Architecture guide

Design guidelines for the HP ADVPN solution

Table of contents

Introduction

Virtual Private Networks (VPNs) are a critical part of many enterprise networks. They are deployed on a public network infrastructure but utilize the same security, management, and quality of service policies that are applied in a private network. VPN services are offered in two different service paradigms: overlay and peer-to-peer, which can be difficult and expensive to manage as networks scale.

The HP Auto Discovery VPN (ADVPN) solution provides a mechanism to automatically setup overlay IPsec VPN tunnels using address management, to provide inexpensive IP circuit connectivity over the public Internet or WAN for hub and spoke and full mesh topologies. HP ADVPN is especially useful when branch offices have dynamic public IP addresses and secure connectivity to the corporate network is required. This offers enterprises considerably reduced WAN connectivity costs when compared to peer-to-peer MPLS VPN and considerably simplified configuration and management when compared to overlay IPsec VPN.

The HP ADVPN solution is based on the HP Comware v7 operating system and is the second generation of the HP Dynamic VPN (DVPN) solution, which is based on the HP Comware 5 operating system. HP ADVPN is compatible with HP DVPN solutions, with a hybrid system having the properties of HP DVPN.

This guide provides technical pre-sales design guidelines for the HP ADVPN solution. The intended audience is HP Solution Architects, HP Technical Consultants, partner technical presales staff, and customers.

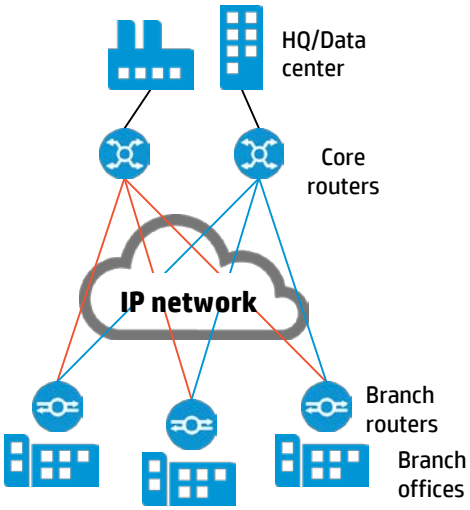
Value proposition

HP ADVPN is an enhancement to the original HP Dynamic VPN (DVPN) solution:

- ADVPN is supported in HP Comware v7
- ADVPN is compatible with HP DVPN
- Supports large scale networks
- Multidomain
- Single or many hub-groups within a domain
- Load balancing at hubs
- Supports NAT traversal
- IPv6 support in ADVPN network

A VPN is a secure way of connecting to a private LAN at a remote location to access information. VPN services are offered in two different service paradigms: overlay and peer-to-peer. In the overlay model the VPN network is built on top of the public network. Routers in the overlay (figure 1) can be thought of as being directly connected by logical links with the public network/Internet being transparent to the overlay devices. What this means is enterprises running overlays can run their networks irrespective of the kind of WAN connectivity technology.

Figure 1. VPN connectivity for branch offices



The best example of an overlay VPN is an IPsec VPN. However, as is well known, there are serious scalability concerns as the number of tunnels proliferate in the overlay model. Besides that, the routing configuration, IP protocols, and assortment of encryption options need to be enabled for the overlay model, often keeping the most tech-savvy administrators needlessly spinning their wheels for days.

In the peer-to-peer VPN model, the service provider participates in customer routing. An example of such a VPN is MPLS VPN. What enterprises like most about MPLS is reliability, stable performance, and fast recovery. Of course enterprise-class reliability comes at a price: MPLS T1/E1 connection can cost up to 100 times the US $4 to US $15 per megabit cost of broadband Internet service. This can translate to an extra few hundred dollars per branch, resulting in enormous expenses for the enterprise.

With these tradeoffs, enterprises have been looking at alternative solutions to address the cost and scalability challenges associated with overlay VPNs. To address these challenges, HP has developed a solution called HP ADVPN, which is focused on the HP MSR Series and HP HSR6600 Router Series. The HP ADVPN solution supports both hub and spoke as well as full mesh topologies for enterprises connecting various branch offices and remote offices to the HQ, campus, and data center locations.

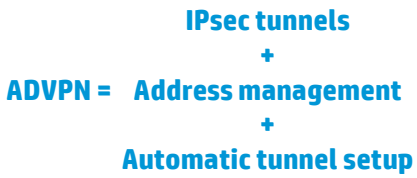
Challenges for enterprises connecting branch offices include:

- Number of branch offices are increasing
- Reduced IT staff at branch offices
- WAN overlays get complex as they scale
- Dedicated WAN connectivity is expensive
- Security on private networks is often required

The HP ADVPN solution provides a mechanism to automatically setup overlay IPsec VPN tunnels using address management to provide inexpensive IP circuit connectivity over the public Internet for hub and spoke and full mesh topologies. This offers enterprises a considerably reduced WAN connectivity costs compared to peer-to-peer MPLS VPN and a considerably simplified configuration and management when compared to overlay IPsec VPN.

HP ADVPN is an architecture and not a protocol. For spoke-to-spoke communications in a full mesh topology, the traffic travels directly between the spokes, bypassing the hubs, thus reducing the load on the hubs which otherwise can very quickly become bottlenecks. In short the HP ADVPN solution provides connectivity with little management overhead.

Figure 2. HP ADVPN basics



The HP ADVPN solution provides:

- DVPN tunnel setup
- Reduced configuration complexity
- Multiple transport options
- Security across tunnels

The HP ADVPN solution provides advantages including:

- Considerably easier to configure and deploy than conventional VPN solutions
- Managed deployment through IMC BIMS
- Supports UDP encapsulation for NAT traversal
- Native routing protocol support in the tunnel
- Can be used over any IP network (MPLS, Internet, 3G)

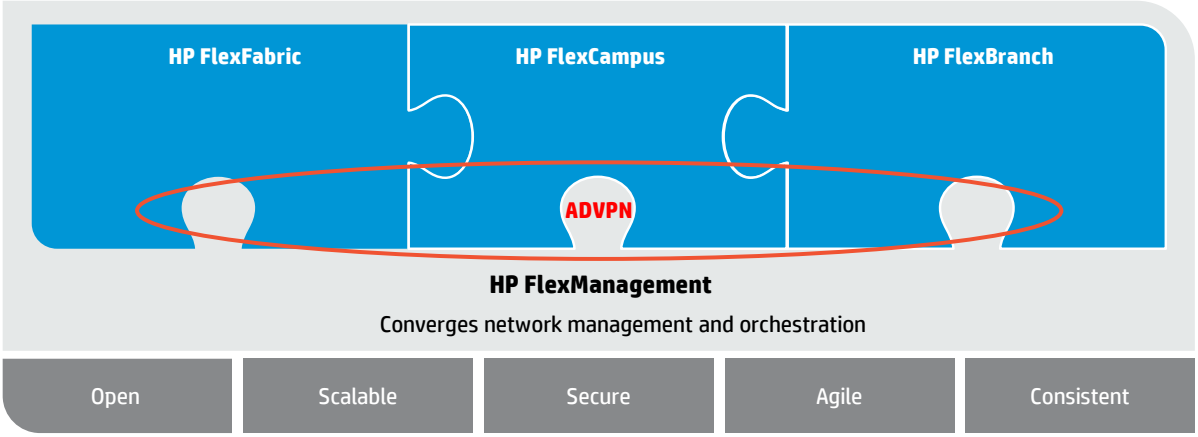
The dynamic aspect of the HP ADVPN solution comes from the fact that the configuration on the hub is automatically updated and the connections to the spoke dynamically created whenever a new spoke is added or deleted. This is something we call “Instant-on hub”. The hub or spoke can be assigned a different address every time a router comes “up” if using DHCP or PPPoE. Using a static configuration instead of ADVPN is therefore not only highly cumbersome but also not possible or desired. ADVPN does away for the need for static configuration per spoke.

To support address management and configuration challenges in an automated way, HP has defined a simple protocol called the VPN Address Management (VAM) protocol. Dynamic key exchange for IPsec is achieved using Internet Key Exchange (IKE), which helps prevent issues with long lived manual keys as well as key rollovers, which are essential for enterprise security.

Another key benefit of ADVPN is that routing protocols RIP, OSPF, and BGP can run natively over the ADVPN tunnels. This means the operator does not need to perform complex configurations and tweaks to make routing work on the ADVPN tunnels. In short, ADVPN solves the scaling and configuration management issues with overlay VPNs while still reducing the VPN costs. HP ADVPN is an HP architecture for creating "dynamic" overlay VPN tunnels while also simplifying the configuration management.

The HP ADVPN solution fits within the HP FlexNetwork architecture as part of a WAN architecture that allows remote sites to connect into the same head end routers and provides greater scalability with multiple head-end routers (known as hubs in the HP ADVPN solution). The FlexNetwork architecture is a blueprint that enables enterprises to align their networks with their business needs by segmenting their networks. This architecture is designed to allow IT to manage these different network segments through a single pane-of-glass management application. And because the FlexNetwork architecture is based on open standards, customers have the freedom to choose proven solutions for their businesses. Enterprises can segment their networks into the four interrelated modular building blocks of the HP FlexNetwork architecture, illustrated in the figure below: HP FlexManagement, HP FlexFabric, HP FlexCampus, and HP FlexBranch.

Figure 3. HP FlexNetwork architecture with ADVPN



Design guidelines

Where is HP ADVPN used

HP ADVPN technology fits in well for any hub and spoke or even full mesh network topologies, for example:

- Where multiple ATM machines connect to the data center, ADVPN is an ideal solution.
- Where spoke-to-spoke communication is required ADVPN can be configured into smaller domains.
- With the HP ADVPN solution's scalability, it can meet the needs of even the largest banks.
- HP ADVPN can also be used in enterprises where multiple branches connect to the campus or data center.
- Customers that want to move away from dedicated private line, such as MPLS, for some of their branch offices or remote locations.
- Due to the inherent cost of leased lines there is also a growing requirement of moving sites away from MPLS-based leased line connections to ADVPN-based open Internet connections.
- HP ADVPN connectivity can be used as a backup to MPLS-based VPN connectivity.
- Insurance field offices, mobile exploration trailers in the energy sector could be another application, transportation, and shipping (logistics).
- Customers willing to using a business-class broadband service to lower monthly costs for remote offices.
- Where client requirements demand network level encryption over private networks. This may include examples where the application or host system cannot support encryption natively.

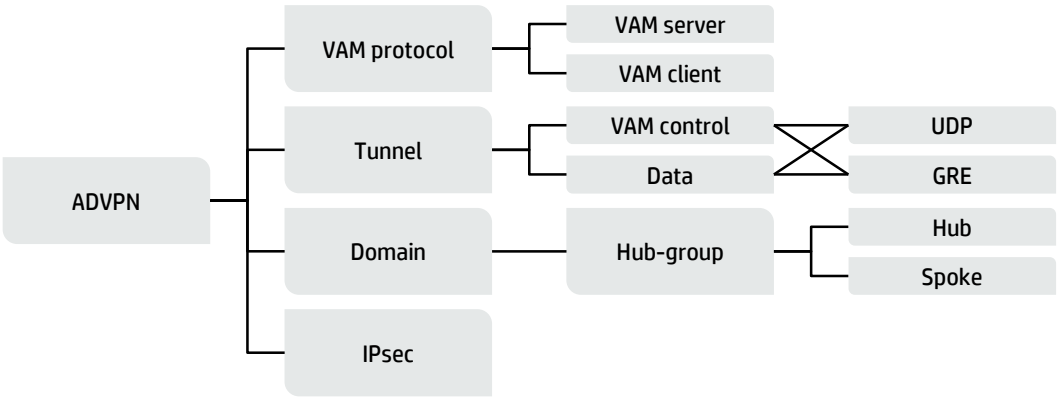
HP ADVPN solution overview

HP ADVPN solution enables enterprise branches that use dynamic public addresses to establish a VPN network. HP ADVPN uses the VAM protocol to collect, maintain, and distribute dynamic public addresses. IPsec can be used to protect ADVPN tunnels.

Concepts used in the HP ADVPN are illustrated in the figure below and include:

- VAM protocol
  - VAM server is used to store VAM client information
  - VAM clients include hubs and spokes
- Tunnels for VAM protocol and data
- An ADVPN domain is a set of VAM clients that are part of the same network
  - A grouping of VAM clients within a domain is called a hub-group
  - Hubs act as the exchange center for routing information and are the forwarding center in the hub and spoke model
  - Spokes act as the gateway of a branch network
- IPsec can be used to secure data over tunnels

Figure 4. Concepts used in the HP ADVPN solution



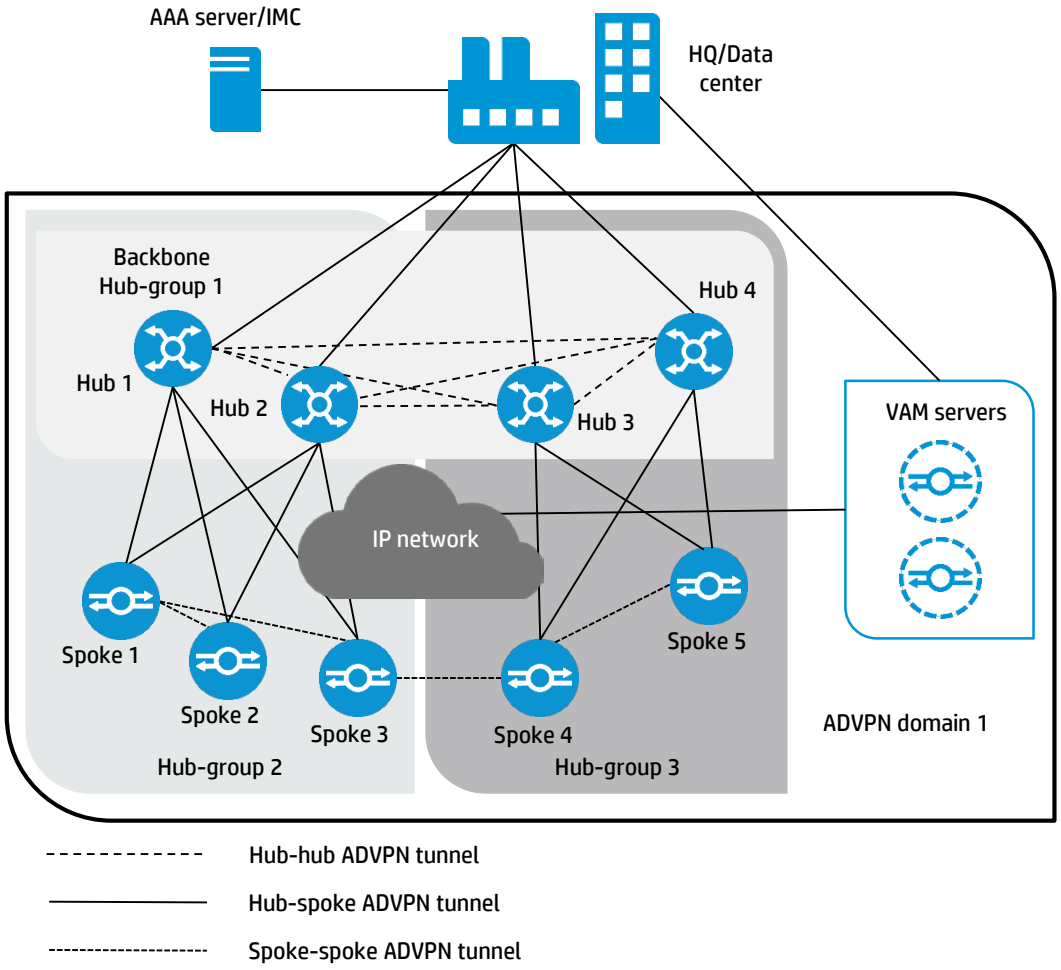
HP ADVPN solution components

The HP ADVPN architecture components include:

- VAM server
  - Up to 2 per ADVPN domain
- VAM client
  - Hub
- Resides at HQ or data center
  - Spoke
- Resides at campus or branch
- Hub-group
  - A group of VAM clients
- Optional AAA server
  - Provides centralized authentication
- Optional HP IMC
  - Resides at HQ or data center
  - BIMS (TR-069)

The components of the HP ADVPN solution are illustrated in figure 5.

Figure 5. Components of the HP ADVPN solution



A VAM server is the central entity managing all the addresses on behalf of the ADVPN solution. It receives address mapping on behalf of the ADVPN nodes and maintains these mappings. To re-emphasize an interesting point here—though the server runs on a router, the VAM server can be a physically separate device from the one that forwards ADVPN data traffic. Two VAM servers can be present in an ADVPN domain to provide redundancy. VAM server(s) collect, maintain, and distribute public and private addresses for each spoke and hub router. The VAM server can also be used to authenticate spoke/hub routers before providing information necessary to join ADVPN domains.

The next component is the VAM client. The VAM clients are entities, which register their addresses with the VAM servers and also perform peer address resolution using the server. Hub and spoke routers are VAM clients. Every VAM client registers its public and ADVPN private IP address to the VAM server. When a VAM client needs to forward traffic to another private network, it requests the peer public IP address from the VAM server by the peer private address, which should be the next hop to the destination. Once it receives the information, a connection is initiated.

The hub is the central device, which is typically located in the data center, campus, or main HQ. A spoke can connect with one or more hubs in each ADVPN hub-group for redundancy and load balancing purposes. An important consideration here is that all the hubs are active at the same time. This feature was pioneered in the HP routers and can help balance traffic between multiple active hubs. The hub acts as the exchange center for routing information and is the forwarding center in the hub and spoke model. Its public IP address can be static or dynamic.

A hub-group is a structure that allows the HP ADVPN solution to accommodate more VAM clients, which allows the HP ADVPN solution to scale. This structure solves the problem that one hub cannot manage all clients, for example, because of a routing protocol's limit to neighbors. An HP ADVPN domain can contain multiple hub-groups. Each hub-group has one or multiple hubs and spokes.

The spoke in itself is typically the gateway for the branch office or other remote location and forwards data traffic to the hub. The hub and spoke have IPsec tunnels among themselves. The public address of a spoke can be static or dynamic.

An optional component is the authentication server, which can be used to authenticate VAM clients as well as to do accounting on behalf of the VAM server. The AAA server needs to have reachability to the VAM server.

With such clear separation of components and modular architecture, the HP ADVPN solution provides an elegant design which is easy to comprehend and deploy. Another optional component is HP IMC and its BIMS module, which can help improve deployments with zero-touch/low-touch capabilities while securely managing the edge routers over any IP network.

An important concept to remember here is for data transfer between the hub and spoke, standards-based IPsec is used. The hub and spoke routers are VAM clients in an ADVPN solution. However, a hub router can also be configured as a VAM server and VAM client within an HP ADVPN domain. We do not recommend configuring the hub as the VAM server in an ADVPN domain unless it is a very small scale HP ADVPN deployment and cost is a primary consideration/barrier.

An HP ADVPN tunnel is point-to-multipoint (P2MP) tunnel, not point-to-point (P2P) tunnel, so the HP ADVPN tunnel has many peers and needs to know all the peer public addresses for encapsulation. The VAM protocol is used for providing peer public IP address information.

HP ADVPN has two encapsulation formats:

- UDP encapsulation:
  - The original IP packet is encapsulated as the payload of a HP DVPN UDP packet
  - A packet with UDP encapsulation includes an HP DVPN header, and the HP DVPN header has the fields about DVPN ID and peer private address, by which the receiver can find the right tunnel.
  - If IPsec is not used, the packets with UDP encapsulation can pass the NAT device, but packets with GRE encapsulation can't do that.
- GRE encapsulation:
  - Original packet is encapsulated into a standard GRE packet
  - A packet with GRE encapsulation doesn't include the ADVPN header. If a packet with GRE encapsulation is received, the receiver finds the right tunnel by judging whether the packet destination address accords to the tunnel source address.
  - When used with IPsec, the UDP or GRE HP DVPN packet is encapsulated in an IPsec packet.

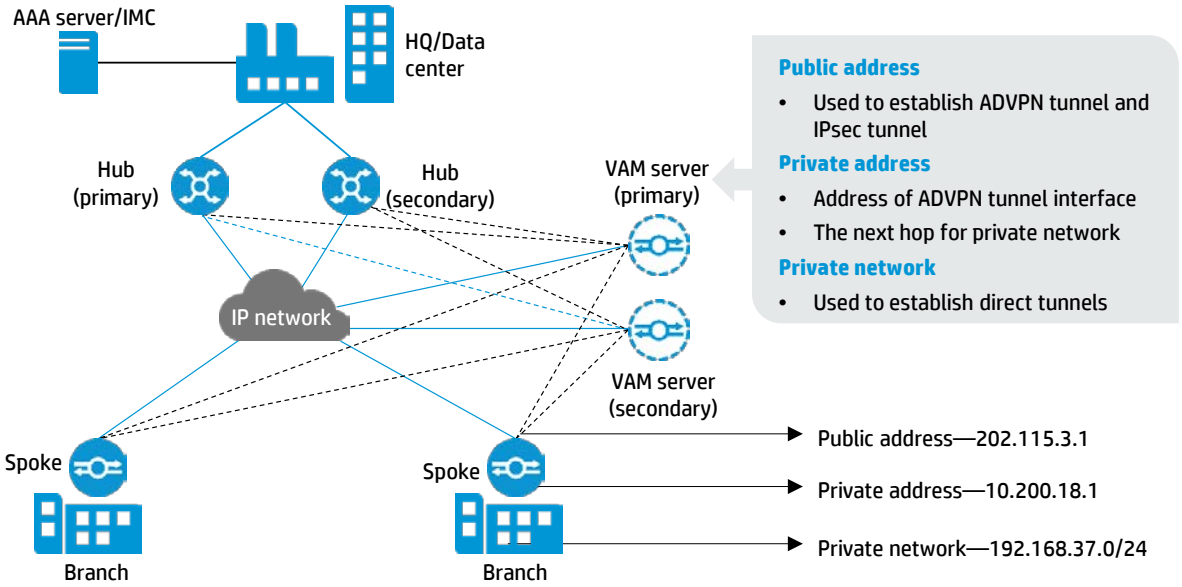
Operation of HP ADVPN solution

The HP ADVPN solution provides connectivity for an enterprise private network where the enterprise has many branches that need to communicate with the central network and communicate each other over a public network. Like a GRE tunnel, HP ADVPN provides a virtual tunnel that can transport private traffic and use the underlying public IP network as the link layer. The original private packet is encapsulated by an outer IP header where the source address is the local public address and the destination address is the peer public address.

VAM is the main protocol used by the HP ADVPN solution. The VAM protocol uses a client/server model:

- Supports 2 tunnel encapsulations: UDP and GRE
- Each client registers mapping of its private and public IP addresses with server using ADVPN control protocol (VAM)

Figure 6. HP VPN Address Management (VAM) protocol



HP ADVPN uses the client/server model and supports two tunnel encapsulation modes: UDP and GRE. An HP ADVPN domain consists of at least one VAM server and multiple VAM clients (at least one hub and one spoke).

Each client registers the mapping of its private address and public address with the VAM server. After a client registers its address mapping with the server, other clients can get the public address of this client from the VAM server. This mechanism helps with ADVPN tunnel establishment between clients. Each client uses the VAM protocol to communicate with the server and uses the ADVPN tunneling protocol to establish, maintain, and remove tunnels to other clients. Whenever there is a change in the topology, the VAM server will be notified automatically.

HP ADVPN tunnel establishment

The HP ADVPN tunnel establishment process consists of three steps:

1. Connection initialization phase

   A VAM client initiates a connection to the VAM server, and the two parties negotiate whether to secure the VAM protocol packets. If yes, the two parties negotiate the packet encryption and integrity validation algorithms and generate the keys. At the end of this phase, a control tunnel is established between the VAM client and the VAM server.

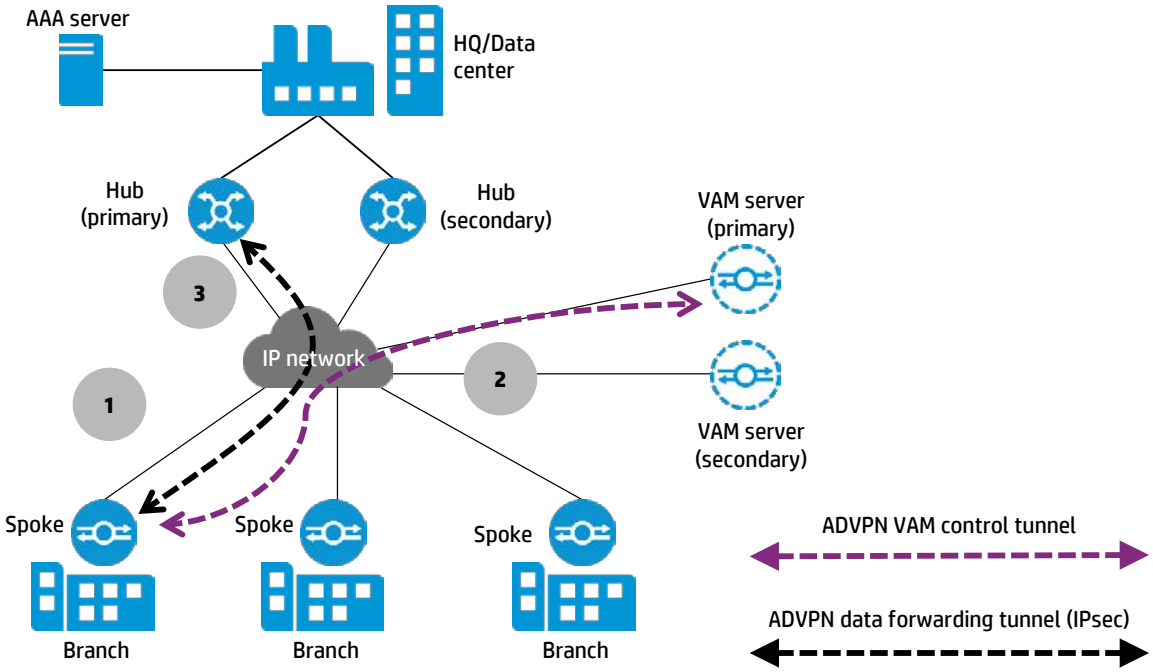
2. Registration phase

   The VAM client sends a registration request to the server through the established control tunnel, and the two parties authenticate each other. If the authentication succeeds, the VAM server saves the registration information of the client.

3. Tunnel establishment phase

   Based on VAM client registration information saved on the VAM server, VAM clients establish data forwarding tunnels between them. Tunnels established between hubs and spokes are permanent, while tunnels established between spokes are dynamic.

Figure 7. HP ADVPN solution tunnel establishment overview



The public address of the VAM server is the only element in an HP ADVPN that must be static. The public address is the address of the interface that connects to the public network. It can be manually configured or dynamically assigned. The private address is the address of the ADVPN tunnel interface. The private address of a client needs to be statically configured, but its public address can be manually configured or dynamically assigned. All the private addresses of the nodes within an HP ADVPN domain must belong to the same network segment. If multiple HP DVPN domains are used, each domain will have unique NBMA overlay addressing. Primary and secondary hubs are both active.

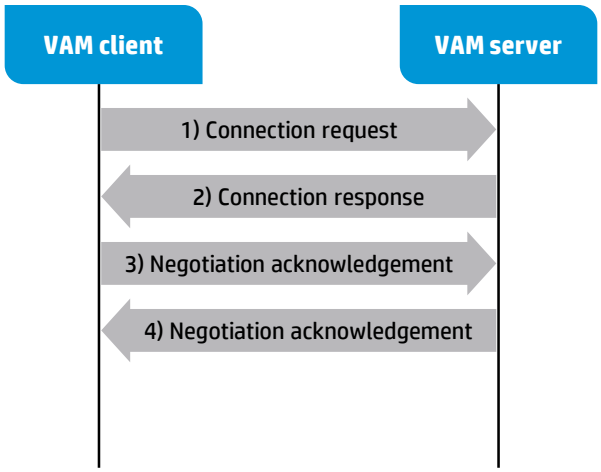
Prerequisites on the VAM client for ADVPN tunnel include:

- IP address and port of VAM server
- Pre-shared-key which is consistent to that of VAM server for key negotiation to encrypt the exchanging packet
- Username/password for authentication
- The tunnel private address and the source interface which is linked to public network
- The public route to access VAM server

The message flow for HP ADVPN connection initialization is illustrated in the next figure, and consists of these steps:

1. The VAM client lookups the FIB and sends the server a connection request, which carries the supported encryption and integrity validation algorithms.
2. The server and the client begin to negotiate the algorithms to be used, with the server dominating the negotiation.
3. The client and server respectively checks whether the algorithm negotiation and key negotiation are successful through the negotiation acknowledge packets.
4. The VAM server sends an acknowledgement packet to the VAM client.

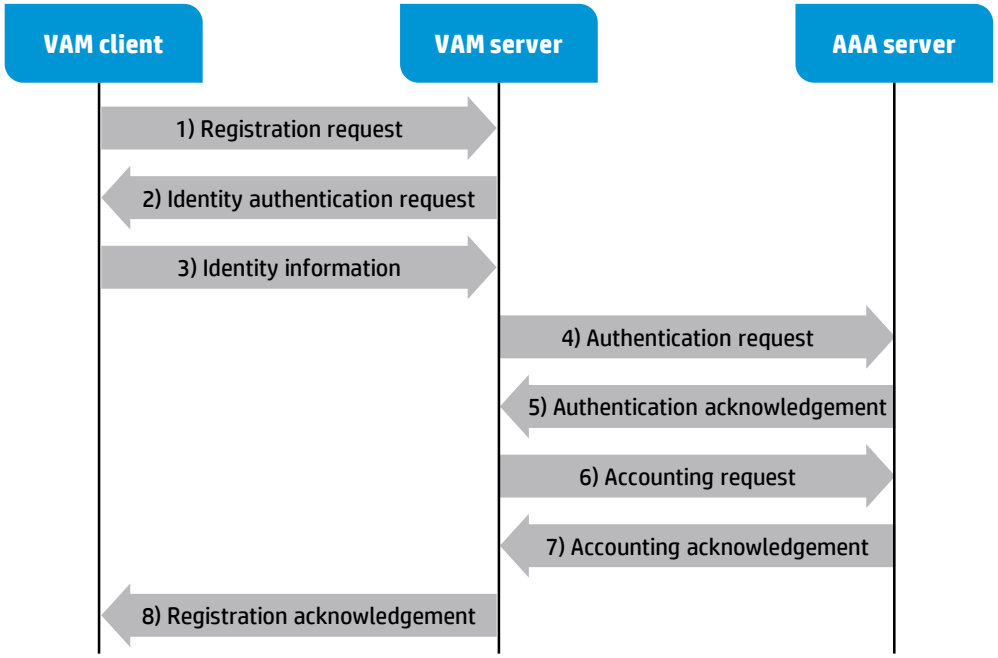
Figure 8. HP ADVPN solution connection initialization message flow



The message flow for HP ADVPN registration phase is illustrated in the next figure, and consists of these steps:

1. A VAM client sends the server a registration request, which carries information about the client.
2. The VAM server receives the registration request.
   A. If identity authentication is not required, the server directly registers the client and sends the client a registration acknowledgement.
   B. Otherwise, the server sends the client an identity authentication request, indicating the required authentication algorithm.
3. The VAM client submits its identity information to the VAM server.
4. After receiving the identity information of the client, the VAM server sends an authentication request to the AAA server, AAA server sends authentication acknowledgement to the VAM server.
5. The VAM server sends an accounting request to the AAA server. The AAA server responds an accounting acknowledgement.
6. When the VAM server receives the accounting acknowledgement, it sends the client a registration acknowledgement, telling the client information about the hubs in the VPN.

Figure 9. HP ADVPN solution registration phase message flow



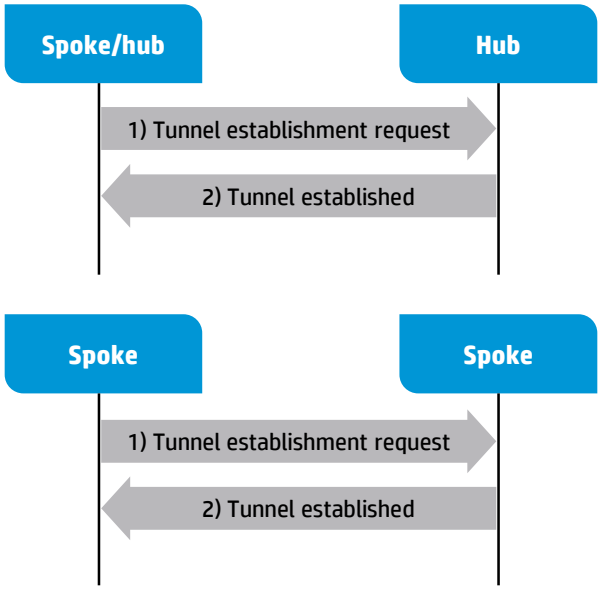
Notes:

1. The packets exchanged between the VAM server and the VAM client are encrypted.
2. For the RADIUS packets between the VAM server and AAA server, only the password is encrypted.

The message flow for the tunnel establishment phase is illustrated in the next figure, and consists of these steps:

1. The initiator originates a tunnel establishment request.
   A. To establish a hub-spoke tunnel:
      i. Upon receiving the registered information about the hubs, the spoke sends a tunnel establishment request to the hub.
   B. To establish a hub-hub tunnel:
      i. Upon receiving the registered information about the other hub in the same VPN domain, the hub sends a tunnel establishment request to the peer hub.
   C. To establish a spoke-spoke tunnel:
      i. In a full mesh network, when a spoke receives a data packet but finds no tunnel for forwarding the packet, it sends an address resolution request to the server, after receiving the resolved address, sends a tunnel establishment request to the peer spoke.
2. The tunnel establishment request receiver saves the tunnel establishment information and sends a response to the sender. If the request sender receives the response, a tunnel is established.

Figure 10. HP ADVPN solution data forwarding tunnel establishment message flow



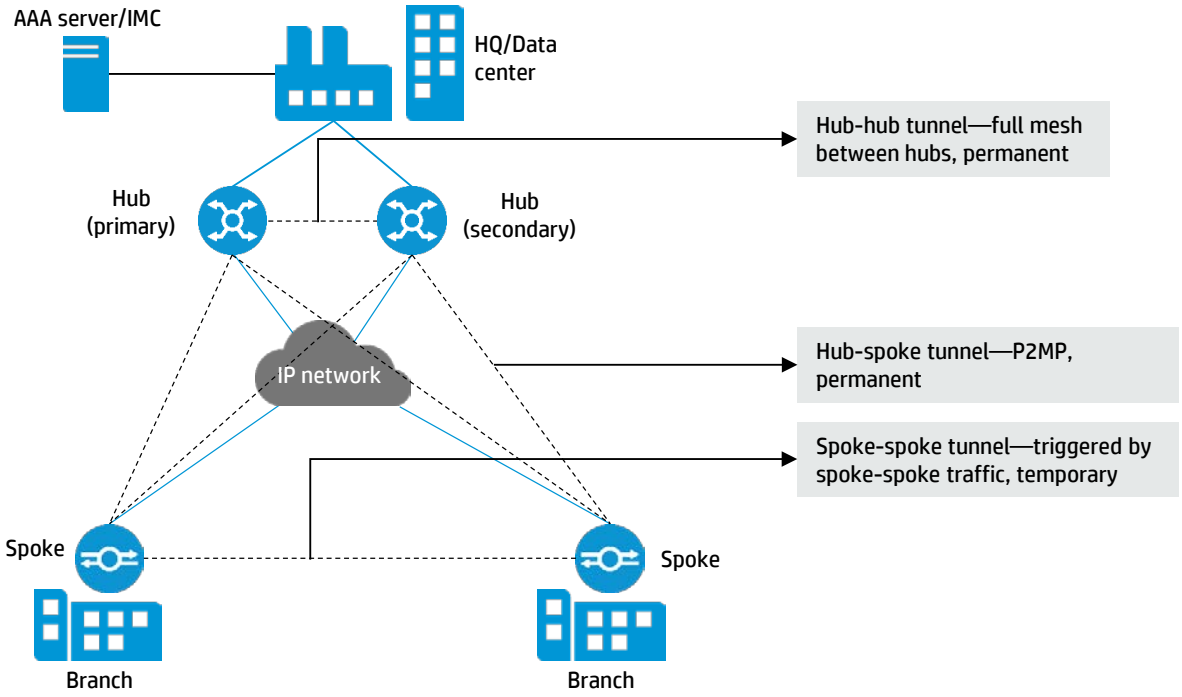
Notes:

1. If IPsec is configured on the ADVPN tunnel interface, it is the ADVPN tunnel establishment request packet that triggers negotiation for the IPsec SA. An IPsec tunnel is then set up and all private packets are sent over the IPsec tunnel.
2. IPsec is not necessary for ADVPN. But for security, it is typically configured.

There are different types of data forwarding tunnels in an HP ADVPN solution that are illustrated in the next figure, including:

- Hub-hub
- Hub-spoke
- Spoke-spoke

Figure 11. HP ADVPN solution data forwarding tunnels



HP ADVPN encapsulation methods

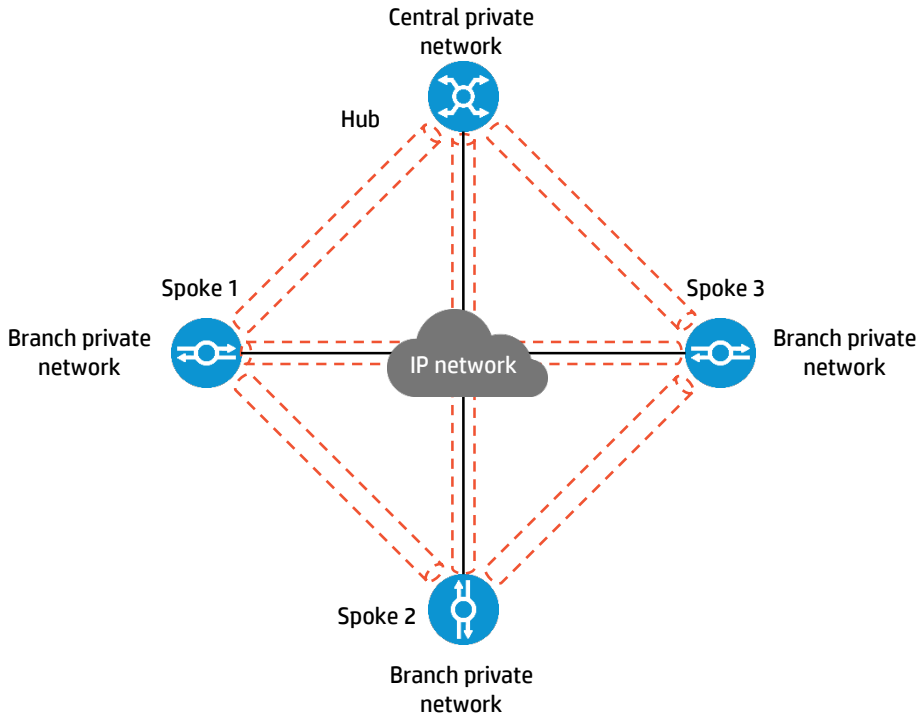
HP ADVPN provides connectivity for an enterprise private network where the enterprise has many branches, which need to communicate with the central network and communicate to each other over a public network. Like a GRE tunnel, HP ADVPN provides a virtual tunnel that can transport private traffic and use the underlying public IP network as the link layer. The original private packet is encapsulated by an outer IP header where the source address is the local public address and the destination address is the peer public address.

HP ADVPN has 2 encapsulation formats:

1. UDP encapsulation: The original IP packet is encapsulated as the payload of an ADVPN UDP packet
2. GRE encapsulation: original packet is encapsulated into a standard GRE packet
   A. When used with IPsec, the UDP or GRE ADVPN packet is encapsulated in an IPsec packet

An ADVPN tunnel is P2MP tunnel, not P2P tunnel, so the ADVPN tunnel has many peers and needs to know all the peer public addresses for encapsulation. The VAM protocol is used for providing peer public IP address information.

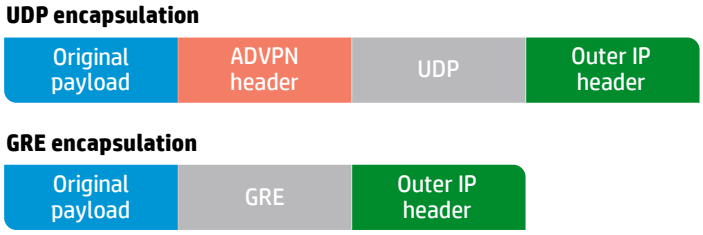
Figure 12. HP ADVPN solution connectivity



What is the difference between UDP and GRE?

1. Two HP ADVPN tunnels using GRE encapsulation have to use different source interfaces, but the two using UDP encapsulation can use the same source interface, because a packet with UDP encapsulation includes an ADVPN header. An ADVPN header has the fields about ADVPN ID and peer private address, by which, the receiver can find the right tunnel. A packet with GRE encapsulation doesn't include the HP ADVPN header. If a packet with GRE encapsulation is received, the receiver finds the right tunnel by judging whether the packet destination address accords to the tunnel source address.
2. If IPsec is not used, the packets with UDP encapsulation can pass the NAT device, but packets with GRE encapsulation cannot do that.

Figure 13. HP ADVPN solution encapsulation methods



Important points regarding HP ADVPN encapsulation methods include:

- When ADVPN packets need to traverse NAT gateway without IPsec protection, UDP encapsulation is required
- When traffic between branch network and central network is encapsulated by MPLS, GRE encapsulation is required
- If the original payload is just IP, either is OK

HP ADVPN route learning and packet forwarding process

Static or dynamic routing must be configured for private networks and HP ADVPN tunnel interfaces to achieve connectivity among private networks. A dynamic routing protocol discovers neighbors, updates routes, and establishes a routing table over HP ADVPN tunnels. From the perspective of private networks, HP ADVPN tunnels are common private links that connect different private networks. The routing protocol exchanges routes between hub and hub, and between hub and spoke. It does not directly exchange routes between spoke and spoke.

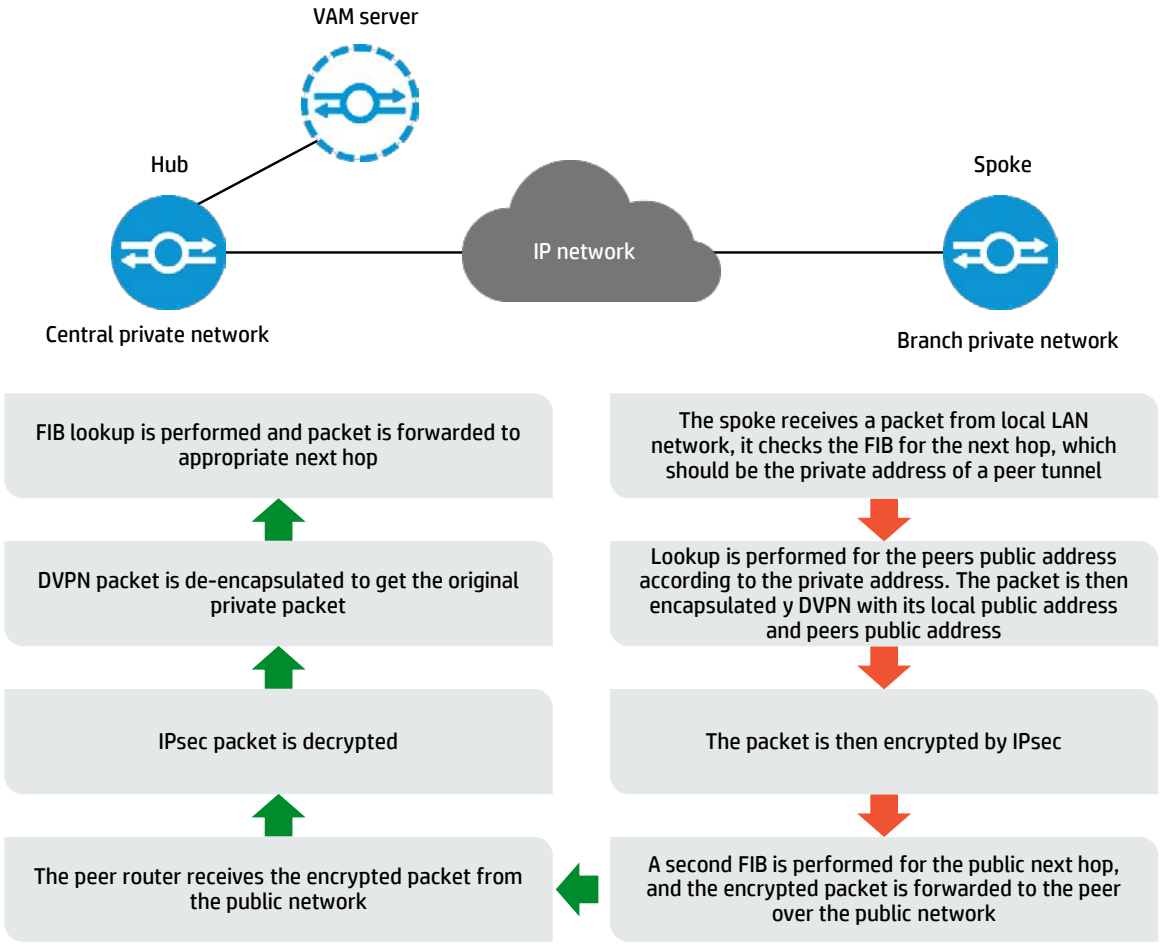
When a spoke receives a packet destined to a remote private network, it performs the following steps to forward the packet:

- Finds the private next hop from the routing table
- Uses the private next hop to obtain the corresponding public address from the VAM server
- Sends the packet to the public address over the ADVPN tunnel

Full-mesh and hub-spoke structures are determined by routing. If the next hop is a spoke, the structure is full-mesh. If the next hop is a hub, the structure is hub-spoke.

After an HP ADVPN tunnel is established between a hub and a spoke or between spokes, the private packets should be forwarded through the tunnel. The packet forwarding process is described below from spoke to hub.

Figure 14. Packet forwarding in an HP ADVPN solution



The next figure shows the format of HP ADVPN packets. ADVPN supports both GRE and UDP encapsulations. In the outer IP header, the source IP address is the public address of the local spoke, and the destination address is the public address corresponding to the private next hop. IPsec can be used to protect ADVPN tunnels.

Figure 15. Packet structure for HP ADVPN solution

An ADVPN tunnel using UDP encapsulation can traverse a NAT gateway:

- If only the tunnel initiator resides behind a NAT gateway, a spoke-spoke tunnel can be established through the NAT gateway.

- If the tunnel receiver is behind a NAT gateway, packets must be forwarded by a hub before the receiver originates a tunnel establishment request. If the NAT gateway uses Endpoint-Independent Mapping, a spoke-spoke tunnel can be established through the NAT gateway.
- If both ends reside behind a NAT gateway, no tunnel can be established and packets between them must be forwarded by a hub.

Routing protocols for HP ADVPN solution

The HP ADVPN solution supports OSPF, RIP, and BGP for IPv4:

- When OSPF is used, set the network type of an OSPF interface to broadcast in a full mesh network and to P2MP in a hub-spoke network.
- When RIP is used, you can use RIP-1 or RIP-2 broadcast in a full mesh network and use RIP-2 multicast and disable split horizon in a hub-spoke network.
- When BGP is used, configure a routing policy to make sure the next hop of a route destined for a remote private network is the IP address of the peer spoke in a full mesh network (EBGP does not support full-mesh), or is the IP address of the hub in a hub-spoke network.

The HP ADVPN solution supports OSPFv3, RIPng, and IPv6 BGP for IPv6:

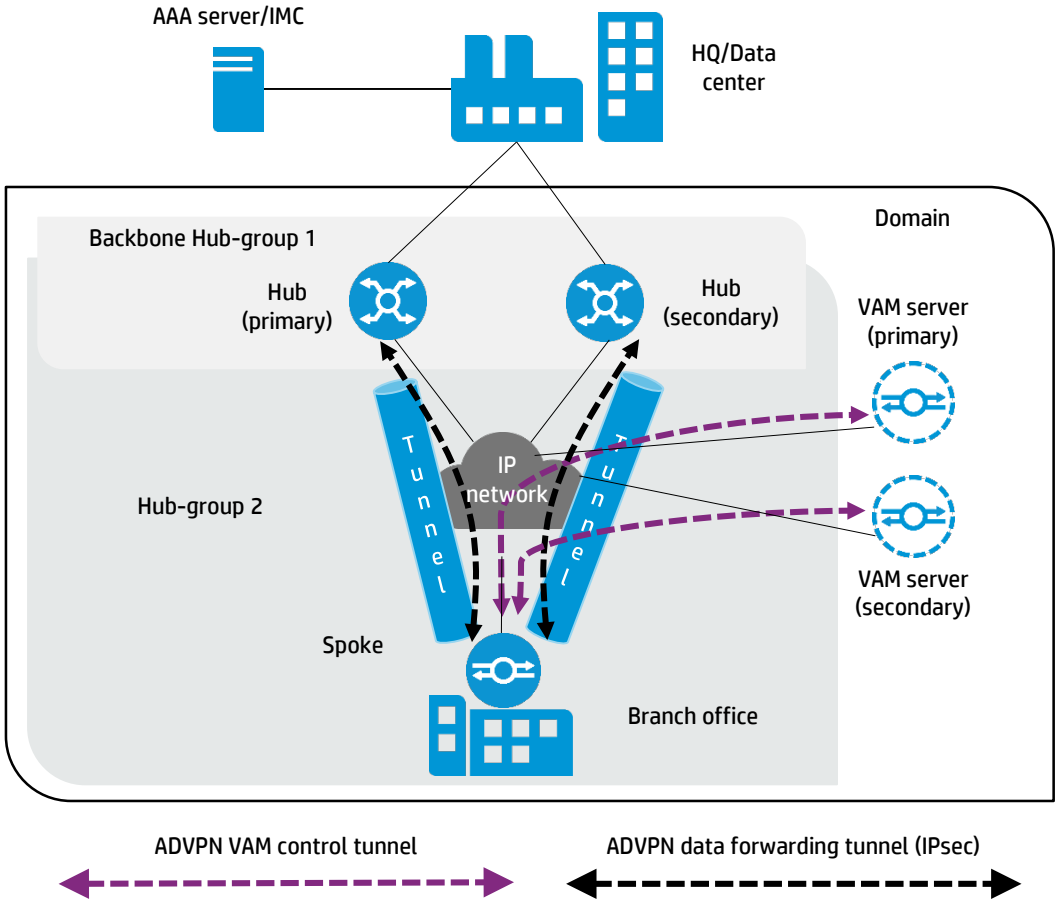
- When OSPFv3 is used, set the network type of an OSPFv3 interface to broadcast in a full mesh network and to P2MP in a hub-spoke network.
- When RIPng is used, only the full-mesh network is supported.
- When IPv6 BGP is used, configure a routing policy to make sure the next hop of a route destined for a remote private network is the IP address of the peer spoke in a full mesh network (EBGP does not support full-mesh), or is the IP address of the hub in a hub-spoke network.

HP ADVPN solution hub and spoke structure

In a hub-spoke HP ADVPN topology, each spoke establishes a permanent tunnel with the hub, but no tunnel can be established between two spokes, and data between spokes has to be forwarded through the hub. The hub is used as both the routing information exchange center and the data forwarding center.

An example of an HP ADVPN solution hub and spoke topology is illustrated in the next figure.

Figure 16. HP ADVPN solution hub and spoke topology



Consider this application scenario example:

- An international banking enterprise has branches in many countries. No single service provider supports establishing a private network for the enterprise and the branches must use the Internet to connect to the headquarters. Each branch only needs to communicate with the headquarters.
- Analysis:
  - Because each branch only needs to communicate with the headquarters, hub-spoke ADVPN is the proper scheme for connectivity and data security.

Advantages of the hub-spoke HP ADVPN scheme include:

- HP ADVPN supports strong encryption, ensuring the secure transmission of data over the Internet.
- Branches are centrally authenticated at the headquarters, implementing access control.
- Branches cannot communicate with each other directly, eliminating possible problems.

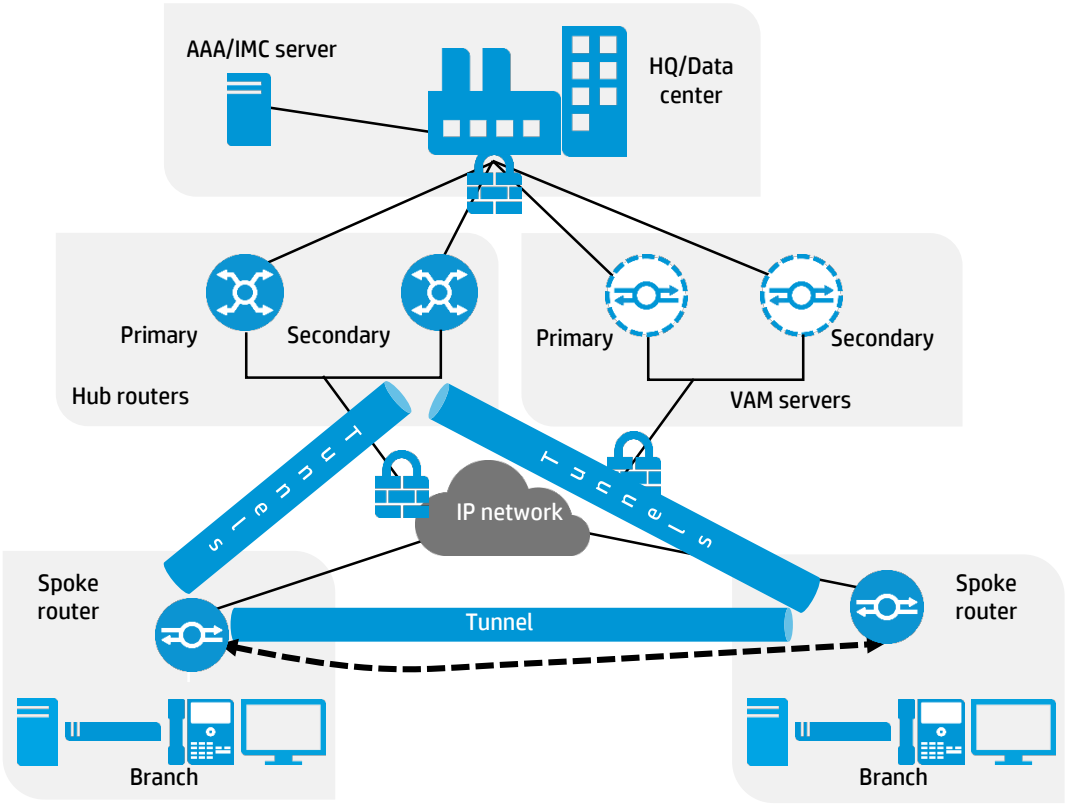
The HP ADVPN overlay is a non-broadcast multiaccess (NBMA) network and is configured as one subnet. Spokes do not have direct connectivity with other spokes, all spoke-to-spoke traffic must traverse the hub router (this is controlled by routing protocol selection and configuration).

HP ADVPN solution full mesh structure

In a full mesh HP ADVPN solution, spokes can communicate with each other directly by establishing tunnels between them, and the hub is mainly used as the routing information exchange center. After the spokes (the clients) register with the VAM server and get the hub information in the HP ADVPN domain, they establish permanent tunnels with the hub. Any two spokes can establish a tunnel directly between them, which is dynamic and will be aged out if no data exchange occurs on it during a specific period of time (the idle timeout for the spoke-spoke tunnel).

An example of an HP ADVPN solution full mesh topology is illustrated in the next figure.

Figure 17. HP ADVPN solution full mesh topology



Consider this application scenario example:

- A large international enterprise is using dedicated lines to connect its branches, representative offices, and researching institutes to the headquarters. With the development of the enterprise, more sites need to access the network and traffic between branches, representative offices, and researching institutes has increased dramatically. The dedicated line solution cannot satisfy the needs anymore because it is not only expensive but also impracticable.
- Analysis:
  - Because branches, representative offices, and researching institutes need to communicate with each other, full mesh ADVPN is the proper scheme for connectivity and data security.

Advantages of the full mesh ADVPN scheme include:

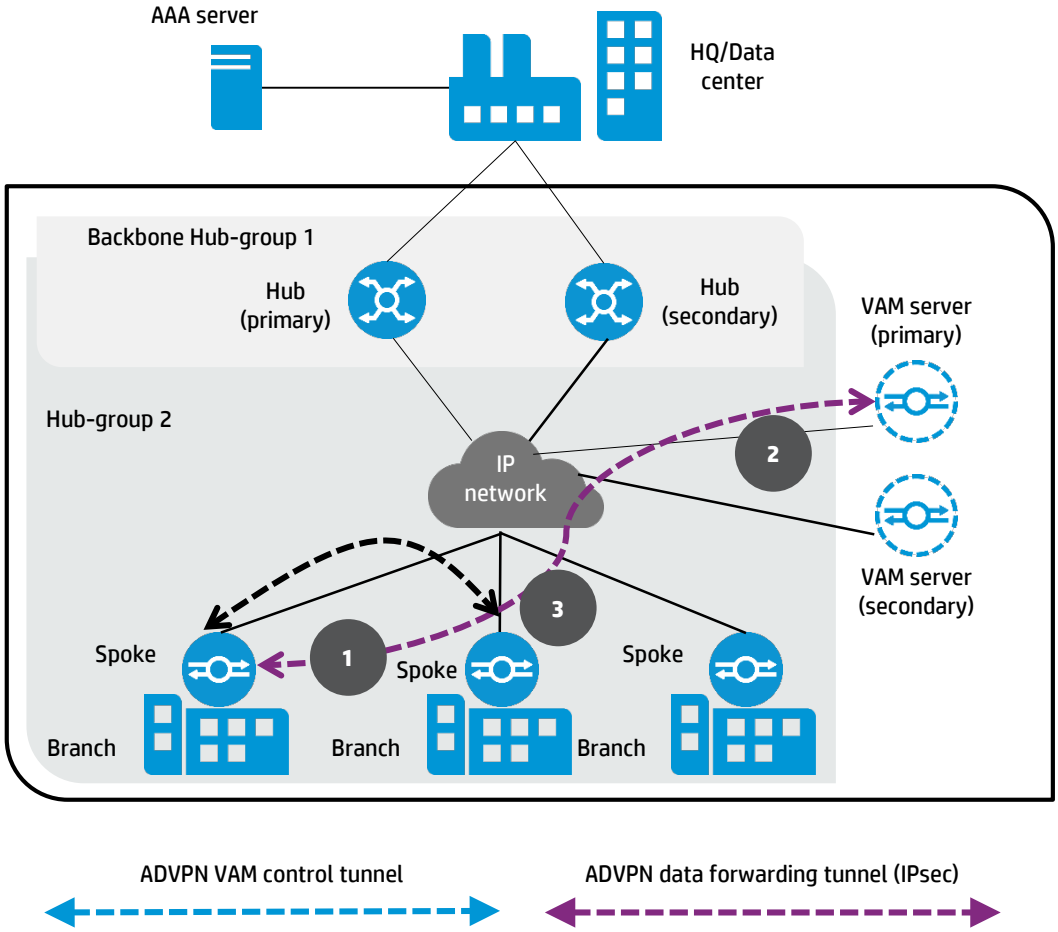
- HP ADVPN supports strong encryption, ensuring the secure transmission of data over the Internet.
- Branches are centrally authenticated at the headquarters, implementing access control.
- Branches can communicate with each other directly and efficiently, without burdening the hub.

The HP ADVPN overlay is an NBMA network just like the hub and spoke topology and is configured as one subnet. In a full mesh or partial mesh topology, direct connectivity between spokes is possible, which makes the data flow direct between spoke sites, eliminating the hub as a hop in the data path. The HP ADVPN solution can support full mesh as well as partial mesh.

As illustrated in the next figure, spoke-to-spoke tunnel setup includes these steps:

1. There are packets sent from branch network A to branch network B.
   A. Before the spoke-spoke session established, packets are transmitted through the hub.
2. Spoke 1 finds the private next hop from the routing table.
   A. Uses the private next hop to obtain the corresponding public address from the VAM server.
3. VAM server responds spoke 1 with spoke 2's public address
4. Spoke 1 establish the spoke-spoke session with spoke 2.
5. Packets are sent on the spoke-spoke session.

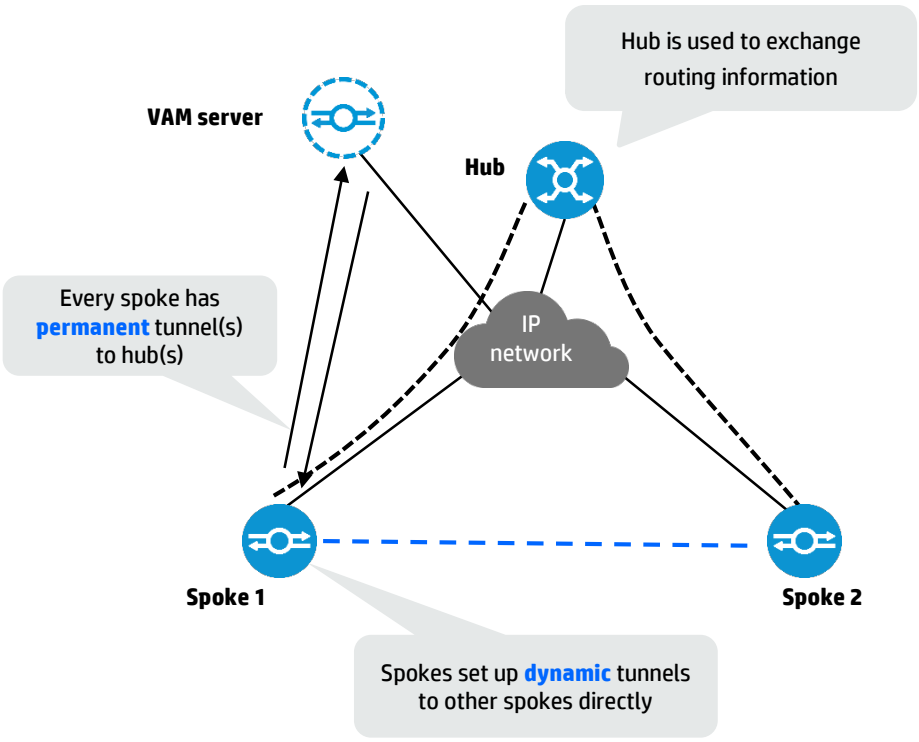
Figure 18. HP ADVPN solution spoke-to-spoke basic operation



Key points of spoke-to-spoke tunnel setup are illustrated in the next figure, including:

- Before the direct tunnel from spoke 1 to spoke 2 is created, traffic will be transferred by hubs.
- Spoke 1 and spoke 2 belong to the same group, they can learn route with each other by OSPF/BGP exchanging between hub-spoke. So, spoke 1 knows that it should query the next hop information of spoke 2 from VAM server.

Figure 19. HP ADVPN solution full mesh message flow



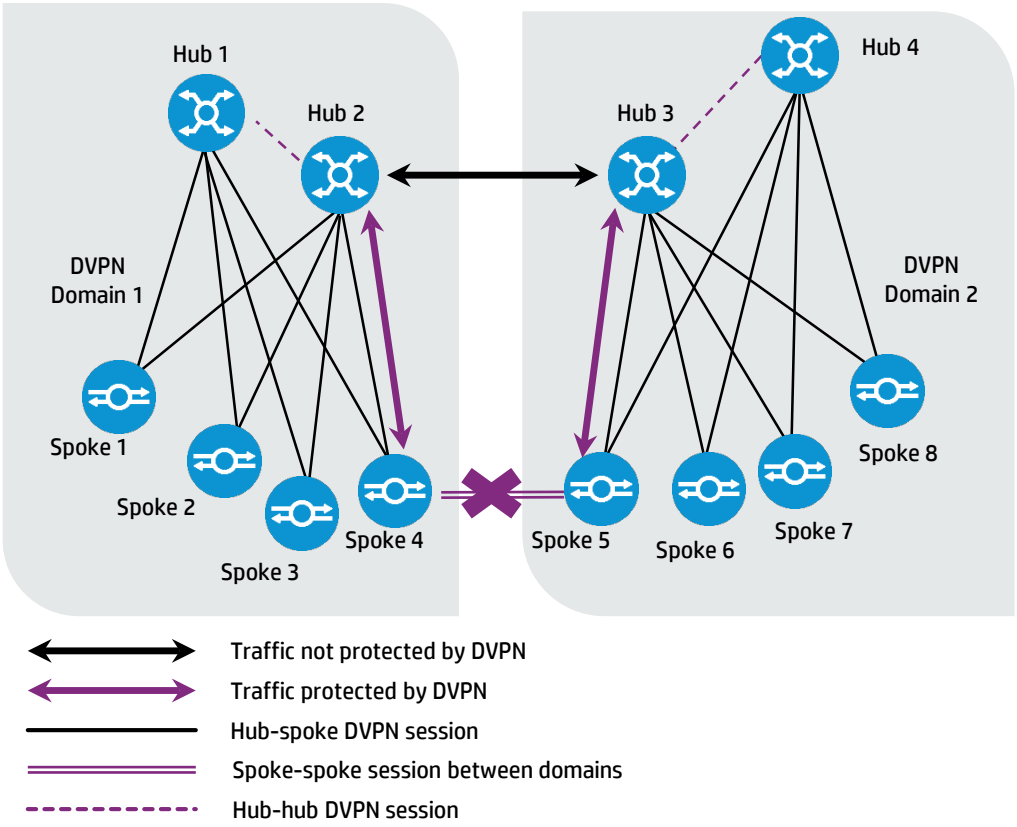
HP ADVPN hub-group structure

When the number of spokes exceed the routing protocol's limit to neighbors, more domains need to be created. However, attributes of interdomain connectivity include:

- Traffic between DVPN domains are not protected by DVPN session.
- Spokes belong to different domains cannot establish direct tunnels.

This is illustrated in the next figure.

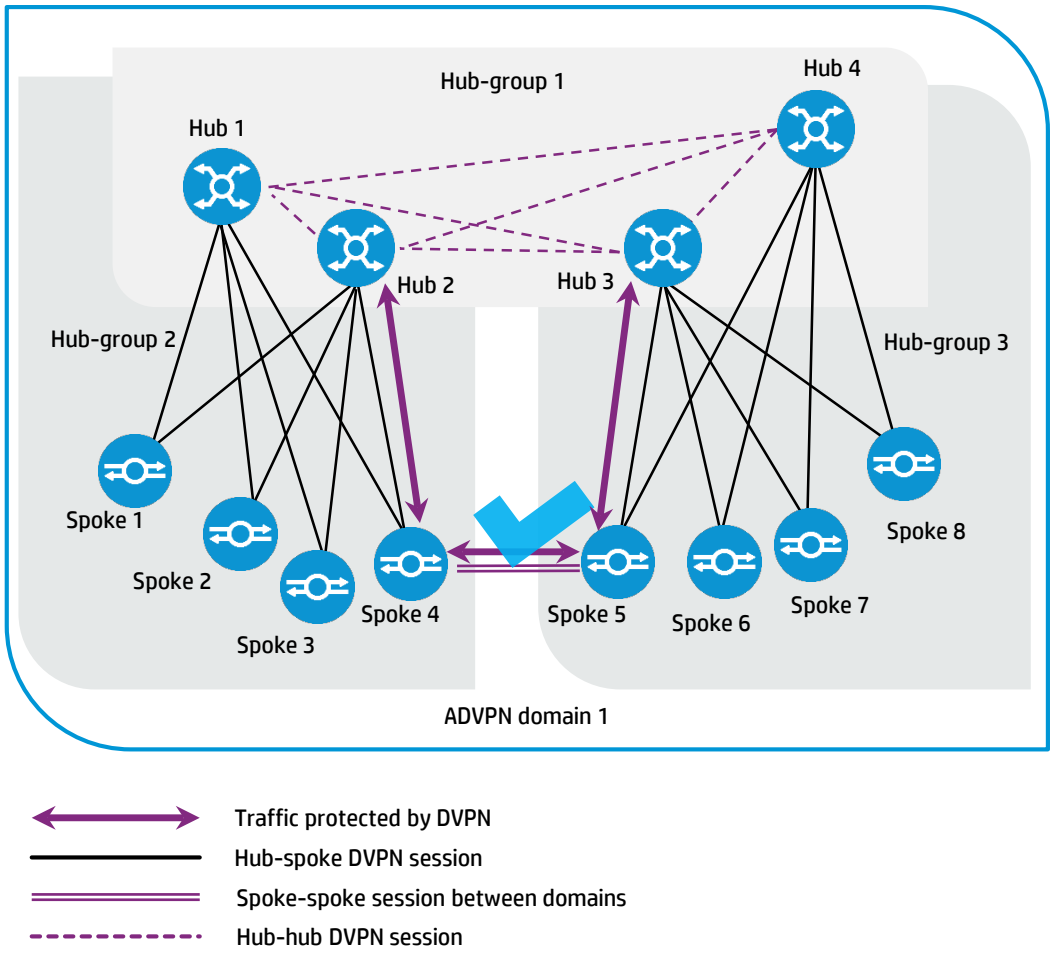
Figure 20. Deficiencies in inter-domain connectivity



When the number of spokes in one hub-group exceed the routing protocol's limit to neighbors, a new hub-group needs to be added. Advantages of hub-groups include:

- The inter-group communications between spokes belonging to different groups will be protected by the HP ADVPN tunnel.
- Spokes belonging to different hub-groups can establish a direct tunnel as a shortcut. And this improves the user experience on latency-sensitive applications such as VoIP.

Figure 21. Advantages of HP ADVPN hub-groups



Rules for HP ADVPN hub-groups include:

- An HP ADVPN domain may contain multiple hub-groups
  - Each hub-group has one or more hubs and spokes
- All hubs must belong to the backbone hub-group
  - This hub-group forms the full-mesh backbone area
- Spokes must belong to non-backbone hub-groups
  - Each non-backbone hub-group includes at least one hub and uses either the full-mesh or hub-spoke topology

A hub-group HP ADVPN structure can accommodate more HP ADVPN clients. This structure solves the problem that one hub cannot manage all clients. A hub-group contains multiple hub groups. Each hub group has one or multiple hubs and spokes.

Use the following guidelines to classify hub groups:

- All hubs must belong to the backbone hub-group. This hub-group forms the full-mesh backbone area. All hubs obtain information about other hubs from the VAM server and establish permanent ADVPN tunnels to each other.
- Spokes must belong to non-backbone hub groups. Each non-backbone hub-group includes at least one hub and uses either the full-mesh or hub-spoke structure. Spokes obtain hub information in the ADVPN domain from the VAM server, and establish permanent tunnels to the hub.

Tunnel establishment and data forwarding in a hub-group depend on the network structure. Inter-group communications between spokes need to pass through the hubs of the groups. To reduce the pressure on hubs during inter-group communications, you can allow spokes in different hub-groups to establish a dynamic tunnel. The dynamic tunnel is deleted if no data exists during the idle-timeout time.

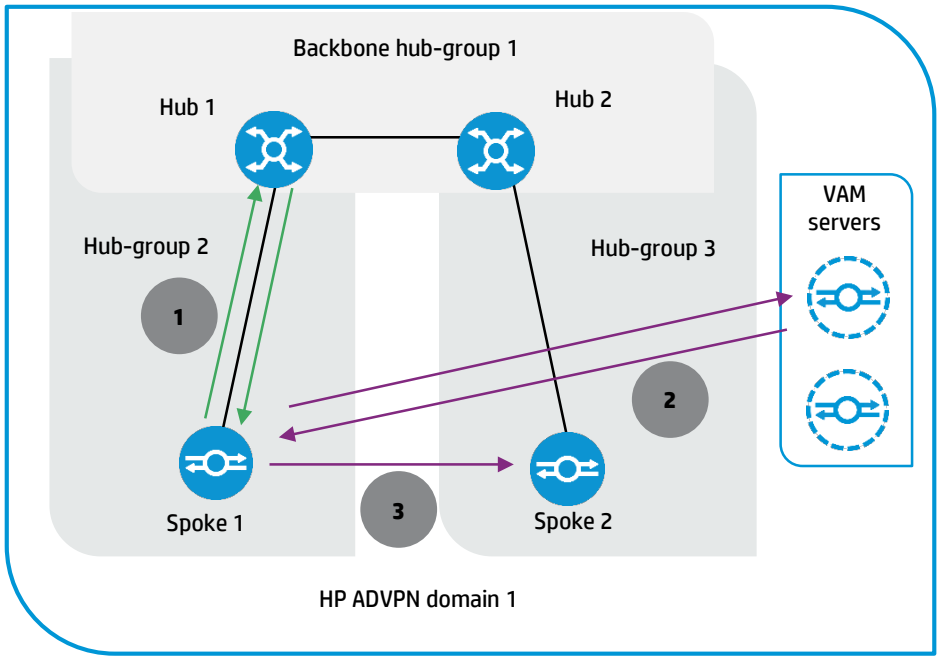
More than two hubs can work together for load balancing in one hub-group. Spokes are divided into different hub-groups according to private-address range or network.

Consider the message flow when spoke 1 and spoke 2 are in different groups and want to setup a spoke-spoke tunnel:

- Packet from spoke 1 → spoke 2
- Hub 1 checks FIB, determines that it came from ADVPN tunnel, so must be transferred to another spoke
  - Hub 1 sends session redirect response to spoke 1
- Spoke 1 queries VAM server
- Using spoke 2's registration, VAM server sends public IP address, private IP address, and private network to spoke 1
- Spoke 1 initiates ADVPN spoke-spoke tunnel with spoke 2
  - Spoke 1 also dynamically adds one VAM route item to its routing table

The message flow for spoke-spoke in different hub-groups is illustrated in the next figure.

Figure 22. HP ADVPN hub-group structure



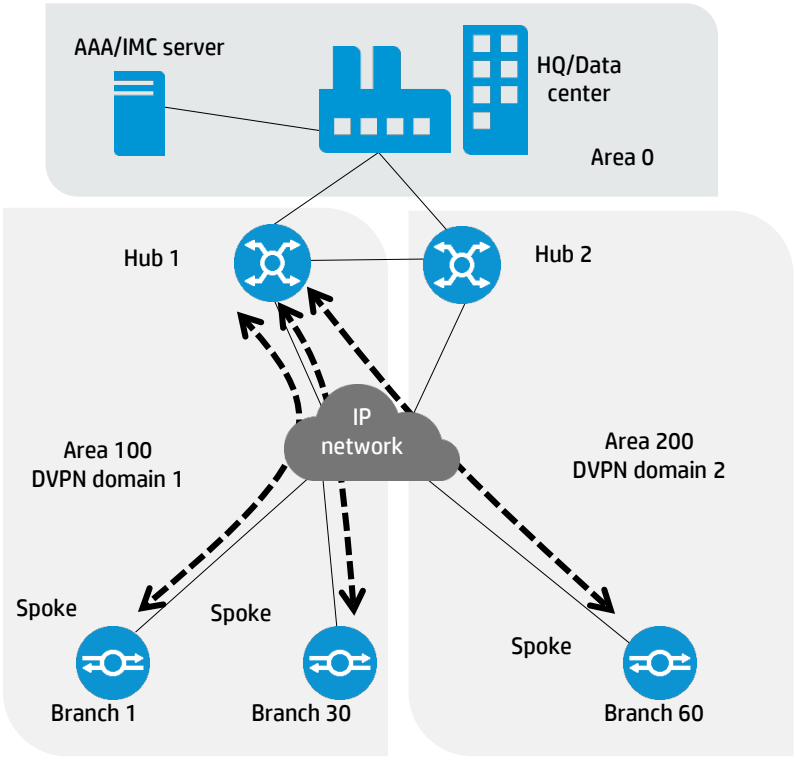
HP ADVPN solution OSPF design

OSPF is suitable for a hub-group with less than 500 branches:

- OSPF supports hub-spoke and full-mesh modes
- Each ADVPN hub-group must be in a single OSPF area

An example of an HP ADVPN solution OSPF design is illustrated in the figure 23.

Figure 23. HP ADVPN OSPF design example



OSPF can be configured for full-mesh (broadcast interface type is recommended and setting OSPF interface priority to ensure DR and BDR are the hub routers. Spoke routers should not participate in Designated Router (DR)/Border Designated Router (BDR) election process (set priority to 0). You can use P2MP interface type for hub and spoke. P2MP also supports mesh, but not dynamically.

The two hubs should be selected as DR/BDR and OSPF packets originated by spokes should only be sent to the Hub, not to other spokes. Originally, a spoke has only two permanent tunnels to the Hubs, so OSPF packets originated by a spoke are only sent to the hubs as the next hop. However, a spoke can calculate the next hop for a route whose destination is inside another branch. The next hop for that route would be the DVPN private address on the destination spoke.

To ensure that this is how the environment operates, set the OSPF DR priority to non-zero values (e.g., 255 for DR and 254 for BDR) on the Hub tunnel interfaces and set the OSPF DR priority on all spoke ADVPN tunnels to zero (0). Setting the hub OSPF tunnel interface DR priority to the highest setting also helps to make sure that when a new router is added to the environment that it will be less likely to cause a DR/BDR election in the ADVPN with default OSPF DR priority configuration.

HP ADVPN solution iBGP design

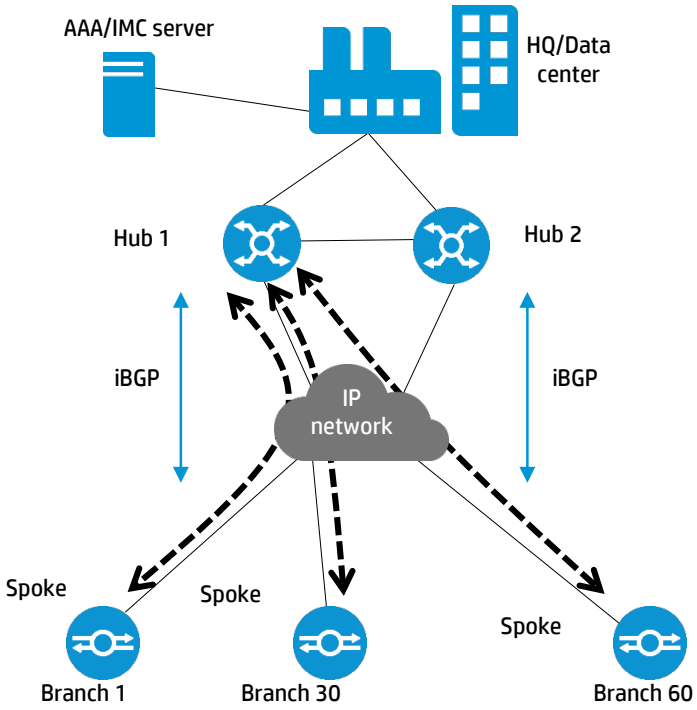
Using iBGP allows for configuration simplification by using a common AS shared across all VAM clients, leverages mechanisms like route reflectors and avoid having to assign lots of AS's for each location.

iBGP supports up to 3,000 branches in an ADVPN hub-groups:

- Method 1:
  - The hub does not advertise routes among spokes, only a default route to a spoke
  - Implies a hub and spoke topology
- Method 2:
  - The hub acts as the route reflector to exchange routes among spokes (up to 1000 spokes for full-mesh)
  - To implement full-mesh communications, configure spokes to not modify the next hops of specific routes learned from hub

An example of an HP ADVPN solution iBGP design is illustrated in the next figure.

Figure 24. HP ADVPN solution iBGP design



Every spoke sets up iBGP peers to the two hubs over the ADVPN tunnel. The hubs are configured as route reflectors (RR) and backup each other. The spokes act as RR clients. By default, when the RR reflects routes from one spoke to another spoke, it doesn't change the next hop information. Therefore, when a spoke receives routes for another destination spoke, the next hop is the tunnel private address of the destination spoke.

Method one uses the "peer x.x.x.x update-no-advertise" to advertise only a default route to the spoke routers. Using this command allows greater scalability. Using this feature takes pressure off of the hub routers allowing for a higher level of scalability per hub.

Performance will be dependent on customer requirements and system resource availability.

HP ADVPN solution eBGP design

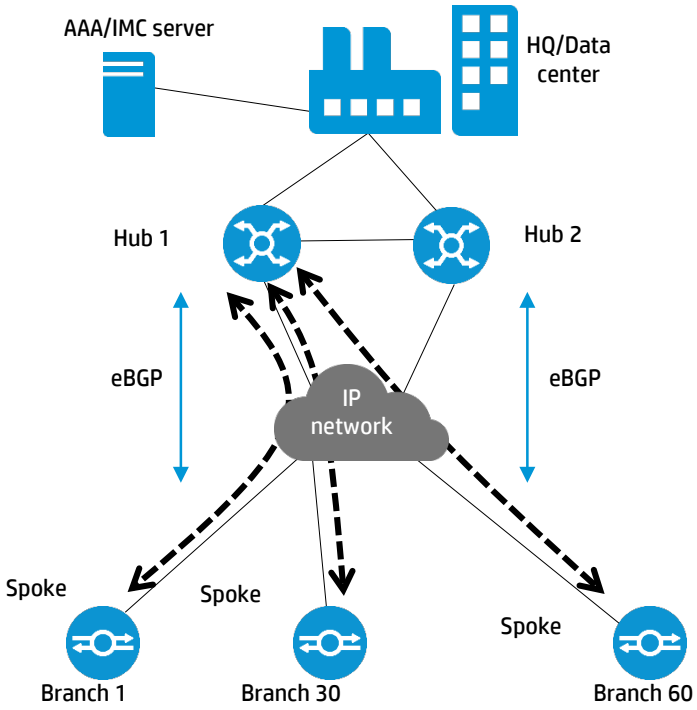
Using eBGP for an HP ADVPN solution is advantageous when spokes need to make a connection to a hub you control and for a hub-spoke connection with connections to other business partners.

By using eBGP, HP ADVPN solution supports up to 3,000 branches:

- Default route method
- Hubs and spokes reside in separate AS
- In hub-spoke mode, a hub enables next hop local feature, then all spokes send packets destined for other spokes via the hub

An example of an HP ADVPN solution eBGP design is illustrated in the next figure.

Figure 25. HP ADVPN solution eBGP design



Method one uses the “peer x.x.x.x update-no-advertise” to advertise only a default route to the spoke routers. Using this command allows greater scalability. Using this feature takes pressure off of the hub routers allowing for a higher level of scalability per hub.

Every spoke needs to set up eBGP peers to the two hubs over the ADVPN tunnels.

It is not necessary to set up eBGP peers between spokes because all ADVPN tunnels on different routers in the same ADVPN hub-group are on the same subnet. When a spoke receives routing information about the destination subnets connected to another spoke from the hub(s), the next hop is the ADVPN tunnel address of the destination spoke, not the hub(s).

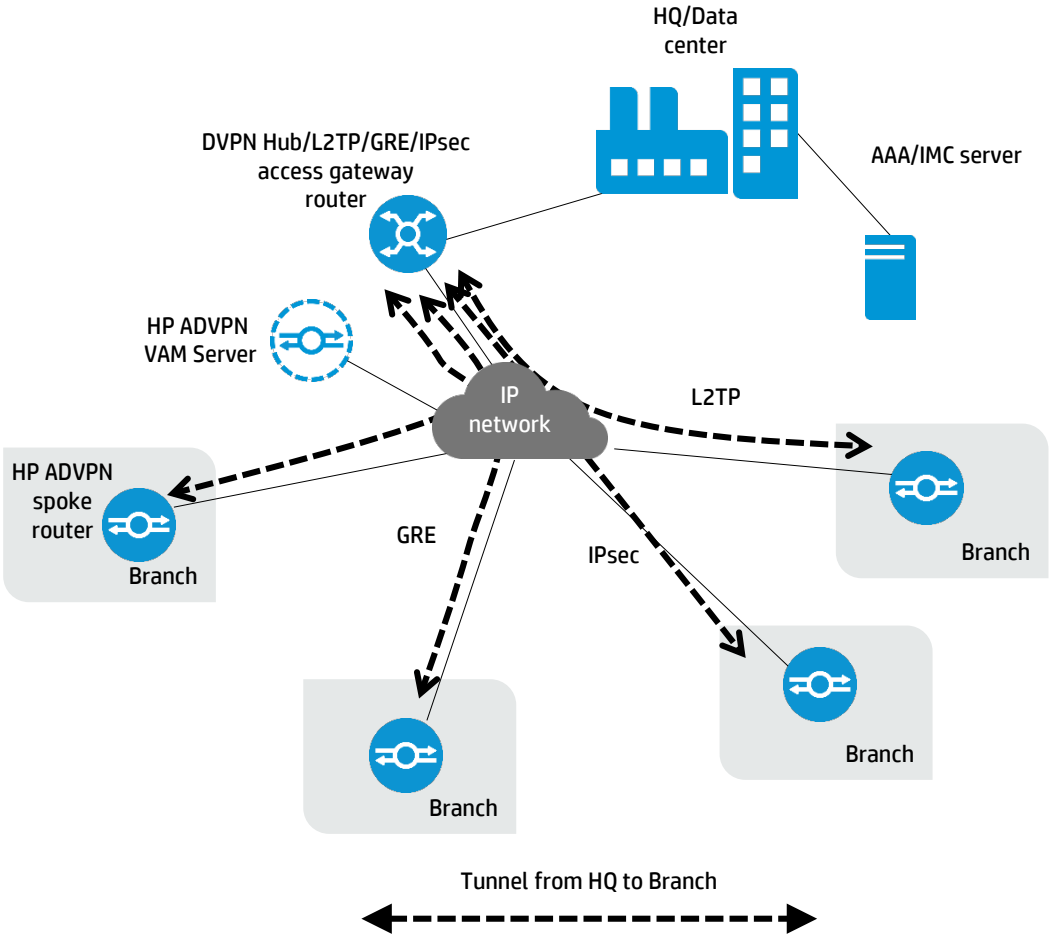
Integration with other vendor’s devices

While all dynamic VPN technologies are proprietary, we can still interoperate using standards based protocols with our hub routers. Other vendors cannot participate in an ADVPN domain, but they can connect to the ADVPN hub concurrently using standard protocols including GRE, L2TP, or IPsec.

HP routers (HP MSR Series Comware v7 and HP HSR6600 Series Comware v7) could run HP ADVPN and other vendors could connect to the same hub routers (same physical interface) using IPsec, L2TP, or GRE. Data transfer is standards-based IPsec between hub and spoke.

An example of an HP ADVPN solution integrating with other vendor devices is illustrated in the next figure.

Figure 26. HP ADVPN solution integration with other vendor devices



Features

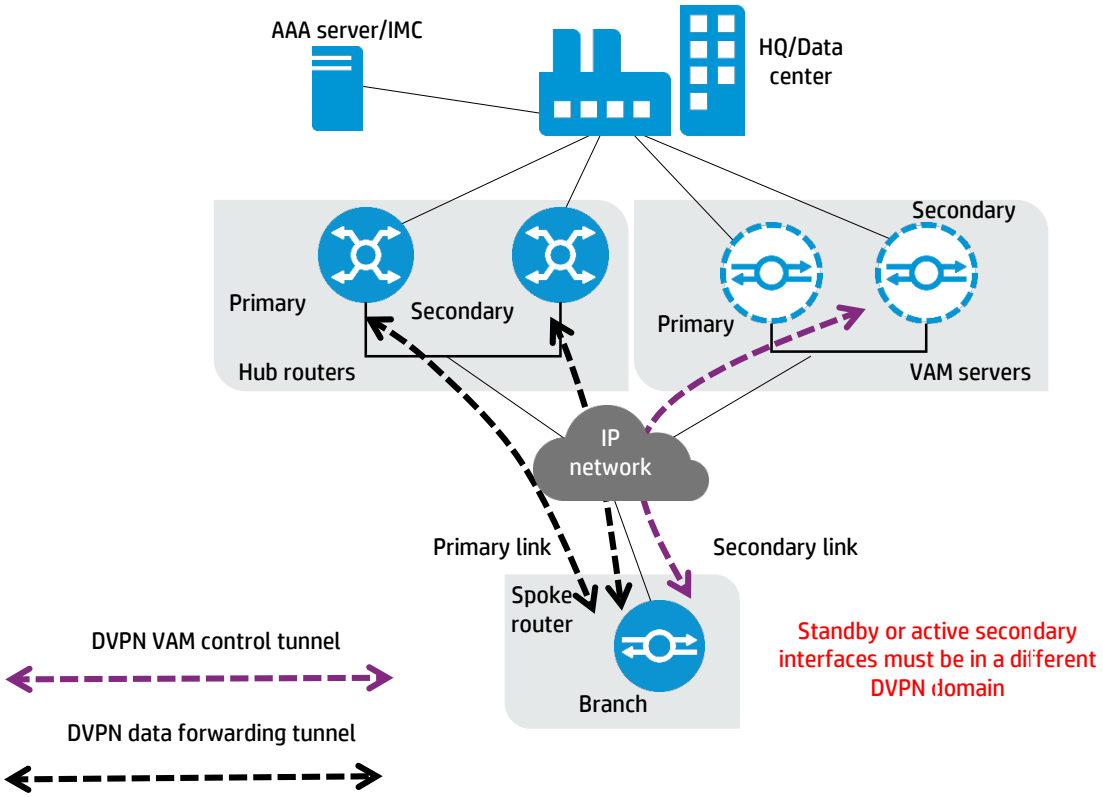
HP ADVPN solution high availability

The HP ADVPN solution provides high availability in its architecture:

- VAM server redundancy
  - Clients register with both at same time
- Hub redundancy
  - Spokes establish tunnels to both hubs
  - Hubs dynamically establish tunnels between each other
- Link redundancy
  - Encryption independent of interface
- Fault detection
  - VAM protocol switchover/recovery
  - Routing protocol convergence
  - BFD

An example of HP ADVPN solution high availability is illustrated in the figure 27.

Figure 27. HP ADVPN solution high availability



HP ADVPN provides three redundancy mechanisms:

- VAM server redundancy. You can deploy two VAM servers. Spokes and hubs register with both VAM servers at the same time, and the VAM servers authenticate the same VAM clients at the same time. Normally, VAM clients send query requests to the primary VAM server first. When the primary VAM server fails, the secondary VAM server provides query service. When the primary VAM server recovers, VAM clients begin to use the primary VAM server. Failure of a single VAM server does not result in service interruption.
- Hub redundancy. You can deploy two hubs. Spokes establish “active” DVPN tunnels to both hubs. When the primary hub fails, the tunnels to the secondary hub are used for data forwarding. Routing protocols can be manipulated (BGP) to share traffic load across both hubs concurrently (half the spokes prefer hub A, the other half hub B is one example).
- Link redundancy. A spoke can connect to the hub through two or more links that back up each other. ADVPN tunnels are mainly based on routing information, and data is encrypted before packets are forwarded. Data encryption is independent of the outbound interface.

In addition, HP ADVPN can cooperate with some common availability features to further improve the service availability. For example, in dual-hub mode, you can configure VRRP to establish routing neighbor relationship between the two hubs to implement route backup.

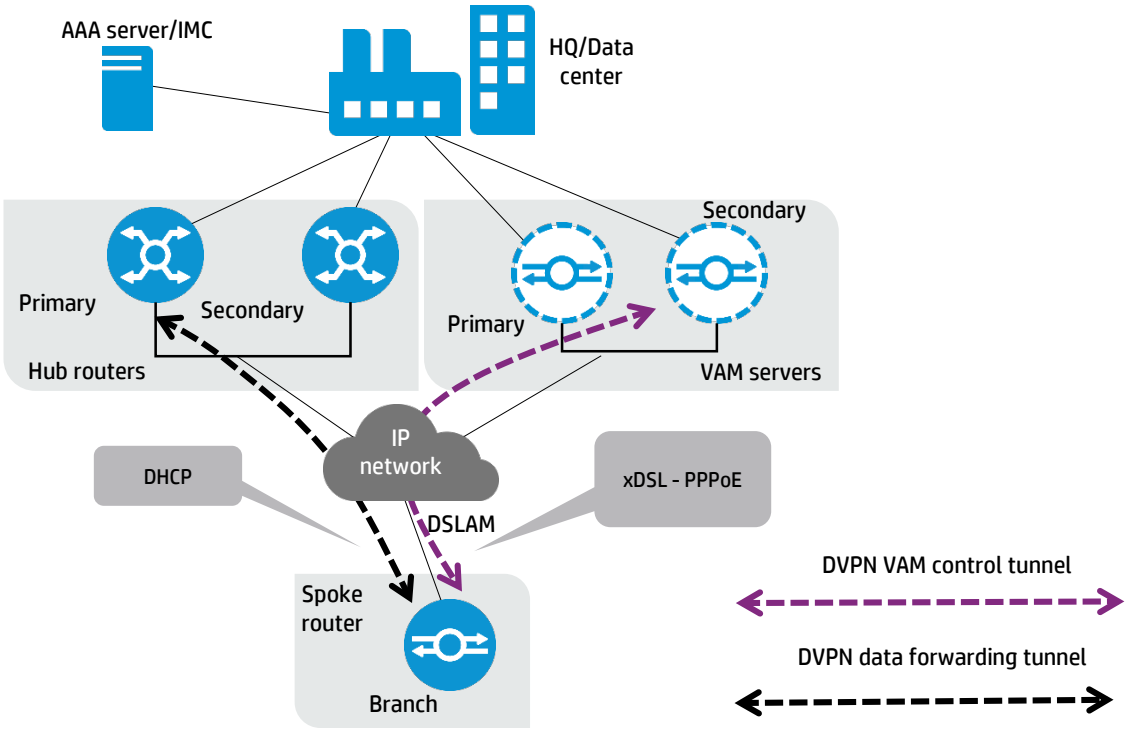
HP ADVPN solution dynamic addressing

The HP ADVPN solution supports multiple dynamic addressing delivery options:

- ADVPN clients can use DHCP or PPPoE to obtain a dynamic public IP address

An example of HP ADVPN solution dynamic addressing is illustrated in the next figure.

Figure 28. HP ADVPN solution dynamic addressing



HP ADVPN solution security

The security features of the HP ADVPN solution include:

- Data plane
  - Uses UDP encapsulation or GRE, allows configuration of IPsec with IKE
  - Encryption algorithm up to: AES-256
  - Authentication algorithm: SHA-1
  - Supports up to DH-group 24 with perfect forward secrecy (PFS)
- Control plane (VAM protocol)
  - Payload encryption algorithm: up to AES-256
  - Payload authentication algorithm: SHA-1
- VAM clients authenticated to an AAA Server inside VAM tunnel
  - Authentication method: Pre-shared key and username/password
  - Authentication protocol: PAP or CHAP with RADIUS

Note:
HP ADVPN is tunneled inside of IPsec when IPsec is used.

Compatibility between HP DVPN and HP ADVPN

HP ADVPN is compatible with HP DVPN, including these aspects:

- HP DVPN runs on HP Comware v5
- HP ADVPN runs on HP Comware v7
- HP ADVPN on Comware v7 is compatible with HP DVPN on Comware v5
- In a hybrid system, the overall functionality is that of Comware v5
- VAM server on Comware v7 is compatible with VAM clients on Comware v5

- VAM clients (hub and spoke) on Comware v7 are compatible with VAM server on Comware v5
- VAM clients (hub and spoke) on Comware v7 are compatible with VAM clients (hub and spoke) on Comware v5

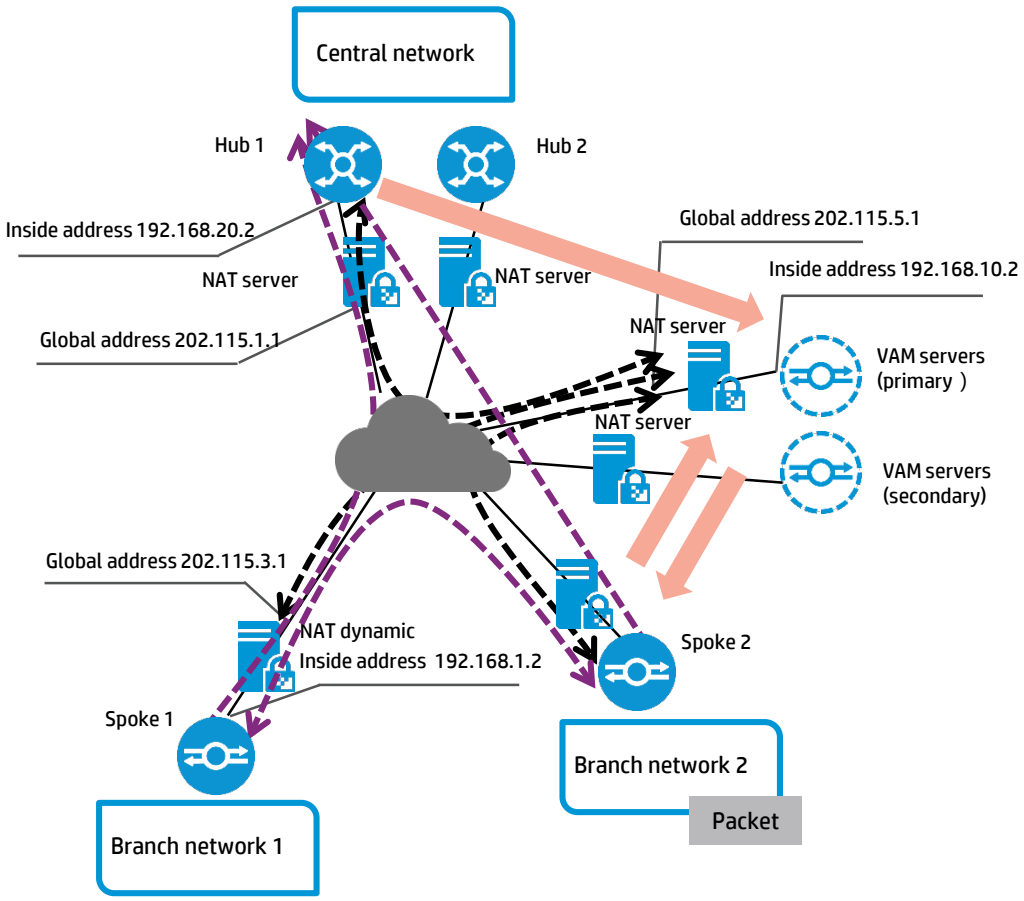
HP ADVPN solution NAT traversal

The HP ADVPN solution supports ADVPN through a NAT gateway. All the hubs, spokes, and VAM servers can be located in the NAT box under some restrictions:

- The VAM server and hubs should be behind the static NAT box
- The NAT box with PAT mode uses the endpoint-independent mapping (EIM) behaviors

The NAT box can be in No-PAT or PAT (port address translation) mode. When the NAT box is in PAT mode, the hub updates the source IPsec port and address information to VAM servers, and the spoke can get the ADVPN peer's NAT-translated port and address from VAM servers. An example of HP ADVPN solution NAT traversal is illustrated in the diagram below.

Figure 29. HP ADVPN solution NAT traversal



The message flow for spoke-spoke tunnel using NAT includes:

- Spoke 1 sets up IPsec tunnel with hub. Hub records the IP address and port of spoke 1, which are translated by NAT 1
- Same with spoke 2
- Hub sends node information update message to VAM server to update the information of spoke 1 and spoke 2
  - Then the VAM server updates the public IP address and port of spoke 1 and spoke 2.
- Spoke 1 sends resolution request message to VAM server
- VAM server sends resolution response message to spoke 1.
- Spoke 1 sets up IPsec tunnel with spoke 2.

HP ADVPN tunnels that use UDP encapsulation support NAT traversal natively, and can traverse any type of NAT gateway. Better than other point-to-multipoint tunneling technologies, ADVPN supports two spokes to reside behind the same NAT gateway and use the same NAT public address.

ADVPN supports dynamic address mapping. You do not need to know the public address or port number that the peer will use when the peer resides behind a NAT gateway. For example, when two spokes need to communicate and at least one of them is behind a NAT gateway, one of the following cases may occur:

- If only the tunnel initiator resides behind a NAT gateway, a spoke-spoke tunnel can be established across the NAT gateway.
- If the tunnel request receiver is behind a NAT gateway, packets must be forwarded by a hub before the receiver originates a tunnel establishment request.
- If both spokes reside behind NAT gateways, no tunnel can be established between them and packets between them will be forwarded by a hub.

If used with IPsec, the ADVPN encapsulation does not matter as ADVPN is encapsulated within the UDP based ESP header, so it already has good interoperability when NAT is involved. This would only make a difference if IPsec was not used and ADVPN tunnel mode UDP would be preferred when NAT is involved.

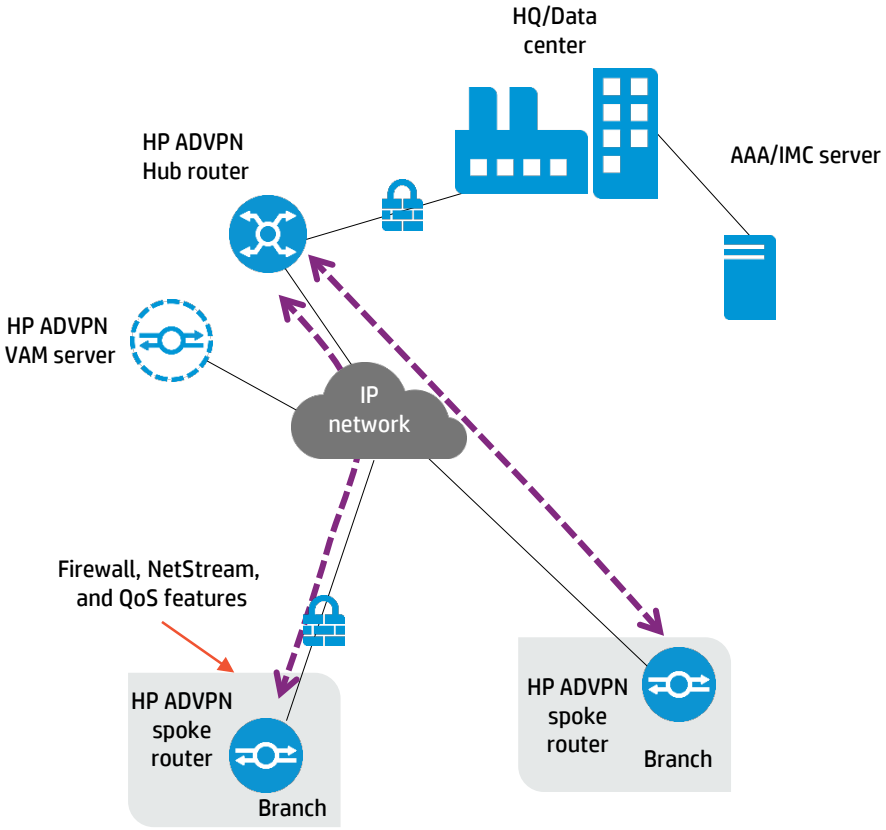
HP ADVPN solution quality of service

Use QoS to guarantee service quality of key traffic flows:

- Hub and spokes identify and mark traffic on internal interface
- Use firewall, NetStream, and QoS to implement ADVPN traffic filtering and statistics
- Single or multitunnel QoS

An example of HP ADVPN solution quality of service is illustrated in figure 30.

Figure 30. HP ADVPN solution quality of service



On the router, an ADVPN interface takes the form of a tunnel interface. Features supported on a tunnel interface, such as firewall and NetStream, can be used to implement ADVPN traffic filtering and statistics. The HP ADVPN solution supports single or multitunnel QoS.

ADVPN supports deploying QoS for key services. It identifies and flags the key service flows on the user side network interface, and performs QoS operations according to the flags (QoS local IDs) on the public network outbound interface. To deploy QoS for ADVPN, you need to perform configurations on both the inbound and outbound interfaces.

Single-tunnel multiservice QoS design:

- The hub and spoke identify and mark traffic (use ACL for identification and use IPP, DSCP, or qos-local-id for marking) on their internal interface.
- The hub and spoke perform standard QoS queue scheduling for different services on their Internet interface.

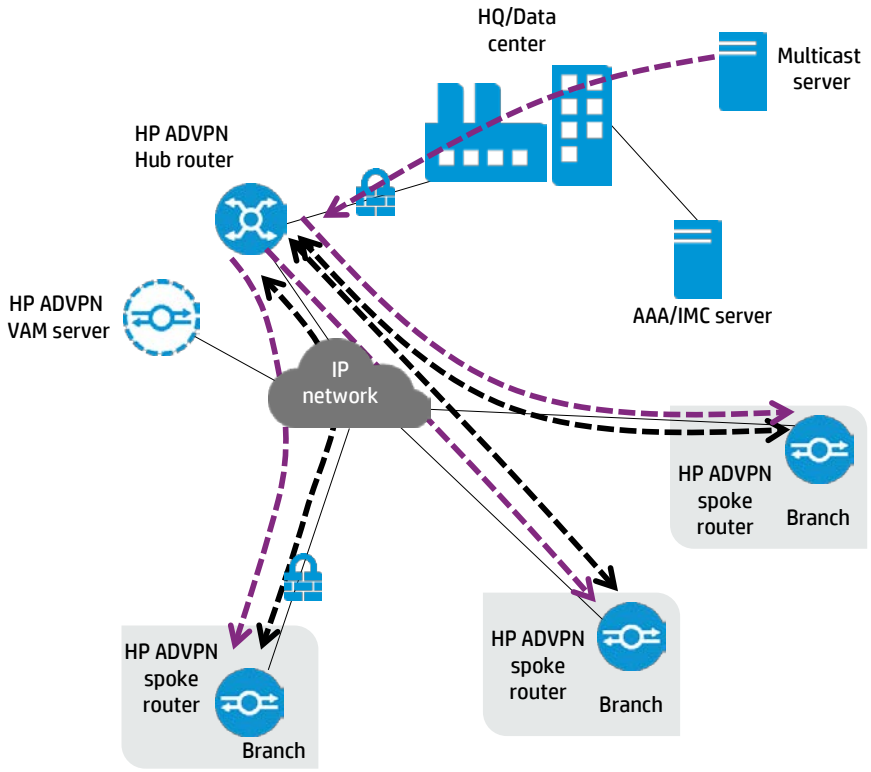
Multitunnel multiservice QoS design:

- Uses a separate tunnel for each service. Other aspects are the same as the previous QoS design. As each service uses a separate tunnel, packet loss of a low-priority service will not affect any high-priority service. See the HP HSR6600 ADVPN solution configuration guide for more details.

HP ADVPN solution and multicast traffic

The HP ADVPN solution supports multicast protocols. An example of HP ADVPN solution with multicast traffic is illustrated in the next figure.

Figure 31. HP ADVPN solution with multicast traffic



A small amount of multicast traffic can be supported today, however, if there are requirements for significant amounts of multicast, recommendations include:

- Can disable IPsec on tunnels to improve multicast forwarding performance, if security requirements are not stringent
- Can send multicast traffic outside of the tunnel for best performance in larger scale deployments
- Can set up a second ADVPN domain and force those sites that need multicast use that second domain

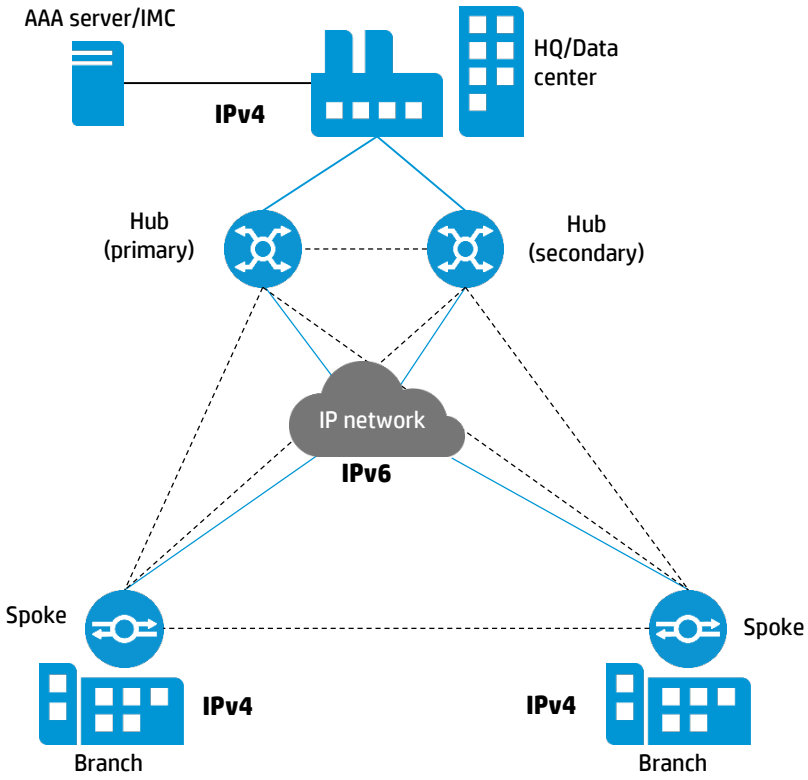
HP ADVPN solution and IPv6

The HP ADVPN solution supports:

- IPv6 packets over ADVPN IPv4 tunnel
- IPv6 packets over ADVPN IPv6 tunnel
- IPv4 packets over ADVPN IPv6 tunnel

An example of using IPv6 in an HP ADVPN solution is illustrated in the next figure.

Figure 32. Using IPv6 in an HP ADVPN solution



HP ADVPN management with IMC BIMS

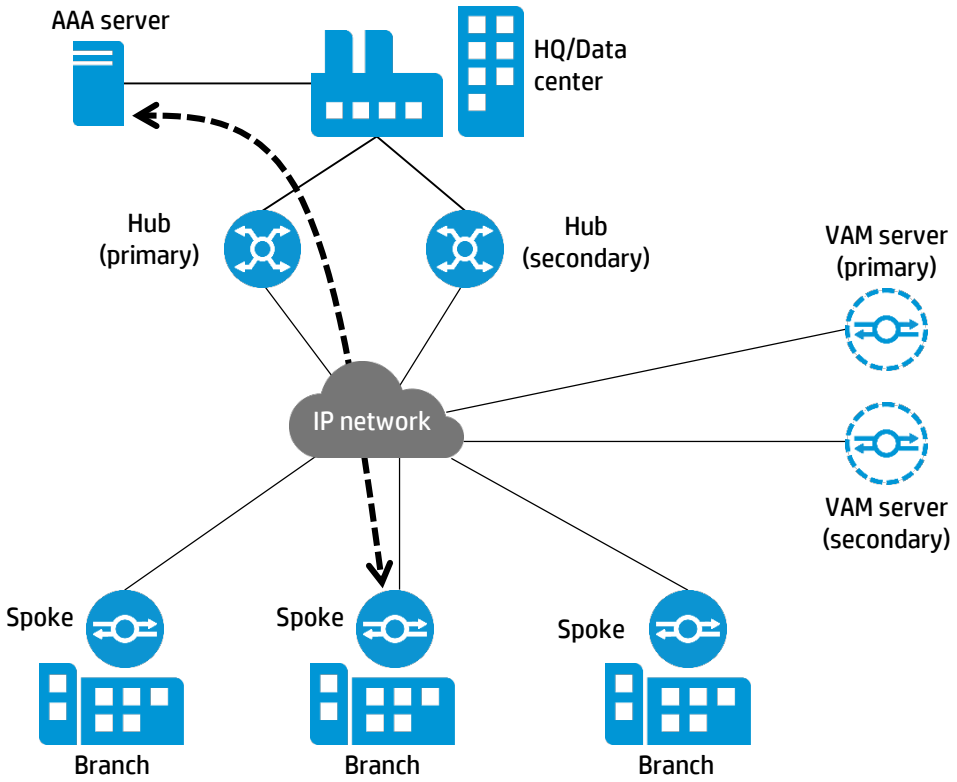
TR-069 is a Broadband Forum's technical specification titled CPE WAN Management Protocol (CWMP) that HP IMC BIMS uses to manage/monitor/configure HP MSR Router Series at the edge of an open WAN (Internet). CWMP is a SOAP/HTTP-based protocol that provides communication between the CPE and the Auto-Configuration Server (ACS). It includes safe auto-configuration and control of other CPE management functions within an integrated framework. The client-server traffic can be configured over SSL to secure management interaction with the device.

The HP ADVPN Solution and HP MSR Router Series support zero touch configuration and software upgrades for branch device deployments:

- Out of path from ADVPN
- Secure with SSL
- Scheduled ad-hoc configuration and software upgrades
- Comprehensive monitoring of physical links
- Scales to 10,000 branches (HP MSR)

An example of HP ADVPN solution, HP IMC BIMS is illustrated in the following figure.

Figure 33. HP ADVPN solution with HP IMC BIMS



An administrator pre-stages a brief CWMP configlet on the spoke router (currently supported on MSR series) and configures the appropriate dynamic IP address method to be used on the Internet facing interface (DHCP, PPPoE) of the router before shipping it to the remote site. The BIMS server pushes the remaining device configuration to the device once the spoke has authenticated with the BIMS server. In this case, BIMS is pushing the ADVPN-related configuration and any other configuration that is required.

Configurations

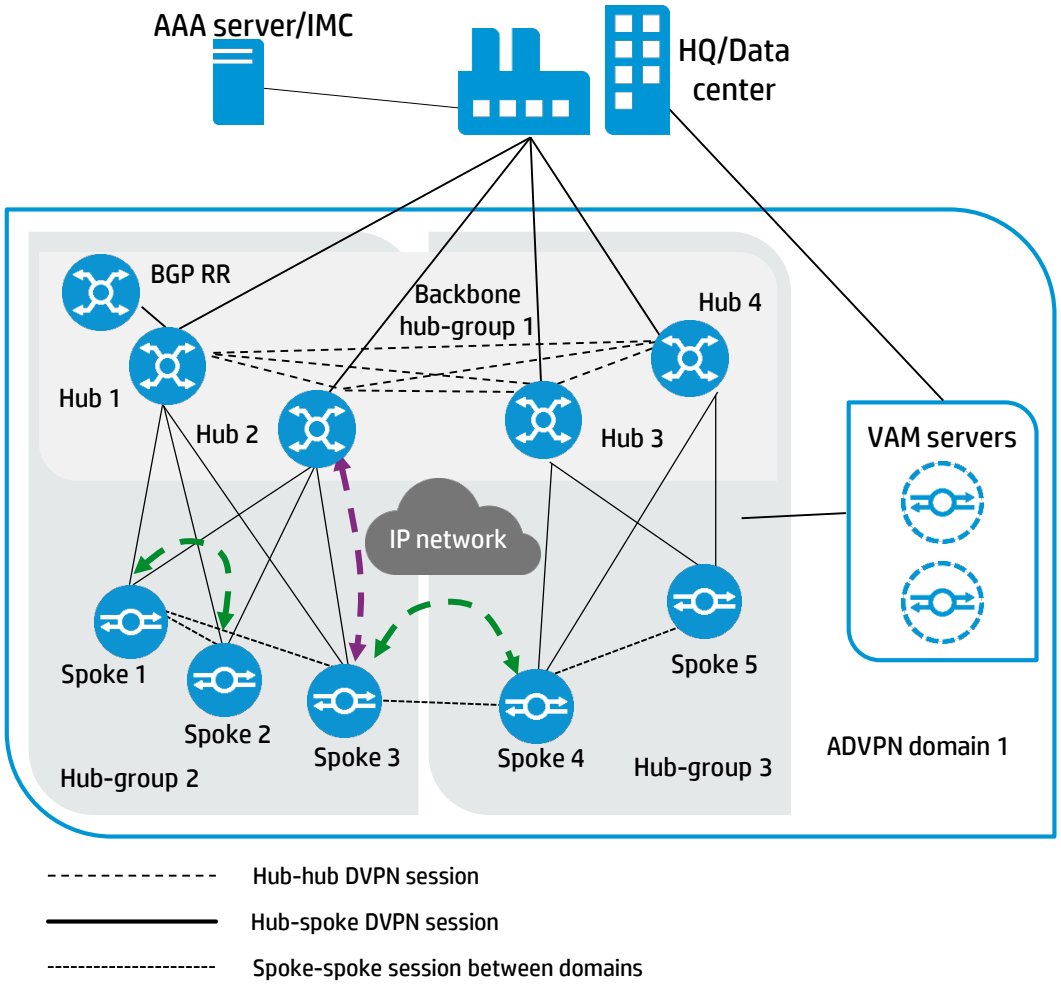
HP ADVPN recommended solutions

The configuration procedure for an HP ADVPN solution typically encompasses these steps:

- Configure VAM servers and VAM clients, so that they can exchange address information
- Configure DVPN tunnel on the hubs and every spoke
- Configure private routing protocol on ADVPN tunnel interfaces. To get different network topologies within ADVPN, use different routing protocols or different configuration modes within a specific routing protocol as desired.
- Configure IPsec on every hub and spoke for security
- All spokes in same domain
- The number of hub-groups required depends on the specifications of the hubs

An example of an HP ADVPN solution typical network architecture is illustrated in the diagram below.

Figure 34. HP ADVPN solution typical network architecture



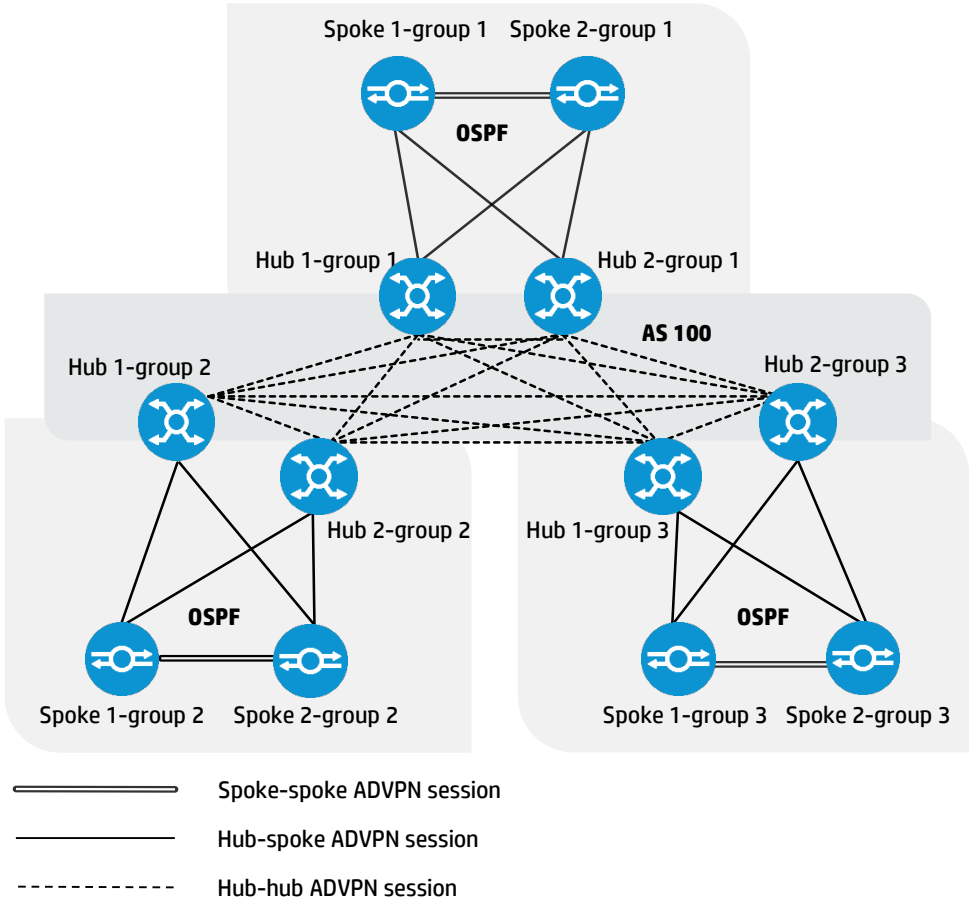
Hub-spoke recommended solution using OSPF

The characteristics of a hub-spoke structure using OSPF includes:

- OSPF is used to exchanging routing information within a hub group.
- All the hubs in the backbone group are IBGP peers.
- If broadcast network type is configured for the tunnel interface, the network structure is full mesh. The spokes in one group can directly communicate with each other.
- If P2MP network type is configured for the tunnel interface, the network structure is hub-spoke. The spokes in one group communicate with each other through the hub.
- Advantage:
  - Configurations on spoke is simple
- Limit:
  - The number of spokes in one group should be less than 500

An example of an HP ADVPN solution using a hub-spoke structure and OSPF is illustrated in the diagram below.

Figure 35. Using OSPF in an HP ADVPN hub-spoke structure



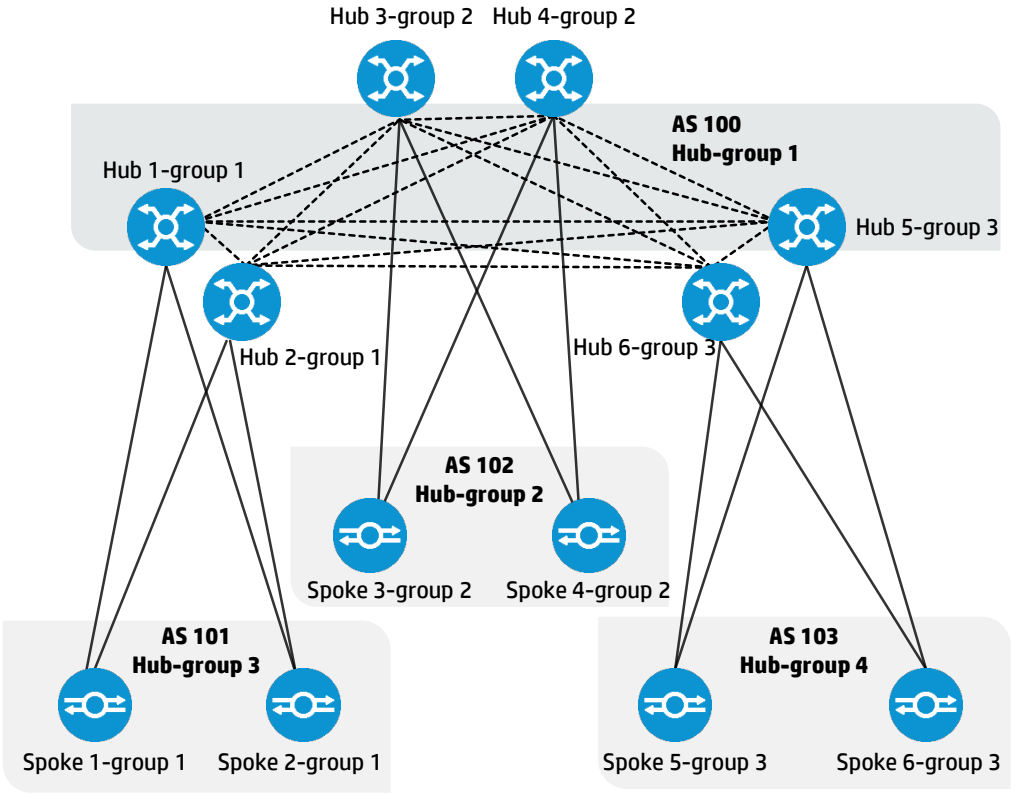
Hub-spoke recommended solution using BGP

The characteristics of a hub-spoke structure using BGP includes:

- All the hubs in the backbone group are iBGP peers
- The hubs and spokes within one group are eBGP peers.
- Each hub should set itself as the next hop for routes sent to other groups. (use peer next-hop-local command)
- The spokes should permit the local AS number to appear in routes from a peer in the same AS.
- Advantage:
  - All the routes on spokes received from the HUB have a next hop direct to the HUB tunnel address. No route policy needed.
- Limit:
  - The number of spokes in one group should be less than 2000 when MSR4000 SPU-300 acts as the HUB

An example of an HP ADVPN solution using a hub-spoke structure and BGP is illustrated in the diagram below.

Figure 36. Using OSPF in an HP ADVPN hub-spoke structure



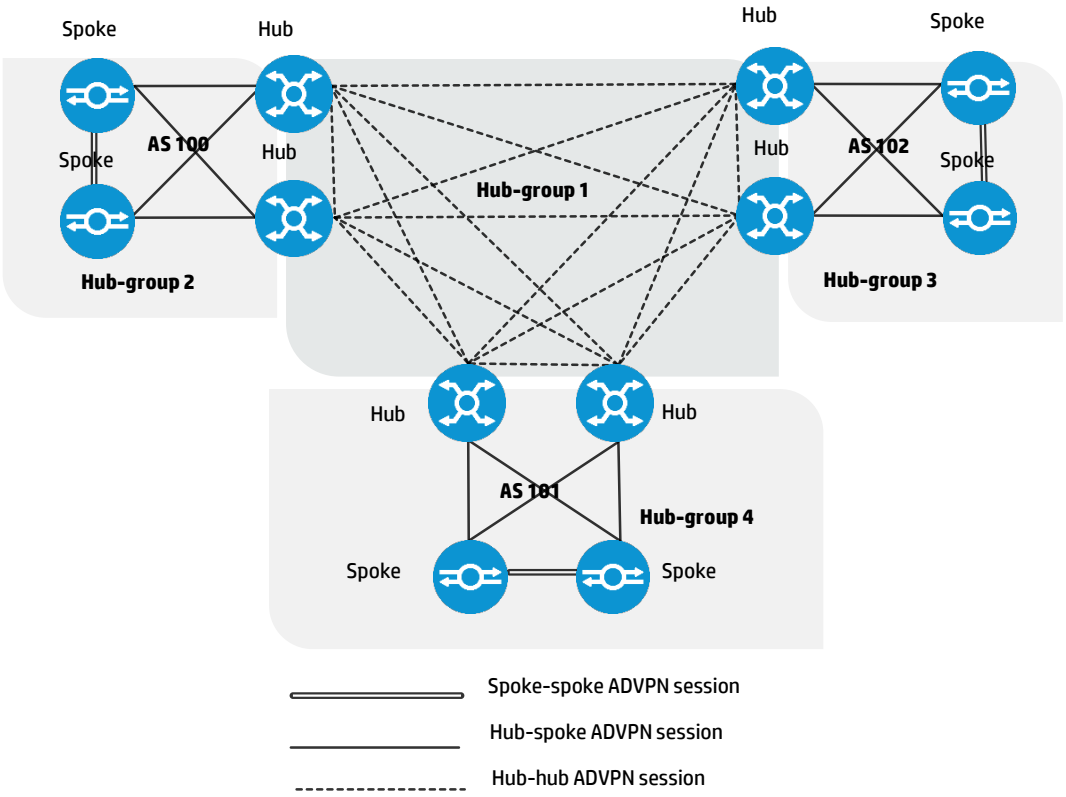
Full mesh recommended solution using BGP

The characteristics of a hub-spoke structure using BGP includes:

- Hubs and spokes in one group are IBGP peers.
- Hubs between different groups are EBGP peers.
- The hubs reflect routes to the spokes that in the same group.
- The spokes should modify the next hop to the HUB when they receive the route to other groups.
- Advantage:
  - In the group, the network structure is full-mesh structure. No more route policy is needed.
- Take note:
  - Between the groups, the spoke need extra route policy to change the next hop.
- Limit:
  - The number of spokes in one group should be less than 1000

An example of an HP ADVPN solution using a spoke-spoke (full mesh) structure and BGP is illustrated in the diagram below.

Figure 37. Using BGP in an HP ADVPN full mesh structure



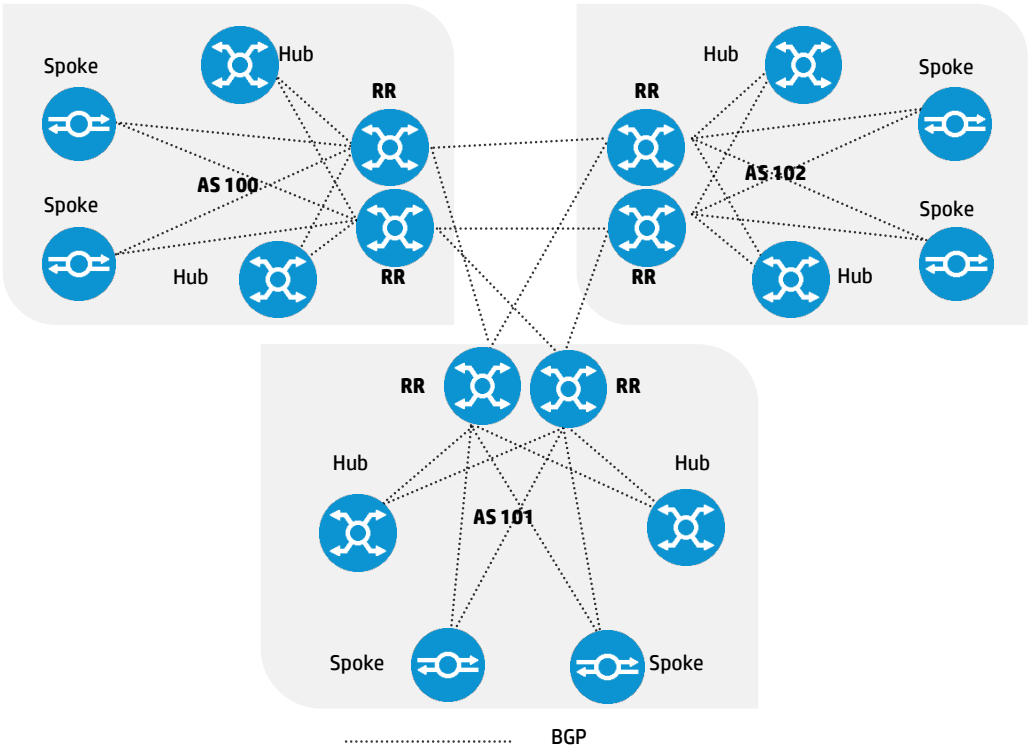
Full mesh recommended solution using BGP route reflector

The characteristics of a spoke-spoke (full mesh) structure using BGP route reflector (RR) includes:

- Each group has their own route reflector.
- And hubs and spokes act as route reflector clients.
- The route reflectors between groups are EBGP peers.
- When the route reflectors receive routes from other groups, they modify the next hop to the HUB that in the same group.
- When the hubs receive routes from other groups, they modify the next hop to the HUB in the group which the routes come from.
- Advantage:
  - In the group, the network structure is full-mesh structure. No more route policy needed for the spokes.

An example of an HP ADVPN solution using a spoke-spoke (full mesh) structure and BGP with route reflector is illustrated in the diagram below.

Figure 38. Using BGP RR in an HP ADVPN full mesh structure

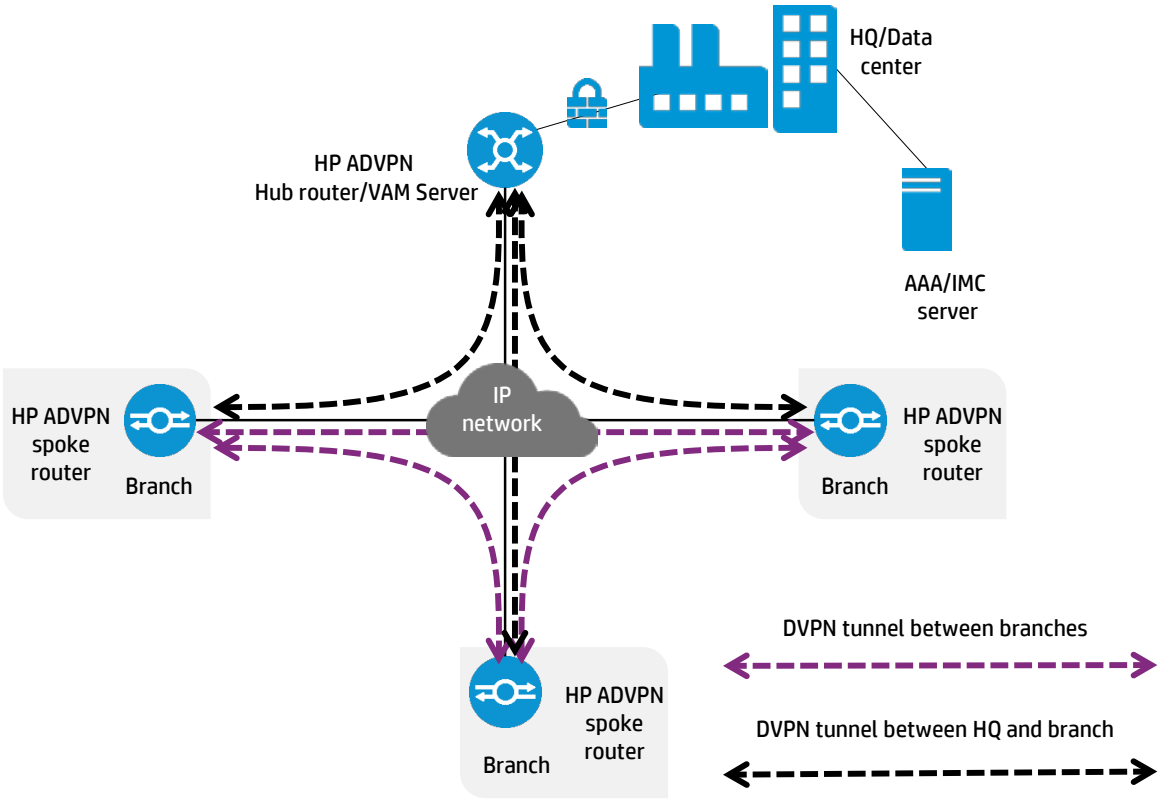


HP ADVPN solution hub and VAM server combination

In a relatively small deployment, you can combine ADVPN hub and ADVPN VAM server on the same router.

An example of HP ADVPN solution with hub and VAM server combination is illustrated in the diagram below.

Figure 39. HP ADVPN solution hub and VAM server combination



We do not recommend doing this with more than 50 sites with HP MSR4000 as the hub. It's also important to know that you can use a less expensive HP MSR router as the VAM server(s) to help reduce cost in smaller deployments, so there are options.

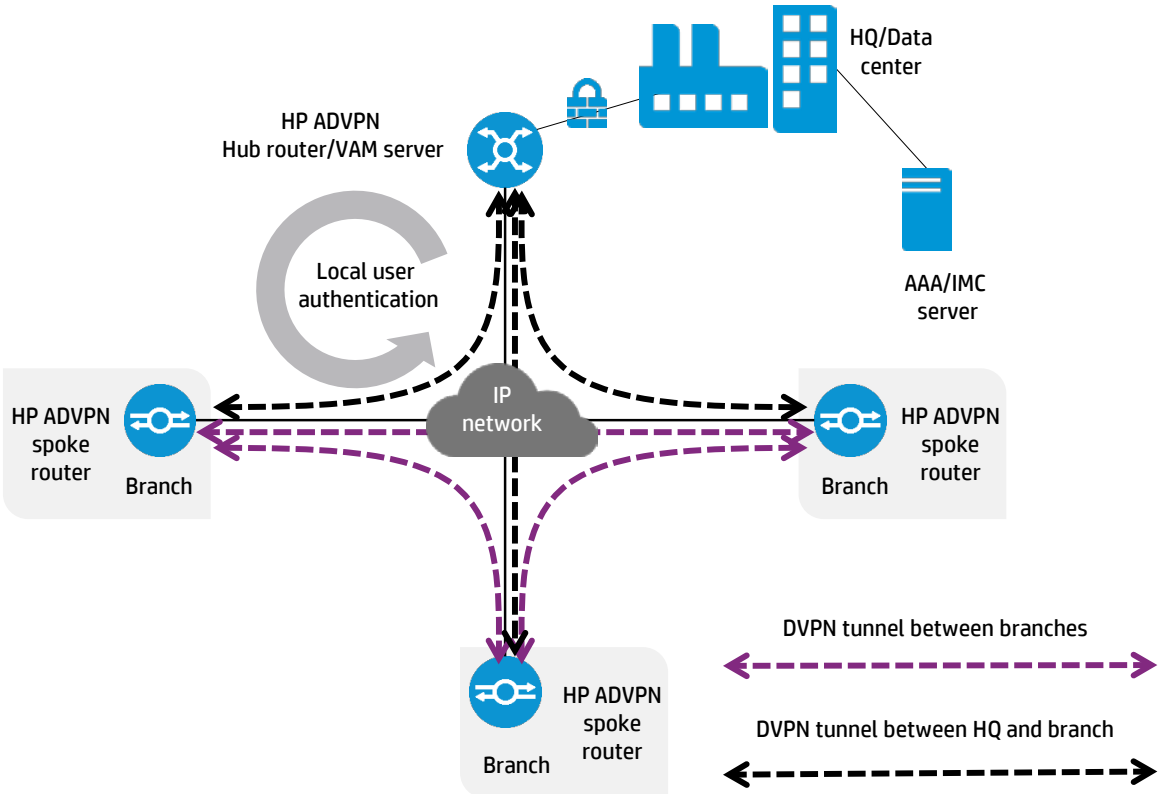
HP ADVPN local user authentication

If no AAA Server is available, can configure local authentication on the ADVPN VAM Server

- Helps reduce investment
- Pay attention to maximum number of local users

An example of HP ADVPN solution with local user authentication is illustrated in the diagram below.

Figure 40. HP ADVPN solution local user authentication



You may want to consider single ADVPN unam/pwd for device auth to simplify the deployment. This can be used and configured in the same default domain that TACACS is configured in for admin authentication. This new feature eliminates the need for two authentication domains within Comware (one for ADVPN and one for TACACS administration) without the need for using realms behind the user ID when an admin needs to login to the router (e.g., username: uname@realm).

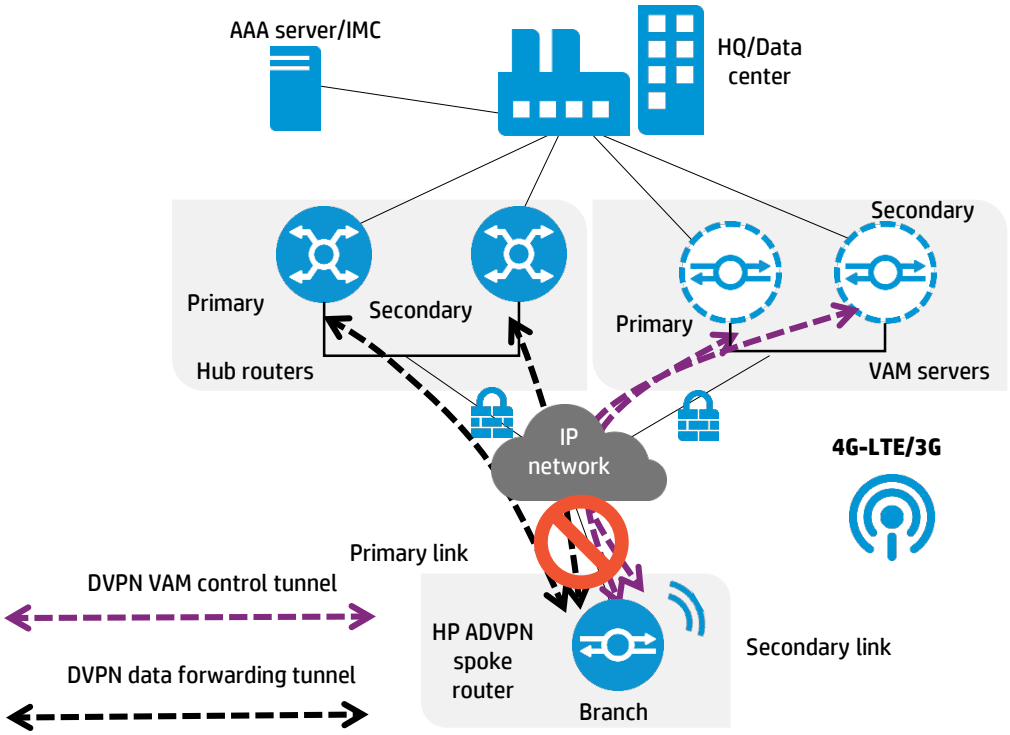
Using 4G-LTE/3G as backup to wired HP ADVPN

With the HP ADVPN solution, you can use 4G-LTE/3G as a backup to wired ADVPN. Standby or active secondary interfaces must be in a different ADVPN domain. When using 4G-LTE/3G as backup for wired ADVPN tunnel:

- Configure two tunnels on the hub. One corresponds to the 4G-LTE/3G wireless tunnel and the other corresponds to the wired tunnel. When the wired tunnel fails, the spoke sends traffic through the 4G-LTE/3G wireless tunnel, which then passes the hub and the core switch to implement inter-domain communication with other spokes.
- The 4G-LTE/3G link and the wired link use different interfaces and tunnels and belong to different ADVPN domains. The hub must support the ADVPN domain of the 4G-LTE/3G link so the spoke can use the 4G-LTE/3G link when the wired link fails. In addition, the spoke needs the core switch to communicate with another spoke through the 4G-LTE/3G link.

An example of HP ADVPN solution using 3G as a backup to wired ADVPN is illustrated in the diagram below.

Figure 41. HP ADVPN solution using 4G-LTE/3G as a backup to wired ADVPN



Here is an example of how redundancy works with separate physical circuits:

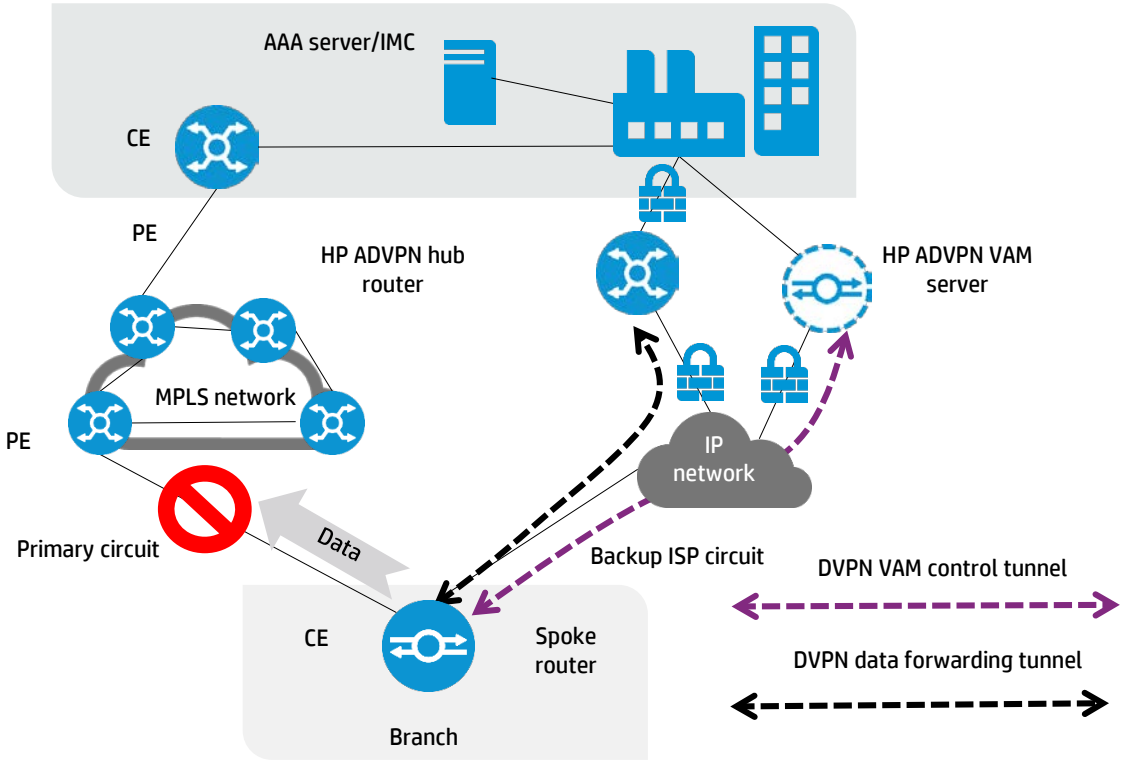
- The proverbial back hoe takes the primary circuit offline. The tunnels and/or routing peers drop.
- We can use either the standby interface level commands (assuming the secondary circuit is priced based on usage) or we can use an active backup link that has parallel tunnels and peers or neighbors established in order to restore connectivity to the DC. In the scenario where the backup link is in standby mode, the failover times will be longer due to the process involved in detecting the link down and bringing secondary link online, acquiring an address, authenticating with the VAM server, establishing a tunnel, establishing adjacencies, etc. In the scenario where the secondary circuit is always active, we are looking at failover times consistent with routing protocol failover.
- Additionally, through routing protocol manipulation, we can also use both links
- Connectivity is then restored to the main link (preferred), tunnels are established and traffic is now re-routed over the main link
- An external 3G modem can be used in this failover scenario or used as a primary circuit and can be supported by wireless providers with some extra planning and configuration.

Using HP ADVPN as backup to MPLS L3 VPN

When using the HP ADVPN solution to back up MPLS VPN, the spoke device uses an ADVPN tunnel to back up the MPLS VPN dedicated line. When the MPLS VPN link fails, the spoke uses the ADVPN tunnel to forward traffic, avoiding service interruption. When the MPLS VPN link recovers, it switches traffic back to the MPLS VPN link. Backup could also be 3G as opposed to wired ISP.

An example of HP ADVPN solution providing backup to MPLS L3 VPN is illustrated in the figure 42.

Figure 42. HP ADVPN solution providing backup to MPLS L3 VPN



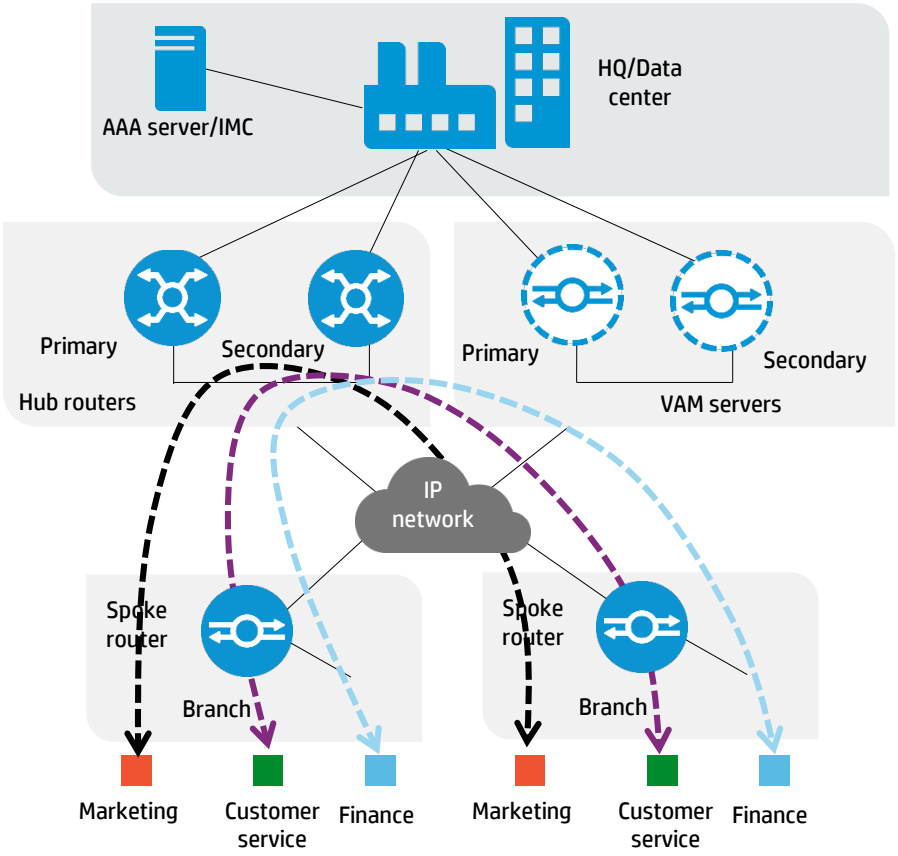
HP ADVPN can be active concurrently with another transport (it is just like another routed interface as previously mentioned) or in standby interface mode, you can manipulate the routing protocol used to achieve the desired behavior if two active links are required.

Using HP ADVPN to create multiple VPNs

The HP ADVPN solution supports the ability to configure multiple ADVPN domains on a hub and spoke for different departments. Configure the spoke to terminate multiple service VLANs, each corresponding to an ADVPN domain and a VRF, and map VLANs to Layer 3 VPNs.

An example of HP ADVPN solution using multiple VPNs is illustrated in the following figure.

Figure 43. HP ADVPN solution and multiple VPNs



Multiple tunnel interfaces in different VRF's sharing a single physical WAN link allows separation of business unit traffic within a site and across the network.

Specifications

Products supporting HP ADVPN solution

The table below shows the products and software versions that support the HP ADVPN solution. A spoke can be any HP MSR2000, MSR3000, or MSR4000 Router Series. A VAM server can be any HP MSR2000/3000/4000 Series or HP HSR6600-X/XG Router Series, and the hub is mainly the HP HSR6600 Series. For smaller scale deployments, the HP MSR4000 Series can be used as a hub.

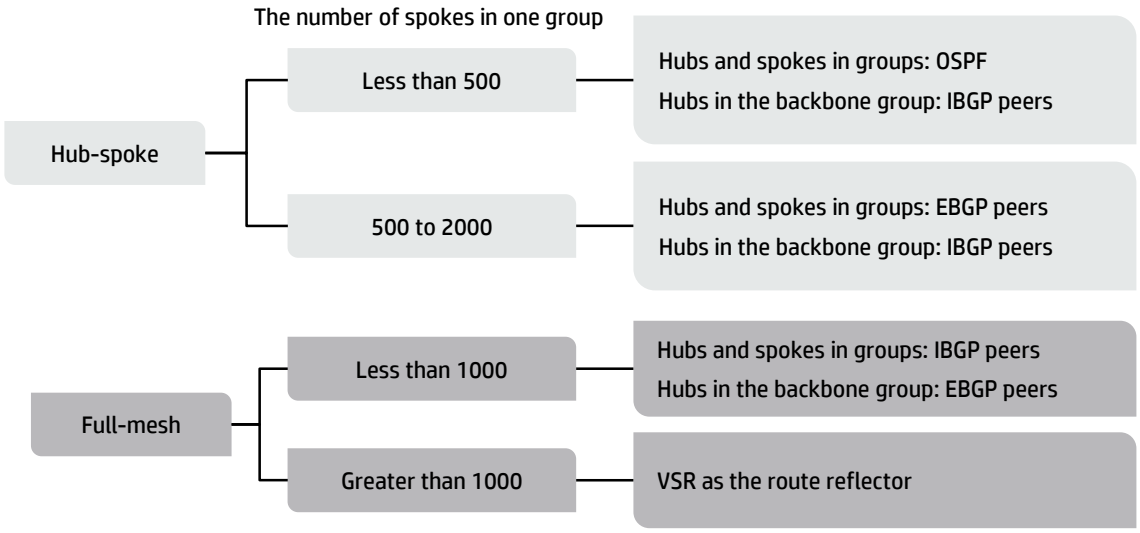
Table 1. HP ADVPN solution hardware and software support

Component	Hardware	Software
Spoke	HSR6602-X/XG MSR2000/3000/4000	MSR CW7 R0106—June 2014
Hub	HSR6602-X/XG MSR2000/3064/4000	MSR CW7 R0106—June 2014
VAM server	HSR6602-X/XG MSR2000/3000/4000	MSR CW7 R0106—June 2014
IMC BIMS	Server Wintel/Linux®	IMC v7—2013

HP ADVPN solution scalability

The scalability of the HP ADVPN solution is illustrated in table 2. The performance values in the Hub (VAM client) column reflect those platforms operating as a hub, not as a VAM server.

Table 2. Scalability of HP ADVPN solution



HP ADVPN hub capacities

The capacities of hubs on a per-product basis are described in the table below.

Table 3. Hub capacities of HP ADVPN solution

Configuration	SPU-300	SPU-200	SPU-100	MSR3064	MSR3044	Notes
Hub-spoke	2000	1100	600	500	300	2G memory, only one BGP route per spoke site, 2M bandwidth with 1500 byte traffic per spoke site.
Full-mesh	1000	-	-	-	-	4G memory, 1000 BGP peer, only one BGP route per spoke site

Summary

The HP ADVPN solution:

- Solves the scaling and configuration issues inherent in overlay VPNs
- Can use lower cost ISP-based transport for WAN backup or private line replacement
- Can be deployed over other IP based transports (such as MPLS)
- Reduced hub configuration (single tunnel interface)
- Routing protocols run natively on tunnel interface
- Clients can use static or dynamic addressing for hub and spoke routers
- Separation of control and data planes
- Data plane encryption is standards-based IPsec

Additional links

Visit hp.com/networking for information on how the HP FlexNetwork Solution helps transform the networking experience.

- For more information on HP ADVPN, HP routers and other HP FlexNetwork content, refer to information available on the HP Networking Resource Finder Technical Documentation tab and selecting “Routers” under “Products, Solutions, and Industries”.

At the HP Customer Care—product support website, use the model name of the HP router, for example “MSR3044” in the HP product name field. For these resources:

- Refer to the product manuals for details on supported commands and configurations
- Click “Knowledge Base”, then click “Manuals” in the pull-down menu
- Refer to the release notes for details on supported features, software and hardware versions, limitations, and known issues
- Find software

Learn more at
hp.com/networking/routers

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-6340ENW, March 2015