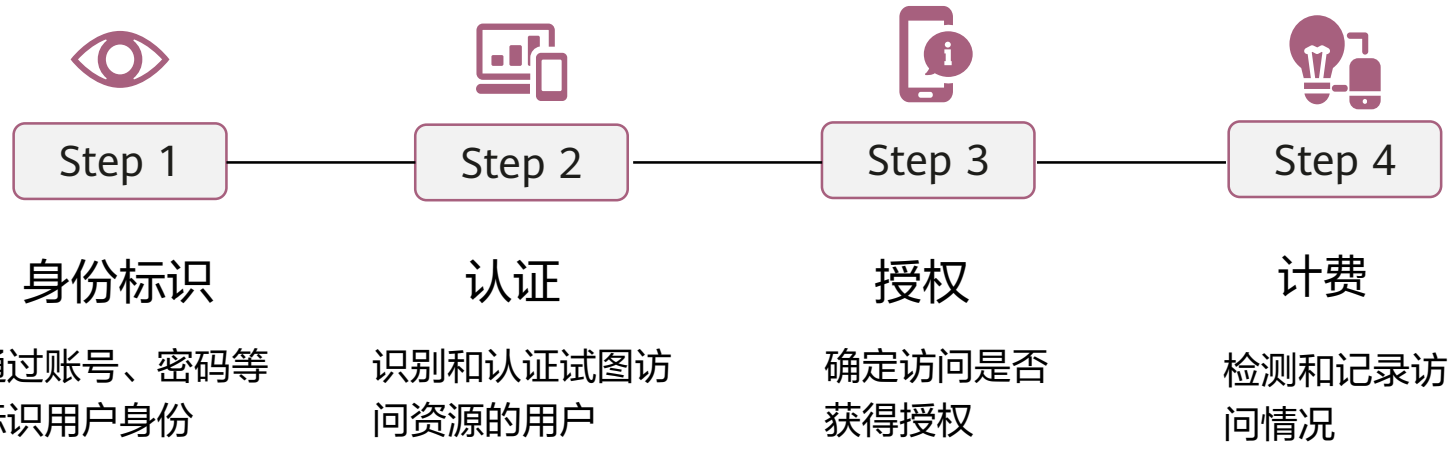
AAA原理与配置

主讲人：鲍婷婷

目录

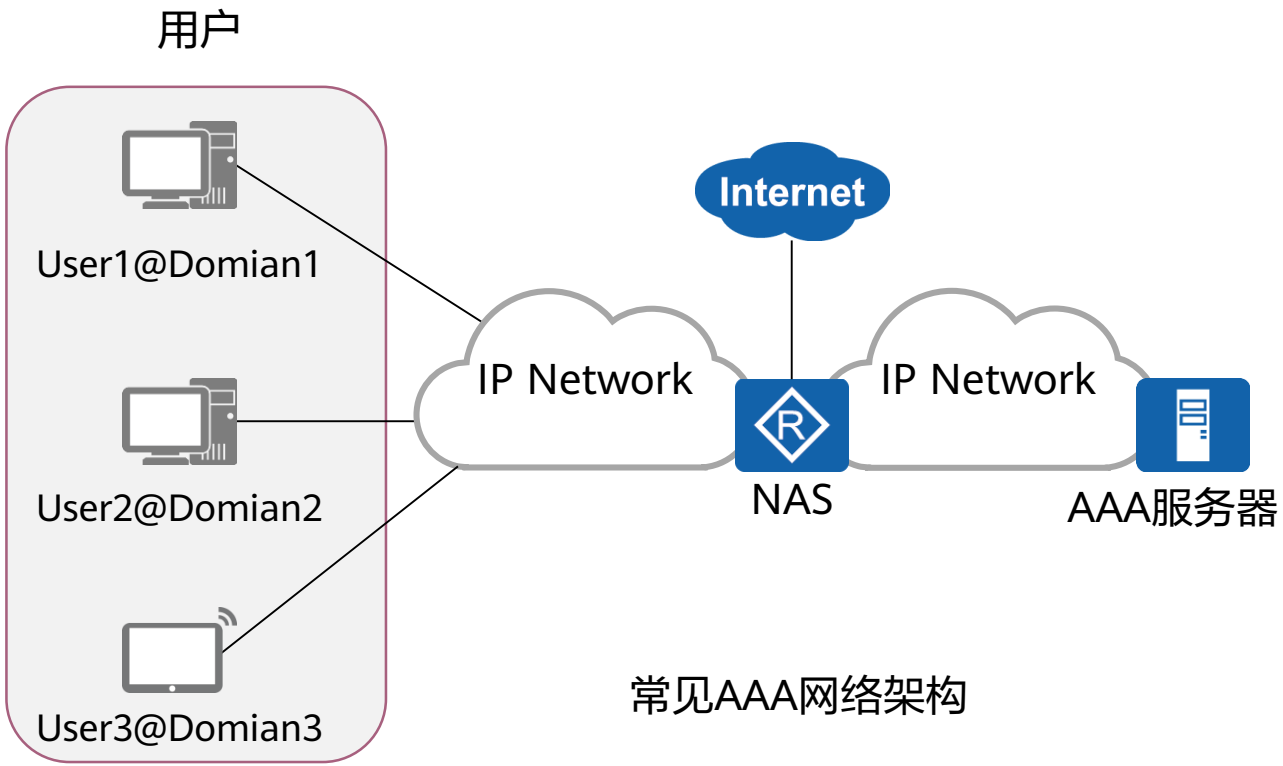
AAA基本概念

- AAA是Authentication（认证）、Authorization（授权）和Accounting（计费）的简称，是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。



AAA常见架构

- AAA常见网络架构中包括用户、NAS（Network Access Server）、AAA服务器（AAA Server）。

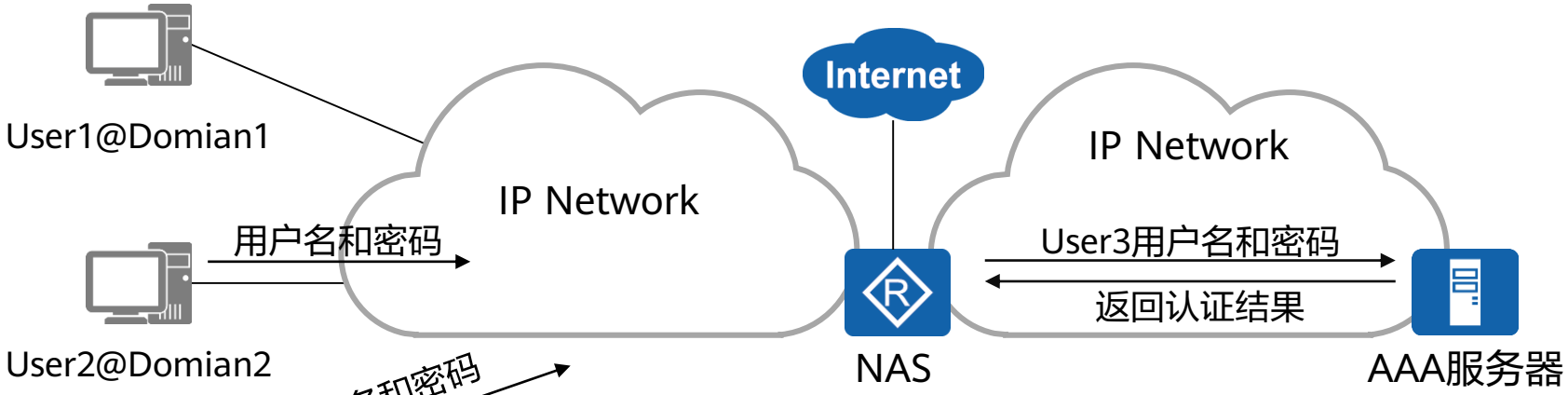


常见AAA网络架构

- NAS负责集中收集和管理用户的访问请求。
- 在NAS上会创建多个域来管理用户。不同的域可以关联不同的AAA方案。AAA方案包含认证方案，授权方案，计费方案。
- 当收到用户接入网络的请求时，NAS会根据用户名来判断用户所在的域，根据该域对应的AAA方案对用户进行管控。

认证（Authentication）

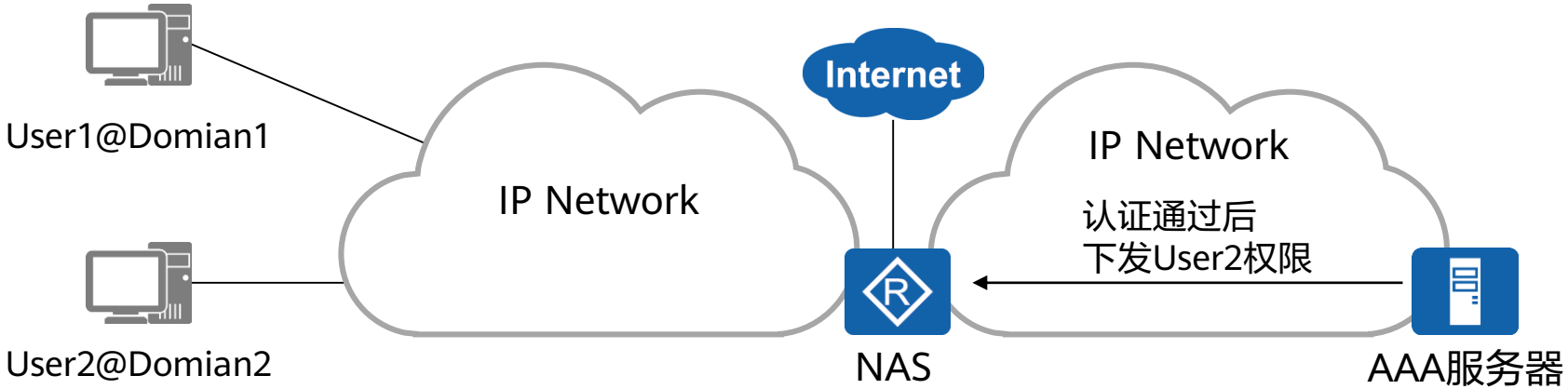
- AAA支持的认证方式有：不认证，本地认证，远端认证。



用户	域	认证方式
User1@Domian1	Domain1	不认证
User2@Domian2	Domain2	本地认证
User3@Domian3	Domain3	远端认证

授权（Authorization）

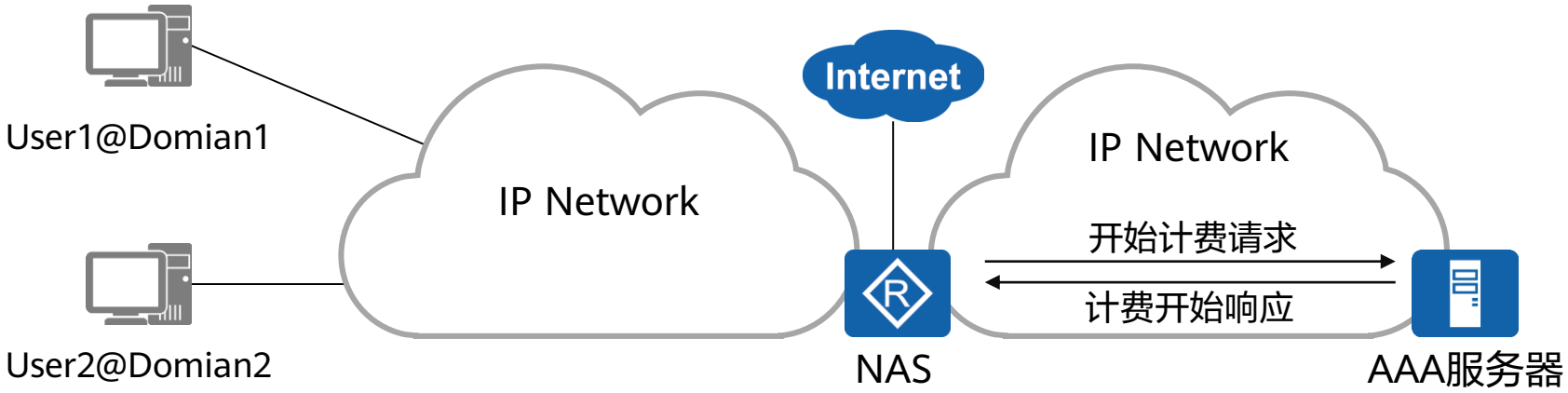
- AAA支持的授权方式有：不授权，本地授权，远端授权。
- 授权信息包括：所属用户组、所属VLAN、ACL编号等。



用户	域	授权方式	授权内容
User1@Domian1	Domain1	不授权	无
User2@Domian2	Domain2	本地授权	可以访问Internet
User3@Domian3	Domain3	远端授权	由远端服务器授权

计费（Accouting）

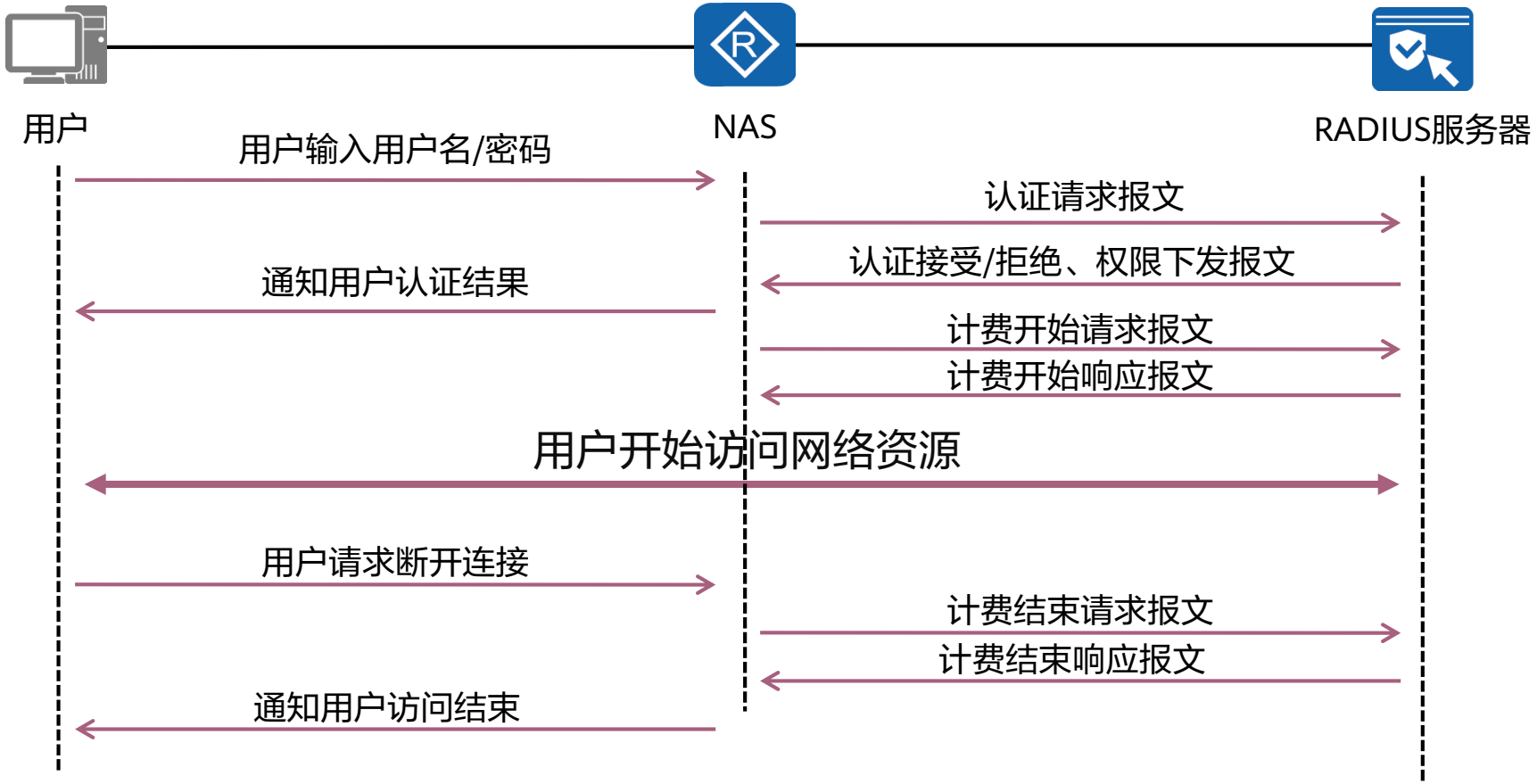
- 计费功能用于监控授权用户的网络行为和网络资源的使用情况。
- AAA支持的计费方式有：不计费，远端计费。



用户	域	计费方式
User1@Domian1	Domain1	不计费
User2@Domian2	Domain2	不计费
User3@Domian3	Domain3	远端计费

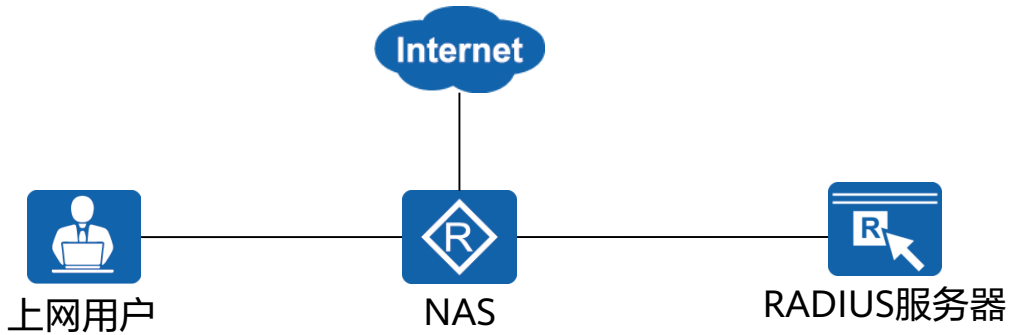
AAA实现协议 - RADIUS

- AAA可以用多种协议来实现，最常用的是RADIUS协议。



AAA常见应用场景

通过RADIUS提供上网用户的AAA



对管理用户进行本地认证和授权

目录

AAA配置 (1)

1. 进入AAA视图

```
[Huawei] aaa
```

从系统视图进入AAA视图进行配置

2. 创建认证方案

```
[Huawei-aaa] authentication-scheme authentication-scheme-name
```

创建认证方案并进入相应的认证方案视图

```
[Huawei-aaa-authentication-scheme-name] authentication-mode { hwtacacs | local | radius }
```

配置认证方式，local指定认证方式为本地认证。缺省情况下，认证方式为本地认证。

AAA配置 (2)

3. 创建domain并绑定认证方案

[Huawei-aaa] **domain** *domain-name*

创建domain并进入相应的domain视图

[Huawei-aaa-domain-name] **authentication-scheme** *authentication-scheme-name*

在相应的domain视图下绑定认证方案

4. 创建用户

[Huawei-aaa] **local-user** *user-name* **password cipher** *password*

创建本地用户，并配置本地用户的密码：

- 如果用户名中带域名分隔符，如@，则认为@前面的部分是用户名，后面部分是域名
- 如果没有@，则整个字符串为用户名，域为默认域

AAA配置 (3)

5. 配置用户接入类型

```
[Huawei-aaa] local-user user-name service-type { { terminal | telnet | ftp | ssh | snmp | http } | ppp | none }
```

设置本地用户的接入类型。缺省情况下，本地用户关闭所有的接入类型。

6. 配置用户级别

```
[Huawei-aaa] local-user user-name privilege level level
```

指定本地用户的权限级别。

AAA配置案例

- 在设备R1上配置用户密码和级别，使主机A可以通过配置的用户名和密码远程登录到设备。


```
[R1]aaa
[R1-aaa]local-user huawei password cipher huawei123
[R1-aaa]local-user huawei service-type telnet
[R1-aaa]local-user huawei privilege level 0
[R1]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode aaa
```

配置验证（1）

- AAA中，每个域都会与相应的认证授权和计费方案相关联，当前为默认域。

```
[R1]display domain name default_admin
  Domain-name:                  default_admin
  Domain-state:                 Active
  Authentication-scheme-name:   default
  Accounting-scheme-name:       default
  Authorization-scheme-name:    -
  Service-scheme-name:          -
  RADIUS-server-template:       -
  HWTACACS-server-template:     -
  User-group:                   -
```

配置验证 (2)

- 用户正常登录并且下线之后可以看到用户的记录信息。

```
[R1]display aaa offline-record all
  ------------------------------------------------------------------
  User name:              huawei
  Domain name:            default_admin
  User MAC:               00e0-fc12-3456
  User access type:       telnet
  User IP address:        10.1.1.2
  User ID:                1
  User login time:        2019/12/28 17:59:10
  User offline time:      2019/12/28 18:00:04
  User offline reason:    user request to offline
```

本章总结

- AAA技术为了提高企业网络的安全性，防止非法用户登录，需要对企业内部员工，外部客户等进行身份的认证，可访问资源的授权和上网为行为的监控。
  - 认证（Authentication）
  - 授权（Authorization）
  - 计费（Accounting）
- AAA技术可以本地实现，也可以通过远端服务器实现。
- AAA可以用多种协议来实现，最常用的是RADIUS协议。