Contenido

Introducción

Este documento describe un procedimiento paso a paso de agregar el servicio de autenticación del Terminal Access Controller Access Control System (TACACS+) en la revisión corriente del software del switch de Cisco MGX 8850/8950/8830 mayor de 5.0, con la versión 4.2 y posterior del Access Control Server de Cisco (ACS).

Prerrequisitos

Requisitos

Cisco recomienda que usted cumple este los requisitos antes de que usted intente esta configuración:

- ¿? El servidor de AAA es accesible del MGX

Componentes Utilizados

Este documento se restringe a la revisión corriente del software del switch de Cisco MGX 8850/8950/8830 mayor de 5.0 y con el ACS versión sobre 4.2.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Configuración en el MGX

Un ejemplo de la configuración requerida en el MGX se muestra aquí

Paso 1. Verifique la versión de software de switch. Usted necesita la versión 5.0 o posterior configurar el TACACS+

```
8950A.7.PXM.a > dspversion
 Versión del tipo de placa del tipo del estante del tipo de
imagen construida encendido
 ----------   ----------   ----------    ------------   ------------
   Runtime MGX PXM45 5.1(20.200) 23 de junio 2005, 21:36:08
     Inicio MGX PXM45 4.0(0.11)P2 -
```

Paso 2. Verifiquele tienen la dirección IP correcta:

```
8950A.7.PXM.a > dspifip
  Addr del broadcast del subnet mask de la dirección IP del indicador de
la interfaz
  ---------------  ----  ---------------  ---------------  --------------
-
  Ethernet/lnPci0 SUBEN 10.66.69.57 255.255.255.128 10.255.255.255
   SLIP/sl0 SUBEN 127.0.0.2 255.0.0.0 (N/A)
   ATM/atm0 ABAJO 0.0.0.0 0.0.0.0 (N/A)
```

Paso 3. Verifiquele puede hacer ping al servidor ACS: (El servidor ACS está en 10.106.60.182)

```
8950A.7.PXM.a > ping 10.106.60.182
PING 10.106.60.182: 56 bytes de datos
64 bytes de 10.106.60.182: icmp_seq=0. time=250. ms
64 bytes de 10.106.60.182: icmp_seq=1. time=240. ms
64 bytes de 10.106.60.182: icmp_seq=2. time=240. ms
----10.106.60.182 Estadísticas del PING----
3 paquetes transmitidos, 3 paquetes recibidos, pérdida del paquete del
0%
minuto ida-vuelta (del ms)/avg/= 240/243/250 máximo
```

¿Si doesn del ping? t va a través, nosotros necesita marcar el alcance IP. También verifique el **dspifip** y el **bootchange** se configura con la dirección IP correcta.

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

“.” = campo claro;  “-” = vaya al campo anterior;  ^D = salido

dispositivo de arranque: lnPci0
número del procesador: 0
nombre del host:
nombre del archivo:
```

```
inet en los Ethernetes (e): 172.16.157.88 >>
inet en el backplane (b):
inet del host (h):
(G) del inet del gateway: 172.16.157.1 >>
usuario (u):
contraseña ftp (picovatio) (espacio en blanco = uso rsh):
indicadores (f): 0x0
nombre objetivo (tn):
secuencia de mandos del inicio (s):
el otro (o):
```

Nota: Marque la configuración de los parámetros del dspifip y cambió el IP Address principal de la Administración de redes para interconectar el IP LAN y el ATM Address como secundario (usando el **cnfndparm**). También usted necesita configurar los parámetros del bootchange que ponen la dirección IP correcta y el gateway LAN. La salida de comando del **routeshow** debe indicar el default gateway para 0.0.0.0 como dirección IP LAN.

Paso 4. Verifique la configuración AAA usando el **dspaaa.** Por abandono no se configura ningún AAA

```
8950A.7.PXM.a > dspaaa
CONFIGURACIÓN AAA:
 Métodos de autentificación:  Cisco local
 Métodos de autorización:  Cisco local
 Tipo de autorización:  grupo
 Nivel de privilegio predeterminado:  NOUSER_GP
 Visualización pronto:  acs
 Tipo de mensaje SSH/FTP:  Ingreso de ASCII entrante
 Lista de la exclusión IOS:

SERVIDORES TACACS+:    primario se muestra primero

          Tiempo absolutamente solo
 El puerto de la dirección IP hacia fuera mide el tiempo de la clave de
encripción compartida las conec
---------------  ----  ---  ----  ------ ------------------------------
--------
```

Paso 5. Configure la dirección IP y la clave del servidor de AAA:

```
8950A.7.PXM.a > cnfaaa-servidor tacacs+ - IP 10.66.79.246
¿Usted quiere cambiar la clave de encripción (sí/no)? sí
Ingrese la clave de encripción: Cisco
Entre la clave de encripción de nuevo: Cisco

SERVIDORES TACACS+:    primario se muestra primero

          Tiempo absolutamente solo
 El puerto de la dirección IP hacia fuera mide el tiempo de la clave de
encripción compartida las conec
---------------  ----  ---  ----  ------ ------------------------------
--------
```

```
10.66.79.246 49 5 0 Cisco verdaderos
```

Paso 6. Autenticación de la configuración:

```
8950A.7.PXM.a > cnfaaa-authen
Sintaxis: cnfaaa-authen el [<method>…] del <method>

   método -- {local | predeterminado | tacacs+ | Cisco}
     local: Utilice la base de datos local para la autenticación.
    valor por defecto: Lo mismo que el local.
    tacacs+: Utilice el protocolo TACACS+ para la autenticación.
    Cisco: Solamente se permite al usuario raíz de "Cisco" iniciar
sesión.
```

Aquí estamos haciendo el Local y entonces Cisco TACACS+ entonces. (Se recomienda para tener Cisco como último recurso adentro allí?)

```
8950A.7.PXM.a > cnfaaa-authen el local Cisco tacacs+
CONFIGURACIÓN AAA:
 Métodos de autentificación:  local Cisco tacacs+
 Métodos de autorización:  Cisco local
 Tipo de autorización:  grupo
 Nivel de privilegio predeterminado:  NOUSER_GP
 Visualización pronto:  acs
 Tipo de mensaje SSH/FTP:  Ingreso de ASCII entrante
 Lista de la exclusión IOS:
```

ADVERTENCIA: La autenticación/los métodos de autorización nuevamente configurados se aplica a las nuevas sesiones. Esta configuración no tiene ningún impacto en las sesiones existentes.

Paso 7. Configure el nivel de privilegio predeterminado si usted quiere. No lo configuramos en este ejemplo, es decir lo dejamos como valor por defecto:

```
8950A.7.PXM.a > cnfaaa-priv
Sintaxis: cnfaaa-priv <CISCO_GP | SERVICE_GP | SUPER_GP | GROUP1 |
ANYUSER |
         NOUSER_GP | default>
         (NOTA: el "valor por defecto" es lo mismo que NOUSER_GP.)

valor por defecto 8950A.7.PXM.a > del cnfaaa-priv
CONFIGURACIÓN AAA:
 Métodos de autentificación:  local Cisco tacacs+
 Métodos de autorización:  local Cisco tacacs+
 Tipo de autorización:  grupo
 Nivel de privilegio predeterminado:  NOUSER_GP
 Visualización pronto:  acs
 Tipo de mensaje SSH/FTP:  Ingreso de ASCII entrante
 Lista de la exclusión IOS:
```

Paso 8. Verifique la configuración:

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

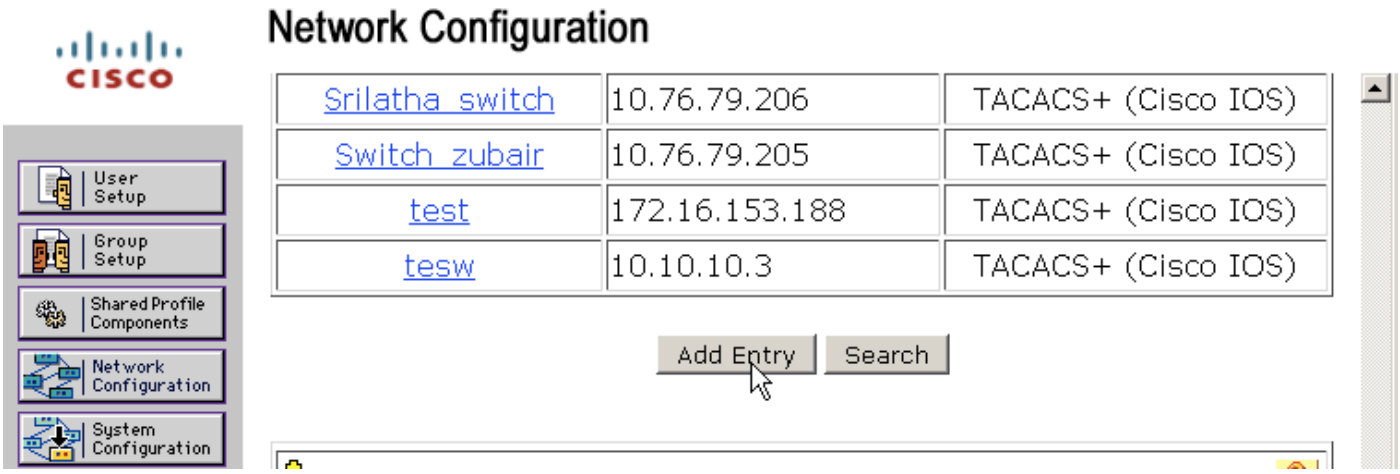
```
CONFIGURACIÓN AAA:
 Métodos de autentificación:  local Cisco tacacs+
 Métodos de autorización:  local Cisco tacacs+
 Tipo de autorización:  grupo
 Nivel de privilegio predeterminado:  NOUSER_GP
 Visualización pronto:  acs
 Tipo de mensaje SSH/FTP:  Ingreso de ASCII entrante
 Lista de la exclusión IOS:

SERVIDORES TACACS+:    primario se muestra primero

          Tiempo absolutamente solo
 El puerto de la dirección IP hacia fuera mide el tiempo de la clave de
encripción compartida las conec
---------------  ----  ---  ----  ------ ------------------------------
--------
10.66.79.246 49 5 0 Cisco verdaderos

8950A.7.PXM.a > dspaaa-servidores
SERVIDORES TACACS+:    primario se muestra primero

          Tiempo absolutamente solo
 El puerto de la dirección IP hacia fuera mide el tiempo de la clave de
encripción compartida las conec
---------------  ----  ---  ----  ------ ------------------------------
--------
10.66.79.246 49 5 0 Cisco verdaderos
```

Configuración en el ACS

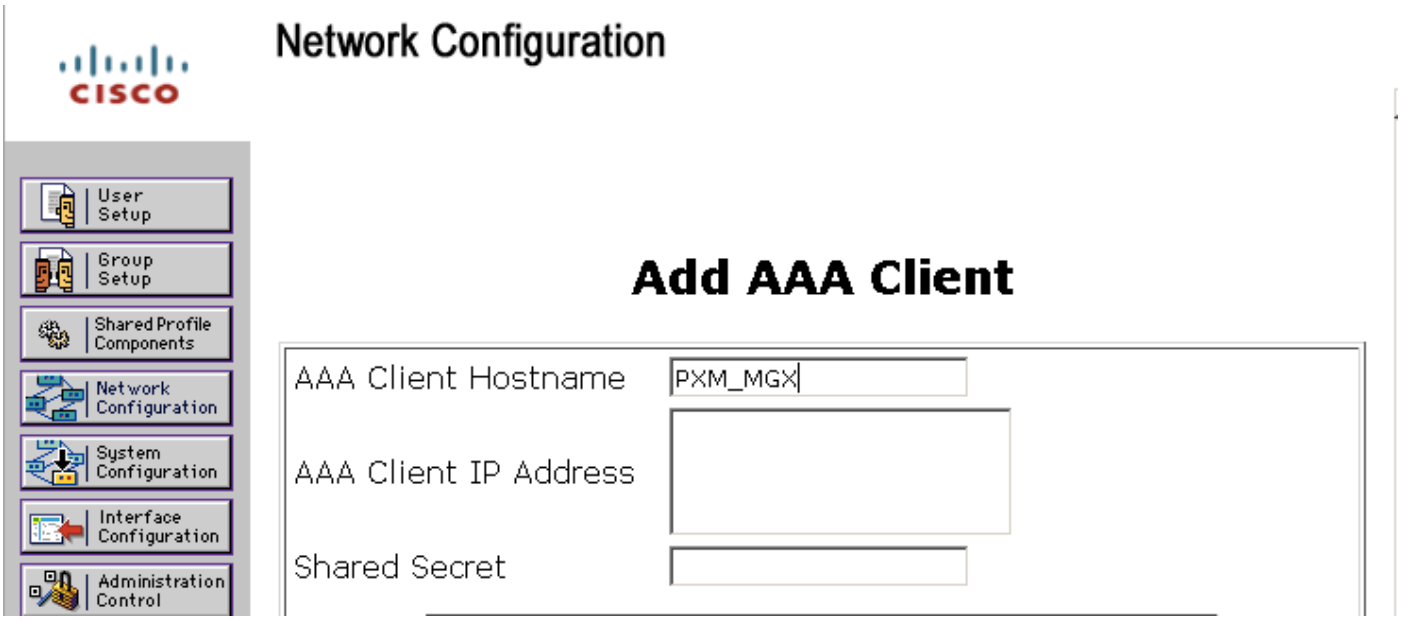
Un ejemplo de la configuración requerida en el ACS se muestra aquí:

Paso 1. Agregue el MGX como cliente en el ACS: (el nombre usado aquí es PXM_MGX, puede ser cualquier cosa)

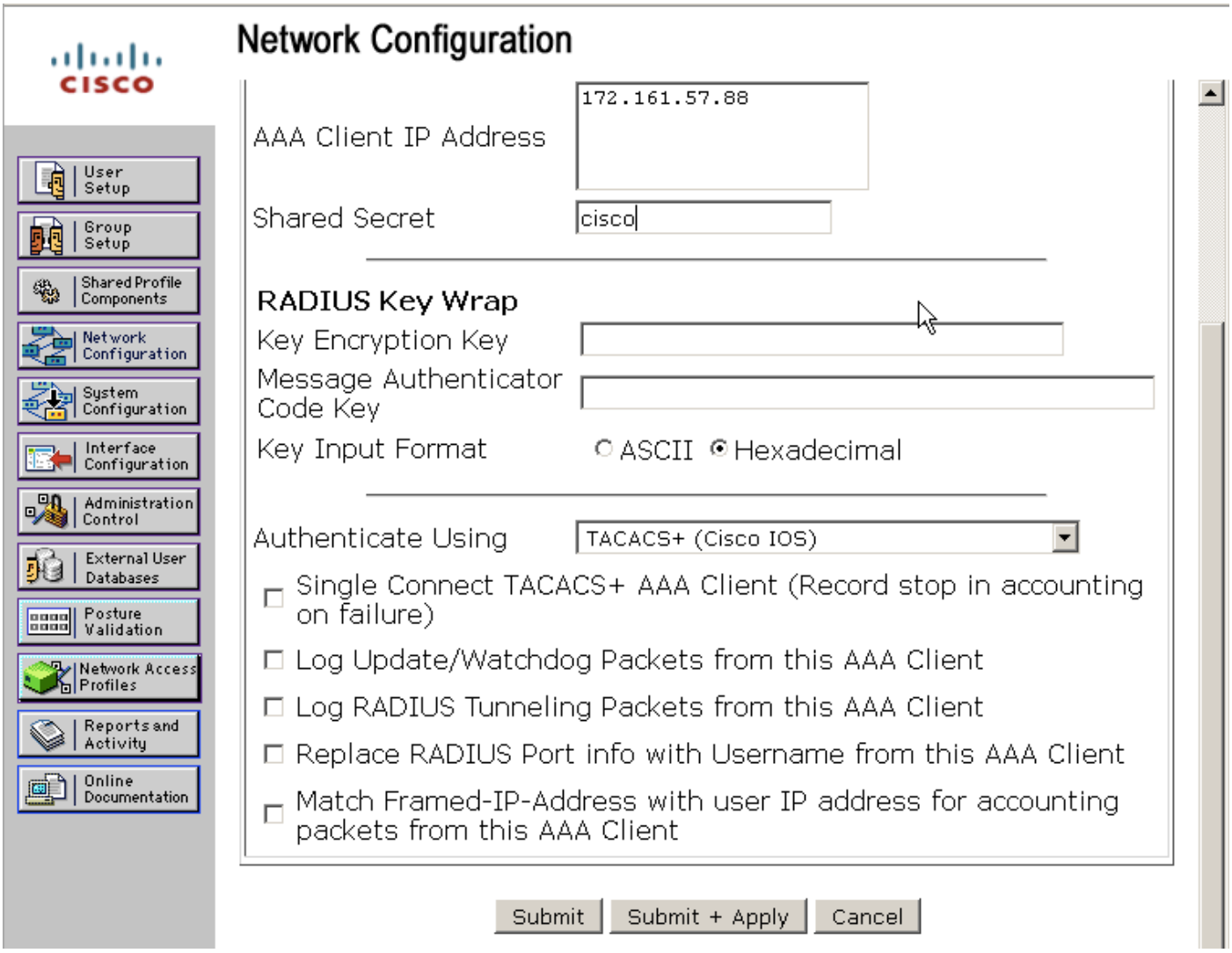
Haga clic en la **configuración de red**
(el nombre usado aquí es PXM_MGX, puede ser cualquier cosa)



Paso 2. El tecleo **agrega el** nombre de host del cliente de la **entrada** y de la configuración

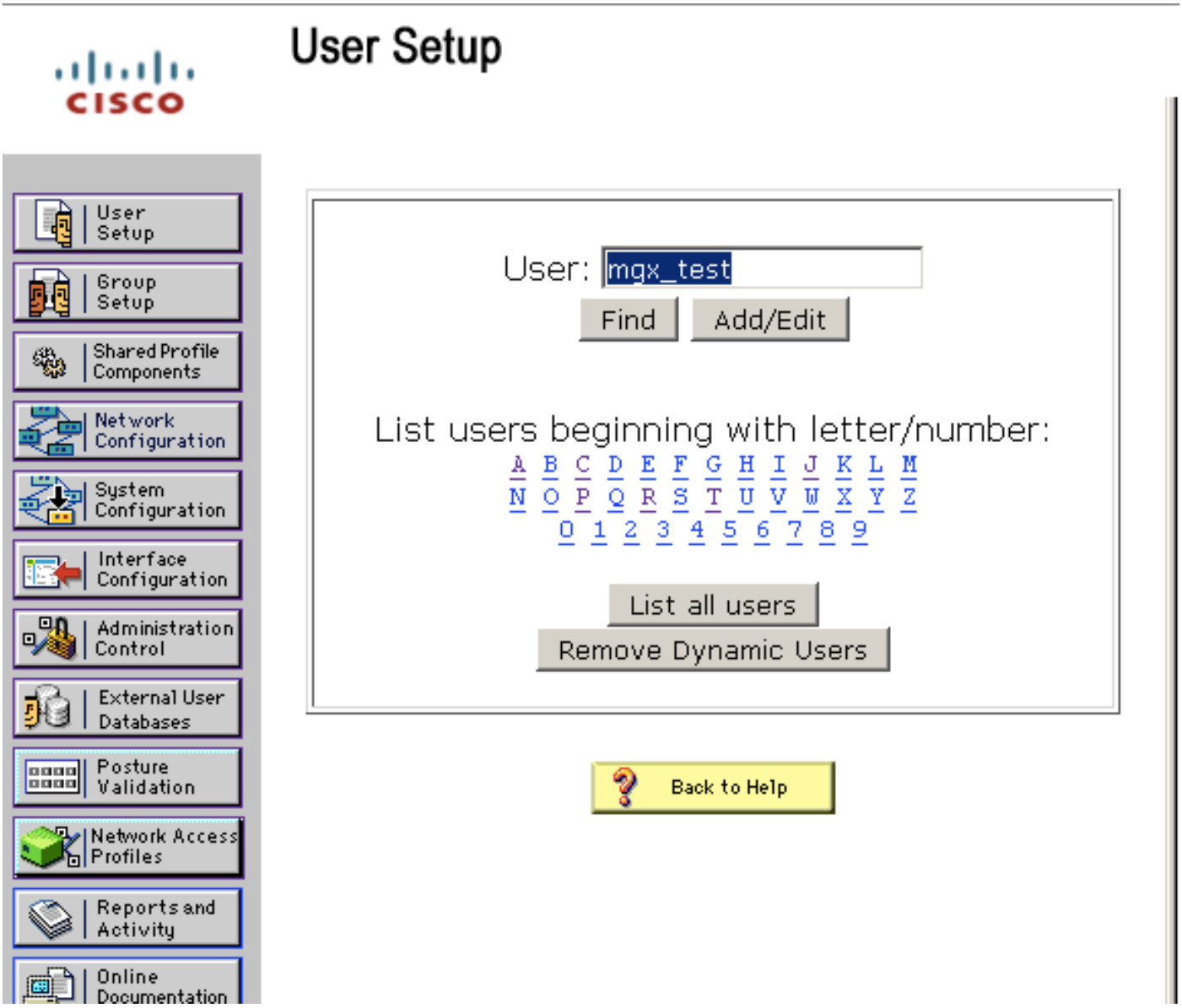


Paso 3. ¿Configure la dirección IP del cliente AAA (**MGX** en este caso) y? ¿**clave**? ¿cuál debe hacer juego con los config MGX (la clave usada aquí es? **Cisco**?).

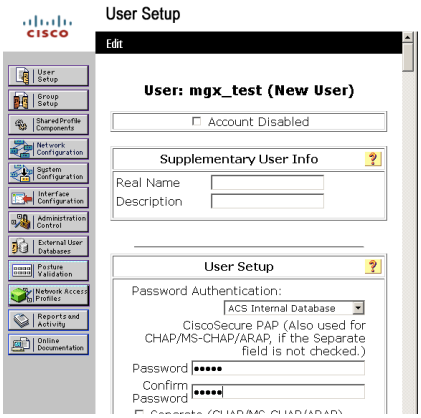


Tecleo **Submit+Apply**

Paso 4. Configure a un USUARIO. Haga clic en la **configuración de usuario.** ¿Llaman el usuario aquí? ¿el más mgx_test? . El tecleo **agrega/edita**, después de teclear en un nuevo nombre de usuario

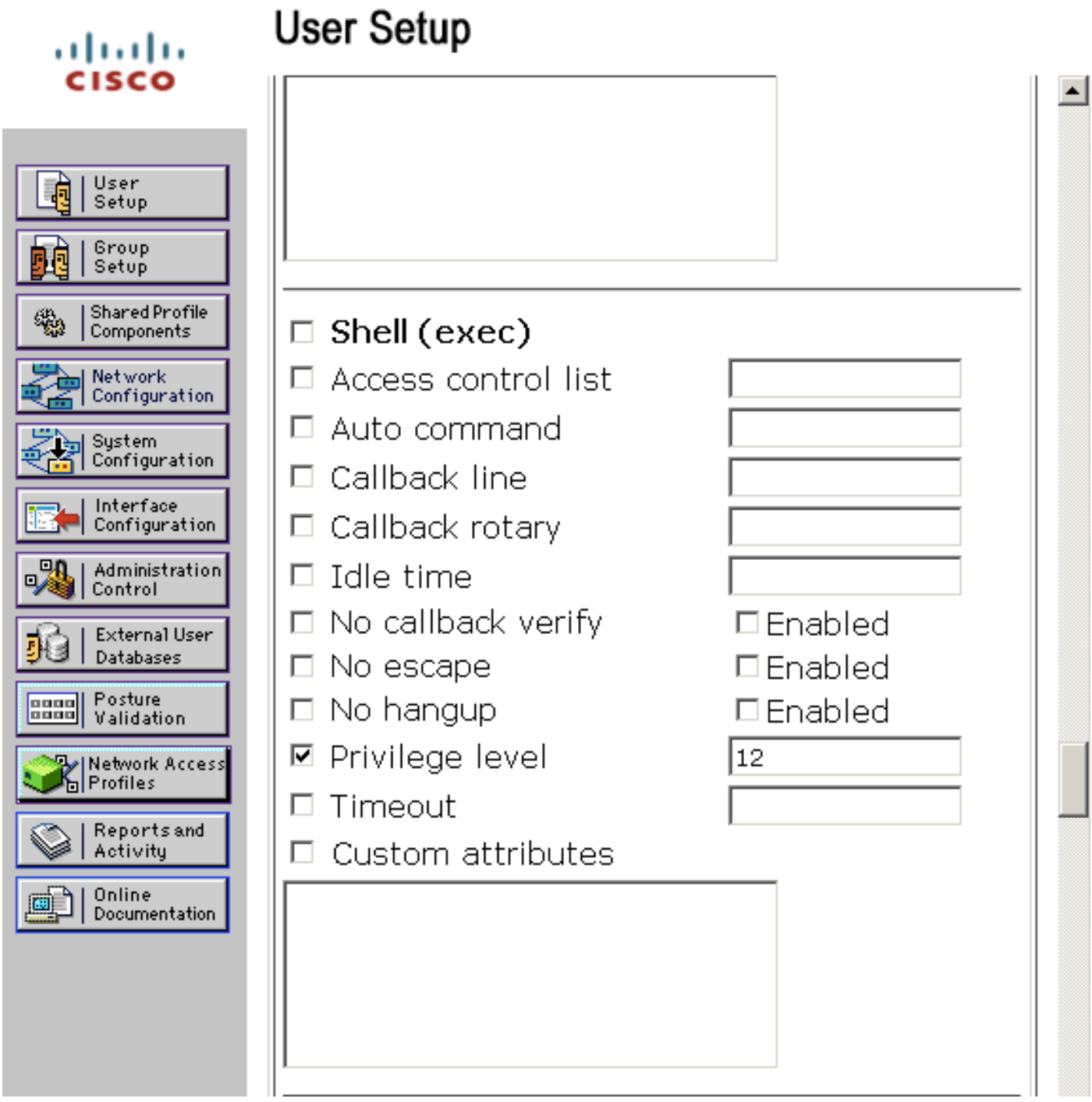


Paso 5. Configure una contraseña para el usuario. Configuramos una contraseña “**Cisco**” en este ejemplo



Paso 6. Ponga el nivel de privilegio del usuario bajo **shell (exec)**. Aquí dan el usuario el nivel de privilegio 12 o Service_GP.

Nota: Ésta es la diferencia principal con la autenticación IOS. Con el PXM no estamos asignando el privilegio del permiso, nosotros estamos asignando bastante el privilegio del shell (exec) al usuario.



El tecleo **somete** para confiar los cambios.

Verificación

Telnet al MGX y se asegura que el usuario consiga el nivel de privilegio que configuramos en el

servidor ACS (es decir SERVICE_GP o el nivel de privilegio 12):

```
telnet 172.16.157.88 del aptcwm02%
Intentando 172.16.157.88…
Conectado con 172.16.157.88.
El carácter de escape es "^]".
Nombre de usuario: el más mgx_test
Contraseña Cisco


8950A.7.PXM.a > quién

Acceso UserId de la marcha lenta del slot del puerto de comenzado en
-------------------------------------------------------------------
-------
puerto de la consola 20:55:29 JUL28 de la consola 7 0:00:14 Cisco
CISCO_GP
telnet.01 * 7 el <<< más mgx_test de 0:00:00 SERVICE_GP 10.66.69.126
21:04:11 JUL28
```

Marque el stats AAA para ver autenticación de TACACS+ el suceso:

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

Último borrado encendido: 07/28/2005 17:55:42 (PST)


El buen login más reciente authen: el telnet.01 más
mgx_test 10.66.69.126
           tacacs+ 10.66.79.246/49
           07/28/2005 21:27:34 (PST)
El buen priv más reciente del grp:     el telnet.01 más
mgx_test 10.66.69.126
           tacacs+ 10.66.79.246/49
           07/28/2005 21:27:34 (PST)
Cmd fallado último:        NINGUNO

Teclee <CR> para continuar, Q<CR> a parar:

NIVEL COUNTS__ ____SWITCH
Método:                 Cisco TACACS local
# authen los errores:      0 18 0
# errores del autor del grp:  0 0 0
# errores del autor del cmd:  0                 -----             0
# authen las caídas de nuevo a: 0 32 0
# el autor recurre a: 0 1 0
# authen inalcanzable:   -----             -----             0
# autor inalcanzable:   -----             -----             0
# desafíos RX:        -----             -----             0
# válvulas reguladoras del socket:     -----             -----
            0
# mensajes TX:          -----             -----             9
# mensajes RX:          -----             -----             9
```

```
# mensajes vaciados:     -----              -----              0
# mensajes del aborto enviados:  -----              -----              0
# AVP soportados RX:    -----              -----              2
# AVP sin apoyo RX:  -----              -----              0
# AVP desconocidos RX:      -----              -----              0

Teclee <CR> para continuar, Q<CR> a parar:

NIVEL COUNTS__ DEL SERVIDOR ____TACACS+
Dirección IP del servidor:       10.66.79.246 0.0.0.0 0.0.0.0
Puerto de servidor:             49 0 0
# authen los errores:       0 0 0
# errores del autor del cmd:  0 0 0
# authen las caídas de nuevo a: 0 0 0
# el autor recurre a: 0 0 0
# authen inalcanzable:    0 0 0
# autor inalcanzable:    0 0 0
# desafíos RX:         0 0 0
# mensajes TX:           9 0 0
# mensajes RX:           9 0 0
# mensajes vaciados:      0 0 0
# mensajes del aborto enviados:  0 0 0
# AVP soportados RX:    2 0 0
# AVP sin apoyo RX:  0 0 0
# AVP desconocidos RX:       0 0 0
Retardo de la respuesta del avg:      9 0 0
Retardo máximo de la respuesta:      15 0 0
```

Los siguientes comandos se relacionan con el TACACS en el MGX:

```
¿M7.8.PXM.a >? aaa

  Comandos disponibles
  ------------------
  cnfaaa-authen
  cnfaaa-autor
  cnfaaa-ftpssh
  cnfaaa-ignorar-IOS
  cnfaaa-priv
  cnfaaa-prompt
  cnfaaa-servidor
  delaaa-servidor
  dspaaa
  dspaaa-servidores
  dspaaa-stats
  dspaaa-TAC-traza
  setaaa-TAC-traza
```

Información Relacionada

- 8800/8900 Series guía de configuración de software de Cisco MGX, versión 5.4
- Soporte Técnico y Documentación - Cisco Systems