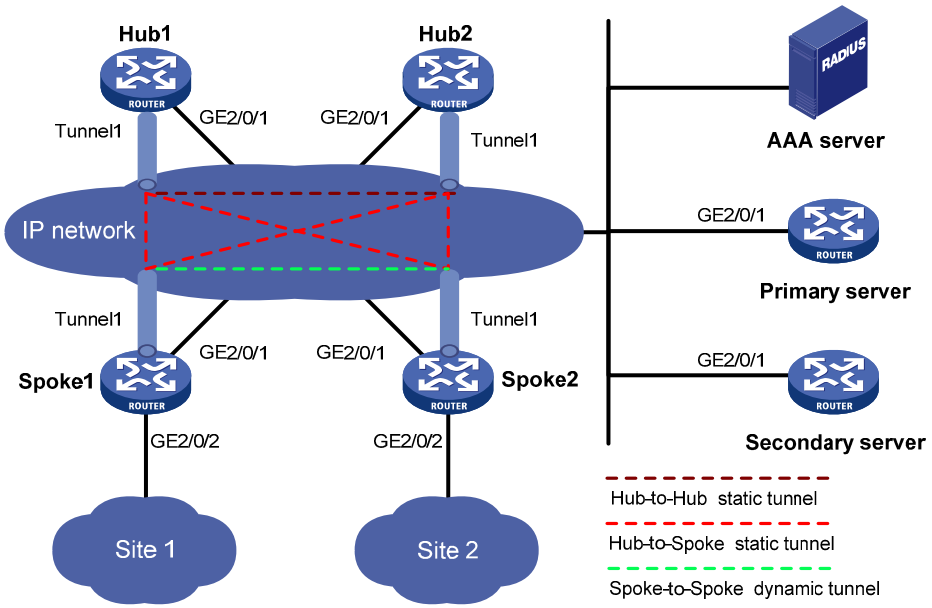
1.10.1 IPv4 Full-Mesh类型ADVPN典型配置举例

1. 组网需求

- 在 IPv4 Full-Mesh 的组网方式下，主、备 VAM Server 负责管理、维护各个节点的信息；AAA 服务器负责对 VAM Client 进行认证和计费管理；两个 Hub 互为备份，负责数据的转发和路由信息的交换。
- Spoke 与 Hub 之间建立永久的 ADVPN 隧道。
- 同一 ADVPN 域中，任意的两个 Spoke 之间在有数据时动态建立 ADVPN 隧道。

2. 组网图

图1-7 IPv4 Full-Mesh 类型 ADVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
Hub 1	GE2/0/1	1.0.0.1/24	Spoke 1	GE2/0/1	1.0.0.3/24
	Tunnel1	192.168.0.1/24		GE2/0/2	192.168.1.1/24
Hub 2	GE2/0/1	1.0.0.2/24		Tunnel1	192.168.0.3/24
	Tunnel1	192.168.0.2/24	Spoke 2	GE2/0/1	1.0.0.4/24
AAA server		1.0.0.10/24		GE2/0/2	192.168.2.1/24
Primary server	GE2/0/1	1.0.0.11/24		Tunnel1	192.168.0.4/24
Secondary server	GE2/0/1	1.0.0.12/24			

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
[PrimaryServer] radius scheme abc
```

```
[PrimaryServer-radius-abc] primary authentication 1.0.0.10 1812
[PrimaryServer-radius-abc] primary accounting 1.0.0.10 1813
[PrimaryServer-radius-abc] key authentication simple 123
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```

配置 ISP 域的 AAA 方案。

```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
[PrimaryServer] domain default enable abc
```

- 配置 VAM Server

创建 ADVPN 域 abc。

```
[PrimaryServer] vam server advpn-domain abc id 1
```

创建 Hub 组 0。

```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```

指定 Hub 组内 Hub 的 IPv4 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.1
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.2
```

指定 Hub 组内 Spoke 的 IPv4 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] spoke private-address network
192.168.0.0 255.255.255.0
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```

配置 VAM Server 的预共享密钥为 123456。

```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```

配置对 VAM Client 进行 CHAP 认证。

```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```

启动该 ADVPN 域的 VAM Server 功能。

```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```

(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1。

```
<Hub1> system-view
[Hub1] vam client name Hub1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub1-vam-client-Hub1] advpn-domain abc
```

配置 VAM Client 的预共享密钥为 123456。

```
[Hub1-vam-client-Hub1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub1，密码为 hub1。

```
[Hub1-vam-client-Hub1] user hub1 password simple hub1
```

配置 VAM Server 的 IP 地址。

```
[Hub1-vam-client-Hub1] server primary ip-address 1.0.0.11
[Hub1-vam-client-Hub1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1] client enable
[Hub1-vam-client-Hub1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub1] ike keychain abc
[Hub1-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub1-ike-keychain-abc] quit
[Hub1] ike profile abc
[Hub1-ike-profile-abc] keychain abc
[Hub1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub1] ipsec transform-set abc
[Hub1-ipsec-transform-set-abc] encapsulation-mode transport
[Hub1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub1-ipsec-transform-set-abc] quit
[Hub1] ipsec profile abc isakmp
[Hub1-ipsec-profile-isakmp-abc] transform-set abc
[Hub1-ipsec-profile-isakmp-abc] ike-profile abc
[Hub1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub1] ospf 1
[Hub1-ospf-1] area 0
[Hub1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub1-ospf-1-area-0.0.0.0] quit
[Hub1-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel1 mode advpn gre
[Hub1-Tunnel1] ip address 192.168.0.1 255.255.255.0
[Hub1-Tunnel1] vam client Hub1
[Hub1-Tunnel1] ospf network-type broadcast
[Hub1-Tunnel1] source gigabitethernet 2/0/1
[Hub1-Tunnel1] tunnel protection ipsec profile abc
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）

- 配置 VAM Client

创建 VAM Client Hub2。

```
<Hub2> system-view
[Hub2] vam client name Hub2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 Hub2，密码为 Hub2。

```
[Hub2-vam-client-Hub2] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2] server primary ip-address 1.0.0.11
[Hub2-vam-client-Hub2] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2] client enable
[Hub2-vam-client-Hub2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub2] ike keychain abc
[Hub2-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub2-ike-keychain-abc] quit
[Hub2] ike profile abc
[Hub2-ike-profile-abc] keychain abc
[Hub2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub2] ipsec transform-set abc
[Hub2-ipsec-transform-set-abc] encapsulation-mode transport
[Hub2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub2-ipsec-transform-set-abc] quit
[Hub2] ipsec profile abc isakmp
[Hub2-ipsec-profile-isakmp-abc] transform-set abc
[Hub2-ipsec-profile-isakmp-abc] ike-profile abc
[Hub2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub2] ospf 1
[Hub2-ospf-1] area 0
[Hub2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub2-ospf-1-area-0.0.0.0] quit
[Hub2-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub2] interface tunnel 1 mode advpn gre
[Hub2-Tunnel1] ip address 192.168.0.2 255.255.255.0
```

```
[Hub2-Tunnel1] vam client Hub2
[Hub2-Tunnel1] ospf network-type broadcast
[Hub2-Tunnel1] source gigabitethernet 2/0/1
[Hub2-Tunnel1] tunnel protection ipsec profile abc
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

(5) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。

```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。

```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```

配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ip-address 1.0.0.11
[Spoke1-vam-client-Spoke1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke1] ike keychain abc
[Spoke1-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke1-ike-keychain-abc] quit
[Spoke1] ike profile abc
[Spoke1-ike-profile-abc] keychain abc
[Spoke1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke1] ipsec transform-set abc
[Spoke1-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke1-ipsec-transform-set-abc] quit
[Spoke1] ipsec profile abc isakmp
[Spoke1-ipsec-profile-isakmp-abc] transform-set abc
[Spoke1-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke1] ospf 1
```

```
[Spoke1-ospf-1] area 0
[Spoke1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.0] quit
[Spoke1-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。将 Spoke1 的 DR 优先级配置为 0，以使 Spoke1 不参与 DR/BDR 选举。

```
[Spoke1] interface tunnel1 mode advpn gre
[Spoke1-Tunnel1] ip address 192.168.0.3 255.255.255.0
[Spoke1-Tunnel1] vam client Spoke1
[Spoke1-Tunnel1] ospf network-type broadcast
[Spoke1-Tunnel1] ospf dr-priority 0
[Spoke1-Tunnel1] source gigabitethernet 2/0/1
[Spoke1-Tunnel1] tunnel protection ipsec profile abc
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```

(6) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。

```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。

```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```

配置 VAM Server 的 IP 地址。

```
[Spoke2-vam-client-Spoke2] server primary ip-address 1.0.0.11
[Spoke2-vam-client-Spoke2] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke2] ike keychain abc
[Spoke2-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke2-ike-keychain-abc] quit
[Spoke2] ike profile abc
[Spoke2-ike-profile-abc] keychain abc
[Spoke2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke2] ipsec transform-set abc
[Spoke2-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke2-ipsec-transform-set-abc] quit
[Spoke2] ipsec profile abc isakmp
[Spoke2-ipsec-profile-isakmp-abc] transform-set abc
[Spoke2-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke2] ospf 1
[Spoke2-ospf-1] area 0
[Spoke2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.0] quit
[Spoke2-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。将 Spoke2 的 DR 优先级配置为 0，以使 Spoke2 不参与 DR/BDR 选举。

```
[Spoke2] interface tunnel1 mode advpn gre
[Spoke2-Tunnel1] ip address 192.168.0.4 255.255.255.0
[Spoke2-Tunnel1] vam client Spoke2
[Spoke2-Tunnel1] ospf network-type broadcast
[Spoke2-Tunnel1] ospf dr-priority 0
[Spoke2-Tunnel1] source gigabitethernet 2/0/1
[Spoke2-Tunnel1] tunnel protection ipsec profile abc
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[PrimaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    No   0H 52M  7S
0          192.168.0.2      1.0.0.2                   Hub    No   0H 47M 31S
0          192.168.0.3      1.0.0.3                   Spoke  No   0H 28M 25S
0          192.168.0.4      1.0.0.4                   Spoke  No   0H 19M 15S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[SecondaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    No   0H 52M  7S
0          192.168.0.2      1.0.0.2                   Hub    No   0H 47M 31S
```

```
0          192.168.0.3      1.0.0.3                    Spoke  No   0H 28M 25S
0          192.168.0.4      1.0.0.4                    Spoke  No   0H 19M 15S
```

以上显示信息表示 Hub1、Hub2、Spoke1 和 Spoke2 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv4 ADVPN 隧道信息。

```
[Hub1] display advpn session
Interface         : Tunnel1
Number of sessions: 3
Private address  Public address              Port  Type  State      Holding time
192.168.0.2      1.0.0.2                     --    H-H   Success    0H 46M  8S
192.168.0.3      1.0.0.3                     --    H-S   Success    0H 27M 27S
192.168.0.4      1.0.0.4                     --    H-S   Success    0H 18M 18S
```

以上显示信息表示 Hub1 与 Hub2、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv4 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address  Public address              Port  Type  State      Holding time
192.168.0.1      1.0.0.1                     --    S-H   Success    0H 46M  8S
192.168.0.2      1.0.0.2                     --    S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

在 Spoke1 上 ping Spoke2 的私网地址 192.168.0.4。

```
[Spoke2] ping 192.168.0.4
Ping 192.168.0.4 (192.168.0.4): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.0.4: icmp_seq=0 ttl=255 time=4.000 ms
56 bytes from 192.168.0.4: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 192.168.0.4 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.000/4.000/1.549 ms
```

显示 Spoke1 上的 IPv4 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 3
Private address  Public address              Port  Type  State      Holding time
192.168.0.1      1.0.0.1                     --    S-H   Success    0H 46M  8S
192.168.0.2      1.0.0.2                     --    S-H   Success    0H 46M  8S
192.168.0.4      1.0.0.4                     --    S-S   Success    0H  0M  1S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke1 与 Spoke2 建立了 Spoke-Spoke 临时隧道。Spoke2 上的显示信息与 Spoke1 类似。

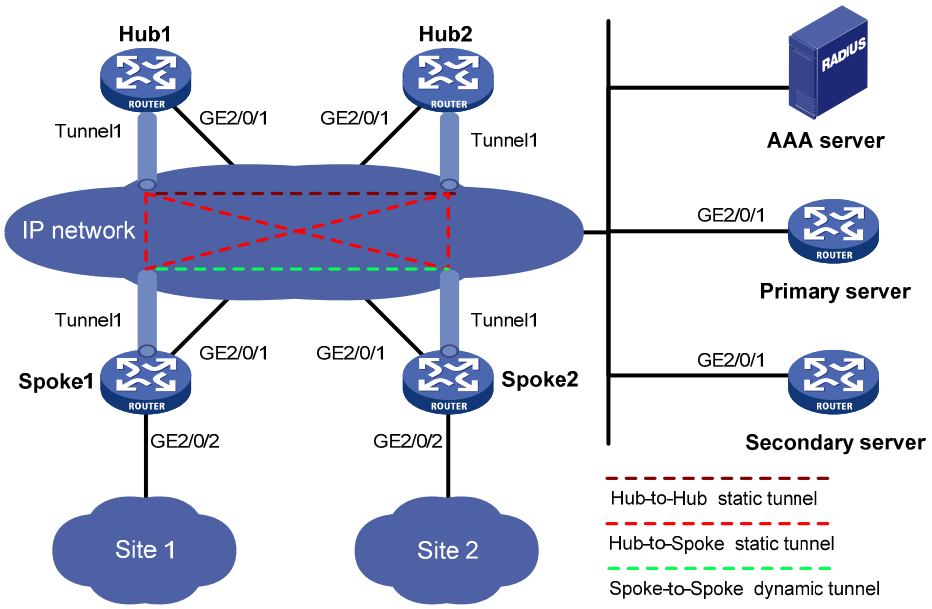
1.10.2 IPv6 Full-Mesh类型ADVPN典型配置举例

1. 组网需求

- 在 IPv6 Full-Mesh 的组网方式下，主、备 VAM Server 负责管理、维护各个节点的信息；AAA 服务器负责对 VAM Client 进行认证和计费管理；两个 Hub 互为备份，负责数据的转发和路由信息的交换。
- Spoke 与 Hub 之间建立永久的 ADVPN 隧道。
- 同一 ADVPN 域中，任意的两个 Spoke 之间在有数据时动态建立 ADVPN 隧道。

2. 组网图

图1-8 IPv6 Full-Mesh 类型 ADVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
Hub 1	GE2/0/1	1::1/64	Spoke 1	GE2/0/1	1::3/64
	Tunnel1	192:168::1/64		GE2/0/2	192:168:1::1/64
Hub 2	GE2/0/1	1::2/64		Tunnel1	192:168::3/64
	Tunnel1	192:168::2/64	Spoke 2	GE2/0/1	1::4/64
AAA server		1::10/64		GE2/0/2	192:168:2::1/64
Primary server	GE2/0/1	1::11/64		Tunnel1	192:168::4/64
Secondary server	GE2/0/1	1::12/64			

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
[PrimaryServer] radius scheme abc
[PrimaryServer-radius-abc] primary authentication ipv6 1::10 1812
[PrimaryServer-radius-abc] primary accounting ipv6 1::10 1813
```

```
[PrimaryServer-radius-abc] key authentication simple 123
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```

配置 ISP 域的 AAA 方案。

```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
[PrimaryServer] domain default enable abc
```

- 配置 VAM Server

创建 ADVPN 域 abc。

```
[PrimaryServer] vam server advpn-domain abc id 1
```

创建 Hub 组 0。

```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```

指定 Hub 组内 Hub 的 IPv6 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::1
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::2
```

指定 Hub 组内 Spoke 的 IPv6 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] spoke ipv6 private-address network
192:168::0 64
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```

配置 VAM Server 的预共享密钥为 123456。

```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```

配置对 VAM Client 进行 CHAP 认证。

```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```

启动该 ADVPN 域的 VAM Server 功能。

```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```

(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1。

```
<Hub1> system-view
[Hub1] vam client name Hub1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub1-vam-client-Hub1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub1-vam-client-Hub1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub1，密码为 hub1。

```
[Hub1-vam-client-Hub1] user hub1 password simple hub1
```

配置主、被 VAM Server 的 IP 地址。

```
[Hub1-vam-client-Hub1] server primary ipv6-address 1::11
[Hub1-vam-client-Hub1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1] client enable
[Hub1-vam-client-Hub1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub1] ike keychain abc
[Hub1-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Hub1-ike-keychain-abc] quit
[Hub1] ike profile abc
[Hub1-ike-profile-abc] keychain abc
[Hub1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub1] ipsec transform-set abc
[Hub1-ipsec-transform-set-abc] encapsulation-mode transport
[Hub1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub1-ipsec-transform-set-abc] quit
[Hub1] ipsec profile abc isakmp
[Hub1-ipsec-profile-isakmp-abc] transform-set abc
[Hub1-ipsec-profile-isakmp-abc] ike-profile abc
[Hub1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Hub1] ospfv3 1
[Hub1-ospfv3-1] router-id 0.0.0.1
[Hub1-ospfv3-1] area 0
[Hub1-ospfv3-1-area-0.0.0.0] quit
[Hub1-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装模式的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel1 mode advpn gre ipv6
[Hub1-Tunnel1] ipv6 address 192:168::1 64
[Hub1-Tunnel1] ipv6 address fe80::1 link-local
[Hub1-Tunnel1] vam ipv6 client Hub1
[Hub1-Tunnel1] ospfv3 1 area 0
[Hub1-Tunnel1] ospfv3 network-type broadcast
[Hub1-Tunnel1] source gigabitethernet 2/0/1
[Hub1-Tunnel1] tunnel protection ipsec profile abc
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）

- 配置 VAM Client

创建 VAM Client Hub2。

```
<Hub2> system-view
[Hub2] vam client name Hub2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub2，密码为 hub2。

```
[Hub2-vam-client-Hub2] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2] server primary ipv6-address 1::11
[Hub2-vam-client-Hub2] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2] client enable
[Hub2-vam-client-Hub2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub2] ike keychain abc
[Hub2-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Hub2-ike-keychain-abc] quit
[Hub2] ike profile abc
[Hub2-ike-profile-abc] keychain abc
[Hub2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub2] ipsec transform-set abc
[Hub2-ipsec-transform-set-abc] encapsulation-mode transport
[Hub2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub2-ipsec-transform-set-abc] quit
[Hub2] ipsec profile abc isakmp
[Hub2-ipsec-profile-isakmp-abc] transform-set abc
[Hub2-ipsec-profile-isakmp-abc] ike-profile abc
[Hub2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Hub2] ospfv3 1
[Hub2-ospfv3-1] router-id 0.0.0.2
[Hub2-ospfv3-1] area 0
[Hub2-ospfv3-1-area-0.0.0.0] quit
[Hub2-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub2] interface tunnel1 mode advpn gre ipv6
[Hub2-Tunnel1] ipv6 address 192:168::2 64
```

```
[Hub1-Tunnel1] ipv6 address fe80::2 link-local
[Hub2-Tunnel1] vam ipv6 client Hub2
[Hub2-Tunnel1] ospfv3 1 area 0
[Hub2-Tunnel1] ospfv3 network-type broadcast
[Hub2-Tunnel1] source gigabitethernet 2/0/1
[Hub2-Tunnel1] tunnel protection ipsec profile abc
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

(5) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。

```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。

```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```

配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ipv6-address 1::11
[Spoke1-vam-client-Spoke1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke1] ike keychain abc
[Spoke1-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Spoke1-ike-keychain-abc] quit
[Spoke1] ike profile abc
[Spoke1-ike-profile-abc] keychain abc
[Spoke1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke1] ipsec transform-set abc
[Spoke1-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke1-ipsec-transform-set-abc] quit
[Spoke1] ipsec profile abc isakmp
[Spoke1-ipsec-profile-isakmp-abc] transform-set abc
[Spoke1-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Spoke1] ospfv3 1
[Spoke1-ospfv3-1] router-id 0.0.0.3
[Spoke1-ospfv3-1] area 0
[Spoke1-ospfv3-1-area-0.0.0.0] quit
[Spoke1-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。将 Spoke1 的 DR 优先级配置为 0，以使 Spoke1 不参与 DR/BDR 选举。

```
[Spoke1] interface tunnel1 mode advpn gre ipv6
[Spoke1-Tunnel1] ipv6 address 192:168::3 64
[Spoke1-Tunnel1] ipv6 address fe80::3 link-local
[Spoke1-Tunnel1] vam ipv6 client Spoke1
[Spoke1-Tunnel1] ospfv3 1 area 0
[Spoke1-Tunnel1] ospfv3 network-type broadcast
[Spoke1-Tunnel1] ospfv3 dr-priority 0
[Spoke1-Tunnel1] source gigabitethernet 2/0/1
[Spoke1-Tunnel1] tunnel protection ipsec profile abc
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```

(6) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。

```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。

```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```

配置 VAM Server 的 IP 地址。

```
[Spoke2-vam-client-Spoke2] server primary ipv6-address 1::11
[Spoke2-vam-client-Spoke2] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke2] ike keychain abc
[Spoke2-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Spoke2-ike-keychain-abc] quit
[Spoke2] ike profile abc
```

```
[Spoke2-ike-profile-abc] keychain abc
[Spoke2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke2] ipsec transform-set abc
[Spoke2-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke2-ipsec-transform-set-abc] quit
[Spoke2] ipsec profile abc isakmp
[Spoke2-ipsec-profile-isakmp-abc] transform-set abc
[Spoke2-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Spoke2] ospfv3 1
[Spoke2-ospfv3-1] router-id 0.0.0.4
[Spoke2-ospfv3-1] area 0
[Spoke2-ospfv3-1-area-0.0.0.0] quit
[Spoke2-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。将 Spoke2 的 DR 优先级配置为 0，以使 Spoke2 不参与 DR/BDR 选举。

```
[Spoke2] interface tunnel1 mode advpn gre ipv6
[Spoke2-Tunnel1] ipv6 address 192:168::4 64
[Spoke2-Tunnel1] ipv6 address fe80::4 link-local
[Spoke2-Tunnel1] vam ipv6 client Spoke2
[Spoke2-Tunnel1] ospfv3 1 area 0
[Spoke2-Tunnel1] ospfv3 network-type broadcast
[Spoke2-Tunnel1] ospfv3 dr-priority 0
[Spoke2-Tunnel1] source gigabitethernet 2/0/1
[Spoke2-Tunnel1] tunnel protection ipsec profile abc
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv6 私网地址映射信息。

```
[PrimaryServer] display vam server ipv6 address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address       Public address         Type   NAT  Holding time
0          192:168::1            1::1                   Hub    No   0H 52M  7S
0          192:168::2            1::2                   Hub    No   0H 47M 31S
0          192:168::3            1::3                   Spoke  No   0H 28M 25S
0          192:168::4            1::4                   Spoke  No   0H 19M 15S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv6 私网地址映射信息。

```
[SecondaryServer] display vam server ipv6 address-map
ADVPN domain name: 1
```

```
Total private address mappings: 4
Group      Private address       Public address         Type   NAT  Holding time
0          192:168::1            1::1                   Hub    No   0H 52M  7S
0          192:168::2            1::2                   Hub    No   0H 47M 31S
0          192:168::3            1::3                   Spoke  No   0H 28M 25S
0          192:168::4            1::4                   Spoke  No   0H 19M 15S
```

以上显示信息表示 Hub1、Hub2、Spoke1 和 Spoke2 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv6 ADVPN 隧道信息。

```
[Hub1] display advpn ipv6 session
Interface         : Tunnel1
Number of sessions: 3
Private address       Public address        Port  Type  State      Holding time
192:168::2            1::2                  --    H-H   Success    0H 46M  8S
192:168::3            1::3                  --    H-S   Success    0H 27M 27S
192:168::4            1::4                  --    H-S   Success    0H 18M 18S
```

以上显示信息表示 Hub1 与 Hub2、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv6 ADVPN 隧道信息。

```
[Spoke1] display advpn ipv6 session
Interface         : Tunnel1
Number of sessions: 2
Private address       Public address        Port  Type  State      Holding time
192:168::1            1::1                  --    S-H   Success    0H 46M  8S
192:168::2            1::2                  --    S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

在 Spoke1 上 ping Spoke2 的私网地址 192:168::4。

```
[Spoke2] ping ipv6 192:168::4
Ping6(56 data bytes) 192:168::4 --> 192:168::4, press CTRL_C to break
56 bytes from 192:168::4, icmp_seq=0 hlim=64 time=3.000 ms
56 bytes from 192:168::4, icmp_seq=1 hlim=64 time=0.000 ms
56 bytes from 192:168::4, icmp_seq=2 hlim=64 time=1.000 ms
56 bytes from 192:168::4, icmp_seq=3 hlim=64 time=1.000 ms
56 bytes from 192:168::4, icmp_seq=4 hlim=64 time=1.000 ms

--- Ping6 statistics for 192:168::4 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.200/3.000/0.980 ms
```

显示 Spoke1 上的 IPv6 ADVPN 隧道信息。

```
[Spoke1] display advpn ipv6 session
Interface         : Tunnel1
Number of sessions: 3
Private address       Public address        Port  Type  State      Holding time
192:168::1            1::1                  --    S-H   Success    0H 46M  8S
192:168::2            1::2                  --    S-H   Success    0H 46M  8S
192.168::4            1::4                  --    S-S   Success    0H  0M  1S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke1 与 Spoke2 建立了 Spoke-Spoke 临时隧道。Spoke2 上的显示信息与 Spoke1 类似。

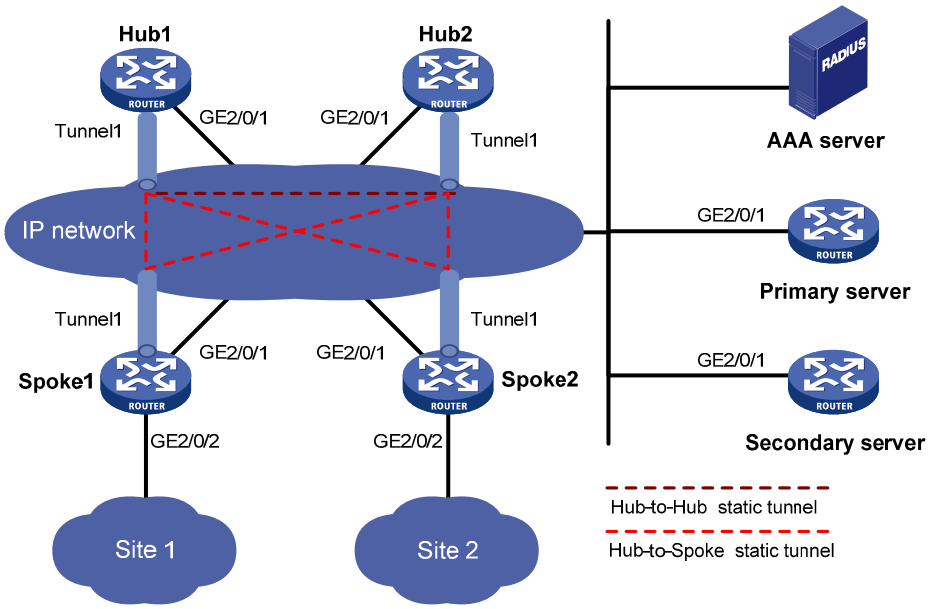
1.10.3 IPv4 Hub-Spoke类型ADVPN典型配置举例

1. 组网需求

- 在 IPv4 Hub-Spoke 的组网方式下，数据通过 Hub-Spoke 隧道进行转发。主、备 VAM Server 负责管理、维护各个节点的信息；AAA 服务器负责对 VAM Client 进行认证和计费管理；两个 Hub 互为备份，负责数据的转发和路由信息的交换。
- Spoke 与 Hub 之间建立永久的 ADVPN 隧道。

2. 组网图

图1-9 IPv4 Hub-Spoke 类型 ADVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
Hub 1	GE2/0/1	1.0.0.1/24	Spoke 1	GE2/0/1	1.0.0.3/24
	Tunnel1	192.168.0.1/24		GE2/0/2	192.168.1.1/24
Hub 2	GE2/0/1	1.0.0.2/24		Tunnel1	192.168.0.3/24
	Tunnel1	192.168.0.2/24	Spoke 2	GE2/0/1	1.0.0.4/24
AAA server		1.0.0.10/24		GE2/0/2	192.168.2.1/24
Primary server	GE2/0/1	1.0.0.11/24		Tunnel1	192.168.0.4/24
Secondary server	GE2/0/1	1.0.0.12/24			

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
[PrimaryServer] radius scheme abc
[PrimaryServer-radius-abc] primary authentication 1.0.0.10 1812
```

```
[PrimaryServer-radius-abc] primary accounting 1.0.0.10 1813
[PrimaryServer-radius-abc] key authentication simple 123
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```

配置 ISP 域的 AAA 方案。

```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
[PrimaryServer] domain default enable abc
```

- 配置 VAM Server

创建 ADVPN 域 abc。

```
[PrimaryServer] vam server advpn-domain abc id 1
```

创建 Hub 组 0。

```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```

指定 Hub 组内 Hub 的 IPv4 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.1
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.2
```

指定 Hub 组内 Spoke 的 IPv4 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] spoke private-address network
192.168.0.0 255.255.255.0
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```

配置 VAM Server 的预共享密钥为 123456。

```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```

配置对 VAM Client 进行 CHAP 认证。

```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```

启动该 ADVPN 域的 VAM Server 功能。

```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```

(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1。

```
<Hub1> system-view
[Hub1] vam client name Hub1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub1-vam-client-Hub1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub1-vam-client-Hub1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub1，密码为 hub1。

```
[Hub1-vam-client-Hub1] user hub1 password simple hub1
```

配置 VAM Server 的 IP 地址。

```
[Hub1-vam-client-Hub1] server primary ip-address 1.0.0.11
[Hub1-vam-client-Hub1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1] client enable
[Hub1-vam-client-Hub1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub1] ike keychain abc
[Hub1-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub1-ike-keychain-abc] quit
[Hub1] ike profile abc
[Hub1-ike-profile-abc] keychain abc
[Hub1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub1] ipsec transform-set abc
[Hub1-ipsec-transform-set-abc] encapsulation-mode transport
[Hub1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub1-ipsec-transform-set-abc] quit
[Hub1] ipsec profile abc isakmp
[Hub1-ipsec-profile-isakmp-abc] transform-set abc
[Hub1-ipsec-profile-isakmp-abc] ike-profile abc
[Hub1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub1] ospf 1
[Hub1-ospf-1] area 0
[Hub1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub1-ospf-1-area-0.0.0.0] quit
[Hub1-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel1 mode advpn gre
[Hub1-Tunnel1] ip address 192.168.0.1 255.255.255.0
[Hub1-Tunnel1] vam client Hub1
[Hub1-Tunnel1] ospf network-type p2mp
[Hub1-Tunnel1] source gigabitethernet 2/0/1
[Hub1-Tunnel1] tunnel protection ipsec profile abc
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub2。

```
<Hub2> system-view
[Hub2] vam client name Hub2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 Hub2，密码为 Hub2。

```
[Hub2-vam-client-Hub2] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2] server primary ip-address 1.0.0.11
[Hub2-vam-client-Hub2] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2] client enable
[Hub2-vam-client-Hub2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub2] ike keychain abc
[Hub2-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub2-ike-keychain-abc] quit
[Hub2] ike profile abc
[Hub2-ike-profile-abc] keychain abc
[Hub2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub2] ipsec transform-set abc
[Hub2-ipsec-transform-set-abc] encapsulation-mode transport
[Hub2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub2-ipsec-transform-set-abc] quit
[Hub2] ipsec profile abc isakmp
[Hub2-ipsec-profile-isakmp-abc] transform-set abc
[Hub2-ipsec-profile-isakmp-abc] ike-profile abc
[Hub2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub2] ospf 1
[Hub2-ospf-1] area 0
[Hub2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub2-ospf-1-area-0.0.0.0] quit
[Hub2-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub2] interface tunnel1 mode advpn gre
[Hub2-Tunnel1] ip address 192.168.0.2 255.255.255.0
[Hub2-Tunnel1] vam client Hub2
```

```
[Hub2-Tunnel1] ospf network-type p2mp
[Hub2-Tunnel1] source gigabitethernet 2/0/1
[Hub2-Tunnel1] tunnel protection ipsec profile abc
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

(5) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。

```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```

配置 VAM Client 的 ADVPN 域为 abc。

```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。

```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```

配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ip-address 1.0.0.11
[Spoke1-vam-client-Spoke1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke1] ike keychain abc
[Spoke1-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke1-ike-keychain-abc] quit
[Spoke1] ike profile abc
[Spoke1-ike-profile-abc] keychain abc
[Spoke1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke1] ipsec transform-set abc
[Spoke1-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke1-ipsec-transform-set-abc] quit
[Spoke1] ipsec profile abc isakmp
[Spoke1-ipsec-profile-isakmp-abc] transform-set abc
[Spoke1-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke1] ospf 1
[Spoke1-ospf-1] area 0
```

```
[Spoke1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.0] quit
[Spoke1-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Spoke1] interface tunnel1 mode advpn gre
[Spoke1-Tunnel1] ip address 192.168.0.3 255.255.255.0
[Spoke1-Tunnel1] vam client Spoke1
[Spoke1-Tunnel1] ospf network-type p2mp
[Spoke1-Tunnel1] source gigabitethernet 2/0/1
[Spoke1-Tunnel1] tunnel protection ipsec profile abc
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```

(6) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。

```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。

```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```

配置 VAM Server 的 IP 地址。

```
[Spoke2-vam-client-Spoke2] server primary ip-address 1.0.0.11
[Spoke2-vam-client-Spoke2] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke2] ike keychain abc
[Spoke2-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke2-ike-keychain-abc] quit
[Spoke2] ike profile abc
[Spoke2-ike-profile-abc] keychain abc
[Spoke2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke2] ipsec transform-set abc
[Spoke2-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke2-ipsec-transform-set-abc] esp authentication-algorithm sha1
```

```
[Spoke2-ipsec-transform-set-abc] quit
[Spoke2] ipsec profile abc isakmp
[Spoke2-ipsec-profile-isakmp-abc] transform-set abc
[Spoke2-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke2] ospf 1
[Spoke2-ospf-1] area 0
[Spoke2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.0] quit
[Spoke2-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Spoke2] interface tunnel1 mode advpn gre
[Spoke2-Tunnel1] ip address 192.168.0.4 255.255.255.0
[Spoke2-Tunnel1] vam client Spoke2
[Spoke2-Tunnel1] ospf network-type p2mp
[Spoke2-Tunnel1] source gigabitethernet 2/0/1
[Spoke2-Tunnel1] tunnel protection ipsec profile abc
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[PrimaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    No   0H 52M  7S
0          192.168.0.2      1.0.0.2                   Hub    No   0H 47M 31S
0          192.168.0.3      1.0.0.3                   Spoke  No   0H 28M 25S
0          192.168.0.4      1.0.0.4                   Spoke  No   0H 19M 15S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[SecondaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    No   0H 52M  7S
0          192.168.0.2      1.0.0.2                   Hub    No   0H 47M 31S
0          192.168.0.3      1.0.0.3                   Spoke  No   0H 28M 25S
0          192.168.0.4      1.0.0.4                   Spoke  No   0H 19M 15S
```

以上显示信息表示 Hub1、Hub2、Spoke1 和 Spoke2 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv4 ADVPN 隧道信息。

```
[Hub1] display advpn session
Interface         : Tunnel1
```

```
Number of sessions: 3
Private address  Public address              Port  Type  State      Holding time
192.168.0.2      1.0.0.2                     --    H-H   Success    0H 46M  8S
192.168.0.3      1.0.0.3                     --    H-S   Success    0H 27M 27S
192.168.0.4      1.0.0.4                     --    H-S   Success    0H 18M 18S
```

以上显示信息表示 Hub1 与 Hub2、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv4 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address  Public address              Port  Type  State      Holding time
192.168.0.1      1.0.0.1                     --    S-H   Success    0H 46M  8S
192.168.0.2      1.0.0.2                     --    S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

在 Spoke1 上 ping Spoke2 的私网地址 192.168.0.4。

```
[Spoke2] ping 192.168.0.4
Ping 192.168.0.4 (192.168.0.4): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.0.4: icmp_seq=0 ttl=255 time=4.000 ms
56 bytes from 192.168.0.4: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 192.168.0.4 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.000/4.000/1.549 ms
```

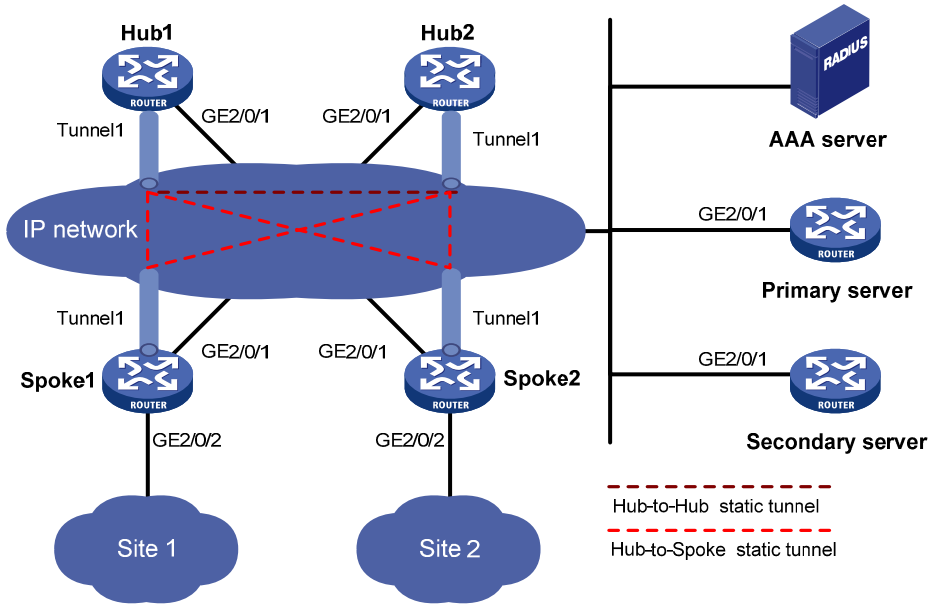
1.10.4 IPv6 Hub-Spoke类型ADVPN典型配置举例

1. 组网需求

- 在 IPv6 Hub-Spoke 的组网方式下，数据通过 Hub-Spoke 隧道进行转发。主、备 VAM Server 负责管理、维护各个节点的信息；AAA 服务器负责对 VAM Client 进行认证和计费管理；两个 Hub 互为备份，负责数据的转发和路由信息的交换。
- Spoke 与 Hub 之间建立永久的 ADVPN 隧道。

2. 组网图

图1-10 IPv6 Hub-Spoke 类型 ADVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
Hub 1	GE2/0/1	1::1/64	Spoke 1	GE2/0/1	1::3/64
	Tunnel1	192:168::1/64		GE2/0/2	192:168:1::1/64
Hub 2	GE2/0/1	1::2/64		Tunnel1	192:168::3/64
	Tunnel1	192:168::2/64	Spoke 2	GE2/0/1	1::4/64
AAA server		1::10/64		GE2/0/2	192:168:2::1/64
Primary server	GE2/0/1	1::11/64		Tunnel1	192:168::4/64
Secondary server	GE2/0/1	1::12/64			

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
[PrimaryServer] radius scheme abc
[PrimaryServer-radius-abc] primary authentication ipv6 1::10 1812
[PrimaryServer-radius-abc] primary accounting ipv6 1::10 1813
[PrimaryServer-radius-abc] key authentication simple 123
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```

配置 ISP 域的 AAA 方案。

```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
```

```
[PrimaryServer] domain default enable abc
```

- 配置 VAM Server

创建 ADVPN 域 abc。

```
[PrimaryServer] vam server advpn-domain abc id 1
```

创建 Hub 组 0。

```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```

指定 Hub 组内 Hub 的 IPv6 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::1
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::2
```

指定 Hub 组内 Spoke 的 IPv6 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] spoke ipv6 private-address network
192:168::0 64
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```

配置 VAM Server 的预共享密钥为 123456。

```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```

配置对 VAM Client 进行 CHAP 认证。

```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```

启动该 ADVPN 域的 VAM Server 功能。

```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```

(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1。

```
<Hub1> system-view
[Hub1] vam client name Hub1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub1-vam-client-Hub1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub1-vam-client-Hub1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub1，密码为 hub1。

```
[Hub1-vam-client-Hub1] user hub1 password simple hub1
```

配置 VAM Server 的 IP 地址。

```
[Hub1-vam-client-Hub1] server primary ipv6-address 1::11
[Hub1-vam-client-Hub1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1] client enable
[Hub1-vam-client-Hub1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub1] ike keychain abc
```

```
[Hub1-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Hub1-ike-keychain-abc] quit
[Hub1] ike profile abc
[Hub1-ike-profile-abc] keychain abc
[Hub1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub1] ipsec transform-set abc
[Hub1-ipsec-transform-set-abc] encapsulation-mode transport
[Hub1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub1-ipsec-transform-set-abc] quit
[Hub1] ipsec profile abc isakmp
[Hub1-ipsec-profile-isakmp-abc] transform-set abc
[Hub1-ipsec-profile-isakmp-abc] ike-profile abc
[Hub1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Hub1] ospfv3 1
[Hub1-ospfv3-1] router-id 0.0.0.1
[Hub1-ospfv3-1] area 0
[Hub1-ospfv3-1-area-0.0.0.0] quit
[Hub1-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel1 mode advpn gre ipv6
[Hub1-Tunnel1] ipv6 address 192:168::1 64
[Hub1-Tunnel1] ipv6 address fe80::1 link-local
[Hub1-Tunnel1] vam ipv6 client Hub1
[Hub1-Tunnel1] ospfv3 1 area 0
[Hub1-Tunnel1] ospfv3 network-type p2mp
[Hub1-Tunnel1] source gigabitethernet 2/0/1
[Hub1-Tunnel1] tunnel protection ipsec profile abc
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub2。

```
<Hub2> system-view
[Hub2] vam client name Hub2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub2，密码为 hub2。

```
[Hub2-vam-client-Hub2] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2] server primary ipv6-address 1::11
[Hub2-vam-client-Hub2] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2] client enable
[Hub2-vam-client-Hub2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub2] ike keychain abc
[Hub2-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Hub2-ike-keychain-abc] quit
[Hub2] ike profile abc
[Hub2-ike-profile-abc] keychain abc
[Hub2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub2] ipsec transform-set abc
[Hub2-ipsec-transform-set-abc] encapsulation-mode transport
[Hub2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub2-ipsec-transform-set-abc] quit
[Hub2] ipsec profile abc isakmp
[Hub2-ipsec-profile-isakmp-abc] transform-set abc
[Hub2-ipsec-profile-isakmp-abc] ike-profile abc
[Hub2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Hub2] ospfv3 1
[Hub2-ospfv3-1] router-id 0.0.0.2
[Hub2-ospfv3-1] area 0
[Hub2-ospfv3-1-area-0.0.0.0] quit
[Hub2-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub2] interface tunnel1 mode advpn gre ipv6
[Hub2-Tunnel1] ipv6 address 192:168::2 64
[Hub2-Tunnel1] ipv6 address fe80::2 link-local
[Hub2-Tunnel1] vam ipv6 client Hub2
[Hub2-Tunnel1] ospfv3 1 area 0
[Hub2-Tunnel1] ospfv3 network-type p2mp
[Hub2-Tunnel1] source gigabitethernet 2/0/1
[Hub2-Tunnel1] tunnel protection ipsec profile abc
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

(5) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。

```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。

```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```

配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ipv6-address 1::11
[Spoke1-vam-client-Spoke1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke1] ike keychain abc
[Spoke1-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Spoke1-ike-keychain-abc] quit
[Spoke1] ike profile abc
[Spoke1-ike-profile-abc] keychain abc
[Spoke1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke1] ipsec transform-set abc
[Spoke1-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke1-ipsec-transform-set-abc] quit
[Spoke1] ipsec profile abc isakmp
[Spoke1-ipsec-profile-isakmp-abc] transform-set abc
[Spoke1-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Spoke1] ospfv3 1
[Spoke1-ospfv3-1] router-id 0.0.0.3
[Spoke1-ospfv3-1] area 0
[Spoke1-ospfv3-1-area-0.0.0.0] quit
[Spoke1-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Spoke1] interface tunnel1 mode advpn gre ipv6
[Spoke1-Tunnel1] ipv6 address 192:168::3 64
[Spoke1-Tunnel1] ipv6 address fe80::3 link-local
[Spoke1-Tunnel1] vam ipv6 client Spoke1
[Spoke1-Tunnel1] ospfv3 1 area 0
[Spoke1-Tunnel1] ospfv3 network-type p2mp
[Spoke1-Tunnel1] source gigabitethernet 2/0/1
[Spoke1-Tunnel1] tunnel protection ipsec profile abc
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```

(6) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。

```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。

```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```

配置 VAM Server 的 IP 地址。

```
[Spoke2-vam-client-Spoke2] server primary ipv6-address 1::11
[Spoke2-vam-client-Spoke2] server secondary ipv6-address 1::12
```

开启 VAM Client 的功能。

```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke2] ike keychain abc
[Spoke2-ike-keychain-abc] pre-shared-key address ipv6 :: 0 key simple 123456
[Spoke2-ike-keychain-abc] quit
[Spoke2] ike profile abc
[Spoke2-ike-profile-abc] keychain abc
[Spoke2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke2] ipsec transform-set abc
[Spoke2-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke2-ipsec-transform-set-abc] quit
[Spoke2] ipsec profile abc isakmp
[Spoke2-ipsec-profile-isakmp-abc] transform-set abc
[Spoke2-ipsec-profile-isakmp-abc] ike-profile abc
```

```
[Spoke2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Spoke2] ospfv3 1
[Spoke2-ospfv3-1] router-id 0.0.0.4
[Spoke2-ospfv3-1] area 0
[Spoke2-ospfv3-1-area-0.0.0.0] quit
[Spoke2-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 GRE 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Spoke2] interface tunnel1 mode advpn gre ipv6
[Spoke2-Tunnel1] ipv6 address 192:168::4 64
[Spoke2-Tunnel1] ipv6 address fe80::4 link-local
[Spoke2-Tunnel1] vam ipv6 client Spoke2
[Spoke2-Tunnel1] ospfv3 1 area 0
[Spoke2-Tunnel1] ospfv3 network-type p2mp
[Spoke2-Tunnel1] source gigabitethernet 2/0/1
[Spoke2-Tunnel1] tunnel protection ipsec profile abc
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv6 私网地址映射信息。

```
[PrimaryServer] display vam server ipv6 address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address       Public address         Type   NAT  Holding time
0          192:168::1            1::1                   Hub    No   0H 52M  7S
0          192:168::2            1::2                   Hub    No   0H 47M 31S
0          192:168::3            1::3                   Spoke  No   0H 28M 25S
0          192:168::4            1::4                   Spoke  No   0H 19M 15S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv6 私网地址映射信息。

```
[SecondaryServer] display vam server ipv6 address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address       Public address         Type   NAT  Holding time
0          192:168::1            1::1                   Hub    No   0H 52M  7S
0          192:168::2            1::2                   Hub    No   0H 47M 31S
0          192:168::3            1::3                   Spoke  No   0H 28M 25S
0          192:168::4            1::4                   Spoke  No   0H 19M 15S
```

以上显示信息表示 Hub1、Hub2、Spoke1 和 Spoke2 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv6 ADVPN 隧道信息。

```
[Hub1] display advpn ipv6 session
Interface         : Tunnel1
Number of sessions: 3
Private address       Public address        Port  Type  State      Holding time
192:168::2            1::2                  --    H-H   Success    0H 46M  8S
```

```
192:168::3            1::3                  --    H-S   Success    0H 27M 27S
192:168::4            1::4                  --    H-S   Success    0H 18M 18S
```

以上显示信息表示 Hub1 与 Hub2、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv6 ADVPN 隧道信息。

```
[Spoke1] display advpn ipv6 session
Interface         : Tunnel1
Number of sessions: 2
Private address       Public address        Port  Type  State      Holding time
192:168::1            1::1                  --    S-H   Success    0H 46M  8S
192:168::2            1::2                  --    S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

在 Spoke1 上 ping Spoke2 的私网地址 192:168::4。

```
[Spoke2] ping ipv6 192:168::4
Ping6(56 data bytes) 192:168::4 --> 192:168::4, press CTRL_C to break
56 bytes from 192:168::4, icmp_seq=0 hlim=64 time=3.000 ms
56 bytes from 192:168::4, icmp_seq=1 hlim=64 time=0.000 ms
56 bytes from 192:168::4, icmp_seq=2 hlim=64 time=1.000 ms
56 bytes from 192:168::4, icmp_seq=3 hlim=64 time=1.000 ms
56 bytes from 192:168::4, icmp_seq=4 hlim=64 time=1.000 ms

--- Ping6 statistics for 192:168::4 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.200/3.000/0.980 ms
```

1.10.5 IPv4 划分多个Hub组ADVPN典型配置举例

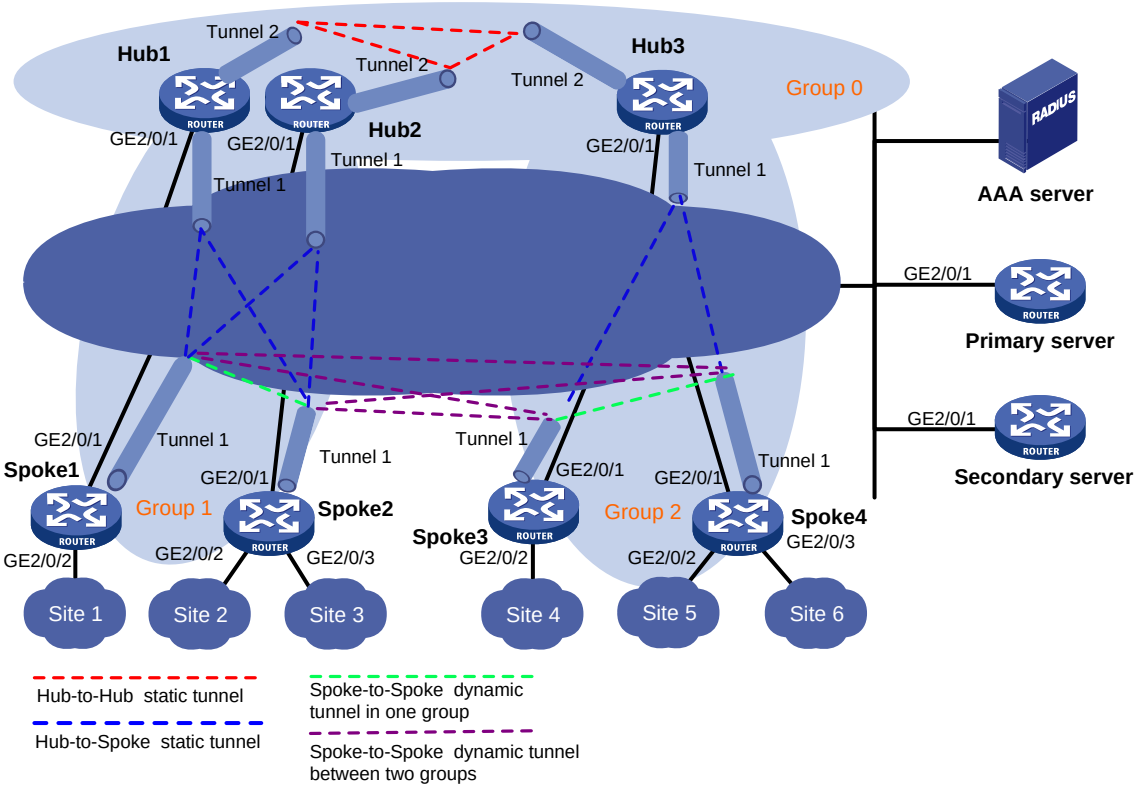
1. 组网需求

ADVPN 域中包含的 ADVPN 节点较多，通过划分多个 Hub 组来减轻 Hub 的负担。具体需求如下：

- 主、备 VAM Server 负责管理、维护各个节点的信息。
- AAA 服务器负责对 VAM Client 进行认证和计费管理。
- 将 ADVPN 域划分为三个 Hub 组：Hub1、Hub2 和 Hub3 属于 Hub 组 0；Hub1、Hub2、Spoke1 和 Spoke2 属于 Hub 组 1，两个 Hub 互为备份；Hub3、Spoke3 和 Spoke4 属于 Hub 组 2。
- Hub 组 1 和 Hub 组 2 内采用 Full-Mesh 组网方式。
- 允许所有的 Spoke 建立跨 Hub 组的 Spoke-Spoke 直连隧道。

2. 组网图

图1-11 IPv4 划分多个 Hub 组 ADVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
Hub 1	GE2/0/1	1.0.0.1/24	Spoke 1	GE2/0/1	1.0.0.4/24
	Tunnel1	192.168.1.1/24		GE2/0/2	192.168.10.1/24
	Tunnel2	192.168.0.1/24		Tunnel1	192.168.1.3/24
Hub 2	GE2/0/1	1.0.0.2/24	Spoke 2	GE2/0/1	1.0.0.5/24
	Tunnel1	192.168.1.2/24		GE2/0/2	192.168.20.1/24
	Tunnel2	192.168.0.2/24		GE2/0/3	192.168.30.1/24
Hub 3	GE2/0/1	1.0.0.3/24		Tunnel1	192.168.1.4/24
	Tunnel1	192.168.2.1/24	Spoke 3	GE2/0/1	1.0.0.6/24
	Tunnel2	192.168.0.3/24		GE2/0/2	192.168.40.1/24
AAA server		1.0.0.10/24		Tunnel1	192.168.2.2/24
Primary server	GE2/0/1	1.0.0.11/24	Spoke 4	GE2/0/1	1.0.0.7/24
Secondary server	GE2/0/1	1.0.0.12/24		GE2/0/2	192.168.50.1/24
				GE2/0/3	192.168.60.1/24
				Tunnel1	192.168.2.3/24

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
[PrimaryServer] radius scheme abc
[PrimaryServer-radius-abc] primary authentication 1.0.0.10 1812
[PrimaryServer-radius-abc] primary accounting 1.0.0.10 1813
```

```
[PrimaryServer-radius-abc] key authentication simple 123
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```

配置 ISP 域的 AAA 方案。

```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
[PrimaryServer] domain default enable abc
```

- 配置 VAM Server

创建 ADVPN 域 abc。

```
[PrimaryServer] vam server advpn-domain abc id 1
```

创建 Hub 组 0。

```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```

指定 Hub 组内 Hub 的 IPv4 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.1
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.2
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.3
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```

创建 Hub 组 1。

```
[PrimaryServer-vam-server-domain-abc] hub-group 1
```

指定 Hub 组内 Hub 的 IPv4 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-1] hub private-address 192.168.1.1
[PrimaryServer-vam-server-domain-abc-hub-group-1] hub private-address 192.168.1.2
```

指定 Hub 组内 Spoke 的 IPv4 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-1] spoke private-address network
192.168.1.0 255.255.255.0
```

允许建立跨组 Spoke-Spoke 直连隧道。

```
[PrimaryServer-vam-server-domain-abc-hub-group-1] shortcut interest all
[PrimaryServer-vam-server-domain-abc-hub-group-1] quit
```

创建 Hub 组 2。

```
[PrimaryServer-vam-server-domain-abc] hub-group 2
```

指定 Hub 组内 Hub 的 IPv4 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-2] hub private-address 192.168.2.1
```

指定 Hub 组内 Spoke 的 IPv4 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-2] spoke private-address network
192.168.2.0 255.255.255.0
```

允许建立跨组 Spoke-Spoke 直连隧道。

```
[PrimaryServer-vam-server-domain-abc-hub-group-2] shortcut interest all
[PrimaryServer-vam-server-domain-abc-hub-group-2] quit
```

配置 VAM Server 的预共享密钥为 123456。

```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```

配置对 VAM Client 进行 CHAP 认证。

```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```
启动该 ADVPN 域的 VAM Server 功能。
```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```
(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1Group0。
```
<Hub1> system-view
[Hub1] vam client name Hub1Group0
```
配置 VAM Client 所属的 ADVPN 域为 abc。
```
[Hub1-vam-client-Hub1Group0] advpn-domain abc
```
配置 VAM Client 的预共享密钥。
```
[Hub1-vam-client-Hub1Group0] pre-shared-key simple 123456
```
配置 VAM Client 的认证用户名为 hub1，密码为 hub1。
```
[Hub1-vam-client-Hub1Group0] user hub1 password simple hub1
```
配置 VAM Server 的 IP 地址。
```
[Hub1-vam-client-Hub1Group0] server primary ip-address 1.0.0.11
[Hub1-vam-client-Hub1Group0] server secondary ip-address 1.0.0.12
```
开启 VAM Client 功能。
```
[Hub1-vam-client-Hub1Group0] client enable
[Hub1-vam-client-Hub1Group0] quit
```
创建 VAM Client Hub1Group1。
```
[Hub1] vam client name Hub1Group1
```
配置 VAM Client 所属的 ADVPN 域为 abc。
```
[Hub1-vam-client-Hub1Group1] advpn-domain abc
```
配置 VAM Client 的预共享密钥。
```
[Hub1-vam-client-Hub1Group1] pre-shared-key simple 123456
```
配置 VAM Client 的认证用户名为 hub1，密码为 hub1。
```
[Hub1-vam-client-Hub1Group1] user hub1 password simple hub1
```
配置 VAM Server 的 IP 地址。
```
[Hub1-vam-client-Hub1Group1] server primary ip-address 1.0.0.11
[Hub1-vam-client-Hub1Group1] server secondary ip-address 1.0.0.12
```
开启 VAM Client 功能。
```
[Hub1-vam-client-Hub1Group1] client enable
[Hub1-vam-client-Hub1Group1] quit
```
- 配置 IPsec 安全框架

配置 IKE 框架。
```
[Hub1] ike keychain abc
[Hub1-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub1-ike-keychain-abc] quit
```

```
[Hub1] ike profile abc
[Hub1-ike-profile-abc] keychain abc
[Hub1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub1] ipsec transform-set abc
[Hub1-ipsec-transform-set-abc] encapsulation-mode transport
[Hub1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub1-ipsec-transform-set-abc] quit
[Hub1] ipsec profile abc isakmp
[Hub1-ipsec-profile-isakmp-abc] transform-set abc
[Hub1-ipsec-profile-isakmp-abc] ike-profile abc
[Hub1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub1] ospf 1
[Hub1-ospf-1] area 0
[Hub1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub1-ospf-1-area-0.0.0.0] quit
[Hub1-ospf-1] area 1
[Hub1-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Hub1-ospf-1-area-0.0.0.1] quit
[Hub1-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel1 mode advpn udp
[Hub1-Tunnel1] ip address 192.168.1.1 255.255.255.0
[Hub1-Tunnel1] vam client Hub1Group1
[Hub1-Tunnel1] ospf network-type broadcast
[Hub1-Tunnel1] source gigabitethernet 2/0/1
[Hub1-Tunnel1] tunnel protection ipsec profile abc
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel2。

```
[Hub1] interface tunnel2 mode advpn udp
[Hub1-Tunnel2] ip address 192.168.0.1 255.255.255.0
[Hub1-Tunnel2] vam client Hub1Group0
[Hub1-Tunnel2] ospf network-type broadcast
[Hub1-Tunnel2] source gigabitethernet 2/0/1
[Hub1-Tunnel2] tunnel protection ipsec profile abc
[Hub1-Tunnel2] undo shutdown
[Hub1-Tunnel2] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub2Group0。

```
<Hub2> system-view
[Hub2] vam client name Hub2Group0
```
配置 VAM Client 所属的 ADVPN 域为 abc。
```
[Hub2-vam-client-Hub2Group0] advpn-domain abc
```
配置 VAM Client 的预共享密钥。
```
[Hub2-vam-client-Hub2Group0] pre-shared-key simple 123456
```
配置 VAM Client 的认证用户名为 hub2，密码为 hub2。
```
[Hub2-vam-client-Hub2Group0] user hub2 password simple hub2
```
配置 VAM Server 的 IP 地址。
```
[Hub2-vam-client-Hub2Group0] server primary ip-address 1.0.0.11
[Hub2-vam-client-Hub2Group0] server secondary ip-address 1.0.0.12
```
开启 VAM Client 功能。
```
[Hub2-vam-client-Hub2Group0] client enable
[Hub2-vam-client-Hub2Group0] quit
```
创建 VAM Client Hub2Group1。
```
[Hub2] vam client name Hub2Group1
```
配置 VAM Client 所属的 ADVPN 域为 abc。
```
[Hub2-vam-client-Hub2Group1] advpn-domain abc
```
配置 VAM Client 的预共享密钥。
```
[Hub2-vam-client-Hub2Group1] pre-shared-key simple 123456
```
配置 VAM Client 的认证用户名为 hub2，密码为 hub2。
```
[Hub2-vam-client-Hub2Group1] user Hub2 password simple Hub2
```
配置 VAM Server 的 IP 地址。
```
[Hub2-vam-client-Hub2Group1] server primary ip-address 1.0.0.11
[Hub2-vam-client-Hub2Group1] server secondary ip-address 1.0.0.12
```
开启 VAM Client 功能。
```
[Hub2-vam-client-Hub2Group1] client enable
[Hub2-vam-client-Hub2Group1] quit
```
- 配置 IPsec 安全框架

配置 IKE 框架。
```
[Hub2] ike keychain abc
[Hub2-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub2-ike-keychain-abc] quit
[Hub2] ike profile abc
[Hub2-ike-profile-abc] keychain abc
[Hub2-ike-profile-abc] quit
```
配置 IPsec 安全框架。
```
[Hub2] ipsec transform-set abc
[Hub2-ipsec-transform-set-abc] encapsulation-mode transport
[Hub2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub2-ipsec-transform-set-abc] quit
[Hub2] ipsec profile abc isakmp
[Hub2-ipsec-profile-isakmp-abc] transform-set abc
[Hub2-ipsec-profile-isakmp-abc] ike-profile abc
```

```
[Hub2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub2] ospf 1
[Hub2-ospf-1] area 0
[Hub2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub2-ospf-1-area-0.0.0.0] quit
[Hub2-ospf-1] area 1
[Hub2-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Hub2-ospf-1-area-0.0.0.1] quit
[Hub2-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub2] interface tunnel1 mode advpn udp
[Hub2-Tunnel1] ip address 192.168.1.2 255.255.255.0
[Hub2-Tunnel1] vam client Hub2Group1
[Hub2-Tunnel1] ospf network-type broadcast
[Hub2-Tunnel1] source gigabitethernet 2/0/1
[Hub2-Tunnel1] tunnel protection ipsec profile abc
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel2。

```
[Hub2] interface tunnel2 mode advpn udp
[Hub2-Tunnel2] ip address 192.168.0.2 255.255.255.0
[Hub2-Tunnel2] vam client Hub2Group0
[Hub2-Tunnel2] ospf network-type broadcast
[Hub2-Tunnel2] source gigabitethernet 2/0/1
[Hub2-Tunnel2] tunnel protection ipsec profile abc
[Hub2-Tunnel2] undo shutdown
[Hub2-Tunnel2] quit
```

(5) 配置 Hub3

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub3Group0。

```
<Hub3> system-view
[Hub3] vam client name Hub3Group0
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub3-vam-client-Hub3Group0] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub3-vam-client-Hub3Group0] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub3，密码为 hub3。

```
[Hub3-vam-client-Hub3Group0] user hub3 password simple hub3
```

配置 VAM Server 的 IP 地址。

```
[Hub3-vam-client-Hub3Group0] server primary ip-address 1.0.0.11
[Hub3-vam-client-Hub3Group0] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub3-vam-client-Hub3Group0] client enable
[Hub3-vam-client-Hub3Group0] quit
```

创建 VAM Client Hub3Group1。

```
[Hub3] vam client name Hub3Group1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub3-vam-client-Hub3Group1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub3-vam-client-Hub3Group1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub3，密码为 hub3。

```
[Hub3-vam-client-Hub3Group1] user hub3 password simple hub3
```

配置 VAM Server 的 IP 地址。

```
[Hub3-vam-client-Hub3Group1] server primary ip-address 1.0.0.11
[Hub3-vam-client-Hub3Group1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Hub3-vam-client-Hub3Group1] client enable
[Hub3-vam-client-Hub3Group1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub3] ike keychain abc
[Hub3-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Hub3-ike-keychain-abc] quit
[Hub3] ike profile abc
[Hub3-ike-profile-abc] keychain abc
[Hub3-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub3] ipsec transform-set abc
[Hub3-ipsec-transform-set-abc] encapsulation-mode transport
[Hub3-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub3-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub3-ipsec-transform-set-abc] quit
[Hub3] ipsec profile abc isakmp
[Hub3-ipsec-profile-isakmp-abc] transform-set abc
[Hub3-ipsec-profile-isakmp-abc] ike-profile abc
[Hub3-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub3] ospf 1
[Hub3-ospf-1] area 0
[Hub3-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub3-ospf-1-area-0.0.0.0] quit
[Hub3-ospf-1] area 2
[Hub3-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Hub3-ospf-1-area-0.0.0.2] quit
[Hub3-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub3] interface tunnel1 mode advpn udp
[Hub3-Tunnel1] ip address 192.168.2.1 255.255.255.0
[Hub3-Tunnel1] vam client Hub3Group1
[Hub3-Tunnel1] ospf network-type broadcast
[Hub3-Tunnel1] source gigabitethernet 2/0/1
[Hub3-Tunnel1] tunnel protection ipsec profile abc
[Hub3-Tunnel1] undo shutdown
[Hub3-Tunnel1] quit
```

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel2。

```
[Hub3] interface tunnel2 mode advpn udp
[Hub3-Tunnel2] ip address 192.168.0.3 255.255.255.0
[Hub3-Tunnel2] vam client Hub3Group0
[Hub3-Tunnel2] ospf network-type broadcast
[Hub3-Tunnel2] source gigabitethernet 2/0/1
[Hub3-Tunnel2] tunnel protection ipsec profile abc
[Hub3-Tunnel2] undo shutdown
[Hub3-Tunnel2] quit
```

(6) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。

```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。

```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```

配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ip-address 1.0.0.11
[Spoke1-vam-client-Spoke1] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke1] ike keychain abc
[Spoke1-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke1-ike-keychain-abc] quit
[Spoke1] ike profile abc
[Spoke1-ike-profile-abc] keychain abc
[Spoke1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke1] ipsec transform-set abc
[Spoke1-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke1-ipsec-transform-set-abc] quit
[Spoke1] ipsec profile abc isakmp
[Spoke1-ipsec-profile-isakmp-abc] transform-set abc
[Spoke1-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke1] ospf 1
[Spoke1-ospf-1] area 1
[Spoke1-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.1] network 192.168.10.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.1] quit
[Spoke1-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。将 Spoke1 的 DR 优先级配置为 0，以使 Spoke1 不参与 DR/BDR 选举。

```
[Spoke1] interface tunnel1 mode advpn udp
[Spoke1-Tunnel1] ip address 192.168.1.3 255.255.255.0
[Spoke1-Tunnel1] vam client Spoke1
[Spoke1-Tunnel1] ospf network-type broadcast
[Spoke1-Tunnel1] ospf dr-priority 0
[Spoke1-Tunnel1] advpn network 192.168.10.0 255.255.255.0
[Spoke1-Tunnel1] source gigabitethernet 2/0/1
[Spoke1-Tunnel1] tunnel protection ipsec profile abc
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```

(7) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。

```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。

```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```

配置 VAM Server 的 IP 地址。

```
[Spoke2-vam-client-Spoke2] server primary ip-address 1.0.0.11
```

```
[Spoke2-vam-client-Spoke2] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke2] ike keychain abc
[Spoke2-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke2-ike-keychain-abc] quit
[Spoke2] ike profile abc
[Spoke2-ike-profile-abc] keychain abc
[Spoke2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke2] ipsec transform-set abc
[Spoke2-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke2-ipsec-transform-set-abc] quit
[Spoke2] ipsec profile abc isakmp
[Spoke2-ipsec-profile-isakmp-abc] transform-set abc
[Spoke2-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke2] ospf 1
[Spoke2-ospf-1] area 1
[Spoke2-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.1] network 192.168.20.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.1] network 192.168.30.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.1] quit
[Spoke2-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。将 Spoke2 的 DR 优先级配置为 0，以使 Spoke2 不参与 DR/BDR 选举。

```
[Spoke2] interface tunnel1 mode advpn udp
[Spoke2-Tunnel1] ip address 192.168.1.4 255.255.255.0
[Spoke2-Tunnel1] vam client Spoke2
[Spoke2-Tunnel1] ospf network-type broadcast
[Spoke2-Tunnel1] ospf dr-priority 0
[Spoke2-Tunnel1] advpn network 192.168.20.0 255.255.255.0
[Spoke2-Tunnel1] advpn network 192.168.30.0 255.255.255.0
[Spoke2-Tunnel1] source gigabitethernet 2/0/1
[Spoke2-Tunnel1] tunnel protection ipsec profile abc
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

(8) 配置 Spoke3

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke3。

```
<Spoke3> system-view
[Spoke3] vam client name Spoke3
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke3-vam-client-Spoke3] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke3-vam-client-Spoke3] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke3，密码为 spoke3。

```
[Spoke3-vam-client-Spoke3] user spoke3 password simple spoke3
```

配置 VAM Server 的 IP 地址。

```
[Spoke3-vam-client-Spoke3] server primary ip-address 1.0.0.11
[Spoke3-vam-client-Spoke3] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke3-vam-client-Spoke3] client enable
[Spoke3-vam-client-Spoke3] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke3] ike keychain abc
[Spoke3-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke3-ike-keychain-abc] quit
[Spoke3] ike profile abc
[Spoke3-ike-profile-abc] keychain abc
[Spoke3-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke3] ipsec transform-set abc
[Spoke3-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke3-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke3-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke3-ipsec-transform-set-abc] quit
[Spoke3] ipsec profile abc isakmp
[Spoke3-ipsec-profile-isakmp-abc] transform-set abc
[Spoke3-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke3-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke3] ospf 1
[Spoke3-ospf-1] area 2
[Spoke3-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Spoke3-ospf-1-area-0.0.0.2] network 192.168.40.0 0.0.0.255
[Spoke3-ospf-1-area-0.0.0.2] quit
[Spoke3-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。将 Spoke3 的 DR 优先级配置为 0，以使 Spoke3 不参与 DR/BDR 选举。

```
[Spoke3] interface tunnel 1 mode advpn udp
[Spoke3-Tunnel1] ip address 192.168.2.2 255.255.255.0
[Spoke3-Tunnel1] vam client Spoke3
[Spoke3-Tunnel1] ospf network-type broadcast
[Spoke3-Tunnel1] ospf dr-priority 0
[Spoke3-Tunnel1] advpn network 192.168.40.0 255.255.255.0
[Spoke3-Tunnel1] source gigabitethernet 2/0/1
[Spoke3-Tunnel1] tunnel protection ipsec profile abc
[Spoke3-Tunnel1] undo shutdown
[Spoke3-Tunnel1] quit
```

(9) 配置 Spoke4

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke4。

```
<Spoke4> system-view
[Spoke4] vam client name Spoke4
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke4-vam-client-Spoke4] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke4-vam-client-Spoke4] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke4，密码为 spoke4。

```
[Spoke4-vam-client-Spoke4] user spoke4 password simple spoke4
```

配置 VAM Server 的 IP 地址。

```
[Spoke4-vam-client-Spoke4] server primary ip-address 1.0.0.11
[Spoke4-vam-client-Spoke4] server secondary ip-address 1.0.0.12
```

开启 VAM Client 功能。

```
[Spoke4-vam-client-Spoke4] client enable
[Spoke4-vam-client-Spoke4] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke4] ike keychain abc
[Spoke4-ike-keychain-abc] pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[Spoke4-ike-keychain-abc] quit
[Spoke4] ike profile abc
[Spoke4-ike-profile-abc] keychain abc
[Spoke4-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke4] ipsec transform-set abc
[Spoke4-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke4-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke4-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke4-ipsec-transform-set-abc] quit
[Spoke4] ipsec profile abc isakmp
```

```
[Spoke4-ipsec-profile-isakmp-abc] transform-set abc
[Spoke4-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke4-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke4] ospf 1
[Spoke4-ospf-1] area 2
[Spoke4-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Spoke4-ospf-1-area-0.0.0.2] network 192.168.50.0 0.0.0.255
[Spoke4-ospf-1-area-0.0.0.2] network 192.168.60.0 0.0.0.255
[Spoke4-ospf-1-area-0.0.0.2] quit
[Spoke4-ospf-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。将 Spoke4 的 DR 优先级配置为 0，以使 Spoke4 不参与 DR/BDR 选举。

```
[Spoke4] interface tunnel1 mode advpn udp
[Spoke4-Tunnel1] ip address 192.168.2.3 255.255.255.0
[Spoke4-Tunnel1] vam client Spoke4
[Spoke4-Tunnel1] ospf network-type broadcast
[Spoke4-Tunnel1] ospf dr-priority 0
[Spoke4-Tunnel1] advpn network 192.168.50.0 255.255.255.0
[Spoke4-Tunnel1] advpn network 192.168.60.0 255.255.255.0
[Spoke4-Tunnel1] source gigabitethernet 2/0/1
[Spoke4-Tunnel1] tunnel protection ipsec profile abc
[Spoke4-Tunnel1] undo shutdown
[Spoke4-Tunnel1] quit
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[PrimaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 10
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    No   0H 52M  7S
0          192.168.0.2      1.0.0.2                   Hub    No   0H 47M 31S
0          192.168.0.3      1.0.0.3                   Hub    No   0H 28M 25S
1          192.168.1.1      1.0.0.1                   Hub    No   0H 52M  7S
1          192.168.1.2      1.0.0.2                   Hub    No   0H 47M 31S
1          192.168.1.3      1.0.0.4                   Spoke  No   0H 18M 26S
1          192.168.1.4      1.0.0.5                   Spoke  No   0H 28M 25S
2          192.168.2.1      1.0.0.3                   Hub    No   0H 28M 25S
2          192.168.2.2      1.0.0.6                   Spoke  No   0H 25M 40S
2          192.168.2.3      1.0.0.7                   Spoke  No   0H 25M 31S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[SecondaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 10
```

```
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    No   0H 52M  7S
0          192.168.0.2      1.0.0.2                   Hub    No   0H 47M 31S
0          192.168.0.3      1.0.0.3                   Hub    No   0H 28M 25S
1          192.168.1.1      1.0.0.1                   Hub    No   0H 52M  7S
1          192.168.1.2      1.0.0.2                   Hub    No   0H 47M 31S
1          192.168.1.3      1.0.0.4                   Spoke  No   0H 18M 26S
1          192.168.1.4      1.0.0.5                   Spoke  No   0H 28M 25S
2          192.168.2.1      1.0.0.3                   Hub    No   0H 28M 25S
2          192.168.2.2      1.0.0.6                   Spoke  No   0H 25M 40S
2          192.168.2.3      1.0.0.7                   Spoke  No   0H 25M 31S
```

以上显示信息表示 Hub1、Hub2、Hub3、Spoke1、Spoke2、Spoke3 和 Spoke4 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv4 ADVPN 隧道信息。

```
[Hub1] display advpn session
Interface         : Tunnel1
Number of sessions: 3
Private address  Public address             Port  Type  State      Holding time
192.168.1.2      1.0.0.2                    18001 H-H   Success    0H 46M  8S
192.168.1.3      1.0.0.3                    18001 H-S   Success    0H 27M 27S
192.168.1.4      1.0.0.4                    18001 H-S   Success    0H 18M 18S

Interface         : Tunnel2
Number of sessions: 2
Private address  Public address             Port  Type  State      Holding time
192.168.0.2      1.0.0.2                    18001 H-H   Success    0H 46M  8S
192.168.0.3      1.0.0.3                    18001 H-H   Success    0H 27M 27S
```

以上显示信息表示 Hub1 与 Hub2、Hub3、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv4 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address  Public address             Port  Type  State      Holding time
192.168.1.1      1.0.0.1                    18001 S-H   Success    0H 46M  8S
192.168.1.2      1.0.0.2                    18001 S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

显示 Spoke3 上的 IPv4 ADVPN 隧道信息。

```
[Spoke3] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address  Public address             Port  Type  State      Holding time
192.168.2.1      1.0.0.3                    18001 S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke3 与 Hub3 建立了 Hub-Spoke 永久隧道。Spoke4 上的显示信息与 Spoke3 类似。

1.10.6 IPv6 划分多个Hub组ADVPN典型配置举例

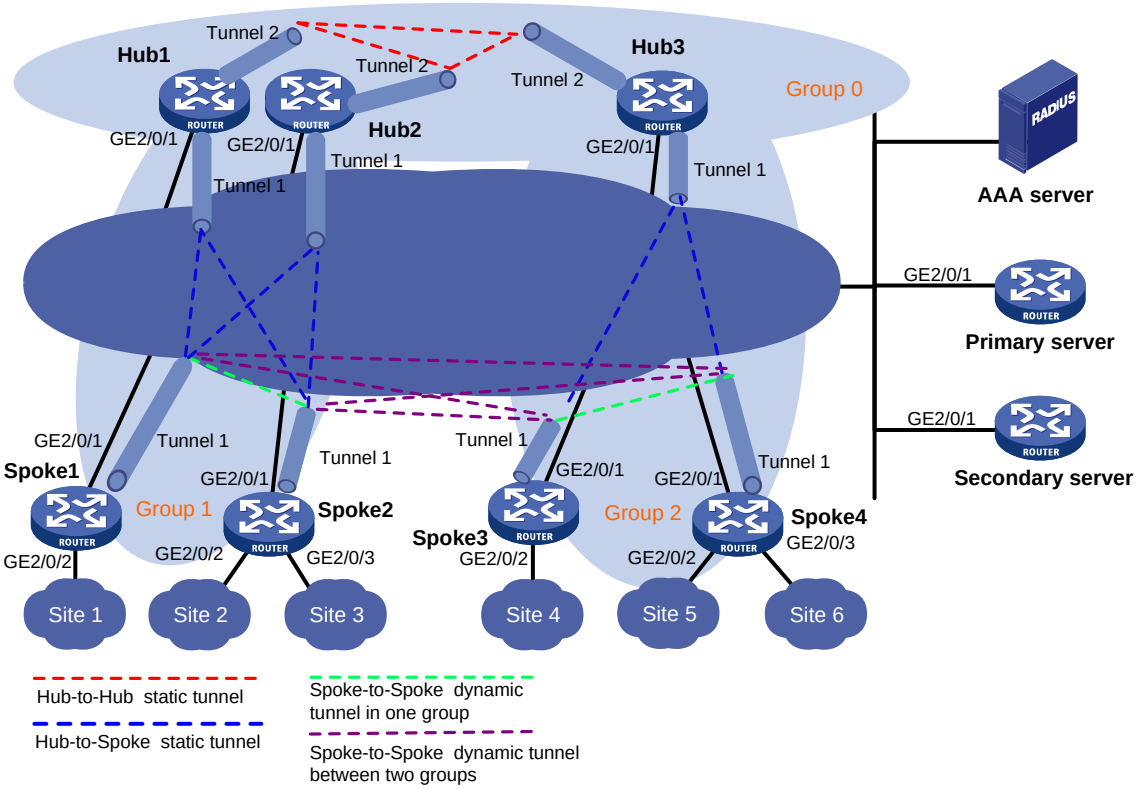
1. 组网需求

ADVPN 域中包含的 ADVPN 节点较多，通过划分多个 Hub 组来减轻 Hub 的负担。具体需求如下：

- 主、备 VAM Server 负责管理、维护各个节点的信息。
- AAA 服务器负责对 VAM Client 进行认证和计费管理。
- 将 ADVPN 域划分为三个 Hub 组：Hub1、Hub2 和 Hub3 属于 Hub 组 0；Hub1、Hub2、Spoke1 和 Spoke2 属于 Hub 组 1，两个 Hub 互为备份；Hub3、Spoke3 和 Spoke4 属于 Hub 组 2。
- Hub 组 1 和 Hub 组 2 内采用 Full-Mesh 组网方式。
- 允许所有的 Spoke 建立跨 Hub 组的 Spoke-Spoke 直连隧道。

2. 组网图

图1-12 IPv6 划分多个 Hub 组 ADVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
Hub 1	GE2/0/1	1::1/64	Spoke 1	GE2/0/1	1::4/64
	Tunnel1	192:168:1::1/64		GE2/0/2	192:168:10::1/64
	Tunnel2	192:168::1/64		Tunnel1	192:168:1::3/64
Hub 2	GE2/0/1	1::2/64	Spoke 2	GE2/0/1	1::5/64
	Tunnel1	192:168:1::2/64		GE2/0/2	192:168:20::1/64
	Tunnel2	192:168::2/64		GE2/0/3	192:168:30::1/64
Hub 3	GE2/0/1	1::3/64		Tunnel1	192:168:1::4/64
	Tunnel1	192:168:2::1/64	Spoke 3	GE2/0/1	1::6/64
	Tunnel2	192:168::3/64		GE2/0/2	192:168:40::1/64
AAA server		1::10/64		Tunnel1	192:168:2::2/64
Primary server	GE2/0/1	1::11/64	Spoke 4	GE2/0/1	1::7/64
Secondary server	GE2/0/1	1::12/64		GE2/0/2	192:168:50::1/64
				GE2/0/3	192:168:60::1/64
				Tunnel1	192:168:2::3/64

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
[PrimaryServer] radius scheme abc
[PrimaryServer-radius-abc] primary authentication ipv6 1::10 1812
[PrimaryServer-radius-abc] primary accounting ipv6 1::10 1813
[PrimaryServer-radius-abc] key authentication simple 123
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```

配置 ISP 域的 AAA 方案。

```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
[PrimaryServer] domain default enable abc
```

- 配置 VAM Server

创建 ADVPN 域 abc。

```
[PrimaryServer] vam server advpn-domain abc id 1
```

创建 Hub 组 0。

```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```

指定 Hub 组内 Hub 的 IPv6 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::1
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::2
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub ipv6 private-address 192:168::3
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```

创建 Hub 组 1。

```
[PrimaryServer-vam-server-domain-abc] hub-group 1
```

指定 Hub 组内 Hub 的 IPv6 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-1] hub ipv6 private-address 192:168:1::1
[PrimaryServer-vam-server-domain-abc-hub-group-1] hub ipv6 private-address 192:168:1::2
```

指定 Hub 组内 Spoke 的 IPv6 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-1] spoke ipv6 private-address network
192:168:1::0 64
```

允许建立跨组 Spoke-Spoke 直连隧道。

```
[PrimaryServer-vam-server-domain-abc-hub-group-1] shortcut ipv6 interest all
[PrimaryServer-vam-server-domain-abc-hub-group-1] quit
```

创建 Hub 组 2。

```
[PrimaryServer-vam-server-domain-abc] hub-group 2
```

指定 Hub 组内 Hub 的 IPv6 私网地址。

```
[PrimaryServer-vam-server-domain-abc-hub-group-2] hub ipv6 private-address 192:168:2::1
```

指定 Hub 组内 Spoke 的 IPv6 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-2] spoke ipv6 private-address network
192:168:2::0 64
[PrimaryServer-vam-server-domain-abc-hub-group-1] shortcut ipv6 interest all
[PrimaryServer-vam-server-domain-abc-hub-group-2] quit
```

配置 VAM Server 的预共享密钥为 123456。

```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```

配置对 VAM Client 进行 CHAP 认证。

```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```

启动该 ADVPN 域的 VAM Server 功能。

```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```

(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1Group0。

```
<Hub1> system-view
[Hub1] vam client name Hub1Group0
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub1-vam-client-Hub1Group0] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub1-vam-client-Hub1Group0] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub1，密码为 hub1。

```
[Hub1-vam-client-Hub1Group0] user hub1 password simple hub1
```

配置 VAM Server 的 IP 地址。

```
[Hub1-vam-client-Hub1Group0] server primary ipv6-address 1::11
[Hub1-vam-client-Hub1Group0] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1Group0] client enable
[Hub1-vam-client-Hub1Group0] quit
```

创建 VAM Client Hub1Group1。

```
[Hub1] vam client name Hub1Group1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub1-vam-client-Hub1Group1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub1-vam-client-Hub1Group1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub1，密码为 hub1。

```
[Hub1-vam-client-Hub1Group1] user hub1 password simple hub1
```

配置 VAM Server 的 IP 地址。

```
[Hub1-vam-client-Hub1Group1] server primary ipv6-address 1::11
[Hub1-vam-client-Hub1Group1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1Group1] client enable
[Hub1-vam-client-Hub1Group1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub1] ike keychain abc
[Hub1-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
[Hub1-ike-keychain-abc] quit
[Hub1] ike profile abc
[Hub1-ike-profile-abc] keychain abc
[Hub1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub1] ipsec transform-set abc
[Hub1-ipsec-transform-set-abc] encapsulation-mode transport
[Hub1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub1-ipsec-transform-set-abc] quit
[Hub1] ipsec profile abc isakmp
[Hub1-ipsec-profile-isakmp-abc] transform-set abc
[Hub1-ipsec-profile-isakmp-abc] ike-profile abc
[Hub1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Hub1] ospfv3 1
[Hub1-ospfv3-1] router-id 0.0.0.1
[Hub1-ospfv3-1] area 0
[Hub1-ospfv3-1-area-0.0.0.0] quit
[Hub1-ospfv3-1] area 1
[Hub1-ospfv3-1-area-0.0.0.1] quit
[Hub1-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel1 mode advpn udp
[Hub1-Tunnel1] ipv6 address 192:168:1::1 64
[Hub1-Tunnel1] ipv6 address fe80::1:1 link-local
[Hub1-Tunnel1] vam ipv6 client Hub1Group1
[Hub1-Tunnel1] ospfv3 1 area 1
[Hub1-Tunnel1] ospfv3 network-type broadcast
[Hub1-Tunnel1] source gigabitethernet 2/0/1
[Hub1-Tunnel1] tunnel protection ipsec profile abc
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel2。

```
[Hub1] interface tunnel2 mode advpn udp
```

```
[Hub1-Tunnel2] ipv6 address 192:168::1 64
[Hub1-Tunnel2] ipv6 address fe80::1 link-local
[Hub1-Tunnel2] vam ipv6 client Hub1Group0
[Hub1-Tunnel2] ospfv3 1 area 0
[Hub1-Tunnel2] ospf network-type broadcast
[Hub1-Tunnel2] source gigabitethernet 2/0/1
[Hub1-Tunnel2] tunnel protection ipsec profile abc
[Hub1-Tunnel2] undo shutdown
[Hub1-Tunnel2] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub2Group0。

```
<Hub2> system-view
[Hub2] vam client name Hub2Group0
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2Group0] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2Group0] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub2，密码为 hub2。

```
[Hub2-vam-client-Hub2Group0] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2Group0] server primary ipv6-address 1::11
[Hub2-vam-client-Hub2Group0] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2Group0] client enable
[Hub2-vam-client-Hub2Group0] quit
```

创建 VAM Client Hub2Group1。

```
[Hub2] vam client name Hub2Group1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub2-vam-client-Hub2Group1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub2-vam-client-Hub2Group1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub2，密码为 hub2。

```
[Hub2-vam-client-Hub2Group1] user hub2 password simple hub2
```

配置 VAM Server 的 IP 地址。

```
[Hub2-vam-client-Hub2Group1] server primary ipv6-address 1::11
[Hub2-vam-client-Hub2Group1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub2-vam-client-Hub2Group1] client enable
[Hub2-vam-client-Hub2Group1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub2] ike keychain abc
```

```
[Hub2-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
[Hub2-ike-keychain-abc] quit
[Hub2] ike profile abc
[Hub2-ike-profile-abc] keychain abc
[Hub2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub2] ipsec transform-set abc
[Hub2-ipsec-transform-set-abc] encapsulation-mode transport
[Hub2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub2-ipsec-transform-set-abc] quit
[Hub2] ipsec profile abc isakmp
[Hub2-ipsec-profile-isakmp-abc] transform-set abc
[Hub2-ipsec-profile-isakmp-abc] ike-profile abc
[Hub2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Hub2] ospfv3 1
[Hub2-ospfv3-1] router-id 0.0.0.2
[Hub2-ospfv3-1] area 0
[Hub2-ospfv3-1-area-0.0.0.0] quit
[Hub2-ospfv3-1] area 1
[Hub2-ospfv3-1-area-0.0.0.1] quit
[Hub2-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub2] interface tunnel1 mode advpn udp
[Hub2-Tunnel1] ipv6 address 192:168:1::2 64
[Hub2-Tunnel1] ipv6 address fe80::1:2 link-local
[Hub2-Tunnel1] vam ipv6 client Hub2Group1
[Hub2-Tunnel1] ospfv3 1 area 1
[Hub2-Tunnel1] ospfv3 network-type broadcast
[Hub2-Tunnel1] source gigabitethernet 2/0/1
[Hub2-Tunnel1] tunnel protection ipsec profile abc
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel2。

```
[Hub2] interface tunnel2 mode advpn udp
[Hub2-Tunnel2] ipv6 address 192:168::2 64
[Hub2-Tunnel2] ipv6 address fe80::2 link-local
[Hub2-Tunnel2] vam ipv6 client Hub2Group0
[Hub2-Tunnel2] ospfv3 1 area 0
[Hub2-Tunnel2] ospfv3 network-type broadcast
[Hub2-Tunnel2] source gigabitethernet 2/0/1
[Hub2-Tunnel2] tunnel protection ipsec profile abc
[Hub2-Tunnel2] undo shutdown
[Hub2-Tunnel2] quit
```

(5) 配置 Hub3

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub3Group0。

```
<Hub3> system-view
[Hub3] vam client name Hub3Group0
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub3-vam-client-Hub3Group0] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub3-vam-client-Hub3Group0] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub3，密码为 hub3。

```
[Hub3-vam-client-Hub3Group0] user hub3 password simple hub3
```

配置 VAM Server 的 IP 地址。

```
[Hub3-vam-client-Hub3Group0] server primary ipv6-address 1::11
[Hub3-vam-client-Hub3Group0] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub3-vam-client-Hub3Group0] client enable
[Hub3-vam-client-Hub3Group0] quit
```

创建 VAM Client Hub3Group1。

```
[Hub3] vam client name Hub3Group1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub3-vam-client-Hub3Group1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub3-vam-client-Hub3Group1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub3，密码为 hub3。

```
[Hub3-vam-client-Hub3Group1] user hub3 password simple hub3
```

配置 VAM Server 的 IP 地址。

```
[Hub3-vam-client-Hub3Group1] server primary ipv6-address 1::11
[Hub3-vam-client-Hub3Group1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Hub3-vam-client-Hub3Group1] client enable
[Hub3-vam-client-Hub3Group1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Hub3] ike keychain abc
[Hub3-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
[Hub3-ike-keychain-abc] quit
[Hub3] ike profile abc
[Hub3-ike-profile-abc] keychain abc
[Hub3-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Hub3] ipsec transform-set abc
[Hub3-ipsec-transform-set-abc] encapsulation-mode transport
```

```
[Hub3-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Hub3-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Hub3-ipsec-transform-set-abc] quit
[Hub3] ipsec profile abc isakmp
[Hub3-ipsec-profile-isakmp-abc] transform-set abc
[Hub3-ipsec-profile-isakmp-abc] ike-profile abc
[Hub3-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Hub3] ospfv3 1
[Hub3-ospfv3-1] router-id 0.0.0.3
[Hub3-ospfv3-1] area 0
[Hub3-ospfv3-1-area-0.0.0.0] quit
[Hub3-ospfv3-1] area 2
[Hub3-ospfv3-1-area-0.0.0.2] quit
[Hub3-ospfv3-1] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。

```
[Hub3] interface tunnel1 mode advpn udp
[Hub3-Tunnel1] ipv6 address 192:168:2::1 64
[Hub3-Tunnel1] ipv6 address fe80::2:1 link-local
[Hub3-Tunnel1] vam ipv6 client Hub3Group1
[Hub3-Tunnel1] ospfv3 1 area 2
[Hub3-Tunnel1] ospfv3 network-type broadcast
[Hub3-Tunnel1] source gigabitethernet 2/0/1
[Hub3-Tunnel1] tunnel protection ipsec profile abc
[Hub3-Tunnel1] undo shutdown
[Hub3-Tunnel1] quit
```

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel2。

```
[Hub3] interface tunnel2 mode advpn udp
[Hub3-Tunnel2] ipv6 address 192:168::3 64
[Hub3-Tunnel2] ipv6 address fe80::3 link-local
[Hub3-Tunnel2] vam ipv6 client Hub3Group0
[Hub3-Tunnel2] ospfv3 1 area 0
[Hub3-Tunnel2] ospfv3 network-type broadcast
[Hub3-Tunnel2] source gigabitethernet 2/0/1
[Hub3-Tunnel2] tunnel protection ipsec profile abc
[Hub3-Tunnel2] undo shutdown
[Hub3-Tunnel2] quit
```

(6) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。

```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。

```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```

配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ipv6-address 1::11
[Spoke1-vam-client-Spoke1] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke1] ike keychain abc
[Spoke1-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
[Spoke1-ike-keychain-abc] quit
[Spoke1] ike profile abc
[Spoke1-ike-profile-abc] keychain abc
[Spoke1-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke1] ipsec transform-set abc
[Spoke1-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke1-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke1-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke1-ipsec-transform-set-abc] quit
[Spoke1] ipsec profile abc isakmp
[Spoke1-ipsec-profile-isakmp-abc] transform-set abc
[Spoke1-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke1-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Spoke1] ospfv3 1
[Spoke1-ospfv3-1] router-id 0.0.0.4
[Spoke1-ospfv3-1] area 1
[Spoke1-ospfv3-1-area-0.0.0.1] quit
[Spoke1-ospfv3-1] quit
[Spoke1] interface gigabitethernet 2/0/2
[Spoke1-GigabitEthernet2/0/2] ospfv3 1 area 1
[Spoke1-GigabitEthernet2/0/2] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。将 Spoke1 的 DR 优先级配置为 0，以使 Spoke1 不参与 DR/BDR 选举。

```
[Spoke1] interface tunnel1 mode advpn udp
[Spoke1-Tunnel1] ipv6 address 192:168:1::3 64
[Spoke1-Tunnel1] ipv6 address fe80::1:3 link-local
```

```
[Spoke1-Tunnel1] vam ipv6 client Spoke1
[Spoke1-Tunnel1] ospfv3 1 area 1
[Spoke1-Tunnel1] ospfv3 network-type broadcast
[Spoke1-Tunnel1] ospf dr-priority 0
[Spoke1-Tunnel1] advpn ipv6 network 192:168:10::0 64
[Spoke1-Tunnel1] source gigabitethernet 2/0/1
[Spoke1-Tunnel1] tunnel protection ipsec profile abc
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```

(7) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。

```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。

```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```

配置 VAM Server 的 IP 地址。

```
[Spoke2-vam-client-Spoke2] server primary ipv6-address 1::11
[Spoke2-vam-client-Spoke2] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke2] ike keychain abc
[Spoke2-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
[Spoke2-ike-keychain-abc] quit
[Spoke2] ike profile abc
[Spoke2-ike-profile-abc] keychain abc
[Spoke2-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke2] ipsec transform-set abc
[Spoke2-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke2-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke2-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke2-ipsec-transform-set-abc] quit
[Spoke2] ipsec profile abc isakmp
[Spoke2-ipsec-profile-isakmp-abc] transform-set abc
[Spoke2-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke2-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Spoke2] ospfv3 1
[Spoke2-ospfv3-1] router-id 0.0.0.5
[Spoke2-ospfv3-1] area 1
[Spoke2-ospfv3-1-area-0.0.0.1] quit
[Spoke2-ospfv3-1] quit
[Spoke1] interface gigabitethernet 2/0/2
[Spoke1-GigabitEthernet2/0/2] ospfv3 1 area 1
[Spoke1-GigabitEthernet2/0/2] quit
[Spoke1] interface gigabitethernet 2/0/3
[Spoke1-GigabitEthernet2/0/3] ospfv3 1 area 1
[Spoke1-GigabitEthernet2/0/3] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。将 Spoke2 的 DR 优先级配置为 0，以使 Spoke2 不参与 DR/BDR 选举。

```
[Spoke2] interface tunnel1 mode advpn udp
[Spoke2-Tunnel1] ipv6 address 192:168:1::4 64
[Spoke2-Tunnel1] ipv6 address fe80::1:4 link-local
[Spoke2-Tunnel1] vam ipv6 client Spoke2
[Spoke2-Tunnel1] ospfv3 1 area 1
[Spoke2-Tunnel1] ospfv3 network-type broadcast
[Spoke2-Tunnel1] ospf dr-priority 0
[Spoke2-Tunnel1] advpn ipv6 network 192:168:20::0 64
[Spoke2-Tunnel1] advpn ipv6 network 192:168:30::0 64
[Spoke2-Tunnel1] source gigabitethernet 2/0/1
[Spoke2-Tunnel1] tunnel protection ipsec profile abc
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

(8) 配置 Spoke3

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke3。

```
<Spoke3> system-view
[Spoke3] vam client name Spoke3
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke3-vam-client-Spoke3] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke3-vam-client-Spoke3] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke3，密码为 spoke3。

```
[Spoke3-vam-client-Spoke3] user spoke3 password simple spoke3
```

配置 VAM Server 的 IP 地址。

```
[Spoke3-vam-client-Spoke3] server primary ipv6-address 1::11
[Spoke3-vam-client-Spoke3] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke3-vam-client-Spoke3] client enable
[Spoke3-vam-client-Spoke3] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke3] ike keychain abc
[Spoke3-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
[Spoke3-ike-keychain-abc] quit
[Spoke3] ike profile abc
[Spoke3-ike-profile-abc] keychain abc
[Spoke3-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke3] ipsec transform-set abc
[Spoke3-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke3-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke3-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke3-ipsec-transform-set-abc] quit
[Spoke3] ipsec profile abc isakmp
[Spoke3-ipsec-profile-isakmp-abc] transform-set abc
[Spoke3-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke3-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Spoke3] ospfv3 1
[Spoke3-ospfv3-1] router-id 0.0.0.6
[Spoke3-ospfv3-1] area 2
[Spoke3-ospfv3-1-area-0.0.0.2] quit
[Spoke3-ospfv3-1] quit
[Spoke3] interface gigabitethernet 2/0/2
[Spoke3-GigabitEthernet2/0/2] ospfv3 1 area 2
[Spoke3-GigabitEthernet2/0/2] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。将 Spoke3 的 DR 优先级配置为 0，以使 Spoke3 不参与 DR/BDR 选举。

```
[Spoke3] interface tunnel1 mode advpn udp
[Spoke3-Tunnel1] ipv6 address 192:168:2::2 64
[Spoke3-Tunnel1] ipv6 address fe80::2:2 link-local
[Spoke3-Tunnel1] vam ipv6 client Spoke3
[Spoke3-Tunnel1] ospfv3 1 area 2
[Spoke3-Tunnel1] ospfv3 network-type broadcast
[Spoke3-Tunnel1] ospf dr-priority 0
[Spoke3-Tunnel1] advpn ipv6 network 192:168:40::0 64
[Spoke3-Tunnel1] source gigabitethernet 2/0/1
[Spoke3-Tunnel1] tunnel protection ipsec profile abc
[Spoke3-Tunnel1] undo shutdown
[Spoke3-Tunnel1] quit
```

(9) 配置 Spoke4

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke4。

```
<Spoke4> system-view
[Spoke4] vam client name Spoke4
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke4-vam-client-Spoke4] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke4-vam-client-Spoke4] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke4，密码为 spoke4。

```
[Spoke4-vam-client-Spoke4] user spoke4 password simple spoke4
```

配置 VAM Server 的 IP 地址。

```
[Spoke4-vam-client-Spoke4] server primary ipv6-address 1::11
[Spoke4-vam-client-Spoke4] server secondary ipv6-address 1::12
```

开启 VAM Client 功能。

```
[Spoke4-vam-client-Spoke4] client enable
[Spoke4-vam-client-Spoke4] quit
```

- 配置 IPsec 安全框架

配置 IKE 框架。

```
[Spoke4] ike keychain abc
[Spoke4-ike-keychain-abc] pre-shared-key address :: 0 key simple 123456
[Spoke4-ike-keychain-abc] quit
[Spoke4] ike profile abc
[Spoke4-ike-profile-abc] keychain abc
[Spoke4-ike-profile-abc] quit
```

配置 IPsec 安全框架。

```
[Spoke4] ipsec transform-set abc
[Spoke4-ipsec-transform-set-abc] encapsulation-mode transport
[Spoke4-ipsec-transform-set-abc] esp encryption-algorithm des-cbc
[Spoke4-ipsec-transform-set-abc] esp authentication-algorithm sha1
[Spoke4-ipsec-transform-set-abc] quit
[Spoke4] ipsec profile abc isakmp
[Spoke4-ipsec-profile-isakmp-abc] transform-set abc
[Spoke4-ipsec-profile-isakmp-abc] ike-profile abc
[Spoke4-ipsec-profile-isakmp-abc] quit
```

- 配置 OSPFv3 路由

启动 OSPFv3，以发布私网的路由信息。

```
[Spoke4] ospfv3 1
[Spoke4-ospfv3-1] router-id 0.0.0.7
[Spoke4-ospfv3-1] area 2
[Spoke4-ospfv3-1-area-0.0.0.2] quit
[Spoke4-ospfv3-1] quit
[Spoke4] interface gigabitethernet 2/0/2
[Spoke4-GigabitEthernet2/0/2] ospfv3 1 area 2
[Spoke4-GigabitEthernet2/0/2] quit
```

```
[Spoke4] interface gigabitethernet 2/0/3
[Spoke4-GigabitEthernet2/0/3] ospfv3 1 area 2
[Spoke4-GigabitEthernet2/0/3] quit
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv6 ADVPN 隧道接口 Tunnel1。将 Spoke4 的 DR 优先级配置为 0，以使 Spoke4 不参与 DR/BDR 选举。

```
[Spoke4] interface tunnel1 mode advpn udp
[Spoke4-Tunnel1] ipv6 address 192:168:2::3 64
[Spoke4-Tunnel1] ipv6 address fe80::2:3 link-local
[Spoke4-Tunnel1] vam ipv6 client Spoke4
[Spoke4-Tunnel1] ospfv3 1 area 2
[Spoke4-Tunnel1] ospfv3 network-type broadcast
[Spoke4-Tunnel1] ospf dr-priority 0
[Spoke4-Tunnel1] advpn ipv6 network 192:168:50::0 64
[Spoke4-Tunnel1] advpn ipv6 network 192:168:60::0 64
[Spoke4-Tunnel1] source gigabitethernet 2/0/1
[Spoke4-Tunnel1] tunnel protection ipsec profile abc
[Spoke4-Tunnel1] undo shutdown
[Spoke4-Tunnel1] quit
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv6 私网地址映射信息。

```
[PrimaryServer] display vam server ipv6 address-map
ADVPN domain name: 1
Total private address mappings: 10
Group      Private address       Public address         Type   NAT  Holding time
0          192:168::1            1::1                   Hub    No   0H 52M  7S
0          192:168::2            1::2                   Hub    No   0H 47M 31S
0          192:168::3            1::3                   Hub    No   0H 28M 25S
1          192:168:1::1          1::1                   Hub    No   0H 52M  7S
1          192:168:1::2          1::2                   Hub    No   0H 47M 31S
1          192:168:1::3          1::4                   Spoke  No   0H 18M 26S
1          192:168:1::4          1::5                   Spoke  No   0H 28M 25S
2          192:168:2::1          1::3                   Hub    No   0H 28M 25S
2          192:168:2::2          1::6                   Spoke  No   0H 25M 40S
2          192:168:2::3          1::7                   Spoke  No   0H 25M 31S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv6 私网地址映射信息。

```
[SecondaryServer] display vam server ipv6 address-map
ADVPN domain name: 1
Total private address mappings: 10
Group      Private address       Public address         Type   NAT  Holding time
0          192:168::1            1::1                   Hub    No   0H 52M  7S
0          192:168::2            1::2                   Hub    No   0H 47M 31S
0          192:168::3            1::3                   Hub    No   0H 28M 25S
1          192:168:1::1          1::1                   Hub    No   0H 52M  7S
1          192:168:1::2          1::2                   Hub    No   0H 47M 31S
1          192:168:1::3          1::4                   Spoke  No   0H 18M 26S
1          192:168:1::4          1::5                   Spoke  No   0H 28M 25S
```

```
2          192:168:2::1          1::3                  Hub    No   0H 28M 25S
2          192:168:2::2          1::6                  Spoke  No   0H 25M 40S
2          192:168:2::3          1::7                  Spoke  No   0H 25M 31S
```

以上显示信息表示 Hub1、Hub2、Hub3、Spoke1、Spoke2、Spoke3 和 Spoke4 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv6 ADVPN 隧道信息。

```
[Hub1] display advpn ipv6 session
Interface         : Tunnel1
Number of sessions: 3
Private address       Public address        Port  Type  State      Holding time
192:168:1::2          1::2                  18001 H-H   Success    0H 46M  8S
192:168:1::3          1::3                  18001 H-S   Success    0H 27M 27S
192:168:1::4          1::4                  18001 H-S   Success    0H 18M 18S

Interface         : Tunnel2
Number of sessions: 2
Private address       Public address        Port  Type  State      Holding time
192:168::2            1::2                  18001 H-H   Success    0H 46M  8S
192:168::3            1::3                  18001 H-H   Success    0H 27M 27S
```

以上显示信息表示 Hub1 与 Hub2、Hub3、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv6 ADVPN 隧道信息。

```
[Spoke1] display advpn ipv6 session
Interface         : Tunnel1
Number of sessions: 2
Private address       Public address        Port  Type  State      Holding time
192:168:1::1          1::1                  18001 S-H   Success    0H 46M  8S
192:168:1::2          1::2                  18001 S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

显示 Spoke3 上的 IPv6 ADVPN 隧道信息。

```
[Spoke3] display advpn ipv6 session
Interface         : Tunnel1
Number of sessions: 2
Private address       Public address        Port  Type  State      Holding time
192:168:2::1          1::3                  18001 S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke3 与 Hub3 建立了 Hub-Spoke 永久隧道。Spoke4 上的显示信息与 Spoke3 类似。

1.10.7 IPv4 Full-Mesh穿越NAT类型ADVPN典型配置举例

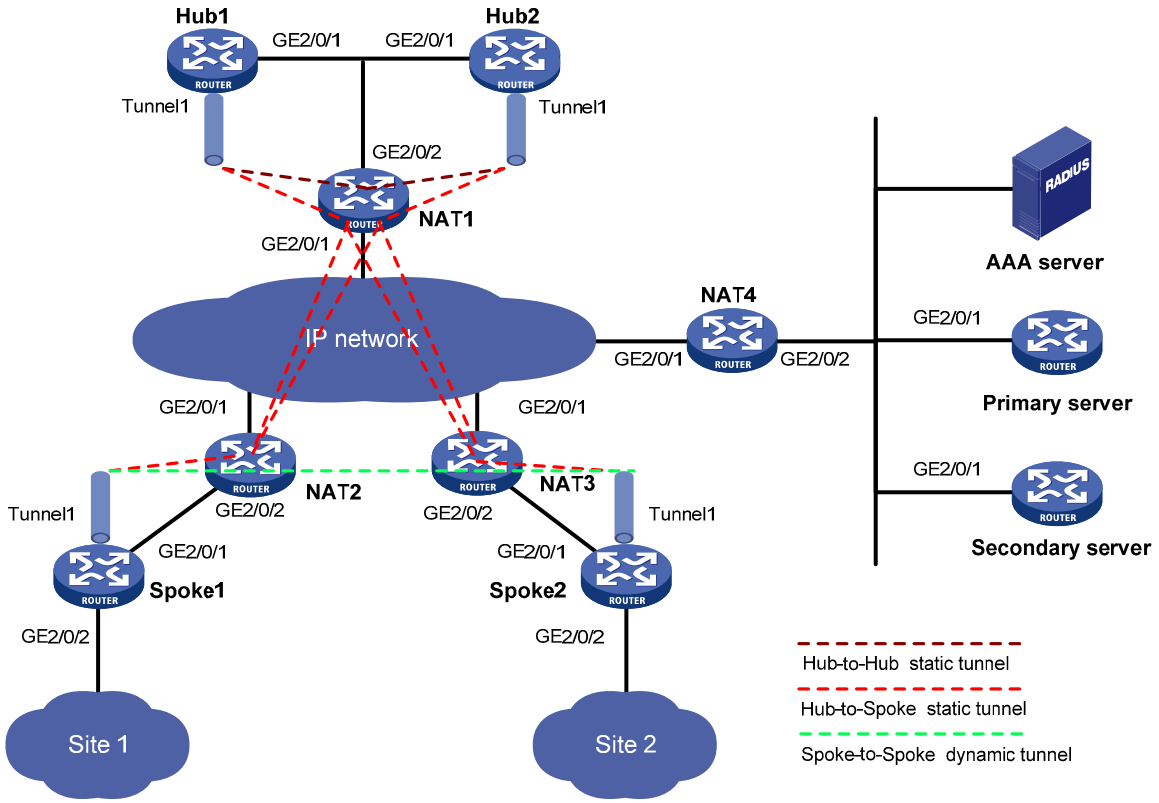
1. 组网需求

- 在 IPv4 Full-Mesh 的组网方式下，主、备 VAM Server 负责管理、维护各个节点的信息；AAA 服务器负责对 VAM Client 进行认证和计费管理；两个 Hub 互为备份，负责数据的转发和路由信息的交换。

- Spoke 与 Hub 之间建立永久的 ADVPN 隧道。
- 同一 ADVPN 域中，任意的两个 Spoke 之间在有数据时动态建立 ADVPN 隧道。
- VAM Server 和各个节点均在 NAT 网关之后。

2. 组网图

图1-13 IPv4 Full-Mesh 穿越 NAT 类型 ADVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
Hub 1	GE2/0/1	10.0.0.2/24	Spoke 1	GE2/0/1	10.0.0.2/24
	Tunnel1	192.168.0.1/24		GE2/0/2	192.168.1.1/24
Hub 2	GE2/0/1	10.0.0.3/24		Tunnel1	192.168.0.3/24
	Tunnel1	192.168.0.2/24	Spoke 2	GE2/0/1	10.0.0.2/24
NAT1	GE2/0/1	1.0.0.1/24		GE2/0/2	192.168.2.1/24
	GE2/0/2	10.0.0.1/24		Tunnel1	192.168.0.4/24
NAT2	GE2/0/1	1.0.0.2/24	NAT4	GE2/0/1	1.0.0.4/24
	GE2/0/2	10.0.0.1/24		GE2/0/2	10.0.0.1/24
NAT3	GE2/0/1	1.0.0.3/24	AAA server		10.0.0.2/24
	GE2/0/2	10.0.0.1/24	Primary server	GE2/0/1	10.0.0.3/24
			Secondary server	GE2/0/1	10.0.0.4/24

3. 配置步骤

(1) 配置主 VAM Server

- 配置各个接口的 IP 地址（略）
- 配置 AAA 认证

配置 RADIUS 方案。

```
<PrimaryServer> system-view
```

```
[PrimaryServer] radius scheme abc
[PrimaryServer-radius-abc] primary authentication 10.0.0.2 1812
[PrimaryServer-radius-abc] primary accounting 10.0.0.2 1813
[PrimaryServer-radius-abc] key authentication simple 123
[PrimaryServer-radius-abc] key accounting simple 123
[PrimaryServer-radius-abc] user-name-format without-domain
[PrimaryServer-radius-abc] quit
[PrimaryServer] radius session-control enable
```

配置 ISP 域的 AAA 方案。

```
[PrimaryServer] domain abc
[PrimaryServer-isp-abc] authentication advpn radius-scheme abc
[PrimaryServer-isp-abc] accounting advpn radius-scheme abc
[PrimaryServer-isp-abc] quit
[PrimaryServer] domain default enable abc
```

- 配置 VAM Server

创建 ADVPN 域 abc。

```
[PrimaryServer] vam server advpn-domain abc id 1
```

创建 Hub 组 0。

```
[PrimaryServer-vam-server-domain-abc] hub-group 0
```

指定 Hub 组内的 Hub：

- Hub1：IPv4 私网地址为 192.168.0.1，公网地址为 1.0.0.1（NAT 转换后的地址），ADVPN 报文的源 UDP 端口号为 4001（NAT 转换后的 UDP 端口号）。
- Hub2：IPv4 私网地址为 192.168.0.2，公网地址为 1.0.0.1（NAT 转换后的地址），ADVPN 报文的源 UDP 端口号为 4002（NAT 转换后的 UDP 端口号）。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.1
public-address 1.0.0.1 advpn-port 4001
[PrimaryServer-vam-server-domain-abc-hub-group-0] hub private-address 192.168.0.2
public-address 1.0.0.1 advpn-port 4002
```

指定 Hub 组内 Spoke 的 IPv4 私网地址范围。

```
[PrimaryServer-vam-server-domain-abc-hub-group-0] spoke private-address network
192.168.0.0 255.255.255.0
[PrimaryServer-vam-server-domain-abc-hub-group-0] quit
```

配置 VAM Server 的预共享密钥为 123456。

```
[PrimaryServer-vam-server-domain-abc] pre-shared-key simple 123456
```

配置对 VAM Client 进行 CHAP 认证。

```
[PrimaryServer-vam-server-domain-abc] authentication-method chap
```

启动该 ADVPN 域的 VAM Server 功能。

```
[PrimaryServer-vam-server-domain-abc] server enable
[PrimaryServer-vam-server-domain-abc] quit
```

- 配置默认路由。

```
[PrimaryServer] ip route-static 0.0.0.0 0 10.0.0.1
```

(2) 配置备 VAM Server

除 IP 地址外，备 VAM Server 的 ADVPN 配置与主 VAM Server 相同，不再赘述。

(3) 配置 Hub1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub1。

```
<Hub1> system-view
[Hub1] vam client name Hub1
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Hub1-vam-client-Hub1] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Hub1-vam-client-Hub1] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 hub1，密码为 hub1。

```
[Hub1-vam-client-Hub1] user hub1 password simple hub1
```

配置主 VAM Server 的 IP 地址为 1.0.0.4（NAT 转换后的地址），端口号为 4001（NAT 转换后的端口号）。

```
[Hub1-vam-client-Hub1] server primary ip-address 1.0.0.4 port 4001
```

配置备 VAM Server 的 IP 地址为 1.0.0.4（NAT 转换后的地址），端口号为 4002（NAT 转换后的端口号）。

```
[Hub1-vam-client-Hub1] server secondary ip-address 1.0.0.4 port 4002
```

开启 VAM Client 功能。

```
[Hub1-vam-client-Hub1] client enable
[Hub1-vam-client-Hub1] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Hub1] ospf 1
[Hub1-ospf-1] area 0
[Hub1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub1-ospf-1-area-0.0.0.0] quit
[Hub1-ospf-1] quit
```

配置默认路由。

```
[Hub1] ip route-static 0.0.0.0 0 10.0.0.1
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。

```
[Hub1] interface tunnel 1 mode advpn udp
[Hub1-Tunnel1] ip address 192.168.0.1 255.255.255.0
[Hub1-Tunnel1] vam client Hub1
[Hub1-Tunnel1] ospf network-type broadcast
[Hub1-Tunnel1] source gigabitethernet 2/0/1
[Hub1-Tunnel1] undo shutdown
[Hub1-Tunnel1] quit
```

(4) 配置 Hub2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Hub2。

```
<Hub2> system-view
```

```
[Hub2] vam client name Hub2
```
配置 VAM Client 所属的 ADVPN 域为 abc。
```
[Hub2-vam-client-Hub2] advpn-domain abc
```
配置 VAM Client 的预共享密钥。
```
[Hub2-vam-client-Hub2] pre-shared-key simple 123456
```
配置 VAM Client 的认证用户名为 hub2，密码为 hub2。
```
[Hub2-vam-client-Hub2] user hub2 password simple hub2
```
配置 VAM Server 的 IP 地址。
```
[Hub2-vam-client-Hub2] server primary ip-address 1.0.0.4 port 4001
[Hub2-vam-client-Hub2] server secondary ip-address 1.0.0.4 port 4002
```
开启 VAM Client 功能。
```
[Hub2-vam-client-Hub2] client enable
[Hub2-vam-client-Hub2] quit
```
- 配置 OSPF 路由

配置私网的路由信息。
```
[Hub2] ospf 1
[Hub2-ospf-1] area 0
[Hub2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Hub2-ospf-1-area-0.0.0.0] quit
[Hub2-ospf-1] quit
```
配置默认路由。
```
[Hub2] ip route-static 0.0.0.0 0 10.0.0.1
```
- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。
```
[Hub2] interface tunnel1 mode advpn udp
[Hub2-Tunnel1] ip address 192.168.0.2 255.255.255.0
[Hub2-Tunnel1] vam client Hub2
[Hub2-Tunnel1] ospf network-type broadcast
[Hub2-Tunnel1] source gigabitethernet 2/0/1
[Hub2-Tunnel1] undo shutdown
[Hub2-Tunnel1] quit
```
(5) 配置 Spoke1

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke1。
```
<Spoke1> system-view
[Spoke1] vam client name Spoke1
```
配置 VAM Client 所属的 ADVPN 域为 abc。
```
[Spoke1-vam-client-Spoke1] advpn-domain abc
```
配置 VAM Client 的预共享密钥。
```
[Spoke1-vam-client-Spoke1] pre-shared-key simple 123456
```
配置 VAM Client 的认证用户名为 spoke1，密码为 spoke1。
```
[Spoke1-vam-client-Spoke1] user spoke1 password simple spoke1
```
配置 VAM Server 的 IP 地址。

```
[Spoke1-vam-client-Spoke1] server primary ip-address 1.0.0.4 port 4001
[Spoke1-vam-client-Spoke1] server secondary ip-address 1.0.0.4 port 4002
```

开启 VAM Client 功能。

```
[Spoke1-vam-client-Spoke1] client enable
[Spoke1-vam-client-Spoke1] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke1] ospf 1
[Spoke1-ospf-1] area 0
[Spoke1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Spoke1-ospf-1-area-0.0.0.0] quit
[Spoke1-ospf-1] quit
```

配置默认路由。

```
[Spoke1] ip route-static 0.0.0.0 0 10.0.0.1
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。将 Spoke1 的 DR 优先级配置为 0，以使 Spoke1 不参与 DR/BDR 选举。

```
[Spoke1] interface tunnel1 mode advpn udp
[Spoke1-Tunnel1] ip address 192.168.0.3 255.255.255.0
[Spoke1-Tunnel1] vam client Spoke1
[Spoke1-Tunnel1] ospf network-type broadcast
[Spoke1-Tunnel1] ospf dr-priority 0
[Spoke1-Tunnel1] source gigabitethernet 2/0/1
[Spoke1-Tunnel1] undo shutdown
[Spoke1-Tunnel1] quit
```

(6) 配置 Spoke2

- 配置各接口的 IP 地址（略）
- 配置 VAM Client

创建 VAM Client Spoke2。

```
<Spoke2> system-view
[Spoke2] vam client name Spoke2
```

配置 VAM Client 所属的 ADVPN 域为 abc。

```
[Spoke2-vam-client-Spoke2] advpn-domain abc
```

配置 VAM Client 的预共享密钥。

```
[Spoke2-vam-client-Spoke2] pre-shared-key simple 123456
```

配置 VAM Client 的认证用户名为 spoke2，密码为 spoke2。

```
[Spoke2-vam-client-Spoke2] user spoke2 password simple spoke2
```

配置 VAM Server 的 IP 地址。

```
[Spoke2-vam-client-Spoke2] server primary ip-address 1.0.0.4 port 4001
[Spoke2-vam-client-Spoke2] server secondary ip-address 1.0.0.4 port 4002
```

开启 VAM Client 功能。

```
[Spoke2-vam-client-Spoke2] client enable
[Spoke2-vam-client-Spoke2] quit
```

- 配置 OSPF 路由

配置私网的路由信息。

```
[Spoke2] ospf 1
[Spoke2-ospf-1] area 0
[Spoke2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Spoke2-ospf-1-area-0.0.0.0] quit
[Spoke2-ospf-1] quit
```

配置默认路由。

```
[Spoke2] ip route-static 0.0.0.0 0 10.0.0.1
```

- 配置 ADVPN 隧道

配置 UDP 封装的 IPv4 ADVPN 隧道接口 Tunnel1。将 Spoke2 的 DR 优先级配置为 0，以使 Spoke2 不参与 DR/BDR 选举。

```
[Spoke2] interface tunnel1 mode advpn udp
[Spoke2-Tunnel1] ip address 192.168.0.4 255.255.255.0
[Spoke2-Tunnel1] vam client Spoke2
[Spoke2-Tunnel1] ospf network-type broadcast
[Spoke2-Tunnel1] ospf dr-priority 0
[Spoke2-Tunnel1] source gigabitethernet 2/0/1
[Spoke2-Tunnel1] undo shutdown
[Spoke2-Tunnel1] quit
```

(7) 配置 NAT1

- 配置各接口的 IP 地址（略）
- 配置 NAT 内部服务器

配置 ACL 2000，允许对内部网络中 10.0.0.0/24 网段的报文进行地址转换。

```
<NAT1> system-view
[NAT1] acl number 2000
[NAT1-acl-basic-2000] rule permit source 10.0.0.0 0.0.0.255
[NAT1-acl-basic-2000] quit
```

在接口 GigabitEthernet2/0/1 上配置 NAT 内部服务器，允许外网 ADVPN 节点使用地址 1.0.0.1 访问内网 Hub1 和 Hub2。Hub1 和 Hub2 使用的 ADVPN 报文源 UDP 端口号均为缺省值 18001，NAT 映射的外网端口号分别为 4001 和 4002。

```
[NAT1] interface gigabitethernet 2/0/1
[NAT1-GigabitEthernet2/0/1] nat server protocol udp global current-interface 4001 inside
10.0.0.2 18001
[NAT1-GigabitEthernet2/0/1] nat server protocol udp global current-interface 4002 inside
10.0.0.3 18001
[NAT1-GigabitEthernet2/0/1] nat outbound 2000
[NAT1-GigabitEthernet2/0/1] quit
```

在接口 GigabitEthernet2/0/2 上使能 NAT hairpin 功能。

```
[NAT1] interface gigabitethernet 2/0/2
[NAT1-GigabitEthernet2/0/2] nat hairpin enable
[NAT1-GigabitEthernet2/0/2] quit
```

(8) 配置 NAT2

- 配置各接口的 IP 地址（略）
- 配置 NAT 内部服务器

配置 ACL 2000，允许对内部网络中 10.0.0.0/24 网段的报文进行地址转换。

```
<NAT2> system-view
[NAT2] acl number 2000
[NAT2-acl-basic-2000] rule permit source 10.0.0.0 0.0.0.255
[NAT2-acl-basic-2000] quit
```

创建地址组 1。

```
[NAT2] nat address-group 1
```

添加地址组成员 1.0.0.2。

```
[NAT2-nat-address-group-1] address 1.0.0.2 1.0.0.2
[NAT2-nat-address-group-1] quit
```

在接口 GigabitEthernet2/0/1 上配置内网可以进行目的地址转换。

```
[NAT2] interface gigabitethernet 2/0/1
[NAT2-GigabitEthernet2/0/1] nat outbound 2000 address-group 1
[NAT2-GigabitEthernet2/0/1] quit
```

配置 PAT 方式下的地址转换模式为 EIM，即只要是来自相同源地址和源端口号的且匹配 ACL 2000 的报文，不论其目的地址是否相同，通过 PAT 转换后，其源地址和源端口号都被转换为同一个外部地址和端口号。

```
[NAT2] nat mapping-behavior endpoint-independent acl 2000
```

(9) 配置 NAT3

NAT3 的配置与 NAT2 的配置相似，这里省略。

(10) 配置 NAT4

- 配置各接口的 IP 地址（略）
- 配置 NAT 内部服务器

在接口 GigabitEthernet2/0/1 上配置 NAT 内部服务器，允许外网 VAM Client 使用地址 1.0.0.4 访问内网的 VAM Server。VAM 报文的源 UDP 端口号固定为 18000，主、备 VAM server 通过 NAT 映射的外网端口号分别为 4001 和 4002。

```
<NAT4> system-view
[NAT4] interface gigabitethernet 2/0/1
[NAT4-GigabitEthernet2/0/1] nat server protocol udp global current-interface 4001 inside
10.0.0.3 18000
[NAT4-GigabitEthernet2/0/1] nat server protocol udp global current-interface 4002 inside
10.0.0.4 18000
```

4. 验证配置

显示注册到主 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[PrimaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 4
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    Yes  0H 52M  7S
0          192.168.0.2      1.0.0.1                   Hub    Yes  0H 47M 31S
0          192.168.0.3      1.0.0.2                   Spoke  Yes  0H 28M 25S
0          192.168.0.4      1.0.0.3                   Spoke  Yes  0H 19M 15S
```

显示注册到备 VAM Server 的所有 VAM Client 的 IPv4 私网地址映射信息。

```
[SecondaryServer] display vam server address-map
ADVPN domain name: 1
Total private address mappings: 4
```

```
Group      Private address  Public address             Type   NAT  Holding time
0          192.168.0.1      1.0.0.1                   Hub    Yes  0H 52M  7S
0          192.168.0.2      1.0.0.1                   Hub    Yes  0H 47M 31S
0          192.168.0.3      1.0.0.2                   Spoke  Yes  0H 28M 25S
0          192.168.0.4      1.0.0.3                   Spoke  Yes  0H 19M 15S
```

以上显示信息表示 Hub1、Hub2、Spoke1 和 Spoke2 均已将地址映射信息注册到 VAM Server。

显示 Hub1 上的 IPv4 ADVPN 隧道信息。

```
[Hub1] display advpn session
Interface         : Tunnel1
Number of sessions: 3
Private address  Public address             Port  Type  State      Holding time
192.168.0.2      1.0.0.1                    4002  H-H   Success    0H 46M  8S
192.168.0.3      1.0.0.2                    2001  H-S   Success    0H 27M 27S
192.168.0.4      1.0.0.3                    2001  H-S   Success    0H 18M 18S
```

以上显示信息表示 Hub1 与 Hub2、Spoke1、Spoke2 建立了永久隧道。Hub2 上的显示信息与 Hub1 类似。

显示 Spoke1 上的 IPv4 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address  Public address             Port  Type  State      Holding time
192.168.0.1      1.0.0.1                    4001  S-H   Success    0H 46M  8S
192.168.0.2      1.0.0.1                    4002  S-H   Success    0H 46M  8S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke2 上的显示信息与 Spoke1 类似。

在 Spoke1 上 ping Spoke2 的私网地址 192.168.0.4。

```
[Spoke2] ping 192.168.0.4
Ping 192.168.0.4 (192.168.0.4): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.0.4: icmp_seq=0 ttl=255 time=4.000 ms
56 bytes from 192.168.0.4: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 192.168.0.4: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 192.168.0.4 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.000/4.000/1.549 ms
```

显示 Spoke1 上的 IPv4 ADVPN 隧道信息。

```
[Spoke1] display advpn session
Interface         : Tunnel1
Number of sessions: 3
Private address  Public address             Port  Type  State      Holding time
192.168.0.1      1.0.0.1                    4001  S-H   Success    0H 46M  8S
192.168.0.2      1.0.0.1                    4002  S-H   Success    0H 46M  8S
192.168.0.4      1.0.0.3                    2001  S-S   Success    0H  0M  1S
```

以上显示信息表示 Spoke1 与 Hub1、Hub2 建立了 Hub-Spoke 永久隧道。Spoke1 与 Spoke2 建立了 Spoke-Spoke 临时隧道。Spoke2 上的显示信息与 Spoke1 类似。