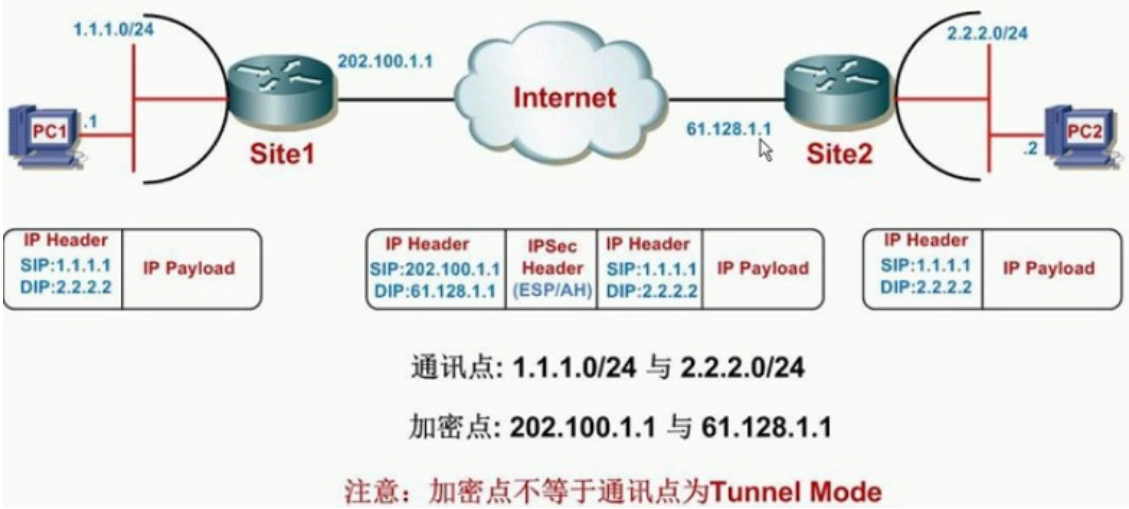
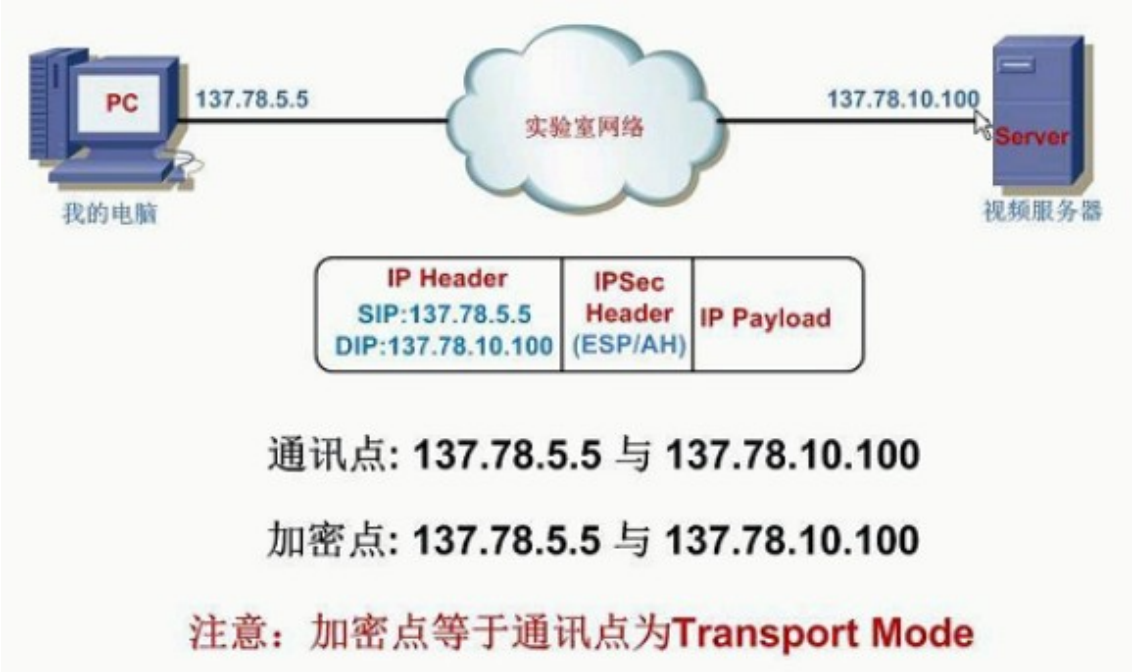
VPN 技术概述


加密
DES 3DES AES
验证
MD5 SHA-1
封装协议
ESP AH
模式
Transport Tunnel
密钥有效期
3600 1800


1.1.1.0/24
202.100.1.1
Internet
2.2.2.0/24
PC1
.1
Site1
61.128.1.1
Site2
.2
PC2
IP Header
SIP:1.1.1.1
DIP:2.2.2.2
IP Payload
IP Header
SIP:202.100.1.1
DIP:61.128.1.1
IPSec Header
(ESP/AH)
IP Header
SIP:1.1.1.1
DIP:2.2.2.2
IP Payload
IP Header
SIP:1.1.1.1
DIP:2.2.2.2
IP Payload
通讯点: 1.1.1.0/24 与 2.2.2.0/24
加密点: 202.100.1.1 与 61.128.1.1
注意：加密点不等于通讯点为Tunnel Mode



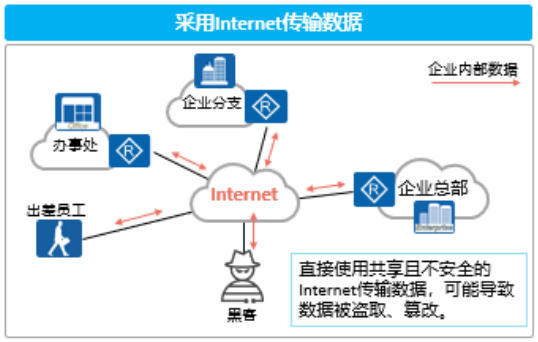
	主模式	野蛮模式
消息交互	交互6个消息	交互3个消息
身份ID	以IP地址作为身份ID，自动生成本端身份ID和对端身份ID	可以以多种形式（IP，字符串等）手动或自动的生成本端和对端的身份ID
域共享密钥	只能基于IP地址来确定预共享密钥。	基于ID信息（主机名和IP地址）来确定预共享密钥。
安全性	**较高** 前4个消息以明文传输，最后两个消息加密，对对端身份进行了保护	**较低** 前两个消息以明文传输，最后一个消息进行加密，不保护对端身份
速度	较慢	较快

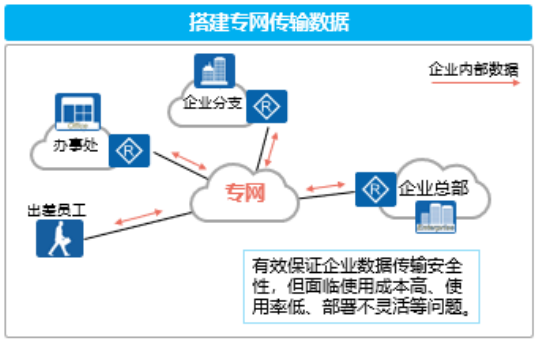
- 对于规模较大的企业来说，网络访问需求不仅仅局限于公司总部网络内，分公司、办事处、出差员工、合作单位等也需要访问公司总部的网络资源，可以采用 VPN（Virtual Private Network，虚拟专用网络）技术来实现这一需求。VPN 可以在不改变现有网络结构的情况下，建立虚拟专用连接。因其具有廉价、专用和虚拟等多种优势，在现网中应用非常广泛。

- VPN 是一类技术的统称，不同的 VPN 技术拥有不同的特性和实现方式，常见的 VPN 技术包括 IPSec VPN、GRE VPN、L2TP VPN、MPLS VPN 等。
- 本课程将从 VPN 的定义、常见的 VPN 类型与应用场景等几个方面对 VPN 进行一个简单而又全面的介绍。

技术背景

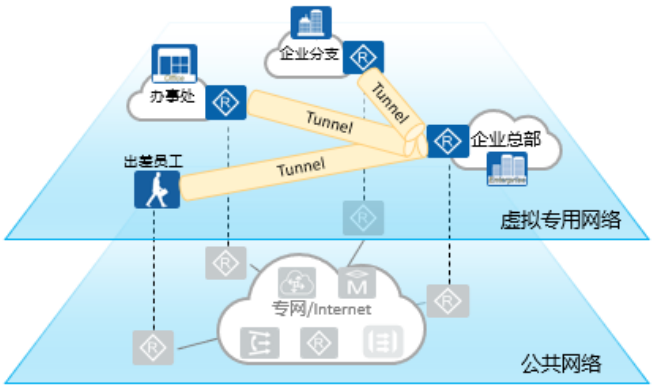
- 在VPN出现之前，企业分支之间的数据传输只能依靠现有物理网络（例如Internet）。由于Internet中存在多种不安全因素，报文容易被网络中的黑客窃取或篡改，最终造成数据泄密、重要数据被破坏等后果。
- 除了通过Internet，还可以通过搭建一条物理专网连接保证数据的安全传输，但其费用会非常昂贵，且专网的搭建和维护十分困难。





VPN简介

VPN即虚拟专用网，泛指通过VPN技术在公用网络上构建的虚拟专用网络。VPN用户在此虚拟网络中传输私网流量，在不改变网络现状的情况下实现安全、可靠的连接。



专用（Private）

VPN网络是专门供VPN用户使用的网络，对于VPN用户，使用VPN与使用传统专网没有区别。VPN能够提供足够的安全保证，确保VPN内部信息不受外部侵扰。VPN与底层承载网络（一般为IP网络）之间保持资源独立，即VPN资源不被网络中非该VPN的用户所使用。

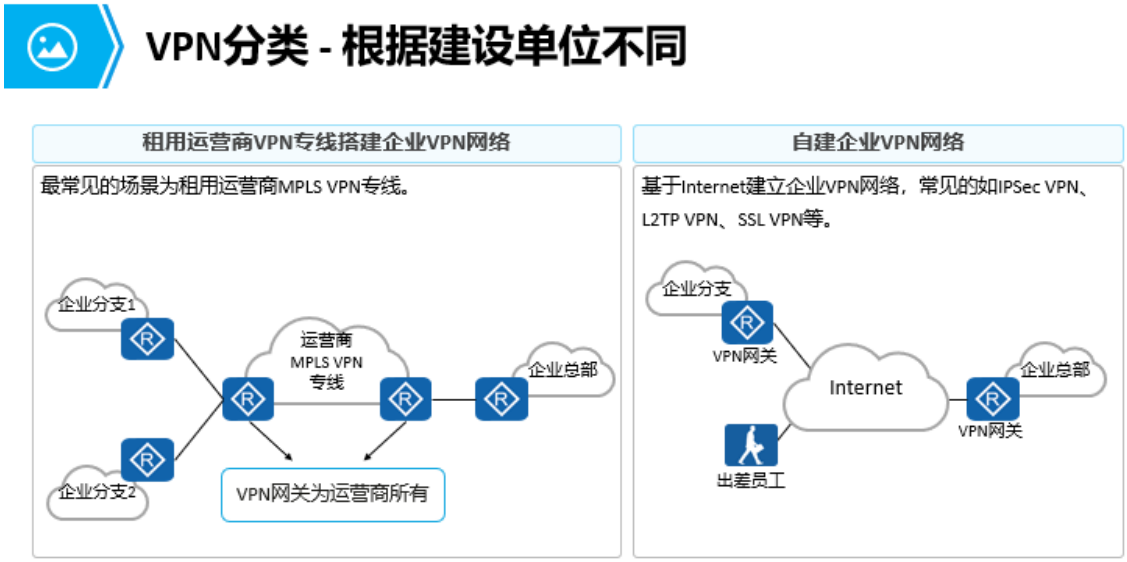
虚拟（Virtual）

VPN用户的通信是通过公共网络进行的，而这个公共网络同时也可以被其他非VPN用户使用，VPN用户获得的只是一个逻辑意义上的专网。

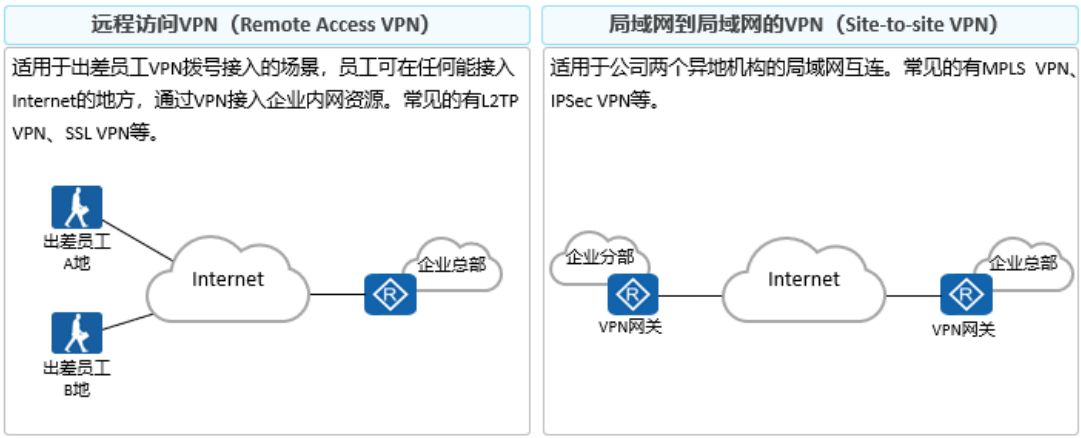
- VPN 和传统的数据专网相比具有如下优势：
- 安全：在远端用户、驻外机构、合作伙伴、供应商与公

司总部之间建立可靠的连接，保证数据传输的安全性。这对于实现电子商务或金融网络与通讯网络的融合特别重要。

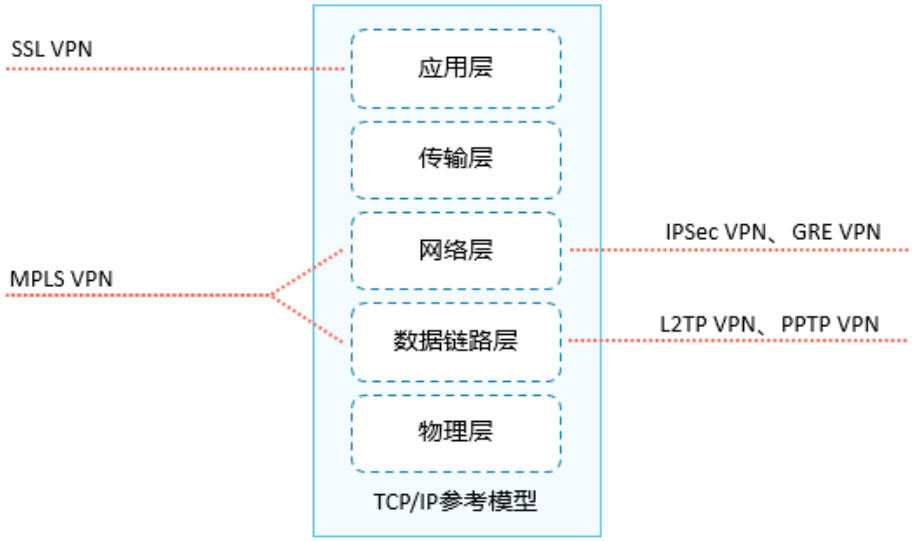
- 廉价：利用公共网络进行信息通讯，企业可以用更低的成本连接远程办事机构、出差人员和业务伙伴。
- 支持移动业务：支持驻外 VPN 用户在任何时间、任何地点的移动接入，能够满足不断增长的移动业务需求。
- 可扩展性：由于 VPN 为逻辑上的网络，物理网络中增加或修改节点，不影响 VPN 的部署。
- 公共网络又经常被称为 VPN 骨干网（VPN Backbone），公共网络可以是 Internet，也可以是企业自建专网或运营商租赁专网。



VPN分类 - 根据组网方式不同



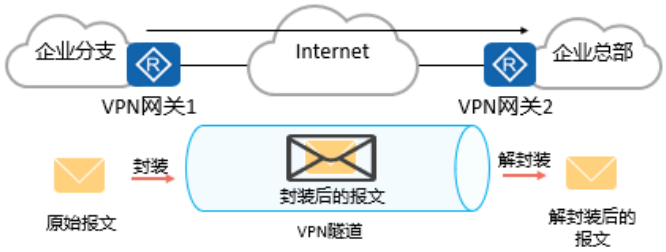
VPN分类 - 根据实现的网络层次



- 工作在网络层和数据链路层的 VPN 又被称为三层 VPN 和二层 VPN。

VPN关键技术 - 隧道技术

- VPN技术的基本原理是利用隧道（Tunnel）技术，对传输报文进行封装，利用VPN骨干网建立专用数据传输通道，实现报文的安全传输。
- 位于隧道两端的VPN网关，通过对原始报文的“封装”和“解封装”，建立一个点到点的虚拟通信隧道。



- 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。
- 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。
- 部分隧道可以混合使用，如 GRE Over IPSec 隧道。

VPN关键技术 - 身份认证、数据加密与验证

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：

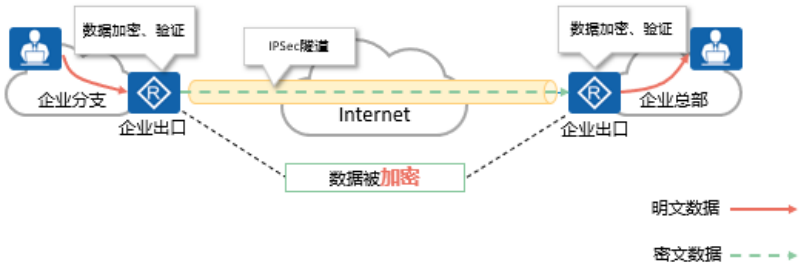
- 身份认证：可用于部署了远程接入VPN的场景，VPN网关对用户的身份进行认证，保证接入网络的都是合法用户而非恶意用户。也可以用于VPN网关之间对对方身份的认证。
- 数据加密：将明文通过加密变成密文，使得数据即使被黑客截获，黑客也无法获取其中的信息。
- 数据验证：通过数据验证技术对报文的完整性和真伪进行检查，丢弃被伪造和被篡改的报文。

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。

IPSec GRE L2TP MPLS

IPSec概述

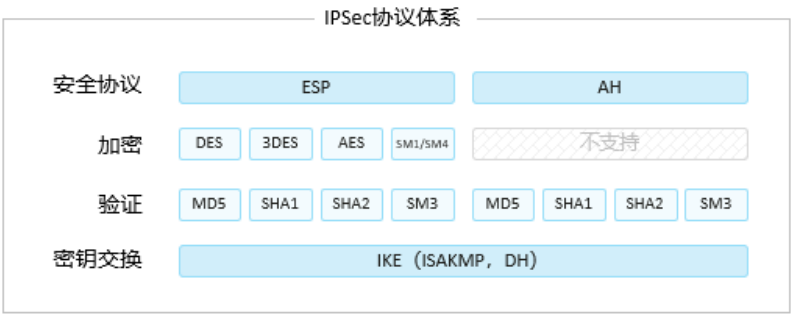
IPSec（IP Security） VPN一般部署在企业出口设备之间，通过加密与验证等方式，实现了数据来源验证、数据加密、数据完整性保证和抗重放等功能。



- 数据来源验证：接收方验证发送方身份是否合法。
- 数据加密：发送方对数据进行加密，以密文的形式在Internet上传送，接收方对接收的加密数据进行解密后处理或直接转发。
- 数据完整性：接收方对接收的数据进行验证，以判定报文是否被篡改。
- 抗重放：接收方拒绝旧的或重复的数据包，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。

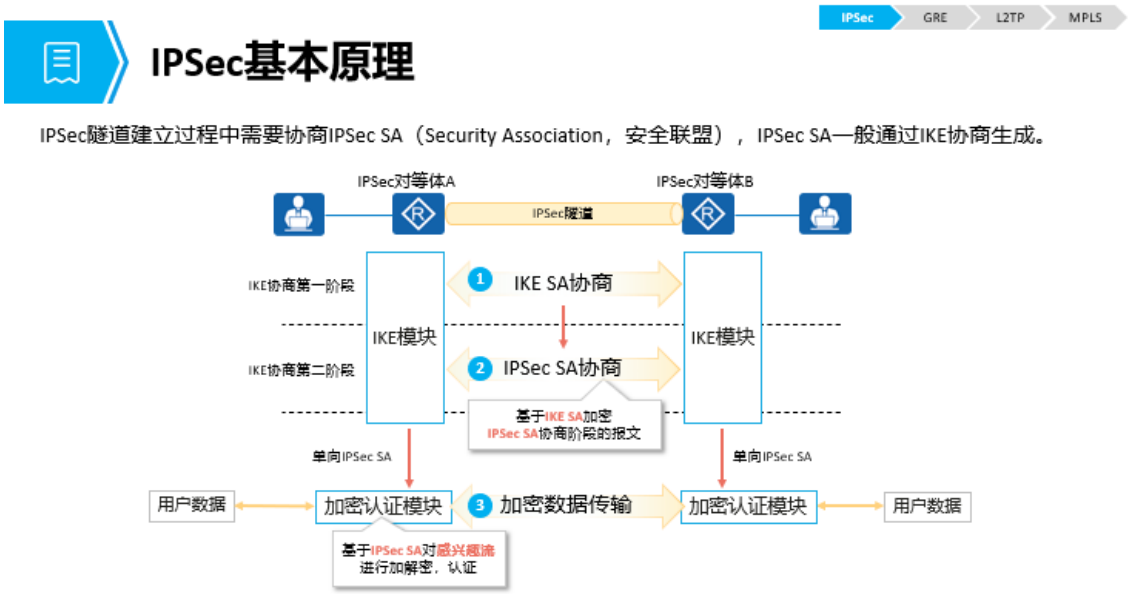
IPSec协议体系

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，包括AH（Authentication Header）、ESP（Encapsulating Security Payload）、IKE（Internet Key Exchange）等协议。



- 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。
- AH 和 ESP 协议提供的安全功能依赖于协议采用的验证、加密算法。
- AH 仅支持认证功能，不支持加密功能。ESP 支持认证和加密功能。
- 安全协议提供认证或加密等安全服务需要有秘钥的存在。
- 秘钥交换的方式有两种：
- 带外共享密钥：在发送、接收设备上手工配置静态的加密、验证密钥。双方通过带外共享的方式（例如通过电话或邮件方式）保证密钥一致性。这种方式的缺点是可扩展性差，在点到多点组网中配置密钥的工作量成倍增加。另外，为提升网络安全性需要周期性修改密钥，这种方式下也很难实施。
- 通过 IKE 协议自动协商密钥：IKE 建立在 Internet 安全联盟和密钥管理协议 ISAKMP 定义的框架上，采用 DH（Diffie-Hellman）算法在不安全的网络上安全地分发密钥。这种方式配置简单，可扩展性好，特别是在大型动态的网络环境下此优点更加突出。同时，通信双方通过交换密钥交换材料来计算共享的密钥，即使第三方截获了双方用于计算密钥的所有交换数

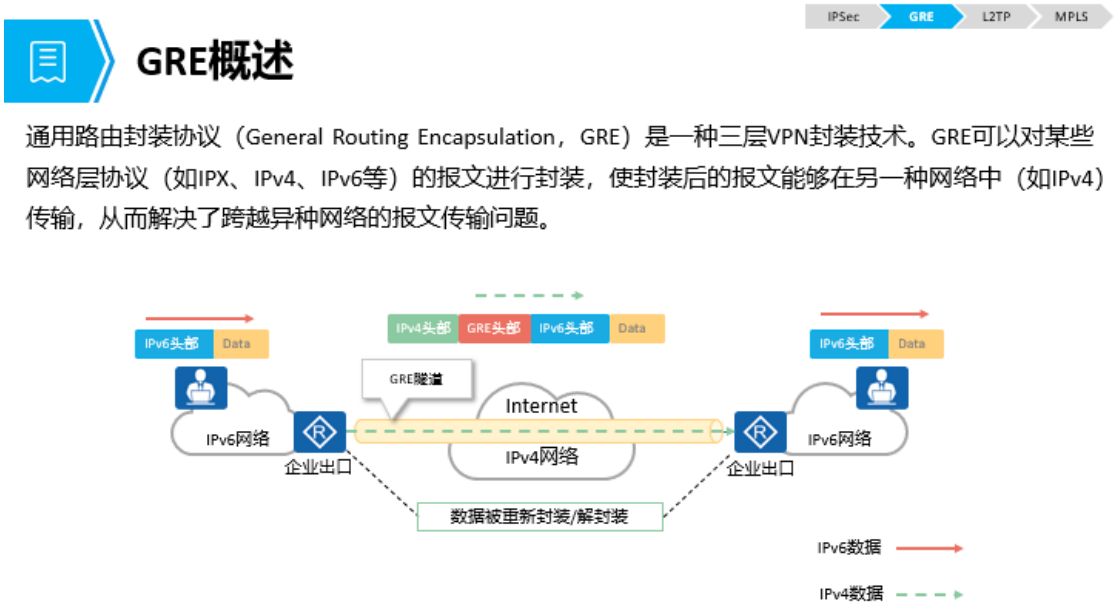
据，也无法计算出真正的密钥。



- SA 由一个三元组来唯一标识，这个三元组包括安全参数索引 SPI（Security Parameter Index）、目的 IP 地址和使用的安全协议号（AH 或 ESP）。其中，SPI 是为唯一标识 SA 而生成的一个 32 位比特的数值，它在 AH 和 ESP 头中传输。在手工配置 SA 时，需要手工指定 SPI 的取值。使用 IKE 协商产生 SA 时，SPI 将随机生成。
- SA 是单向的逻辑连接，因此两个 IPSec 对等体之间的双向通信，最少需要建立两个 SA 来分别对两个方向的数据流进行安全保护。
- IKE 作为秘钥协商协议，存在两个版本：IKEv1 和 IKEv2，本课程采用 IKEv1 为例进行介绍，IKEv2 内容可参考产品文档对应内容。
- 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。
- IKEv1 协商阶段 2 的目的就是建立用来安全传输数据的 I

PSec 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。

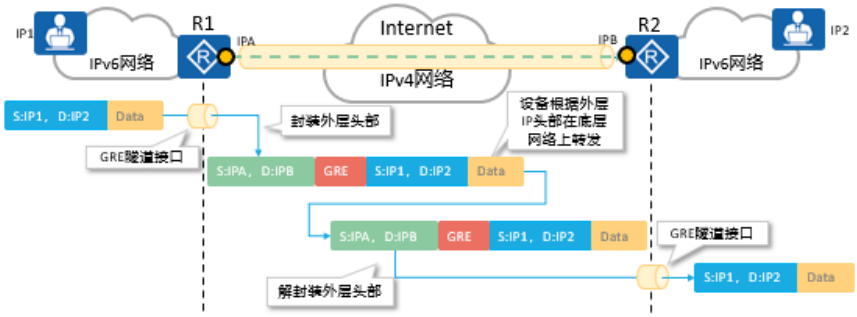
- IKE 协商成功意味着双向的 IPSec 隧道已经建立，可以通过 ACL 方式或者安全框架方式定义 IPSec“感兴趣流”，符合感兴趣流流量特征的数据都将被送入 IPSec 隧道进行处理。
- 感兴趣流：需要被 IPSec 保护的数据流。



- 如图所示，通过在 IPv4 网络上建立 GRE 隧道，解决了两个 IPv6 网络的通信问题。
- GRE 还具备封装组播报文的能力。由于动态路由协议中会使用组播报文，因此更多时候 GRE 会在需要传递组播路由数据的场景中被用到，这也是 GRE 被称为通用路由封装协议的原因。

GRE基本原理

- GRE构成要素分为3个部分：乘客协议、封装协议和运输协议。
  - 乘客协议是指用户在传输数据时所使用的原始网络协议。
  - 封装协议的作用就是用来“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。
  - 运输协议是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。



- 隧道接口（Tunnel Interface）是为实现报文的封装而提供的一种点对点类型的虚拟接口，与 Loopback 接口类似，都是一种逻辑接口。
- 如图所示，乘客协议为 IPv6，封装协议为 GRE，运输协议为 IPv4。整体转发流程如下：
- 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。
- 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。
- 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。
- 解封装过程和封装过程相反，这里不再赘述。

IPSec GRE L2TP MPLS

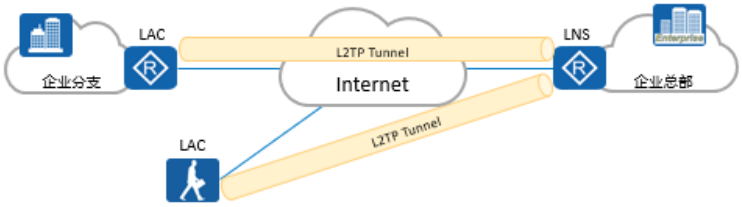
GRE Over IPSec

- 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。
- IPSec的主要缺点是只支持IP协议，且不支持组播。
- 可通过部署GRE Over IPSec结合两种VPN技术的优点。

IPSec GRE L2TP MPLS

L2TP概述

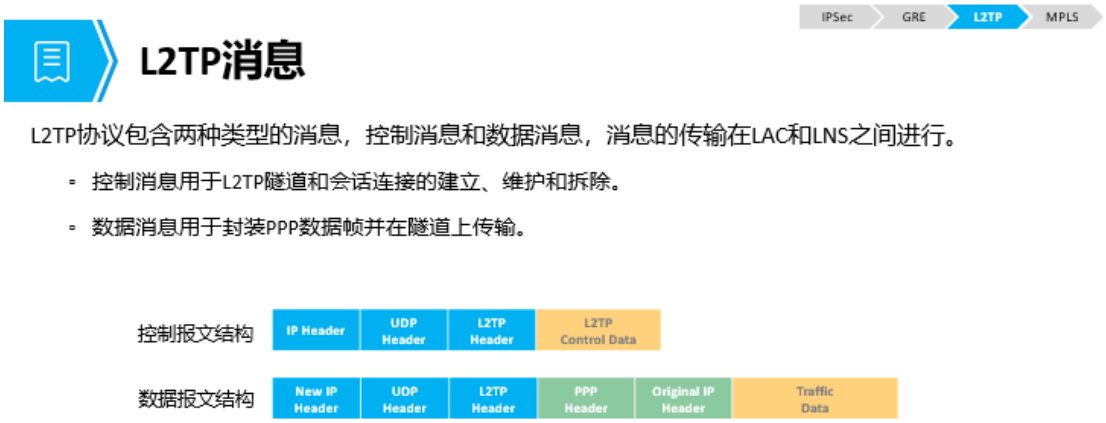
- L2TP是虚拟私有拨号网VPDN（Virtual Private Dial-up Network）隧道协议的一种，它扩展了点到点协议PPP的应用，是一种在远程办公场景中为出差员工或企业分支远程访问企业内网资源提供接入服务的VPN。
- L2TP组网架构中包括LAC（L2TP Access Concentrator，L2TP访问集中器）和LNS（L2TP Network Server，L2TP网络服务器）



- 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。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。
- 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。

- 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。

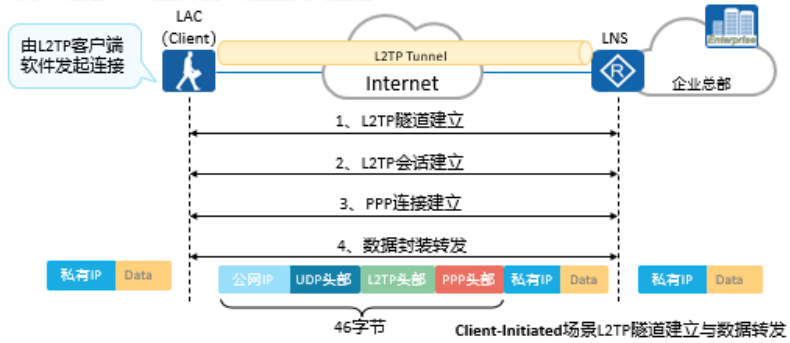


- 控制消息
- 用于 L2TP 隧道和会话连接的建立、维护和拆除。在控制消息的传输过程中，使用消息丢失重传和定时检测隧道连通性等机制来保证控制消息传输的可靠性，支持对控制消息的流量控制和拥塞控制。
- 控制消息承载在 L2TP 控制通道上，控制通道实现了控制消息的可靠传输，将控制消息封装在 L2TP 报头内，再经过 IP 网络传输。
- 数据消息
- 用于封装 PPP 数据帧并在隧道上传输。数据消息是不可靠的传输，不重传丢失的数据报文，不支持对数据消息的流量控制和拥塞控制。
- 数据消息携带 PPP 帧承载在不可靠的数据通道上，对 PPP 帧进行 L2TP 封装，再经过 IP 网络传输。

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：

- NAS-Initiated场景：拨号用户通过NAS访问企业内网
- Client-Initiated场景：移动办公用户访问企业内网
- Call-LNS场景：通过LAC自主拨号实现企业内网互连

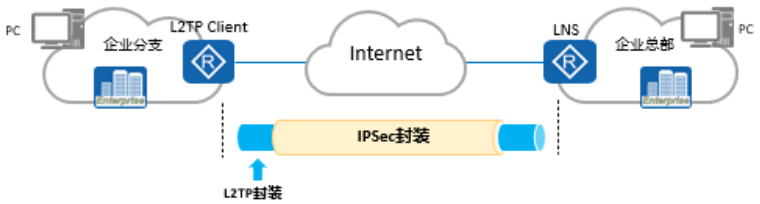


- NAS-Initiated 场景：由远程拨号用户发起，远程系统通过 PSTN/ISDN 拨入 LAC，由 LAC 通过 Internet 向 LNS 发起建立隧道连接请求。拨号用户地址由 LNS 分配；对远程拨号用户的验证与计费既可由 LAC 侧的代理完成，也可在 LNS 完成。
- 用户必须采用 PPP 的方式接入到 Internet，也可以是 PPPoE 等协议。
- 运营商的接入设备（主要是 BAS 设备）需要开通相应的 VPN 服务。用户需要到运营商处申请该业务。
- L2TP 隧道两端分别驻留在 LAC 侧和 LNS 侧，且一个 L2TP 隧道可以承载多个会话。
- Client-Initialized 场景：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。
- 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。

- 用户上网的方式和地点没有限制，不需 ISP 介入。
- 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。
- 该场景建立过程如下：
- 移动办公用户与 LNS 建立 L2TP 隧道。
- 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。
- 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。
- 移动办公用户发送业务报文访问企业总部服务器。
- Call-LNS 场景：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。

L2TP Over IPSec

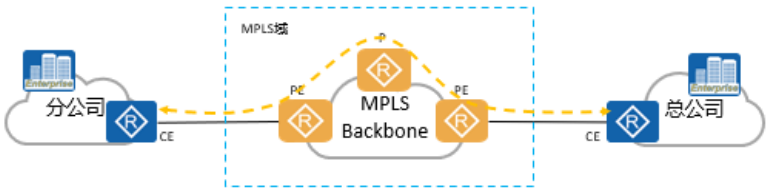
当企业对数据和网络的安全性要求较高时，L2TP无法为报文传输提供足够的保护。这时可以和IPSec功能结合使用，保护传输的数据，有效避免数据被截取或攻击。



- 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。

MPLS VPN概述

- MPLS是一种利用标签（Label）进行转发的技术，最初为了提高IP报文转发速率而被提出，现主要应用于VPN和流量工程、QoS等场景。
- 根据部署的不同，MPLS VPN可分为MPLS L2 VPN或者MPLS L3 VPN。
- 企业可以自建MPLS专网也可以通过租用运营商MPLS专网的方式获得MPLS VPN接入服务。



- MPLS VPN 网络一般由运营商搭建，VPN 用户购买 VP

N 服务来实现用户网络之间（图中的分公司和总公司）的路由传递、数据互通等。

- 基本的 MPLS VPN 网络架构由 CE（Customer Edge）、PE（Provider Edge）和 P（Provider）三部分组成：
- CE：用户网络边缘设备，有接口直接与运营商网络相连。CE 可以是路由器或交换机，也可以是一台主机。通常情况下，CE“感知”不到 VPN 的存在，也不需要支持 MPLS。
- PE：运营商边缘路由器，是运营商网络的边缘设备，与 CE 直接相连。在 MPLS 网络中，对 VPN 的所有处理都发生在 PE 上，对 PE 性能要求较高。
- P：运营商网络中的骨干路由器，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力，不维护 VPN 相关信息。
- 更多 MPLS 及 MPLS VPN 的相关内容，参考 HCIP-Datacom-Advance 相应课程。

思考题：

- （判断题）L2TP VPN 工作在网络层。
  A. 正确
  B. 错误
- （多选题）IPSec SA 包含以下哪些内容？
  A. SPI
  B. 安全协议
  C. 源地址
  D. 目的地址

答案：

- B
- ABD