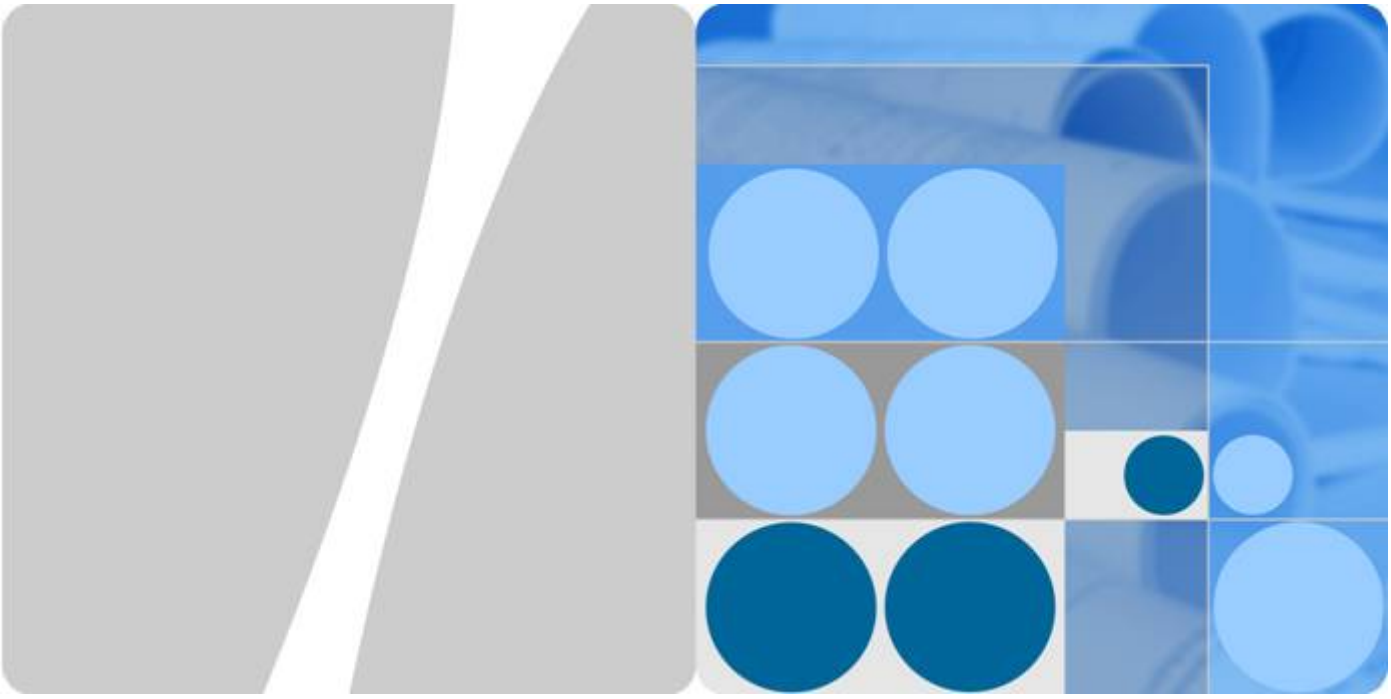


User Group Policy

Technical White Paper

Issue 01

Date 2012-10-31

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://enterprise.huawei.com

About This Document

Change History

Changes between document issues are cumulative. The latest document issue contains all changes made in previous issues.

Changes in Issue 01 (2012-10-31)

Initial commercial release.

Contents

1 Introduction to User Group Policy

Definition

User group policy includes ACL rules, QoS profile, inter-group user isolation, and intra-group user isolation. The RADIUS server divides users to different user groups to control user access rights.

Purpose

With the application and development of network technologies, users have increasing requirements for the information network and depend on the network more. However, potential risks of security increase. Network security, which predominates over network reliability, switching capability, and QoS, is the major concern of enterprise users, and network security facilities are the core in building enterprise networks.

The network access control (NAC) solution ensures secure access of users to networks by integrating network access control with security products. Through association among STAs, access control components, network devices (switches, routers, firewalls, and ACs), and third-party software (antivirus software and patch servers), this solution forcibly implements security policies on STAs to control their network behaviors. This solution improves the proactive protection capability of STAs and offers network administrators with an efficient and easy-to-use management tool.

User group policy is one of the NAC technologies. In NAC applications, there are a lot of access users, but user types are usually limited within five to eight types. Different control rules are configured for user groups. Users belonging to different groups have different access rights.

2 Principles

Basic Concepts

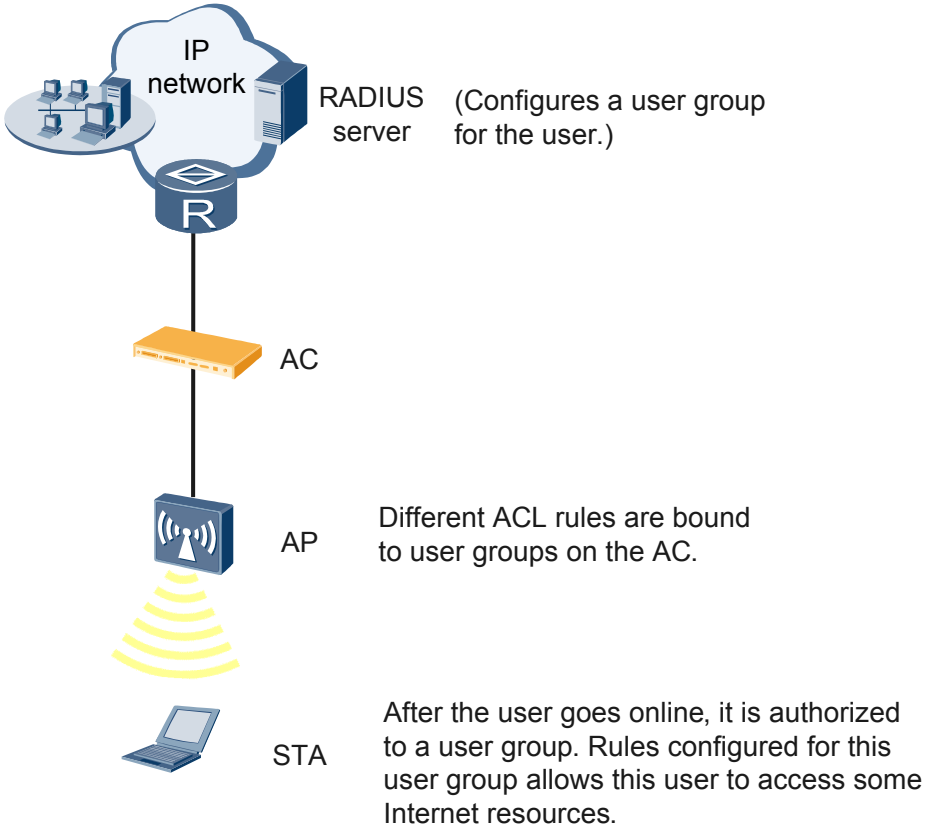
- User group: Users with the same user access rights are classified into one user group. After a user in this user group is granted a certain access right, all users in this group have the same right as this user. This reduces burdens on the AC.
- Access control list (ACL): The ACL is an access control technology that defines a set of rules to filter traffic on a network.
- Quality of service (QoS): The QoS defines user bandwidth and packet priority.
- Isolation: Inter-group isolation and intra-group isolation are used to control communication of users in the same group or different groups.

Delivery of ACL Rules Based on User Groups

The AC needs to dynamically authorize WLAN users after they go online to limit the network resources users can access.

After a user is authenticated, the RADIUS server sends the UserGroup attribute to the AC to specify to which user group the user belongs. Each user group can be associated with ACL rules to control the authorization information of users in the group. That is, users of the same type have the same authorization information.

Figure 2-1 Delivery of ACL rules based on user groups



The process of delivering ACL rules based on user groups is as follows:

1. After a user is authenticated, the RADIUS server authorizes the user to a group through the Access Accept packet.
2. The AC obtains the UserGroup attribute from the Access Accept packet.
3. The AC delivers an ACL rule bound to the UserGroup to an AP.
4. When the user goes online and accesses a network, the AC and AP work together to control the access right of this user.
5. If the RADIUS server sends no ACL rule to the AC, the user can access any network resource by default. To control the resources that the user can access, the RADIUS server must deliver an ACL rule.

Perform the following configurations to bind an ACL rule to a user group:

```
<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
```

Delivery of the QoS Profile Based on User Groups

You can bind a QoS profile to a user group to limit bandwidth for users in this group.

The process of binding a QoS profile to a user group is as follows:

1. After a user is authenticated, the RADIUS server authorizes the user to a group through the Access Accept packet.
2. The AC obtains the UserGroup attribute from the Access Accept packet.
3. The AC delivers the rate limit value and user priority configured by the QoS profile for the UserGroup to an AP.
4. When the user goes online and accesses a network, the AC and AP work together to control the bandwidth and priority of this user.

Perform the following configurations to bind a QoS profile to a user group:

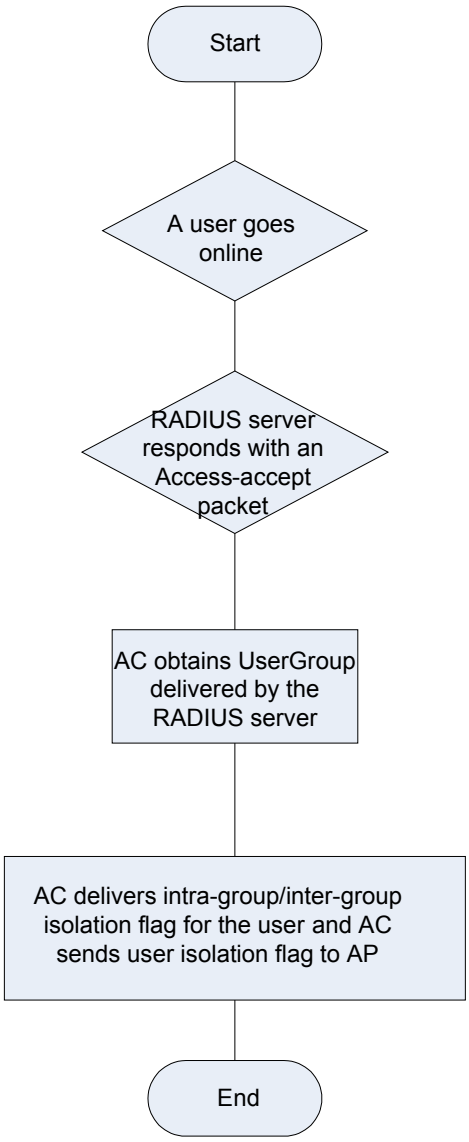
```
<Quidway> system-view
[Quidway] qos-profile name test
[Quidway-qosprofile-test] car inbound cir 10000
[Quidway-qosprofile-test] car outbound cir 10000
[Quidway-qosprofile-test] quit
[Quidway] user-group test
[Quidway-user-group-test] qos-profile test
[Quidway-user-group-test] quit
```

Delivery of User Isolation Flags Based on User Groups

You can configure inter-group or intra-group isolation flags to control access of users in the same or different groups. Intra-group isolation flag prevents users in the same group from accessing one another. Inter-group isolation flag prevents users in one group from accessing users in another group.

Figure 2-2 shows the process of user authorization through intra-group and inter-group isolation.

Figure 2-2 Process of user authorization through intra-group and inter-group isolation



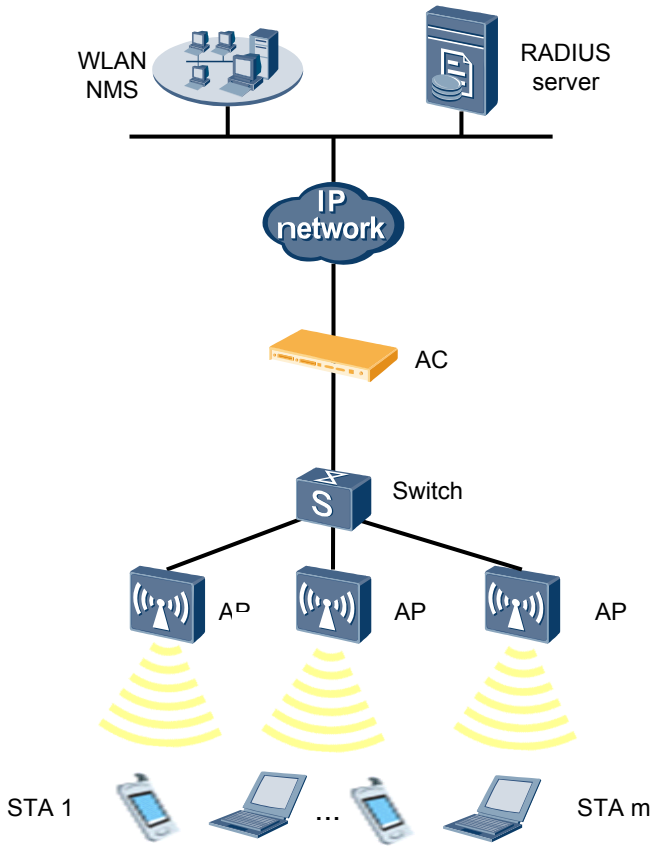
1. After a user is authenticated, the RADIUS server authorizes the user to a group through the Access Accept packet.
2. The AC obtains the UserGroup attribute from the Access Accept packet.
3. The AC delivers intra-group and inter-group isolation flags for the UserGroup to an AP.
4. When the user goes online and accesses a network, the AC and AP work together to control the access right of this user.

Perform the following configurations to configure user isolation for a user group:

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

3 Applications

Figure 3-1 Typical application of user group



After a user is associated with an AP, the user initiates an authentication request. After the user is authenticated, the RADIUS server authorizes it to a user group.

If no user group is configured on the AC, authorization fails. The AC determines whether the user can go online based on the policy for authorization failure. (By default, the AC does not allow the user to go online.)

If the user group to which the user belongs is configured on the AC, the AC delivers configurations of this user group (including ACL rules, QoS profile, and isolation flags) to the AP. After the user goes online successfully, the AP controls the user access right.