RADIUS Authentication Problems in ONS 15454 Version 6.0

Document ID: 68072

Contents

Introduction

This document describes a couple of known issues with Remote Authentication Dial−In User Service (RADIUS) server authentication in ONS 15454 version 6.0 in a Cisco ONS 15454 environment.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ONS 15454
- RADIUS server

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ONS 15454 version 6.0

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.

Conventions

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

Background Information

RADIUS is a system of distributed security that secures remote access to networks and network services against unauthorized access. RADIUS comprises these three components:

- A protocol with a frame format that utilizes User Datagram Protocol (UDP)/IP
- A server
- A client

An ONS 15454 node operates as a client of RADIUS. The client passes user information to designated RADIUS servers, and then acts on the response. RADIUS servers receive user connection requests, authenticate the user, and return all configuration information necessary for the client to deliver service to the user.

A shared secret authenticates transactions between the RADIUS client and server. The shared secret is never sent over the network. In addition, any user passwords are encrypted when exchanged between the client and RADIUS server. The encryption process eliminates the possibility of someone who monitors an unsecured network to determine the password of a user.

Shared Secret

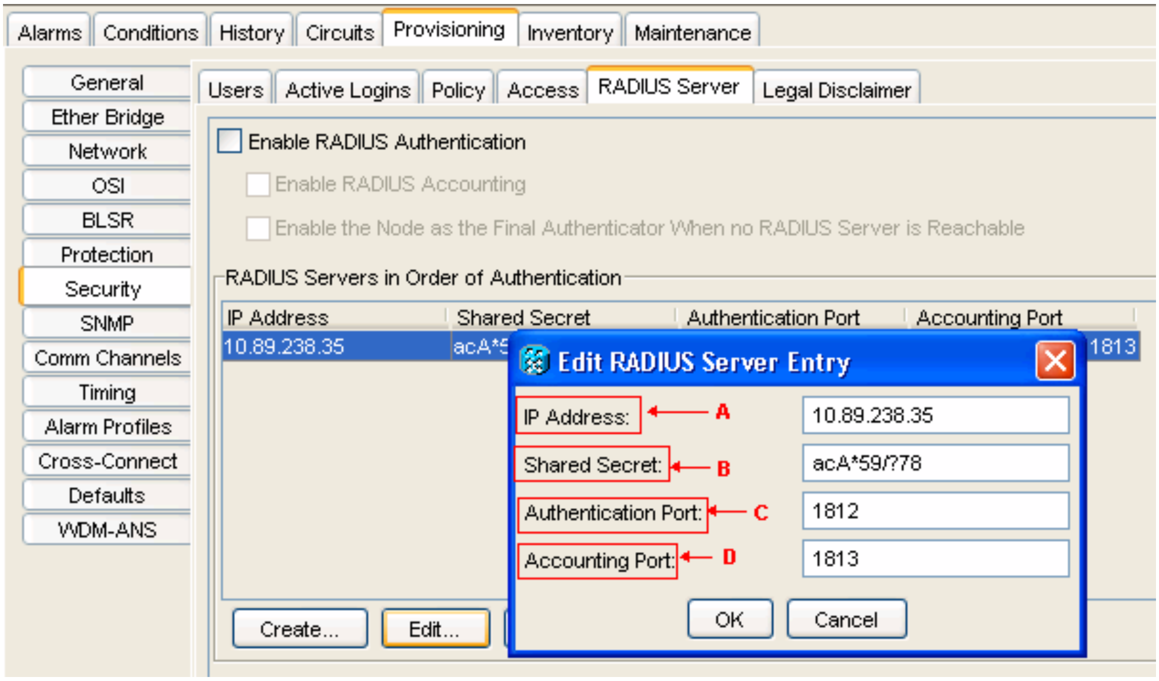
A shared secret is a text string that serves as a password between the ONS15454 RADIUS client and the RADIUS server. Complete these steps in order to create a shared secret:

1. Log into Cisco Transport Controller (CTC).
2. Go to the Network view.
3. Select a specific ONS 15454 in order to go to the Shelf view.
4. Click **Provisioning > Security > RADIUS Server**.
5. Type the IP address of the RADIUS server in the IP Address field (see arrow A in Figure 1).
6. Type a shared secret in the Shared Secret field. A shared secret is a text string that serves as a password between a RADIUS client and RADIUS server (see arrow B in Figure 1).
7. Type the RADIUS authentication port number in the Authentication Port field (see arrow C in Figure 1).

   The default authentication port number is 1812. If the node is an ENE, set the authentication port to a number within the range of 1860 and 1869.
8. Type the RADIUS accounting port number in the Accounting Port field (see arrow D in Figure 1).

   The default accounting port number is 1813. If the node is an ENE, set the accounting port to a number within the range of 1870 and 1879.

   Figure 1 Security: RADIUS Server



□ Enable RADIUS Authentication

□ Enable RADIUS Accounting

□ Enable the Node as the Final Authenticator When no RADIUS Server is Reachable

RADIUS Servers in Order of Authentication

IP Address	Shared Secret	Authentication Port	Accounting Port
10.89.238.35	acA*5		1813

IP Address: 10.89.238.35

Shared Secret: acA*59/?78

Authentication Port: 1812

Accounting Port: 1813

Use shared secrets to ensure that a RADIUS−enabled device that you have configured with the same shared secret sends all RADIUS messages except the Access−Request message.

Shared secrets make sure that the RADIUS message does not get modified in transit. In other words, shared secrets maintain message integrity. Shared secrets also encrypt some RADIUS attributes, for example, User−Password and Tunnel−Password.

ONS 15454 version 6.0 limits the length of a shared secret to 16 characters. However, from ONS 15454 version 6.2 onwards, Cisco plans to increase the maximum length to 128 characters. Refer to Cisco bug ID CSCsc16614 (registered customers only) for more information.

Shared secret character group supports:

- Letters (uppercase and lowercase), for example, A, B, a and b.
- Numerals, for example, 1, 2 and 3.
- Symbols, which represent all characters that are not defined as letters or numerals, for example, >, (, and *.

User Security Group Mapping

An attribute−value (AV) pair represents a variable and one of the possible values that the variable can hold. Within ONS 15454, users are mapped to different security groups based on Cisco AV Pair. Here is an example:

"shell:priv−lvl=X" where X can be value of 0 to 3:

- 0 represents RTRV.
- 1 represents PROV.
- 2 represents MAINT.
- 3 represents SUPER.

Password

The RADIUS server and client do not limit the characters you use for a password. However, CTC has a limitation. For ONS 15454 version 6.0, here are the characters that CTC supports:

- Letters (uppercase and lowercase), for example, A, B, a and b.
- Numerals, for example, 1, 2 and 3.
- Only the #, %, and + special symbols.

Cisco plans to remove the limitation of special symbols in later versions of ONS 15454. Refer to Cisco bug ID CSCsc16604 (registered customers only) for more information.

Related Information

- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map

Updated: Nov 17, 2005 Document ID: 68072