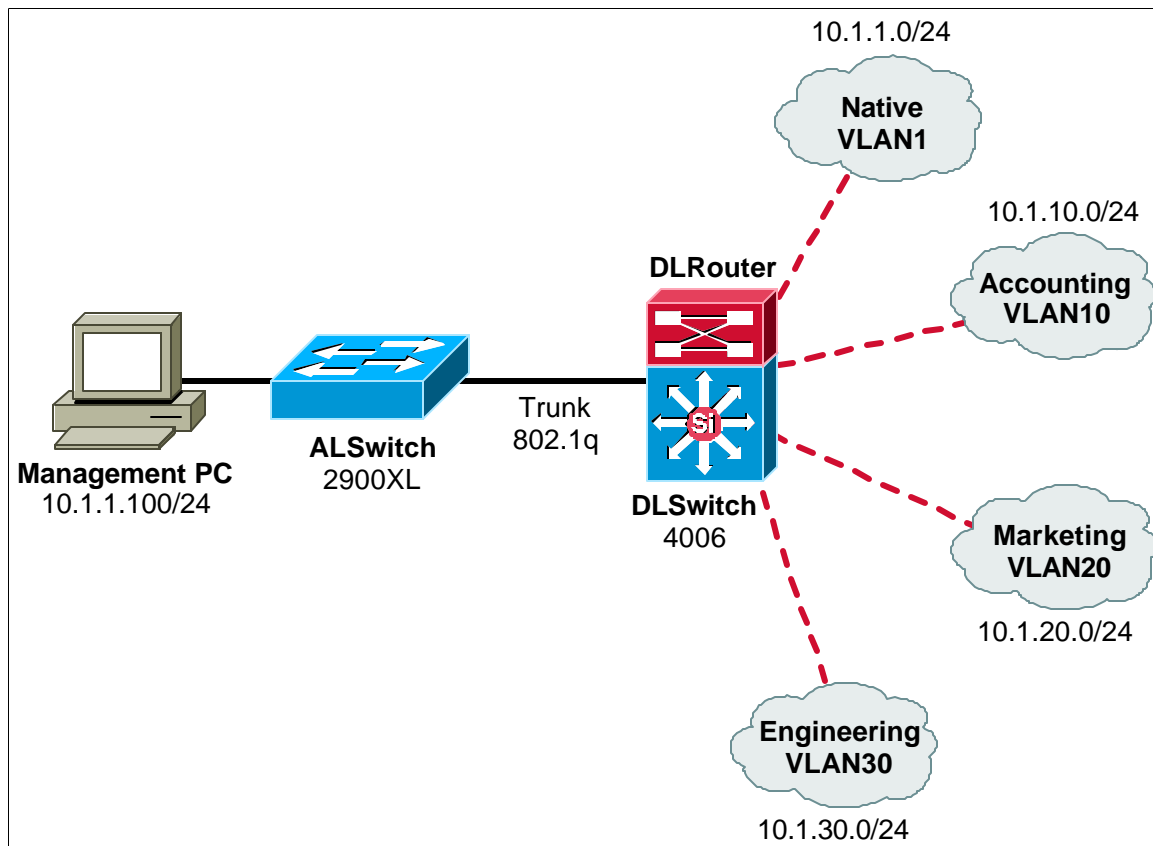


Lab 10.2.2 Local Switch Security for Controlled User Access



Objective:

Use local switch 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 DO NOT have a TACACS+ or RADIUS server available for centralized access. Configure each device as required. The following security information should be used.

Local Passwords

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, and 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 an 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 authentication

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

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

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

- c. Configure a local enable password

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

5. The next device to be configured will be 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 local
```

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

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

c. Configure a local enable password

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

8. The next device to be configured will be 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}
```

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.

```
Switch(config)#debug aaa authentication
```

- b. On the ALSwitch or DLRouter, what is the AAA authentication START method?
-

- c. When debugging AAA authentication, does the password display as part of the debug information?
-

- d. On the ALSwitch or DLRouter, what is the AAA/CONT method used to access privileged mode?
-