Contents

Introduction

This document describes a step by step procedure of adding Terminal Access Controller Access Control System (TACACS+) authentication service on the Cisco MGX 8850/8950/8830 running switch software revision greater than 5.0, with Cisco Access Control Server (ACS) version 4.2 and above.

Prerequisites

Requirements

Cisco recommends that you meet this requirements before you attempt this configuration:

- AAA Server is reachable from the MGX

Components Used

This document is restricted to Cisco MGX 8850/8950/8830 running switch software revision greater than 5.0 and with ACS version above 4.2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Configuration on MGX

An example of the configuration required on MGX is shown here

Step 1**.** Verify the switch software version. You need version 5.0 or later to configure TACACS+

```
8950A.7.PXM.a > dspversion
  Image Type   Shelf Type    Card Type         Version   Built On
  ----------   ----------   ----------    ------------   ------------
     Runtime          MGX        PXM45     5.1(20.200)   Jun 23 2005,
21:36:08
        Boot          MGX        PXM45     4.0(0.11)P2   -
```

Step 2**.** Verify you have the right IP address:

```
8950A.7.PXM.a > dspifip
    Interface        Flag  IP Address       Subnetmask       Broadcast
Addr
    ---------------  ----  ---------------  ---------------  -----------
----
    Ethernet/lnPci0  UP    10.66.69.57      255.255.255.128
10.255.255.255
    SLIP/sl0         UP    127.0.0.2        255.0.0.0
(N/A)
    ATM/atm0         DOWN  0.0.0.0          0.0.0.0
(N/A)
```

Step 3**.** Verify you can ping the ACS server: (ACS server is at 10.106.60.182)

```
8950A.7.PXM.a > ping 10.106.60.182
PING 10.106.60.182: 56 data bytes
64 bytes from 10.106.60.182: icmp_seq=0. time=250. ms
64 bytes from 10.106.60.182: icmp_seq=1. time=240. ms
64 bytes from 10.106.60.182: icmp_seq=2. time=240. ms
----10.106.60.182 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 240/243/250
```

If ping doesn't go through, we need to check IP reachability. Also verify **`dspifip`** and **`bootchange`** are configured with correct IP address.

```
8950A.7.PXM.a > bootchange

'.' = clear field;  '-' = go to previous field;  ^D = quit

boot device          : lnPci0
processor number     : 0
host name            :
file name            :
inet on ethernet (e) : 172.16.157.88 >>
inet on backplane (b):
```

```
host inet (h)         :
gateway inet (g)      : 172.16.157.1  >>
user (u)              :
ftp password (pw) (blank = use rsh):
flags (f)             : 0x0
target name (tn)      :
startup script (s)    :
other (o)             :
```

Note: Check the configuration of dspifip parameters and changed the Primary IP address of network management to Interface LAN IP and ATM address as secondary (using **cnfndparm**). Also you need to configure the bootchange parameters putting correct LAN IP address and gateway. The **routeshow** command output should indicate the default gateway for 0.0.0.0 as LAN IP address.

Step 4. Verify AAA configuration using **dspaaa .** By default no AAA is configured

```
8950A.7.PXM.a > dspaaa
AAA CONFIGURATION:
   Authentication Methods  :  local cisco
   Authorization Methods   :  local cisco
   Authorization Type      :  group
   Default Privilege Level :  NOUSER_GP
   Prompt Display          :  acs
   SSH/FTP Message Type    :  Inbound ASCII Login
   IOS Exclusion List      :

TACACS+ SERVERS:    primary is shown first

                        Time Dead  Single
   IP Address     Port  Out  Time  Conn   Shared Encryption Key
---------------  ----  ---  ----  ------ ------------------------------
--------
```

Step 5. Configure the AAA server IP address and key:

```
8950A.7.PXM.a > cnfaaa-server tacacs+ -ip 10.66.79.246
Do you want to change the encryption key (yes/no)?yes
Enter the encryption key: cisco
Re-enter the encryption key: cisco

TACACS+ SERVERS:    primary is shown first

                        Time Dead  Single
   IP Address     Port  Out  Time  Conn   Shared Encryption Key
---------------  ----  ---  ----  ------ ------------------------------
--------
10.66.79.246      49    5    0     true   Cisco
```

Step 6. Configure Authentication:

```
8950A.7.PXM.a > cnfaaa-authen
```

```
Syntax: cnfaaa-authen <method> [<method>...]

        method -- {local | default | tacacs+ | cisco}
          local  : Use the local database for authentication.
          default: Same as local.
          tacacs+: Use the TACACS+ protocol for authentication.
          cisco  : Only the root user of 'cisco' is allowed to login.
```

Here we are doing TACACS+ then Local and then Cisco. (It is recommended to have cisco as a last resort in there…)

```
8950A.7.PXM.a > cnfaaa-authen tacacs+ local cisco
AAA CONFIGURATION:
   Authentication Methods  :  tacacs+ local cisco
   Authorization Methods   :  local cisco
   Authorization Type      :  group
   Default Privilege Level :  NOUSER_GP
   Prompt Display          :  acs
   SSH/FTP Message Type    :  Inbound ASCII Login
   IOS Exclusion List      :
```

WARNING: The newly configured authentication/authorization methods applies to the new sessions. This configuration has no impact on existing sessions.

Step 7**.** Configure the default privilege level if you want. We do not configure it in this example, i.e. we leave it as default:

```
8950A.7.PXM.a > cnfaaa-priv
Syntax: cnfaaa-priv <CISCO_GP | SERVICE_GP | SUPER_GP | GROUP1 | ANYUSER
|
                     NOUSER_GP | default>
                    (NOTE: 'default' is same as NOUSER_GP.)

8950A.7.PXM.a > cnfaaa-priv default
AAA CONFIGURATION:
   Authentication Methods  :  tacacs+ local cisco
   Authorization Methods   :  tacacs+ local cisco
   Authorization Type      :  group
   Default Privilege Level :  NOUSER_GP
   Prompt Display          :  acs
   SSH/FTP Message Type    :  Inbound ASCII Login
   IOS Exclusion List      :
```

Step 8**.** Verify Configuration:

```
8950A.7.PXM.a > dspaaa
AAA CONFIGURATION:
   Authentication Methods  :  tacacs+ local cisco
   Authorization Methods   :  tacacs+ local cisco
   Authorization Type      :  group
   Default Privilege Level :  NOUSER_GP
   Prompt Display          :  acs
   SSH/FTP Message Type    :  Inbound ASCII Login
```

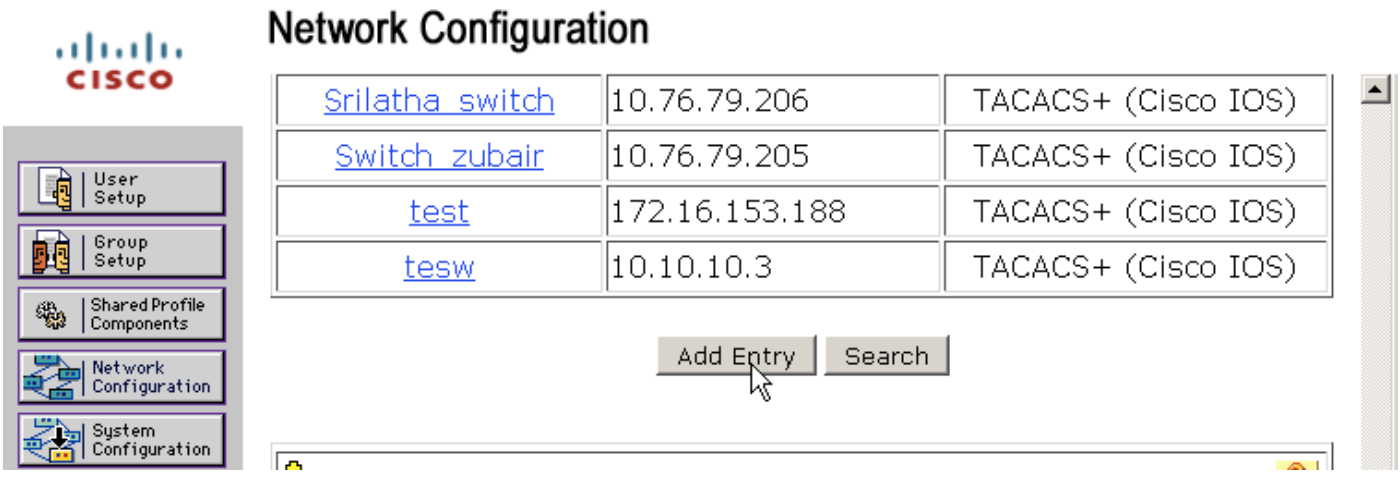
```
   IOS Exclusion List      :

TACACS+ SERVERS:    primary is shown first

                         Time Dead  Single
   IP Address     Port   Out  Time  Conn   Shared Encryption Key
---------------  ----   ---  ----  ------ ------------------------------
--------
10.66.79.246      49     5    0     true   cisco

8950A.7.PXM.a > dspaaa-servers
TACACS+ SERVERS:    primary is shown first

                         Time Dead  Single
   IP Address     Port   Out  Time  Conn   Shared Encryption Key
---------------  ----   ---  ----  ------ ------------------------------
--------
10.66.79.246      49     5    0     true   cisco
```

Configuration on ACS

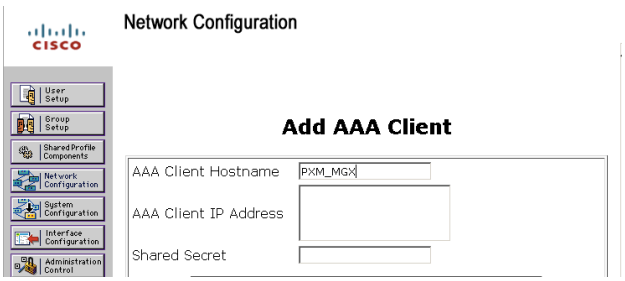
An example of the configuration required on ACS is shown here:

Step 1. Add the MGX as client on the ACS: (the name used here is PXM_MGX, can be anything)

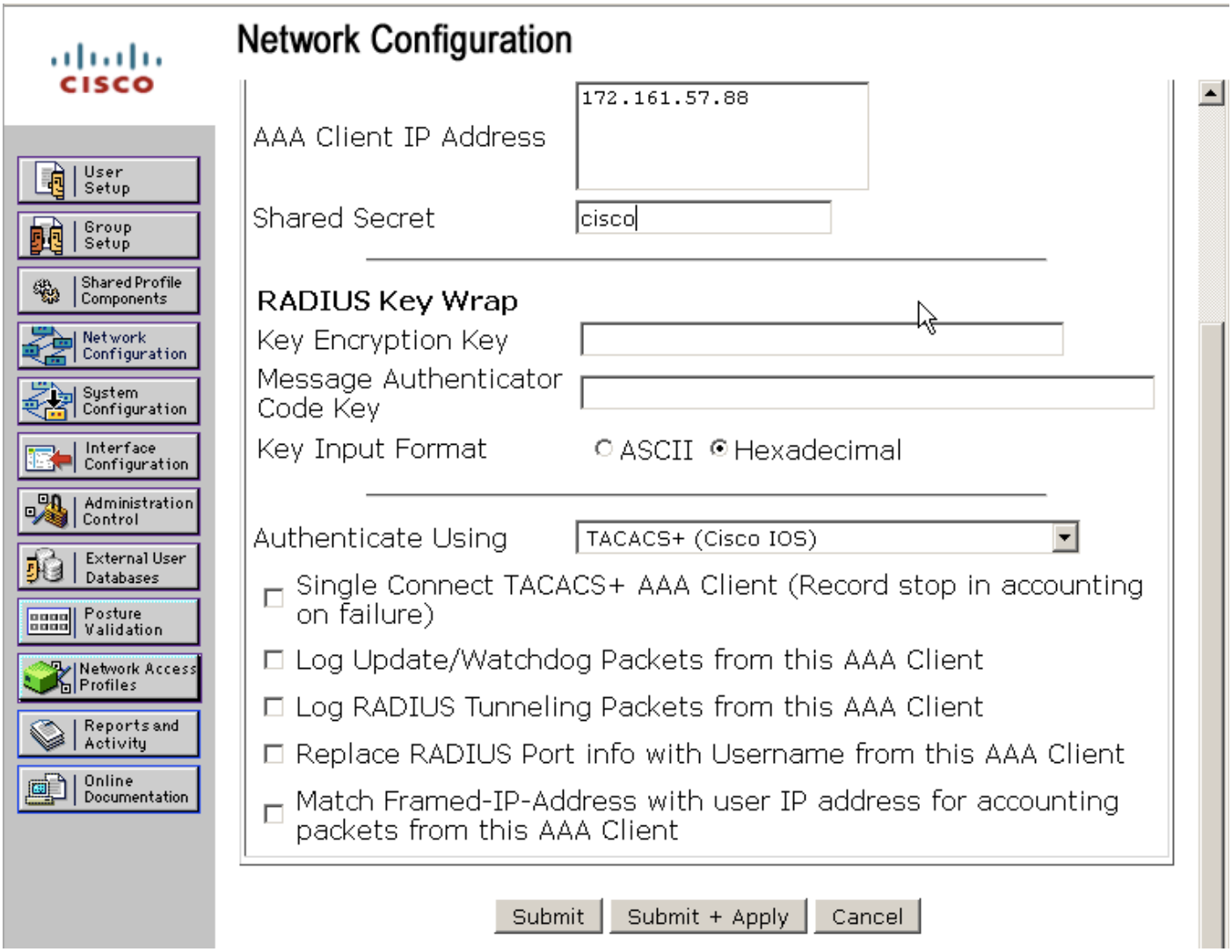
Click on **Network Configuration**
(the name used here is PXM_MGX, can be anything)



Step 2. Click **Add Entry** and configure client hostname

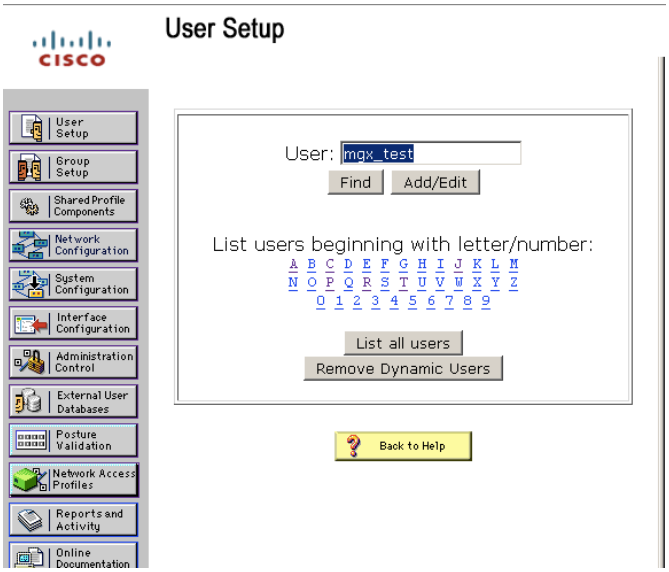


Step 3. Configure the IP address of the AAA client (**MGX** in this case) and the '**key**' which must match with the MGX config (the key used here is '**cisco**').

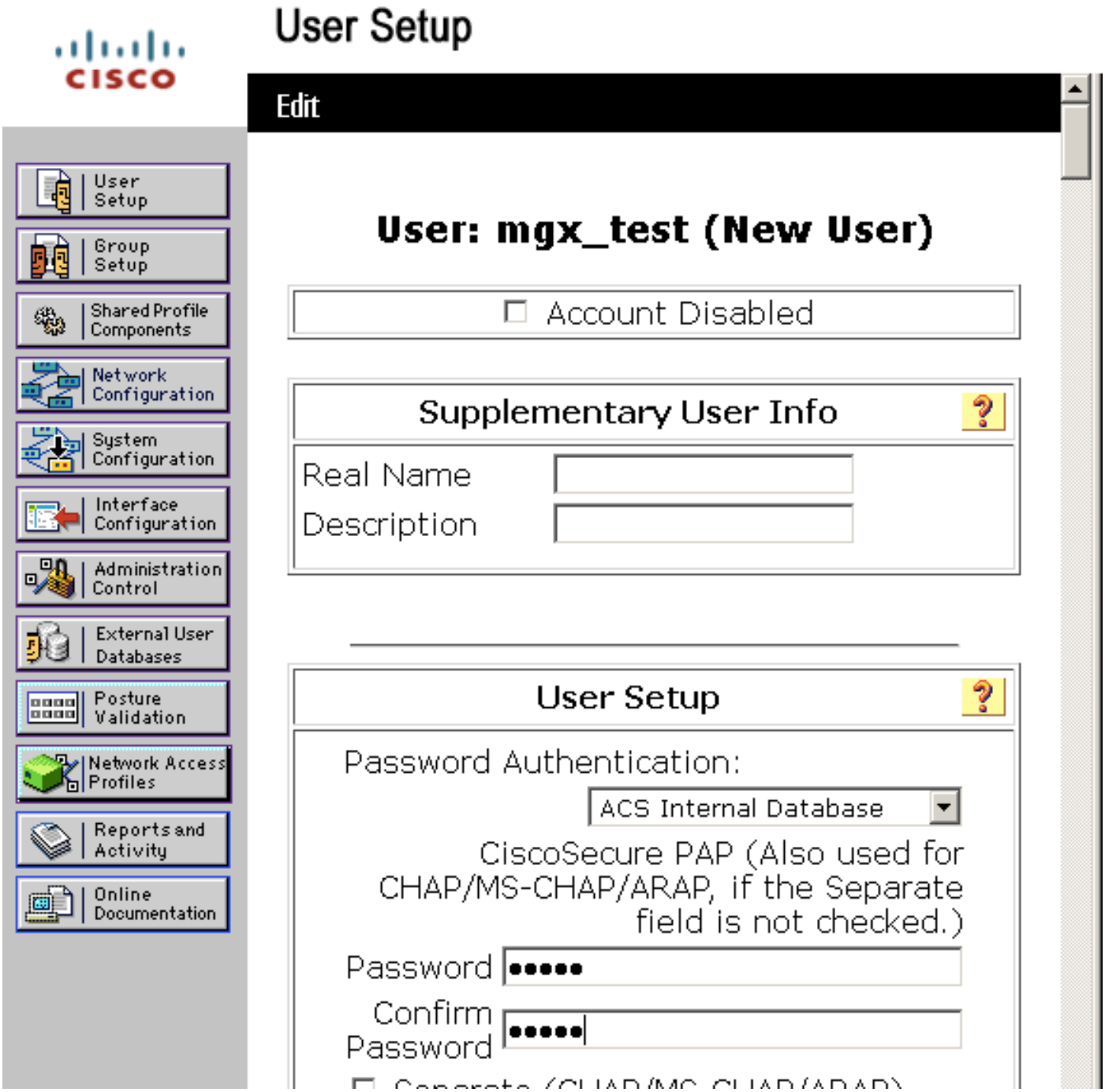


Click **Submit+Apply**

Step 4. Configure a USER. Click on **User Setup.** The user here is called 'mgx_test' . Click **Add/Edit**, after typing in a new username

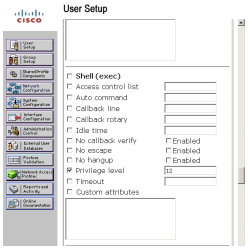


Step 5. Configure a password for the user. We configure a password "**cisco**" in this example



Step 6. Setup the Privilege level of the user under **Shell (exec)**. Here the user is given privilege level 12 or Service_GP.

Note: This is the main difference with IOS authentication. With PXM we are not assigning enable privilege, rather we are assigning shell (exec) privilege to the user.



Click **Submit** to commit the changes.

Verify

Telnet to MGX and ensure the user get the privilege level we configured on the ACS server (i.e. SERVICE_GP or privilege level 12):

```
aptcwm02% telnet 172.16.157.88
Trying 172.16.157.88...
Connected to 172.16.157.88.
Escape character is '^]'.
Username: mgx_test
Password: cisco


8950A.7.PXM.a > who

Port        Slot    Idle    UserId       Access     From
Started At
-------------------------------------------------------------------------
-------
console        7    0:00:14 cisco        CISCO_GP console port
20:55:29 JUL28
telnet.01 *    7    0:00:00 mgx_test     SERVICE_GP 10.66.69.126
21:04:11 JUL28 <<<
```

Check the AAA stats to see TACACS+ authentication happening:

```
8950A.7.PXM.a > dspaaa-stats

Last cleared on: 07/28/2005 17:55:42  (PST)


Last good login authen: mgx_test      telnet.01    10.66.69.126
                        tacacs+   10.66.79.246/49
                        07/28/2005 21:27:34  (PST)
Last good grp priv:     mgx_test      telnet.01    10.66.69.126
                        tacacs+   10.66.79.246/49
                        07/28/2005 21:27:34  (PST)
Last failed cmd:        NONE

Type <CR> to continue, Q<CR> to stop:

____SWITCH LEVEL COUNTS____
Method:                 cisco             local
TACACS
# authen failures:      0                 18                0
# grp author failures:  0                 0                 0
# cmd author failures:  0                 -----             0
# authen falls back to: 0                 32                0
# author falls back to: 0                 1                 0
```

```
# authen unreachable:   -----             -----             0
# author unreachable:   -----             -----             0
# challenges RX:        -----             -----             0
# socket throttles:     -----             -----             0
# Messages TX:          -----             -----             9
# Messages RX:          -----             -----             9
# Messages Flushed:     -----             -----             0
# Abort Messages Sent:  -----             -----             0
# Supported AVPs RX:    -----             -----             2
# Unsupported AVPs RX:  -----             -----             0
# Unknown AVPs RX:      -----             -----             0

Type <CR> to continue, Q<CR> to stop:

____TACACS+ SERVER LEVEL COUNTS____
Server IP Address:      10.66.79.246      0.0.0.0
0.0.0.0
Server Port:            49                0                 0
# authen failures:      0                 0                 0
# cmd author failures:  0                 0                 0
# authen falls back to: 0                 0                 0
# author falls back to: 0                 0                 0
# authen unreachable:   0                 0                 0
# author unreachable:   0                 0                 0
# challenges RX:        0                 0                 0
# Messages TX:          9                 0                 0
# Messages RX:          9                 0                 0
# Messages Flushed:     0                 0                 0
# Abort Messages Sent:  0                 0                 0
# Supported AVPs RX:    2                 0                 0
# Unsupported AVPs RX:  0                 0                 0
# Unknown AVPs RX:      0                 0                 0
Avg Response Delay:     9                 0                 0
Max Response Delay:     15                0                 0
```

The following commands are related to TACACS on MGX:

```
M7.8.PXM.a > ? aaa

    Available commands
    ------------------
    cnfaaa-authen
    cnfaaa-author
    cnfaaa-ftpssh
    cnfaaa-ignore-ios
    cnfaaa-priv
    cnfaaa-prompt
    cnfaaa-server
    delaaa-server
    dspaaa
    dspaaa-servers
    dspaaa-stats
    dspaaa-tac-trace
```

```
setaaa-tac-trace
```

Related Information

- Cisco MGX 8800/8900 Series Software Configuration Guide, Release 5.4
- Technical Support & Documentation - Cisco Systems