Nways Manager

Nways VPN Manager User’s Guide

GA27-4233-00

Nways Manager

Nways VPN Manager User's Guide

GA27-4233-00

Note

Before using this information and the product it supports, be sure to read the general information under “Appendix. Notices” on page 73.

First Edition (May 1999)

This edition applies to the IBM Nways VPN Manager,.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

Forms for readers’ comments appear at the back of this publication. If the forms have been removed, address your comments to:

Department CGFA
Design & Information Development
IBM Corporation
PO Box 12195
RESEARCH TRIANGLE PARK, NC 27709-9990
USA

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Chapter 1. Introduction

This chapter provides a brief description of the VPN Manager, lists the IBM hardware components that it supports, and lists the hardware and software requirements for using VPN Manager.

About VPN Manager

The Nways VPN Manager provides monitoring, event reporting, troubleshooting, operational control, and application launching functions for IBM's implementation of virtual private networks.

Hardware Support

Version 2.0 of the Nways VPN Manager provides monitoring and operational control for the VPN capabilities implemented in the following devices:

- IBM 2210 Nways Multiprotocol Router
- IBM 2212 Access Utility
- IBM 2216 Nways Multiaccess Connector
- IBM Network Utility

Hardware and Software Prerequisites

Nways VPN Manager requires either Nways Element Manager Version 2.0 for one of the following platforms:

- AIX
- HP-UX
- Windows NT

Because the minimum hardware requirements for Nways Element Manager exceed those for Nways VPN Manager, there are no additional hardware requirements.

Chapter 2. Introduction to VPNs

A *Virtual Private Network* (VPN) provides end users a means to securely transport information from an intranet across a public IP network such as the internet. A VPN may be made up of Layer-2 Tunnels, IPSec Tunnels and Policies. The Layer-2 Tunnels provide VPN capabilities for remote dial-in users. The IPSec Tunnels provide VPN capabilities for IP users. The Policies provide access control to resources.

This chapter provides an overview of:

- Layer-2 Tunneling
- IPSec Tunneling
- Policies

Layer-2 Tunneling

Layer-2 Tunneling protocols are capable of securely transporting private Point-to-Point Protocol (PPP) traffic across a public IP network. There are three Layer-2 Tunneling protocols which employ two network models. The three Layer-2 Tunneling protocols are the Layer-2 Tunneling Protocol (L2TP), the Layer-2 Forwarding (L2F) protocol and Point-to-Point Tunneling Protocol (PPTP). The two network models are Compulsory Tunneling and Voluntary Tunneling.

Terminology

A *Network Access Server* (NAS) is a device attached to a switched network fabric such as a *Public Switched Telephone Network* (PSTN) or an *Integrated Services Digital Network* (ISDN) and contains a Point-To-Point (PPP) end system. A NAS which is capable of initiating an L2TP tunnel is referred to as a *L2TP Access Concentrator* (LAC). The NAS is the initiator of incoming calls and receiver of outgoing calls. A Gateway is a device which is capable of PPP termination and handles the server side of the communications. A Gateway is also referred to as a *L2TP Network Server* (LNS). The Gateway is the initiator of outgoing calls and the receiver of incoming calls.

Compulsory Tunneling

Compulsory Tunneling allows dial-in Clients which do not have tunneling software enabled to start a PPP Session which is tunneled from the Network Access Server (NAS) to the Corporate Network. In this model, the PPP Session exists between the Client and the Gateway and the Tunnel exists between the NAS and the Gateway.

Voluntary Tunneling

Voluntary Tunneling, on the other hand, requires the dial-in Clients to be tunneling enabled. In this model the Client initially dials into its service provider to gain internet access. After the connection to the service provider is established, the Client creates a

Layer-2 Tunnel to the Gateway and then an end-to-end PPP Session over the newly established Tunnel. In this model, the PPP Session and Tunnel exist between the Client and the Gateway.

Layer-2 Tunneling Protocols

Layer-2 Tunneling uses the following protocols:

L2TP The Layer-2 Tunneling Protocol, is an Internet Engineering Task Force (IETF) standards-track protocol which evolved from Layer-2 Forwarding (L2F) protocol and the Point-to-Point Tunneling Protocol (PPTP). L2TP uses well-known UDP port 1701 for its initial tunnel control message handshake and has the ability to pick available UDP source ports on both sides of the connection. UDP is also used as the packet transport for tunneled PPP packets. L2TP utilizes both the Compulsory Tunneling and the Voluntary Tunneling network models.

L2F The Layer-2 Forwarding protocol, is an non-standards based Layer 2 Tunneling protocol which was originally implemented by Cisco Systems. It uses well-known UDP port 1701 (fixed) for transmission of tunnel and call control messages as well as for transporting tunneled PPP packets from NAS to gateway. L2F employs the Compulsory Tunneling model.

PPTP The Point-To-Point Tunneling Protocol, is another non-standards based Layer 2 Tunneling protocol which was originally implemented by Microsoft on its Windows 95 and Windows NT platforms. PPTP uses TCP to open both tunnel and session control structures. After session establishment, PPP packets are tunneled using Generic Routing Encapsulation (GRE) . PPTP employs the Voluntary Tunneling network model.

Layer-2 Tunneling Capabilities

The Layer-2 Tunneling protocols can directly or indirectly provide authentication, encryption, and compression.

The Layer-2 Tunneling protocols can directly provide Tunnel Authentication and indirectly provide User Authentication. Tunnel Authentication is performed between the NAS and the gateway. User Authentication is performed by the underlying Point-to-Point Protocol.

The Layer-2 Tunneling protocols can indirectly provide data Encryption. All of the Layer-2 Tunneling protocols can transport data encrypted at the application layer. L2TP can be used with IPSec which can perform data Encryption. PPTP can use the Microsoft Point-to-Point Encryption (MPPE) facility.

The Layer-2 Tunneling protocols can indirectly provide data Compression. The Layer-2 Tunneling protocols accomplish this by use of the underlying Point-to-Point Protocol which has a data Compression capability.

IPSec Tunneling

IPSec is an Internet Engineering Task Force (IETF) standard which defines a tunnel mechanism to securely transport IP traffic across a public IP network. IPSec Tunnels are implemented using a pair of tunnels. There is an IPSec Key Management and an IPSec Data Management Tunnel. An IPSec Key Management Tunnel is often referred to as a Phase-1 Tunnel or an Internet Key Exchange (IKE) Tunnel and is a Control Tunnel for one or more follow-on IPSec Phase-2 User-Data Tunnels. IPSec Tunnels are commonly implemented in either an End-To-End or Gateway-To-Gateway network model.

Terminology

Authentication is the property of knowing the data received is the same as the data that was sent and the claimed sender is in fact the actual sender. The IPSec Authentication Method can be either a manually entered Pre-Shared Key or a Digital Signature. In addition to authentication, Digital Signatures guarantees that the message is uniquely associated with sender and unforgeable by the recipient. Message Digest 5 (MD5: 128 bit hashing) and the Secure Hash Algorithm (SHA: 160 bit hashing) are the commonly used in the IPSec Tunnel authentication scheme.

Integrity is the property of ensuring that data is transmitted from the source to the destination without undetected alteration. Hashed Message Authentication Code Message Digest 5 (HMAC-MD5: 2x128 bit hashing) and the Hashed Message Authentication Code Message Secure Hash Algorithm (HMAC-SHA: 2x160 bit hashing) are the commonly used in the IPSec integrity scheme.

Confidentiality is the property of communicating such that the intended recipients know what was sent but unintended parties cannot determine what was sent. Encapsulation and Encryption are used by IPSec to provide Confidentiality. The original IP data packet is encapsulated in an IPSec data packet. The original IP Header and Payload are encapsulated in Tunnel Mode which is typically used by Gateways. In contrast, only the original Payload is encapsulated Transport Mode which is typically used by Hosts. Data Encryption Standard (DES - 56 bit encryption), Triple Data Encryption Standard (DES-3 - 3x56 bit encryption) and the Commercial Data Masking Facility (CMDF - 40 bit encryption) are commonly used in the IPSec encryption scheme. .

A *Security Association* (SA) is a relationship between a given set of network connections that establishes a set of shared security information. Security Associations are negotiated based on secret keys, cryptographic algorithms, authentication algorithms and encapsulation modes. The Diffie-Hellman key agreement protocol (Group-1: 768 bit keying, Group-2: 1024 bit keying) is used by IKE to generate a Shared Secret, i.e. key, between the two IPSec entities. It should be noted that IKE was formerly known as ISAKMP/Oakley (Internet Security Association and Key Management protocol slash Oakley Protocol). The duration of an SA is specified by a Lifetime (duration in seconds) or a Lifesize (duration in Kbytes)

End-to-End Tunneling

End-To-End IPSec Tunneling allows an IP Host at one end of the network to securely communicate with an IP Host at the other end of the network. This model is similar to a specific Peer-To-Peer model and requires both IP Hosts to be IPSec enabled. The IPSec Tunnel is made of one Key Management Tunnel and one Data Management Tunnel between the two IP Hosts.

Gateway-to-Gateway Tunneling

Gateway-To-Gateway IPSec Tunneling allows one or more IP Hosts at one end of the network to securely communicate with one or more IP Hosts at the other end of the network. This model is similar to an Any-To-Any model in which the Gateways must be IPSec enabled but none of the IP Hosts needed to be IPSec enabled. The IPSec Tunnel is made of one Key Management Tunnel and one or more Data Management Tunnels between the two Gateways. The Gateways connect over their Public Interface and protect one or Private Interfaces behind them. A Private Interface may be an IP Subnet, range of IP addresses or a single IP address.

Key Management

An IPSec Key Management Tunnel is often referred to as an Internet Key Exchange (IKE) Tunnel or an IPSec Phase-1 Tunnel and is a Control Tunnel for one or more follow-on IPSec Phase-2 User-Data Tunnels. The IPSec Key Management Tunnel is negotiated in either Main Mode which utilitizes a six message exchange or Aggressive Mode which utilitizes a three message exchange. The negotiation entails authenticating the entities, establishing a Shared Secret and establishing parameters for the Security Association. After the successful completion of the negotiation, the IPSec Key Management Tunnel uses a single bi-directional Security Association (SA) for communication. Throughout the lifetime of a given IPSec Key Management Tunnel, the SA may expire and a new one created.

Data Management

An IPSec Data Management Tunnel is often referred to as an IPSec Phase-2 User-Data Tunnel or an IPSec Tunnel and is used to securely transport IP traffic. The IPSec Data Management Tunnel is negotiated in Quick Mode which utilizes a three message exchange. The negotiation entails exchanging identities, deciding whether or not to enforce Replay Prevention, generating a key if Perfect Forward Secrecy is required, agreeing on the future handling of the Don’t Copy Fragment Bit and establishing parameters for the Security Association(s). The security parameters may consist of Authentication Header (AH) and/or Encapsulating Security Payload (ESP) processing attributes. While both AH and ESP provide packet integrity and data origin authentication, only ESP provides encryption. The IPSec Data Management Tunnels use one or more inbound SAs and one or outbound SAs. Throughout the lifetime of a given IPSec Data Management Tunnel, the SA(s) may expire and a new one(s) created. During this switch-over period, there are actually two SAs (one with a status of CURRENT and one with a status of EXPIRING) for each original inbound SA.

IPSec Tunneling Capabilities

IPSec Tunneling can directly provide authentication, encryption, and integrity.

Authentication is performed on a tunnel basis and optionally on a packet basis. Tunnel authentication is performed by the IKE peers using either a Pre-Shared Key or a Digital Signature.

Packet authentication can be done by either the AH or ESP processing using either the HMAC-MD5 or HMAC-SHA algorithm. Encryption is optionally performed on a packet basis by the ESP processing. Packet encryption employs either the DES, DES-3 or CMDF algorithm.

Integrity is optionally performed on a packet basis. Integrity can be done by either the AH or ESP processing and employs either the HMAC-MD5 or HMAC-SHA algorithm.

Policies

A Policy consists of a Profile and an Action. The Profile defines a set of attributes for the Source and Destination of an connection. The Action is actually a set of actions or sub-policies which are used for IPSec Key Management, IPSec Data Management, Differentiated Services and RSVP. When a connection is to be established, the Defined Policy Profiles are searched for a match. If a Profile match is found, Action Proposals are exchanged. If the Proposal Phase ends successfully the connection is established and a Current Instance of the Defined Policy is created. Multiple Policy Instances may be created from a single Defined Policy.

Policy Component Relationships

A VPN Policy must contain a Policy Condition consisting of a Validity Period and a Traffic Profile and at least one Policy Action. The Validity Period component definition may be used in multiple Policies as it does not contain any device specific information. The Traffic Profile component definition is unique to the Policy as it contains device specific IP Address information. The Key Management Action and Key Management Proposal component definitions of the IPSec Action may be used in multiple Policies as neither contains any device specific information. The Data Management Action component definition of the IPSec Action is unique to the Policy as it contains device specific IP Address information. The Data Management Action, Data Management Proposal, Authentication Header (AH) Transform and Encapsulated Security Payload (ESP) Transform component definitions of the IPSec Action may be in multiple Policies as none of them contain device specific information. The Differential Services Action and the RSVP Action component definitions may be used in multiple Policies as neither contains any device specific information. The following table illustrates the relationships of the components of a VPN Policy.

Policy Component	Relationship
Policy Conditions	Policy must contain a validity period and a traffic profile
Validity Period	Can be shared by multiple policies
Traffic Profile	Unique to policy with the exception of the All-Traffic Profile
Policy Actions	Policy must contain at least one action
IPSec Action	Must contain a key and a data mangement action
Key Management (KM) Action	Can be shared by multiple policies
Key Management (KM) Proposal	Can be shared by multiple Key Management Actions
Data Management (DM) Action	Unique to policy (Contains IP address information)
Data Management (DM) Proposal	Can be shared by multiple Data Management Actions
AH Transform	Can be shared by multiple Data Management Proposals
ESP Transform	Can be shared by multiple Data Management Proposals
Differential Services Action	Can be shared by multiple policies
RSVP Action	Can be shared by multiple policies

LDAP

The *Light Weight Directory Access Protocol* (LDAP) is an internet directory standard which evolved from the X.500 Directory Access Protocol (DAP) and is capable of providing client devices open access to directory servers on the intranet/internet. The protocol provides this capability by passing text-based exchanges based on a schema between a client and a server over TCP/IP. One or more schemas may be supported by the Client and the Server with each schema used to define a collection of related objects.

The Directory-Enabled Networking Initiative (DEN) has identified LDAP in its specification as the mechanism which will be used to access information. DEN began in 1997 and is currently supported by a variety of vendors such as IBM, Microsoft, Cisco Systems and Netscape. The objective is to provide an information model specification for an integrated directory that stores information about people, network devices and applications. Within the networking industry, DEN is currently viewed as a key piece to building intelligent networks, where products from multiple vendors can store and retrieve topology and configuration related data from an LDAP Server.

From a VPN perspective, a Policy Configuration Application and the VPN Devices are LDAP Clients which communicate with an LDAP Server. The Policy Configuration Application interacts with LDAP Server to create, update and delete VPN Policies. The VPN Devices interact with the LDAP Server to retrieve it’s VPN Policies. The exchanges between the LDAP Clients and LDAP Server are based on a Policy Schema which defines the objects or data which are used to represent a VPN Policy.

Device Interactions

The Policy Configuration Application is used to define VPN Policies for all VPN Devices. The VPN Policies are stored in an LDAP Server and subsequently downloaded to the VPN Devices during initialization, upon request from the Policy Configuration Application or upon request from a VPN Monitor Application.

Chapter 3. Using VPN List Manager

This chapter contains the following sections:

- About the VPN List
- The VPN List Manager Information Panel
- The VPN Device List

About the VPN List

The Nways VPN List allows you to view a list of devices that are being maintained by a Nways service called the VPN List Manager. This service receives devices from users of this application and from the NetView and OpenView Databases. To be added to the list from NetView or OpenView devices must pass a filtering test that verifies that the device supports Virtual Private Networking as implemented by IBM. You can use this application to add devices to the list by adding devices to a user list of devices that all clients of the VPN List Manager have access to. This is useful for devices that are unknown to NetView and OpenView or that do not pass the filter test as implemented in this release of the VPN List Manager.

This application allows user control of the VPN List Manager. You can reset the VPN List Manager's list or have it add to the list by accessing your manual added list or by checking the NetView or OpenView database for new devices that may have changed. A device's ability to pass the filter test can change due to software upgrades since it was first tested by the filter.

The application presents you with a list of devices in tabular form that allows scrolling, searching, and sorting. By clicking on a device in the list, you can see more details about the device and launch the VPN Monitor application to see specific VPN information on this device.

About the VPN List Manager Information Panel

This panel contains the following sections:

- Information
- Log File Settings
- Reset VPN Manager List
- Password
- Change Password

To position a section in the viewable area of the panel, single-click on the name of the section in the selection list on the left side of the panel.

Control Action Priorities

The VPN List Manager will only perform one action at a time from this panel. If multiple changes are requested on this panel, the VPN List Manager will use the following hierarchy to determine which of the actions to perform:

1. Password change
2. Logging status change
3. Reset list

Information

This section contains the following fields:

VPN List Manager Host Name:
The hostname of the system where the VPN List Manager is running.

VPN List Manager IP Address:
The IP address of the system where the VPN List Manager is running.

VPN List Manager Version:
The version of VPN List Manager that is running.

VPN List Started on:
The time and date that the VPN List Manager was started.

Current Time on VPN List Manager:
The current time and date being on the system that the VPN List Manager is running on.

Number of Devices:
The current number of devices in the list that the VPN List Manager is maintaining.

Compare this number to the number of devices being used by this client. If the numbers are not the same, use the **Refresh** button on the VPN Device List Panel to refresh the client list from the VPN List Manager.

Number of Clients:
The number of clients that have registered with the VPN List Manager to receive update notices when the list changes. Changes can be from other clients or the result of the VPN List Manager being notified by the OpenView or Netview that a new device has been discovered or added.

This Client Notify Status:
Indicates whether this client will receive updates from the VPN List Manager when the list changes.

Clients register for updates when the VPN Manager Application is initialized. The status should be *enabled*. If the status is not *enabled*, this indicates a problem in the connection to the VPN List Manager. Try viewing the VPN Device List Panel again and returning to the VPN List Manager Control Panel to see if the status has changed.

Log File Settings

This section contains the following fields:

Current Logging Status:
Indicates whether the VPN List Manager is logging its activities to a file. Changing this status requires users to enter the current password and click **Apply** to activate the change.

If the log file is being created, it is named vpnlist.log, and is located with the other Nways Manager log files.

Reset List

This section contains the following fields:

Current System Device Status:
Indicates whether the VPN List Manager was able to access the NetView or OpenView (system) database of devices that the List Manager maintains.

Possible values are:

Failed to Load
Indicates that the VPN List Manager was unable to contact the system database, and therefore unable to load the device list.

Unknown
Indicates that the VPN List Manager does not know the status of the system database. This indicates a problem with the VPN List Manager.

Loaded
The normal state, indicating that the system has responded to the VPN List Manager’s request for devices. This indicates that the VPN List Manager has successfully added any devices that are VPN capable to its list.

Waiting for System to Respond
Indicates that the VPN List Manager has not yet added any devices from the system database. The system is still gathering device information from the network and will pass the device information to the VPN List Manager when that task is completed.

Loading in progress...
Indicates that the system is currently passing information on devices to the VPN List Manager.

Current User Device Status
Indicates the status of devices that users have manually added to the VPN List Manager.

Possible values are:

Failed to Load
Indicates that the VPN List Manager was unable to load the specified user file. This indicates a problem with the user file.

Unknown
Indicates that the VPN List Manager does not know the status of the user file. This indicates a problem with the VPN List Manager.

Loaded
This is the normal state once the user file has been read by the VPN List Manager. This indicates that the VPN List Manager has successfully added the devices in the user file to its list of devices.

Loading in progress...
Indicates that the VPN List Manager is currently reading the user file.

Reset List
Allows you to refresh or add to the current list of devices. To reset the list, you must enter the current password. Click **Apply** to reset the list with the selected reset type.

Password

This section contains the following field:

Current Password:
Users must enter a valid password to have the VPN List Manager make changes to device lists. Changes to the VPN List Manager's device lists affect other clients using this VPN List Manager and should be made with care.

The default password is **OK**.

Change Password

This section contains the following fields:

Change Password
This action requires you to enter the current password. You must enter the new password twice for confirmation. After you have entered the new password, click **Apply** to change the current password.

About the VPN Device List Panel

The VPN Device List Panel contains the following sections:

- Devices
- Details
- Print

Devices

This section contains the following fields and buttons:

Device Table

The device table displays information about the devices in the current VPN List Manager device list in a tabular format that allows you to search for information, scroll through information, and select individual devices.

Selecting a row in the table by clicking it while the pointer is over data in the row updates other information displayed in the panel to reflect the selected row.

Selecting a column in the table sorts the table in ascending or descending order based on the data in the column selected.

Double clicking on a row performs the same function as the **Monitor** button, launching the VPN Monitor Application for the device.

The table displays the following columns:

Device Name

The name given to the device by the user or the network management platform.

IP Address

The IP address of the device

Device Type

The device type of this device.

Search Fields

The search fields use the asterisk (*) as a wild card character. The wild card can be used at the beginning of a field, the end, or both. The wild card cannot be used within the search string. You can search for devices by device name, IP address, or both.

Device Name

The name to search for.

IP Address

The IP address to search for.

Search Button

Executes a search using the information from the top row of the current list view.

Search Next Button

Executes a search using the information entered on the row after the currently selected row in the current list view.

Details

This section contains the following fields and buttons:

Total Number of Devices in List:

Indicates the total number of devices in the currently displayed list.

Device Name:

The user-defined name of the current device.

IP Address:
The IP address of the current device.

Read Community Name:
The SNMP Read access community name for the current device. The device can have multiple access levels for read and write. This is the name associated with read-only access.

Write Community Name:
The SNMP Write access community name for the current device. The device can have multiple access levels for read and write. This is the name associated with read-write access.

Device Type:
The device type of the current device.

Add Button:
Clicking this button adds new devices to the list using the information entered.

Change Button:
Changes attributes of devices that have been manually added to the list. Use the system management platform to make changes to devices that have been added to the list by the system.

Delete Button:
Deletes devices that have been manually added to the list. Use the system management platform to delete devices added by the system.

Monitor Button:
Launches the VPN Monitor application on the current device.

Print

This section allows you to print the information displayed in the list. You can enter header and footer text that will be included on each printed page.

This section displays the following fields and buttons:

Header:
Enter header text to be printed at the top of each page.

Footer:
Enter footer text to be printed at the bottom of each page.

Print Button
Pressing this button displays a printer selection list. Select a printer to have the output formatted for the correct printer type.

Note: If no printer is defined on the system, the print function will be unable to format the device list, and will return to the VPN Device List Panel and respond with the message:

```
Print Cancelled
```

Chapter 4. VPN Monitor

The VPN Monitor gives you monitoring, event reporting, troubleshooting, operational control, and application launching functions for VPN-capable devices in your network, and for VPNs using those devices.

This section includes information on the VPN Manager Window. It contains the following sections:

- The VPN Monitor window
- VPN Monitor Functions

VPN Monitor Window

The VPN Monitor Window has three parts:

- Navigation Tree
- Information Panel
- Message Area

Navigation Tree Panel

The navigation tree is a hierarchical structure that enables you to view the range of management information about the managed device.

Icons

The navigation tree uses several icons to represent monitored resources:

Folder A higher level resource that represents one or more dependent items. The folder at the top of the tree, for example, usually represents the device itself. Other folders at subsequent levels might represent configuration information or fault information.

Within each folder are items that make up part of the overall folder of information. The status indicated for a folder is calculated from the statuses of immediate dependent items. Click on the plus (+) next to a folder to see and take action on the items within the folder.

Page A dependent resource that consists of information only, such as configuration information. This resource may or may not allow user changes, depending on the item, the device being managed, and the access rights of the user.

Navigating

Expand folders by clicking the plus (+) next to the icon to display dependent items.

Collapse folders by clicking the minus (−) next to the icon to hide dependent items.

Information Panel

The Information panel displays information about the function selected in the Navigation tree panel. From this panel you can perform all of the functions of the VPN Monitor.

Message Area

The Message Area displays status information from the VPN Monitor application.

VPN Monitor Functions

The VPN Monitor provides the following functions:

- Monitoring
- Event Reporting
- Operational Control
- Troubleshooting
- Launching Applications

This rest of this section describes how to use these functions to manage your VPN and the location of the functions in the navigation tree.

Monitoring

The VPN Monitor displays information about multiple facets of your network, including tunnels, clients, and policies. The Chapter 6. VPN Monitor Global Status Folder provides general information about the status of the elements of your VPN network. To view more information, use the Chapter 7. VPN Monitor Tunnels Folder, theChapter 8. VPN Monitor Clients Folder, the Chapter 10. VPN Monitor Policies Folder, and the Chapter 9. VPN Monitor Quality of Service Folder.

These folders give you important information about the status of elements in your network.

Event Reporting

To provide additional information about your VPN, the VPN Monitor Application provides logs and counters of events that occur in your network. These are displayed in the Chapter 11. VPN Monitor Events Folder.

The Events folder displays event logs and counters for Layer-2 tunnel and session successes and failures, and for IPSec tunnel and encryption successes and failures.

Operational Control

The VPN Monitor Application also allows you to control tunnels, clients, and policies from your management workstation. Using the Chapter 12. VPN Monitor Operational Folder, you can enable or disable IPSec and Layer-2 tunnels, enable and disable clients, and refresh your policies.

Troubleshooting

You can track down connectivity problems in your network, the VPN Monitor Application provides a variety of tools in the Chapter 13. VPN Monitor Tests Folder to help you test potential connectivity, test the effects of new policies before implementing them in your network, and test the round trip time for a specified tunnel or to a specified host.

Launching Applications

The VPN Monitor Application gives you the ability to launch some applications to help you manage your network, including:

- Telnet
- The JMA of the monitored device
- MIB Browser
- Your Web Browser

Chapter 5. VPN Monitor General Folder

The VPN Monitor General folder provides information on VPN Devices in your network. It contains two dependent items:

- Identification
- Administration

Identification

The Identification panel provides general information describing the selected VPN device. It contains the following fields, which contain information retrieved from the device's MIB.

Description
A description of the device.

Device ID
The system object identifier (SYSOID) for the device.

Contact
The contact information contained in the device's MIB. Authorized users can modify this information from the Identification panel.

Domain Name
The IP domain name used by the device. Authorized users can modify this information from the Identification panel.

Location
The location information for the device. Authorized users can modify this information from the Identification panel.

Up Time
The length of time since the device was last started or restarted.

System Services
A number representing the capabilities of the device.

System Service Functions
A text description of the capabilities represented by the System Services number.

Administration

The Administration panel displays the SNMP parameters that VPN Monitor uses to communicate with the device. Authorized users can modify this information from the Administration panel.

The Administration panel contains the following fields:

IP Address
The IP address used for SNMP requests

Community Name (Read)
The SNMP community name used for Read requests.

Community Name (Write)
The SNMP community name used for Write requests.

Remote Port
The port on the device used for SNMP requests.

Timeout (ms)
The timeout value, in milliseconds, used for SNMP requests.

Retries The number of retries used for SNMP requests.

Polling Interval
The polling interval, in milliseconds, used for SNMP requests.

Chapter 6. VPN Monitor Global Status Folder

The VPN Monitor Global Status folder provides a view of VPN processing on the selected device. It contains the following dependent items:

- At-A-Glance

At-A-Glance

The At-A-Glance panel provides summary information about VPN processing on the selected device. It contains the following sections:

- Levels
- Tunnels
- Clients
- Policy
- Events

Levels

The levels section provides information on the MIBs and protocol code being used by the device. It contains the following fields:

Layer-2 MIB Version
The version of the Layer-2 MIB being used by the device.

Layer-2 Protocol Version
he version of the Layer-2 Protocol code being used by the device.

IPSec MIB Version
The version of the IPSec MIB being used by the device.

Policy MIB Version
The version of the Policy MIB being used by the device.

Tunnels

The Tunnels section provides information on the number of currently active Layer-2 and IPSec tunnels on this device.

Clients

The Clients section displays the number of currently active Layer-2 sessions on this device.

Policy

The Policy section provides information on the VPN policy currently being used by the device. It contains the following fields:

Policy Up Time
The up time of the current Policy component code.

Device Up Time
The up time of the device.

Device Current Time
The current time being used by the device.

Hours from UTC
The difference in the time being used by the device and the current Coordinated Universal Time (UTC).

Current Config Source
The source for the current Policy configuration.

Policy Load Status
The results from the last attempt to lad a Policy.

Events

The Events section provides information on events monitored by the VPN Monitor for this device. It contains the following fields:

Layer-2 Tunnel Successes
The number of Layer-2 tunnels successfully activated for this device.

Layer-2 Tunnel Failures
The number of Layer-2 tunnels for this device for which an attempt was made to activate, but was unsuccessful.

Layer-2 Session Successes
The number of Layer-2 sessions successfully activated for this device.

Layer-2 Session Failures
The number of unsuccessful attempts to activate a Layer-2 session for this device.

IPSec In Authentications
The number of successful inbound IPSec authentications.

IPSec In Authentication Failures
The number of failed inbound IPSec authentications attempted.

IPSec In Decryptions
The number of inbound IPSec decryptions successfully performed.

IPSec In Decryption Failures
The number of failed inbound IPSec decryptions attempted.

IPSec Out Authentications
The number of successful outbound IPSec authentications.

IPSec Out Authentication Failures
The number of failed outbound IPSec authentications attempted.

IPSec Out Encryptions
The number of outbound IPSec encryptions successfully performed.

IPSec Out Encryption Failures
The number of failed outbound IPSec encryptions attempted.

Chapter 7. VPN Monitor Tunnels Folder

The VPN Monitor Tunnels folder contains information on the status of Layer-2 and IPSec tunnels used by the selected device. This folder has the following dependent items:

- Layer-2 Tunnels folder
- IPSec Tunnels folder

Layer-2 Tunnels Folder

The Layer-2 Tunnels folder provides information on active and previous Layer-2 tunnels on the selected device. It has the following dependent items:

- Active Tunnels panel
- Previous Tunnels panel

Active Folder

The Layer-2 Active Layer-2 Tunnels folder provides information for all active Layer-2 tunnels associated with the selected device. It has the following dependent items:

- Status panel
- Attributes panel
- Statistics panel
- End-Points panel

Status Panel

The Status panel provides information on the status of active Layer-2 Tunnels associated with the selected device. It contains the following fields:

Tunnel The index number of the tunnel.

Status The status of the tunnel: active or destroy. Authorized users can change this value from the Status view.

Type The tunnel type: L2TP, L2F, or PPTP.

Remote Host
The name of the remote host associated with this tunnel

Active Time
The length of time the tunnel has been active.

Active Sessions
The number of active sessions associated with this tunnel.

Previous Sessions
The number of previously active sessions associated with this tunnel.

Destroy All Tunnels
The trigger to destroy all Layer-2 tunnels. Authorized users can change this value from the Status view.

Attributes Panel

The Attributes panel provides information on the attributes of a selected tunnel. It contains the following fields:

Local Control ID
The local control ID for the tunnel.

Peer Control ID
The peer control ID for the tunnel.

Control State
The control state of the tunnel.

Control Timouts
The number of control timeouts recorded for this tunnel.

Remote Host
The name of the remote host associated with this tunnel.

Remote Vendor Name
The name of the vendor of the remote host.

Remote Firmware Version
The version of firmware running on the remote host.

Remote Protocol Version
The protocol version being used by the remote host.

Init Connect
Indicates whether the tunnel was generated by the local host.

Local Receive Packet Window
The size of the receive packet window being used by the local host.

Remote Receive Packet Window
The size of the receive packet window being used by the remote host.

Next Send Sequence
The value of the next send sequence number.

Next Receive Sequence
The value of the next receive sequence number.

Statistics Panel

The Statistics panel provides statistics about the specified Layer-2 tunnel. It contains the following fields:

In Bytes
The number of bytes received over this tunnel.

In Packets
The number of packets received over this tunnel.

In Discarded Packets
The number of packets discarded during reception over this tunnel.

Out Bytes
The number of bytes sent over this tunnel by the local host.

Out Packets
The number of packets sent over this tunnel by the local host.

Out Discarded Packets
The number of packets discarded during sending over this tunnel by the local host.

End Points Panel

The End Points panel provides information about the end point of a selected tunnel. It contains the following fields:

Remote IP Address
The remote IP address associated with the selected tunnel.

Local IP Address
The local IP address of the selected tunnel.

Source Port
The port on the local host associated with this tunnel.

Destination Port
The port on the remote host associated with this tunnel.

Previous Tunnels Folder

The Previous Layer-2 Tunnels folder provides summary and statistics information for specified previous Layer-2 tunnels associated with the selected device. The number of previous entries for which information is displayed can be specified from the Summary panel. The Previous Layer-2 Tunnels folder has the following dependent items:

- Summary panel
- Statistics panel

Summary Panel

The summary panel provides information on a selected previously active Layer-2 tunnel. It contains the following fields:

Order The order in which the tunnel ended.

Tunnel The index of the tunnel.

Type The tunnel type: L2TP, L2F, PPTP.

Remote Host
The name of the remote host associated with the tunnel.

Remote IP Address
The remote IP address associated with the tunnel.

Remote Port
The remote port associated with the tunnel.

Local IP Address
The local IP address associated with the tunnel.

Local Port
The local port associated with the tunnel.

Total Sessions
The total number of active sessions that used the tunnel.

Tunnel Up Time
The length of time that the tunnel was active.

Statistics Panel

The statistics panel provides information about the use of a previous tunnel. It contains the following fields:

In Bytes
The number of bytes received by the monitored device over this tunnel.

In Packets
The number of packets received by the monitored device over this tunnel.

In Discarded Packets
The number of packets discarded during reception over this tunnel by the monitored device.

Out Bytes
The number of bytes sent over this tunnel by the monitored device.

Out Packets
The number of packets sent over this tunnel by the monitored device.

Out Discarded Packets
The number of packets discarded by the monitored device during sending over this tunnel.

IPSec Tunnels Folder

The IPSec Control Tunnels folder provides information on active and previous IPSec tunnels on the selected device. It has the following dependent items:

- Active Tunnels folder
- Previous Tunnels folder

Active Tunnels Folder

The IPSec Active Tunnels folder provides information on active IPSec control and user-data tunnels. It has the following dependent items:

- IPSec Control Tunnels folder
- IPSec User-Data Tunnels folder

IPSec Control Tunnels Folder

The IPSec Control Tunnels folder provides information about active IPSec control tunnels associated with the selected device. It contains the following panels:

- Status
- Attributes
- Statistics
- Processing

Status: The Status panel provides information on the Status of a selected IPSec control tunnel. It contains the following fields:

Tunnel The index number of the selected tunnel.

Status The status of the tunnel: active or destroy. Authorized users can change this value from the Status panel.

ID The ID of the selected tunnel.

Remote Name
The remote name of the tunnel.

Remote Address
The remote IP address of the tunnel.

Local Name
The local name of the tunnel.

Local Address
The local IP address of the tunnel.

Up Time
The length of time the tunnel has been active.

Destroy All Tunnels
The trigger to destroy all active IPSec control tunnels. Authorized users can change this value from the Status panel.

Attributes: The Attributes panel provides information on the attributes of the selected IPSec control tunnel. It contains the following fields:

Negotiation Mode
The mode being used by the selected IPSec control tunnel to negotiate new connections with remote hosts.

SA Lifetime
The Security Association lifetime of the tunnel in seconds.

SA Refresh Threshold Percent
The Security Association refresh threshold percent.

Total SA Refreshes
The number of Security Association refreshes performed.

Statistics: This panel provides statistics about the selected IPSec control tunnel. It contains the following fields:

In Bytes
The number of bytes received by the monitored device over this tunnel.

In Packets
The number of packets received by the monitored device over this tunnel.

In Dropped Packets
The number of packets discarded during reception over this tunnel by the monitored device.

Out Bytes
The number of bytes sent over this tunnel by the monitored device.

Out Packets
The number of packets sent over this tunnel by the monitored device.

Out Dropped Packets
The number of packets discarded by the monitored device during sending over this tunnel.

Processing: This panel provides information on processing related to the selected IPSec control tunnel. It contains the following fields:

In Notifys
The number of notifys received over this tunnel.

In Proposals
The number of proposals received over this tunnel.

In Invalid Proposals
The number of proposals received over this tunnel that were invalid.

In Rejected Proposals
The number of proposals received over this tunnel that were rejected.

In SA Deletes
The number of security association deletes received over this tunnel.

Out Notifys
The number of notifys sent over this tunnel.

Out Proposals
The number of proposals sent over this tunnel.

Out Invalid Proposals
The number of proposals sent over this tunnel that were invalid.

Out Rejected Proposals
The number of proposals sent over this tunnel that were rejected.

Out SA Deletes
The number of security association deletes sent over this tunnel.

Active IPSec User-Data Tunnels Folder

This folder provides information about active IPSec user-data tunnels associated with the selected device. It has the following dependent items:

- Status panel
- Attributes panel
- Statistics panel
- End Points panel
- Security Protection Indices Panel

Status Panel: This panel provides information on the status of the selected IPSec user-data tunnel. It contains the following fields:

Tunnel The index number of the selected tunnel.

Status The status of the selected tunnel: active or destroy. Authorized users can change this value from the Status panel.

Remote IP Address
The remote IP address of the tunnel.

Local IP Address
The local IP address of the tunnel.

Up Time
The length of time the tunnel has been active.

Total Security Association Refreshes
The total number of security association refreshes performed.

Current Security Associations
The number of current security associations.

Expired Security Associations
The number of expired security associations.

Destroy All Tunnels
The trigger to destroy all active IPSec user-data tunnels. Authorized users can change this value from the Status panel.

Attributes Panel: This panel provides information on the attributes of the selected IPSec user-data tunnel. It contains the following fields:

ID The index number of the tunnel.

Control Tunnel
The index number of the IPSec control tunnel associated with this IPSec user-data tunnel.

Key Type
The key type of the tunnel.

Encapsulation Mode
The encapsulation mode of the tunnel.

Security Association Lifetime
The security association lifetime of the tunnel in seconds.

Security Association Refresh Threshold Percent
The security association refresh threshold percent.

In SA Encryption
The inbound encryption type in use for this tunnel.

In SA Authentication
The inbound authentication algorithm in use for this tunnel.

Out SA Encryption
The outbound encryption type in use for this tunnel.

Out SA Authentication
The outbound authentication algorithm in use for this tunnel.

Statistics Panel: This panel provides usage statistics for the selected IPSec user-data tunnel. It contains the following fields:

In Bytes
The number of bytes received over this tunnel.

In Byte Counter Wraps
The number of times the in byte counter has wrapped.

In Decompressed Bytes
The number of decompressed bytes received over this tunnel.

In Decompressed Byte Wraps
The number of times the in decompressed byte counter has wrapped.

In Packets
The number of packets received over this tunnel.

In Dropped Packets
The number of packets dropped during reception over this tunnel.

In Authentications
The number of inbound authentications performed for this tunnel.

In Authentication Failures
The number of inbound authentications performed for this tunnel that were unsuccessful.

In Decryptions
The number of inbound decryptions performed for this tunnel.

In Decryption Failures
The number of inbound decryptions performed for this tunnel that were unsuccessful.

Out Bytes
The number of bytes sent over this tunnel.

Out Byte Counter Wraps
The number of times the out byte counter has wrapped.

Out Decompressed Bytes
The number of decompressed bytes sent over this tunnel.

Out Decompressed Byte Wraps
The number of times the out decompressed byte counter has wrapped.

Out Packets
The number of packets sent over this tunnel.

Out Dropped Packets
The number of packets dropped during transmission over this tunnel.

Out Authentications
The number of outbound authentications performed for this tunnel.

Out Authentication Failures
The number of outbound authentications performed for this tunnel that were unsuccessful.

Out Encryptions
The number of outbound encryptions performed for this tunnel.

Out Encryption Failures
The number of outbound encryptions performed for this tunnel that were unsuccessful.

End Points Panel: This panel provides information on the end points of the selected tunnel. It contains the following fields:

Local Name
The local name of the tunnel.

Local Type
The local addressing type: subnet or range.

Local Protocol
The local protocol of the tunnel.

Local Subnet Mask
The local subnet mask used for the tunnel.

Local Low IP Address
The local low IP address for the tunnel.

Local High IP Address
The local high IP address for the tunnel.

Local Port
The local port used by the tunnel.

Remote Name
The remote name of the tunnel.

Remote Type
The remote addressing type: subnet or range.

Remote Protocol
The remote protocol of the tunnel.

Remote Subnet Mask
The remote subnet mask used for the tunnel.

Remote Low IP Address
The remote low IP address for the tunnel.

Remote High IP Address
The remote high IP address for the tunnel.

Remote Port
The remote port used by the tunnel.

Security Protection Indices Panel: This panel provides information about the security protection index (SPI) being used by the tunnel. It contains the following fields:

SPI The security protection index being used by the tunnel.

Direction
The direction of traffic to which the SPI is being applied: in or out.

Value The value of the SPI.

Protocol
The protocol used by the SPI.

Previous IPSec User-Data Tunnels Folder

This folder provides information on IPSec user-data tunnels that are no longer active. It contains the following panels:

- Summary panel
- Statistics panel

Summary Panel: This panel provides summary information about previous IPSec user-data tunnels. It contains the following fields:

Order The order in which the tunnel ended.

ID The ID of the tunnel.

Remote IP Address
The remote IP address used by the tunnel.

Local IP Address
The local IP address used by the tunnel.

Up Time
The length of time the tunnel was active.

Total SA Refreshes
The number of security association refreshes performed for this tunnel.

Total SAs
The total number of security associations for this tunnel.

Statistics Panel: This panel provides usage statistics for a selected, previously-active IPSec user-data tunnel. It contains the following fields:

In Bytes
The number of bytes received over this tunnel.

In Byte Counter Wraps
The number of times the in byte counter has wrapped.

In Decompressed Bytes
The number of decompressed bytes received over this tunnel.

In Decompressed Byte Wraps
The number of times the in decompressed byte counter has wrapped.

In Packets
The number of packets received over this tunnel.

In Dropped Packets
The number of packets dropped during reception over this tunnel.

In Authentications
The number of inbound authentications performed for this tunnel.

In Authentication Failures
The number of inbound authentications performed for this tunnel that were unsuccessful.

In Decryptions
The number of inbound decryptions performed for this tunnel.

In Decryption Failures
The number of inbound decryptions performed for this tunnel that were unsuccessful.

Out Bytes
The number of bytes sent over this tunnel.

Out Byte Counter Wraps
The number of times the out byte counter has wrapped.

Out Decompressed Bytes
The number of decompressed bytes sent over this tunnel.

Out Decompressed Byte Wraps
The number of times the out decompressed byte counter has wrapped.

Out Packets
The number of packets sent over this tunnel.

Out Dropped Packets
The number of packets dropped during transmission over this tunnel.

Out Authentications
The number of outbound authentications performed for this tunnel.

Out Authentication Failures
The number of outbound authentications performed for this tunnel that were unsuccessful.

Out Encryptions
The number of outbound encryptions performed for this tunnel.

Out Encryption Failures
The number of outbound encryptions performed for this tunnel that were unsuccessful.

Chapter 8. VPN Monitor Clients Folder

The VPN Monitor Clients folder provides information on Layer-2 sessions. It contains the following subfolders:

- Layer-2 Sessions

Layer-2 Sessions Folder

This folder provides information on Layer-2 sessions for the selected device. It contains the following subfolders:

- Active Sessions
- Previous Sessions

Active Sessions Folder

This folder provides information on active Layer-2 sessions for the selected device. It contains the following panels:

- Status
- Statistics

Status Folder

This folder provides status information about a selected Layer-2 session. It contains the following panels:

- Status
- Attributes
- Statistics

Status Panel: This panel provides information on the status of a selected Layer-2 session. It contains the following fields:

Tunnel The index of the tunnel used by the selected session.

Session
The index of the session.

Status The status of the session: active or destroy. Authorized users can change this value from the Status panel.

Session Up Time
The length of time the session has been active.

Connect BPS
The speed of the connection in bits per second.

Authentication Method
The authentication method used by this session.

Encryption/Decryption
The encryption/decryption indicator for this session. True indicates that encryption and decryption are in use for the session, False indicates that they are not.

Destroy All Sessions
The trigger to destroy all Layer-2 session. Authorized users can change this value from the Status panel.

Attributes Panel: This panel lists the attributes of the selected session. It contains the following fields:

Remote Name
The remote name of the session.

Line State
The line state of the session.

Local ID
The local ID of the session.

Remote ID
The remote ID of the session.

Device Number
The device number being used by the session.

Serial Number
The serial number of the device being used by the session.

Bearer Type
The bearer type being used by the session: digital or analog.

Framing Type
The framing type being used by the session: synchronous or asynchronous.

Local Packet Window
The size of the local packet window.

Remote Packet Window
The size of the remote packet window.

Timeouts
The number of timeouts that have occurred during this session.

Next Send Sequence
The value of the next send sequence number.

Next Receive Sequence
The value of the next receive sequence number.

Remote PPD
The length of the remote packet processing delay.

Statistics Panel: This panel provides statistical information for the selected Layer-2 session. It contains the following fields:

In Bytes
The number of bytes received.

In Uncompressed Bytes
The number of uncompressed bytes received.

In Packets
The number of packets received.

In Discarded Packets
The number of packets discarded during reception.

Out Bytes
The number of bytes sent.

Out Uncompressed Bytes
The number of uncompressed bytes sent.

Out Packets
The number of packets sent.

Out Discarded Packets
The number of packets discarded during sending.

Previous Layer-2 Sessions Folder

This folder provides information on previous Layer-2 sessions on the selected device. It contains the following dependent items:

- Summary Panel
- Statistics Panel

Summary Panel: This panel provides summary information about a selected Layer-2 session on the selected device. It contains the following fields:

Order The order in which the session ended.

Tunnel The index of the tunnel used by the session.

Session
The index of the previously active session.

Authentication Method
The authentication method used by the session.

Encryption/Decryption
The encryption/decryption indicator for the session. True indicates that encryption/decryption were used for the session, False indicates that they were not.

Up Time
The length of time the session was active.

Statistics Panel: This panel provides statistical information about a previously active Layer-2 session on the selected device. It contains the following fields:

In Bytes
The number of bytes received.

In Uncompressed Bytes
The number of uncompressed bytes received.

In Packets
The number of packets received.

In Discarded Packets
The number of packets discarded during reception.

Out Bytes
The number of bytes sent.

Out Uncompressed Bytes
The number of uncompressed bytes sent.

Out Packets
The number of packets sent.

Out Discarded Packets
The number of packets discarded during sending.

Chapter 9. VPN Monitor Quality of Service Folder

This folder provides information on the quality of service for a selected session using Resource Reservation Protocol (RSVP). It has the following depended item:

- RSVP

RSVP Folder

This folder contains information about the Resource Reservation Protocol (RSVP) in use for a selected session. It contains the following panels:

- Sessions
- Sender PATH Messages
- Upstream RESV Messages

Sessions Panel

This panel provides RSVP information for a selected session. It contains the following fields:

Session Index
The session index.

Session Type
The session type.

IP Protocol
The IP protocol used by the session.

Destination Address
The destination address of the session.

Destination Port
The destination port of the session.

Number of Senders
The number of senders in the session.

Number of RSVP Requests Received
The number of RSVP requests received by the selected device.

Number of RSVP Requests Sent
The number of RSVP requests sent by the selected device.

Sender PATH Messages Panel

This panel contains path information for the selected session. It has the following fields:

Session Index
The index of the session.

Sender Index
The index of the sender associated with this session.

Session Type
The type of session.

IP Protocol
The IP protocol of the session.

Destination Address
The destination address associated with this session.

Destination Port
The destination port associated with this session.

Source Address
The source address associated with this session.

Source Port
The source port associated with this session.

IPv6 Flow Identifier
The IPv6 flow identifier for this session.

Previous Hop Address
The IP address of the previous hop.

Previous Hop Logical Interface Handle
The logical interface handle of the previous hop.

Last Interface Index
The last interface index.

Average BPS
The average connection speed of this session, in bits per second.

Peak BPS
The peak connection speed of this session, in bits per second.

Maximum Expected Bytes
The maximum number of bytes expected over this connection.

Minimum Message Size
The minimum message size in use for this session.

Maximum Message Size
The maximum message size in use for this session.

Refresh Message Interval
The interval at which refresh messages are sent for this session.

Previous Hop Is RSVP
Indicates whether the previous hop was an RSVP hop.

Path Message Last Change
The time at which the path message changed last.

Policy The policy associated with this sender.

Last TTL Value
The last time-to-live value in use for this session.

Non-IS Hop Detected
Indicates whether a non-IS hop was detected for this session.

Hop Count
The hop count for this session.

Path Bandwidth
The patch bandwidth.

Minimum Path Latency
The minimum path latency.

Maximum Transmission Unit
The maximum transmission unit (MTU) size for this session.

Guaranteed Service
Indicates whether service is guaranteed for this session.

Break In Service
Indicates whether a break in service occurred for this session.

Hop Count Override
The hop count override for this session.

Path Bandwidth Override
The path bandwidth override for this session.

Minimum Path Latency Override
The minimum path latency override for this session.

Maximum Transmission Unit Override
The maximum transmission unit override for this session.

Upstream RESV Messages Panel

This panel provides information on upstream RESV messages for the selected session. It contains the following fields:

Session Index
The index of the session.

Request Index
The index of the request.

Session Type
The session type.

IP Protocol
The IP protocol in use for this session.

Destination Address
The destination address associated with this session.

Destination Port
The destination port associated with this session.

Source Address
The source address associated with this session.

Source Port
The source port associated with this session.

Previous Hop Address
The IP address of the previous hop.

Previous Hop Logical Interface Handle
The logical interface handle of the previous hop.

Last Interface Index
The last interface index.

Quality of Service
The quality of service classification requested for this session.

Average BPS
The average speed of this connection, in bits per second.

Peak BPS
The peak speed of this connection, in bits per second.

Maximum Expected Bytes
The maximum number of bytes expected over this connection.

Minimum Message Size
The minimum message size in use for this connection.

Maximum Message Size
The maximum message size in use for this connection.

Refresh Message Interval
The refresh message interval for this connection.

Scope The value of the scope object.

Shared Reservation
The shared reservation indicator.

Explicit Senders
The explicit senders indicator.

Next Hop Is RSVP Hop
Indicates whether the next hop is an RSVP hop.

Last Change
The time of the last change.

Policy The policy associated with this request.

Last TTL Value
The last time-to-live value received.

IPv6 Flow Identifier
The IPv6 flow identifier.

Chapter 10. VPN Monitor Policies Folder

This folder contains information on the policies used to govern VPN connections. It has the following dependent items:

- Device Folder
- Conditions Folder
- Actions Folder

Device Folder

The Device folder provides information on the policies created for a selected device. It contains the following panels:

- Policies
- Filter Rules
- Policy to Rule

The Device folder provides the same fields for all three views of policy information. They are:

Policy Name
The name of the policy.

Status
The status of the policy: enable or disable. Authorized users can change this value from the Policies panel.

Priority
The priority of the policy.

Validity
The validity indicator for the policy.

IPSec Manual ID
The IPSec Manual tunnel ID.

Matches
The number of matches for this policy.

Validity Period
The name of the validity period for this policy.

Traffic Profile
The name of the traffic profile for this policy.

Key Management Action
The name of the key management action for this policy.

Data Management Action
The name of the data management action for this policy.

Differential Services Action
The name of the differential services action for this policy.

RSVP Action
The name of the RSVP action for this policy.

Conditions Folder

The Policy Conditions folder provides information on validity periods and policy actions for a selected policy. It contains the following dependent items:

- Validity Periods Panel
- Traffic Profiles Folder

Validity Periods Panel

The Validity Periods panel provides a view of all validity period definitions. It contains the following fields:

Validity Period Name
The name of the validity period.

Start Date and Time
The starting date and time for the validity period.

End Date and Time
The ending date and time for the validity period.

Month Mask
The mask used to determine the months of the validity period.

Days Mask
The mask used to determine the days of the validity period.

Start Time of Day
The starting time of day for the validity period.

End Time of Day
The ending time of day for the validity period.

Traffic Profiles Folder

The Traffic Profiles folder provides information on the traffic profiles associated with a policy. It contains the following panels:

- Base Profiles
- Ingress/Egress Profiles
- Remote ID Profiles

Base Profiles Panel: The Base Profiles panel provides information on the base profiles associated with a policy. It contains the following fields:

Traffic Profile Name
The name of the traffic profile.

Low Protocol
The low protocol number.

High Protocol
The high protocol number.

Source Low IP Address
The low source IP address associated with this profile.

Source High IP Address
The high source IP address associated with this profile.

Source High Port
The high port associated with this profile.

Source Low Port
The low port associated with this profile.

Destination of Low IP Address
The low destination IP address.

Destination of High IP Address
The high destination IP address.

Destination Low Port
The low destination port number.

Destination High Port
The high destination port number.

Type-of-Service Byte Mask
The type-of-service byte mask.

Type-of-Service Byte Match
The type-of-service byte match value.

Local ID Type
The local ID type.

Local ID Value
The local ID value.

Remote ID Group Name
The name of the remote ID group.

Ingress/Egress Profiles: The view provides information on ingress/egress profiles. It contains the following fields:

Traffic Profile Name
The name of the traffic profile.

Traffic Profile Ingress/Egress Index
The index of the interface pair.

Ingress IP Address
The IP address of inbound traffic.

Egress IP Address
The IP address of outbound traffic.

Remote ID Profiles Panel: This panel provides information on the remote IDs associated with a traffic profile. It contains the following fields:

Traffic Profile Name
The name of the traffic profile.

Traffic Profile Remote Group
The name of the remote group.

Index The index of the remote ID.

Type The type of the remote ID.

Value The value of the remote ID>

Authentication Mode
The authentication mode used for this remote ID.

Actions Folder

This folder provides information on IPSec key management, IPSec data management, differential services, and resource reservation protocol (RSVP). It has the following dependent items:

- IPSec folder
- Differential Services panel
- RSVP panel

IPSec Folder: The IPSec folder provides information on IPSec key management and IPSec data management. It has the following dependent items:

- Key Management folder
- Data Management folder

Key Management Folder: The Key Management folder provides information on IPSec key management. It contains the following panels:

- Actions
- Proposals
- Actions-to-Proposals
- Active Instances

Actions Panel: The Actions panel provides information on key management actions. It contains the following fields:

Key Management Action Name
The name of the key management action.

Exchange Mode
the exchange mode.

Connection SA Lifetime
The connection Security Association lifetime in seconds.

Connection SA Lifesize
The connection Security Association lifesize in kilobytes.

Policy Role
The policy role.

Minimum Percent Refresh
The minimum Security Association refresh percentage.

Auto Start
The auto start indicator: true or false.

Matches
The number of matches for this action.

Proposals Panel: This panel provides information on key management proposals. It contains the following fields:

Key Management Proposal Name
The name of the key management proposal.

Authentication Method
The authentication method used for this proposal.

Hash Algorithm
The name of the has algorithm used for this proposal.

Cipher Algorithm
The name of the cipher algorithm used for this proposal.

Diffie Hellman Group ID
The diffie hellman group ID of this proposal.

SA Lifetime
The Security Association lifetime in seconds.

SA Lifesize
The Security Association lifesize in kilobytes.

Actions-To-Proposals Panel: This panel provides information on key actions and key proposals. It contains the following fields:

Key Management Action Name
The name of the key management action.

Proposal Name
The name of the key management proposal

Proposal Order
The order of the key management proposal.

Action Details
A summary of the information in the Action panel. See Actions Panel for more information.

Proposal Details
A summary of the information in the Proposals panel. See Proposals Panel for more information.

Active Instances Panel: This panel gives information on active key management instances. It contains the following fields:

Action Name
The name of the key management action.

Create Order
The order in which this action was created.

KM Tunnel ID
The Key Management tunnel ID.

KM Tunnel Index
The Key Management tunnel index.

Action Details
A summary of the information in the Action panel. See Actions Panel for more information.

Status The status of the active tunnel: active or destroy. Authorized users can change this value from the Active Instances panel.

IPSec Data Management Folder: This folder provides information on IPSec data management. It contains the following dependent items:

- Actions panel
- Proposals panel
- Active Instances panel
- Transforms folder
- Correlations folder

Actions Panel: This panel provides information on IPSec data management actions. It contains the following fields:

Data Management Action Name
The name of the Data Management action.

Type The type of action: permit or deny.

Tunnel Start IP Address
The starting IP address of the tunnel.

Tunnel End IP Address
The ending IP address of the tunnel.

Local Proxy Type
The type of local proxy.

Local Proxy Value
The value of the local proxy.

Local Proxy Protocol
The protocol of the local proxy.

Local Proxy Source Port
The local proxy source port number.

Remote Proxy Type
The type of remote proxy.

Remote Proxy Value
The value of the remote proxy.

Remote Proxy Protocol
The protocol of the remote proxy.

Remote Proxy Source Port
The remote proxy source port number.

SA Refresh Threshold Percent
The Security Association refresh threshold.

Minimum SA Refresh Threshold Percent
The minimum Security Association refresh threshold.

Tunnel-In-Tunnel
The tunnel-in-tunnel indicator.

Auto Start
The auto start setting: enable or disable.

Don’t Fragment Bit Handling
The don’t fragment bit handling indicator.

Replay Prevention
The replay prevention setting.

Matches
The number of matches for this action.

Proposals Panel: This panel provides information on Data Management proposals. It contains the following fields:

Name The name of the Data Management Action.

Perfect-Forward-Secrecy
The perfect forward secrecy setting: enable or disable.

Diffie Hellman Group ID
The diffie hellman group ID.

Active Instances Panel: This panel provides information on active Data Management instances. It contains the following fields:

Data Management Action
The name of the Data Management action.

Creation Order
The order in which the Data Management action was created.

Key Management Tunnel ID
The Key Management tunnel ID.

Data Management Tunnel Index
The Data Management tunnel index.

Data Management Action Details
A summary of the Data Management Action panel. See “Actions Panel” on page 52 for more information.

Key Management Action Details
A summary of the Key Management Action panel. See “Actions Panel” on page 50 for more information.

Transforms Folder: This folder provides information on Data Management transforms. It has the following panels:

- AH Transforms
- ESP Transforms
- IPCOMP Transforms

AH Transforms Panel: This panel provides information on authentication header (AH) transforms. It contains the following fields:

AH Transform Name
The name of the authentication header transform.

Encapsulation Algorithm
The encapsulation algorithm used by the AH transform.

Integrity Algorithm
The integrity algorithm used by the AH transform.

SA Lifetime
The Security Association lifetime in seconds.

SA Lifesize
The Security Association lifesize in kilobytes.

ESP Transforms Panel: This panel provides information on Encapsulating Security Payload (ESP) transforms. It contains the following fields:

ESP Transform Name
The name of the ESP transform.

Encapsulation Algorithm
The encapsulation algorithm used by the ESP transform.

Integrity Algorithm
The integrity algorithm used by the ESP transform.

SA Lifetime
The Security Association lifetime in seconds.

SA Lifesize
The Security Association lifesize in kilobytes.

IPCOMP Transforms Panel: This panel provides information on IPCOMP transforms. It contains the following fields:

Name The name of the IPCOMP transform.

IPCOMP Algorithm
The name of the compression algorithm.

IPCOMP Vendor Algorithm
The name of the vendor algorithm.

SA Lifetime
The Security Association lifetime in seconds.

SA Lifesize
The Security Association lifesize in kilobytes.

Correlation Folder: This folder provides information on correlation between IPSec Data Management Proposals and active transforms. It contains the following panels:

- Data Management Proposal Correlation
- AH Correlation
- ESP Correlation
- IPCOMP Correlation

Data Management Proposal Correlation Panel: This panel provides information on Data Management Proposal correlations. It contains the following fields:

Action Name
The name of the Data Management action.

Proposal Name
The name of the Data Management proposal.

Proposal Order
The order of the Data Management proposal.

Data Management Action Details
A summary of the Data Management Actions panel. See “Actions Panel” on page 52 for more information.

Data Management Proposal Details
A summary of the Data Management Proposals panel. See “Proposals Panel” on page 53 for more information.

AH Correlation Panel: This panel provides information on authentication header (AH) correlations. It contains the following fields:

Proposal Name
The name of the Data Management proposal.

AH Transform Name
The name of the AH transform.

AH Transform Order
The order of the AH transform.

Data Management Action Details
A summary of the Data Management Actions panel. See “Actions Panel” on page 52 for more information.

AH Transform Details
A summary of the AH Transform panel. See “AH Transforms Panel” on page 54

ESP Correlation Panel: This panel provides information on Encapsulating Security Payload (ESP) correlations. It contains the following fields:

Proposal Name
The name of the Data Management proposal.

ESP Transform Name
The name of the ESP transform.

ESP Transform Order
The order of the ESP transform.

Data Management Action Details
A summary of the Data Management Actions panel. See “Actions Panel” on page 52 for more information.

ESP Transform Details
A summary of the ESP Transform panel. See “ESP Transforms Panel” on page 54

IPCOMP Correlation Panel: This panel provides information on IPCOMP correlations. It contains the following fields:

Proposal Name
The name of the Data Management proposal.

IPCOMP Transform Name
The name of the IPCOMP transform.

IPCOMP Transform Order
The order of the IPCOMP transform.

Data Management Action Details
A summary of the Data Management Actions panel. See “Actions Panel” on page 52 for more information.

IPCOMP Transform Details
A summary of the IPCOMP Transform panel. See “IPCOMP Transforms Panel” on page 55

Differential Services Actions Panel: This panel provides a view of all differential services action definitions. It contains the following fields:

Differential Services Action Name
The name of the differential services action.

Permission
The permission value of the action: permit or deny.

Queue Priority
The queue priority of the action.

Bandwidth Type
The bandwidth type of the action.

Bandwidth Share
The bandwidth share of the action.

TOS Mask
The type-of-service byte mask.

TOS Match
The type-of-service byte match.

Matches
The number of matches for this action.

RSVP Actions: This panel provides a view of all RSVP action definitions. It contains the following fields:

Name The name of the RSVP action.

Permission
The permission value of the action: permit or deny.

Max Rate/Flow
The maximum rate per flow in kilobytes.

Max Token-Bucket/Flow
The maximum token-bucket per flow.

Max Flow Duration
The duration of the maximum flow in seconds.

Min Delay
The minimum delay in seconds.

Differential Services Action
The name of the differential services action.

Differential Services Action Details
A summary of the Differential Services Action panel. See “Differential Services Actions Panel” on page 56 for more information.

Chapter 11. VPN Monitor Events Folder

The VPN Monitor Events folder provides information on event reporting performed by the VPN Monitor. It has the following dependent items:

- Layer-2 Authentication folder
- IPSec Authentication/Encryption folder

Layer-2 Authentication Folder

The folder provides information on Layer-2 authentications performed by the monitored device. It contains the following panels:

- Statistics
- Tunnel Failure Log
- Session Failure Log

Statistics Panel

This panel provides statistics on Layer-2 authentications performed by the monitored device. It contains the following fields:

Tunnel Successes
The number of Layer-2 tunnels that have been activated.

Tunnel Failures
The number of Layer-2 tunnels that could not be authenticated, and were not activated.

Session Successes
The number of Layer-2 sessions that have been activated.

Session Failures
The number of Layer-2 sessions that could not be authenticated, and were not activated.

Tunnel Failure Log Panel

This panel provides information about Layer-2 tunnels that could not be authenticated, and therefore were not opened. It has the following fields:

Failure Number
The failure number.

Host The host for the failed tunnel.

IP Address
The IP address for the failed tunnel.

Time The time of the failure.

Session Failure Log Panel

This panel provides information about Layer-2 sessions that could not be authenticated, and therefore were not opened. It has the following fields:

Failure Number
The failure number

User ID
The user ID associated with the failed tunnel.

Time The time of the failure.

IPSec Authentication/Encryption Folder

This folder provides information about IPSec authentications and encryptions performed by the monitored device. It contains the following panels:

- Statistics
- IPSec Failure Log

Statistics Panel

This panel provides statistics for IPSec authentications and encryptions performed by the monitored device. It contains the following fields:

In Authentications
The number of IPSec inbound authentications performed.

In Authentication Failures
The number of failed IPSec inbound authentications.

In Decryptions
The number of IPSec inbound decryptions performed.

In Decryption Failures
The number of failed IPSec inbound decryptions.

Out Authentications
The number of IPSec outbound authentications performed.

Out Authentication Failures
The number of failed IPSec outbound authentications.

Out Encryptions
The number of IPSec outbound encryptions performed.

Out Encryptions Failures
The number of failed IPSec outbound encryptions.

IPSec Failure Log Panel

This panel provides information on IPSec authentication and encryption failures. It contains the following fields:

Failure Number
The failure number.

Reason
The reason for the failure.

Time The time of the failure.

Tunnel ID
The tunnel ID of the failure.

SA SPI The Security Association Security Protection Index of the failure.

Source IP Address
The source IP address of the failure.

Destination IP Address
The destination IP address of the failure.

Chapter 12. VPN Monitor Operational Folder

This folder provides information on the operation of the monitored device. It has the following dependent items:

- Tunnels folder
- Clients folder
- Policies folder
- LDAP folder
- Traps folder

Tunnels Folder

This folder provides view and operational capabilities for Layer-2 history and log table sizes, active Layer-2 tunnels, active IPSec control tunnels, and active IPSec user tunnels. It has the following panels:

- Table Size
- Inactivate Layer-2 Tunnels
- Inactivate IPSec Control Tunnels
- Inactivate IPSec User Tunnels

Table Size Panel

This panel provides information on Layer-2 history and log table sizes. It has the following fields:

Layer-2 History Tables
The number of entries to keep for previous Layer-2 tunnels and sessions. Authorized users can change this value from the Table Size panel.

Layer-2 Authentication Failure Tables
The number of entries to keep in the Layer-2 Authentication Failure table. Authorized users can change this value from the Table Size panel.

Inactivate Layer-2 Tunnels Panel

This panel allows authorized users to deactivate Layer-2 tunnels. It contains the following fields:

Active Layer-2 Tunnels Details
A summary of the Active Layer-2 Tunnels panel.

Status The trigger to destroy a single tunnel. Authorized users can change this value from the Inactivate Layer-2 Tunnels Panel.

Destroy All Tunnels
The trigger to destroy all tunnels. Authorized users can change this value from the Inactivate Layer-2 Tunnels Panel.

Inactivate IPSec Control Tunnels Panel

This panel allows authorized users to deactivate IPSec control tunnels. It has the following fields:

Active IPSec Control Tunnel Details
A summary of the Active IPSec Control Tunnels panel.

Status The trigger to destroy a single tunnel. Authorized users can change this value from the Inactivate IPSec Control Tunnels Panel.

Destroy All Tunnels
The trigger to destroy all tunnels. Authorized users can change this value from the Inactivate IPSec Control Tunnels Panel.

Inactivate IPSec User Tunnels Panel

This panel allows authorized users to deactivate IPSec user tunnels. It has the following fields:

Active IPSec user Tunnel Details
A summary of the Active IPSec user Tunnels panel.

Status The trigger to destroy a single tunnel. Authorized users can change this value from the Inactivate IPSec user Tunnels Panel.

Destroy All Tunnels
The trigger to destroy all tunnels. Authorized users can change this value from the Inactivate IPSec user Tunnels Panel.

Clients Folder

This folder provides view and control capabilities for Layer-2 sessions. It has the following panels:

- Inactivate Layer-2 Sessions

Inactivate Layer-2 sessions Panel

This panel allows authorized users to deactivate Layer-2 sessions. It contains the following fields:

Active Layer-2 Sessions Details
A summary of the Active Layer-2 Sessions panel.

Status The trigger to destroy a single session. Authorized users can change this value from the Inactivate Layer-2 Sessions Panel.

Destroy All sessions
The trigger to destroy all sessions. Authorized users can change this value from the Inactivate Layer-2 Sessions Panel.

Policies Folder

This folder provides view and control capabilities for VPN device policies. It contains the following panels:

- Enable/Disable Policies
- Reload Device Policies

Enable/Disable Policies Panel

This panel enables users to enable or disable a selected device policy. It contains the following fields:

Policy Details
A summary of the Policies panel.

Status The trigger to enable or disable a policy. Authorized users can change this value from this panel.

Reload Device Policies Panel

This panel enables users to reload the policies in use for a monitored device. It contains the following fields:

Administrative Definition Details
A summary of the administrative Lightweight Directory Access Protocol (LDAP) definitions. See “Administrative Parameters Panel” on page 66 for more information.

Operational Definition Details
A summary of the operational LDAP definitions. See “Operational Parameters Panel” on page 65 for more information.

Reload Policies
The trigger to reload policies. Authorized users can reload policies from this panel.

LDAP Folder

This folder provides view and control capabilities for the Lightweight Directory Access Protocol (LDAP) parameters. It contains the following panels:

- Operational Parameters
- Administrative Parameters

Operational Parameters Panel

This panel provides information on LDAP operational parameters. It contains the following fields:

Status The status of the definition: enable or disable.

Primary LDAP Server IP Address
The IP address of the primary LDAP server.

Secondary LDAP Server IP Address
The IP address of the secondary LDAP server.

LDAP Server Level
The level of the LDAP server.

Policy Base Name
The name of the policy base object for the device.

Port The port number used by the LDAP server.

Timeout
The timeout value used by the LDAP server.

Retry Interval
The retry interval used by the LDAP server.

User ID
The user ID of the LDAP server.

Administrative Parameters Panel

This panel provides control of the LDAP parameters. It contains the same fields as the Operational Parameters panel, but authorized can change the value of any of the parameters on this panel.

Traps Folder

This folder provides view and control capabilities for VPN traps. It contains the following panels:

- Layer-2 Trap Control
- IPSec Trap Control

Layer-2 Trap Control Panel

This panel provides information on and control of Layer-2 traps on the selected device. Authorized users can change the values of all fields in this panel. The Layer-2 Trap Control panel contains the following fields:

Tunnel Start Traps
The status of tunnel start trap processing: enable or disable.

Tunnel Stop Traps
The status of tunnel stop trap processing: enable or disable.

Tunnel Authentication Failure Traps
The status of tunnel authentication failure trap processing: enable or disable.

User Authentication Failure Traps
The status of user authentication failure trap processing: enable or disable.

IPSec Trap Control Panel

This panel provides information on and control of IPSec traps on the selected device. Authorized users can change the values of all fields in this panel. The IPSec Trap Control panel contains the following fields:

Control Tunnel Start Traps
The status of control tunnel start trap processing: enable or disable.

Control Tunnel Stop Traps
The status of control tunnel stop trap processing: enable or disable.

User-Data Tunnel Start Traps
The status of user-data tunnel start trap processing: enable or disable.

User-Data Tunnel Stop Traps
The status of user-data tunnel stop trap processing: enable or disable.

Authentication Failure Traps
The status of authentication failure trap processing: enable or disable.

Decryption Failure Traps
The status of decryption failure trap processing: enable or disable.

Chapter 13. VPN Monitor Tests Folder

This folder allows users to test policies, connectivity, and response time to and from hosts. It contains the following dependent items:

- Policy Test panel
- Layer-2 Tests folder
- Remote Ping panel

Policy Test Panel

This panel gives you the ability to execute policy tests and review the results. You can start a test by specifying the source and destination addresses, source and destination ports, the protocol to be used and the type of service requested. When the test is complete, the selected policies and actions are displayed. The Policy Test panel contains the following fields:

Test Index
The index of the test.

Result
The result of the test.

Status
The status of the test entry.

Source IP Address
The source IP address to use in the test. You can change this value here.

Source Port
The source port to use in the test. You can change this value here.

Destination IP Address
The destination IP address to use in the test. You can change this value here.

Destination Port
The destination port to use in the test. You can change this value here.

Protocol
The protocol to use in the test. You can change this value here.

TOS Byte
The type-of-service byte to use in the test. You can change this value here.

Key Management Policy
The selected key management policy.

Key Management Action
The selected key management action.

Data Management Policy
The selected data management policy.

Data Management Action
The selected data management action.

Diff Services Policy
The selected differential services policy.

Diff Services Action
The selected differential services action.

RSVP Policy
The selected RSVP policy.

RSVP Action
The selected RSVP action.

Layer-2 Tests Folder

This folder allows you to test connectivity and response time for Layer-2 tunnels. It contains the following panels:

- Layer-2 Connection Test
- Layer-2 Response Time Test

Layer-2 Connection Test Panel

This panel allows you to test the potential Layer-2 connectivity to a host. To start the test, select the name of a potential host. When the test is complete, the availability of the connection is displayed. This panel contains the following fields:

Test Index
The index of the test.

Host The host to test connectivity to. You can change this value here.

Result The result of the test.

Tunnel Type
The tunnel type used for the test.

Layer-2 Response Time Test Panel

This panel allows you to test the response time of an active host. To start the test, select the name of an active host. When the test is complete, the round trip time of a packet to the selected host is displayed. This panel contains the following fields:

Test Index
The index of the test.

Host The host to test connectivity to. You can change this value here.

Result The result of the test.

Round Trip Time
The round trip time of the test packet.

Remote Ping Panel

This panel allows you to test the response time from the current VPN device to another device. To start the Ping, specify the IP address of the remote host, the packet size, and the timeout value to be used for the test. When the test is complete, the round trip time of a packet to the host is displayed. This panel contains the following fields:

IP Address
The IP address to ping. You can change this value here.

Packet Size
The packet size to use for the ping. You can change this value here.

Timeout Value
The timeout value to use for the ping. You can change this value here.

Result The result of the ping.

Ping Time
The round trip time of the test.

Appendix. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area.

References in this publication to IBM products, programs, and services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the user's responsibility.

IBM may have patents or pending patent applications covering the subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

DB2	IBM
Nways	DB2 Universal Database

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows 95 and Windows 98 logos are trademarks or registered trademarks of Microsoft Corporation.

Pentium is a registered trademark of Intel Corporation in the U.S. and other countries.

Netfinity is a trademark of Tivoli Systems, Inc. in the United States or other countries or both.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Freelance Graphics is a trademark of Lotus Development Corporation in the United States or other countries or both.

Other company, product, and service names may be trademarks or service marks of others.

Readers' Comments — We'd Like to Hear from You

Nways Manager
Nways VPN Manager User's Guide

Publication No. GA27-4233-00

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name	Address
Company or Organization	
Phone No.	

Readers' Comments — We'd Like to Hear from You
GA27-4233-00

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Department CJBA
Design & Information Development
IBM Corporation
PO Box 12195
RESEARCH TRIANGLE PARK, NC
USA 27709

Fold and Tape **Please do not staple** Fold and Tape

GA27-4233-00

Cut or Fold
Along Line

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

Nways Management Web site:
http://www.networking.ibm.com/netmgt

GA27-4233-00