



警示

1. 实验心得体会如有雷同，雷同各方当次实验心得体会成绩均以 0 分计。
2. 在规定时间内未上交实验报告的，不得以其他方式补交，当次心得体会成绩按 0 分计。
3. 报告文件以 PDF 文件格式提交。

本报告主要描述学生在实验中承担的工作、遇到的困难以及解决的方法、体会与总结等。

院系		班 级	
学号	22336057	实验名称:	VPAN 实验
学生	丁晓琪		

一. 本人承担的工作

完成主机 A 相关配置


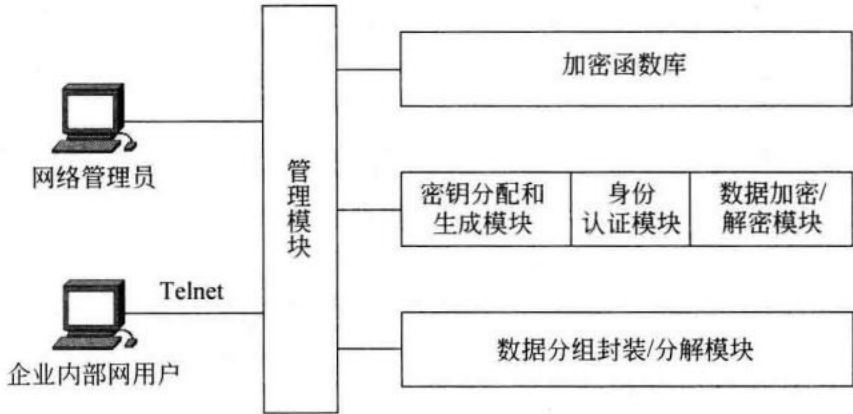
参与交换机和路由器的配置

二. 遇到的困难及解决方法

- 问题：在 10-1 步骤三中发现完成基础配置后主机 A 和主机 B ping 不通
解决：向老师请教后发现书上的 loopback 逻辑端口配置在实际实验上不可行，更改配置到和主机直连的物理端口上
- 问题：在捕获数据包，检验通信安全性的时候发现在主机 B 上抓取的数据包无论是否配置 IPSec VPAN 都是明文传输
解决：经过分析与讨论发现只有两个路由器之间的链路配置了 IPSec VPAN，为了检验数据包是否加密应该抓取路由器之间的数据包分析
- 问题：在配置路由器之间的镜像端口时发现连接路由器的 Serial 端口无法配置镜像端口
解决：修改实验拓扑



三. 体会与总结

概念	<p>定义：通过公用网络建立临时的，安全的连接</p> <p>主要目的：保护从信道一端传输到另一端的信息流</p>
VPN 安全技术	<p>隧道技术，加/解密技术，密钥管理技术，用户与设备身份认证技术</p> <p>隧道技术：</p> <p>利用附加的报头封装帧，附加报头提供路由信息</p>  <p>第二层隧道协议：在数据链路层实现数据封装</p> <p>第三层隧道协议：在网络层实现数据封装</p>
加密系统	<p>DES,3DES,Hash, 密钥交换</p>
IPSec 协议	<p>属于第三层隧道协议：应用于 IP 层网络数据安全的一整套体系结构</p> <ul style="list-style-type: none">组成：  <p>图 10-7 IPSec VPN 系统的组成</p>



• 主要协议：

ESP

- 功能：数据加密，数据源认证，数据完整性校验，防报文重放
- 原理：在数据包的 IP 头后加 ESP 报文头，数据包后加 ESP 报文尾。先将用户数据加密后再封装到 IP 包



ESP 报文头字段包括以下两部分：

- (1) 安全参数索引(Security Parameters Index, SPI)：32 位，用于标识有相同 IP 地址和相同安全协议的不同 SA。由 SA 的创建者定义，只有逻辑意义。
- (2) 序列号(Sequence Number)：32 位，一个单项递增的计数器，用于防止重放攻击，SA 建立之初初始化为 0，序列号不允许重复。

ESP 报文尾字段包括以下三部分：

- (1) 填充项(Padding)：0~255B。交换算法要求数据长度(以位为单位)模 512 的值为 448，若应用数据长度不足，则用扩展位填充。
 - (2) 填充长度(Padding Length)：接收端根据该字段长度去除数据中扩展位。
 - (3) 下一个报文头(Next Header)：识别下一个使用 IP 协议号的报文头，如 TCP 或 UDP。
- ESP 报文尾字段中的验证数据(Authentication Data, AD)包含完整性检查和。完整性检查部分包括 ESP 报文头、有效载荷(应用程序数据)和 ESP 报文尾。

AH
协
议

功能：提供数据源认证，数据完整性校验和防报文重放。能保护通信免受篡改，但是不能防止窃听

原理：数据包加上身份校验报头



AH 协议头的格式如图 10-9 所示。

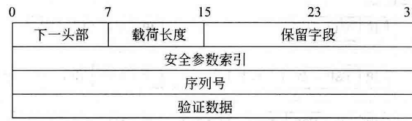


图 10-9 AH 协议头的格式

AH 协议头各字段含义如下。

- (1) 下一头部：8 位，标识认证头后面的下一个负载类型。
- (2) 载荷长度：8 位，表示以 32 位为单位的 AH 头部长度减 2，默认值为 4。
- (3) 保留字段：16 位，保留将来使用，默认值为 0。
- (4) 安全参数索引：32 位，用于标识有相同 IP 地址和相同安全协议的不同 SA。由 SA 的创建者定义，只有逻辑意义。
- (5) 序列号：32 位，一个单项递增的计数器，用于防止重放攻击，SA 建立之初初始化为 0，序列号不允许重复。
- (6) 验证数据：一个变长字段，由 SA 初始化时指定的算法计算，长度为整数倍 32 位。

IKE
协
议

功能：管理密钥交换

IPSec
的工作
模式

协议 \ 模式	传输模式	隧道模式
AH	IP AH 数据	IP AH IP 数据
ESP	IP ESP 数据 ESP-T	IP ESP IP 数据 ESP-T
AH-ESP	IP AH ESP 数据 ESP-T	IP AH ESP IP 数据 ESP-T

图 10-10 隧道模式和传输模式下的数据封装形式

- 隧道模式：整个 IP 数据包用于计算 AH/ESP 报文头，用于两个网关之间
- 传输模式：只有传输层数据用于计算，用于网关和主机之间，主机和主机之间

【交报告】

上传报告：助教

说明:上传文件名：小组号_学号_姓名_XX 实验.pdf