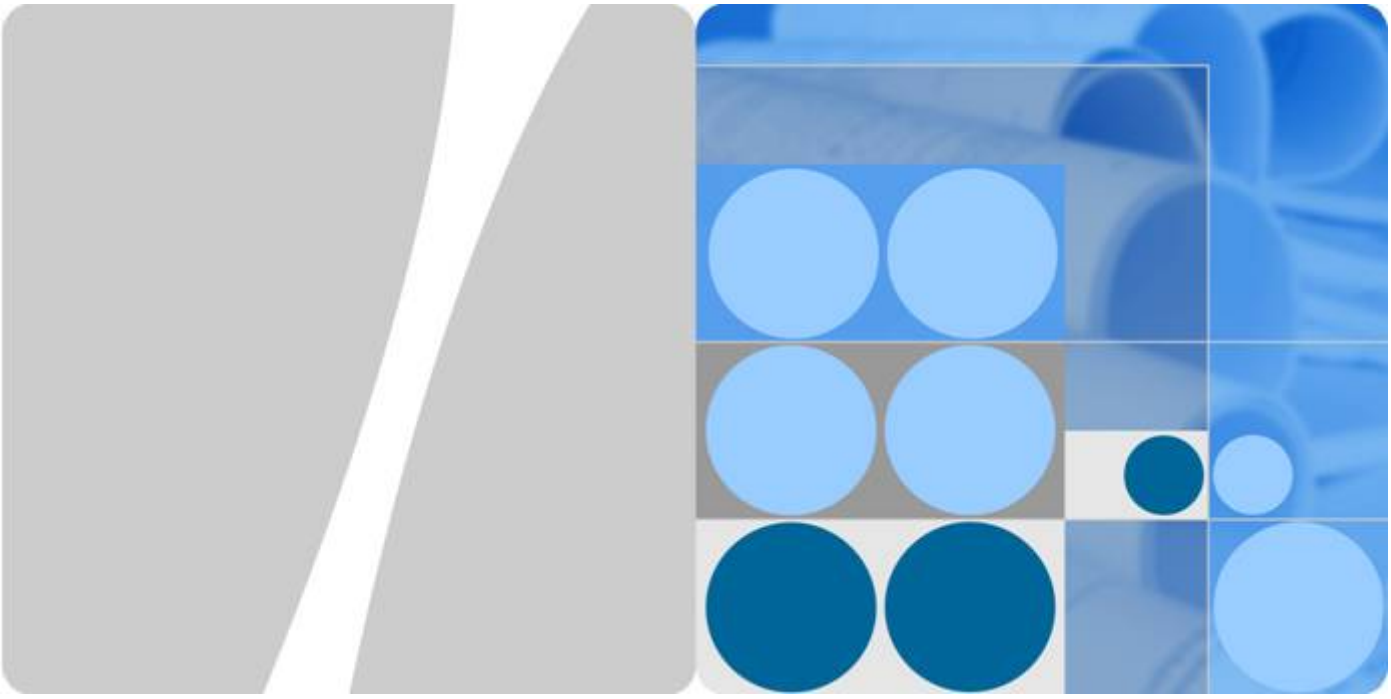


用户组策略

技术白皮书

文档版本　01

发布日期　2012-10-31

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://enterprise.huawei.com

客户服务邮箱： ChinaEnterprise_TAC@huawei.com

客户服务电话： 4008229999

前 言

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2012-10-31)

第一次正式发布。

目 录

1 介绍

定义

用户组包括 ACL 规则、Qos-profile、组间组内隔离等，RADIUS 通过将用户授权到用户组，以确定该用户权限。

目的

随着网络技术的应用与发展，人们对信息网络的应用需求不断提升，对网络的依赖性也越强，伴随而来的信息安全威胁也在不断增加。网络安全已经超过对网络可靠性、交换能力和服务质量的需求，成为企业用户最关心的问题，网络安全基础设施也日渐成为企业网建设的重中之重。

网络准入控制（NAC）方案从控制用户终端安全接入网络的角度入手，通过用户端、准入控制组件、网络设备（交换机、路由器、防火墙、无线）以及第三方软件（杀毒软件、补丁服务器）的联动，对接入网络的用户终端强制实施安全策略，严格控制终端用户的网络使用行为，有效加强用户终端的主动防御能力，为网络管理人员提供有效、易用的管理工具和手段。

用户组属于 NAC 技术的一种，实际应用场景中接入的用户数量虽多，但是用户类别是很有限的，一般部署场景下，能支持 5-8 类用户即可。通过在用户组下配置不同的控制规则，服务器授权用户到不同的组别，从而对各类型的用户实现访问权限的控制。

2 原理描述

用户组基本概念

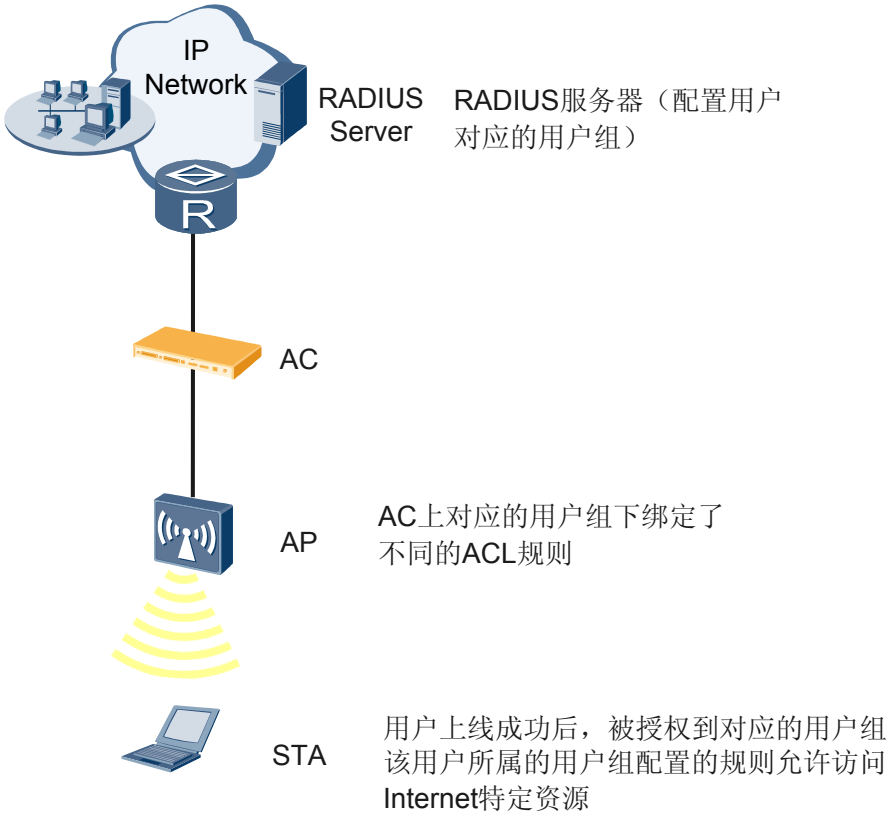
- 用户组：在整个网络中，各个访问网络的用户的权限可能是各不相同的，可以将具有相同权限的用户划为一组，即一个 UserGroup。这样，可以减少 AC 的负担，也就是说，只要对这个用户组赋予一定的权力，那么该组内的用户就具有相同的权力。
- ACL：访问控制列表(Access Control List，ACL)，可以过滤网络中的流量，是控制访问的一种网络技术手段。
- QoS：服务质量保证(Quality of Service)，对用户带宽，报文优先级等进行定义。
- 隔离：包括组间隔离和组内隔离，对用户组内、组间的用户互访进行控制。

用户组下发 ACL 的基本原理

WLAN 用户上线后，为了满足用户访问特定的某些网络资源，需要对用户进行动态授权。

用户组下发 ACL 是指用户认证成功后，RADIUS 服务器下发用户分组，将用户进行分类，每个用户分组可以关联对应的 ACL 规则，通过用户分组和 ACL 规则的关联，实现对每类用户进行 ACL 授权信息控制，即同类用户采用同样的授权信息。

图 2-1 用户组下发 ACL 的基本原理



用户组下发 ACL 原理如下：

1. 用户认证成功后，RADIUS 服务器通过回应授权信息，将该用户授权到对应的用户组。
2. AC 获取 RADIUS 服务器回应报文中的的 UserGroup。
3. AC 将该 UserGroup 下绑定的 ACL 下发给 AP。
4. 用户上线成功后访问网络时，由 AP 与 AC 共同实现对用户权限的控制。
5. 如果 RADIUS 服务器未下发任何 ACL，则意味着不限制用户任何访问权限，即用户默认权限为可以访问任何网络资源。如果要控制用户访问权限，则 RADIUS 服务器必须下发 ACL。

用户组下可以绑定 ACL 规则，基本配置如下：

```
<Quidway> system-view
[Quidway] acl 3001
[Quidway-acl-adv-3001] rule 5 deny ip destination 108.1.1.1 0
[Quidway-acl-adv-3001] quit
[Quidway] user-group test
[Quidway-user-group-test] acl-id 3001
[Quidway-user-group-test] quit
```

用户组下发 Qos-profile 基本原理

用户组通过绑定一个 QoS 模板，对用户组内的用户的带宽进行限速。

用户 QoS 原理如下：

1. 用户认证成功后，RADIUS 服务器通过回应授权信息，将该用户授权到对应的用户组。
2. AC 获取 RADIUS 服务器回应报文中的的 UserGroup。
3. AC 将该 UserGroup 下 Qos-profile 所配置的限速值和用户优先级下发给 AP。
4. 用户上线成功后访问网络，由 AP 与 AC 共同实现对用户带宽和优先级的控制。

用户组下可以绑定 Qos-profile，其基本的配置如下：

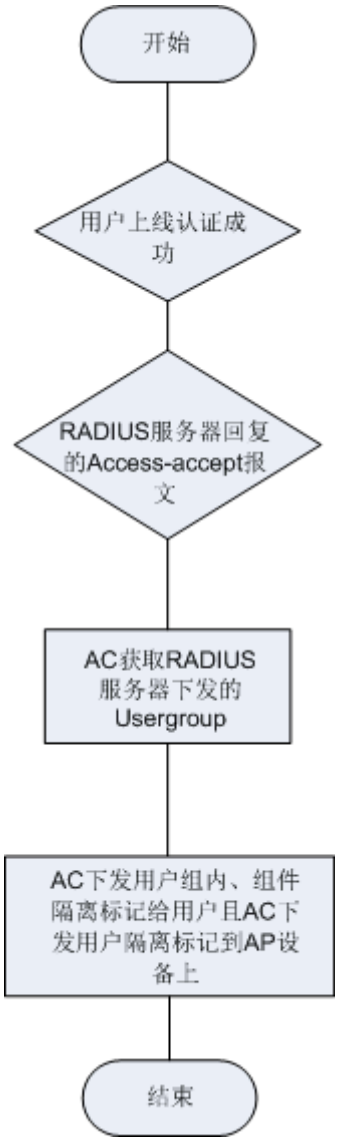
```
<Quidway> system-view
[Quidway] qos-profile name test
[Quidway-qosprofile-test] car inbound cir 10000
[Quidway-qosprofile-test] car outbound cir 10000
[Quidway-qosprofile-test] quit
[Quidway] user-group test
[Quidway-user-group-test] qos-profile test
[Quidway-user-group-test] quit
```

用户组下发用户隔离基本原理

为了对用户互访权限进行控制，可以在用户组内配置隔离标记，对用户组内和组间的用户互访进行隔离。组内隔离标记表示组内用户不能互访，组间隔离标记表示该组内用户不能访问其他组的用户。

用户组内组间隔离授权流程图如图 2-2 所示：

图 2-2 用户组内组间隔离授权流程图



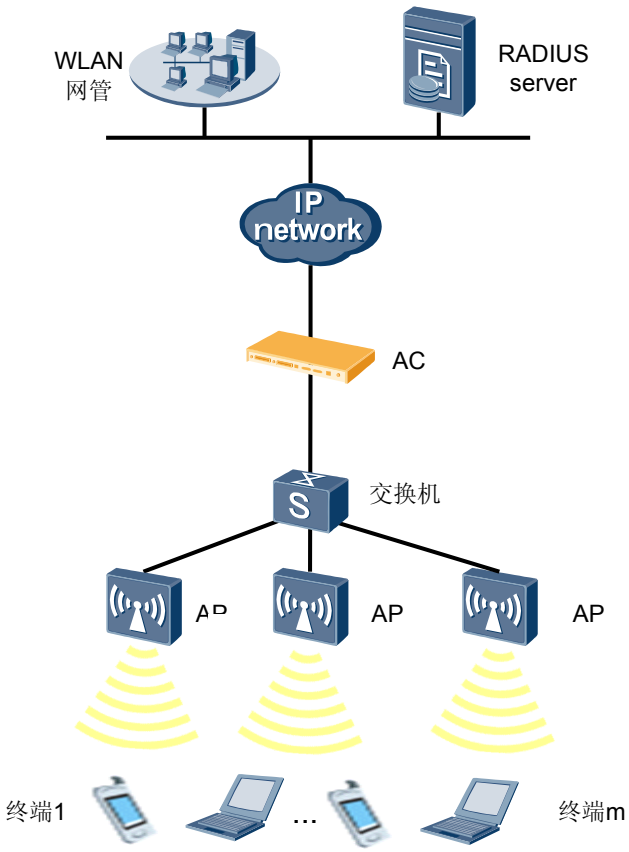
1. 用户认证成功后，RADIUS 服务器通过回应授权信息，将该用户授权到对应的用户组。
2. AC 获取 RADIUS 服务器回应报文中的的 UserGroup。
3. AC 将该用户组的组内、组间隔离标记下发给 AP。
4. 用户上线成功后访问网络，由 AP 与 AC 共同实现对用户互访权限的控制。

用户组下可以配置用户隔离，其基本的配置如下：

```
<Quidway> system-view
[Quidway] user-group test
[Quidway-user-group-test] user-isolated inter-group inner-group
[Quidway-user-group-test] quit
```

3 应用

图 3-1 用户组典型应用



用户关联 AP 后，发起认证请求，认证成功后，RADIUS 服务器将该用户授权到用户组。

如果设备上未配置对应的用户组，则授权失败，根据配置的授权失败策略，判断是否允许用户上线（AC 上默认不允许用户上线）。

如果找到相应的用户组，则将用户组下的配置（包括 ACL、Qos-profile、隔离标记）下发到 AP。在用户上线成功后，控制用户的访问权限。