Security Mechanism for User Access to Single SSID WLAN

Li Wang[1], Mingshan Xia[1], Fazhi Qi[1]

[1] IHEP, 19B Yuquan Road, Beijing, 100049 China

Single SSID WLAN Network Security Problem:

1. User connect to the wireless network with some virus that may spread throughout the network.
2. The same network resources will be accessed by users with different identities after they connected to the wireless network.
3. The users connected to the wireless network ,with different identities will share the network bandwidth.

Table1: Grouping Users

Devices	Identify	Group	BW	authority
PC1	Staff	Group100	50MB/s	Intranet\Internet
PC2	Visitor	Group300	120MB/s	Internet
PC3	unauthorized	Group200	default	No-access

Authentication Process:

1.When the user first requests to access the wireless network, it will be forced to request the WebPortal server for registration.

2.The user selects the appropriate identity, fills in the equipment information and submits the form.

3. Approval will be given by the appropriate administrator..

4.After the approval, the database will save the grouping information of Users identify and device information.

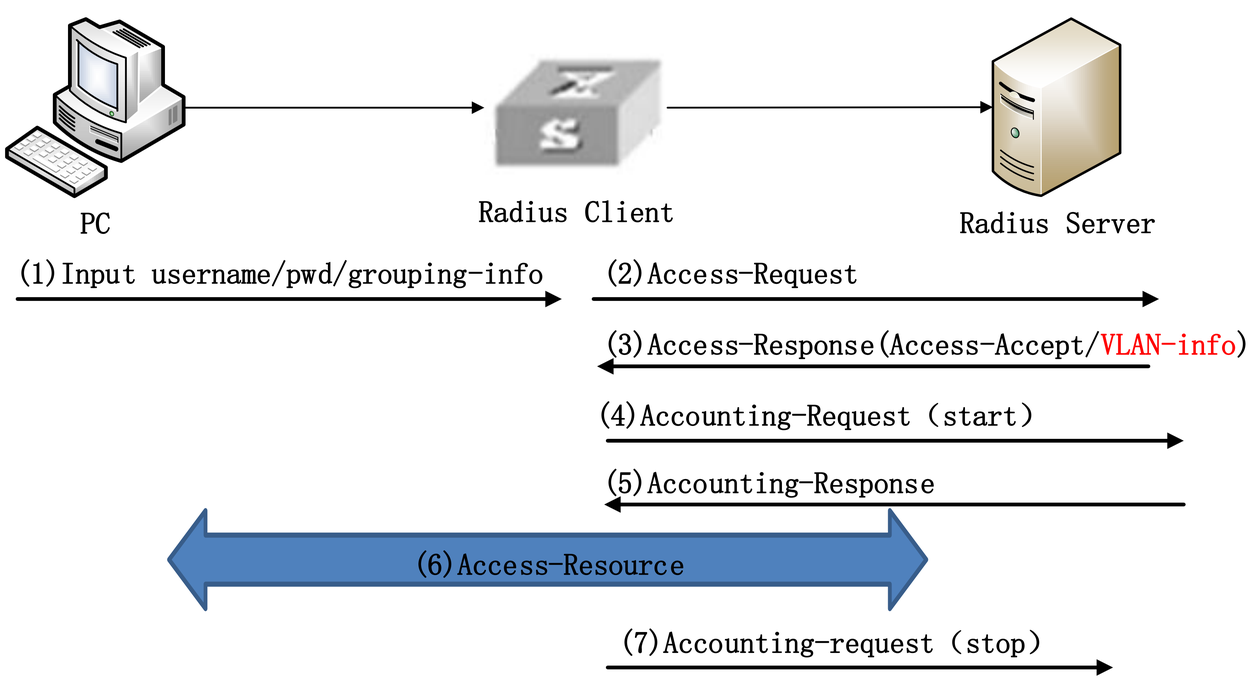

Figure 2: Radius authentication and authorization Workflow

Testing and Results:

```
Total Sta Num : 396
STA MAC        IPV4 Address AP                Wlan Vlan Status       Asso Auth Net Auth Up time
-------------- ------------ ----------------- ---- ---- ------------ --------- -------- ------------
e446.da40.22b2 10.202.1.2   CSNS_A1_F3_AP05/2 4    2002 144.5M/D/an  WPA_1X    OPEN       0:00:00:21
CSNS-WIFI-WS5708-1#
```

Figure 3: Group 200

```
Total Sta Num : 402
STA MAC        IPV4 Address  AP                Wlan Vlan Status       Asso Auth Net Auth Up time
-------------- ------------- ----------------- ---- ---- ------------ --------- -------- ------------
e446.da40.22b2 10.203.1.2    CSNS_A1_F3_AP05/2 4    2003 117.0M/E/an  WPA_1X    OPEN       0:00:00:46
CSNS-WIFI-WS5708-1#
```

Figure 4: Group 300

Solution:

In order to solve the security problems existed in the current single SSID wireless network, we adopted a new solution which grouping users access to the wireless network based on 802.1 X and VLAN technology and implements the solution with FreeRADIUS technology.

Grouping Users:

✓Registered users are grouped according to their identity by wireless network access control system.

✓ we divide users into three categories, Staff users, visitor users and unauthorized users

✓How to integrate the volunteer computing resources into DIRAC system in a secure way?

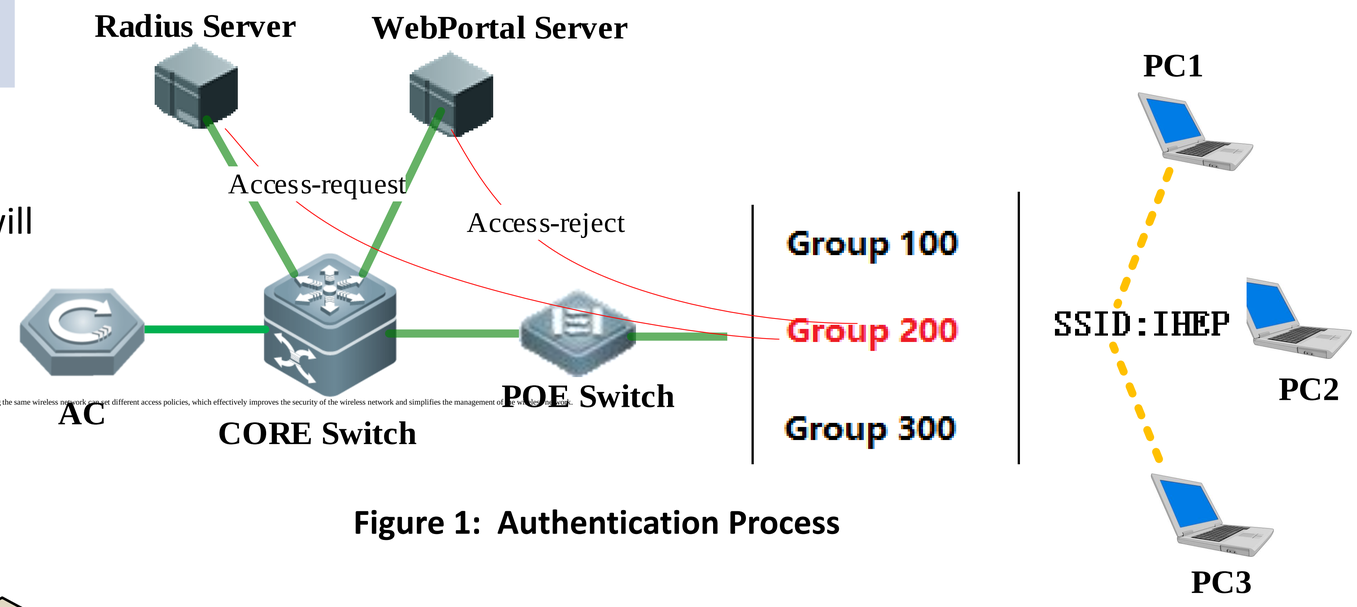

Figure 1: Authentication Process

- (1) Enters a account and password and waits for the return result.
- (2) RADIUS client sends an access-request to RADIUS server according to user name, pwd and other information.
- (3) RADIUS server will compare and analyze the user information from database. It will send permission information (Accept, Reject) to the RADIUS client
- (4) RADIUS client accesses/rejects users according to the authentication result received. If the user can be accessed, the RADIUS client sends the account-request package to the RADIUS server, and the status-type value is start.
- (5) RADIUS server returns accounting-response package;
- (6) RADIUS client sends account-request package to RADIUS server, and status-type value is stop;
- (7) RADIUS server returns account-response.
- (8) After RADIUS client receives account and pwd, it buids an access-request package and sends it to the RADIUS server.
- (9) Packet contains user name, pwd and other relevant information. The password is encrypted by MD5. If non-response for a long time and access request packet retransmitted several times, it will be considered as a server or network failure. The access request package will be sent to the alternate RADIUS server.

```
Total Sta Num : 401
STA MAC        IPV4 Address AP                Wlan Vlan Status       Asso Auth Net Auth Up time
-------------- ------------ ----------------- ---- ---- ------------ --------- -------- ------------
e446.da40.22b2 10.201.1.2   CSNS_A1_F3_AP05/1 4    2001 6.5M/D/bgn   WPA_1X    OPEN       0:00:00:07
CSNS-WIFI-WS5708-1#
```

Figure 5: Group 100

The deployment experiment of the solution proves that users of different identities accessing the same wireless network can set different access policies, which effectively improves the security of the wireless network and simplifies the management of the wireless network.