Configuring TACACS+, RADIUS, and Kerberos on Cisco Catalyst Switches

Document ID: 13847

Contents

Introduction

The Cisco Catalyst family of switches (Catalyst 4000, Catalyst 5000, and Catalyst 6000 that run CatOS) has supported some form of authentication, which begins in the 2.2 code. Enhancements have been added with later versions. The TACACS+ TCP port 49, not XTACACS User Datagram Protocol (UDP) port 49), RADIUS, or Kerberos server user setup for authentication, authorization, and accounting (AAA) is the same as for router users. This document contains examples of the minimal commands necessary in order to enable these functions. Additional options are available in the switch documentation for the version in question.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Since later versions of code support additional options, you need to issue the **show version** command in order to determine the version of code on the switch. Once you have determined the version of code that is used on the switch, use this table in order to determine what options are available on your equipment, and which options you wish to configure.

Always remain in the switch when you add authentication and authorization. Test the configuration in another window in order to avoid being accidentally locked out.

Method (minimum)	**Cat Version 2.2 to 5.1**	**Cat Version 5.1 to 5.4.1**	**Cat Version 5.4.1 to 7.5.1**	**Cat Version 7.5.1 and later**
TACACS+ Authentication OR	Step A	Step A	Step A	Step A
RADIUS Authentication OR	N/A	Step B	Step B	Step B
Kerberos Authentication OR	N/A	N/A	Step K	Step K
Local Username Authentication/Authorization	N/A	N/A	N/A	Step C
Plus (options)				
TACACS+ Command Authorization	N/A	N/A	Step D	Step D
TACACS+ Exec Authorization	N/A	N/A	Step E	Step E
RADIUS Exec Authorization	N/A	N/A	Step F	Step F
Accounting − TACACS+ or RADIUS	N/A	N/A	Step G	Step G
TACACS+ Enable Authorization	Step H	Step H	Step H	Step H
RADIUS Enable Authorization	N/A	Step I	Step I	Step I
TACACS+ Enable Authorization	N/A	N/A	Step J	Step J

Configuration Steps

Step A − TACACS+ Authentication

With earlier versions of code, commands are not as complex as with some later versions. Additional options in later versions can be available on your switch.

1. Issue the **set authentication login local enable** command in order to make sure there is a back door into the switch if the server is down.
2. Issue the **set authentication login tacacs enable** command in order to enable TACACS+ authentication.
3. Issue the **set tacacs server #.#.#.#** command in order to define the server.
4. Issue the **set tacacs key** *your_key* command in order to define the server key, which is optional with TACACS+, as it causes switch−to−server data to be encrypted. If used, it must agree with the server.

   Note: Cisco Catalyst OS software does **not** accept the question mark (**?**) to be part of any keys or passwords. The question mark is explicitly used for help on the command syntax.

Step B − RADIUS Authentication

With earlier versions of code, commands are not as complex as with some later versions. Additional options in later versions can be available on your switch.

1. Issue the **set authentication login local enable** command in order to make sure there is a back door into the switch if the server is down.
2. Issue the **set authentication login radius enable** command in order to enable RADIUS authentication.
3. Define the server. On all other Cisco equipment, the default RADIUS ports are 1645/1646 (authentication/accounting).

   On the Catalyst, the default port is 1812/1813. If you use Cisco Secure or a server that communicates with other Cisco equipment, use the 1645/1646 port. Issue the **set radius server #.#.#.# auth−port 1645 acct−port 1646 primary** command in order to define the server and the equivalent command in the Cisco IOS as **radius−server source−ports 1645−1646**.
4. Define the server key.

   This is mandatory, as it causes the switch−to−server password to be encrypted as in the RADIUS Authentication/Authorization RFC 2865 and RADIUS Accounting RFC 2866 . If used, it must agree with the server. Issue the **set radius key** *your_key* command.

Step C − Local Username Authentication/Authorization

Starting in CatOS version 7.5.1, local user authentication is possible. For example, you can achieve authentication/authorization with the use of a username and password stored on the Catalyst, instead of authentication with a local password.

There are only two privilege levels for local user authentication, 0 or 15. Level 0 is the non−privileged exec level. Level 15 is the privileged enable level.

If you add these commands in this example, the user `poweruser` arrives in enable mode on a Telnet or console to the switch and the user `nonenable` arrives in exec mode on a Telnet or console to the switch.

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

Note: If the user `nonenable` knows the **set enable** password, that user can continue to enable mode.

After the configuration, the passwords are stored encrypted.

Local username authentication can be used in conjunction with remote TACACS+ exec, command accounting, or remote RADIUS exec accounting. It can also be used in conjunction with remote TACACS+

exec or command authorization, but it does not make sense to use it this way because the username needs to be stored both on the TACACS+ server as well as locally on the switch.

Step D − TACACS+ Command Authorization

In this example, the switch is told to require authorization for only configuration commands with TACACS+. In the event that the TACACS+ server is down, authentication is none. This applies to both the console port and Telnet session. Issue this command:

set authorization commands enable config tacacs none both

In this example, you can configure the TACACS+ server to permit when you set these parameters:

```
command=set
arguments (permit)=port 2/12
```

The **set port enable 2/12** command is sent to the TACACS+ server for verification.

Note: With command authorization enabled, unlike in the router where enable is not considered a command, the switch sends the **enable** command to the server when an enable is attempted. Make sure that the server is also configured to allow the **enable** command.

Step E − TACACS+ Exec Authorization

In this example, the switch is told to require authorization for an exec session with TACACS+. In the event that the TACACS+ server is down, authorization is none. This applies to both the console port and the Telnet session. Issue the **set authorization exec enable tacacs+ none both** command

In addition to the authentication request, this sends a separate authorization request to the TACACS+ server from the switch. If the user profile is configured for shell/exec on the TACACS+ server, that user is able to access the switch.

This prevents users without shell/exec service configured on the server, such as PPP users, from logging into the switch. You get a message that reads `Exec mode authorization failed`. In addition to permitting/denying exec mode for users, you can be forced into enable mode when you enter with the privilege level 15 assigned on the server. It must runcode in which Cisco bug ID CSCdr51314 (registered customers only) is fixed.

Step F − RADIUS Exec Authorization

There is no command to enable RADIUS exec authorization. The alternative is to set the Service−Type (RADIUS attribute 6) to Administrative (a value of 6) in the RADIUS server to launch the user into enable mode in the RADIUS server. If the service−type is set for anything other than 6−administrative, for example, 1−login, 7−shell, or 2−framed, the user arrives at the switch exec prompt, but not the enable prompt.

Add these commands in the switch for authentication and authorization:

```
aaa authorization exec TEST group radius
 line vty 0 4
 authorization exec TEST
 login authentication TEST
```

Step G − Accounting − TACACS+ or RADIUS

In order to enable TACACS+ accounting for:

1. If you get the switch prompt, issue the **set accounting exec enable start−stop tacacs+** command.
2. Users that Telnet out of the switch issue the **set accounting connect enable start−stop tacacs+** command.
3. If you reboot the switch, issue the **set accounting system enable start−stop tacacs+** command.
4. Users that perform commands, issue the **set accounting commands enable all start−stop tacacs+** command.
5. Reminders to the server, for example, to update records once a minute in order to show that the user is still logged in, issue the **set accounting update periodic 1** command.

In order to enable RADIUS accounting for:

1. Users that get the switch prompt, issue the **set accounting exec enable start−stop radius** command.
2. Users that Telnet out of the switch, issue the **set accounting connect enable start−stop radius** command.
3. When you reboot the switch, issue the **set accounting system enable start−stop radius** command.
4. Reminders to the server, for example, to update records once a minute in order to show that the user is still logged in, issue the **set accounting update periodic 1** command.

TACACS+ Freeware Records

This output is an example of how the records can appear on the server:

```
Fri Mar 24 13:22:41 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=5 start_time=953936729 timezone=UTC
service=shell disc−cause=2 elapsed_time=236
Fri Mar 24 13:22:50 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=15 start_time=953936975 timezone=UTC
service=shell priv−lvl=0 cmd=enable
Fri Mar 24 13:22:54 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=16 start_time=953936979 timezone=UTC
service=shell priv−lvl=15 cmd=write terminal
Fri Mar 24 13:22:59 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=17 start_time=953936984 timezone=UTC
service=shell priv−lvl=15 cmd=show version
Fri Mar 24 13:23:19 2000 10.31.1.151 pinecone telnet85
171.68.118.100 update task_id=14 start_time=953936974 timezone=UTC
service=shell
```

RADIUS on UNIX Record Output

This output is an example of how the records can appear on the server:

```
Client−Id = 10.31.1.151
NAS−Port−Type = 0
User−Name = "login"
Acct−Status−Type = Start
Acct−Authentic = RADIUS
User−Service−Type = 7
Acct−Session−Id = "0000002b"
Acct−Delay−Time = 0

Client−Id = 10.31.1.151
NAS−Port−Type = 0
User−Name = "login"
Calling−Station−Id = "171.68.118.100"
```

```
Acct−Status−Type = Start
User−Service−Type = Login−User
Acct−Session−Id = "0000002c"
Login−Service = Telnet
Login−Host = 171.68.118.100
Acct−Delay−Time = 0

Client−Id = 10.31.1.151
NAS−Port−Type = 0
User−Name = "login"
Calling−Station−Id = "171.68.118.100"
Acct−Status−Type = Stop
User−Service−Type = Login−User
Acct−Session−Id = "0000002c"
Login−Service = Telnet
Login−Host = 171.68.118.100
Acct−Session−Time = 9
Acct−Delay−Time = 0

Client−Id = 10.31.1.151
NAS−Port−Type = 0
User−Name = "login"
Acct−Status−Type = Stop
Acct−Authentic = RADIUS
User−Service−Type = 7
Acct−Session−Id = "0000002b"
Received unknown attribute 49
Acct−Session−Time = 30
Acct−Delay−Time = 0
```

Step H − TACACS+ Enable Authentication

Complete these steps:

1. Issue the **set authentication enable local enable** command in order to make sure that there is a back door in if the server is down.
2. Issue the **set authentication enable tacacs enable** command in order to tell the switch to send enable requests to the server.

Step I − RADIUS Enable Authentication

Add these commands in order to get the switch to send the username `$enab15$` to the RADIUS server. Not all RADIUS servers support this kind of a username. See Step E for another alternative, for example, if you set a service−type [RADIUS attribute 6 − to Administrative], which launches individual users into enable mode.

1. Issue the **set authentication enable local enable** command in order to make sure there is a back door in if the server is down.
2. Issue the **set authentication enable radius enable** command in order to tell the switch to send enable requests to the server if your RADIUS server supports the $enab15$ username.

Step J − TACACS+ Enable Authorization

The addition of this command results in the switch sending enable to the server when the user tries to enable. The server needs to have the **enable** command permitted. In this example, there is a failover to none in the event the server is down:

set author enable enable tacacs+ none both

Step K − Kerberos Authentication

Refer to Controlling and Monitoring Access to the Switch Using Authentication, Authorization, and Accounting for more information on how to set up Kerberos to the switch.

Password Recovery

Refer to Password Recovery Procedures for more information on Password Recovery procedures.

This page is the index of password recovery procedures for Cisco products.

ip permit Commands for Additional Security

For additional security, the Catalyst can be configured to control Telnet access through the **ip permit** commands:

set ip permit enable telnet

set ip permit *range mask|host*

This allows only the range or hosts specified to Telnet into the switch.

Debug on the Catalyst

Prior to enabling debugging on the Catalyst, check the server logs for reasons for failure. This is easier and less disruptive to the switch. On earlier switch versions, the **debug** was performed in engineering mode. It is not necessary to access engineering mode in order to execute **debug** commands in later versions of code:

set trace tacacs|radius|kerberos 4

Note: The **set trace tacacs|radius|kerberos 0** command returns the Catalyst to the no−tracing mode.

Refer to Switches Product Support Page for more information on multilayer LAN Switches.

Related Information

- **TACACS+ and RADIUS Comparison**
- **RADIUS, TACACS+, and Kerberos in Cisco IOS Documentation**
- **RADIUS Support Page**
- **TACACS/TACACS+ Support Page**
- **Kerberos Support Page**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Dec 27, 2007 Document ID: 13847