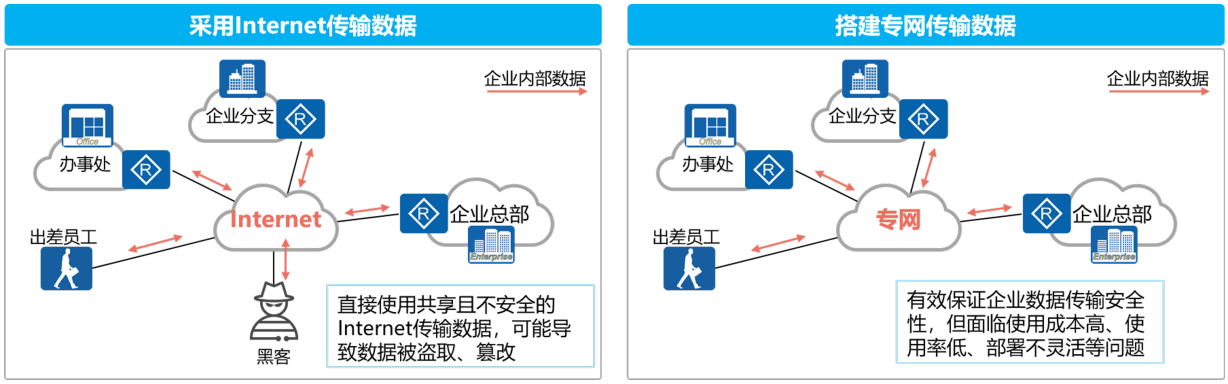
IPSec VPN

一、VPN的技术背景

1、在VPN出现之前，企业分支之间的数据传输只能依靠现有物理网络【例如Internet】。由于Internet中存在多种不安全因素，报文容易被网络中的黑客窃取或篡改，最终造成数据泄密、重要数据被破坏等后果

2、除了通过Internet，还可以通过搭建一条物理专网连接保证数据的安全传输，但其费用会非常昂贵，且专网的搭建和维护十分困难



二、VPN的概念

1、VPN【Virtual Private Network | 虚拟私有网络】

2、利用运营商已经构建好的不安全的互联网络，来安全的传递自己的私有数据的网络就称之为VPN

3、总部与分支【Hub-and-Spoke】

4、在没有VPN技术之前，总部与分支机构之间互通的数据，或通过不安全的Internet来发送，或构建属于本公司自己的专线

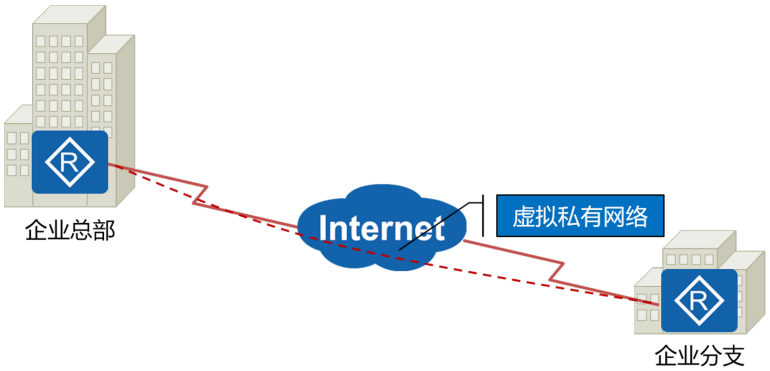
5、通过Internet来传递文件、数据，优势在于成本低，无需用户自行维护，缺点在于Internet不安全，其中存在诸多的网络攻击、黑客、病毒，在Internet上传递数据几乎丧失了所有的安全、私密性，同时需要承担数据被篡改的可能性

6、若部署专线，则无需担心网络安全问题，专线是令运营商为用户自行搭建并部署一套完全属于客户自身的私有网络（大私网），因此安全性极高，但费用极其昂贵，且部署不灵活，对专线的维护较为复杂

7、在上述的基础之上，VPN技术应运而生

8、VPN依旧是利用ISP已经构建好的Internet，在互联网已经联通的基础之上，部署自身的私密连接

9、VPN的优势在于令部署VPN技术的两端设备在原有的数据包外面再添加一个新的IP头部，新的IP头部负责在Internet上提供通讯功能，令来自于企业总部与分支之间的私有地址可以穿越公有互联网实现通讯



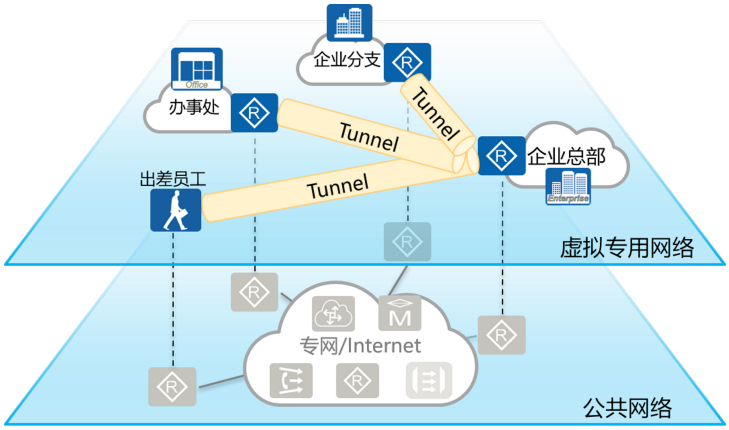
三、VPN的优势

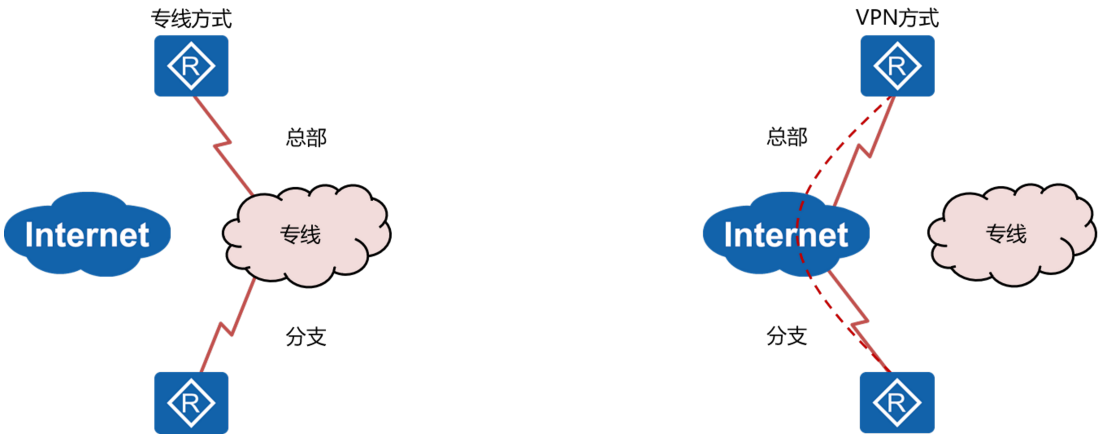
VPN相较于专线而言，具有诸多优势：

1、VPN的优势：费用较低、部署灵活、隧道化管理，维护与部署完全由客户自行完成，方便后续的变迁、维护及管理

2、专线的优势：令ISP为客户自行搭建一套大的私有网络，提供足够高的安全机制

3、专线的缺点：费用极高、部署复杂，维护复杂，网络的变迁不灵活



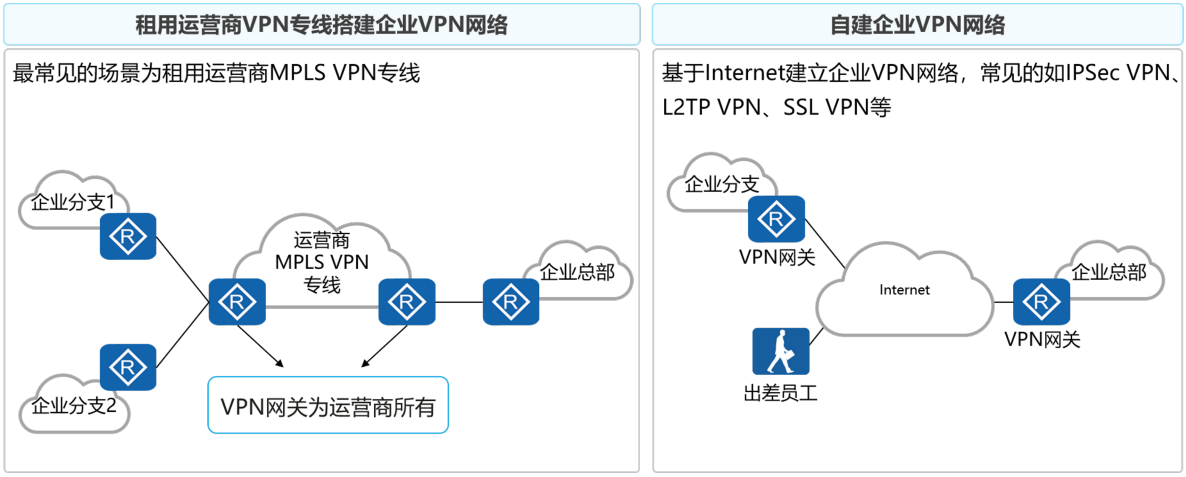


四、VPN的结构及分类

1、按照建设单位不同，VPN可分为2大类：

1.1、用户自行维护建设：客户自行在企业边界路由器上（VPN网关设备）上配置并部署VPN，一切的建设与维护工作，均由客户自行完成

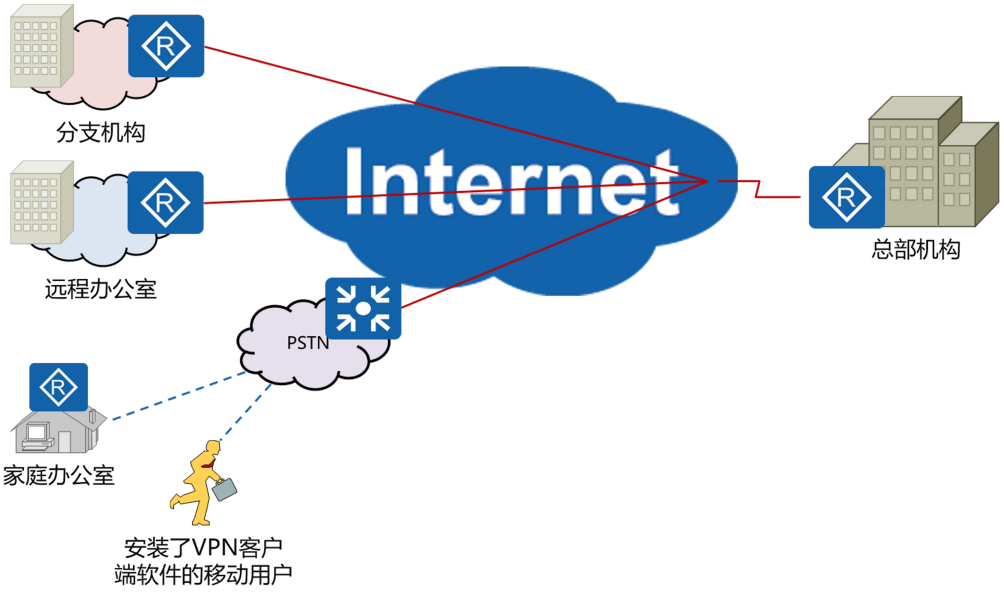
1.2、运营商维护建设：在客户的网络不断的扩大，以至于拥有了诸多的分支机构、办事处、SOHO时，再让客户自行维护VPN将变得困难且繁琐，此时可以由ISP来部署VPN，ISP获取相应的费用来提供增值性服务，通过部署（如：MPLS VPN等）技术，来为客户搭建并维护VPN网络



2、按照组网方式不同，VPN又可以被分为2大类：

2.1、站点到站点【Site-to-Site】的VPN（三层VPN）：构建在企业总部与分支之间的VPN网关设备之间的，能够满足来自于总部与分支之间的多用户之间的通讯

2.2、远程访问的【Remote】VPN（二层VPN）：构建在移动外出人员与总部的VPN网关设备之间的，外出移动人员无需配置VPN，仅仅需要安装一个VPN客户端软件，提交用于连接VPN的用户名及密钥即可，能够满足来自于一个移动用户与总部服务器之间的通讯



五、VPN的工作原理

1、定义感兴趣流量：只有满足了VPN网关设备定义的感兴趣流量，VPN网关才会按照VPN传输的方式加以处理，否则直接走NAT做地址转换，访问公网

2、数据加密：通过各种各样的加密算法来为用户发送的原始明文数据进行加密，保证数据的机密性

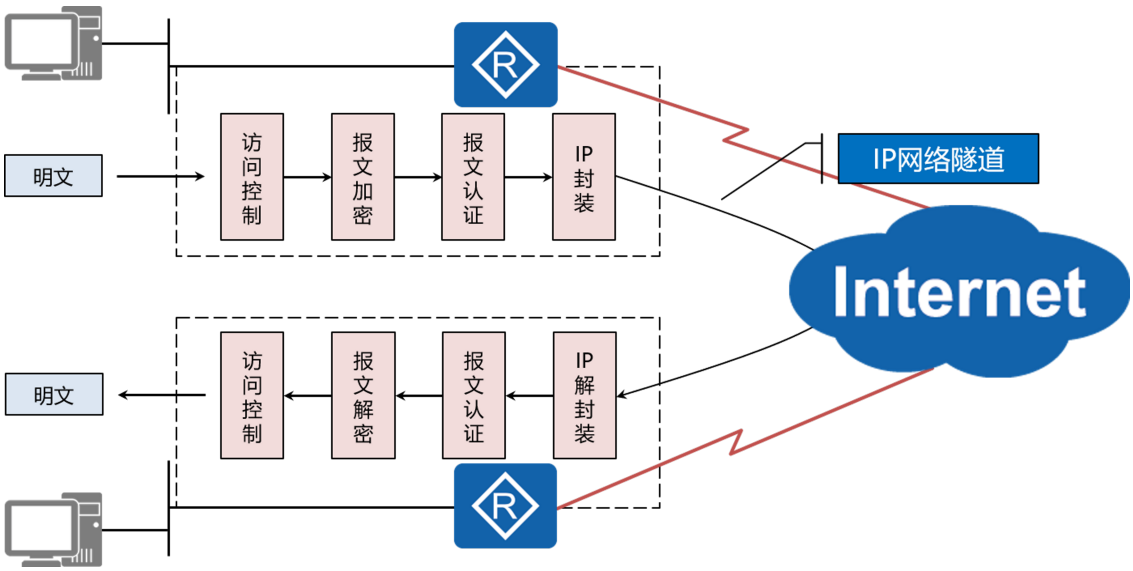
3、报文认证：通过各种各样的认证机制，保证数据的完整性不被篡改

4、IP重封装：为原始封装的数据添加新的IP头部，形成隧道，利用公有互联网络来传递封装后的报文数据

注1：对端的VPN网关设备执行完全相反的逆运算，该过程不再赘述

注2：VPN的精髓就在于：VPN = 加密 + 隧道

VPN = 加密 + 隧道



五、VPN的关键技术

1、安全的隧道技术

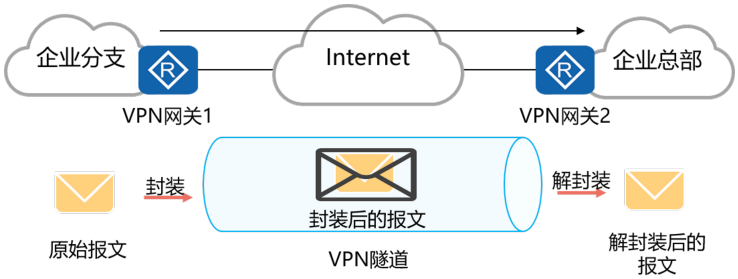
1.1、VPN技术利用隧道技术【Tunnel】来对用户发送的原始数据进行二次封装，来利用VPN专用网络（Internet）来建立专用的数据传输通道

1.2、配置VPN两端的VPN网关设备在隧道的两端执行"封装"与"解封装"技术，来建立一个虚拟的点对点的虚拟通信隧道

1.3、隧道的功能就是在两个网络节点之间提供一条通路，使数据能够在这个通路上透明传输。VPN隧道一般是指在VPN骨干网的VPN节点之间建立的用来传输VPN数据的虚拟连接。隧道是构建VPN不可或缺的部分，用于把VPN数据从一个VPN节点透明传送到另一个上

1.4、隧道通过隧道协议实现。目前已存在不少隧道协议，如GRE（Generic Routing Encapsulation）、L2TP（Layer 2 Tunneling Protocol）等。隧道协议通过在隧道的一端给数据加上隧道协议头，即进行封装，使这些被封装的数据能都在某网络中传输，并且在隧道的另一端去掉该数据携带的隧道协议头，即进行解封装。报文在隧道中传输前后都要通过封装和解封装两个过程

1.5、部分隧道可以混合使用，如GRE Over IPSec隧道



2、身份认证、数据加密与验证

2.1、身份认证、数据加密和认证技术可以有效保证VPN网络与数据的安全性：

2.2、身份认证：可用于部署了远程接入VPN的场景，VPN网关对用户的身份进行认证，保证接入网络的都是合法用户而非恶意用户。也可以用于VPN网关之间对对方身份的认证

2.3、数据加密：将明文通过加密变成密文，使得数据即使被黑客截获，黑客也无法获取其中的信息

2.4、数据验证：通过数据验证技术对报文的完整性和真伪进行检查，丢弃被伪造和篡改的报文

VPN	用户身份认证	数据加密和验证	备注
GRE	不支持	支持简单的关键字验证、检验和验证	可以结合IPSec使用，利用IPSec的数据加密和验证特性
L2TP	支持基于PPP的CHAP、PAP、EAP认证	不支持	
IPSec	支持	支持	支持预共享秘钥验证或证书认证；支持IKEv2的EAP认证
SSL	支持	支持	支持用户名/密码或证书认证
MPLS	不支持	不支持	一般运行在专用的VPN骨干网络

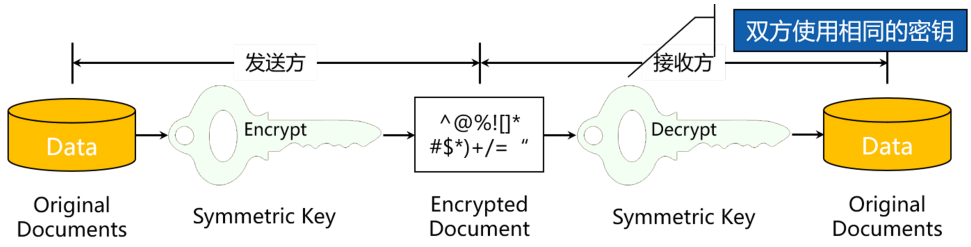
3、加密技术

在网络中常见的加密技术公有3种：

3.1、对称加密：加密一方与解密一方使用完全相同的密钥

加密技术：DES（56bit）、3DES（112bit、168bit）、AES（128bit、192bit、256bit）等

对称加密的最大问题在于密钥的管理与传递



3.2、非对称加密：加密一方与解密一方使用不同的密钥

3.2.1、私钥：有且只有1把，不需要传递

3.2.2、公钥：可以有很多把，可以传递

非对称加密规定：

a、用私钥加密的数据，公钥可以解密

b、用公钥加密的数据，只有私钥可以解密

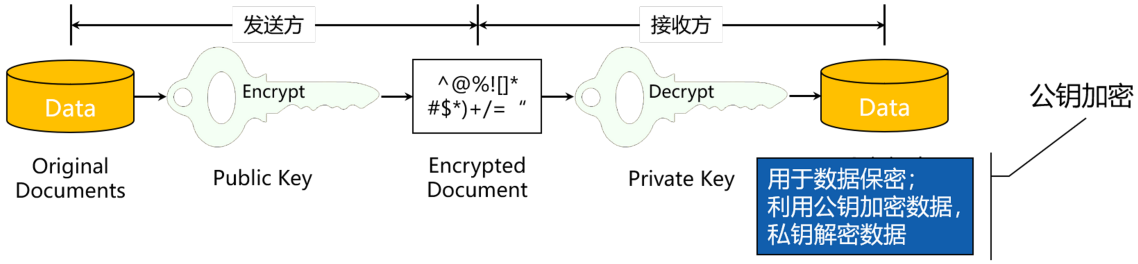
c、用公钥加密的数据，用公钥不可以解密

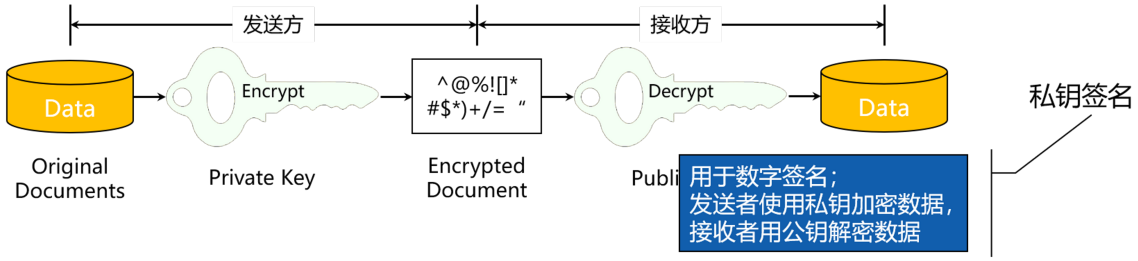
注1：私钥无需传递，在本地保存，具有极高的安全性，公钥的传递有2个方法：

a、直接通过Internet传递，较为不安全

b、从一个第三方的受信机构申请，通讯双方均从该受信机构下载私有与公钥

注2：当用户使用私钥进行加密时，因为私有有且只有1把，且不会传递，因此在使用私钥加密数据的过程中，不仅仅可以起到增加数据机密性的作用，同时也能够起到数字签名的作用，实现用户认证功能，增加数据的不可抵赖性





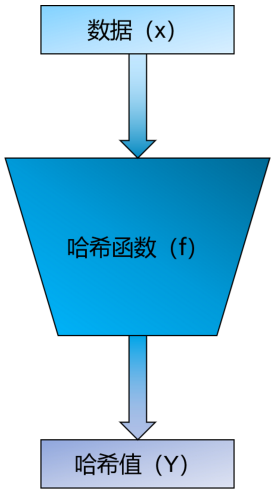
3.3、HASH加密

3.1、能够将任意长度的数据加密为定长的256bit

3.2、HASH加密的碰撞率极低

3.3、HASH加密的速度极快

3.4、HASH加密不可逆运算



六、隧道协议的种类

1、远程访问【二层】VPN

1.1、Cisco Easy VPN

1.2、L2TP VPN【Layer 2 Tunnel Protocol】

1.3、PPTP VPN【Point To Point Tunnel Protocol】

1.4、L2F【Layer 2 Forwarding】

2、站点到站点【三层】VPN

2.1、IPSec VPN【IP Security Protocol】

2.2、GRE Tunnel【Generic Routing Encapsulation】

2.3、GRE over IPSec VPN

2.4、MPLS VPN【Mutil-Protocol Label Switch】

七、IPSec VPN的基本概念

1、IPSec —— IP Security VPN【IP安全VPN】

2、IPSec VPN往往部署在企业边界设备上（边界路由器），通过加密与验证等方式，来增强网络发送数据的机密性、数据的完整性、验证数据的来源，同时能够起到抗重放攻击的作用

注：重放攻击：指网络攻击者将截获的数据不停的发送给接收方，让接收方接收大量的重复的、旧的报文

3、IPSec不是一个单独的独立协议，而是一整套安全协议的框架集

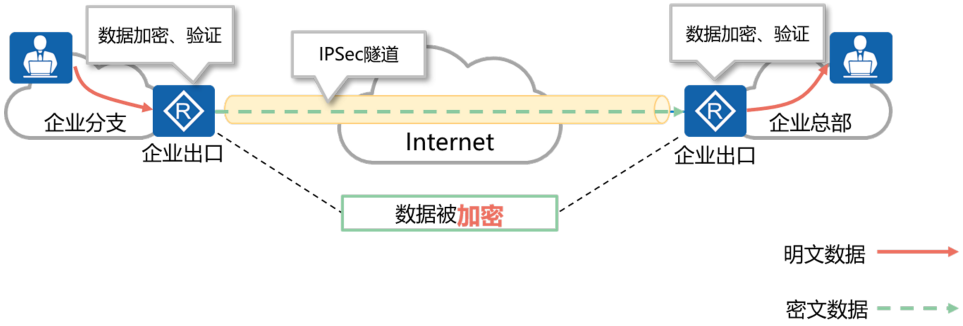
4、IPSec基本上是由3个独立的安全协议所组成的：

4.1、AH【Authentication Header | 验证头部】：仅仅只具有验证的功能与防重放攻击的功能，不具有加密数据的功能（AH的验证强度比ESP强）

4.2、ESP【Encapsulating Security Payload | 封装的安全载荷】：同时具有验证与加密的功能

4.3、IKE【Internet Key Exchange | 互联网密钥交换协议】：用来自动协商AH与ESP所使用的密码算法

5、IPSec使用AH与ESP来提供传输与封装数据的能力，提供认证与加密等安全服务



八、IPSec协议体系

1、IPSec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

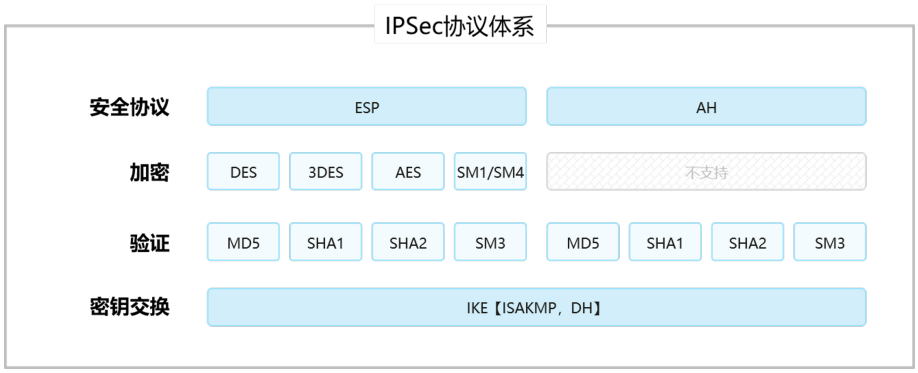
2、IPSec使用认证头AH（Authentication Header）和封装安全载荷ESP（Encapsulating Security Payload）两种安全协议来传输和封装数据，提供认证或加密等安全服务

2.1、AH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

2.2、ESP协议：提供AH协议的所有功能外，还可以提供对IP报文的加密功能

3、IKE协议提供密钥协商，建立和维护安全联盟SA等服务

3.1、IKE协议：用于自动协商AH和ESP所使用的密码算法



九、SA【安全联盟 | Security Association】

1、SA就是一整套安全参数的集合框架：

1.1、使用的封装模式【传输模式、隧道模式】

1.2、使用的验证算法

1.3、使用的加密算法

1.4、使用的加密密钥

1.5、本地地址与对端地址

1.6、本地SPI值与对端SPI值等

2、SA是单向的，因此在建立IPSec VPN的过程中，至少需要配置2个SA（两端都需要配置）

3、SA主要是由3元组构成的：

3.1、SPI【安全参数索引值】：一个系统自动生成的32bit的值，通过ESP或AH的头部传递给对端

3.2、对端的IP地址：明确指点对端与本地建立IPSec关系的地址

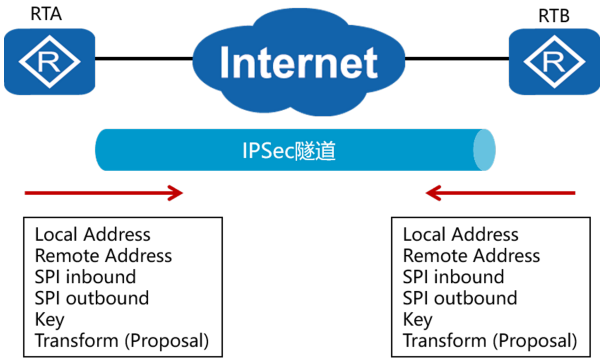
3.3、所使用的安全协议：ESP、AH、ESP&AH

4、SA的建立方式：

4.1、手工建立（带外）模式：在SA建立过程中所需要使用的所有安全参数全部需要管理员自行手工创建（主要SPI值）；在点到多点的网络环境中，若需要让总部路由与多个分支机构的路由之间手动创建各项安全参数将会造成极大的工作量，且容易出错，不推荐使用

4.2、自动协商模式：只需要通讯双方配置好IKE协商参数，由IKE自动协商来完成和创建SA，无需管理员手动配置SPI值，对于中到大型企业网

络，推荐使用自动协商模式



十、IPSec VPN的工作原理

IPSec VPN的建立需要2个阶段：

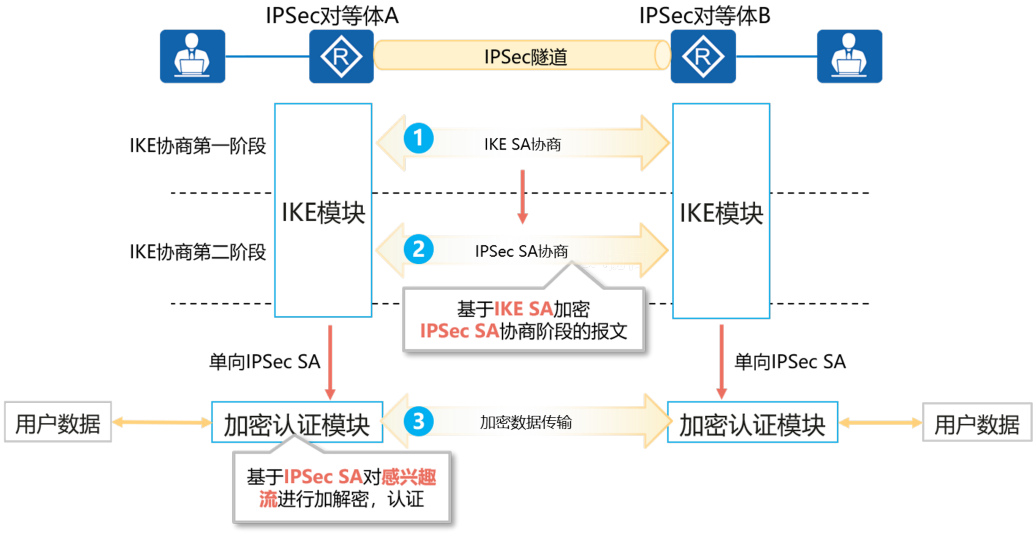
1、阶段一：IKE SA阶段

IKEv1协商阶段1的目的是建立IKE SA。IKE SA建立后对等体间的所有ISAKMP消息都将通过加密和验证，这条安全通道可以保证IKEv1第二阶段的协商能够安全进行。IKE SA是一个双向的逻辑连接，两个IPSec对等体间只建立一个IKE SA

2、阶段二：IPSec SA阶段

IKEv1协商阶段2的目的就是建立用来安全传输数据的IPSec SA，并为数据传输衍生出密钥。该阶段使用IKEv1协商阶段1中生成的密钥对ISAKMP消息的完整性和身份进行验证，并对ISAKMP消息进行加密，故保证了交换的安全性

3、IKE协商成功意味着双向的IPSec隧道已经建立，可以通过ACL方式或者安全框架方式定义IPSec“感兴趣流”，符合感兴趣流流量特征的数据都将被送入IPSec隧道进行处理



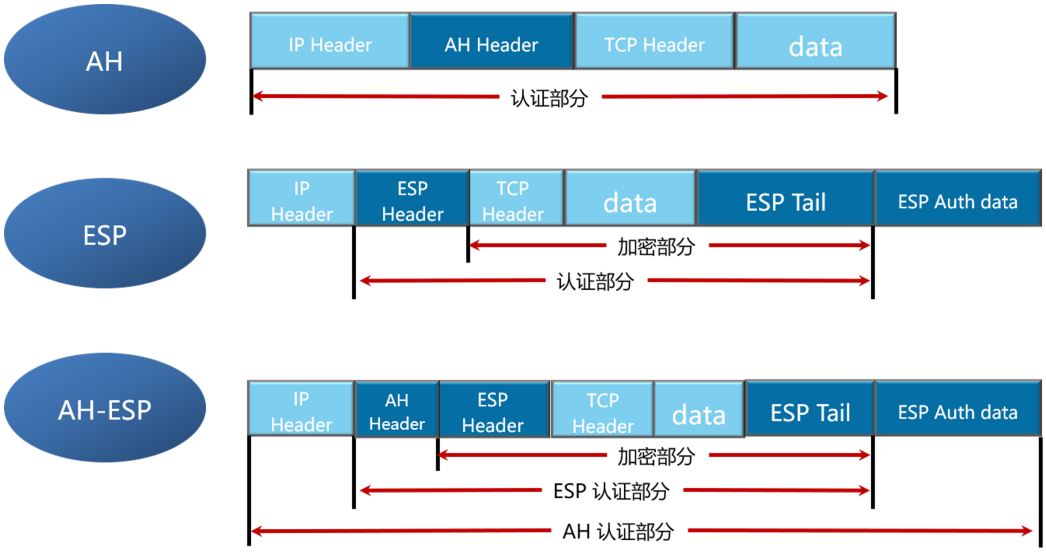
十一、IPSec的工作模式有2种：

1、传输模式：传输模式下， AH或ESP报头位于IP报头和传输层报头之间；传输模式中的AH或ESP主要对上层协议数据提供保护

1.1、传输模式中的AH：在IP头部之后插入AH头，对整个IP数据包进行完整性校验

1.2、传输模式中的ESP：在IP头部之后插入ESP头，在数据字段后插入尾部以及认证字段。对高层数据和ESP尾部进行加密，对IP数据包中的ESP报文头，高层数据和ESP尾部进行完整性校验

1.3、传输模式中的AH+ESP：在IP头部之后插入AH和ESP头，在数据字段后插入尾部以及认证字段

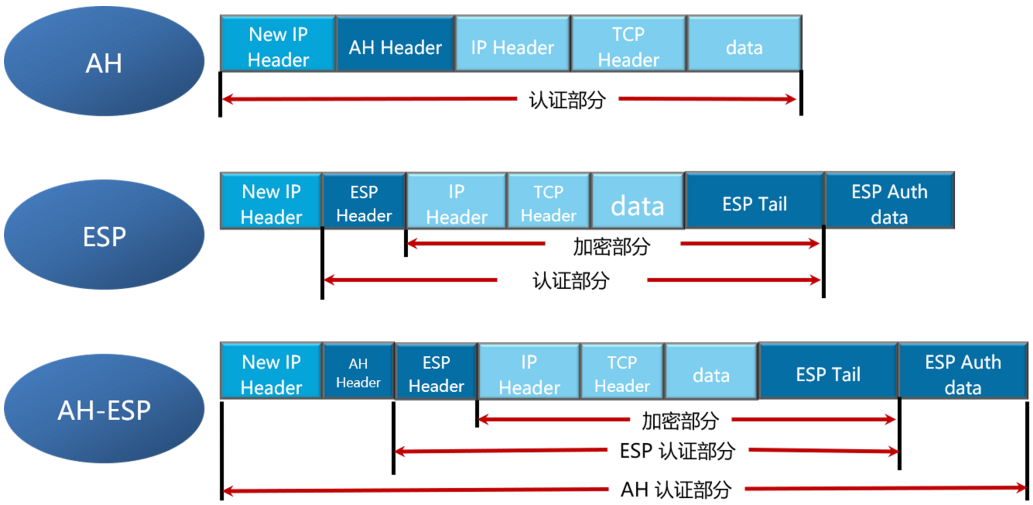


2、隧道模式：IPSec会另外生成一个新的IP报头，并封装在AH或ESP之前；隧道模式中，AH或ESP头封装在原始IP报文头之前，并另外生成一个新的IP头封装到AH或ESP之前。隧道模式可以完全地对原始IP数据报进行认证和加密，而且，可以使用IPSec对等体的IP地址来隐藏客户机的IP地址

2.1、隧道模式中的AH：对整个原始IP报文提供完整性检查和认证，认证功能优于ESP。但AH不提供加密功能，所以通常和ESP联合使用

2.2、隧道模式中的ESP：对整个原始IP报文和ESP尾部进行加密，对ESP报文头、原始IP报文和ESP尾部进行完整性校验

2.3、隧道模式中的AH+ESP：对整个原始IP报文和ESP尾部进行加密，AH、ESP分别会对不同部分进行完整性校验



十二、GRE【通用的路由封装】

1、GRE的概述

1.1、GRE最早由Cisco开发，目的是希望能够在建立VPN隧道的两端实现路由协议的相互传输，替代掉IPSec VPN手动建立感兴趣流的繁杂操作（IPSec VPN需要管理员手动配置ACL来定义需要加密的感兴趣流量）

1.2、GRE隧道可以在其中透传组播流量

1.3、令其它的非IP网络协议【IPX、AppleTalk】也能够在IP协议中进行透传

1.4、GRE属于无状态协议，在隧道传送数据前不调整任何参数

1.5、GRE几乎没有任何的安全性可言，不支持加密和认证

1.6、GRE需要创建隧道接口，只要隧道的目的地是可路由的，GRE的隧道便能够建立成功，将各种数据封装在其中

1.7、GRE需要至少添加一个24Byte的头部，其中新的IP头部占20Byte，GRE头部默认只有4Byte

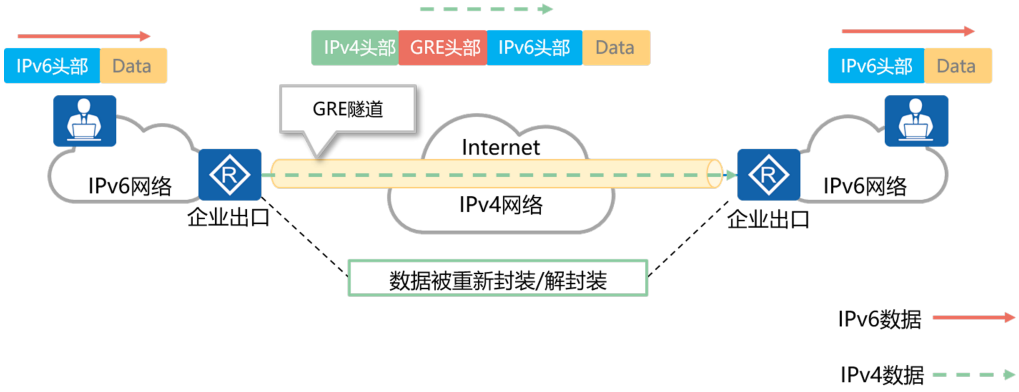
1.8、GRE的4Byte头部可分为2对儿：

1.8.1、第一对儿字节（0 — 15bit）为GRE标志字段，表明是否有GRE可选项【校验和（4Byte）、密钥（4Byte）、序列号（4Byte）】

1.8.2、第二对儿字节为GRE的协议字段

1.9、IPSec需要手动配置感兴趣流，且IPSec只支持IP协议，且不支持组播；而GRE又没有安全性可言，因此在部署时，往往将GRE与IPSec共同使用，组成GRE over IPSec VPN

注：GRE隧道需要创建一个隧道接口，该隧道接口类似于Loopback接口，是一个逻辑接口，主要用来跨网段建立隧道使用

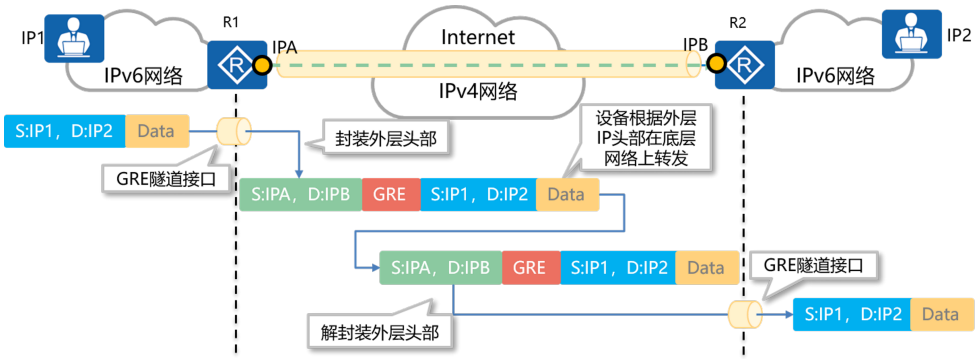


2、GRE构成要素分为3个部分：乘客协议、封装协议和运输协议

2.1、乘客协议：指用户在传输数据时所使用的原始网络协议

2.2、封装协议：作用就是用来"包装"乘客协议对应的报文，使原始报文能够在新的网络中传输

2.3、运输协议：指被封装以后的报文在新网络中传输时所使用的网络协议



3、上图的整体转发流程如下：

3.1、当R1收到IP1发来的IPv6数据包，查询设备路由表，发现出接口是隧道接口，则将此报文发给隧道接口处理

3.2、隧道接口给原始报文添加GRE头部，然后根据配置信息，给报文加上IP头。该IP头的源地址就是隧道源地址，IP头的目的地址就是隧道目的地址

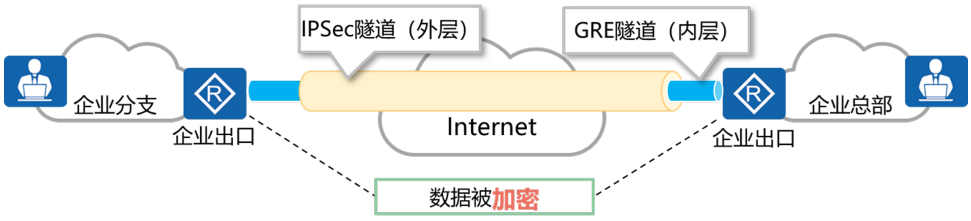
3.3、封装后的报文在IPv4网络中进行普通的IPv4路由转发，最终到达目的地R2

4、GRE Over IPSec

4.1、GRE的主要缺点是不支持加密和认证，数据的安全传输得不到很好的保障

4.2、IPSec的主要缺点是只支持IP协议，且不支持组播

4.3、可通过部署GRE Over IPSec结合两种VPN技术的优点



十三、L2TP VPN

1、L2TP VPN的概念

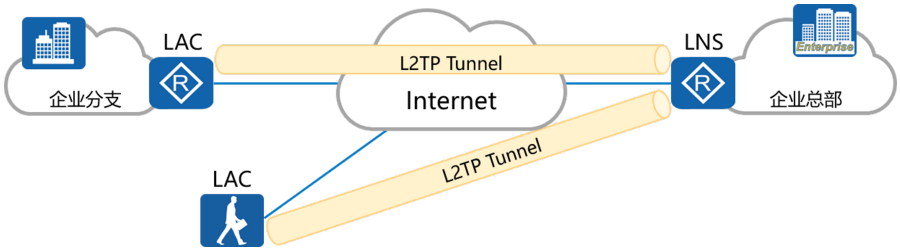
1.1、L2TP VPN属于二层VPN，与L2TP VPN相似的二层VPN还包括：PPTP VPN、Cisco Easy VPN、L2F等

1.2、L2TP是虚拟私有拨号网VPDN【Virtual Private Dial-up Network】隧道协议的一种，它扩展了点到点协议PPP的应用，是一种在远程办公场景中为出差员工或企业分支远程访问企业内网资源提供接入服务的VPN

1.3、VPDN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，为企业、小型ISP、移动办公人员提供接入服务

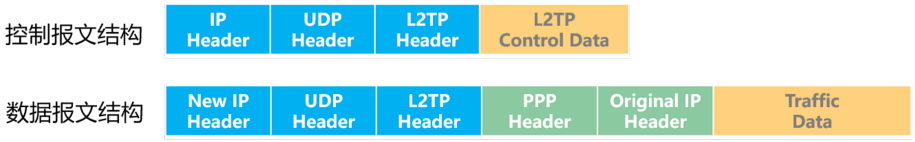
1.4、VPDN采用专用的网络加密通信协议，在公共网络上为企业建立安全的虚拟专网。企业驻外机构和出差人员可从远程经由公共网络，通过虚拟加密隧道实现和企业总部之间的网络连接，而公共网络上其它用户则无法穿过虚拟隧道访问企业网内部的资源。VPDN隧道协议有多种，目前使用最广泛的是L2TP

1.5、L2TP组网架构中包括LAC【L2TP Access Concentrator | L2TP访问集中器】和LNS【L2TP Network Server | L2TP网络服务器】
1.6、LAC是网络上具有PPP和L2TP协议处理能力的设备。LAC负责和LNS建立L2TP隧道连接。在不同的组网环境中，LAC可以是不同的设备，可以是一台网关设备，也可以是一台终端设备。LAC可以发起建立多条L2TP隧道使数据流之间相互隔离
1.7、LNS是LAC的对端设备，即LAC和LNS建立了L2TP隧道；LNS位于企业总部私网与公网边界，通常是企业总部的网关设备

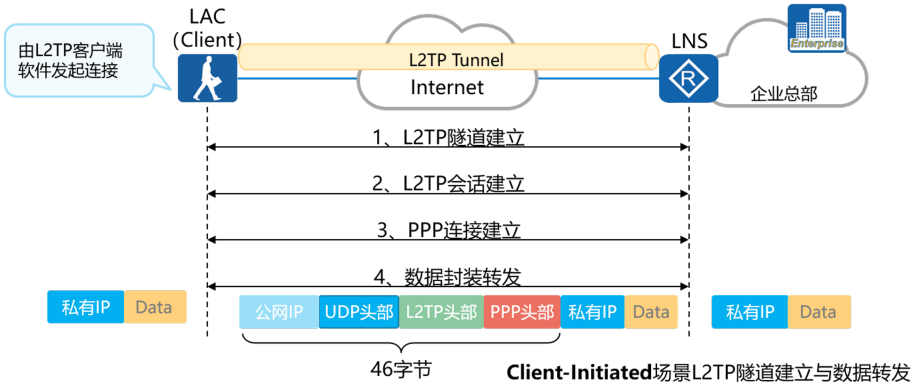


2、L2TP的消息类型
L2TP协议包含两种类型的消息，控制消息和数据消息，消息的传输在LAC和LNS之间进行
2.1、控制消息：用于L2TP隧道和会话连接的建立、维护和拆除
2.1.1、在控制消息的传输过程中，使用消息丢失重传和定时检测隧道连通性等机制来保证控制消息传输的可靠性，支持对控制消息的流量控制和拥塞控制
2.1.2、控制消息承载在L2TP控制通道上，控制通道实现了控制消息的可靠传输，将控制消息封装在L2TP报头内，再经过IP网络传输

2.2、数据消息：用于封装PPP数据帧并在隧道上传输
2.2.1、数据消息是不可靠的传输，不重传丢失的数据报文，不支持对数据消息的流量控制和拥塞控制
2.2.2、数据消息携带PPP帧承载在不可靠的数据通道上，对PPP帧进行L2TP封装，再经过IP网络传输



3、L2TP工作过程
L2TP主要可分为以下三种工作场景，其工作过程并不相同：



Client-Initiated场景L2TP隧道建立与数据转发

3.1、NAS-Initiated场景：拨号用户通过NAS访问企业内网
3.1.1、由远程拨号用户发起，远程系统通过PSTN/ISDN拨入LAC，由LAC通过Internet向LNS发起建立隧道连接请求。拨号用户地址由LNS分配；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
3.1.2、用户必须采用PPP的方式接入到Internet，也可以是PPPoE等协议
3.1.3、运营商的接入设备【主要是BAS设备】需要开通相应的VPN服务。用户需要到运营商处申请该业务
3.1.4、L2TP隧道两端分别驻留在LAC侧和LNS侧，且一个L2TP隧道可以承载多个会话
注：BAS【宽带接入服务器】：随着宽带城域网和宽带业务的发展，对于用户已不能简单地采用包月制、无认证的管理办法。宽带接入服务器【BAS】是一种设置在网络汇聚层的用户接入服务设备，可以智能化地实现用户的汇聚、认证、计费等服务，还可以根据用户的需要，方便地提供多种IP增值业务

3.2、Client-Initiated场景：移动办公用户访问企业内网

3.2.1、直接由LAC客户【指可在本地支持L2TP协议的用户】发起。客户需要知道LNS的IP地址。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，并且给LAC客户分配私有IP地址

3.2.2、用户需要安装L2TP的拨号软件。部分操作系统自带L2TP客户端软件

3.2.3、用户上网的方式和地点没有限制，不需ISP介入

3.2.4、L2TP隧道两端分别驻留在用户侧和LNS侧，一个L2TP隧道承载一个L2TP会话

3.2.5、该场景建立过程如下：

a、移动办公用户与LNS建立L2TP隧道

b、移动办公用户与LNS建立L2TP会话：移动办公用户在第3步会与LNS间建立PPP连接，L2TP会话用来记录和管理它们之间的PPP连接状态。因此，在建立PPP连接以前，隧道双方需要为PPP连接预先协商出一个L2TP会话。会话中携带了移动办公用户的LCP协商信息和用户认证信息，LNS对收到的信息认证通过后，通知移动办公用户会话建立成功。L2TP会话连接由会话ID进行标识

c、移动办公用户与LNS建立PPP连接。移动办公用户通过与LNS建立PPP连接获取LNS分配的企业内网IP地址

d、移动办公用户发送业务报文访问企业总部服务器

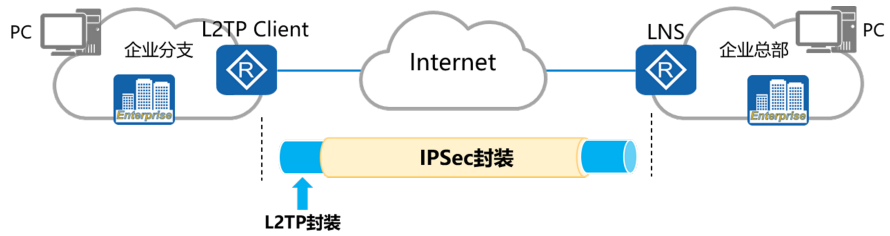
3.3、Call-LNS场景：通过LAC自主拨号实现企业内网互连

L2TP除了可以为出差员工提供远程接入服务以外，还可以进行企业分支与总部的内网互联，实现分支用户与总部用户的互访。一般是由分支路由器充当LAC与LNS建立L2TP隧道，这样就可实现分支与总部网络之间的数据通过L2TP隧道互通

4、L2TP over IPSec

4.1、当企业对数据和网络的安全性要求较高时，L2TP无法为报文传输提供足够的保护。这时可以和IPSec功能结合使用，保护传输的数据，有效避免数据被截取或攻击

4.2、企业出差用户和总部通信，使用L2TP功能建立VPN连接，总部部署为LNS对接入的用户进行认证。当出差用户需要向总部传输高机密信息时，L2TP无法为报文传输提供足够的保护，这时可以和IPSec功能结合使用，保护传输的数据。在出差用户的PC终端上运行拨号软件，将数据报文先进行L2TP封装，再进行IPSec封装，发往总部。在总部网关，部署IPSec策略，最终还原数据。这种方式IPSec功能会对所有源地址为LAC、目的地址为LNS的报文进行保护



十四、IPSec VPN、GRE隧道、GRE over IPSec VPN、L2TP VPN的配置

详细配置见实验手册