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

- L2TP协议的架构和流程
- L2TP协议安全性分析
- L2TPv2和L2TPv3的区别

提纲

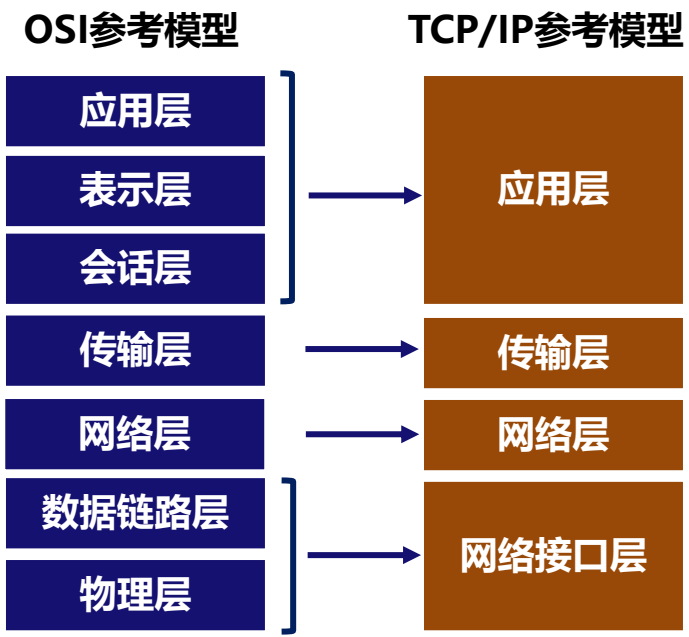
概述

- 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)

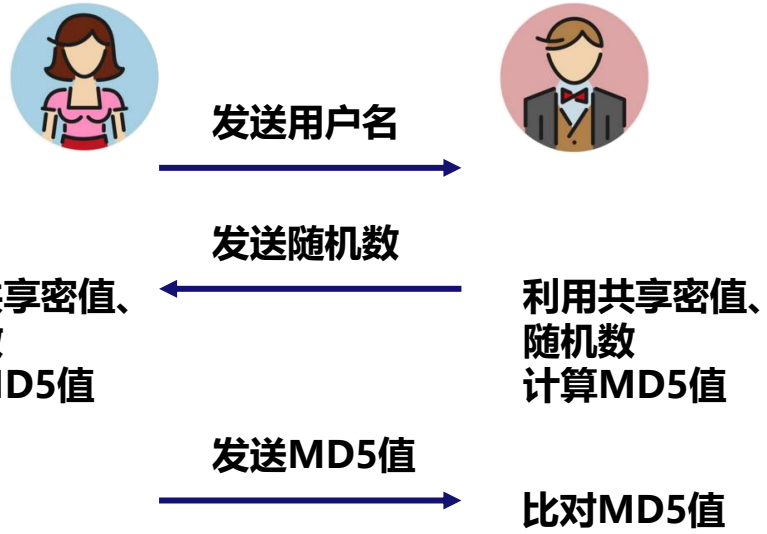


PPP协议

- 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**）
    - 例如，IP控制协议（IPCP）

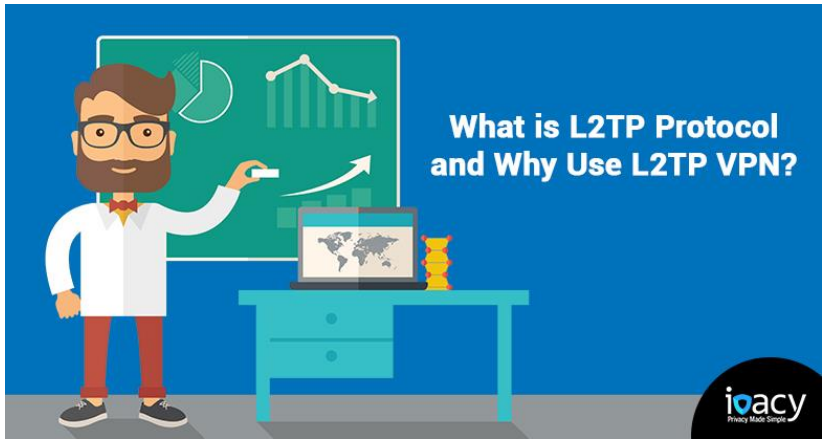
二 PPP协议

- PAP：基于口令的认证协议
- CHAP：挑战握手认证协议



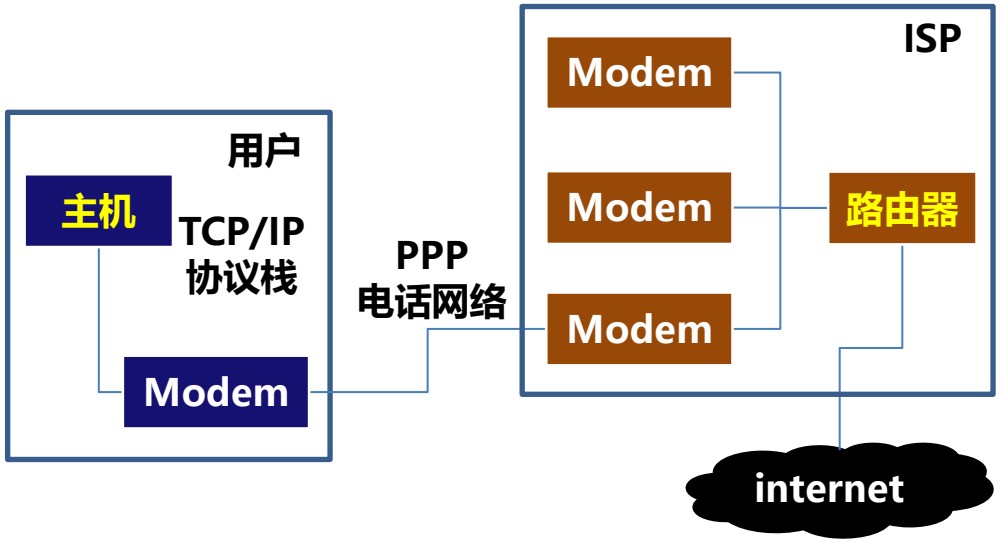
L2TP协议

- L2TP是一种工业标准的Internet隧道协议，L2TP对PPP进行了扩展，它允许链路端点跨越多个网络。
- 与L2TP密切相关的是思科第二层转发（Cisco Layer Two Forward，L2F）和点到点隧道协议（Point Tunnel Protocol，PPTP)。



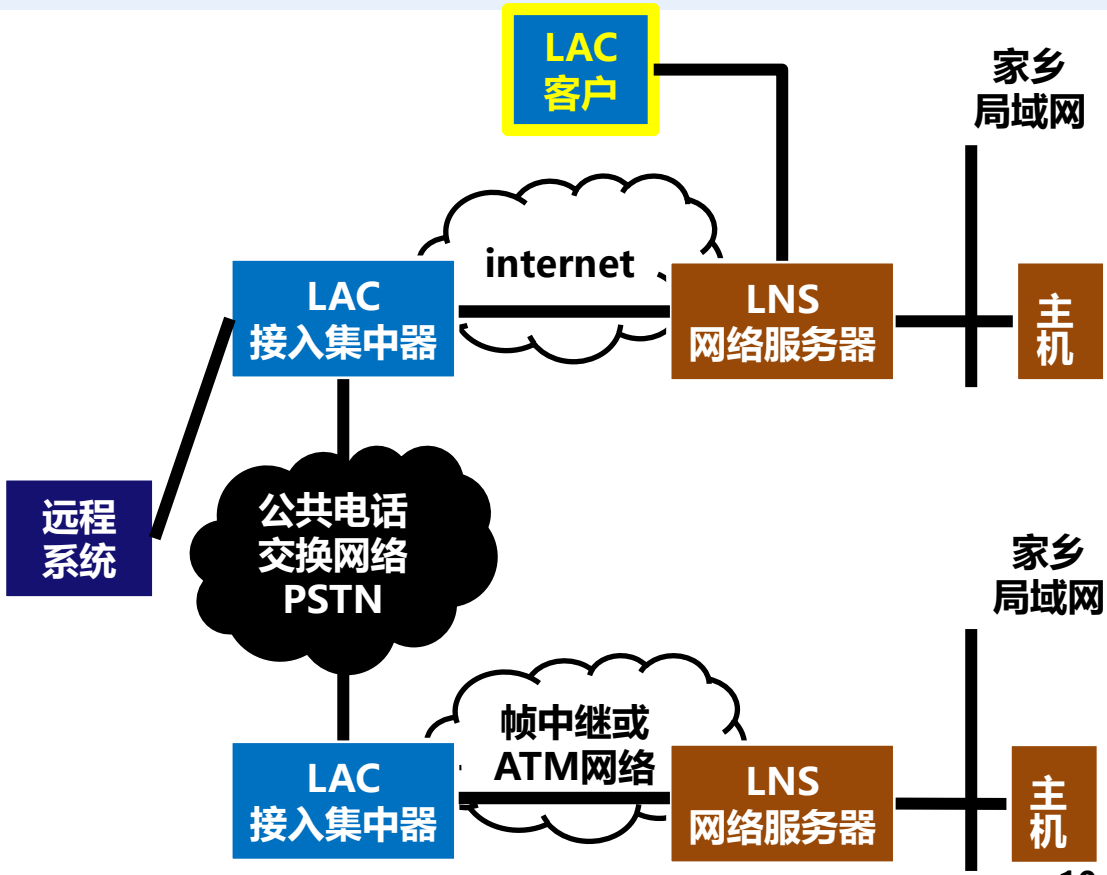
L2TP协议架构

- 回顾PPP应用场景
  - 调制解调器（Modulator and Demodulator，Modem）是PPP网络的关键设备，它提供模拟信号与数字信号的转换功能。



L2TP协议架构

- L2TP应用场景
  - L2TP接入集中器和L2TP网络服务器是L2TP的两个关键组件，它们之间通过协商建立隧道，用以转发PPP报文。



L2TP协议架构

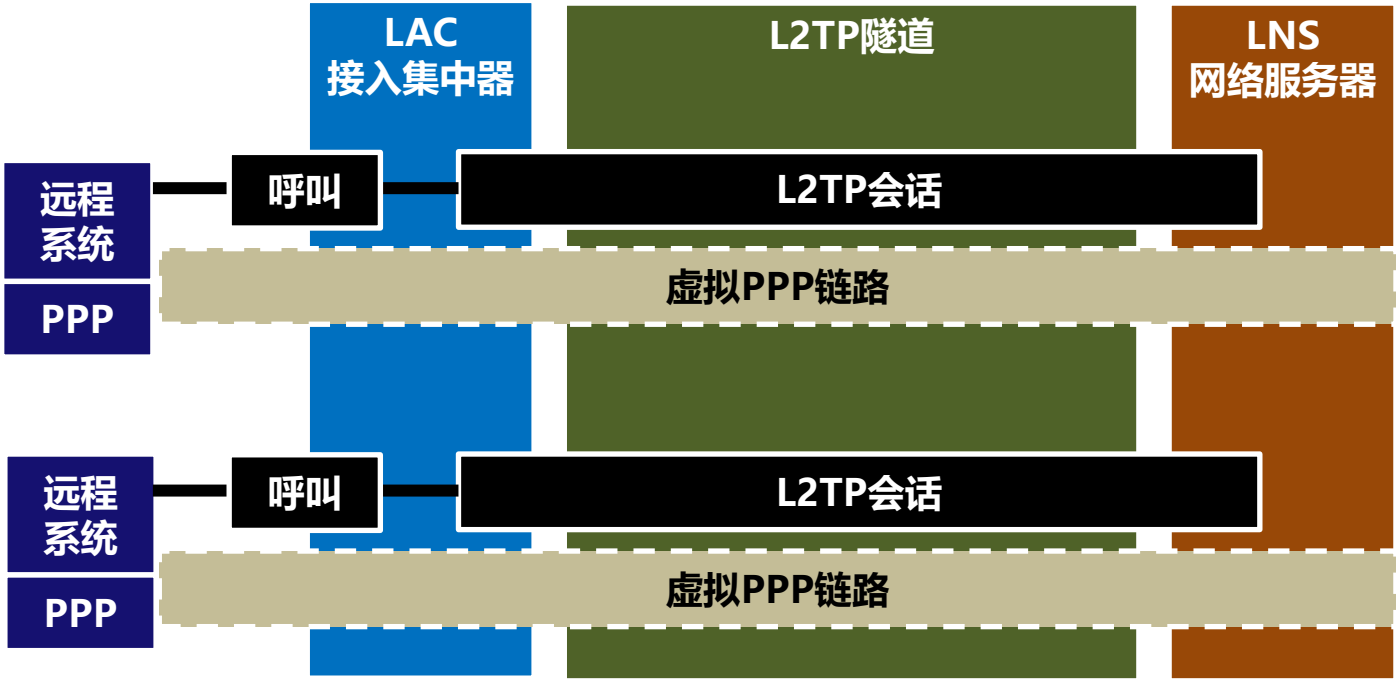
- L2TP协议层次结构
  - 除了IP网络，L2TP也支持ATM和帧中继（Frame Relay，FR）等多种网络类型。
  - 从TCP/IP协议族分层的角度，L2TP也属于应用层协议（会话层），使用端口1071。

L2TP协议架构

- L2TP工作在数据链路层，基于UDP，其报文分为数据消息和控制消息两类。
  - **数据消息**用投递PPP帧，该帧作为L2TP报文的数据区。L2TP不保证数据消息的可靠投递，若数据报文丢失，不予重传，不支持对数据消息的流量控制和拥塞控制。
  - **控制消息**用以建立、维护和终止控制连接及会话，L2TP确保其可靠投递，并支持对控制消息的流量控制和拥塞控制。

L2TP协议架构

- L2TP隧道、控制连接及会话之间的关系



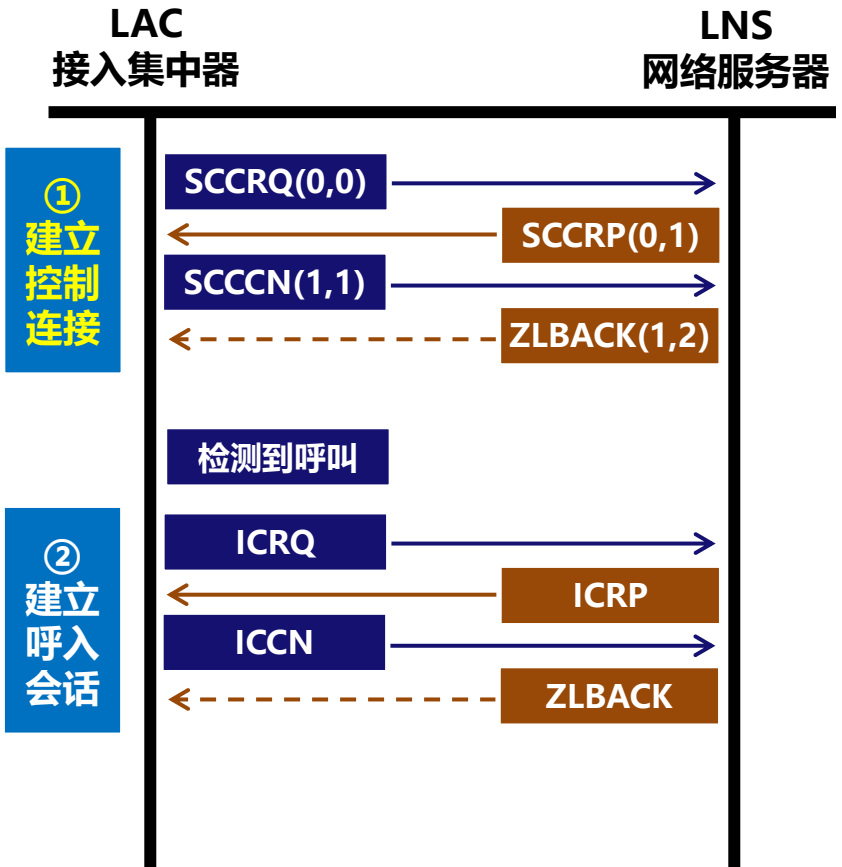
L2TP协议流程

- 一次完整的交互包括以下步骤：
  - 建立控制连接
  - 建立会话
  - 数据传输
  - 终止会话
  - 终止控制连接

- L2TP流程的每个步骤中都可能需要使用ZLBACK报文，表示Zero Length Body ACK，即实体长度为0的确认报文。

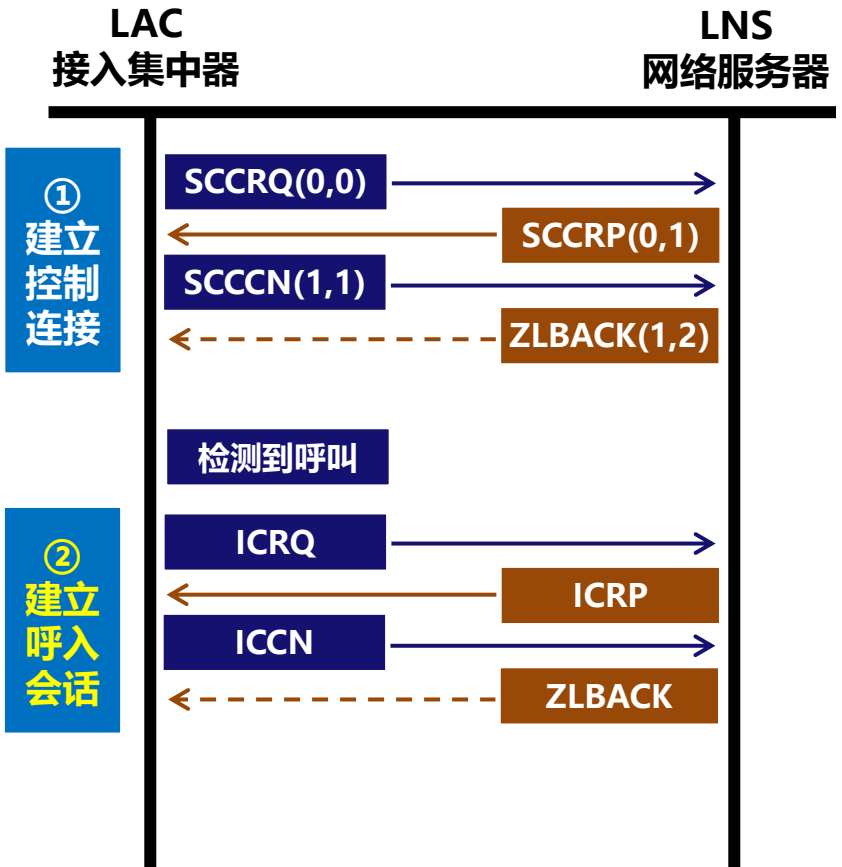
L2TP协议流程

- 建立控制连接SCC
  - 在建立控制连接阶段，LAC和LNS协商控制连接参数，并利用CHAP互相验证对方的身份。



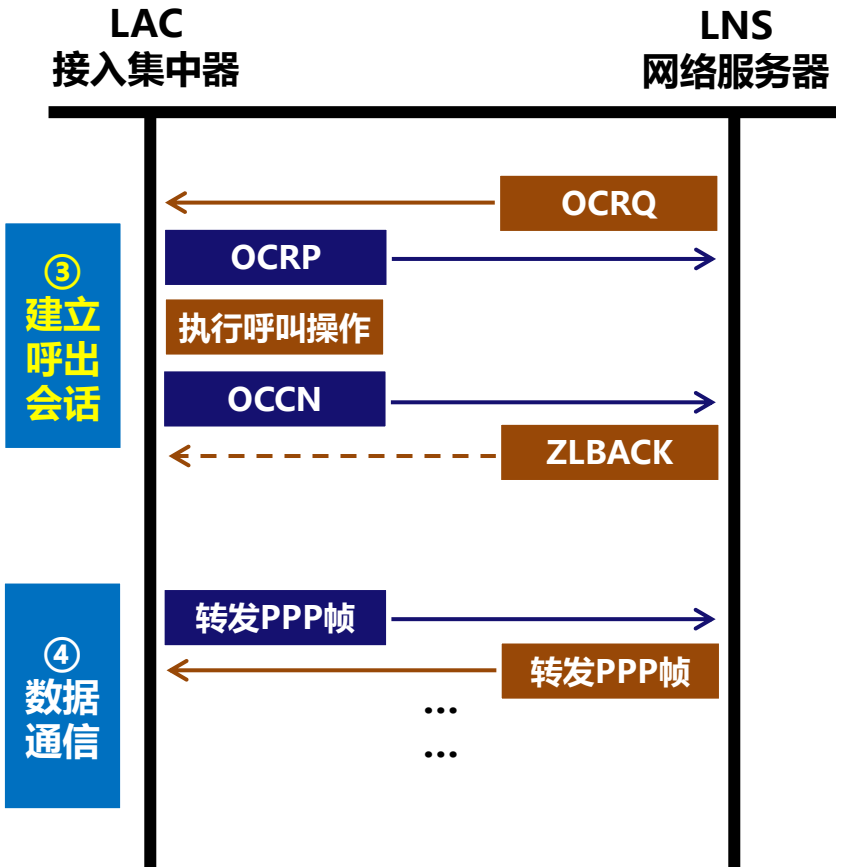
L2TP协议流程

- 建立呼入会话
  - 呼入：当LAC检测到来自远程客户的呼叫时，应向LNS建立呼入（Incoming Call，IC）会话。



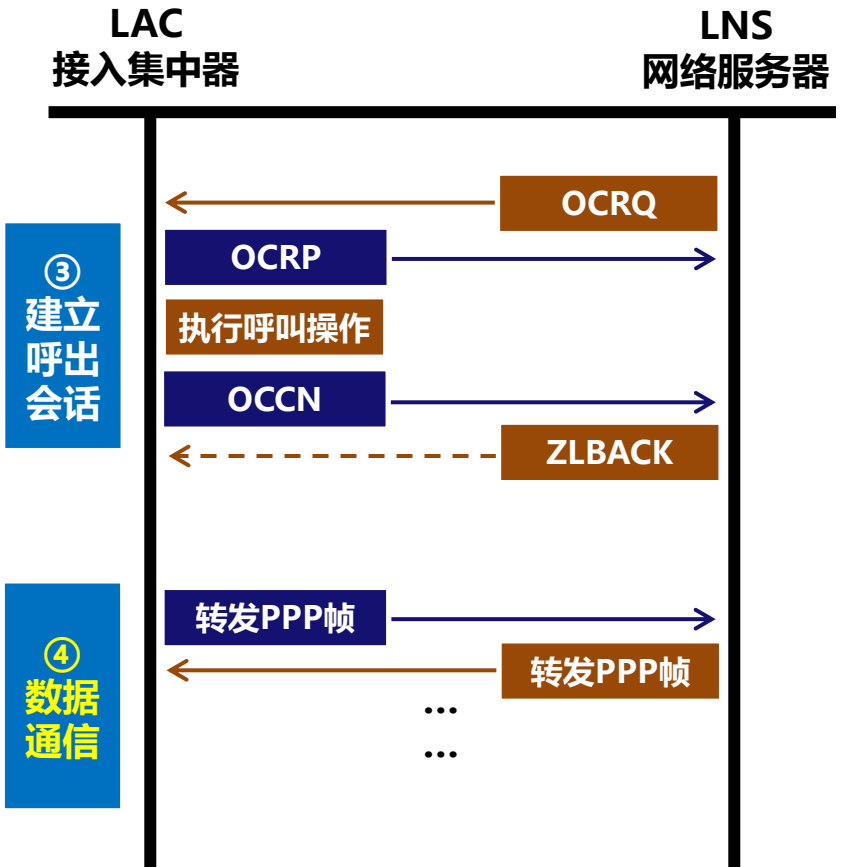
L2TP协议流程

- 建立呼出会话
  - 呼出：当收到来自LNS的会话建立请求时，应建立呼出（Outcoming Call，OC）会话。



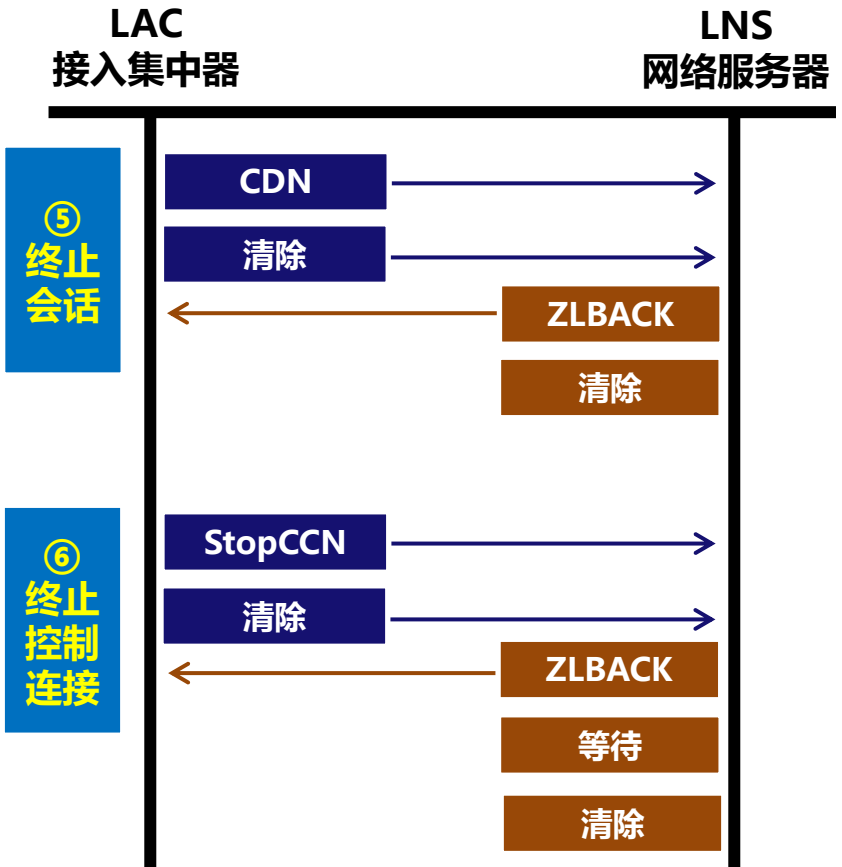
L2TP协议流程

- 数据通信
  - 呼出：当收到来自LNS的会话建立请求时，应建立呼出（Outcoming Call，OC）会话。



L2TP协议流程

- 终止会话
  - 终止会话前，发起方发送呼叫断连通告（Call Disconnect Notify，CDN）报文，
- 终止控制连接



二 L2TP协议流程

- L2TP其他附加功能：
  - 活动性检测
  - 会话参数更改
  - 错误通告
  - 代理认证
  - LCP配置请求转发

二 L2TP协议流程

- 可靠性机制，确保控制消息可靠投递
  - 每个报文都包含序号，从而为检测报文丢失和乱序提供了基础。
  - L2TP使用肯定确认防止报文丢失，即接收方收到报文后应发回确认；发送方若在一段时间之内没有收到确认，则重发报文。
  - L2TP使用滑动窗口技术来提高通信效率并进行流量控制。
  - L2TP使用慢启动策略防止拥塞。

提纲

一、L2TP协议

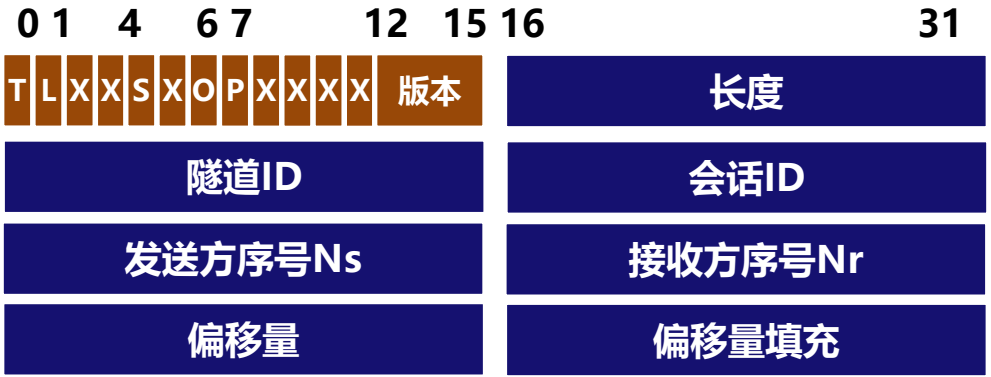
二、报文和安全性分析

三、L2TPv2和L2TPv3的区别

四、应用分析

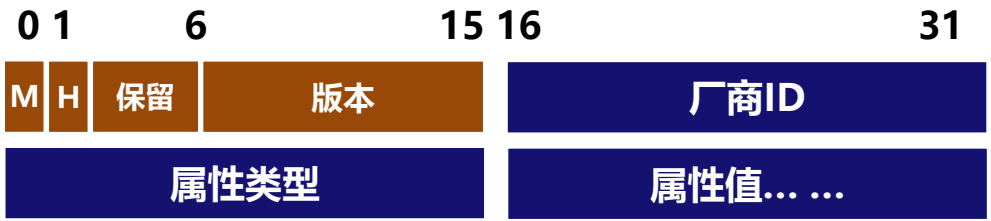
二 L2TP报文

- 报文首部
  - L2TP报文由首部和主体两部分构成。
  - 数据消息的主体部分是PPP帧，控制消息的主体部分则描述了控制报文类型，以及与报文类型相关的信息，这些信息都以属性值对（Attribute ValuePair，AVP)的形式出现。



二 L2TP报文

- 属性值对（Attribute Value Pair，AVP）
  - L2TP控制消息中所包含的所有信息都以AVP的形式存在，比如：SCCRQ报文中可能包含“消息类型AVP”，“成帧方法AVP”、“载波信号类型AVP”等。
  - 由于加密属性值需使用随机向量RV，所以每个包含隐藏AVP的L2TP报文中都应该包含“随机向量AVP”，且在所有隐藏AVP之前出现。多个隐藏AVP可共用同一RV，每个隐藏AVP都使用其前边最近的RV。

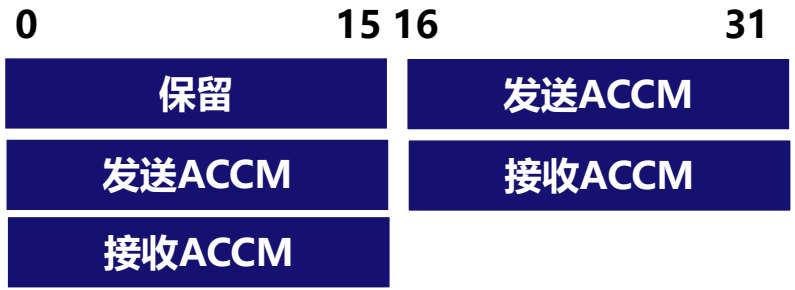


二 L2TP报文

- 呼叫错误AVP属性值格式
  - CRC错误
  - 成帧错误
  - 硬件越界
  - 缓冲区越界
  - 超时错误
  - 对齐错误

二 L2TP报文

- ACCM AVP属性值格式
  - “发送”表示供处理其发送的报文
  - “接收”表示供处理其接收的报文。



二 安全性分析

- L2TP不提供对PPP数据的机密性和完整性保护，若使用CHAP，则可体现端点身份认证的功能。CHAP依赖共享秘密，但L2TP并未讨论秘密的生成和更新方法。

- L2TP应被看作一个隧道协议，而有的技术人员将其称为“Safe Protocol”，而不是"Security Protocol”。从安全的角度考虑，L2TP应与IP或传输层的安全协议结合使用。

提纲

一、L2TP协议

二、报文和安全性分析

三、L2TPv2和L2TPv3的区别

四、应用分析

三 国际标准版本

- 2005年3月以RFC3931的形式公布了L2TPv3标准，L2TPv3较L2TPv2，支持除PPP协议之外的其他数据链路层协议，例如帧中继、以太网等。
  - 将涉及PPP的AVP，包括L2TP首部中与PPP相关部分剥离开来，这就使得其适用于更多的二层协议；
  - 将隧道ID和会话ID的长度由2B拓展到4B，增大了命名空间，也增大了攻击者进行密码破解的难度；
  - 将认证机制拓展到整个控制消息而不是其中的一部分，提升了安全性。

提纲

一、L2TP协议

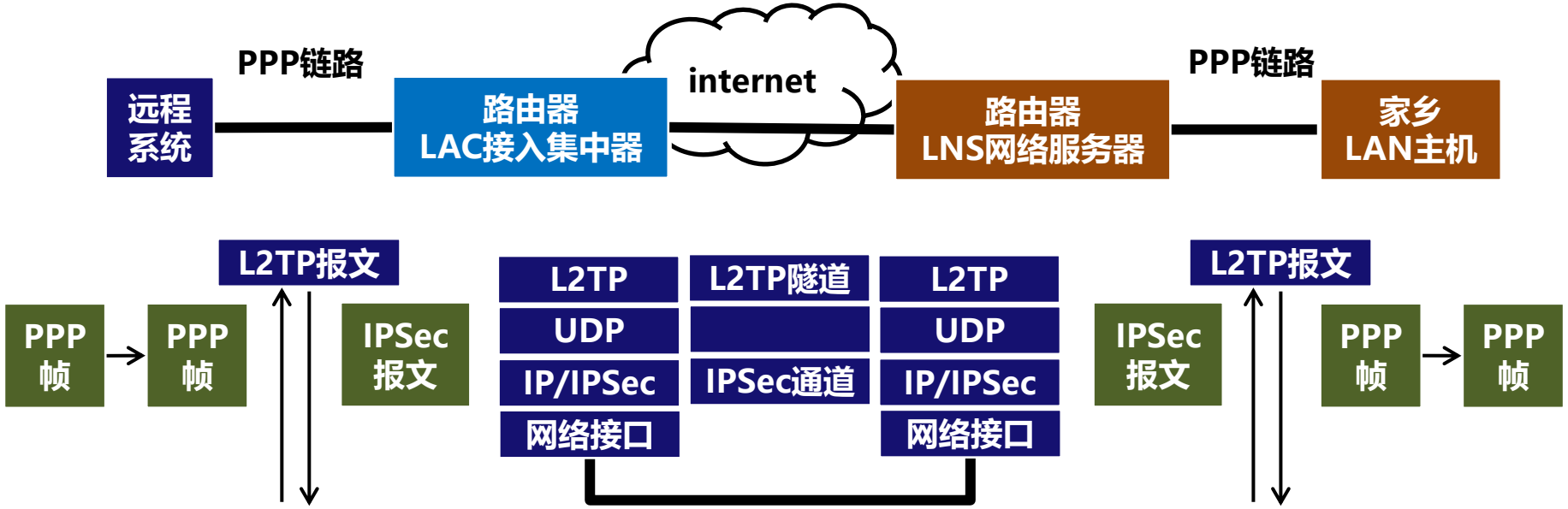
二、报文和安全性分析

三、L2TPv2和L2TPv3的区别

四、应用分析

四 应用

- 在路由器上部署L2TP/IPSec的案例



四 小结

- L2TP对PPP进行了扩展，它允许PPP链路端点跨越多个IP、ATM或帧中继网络。
- L2TP协议流程包括建立控制连接（隧道）、建立会话、数据通信、终止会话和终止控制连接等步骤。此外，它还定义了活动性检测、可靠性机制、代理认证等功能。
- L2TP不是一个严格意义上的安全协议，但其使用的CHAP具备安全协议的特征。

办公地点：理科大楼B1715

联系方式：17621203829

邮箱：liuhongler@foxmail.com