

Using TACACS+ for Telnet Login Authentication

[Requirements]

To telnet to the router, you shall enter the correct user name **h3c** and password **h3c123** to pass the authentication by the TACACS server.

[Configuration script]

Configuration script (RouterA)

```
#
sysname Quidway
#
hwtaacs nas-ip 192.168.1.254 /Set TACACS+ source address/
#
hwtaacs scheme test /Create the hwtaacs scheme test/
primary authentication 192.168.1.100 /Configure address for the primary authentic
ation server/
primary authorization 192.168.1.100 /Configure address for the primary authorizati
on server/
key authentication huawei /Configure authentication key/
key authorization huawei /Configure authorization key/
user-name-format without-domain /Set the account format to without domain na
me/
#
radius scheme system
#
domain system
scheme hwtaacs-scheme test /Apply the hwtaacs scheme test/
accounting optional /Enable accounting optional/
#
interface Ethernet1/0/0
ip address 192.168.1.254 255.255.255.0
#
interface NULL0
#
user-interface con 0
user-interface vty 0 4
authentication-mode scheme /Set scheme authentication/
#
return
```

[Verification]

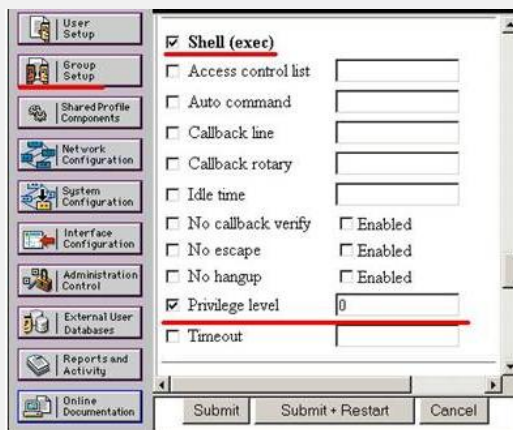
Enter the user name **h3c** and password **h3c123** to telnet to the system, and success fully log in after the account and password pass the authentication on the TACACS s erver.

[Tip]

1. After creating the account and password **h3c/h3c123** on the TACACS server, you can use the account to telnet to the router.
2. If the **user-name-format without-domain** command is not configured, the accoun t sent by the router will contain the domain name **h3c@system**, and the authenticatio n will fail.
3. Make sure that the key on the router is the same as that on the TACACS server.
4. In this mode, it is only necessary to authenticate the account with no need of accou nting so that the parameters of the accounting server are not configured, and accou nting optional is enabled.

Where there is no accounting server available or the communication with the account ing server fails, the user can keep using the network resources if the **accounting opt ional** command is configured; otherwise, the user will be cut off. This command is us ually used in the case of authentication only (no accounting).

5. **This configuration is interoperable with the CISCO ACS 3.1.** Do not forget to a uthorize the account in the relevant group.



The image shows the 'Shell (exec)' configuration window in the Cisco IOS User Configuration Wizard. The left sidebar contains a list of configuration tabs: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The 'Shell (exec)' tab is selected and highlighted with a red line. The main area of the window contains a list of configuration options, each with a checkbox and a text input field. The 'Privilege level' option is checked and its value is set to 0, also highlighted with a red line. The 'Access control list' option is unchecked and its field is empty. The 'Auto command' option is unchecked and its field is empty. The 'Callback line' option is unchecked and its field is empty. The 'Callback rotary' option is unchecked and its field is empty. The 'Idle time' option is unchecked and its field is empty. The 'No callback verify' option is unchecked, and its 'Enabled' checkbox is also unchecked. The 'No escape' option is unchecked, and its 'Enabled' checkbox is also unchecked. The 'No hangup' option is unchecked, and its 'Enabled' checkbox is also unchecked. The 'Timeout' option is unchecked and its field is empty. At the bottom of the window, there are three buttons: 'Submit', 'Submit + Restart', and 'Cancel'.

Option	Checkbox	Value
Shell (exec)	☒	
Access control list	☐	
Auto command	☐	
Callback line	☐	
Callback rotary	☐	
Idle time	☐	
No callback verify	☐	☐ Enabled
No escape	☐	☐ Enabled
No hangup	☐	☐ Enabled
Privilege level	☒	0
Timeout	☐	

Submit Submit + Restart Cancel