CISCO SYSTEMS

User Guide for the Cisco Secure User Registration Tool

CONTENTS

Preface

This guide describes how to use the User Registration Tool (URT).

Audience

This guide is for anyone who installs, configures, verifies, and uses the Cisco Secure URT application. Network administrators and operators should have the following skills:

- Network management and configuration.
- VLAN management and configuration using switch and router command lines.

If you are using URT with Novell NetWare, you are expected to understand basic NetWare administration and be able to:

- Add users to the network.
- Use ZENworks.
- Configure Dynamic Host Configuration Protocol (DHCP) servers and clients.

If you are using URT with Microsoft Networking, you should be able to:

- Add users to the NT domain server Security Accounts Manager (SAM) database.
- Configure DHCP servers and clients.
- Configure computer names to dynamic IP addresses using the Windows Internet Naming Service (WINS).

If you are using Lightweight Directory Access Protocol (LDAP) servers (such as Active Directory and Novell Directory Service) or Remote Authentication Dial-In User Service (RADIUS) servers, you should know how to configure them.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	`boldface screen` font
Variables you enter	`italic screen` font
Menu items and button names	**boldface** font
Selecting a menu item	**Option > Network Preferences**

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

✎

Note Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review the URT documentation on Cisco.com for any updates.

The following additional documentation is available:

Paper Documentation

- *Release Notes for the Cisco Secure User Registration Tool and the VLAN Policy Server*
- *Installation and Setup Guide for the Cisco 1101 VLAN Policy Server*
- *Regulatory Compliance and Safety Information for the Cisco 1101 VLAN Policy Server*

Online Documentation

- Context-sensitive online help accessed from the URT main window by selecting **Help > Contents**.
- PDFs for :
  - *User Guide for the Cisco Secure User Registration Tool*
  - *Installation and Setup Guide for the Cisco Secure User Registration Tool*
  - *Installation and Setup Guide for the Cisco 1101 VLAN Policy Server*
  - *Regulatory Compliance and Safety Information for the Cisco 1101 VLAN Policy Server*
  - *User Registration Tool Software Developer's Guide*

  ✎

  Note Adobe Acrobat Reader 4.0 or later is required.

- Supported devices table, which you can view at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/fam_prod/user_reg/2_5/index.htm

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Feedback** at the top of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

- Order Cisco learning materials and merchandise

- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.

- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.

- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

Understanding the Basics

User Registration Tool (URT) helps you simplify your network management and control access to key services in your network.

These topics provide basic information about how URT works:

- Understanding What URT Does, page 1-1
- Understanding VLAN Policies, page 1-6
- Processing User Logons and User Logoffs, page 1-11
- Implementing URT in Your Network, page 1-20

Understanding What URT Does

User Registration Tool (URT) is a security application in the Cisco Secure product line that controls user access to the LAN. User access is granted through authentication to Windows NT, Novell Directory Services (NDS), or Active Directory (AD) domain controllers. Until a user is authenticated, URT places the user in a *logon VLAN* that cannot access corporate data servers.

URT facilitates enterprise security, mobile user access, and corporate reorganizations. You can develop VLAN-based security policies and make sure that users access only the authorized services.

As users move from system to system in your network, URT identifies them based on their logon username and applies the appropriate VLAN policy for each user. You can use URT to create and manage VLAN-based security policies based on a username or a user's membership in a group or organizational unit.

URT supports Microsoft Windows clients for traditional logon and Linux and MacOS clients for web logon.

For more information about the web browsers and client platforms supported, see *Installation and Setup Guide for the Cisco Secure User Registration Tool.*

Figure 1-1 shows the relationship between the required network resources and URT.

✎

Note   The relationship in this illustration is only a generalization: you do not have to place all of the systems on the same network segment.

Figure 1-1   Role of URT in the Network
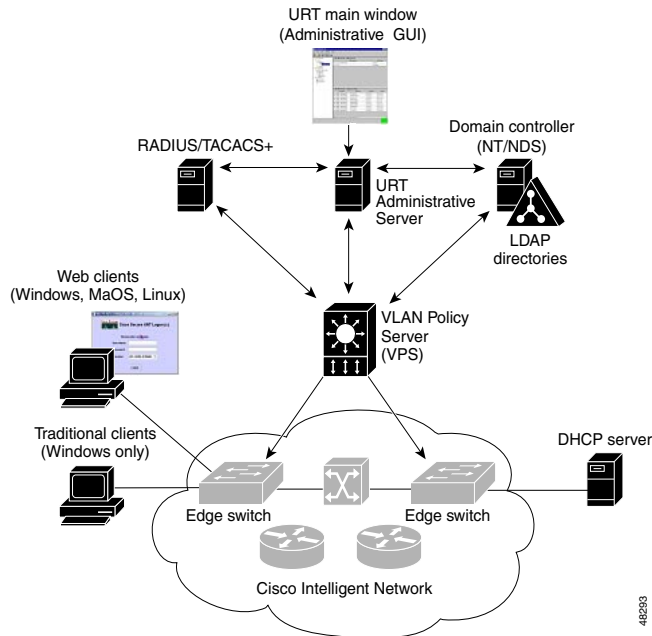
URT Components

Table 1-1 describes the URT components.

Table 1-1   URT Components

Component	Function
VLAN Policy Server (VPS)	Runs on an external appliance and sets a client switch port based on logon username, group name, organizational unit, or MAC address. The VPS handles all logons and acts as a server, delivering VLAN policies to the switches on the network. The VPS has a DNS server and a web server for authenticating and assigning VLANs to web clients.
URT Administrative Server and URT Administrative GUI (URT main window)	• The URT Administrative Server stores your VLAN policies and updates the VPS with the VLAN policies. • The URT Administrative Graphical User Interface (GUI) lets you create VLAN policies and manage URT. You perform almost all URT functions from the URT main window (the main feature of the Administrative GUI). **Note** When you start URT, the main window is displayed, and a separate DOS window (Java console) displays program status and error messages. The DOS window remains open while the Administrative GUI is running. When you close the DOS window, the main window also closes.
URT Client Module	Allows traditional users (those using non-web logons) to log onto the appropriate domain. You can install this module automatically on Windows NT and Windows 2000 client systems.
URT Web Client Interface	Lets web users log on and log off using a web browser. This Java-based interface prompts for a user ID, password, and authentication domain.
Domain server	A Microsoft or Novell server on which software (such as the URT Client Module) required for users' workstations is installed. Domain servers ensure that logons are channeled through the VPSs for VLAN assignments. **Note** In this guide, the terms *NT host* and *NT domain* also refer to Windows 2000 hosts and Windows 2000 domains.

Table 1-1   URT Components (continued)

Component	Function
Lightweight Directory Access Protocol (LDAP) server	Provides authentication and policy management for traditional and web logon clients.
Remote Authentication Dial-In User Service (RADIUS) server	Provides authentication and policy management for web logon clients.

Other Components

Table 1-2 describes other components that URT accesses on the network.

Table 1-2   Other Components URT Accesses on the Network

Component	Function
Switches	Because no URT components exist on switches, you must configure the switches in URT as VLAN Management Policy Server (VMPS) clients so they use the appropriate VPS. **Note** You can enable the VMPS from the switch command-line interface.
DHCP server	The URT Client Module issues appropriate notifications to the VPS and issues DHCP requests to the DHCP server. For web logons, you must modify the DHCP setting for the logon VLAN so it uses the VPS as the DNS setting. When a user logs on from the web, the web page address is queried in DNS. The response to the query is the IP address of the current VPS.

Tips

- To enable URT, switches must run the VMPS client.

- When you configure switches to use a URT VPS, you are setting the switch VMPS configuration.

- When configuring switches from the command line to use a URT VPS, you use the switch **vmps** commands.

- You can use the URT main window to create host-based VLAN policies to run switch-based VMPSs for host-based VLAN policies.

Understanding Traditional Logons and Web Logons

Because traditional URT is not web-based, users log on using the Windows logon.

Note   Traditional logon applies only to Windows clients using Microsoft Networking or Novell NetWare.

Users can also log on from the web on Windows, Linux, and MacOS systems. Web clients are authenticated through LDAP or RADIUS servers.

The same URT Administrative Server and VPS can manage both traditional logons and web logons.

Note   To distinguish between the types of logons, the terms *traditional logon* and *web logon* are used in this guide.

URT Security Features

Table 1-3 describes the URT security features for both traditional logons and web logons.

Table 1-3   URT Security Features for Traditional Logons and Web Logons

Security Feature	Description
Preventing access until authorized	The URT logon VLAN is used as the default VLAN for a VTP domain. Users are typically assigned to the logon VLAN during initial stages of logon, ensuring that they are authenticated before connecting to other VLANs on the network.
Detecting port down state	URT automatically places a port into the logon VLAN whenever the port state changes to down (for example, when a user disconnects a workstation).

Table 1-3   URT Security Features for Traditional Logons and Web Logons (continued)

Security Feature	Description
Using secure link between client and VPS	URT security authentication and data encryption provide a more secure connection between the client and the URT VPS. URT uses these VScape Secure Packet Stream (VSPS) protocol specifications: • Diffie-Hellman key exchange (1024 bits). • HMAC-MD5 or HMAC-SHA1 for authenticating message payload. • Payload data field is encrypted (Twofish 256-bit block cipher, CBC mode). Every client logon generates a different session key, thereby making client logon, client logoff, and sync packets more difficult for others to replay. For data encryption, URT generates four extra packets between the VPS and each logon client. Web clients also have built-in authentication using RADIUS or LDAP servers.
Using MAC security options	You can select only MAC-assigned VLANs and place unauthorized users in a security violation VLAN (rather than the default logon VLAN) or shut down unauthorized users' ports.

Understanding VLAN Policies

You can use both user-based (URT) and host-based (MAC address) VLAN policies in your network, as described in the following topics:

Using User-Based Policies

You can create *user-based VLAN policies* based on a Windows NT or Windows 2000 user or group name, or a Novell NetWare user or organizational unit name. Using these types of policies allows a user to move from one system to another and remain assigned to the appropriate VLAN and subnet (assuming that a single workstation is connected directly to a switch that supports URT).

User with mobile systems (such as laptops) can connect to any supported switch port and be connected to the correct VLAN and subnet. You must define the associated port as *dynamic*—if the port has a static VLAN assignment, URT does not override that assignment.

Using Host-Based Policies

You can *create host-based VLAN policies* by assigning a MAC address to a VLAN. Use host-based VLAN policies primarily with servers directly connected to a supported switch (for example, UNIX or Linux servers). To place a host that does not support user registration in a preassigned VLAN when it starts communicating on the network, you must create host-based VLAN policies.

To create a host-based VLAN policy, you assign VLANs based on the host MAC address associated with the system network interface card (NIC). Because the VLAN policy is based on the MAC address, the host is mapped to a VLAN as soon as it starts communicating on a port. Therefore, no user logon is required.

If there is a one-to-one correspondence between users and hosts (that is, users do not move from host to host), host and user registration provides essentially identical network policy control. Because the VLAN is based on the host MAC address, not the switch port, you can move the host to a different port and make sure that the same VLAN policy is applied. (For example, you can move a laptop between buildings.)

You can use a host-based VLAN policy with any host directly attached to a port on a supported switch. (For example, to register a network-attached server that no user can log onto, use a host-based VLAN policy.)

Note You cannot use host-based VLAN policies with hosts attached to hubs, routers, or unsupported switches.

If you are using traditional logons, host-based VLAN policies allow you to include MacOS, Linux, UNIX, and other non-Windows types of hosts in your dynamic VLAN planning. You can also use host-based VLAN policies with Windows systems—even if the Windows version supports user registration.

Using Both User-Based and Host-Based Policies

You can combine user-based and host-based VLAN policies in the same network by mapping the host MAC address to a VLAN.

- If a VLAN policy exists for a user who logs onto the host, the user is assigned to the user-based VLAN.

- If no VLAN policy exists for another user who logs onto the host, the user is assigned to the host-based VLAN.

Therefore, for *open use* systems, you can define a more restrictive host-based VLAN while giving trusted users their typical user-based VLAN resources.

For client hosts that support both user-based and host-based VLAN policies:

- URT allows you to create policies based on username, group, or organizational unit. Regardless of which host users log onto, they can access the same network resources.

> **Note**   User-based policies work well with a mobile user base.

- URT requires that you use TCP/IP with Microsoft Networking or Novell NetWare running over IP. If you do not want to use TCP/IP as the base protocol, you must use host-based VLAN policies.

Retaining MAC-to-VLAN Associations

URT has an option that determines whether systems logging onto the network with MAC-to-VLAN mappings retain those mappings or if they use URT user-based VLAN policies.

Step 1   Select **Customize > Options**.

The URT Options dialog box is displayed.

Step 2   Click the Logon tab.

Step 3   To keep these mappings, select the Retain MAC to VLAN Associations checkbox.

> **Note**   If you select this option when the system does not have MAC-to-VLAN associations, user-based VLAN policies are used.

Step 4   Click **OK**.

How URT Assigns VLANs

User-based registration takes precedence over host-based VLAN policies. URT applies VLAN assignments in the priority order shown in Figure 1-2.

Figure 1-2   How URT Prioritizes VLAN Assignments
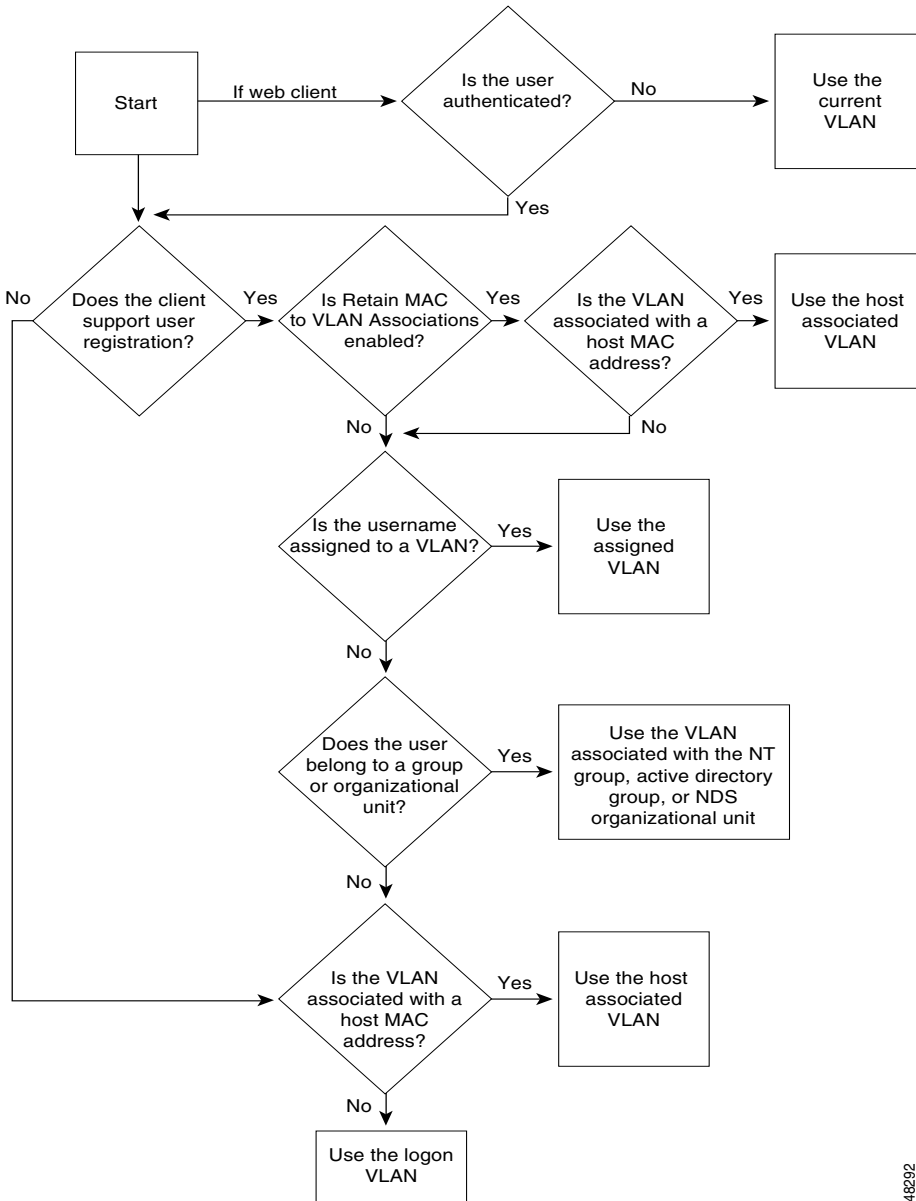
VLANs are assigned in the priority order described in Table 1-4.

Table 1-4   Priority in Assigning VLANs

Priority	Description
URT option	If you have enabled the URT Retain MAC to VLAN Associations option and the MAC address is mapped to a VLAN, the host-based VLAN is used.
Username	If you assign a specific VLAN to a username, that VLAN is used.
Membership in an NT group, Active Directory group, or organizational unit	If a username is not assigned to a VLAN, URT determines whether the username is a member of an NT group, Active Directory group, or organizational unit. If the username is a member of one of these, URT uses the VLAN assigned to it.
MAC address	If a username does not have a VLAN assignment nor is it a member of a group or organizational unit that has a VLAN assignment, URT uses the VLAN assigned to the MAC address of the system (as a host-based VLAN policy). **Note** For clients that do not support user registration, only the MAC address VLAN assignment is checked.
Logon VLAN	If there are no VLAN assignments for the username, group name, organizational unit, or MAC address, the user remains in the logon VLAN.

Processing User Logons and User Logoffs

After URT is initiated and a user logs onto the domain (and is authenticated using the VLAN policies previously defined through URT), the user is assigned to an appropriate VLAN and subnet and is automatically assigned a new IP address in the appropriate subnet from the DHCP server.

URT VPSs replace switch-based VMPSs in your network.

Note   Switches must continue to run the VMPS client to communicate with the URT VPSs.

Before URT places users in the mapped VLAN, they are placed in a logon VLAN that you define for the VTP domain using the URT Administrative GUI. The logon VLAN is used as the default VLAN, giving unmapped users network connectivity. The logon VLAN ensures that users can be authenticated before connecting to your network.

The URT logon process is transparent. However, to manage user logon and logoff processes transparently, URT starts a *lightweight service* in the background (that does not affect system performance) on the client system.

Users are assigned to their associated VLAN only if they connect to the network through a dynamic switch port. Table 1-5 shows the relationships among the switch port state, the URT VLAN policy, and the resulting VLAN.

Table 1-5   How Users are Placed in VLANs Using URT

Switch Port State	User-Based or Host-Based VLAN Policy in URT?	Resulting VLAN
Dynamic	Yes	VLAN association defined in URT.
Dynamic	No	Logon VLAN defined in URT for the switch VTP domain.
Static	Yes	VLAN defined on the switch port. URT does not apply.
Static	No	VLAN defined on the switch port. URT does not apply.

Understanding Logon Processing

Users must log onto a domain server before gaining access to the network in their preassigned VLANs. Before URT places users in the mapped VLAN, they are placed in a *logon VLAN* that you define for the VTP domain (see the "Setting a Default Logon VLAN" section on page 5-3).

The logon VLAN is used as the default VLAN, giving unmapped users network connectivity. The logon VLAN ensures that users are authenticated before connecting to your network.

- Figure 1-3 illustrates a traditional logon to URT on the network; Table 1-6 describes the logon sequence.
- Figure 1-4 illustrates a web logon to URT on the network; Table 1-7 describes the logon sequence.

Figure 1-3   URT-Based Traditional Logon Sequence
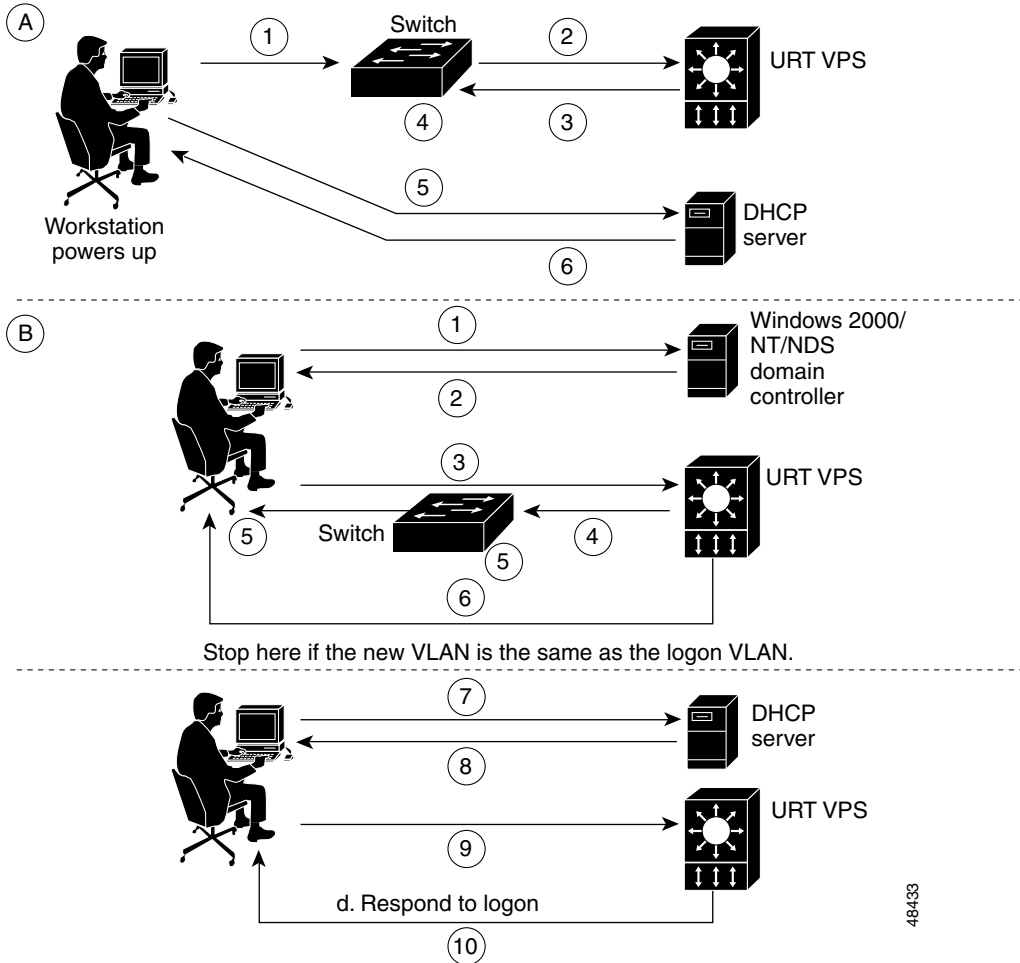
Table 1-6   Description of Traditional Logon Sequence

Step	Description
A1	After the client powers up the workstation, the first packet is sent to the switch.
A2	The switch sends a VLAN Query Protocol (VQP) packet to the URT VPS.
A3	The VPS returns a VQP response to the switch.
A4	The client is put into the logon or MAC VLAN.
A5	The client releases the IP address from the DHCP server.
A6	The client renews the IP address from the DHCP server.
B1	The user logs onto the domain through the domain controller.
B2	The urt.bat login script runs.
B3	A logon packet is sent to the VPS.
B4	If changing VLANs, the VPS returns a VQP response to the switch.
B5	The client is put into the user, group, or organization unit VLAN. **Note** Process continues with step B7.
B6	If not changing VLANs, the VPS responds to the logon. **Note** Process ends with this step.
B7	The client releases the IP address from the DHCP server.
B8	The client renews the IP address from the DHCP server.
B9	The second logon packet is sent to the VPS.
B10	The VPS responds to the logon request.

Figure 1-4   URT-Based Web Logon Sequence
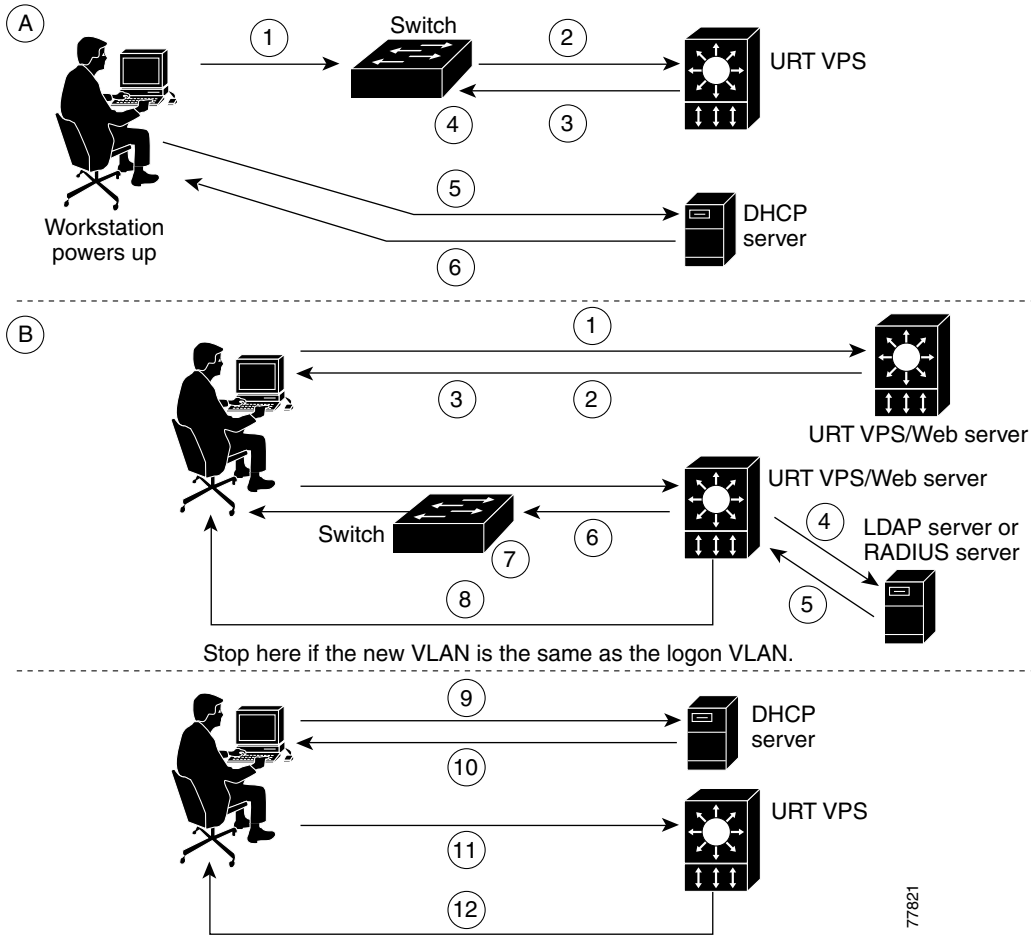
Table 1-7   Description of Web Logon Sequence

Step	Description
A1	After the client powers up the workstation, the first packet is sent to the switch.
A2	The switch sends a VLAN Query Protocol (VQP) packet to the URT VPS.
A3	The VPS returns a VQP response to the switch.
A4	The client is put into the logon or MAC VLAN.
A5	The client releases the IP address from the DHCP server.
A6	The client renews the IP address from the DHCP server.
B1	The client connects to the web server.
B2	The client downloads the web logon page from the web server.
B3	A logon packet is sent to the VPS.
B4	The URT VPS sends a packet to the LDAP or RADIUS server to authenticate the user.
B5	The LDAP or RADIUS server sends an authentication response to the VPS.
B6	If changing VLANs, the VPS returns a VQP response to the switch. **Note** If authentication fails, process continues with step B7.
B7	The client is put into the user or group VLAN. **Note** Process continues with step B9.
B8	If not changing VLANs, the VPS responds to the logon. **Note** Process ends with this step.
B9	The client releases the IP address from the DHCP server.
B10	The client renews the IP address from the DHCP server.
B11	The second logon packet is sent to the VPS.
B12	The VPS responds to the logon request.

Differences Between Microsoft Networking and Novell NetWare

Handling of Microsoft Networking Logons

1. If the username is mapped to a VLAN, URT switches to the selected VLAN.

2. If the username is not mapped to a VLAN, but the user's primary group is mapped, URT switches to the group VLAN.

3. If neither of the previous two conditions applies, but the user is a member of any group mapped to a VLAN, URT switches to the group VLAN. (Select the first group in the Groups list that has a VLAN policy.)

4. If none of the previous three conditions apply, URT uses the default VLAN for the VTP domain.

Handling of Novell NetWare Logons

1. If the NDS username is mapped to a VLAN, URT switches to the selected VLAN.

2. If the NDS username is not mapped to a VLAN, but the user is a member of an organizational unit, URT switches to the organizational unit VLAN (if one is assigned).

3. URT checks VLAN policies to find organizational units that contain the user.

   An example of an organizational unit for user Ken might be:

   Ken.California.USA.NorthAmerica.

   In this example, the organizational unit *California* contains the user *Ken*. URT looks for VLAN policies in the same order: Ken, then California. URT switches to the organizational unit-based VLAN policy for California (if one is found).

4. If neither of the previous conditions applies, URT uses the default VLAN for the VTP domain.

Web-Based Logon Authentication

URT supports web-based authentication for Windows, Linux, and MacOS clients through LDAP (Active Directory and NDS) and RADIUS servers. The VPS determines the VTP domain of the switch and uses the corresponding VLAN to assign the switch port VLAN.

Note   You must modify the DHCP setting so the logon VLAN uses the VPS as the DNS setting. When a user logs on from the web, the web page address is queried in DNS. The response to the query is the IP address of the current VPS system; the URT web logon page is then displayed.

For RADIUS servers, you must add a server attribute to indicate the VTP/VLAN assigned to a user. The RADIUS server returns this attribute when a user is successfully authenticated.

Understanding Logoff Processing

Figure 1-5 illustrates a user logging off the network with URT installed; Table 1-8 explains the logoff sequence.

Note   The process is essentially the same whether the user logs off from a Windows/NDS domain controller or from the web.

Figure 1-5   URT-Based Traditional and Web Logoff Sequence
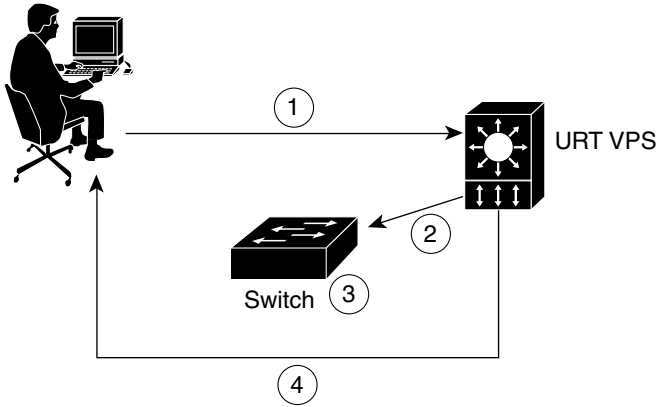
Stop here if VLAN is not changed on switch port in step 3.
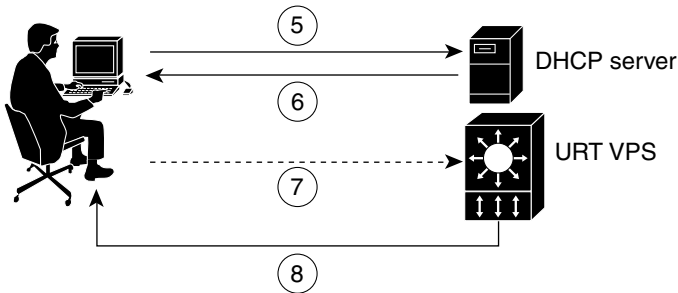
Table 1-8   Description of Traditional and Web Logoff Sequence

Step	Description
1	A logoff packet is sent to the URT VPS.
2	If changing VLANs, the VPS sends a VQP response to the switch.
3	The client is put into the logon/MAC VLAN. **Note** Process continues with step 4.
4	If not changing VLANs, the VPS responds to the logoff. **Note** Process ends with this step.
5	The client releases the IP address from the DHCP server.
6	The client renews the IP address from the DHCP server.
7	The second logoff packet is sent to the VPS.
8	The VPS responds to the logoff request.

Implementing URT in Your Network

After reading the material in this chapter to familiarize yourself with the URT basics, perform the following tasks to implement URT in your network.

Step 1   Import data from CiscoWorks2000 or a comma-separated value (CSV) file, then add switches manually. (See Chapter 2, "Getting Started with URT.")

Step 2   Add VPSs and configure switches to use them. (See Chapter 3, "Managing VLAN Policy Servers.")

Step 3   Configure domains, directories, and servers:

- Configure domain options.
- Install the URT logon script.
- If applicable, add and configure RADIUS servers.
- If applicable, add and configure LDAP servers.

(See Chapter 4, "Setting Up Domains, Directories, and Servers.")

Step 4   Associate VLANs and users:

- Enter subnets and masks for each VLAN.

- Set a default logon VLAN.

- Associate users to VLANs.

(See Chapter 5, "Managing VLANs and Users.")

Step 5   Customize the Web Client Interface for web logons. (See Chapter 6, "Setting Up and Using the URT Web Client Interface.")

Step 6   Install the URT Client Module for traditional logons (if not done automatically). (See Chapter 7, "Managing the Traditional Client Module.")

Step 7   (Optional.) You might need to remove URT from your network. (See Chapter 8, "Removing URT.")

Getting Started with URT

These topics explain how to get started with the User Registration Tool (URT):

- Starting URT, page 2-1
- Using the URT Main Window, page 2-2
- Adding Information to the URT Administrative Server, page 2-9
- Customizing URT Options, page 2-13
- Backing Up and Restoring the URT Administrative Server, page 2-17

Starting URT

To make administrative changes to URT, you must first start the application. URT VPSs and clients are typically started automatically when the systems on which they are installed are booted.

To start URT, select **Start > Programs > Urt > Start User Registration Tool**.

The URT main window is displayed; this is the starting point for using the URT Administrative GUI.

Using the URT Main Window

When you start URT, the main window is displayed, showing folder information in the left pane and information about the selected folder item in the right pane.

Note   Unless otherwise noted, you run all procedures in this guide from the URT main window.

Figure 2-1 shows the URT main window.

Figure 2-1   URT Main Window
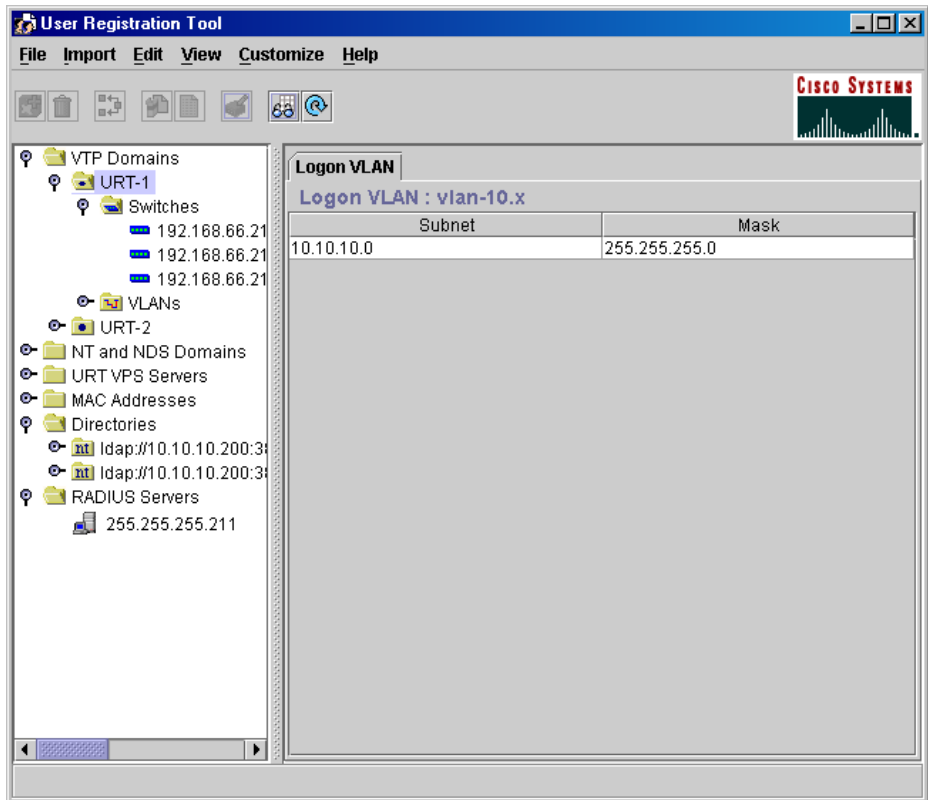
Understanding Folder Items

The expandable folders show the following:

- VTP domains—including switches and VLANs.
- NT and Novel Directory Services (NDS) domains—including usernames, groups, organizational units, and NT hosts.
- URT VPSs.
- MAC addresses.
- Directories (LDAP servers including Active Directory and NDS domains).
- RADIUS servers.

Tips for Working with Folder Items

- To change the settings for a folder item, select the item, then select an appropriate command from the menus.
- To change the associated attributes for usernames, groups, organizational units, or VLANs, double-click the folder name.
- To expand or collapse a folder, click the icon next to the folder or click the folder.

Understanding Folder Item Information

When you start URT, all VTP domains, switches, and VLANs known to URT are displayed in the left pane. You can add or import additional network information from CiscoWorks2000, from a comma-separated value (CSV) file, or by adding individual devices.

You must add NT domains, NDS and LDAP directories, and RADIUS servers manually.

The selected folder item attributes are displayed in the right pane of the URT main window.

Note If no attributes are associated with the selected item, nothing is displayed in the right pane.

Tips

- To rearrange the columns, click a column heading, then drag it to the desired location in the display.

- To sort the column information, click the column heading.

- You cannot print any of the displays.

Table 2-1 describes the information displayed for selected folder items.

Table 2-1   Information Associated with URT Folder Items

Column	Information Displayed	Description
Name of VTP domain (folder)	Logon VLAN	Information about the logon VLAN for the VTP domain. If more than one subnet and subnet mask are used on the VLAN, separate lines are displayed for each subnet and mask pair.
Switch (items in the Switch folder in a VTP domain)	VPS Address	IP addresses for the URT VPSs used by the switch, including VPS types (primary or secondary) and which server is currently being used by the switch.
VLAN (items in the VLAN folder in a VTP domain)	Logged On Users	Logged on users associated with the VLAN.
NT or NDS domain	Logged On Users	Detailed information about users logged onto the domain: • Username • Hostname • IP Address • Subnet • Gateway • VTP domain • VLAN • Switch • MAC Address • Port • Last Seen

Table 2-1   Information Associated with URT Folder Items (continued)

Column	Information Displayed	Description
NT or NDS domain (continued)	Logged On Users	To move the columns, drag and drop them; to sort the data, double-click a column heading. To assign a VLAN more quickly, you can select an NT group to display users in that group, rather than displaying the whole domain.
User name	VLAN Associations	VLAN associations you created for the logged on user. There are separate lines for each VTP domain in which you created a VLAN association for the user.
Group or organizational unit	VLAN Associations	VLAN associations you created for the group or organizational unit. There are separate lines for each VTP domain in which you created a VLAN association for the group or organizational unit. Also lists logged on users.
NT Hosts	Host List	Windows NT systems in the NT domain, including the status and current version of the URT Client Module on that system. Systems are not listed for NDS directories.
VPS (item in the URT VPS Servers folder)	VPS Clients	Switches configured to use the URT VPS as a VMPS; also indicates whether the server is a primary or secondary VPS for the switch.
MAC Addresses	MAC Addresses	All MAC addresses for which there are VLAN mappings. **Note** To map VLANs to MAC addresses, see the "Adding MAC Addresses and Host Mappings" section on page 5-10.
Directory	LDAP Users	Configured LDAP (NDS and AD) directories and logged on users.
RADIUS Server	RADIUS Users	Configured RADIUS servers and logged on users.

Understanding Folder Icons

After you add a domain or directory, URT queries the server and shows all users, groups, and organizational units defined in that domain or directory.

Table 2-2 describes how user, group, and organizational unit name icons are color-coded to indicate their status.

Table 2-2   Color-Coding of URT Icons

This Icon Color...	Indicates that the name is...
Gray	Not associated with a specific VLAN.
Blue	Associated with a specific VLAN in at least one VTP domain.
Gray with red X	Currently defined in the URT Administrative Server database but no longer defined in the domain server, NetWare server, or directory. **Note** This name is automatically deleted from the database the next time you save your changes in the URT Administrative Server. A red X icon also indicates deleted VLANs and VPSs that are unavailable. When a VPS becomes available, the red X is no longer displayed.
Gray with blue X	Associated with a VLAN that no longer exists. You should associate this name with a different VLAN.

Refreshing Folder Contents

Any changes you make in the NT domains and NDS directories are not reflected in the URT folders until you refresh those folders. For example, you should refresh your view if you add or delete a user, group, or organizational unit in the domain or NDS NetWare server.

- If your NT user account does not have Administrator authority in an NT domain that you are refreshing, you are prompted for a username and password that *do* have Administrator authority. Enter the username using the format *NT_domain\username*.

- To refresh NDS directories, you must have browse and read privileges for the directory. If you do not have these privileges, you must exit URT and log onto the NetWare network from an appropriate account.

Note A refresh updates the URT list folder, but changes to NT group or organizational unit membership do not affect user logons until the VPS lists are also refreshed.

Step 1 Select a folder.

Step 2 Click **Refresh**, or select **View > Refresh**.

Note Refreshing a VTP domain does not refresh the list of switches in the domain. If you add or delete switches in your network, you must add or delete the switches in URT.

Finding a User or Resource in a Folder

If there is a large number of users or other resources (such as VLANs, VTP domains, switches, and so on), you can use the **Find** command to search for them.

Step 1 Select **Edit > Find**.

Note You can use the **Find** command only to find items in folders. You cannot search for information displayed in the right pane.

The **Find** command searches down through the folders from the current cursor position. If the search finds no match, move the cursor to the topmost folder, then retry the search.

Step 2   Enter the text or IP address you want to find.

> ✎
>
> **Note**   Check **Match Case** if you want to find only those items spelled exactly
> as you entered them.

Step 3   Click **Find Next**.

If found, the item is highlighted. If the item is found in a closed folder, that folder
opens.

Using Common Buttons

The button bar in the URT main window contains icons that you can use as
shortcuts for common tasks. These buttons—displayed below the main menu
items (**File**, **Import**, **Edit**, and so on)—perform the same function as the menu
items. For example, clicking **Add** produces the same results as selecting
Edit > Add.

Some commonly used buttons are described in Table 2-3.

> 🔍
>
> **Tip**   Move your mouse over each button for information about its function.

Table 2-3   Common Buttons

Button	Function	Usage Notes
	Add	To add a user, server, directory, or other component, select a folder in the left pane, then click **Add**.
	Delete	To delete a user, server, directory, or other component, select a folder item in the left pane, then click **Delete**.

Table 2-3   Common Buttons (continued)

Button	Function	Usage Notes
	Configure	To set options for the user, server, directory or other component, select a folder item in the left pane, then click **Configure**.
	Refresh	To refresh the contents of the main window or the History Log window, click **Refresh**.

Adding Information to the URT Administrative Server

You must add network information to the URT Administrative Server to provide URT with data to manage logons—including the assignment of users, groups, or organizational units to specific VLANs. You can:

- Import data from CiscoWorks2000.
- Import data from a comma-separated value (CSV) file.
- Add or delete individual switches.

If URT is already active on the network, changes to the Administrative Server take effect immediately.

Importing Network Information from CiscoWorks2000

To provide URT with information collected by CiscoWorks2000, you can import network information from a CiscoWorks2000 Web Server into your network. URT imports the following information:

- VTP domains
- VLANs
- Switches
- SNMP community strings for any imported switches
- MAC addresses discovered by CiscoWorks2000

Step 1 Select **Import > Import from CiscoWorks2000**.

Step 2 Enter the IP address of your CiscoWorks2000 Web Server.

Step 3 Enter the port that the server uses (typically port 1741).

Step 4 Enter your username and password.

Step 5 Click **Connect**.

URT downloads network information from the CiscoWorks2000 Web Server and displays the imported information in the URT main window.

> ✎
>
> **Note** The information you enter in the Import from CiscoWorks2000 window is saved in URT and used when you refresh information from CiscoWorks2000. To delete this information from URT, click **Delete** in the Import from CiscoWorks2000 window.

Refreshing Network Information from CiscoWorks2000

If you imported network information from CiscoWorks2000, you can refresh the data by selecting **View > Refresh from CiscoWorks2000**.

If an error message tells you there is no CiscoWorks2000 Server from which to import data, this indicates that no logon information for the CiscoWorks2000 Server is stored in URT. In this case you must reenter the login information.

Step 1 Select **Import > Import from CiscoWorks2000**.

Step 2 Enter the logon information.

Step 3 Click **Connect** to refresh the data.

For information about deleting switch and VTP domain information from URT, see the "Deleting Switches from URT" section on page 2-12.

If any information you deleted was imported from the CiscoWorks2000 Server, you can import the information into URT again when you select **View > Refresh from CiscoWorks2000**.

Debugging VPS Information from the CiscoWorks2000 Server

To access the CiscoWorks2000 Server for debugging VPS information, enter the following URL in your browser:

```
http:VPS_address/cw2000.html
```

Importing Network Information from a Comma-Separated Value File

You can import network information from a comma-separated value (CSV) file you create. Doing this might be useful if you do not have CiscoWorks2000, and you have a large number of switches to import.

Step 1 Create a CSV file using the following format: IP address, SNMP read-only community string, SNMP read-write community string.

For example:

```
10.10.10.10, public, private,
20.20.20.20, public, private,
```

Step 2 Repeat step 1 for every switch you need to import.

Step 3 Save the CSV file.

Step 4 Start URT.

Step 5 Select **Import>Import from file**.

Step 6 Navigate to the directory that contains your CSV file.

Step 7 Select the CSV file.

Step 8 Click **Import**.

URT imports the information from the CSV file and displays it in the main window.

Adding Switches to URT

You can add individual switches to be managed by the URT Administrative Server.

Step 1   Under the applicable VTP domain, select the Switches folder.

Step 2   Click **Add** or select **Import>Add Switch**.

Step 3   Enter the IP address of the new switch.

Step 4   Enter the SNMP community strings.

> ✎
>
> **Note**   The SNMP community strings are added to the URT database; URT does not change the SNMP community strings on the switch.

Step 5   Click **Add**.

URT adds the switch to the appropriate VTP domain in the main window.

Deleting Switches from URT

You can delete switches from the network information managed by the URT Administrative Server.

Step 1   From the VTP domain folder in the left pane, select a switch or switches.

Step 2   Click **Delete** or select **Edit>Delete**.

Step 3   In the confirmation dialog box, click **Yes**.

Step 4   To delete a VTP domain after you have deleted all switches in the domain, select the VTP domain folder.

Step 5   Click **Delete** or select **Edit>Delete**.

Step 6   In the confirmation dialog box, click **Yes**.

Any switch that you delete from URT must be reconfigured to use a switch-based VMPS instead of a URT VPS.

If you imported network information from CiscoWorks2000, network information is reimported every time you select **View > Refresh** in the CiscoWorks2000 Server. If the switch still exists in the network, the switch is displayed again in the folder after the refresh.

Customizing URT Options

To set the global URT parameters, select **Customize > Options**.

These topics describe the global parameters in more detail:

- Setting Web Options, page 2-13
- Enabling Trace and Refreshing User Data, page 2-14
- Setting History Options, page 2-15
- Retaining MAC-to-VLAN Associations, page 2-15
- Setting MAC Security Options, page 2-16

Setting Web Options

You can use web options to customize the page that web clients see upon logon. To do so, click the Web tab in the URT Options dialog box.

For more information about the web options, see the "Customizing the Web Logon Page" section on page 6-2.

Enabling Trace and Refreshing User Data

You use the administrative options to determine:

- Whether to include trace and debug messages in the URT Administrative Server log file. By default, this log file, which records interactions with the URT VPSs, resides in C:\Program Files\Urt\data\UrtAdminServer.log.

- The time of day to refresh the URT VPSs with updated group data.

> ✎
>
> **Note**   Setting this option affects *all* domain servers.

For each domain, you can enter a list of domain controllers to determine the order the Administrative Server uses during group refreshes. During a refresh, the Administrative Server checks the domain controllers in the order you specify. If the first one in the list is unavailable, it checks the next one in the list, and so on.

For more information about the domain options, see the "Configuring Domain Options" section on page 4-4.

Step 1   Select **Customize > Options**.

The URT Options dialog box is displayed.

Step 2   Click the Admin tab.

Step 3   Set the time at which to refresh the VPS with updated group entries.

The entries are refreshed once every 24 hours at the time you specify. If you do not set this time, the default value of midnight (00:00) is used.

Step 4   To add debugging and trace messages to the log file, select the Enable Trace checkbox.

Step 5   To change the name and location of the log file, enter a new filename and location or browse to select a file.

The log file shows interactions between the URT Administrative Server and the VPSs.

Step 6   Click **OK**.

Setting History Options

You use history options to determine whether to trace user logons and logoffs to the domain server. History files are stored in a central location.

Step 1   Select **Customize > Options**.

The URT Options dialog box is displayed.

Step 2   Click the History tab.

Step 3   To create history files, select the Enable history logging checkbox.

Step 4   Enter the log filename and location in the Logging directory text box or browse to select a file.

Step 5   You can manage files by date or by size.

- If you select **Date**, you can also select the Total days of history to store checkbox, then enter the number days for which you want to keep data.

- If you select **Size**, you can enter a maximum log file size and a maximum number of log files to store.

Step 6   Click **OK**.

Retaining MAC-to-VLAN Associations

You use URT global logon options to determine whether a system logging onto the network with MAC-to-VLAN mappings retains those mappings or if it uses URT user-based VLAN policies.

Note   Setting this option affects *all* systems logging onto the network.

You can also set specific logon options for different domains. For more information about the logon options, see the "Configuring Domain Options" section on page 4-4.

Step 1	Select **Customize > Options**.

The URT Options dialog box is displayed.

Step 2	Click the Logon tab.

Step 3	To preserve these mappings, select the Retain MAC to VLAN Associations checkbox.

> **Note** If you select this option but the system does not have MAC-to-VLAN associations, user-based VLAN policies are used**.**

Step 4	Click **OK**.

Setting MAC Security Options

For security reasons, you can use only MAC-assigned VLANs and block unregistered MAC addresses. A MAC address is registered if it has a VLAN association. If a system powers on with an unregistered MAC address, you can use one of these MAC security options:

- Place unauthorized users in a security violation VLAN instead of defaulting to the logon VLAN. For each VTP domain, you can define an unauthorized MAC VLAN to provide a higher level of security without requiring any changes to the switch.

- Shut down the port of unauthorized users. After a port is shut down, you can reenable it on the switch using the command-line interface or SNMP to provide the highest level of security.

Step 1   Select **Customize > Options**.

The URT Options dialog box is displayed.

Step 2   Click the MAC Security tab.

Step 3   To preserve these mappings, select the Only Allow MAC Assigned VLANs checkbox.

> ✎
>
> **Note**   If you select this option, select one of the options in step 4.

Step 4   Select one of the following:

- Use Unauthorized MAC VLAN—Places a user in a security VLAN if the MAC address does not have a MAC-assigned VLAN.

- Shut Down Port—Shuts down a user port if the MAC address does not have a MAC-assigned VLAN.

Step 5   Click **OK**.

Backing Up and Restoring the URT Administrative Server

The URT database contains XML files stored in the data folder on the disk drive where the URT Administrative Server is installed. As part of regular system maintenance, you should back up these files. If the system on which the URT Administrative Server resides becomes inoperable, you will need these files to quickly restore the URT Administrative Server on another system.

Step 1   Install the URT Administrative Server on the selected system.

For more information about the installation process, see *Installation and Setup Guide for the Cisco Secure User Registration Tool*.

Step 2   Move all XML files from the backup copy of the URT data folder to the URT data folder on the new system.

Step 3   To restore communication between the URT Administrative Server and the VPSs and domain servers, perform the following tasks from the main window:

   a. To delete the VPSs from URT, select the servers from the URT VPS folder.

   b. Click **Delete**.

   c. Add the same VPSs to URT. (See the "Adding a VPS" section on page 3-1.)

   d. When adding the servers again, you are prompted to reinstall the URT logon script on each domain server. To do so, follow the installation prompts.

Managing VLAN Policy Servers

Because all user logons to Windows NT domains or Novell Directory Services (NDS) directories use VLAN Policy Servers (VPSs), the VPSs must run smoothly and reliably. For web logons, VPSs authenticate users and use a web server to download the web logon page.

These topics describe how to manage your VPSs:

Adding a VPS

You can add VPSs to help balance the logon load and ensure better network performance.

Step 1   Highlight the URT VPS Servers folder.

Step 2   Click **Add** or select **Edit > Add**.

The Add URT VPS dialog box is displayed.

Step 3   Enter the IP address of the VPS and the appropriate port.

Step 4   Click **Add**.

URT displays a dialog box for each configured domain server or NDS NetWare server.

Step 5   To install the URT logon script on each domain server, click **Yes** in each dialog box.

> ✎
> **Note**   Reinstalling the logon script ensures that the URT Client Module acknowledges the new VPS.

To balance the logon load across all VPSs, you must decide which switches should be reconfigured to use the new VPS.

Step 6   Configure these switches to use the new server as a primary or secondary server by selecting the desired switches, then clicking **Configure Device** or selecting **Customize > Configure.**

Deleting a VPS

Before you delete a VPS, you should reconfigure switches that use that server. After you delete a VPS, you must reinstall the URT logon script to make sure that clients do not try to use the deleted server.

> ✎
> **Note**   If the deleted VPS was used for web logons and as a DNS, you must also change the settings on the DHCP server.

Step 1   Select the switches that use the VPS as a primary or secondary server.

Step 2   Configure those switches to use other VPSs.

> 🔍
> **Tip**   To determine which switches use a VPS, select the server; switches for that VPS are displayed in the VPS Clients list on the right pane.

Step 3   From the URT VPSs folder, select the server to delete.

Step 4   Click **Delete** or select **Edit > Delete**.

URT displays a dialog box for each configured domain server or NDS NetWare server.

Step 5   To install the revised logon script on each domain server, click **Yes** in each dialog box.

> ✎
> **Note**   Reinstalling the logon script ensures that the URT Client Module does not try to communicate with the deleted VPS.

> **Tip**
> If you prefer, you can use the switch command-line interface (CLI) to change the VMPS configuration on the switch.

Viewing and Configuring VPS Characteristics

VPSs are listed by IP address in the URT VPSs folder. You can view more detailed information about the servers or change configuration settings.

Step 1   All switches that use the selected VPS are displayed in the right pane with their VPS types (primary or secondary). Double-click the IP address of the VPS you want to configure.

> 🔍
> **Tip**   To view the most recent entries in a VPS log file, select a server, then select **View > Watch Server Log File**.

Table 3-1 describes the fields displayed in the configuration window.

Table 3-1   URT VPS Configuration Window

Field	Description
IP Address	Server IP address.
UDP port	The UDP port that the server uses.
Up since	The last date on which the server was restarted.
Server Version	Server software version.
Time Zone	Set the time zone for the VPS by selecting the appropriate time zone from the list. For more information about configuring the clock, see *Installation and Setup Guide for the Cisco 1101 VLAN Policy Server.*
Enable trace	If Enable trace is selected (the default), debugging and trace messages are written to the VPS log file. Deselect Enable trace to omit trace information from the log file.

Step 2   Click **OK**.

Note   For more information about the time the URT Administrative Server refreshes the VPS with user data, see the "Enabling Trace and Refreshing User Data" section on page 2-14.

Viewing VPS Log Files

A log file is created for each URT VPS. By default, diagnostic and debugging information is included in the log file, but you can omit this information by disabling trace for the server.

You can open a Watch Server Log File window for each VPS. The VPS IP address is displayed in the title bar of the Watch Server Log File window.

For more information about enabling or disabling trace, see the "Viewing and Configuring VPS Characteristics" section on page 3-3.

You can view the most recent entries in the log files and monitor new entries as they are added.

Step 1   Select a server from the URT VPSs folder.

Step 2   Select **View > Watch Server Log File**.

You can view the complete contents of a VPS log file.

Step 1   Open the CiscoWorks2000 Server on the system on which the VPS resides.

Step 2   Select **Server Configuration > Diagnostics > View Server Logs**. (The log file for the VPS is UrtVpsServer.log.)

> ✎
> **Note**   Interactions between the URT Administrative Server and the VPS are also logged. For more information, see the "Enabling Trace and Refreshing User Data" section on page 2-14.

Configuring Switches to Use a VPS

Before URT can place a user into a VLAN, you must configure the switch to which the user's system is attached to use the VPS as a VMPS. Switches use the VPS to obtain information about VLANs and the users and systems assigned to those VLANs.

You must configure a switch whenever:

- You add a new switch to the network. (You need to configure only the new switch.)

- You add a new VPS. (You must add the VPS as a primary or secondary server to the VMPS configuration of all switches that you want to use the new VPS.)

- You delete a VPS. (You must delete the VPS from the VMPS configuration on all switches that use it.)

- VPSs that are primary and secondary to a switch are configured to send keepalive packets to each other to confirm operational status.

When you configure switches to use a VPS, the VPS begins assigning users to VLANs. If the domain servers in the network have not yet been configured to run the logon script, users are assigned to MAC-based dynamic VLANs or the default logon VLAN.

For more information, see the "Setting Domain Logon Options" section on page 4-4.

Using Primary and Secondary VPSs

You can use more than one VPS to provide fault tolerance. You can install two or more VPSs and configure the switches to alternate between the server that is used as the primary server and the server that is used as the secondary server.

Note   You can designate up to two secondary VPSs for each switch.

By using more than one server, you ensure network connectivity even if one server becomes unavailable.

Keepalive packets are sent to the VPSs every 60 seconds to determine if they are up and running. If all VPSs fail, users connected at the time of failure are not affected. Users who power up or try to log onto switches that use the failed servers are placed in the default VLAN defined on the switch (for static ports) or the VLAN to which they are currently connected (for dynamic ports).

If a user is connected to a dynamic port and restarts (or initially switches on) the workstation while all VPSs are down, that user cannot be connected to a VLAN.

Note   This is the only situation in which URT can prevent a user from connecting to the network.

Configuring Switches From the URT Main Window

⚠️

Caution   You must configure switches using the URT main window; do not use the switch command line.

For URT to configure VMPS on a switch, you must first set the correct SNMP write community string for the switch.

Step 1   In the main window, select **VTP Domains > Switches**.

Step 2   Select the switch to configure.

🔍

Tip
- You can select a range of switches using the **Shift** and **Ctrl** keys. The selected switches are assigned the same VPSs.
- If you want all switches to use the same VPS configuration, you can select the Switches folder or the VTP domain folder instead of selecting individual switches.

Step 3   Click **Configure Device** or select **Customize > Configure**.

The Device Configuration dialog box is displayed.

Step 4   Select the IP address for the first, second, and third VPS.

Step 5   Select whether the switch should use the server as a primary or secondary server.

✎

Note   A switch can have two secondary servers but only one primary server.

Step 6   In the Reconfirm Interval text box, enter a value of 60 minutes or less.

A reconfirm interval of 60 minutes reconfirms the VPS once each hour. Reconfirming more frequently puts more load on your switches.

✎

Note   Some switches do not allow you to edit the reconfirm interval.

Step 7   In the Retry Attempts text box, enter **3** (the default).

This is the number of times a switch retries to reconfirm before going to a secondary VPS.

✎
Note   Some switches do not allow you to edit the retry interval.

Step 8   Click **OK**.

Switch Configuration Notes

- If a switch does not allow modifications to some settings, those options are grayed-out in the Device Configuration dialog box.
- The switch uses the primary server unless it is unavailable, in which case it reverts to the secondary servers in the order you specified.

✎
Note   To determine which server the switch is using, select the switch, then look at the VPS Address column.

- If all VPSs that a switch uses are unavailable (because of network connectivity or hardware problems), users connected to that switch remain in the default VLANs defined on the switch ports. Users are not prevented from logging onto the network.
- You can designate only one VPS as the primary server for any switch.
- All switches that use the selected VPS are displayed in the right pane with their VPS type (primary or secondary).
- If you have a large network of users accessing a logon VLAN, consider setting up a VPS to serve all web logons. You can configure this VPS as the secondary VPS to the switch.

- If you prefer, you can use switch commands to set the VPS as the switch VMPS.

- You can load-balance between a set of VPSs by assigning one VPS as the primary server for some switches, and a secondary server for other switches.

> **Note** Do not designate a single VPS the primary server for all switches unless you have only one VPS.

Verifying the Switch Configuration

To verify that URT configured the switch, telnet to the switch and use the **show vmps** command. The results should show that VMPS is disabled, indicating that there is no VMPS on the switch.

If the VMPS is enabled, use the **set vmps state disable** command to disable it. The **show vmps** command should also show the URT VPS IP address being used for the VMPS domain server.

> **Note** For the appropriate commands, see your switch documentation.

VPS Switch Reconfirms and Retries

The VPS sends device reconfirms to only five switches simultaneously and waits 5 seconds before sending more reconfirms. This method staggers and slows the reconfirming of multiple switches to avoid the packet loss that can occur when many switches reply simultaneously.

The retry attempts value is the number of times a switch retries a reconfirm before going to a secondary VPS. Three retries are recommended.

You can view and edit the reconfirm interval and retry setting for most switches. For more information, see the "Configuring Switches From the URT Main Window" section on page 3-7.

> **Note** Some switches do not allow you to edit the reconfirm and retry settings.

Updating VPSs with New Group or Organizational Unit Lists

The VPSs refresh their lists of NT group members once a day at the time specified in the URT options. For information about setting the related options, see the "Enabling Trace and Refreshing User Data" section on page 2-14.

You can also check manually by clicking **Refresh** or selecting **View > Refresh**.

If you make many changes to NT group membership, those changes do not affect user logons until the VPSs refresh their lists.

You can enter a list of domain controllers for each domain to determine the order the Administrative Server should use during group refreshes. During a refresh, the Administrative Server checks the domain controllers in the order you specify. If the first controller in the list is unavailable, it checks the next one on the list, and so on. For more information, see the "Configuring Domain Options" section on page 4-4.

You can force URT to update the NT group lists.

Step 1 Select the groups or NT domain for the user lists you want to update in the URT VPSs.

> ✎
>
> **Note** If you select a group or domain, all groups for the domain are updated.

Step 2 Select **Configure > Update URT VPS Group Entries**.

The VPSs update the group and organizational unit membership lists with the information currently in the domain servers.

Setting Up Domains, Directories, and Servers

Traditional logon domains are NT and Novell Directory Services (NDS) domains. Web logon domains include Lightweight Directory Access Protocol (LDAP) directories (AD and NDS) and Remote Authentication Dial-In User Service (RADIUS) domains.

These topics describe how to set up domains, directories, and servers:

Having Authority in Domains

Table 4-1 describes the authorities you must have to change domains or directories in URT.

Table 4-1   Authorities Required to Change Domains and Directories

Domain or Directory	Required Authority
Microsoft Networking domain	To install files on the domain server and view the domain, you must have Administrator authority in that domain.
	If you try to perform tasks on a domain for which you do not have Administrator authority, URT prompts you for a username and password with the appropriate authority. Enter the username using the format *NT_domain\username*.
	If you log onto a domain from a non-Administrator account, you cannot make changes to settings for that domain in URT.
Novell NetWare NDS directory	To make changes to an NDS directory, you must have read and browse privileges for that directory.
	• If you are not logged onto the NDS directory you are changing, you are prompted to log on with a user account with privileges.
	• If you are logged onto NDS without browse and read privileges for the directory, you must exit URT and log onto the NetWare network from an appropriate account.
LDAP directory	To manage LDAP servers, you must enter your LDAP user ID in LDAP format (for example, `cn=`*`username`*, `cn=`*`Users`*, `dc=`*`domainname`*, `dc=`*`company`*, `dc=`*`com`*) and enter your LDAP password.
RADIUS server	To manage RADIUS servers, you must enter your RADIUS authentication and accounting keys.

Adding NT Domains and NDS Directories to URT

You must add the NT domains and NDS directories you want URT to manage to the NT and NDS Domains folder.

Note   When you add an NT domain or NDS directory to your network, you must also add the domain or directory to URT.

You must have NT Administrator authority in the domain or NDS read and browse privileges in the directory. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1   Select the NT and NDS Domains folder.

Step 2   Click **Add** or select **Edit > Add**.

The Domain Name window is displayed.

Step 3   Select the name of the NT domain or NDS directory you want to add. If the domain or directory is not in the list, enter it in the text box.

Step 4   Click **OK**.

URT creates a folder for the NT domain or NetWare directory, listing all users defined in the domain or directory.

Note
- If the domain or directory has a long list of users, groups, or organizational units, it might take several minutes to download the list.

- Users, groups, and organizational units assigned to a VLAN are represented by blue icons; those not assigned to a VLAN are represented with gray icons.

Configuring Domain Options

You must configure domain logon options for each domain server. You can also enter a list of domain controllers for each domain to determine the order the Administrative Server uses during group (membership) to VLAN assignment refreshes.

Setting Domain Logon Options

You can set domain logon options to edit the URT logon script that resides on each domain server and runs from the network logon script. All users in a domain are assigned the domain logon options you configure.

You must have NT Administrator authority in the domain or NDS read and browse privileges in the directory. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1 Open the NT and NDS Domains folder.

Step 2 Select a domain folder.

Step 3 Select **Customize > Configure Domain Options**.

Step 4 Click the Logon Options tab.

Step 5 Select the desired domain options.

Step 6 Enter any required information.

Each option is described in Table 4-2.

Step 7 Click **OK**.

URT displays a list of domain servers or NDS NetWare servers found in the selected domain.

Step 8 To install the new logon script options on the domain servers, click **Yes.**

> ✏️
>
> **Note** Your changes do not take effect until you install them on the domain servers; to do so, click **Yes.**

Table 4-2   Domain Logon Options

Option	Description	Usage Notes
Enable auto install and upgrade for Windows NT/2000 (*supported on Microsoft Networking only*)	Installs and upgrades the URT Client Module automatically on Windows NT, Windows 2000, and Windows XP (Professional) clients (enabled by default).	If you use NetWare, you must use ZENworks to automate installation of the URT Client Module.
Sleep time to wait for auto install completion (in seconds)	Number of seconds to wait before retrying automatic installation of the URT Client Module.	Enter the number of seconds; use this option on slower systems.
Unmap network drives on log out	Unmaps network drives when the user logs off.	Select to enable.
Enable trace	Adds debug and trace information to the OnOffHandler.log and UrtService.log files on users' workstations. When trace is not enabled, only error and critical messages are written to the log files. • The OnOffHandler.log file, stored in the user's %TEMP% directory, or (depending on the Windows platform) *drive*:\Windows\Temp or *drive*:\WINNT\Temp, records the installation and upgrade of the Client Module. • The UrtService.log file, stored in the user's %TEMP% directory, or (depending on the Windows platform) *drive*:\Windows\Temp or *drive*:\WINNT\Temp, records interactions between the Client Module and the VPS.	Enable to troubleshoot or debug a problem.

Table 4-2   Domain Logon Options (continued)

Option	Description	Usage Notes
Quit when logon failure occurs	Logs off users on static and dynamic ports after logon failures.	Select if there are several static ports in your network. Static port logon failures can cause excessive network traffic.
Delay running of URT Client Module after logon (secs)	Number of seconds to delay running the Client Module.	Enter the number of seconds to delay. Use this option to avoid conflicts between the Client Module and other services on startup.
Delay switching of VLAN after logoff (secs)	Number of seconds to delay switching a user's VLAN on logoff (selected by default with a delay value of 1).	Enter the number of seconds to delay. Use this option to provide Windows 2000 enough time to write a user's roaming profile during logoff.
Batch file to execute after URT Client module completes	Batch filename and path to run automatically after the Client Module completes.	Enter a batch filename and path to run. Use this option for map files or to run programs such as a virus detection program.
Other future options	Reserved for future use.	—

Setting the Group Refresh Order

To determine the order that the Administrative Server uses during group refreshes, you can enter a list of domain controllers for each domain. During a refresh, the Administrative Server checks the domain controllers in the order you specify. If the first controller in the list is unavailable, the server checks the next one on the list, and so on.

By default, the Primary Domain Controller (PDC) is first in the list, followed by all Backup Domain Controllers (BDCs).

✎

Note   You can rearrange the order to suit your needs. For example, you can place BDCs at the top to refresh first and reduce the load on your PDCs. If you move a BDC to the top of the list, it is checked before the PDC; however, you must first make sure that the BDC is properly synchronized with the PDC. You can also remove the PDCs from the list to further reduce the load.

Step 1   Select **Customize > Configure Domain Options**.

Step 2   Click the Group Refresh Order tab.

Step 3   To change the position of a BDC in the list, select the BDC, then click **Up** (to move it higher) or **Down** (to move it lower).

✎

Note   Click **Refresh Group List** to return the list to the default order. If you click this in error, click **Cancel**. If a domain controller has recently been added to or deleted from the network, the changes are reflected when you click **Refresh Group List**.

Step 4   To delete a domain controller from the refresh list, select the domain controller, then click **Remove**.

Step 5   To confirm the deletion, click **Yes**.

Step 6   After reordering the domain controllers, click **OK**.

Manually Installing the URT Logon Script

URT automatically prompts you to reinstall the logon script when you make changes that require it (for example, when changing domain logon options).

If you did not install the logon script when prompted, you can do so later using the instructions in this section.

You must have NT Administrator authority in the domain or NDS read and browse privileges in the directory. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1   Select an NT domain or NDS directory.

Step 2   Select **Customize > Install URT Logon Script**.

URT displays a list of domain servers or NDS NetWare servers found in the selected domain.

Step 3   Click **Yes**.

URT installs the URT logon script (urt.bat) on the domain servers and NDS NetWare servers, and displays a message box to show the status of the installation.

Step 4   If necessary, repeat this procedure for every NT domain or NDS directory in your network.

> **Note**   You must manually add any NT domains or NDS directories that are missing from the NT and NDS Domains folder. To do so, select the NT and NDS Domains folder, then click **Add** or select **Edit > Add**. Enter the name of the missing domain or directory (or select one from the list), then click **OK**.

Configuring Users to Run the Domain Logon Script

You must update (or create) the URT logon script (urt.bat), on your primary domain server. You run this procedure once to make sure that users run the logon script at logon. Running the script directs user logons to the URT VPSs.

- To edit the logon script on the NT domain server, you must log onto the system from an account that has Administrator privileges, or be able to connect to the drive containing the script from another workstation where you have Administrator privileges.

- For NDS, you must have read and browse privileges in the directory. For more information, see the "Having Authority in Domains" section on page 4-2.

Domain Logon Script Configuration Procedure for Microsoft Networking

If you do not already have a logon script, you must either create one or associate users directly with urt.bat as the logon script.

For NT domain servers, the urt.bat file is installed in the NETLOGON directory.

The directory is *%SYSTEMROOT%*\system32\repl\import\scripts, where *%SYSTEMROOT%* is the root directory for operating system files.

For example, if you installed Windows NT into C:\WINNT, the NETLOGON directory is C:\WINNT\system32\repl\import\scripts.

> **Note**   If you set NT replication to include logon scripts and one of the backup NT domain servers is unavailable during Client Module installation, the logon scripts are copied to that domain server. If you are not using replication for logon scripts, you must update the logon script on all domain servers.

Step 1   To update a logon script, add the following instruction as the first line of the logon script on the NT primary domain server:

```
@call %0\..\urt.bat
```

Step 2   To associate users directly with urt.bat as the logon script:

   a.   Start the Windows User Manager administrative tool.

   b.   Double-click a username.

   c.   In the User Properties window, click **Profile**.

   d.   In the User Environment Profile, enter **urt.bat** in the Logon Script Name text box, then click **OK**.

Domain Logon Script Configuration Procedure for Novell NetWare

⚠️

Caution   If you are using Novell NetWare, do not edit the urt.bat file.

Use the Novell Application Launcher (NAL) program to add this instruction to the logon properties for the organization object that contains the users, groups, and other organizational units you want to manage:

```
@\\%FILE.SERVER\sys\public\urt\urt.bat %FILE_SERVER
```

Deleting NT Domains or NDS Directories from URT

If you no longer want to manage the users in a particular NT domain or NDS directory, you can remove the domain or directory from the NT and NDS Domains folder in URT.

✎

Note   Deleting a domain or directory removes all user associations to VLANs for that domain or directory.

You must have NT Administrator authority in the domain or NDS read and browse privileges in the directory. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1   Select the domain or directory in the NT and NDS Domains folder.

Step 2   Click **Delete** or select **Edit > Delete**.

Step 3   In the confirmation dialog box, click **Yes**.

Step 4   To remove URT completely from the domain:

    a. Remove the Client Module from user workstations in the domain. For instructions, see the"Removing the URT Client Module from the Network" section on page 8-3.

    b. Stop the domain servers from directing user logons to URT VPSs, then delete the urt.bat file. For instructions, see the "Removing URT from Its Role in Handling User Logons" section on page 8-7.

Deleting a VTP Domain from URT

You can delete a VTP domain after all switches in the domain are removed.

Step 1   Select the VTP domain folder to delete.

Step 2   Click **Delete** or select **Edit > Delete**.

Step 3   In the confirmation dialog box, click **Yes**.

Managing LDAP Servers

For web logons, URT supports Active Directory (AD) and NDS domains that use Lightweight Directory Access Protocol (LDAP). When a web client logs on from an LDAP domain, the VPS searches that LDAP tree to locate the user. URT searches the LDAP tree from bottom to top until it finds a VLAN association for the user. If no VLAN associations are found, the user remains in the current (logon) VLAN.

URT supports redundant LDAP servers. If the primary LDAP server fails, URT can query a second or third LDAP server for the user, group, or organizational unit assignment.

Searching an LDAP Directory

When searching for a string in the Directories folder, URT looks only in the expanded folders in the left pane, not in closed folders. You can expand your search to specific directories.

Step 1   Expand the folders under the Directories folder.

Step 2   Select the top-level directory.

Step 3   Select **Edit > Find**.

Step 4   Enter the search string.

Adding LDAP Servers

You must add the LDAP servers you want URT to manage to the Directories folder in URT. You can add multiple LDAP directories and assign VLANs at any point in the LDAP tree to users, groups, or organizational units. The tree supports multiple tree levels.

You must have an LDAP logon and have NDS read and browse privileges in the directory. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1   Select the Directories folder.

Step 2   To add a new directory, click **Add** or select **Edit > Add**.

Step 3   In the Add Directory window, click the AD or NDS tab (depending on your platform).

Step 4   Enter the LDAP server host and port for the LDAP server.

Step 5   Enter your LDAP user ID in LDAP format (for example, `cn=`*`username`*, `cn=`*`Users`*, `dc=`*`domainname`*, `dc=`*`company`*, `dc=`*`com`*).

Step 6   Enter your LDAP password.

Step 7   Select the interval at which the Client Module looks up the user in the LDAP tree to determine if the user's Distinguished Name (DN) has changed.

Step 8   Enter the base DN.

The base DN is the base name used to search for organizational units and users. To obtain the base DNs on the server, click **Get Initial DN**.

✎

Note   You can add the same LDAP server multiple times if the base DN is unique for each instance.

Step 9   If you are adding a directory exclusively for web logons, select the Web-only logon domain checkbox.

✎

Note   If you also want to use the directory for traditional logons, do not select this checkbox.

   • For AD servers—Enter the NT Administrator user ID and password in the User ID and Password fields.

     URT installs the logon batch script on the domain controller and supports auto-install of NT clients.

   • For NDS servers—Enter the domain name or select it from the Domain Name list.

     URT cannot retrieve the domain name for NDS servers. Because NDS does not support auto-install, the NT user ID and password are not required. (NDS has a proprietary Novell logon screen that prompts for a user ID and password during installation of the NDS logon script.)

Step 10   Click **OK**.

URT creates a folder for the domain or directory, and all defined users are listed in the new folder.

✎

Note   • Users who are not assigned to a VLAN are represented by gray icons.

   • Hosts assigned to a VLAN are represented by blue icons.

Configuring LDAP Servers

You might need to change configuration settings after adding an LDAP server.

You must have an LDAP logon and NDS read and browse privileges in the directory. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1   In the Directories folder, click the LDAP server to be reconfigured.

Step 2   Click **Configure** or select **Customize > Configure**.

Step 3   Make the desired changes to the configuration setup.

Step 4   Click **OK**.

Deleting LDAP Servers

You must have an LDAP logon and NDS read and browse privileges in the directory. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1   In the Directories folder, click the LDAP server to delete.

Step 2   Click **Delete** or select **Edit > Delete**.

Step 3   Click **Yes** in the confirmation dialog box.

Setting LDAP Web Associations

In addition to VLAN associations, you can set web associations for an LDAP server.

Step 1   In the Directories folder, double-click an LDAP server.

Step 2   Click the Web Associations tab.

Step 3   To log on the user and remove the logoff window, select the checkbox.

> ✎
> **Note**   If you select this option, web users do not have a logoff window. They remain logged on until they power off or disconnect their systems.

Step 4   Click **OK**.

Managing RADIUS Servers

For web logons, URT supports the use of RADIUS server authentication from Cisco Secure ACS and other AAA servers. You can add multiple RADIUS servers to authenticate web clients.

Overview of RADIUS Authentication Support

When a web user logs onto a RADIUS domain, the RADIUS server authenticates the user ID and password. If the user is successfully authenticated, the RADIUS attribute for the VLAN mappings is checked.

- If no VLAN mapping is found, the user remains in the current VLAN and the event is logged.
- If the VLAN mapping is found, URT searches the VTP domain and places the user in the assigned VLAN.

The RADIUS attribute has the following syntax:

```
VTPDomainName\VLANName;VTPDomainName\VLANName;
```

For example:

```
URT:Vlan-Association=URT-1\Vlan6;
URT:Vlan-Association=URT-2\Vlan16;
URT:Allow-Multiple-Users=TRUE;
URT:Logon-User-Only=FALSE
```

Table 4-3 shows the URT attributes that correspond with the RADIUS attributes.

Table 4-3   Corresponding URT and RADIUS Attributes

URT Attribute	RADIUS Attribute (Attribute Number)
User Name	User-Name (1)
Client IP Address	Framed-IP-Address (8)
MAC Address	Calling-Station-Id (31)
Subnet Address	Framed-IP-Netmask (9)
Gateway Address	Framed-Route (20)
Switch Address	NAS-IP-Address (4)
Switch Port	NAS-Port (5)
URT VPS	Called-Station-ID (30)
VTP Domain Name/VLAN Name	Vendor-Specific (24)

URT sends accounting records to the RADIUS server. The RADIUS server that authenticates a web user maintains the logon and logoff accounting data for that user. At a set interval, accounting packets are updated for all users logged onto URT.

Adding RADIUS Servers

You must have RADIUS authentication. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1   Select the RADIUS Servers folder.

Step 2   Click **Add** or select **Edit > Add**.

The Add RADIUS Server window is displayed (Figure 4-1).

Figure 4-1   Adding a RADIUS Server

Step 3 Enter the RADIUS server IP address.

Step 4 Enter the RADIUS server authentication port.

Step 5 Enter the RADIUS server accounting port.

Step 6 Enter the RADIUS reconfirm interval (in seconds). This is the frequency for sending accounting packets for currently logged on users.

Step 7 To verify client attributes while a client is logged on, select the Verify associations while logged on checkbox.

> **Note** If you do not select this checkbox, the VPS does not verify whether client attributes have changed while a client is logged on. Attributes are checked the next time the client logs on.

Step 8 Enter the interval for verifying client attributes. A client sync message takes 5 minutes and the default interval is 12 minutes; therefore, verification occurs every 60 minutes (12 x 5).

Step 9 Enter the domain name to display during web client logon.

Step 10 From the URT VPS Servers list, select the desired server.

Step 11 Enter the RADIUS authentication key.

Step 12 Enter the RADIUS accounting key.

> **Note** The authentication and accounting keys are the same for the Cisco ACS RADIUS server.

Step 13 Click **Add**.

> **Tip** You can reuse the domain name for a secondary (backup) RADIUS server.

Configuring RADIUS Servers

You might need to edit configuration settings after adding a RADIUS server.

You must have RADIUS authentication privileges. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1	In the RADIUS Servers folder, click the RADIUS server to reconfigure.
Step 2	Click **Configure** or select **Customize > Configure**.
Step 3	Make the desired changes to the configuration setup.
Step 4	Click **Add**.

Deleting RADIUS Servers

You must have RADIUS authentication. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1	In the RADIUS Servers folder, click the RADIUS server to delete.
Step 2	Click **Delete** or select **Edit > Delete**.
Step 3	Click **Yes** in the confirmation dialog box.

Managing VLANs and Users

These topics describe how to use URT to manage VLANs and users:

- Configuring VLANs for URT, page 5-1
- Managing VLAN Policies, page 5-5
- Managing Users in the Network, page 5-16

For a general overview of VLAN policies and how URT handles user logons and logoffs from VLANs, see:

- Understanding VLAN Policies, page 1-6
- Processing User Logons and User Logoffs, page 1-11

Configuring VLANs for URT

URT VLAN-based policies control user access to VLANs. When using URT you must:

- Enter all subnet/mask pairs for every VLAN you want URT to control.
- Designate one VLAN per VTP domain as the default or logon VLAN for the domain. This logon VLAN is accessible to nearly every user who tries to enter the network through a switch in this VTP domain.
- Make sure your logon VLAN is secure from intrusions.

To grant access to VLANs other than the logon VLAN, you must create VLAN policies for users, groups, or organizational units by assigning them to the appropriate VLANs.

Before a user can access a VLAN and its services, you must assign a VLAN policy to that user.

Although you do not add or delete VLANs using URT, added and deleted VLANs affect your URT VLAN policies.

The following tasks describe how to set up and maintain VLANs for use with URT:

Entering Subnets and Masks for Each VLAN

For each VTP domain, you must add the subnets and masks for each VLAN.

Step 1   From the VTP Domains folder, select the VTP domain.

Step 2   Select **Edit > Configure VLAN Subnets**.

Step 3   In the Subnet Configuration window, select a VLAN from the list.

Step 4   Click **Add**.

Step 5   In the VLAN Configuration window, enter the IP addresses for any missing subnet and masks, then click **OK**.

Step 6   Repeat steps 3 through 5 until all subnet/mask pairs are displayed in the Subnet Configuration window.

Note   • If there is an incorrect IP address or mask in the Subnet/Mask list, click **Edit**. Edit the subnet or mask as required.

   • If there is an extra pair (one that is not used on the VLAN) in the Subnet/Mask list, select that pair in the Subnet/Mask text box, then click **Remove**.

Setting a Default Logon VLAN

Every VTP domain has a default logon VLAN. When users log on, they are initially placed in that default logon VLAN. Users who are not associated with a specific VLAN remain in the default logon VLAN. If URT finds an association for a user, the user is placed in that VLAN.

The default logon VLAN provides unmapped users with network connectivity and ensures that they are authenticated before connecting to your network. When users log off, they are switched back to the logon VLAN.

To determine the logon VLAN for a VTP domain, select the VTP Domains folder in the left pane of the main window. Logon VLAN information for that domain is displayed in the right pane.

Step 1 In the VTP Domains folder, select the VTP domain.

This is the VTP domain for which you are setting the logon VLAN.

> **Note** Do not use the management VLAN (usually VLAN 1) as the URT logon VLAN. The management VLAN includes the IP addresses of the switches and is used to carry SNMP information.

Step 2 Select **Edit > Assign Logon VLAN**.

The VTP Domain Configuration dialog box is displayed.

Step 3 Select the appropriate settings, as described in Table 5-1.

Table 5-1   VTP Domain Configuration Dialog Box

Setting	Description
VTP Domain	Shows the selected VTP domain. The VLAN you select is used for this domain only.
Logon VLAN	Displays a list of VLANs from which you select the default logon VLAN.
	Select the default logon VLAN for the domain.
	Note Make sure you select a VLAN that has a subnet with enough IP addresses for all users in the VTP domain. Otherwise, users might have problems logging on and off the network.
Subnet/Mask	Displays the subnet and mask pairs used on the VLAN (for example, 10.10.10.0/255.255.255.240). Click the arrow to show the full list.
	Edit the information as described in step 4.

Step 4   Edit the subnet/mask information as follows:

- If a subnet is *not listed*, click **Add**. In the VLAN Configuration dialog box, enter the IP addresses for the missing subnet and mask, then click **OK**. Repeat this step until all pairs are listed.

- If a listed subnet is *incorrect*, select it in the Subnet/Mask text box, then click **Edit**. In the VLAN Configuration dialog box, edit the subnet or mask as required, then click **OK**.

- If a listed subnet is *not used* on the VLAN, select it in the Subnet/Mask text box, then click **Remove**. Click **Yes** in the Delete Subnet Confirmation dialog box.

Step 5   In the VTP Domain Configuration dialog box, click **OK**.

Managing VLAN Policies

These topics describes the tasks associated with mapping users and groups to VLANs.

- Associating or Reassigning a User, Group, or Organizational Unit to a VLAN, page 5-5
- Adding a VLAN to Your Network, page 5-8
- Deleting a VLAN from Your Network, page 5-8
- Deleting Users, Groups, or Organizational Units from a VLAN, page 5-9
- Mapping Hosts to VLANs, page 5-10
- Mapping Users or Hosts Using the Command-Line Interface, page 5-14

Associating or Reassigning a User, Group, or Organizational Unit to a VLAN

By associating or reassigning a user, group, or organizational unit to a VLAN, you ensure that users connect to the network in the correct VLAN—even if they log on through different systems or switch ports (for example, from a laptop).

Because the user always connects to the network in the same VLAN, you can create security policies based on VLANs and avoid MAC address-based VLAN mappings.

Tip   If a user has changed jobs within the company, you can move the user to the appropriate VLAN.

A user's VLAN association overrides any group or organizational unit VLAN association. If the user has no VLAN association and you create one for a group or organizational unit to which the user belongs, the user is associated with the group or organizational unit VLAN.

Note   URT does not override static VLAN assignments on switch ports.

VLAN associations differ slightly for Microsoft Networking and Novell NetWare:

- Microsoft Networking—If there is no user VLAN association and the user belongs to multiple groups, the VLAN association for the user's primary group takes precedence. If there is no primary group or no association for the primary group, URT randomly selects a VLAN association.

- Novell NetWare—If there is no user VLAN association, the VLAN association for the organizational unit that directly contains the user takes precedence. If there is no association for that organizational unit, URT moves up the Novell Directory Services (NDS) tree until it finds an organizational unit with a VLAN mapping.

Deciding How to Map Users, Groups, or Organizational Units to VLANS

You must decide how you want to map users, groups, and organizational units to VLANs. Although you can later change VLAN mappings, developing a plan now for user-to-VLAN mappings can simplify your network management tasks.

If a user is likely to connect to the network from different locations, consider creating a VLAN mapping for each VTP domain the user is likely to access. To simplify VLAN associations, you can associate groups or organizational units to VLANs instead of users.

You must add the NT domain or NDS directory in which the user resides *before* you can assign the user to a VLAN. For more information, see the "Adding NT Domains and NDS Directories to URT" section on page 4-3.

> **Note** You must have NT Administrator authority in the domain or NDS read and browse privileges in the directory. For more information, see the "Having Authority in Domains" section on page 4-2.

For Microsoft Networking, URT recognizes only Windows NT global groups, not Windows NT local groups. If an NT group is not displayed in URT, it might be defined as a local group.

You can map a user to one VLAN per VTP domain. If a user connects to the network in a VTP domain for which you have not provided a VLAN mapping, the user is logged onto the default logon VLAN for the local VTP domain. The user also remains in the default logon VLAN if the assigned VLAN is not defined on the switch.

Step 1   To open the Associate VLAN window, use *one* of these methods:

- In the NT and NDS Domains or Directories folder, double-click the user, group, or organizational unit name.

- In the list, select the user, group, or organizational unit name, then select **Edit > Associate**. You must make a selection from this list; you cannot drag and drop users or groups to the desired VLAN. You can select multiple users, groups, or organizational units by pressing the **Shift** key or the **Ctrl** key. All names you select must be associated with the same VLAN.

- In the list, select the user, group, or organizational unit name, then click **Associate VLAN with Users/Groups**.

> **Note**   If a user is assigned to a VLAN, the icon is displayed in blue. When you select a user, the VLAN assignments for that user are displayed in the right pane.

Step 2   In the Associate VLAN window, select the VTP domain and the VLAN to which you want to map the user, group, or organizational unit.

Step 3   Click **OK**.

If the user was already assigned to a different VLAN, the user is changed to the new VLAN the next time the switch polls the VPS.

Adding a VLAN to Your Network

After you add new VLANs to a VTP domain, you can associate users, groups, and organizational units with those VLANs in URT. If URT is already running, refresh the network information so that the new VLANs are displayed in the main window, using one of these methods:

- If you have previously imported data from CiscoWorks2000, select **View > Refresh from CiscoWorks2000**.

- Select the VTP domain to which you added VLANs, then select **View > Refresh**.

For information about the steps required to associate users and groups to the new VLANS, see the "Associating or Reassigning a User, Group, or Organizational Unit to a VLAN" section on page 5-5.

Deleting a VLAN from Your Network

Before deleting a VLAN from your network, you should reassociate users in URT. If you do not reassociate users but delete their VLAN, they stay in their logon VLAN and an error message is displayed on the VPS.

You must have NT Administrator authority in the domain or NDS read and browse privileges in the directory. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1   In the VTP domains folder, select the VLAN to delete.

Step 2   In the NT and NDS Domains folder, select each user, group, or organizational unit.

> **Note**   Users, groups, or organizational units associated with a nonexistent VLAN are displayed with a blue X in their icon.

Step 3   To associate the selected user, group, or organizational unit with a different VLAN, click **Associate** or select **Edit > Associate**.

Step 4   Verify that the VLAN is not used as a logon VLAN by selecting the VTP domains folder and looking at the Logon VLAN list in the right pane. If the VLAN is listed there, edit the logon VLAN by selecting **Edit > Assign Logon VLAN**.

Step 5   When no associations for the VLAN remain in URT, delete the VLAN from the network.

Step 6   Click **Refresh** in the URT main window or select **View > Refresh** to update the window.

When you select the VTP domain, the deleted VLAN is no longer displayed.

Deleting Users, Groups, or Organizational Units from a VLAN

If you no longer want a user, group, or organizational unit to be associated with a particular VLAN, you can delete the VLAN association.

Note   If you delete the association without reassigning the user, group, or organizational unit to another VLAN, they use the default logon VLAN.

You must have NT Administrator authority in the domain or NDS read and browse privileges in the directory. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1   In the NT and NDS Domains or Directories folder, select the user, group, or organizational unit.

Note   Users, groups, or organizational units not assigned to a VLAN are displayed with gray icons.

Step 2   Select **Edit > Delete Association**.

Step 3   Click **Yes** in the confirmation dialog box.

The user, group, or organizational unit is not deleted from the NT and NDS Domains folder—only the VLAN association is deleted.

Mapping Hosts to VLANs

You can use URT to create host-based dynamic VLAN policies. These topics describe the tasks for implementing host-based VLAN policies:

Adding MAC Addresses and Host Mappings

The list of MAC addresses in the URT main window displays only MAC addresses that have VLAN mappings.

Step 1   Select the MAC Addresses folder.

Step 2   Click **Add** or select **Edit > Add**.

The Host Association dialog box is displayed (Figure 5-1). URT displays all unmapped MAC addresses in the Discovered MACs list. If a MAC address is already mapped to a VLAN, it is not displayed in the list (mapped MAC addresses are displayed only in the main window).

Figure 5-1   Adding MAC Address Mappings
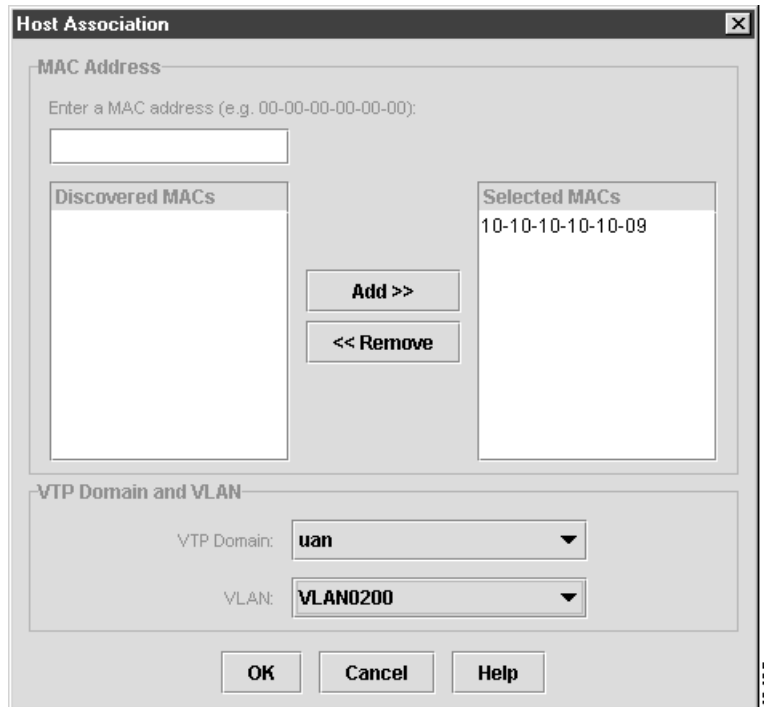
Step 3   Enter or select the MAC addresses to map.

✎

Note   You can select multiple MAC addresses by pressing the **Shift** key or the **Ctrl** key. All addresses you select must be associated with the same VLAN.

You can map more than one address at a time to the same VLAN.

a. To quickly find out if a specific MAC address is in the discovered MAC list, enter the MAC address in the Enter a MAC Address text box. As you enter text, URT scrolls through the list of discovered MACs to the next address that matches your entry. If URT discovers the MAC address, it is highlighted.

✎
Note   Use hyphens—not colons—to separate the bytes in the MAC address.

b. If a desired address is not in the discovered MACs list, enter the full MAC address in the Enter a MAC Address text box, then click **Add>>** to add it to the list.

c. From the list of discovered addresses, select the MAC addresses to map to a specific VLAN, then click **Add** to add them to the selected MACs list.

Step 4   When you have selected all MAC addresses you want to map to the same VLAN, select the VTP domain and the desired VLAN.

Step 5   Click **OK**.

Tips

- You can create different VLAN mappings for each of your VTP domains for each MAC address.

- When you select a MAC address in the main window, the VLAN mapping for each VTP domain for which there is a mapping is displayed in the right pane.

- When you select a VLAN folder in the main window, URT does not display MAC addresses mapped to the VLAN.

Retaining MAC-to-VLAN Associations

By default, URT ignores MAC-to-VLAN associations if the user logging on is assigned to a different VLAN in URT. You can require URT to use the MAC-to-VLAN association.

Step 1   Select **View > Options**.

Step 2   In the URT Options window, click the Logon tab.

Step 3   Click the **Retain MAC to VLAN Associations** checkbox.

Step 4   Click **OK**.

Editing Host Mappings

You can edit the VLAN mappings for any host that has a mapping.

Step 1   To open the Associate VLAN window, use one of these methods:

- In the MAC Addresses folder, double-click the MAC address to edit.
- Select the address, then click **Associate VLAN with Users/Groups**.
- Select the address, then select **Edit > Associate VLAN**.

Step 2   In the Associate VLAN window, select the desired VTP domain and VLAN.

Step 3   Click **OK**.

Deleting MAC Addresses and Host Mappings

If you no longer want to use host-based VLAN policies with a host, you can delete those host mappings from URT.

Step 1   In the MAC Addresses folder, select the MAC address to delete.

Step 2   Click **Delete** or select **Edit > Delete**.

URT deletes the MAC address and its VLAN mappings.

Mapping Users or Hosts Using the Command-Line Interface

You can add user-to-VLAN or host-to-VLAN mappings using the command-line interface (CLI). Doing this is useful if you use an automated method of creating a text file with your mappings. You can create batch mappings by piping your text file into the **urt** command.

Note   Make sure you define the NT domain or NDS tree using the URT main window *before* entering mappings for them on the command line. You cannot add domains or trees using the CLI.

The urt.bat file that launches the URT Administrative GUI (main window) resides in the bin subdirectory of the URT root directory.

urt Command Syntax

The syntax of the urt command is:

```
urt -cli < [textfile]
```

Tip   For online help, enter `urt -help`.

Table 5-2 describes the command syntax in more detail.

Table 5-2   urt Command Syntax

Command	Function
`urt -cli`	Indicates that you are running URT from the command line rather than the GUI.

`< textfile`	(Optional.) The name of a text file that contains the user-to-VLAN and host-to-VLAN mappings. If you do not specify a file, you must enter the mappings at the command prompt after you start the command. Any mappings you enter override existing mappings in the URT database.
	
	In either case, you must enter the mappings in one of these formats:
	
	• For host-to-VLAN mappings:
	
	   MAC-address, VTP-domain, VLAN
	
	   For example:
	
	   `00-5f-62-00-00-b1,VTP1,VLAN5`
	
	• For NT-user-to-VLAN mappings:
	
	   NT-domain\username, VTP-domain, VLAN
	
	   For example:
	
	   `ENG_DOMAIN\user1,VTP2,VLAN12`
	
	• For NDS-user-to-VLAN mappings:
	
	   NDS-tree\username, VTP-domain, VLAN
	
	   For example:
	
	   `CORP_TREE\USA\CALIF\user1,VTP2,VLAN12`

Managing Users in the Network

These topics describe the broader tasks of managing users within your network. Some of these tasks require using software other than URT and will help you to understand how URT fits into your typical user management procedures.

Adding Users to the Network

If a user requires a Microsoft Networking or Novell NetWare user account, follow this general procedure for adding the user to the network.

Step 1   Add the user to the appropriate NT domain server or NDS directory.

Note   For more information about adding users, see the Microsoft or Novell documentation.

Step 2   From the URT main window, select the folder for the domain or directory.

Step 3   Select **View > Refresh**.

The newly added user is displayed in the folder for the domain or directory.

Step 4   If you already assigned the user to an existing group or organizational unit with a VLAN association, you do not need to create a VLAN association. Otherwise, assign the user to a VLAN.

Deleting Users from the Network

When you delete users from the network, you should delete all of their accounts. When you delete users' NT and NDS user accounts, you also delete their VLAN associations.

When you restart URT or refresh the NT domain or NDS directory user list, users no longer defined are displayed with gray icons with a red X.

Note   Deleting a user from the network does not delete the URT Client Module from the user's system. See the "Removing the URT Client Module from the Network" section on page 8-3.

Moving Users to Another Domain

URT does not maintain a user's VLAN associations if you move the user account from one NT domain or NDS directory to another.

Step 1 In the URT main window, select the username in the old NT domain or NDS directory.

> ✎
>
> **Note**   The VLAN Associations list in the right pane shows the old VLAN associations for the user. To keep the same associations, write them down.

Step 2 Move the user account on the NT domain servers or NDS directories.

> ✎
>
> **Note**   For information about moving user accounts, see the Microsoft or Novell documentation.

Step 3 In URT, select the username in the new NT domain or NDS directory.

Step 4 Associate the user with the desired VLANs. For more information about the procedure, see the "Associating or Reassigning a User, Group, or Organizational Unit to a VLAN" section on page 5-5.

Viewing User VLAN Information

To view a user's current VLAN information, select a domain or directory in the URT main window. The right pane shows the logged on users list as described in Table 5-3. You can use this information to troubleshoot or evaluate mappings.

If you select a user, group, or organizational unit, the VTP domain and VLAN to which the user is mapped are displayed in the right pane.

> ✎
>
> **Note**   You cannot print a list of logged on users, VLAN associations, or other URT settings.

A mismatch between a VLAN association and the VLAN to which a user is actually attached might occur if:

- The switch to which the user is attached is not in the VTP domain you mapped. The user is placed in the default VLAN for the VTP domain.

- The switch port is defined as static, not dynamic. The user is placed in the VLAN defined on the switch port instead of in the mapped VLAN.

- The user belongs to more than one group and the VLAN associations are for the groups, not the user. The user is placed in the primary group VLAN. If no primary group is assigned, the user is randomly placed in an associated VLAN.

Monitoring Users

You can monitor the users connected to your network. For each user, you can see which network components are in use—for example, the switch, its port, and the VLAN to which the user is connected. You can also see the date and time the user was last seen on the network.

To keep track of user logons and logoffs over time, you can enable history logging. To minimize the amount of disk space devoted to history files, you can establish how many files to retain.

With history logging enabled, you can view history from the URT main window.

These topics describe how to monitor users with URT:

- Determining Which Users are Logged Onto the Network, page 5-20
- Enabling the URT History Log, page 5-21
- Viewing URT History Files, page 5-22

Determining Which Users are Logged Onto the Network

URT keeps track of which users are logged onto the network. When you select an NT or RADIUS domain or NDS or LDAP directory, the users connected in that domain or directory are displayed in the right pane.

Table 5-3 describes the information shown for logged on users.

Table 5-3   Logged On Users List

Column	Description
Username	Domain or directory username. Names are shown in one of these formats: • *NT_DOMAIN\username* • *NDS_Directory\username.context* **Note** This column is not displayed when you view this list by selecting a username.
IP Address	System IP address.
Subnet	Subnet on which the system is connected.
Gateway	IP address of the router (gateway) used by the system.
VTP Domain	VTP domain to which the system is connected.
VLAN	VLAN to which the system is connected.
Switch	IP address of the switch to which the system is connected.
MAC Address	MAC address of the network interface card (NIC) in the system.
Port	Port on the switch to which the system is connected.
Last Seen	Date and time the user was last seen on the network, in the format *mm/dd HH*:*MM*:*SS* (month/day hour:minutes:seconds).

Enabling the URT History Log

You can view historical information about user logons and logoffs and MAC addresses in centralized files maintained by URT. URT history files contain the following data:

- Username

- Client MAC address

- Client IP address

- Subnet address

- Gateway address

- VTP domain of the client

- VLAN assigned to the user

- IP address of the switch to which the client was connected

- Switch port to which the client was connected

- URT VPS IP address

- Time of event (reflects the VPS time zone setting. For more information about setting the time zone, see the "Viewing and Configuring VPS Characteristics" section on page 3-3.)

- Type of event (user logon or logoff)

✎ **Note** When viewing user events, most of this data is displayed. When viewing MAC events, only a subset of this data is displayed.

Step 1 Select **View> Options**.

Step 2 Click the History tab.

Step 3 The Enable history logging checkbox is selected by default.

- To disable history logging, deselect the checkbox, then click **OK**.

- If you are not disabling history logging, continue to step 4.

Step 4 Select the location in which to store the history files.

Step 5   You can manage history files by size or date. By default, the Date radio button is
selected:

- To create a new file daily, select **Date**, then set the number of days of history
  to save.

> ✎
>
> **Note**   If you do not enter the number of days, a default value of 999 days is
> used.

- To create a new file when the current file reaches a size limit, select **Size**. Set
  the values for the maximum log file size and maximum number of log files.

> ✎
>
> **Note**   If you do not enter any values, URT uses the default values (10 MB
> for the maximum log file size, and 999 for the maximum number of
> log files).

Step 6   Click **OK**.

Viewing URT History Files

In the URT history files, you can view details about user logon and logoff and
events for new MAC addresses displayed on a switch port.

You can also rearrange column headings, sort the history by column, and delete
rows of history.

You must have history logging enabled. Refer to the "Enabling the URT History
Log" section on page 5-21 for more information.

Step 1   Select **View > History**.

> 🔍
>
> **Tip**   Click **Refresh** to update the history log with recent information.

The View History Files dialog box is displayed.

Step 2   Click the radio button for User events or MAC events.

Step 3   Select the files you want to view or click **Select All** to view all files in that directory.

Step 4   Click **OK**.

The History Log displays and the rows are color-coded:

- Yellow rows display logon events.
- Blue rows display logoff events.

Step 5   To find a specific history record:

a.   Click **Find next row** or select **Edit > Find**.

The Find dialog box is displayed.

b.   On the Simple tab, enter the string you want to find.

- To match case, click the Match case checkbox.

- To search a specific column or group of columns, click the Advanced tab. By default, checkboxes for all columns are selected. If there are many history records, clear all checkboxes, but leave those for the columns that you want to search (for example, you might leave only the username checkbox selected).

> ✎
> **Note**   Do not select more than 20 MB of history data to display at any one time. When you view all history files, sorting or scrolling can be slowed.

c.   Click **Find Next** in the Find dialog box.

The history log scrolls to the next matching record, if found.

Step 6   You can edit the history log using one of these methods:

- To reorder the columns, click a column heading, then drag it to the desired location in the heading.
- To sort the information by the contents of a particular column, click the column heading.
- To delete selected history records, select the records, then click **Delete one or more rows** or select **Edit > Delete Rows**.

Managing Unmapped Users or Groups

Users or groups not mapped to VLANs are displayed with gray icons in the left pane. To find these users or groups, open the directory or domain folder and look for gray icons.

Users not mapped to a particular VLAN are assigned a VLAN as follows:

- Users connected to a static switch port remain in the VLAN defined for the port.

- Users connected to a dynamic switch port are placed in their group or organizational unit VLAN, if applicable. If not applicable, they are placed in the logon VLAN for their VTP domain.

Managing User Logons Over a Serial Connection

URT can switch users into VLANs only if their workstations are directly connected to a supported switch. Because users connecting over serial lines are not connected to switches of the appropriate type, URT does not handle or otherwise affect these users. Their network connections remain unchanged after you deploy URT in your network.

Managing User Logons from Remote Locations

You can map a user to one VLAN for each VTP domain. If you have separate VTP domains in each remote location, you can create an appropriate association for your mobile users for each location they visit.

If you do not assign a mobile user specific associations for each VTP domain, the user might be switched to a VLAN as follows:

- If the user connects to the network through a VTP domain where no specific association exists, the user is placed in the logon VLAN.

- If the user connects to the network through a VTP domain where the user is a member of a Microsoft Networking group or organizational unit, the user is placed in the VLAN defined for the group or unit.

If the logon VLAN you create for the VTP domain is sufficient for your mobile users, you do not need to create associations for each VTP domain.

Managing Users Connected to Static Switch Ports

If a workstation is directly connected to a static switch port—that is, a port assigned to a specific VLAN—the user remains in the VLAN defined on the switch, even if you map the user to another VLAN in URT.

URT does not override static VLAN assignments on switch ports.

Setting Up and Using the URT Web Client Interface

Web-based clients use the URT Web Client Interface to authenticate and assign VLANs to web users. Any configured LDAP or RADIUS domain can authenticate web clients.

For more information about adding LDAP directories and RADIUS servers, see Chapter 4, "Setting Up Domains, Directories, and Servers."

These topics describe administrative and client tasks for using the Web Client Interface:

- Configuring DNS Servers in the DHCP Manager, page 6-2
- Setting Web Logon Options, page 6-2
- Enabling Root on MacOS Clients, page 6-4
- Setting Up Linux Web Clients, page 6-6
- Logging On as a Web Client, page 6-7
- Logging Off as a Web Client, page 6-8

Configuring DNS Servers in the DHCP Manager

In the DNS field of the DHCP server Logon Vlan scope, add the IP addresses of your VPSs. Doing this allows the web client to be redirected to the VPS for the URT web logon page. If one VPS is down, the secondary VPS is accessed to display the web logon page.

Before logon, any URL the web user enters into the browser is automatically redirected to the URT web logon page. After logon, the user can browse to any permitted URL without editing any browser settings.

The DNS server that runs on the VPS replies to all queries from the current system IP address before logon.

Note You must modify the DHCP setting for the logon VLAN to use the VPS as the DNS setting. When a user logs on from the web, the web address is queried in DNS. The response to the query is the IP address of the current VPS system; the URT web logon page is displayed.

Setting Web Logon Options

The following topics describe the administrative tasks you must perform for web logons:

- Customizing the Web Logon Page, page 6-2
- Setting Web Associations, page 6-3
- Viewing Web Trace (Linux and MacOS Systems Only), page 6-4

Customizing the Web Logon Page

The VPS generates a web page for web clients to enter their user ID, password, and domain name for authentication. The web logon page is the page users see when they first start their browsers.

You can add customized advertisement or announcement text to this page. When you edit the customized text, the page is regenerated. You make these changes on the Administrative Server and they are pushed to the VPS.

The web logon page is also regenerated when you add or remove an LDAP domain or RADIUS server.

Step 1   Select **Options > URT Options**.

Step 2   Click the Web tab.

Step 3   Enter the HTML code for the text you want to display on the logon page.

Step 4   Enter the title you want to be displayed on the page.

> **Note**   No HTML tags are necessary for the title.

Step 5   (Recommended.) If you want the web browser to close, select the Close web browser window after launching URT Web Client option (default).

Step 6   Select the language for the logon page.

> **Note**   English is the only supported language at this time.

Step 7   Click **OK**.

The HTML code is immediately pushed out to all URT VPSs. The logon page is regenerated and all subsequent clients logging on will see the updated page.

Setting Web Associations

In addition to VLAN associations, you can set web associations for an LDAP server.

Step 1   In the Directories folder, click a group or user.

Step 2   Click the Web Associations tab in the right pane.

Step 3   Double-click on the user or group again (in the left pane).

The Web Associations dialog box is displayed.

Step 4   Select these checkboxes as appropriate:

- Allow multiple users on a port—URT allows multiple users (multiple MAC addresses) for the logged on user. Multiple web users connected to a hub can be served by a single switch port. This option is based on the user or group ID you select. All users behind the hub are assigned to the same VLAN.

- Log on user and remove logoff window—If you select this option, web users do not have a logoff window. They remain logged on until they either power off or disconnect their systems.

Step 5   Click **OK**.

Viewing Web Trace (Linux and MacOS Systems Only)

Logging is enabled by default, and the logged information is written to the UrtWebClient.log trace file in the user's %TEMP% directory.

To view the information logged to the trace file, press **F10**. The information in the log shows several different events.

Step 1   Open a DOS command window.

Step 2   Enter `cd %TEMP%`

The full path to the log file is displayed.

Enabling Root on MacOS Clients

To use URT, all Macintosh Operating System (MacOS) clients must enable root and must log onto the system as root. Doing so allows MacOS users to release and renew their IP addresses as required by URT.

In situations where root is enabled and you try to log on as root, but the initial MacOS logon screen does not list root as a user, you must switch to the logon screen where you can enter the username, then enter the username root.

> **Note** The default administrator on MacOS systems is called *System Administrator*.

Each MacOS user must create the root user only once, using one of the methods described in the following topics:

- Enabling Root Using Menus, page 6-5
- Enabling Root Using a Terminal Window, page 6-5

Enabling Root Using Menus

Step 1   Select **Applications > Utilities > Net Info Manager**.

Step 2   Select **Domain > Security > Authenticate**.

Step 3   If prompted, enter the admin password.

Step 4   Select **Domain > Security > Enable Root User**.

Step 5   Enter a new root user password.

Step 6   Confirm the new password.

Enabling Root Using a Terminal Window

Step 1   Open a terminal window and type the following at the prompt:

```
sudo passwd root
```

Step 2   Enter the admin password.

Step 3   When prompted for a root login password, enter the new password.

Step 4   Enter `su`.

Step 5   Enter your root password to log on as root.

Setting Up Linux Web Clients

URT supports Linux users who use the DHCP pump, dhcpcd, or dhclient clients. On Linux systems with multiple users, you can provide all users with the required privileges to release and renew their IP addresses.

There are two methods for assigning the necessary privileges to users:

- Allowing Users to Control the Interface, page 6-6
- Allowing Users to Control the dhcp Client, page 6-7

Allowing Users to Control the Interface

Step 1   Create a group for the users (for example, netctl).

Step 2   To add all users to the new group, use a text editor to edit the /etc/group file.

Step 3   Enter `chgrp` *groupname* for the ifup, ifdown, pump, and *usergroupname* programs.

Step 4   Edit the /etc/sysconfig/network-scripts/ifcfg-IFACE file.

Step 5   In the line that contains your new group, change no to yes.

⚠
Caution   This method provides users with higher privileges than they would normally have.

Allowing Users to Control the dhcp Client

You can allow users to control the dhcp client. To do so, enter the following command:

```
Chmod u+s /sbin/pump
```

> ⚠️
>
> **Caution**   This method provides users with higher privileges than they would normally have.

Logging On as a Web Client

To use the web client, the user must log onto the local system as an Administrator or root user.

The VPS generates a web page for web logon clients. Web clients see this page when they first start their browsers. The web logon page contains user ID, password, and domain name fields.

Before logon, any URL the web user types into the browser is automatically redirected to the URT web logon page. After logon, the user can browse to any allowed URL without changing any browser settings.

> ✎
>
> **Note**   In an environment with several web users, you should consider setting up a dedicated VPS for authenticating web logons. For more information, see the "Updating VPSs with New Group or Organizational Unit Lists" section on page 3-10.

Logging on Using Netscape Navigator

The first time URT web users open Netscape Navigator on MacOS and Linux systems using Netscape Navigator, they might be requested to install the Java plug-in. In this case, instructions are provided during the logon sequence to install the plug-in. This step is required only once; subsequent logons do not require it.

Client Logon Procedure

Users can enter their logon information in the URT web logon page.

URT authenticates the user, then gathers MAC address DHCP data from the client system to send to the VPS. If necessary, URT releases and renews the web user's IP address.

Note All web users must have root privileges to release and renew their current IP address so that URT can perform this step, if necessary. For information about setting up MacOS clients, see the "Enabling Root on MacOS Clients" section on page 6-4. For information about how URT processes user logons and logoffs, see the "Processing User Logons and User Logoffs" section on page 1-11.

Step 1 In the User Name field, enter your username.

Step 2 In the Password field, enter your password.

Step 3 In the Domains list, select your domain.

Every LDAP and RADIUS domain added to URT is displayed.

Step 4 Click **Logon**.

The URT logoff page shows your connection time. However, if you selected the Log on user and remove logoff window option, the connection time is not displayed.

Logging Off as a Web Client

The web associations determine how a client logs off. If you select the Log on user and remove logoff window option, no logoff window is displayed. Clients remain connected until they power off or disconnect their systems from the network.

If this web association is not selected, a logoff window remains open for the user to log off at any time.

- If the user clicks **Log Off**, a confirmation message is displayed.

- If the user closes the logoff window by clicking the **X** in the upper right corner instead, URT tries to log off the client.

- If the port link goes down or the user disconnects or powers off the system, URT logs off the user.

URT uses a *synchronizing thread* to send synchronized packets every five minutes for the logged on client, to ensure that the user is still logged on. When the synchronized packets are no longer received by the VPS, the client is moved back to the logon VLAN. This happens when the client system logs off in an abnormal state, such as when the browser freezes.

Note   If users disconnect their systems by unplugging a cable, logoff takes about 10 minutes (the time it takes for two synchronizing messages to be generated).

Logging Off as a Web Client

Managing the Traditional Client Module

The URT Client Module is usually installed automatically and requires little manual intervention. However, you should make sure it is installed properly on client systems and that it starts correctly during logon.

These topics describe how to manage the Client Module for traditional logons:

- Installing the URT Client Module, page 7-2
- Starting, Stopping, or Disabling the Client Module on Windows Systems, page 7-7

Installing the URT Client Module

The URT Client Module is usually installed automatically.

- Installation is *automatic* in Windows NT, Windows 2000, and Windows XP (Professional) clients in a *Microsoft Networking* environment (not Novell NetWare). Automatic installation is enabled by default in the domain option Enable auto install and upgrade for Windows NT/2000. To change this option, see the "Setting Domain Logon Options" section on page 4-4.

- Installation is *not automatic* for:

  - Any client, including Windows clients, *in a Novell NetWare network*. For Novell NetWare, you must install the Client Module manually.

  - Windows NT, Windows 2000, and Windows XP (Professional) clients in a *Microsoft Networking* environment if automatic installation is disabled in the domain option Enable auto install and upgrade for Windows NT/2000. To change this option, see the "Setting Domain Logon Options" section on page 4-4.

Automatic Installation of the Client Module

When automatic installation is enabled, the Client Module is installed after you install the URT logon script on the domain server.

If automatic installation is enabled in a Microsoft Networking environment, and a Windows NT or Windows 2000 system logs onto the network, the following events occur:

1. The logon script tries to run a utility on the system to verify whether the latest version of the Client Module is installed.

2. If the logon script does not find this utility on the system, the script copies the utility to the system and runs it.

3. If the Client Module is not installed, or the installed Client Module is not the latest version, the utility:

    a. Obtains the latest version of the executable files from the domain server.

    b. Tries to install or upgrade to the latest version of the Client Module.

4. If the attempt to install or upgrade fails:

    a. The utility sends a packet to the VPS to request installation of the Client Module on the system.

    b. The VPS notifies the URT Administrative Server to install the Client Module on the specified system.

After installation, the client runs normally.

Installing the Client Module Manually on Windows Systems

Manual installation of the Client Module is different for Microsoft Networking and Novell NetWare clients, as described in these topics:

- Installing the Client Module on Microsoft Networking Clients, page 7-3
- Installing the Client Module on Novell NetWare Clients, page 7-5

Note If a workstation runs both Microsoft Networking *and* NetWare, you must follow the instructions in *both* topics.

Installing the Client Module on Microsoft Networking Clients

Follow the instructions in this section to manually install the URT Client Module on a Windows NT, Windows 2000, or Windows XP (Professional) workstation running Microsoft Networking.

Note You must install the Client Module in every NT domain in your network.

- Select a time of day when most of the Windows systems are up and running on the network (even if users are not logged on). You can install the Client Module only on systems running and connected to the network.

- You must have NT Administrator authority in the domain. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1 In the URT main window, select NT Computers in the folder for an NT domain.

Alternately, if you are installing the Client Module on all Windows NT or Windows 2000 systems in a domain, you can select the domain. You can also select multiple systems by pressing the **Shift** key or the **Ctrl** key.

> ✎
>
> **Note** You can install the Client Module only on systems that use DHCP. If a selected system does not use DHCP, the Client Module installation fails.

Step 2 A list of Windows NT and Windows 2000 clients is shown in the right pane. The client attributes are described in Table 7-1.

Table 7-1   NT Hosts—Right Pane Information

Attribute	Description
Name	Client name.

Service Status	Status of Client Module on the system:
	
	• Installed—The service is installed.
	
	• Installed Running—The service is installed and active.
	
	• Query Pending—URT is waiting for a reply from the client.
	
	• Service Query Error—URT could not determine the status of the service. This might indicate that:
	
	  – The system is not running.
	
	  – The IP address for the system has changed since the last time WINS was updated. After 5 to 10 minutes, this problem should resolve itself.
	
	• Not Installed—The service is not installed on the client.
	
	• Host Unreachable—URT did not receive a reply from the client.

Version	Client Module version number (if installed).

Step 3 To install the Client Module on all listed NT hosts, do not select any systems in the list. Otherwise, select the system on which you want to install the Client Module.

Step 4 Click **Install Client Module** or select **Customize > Install Client Module**.

URT installs the Client Module on the selected clients, and displays a message window so that you can monitor installation status.

Installing the Client Module on Novell NetWare Clients

Use the instructions in this section to manually install the Client Module on a Windows NT or Windows 2000 workstation running Novell NetWare.

- You must have Administrator or Administrator-equivalent authority to install the Client Module on systems defined in the Novell Directory Services (NDS) directory tree.

- You must also have installed the ZENworks Starter Pack and created the WINNT User Package and WINNT Workstation Package *policy objects*. These policy objects must be associated with the organizational object that contains the users and groups on whose workstations you will install the Client Module.

✎
Note   For more information, see the Novell documentation.

Step 1 To run ZENworks Novell Application Launcher (NAL), enter `nal` at a command prompt on a NetWare client.

Step 2 Double-click the NWAdmin32 application.

The NDS directory tree is displayed in the NWAdmin32 application.

If no NWAdmin32 icon displays, you must log onto NDS as administrator again.

Step 3 In the NDS directory tree, double-click the WINNT Workstation Package.

Step 4   Click **Add Action**.

The Create Scheduled Action window is displayed.

Step 5   Enter a meaningful name for the action (for example, Install URT).

Step 6   Click **Create**.

NAL creates the action and displays the Scheduled Action window.

Step 7   Select the newly created action.

Step 8   Click **Details**.

Step 9   Select Ignore package default schedule and use the following settings:

    a. In Scheduled Action, click **Details**.

    The Action Properties window is displayed.

    b. Click the General tab.

    c. Select these characteristics (allowing the others to default):

    Priority—Normal
    Impersonation—System

    d. Click the Items tab.

    e. Click **Add**.

    The Item Properties window is displayed.

    f. Enter the filename of the Client Module installation program in this format:

    `\\`*Novellserver*`\sys\public\urt\UrtClientInstall.bat`

    where *Novellserver* is the name of the server where you install the URT logon script. When the logon script is installed, URT installs the Client Module installation and uninstallation program on the server.

    g. Click the Schedule tab.

    h. Select User Logon for Event.

    i. Click the Advanced tab.

    j. Select the Disable action after completion checkbox.

The Client Module is installed the first time the user logs onto the NetWare domain.

Tips

- While you are creating the Install URT object, you might want to create an Uninstall URT object. This object would have the same properties described in the preceding procedure, but the filename is:

  Novellserver\sys\public\urt\UrtClientUninstall.bat.

- Unless you are uninstalling the client, deselect the Uninstall URT item in the Scheduled Action window. If you uninstall the client, deselect the Install URT object.

> **Note**   For more information about uninstalling software from NetWare clients, see the Novell ZENworks documentation.

Starting, Stopping, or Disabling the Client Module on Windows Systems

The Client Module starts and stops automatically and should require no manual intervention. However, you can manually stop the service on Windows NT, Windows 2000, or Windows XP (Professional) systems to help with problem diagnosis, or disable it so that it does not restart when you restart the system.

> **Note**   You cannot manually start or stop the Client Module on Windows 98 or Windows XP systems.

Step 1   On the Windows NT or Windows 2000 client, open the Services control panel by selecting **Start > Settings > Control Panel**, then double-clicking **Services**.

Step 2   Find URT Administrative Service in the list of services.

> **Note**   For Windows NT and Windows 2000, the Client Module is displayed as urtclsvc.exe on the Windows Task Manager Processes tab.
>
> For Windows 98 and Windows XP, the Client Module is displayed as urt95svc.exe.

Step 3   Status should usually be Started, and Startup should be Automatic.

- To stop the service, select it, then click **Stop**.

- To start the service, select it, then click **Start**.

- To change how the service is started, select it, then click **Startup**. In the next dialog box, select how you want to start the service (automatically or manually), or disable the service.

Tips

- For Windows NT and Windows 2000, the Client Module is displayed as urtclsvc.exe on the Windows Task Manager Processes tab.

- For Windows 98 and Windows XP, the Client Module is displayed as urt95svc.exe.

Removing URT

The following topics describe how to remove URT from your network:

- Redirecting Switches to Use a Switch-Based VMPS Before Removing URT, page 8-1
- Removing the URT Client Module from the Network, page 8-3
- Removing URT from Its Role in Handling User Logons, page 8-7
- Removing URT VPSs, page 8-8
- Removing the URT Administrative Server, page 8-8

Redirecting Switches to Use a Switch-Based VMPS Before Removing URT

Because the URT VPS is used by your network switches in place of a VMPS, you must change your switch VMPS configurations before removing URT.

⚠️

Caution   If you do not perform this step first, users cannot successfully connect to your network.

You can update the VMPS configuration on the switches using the switch command-line interface or the URT main window. The following procedure assumes you are using URT.

Select those switches in your network that you want to use as VMPSs and configure them accordingly.

For information about configuring VMPSs, see the applicable switch documentation.

After switches are set up as VMPSs, you can configure other switches to use them in place of the URT VPSs.

Step 1   Select a VTP domain, then open the Switches folder for that domain.

Step 2   Select the switches to reconfigure.

> ✎
>
> **Note**   You can select multiple switches by pressing the **Shift** key or the **Ctrl** key. All switches you select are assigned the same VMPSs. If you select more than one switch, all selected switches are configured to use the same primary and secondary VMPSs.

Step 3   Click **Configure Device** or select **Customize > Configure**.

The Device Configuration dialog box is displayed.

Step 4   Replace the IP address for each URT VPS (VPS 1 through VPS 3) with the IP address for the first, second, and third VMPSs. Specify whether the switch should use the VMPS as a primary or secondary server.

The switch uses the primary VMPS unless it is unavailable; then, the switch uses the secondary servers in the order you specify.

Step 5   Click **OK**.

Removing the URT Client Module from the Network

You must remove the URT Client Module from all systems before you remove the URT Administrative Server.

Note   Leaving the Client Module installed on the workstations should not affect the way they function, but will unnecessarily consume a small amount of system resources.

For some clients, the uninstall process differs depending on the operating system and type of networking (Microsoft Networking or Novell NetWare) used on the workstation. These topics describe the different uninstall procedures:

- Removing the Client Module from Windows 98 and Windows XP Systems, page 8-3
- Removing the Client Module from Windows NT and Windows 2000 Systems (Using Microsoft Networking), page 8-4
- Removing the Client Module from Novell NetWare Systems, page 8-5

Removing the Client Module from Windows 98 and Windows XP Systems

You can remove the Client Module from Windows 98 and Windows XP systems using the same procedure on both NetWare and Microsoft networks.

Note   You cannot use the Add/Remove Programs control panel to uninstall the Client Module.

You must have NT Administrator authority in the domain. For more information, see the "Having Authority in Domains" section on page 4-2.

Windows 98 and Windows XP systems automatically install the Client Module at network logon. Therefore, you cannot permanently remove the Client Module from a specific client unless the client remains standalone.

Step 1   On the primary domain server, edit the urt.bat file in the NETLOGON folder.

Step 2   Add the -remove parameter to the onoffhandler command.

The command located is near the end of the urt.bat file, preceded by the label :urt_command. The following is an example of the onoffhandler command at the end of the urt.bat file:

```
:urt_common
%WINDIR%\onoffhandler -domain URT2000DOMAIN1 -addr 10.10.22.10.15001; -trace -remove
:urt_exit
```

Step 3   Restart the user's system.

Step 4   Log onto the network.

Step 5   Use the onoffhandler command to uninstall the Client Module from the clients.

Step 6   If you are removing the Client Module from a single Windows 98 or Windows XP system, you must modify the user profile to remove urt.bat.

Removing the Client Module from Windows NT and Windows 2000 Systems (Using Microsoft Networking)

Use the URT main window to remove the Client Module from Windows NT and Windows 2000 clients using Microsoft Networking.

Note   You cannot use the Add/Remove Programs control panel to uninstall the URT Client Module.

You must have NT Administrator authority in the domain. For more information, see the "Having Authority in Domains" section on page 4-2.

Step 1   In the URT main window, select the NT Hosts item in the domain folder.

Step 2   To uninstall the Client Module on all listed systems, do not select any systems in the list. Otherwise, select the system from which you want to uninstall the Client Module.

Step 3   Select **Customize > Uninstall Client Module**.

URT uninstalls the service on the selected clients, and displays a message box so you can monitor the status of the uninstallation.

Removing the Client Module from Novell NetWare Systems

You use the Novell Application Launcher (NAL) program to remove the Client Module from Windows NT or Windows 2000 clients using Novell NetWare. You cannot use the Add/Remove Programs control panel to uninstall the URT Client Module. To prevent clients from subsequently reinstalling the Client Module, you can delete or disable the Install URT item.

For more information about uninstalling software from NetWare clients, see the Novell ZENworks documentation.

For NetWare, you must have Administrator or Administrator-equivalent authority to uninstall the Client Module on systems defined in the Novell Directory Services (NDS) directory tree.

Step 1   To run ZENworks Novell Application Launcher (NAL), enter `nal` at a command prompt on a NetWare client.

Step 2   Double-click the NWAdmin32 application.

The NDS directory tree is displayed in the NWAdmin32 application.

Step 3   In the NDS directory tree, double-click the WINNT Workstation Package.

Step 4   Click **Add Action**.

The Create Scheduled Action window is displayed.

Step 5   Enter a meaningful name for the action (for example, Uninstall URT).

Step 6   Click **Create**.

Step 7   Select the newly created action.

Step 8   Click **Details**.

Step 9   Select the Ignore package default schedule option and use the following settings:

     a.   In Scheduled Action, click **Details**.

     b.   Click the General tab.

     c.   Select these characteristics (allowing the others to default):

        Priority—Normal
        Impersonation—System

     d.   Click the Items tab.

     e.   Click **Add**.

        The Item Properties window is displayed.

     f.   Enter the filename of the Client Module uninstallation program in this format:

        `\\`*`Novellserver`*`\sys\public\urt\UrtClientUnInstall.bat`

        where *`Novellserver`* is the name of the server where you install the
        URT logon script. When the logon script is installed, URT installs the Client
        Module installation and uninstallation program on the server.

     g.   Click the Schedule tab.

     h.   Select User Login for Event.

     i.   Click the Advanced tab.

     j.   Select the Disable action after completion checkbox.

The Client Module is installed the next time the user logs onto the
NetWare domain.

Removing URT from Its Role in Handling User Logons

When you remove URT from your network, you must also remove the changes you made that enabled URT to direct user logons to the URT VPSs.

Step 1   To stop running the domain logon script when users log on, use one of these methods:

- In a Microsoft Networking environment—If the logon script in the NT domain server NETLOGON directory runs urt.bat, remove the command to run urt.bat.

- In a Microsoft Networking environment—If user profiles are directly associated with urt.bat, use the User Manager to update user profiles, and remove urt.bat as the logon script option.

- In a Novell NetWare environment—Use NAL to remove the following line from the logon properties for the organizational object that contains the users, groups, and other organizations you manage with URT:

    `@\\%FILE.SERVER\sys\public\urt\urt.bat %FILE_SERVER`

Step 2   Delete the urt.bat file.

In a Microsoft Networking environment, the urt.bat file is in the same directory as the logon script.

Tip   If you are not sure of the location of the logon script, use the Windows **Start > Find > Files or Folders** command to locate urt.bat. The logon script is located in the same directory.

Removing URT VPSs

Before you remove the URT VPSs, you must update your switches to direct them to switch-based VMPSs. For more information, see:

- Redirecting Switches to Use a Switch-Based VMPS Before Removing URT, page 8-1
- Deleting a VPS, page 3-2

Removing the URT Administrative Server

You can remove the URT Administrative Server from the Windows control panel.

Step 1   Log onto the system on which the URT Administrative Server resides.

Step 2   Select **Start > Control Panel > Add/Remove Programs**.

Step 3   Select **URT Administrative Server.**

Step 4   Click **Add/Remove**.

Step 5   Follow the online instructions.

.

U