

# 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[MGX の設定](#)

[ACS の設定](#)

[確認](#)

[関連情報](#)

## 概要

この資料は大きい Cisco MGX 8850/8950/8830 実行スイッチソフトウェアのリビジョンに Terminal Access Controller Access Control System ( TACACS+ ) 認証サービスを追加するステップバイステップ手順を Cisco Access Control Server ( ACS ) バージョン 4.2 および それ 以上とのより 5.0、記述したものです。

## 前提条件

### 要件

Cisco はこの設定を試みる前にこの必要条件を満たしていることを推奨します:

? AAAサーバは MGX から到達可能です

### 使用するコンポーネント

この資料は大きい Cisco MGX 8850/8950/8830 実行スイッチソフトウェアのリビジョンにより 5.0 および 4.2 の上の ACS バージョンと制限 されます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 設定

注 このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登](#)

[録ユーザ専用](#) ) を使用してください。

#### MGX の設定

MGX で必要な設定の例がここに示されています

ステップ 1. スイッチソフトウェアバージョンを確認して下さい。バージョン 5.0 またはそれ以降が TACACS+ を設定することを必要とします

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

```
-----  
MGX PXM45 5.1(20.200) 2005 6 23 21:36:08  
MGX PXM45 4.0(0.11) P2 -
```

ステップ 2. 右の IP アドレスがあることを確認して下さい:

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

```
Interface Flag IP Address Subnetmask Broadcast Addr
```

```
-----  
-  
Ethernet/lnPci0 10.66.69.57 255.255.255.128 10.255.255.255  
SLIP/sl0 127.0.0.2 255.0.0.0 N/A  
ATM/atm0 DOWN 0.0.0.0 0.0.0.0 N/A
```

ステップ 3. ACS サーバを ping できることを確認して下さい: ( ACS サーバは 10.106.60.182 ) にあります

```
8950A.7.PXM.a > PING 10.106.60.182
```

```
PING 10.106.60.182: 56  
10.106.60.182 64 : icmp_seq=0. time=250.  
10.106.60.182 64 : icmp_seq=1. time=240.  
10.106.60.182 64 : icmp_seq=2. time=240.  
----10.106.60.182 PING ----  
3 3 0%  
ms/avg/ = 240/243/250
```

PING なら doesn't か。t は、私達 IP 到達性をチェックする必要があります行きます。また dspifip および bootchange 正しい IP アドレスで設定されることを確認して下さい。

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

```
= CLEAR ; -= ; ^D =
```

```
boot device : lnPci0  
processor number : 0  
:  
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) :
```

**注** dspifip パラメータの設定をチェックし、セカンダリとして LAN IP および ATM アドレスをインターフェイスさせるためにネットワーク管理のプライマリ IP アドレスを変更しました (cnfndparm を使用して)。また正しい LAN IP アドレスおよびゲートウェイを置く bootchange パラメータを設定する必要があります。routeshow コマンド 出力は LAN IP アドレスとして 0.0.0.0 のためのデフォルト ゲートウェイを示す必要があります。

ステップ 4. dspaaa を使用して AAA 設定を確認して下さい。デフォルトで AAA は設定されません

```
8950A.7.PXM.a > dspaaa
AAA:
 : Cisco
 : Cisco
 :
 : NOUSER_GP
 : acs
SSH/FTP : ASCII
IOS :
```

TACACS+ :

```
IP Conn
-----
```

ステップ 5. AAA サーバ IP アドレスを設定し、キー入力して下さい:

```
8950A.7.PXM.a > cnfaaa TACACS+ - IP 10.66.79.246
yes/noyes
: cisco
: cisco
```

TACACS+ :

```
IP Conn
-----
10.66.79.246 49 5 0 Cisco
```

ステップ 6.:

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

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

```
-- { | | TACACS+ | cisco}
:
:
TACACS+: TACACS+
cisco: cisco
```

次にここに TACACS+ そしてローカルおよび Cisco をしています。（最終的な解決策として cisco があることをそこで推奨しますか。）

```
8950A.7.PXM.a > TACACS+ Cisco cnfaaa-authen
```

```
AAA:
```

```
: TACACS+ Cisco
: Cisco
:
: NOUSER_GP
: acs
SSH/FTP : ASCII
IOS :
```

```
/
```

ステップ 7. ほしい場合デフォルト特権レベルを設定して下さい。この例でそれを設定しません、すなわちデフォルトとしてそれを残します:

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

```
cnfaaa-priv <CISCO_GP | SERVICE_GP | SUPER_GP | GROUP1 | ANYUSER |
NOUSER_GP | default>
NOUSER_GP
```

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

```
AAA:
```

```
: TACACS+ Cisco
: TACACS+ Cisco
:
: NOUSER_GP
: acs
SSH/FTP : ASCII
IOS :
```

ステップ 8. 設定を確認して下さい:

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

```
AAA:
```

```
: TACACS+ Cisco
: TACACS+ Cisco
:
: NOUSER_GP
: acs
SSH/FTP : ASCII
IOS :
```

TACACS+ :

```
IP Conn
-----
-----
10.66.79.246 49 5 0 cisco
```

```
8950A.7.PXM.a > dspaaa
TACACS+ :
```

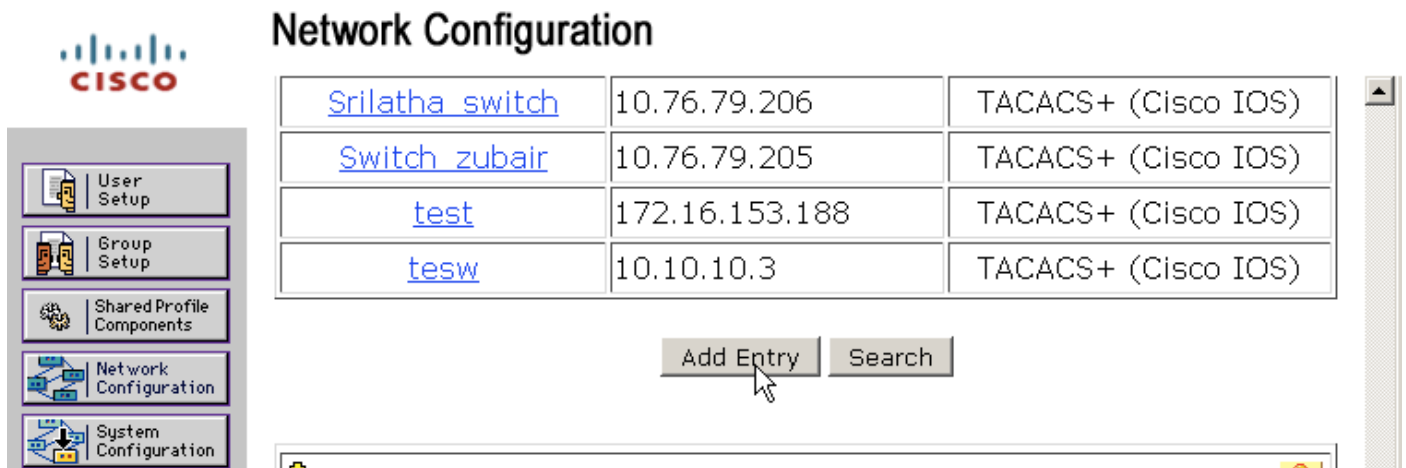
```
IP Conn
-----
-----
10.66.79.246 49 5 0 cisco
```

### ACS の設定

ACS で必要な設定の例がここに示されています:

**ステップ 1.** ACS のクライアントとして MGX を追加して下さい: (ここでは使用される名前は PXM\_MGX、何でもである場合もあります)

『Network Configuration』 をクリックして下さい  
(ここでは使用される名前は PXM\_MGX、何でもである場合もあります)

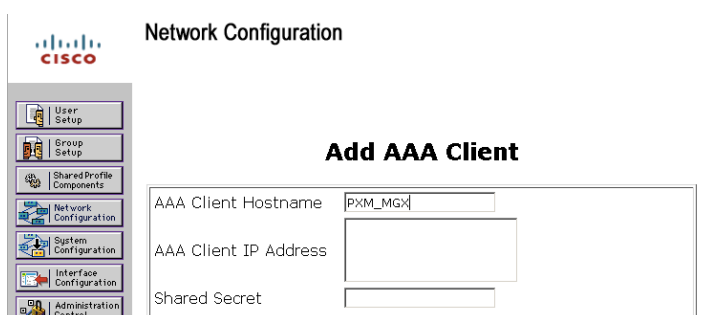


The screenshot shows the Cisco ACS Network Configuration page. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), and System Configuration. The main area displays a table of existing clients:

Client Name	IP Address	Protocol
<a href="#">Srilatha_switch</a>	10.76.79.206	TACACS+ (Cisco IOS)
<a href="#">Switch_zubair</a>	10.76.79.205	TACACS+ (Cisco IOS)
<a href="#">test</a>	172.16.153.188	TACACS+ (Cisco IOS)
<a href="#">tesw</a>	10.10.10.3	TACACS+ (Cisco IOS)

Below the table are two buttons: 'Add Entry' and 'Search'. A mouse cursor is pointing at the 'Add Entry' button.

**ステップ 2.** クライアント ホスト名を 『Add Entry』 をクリックし、設定して下さい-



The screenshot shows the 'Add AAA Client' configuration form. The left navigation menu is visible, with 'Network Configuration' selected. The form fields are:

- AAA Client Hostname:
- AAA Client IP Address:
- Shared Secret:

ステップ 3. AAA クライアント ( MGX の場合 ) の IP アドレスをおよび設定して下さい。キーか。 MGX 構成とどれが一致する必要があります ( ここでは使用されるキーはありますか。 cisco が ) 。

Network Configuration

AAA Client IP Address: 172.161.57.88

Shared Secret: cisco

**RADIUS Key Wrap**

Key Encryption Key: [ ]

Message Authenticator Code Key: [ ]

Key Input Format:  ASCII  Hexadecimal

Authenticate Using: TACACS+ (Cisco IOS)

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client
- Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Submit Submit + Apply Cancel

Submit+Apply をクリックして下さい

ステップ 4. ユーザを設定して下さい。『User Setup』 をクリックして下さい。このユーザは問い合わせられますか。 mgx\_test か。 を探します。新しいユーザ名を入力した後、『Add/Edit』 をクリックして下さい

User Setup

User: mgx\_test

Find Add/Edit

List users beginning with letter/number:

A B C D E F G H I J K L M  
N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9

List all users

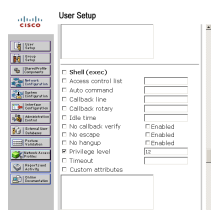
Remove Dynamic Users

Back to Help

ステップ 5. ユーザ向けのパスワードを設定して下さい。この例のパスワード「cisco」を設定します

ステップ 6. Shell (exec) の下でユーザの特権レベルを設定して下さい。ここにユーザは特権レベル 12 か Service\_GP を与えられます。

注 これは IOS 認証を用いる主な違いです。PXM を使うとユーザにイネーブル 特権を、むしろ私達割り当てています shell (exec) 特権を割り当てていません。



変更を保存するために『SUBMIT』をクリックして下さい。

## 確認

MGX への Telnet はユーザを得ます ACS サーバで設定した特権レベルを確認し、( すなわち SERVICE\_GP か 12 ) 特権レベル:

```
aptcwm02% telnet 172.16.157.88
172.16.157.88 ...
172.16.157.88
Escape character is '^]'.
mgx_test
cisco
```

8950A.7.PXM.a >

USERID

```
-----
-----
 7 0:00:14 cisco CISCO_GP 20:55:29 JUL28
telnet.01 * 7 0:00:00 mgx_test SERVICE_GP 10.66.69.126 21:04:11 JUL28
<<<
```

TACACS+ AAA:

8950A.7.PXM.a > dspaaa

: 07/28/2005 17:55:42 PST

```
authen: mgx_test telnet.01 10.66.69.126
        TACACS+ 10.66.79.246/49
        07/28/2005 21:27:34 PST
GRP priv:      mgx_test telnet.01 10.66.69.126
        TACACS+ 10.66.79.246/49
        07/28/2005 21:27:34 PST
cmd:
```

<CR> Q<CR>:

```
____SWITCH  COUNTS____
Method                cisco  TACACS
# authen:              0 18 0
# GRP :                0 0 0
# cmd :                0      0
# authen: 0 32 0
#: 0 1 0
# authen:  -----  -----  0
#:  -----  -----  0
# RX:                -----  -----  0
```



```

# : ----- 0
# TX: ----- 9
# RX: ----- 9
#: ----- 0
# : ----- 0
# AVP RX : ----- 2
# AVP RX: ----- 0
# AVP RX: ----- 0

```

<CR> Q<CR>:

```

_____TACACS+   COUNTS_____
[Server IP address] 10.66.79.246 0.0.0.0 0.0.0.0
:                49 0 0
# authen:         0 0 0
# cmd : 0 0 0
# authen: 0 0 0
#: 0 0 0
# authen: 0 0 0
#: 0 0 0
# RX: 0 0 0
# TX: 9 0 0
# RX: 9 0 0
#: 0 0 0
# : 0 0 0
# AVP RX : 2 0 0
# AVP RX: 0 0 0
# AVP RX: 0 0 0
Avg : 9 0 0
: 15 0 0

```

次のコマンドは MGX の TACACS と関連しています:

M7.8.PXM.a > AAA

```

-----
cnfaaa-authen
cnfaaa
cnfaaa-ftpssh
cnfaaa ios
cnfaaa-priv
cnfaaa
cnfaaa
delaaa
dspaaa
dspaaa
dspaaa
dspaaa TAC
setaaa TAC

```

## 関連情報

- [Cisco MGX 8800/8900 シリーズ ソフトウェア コンフィギュレーション ガイド、リリース 5.4](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)