第 10 章

隧道技术

本章将讨论 CCIE 路由和交换考试要求掌握的各种 VPN（Virtual Private Network，虚拟专用网）技术。这些 VPN 技术的种类很多，掌握这些 VPN 技术必须了解与之相对应的各种认证或加密特性。本章将重点讨论部署这些基本功能特性所需的配置技巧，这些都属于实验考试的一部分。

请注意，本章在讨论每种 VPN 技术的时候，都尽量不过多的扩展安全方面的细节信息。

10.1 “我已经知道了吗？”测试题

表 10-1 列出了本章的基本主题以及与之相应的测试题。

表 10-1 “我已经知道了吗？”基本主题与测试题对照表

基本主题	测试题
DMVPN	1～3
IPv6 隧道	4
二层 VPN	5～7
GET VPN	8～9
得分	

为了提高每章前面的测试评价效果，请务必严格评分。参考答案请参见附录 A。

1. DMVPN 的主要优势在于允许传统的星型网络设计更好地支持下列哪种功能特性？
   a. 包传输
   b. 扩展性
   c. 服务质量
   d. 流量整形
2. 虽然支持 DMVPN 解决方案的协议有很多，但稳定的 DMVPN 环境完全依赖于多项 Cisco 增强型技术，请选出这些正确的技术。
   a. GRE（Generic Routing Encapsulation，通用路由封装）协议
   b. FHRP（First-Hop Redundancy Protocol，第一跳冗余协议）
   c. NHRP（Next-Hop Resolution Protocol，下一跳解析协议）

d. 动态路由协议
e. 安全 DMVPN
f. IPSec 加密协议

3. 中心路由器可以向分支路由器发送哪种类型的新消息，使得分支路由器能够知道有比经过中心路由器更好的路径到达其他分支路由器？
   a. ICMP 重定向
   b. 代理 ARP
   c. NHRP 重定向
   d. 本地代理 ARP

4. 对于 **ipv6ip auto-tunnel** 来说，利用隧道接口地址的哪个部分可以自动确定与 IPv4 兼容的隧道目的地址？
   a. 高阶 32 比特
   b. 低阶 16 比特
   c. 高阶 16 比特
   d. 低阶 32 比特

5. L2VPN 是一种允许客户端管理下列哪种网络功能特性的最简单的解决方案？
   a. 路由协议
   b. 监管策略
   c. QoS 机制
   d. IOS 管理协议
   e. IP 管理

6. 下列命令的输出结果表明与 DMVPN 配置相关联的状态是什么？

```
R2# show xconnect all

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware
XC ST Segment 1 S1 Segment 2 S2
------+---------------------------------+--+---------------------------------
+--
DN ac Fa0/0(Ethernet) AD mpls 4.4.4.4:204 DN
```

   a. 伪线链路处于 up 状态
   b. 伪线链路处于管理性 down 状态
   c. 伪线链路处于 down 状态
   d. 伪线链路处于正常运行状态

7. MPLS 二层伪线使用的两个主要段是什么？
   a. 段 1
   b. 段 A

c. 段 B
d. 段 1-2
e. 段 2

8. DMVPN 解决方案中的密钥服务器最重要的功能就是生成加密密钥，该进程将生成哪两种密钥？
   a. RSA
   b. TEK
   c. SHA1
   d. TLS
   e. KEK
9. 配置 DMVPN 组成员时，需要利用 IPSec 配置简档（Profile）来创建加密策略，那么将使用下面哪个工具来标识需要加密的数据包？
   a. ip prefix-list
   b. PACL
   c. ACL
   d. VACL

基本主题

10.2 GRE 隧道

GRE 定义了从一台路由器到另一台路由器的数据隧道化方法。为了实现流量的隧道化传输，发送路由器需要将一种网络协议（称为乘客协议）的数据包封装到另一种协议（称为传输协议）中，然后再将封装后的数据包传输到另一台路由器，接收路由器负责解封装并转发原始乘客协议的数据包。该进程允许网络中的路由器转发中间路由器可能不支持的流量。例如，如果某些路由器不支持 IP 多播，那么就可以利用 IP 单播包将 IP 多播流量从一台路由器隧道化传输到另一台路由器。

GRE 隧道可以完成多种任务。从网络角度来看，可以将 GRE 隧道流量视为 GRE 流量，也就是说，不是 IP 单播流量、多播流量、IPSec 流量或者其他被封装的任何流量，因而可以利用 GRE 隧道化可能无法在网络中传输的流量。例如，将 IP 多播流量封装到 GRE 隧道中之后，就可以通过不支持多播的网络传输这些多播流量。

GRE 隧道也可以用来封装流量，使得隧道内的流量不感知网络拓扑结构。无论源端与目的端之间的网络跳数是多少，穿越 GRE 隧道的流量都仅将其视为一跳。由于隧

道可以隐藏网络的拓扑结构，因而穿越网络的实际流量路径对于隧道内部的流量来说并不重要。如果源地址和目的地址使用的是环回地址，那么只要这两个环回地址之间存在可用路由，隧道就能够为源端和目的端提供连接性，即便出站接口处于中断状态，流量依然能够通过隧道进行传输。

IPSec VTI（Virtual Tunnel Interface，虚拟隧道接口）是一种终结 IPSec 隧道的可路由接口，可以很容易地为站点之间定义保护机制。VTI 可以简化远程链路的 IPSec 保护配置、简化网络管理并支持多播，而且 IPSec VTI 还能加强物理接口收发 IP 单播及多播加密流量的灵活性。出于 CCIE 考试的目的，必须理解 VTI 的作用，并掌握利用包括 GRE、L2VPN（Layer 2 Virtual Private Network，二层虚拟专用网）以及 MPLS（Multiprotocol Label Switching，多协议标签交换）在内的各种隧道机制配置 VTI 的方式。

请注意，必须将路由器配置为能够通过隧道传输期望流量，通常利用静态路由将流量指向隧道接口即可。

例 10-1 给出了两台路由器的常见隧道配置示例。这两台路由器都将环回接口作为流量的源端，并指向对端环回接口。同时还为这些路由器的环回接口分配了新子网中的 IP 地址。

例 10-1 GRE 隧道配置

```
R2# show run int lo0
interface Loopback0
ip address 150.1.2.2 255.255.255.0
R2# show run int tun0
  interface Tunnel0
  ip address 192.168.201.2 255.255.255.0
  tunnel source Loopback0
  tunnel destination 150.1.3.3
! Now on to R3:
R3# show run int lo0
interface Loopback0
ip address 150.1.3.3 255.255.255.128
R3# show run int tun0
interface Tunnel0
 ip address 192.168.201.3 255.255.255.0
 tunnel source Loopback0
 tunnel destination 150.1.2.2
R3# show ip interface brief
Interface              IP-Address      OK? Method Status      Protocol
Serial0/2              144.254.254.3   YES TFTP up            up
Serial0/3              unassigned      YES NVRAM up           down
Virtual-Access1        unassigned      YES unset up           up
Loopback0              150.1.3.3       YES NVRAM up           up
Tunnel0                192.168.201.3   YES manual up          up
```

10.2.1 DMVPN 隧道

事实证明，基于 VPN 的安全架构对于现代分布式基础设施来说非常有用。由于网络需求在不断变化，通过各种介质（很多情况下都像 Internet 一样）将敏感数据从一点传输到另一点时难以保证其安全性，当然保护数据安全性的相关工具也在不断发展演进。

技术演进并不是推动网络架构优化的唯一外部动因。作为网络工程师，必须经常研究各种网络功能的传统实现方式，分析这些方法是否能够满足企业的效率与扩展性需求。通常都采用基于 IPSec 的星型部署模型。虽然该解决方案在数十年来已经为站点到站点的网络提供了良好的互连架构，但依然应该常常分析是否能够真正满足企业的需求。事实表明过去的传统解决方案已经越来越难以满足大型企业网的需求，这些大型企业网需要部署可扩展的动态解决方案，通过 IPSec 等动态功能特性经广域网拓扑进行信息的安全传输，通过降低延迟、提高带宽利用率来优化网络性能。

DMVPN（Dynamic Multipoint VPN，动态多点 VPN）技术就是这样的功能特性。DMVPN 可以为分布式网络基础设施提供非常好的扩展能力。从本质上来说，可扩展性能够帮助网络实现简便的扩展能力，从而充分发挥网络基础设施的潜力。

1. DMVPN 概述

DMVPN 的主要优势在于能够提高传统星型网络架构的扩展性。这种实现更大服务容量的增强型能力可以为多站点间的流量交换提供更小的延迟和更优的性能。虽然这种增强能力很简单，但是却能带来如下好处：

- 跨星型拓扑结构的动态隧道；
- 提升网络性能；
- 降低延迟，为“实时应用”提供显著的优化效果；
- 简化路由器配置；
- 可以在不修改中心路由器配置的情况下（“零接触”）为新站点动态添加更多的隧道；
- 减少丢包的动态 IPSec 加密能力；
- 能够在旁路中心站点的情况下动态创建站点间的“分支到分支”隧道（站点间通信）；
- 可以在单条或所有隧道上支持路由协议；
- 支持多播流量；
- 感知 VRF（Virtual Routing and Forwarding，虚拟路由和转发）；
- 支持 MPLS；

- 支持负载均衡；
- 网络出现故障后能够自动重路由流量。

长期困扰分布式网络部署模型的主要因素包括站点的地理位置隔离以及在站点间传输数据的互连链路“速度慢”，当然还有其他困扰因素，如网络可用性以及安全通信等。DMVPN 是解决这类问题的优选方案，因为 DMVPN 不但安全，而且还具备优异的扩展性和自愈能力。

2. DMVPN 组件

虽然 DMVPN 解决方案涉及多种协议，但 DMVPN 环境的稳定运行在很大程度上完全取决于 Cisco 提供的以下增强型技术：

- GRE 协议；
- NHRP；
- 动态路由协议；
- IPSec 加密协议。

3. DMVPN 操作

DMVPN 的主要操作就是创建动态隧道叠加网络，此时每个分支路由器都成为一个永久的去往中心路由器的 IPSec 隧道。需要记住的是，该应用场景下的分支路由器之间并不建立隧道。为了保证隧道创建过程的可靠性，拓扑结构中的所有分支路由器都必须知道中心路由器的地址。有了地址信息之后，分支路由器就可以将自己的实际地址作为客户端注册到运行在中心路由器上的 NHRP 服务器进程。该 NHRP 服务器负责维护每台分支路由器在注册进程中使用的所有公用接口地址的数据库。如果分支路由器需要将数据包发送给其他分支路由器上目的端（对于本例来说，该目的端是私有地址），那么就会请求 NHRP 服务器提供对端分支设备的公有（外部）地址，从而创建一条直达隧道。有了 NHRP 服务器之后，就不再需要通过动态路由协议去发现到达分支路由器的路由了。虽然我们在前文中提到了动态路由协议，但这些路由协议仅在分支路由器与中心路由器之间创建连接性。

分支路由器获得目的端设备（分支路由器）的对等体地址之后，就可以向目标发起一条动态 IPSec 隧道，从而在 DMVPN 拓扑结构之上创建一条动态的分支到分支的隧道。这类隧道都是按需建立的，也就是说在分支路由器之间需要转发流量时才建立这些隧道。成功建立了隧道之后，分支路由器之间就可以直接转发流量，而不再通过中心路由器。

为了更清楚地解释上述进程，下面将通过命令行来解释 DMVPN 的部署方式，分析该功能特性建议的三阶段部署方案。

DMVPN 阶段 1 将建立一个简单的星型拓扑结构，此时分支路由器使用的都是动

态 IP 地址（如例 10-2 所示）。

例 10-2 采用动态 IP 地址的简单星型拓扑结构

```
!First we need ISAKMP Policy with pre-shared key configured. Note that in DMVPN we
!need to configure so-called "wildcard PSK" because there may be many peers. This
!is why a more common solution in DMVPN is to use certificates and PKI.

R1(config)# crypto isakmp policy 1
R1(config-isakmp)# encr 3des
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
R1(config)# crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R1(cfg-crypto-trans)# mode transport

!The "mode transport" is used for decreasing IPSec packet size (an outer IP header
!which is present in tunnel mode is not added in the transport mode).

R1(cfg-crypto-trans)# crypto ipsec profile DMVPN
R1(ipsec-profile)# set transform-set TSET
R1(ipsec-profile)# exi

!There is only one interface Tunnel on every DMVPN router. This is because we use
!GRE \ multipoint type of the tunnel.

R1(config)# interface Tunnel0
R1(config-if)# ip address 172.16.145.1 255.255.255.0
R1(config-if)# ip mtu 1400

!Maximum Transmission Unit is decreased to ensure that DMVPN packet would not
!exceed IP MTU set on non-tunnel IP interfaces - usually a 1500 bytes (When
!"transport mode" isused then DMVPN packet consists of original IP Packet, GRE
!header, ESP header and outer IPSec IP header. If original IP packet size is close
!to the IP MTU set on real IP interface then adding GRE and IPSec headers may lead
!to exceeding that value)

R1(config-if)# ip nhrp authentication cisco123
R1(config-if)# ip nhrp map multicast dynamic
R1(config-if)# ip nhrp network-id 12345

!The Hub works as NHS (Next Hop Server). The NHRP configuration on the Hub is
!straight forward. First, we need NHRP network ID to identify the instance and
!authenticate key to secure NHRP registration. There is a need for NHRP static
!mapping on the Hub. The Hub must be able to send down all multicast traffic so
!that dynamic routing protocols can distribute routes between spokes. The line "ip
!nhrp map multicast dynamic" simply tells the NHRP server to replicate all multi
!cast traffic to all dynamic entries in the NHRP table (entries with flag
!"dynamic").

R1(config-if)# no ip split-horizon eigrp 145
!Since we use EIGRP between the Hub and the Spokes, we need to disable Split Horizon
!for that protocol to be able to send routes gathered from one Spoke to the other
!Spoke. The Split Horizon rule says: "information about the routing is never sent
!back in the direction from which it was received". This is basic rule for loop
!prevention.

R1(config-if)# tunnel source FastEthernet0/0
R1(config-if)# tunnel mode gre multipoint
```

```
R1(config-if)# tunnel key 12345
R1(config-if)# tunnel protection ipsec profile DMVPN

!A regular GRE tunnel usually needs source and destination of the tunnel to be
!specified. However in the GRE multipoint tunnel type, there is no need for a
!destination. This is because there may be many destinations, as many Spokes are
!out there. The actual tunnel destination is derived form NHRP database. The tunnel
!has a key for identification purposes, as there may be many tunnels on one
!router and the router must know what tunnel the packet is destined to.
```

DMVPN 阶段 2 将部署一个新功能特性，通过 DMVPN 网络实现分支路由器之间的直接通信。对于企业来说，如果分支机构之间有通信需求且希望减轻中心站点的压力，那么该功能特性将非常有用。例 10-3 给出了使用 EIGRP（Enhanced Interior Gateway Routing Protocol，增强型内部网关路由协议）的 DMVPN 阶段 2 的配置示例。理解并掌握 DMVPN 解决方案中使用不同路由协议时的区别非常重要，必须配置并调整这些路由协议以保证其工作在最佳扩展性且最高效率的状态下，但每种路由协议都有其不足之处。

例 10-3 存在分支到分支连接的星型拓扑结构

```
R1(config)# crypto isakmp policy 1
R1(config-isakmp)# encr 3des
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
R1(config)# crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R1(cfg-crypto-trans)# mode transport
R1(cfg-crypto-trans)# crypto ipsec profile DMVPN
R1(ipsec-profile)# set transform-set TSET
R1(ipsec-profile)# exi
R1(config)# interface Tunnel0
R1(config-if)# ip address 172.16.145.1 255.255.255.0
R1(config-if)# ip mtu 1400
R1(config-if)# ip nhrp authentication cisco123
R1(config-if)# ip nhrp map multicast dynamic
R1(config-if)# ip nhrp network-id 12345
R1(config-if)# no ip split-horizon eigrp 145
R1(config-if)# no ip next-hop-self eigrp 145

!The difference is in routing protocol behavior. The DMVPN Phase 2 allows for
!direct Spoke to Spoke communication. Hence, one spoke must send the traffic to the
!other spoke using its routing table information. In DMVPN Phase 1 the spoke sends
!all traffic up to the Hub and uses the Hub for Spoke to Spoke communication. How
!ever,in DMVPN Phase 2 a spoke must point to the other spoke directly.

!This is achieved by changing the routing protocol behavior. The EIGRP changes next
!hop in the routing update when sending it further so that, the Hub changes the
!next hop to itself when sending down the routing updates to the Spokes. This
!behavior can be changed by the command "no ip next-hop-self eigrp AS".

R1(config-if)# tunnel source FastEthernet0/0
R1(config-if)# tunnel mode gre multipoint

!Note that in DMVPN Phase 2 the Hub is in GRE Multipoint mode as it was in Phase 1.
```

```
R1(config-if)# tunnel key 12345
R1(config-if)# tunnel protection ipsec profile DMVPN
R1(config-if)# exi
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config)# router eigrp 145
R1(config-router)# network 172.16.145.0 0.0.0.255
R1(config-router)# network 192.168.1.0
R1(config-router)# no auto-summary
R1(config-router)# exi
```

完成上述配置之后，可以通过多种命令来验证上述配置信息（如例 10-4 所示）。

例 10-4　验证 DMVPN

```
R1# sh crypto ipsec sa
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.1.12.1
protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.12.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.24.4/255.255.255.255/47/0)
current_peer 10.1.24.4 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 19, #pkts encrypt: 19, #pkts digest: 19
#pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

!The traffic is going through the tunnel between the Hub and the Spoke. This traffic
!is an EIGRP updates as we have not initiated any traffic yet.

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.24.4
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x49DC5EAF(1239178927)
inbound esp sas:
spi: 0xF483377E(4102240126)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2003, flow_id: NETGX:3, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4524624/3565)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x49DC5EAF(1239178927)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2004, flow_id: NETGX:4, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4524622/3565)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
outbound ah sas:
outbound pcp sas:
```

```
protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.12.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.25.5/255.255.255.255/47/0)
current_peer 10.1.25.5 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 17, #pkts encrypt: 17, #pkts digest: 17
#pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

!The traffic is going through the tunnel between the Hub and the Spoke. This traffic
!is an EIGRP update as we have not initiated any traffic yet.

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.25.5
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x1FB68E8D(532057741)
inbound esp sas:
spi: 0xE487940A(3834090506)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4411380/3563)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x1FB68E8D(532057741)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4411379/3563)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
outbound ah sas:
outbound pcp sas:
```

Cisco 在 DMVPN 阶段 3 解决了阶段 2 存在的一些不足之处，特别是扩展性和性能问题。例 10-5 解释了该 DMVPN 进程的部署方式。

- 阶段 2 允许中心路由器菊花链、OSPF（Open Shortest Path First，开放最短路径优先）单区域以及有限数量的中心路由器（因为 OSPF DR/DBR 选举进程）。
- 扩展性：阶段 2 不允许在中心路由器上执行路由汇总操作，必须将所有前缀都分发给所有分支路由器，这样才能建立分支到分支的直达隧道。
- 性能：阶段 2 使用进程交换机制（而不是 CEF[Cisco Express Forwarding，Cisco 快速转发]）通过中心路由器发送第一个数据包，因而会出现 CPU 尖峰。
- DMVPN 阶段 3 通过以下两种 NHRP 增强技术解决了阶段 2 存在的上述问题。
  - **NHRP 重定向（NHRP Redirect）**：是一种由中心路由器发送给分支路由器的新消息，其作用是让分支路由器知道有比经过中心路由器去往其他分支

路由器更优的路由。

- **NHRP 捷径（NHRP Shortcut）**：在分支路由器上更改（改写）CEF 信息的一种新形式。

例 10-5 DMVPN 阶段 3

```
R2(config)# crypto isakmp policy 10
R2(config-isakmp)# encr 3des
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)# crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
R2(config)# crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R2(cfg-crypto-trans)# mode transport
R2(cfg-crypto-trans)# crypto ipsec profile DMVPN
R2(ipsec-profile)# set transform-set TSET
R2(ipsec-profile)# exi
R2(config)# int Tunnel0
R2(config-if)# ip address 172.16.245.2 255.255.255.0
R2(config-if)# ip mtu 1400
R2(config-if)# ip nhrp authentication cisco123
R2(config-if)# ip nhrp map multicast dynamic
R2(config-if)# ip nhrp network-id 123
R2(config-if)# ip nhrp redirect

!NHRP Redirect is a special NHRP message sent by the Hub to the spoke to tell the
!spoke that there is a better path to the remote spoke than through the Hub. All
!it does is enforces the spoke to trigger an NHRP resolution request to IP
!destination. The "ip nhrp redirect" command should be configured on the Hub only.

R2(config-if)# tunnel source s0/1/0
R2(config-if)# tunnel mode gre multipoint
R2(config-if)# tunnel key 123
R2(config-if)# tunnel protection ipsec profile DMVPN
R2(config-if)# no ip split-horizon eigrp 245
Note that we do not need "no ip next-hop-self eigrp" command in the DMVPN Pahse 3.
R2(config-if)# exi
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config)# router eigrp 245
R2(config-router)# no auto
R2(config-router)# net 172.16.245.2 0.0.0.0
R2(config-router)# net 192.168.2.2 0.0.0.0
R2(config-router)# exi
```

10.2.2 IPv6 隧道及其相关技术

虽然从 20 世纪 90 年代开始，IPv6 就在全球范围内得到了逐步部署，但目前的绝大多数网络仍然建立在 IPv4 基础设施之上。因而如大家所预料的那样，很多组织机构都意识到必须采取某些方式通过 IPv4 网络传输 IPv6 流量，反之亦然。

采用隧道技术的根本原因就在于目前的 Internet 基于 IPv4，但是至少有两个重要的学术与研究网络正在使用纯 IPv6，因而必须提供某种机制以允许这些网络上的主机能够通过 IPv4 Internet 到达对端，而隧道技术就是支持该通信场景的一种实现方式。

正如大家所预期的那样，隧道技术能够满足 IPv4 与 IPv6 混合场景的很多需求，因而出现了大量隧道方法与技术。本节将介绍一些最常用的隧道技术。

1. 隧道概述

从本质上来说，隧道化就是封装数据流量。具体而言，术语隧道化通常指的是在 OSI 七层参考模型的给定层将流量封装到运行在同一层的其他协议中的过程，因而将 IPv6 数据包封装到 IPv4 数据包中以及将 IPv4 数据包封装到 IPv6 数据包中都属于隧道化过程。

由于本书的目的是满足 CCIE 路由和交换考试的需求，因而本节将主要讨论如何通过 IPv4 网络承载 IPv6，而不考虑如何通过 IPv6 网络承载 IPv4，而且也不讨论将 IPv6 封装到 IPv6 的隧道化方法，但大家必须知道确实存在这两种隧道化方式。在讨论这些隧道化方法之前，首先看一下表 10-2 的汇总信息。

表 10-2 隧道化方法汇总

隧道模式	拓扑结构和地址空间	应用
自动 6to4（Automatic 6to4）	点到多点；地址空间为 2002::/16	连接相互隔离的 IPv6 孤岛网络
手工配置	点到点；任意地址空间；要求两端均支持双栈	通过 IPv4 网络承载 IPv6 数据包
IPv6 over IPv4 GRE	点到点；单播地址；要求两端均支持双栈	承载 IPv6、CLNS 以及其他流量
ISATAP	点到多点；任意多播地址	用于在单个站点内连接 IPv6 主机
自动 IPv4 兼容隧道（Automatic IPv4-Compatible Tunnels）	点到多点；地址空间为::/96；要求两端均支持双栈	已被废弃，Cisco 建议使用 ISATAP（Intra-Site Automatic Tunnel Addressing Protocol，站点内自动隧道编址协议）隧道替代该隧道模式，本书不再过多描述

如果还不太熟悉 IPv4 隧道的部署方式，那么就可以看看以下基本配置步骤。

第 1 步：确保隧道端点之间的端到端 IPv4 可达性。

第 2 步：利用 **interface tunnel** *n* 命令创建隧道接口。

第 3 步：选择隧道源接口并利用 **tunnel source interface** { *interface-type-number* | *ip-address* }命令配置该接口。

第 4 步：对于非自动隧道类型来说，利用 **tunnel destination** { *ip-address* | *ipv6-address* | *hostname* }命令配置隧道目的端。如果使用参数 *hostname*，那么就需要 DNS（Domain Name System，域名系统）或本地主机的域名到 IP 地址映射。

第 5 步：配置隧道 IPv6 地址（或前缀，具体取决于隧道类型）。

第 6 步：利用 **tunnel mode** *mode* 命令配置隧道模式。

表 10-3 列出了本节讨论的隧道类型的 Cisco IOS 隧道模式以及相应的目的端。

表 10-3　　Cisco IOS 隧道模式及目的端

隧道类型	隧道模式	目的端
手工隧道	**ipv6ip**	IPv4 地址
GRE over IPv4 隧道	**gre ip**	IPv4 地址
自动 6to4 隧道	**ipv6ip 6to4**	自动确定
ISATAP 隧道	**ipv6ip isatap**	自动确定
自动 IPv4 兼容隧道	**ipv6ip auto-tunnel**	自动确定

下面将详细讨论通过 IPv4 网络承载 IPv6 流量的各种隧道方法。

2. 手工配置隧道

这种隧道的本质是点对点隧道。Cisco IOS 要求为这类隧道静态配置目的地址。手工配置 IPv6-over-IPv4 隧道的方式与配置 IPv4 GRE 隧道的方式非常相似，唯一的区别在于设置隧道模式。例 10-6 和图 10-1 给出了手工配置隧道的示例。请注意，本例已经配置并验证了 IPv4 的可达性，只是没有显示而已。

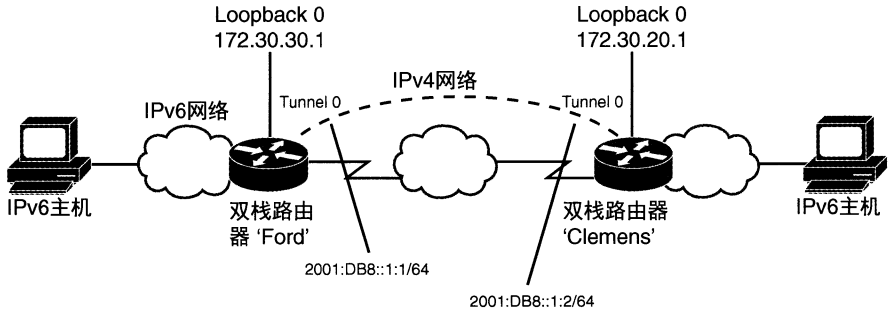

图 10-1　手工配置隧道

例 10-6　手工隧道配置

```
! In this example, Clemens and Ford are running IPv4 and OSPFv2 on their
! loopback 0 interfaces and the link that connects the two routers. This provides
! the IPv4 connectivity required for these tunnels to work.
!Configuration on the Ford router:
Ford# show run interface tunnel0
interface Tunnel0
 no ip address
 ipv6 address 2001:DB8::1:1/64
 tunnel source Loopback0
```

```
 ! In the tunnel destination, 172.30.20.1 is Clemens's Loopback0 interface:
 tunnel destination 172.30.20.1
 tunnel mode ipv6ip
Ford#
! Configuration on the Clemens router:
Clemens# show run interface tunnel0
interface Tunnel0
 no ip address
 ipv6 address 2001:DB8::1:2/64
 tunnel source Loopback0
! In the tunnel destination, 172.30.30.1 is Ford's Loopback0 interface:
 tunnel destination 172.30.30.1
 tunnel mode ipv6ip
! Demonstrating reachability across the tunnel:
Clemens# ping 2001:DB8::1:1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8::1:1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/36/40 ms
Clemens#
```

3. 自动 IPv4 兼容隧道

该类型的隧道为隧道接口使用与 IPv4 兼容的 IPv6 地址，这些地址来自::/96 地址空间，也就是说，隧道接口地址的前 96 个比特为全 0，剩下的 32 个比特来自 IPv4 地址。这类地址的书写形式为 0:0:0:0:0:0:A.B.C.D 或::A.B.C.D，其中的 A.B.C.D 表示 IPv4 地址。

IPv4 兼容隧道的隧道目的地址可以通过隧道接口地址的低阶 32 比特自动确定。如果要部署这类隧道，需要在隧道接口配置模式下使用 **tunnel mode ipv6ip auto-tunnel** 命令。

与 IPv4 兼容的 IPv6 编址应用范围并不广泛，这是因为这种方式与全球目前的 IPv6 地址空间使用方式并不相符，而且这种隧道方法也不具备可扩展性，因而 Cisco 建议使用 ISATAP 隧道来替代该隧道技术。出于以上原因，本书将不再继续讨论该隧道类型。

4. IPv6-over-IPv4 GRE 隧道

GRE 隧道可以提供其他隧道类型不具备的两种功能选项，即能够封装 IPv6 以及其他流量，而且还支持 IPSec。与手工配置隧道相似，GRE 隧道主要用于点到点应用场景。将 IPv6 作为乘客协议，通常在边缘路由器之间部署这类隧道，通过 IPv4 网络为 IPv6 孤岛提供连接性。

配置 GRE 隧道以通过 IPv4 网络传输 IPv6 数据包很简单。GRE 隧道与手工配置隧道之间的唯一区别就在于 **tunnel mode** 命令的语法形式，GRE 隧道使用的命令形式是 **tunnel mode gre ipv6**（如例 10-6 所示）。

5. 自动 6to4 隧道

与前面讨论过的两种隧道类型不同，自动 6to4 隧道本质上是点到多点隧道。这类隧道将底层的 IPv4 网络视为 NBMA（NonBroadcast MultiAccess，非广播多路接入）网络。

考试要点

对于自动 6to4 隧道来说，隧道操作方式是以每个数据包为单位将流量封装到正确的目的端，因而在本质上属于点到多点隧道。这些隧道确定目的地址的方式是将 IPv6 前缀与全局唯一的目的 6to4 边界路由器的 IPv4 地址组合在一起，以前缀 2002::/16 开头，具体格式如下：

2002:边界路由器的 IPv4 地址::/48

这种利用前缀生成目的地址的方法为给定站点内的网络编址留出了 64 比特前缀中的 16 比特。

Cisco IOS 在一台给定路由器上只能配置一条自动 6to4 隧道。自动 6to4 隧道的配置方式与前面讨论过的其他隧道配置方式相似，区别在于需要使用 **tunnel mode ipv6ip** 6to4 命令配置隧道模式，而且不用为 6to4 隧道显式配置隧道目的地址，这是因为 6to4 隧道确定每个数据包的目的前缀的方法完全是自动完成的。

除了基本的隧道配置之外，还需要其他配置步骤以通过隧道路由期望数据包。通常使用静态路由即可完成该工作。例如，如果希望通过 6to4 隧道接口 tunnel0 将数据包路由到前缀 2002::/16，那么就可以配置如下静态路由：

ipv6 route 2002::/16 tunnel 0

例 10-7 和图 10-2 给出了 6to4 隧道的配置示例以及该路由器与 6to4 隧道相关联的其他接口情况。请注意，本例中的快速以太网接口和隧道接口是从接口 Ethernet 0 的 IPv4 地址 10.1.100.1 得到前缀 2002: 0a01:6401 ::中的黑体部分的。为了保证隧道的正常工作，隧道源接口必须是连接外部网络的接口，即本例中的接口 Ethernet 2/0。此外，每个连接主机的快速以太网接口都是（也必须是）不同的 IPv6 子网（前缀为 2002:0a01:6401）。

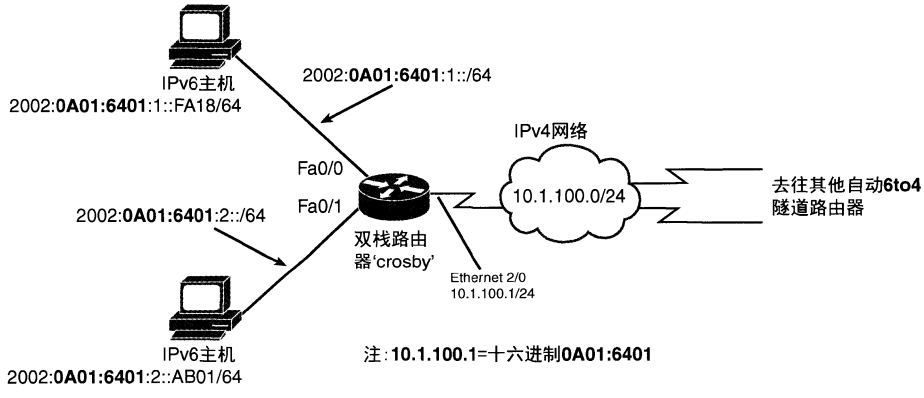

图 10-2 自动 6to4 隧道拓扑结构

例 10-7 自动 6to4 隧道配置

```
crosby# show running-config
! output omitted for brevity
interface FastEthernet0/0
 description IPv6 local host network interface 1 of 2
 ipv6 address 2002:0a01:6401:1::1/64
!
interface FastEthernet0/1
 description IPv6 local host network interface 2 of 2
 ipv6 address 2002:0a01:6401:2::1/64
!
interface Ethernet2/0
description Ethernet link to the outside world
 ip address 10.1.100.1 255.255.255.0
!
interface Tunnel0
 no ip address
 ipv6 address 2002:0a01:6401::1/64
 tunnel source Ethernet 2/0
 tunnel mode ipv6ip 6to4
!
ipv6 route 2002::/16 tunnel 0
```

6. ISATAP 隧道

ISATAP 定义在 RFC 4214 中。与 6to4 隧道相似，ISATAP 隧道也将底层 IPv4 网络视为 NBMA 网络，因而与 6to4 相似，ISATAP 隧道在本质上也支持点到多点操作，而且也根据每个数据包来确定目的地址。但 ISATAP 确定主机和隧道接口地址的方法与 6to4 隧道不同，否则 ISATAP 隧道就与自动 6to4 隧道完全相同了。

ISATAP 使用如下地址格式来确定其编址方案：

[64 比特链路本地或全局单播前缀]:0000:5EFE:[ISATAP 链路的 IPv4 地址]

ISATAP 接口标识符是地址的中间部分 0000:5EFE。

举例来说，假设 IPv6 前缀是 2001:0DB8:0ABC:0DEF::/64，IPv4 隧道目的地址是 172.20.20.1，将 IPv4 地址转换为十六进制形式则为 AC14:1401，因而 ISATAP 地址为：

2001:0DB8:0ABC:0DEF:0000:5EFE:AC14:1401

在路由器上配置 ISATAP 隧道的方式与前面讨论过的隧道类型存在少量差异，ISATAP 隧道需要使用不同的隧道模式（**ipv6ip isatap**），而且还必须配置成使用 EUI-64 方法生成 IPv6 地址。隧道接口上的 EUI-64 编址方式与非隧道接口上的 EUI-64 编址方式不同，因为此时需要从隧道源接口的 IPv4 地址生成接口 ID 的最后 32 比特。该方法对于 ISATAP 隧道来说是必需的，因为该机制可以让其他隧道路由器知道如何到达该路由器。

ISATAP 隧道还有一个非常关键的不同之处，隧道接口默认禁用 RA（Router Advertisement，路由器宣告），但是必须在 ISATAP 隧道上启用 RA 以支持客户端的自动配置。利用 **no ipv6 nd suppress-ra** 命令即可在 ISATAP 隧道上启用 RA。

7. SLAAC 与 DHCPv6

DHCPv6（Dynamic Host Configuration Protocol for IPv6，用于 IPv6 的动态主机配置协议）是一种上层协议，可以实现 IPv6 地址的动态分配。与 IPv4 相比，IPv6 更加复杂，也提供了更多的可选项。DHCPv6 不但可以提供状态化 DHCP 服务，而且还可以提供 SLAAC（Stateless Address Autoconfiguration，无状态地址自动配置）服务。SLAAC 定义在 RFC 4862（IPv6 Stateless Address Autoconfiguration）中。SLAAC 不需要 DHCP 服务器的服务。在某些情况下，SLAAC 仅包含路由器以及 RA 消息，但对于其他场景来说，可能不但需要 RA 消息，而且还需要从 DHCP 服务器获得其他配置参数。SLAAC 可以在无 DHCP 服务的情况下实现动态编址功能。

8. NAT-PT

从技术上来说，NAT-PT（Network Address Translation–Protocol Translation，网络地址转换-协议转换）并不是隧道技术，而是一种互连 IPv6 与 IPv4 网络的方法。NAT-PT 定义在 RFC 2765 和 RFC 2766（目前已被 RFC 4966 替代）中。NAT-PT 的工作方式是在 IPv4/IPv6 网络边界执行网关功能，NAT-PT 负责在网络边界实现 IPv4 与 IPv6 的转换操作。该方法允许 IPv4 主机与 IPv6 主机进行通信，而不需要在这些主机上运行双协议栈，反之亦然。

与 IPv4 的 NAT 和 PAT（超量 NAT）非常相似，NAT-PT 也支持静态和动态转换，而且还支持端口转换操作。

9. NAT ALG

NAT-PT 被设计用于网络层通信，负责 IPv6 到 IPv4 网络的转换操作。ALG（Application Level Gateway，应用级网关）运行在 OSI 模型的应用层，而 NAT-PT 则不检查净荷，因而 ALG 允许两个不同的网络（一个是 IPv6 网络，另一个是 IPv4 网络）进行应用层通信。

10. NAT64

与隧道相比，网络转换的两大好处是：

- 服务提供商可以为 IPv6 Internet 用户提供透明服务；
- 无缝迁移到 IPv6。

定义在 RFC 6144 中的 NAT64（Network Address Translation IPv6 to IPv4，IPv6 到 IPv4 的网络地址转换）将替代 NAT-PT。NAT64 与 DNS64 联合可以允许纯 IPv6 客户端与纯 IPv4 服务器进行通信，此时可以采用手工或静态绑定方式。此外，RFC 6146（Stateful NAT64）也定义了 NAT64。NAT64 执行转换操作时，使用 RFC 6145（IP/ICMP Translation Algorithm）和 RFC 6052（IPv6 Addressing of IPv4/IPv6 Translators）定义的

算法在 IPv6 与 IPv4 之间执行 IP 报头转换以及 IP 地址转换操作。NAT64 包含 NAT64 前缀、NAT64 路由器以及 DNS64 服务器等三个组件。

10.2.3 二层 VPN

随着当前高带宽业务及通过 IP 进行传输的应用的不断增多，再加上旺盛的市场需求，服务提供商不得不改变以前的惯用做法，其中的一个改变就是大多数服务提供商都开始部署 MPLS VPN 以满足带宽需求。需要注意的是，服务提供商可以有两种 VPN 服务：二层 VPN 或三层 VPN。本节将主要讨论二层 VPN，因为二层 VPN 不但能够帮助服务提供商解决高带宽需求，而且还能通过支持 IP/MPLS 的服务提供商网络为物理上相互隔离的网络提供“二层”邻接性。该服务（二层 VPN）为希望管控自己网络的客户提供了可能性。如果客户希望管理自己的路由协议、IP 网络管理以及 QoS 机制，那么二层 VPN 将是最简单的解决方案，此时服务提供商只要提供高吞吐量的二层连接即可。在很多情况下，通常都将这类二层 VPN 连接解决方案称为“伪线（pseudowire）”连接。

以太网 PW（PseudoWire，伪线）可以通过 MPLS 网络传输以太网帧，服务提供商可以利用该解决方案扩展站点之间的二层邻接性。也就是说，将在链路上运行生成树，而且通过这些链路连接的设备都将使用相同的子网。通常将这类服务称为仿真服务（Emulated Service），它们都运行在伪线上。除此以外，还要求具备可用的分组标签交换网络（MPLS 网络）。

以太网 PW 支持两种运行模式：标记模式（tagged mode）和原始模式（raw mode）。

1. 标记模式

标记模式中的“标记”指的是 802.1Q 标记。在伪线场景下，标记对于本地设备以及端点设备来说具有非常重要的意义。需要指出的是，如果网络边缘的 PE（Provider Edge，提供商边缘）设备修改了 VLAN 标识符，那么以太网 STP（Spanning Tree Protocol，生成树协议）将无法正确运行，这是因为连接两端的 AC（Attachment Circuit，接入电路）要求该标识符必须匹配，链路两端的标识符或 VLAN 标记必须匹配。标记模式使用的伪线类型是 0x0004。对于每个用户来说，在 PW 上发送的每个帧都必须有不同的 VLAN，称为“服务定界”VLAN 标记。如果 PE 从 AC 收到的帧缺少服务定界 VLAN 标记，那么 PE 将该帧发送到 PW 上之前必须在该帧前附加一个假的 VLAN 标记。

2. 原始模式

如果伪线工作在原始模式下，那么就可以在帧上添加服务定界标记，也可以不添加服务定界标记，对于端节点来说都没有什么影响。原始模式使用的伪线类型是 0x0005。如果以太网 PW 运行在原始模式下，那么 PE 就不能通过 AC 传送服务定界标记；强制要求在发送帧之前剥离服务定界标记。

3. L2TPv3

L2TPv3（Layer 2 Tunneling Protocol version 3，二层隧道协议版本 3）是二层 VPN 的扩展功能特性。根据 IETF 工作组的定义（RFC 3931 和 RFC 4719），L2TPv3 可以为 L2TP 提供多种增强功能，能够通过 L2TP 隧道化所有二层净荷，这些 RFC 定义了 L2TP 协议利用二层 VPN 通过 IP 骨干网隧道化二层净荷的方法。L2TPv3 使用的 IP 协议号是 115。如果要在 Cisco IOS 设备上配置 L2TPv3，那么就必须了解两个非常重要的前提条件：第一个前提条件是必须利用 **ip cef** 或 **ip cef distributed** 命令启用 CEF 特性；第二个前提条件是环回接口必须拥有一个有效的 IP 地址，使得 L2TPv3 控制信道对端的远程 PE 设备能够到达该接口。

4. AToM

例 10-8 给出了 AToM（Any Transport over MPLS，MPLS 上的任意传输）配置示例，该例在两个地理上相互隔离的站点之间建立了二层邻接性。

例 10-8 AToM 配置

```
!First we will create the xconnect configuration on routers.

R2(config)# int f0/0
R2(config-if)# xconnect 4.4.4.4 204 encapsulation mpls
R2(config-if-xconn)# end

!Now we do the matching configuration on the other device.

R4(config)# int f0/0
R4(config-if)# xconnect 2.2.2.2 204 encapsulation mpls
R4(config-if-xconn)# end
```

在两台路由器的 F0/0 接口上配置的 **xconnect** 命令可以按照指定的目的地创建桥接式连接。该命令在关键字 **xconnect** 的后面是对等路由器的 IP 地址以及唯一的 VCID（Virtual Circuit ID，虚电路 ID）。桥接式连接的两端 VCID 必须匹配，封装方式可以是 L2TPv2、L2TPv3 或 MPLS。需要注意的是，对于每条 **xconnet** 来说，每台路由器都必须有一个唯一的地址。例 10-9 给出了验证刚刚创建的伪线的方式。

例 10-9 伪线验证

```
R2# show xconnect all

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware
XC ST Segment 1 S1 Segment 2 S2
------+---------------------------------+--+---------------------------------+--
DN ac Fa0/0(Ethernet) AD mpls 4.4.4.4:204 DN
```

MPLS 二层伪线有两段：S1（Segment 1，段 1）用于面向客户端的端口；S2（Segment 2，段 2）则与骨干网配置相关。从 **show** 命令输出结果可以看出，该连接的 S1 已被管

理性关闭。如果要解决该问题，只要将其余链路的每一端均激活即可（如例 10-10 所示），然后可以重复上述验证操作。

例 10-10 激活链路并验证

```
!On all devices in the configuration bring up the interfaces on the media.

int f0/0
no shut

!Now we will verify the configuration.

R4# show xconnect peer 2.2.2.2 vcid 204

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware
XC ST Segment 1 S1 Segment 2 S2
------+---------------------------------+--+---------------------------------+--
UP ac Fa0/0(Ethernet) UP mpls 2.2.2.2:204 UP

!The S2 section has now been configured and verified to be working properly with
!state !(ST) of active(ac).
```

5. VPLS

VPLS 是一种二层 VPN 服务，可以通过 MPLS 网络将地理上相互隔离的 LAN 网段互连为单个桥接域。VPLS over GRE 可以让 VPLS 穿越 IP 网络，VPLS over GRE 的 PE 路由器必须支持 VPLS 以及 GRE 的封装与解封装，同时必须在每台 PE 路由器上都配置一个 VPLS 实例。

6. OTV

OTV（Overlay Transport Virtualization，叠加传输虚拟化）与 VPLS 相似，不需要三层 VPN 用到的 MPLS 传输以及多播支持。但是与 VPLS 不同的是，OTV 通常部署在 CE（Customer Edge，客户边缘）上，需要在每台 CE 路由器或交换机上配置 OTV。OTV 可以通过三层、二层或 MPLS 网络扩展二层 LAN。截至本书出版之时，Cisco IOS XE Software Release 3.5 及以后版本与 Cisco NX-OS Release 6.2(2)及以后版本均支持 OTV。OTV 的一个重要优势在于故障域隔离特性，不会改变生成树的树根。由于每个 CE 都有自己的树根，因而服务提供商不需要提供相应的干预或规划操作。此外，OTV 还支持多归属的自动检测以及 ARP 优化功能。

10.2.4 GET VPN

GET（Group Encrypted Transport，组加密传输）VPN 可以对通过非安全网络进行传输的流量进行加密，利用 IPSec 协议集来实现数据的完整性和机密性。典型的 GET 配置包括被称为 KS（Key Server，密钥服务器）的路由器以及若干个被称为 GM（Group Member，组成员）的路由器。KS 负责创建、维护并向 GM 发送“策略”，由策略告

诉 GM 应该对哪些流量进行加密以及必须采用何种加密算法。KS 最重要的概念就是生成加密密钥。目前使用以下两种密钥。

- **TEK（Transport Encryption Key，传输加密密钥）**：GM 利用该密钥加密数据。
- **KEK（Key Encryption Key，密钥加密密钥）**：用来在 KS 与 GM 之间加密信息。

GET 的一个重要特性就是不在 GM 之间建立任何 IPSec 隧道。与 DMVPN 不同，每个 GM 都有自己的策略（加密哪些流量、使用何种加密算法以及加密算法使用哪个密钥），而且仅对符合指定策略的数据包进行加密，并利用 ESP（Encapsulated Security Payload，封装安全净荷）将加密后的数据包发送到网络上。请注意，GM 使用原始 IP 地址向外路由数据包（称为 IP 报头保留[IP Head Preservation]机制），因而可以将这些数据包路由到网络中的每一台路由器（只要路由表中存在相应的路由信息）。

例 10-11 给出了创建 GET VPN 的初始配置示例。首先，KS 需要为 Rekey（密钥更新）进程使用 RSA（Rivest, Shamir, and Adelman）密钥。KS 必须在 TEK 到期（默认为 3600 秒）之前向外发送一个新的 TEK（以及 KEK）。KS 在 Rekey 阶段完成该操作，该阶段由 KS 与 GM 之间建立的 ISAKMP SA 进行认证并负责相应的安全性。ISAKMP 利用 GDOI（Group Domain of Interpretation，组解释域）消息（可以将其视为 IKE[Internet Key Exchange，Internet 密钥交换]的变化形式）构建 SA 并加密 GM 注册消息。与 IKE 使用 UDP/500 不同，GDOI 使用的是 UDP/848。

KS 在 Rekey 进程中认证 GM 的时候需要使用 RSA 密钥。

例 10-11 GET VPN 的基本配置

```
!Remember that to generate new RSA keys you must have Hostname and Domain-name
!configured on the router.

R1(config)# ip domain-name cisco.com
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.cisco.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
%SSH-5-ENABLED: SSH 1.99 has been enabled
Then we need ISAKMP paramaters, just like in regular IPSec configuration. Pre-shared
key must be specified on both KS and GM to be able to authenticate. This will be
used to establish ISAKMP SA to secure further GDOI messages.
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# exi
R1(config)# crypto isakmp key GETVPN-R5 address 10.1.25.5
R1(config)# crypto isakmp key GETVPN-R4 address 10.1.24.4

!The IPSec parameters must be configured on KS. These parameters are not used by KS
!itself. They are part of policy that will be sent down to the GMs. The IPSec
!profile tells the GM what encryption algorithm use.

R1(config)# crypto ipsec transform-set TSET esp-aes esp-sha-hmac
R1(cfg-crypto-trans)# crypto ipsec profile GETVPN-PROF
R1(ipsec-profile)# set transform-set TSET
```

```
!Now it's time to configure KS. To do that we need to specify The Group. One KS
!may have many groups and each group may have different security policy.

R1(ipsec-profile)# crypto gdoi group GETVPN
R1(config-gdoi-group)# identity number 1
R1(config-gdoi-group)# server local
%CRYPTO-6-GDOI_ON_OFF: GDOI is ON
```

接下来需要指定 Rekey 参数。Rekey 阶段支持以下两种运行方式。

- **单播 Rekey**：如果网络基础设施不支持多播（可能是 ISP 的 IP VPN 网络不支持多播），那么 KS 就要向知道的每一个 GM 发送一个 Rekey 包。
- **多播 Rekey**：如果网络基础设施支持多播，那么就可以启用多播 Rekey，KS 只要生成一个 Rekey 包并同时向所有 GM 发送一次 Rekey 包即可。

例 10-12 给出了指定 Rekey 参数的配置示例。

例 10-12 Rekey 参数

```
R1(gdoi-local-server)# rekey authentication mypubkey rsa R1.cisco.com
R1(gdoi-local-server)# rekey retransmit 10 number 2
R1(gdoi-local-server)# rekey transport unicast

!By default every GM can register to KS as long as it has correct PSK configured (or
!valid Certificate in case of PKI). To authorize GMs to be able to register in this
!group on KS, you need to specify a standard ACL with GM's IP addresses. Our ACL is
!named GM-LIST.

R1(gdoi-local-server)# authorization address ipv4 GM-LIST
```

接下来需要为 GM 配置策略。可以利用前面配置的 IPSec 配置简档来创建加密策略。为了告诉 GM 应该加密哪些数据包，需要配置 ACL（此处用到的是扩展 ACL）。本例配置的 ACL 名为 LAN-LIST。为了实现基于时间的反重放攻击保护，还可以指定窗口大小。最后一个非常重要的参数就是 KS 的 IP 地址。由于 KS 可以运行在不同的 IP 地址（如环回地址）之上，因而必须将该参数向下发送给 GM。

例 10-13 给出了 GET VPN 策略的配置示例。

例 10-13 GET VPN 策略

```
R1(gdoi-local-server)# sa ipsec 1
R1(gdoi-sa-ipsec)# profile GETVPN-PROF
R1(gdoi-sa-ipsec)# match address ipv4 LAN-LIST
R1(gdoi-sa-ipsec)# replay counter window-size 64
R1(gdoi-sa-ipsec)# address ipv4 10.1.12.1
R1(gdoi-local-server)#
%GDOI-5-KS_REKEY_TRANS_2_UNI: Group GETVPN transitioned to Unicast Rekey.
R1(gdoi-local-server)# exi
R1(config-gdoi-group)# exi
R1(config)# ip access-list standard GM-LIST
R1(config-std-nacl)# permit 10.1.25.5
R1(config-std-nacl)# permit 10.1.24.4
R1(config-std-nacl)# exi
```

```
!Here's our "policy ACL". Note that we must exclude GDOI (UDP/848) from this policy
!as there is not much sense to encrypt something already encrypted.
R1(config)# ip access-list extended LAN-LIST
R1(config-ext-nacl)# deny udp any eq 848 any eq 848
R1(config-ext-nacl)# permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
R1(config-ext-nacl)# exi
```

接下来配置 GM。需要在每个 GM 上按照例 10-14 所示的方式进行相应的配置操作。

例 10-14　GM 配置

```
R5(config)# crypto isakmp policy 10
R5(config-isakmp)# authentication pre-share
R5(config-isakmp)# exi
R5(config)# crypto isakmp key GETVPN-R5 address 10.1.12.1
R5(config)# crypto gdoi group GETVPN
R5(config-gdoi-group)# identity number 1
R5(config-gdoi-group)# server address ipv4 10.1.12.1
R5(config-gdoi-group)# exi

!This ACL is optional. In general we should configure our policy on KS only, but
!there are some situations when we need to exclude some flows from encryption. Like
!here, we were asked for excluding SSH traffic between 192.168.4.0/24 AND
!192.168.5.0/24 networks.

R5(config)# ip access-list extended DO-NOT-ENCRYPT
R5(config-ext-nacl)# deny tcp 192.168.4.0 0.0.0.255 eq 22 192.168.5.0 0.0.0.255
R5(config-ext-nacl)# deny tcp 192.168.5.0 0.0.0.255 192.168.4.0 0.0.0.255 eq 22
R5(config-ext-nacl)# deny tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 22
R5(config-ext-nacl)# deny tcp 192.168.5.0 0.0.0.255 eq 22 192.168.4.0 0.0.0.255
R5(config-ext-nacl)# exi
R5(config)# crypto map CMAP-GETVPN 10 gdoi
% NOTE: This new crypto map will remain disabled until a valid
group has been configured.
R5(config-crypto-map)# set group GETVPN
R5(config-crypto-map)# match address DO-NOT-ENCRYPT
R5(config-crypto-map)# exi
R5(config)# int s0/1/0.52
R5(config-subif)# crypto map CMAP-GETVPN
R5(config-subif)# exi
R5(config)#
%CRYPTO-5-GM_REGSTER: Start registration to KS 10.1.12.1 for group GETVPN using
  addr
10.1.25.5
R5(config)#
%CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R5(config)#
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group GETVPN transitioned to Unicast Rekey.
%GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.12.1 complete for group GETVPN using
address 10.1.25.5

!See above SYSLOG messages. They indicate that GM has started registration process
!with KS and registered successfully.
```

最后，可以验证上述 GET VPN 的配置情况（如例 10-15 所示）。

例 10-15　验证 GET VPN

```
R1# sh crypto gdoi group GETVPN
Group Name               : GETVPN (Unicast)
Group Identity           : 1
```

```
Group Members          : 2
IPSec SA Direction     : Both
Active Group Server    : Local
Group Rekey Lifetime   : 86400 secs
Group Rekey
Remaining Lifetime     : 86361 secs
Rekey Retransmit Period     : 10 secs
Rekey Retransmit Attempts   : 2
Group Retransmit
Remaining Lifetime          : 0 secs
IPSec SA Number             : 1
IPSec SA Rekey Lifetime     : 3600 secs
Profile Name                : GETVPN-PROF
Replay method               : Count Based
Replay Window Size          : 64
SA Rekey
Remaining Lifetime          : 3562 secs
ACL Configured              : access-list LAN-LIST
Group Server list           : Local

R1# sh crypto gdoi ks policy
Key Server Policy:
For group GETVPN (handle: 2147483650) server 10.1.12.1 (handle: 2147483650):
# of teks : 1 Seq num : 0
KEK POLICY (transport type : Unicast)
spi : 0x76749A6D99B3C0A3827FA26F1558ED63
management alg    : disabled encrypt alg         : 3DES
crypto iv length  : 8           key size          : 24
orig life(sec)    : 86400   remaining life(sec): 86355
sig hash algorithm : enabled   sig key length    : 162
sig size          : 128
sig key name      : R1.micronicstraining.com
TEK POLICY (encaps : ENCAPS_TUNNEL)
spi               : 0xAF4FA6F8 access-list     : LAN-LIST
# of transforms   : 0 transform          : ESP_AES
hmac alg          : HMAC_AUTH_SHA
alg key size      : 16          sig key size        : 20
orig life(sec)    : 3600        remaining life(sec) : 3556
tek life(sec)     : 3600        elapsed time(sec)   : 44

R1# sh crypto gdoi ks acl
Group Name        : GETVPN
Configured ACL:
access-list LAN-LIST deny udp any port = 848 any port = 848
access-list LAN-LIST permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

!Here's the ACL which tells the GMs what traffic they should encrypt.

R1# sh crypto gdoi ks members
Group Member Information :
Number of rekeys sent for group GETVPN : 1
Group Member ID   : 10.1.24.4
Group ID          : 1
Group Name        : GETVPN
Key Server ID     : 10.1.12.1
Rekeys sent       : 0
Rekeys retries    : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0
Sent seq num      : 0  0    0    0
Rcvd seq num      : 0  0    0    0
Group Member ID   : 10.1.25.5
```

```
Group ID          : 1
Group Name        : GETVPN
Key Server ID     : 10.1.12.1
Rekeys sent       : 0
Rekeys retries    : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0
Sent seq num      : 0  0    0    0
Rcvd seq num      : 0  0    0    0
```

备考任务

表 10-4 列出了与本章相关的主要协议以及相应的标准文档信息。

表 10-4 第 10 章的协议与标准

主题	标准
Generic Routing Encapsulation	RFC 2784
NHRP (Next-Hop Resolution Protocol)	RFC 2332
Basic Transition Mechanisms for IPv6 Hosts and Routers	RFC 4213
The Group Domain of Interpretation	RFC 3547
Layer 2 Virtual Private Network (L2VPN)	RFC 6136
Layer 2 Tunnel Protocol version 3	RFC 3931 和 RFC 4719
IPv6 Stateless Address Autoconfiguration	RFC 4862
Stateful NAT64: Network Address and Protocol Translation	RFC 6146
Framework for IPv4/IPv6 Translation	RFC 6144

10.3 理解与记忆

与所有的 Cisco CCIE 笔试一样，CCIE 路由和交换笔试也包含了非常广泛的考试主题，因而本节提供了一些有用工具，来帮助大家加深理解并记忆本章所涵盖的广泛的考试主题内容。

10.3.1 定义关键术语

请写出本章涉及的下列关键术语，然后在术语表中核对正确答案：

GRE、ISATAP、6to4、L2VPN、AtoM、标记模式、原始模式、DMVPN、GDOI、NHRP、密钥服务器、组成员、IPSec 配置简档、TEK、KEK、单播 Rekey、多播 Rekey

本章主要讨论以下主题：

- 部署 MPLS（Multiprotocol Label Switching，多协议标签交换）三层 VPN；
- 部署 MPLS；
- 在 PE、P 以及 CE 路由器上部署 MPLS VPN；
- 部署 VRF（Virtual Routing and Forwarding，虚拟路由和转发）；
- 部署 Multi-VRF CE（VRF Lite）。