

第 3 篇 传统 VPN 技术

第 8 章 VPN 概述

第 9 章 GRE VPN

第 10 章 L2TP VPN

第8章 VPN 概述

传统上，企业基于专用的通信线路构建 Intranet。这种方式昂贵而缺乏灵活性。而通过 Internet 直接连接各个分支机构又缺乏安全性和扩展性。因此 VPN（Virtual Private Network，虚拟专用网）技术应运而生。

8.1 本章目标

课程目标

● 学习完本课程，您应该能够：

- 理解传统企业网发展中遇到的挑战，描述企业网对VPN技术的需求
- 描述VPN关键概念术语
- 描述VPN的主要分类方法
- 列举主要VPN技术并描述其功能




www.h3c.com

8.2 企业网对VPN的需求

8.2.1 传统企业网面临的问题

传统企业网面临的问题



核心企业 数字化解决方案领导者

- **直接通过Internet或运营商骨干网络连接分支机构的缺点：**
 - 网络层协议必须统一
 - 必须使用统一的路由策略
 - 必须使用同一公网地址空间
- **企业直接通过专线、电路交换或分组交换的广域网技术连接其分支机构的缺点：**
 - 布署成本高
 - 变更不灵活
 - 移动用户远程拨号接入费用高

www.h3c.com

现代企业在发展过程中，对网络提出了越来越高的要求。而仅采用传统路由交换和广域网连接技术构建企业网时，网络将面对路由设计、地址规划、安全保护、成本、灵活性等各方面的挑战。

传统企业网要么通过 Internet 或运营商骨干 IP 网络，要么通过专线、电路交换或分组交换的广域网技术连接其各分支机构。

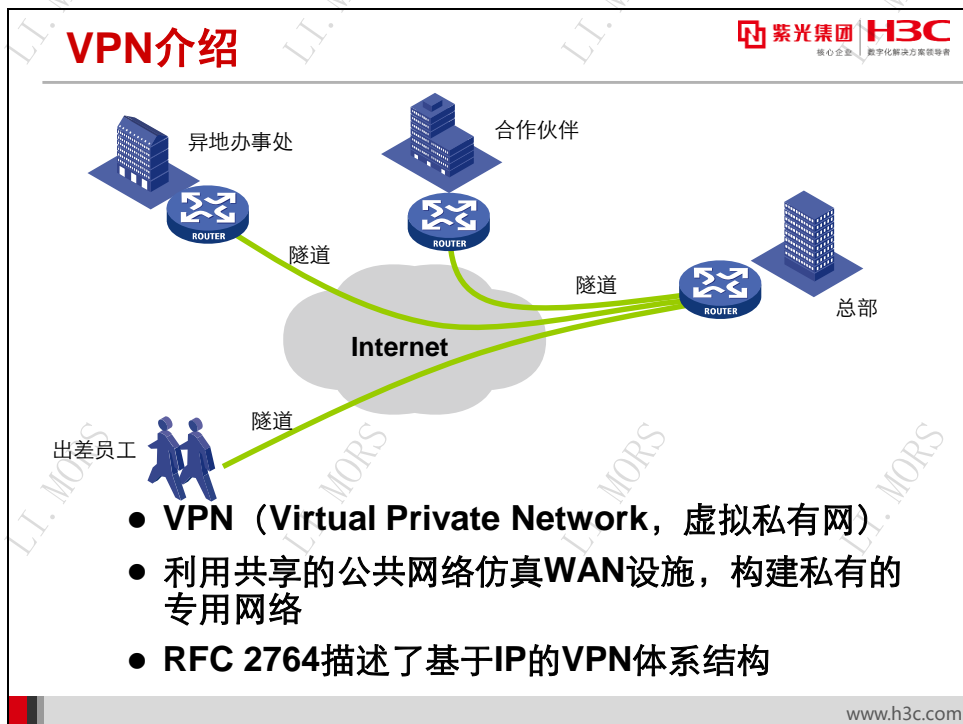
企业通过 Internet 或运营商骨干网络连接分支机构的方式具有以下缺点：

- **网络层协议必须统一：**企业路由器与运营商路由器运行相同的网络层协议，不支持多协议。例如当跨越 Internet 进行通信时，企业分支间的 IPX 协议通信无法实现。
- **必须使用统一的公网地址空间规划：**当直接跨越 Internet 进行通信时，运营商路由器和所有企业路由器都必须处于统一的 Internet 地址空间内，企业无法自行规划和使用私有地址空间互联，这势必会进一步加剧公网地址的匮乏情况。而 NAT 技术的复杂性使其无法有效解决这一问题。
- **必须使用统一的路由策略：**企业路由器与运营商路由器运行相同的路由协议，互相交换路由信息。一方面，企业网内部路由信息完全泄漏，产生安全隐患；另一方面，由于运营商面对大量企业提供服务，将导致路由表规模过大，消耗处理资源。

企业通过专线、电路交换或分组交换的广域网技术连接其分支机构的方案具有以下缺点：

- **布署成本高：**企业需要向运营商租用昂贵的点对点专线或虚电路建立站点间连接，费用高昂。
- **变更不灵活：**专线或虚电路的建立和变更需要运营商配合，操作周期长，时间成本高。
- **移动用户远程拨号接入费用高：**若采用 PSTN/ISDN 等拨号方式远程接入企业网，不但速度慢，而且必须支付昂贵的长途电话费用。

8.2.2 什么是 VPN




VPN (Virtual Private Network, 虚拟私有网) 是近年来随着 Internet 的发展而迅速发展起来的一种技术。VPN 是利用共享的公共网络设施对广域网设施进行仿真而构建的私有专用网络。可用于构建 VPN 的公共网络并不局限于 Internet，也可以是 ISP 的 IP 骨干网络，甚至是企业私有的 IP 骨干网络等。在公共网络上组建的 VPN 可以像企业现有的私有网络一样提供安全性、可靠性和可管理性等。

RFC 2764 描述了基于 IP 的 VPN 框架结构。利用基于 IP 的 Internet 实现 VPN 的核心是各种隧道 (Tunnel) 技术。通过隧道，企业私有数据可以跨越公共网络安全地传递。传统的广域网连接是通过专线或者电路交换连接来实现的。而 VPN 是利用公共网络来建设虚拟的隧道，在远程移动用户、驻外机构、合作伙伴、供应商与公司总部之间建立广域网连接，既可以保证连通性，也可以保证安全性。

8.2.3 VPN 的优势

VPN的优势

- 可以快速构建网络，降低布署周期
- 与私有网络一样提供安全性、可靠性和可管理性
- 可利用Internet，无处不连通，处处可接入
- 简化用户侧的配置和维护工作
- 提高基础资源利用率
- 于客户可节约使用开销
- 于运营商可以有效利用基础设施，提供大量、多种业务



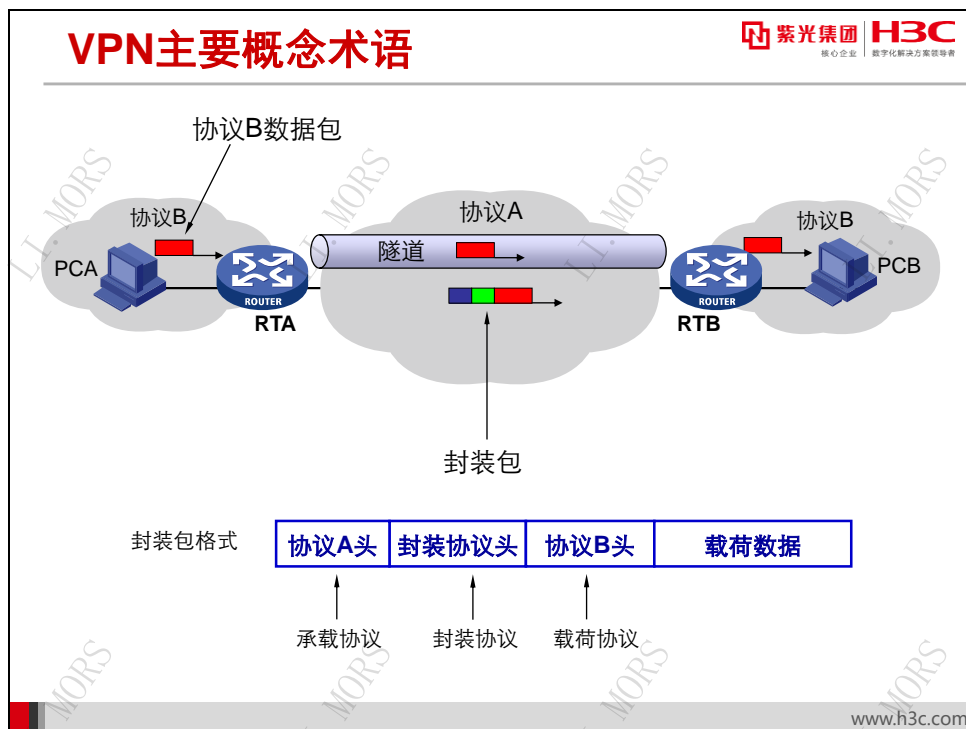
核心企业 | 数字化解决方案领导者

www.h3c.com

VPN 的应用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。无需改动基础硬件设施，仅通过修改软件配置就可以增加、删除 VPN 用户，使得 VPN 相关应用具有非常好的灵活性，可以大大缩短布署周期，加快业务响应速度。VPN 可以基于 Internet 基础设施实施，使用户可以在任何时间、任何地点实现接入，这将很好地满足快速增长和变化的移动业务需求。VPN 技术允许构建具有安全保证和服务质量保证的虚拟私有网络，可为 VPN 用户提供不同等级的安全性和服务质量承诺。

利用公共网络进行通信，一方面使企业能够以更低的成本连接远程分支机构、移动办公人员和合作伙伴，另一方面使 ISP（Internet Service Provider，Internet 服务提供商）能够极大地提高网络资源利用率，增加综合收益。

8.3 VPN主要概念术语



在图示网络中，支持协议 B 的两个网络互相之间没有直接的广域网连接，而是通过一个协议 A 的网络互连，但它们仍然需要互相通信。

直接在协议 A 网络上传送协议 B 的数据包显然是不实现的，因为协议 A 无法识别协议 B 的数据包格式。在这个网络模型中要实现 VPN，就可以使用某种类型的隧道（Tunnel）机制，使 PCA 和 PCB 的通信能够通过该隧道技术跨越协议 A 网络进行。

PCA 对 PCB 发送的数据包须经过以下过程才能到达 PCB：

- 首先 PCA 发送协议 B 数据包；
- 数据包到达隧道端点设备 RTA，RTA 将其封装成协议 A 数据包，通过协议 A 网络发送给隧道的另一端点设备 RTB；
- 隧道终点设备将协议 A 数据包解开，还原协议 B 数据包，发送给 PCB。

在这种情况下，协议 A 称为承载协议（Delivery Protocol），协议 A 的包称为承载协议包（Delivery Protocol Packet）；协议 B 称为载荷协议（Payload Protocol），协议 B 的包称为载荷协议包（Payload Protocol Packet）。而决定如何实现隧道的协议称为隧道协议（Tunnel Protocol）。

为了便于标识承载协议包中封装了载荷协议包，往往需要在承载协议报文头部和载荷协议报文头部之间加入一个新的协议报文头部，这个协议称为封装协议（Encapsulation Protocol），经过封装协议封装的包称为封装协议包（Encapsulation Protocol Packet）。

在典型的 VPN 应用场景中，PCA 和 PCB 所在的协议 B 网络为企业内部网络，称为私网（Private Network）；作为承载协议的协议 A 网络为运营商骨干网络或 Internet，称为公网（Public Network）。

8.4 VPN分类

VPN的分类方法

- 按照业务用途
 - Intranet VPN、Extranet VPN
- 按照运营模式
 - CPE-Based VPN、Network-Based VPN
- 按照组网模型
 - VPDN、VPRN、VLL、VPLS
- 按照网络层次
 - Layer 2 VPN、Layer 3 VPN



紫光集团 H3C
核心企业 数字化解决方案领导者

www.h3c.com

依据不同的划分标准，可以将 VPN 划分为多种类型。

按照业务用途的不同，可以将 VPN 划分为 Intranet VPN、Extranet VPN 等：

- **Intranet VPN:** 通过使用 Intranet VPN，组织可以跨越公共骨干网络，甚至可以跨越 Internet，在全球范围内连接其各个分支节点。而与此同时，组织仅需支付较少的费用。因为 Intranet VPN 主要用于站点间的互连，所以又称为 **Site-to-Site VPN**（站点到站点 VPN）。Intranet VPN 可以减少组织花费在租用运营商专线或广域网连接上的巨额费用。同时，企业可以自由规划网络的逻辑连接结构，随时布署新的逻辑拓扑，大大缩短了变更周期。通过额外的逻辑和物理连接，还可以利用 Intranet VPN 强化 Intranet 的可靠性。
- **Extranet VPN:** Extranet VPN 通过共享的 Internet 基础设施，将企业与其客户、上游供应商、合作伙伴及相关组织等连接在一起。Extranet VPN 不但可以提供组织之间的互通，而且随着业务和相关组织的变化，组织可以随时扩充、修改或重新布署 Extranet VPN 网络结构。

按照运营模式的不同，可以将 VPN 划分为 CPE-Based VPN、Network-Based VPN 等：

- **CPE-Based VPN:** CPE（Customer Premise Equipment，用户前端设备）是指放置在用户侧，直接连接到运营商网络的网络设备。CPE 可以是一台路由器、防火墙、或者是专用的 VPN 网关。在 CPE-Based VPN 中，CPE 必须支持 VPN 特性，负责建立和维护 VPN 连接，连接到 VPN 隧道的另一个终结点——其它的 CPE 设备。因此用

户通常需要自行采购这些 CPE 设备，并且自行在各个站点之间配置 VPN 隧道。有时也可以委托运营商或第三方服务提供商进行配置和管理。

CPE-Based VPN 的好处是，用户可以自由布署、任意扩展 VPN 网络结构，但同时也必须具有相当的专业技术能力。在没有运营商支持的情况下，CPE-Based VPN 的服务质量保障也同样是一个问题。

- **Network-Based VPN:** 在 Network-Based VPN 中，VPN 的发起和终结设备放置在运营商网络侧，由运营商负责采购此类支持复杂 VPN 特性的设备，布署并管理 VPN 网络。用户 CPE 设备不需要感知 VPN 的存在，也不需要支持复杂的 VPN 特性。用户无须关心 VPN 的具体实现，只需要向运营商提出需求，订购服务即可。

Network-Based VPN 不但把用户从繁杂的 VPN 设计、布署和维护中解放出来；而且为运营商提供了低价格高价值的新业务产品。在 Network-Based VPN 中，有了运营商的全面参与，服务质量也可以得到有效保障。

按照组网模型的不同，可以将 VPN 划分为 VPDN、VPRN、VLL、VPLS 等：

- **VPDN (Virtual Private Dial Networks, 虚拟私有拨号网络):** VPDN 允许远程移动用户根据需要访问企业内部网络。用户可以通过诸如 PSTN 和 ISDN 这样的拨号网络接入，其数据包通过隧道穿越公共网络，到达中心站点。
由于涉及远程用户从任意地点访问，VPDN 必须提供足够安全的身份验证功能，以确保接入用户的合法性。
- **VPRN (Virtual Private Routed Networks, 虚拟私有路由网络):** VPRN 根据网络层路由信息，在网络层转发数据包。由于使用相同的网络层转发表，VPN 之间只能通过不同的路由信息加以区分。
因为通过网络层转发，所以一个 VPRN 网络只能支持一种网络层协议，而为另一种协议配置一个新的 VPRN。通过路由区分 VPN 还会导致全网必须使用统一的地址空间，如果将其部署于运营网络，则独立的管理区域与路由配置的复杂性之间必将存在天然矛盾，要解决这个问题，就要求 VPRN 中的 ISP 网络设备支持多个独立的路由表。
- **VLL (Virtual Leased Lines, 虚拟专线):** 在 VLL 中，运营商通过 VPN 技术建立基础网络，为客户提供虚拟专线服务。对于客户来说，CPE 到运营商 PE 的接口是普通的专线接口，链路层协议是普通的 WAN 协议，客户所获得的服务就像是普通专线服务一样。而运营商在 IP 骨干网络两端的 PE 之间建立隧道，封装客户的数据帧并在 IP 骨干网络上发送。
例如，客户向运营商订购 Frame Relay 服务，而运营商并不通过真正的 Frame Relay 网络提供服务，而是在其 IP 骨干网络两端的边界设备之间建立 IP 隧道，将客户的 Frame Relay 帧封装在 IP 隧道中传送。
- **VPLS (Virtual Private LAN Segment, 虚拟私有局域网段):** VPLS 可以用 VPN 网络透明地传送以太帧，使各个站点的 LAN 可以直接相连，所以 VPLS 又称为 TLS (Transparent LAN Service, 透明局域网服务)。
由于被传送的是链路层以太帧，所以 CPE 可以是一个简单二层设备，而处于公网

络的运营商设备必须能够采用某种隧道技术对以太网帧加以封装，并传送到正确的目的站点。

按照 OSI 模型层次的不同，可以将 VPN 划分为 Layer 2 VPN、Layer 3 VPN 等：

- **L2 VPN (Layer 2 VPN, 二层 VPN)：**在 L2 VPN 中，载荷协议处于 OSI 参考模型的数据链路层，承载协议直接封装载荷协议帧 (Frame)。比较典型的 L2 VPN 技术是 L2TP (Layer 2 Tunnel Protocol, 二层隧道协议)。L2TP 允许在 IP 隧道中传送二层的 PPP 帧。
- **L3 VPN (Layer 3 VPN, 三层 VPN)：**在 L3 VPN 中，载荷协议处于 OSI 参考模型的网络层，承载协议直接封装载荷协议包 (Packet)。比较典型的 L3 VPN 技术是 GRE (Generic Routing Encapsulation, 通用路由封装)。GRE 对三层数据包加以封装，可以构建 GRE 隧道，这就是一种网络层隧道。

8.5 主要VPN技术

主要VPN技术

- 主要的L2 VPN技术
 - L2TP
 - QinQ
 - MPLS L2 VPN
- 主要的L3 VPN技术
 - GRE
 - IPsec
 - BGP/MPLS VPN



核心企业 | 数字化解决方案领导者

www.h3c.com

目前一些 VPN 技术已得到普遍应用，或具备一定的代表性。

主要的 L2 VPN 技术包括：

- **L2TP (Layer 2 Tunneling Protocol)**: 二层隧道协议，由 IETF 起草，微软等公司参与，结合了 PPTP 和 L2F 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），也可用于实现专线 VPN 业务。
- **QinQ**: QinQ 是 802.1Q in 802.1Q 的简称，是基于 IEEE 802.1Q 技术的一种比较简单的二层 VPN 协议。通过将一层 VLAN Tag 封装到私网报文上，使其携带两层 VLAN Tag 穿越运营商的骨干网络，从而使运营商能够利用一个 VLAN 为包含多个 VLAN 的用户网络提供服务。
- **MPLS L2 VPN**: 在 MPLS (Multi-Protocol Label Switching, 多协议标签交换) 的基础上发展出了多种二层 VPN 技术，如 Martini 和 Kompella, CCC 实现的 VLL 方式的 VPN，以及 VPLS 方式的 VPN。

主要的 L3 VPN 技术包括：

- **GRE (Generic Routing Encapsulation, 通用路由封装)**: GRE 是为了在任意一种协议中封装任意一种协议而设计的封装方法。IETF 在 RFC 2784 中规范了 GRE 的标准。GRE 封装并不要求任何一种对应的 VPN 协议或实现，任何的 VPN 体系均可以选择 GRE 或者其它方法用于其 VPN 隧道。GRE 可以用来对任意一种网络层协议（如

IPv6) 的数据报文进行封装, 使这些被封装的数据报文能够在另一个网络 (如 IPv4) 中传输。封装前后数据报文的网络层协议可以相同, 也可以不同。封装后的数据报文在网络中传输的路径, 称为 GRE 隧道。GRE 隧道是一个虚拟的点到点的连接, 其两端的设备分别对数据报文进行封装及解封装。

- **IPsec (IP Security):** 是 IETF 制定的三层隧道加密协议, 它为 Internet 上传输的数据提供了高质量的、基于密码学的安全保证。IPsec 通过在特定通信方之间 (例如两个安全网关之间) 建立 “通道”, 来保护通信方之间传输的用户数据, 该通道通常称为 IPsec 隧道。IPsec 协议不是一个单独的协议, 它为 IP 层上的网络数据安全提供了一整套安全体系结构, 包括安全协议 AH (Authentication Header, 认证头) 和 ESP (Encapsulating Security Payload, 封装安全载荷)、IKE (Internet Key Exchange, 互联网密钥交换) 以及用于网络认证及加密的一些算法等。其中, AH 协议和 ESP 协议用于提供安全服务, IKE 协议用于密钥交换。IPsec 可以实现对数据的私密性、完整性保护和源验证。
- **BGP/MPLS L3 VPN:** 是利用 MPLS 和 MP-BGP (Multi-Protocol BGP, 多协议 BGP) 技术实现的三层 VPN。它不但实现了网络控制平面与转发平面相分离, 核心承载网络路由与客户网络路由相分离, 边缘策略与核心转发相分离, CPE 设备与复杂的 VPN 基础构造配置相分离, IP 地址空间隔离等, 而且具备了良好的灵活性、可维护性和扩展性。

其它VPN技术



- **SSL VPN (Secure Sockets Layer Virtual Private Network , 安全套接字层虚拟专用网络)**
- **ADVPN (Auto Discovery Virtual Private Network, 自发现虚拟专用网络)**

www.h3c.com

另外还有很多其它的 VPN 技术, 例如:

- **SSL (Secure Sockets Layer) VPN:** SSL 是由 Netscape 公司开发的一套 Internet 数据安全协议, 它已被广泛地用于 Web 浏览器与服务器之间的身份验证和加密数据

传输。SSL 位于 TCP/IP 协议与各种应用层协议之间，为数据通讯提供安全支持。SSL VPN 是采用 SSL 协议来实现远程移动用户接入的 VPN 技术，具有安全性高、配置简单、多种网络环境适应性强等诸多优点。

- **ADVPN (Auto Discovery Virtual Private Network, 自发现虚拟专用网络):** 通过 VAM (VPN Address Management, VPN 地址管理) 协议收集、维护和分发动态变化的公网地址等信息，解决了当企业分支机构采用动态地址接入公共网络时，通信一方无法事先知道对端的公网地址进而无法组建 VPN 网络的难题。ADVPN 把连接到公网上的各节点组成的网络看作 VPN 网络，把公网看作 VPN 网络的链路层，ADVPN 隧道作为企业内部子网之间的虚通道，相当于网络层。ADVPN 通过 VAM 获取通信对端的公网地址，帮助用户快捷、方便的建立起内部的安全隧道。

8.6 本章总结

本章总结

- 通过专用线路或Internet互连分支机构都无法满足企业网的需求
- VPN能综合平衡费用、灵活性、扩展性和安全性等需求
- VPN通常通过隧道技术实现
- VPN可以根据多种标准进行分类
- 常用的L2 VPN技术包括L2TP、QinQ、MPLS L2 VPN等，L3 VPN技术包括GRE、IPsec、BGP/MPLS VPN等

www.h3c.com

8.7 习题和解答

8.7.1 习题

1. 下列描述中正确的是（ ）
A. VPDN 允许远程移动用户通过诸如 PSTN 和 ISDN 这样的拨号网络接入。
B. CPE-Based VPN 允许用户自由布署 VPN 网络结构。
C. 一个 VPRN 网络可以支持多种网络层协议
D. 在 VLL 中，运营商通过 VPN 技术建立基础网络，为客户提供虚拟专线服务。
2. 按照业务用途的不同，可以将 VPN 分为以下哪些类型？（ ）
A. VPRN B. Intranet VPN C. Extranet VPN D. VPDN
3. 按照组网模型的不同，可以将 VPN 分为以下哪些类型？（ ）
A. VPRN B. Intranet VPN
C. Extranet VPN D. VPDN
4. 下列描述正确的是（ ）
A. 在 VPN 隧道封装时，承载协议包被封装在载荷协议包中
B. 在 VPN 隧道封装时，载荷协议包被封装在承载协议包中
C. 在 VPN 隧道封装时，封装协议头处于最外层，以便将承载协议封装起来
D. 在 VPN 隧道封装时，封装协议头处于最外层，以便将载荷协议封装起来
5. 下列 VPN 技术中，属于 L2 VPN 技术的有（ ）
A. GRE VPN B. IPsec VPN C. BGP/MPLS L3 VPN D. L2TP VPN

8.7.2 习题答案

1. ABD
2. BC
3. AD
4. B
5. D

第9章 GRE VPN

通过 GRE（Generic Routing Encapsulation，通用路由封装）实现的 GRE VPN 是一种典型的 L3 VPN，也是最基本的一种。本章首先讲解 GRE 封装格式，随后将探讨在纯 IPv4 环境下用 GRE 封装 IP 包的方法，以及 GRE VPN 的工作原理和配置等。

9.1 本章目标

课程目标

● 学习完本课程，您应该能够：

- 描述GRE隧道工作原理、GRE VPN的特点以及部署GRE VPN的考虑因素
- 配置GRE VPN
- 使用display命令和debugging命令获取GRE VPN配置和运行信息，了解GRE VPN运行时的重要事件和异常情况
- 理解GRE VPN的典型应用



www.h3c.com

9.2 GRE VPN概述

GRE VPN

- **GRE (Generic Routing Encapsulation)**
 - 在任意一种网络协议上传送任意一种其它网络协议的封装方法
 - RFC 2784定义了标准GRE封装
- **GRE VPN**
 - 直接使用GRE封装建立GRE隧道，在一种协议的网路上传送其它协议
 - 虚拟的隧道（Tunnel）接口

www.h3c.com

GRE（Generic Routing Encapsulation，通用路由封装）是一种封装方法的名称，而不是特指 VPN。IETF 首先在 RFC 1701 中描述了 GRE，一个在任意一种网络协议上传送任意一种其他网络协议的封装方法。稍后，IETF 又在 RFC 1702 中描述了如何用 GRE 在 IPv4 网络上传送其他的网络协议。最终，RFC 2784 规范了 GRE 的标准。

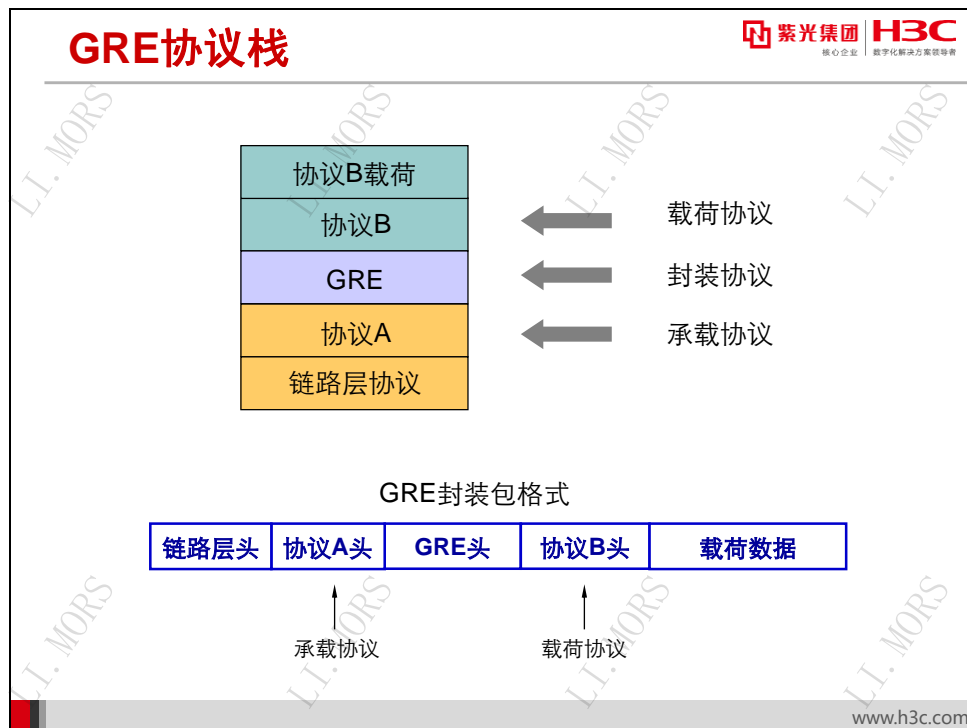
GRE 只是一种封装方法。对于隧道和 VPN 操作的处理机制，例如如何建立隧道，如何维护隧道，如何拆除隧道，如何保证数据的安全性，当出现数据错误或意外发生时如何处理等等，GRE 本身并没有做出任何规范。

GRE 封装并不要求任何一种对应的 VPN 协议或实现。任何的 VPN 体系均可以选择 GRE 或者其他方法用于其 VPN 隧道。通过为不同的协议分配不同的协议号码，GRE 可以应用于在绝大部分的隧道封装场合。

所谓的 GRE VPN 实际上是指直接使用 GRE 封装，在一种网络协议上传送其他协议的一种 VPN 实现。在 GRE VPN 中，网络设备根据配置信息，直接利用 GRE 的多层封装构造隧道（Tunnel），从而在一个网络协议上透明传送其他协议分组。这是一种相对简单却相当有效的实现方法。理解 GRE VPN 工作原理是理解其他 VPN 协议的基础。

9.3 GRE封装格式

9.3.1 GRE 协议栈



在 GRE 隧道中，数据包使用 GRE 封装，其协议栈和格式如图所示。此时 GRE 作为封装协议（Encapsulation Protocol）存在。

在承载协议头之后加入的 GRE 头本身就可以告诉目标设备“上层有载荷分组”，使目标设备可以做出不同于 A 协议标准包的处理。当然这还是不够的，GRE 必须表达一些其它的信息，以便设备继续执行正确的处理。例如 GRE 头必须包含上层协议的类型，以便设备在解封装之后，可以把载荷分组递交到正确的协议栈继续处理。

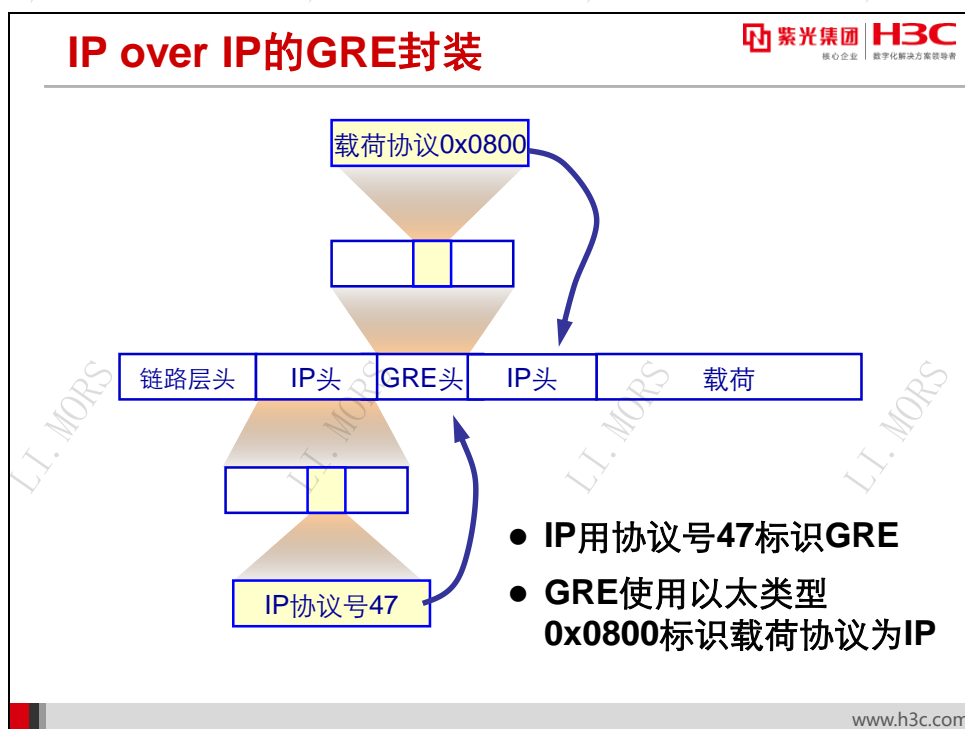
RFC 2784 定义了 GRE 标准头格式。其中有一个 2 字节长的 Protocol Type 字段用于指示载荷协议的类型。该字段使用 IANA（Internet Assigned Number Authority，因特网编号授权委员会）定义的以太网协议类型来标识载荷包的协议。一些常见的 GRE 载荷协议及其协议号如下表所示。

协议名	协议类型号（16 进制）
SNA	0004
OSI network layer	00FE
XNS	0600
IP	0800

DECnet (Phase IV)	6003
Ethertalk (Appletalk)	809B
Novell IPX	8137

出于对日益复杂的网络环境和应用的适应，RFC 2890 对 GRE 进行了增强，形成了 GRE 扩展头格式。扩展的 GRE 头在原有 GRE 头格式基础上，增加了 2 个可选字段 Key 和 Sequence Number，从而使 GRE 具备了标识数据流和分组次序的能力。

9.3.2 IP over IP 的 GRE 封装



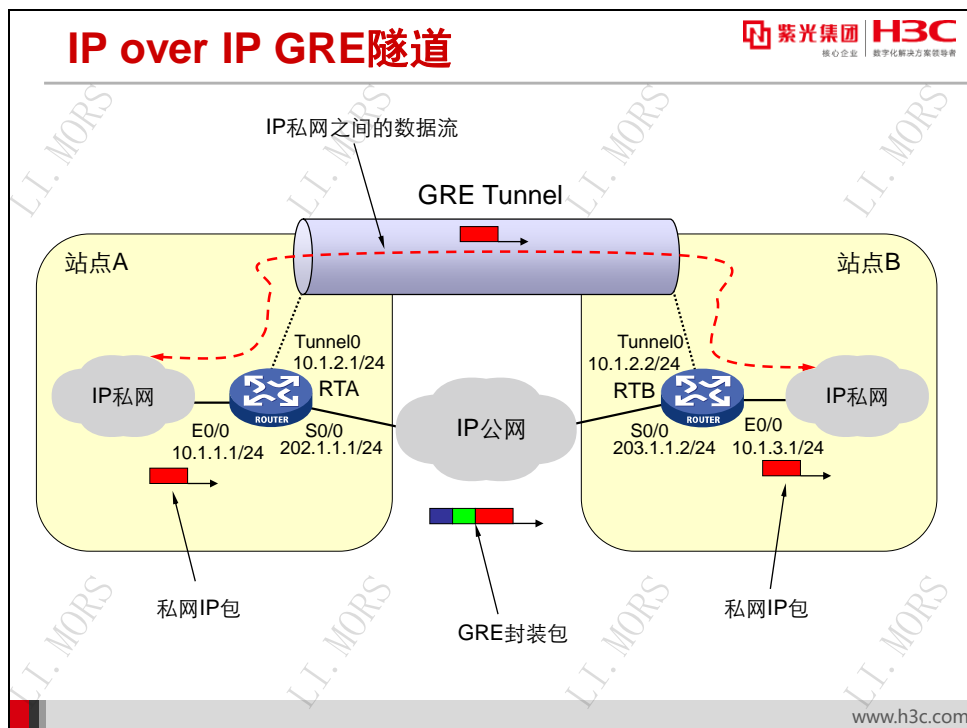
由于 IP 网络的普遍应用，主要的 GRE VPN 部署多采用以 IP 同时作为载荷协议和承载协议的 GRE 封装，又称为 IP over IP 的 GRE 封装。企业在总部与分支之间部署 GRE VPN，通过公共 IP 网络传送内部 IP 网的数据，从而实现网络层的 Site-to-Site VPN。

IP 用协议号 47 标识 GRE 头。当 IP 头中的 Protocol 字段值为 47 时，说明 IP 包头后面紧跟的是 GRE 头。GRE 用以太网协议类型 0x0800 标识 IP，当 GRE 头的 Protocol Type 字段值为 0x0800 时，说明 GRE 头后面紧跟的是 IP 头。

这种封装结构正是最为普遍的 GRE VPN 应用，也是本章的讨论重点。在后续讨论中，如无特别说明，所称的 GRE 隧道都是 IP over IP 的 GRE 隧道。

9.4 GRE隧道工作流程

9.4.1 GRE 隧道构成



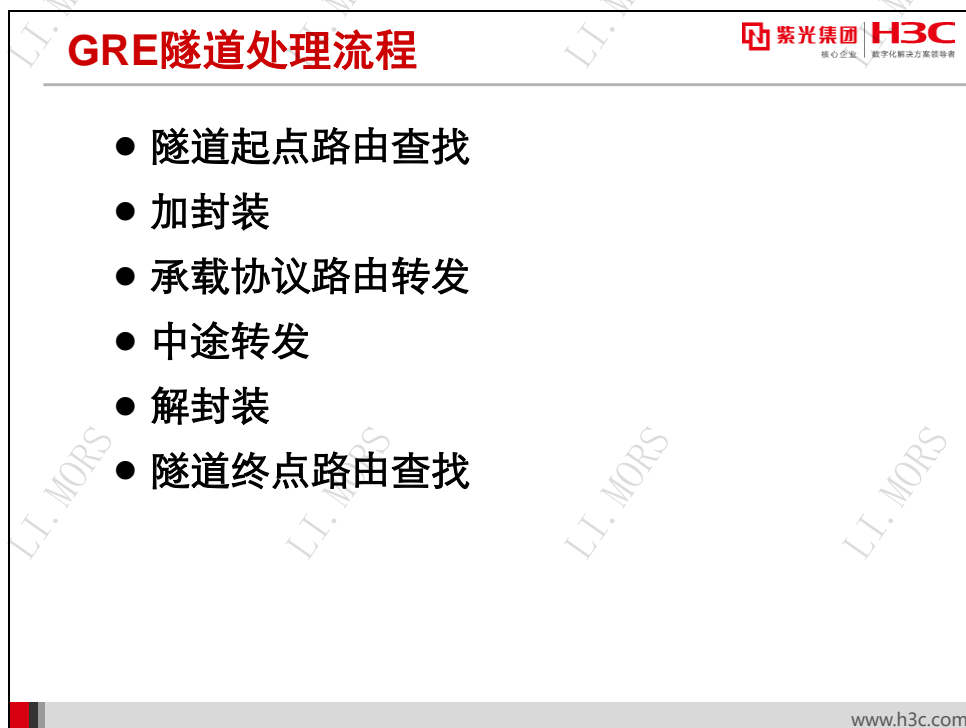
为了使点对点的 GRE 隧道像普通链路一样工作，路由器引入了一种称为 Tunnel 接口的逻辑接口。在隧道两端的路由器上各自通过物理接口连接公共网络，并依赖物理接口进行实际的通信。两个路由器上分别建立一个 Tunnel 接口，两个 Tunnel 接口之间建立点对点的虚拟连接，就形成了一条跨越公共网络的隧道。物理接口具有承载协议的地址和相关配置，直接服务于承载协议；而 Tunnel 接口则具有载荷协议的地址和相关配置，负责为载荷协议服务。当然实际的载荷协议包需要经过 GRE 封装和承载协议封装，再通过物理接口传送。

图示为典型的 IP over IP 的 GRE 隧道的系统构成。站点 A 和站点 B 的路由器 RTA 和 RTB 的 E0/0 和 Tunnel0 接口均具有私网 IP 地址，而 S0/0 接口具有公网 IP 地址。此时，要从站点 A 发送私网 IP 包到站点 B，经过的基本过程如下：

- RTA 根据私网 IP 包的目标地址，查找路由表，找到一个出站接口；
- 如果出站接口是 GRE VPN 的 Tunnel0 接口，RTA 即根据配置，对私网 IP 包进行 GRE 封装，再加以公网 IP 封装，变成一个公网 IP 包，其目的是 RTB 的公网地址；
- RTA 根据封装的公网 IP 包头目标地址，再次查找路由表，将数据包经物理接口 S0/0 发出；
- 此数据包穿越 IP 公共网，到达 RTB；

- RTB 接收到数据包后，由于其目的地址为 RTB，且 IP 包头中的协议号为 47，RTB 根据源地址将该数据包交给对应的 Tunnel0 接口，由 GRE 模块进行解封装处理；
- RTB 解开数据包的 GRE 封装后，根据得到的原始私网 IP 包目的地址再进行下一步的路由查找，最终通过 E0/0 将私网 IP 包发送到站点 B 的私网去。

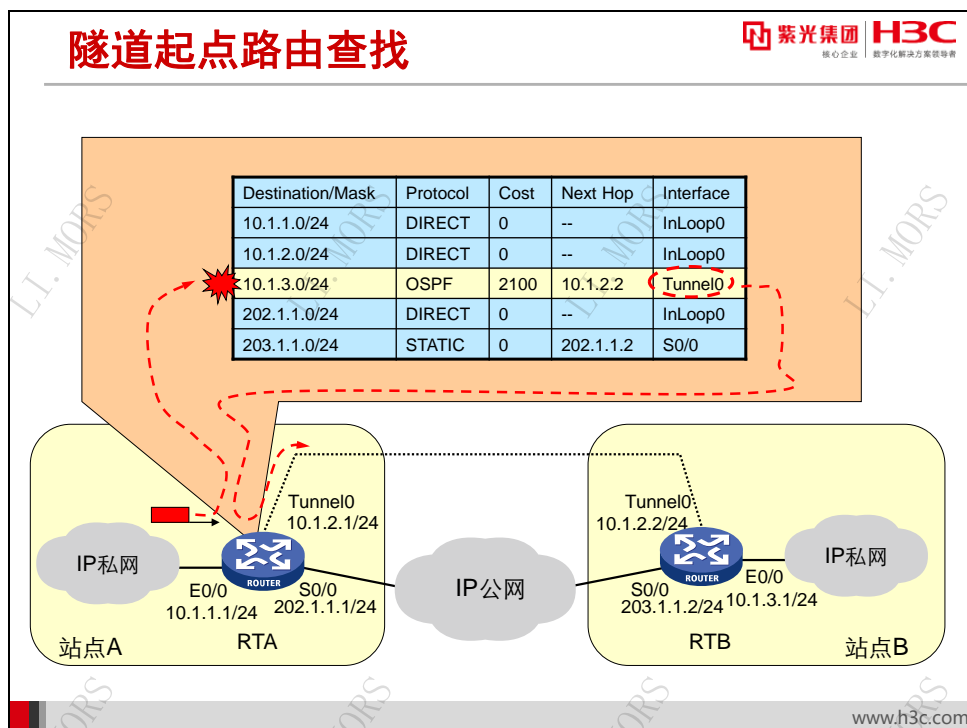
9.4.2 GRE 隧道处理流程



GRE 隧道的工作过程包括以下基本步骤：

- 隧道起点路由查找
- 加封装
- 承载协议路由转发
- 中途转发
- 解封装
- 隧道终点路由查找

9.4.3 隧道起点路由查找

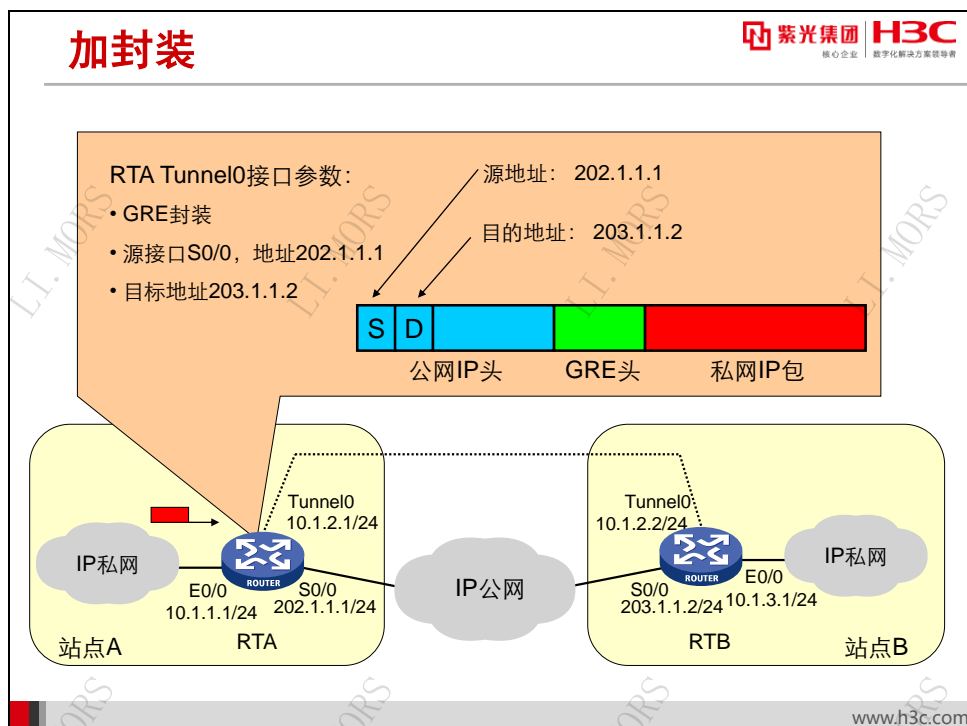


作为隧道两端的 RTA 和 RTB 必须同时具备连接私网和公网的接口，本例中分别是 E0/0 和 S0/0；同时也必须各具有一个虚拟的隧道接口，本例中是 Tunnel0。

当一个私网 IP 包到达 RTA 时，如果其目的地址不属于 RTA，则 RTA 需要执行正常的路由查找流程。RTA 查看 IP 路由表，结果有以下可能：

- 若找不到匹配表项，则丢弃此包；
- 若匹配一条出站接口为普通接口的路由表项，则执行正常转发流程；
- 若匹配一条出站接口为 Tunnel0 的路由表项，则执行 GRE 封装和转发流程。

9.4.4 加封装



假设此私网数据包的路由查找过程已完成，出站接口为 Tunnel0，则此数据包应该由 Tunnel0 接口发出。但 Tunnel0 接口是虚拟的，无法直接发送数据，所有数据包必须由物理接口发出。因此在转发之前，必须将此数据包用 GRE 封装在一个 IP 公网数据包中。

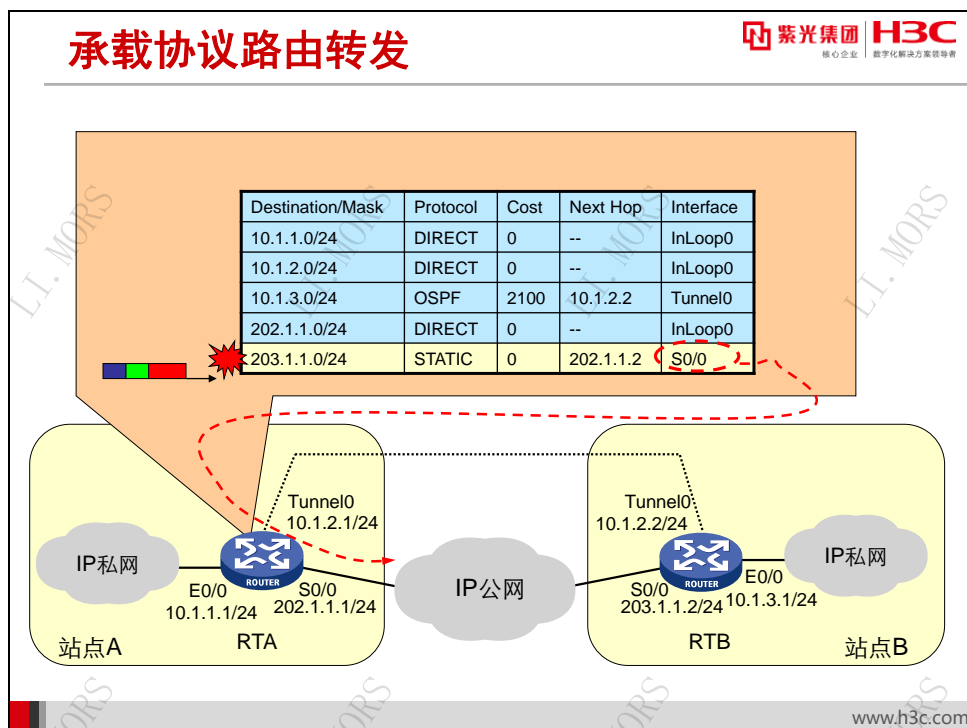
要执行 GRE 封装，RTA 需要从 Tunnel0 接口的配置中获得一系列参数：

- RTA 首先得知需要使用 GRE 封装格式，于是在原私网 IP 包前添加 GRE 头，并填充适当的字段。
- 同时 RTA 获知一个源地址和一个目标地址，作为最后构造的公网 IP 包的源地址和目标地址。这个源地址通常是 RTA 与 IP 公网相连的接口地址，例如 RTA 接口 S0/0 的地址；目标地址通常是隧道终点 RTB 与 IP 公网相连的接口地址，例如 RTB 接口 S0/0 的地址。当然，这两个地址在两台路由器上必须是一一对应的，也就是说在 RTA 和 RTB 上应该有呈镜像关系的端点地址配置。另外，RTA 和 RTB 双方的这两个公网地址必须是互相路由可达的。

之后，RTA 利用这两个地址，为 GRE 封装包添加公网 IP 头，并填充其它适当的字段。

这样，一个包裹着 GRE 头和私网 IP 包的公网 IP 包——也就是承载协议包——就形成了。接下来要执行的是将这个数据包真正地发送至公网。

9.4.5 承载协议路由转发

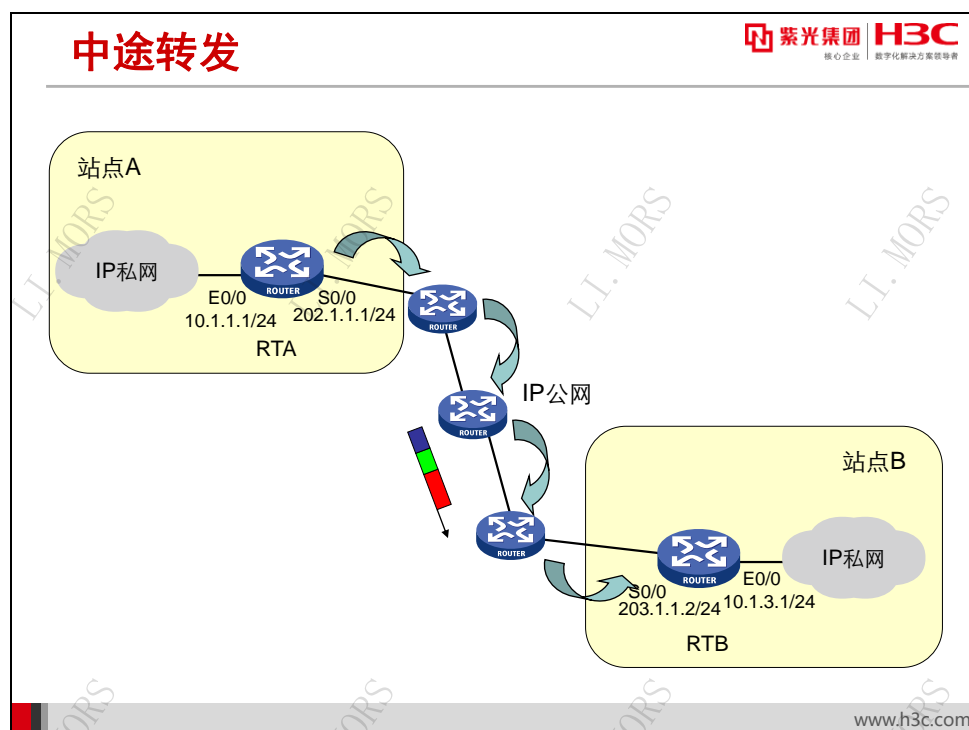


RTA 针对这个公网 IP 包再次进行常规路由表查找。类似地，查找的结果可能有：

- 若找不到匹配表项，则丢弃此包；
- 若匹配一条路由表项，则执行正常转发流程；

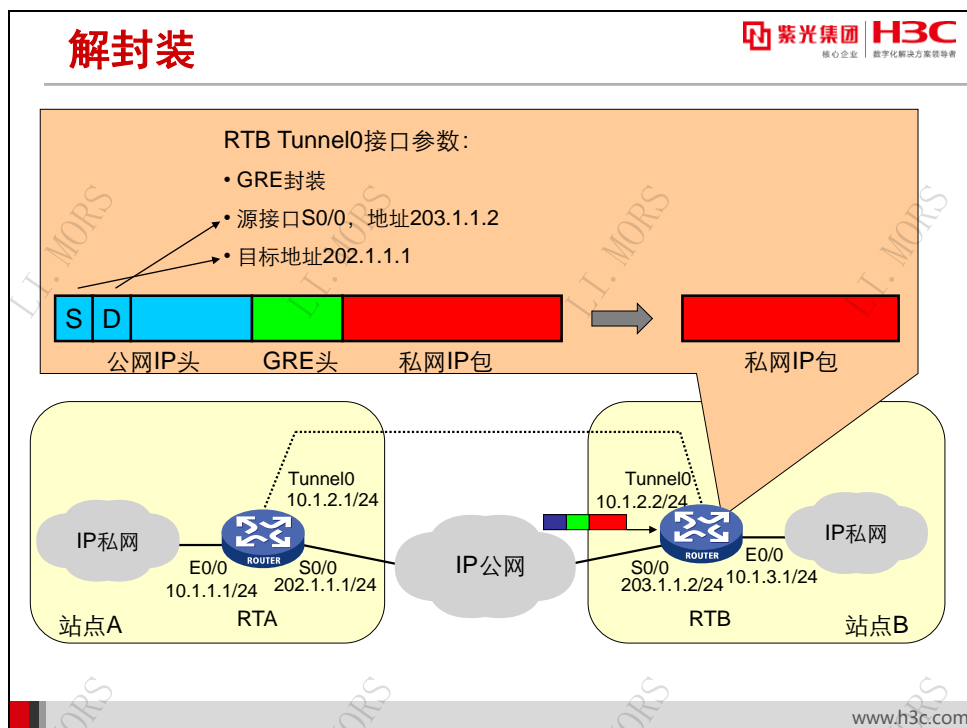
假设 RTA 找到一条匹配的路由，则根据这条路由的下一跳地址转发此包。当然，不能排除存在递归查找的可能，但这些过程与普通的 IP 路由查找和转发没有区别，所以不再讨论。

9.4.6 中途转发



数据报文从 RTA 发出后, 这个 IP 包必须通过公共网络, 到达 RTB。假设 RTA 和 RTB 具有公网 IP 可达性, 中途路由器仅需依据公网 IP 包头执行正常的路由转发即可。

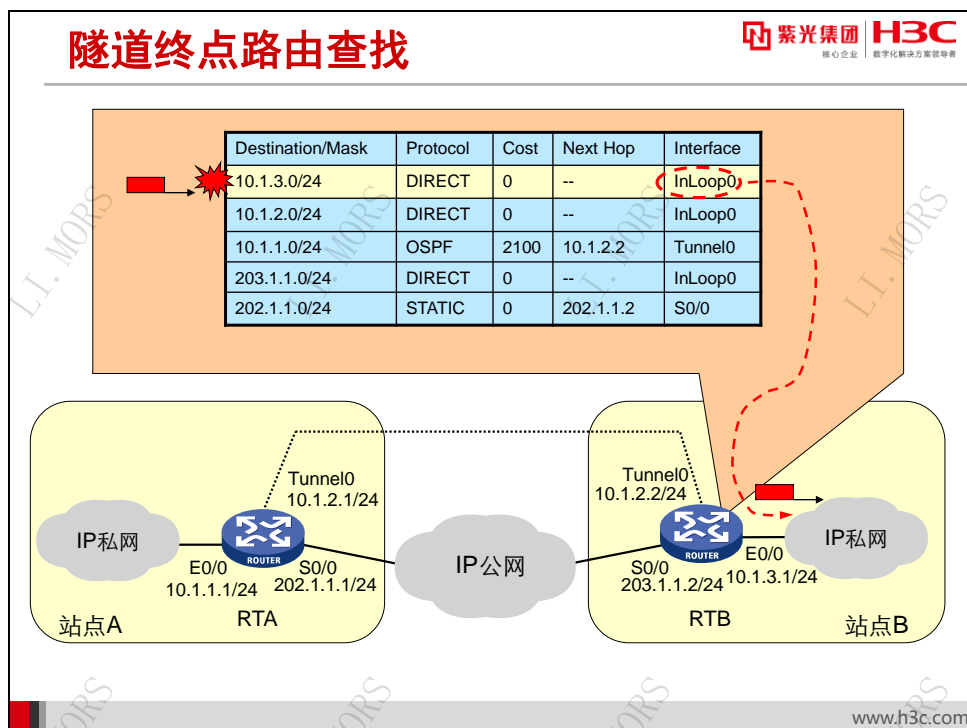
9.4.7 解封装



这个公网 IP 包到达 RTB 之后：

- RTB 检查数据包目的 IP 地址，发现此数据包的目标是自己的本地接口地址；
- RTB 检查公网 IP 头，发现上层协议号是 47，表示此载荷为 GRE 封装；
- RTB 解开公网 IP 头，检查 GRE 头，若无错误发生，则解开 GRE 头；
- RTB 根据公网 IP 包头目的地址，将得到的私网 IP 包提交给相应的 Tunnel 接口，就如同这个数据包是由 Tunnel 接口收到的一样。本例中的 Tunnel 接口是 Tunnel0。

9.4.8 隧道终点路由查找



Tunnel 接口收到这个私网 IP 包后，处理方法与普通接口收到 IP 包时完全相同。如果这个私网 IP 包的目的地址属于 RTB，则 RTB 将此包解开并转给上层协议处理；如果这个 IP 包的目的地址不属于 RTB，则 RTB 需要执行正常的路由查找流程。RTB 查看 IP 路由表，结果有以下可能：


- 若找不到匹配表项，则丢弃此包；
- 若匹配一条路由表项，则执行正常转发流程。

在本例中，数据包将从出接口 E0/0 转发至站点 B 的 IP 私网中。

9.5 部署GRE VPN的考虑因素

9.5.1 GRE VPN 的特点

GRE VPN的特点



紫光集团 H3C
核心企业 | 数字化解决方案领导者

- 优点
 - 可以用当前最为普遍的IP网络作为承载网络
 - 支持多种协议
 - 支持路由协议和IP组播
 - 配置简单，容易部署
- 缺点
 - 点对点隧道
 - 静态配置隧道参数
 - 部署复杂连接关系时代价巨大
 - 缺乏安全性
 - 不能分隔地址空间

www.h3c.com

使用 GRE 隧道实现的 VPN 实现具有很多优点：

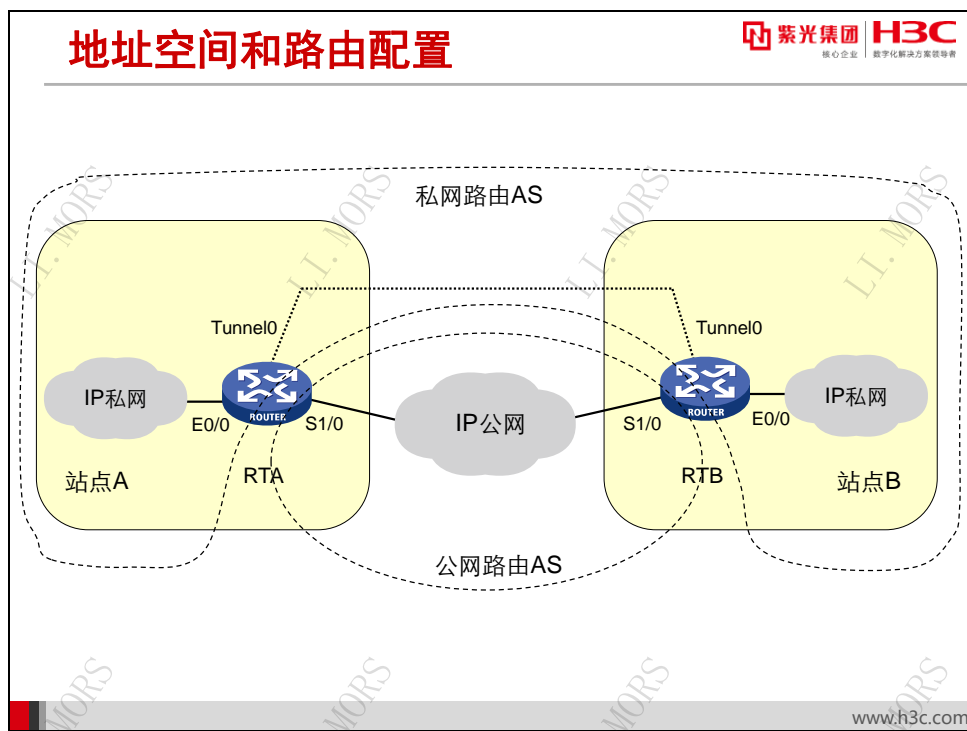
- GRE VPN 可以用当前最为普遍的 IP 网络（包括互联网）作为承载网络，因而可以最大程度地扩展 VPN 的范围。
- Internet 是一个纯粹的 IP 网络，任何非 IP 网络层协议都不会被 Internet 路由器承认，也不能得到路由。然而，很多情况下，企业仍然会使用一些遗留或特殊的其它网络层协议，例如 IPX 等。GRE 封装可以支持多种协议。GRE VPN 可以承载多种上层协议载荷，从而可以跨越公共网使用一些传统和特殊协议。
- GRE VPN 并不局限于单播报文的传送。事实上，任何需要从 Tunnel 接口发出的数据包均可以获得 GRE 封装并穿越隧道。这使 GRE VPN 能支持 IP 动态路由协议和应用越来越广泛的 IP 组播路由技术。
- 另外，GRE VPN 没有复杂的隧道建立和维护机制，因此可以说是最容易理解、最易于部署、最容易维护的 VPN 技术之一。

但是，GRE VPN 也具有很多不足之处：

- 首先，GRE 隧道是一种点对点隧道，在隧道两端建立的是点对点连接，隧道双方地位是平等的，因而只适用于站点对站点的场合。

- 同时，GRE VPN 要求在隧道的两个端点上静态配置隧道接口，并指定本端和对端地址。要想修改隧道配置，必须同时手工修改两端的参数。
- 当需要在所有站点间建立直接的 Full-mesh 连接时，必须在每一个站点上指定所有其它隧道端点的参数。当站点数量较大时，部署和修改 GRE VPN 的代价是呈平方数量级增加的。
- GRE VPN 只提供有限的差错校验、序列校验、验证等机制，并不提供数据加密等服务，必须使用 IPSec 等其它技术才能获得足够的安全性。
- 从收到数据包开始，到数据包转发结束，GRE 隧道端点路由器必须两次查找路由表。但是实际上路由器只有一个路由表。也就是说，当使用 IP over IP 方式时，公网和私网接口实际上不能具有重合的地址。因此 GRE 隧道并不能真正分割公网和私网，不能实现互相独立的地址空间。

9.5.2 地址空间和路由配置



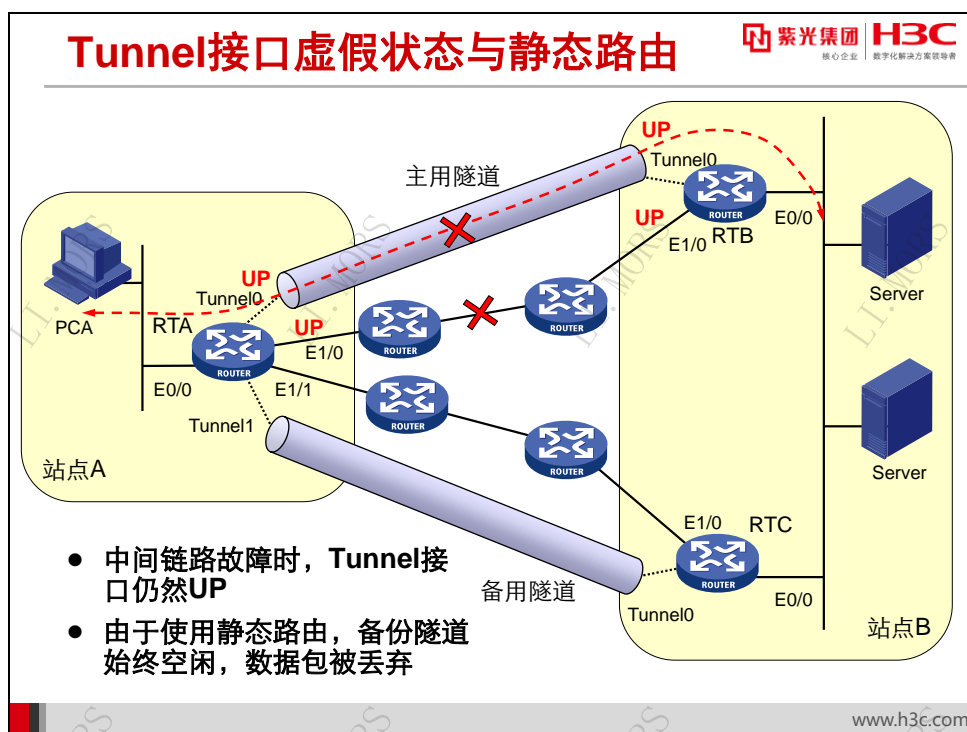
GRE 是一种 VPRN 技术，但每一个运行 GRE 的路由器只有一个路由表，公网与私网之间只能通过不同的路由加以区分。因此，公网和私网的 IP 地址空间不能重合。但公网和私网路由策略是不同的。实际上，对隧道端点路由器来说：

- 其连接到私网的物理接口和 Tunnel 接口属于私网路由 AS，它们采用一致的私网路由策略。
- 其连接到公网的物理接口属于公网路由 AS，它必须与公网使用一致的路由策略。

企业连接到 IP 公网的边缘路由器通常从 IP 公网获得一个公网路由，以保证隧道两端路由器的物理接口的可达性。而为私网转发数据的 Tunnel 接口则可以使用静态路由或动态路由协议获得对方站点的私网路由：

- 静态路由配置：需手工配置到达目的 IP 私网网段（不是 Tunnel 的目的地址，而是未进行 GRE 封装的报文的目的地址所属网段）的路由，下一跳是对端 Tunnel 接口的地址。在 Tunnel 的两端都要进行这些配置。
- 动态路由配置：需将隧道和私网作为一个自治系统对待，在 IP 私网接口和 Tunnel 接口上启动相应的动态路由协议。例如，如果图示的 IP 私网要求运行 OSPF，则应对 RTA 和 RTB 的 Tunnel0 接口均运行 OSPF 保证 RTA 和 RTB 互相学习到对方站点的私网路由。

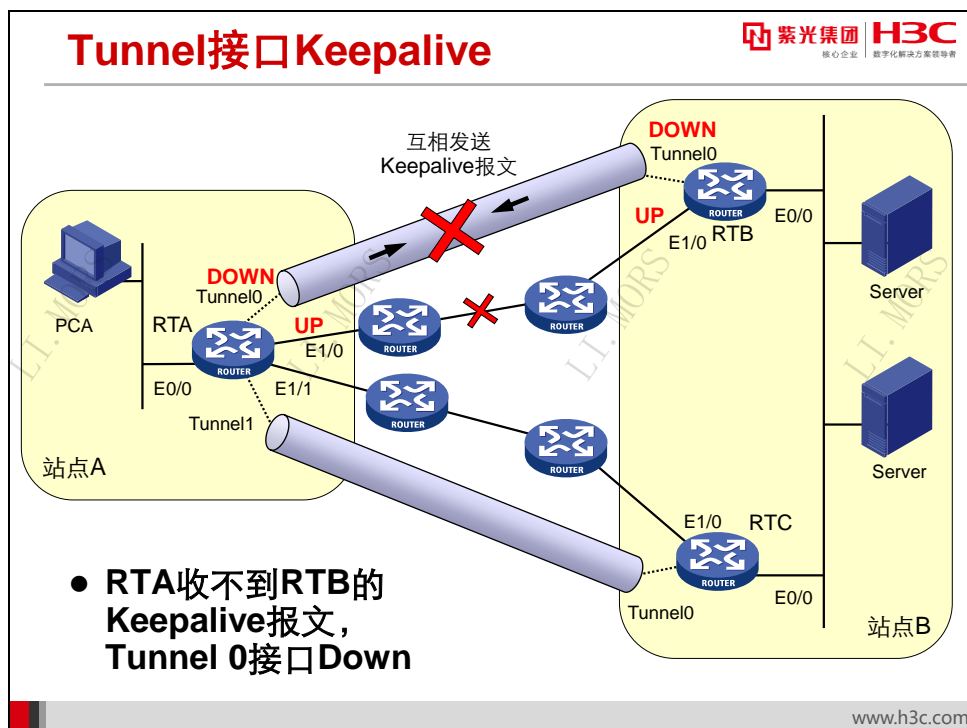
9.5.3 Tunnel 接口 Keepalive



GRE 隧道根据手工的配置启动。但是，GRE 本身并不提供对隧道状态的检测和维护机制。默认情况下，系统根据隧道源物理接口状态设置 Tunnel 接口状态。

如图，隧道两端的物理接口状态正常，但在隧道经过的物理路径上有一个中间链路发生故障，由于 RTA 的接口 E1/0 状态仍然 up，Tunnel0 接口的状态也会保持 up。如果使用静态路由，则 RTA 上的路由表不会发生任何变化。因此，即使存在备用的隧道，隧道封装包仍会由主用隧道发出，随后在途中被丢弃。

因此，要为 GRE VPN 配置静态路由，就需要有一种手段维护隧道的状态，从而实现故障探测和路由备份的目的。



Tunnel 接口 Keepalive 功能允许路由器探测并感知隧道的实际工作情况，并随之修改 Tunnel 接口的状态。启动了 Keepalive 功能后，路由器会从 Tunnel 接口周期性发送 Keepalive 报文。默认情况下，一旦路由器连续 3 次收不到对方响应的 Keepalive 报文，即认为隧道不可用，随即将 Tunnel 接口的状态置为 Down。


这样，以此 Tunnel 接口为出接口的静态路由表项就会从路由表中消失，避免造成路由错误。

如果使用路由协议，则由于路由协议自身可以动态发现并适应网络的变化，Keepalive 功能不再是必需的。

9.6 GRE VPN配置

9.6.1 GRE VPN 基本配置

GRE VPN基本配置



紫光集团 H3C
核心企业 | 数字化解决方案领导者

- 创建Tunnel接口，并进入其接口视图

```
[Router] interface tunnel interface-number mode gre
```

- 指定Tunnel的源端

```
[Router-Tunnel0] source { ip-address | interface-type interface-number }
```

- 指定Tunnel的目的端

```
[Router-Tunnel0] destination ip-address
```

- 设置Tunnel接口的IP地址

```
[Router-Tunnel0] ip address ip-address { mask | mask-length }
```

www.h3c.com

要配置 GRE 隧道，必须首先创建 GRE 模式的 Tunnel 接口，才能在 Tunnel 接口上进行其它功能特性的配置。当删除 Tunnel 接口后，该接口上的所有配置也将被删除。

要创建 Tunnel 接口，请在系统视图下使用命令：

interface tunnel interface-number mode gre

interface-number 为设定的 Tunnel 接口号。但实际可建的 Tunnel 数目受到设备类型、版本、接口总数及内存状况的限制。

要删除 Tunnel 接口，请在系统视图下使用命令：

undo interface tunnel interface-number

缺省情况下，路由器上未创建 Tunnel 接口。

在创建 Tunnel 接口后，还要指明 Tunnel 隧道的源端地址和目的端地址，即发出和接收 GRE 报文的实际物理接口地址。Tunnel 的源端地址与目的端地址唯一标识了一个隧道。这些配置在 Tunnel 两端必须配置。要设置 Tunnel 接口的源端地址，请在 Tunnel 接口视图下使用命令：

source { ip-address | interface-type interface-number }

如果使用 `source` 命令指定了一个接口，则系统会以此接口为源端接口，以该端口地址为源端地址。

要设置 Tunnel 通道的目的端地址，请在 Tunnel 接口视图下使用命令：

destination ip-address


另外还需要设置 Tunnel 接口的网络层地址。一个隧道两端的 Tunnel 接口网络层地址应该位于同一网段上。请在 Tunnel 接口视图下使用命令：

ip address ip-address { mask | mask-length }

除此以外，在源端路由器和目的端路由器上都必须存在经过 Tunnel 转发数据包的路由，这样 GRE 封装后的报文才能正确转发。可以配置静态路由，也可以配置动态路由。

9.6.2 GRE VPN 高级配置

GRE VPN高级配置

 紫光集团 H3C
核心企业 数字化解决方案领导者

- 设置Tunnel两端进行端到端校验
- [Router-Tunnel0] gre checksum
- 设置Tunnel接口的识别关键字
- [Router-Tunnel0] gre key key-number
- 配置Tunnel的Keepalive功能
- [Router-Tunnel0] keepalive [interval [times]]

www.h3c.com

GRE VPN 支持数据校验功能。若 GRE 头中的 Checksum Present 位置位，则校验和有效。发送方将根据 GRE 头及 Payload 信息计算校验和，并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比较，如果一致则对报文进一步处理，否则丢弃。

隧道两端可以根据实际应用的需要，选择启用或禁用校验和功能。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，但对发送的报文计算校验和；相反，如果本端没有配置校验和而对端已配置，则本端将对对端发来的报文进行校验和检查，但对发送的报文不计算校验和。缺省情况下，禁止 Tunnel 两端进行端到端校验。要配置校验和，在 Tunnel 接口视图下使用命令：

gre checksum

若 GRE 头中的 Key Present 位置位，则收发双方将使用隧道识别关键字进行验证。只有 Tunnel 两端设置的识别关键字完全一致时才能通过验证，否则将丢弃报文。要设置 GRE 隧道接口的密钥并启动验证，在 Tunnel 接口视图下使用命令：

gre key key-number

其中 *key-number* 可取值为 0~4294967295 之间的整数。缺省情况下，Tunnel 不使用验证。

要设置 Tunnel 的 Keepalive 功能，在 Tunnel 接口视图下使用命令：


keepalive seconds times

其中 *seconds* 参数指定 Keepalive 报文发送周期，取值范围为 1~32767，缺省为 10 秒。*times* 参数指定判断隧道中断所需的 Keepalive 报文的传送次数，取值范围为 1~255，缺省为 3 次。

配置了该命令后，设备会从 Tunnel 口定期发送 GRE 隧道的 Keepalive 报文。如果超时时间内没有收到隧道对端的 Keepalive 响应报文，则本端继续重新发送 Keepalive 报文。如果超过 *times* 参数规定的传送次数后仍然没有收到对端的 Keepalive 响应报文，则把本端 Tunnel 接口的协议状态置为 Down。如果 Tunnel 口处于 Down 状态时收到对端的 Keepalive 确认报文，Tunnel 接口的状态将转换为 Up，否则继续保持 Down 状态。缺省情况下不启动 GRE 的 Keepalive 功能。

9.6.3 GRE VPN 信息的显示和调试

display interface tunnel命令



核心企业 数字化解决方案领导者

```

<H3C>display interface tunnel 0
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1476
Internet Address is 10.1.2.1/24 Primary
Tunnel source 202.1.1.1, destination 203.1.1.2
Tunnel keepalive disabled
Tunnel TTL 255
Tunnel protocol/transport GRE/IP
GRE key disabled
Checksumming of GRE packets disabled
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

```

www.h3c.com

执行 **display interface tunnel** 命令可以显示配置后 GRE 隧道接口的运行情况，通过查看显示信息以验证配置的效果：

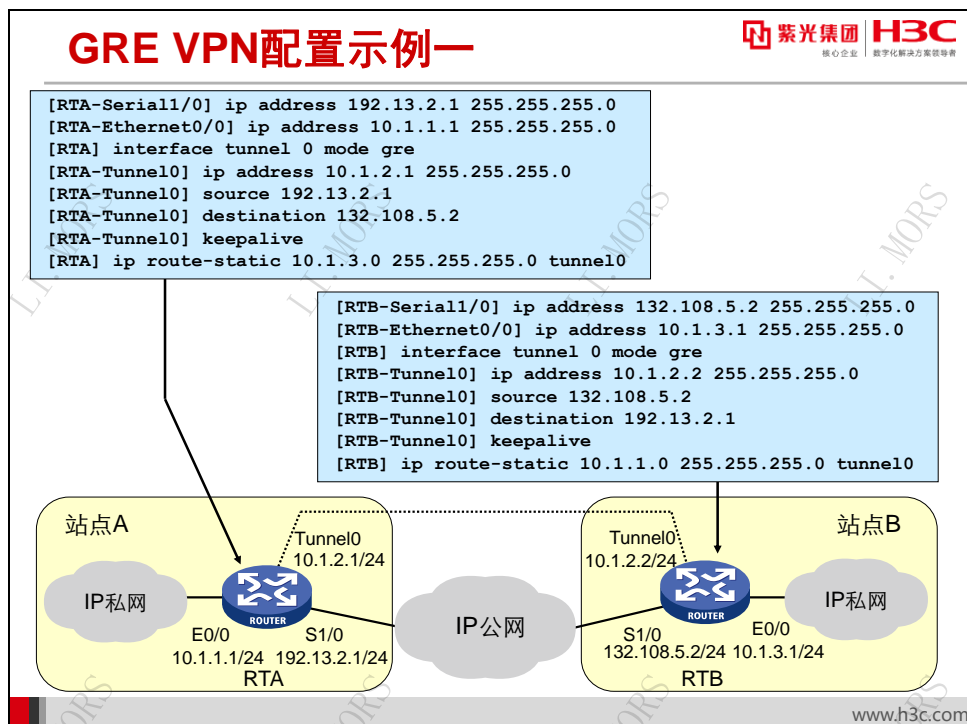
display interface tunnel [number]

显示 Tunnel 接口工作状态的输出信息，例如：

```
<Router> display interface tunnel 0
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1476
Internet Address is 10.1.2.1/24 Primary
Tunnel source 202.1.1.1, destination 203.1.1.2
Tunnel keepalive disabled
Tunnel TTL 255
Tunnel protocol/transport GRE/IP
  GRE key disabled
  Checksumming of GRE packets disabled
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

以上信息表示 Tunnel0 接口处于 Up 状态，MTU 为 1476 字节，Tunnel0 的 IP 地址为 10.1.2.1/24，源端地址为 202.1.1.1，目的地地址为 203.1.1.2，没有启动验证功能，也没有启动校验功能。

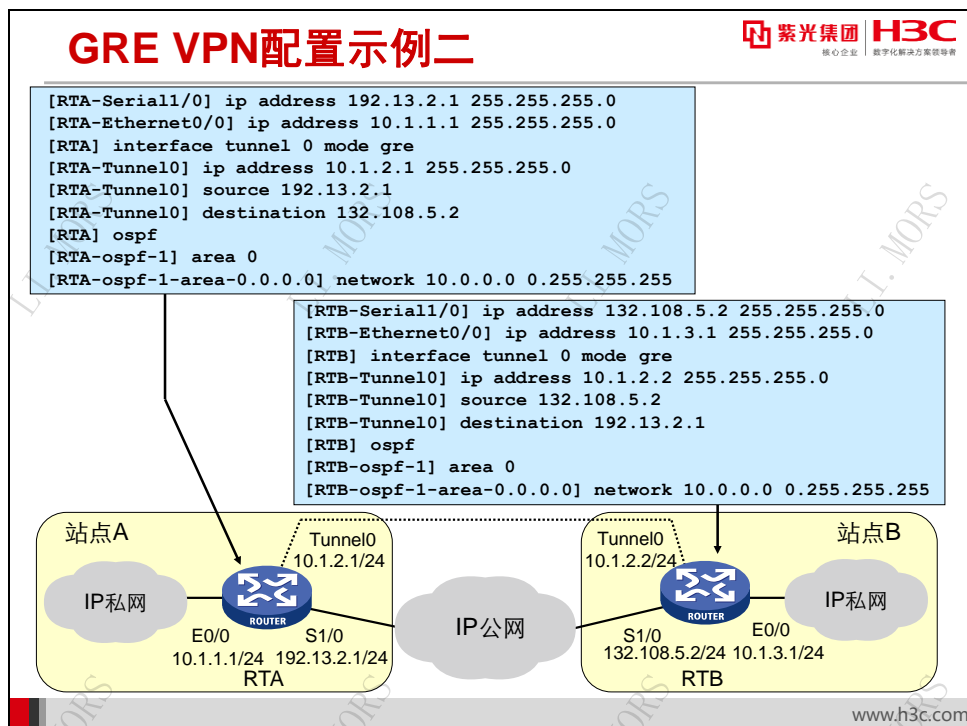
9.6.4 GRE VPN 配置示例一



如图，站点 A 和站点 B 运行 IP 协议，并使用私有地址空间 10.0.0.0/8。两个站点通过在路由器 RTA 和路由器 RTB 之间使用 GRE 隧道，跨越公网实现互联。在本例中，由于使用静态路由，RTA 和 RTB 都启动了 Keepalive 功能，并采用默认参数。

本例并未列出保证 RTA 到 RTB 可达性的相关路由配置，但是这种可达性的要求是隐含的，也是必须保证的。

9.6.5 GRE VPN 配置示例二



在本例中，私网 AS 使用了 OSPF 路由协议，因此在 RTA 和 RTB 上启用了 OSPF 协议，并在 Tunnel0 接口和 E0/0 接口启动了 OSPF。

本例并未列出保证 RTA 到 RTB 可达性的相关路由配置，但是这种可达性的要求同样是必须保证的。

9.7 本章总结

本章总结

- GRE VPN是由GRE隧道构成的Site-to-Site VPN
- GRE隧道通过GRE封装实现
- GRE VPN简单而容易部署，支持多协议，但其不能分隔地址空间，且安全性较差

www.h3c.com

9.8 习题和解答

9.8.1 习题

习题 5 道，测试点包括：GRE 隧道工作流程、GRE VPN 的特点、GRE 配置命令等

1. 下列关于 GRE 的说法正确的是（ ）
A. GRE 封装只能用于 GRE VPN B. GRE 封装并非只能用于 GRE VPN
C. GRE VPN 不能分隔地址空间 D. GRE VPN 可以分隔地址空间
2. 承载网 IP 头以（ ）标识 GRE 头。
A. IP 协议号 47 B. 以太协议号 0x0800
C. UDP 端口号 47 D. TCP 端口号 47
3. 关于 GRE 隧道 Tunnel 接口的配置，以下说法正确的是（ ）
A. Tunnel 接口是一种逻辑接口，需要手工创建
B. 配置 GRE 隧道时，在隧道两个端点路由器上为 Tunnel 接口指定的源地址必须相同
C. 配置 GRE 隧道时，在隧道两个端点路由器上为 Tunnel 接口指定的目的地址必须相同
D. 配置 GRE 隧道时，在隧道两个端点路由器上为 Tunnel 接口指定的 IP 地址必须相同
4. 要配置 GRE 隧道 Tunnel 接口的 Keepalive 时间为 45s，应使用命令（ ）
A. tunnel keepalive 45 B. keepalive 45
C. gre keepalive 45 D. gre tunnel keepalive 45
5. 指定 Tunnel 的源端为 1.1.1.2，应在 Tunnel 接口视图下使用命令（ ）
A. source address 1.1.1.2 B. destination address 1.1.1.2
C. source 1.1.1.2 D. destination 1.1.1.2

9.8.2 习题答案

1、BC 2、A 3、A 4、B 5、C

第10章 L2TP VPN

移动用户和临时办公场所通常不具备永久性的连接，因此常使用 PSTN/ISDN 等拨号技术接入企业内部网络。但这种方式可能需要支付高昂的长途拨号费用。而作为 Access VPN 的 L2TP（Layer 2 Tunneling Protocol，二层隧道协议）正好可以在降低费用的同时满足接入企业内部网络的需要。L2TP 支持“独立 LAC”和“客户 LAC”两种模式，使其既可用于实现 VPDN，也可用于实现站点到站点（Site-to-Site）VPN 业务。

10.1 本章目标

课程目标

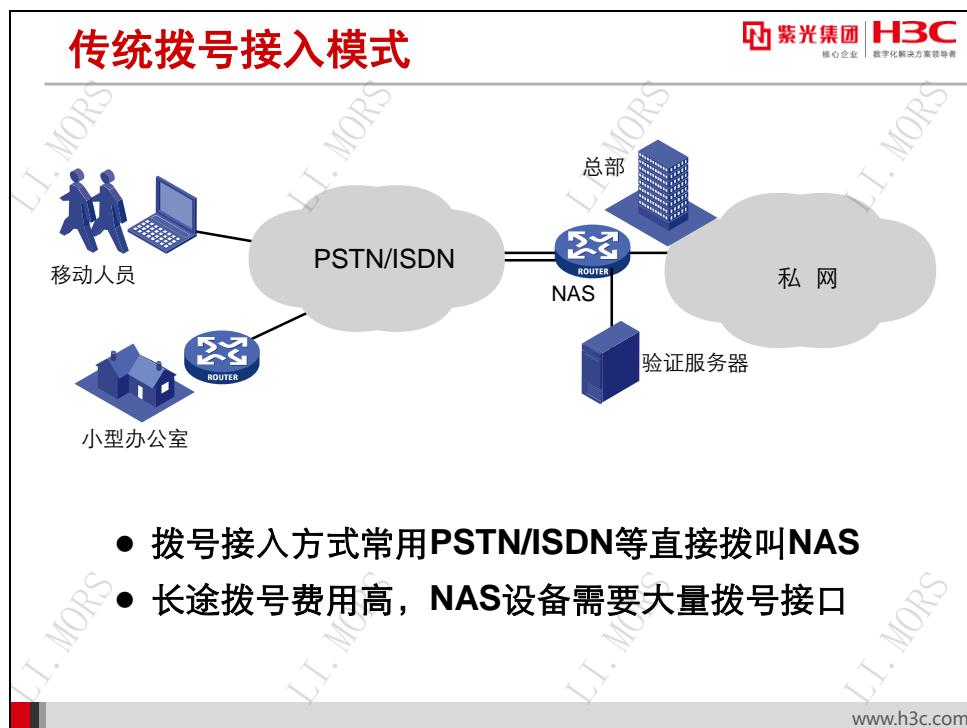
学习完本课程，您应该能够：

- 理解企业网远程用户接入的需求，描述 L2TP 的特点、适用场合及工作原理
- 配置独立 LAC 模式和客户 LAC 模式 L2TP
- 用 display 命令获取 L2TP 配置和运行信息



10.2 L2TP VPN概述

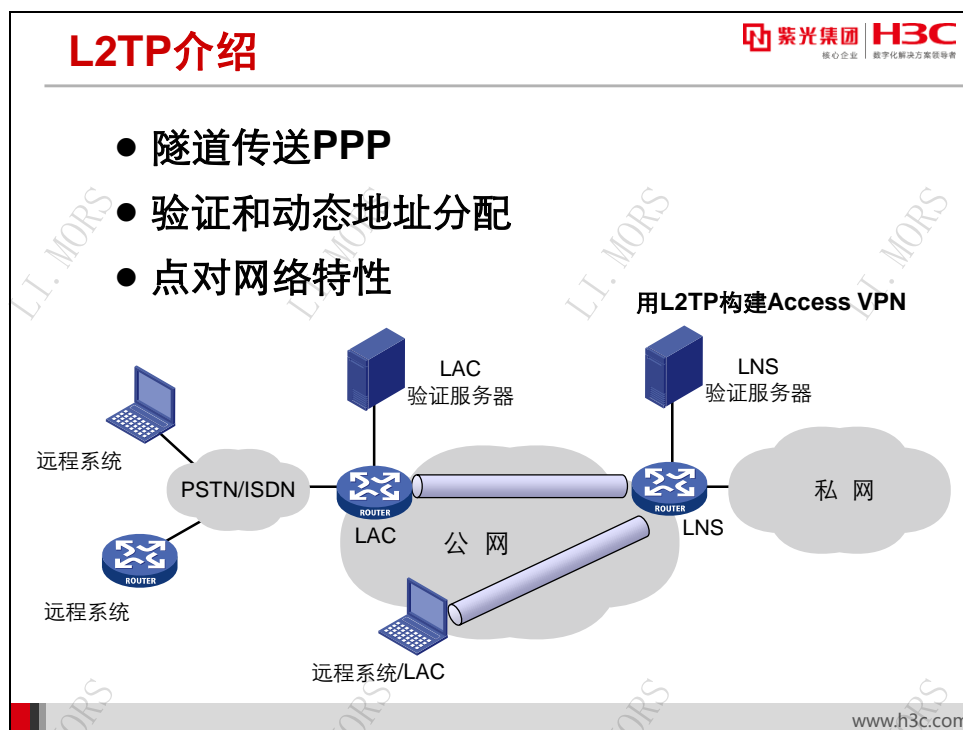
10.2.1 传统拨号接入模式



在传统的拨号接入方式中，小型办公室或漫游用户通过 PSTN/ISDN 之类的技术，直接对 NAS（Network Access Server，网络访问服务器）发起远程呼叫，建立二层的点到点链路。用户端设备与 NAS 之间通常使用 PPP（Point to Point Protocol，点到点协议）协议，以实现验证并支持多种网络层协议。

这样的接入方式需要消耗大量的长途呼叫费用，企业还必须为 NAS 设备配备大量的拨号接入端口。

10.2.2 L2TP 介绍



IETF 在 RFC 2661 中定义了 L2TP 协议（Layer Two Tunnel Protocol，二层隧道协议）。L2TP 提供了对 PPP 链路层数据包的隧道（Tunnel）传输支持。它允许二层链路端点和 PPP 会话点驻留在不同设备上，并且采用分组交换网络技术进行信息交互，从而扩展了 PPP 模型。L2TP 协议结合了 L2F 协议和 PPTP 协议的各自优点，成为 IETF 有关二层隧道协议的工业标准。

L2TP 是一种典型的 Access VPN 技术。使用 L2TP 时，用户不必长途拨号直接连接到总部路由器，而是使用 PSTN/ISDN 拨号、xDSL 等方式直接连接到 ISP（Internet Service Provider，因特网服务提供商）位于本地的 POP（Point Of Presence，存在点），然后由 ISP 设备跨越 Internet 建立 L2TP 隧道，将用户接入到组织内部网络。而具备直接 Internet 连接的移动用户也可以在�有 LAC 的情况下，以客户端 LAC 的方式访问总部资源。这样，用户可以节约大量的长途拨号费用，并可以方便地接入组织内部网络。

L2TP 支持对用户和隧道的验证，也支持对客户端的动态地址分配。使用 L2TP，企业不仅可以通过 PPP 连接自行验证用户身份并分配 IP 地址，而且可以通过 ISP 的 LAC 执行额外的 AAA 验证。企业还可以在防火墙和内部服务器上实施访问控制，从而确保了安全性。

L2TP 具备点到网的特性，特别适合单个或少数远程用户接入企业中心网络的情况。企业的小型远程办公室和出差人员可以花费较少的本地接入费用接入其组织中心。

由于 L2TP 隧道由 PPP 触发，承载 PPP 帧，因而其适应性强，可以支持任意的网络层协议。

但是 L2TP 不提供任何加密能力，跨越公共网络的数据很容易遭到窃听或篡改。因此在保密性要求比较高的情况下，需要结合其它加密手段——例如 IPSec——保证数据安全性。

在 L2TP 协议体系中，用户通过二层链路连接到一个访问集中器（Access Concentrator），然后访问集中器将 PPP 协议帧通过隧道传送到 NAS，这个隧道可以基于一个共享的网络，甚至是 Internet。这样，物理链路终止在集中器上，而 PPP 链路却可以延伸到遥远的目标站点。

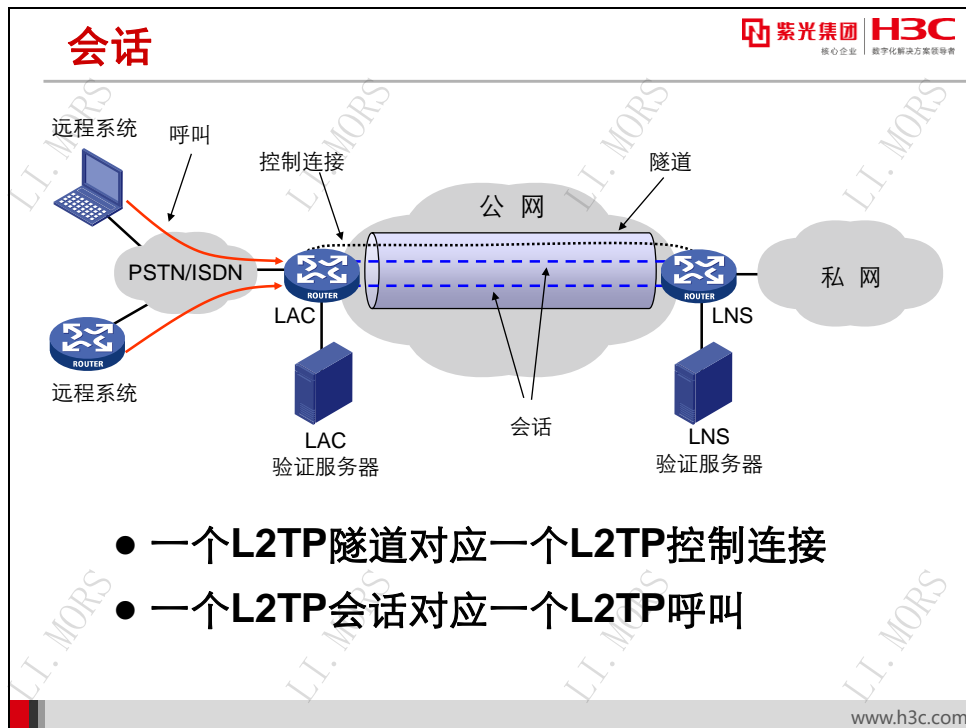
与 PPP 模块配合，L2TP 支持本地和远端的验证、授权和计费（Authentication, Authorization and Accounting, AAA）功能，也可根据需要采用全用户名，用户域名和用户拨入的特殊服务号码来识别是否为 VPN 用户。同时，L2TP 也支持对接入用户动态分配地址。

主要的 L2TP 组件包括：

- **远程系统（Remote System）**：远程系统是一台终端计算机，或者是一台路由器。远程系统连接到诸如 PSTN 一类的远程接入网络上。它既可以是呼叫发起者，也可以是呼叫接受者。又称为拨号客户（Dial-up Client）或者虚拟拨号客户（Virtual Dial-up Client）。
- **LAC（L2TP Access Concentrator，L2TP 访问集中器）**：LAC 是 L2TP 的隧道端点之一。LAC 与 LNS 互为 L2TP 隧道的对等节点，L2TP 隧道在 LAC 和 LNS 之间建立，由 LAC 和 LNS 共同维护。LAC 把从远程系统接收的报文封装后发给 LNS，把 LNS 发来的报文解封后发给远程系统。LAC 的位置处于远程系统与 LNS 之间，或者就存在于远程系统上。
- **LNS（L2TP Network Server，L2TP 网络服务器）**：LNS 是 L2TP 的隧道端点之一。LAC 与 LNS 互为 L2TP 隧道的对等节点，L2TP 隧道在 LAC 和 LNS 之间建立，由 LAC 和 LNS 共同维护。同时，LAC 和 LNS 也是会话（Session）的终结点。
- **NAS（Network Access Server，网络访问服务器）**：NAS 是一个常规的抽象概念。NAS 是远程访问网络的接入点，为远程客户提供接入服务。它既可以是 LAC，也可以是 LNS。

10.3 L2TP工作原理

10.3.1 L2TP 概念术语



L2TP 协议中还有一些需要掌握的术语，包括：

- 呼叫 (Call)
- 隧道 (Tunnel)
- 控制连接 (Control Connection)
- 控制消息 (Control Message)
- 会话 (Session)

L2TP 呼叫 (Call) 是指远程系统到 LAC 的连接。例如，一个远程系统用 PSTN 拨号连接到 LAC，则这个连接就是一个 L2TP 呼叫。呼叫成功之后，如果隧道存在，LAC 就会在隧道中发起 L2TP 会话；如果隧道不存在，就会先触发隧道的建立，然后再发起会话。

L2TP 隧道 (Tunnel) 存在于一对 LAC 与 LNS 之间。一个隧道内包括一个控制连接 (Control Connection) 以及 0 个或多个会话 (Session)。隧道承载 L2TP 控制消息 (Control Messages) 以及封装后的 PPP 帧。PPP 帧以 L2TP 封装格式传送。

L2TP 控制连接 (Control Connection) 存在于 L2TP 隧道内部，在 LAC 和 LNS 之间建立。控制连接的作用是建立、维护和释放隧道中的会话以及隧道本身。

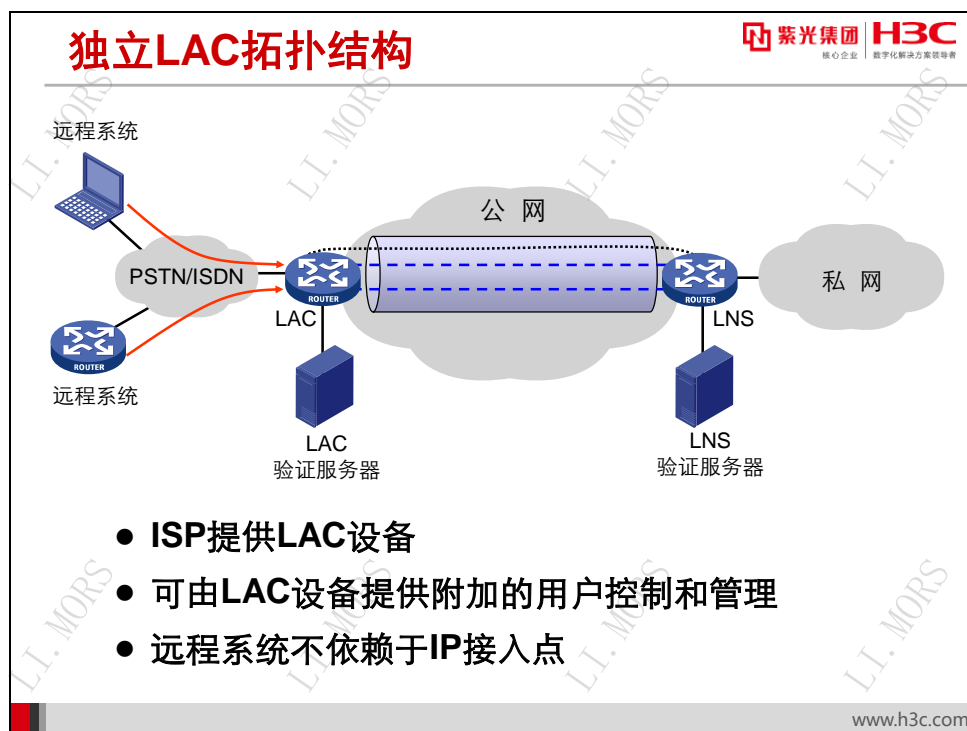
L2TP 控制消息（Control Messages）是在 LAC 和 LNS 之间交换的。可以看作是 L2TP 隧道的带内消息。控制消息被用于 LAC 和 LNS 的沟通，以便建立、维护和释放隧道中的会话以及隧道本身。L2TP 的控制消息中包含了 AVP（Attribute Value Pair，属性值对）。AVP 是一系列属性及其具体值，控制消息通过其携带的 AVP 使隧道两端设备能沟通信息，管理会话和隧道。

L2TP 是面向连接的，可以为其传送的控制信息提供一定的可靠性。LAC 和 LNS 维护远程系统与 LAC 的每一个呼叫的状态和信息。

当一个远程系统建立了到 LNS 的 PPP 连接时，一个 L2TP 会话（Session）就会相应地存在于 LAC 和 LNS 之间。来自这个呼叫的 PPP 帧在相应的会话中被封装，并传送给 LNS。因此，L2TP 会话与 L2TP 呼叫是一一对应的。一对 LAC 和 LNS 也同时维护在两者之间的会话信息和状态。

10.3.2 L2TP 拓扑结构

根据不同的应用需求，L2TP 可使用两种不同的拓扑结构——独立 LAC 方式和客户 LAC 方式。



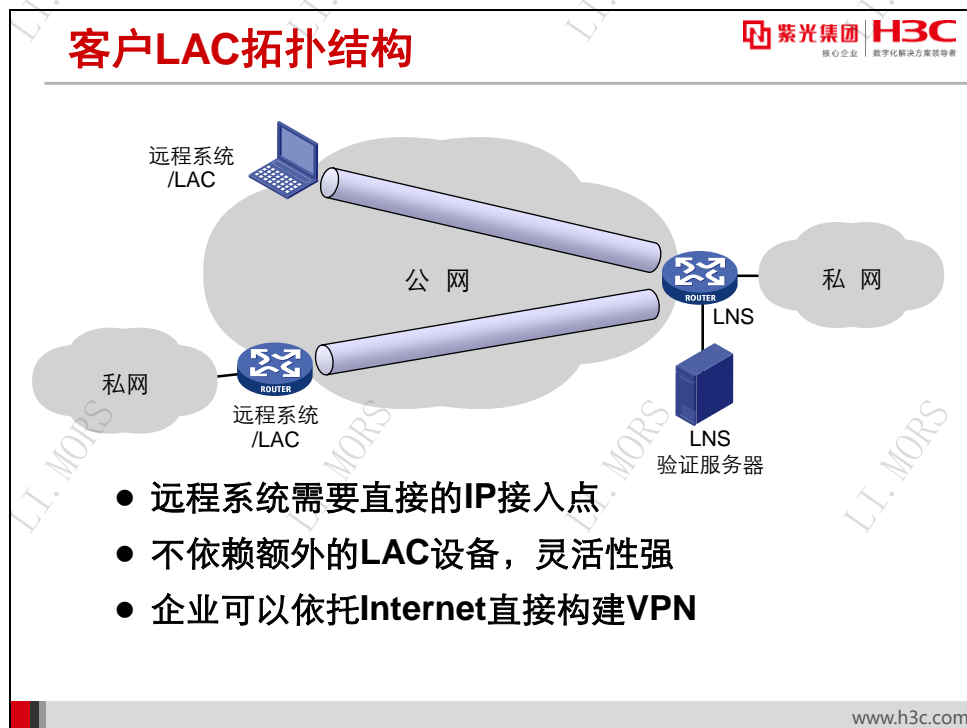
在独立 LAC 方式中，远程系统通过一个远程接入方式接入到 LAC 中，由 LAC 对 LNS 发起隧道并建立会话。

例如，一个企业的员工通过 PSTN/ISDN 接入位于 ISP 的 LAC 设备。该 LAC 提供用户接入的 AAA 服务，并通过 Internet 向位于企业总部的 LNS 发起建立隧道连接请求，以建立隧道

和会话连接。而企业总部的 LNS 作为 L2TP 企业侧的 VPN 服务器，接收来自 LAC 的隧道和会话请求，完成对用户的最终授权和验证，并建立连接 LNS 和远程系统的 PPP 通道。

这种方式的好处在于，所有 VPN 操作对终端用户是透明的。终端用户不需要配置 VPN 拨号软件，只需要执行普通拨号，一次登录就可以接入企业网络。并且，员工即使不能访问 Internet，只要他能够拨号到 ISP 的 LAC，就可以访问公司资源。用户验证和内部地址分配由私网进行，使用私有地址空间，不占用公共地址。对拨号用户的计费可由 LNS 或 LAC 侧的 AAA 完成。

但这种方式需要 ISP 支持 L2TP 协议，需要验证系统支持 VPDN 属性。



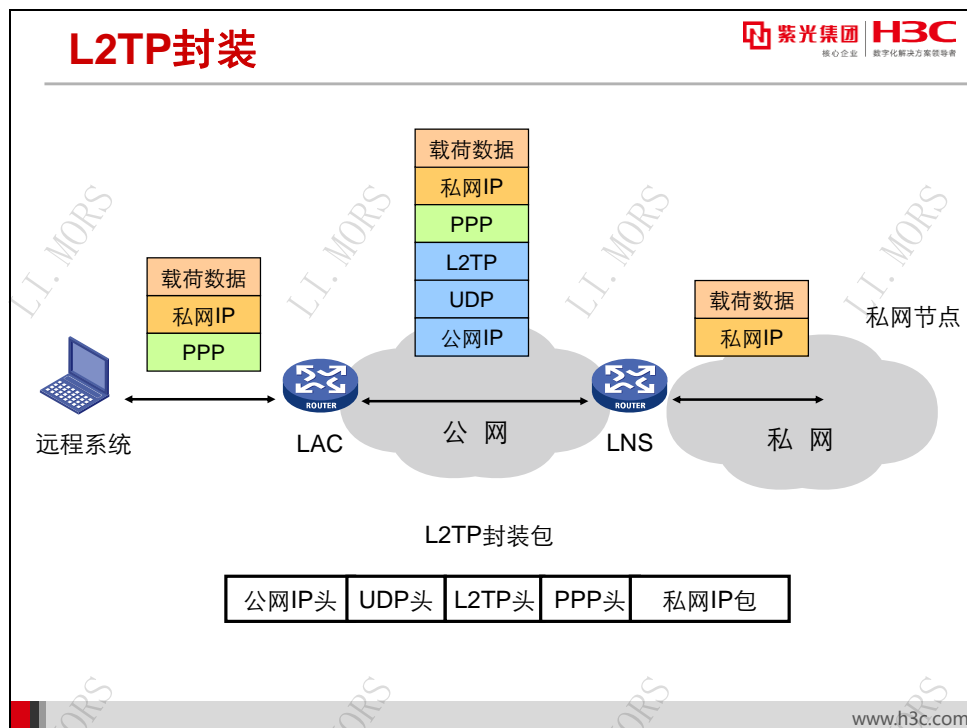
在客户 LAC 方式中，LAC 设备存在于远程系统计算机上。远程系统本身具有 Internet 连接，并采用一个内部机制——例如 VPDN 客户端软件——跨越 Internet 对 LNS 发起呼叫，并建立隧道和会话。

例如，企业员工直连接到 Internet 获得数据通信服务。在员工的计算机上配置 VPN 拨号软件，就可以与总部建立 VPN 连接。用户端计算机同时实现了远程系统和 LAC 的功能，直接与位于企业总部的 LNS 建立隧道和会话。此时，对用户的验证仅由 LNS 侧执行。

这种方式的好处在于，用户上网的方式和地点没有限制，不需依赖 ISP 的独立 LAC 介入，只要客户端具有 Internet 接入能力，就可以实现 VPDN。

但是远程用户需要具备 Internet 连接，并安装专用的客户端软件，与独立 LAC 模式相比较，客户端侧的设置操作更复杂。

10.3.3 L2TP 封装



在 L2TP 隧道中，L2TP 的控制通道和数据通道都采用同样的 L2TP 头格式，只是其中的具体字段有所不同。

L2TP 头以 T (Type) 位表明本消息的类型。值为 1 表示此消息是控制消息，值为 0 表示此消息是数据消息。L2TP 头中的 Tunnel ID 字段是 L2TP 控制连接的标识符，也就是 L2TP 隧道的标识符。Tunnel ID 是在隧道建立时通过 Assigned Tunnel ID AVP 协商的。L2TP 头中的 Session ID 字段用来标识一个隧道中的各个会话。Session ID 是在隧道建立时通过 Assigned Session ID AVP 协商的。

在 IP 网络中，L2TP 以 UDP/IP 作为承载协议，使用 IANA 注册的 UDP 端口 1701。整个 L2TP 报文，包括 L2TP 头及其载荷，都封装在 UDP 中发送。

上图说明了数据包在传输过程中协议栈结构变化和封装过程。

下面以一个用户侧的 IP 报文的传递过程来描述 L2TP 的封装与传输过程：

- 1) 从远程系统向服务器方向发送的原始用户 IP 报文先经过 PPP 封装，发送到 LAC。
- 2) LAC 的链路层将 PPP 帧传递给 L2TP 协议，L2TP 对其添加 L2TP 头，再将其封装入 UDP，并继续封装成可以在 Internet 上传输的公网 IP 包。L2TP 头中标识了用户数据包的相应隧道和会话等参数。此时的结果就是 IP 包中有 PPP 帧，PPP 帧中还有 IP 包。但两个 IP 包的地址不同，用户数据包的 IP 地址是私网地址，而 LAC 生成的公网 IP 包的地址为公网地址。

- 3) 至此完成了 VPN 的私有数据的封装。LAC 将此报文通过公网发送到 LNS。
- 4) LNS 收到 VPN 封装的 IP 报文后，依次将 IP、UDP、L2TP 头去掉，就获得了用户的 PPP 帧，并交送到 PPP 协议进行处理。
- 5) LNS 将 PPP 报文头去掉就可以得到原始 IP 报文，然后可以根据 IP 头执行相应操作，例如提交上层协议处理或转发。

从服务器向远程系统发送数据包的过程与上述描述恰恰相反，这里不再赘述。

可见，依赖公网 IP 包的 L2TP 隧道封装存在于 LAC 与 LNS 之间，而 PPP 封装却存在于远程系统与 LNS 之间，这就相当于在远程系统与 LNS 之间建立了一条直接边接的 PPP 链路。

10.3.4 L2TP 协议操作

L2TP协议操作

- 建立控制连接
- 建立会话
- 转发PPP帧
- Keepalive
- 关闭会话
- 关闭控制连接

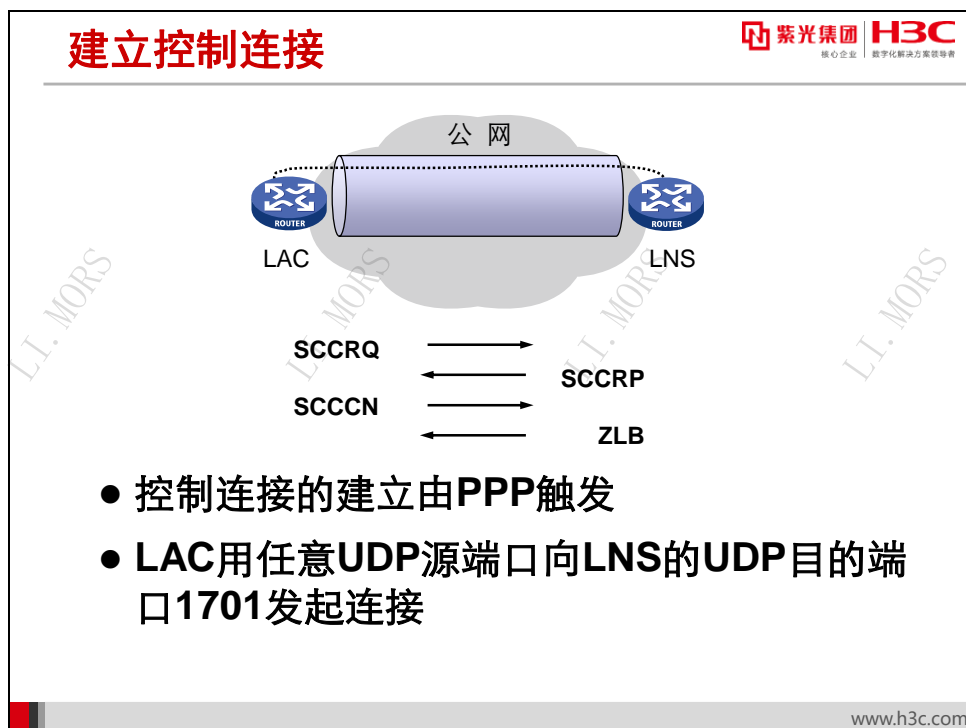


紫光集团 H3C
核心企业 数字化解决方案领导者

www.h3c.com

L2TP 协议的主要操作包括：

- 建立控制连接
- 建立会话
- 转发 PPP 帧
- Keepalive
- 关闭会话
- 关闭控制连接



为了在 VPN 用户和服务器之间传递数据报文，必须首先在 LAC 和 LNS 之间建立传递数据报文的隧道及会话。所以，建立一个控制连接是一切后续操作的基础。在隧道建立过程中，双方需要互相检查对方的身份，并协商一些参数。

远程系统通过 PPP 链路拨叫 LAC 成功后，随即由 PPP 触发 LAC 发起控制连接的建立。LNS 在 UDP 端口 1701 侦听 L2TP 控制连接建立请求。LAC 使用任意 UDP 端口向 LNS 的 UDP 端口 1701 发起控制连接。

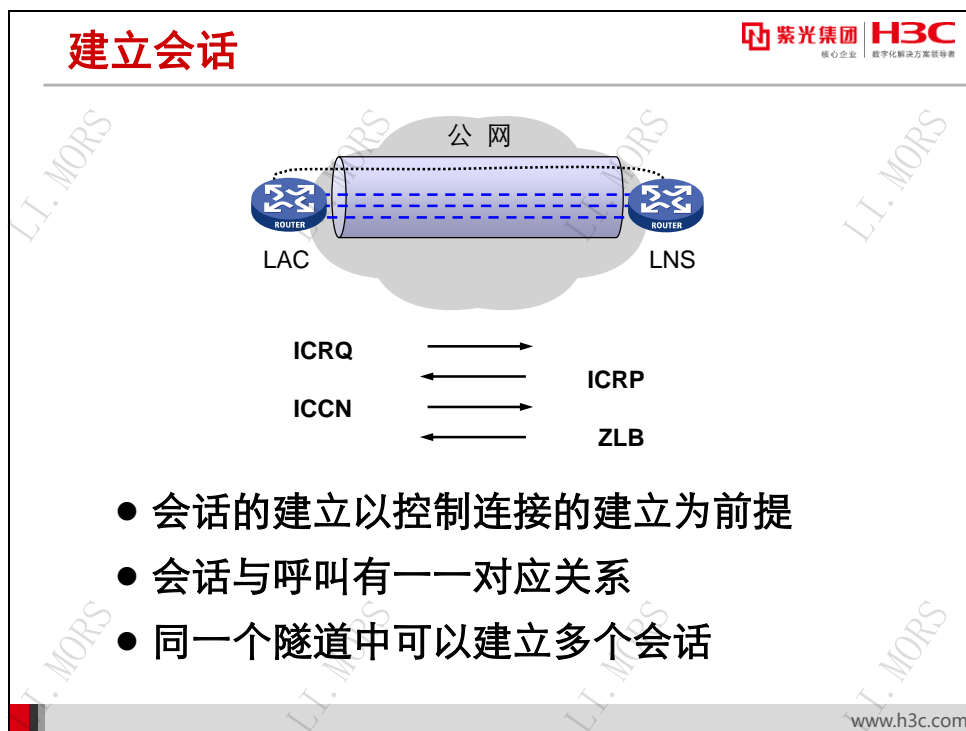
建立控制连接时，通常：

- 首先由 LAC 发送 SCCRQ (Start-Control-Connection-Request, 打开控制连接请求)，发起隧道建立；
- LNS 收到请求后用 SCCRP (Start-Control-Connection-Reply, 打开控制连接应答) 进行应答；
- LAC 在收到应答后返回 SCCCN (Start-Control-Connection-Connected, 打开控制连接已连接) 确认；
- LNS 收到 SCCCN 后，用 ZLB (Zero-Length Body, 零长度体) 消息作为最后应答，隧道建立。

其中 ZLB 消息是一个只有 L2TP 头的控制消息，其作用是作为一个显示确认，以确保控制消息的可靠传递。

在控制连接建立的过程中，L2TP 可以执行一个隧道验证过程。LAC 或 LNS 均可用此方法验证对方的身份。这个验证过程与 CHAP 非常类似，LAC 和 LNS 可以在 SCCRQ 或 SCCRP

消息中添加 Challenge AVP（挑战 AVP），发起验证；接收方必须在 SCCRП 或 SCCCН 消息中以 Challenge Response AVP（挑战响应 AVP）响应验证。如果验证不通过，隧道就无法建立。



为了传送用户数据，在建立了控制连接后，就需要为用户建立会话。多个会话可以复用在一个隧道连接上。

会话的建立是由 PPP 模块触发，如果该会话在建立时没有可用的隧道，那么先建立隧道连接。会话建立完毕后，才开始进行用户数据传输。

会话建立的过程与控制连接的建立过程类似，通常 LAC 首先接收到一个入站呼叫（incoming call），触发会话的建立过程：

- LAC 对 LNS 发送 ICRQ（Incoming-Call-Request，入呼叫请求）发起会话的建立；
- LNS 收到请求后返回 ICRP（Incoming-Call-Reply，入呼叫应答）；
- LAC 收到应答后返回 ICCN（Incoming-Call-Connected，入呼叫已连接）确认；
- LNS 收到 ICCN 后，用 ZLB 消息作为最后应答，会话建立。


LNS 也可以发起会话的建立过程：

- LNS 发送 OCRQ（Outgoing-Call-Request，出呼叫请求）要求建立会话；
- LAC 返回 OCRP（Outgoing-Call-Reply，出呼叫应答）；
- LAC 执行呼叫；

- 呼叫成功后，LAC 返回 OCCN（Outgoing-Call-Connected，出呼叫已连接）进行确认；
- LNS 收到 OCCN 后，用 ZLB 消息作为最后应答，会话建立。

转发PPP帧

- 会话建立后，即可转发PPP帧
- 用Tunnel ID和Session ID区分不同隧道和不同会话的数据



紫光集团 H3C
核心企业 数字化解决方案领导者

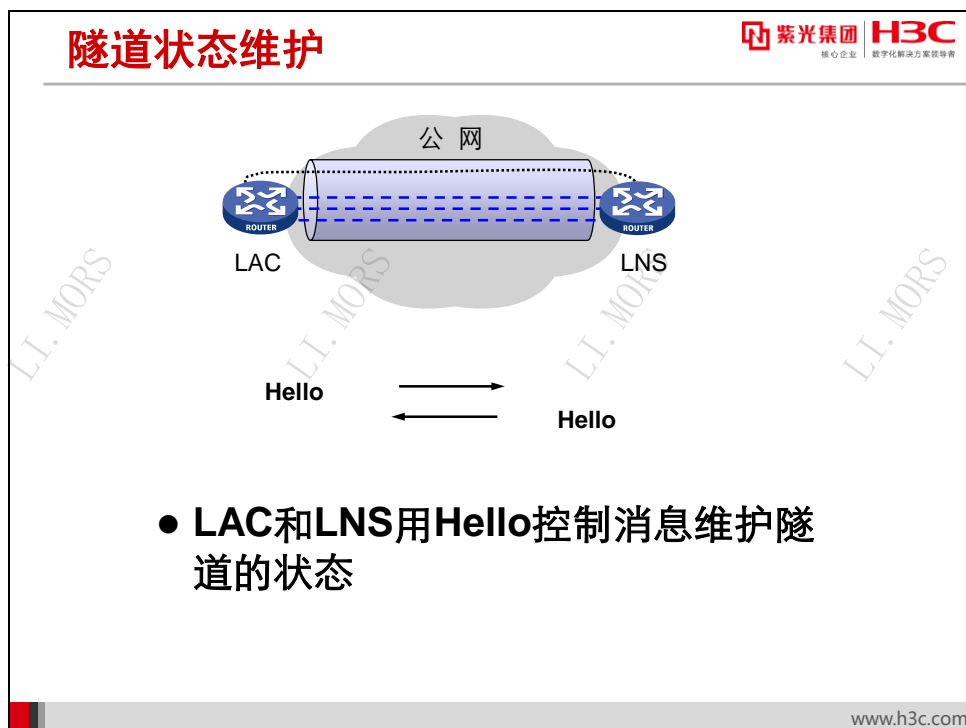
www.h3c.com

一旦会话建立，就可以为用户转发数据了。

用户 IP 包被封装在 PPP 帧中，这些 PPP 帧从远程系统到达 LAC 后，被传递给 L2TP 协议，L2TP 对其添加 L2TP 头，并以 Tunnel ID 和 Session ID 对其隧道和会话属性进行标识，然后再将其封装成 UDP，并继续封装成可以在 Internet 上传输的公网 IP 报文。LAC 将此报文通过公网发送到 LNS。

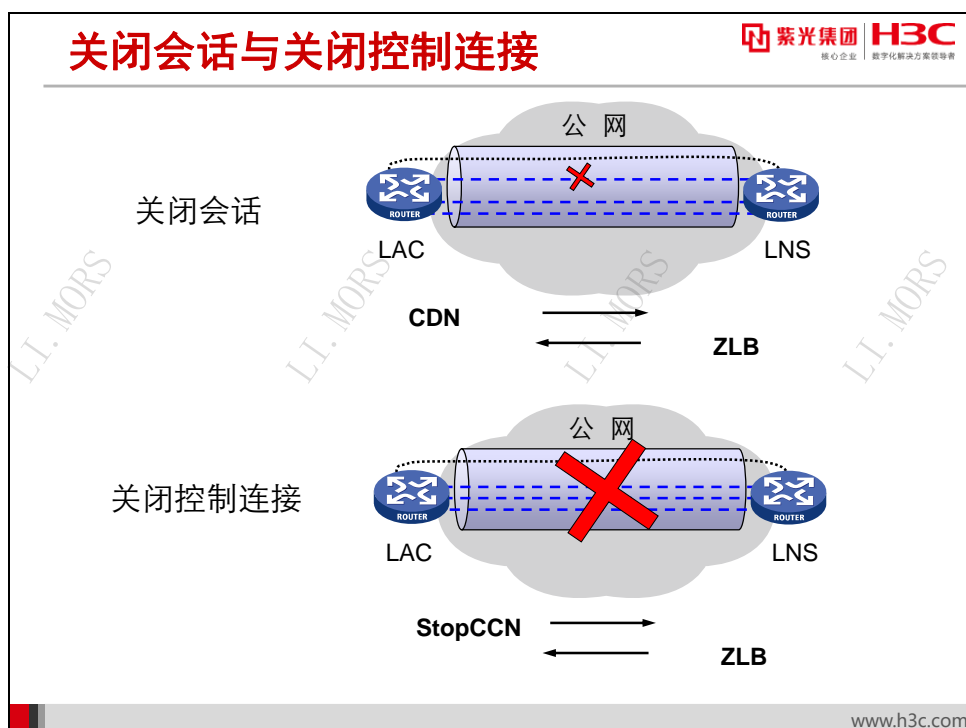
LNS 在收到这些 IP 报文后，依次将 IP、UDP、L2TP 头去掉，就获得了用户的 PPP 帧。LNS 根据相应的 Tunnel ID 和 Session ID 将其递交给正确的处理点（例如一个 virtual-template 接口）的 PPP 协议进行处理。该处理点将 PPP 帧头去掉就可以得到原始私网 IP 报文，然后可以根据 IP 头做相应操作，例如转上层协议处理或继续转发。

相反的方向上执行的操作也是类似的。



为了解隧道的运作情况，检测 LAC 与 LNS 之间的连接故障，L2TP 的 LAC 和 LNS 使用 Hello 控制消息维持彼此的状态。

自最近一次收到的数据或控制消息起开始计算，如果达到一个特定周期时间，则开始发送 Hello 控制消息。如果 Hello 控制消息不能可靠送达，隧道会被关闭。



隧道端点双方均可以要求关闭一个会话。会话的关闭并不影响隧道的状态。

如图所示，若 LAC 试图关闭一个会话，则：

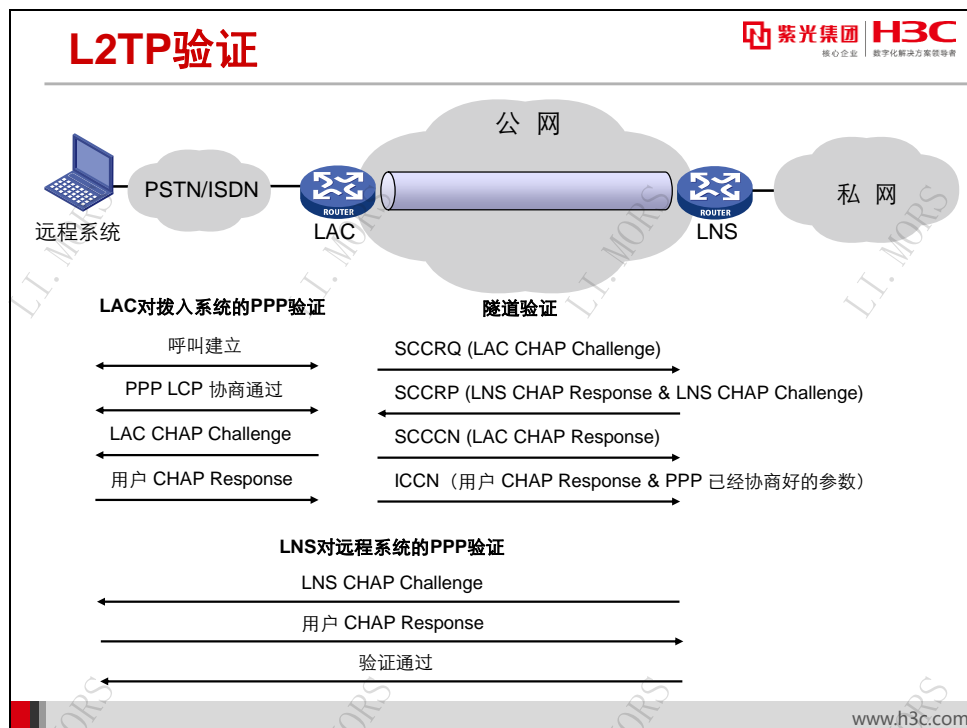
- 其首先发送一个 CDN（Call-Disconnect-Notify，呼叫断开通知）消息，通告对方关闭某条会话；
- 对方收到 CDN 后，以 ZLB 消息作为最后应答，会话关闭。

隧道端点双方均可以要求关闭一个隧道。关闭隧道的同时，该隧道承载的所有会话均会关闭。

如图所示，若 LAC 试图关闭一个隧道，则：

- 其首先发送一个 StopCCN（Stop-Control-Connection-Notification，停止控制连接通知）消息，通告对方关闭控制连接；
- LNS 收到 StopCCN 后，以 ZLB 消息作为最后应答，控制连接关闭。

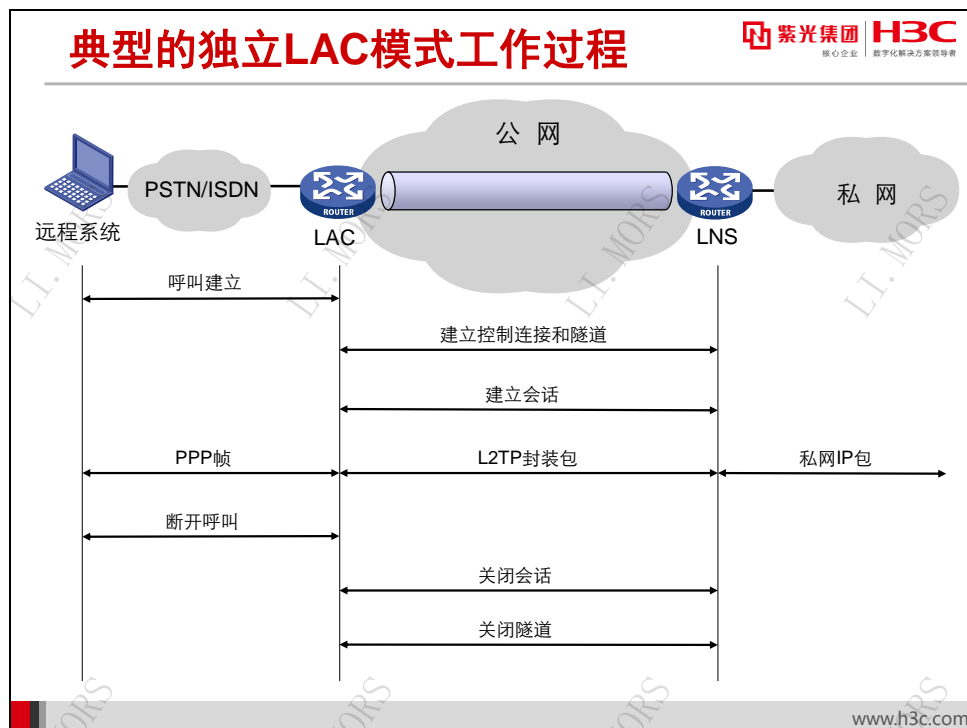
10.3.5 L2TP 验证



L2TP 的验证可以包括三步：

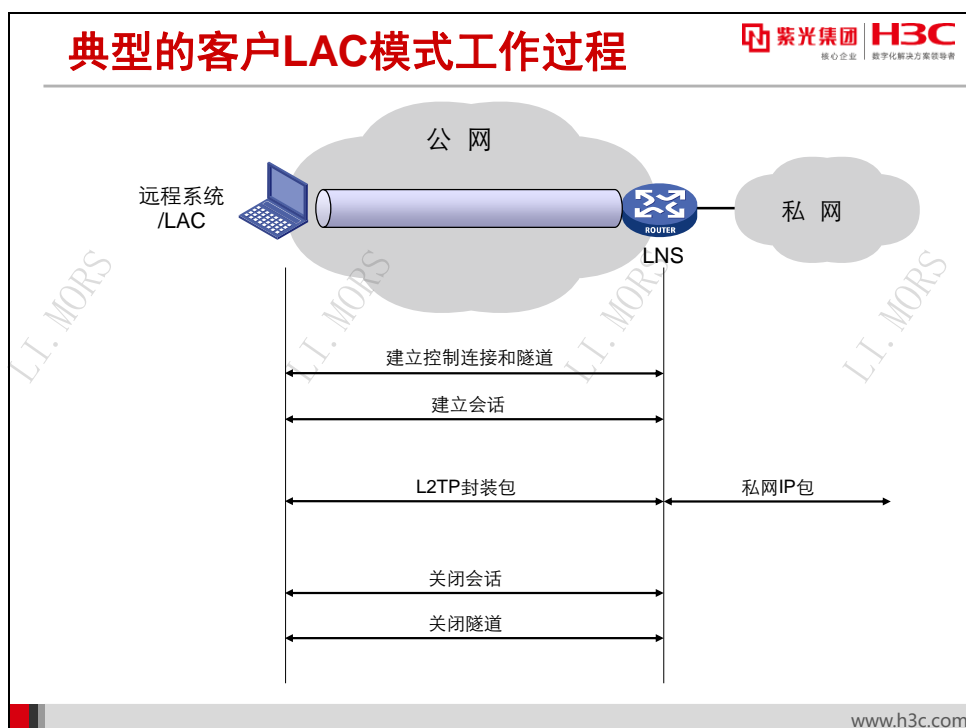
- **对拨入的远程系统的初始 PPP 验证：**在 LAC 与远程系统之间进行，用于验证拨入用户的合法性。可以使用 CHAP 或 PAP 验证。
- **对 LAC 和 LNS 之间隧道的验证：**在 LAC 与 LNS 之间进行，用于验证隧道端点的合法性。采用类似 CHAP 的验证方式。这一验证是可选的。
- **LNS 对远程系统的再次 PPP 验证：**在 LNS 与远程系统之间进行，用于验证远程系统的身份，以便决定其是否能够访问私网资源。这一步验证又可分为下列三种：
 - ◆ **代理验证：**LAC 将它从远程系统得到的所有验证信息及 LAC 端本身配置的验证方式发送给 LNS。
 - ◆ **强制 CHAP 验证：**LNS 直接对远程系统进行 CHAP 验证。
 - ◆ **LCP 重协商：**LNS 将与远程系统重新进行 LCP 协商，并采用相应的虚拟模板接口上配置的验证方式进行验证。

10.3.6 典型 L2TP 工作过程



一个典型的 L2TP 独立 LAC 模式工作过程如图所示：

- 1) 用户端 PC 机对 LAC 发起连接呼叫。PC 机和 LAC 进行 PPP LCP 协商，确认之间的物理链路正常。LAC 对 PC 机提供的用户信息进行 PPP 验证。如果验证通过则呼叫建立。
- 2) LAC 查找该用户对应的 LNS 地址等相关信息，对 LNS 发起控制连接建立请求。LNS 与 LAC 之间可以进行隧道验证。如果验证通过，控制连接即隧道建立成功。
- 3) LAC 要求建立一个会话，以便为拨入的远程系统传输数据。如果使用代理验证，则 LAC 将它从用户得到的所有验证信息及 LAC 端本身配置的验证方式发送给 LNS；如果使用强制 CHAP 验证或强制 LCP 重协商，则 LNS 负责对远程系统再次进行验证。如果验证通过，则会话建立。
- 4) 位于远程系统的用户可以与私网主机进行通信，访问私网内部资源。
- 5) 用户结束资源访问，断开呼叫。
- 6) LAC 向 LNS 请求关闭会话。
- 7) 如果隧道中的所有会话都关闭，且隧道没有必要继续维持，则 LAC 向 LNS 请求关闭隧道。




一个典型的 L2TP 客户 LAC 模式工作过程如图所示：

- 1) 同时作为远程系统和 LAC 的用户端主机需要访问私网资源时，主动向 LNS 发起建立控制连接请求。其与 LNS 之间可以进行隧道验证。如果验证通过，控制连接即隧道建立成功。
- 2) 用户端主机随后请求建立一个会话，以便为拨入的远程系统传输数据。这一阶段同样可以进行必要的验证。如果验证通过，则会话建立。
- 3) 位于远程系统的用户可以与私网主机进行通信，访问私网内部资源。
- 4) 用户断开呼叫时，用户端主机向 LNS 请求关闭会话。
- 5) 用户端主机向 LNS 请求关闭隧道。

10.4 配置独立LAC模式

10.4.1 独立 LAC 模式配置任务

独立LAC模式配置任务

 紫光集团 H3C
核心企业 数字化解决方案领导者

- **配置L2TP基本功能**
 - 启用L2TP
 - 创建L2TP组
 - 配置隧道本端名称
- **LAC侧**
 - 配置LAC发起L2TP连接请求的触发条件
 - 配置LNS的IP地址
 - 配置LAC侧的AAA认证
- **LNS侧**
 - 配置虚接口模板
 - 配置LNS接受L2TP隧道建立请求
 - 配置LNS侧的用户重验证
 - 配置LNS侧的AAA认证

www.h3c.com


配置 L2TP 时，根据其工作方式的不同，必须完成的配置项也有所不同。


对于独立 LAC 方式，L2TP 的配置分为远程系统、LAC、LNS 三部分。如果配置了远程验证，则还需要配置验证服务器。其中远程系统仅使用普通的拨号客户端即可。远程系统和验证服务器的配置此处不再赘述。此外用户还必须完成 LAC 侧的配置和 LNS 侧的配置。

在将设备配置为 LAC 或 LNS 之前，必须首先使能 L2TP 功能、创建 L2TP 组，使设备具有基本的 L2TP 处理能力；然后根据不同的使用环境，分别进行 LAC 或 LNS 的特性配置，使设备具有独立的 L2TP 隧道端点功能。

10.4.2 L2TP 基本功能配置

L2TP基本功能配置

紫光集团

H3C
核心企业 | 数字化转型方案领导者

- 启用L2TP

```
[Router] l2tp enable
```

- 创建L2TP组，并进入L2TP组视图

```
[Router] l2tp-group group-number mode { lac | lns }
```

- 配置隧道本端名称

```
[Router-l2tp1] tunnel name name
```

www.h3c.com

只有启用 L2TP 后，设备上的 L2TP 功能才能正常发挥作用；如果未启用 L2TP，则即使配置了 L2TP 的参数，设备也不会提供相关功能。默认情况下，L2TP 功能处于关闭状态。要启用 L2TP 功能，在系统视图下使用命令：

l2tp enable

为了进行 L2TP 的相关参数配置，还需要创建 L2TP 组。L2TP 组的使用允许在设备上灵活配置 L2TP 功能，方便地实现了 LAC 和 LNS 之间一对一、一对多的组网应用。L2TP 组在 LAC 和 LNS 上独立编号，只需要保证 LAC 和 LNS 之间关联的 L2TP 组的相关配置（如隧道对端名称、LNS 地址等）保持对应关系即可。默认情况下没有创建任何 L2TP 组。要创建 L2TP 组并进入 L2TP 组视图，在系统视图下使用命令：


l2tp-group group-number mode { lac | lns }

隧道名在 LAC 和 LNS 进行隧道协商时使用。LAC 侧隧道名称要与 LNS 侧配置的接收 L2TP 连接请求的隧道对端名称保持一致。默认情况下，隧道本端的名称为系统的名称。要配置隧道本端的名称，在 L2TP 组视图下使用命令：

tunnel name name

10.4.3 LAC 基本配置命令

LAC基本配置命令

 紫光集团 **H3C**
核心企业 数字化转型方案领导者

- **配置LAC发起L2TP连接请求的触发条件**

```
[H3C-l2tp1]user { domain domain-name | fullusername user-name }
```

- **配置LNS的IP地址**

```
[H3C-l2tp1]lns-ip { ip-address }<1-5>
```

- **配置LAC侧的AAA验证**

→ 可以使用本地验证或远程验证

www.h3c.com

只有在满足一定的条件时，LAC 才会向 LNS 发出建立 L2TP 连接请求。通过配置对接入的 PPP 用户信息的判别条件，并指定相应的 LNS 端的 IP 地址，LAC 设备可以鉴定用户是否为 L2TP VPN 用户，并决定是否向 LNS 发起连接。

LAC 发起 L2TP 连接请求时，支持两种用户名的触发——完整的用户名（fullusername）和带特定域名的用户名（domain）。

要配置本端作为 L2TP LAC 端时向 LNS 发起隧道建立请求的触发条件，在 L2TP 组视图下使用命令：

```
user { domain domain-name | fullusername user-name }
```

每个 LAC 的 L2TP 组最多可以设置五个 LNS，即允许存在备用 LNS。正常运行时，LAC 按照 LNS 配置的先后顺序，依次进行 L2TP 连接请求，直到某个 LNS 接受连接请求，该 LNS 就成为 L2TP 隧道的对端。

要配置 LNS 的 IP 地址，在 L2TP 组视图使用命令：

```
lns-ip { ip-address }<1-5>
```


通过在 LAC 侧配置对 VPN 用户的 AAA 验证，可以对远程拨入用户的身份予以检验和确认。验证通过后才能发起建立隧道连接的请求。设备支持的 AAA 验证方式包括：

- **本地验证：**需要在 LAC 侧配置本地用户名、密码和服务类型等信息。LAC 通过检查用户名与密码是否与本地注册用户名/密码相符合来进行用户身份验证。

- **远程验证：**需要与 RADIUS/HWTACACS 服务器协同进行验证。LAC 将用户名和密码发往服务器进行验证申请，服务器负责保存 VPN 用户的用户名和密码，进行用户身份验证，并将验证结果反馈给 LAC。

10.4.4 LNS 基本配置命令

LNS基本配置命令



- 创建虚模板接口，进入虚模板接口视图

```
[H3C]interface virtual-template virtual-template-number
```

- 配置虚模板接口的IP地址

```
[H3C-Virtual-Template1]ip address ip-address { mask-length | mask } [ sub ]
```

- 配置为用户分配的地址池

```
[H3C-Virtual-Template1]remote address { ip-address | pool pool-name }
```

- 配置PPP验证

```
[H3C-Virtual-Template1]ppp authentication-mode { chap | ms-chap | ms-chap-v2 | pap } * [ [ call-in ] domain isp-name ]
```

www.h3c.com

虚模板 VT（Virtual-Template，虚拟模板）接口是一种虚拟的逻辑接口。L2TP 会话连接建立之后，需要创建一个 VA（Virtual Access，虚拟访问）接口用于和 LAC 端交换数据。VA 接口是基于 VT 接口上配置的参数动态创建，因此配置 LNS 时需要首先创建 VT 接口，并配置该接口的参数。默认情况下系统没有创建虚模板接口。要配置虚模板接口并进入其接口视图，在系统视图下使用命令：

```
interface virtual-template number
```

虚模板接口本身需要一个 IP 地址。要配置本端 IP 地址，在虚模板接口视图下使用命令：

```
ip address ip-address { mask | mask-length } [ sub ]
```

当 LAC 与 LNS 之间的 L2TP 隧道连接建立之后，LNS 需要为 VPN 用户分配 IP 地址。地址分配包括两种方式：指定地址池或直接配置 IP 地址。在指定地址池之前，需要在系统视图下用 **ip pool** 命令先定义一个地址池。要指定给对端分配地址所用的地址池或直接给对端分配 IP 地址，在虚模板接口视图下使用命令：


```
remote address { pool [ pool-number ] | ip-address }
```

当 LNS 对远程系统进行验证时，需要使用一些验证参数信息，配置在虚模板接口中。要配置本端对远程系统进行某种方式的 PPP 验证，在虚模板接口视图下使用命令：

```
ppp authentication-mode { chap | ms-chap | ms-chap-v2 | pap } [ [ call-in ] |
domain isp-name ]
```

默认情况下不进行验证。

LNS基本配置命令（续）



- 配置LNS接受L2TP隧道建立请求
 - L2TP组号不为1时：


```
[Router-l2tp2] allow l2tp virtual-template virtual-template-
number remote remote-name
```
 - L2TP组号为1时：


```
[Router-l2tp1] allow l2tp virtual-template virtual-template-
number [ remote remote-name ]
```

www.h3c.com

LNS 可以使用不同的虚模板接口接收不同 LAC 的创建隧道的请求。接收到来自 LAC 的请求后，LNS 需要检查 LAC 的隧道本端名称是否与本地配置的隧道对端名称相符合，从而决定是否允许与对端建立隧道。要指定接收呼叫的虚模板接口、隧道对端名称等参数，在 L2TP 组视图下使用 **allow l2tp** 命令。

当 L2TP 组号为 1（默认的 L2TP 组号）时，可以不指定隧道对端名，即 LNS 可以接受任何名称的隧道对端的隧道建立请求，使用命令：

```
allow l2tp virtual-template virtual-template-number [ remote remote-name ]
```

当 L2TP 组号不为 1 时，使用命令：

```
allow l2tp virtual-template virtual-template-number remote remote-name
```

10.4.5 高级配置命令

LAC和LNS高级配置命令

 紫光集团  H3C
核心企业 数字化转型方案领导者

- 启用隧道验证功能

[Router-l2tp1] tunnel authentication

- 配置隧道验证密码

[Router-l2tp1] tunnel password { cipher | simple } password

- 设置隧道Hello报文发送时间间隔

[Router-l2tp1] tunnel timer hello hello-interval

- 强制挂断隧道

<Router> reset l2tp tunnel { id tunnel-id | name remote-name }

www.h3c.com

管理员可根据实际需要，决定是否在创建隧道连接之前进行隧道验证。隧道验证请求可由 LAC 或 LNS 任何一侧发起。只要有一方启用了隧道验证，则只有在对端也启用了隧道验证、两端密码完全一致并且不为空的情况下，隧道才能建立；否则本端将自动将隧道连接断开。

若隧道两端都配置了禁止隧道验证，隧道验证的密钥一致与否将不影响隧道建立。

为了保证隧道安全，建议用户最好不要禁用隧道验证的功能。如果用户需要修改隧道验证的密钥，请在隧道开始协商前进行，否则修改的密钥不生效。

在 L2TP 组视图下使用 **tunnel authentication** 命令启用 L2TP 的隧道验证功能。默认情况下，L2TP 隧道验证功能处于开启状态。

要配置隧道验证密码，在 L2TP 组视图下使用命令：

tunnel password { simple | cipher } password

默认情况下，没有配置隧道验证密码。


为了检测 LAC 和 LNS 之间隧道的连通性，LAC 和 LNS 会定期向对端发送 Hello 消息，接收方接收到 Hello 报文后会进行响应。当 LAC 或 LNS 在指定时间间隔内未收到对端的 Hello 消息时，将重复发送 Hello 消息。如果重复发送超过 5 次都没有收到对端的 Hello 消息，则认为 L2TP 隧道已经断开。默认情况下，隧道中 Hello 报文的发送时间间隔为 60 秒。要配置隧道 Hello 消息的发送时间间隔，在 L2TP 组视图下使用命令：

tunnel timer hello hello-interval

要强制断开指定的隧道连接，在用户视图下执行命令：

```
reset l2tp tunnel { id tunnel-id | name remote-name }
```

LNS高级配置命令

 紫光集团 **H3C**
核心企业 数字化解决方案领导者

- **配置强制CHAP验证**
- [H3C-l2tp1]mandatory-chap
- **配置强制LCP重新协商**
- [H3C-l2tp1]mandatory-lcp
- **配置LNS侧的AAA认证**
- 可以使用本地验证或远程验证

www.h3c.com

当 LAC 对用户进行验证后，为了增强安全性，LNS 可以再次对用户进行验证。在这种情况下，将对用户进行两次验证，第一次发生在 LAC 侧，第二次发生在 LNS 侧，只有两次验证全部成功后，L2TP 隧道才能建立。

在 L2TP 组网中，LNS 侧对用户的验证方式有三种：1、代理验证：由 LAC 代替 LNS 对用户进行验证，并将用户的所有验证信息及 LAC 端本身配置的验证方式发送给 LNS。LNS 根据接收到的信息及本端配置的验证方式，判断用户是否合法。2、强制 CHAP 验证：强制在 LAC 代理验证成功后，LNS 再次对用户进行 CHAP 验证。3、LCP 重协商：忽略 LAC 侧的代理验证信息，强制 LNS 与用户间重新进行 LCP（Link Control Protocol，链路控制协议）协商。

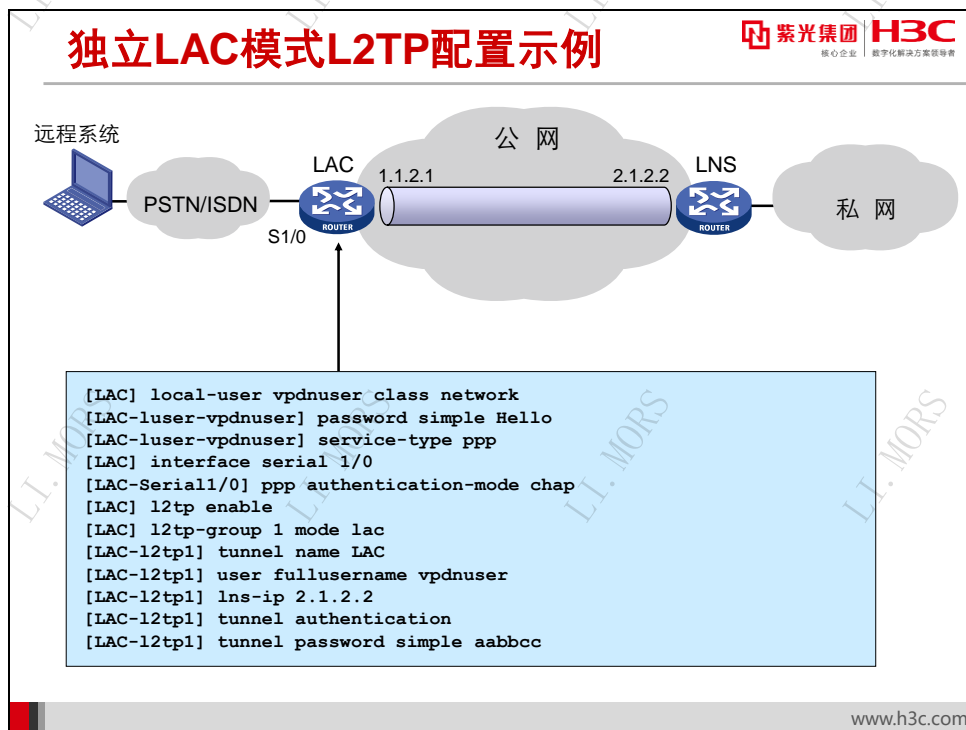
关于强制 CHAP 验证，启用该配置后，对于 NAS-Initiated 模式 L2TP 隧道的用户来说，会经过两次验证：一次是在 NAS 端的验证，另一次是在 LNS 端的验证。一些用户可能不支持进行第二次验证，这时，LNS 端的 CHAP 重新验证会失败。在这种情况下，建议不要开启 LNS 的强制 CHAP 验证功能。配置强制 CHAP 验证时，需要在 LNS 的 VT 接口下配置 PPP 用户的验证方式为 CHAP 认证。

关于强制 LCP 重协商，启用该配置后，对于 NAS-Initiated 模式 L2TP 隧道的 PPP 用户，在 PPP 会话开始时，先和 NAS 进行 PPP 协商。若协商通过，则由 NAS 触发建立 L2TP 隧道，并将用户信息传递给 LNS，由 LNS 根据收到的代理验证信息，判断用户是否合法。但在某些特定的情况下（如 LNS 不接受 LAC 的 LCP 协商参数，希望和用户重新进行参数协商），需要强制 LNS 与用户重新进行 LCP 协商，并采用相应的虚拟模板接口上配置的验证方式对用户进

行验证。启用 LCP 重协商后，如果相应的虚拟模板接口上没有配置验证，则 LNS 将不对用户进行二次验证（这时用户只在 LAC 侧接受一次验证）。

验证方式的优先级从高到底依次为：LCP 重协商、强制 CHAP 验证和代理验证。如果在 LNS 上同时配置 LCP 重协商和强制 CHAP 验证，L2TP 将使用 LCP 重协商；如果只配置强制 CHAP 验证，则在 LAC 代理验证成功后，LNS 再次对用户进行 CHAP 验证；如果既不配置 LCP 重协商，也不配置强制 CHAP 验证，则对用户进行默认代理验证。

10.4.6 配置示例



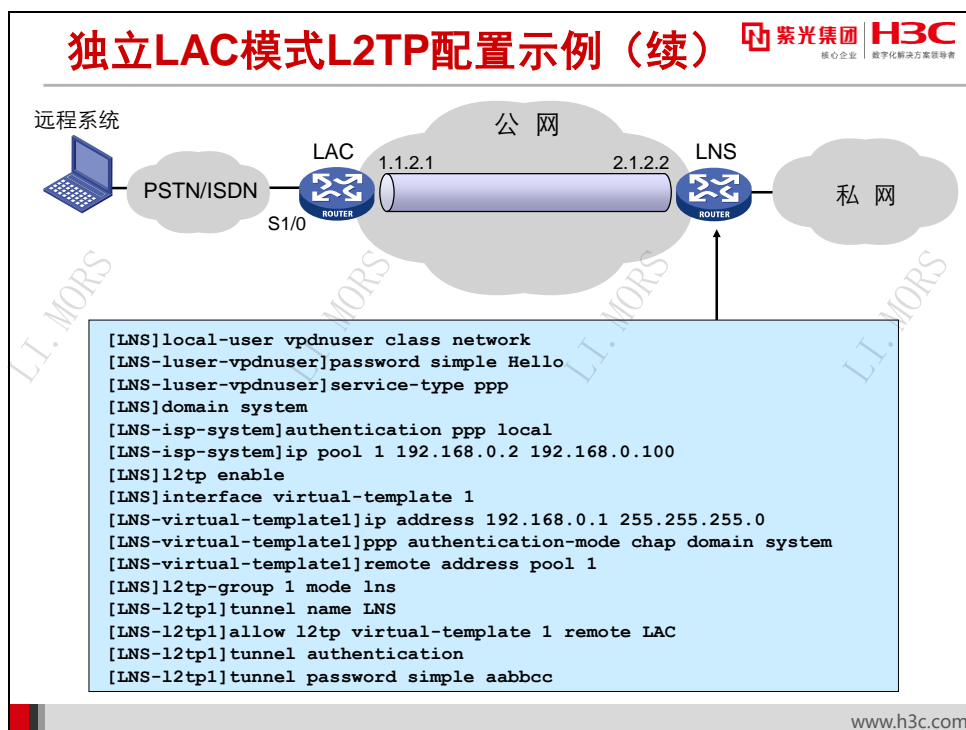
这是一个典型的 L2TP 独立 LAC 模式配置示例。在本例中，某企业以 MSR 路由器作为 LAC 和 LNS，远程移动用户使用 Windows 系统，通过 PSTN 拨号到 LAC 的串口 S1/0 接入，与企业总部互联。

该公司总部网络采用私网地址。通过建立 L2TP VPN，用户就可以通过普通电话线路访问公司内部网络的数据。

上图显示的是 LAC 侧的主要配置。为简化起见，LAC 采用了本地验证方式，并配置了拨号用户的用户名 vpdnuser 和密码 Hello。

当然，在 LAC 上还需要为公网接口配置公网地址 1.1.2.1。在串口 S1/0 上还需完成接受拨号的相关配置。S1/0 并不需要配置 IP 地址，客户端的地址将由 LNS 分配。

另外，在用户侧 PC 上需配置拨号客户端，使用用户名 vpdnuser 和密码 Hello 进行拨号。



上图显示的是 LNS 侧的主要配置。为简化起见，LNS 同样采用了本地验证方式，并配置了拨号用户的用户名 vpdnuser 和密码 Hello。LNS 创建了虚模板接口 virtual-template1，以便对客户端 PC 机进行验证、分配 IP 地址并进行 IP 数据报文转发。

在 LNS 上还需要为公网接口配置公网地址 2.1.2.2。

10.5 用iNode客户端实现客户LAC模式

10.5.1 iNode 客户端介绍

iNode客户端介绍

紫光集团 H3C
核心企业 数字化解决方案领导者

- H3C研发的专业化安全客户端软件
- 支持802.1X、Portal等接入认证方式
- 支持L2TP VPN
- 完善的安全性
 - 支持IKE/IPSec和NAT穿越
 - 支持RSA动态口令验证和SecKey

www.h3c.com

H3C iNode 客户端软件是一款成熟而专业化的安全客户端软件。安装有 iNode 客户端的 PC 机可以通过多种方式与安全网关设备建立 VPN 隧道,也可以通过 802.1X、Portal 等方式实现接入身份验证并获取网络资源。

iNode 可以提供独立 LAC 模式 L2TP 客户端功能,只要远端用户能够通过 xDSL 和小区宽带等方式接入到 Internet,就可以和总部的 VPN 网关之间建立 L2TP 隧道,允许移动用户安全、快捷地通过 Internet 访问其组织私网内的资源。

iNode VPN 客户端软件支持 IKE/IPSec 特性。IPSec 使特定的通信双方在 IP 层通过加密与数据源验证等方式,保证数据在公共网络上传输时的私密性、完整性、真实性,并可以在一定程度上抵御防重播攻击。

iNode VPN 客户端软件支持智能卡 (USB Key)、数字证书等认证方式,加强身份验证的安全强度,减少用户身份信息被盗用的风险,同时减少客户端配置管理工作,最终帮助企业实现大规模移动 VPN 用户接入的部署和维护工作。

注意:

iNode 客户端的功能依据其版本有所不同。如需使用 L2TP 客户端,请使用支持 L2TP VPN 的 iNode 客户端版本。

10.5.2 客户 LAC 模式配置任务

客户LAC模式配置任务

紫光集团 H3C
核心企业 数字化转型方案领导者

- **配置LNS**
 - 配置命令与独立LAC模式相同
- **配置远程系统的公网连接**
 - 以任意方式获得公网接入，与LNS建立连通性
- **配置iNode客户端**
 - 安装iNode客户端
 - 创建VPN连接
 - 配置用户名和密码
 - VPN连接基本设置
 - VPN连接高级属性

www.h3c.com

在 L2TP 客户 LAC 组网模式中，LNS 的配置与独立 LAC 模式相同，但远程系统的配置有所不同。由于远程系统必须同时执行 LAC 功能，因此要求其必须具备可用的公网连接，具备与 LNS 的 IP 可达性。

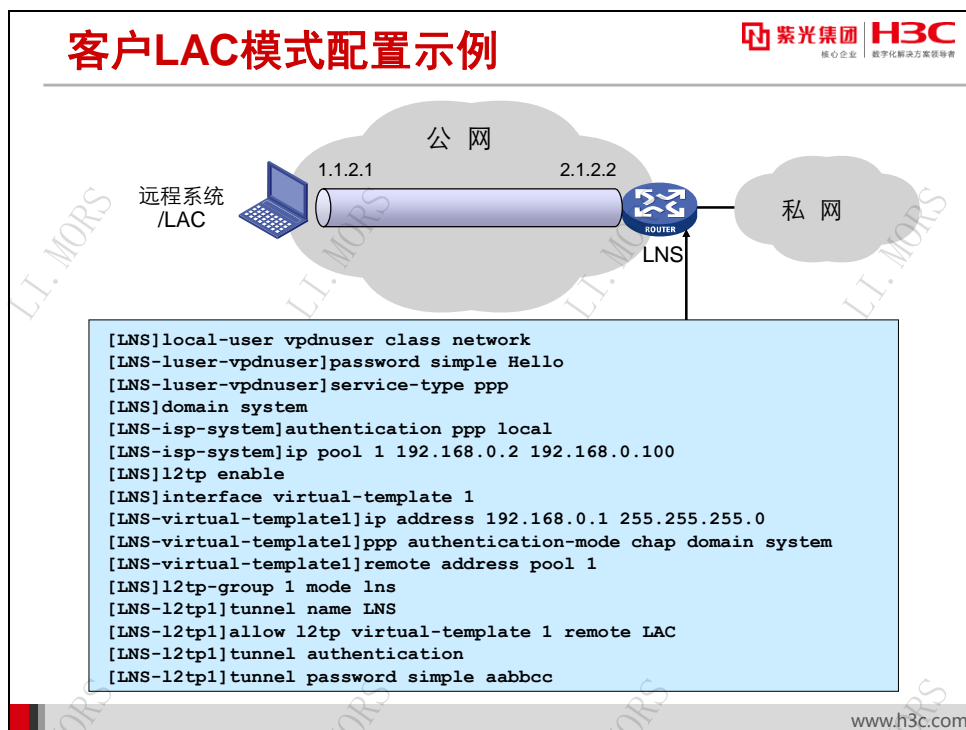
在 Windows 系统中安装 iNode 客户端非常简便，根据图形化向导的指示完成安装即可。

配置 iNode 客户端实现 L2TP 的基本配置任务包括：

- 创建 L2TP VPN 连接
- 配置登录用户名和密码
- VPN 连接基本设置
- VPN 连接高级属性

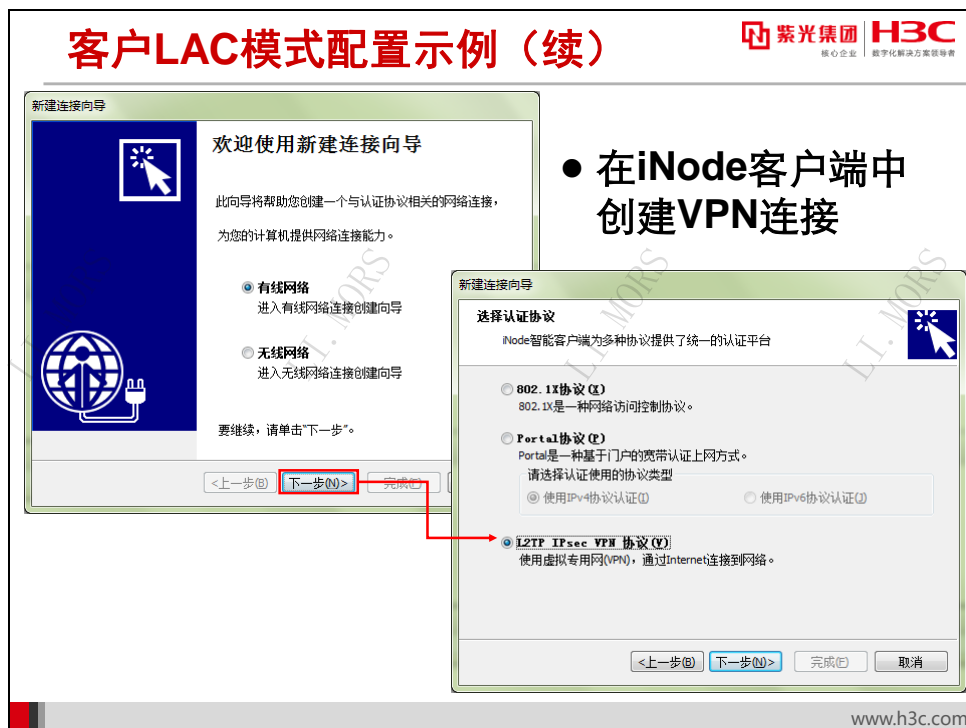
此外还可以配置 RSA 验证、智能卡、IPSec 等参数。

10.5.3 客户 LAC 模式配置示例



在本例中，远程移动用户希望通过 Internet 将自己的便携计算机以 L2TP VPN 连接到公司内网，访问私网资源。

首先在公司总部路由器侧配置 LNS，允许用户通过 L2TP 接入。LNS 的主要配置如图所示。



接下来，在用户的便携计算机上配置 Internet 连接，使其能正确地获得公网地址，并与 LNS 通过 Internet 互通。

随后，在用户的便携计算机上安装 iNode 客户端。跟随安装向导的指示，使用默认参数即可。安装完成后即可开始配置 iNode 客户端。

在 iNode 客户端主界面菜单中点击【文件】|【新建连接】进入【新建连接向导】，保持选中【有线网络】，单击【下一步】，进入【选择认证协议】窗口。单击选中【L2TP IPsec VPN 协议】，单击【下一步】，进入【选择连接类型】窗口。

注意：

不同版本的 iNode 客户端功能和界面可能有所差别，具体情况请参考相应的用户手册。

客户LAC模式配置示例（续）

紫光集团 H3C
核心企业 数字化转型方案领导者

● 设置用户名和密码

www.h3c.com

在【选择连接类型】窗口中保持选中【普通连接】，单击【下一步】，进入图示窗口。在对话框中，可输入连接名例如“我的VPN连接”，并设置用户名vpdnuser和密码Hello。

如需避免每次登录时重复手工输入用户名和密码，单击选中【保存用户密码】复选框。

单击【下一步】，进入【VPN连接基本设置】窗口。



● L2TP连接基本设置

在【VPN 连接基本设置】窗口的【LNS 服务器】处输入 LNS 地址 2.1.2.2。注意不要选中【启用 IPsec 安全协议】。

单击【高级】进入【VPN 连接高级属性】窗口。单击【L2TP 设置】选项卡，输入隧道名称 LAC，在【选择认证模式】处选择【CHAP】，选中【使用隧道验证密码】并将【隧道验证密码】设置为 aabbcc。单击【确定】按钮，确认设置。

在【VPN 连接基本设置】窗口中单击【完成】按钮，即可完成 L2TP 客户端配置。

使用 L2TP VPN 时首先启动 iNode 客户端，双击“我的 VPN 连接”即可启动连接。

10.6 L2TP信息显示和调试

L2TP信息显示命令

● 显示当前L2TP隧道的信息

```
[LNS-12tp1]display l2tp tunnel
```

LocalTID	RemoteTID	State	Sessions	RemoteAddress	RemotePort	RemoteName
10878	21	Established	1	2.1.1.1	1701	PC

● 显示当前L2TP会话的信息

```
[LNS-12tp1]display l2tp session
```

LocalSID	RemoteSID	LocalTID	State
89	36245	10878	Established

www.h3c.com

在任意视图下执行 **display l2tp** 命令可以显示配置后 L2TP 的运行情况。

使用命令 **display l2tp tunnel [statistics]** 可显示当前的 L2TP 隧道信息。显示信息中各字段的含义如下表所示。

字段	描述
Total tunnel	隧道的数目
LocalTID	本端隧道ID
RemoteTID	对端隧道ID
State	隧道状态
Sessions	此隧道上的会话数目
RemoteAddress	对端的IP地址
RemotePort	对端使用的UDP端口号
RemoteName	对端的名称

使用命令 **display l2tp session [statistics]** 可显示当前的 L2TP 会话的信息。显示信息中各字段的含义如下表所示。

字段	描述
Total session	会话的数目
LocalSID	本端会话ID
RemoteSID	对端会话ID
LocalTID	本端隧道ID
State	会话的状态

10.7 本章总结

本章总结

- L2TP是适用于远程分支和移动用户接入的 Access VPN技术
- L2TP拓扑结构分为独立LAC模式和客户LAC模式
- iNode客户端支持包括L2TP在内的多种接入技术
- L2TP可以以低成本实现多协议远程接入，但不能提供足够的安全保护

10.8 习题和解答

10.8.1 习题

1. 下列描述中正确的是 ()
 - A. L2TP 是一种 VPDN
 - B. L2TP 支持多种网络层协议
 - C. L2TP 隧道只能由客户端主机发起建立
 - D. 彻底无安全性保证
2. L2TP 拓扑类型包括 ()
 - A. 客户 LAC 模式
 - B. 独立 LAC 模式
 - C. 客户端发起模式
 - D. LAC 发起模式
3. 下列关于隧道、会话和 PPP 连接的描述正确的是 ()
 - A. 每个 PPP 连接触发建立一个隧道
 - B. 一个隧道对应一个会话
 - C. 一个 PPP 连接对应一个会话
 - D. 以上都不对
4. L2TP 的验证包括下列哪三项? ()
 - A. LAC 对远程系统的初始 PPP 验证
 - B. LAC 与 LNS 之间的隧道验证
 - C. LNS 对远程系统的再次 PPP 验证
 - D. 内网验证服务器对远程系统的 PPP 验证
5. 在 LAC 发起控制连接时, 要使 LNS 对此连接进行验证, 应使用命令 ()
 - A. **ppp authentication chap**
 - B. **ppp authentication-mode chap domain system**
 - C. **mandatory-chap**
 - D. **tunnel authentication**

10.8.2 习题答案

- 1、AB 2、AB 3、C 4、ABC 5、D