MSR系列路由器DVPN功能(Full-mesh)的配置

姚忆斌　2007-10-27 发表

MSR系列路由器

DVPN功能(Full-mesh)的典型配置

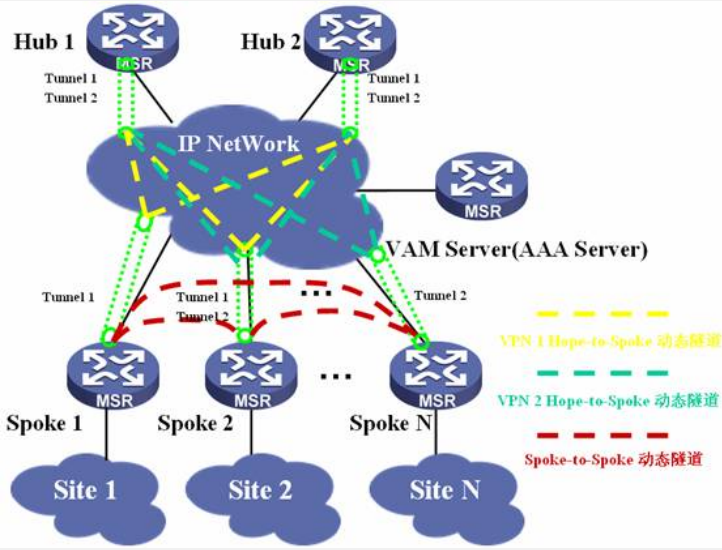
关键字：MSR; DVPN; 动态隧道

一、**组网需求**:

在Full-Mesh的组网方式下， 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建立永久隧道连接。任意的两个Spoke之间在有数据时动态建立隧道连接。

设备清单：MSR系列路由器6台

二、组网图:



设备	接口	IP 地址	设备	接口	IP 地址
Hub 1	G0/0	192.168.1.1/24	Spoke 1	G0/0	192.168.1.3/24
	Tunnel1	10.0.1.1/24		Tunnel1	10.0.1.3/24
	Tunnel2	10.0.2.1/24	Spoke 2	G0/0	192.168.1.4/24
Hub 2	G0/0	192.168.1.2/24		Tunnel1	10.0.1.4/24
	Tunnel1	10.0.1.2/24		Tunnel2	10.0.2.4/24
	Tunnel2	10.0.2.2/24	Spoke n	…	…
Main server	G0/0	192.168.1.22/24	AAAServer	G0/0	192.168.1.22/24

三、配置步骤:

适用设备和版本：MSR系列、Version 5.20, Release 1508后所有版本（标准版）。

VAM Server AAA Server配置

```
#
 sysname VAMSERVER
#
 //指定VAM Server上的监听IP地址
 vam server ip 192.168.1.22
#
 domain default enable system
#
//配置认证方式，本例中路由器作为AAA Server
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
//创建VPN，域ID为1
vam server vpn 1
 server enable
 //预共享密钥为123
 pre-shared-key simple 123
 //指定VPN 1 的两个Hub地址
 hub private-ip 10.0.1.1
 hub private-ip 10.0.1.2
#
//创建VPN，域ID为2
vam server vpn 2
 server enable
 authentication-method pap
 pre-shared-key simple 456
 hub private-ip 10.0.2.1
 hub private-ip 10.0.2.2
#
//创建本地用户，用于认证Hub和Spoke设备
local-user dvpn1hub1
 password simple dvpn1hub1
 level 3
 service-type dvpn
local-user dvpn1hub2
 password simple dvpn1hub2
 level 3
 service-type dvpn
local-user dvpn1spoke1
 password simple dvpn1spoke1
 level 3
 service-type dvpn
local-user dvpn1spoke2
 password simple dvpn1spoke2
 level 3
 service-type dvpn
local-user dvpn2hub1
 password simple dvpn2hub1
 level 3
 service-type dvpn
local-user dvpn2hub2
 password simple dvpn2hub2
 level 3
 service-type dvpn
local-user dvpn2spoke2
 password simple dvpn2spoke2
 level 3
 service-type dvpn
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 192.168.1.22 255.255.255.0
#
user-interface con 0
user-interface tty 97 102
user-interface aux 0
user-interface vty 0 4
#
```

HUB 1 配置

```
#
 sysname hub1
#
//配置IKE对等体
ike peer vam
 pre-shared-key abcde
#
//配置IPSec安全提议
ipsec proposal vam
 esp authentication-algorithm sha1
#
//配置IPSec安全框架
ipsec profile vamp
 pfs dh-group2
 //引用配置好的IKE 对等体
 ike-peer vam
 //引用配置好的IPSec安全提议
 proposal vam
 sa duration traffic-based 600
#
//创建VPN域1的客户端dvpn1hub1
vam client name dvpn1hub1
 client enable
 //配置VAM Server 的IP
 server primary ip-address 192.168.1.22
 user dvpn1hub1 password simple dvpn1hub1
 vpn 1
 //配置VAM Client 的预共享密钥
 pre-shared-key simple 123
#
//创建VPN域2的客户端dvpn2hub1
vam client name dvpn2hub1
 client enable
 server primary ip-address 192.168.1.22
 user dvpn2hub1 password simple dvpn2hub1
 vpn 2
 pre-shared-key simple 456
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
#
//配置VPN域1的隧道接口Tunnel1
interface Tunnel1
 ip address 10.0.1.1 255.255.255.0
 tunnel-protocol dvpn udp
 source GigabitEthernet0/0
 ospf network-type broadcast
 vam client dvpn1hub1
 ipsec profile vamp
#
//配置VPN域2的隧道接口Tunnel2
interface Tunnel2
 ip address 10.0.2.1 255.255.255.0
 tunnel-protocol dvpn udp
 source GigabitEthernet0/0
 ospf network-type broadcast
 vam client dvpn2hub1
 ipsec profile vamp
#
//配置公网路由
ospf 100
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
//配置私网路由
ospf 200
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
#
ospf 300
 area 0.0.0.0
  network 10.0.2.0 0.0.0.255
#
```

HUB 2 配置

```
#
 sysname hub2
#
//配置IKE对等体
ike peer vam
 pre-shared-key abcde
#
//配置IPSec安全提议
ipsec proposal vam
 esp authentication-algorithm sha1
#
//配置IPSec安全框架
ipsec profile vamp
 pfs dh-group2
 //引用配置好的IKE 对等体
 ike-peer vam
 //引用配置好的IPSec安全提议
 proposal vam
 sa duration traffic-based 600
#
//创建VPN域1的客户端dvpn1hub2
vam client name dvpn1hub2
 client enable
 server primary ip-address 192.168.1.22
 user dvpn1hub2 password simple dvpn1hub2
 vpn 1
 pre-shared-key simple 123
#
//创建VPN域2的客户端dvpn2hub2
vam client name dvpn2hub2
 client enable
 server primary ip-address 192.168.1.22
 user dvpn2hub2 password simple dvpn2hub2
 vpn 2
 pre-shared-key simple 456
#
interface Ethernet0/0
 port link-mode route
 ip address 192.168.1.2 255.255.255.0
#
//配置VPN域1的隧道接口Tunnel1
interface Tunnel1
 ip address 10.0.1.2 255.255.255.0
 tunnel-protocol dvpn udp
 source Ethernet0/0
 ospf network-type broadcast
 vam client dvpn1hub2
 ipsec profile vamp
#
//配置VPN域2的隧道接口Tunnel2
interface Tunnel2
 ip address 10.0.2.2 255.255.255.0
 tunnel-protocol dvpn udp
 source Ethernet0/0
 ospf network-type broadcast
 vam client dvpn2hub2
 ipsec profile vamp
#
//配置公网路由
ospf 100
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
//配置私网路由
ospf 200
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
#
ospf 300
 area 0.0.0.0
  network 10.0.2.0 0.0.0.255
#
```

Spoke 1 配置

```
#
 sysname spoke1
#
//配置IKE对等体
ike peer vam
 pre-shared-key abcde
#
//配置IPSec安全提议
ipsec proposal vam
 esp authentication-algorithm sha1
#
//配置IPSec安全框架
ipsec profile vamp
 pfs dh-group2
 ike-peer vam
 proposal vam
 sa duration traffic-based 600
#
//创建VPN域1的客户端dvpn1spoke1
vam client name dvpn1spoke1
 client enable
 server primary ip-address 192.168.1.22
 user dvpn1spoke1 password simple dvpn1spoke1
 vpn 1
 pre-shared-key simple 123
#
interface Ethernet0/0
 port link-mode route
 ip address 192.168.1.3 255.255.255.0
#
//配置VPN域1的隧道接口Tunnel1
interface Tunnel1
 ip address 10.0.1.3 255.255.255.0
 tunnel-protocol dvpn udp
 source Ethernet0/0
 ospf network-type broadcast
 vam client dvpn1spoke1
 ipsec profile vamp
#
ospf 100
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
ospf 200
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
#
```

Spoke 2 配置

```
#
 sysname spoke2
#
//配置IKE对等体
ike peer vam
 pre-shared-key abcde
#
//配置IPSec安全提议
ipsec proposal vam
 esp authentication-algorithm sha1
#
//配置IPSec安全框架
ipsec profile vamp
 pfs dh-group2
 ike-peer vam
 proposal vam
 sa duration traffic-based 600
#
//创建VPN域1的客户端dvpn1spoke2
vam client name dvpn1spoke2
 client enable
 server primary ip-address 192.168.1.22
 user dvpn1spoke2 password simple dvpn1spoke2
 vpn 1
 pre-shared-key simple 123
#
//创建VPN域2的客户端dvpn2spoke2
vam client name dvpn2spoke2
 client enable
 server primary ip-address 192.168.1.22
 user dvpn2spoke2 password simple dvpn2spoke2
 vpn 2
 pre-shared-key simple 456
#
interface Ethernet0/0
 port link-mode route
 ip address 192.168.1.4 255.255.255.0
#
//配置VPN域1的隧道接口Tunnel1
interface Tunnel1
 ip address 10.0.1.4 255.255.255.0
 tunnel-protocol dvpn udp
 source Ethernet0/0
 ospf network-type broadcast
 vam client dvpn1spoke2
 ipsec profile vamp
#
//配置VPN域2的隧道接口Tunnel2
interface Tunnel2
 ip address 10.0.2.4 255.255.255.0
 tunnel-protocol dvpn udp
 source Ethernet0/0
 ospf network-type broadcast
 vam client dvpn2spoke2
 ipsec profile vamp
#
ospf 100
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
ospf 200
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
#
ospf 300
 area 0.0.0.0
  network 10.0.2.0 0.0.0.255
#
```

四、**配置关键点**:

1) DVPN在V5平台上的实现与V3平台有极大的区别，配置命令改变较大，在V3平台上支持的是DVPN第一期，而在V5平台上支持的是DVPN第二期；

2) 本例中将AAA Server和VAM集中在同一台MSR上，在实际应用中可以使用单独的设备作为AAA Server，具体配置方法可参考操作手册安全一章；

五、验证

1）通过命令dis vam server address-map all可以查看注册到VAM Server上的设备信息，确保所有的HUB和Spoke都正常注册到VAM Sever；

```
<VAMSERVER>dis vam server address-map all
 VPN name:  1
 Total address-map number:  4
 Private-ip     Public-ip       Type       Holding time
 10.0.1.1       192.168.1.1     Hub        0H 22M  8S
```

10.0.1.2 192.168.1.2 Hub 0H 37M 0S
10.0.1.3 192.168.1.3 Spoke 0H 29M 11S
10.0.1.4 192.168.1.4 Spoke 0H 22M 51S
VPN name: 2
Total address-map number: 3
Private-ip Public-ip Type Holding time
10.0.2.1 192.168.1.1 Hub 0H 22M 8S
10.0.2.2 192.168.1.2 Hub 0H 36M 45S
10.0.2.4 192.168.1.4 Spoke 0H 22M 50S

2）在HUB设备设备使用命令dis dvpn session all可以看到所有建立好的隧道信息；

<hub1>dis dvpn session all
Interface: Tunnel1 VPN name: 1 Total number: 3
Private IP: 10.0.1.2
Public IP: 192.168.1.2
Session type: Hub-Hub
State: SUCCESS
Holding time: 0h 12m 1s
Input: 101 packets, 100 data packets, 1 control packets
87 multicasts, 0 errors
Output: 106 packets, 99 data packets, 7 control packets
87 multicasts, 10 errors
Private IP: 10.0.1.4
Public IP: 192.168.1.4
Session type: Hub-Spoke
State: SUCCESS
Holding time: 0h 22m 39s
Input: 183 packets, 182 data packets, 1 control packets
157 multicasts, 0 errors
Output: 186 packets, 185 data packets, 1 control packets
155 multicasts, 0 errors
Private IP: 10.0.1.3
Public IP: 192.168.1.3
Session type: Hub-Spoke
State: SUCCESS
Holding time: 0h 8m 7s
Input: 164 packets, 163 data packets, 1 control packets
54 multicasts, 0 errors
Output: 77 packets, 76 data packets, 1 control packets
55 multicasts, 0 errors
Interface: Tunnel2 VPN name: 2 Total number: 2
Private IP: 10.0.2.2
Public IP: 192.168.1.2
Session type: Hub-Hub
State: SUCCESS
Holding time: 0h 12m 4s
Input: 97 packets, 96 data packets, 1 control packets
84 multicasts, 0 errors
Output: 100 packets, 93 data packets, 7 control packets
80 multicasts, 10 errors
Private IP: 10.0.2.4
Public IP: 192.168.1.4
Session type: Hub-Spoke
State: SUCCESS
Holding time: 0h 22m 40s
Input: 165 packets, 164 data packets, 1 control packets
151 multicasts, 0 errors
Output: 162 packets, 161 data packets, 1 control packets
148 multicasts, 0 errors

3）在Spoke1设备上使用命令dis dvpn session all可以看到所有建立好的隧道信息，这时候所有的隧道都是静态隧道，还没有动态隧道；

<spoke1>dis dvpn session all
Interface: Tunnel1 VPN name: 1 Total number: 2
Private IP: 10.0.1.1
Public IP: 192.168.1.1

```
  Session type:   Spoke-Hub
  State:  SUCCESS
  Holding time: 0h 9m 57s
  Input:  88 packets,  87 data packets,  1 control packets
          66 multicasts,  0 errors
  Output: 197 packets,  196 data packets,  1 control packets
          65 multicasts,  0 errors
  Private IP:     10.0.1.2
  Public IP:      192.168.1.2
  Session type:   Spoke-Hub
  State:  SUCCESS
  Holding time: 0h 9m 57s
  Input:  78 packets,  77 data packets,  1 control packets
          62 multicasts,  0 errors
  Output: 80 packets,  79 data packets,  1 control packets
          65 multicasts,  0 errors
```

如果Ping Spoke 2的tunnle地址后在使用上述命令，会发现多出一条动态的隧 道信息，如下红色字体部分；

```
<spoke1>ping 10.0.1.4
  PING 10.0.1.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.4: bytes=56 Sequence=1 ttl=254 time=6 ms
    Reply from 10.0.1.4: bytes=56 Sequence=2 ttl=255 time=3 ms
    Reply from 10.0.1.4: bytes=56 Sequence=3 ttl=255 time=3 ms
    Reply from 10.0.1.4: bytes=56 Sequence=4 ttl=255 time=3 ms
    Reply from 10.0.1.4: bytes=56 Sequence=5 ttl=255 time=3 ms
  --- 10.0.1.4 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/6 ms
<spoke1>dis dvpn session all
 Interface: Tunnel1  VPN name: 1  Total number: 3
  Private IP:     10.0.1.1
  Public IP:      192.168.1.1
  Session type:   Spoke-Hub
  State:  SUCCESS
  Holding time: 0h 17m 57s
  Input:  143 packets,  142 data packets,  1 control packets
          114 multicasts,  0 errors
  Output: 347 packets,  346 data packets,  1 control packets
          113 multicasts,  0 errors
  Private IP:     10.0.1.2
  Public IP:      192.168.1.2
  Session type:   Spoke-Hub
  State:  SUCCESS
  Holding time: 0h 17m 57s
  Input:  131 packets,  130 data packets,  1 control packets
          110 multicasts,  0 errors
  Output: 134 packets,  132 data packets,  2 control packets
          113 multicasts,  0 errors
  Private IP:     10.0.1.4
  Public IP:      192.168.1.4
  Session type:   Spoke-Spoke
  State:  SUCCESS
  Holding time: 0h 0m 3s
  Input:  5 packets,  4 data packets,  1 control packets
          0 multicasts,  0 errors
  Output: 5 packets,  4 data packets,  1 control packets
          0 multicasts,  0 errors
```