DIGITAL NetRider

DIGITAL Remote Access Security Use

Part Number: AA-QWW5B-TE

June 1997

Revision/UpdateInformation:	This is a revised document.
Operating System:	Microsoft Windows NT, Version 3.51 or 4.0
	Microsoft Windows 95
Software and Version:	DIGITAL Remote Access Security, Version 2.2

Contents

Preface

1 DIGITAL Remote Access Security Description

2 Concepts

3 Managing the DRAS Server

4 Accounting and Events

A Sample Configurations

B RADIUS Attributes

Index

Preface

Overview

Purpose

This book explains how to use the DIGITAL Remote Access Security (DRAS) software to manage a DRAS server and its databases.

Intended Audience

This book is written for system and network administrators responsible for making network access server products available on their local and wide area networks (LANs and WANs). Readers should be familiar with Internet network management concepts and the Microsoft Windows NT operating system.

Conventions

This book uses the following conventions:

Convention	Description
bold face text	Bold face text indicates new terms.
`monospace text`	Monospace text in command examples indicates system output.
`bold monospace text`	Monospace text in bold face type in command examples indicates user input.

Associated Documents

The following documents are available:

- *DIGITAL Remote Access Security Installation*
- DRAS Manager online help
- *Network Access Server Management*

How to Order Additional Documentation

To order additional documentation, use the following information:

To Order:	Contact:
By Telephone	USA (except Alaska, New Hampshire, and Hawaii): 1-800-DIGITAL (1-800-344-4825) Alaska, New Hampshire, and Hawaii: 1-603-884-6660 Canada: 1-800-267-6215
Electronically (USA only)	Dial 1-800-DEC-DEMO (For assistance, call 1-800-DIGITAL)
By Mail (USA and Puerto Rico)	DIGITAL EQUIPMENT CORPORATION P.O. Box CS2008 Nashua, New Hampshire 03061 (Place prepaid orders from Puerto Rico with the local DIGITAL subsidiary: 809-754-7575)
By Mail (Canada)	DIGITAL EQUIPMENT of CANADA LTD. 940 Belfast Road Ottawa, Ontario, Canada K1G 4C2 Attn.: A&SG Business Manager
Internationally	DIGITAL EQUIPMENT CORPORATION Attn.: A&SG Business Manager c/o local DIGITAL subsidiary or approved distributor
Internally	U.S. Software Supply Business (SSB) DIGITAL EQUIPMENT CORPORATION 8 Cotton Road Nashua, New Hampshire 03063

Correspondence

Documentation Comments

If you have comments or suggestions about this document, send them to the DIGITAL documentation organization.

Attn.:	Documentation Project Manager
FAX:	(508) 486-5655
E-MAIL:	doc_quality@lkg.mts.dec.com

Online Services

To locate product-specific information, refer to the following online services:

BBS

To read the Bulletin Board System, set your modem to 8 bits, no parity, 1 stop bit, and dial 508-486-5777(U.S.). Outside of the U.S., dial (access code) 1-508-486-5777.

WWW

The Digital Equipment Corporation Network Products Business Home Page on the World Wide Web is at the following addresses:

North America:	http://www.networks.digital.com
Europe:	http://www.networks.europe.digital.com
Australia:	http://www.digital.com.au/networks

Chapter 1

DIGITAL Remote Access Security Description

Overview

Introduction

This chapter describes the components in the DIGITAL Remote Access Security product, how it operates, and the services it provides.

In This Chapter

This chapter describes the DIGITAL Remote Access Security (DRAS) features and components, as well as a how the DRAS server operates. This chapter contains the following topics:

- What Is DIGITAL Remote Access Security?
- Product Features
- Components
- Server Operation
- Services Overview
- Authentication Services
- Authorization Services
- Accounting Services

What Is DIGITAL Remote Access Security?

Introduction

DIGITAL Remote Access Security (DRAS) is an application that allows you to configure and manage secure remote access to your network. You can control who accesses your network, when they can access it, and what they can do when connected to the network. In addition, you can track a user's activities for accounting purposes.

DRAS Protocol

The DRAS software uses the Remote Authentication Dial-In User Service (RADIUS) protocol as defined in the current Internet Engineering Task Force (IETF) RFC 2058 and RFC 2059. Any network access server that communicates with the DRAS server needs to support the RADIUS protocol.

Product Features

Client/Server Model

DRAS uses a client/server model to ensure secure remote access to your network. In a typical configuration, a network access server (NAS) acts as a client to the DRAS server. The NAS passes user information to the DRAS server and acts on the response that it receives. When the DRAS server receives an access request from a client, it authenticates the request and returns any necessary configuration information to the client.

Remote Management

You can use the DRAS Manager, a Windows based management application, to manage local *and* remote DRAS servers running on Windows NT, OpenVMS, and DIGITAL UNIX systems.

Network Security

Authentication through the use of encrypted passwords ensures that the transactions between the DRAS server and a client are secure. In addition, all user passwords that the DRAS server and the client transmit are encrypted, preventing unauthorized users from obtaining the password.

Easy-to-Use Management Utility

The DRAS Manager has an easy-to-use graphic user interface that allows you to configure local and remote DRAS databases quickly and manage the DRAS server's operation.

Multiple Authentication Methods

The DRAS server supports several methods for authenticating users. For example, it can support:

- Password authentication that uses either user passwords entered into DRAS or uses existing passwords in the DRAS server host's database
- Hardware authentication tokens, such as Security Dynamics Technologies' SecurID, Racal-Guardata's WatchWord, and Digital Pathways' Defender
- One -time password authentication, such as One-Time Password (OTP)

Components

Introduction

The DRAS product has two major components:

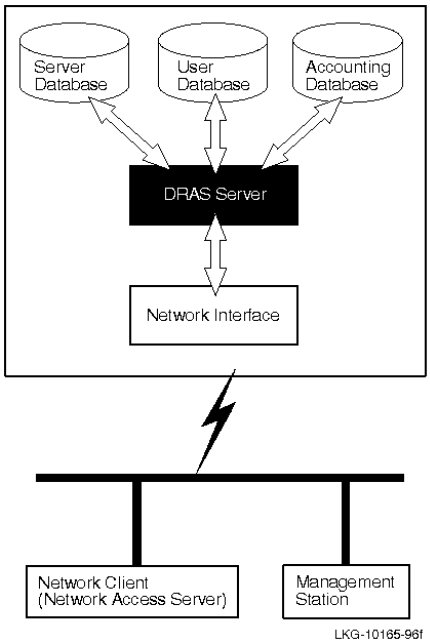
- DRAS server
- DRAS Manager

DRAS Server

The DRAS server is the application that communicates with various clients that send it access requests. A client can be a network access server (NAS) or a remote management workstation. The DRAS server stores information about users, clients, sessions, and authentication methods as objects in a local database. The DRAS server operates on systems that run the OpenVMS, Windows NT, or DIGITAL UNIX operating systems.

Diagram

The following diagram shows the components with which the DRAS server interacts:



Local Databases

Each DRAS server has local databases. The local databases contain objects for:

- All RADIUS clients (for example, network access servers) that send authentication, authorization, and accounting requests to the DRAS server.
- All remote management stations that you want to allow access to the DRAS server's databases.
- All users for whom the DRAS server performs authentication. The users do not interact directly with the DRAS server. Users interact with a RADIUS client, which then sends the authentication requests to the DRAS server.
- All administrative users that you want to allow access to the DRAS server's databases for remote management purposes.

DRAS Manager

The DRAS Manager is the Windows based application that you use to manage the DRAS server and configure its databases. The DRAS Manager operates on systems running the Windows NT and Windows 95 operating systems.

The DRAS Manager allows you to:

- Stop, pause, and resume a remote or local DRAS server.
- Enable and disable authentication or accounting requests.
- View status of local or remote servers.
- Manage objects in local and remote DRAS server databases.

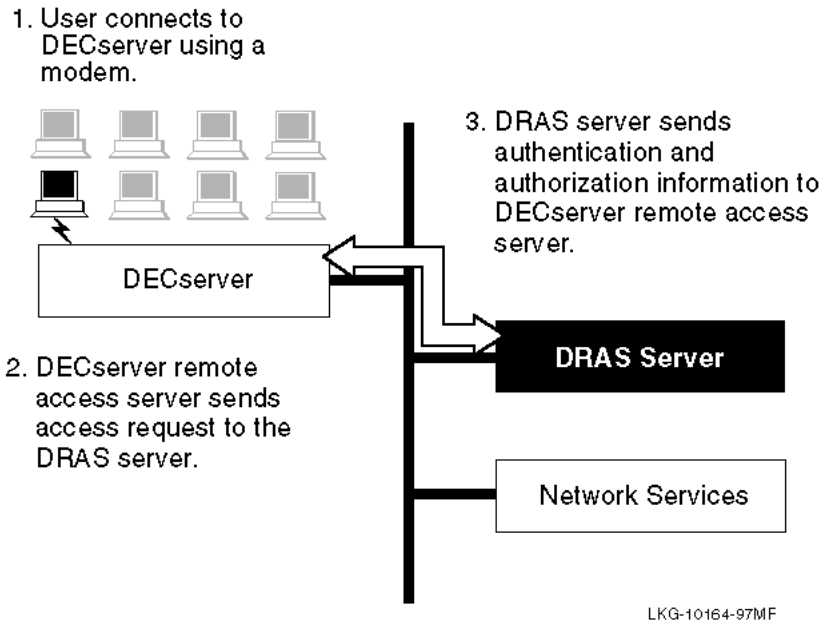
Server Operation

Introduction

This topic describes some of the ways in which the DRAS server interacts with its clients.

Diagram

The following diagram illustrates the process of a user requesting access to a remote network. In this diagram, a DECserver unit is the remote network access server (NAS). After the DRAS server completes the authentication and authorization process, the user can use network services as defined in the DRAS database.



Client/Server Interaction

The following table describes the stages of the NAS and DRAS server interaction:

Stage	Description
1	A NAS receives authentication information from an external user. **Example:** An external user dials a NAS and provides a user name and password.
2	The NAS creates an Access-Request data packet that contains attributes such as the user's name, the user's password, the ID of the client, and the port ID that the user is accessing.
3	The NAS sends the Access-Request packet to the DRAS server using the network.
4	The DRAS server receives the request and consults its users database to find the user whose name matches the request. The user entry in the database contains a list of requirements that must be met to allow access for the user.
5	If any condition is not met, the DRAS server sends an Access-Reject packet to the NAS, indicating that the user request is invalid.
6	If all conditions are met and the DRAS server wishes to issue a challenge to which the user must respond, the DRAS server sends an Access-Challenge response to the NAS.
7	If the NAS receives an Access-Challenge and supports challenge/response operations, it prompts the user for a response. It then re-submits its original Access-Request with a new request ID and the user response (encrypted).
8	If all conditions are met, the DRAS server sends a list of configuration values for the user to the NAS in an Access-Accept packet.

Services Overview

Types of Services

The DRAS server provides the following services to its clients:

Service	Description
Authentication	Allows the NAS to correctly and reliably identify an external user requesting network access.
Authorization	Defines what services the user may access on the network.
Accounting	Provides information about the services used by the user for billing, audit trail, and troubleshooting purposes.

Data Storage Areas

To provide these services, the server retrieves the necessary information from local user, accounting, or server databases. The DRAS management utility allows you to manage the data storage areas.

Authentication Services

Introduction

The authentication services determine whether an external user can access the network.

Supported Authentication Methods

The DRAS server supports the following methods of authentication:

Authentication Method	Description
CHAP	Static password using CHAP is a challenge/ response authentication protocol used by PPP.
DEFENDER	This is Digital Pathways' challenge/response, two-factor authentication. It uses the DES algorithm to generate unique, one-time passwords.
HOST	This authentication method uses the DRAS server's host login authentication.
OTP	This is an MD5-based challenge/response authentication. It implements a one-time password authentication system. OTP is derived from Bellcore's S/Key.
PASSWORD	The DRAS server uses a static password, in conjunction with a user name, registered in its database for the user. Typically, the user can change this password. In this case, you change the password registered in the DRAS server database.
SECURID	Performs user authentication using the Security Dynamics Technologies' SecurID token cards. You need an SDI ACE/Server on the network for this authentication method.
WATCHWORD	This is Racal-Guardata's challenge/response authentication. It uses the encryption algorithm that the WatchWord calculator implements.

Authorization Services

Introduction

User authorization consists of validating the user after authentication completes. In addition, authorization services include security facilities.

Authorization Criteria

The following table lists the criteria that the DRAS server uses for authorization:

Criteria	Description
User account enabled	The DRAS server checks the user object in its database to determine whether the user account enabled flag is set. User objects are likely to be disabled following a break-in detection, or a configurable amount of time during which the object is not used.
User account expiration	The DRAS server checks the user expiration date and time in the user database against the current local time.
User account access hours	The server checks the user access hours (which defines a weekly access schedule) against the local time.
User group check	The DRAS server checks group objects in its database against the following criteria: • Group enabled • Group expiration • Group access hours

Security Facilities

The DRAS server provides the following security-related functions in addition to normal user authorization.

Break-In Detection

Break-In detection automatically detects if a remote access system is under attack.

If:	Then the DRAS Server:
Several consecutive authentication failures for a particular user	Disables the user account. Enabling requires manual intervention.
Several consecutive authentication failures from a particular port/NAS	Rejects any further access request from this port on the NAS. The DRAS server puts the port/NAS combination on a “blacklist”.

Duress Login Detection

Certain authentication devices allow a user under a threat to connect and tell the NAS that the connection is occurring under abnormal conditions. When detecting this, the NAS must allow the connection, but tracks, flags, and possibly reports the exception to a management station. This detection depends on the capabilities of the authentication method in use:

- For built-in static password authentication, users signify a duress login by doubling the last character of its normal password.
- For WatchWord authentication, the user types the secondary PIN (personal identification number) of the calculator.

Accounting Services

Introduction

Clients generate accounting information related to the usage and operation of the remote access system (which comprises the NAS and the local DRAS server). You use the DRAS Manager to display this information.

Event Types

The DRAS server stores accounting information by types of events. The following table describes these types:

Type	Description
Accounting event	This event is generated for each RADIUS Accounting Request packet received from a NAS.
Connection events	This event is generated for each Access-Request packet received from a NAS.
Distributed operations events	This event is generated for each Access-Request packet received from a remote NAS or management station.
General events	This event is generated for each operational exception (startup, shutdown) of the local DRAS server.
Security events	This event is generated for any security-related events, such as: break-in detection on port, user duress login, or password/secret change.

Chapter 2

Concepts

Overview

Introduction

Before you start using the DRAS software, it is useful to understand the concepts that this chapter describes.

In This Chapter

This chapter contains the following the topics:

- Shared Secret
- Authentication Methods
- Registration
- Databases
- Database Objects

Shared Secret

Introduction

Once active, the DRAS server waits for access requests from **clients**. A client can be a network access server (NAS) or a remote management station that supports the Remote Authentication Dial In User Service (RADIUS) protocol. The DRAS server and the client share a **secret** (password) to determine if communications between the two can occur.

Process

For communication between DRAS servers and clients to occur:

Step	Action
1	Configure your client so it can perform RADIUS operations (see the documentation that ships with your client for instructions). During the configuration, you define a unique secret for the client.
2	Register a client object in the DRAS server database and specify the client's unique secret. The secret must match the secret defined on the client.

Secrets Must Match

The client secret you register in the DRAS database and the secret defined on the client *must match exactly* (secrets are case sensitive). If they do not match, communications between the DRAS server and the client cannot occur.

How Clients and DRAS Servers Use Secrets

The following table describes how the DRAS server and client share the client secret during authentication:

Stage	Action
1	When a client sends an access request to the DRAS server, it sends authentication information with the request. The authentication information contains a randomly generated number. The client uses this number to authenticate responses that it receives from the DRAS server. **Secret Usage:** The client also uses the secret to encrypt user passwords that it transmits across the network. This helps prevent unauthorized access to user passwords during network communications.
2	The DRAS server encrypts this number with the client secret that you registered in its database and returns the result to the client.
3	The client uses the returned information to verify that the response came from a valid DRAS server.

Authentication Methods

What Is Authentication?

DRAS supports several authentication methods to prevent users from gaining unauthorized access to your network.

Authentication includes challenge/responses, static and dynamic passwords, token cards, security keys, and encryption algorithms. Some authentication processes may include a combination of methods.

Before you configure your database, decide what type of authentication method best suits your environment. This section briefly describes the security methods that DRAS supports.

Challenge/Response Example

Many of the authentication methods that DRAS supports use a challenge/response operation.

The following occurs during a challenge/response operation:

Stage	Description
1	When the NAS sends an Access-Request, the DRAS server responds with an Access-Challenge packet. The Access-Challenge packet typically contains a Reply-Message that includes challenge information that the NAS displays to the external user (for example, a numeric value unlikely ever to be repeated). Usually, the DRAS server obtains the challenge from an external server.
2	The NAS displays the number, challenging the user to encrypt it, and returns the result to the DRAS server.
3	Authorized users have special devices, such as smart cards, that facilitate calculation of the correct response with ease. The user enters the challenge into the device, which calculates a response. The user provides the NAS with the response. The NAS forwards the response to the DRAS server in a second Access-Request packet.
4	If the response matches the expected response, the DRAS server replies with an Access-Accept packet and the external user gains access to the network. If the response does not match, the DRAS server sends an Access-Reject packet and the external user cannot access the network.

CHAP Authentication Operation

CHAP (Challenge-Handshake Authentication Protocol) authentication uses a challenge/response operation. This is the one of the two authentication methods that PPP uses. See also the Password or PAP Authentication section in this chapter.

CHAP Authentication Process

The following occurs during a CHAP authentication operation:

Stage	Action
1	When the external user begins the connection process, the NAS generates a 16-octet random challenge and sends it to the user requesting authentication.
2	The user responds with a CHAP response, a CHAP ID, and a CHAP user name.
3	The NAS sends an Access-Request packet to the DRAS server that contains the CHAP authentication information.
4	The DRAS server examines the CHAP response it receives, encrypts the challenge, and compares that to the user's CHAP response.
5	If they match, the DRAS server sends an Access-Accept packet to the NAS and the external user gains access to the network. If they do not match, the DRAS server sends an Access-Reject packet to the NAS. The external user cannot access the network in this situation.

If you want to use CHAP authentication when you use PPP, make sure you configure your system to use CHAP authentication and not password or PAP authentication.

Defender Authentication Operation

Defender authentication is a challenge/response authentication protocol that uses the Digital Pathways SecureNet Key, which is a personal identification token that resembles a pocket calculator. To use Defender authentication, you must have a properly installed and configured Defender server and you must configure DRAS to be able to connect to the Defender server. Place the following Defender configuration parameters into the [Defender] section of the DRAS configuration file:

```
[Defender]
agentkey=
agentid=
dss_address
```

A user uses a unique PIN and a DES key to generate a one-time password. Note that the user's PIN does not pass over the network.

Defender Authentication Operation

The following occurs during a Defender authentication operation:

Stage	Action
1	The external user enters a user name and enters a carriage return at the password prompt.
2	The DRAS server responds with a challenge.
3	The user enters his or her unique PIN and the challenge into the SecureNet Key.
4	The user enters the response the SecureNet key provides.

Because CHAP authentication requires access to the user's unencrypted password but Defender authentication cannot provide the user's password to the DRAS server, PPP CHAP clients are incompatible with Defender authentication. You must configure LCP authentication for PPP PAP.

Host Authentication Operation

Host authentication involves the DRAS server using the host's standard interactive logon service and native user database to authenticate a user.

When registering a user in the DRAS database, you do not need to enter information in the user's password field.

Host Authentication Operation

The following occurs during a host authentication operation:

Stage	Action
1	The external user enters a user name and a password.
2	The DRAS server authenticates the user by using the host's standard interactive logon service and native user database.

Because CHAP authentication requires access to the user's unencrypted password but host authentication cannot provide the user's password to the DRAS server, PPP CHAP clients are incompatible with host authentication. You must configure LCP authentication for PPP PAP.

Password or PAP Authentication

Password authentication, also known as PAP (Password Authentication Protocol), is one of the two authentication methods that PPP uses. See also the CHAP Authentication Operation section in this chapter.

You need to enter a user's password in the password field when registering the user in the DRAS database. You can also allow a user to change their own passwords when they log in through a NAS.

Password Authentication Operation

The following occurs during a password authentication operation:

Stage	Action
1	The external user enters a user name and password.
2	The DRAS server uses the static password and user name registered in the DRAS database to authenticate the user.

If you want to use password authentication when you use PPP, make sure you configure your system to use password authentication and not CHAP authentication.

Note that user passwords do pass over the telephone network connection from the user to the NAS.

OTP Authentication Operation

One-Time Password (OTP) authentication, also known as S/Key, uses a one-time password authentication system. OTP provides authentication for system access (login) and applications that require authentication that is secure against passive attacks. Passive attacks are based on replaying captured reusable passwords.

OTP evolved from Bellcore's S/Key One-Time Password System. OTP is described in RFC 1938 (May 1996), which is the product of the One Time Password Authentication Working Group of the IETF. This is now a Proposed Standard Protocol.

Establishing OTP Authentication for a User

To establish OTP authentication for a user, do the following:

Step	Action
1	Open an existing user record or create a new user record.
2	Select OTP as the authentication method.
3	Enter the user's pass-phrase (and optionally, the number of passwords to generate and a seed) into the Password field. The format of the password field is: pass-phrase+count+seed where pass-phrase, count, and seed are character strings separated by the + character.

The pass-phrase range is 10 to 63 characters. This pass-phrase is known only by the user and never passes over the network. A user can safely use the same OTP pass-phrase on multiple systems as long as the seed is different on the various systems.

The count is the number of passwords to generate for this user. It is effectively the number of times the user may authenticate using this system.

The seed is a number consisting of numeric characters and must be 1 to 16 characters long. The server generates a seed if one is not supplied.

Authenticating and Logging In with OTP

To log in, do the following:

Step	Action
1	Enter your user name. The password is not required. The DRAS server ignores anything you enter in the password field.
2	The DRAS server returns a challenge in the form: otp-md5 <sequence integer> <seed>
3	Enter the sequence integer, seed, and secret pass-phrase into the OTP calculator to generate a response. This response is the currently valid one-time password.

Because the DRAS server supports only the MD5 hash algorithm, make sure the OTP calculator you use supports the MD5 hash algorithm.

The sequence number decreases every time a user successfully authenticates. Although the challenge displays the current sequence number, the DRAS server generates an additional warning message when the sequence number is less than 10.

Because CHAP authentication requires access to the user's unencrypted password but OTP authentication cannot provide the user's password to the DRAS server, PPP CHAP clients are incompatible with OTP authentication. You must configure LCP authentication for PPP PAP.

SecurID Authentication Operation

SecurID authentication uses a time-varying, one-time password operation. This method requires that users have a SecurID passcode; therefore, you do not need to enter information in the user's password field when registering users in the DRAS database.

Your DRAS server must be registered as a client on the Security Dynamics ACE server and you must have a copy of sdconf.rec file, which is created during ACE server installation, in your DRAS_DIR (or DRAS$DIR for OpenVMS) directory.

SecurID Authentication Process

The following occurs during a SecurID authentication operation:

Stage	Action
1	The user enters a user name.
2	The user enters the SecurID passcode at the password prompt.
3	If the user does not enter a passcode at the password prompt, a RADIUS request is issued to the DRAS server.
4	The DRAS server recognizes the user's authentication method as being SecurID and contacts the SecurID server.
5	The SecurID server requests the user's passcode, for which the DRAS server challenges the user.
6	The user enters the passcode at the password prompt, which the DRAS passes on to the SecurID server for authentication.

Because CHAP authentication requires access to the user's unencrypted password but SecurID authentication cannot provide the user's password to the DRAS server, PPP CHAP clients are incompatible with SecurID authentication. You must configure LCP authentication for PPP PAP.

WatchWord Authentication Operation

WatchWord authentication uses a DES-based challenge/response operation. The user uses the WatchWord token to generate dynamic passwords.

When you register a user in the DRAS database, you need to enter the user's DES key into the password field. The key is encrypted before being entered into the DRAS database.

WatchWord Authentication Operation

The following occurs during a WatchWord authentication operation:

Stage	Action
1	The user enters a user name.
2	The user uses the WatchWord token to generate a DES key.
3	The user enters the password at the Password prompt.

Because CHAP authentication requires access to the user's unencrypted password but WatchWord authentication cannot provide the user's password to the DRAS server, PPP CHAP clients are incompatible with WatchWord authentication. You must configure LCP authentication for PPP PAP.

Registration

Definition

Registration refers to creating entries in a database that contain properties for users and clients. These entries are called *objects*. An object's properties determine who can connect to the network, when they can make a connection, and what they can do once connected.

What You Register

Use the DRAS server management utility to register the following types of objects in the databases:

Object	Description
Authentication methods	The method the DRAS server uses to authenticate users requesting access to the network. For each user you register, you specify which authentication method the DRAS server uses.
Client	This identifies the clients with which the DRAS server communicates.
Groups	Special user objects whose properties apply to all users associated with it. This is useful if you want to apply the same properties to multiple users.
Sessions	A set of properties that the DRAS server uses for a specific service type. You can define a set of session properties that you apply to many users, or you can define session properties specific to one user.
Users	You can register the following types of users: • Administrators—users with administrator access. They can add to or modify the DRAS server databases. • Nonprivileged users—users that can access the network but cannot change the DRAS server databases.

Databases

Database Types

The DRAS server contains the following databases:

Database	Description
User	Contains information about individual users: who they are, when they can access the network, and what they can do after connecting to it. When you register users, groups, and sessions, the DRAS management utility stores their properties in this database.
Server	Contains information about the clients that communicate with the DRAS server and the types of authentication methods it uses. When you register clients and authentication methods, the DRAS management utility stores their properties in this database. **Client Types:** A client can be a network access server (NAS) that supports the RADIUS protocol or a remote management workstation.
Accounting;:	Contains information about external user and client events. The DRAS server receives this information from its clients and stores it in this database.

Database Objects

Introduction

The DRAS server databases contain the following object types:

- Group
- User
- Client
- Session
- Authentication

Group Objects

Groups are special types of user objects; all user objects belong to a group object. Group objects are useful if you want to set the same access hours for multiple users. An administrator group object (a group object that has the Administration Group box checked) must exist before you an assign administrative privileges to users.

User Objects

User objects contain all of the information that the DRAS server requires to authenticate and authorize a user's request for network access. The properties stored in the user object determine what the user is allowed to do after making a connection to the network.

Client Objects

Client objects define what communicates with the DRAS server. A client is either a network access server (NAS) or a remote management station.

When a client is a NAS, an external user connects to the NAS, usually using a modem, and the NAS communicates with the DRAS server to determine if the user is authorized to access the network.

When the client is a remote management station, and you also create a user object in the DRAS server's database, you can remotely manage the DRAS server.

Session Objects

A *session object* provides a convenient way to store authorization properties that you apply to one or more users in one place. The authorization properties vary according to the type of service that the client provides to the user.

When you associate a generic session object with a user object, the DRAS Manager creates a private copy of the generic session object in the user object. You can then customize the session properties to meet the user's specific needs. The changes you make to the private copy do not affect the original generic session object. Conversely, changes you make to a generic session object do not affect the private copy in a user object.

Authentication Objects

An *authentication object* defines an authentication method that the DRAS server can use when it receives a client request for user authentication. This method requires a user to supply the client with a password. The client sends this password, in encrypted form, to the DRAS server. The DRAS server checks the appropriate user object to determine if it received a password it recognizes.

The DRAS server implements each authentication method as a separate module (if using the Windows NT operating system, this is a DLL file). To register an authentication module, you supply a name for the authentication method and the image's file name (without the file extension).

Chapter 3

Managing the DRAS Server

Overview

Introduction

Use the DRAS Manager to:

- Configure and maintain local and remote DRAS server databases.
- Manage DRAS server operation.

Installation Instructions

See the *DIGITAL Remote Access Security Installation* book for installation instructions.

In This Chapter

This chapter contains the following topics:

- Configuration Tasks
- Logging On
- Registering Clients
- Registering Groups
- Registering Administrators
- Registering Sessions
- Registering Users
- Registering Authentication Methods
- Managing DRAS Server Operation

Configuration Tasks

Initial Database Configuration

The following table lists the tasks you complete to configure the initial database:

Step	Action
1	Run the SetupDb utility (optional), which is a utility for Windows NT and DIGITAL UNIX that allows you to create an initial DRAS server database after the software installation. See the *DIGITAL Remote Access Security Installation* guide for instructions.
2	Log on to the DRAS Manager.
3	Plan your database structure.
4	Select an authentication method for users.
5	Register any or all of the following database objects: • Clients • Administrators • Sessions • Users • New authentication methods

Logging On

Procedure

To log on:

Step	Action
1	Click the DRAS Manager icon in the DRAS program group. The utility displays the Logon dialog box.
2	Log on to the DRAS Manager. Do the following (logon information is case sensitive): **a** If accessing a local DRAS server database, or if this is the first time you are logging in after installation, you can choose to leave the Logon boxes blank. **b** If accessing a remote DRAS server database, enter the user name, password, and secret for your management station as registered in user and client objects in the remote DRAS server database. **c** Click OK.
3	After you log on, the utility displays the browser window. To display available DRAS servers in the same subnet, select Scan Network from the Servers menu. If you want to access DRAS servers outside of your subnet, add the Server by selecting Add from the Servers menu and entering the DRAS server's Internet address or fully qualified domain name.
4	Click the icon next to the DRAS server to which you want to connect. • If the information you entered at login time does not match a user and client object in the selected DRAS server's database, the DRAS Manager asks you to log on again. • If the login information you enter matches a user and client object in the selected DRAS server's database, the DRAS Manager displays the DRAS server's database objects.

Registering Clients

Introduction

This topic explains how to register network access server and management station client objects.

Client objects identify the clients that can communicate with the DRAS server. If the client is a network access server (NAS), configure the NAS to be a RADIUS client.

Registration Instructions

See the DRAS Manager's online help for step-by-step instructions for registering new client objects.

Properties

The following table lists the properties you can set for client objects:

Attribute Type	Description
Name	The client's fully qualified domain name or Internet address.
Secret	The secret the client shares with the DRAS server. The secret you enter here *must* match the secret defined on the client exactly (secrets are case sensitive).
Description	A description of the client, which must be less than 255 characters (optional).
Enable	Indicates whether the DRAS server responds to the specified client's requests.
Type	The type of client (for example, DECserver access server or management station).

Registering a Remote Management Station

To allow a management station to manage a remote DRAS server:

Step	Action
1	Create a client object that identifies the management station. Be sure to check the Enabled box to activate the object.
2	Create a group with the Administration group box checked.
3	Create a user object for each person using the management station. Associate the user object with the administration group. This allows you (or other administrators) to manage the local database from a remote management station.

After Registering the Remote Management Station

When logging in, the administrator *must* enter the client secret defined in the client object to access the DRAS server.

Registering a NAS

To register a NAS:

Step	Action
1	Register the client object. Be sure to check the Enabled box to activate the object.
2	Enter the client secret that matches the secret defined on the NAS. If the two secrets, the one stored in the DRAS server database and the one defined on the NAS, do not match exactly, communication between the NAS and the DRAS server cannot take place.

Registering Groups

Introduction

This topic explains how to register administrator and user groups objects. Group objects are a way to organize the information about the users who access your network remotely. In addition, group objects allow you to set:

- Administration privileges for multiple administrators
- Access hours properties for multiple users

Registration Instructions

The DRAS Manager's online help contains step-by-step instructions for registering new client objects.

Recommendation

Create your group objects before creating user objects. When you register user objects, you must associate them with a group object.

Properties

You can set general and access hours properties for group objects.

General Properties

The following table describes these properties:

Attribute Type	Description
Group Enabled	When checked, enables users associated with the group to access the network.
Name	The name you assign to the group object.
Administration Group	When checked, gives all users associated with the group administrator privileges.
Description	A description of the group object. (optional)
Expiration Date	When checked, allows you to set a date when the group object expires. If the group object expires, users associated with it cannot access the network.

Access Hours Properties

The days and hours when users associated with this group can access the network.

Registering Administrator Groups

An administrator group gives all users associated with it access to the DRAS databases. To register an administrator group:

Step	Action
1	Create a group and check the Administration group box.
2	Set the access hours properties. These properties apply to all users associated with the group object. • If the access hour properties you set are more restrictive than those set for a user object, the DRAS server tells a client to use the more restrictive properties. • If the access hours set for the user object associated with this group are more restrictive, the DRAS server uses these properties instead of the administration group access hours properties.

Registering User Groups

A user group is a way of organizing the users that access your network remotely. To register a user group:

Step	Action
1	Create a group. Do not check the Administration group box.
2	Set the access hours properties. If these access hour properties are more restrictive than those assigned to a user, the DRAS server sends these properties to the client. If the access hours set for the user object associated with this group are more restrictive, the DRAS server uses these properties instead of the administration group access hours properties.

Registering Administrators

Introduction

Users with administrator privileges can add or change properties in the DRAS server's user, server, and accounting databases. To give a user administrator privileges, you associate the user object with a group that has the Administration attribute enabled.

If you run the SetupDb utility after installing your software, it creates a default administrative user object. You can continue to log on as that user, or register a new administrator.

Registration Instructions

The DRAS Manager's online help contains step-by-step instructions for registering new user objects.

Properties

Set the same properties as you set for user objects. In addition, check the Administration group box in the General properties page.

Procedure

To assign administrator privileges:

Step	Action
1	Create a group object that has the Administration group box checked, if one does not already exist.
2	Associate the user object with the group object. Enter the name of the administration group in the Group field on the user object's General properties page. **Access Hours:** It is not required that you set the access hours properties in the user object. Set these properties if you want to specify more restrictive properties than exist in the administration group object. The DRAS server examines both the user and group object properties and tells the client to use the most restrictive access hour properties.

Registering Sessions

Introduction

The user database contains session objects that provide information about the sessions that the client is supposed to provide to external users. Registering session objects is a convenient way to store authorization properties that you apply to one or more users in one place. When you register user objects, you associate them with session objects and customize the session properties to meet the user's needs.

Registration Instructions

The DRAS Manager's online help contains step-by-step instructions for registering new and modifying existing session objects.

Session Objects Are Templates

The session objects you register in the DRAS server database are generic templates that you can apply to any user object. When you associate a generic session object with a user object, the DRAS Manager creates a private copy of the generic session object in the user object. You can then customize the session properties to meet the user's specific needs. The changes you make to the private copy do not affect the original generic session object. Conversely, changes you make to a generic session object do not affect the private copy in a user object.

You can view and customize the properties of the private copy of the session object only by accessing the user object.

Recommendations

Register session objects before registering user objects. You cannot associate a user object with a session object that does not exist.

Depending on the session type you select, you can configure additional session properties. Configure as many of the properties that apply to most users. This reduces the amount of customization required when you register user objects.

Properties

The following table lists the properties you can set for session objects:

Attribute Type	Description
Session Name	The name you assign to the session object.
Session Type	The type of session to be applied to users: • Telnet • Rlogin • Portmaster • TCP • LAT • IPX • AppleTalk For all session types, excluding Rlogin and Portmaster, you need to configure additional properties. The appropriate fields display in the window when you select a session type. The DRAS Manager's online help describes each field in detail.
Description	A description of the session object.

Registering a Generic Session Object

To create a generic session object:

Step	Action
1	Create a session object and give it a descriptive name. For example, if registering a session object for a Telnet session, you might call it Telnet.
2	Select the session type.
3	Configure the session properties that appear in the window. The DRAS Manager displays the properties appropriate to the session type you select. **Recommendation:** Configure only those properties that typically apply to all users. When you associate the session object with a user object, you can customize the properties to meet the user's needs.

Registering Users

Introduction

This topic explains:

- The properties you can set for user objects
- How to register new user objects
- How to use generic session templates to set user-specific session properties

The user database contains the properties that affect who can access the network and what that user can do when authorized to make a connection. The DRAS server stores properties for each user in a user object.

Registration Instructions

The DRAS Manager's online help contains step-by-step instructions for registering new client objects.

Properties

You can set the following types of properties for user objects:

Property Type	Description
General	General properties for the user object.
Services	The types of services the client provides to the user.
Access Hours	The days and hours when users can access the network. The default is to provide access on all days, at all times. You select the days and times when you deny access to the user.
DECserver	Vendor-specific properties that DECserver access servers support.
Password Management	Password management data that determines when passwords expire and allows users to change their own passwords. This property applies only to users using password authentication.

General Properties

The following table lists the general properties you can set for each user object:

Properties	Description
Account Enabled	When checked, indicates the user is allowed to access the network. When left blank, the user cannot access the network.
Name	The user name that the external user enters when logging on to the client. Identifies the user who connects to the network.
Group	The group entry with which the user is associated.
Authentication Method	The method that the DRAS server uses to authenticate the user during an attempt to connect to the network.
Description	A description of the user entry (optional).
Password	The password or other authentication information that the external user enters when logging in to the client. **For Host and SecurID Password:** This property is not applicable. **For OTP:** Enter the user's pass-phrase, and optionally, the sequence number and challenge value. **For WatchWord:** Enter the user's DES key.
Account	The account number for the user (optional).
Location	The location of the user (optional).
Cost Center	The cost center to which the user belongs (optional).
Expiration	The date when the entry expires.

Services Properties

These properties specify the type of service that the client should provide to the external user (for example, Telnet or PPP). Depending on the service type you select, you might also need to configure session properties that the client uses while the external user is connected to the network.

The following table lists the services properties that you can set:

Property	Description
Service Type	The type of service that the client provides to the user. Some service types require additional properties; the appropriate fields are displayed when you select these service types.
Framed Protocol	This field is active only when you select a service type that supports framed protocols. The supported framed protocols are PPP and SLIP.
Session Timeout	The amount of time, in seconds, after which the client should terminate the session.
Idle Timeout	The amount of time, in seconds, after which the client should terminate the current session if it detects no user activity.
Available Sessions	If session objects exist that support a selected service type, the session object names appear in this box. To apply the session object to the user object: **1** Select the session object name. **2** Click Add.
Selected Session	The name of the session object associated with the user object. • To reconfigure the session properties, click the Configure button. • To view the properties, click the View button.

Service Types

For some service types that you select, you need to configure sessions for the user. The following table lists the supported service types and the types of sessions you can configure for them:

This Service Type:	Does This:	And Can Have This Session Type:
Login	Connects the user to a specific host using Telnet, rlogin, or LAT protocols.	One of the following: • LAT • Telnet
Framed	Starts a framed protocol connection for the user, such as PPP or SLIP.	TCP/IP
Callback Login	Disconnects the user, dials a specified number, and connects the user to a host using LAT, Telnet, or rlogin protocol.	One of the following: • LAT • Telnet
Callback Framed	Disconnects the user, dials a specified number, and starts a framed protocol for the user, such as PPP or SLIP.	TCP/IP
Outbound User	Connects the user to a service on a port (for example, a modem pool, a Telnet listener, or reverse LAT). DECserver access servers do not currently support this service type.	No session type is applicable.
Administrative User	Gives the user privileged access to the client's command shell.	No session type is applicable.
NAS Prompt	Gives the user nonprivileged access to the client's command shell.	No session type is applicable.

This Service Type:	Does This:	And Can Have This Session Type:
Authenticate Only	Performs authentication only. The client does not receive any authorization information for the user. In general, proxy servers (other RADIUS servers) use this service rather than a NAS. DECserver access servers do not currently support this service type.	No session type is applicable.
Callback NAS Prompt	Disconnects the user, dials a specified number, and provides nonprivileged access to the client's command shell.	No session type is applicable.

DECserver Specific Properties

If you select NAS Prompt or Callback NAS Prompt as your service type and the client is a DECserver access server, select the DECserver tab and set the appropriate DECserver properties.

DECserver Properties

The following table lists the DECserver properties that you can set for each user object:

Property	Description
Permissions	The type of service or privilege level that the DECserver access server provides. This applies to the NAS Prompt service type.
Dialback Numbers	The list of telephone numbers that the user can specify when requesting dial-back service. If the user specifies a number not on the list, the DRAS server tells the client not to implement the service.
Dialout Numbers	The list of telephone numbers the user can specify when requesting dial-out service. If the user specifies a number not on the list, the DRAS server tells the client not to implement the service.
Dialout Services	The name of the dialer service defined on the DECserver access server. You configure the dialer service on the DECserver access server, which then implements it during a dial-out operation.

Password Management Properties

The following table lists the password management properties that you can set for each user object:

Property	Description
Expiration Enable	When checked, indicates that a password will expire at a predetermined time. When left blank, indicates there is no predetermined time for the password to expire.
Expiration Date/ Time	Indicates the month, day, and year when a user password expires.
Password Lifetime	The number of days the password is valid before expiration.
Permission to Change Password	When checked, indicates the user is allowed to change the password. When left blank, the user cannot change the password.
Minimum Length	Indicates the minimum number of characters the user can supply for a password.
Notification Enable	When checked, indicates that the user will be notified when the password expires. When left blank, the user will not be notified of password expiration.
Days Ahead to Notify Expiration	Indicates the number of days prior to password expiration when the user is notified.

Remember that this feature applies only to users that select the password authentication method.

Registering New Users

To register new users:

Step	Action
1	Create a group object, if one does not already exist.
2	Create a user object and enter the name of the group in the Group field on the user object's General property page.
3	Set the appropriate properties on the General, Services, Access Hours, DECserver, and Password Management property pages. **Notes:** When setting the access hours properties, keep in mind that the DRAS server examines these properties in the group and user objects. It then tells the client to use the most restrictive settings. Set the DECserver properties when you select the NAS Prompt or the Callback NAS Prompt as the service type on the Services property page.

Using Generic Session Objects

The service type that you assign to each user object determines what type of session properties can apply. The DRAS server assumes that the client through which the user gains access to the network can support the service and session types that you set in the user objects.

To use generic session objects to configure user-specific session properties:

Step	Action
1	When you register a user object, select an available session object from the Services property page. This session object is a generic template.
2	Customize the session object by clicking Configure. For example, you may need to add a user-specific Internet address that is not configured in the generic session template. The changes you make here do not change the original generic session template. The user-specific properties that you enter apply to the user for the duration of the user's session.

Registering Authentication Methods

Introduction

The Server database contains information about the clients and the authentication methods that they should use. The DRAS server stores properties for each specified authentication method in an *authentication object*.

Generally, you do not need to register new authentication methods, unless the ones supplied with the application do not meet your needs.

Registration Instructions

See the DRAS Manager's online help for step-by-step instructions for registering new authentication objects.

DIGITAL-Supplied Authentication Methods

When you perform remote management, you must have the appropriate authentication callout modules available locally for any authentication methods you intend to use or specify on the remote system.

If you install DRAS normally, the necessary authentication callout modules will reside in the appropriate location on your system or systems.

The DRAS software ships with the authentication modules for the following authentication methods:

- CHAP
- DEFENDER
- HOST
- OTP
- PASSWORD
- SECURID
- WATCHWORD

Properties

The following table lists the properties that you can set for authentication objects:

Property Type	Description
Authentication	The name you assign to the authentication object (see the Naming Conventions topic).
Callout	The image that the DRAS server calls during authentication. Enter the name of the file or library, without the file extension. For example, if running your DRAS server on a Windows NT machine, the image name is usually the name of a DLL file.

Naming Conventions

When registering authentication modules, use descriptive names. DIGITAL uses the following naming conventions for the modules it supplies:

Object Name	Description	Module Name (Callout)
CHAP	CHAP static password authentication	drascoch
DEFENDER	Defender authentication	drascods
HOST	Host login authentication	drascohp
OTP	OTP authentication	drascosk
PASSWORD	PAP static password authentication	drascosp
SECURID	SecurID authentication	drascosd
WATCHWORD	WatchWord authentication	drascoww

Registering Authentication Objects

To register authentication objects:

Step	Action
1	Install the image file for the authentication method on the system where your DRAS server operates.
2	Create a new authentication object: **a** Enter the name of the authentication method. **b** Enter the image file name (without file extension).

Managing DRAS Server Operation

Introduction

When the DRAS Servers window is active, you can access the Servers menu. The Servers menu lists the options available for managing DRAS server operation.

Tasks

The options on the Servers menu allow you to do the following:

- Stop, pause, or resume DRAS server activity.
- Scan the local subnet for DRAS servers.
- Add DRAS servers to the Server database. This allows you to connect to remote DRAS servers not in your subnet.
- Delete DRAS servers from the server database.
- View DRAS server properties.

Operation Instructions

The DRAS Manager's online help contains step-by-step instructions for controlling the DRAS server's operation.

Chapter 4

Accounting and Events

Overview

Introduction

The DRAS server collects accounting and event information about the DRAS server operation and connection activity. The DRAS server stores this information in its accounting database.

In This Chapter

This chapter contains the following topics:

- Event Description
- Event/RADIUS Accounting Log File
- Displaying Accounting Information
- Displaying Event Information
- Exporting RADIUS Accounting Information

Event Description

Introduction

When the DRAS server receives an accounting or access request from a NAS, it writes an event record to an event log file. This information helps you to:

- Understand the usage of the network access servers on your network
- Track unauthorized attempts to access your network
- Collect information about user connections for accounting and billing purposes

Event Types

The following table lists the types of event information that you can view using the DRAS Manager:

Event Type	Description
General	Events that each operational exception generates on the local DRAS server. **General Event Examples:** • Startup • Shutdown
Request	Events that each RADIUS Access-Request from a NAS generates when the DRAS server receives the request.
Security	Events that any security-related event generates. **Security Event Examples:** • Break-in detection on port • User duress login • Password or secret change
Distributed	Events that each access request generates when a remote DRAS server or DRAS Manager receives the request.
Accounting	Events that each RADIUS accounting request packet generates when the DRAS server receives the accounting request.

Event Severity Levels

The event severity levels indicate the general importance of the event. The severity levels are:

- Normal
- Critical
- Indeterminate
- Major
- Minor

Event/RADIUS Accounting Log File

Introduction

When the DRAS server receives event information, it writes it to a log file. When you display event or accounting information, the DRAS Manager opens the log file and displays its contents.

To access the information in the log file, use the DRAS Manager.

Maintaining the Log File

The DRAS server continues writing event information to the end of the log file. Depending on your client and DRAS server activity, this file can become very large. Periodically delete it to conserve disk space.

If you delete the file, the DRAS server creates a new file when it receives event information and cannot find an existing event log file.

Log File Names and Locations

The following table lists the names of the log files and their locations:

This File:	Is Named:	And Has a Default Path of:
OpenVMS log file	DRAS$ACCOUNTING.DAT	SYS$COMMON:[SYSEXE]
Windows NT log file	DRASACCT.DAT	\DRAS
DIGITAL UNIX log file	drasaccounting.dat	/usr/opt/dras/database

Displaying Accounting Information

Introduction

Use the DRAS Manager to view the accounting information that the DRAS server stores in the accounting database. You can view all accounting records or you can use filtering to customize what the DRAS Manager displays.

Procedure

To display detailed accounting information:

Step	Action
1	Start the DRAS Manager and select a DRAS server.
2	From the Tools menu, select Accounting.
3	Select the filtering criteria from the Accounting Events Selection window: • To display records between specific dates, select Start/End and enter the appropriate dates in the Start Date and End Date boxes. • To display records for a specific number of hours prior to the current time, select Last and enter the number of hours. • To display records that a specific user request generates, enter the user name as stored in the DRAS server database in the Username box. • To display records for all user requests, enter an asterisk (*) in the Username box. • To display records with a specific severity level, check the appropriate Severity box.
4	Click OK. The DRAS Manager retrieves the accounting records and displays them. The online help for this window describes each field.
5	To display the complete record for a specific event, click the event's text.

Displayed Information

The following table lists the information that the DRAS Manager displays when you open the Accounting Events window:

Field	Description
Date/Time	The date and time when the DRAS server received the Accounting-Request packet.
User Name	The name of the user requesting access.
Status Type	The status of the event: start or stop.
Authentic	The authentication method that the NAS used.
Session ID	The identification number (in hexadecimal) that the NAS assigns to a session.
Client IP	The Internet address for the client that initiated the accounting request.
Client Port	The port that the client uses for communication with the DRAS server.
Session Time	The number of seconds the session was active.
Termination Cause	The reason the session terminated.

Complete Event Record Contents

The following table lists the information that the DRAS Manager displays when you enable event text in the Accounting Events window:

Attribute	Description
Authentic	Authentication method that the NAS used.
Framed AppleTalk Link	AppleTalk network number that the NAS uses for the serial link to the user, when the user is an AppleTalk router.
Framed AppleTalk Network	AppleTalk network number that the NAS used to allocate an AppleTalk node for the user, when the user is an AppleTalk router.
Framed Compression	Type of compression protocol used on the link: Van Jacobsen TCP/IP header compression or IPX header compression.

Attribute	Description
Framed IPX Network	The IPX-specific routing information.
Framed MTU	The maximum transmission unit that the NAS used.
Framed Protocol	The type of framed protocol used: PPP or SLIP.
Framed Routing	The routing method used: 0 None 1 Send 2 Listen 3 Send & Listen
Idle Timeout	The maximum number of idle seconds of service that the NAS provides to the user.
Input Octets	The number of characters that the NAS receives from the user.
Input Packets	The number of packets that the NAS receives from the user.
Login Port	The TCP or LAT port to which the NAS connects the user.
NAS Identifier	The name of the NAS requesting user authentication.
NAS IP Address	The Internet address of the NAS requesting user authentication.
NAS Port	The physical port number of the NAS requesting user authentication.
Output Octets	The number of characters that the NAS sends to the user.
Output Packets	The number of packets that the NAS sends to the user.
Session ID	The identification number (in hexadecimal) that the NAS assigns to the session.
Session Time	The number of seconds the user is connected to the NAS.

Attribute	Description
Session Timeout	The maximum number of seconds of service that the NAS provides to the user.
Stats Type	The status of the event.
Termination Cause	The reason why the NAS terminated the session.
Time Stamp	The time that the DRAS server received the event record.
User Name	The name of the user requesting network access.

Displaying Event Information

Introduction

Use the DRAS Manager to view event information. You can view all events or you can use the filtering options on the Events Selection window to customize what the DRAS Manager displays.

Procedure

To display events:

Step	Action
1	Start the DRAS Manager and select a DRAS server.
2	From the Tools menu, select Events....
3	Select the filtering criteria from the Events Selection window: • To display records between specific dates, select Start/End and enter the appropriate dates in the Start Date and End Date boxes. • To display records for a specific number of hours prior to the current time, select Last and enter the number of hours. • To display only specific event types, check the appropriate Event Type box. • To display records with a specific severity level, check the appropriate Severity box.
4	Click OK. The DRAS Manager retrieves the event records and displays them. The online help for this window describes each field.
5	To display the complete record for a specific event, click the event's text.

Displayed Information

The following table lists the information that the DRAS Manager displays when you open the Events window:

Field	Description
Date/Time	The date and time the event occurred.
Type	The type of event.
Severity	The severity level of the event.
Information	A description of the event.

Complete Event Record Contents

The following table lists the information that the DRAS Manager displays when you click a specific event in the Accounting Events window:

Attribute	Description
Duress	An indication of whether the login occurred under duress.
Event Type	The type of event.
Information	A description of the event.
NAS ID	The name of the NAS requesting user authentication.
Severity	The severity level of the event.
Time Stamp	The time the DRAS server received the event record.
User Name	The name of the user requesting network access.

Exporting RADIUS Accounting Information

Introduction

The DRAS Manager allows you to export displayed RADIUS accounting information to a text file. You can then use the text file to print the RADIUS accounting information or import the file into other applications. The file format is a common delimited text file in which the first line is the field names and subsequent lines are data records.

Procedure

To export RADIUS accounting information, do the following:

Step	Action
1	Display RADIUS accounting information (see Displaying Accounting Information in this chapter).
2	Click Export.
3	Enter the path for the file you want to create and click OK. The DRAS Manager writes all of the displayed information into the file you specified.

Appendix A

Sample Configurations

Overview

Introduction

For all management tasks, use the DRAS Manager.

Online Help

For detailed step-by-step procedures, see the DRAS Manager's online help.

In This Appendix

This appendix describes the user properties you need to set for common remote access configurations. This appendix contains the following topics:

- Example: Interactive Connections
- Example: Dedicated Login Connections
- Example: Framed Connections
- Example: PPP Dial-Back Connections
- Example: Interactive Dial-Back Connections
- Example: Dial-Out Connections

Example: Interactive Connections

Description

The interactive user can use Telnet and LAT services from a character-cell session. The user can also use the NAS interactive command language.

User Properties

The following table lists examples of the types of properties that you need to set when registering interactive users:

On This Property Page:	Set These Properties:
General	• Account Enabled — Enables the object. • Name — The user name that the user provides to the NAS. • Authentication — Password. • Password — The password that the user provides to the NAS. • Expiration Date — The date you want the object to expire.
Services	• Service Type — NAS prompt. • Session Timeout — Amount of idle time (seconds) after which the client terminates the session. • Idle Timeout — Amount of idle time (seconds) allowed after which the client terminates the session.
Access Hours	Days and times when the user does not have access to the network.

Example: Dedicated Login Connections

Description

The user is automatically connected to a specific host using a specified protocol (for example, Telnet and LAT).

User Properties

The following table lists examples of the types of properties that you need to set when registering users with dedicated login connections:

On This Property Page:	Set These Properties:
General	• Account Enabled — Enables the object. • Name — The user name that the user provides to the NAS. • Authentication — Password. • Password — The password the user provides to the NAS. • Expiration Date — The date you want the object to expire.
Services	• Service Type — Login. • Session Timeout — Amount of time (seconds) after which the client terminates the session. • Idle Timeout — Amount of idle time (seconds) allowed after which the client terminates the session. • Session — Session object configured for Telnet or LAT.
Access Hours	Days and times when the user does not have access to the network.

Example: Framed Connections

Description

The user is connected using either the PPP or SLIP protocol.

User Properties

The following table lists examples of the types of properties that you need to set when registering users with framed connections.

On This Property Page:	Set These Properties:
General	• Account Enabled — Enables the object. • Name — The user name that the user provides to the NAS. • Authentication — Password. • Password — The password the user provides to the NAS. • Expiration Date — The date you want the object to expire.
Services	• Service Type — Framed. • Framed Protocol — PPP or SLIP. • Session Timeout — Amount of time (seconds) after which the client terminates the session. • Idle Timeout — Amount of idle time (seconds) allowed after which the client terminates the session. • Session — One or more session objects configured for TCP, TCP/IP, IPX, or AppleTalk.
Access Hours	Days and times when the user does not have access to the network.

Example: PPP Dial-Back Connections

Description

The user is connected using either the PPP protocol. After authentication is complete, the client terminates the session and dials the user with a predefined telephone number.

User Properties

The following table lists examples of the types of properties that you need to set when registering users with PPP dial-back connections:

On This Property Page:	Set These Properties:
General	• Account Enabled — Enables the object. • Name — The user name that the user provides to the NAS. • Authentication — Password. • Password — The password the user provides to the NAS. • Expiration Date — The date you want the object to expire.
Services	• Service Type — Callback Framed. • Callback Number — The telephone number the client dials. • Framed Protocol — PPP. • Session Timeout — Amount of time (seconds) after which the client terminates the session. • Idle Timeout — Amount of idle time (seconds) allowed after which the client terminates the session. • Session — One or more Session objects configured for TCP, TCP/IP, IPX, or AppleTalk.
Access Hours	Days and times when the user does not have access to the network.

Example: Interactive Dial-Back Connections

Description

The interactive user can use the NAS interactive command language from a character-cell session. After authentication is complete, the client terminates the session and dials the user.

User Properties

The following table lists examples of the types of properties that you need to set when registering users with interactive dial-back connections:

On This Property Page:	Set These Properties:
General	• Account Enabled — Enables the object. • Name — The user name that the user provides to the NAS. • Authentication — Password. • Password — The password the user provides to the NAS. • Expiration Date — The date you want the object to expire.
Services	• Service Type — Callback NAS prompt. • Callback Number — The telephone number the client dials. • Session Timeout — Amount of time (seconds) after which the client terminates the session. • Idle Timeout — Amount of idle time (seconds) allowed after which the client terminates the session.
Access Hours	Days and times when the user does not have access to the network.

Example: Dial-Out Connections

Description

Dial-out allows a user to connect to the NAS and dial a number to connect to a modem on a different port on the NAS.

User Properties

The following table lists examples of the types of properties that you need to set when registering users with dial-out connections:

On This Property Page:	Set These Properties:
General	• Account Enabled — Enables the object. • Name — The user name that the user provides to the NAS. • Authentication — Password. • Password — The password the user provides to the NAS. • Expiration Date — The date you want the object to expire.
Services	• Service Type — NAS prompt. • Session Timeout — Amount of time (seconds) after which the client terminates the session. • Idle Timeout — Amount of idle time (seconds) allowed after which the client terminates the session.
Access Hours	Days and times when the user does not have access to the network.
DECserver	• Dialout Number — Number the client dials after the user successfully connects to the client.

Appendix B

RADIUS Attributes

Overview

Introduction

This appendix lists the RADIUS attributes that the DRAS server supports.

In This Appendix

This appendix contains the following topics:

- General Session Attributes
- Framed Session Attributes
- Interactive Session Attributes
- Vendor-Specific Attributes

General Session Attributes

User-Name (1)

Description

Indicates the name of the user that the DRAS server should authenticate. This attribute appears only in Access-Request packets.

User-Password (2)

Description

Indicates the password of the user that the DRAS server should authenticate, or the user's input following an access challenge. The RADIUS client uses the shared secret to transmit the password in an encrypted format. This attribute appears only in Access-Request packets.

CHAP-Password (3)

Description

Indicates the response value that a PPP CHAP user provides in response to a challenge. This attribute appears only in Access-Request packets.

NAS-IP-Address (4)

Description

Indicates the identifying Internet address of a network access server (NAS) that is requesting user authentication. This attribute appears only in Access-Request packets. The NAS-Identifier attribute can appear instead of the NAS-IP-Address attribute.

NAS-Identifier (32)

Description

A string that identifies the network access server (NAS) that is requesting user identification. This attribute appears only in Access-Request packets. The NAS-IP-Address attribute can appear instead of the NAS-Identifier attribute.

NAS-Port (5)

Description

Indicates the physical port number of the NAS that is requesting user authentication. This attribute appears only in Access-Request packets. The NAS-Port-Type attribute can appear instead of or in addition to the NAS-Port attribute.

NAS-Port-Type (61)

Description

Indicates the type of physical port that the NAS requesting user authentication uses (for example, asynchronous, synchronous, ISDN synchronous, ISDN asynchronous). This attribute appears only in Access-Request packets. The NAS-Port attribute can appear instead of or in addition to the NAS-Port-Type attribute.

Service-Type (6)

Description

Indicates the type of service that a user is requesting or the type of service a RADIUS client should provide to the user. This attribute can appear in Access-Request and Access-Accept packets.

If the service type is one that the NAS does not recognize or support, it must respond as if it received an Access-Reject packet from the DRAS server.

Values

The following table lists the values for the Service-Type attribute:

Value	Description
1 Login	Delivers a dedicated connection to a specified host, using one of the following protocols: • Telnet • Rlogin • LAT
2 Framed	Delivers a network (framed) protocol connection using PPP or SLIP.

Value	Description
3 Callback Login	Terminates the initial connection, dials a specified telephone number, and establishes a dedicated connection to a specified host, using one of the following protocols: • Telnet • Rlogin • LAT
4 Callback Framed	Terminates the initial connection, dials a specified telephone number, and establishes a network (framed) protocol connection using PPP or SLIP.
5 Outbound User	Delivers a connection to a service on a port. For example, a modem pool.
6 Administrative User	Delivers a NAS prompt connection with privileged status.
7 NAS Prompt	Delivers a connection with access to the NAS user interface.
8 Authenticate Only	Used for proxy authentication between RADIUS servers.
9 Callback NAS Prompt	Terminates the initial connection, dials a specified telephone number, and establishes a connection with access to the NAS user interface.

Session-Timeout (27)

Description

The maximum number of seconds of service that the client is supposed to provide to the user prior to terminating the session. This attribute appears in Access-Accept and Access-Challenge packets.

Idle-Timeout (28)

Description

The maximum number of consecutive seconds of idle connection allowed to the user prior to terminating the session. This attribute appears in Access-Accept and Access-Challenge packets.

Framed Session Attributes

Framed-Protocol (7)

Description

Indicates the type of framed protocol to use for a session. This attribute can appear in Access-Request and Access-Accept packets. Values for this attribute are:

1 PPP

2 SLIP

Framed-IP-Address (8)

Description

Indicates the Internet address that a NAS should configure for the user (when DHCP or similar protocol is not used). This attribute can appear in Access-Accept and Access-Request packets.

Special Values

The value 255.255.255.255 indicates that the RADIUS server should allow the PPP client to negotiate the use of its local Internet address using IPCP, subject to the DECserver remote access server's subnet containment rules.

The value 255.255.255.254 indicates that the RADIUS server should assign the port's PPP address to the PPP or SLIP client, if the address exists.

Framed-IP-Netmask (9)

Description

Indicates the IP netmask that the NAS should configure when the user is a router to a network. This attribute can appear in Access-Accept and Access-Request packets.

Framed-Routing (10)

Description

Indicates the routing method for the user, when the user is a router to the network. This attribute appears in Access-Accept packets. The values for this attribute are:

0 None

1 Send routing packets

2 Listen for routing packets

3 Send and listen for routing packets

Filter-Id (11)

Description

Indicates the name of the filter list for the user that resides on the NAS. The filter format and functionality is NAS specific. The DRAS server can send zero or more Filter-Id attributes in an Access-Accept packet.

Framed-MTU (12)

Description

Indicates the maximum transmission unit that the NAS should configure for the user, when a dial-up user and NAS do not negotiate this value (for example, using PPP). This attribute appears only in Access-Accept packets.

Framed-Compression (13)

Description

Indicates the type of compression protocol used on the link. This attribute appears in Access-Accept packets.

Values

1 Van Jacobsen TCP/IP header compression

2 IPX header compression

Callback-Number (19)

Description

Indicates the telephone number that the client calls after terminating the user session. This attribute is a printable ASCII string. Typically, it contains the characters that follow the ATDT modem command. This attribute can appear in Access-Request and Access-Accept packets.

Callback-Id (20)

Description

Indicates the name of a place that the NAS should call. The NAS must have a site-name translation database for this to work properly. This attribute appears in Access-Accept packets.

Framed-Route (22)

Description

Provides generic routing information that the NAS should configure for the user. This attribute is a readable ASCII string that you can use in an ADD ROUTE command. This attribute can appear multiple times in an Access-Accept packet.

IP Route Information

For IP routes, this attribute should contain a destination prefix in dotted quad form, optionally followed by a slash and a decimal specifier stating the number of high-order bits of the prefix that the NAS should use. This is followed by a space, a gateway address in dotted quad form, a space, and one or more metrics separated by spaces. If you omit the decimal specifier, the value defaults to 8 bits for a Class A Internet address, 16 bits for a Class B Internet address, and 24 bits for a Class C Internet address.

If the gateway address is 0.0.0.0, the NAS should use the user's Internet address as the gateway address.

Framed-IPX-Network (23)

Description

Provides IPX-specific routing information, such as the IPX network number that the client should configure for the user. If the value for this attribute is 0xFFFFFFFE, the NAS should select an IPX network for the user. Other values indicate that the NAS should use the specified value as the IPX network for the link to the user. This attribute appears in Access-Accept packets.

Framed-AppleTalk-Link (37)

Description

Indicates the AppleTalk network number that the NAS should use for the serial link to the user when the user is another AppleTalk router. This attribute appears only in Access-Accept packets.

Special Values

The value 0 indicates that the link is an unnumbered serial link.

A value of 1 to 65535 indicates that the NAS should assign the specified value to the serial line between the NAS and the user.

Framed-AppleTalk-Network (38)

Description

Indicates the AppleTalk network number that the NAS should probe to allocate an AppleTalk node for the user when the user is an AppleTalk router. Multiple instances of this attribute indicate that the NAS can probe using any of the specified network numbers. This attribute appears only in Access-Accept packets.

Not implemented in DNAS Version 2.0.

Special Values

The value 0 indicates that the NAS should assign a network for the user, using its default cable range.

A value of 1 to 65535 (inclusive) indicates that the NAS should probe the specified AppleTalk network to find an address for the user.

Framed-AppleTalk-Zone (39)

Description

Indicates the name of the AppleTalk default zone that the NAS should assign to the user. This attribute appears only in Access-Accept packets.

Interactive Session Attributes

Login-IP-Host (14)

Description

Specifies the Internet address of the host system to which the user automatically connects. This attribute can appear in Access-Request and Access-Accept packets.

Special Values

- A value of 255.255.255.255 indicates that the NAS should allow the user to select an address.
- A value of 0.0.0.0 indicates that the NAS should select the host to which the user connects.
- Other values indicate the address of a host to which the user connects.

Login-Service (15)

Description

Indicates the service that the NAS should use to connect the user to the login host. This attribute appears only in Access-Accept packets. The values for this attribute are:

0 Telnet

1 Rlogin

2 TCP Clear

3 Portmaster (proprietary)

4 LAT

Login-Port (16)

Description

When the Login-Service attribute is present, indicates the TCP or LAT port to which the NAS connects the user. This attribute appears only in Access-Accept packets.

Login-LAT-Service (34)

Description

Indicates the system with which the NAS connects the user with the LAT protocol. This attribute appears only when LAT is the specified Login-Service. It appears only in Access-Accept packets.

This attribute is useful when you have clustered systems (for example, a VAXcluster).

Login-LAT-Node (35)

Description

Indicates the node to which the NAS should connect the user with the LAT protocol. This attribute appears only when LAT is the specified Login-Service. It appears only in Access-Accept packets.

Login-LAT-Groups (36)

Description

A string that identifies LAT group codes that the user is authorized to use. This attribute appears only when LAT is the specified Login-Service. It appears only in Access-Accept packets.

Vendor-Specific Attributes

Vendor-Specific (26)

Description

Indicates a DIGITAL-specific attribute, prefixed by the assigned vendor ID (see the Assigned Numbers RFC 1700). This attribute can appear in all packets except for an Access-Reject packet.

Service-Permissions (1)

Description

Indicates the permissions that the DECserver remote access server should provide to the user in the NAS Prompt service. The values are:

- Dialout
- Dialback
- LAT
- Telnet
- SLIP
- PPP
- Privileged

Dialout-Number (2)

Description

A text string containing the telephone number the NAS uses for dial-out services. This attribute can appear multiple times.

Dialback-Number (3)

Description

A text string containing the telephone number that the NAS should for dial-back services. This attribute can appear multiple times.

Dialout-Service (4)

Description

The name of the dial service that the NAS should use for the user. This attribute can appear multiple times.

Index

Symbols

A

B

C

D

E

F

G

H

I

L

N

O

P

R

S

U

V

W