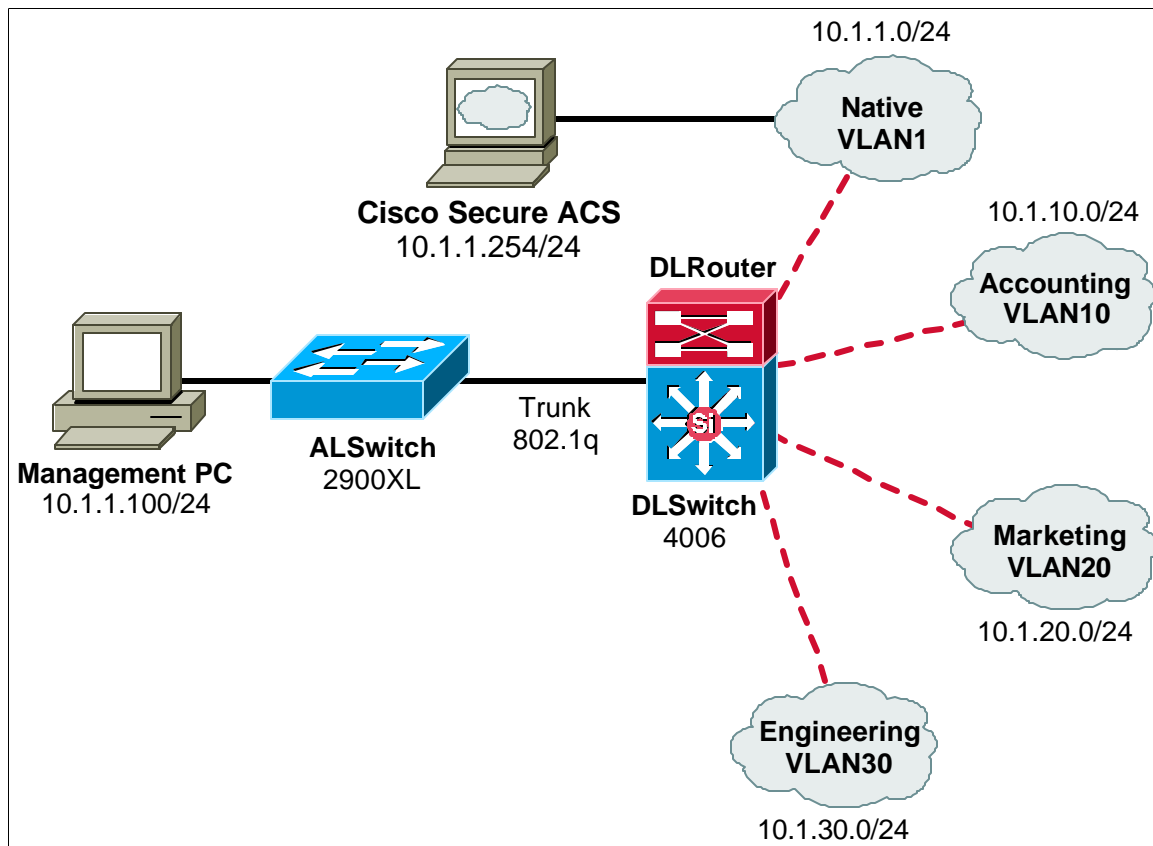


## Lab 10.2.4 Cisco Secure ACS Switch Security for Controlled User Access



### Objective:

Use Cisco Secure ACS security for controlled user access

### Scenario:

Your network consists of several network devices. You would like to configure access security to your devices by user where possible. You have a TACACS+ Cisco Secure Server for centralized authentication. Configure each device for secure access while also configuring local access as a fallback in case the ACS server is not available. The following information should be used.

#### TACACS+ (these must be created on the ACS server prior to this lab)

User = smith

Password = cisco

Enable password = tacacs

Key = superman

#### LOCAL

User = admin

Password = cisco

Enable password = enable

## Lab Tasks:

1. Cable the lab as shown in the diagram.
2. The first device to be configured will be the Catalyst 2900XL. Log into the switch, enter privileged mode, clear the NVRAM and then restart.
3. Configure **ALSwitch** including all basic information and trunking information.

- a. Configure the hostname

```
Switch(config)#hostname ALSwitch
```

- b. Configure the switch trunking information on FastEthernet0/1 and PortFast on FastEthernet0/2

```
ALSwitch(config)#interface FastEthernet0/1  
ALSwitch(config-if)#switchport trunk encapsulation dot1q  
ALSwitch(config-if)#switchport mode trunk  
ALSwitch(config)#interface FastEthernet0/2  
ALSwitch(config-if)#spanning-tree portfast
```

- c. Configure the IP address for the management VLAN.

```
ALSwitch(config)#interface VLAN1  
ALSwitch(config-if)#ip address 10.1.1.3 255.255.255.0
```

4. Configure **ALSwitch** security for local AAA authentication.

- a. Configure the security for local fallback authentication

```
ALSwitch(config)#aaa new-model  
ALSwitch(config)#aaa authentication login default group tacacs+ local
```

- b. Configure the security for ACS authentication

```
ALSwitch(config)#aaa authentication enable default group tacacs+ enable  
ALSwitch(config)#aaa authorization exec tacacs+  
ALSwitch(config)#tacacs-server host 10.1.1.254  
ALSwitch(config)#tacacs-server timeout 30  
ALSwitch(config)#tacacs-server key superman
```

- c. Configure the local user account with user level access only

```
ALSwitch(config)#username admin password 0 cisco
```

- d. Configure a local enable password

```
ALSwitch(config)#enable password enable
```

5. The next device to be configuring the Catalyst 4006 L3 Module. From the console port on the L3 module, log into the router, enter privileged mode, clear the NVRAM and then restart.

6. Configure **DLRouter** including all basic information and trunking information.

a. Configure the hostname

```
Router(config)#hostname DLRouter
```

b. Configure the basic connectivity information including IP addressing and trunking settings

```
DLRouter(config)#interface Port-channel1
DLRouter(config-if)#ip address 10.1.1.1 255.255.255.0

DLRouter(config)#interface Port-channel1.10
DLRouter(config-if)#encapsulation dot1Q 10
DLRouter(config-if)#ip address 10.1.10.1 255.255.255.0

DLRouter(config)#interface Port-channel1.20
DLRouter(config-if)#encapsulation dot1Q 20
DLRouter(config-if)#ip address 10.1.20.1 255.255.255.0

DLRouter(config)#interface Port-channel1.30
DLRouter(config-if)#encapsulation dot1Q 30
DLRouter(config-if)#ip address 10.1.30.1 255.255.255.0

DLRouter(config)#interface GigabitEthernet3
DLRouter(config-if)#no ip address
DLRouter(config-if)#channel-group 1

DLRouter(config)#interface GigabitEthernet4
DLRouter(config-if)#no ip address
DLRouter(config-if)#channel-group 1
```

7. Configure **DLRouter** security for local AAA authentication.

a. Configure the security for local authentication

```
DLRouter(config)#aaa new-model
DLRouter(config)#aaa authentication login default tacacs+ local
DLRouter(config)#aaa authorization exec tacacs+
```

b. Configure the security for ACS authentication

```
DLRouter(config)#aaa authentication enable default tacacs+ enable
DLRouter(config)#tacacs-server host 10.1.1.254
DLRouter(config)#tacacs-server timeout 30
DLRouter(config)#tacacs-server key superman
```

c. Configure the local user account with user level access only

```
DLRouter(config)#username admin password 0 cisco
```

d. Configure a local enable password

```
DLRouter(config)#enable password enable
```

8. The next device to be configuring the Catalyst 4006 Switch Module. From the console port on the switch, log in, enter privileged mode, clear the NVRAM and then restart.
9. Configure **DLSwitch** including all basic information and trunking information.

- a. Configure the hostname

```
Switch (enable)# set system name DLSwitch
```

- b. Configure other basic information

```
DLSwitch> (enable)set vtp domain corp
DLSwitch> (enable)set vtp mode server
DLSwitch> (enable)set vlan 1 name default
DLSwitch> (enable)set vlan 10 name Accounting
DLSwitch> (enable)set vlan 20 name Marketing
DLSwitch> (enable)set vlan 30 name Engineering
DLSwitch> (enable)set interface sc0 1 10.1.1.2/255.255.255.0
10.1.1.255
DLSwitch> (enable)set ip route 0.0.0.0/0.0.0.0 10.1.1.1
DLSwitch> (enable)set port channel 2/3-4 89
DLSwitch> (enable)set port channel 2/1-2 156
DLSwitch> (enable)set vlan 10 2/19-24
DLSwitch> (enable)set vlan 20 2/25-30
DLSwitch> (enable)set vlan 30 2/31-34
DLSwitch> (enable)set trunk 2/1 nonegotiate dot1q 1-1005
DLSwitch> (enable)set trunk 2/2 nonegotiate dot1q 1-1005
DLSwitch> (enable)set trunk 2/3 nonegotiate dot1q 1-1005
DLSwitch> (enable)set spantree portfast 2/4 enable
DLSwitch> (enable)set port channel 2/1-2 mode on
```

- c. Configure local security. You will notice that we will only set local access passwords and not users.

```
DLSwitch> (enable)set password {set this to cisco}
DLSwitch> (enable)set enablepass {set this to enable}
```

- d. Configure ACS security.

```
DLSwitch> (enable)set tacacs server 10.1.1.254 primary
DLSwitch> (enable)set tacacs key superman
DLSwitch> (enable)set tacacs timeout 30
DLSwitch> (enable)set authentication login tacacs enable
DLSwitch> (enable)set authentication enable tacacs enable
```

## 10. Test authentication

- a. Connect to the console port of each switch. Use the user ID and passwords assigned for each switch to test authentication. Enable the following on each of the AAA enabled switches and answer the following questions.

For **DLRouter** and **ALSwitch** use the following:

```
DLRouter(config)#debug tacacs
DLRouter(config)#debug aaa authentication
DLRouter(config)#debug aaa authorization
```

For **DLSwitch** us the following:

```
DLSwitch> (enable)set trace tacacs
```

- b. What command would disable tracing on the 4006 switch?

-----

- c. On each switch or router, are you able to log on using local authentication if the TACACS authentication is functioning?

-----

- d. Disconnect the ACS server from the network. Are you able to log on locally? (Reconnect after this step is complete.)

-----