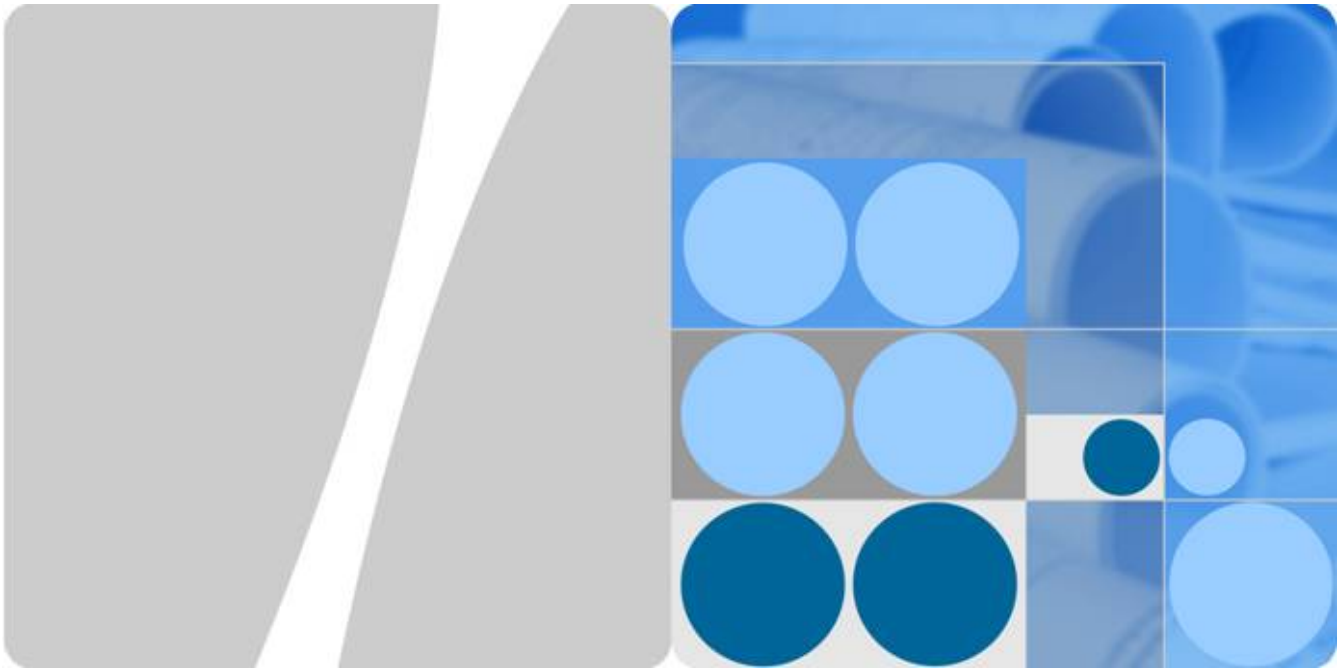


Quidway Eudemon 8080E/8160E 防火墙
V100R003

特性描述

文档版本 04

发布日期 2011-01-05

华为技术有限公司

HUAWEI

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 0755-28560000 4008302118

客户服务传真： 0755-28560111

前 言

读者对象

本文档介绍 Eudemon 8080E/8160E 的功能特性，包括防火墙概述、产品特性、安全特性、VPN 和高可靠性。

本文档主要适用于以下工程师：

- 技术支持工程师
- 维护工程师
- 网络工程师
- 网络管理员
- 网络维护工程师

目 录

插图目录

表格目录

1 概述

关于本章

1.1 网络安全概述

1.1.1 威胁

随着互联网的迅速发展，越来越多的企业借助网络服务来加速自身的发展。如何在一个开放的网络环境中守卫自身的机密数据和资源已越来越为人们所关注。

目前，常见的网络安全威胁主要分为以下几类：

- 非法使用

  资源被未授权的用户（非法用户）或合法用户以未授权方式（非法权限）使用。例如，攻击者通过猜测帐号和密码，进入计算机系统，非法使用资源。
- 拒绝服务

  服务器拒绝合法用户正常访问信息或资源的请求。例如，攻击者短时间内使用大量数据包不断向服务器发起连接，致使服务器负荷过重而不能处理正常访问。
- 信息盗窃

  攻击者并不直接入侵目标系统，而是通过窃听网络来获取重要数据或信息。
- 数据篡改

  攻击者对系统数据或消息流进行有选择的修改、删除、延误、重排序及插入虚假消息等操作，破坏数据的一致性。

1.1.2 服务种类

针对各种安全威胁而采取的安全防护措施称为安全服务，它主要分为以下几类：

- 可用性服务

  保证信息或数据在需要时能够被合法用户正常访问。
- 机密性服务

  保证敏感信息或数据不被泄漏给未授权的用户。
- 完整性服务

  保证信息或数据不被未经授权的用户改动或破坏。
- 鉴别服务

  保证某个通信实体身份的合法性。
- 授权服务

  对资源的使用实施控制，规定访问者的权限。

1.1.3 服务实现

加密

加密是将可读的明文文本转化为不可读的加密文本的过程。加密不仅为用户提供通信方面的安全保证，同时也是其他许多安全机制的基础。

加密的方式主要分为三种：

- 对称密码体制

  其特征是用于加密和解密的密钥是同一个，通信双方通过共享同一密钥来交换消息。密钥必须秘密保存。典型代表包括：DES（Data Encryption Standard）、3DES（Triple DES）等。

- 公钥密码体制

  不同于对称密码体制，公钥密码体制有两个不同密钥，可将加密功能和解密功能分开。一个密钥称为私钥，必须秘密保存；另一个称为公钥，可被公开分发。典型代表包括：DH（Diffie-Hellman）、RSA（Rivest，Shamir，Adleman）。

- 散列函数机制

  其特征是将一个变长的消息压缩到一个定长的编码字中，成为一个散列或消息摘要。典型代表包括：MD5（Message-Digest Algorithm 5）、SHA（Secure Hash Algorithm）。

加密技术能够应用在以下安全机制中：

- 认证口令设计
- 安全通信协议设计
- 数字签名设计

认证

认证通常在访问网络前或网络提供服务前进行，用于鉴别用户身份的合法性。

认证服务可以由网络上的设备在本地提供，也可以通过专用的认证服务器提供。相比较而言，后者具有更好的灵活性、可控性和可扩展性。目前，在异构网络环境中，认证服务主要使用 RADIUS（Remote Authentication Dial in User Service）这一开放的标准。

访问控制

访问控制是一种加强授权的方法，一般分为两种：

- 基于操作系统的访问控制

  对用户访问某计算机系统资源时的特定访问行为进行授权。可以基于身份、组、规则等属性配置访问控制策略。

- 基于网络的访问控制

  限制接入网络的权限。由于网络的复杂性，其机制远比基于操作系统的访问控制更为复杂。一般在访问请求者和访问目标之间的一些中间设备（例如防火墙）上配置访问控制策略，从而实现基于网络的接入控制。

安全协议

安全协议是网络安全的重要内容。下面将从 TCP/IP（Transmission Control Protocol/Internet Protocol）的分层模型角度来介绍目前广泛使用的安全协议：

- 应用层安全

提供从一台主机上的应用程序到另一台主机上的应用程序的端到端的安全保障。应用层安全机制必须根据具体的应用而定，因此不存在通用的应用层安全协议。

例如，SSH（Secure Shell）协议可以建立安全的远程登录会话，为 Telnet、FTP 等提供安全的连接通道。

- 传输层安全

  提供同一台主机的进程之间，或不同主机的进程之间的安全保障。在传输层中提供安全服务的方法是强化通信实体双方的交互过程，具体包括通信实体的认证、数据加密密钥的交换等。

  例如，SSL（Secure Socket Layer）可以在 TCP 的基础上提供安全保障。

- 网络层安全

  网络层安全是整个 TCP/IP 安全的基础，也是 Internet 安全的核心。即使上层协议没有实现安全性保障，通过对网络层报文进行保护，用户信息也能够从网络层得到安全保障。

  目前，网络层最重要的安全协议是 IPSec（IP Security Protocol）。IPSec 是一系列网络安全协议的总称，包括安全协议、加密协议等，能够为通讯双方提供访问控制、无连接的完整性、数据源认证、防重放、加密以及对数据流分类加密等服务。

- 数据链路层安全

  提供点到点的安全性，如在一个点到点链路或帧中继的永久虚链路上提供安全性。链路层安全的主要实现方法是在链路的每一端使用专用设备完成加密和解密。

1.2 防火墙概述

1.2.1 简介

在实际的网络环境中，单一的安全防护技术不足以确保网络的安全，多种安全防护技术的综合应用才能够将安全风险控制在尽量小的范围内。

一般而言，构建一个安全防范体系具体实施的第一项内容就是在内部网络和外部网络之间构筑一道防线，以抵御来自外部的绝大多数攻击。完成这项任务的网络产品的作用类似于建筑行业中用于防止火灾蔓延的隔断墙，因此我们称这种网络产品为防火墙。

防火墙是监控可信任网络（内部网络）和不可信任网络（外部网络）之间的访问通道。它一方面阻止来自外部网络的用户对内部网络的未授权访问，另一方面允许内部网络的用户对外部网络进行访问。防火墙也可以作为一个访问因特网的权限控制关口，如允许组织内的特定的主机可以访问因特网。现在的许多防火墙同时还具有一些其他特点，如进行身份鉴别，对信息进行安全处理（如加密）等等。

防火墙不单用于对因特网的连接，也可以用来保护内部网络的大型机和重要的资源（如数据）。对受保护数据的访问都必须经过防火墙的过滤，即使网络内部用户要访问受保护的数据，也要经过防火墙。

防火墙主要用于以下目的：

- 限制用户或信息由一个特定的被严格控制的站点进入。
- 阻止攻击者接近其他安全防御设施。

- 限制用户或信息由一个特定的被严格控制的站点离开。

1.2.2 发展历史

第一代防火墙－包过滤防火墙

包过滤机制是指设备在网络层对每一个数据包进行检查，根据配置的安全策略转发或丢弃数据包。

包过滤防火墙的基本原理是通过配置 ACL（Access Control List），根据源/目的 IP 地址、源/目的端口号、协议类型和报文传递的方向等信息制定规则，对匹配规则的报文采取相应（允许或拒绝）的操作。

包过滤防火墙设计简单，易于实现，而且价格便宜。但其缺点也不容忽视，主要表现在：

- 随着 ACL 数量的增加，防火墙过滤性能急剧下降。
- 静态配置的 ACL 灵活性差，难以适应动态的安全要求。
- 包过滤机制不检查会话状态也不分析数据内容，安全性低。

  例如，攻击者可以使用假冒地址进行欺骗，通过把自己主机 IP 地址设成一个合法主机 IP 地址，就能轻易地通过报文过滤器，达到攻击目的。

第二代防火墙－代理防火墙

代理服务作用于网络的应用层，其工作原理是接管内部网络和外部网络用户之间直接进行的业务。代理服务检查来自内部网络客户端的请求，认证通过后，将代表客户端与真正的外部网络服务器建立连接，转发客户端的请求，并将服务器返回的响应回送给客户端。

代理防火墙能够完全控制会话过程和信息交换，具有较高的安全性。但其缺点也同样突出，主要表现在：

- 代理服务由软件实现，限制了处理速度，容易遭受拒绝服务攻击。
- 需要针对每一种协议开发应用层代理，开发代价大并且升级困难。

第三代防火墙－状态检测防火墙

状态检测技术是包过滤技术的扩展（非正式的也可称为“动态包过滤”）。状态检测防火墙的基本原理如下：

- 通过各种状态表来追踪激活的 TCP（Transmission Control Protocol）会话和 UDP（User Datagram Protocol）伪会话，由 ACL 规则来决定哪些会话允许建立，只有与被允许建立的会话相关联的数据包才被转发。

  说明

  UDP 伪会话是指防火墙在处理基于 UDP 的数据包时为 UDP 建立虚拟连接，以便对 UDP 连接过程进行状态监控的会话过程。

- 状态检测防火墙在网络层截获数据包，然后从数据包中提取出安全策略所需要的状态信息，并保存到动态状态表中。通过分析这些状态表和与该数据包有关的后续连接请求来做出恰当决定。

状态检测防火墙具有以下优点：

- 速度快

  状态检测防火墙对数据包进行 ACL 检查的同时，可以将数据包连接状态记录下来，后续数据包则无需再进行 ACL 检查，只需根据状态表进行连接记录检查即可。检查通过后，该连接状态记录将被刷新，从而避免重复检查具有相同连接状态的数据包。连接状态表里的记录可以随意排列，防火墙可采用诸如二叉树或哈希（hash）等算法进行快速搜索，提高了处理效率。

- 安全性较高

  连接状态表是动态管理的，老化时间到期后，防火墙会删除连接状态表项，保障了内部网络的实时安全。同时，防火墙采用连接状态实时监控技术，通过在状态表中识别诸如应答响应等连接状态因素，增强了系统的安全性。

1.3 Eudemon 系列产品介绍

华为公司的 Eudemon 系列硬件防火墙是一系列改进型的状态检测防火墙，结合华为公司特有的 ASPF（Application Specific Packet Filter）技术，兼具代理防火墙安全性高、状态检测防火墙速度快的优点。

Eudemon 系列防火墙采用专门设计的高可靠性硬件系统和具有自主知识产权的专有操作系统，将高效的包过滤功能、透明的代理服务、改进的状态检测安全技术、丰富的统计分析功能等多种安全保障措施集于一身，并提供多类型接口和工作模式。

Eudemon 系列防火墙包括多种型号，处理能力从低端数十兆到高端数千兆，结合路由器产品和交换机产品，能够为小型、中小型和大中型客户提供先进的、全方位的网络安全解决方案。

1.4 Eudemon 8080E/8160E 产品特性

高安全性

Eudemon 8080E/8160E 采用业界领先的“NP+多核 CPU+分布式”架构，与传统的防火墙相比，突破了传统架构带来的性能约束，提供强大的处理性能，丰富的业务和强大的安全防范性能,并且易于扩展。

与基于通用操作系统的软件防火墙相比，Eudemon 8080E/8160E 采用专门设计的硬件平台和具有自主知识产权的安全操作系统，报文处理和操作系统完全分开，大大提高了系统的安全性。

Eudemon 8080E/8160E 采用 ACL 完成包过滤，还提供数十种攻击防范能力，这些都有效地保障了网络的安全。

高可靠性

Eudemon 8080E/8160E 的电源模块采用双电源（1+1 备份），两个电源模块互相热备份，电源倒换时不影响系统运行。同时，交换网板采用 3+1 负载分担冗余备份工作方式，当一块交换网板损坏或更换时，另外三块将自动分担其业务，保证业务数据不会中断。

Eudemon 8080E/8160E 支持 VRRP（Virtual Router Redundancy Protocol）、VGMP（VRRP Group Management Protocol）和 HRP（Huawei Redundancy Protocol）协议，支持双机热备份，满足电信级用户对设备的高可靠性的要求。

高性能处理

Eudemon 8080E/8160E 是电信级的高端防火墙，采用 NP 技术和多核 CPU 技术，提供线速的高性能安全防范和报文处理能力。在提供高性能的同时，还可以支持数万条 ACL 规则。

强大的组网和业务支撑能力

Eudemon 8080E/8160E 除了具备各种安全防范功能，提供高效的安全保障能力外，还集成了路由能力，如静态路由及 RIP（Routing Information Protocol）、OSPF（Open Shortest Path First）、BGP（Border Gateway Protocol）动态路由，同时还支持路由策略、路由迭代和路由管理，从而使组网应用更加灵活。

强大的日志和统计分析功能

Eudemon 8080E/8160E 提供完整、统一的日志信息描述，包括攻击防范日志、流量监控日志、黑名单日志等日志类型，同时提供强大的统计分析功能，在安全分析和事后追踪等方面提供了有力的帮助。

1.5 Eudemon 8080E/8160E 功能列表

Eudemon 8080E/8160E 提供强大的安全和攻击防范、丰富的业务组网、高可靠性能力，支持灵活的维护管理以及增强的日志功能，最大程度的满足用户的需求。

Eudemon 8080E/8160E 的功能列表如表 1-1 所示。

表 1-1 Eudemon 8080E/8160E 功能列表

属性	说明	
安全防范	包过滤	● 支持基本 ACL、高级 ACL。 ● 支持基于时间段 ACL。 ● 支持配置顺序优先的排序。 ● 支持动态插入 ACL 规则。 ● 支持黑名单。 ● 支持应用层包过滤 ASPF、提供状态检测。 ● 提供端口映射机制。
	NAT	● 支持 NAT 方式、NAPT 方式和地址池方式的地址转换。 ● 支持内部服务器地址静态映射。 ● 支持基于安全域的内部服务器地址静态映射。 ● 支持多种 NAT ALG，包括 FTP、PPTP、SMTP、RTSP、MSN、QQ 等。

属性	说明	
	攻击防范	● 防范多种 DoS 攻击：包括 SYN Flood、ICMP Flood、UDP Flood、WinNuke、ICMP 重定向和不可达报文、Land、Smurf 和 Fraggle 等。 ● 防范扫描窥探：包括 IP 地址扫描、端口扫描、IP 源站选路选项、IP 路由记录选项、ICMP 探测报文。 ● 防范其他攻击：如 IP Spoofing 等。 ● TCP 反向源认证。
	认证	● 支持 AAA、RADIUS、HWTACACS。 ● 支持基于域的管理。 ● 支持本地用户管理。
网络互联	链路层协议	● 支持 Ethernet。 ● 支持 VLAN。 ● 支持 PPP。 ● 支持 HDLC。 ● 支持 Trunk。 ● 支持 IP-link。
	IP 服务	支持 ARP 地址解析。
	路由协议	● 支持静态路由。 ● 支持 RIP、OSPF、BGP 动态路由。 ● 支持策略路由。 ● 支持路由策略、路由迭代和路由管理。
	VPN	● 支持 AH、ESP 认证协议，支持传输和隧道模式封装。 ● 支持 IKE、IKEv2 密钥交换协议。 ● 支持 L2TP VPN。 ● 支持 GRE VPN。 ● 支持 IPSec VPN。
配置与管理	工作模式	● 支持路由模式。 ● 支持透明模式。 ● 支持混合模式。

属性	说明	
	配置方式	● 支持通过 Console 口进行本地配置和维护。 ● 支持通过 AUX 接口 Modem 拨号接入进行远程配置和维护。 ● 支持通过 Telnet 方式进行本地或远程配置，支持 Telnet Server、Telnet Client。 ● 支持通过 SSH 方式进行安全的维护管理。
	维护和管理	● 支持命令行分级保护，确保未授权用户无法侵入。 ● 支持文件系统，提供多配置文件和多程序文件。 ● 支持 NTP，提供高时间精度。 ● 提供 ping 和 tracert 功能。 ● 支持动态加载热补丁和网络处理器热补丁。
维护和可靠性	产品设计	● 符合多种国内和国际的认证和设计标准。 ● 支持双电源（1+1 备份），支持电源热插拔。 ● 提供电源极性反接保护。 ● 支持不带业务的接口板热插拔。 ● 支持交换网板 3+1 负载分担冗余备份。
	系统管理	支持标准网管协议 SNMP v1、SNMP v2c 和 SNMP v3 版本。
	双机热备份	支持 VRRP、VGMP 和 HRP。
系统日志	● 支持 SYSLOG 和二进制高速流方式输出日志信息。 ● 可通过日志服务器进行日志浏览和查询，支持 eLog 日志服务器。 ● 统计输入和输出的 IP 报文、攻击防范日志、流量监控日志、黑名单日志。	

2 入门

关于本章

2.1 工作模式

2.1.1 分类

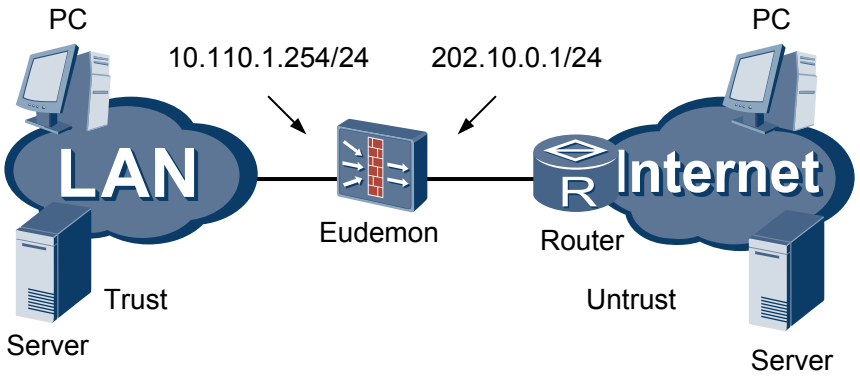
目前，Eudemon 能够工作在三种模式下：路由模式、透明模式、混合模式。

- 路由模式

  路由模式下 Eudemon 以第三层对外连接，所有接口都需要配置 IP 地址。此时需要将 Eudemon 与内部网络、外部网络相连的接口分别配置成不同网段的 IP 地址，并重新规划原有的网络拓扑。此时的 Eudemon 相当于一台路由器。

  如图 2-1 所示，Eudemon 的 Trust 区域接口与公司内部网络相连，Untrust 区域接口与外部网络相连。值得注意的是，Trust 区域接口和 Untrust 区域接口分别处于两个不同的子网中。

  图 2-1 路由模式组网图

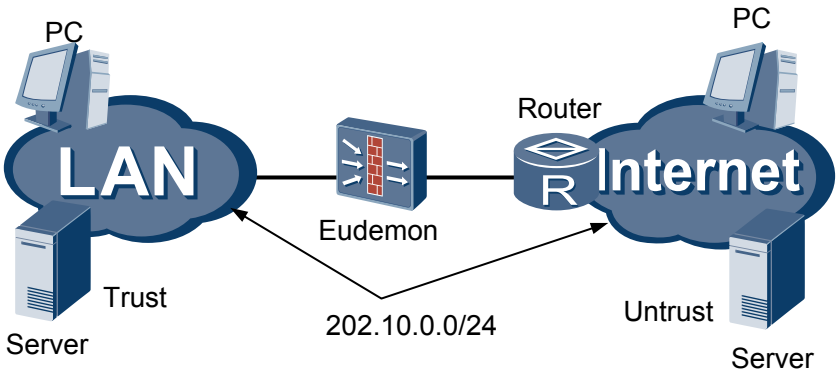
  采用路由模式的优点是可以完成 ACL 包过滤的功能。缺点是需要对网络拓扑进行修改。例如，内部网络用户需要更改网关，路由器需要更改路由配置等。

- 透明模式

  透明模式下 Eudemon 通过第二层与外界连接，所有接口都不能配置 IP 地址。此时防火墙对于子网用户和路由器来说是完全透明的，用户完全感觉不到防火墙的存在。

  如图 2-2 所示，Eudemon 的 Trust 区域接口与公司内部网络相连，Untrust 区域接口与外部网络相连。需要注意的是内部网络和外部网络必须处于同一个子网。

图 2-2 透明模式组网图



透明模式可以避免改变拓扑结构造成的麻烦。采用透明模式时，只需在网络中像放置网桥（bridge）一样插入 Eudemon 即可，无需修改任何已有的配置。IP 报文同样会经过相关的过滤检查，内部网络用户依旧受到防火墙的保护。

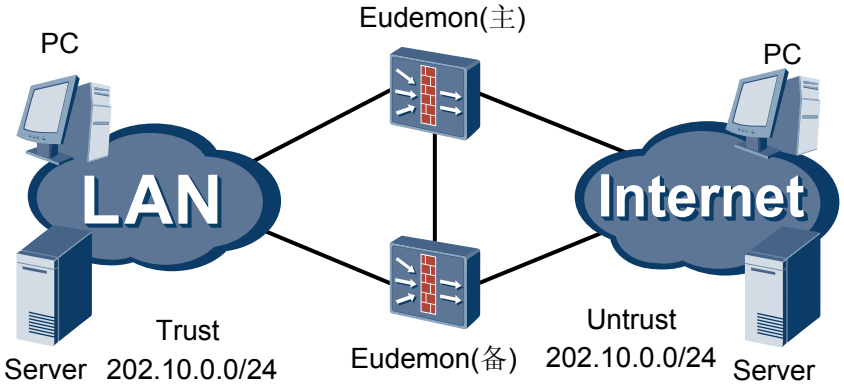
- 混合模式

  混合模式既存在工作在路由模式的接口（接口具有 IP 地址），又存在工作在透明模式的接口（接口无 IP 地址）。

  混合模式主要用于透明模式作双机热备份的情况，此时启动 VRRP（Virtual Router Redundancy Protocol）功能的接口需要配置 IP 地址，其他接口不配置 IP 地址。透明模式双机备份相关介绍请参见*《Quidway Eudemon 8080E/8160E 防火墙 配置指南 可靠性分册》*。

  防火墙混合模式的典型组网方式如图 2-3 所示。

图 2-3 混合模式组网图



主/备 Eudemon 的 Trust 区域接口与公司内部网络相连；Untrust 区域接口与外部网络相连；主/备 Eudemon 互相连接，并运行 VRRP 进行备份。需要注意的是内部网络和外部网络必须处于同一个子网。

2.1.2 工作原理

三种工作模式的工作原理如下：

- 路由模式

  Eudemon 工作在路由模式下时，所有接口都需要配置 IP 地址。不同的安全区域相关的接口连接的外部用户属于不同的子网。

  当报文在接口间进行转发时，根据报文的 IP 地址来查找路由表。此时 Eudemon 表现为一个路由器。但是，Eudemon 与路由器不同，Eudemon 转发的 IP 报文还需要送到上层进行相关过滤等处理，通过检查会话表或 ACL 规则以确定是否允许该报文通过。除此之外，防火墙还需要完成其他防攻击检查。

- 透明模式

  Eudemon 工作在透明模式（也可以称为桥模式）下时，所有接口都不能配置 IP 地址。透明模式下所有相关接口连接的外部用户同属一个子网。

  当防火墙转发报文时，需要根据报文的 MAC（Media Access Control）地址寻找出接口。此时 Eudemon 表现为一个透明网桥。但是，Eudemon 与网桥不同，Eudemon 转发的 IP 报文还需要送到上层进行相关过滤等处理，通过检查会话表或 ACL 规则以确定是否允许该报文通过。此外，防火墙还需要完成其他防攻击检查。

  工作在透明模式下的 Eudemon 在数据链路层连接局域网（LAN），网络终端用户无需为连接网络而对设备进行特别配置，就像 LAN Switch 进行网络连接。

- 混合模式

  Eudemon 工作在混合模式下时，部分接口配置 IP 地址，部分接口不能配置 IP 地址。配置 IP 地址的接口，接口上启动 VRRP 功能，用于双机热备份；而未配置 IP 地址的接口，相关接口连接的外部用户同属一个子网。

  当报文在透明模式下的接口间进行转发时，转发过程与透明模式的工作过程完全相同。当防火墙进行双机热备份时，转发过程类似路由模式的工作过程。

2.2 安全区域

2.2.1 概述

区域（zone）是防火墙产品所引入的一个安全概念，是防火墙产品区别于路由器的主要特征。

对于路由器，各个接口所连接的网络在安全上可以视为是平等的，没有明显的内外之分，所以即使进行一定程度的安全检查，也是在接口上完成的。这样，一个数据流单方向通过路由器时有可能需要进行两次安全规则的检查：入接口的安全检查和出接口的安全检查，以便使其符合每个接口上独立的安全定义。

而这种思路对于防火墙不适合，因为防火墙放置于内部网络和外部网络之间，用于保护内部网络不受外部网络上恶意用户的侵害，有着明确的内外之分。当一个数据流通过 Eudemon 的时候，根据其发起方向的不同，所引起的操作是截然不同的。由于这种安全级别上的差别，采用在接口上检查安全策略的方式已经不适用。因此，Eudemon 提出了安全区域的概念。

一个安全区域是一个或多个接口的组合，具有一个安全级别。

安全区域有如下特点：

- 安全级别通过 1 ～ 100 的数字表示，数字越大表示安全级别越高。
- 不存在两个具有相同安全级别的安全区域。

只有当数据在分属于两个不同安全级别的区域之间流动时，才会激活防火墙的安全规则检查功能。数据在属于同一个安全区域的不同接口间流动时不会引起任何检查。

2.2.2 划分

Eudemon 8080E/8160E 缺省保留四个安全区域，划分如下：

- 非受信区域 Untrust
  低安全级别的安全区域，安全级别为 5。
- 非军事化区域 DMZ（Demilitarized Zone）
  中等安全级别的安全区域，安全级别为 50。
- 受信区域 Trust
  较高安全级别的安全区域，安全级别为 85。
- 本地区域 Local
  最高安全级别的安全区域，安全级别为 100。

这四个区域无需创建，也不能删除，同时其安全级别也不能重新设置。

根据实际组网需要，用户可以自行创建安全区域并定义其安全级别。

说明

- DMZ 这一术语起源于军方，指的是介于严格的军事管制区和松散的公共区域之间的一种有着部分管制的区域。
- 防火墙引用了这一术语，指代一个逻辑上和物理上都与内部网络和外部网络分离的区域。该区域可以放置需要对外提供网络服务的设备，如 WWW Server、FTP Server 等。上述服务器如果放置于外部网络，则防火墙无法保障它们的安全；如果放置于内部网络，外部恶意用户则有可能利用某些服务的安全漏洞攻击内部网络。DMZ 区域很好地解决了服务器的放置问题。

2.2.3 接口、网络与安全区域的关系

注意

- 系统不允许两个安全区域具有相同的安全级别。
- 系统不允许同一接口属于两个不同的安全区域。

接口、网络与安全区域的关系如下：

- 接口与安全区域的关系
  一个安全区域可以包括一个或多个接口，具有一个安全级别。
  除 Local 区域外，使用其他安全区域前，都需要将安全区域分别与防火墙的特定接口关联，即将接口加入安全区域。
- 网络与安全区域的关系

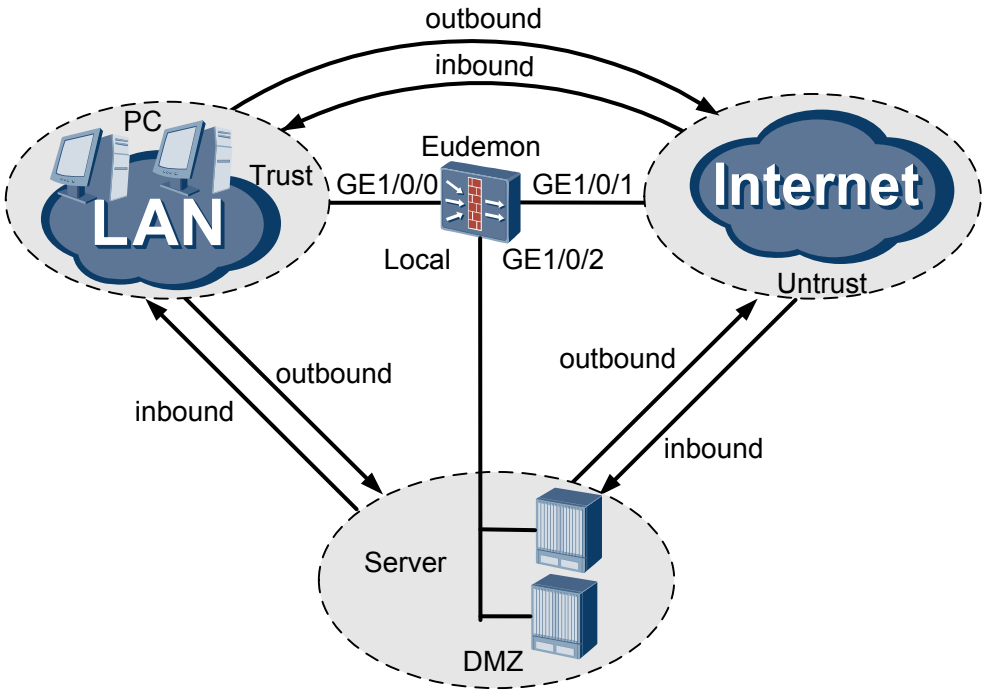
安全区域与各网络的关联遵循如下原则：

- 需要保护的网络应安排在安全级别较高的区域，如 Trust 区域。
- 外部网络应安排在安全级别较低的区域，如 Untrust 区域。
- 对外提供有条件服务的网络应安排在中等安全级别的区域，如 DMZ 区域。
- Local 区域不包含任何接口，防火墙设备本身即可认为是 Local 区域。

- 接口、网络与安全区域之间的关系

  接口、网络与安全区域之间的关系如图 2-4 所示。

图 2-4 接口、网络和安全区域的关系示意图



2.2.4 数据流方向

两个安全区域之间（简称安全域间）的数据流分两个方向：

- 入方向（inbound）

  数据由低安全级别的安全区域向高安全级别的安全区域传输的方向。

- 出方向（outbound）

  数据由高安全级别的安全区域向低安全级别的安全区域传输的方向。

不同安全级别的安全区域间的数据流动都将激发防火墙进行安全策略的检查。可以事先为同一安全域间的不同方向设置不同的安全策略，当有数据流在此安全域间的两个不同方向上流动时，将触发不同的安全策略检查。

在 Eudemon 上，判断数据传输是出方向还是入方向，总是相对高安全级别的安全区域一侧而言。数据流的具体出、入方向如下：

- 从 Local 安全区域到 Trust 安全区域的数据流动方向为出方向，反之为入方向。
- 从 Local 安全区域到 DMZ 安全区域的数据流动方向为出方向，反之为入方向。

- 从 Local 安全区域到 Untrust 安全区域的数据流动方向为出方向，反之为入方向。
- 从 Trust 安全区域到 DMZ 安全区域的数据流动方向为出方向，反之为入方向。
- 从 Trust 安全区域到 Untrust 安全区域的数据流动方向为出方向，反之为入方向。
- 从 DMZ 安全区域到 Untrust 安全区域的数据流动方向为出方向，反之为入方向。

说明

- 在防火墙上，当报文从高安全级别的安全区域向低安全级别的安全区域发起连接时，如果允许高安全级别的安全区域用户自由访问外部网络，可以配置域间缺省过滤规则为允许报文通过。
- 路由器上数据流动方向的判定是以接口为主：由接口发送的数据方向称为出方向；由接口接收的数据方向称为入方向。这也是路由器有别于防火墙的重要特征。

3 安全特性

关于本章

3.1 ACL

3.1.1 定义

防火墙必须具备控制网络数据流的能力，用于满足安全性、QoS（Quality of Service）需求和各种策略制定等各个方面。实现数据流控制的手段之一是使用访问控制列表 ACL。

ACL 是由 permit 或 deny 语句组成的一系列有顺序的规则，这些规则主要通过数据包的源地址、目的地址、端口号、上层协议等信息来描述。

3.1.2 应用

作为数据流控制的一种常用的手段，ACL 被应用于很多方面。例如：

- 包过滤

  包过滤作为一种网络安全保护机制，用于在两个不同安全区域之间控制流入和流出的数据。为了实现包过滤，需要通过 ACL 定义一系列的过滤规则，然后将 ACL 规则应用于防火墙的不同安全区域之间。防火墙转发数据包时，会将数据包的信息（例如源地址/目的地址、源端口/目的端口和上层协议等）与设定的 ACL 规则进行比较，根据比较的结果决定对该数据包进行转发还是丢弃处理。

- NAT

  NAT（Network Address Translation）是将数据报报头中的 IP 地址转换为另一个 IP 地址的过程，主要用于实现内部网络（私有 IP 地址）访问外部网络（公有 IP 地址）以及解决 IP 地址缺乏的问题。

  在实际应用中，我们可能仅希望某些内部主机（具有私有 IP 地址）具有访问 Internet（外部网络）的权限，而其他内部主机则不允许。这种情况是通过将 ACL 和 NAT 地址池进行关联来实现的，即只有满足 ACL 条件的数据报文才可以进行地址转换，从而有效地控制地址转换的使用范围。

- IPSec

  IPSec 协议族是 IETF（Internet Engineering Task Force）制定的一系列协议，它通过 IP 层的加密与数据源验证机制，确保在 Internet 上参与通信的两个网络节点之间传输的数据包具有私有性、完整性和真实性。

  IPSec 能够对不同的数据流施加不同的安全保护，例如对不同的数据流使用不同的安全协议、算法和密钥。实际应用中，数据流首先通过 ACL 来定义，匹配同一个 ACL 的所有流量在逻辑上作为一个数据流。然后，通过在安全策略中引用该 ACL，从而确保指定的数据流受到保护。

- QoS

  QoS 用来评估服务方满足客户需求的能力。在 Internet 上保证 QoS 的有效办法是增加网络层在流量控制和资源分配上的功能，为有不同服务需求的业务提供有区别的服务。

流分类是有区别地进行服务的前提和基础。实际应用中，首先制定流分类策略（规则），流分类规则既可以使用 IP 报文头的 ToS（Type of Service）字段内容来识别不同优先级特征的流量，也可以通过 ACL 定义流分类的策略，例如综合源地址/目的地址/MAC 地址、IP 协议或应用程序的端口号等信息对流进行分类。然后，在流量监管、流量整形、拥塞管理和拥塞避免等具体实施上引用流分类策略或 ACL。

- 路由策略

  路由策略是指在发送与接收路由信息时所实施的策略，它能够对路由信息进行过滤。

  路由策略有多种过滤方法。其中，ACL 作为它的一个重要过滤器被广泛使用，即用户使用 ACL 指定一个 IP 地址或子网的范围，作为匹配路由信息的目的网段地址、源网段地址或下一跳地址。

3.1.3 步长设定

配置 Eudemon 的 ACL 时，可以为一个 ACL 规则组指定一个“步长”。步长的含义是：自动为 ACL 子规则分配编号的时候，每个 ACL 规则组的子规则编号之间的差值。如果步长设定为 5，子规则编号分配是按照 5、10、15……这样的规则分配的。默认情况下，ACL 规则组的步长为 5。

只有 ACL 规则组下没有子规则时，才能改变步长。ACL 规则组下有子规则时，必须删除已经存在的子规则，然后再使用 **step** 命令改变步长或者使用 **undo step** 命令将步长变为默认值。

使用步长设定的好处是，可以方便在子规则之间插入新的规则。例如配置好了 4 个规则，子规则编号为：5、10、15、20。此时希望能在第一条规则之后插入一条规则，则可以使用 **rule 6 xxxx** 命令在 5 和 10 之间插入一条编号为 6 的子规则。

3.1.4 Eudemon 8080E/8160E 支持的 ACL

支持的 ACL 类型

Eudemon 8080E/8160E 支持的 ACL 类型如表 3-1 所示。

表 3-1 Eudemon 8080E/8160E 支持的 ACL 类型

ACL 类型	数字范围	描述
基本 ACL	2000 ～ 2999	仅使用源地址信息定义数据流。
高级 ACL	3000 ～ 3999	可以根据报文的源 IP 地址、目的 IP 地址、源端口号、目的端口号、上层协议信息（例如 ICMP 协议的消息类型、消息码）等多种元素组合定义规则。

匹配顺序

一个 ACL 规则可以由多条 **permit** 或 **deny** 语句组成，每一条语句描述的规则是不相同的，这些规则可能存在重复或矛盾的地方。在将一个数据包和 ACL 规则进行匹配的时候，需要确定规则的匹配顺序。Eudemon 8080E/8160E 按照如下原则进行匹配：

- 在同一 ACL 规则组中，rule-id 小的规则被优先匹配。
- 不同 ACL 规则组，按照用户配置 ACL 规则的先后顺序进行匹配。

数据流一旦与一条 rule 规则匹配成功，将不再继续向下一规则匹配。防火墙将根据该 rule 规则的动作，对数据流进行后续操作。

源地址和通配符掩码

在使用 ACL 时，需要指定源地址。源地址可以指一台主机、一组主机、整个子网或整个网络。源地址的范围是由通配符掩码字段来确定的。

通配符掩码不同于子网掩码，它是以 0 表示必须匹配的位，以 1 表示无需匹配的位，即先将 source-wildcard 取反，然后和 source-address 进行“与”运算，从而得出源地址范围。例如：

source-address = 192.168.15.16　　11000000.10101000.00001111.00010000
source-wildcard = 0.0.0.255　　00000000.00000000.00000000.11111111
源地址范围 = 192.168.15.0　　11000000.10101000.00001111.00000000

any 的含义指来自任何地址的包都符合匹配条件，此时 *source-wildcard* 取 255.255.255.255，*source-address* 可以取任意地址。

基于时间段的 ACL 规则

在允许或拒绝用户对资源的访问方面，当今的网络安全策略需要有更大的控制灵活性。例如在某些情况下，系统管理员可能只想在某些特定时间段才允许某些数据流通过，或只允许用户在一天的某些时间段访问某些资源。此时可以使用基于时间段的 ACL 规则。

引用地址组和端口组的 ACL 规则

为简化 ACL 规则的配置和维护，防火墙支持引用地址组和端口组的 ACL。

通过地址组和端口组描述的一条 rule 规则，在使用时体现为具有相同优先级的传统 rule 规则的集合。具体公式为：

新集合中相同优先级的 rule 规则元素个数=地址组 1 元素个数×地址组 2 元素个数×端口组 1 元素个数×端口组 2 元素个数

例如，配置两个地址组和一个端口组，分别包含两个元素，并在 ACL 3000 中应用。

```
<Eudemon> system-view
[Eudemon] ip address-set a1
[Eudemon-address-set-a1] address 1 1.1.1.1 0
[Eudemon-address-set-a1] address 2 2.2.2.1 0
[Eudemon-address-set-a1] quit
[Eudemon] ip address-set a2
[Eudemon-address-set-a2] address 1 3.3.3.1 0
[Eudemon-address-set-a2] address 2 4.4.4.1 0
[Eudemon-address-set-a2] quit
[Eudemon] ip port-set p1 protocol tcp
[Eudemon-tcp-port-set-p1] port 1 eq 21
[Eudemon-tcp-port-set-p1] port 2 eq 22
[Eudemon-tcp-port-set-p1] quit
```

```
[Eudemon] acl 3000
[Eudemon-acl-adv-3000] rule permit tcp source address-set a1 destination address-set a2 destination-port port-set p1
```

上述命令的配置效果与如下几个 ACL 规则的配置效果相同：

```
<Eudemon> system-view
[Eudemon] acl 3000
[Eudemon-acl-adv-3000] rule permit tcp source 1.1.1.1 0 destination 3.3.3.1 0 destination-port eq 21
[Eudemon-acl-adv-3000] rule permit tcp source 1.1.1.1 0 destination 3.3.3.1 0 destination-port eq 22
[Eudemon-acl-adv-3000] rule permit tcp source 1.1.1.1 0 destination 4.4.4.1 0 destination-port eq 21
[Eudemon-acl-adv-3000] rule permit tcp source 1.1.1.1 0 destination 4.4.4.1 0 destination-port eq 22
[Eudemon-acl-adv-3000] rule permit tcp source 2.2.2.1 0 destination 3.3.3.1 0 destination-port eq 21
[Eudemon-acl-adv-3000] rule permit tcp source 2.2.2.1 0 destination 3.3.3.1 0 destination-port eq 22
[Eudemon-acl-adv-3000] rule permit tcp source 2.2.2.1 0 destination 4.4.4.1 0 destination-port eq 21
[Eudemon-acl-adv-3000] rule permit tcp source 2.2.2.1 0 destination 4.4.4.1 0 destination-port eq 22
```

3.2 安全策略

3.2.1 包过滤

包过滤作为一种网络安全保护机制，用于在两个不同安全级别的网络之间控制流入和流出网络的数据。防火墙转发数据包时，先检查包头信息（例如包的源地址/目的地址、源端口/目的端口和上层协议等），然后与设定的规则进行比较，根据比较的结果决定对该数据包进行转发还是丢弃处理。

为了实现数据包过滤，需要配置一系列的过滤规则。采用 ACL 定义过滤规则，然后将 ACL 应用于防火墙不同区域之间，从而实现包过滤。

3.2.2 ASPF

ASPF 是针对应用层的包过滤，即基于状态的报文过滤。它和普通的静态防火墙协同工作，以便于实施内部网络的安全策略。ASPF 能够检测试图通过防火墙的应用层协议会话信息，阻止不符合规则的数据报文穿过。

为保护网络安全，基于 ACL 规则的包过滤可以在网络层和传输层检测数据包，防止非法入侵。

ASPF 能够检测应用层协议的信息，并对应用的流量进行监控。ASPF 通过维护会话的状态和检查会话报文的协议和端口号等信息，阻止恶意的入侵。

在 Eudemon 8080E/8160E 中，ASPF 还提供以下功能：

- Java 阻断（Java Blocking），保护网络不受有害 Java Applets 的破坏。
- ActiveX 阻断（ActiveX Blocking），保护网络不受有害 ActiveX 的破坏。

ASPF 支持的协议包括：DNS、FTP、H323、MGCP、MMS、MSN、PPTP、QQ、RTSP、SIP、SQLNET、ILS、NETBIOS、RSH、user-defined。

QQ/MSN 聊天的检测

目前，为了节省有限的 IP 地址资源，绝大部分网络均部署了 NAT 设备以提供地址转换。对于纯文本聊天，由于在 QQ/MSN 服务器中保存了聊天用户的地址映射信息，信息交互可以顺利地通过 QQ/MSN 服务器中转。

聊天用户可能传送文件或进行音频/视频聊天，如果 QQ/MSN 服务器中转此类报文将消耗过多资源，无法保证对纯文本聊天报文的正常中转。QQ/MSN 服务器希望两个用户通过网络设备直接交互大流量的文件/音频/视频信息，但是由于一般 NAT 设备需要转换聊天用户的地址信息，无法实现该需求。

配置 Eudemon 的 NAT 功能时，可以在相关安全域间启动 QQ/MSN 检测功能，防火墙在 QQ/MSN 聊天启动时则会创建地址映射关系，从而使两个私网用户直接传送文件和进行音频/视频聊天。

三元组 ASPF

Eudemon 相当于一个五元组的 NAT 设备，即防火墙上的每个会话的建立都需要五元组：源 IP 地址、源端口、目的 IP 地址、目的端口、协议号。只有这些元素都具备了，会话才能建立成功，报文才能通过。而一些象 QQ、MSN 等实时通讯工具，通过 NAT 设备，却需要按三元组处理：源 IP 地址，源端口、协议号。Eudemon 为了适配类似 QQ、MSN 等通讯机制，变五元组处理方式为三元组方式，让类似 QQ、MSN 等的通讯方式能够正常的穿越。

除 QQ、MSN 穿越 NAT 设备外，其他仅使用源 IP 地址、源端口、协议号的会话，如 TFTP（Trivial File Transfer Protocol），同样需要配置防火墙三元组 ASPF。

3.2.3 黑名单

黑名单是防火墙一个重要的安全特性，其特点为可以由 Eudemon 动态地进行添加或删除。同基于 ACL 的包过滤功能相比，由于黑名单仅对 IP 地址进行匹配，可以以很高的速度实现黑名单表项匹配，从而快速有效地屏蔽特定 IP 地址的用户。

黑名单表项有如下两种创建方式：

- 通过命令行手工创建。
- 通过攻击防范模块动态创建。

当防火墙根据报文的行为特征察觉到特定 IP 地址的用户的攻击企图后，主动将其插入黑名单表项，过滤从该 IP 地址发送的报文，从而保障网络安全。

3.2.4 端口映射

应用层协议一般使用通用的端口号（知名端口号）进行通信。端口映射 PAM（Port to Application Mapping）允许用户针对不同的应用在系统定义的端口号之外定义一组新的

端口号。端口映射提供了一些机制来维护和使用用户定义的端口配置信息。端口映射能够对不同的应用协议创建和维护一张系统定义（system-defined）和用户定义（user-defined）的端口映射表。

端口映射支持基于基本访问控制列表（ACL）的主机端口映射。

主机端口映射是对去往某些特定主机的报文建立自定义端口号和应用协议的映射，例如：将去往 10.110.0.0 网段的主机使用 8080 端口的 TCP 报文识别为 HTTP 报文。主机的范围可由基本 ACL 指定。

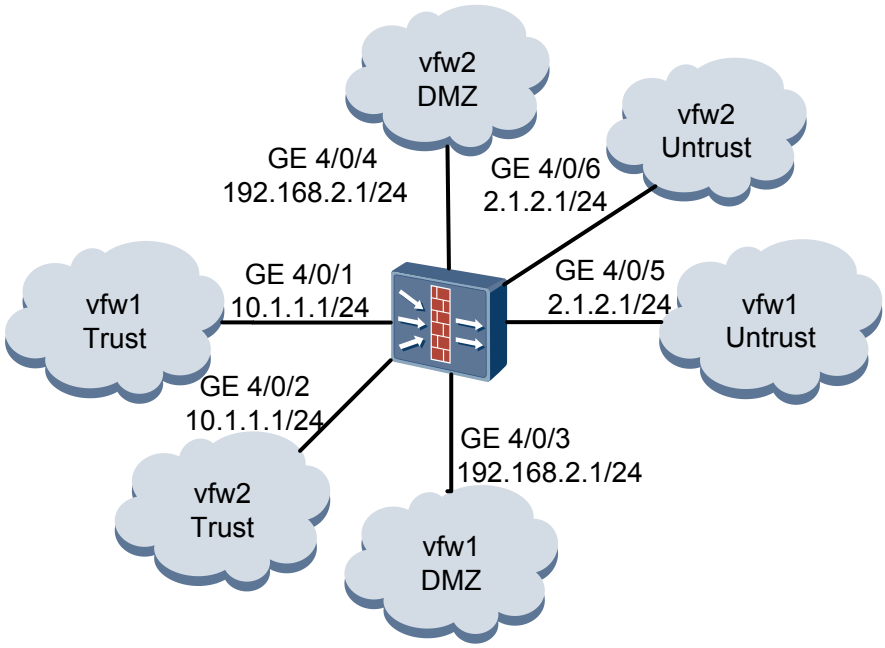
3.2.5 虚拟防火墙

近年来小型私有网络不断增加，这些网络一般对应小型企业。此类用户有如下特点：

- 有较强的安全防范需求。
- 经济上无法负担一台专有安全设备。

华为公司推出 Eudemon 多实例解决方案。防火墙多实例的配置案例组网图如图 3-1 所示。图 3-1 中将一台防火墙从逻辑上划分为多个 VPN 实例，向多个小型私有网络提供相对独立的安全保障。对于网络运营商，可以采用虚拟防火墙技术向多个小型私有网络提供相互隔离的网络安全保障服务。

图 3-1 虚拟防火墙配置组网图



每台虚拟防火墙都是 VPN 实例（VPN-Instance）、安全实例和配置实例的综合体。它能够为用户提供私有的路由转发平面、安全服务和配置管理平面。

VPN 实例

VPN 实例为虚拟防火墙用户提供相互隔离的 VPN 路由，与虚拟防火墙一一对应。这些 VPN 路由将为各虚拟防火墙接收的报文提供路由支持。

安全实例

安全实例为虚拟防火墙用户提供相互隔离的安全服务，与虚拟防火墙一一对应。这些安全实例具备私有的接口、安全区域、安全域间、ACL 和 NAT 地址池，并能为虚拟防火墙用户提供地址绑定、黑名单、NAT、包过滤、统计、攻击防范、ASPF 等私有的安全服务。

配置实例

配置实例为虚拟防火墙用户提供相互隔离的配置管理平面，与虚拟防火墙一一对应。这些配置实例使虚拟防火墙用户能够登录到各自的虚拟防火墙，并管理和维护上述私有 VPN 路由和安全实例。

3.3 NAT

3.3.1 NAT 简介

NAT 是将 IP 数据报报头中的 IP 地址转换为另一个 IP 地址的过程，主要用于实现内部网络（私有 IP 地址）访问外部网络（公有 IP 地址）的功能。

在实际应用中，内部网络一般使用私有地址。RFC（Request For Comments）1918 为私有、内部的使用留出了三个 IP 地址块。具体如下：

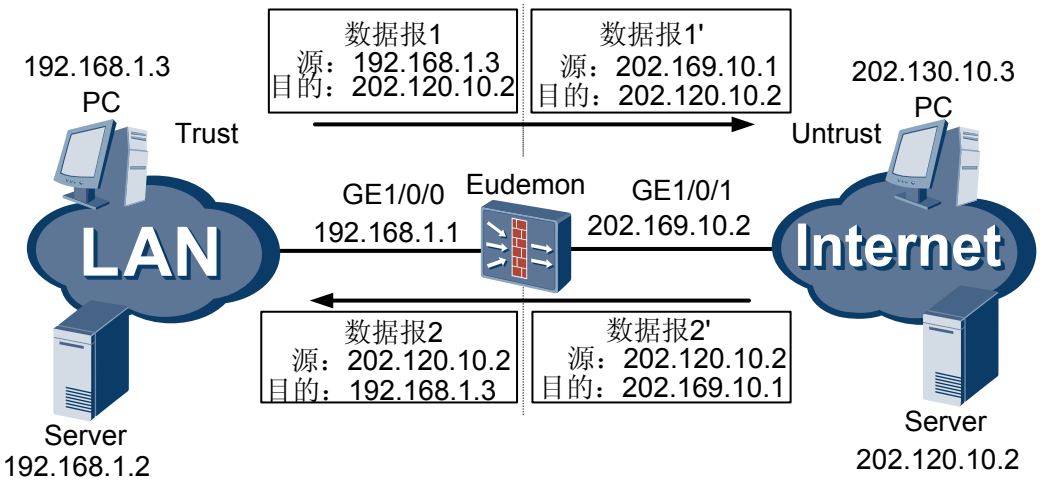
- A 类 10.0.0.0 ～ 10.255.255.255（10.0.0.0/8）
- B 类 172.16.0.0 ～ 172.31.255.255（172.16.0.0/12）
- C 类 192.168.0.0 ～ 192.168.255.255（192.168.0.0/16）

上述三个范围内的地址不会在 Internet 上被分配，因而可以不必向 ISP（Internet Service Provider）或注册中心申请而在公司或企业内部自由使用。

NAT 主要用于实现内部网络访问外部网络的功能。通过应用 NAT，能够使多数的私有 IP 地址转换为少数的公有 IP 地址，减缓可用 IP 地址空间枯竭的速度。

图 3-2 描述了一个基本的 NAT 应用。

图 3-2 地址转换的基本过程



NAT 设备（如 Eudemon）处于私有网络和公有网络的连接处。内部 PC 与外部服务器的交互报文全部通过该 NAT 设备。地址转换的过程如下。

1. 内部 PC（192.168.1.3）发往外部服务器（202.120.10.2）的数据报 1 到达 NAT 设备后，NAT 设备查看报头内容，发现该数据报头中的信息匹配上了某条 NAT 策略。
2. NAT 设备将数据报 1 的源地址字段的私有地址 192.168.1.3 换成一个可在 Internet 上选路的公有地址 202.169.10.1，发送到外部服务器，同时在网络地址转换表中记录这一地址转换映射。
3. 外部服务器收到数据报 1’后，向内部 PC 发送应答报文，即数据报 2’，初始目的地址为 202.169.10.1。
4. 数据报 2’到达 NAT 设备后，NAT 设备查看报头内容，查找当前网络地址转换表的记录，用私有地址 192.168.1.3 替换目的地址，发送给内部 PC。

上述的 NAT 过程对 PC 和外部服务器来说是透明的。内部 PC 认为与外部服务器的交互报文没有经过 NAT 设备的干涉；外部服务器认为内部 PC 的 IP 地址就是 202.169.10.1，并不知道存在 192.168.1.3 这个地址。

Eudemon 支持的 NAT 功能包括对源 IP 地址进行转换，和对目的 IP 地址进行转换两种方式。

其中，基于源 IP 地址的转换可以从以下两个方面进行划分：

- 转换的方向。
- 端口是否转换。

按照转换的方向可以将源 IP 地址转换划分为以下两类：

- Inbound 方向

  数据包由低安全级别的安全区域向高安全级别的安全区域方向传输时，基于源 IP 地址进行的转换。
- Outbound 方向

  数据包由高安全级别的安全区域向低安全级别的安全区域方向传输时，基于源 IP 地址进行的转换。

按照端口是否转换可以将源 IP 地址转换划分为以下两类：

- No-PAT (Port Address Translation)方式的 NAT

主要用于一对一的 IP 地址的转换，端口不进行转换。

- NAPT(Network Address Port Translation)方式的 NAT

  主要用于多对一或多对多的地址转换，转换时地址和端口号同时进行转换。

按照功能不同，可以将基于目的 IP 地址的转换分为以下两类：

- NAT Server

  主要应用于实现私网服务器以公网 IP 地址对外提供服务的功能。

- 目的 NAT

  主要应用于实现手机用户上网时，需要修改目的网关地址的功能。

3.3.2 NAT 地址池及转换控制

NAT 地址池是一些连续的 IP 地址集合，当来自私网的报文通过地址转换到公网 IP 时，将会选择地址池中的某个地址作为转换后的地址。

NAT 地址池中的地址可以是一个公网 IP 地址，也可以是多个公网 IP 地址。Eudemon 的一个地址池中最多可以包含 4096 个地址。

在配置域间 NAT 或域内 NAT 时，需要首先配置 NAT 地址池，然后将 NAT 地址池与 ACL 绑定，通过选择不同的参数，实现不同功能的 NAT。

在实际应用中，用户可能希望其内部网络中某些主机具有访问 Internet 的权利，而某些主机没有。即当 NAT 进程查看数据报报头内容时，如果发现源 IP 地址是为那些不允许访问外部网络的内部主机所拥有的，将不进行 NAT 转换。这就是一个对地址转换进行控制的问题。

将一个地址池和一个 ACL 规则关联起来，即指定了“具有某些特征的 IP 报文”才可以使用“这个地址池中的地址”。当报文到达 Eudemon 时，Eudemon 首先根据访问列表判定是否是允许的数据包，然后根据转换关联找到与之对应的地址池，这样就把一个地址转换成这个地址池中的另一个地址，完成地址转换过程。

3.3.3 NAT No-PAT

NAT No-pat 也可以称为“一对一地址转换”，在地址转换过程中，数据包的源 IP 地址由私网地址转换为公网地址，但端口号不做转换。

例如，地址池中的公网 IP 地址只有两个，当所有私网的主机访问公网时，只能拥有两个公网 IP 地址，因此，这种情况只允许最多有两台私网主机同时访问公网，其他的私网主机要等到公网 IP 地址被释放后，才可以再做地址转换访问公网。

当配置了 No-PAT 方式的 NAT 后，Eudemon 会为有流量的私网 IP 地址分配一个公网地址，同时建立 Server-map 表。Server-map 表用于存放私网 IP 地址与公网 IP 地址的映射关系。后续从该私网 IP 发出的所有报文，都将命中 Server-map 表转换成该公网地址，这种地址转换关系是一一对应的。

3.3.4 NAPT

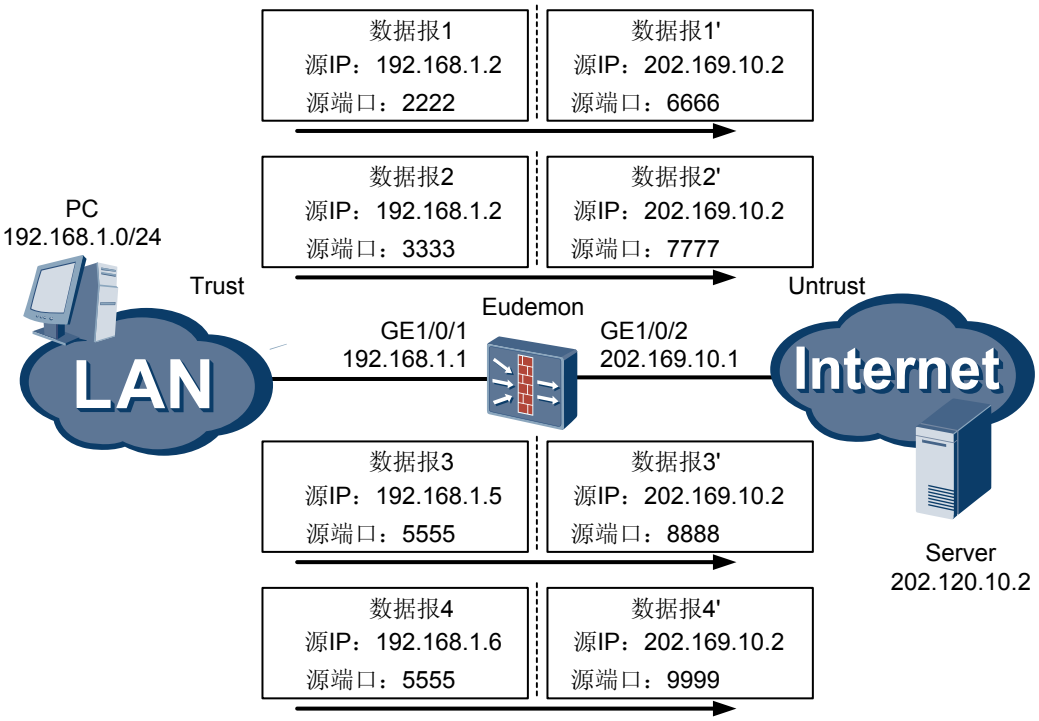
NAT No-PAT 功能可以实现 Eudemon 一对一的地址转换，但是在实际应用中，在公网 IP 地址非常有限的情况下，如果大量的私网用户需要同时访问 Internet，则 NAT No-PAT 功能无法满足用户需求。

Eudemon 的 NAPT 功能可以解决多个私网 IP 地址同时映射为少个或一个公网 IP 地址的问题。

NAPT 也可以称之为“地址复用”。通过配置 NAPT 功能，Eudemon 同时对端口号和 IP 地址进行映射，允许多个私网 IP 地址同时映射到同一个公网 IP 地址，相同的公网 IP 地址通过不同的端口号区分映射不同的私网 IP 地址，从而实现多对一或多对多的地址转换。

下面对 NAPT 转换原理进行说明。

图 3-3 NAPT 转换原理示意图



如图 3-3 所示，四个带有私网 IP 地址的数据报到达 Eudemon，其中数据报 1 和 2 来自同一个私网 IP 地址但有不同的源端口号，数据报 3 和 4 来自不同的私网 IP 地址但具有相同的源端口号。通过 NAT 转换，四个数据报都被转换到同一个公网 IP 地址，但每个数据报都赋予了不同的源端口号，因而仍保留了报文之间的区别。当回应报文到达 Eudemon 时，NAT 进程仍能够根据回应报文的目的地址和端口号来区别该报文应转发到的相应的内部主机。

3.3.5 NAT Server

NAT 隐藏了内部网络的结构，具有“屏蔽”内部主机的作用。但是在实际应用中，可能需要提供给外部一个访问内部主机的机会，如提供给外部一台 Web 服务器，或是一台 FTP 服务器。使用 NAT 可以灵活地添加 NAT Server。Eudemon 提供两种方式为 NAT Server 指定外部地址：

- 可以使用 202.169.10.10 作为 Web 服务器的外部地址。
- 可以使用 202.110.10.12:8080 作为 Web 服务器的外部地址。

Eudemon 的 NAT 能够为外部网络用户提供访问的 NAT Server。外部用户访问 NAT Server 时，有如下两部分操作：

- Eudemon 将外部用户的请求报文的目的地址转换成 NAT Server 的私有地址。
- Eudemon 将 NAT Server 的回应报文的源地址（私网地址）转换成公网地址。

Eudemon 支持为外部用户提供多台同样的服务器，例如，提供多台 Web 服务器。

说明

允许外部用户访问的 NAT Server 通常置于 Eudemon 的 DMZ 区。正常情况下不允许这个区域中的设备主动向外发起连接。

3.3.6 目的 NAT

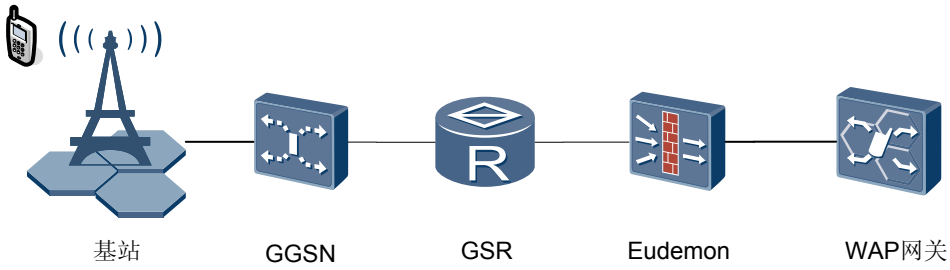
手机用户需要通过登录 WAP（Wireless Application Protocol）网关来实现上网的功能。目前，大量用户直接从国外购买手机使用，这些手机出厂时，缺省设置的 WAP 网关地址与本国 WAP 网关地址不符，且无法自行修改，从而导致用户不能移动上网。

为解决这一问题，无线网络中，在 WAP 网关与用户之间部署 Eudemon。通过在 Eudemon 上配置目的 NAT 功能，使这部分手机用户能够正常获取网络资源。

如图 3-4 所示，当手机用户上网时，目的 NAT 处理过程如下：

1. 当手机用户上网时，请求报文经过基站及其他中间设备到达 Eudemon。
2. 到达 Eudemon 的报文如果匹配 Eudemon 上所配置的目的 NAT 策略，则将此数据报文的目的 IP 地址转换为已配置好的 WAP 网关的 IP 地址，并送往 WAP 网关。
3. WAP 网关对手机客户端提供相应的业务服务（如视频服务、网页服务等），并将回应报文发往 Eudemon。
4. 回应报文在 Eudemon 上命中会话，Eudemon 转换该报文的源 IP 地址，并将该报文发往手机用户，完成一次通信。

图 3-4 手机用户上网目的 NAT 组网图



3.3.7 域内 NAT

典型应用一

在配置 NAT Server 过程中，可能会遇到这样的情况，当用户和内部服务器处于同一个安全区域，并且 IP 地址在同一网段时，当用户访问服务器时，请求报文会不经过 Eudemon 而直接到达内部服务器。

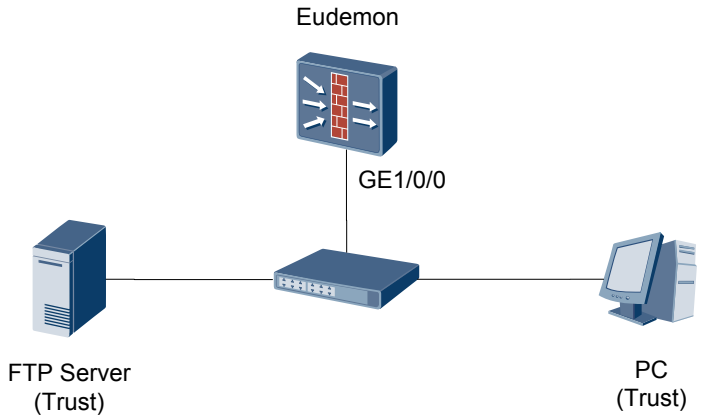
如图 3-5 所示，FTP 服务器和 PC 均在防火墙的 Trust 安全区域，二者通过交换机与防火墙同一个接口相连。FTP 服务器通过公网地址对用户提供 FTP 服务，如果 PC 和 FTP 服

务器都具有内网地址，且位于同一个网段，那么当 PC 访问 FTP 服务器时，请求报文会直接到达 FTP 服务器，而不经过 Eudemon。

为避免这一情况，保证统一安全区域的用户访问 FTP 服务器的报文也要经过 Eudemon，那么，就需要在 Eudemon 上配置域内 NAT 功能。

当 PC 访问 FTP 服务器的公网地址时，PC 的地址也进行地址转换，由私网地址转换为公网地址，以保证 PC 和 FTP 服务器交互的所有报文都经过 Eudemon，同时保证 Eudemon 对报文正确处理。

图 3-5 内部服务器供域内用户访问典型组网图

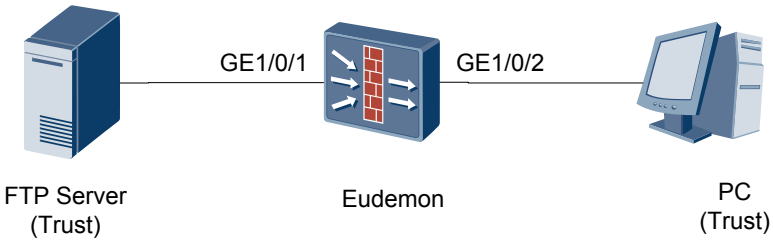


典型应用二

如图 3-6 所示，FTP 服务器和 PC 均在防火墙的 Trust 安全区域，二者分别与防火墙的不同接口相连。PC 访问 FTP 服务器时，私网地址需要转换为公网地址。

通过配置域内 NAT 功能，可以实现由 PC 发出的报文源 IP 地址私网地址转换为公网地址，从而实现同一安全区域内的地址转换。

图 3-6 内部服务器供域内用户访问典型组网图二



3.3.8 双向 NAT

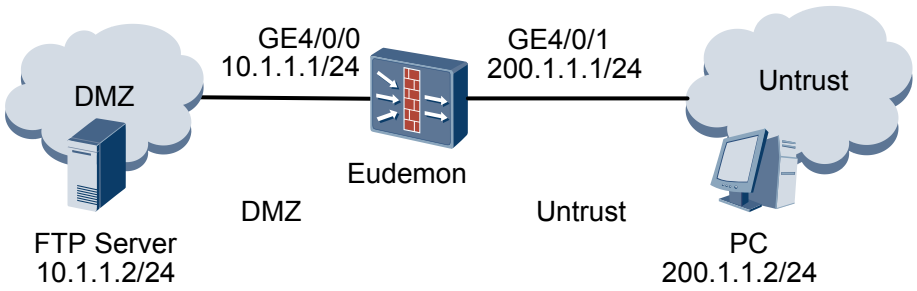
当既要对报文的源 IP 地址做 NAT，又要对此报文的目的 IP 地址做 NAT 时，则需要配置双向 NAT。

双向 NAT 应用环境如下：

- 低优先级区域的用户访问公网地址时将报文的目的地址转换为 NAT Server 服务器的私网地址，但 NAT Server 服务器需要配置到该公网地址的路由。也可以配置从低优先级区域到高优先级区域方向的 NAT，即 inbound 方向的 NAT，实现低优先级区域的用户访问公网地址。此方法可以简化配置，避免配置到公网地址的路由。
- 同一个安全区域内的访问需要作 NAT，则需要配置域内 NAT 和 NAT Server 功能。

如图 3-7 所示，在 Eudemon 上配置从低优先级区域到高优先级区域方向的 NAT。以配置从 Untrust 区域到 DMZ 区域方向的 NAT 为例，进行说明。

图 3-7 从低优先级区域到高优先级区域的 NAT 组网图



当 Untrust 区域的用户访问 DMZ 的服务器时，有如下两部分操作：

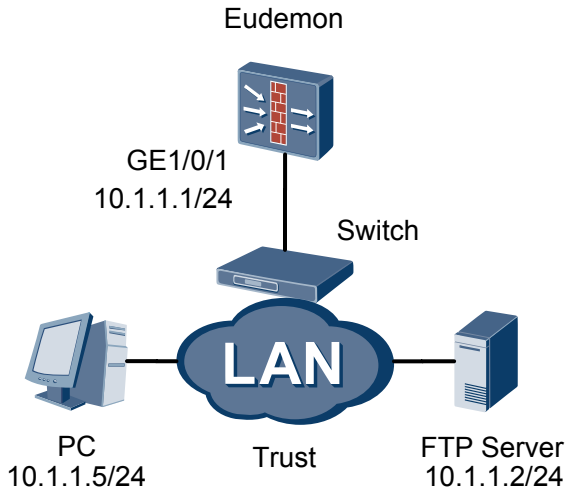
- Eudemon 将外部用户的请求报文的目的地址转换成内部服务器的私有地址，源地址转换成地址池中的地址（私网地址）。
- Eudemon 将内部服务器的回应报文的源地址（私网地址）转换成公网地址，目的地址（私网地址）转换为公网地址。

说明

允许外部用户访问的内部服务器通常置于 Eudemon 的 DMZ 区域。正常情况下不允许这个区域中的设备主动向外发起连接。

如图 3-8 所示，在 Eudemon 上配置同一个区域内的 NAT。以配置 Trust 域内的 NAT 为例，进行说明。

图 3-8 域内 NAT 组网图



当 Trust 域的用户访问 Trust 域的服务器时，有如下两部分操作：

- Eudemon 将内部用户的请求报文的目的地址转换成内部服务器的私有地址，源地址转换成地址池中的地址（公网地址）。
- Eudemon 将内部服务器的回应报文的源地址（私网地址）转换成公网地址，目的地址（公网地址）转换为私网地址。

3.3.9 NAT ALG

通常 NAT 只能对 IP 报文的头部地址和 TCP/UDP 头部的端口信息进行转换，但是对于一些特殊的协议，比如 FTP 等协议，则需要由数据连接和控制连接共同完成，而且数据连接的建立要由控制连接载荷字段中的报文信息动态的决定，这就需要能够根据控制连接的载荷字段中的报文解析出数据连接要使用的地址和端口号，也就是说 Eudemon 必须能够辨识 FTP 应用载荷字段中包含的端口号和地址信息，才能进行有效的 NAT 处理，否则可能导致 NAT 功能失败。

为解决这一问题，当 NAT 功能与 FTP、MSN、PPTP、QQ、RTSP、TFTP 等协议共同使用时，需要在 Eudemon 上配置 NAT ALG（Application Level Gateway）功能，通过配置 NAT ALG 功能，Eudemon 对数据包进行深度解析，并改变封装在 IP 报文数据部分中的 IP 地址和端口号信息，从而实现 NAT 功能。

域间 NAT ALG 支持的协议包括：DNS、FTP、H323、MGCP、MMS、MSN、PPTP、QQ、RTSP、SIP、SMTP、SQLNET、user-defined。

域内 NAT ALG 支持的协议包括：FTP 和 RTSP。

注意

仅当配置域内 NAT 时，NAT ALG 功能需要在安全区域视图下配置，即域内视图下配置。

3.4 攻击防范

3.4.1 概述

通常的网络攻击，一般是侵入或破坏网上的服务器（主机），盗取服务器的敏感数据或干扰破坏服务器对外提供的服务；也有直接破坏网络设备的网络攻击，这种破坏影响较大，会导致网络服务异常，甚至中断。

在 Eudemon 中，防火墙的攻击防范功能能够检测出多种类型的网络攻击，并能采取相应的措施保护内部网络免受恶意攻击，保证内部网络及系统的正常运行。

3.4.2 网络攻击类型介绍

网络攻击可分为拒绝服务型攻击、扫描窥探攻击和畸形报文攻击三大类：

- 拒绝服务型攻击
  - DoS（Deny of Service）攻击是使用大量的数据包攻击系统，使系统无法接受正常用户的请求，或者主机挂起不能提供正常的工作。主要 DoS 攻击有 SYN Flood、UDP Flood、DNS Flood 等。拒绝服务攻击和其他类型的攻击不同之处在于：攻击者并不是去寻找进入内部网络的入口，而是阻止合法用户访问资源或设备。
  - DDoS（Distributed Denial of Service）攻击是一种 DoS 攻击。这种攻击是使用攻击者控制的几十台或几百台计算机攻击一台主机，使系统无法接受正常用户的请求，或者挂起不能正常的工作。
- 扫描窥探攻击

  扫描窥探攻击主要包括 IP 地址扫描和端口扫描。IP 地址扫描是指攻击者发送目的地址不断变化的 IP 报文（TCP/UDP/ICMP）来发现网络上存在的主机和网络，从而准确的发现潜在的攻击目标。端口扫描是指通过扫描 TCP 和 UDP 的端口，检测被攻击者的操作系统和潜在服务。攻击者通过扫描窥探就能大致了解目标系统提供的服务种类和潜在的安全漏洞，为进一步侵入系统做好准备。
- 畸形报文攻击

  畸形报文攻击是通过向目标系统发送有缺陷的 IP 报文，使得目标系统在处理这样的 IP 包时会出现崩溃，给目标系统带来损失。主要的畸形报文攻击有 Ping of Death、Teardrop 等。

3.4.3 典型网络攻击介绍

目前网络上的典型攻击有如下几种：

- 拒绝服务型攻击
  - SYN Flood 攻击

    由于资源的限制，TCP/IP 栈的实现只能允许有限个 TCP 连接。而 SYN Flood 攻击正是利用这一点，它伪造一个 SYN 报文（其源地址是伪造的或者是一个不存在的地址）向服务器发起连接，服务器在收到报文后用 SYN-ACK 应答，而此应答发出去后，不会收到 ACK 报文，造成一个半连接。如果攻击者发送大量这样的报文，会在被攻击主机上出现大量的半连接，消耗尽其资源，使正常的用户无法访问。直到半连接超时。在一些创建连接不受限制的实现里，SYN Flood 具有类似的影响，它会消耗掉系统的内存等资源。
  - ICMP Flood 攻击

    攻击者通过向服务器发送大量的 ICMP 消息（如 ping），占用服务器的链路带宽，导致服务器负担过重而不能正常向外提供服务。
  - UDP Flood 攻击

    攻击者通过向服务器发送大量的 UDP 报文，占用服务器的链路带宽，导致服务器负担过重而不能正常向外提供服务。
  - DNS-flood 攻击

    DNS-flood 攻击是一种 DDoS 攻击手段。攻击者在短时间内通过向 DNS（Domain Name System）服务器发送大量的查询报文，使得服务器不得不对所有的查询请求进行回应，进而，导致 DNS 服务器无法为合法用户提供服务。

- 扫描窥探攻击

  地址扫描与端口扫描攻击，即运用扫描工具探测目标地址和端口，对此作出响应的表示其存在，用来确定哪些目标系统确实存活着并且连接在目标网络上，这些主机使用哪些端口提供服务。

- 畸形报文攻击

  - IP 地址欺骗攻击

    为了获得访问权，入侵者生成一个带有伪造源地址的报文。对于使用基于 IP 地址验证的应用来说，此攻击方法可以导致未被授权的用户可以访问目的系统，甚至是以 root 权限来访问。即使响应报文不能达到攻击者，同样也会造成对被攻击对象的破坏。这就造成 IP 地址欺骗攻击。

  - Land 攻击

    所谓 Land 攻击，就是把 TCP SYN 包的源地址和目标地址都配置成受害者的 IP 地址。这将导致受害者向它自己的地址发送 SYN-ACK 消息，结果这个地址又发回 ACK（ACKnowledgement）消息并创建一个空连接，每一个这样的连接都将保留直到超时掉。各种受害者对 Land 攻击反应不同，许多 UNIX 主机将崩溃，Windows NT 主机会变的极其缓慢。

  - Smurf 攻击

    简单的 Smurf 攻击，用来攻击一个网络。方法是发 ICMP 应答请求，该请求包的目标地址配置为受害网络的广播地址，这样该网络的所有主机都对此 ICMP 应答请求作出答复，导致网络阻塞，这比 ping 大包的流量高出一或两个数量级。高级的 Smurf 攻击，主要用来攻击目标主机。方法是将上述 ICMP 应答请求包的源地址改为受害主机的地址，最终导致受害主机雪崩。攻击报文的发送需要一定的流量和持续时间，才能真正构成攻击。理论上讲，网络的主机越多，攻击的效果越明显。Smurf 攻击的另一个变体为 Fraggle 攻击。

  - Fraggle 攻击

    UDP 端口 7（ECHO）和端口 19（Chargen）在收到 UDP 报文后，都会产生回应。在 UDP 的 7 号端口收到报文后，会像 ICMP Echo Reply 一样回应收到的内容；而 UDP 的 19 号端口在收到报文后，会产生一串字符流。就像 ICMP 一样，这两个 UDP 端口都会产生大量无用的应答报文，占满网络带宽。

    攻击者可以向攻击目标所在的网络发送源地址为被攻击主机、而目的地址为其所在子网的广播地址或子网网络地址的 UDP 报文，目的端口号为 7 或 19。子网中启用了此功能的每个系统都会向受害主机发送回应报文，从而产生大量的流量，导致受害网络的阻塞或受害主机的崩溃。

    子网上没有启动这些功能的系统将产生一个 ICMP 不可达消息，因而仍然消耗带宽。也可将源端口改为 Chargen，目的端口为 ECHO，这样会自动不停地产生回应报文，其危害性更大。

  - WinNuke 攻击

    WinNuke 攻击通常向装有 Windows 系统的特定目标的 NetBIOS 端口（139）发送 OOB（Out-Of-Band）数据包，引起一个 NetBIOS 片断重叠，致使目标主机崩溃。还有一种是 IGMP（Internet Group Management Protocol）分片报文，一般情况下，IGMP 报文是不会分片的，所以，不少系统对 IGMP 分片报文的处理有问题。如果收到 IGMP 分片报文，则可能是受到了 WinNuke 攻击。

  - Large ICMP 攻击

    Large ICMP 攻击是指利用尺寸超大的 ICMP 报文对目标系统进行攻击。对于有些设备，在接收到超大 ICMP 报文后，由于处理不当，会造成系统崩溃、死机或重启。

  - Ping of Death 攻击

IP 报文的长度字段为 16 位，这表明一个 IP 报文的最大长度为 65535 字节。对于 ICMP 回应请求报文，如果数据长度大于 65507，就会使 ICMP 数据+IP 头长度(20)+ICMP头长度（8）>65535。对于有些设备，在接收到一个这样的报文后，由于处理不当，会造成系统崩溃、死机或重启。所谓 Ping of Death，就是利用一些尺寸超大的 ICMP 报文对系统进行的一种攻击。

3.4.4 攻击防范原理介绍

DNS-flood 攻击防范原理介绍

Eudemon 根据 DNS 报文查询速率进行 DNS-Flood 攻击检测。限制 DNS 报文的查询速率，对于超过指定速率的 DNS 报文直接丢弃。

SYN Flood 攻击防范原理介绍

Eudemon 通过限制 SYN 报文的速率来防范 SYN Flood 攻击。可以基于接口、IP 地址和安全区域来限制 SYN 报文的速率。

当报文的来回路径一致时，可以开启 TCP 代理（TCP Proxy）功能，对 SYN Flood 攻击进行防范。

当报文的来回路径不一致时，可以配置 TCP 反向源探测，通过对 TCP 协议的源 IP 进行反向探测技术，解决了虚假 IP 发起的 SYN-Flood 攻击防范。

TCP 反向源探测是对攻击者采用虚假 IP 进行攻击的一种有效防范。当启动了 TCP 反向源探测后，防火墙对经过的 TCP SYN 报文进行源 IP 地址的反向探测，确定源 IP 地址为有效 IP 后方允许报文通过。

说明

TCP 反向源探测是基于实接口进行配置，所有虚接口（子接口、trunk、Vlanif 等）都不能配置该功能。

同时配置 TCP 代理功能和 TCP 反向源探测功能时，优先采用 TCP 反向源探测方式进行 SYN Flood 攻击防范。

UDP Flood 攻击防范原理介绍

Eudemon 通过限制 UDP 报文的速率来防范 UDP Flood 攻击。可以基于接口、IP 地址和安全区域来限制 UDP 报文的速率。

ICMP Flood 攻击防范原理介绍

Eudemon 通过限制 ICMP 报文的速率来防范 ICMP Flood 攻击。可以基于接口、IP 地址和安全区域来限制 ICMP 报文的速率。

IP 地址/端口扫描攻击防范原理介绍

Eudemon 对某个 IP 地址或端口的连接速率进行检测，当速率超过阈值时，则认为发生了扫描攻击，将该 IP 地址或端口加入黑名单，禁止建立新的连接。当黑名单老化时间到期后，才允许此 IP 地址或端口建立新的连接。

其他协议报文攻击防范原理介绍

Eudemon 处理非 TCP、UDP、ICMP 协议的报文时不创建会话表，每个报文都相当于首包报文。Eudemon 通过限制此类报文的速率进行攻击防范，超过速率限制的报文将被丢弃。

基于会话的 TCP/UDP/ICMP 攻击防范原理介绍

当 Eudemon 发现 TCP/UDP/ICMP 会话上的报文速度超过设定阈值时，则认为发生了攻击。此时 Eudemon 锁定此会话，后续此会话上不再允许报文通过。当此会话连续 3 秒或者 3 秒以上没有流量时，解锁此会话，后续此会话上的报文可以继续通过。

3.5 认证与授权

3.5.1 概述

认证与授权一般采用客户端/服务器结构。客户端运行于被管理的资源这一侧，服务器上则集中存放用户信息。这种结构既具有良好的可扩展性，又便于用户信息的集中管理。

认证功能

Eudemon 支持如下认证方式：

- 不认证

  对用户非常信任，不对其进行合法性检查。一般不采用这种方式。
- 本地认证

  当用户接入时，根据防火墙本地配置的用户信息（包括用户名、密码及其他属性）进行认证。本地认证的优点是速度快，可以为运营降低成本；缺点是存储信息量受设备硬件条件限制。
- 远端认证

  当用户接入时，支持通过 RADIUS（Remote Authentication Dial In User Service)协议或 HWTACACS(HuaWei Terminal Access Controller Access Control System)协议进行远端认证，由 Eudemon 作客户端，与 RADIUS 服务器通信或 HWTACACS 服务器通信。对于 RADIUS 协议可以采用标准 RADIUS 协议或华为公司的扩展 RADIUS 协议，与 iTELLIN/CAMS(Comprehensive Access Management Sever)等设备配合完成认证。

授权功能

Eudemon 支持以下授权方式：

- 直接授权

  对用户非常信任，直接授权通过。
- 本地授权

  根据防火墙上为本地用户账号配置的相关属性进行授权。
- if-authenticated 授权

  如果用户通过了验证，并且使用的验证方法不是 none，则对用户授权通过。
- RADIUS 认证成功后授权

  由 RADIUS 服务器对用户认证通过后，即可授权。这是由于 RADIUS 协议的认证和授权是绑定在一起的，不能单独使用 RADIUS 进行授权。
- HWTACACS 授权

  由 HWTACACS 服务器对用户进行授权。

3.5.2 RADIUS 协议简介

认证与授权可以用多种协议来实现，最常用的是 RADIUS 协议。RADIUS 协议最初用来管理使用串口和调制解调器的大量分散用户，后来广泛应用于 NAS（Network Access Server）系统。

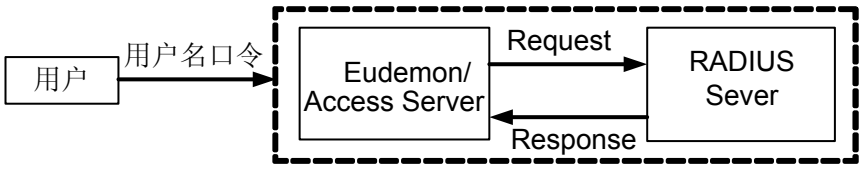
当用户想要通过某个网络（如电话网）与 NAS 建立连接，从而获得访问其他网络或取得使用某些网络资源的权利时，NAS 起到了验证用户或对应连接的作用。NAS 负责把用户的验证、授权信息传递给 RADIUS 服务器。RADIUS 协议规定了 NAS 与 RADIUS 服务器之间如何传递用户信息。

RADIUS 服务器负责接收用户的连接请求，完成验证，并把用户所需的授权信息返回给 NAS。NAS 和 RADIUS 之间的验证信息的传递通过密钥的参与来完成，避免了用户密码在不安全的网络上被窃取。

RADIUS 的消息流程

RADIUS 协议规定了客户/服务器间消息交互的消息流程和消息结构。采用 RADIUS 协议时，服务器就叫 RADIUS 服务器。RADIUS 协议规定的简单消息流程如图 3-9 所示。

图 3-9 RADIUS 客户/服务器间消息流程



此时，Eudemon 是作为接入服务器（Access Server）。当用户登录 Eudemon 时，会遵循如下操作流程。

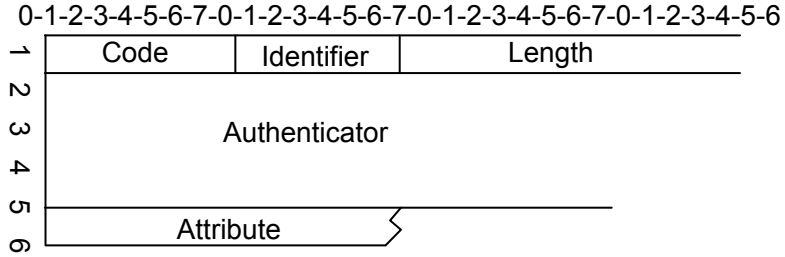
1. 用户将用户名和口令发送给 Eudemon。
2. Eudemon 中的 RADIUS 客户端接收到用户名和口令后，向 RADIUS 服务器发送认证请求。
3. RADIUS 服务器接收到合法的请求后，完成验证，并把所需的用户授权信息返回给客户端。

登录的用户可以是使用网络资源的 PPP（Point-to-Point Protocol）用户，也可以是对网络设备进行配置、维护的管理用户。

RADIUS 的消息结构

RADIUS 的消息结构如图 3-10 所示。

图 3-10 RADIUS 消息结构



具体介绍如下：

- Code

  用于表示 RADIUS 的消息类型，如接入请求、接入允许等。
- Identifier

  一般是顺序递增的数字，用于匹配请求包和回应包。
- Length

  所有域的总长度。
- Authenticator

  验证字，用于验证 RADIUS 的合法性。
- Attribute

  消息的内容主体，主要是用户相关的各种属性，包括用户名、用户密码、NAS IP 地址等属性。

RADIUS 的特点

RADIUS 有如下特点：

- 使用 UDP 作为传输协议，具有良好的实时性。
- 支持重传机制和备用服务器机制，具有较好的可靠性。
- 实现比较简单，适用于大用户量时服务器端的多线程结构。

上述特点使得 RADIUS 协议得到了广泛的应用。

作为 RADIUS 协议客户端，NAS 能够实现以下功能：

- 标准 RADIUS 协议及扩充属性，包括 RFC2865、RFC2866。
- 华为扩展的 RADIUS ＋ 1.1 协议。
- 对 RADIUS 服务器状态的主动探测功能。

如果当前服务器的状态为 DOWN，防火墙收到认证消息后，启动服务器探测处理，将消息转换为探测报文后向当前服务器发送。如果收到 RADIUS 服务器的回应，则认为该服务器重新可用。

- RADIUS 服务器的自动切换功能。

  当报文等待定时器超时的时候，如果当前发送的 Server 的状态为不可发送，或者发送次数超过当前 Server 的最大重传次数，则需要在配置的服务器组中选择另外的服务器发送报文。

3.5.3 HWTACACS 协议简介

HWTACACS 是在 TACACS（RFC 1492）基础上进行了功能增强的一种安全协议。该协议与 RADIUS 协议类似，主要是通过 Server/Client 模式实现多种用户的认证与授权功能，可用于 PPP 和 VPDN 接入用户及 login 用户的认证、授权和计费。

与 RADIUS 相比，HWTACACS 具有更加可靠的传输和加密特性，更加适合于安全控制。HWTACACS 协议与 RADIUS 协议的主要区别如表 3-2 所示。

表 3-2 HWTACACS 协议与 RADIUS 协议的比较

HWTACACS	RADIUS
使用 TCP 协议，网络传输更可靠	使用 UDP 协议
除了标准的 HWTACACS 报文头，对报文主体全部进行加密	只是对认证报文中的密码字段进行加密
认证与授权分离	认证与授权一起处理
适于进行安全控制	适于进行计费
支持对配置命令进行授权使用	不支持

HWTACACS 消息流程

HWTACACS 协议的消息流程和 RADIUS 协议的消息流程类似。不同在于 HWTACACS 协议当用户认证通过之后，服务器返回的是认证回应，而不返回用户的权限，只有当授权流程完成后才会返回用户的权限。

HWTACACS 协议支持按命令行授权

用户通过 Telnet 或者 SSH 登录到防火墙上后，如果该用户需要进行命令行授权，可以将该级别用户的命令行授权方法设置为 HWTACACS，该用户输入的每一条命令都要通过 HWTACACS 服务器授权。如果授权通过，命令就可以被执行。否则，HWTACACS 服务器输出信息，通知用户该命令的授权失败，不能执行。

命令行授权可以使用本地授权的方法作为备选方法，这样，如果因为服务器的问题导致命令行授权失败时，可以将命令行授权转入本地授权处理。

如果在用户配置的超时时间内，防火墙没有接收到 HWTACACS 服务器的授权结果，则授权超时，该命令不能被执行。

用户还可以配置服务器无响应或本地未配置用户时命令授权失败的策略，可以选择让用户继续在线，也可以选择授权失败次数超过阈值后下线。

说明

按命令授权失败的策略仅仅使用于因 HWTACACS 服务器不可用或本地未配置用户而导致的按命令行授权失败情况。下面的两种情况不能触发命令行授权失败时的策略:

- 服务器正常时，所执行的命令行未能通过在 HWTACACS 服务器端的授权。
- 服务器不可用后，按命令行授权转入本地授权后，因执行的命令级别高于本地配置的级别而授权失败。

HWTACACS 协议支持对用户级别提升进行认证

用户通过 Telnet 或者 SSH 登录到防火墙后，可以通过在用户模式下使用 **super** 命令来提升或降低自己的级别。这时，防火墙对用户的密码进行验证。

防火墙将用户的密码发送到 HWTACACS 服务器上进行认证，如果认证通过，用户的权限就可以得到提升，否则，用户的权限不能提升。特权等级更改的结果只影响本次登录。

如果在用户配置的超时时间内，防火墙没有接收到 HWTACACS 服务器用户级别提升的认证结果，则认证超时，用户不能提升权限。

说明

使用防火墙对用户级别提升进行验证的时候，各级别的密码可以不同；使用 HWTACACS 服务器对用户级别进行提升进行验证时，各级别密码必须相同。

3.5.4 域简介

防火墙对用户的管理包括两个层次：

- 通过域进行管理
- 通过用户账号进行管理

所有用户都属于某个域。

域下可以进行缺省授权配置、RADIUS 模板配置、认证方案的配置等。

域下配置的授权信息较认证与授权服务器的授权信息优先级低。即，优先使用认证与授权服务器下发的授权属性，在服务器无该项授权或不支持该项授权时，域的授权属性生效。这样处理的优点是：可以凭借域管理灵活增加业务，而不必受限于服务器提供的属性。

当域和域下的用户同时配置了某一属性时，基于用户的配置优先级高于域的配置。

3.5.5 本地用户管理简介

在防火墙上，可以使用认证与授权建立本地用户数据库，维护用户信息，并对用户进行管理。除了可以建立本地用户账号外，还可以进行本地认证。

说明

用户信息在本地用户数据库上的用户称为本地用户。

在 Eudemon 目前的实现中，可以单独配置本地用户。

4 GTP

关于本章

4.1 介绍

定义

随着 3GPP（the 3rd Generation Partnership Project）协议的演进，移动通信组网及其提供的业务也在不断发展变化：

- 移动通信网络

  从 2G GSM（Global System for Mobile Communications）经过 2.5G GPRS（General Packet Radio Service）演进到 3G UMTS（Universal Mobile Telecommunications System），移动通信网络实现了广域覆盖、高速无线数据传输和与因特网的融合。

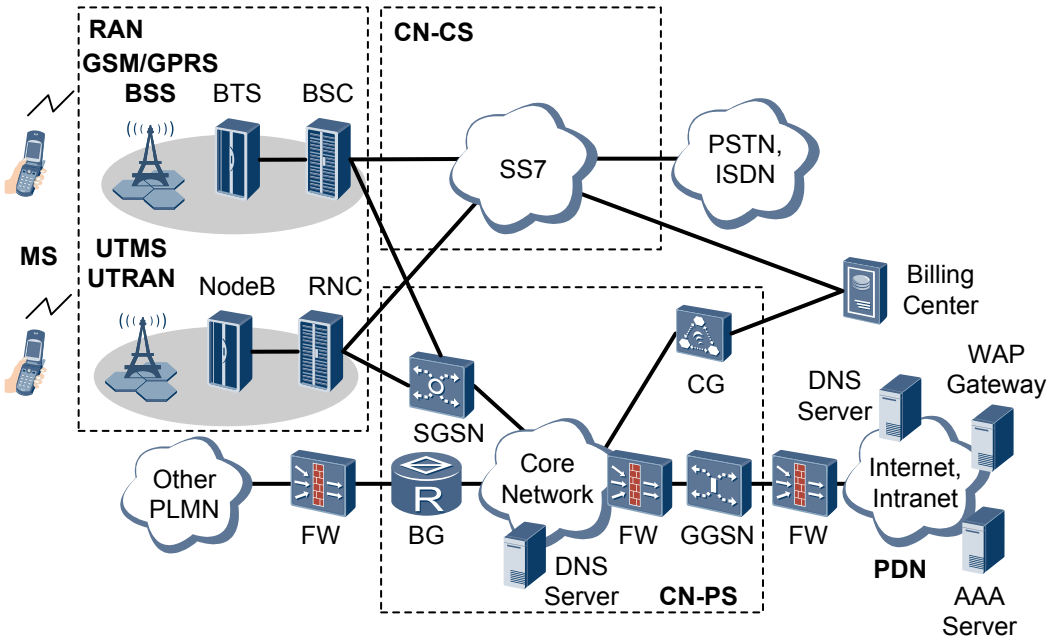
- 提供的业务

  提供语音、数据、视频等丰富多彩的业务，极大满足了用户随时随地多种方式相互通信的需求。

其中，GPRS 是为了支持分组业务而在 GSM 网络的基础上发展而来的 2.5G 网络；TD-SCDMA（Time Division-Synchronous Code Division Multiple Access）/WCDMA（Wideband Code Division Multiple Access）是 3G 网络，支持 CS（Circuit Switching）和 PS（Packet Switching）业务。TD-SCDMA/WCDMA 分组域与 GPRS 网络的结构相同。

GPRS/TD-SCDMA/WCDMA 网络结构如图 4-1 所示，其中核心网 CS 域中有一系列的设备，在图 4-1 中没有体现。

图 4-1 GPRS/TD-SCDMA/WCDMA 网络结构



MS：Mobile Station，移动台

RAN：Radio Access Network，无线接入网络

CN-CS：Core Network-Circuit Switching，核心网电路交换域

CN-PS：Core Network-Packet Switching，核心网分组交换域

BSS：Base Station System，基站子系统

UTRAN：Universal Terrestrial Radio Access Network，UMTS 陆地无线接入网

BTS：Base Transceiver Station，基站收发信台	BSC：Base Station Controller，基站控制器
NodeB：UMTS 基站	RNC：Radio Network Controller，无线网络控制器
SS7：CCITT Signaling System No.7，CCITT 7 号信令系统	CG：Charging Gateway，计费网关
SGSN：Serving GPRS Support Node，服务 GPRS 支持节点	GGSN：Gateway GPRS Support Node，网关 GPRS 支持节点
BG：Border Gateway，边缘网关	Billing Center：计费中心
DNS Server：域名服务器	AAA Server：认证、授权和计费服务器
WAP Gateway：Wireless Access Protocol Gateway，无线接入协议网关	FW：Firewall，防火墙
PDN：Public Data Network，公众数据网	PLMN：Public Land Mobile Network，公用陆地移动通信网

在 GPRS 网络中，数据从手机到达 Internet，需要经过四个设备：MS、BSS、SGSN 和 GGSN。这四个设备的功能分别描述如下：

- MS

  MS 是移动用户设备，可以通过空中接口发起、接收呼叫。当进行数据业务时，MS 和核心网分组域建立逻辑链路。

- BSS

  包括一系列设备，负责分配空中的信道资源，并在 MS 和 SGSN 之间转发信息。

- SGSN

  SGSN 是为提供分组数据业务功能而引入的一个新的网元设备，主要的作用是为本 SGSN 服务区域的 MS 转发输入/输出的 IP 分组。

  SGSN 主要提供用户分组数据包的路由与转发、加密与鉴权、会话管理、移动性管理、逻辑链路管理和计费信息产生和输出等功能。

- GGSN

  GGSN 也是为提供分组数据业务功能而引入的一个新的网元设备，提供数据包在 GPRS/TD-SCDMA/WCDMA 网和外部数据网之间的路由和封装。

  GGSN 是 MS 接入外部分组网络的网关，从外部网络来看，GGSN 类似是可寻址 GPRS/TD-SCDMA/WCDMA 网络中所有用户 IP 地址的路由器。GGSN 接收 MS 发送的数据，选路到相应的外部网络；或者接收外部网络的数据，根据其目的地址选择 GPRS/TD-SCDMA/WCDMA 网中的传输通道，发送给相应的 SGSN。

GPRS 网络是在现有的 GSM 网络中，通过增加一些网元（如 SGSN、GGSN），改造而成的承载网。这些网元统称为 GSN（GPRS Supporting Node）。

为了保证新增的网元之间以及这些网元与其它网络之间的通信，增加了统称为 G 接口的新接口，这些接口分别是 Gb、Gn、Gp、Gi 等数据接口，Gr、Gs、Gd、Gf 等信令接口。在 Eudemon 的应用场景中，需要重点关注 Gn、Gp、Gi 三个接口。

- Gn

  同一个 PLMN 中的不同 GSN 之间的接口。Gn 接口运行 GTP（GPRS Tunneling Protocol）协议，确保在同一个 PLMN 中的 SGSN 和 GGSN 之间的互通。

- Gp

  不同 PLMN 之间的 GSN 之间的接口，用来实现不同 PLMN 之间的数据漫游业务。Gp 接口运行 GTP 协议，确保在不同的 PLMN 之间的 SGSN 和 GGSN 之间的互通。

- Gi

GGSN 和 PDN 之间的接口。该接口实现 GPRS 网络和外部数据网的互连。Gi 接口运行 IP 协议，保证 GGSN 与外部网络的数据传输。

GTP 是为 Gn 和 Gp 接口定义的一个隧道协议，用来支持 GSN 之间的数据通信。GTP 基于 UDP 协议，包括 GTP 控制平面（GTP-C）和 GTP 用户平面（GTP-U）。

- GTP 控制平面（GTP-C）

  在控制平面，使用信令机制创建、修改和删除隧道。
- GTP 用户平面（GTP-U）

  在用户平面，使用隧道机制传送用户数据包。

GTP 包括 Version 0 和 Version 1 两个版本。前者属于 3GPP Release 97 协议，用于 GPRS 网络；后者属于 3GPP Release 99 协议，用于 3G 网络。GTP Version 1 可兼容 Version 0，两者可以通过 GTP 报文头的版本字段取值来区分。

除此之外，GTP 还包括用于计费的 GTP’协议。

目的

GTP 控制平面和用户平面使用了多种消息进行报文交互，例如：

- 路径管理消息
- 隧道管理消息
- 位置管理消息
- 移动性管理消息
- 信息元素 IE（Information Element）等

由于 GPRS 网络的数据业务都是承载在 GTP 隧道中，因此 Eudemon 的主要应用是对 GTP 协议进行解析，根据预先设置的规则，对 GTP 报文进行过滤，确保 GPRS 网络的安全性。

收益

Eudemon 在核心网 PS 域中主要有以下几种的应用：

- 工作在 Gn 接口，过滤掉恶意报文，保证同一个 PLMN 内网元的安全。
- 工作在 Gp 接口，当一个 PLMN 网络与其他 PLMN 网络相连时，过滤掉来自其他 PLMN 网络的恶意报文，保证 PLMN 网络内网元的安全。
- 工作在 Gi 接口，当 PLMN 网络与外部 IP 网络相连时，过滤掉来自外部 IP 网络的恶意报文，保证 PLMN 网络内网元的安全。
- 对 GTP 计费溢出攻击进行防范。

Eudemon 上的接口工作在路由模式或透明模式时，都支持 GTP 协议。

4.2 规格

GTP 特性的相关规格如下：

- Eudemon 支持创建的 GTP 策略的最大个数为 32 个。

- Eudemon 对 RELOCATION 消息进行过滤时，支持配置的 SGSN 的 IP 地址的最大个数为 20 个。
- Eudemon 对 LOCATION 管理消息进行过滤时，支持配置的 GGSN 的 IP 地址的最大个数为 20 个。
- Eudemon 整机支持配置的 GTP 消息内容过滤规则的最大个数为 2000 个，每个 GTP 策略中支持配置的 GTP 消息内容过滤规则的最大个数为 256 个。
- Eudemon 支持配置的 MCC（Mobile Country Code）的最大个数为 100 个。

4.3 参考标准和协议

与 GTP 特性相关的参考标准与协议如下：

- 3GPP TS 23.060
  General Packet Radio Service (GPRS) Service description Stage 2
- 3GPP TS 29.060
  GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.061
  Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)

4.4 可获得性

版本支持

产品	最低支持版本
Quidway Eudemon 8080E/8160E	V100R003

特性依赖

无

4.5 GTP 策略

内容过滤

GTP 控制层面的消息可以包含多个信息元素（Information Element），例如：

- APN（Access Point Name）
  接入点名称，在 GGSN 中用于标识一个指定的外部网络和一种服务的 ISP，在 SGSN 中可根据 APN 通过 DNS 域名解析得到与此 APN 对应的 GGSN 地址。
- IMSI（International Mobile Subscriber Identity）
  国际移动用户识别码，区别移动用户的标志。IMSI 由三部分元素构成：MCC（Mobile Country Code）、MNC（Mobile Network code）和 MSIN（Mobile Subscriber

Identification Number）。MCC 和 MNC 购成了 IMSI 的前缀，标识移动用户的本地网或 PLMN。

- MSISDN（Mobile Station International ISDN Number)

  移动台国际 ISDN 号码，用于标识公用交换电信网（PSTN）或综合业务数字网（ISDN）拨向 GSM 系统的号码。

- RAI（Routing Area Identity）

  路由区标识，用来标识 SGSN 的属性，也包括 MCC 和 MNC。

Eudemon 支持 APN、IMSI 前缀、MSISDN、RAI 前缀以及以上四种信息元素组合的方式对 GTP 报文进行过滤。

类型过滤

Eudemon 支持通过判断消息类型对 GTP 报文进行过滤，有以下几种方式：

- 过滤指定类型的消息

  对所有的 GTP 消息、GTP'消息以及未知的 GTP 消息进行过滤。另外，GTP 的 Version 0 和 Version 1 版本中包含多个消息类型，还可以配置对指定的消息类型进行过滤。

- 过滤非法的 RELOCATION 消息

  由于 RELOCATION 消息只会在相临的 SGSN 之间产生，因此通过严格限制 SGSN 的源 IP 地址，可以对不合法的 RELOCATION 消息进行过滤，防止攻击。

- 过滤非法的 LOCATION 管理消息

  当 SGSN 为 GGSN 提供位置查询功能时，一般只会为本地的 GGSN 服务，因此通过严格限制 GGSN 的源 IP 地址，可以对不合法的 LOCATION 管理消息进行过滤，防止攻击。

长度过滤

GTP 消息长度是以字节为单位的净荷长度，即分组中除了 GTP 头的必选部分外剩余部分的长度（即除去前面的 8 个字节），不包括 GTP 报文头长度、UDP 头长度和 IP 头长度。

Eudemon 通过解析 GTP 消息头中的长度字段，得到 GTP 报文的消息长度，如果该长度处于配置的最小长度和最大长度范围之内，则允许 GTP 报文通过，否则 GTP 报文将被丢弃。

IE 过滤

GTP 消息中可以包含很多个不同的 IE，这些 IE 有三种状态：必选、可选、有条件选择，Eudemon 支持对必选 IE、可选 IE 和重复 IE 进行检测，避免恶意报文攻击：

- 必选 IE 检测

  当 Eudemon 收到 GTP 消息后，会自动对必选 IE 进行检测，如果 GTP 消息中没有完全包含协议规范要求的必选 IE，则丢弃此 GTP 消息。此功能无需使用命令开启。

- 可选 IE 检测

  用户可以通过命令配置 Eudemon 对某个可选 IE 进行检测，当 Eudemon 收到的 GTP 消息中没有包含该可选 IE，则丢弃此 GTP 消息。

- 重复 IE 检测

GTP 协议规范要求如果网元收到非协议规定的重复 IE 时，只处理第一个 IE。Eudemon 支持对重复的必选 IE 进行检测，当 GTP 消息中必选 IE 重复出现时，丢弃此 GTP 消息。

扩展头过滤

在 GTP 协议 v1 版本中，GTP 消息头中可以添加扩展头，容易引起攻击，因此需要针对扩展头进行检测。

Eudemon 支持以下两种方式对扩展头进行检测：

- 对扩展头的类型进行过滤，只有带有指定类型扩展头的 GTP 消息可以通过。
- 过滤带有重复扩展头的 GTP 消息。

日志

为了监控 GTP 的工作状态，Eudemon 提供以下日志功能：

- 根据对 GTP 报文不同的处理结果，记录日志。

  一个 GTP 协议报文经过 Eudemon 处理后其结果状态可能为：

  - **forward**

    报文匹配 GTP 通过规则，Eudemon 转发该报文。
  - **prohibit**

    报文匹配 GTP 拒绝规则，Eudemon 丢弃该报文。
  - **rate-limit**

    报文超过 GTP 隧道最大速率限制，Eudemon 丢弃该报文。
  - **state-invalid**

    报文的 GTP 状态检测失败，Eudemon 丢弃该报文。
  - **tunnel-limit**

    GTP 隧道已经超过最大限制数量，Eudemon 丢弃该报文。
- 根据指定的条件，记录日志。

  通过指定 APN、IMSI、MSISDN 的值或者消息的类型，Eudemon 对匹配的 GTP 报文记录日志。

日志采用 SYSLOG 方式由 GTP 模块发送给信息中心，有两种信息格式：

- **basic**

  基本的 log 信息，包括：时间戳、源 IP 地址、目的 IP 地址、消息类型、报文状态(forwarded，prohibited，rate-limited，state-invalid，tunnel-limited，matchmsgtype，matchimsi，matchmsisdn，matchapn)、接口等信息。
- **extended**

  扩展的 log 信息，除了包含 basic 的信息外，还包括：IMSI、MSISDN、APN、选择模式、信令 SGSN 地址、数据 SGSN 地址、信令 GGSN 地址、数据 GGSN 地址等信息。

4.6 GTP 计费溢出攻击防范

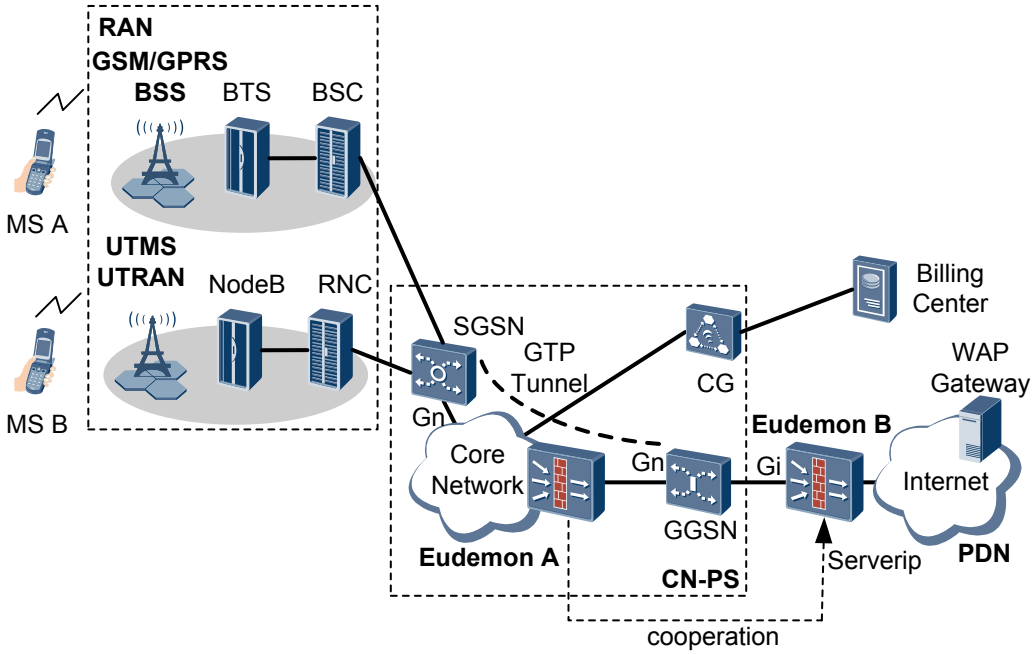
在移动分组业务中，类似于传统 IP 网络通信，MS 和 PDN 中的主机服务器都有一个 IP。PDN 中主机服务器的 IP 通常是固定并且对 GPRS 可见，可以是 Web 服务器、流媒体服务器等，为 MS 提供各种分组数据业务。MS 的 IP 地址通常都是动态获得的。

GTP 计费溢出攻击的产生过程如下：

1. MS A 激活 GTP 业务后，从 GGSN 获得 IP 地址 10.10.10.10，并向 Internet 上的主机请求大量分组数据。
2. MS A 请求大量数据后，不等待数据传输完毕就立即退出。此时 MS A 把 IP 地址 10.10.10.10 归还给 GGSN，GGSN 因查询不到 GTP 隧道而把来自 Internet 的分组数据丢弃。
3. MS B 激活 GTP 业务后，获得 IP 地址 10.10.10.10，此时 GGSN 可以重新查询到 GTP 隧道，因此把来自 Internet 的分组数据发给 MS B，并对 MS B 计费。虽然这些分组数据并不是 MS B 请求的，但 MS B 将为所有的分组数据付费，此时开始发生计费溢出。

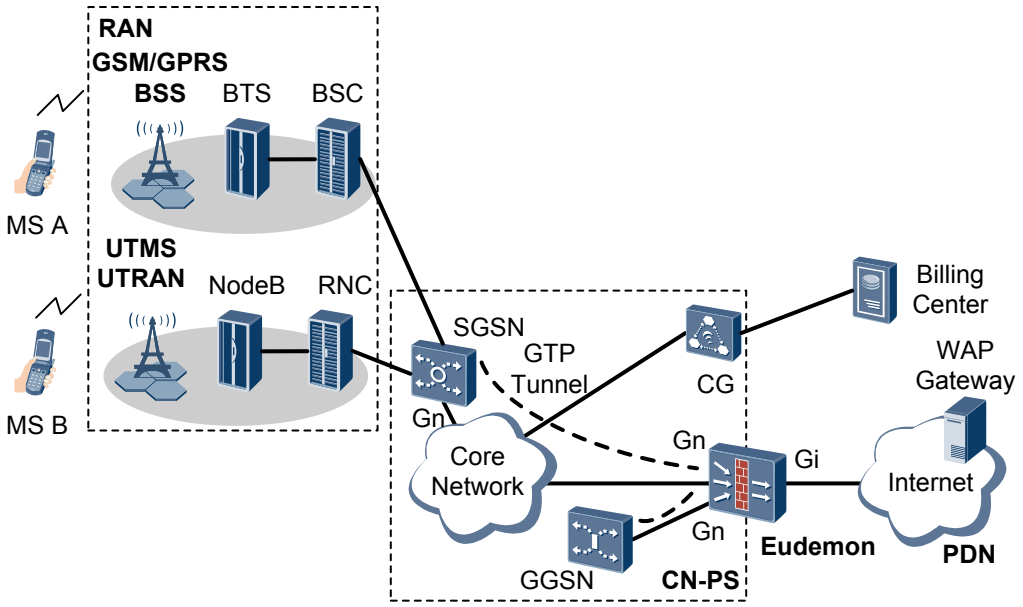
防范计费溢出攻击的关键是阻止 Internet 响应 MS A 请求的分组数据到达 GGSN，这就需要在 GGSN 接收到分组数据之前识别并丢弃流量，即在 Gi 接口进行防范。由于 GTP 协议运行于 Gn 和 Gp 接口，Gi 接口并不运行 GTP 协议，Gi 接口无法同步获得每个 GTP 隧道结束的消息。因此需要在 Eudemon A 上对用户会话去激活信息进行识别，然后通知位于 Gi 接口的 Eudemon B 对 Internet 响应此用户请求的分组数据进行过滤，如图 4-2 所示。

图 4-2 联动方式的 GTP 计费溢出攻击防范组网图



此外，Eudemon 还支持在一台设备上对计费溢出攻击进行防范，不需要两台设备进行联动。如图 4-3 所示，Eudemon 上既支持 Gn 接口又支持 Gi 接口，Gi 接口和 Gn 接口处于不同的虚拟防火墙中，Eudemon 在逻辑上还是相当于两台设备。当 Gn 接口收到 MS 下线信息后，将 MS 的 IP 地址记录到下线 IP 表中。然后 Gi 接口对收到的非 GTP 报文进行检测，如果报文的 IP 地址匹配了下线 IP 表中的 IP 地址，则将报文丢弃。

图 4-3 单机方式的 GTP 计费溢出攻击防范组网图



4.7 GTP 全局参数

老化时间

Eudemon 支持对状态表定时检测，老化超时的状态信息。老化时间缺省为 3600 秒，用户可以根据实际需要，设置不同的老化时间。

注意

在 GTP 正在运行的情况下更改老化时间后，对于新建立的 GTP 隧道，将会按照新的老化时间进行老化，已经建立的 GTP 隧道不会受到影响。

GTP-in-GTP 过滤

Eudemon 支持对 GTP-U 报文的载荷进行检测，如果 GTP-U 报文中又包含 GTP 报文，则将该报文丢弃。

流量和隧道数限制

Eudemon 支持以下两种方式对 GTP 进行限制：

- 限制 GTP 流量

  限制 Eudemon 上的 GTP 控制平面和 GTP 用户平面的流量，保护 GPRS 网络内的 GSN 节点不受到过量 GTP 数据包的攻击。此外，Eudemon 还支持通过限制 Supported Extension Headers Notification 消息的通过速度来防止路径拥塞攻击。

- 限制 GTP 隧道数

  检测 Eudemon 上的 GTP 隧道数是否超过设置的阈值，丢弃超过阈值的 GTP 报文。

MNC 所占位数

移动国家码 MCC（Mobile Country Code）由 3 位数组成，唯一地识别移动用户所属的国家，例如，中国的 MCC 规定为 460。移动网络码 MNC（Mobile Network code）由 2 或 3 位数组成，识别移动用户所属的移动通信网。

在信息元素 IMSI 和 RAI 中都存在 MCC 和 MNC 字段，所以 Eudemon 在对信息元素进行解码时会根据 MCC 确定 MNC 的位数。如果没有指定 MNC 的位数，缺省认为 MNC 为两位。

状态检测

在 GTP 隧道建立初始，Eudemon 为此隧道的上下文建立状态表。当后续的消息（响应类和相关的数据消息）到来时，针对 GTP 报文的交互过程，Eudemon 检索状态表，对 GTP 报文进行状态的合法性检测。如果状态合法，则允许该报文通过；反之，则丢弃该报文。

同时，Eudemon 定时检测状态表，老化超时的状态信息。

注意

配置 GTP 状态检测功能后，如果 Eudemon 上的 GTP 状态和 SGSN、GGSN 上的 GTP 状态表项没有同步，Eudemon 将会根据协议规范丢弃掉 create-pdp-context、GTP-U 等报文。而 create-pdp-context、GTP-U 等报文对 SGSN 和 GGSN 来说都属于关键报文，这些报文被丢弃后将会对业务造成很大的影响，因此一般情况下不建议配置该功能。

统计

Eudemon 支持对收到的 GTP 总的报文数、允许通过的 GTP 报文数、被丢弃的 GTP 报文数、GTP 隧道数、GTP 隧道持续时间等信息进行统计，更好的监控 GTP 的运行状态。

隧道日志

当 GTP 隧道被清除时，Eudemon 支持对 GTP 隧道的状态记录日志，便于用户查询。

4.8 GTP 应用

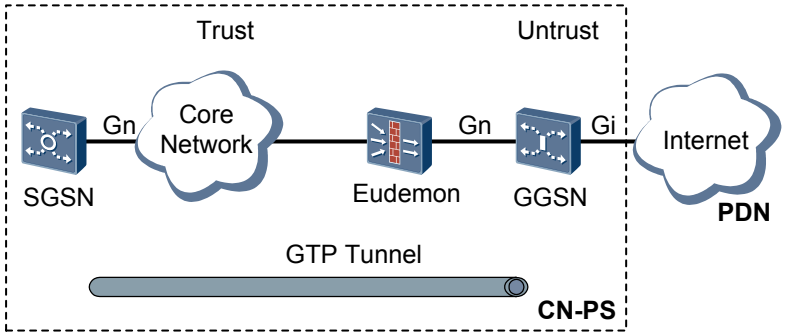
4.8.1 GTP 策略在核心网中的应用

Eudemon 部署在核心网中，根据实际需求，应用相应的 GTP 策略，保护 SGSN 和 GGSN 设备之间数据传输的安全性。

以图 4-4 为例，Eudemon 工作在 Gn 接口，通过配置并应用 GTP 策略，实现如下需求：

- 过滤 APN 为 test 的 GTP 报文。
- 过滤 GTP'报文。
- 限制 GTP 消息的长度为 0 ～ 1400 字节，过滤不符合长度要求的 GTP 报文。
- 对重复 IE 进行检测，过滤非协议规定的重复 IE。
- 对命中允许通过规则和拒绝通过规则的 GTP 报文记录日志，日志信息格式为 extended。

图 4-4 GTP 策略在核心网中的应用

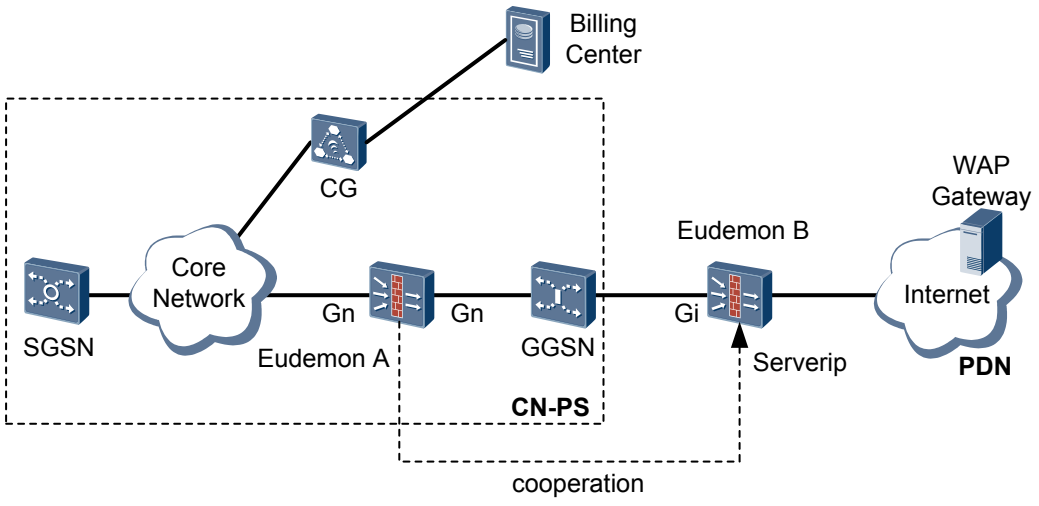


4.8.2 防范 GTP 计费溢出攻击

EudemonA 工作在 Gn 接口，EudemonB 工作在 Gi 接口，EudemonA 和 EudemonB 之间联动，对 GTP 计费溢出攻击进行防范。

以图 4-5 为例，配置 GTP 计费溢出攻击防范，当 MS 下线时，工作在 Gn 接口的 EudemonA 会及时通知工作在 Gi 接口的 EudemonB，EudemonB 将会丢弃该用户的后续数据报文，防范了对其他用户的计费溢出攻击。

图 4-5 配置 GTP 计费溢出攻击防范组网图



5 入侵防御（IPS）

关于本章

入侵防御（IPS，Intrusion Prevention System）能够有效防御应用层攻击，如：缓冲区溢出攻击、木马、后门攻击、蠕虫等。

5.1 介绍

介绍 IPS 特性的定义和目的。

定义

IPS 是通过监控或者分析系统事件，检测入侵的发生，并通过一定的响应方式，实时地中止入侵行为的一种安全机制。

目的

保护系统或系统资源不受未经授权的访问。IPS 可以防范的威胁包括：蠕虫、病毒、广告软件、来自 Internet 的无授权访问、内部用户的安全违规等。

5.2 规格

介绍 IPS 特性的规格信息。

IPS 特性的规格如下：

- 使用 Symantec 入侵检测和防御技术
- 支持分片重组
- 支持流重组
- 支持基于特征的检测和基于协议异常的检测
- 支持协议识别
- 支持自定义签名和预定义签名
- 支持细粒度的 IPS 策略设置
- 支持特权策略
- 支持直路和旁路的工作方式
- 支持签名按类别显示
- 支持签名的查询
- IPS 签名库的升级，包括自动升级、手动升级、本地升级、版本回退

5.3 可获得性

介绍 IPS 特性的 License 支持信息。

只有获取了支持 IPS 升级服务的 License，才能使用 IPS 功能。当 License 过期后，IPS 功能仍可以使用，但不能升级签名库和引擎。

5.4 原理描述

介绍 IPS 特性的实现原理。

产生背景

随着攻击手段和工具的不断涌现、攻击技术的日趋成熟，传统的防火墙网络层攻击检测已无法满足安全需要。在此背景下，出现了 IPS 技术。

IPS 设备与传统防火墙以及 IDS（Intrusion Detection System）设备相比主要有以下不同：

- 传统防火墙很难对基于应用层的攻击进行预防和阻止。IPS 设备能够有效防御应用层攻击，如：缓冲区溢出攻击、木马、后门攻击、蠕虫等。
- IDS 设备只检测和告警。IPS 设备不仅能够检测入侵的发生，而且能通过一定的响应方式，实时地中止入侵行为的发生和发展，实时地保护信息系统不受实质性的攻击。

IPS 处理流程

IPS 的基本处理流程如下：

1. 重组应用数据

   Eudemon 支持对 IP 分片报文重组以及 TCP 流重组，确保了应用数据的连续性，防止躲避 IPS 检测的攻击行为。

2. 协议识别

   与传统的根据端口识别协议不同，Eudemon 能根据报文内容识别多种常见应用层协议，并对这些数据进行检测，提高了攻击行为的检测率。

3. 匹配签名

   Eudemon 采用基于状态的匹配引擎，通过将报文内容与签名进行比较，能够准确识别出真实的应用层协议类型以及攻击行为。

4. 完成检测后，Eudemon 根据用户配置的策略和响应方式对匹配到 IPS 签名的报文进行处理。

   说明

   关于 IPS 签名、策略和响应方式的概念请参见下文中的 IPS 签名、策略定制和响应方式。

IPS 签名

IPS 签名用来描述网络中存在的攻击行为的特征，Eudemon 将报文内容和 IPS 签名进行比较，来检测和防范攻击。

Eudemon 的签名分为两类：

- 预定义签名

  Eudemon 中预先定义的签名。用户购买了带 IPS 升级功能的 License 后即可获得包含预定义签名的签名库，并且能够不断地从安全服务中心获取新的 IPS 版本来更新签名库。

- 自定义签名

  用户根据网络流量特点对特定的入侵行为自行定义的签名，自定义签名的攻击特征使用正则表达式定义。

策略定制

传统的 IPS 策略基本上不区分受保护对象，对所有流量都进行检测。因此会出现将一些不需要检测的流量也进行了检测，导致检测性能低下。Eudemon 支持用户根据实际网络情况定制细致的 IPS 策略，并应用在特定的流量上，提高了检测性能。

Eudemon 可以通过以下方式定制 IPS 策略：

- 引用模板

  Eudemon 提供了策略模板，模板内容为针对指定场景预先定义的签名集及其启用状态和响应方式。如果模板内容可满足安全需求，用户可以直接在 IPS 策略中引用模板，从而减少配置工作。

- 配置签名集

  签名集是满足指定过滤条件的签名的集合。用户根据需要配置各种过滤条件来过滤签名集中包含的签名，并配置签名集的启用状态和响应方式。

- 配置覆盖签名

  当需要对某个签名配置指定的启用状态和响应方式时，可以采用在 IPS 策略中配置覆盖签名的方式实现。自定义签名必须通过覆盖签名方式应用到 IPS 策略中。

  说明

  覆盖签名优先级高于签名集的配置，如果配置的覆盖签名和签名集中的配置有冲突时以覆盖签名为准。

完成 IPS 策略配置后，需要将 IPS 策略应用在指定的域内或域间才能使 IPS 功能生效。

Eudemon 还支持从已有的 IPS 策略中选取一个作为特权策略。特权策略替换所有已经在域内或域间应用的 IPS 策略，没有应用 IPS 策略的域内或域间不添加特权策略。

IPS 策略经过编译后才能生效，Eudemon 支持手动提交配置来编译 IPS 策略。另外，以下三种情况也会触发 IPS 策略的编译，而且与手动提交配置的编译效果相同。

- 域内或域间应用 IPS 策略（当修改后未提交配置进行编译时）
- 配置特权策略或取消已配置的特权策略（当修改后未提交配置进行编译时）
- 升级 IPS 版本（一定会触发 IPS 策略的编译）

攻击响应方式

一个签名包含一种攻击特征，当报文命中签名时，Eudemon 将该报文识别为攻击报文，然后按照签名的攻击响应方式处理该报文。

说明

当报文命中多个签名，对该报文的响应方式如下：

- 如果这些签名的响应方式都为 **Alert** 时，响应方式为告警。
- 如果这些签名中至少有一个签名的响应方式为 **Block** 时，响应方式为阻断。

IPS 攻击响应方式如表 5-1 所示。

表 5-1 攻击响应方式

处理策略	工作模式	实际动作
告警	防护模式	Eudemon 不对文件进行处理，记录日志。
	告警模式	
阻断	防护模式	Eudemon 阻断文件，记录日志。
	告警模式	Eudemon 不对文件进行处理，记录日志。

6 VPN

关于本章

6.1 概述

6.1.1 VPN 简介

VPN（Virtual Private Network）是近年来随着 Internet 的广泛应用而迅速发展起来的一种新技术，用于实现在公用网络上构建私人专用网络。“虚拟”主要指这种网络是一种逻辑上的网络。

伴随企业和公司的不断扩张，员工出差日趋频繁，驻外机构及客户群分布日益分散，合作伙伴日益增多，越来越多的现代企业迫切需要利用公共 Internet 资源来进行促销、销售、售后服务、培训、合作及其它咨询活动，这为 VPN 的应用奠定了广阔市场。

VPN 的特点

VPN 的特点如下：

- VPN 有别于传统网络，它并不实际存在，而是利用现有公共网络，通过资源配置而成的虚拟网络，是一种逻辑上的网络。
- VPN 只为特定的企业或用户群体所专用。

  从 VPN 用户角度看来，使用 VPN 与传统专网没有区别：

  - VPN 作为私有专网，与底层承载网络之间保持资源独立性，即在一般情况下，VPN 资源不会被承载网络中的其它 VPN 或非该 VPN 用户的网络成员所使用。
  - VPN 提供足够安全性，确保 VPN 内部信息不受外部的侵扰。
- VPN 不是一种简单的高层业务。

  该业务建立专网用户之间的网络互联，包括建立 VPN 内部的网络拓扑、路由计算、成员的加入与退出等，因此 VPN 技术比各种普通的点对点的应用机制要复杂得多。

VPN 的优势

VPN 的优势如下：

- 在远端用户、驻外机构、合作伙伴、供应商与公司总部之间建立可靠的安全连接，保证数据传输的安全性。

  这一优势对于实现电子商务或金融网络与通讯网络的融合将有特别重要的意义。
- 利用公共网络进行信息通讯，一方面使企业以明显更低的成本连接远地办事机构、出差人员和业务伙伴，另一方面极大的提高了网络的资源利用率，有助于增加 ISP 的收益。
- 只需要通过软件配置就可以增加、删除 VPN 用户，无需改动硬件设施。这使得 VPN 的应用具有很大灵活性。

- 支持驻外 VPN 用户在任何时间、任何地点的移动接入，这将满足不断增长的移动业务需求。
- 构建具有服务质量保证的 VPN，可为 VPN 用户提供不同等级的服务质量保证，通过收取不同的业务使用费用可获得更多的利润。

6.1.2 VPN 分类

IP VPN 是指利用 IP 设施（包括公用的 Internet 或专用的 IP 骨干网）实现 WAN 设备专线业务（如远程拨号、DDN 等）的仿真。IP VPN 可有以下几种分类方法。

按运营模式划分

IP VPN 按经营模式可划分为：

- CPE-based VPN（Customer Premises Equipment based VPN）

  用户不但要安装价格昂贵的设备及专门认证工具，还要负责繁杂的 VPN 维护（如隧道维护、带宽管理等）。这种方式组网复杂度高、业务扩展能力弱。
- NBIP-VPN（Network-based VPN）

  将 VPN 的维护等外包给 ISP 实施（也允许用户在一定程度上进行业务管理和控制），并且将其功能特性集中在网络侧设备处实现，这样可以降低用户投资、增加业务灵活性和扩展性，同时也可为运营商带来新的收入。

按业务用途划分

IP VPN 按业务用途可划分为：

- 企业内部虚拟专网（Intranet VPN）

  Intranet VPN 通过公用网络进行企业内部各个分布点互联，是传统的专线网或其它企业网的扩展或替代形式。
- 远程访问虚拟专网（Access VPN）

  Access VPN 向出差流动员工、远程办公人员和远程小办公室提供了通过公用网络与企业的 Intranet 和 Extranet 建立私有的网络连接。Access VPN 的结构有两种类型，一种是用户发起（Client-initiated）的 VPN 连接，另一种是接入服务器发起（NAS-initiated）的 VPN 连接。
- 扩展的企业内部虚拟专网（Extranet VPN）

  Extranet VPN 是指利用 VPN 将企业网延伸至供应商、合作伙伴与客户处，使不同企业间通过公网来构筑 VPN。

按组网模型划分

IP VPN 按组网模型可划分为：

- 虚拟租用线（VLL）

  VLL（Virtual Leased Line）是对传统租用线业务的仿真，通过使用 IP 网络对租用线进行模拟，提供非对称、低成本的“DDN（Digital Data Network）”业务。从虚拟租用线两端的用户来看，该虚拟租用线近似于过去的租用线。
- 虚拟专用拨号网络（VPDN）

VPDN（Virtual Private Dial Network）是指利用公共网络（如 ISDN 和 PSTN）的拨号功能及接入网来实现虚拟专用网，从而为企业、小型 ISP、移动办公人员提供接入服务。

- 虚拟专用 LAN 网段（VPLS）

  VPLS（Virtual Private LAN Segment）借助 IP 公共网络实现 LAN 之间通过虚拟专用网段互联，是局域网在 IP 公共网络上的延伸。

- 虚拟专用路由网（VPRN）

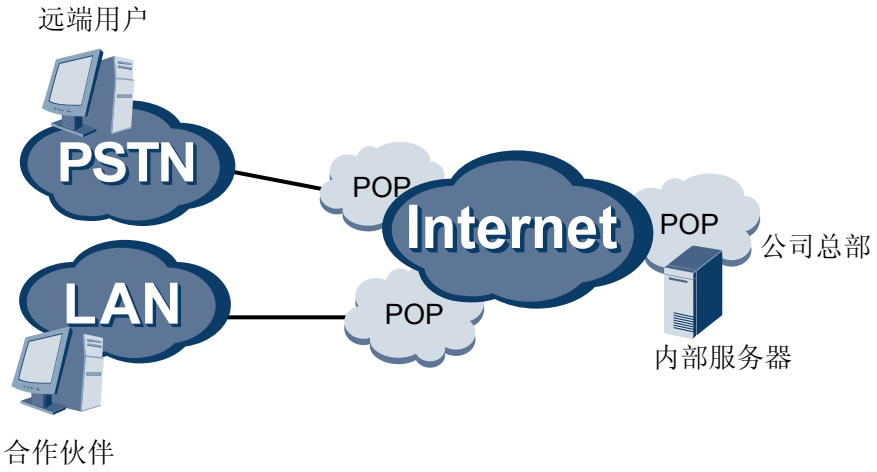
  VPRN（Virtual Private Routing Network）借助 IP 公共网络实现总部、分支机构和远端办公室之间通过网络管理虚拟防火墙进行互联，业务实现包括两类。

  - 使用传统 VPN 协议（如 IPSec、GRE 等）实现的 VPRN。
  - MPLS 方式的 VPRN。

6.1.3 典型组网应用

以某企业为例，通过 VPN 建立的企业内部网如图 6-1 所示。

图 6-1 VPN 组网示意图



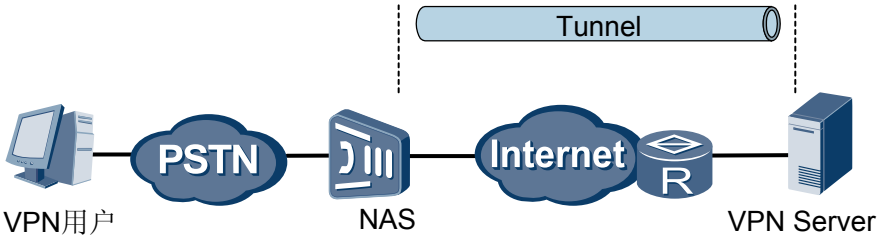
从上图可以看出，企业内部资源享用者通过 PSTN/ISDN（Public Switched Telephone Network/Integrated Services Digital Network)或局域网就可以连入本地 ISP 的 POP（Point of Presence）服务器，从而访问公司内部资源。而利用传统的 WAN 组建技术，相互之间要有专线相连才可以达到同样的目的。虚拟网组成后，远端用户和外地客户甚至不必拥有本地 ISP 的上网权限就可以访问企业内部资源，这对于流动性很大的出差员工和分布广泛的客户来说是很有意义的。

企业开设 VPN 业务所需的设备很少，只需在资源共享处放置一台支持 VPN 的服务器（如一台 Eudemon）就可以了。资源享用者通过 PSTN/ISDN 或局域网连入本地 POP 服务器后，直接呼叫企业的远程服务器（VPN 服务器），呼叫接续过程由 ISP 的接入服务器（Access Server）与 VPN 服务器共同完成。

6.1.4 VPN 原理

VPN 的原理如图 6-2 所示。

图 6-2 VPN 接入示意图



VPN 用户通过 PSTN/ISDN 或局域网拨入 ISP 的 NAS，NAS 通过用户名或接入号码识别出该用户为 VPN 用户后，就和用户的目的 VPN 服务器建立一条连接，称为隧道（Tunnel），然后将用户数据包封装成 IP 报文后通过该隧道传送给 VPN 服务器，VPN 服务器收到数据包并拆封后就可以读到真正有意义的报文了。反向的处理也一样。对用户来说，隧道是其 PSTN/ISDN 链路的逻辑延伸，操作起来和实际物理链路相同。

隧道可以通过隧道协议来实现。根据是在 OSI（Open Systems Interconnection）模型的第二层还是第三层实现隧道，隧道协议分为第二层隧道协议和第三层隧道协议，其说明如下：

- 第二层隧道协议

  第二层隧道协议是将整个 PPP 帧封装在内部隧道中。现有的第二层隧道协议有三种。

  - PPTP（Point-to-Point Tunneling Protocol）

    PPTP 在 Windows NT 4.0 以上版本中支持。该协议支持 PPP 在 IP 网络上的隧道封装，PPTP 作为一个呼叫控制和管理协议，使用一种增强的 GRE（Generic Routing Encapsulation）技术为传输的 PPP 报文提供流控和拥塞控制的封装服务。

  - L2F（Layer Two Forwarding）协议

    L2F 协议支持对更高级协议链路层的隧道封装，实现了拨号服务器和拨号协议连接在物理位置上的分离。

  - L2TP（Layer 2 Tunneling Protocol）

    L2TP 结合了上述两个协议的优点，为众多公司所接受。并且已经成为标准 RFC。L2TP 既可用于实现拨号 VPN 业务（VPDN 接入），也可用于实现 VPN 业务。

- 第三层隧道协议

  第三层隧道协议的起点与终点均在 ISP 内，PPP 会话终止在 NAS 处，隧道内只携带第三层报文。现有的第三层隧道协议主要有两种。

  - GRE 协议

    GRE 用于实现任意一种网络层协议在另一种网络层协议上的封装。

  - IPSec 协议

    IPSec 协议不是一个单独的协议，它给出了 IP 网络上数据安全的一整套体系结构，包括 AH（Authentication Header）、ESP（Encapsulating Security Payload）、IKE（Internet Key Exchange）等协议。

  GRE 和 IPSec 主要用于实现 VPN 业务。

- 第二、三层隧道协议之间的异同

  第三层隧道与第二层隧道相比，优势在于它的安全性、可扩展性与可靠性。

- 从安全性的角度看，由于第二层隧道一般终止在用户侧设备上，对用户网的安全及防火墙技术提出十分严峻的挑战；而第三层隧道一般终止在 ISP 网关上，因此一般情况下不会对用户网的安全技术提出较高要求。
- 从扩展性的角度看，第二层隧道内封装了整个 PPP 帧，这可能产生传输效率问题。其次，PPP 会话贯穿整个隧道并终止在用户侧设备上，导致用户侧网关必须要保存大量 PPP 会话状态与信息，这将对系统负荷产生较大的影响，也会影响到系统的扩展性。此外，由于 PPP 的 LCP（Link Control Protocol）及 NCP（Network Control Protocol）协商都对时间非常敏感，这样隧道的效率降低会造成 PPP 对话超时等一系列问题。相反，第三层隧道终止在 ISP 的网关内，PPP 会话终止在 NAS 处，用户侧网关无需管理和维护每个 PPP 对话的状态，从而减轻了系统负荷。
- 一般地，第二层隧道协议和第三层隧道协议都是独立使用的，如果合理地将这两层协议结合起来使用，将可能为用户提供更好的安全性（如将 L2TP 和 IPSec 协议配合使用）和更佳的性能。

6.2 L2TP

L2TP 是二层 VPN 技术，提供了对 PPP 链路层数据包的通道（Tunnel）传输支持，允许二层链路端点和 PPP 会话点驻留在不同设备上，并且采用包交换网络技术进行信息交互，扩展了 PPP 模型。

6.2.1 介绍

定义

PPP 协议定义了一种封装技术，可以在二层点到点链路上传输多种协议数据包，这时，用户与 NAS 之间运行 PPP，二层链路端点与 PPP 会话点在相同硬件设备上。

L2TP 协议提供了对 PPP 链路层数据帧的隧道（Tunnel）传输支持，允许二层链路端点和 PPP 会话点驻留在不同设备上，并采用包交换技术进行信息交互，从而扩展了 PPP 模型。

L2TP 协议结合了 L2F 协议和 PPTP 协议的优点，成为 IETF 有关二层隧道协议的工业标准。

目的

L2TP 可以在非点对点的网络上建立点对点的 PPP 会话连接，用于在用户和企业的服务器之间透明传输 PPP 报文。

6.2.2 参考标准和协议

与 L2TP 特性相关的参考标准与协议如下：

- RFC 1661：The Point-to-Point Protocol (PPP)
- RFC 1918：Address Allocation for Private Internets
- RFC 2661：Layer Two Tunneling Protocol "L2TP"
- RFC 2809：Implementation of L2TP Compulsory Tunneling via RADIUS
- RFC 2888：Secure Remote Access with L2TP

6.2.3 可获得性

License 支持

本特性无须 License 支持。

版本支持

产品	支持版本
Quidway Eudemon 8080E/8160E	V100R003

6.2.4 VPDN 简介

L2TP（Layer 2 Tunneling Protocol）属于 VPDN 隧道协议的一种。为了更好的理解 L2TP，下面先简单介绍 VPDN。

VPDN（Virtual Private Dial Network）采用专用的网络加密通信协议，在公共网络上为企业建立安全的虚拟专网。企业驻外机构和出差人员可以远程经由公共网络，通过虚拟加密隧道实现和企业总部之间的网络连接，而公共网络上其他用户则无法穿过虚拟隧道访问企业网内部的资源。

VPDN 有以下两种实现方式：

- 接入服务器发起 VPDN 连接

  NAS（Network Access Server，网络接入服务器）通过使用 VPDN 隧道协议，将客户的 PPP 连接直接连到企业的 VPDN 网关上，从而与 VPDN 网关建立隧道。

  其优势在于：对用户透明，用户只需要登录一次就可以接入企业网络，由企业网进行用户认证和地址分配，不占用公共地址，用户可使用各种平台上网。

  这种方式需要 NAS 支持 VPDN 协议，需要认证系统支持 VPDN 属性，网关一般使用 Eudemon 或 VPN 专用服务器。

- 用户发起 VPDN 连接

  客户端与 VPDN 网关建立隧道。这种方式由客户端先建立与 Internet 的连接，再通过专用的客户软件（如 Windows 2000 支持的 L2TP 客户端）与 VPDN 网关建立隧道连接。优缺点如下：

  - 优点：用户上网的方式和地点没有限制，不需 ISP 介入。

- 缺点：用户需要安装专用的软件（一般都是 Win2000 平台的 L2TP 客户端），限制了用户使用的平台。

VPDN 隧道协议可分为：

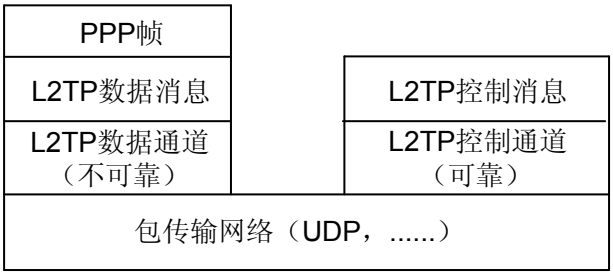
- PPTP（Point-to-Point Tunneling Protocol，点到点隧道协议）
- L2F（Layer 2 Forwarding，二层转发）
- L2TP（Layer 2 Tunneling Protocol，二层隧道协议）

目前使用最广泛的是 L2TP。

6.2.5 L2TP 协议简介

L2TP 协议结构

图 6-3 L2TP 协议结构



如图 6-3 所示，L2TP 协议结构描述了 PPP 帧、控制消息和控制通道以及数据消息、数据通道之间的关系。PPP 帧在不可靠的 L2TP 数据通道上进行传输，控制消息在可靠的 L2TP 控制通道内传输。

通常 L2TP 数据以 UDP 报文形式发送。L2TP 注册了 UDP 端口 1701，但是这个端口仅用于初始的隧道建立过程。L2TP 隧道发起方（LAC）任选一个空闲端口（未必是 1701）向接收方（LNS）的 1701 端口发送报文；LNS 收到报文后，也任选一个空闲端口（未必是 1701），给 LAC 的指定端口回送报文。至此，双方的端口选定，并在隧道保持连通的时间段内不再改变。

隧道和会话的概念

在 LNS（L2TP Network Server，L2TP 网络服务器）和 LAC（L2TP Access Concentrator，L2TP 访问集中器）对之间存在着两种类型的连接：

- 隧道（Tunnel）连接：它定义了互相通信的两个实体 LNS 和 LAC。
- 会话（Session）连接：它复用在隧道连接之上，用于表示承载在隧道连接中的每个 PPP 会话过程。

在同一对 LAC 和 LNS 之间可以建立多个 L2TP 隧道，隧道由一个控制连接和至少一个会话（Session）组成。会话连接必须在隧道建立（包括身份保护、L2TP 版本、帧类型、硬件传输类型等信息的交换）成功之后进行，每个会话连接对应于 LAC 和 LNS 之间的一个 PPP 数据流。控制消息和 PPP 数据报文都在隧道上传输。

L2TP 使用 Hello 报文来检测隧道的连通性。LAC 和 LNS 定时向对端发送 Hello 报文，如果在一段时间内未收到 Hello 报文的应答，该会话将被清除。

控制消息和数据消息的概念

L2TP 中存在控制消息和数据消息两种消息，其中：

- 控制消息用于隧道和会话连接的建立、维护以及传输控制。

  控制消息的传输是可靠传输，并且支持对控制消息的流量控制和拥塞控制。
- 数据消息则用于封装 PPP 帧并在隧道上传输。

  数据消息的传输是不可靠传输，如果数据报文丢失，不予重传，不支持对数据消息的流量控制和拥塞控制。

控制消息和数据消息共享相同的报文头。L2TP 报文头中包含隧道标识符（Tunnel ID）和会话标识符（Session ID）信息，用来标识不同的隧道和会话。隧道标识相同、会话标识不同的报文将被复用在一个隧道上，报文头中的隧道标识符与会话标识符由对端分配。

两种典型的 L2TP 隧道模式

Eudemon 支持两种典型的 L2TP 隧道模式：

- NAS-Initialized

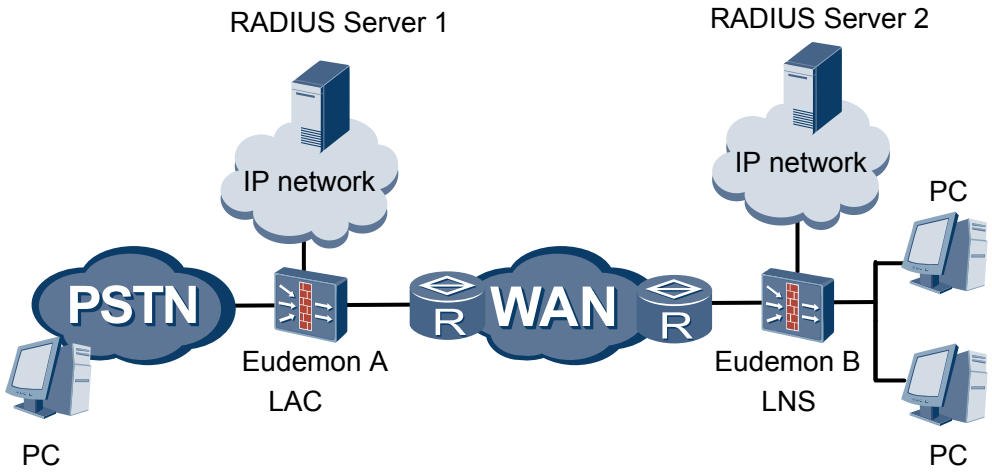
  远端系统通过 PSTN/ISDN 拨入 LAC，由 LAC（NAS）通过 Internet 向 LNS 发起建立隧道连接请求。由 LNS 为拨号用户分配私有 IP 地址，对远程拨号用户的验证与计费既可由 LAC 侧的代理完成，也可在 LNS 完成。
- Client-Initialized

  LAC 客户可直接向 LNS 发起隧道连接请求，无需再经过一个单独的 LAC 设备。在 LNS 设备上收到了 LAC 客户的请求之后，根据用户名、密码进行验证，并且为 LAC 客户分配私有 IP 地址。

L2TP 隧道会话的建立过程

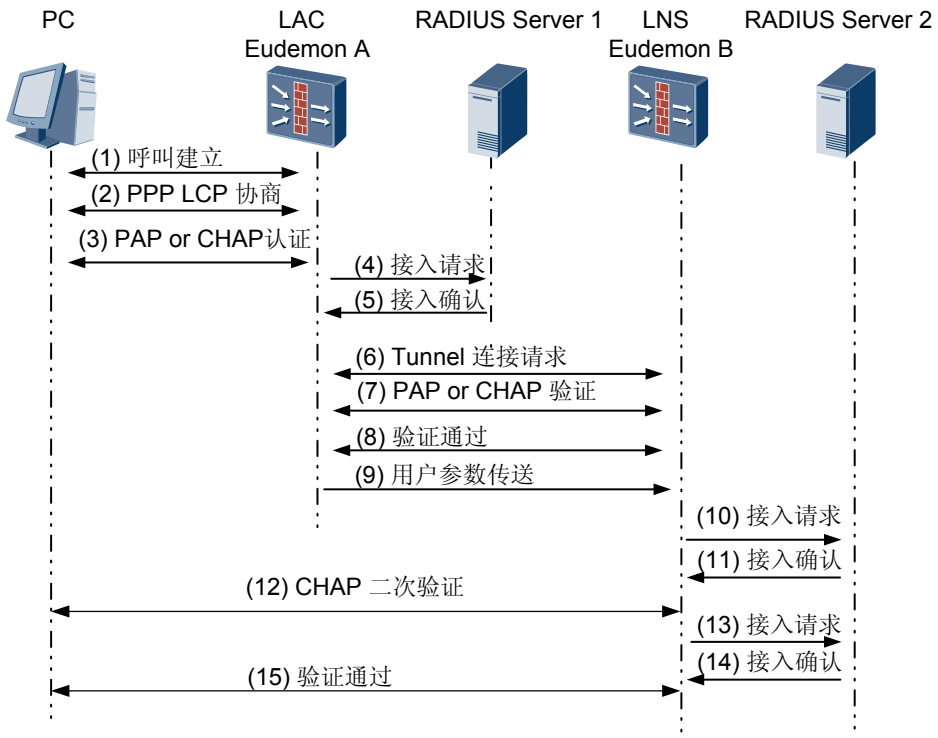
L2TP 的典型组网如图 6-4 所示。

图 6-4 L2TP 隧道的典型组网示意图



L2TP 隧道的呼叫建立流程如图 6-5 所示。

图 6-5 L2TP 隧道的呼叫建立流程



L2TP 隧道的呼叫建立流程过程如下。

1. 用户端 PC 发起呼叫连接请求。
2. PC 和 LAC 端（Eudemon A）进行 PPP LCP 协商。
3. LAC 对 PC 提供的用户信息进行 PAP（Password Authentication Protocol）或 CHAP（Challenge Handshake Authentication Protocol）认证。
4. LAC 将认证信息（用户名、密码）发送给 RADIUS 服务器（RADIUS Sever 1）进行认证。
5. RADIUS 服务器（RADIUS Sever 1）认证该用户，如果认证通过则返回该用户对应的 LNS（Eudemon B）地址等相关信息，并且 LAC 准备发起 Tunnel 连接请求。
6. LAC 端向指定 LNS 发起 Tunnel 连接请求。
7. LNS 对 LAC 进行 PAP 或 CHAP 验证。

   Eudemon 8080E/8160E 支持 PPP 的 PAP 和 CHAP 两种验证方式。

   - PAP 验证为两次握手验证，口令为明文

     LAC 端向 LNS 端发送用户名和口令，LNS 根据本端用户表查看用户名和口令是否正确，然后返回不同的响应（Acknowledge or Not Acknowledge）。
   - CHAP 验证为三次握手验证，口令为密文（密钥）

     LAC 端向指定 LNS 发送 CHAP challenge 信息，LNS 回送该 challenge 响应消息 CHAP response，并发送 LNS 侧的 CHAP challenge，LAC 返回该 challenge 的响应消息 CHAP response。
8. 隧道验证通过。
9. LAC 端将用户 CHAP response、response identifier 和 PPP 协商参数传送给 LNS。
10. LNS 将接入请求信息发送给 RADIUS 服务器（RADIUS Sever 2）进行认证。

11. RADIUS 服务器认证该请求信息，如果认证通过则返回响应信息。
12. 若用户在 LNS 侧配置强制本端 CHAP 认证，则 LNS 对用户进行认证，发送 CHAP challenge，用户侧回应 CHAP response。
13. LNS 再次将接入请求信息发送给 RADIUS 服务器进行认证。
14. RADIUS 服务器认证该请求信息，如果认证通过则返回响应信息。
15. 验证通过，用户访问企业内部资源。

说明

Eudemon 8080E/8160E 不支持 LAC（L2TP Access Concentrator）功能。可以选用其他支持 LAC 的 Eudemon 设备。

L2TP 协议的特点

L2TP 协议有如下特点：

- 灵活的身份验证机制以及高度的安全性
  - L2TP 协议本身并不提供连接的安全性，但它可依赖于 PPP 提供的认证（比如 CHAP、PAP 等），因此具有 PPP 所具有的所有安全特性。
  - L2TP 可以与 IPSec 结合，使通过 L2TP 所传输的数据更难被攻击。
  - 可根据特定的网络安全要求，在 L2TP 之上采用通道加密技术、端对端数据加密或应用层数据加密等方案来提高数据的安全性。
- 多协议传输

  L2TP 传输 PPP 数据包，这样就可以在 PPP 数据包内封装多种协议。
- 支持 RADIUS 服务器的验证

  LAC 端将用户名和密码发往 RADIUS 服务器进行验证申请，由 RADIUS 服务器负责接收用户的验证请求，完成验证。
- 支持内部地址分配

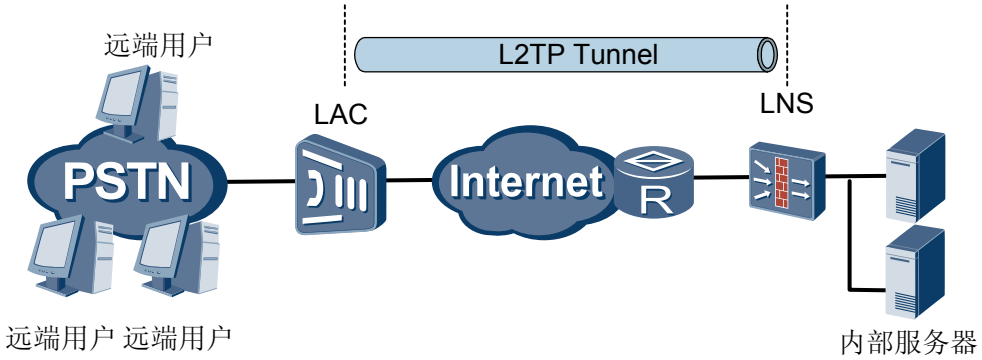
  LNS 可以对远端用户的地址进行动态的分配和管理，可支持私有地址应用。为远端用户所分配的地址不是 Internet 地址而是企业内部的私有地址，这样方便了地址的管理并可以增加安全性。
- 可靠性

  L2TP 协议支持备份 LNS，当一个主 LNS 不可达之后，LAC 可以重新与备份 LNS 建立连接，增加了 VPN 服务的可靠性和容错性。

6.2.6 L2TP 典型应用

使用 L2TP 协议构建的 VPDN 应用的典型组网如图 6-6 所示。

图 6-6 应用 L2TP 构建的 VPDN 服务



其中，LAC（L2TP Access Concentrator）表示 L2TP 访问集中器，是附属在交换网络上的具有 PPP 端系统和 L2TP 协议处理能力的设备。LAC 一般是一个 NAS，主要是通过 PSTN/ISDN 网络为用户提供接入服务。LNS（L2TP Network Server）表示 L2TP 网络服务器，是 PPP 端系统上用于处理 L2TP 协议服务器端部分的设备。

LAC 位于 LNS 和远端系统（远地用户和远地分支机构）之间，用于在 LNS 和远端系统之间传递信息包，把从远端系统收到的信息包按照 L2TP 协议进行封装并送往 LNS，将从 LNS 收到的信息包进行解封装并送往远端系统。LAC 与远端系统之间可以采用本地连接或 PPP 连接，VPDN 应用中通常为 PPP 连接。LNS 作为 L2TP 隧道的另一侧端点，是 LAC 的对端设备，是被 LAC 进行隧道传输的 PPP 会话的逻辑终止端点。

6.3 GRE

GRE 是三层隧道的封装协议,对某些网络层协议的数据报文进行封装并在另一网络层协议中传输。提供了将一种协议的报文封装在另一种协议报文中的机制，使报文能够在隧道中传输。

6.3.1 介绍

定义

GRE（General Routing Encapsulation，通用路由封装）是对某些网络层协议的数据报文进行封装，使这些被封装的报文能够在另一网络层协议中传输。

GRE 可以作为 VPN 的第三层隧道协议，在协议层之间采用了一种被称之为隧道（Tunnel）的技术。Tunnel 是一个虚拟的点对点的连接，在实际中可以看成仅支持点对点连接的虚拟接口，这个接口提供了一条通路使封装的数据报文能够在这个通路上传输，并且在一个 Tunnel 的两端分别对数据报文进行封装及解封装。

目的

为了使某些网络层协议的报文能够在 IPv4 网络中传输，可以将某些网络层协议的报文进行封装，以此解决了异种网络的传输问题。

GRE 也可以作为 VPN 的第三层隧道协议，为 VPN 数据提供透明传输通道。

6.3.2 参考标准和协议

与 GRE 特性相关的参考标准与协议如下：

- RFC1701：Generic Routing Encapsulation（GRE）

- RFC1702：Routing Encapsulation over IPv4 networks
- RFC2784：Generic Routing Encapsulation (GRE)
- draft-ietf-l3vpn-greip-2547-02：Use of PE-PE GRE or IP in BGP/MPLS IP VPNs
- draft-ietf-mpls-in-ipor-gre-08：Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)

6.3.3 可获得性

License 支持

本特性无须 License 支持。

版本支持

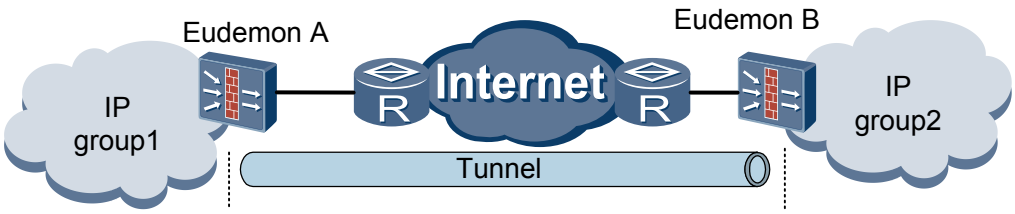
产品	支持版本
Quidway Eudemon 8080E/8160E	V100R003

6.3.4 GRE 的实现

报文在 GRE 中的传输过程

一个数据报文要在 Tunnel 中传输，必须经过封装与解封装两个过程，下面以图 6-7 的网络为例说明这两个过程：

图 6-7 私有 IP 网络通过 GRE 隧道互连



- 加封装过程

  Eudemon A 连接 IP group1 的接口收到 IP 数据报后首先交由 IP 协议处理，IP 协议检查 IP 报头中的目的地址域来确定如何转发此包。若报文的目的地址要经过 Tunnel 的虚拟网络地址，则将此报文发给 Tunnel 端口。Tunnel 口收到此包后进行 GRE 封装，封装完成后交给 IP 模块处理，在封装 IP 报文头后，根据此包的目的地址及路由表交由相应的网络接口处理。

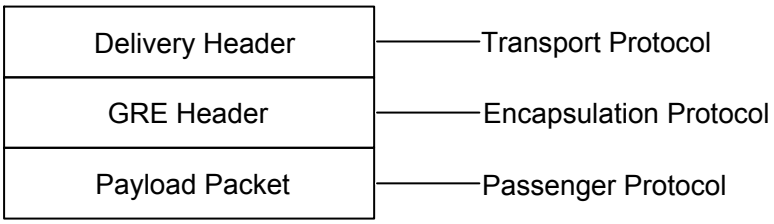
- 解封装的过程

  解封装过程和封装过程相反。Eudemon B 从 Tunnel 接口收到 IP 报文后检查目的地址，若发现目的地为 Eudemon B，则交给 GRE 协议模块处理（进行检验识别关键字、检查校验等）；GRE 协议模块完成相应的处理后，去掉 IP 头和 GRE 报头，再交由 IP 协议模块处理，IP 协议模块象对待一般数据报一样对此数据报进行处理。

GRE 报文格式

系统收到需要进行封装和路由的某网络层协议数据时，将首先对其加上 GRE 报文头，使之成为 GRE 报文，再被封装在 IP 报文中，这样就可完全由 IP 层负责此报文的转发（Forwarded）。封装后的 GRE 报文格式如图 6-8 所示。

图 6-8 封装好的 GRE 报文格式

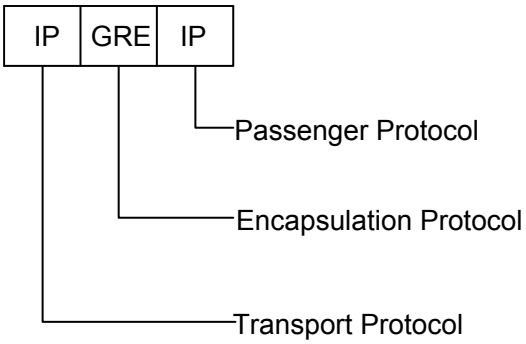


其中：

- 净荷（Payload）
  系统收到的需要封装和路由的数据报称为净荷。
- 乘客协议（Passenger Protocol）
  封装前的报文协议称为乘客协议。
- 封装协议（Encapsulation Protocol）
  上述的 GRE 协议称为封装协议，也称为运载协议（Carrier Protocol）。
- 传输协议（Transport Protocol 或者 Delivery Protocol）
  负责对封装后的报文进行转发的协议称为传输协议。

举例来说，一个封装在 IP Tunnel 中的 IP 传输报文的格式如图 6-9 所示。

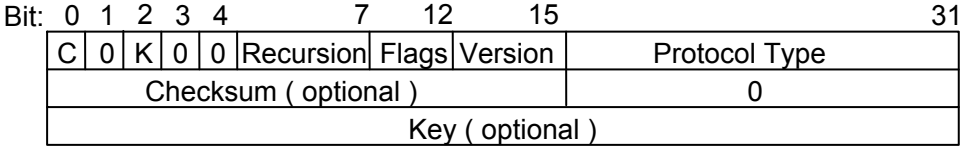
图 6-9 封装在 IP Tunnel 中的 IP 传输报文格式



GRE 报文头

GRE 实现遵循 RFC 标准。GRE 头格式如图 6-10 所示。

图 6-10 GRE 头格式



各字段解释如下：

- C

  校验和验证位。如果该位置 1，表示 GRE 头插入了校验和（Checksum）字段；该位为 0 表示 GRE 头不包含校验和字段。

- K

  关键字位。如果该位置 1，表示 GRE 头插入了关键字（Key）字段；该位为 0 表示 GRE 头不包含关键字字段。

- Recursion

  用来表示 GRE 报文被封装的层数。完成一次 GRE 封装后将该字段加 1。该字段的作用是防止报文被无限次的封装。

  Eudemon 8080E/8160E 只支持一次 GRE 封装。

- Flags

  预留字段。当前必须设为 0。

- Version

  版本字段，必须置为 0。Version 为 1 是使用在 RFC2637 的 PPTP 中。

- Protocol Type

  乘客协议的协议类型。

- Checksum

  GRE 头及其负载的校验和字段。

- Key

  关键字字段，隧道接收端用于对收到的报文进行验证。

说明

GRE 头不包含源路由字段，Bit 1、Bit3 和 Bit 4 都置为 0。

GRE 的特点

GRE 主要有以下特点：

- 机制简单，对隧道两端设备的 CPU 负担小。
- 本身不提供数据的加密，可以与 IPSec 结合使用。
- 不提供流量控制和 QoS。

6.3.5 安全机制

GRE 本身提供两种安全机制：

- 校验和验证
- 识别关键字验证

校验和验证

校验和验证是指对封装的报文进行端到端校验。

RFC1701 中规定：如果 GRE 报文头中的 C 位置位，则校验和有效。校验和是 GRE 头中的可选字段。如果 C 位置 1，则发送方将根据 GRE 头及 payload 信息计算校验和，在报文头的 Checksum 字段的位置插入校验和，将包含校验和的报文发送给对端。接收方

对接收到的报文计算校验和，并与报文中的校验和进行比较。如果计算出来的校验和与报文中的校验和一致，则对报文进一步处理，否则丢弃报文。

隧道两端可以根据实际需要选择是否配置校验和，从而决定是否触发校验功能。如果本端配置了校验和而对端没有配置，则本端将不会对接收到的报文进行校验和检查；相反本端没有配置校验和而对端已配置，本端将对从对端发来的报文进行校验和检查。

因校验和配置不同，对收发报文的处理方式也不同，请参见表 6-1。

表 6-1 校验和与报文处理

本端	对端	本端对接收报文的处理	本端对发送报文的处理
配置校验和	没有配置校验和	不检查校验和	计算校验和
没有配置校验和	配置校验和	检查校验和	不计算校验和

识别关键字验证

识别关键字（key）是指对 Tunnel 接口进行校验。通过这种安全机制，可以防止错误识别、接收其它隧道来的报文。

RFC1701 中规定：若 GRE 报文头中的 K 位置 1，则在 GRE 头中插入关键字字段，收发双方将进行遂道识别关键字的验证。

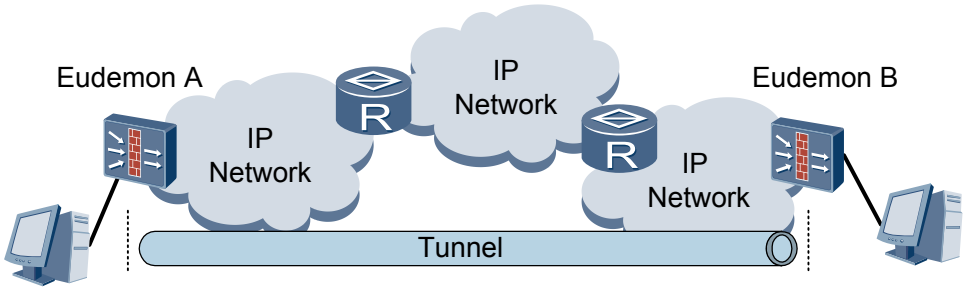
关键字字段是一个四字节长的数，在报文封装时被插入 GRE 头。关键字的作用是认证隧道。属于同一流量的报文使用相同的关键字。在报文解封装时，隧道端将基于关键字来识别属于相同流量的数据报。

只有 Tunnel 两端设置的识别关键字完全一致时才能通过验证，否则将报文丢弃。这里的“完全一致”是指两端都不设置识别关键字；或者两端都设置关键字，且关键字的值相等。

6.3.6 GRE 典型应用

扩大跳数受限的网络工作范围

图 6-11 扩大网络工作范围



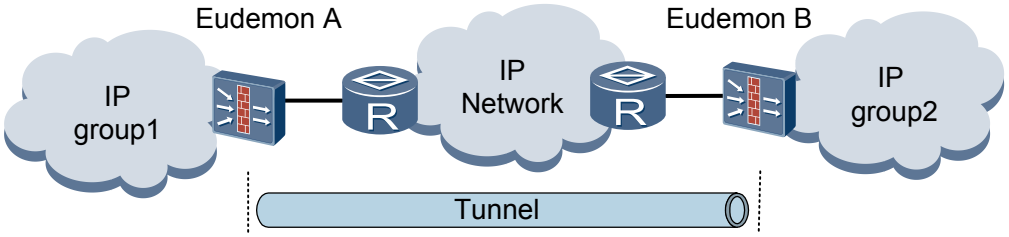
如图 6-11 所示，网络运行 IP 协议，假设 IP 协议限制的跳数为 255。如果两台 PC 之间的跳数超过 255，它们将无法通信。在网络中使用隧道（Tunnel）可以隐藏一部分跳数，从而扩大网络的工作范围。

将不连续的子网连接起来，用于组建 VPN

使用 GRE 隧道可以将不连续的子网连接起来，实现跨越广域网的 VPN。

例如，两个 VPN 子网 group1 和 group2 位于不同的城市，通过在网络边界设备之间建立 GRE 隧道，可以把这两个子网连接成一个连续的 VPN 网络。

图 6-12 Tunnel 连接不连续子网



如图 6-12 所示，运行 IP 协议的两个子网 group1 和 group2 分别在不同的城市，通过使用隧道可以实现跨越广域网的 VPN。

6.4 IPSec

IPSec 是一系列为 IP 网络提供完整安全性的协议和服务的集合。IPSec 工作在 IP 层，为上层协议和应用提供透明的安全服务。

6.4.1 介绍

定义

IPSec（Internet Protocol Security）是一个工业标准网络安全协议，为 IP 网络通信提供透明的安全服务，保护 TCP/IP 通信免遭窃听和篡改，可以有效抵御网络攻击，同时保持易用性。

IPSec 通过 AH（Authentication Header）和 ESP（Encapsulating Security Payload）这两个安全协议来实现私有性、完整性、真实性和防重放，并且还可以通过 IKE 为 IPSec 提供自动协商交换密钥、建立和维护安全联盟的服务，以简化 IPSec 的使用和管理。

目的

IPSec 为 IP 数据报文提供了高质量的、可互操作的、基于密码学的安全性。IPSec 协议是特定的通信方之间在 IP 层通过加密与数据源验证等方式，来保证数据报在网络上传输时的私有性、完整性、真实性和防重放。

由于 IP 包本身并不集成任何安全特性，很容易便可伪造出 IP 包的地址、修改其内容、重播以前的包以及在传输途中拦截并查看包的内容。针对这些问题，IPSec 可有效地保护 IP 数据报文的安全。

6.4.2 参考标准和协议

与 IPSec 特性相关的参考标准与协议如下：

- RFC3948：UDP Encapsulation of IPsec ESP Packets
- RFC 2403：The Use of HMAC-MD5-96 within ESP and AH
- RFC 2857：The Use of HMAC-RIPEMD-160-96 within ESP and AH
- RFC 4305：Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4359：The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 2409： The Internet Key Exchange (IKE)
- RFC 3625：More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3664：The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 3706：A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3947：Negotiation of NAT-Traversal in the IKE
- RFC 4109：Algorithms for Internet Key Exchange version 1 (IKEv1)
- RFC 4306：Internet Key Exchange (IKEv2) Protocol
- RFC 4307：Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4322：Opportunistic Encryption using the Internet Key Exchange (IKE)
- RFC 4434：The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4478：Repeated Authentication in Internet Key Exchange (IKEv2)

6.4.3 可获得性

License 支持

用户能够创建的隧道数由所购买的 License 决定，创建超出 License 限制数目的安全策略不起作用。

版本支持

产品	支持版本
Quidway Eudemon 8080E/8160E	V100R003

6.4.4 IPSec 协议简介

IPSec 协议是特定的通信方之间在 IP 层通过加密与数据源验证等方式，来保证数据报在网络上传输时的私有性、完整性、真实性和防重放。具体解释如下：

- 私有性（Confidentiality）

  指对用户数据进行加密保护，用密文的形式传送。
- 完整性（Data integrity）

  指对接收的数据进行验证，以判定报文是否被篡改。
- 真实性（Data Authenticity）

  指验证数据源，以保证数据来自真实的发送者。
- 防重放（Anti-replay）

  指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝重复的数据包。

IPSec 通过 AH 和 ESP 两个安全协议实现了上述目标。为简化 IPSec 的使用和管理，IPSec 还可以通过 IKE 进行自动协商交换密钥、建立和维护安全联盟的服务。具体介绍如下：

- AH（Authentication Header）协议

  AH 是报文头验证协议，主要提供的功能有数据源验证、数据完整性校验和防报文重放功能。然而，AH 并不加密所保护的数据报。
- ESP（Encapsulating Security Payload）协议

  ESP 是封装安全载荷协议。它除提供 AH 协议的所有功能外（但其数据完整性校验不包括 IP 头），还可提供对 IP 报文的加密功能。
- IKE（Internet Key Exchange）协议

  IKE 协议用于自动协商 AH 和 ESP 所使用的密码算法。

说明

- AH 和 ESP 可以单独使用，也可以同时使用。
- IKE 协商并不是必须的，IPSec 所使用的策略和算法等也可以采用手工方式。

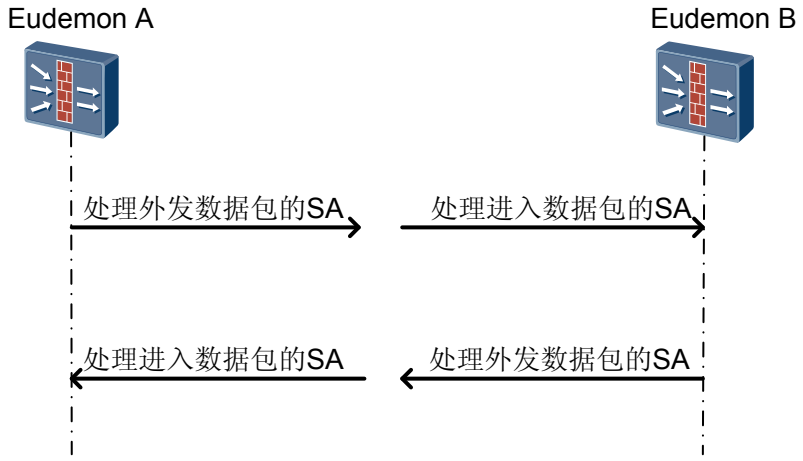
6.4.5 安全联盟

IPSec 在两个端点之间提供安全通信，端点被称为 IPSec 对等体。

安全联盟是 IPSec 对等体间对某些要素的约定，例如，使用哪种协议（AH、ESP 还是两者结合使用）、协议的封装模式（传输模式和隧道模式）、加密算法（DES 和 3DES）、特定数据流中保护数据的共享密钥以及密钥的生存周期等。

安全联盟是单向的。如果有两个 Eudemon（A 和 B）使用 ESP 进行安全通信，EudemonA 就需要两个 SA，一个 SA 处理外发数据包，另一个 SA 处理进入的数据包。同样，EudemonB 也需要两个 SA。如图 6-13 所示。

图 6-13 安全联盟是单向的逻辑连接



安全联盟还与协议相关。如果 EudemonA 和 EudemonB 同时使用 AH 和 ESP 进行安全通信，对于 EudemonA 就需要四个 SA，AH 协议的两个 SA（出方向和入方向各一个）和 ESP 协议的两个 SA（出方向和入方向各一个）。同样，EudemonB 也需要四个 SA。

安全联盟由一个三元组来唯一标识，这个三元组包括：

- SPI（Security Parameter Index）

  SPI 是为唯一标识 SA 而生成的一个 32 比特的数值，它在 AH 和 ESP 头中传输。
- 目的 IP 地址
- 安全协议号（AH 或 ESP）

安全联盟由一个三元组来唯一标识，这个三元组包括 SPI（Security Parameter Index）、目的 IP 地址、安全协议号（AH 或 ESP）。SPI 是为唯一标识 SA 而生成的一个 32 比特的数值，它在 AH 和 ESP 头中传输。

安全联盟的生存周期

安全联盟具有生存周期。生存周期的计算包括两种方式：

- 以时间为限制，每隔指定的时间就进行更新。
- 以流量为限制，每传输指定的数据量（字节）就进行更新。

安全联盟的协商方式

安全联盟的协商方式有两种：

- 手工方式（**manual**）

  手工方式配置比较复杂，创建安全联盟所需的全部信息都必须手工配置，并且不支持 IPSec 的一些高级特性（例如定时更新密钥）。

  优点是可以不依赖 IKE 而单独实现 IPSec 功能。

- IKE 自动协商方式（**isakmp**）

  IKE 自动协商方式相对比较简单，只需要配置好 IKE 协商安全策略的信息，由 IKE 自动协商来创建和维护安全联盟。

当与 Eudemon 进行通信的对等体设备数量较少时，或是在小型网络环境中，手工配置安全联盟是可行的。对于中、大型的网络环境中，推荐使用 IKE 协商建立安全联盟。

6.4.6 数据保护方式

IPSec 通过对要保护数据进行加密和验证来提供隧道保护。

用户可以在 Eudemon 上配置 IPSec 采用 AH 方式、ESP 方式或者同时使用 AH 和 ESP 方式对需要通过隧道传输的数据进行保护。

AH 保护方式

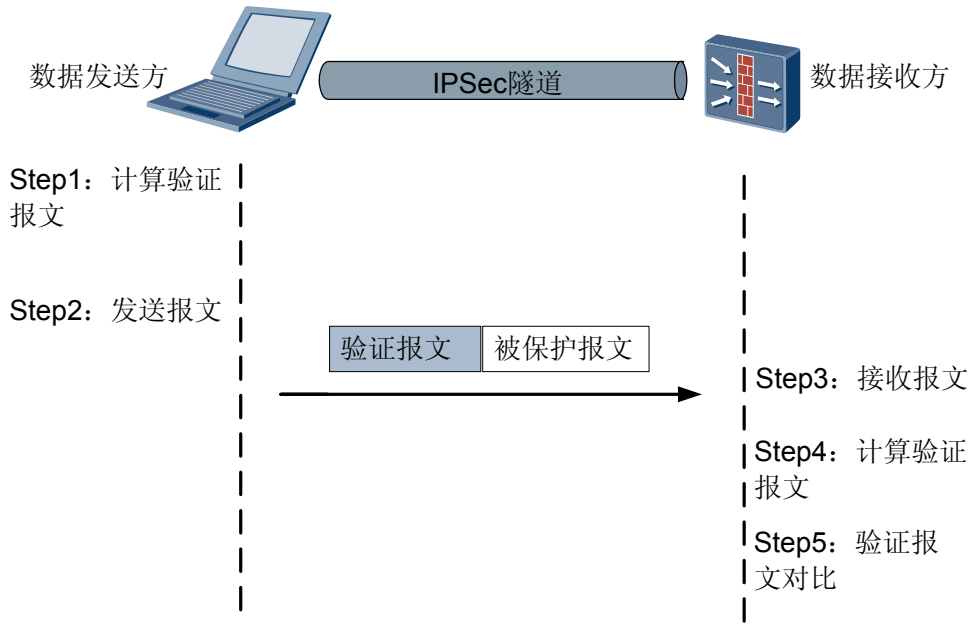
当用户配置 IPSec 采用 AH 方式对要传送数据进行保护时，可以实现如下功能：

- 数据完整性校验

  防止数据在发送过程中被非法篡改。通过数据发送方和数据接收方持有相同验证密钥，并使用相同验证算法对要保护的数据进行验证来实现。

  验证过程如图 6-14 所示，数据发送方在发送数据前使用验证密钥和指定验证算法对要发送的数据进行运算，并将运算后的结果随同要发送的数据报文一同发送给接收方；接收方接收到报文后，也使用相同的验证密钥和验证算法对报文内容进行运算，如果计算出来的结果与随同在数据报文中的发送方的计算结果一致，则认为数据报文在网络传送过程中没有被非法篡改，否则会认为已经被篡改并丢弃。

图 6-14 IPSec 数据完整性验证过程



当 Eudemon 配置使用 AH 保护方式对数据进行保护时，会对整个 IP 报文进行验证，安全性较 ESP 方式更高。

- 数据源验证

  验证报文的发送方是否合法。

- 防报文重放功能

  当数据接收方遭到来自网络上的重复报文攻击时，可以防止数据接收方重复处理同一个数据报文。

ESP 保护方式

当用户配置 IPSec 采用 ESP 方式对要传送数据进行保护时，可以实现如下功能：

- 数据完整性校验

  防止数据在发送过程中被非法篡改。通过数据发送方和数据接收方持有相同验证密钥，并使用相同验证算法对要保护的数据进行验证来实现。

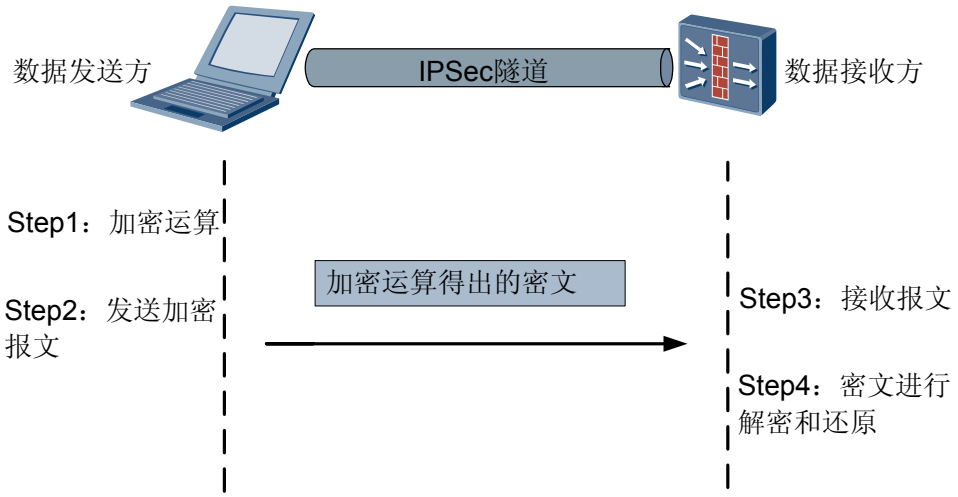
  验证过程与 AH 方式相同，当 Eudemon 配置使用 ESP 保护方式对数据进行保护时，不会对整个 IP 报文进行验证，仅对 IP 报文头之外的内容进行验证，其安全性没有 AH 方式高。

- 数据加密

  防止数据在传送过程中被非法查看。通过数据发送方和数据接收方持有相同加密密钥，并使用相同加密算法对要保护的数据分别进行加密和解密还原实现。

  加密和解密过程如图 6-15 所示，数据发送方在发送数据前使用加密密钥和指定加密算法对要发送的数据进行加密，将加密后的密文发送给接收方；接收方接收到密文后，也使用相同的加密密钥和加密算法对报文内容解密和还原，由于使用密文传输，为要传送报文提供了安全保护。

图 6-15 IPSec 数据加密过程



- 数据源验证

  验证报文的发送方是否合法。

- 防报文重放功能

当数据接收方遭到来自网络上的重复报文攻击时，可以防止数据接收方重复处理同一个数据报文。

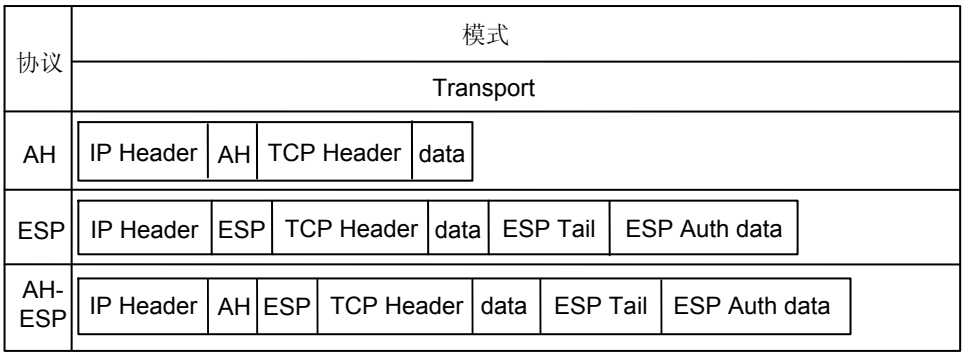
6.4.7 封装模式

IPSec 协议的封装模式有两种：

- 传输模式

  在传输模式下，AH 或 ESP 被插入到 IP 头之后但在所有传输层协议之前，或所有其他 IPSec 协议之前。以 TCP 为例，如图 6-16 所示。

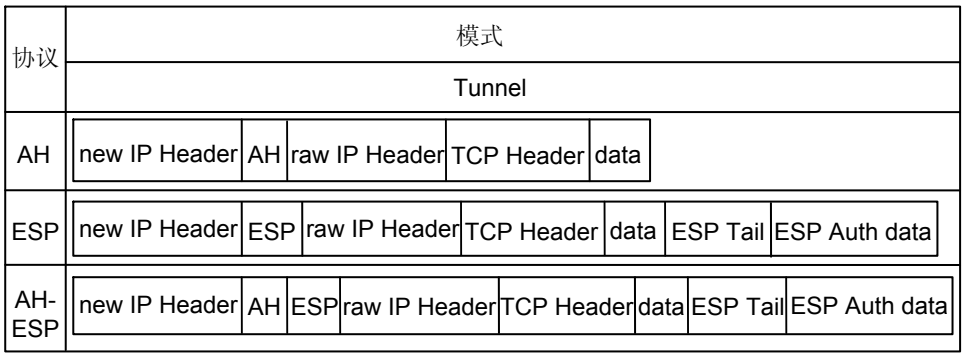
图 6-16 IPSec 协议的传输模式



- 隧道模式

  在隧道模式下，AH 或 ESP 插在原始 IP 头之前，另外生成一个新的报文头放到 AH 或 ESP 之前。以 TCP 为例，如图 6-17 所示。

图 6-17 IPSec 协议的隧道模式



选择隧道模式还是传输模式可以从以下方面考虑：

- 从安全性来讲，隧道模式优于传输模式。它可以完全地对原始 IP 数据报进行验证和加密，而且，可以使用 IPSec 对等体的 IP 地址来隐藏客户机的 IP 地址。
- 从性能来讲，隧道模式因为有一个额外的 IP 头，所以它将比传输模式占用更多带宽。

6.4.8 验证算法与加密算法

验证算法

AH 和 ESP 都能够对 IP 报文的完整性进行验证，以判别报文在传输过程中是否被篡改。验证算法的实现主要是通过杂凑函数，杂凑函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPSec 对等体计算摘要，如果两个摘要是相同的，则表示报文是完整未经篡改的。

一般来说 IPSec 使用两种验证算法：

- MD5（Message Digest 5）

  MD5 通过输入任意长度的消息，产生 128bit 的消息摘要。
- SHA-1（Secure Hash Algorithm）

  SHA-1 通过输入长度小于 2^{64}bit 的消息，产生 160bit 的消息摘要。

SHA-1 的摘要长于 MD5，因而是更安全的。

加密算法

ESP 能够对 IP 报文内容进行加密保护，防止报文内容在传输过程中被窥探。加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。

一般来说 IPSec 使用加密算法有以下几种：

- DES（Data Encryption Standard）

  使用 56bit 的密钥对一个 64bit 的明文块进行加密。
- 3DES（Triple Data Encryption Standard）

  使用三个 56bit 的 DES 密钥（共 168bit 密钥）对明文进行加密。
- AES（Advanced Encryption Standard）

  使用 AES 密钥对明文进行加密。密钥的长度分为 128bit、192bit、256bit。

3DES 比 DES 具有更高的安全性，但其加密数据的速度要比 DES 慢得多。

6.4.9 IPSec NAT 穿越

NAT 穿越（NAT Traversal）

IPSec 的一个主要应用是建立 VPN，但在实际组网应用中，有一种情况会对部署 IPSec VPN 网络造成障碍：如果发起者位于一个私网内部，而它希望在自己与远端响应者之间直接建立一条 IPSec 隧道，这就涉及到 IPSec 与 NAT 的配合，主要问题在于，IKE 在协商过程中如何发现两个端点之间存在 NAT 网关，以及如何使 ESP 报文正常穿越 NAT 网关。

首先，建立 IPSec 隧道的两端需要进行 NAT 穿越能力协商，这是在 IKE 协商的前两个消息中进行的，通过 Vendor ID 载荷指明的一组数据来标识，该载荷数据的定义与所采用草案（draft）版本的不同而不同。

而 NAT 网关发现是通过 NAT-D 载荷来实现的，该载荷用于两个目的：

- 在 IKE Peer 之间发现 NAT 的存在。
- 确定 NAT 设备在 Peer 的哪一侧。

NAT 侧的 Peer 作为发起者，需要定期发送 NAT-Keepalive 报文，以使 NAT 网关确保安全隧道处于激活状态。

IPSec 穿越 NAT 的处理

IPSec 穿越 NAT，简单来说就是在原报文的 IP 头和 ESP 头间增加一个标准的 UDP 报头。当 ESP 报文穿越 NAT 网关时，NAT 对该报文的外层 IP 头和增加的 UDP 报头进行地址和端口号转换；转换后的报文到达 IPSec 隧道对端时，与普通 IPSec 处理方式相同，但在发送响应报文时也要在 IP 头和 ESP 头之间增加一个 UDP 报头。

6.4.10 IPSec 隧道化

概述

IPSec 隧道化是指将 IPSec 策略应用到 Tunnel 逻辑接口上而不用和具体的物理接口绑定。通过配置路由，任何物理接口收到的报文到可以被引导到 Tunnel 接口进行 IPSec 处理，经过处理后的 IPSec 报文通过路由来选择出接口，可以实现出接口的链路备份。

配置 IPsec 隧道化具有以下优点：

- 简化配置

  通过配置路由可以将任何物理接口的报文引到到 Tunnel 接口进行 IPSec 处理。简化了 IPSec 策略的配置，并且使 IPSec 配置不会受到网络规划的影响，增强了网络规划的可扩展性。
- 业务应用更灵活

  IPSec 隧道化在实施过程中明确地区分出“加密前”和“加密后”两个阶段，用户可以根据不同的组网需求灵活选择其它业务（例如 NAT、QoS）实施的阶段。
- 增强了链路可靠性

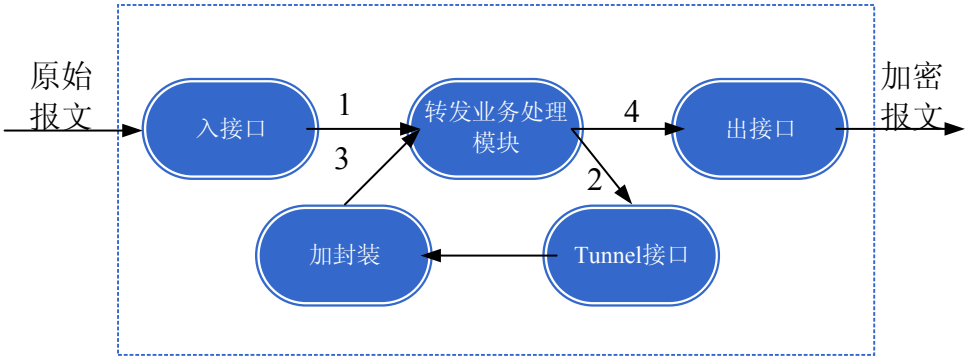
  IPSec 隧道化可以实现出接口链路的备份，增强了链路的可靠性。

工作原理

IPSec 隧道化对报文的加封装/解封装都在 Tunnel 接口上进行。报文到达 IPSec 设备后，需要 IPSec 处理的报文会被转发到 Tunnel 接口上进行加封装/解封装。

如图 6-18 所示，Tunnel 接口上报文进行加封装的过程如下：

图 6-18 IPSec 隧道化加封装原理



- Eudemon 的接口板将从入接口接收到的 IP 报文送到转发业务处理模块进行处理。
- 转发业务处理模块依据路由查询结果进行报文转发。若报文的出接口的 Tunnel 接口，且封装类型为 IPSec，则将此报文发送到 Tunnel 接口进行 IPSec 加封装处理。

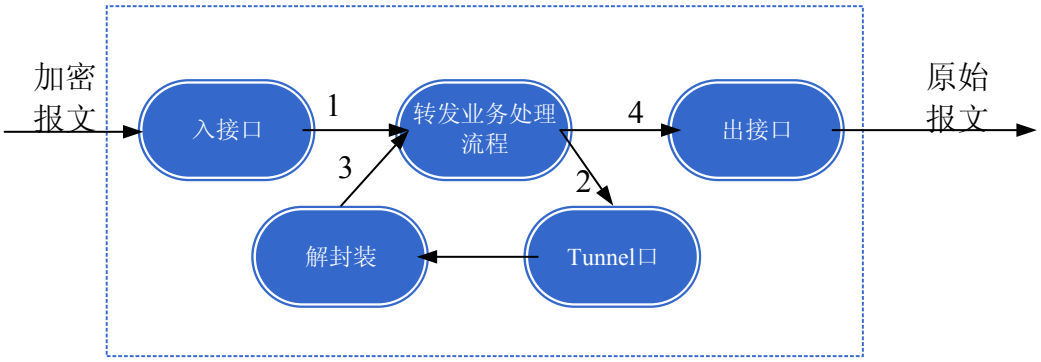
原始 IP 报文被封装在一个新的 IP 报文中，新 IP 头中的源地址和目的地址分别为 Tunnel 接口的源地址和目的地址。

- Tunnel 接口完成对报文的加封装处理后，将加密后的报文发送到转发业务处理模块进行处理。
- 转发业务处理模块进行第二次路由查询，将加密报文通过实际物理接口转发出去。

  IPSec 加封装流程中会对报文进行 ACL 规则匹配，在普通接口的 IPSec 报文处理过程中，如果报文没有命中 ACL 规则，则对报文进行透传处理。由于 Tunnel 接口是一个逻辑接口，如果不命中 ACL 规则，则无法为该报文确定出接口，报文将直接被丢弃。

如图 6-19 所示，Tunnel 接口上报文进行解封装的过程如下：

图 6-19 IPSec 隧道化解封装原理



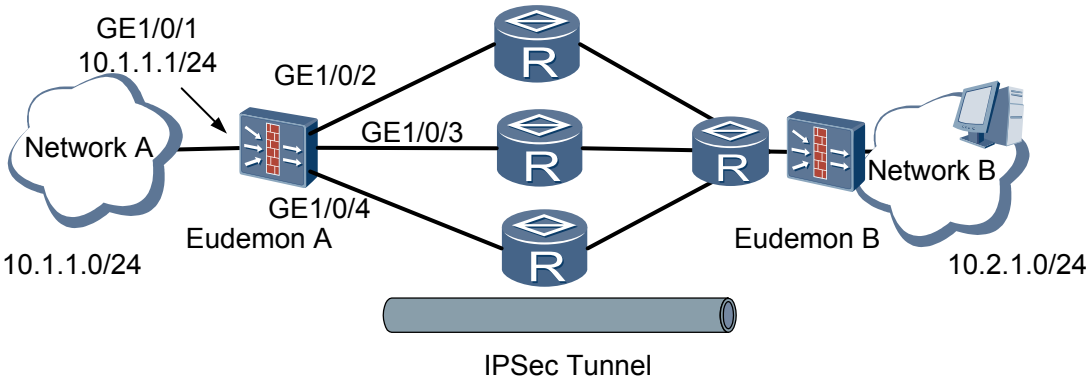
- Eudemon 的接口板将从入接口接收到的 IP 加密报文送到转发业务处理模块进行处理。
- 转发业务处理模块识别到此加密报文的目的地为本设备的 Tunnel 接口地址时，会将此加密报文送到相应的 Tunnel 接口进行 IPSec 解封装处理。将 IP 密文的外层 IP 头去掉，对内层 IP 报文进行解密处理。

  如果检查出该报文为应加密而未加密或不该加密却加密了的报文时，则进行丢弃处理。
- Tunnel 接口完成对加密报文的解封装处理之后，将 IP 明文重新送回转发业务处理模块处理。
- 转发业务处理模块进行第二次路由查询后，将 IP 明文从隧道的实际物理接口转发出去。

典型应用场景

IPSec 隧道化的典型应用场景如图 6-20。经 IPSec 处理后的 IPSec 报文，通过路由来选择出接口，可以实现出接口的链路备份。

图 6-20 IPSec 隧道化典型应用场景



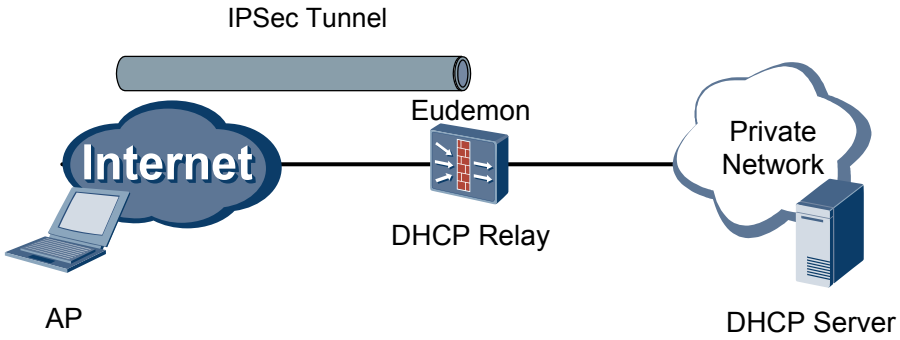
6.4.11 DHCP over IPSec

DHCP over IPSec 适用于远程移动设备访问公司内部网络的场景。

应用场景

如图 6-21 所示,移动设备 AP（Access Point）已经存在一个公网的 IP 地址，要访问公司内部网络可以通过向 DHCP 服务器发送请求获取相应的私有 IP 地址来实现。

图 6-21 DHCP over IPSec



DHCP 简介

DHCP(Dynamic Host Configuration Protocol)采用客户/服务器通信模式，由客户端向服务器提出配置申请（包括分配的 IP 地址、子网掩码、缺省网关等参数），服务器根据策略返回相应配置信息。协议中所定义的成员包括：

- DHCP 客户端
  网络中利用 DHCP 协议来获取配置参数（如：IP 地址）的主机。
- DHCP 服务器
  网络中向 DHCP 客户端返回配置参数的主机。
- DHCP 中继
  在 DHCP 服务器和 DHCP 客户端之间传输 DHCP 报文的设备。

DHCP 中继为处于不同网段的 DHCP 客户端和服务器承担中继服务，可以将 DHCP 协议报文跨网段中继到目的 DHCP 服务器（或客户端）。

DHCP 报文类型

对 DHCP 的报文类型说明如下：

- DHCPDISCOVER

  DHCP 客户端发送的广播报文，用来查找可用的 DHCP 服务器。
- DHCPOFFER

  DHCP 服务器用来响应客户端发送的 DHCPDISCOVER 报文，在此报文中指定相应的配置参数。
- DHCPREQUEST

  由 DHCP 客户端发送给服务器的报文，用来请求配置参数、配置确认或者续借租期。
- DHCPACK

  由 DHCP 服务器发送给客户端的确认报文，报文中含有配置参数包括 IP 地址等。
- DHCPDELINE

  当客户端发现服务器分配给自己的地址已经被使用时发送此报文，用来通知服务器重新分配地址。
- DHCPNAK

  当客户端的地址请求不正确或者租期已过期时，由 DHCP 服务器发送给客户端的报文拒绝报文。
- DHCPINFORM

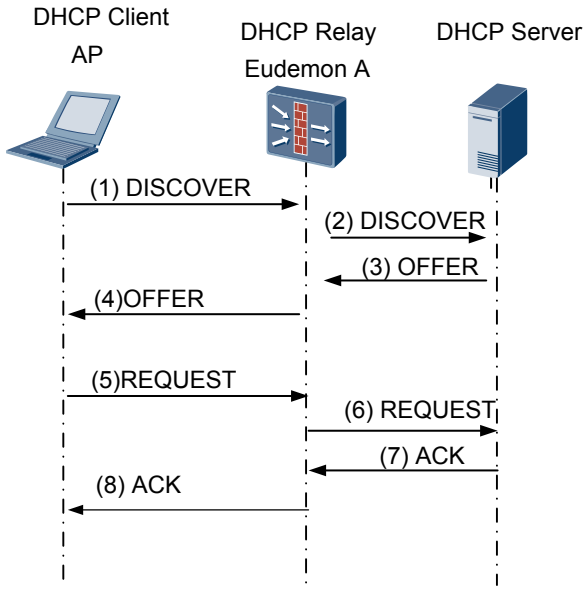
  DHCP 客户端已经有 IP 地址时，发送此报文来向服务器请求其他的配置参数。
- DHCPRELEASE

  DHCP 客户端要释放 IP 地址时，发送此报文通知服务器。

存在 DHCP 中继时的 DHCP 的交互过程

如图 6-22 所示，Eudemon 为 DHCP 中继，对此种情况下的 DHCP 交互过程说明如下。

图 6-22 交互过程



1. DHCP 客户端发送 DHCPDISCOVER 广播报文给 Eudemon，并有 Eudemon 将此报文发送给 DHCP 服务器。
2. DHCP 服务器收到 DHCPDISCOVER 报文后，发送 DHCPOFFER 报文给 Eudemon，并有 Eudemon 将此报文发送给 DHCP 客户端。
3. DHCP 客户端发送 DHCPREQUEST 给 Eudemon，通过 Eudemon 向 DHCP 服务器请求配置参数。
4. DHCP 服务器确认请求合法时，发送 DHCPACK 报文给 Eudemon，并通过 Eudemon 将报文传给 DHCP 客户端。DHCP 客户端从 DHCPACK 报文中获取相应的配置参数，包括 IP 地址等。

DHCP over IPSec 的隧道建立过程

在 DHCP 客户端与 Eudemon 之间会建立两种 IPSec SA。首先建立的 IPSec SA 此处称为 DHCP SA。说明如下。

- 建立 DHCP SA
  1. 由 DHCP Client 发起协商，和 Eudemon 建立 IKE SA。
  2. Client 和 Eudemon 建立 DHCP SA (IPSec SA)，保护 Client 和 DHCP 服务器信息的传输。
  3. DHCP 四条消息加密交互，交互完毕后 DHCP Client 获得 DHCP Server 分配的地址以及其他信息。
- 建立 IPSec SA
  1. DHCP Client 在获得 DHCP 信息之后，删除已建立的 DHCP SA，在以后需要更新 DHCP 消息时再建立新的 DHCP SA。
  2. DHCP Client 根据分配的 IP 与 Eudemon 协商一条新的 IPSec SA，用于传输数据。后续客户端发送的所有 DHCP 消息也都会通过新建立的 IPSec SA 进行传输。

Eudemon 的作用

Eudemon 为 DHCP 中继，其作用如下：

- Eudemon 用 DHCP SA 解密客户端发送过来的 DHCP 报文，把广播报文转换成单播报文，修改 DHCP 报文内容后发送给 DHCP 服务器。
- 服务器对报文进行响应后,Eudemon 把单播报文转换为广播报文或单播报文,修改 DHCP 报文内容后加密转发。
- 由于 DHCP relay 是一种无状态的转发，Eudemon 必须加入适当的信息到 DHCP 报文里,才能对返回报文使用正确的 DHCP SA 加密，发送给相应的客户端。

6.4.12 IPSec 在 Eudemon 上的实现

Eudemon 8080E/8160E 实现了上述所介绍的 IPSec 的全部内容。

通过 IPSec，对等体之间（此处是指 Eudemon 8080E/8160E 及其对端）能够对不同的数据流实施不同的安全保护（验证、加密或两者同时使用）。

简要的实现过程如下。

1. 定义被保护的数据流。

   通过配置 ACL 来区分数据流。

2. 定义安全提议。

   通过配置安全提议来确定安全保护所用到的安全协议、认证算法、加密算法和封装模式。

3. 定义安全策略或安全策略组。

   通过配置安全策略或安全策略组来确定数据流和安全提议的关联（即定义对何种数据流实施何种保护）、SA 的协商方式、对等体 IP 地址的设置（即保护路径的起/终点）、所需要的密钥和 SA 的生存周期等。

4. 在 Eudemon 8080E/8160E 接口上实施安全策略。

定义被保护的数据流

数据流是一组流量（traffic）的集合，由源地址/掩码、目的地址/掩码、IP 报文承载的协议号、源端口号、目的端口号等来规定。

一个数据流用一个 ACL 来定义，所有匹配一个访问控制列表规则的流量，在逻辑上作为一个数据流。一个数据流可以小到是两台主机之间单一的 TCP 连接；也可以大到是两个子网之间所有的流量。IPSec 能够对不同的数据流施加不同的安全保护，因此 IPSec 配置的第一步就是定义数据流。

定义安全提议

安全提议规定了对要保护的数据流所采用的安全协议、验证或加密算法、操作模式（即报文的封装方式）等。

Eudemon 8080E/8160E 支持 AH 和 ESP 安全协议，两者既可单独使用，也可联合使用。其中，AH 支持 MD5 和 SHA-1 验证算法；ESP 协议支持 MD5、SHA-1 验证算法和 DES、3DES、AES 加密算法。Eudemon 8080E/8160E 支持的操作模式包括传输模式和隧道模式。

对同一数据流，对等体两端必须设置相同的协议、算法和操作模式。另外，对于两个安全网关（例如防火墙之间）实施 IPSec，建议采用隧道模式，以隐藏实际通信的源和目的 IP 地址。

因此，请先根据需要配置好一个安全提议，以便下一步将数据流和安全提议相关联。

定义安全策略或安全策略组

安全策略规定了对什么样的数据流采用什么样的安全提议。一条安全策略由“名字”和“顺序号”共同唯一确定。安全策略分为手工安全策略和 IKE 协商安全策略，前者需要用户手工配置密钥、SPI、SA 的生存周期等参数，在隧道模式下还需要手工配置安全隧道两个端点的 IP 地址；后者则由 IKE 自动协商生成这些参数。

安全策略组是所有具有相同名字、不同顺序号的安全策略的集合。在同一个安全策略组中，顺序号越小的安全策略，优先级越高。

接口实施安全策略

在接口上应用安全策略组，安全策略组中的所有安全策略同时应用在这个接口上，从而实现对流经这个接口的不同的数据流进行不同的安全保护。

Eudemon 8080E/8160E 是分布式平台，在 IPSec 的实现上和集中式平台有所区别。普通的报文，由接口板处理并送到业务板。如果需要做 IPSec，业务板会查找报文是否命中 ACL 规则，如果命中 ACL 规则则将报文送到隧道所在的 CPU，并建立会话。

隧道所在 CPU 收到报文后，如果发现是到本地的加密报文，则进行解密处理，解密完成后变成普通报文，进行转板或者其他业务处理（比如 L2TP 的处理）。

6.4.13 IPSec 在硬件上的实现

实际应用中，使用 IPSec 软件进行加密/解密运算会占用大量的 CPU 资源，影响整机性能。为解决这一问题，Eudemon 8080E/8160E 本身集成了 SAE(Security Accelerate Engine) 加密引擎，以硬件方式完成数据的加/解密运算，消除了软件处理 IPSec 协议对性能的影响，提高了防火墙工作效率。

使用加密引擎进行加密/解密的工作过程如下。

1. Eudemon 8080E/8160E 的某个特定处理器将需要加密/解密的数据发送给加密引擎。
2. 加密引擎对数据进行加密/解密运算。
3. 加密引擎将完成加密/解密的数据发送回原来处理器。
4. 处理器对加密引擎处理后的数据进行后续处理。

加密引擎与 IPSec 模块对数据的处理机制完全相同，区别在于加密引擎是通过硬件实现加密/解密处理，而 IPSec 模块是通过软件实现加/解密处理。

6.5 IKE

IKE 是 IPSec VPN 实现中的密钥交换协议。IKE 通过自动协商交换密钥建立安全联盟 SA，保证了 SA 建立过程的安全性和动态性。

6.5.1 介绍

定义

IKE 协议是建立在由 Internet 安全联盟和密钥管理协议 ISAKMP（Internet Security Association and Key Management Protocol）定义的框架上。它能够为 IPSec 提供自动协商交换密钥、建立安全联盟的服务，以简化 IPSec 的使用和管理。

作为 IPSec VPN 实现中的首选密钥交换协议，IKE 保证了安全关联 SA 建立过程的安全性和动态性。IKE 协议是一个混合型协议，其自身的复杂性不可避免地带来一些安全及性能上的缺陷，已经成为目前实现的 IPSec 系统的瓶颈。新版的 IKEv2 协议保留了传统 IKE 的基本功能，并针对 IKE 研究过程中发现的问题进行修订，同时兼顾简洁性、高效性、安全性和健壮性的需要，整合了 IKE 的相关文档，由 RFC4306 单个文档替代。通过核心功能和默认密码算法的最小化规定，新协议极大地提高了不同 IPSec VPN 系统的互操作性。

目的

IKE 具有一套自保护机制，可以在不安全的网络上安全地分发密钥、验证身份、建立 IPSec 安全联盟。

6.5.2 参考标准和协议

与 IKE 特性相关的参考标准与协议如下：

- RFC3948：UDP Encapsulation of IPsec ESP Packets
- RFC 2403：The Use of HMAC-MD5-96 within ESP and AH
- RFC 2857：The Use of HMAC-RIPEMD-160-96 within ESP and AH
- RFC 4305：Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4359：The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 2409： The Internet Key Exchange (IKE)
- RFC 3625：More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3664：The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 3706：A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers

- RFC 3947：Negotiation of NAT-Traversal in the IKE
- RFC 4109：Algorithms for Internet Key Exchange version 1 (IKEv1)
- RFC 4306：Internet Key Exchange (IKEv2) Protocol
- RFC 4307：Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4322：Opportunistic Encryption using the Internet Key Exchange (IKE)
- RFC 4434：The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4478：Repeated Authentication in Internet Key Exchange (IKEv2)

6.5.3 可获得性

License 支持

本特性无须 License 支持。

版本支持

产品	支持版本
Quidway Eudemon 8080E/8160E	V100R003

6.5.4 IKEv1 协议简介

IKE 的安全机制

IKE 的安全机制如下：

- DH（Diffie-Hellman）交换及密钥分发

  Diffie-Hellman 算法是一种公共密钥算法。通信双方在不传送密钥的情况下通过交换一些数据，计算出共享的密钥。加密的前提是交换加密数据的双方必须要有共享的密钥。IKE 的精髓在于它永远不在不安全的网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方的密钥。即使第三者（如黑客）截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。

- 完善的前向安全性

  PFS（Perfect Forward Secrecy）是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。PFS 是由 DH 算法保障的。此特性是通过在 IKE 阶段 2 的协商中增加密钥交换来实现的。

- 身份验证

  身份验证确认通信双方的身份。有以下协商方式：

  - pre-share：需要为每个对端配置预共享密钥。建立安全连接的两个对端的预共享密钥必须一致。 验证字用来作为一个输入产生密钥，验证字不同是不可能在双方产生相同的密钥的。验证字是验证双方身份的关键。
  - rsa-sig：需要配置本地证书。

- 身份保护

  身份数据在密钥产生之后加密传送，实现了对身份数据的保护。

IKE 的交换阶段

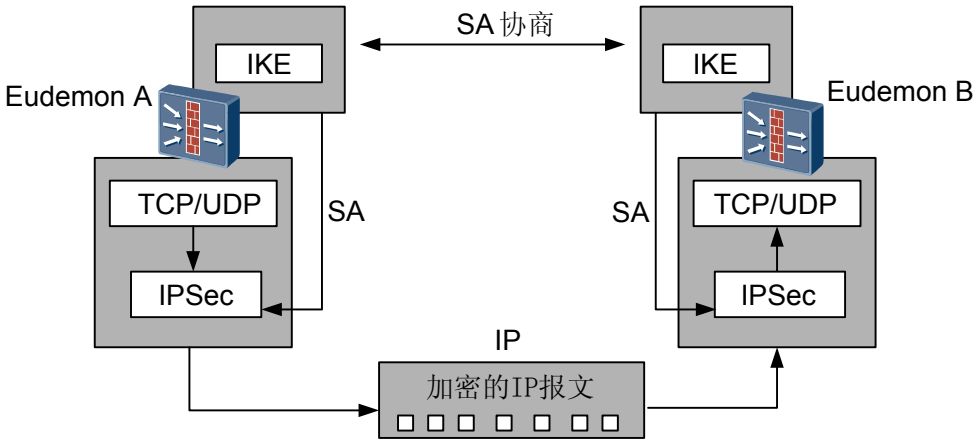
IKE 使用了两个阶段为 IPSec 进行密钥协商并建立安全联盟：

- 第一阶段交换，建立一个保密和验证无误的通信信道（IKE SA），以及建立验证过的密钥，为双方的 IKE 通信提供机密性、消息完整性以及消息源验证服务。

  第一阶段交换（无论主模式还是野蛮模式）必须在第二阶段交换之前完成。
- 第二阶段交换，利用在第一阶段建立的安全联盟为 IPSec 协商安全服务，即为 IPSec 协商具体的安全联盟，建立 IPSec SA。IPSec SA 用于最终的 IP 数据安全传送。

IKE 和 IPSec 的关系如图 6-23 所示。

图 6-23 IKE 和 IPSec 的关系图



具体安全联盟的建立过程如图 6-24 所示。

图 6-24 安全联盟建立过程

安全联盟建立的过程解析如下：

1. 当一个报文从某接口外出时，如果此接口应用了 IPSec，会进行安全策略的匹配。

2. 如果找到匹配的安全策略，会查找相应的安全联盟。如果安全联盟还没有建立，则触发 IKE 进行协商。IKE 首先建立第一阶段的安全联盟，即 IKE SA。
3. 在第一阶段安全联盟的保护下协商第二阶段的安全联盟，即 IPSec SA。
4. 使用 IPSec SA 保护通讯数据。

IKE 的协商模式

在 RFC 2409（The Internet Key Exchange）中规定，IKE 第一阶段的协商可以采用两种模式：

- 主模式（Main Mode）

  主模式被设计成将密钥交换信息与身份、认证信息相分离。这种分离保护了身份信息；交换的身份信息受已生成的 Diffie-Hellman 共享密钥的保护，但这增加了开销。

- 野蛮模式（Aggressive Mode）

  野蛮模式则允许同时传送与 SA、密钥交换和认证相关的载荷。将这些载荷组合到一条消息中减少了消息的往返次数，但是就无法提供身份保护了。

  虽然野蛮模式存在一些功能限制，但可以满足某些特定的网络环境需求。例如：远程访问时，如果响应者（服务器端）无法预先知道发起者（终端用户）的地址、或者发起者的地址总在变化，而双方都希望采用预共享密钥验证方法来创建 IKE SA，那么，不进行身份保护的野蛮模式就是唯一可行的交换方法；另外，如果发起者已知响应者的策略，或者对响应者的策略有全面的了解，采用野蛮模式能够更快地创建 IKE SA。

6.5.5 IKEv2 协议简介

IKEv2 优点

为了解决 IKE 的诸多缺点，IKEv2 与传统 IKE 相比有以下优点：

- 用 4 条消息就可以完成一个 IKE SA 和一对 IPSec SA 的协商建立，提高了协商效率。
- 删除了原有协议中的 DOI、SIT 以及域名标识符、提交位这些功能不强且难以理解、容易混淆的数据结构。
- 修复了多处公认的密码学方面的安全漏洞，提高了安全性能。
- 定义了独立的通讯量选择载荷，分担了原有 ID 载荷的部分功能，增加了协议灵活性。
- 加入对 EAP 身份认证方式的支持，提高了认证方式的灵活性和可扩展性。

IKEv2 的协商过程

要建立一对 IPSec SA，传统 IKE 需要经历两个阶段：“主模式＋快速模式”或者“野蛮模式＋快速模式”。前者需要交换至少 9 条消息，后者也至少需要 6 条消息。而 IKEv2 建立一对 IPSec SA，正常情况使用两次交换 4 条消息就可以完成一个 IKE SA 和一对 IPSec SA 的协商建立，如果要求建立的 IPSec SA 大于一对时，每一对 SA 只需额外增加一次交换，也就是两条消息就可以完成。这比传统 IKE 要简化很多。

IKEv2 与 EAP 认证

EAP（Extensible Authentication Protocol）是一种支持多种认证方法的认证协议，可扩展性是其最大的优点，即若想加入新的认证方式，可以像组件一样加入，而不用变动原来的认证体系。采用 EAP 方式认证，可以方便的继承系统原有的认证机制。

IKEv2 中支持采用 EAP 对协商的发起方(Initiator)进行第三方认证。响应方根据发起方消息中有无 AUTH 载荷来判断是否需要 EAP 认证。

如果没有 AUTH (Authentication) 载荷则表示发起方请求 EAP 认证，在响应方发回的 Response 消息选择了自己允许的 EAP 认证方法。发起方的下一个 Request 消息携带了对应于该 EAP 方法的认证信息，收到该消息后响应方向第三方的 EAP 认证服务器按照 RFC 3748（Extensible Authentication Protocol）的规范进行认证。然后在 Response 消息中发回认证成功或失败的信息。

在实现中响应方可以完全不用知道具体的认证方法和过程，而仅充当发起方和 EAP 认证服务器的中转(pass through 模式)，由发起方和 EAP 认证服务器来完成认证的全过程而响应方只需要得到认证结果。这样可以支持很多的认证方式，包括很多高强度的认证算法而不用增加响应方的软件复杂度。

6.5.6 IKEv2 的安全性分析

IKEv2 对传统 IKE 存在的安全漏洞进行了修订，提高了密钥协商的安全性，并明确规定了所有的消息必须以请求/响应对的形式存在，有效的解决了使用 UDP 作为传输层协议的不可靠性问题。

以下从三方面来讨论 IKEv2 的安全性问题。

抵御中间人攻击

中间人攻击（Man-in-the-middle Attack）是一种主动攻击，指攻击者对通信双方进行窃听，截获通信双方的消息并进行任意插入、删除或篡改消息，之后返回消息给发送者，或者重放旧消息以及重定向消息，是最危险的攻击。IKEv2 中抵御中间人攻击的机制和方法：

- 密钥材料生成方式

  与传统 IKE 相比，IKEv2 的密钥材料发生了变化，双方用于后继交互使用的加密密钥与认证密钥都是不同的。这些密钥是从 prf+输出流中依次提取，从而增加了攻击者猜测密钥的难度，减少了密钥泄漏的可能性，增强了传输的安全性，一定程度上可以抵御中间人攻击。

- 身份认证

  IKEv2 使用预共享密钥和数字签名方式进行身份认证。身份认证方式具有交互性，参与协商的实体彼此都对对方的身份进行认证；具有对称性，参与协商的双方都使用相同的机制或方法对对方的身份进行认证。双向的身份认证可以有效地抵御中间人攻击。同时 IKEv2 定义了扩展认证交互，即使用扩展认证协议（EAP）描述的方法对 IKEv2 协商进行身份认证，支持非对称双向认证，进一步加强了认证的灵活性和协商的可扩展性。

- 消息交换

  IKEv2 将传统 IKE 主模式交换的六条消息修订为四条消息，将 SA 载荷和 KE 载荷、nonce 载荷一同发送，这样，消息中包含随机的 nonce 值，如果攻击者伪装成响应方进行应答，将收到的发起方的消息基本上不做改变，再发回给发起方，发起方可以根据消息内容判断消息的真假，在一定程度上可以抵御重放攻击。每个 IKEv2 消息的头都包含了一个消息 ID，用于匹配对应的请求和响应消息以及识别消息重

传。当发送和接收到请求时，必须对消息 ID 值顺序增加，且除了 IKE_SA_INIT 交互外其值受加密和完整性保护，使得它能够防重放攻击。同时 IKEv2 加入了滑动窗口机制，使交互能够更加有效地抵御重放攻击的威胁。

抵御 DDoS 攻击

IKEv2 中抵御 DDoS 攻击的机制和方法：

- SPI 值

  IKEv2 消息头部有发起方 SPIi 和响应方 SPIr，它们是内核产生的 8 字节的随机数，用来标识 SA，同时也可以标识进行消息交换的一对节点。具有相同 SPI 值的请求处理一次（重传消息除外），而把其他请求作为重复数据报丢弃，可以在一定程度上防止 DDoS 攻击。

- 带 Cookie 交互

  IKEv2 中使用 N 载荷携带 Cookie 的辅助交换来抵御拒绝服务攻击。在通信过程中，响应方认为自己正受到 DDoS 攻击时，可以向发起方请求回复一个无状态 cookie。

  响应方收到对方发来的第一条消息后并不急于进行 IKE_SA_INIT 交互，而是再产生一个新的 cookie，封装在通知载荷中发送给对方。如果发起方不是攻击者，就可以收到这条消息，然后重新开始协商，并将响应方的 cookie 封装在该消息中，其它载荷内容保持不变。

- 重传约定

  IKEv2 中所有消息都是成对出现，在每对消息中，发起方负责重传事件，响应方不必对其响应消息进行重传，除非收到对方的一个重传请求。避免了双方同时发起重传，造成资源的浪费，同时也可以防止攻击者截获消息后，伪装成协商者不断地发送重传消息，耗费协商双方的资源。

- 丢弃半开（half-open）连接

  IKEv2 只能通过两种情况判断对方是否失效：一种是重复尝试联系对方，直到应答时间过期；另一种是收到对方的不同 IKE SA 加密保护下的 INITIAL CONTACT 通知消息。IKEv2 发起方允许多个响应方响应第一条消息，并把所有的响应方视为合法并作回应。发起方发送一些消息后，一旦收到一个有效的加密的响应消息，将其他的响应消息忽略，并将其他所有的无效的半连接丢弃。这样在协商开始时就可以避免受到 DDoS 攻击。

完善的前向安全性 PFS

完善的前向安全性，即限制单密钥只能解密受该单密钥保护的数据。即使攻击者攻克了一个密钥，也只能破解这个密钥保护的数据，而不能破解受其它密钥保护的数据。对于 IPSec VPN 来说，是指在 IKE 协商阶段所用的加密密钥同 IPSec 使用的加密密钥，源于不同密钥衍生材料，即使攻击者攻克 IKE 协商阶段密钥，也并不能破解 IPSec 加密消息。

IKEv2 初始交互的密钥衍生材料不被用于衍生供 IPSec SA 使用的相关密钥，而是通过在 CREATE_IPSec_SA 交互中引入可选的 KE 载荷重新生成密钥材料，以此有效完成 PFS 服务要求。

6.5.7 IKE 在 Eudemon 上的实现

传统 IKE 在 Eudemon 上的实现

Eudemon 支持传统 IKE 的主模式和野蛮模式，并基于 RFC2408、RFC2409 实现，能够与大多数主流设备互通。

目前，Eudemon 上的 IPSec，如果需要进行 NAT 穿越，则安全协议应采用 ESP，并且以隧道模式（tunnel）封装报文。

Eudemon 上 IKE 的实现步骤如下。

1. 设置 IKE 交换过程中所使用的本地 ID。
2. 指定对端（IKE Peer）的一系列属性（包括 IKE 协商模式、预共享密钥值、对端 IP 地址或对端 ID、是否需要进行 NAT 穿越等），以保证 IKE 协商阶段的正确性。
3. 创建 IKE 安全提议，以确定 IKE 交换过程中算法的强度，即安全保护的强度（包括身份验证方法、加密算法、验证算法、DH 组等）。不同的算法的强度不同，强度越高的算法，受保护数据越难被破解，但消耗的计算资源越多。一般来说，密钥越长的算法强度越高。
4. 此外，除上述基本步骤外，IKE 还具有 Keepalive 机制，可以判断对端是否能够正常通讯。可配置 Keepalive 的“interval”和“timeout”两个参数。

   同时，IKE 具有 DPD（Dead Peer Detection）机制，相比 Keepalive 具有更好的性能和响应时间。可以配置 DPD 的“interval”参数。

   当配置了 IPSec 的 NAT 穿越时，还可配置发送 NAT 更新报文的时间间隔。

说明

当上述 IKE 配置完毕后，需要在 IPSec 的安全策略视图下引用 IKE Peer，以完成自动协商的 IPSec 的配置。

IKEv2 在 Eudemon 上的实现

Eudemon 目前实现了 IKEv2 的基本功能，支持基本交互和信息交互，支持 NAT 穿越和 DPD 特征，能够与主流设备的实现互通。

Eudemon 上 IKEv2 的配置和传统 IKE 的配置基本相同，具体的配置请参见*《Quidway Eudemon 8080E/8160E 防火墙 配置指南 安全防范分册》*。

7 证书

关于本章

7.1 介绍

定义

数字证书简称证书，用来证明一台设备的身份，解决了通信双方之间的信任问题，同时可以保证信息在传输过程中的安全性、完整性和不可否认性。

证书文件通常由第三方通常是数字证书认证中心颁发，包含设备信息、公开密钥以及颁发者签名。

目的

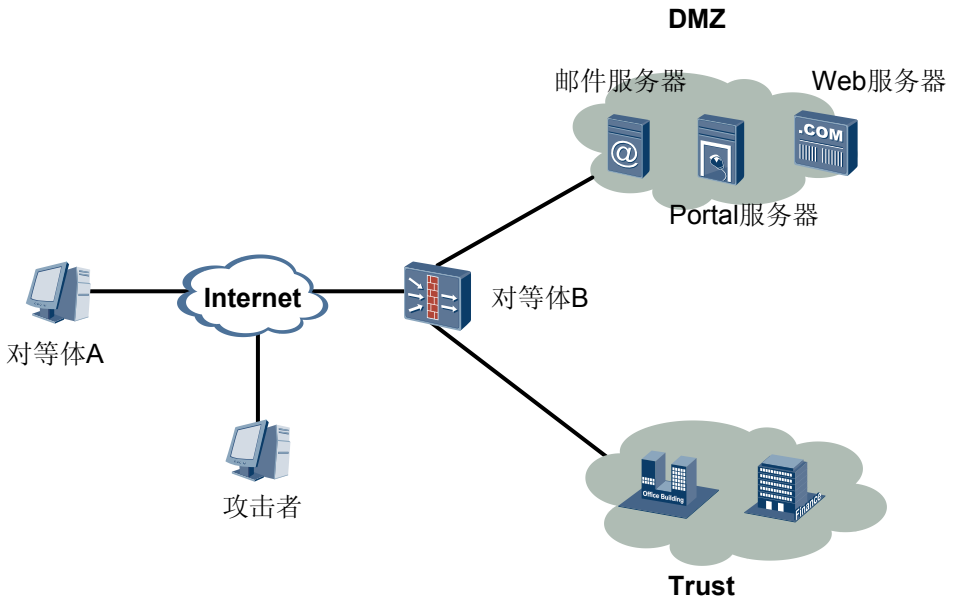
随着电子商务、网上银行及网上证券交易的飞速发展，Internet 的安全性越来越重要。部分不道德的个人，会截取应用的明文数据，进行中间人攻击。

以图 7-1 为例，对等体 A 要与对等体 B 创建 IPSec VPN，但是攻击者中途拦截了对等体 A 发送给对等体 B 的信息，冒充对等体 B 与之建立连接。考虑到这种安全问题，对等体 A 和对等体 B 必须在彼此建立通信之前检验双方身份。

数字证书为 VPN 实施提供了设备验证方式。

对等体事先向证书颁发机构申请证书，在建立 VPN 连接之前，会共享它们的证书，并验证对方证书是否合法，只有通过了合法性认证，才会与对方建立连接，从而有效防止中间人攻击。

图 7-1 中间人攻击例子



受益

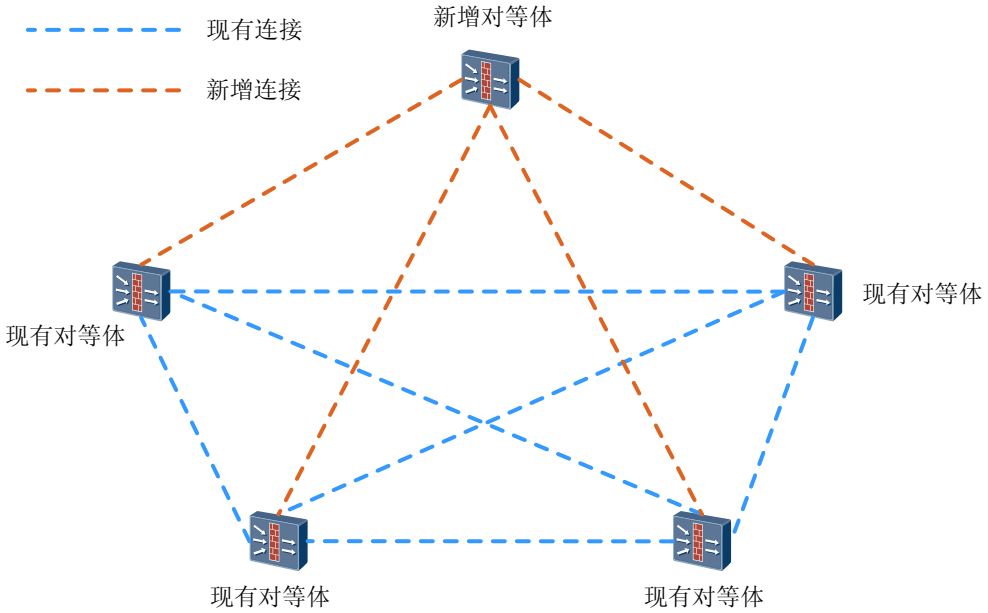
在 IPSec VPN 中，预共享密钥和证书是验证对等体身份的两种常用方法。

预共享密钥是指两台设备事先配置相同密钥，通过检查对方密钥与自己密钥是否一致来完成验证，易于配置。

但当网络中设备数量较多时，每新增一台设备，都需要在所有设备上重新配置预共享密钥，工作量会以指数级速度增长，以图 7-2 为例，有 4 个对等体配置了预共享密钥，如果新增了第 5 台设备，需要从那 4 个站点建立到这台新设备的 VPN 连接。为了确保安全，不得不对每一个对等体建立一个不同密钥。在这台新设备上，需要对其他 4 台设备建立 4 个密钥，在其它 4 台设备上，也需要配置到这台新设备的密钥。

为了帮助用户将设备验证扩展到很大范围内的设备，并且减少中间人攻击的风险，在大型 VPN 中，可以使用证书来进行设备验证。

图 7-2 使用预共享密钥验证方式示意图



7.2 规格

证书特性的相关规格如下：

- Eudemon 支持创建的 PKI 实体的最大个数为 10 个。
- Eudemon 支持创建的 PKI 域的最大个数为 10 个。

7.3 参考标准和协议

与证书特性相关的参考标准与协议如下：

- RFC2510
  Internet X.509 Public Key Infrastructure Certificate Management Protocols
- RFC2511
  Internet X.509 Certificate Request Message Format

- RFC2527

  Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

7.4 可获得性

版本支持

产品	最低支持版本
Quidway Eudemon 8080E/8160E	V100R003

特性依赖

在 Eudemon 8080E/8160E 上，证书特性可以与 IPSec 特性配合使用，为建立 IPSec VPN 会话提供证书的设备认证方式。

7.5 PKI 体系

PKI（Public Key Infrastructure，公钥基础设施）是一个利用公共密钥理论和技术来实现信息安全服务并具有通用安全性的安全基础设施。

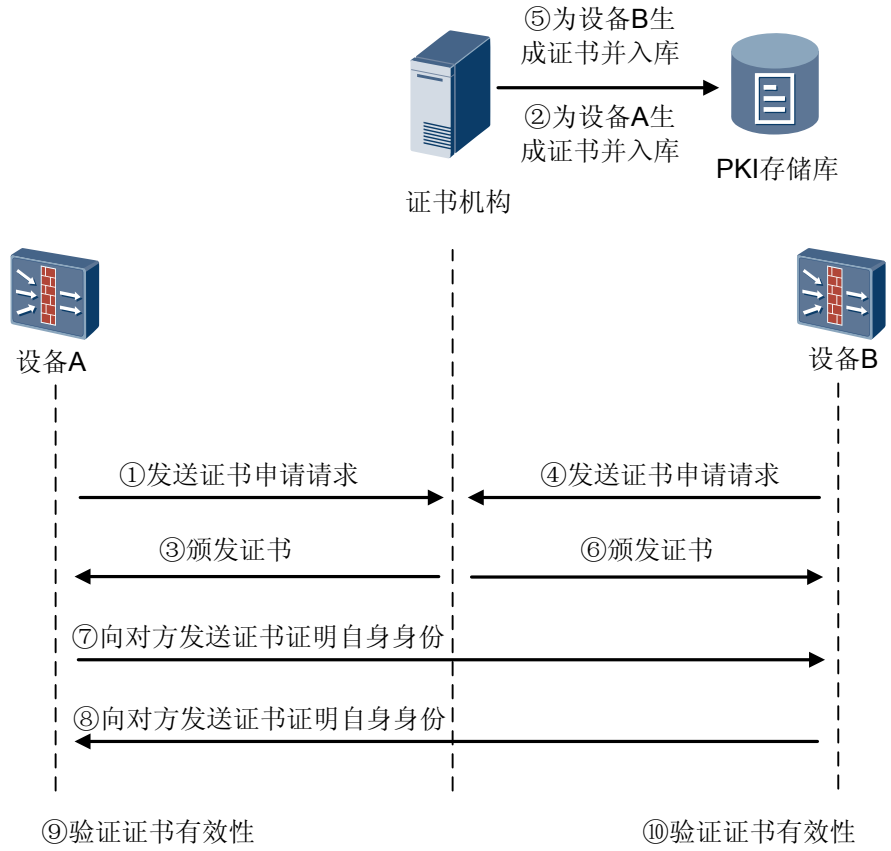
一个 PKI 体系由证书机构、终端实体、PKI 存储库等部分组成，如表 7-1 所示。

表 7-1 PKI 体系组件

组件名称	组件作用
终端实体	证书申请者和使用者，也就是 Eudemon。
证书机构（CA，Certificate Authority）	用于签发并管理数字证书的第三方机构，其作用包括：发放证书、规定证书的有效期和通过发布 CRL（Certificate Revocation List）确保必要时可以废除证书。
PKI 存储库	各个终端实体证书以及 CRL 列表等信息的集中存放地，提供公众查询，可以是 LDAP 服务器或普通数据库。

各个组件的交互过程如图 7-3 所示。

图 7-3 PKI 体系示意图



1. 以设备 A 为例，设备 A 向 CA 发送证书建立请求，在请求中包括描述终端特征的实体信息，CA 将使用这些信息来为设备 A 建立实体证书。
2. CA 对收到的设备信息进行验证，为设备 A 生成证书并保存到 PKI 存储库里。

   说明

   有两种类型的证书：根证书（CA 证书）和实体证书。根证书代表 CA，用来证明 CA 身份，实体证书代表在 CA 域内的设备，用来证明设备身份。在一个 CA 域内，每一个证书都将有一个唯一的序列号，来核实这个证书是否有效或者被吊销。
3. CA 将根证书和设备证书同时颁发给设备 A。
4. 设备 A 使用根证书来验证设备证书的有效性，即验证设备证书是由合法 CA（而不是冒充 CA 的攻击者）颁发的。
5. 设备 B 向 CA 申请证书过程与设备 A 相同。
6. 当设备想使用证书来证明自己身份时，例如通过 IKE 方式建立 IPSec VPN 时，设备可以将自己的证书发送给对等体来进行身份证明。

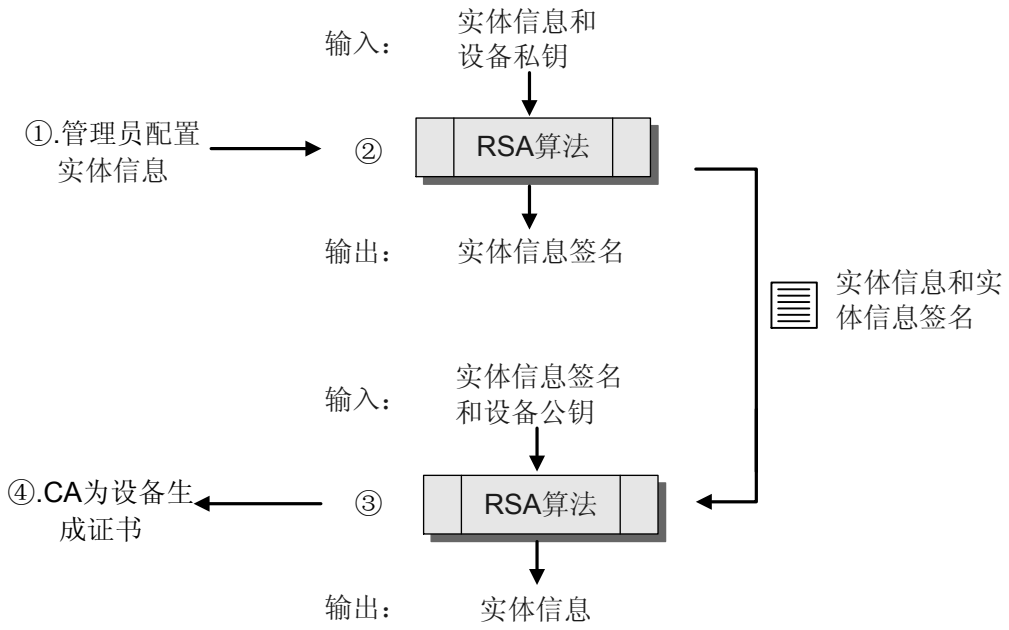
7.6 证书申请

CA 通过对表示设备特征的实体信息进行签名来为产生实体证书的，因此设备在向 CA 请求建立个人证书时，必须向 CA 提供实体信息。

证书申请过如图 7-4 所示，为了保证实体信息在传输过程中没有被篡改，设备会先使用自己的私钥对包括设备公钥在内的实体信息进行签名，然后，将实体信息和产生的签名一起用于产生一个证书请求发送给 CA。

CA 在收到设备的证书申请请求后，使用包含在实体信息里的公钥来验证实体信息签名，只有签名通过验证，CA 才会为设备建立证书。

图 7-4 证书申请过程示意



目前，Eudemon 只支持带外的证书申请发送方式，将请求文件放入到一张软盘或者 CD-ROM 中，或者用 E-mail 形式发送给 CA 的管理员。

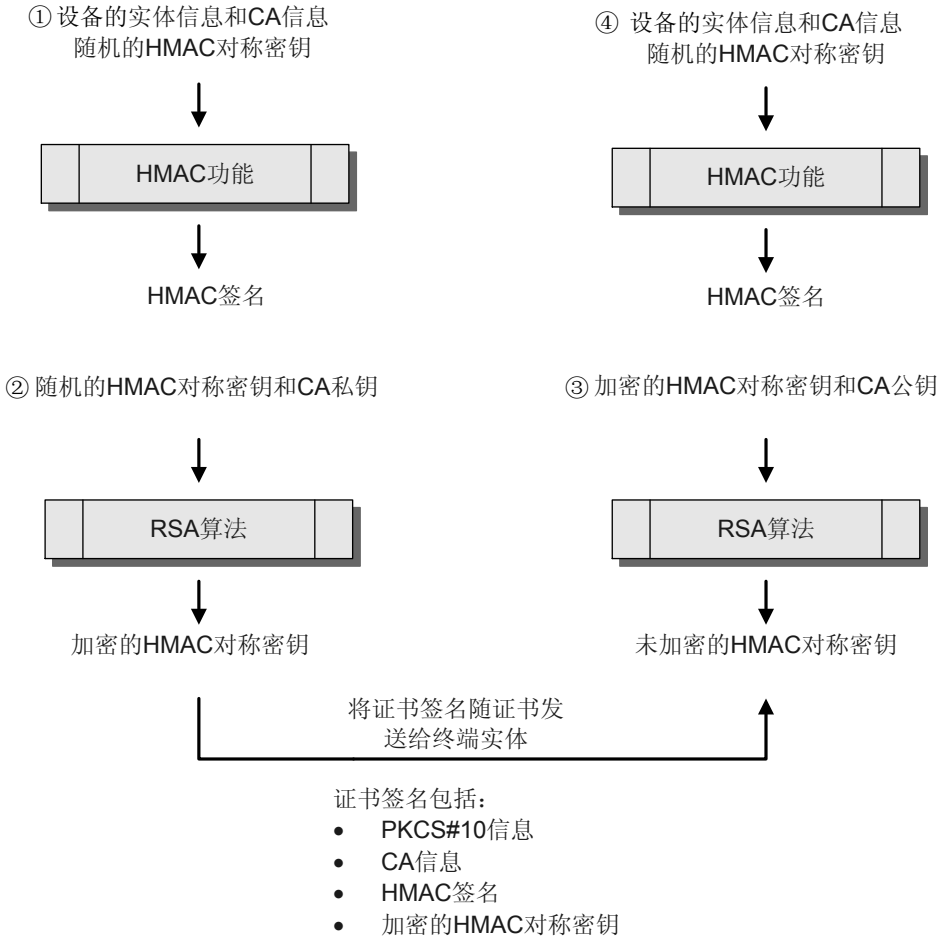
7.7 证书生成

CA 收到实体信息后，如果设备签名通过了验证（验证过程可参考证书申请的证书申请过程示意图），CA 将使用自己的某些信息，和某些来自设备的信息为设备建立实体证书，并使用自己私钥对证书进行签名，签名过程如图 7-5 所示：

1. CA 随机产生一个随机的对称密钥，并且将这个随机产生的对称密钥、从设备收到的实体信息、CA 本身提供的信息（一个 CA 域内唯一的序列号、证书有效期、CA 公钥）进行 HASH 运算，最终产生一个 HMAC（Hash Message Authentication Code）签名。
2. CA 使用自己私钥对刚刚产生的随机 HMAC 对称密钥进行加密。
3. CA 将产生的的证书签名随同证书发送给终端实体。
4. 终端实体收到 CA 颁发证书后，将对证书签名进行验证。
5. 设备从根证书中获取 CA 公钥，并使用 CA 公钥来解密签名中的 HMAC 对称密钥。

6. 把证书信息（设备提供给 CA 的实体信息、CA 本身提供的信息）和刚刚解密得到的 HMAC 密钥进行 HASH 运算，得到一个签名，比较刚刚计算出来的签名与证书上的 HMAC 签名是否相同，如果相同，则证明证书是真实有效的，否则证书无效。

图 7-5 证书签名的建立



最后，CA 将使用 DER（原始二进制）或者 PEM（二进制-64）编码方式对证书进行编码，如果设备只支持其中一种类型，需要事先通知 CA，使得 CA 管理员使用正确的编码方案。

7.8 证书获取

CA 生成证书后，设备需要从 CA 下载根证书和实体证书。

Eudemon 支持在线和离线的方式下载证书：

- 在线方式

  通过 HTTP 或 LDAP 协议与 CA 服务器通信，将根证书和本地证书下载到 Eudemon 的 CF 卡中。

- 离线方式

通过 FTP、磁盘、电子邮件等方式获得根证书和本地证书后，上传到 Eudemon 的 CF 卡中。

7.9 证书吊销列表

证书吊销是指当证书过期或作废时，CA 会吊销证书的使用，有许多原因导致实体证书被吊销，例如：

- 用户的信息变更。
- 用户的私钥泄漏。
- CA 的私钥泄漏
- 证书已经过期，设备需要一个新的实体证书。
- 安全策略改变，对签名功能需要更长（或者更短）的密钥，因此需要一个新的公钥/私钥对、一个新的签名和一个新的实体证书。

当收到来自对方的证书后，设备需要验证这个证书是否被 CA 吊销，保证对方证书有效性最简单办法是每次验证对方的时候，都从对方和 CA 下载最新的证书。但这将非常消耗系统资源，并且执行重验证的延迟会导致业务重新建立连接，影响设备之间的通信。

可以通过如下方式来解决这个问题：

- CA 把吊销证书的序列号保存到证书吊销列表中。
- 设备将对方证书缓存到本地，并周期性地从 CA 下载证书吊销列表。
- 当设备需要验证对方时，由于在缓存中存有对方证书，只需要将证书序列号和 CRL 中的序列号进行对比：如果找到了匹配，则对方证书已经被吊销了，应当向对方和 CA 重新请求证书；如果没有找到匹配，则证明证书是有效的，可以使用存储在本地缓存中的对方证书。

Eudemon 可以通过以下两种方式更新 CRL：

- 自动更新方式

  Eudemon 通过 HTTP 或 LDAP 协议与 CRL 服务器通信，定期向 CRL 服务器发送更新请求，从 CRL 服务器自动下载 CRL。
- 手动更新方式

  通过在 Eudemon 上手动执行命令，从 CRL 服务器自动下载 CRL。

7.10 证书应用

7.10.1 证书在 IPSec VPN 中的应用

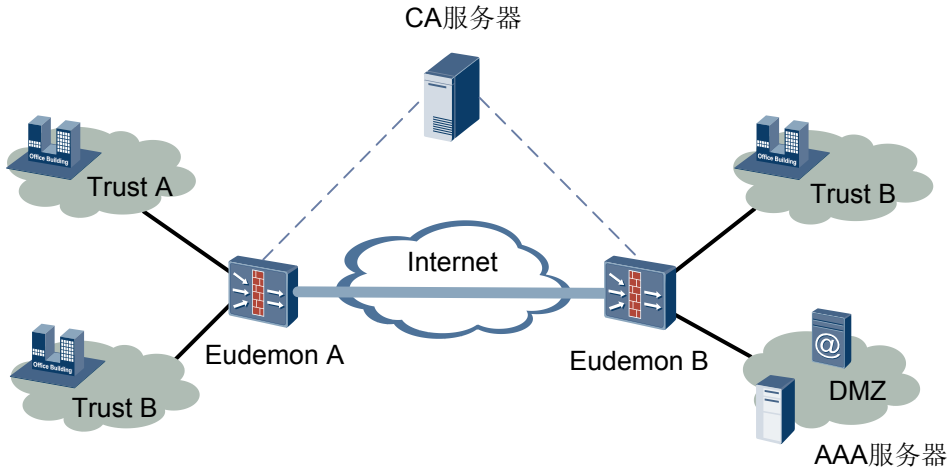
在站点到站点和远程访问的 VPN 应用中，当两台设备彼此通信时，用数字证书来检验身份。

以图 7-6 为例，Eudemon A 和 Eudemon B 都向同一个 CA 申请设备证书，并将根证书和实体证书都下载到了本地。当 Eudemon A 和 Eudemon B 有数据流量要建立 IPSec VPN 时，它们执行如下的验证过程：

1. 双方设备初始联系之后，它们将共享他们的实体证书。
2. 使用存储在本地的根证书的公钥来核实对方的实体证书签名，CA 在给设备颁发实体证书时，会在实体证书后附加一个签名，我们可以通过根证书中的 CA 公钥来核实对方实体证书的签名，验证过程参见证书生成的证书签名建立示意图。
3. 如果通过了证书签名真实性验证，设备将当前时间和证书上的开始和终止时间做对比。如果设备时间在这两个值的范围内，有效期验证通过，否则，验证失败。
4. 如果开启了 CRL 验证（依赖于设备的配置），设备将会在 CRL 中查找对方证书中的序列号，如果找到了序列号，则认为证书是无效的，验证失败；如果没有找到序列号，则证书验证通过。

一旦证书验证通过，Eudemon A 和 Eudemon B 就可以建立 IPSec VPN。

图 7-6 证书在 IPSec VPN 中的应用



7.10.2 基于证书属性的 VPN 访问控制

基于属性的证书访问控制，允许在验证证书有效性之前执行额外的步骤。只有符合特定条件的证书才能通过验证，进而对用户的访问权限进行精细化控制。

设备可以为证书的特定字段制定匹配条件，当设备收到一个证书时，会先查看证书上的特定字段。如果符合匹配条件，设备将接受这个证书，并检查 CA 的签名来核实它的真实性、检查有效日期和吊销状态（最后一项可选，取决于是否配置 CRL 检查），否则将直接拒绝这个证书。

以图 7-7 为例：

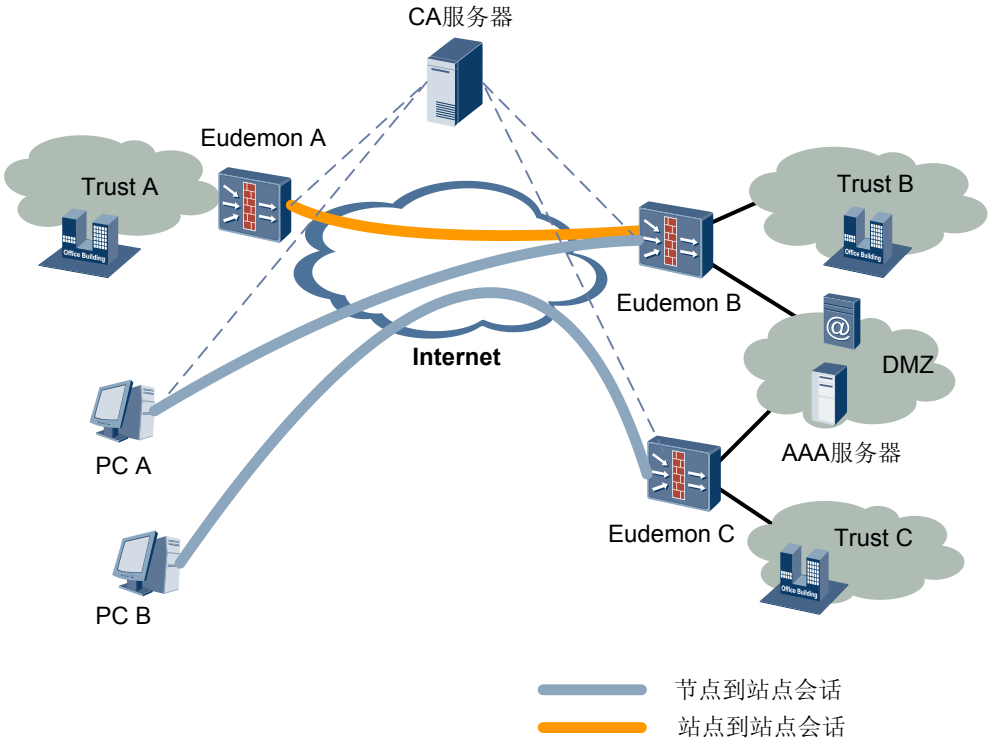
- Eudemon A 通过与 Eudemon B 建立站点到站点的 VPN 会话来实现区域 Trust A 与区域 Trust B 的互访，Eudemon A 和 Eudemon B 通过证书方式进行设备验证。
- PC A 通过与 Eudemon B 建立节点到站点的 VPN 会话来实现对区域 Trust B 的远程访问，其中，PC A 和 Eudemon B 通过证书方式来进行设备验证，通过 AAA 实现用户验证。
- PC B 通过与 Eudemon C 建立节点到站点的 VPN 会话来实现对区域 Trust C 的访问，PC B 和 Eudemon C 通过证书方式来进行设备验证，通过 AAA 实现用户验证。
- Eudemon B 和 Eudemon C 使用 DMZ 区域中的同一个 AAA 服务器来对远端用户进行验证，并且 Eudemon B 和 Eudemon C 的证书是由同一个 CA 服务器颁发的。

这样会导致一个问题，由于 Eudemon B 和 Eudemon C 使用同一台 AAA 服务器，并且 Eudemon B 和 Eudemon C 的实体证书是由同一个 CA 服务器颁发的，因此 PC B 也可以建立到Eudemon B 的 IPSec 远程访问会话。

为了在 Eudemon B 上限制 PC B 对 Eudemon B 发起的远程访问会话，可以在 Eudemon B 上定义一个基于证书属性的访问控制策略，只有当证书的主题名 DN 字段等于“pca”时，才会启动证书的有效性检查，否则直接认为证书无效，设备验证失败。

Eudemon 支持根据证书主题名、证书颁发者名和证书备用主题名为内容，以包含（ctn）、相等（equ）、不包含（nctn）、不等（nequ）为判断条件，对证书进行过滤。

图 7-7 基于证书属性的 VPN 访问控制



8 IPv6

关于本章

IPv6 是为优化目前网络的缺陷而出现的下一代网络。IPv6 以其简化的报文头格式、充足的地址空间、层次化的地址结构、灵活的扩展头、增强的邻居发现机制将在未来的市场竞争中充满活力。

8.1 介绍

定义

IPv6（Internet Protocol Version 6）是网络层协议的第二代标准协议，也被称为 IPng（IP Next Generation）。它是 IETF（Internet 工程任务组）设计的一套规范，是 IPv4（Internet Protocol Version 4）的升级版本。IPv6 和 IPv4 之间最显著的区别就是 IP 地址长度从原来的 32 位升级为 128 位。

目的

以 IPv4 为核心技术的 Internet 获得巨大成功，促使 IP 技术得到广泛应用。然而，随着因特网的迅猛发展，IPv4 设计的不足也日益明显，主要有以下几点：

- IPv4 地址空间不足

  IPv4 地址采用 32 比特标识，理论上能够提供的地址数量是 43 亿。但由于地址分配的原因，实际可使用的数量不到 43 亿。另外，IPv4 地址的分配也很不均衡：美国占全球地址空间的一半左右，而欧洲则相对匮乏；亚太地区则更加匮乏。与此同时，移动 IP 和宽带技术的发展需要更多的 IP 地址。IPv4 地址资源紧张直接限制了 IP 技术应用的进一步发展。

  针对 IPv4 的地址短缺问题，也曾先后出现过几种解决方案。比较有代表性的是 CIDR(Classless Inter-Domain Routing)和 NAT(IP Network Address Translator)。但是 CIDR 和 NAT 都有各自的弊端和不能解决的问题，由此推动了 IPv6 的发展。

- 骨干路由器维护的路由表表项数量过大

  由于 IPv4 发展初期的分配规划问题，造成许多 IPv4 地址分配不连续，不能有效聚合路由。日益庞大的路由表耗用较多内存，对设备成本和转发效率产生影响，这一问题促使设备制造商不断升级其路由器产品，以提高路由寻址和转发性能。

- 不易进行自动配置和重新编址

  由于 IPv4 地址只有 32 比特，并且地址分配不均衡，导致在网络扩容或重新部署时，经常需要重新分配 IP 地址。因此需要能够进行自动配置和重新编址以减少维护工作量。

- 不能解决日益突出的安全问题

  随着因特网的发展，安全问题越来越突出。IPv4 协议制定时并没有仔细针对安全性进行设计，因此固有的框架结构并不能支持端到端的安全。IPv6 将 IPSec 作为它的 标准扩展头实现，可以提供端到端的安全特性。

IPv6 技术从根本上解决了 IP 地址短缺的问题；且易于部署，能够兼容当前的各种应用，方便用户的平滑过渡；同时可实现与 IPv4 网络的共存和互通。由于 IPv4 存在以上种种弊端和不足，IPv6 技术的优越性显而易见，因此 IPv6 技术得以迅猛发展。

8.2 规格

IPv6 特性的相关规格如下：

- 支持 IPv6 重定向报文。
- 支持 IPv6 基本报文头和扩展报文头。

- 支持发送差错和信息 ICMPv6 报文。
- 支持 ICMPv6 校验和。
- 支持自动/手动配置 Link-Local 地址。
- 支持动态 PMTU 表项老化。
- 支持基本和高级 ACL6。
- 支持基于 IPv6 地址的 Ping、Tracert 和 Telnet。
- 支持 NAT-PT。
- 支持 IPv6 over IPv4 隧道。
- 支持 IPv4 over IPv6 隧道。

8.3 参考协议和标准

本特性的参考资料清单如下：

- RFC793：Transmission Control Protocol
- RFC768：User Datagram Protocol
- RFC1981：Path MTU Discovery for IP version 6
- RFC2461：Neighbor Discovery for IP Version 6 (IPv6)
- RFC2463：Internet Control Message Protocol for the Internet Protocol Version 6 Specification
- RFC2465：Management Information Base for IP Version 6:Textual Conventions and General Group
- RFC2466：Management Information Base for IP Version 6:ICMPv6 Group
- RFC2893：Transition Mechanisms for IPv6 Hosts and Routers
- RFC3056：Connection of IPv6 Domains via IPv4 Clouds
- RFC4214：Intra-Site Automatic Tunnel Addressing Protocol(ISATAP)

8.4 可获得性

License 支持

本特性无须 License 支持。

版本支持

产品	支持版本
Quidway Eudemon 8080E/8160E	V100R003

8.5 IPv6 地址

IPv6 地址的书写格式

IPv6 的 128 位 IP 地址有以下两种表示形式。

- X:X:X:X:X:X:X:X

  在这种形式中，128 位的 IPv6 地址被分为 8 组，每组的 16 位用 4 个十六进制字符（0 ～ 9，A ～ F）来表示，组和组之间用冒号（:）隔开。其中每个“X”代 表一组十六进制数值。比如下面这个 IPv6 地址：

  2031:0000:130F:0000:0000:09C0:876A:130B

  为了书写方便，每组中的前导“0”都可以省略，所以上述地址可写为：

  2031:0:130F:0:0:9C0:876A:130B。

  另外，地址中包含的连续两个或多个均为 0 的组，可以用双冒号“::”来代替，这样可以压缩 IPv6 地址书写时的长度，所以上述地址又可以进一步简写为：

  2031:0:130F::9C0:876A:130B。

  说明

  在一个 IPv6 地址中只能使用一次双冒号“::”，否则当计算机将压缩后的地址恢复成 128 位时，无法确定每段中 0 的个数。

- X:X:X:X:X:X:d.d.d.d

  分为如下两种类型：

  - IPv4 兼容 IPv6 地址。地址格式为：0:0:0:0:0:0:IPv4-address，其高阶 96bits 均为 0，其低阶 32bits 是一个 IPv4 地址。该 IPv4 地址必须是 IPv4 网络中可达的 IPv4 地址，且不能是组播地址、广播地址、环回地址或未指定的地址（0.0.0.0）。
  - IPv4 映射 IPv6 地址。地址格式为：0:0:0:0:0:FFFF:IPv4-address。该地址用来将 IPv4 节点的地址表示为 IPv6 地址。

  其中 IPv4 兼容 IPv6 地址用于配置 IPv6 over IPv4 隧道。

  其中“X”代表高阶的六组数字，用十六进制数来表示每组的 16 比特。“d”代表低阶的四组数字，用十进制数表示每组的 8 比特。后边的部分（d.d.d.d）其实就是一个标准的 IPv4 地址。

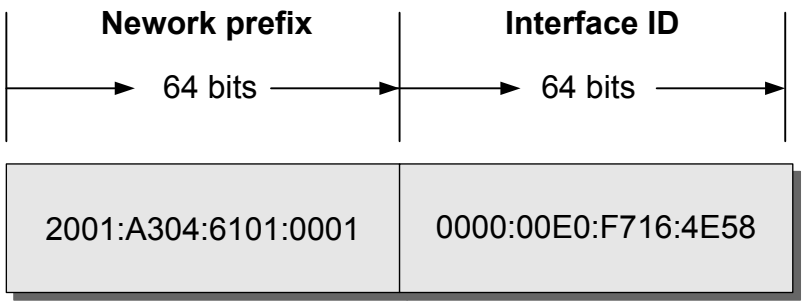
IPv6 地址的结构

一个 IPv6 地址可以分为如下两部分：

- 网络前缀：n 比特，相当于 IPv4 地址中的网络 ID
- 接口标识：128-n 比特，相当于 IPv4 地址中的主机 ID

地址 2001:A304:6101:1::E0:F726:4E58 /64 的构成如图 8-1 所示。

图 8-1 地址 2001:A304:6101:1::E0:F726:4E58 /64 的构成示意图



IPv6 的地址分类

IPv6 主要有三种类型的地址：单播地址、组播地址和任播地址。

- 单播地址：用来唯一标识一个接口，类似于 IPv4 的单播地址。发送到单播地址的数据报文将被传送给此地址所标识的接口。
- 组播地址：用来标识一组接口（通常这组接口属于不同的节点），类似于 IPv4 的组播地址。发送到组播地址的数据报文被传送给此地址所标识的所有接口。
- 任播地址：用来标识一组接口（通常这组接口属于不同的节点）。发送到任播地址的数据报文被传送给此地址所标识的一组接口中距离源节点最近（根据使用的路由协议进行度量）的一个接口。

说明

IPv6 中没有广播地址，广播地址的功能通过组播地址来实现。

IPv6 地址类型是由地址前面几位（称为格式前缀）来指定的，主要地址类型与格式前缀的对应关系如表 1 所示。

表 8-1 IPv6 单播地址类型

地址类型		二进制前缀	IPv6 前缀标识
单播地址	链路本地单播地	1111111010	FE80::/10
	环回地址	00...1 (128 bits)	::1/128
	未指定地址	00...0 (128 bits)	::/128
	全球单播地址	其他	-
组播地址		11111111	FF00::/8
任播地址		从单播地址空间中进行分配，使用单播地址的格式	

表中各类地址的意义如下：

IPv6 单播地址的类型可有多种，包括全球单播地址、链路本地地址和站点本地地址等。

- 链路本地单播地址：

  用于邻居发现协议和无状态自动配置进程中链路本地上节点之间的通信。使用链路本地地址作为源或目的地址的数据包不会被转发到其他链路上。使用链路本地前缀 FE80::/10(1111 1110 10)和 IEEE EUI-64 格式的接口标识符（EUI-64 可来源于 EUI-48）可在任意接口对其进行自动配置。

- 环回地址：

  环回地址 0:0:0:0:0:0:0:1 或::1，不会被分配给任何接口。它的作用与在 IPv4 中的 127.0.0.1 相同，即节点将 IPv6 报文发送给自己。

- 未指定地址

  地址“::”称为未指定地址，不能被分配给任何节点，也不能作为目的地址。在主机初始化且没有取得自己的地址时，未指定地址可以用在 IPv6 报文的源地址字段，例如重复地址探测时，NS 报文的源地址就是未指定地址。

- 全球单播地址

  全球单播地址等同于 IPv4 公网地址。用于可以聚合的链路，最后提供给网络服务提供商。这种地址类型的结构允许路由前缀的聚合，从而满足全球路由表项的数量限制。地址包括运营商管理的 48 位路由前缀和本地站点管理的 16 位子网 ID，以及 64 位接口 ID。如无特殊说明，全球单播地址包括站点本地单播地址。

- 组播地址

  Multicast）：用来标识属于不同节点的一组接口，类似 IPv4 的组播地址。发送到组播地址的数据包被传输给此地址所标识的所有接口。

  表 8-2 所示的组播地址，是预留的特殊用途的组播地址。

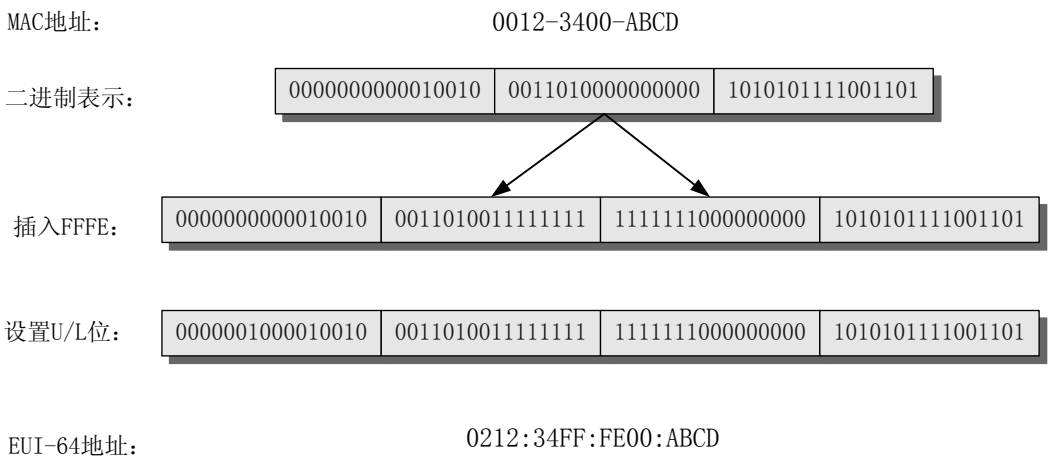
表 8-2 预留的 IPv6 组播地址列表

地址	应用
FF01::1	节点本地范围所有节点组播地址
FF02::1	链路本地范围所有节点组播地址
FF01::2	节点本地范围所有路由器组播地址
FF02::2	链路本地范围所有路由器组播地址
FF05::2	站点本地范围所有路由器组播地址

IEEE EUI-64 格式的接口标识符

IPv6 地址中的 64 位接口标识符（Interface ID）用来标识链路上的唯一接口。这个地址是从接口的链路层地址（如 MAC 地址）变化而来的。IPv6 地址中的接口标识符是 64 位，而 MAC 地址是 48 位，因此需要在 MAC 地址的中间位置插入十六进制数 FFFE（1111 1111 1111 1110）。然后将 U/L 位（从高位开始的第 7 位）设置为“1”，这样就得到了 EUI-64 格式的接口 ID。具体转换过程如图 8-2。

图 8-2 MAC 地址到 EUI-64 格式接口标识符的转换过程



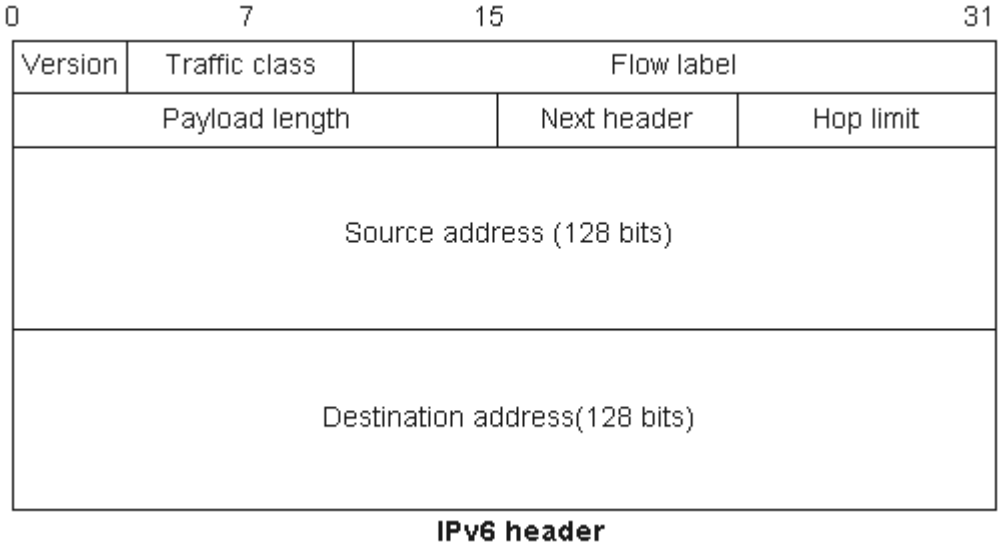
8.6 IPv6 报文格式

IPv6 的报文头格式

IPv6 报文的头部信息和一般的 IP 报文（即 IPv4 报文）有一定差异。

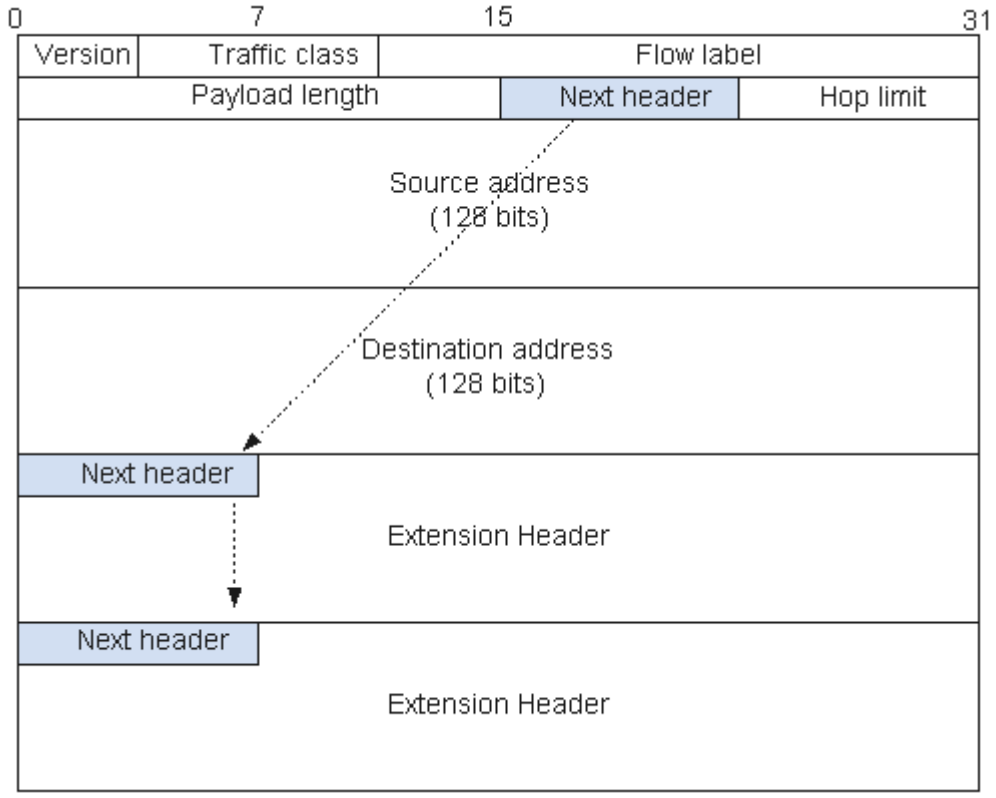
图 8-3 所示为 IPv6 报文头结构。

图 8-3 IPv6 报文头格式



- Version（版本）：该字段表示 IP 版本，值为 6。
- Traffic class（流量类别）：该字段及其功能类似于 IPv4 的业务类型字段。该字段以区分业务编码点（DSCP）标记一个 IPv6 数据包，以此指明数据包应当如何处理。
- Flow label（流标签）：该字段用来标记 IP 数据包的一个流，当前的标准中没有定义如何管理和处理流标签的细节。
- Payload length（有效载荷长度）：该字段表示有效载荷的长度，有效载荷是指紧跟 IPv6 基本报头的数据包，包含 IPv6 扩展报头。
- Next header（下一报头）：该字段指明了跟随在 IPv6 基本报头后的扩展报头的信息类型。如图 8-4 所示。

图 8-4 Next header 在 IPv6 报文头中的作用



- Hop limit（跳数限制）：该字段定义了 IPv6 数据包所能经过的最大跳数，这个字段和 IPv4 中的 TTL 字段非常相似。
- Source address（报文源地址）：该字段表示该报文的源地址。
- Destination address（报文目的地址）：该字段表示该报文的目的地址。

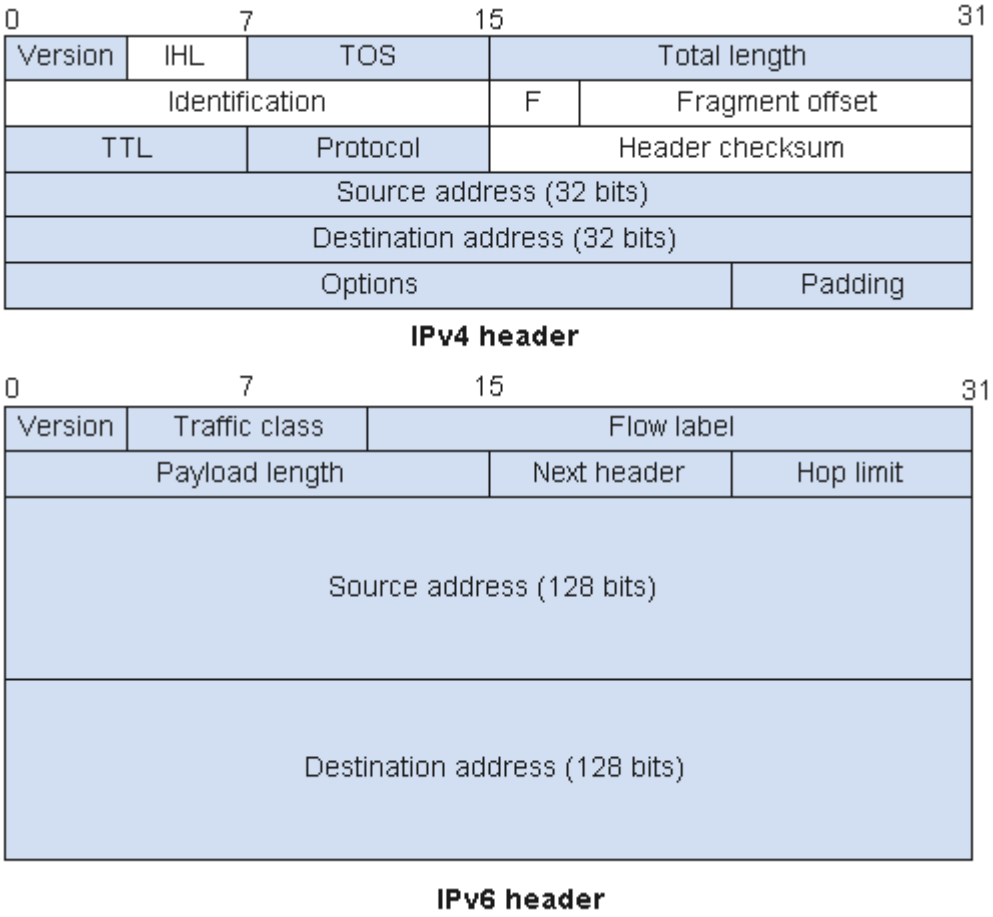
和 IPv4 报文头的比较

IPv6 通过将不重要的字段和选项字段移入扩展报头来减小报头的负载，使中间路由设备对报文的处理更有效。

尽管 IPv6 地址长度是 IPv4 地址长度的四倍，但 IPv6 基本报头的长度只有 IPv4 报头的两倍。

IPv4 和 IPv6 报头不具有互操作性，而且 IPv6 协议不能向后兼容 IPv4 协议。为了识别和处理两种报头格式，主机或路由设备必须同时运行 IPv4 和 IPv6 两种协议。

图 8-5 IPv4 和 IPv6 报文头格式比较



8.7 IPv6 的特点

简化的报文头格式

通过将 IPv4 报文头中的某些字段裁减或移入到扩展报文头，减小了 IPv6 基本报文头的长度。IPv6 使用固定长度的基本报文头，从而简化了转发设备对 IPv6 报文的处理，提高了转发效率。尽管 IPv6 地址长度是 IPv4 地址长度的四倍，但 IPv6 基本报文头的长度只有 40 字节，为 IPv4 报文头长度（不包括选项字段）的两倍。

充足的地址空间

IPv6 的源地址与目的地址长度都是 128 比特（16 字节）。它可以提供超过 3.4×10^{38} 种可能的地址空间，完全可以满足多层次的地址划分需要，以及公有网络和机构内部私有网络的地址分配。

层次化的地址结构

IPv6 的地址空间采用了层次化的地址结构，利于路由快速查找，同时借助路由聚合，可减少 IPv6 路由表的大小，提高路由设备的转发效率。

地址自动配置

为了简化主机配置，IPv6 支持有状态地址配置（Stateful Address Autoconfiguration）和无状态地址配置（Stateless Address Autoconfiguration）。

- 对于有状态地址配置，主机通过服务器获取地址信息和配置信息。
- 对于无状态地址配置，主机自动配置地址信息，地址中带有本地路由设备通告的前缀和主机的接口标识。如果链路上没有路由设备，主机只能自动配置链路本地地址，实现与本地节点的互通。

支持 QoS

IPv6 报头的新字段定义了流量应该被如何标识和处理。通过报文头里的流标签（Flow Label）字段完成流量标识，允许路由设备对某一流中的报文进行识别并提供特殊处理。

由于 IPv6 报头可对流量进行识别，即使是带有 IPSec 加密的报文载荷也可对其 QoS 进行保证

内置安全性

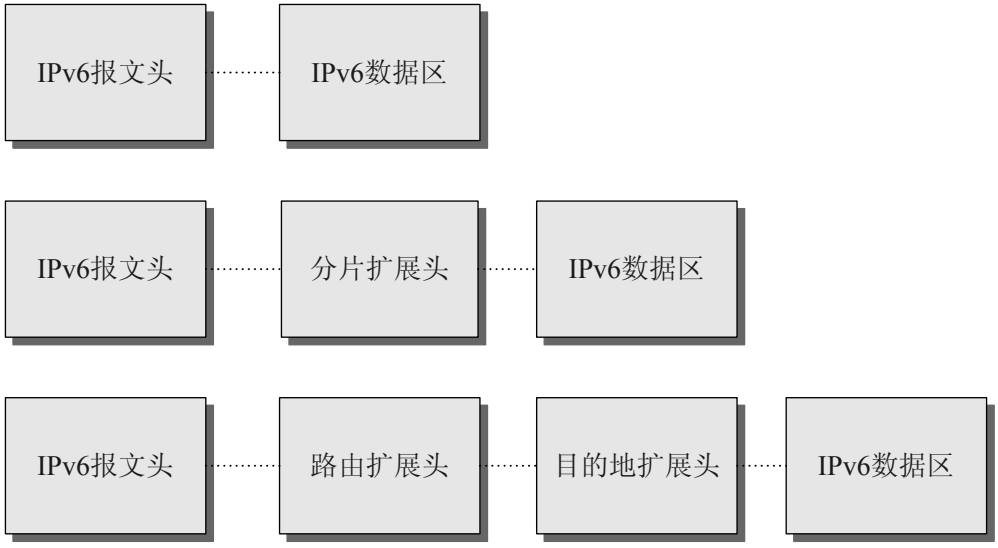
IPv6 将 IPSec 作为它的扩展报头实现，提供端到端的安全特性。这一特性为解决网络安全问题提供了标准，并提高了不同 IPv6 实现的互操作性。

灵活的扩展报文头

IPv4 报头只能支持 40 字节的选项，而 IPv6 扩展报头的大小只受到 IPv6 报文大小的限制。

IPv6 取消了 IPv4 报头中的选项字段，并引入了多种扩展报文头，在提高处理效率的同时还增强了 IPv6 的灵活性，为 IP 协议提供了良好的扩展能力。如图 8-6 所示。

图 8-6 IPv6 扩展报文头



当超过一种扩展报头被用在同一个分组里时，报头必须按照下列顺序出现：

- IPv6 基本报头
- 逐跳选项扩展报头
- 目的选项扩展报头
- 路由扩展报头
- 分片扩展报头
- 授权扩展报头
- 封装安全有效载荷扩展报头
- 目的选项扩展报头（指那些将被分组报文的最终目的地处理的选项）
- 上层扩展报头

不是所有的扩展报头都需要被转发路由设备查看和处理的。路由设备转发时根据基本报头中 Next Header 值来决定是否要处理扩展头。

除了目的选项扩展报头出现两次（一次在路由扩展报头之前，另一次在上层扩展报头之前），其余扩展报头只出现一次。

增强的邻居发现机制

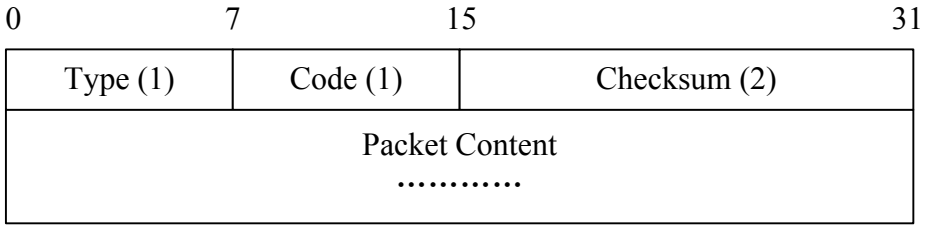
IPv6 的邻居发现协议是通过一组 ICMPv6（Internet Control Message Protocol for IPv6，IPv6 的因特网控制报文协议）消息实现的，管理着邻居节点间（即同一链路上的节点）信息的交互。它代替了 ARP（Address Resolution Protocol，地址解析协议）、ICMPv4 路由器发现和 ICMPv4 重定向消息，并提供了一系列其他功能。

8.8 ICMPv6

ICMPv6（Internet Control Message Protocol for the Internet Protocol Version 6）是 IPv6 的基础协议之一，具有差错报文和信息报文两种，用于 IPv6 节点报告报文处理过程中的错误和信息。

ICMPv6 报文的报文格式如图 8-7 所示

图 8-7 ICMPv6 报文格式



报文中各个字段的解释如下：

- Type 字段表明消息的类型，0 至 127 表示差错报文类型，128 至 255 位消息报文类型。
- Code 字段表示此消息类型细分的类型。
- Checksum 表示 ICMPv6 报文的校验和。

ICMPv6 错误报文的分类

- 目的不可达错误报文

  在 IPv6 节点转发 IPv6 报文过程中，发现目的地址不可达时，就会向发送报文的源节点发送 ICMPv6 目的不可达错误报文。同时报文中会携带引起该错误报文的具体原因。目的不可达错误报文又细分为以下几种：

  - 没有到目的地的路由
  - 地址不可达
  - 端口不可达

- 数据包过大错误报文

  在 IPv6 节点转发 IPv6 报文过程中，发现报文超过出接口的链路 MTU 时，则向发送报文的源节点发送 ICMPv6 数据包过大错误报文，其中携带出接口的链路 MTU 值。数据包过大错误报文是 Path MTU 发现机制的基础。

- 时间超时错误报文

  在 IPv6 报文收发过程中，当路由器收到 Hop Limit 值等于 0 的数据包，或者当路由器将 HopLimit 值减为 0 时，会向报文的源节点发送 ICMPv6 超时错误报文。对于分段重组报文的操作，如果超过定时时间，也会产生一个 ICMPv6 超时报文。

- 参数错误报文

  当目的节点收到一个 IPv6 报文时，会对报文进行有效性检查，如果发现以下问题会向报文的源节点回应一个 ICMPv6 参数错误差错报文。

  - IPv6 基本头或扩展头的某个域有错误
  - IPv6 基本头或扩展头的 NextHeader 值不可识别
  - 扩展头中出现未知的选项

ICMPv6 信息报文的分类

请求信息（Echo Request）和应答信息（Echo Reply）。可以利用 ICMPv6 报文实现网络故障诊断、PMTU 发现和邻居发现等功能。在两节点的互通性检测中，收到 Echo Request 报文的节点向源节点回应 Echo Reply 报文，实现两节点间报文的收发。

8.9 ACL6

ACL6 的分类

根据应用目的，可将 ACL6 分为两种：

- 基本 ACL6，基本 ACL6 只能使用源地址信息做为定义 ACL6 规则的元素。
- 高级 ACL6，高级 ACL6 可以使用数据包的源地址信息、目的地址信息、IP 承载的协议类型、针对协议的特性定义规则，例如 TCP 的源端口、目的端口，ICMPv6 协议的类型、ICMPv6 Code 等。可以利用高级 ACL6 定义比基本 ACL6 更准确、更丰富、更灵活的规则。

ACL6 的匹配顺序

一个 ACL 中可以包含多个规则，而每个规则都指定不同的报文匹配选项，这些规则可能存在重复或矛盾的地方，在将一个报文和 ACL 的规则进行匹配的时候，到底采用哪些规则呢？就需要确定规则的匹配顺序。

ACL6 支持两种匹配顺序：

- 配置顺序：按照用户配置规则的先后顺序进行规则匹配。
- 自动排序：按照“深度优先”的顺序进行规则匹配。
  - 基本 ACL6 的“深度优先”顺序判断原则如下
    1. 先比较源 IPv6 地址范围，源 IPv6 地址范围小（前缀长）的规则优先。
    2. 如果源 IPv6 地址范围相同，则先配置的规则优先。
  - 高级 ACL6 的“深度优先”顺序判断原则如下
    1. 先比较协议范围，指定了 IPv6 协议承载的协议类型的规则优先。
    2. 如果协议范围相同，则比较源 IPv6 地址范围，源 IPv6 地址范围小（前缀长）的规则优先。
    3. 如果协议范围、源 IPv6 地址范围相同，则比较目的 IPv6 地址范围，目的 IPv6 地址范围小（前缀长）的规则优先。
    4. 如果协议范围、源 IPv6 地址范围、目的 IPv6 地址范围相同，则比较四层端口号（TCP/UDP 端口号）范围，四层端口号范围小的规则优先。
    5. 如果上述范围都相同，则先配置的规则优先。

    在报文匹配规则时，会按照匹配顺序去匹配定义的规则，一旦有一条规则被匹配，报文就不再继续匹配其它规则了，设备将对该报文执行第一次匹配的规则指定的动作。

8.10 邻居发现

邻居发现 ND（Neighbor Discovery）是确定邻居节点之间关系的一组消息和进程。邻居发现协议替代了 IPv4 的 ARP（Address Resolution Protocol）、ICMP 路由器发现（Router Discovery）和 ICMP 重定向（Redirect）消息，并提供了其他功能。

对于一个节点而言，当其配置一个 IPv6 地址之后，首先会确定此地址是否可用、不冲突。当一个节点是主机时，路由器需要通知主机向特定目的地址转发报文的理想下一跳地址；当一个节点是路由器时，需要发布自己的地址、地址前缀和其他配置参数以指导主机进行参数配置。在 IPv6 报文转发过程中，节点需要确定邻居节点的链路层地址和其可达性。IPv6 邻居发现机制提供了 5 种不同类型的 ICMPv6 报文。

- 路由器请求报文 RS（Router Solicitation）：主机启动后，通过 RS 报文向路由设备发出请求，路由设备则会以 RA 报文响应。
- 路由器通告报文 RA（Router Advertisement）：路由设备周期性的发布 RA 报文，其中包括前缀和一些标志位的信息。
- 邻居请求报文 NS（Neighbor Solicitation）：IPv6 节点通过 NS 报文可以得到邻居的链路层地址，检查邻居是否可达，也可以进行重复地址检测。
- 邻居通告报文 NA（Neighbor Advertisement）：NA 报文是 IPv6 节点对 NS 报文的响应，同时 IPv6 节点在链路层变化时也可以主动发送 NA 报文。
- 重定向报文（Redirect）：路由设备发现报文的入接口和出接口相同时，可以通过重定向报文通知主机选择另外一个更好的下一跳地址。

IPv6 邻居发现协议主要包括以下功能：

地址冲突检测功能

地址冲突检测 DAD（Duplicate address detect）是确定 IPv6 地址是否可用的一种探测机制。具体执行过程如下：

1. 当一个节点配置了 IPv6 地址，为了查看该地址是否被其他邻居节点所使用，会即时发送邻居请求报文来确定其可用性。
2. 当其他邻居节点收到该报文后会查找本地的 IPv6 地址中是否存在相同的 IPv6 地址，若存在会回应一个邻居通告报文给源节点，并携带此 IPv6 地址信息。
3. 源节点收到邻居的回应报文则认为该 IPv6 地址已被邻居使用。反之，如果源节点发出的邻居请求报文没有收到相应的回应报文，则表示配置的 IPv6 地址是可用的。

邻居发现功能

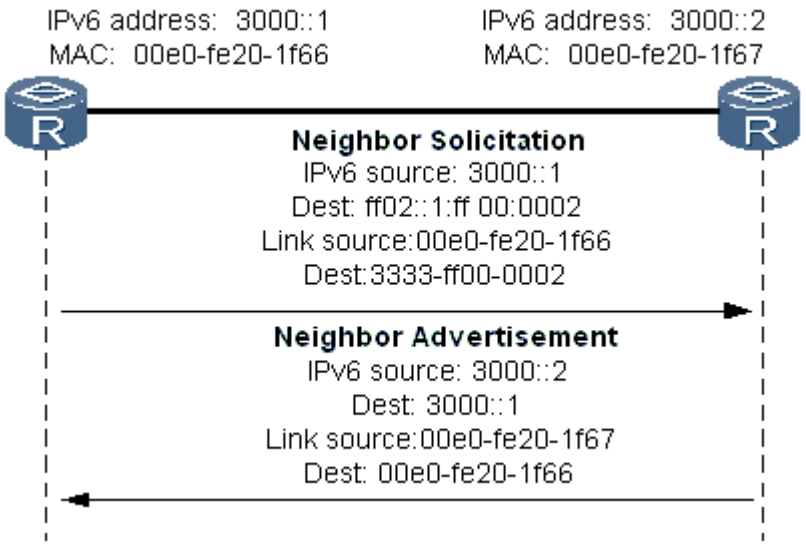
邻居发现功能和 IPv4 中的 ARP 功能类似，主要实现对邻居地址的解析和邻居可达性的探测，依赖于邻居请求和邻居通告报文完成。

当一个节点需要得到同一本地链路上另外一个节点的链路层地址时，就会发送 ICMPv6 类型为 135 的邻居请求报文。此报文类似于 IPv4 中的 ARP 请求报文，不过使用组播地址而不使用广播地址，只有被请求节点的最后 24 比特和此组播地址相同的节点才会收到此报文，减少了广播风暴的可能。目的节点在响应报文中填充其链路层地址。

邻居请求报文也用来在邻居的链路层地址已知时，验证邻居的可达性。IPv6 邻居通告报文是对 IPv6 邻居请求报文的响应。收到邻居请求报文后，目的节点通过在本地链路上发送 ICMPv6 类型为 136 的邻居通告报文进行响应。收到邻居通告后，源节点和目的节点可以进行通信。当一个节点的本地链路上的链路层地址改变时也会主动发送邻居通告报文。

图 8-8 所示为 IPv6 邻居发现过程。

图 8-8 IPv6 邻居发现过程



路由器发现功能

路由器发现功能用来定位邻居路由设备，同时学习和地址自动配置有关的前缀和配置参数。IPv6 路由发现由下面两种机制实现：

- 路由器请求

  当主机没有配置单播地址时（例如系统刚启动），就会发送路由器请求报文 RS。路由器请求报文有助于主机迅速进行自动配置而不必等待 IPv6 路由设备的周期性路由器通告报文。IPv6 路由器请求也是 ICMPv6 报文，类型为 133。

- 路由器通告

  每个 IPv6 路由设备的接口在配置了 IPv6 RA 去抑制的前提下会周期发送路由器通告报文。在本地链路上收到 IPv6 节点的路由器请求报文后，路由设备也会回应路由器通告报文。IPv6 路由器通告报文发送到所有节点多播地址（FF02::1）或发送路由器请求报文节点的 IPv6 单播地址。路由器通告为 ICMPv6 报文，类型为 134，包含以下内容：

  - 是否使用地址自动配置
  - 标记支持的自动配置类型（无状态或有状态自动配置）
  - 一个或多个本地链路前缀（本地链路上的节点可以使用这些前缀完成地址自动配置）
  - 通告的本地链路前缀的生存期
  - 发送路由器通告的路由设备是否可作为缺省路由设备，如果可以，还包括此路由设备可作为缺省路由设备的时间（用秒表示）
  - 和主机相关的其它信息，如跳数限制、主机发起的报文可以使用的最大 MTU

  本地链路上的 IPv6 节点接收路由器通告报文，并用其中的信息得到更新的缺省路由设备、前缀列表以及其它配置。

地址自动配置功能

通过使用路由器通告报文和针对每一前缀的标记，路由设备可以通知主机如何进行地址自动配置。例如，路由设备可以指定主机是使用有状态（DHCPv6）地址配置还是无状态地址自动配置进行地址配置。

对于无状态地址自动配置而言，当主机收到路由器通告报文后，使用其中的前缀信息和本地接口 ID 自动形成 IPv6 地址，同时还可以根据其中的默认路由设备信息设置默认路由设备。

重定向功能

重定向报文用来通知主机去往目的地的理想下一跳 IPv6 地址。和 IPv4 类似，IPv6 路由设备发送重定向报文的目的仅限于把报文重新路由到更合适的路由设备。收到重定向报文的节点随后会把后续报文发送到更合适的路由设备。路由设备只针对单播流发送重定向报文，重定向报文只发送给引起重定向的报文的节点（主机），并被处理。

8.11 Path MTU

网络上的 MTU 问题

由于 IPv6 报文在传输过程中不允许在中间节点分片转发，所以在转发过程中经常会出现报文长度大于路径 IPv6 MTU 的情形，这就需要源节点不断的进行重传，降低了传输

的效率，如果在源节点使用最小链接 IPv6 MTU（1280）作为分片的最大长度，在大多数情况下，路径的 IPv6 MTU 是大于最小链接的 IPv6 MTU 的，一个节点发出的分片远小于路径 IPv6 MTU，这是对网络资源的一种浪费，为了解决这个问题，提出了路径 MTU 发现协议。

Path MTU 的工作原理

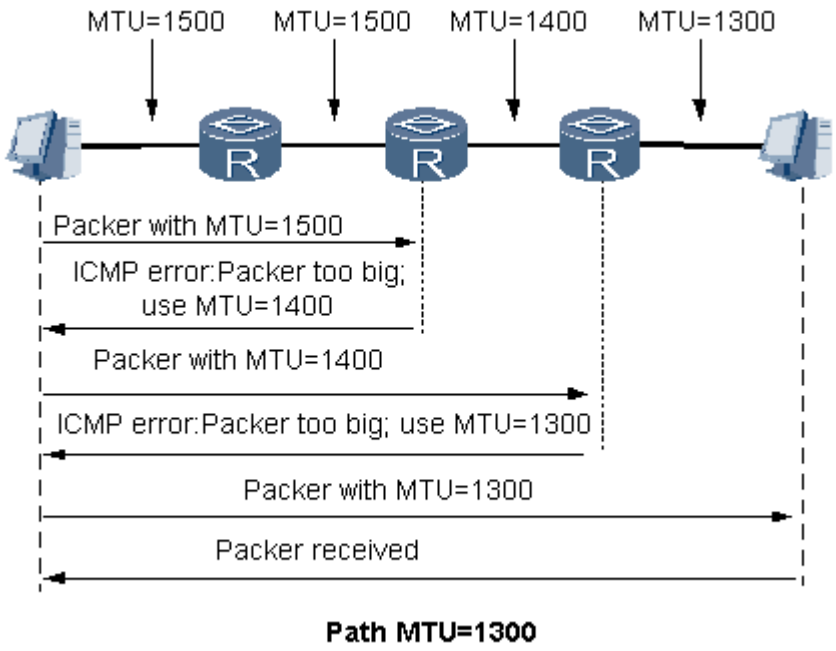
Path MTU（以下简称 PMTU），是确定从源端到目的端路径上合适的 IPv6 MTU 值的一种机制。PMTU 发现协议描述了一种动态发现任意路径的 PMTU 的方法。当一个 IPv6 节点发送大量数据到另一节点时，数据通过一系列 IPv6 分片传送。当这些分片具有从源节点到信宿节点能够成功传送所允许的最大长度时，我们认为它达到理想状态，这个分片长度被称为路径 MTU。

一个源节点开始会假设一个路径的 PMTU 是路径中第一跳的已知的 IPv6 MTU，如果从那个路径发出的报文太大以至于不能沿着路径转发，中间节点将丢弃此报文并返回一个 ICMPv6 数据过大差错报文给源节点，根据数据过大消息中的 IPv6 MTU 值来设置此路径的 PMTU 值。

当节点学习到的 PMTU 值小于或者等于实际的 PMTU 时，PMTU 的发现过程结束。注意在 PMTU 发现过程结束之前，可能会出现反复发送报文和收到报文太大消息，这是因为可能会不断发现更远的路径链路有更小的 IPv6 MTU。

如图 8-9 所示，PMTU 发现的工作过程是：源端主机先使用自己的 MTU 值向目的主机发送报文，如果中间路由设备给源端返回一个错误消息，其中包括该网络的 MTU 值，源端主机使用该 MTU 值来重新发送这个报文，如此反复，直到目的端主机收到这个报文，从而确定网络中两台主机之间能够处理的最大报文的大小。

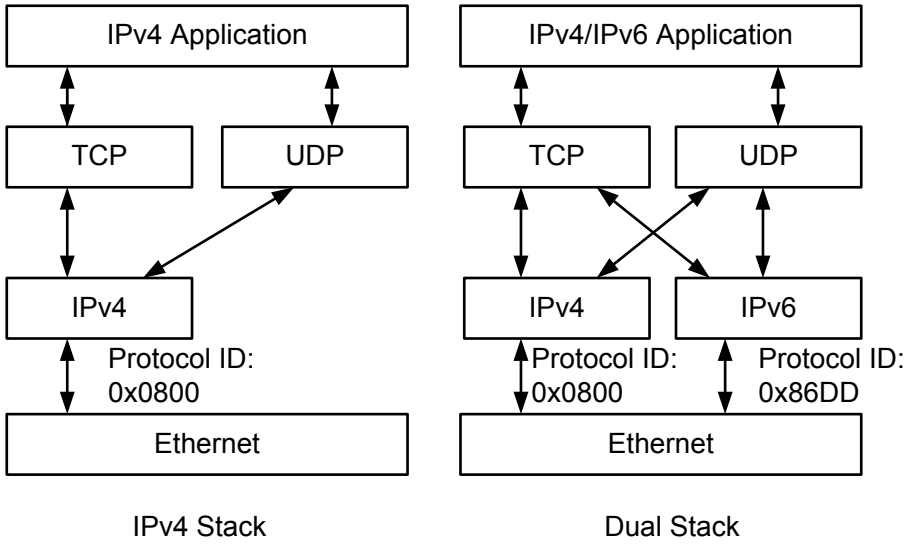
图 8-9 PMTU 发现的工作过程



8.12 双协议栈

对于 IPv6 节点来说，兼容 IPv4 的最直接有效的办法就是保留一个完整的 IPv4 协议栈，这样的节点即为双协议栈节点。单协议栈和双协议栈结构示例如图 8-10 所示。

图 8-10 单协议栈与双协议栈结构（以太网）



双协议栈具有以下特点：

- 多种链路协议支持双协议栈

  多种链路协议（如以太网）支持双协议栈。图中的链路层是以太网，在以太网帧上，如果协议类型字段的值为 0x0800，表示网络层是 IPv4 报文，如果为 0x86DD，表示网络层是 IPv6 报文。

- 多种应用支持双协议栈

  多种应用（如 DNS/FTP/Telnet 等）支持双协议栈。上层应用（如 DNS）可以选用 TCP 或 UDP 作为传输层的协议，但优先选择 IPv6 协议栈，而不是 IPv4 协议栈作为网络层协议。

8.13 NAT-PT

NAT-PT（Network Address Translation-Protocol Translation）是附带协议转换的网络地址转换，它通过修改 IP 报文头中的地址和协议字段，使 IPv6 网络和 IPv4 网络之间可以互通。

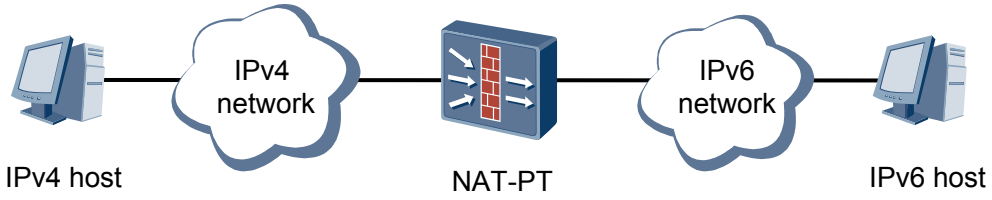
NAT-PT 应用场景

IPv6 的应用是个循序渐进的过程，在很长时间内，IPv4 网络和 IPv6 网络会同时存在且需要相互通信。在 IPv4 网络完全过渡到 IPv6 网络之前，两个网络之间直接的通信可以

通过 NAT-PT 来实现。NAT-PT 提供了 IPv4 和 IPv6 地址之间的相互转换功能，例如，使用此技术可以使 IPv6 网络中的主机直接访问 IPv4 网络中的 FTP 服务器。

如图 8-11 所示，NAT-PT 作用于 IPv4 和 IPv6 网络边缘设备上，所有的地址转换过程都在该设备上实现，对 IPv4 和 IPv6 网络来说是透明的，即用户不必改变目前的 IPv4 网络中主机的配置就可实现与 IPv6 网络的通信。

图 8-11 NAT-PT 示意图



NAT-PT 机制

有两种 NAT-PT 机制可实现 IPv4 和 IPv6 地址之间的相互转换：

- 静态映射

  静态映射是指采用手工配置的 IPv6 地址与 IPv4 地址的一一对应关系来实现 IPv6 地址与 IPv4 地址的转换。

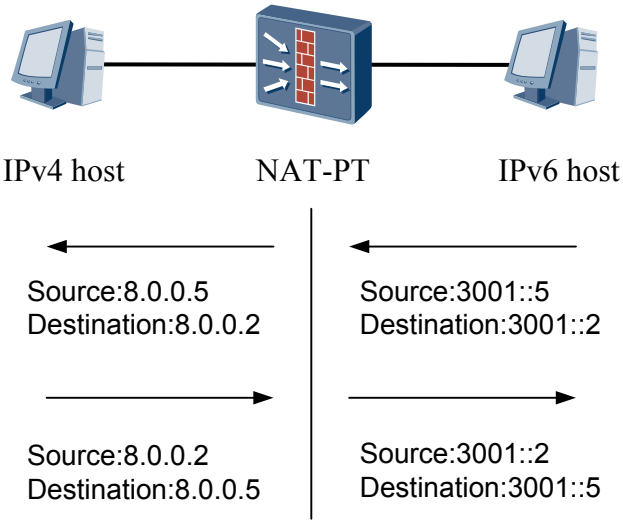
- 动态映射

  动态映射是指动态地创建 IPv6 地址与 IPv4 地址的对应关系来实现 IPv6 地址与 IPv4 地址的转换。和静态映射不同，动态映射中 IPv6 和 IPv4 地址之间不存在固定的一一对应关系。

NAT-PT 实现过程

IPv6 主机访问 IPv4 主机的 NAT-PT 实现过程，如图 8-12 所示。

图 8-12 NAT-PT 的实现过程



1. 判断是否进行 NAT-PT 转换：

   NAT-PT 设备接收到 IPv6 网络主机（IPv6 host）发送给 IPv4 网络主机（IPv4 host）的报文后，判断该报文是否要转发到 IPv4 网络。如果报文目的 IPv6 地址前缀与设备上预先配置的 NAT-PT 前缀相同，则该报文需要转发到 IPv4 网络，需要进行 NAT-PT 转换。

2. 转换源 IP 地址：

   设备根据 IPv6 侧配置的静态或者动态映射，进行 IPv6 地址到 IPv4 地址的转换，将报文的源 IPv6 地址转换为 IPv4 地址。

3. 转换目的 IP 地址：

   设备根据 IPv4 侧配置的静态映射将目的 IPv6 地址转换为 IPv4 地址。如果没有配置静态映射，那么，如果报文中的目的 IPv6 地址的低 32 位可以直接转换为合法的 IPv4 地址，则直接转换为目的 IPv4 地址；否则，转换不成功。

4. 转发报文并记录映射关系：

   报文的源 IPv6 地址和目的 IPv6 地址都转换为 IPv4 地址后，设备按照正常的转发流程将报文转发到 IPv4 网络中的主机。同时，将 IPv6 地址与 IPv4 地址的映射关系保存在设备中。

5. 根据记录的映射关系转发应答报文：

   IPv4 网络主机发送给 IPv6 网络主机的报文到达 NAT-PT 设备后，设备将根据已保存的映射关系进行相反的转换，从而将报文发送给 IPv6 网络主机。

应用 DNS-ALG 的 NAT-PT 机制

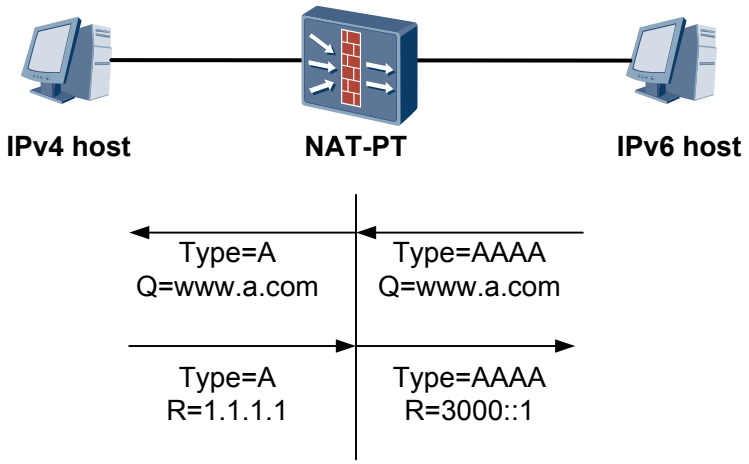
IPv6 主机如果要通过主机名而不是 IP 地址与 IPv4 主机通信，就需要先使用 NAT-PT 的 DNS-ALG（Application Level Gateway）对主机名进行解析。

DNS-ALG 具体支持的 DNS 报文类型如下：

- IPv4 主机发出的 A 查询报文（查询域名对应的 IPv4 地址）
- IPv6 主机发出的 AAAA 查询报文（查询域名对应的 IPv6 地址）
- IPv4 DNS 服务器发出的 A 响应报文（DNS 服务器对 A 查询报文的响应）
- IPv6 DNS 服务器发出的 AAAA 响应报文（DNS 服务器对 AAAA 查询报文的响应）

下面以图 8-13 为例，说明 DNS-ALG 支持主机名解析的过程。

图 8-13 应用 DNS-ALG 的 NAT-PT 机制



1. IPv6 主机发送 AAAA 查询报文，要求解析名字“www.a.com”。该报文的目的地址是在 IPv6 主机上静态配置的 DNS 服务器 IPv6 地址。
2. NAT-PT 设备接收 IPv6 的查询报文后，将 AAAA 请求报文转换为 A 请求报文。转换后的请求报文中的 DNS 服务器地址为 IPv4 地址形式。报文的 IPv6 源地址（IPv6 主机的 IPv6 地址）可静态或动态的转换为 IPv4 地址。
3. IPv4 的 DNS 服务器响应 A 请求报文，并将响应报文发送给 NAT-PT 设备。
4. NAT-PT 设备将 DNS 的 A 响应报文转换为 AAAA 响应报文（包括进行 IPv4 到 IPv6 地址的转换），并发给 IPv6 主机。

通过以上步骤，IPv6 主机查询到了“www.a.com”的 IPv6 地址。IPv6 主机可以通过主机名而不是 IP 地址与 IPv4 主机通信了。

说明

IPv6 主机获得目的 IPv4 主机地址后，IPv6 主机与目的 IPv4 主机通信过程中的 IP 地址转换与上面步骤中相同，可以是静态转化，也可以是动态转换。

NAT-PT 的局限性

NAT-PT 具有下列一些局限性：

- 属于同一会话的请求和响应都必须通过同一台 NAT-PT 设备，才能进行 NAT-PT 转换。
- 不能转换 IPv4 报文头的可选项部分。
- 缺少端到端的安全性。

因此，在一些场合不推荐使用 NAT-PT，例如，IPv6 网络中主机跨越 IPv4 网络与另一 IPv6 网络中主机通信时，推荐使用隧道技术。

8.14 IPv6 over IPv4 隧道

在 IPv4 网络向 IPv6 网络过渡的初期，IPv4 网络已被大量部署，而 IPv6 网络只是散步在世界各地的一些孤岛。利用隧道技术可以在 IPv4 网络上创建隧道，从而实现 IPv6 孤岛之间的互连。在 IPv4 网络上用于连接 IPv6 孤岛的隧道称为 IPv6 over IPv4 隧道。为了实现 IPv6 over IPv4 隧道，需要在 IPv4 网络与 IPv6 网络交界的边界路由设备上启动 IPv4/IPv6 双协议栈。

IPv6 over IPv4 隧道技术的原理如图 8-14 所示。

1. 启动 IPv4/IPv6 双协议栈

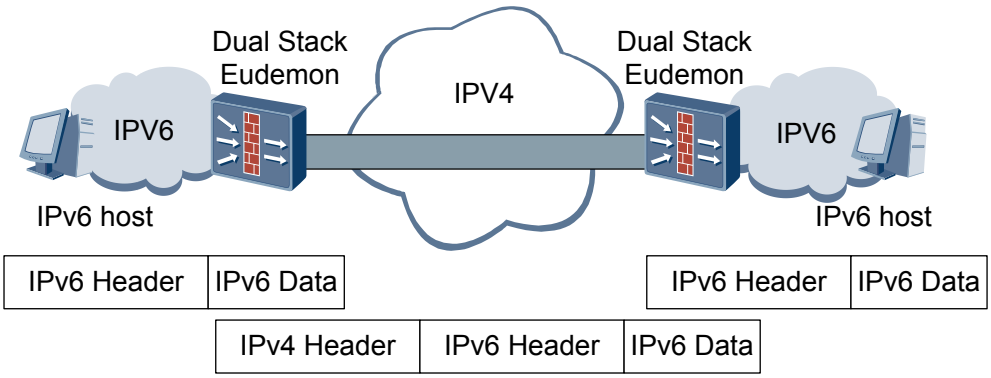
   边界路由设备启动 IPv4/IPv6 双协议栈。
2. 封装 IPv6 报文

   边界路由设备在收到从 IPv6 网络侧来的报文后，根据路由表判定该报文要通过隧道进行转发，就把收到的 IPv6 报文作为负载，加上 IPv4 报文头，封装到 IPv4 报文里。
3. 传递封装后的报文

   在 IPv4 网络中，封装后的报文被传递到对端的边界路由设备上。
4. 对报文解封装

对端边界路由设备对报文解封装，去掉 IPv4 报文头，然后将解封装后的 IPv6 报文转发到对端的 IPv6 网络中。

图 8-14 IPv6 over IPv4 隧道原理图



在两个边界路由设备之间用来传递 IPv6 报文的虚拟的通道就是 IPv6 over IPv4 隧道。根据创建隧道的方式，可以对隧道进行分类。目前，常用的 IPv6 over IPv4 隧道模式有以下几种。

- IPv6 over IPv4 手动隧道
- IPv6 over IPv4 GRE 隧道（简称 GRE 隧道）
- IPv6 over IPv4 自动隧道（简称自动隧道）
- 6to4 隧道

IPv6 over IPv4 手动隧道

IPv6 over IPv4 手动隧道是在隧道两端的边界路由设备上通过人工配置而创建的。它需要静态指定隧道的源 IPv4 地址和目的 IPv4 地址。

手动隧道相当于通过 IPv4 骨干网连接的两个 IPv6 域的永久链路，是边界路由设备之间进行定期安全通信的固定通道。

手动隧道可用于 IPv6 孤岛之间的通信，也可在边界路由设备与主机之间配置。隧道两端的主机和路由设备均需支持 IPv4 和 IPv6 协议栈。

IPv6 over IPv4 GRE 隧道

使用 IPv4 的 GRE（Generic Routing Encapsulation）隧道也可以承载 IPv6 报文，此时的 GRE 隧道称为 IPv6 over IPv4 GRE 隧道。与 IPv6 over IPv4 手动隧道相同，GRE 隧道也是两点之间的链路，每条链路都是一条单独的隧道。GRE 隧道不与特定的乘客或传输协议绑定，只把 IPv6 作为乘客协议，把 GRE 作为承载协议。

GRE 隧道也是在隧道两端的边界路由设备上通过人工配置而创建的，也需要静态指定隧道的源 IPv4 地址和目的 IPv4 地址。与手动隧道不同的是，GRE 隧道为了增强隧道的安全性，可以设置对 GRE 报文头进行校验以及对隧道的关键字进行验证。

GRE 隧道可用于边界路由设备之间，或者用于边界路由设备与主机系统之间。隧道两端的主机和路由设备均需支持 IPv4 和 IPv6 协议栈。

有关 GRE 配置的详细介绍请参见《配置指南 VPN 分册》。

IPv6 over IPv4 自动隧道

要创建 IPv6 over IPv4 自动隧道，需要使用一类特殊的 IPv6 地址，即兼容 IPv4 的 IPv6 地址。兼容 IPv4 的 IPv6 地址格式为：

0:0:0:0:0:0:IPv4-address

其高阶 96bits 均为 0，其低阶 32bits 是一个 IPv4 地址。该 IPv4 地址必须是 IPv4 网络中可达的 IPv4 地址，且不能是组播地址、广播地址、环回地址或未指定的地址（0.0.0.0）。

在配置自动隧道时，只需要在边界路由设备或主机上指定隧道源地址，不需要指定隧道的目的地址。隧道目的地址是从原始的 IPv6 报文的目的地址中获取的。

IPv6 over IPv4 自动隧道通常用于孤立的 IPv4/IPv6 双协议栈主机需要穿过 IPv4 网络访问远端 IPv6 网络的情况。在孤立的 IPv4/IPv6 主机和 IPv4/IPv6 路由设备之间需要配置自动隧道。

在建立自动隧道时，需要隧道两端都要配置兼容 IPv4 的 IPv6 地址，兼容 IPv4 的 IPv6 地址又依赖于隧道的物理接口的 IPv4 地址，受到 IPv4 地址短缺的限制，因而有一定的局限性。

6to4 隧道

6to4 隧道也是一种将多个 IPv6 孤岛通过 IPv4 网络互连的机制。6to4 隧道可在孤立的 IPv6 网络和 IPv4 网络之间的边界路由设备上配置。6to4 隧道两端的边界路由设备必须同时支持 IPv4 和 IPv6 双协议栈。

6to4 隧道与手动配置隧道的主要区别在于：6to4 隧道可以是点到多点的连接，而手动隧道仅是点到点的连接。所以 6to4 隧道的路由设备并不是成对配置的。

6to4 隧道与自动隧道类似，它可自动查找隧道的另一端点，但它不需要指定兼容 IPv4 的 IPv6 地址。

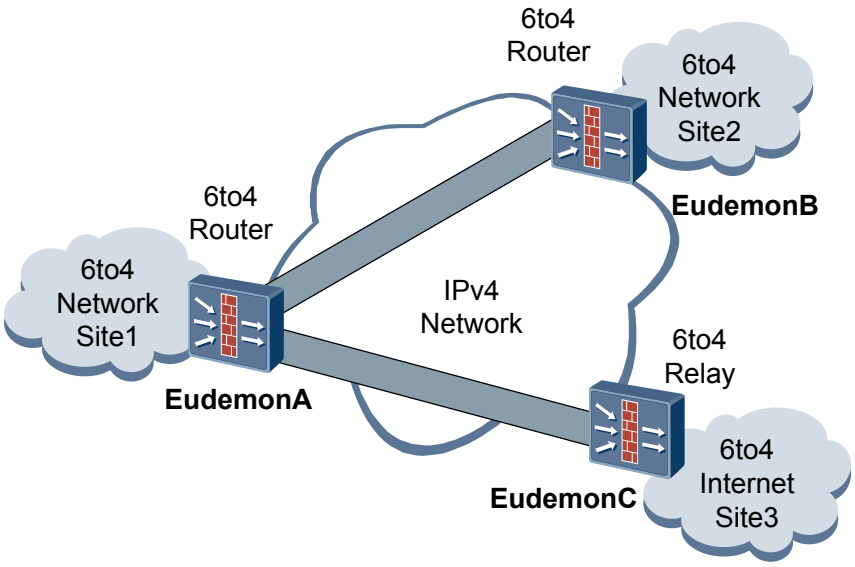
6to4 隧道使用了一种特殊的 IPv6 地址，即 6to4 地址，其格式为：

2002:IPv4 地址:子网 ID:接口 ID

6to4 地址的前缀是 **2002:IPv4 地址**，前缀长度为 48bits。其中 IPv4 地址是为 IPv6 孤岛申请的一个全球唯一的 IPv4 地址。在 IPv6/IPv4 边界路由设备与 IPv4 网络链接的物理接口上必须配置该 IPv4 地址。子网 ID 的长度为 16bits，接口 ID 的长度为 64bits，均由用户在 IPv6 孤岛内分配。

如图 8-15 所示，Site1 和 Site2 均为 6to4 网络，6to4 网络内的主机和路由设备被分配了 6to4 地址。Site1 内的主机和路由设备的 6to4 地址内嵌入的 IPv4 地址就是 EudemonA 到 IPv4 网络接口的 IPv4 地址。Site2 内的主机和路由设备的 6to4 地址内嵌入的 IPv4 地址就是 EudemonB 到 IPv4 网络接口的 IPv4 地址。EudemonA 和 EudemonB 均为 6to4 路由设备。

图 8-15 6to4 隧道和 6to4 中继



Site1 内的主机要访问 Site2 内的主机时，其工作原理如下：

1. IPv6 报文被传送到 EudemonA；
2. EudemonA 检查 IPv6 报文的目的地址，发现是 6to4 地址，从该 6to4 地址中获得 6to4 隧道对端的 IPv4 地址；
3. EudemonA 将该 IPv6 报文封装到 IPv4 报文中，IPv4 报文头的目的地址就是隧道对端的 IPv4 地址，源地址就是隧道本端的 IPv4 地址；
4. EudemonA 将该 IPv4 报文通过 IPv4 网络转发到 EudemonB；
5. EudemonB 进行解封装操作，获得原来的 IPv6 报文，然后将该 IPv6 报文在 Site2 内被送到目的主机。

上面介绍的过程可以实现 6to4 网络之间的通信。为了实现 6to4 网络与本地（Native）IPv6 网络之间的通信，就需要 6to4 中继路由设备了。所谓本地 IPv6 网络，就是它内部的主机或路由设备均不配置 6to4 地址。

6to4 中继路由设备是 6to4 网络与本地 IPv6 网络之间的网关。6to4 中继路由设备的一侧连接本地 IPv6 网络，其另一侧连接 IPv4 网络，并与 6to4 路由设备建立 6to4 隧道。如图 8-15 所示，6to4 网络内的主机要访问 IPv6 Internet 时，其工作过程如下。

1. IPv6 报文被路由到 EudemonA；
2. EudemonA 与路由设备 C 之间建立 6to4 隧道；
3. IPv6 报文封装在 IPv4 报文中被送到 EudemonC；
4. EudemonC 执行解封装操作，将 IPv6 Internet 内的原 IPv6 报文被送到目的主机。

ISATAP 隧道

ISATAP（Intra-site Automatic Tunnel Addressing Protocol）隧道用于 IPv4 网络中的 IPv4/IPv6 主机访问 IPv6 网络的情况，可以在 ISATAP 主机与 ISATAP 路由设备之间建立 ISATAP 隧道。

建立 ISATAP 隧道时，需要使用 ISATAP 格式地址，其结构如下：

Prefix(64bit)::5EFE:IPv4-Address

在创建 ISATAP 隧道时，由于 IPv4/IPv6 主机和 ISATAP 路由设备在同一个 IPv4 网络里，ISATAP 地址中嵌入的 IPv4 地址可以是公网地址，也可以是私网地址。

如图 8-16 所示，IPv4/IPv6 主机获得 IPv6 地址的过程如下：

1. IPv4/IPv6 主机发送路由设备请求消息

   IPv4/IPv6 主机使用 ISATAP 格式的链路本地地址向 ISATAP 路由设备发送路由设备请求消息，该路由设备请求消息被封装在 IPv4 报文中。

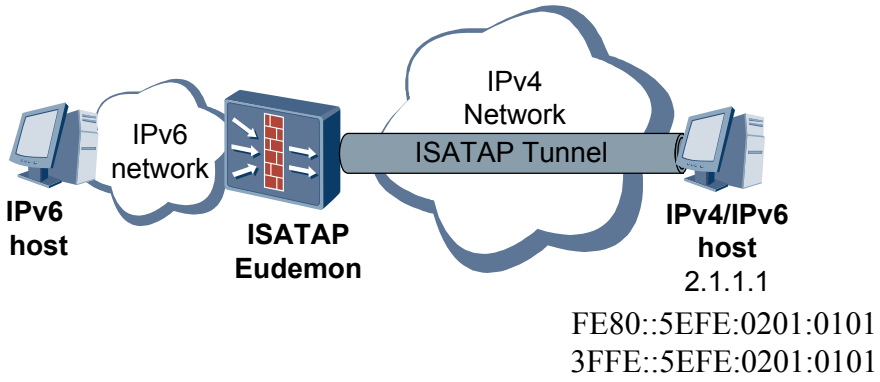
2. ISATAP 路由设备响应请求

   ISATAP 路由设备使用路由设备通告消息响应主机的路由设备请求。路由设备通告消息中包含 ISATAP 前缀（ISATAP 前缀在路由设备上通过人工配置）。

3. IPv4/IPv6 主机得到自己的 IPv6 地址

   IPv4/IPv6 主机将 ISATAP 前缀与 **5EFE:IPv4-Address** 组合得到自己的 IPv6 地址，并用此地址访问 IPv6 主机。

图 8-16 ISATAP 隧道



IPv4/IPv6 主机要访问 IPv6 Internet 时，其工作原理如下。

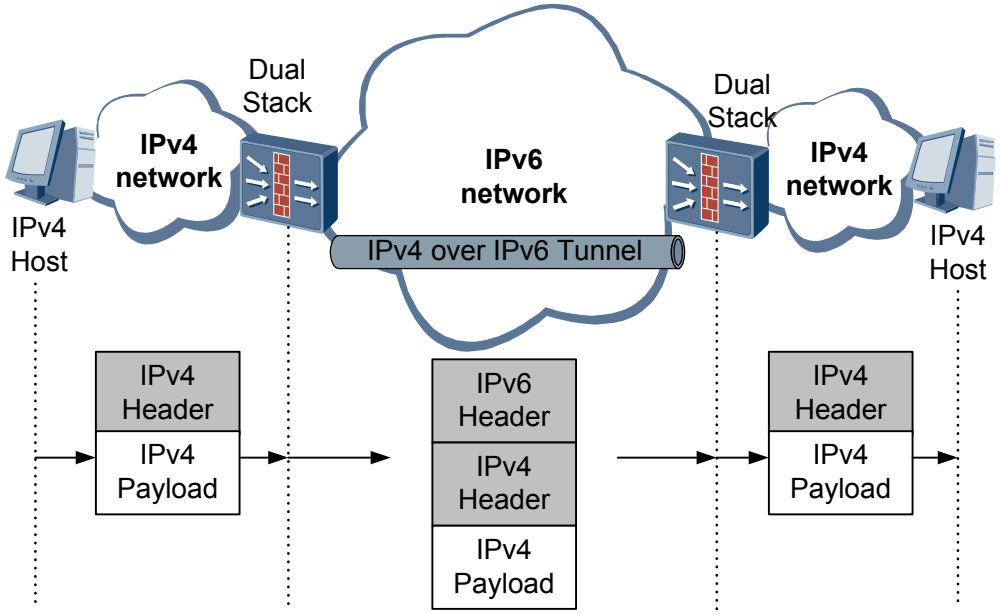
1. IPv4 网络中的 IPv4/IPv6 主机按照上面的过程获得自己的 IPv6 地址。
2. IPv4/IPv6 主机发送访问 IPv6 网络的 IPv6 主机的报文，该报文封装在 IPv4 中。
3. ISATAP 路由设备接收该 IPv4 报文后执行解封装操作，将其中的 IPv6 报文发送到 IPv6 网络中的 IPv6 主机。

8.15 IPv4 over IPv6 隧道

在 IPv4 Internet 向 IPv6 Internet 过渡的后期，IPv6 网络已被大量部署，此时可能出现 IPv4 孤岛。利用隧道技术可在 IPv6 网络上创建隧道，从而实现 IPv4 孤岛的互连。这类似于在 IP 网络上利用隧道技术部署 VPN。在 IPv6 网络上用于连接 IPv4 孤岛的隧道，称为 IPv4 over IPv6 隧道。

IPv4 over IPv6 技术原理

图 8-17 IPv4 over IPv6 隧道组网图



IPv4 over IPv6 隧道技术的原理如图 8-17 所示。

1. 启动 IPv4/IPv6 双协议栈

   边界路由设备启动 IPv4/IPv6 双协议栈。

2. 封装 IPv6 报文

   边界路由设备在收到从 IPv4 网络侧来的报文后，如果报文的目的地不是自身，就把收到的 IPv4 报文作为净荷，加上 IPv6 报文首部，封装到 IPv6 报文里。

3. 传递封装后的报文

   在 IPv6 网络中，封装后的报文被传递到对端的边界路由设备。

4. 对报文解封装

   对端边界路由设备对报文解封装，去掉 IPv6 报文首部，然后将解封装后的 IPv4 报文转发到 IPv4 网络中。

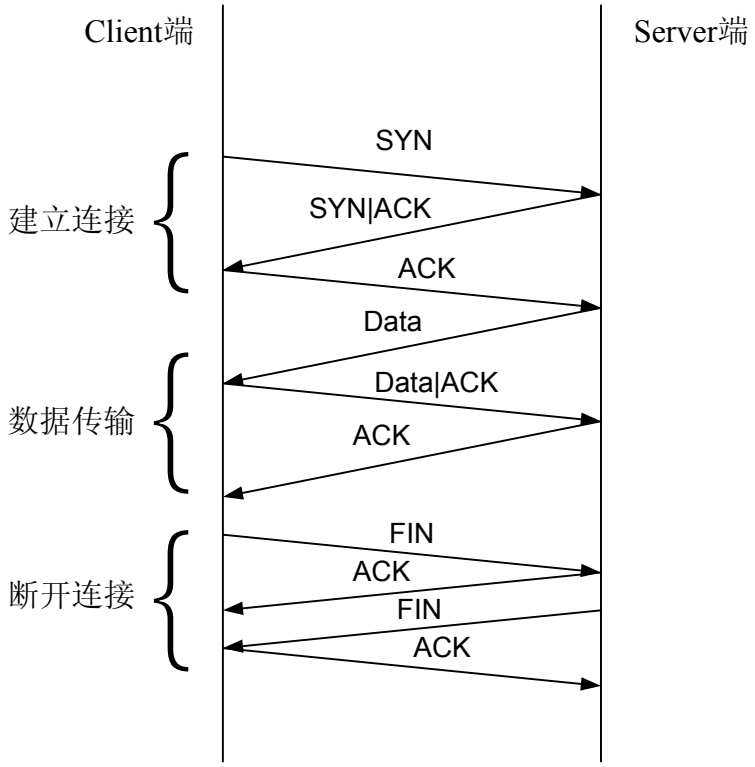
8.16 TCP6

TCP6 提供了在两个端点的进程间建立虚电路的机制，一个 TCP6 虚连接如同在系统间承载数据的全双工电路。由于 TCP6 中提供了进程间数据的可靠传输，因此被称为可靠协议，它还提供了根据当前网络状态来优化传输性能的机制。在所有数据均可收到和确认的情况下，传输速率可以逐渐增加。延时将导致发送主机在收到进一步的确认前降低发送速率。

TCP6 通常用于交互式应用，如 WEB 之类，某些数据接收差错将影响正常的工作能力。TCP6 使用了“三次握手”机制来建立虚电路，所有的虚电路都需使用“四次握手”拆除。这种连接方式可以提供多种校验和及其他可靠性功能，但是增加了使用 TCP6 的开销并导致其效率低于 UDP6。

如图 8-18 表示了 TCP6 连接建立和拆除的过程。

图 8-18 TCP6 连接建立和拆除过程示意图



8.17 UDP6

UDP6 是用来在互连网络环境中提供包交换的计算机通信协议。有如下特点：

- 只使用源和目的信息，主要用于简单的请求/响应式结构。
- 不可靠，即没有任何控制能确定 UDP6 数据报是否已被接收。
- 无连接，即在主机间传输数据时，不需要任何类型的虚电路。

UDP6 的无连接特性使得 UDP6 可以向广播地址发送数据；而 TCP6 则不同，它要求特定的源地址和目的地址。

8.18 RawIP6

RawIP6 较为简单，只填充 IPv6 首部的有限几个字段，允许应用进程提供自己的 IPv6 首部。

RawIP6 类似于 UDP6：

- 不可靠，即没有任何控制能确定 RawIP6 数据报是否已被接收。
- 无连接，即在主机间传输数据时，不需要任何类型的虚电路。

RawIP6 相比 UDP6 的区别在于，RawIP6 允许应用程序直接通过 Socket 接口操作 IP 层。对于许多需要跟下层直接交互的应用来说，非常方便。

9 SEND

关于本章

9.1 介绍

定义

安全邻居发现 SEND（SEcure Neighbor Discovery）协议是 ND（Neighbor Discovery）的增强，通过引入新的消息类型和选项字段，在地址所有权证明、消息保护和路由器授权方面提高了 ND 的安全性。

目的

由于 ND 建立在完全可信网络的基础上，其前提是假定所有节点都严格按照协议标准发送正常的 ND 消息，因此存在一定的安全威胁，常见的安全威胁有以下几种：

- NS/NA 欺骗

  攻击者发送包含虚假链路层地址的 NS/NA 消息更新被攻击者的邻居缓存，导致被攻击者将报文转发到虚假的链路层地址，类似于 IPv4 中的 ARP 欺骗。

- DAD 攻击

  攻击者通过响应所有的 DAD 消息，声称已使用被攻击者请求的地址，被攻击者将无法获取 IPv6 地址，无法与其它节点正常通信。

- 重定向攻击

  攻击者使用被攻击者的缺省网关（第一跳路由器）的链路层地址作为源地址，发送重定向报文给被攻击者，将其下一跳路由定向到一个不存在的地址，从而造成被攻击者的通信中断。

- 参数欺骗

  攻击者冒充本地路由器发送伪造的 RA 消息，消息中包含一虚假网段的地址前缀，并设置 Autonomous 标志。被攻击者将使用此地址前缀进行无状态地址自动配置，生成一个虚假网段的 IPv6 地址。当被攻击者以此地址为源地址与外界通信时，外界回应的报文将被本地路由器丢弃，导致被攻击者无法正常通信。

- 重放攻击

  攻击者截获节点发送的消息，并在一段时间后重新发送该消息，使被攻击者接收过期的消息。

通过应用 SEND 特性，可以有效地防范上述的安全威胁，提高 ND 的安全性。

受益

SEND 在 ND 的基础上引入了 CGA（Cryptographically Generated Addresses）、RSA（Rivest Shamir and Adleman）、Timestamp 和 Nonce 选项字段和 CPS（Certification Path Solicitation）、CPA（Certification Path Advertisement）两种消息类型。通过这些新的选项字段和消息类型，SEND 可以提供如下的安全增强功能：

- 地址所有权证明

  CGA 实现了 IPv6 地址和报文的绑定，避免 IPv6 地址被恶意盗用。通信双方通过生成和验证 CGA，可以防止地址欺骗，有效地抵御了 NS/NA 欺骗和 DAD 攻击。

- 消息保护

  通过 RSA 签名和验证，实现了消息完整性保护。同时，通信双方通过检查 Timestamp 和 Nonce 选项，增强了消息的时效性，有效地抵御了重放攻击。

- 路由器授权

  通过证书验证机制，实现了路由器的身份验证，防止攻击者冒充路由器发送恶意报文，有效地抵御了重定向攻击和参数欺骗。

9.2 参考标准和协议

与 SEND 特性相关的参考标准与协议如下：

- RFC2461

  Neighbor Discovery for IP Version 6 (IPv6)
- RFC2462

  IPv6 Stateless Address Autoconfiguration
- RFC3756

  IPv6 Neighbor Discovery (ND) Trust Models and Threats
- RFC3971

  SEcure Neighbor Discovery (SEND)
- RFC3972

  Cryptographically Generated Addresses (CGA)

9.3 可获得性

版本支持

产品	最低支持版本
Quidway Eudemon 8080E/8160E	V100R003

特性依赖

SEND 建立在 ND 的基础上，依赖于 ND 的正常运行。

9.4 CGA

CGA 是通过公钥结合 HASH 算法生成的一个 IPv6 地址，节点通过验证 CGA 地址，丢弃与 CGA 不符的报文，防范欺骗性攻击。结合 RSA 签名机制，还可以实现报文的完整性保护。

CGA 和 RSA 签名生成过程如下：

1. 获取 RSA 密钥对。
2. 生成 CGA 参数表，包含公钥等信息。
3. 对 CGA 参数表进行 HASH 运算，输出散列值，取后 64 位作为网络 ID。
4. 将前缀信息和网络 ID 组合，生成 CGA 地址。

5. 构造报文，源地址使用 CGA 地址，同时将 CGA 参数表填充到 CGA 选项中。然后使用私钥对报文进行签名，将签名填充到 RSA 选项中。

当节点收到带有 CGA 选项和 RSA 选项的报文后，验证过程如下：

1. 从报文的 CGA 选项中获取 CGA 参数表。
2. 对 CGA 参数表进行 HASH 运算，输出散列值，取后 64 位作为网络 ID。
3. 检查生成的网络 ID 是否与报文源地址的网络 ID 匹配。
4. 从 CGA 参数表中获取公钥，验证 RSA 签名。

生成 CGA 地址后，接口发送 ND 报文时将会遵循如下规则：

- 接口发送的 NS（不包含 DAD 消息）、NA、RA 和 Redirect 消息的源地址都将使用 CGA 地址。
- 接口发送的 NS、NA、RA 和 Redirect 消息中将会带有 CGA 选项，内容为 CGA 参数表。
- 接口发送的 NS、NA、RA 和 Redirect 消息中将会带有 RSA 选项，内容为签名。
- 接口发送的 NS、NA、RA 和 Redirect 消息中会带有 Timestamp 选项，内容为设备当前的时间。
- 接口发送的 NS 消息中会带有 Nonce 选项，内容为随机数。接口回复的 NA 消息中也会带有 Nonce 选项，内容为接口收到的 NS 消息中的 Nonce 值。

9.5 Timestamp 和 Nonce

Timestamp 指的是 ND 报文中的时间标签，主要用于非 NS/NA 消息交互过程中对重放攻击进行防范。开启 SEND 功能后，节点维护了 Delta 和 Fuzz 参数。当节点收到 ND 报文时，根据 RFC3971 中定义的公式，对报文的时效性进行检测，丢弃不附合要求的报文。

Nonce 是一个随机数，可以看作是当前会话的标签，主要用于 NS/NA 消息交互过程中对重放攻击进行防范。节点发送 NS 消息请求其他节点的链路层地址时，生成一个随机数置于 NS 消息中。接收节点在响应该请求时，回复的 NA 消息中必须带有该随机数，以表明回复的 NA 消息是针对当前的 NS 消息。

9.6 路由器授权

为了防止路由器被攻击者冒充，SEND 引入了两个新的消息类型 CPS 和 CPA，用于路由器的身份认证。

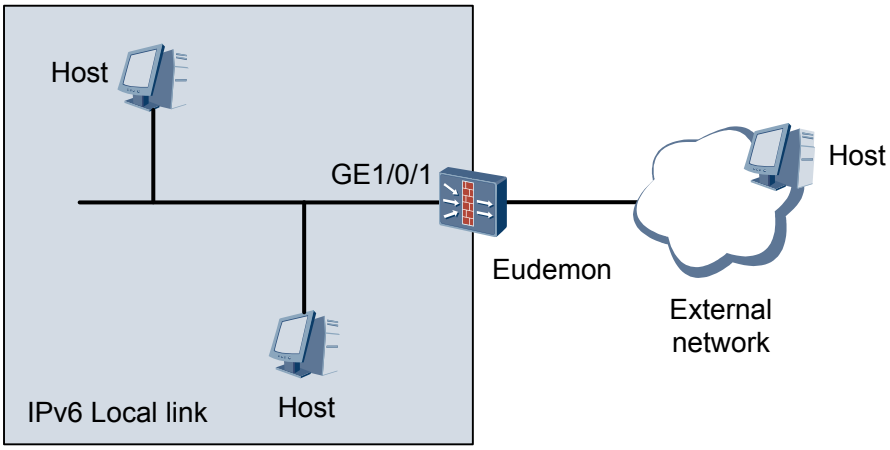
路由器必须先向 CA（Certificate Authority）服务器申请证书，证书中包含路由器的身份信息、公钥信息以及 CA 的数字签名信息。在无状态自动配置环境中，当主机收到 RA 消息后，发送 CPS 消息请求路由器的证书。路由器通过 CPA 消息发送自己的证书，响应主机的请求。主机收到 CPA 消息后，对消息中的证书进行验证，只有通过验证的路由器才会被主机作为默认路由器。

关于证书的详细介绍请参见证书部分。

9.7 应用

如图 9-1 所示，Eudemon 作为本地链路内 Host 的默认路由器，与外部网络连接。

图 9-1 SEND 应用组网图



为了防范本地链路内恶意节点针对 ND 的攻击，可以在所有节点上部署 SEND 功能，构建安全的邻居发现环境。例如，在 Eudemon 上配置如下功能：

- 配置接口 GigabitEthernet 1/0/1 生成 CGA 地址，丢弃接收到的不带有 CGA、RSA、Timestamp 和 Nonce 选项的 ND 报文，防止地址欺骗。
- 根据 RFC3971 中定义的时间戳验证机制，接口 GigabitEthernet 1/0/1 通过 **delta** 参数和 **fuzz** 参数对 ND 报文的时效性进行检测，防止重放攻击。
- 配置接口 GigabitEthernet 1/0/1 引用证书，当接口收到 Host 发送的 CPS 消息时，通过 CPA 消息发送设备的证书，响应主机的请求，防止 Eudemon 被攻击者冒充。

10 高可靠性

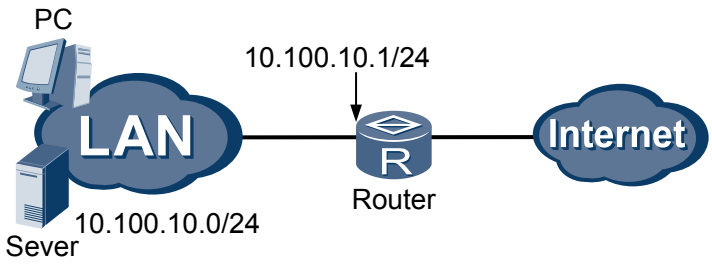
关于本章

10.1 网络可靠性要求

在当前的组网应用中，用户对网络可靠性的要求越来越高，特别是在一些重要的业务入口或接入点上需要保证网络不间断运行。对于这些重要的业务点如何保证网络的不间断传输，成为必须解决的一个问题。

传统的组网方式如图 10-1 所示，图中内部网络的主机都配置一条缺省路由，下一跳为出口路由器的接口 IP 地址 10.100.10.1。内部用户和外部用户的交互报文全部通过 Router A。如果 Router A 出现故障，内部网络中所有以 Router A 为缺省路由下一跳的主机与外部网络之间的通讯将中断，通讯可靠性无法保证。

图 10-1 采用缺省路由的组网



与路由器一样，Eudemon 作为内外网的一个接入点，高可靠性至关重要。为了防止因为一台设备出现故障而导致网络业务中断的现象，Eudemon 采用双机热备份技术，从而大大提高整个系统的稳定性和可靠性。

10.2 双机热备份概述

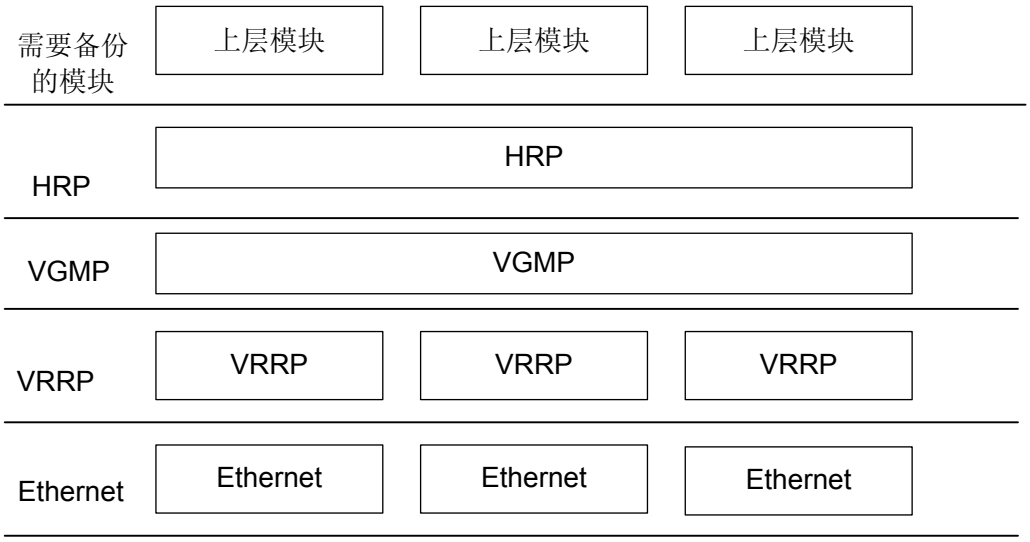
双机热备是指双机状态备份。当两台设备，在确定主用（Master）设备和备用（Backup）设备后，由主用设备进行业务的转发，而备用设备处于监控状态，同时主用设备定时向备用设备发送状态信息和需要备份的信息，当主用设备出现故障后，备用设备及时接替主用设备的业务运行。

双机热备份包含以下三种协议：

- VRRP（Virtual Router Redundancy Protocol）
  用于发现防火墙的故障情况。
- VGMP（VRRP Group Management Protocol）
  用于对 VRRP 备份组进行管理。
- HRP（Huawei Redundancy Protocol）
  用于对防火墙的动态状态数据进行实时备份。

这三个协议的体系结构如图 10-2 所示。

图 10-2 双机热备协议体系结构



10.3 VRRP 概述

10.3.1 VRRP 简介

VRRP 定义

虚拟路由器冗余协议 VRRP（Virtual Router Redundancy Protocol）作为一种容错协议，适用于支持组播或广播的局域网（如以太网等）。它将同一个广播域的一组路由器组织成一个虚拟路由器，称之为一个备份组。在同一个备份组中的所有路由器中，只有一台处于活动状态，称为主用（Master）路由器，其余都处于备用状态，称为备用（Backup）路由器。

VRRP 的工作原理

VRRP 的工作机制是把几个路由器组成一个虚拟路由器，即一个 VRRP 组，提供统一的虚拟 IP 地址和虚拟 MAC 地址，并通过优先级方式选举出主用路由器。只有主用路由器才会接收并转发以虚拟 IP 地址为下一跳的报文，备用路由器则处于监控状态，用于保证有且只有一个设备处于主用状态并转发用户报文。这样在 VRRP 组中只要有一个设备为主用状态，就可以保证链接不中断。

VRRP 状态切换原理

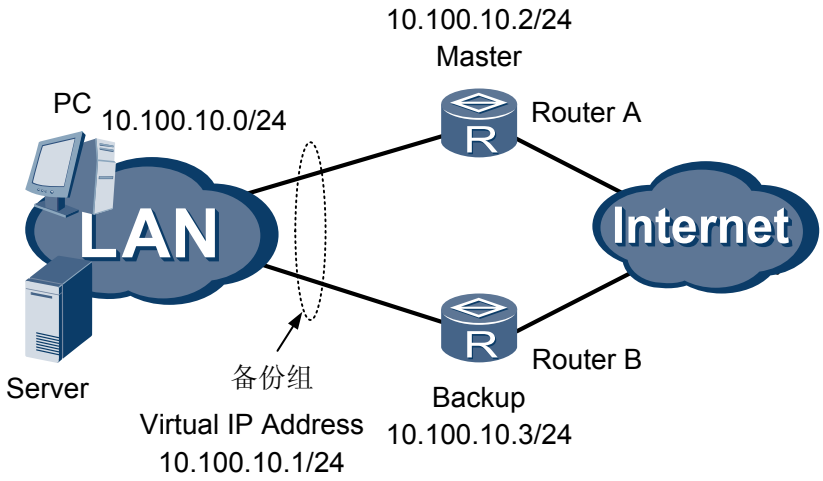
主用设备通过组播方式定期发送通告报文（HELLO 报文），备用设备则负责监听 HELLO 报文。备用设备收到主用设备发出的 HELLO 报文后会更新其监测定时器。如果备用设备在三个报文周期内收不到 VRRP HELLO 报文，它就把自己变为主用设备，自动启用备份组的虚拟 IP，同时发送虚拟 IP 的免费 ARP 报文，通知上下行设备刷新 ARP 表项，将业务流量切换到自己提供的业务端口，并转发以虚拟路由器 IP 地址作为下一跳的报文。

如果原主用设备收到另一个主用设备的 HELLO 报文，表明发生了抢占。如果 VRRP 配置为抢占方式，原主用设备收到报文时会比较报文的优先级和自己的优先级，一旦发现自己的优先级比当前报文中的 VRRP 的优先级高，则不会更新监测定时器，这样超时后便它会发送 HELLO 报文重新抢占成为主用设备。

VRRP 应用举例

如图 10-3 所示，为两台路由器组成的备份组。

图 10-3 采用 VRRP 的虚拟路由器组网



如图 10-3 所示：

- Router A、Router B 组成了一个备份组，相当于一台虚拟路由器，虚拟 IP 地址为 10.100.10.1。
- 备份组内 Router A 充当主用设备，IP 地址为 10.100.10.2。
- Router B 充当备用设备，IP 地址分别为 10.100.10.3。
- 内部网络中的所有主机仅知道该虚拟 IP 地址 10.100.10.1，而并不知道具体的主用（Master）设备或备份（Backup）设备的 IP 地址，因此各主机都将缺省路由配置为去往该虚拟 IP 地址。于是，内部网络中的各主机就通过该备份组与外部网络进行通信。
- 对于 VRRP 而言，只有主用设备能转发以虚拟 IP 地址为下一跳的报文，并定时发送 VRRP HELLO 报文。如果备用设备在连续的三个 HELLO 报文时间间隔都没有收到 HELLO 报文，则 Router B 会成为主用设备，并转发报文，从而保证业务正常运行。

10.3.2 VRRP 在 Eudemon 上的应用

Eudemon 备份的典型组网

两台 Eudemon 提供双机热备份功能时，需要在一台 Eudemon 上配置多个 VRRP 备份组，用于监视和该安全区域相连的接口的工作状态，即 Eudemon 上和每个区域相连的相关接口组成一个备份组（虚拟防火墙），并具有一个虚拟 IP 地址。

Eudemon 备份的典型组网如图 10-4 所示。

图 10-4 Eudemon 备份的典型组网

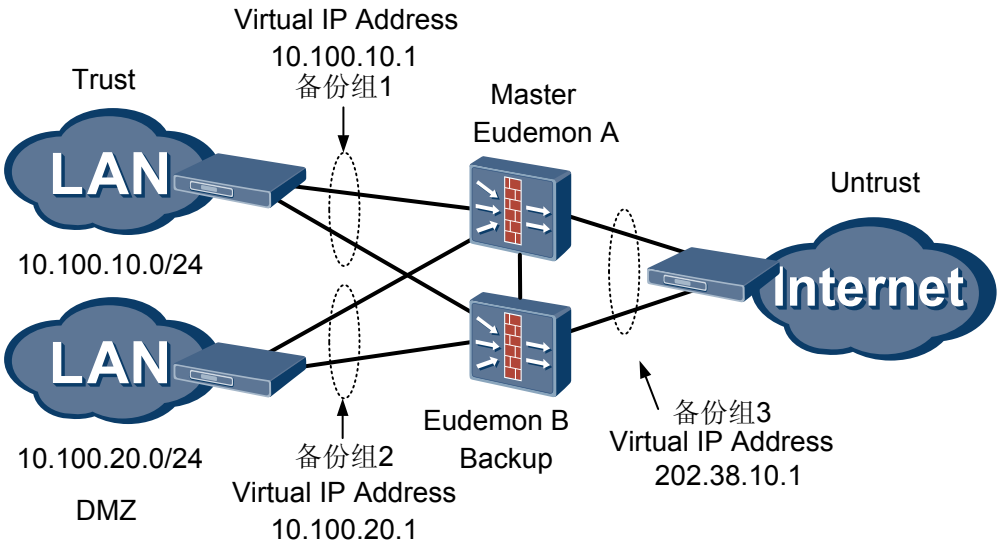


图 10-4 中：

- Eudemon A 作为主用（Master）设备，Eudemon B 作为备用（Backup）设备。
- 主用设备及备用设备上和 Trust 区域相连的接口组成备份组 1，拥有虚拟 IP 地址 10.100.10.1。
- 主用设备及备用设备上和 DMZ 区域相连的接口组成备份组 2，拥有虚拟 IP 地址 10.100.20.1。
- 主用设备及备用设备上和 Untrust 区域相连的接口组成备份组 3，拥有虚拟 IP 地址 202.38.10.1。

VRRP 应用的局限性

由于 Eudemon 是状态防火墙，只检测会话流的首包，当首包检测通过后，会在安全区域之间形成动态的会话表，后续报文（包括返回报文）只有命中该会话表才能够通过 Eudemon。这就要求某会话的进路径和出路径一致。当某会话的进路径和出路径不一致时，后续报文将无法命中会话表项，导致报文被丢弃。

Eudemon 主备备份的典型数据路径如图 10-5 所示。

图 10-5 Eudemon 主备备份的典型数据路径

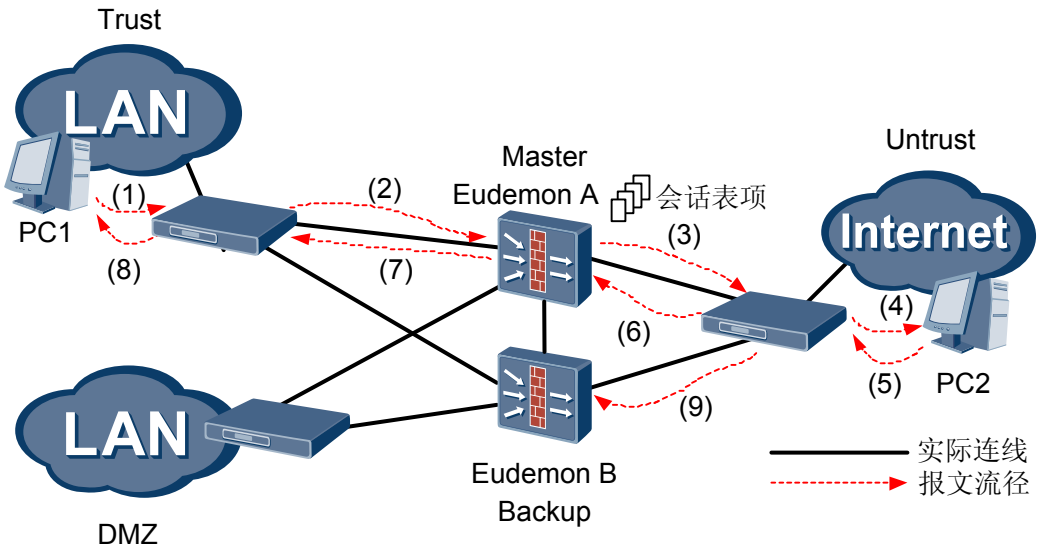


图 10-5 中，假设 Eudemon A 和 Eudemon B 的 VRRP 状态一致，即 Eudemon A 的所有接口均为主用状态，Eudemon B 的所有接口均为备用状态。

此时，Trust 区域的 PC1 访问 Untrust 区域的 PC2，报文的转发路线为(1)-(2)-(3)-(4)。Eudemon A 转发访问报文时，动态生成会话表项。当 PC2 的返回报文经过(5)-(6)到达 Eudemon A 时，由于能够命中会话表项，才能再经过(7)-(8)到达 PC1，顺利返回。

假设 Eudemon A 和 Eudemon B 的 VRRP 状态不一致，例如，当 Eudemon B 与 Trust 区域相连的接口为备用状态，但与 Untrust 区域的接口为主用状态，则 PC1 的报文通过 Eudemon A 设备到达 PC2 后，在 Eudemon A 上动态生成会话表项。PC2 的返回报文通过路线(5)-(9)返回。此时由于 Eudemon B 上没有相应数据流的会话表项，在没有其他报文过滤规则允许通过的情况下，Eudemon B 将丢弃该报文，导致会话中断。

简而言之，VRRP 状态一致意味着 Eudemon 上和各安全区域相连的若干接口状态相同，即同时处于主用状态，或同时处于备用状态。

Eudemon 连接多个安全区域，和每个安全区域相关的接口均形成一个备份组，按照传统的 VRRP 机制，VRRP 均为相对独立，且单独工作的。由此，无法保证同一防火墙上各接口的 VRRP 状态都为主用或都为备用，即传统 VRRP 方式将无法实现 Eudemon VRRP 状态的一致性。

即使 VRRP 状态一致，如果发生状态切换，主用设备上生成的会话表不会备份到备用设备上，同样会导致业务中断。

为了保证 VRRP 状态一致和主用设备会话表信息的备份，华为公司推出了 VGMP 和 HRP 两个协议。

10.4 VGMP 概述

10.4.1 VGMP 简介

VGMP 的作用

由于每个传统的 VRRP 备份组是相互独立的，无法保证其状态的一致性。为防止 VRRP 状态不一致现象的发生，华为公司在 VRRP 基础上进行了扩展，推出了 VRRP 组管理协议 VGMP（VRRP Group Management Protocol），来弥补 VRRP 在状态防火墙上使用时存在的局限。

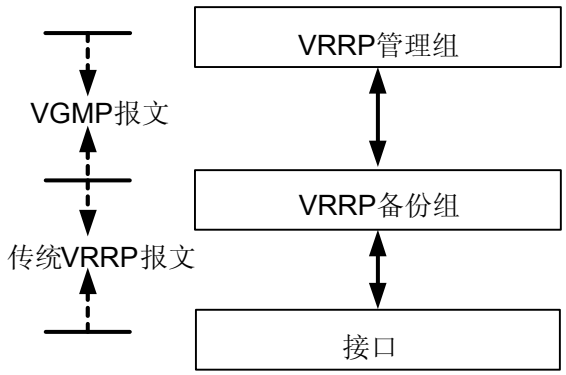
VGMP 提出 VRRP 管理组的概念，将同一台防火墙上的多个 VRRP 备份组都加入到一个 VRRP 管理组。由管理组统一管理所有 VRRP 备份组。通过统一控制各 VRRP 备份组状态的切换，来保证管理组内的所有 VRRP 备份组状态都是一致的。

VRRP 管理组和备份组的协议层次关系

VRRP 管理组相当于在 VRRP 备份组的基础上叠加了一层逻辑层。VRRP 管理组之间通过 VGMP 报文进行信息交互，VRRP 备份组和接口之间通过传统 VRRP 报文进行交互。

VRRP 管理组和备份组的协议层次关系如**图 10-6** 所示。

图 10-6 VRRP 管理组和备份组的协议层次关系



VRRP 备份组向 VRRP 管理组汇报自己的状态，并接受 VRRP 管理组的管理。例如某备份组中某一接口或相关链路出现故障，导致备份组状态发生改变，此时备份组状态可能会影响到 VRRP 管理组状态。

VRRP 管理组提供的功能

VRRP 管理组提供的功能包括：

- 状态一致性管理

  各 VRRP 备份组的主/备状态变化都需要通知其所属的 VRRP 管理组，由 VRRP 管理组决定是否允许 VRRP 备份组进行主/备状态切换。
- 抢占管理

无论 VRRP 备份组内的 Eudemon 是否开启了抢占功能，抢占行为发生与否必须由 VGMP 管理组统一决定。

10.4.2 VGMP 管理组之间的通讯

主备设备上的 VGMP 管理组依靠 VGMP 报文进行通讯，交换各自的运行状态信息，以维持主备状态的稳定，并在必要时协调主备状态的切换。

VGMP 报文是 VRRP 报文的扩展。VGMP 报文主要包括 HELLO 报文、状态切换请求报文、允许状态切换的应答报文、拒绝状态切换的应答报文。

- HELLO 报文

  与 VRRP 类似，主用设备的 VGMP 也会定期向对端发送 HELLO 报文，通知备用设备它本身的运行状态（包括优先级、VRRP 成员状态等）。与 VRRP 不同的是，备用设备收到 HELLO 报文后，会回应一个 ACK 消息，该消息中也会携带本身的优先级、VRRP 成员状态等。两台防火墙通过 HELLO 报文交互各自的状态信息。

  VGMP HELLO 报文发送周期缺省为 1 秒。当备用设备在三个 HELLO 报文周期没有收到对端发送的 HELLO 报文时，会认为对端出现故障，从而将自己切换到主用状态。

- 状态切换请求报文

  当主用设备上一个备份组成员出现故障时，VGMP 能立即感知到这个故障。此时 VGMP 会调整自己的优先级，并立即发送一个状态切换请求报文到对端。对端收到该报文后，会比较报文中的优先级和本身的优先级。如果本身优先级比报文中携带的优先级高，则会回应一个允许状态切换的应答报文（ACK），同时立即将自己切换到主用状态；发生故障的设备收到该应答报文后，会立即将自己切换到备用状态。在管理组状态切换的同时，也会强制将管理组中的所有 VRRP 备份组成员的状态一起切换。

  如果对端的优先级比报文中的优先级低，则会回应一个拒绝状态切换的应答报文（NACK）。这样两端都不会进行状态切换。

  由于 VGMP 感知到端口故障后，能立即主动发送状态切换请求报文，不再依赖于三次 HELLO 报文超时，因此大大提高了防火墙的故障响应速度。

  说明

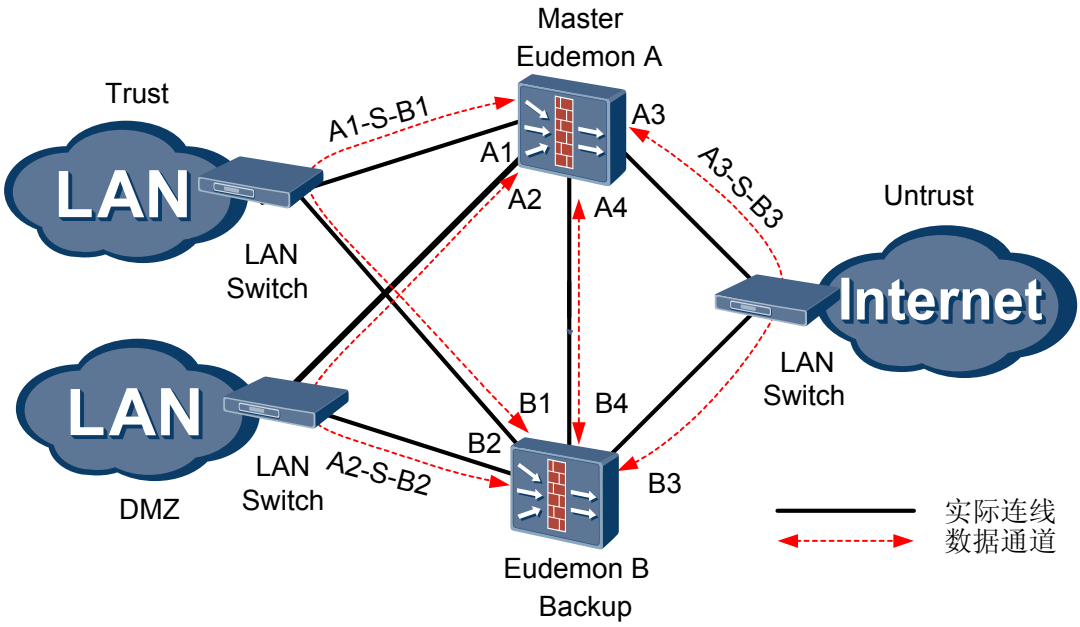
  如果是防火墙整机故障（如死机、掉电、重启等），还是只能依赖于三次 HELLO 报文超时的机制来发现故障。

10.4.3 VGMP 数据通道

两台防火墙的 VGMP 管理组之间通信的 VGMP 报文、数据备份的 HRP 报文，都是通过 VGMP 管理组中的数据通道进行传输的。数据通道是指两端防火墙的 VGMP 管理组中相对应的一对 VRRP 备份组成员。

VGMP 报文传输的数据通道如图 10-7 所示。

图 10-7 VGMP 报文传输的数据通道



A1、A2、A3、A4	Eudemon A 的接口
B1、B2、B3、B4	Eudemon B 的接口

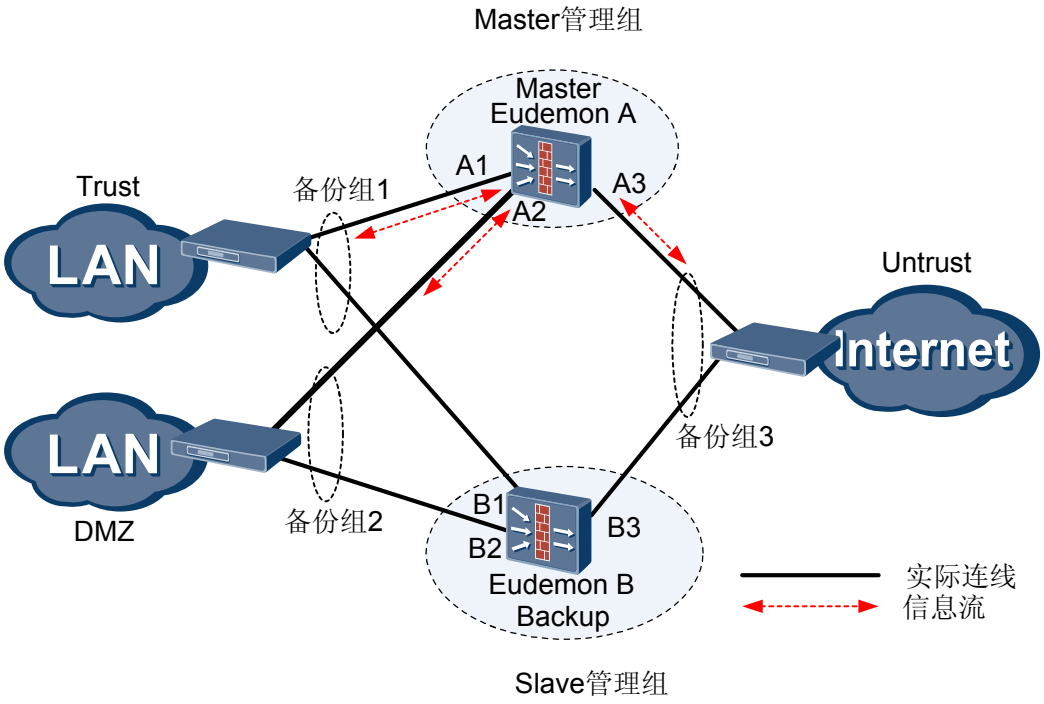
主用（Master）设备和各个安全区域相连的接口都可以作为数据通道的起始端，数据通道的终点端在备用（Backup）设备上，这样跨越 LAN Switch 形成了数据通道，假如图中 A、B 符号都表示接口，并且用 S 指代 LAN Switch，则 A1-S-B1、A2-S-B2、A3-S-B3 都可以成为数据通道。

在某些情况下，考虑到链路带宽因素，为了避免 VRRP 状态信息干扰业务流保质保量传输，可以在主用设备和备用设备之间直接连线，从而在主用设备和备用设备之间形成 A4-B4 数据通道。

10.4.4 VRRP 管理组、备份组、接口之间的关系

VRRP 管理组负责统一管理所有 VPPP 备份组。每个 Eudemon 上的管理组和备份组之间的关系如图 10-8 所示。

图 10-8 VRRP 管理组和备份组之间的关系



A1、A2、A3	Eudemon A 的接口
B1、B2、B3	Eudemon B 的接口

- 两个防火墙上各接口之间的关系

  两个防火墙上的接口和安全区域的连接必须严格对应，包括接口插槽、类型、编号、相关配置等（IP 地址除外）。这就是说 Eudemon A 上的 A1 接口必须和 Eudemon B 上的 B1 接口完全一样，例如都为以太网接口、编号都为 1/0/0、都和备份组 1 关联，以此类推。

- 两个防火墙上 VRRP 备份组之间的关系

  两个防火墙上的备份组编号、构成必须完全一样。即 Eudemon A 上的 A1 接口关联备份组 1，A2 接口关联备份组 2，A3 接口关联备份组 3；则 Eudemon B 上的 B1、B2 和 B3 接口也必须分别关联备份组 1、2 和 3。

- 两个 Eudemon 防火墙上各 VRRP 管理组之间的关系

  每个 Eudemon 上可以配置一个 Master 管理组和一个 Slave 管理组。双击热备的两个 Eudemon，一个 Eudemon 上配置的 Master 管理组可以和另一个 Eudemon 上配置的 Slave 管理组进行通信，这两个管理组的构成必须完全一样。如图 10-8 所示，在 Eudemon A 上配置了一个 Master 管理组，包括备份组 1、备份组 2 和备份组 3。在 Eudemon B 上配置了一个 Slave 管理组，包括备份组 1、备份组 2 和备份组 3。

- 同一防火墙上接口、备份组、管理组之间的关系

  同一防火墙（例如 Eudemon A）上，一个物理接口可以关联多个 VRRP 备份组。一个备份组能关联多个物理接口，对应多个虚拟 IP 地址。同一 VRRP 管理组可以包含多个备份组，但是相同备份组不能同时隶属于 Master 管理组和 Slave 管理组。

10.4.5 备份方式分类

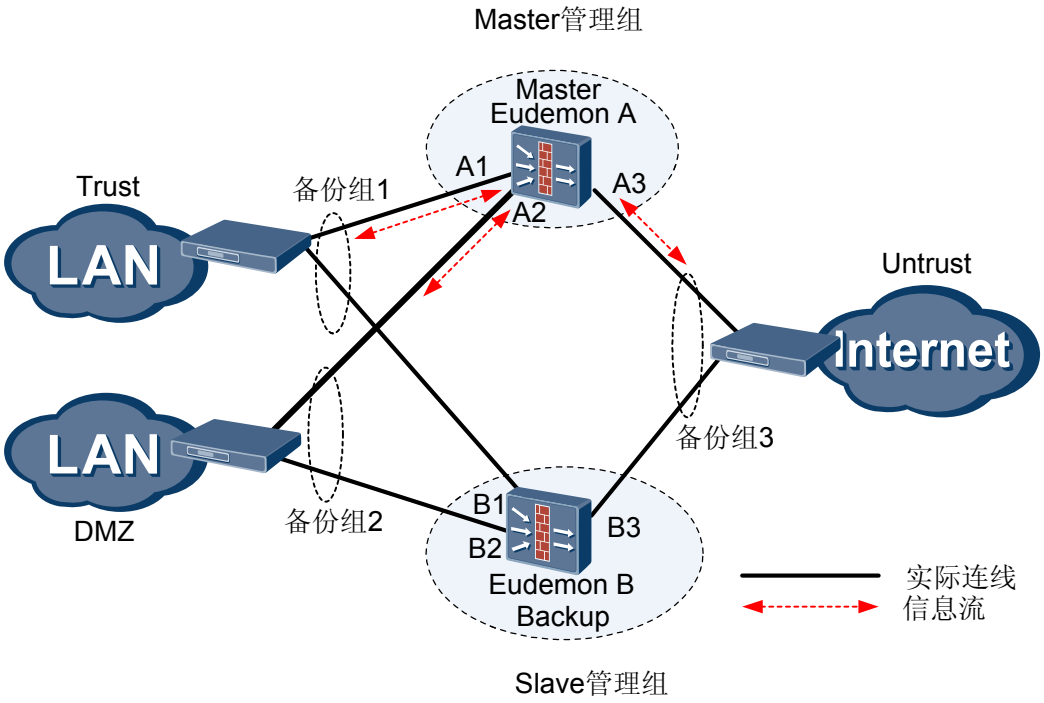
概述

通过接口、备份组、管理组之间的不同组合，可以实现两台 Eudemon 主备备份、负载分担等方式。

主备备份

借助 VGMP 机制，可以实现主备备份。如图 10-9 所示，在 Eudemon A 上配置一个 Master 管理组，在 Eudemon B 上配置一个 Slave 管理组。

图 10-9 主备备份组网



A1、A2、A3	Eudemon A 的接口
B1、B2、B3	Eudemon B 的接口

图 10-9 中备份组关系如下：

- 备份组 1 包括 Eudemon A 的 A1 接口、Eudemon B 的 B1 接口。
- 备份组 2 包括 Eudemon A 的 A2 接口、Eudemon B 的 B2 接口。
- 备份组 3 包括 Eudemon A 的 A3 接口、Eudemon B 的 B3 接口。

图 10-9 中管理组关系如下：

- 配置 Eudemon A 的 VGMP 管理组为 Master 管理组，包含备份组 1、2、3，优先级为 Level1（45001+单板优先级）。
- 配置 Eudemon B 的 VGMP 管理组为 Slave 管理组，包含备份组 1、2、3，优先级为 Level2（45000+单板优先级）。

说明

单板优先级为 1000 ×（业务板个数 + 接口板个数）。若当前总共有 n 块业务板和接口板可用，则 Master 管理组优先级为 45001+n × 1000；Slave 管理组优先级为 45000+n × 1000。

由于 Level1>Level2，所以 Eudemon A 作为主用防火墙，Eudemon B 作为备用防火墙。

主备备份方式下各设备的状态如表 10-1 所示。

表 10-1 主备备份方式下各设备的状态

防火墙设备	管理组	成员	优先级	状态	会话量
A	Master	备份组 1，2，3	Level1	主用	全部
B	Slave	备份组 1，2，3	Level2	备用	0

Trust、DMZ 和 Untrust 区域内的主机将业务数据分别发送到 Eudemon A 的 A1、A2 和 A3 接口，由该防火墙承担全部会话业务。

当 Eudemon A 出现故障或相关链路故障时，状态发生切换，Eudemon B 由备用转变为主用，并开始承担全部会话业务。

负载分担

所谓负载分担，也可以称为“互为主备”。构成备份机制的两台防火墙同时处理业务，当其中一台防火墙发生故障时，另外一台防火墙会立即承担其业务，保证原来需要通过这台防火墙的业务不中断。

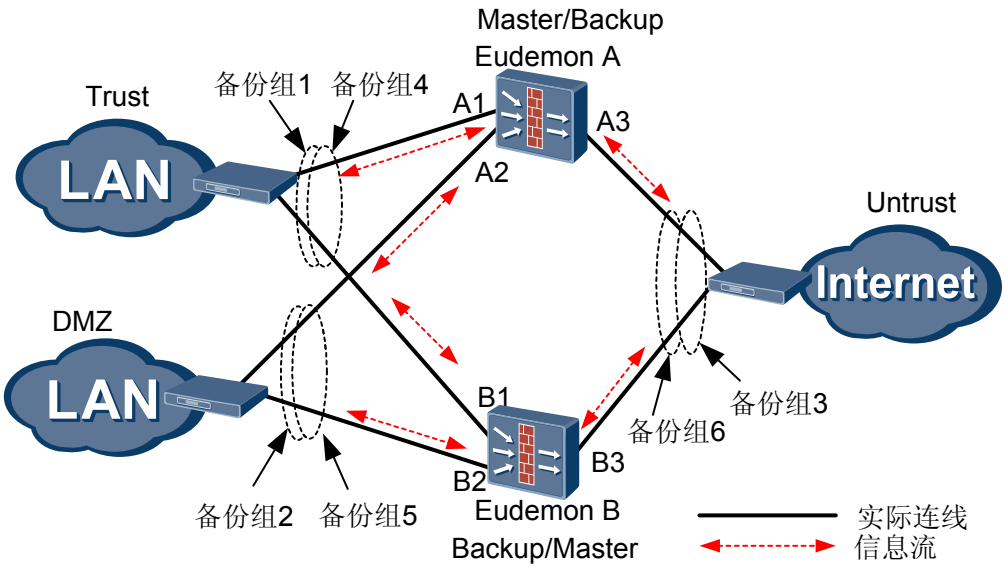
由于两台防火墙互为主备，负载分担机制实际上相当于同时运行两套主备备份机制，也就是每个防火墙上存在两个 VGMP 管理组。Eudemon A 的 Master 管理组和 Eudemon B 的 Slave 管理组构成一套主备备份机制；Eudemon A 的 Slave 管理组和 Eudemon B 的 Master 管理组构成一套主备备份机制。

负载分担分为以下两种：

- 简化的负载分担

  每个 Eudemon 上分别配置 Master 和 Slave 两个 VGMP 管理组，具有不同的优先级，如图 10-10 所示。

图 10-10 简化负载分担组网图



A1、A2、A3	Eudemon A 的接口
B1、B2、B3	Eudemon B 的接口

图 10-10 所示的组网中存在的备份组如下：

- 备份组 1、4 包括 Eudemon A 的 A1 接口、Eudemon B 的 B1 接口。
- 备份组 2、5 包括 Eudemon A 的 A2 接口、Eudemon B 的 B2 接口。
- 备份组 3、6 包括 Eudemon A 的 A3 接口、Eudemon B 的 B3 接口。

Eudemon A 的 VGMP 管理组如下：

- Eudemon A 的 Master 管理组包含备份组 1、2、3，优先级为 Level1（45001+单板优先级）。
- Eudemon A 的 Slave 管理组包含备份组 4、5、6，优先级为 Level2（45000+单板优先级）。

Eudemon B 的 VGMP 管理组如下：

- Eudemon B 的 Slave 管理组包括备份组 1、2、3，优先级为 Level3（45000 ＋单板优先级）。
- Eudemon B 的 Master 管理组包含备份组 4、5、6，优先级为 Level4（45001 ＋单板优先级）。

其中，Eudemon A 和 Eudemon B 的管理组优先级关系如下：

- Level1>Level3。
- Level2<Level4。

由两台防火墙的两个 VGMP 管理组分别协商，使得两台防火墙都是主用设备又同时都为备用设备：

- Eudemon A 的 Master 管理组与 Eudemon B 的 Slave 管理组协商，得出 Eudemon A 为主用，Eudemon B 为备用。
- Eudemon B 的 Master 管理组与 Eudemon A 的 Slave 管理组协商，得出 Eudemon B 为主用，Eudemon A 为备用。

两台防火墙都正常工作情况下，各设备的状态如表 10-2 所示。

表 10-2 简化负载分担方式下各设备的状态（1）

防火墙设备	管理组	备份组	优先级	状态	会话量
A	Master	备份组 1，2，3	Level1	主用	部分
	Slave	备份组 4，5，6	Level2	备用	0
B	Slave	备份组 1，2，3	Level3	备用	0
	Master	备份组 4，5，6	Level4	主用	部分

由于 Eudemon A 和 Eudemon B 的两个 VGMP 管理组的优先级存在交叉关系，即上文所说的 Level1>Level3、Level2<Level4，所以 Trust、DMZ 和 Untrust 区域内的主机将业务数据分别发送到 Eudemon A 的 A1、A2 和 A3 接口，另一部分会话业务发送到 Eudemon B 的 B1、B2 和 B3 接口，由两台防火墙共同分担话务量。

如果 Eudemon B 出现故障，则 VGMP 管理组将重新裁决各设备的状态，Eudemon A 状态切换为主用，Eudemon B 状态切换为备用。此时 Eudemon A 承担全部会话业务。各设备的状态则变为如表 10-3 所示。

表 10-3 简化负载分担方式下各设备的状态（2）

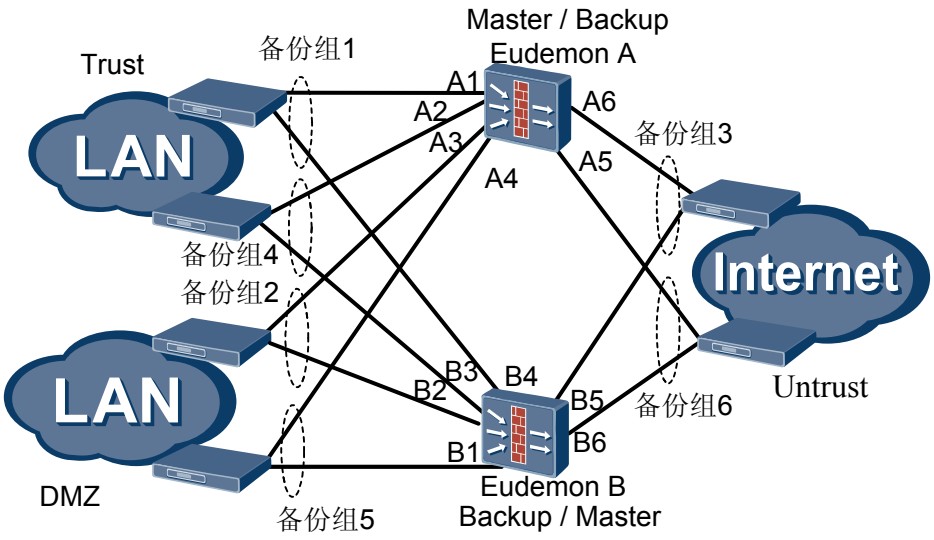
防火墙设备	管理组	备份组	优先级	状态	会话量
A	Master	备份组 1，2，3	Level1	主用	部分
	Slave	备份组 4，5，6	Level2	主用	部分
B	Slave	备份组 1，2，3	Level3	备用	0
	Master	备份组 4，5，6	Level4	备用	0

当 Eudemon B 恢复正常后，Eudemon B 将继续成为主用设备，流量将在两个防火墙之间负载分担。

- 复杂的负载分担

  当 Eudemon 的接口速率难以顺畅传输高速业务流时，为了保证一条物理线路上传输顺畅，建议为 Eudemon 添加新接口，并基于新接口配置用于负载分担的备份组。如图 10-11 所示。

图 10-11 复杂负载分担组网图



A1、A2、A3、A4、A5、A6	Eudemon A 的接口
B1、B2、B3、B4、B5、B6	Eudemon B 的接口

原有备份组为备份组 1、2 和 3，各备份组的情况如下：

- 备份组 1 包括 Eudemon A 的 A1 接口、Eudemon B 的 B4 接口。
- 备份组 2 包括 Eudemon A 的 A3 接口、Eudemon B 的 B2 接口。

- 备份组 3 包括 Eudemon A 的 A6 接口、Eudemon B 的 B5 接口。

添加三个新的备份组 4、5 和 6，各备份组的情况如下：

- 备份组 4 包括 Eudemon A 的 A2 接口、Eudemon B 的 B3 接口。
- 备份组 5 包括 Eudemon A 的 A4 接口、Eudemon B 的 B1 接口。
- 备份组 6 包括 Eudemon A 的 A5 接口、Eudemon B 的 B6 接口。

Eudemon A 和 Eudemon B 的 VGMP 管理组构成的关系如下：

- Eudemon A 的 Master 管理组和 Eudemon B 的 Slave 管理组包含备份组 1、2 和 3。
- Eudemon A 的 Slave 管理组和 Eudemon B 的 Master 管理组包含备份组 4、5 和 6。

Eudemon A 的 Master 管理组与 Eudemon B 的 Slave 管理组协商，得出 Eudemon A 为主用设备，Eudemon B 为备用设备。

Eudemon B 的 Master 管理组与 Eudemon A 的 Slave 管理组协商，得出 Eudemon B 为主用设备，Eudemon A 为备用设备。

10.5 HRP 概述

10.5.1 HRP 简介

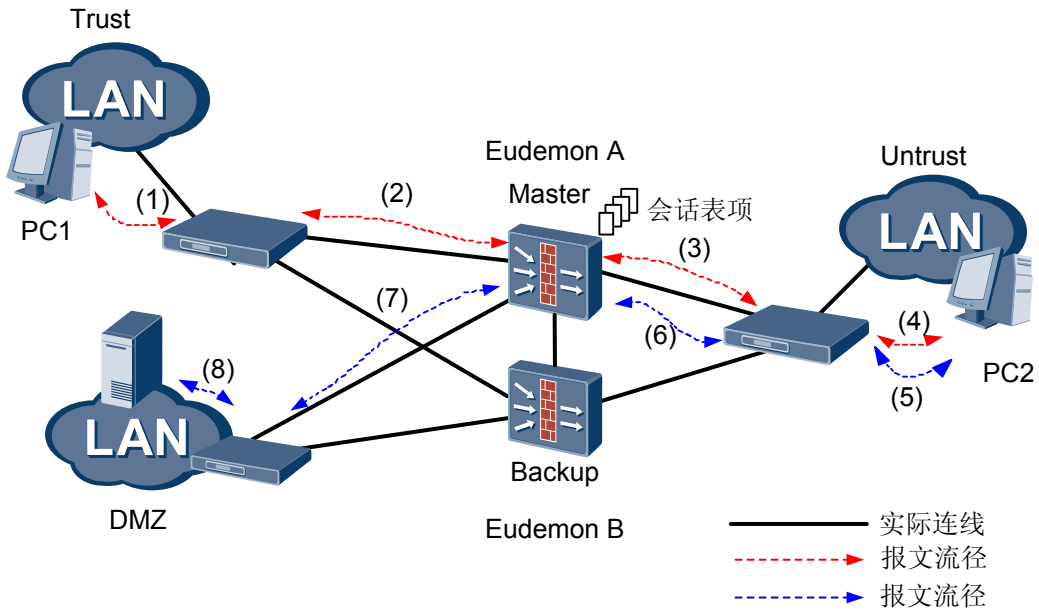
HRP 的定义

华为公司冗余协议 HRP（Huawei Redundancy Protocol）是承载在 VGMP 报文上进行传输的。HRP 用于在主用设备和备用设备之间备份关键配置命令和会话表状态信息。

HRP 的作用

图 10-12 是 Eudemon 双机热备的基本组网图。

图 10-12 Eudemon 双机热备的基本组网



由于 Eudemon 是状态防火墙，对于每一个动态生成的会话连接，Eudemon 上都有一个会话表项与之对应。

如果主用（Master）设备 Eudemon A 出现故障或相关链路出现问题，备用（Backup）设备 Eudemon B 将会切换状态而变成新的主用设备，并且开始承担传输任务。如果状态切换前，会话表项和配置命令没有备份到 Eudemon B，则先前经过 Eudemon A 的所有会话都会因为无法命中 Eudemon B 的会话表而断链，导致业务中断。这种 Eudemon 设备的状态切换是失败的。

为了实现主用设备出现故障时能由备用设备平滑地接替工作，需要在主用设备和备用设备之间备份关键配置命令和会话表状态信息，这就是 HRP 协议的重要作用。

10.5.2 配置命令和状态信息的备份

目前，Eudemon 防火墙的双机热备份功能支持配置命令和连接状态信息的备份，可以通过自动备份、手工批量备份和快速备份三种方式实现。

备份内容

防火墙备份的内容包括：

- 状态信息

  防火墙备份的状态信息包括以下方面。

  - 防火墙生成的会话表表项
  - 源 IP 监控表
  - 接口板动态 ARP（Address Resolution Protocol）表项
  - Servermap 表项，包括使用 QQ，MSN，STUN（Simple Traversal of UDP Through Network Address Translators）协议、NAT Server、NO-PAT 地址分配表项、快速备份时的 ASPF 生成的 Servermap 表项

- IPSec 隧道状态
- 配置命令

  防火墙备份的配置命令包括以下方面。

  - ACL（Access Control List）包过滤命令
  - 攻击防范命令
  - 黑名单命令

    包括黑名单的启动命令、手工添加黑名单表项命令。
  - 日志命令
  - NAT 命令

    包括 NAT 地址池、NatServer、以及 NAT 在域间应用的命令。
  - 区域命令

    包括创建安全区域，设置区域优先级，接口加入安全区域以及域间配置命令。
  - ASPF 命令
  - AAA 命令
  - IPSec 配置命令
  - 清除会话表项的命令
  - 清除配置的命令

备份方向

状态信息是从管理组中的主用设备备份到备用设备。如果进行负载分担双机热备份的两台防火墙分别是两个管理组的主用，则连接状态会互相备份，由系统决定需要备份的连接状态信息的内容。

配置命令则只能进行单向备份。即备份方向只能从配置主设备到配置从设备，不能反向备份。

说明

配置主设备和配置从设备将在 **10.5.3 配置设备的主从划分**一节中详细介绍。

自动备份

下面分别针对配置命令的备份和连接状态信息的备份两方面进行说明。

- 配置命令的备份

  在防火墙运行过程中，当主用设备识别到启动双机热备份的命令时，主用设备自动将配置命令备份到备用设备，从而实现备用设备运行这些配置命令。

  在主用设备、备用设备都正常工作的情况下，如果启动自动实时备份功能，则在主用设备上每输入一条双机热备份需要的命令时，此配置命令将被传送到备用设备并执行；如果在主用设备上输入双机热备份不需要的命令，则该命令仅在主用设备上执行，不会被传送到备用设备。对于在备用设备上执行的命令，不会被传送到主用设备。当备用设备未工作或工作异常时，自动备份无法进行。
- 连接状态信息的备份

  在防火墙运行过程中，当主用设备上产生了需要备份的连接状态信息时，主用设备自动将连接状态信息备份到备用设备，并由备用设备进行状态处理。

手工批量备份

手工批量备份包括：

- 配置命令的备份

  当主用设备、备用设备都正常工作时，且主用设备上启动手工批量同步备份功能，则主用设备将双机热备份需要的配置命令批量发送到备用设备，从而实现备用设备执行这些配置命令。当备用设备未工作或工作异常时，手工批量备份无法进行。

- 连接状态信息的备份

  当主用设备、备用设备都正常工作时，且主用设备上启动手工批量同步备份功能，则主用设备将双机热备份需要的连接状态信息批量发送到备用设备，并由备用设备进行状态更新。当备用设备未工作或工作异常时，手工批量备份无法进行。

快速备份

当防火墙工作于双机热备份组网环境下，如果报文的来回路径不一致，主用设备的信息没有备份到备用设备，备用设备会将到达的报文丢弃。

为防止上述现象发生，可以通过快速备份会话，将主用设备的相应的会话表项快速备份到备用设备，使返回报文在备用设备上能够查找到会话表项，从而能够通过备用设备，保证内外部用户的会话不中断。

检查主备设备配置一致性

配置命令和连接状态信息备份完之后，需要检查主备设备配置的一致性。当防火墙工作于双机热备份组网环境下，如果主备设备的配置不匹配，主用设备出现故障后，报文被备用设备丢弃，从而导致内外部用户的会话无法通过备用设备而中断。

在这种情况下，需要检查主备设备配置的一致性。当发现配置不一致时，即可进行相应修改。

10.5.3 配置设备的主从划分

说明

配置设备的主从划分仅是在负载分担方式下引入的概念，主备备份方式下不涉及配置设备主从划分。

当采用负载分担方式时，网络中存在两台主用设备，用户可能在两台主用设备上输入了很多命令。当其中一台主用设备出现故障时，如何在这两台防火墙之间备份信息、需要备份哪些命令以及备份方向如何都是需要考虑的问题。

为了避免备份时混乱，Eudemon 中引入了配置主设备、配置从设备概念。发送配置备份内容的防火墙被称为配置主设备，接收配置备份内容的防火墙称为配置从设备。判断一台防火墙是否是配置主设备，需要遵循如下原则：

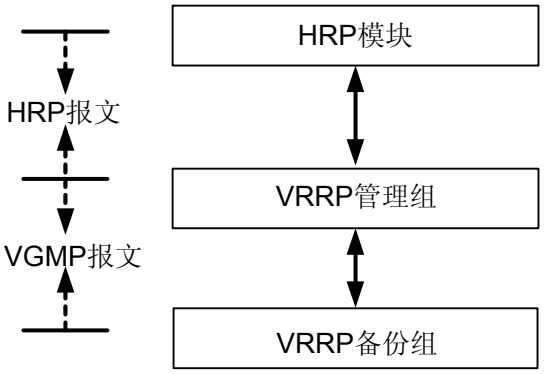
- 只有 VRRP 管理组中状态为主用的设备才有机会成为配置主设备。
- 在负载分担方式下，参与双机热备份的两台 Eudemon 都是主用设备，此时则按照接口真实 IP 地址从大到小的顺序选择配置主设备。

除非配置主设备出现故障或者退出 VRRP 备份组，否则配置主设备、从设备之间不进行转换，从而尽力保证了配置主设备的稳定性。

10.5.4 VRRP 管理组、备份组和 HRP 之间的协议层次关系

VRRP 备份组、管理组和 HRP 之间的协议层次关系如**图 10-13** 所示。

图 10-13 VRRP 备份组、管理组和 HRP 之间的协议层次关系



当 VRRP 备份组状态变化时，由 VRRP 管理组来决定其本身的状态是否需要变化。

当 VRRP 管理组状态变化时，系统将通知 HRP 状态和配置主/从设备的状态发生相应的变化，从而确保两台防火墙之间配置命令和会话状态信息得到及时备份。

10.6 BFD

10.6.1 介绍

定义

双向转发检测 BFD（Bidirectional Forwarding Detection）用于快速检测系统之间的通信故障，并在出现故障时通知上层应用。

可以把 BFD 看作是系统提供的一种服务：

- 上层应用向 BFD 提供检测地址、检测时间等参数。
- BFD 根据这些信息创建、删除或修改 BFD 会话，并把会话状态通告给上层应用。

上层应用对 BFD 会话状态变更采取什么措施完全由上层应用自己决定。

目的

为了减小设备故障对业务的影响，提高网络的可用性，网络设备需要能够尽快检测到与相邻设备间的通信故障，以便及时采取措施，保证业务继续进行。

现有的故障检测机制主要包括：

- 硬件检测：例如通过 SDH（Synchronous Digital Hierarchy）告警检测链路故障。硬件检测的优点是可以很快发现故障，但并不是所有介质都能提供硬件检测。
- 慢 Hello 机制：通常是指路由协议的 Hello 机制，这种机制检测到故障所需时间为秒级。对于高速数据传输，例如吉比特速率级，超过 1 秒的检测时间将导致大量数据丢失；对于时延敏感的业务，例如语音业务，超过 1 秒的延迟也是不能接受的。
- 其他检测机制：不同的协议或设备制造商有时会提供专用的检测机制，但在系统间互联互通时，这样的专用检测机制通常难以部署。

BFD 就是为解决现有检测机制的不足而产生的，其目标如下：

- 为相邻转发引擎之间的通道提供轻负荷的、快速的故障检测。这些故障包括接口、数据链路、甚至有可能是转发引擎本身的故障。
- 提供一个单一的机制，能够对所有类型的介质、协议进行检测，实现全网统一的检测机制。

10.6.2 规格

BFD 特性的相关规格如下：

- Eudemon 单板支持创建的 BFD 会话最大个数为 512 个。
- Eudemon 整机支持创建的 BFD 会话最大个数为 8192 个。

10.6.3 参考标准和协议

与 BFD 特性相关的参考标准与协议如下：

- draft-ietf-bfd-base-08
  Bidirectional Forwarding Detection
- draft-ietf-bfd-generic-04
  Generic Application of BFD
- draft-ietf-bfd-multihop-06
  BFD for Multihop Paths
- draft-ietf-bfd-v4v6-1hop-08
  BFD for IPv4 and IPv6 (Single Hop)

10.6.4 可获得性

版本支持

产品	最低支持版本
Quidway Eudemon 8080E/8160E	V100R003

特性依赖

无

10.6.5 BFD 机制

BFD 检测机制

BFD 的检测机制是两个系统建立 BFD 会话，并沿它们之间的路径周期性发送 BFD 控制报文，如果一方在规定的时间内没有收到 BFD 控制报文，则认为路径上发生了故障。

BFD 控制报文封装在 UDP 报文中传送。会话开始阶段，双方系统通过控制报文中携带的参数（会话标识符、期望的收发报文最小时间间隔、本端 BFD 会话状态等）进行协商。协商成功后，以协商的报文收发时间为事件间隔在彼此之间的路径上定时发送 BFD 控制报文。

说明

为满足快速检测的需求，BFD 草案规定发送间隔和接收间隔的时间单位是微秒。但限于目前的设备处理能力，大部分厂商的设备配置 BFD 时只能达到毫秒级，在进行内部处理时再转换到微秒。Eudemon 支持的最小检测时间为 30 毫秒。

BFD 提供两种检测模式：

- 异步模式：异步模式是 BFD 的主要操作模式。在这种模式下，BFD 会话建立起来后，两个系统之间相互周期性地发送 BFD 控制报文，如果某个系统在检测时间内没有收到对端发来的报文，就认为此 BFD 会话的状态是 Down。
- 查询模式：查询模式是 BFD 的第二种操作模式。当一个系统中存在大量 BFD 会话时，为防止周期性发送 BFD 控制报文的开销影响到系统的正常运行，可以采用查询模式。在查询模式下，一旦 BFD 会话建立，系统就不再周期性发送 BFD 控制报文，而是通过其他与 BFD 无关的机制检测连通性（比如路由协议的 Hello 机制、硬件检测机制等），从而减少 BFD 会话带来的开销。

两种模式的一个辅助功能是回声功能。当回声功能激活时，一个 BFD 控制报文按照如下方式发送：本地发送一个 BFD 控制报文，远端系统通过它的转发通道将它们环回回来。如果连续几个回声包都没有接收到，会话状态就被宣布为“Down”。回声功能可以与异步模式或者查询模式一起使用。

目前 Eudemon 只支持异步模式，不支持查询模式和回声功能。

BFD 会话状态

BFD 会话有四种状态：Down、Init、Up 和 AdminDown。

- Down：会话处于 Down 状态或刚刚创建。
- Init：已经能够与对端系统通信，本端希望使会话进入 Up 状态。
- Up：会话已经建立成功。
- AdminDown：会话处于管理性 Down 状态。

会话状态通过 BFD 控制报文的 State 字段传递，系统根据自己本地的会话状态和接收到的对端会话状态驱动状态改变。

BFD 会话的建立方式

BFD 会话的建立有两种方式，即静态配置 BFD 会话和动态建立 BFD 会话。

BFD 通过控制报文中的 My Discriminator 和 Your Discriminator 区分不同的会话。静态和动态创建 BFD 会话的主要区别在于 My Discriminator 和 Your Discriminator 的配置方式不同。

- 静态配置 BFD 会话

  静态配置 BFD 会话是指通过命令行手工配置 BFD 会话参数，包括了配置本地标识符和远端标识符等，然后手工下发 BFD 会话建立请求。

- 动态建立 BFD 会话

  动态建立 BFD 会话时，系统对本地标识符和远端标识符的处理方式如下：

  - 动态分配本地标识符

    当应用程序触发动态创建 BFD 会话时，系统分配属于动态会话标识符区域的值作为 BFD 会话的本地标识符。然后向对端发送 Your Discriminator 的值为 0 的 BFD 控制报文，进行会话协商。

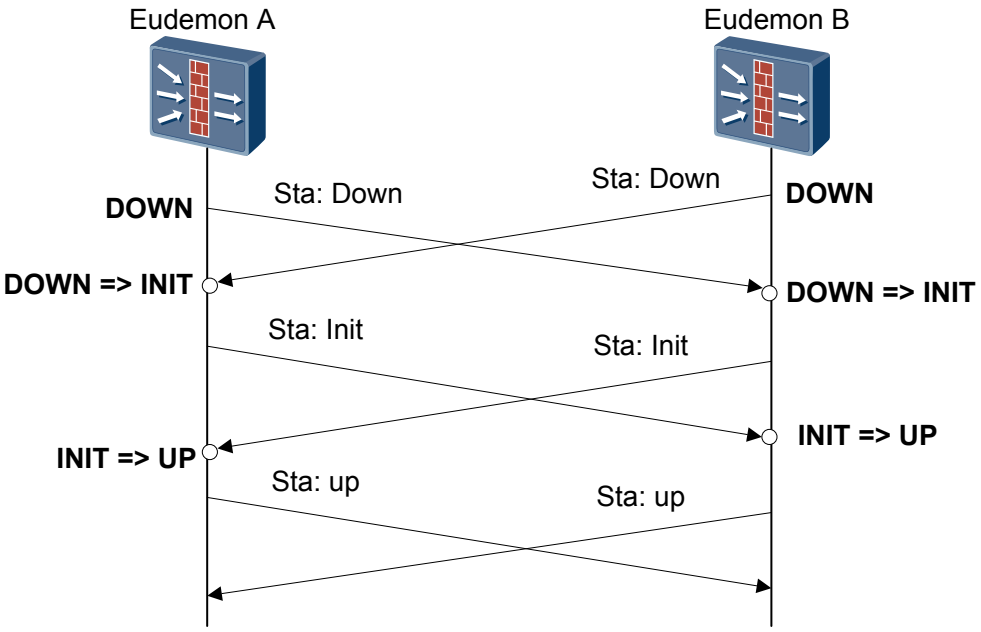
  - 自学习远端标识符

    当 BFD 会话的一端收到 Your Discriminator 的值为 0 的 BFD 控制报文时，判断该报文是否与本地 BFD 会话匹配，如果匹配，则学习接收到的 BFD 报文中 My Discriminator 的值，获取远端标识符。

BFD 会话的建立过程

BFD 状态机的建立和拆除都采用三次握手机制，以确保两端系统都能知道状态的变化。图 10-14 以 BFD 会话建立为例，简单介绍状态机的迁移过程。

图 10-14 BFD 会话连接建立



1. Eudemon A 和 Eudemon B 各自启动 BFD 状态机，初始状态为 Down，发送状态为 Down 的 BFD 报文。对于静态配置 BFD 会话，报文中的 Your Discriminator 的值是用户指定的；对于动态创建 BFD 会话，Your Discriminator 的值是 0。
2. Eudemon B 收到状态为 Down 的 BFD 报文后，状态切换至 Init，并发送状态为 Init 的 BFD 报文。
3. Eudemon B 本地 BFD 状态为 Init 后，不再处理接收到的状态为 Down 的报文。
4. Eudemon A 的 BFD 状态变化同 Eudemon B。
5. Eudemon B 收到状态为 Init 的 BFD 报文后，本地状态切换至 Up。
6. Eudemon A 的 BFD 状态变化同 Eudemon B。

Eudemon A 和 Eudemon B 发生“DOWN => INIT”的状态迁移后，会启动一个超时定时器。如果定时器超时仍未收到状态为 Init 或 Up 的 BFD 报文，则本地状态自动切换回 Down。

10.6.6 BFD for IP

在 IP 链路上建立 BFD 会话，利用 BFD 检测机制快速检测故障。

BFD for IP 支持单跳检测和多跳检测：

- BFD 单跳检测是指对两个直连系统进行 IP 连通性检测，这里所说的“单跳”是 IP 的一跳。在进行 BFD 单跳检测的两个系统中，对于一种给定的数据协议，在指定接口上只存在一个 BFD 会话。
- BFD 多跳检测是指 BFD 可以检测两个系统间的任意路径，这些路径可能跨越很多跳，也可能在某些部分发生重叠。

组网应用

典型应用一：

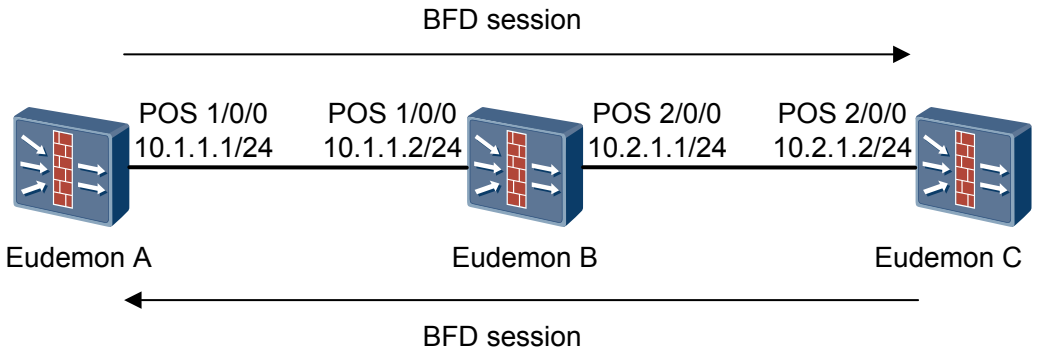
如图 10-15 所示，BFD 检测两台设备之间的单跳路径，BFD 会话绑定出接口。

图 10-15 单跳 BFD for IP

典型应用二：

如图 10-16 所示，BFD 检测 Eudemon A 和 Eudemon C 之间的多跳路径，BFD 会话绑定对端 IP 但不绑定出接口。

图 10-16 多跳 BFD for IP



10.6.7 应用

BFD for HRP

在双机热备份组网环境下，当 Eudemon 的上下行链路发生故障时，需要进行 HRP 主备状态的切换，以确保业务正常进行。

通过配置 BFD，可以快速检测到 Eudemon 上下行链路的故障，也可以快速检测与 Eudemon 不直接相连的链路的故障。

BFD for HRP 就是通过配置 HRP 绑定 BFD，在 BFD 会话快速检测到链路 DOWN 时，立即降低 Eudemon 上 VGMP 管理组对应的优先级，从而触发 HRP 主备状态的快速切换。链路状态恢复正常时,被绑定的 BFD 能够检测到链路状态的变化，恢复 Eudemon 上 VGMP 管理组的优先级。

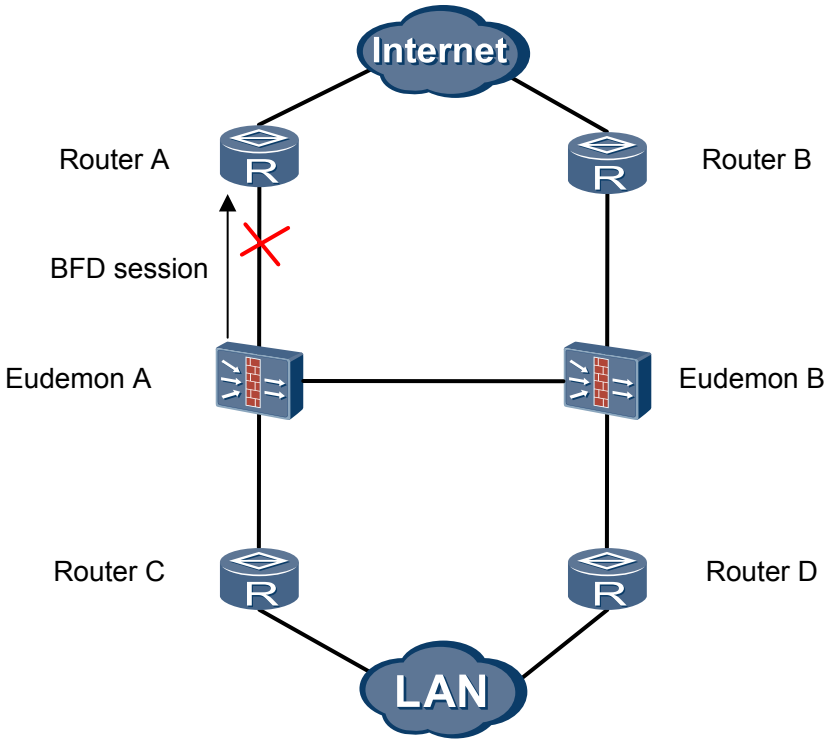
说明

当 VGMP 管理组绑定的 BFD 会话 DOWN 时，对应的 VGMP 管理组的优先级减 2。HRP 主备状态是否切换是根据 VGMP 管理组的优先级计算规则来统一管理的。

组网应用

如图 10-17 所示，Eudemon A 和 Eudemon B 工作在双机热备环境下，正常情况下，Eudemon A 的 HRP 状态为主，Eudemon B 的 HRP 状态为备，业务流量通过 Eudemon A 进行转发。在 Eudemon A 上配置 BFD 会话来检测 Eudemon A 到 Router A 的链路，Eudemon A 上的 VGMP 管理组绑定 BFD 会话。当 Eudemon A 到 Router A 的链路发生故障时，BFD 会话检测到链路 DOWN，会立即降低 Eudemon A 上 VGMP 管理组的优先级，从而触发 HRP 主备状态的快速切换。切换后 Eudemon A 的 HRP 状态为备，Eudemon B 的 HRP 状态为主，业务流量通过 Eudemon B 进行转发。

图 10-17 BFD for HRP 组网图



BFD for USR

BFD for USR（Unicast Static Route）用于支持 IPv4 单播静态路由，支持 IPv4 单播静态路由绑定后快速感知链路状态。

与动态路由协议不同，单播静态路由自身没有检测机制，当网络发生故障的时候，需要管理员介入。BFD for USR 特性可为公网 IPv4 单播静态路由绑定 BFD 会话，利用 BFD 会话来检测单播静态路由所在链路的状态。

BFD for USR 可为每条 IPv4 单播静态路由绑定一个 BFD 会话，当这条 USR 上绑定的 BFD 会话检测到链路故障（由 Up 转为 Down）后，BFD 会将故障上报路由管理模块，由路由管理模块将这条路由设置为“非激活”状态（此条路由不可用，从 IP 路由表中删除）。

当这条 USR 上绑定的 BFD 会话成功建立或者从故障状态恢复后（由 Down 转为 Up），BFD 会上报路由管理模块，由路由管理模块将这条路由设置为“激活”状态（此路由可用，加入 IP 路由表）。

BFD for OSPF

网络上的链路故障或拓扑变化都会导致 Eudemon 重新进行路由计算，要提高网络的可用性，缩短路由协议的收敛时间非常重要。由于链路故障无法完全避免，因此，加快故障感知速度并将故障快速通告给路由协议是一种可行的方案。

BFD for OSPF 就是将 BFD 和 OSPF 协议关联起来，通过 BFD 对链路故障的快速感应进而通知 OSPF 协议，从而加快 OSPF 协议对于网络拓扑变化的响应。

表 10-4 显示了 OSPF 协议在有、无 BFD 协议下收敛速度的数据。

表 10-4 OSPF 协议收敛速度的数据

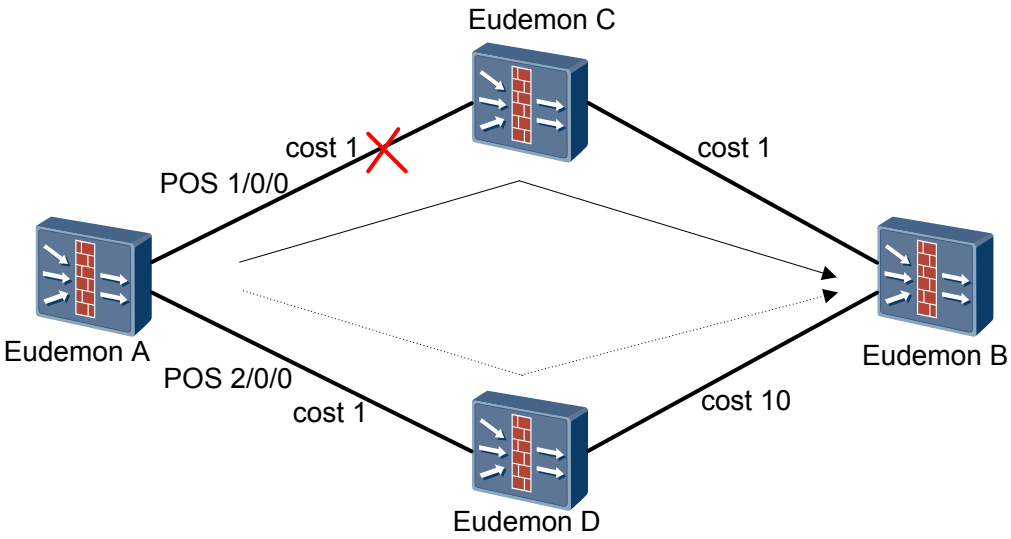
有无 BFD	链路故障检测机制	收敛速度
无 BFD	OSPF Hello Keepalive 定时器超时	秒级
有 BFD	BFD 会话 Down	毫秒级

如图 10-18 所示，Eudemon A 分别与 Eudemon C 和 Eudemon D 建立 OSPF 邻居关系，根据 OSPF 路由的选路规则，Eudemon A 到 Eudemon B 的路由出接口为 POS1/0/0，经过 Eudemon C 到达 Eudemon B。邻居状态到达 FULL 状态时通知 BFD 建立 BFD 会话。

1.当 Eudemon A 和 Eudemon C 之间链路出现故障，BFD 首先感知到并通知 Eudemon A。

2.Eudemon A 处理邻居 Down 事件，重新进行路由计算，新的路由出接口为 POS2/0/0，经过 Eudemon D 到达 Eudemon B。

图 10-18 BFD for OSPF 组网图



BFD for BGP

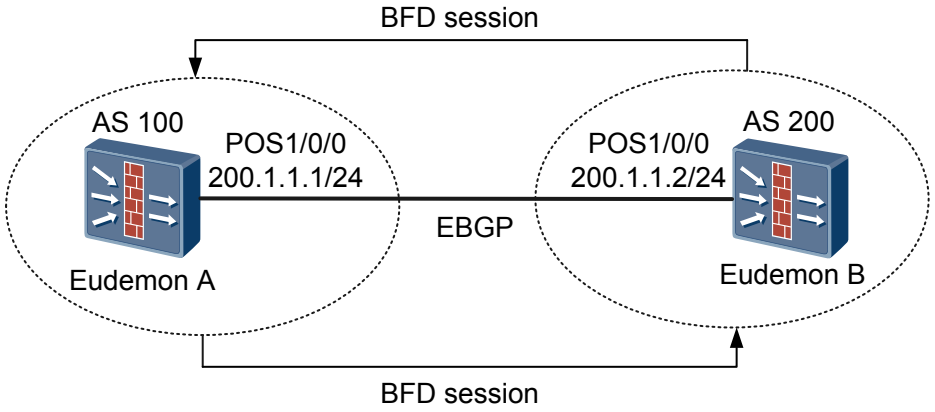
BGP 协议通过周期性的向对等体发送 Keepalive 报文来实现邻居检测机制。但这种机制检测到故障所需时间比较长，超过 1 秒钟，当数据达到吉比特速率级别时，将会导致大量的数据丢失，从而无法满足电信级网络高可靠性的需求。

因此，BGP 协议通过引入 BFD for BGP 特性，利用 BFD 的快速检测机制，迅速发现 BGP 对等体间链路的故障，并报告给 BGP 协议，从而实现 BGP 路由的快速收敛。

组网应用

如图 10-19 所示，Eudemon A 和 Eudemon B 分别属于 AS100 和 AS200，两台设备直接相连并建立 EBGP 连接。使用 BFD 检测 Eudemon A 和 Eudemon B 之间的 BGP 邻居关系，当 Eudemon A 和 Eudemon B 之间的链路发生故障时，BFD 能够快速检测到故障并通告给 BGP 协议。

图 10-19 BFD for BGP 组网图



A 术语

A

AAA 授权、验证（鉴权）和计费，提供了一个用来对认证、授权和计费这三种安全功能进行配置的一致性框架，它是对网络安全的一种管理。

ACL 访问控制列表，ACL 是由 permit | deny 语句组成的一系列有顺序的指令列表，防火墙根据 ACL 判断哪些数据包可以接收，哪些数据包需要拒绝。在 QoS 中，ACL 也用于流分类。

AES 高级加密标准，NIST(美国国家标准与技术协会）制定的用以替代 DES 的加密算法

AH 报文认证头协议，在传输模式和隧道模式下使用，为 IP 包提供数据完整性和验证服务。

ARP 地址解析协议，用于将 IP 地址映射为以太网 MAC 地址。由 RFC826 定义。

ASPF 基于应用层的包过滤，即基于状态的报文过滤。ASPF 和普通的静态防火墙协同工作，以便于实施内部网络的安全策略。由于 ASPF 基于应用层协议会话信息，因此可以智能地过滤 TCP 和 UDP 数据包，能够检测由防火墙任意一侧发起的会话。

AUX 辅助端口，该端口提供了一个 EIA/TIA-232 DTE 接口，通常用于通过 Modem 进行拨号访问。

B

BGP 边界网关协议，是运行于 TCP 上的一种自治系统的路由协议。BGP 是唯一一个用来处理像因特网大小的网络的协议，也是唯一能够妥善处理好不相关路由域间的多路连接的协议。BGP 构建在 EGP 的经验之上。BGP 系统的主要功能是和其他的 BGP 系统交换网络可达信息。网络可达信息包括列出的自治系统（AS）的信息。这些信息有效地构造了 AS 互联的拓朴图并由此清除了路由环路，同时在 AS 级别上可实施策略决策。

C

CHAP 盘问握手认证协议，是密文传送的密码验证方式，为三次握手验证，口令为密文（密钥）。首先是验证方向被验证方发送一些随机产生的报文（Challenge）；然后被验证方用自己的口令字和 MD5 算法对该随机报文进行加密，将生成的密文发回验证方（Response）；最后验证方用自己保存的被验证方口令字和 MD5 算法对原随机报文加密，比较二者的密文，根据比较结果返回不同的响应（Acknowledge or Not Acknowledge）。

CPE-based VPN 基于用户侧设备的 VPN 应用，VPN 功能集中在用户侧设备实现，VPN 的维护管理由用户自己实现。

D

DDoS 分布式拒绝服务，在 Internet 中分布式的服务拒绝攻击指多个安全遭受危害的系统对单个目标进行攻击，因此引起了目标系统用户的服务拒绝。

DES 数据加密标准，明文按照 64 比特块进行加密，并生成 64 比特的密文。

DH Diffie-Hellman 算法，一种允许陌生人建立共享密钥的协议，最初由 Diffie 和 Hellman 发明，主要基于双方都知道的两个大质数 p 和 g，并且存在等式关系：da mod p = cb mod p = gab mod p。

DMZ 非军事化区域，防火墙引用了这一术语，指代一个逻辑上和物理上都与内部网络和外部网络分离的区域。该区域可以放置需要对外提供网络服务的设备，如 WWW Server、FTP Server 等。上述服务器如果放置于外部网络，则防火墙无法保障它们的安全；如果放置于内部网络，外部恶意用户则有可能利用某些服务的安全漏洞攻击内部网络。DMZ 区域很好地解决了服务器的放置问题。

DNS 域名系统，二十世纪八十年代中期发明的一种追踪域名和域地址的分级式方法。DNS 数据库不是依赖于一个文件或一个服务器，而是分布于因特网的几台关键电脑上以防止在一台或几台计算机崩溃时也遭到致命摧毁。DNS 是属于 OSI 模块的申请层的 TCP/IP 服务。

E

ESP 报文安全封装协议，在传输模式和隧道模式下使用，它采用加密和验证机制，为 IP 数据包提供数据源验证、数据完整性、反重放和机密安全服务。

F

FTP FTP 协议，在 TCP/IP 协议族中属于应用层协议，主要向用户提供远程主机之间的文件传输，FTP 协议基于相应的文件系统实现。

G

GRE	通用路由封装协议，当通过 Internet 隧道通信时，隧道服务器提供一个安全的虚拟专用网的一种基本操作。

H

HTTP	超文本传输协议，用于将浏览器发出的请求发送至 Web 服务器并将服务器上的网页传输回请求浏览器。虽然 HTTP 在 Web 上使用得非常广泛，但是它是一种特别不安全的协议。

I

ICMP	Internet 控制消息协议，是 IP 协议的一个组成部分，它用来处理差错和控制报文。
IDS	入侵检测系统，进行入侵检测的软件与硬件的组合，主要用于检测 Hacker 或 Cracker 通过网络进行的入侵行为。
IETF	Internet 工程任务组，致力于发展和设计 TCP/IP 协议栈和 Internet 的组织。
IKE	因特网密钥交换协议，它通过 ISAKMP 实现 Oakley 和 SKEME 密钥交换的混合协议。
IP	互联网协议，是 TCP/IP 协议栈中提供无连接互连网络服务的网络层协议。
IPSec	IP 网络安全协议，IPSec 协议不是一个单独的协议，它定义了 IP 网络上数据安全的一整套体系结构，包括 AH、ESP 和 IKE 等协议。
ISAKMP	互联网安全认证与密钥管理协议，提供了认证和密钥交换的框架，但并没有定义认证和密钥交换的具体实现方式。

L

L2F	二层转发协议，提供对更高级协议链路层的隧道封装，实现了拨号服务器和拨号协议连接在物理位置上的分离。
L2TP	二层隧道协议，由 IETF 起草，微软等公司参与，结合了 PPTP 和 L2F 两个协议的优点，为众多公司所接受，并且已经成为标准 RFC。L2TP 既可用于实现拨号 VPN 业务（VPDN 接入），也可用于实现 VPN 业务。
LAC	L2TP 访问集中器，是附属在交换网络上的具有 PPP 端系统和 L2TP 协议处理能力的设备，通常 LAC 为用户提供接入服务。
LAN	局域网，由处于同一建筑或方圆几公里范围内的个人计算机和工作站相连接而组成的网络，具有高速和低错误率的特点，Ethernet、FDDI、令牌环是 LAN 的三种主要实现技术。

LCP 链路控制协议，在点到点控制协议中，链路控制协议建立、配置并测试数据链路因特网连接。

LNS L2TP 网络服务器，是 PPP 端系统上用于处理 L2TP 协议服务器端部分的软件。

M

MAC 媒体访问控制，在 OSI 七层模型的数据链路层中，MAC 层是较靠近物理层。

MD5 消息摘要算法，由 Ron Rivest 设计的散列函数系列的第 5 个，通过将任意长度的输入信息转换为 128 位的“手印”或摘要信息，实现数字签名，确保网络中信息传输的完整性。

N

NAPT 网络地址端口转换，转换传送标识符（如 TCP 和 UDP 端口数、ICMP 查询标识符）。它将多个私有主机的传送标识符复用进一个单独外部地址的传送标识符中。它使多个主机共享一个单独外部地址。

NAS 网络接入服务器，为 PSTN/ISDN 拨号用户提供访问 Internet 的接入服务。

NAT 网络地址转换，可将内部网络私有 IP 地址转换为公有 IP 地址，以减轻对公有 IP 地址的需求。

NCP 网络控制协议，用于切换虚拟电路连接，实现通路控制，并且操作同步数据链接控制。用来协商网络层协议的参数。

NP 网络处理器，一个主要适用于网络应用领域的集成电路。网络处理器通常是由软件控制的，它跟用于各种设备和产品中的一般用途的 CPU 有相似的特性。

NTP 网络时间协议用于全球范围内维护因特网主机。因特网的许多系统都运行 NTP 协议，保持同一时间（格林威治时间），误差约一秒。

O

OSI 开放系统互连，是对通信网络中信息在两个点之间怎样传输的一种标准的描述或参考模型。

OSPF 开放式最短路径优先是在 Internet 团体中作为 RIP（路由选择信息协议）的后继者而提议的链路状态分层 IGP（内部网关协议）路由选择算法。OSPF 具有最低代价路由选择、多路径路由选择和负载平衡等特点。OSPF 是从 IS-IS 协议的早期版本演变而来的。

P

PAM 端口到应用的映射，将用于网络业务或应用的 TCP 或者 UDP 端口号客户化。当与应用程序相关的注册端口或者众所周知的的端口不同的端口用于运行业务的环境中，PAM 通过这种信息支持上述网络环境。

PAP 密码验证协议，PAP 验证为两次握手验证，口令为明文。首先是被验证方发送用户名和口令到验证方；然后验证方根据用户配置查看是否有此用户以及口令是否正确，返回不同的响应（Acknowledge or Not Acknowledge）。

PPP 点到点协议，在两个设备间的专用传输链路。

PPTP 点到点隧道协议，由微软、Ascend 和 3COM 等公司支持，实现在 IP 网络上隧道封装点到点 PPP 协议。

Q

QoS 业务质量，指对 IP 网络投递分组的服务能力的评估。通常以对延迟、延迟抖动、丢包率等服务需求提供支持的能力作为核心评估对象。

R

RADIUS 远端拨入用户认证服务，最初由 Livinggston Enterprise 公司开发，作为一种分布式的客户机/服务器系统，能提供 AAA 功能。目前可以使用串口和 Modem 的大量分散用户的接入验证、授权和计费等。

RAS 远程访问服务软件，一种 Windows 环境下的软件，允许用户通过调制解调器远程访问网络服务器。

RFC 请求注解，Internet 标准(草案)。

RIP 路由信息协议，采用距离－矢量算法计算路由，使用步跳数选择路由，广泛使用于小型网络中，是最常见的一种内部网关协议。

RTSP 实时流协议是一种客户端/服务器应用级协议。这种协议用来控制数据的实时传输。

S

SA 安全联盟，IPSec 对数据流提供的安全服务通过安全联盟 SA 来实现，它包括协议、算法、密钥等内容，具体确定了如何对 IP 报文进行处理。

SIP 会话发起协议，是一个互联网工程任务组（IETF）标准协议，它用于发起视频、语音、聊天、游戏以及虚拟现实等多媒体元素的交互用户会话。

SMTP 简单邮件传送协议，实际上是通过 Internet 传送 e-mail 的标准。

SNMP 简单网络管理协议，TCP/IP 协议族的一部分，用于控制和管理 IP 网关，以及其他一些网络功能。

SPI 安全变量索引，是一个 32 比特的数值，在每一个 IPSec 报文中都携带该值。SPI、目的 IP 地址、安全协议号三者结合起来共同构成三元组，来唯一标识一个特定的安全联盟。

SSH 安全外壳，SSH 连接可以提供安全的 Telnet 访问。

SSL 加密套接字协议层，SSL 是一种安全协议，它为网络（例如因特网）的通信提供私密性。

T

TCP 传输控制协议，TCP/IP 标准传输层协议，它为许多应用协议提供可靠的、全双工、数据流式服务。

TCP/IP 传输控制协议/互联网协议，用于在因特网上连接主机的一套通信协议。最主要的两个协议是 TCP 协议和 IP 协议。

TE 流量工程，包括流量管理，容量管理，容量度量和模型化，网络模型化和性能分析。

TFTP 简单文件传输协议，TCP/IP FTP 协议的一种无需用户名和密码的版本。

U

UDP 用户数据报协议，是 TCP/IP 协议族中的无连接传输层协议。它是一种无需确认或者担保投递就能交换数据报的简单协议。

V

VGMP VRRP 组管理协议，为防止 VRRP 状态不一致现象的发生，华为公司在 VRRP 基础上进行了扩展，推出了 VRRP 组管理协议 VGMP（VRRP Group Management Protocol），负责统一管理加入其中的各备份组 VRRP 状态。借助 VGMP 机制，可以实现对多个 VRRP 备份组（虚拟防火墙）的状态一致性管理、抢占管理和通道管理等。

VLAN 虚拟局域网，把一个 LAN 划分成多个逻辑的“LAN”，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样。

VPDN 虚拟专用拨号网络，即利用公共网络（如 ISDN 和 PSTN）的拨号功能及接入网来实现虚拟专用网。

VPLS 虚拟专用局域网网段，借助 IP 公共网络实现 LAN 之间通过虚拟专用网段互连，是局域网在 IP 公共网络上的延伸。

VPN 虚拟专用网，是近年来随着 Internet 的广泛应用而迅速发展起来的一种新技术，以实现在公用网络上构建私人专用网络。“虚拟”主要指这种网络是一种逻辑上的网络。

VPRN 虚拟专用路由网络，即借助 IP 公共网络实现总部、分支机构和远端办公室之间通过网络管理虚拟路由器进行互连。

VRRP 虚拟路由冗余协议，它为具有多播或广播能力的局域网设计，将局域网的一组路由器（包括一个 Master 和若干个 Backup）组织成一个虚拟的路由器，称之为一个备份组。

W

WWW 全球超媒体信息网，一种允许用户浏览信息的大规模、超媒体信息服务系统。

B 缩略语

Numerics

3DES	Triple DES	三层数据加密标准

A

AAA	Authorization, Authentication and Accounting	授权、验证（鉴权）和计费
ACK	ACKnowledgement	应答
ACL	Access Control List	访问控制列表
AES	Advanced Encryption Standard	高级加密标准
AH	Authentication Header	报文认证头
ALG	Application Layer Gateway	应用层网关
ARP	Address Resolution Protocol	地址解析协议
ASPF	Application Specific Packet Filter	基于应用层的包过滤
AUX	Auxiliary port	备份口

B

BFD	Bidirectional Forwarding Detection	双向转发检测
BGP	Border Gateway Protocol	边界网关协议

C

CHAP	Challenge Handshake Authentication Protocol	盘问握手认证协议

CPE-based VPN	Customer Premises Equipment based VPN	基于用户侧设备的 VPN 应用
CPU	Central Processing Unit	中央处理单元
D		
DDN	Digital Data Network	数字数据网
DDoS	Distributed Denial of Service	分布式拒绝服务
DES	Data Encryption Standard	数据加密标准
DH	Diffie-Hellman algorithm	Diffie-Hellman 算法
DMZ	Demilitarized Zone	非军事化区域
DNS	Domain Name System	域名系统
DoS	Denial of Service	拒绝服务
E		
EAP	Extensible Authentication Protocol	可扩展认证协议
ESP	Encapsulating Security Payload	封装安全载荷
F		
FTP	File Transfer Protocol	文件传输协议
G		
GE	Gigabit Ethernet	千兆以太网
GRE	Generic Routing Encapsulation	通用路由封装
H		
HDLC	High level Data Link Control	高级数据链路控制
HRP	Huawei Redundancy Protocol	华为冗余协议
HTTP	Hypertext Transfer Protocol	超文本传输协议
I		
IBGP	internal BGP	内部边界网关协议
ICMP	Internet Control Message Protocol	Internet 控制消息协议

ID	Identity	标识
IDS	Intrusion Detection System	入侵检测系统
IETF	Internet Engineering Task Force	互连网工程任务组
IGMP	Internet Group Management Protocol	因特网组管理协议
IKE	Internet Key Exchange	因特网密钥交换协议
IP	Internet Protocol	互联网协议
IPSec	IP Security Protocol	IP 网络安全协议
ISAKMP	Internet Security Association and Key Management Protocol	互联网安全认证与密钥管理协议
ISDN	Integrated Services Digital Network	综合业务数字网
ISP	Internet Service Provider	互联网服务供应商
L		
L2F	Layer Two Forwarding	二层转发
L2TP	Layer Two Tunneling Protocol	二层隧道协议
LAC	L2TP Access Concentrator	L2TP 访问集中器
LAN	Local Area Network	局域网
LCP	Link Control Protocol	链路控制协议
LNS	L2TP Network Server	L2TP 网络服务器
M		
MAC	Media Access Control	媒体访问控制
MD5	Message Digest Algorithm 5	信息-摘要算法 5
MPLS	MultiProtocol Label Switching	多协议标签交换
N		
NAPT	Network Address and Port Translation	网络地址端口转换
NAS	Network Access Server	网络接入服务器
NAT	Network Address Translation	网络地址转换
NBIP-VPN	Network-based VPN	基于网络侧设备的 VPN 应用
NCP	Network Control Protocol	网络控制协议

NP	Network Processor	网络处理器
NTP	Network Time Protocol	网络时间协议
O		
OOB	Out-Of-Band	越界
OSI	Open Systems Interconnection	开放系统互连
OSPF	Open Shortest Path First	开放最短路径优先
P		
PAM	Port to Application Mapping	端口到应用的映射
PAP	Password Authentication Protocol	密码验证协议
PFS	Perfect Forward Secrecy	完善的前向安全性
POP	Point of Presence	显示点
PPP	Point-to-Point Protocol	点到点协议
PPTP	Point-to-Point Tunneling Protocol	点对点隧道协议
PSTN	Public Switched Telephone Network	公共电话交换网
Q		
QoS	Quality of Service	业务质量
R		
RADIUS	Remote Authentication Dial in User Service	远端拨入用户认证服务
RAS	Remote Access service	远程访问服务软件
RFC	Request For Comments	请求注释
RIP	Routing Information Protocol	路由信息协议
RSA	Rivest, Shamir, Adleman	通用关键字密码算法
RTSP	Real-Time Streaming Protocol	实时流协议
S		
SA	Security Association	安全联盟
SAE	Security Accelerate Engine	安全加速引擎

SHA	Secure Hash Algorithm	安全散列算法
SIP	Session Initiation Protocol	会话发起协议
SMTP	Simple Mail Transfer Protocol	简单邮件传送协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SPI	Security Parameters Index	安全变量索引
SSH	Secure Shell	安全外壳
SSL	Secure Socket Layer	加密套接字协议层
SYN Flood	Synchronization Flood	同步泛洪

T

TCP	Transmission Control Protocol	传输控制协议
TCP/IP	Transmission Control Protocol/ Internet Protocol	传输控制协议/互联网协议
TE	Traffic Engineering	流量工程
TFTP	Trivial File Transfer Protocol	简单文件传输协议
ToS	Type of Service	服务类型

U

UDP	User Datagram Protocol	用户数据报协议
URL	Universal Resource Locator	统一资源定位器

V

VGMP	VRRP Group Management Protocol	VRRP 组管理协议
VLAN	Virtual LAN	虚拟局域网
VLL	Virtual Leased Line	虚拟租用线
VPDN	Virtual Private Dial Network	虚拟专用拨号网
VPLS	Virtual Private LAN Segment	虚拟专用局域网网段
VPN	Virtual Private Network	虚拟专用网
VPRN	Virtual Private Routing Network	虚拟专用路由网
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议

W		
WWW	World Wide Web	全球超媒体信息网