引入

- AAA是认证、授权、计费的简称
- AAA是一个综合的安全架构
- 与其他安全技术配合使用，提升网络和设备的安全性
- 常用AAA协议有RADIUS和TACACS+

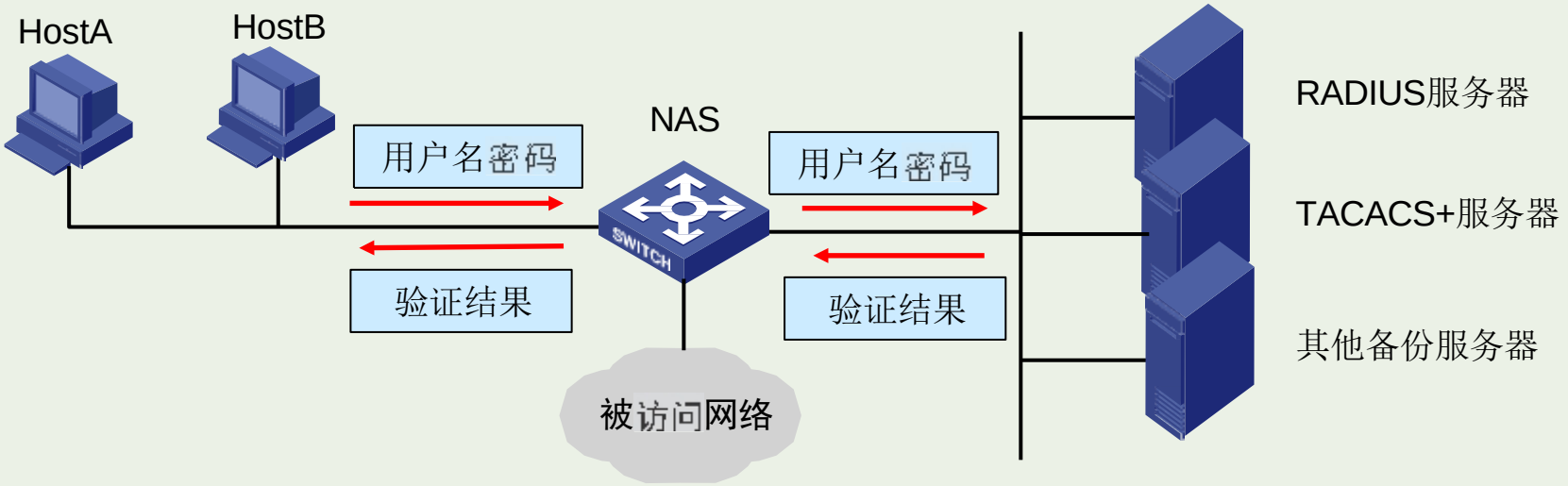
课程目标

学习完本课程，您应该能够：

- 掌握AAA认证架构
- 掌握RADIUS、TACACS+认证原理
- 熟悉AAA、RADIUS和HWTACACS相关配置命令

- AAA架构
- RADIUS协议
- TACACS+协议

AAA基本结构



- **AAA包含三种功能：认证、授权、计费**

  常用RADIUS协议和TACACS+协议

  使用远程服务器，或交换机设备本身作本地认证服务器

AAA支持的服务

- AAA通过对服务器的详细配置，对多种服务提供安全保证

  支持FTP、TELNET、PPP、端口接入

- 验证动作包含核对用户名、密码、证书
- 授权表现为下发用户权限、访问 、用户级别等
- 计费表现为记录用户上网流量、时长等

配置AAA

- **AAA认证方案：配置本地认证或远程认证方案**

  远程认证需要配置RADIUS方案或TACACS+方案

- **AAA实现方法：在ISP域中引用已经配置的AAA方案**

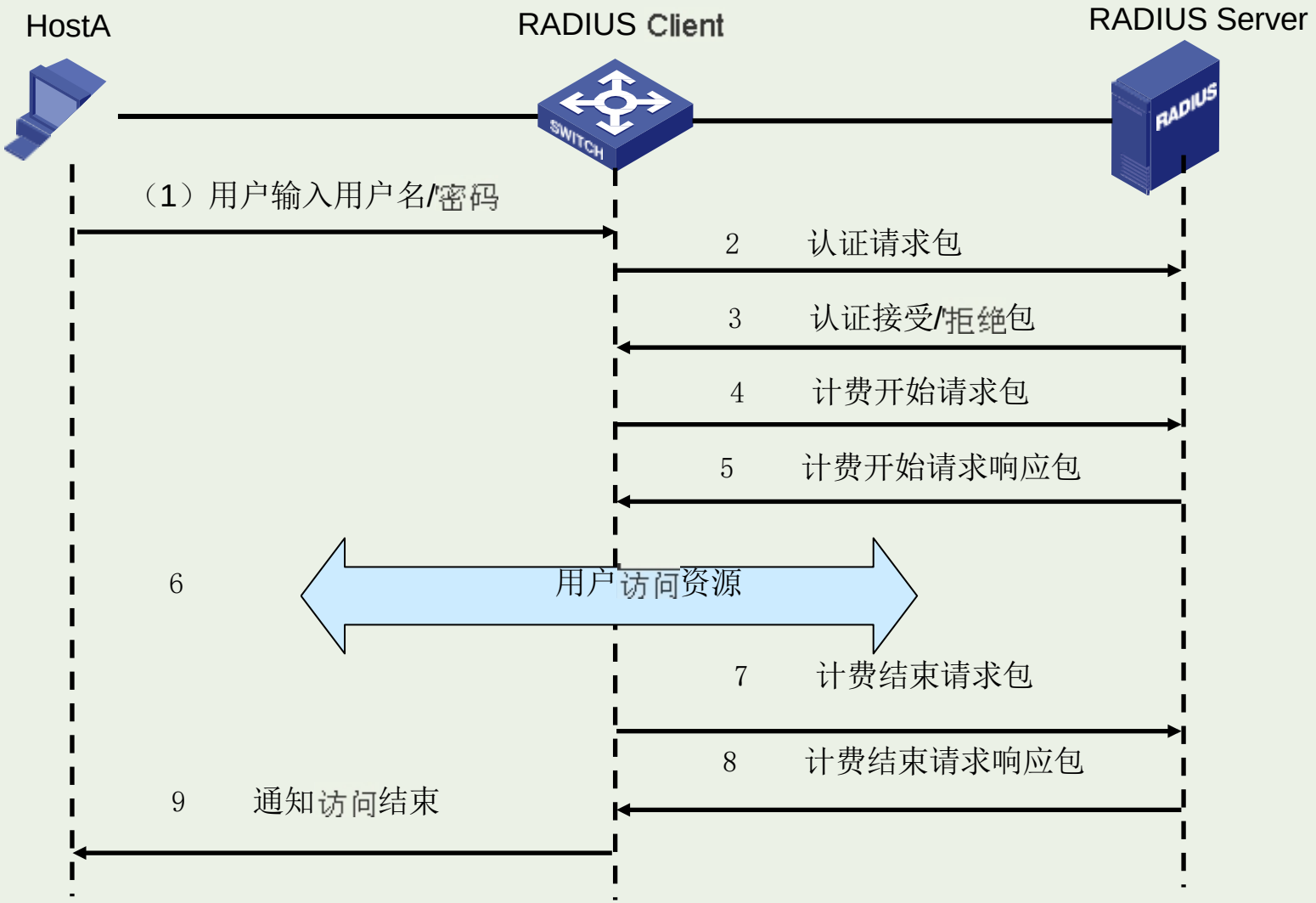
[sysname-isp-ispname] authentication default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

- AAA架构
- RADIUS协议
- TACACS+协议

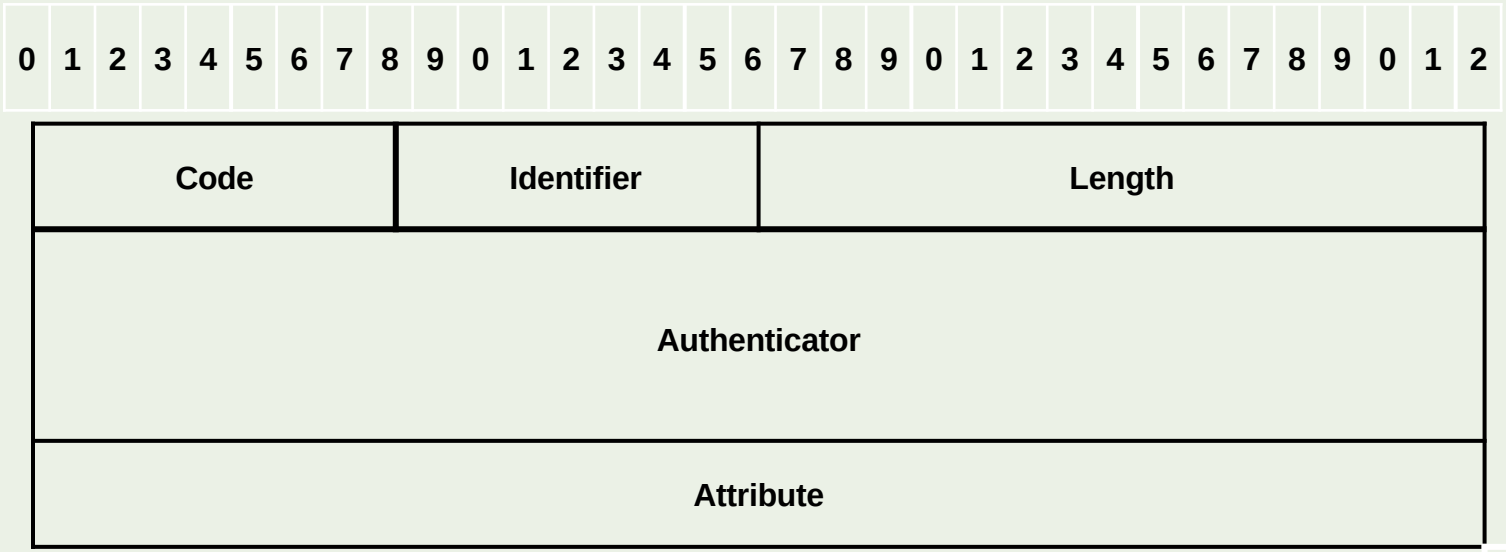
RADIUS协议概述

- RADIUS（Remote Authentication Dial-In User Service，远程认证拨号系统）是分布式的交互协议
- 客户端/服务器结构
- 基于UDP传输，　　、　　端口
- 共享密钥、多种认证方式
- TLV结构，利于扩展

RADIUS消息交互流程



RADIUS报文结构



- **Code字段决定报文类型**

  值为1、2、3表示认证报文

  值为4、5表示计费报文

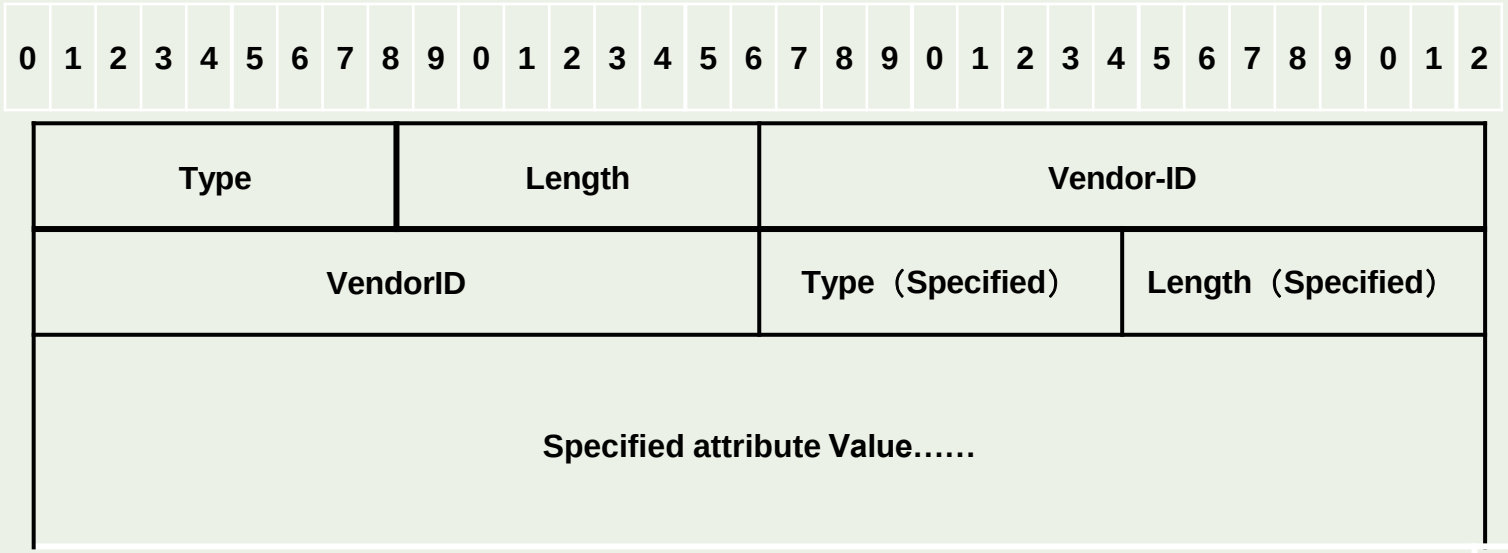
RADIUS属性

- Attribute字段携带认证、授权、计费信息
- 采用（Type，Length，Value）三元组格式
- 常用属性

编号	属性名称	编号	属性名称
1	User-Name	11	Filter-ID
2	User-Password	15	Login-Service
4	NAS-IP-Address	26	Vendor-Specific
8	Framed-IP-Address	31	Calling-Station-ID

RADIUS扩展属性

- RADIUS协议中26号属性用于扩展



RADIUS配置

- 创建RADIUS方案

[sysname] radius scheme *radius-scheme-name*

- 配置RADIUS主认证授权、计费服务器

[sysname-radius-name] {primary|secondary} { **accounting | authentication** } *ip-address* [*port-number*]

- 配置RADIUS共享密钥

[sysname-radius-name] key { **authentication | accounting** } *string*