第22讲讲VPN：朝中有人好做官

VPN，全名Virtual Private Network，虚拟专用网，就是利用开放的公众网络，建立专用数据传输通道，将其他人联系起来。

通过隧道技术，仿真，点对点通信，利用一种协议仿真一种协议，同时确保传输的安全和私密性。隧道协议的核心就是封装，把一个IP包封装起来，利用外部的传输协议进行二次封装。隧道在其他当中的应用还包括：

这里指的隧道技术，是指基于IPv4隧道来传送IPv6数据报文的隧道技术。为了实现在IPv4海洋中传递IPv6信息，可以将IPv4作为隧道载体，将IPv6报文整个封装在IPv4数据报文中，使IPv6报文能够穿透IPv4海洋到达另一个IPv6小岛。

关于这个技术来打个比方，一个快递公司收件之后，发现目的地自己没有站点，无法投送，则将此包裹转交给能到达目的地的快递公司（例如中国邮政）来投递。也就是说将快递公司已经封装好的包裹（类似于IPv6报文），外面再用中国邮政的包装再封装一次（类似于封装成IPv4报文），以便于这个包裹能在中国邮政的系统（IPv4海洋）中被正常投递。

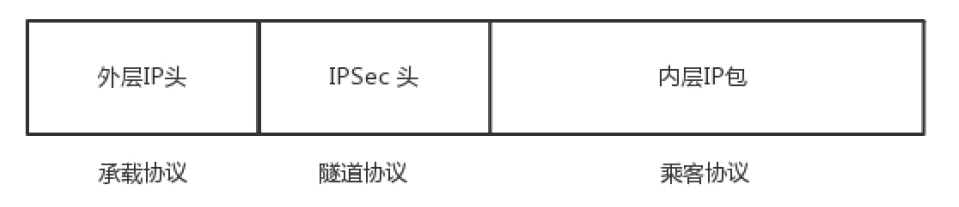
隧道包含的协议有：乘客协议，隧道协议，承载协议。

以一个例子为例，从大陆到海南岛，就相当于大陆和海南岛是点对点连接。

去海南要用到轮渡，就是隧道协议。

自己协议本身如何在马路上形式的协议，是乘客协议。

在海上坐船航行，海上航行的方式，就是承载协议。

IPsec协议（安全隧道协议），用来保证传输的加密性，但是这种**点对点基于IP协议**本身效率低，以为是基于IP协议的，IP协议本身就不是面向连接的协议，会尝试不同的路径。

ATM协议，是在正式建立一条数据通信之前，通过建立一条路径，以后都是通过这条路径进行传输。但是缺点是一旦中间的链路断掉这条连接也就短了。

多协议标签交换（MPLS，Multi-Protocol Label Switching）将两者的优势集中了起来。

### 总结

（1）VPN可以将一个机构的多个数据中心通过隧道的方式连接起来，让机构感觉在一个数据中心里面，就像自驾游通过琼州海峡一样；

（2）完全基于软件的IPsec VPN可以保证私密性、完整性、真实性、简单便宜，但是性能稍微差一些；

（3）MPLS-VPN综合了IP转发模式和ATM的标签转发模式的优势，性能较好，但是需要从运营商购买。