

## Contents

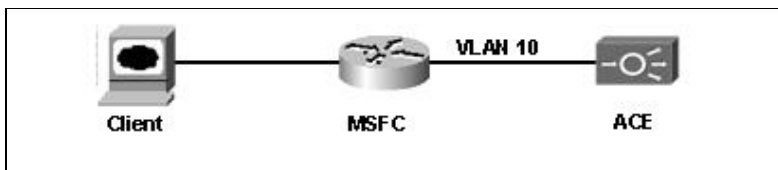
- [1 Purpose](#)
- [2 Design](#)
- [3 Configuration](#)
- [4 Comments](#)
- [5 show running-config](#)
- [6 Related Information](#)

## Purpose

Configure remote access to allow telnet, ssh, and other mgmt protocols access to the ACE via the Admin context.

## Design

In the typical scenario, the MSFC is used to route remote access connection from a client to the ACE. It is recommended to have a dedicated VLAN for remote management when feasible; however, it is not required. In fact, it is common to see a management service policy apply to client vlans when ACE is integrated into an existing network.



## Configuration

Remote access is denied by default on the ACE module. To enable remote access you need to configure the following objects:

- class-map to classify the remote management traffic which can access the ACE control plane
- policy-map to allow the classified protocols
- interface vlan to receive the remote access connections

To begin the configuration, use a console connection or session to the ACE from the Sup720 (session slot <#>proc 0). It is common to allow all of the management protocols to the Admin context using the management policy-map with the default class.


```
policy-map type management first-match unrestricted-remote-mgmt
  class class-default
  permit
```

However, if security is a concern ACE can be configured to only accept the require protocols from well defined hosts. This follow example shows a common configuration where only ssh, snmp, and https management protocols are allowed.


```
class-map type management match-any remote-access
  2 match protocol ssh any
```

## Initial\_Remote\_Access\_to\_ACE\_Configuration\_Example

```
3 match protocol snmp any
4 match protocol https any
```

 **Note:** To restrict access based on host, simply change the ?any? to a well define host match.

```
policy-map type management first-match remote-mgmt
  class remote-access
    permit
```

 **Note:** To further restrict access, policies can be used to deny remote access traffic. Although policies to deny remote access traffic are not commonly used, they useful when one needs to allow a subnet remote access, and restrict a single host within that subnet.

```
interface vlan 10
  description "Client side connectivity"
  ip address 172.16.1.5 255.255.255.0
  service-policy input remote-mgmt
  no shutdown
```

```
ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

Related 'show' commands  
DC1-Cat6k1#show users  
DC1-Cat6k1#show telnet  
DC1-Cat6k1#show ssh session-info  
DC1-Cat6k1#show conn

## Comments

There is a limit of 4 simultaneous TELNET sessions or 4 simultaneous SSH sessions per context at any given time.

## show running-config

```
ACE/Admin# sho run
Generating configuration....

login timeout 0
hostname Pod1-ACE

class-map type management match-any remote-access
  2 match protocol ssh any
  3 match protocol snmp any
  4 match protocol https any

policy-map type management first-match remote-mgmt
  class remote-access
    permit

interface vlan 10
  description "Client side connectivity"
  ip address 172.16.1.5 255.255.255.0
  service-policy input remote-mgmt
  no shutdown

ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

## **Related Information**

[Technical Support & Documentation - Cisco Systems](#)