G-LAB

G-CNP v2.0课程

讲师：沈老师

课程介绍

01 IPSec理论、L2L-VPN

02 IPSec-VPN网络穿越问题

03 IPSec-VPN高可用性技术

04 DMVPN技术

课程内容

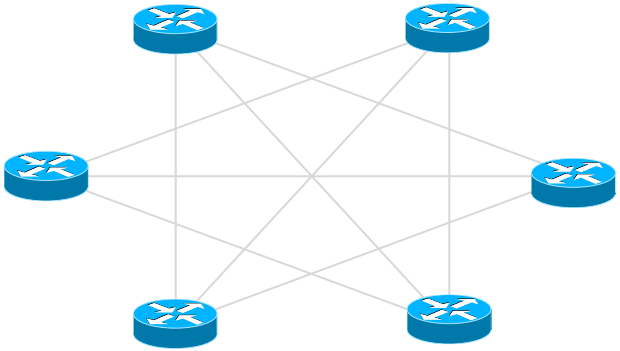
1. L2L基本理论

2. L2L实验

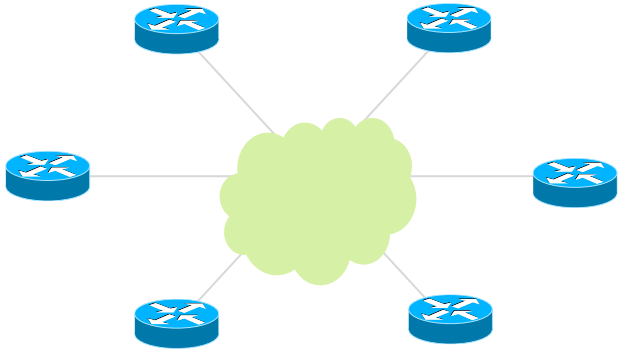
3. GRE OVER IPSEC

实施VPN的动机

专线连接



利用公网资源



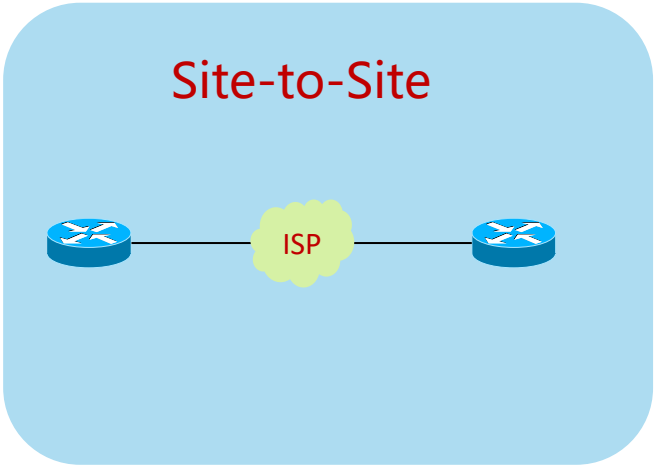
最大的动机是：省钱

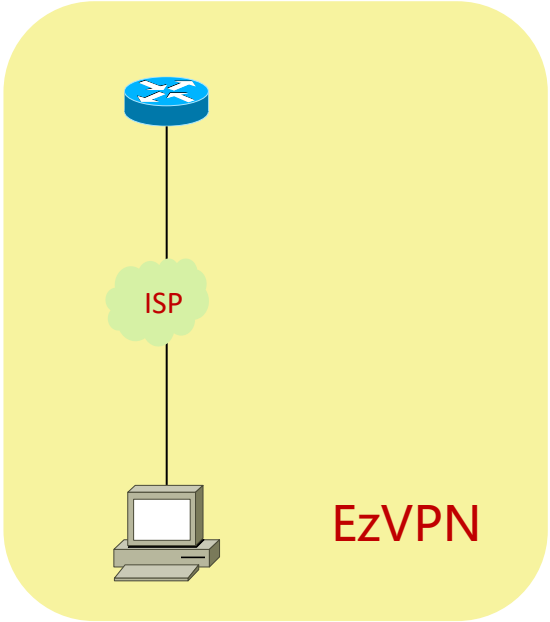
使用VPN带来的问题

数据安全

带宽保障

两种VPN模型





站点到站点VPN

1. ATM
2. Frame Relay
3. MPLS VPN
4. IPSec

远程访问VPN

1. IPSec
2. PPTP
3. L2TP+IPSec
4. SSLVPN

IPSec 简介

“Internet 协议安全性 (IPSec)”是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议 (IP) 网络上进行保密而安全的通讯

IPSec 框架

1. 加密　DES/3DES/AES…
2. 验证　MD5/SHA-1….
3. 封装协议 ESP/AH….
4. 模式　Transport/Tunnel
5. 密钥有效期　3600/1800
6. …….

IPSec 两种加密学算法

1. 对称加密算法
2. 非对称加密算法

IPSec 对称加密学算法

特点：同一个密钥用于加解密

优点：速度快
安全
紧凑

缺点：明文传输共享密钥
密钥数量指数增长
密钥管理和存储很大问题
不支持数字签名和不可否认性

非对称加密特点

- **特点：**
  - 用一个密钥加密的东西只能用另一个密钥来解密。
  - 仅仅只用于:密钥交换（加密密钥）和数字签名（加密散列）。
- **优点：**
  - 安全。
  - 因为不必发送密钥给接受者，所以非对称加密不必担心密钥被中途截获的问题。
  - 密钥数目和参与者的数目一样。
  - 不需要事先在各参与者之间建立关系以交换密钥。
  - 技术支持数字签名和不可否认性。
- **缺点：**
  - 非常非常慢。
  - 密文会变长。

理想的解决方案

1. 必须安全
2. 速度必须快
3. 加密后的密文必须紧凑
4. 适应参与者很多的情况
5. 必须抵抗密钥窃听
6. 不能要求事先在参与者之间建立某种关系
7. 必须支持数字签名和不可否认性

理想的解决方案

流行的加密算法

对称加密算法：

DES（56）

3DES（3X56）

AES

RH4

非对称加密算法：

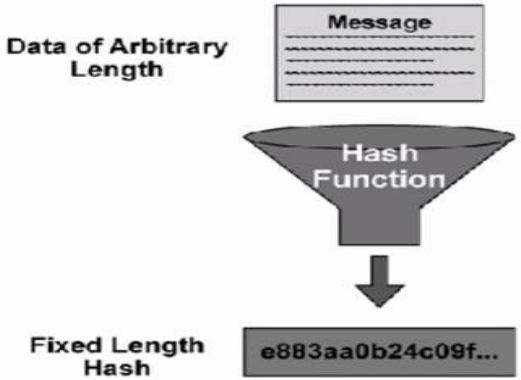
RSA

DH

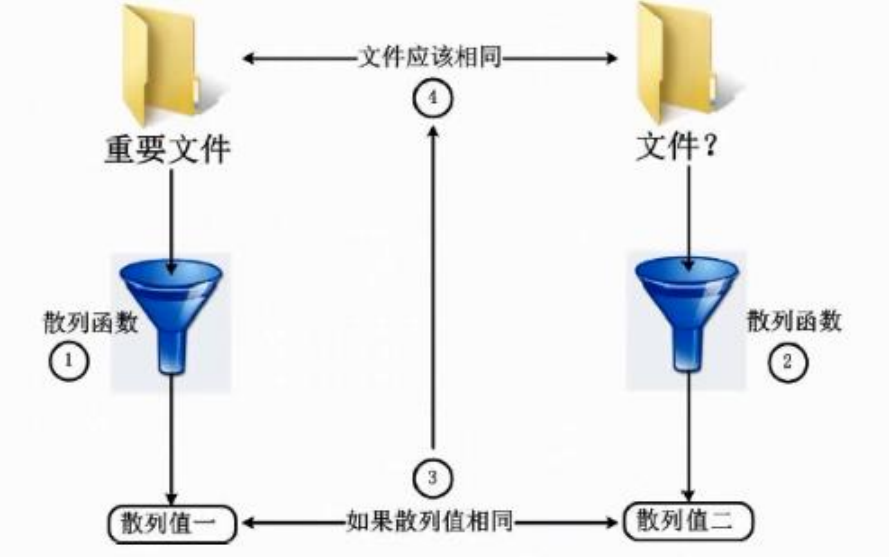
ECC

散列函数

A hash function is a means of turning data into a relatively small number that then may act as a digital **fingerprint** of the data。



散列函数特点



1. 固定大小
2. 雪崩效应
3. 单向
4. 冲突避免

流行的散列算法
MD5
SHA

散列函数应用

1.动态路由协议验证
2.IOS image校验
3.Chap认证
4.数字签名
5.IPSec

路由器配置的hash：

```
Router#verify /md5 system:running-config
.Done!
verify /md5 (system:running-config) = c60936ba773c54224b9502b550fbf47c
```

IPSec 组成部分

安全协议：AH ESP

密钥管理：ISAKMP IKE SKEME

算法：用于加密和身份验证

IPSec 两种模式

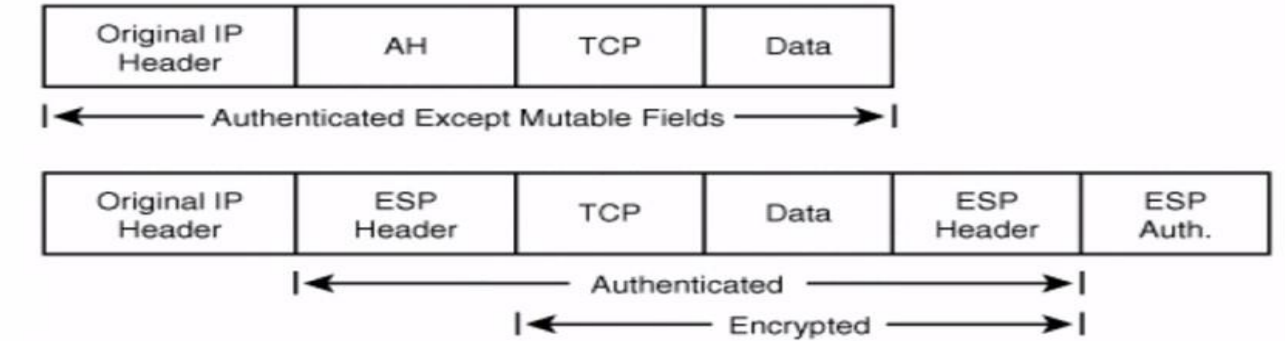
Transport Mode

从IPSec VPN的角度考虑，这种模式在需要保护的是两台主机之间

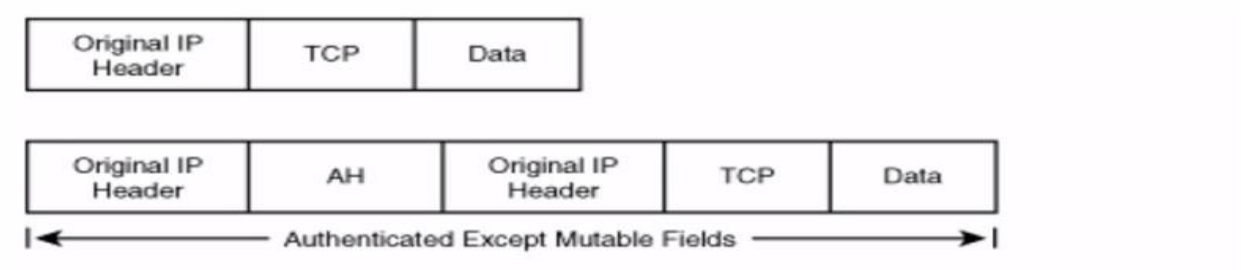
Tunnel Mode

从IPSec VPN的角度考虑，这种模式在需要保护的是多台主机的两个站点之间

Transport Mode

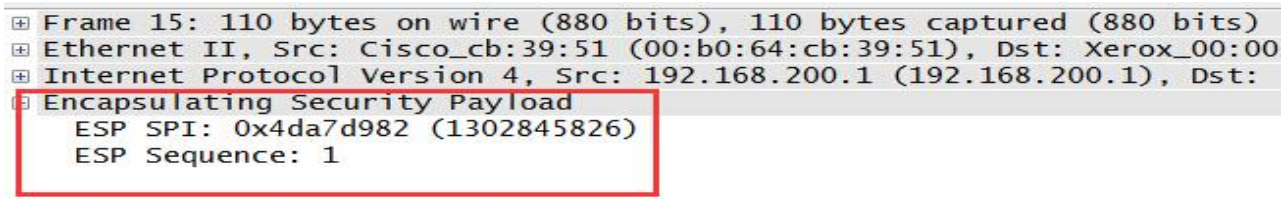


Tunnel Mode



注意：AH(51)只能验证；ESP(50)既能验证也能加密

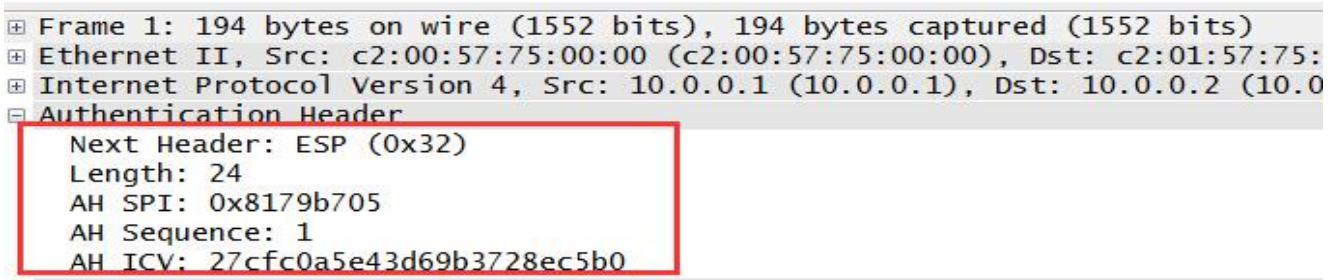
ESP 包格式



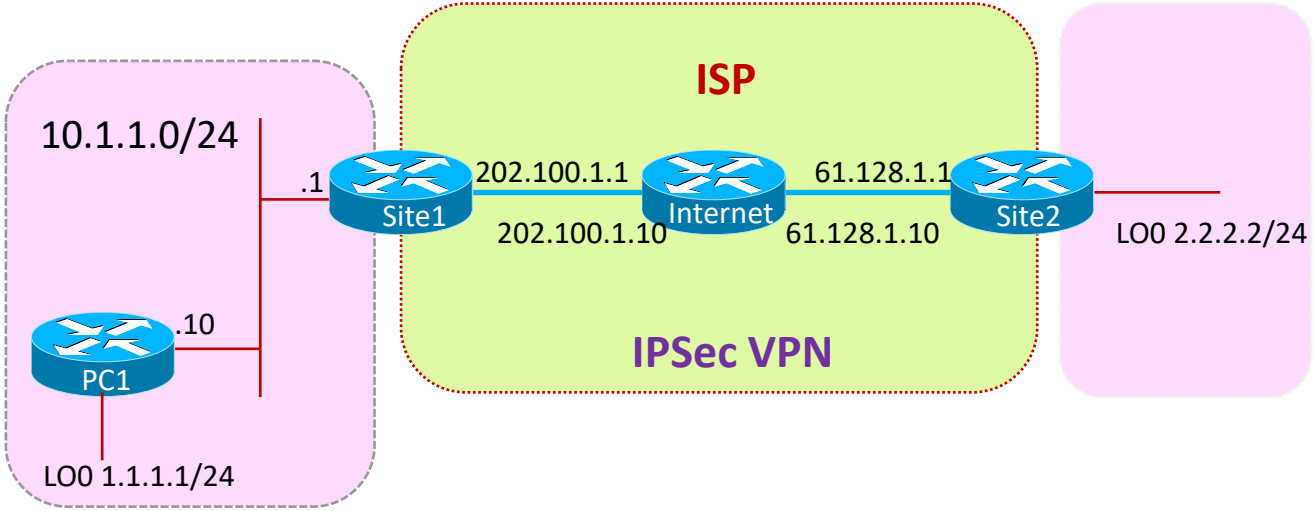
SPI：是目标对等体在IKE协商期间随意选择的一个数字，
类似于索引，在SADB中查找SA

序列号：发送方插入到ESP包头，提供反重放服务

AH 包格式



L2L实例拓扑



IP Header SIP:202.100.1.1 DIP:61.128.1.1	IPSEC Header ESP	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

PC to PC实例拓扑

通讯点：1.1.1.0/24与2.2.2.0/24

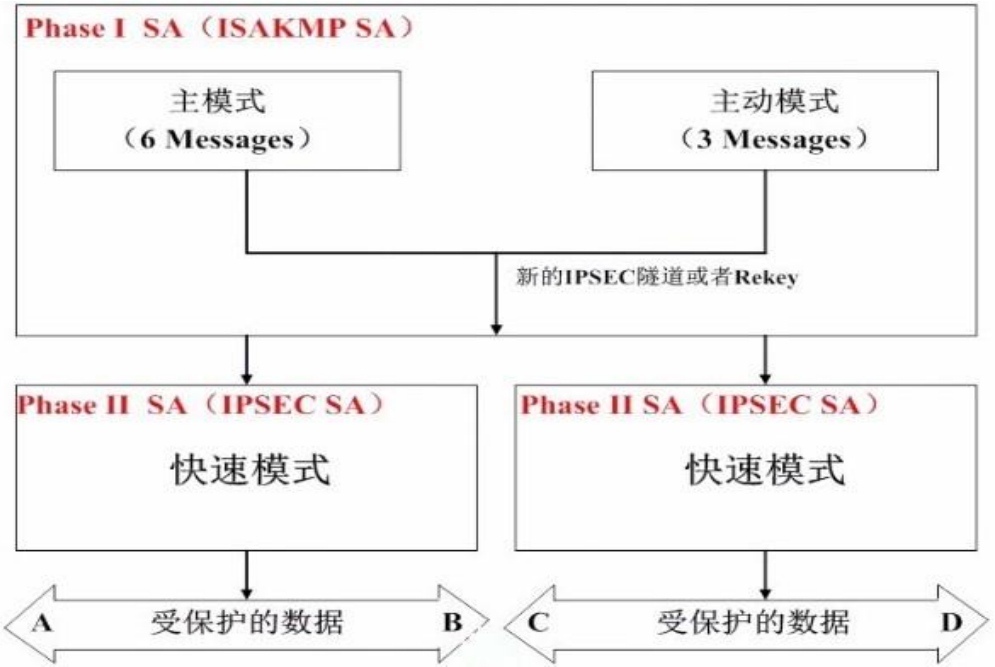
加密点：1.1.1.1与2.2.2.2

IKE 介绍

IKE负责建立和维护IKE SAs和 IPSec SAs。功能主要体现在如下几个方面：

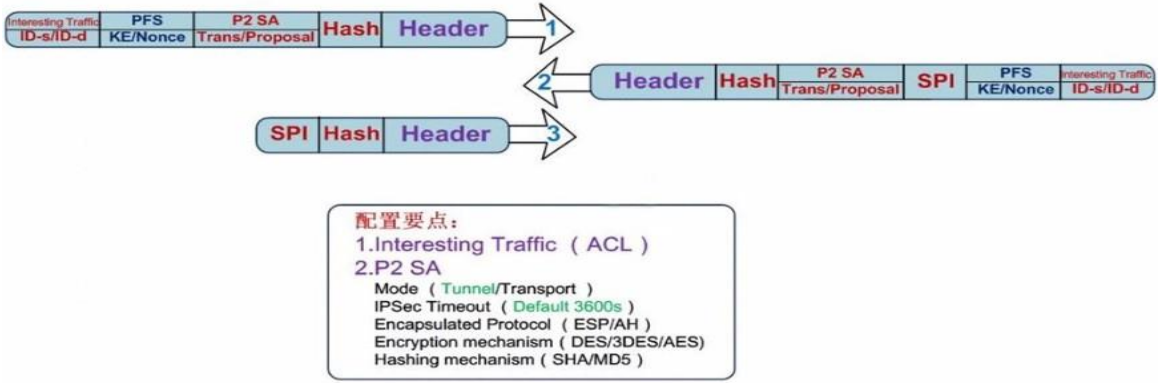
- 对双方进行认证
- 交换公共密钥，产生密钥资源，管理密钥。
- 协商协议参数（封装，加密，验证....）

IKE 的三个模式

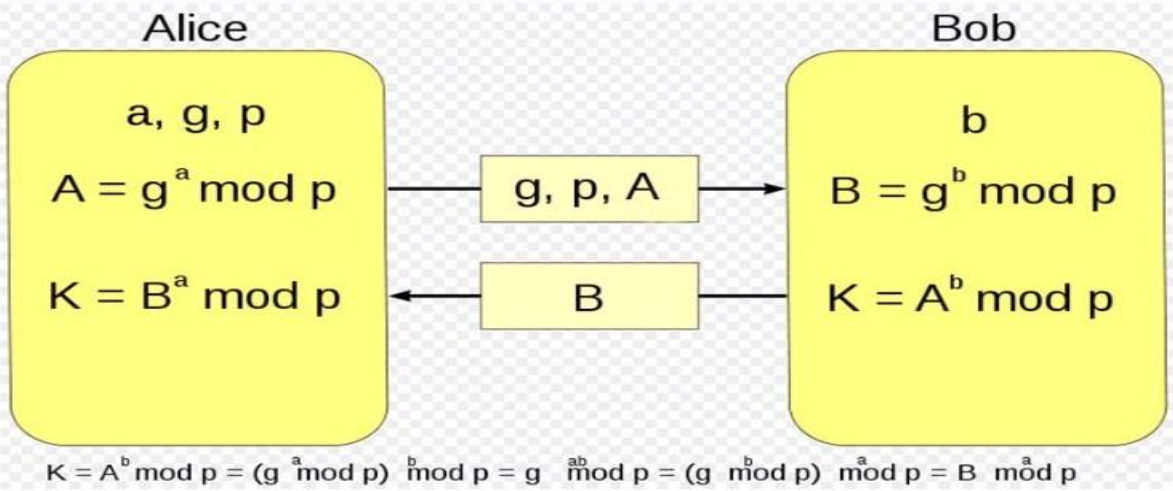


Main Mode示意图

Quick Mode示意图



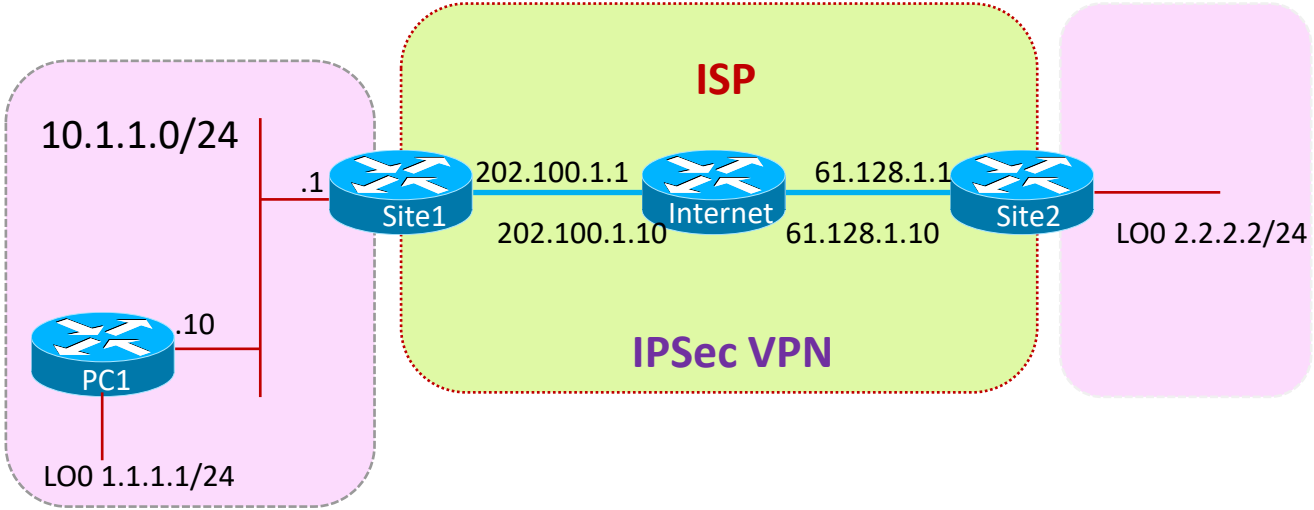
DH 密钥管理协议



L2L配置步骤

1. ISAKMP policy
2. Transform set
3. Interesting traffic
4. Crypto map

实验拓扑



IPSec VPN查看命令

- Show crypto isakmp sa
- Show crypto engine connections active
- Show crypto session

- Clear crypto isakmp 清除ISAKMP/IKE SA
- Clear crypto sa清除 IPSec SA

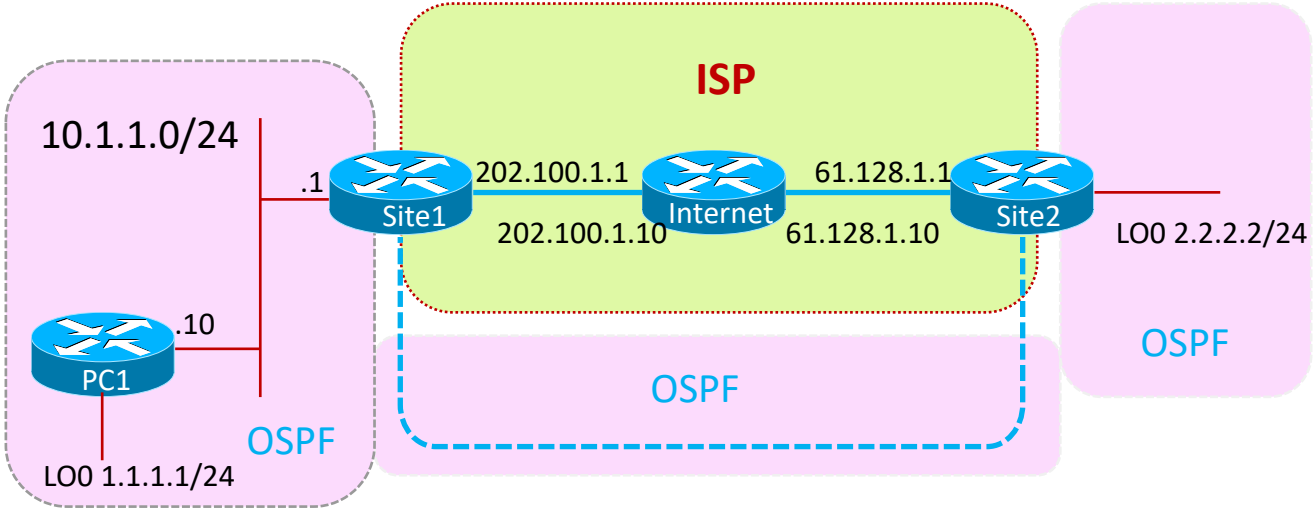
传统L2L几大问题

1. 不支持直接加密组播（最本质问题）
2. 不支持动态路由协议
3. 不提供QoS/FW.....

解决方案

1. GRE Over IPSec
2. SVTI（CCSP重点介绍）

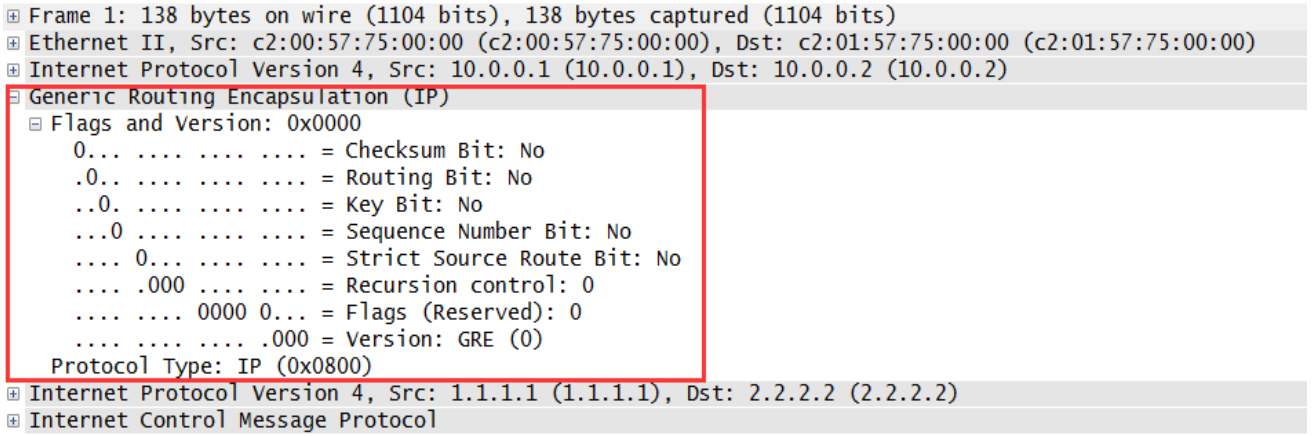
GRE Over IPSec



思考：

1. GRE的缺点是什么？
2. Tranfrom和Tunnel模式的数据封装区别？

GRE包头格式



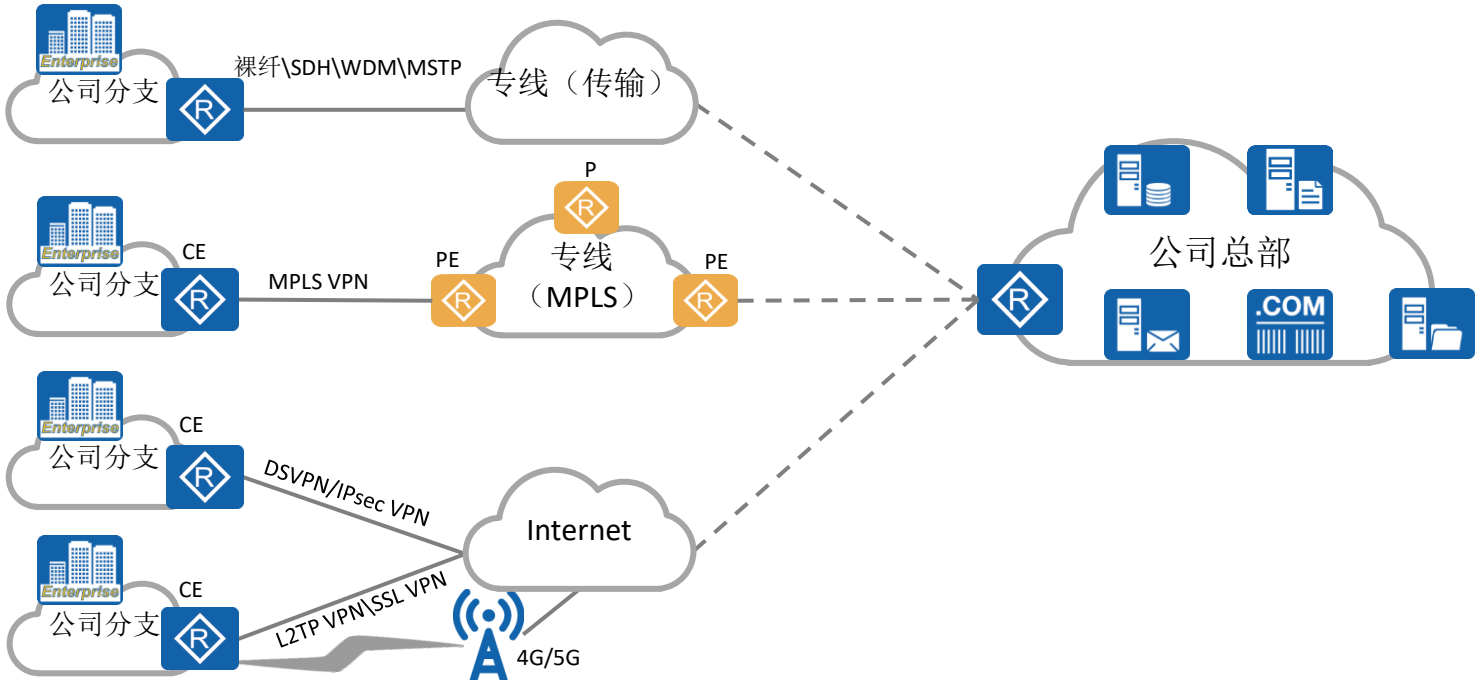
Tunnel VS Transport

前言

- 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。

企业网络广域互联典型架构

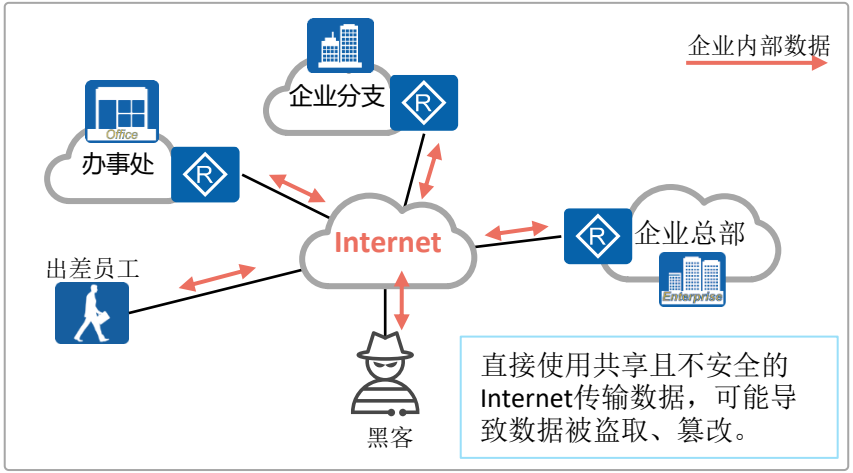
- 企业广域互联方式较多，基于企业不同的需求，一般会使用一种或多种互联方式。



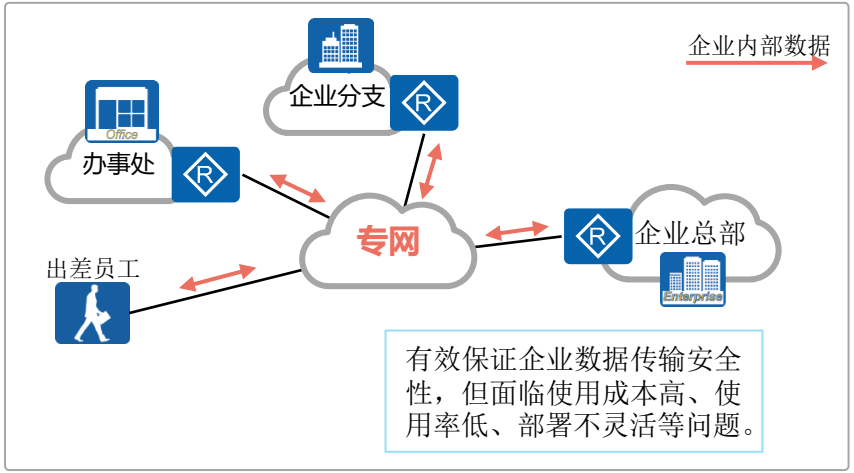
技术背景

- 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。

采用Internet传输数据



搭建专网传输数据



专线与VPN的对比

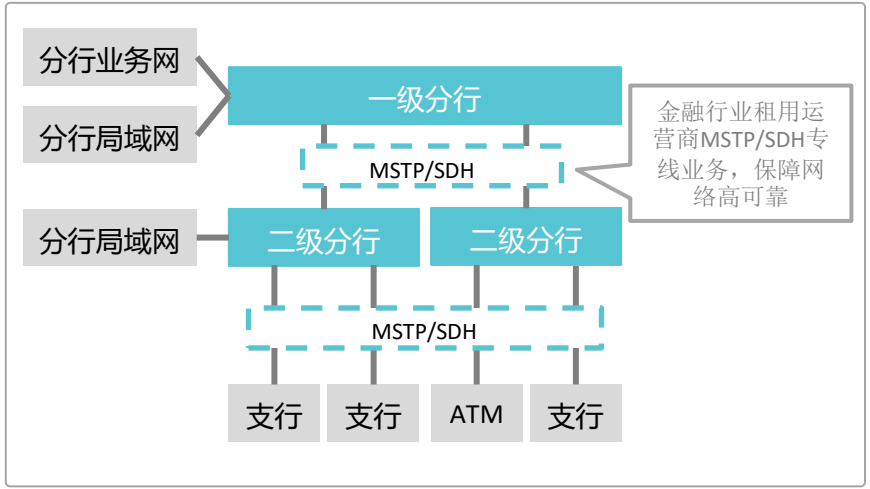
- 专线业务出现非常早，它能够很好的满足企业之间互联的需求，对于可靠性和安全性也有很好的保障，但是价格一直比较昂贵。
- 随着网络的发展，VPN技术开始占有更多的市场，但是部分对于网络有高安全高可靠性诉求的行业，比如金融行业依然愿意选择专线技术。
- 对于专线和VPN技术的取舍应该基于公司业务，从多方面比较。

	专线技术	VPN技术
安全性	比较高，安全依赖于ISP	非常高，数据加密传输，安全控制由用户掌握
可靠性	很高，主要依赖ISP的网络可靠性	比较高，依赖Internet线路的可靠性
可扩展性	依赖ISP，扩展存在中间环节，扩展性一般	基于TCP/IP，接入方式灵活，主要网络可达就可以扩展
投资成本	费用很高，需要按月支付专线租用费用，且网络建设初期需要投入设备费用	设备一次性费用投入，无需支出每月的运营费用
对移动用户的支持	只能连接专线到达的网络，不支持离开局域网的内部移动用户接入网络	内部移动用户可以使用Internet安全接入，消除地域差异
传输带宽	由于价格昂贵，一般租用的带宽都比较小	Internet价格低廉，租用带宽一般比较大
升级	依赖电信部门	自主可控，设备便宜

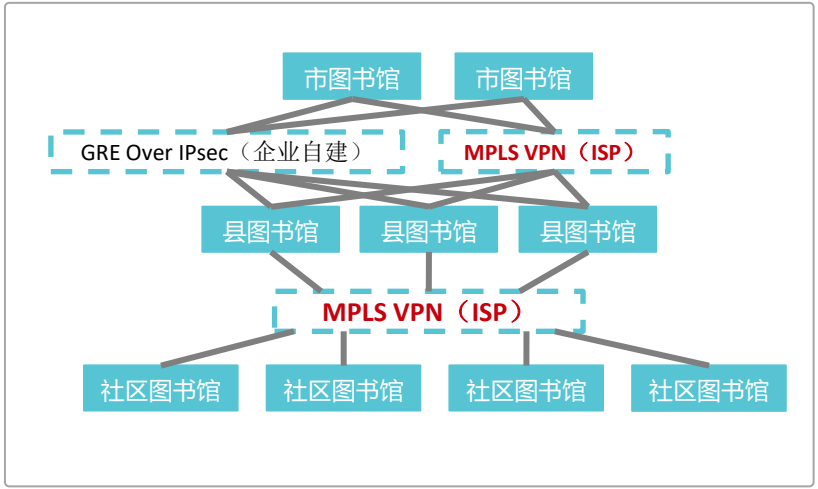
运营商专线介绍

- 运营商拥有大量线路资源，基于不同的行业与场景，运营商推出不同专线业务。
- 运营商高品质的传输专线业务主要是SDH，MSTP，裸纤等，价格昂贵，但是性能优异。
- 运营商还有一类专线业务是MPLS VPN，MPLS VPN专线能提供稍逊于传输专线的性能，但价格便宜。

运营商专线（金融行业专线网络）



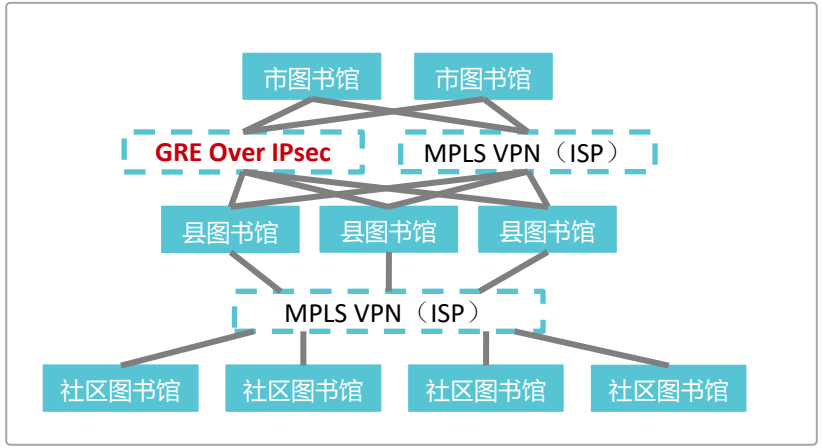
运营商专线（某省图书馆MPLS VPN网络）



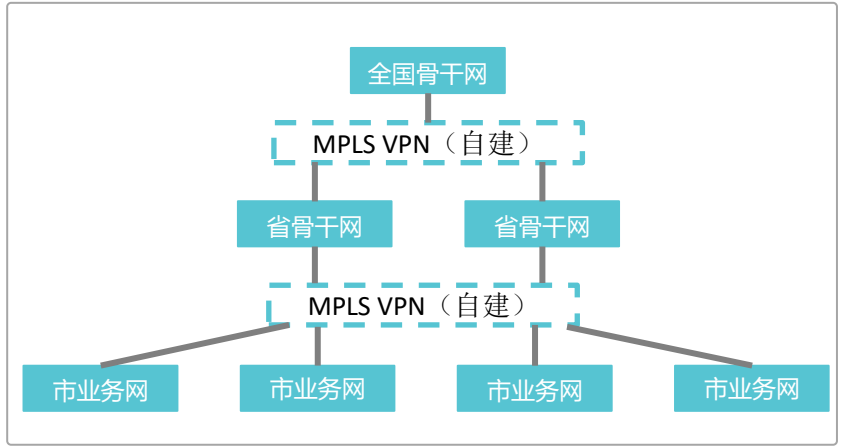
企业自建专线与VPN介绍

- 企业可以通过运营商网络自行建立VPN，比如：SSL VPN，DSVPN，IPsec VPN等。
- 部分大型企业有自行铺设光纤的能力，能够搭建企业MPLS VPN专线，但是拥有自行铺设光纤能力的企业较少。
- 企业自建VPN由于价格低廉，扩展方便，企业可控性强，使用越来越多。

企业自建VPN（某省图书馆VPN网络）



企业自建专线（能源行业业务MPLS VPN网络）

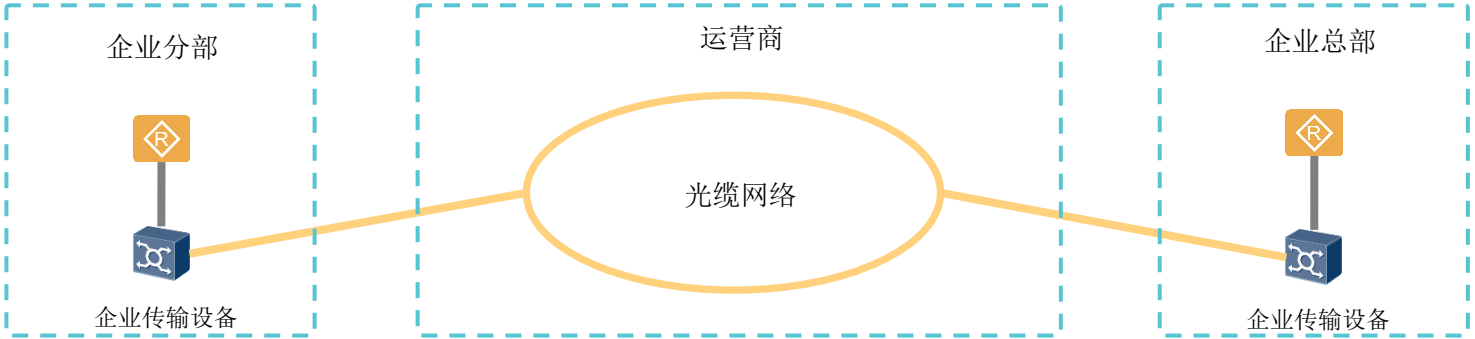


专线技术概述

- 专线技术诞生很早，由于网络的发展，很多技术已经不再使用，比如：帧中继，ATM等，现在使用比较多的专线技术基本分以下几种：
  - 裸纤：也叫裸光纤，运营商会提供光纤，中间不经过别的设备，光纤价格昂贵。
  - SDH/MSTP/WDM：传输类专线，这类专线使用传输设备在光纤上构建硬管道，能够保障良好的性能，价格比裸纤便宜。
  - MPLS VPN：MPLS专线，这类专线使用以太网做接入，基本不构建硬管道，在性能上比传输类专线弱，但是价格是专线中最便宜的。

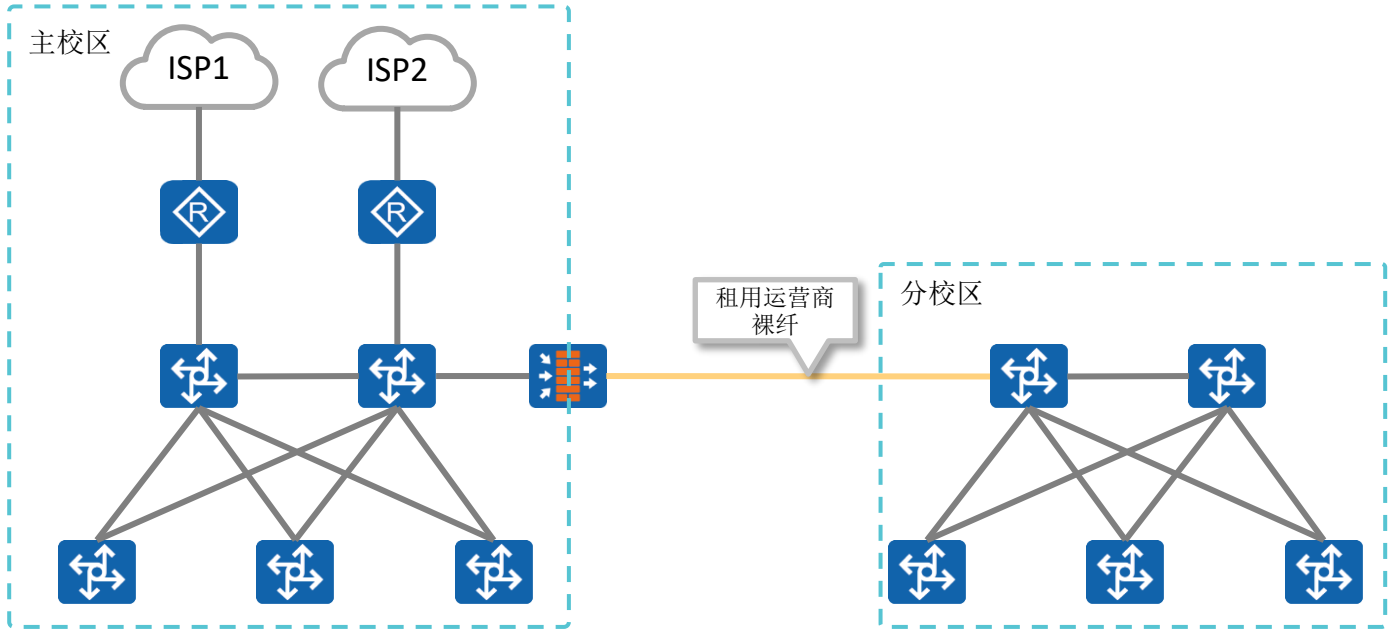
裸纤专线介绍

- 裸纤也叫裸光纤，运营商提供一条纯光纤线路，中间不经过任何设备，网络容量取决于光纤两端的企业设备。
- 裸纤按照距离收费，距离越远越贵，光纤有最大长度，一般认为光纤一跳最大距离是300 KM，超过300 KM的站点之间需要架设中继设备。



裸纤专线应用场景

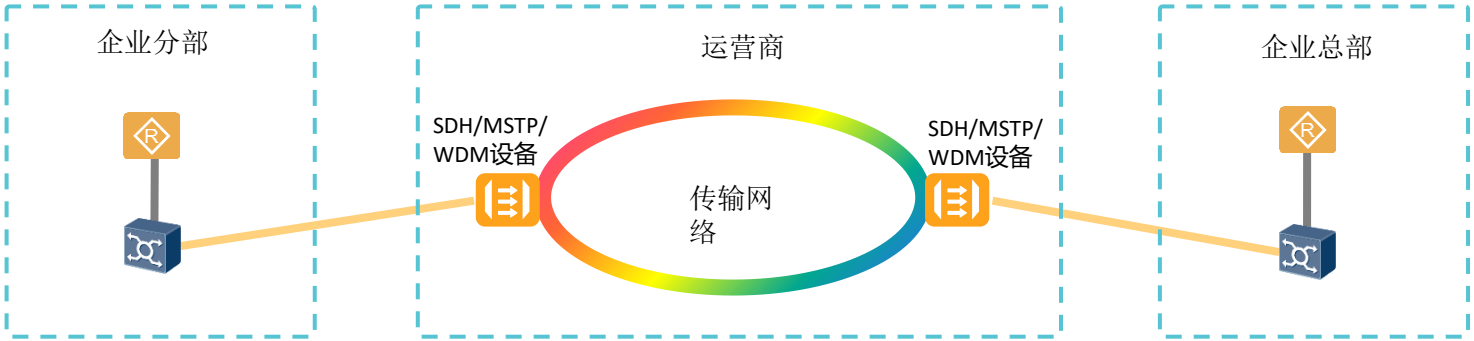
裸纤专线应用场景



- 同城的主校区和分校区之间可以租用运营商裸纤，将两个校区互联，简化网络管理和接入认证管理。

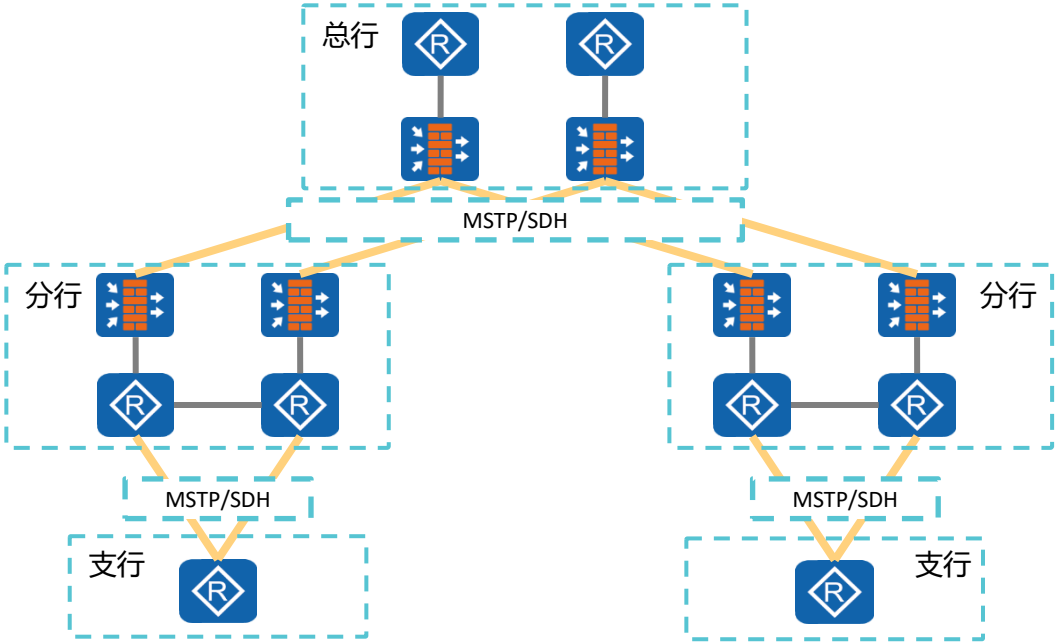
SDH/MSTP/WDM专线介绍

- 对于需要长距离传输且对网络可靠性和安全性有需求的企业，可以租用SDH/MSTP/WDM专线。
- 此类专线属于传输类专线，租户独占传输专线的一部分带宽，由于是多个用户共享线路，所以价格比裸纤便宜。虽然传输类专线共享线路，但是由于带宽独占，且使用的是硬管道。所以能够提供非常高的可靠性和安全性。
- 现网中使用比较多的是MSTP与WDM专线，少量区域还在使用SDH专线。



SDH/MSTP/WDM专线应用场景

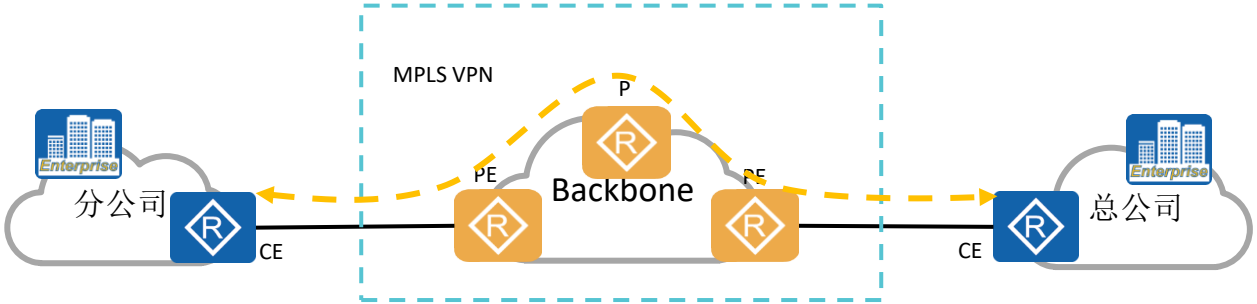
SDH/MSTP/WDM专线应用场景



- 金融分支站点互联时，为了保障网络的高可靠和高安全，一般会选用MSTP或SDH专线。

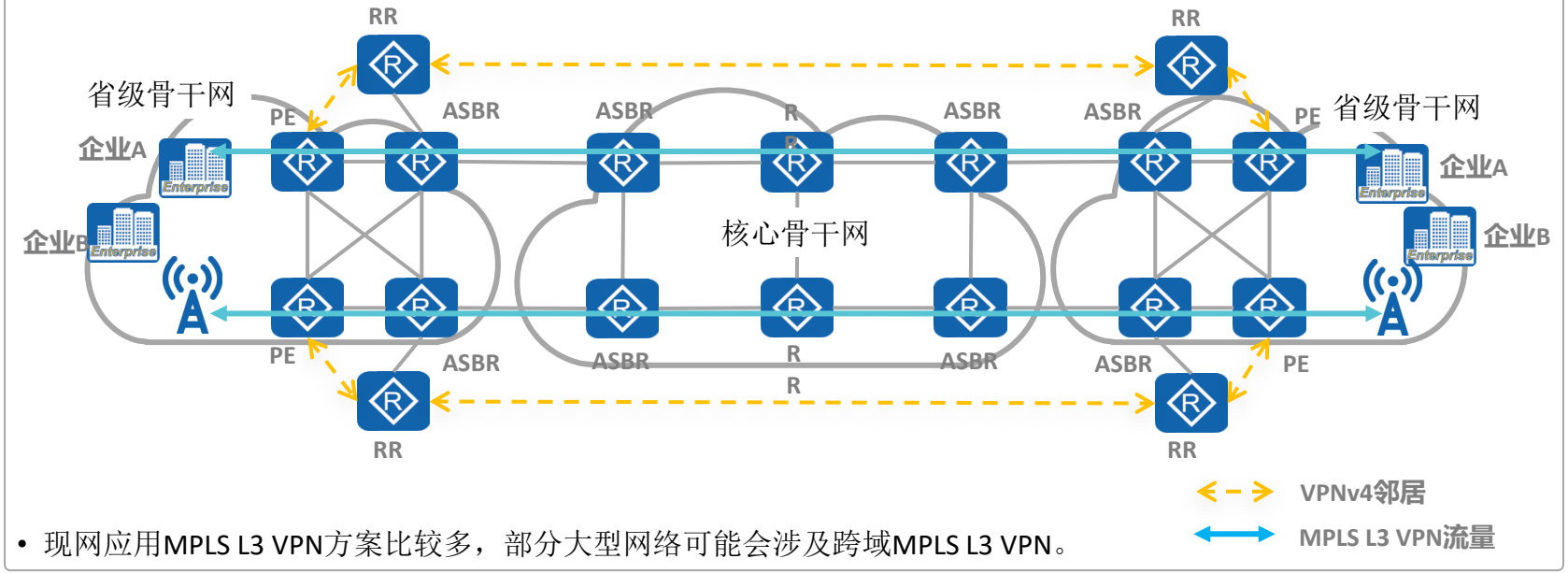
MPLS VPN专线

- MPLS VPN技术被广泛的用于企业互联场景，根据企业需求可以部署MPLS L2 VPN或者MPLS L3 VPN，MPLS VPN作为价格和性能均衡的方案，是一种很受欢迎的专线业务。
- 对于能够自建广域网的企业，比如：铁路，电力等，MPLS VPN是一种易管理，低成本的VPN技术，对于无法自建广域网的企业，MPLS VPN价格稍显昂贵。
- 对于一些有安全需求的企业可以使用MPLS VPN作为主链路，使用GRE Over IPsec作为备用链路。



MPLS VPN专线应用场景

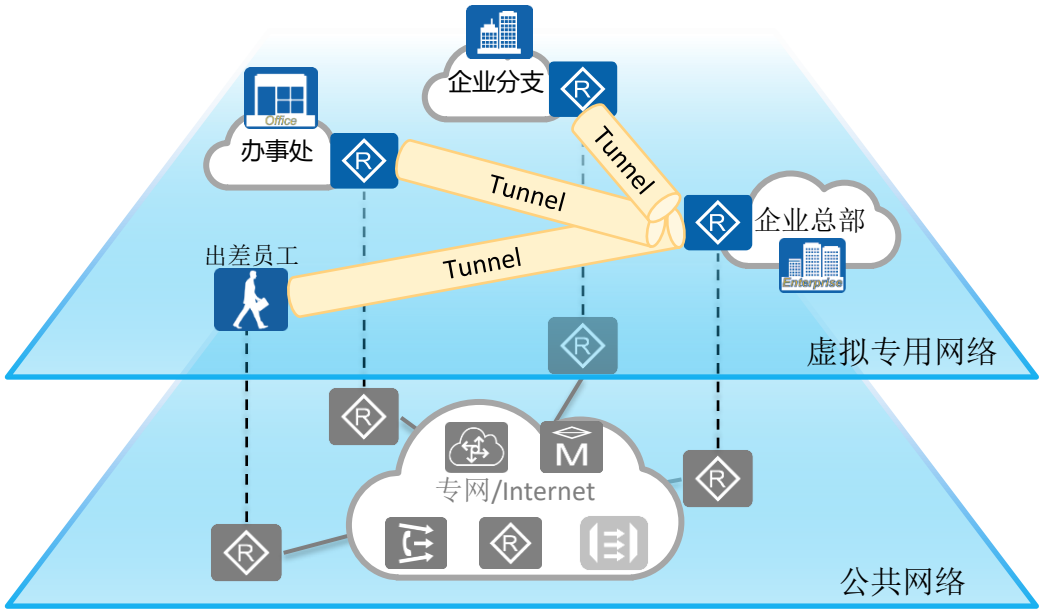
MPLS VPN专线应用场景



- 现网应用MPLS L3 VPN方案比较多，部分大型网络可能会涉及跨域MPLS L3 VPN。

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。

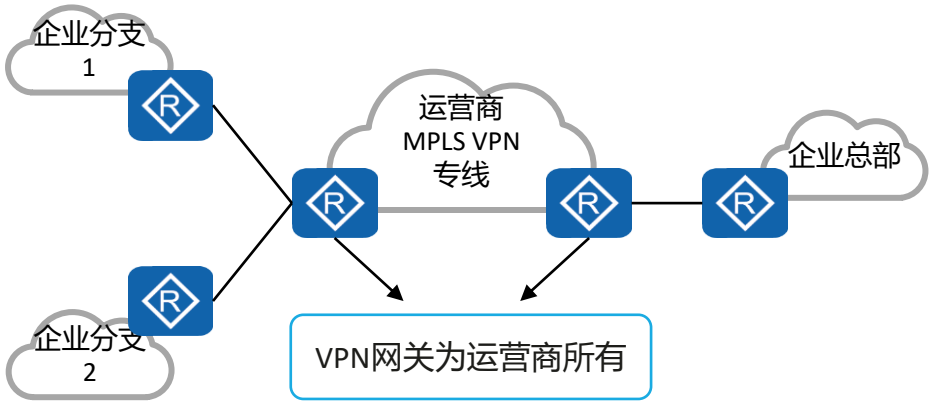
虚拟（Virtual）

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分类 - 根据建设单位不同

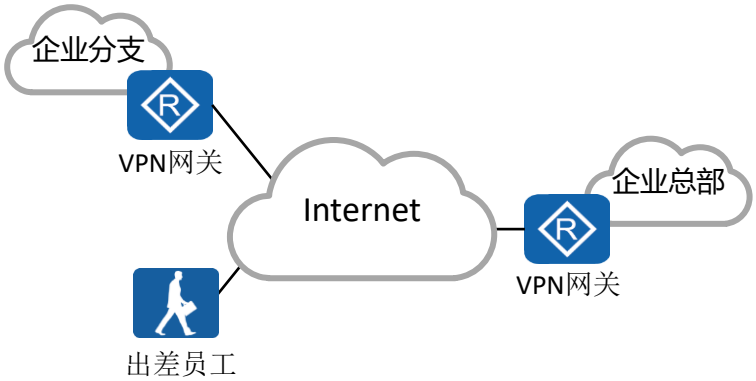
租用运营商VPN专线搭建企业VPN网络

最常见的场景为租用运营商MPLS VPN专线。



自建企业VPN网络

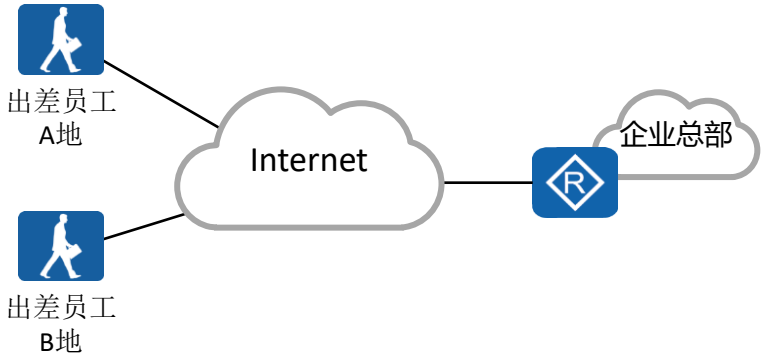
基于Internet建立企业VPN网络，常见的如IPSec VPN、L2TP VPN、SSL VPN等。



VPN分类 – 根据组网方式不同

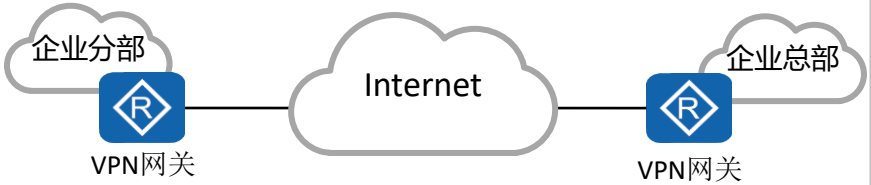
远程访问VPN（Remote Access VPN）

适用于出差员工VPN拨号接入的场景，员工可在任何能接入Internet的地方，通过VPN接入企业内网资源。常见的有L2TP VPN、SSL VPN等。

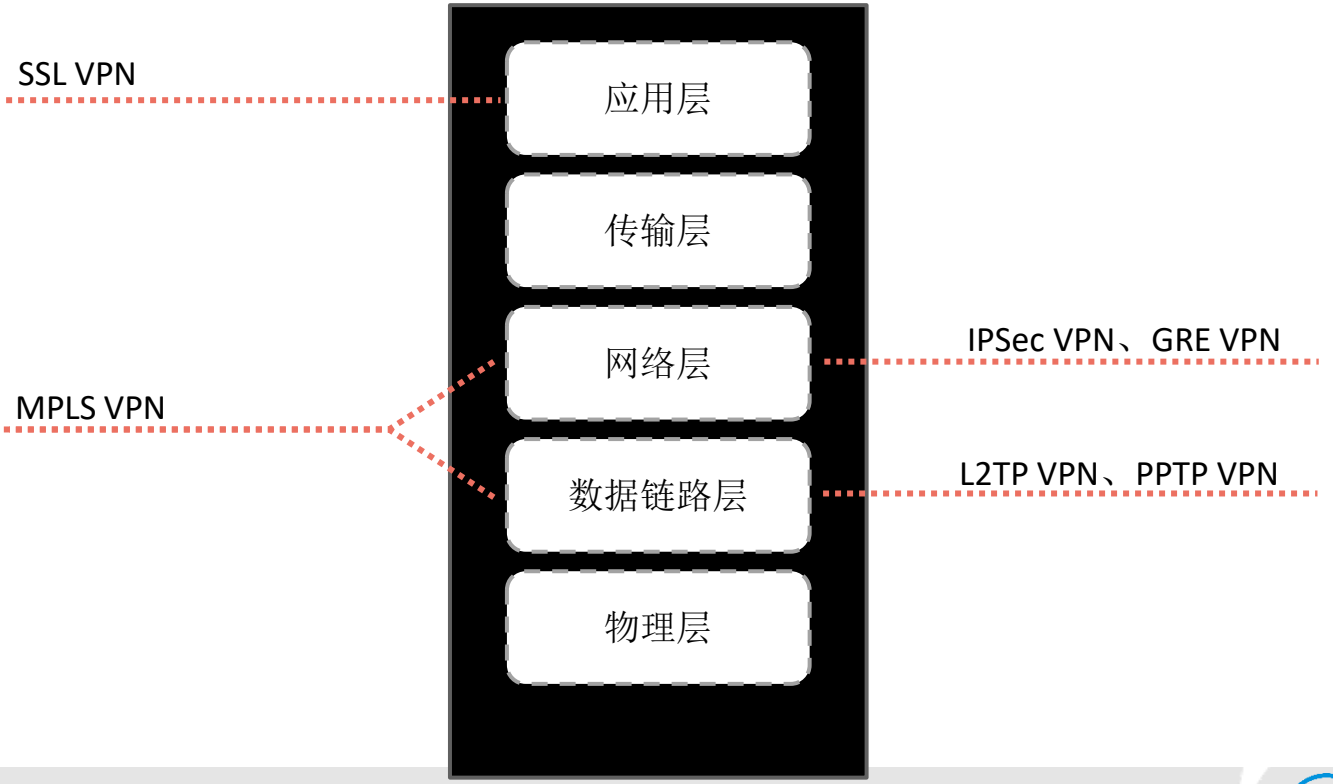


局域网到局域网的VPN（Site-to-site VPN）

适用于公司两个异地机构的局域网互连。常见的有MPLS VPN、IPSec VPN等。



VPN分类 – 根据实现的网络层次

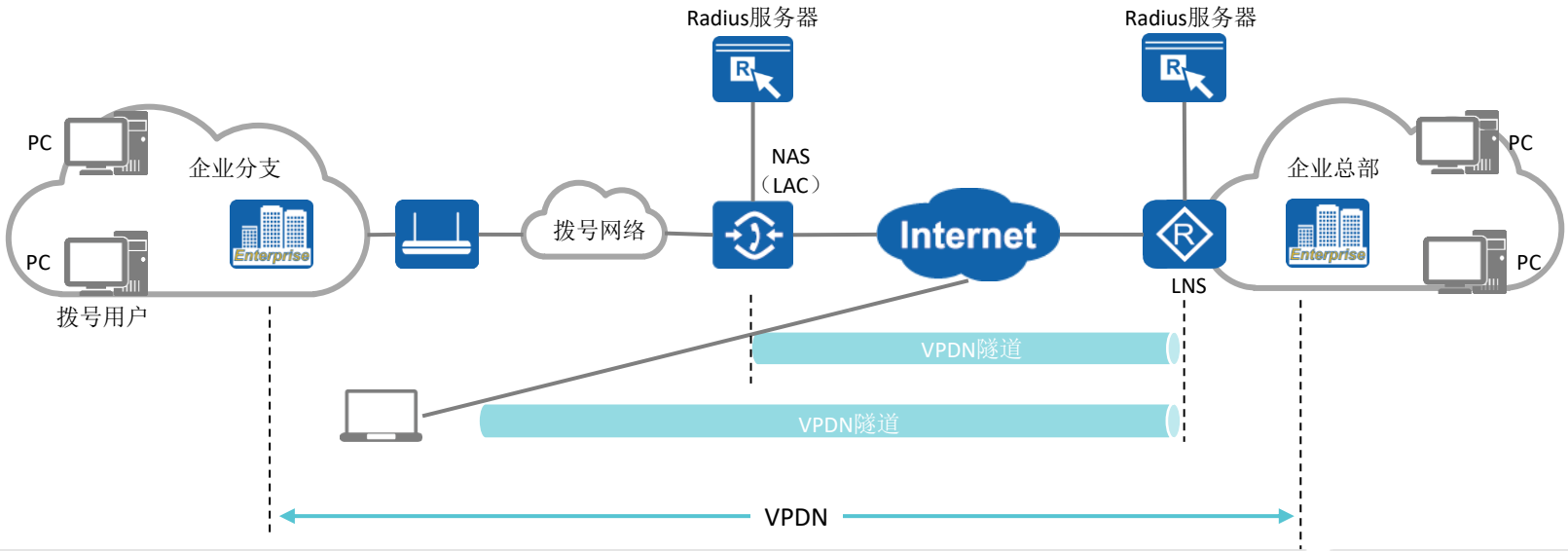


VPN分类 - 根据业务用途

- VPN技术按业务用途划分可分成以下三类：
  - Access VPN（远程访问虚拟专网）：又称拨号VPN，远程访问VPN，即VPDN，通常用L2TP VPN技术。
  - Intranet VPN（企业内部虚拟专网）：网关到网关，通过公司的网络架构连接来自同公司的资源，通常用GRE或者DSVPN技术。
  - Extranet VPN（扩展的企业内部虚拟专网）：与合作伙伴企业网构成Extranet，通常用SSL VPN技术。

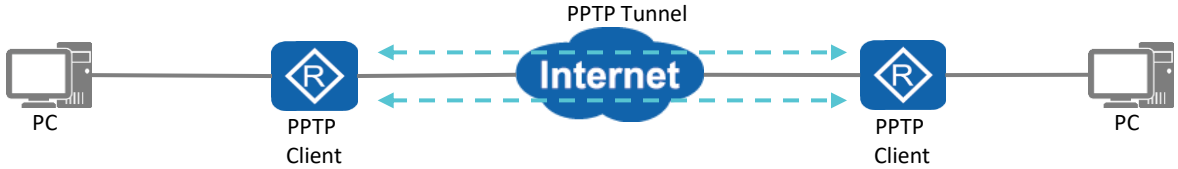
Access VPN介绍

- Access VPN主要使用VPDN技术，VPDN英文为Virtual Private Dial-up Networks，又称为虚拟专用拨号网，是VPN业务的一种，主要基于拨号用户的虚拟专用拨号网业务。可以用于企业互联或者远程访问企业网络。



PPTP简介

- PPTP协议是第一种VPN协议，它已有20多年的历史。该协议依赖于加密，认证和端对端协议（PPP）进行协商。实质上，它只需要用户名，密码和服务器地址就可创建连接。
- PPTP速度很快，但是速度是以弱加密性为代价的。在所有VPN协议中，PPTP加密级别最低，且PPTP必须基于IP网络。

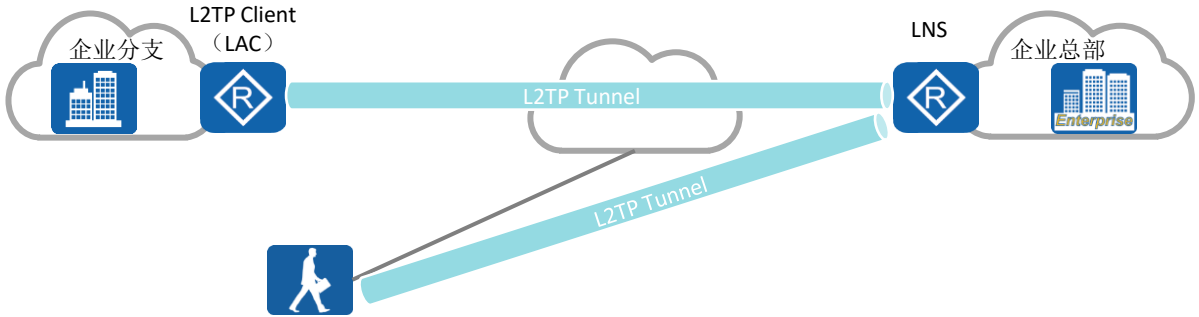


L2F简介

- PPTP发布不久以后，Cisco开发了L2F，试图改进PPTP的缺陷。
- L2F将链路层的协议（如HDLC，PPP，ASYNC等）封装起来传送。因此，网络的链路层完全独立于用户的链路层协议。
- L2F协议是一种安全通信隧道协议，但它的主要缺陷是没有把标准加密方法包括在内，因此它也已经成为一个过时的隧道协议。

L2TP简介

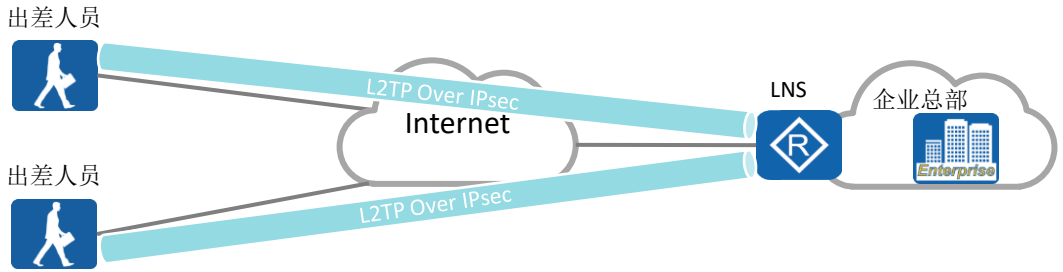
- IETF的开放标准L2TP协议结合了PPTP协议和L2F的优点，特别适合组建远程接入方式的VPN，已经成为事实上的工业标准。
- L2TP只是一种隧道协议，不提供加密，因此一般与IPsec配合使用。
- L2TP被作为常用的企业互联技术之一。在使用L2TP时需要配合AAA服务器，当需要构建L2 VPN时，L2TP是非常好的选择。



Access VPN现网应用

- Access VPN 现网中多用于内网用户远程接入，使用最多的是L2TP over IPsec。
- PPTP由于需要windows系统支持，且外网接入需要将内网的windows服务器通过NAT映射出去，部署不便，使用很少。

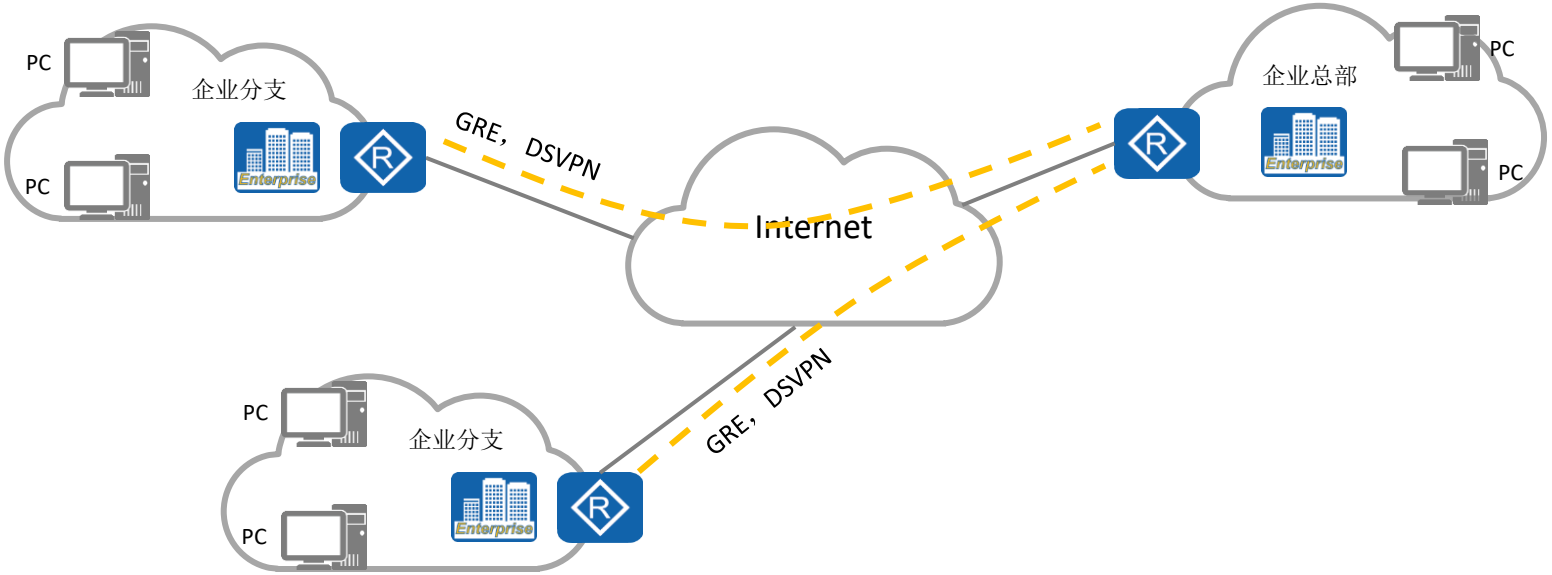
L2TP Over IPsec现网应用



- 分支站点之间也可以使用L2TP链接，但L2TP没有办法传递组播数据，无法在总公司和分公司之间传递路由，所以现网L2TP更多用于远程用户接入。

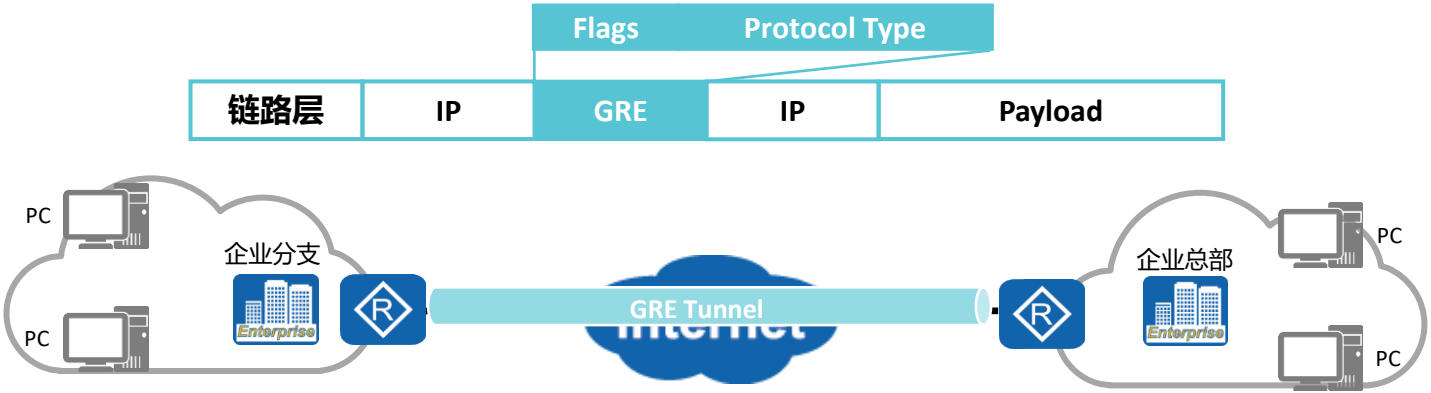
Intranet VPN介绍

- Intranet VPN技术指的是，基于Internet在公司网关之间构建VPN网络，主要用到的技术有GRE，DSVPN等。
- 企业自建分支-总部VPN，主要使用GRE和DSVPN技术。



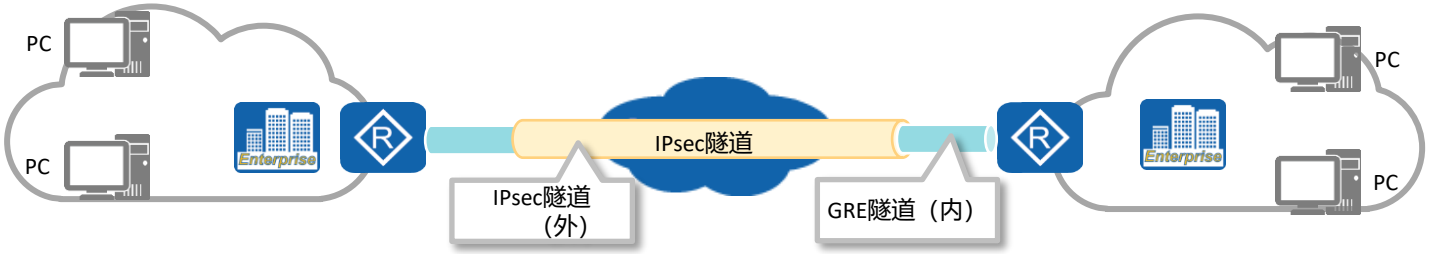
GRE协议简介

- GRE （Generic Routing Encapsulation）：对某些网络层协议（如：IP， IPX， AppleTalk等）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层协议（如IP）中传输。
- GRE一般使用在分支站点比较少的网络中。



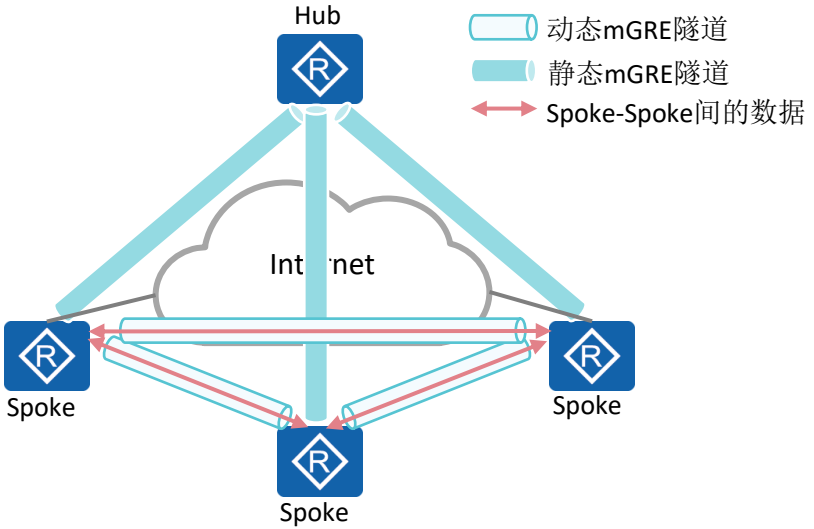
GRE Over IPsec简介

- GRE的主要缺点是不支持加密。IPsec的主要缺点是只支持IP协议，且不支持组播。
- 将GRE封装入IPsec可以结合GRE和IPsec的优点，避免缺点。
- GRE Over IPsec是一种企业常用的点到点VPN技术



DSVPN简介

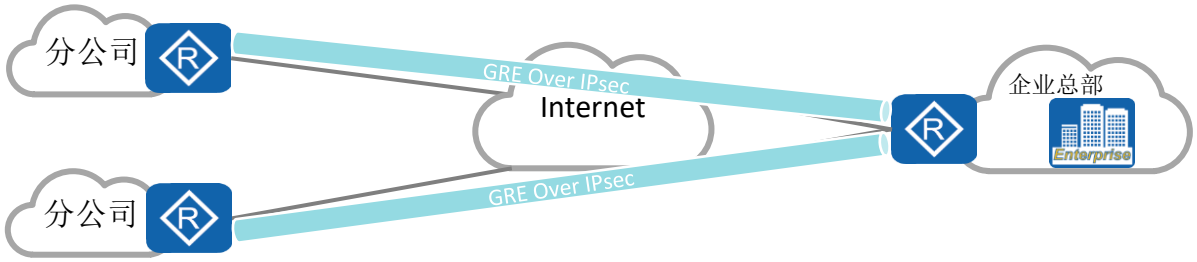
- DSVPN主要解决GRE Over IPsec存在的一些缺陷，使得有大量分支机构的公司也能方便的搭建VPN网络。
- DSVPN是一种动态建立GRE隧道的技术，通过NHRP协议动态收集、维护和发布各节点的公网地址等信息，解决了源分支无法获取目的分支公网地址的问题。
- DSVPN借助mGRE技术，使VPN隧道能够传输组播报文和广播报文，并且一个Tunnel接口可与多个对端建立VPN隧道。
- DSVPN建立的GRE隧道依然可以使用IPsec技术保证隧道的安全性。



Intranet VPN现网应用

- Intranet VPN现网中主要用于企业分支与总部，分支与分支之间互联。
- 现网中使用比较多的是GRE Over IPsec，对于有较多分支的企业，可以使用Efficient VPN简化分支的配置，部署IPsec链路冗余备份后可以保障GRE的可靠性。

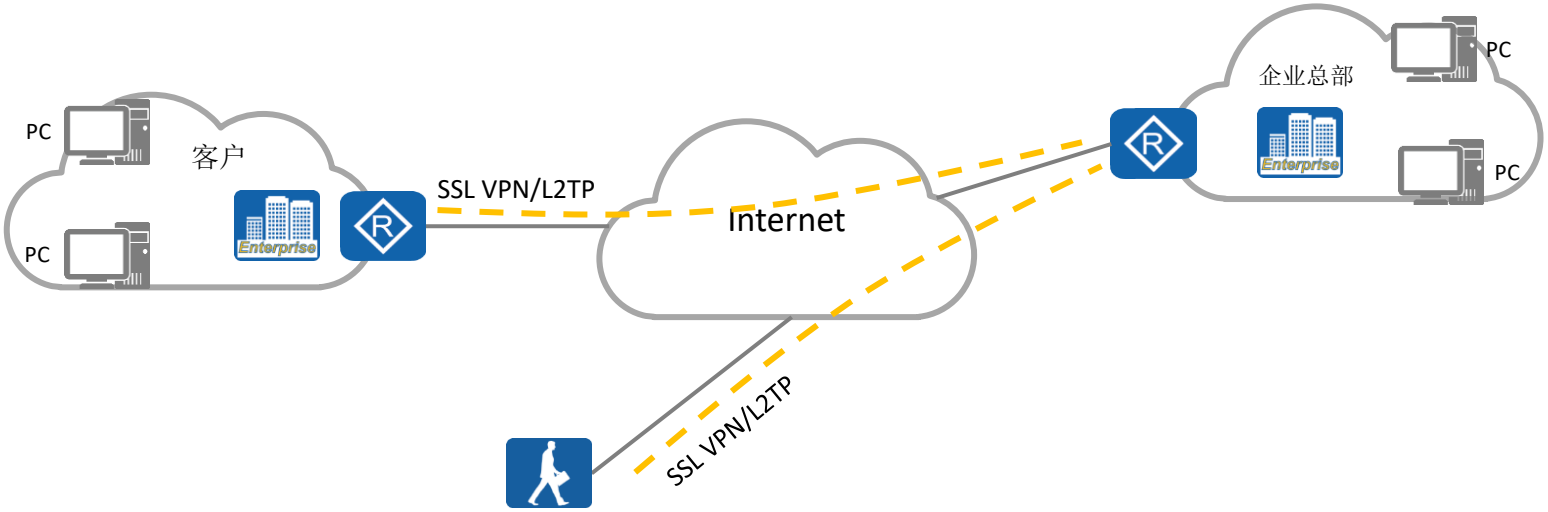
GRE Over IPsec现网应用



- DSVPN在现网使用较少，主要原因：1. 很多企业希望分支之间流量能经过总部，便于管理；2. 企业运维人员对于DSVPN的了解一般，运维较不便。

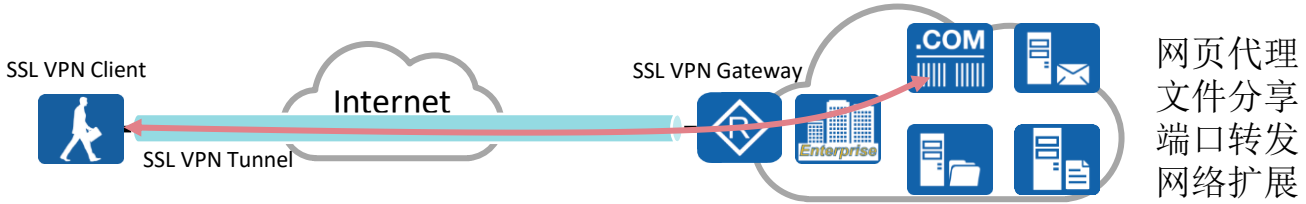
Extranet VPN介绍

- Extranet VPN主要用于在客户或者供应商之间构建安全的访问服务，同时对于出差员工也可以使用Extranet VPN接入公司网络。
- Extranet VPN主要用到的技术是SSL VPN与L2TP。



SSL VPN简介

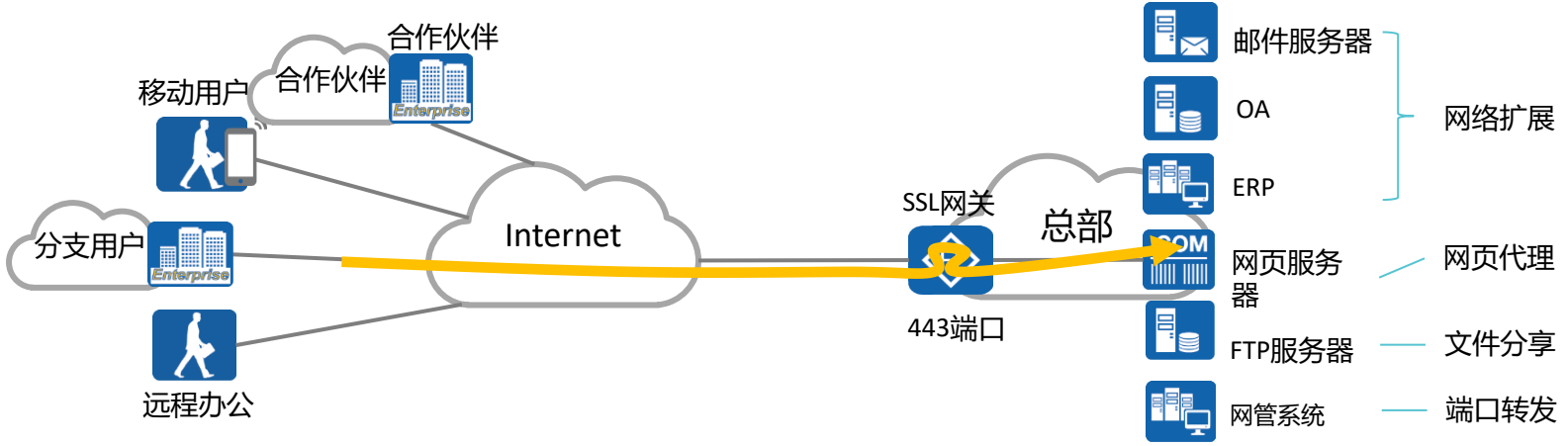
- SSL VPN主要用于出差人员远程接入公司内网，一般被认为是公司内网在广域网上的扩展。
- SSL VPN基于HTTP进行用户认证和控制，用户无需配置，使用简单。



Extranet VPN应用场景

- 外部用户接入内网，使用SSL VPN比较方便，无需安装客户端，直接使用网页认证后即可访问公司内网，且SSL VPN的业务选择较多，比如网页代理，文件分享，端口转发，网络扩展。

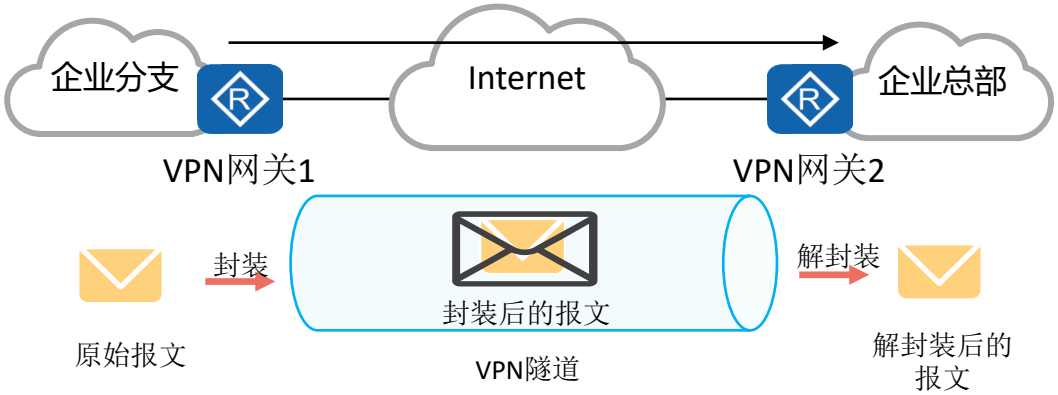
SSL VPN应用场景



- SSL VPN使用方便，只需要使用浏览器即可访问公司内网，但不是所有路由器都支持SSL VPN，对于不支持SSL VPN的路由器，可使用L2TP建立外网对内网的链接。

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。



VPN关键技术 - 身份认证、数据加密与验证

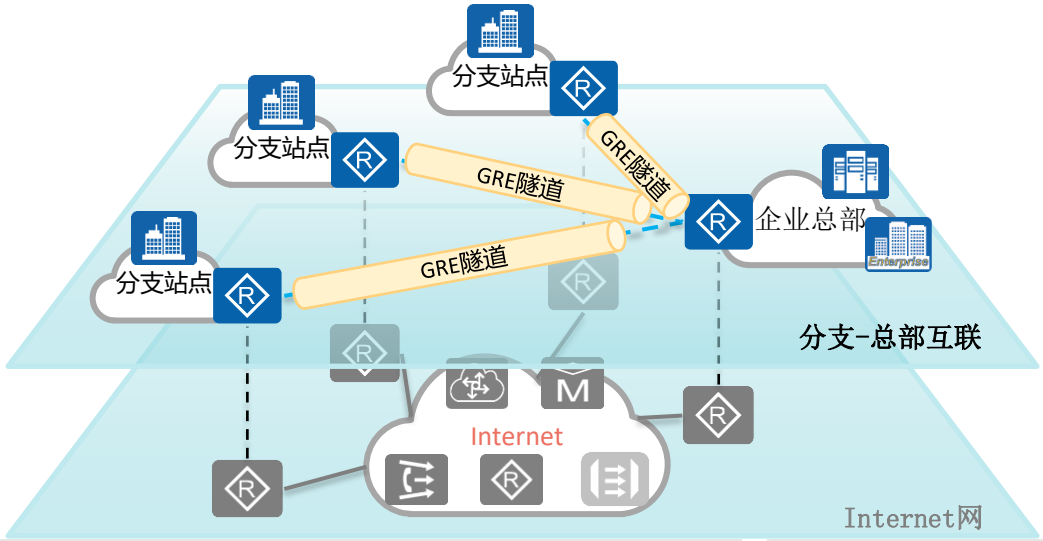
身份认证、数据加密和认证技术可以有效保证VPN网络与数据的安全性：

- 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。

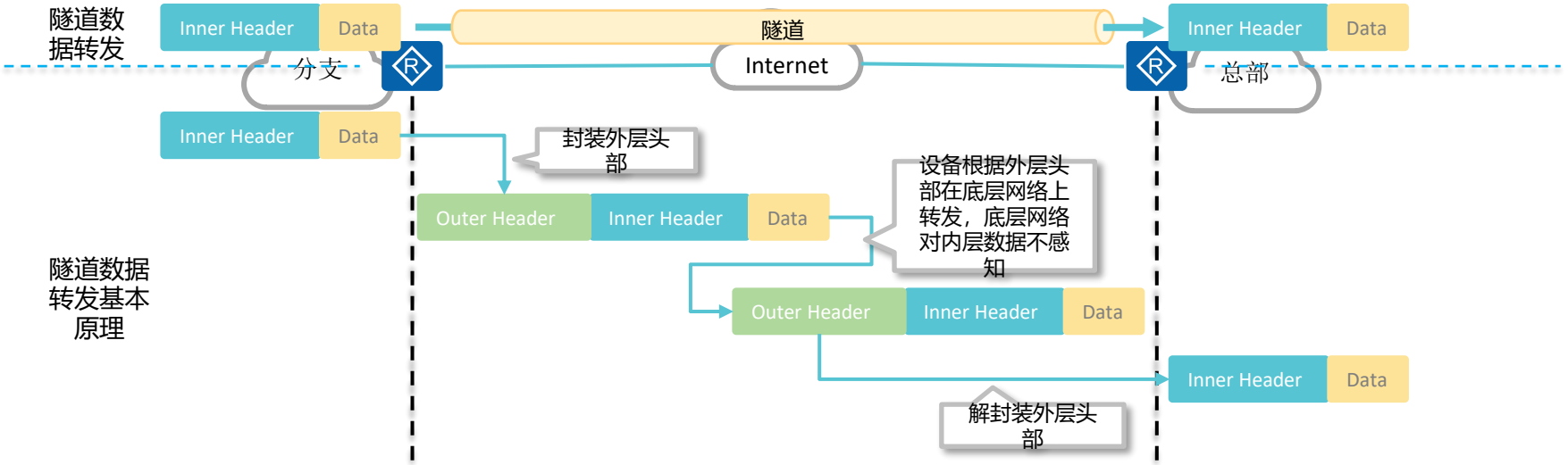
GRE产生背景

- 随着企业的发展，越来越多的企业需要在分支-总部之间进行内网通信。传统分支-总部之间内网通信需要租用专线（比如MPLS，传输专线等）。但是专线价格昂贵，对于中小型企业，或者跨国公司来说，成本较高。
- 由于Internet的发展，Internet网有了足够的带宽和覆盖，通过Internet建立分支-总部内网通信的可行性越来越高，GRE（Generic Routing Encapsulation，通用路由封装协议）就是在这种背景下被提出的。
- 通过GRE隧道，分支和总部之间可以基于Internet建立企业网络。



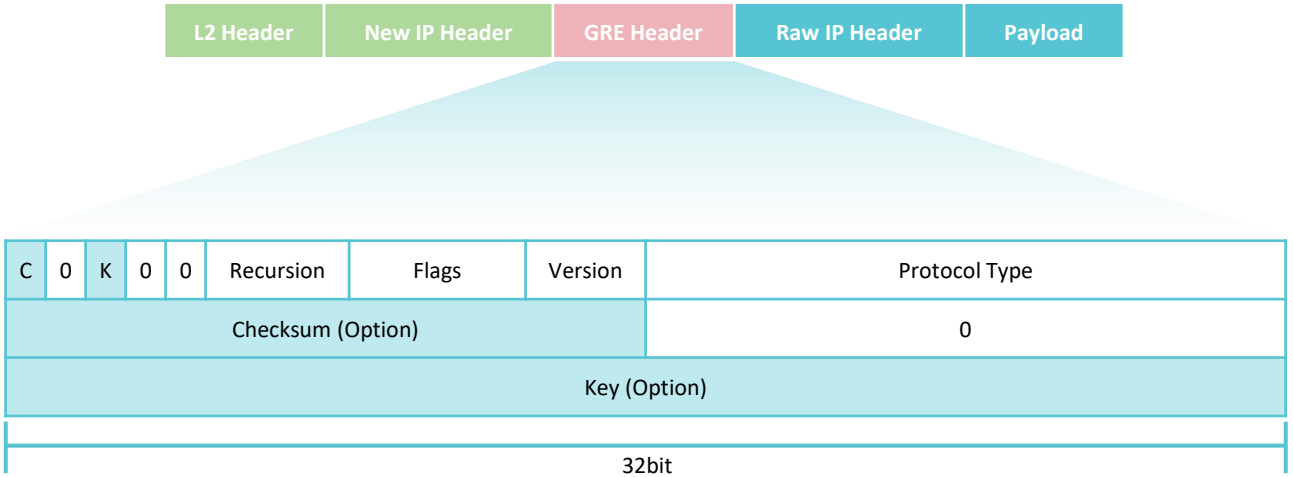
隧道技术简介

- GRE技术本质上是一种隧道技术。隧道技术类似于一座桥，可以在底层网络（比如：Internet）之上构建转发通道，用户可以自行构建隧道网络，不需要底层网络的管理者（比如：ISP）介入。
- 隧道技术的方案很多，常见的隧道技术有：MPLS，GRE，L2TP，VxLAN等，隧道基本原理如下：



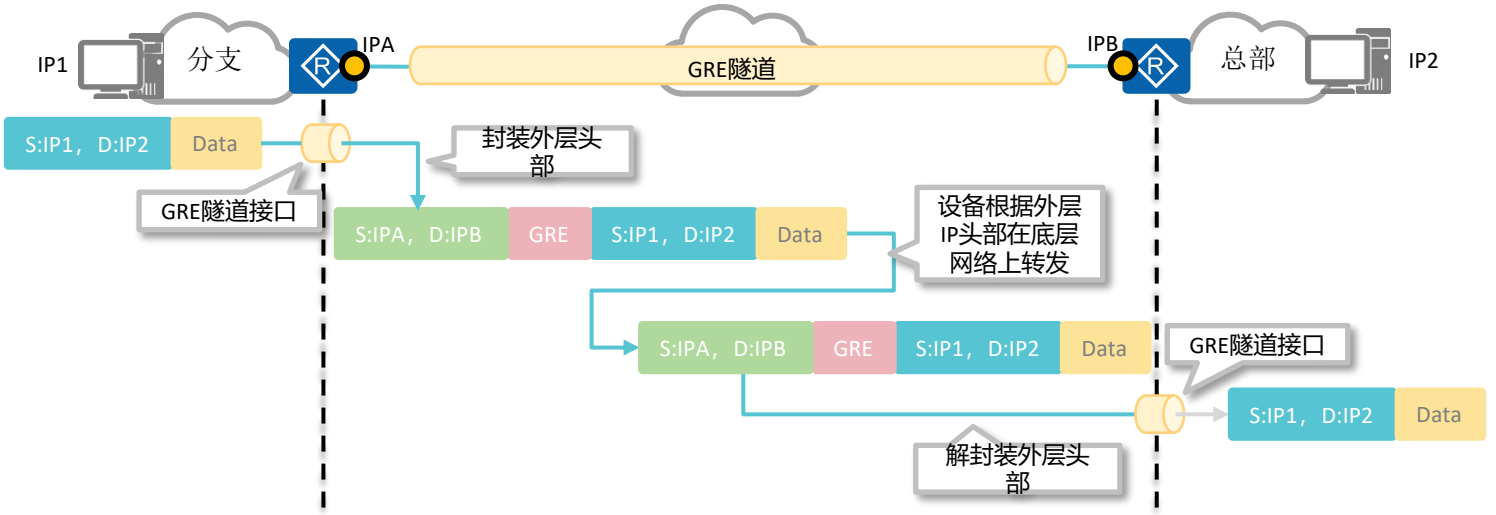
GRE基本概念

- GRE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，是一种三层隧道封装技术，使报文可以通过GRE隧道透明的传输，解决了企业分支与总部互联的问题。
- GRE隧道能够承载IPv4/IPv6的单播、组播、广播报文。
- GRE报文的格式如下：



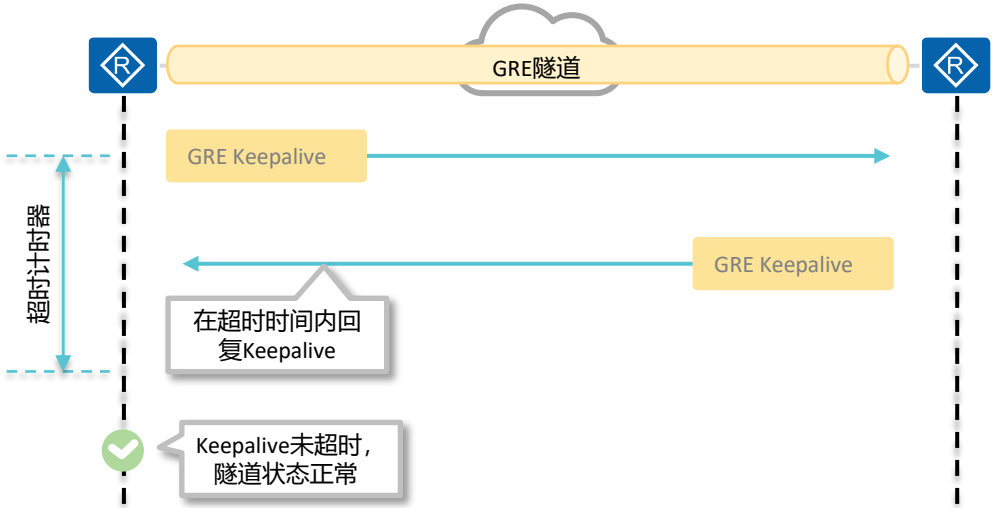
GRE基本工作原理

- GRE隧道是三层隧道，主要承载IPv4/IPv6报文。GRE通过封装外层IP头部，使得数据可在公网上传递，达到企业分支-总部之间的内网互通的目的。
- GRE隧道数据转发过程如下：



GRE Keepalive检测

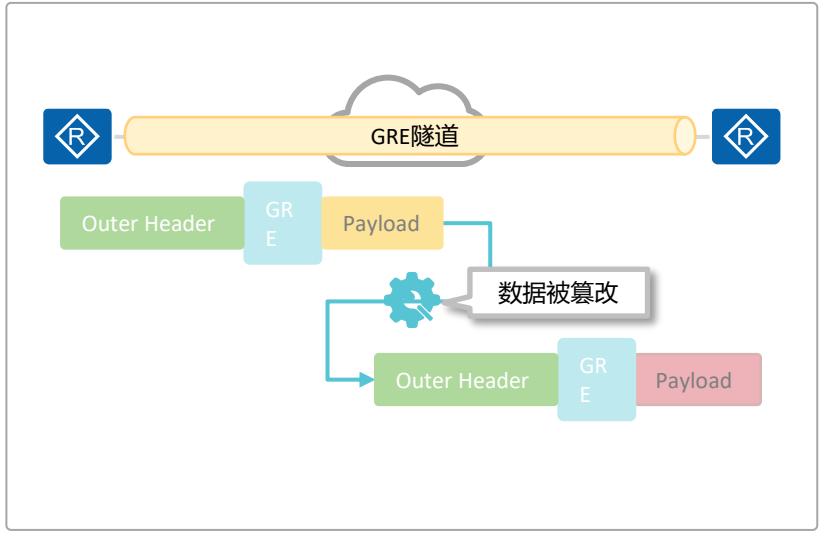
- 由于GRE协议并不具备检测链路状态的功能，如果对端接口不可达，隧道并不能及时关闭该Tunnel连接，这样会造成源端会不断的向对端转发数据，而对端却因隧道不通接收不到报文，由此就会形成流量中断。
- GRE的Keepalive检测功能可以检测隧道状态，即检测隧道对端是否可达。
- Keepalive超时时间=发送周期（默认5 s）*重试次数（默认3次）



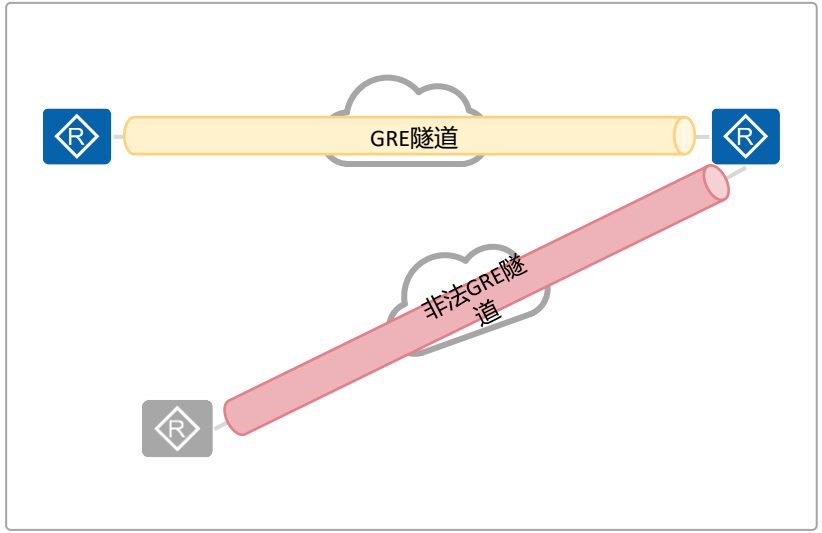
GRE隧道安全威胁

- GRE隧道的主要作用是将数据在分支-总部之间传递，数据并不加密，有被篡改的风险。
- GRE隧道建立也有一定风险，通过伪造IP地址，可以使得非法设备与合法设备之间建立GRE隧道

GRE数据篡改

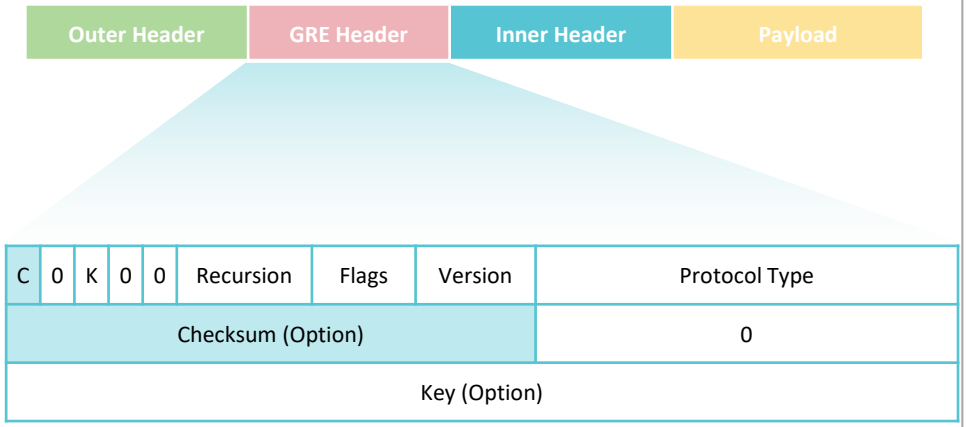


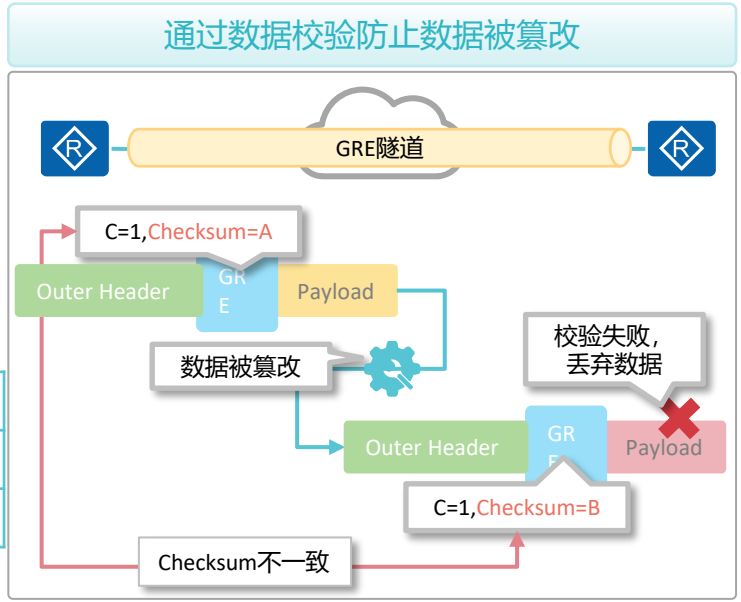
建立非法GRE隧道



GRE数据校验和验证

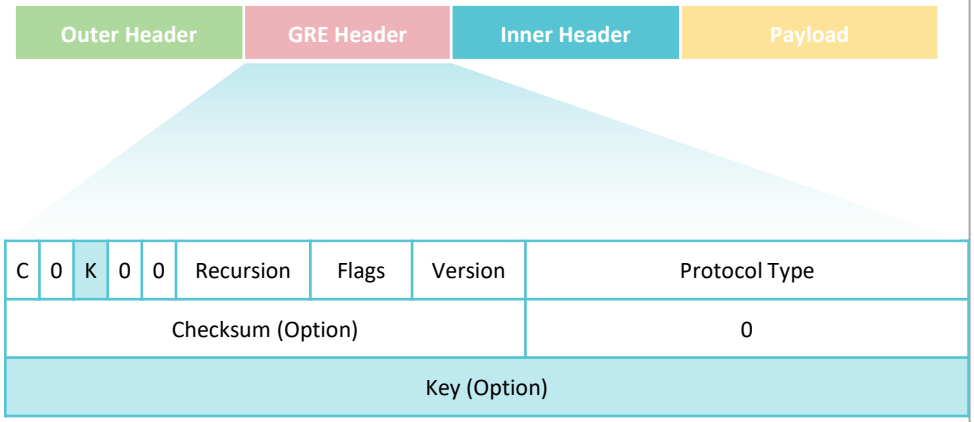
- 校验和验证是指对封装的报文进行端到端校验。
- 若GRE报文头中的C位标识位置1，则校验和有效。发送方将根据GRE头及Payload信息计算校验和，并将包含校验和的报文发送给对端。接收方对接收到的报文计算校验和，并与报文中的校验和比较，如果一致则对报文进一步处理，否则丢弃。

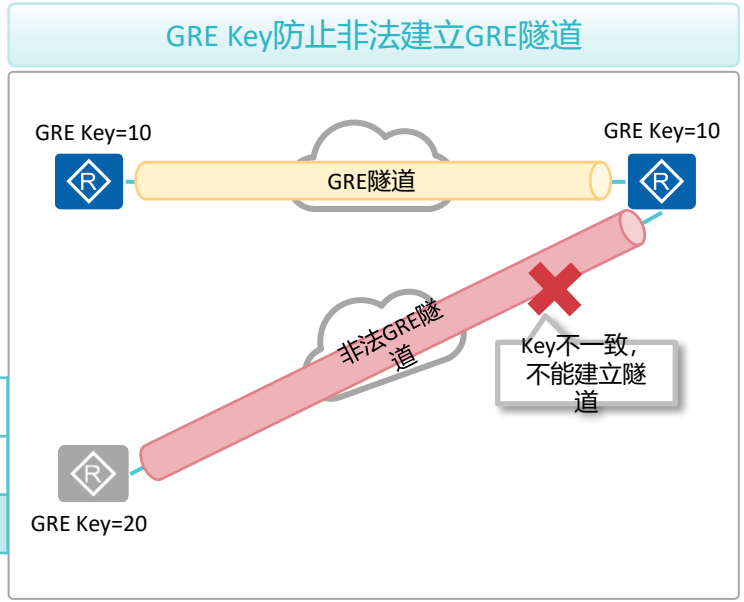




GRE识别关键字

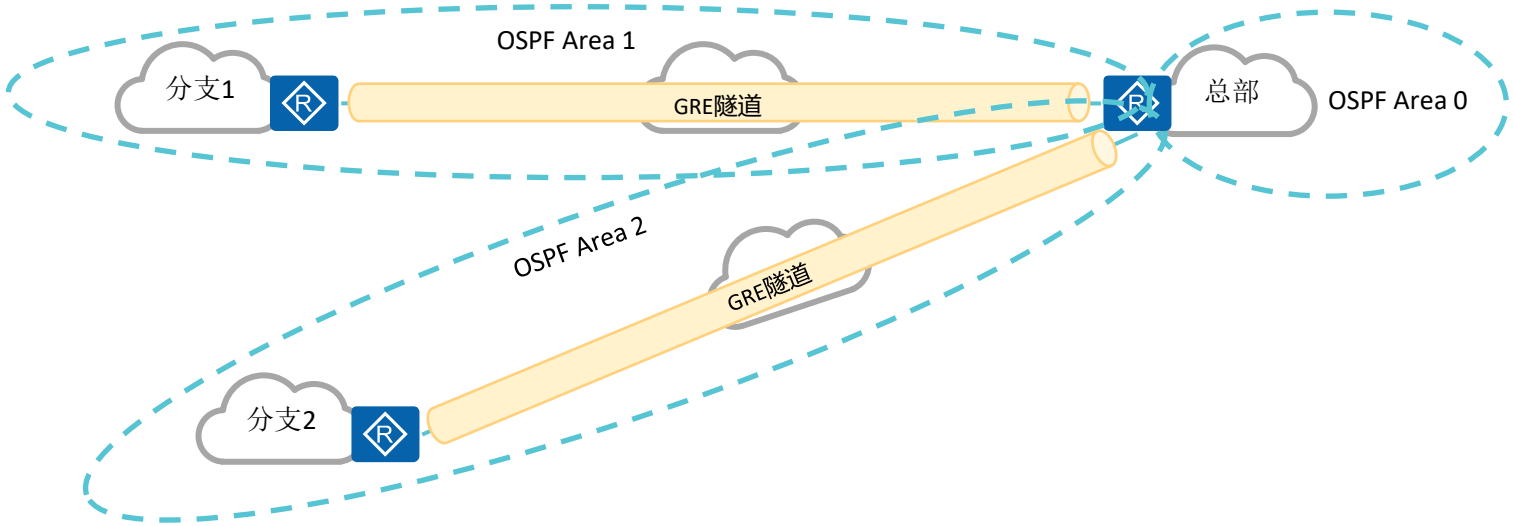
- 识别关键字（Key）验证是指对Tunnel接口进行校验。通过这种弱安全机制，可以防止错误识别、接收其它地方来的报文。
- 若GRE报文头中的K位为1，则在GRE头中插入一个四字节长关键字字段，收发双方将进行识别关键字的验证。





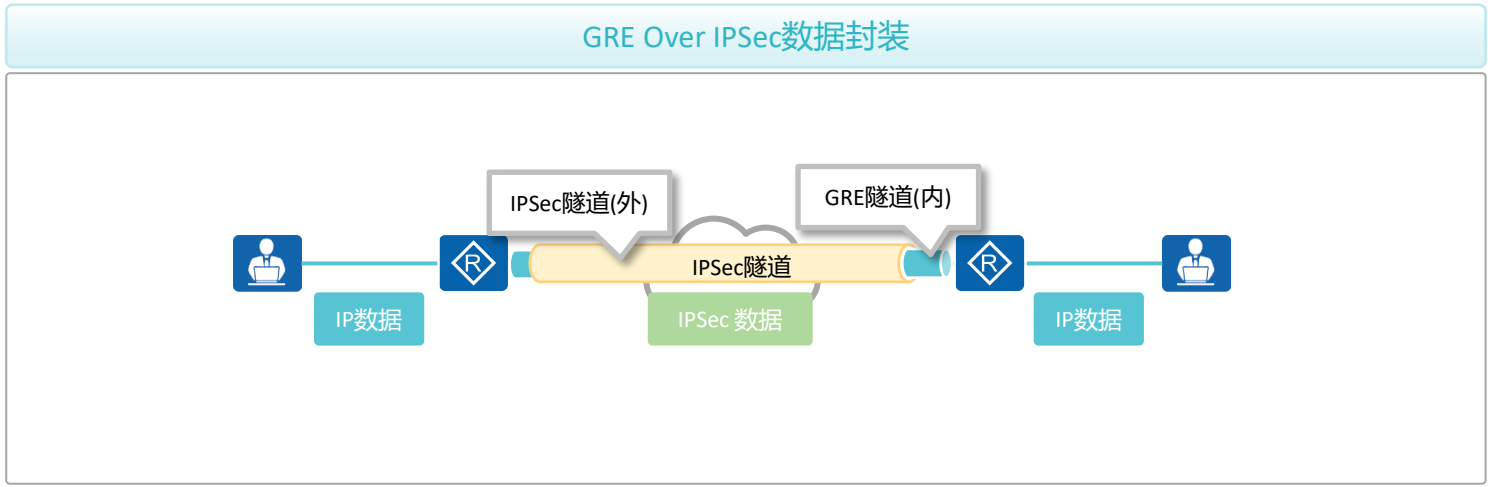
GRE构建分支-总部内网

- GRE隧道能承载IPv4/IPv6单播、组播、广播报文，分支-总部之间可以通过GRE隧道建立内网之间的动态路由协议邻居，使得分支-总部之间内网互联更加方便。



GRE Over IPsec

- GRE技术简单，但是使用GRE隧道传递的数据以明文方式传递的，数据容易被窃取。现网中一般与IPsec技术结合使用。GRE技术构建分支-总部之间的内部网络互联，IPSec技术加密GRE隧道报文。



GRE基本配置

- 背景介绍：
  - 某中小企业有总部（Hub）和一个分支（Spoke1），分布在不同地域，现在用户希望能够实现分支-总部之间的内网互联。
- 配置思路：
  - 保证Spoke和Hub的公网接口能够互通
  - 在Spoke和Hub上配置GRE隧道

Spoke与Hub上创建GRE隧道

- 在Spoke和Hub上的配置类似，配置命令如下：

- GRE隧道需要在隧道两端设备分别配置
- GRE配置思路如下：
  - 保证Spoke和Hub的公网接口能够互通
  - 在Spoke和Hub上创建GRE隧道
  - 配置GRE隧道源末地址

System-view

interface tunnel <interface-num>　//创建隧道接口

ip address <ip-address>　//设置隧道接口的IP地址，该地址的主要作用是用于企业内网互通时作为路由下一跳使用

tunnel-protocol gre　//将隧道类型设置为GRE隧道

source <ip-address>　//设置隧道源地址，对应GRE封装外层IP头部的源IP地址

destination <ip-address>　//设置隧道目标地址，对应GRE封装外层IP头部的目标IP地址

gre key <key-num>　//可选命令，设置GRE Key，用于验证GRE隧道是否能建立

流量引入GRE隧道

- 将流量引入GRE隧道的方法很多，可以使用OSPF，静态路由，BGP等。

查看GRE配置结果

- 当配置完成后可使用以下命令在设备上查看配置结果：

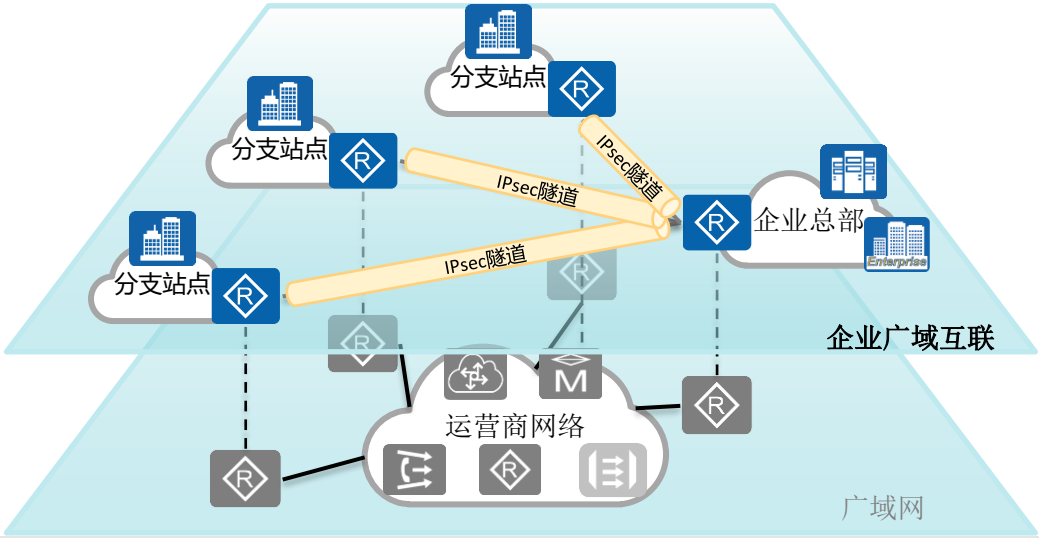
System-view

display interface tunnel [interface-number]　//查看Tunnel接口的工作状态。

display tunnel-info tunnel-id [tunnel-id]　//查看隧道信息。

IPsec产生背景

- 企业分支之间经常有互联的需求，企业互联的方式很多，可以使用专线线路或者Internet线路。
- 部分企业从成本和需求出发会选择使用Internet线路进行互联，但是使用Internet线路存在安全风险，如何保障数据在传输时不会被窃取？
- IPsec技术通过将数据报文加密传输，达到保障企业互联安全性的目的。



IPsec简介

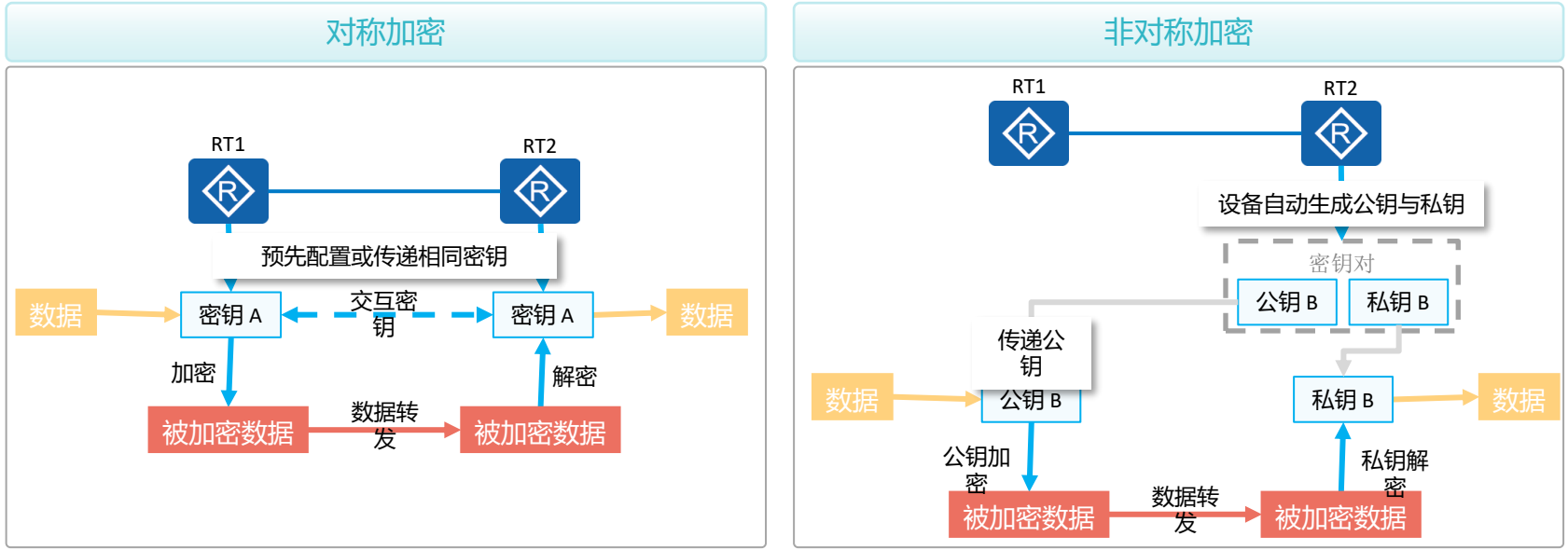
- IPsec（IP Security）协议族是IETF制定的一系列安全协议，它为端到端IP报文交互提供了基于密码学的、可互操作的、高质量的安全保护机制。
- 通过对数据加密、认证，IPsec使得数据能够在Internet网络上安全的传输。
- IPsec VPN技术可以和多种VPN技术结合使用，使得企业互联更加灵活安全。

GRE Over IPsec应用

- 现网中分支站点互联多使用GRE Over IPsec技术，IPsec技术保障数据安全传输，GRE技术保障企业内网之间能够互联。

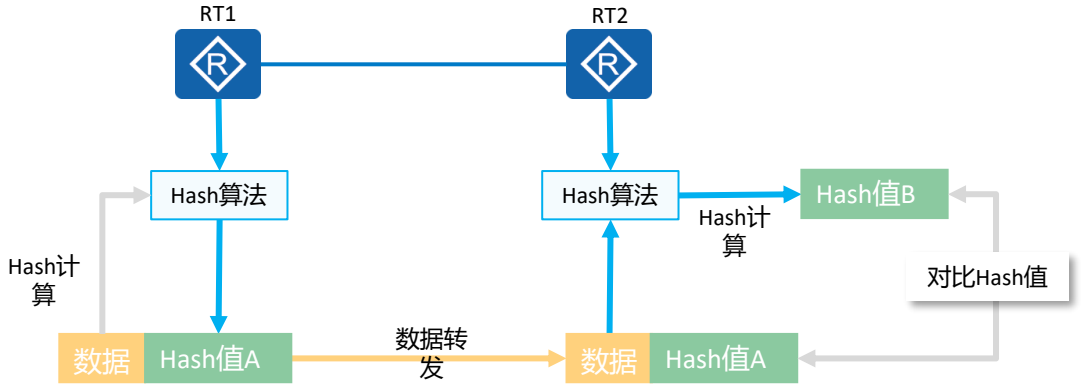
数据加密方式简介

- 数据加密可以避免数据转发时被读取。数据加密一般有两种方案：
  - 对称加密：使用同一个密码加密/解密，效率很高，但是对称加密在互相交互密钥时存在密钥被截取的风险。
  - 非对称加密：使用公钥加密，私钥解密，安全性很高但是加解密效率很低。



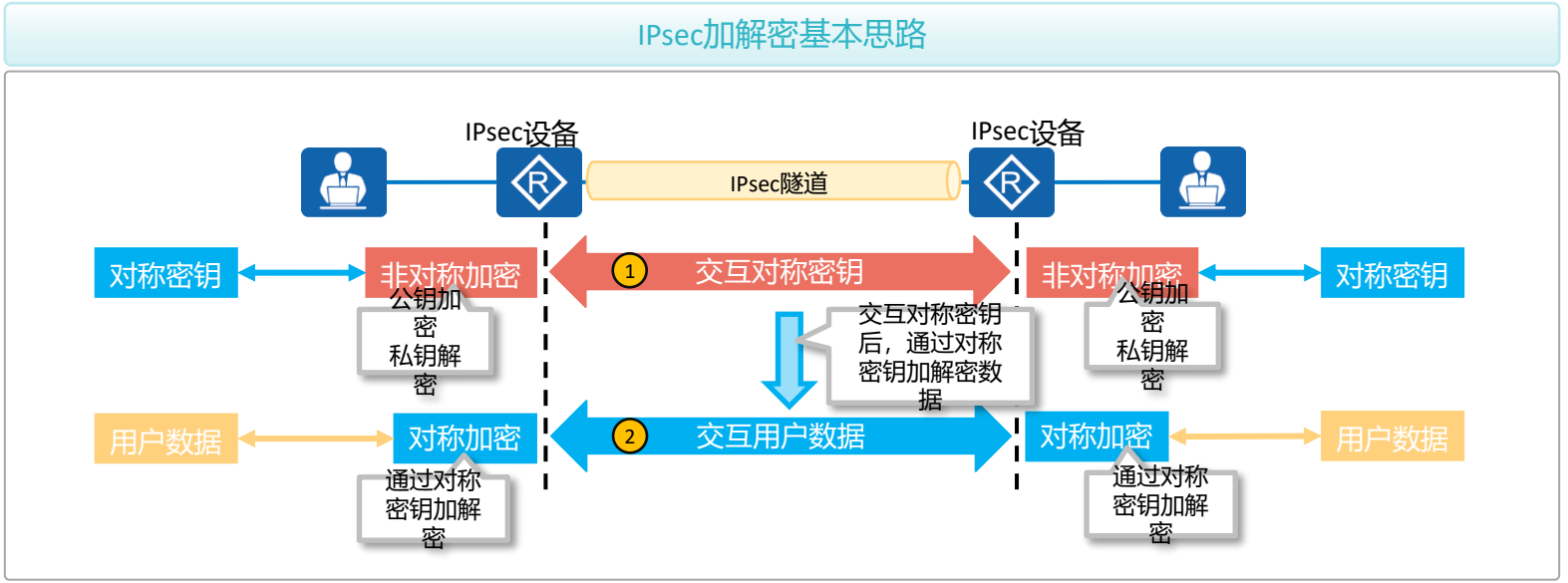
数据认证方式简介

- 数据认证的主要目的是确认数据是否被篡改，数据认证主要基于Hash算法。
  - 数据通过Hash算法计算出一个唯一的Hash值，Hash值携带在数据中转发给对端。
  - 对端设备对数据重新进行Hash，得出Hash值。将收到的Hash值与计算出的Hash值进行比对，一致说明没有被篡改。



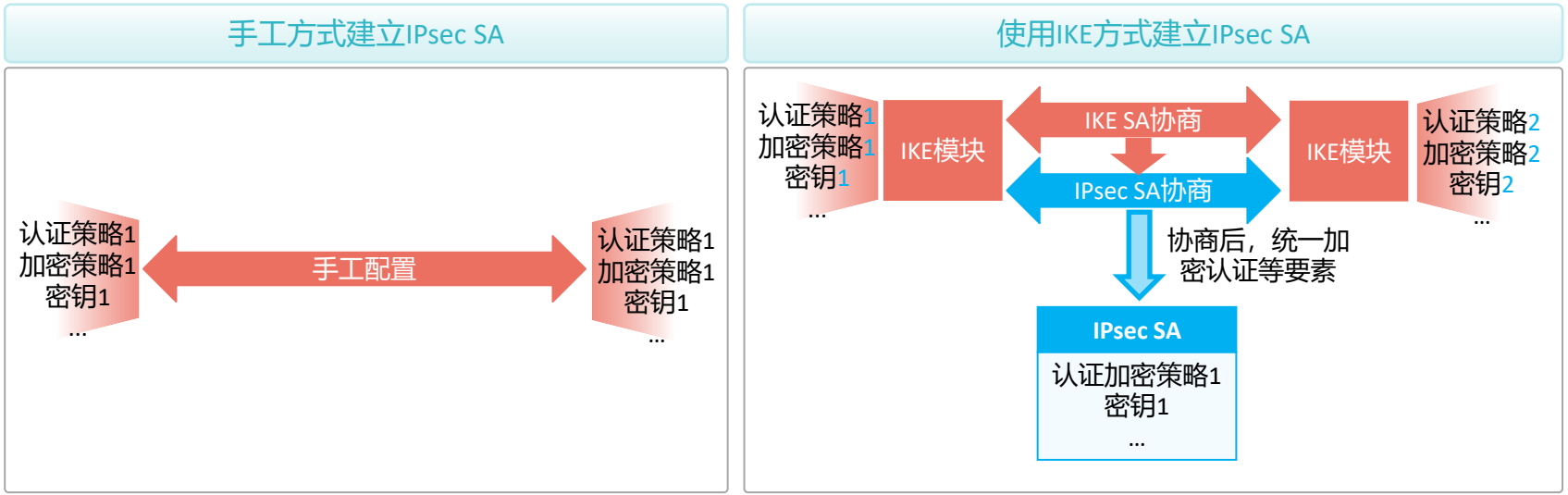
IPsec加密基本思路

- IPsec同时使用对称加密与非对称加密，保证了安全也兼顾了性能。
  - 将对称加密所用的密钥，使用非对称算法加密并传递。
  - 数据通过交互后的对称密钥加密。



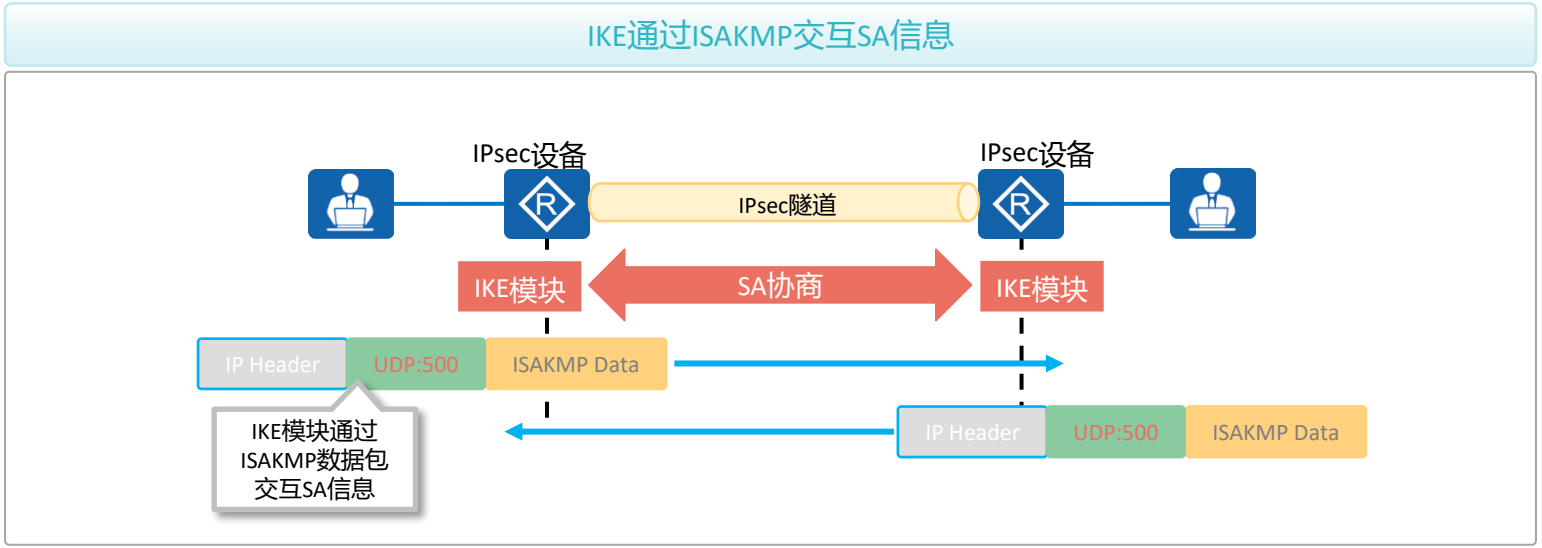
安全联盟介绍

- SA（Security Association，安全联盟）可以帮助IPsec对特定要素进行约定，比如：加密算法使用DES，认证算法使用MD5，封装方式使用Tunnel等。
- 建立IPsec SA一般有两种方式：手工方式和IKE方式。



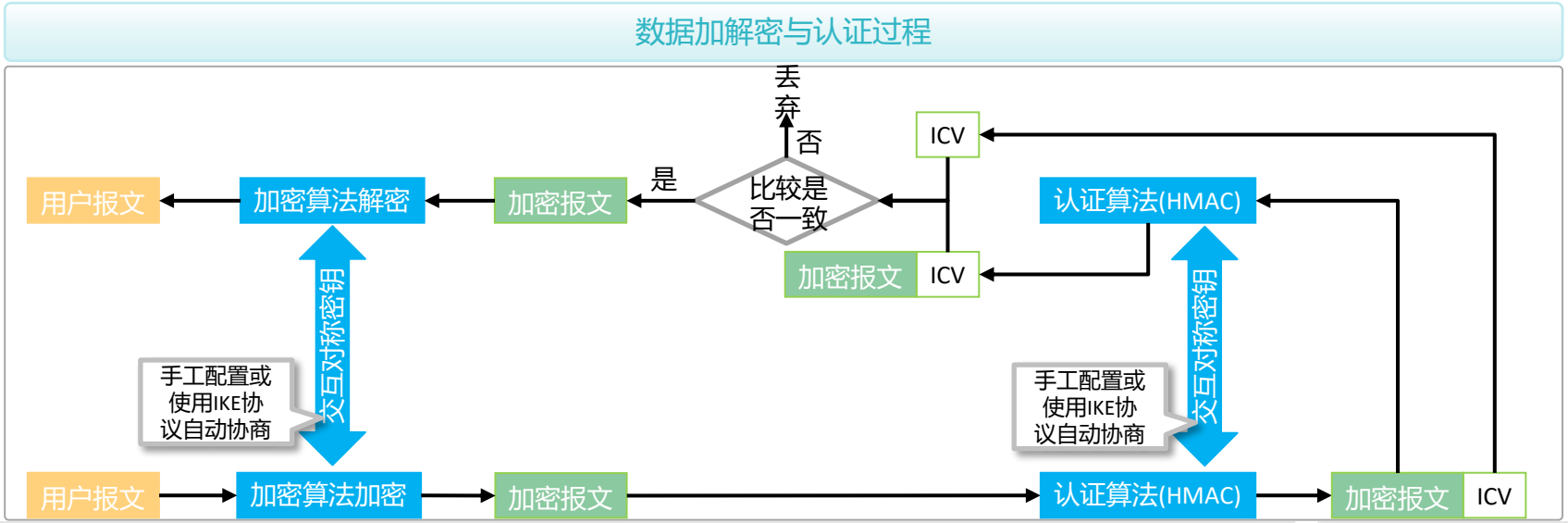
密钥交换介绍

- 现网中交互对称密钥一般会使用密钥分发协议：IKE（Internet Key Exchange，因特网密钥交换）。
- IKE协议建立在ISAKMP（Internet Security Association and Key Management Protocol, Internet安全联盟和密钥管理协议）定义的框架上，是基于UDP的应用层协议。它为IPsec提供了自动协商密钥、建立IPsec安全联盟的服务，能够简化IPsec的配置和维护工作。



数据加密与认证

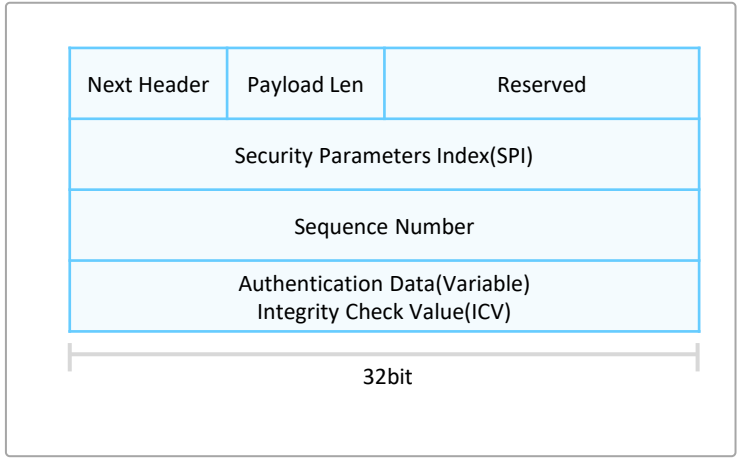
- IPsec提供了两种安全机制：加密和认证。
  - IPsec采用对称加密算法对数据进行加密和解密。数据发送方和接收方使用相同的密钥进行加密、解密。
  - IPsec采用HMAC（Hash-based Message Authentication Code）功能，比较数字签名进行数据完整性和真实性认证。



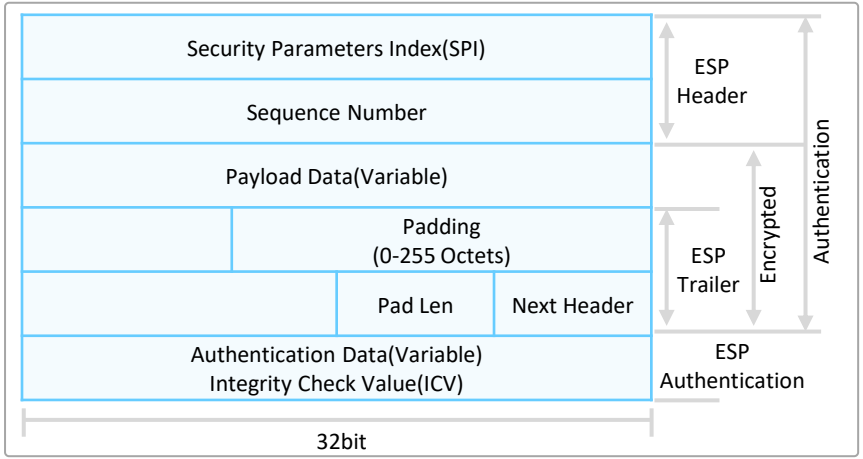
安全协议介绍

- IPsec有两种传输层协议提供认证或加密服务：AH（Authentication Header,认证头），ESP（Encapsulating Security Payload,封装安全载荷）。
  - 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。

AH报文头部结构

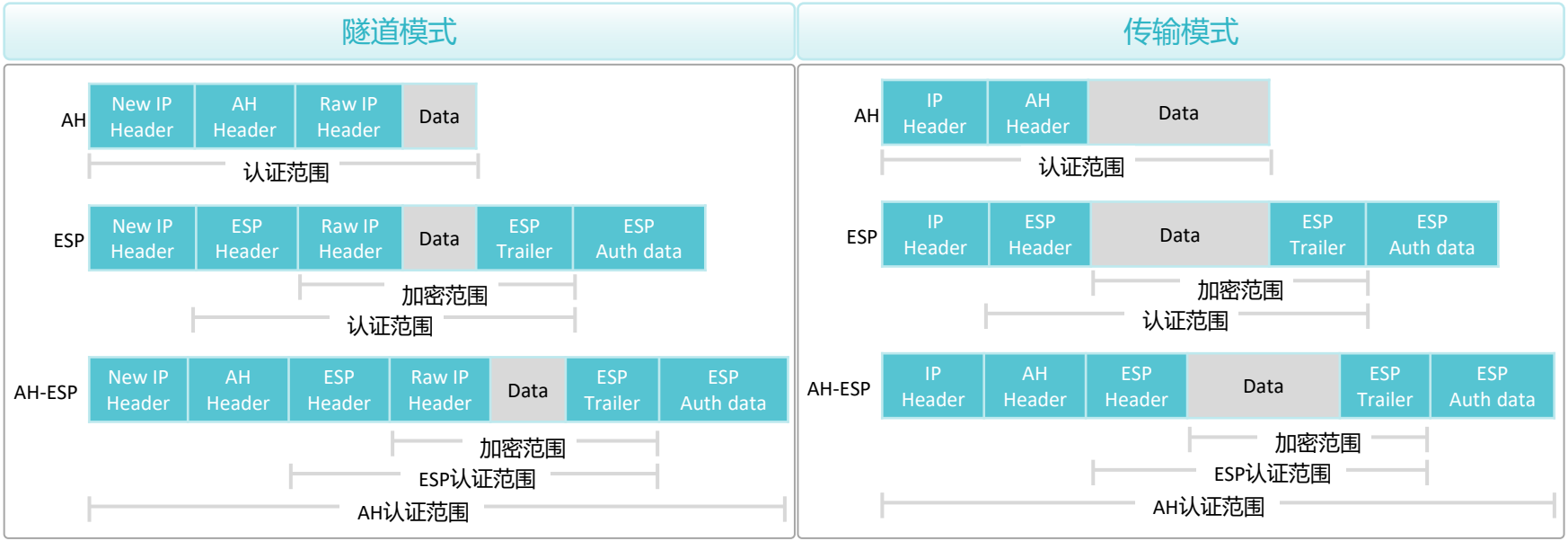


ESP报文头部结构

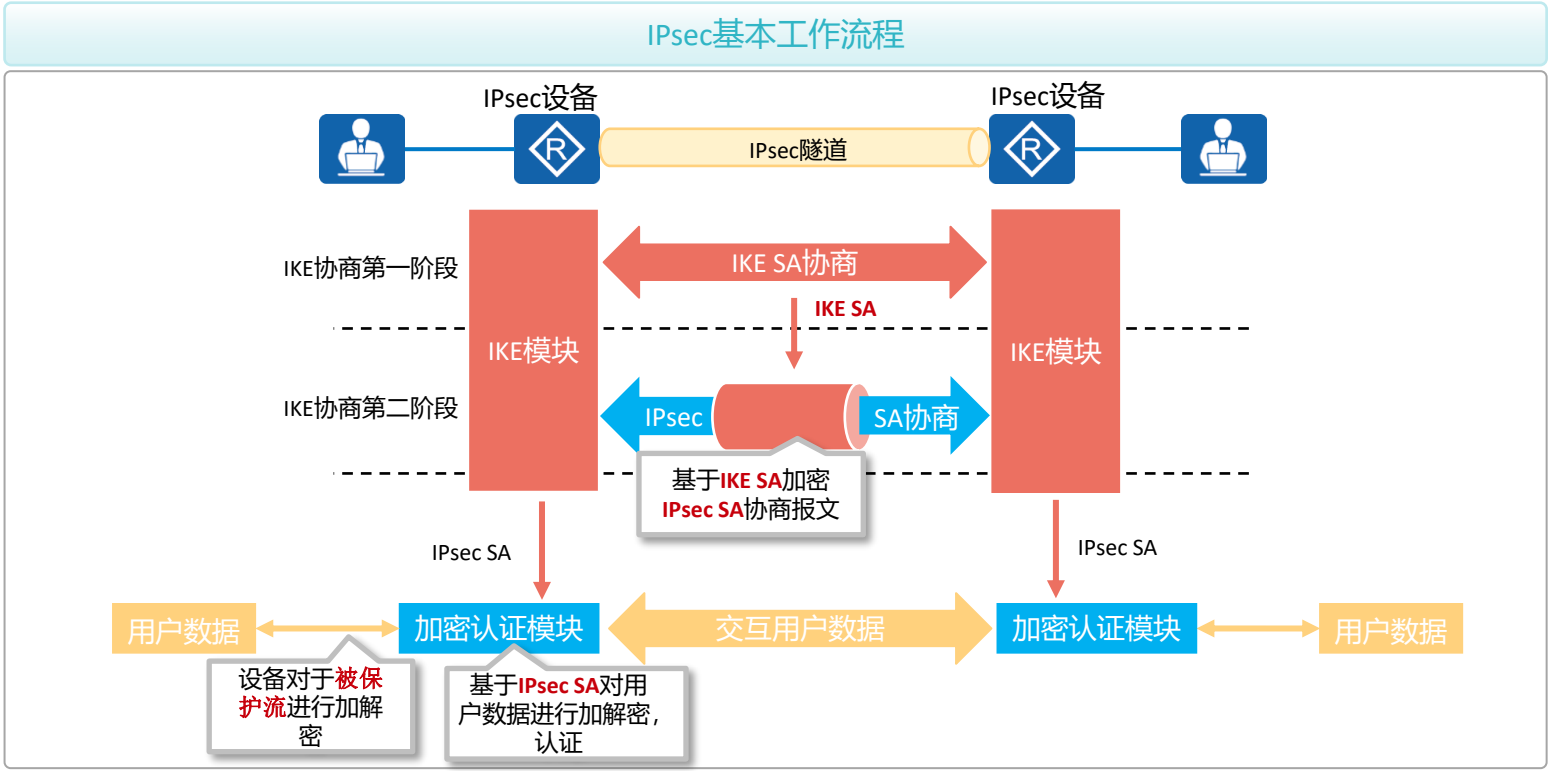


封装模式介绍

- 封装模式是指将AH或ESP相关的字段插入到原始IP报文中，以实现对报文的认证和加密，封装模式有传输模式和隧道模式两种。
- 现网中多使用隧道模式进行封装。

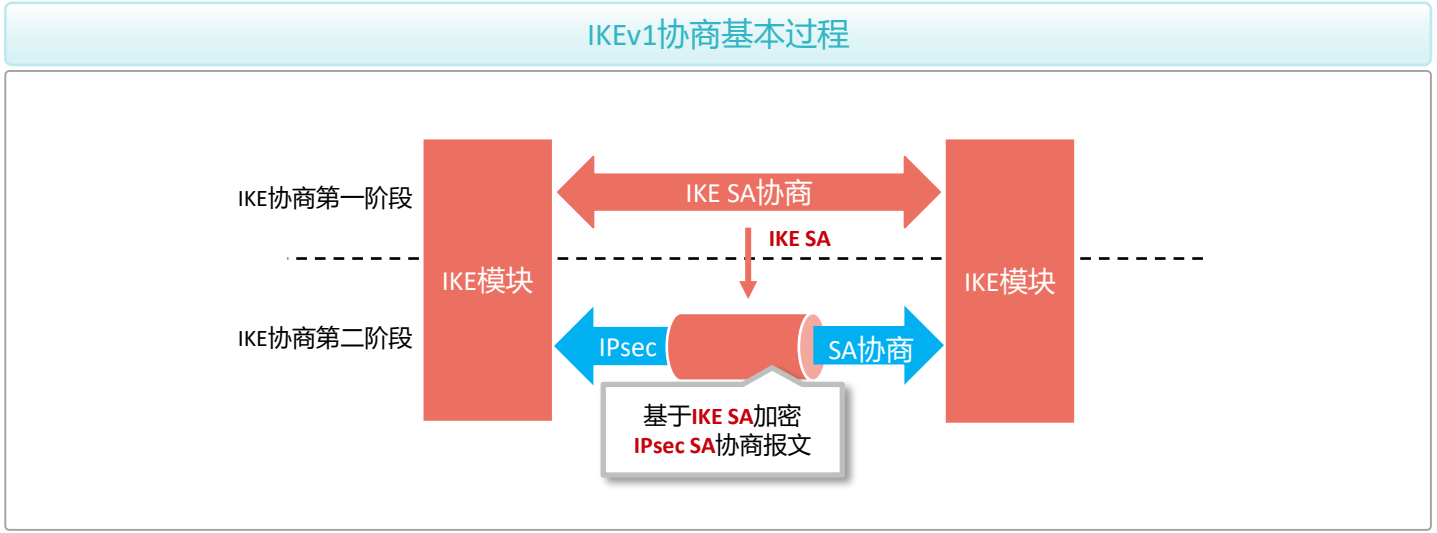


IPsec基本工作流程



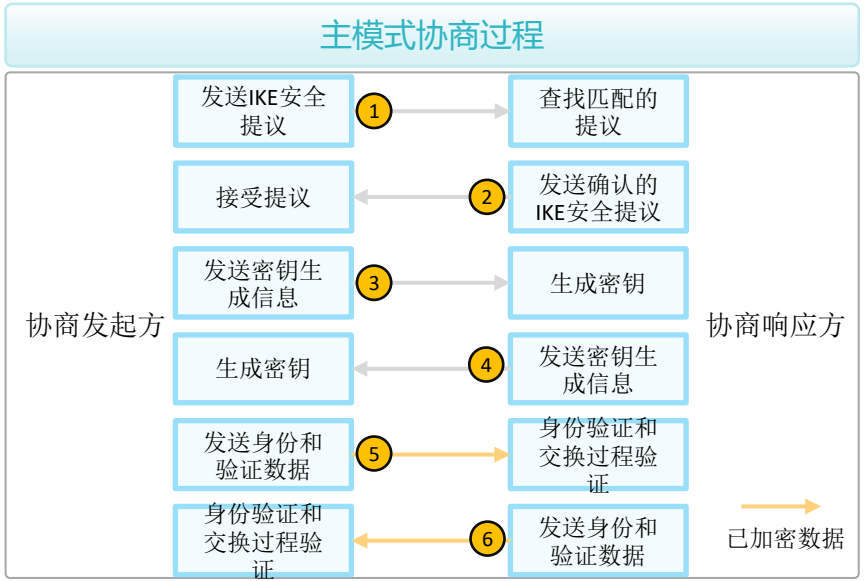
IKEv1介绍

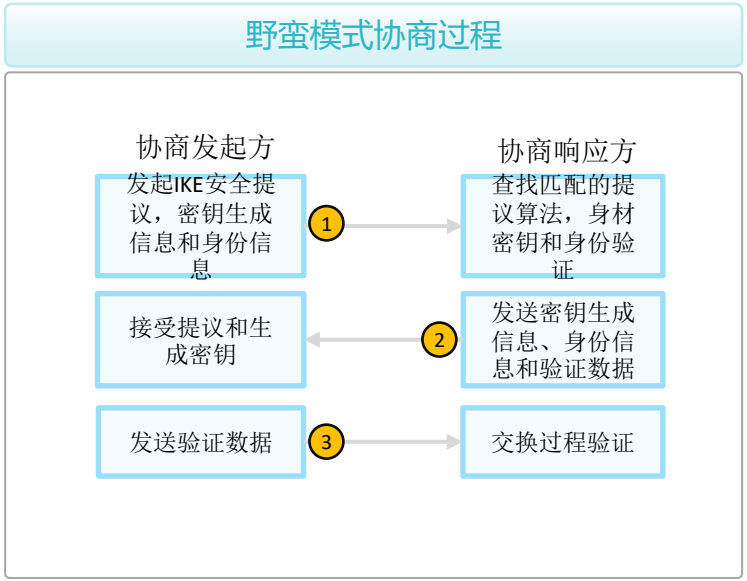
- 采用IKEv1协商安全联盟主要分为两个阶段：第一阶段，通信双方协商并建立IKE协议本身使用的安全通道，即建立一个IKE SA；第二阶段，利用第一阶段已通过认证与安全保护的安全通道，建立一对用于数据安全传输的IPsec SA。



IKEv1协商第一阶段介绍

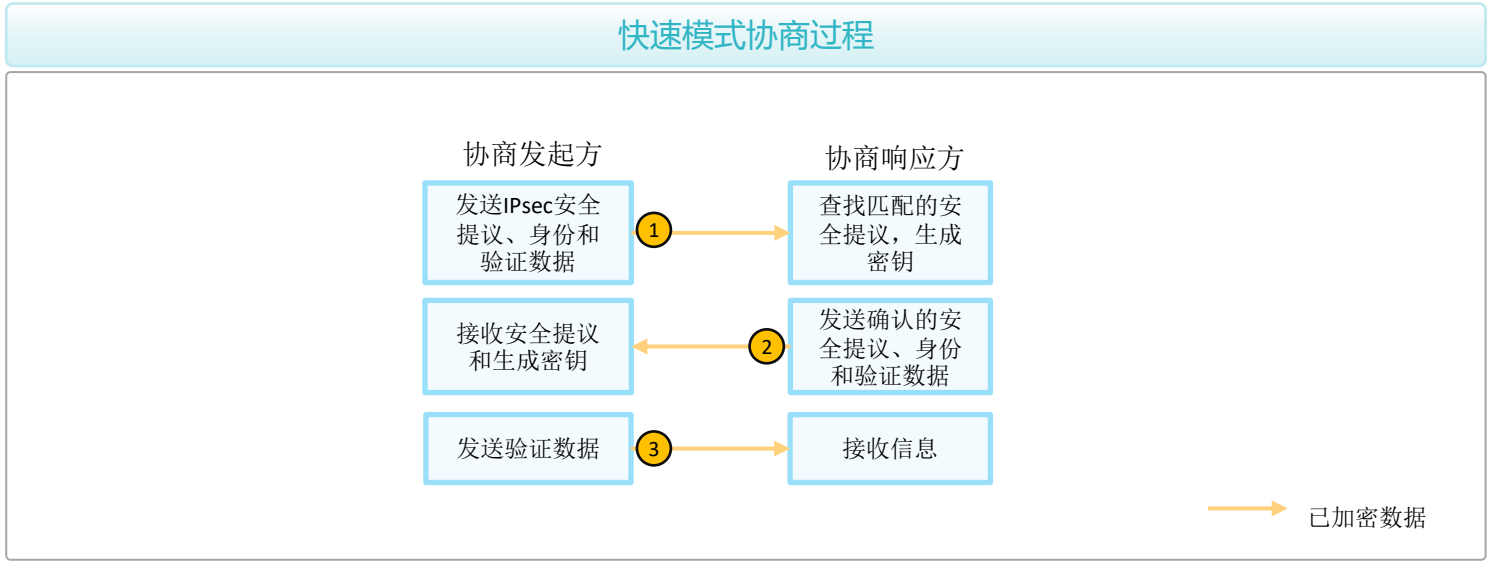
- IKEv1协商第一阶段的目的是建立IKE SA。IKE SA建立后对等体间的所有ISAKMP消息都将通过加密和验证，这条安全通道可以保证IKEv1第二阶段的协商能够安全进行。
- IKEv1协商第一阶段支持两种协商模式：主模式（Main Mode）和野蛮模式（Aggressive Mode）。





IKEv1协商第二阶段介绍

- IKEv1协商第二阶段的目的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。
- 第二阶段采用快速模式（Quick Mode）。该模式使用IKEv1协商第一阶段中生成的密钥对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。

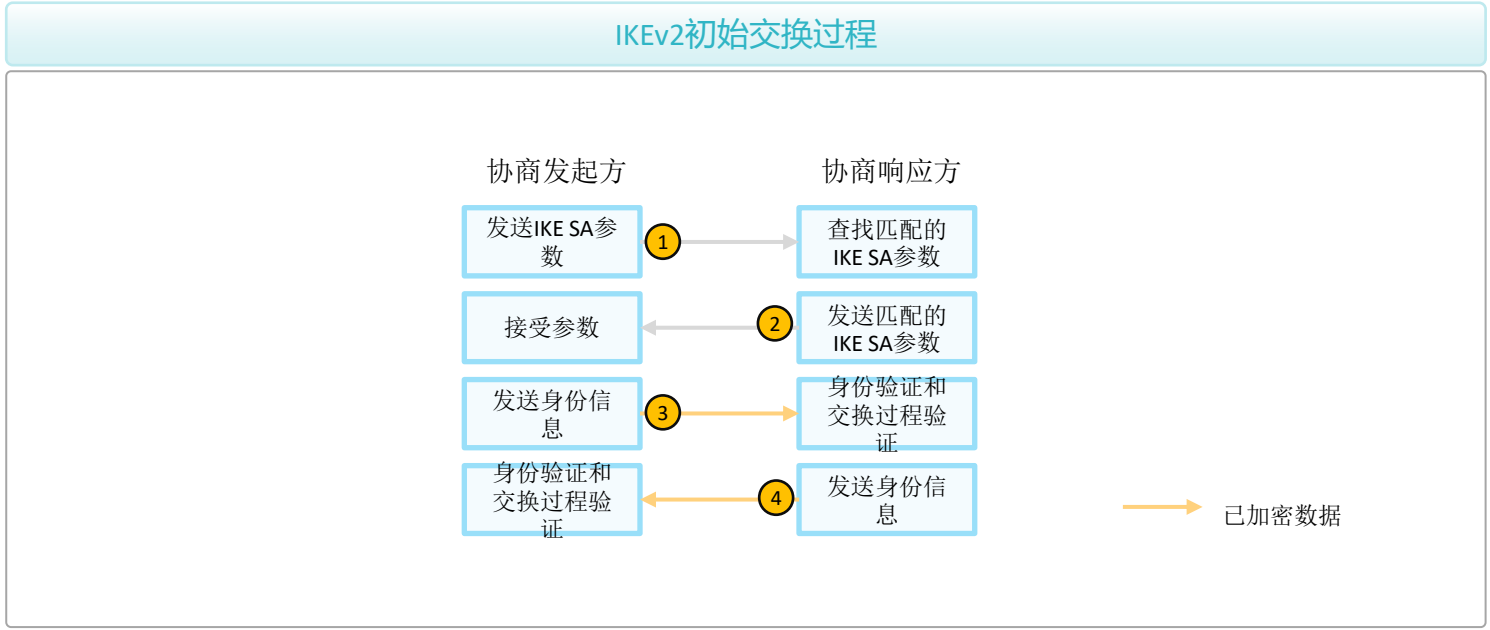


IKEv2介绍

- IKEv2简化了IKEv1协商SA的过程。IKEv2通常使用2次交换共4条消息就可以完成一对IPsec SA的建立，如果要求建立的IPsec SA大于一对时，每一对IPsec SA只需额外增加1次创建子SA交换，也就是2条消息就可以完成。
- IKEv2定义了三种交换：初始交换(Initial Exchanges)、创建子SA交换(Create_Child_SA Exchange)以及通知交换(Informational Exchange)。

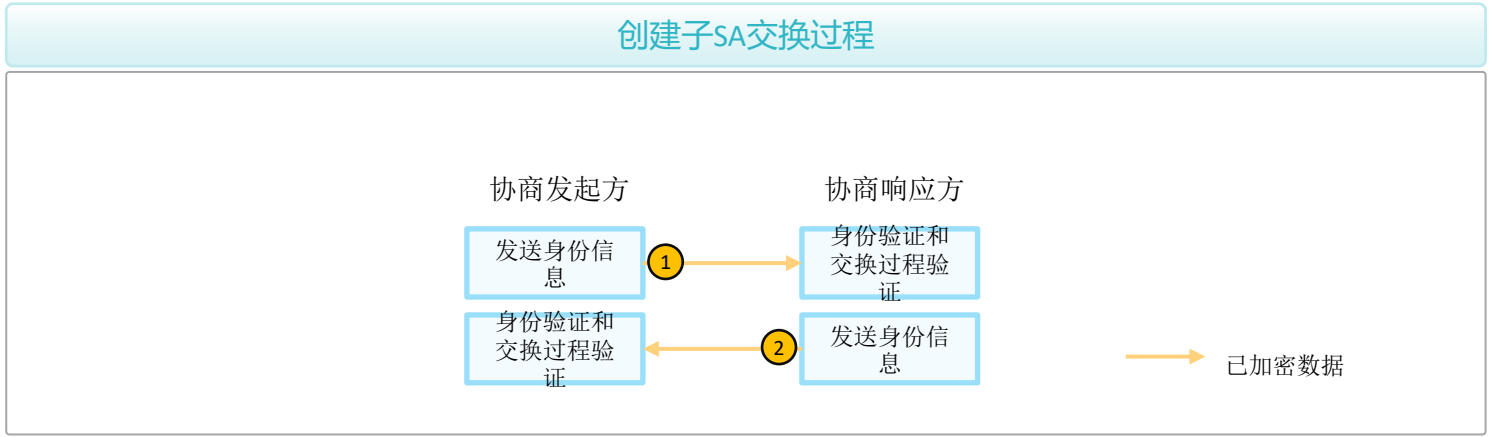
IKEv2初始交换介绍

- IKEv2通过初始交换就可以完成第一对IPsec SA的协商建立。初始交换包含两次交换四条消息。



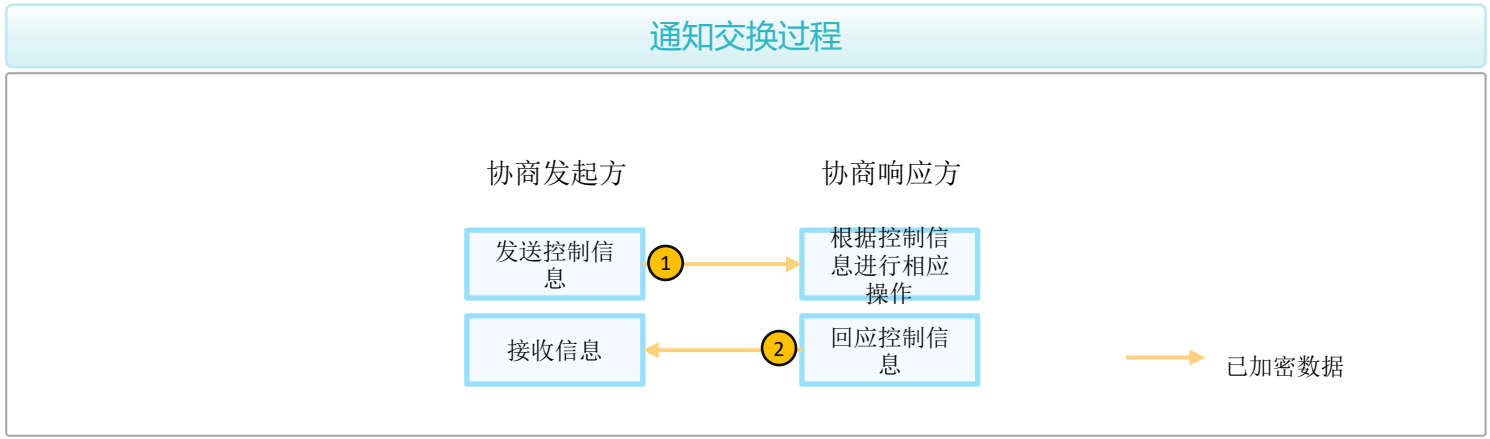
IKEv2创建子SA交换介绍

- 当一个IKE SA需要创建多对IPsec SA时，需要使用创建子SA交换来协商多于一对的IPsec SA。创建子SA交换还可以用于IKE SA的重协商。
- 创建子SA交换包含一个交换两条消息，对应IKEv1协商阶段2，交换的发起者可以是初始交换的协商发起方，也可以是初始交换的协商响应方。



IKEv2通知交换介绍

- 运行IKE协商的两端有时会传递一些控制信息，例如错误信息或者通告信息，这些信息在IKEv2中是通过通知交换完成的。
- 通知交换必须在IKE SA保护下进行，也就是说通知交换只能发生在初始交换之后。控制信息可能是IKE SA的，那么通知交换必须由该IKE SA来保护进行；也可能是某子SA的，那么该通知交换必须由生成该子SA的IKE SA来保护进行。



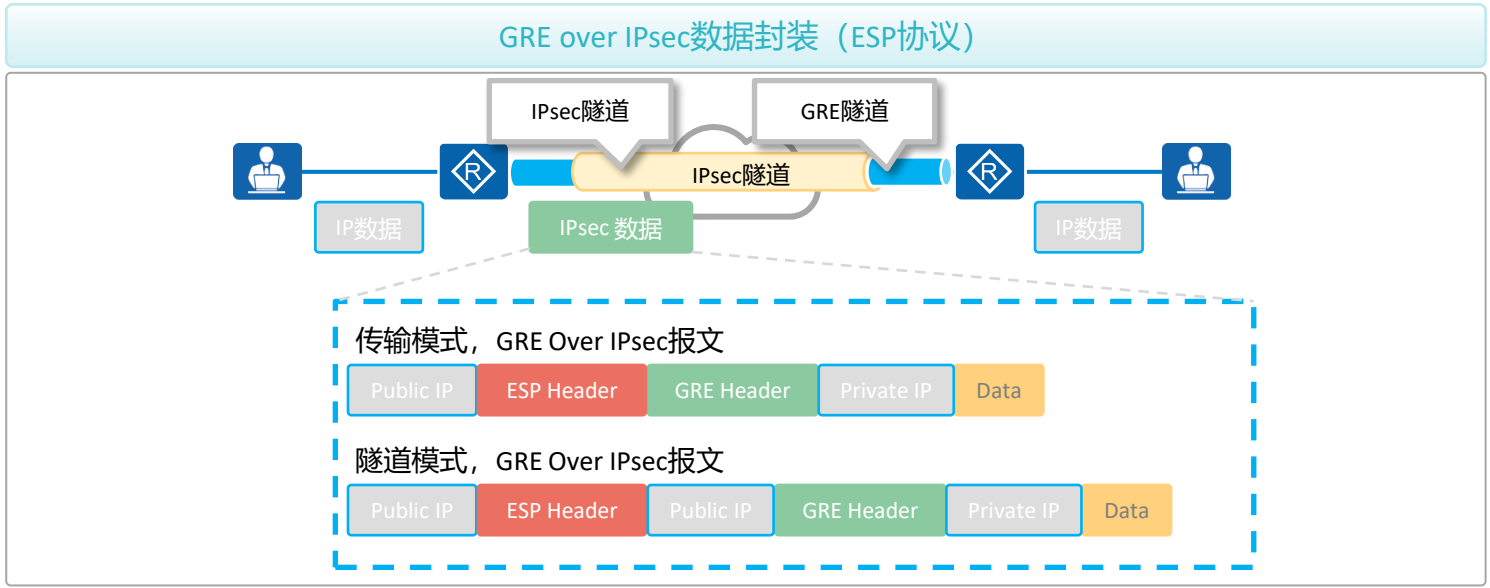
定义IPsec被保护流

- IPsec是基于定义的感兴趣流触发对特定数据的保护，可以通过以下两种方式定义：
  - ACL方式
    - 由ACL来指定要保护的数据流范围，筛选出需要进入IPsec隧道的报文。
  - 路由方式
    - 通过IPsec虚拟隧道接口建立IPsec隧道，将所有路由到IPsec虚拟隧道接口的报文都进行IPsec保护。
- 现网中GRE Over IPsec一般使用路由方式定义被保护流。

目录

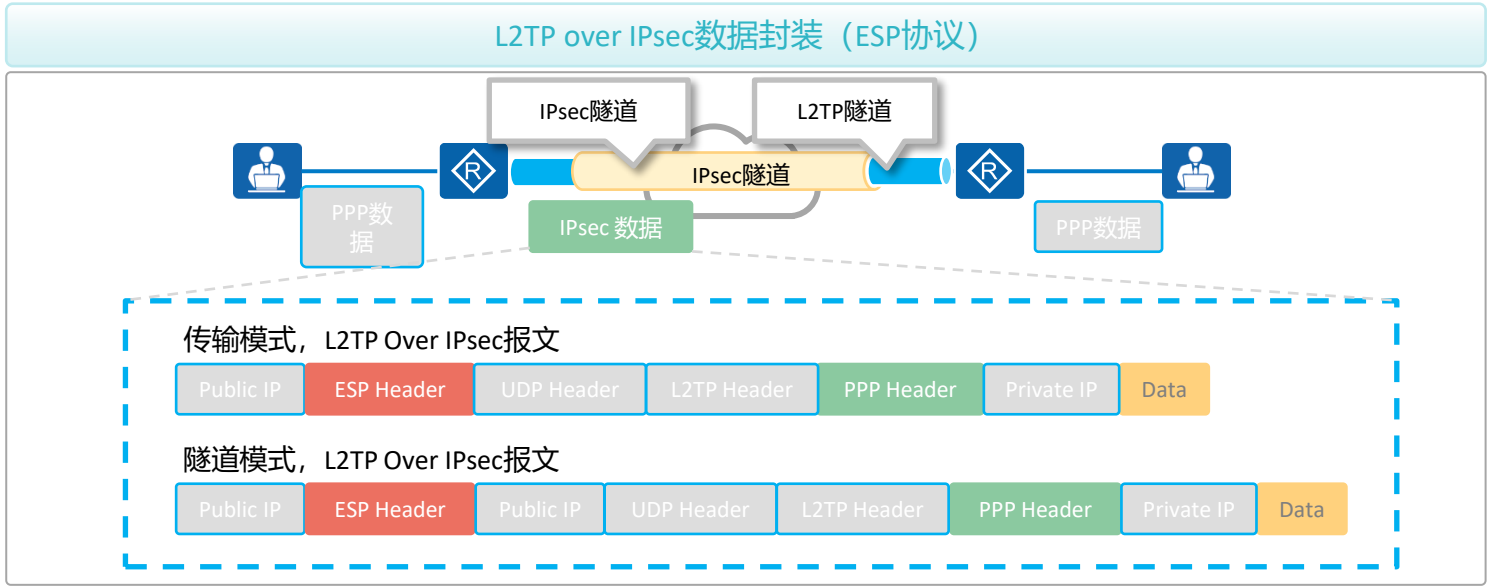
GRE Over IPsec

- GRE over IPsec可利用GRE和IPsec的优势，通过GRE将组播、广播和非IP报文封装成普通的IP报文，通过IPsec为封装后的IP报文提供安全地通信。
- 当网关之间采用GRE over IPsec连接时，先进行GRE封装，再进行IPsec封装。

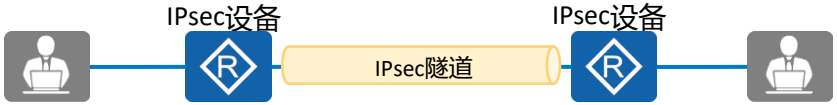


L2TP Over IPsec

- L2TP over IPsec，即先用L2TP封装报文再用IPsec封装，这样可以综合两种VPN的优势，通过L2TP实现用户验证和地址分配，并利用IPsec保障通信的安全性。L2TP over IPsec既可以用于分支接入总部，也可以用于出差员工接入总部。



配置IKE



- IPsec隧道两端设备的配置基本一致，IPsec配置思路如下：
  - 配置IKE安全提议。
  - 配置IKE对等体。
  - 配置感兴趣流，一般使用ACL定义。
  - 配置IPsec安全提议，定义加密认证所用方式。
  - 配置IPsec安全策略，一般使用ISAKMP或者策略模板方式。

- 配置IKE安全提议：

System-view

ike proposal [proposal-number] //创建IKE安全提议

authentication-method [pre-share | rsa-signature | digital-envelope] //配置IKE认证方式，默认使用pre-shared

authentication-algorithm [algorithm] //配置IKEv1所用认证算法，默认使用SHA2-256

encryption-algorithm [algorithm] //配置IKE加密方式，默认使

System-view

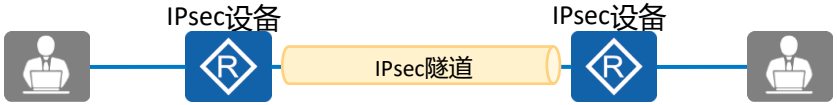
ike peer [peer-name] //创建IKE对等体

ike-proposal [proposal-number] //应用IKE安全提议

pre-shared-key cipher [key] //配置IKE协商的预共享密钥

remote-address [ip-address] //配置IKE协商对端的IP地址

配置IPsec安全提议



- 感兴趣流，一般使用ACL定义，本课程主要描述IPsec配置，ACL配置不再赘述。
- IPsec安全提议是安全策略或者安全框架的一个组成部分，它包括IPsec使用的安全协议、认证/加密算法以及数据的封装模式，定义了IPsec的保护方法，为IPsec协商SA提供各种安全参数。

- 配置安全提议命令如下：

System-view

IPsec proposal [proposal-name]　　//创建IPsec安全提议

transform [ah | esp | ah-esp]　　//配置IPsec使用的安全协议

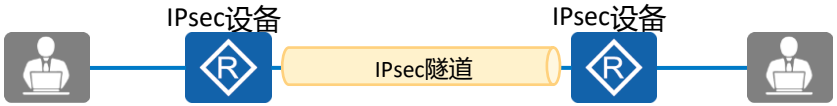
esp authentication-algorithm [algorithm]　//配置ESP安全协议的认证方式

esp encryption-algorithm [algorithm]　　//配置ESP安全协议的加密方式

ah authentication-algorithm [algorithm]　　//配置AH安全协议的认证方式，现网中一般使用ESP安全协议

encapsulation-mode [transport | tunnel]　　//配置IPsec数据包的封装方式

配置ISAKMP方式IPsec安全策略



- ISAKMP方式IPsec安全策略适用于对端IP地址固定的场景。
- ISAKMP方式IPsec安全策略直接在IPsec安全策略视图中定义需要协商的各参数，协商发起方和响应方参数必须配置相同。

- 配置IPsec安全策略命令如下：

System-view

IPsec policy [policy-name] [seq-number] **isakmp** //创建ISAKMP方式IPsec安全策略

security acl [acl-number] //在IPsec安全策略中引用ACL

proposal [proposal-name] //在IPsec安全策略中引用IPsec安全提议

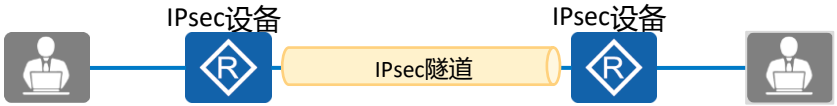
ike-peer [peer-name] //在IPsec安全策略中引用IKE对等体

System-view

interface [interface-type interface-num] //IPsec安全策略可用在普通接口，子接口，隧道接口下

IPsec policy [policy-name] //在接口上应用IPsec安全策略

配置策略模板方式IPsec安全策略



- 采用策略模板方式IPsec安全策略可简化多条IPsec隧道建立时的配置工作量，适用于对端IP地址不固定或存在多个对端的场景。
- 采用策略模板方式IPsec安全策略建立IPsec隧道时，未定义的可选参数由发起方来决定，而响应方会接受发起方的建议。

- 配置IPsec安全策略命令如下：

System-view

IPsec policy-template [template-name] [seq-number] //创建IPsec策略模板

security acl [acl-number] //在IPsec安全策略中引用ACL

proposal [proposal-name] //在IPsec安全策略中引用IPsec安全提议

ike-peer [peer-name] //在IPsec策略中引用IKE对等体

IPsec policy [policy-name] [seq-number] isakmp template [template-

System-view

interface [interface-type interface-num] //IPsec安全策略可用在普通接口，子接口，隧道接口下

IPsec policy [policy-name] //在接口上应用IPsec安全策略

THANK YOU

Ping 通您的梦想～

腾讯课堂交流群：17942636

ADD：苏州市干将东路666号和基广场401-402；Tel：0512-8188 8288；

课程咨询QQ：2853771087 ； 官网 :www.51glab.com