网络安全协议及分析
链路层扩展L2TP

密码与网络安全系　刘虹

2025年春季学期

课程体系

第一章 概述

第二章 链路层扩展L2TP

第三章 IP层安全IPSec

第四章 传输层安全SSL和TLS

第五章 会话安全SSH

第六章 代理安全Socks

第七章 网管安全SNMPv3

第八章 认证协议Kerberos

第九章 应用安全

本章学习目标

- PPP点到点协议的协议流程
- PPP点到点协议的帧格式
- PAP认证协议
- CHAP认证协议

提纲

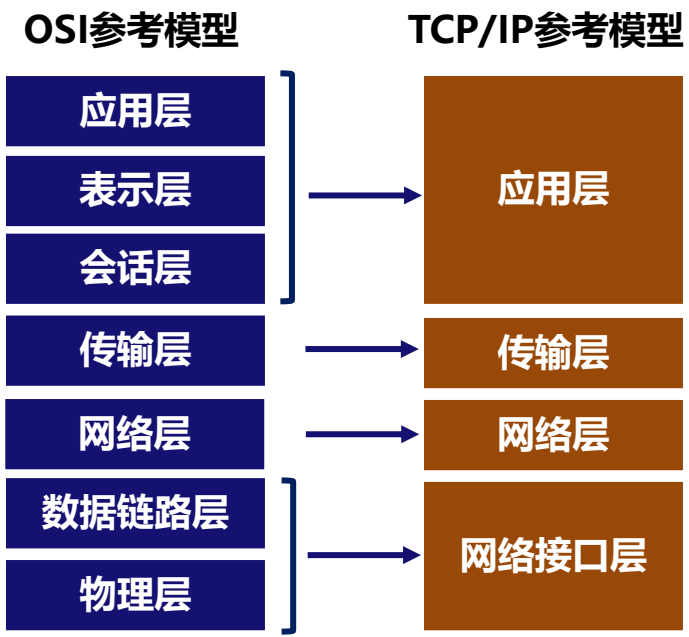
概述

- 传输控制协议/因特网互联协议

(Transmission Control Protocol / Internet Protocol，TCP/IP)

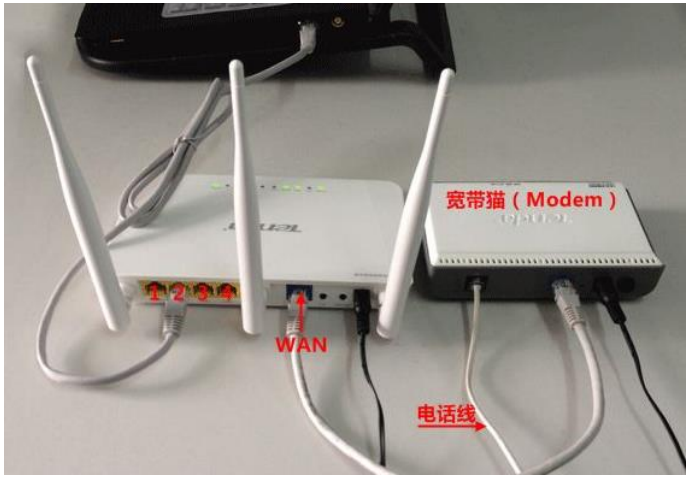
  - TCP：解决可靠传输问题
  - IP：解决异构网络互联问题

第二层隧道协议L2TP
(Layer 2 Tunneling Protocol)



第二层隧道协议L2TP

- PPP协议
  - L2TP对网络接口层PPP协议（Point to Point Protocol）进行了扩展，使得用户可以通过互联网建立一条点到点链路。
  - PPP用于两个对等实体之间的直连链路，这种链路使用**拨号或专线**连接方式，提供全双工的数据传输服务，数据按序传输。



第二层隧道协议L2TP

- IETF制定了L2TP以对PPP进行扩展
  - 其核心是允许客户跨越一个或多个IP网络（或ATM、帧中继等网络）建立虚拟的点到点链路。
  - L2TP不是严格意义上的安全协议，并未提供基于密码学的机密性、完整性、可用性等。提供了对口令等敏感信息的加密方法，以及基于共享秘密的身份认证方法。

提纲

一、引言

二、PPP点到点协议

三、PAP认证协议

四、CHAP认证协议

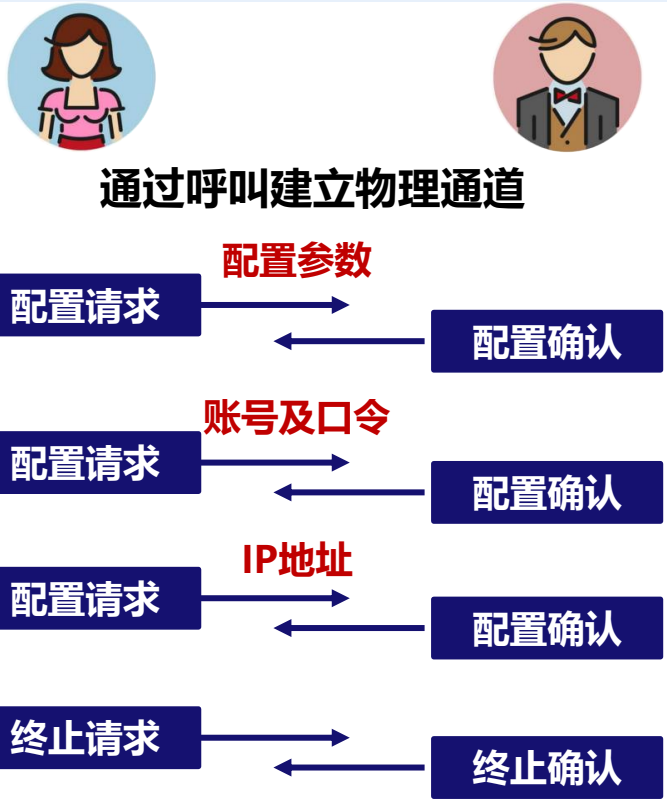
二 PPP协议

- PPP协议规定的内容：
  - 帧格式及成帧方法；
  - 用于建立、配置和测试PPP链路的链路控制协议（Link Control Protocol，LCP）
  - 一组用于建立和配置网络层协议的网络控制协议（Network Control Protocol，NCP）
    - IP数据：IP控制协议（IPCP）
    - DECnet数据：DECnet四阶段控制协议

二 PPP协议

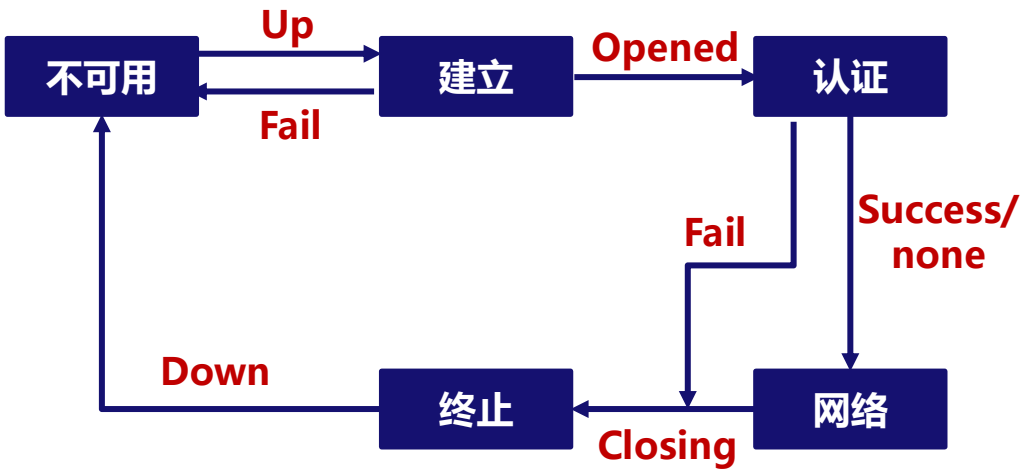
协议流程

- 发起方发送LCP配置请求报文，其中可包含各项配置参数，比如使用的认证协议、最大接收单元和压缩协议等。
- 回应方若同意各项配置参数，则返回确认报文。
- 发起方提供账号和口令，以便回应方验证自己的身份。
- 回应方验证发起方身份成功后向其返回确认报文。
- 发起方发出IPCP配置请求。
- 回应方返回确认，其中包含了分配给发起方的IP地址。
- 发起方发出LCP终止链路请求。
- 回应方返回确认，链路终止。



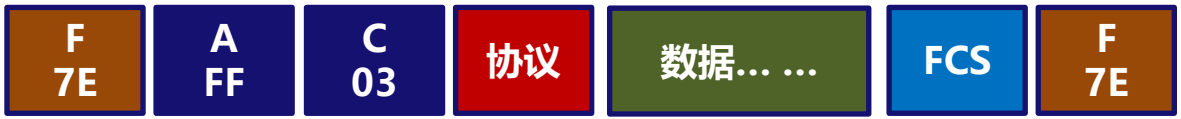
二 PPP协议

- 链路状态转换过程
  - 链路不可用阶段（Dead）
  - 链路建立阶段（Establish）
  - 认证阶段（Authenticate）
  - 网络层协议阶段（Network）
  - 链路终止阶段（Terminate）



二 PPP协议

- 帧格式
  - F：帧定界表
  - A：地址字符
  - C：控制字符
  - FCS ： 帧校验和字段



二 PPP协议

- LCP（Link Control Protocol链路控制协议）：
  - 代码域 code
  - 标识域 Indentifier
  - 长度域 Length
  - 数据域 Data

8bit	8bit	16bit	变长
code	Indentifier	Length	Data

二 PPP协议

- LCP（Link Control Protocol链路控制协议）：
  - 用于配置、维护和终止PPP链路

类型	功能	报文名称	代码
链路配置	建立和配置链路	Configure-Request	1
		Configure-Ack	2
		Configure-Nak	3
		Configure-Reject	4
链路终止	终止链路	Terminate-Request	5
		Terminate-Ack	6
链路维护	管理和调试链路	Code-Reject	7
		Protocol-Reject	8
		Echo-Request	9
		Echo-Reply	10
		Discard-Request	11

二 PPP协议

- LCP协议 **链路配置报文**：发起方向回应方发送报文“Configure-Request”报文，发起链路建立和配置过程，回应方可能的回应包括：
  - 返回确认（Configure-ACK)
  - 返回否认（Configure-NAK)
  - 返回拒绝（Configure-REJECT)

- 最大接收单元
- 认证协议
- 质量协议
- 幻数
- 协议域压缩
- 地址及控制域压缩

二 PPP协议

- 幻字（魔术字）
  - 在链路建立过程中比较重要的一个参数，这个参数是在Config-Request里面被协商的，主要的作用是防止环路
  - 如果在双方不协商魔术字的情况下，某些LCP的数据报文需要使用魔术字时，那么只能是将魔术字的内容填充为全0；反之，则填充为配置参数选项协商后的结果。

二 PPP协议

- LCP协议 **链路终止报文**
  - 当通信的一方欲终止链路时，应向对方发送Terminate-Request报文，对方则Terminate-Ack响应。这两种报文的首部与Configure-Request首部相同，其数据区可以为空，也可以是发送方自定义的数值。
- LCP协议 **链路维护报文**：链路维护报文用于错误通告及链路状态检测。
  - Code-Reject
  - Protocol-Reject
  - Echo-Request、Echo-Reply
  - Discard-Request

二 PPP协议

- IPCP控制协议（IP Control Protocol)
  - 负责完成IP网络层协议通信所需配置参数的选项协商，负责建立和中止IP模块。
  - IPCP在运行的过程当中，主要是完成点对点通信设备的两端动态的协商IP地址。
  - IPCP包在PPP没有达到网络层协议阶段以前不能进行交换，如果有IPCP包在到达此阶段前到达会被抛弃。

二 PPP协议

- IPCP报文的三个配置选项
  - 多个IP地址（类型代码“1"）
  - IP压缩协议（类型代码“2”）
    - 该选项用以协商使用的压缩协议，仅规定“Van Jacobson” 压缩协议，编号为002D
  - IP地址（类型代码“3”）

二 PPP协议

- IPCP控制协议静态协商
  - 点对点的通信设备两端在PPP协商之前已配置好了IP地址，所以就无须在网络层协议阶段协商IP地址，而双方唯一要做的就是告诉对方自身的IP地址。
  - IPCP协议中并未规定点对点两端的IP地址必须在同一网段，通信两端如果是手动设置每一端的IP地址时，无须双方地址在同一网段。

二 PPP协议

- IPCP控制协议动态协商
  - 动态协商是一端配置为动态获取IP地址，另一端通过手动方式配置IP地址，且允许给对端分配IP地址。
  - 发送方连续发送两次Config-Request报文，才能完成发送方的协商过程。
  - 接收方仍然只需要发送一次Config-Request即可完成本端的协商过程。

提纲

一、引言

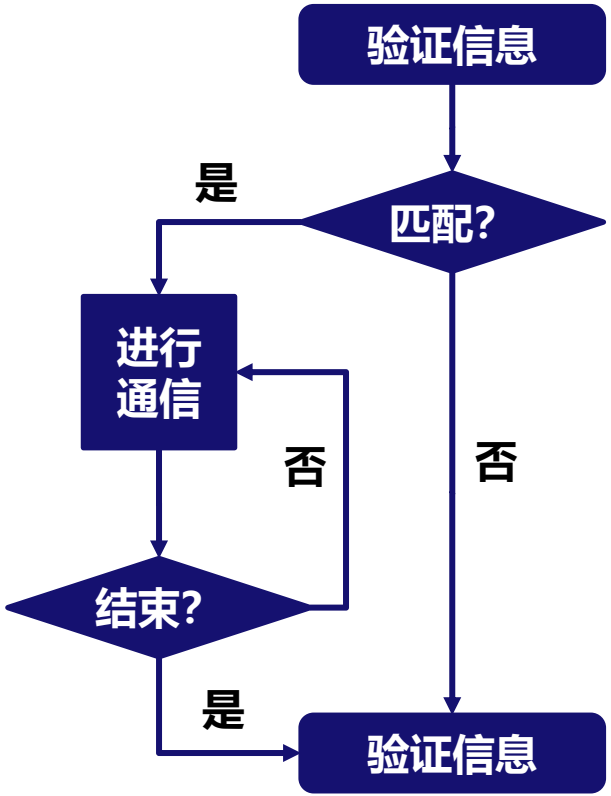
二、PPP点到点协议

三、PAP认证协议

四、CHAP认证协议

三 PAP认证协议

- PAP：基于口令的认证协议（Password Authentication Protocol）
  - 两次握手认证协议，在链路初始化时，被认证端首先发起认证请求，向认证端发送用户名和密码信息进行身份认证。
  - 密码口令以明文发送，所以安全性较低，支持单向和双向认证。



提纲

一、引言

二、PPP点到点协议

三、PAP认证协议

四、CHAP认证协议

四

CHAP认证协议

- CHAP：挑战握手认证协议（Challenge Handshake Authentication Protocol）
  - 通过三次握手验证被认证端的身份，在初始链路建立时完成，为了提高安全性，在链路建立之后周期性进行验证。
  - CHAP比PAP更安全，因为CHAP不在线路上发送明文，而是发送经过MD5过的随机数序列。CHAP支持单向和双向认证。

四 CHAP认证协议

发送用户名

发送随机数

利用共享密值、
随机数
计算MD5值

利用共享密值、
随机数
计算MD5值

发送MD5值

比对MD5值

办公地点：理科大楼B1715

联系方式：17621203829

邮箱：liuhongler@foxmail.com