



STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

北京邮电大学
BEIJING UNIVERSITY OF
POSTS AND
TELECOMMUNICATIONS




网络协议分析与实现
第三章典型通信协议分析
Radius协议



徐鹏

STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK


主要内容



- AAA综述
 - 为什么AAA?
 - 通用AAA体系结构
- Radius协议分析

STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

AAA综述



- 认证(Authentication)
 - 用户在使用网络系统中的资源时**对用户身份的确认**
- 授权(Authorization)
 - 网络系统**授权用户以特定的方式使用其资源**
- 计费(Accounting)
 - 网络系统收集、记录用户对网络资源的使用，以便**向用户收取资源使用费用或者用于审计等目的**

STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

AAA综述 (为什么要AAA?)

• 电信网是可运营、可管理和可赢利的网络

提供多种服务, 并收取不同费用

计费

不同服务费用不同 价格

不同用户使用不同的服务 鉴权

向谁收费?

谁是谁?

认证

STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

AAA综述 (相关研究)

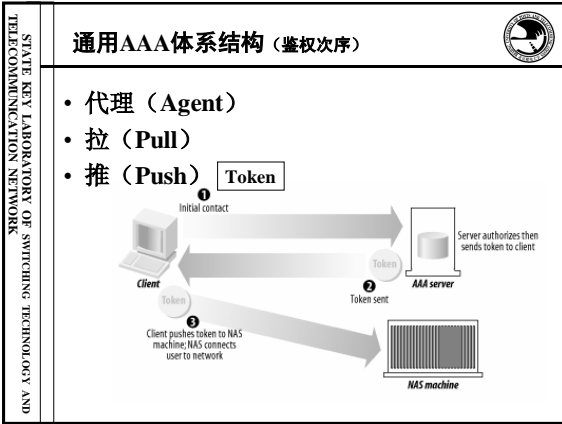
- IETF AAA工作组
 - 研究重点转移到移动IP和NAS,
- IETF AAArch研究组
- 相关规范
 - 4篇RFC
 - 2篇: AAA的Mobile IPv4应用
 - 1篇: AAA Transport Profile
 - 1篇: Diameter基础协议
 - 2篇尚处于实验阶段
 - 基于策略的AAA计费
 - AAA通用体系框架
 - 其余处于报告阶段
 - 认证需求、
 - 认证框架、
 - 认证应用举例
 - IP网络移动业务AAA需求

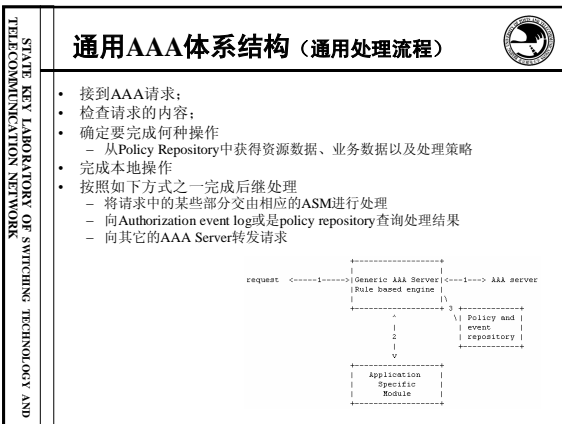
由应用推进规范化的典型

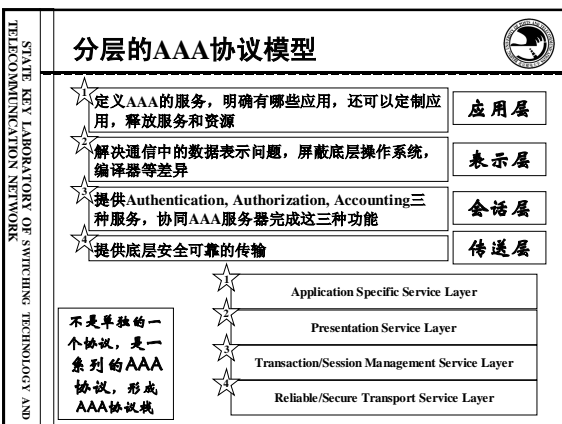
STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

通用AAA体系结构 (RFC2903: Generic AAA Architecture)

- 通用AAA体系结构的构成
 - **Authorization Rule Evaluation**
 - Generic Information
 - ASI (Application Specific Information)
 - ASI → boolean or numerical values
 - **Application Specific Module (ASM)**
 - 管理业务相关资源
 - 提供业务相关数据
 - 完成某些业务相关的功能
 - **Authorization Event Log**
 - **Policy Repository**
 - 数据库
 - 维护可用业务和资源
 - 维护处理请求的规则
 - **Request Forwarding**







STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

Radius综述

- Radius的演进
 - 创立于**1966**年Merit Network, Inc.是密执安大学的一家非营利公司，其业务是**运行维护该校的网络互联MichNet**。1987年，Merit在美国NSF（国家科学基金会）的招标中胜出，赢得了NSFnet（即Internet前身）的运营合同。因为NSFnet是基于IP的网络，而MichNet却基于专有网络协议，Merit面对着如何将MichNet的专有网络协议演变为IP协议，同时也要把MichNet上的大量拨号业务以及其相关专有协议移植到IP网络上。
 - 1991**年，Merit决定招标拨号服务器供应商，几个月后，一家叫Livingston的公司提出了建议，冠名为RADIUS，并为此获得了合同。
 - 1992**年秋天，IETF的NASREQ工作组成立。随之提交了RADIUS作为草案。很快，RADIUS成为事实上的网络接入标准，几乎所有的网络接入服务器厂商均实现了该协议。
 - 1997**年1月，RFC 2058/2059发表
 - 1997**年4月，RFC 2138/2139发表
 - 2000**年6月，RFC 2865/2866发表（当前最新的RADIUS RFC）

STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

Radius综述

- Radius
 - Remote Access Dial-in User Service
 - 设计初衷
 - 是对远程拨号用户访问进行认证
 - 采用Client/Server模型
 - 在NAS（Network Access Server）上运行的是Client端，负责将用户信息传送到指定的Radius服务器上，并根据服务器返回的结果进行相应的处理

```

graph LR
    User[用户] -- Request --> NAS[NAS (Radius Client)]
    NAS -- Request --> AAA[AAA Server (Radius Server)]
    AAA -- Response --> NAS
    NAS -- Response --> User
  
```

STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

Radius综述

- Radius服务器包括两种类型
 - 授权认证服务器
 - 接收用户的连接请求、验证用户身份，并返回给客户需要的相关配置信息
 - 授权认证服务器也可以作为Radius客户的代理，将其连接到另一个授权认证服务器
 - 计费服务器
 - 接受用户计费开始请求和计费结束请求，并实现计费功能


```

graph LR
    User[用户] -- Request --> NAS[NAS (Radius Client)]
    NAS -- Request --> AAA1[AAA Server (Radius Server)]
    AAA1 -- Response --> NAS
    NAS -- Response --> User
    AAA1 -- Request --> AAA2[AAA Server (Radius Server)]
    AAA2 -- Response --> AAA1
  
```

STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

Radius综述

- RFC 2058/2138/2865
 - “Remote Authentication Dial In User Service (RADIUS)”
 - 消息包格式, 消息类型和一些属性(Attribute)
- RFC 2059/2139/2866
 - “RADIUS Accounting”
 - 用于计费的消息类型和属性值



STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

Radius协议特性

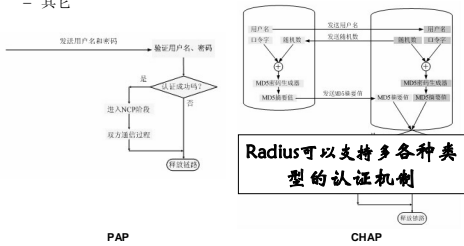
- 网络安全
 - 公钥
 - Transactions between the client and RADIUS server
 - 加密
 - User Passwords
- 扩展性
 - 所有的Transaction均由可变长度的三元组 (3-tuples) 组成
 - 属性-长度-值 (Attrib

对Radius应用的扩展就是增加针对不同应用的三元组的过程

STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

Radius协议特性


- 认证机制
 - PAP (Password Authentication Protocol)
 - CHAP (Challenge Handshake Authentication Protocol)
 - 其它



Radius可以支持多各种类型的认证机制

STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

Radius协议（消息格式）




- Code
 - 1: Access-Request
 - 2: Access-Accept
 - 3: Access-Reject
 - 4: Accounting-Request
 - 5: Accounting-Response
 - 11: Access-Challenge
 - 12: Status-Server (experimental)
 - 13: Status-Client (experimental)
 - 255: Reserved

Code	Identifier	Length
Authenticator		
Attribute		

STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

Radius协议（消息格式）




- Identifier
 - 用于匹配请求包和响应包，随着Attribute域改变、接收到有效响应包而不断变化，而在重传时保持不变。
- Authenticator（16字节）
 - 用于验证RADIUS服务器传输回来的请求，同时用于密码隐藏算法上
 - Request Authenticator
 - 16字节的随机码
 - Response Authenticator
 - 对Code、Identifier、Request Authenticator、Length、Attribute和共享密钥进行MD5算法后的结果。

Code	Identifier	Length
Authenticator		
Attribute		

STATE KEY LABORATORY OF SWITCHING TECHNOLOGY AND TELECOMMUNICATION NETWORK

Radius协议（消息类型）



1: Access_Request

- Attribute域改变则改变；
- 收到相应的有效的Response则改变

Code	Identifier	Length
Request Authenticator		
Attribute		

Request Authenticator
• 每次都改变

2: Access_Accept

- 携带相应Request的identifier

Code	Identifier	Length
Response Authenticator		
Attribute		

Response Authenticator
• 由Request Authenticator中的信息计算得出

RFC 2865: Remote Authentication Dial In User Service (RADIUS)
