EXHIBIT 3

AO88 (Rev 1/94) Subpoena in a Civil Case

Issued by the

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

Alcatel USA Resources, Inc. and Alcatel Internetworking, Inc.

v.

Foundry Networks, Inc.

SUBPOENA IN A CIVIL CASE

Case Number:[1] 1:05 CV 418
U.S.D.C, District of Delaware

TO: Cisco Systems, Inc.
Attention: Legal Department
170 West Tasman Drive
San Jose, CA 95134

☐ YOU ARE COMMANDED to appear in the United States District court at the place, date, and time specified below to testify in the above case.

PLACE OF TESTIMONY	COURTROOM
	DATE AND TIME

☐ YOU ARE COMMANDED to appear at the place, date, and time specified below to testify at the taking of a deposition in the above case.

PLACE OF DEPOSITION	DATE AND TIME

☒ YOU ARE COMMANDED to produce and permit inspection and copying of the following documents or objects at the place, date, and time specified below (list documents or objects): **SEE ATTACHED SCHEDULE A.**

PLACE	DATE AND TIME
Orrick, Herrington & Sutcliffe LLP. 1000 Marsh Road, Menlo Park, CA 94025-1015	04/07/2006

☐ YOU ARE COMMANDED to permit inspection of the following premises at the date and time specified below.

PREMISES	DATE AND TIME

Any organization not a party to this suit that is subpoenaed for the taking of a deposition shall designate one or more officers, directors, or managing agents, or other persons who consent to testify on its behalf, and may set forth, for each person designated, the matters on which the person will testify. Federal Rules of Civil Procedure, 30(b)(6)

ISSUING OFFICER'S SIGNATURE AND TITLE (INDICATE IF ATTORNEY FOR PLAINTIFF OR DEFENDANT)	DATE
Michael F. Heafey Attorney for Defendant	03/20/2006

ISSUING OFFICER'S NAME, ADDRESS AND PHONE NUMBER

Michael F. Heafey, Esq. Orrick, Herrington & Sutcliffe LLP
1000 Marsh Road, Menlo Park, CA 94025-1015, Phone Number: (650) 614-7356

(See Rule 45, Federal Rules of Civil Procedure, Parts C & D on next page)

[1] If action is pending in district other than district of issuance state district under case number

AO88 (Rev 1/94) Subpoena in a Civil Case

PROOF OF SERVICE

DATE TIME

SERVED

SERVED ON (PRINT NAME) MANNER OF SERVICE

SERVED BY (PRINT NAME) TITLE

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Proof of Service is true and correct.

Executed on _____
DATE

_____
SIGNATURE OF SERVER

_____
ADDRESS OF SERVER

Rule 45, Federal Rules of Civil Procedure, Parts C & D:

(c) PROTECTION OF PERSONS SUBJECT TO SUBPOENAS

(1) A party or an attorney responsible for the issuance and service of a subpoena shall take reasonable steps to avoid imposing undue burden or expense on a person subject to that subpoena. The court on behalf of which the subpoena was issued shall enforce this duty and impose upon the party or attorney in breach of this duty an appropriate sanction which may include, but is not limited to, lost earnings and reasonable attorney's fee.

(2) (A) A person commanded to produce and permit inspection and copying of designated books, papers, documents or tangible things, or inspection of premises need not appear in person at the place of production or inspection unless commanded to appear for deposition, hearing or trial.

(B) Subject to paragraph (d) (2) of this rule, a person commanded to produce and permit inspection and copying may, within 14 days after service of subpoena or before the time specified for compliance if such time is less than 14 days after service, serve upon the party or attorney designated in the subpoena written objection to inspection or copying of any or all of the designated materials or of the premises. If objection is made, the party serving the subpoena shall not be entitled to inspect and copy materials or inspect the premises except pursuant to an order of the court by which the subpoena was issued. If objection has been made, the party serving the subpoena may, upon notice to the person commanded to produce, move at any time for an order to compel the production. Such an order to comply production shall protect any person who is not a party or an officer of a party from significant expense resulting from the inspection and copying commanded.

(3) (A) On timely motion, the court by which a subpoena was issued shall quash or modify the subpoena if it

(i) fails to allow reasonable time for compliance;

(ii) requires a person who is not a party or an officer of a party to travel to a place more than 100 miles from the place where that person resides, is employed or regularly transacts business in person, except that, subject to the provisions of clause (c) (3) (B) (iii) of this rule, such a person may in order to attend trial be commanded to travel from any such place within the state in which the trial is held, or

(iii) requires disclosure of privileged or other protected matter and no exception or waiver applies, or

(iv) subjects a person to undue burden.

(B) If a subpoena

(i) requires disclosure of a trade secret or other confidential research, development, or commercial information, or

(ii) requires disclosure of an unretained expert's opinion or information not describing specific events or occurrences in dispute and resulting from the expert's study made not at the request of any party, or

(iii) requires a person who is not a party or an officer of a party to incur substantial expense to travel more than 100 miles to attend trial, the court may, to protect a person subject to or affected by the subpoena, quash or modify the subpoena, or, if the party in who behalf the subpoena is issued shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship and assures that the person to whom the subpoena is addressed will be reasonably compensated, the court may order appearance or production only upon specified conditions.

(d) DUTIES IN RESPONDING TO SUBPOENA.

(1) A person responding to a subpoena to produce documents shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the demand.

(2) When information subject to a subpoena is withheld on a claim that it is privileged or subject to protection as trial preparation materials, the claim shall be made expressly and shall be supported by a description of the nature of the documents, communications, or things not produced that is sufficient to enable the demanding party to contest the claim.

SCHEDULE A – DOCUMENTS TO BE PRODUCED

Category I – For the time period prior to June 1996 please produce:

1. Documents sufficient to identify and describe the features of all Cisco switches that implemented user authentication in June 1996 or earlier.

   a) Cisco means Cisco Systems, Inc. and/or its past or present divisions, affiliates, predecessors, successors, parents or subsidiaries.

   b) The term user authentication means authenticating a user based on a user id and password entered by the user, or based on a MAC address associated with a device that is used by the user.

   c) The term "Cisco switches," means any device including, for example, bridges, switches, routers, or hubs) that performed network interconnection at Layer 2 (according to the International Organization for Standardization) which was made or sold by Cisco.

2. Prior versions (dated June 1996 or earlier) of the document attached as Exhibit 1 entitled "Single-User Access Security TACACS+." (This document is marked with the following copyright notice: "Copyright © 1996 Cisco Systems, Inc.")

3. Prior versions (dated June 1996 or earlier) of the document attached as Exhibit 2, Document ID 13838, entitled "TACACS+ and RADIUS Comparison." (This document is marked with the following copyright notice: "All contents are Copyright © 1992-2006 Cisco Systems, Inc.")

4. Prior versions (dated June 1996 or earlier) of the document attached as Exhibit 3, Document ID 10559, entitled "Cisco – Secure User Registration Tool." (This document is marked with the following copyright notice: "All contents are Copyright © 1992-2006 Cisco Systems, Inc.")

Category II – For the time period prior to June 1996, please produce:

1. Documents sufficient to identify and describe the features of all Cisco switches that implemented secure port-port-based VLANs in June 1996 or earlier.

   a) The term "VLAN," means virtual local area networks.

   b) The term "port-based," means associated with a collection of switch ports on one or more switches across a hub.

   c) The term "secure" means authenticating users, and associating authenticated users to network services and VLANs according the users access rights.

2. Prior versions (on or before June 1996) of the documents attached as:

a) Exhibit 4, entitled "Virtual LAN Communications. (This document is marked with the following copyright notice: "Copyright © 1995 Cisco Systems, Inc.");

b) Exhibit 5, entitled "Cisco VLAN Roadmap," printed December 9, 1996 (This document is marked with the following copyright notice: "Copyright © 1996 Cisco Systems, Inc."); and

c) Exhibit 6, entitled "VLANs and Routers," printed December 9, 1996 (This document is marked with the following copyright notice: "Copyright © 1996 Cisco Systems, Inc.").

3. Documents (including, for example, brochures, bulletins, case studies, data sheets, instruction guides, presentations, product manuals, release notes, technical specifications, and white papers) sufficient to identify and describe the features of "Switched Internetwork Management Applications" made or sold by Cisco Systems, Inc. and/or its past or present divisions, affiliates, predecessors, successors, parents or subsidiaries in June 1996 or earlier, including:

a) VlanDirector;

b) Cisco Secure User Registration Tool;

c) CiscoView; and

d) CISCO IOS

Category III – For the time period prior to June 1996, please produce:

1. Documents (including, for example, brochures, bulletins, case studies, data sheets, instruction guides, presentations, product manuals, release notes, technical specifications, and white papers) sufficient to identify and describe the features of switches made or sold by Cisco in June 1996 or earlier, including switches that implemented support for either TACACS, or TACACS+ authentication.

2. Documents (including, for example, brochures, bulletins, case studies, data sheets, instruction guides, presentations, product manuals, release notes, technical specifications, and white papers) sufficient to identify and describe the features of switches made or sold by Cisco in June 1996 or earlier, including switches that implemented support for RADIUS authentication.

3. Documents (including, for example, brochures, bulletins, case studies, data sheets, instruction guides, presentations, product manuals, release notes, technical specifications, and white papers) sufficient to identify and describe the features of "Catalyst" switches made or sold by Cisco in June 1996 or earlier, including the following Cisco products:

a) Catalyst 5000 Switching System;

b) Catalyst 3000 Family Stackable Switching System (3000 and 3200);

c) Catalyst 2900 Fast Ethernet Switching System;

d) Catalyst 2600 Token Ring Switch;

e) Catalyst 2000/2800 Workgroup Switching Family;

f) Catalyst 1900/2820 Workgroup Switching Family;

g) Catalyst 1800 Token Ring Switch;

h) Catalyst 1200 Workgroup Switch; and

i) LightStream 1010 and 2020 ATM Switches.

4. Documents (including purchase orders, invoices, and sales records) sufficient to show that the products identified in items 1-3 of Category III were sold prior to June 13, 1996.

5. Documents (including price quotations, and responses to requests for quotations) sufficient to show that the products identified in items 1-3 of Category III were offered for sale prior to June 13, 1996.

Exhibit 1



Single-User Network Access Security TACACS+

- TACACS+ Software 10.3(3) Product Announcement
- PR: "TACACS+ -- New Version of Cisco's Server-Based Security Protocol"

Overview

A major paradigm shift in remote network access is the shift from terminal access to LAN access. Single users are connecting to the corporate network with computers (notebooks or PCs from home) that can sustain complete network connections. These users no longer connect as unfriendly terminals but connect in the same way they do at work: as a LAN user.

Companies are moving to the remote node, remote LAN, and remote access server paradigm because it increases user productivity. Remote node technology gives users access to the same corporate network from home or while traveling as they do at work. Connecting to the network means connecting to a NetWare file server or AppleShare. Users are not required to become experts on terminal services and login prompts.

Since the network is now readily available through remote node technology, network access security has become increasingly important. Host security was adequate for terminal access, but network access security is needed for remotely connected users or remote nodes.

General Network Access Security Requirements

Network Access Security (NAS) is evolving from user needs. Network managers are now concerned with three sets of requirements for their NASs: authentication, authorization, and accounting services.

Authentication

Authentication is who is allowed to gain access to the LAN. Simple authorization methods use a database of username and passwords on the terminal server or access server. More advanced authorization systems use methods such as TACACS (a centralized Token card systems) and Kerberos.

However, once users are authenticated to use the LAN, they may still need to apply a username password for access to specific services such as UNIX hosts, NetWare, or AppleShare. A good NAS server supports a variety of authentication options.

Authorization

Authorization, the ability to limit network services to different users, is a dynamically applied access list

(sometimes called a user profile) based on the username/password pair. This feature is useful for two primary reasons: it helps to limit the exposure of the internal network to outside callers and simplifies the view of the network for the less technical remote access user.

Authorization allows users to be mobile. Mobile and temporary users (portable users with modems in hotels and telecommuters with modems or ISDN connections at home) want to connect to the closest local connection and still have the same access privileges of their local networks.

The network administrator must be able to limit network access to users for all access protocols and services (Telnet, IP, IPX, and AppleTalk) while users dial in through the same modem pool. Per-user access list authorization is not limited to specific interfaces but is dynamically assigned to the specific port to which a user attaches. For example, when user A connects to port 1, she can see subnets 1, 2, 3 and AppleTalk zones *bldg D*, *bldg E*, and *bldg F*. When user B connects to port 1, his profile limits him to subnet 1 and AppleTalk zone *bldg D*.

Since a NAS supports many more remote users than its physical lines, each user or group of users can dial into the same phone rotary and receive access to the network. The access list is based on username and, as such, each NAS, and can support thousands of users in its username and password database.

Accounting

Accounting is the third major requirement in a security system. Network administrators may want to bill departments or customers for connection time. Accounting also provides the ability to track suspicious connection attempts into the network.

General Cisco Network Access Security Features

Following are the general network access security features that are currently available on Cisco Access Servers. These features can be internally stored on an access server or centralized database using TACACS.

FEATURE	FUNCTION
Username and password	Basic NAS security
Per-user access lists for IP	Basic authentication
Callback	Reverses phone charges, extra security for telecommuters
PAP and CHAP	Translates PAP or CHAP to TACACS
Logging	Sends start and stop times to external logging server
Absolute time out	Limits the time a user can be connected to connect session limit
Inactivity time out	Cisco supports session timeout, which disconnects a user after a specified time of inactivity. After a session timeout, another person cannot use the connection.

Autocommand	A user can automatically execute a command (if it is available in the internal database).
System script	Automatically connects a user to a specific host or other script capabilities
Autoselect	Automatically provides users with the service they need to connect to the access server. Autoselect supports Telnet, TN3270, SLIP, PPP (for IP or IPX) and ARA. Autoselect limits the user's access to services by automatically providing the appropriate service. For example, a Macintosh user can be automatically dropped into ARA without an exec terminal session. This is both a security and ease-of-use feature.

Manual Service Selection: EXEC

EXEC allows users to connect to the access server "shell," then select services.

Users connected to EXEC may specify various services: UUCP, PPP, SLIP, ARA, TN3270, Telnet, or EXEC to manage the router itself.

Connecting to EXEC allows users to manage the access server or router if they have the appropriate privileges.

Internal or Centrally Managed NAS

All of the security features mentioned can be set up and administered internally on a Cisco access server or passed from a Cisco access server to a centralized database. To send the information to a central database and forward the response to the proper Cisco access server requires a specific protocol.

Cisco implemented the Terminal Access Controller Access System (TACACS) protocol for this exact reason. It was developed by BBN to support multiple communication servers' username/password authentication. It forwards the user's username and password information to a centralized database that also has the TACACS protocol. The centralized database looks up the information and sends back an accept or deny message, which either allows or denies the user access. The centralized database can be modified to control the authorization from either a simple or complex environment.

Centralized Database and TACACS

A client/server (protocol and server) architecture places all security information on a single, central database, instead of being disbursed around a network in different devices. This is especially useful if there are thousands of users who are using thousands of access servers distributed around the network.

A security protocol and server are much more extendible and scalable for large enterprises. TACACS and other remote access security protocols are designed to support thousands of remote connections. In a large network, the user database is usually large, and is best kept on a centralized server. This saves memory in all the access devices and eliminates the need to update every access server when new users

are added, or passwords are modified or changed.

TACACS

TACACS is a an industry standard protocol specification, RFC 1492, that forwards username and password information to a centralized server. The centralized server can either be a TACACS database or a database like the UNIX password file with TACACS protocol support. For example, the UNIX server with TACACS passes requests to the UNIX database and sends the accept or reject message back to the access server.

XTACACS

XTACACS defines the extensions that Cisco added to the TACACS protocol to support new and advanced features.

XTACACS supports:

- Multiple TACACS servers
- *syslog* -- Sends accounting information to a UNIX host
- *connect* -- Where the user is authenticated into the access server "shell" and can Telnet or initiate slip or PPP or ARA after initial

XTACACS is multiprotocol and can authorize connections with:

- SLIP
- enable
- PPP (IP or IPX)
- ARA
- EXEC
- Telnet

TACACS+

TACACS+ allows a separate access server (the TACACS+ server) to provide the services of authentication, authorization, and accounting independently. Each service can be tied into its own database or can use the other services available on that server or on the network.

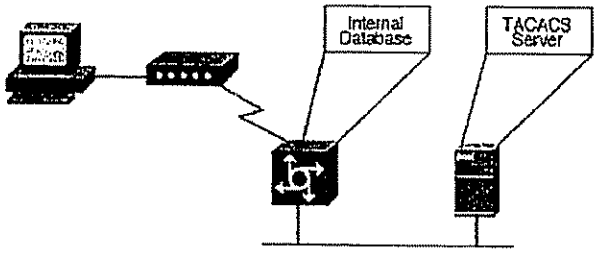


Figure 1: Control Access to Network Via Dial Up

TACACS+ will be supported by the Cisco family of routers and access servers as part of a maintenance of Cisco IOS Release 10.3. This protocol is a completely new version of the TACACS protocol referenced by RFC 1492. Cisco is presenting TACACS+ to the IETF working groups and will contribute to and adopt the emerging NAS protocol standard.

The overall design goal of TACACS+ is to define a standardmethod for managing dissimilar Network Access Servers (NASs) from a single set of management services such as a database. A NAS provides connections to a single user, to a network, or subnetwork, and interconnected networks.

TACACS+ has three major components: the protocol support within the access servers and routers, the protocol specification, and the centralized security database. Similar to an internal security database, TACACS+ supports the following three required features of a good security system.

Authentication

The TACACS+ protocol forwards many types of username password information. This information is encrypted over the network with MD5, an encryption algorithm. TACACS+ can forward the password types for ARA, SLIP, PAP, CHAP, and standard Telnet. This allows clients to use the same username password for different protocols. TACACS+ is extensible to support new password types like KCHAP.

TACACS+ authentication supports multiple challenge and response demands from the TACACS+ server. This allows token card vendors to provide advanced features like sending back a second token-generated number after the first one was manipulated by a security server.

Authorization

TACACS+ provides a mechanism to tell an access server which access list that a user connected to port 1 uses. The TACACS+ server and location of the username/password information identify the access list through which the user is filtered. The access list(s) reside on the access server. The TACACS server responds to a username with an accept and an Access List number which causes that list to be applied.

Accounting

TACACS+ provides accounting information to a database through TCP to insure a more secure and complete accounting log.

The accounting portion of the TACACS+ protocol contains the network address of the user, the username, the service attempted, protocol used, time and date, and the packet-filter module originating the log. For Telnet connections, it also contains source and destination port, action carried (communication accepted, rejected), log, and alert type. Formats are open and configurable.

The billing information includes connect time, user ID, location connected from, start time, and stop time. It identifies the protocol that the user is using and may contain commands being run if the users are connected through exec and Telnet.

Future TACACS+ accounting enhancements will provide connect time updates, which will send an update for current connect time to the accounting server every x minutes. This feature allows companies like Internet providers to bill a customer for an open session even if the access server restarts and loses

the initial start time. Service providers can significantly minimize lost billing time.

The auditing information provides which commands + arguments, location connect from.

The protocol provides enough information so that a server can produce intruder detection routines, reporting statistics, number of packets, and number of bytes.

Users want servers to prevent multiple uses of the same username/password so that customers with flat rates do not share their account with others. Although the decision to give access is made on the server, the protocol is flexible enough to provide the necessary information to detect multiple passwords.

Third-Party Security Solutions

TACACS is an open protocol and can be ported to any username or password database. Many users now want token card support for their remote dial-in access users. Many token card client server companies have ported the TACACS protocol to their central databases. This allows remote node users to connect to a network through a Cisco access server, while using a third-party database and token cards for the remote users.

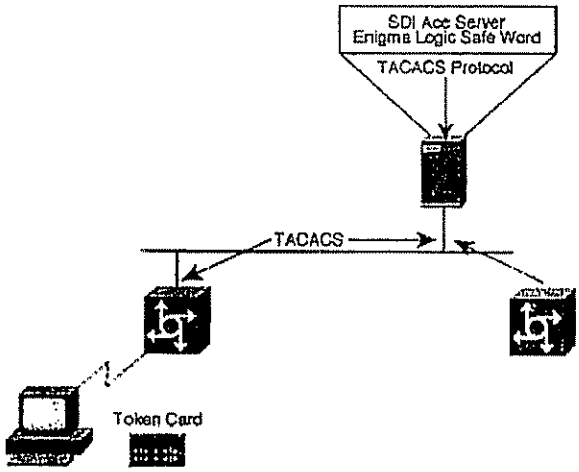


Figure 2: TACACS and Token Card Support

Companies that support this solution today include:

- Enigma Logic
- Security Dynamics
- Digital Pathways

Advantages of the TACACS+ Protocol:

- TCP-based for more security
- Provide three separate protocol components, each of which can be implemented on separate servers

Authentication provides complete server control of the authentication process, which includes:

- login and password query
- Challenge/response
- Messaging support (any)
- Encrypted in MD5
- Replaceable with Kerberos 5

Authorization allows "remote" access control and enhanced granularity. Features include:

- One authentication
- Authorization for each service
- Per-user access list and user profile
- Users can belong to groups
- IP and Telnet support (IPX, ARA future)
- Any access or command and permission or restrictions
    - Initial connection upon starting any command or service
- Primary service
    - Exec or autoselected protocol
- Secondary service
    - Commands from exec or control protocol like PPP NCP and based on connection location

Examples of the "AAA" Functionality

The authorization component in TACACS+ allows greater levels of control over user actions and can be used to create separate administrative groups that are based on user functionality. For example, a network manager might want to restrict a user to perform certain functions on the access server or router. Within the access server, a user might be restricted to PPP or SLIP and only be permitted to connect to a specific host address. Another example of the flexibility of the authorization subsystem is forcing a user to connect to a particular host if an attempt is made to connect to a specific host. In the case of the router's command line user interface, a restriction might be placed on executing particular EXEC commands such as reload.

The authentication protocol can also generate an autocommand. Once a user is authenticated, this runs any command within the access server system and is very powerful for complete access management. Network managers can use the accounting component to track user activity for a security audit trail or to provide billing information. A report might be structured to provide: user identity, start and stop times, executed commands, number of packets, and number of bytes.

Password aging is another example of the capabilities that are now available with TACACS+. A server supporting TACACS+ can send a message back to users, telling them to change their passwords as part of the login sequence. They will not be allowed access unless they change their passwords at that time.

FEATURE	INTERNAL	XTACACS	TACACS+
AUTHENTICATION			
PAP/CHAP	*	*	*
System script	*	*	*
Autocommand	*	*	*
DialBack	95	*	95
Username/password	*	*	*
Use MD5 encryption			*
Token card support		*	*
Via Kerberos 5			95
For exec	*	*	*
For PPP (IP and IPX)	*	*	*
For ARA	*	*	*
Multiple challenge and response			*
Router access authentication	*	*	*
Support for rcmd			*
Try multiple authentication types		*	*
AUTHORIZATION	*	*	
Per user-IP (SLIP and PPP)	*	*	*
Per user IPX	95	95	95
Per user ARA	95	95	95
exec prompt access	*		*
exec and PPP IP address		*	*
exec and Telnet	*	*	*
Router commands	*	*	*
User-changeable password		Dependent on server	Yes, but only with one server
ACCOUNTING			
Time connection start		*	*
Time connection finish		*	*
Total connection time		*	*
# packets, # bytes			
Which commands + argument			95
Location connect from			95
User ID		*	*
User protocol		*	*
Use UDP		*	
Use TCP			*
Absolute time out			
Inactivity time out			

The TACACS+ Protocol Spec

TACACS+ also provides a general-purpose protocol specification that allows the TACACS+ protocol to be integrated into standard databases. The TACACS+ protocol specification will make integration of the TACACS+ protocol into third-party or customer authentication/security databases easier and it also provides more functionality. Current third party support for TACACS includes Security Dymanics, Enigma Logic, and more new customers to be announced.

Third-party token support will be enhanced with TACACS+ in that the custom database will be able to handle challenge response mechanisms for tokencards and other advanced authentication systems.

General

TACACS+ sample server C code and protocol specification will be available from Cisco Connection Online (CCO) on the World Wide Web (http://www.cisco.com) and character-based bulletin board (telnet cco.cisco.com), and through anonymous FTP (ftp.cisco.com).

Cisco is working with the IETF to standardize these security protocols. And is working with other centralized security protocols like Radius. Cisco will participate in the evolution of a single standards-based NAS protocol.

Posted: Mar 30 11:46:18 1995

Copyright 1996 © Cisco Systems Inc.

Exhibit 2

TACACS+ and RADIUS Comparison

TAC Notice: What's Changing on TAC Web

Document ID: 13838

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Optional contact information:

Name:

Email:

Send

Contents

Introduction
Prerequisites
- Requirements
- Components Used
- Conventions

RADIUS Background
- Client/Server Model
- Network Security
- Flexible Authentication Mechanisms
- Server Code Availability

Compare TACACS+ and RADIUS
- UDP and TCP
- Packet Encryption
- Authentication and Authorization
- Multiprotocol Support
- Router Management
- Interoperability
- Traffic
- Device Support

NetPro Discussion Forums - Featured Conversations
Related Information

Introduction

Two prominent security protocols used to control access into networks are Cisco TACACS+ and RADIUS. The RADIUS specification is described in RFC 2865, which obsoletes RFC 2138. Cisco is committed to supporting both protocols with the best of class offerings. It is not the intention of Cisco to compete with RADIUS or influence users to use TACACS+. You should choose the solution that best meets your needs. This document discusses the differences between TACACS+ and RADIUS, so that you can make an informed choice.

Cisco has supported the RADIUS protocol since Cisco IOS® Software Release 11.1 in February 1996. Cisco continues to enhance the RADIUS Client with new features and capabilities, supporting RADIUS

as a standard.

Cisco seriously evaluated RADIUS as a security protocol before it developed TACACS+. Many features were included in the TACACS+ protocol to meet the needs of the growing security market. The protocol was designed to scale as networks grow, and to adapt to new security technology as the market matures. The underlying architecture of the TACACS+ protocol complements the independent authentication, authorization, and accounting (AAA) architecture.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

RADIUS Background

RADIUS is an access server that uses AAA protocol. It is a system of distributed security that secures remote access to networks and network services against unauthorized access. RADIUS comprises three components:

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

The server runs on a central computer typically at the customer's site, while the clients reside in the dial-up access servers and can be distributed throughout the network. Cisco has incorporated the RADIUS Client into Cisco IOS Software Release 11.1 and later and other device software.

Client/Server Model

A network access server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and returning all configuration information necessary for the client to deliver service to the user. The RADIUS servers can act as proxy clients to other kinds of authentication servers.

Network Security

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server. This eliminates the possibility that someone snooping on an unsecured network could determine a user's password.

Flexible Authentication Mechanisms

The RADIUS server supports a variety of methods to authenticate a user. When it is provided with the user name and original password given by the user, it can support PPP, Password Authentication Protocol (PAP), or Challenge Handshake Authentication Protocol (CHAP), UNIX login, and other authentication mechanisms.

Server Code Availability

There are a number of distributions of server code commercially and freely available. Cisco servers include Cisco Secure ACS for Windows, Cisco Secure ACS for UNIX, and Cisco Access Registrar.

Compare TACACS+ and RADIUS

These sections compare several features of TACACS+ and RADIUS.

UDP and TCP

RADIUS uses UDP while TACACS+ uses TCP. TCP offers several advantages over UDP. TCP offers a connection-oriented transport, while UDP offers best-effort delivery. RADIUS requires additional programmable variables such as re-transmit attempts and time-outs to compensate for best-effort transport, but it lacks the level of built-in support that a TCP transport offers:

- TCP usage provides a separate acknowledgment that a request has been received, within (approximately) a network round-trip time (RTT), regardless of how loaded and slow the backend authentication mechanism (a TCP acknowledgment) might be.
- TCP provides immediate indication of a crashed, or not running, server by a reset (RST). You can determine when a server crashes and returns to service if you use long-lived TCP connections. UDP cannot tell the difference between a server that is down, a slow server, and a non-existent server.
- Using TCP keepalives, server crashes can be detected out-of-band with actual requests. Connections to multiple servers can be maintained simultaneously, and you only need to send messages to the ones that are known to be up and running.
- TCP is more scalable and adapts to growing, as well as congested, networks.

Packet Encryption

RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, can be captured by a third party.

TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. For debugging purposes, it is useful to have the body of the packets unencrypted. However, during normal operation, the body of the packet is fully encrypted for more secure communications.

Authentication and Authorization

RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.

TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.

During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

Multiprotocol Support

RADIUS does not support these protocols:

- AppleTalk Remote Access (ARA) protocol
- NetBIOS Frame Protocol Control protocol
- Novell Asynchronous Services Interface (NASI)
- X.25 PAD connection

TACACS+ offers multiprotocol support.

Router Management

RADIUS does not allow users to control which commands can be executed on a router and which cannot. Therefore, RADIUS is not as useful for router management or as flexible for terminal services.

TACACS+ provides two methods to control the authorization of router commands on a per-user or per-group basis. The first method is to assign privilege levels to commands and have the router verify with the TACACS+ server whether or not the user is authorized at the specified privilege level. The second method is to explicitly specify in the TACACS+ server, on a per-user or per-group basis, the commands that are allowed.

Interoperability

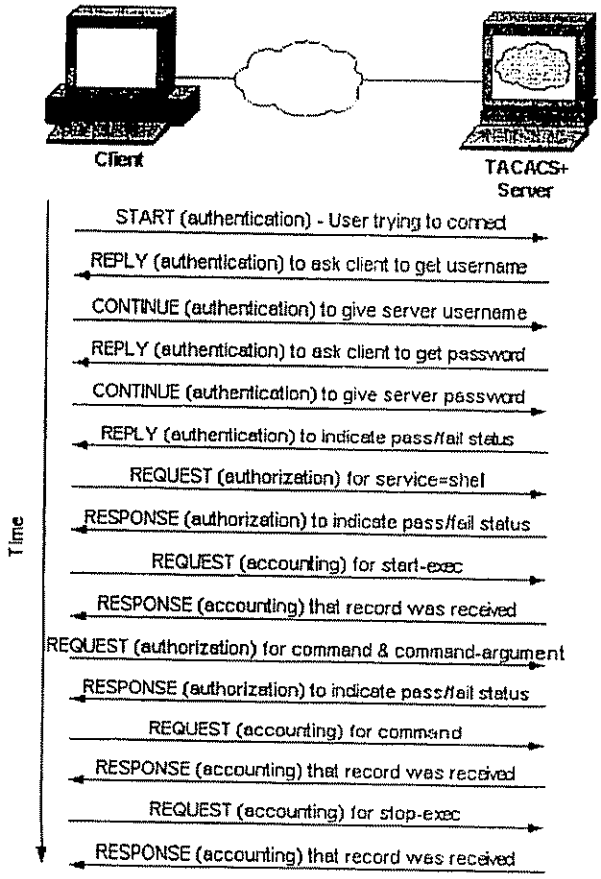
Due to various interpretations of the RADIUS Request for Comments (RFCs), compliance with the RADIUS RFCs does not guarantee interoperability. Even though several vendors implement RADIUS clients, this does not mean they are interoperable. Cisco implements most RADIUS attributes and consistently adds more. If customers use only the standard RADIUS attributes in their servers, they can interoperate between several vendors as long as these vendors implement the same attributes. However, many vendors implement extensions that are proprietary attributes. If a customer uses one of these vendor-specific extended attributes, interoperability is not possible.

Traffic

Due to the previously cited differences between TACACS+ and RADIUS, the amount of traffic generated between the client and server differs. These examples illustrate the traffic between the client and server for TACACS+ and RADIUS when used for router management with authentication, exec authorization, command authorization (which RADIUS cannot do), exec accounting, and command accounting (which RADIUS cannot do).

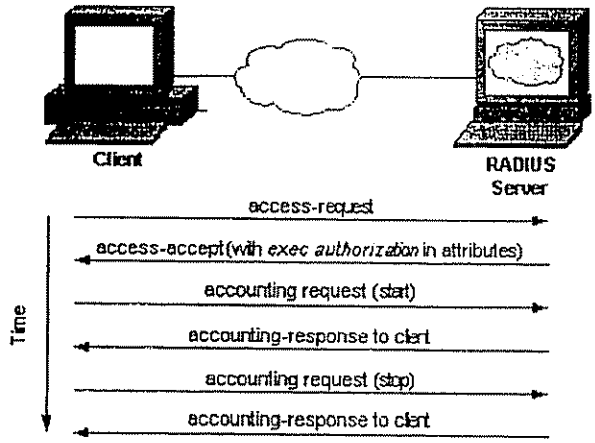
TACACS+ Traffic Example

This example assumes login authentication, exec authorization, command authorization, start-stop exec accounting, and command accounting is implemented with TACACS+ when a user Telnets to a router, performs a command, and exits the router:



RADIUS Traffic Example

This example assumes login authentication, exec authorization, and start-stop exec accounting is implemented with RADIUS when a user Telnets to a router, performs a command, and exits the router (other management services are not available):



Device Support

This table lists TACACS+ and RADIUS AAA support by device type for selected platforms. This includes the software version in which the support was added. Check product release notes for further information, if your product is not in this list.

Cisco Device	TACACS+ authentication	TACACS+ authorization	TACACS+ accounting	RADIUS authentication	RADIUS authorization	RADI accoun
Cisco Aironet[1]	12.2(4)JA	12.2(4)JA	12.2(4)JA	all Access-points	all Access-points	all Acc points
Cisco IOS Software[2]	10.3.3	10.3.3	10.3.3[3]	11.1.1	11.1.1[4]	11.1.1[5]
Cisco Cache Engine	--	--	--	1.5	1.5[6]	--
Cisco Catalyst switches	2.2	5.4.1	5.4.1	5.1	5.4.1[4]	5.4.1[5]
Cisco CSS 11000 Content Services Switch	5.03	5.03	5.03	5.0	5.0[4]	--
Cisco CSS 11500 Content Services Switch	5.20	5.20	5.20	5.20	5.20[4]	--
Cisco PIX Firewall	4.0	4.0[7]	4.2[8,5]	4.0	5.2[7]	4.2[8,5]

Cisco Catalyst 1900/2820 switches	8.x enterprise[9]	--	--	--	--	--
Cisco Catalyst 2900XL/3500XL switches	11.2.(8)SA6[10]	11.2.(8)SA6[10]	11.2.(8) SA6[10]	12.0(5)WC5[11]	12.0(5) WC5[11, 4]	12.0(5) WC5[11]
Cisco VPN 3000 Concentrator [6]	3.0	3.0	--	2.0[12]	2.0	2.0[12]
Cisco VPN 5000 Concentrator	--	--	--	5.2X[12]	5.2X[12]	5.2X[12]

Table Notes

1. Termination of wireless clients only, not management traffic in versions other than Cisco IOS Software Release 12.2(4)JA or later. In Cisco IOS Software Release 12.2.(4)JA or later, authentication for both termination of wireless clients and management traffic is possible.
2. Check Feature Navigator (now obsoleted by Software Advisor (registered customers only)) for platform support within Cisco IOS software.
3. Command accounting is not implemented until Cisco IOS Software Release 11.1.6.3.
4. No command authorization.
5. No command accounting.
6. URL blocking only, not administrative traffic.
7. Authorization for non-VPN traffic through the PIX.

   Note: Release 5.2 - Access-list support for Access Control List (ACL) RADIUS Vendor-Specific Attribute (VSA) or TACACS+ authorization for VPN traffic terminating on PIX Release 6.1 - support for ACL RADIUS attribute 11 authorization for VPN traffic terminating on PIX Release 6.2.2 - support for downloadable ACLs with RADIUS authorization for VPN traffic terminating on PIX Release 6.2 - support for authorization for PIX management traffic through TACACS+.
8. Accounting for non-VPN traffic through the PIX only, not management traffic.

   Note: Release 5.2 - Support for accounting for VPN Client TCP packets through the PIX.
9. Enterprise software only.
10. Needs 8M Flash for image.
11. VPN termination only

NetPro Discussion Forums - Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums - Featured Conversations for Security
Security: Intrusion Detection [Systems]
Installing CSA - Mar 2, 2006 IPS on 2811 router with 2 ISP - Mar 2, 2006 CCA and 802.1X - Mar 2, 2006 4250 appliance not processing packets correctly - Mar 2, 2006 Cannot Launch IPS MC in CiscoWorks VMS - Mar 1, 2006
Security: AAA
help to configure ACS3.3 and ASA5520 for VPN clients profiles - Mar 2, 2006 Documentation on network authentication - Mar 2, 2006 ACS HTML Login not working - Mar 2, 2006 Catalyst 5500 series switch and AAA - Mar 2, 2006 Acct-Terminate-Cause = none - Mar 2, 2006
Security: General
Cisco Router and Switches Security Baseline Configurations - Mar 2, 2006 Creating an ACL - Mar 2, 2006 Sniffing on 2950 series? - Mar 2, 2006 HTTPS with BBSM - Mar 2, 2006 PDM Features - Mar 2, 2006
Security: Firewalling
ASK THE EXPERT – TROUBLESHOOTING PIX/ASA FIREWALLS - Mar 2, 2006 Odd VPN Tunnel Issue - Mar 2, 2006 Can Pix or ASA 5500 do bandwidth throttling? - Mar 2, 2006 MTU discovery - Mar 2, 2006 Where can I get config guide for 6.3 and later?? - Mar 2, 2006

Related Information

- **RADIUS Support Page**
- **RADIUS in IOS Documentation**
- **TACACS+ in IOS Documentation**
- **TACACS/TACACS+ Support Page**
- **Requests for Comments (RFCs)**
- **Technical Support - Cisco Systems**

All contents are Copyright © 1992-2006 Cisco Systems, Inc All rights reserved Important Notices and Privacy Statement.

Updated: Jan 19, 2006 Document ID: 13838

Exhibit 3

Cisco Secure User Registration Tool

Cisco Secure User Registration Tool Version 2.5

Downloads

Cisco Secure User Registration Tool Version 2.5

Table Of Contents

Data Sheet
- Overview
- New Features in Cisco Secure URT v2.5
- Features and Benefits
- Applications
- Ordering Information
- System Requirements
- For More Information
  - Documentation
  - Contacts

Data Sheet

Cisco Secure User Registration Tool Version 2.5

Cisco Secure User Registration Tool (URT) Version 2.5 actively identifies users within the network and creates user-registration-policy bindings for policy registration, mobility, and tracking. Cisco Secure URT v2.5 introduces an extensible Web front-end client and Remote Access Dial-In User Service (RADIUS)-based back-end infrastructure, making the product appealing to an extended range of customer network sizes and applications.

Overview

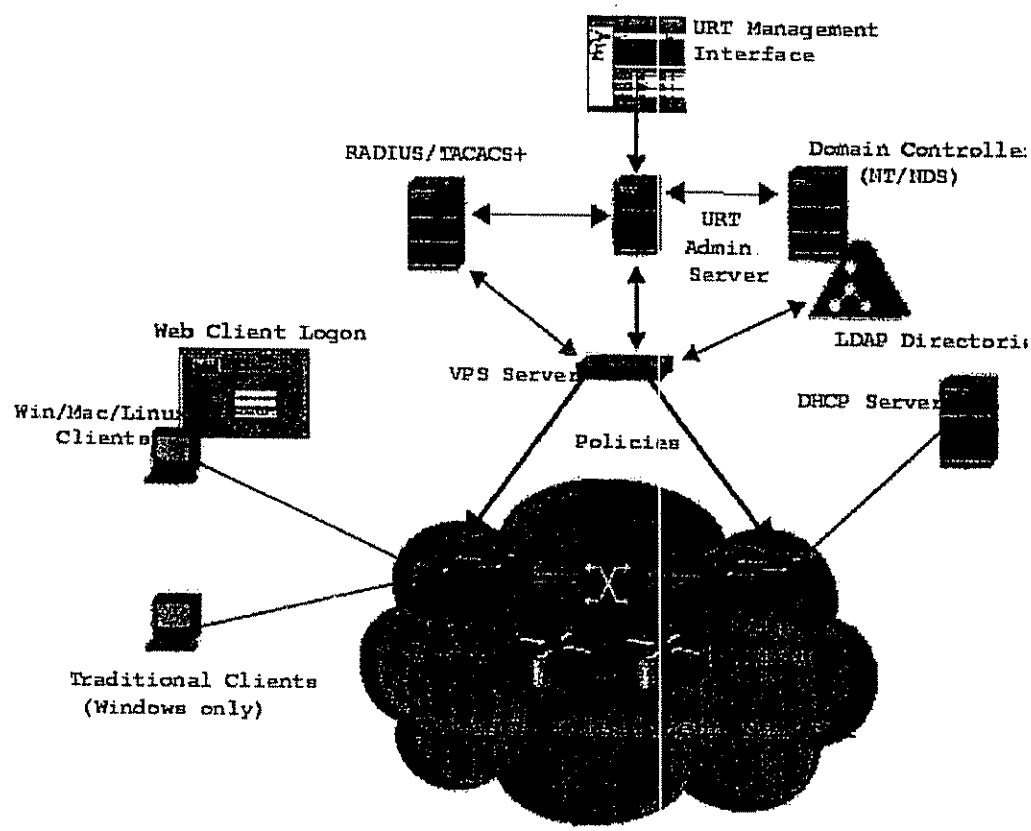
Cisco Secure URT v2.5 is an important piece of the Cisco next-generation identity-management-solution suite. Cisco Secure URT is a virtual LAN (VLAN) assignment service that provides LAN security by actively identifying and authenticating users and then associating them only to the specific network services and resources they need through dynamic VLAN assignments to Cisco Catalyst® Switch networks. URT v2.5 introduces many innovative features, including a Web-based logon from Windows, Macintosh, and Linux clients, RADIUS and Lightweight Directory Access Protocol (LDAP) authentication, and a secure link between the client and the VLAN Policy Server (VPS). It also includes a security feature based on the Media Access Control (MAC) address that prevents users from accessing the network if they are not using authorized machines.

Cisco Secure URT assigns VLAN-based policies to switch ports based on user authentication to existing Microsoft Windows NT, Active Directory, Novell Netware Directory Services (NDS) or RADIUS directories. VLAN policies are applied via Cisco VPS servers, which, when distributed throughout the network, provide better login load sharing and greater availability to the network. Unless a user provides a valid username and password to the authentication server, that user will remain in a "logon VLAN" with no access to the corporate or service provider network. Because URT uses existing user-authentication mechanisms, policies are applied transparently to users and are easily deployed in any existing network.

Cisco Secure URT intelligently monitors and manages user identification, locations, and network access times. It detects when a user is authenticated and places that user into the appropriate VLAN based on policies that are preassigned through the URT administrative interface. Cisco Secure URT also prevents unauthorized access to protected VLANs and subnets by disallowing access to unauthorized users. This protection is accomplished through a user registration process (started at user login) that can result in logically blocking connection to the protected VLAN or subnet if the attached user is not authorized for access.

The Cisco Secure URT architecture consists of the following components (Figure 1):

Cisco Secure URT v2.5 Components and Architecture



- **URT Administrator Server**—Main component of Cisco Secure URT Solution. The Cisco Secure URT Administrator Server operates as a central collection point for events and log information sent from all VPSs under its control.
- **URT Management Interface**—Assigns VLANs to users, groups, organizational units or MAC addresses and also establishes Windows NT, AD, NDS, and RADIUS domains, associations.
- **URT VPS**—Runs on an external one-rack-unit-high appliance and is responsible for setting a client's switch port based on the login user name, group name, organizational unit, or MAC address. It is also used for authenticating and assigning VLANs to Web users.
- **URT Client Module**—The Client module Logon script is pushed from the URT Administrator Server to the Windows NT/NDS domain controllers, and it is automatically installed on the traditional client machine to enable user authentication.
- **URT Web Client Module**—The Web client module is invoked automatically from the user's Netscape or Microsoft Internet Explorer Web browser and performs the same functionality as the URT Client Module. It is downloaded in a signed Java Archive (JAR) file using a Web applet. This application is used to prompt for a user ID, password, and user authentication domain.

With a Web-based secure logon from a Windows, Macintosh, or Linux client, the user logs in to the VPS for authentication without having to download any application on the desktop. Cisco Secure URT provides authentication through any standard RADIUS server such as a Cisco Secure Access Control Server (ACS).

New Features in Cisco Secure URT v2.5

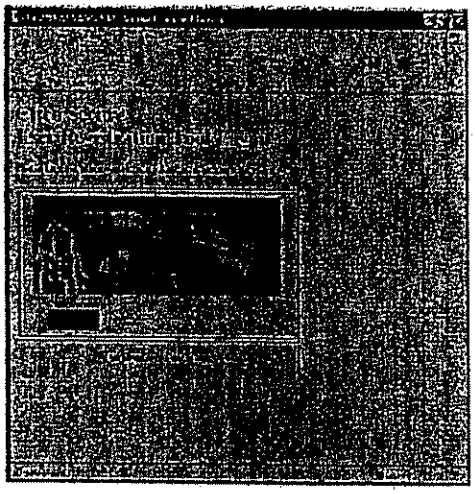
Cisco Secure URT v2.5 introduces the following features:

- **Web Client Logon Interface**—URT v2.5 supports Web-based authentication for Windows, Macintosh, and Linux client platforms. When users launch a Web browser, they are automatically redirected to the URT logon Web page (Figure 2) until they are successfully authenticated and switched to the user-assigned VLAN. Users will be given the choice to authenticate to any LDAP or RADIUS domains that are preprovisioned in the URT Administration Tool. The URT Administrator can also choose to customize the logon Web page to post any advertising or announcement

h c c c e c ec c hee

messages.

Default Web Login Window



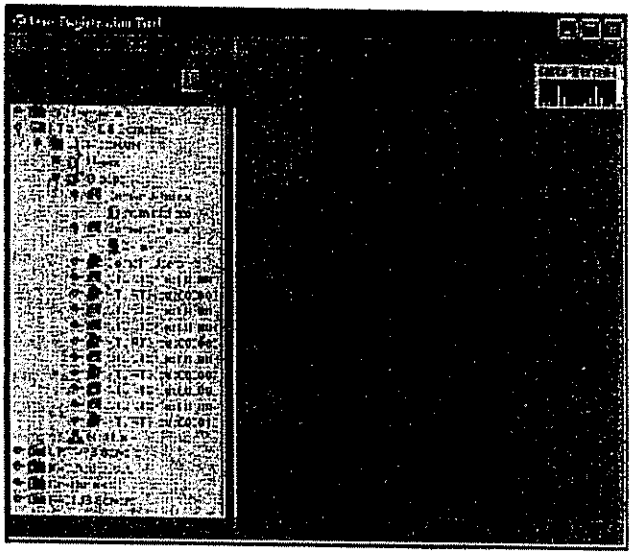
- **MAC-Based Security Option**—The MAC-based security option provides extended security to protect user access to the logon VLAN from unregistered PCs. This feature is particularly important for customers who do not want to expose their logon VLANs to unrecognizable MAC addresses. It allows administrators to control users' access from registered PCs only and thereby reduce the spread of viruses and attacks from infected or non-controlled PCs. When this option is enabled, two options are presented: switching the port to a provisionable "Security Violation VLAN" with limited access capabilities, or shutting down the switch port.
- **RADIUS Authentication and Accounting Support**—In Cisco Secure URT v2.5, RADIUS authentication is offered for Web logon. RADIUS accounting is also supported once a user is successfully authenticated via RADIUS server.

Cisco Secure URT v2.5 was tested with the Cisco Secure Access Control Server (ACS). Please refer to "Configuring RADIUS Server for URT" white paper, at http://www.cisco.com/go/urt for more information.

Secure Link Between Cisco Secure URT Client and VPS Server—Security authentication and data encryption have been added to URT v2.5 to enable a more secure connection from the user. The protocol between the Cisco Secure URT Client Module and the VPS is secured to protect user access against unwanted intrusion or malicious attacks.

- **LDAP Support (Active Directory and NDS directories)**—Cisco Secure URT v2.5 supports Windows' Active Directory and Novell's NDS LDAP servers. Through the Cisco Secure URT Administrator Server, the users, groups, or organizational unit trees are retrieved using LDAP.
- **Multiple Users Per Port**—Previous versions of Cisco Secure URT support only a single user logon on a single port. If more than one MAC address is detected on a port the port will be moved back to the logon VLAN. URT v2.5 has an option to allow multiple users connected to a hub served by single switch port. The URT Administrator can allow only one user per port or multiple users per port based upon the logged-in user ID.
- **Display of Windows NT Groups**—The URT Administrator interface is enhanced to display the users belonging to a Windows NT group. By displaying the users for a group, the administrator can now select the group, get a list of users for that group and then assign a VLAN to a group or a user within a group (Figure 6).

Group/User Display in the Administrator Server



- **MAC Address Events History**—Previous version of URT only reported user-based logon/logoff history events. With URT v2.5 MAC-address-based logon/logoff events are added as an option and reported to the history events tool on the URT Administrator Server.

Features and Benefits

Table 1 outlines the benefits of Cisco Secure URT v2.5.

Table 1 Features and Benefits of Cisco Secure URT v2.5

Features	Benefits
Controls LAN access through Web-based user login	• Access control at the network edge • Complements dialup access security
Works on any LAN port	• User mobility
Is transparent to end users	• Lower cost of installation • Lower cost of ownership
Binds Windows NT primary domain controller (PDC), Active Directory, NDS, and RADIUS users to a VLAN	• Uses existing security servers • Separates user communities
Allows configuration by organizational unit, user group, user, or MAC address	• Provides scalable user management
Works from a Windows, Macintosh, or Linux Web client operating system	• Uses most common operating systems
Connects to RADIUS servers	• Adds an authentication, authorization, and accounting (AAA) mechanism through IETF- compliant RADIUS servers
Complements DHCP server	• Improves user management
Provides redundant policy servers	• Increases availability
Provides centralized administration of policy servers	• Lowers cost of ownership
Supports audit trace	• Increases security audit
Supports import of initial configuration from CiscoWorks	• Lowers cost of installation • Uses existing Cisco network

h c c c e c ec c hee

	management applications

Applications

Network security becomes critical as organizations continue to increasingly use the Internet for e-commerce and extranets. Most organizations have deployed authentication tools at the edge of the network to improve security and to control user access to the network. To minimize costs and ensure consistent, robust security, organizations need to manage these secure networks and their associated services with a controlled user access that is scalable and mobile.

Cisco Secure URT supports the diverse requirements of Cisco customers from small and midsize businesses to large enterprises building corporate intranets and service providers. Cisco Secure URT architecture and secure remote management capabilities enable deployment in a multitude of environments and provide significant flexibility to customers. Cisco Secure URT plays an increasingly important role in midsize-to-large enterprises, enabling them to protect network access points such as conference rooms, shared offices, and other areas common to visitors and vendors. These users might only need to access the Internet and should not be given access to the entire corporate network However, regular employees should be granted the same privileges as if they were accessing the network from their own offices.

Ordering Information

Cisco Secure URT v2.5 is available in the following three packages (Table 2). For part numbers, refer to the Cisco Secure URT v2.5 Product Bulletin.

Table 2 Cisco Secure URT v2.5 Packages

URT v2.5 Packages	Descriptions
Cisco Secure URT v2.5 Starter Package	Includes one VPS appliance and 1 Cisco Secure URT v2.5 application software license
Cisco Secure URT v2.5 Upgrade Kit	Includes software necessary to upgrade from Cisco Secure URT v2.0 to v2.5 (available through Cisco.com download only)
Standalone Cisco Secure URT VPS Appliance	Used in distributed or redundant network deployments; Cisco recommends that you combine at least one unit with the Cisco Secure URT v2.5 Starter Package if using the Web Logon feature

System Requirements

Table 3 summarizes the minimum system requirements and compatibility for Cisco Secure URT v2.5.

URT Admin Server:

- Windows 2000 server SP4
- Windows XP Professional SP1
- Windows Server 2003 (Standard Edition)
- Min H/W (Pentium III, 512MB DRAM, 64 MB of disk space)

URT VPS:

- Cisco VLAN Policy Server 1101
- Cisco VLAN Policy Server 1102

Browsers for Web Logon:

- Netscape version 6.2 and 7.0
- IE version 5.5 (SP2) or 6.0 (SP1)

Client OS:

- Windows 98 SE, Windows NT4 Workstation/Server (SP6), Windows 2000 Professional/server (SP4), Windows XP Professional (SP1), Windows XP (SP1) Home (Web Client Only), Mac OS 10.1 (Web client only), Linux Redhat (7.1)/ SuSE (7.2)/ Mandrake (7.2)/ VA (6.2) (Web Client only)

- Min H/W for Web client (Pentium II, 64MB DRAM, 1 MB of disk space)
- Min H/W for traditional client (Pentium II, 64MB DRAM, 1MB of disk space)

For More Information

Documentation

For more information on Cisco Secure URT 2.5, including the user guide, supported devices, release notes, and supported OS service packs, visit http://www.cisco.com/go/urt.

Contacts

For specific product functionality or technical questions, send e-mail to the Cisco Secure URT product marketing group at URT-MKT@cisco.com

For questions or product ordering, availability, and support contract information, send e-mail to ciscoworks@cisco.com

http://www.cisco.com/pcgi-bin/ibld/view.pl?i=support&m=GUEST

Or send an e-mail to Enterprise Management at ENM-MKT@cisco.com

© 1992-2006 Cisco Systems, Inc All rights reserved Terms and Conditions Privacy Statement, Cookie Policy and Trademarks of Cisco Systems, Inc

h c c c e c ec c hee

Cisco Secure User Registration Tool

Cisco Secure User Registration Tool Version 2.5

Downloads

Cisco Secure User Registration Tool Version 2.5

Table Of Contents

Data Sheet
- Overview
- New Features in Cisco Secure URT v2.5
- Features and Benefits
- Applications
- Ordering Information
- System Requirements
- For More Information
  - Documentation
  - Contacts

Data Sheet

Cisco Secure User Registration Tool Version 2.5

Cisco Secure User Registration Tool (URT) Version 2.5 actively identifies users within the network and creates user-registration-policy bindings for policy registration, mobility, and tracking. Cisco Secure URT v2.5 introduces an extensible Web front-end client and Remote Access Dial-In User Service (RADIUS)-based back-end infrastructure, making the product appealing to an extended range of customer network sizes and applications.

Overview

Cisco Secure URT v2.5 is an important piece of the Cisco next-generation identity-management-solution suite. Cisco Secure URT is a virtual LAN (VLAN) assignment service that provides LAN security by actively identifying and authenticating users and then associating them only to the specific network services and resources they need through dynamic VLAN assignments to Cisco Catalyst® Switch networks. URT v2.5 introduces many innovative features, including a Web-based logon from Windows, Macintosh, and Linux clients, RADIUS and Lightweight Directory Access Protocol (LDAP) authentication, and a secure link between the client and the VLAN Policy Server (VPS). It also includes a security feature based on the Media Access Control (MAC) address that prevents users from accessing the network if they are not using authorized machines.

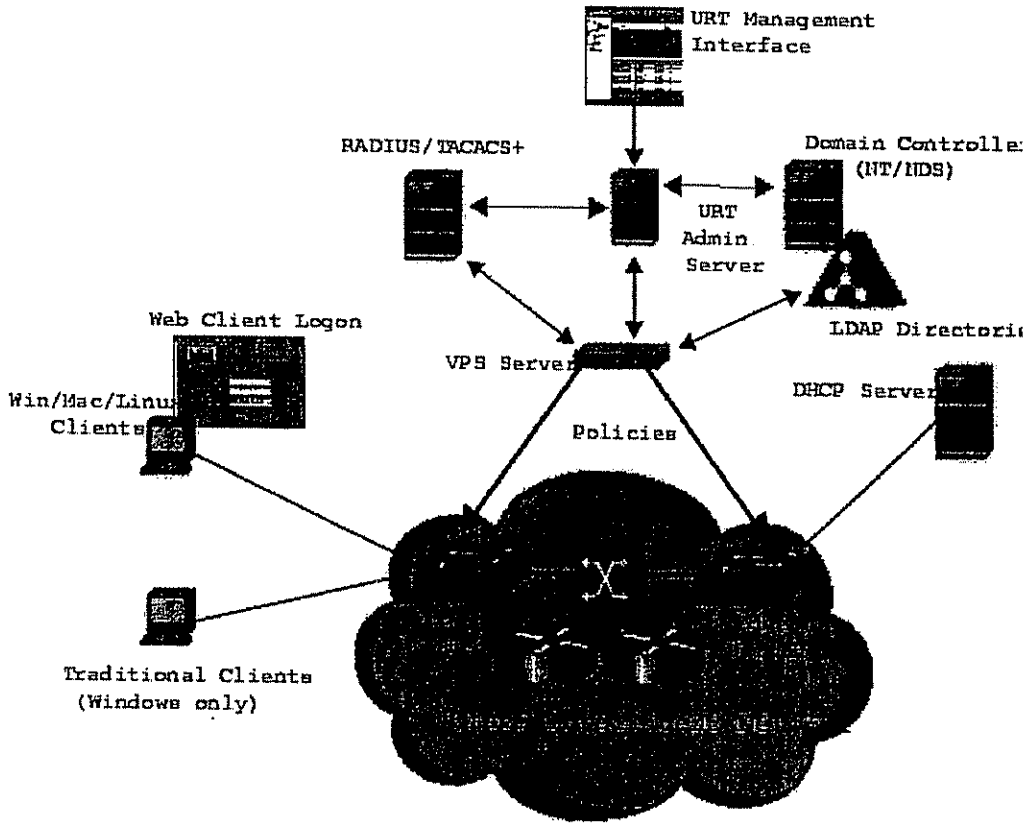
Cisco Secure URT assigns VLAN-based policies to switch ports based on user authentication to existing Microsoft Windows NT, Active Directory, Novell Netware Directory Services (NDS) or RADIUS directories. VLAN policies are applied via Cisco VPS servers, which, when distributed throughout the network, provide better login load sharing and greater availability to the network. Unless a user provides a valid username and password to the authentication server, that user will remain in a "logon VLAN" with no access to the corporate or service provider network. Because URT uses existing user-authentication mechanisms, policies are applied transparently to users and are easily deployed in any existing network.

Cisco Secure URT intelligently monitors and manages user identification, locations, and network access times. It detects when a user is authenticated and places that user into the appropriate VLAN based on policies that are preassigned through the URT administrative interface. Cisco Secure URT also prevents unauthorized access to protected VLANs and subnets by disallowing access to unauthorized users. This protection is accomplished through a user registration process (started at user login) that can result in logically blocking connection to the protected VLAN or subnet if the attached user is not authorized for access.

The Cisco Secure URT architecture consists of the following components (Figure 1):

Cisco Secure URT v2.5 Components and Architecture

h c c c e c ec c hee



- **URT Administrator Server**—Main component of Cisco Secure URT Solution. The Cisco Secure URT Administrator Server operates as a central collection point for events and log information sent from all VPSs under its control.
- **URT Management Interface**—Assigns VLANs to users, groups, organizational units or MAC addresses and also establishes Windows NT, AD, NDS, and RADIUS domains, associations.
- **URT VPS**—Runs on an external one-rack-unit-high appliance and is responsible for setting a client's switch port based on the login user name, group name, organizational unit, or MAC address. It is also used for authenticating and assigning VLANs to Web users.
- **URT Client Module**—The Client module Logon script is pushed from the URT Administrator Server to the Windows NT/NDS domain controllers, and it is automatically installed on the traditional client machine to enable user authentication.
- **URT Web Client Module**—The Web client module is invoked automatically from the user's Netscape or Microsoft Internet Explorer Web browser and performs the same functionality as the URT Client Module. It is downloaded in a signed Java Archive (JAR) file using a Web applet. This application is used to prompt for a user ID, password, and user authentication domain.

With a Web-based secure logon from a Windows, Macintosh, or Linux client, the user logs in to the VPS for authentication without having to download any application on the desktop. Cisco Secure URT provides authentication through any standard RADIUS server such as a Cisco Secure Access Control Server (ACS).

New Features in Cisco Secure URT v2.5

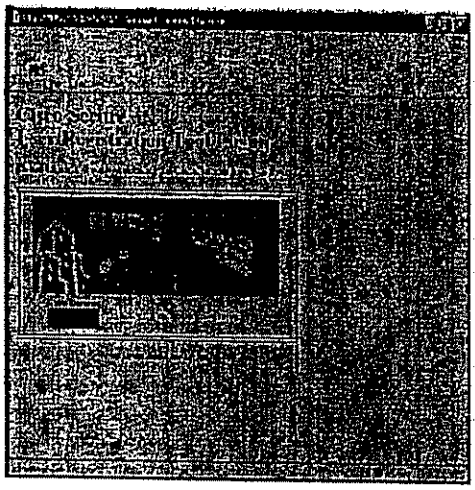
Cisco Secure URT v2.5 introduces the following features:

- **Web Client Logon Interface**—URT v2.5 supports Web-based authentication for Windows, Macintosh, and Linux client platforms. When users launch a Web browser, they are automatically redirected to the URT logon Web page (Figure 2) until they are successfully authenticated and switched to the user-assigned VLAN. Users will be given the choice to authenticate to any LDAP or RADIUS domains that are preprovisioned in the URT Administration Tool. The URT Administrator can also choose to customize the logon Web page to post any advertising or announcement

h c c c e c ec c hee

messages.

Default Web Login Window



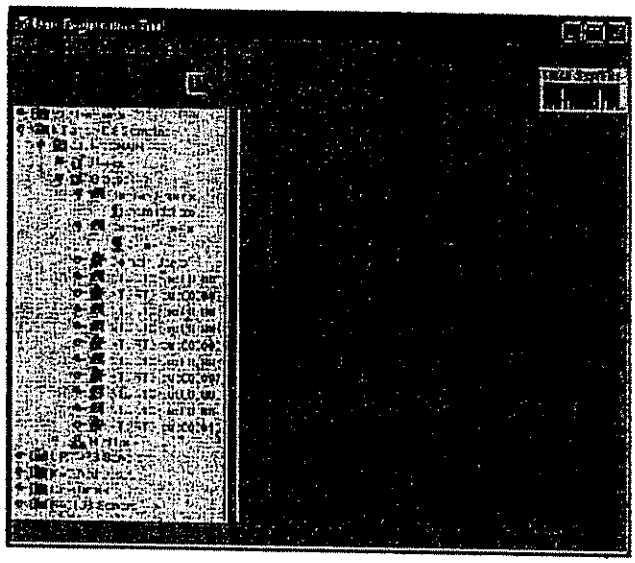
- **MAC-Based Security Option**—The MAC-based security option provides extended security to protect user access to the logon VLAN from unregistered PCs. This feature is particularly important for customers who do not want to expose their logon VLANs to unrecognizable MAC addresses. It allows administrators to control users' access from registered PCs only and thereby reduce the spread of viruses and attacks from infected or non-controlled PCs. When this option is enabled, two options are presented: switching the port to a provisionable "Security Violation VLAN" with limited access capabilities, or shutting down the switch port.
- **RADIUS Authentication and Accounting Support**—In Cisco Secure URT v2.5, RADIUS authentication is offered for Web logon. RADIUS accounting is also supported once a user is successfully authenticated via RADIUS server.

Cisco Secure URT v2.5 was tested with the Cisco Secure Access Control Server (ACS). Please refer to "Configuring RADIUS Server for URT" white paper, at http://www.cisco.com/go/urt for more information.

Secure Link Between Cisco Secure URT Client and VPS Server—Security authentication and data encryption have been added to URT v2.5 to enable a more secure connection from the user. The protocol between the Cisco Secure URT Client Module and the VPS is secured to protect user access against unwanted intrusion or malicious attacks.

- **LDAP Support (Active Directory and NDS directories)**—Cisco Secure URT v2.5 supports Windows' Active Directory and Novell's NDS LDAP servers. Through the Cisco Secure URT Administrator Server, the users, groups, or organizational unit trees are retrieved using LDAP.
- **Multiple Users Per Port**—Previous versions of Cisco Secure URT support only a single user logon on a single port. If more than one MAC address is detected on a port the port will be moved back to the logon VLAN. URT v2.5 has an option to allow multiple users connected to a hub served by single switch port. The URT Administrator can allow only one user per port or multiple users per port based upon the logged-in user ID
- **Display of Windows NT Groups**—The URT Administrator interface is enhanced to display the users belonging to a Windows NT group. By displaying the users for a group, the administrator can now select the group, get a list of users for that group and then assign a VLAN to a group or a user within a group (Figure 6).

Group/User Display in the Administrator Server



- **MAC Address Events History**—Previous version of URT only reported user-based logon/logoff history events. With URT v2.5 MAC-address-based logon/logoff events are added as an option and reported to the history events tool on the URT Administrator Server.

Features and Benefits

Table 1 outlines the benefits of Cisco Secure URT v2.5.

Table 1 Features and Benefits of Cisco Secure URT v2.5

Features	Benefits
Controls LAN access through Web-based user login	• Access control at the network edge • Complements dialup access security
Works on any LAN port	• User mobility
Is transparent to end users	• Lower cost of installation • Lower cost of ownership
Binds Windows NT primary domain controller (PDC), Active Directory, NDS, and RADIUS users to a VLAN	• Uses existing security servers • Separates user communities
Allows configuration by organizational unit, user group, user, or MAC address	• Provides scalable user management
Works from a Windows, Macintosh, or Linux Web client operating system	• Uses most common operating systems
Connects to RADIUS servers	• Adds an authentication, authorization, and accounting (AAA) mechanism through IETF- compliant RADIUS servers
Complements DHCP server	• Improves user management
Provides redundant policy servers	• Increases availability
Provides centralized administration of policy servers	• Lowers cost of ownership
Supports audit trace	• Increases security audit
Supports import of initial configuration from CiscoWorks	• Lowers cost of installation • Uses existing Cisco network

h c c c e c ec c hee

	management applications

Applications

Network security becomes critical as organizations continue to increasingly use the Internet for e-commerce and extranets. Most organizations have deployed authentication tools at the edge of the network to improve security and to control user access to the network. To minimize costs and ensure consistent, robust security, organizations need to manage these secure networks and their associated services with a controlled user access that is scalable and mobile.

Cisco Secure URT supports the diverse requirements of Cisco customers from small and midsize businesses to large enterprises building corporate intranets and service providers. Cisco Secure URT architecture and secure remote management capabilities enable deployment in a multitude of environments and provide significant flexibility to customers. Cisco Secure URT plays an increasingly important role in midsize-to-large enterprises, enabling them to protect network access points such as conference rooms, shared offices, and other areas common to visitors and vendors. These users might only need to access the Internet and should not be given access to the entire corporate network. However, regular employees should be granted the same privileges as if they were accessing the network from their own offices.

Ordering Information

Cisco Secure URT v2.5 is available in the following three packages (Table 2). For part numbers, refer to the Cisco Secure URT v2.5 Product Bulletin.

Table 2 Cisco Secure URT v2.5 Packages

URT v2.5 Packages	Descriptions
Cisco Secure URT v2.5 Starter Package	Includes one VPS appliance and 1 Cisco Secure URT v2.5 application software license
Cisco Secure URT v2.5 Upgrade Kit	Includes software necessary to upgrade from Cisco Secure URT v2.0 to v2.5 (available through Cisco.com download only)
Standalone Cisco Secure URT VPS Appliance	Used in distributed or redundant network deployments; Cisco recommends that you combine at least one unit with the Cisco Secure URT v2.5 Starter Package if using the Web Logon feature

System Requirements

Table 3 summarizes the minimum system requirements and compatibility for Cisco Secure URT v2.5.

URT Admin Server:

- Windows 2000 server SP4
- Windows XP Professional SP1
- Windows Server 2003 (Standard Edition)
- Min H/W (Pentium III, 512MB DRAM, 64 MB of disk space)

URT VPS:

- Cisco VLAN Policy Server 1101
- Cisco VLAN Policy Server 1102

Browsers for Web Logon:

- Netscape version 6.2 and 7.0
- IE version 5.5 (SP2) or 6.0 (SP1)

Client OS:

- Windows 98 SE, Windows NT4 Workstation/Server (SP6), Windows 2000 Professional/server (SP4), Windows XP Professional (SP1), Windows XP (SP1) Home (Web Client Only), Mac OS 10.1 (Web client only), Linux Redhat (7.1)/ SuSE (7.2)/ Mandrake (7.2)/ VA (6.2) (Web Client only)

h c c c e c ec c hee

- Min H/W for Web client (Pentium II, 64MB DRAM, 1 MB of disk space)
- Min H/W for traditional client (Pentium II, 64MB DRAM, 1MB of disk space)

For More Information

Documentation

For more information on Cisco Secure URT 2.5, including the user guide, supported devices, release notes, and supported OS service packs, visit http://www.cisco.com/go/urt

Contacts

For specific product functionality or technical questions, send e-mail to the Cisco Secure URT product marketing group at URT-MKT@cisco.com

For questions or product ordering, availability, and support contract information, send e-mail to ciscoworks@cisco.com

http://www.cisco.com/pcgi-bin/ibld/view.pl?i=support&m=GUEST

Or send an e-mail to Enterprise Management at ENM-MKT@cisco.com

© 1992-2006 Cisco Systems. Inc All rights reserved Terms and Conditions. Privacy Statement, Cookie Policy and Trademarks of Cisco Systems. Inc.

h c c c e c ec c hee