

Cisco Cache Engine を介した RADIUS 認証の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[表記法](#)

[キャッシュエンジンによるRADIUS認証の設定手順](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

概要

このドキュメントでは、キャッシュ エンジンを使用して Microsoft Windows NT 用の Cisco Secure Access Control Server (ACS) に対する RADIUS 認証を設定する方法を説明します。この手順を正しく実行するには、Web Cache Communication Protocol バージョン 2 (WCCPv2) を実行する必要があります。WCCP バージョン 2 の詳細については、『Configuring Web Cache Communication Protocol Version 2 on a Cisco Cache Engine and Router』を参照してください。

前提条件

要件

この設定を開始する前に、次の要件が満たされていることを確認してください。

- Cisco Secure ACS for WindowsまたはUNIXに精通していること。
- ルータとキャッシュエンジンの両方のWCCPv2設定に精通していること。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

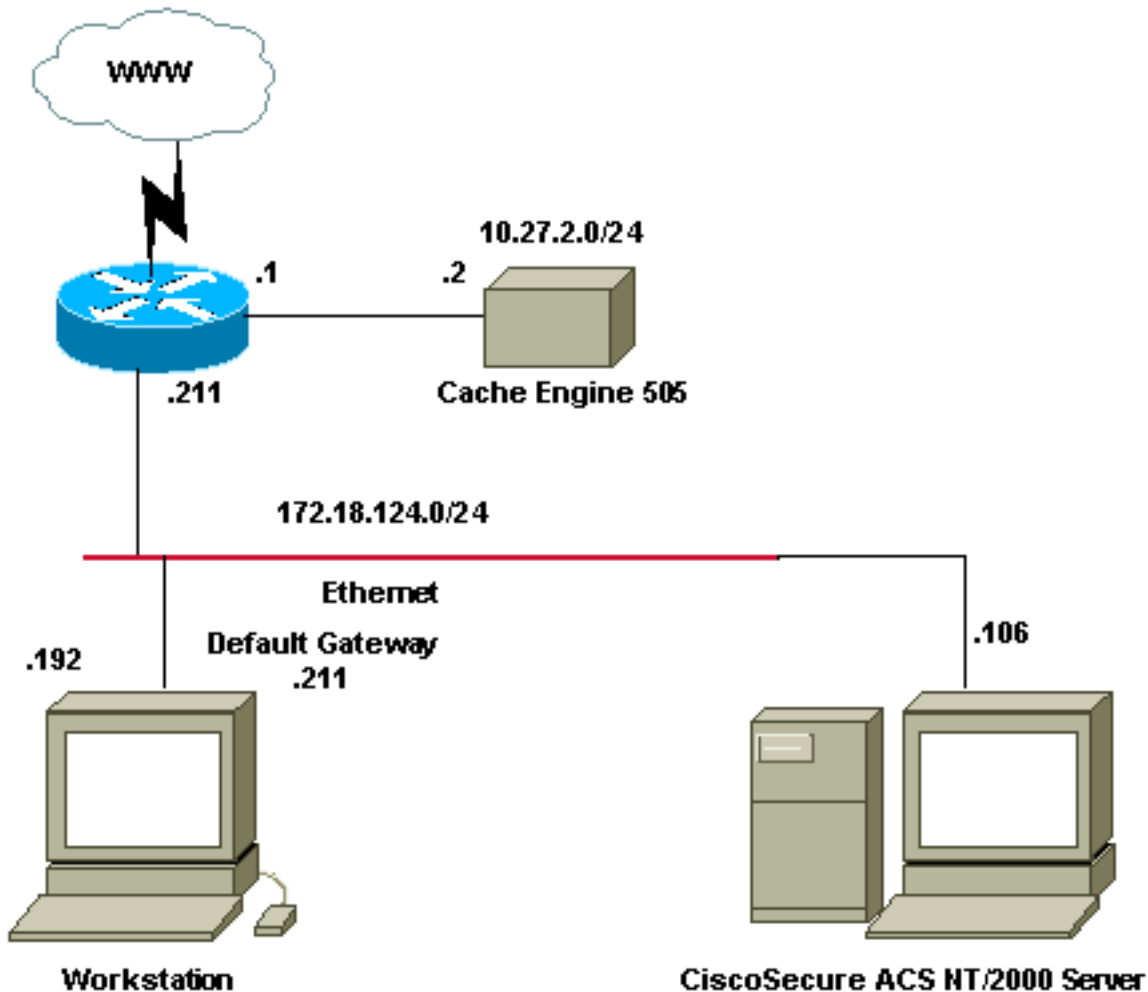
- 設定がクリアなラボ環境でのCisco Cache Engine 505
- Cisco 2600 ルータ
- Cisco Cache Engineソフトウェアリリース2.31

- Cisco IOS®ソフトウェアリリース12.1(3)T3
- Cisco Secure ACS for Microsoft Windows NT/2000 Servers

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



表記法

ドキュメント表記の詳細は、「[シスコテクニカルティップスの表記法](#)」を参照してください。

キャッシュエンジンによるRADIUS認証の設定手順

RADIUS認証用にキャッシュエンジンを設定するには、次の手順を使用します。

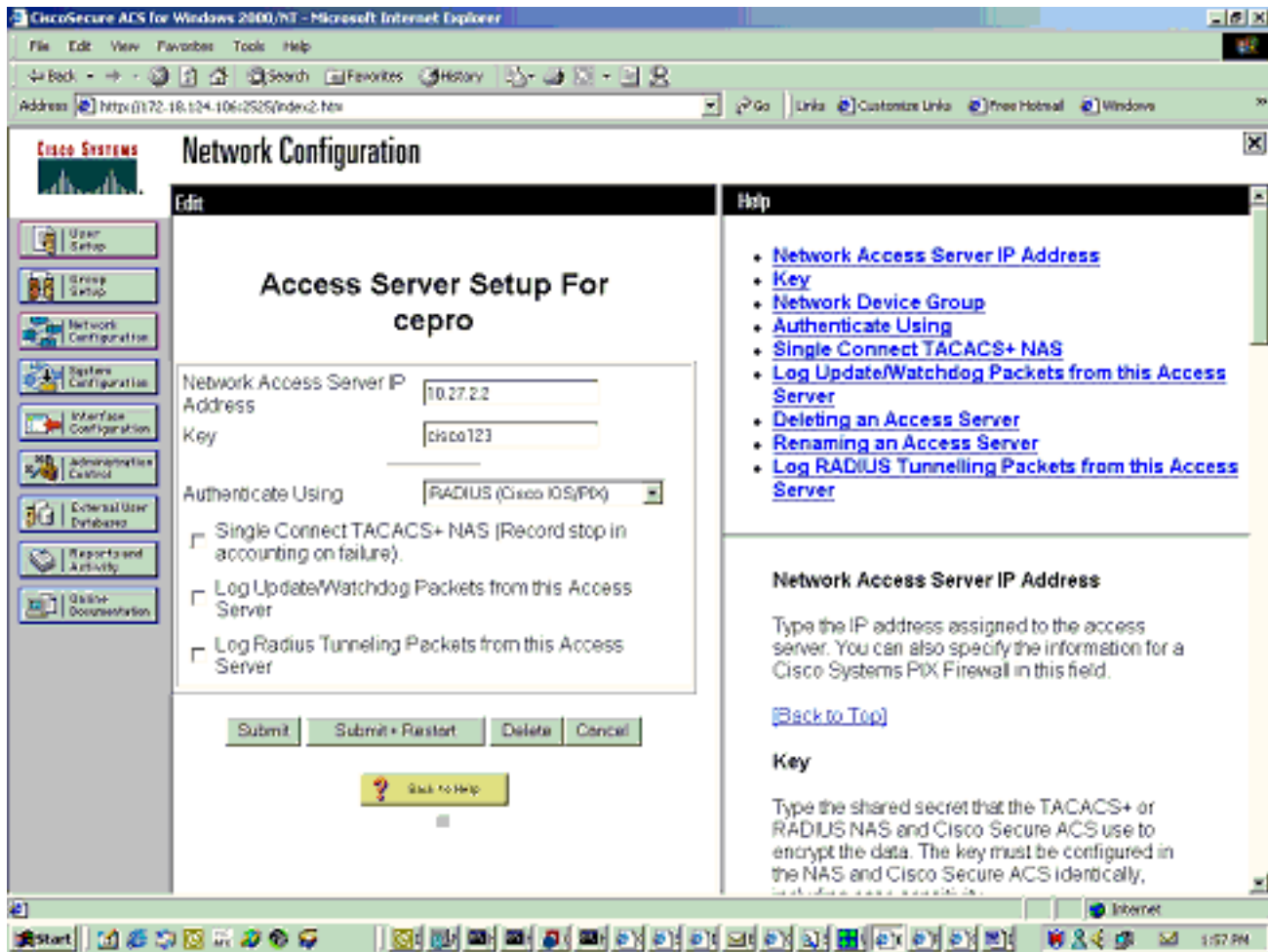
1. Cisco Secure ACS for Windows NTで、Cache Engineをネットワークアクセスサーバ (NAS)として設定します。
2. Cisco Secure ACS for Windows NTでユーザ情報を設定します。
3. RADIUS用のキャッシュエンジンを設定し、ホストとキーの情報を指定します。

```
radius-server host 172.18.124.106
radius-server key cisco123
```

4. WCCP用にルータを設定します。キャッシュエンジンのコマンドラインは次のようになります。

```
cepro#configure terminal
!--- Enter configuration commands, one per line. !--- End with CNTL/Z.
cepro(config)#radius-server host 172.18.124.106
cepro(config)#radius-server key cisco123
cepro#
```

次に、Cisco Secure ACS for Windows NTのキャッシュエンジン/NAS設定を示します。



これは、Cisco Secure ACS for Windows NTの[User Setup]ページです。

CiscoSecure ACS for Windows 2000/NT - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites History

Address http://172.18.124.106:2525/index2.htm

CISCO SYSTEMS User Setup

User Setup

Group Setup

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Database

Reports and Activity

Online Documentation

Edit

User: chbanks

Account Disabled

Supplementary User Info

Real Name

Description

User Field 3

User Setup

Password Authentication:
CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

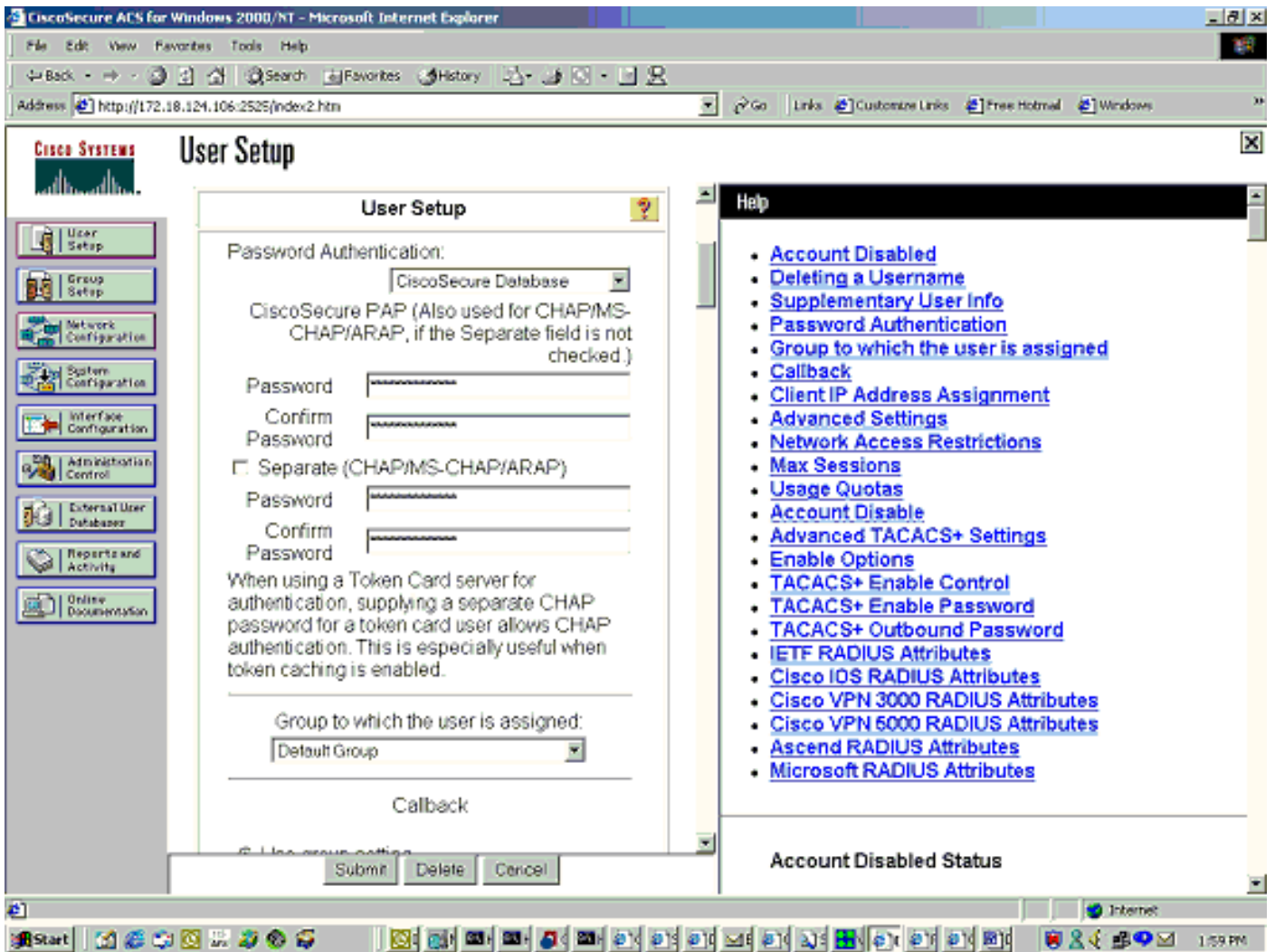
Submit Delete Cancel

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Advanced TACACS+ Settings
- Enable Options
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- IETF RADIUS Attributes
- Cisco IOS RADIUS Attributes
- Cisco VPN 3000 RADIUS Attributes
- Cisco VPN 5000 RADIUS Attributes
- Ascend RADIUS Attributes
- Microsoft RADIUS Attributes

Account Disabled Status

Start Internet 1:50 PM



確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

一部の show コマンドは[アウトプット インタープリタ ツール](#)によってサポートされています ([登録ユーザ専用](#))。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

Cache Engine のコマンド :

- **show version** : キャッシュエンジンで実行されているソフトウェアバージョンを表示します。
- **show hardware** : キャッシュエンジンのソフトウェアバージョンとハードウェアタイプの両方を表示します。
- **show running-config** : キャッシュエンジンの実際の実行コンフィギュレーションを表示します。
- **show stat http usage** : 使用状況の統計情報を表示します。
- **show radius stat [all |プライマリ | secondary]** : プライマリおよびセカンダリRADIUSサーバの認証統計情報を表示します。

show version コマンドの出力例を次に示します。

```
cepro#show version
```

```
Cisco Cache Engine
Copyright (c) 1986-2001 by Cisco Systems, Inc.
Software Release: CE ver 2.31 (Build: FCS 02/16/01)
Compiled: 11:20:14 Feb 22 2001 by bbalagot
Image text-base 0x108000, data_base 0x437534
```

```
System restarted by Reload
The system has been up for 3 hours, 52 minutes, 33 seconds.
System booted from "flash"
```

show hardwareコマンドの出力例を次に示します。

```
cepro#show hardware
Cisco Cache Engine
Copyright (c) 1986-2001 by Cisco Systems, Inc.
Software Release: CE ver 2.31 (Build: FCS 02/16/01)
Compiled: 11:20:14 Feb 22 2001 by bbalagot
Image text-base 0x108000, data_base 0x437534
```

```
System restarted by Reload
The system has been up for 3 hours, 52 minutes, 54 seconds.
System booted from "flash"
```

```
Cisco Cache Engine CE505 with CPU AMD-K6 (model 8) (rev. 12) AuthenticAMD
2 Ethernet/IEEE 802.3 interfaces
1 Console interface.
134213632 bytes of Physical Memory
131072 bytes of ROM memory.
8388608 bytes of flash memory.
```

```
List of disk drives:
 /c0t0d0 (scsi bus 0, unit 0, lun 0)
```

show running-configコマンドの出力例を次に示します。

```
cepro#show running-config
Building configuration...
Current configuration:
!
!
logging recycle 64000
logging trap information
!
user add admin uid 0 password 1 "eeSdy9dcy" capability admin-access
!
!
!
hostname cepro
!
interface ethernet 0
 ip address 10.27.2.2 255.255.255.0
 ip broadcast-address 10.27.2.255
exit
!
!
interface ethernet 1
exit
!
ip default-gateway 10.27.2.1
ip name-server 161.44.11.21
ip name-server 161.44.11.206
```

```

ip domain-name cisco.com
ip route 0.0.0.0 0.0.0.0 10.27.2.1
cron file /local/etc/crontab
!
bypass timer 1
!--- Specify the router list for use with WCCPv2. wccp router-list 1 10.27.2.1 172.18.124.211
!--- Instruct the router to run web cache service with WCCPv2. wccp web-cache router-list-num 1
!--- WCCPv2 enabled. wccp version 2
!!--- RADIUS Server host and port is defined. radius-server host 172.18.124.106 auth-port 1645
radius-server host 172.18.124.103 auth-port 1645
!--- RADIUS key defined. radius-server key ****
authentication login local enable
authentication configuration local enable
transaction-logs enable
rule no-cache url-regex .*cgi-bin.*
rule no-cache url-regex .*aw-cgi.*
!
!
end
cepro#

```

ルータのコマンド：

- **show running-config**：ルータの実際の実行コンフィギュレーションを表示します。
- **show ip wccp**：すべての登録済みサービスを表示します。
- **show ip wccp <service-id> detail**：クラスタ内の各キャッシュのWCCPバケット分配を表示します。たとえば、**show ip wccp web-cache detail**と入力します。

show running-configコマンドの出力例を次に示します。

```

33-ns-gateway#show running-config
Building configuration...
Current configuration:
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 33-Ns-gateway
!
logging buffered 64000 debugging
enable secret 5 $1$IWJr$Nl.NcIr/b9DN7jEQQC17R/
!
!
!
!
!
ip subnet-zero
!--- WCCP enabled. ip wccp web-cache
ip cef
no ip domain-lookup
ip domain-name testdomain.com
ip name-server 161.44.11.21
ip name-server 161.44.11.206
!
!
!
!
interface Ethernet0/0
ip address 10.1.3.50 255.255.255.0
no ip route-cache cef

```

```

!
interface Ethernet1/0
description interface to the CE .5
bandwidth 100
ip address 10.27.2.1 255.255.255.0
full-duplex
!
interface Ethernet1/1
description inter to DMZ
ip address 172.18.124.211 255.255.255.0
!--- Configure the interface to enable the router !--- to verify that the appropriate !-
-- packets are redirected to the cache engine. ip wccp web-cache redirect out
no ip route-cache cef
no ip route-cache
no ip mroute-cache
!
interface Ethernet1/2
description Preconfigured for recreates 10.27.3.0/24 net
ip address 10.27.3.1 255.255.255.0
no ip route-cache cef
!
interface Ethernet1/3
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
no ip http server
!
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
exec-timeout 0 0
line vty 0 4
exec-timeout 0 0
password ww
login
!
end
33-Ns-gateway#

```

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングのためのコマンド

一部の show コマンドは [アウトプット インタープリタ ツール](#) によってサポートされています ([登録ユーザ専用](#))。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

注 : debug コマンドを使用する前に、「[debug コマンドに関する重要な情報](#)」を参照してください。

Cache Engine のコマンド :

- debug authentication all all : 認証をデバッグします。

- **debug radius all all**: WebインターフェイスのRADIUSモジュールのデバッグを表示します。
- **type var/log/translog/working.log**: URLがキャッシュされていること、およびユーザがページにアクセスしていることを確認します。その他のタイプのメッセージについては、[Cisco Technical Support](#)を参照してください。このログのエラーメッセージの最も一般的なタイプは、不明なユーザ認証に失敗した。

次に、**debug radius all all**コマンドと**debug authentication all**コマンドの出力例を示します。

```

RadiusCheck(): Begin
RadiusCheck(): Begin
RadiusCheck(): Begin
RadiusBuildRequest(): Begin
RadiusBuildRequest(): Begin
RadiusBuildRequest(): Begin
[82] User-Name = "chbanks"
[82] User-Name = "chbanks"
[82] User-Name = "chbanks"
[82] NAS-IP-Address = 10.27.2.2
[82] NAS-IP-Address = 10.27.2.2
[82] NAS-IP-Address = 10.27.2.2
[82] NAS-Port = 80
[82] NAS-Port = 80
[82] NAS-Port = 80
RadiusAuthenticate(): Begin
RadiusAuthenticate(): Begin
RadiusAuthenticate(): Begin
CfgGetRadiusInfo(): Begin
CfgGetRadiusInfo(): Begin
CfgGetRadiusInfo(): Begin
UpdatePassword(): Begin
UpdatePassword(): Begin
UpdatePassword(): Begin
[82] radsend: Request to 172.18.124.106 id=1, length=171
[82] radsend: Request to 172.18.124.106 id=1, length=171
[82] radsend: Request to 172.18.124.106 id=1, length=171
RadiusReplyValidate(): Begin
RadiusReplyValidate(): Begin
RadiusReplyValidate(): Begin
RadiusReplyValidate(): [82] Received 26 byte message back
RadiusReplyValidate(): [82] Received 26 byte message back
RadiusReplyValidate(): [82] Received 26 byte message back
RadiusReplyValidate(): Got a valid response from server 172.18.124.106.
RadiusReplyValidate(): Got a valid response from server 172.18.124.106.
RadiusReplyValidate(): Got a valid response from server 172.18.124.106.
DecodeReply(): Begin
DecodeReply(): Begin
DecodeReply(): Begin
DecodeReply: WEB_YES_BLOCKING default
DecodeReply: WEB_YES_BLOCKING default
DecodeReply: WEB_YES_BLOCKING default
RadiusCheck(): WEB_YES_BLOCKING
RadiusCheck(): WEB_YES_BLOCKING
RadiusCheck(): WEB_YES_BLOCKING
RemoteUserAdd(): Begin
RemoteUserAdd(): Begin
RemoteUserAdd(): Begin
RemoteUserAdd(): Updated remote user chbanks
RemoteUserAdd(): Updated remote user chbanks
RemoteUserAdd(): Updated remote user chbanks
RemoteUserAuthenticate(): Begin
RemoteUserAuthenticate(): Begin

```

```
RemoteUserAuthenticate(): Begin
CfgGetRadiusInfo(): Begin
CfgGetRadiusInfo(): Begin
CfgGetRadiusInfo(): Begin
CfgRadiusGetExcludeState(): Begin
CfgRadiusGetExcludeState(): Begin
CfgRadiusGetExcludeState(): Begin
CfgRadiusGetExcludeState(): flag = 0
CfgRadiusGetExcludeState(): flag = 0
CfgRadiusGetExcludeState(): flag = 0
RemoteUserUpdate(): Begin
RemoteUserUpdate(): Begin
RemoteUserUpdate(): Begin
CfgRadiusGetMultipleUserPromptState(): Begin
CfgRadiusGetMultipleUserPromptState(): Begin
CfgRadiusGetMultipleUserPromptState(): Begin
CfgRadiusGetMultipleUserPromptState(): flag = 1
CfgRadiusGetMultipleUserPromptState(): flag = 1
CfgRadiusGetMultipleUserPromptState(): flag = 1
CfgRadiusGetMultipleUserPromptTimeout(): Begin
CfgRadiusGetMultipleUserPromptTimeout(): Begin
CfgRadiusGetMultipleUserPromptTimeout(): Begin
CfgRadiusGetMultipleUserPromptTimeout(): lMultipleUserPromptTimeout = 25
CfgRadiusGetMultipleUserPromptTimeout(): lMultipleUserPromptTimeout = 25
CfgRadiusGetMultipleUserPromptTimeout(): lMultipleUserPromptTimeout = 25
fsgetUsrInfoforIpAddr_radius will be called
fsgetUsrInfoforIpAddr_radius will be called
fsgetUsrInfoforIpAddr_radius will be called
RemoteUserUpdate() returned true
RemoteUserUpdate() returned true
```

RemoteUserUpdate() returned true

ルータコマンド :

- **show ip wccp** : グローバルな WCCP 統計情報を表示します。

関連情報

- [WCCP機能拡張](#)
- [ウェブ キャッシュ通信プロトコル バージョン 2](#)
- [テクニカルサポート - Cisco Systems](#)