Front

Novell Internet Access Server 4.1 ConnectView Guide

About This Guide 7

Introduction 7

Getting Started 9

ConnectView Overview 9
New Features 10
Understanding Management 11
Understanding the List of Available Servers 12
Performance Considerations 12
Determining Product Requirements 12
Software Requirements 13
Hardware Requirements 13
Network Requirements 14
Server Requirements 14
Installing ConnectView 14
Starting ConnectView 16
Exiting ConnectView 16

Basic Server Management 17

Displaying and Managing Servers and Their Resources 17
Managing and Monitoring Connections and Ports 19
Managing Port Connections 20
Viewing Port Status 21
Setting Port Thresholds 22
Managing NASI Connection Service (NCS) Sessions 23
Accessing Log Files and Log Reports 24
Configuring Audit Trail Recording 25
Using Alerts Files 25
Using Audit Trail Files 28
Loading and Unloading Services 31
Setting Application Preferences 32

Displaying and Using Trend Analysis Data 35

Preparing for Trend Analysis 36
Maintaining Audit Trail and Archive Files 36
Ensuring That Server and Workstation Software Is Running 36
Planning for Data Display 37
Displaying Trend Analysis Data 37
Setting the Trend Analysis Display Options 38
Using the Trend Analysis Split Window 38
Interpreting Trend Analysis Data 39

Maximum Ports Usage Graphs . . . 39
Connections by Direction Graphs . . . 42
Connections by Service Graphs . . . 43
Connection Attempts Graphs . . . 45
Connection Duration Graphs . . . 46
Traffic Statistics Graphs . . . 49
Usage by Media Graphs . . . 51
Saving Trend Analysis Data . . . 53
Outputting Trend Analysis Data . . . 54
Copying Trend Analysis Data . . . 54

Setting Up Accounting Profiles and Generating Billing Charges . . . 55

Preparing for Accounting . . . 56
Maintaining Audit Trail and Archive Files . . . 56
Understanding How Accounting Data Is Calculated . . . 57
Matching Start Connection and End Connection Records . . . 57
Applying Rates to Connection Durations . . . 59
Handling Invalid Connections and Duplicate Connection IDs . . . 60
Setting Up Accounting Profiles . . . 61
Setting the Rate per Minute Charge . . . 63
Setting the Rate per Connection Charge . . . 64
Setting the Overhead Rate Charge . . . 66
Entering Billing Rates . . . 67
Viewing Sample Billing Charges . . . 73
Assigning Accounting Profiles and Account Numbers to Users . . . 74
Adding Users and Removing Users from a Profile Assignment . . . 75
Selecting an Accounting Profile . . . 77
Setting Up Account Numbers . . . 78
Displaying Billing Charges . . . 78
Specifying a Billing Period and Accessing the Accounting Log Window . . . 79
Accessing the Accounting Report Window . . . 84
Customizing the Accounting Report . . . 85
Displaying Incomplete Connections and Connections with Duplicate IDs . . . 86
Printing, Copying, and Exporting Accounting Data . . . 87
Copying Accounting Data . . . 88
Printing Accounting Data . . . 88
Exporting Accounting Data . . . 88

Running with ManageWise 89

Installing with ManageWise . . . 89
Using ManageWise SNMP Options . . . 92
Starting from ManageWise . . . 92

Understanding SNMP Management and Security 93

Understanding SNMP Management 93
Understanding ConnectView Security 94
Setting Workstation SNMP Security 95
Viewing Audit Trail, Alerts, Trend Analysis, and Accounting Data 95

Preface

About This Guide

Introduction

This guide contains information for network managers. Read this guide if you are responsible for managing one or more Novell® Internet Access Server 4.1 servers.

This guide assumes that you are familiar with Windows conventions, have a basic knowledge of Novell Internet Access Server 4.1 remote access services and concepts, and have a working knowledge of SNMP.

This guide does not explain how to install, configure, or administer the remote access software. For details about performing those tasks, see the Novell Internet Access Server 4.1 remote access documentation.

Chapter 1 *Getting Started*

ConnectViewTM runs on an IBM* PC or compatible network computer as a standalone Windows-based application. ConnectView enables you to monitor and manage multiple Novell® Internet Access Server 4.1 remote access servers and NetWare® ConnectTM 2.0 servers from your workstation.

Note To run with other Novell management software, see Appendix B, “Understanding SNMP Management and Security,” on page 93

This chapter discusses the following topics:

- “ConnectView Overview” on page 9
- “Determining Product Requirements” on page 12
- “Installing ConnectView” on page 14
- “Starting ConnectView” on page 16
- “Exiting ConnectView” on page 16

ConnectView Overview

ConnectView 2.*x* benefits include

- Novell Internet Access Server 4.1 remote access and NetWare Connect 2.0 server management with a server list defined from the Server Advertising Protocol (SAP)
- Real-time port and connection management to enable you to quickly view and monitor the status of each server's ports and connections
- Graphical display of port status to enable you to quickly determine port utilization and verify important configuration data and modem status

- NetWare Asynchronous Services Interface (NASITM) Connection Service (NCS) session management to enable you to dynamically monitor and manage NCS sessions
- Trend analysis graphs to enable you to evaluate resource utilization, perform capacity planning, proactively anticipate performance problems, and efficiently distribute server usage
- Accounting charges and reporting to enable you to create an accounting system, apply charges to your remote access users, and display and/or export accounting data and reports for further analysis
- Service management to enable you to dynamically load and unload remote access services
- Port threshold setting to enable you to receive proactive notification when port usage reaches a specified level on each managed server
- Generated alerts and audit trail reports with summary and daily information to enable you to print and store histories of network events and records of remote access service access and usage

New Features

ConnectView 2.1 includes the following enhancements:

- Management of Novell Internet Access Server 4.1 remote access software and existing NetWare Connect 2.0 servers
- Port media type (Asynchronous, X.25, ISDN) displayed in the View All and View windows
- Trend analysis for usage by media
- Report preferences to enable you to customize accounting, alert, and audit trail report data
- Enhanced accounting features
    - Additonal fields for connected time and baud rate in the Accounting Log window.
    - An accounting log display option to enable you to limit data in the Accounting Log window by date, account number, and username.

- Additional fields for the total dial-in connections and charges, total dial-out connections and charges, baud rate, and dial type in the Accounting Report window.
- An additional overhead rate option to enable you to apply the overhead charge to all users, including users who did not connect to the remote access software. Previously, the overhead charge was limited to users with valid remote access connections.
- ISDN short hold support.

Understanding Management

ConnectView uses a combination of the Simple Network Management Protocol (SNMP) and the remote Btrieve* client to manage your remote access software.

For ConnectView to manage the remote access software, the Remote Access Management Agent (RAMA) must be enabled and the NetWare SNMP Agent (SNMP.NLM) must be loaded on the server. When an SNMP GET or SET request is performed, the server's SNMP community strings are compared to the workstation's community string settings for that server. If they match, the request is performed. Otherwise, the request is denied. By default, ConnectView sets the workstation community strings to public (monitor=public control=public).

Note ConnectView does not install the Novell TCP/IP stack and does not support SNMP over IP. Also, ensure that BSPXCOM.NLM is loaded on the managed servers and BREQUEST.EXE is running on the ConnectView workstation.

For a more detailed discussion of SNMP and ConnectView security, see Appendix B, “Understanding SNMP Management and Security,” on page 93

ConnectView uses the remote Btrieve client to access records stored in the server-based audit trail log file for the Trend Analysis, Accounting, Audit Trail, and Alerts windows. To display this data, users must have Read/Scan rights to the server's SYS:\SYSTEM\CSLIB directories and files.

For users not logged in to a Novell Directory ServicesTM (NDSTM) tree for NetWare 4.1 servers, ConnectView displays a Bindery login box. The user must enter a valid username and password before ConnectView displays trend analysis, accounting, audit trail, and alert data.

Understanding the List of Available Servers

ConnectView displays a list of all available servers in the View All window. Available servers are servers that respond to the SAP of the server you are logged in to. If you are not logged in to a server, ConnectView uses the SAP notification from the server to which you are attached.

Unavailable servers that become available after ConnectView is started can be added to the View All window by choosing View >Update (F5).

Important

If you want to manage a server that is active but not displayed in the View All window, log in to either the desired server or a server that can receive SAP notification of the desired server. Then, from the View All window choose View > Update.

Performance Considerations

When using ConnectView, it is important to keep several performance issues in mind:

- If large amounts of data are involved in trend analysis, accounting, audit trail, or alert log viewing, ensure that sufficient memory is available.

  A substantial amount of time may be required to process large amounts of data. The time required to process the data depends on the available disk space, the number of records, and your Windows configuration. During low memory conditions, Windows may begin to swap data to disk, increasing the amount of time required to process the data. In extremely low memory conditions, you may not be able to complete the operation.

- If ConnectView is running with other Windows applications, ConnectView competes with the other applications for Windows resources and memory, especially if many windows are open.

Determining Product Requirements

ConnectView has its own set of requirements, which are discussed in the following sections:

- Software requirements
- Hardware requirements

- Network requirements
- Server requirements

Software Requirements

- MS-DOS* 5.0 or higher
- Windows 3.1 or higher
- NetWare Client™ (VLMTM) 1.2 or later Novell Client™ software

Important If you are using the NetWare Client (VLM) 1.2 software, you can run ConnectView in both Windows 3.1 and Windows 95 environments. If you are using the Novell Client for DOS and Windows 3.1*x* software, you can run ConnectView in the Windows 3.1*x* environment. If you are using the Novell Client for Windows 95 software, the statement that loads BREQUEST.EXE is moved from your AUTOEXEC.BAT file to the WINSTART.BAT file, to enable you to run ConnectView in a Windows 95 environment.

Hardware Requirements

The ConnectView workstation must include the following hardware:

- An 80386- or 80486-based IBM PC/AT* compatible or higher computer
- A LAN adapter that, together with the drivers provided by the NetWare workstation shell, connects the ConnectView workstation to a LAN by use of SNMP over the Internetwork Packet ExchangeTM (IPXTM) protocol.
- A VGA or super VGA graphics card and monitor
- A mouse supported by Windows 3.1
- 8 MB of RAM
- 6 MB of disk space

Note If you have removed ManageWise® from your workstation, ensure that the NMS.INI file is removed from the \WINDOWS directory.

Network Requirements

If ConnectView is to operate in a WAN environment, you must have a ConnectView workstation and the hardware and software capable of connecting the WANs. This hardware and software could be a router capable of routing IPX traffic.

Important ConnectView does not support SNMP over IP.

Server Requirements

ConnectView manages the Novell Internet Access Server 4.1 remote access software and NetWare Connect 2.0 servers.

Important The BSPXCOM.NLM and NCMA.NLM files must be loaded on the managed servers.

Installing ConnectView

To install ConnectView, complete the following steps:

1. **Insert and mount the Novell BorderManager CD-ROM.**

2. **Choose File > Run from the Program Manager menu and run the ConnectView SETUP.EXE program from the \CLIENT\CVIEW\DISK1 directory.**

   See your Windows documentation for details about running applications within Windows.

3. **Follow the installation program's directions.**

   The installation program displays a series of windows with dialog boxes that guide you through the installation process. Although the dialog boxes are self-explanatory, when you are installing ConnectView, you should be aware of the following information:

   - The default directory of ConnectView is \NWCVIEW.
   - You can exit the installation program any time; simply click the Exit button. A message appears to confirm the operation.

- ConnectView enables you to specify the target directory to which the Btrieve v6.15 files are copied. By default, the Btrieve files are copied to the \WINDOWS directory. If you want to copy the files to a different directory, click the Btrieve Directory button in the Welcome screen and specify the desired location.
- If any ConnectView files already exist on the target location, ConnectView lists the installation files and the existing files with check boxes for each file. If you want to overwrite the installed files, click the check boxes for the desired version of the displayed files.
- ConnectView edits your AUTOEXEC.BAT file to load the BREQUEST.EXE and SHARE files. If you change the AUTOEXEC.BAT file, the current file is saved as AUTOEXEC.SAV. If you do not change the AUTOEXEC.BAT file, the file with changes suggested by ConnectView is saved as AUTOEXEC.NEW.

Important

If you are using the NetWare Client (VLM)1.2 software, you can run ConnectView in both Windows 3.1 and Windows 95 environments. If you are using the Novell Client for DOS and Windows 3.1*x* software, you can run ConnectView in the Windows 3.1*x* environment. If you are using the Novell Client for Windows 95 software, ConnectView moves the statement that loads BREQUEST.EXE from your AUTOEXEC.BAT file to the WINSTART.BAT file to enable you to run ConnectView in a Windows 95 environment.

- When viewing the AUTOEXEC.BAT file, click the Warning Alerts button to display possible conflicts with files existing in multiple locations. ConnectView also suggests corrective actions to avoid these conflicts.

4. **If your AUTOEXEC.BAT file has changed, reboot your system. Otherwise, restart Windows.**

   If you changed your AUTOEXEC.BAT file to load the BREQUEST.EXE file after the NetWare shell but before Windows, or for any other reason, reboot your system before starting ConnectView. Otherwise, bring down Windows, ensure that the BREQUEST.EXE file is loaded after the NetWare shell, and restart Windows before starting ConnectView. However, if you do not include the statement to load the BREQUEST.EXE file in your AUTOEXEC.BAT file, the next time you reboot the ConnectView workstation you will have to reload the BREQUEST.EXE file before starting ConnectView. If you choose to return to Windows, ensure that the proper action is taken before you attempt to start ConnectView.

5. **Check the ConnectView file NWCVIEW.TXT for product notes.**

   ConnectView provides the NWCVIEW.TXT file for product notes and last-minute feature changes. This file is stored in \NWCVIEW. To access this file anytime, use the Microsoft* Notepad or any text editor.

   See Appendix A, “Running with ManageWise,” on page 89 if you plan to use ConnectView with Novell management software.

Starting ConnectView

ConnectView creates a ConnectView program group in Program Manager with ConnectView, NWCV Help, and NWCV Readme Notes icons. If a ConnectView program item already exists, it is replaced with a new link to the ConnectView 2.1 program files.

To start ConnectView, double-click the ConnectView icon. ConnectView opens the application and displays a View All window with a list of the managed servers.

To manage the remote access software, select the desired server and then click the desired icons in the Tool Bar or choose the commands in the Menu Bar.

Exiting ConnectView

Exit ConnectView whenever you no longer want to monitor or manage the remote access software on the servers displayed in the View All window.

To exit ConnectView, use either of the following methods:

- Choose File > Exit (Alt+F+X).
- Issue the Windows Close command from the Application window. To do this, select the Control-menu box to display the Control menu and then choose Close (Alt+F4). For details about the Close command, see your Windows documentation.

Note

Double-clicking the Control-menu box also allows you to exit ConnectView.

Chapter 2 *Basic Server Management*

ConnectViewTM enables you to perform real-time management of the remote access software on multiple Novell® Internet Access Server 4.1 servers. This includes displaying multiple servers and their resources, managing ports and connections for a selected server, setting a port threshold value for each server, and displaying alerts and audit trail data for each server.

This chapter discusses the following topics:

- "Displaying and Managing Servers and Their Resources" on page 17
- "Managing and Monitoring Connections and Ports" on page 19
- "Accessing Log Files and Log Reports" on page 24

Displaying and Managing Servers and Their Resources

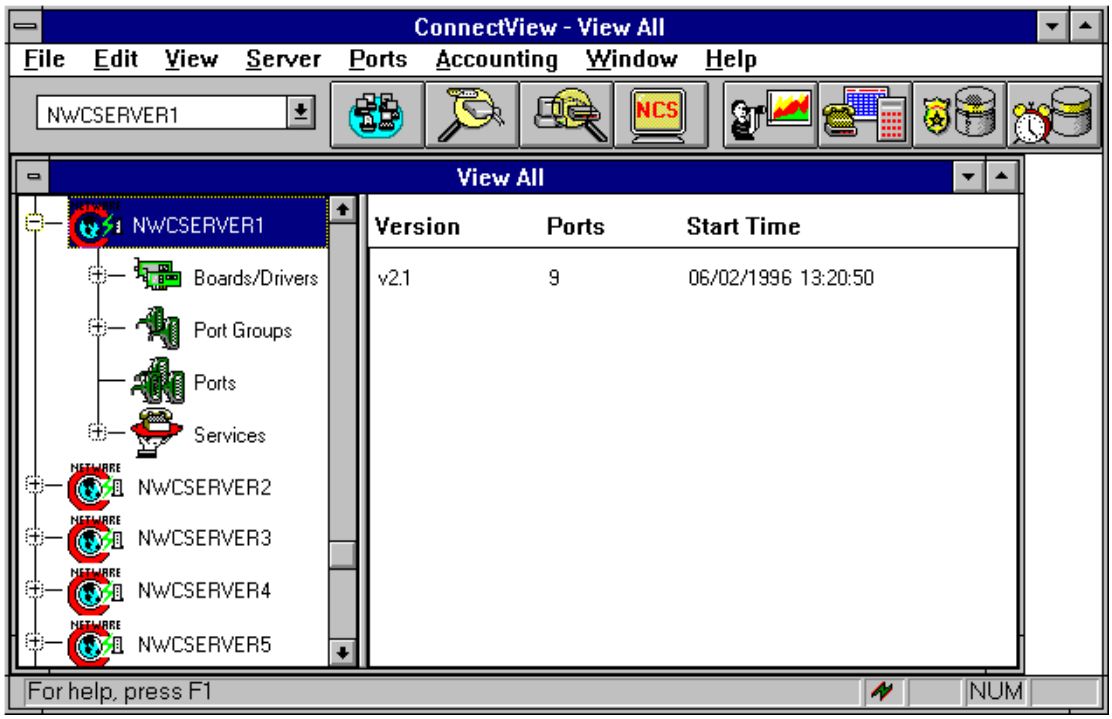
ConnectView opens a View All window whenever the application is started. The View All window enables you to quickly view a list of your managed servers, display and control the servers' resources, and view summary information about them. Server resources include the boards/drivers, port groups, ports, and remote access services. To view this data, you need the Simple Network Management Protocol (SNMP) MonitorCommunity (GET) access rights. Figure 2-1 shows an example View All window.

Note

Only one instance of the View All window can be opened. This window cannot be closed unless you exit the application; however, it can be minimized.

Figure 2-1

View All Window



You can also open View windows to display additional views of resources and data for individual servers. To open a View window, select the desired server and choose Window > New. A View window appears for the selected server.

Server and server resources appear as containers or leaf objects. Container objects (servers, board/driver groups, port groups, and service groups) can be expanded to display additional resources. A plus sign (+) appears in front of the container objects that can be expanded. A minus sign (-) appears in front of the objects that have been expanded and can then be collapsed. Leaf objects (individual boards/drivers, ports, individual port group, and service) are objects that cannot be expanded and do not have either symbol in front of them. Selecting an object causes information for the selected object to appear in the right side of the window.

To expand the objects of a container, either double-click the container or select it and choose View > Expand Object or press +. To return the objects to the container, either double-click the expanded container or select it and choose View > Collapse Object or press -.

Note

The message Gathering data ... appears when data for the server's resources is being obtained. Also, to indicate the application is processing data, a lightning bolt flashes in the Status Bar.

By default, server polling intervals are set to 5 minutes so the data in the View All and View windows is refreshed every 5 minutes. To force an immediate update of the data displayed in the View All window or a View window, select the window and choose View >Update (F5).

If data for a server cannot be retrieved, collapse it and select another object. Then, reselecting and expanding the server icon causes ConnectView to retry retrieving the data.

Managing and Monitoring Connections and Ports

To establish a dial-in or dial-out connection, the remote access software first assigns the user a necessary port and then establishes a connection to the destination device. After the connection is established, the remote access software, and any additional software, such as third-party remote access applications, establishes a session between the calling and receiving applications so that the remote node or remote control communication can take place.

ConnectView enables you to

- Quickly display a summary of port availability through a graph
- Quickly verify the status of a server's port connections and settings information to enable you to easily monitor connections and diagnose configuration problems when they occur
- Reset ports to enable you to perform port maintenance and security functions
- Access a Port Status dialog box for each port to enable you to view port utilization, display error statistics, verify port settings, and check modem status and operation
- Display NetWare® Asynchronous Service InterfaceTM (NASITM) Connection Service (NCS) session data to enable you to manage NCS sessions

Note You need the SNMP MonitorCommunity (GET) access rights to display data and the SNMP ControlCommunity (SET) access rights to perform management operations. Refer to “Setting Workstation SNMP Security” on page 95 for more information about setting community strings.

Managing Port Connections

You manage port connections in the Port Connections window. This window displays data in a graph showing the in-use and available ports, connection information, and detailed port configuration data.

To access the Port Connections window, first either select the desired server in a View All or View window or select the desired server name in the Server combo box in the Tool Bar. Then, either click the Port Connections icon in the Tool Bar or choose Server > View Port Connections. ConnectView opens the Port Connections window for the selected server.

Displaying Connections by User ID, Port Name, Port Status, or Service

ConnectView allows you to limit the display of port connections with the following display options:

- User ID
- Port
- Port status
- Service

Limiting the display of port connections helps you find information quickly and focus on connections and port problems when they occur. To access these options, choose View > Display Options (F4). ConnectView displays the Port Connections Display Options dialog box.

Specify the desired options and click OK.

Updating Port Connections Data

ConnectView updates port connection data based on the server's polling interval. By default, the server polling interval is set to 5 minutes for each managed server. ConnectView also enables you to force an immediate update of the information when it is needed.

Note To change a server's polling interval, choose File > Preferences and click the Server Information tab button.

To force an immediate update of the data in the Port Connections window, choose View > Update (F5). ConnectView replaces the current data with the most up-to-date data available from the network.

Viewing Port Status

To verify port status and configuration data, you can access a Port Status dialog box. This dialog box provides a real-time status of the selected ports, graphs for the level of traffic and errors, summary connection information, and a graphic display of modem and port signals.

To access a Port Status dialog box, first select the desired port in the View All, View, NCS Sessions, or Port Connections window. Then, either click the Port Status icon in the Tool Bar or choose Ports > View Port Status. ConnectView opens the Port Status dialog box for the selected port.

Note Double-clicking a port icon, or a port connection in the above windows also opens the Port Status dialog box.

Updating Port Data

ConnectView polls the selected port every 2 seconds to update the real-time data displayed in the Port Status dialog box. ConnectView updates this data independent of the server's polling interval. ConnectView also enables you to turn off this polling by clicking the Stop Polling button or to force an immediate update of the information by pressing Update.

Resetting Port Statistics

ConnectView enables you to reset the statistics displayed in the Traffic and Errors graphs, so that you focus your analysis on current and future traffic and error rates. By default, these statistics are cumulative for all connections on this port, starting from when the remote access software was started.

To reset the statistics, click the Reset Statistics button. The current statistics are set to zero. Statistics for new traffic and errors accumulate until the dialog box is closed or the statistics are reset again.

Reopening the dialog box displays the current cumulative statistics based on the original data. The statistics return to zero when the remote access software is unloaded and restarted.

Resetting Ports

ConnectView enables you to reset the ports displayed for the current server. Reset a port to terminate an unwanted connection or to perform connection and session maintenance. Resetting a port disconnects the current users and returns the port to its original state. This is equivalent to the remote access software unconditional port reset command.

Note To reset a port, you need the SNMP ControlCommunity (SET) access rights. Refer to “Setting Workstation SNMP Security” on page 95 for more information about setting community strings.

To reset a port, select the desired port and choose Ports > Reset Port. ConnectView resets the selected port.

Note Another way to reset a port is by selecting a port in any ConnectView window that displays ports and choosing Ports > Reset Port.

Setting Port Thresholds

ConnectView enables you to set a port usage threshold, to enable you to receive proactive notification when port usage reaches a specified limit.

When the threshold limit is reached, the remote access software generates a threshold message informing you that the port usage threshold has been reached. This proactive notification can help you efficiently distribute port usage across your servers, optimize port usage, and perform capacity planning.

Note To set a port threshold, you need the SNMP ControlCommunity (SET) access rights. Refer to “Setting Workstation SNMP Security” on page 95 for more information about setting community strings.

To set a port threshold, select the desired server in a View All or a View window, or select the desired server name in the Server combo box in the Tool Bar. Then, choose Ports > Set Port Usage Threshold. ConnectView opens the Threshold Settings dialog box. Enter the desired settings and click OK.

Managing NASI Connection Service (NCS) Sessions

You can manage NCS sessions in the NCS Sessions window. This window provides a status of the NCS sessions on the current server and is updated according to the server's polling interval. By default, the server polling interval is set to 5 minutes for each managed server.

To access the NCS sessions window, first either select the desired server in the View All window or a View window, or select the desired server name in the Server combo box in the Tool Bar. Then, either click the NCS Sessions icon in the Tool Bar or choose Server > View NCS Sessions. ConnectView opens the NCS Sessions window for the selected server.

Displaying Connections by Session ID, Port, Status, or Dial Type

ConnectView allows you to filter the display of NCS session data with the following display options:

- Session ID
- Port
- Status
- Dial type

To access these options, choose View > Display Options (F4). ConnectView displays the NCS Sessions Display Options dialog box.

Updating NCS Session Data

ConnectView updates the data in the NCS Sessions window according to the server polling interval. By default, the server polling interval is set to 5 minutes for each managed server. ConnectView also enables you to force an immediate update of the information displayed in this window.

Note

To change the server's polling interval, choose File > Preferences and click the Server Information tab button.

To force an update of the data in the NCS Sessions window, choose View > Update (F5). ConnectView replaces the current data with the most up-to-date data from the network.

ConnectView enables you to reset the sessions displayed in the NCS Sessions window by resetting the port. This allows you to terminate unwanted connections and perform session maintenance. Resetting a port used by a session disconnects the current users and returns the port to its original state.

Note

You need the SNMP ControlCommunity (SET) access rights to reset a session. Only sessions with a Connected status can be reset. Refer to “Understanding SNMP Management” on page 93 for more information about setting community strings.

To reset a port, select the desired NCS session and choose Ports > Reset Port. ConnectView resets the port used by the selected session.

Accessing Log Files and Log Reports

ConnectView provides access to each managed server’s alerts file and audit trail file and displays data in report format. In addition, ConnectView allows you to customize the data fields that appear in the reports. The alerts file contains a history of a server’s events. The audit trail file contains a record of remote access service access and usage. These files are stored and maintained in the SYS:SYSTEM\CSLIB directories on the remote access servers on your network. Before accessing the log files, ensure that the BSPXCOM.NLM file is loaded on the managed servers and that the BREQUEST.EXE program file is running on the ConnectView workstation.

Important

The audit trail file and/or archived files must be available to display trend analysis, accounting, audit trail, and alert data. To enable the audit trail, choose Server > Configure Audit Trail. If a large audit trail file or archived files are used, obtaining audit trail or alerts data might require a substantial period of time.

This section covers the following topics:

- Configuring audit trail recording
- Using alerts files
- Using audit trail files

Configuring Audit Trail Recording

Audit trail records in the current audit trail file or archived files are required for trend analysis and accounting and for viewing alerts and audit trail logs. ConnectView enables you to dynamically turn on and off remote acess audit trail recording and set audit trail options for archiving files. By default, remote access audit trail recording is enabled; the archive hour is set to 3:00 a.m.; the archive interval is set to 1 day; the number of archived files retained is set to 7.

Note

To change the audit trail options, you need the SNMP ControlCommunity (SET) access rights. Refer to “Understanding SNMP Management” on page 93 for more information about setting community strings.

To toggle the remote access audit trail recording and change other audit trail options, select the desired server and choose Server > Configure Audit Trail. ConnectView opens the Audit Trail Configuration dialog box.

To enable remote access audit trail recording, click the Enable Audit Trail check box. Use the spin controls to set the desired archive hour, archive interval, and the number of archived files retained. To disable audit trail recording, clear the Enable Audit Trail check box.

Note

Enabling and disabling audit trail recording affects the recording of only remote access and NetWare ConnectTM 2.0 records. However, changes to the archive options affect the server's archive files.

To apply the changes and close the Audit Trail Configuration dialog box, click OK. To close this dialog box without applying the changes, click Cancel.

Using Alerts Files

Alerts files contain information about network events detected by the remote access software. Alerts files contain a chronological record of information—such as severity, time the event occurred, port name, and service—based on the current audit trail file. You can use the display options to view the alerts data from the archived files. Data for alerts can be displayed in tabular and report format.

ConnectView provides access to the alerts files of the servers you are managing to enable you to obtain a chronological list of server events and assess server performance.

To access an alerts file, complete the following steps:

1. **Ensure that the desired server is selected.**

   If the desired server is not selected, either select the server icon in the View All window or a View window or select the server name in the Server drop-down combo box located in the left corner of the Tool Bar.

2. **Either click the Alerts icon in the Tool Bar or choose Server > View Alerts.**

   ConnectView prompts you for start and end dates. Enter the desired dates and click OK. ConnectView opens an Alerts window.

   You can further limit the displayed alert data by choosing View > Display Options (F4) and specifying the dates within the specified start and end dates.

Important

Due to table tool limitations, up to 8,000 alert records may be displayed at one time.

Displaying Alert Data by Entry Time, Severity Level, Port, and Service

ConnectView enables you to limit the display of alerts by entry time, severity level, port name, and service.

To limit the data displayed in the Alerts window, choose View > Display Options (F4). ConnectView opens the Alerts Display Options dialog box.

Click the Filter radio button and click the check boxes for the desired options.

To display the alerts data for the specified settings, click OK. To close the Display Options dialog box without changing the current settings, click Cancel.

To return to full display, click the Show All radio button and OK.

Updating Alert Data

Alert data is not updated automatically. However, ConnectView enables you to refresh the data whenever it is necessary.

To force an immediate update of the data in the Alerts window, choose View > Update (F5). ConnectView replaces the current data with the most up-to-date data available from the current audit trail file.

Generating Alert Reports

ConnectView enables you to generate daily and summary alert data in report format. The report format allows you to view and print formatted data for server summaries or daily alert activities. Also, by using the Alerts Display Options dialog box to limit the data in the Alerts window, you can limit the content of the report to a specified time period, severity level, port, and service.

Note To limit the content of the report to a specified time period, severity, port, and service, use the display options in the Alerts window before accessing the report. Due to table tool limitations, up to 8,000 alert records may be displayed at one time.

To display alert data in report format, ensure that the desired server is selected, and from any window choose File > Generate Report > Alerts. ConnectView opens the Alerts Report window and displays the alert data in report format. The Alerts window is also opened in the background.

Note Closing the Alerts window also closes the Alerts Report window.

Customizing the Alert Report

ConnectView allows you to specify which information appears in the Alert Report window and in what order the data columns appear.

To customize the data display in the Alert Report window, choose File > Report Preferences and click the Alert tab button. The Report Preferences dialog box appears with the options for the Alert Report window.

By default, the Alert Report includes summary and detailed information. Detailed information appears in the following order:

- Entry time
- Severity
- Port name
- Service
- Description

Clear the check boxes for the data you do not want to appear in the report.

To change the order of the detailed information, select the desired field and click the Up or Down button.

To save your changes, click OK. The changes take effect the next time the Alert Report window is opened and remain in effect until these options are changed. To close this dialog box without applying the changes, click the Cancel button.

Printing or Copying Alert Report Data

ConnectView allows you to print or copy report data.

To print alert report data, open an Alerts Report window and choose File > Print. ConnectView prints the displayed report.

To copy the alert report data, open an Alerts Report window and choose Edit > Copy. ConnectView copies the displayed report to the Windows clipboard.

Using Audit Trail Files

An audit trail file is integral to network security and management. This file provides information that identifies who used which remote access ports and services, when the ports and services were used, and for how long. When the Audit Trail window is first opened, the data is based on the current audit trail file. You can use the display options to view the audit trail data from the archived files. This data enhances system security and enables efficient planning and resource allocation.

Accessing Audit Trail Records

To access a server's current audit trail file, complete the following steps:

1. **Ensure that the desired server is selected.**

   If the desired server is not selected, either select a server icon in the View All window or a View window or select a server name in the Server drop-down combo box located in the left corner of the Tool Bar.

2. **Either click the Audit Trail icon in the Tool Bar or choose Server > View Audit Trail.**

   ConnectView prompts you for start and end dates. Enter the desired dates and click OK. ConnectView opens an Audit Trail window.

You can further limit the displayed audit trail data by choosing View > Display Options (F4) and entering dates within the specified start and end dates.

Important Due to table tool limitations, up to 8,000 audit trail records may be displayed at one time.

Displaying Audit Trail Data by Entry Time, User ID, Port, Port Status, and Service

ConnectView enables you to limit the data displayed by entry time, user ID, port, port status, and service.

To display audit trail information by any of the display options, choose View > Display Options (F4). ConnectView opens the Audit Trail Display Options dialog box for the Audit Trail window.

Click the Filter radio button and click the check boxes for the desired options.

To display the audit trail data for the specified options, click OK. To close the Display Options dialog box without changing the current settings, click Cancel.

To return to full display, click the Show All radio button and OK.

Updating the Audit Trail Window

ConnectView enables you to update the information displayed in the Audit Trail window so that it reflects the server's most recent audit trail information. This data is not updated automatically.

To refresh the data in the Audit Trail window, choose View > Update (F5). ConnectView replaces the data displayed in the Audit Trail window with the most up-to-date data from the current audit trail file.

Generating Audit Trail Reports

ConnectView enables you to generate audit trail reports with server and daily totals. These reports allow you to easily view and output formatted server and daily summaries of remote access service access and use.

Note To limit the content of the report to a specified time period, user ID, port, port status, and service use the display options in the Audit Trail window before accessing the report. Due to table tool limitations, up to 8,000 audit trail records may be displayed at one time.

To generate an audit trail report, ensure that the desired server is selected and from any window choose File > Generate Report > Audit Trail. ConnectView opens an Audit Trail Report window with the report data. The Audit Trail window is also opened in the background.

Note Closing the Audit Trail window also closes the Audit Trail Report window.

Customizing the Audit Trail Report

ConnectView allows you to specify which information appears in the Audit Trail Report window and in what order the data columns appear.

To customize the data display in the Audit Trail Report window, choose File > Report Preferences and click the Audit Trail tab button. The Report Preferences dialog box appears with the options for the Audit Trail Report window.

By default, the Audit Trail Report includes summary and detailed information. Detailed information appears in the following order:

- Entry time
- User ID
- Port name
- Service
- Description
- Connection ID (not selected)
- Event ID (not selected)

Clear the check boxes for the data you do not wish to appear in the report.

To change the order of the detailed information, select the desired field and click the Up or Down button.

To save your changes, click OK. The changes take effect the next time the Audit Trail Report window is opened and remain in effect until these options are changed. To close this dialog box without applying the changes, click the Cancel button.

Printing or Copying Audit Trail Report Data

ConnectView allows you to print or copy report data.

To print the audit trail report data, open an Audit Trail Report window and choose File > Print. ConnectView prints the displayed report.

To copy the audit trail report data, open an Audit Trail Report window and choose Edit > Copy. ConnectView copies the displayed report to the Windows clipboard.

Loading and Unloading Services

The remote access software provides the following three basic services:

- NASI Connection Service (NCS)

  NCS provides PC and Mac* users dial-in capability with third-party access products and remote control technology. NCS also allows users to dial-out to host resources.

- AppleTalk* Remote Access Service (ARAS)

  ARAS provides Mac users dial-in capability with remote node technology.

- Point-to-Point Protocol/Remote Node Service (PPPRNS)

  PPPRNS provides Unix® and DOS users dial-in capability with remote node technology or ISDN connections.

ConnectView enables you to dynamically load and unload the available services on the current server.

Note

To load and unload services, you need ControlCommunity (SET) access rights. Refer to "Understanding SNMP Management" on page 93 for more information about setting community strings.

To load or unload a service, expand the server to display the desired service, select the desired service, and choose Server > Load Service or Server > Unload Service. ConnectView loads or unloads the selected service.

Setting Application Preferences

ConnectView provides several application preferences to enable you to customize the application for your environment. ConnectView preferences include

- Polling intervals to enable you to control how often the network is polled for data. This is especially useful to limit unnecessary traffic or traffic over slow networks. By default, the server polling interval is set to 5 minutes for each managed server.

- Grace periods to enable you to specify a minimum connection duration to be used for accounting and trend analysis data. By default, a grace period of 30 seconds is used for each service.

- SNMP options to enable you to set workstation community strings for individual servers and SNMP timeout values and retry values. By default, MonitorCommunity and ControlCommunity strings are set to public, the SNMP retry value is set to 2 retries, and the SNMP timeout value is set to 5 seconds.

Note SNMP options are available only when ConnectView is run in standalone mode.

To change a ConnectView preference, choose File > Preferences. ConnectView opens the Preferences dialog box. Click the tab button for the desired option and specify the desired settings.

Setting Server Polling Intervals

The polling interval determines how often your network is polled for data. ConnectView displays data according to the server polling interval in the View All, View, Port Connections, and NCS Sessions windows. By default, the server polling interval is set to 5 minutes for each managed server. You can also force an immediate update of data by opening the desired window and then choosing View > Update (F5).

Note Data in the Port Status dialog box is updated every 2 seconds, independent of the server polling interval.

To change the polling intervals, click the Server Information tab in the Preferences dialog box. The polling options appear. Click the check box in the Polling? column for the desired servers, then enter the desired polling intervals

in minutes in the Polling Interval column. Acceptable values include 1 to 60 minutes.

Important

If you plan to manage many servers or servers over slow networks, consider using a high polling interval to reduce network traffic and improve network performance. In this case, you can always use the Update command (F5) to force an immediate update of the data as needed.

Either click another tab button to make additional changes or click OK to apply the changes and close the Preferences dialog box.

Click Cancel to close this dialog box without applying the changes.

Setting a Grace Period

ConnectView enables you to specify a minimum connection duration so that connections lasting less than the minimum duration are not used to calculate accounting and trend analysis data. By default, ConnectView sets the minimum connection duration at 30 seconds for each service.

To change the minimum connection duration, click the Grace Period tab button. The grace period options appear. Use the spin controls to set the desired grace period for each service. Valid settings include 0 to 999 seconds (approximately 17 minutes).

To make additional changes, click another tab button. To apply the changes and close the Preferences dialog box, click OK.

To close this dialog box without applying the changes, click Cancel.

Setting SNMP Options

ConnectView enables you to set workstation community strings for individual servers, SNMP time-out values, and SNMP retry values. By default, community strings on the ConnectView workstation are set for public access (monitor=public control=public). For SNMP GET and SET requests to be successful, the workstation community strings must match the community strings set on the managed server.

Important

By default, SNMP.NLM on the server side sets the server's MonitorCommunity to public but disables access to the ControlCommunity.

To change the SNMP options, click the SNMP Options tab button in the Preferences dialog box. The SNMP options appear.

To make additional changes, click another tab button. To apply the changes and close the Preferences dialog box, click OK.

To close this dialog box without applying the changes, click Cancel.

Chapter 3 *Displaying and Using Trend Analysis Data*

ConnectView™ enables you to display trend analysis data so you can analyze

- Maximum port usage (ports simultaneously in use)
- Connections by their
  - Direction (dial-in, dial-out, dialback)
  - Service (PPPRNS, NCS, ARAS)
  - Duration (in intervals of minutes)
  - Attempts

  Normal connections (successfully completed connections)
  Abnormal connections (involuntary disconnections)
  Dial-out failures (dial-out or dialback failures)
  Login failures (user login failures)
- Traffic (average bytes or packets sent and received per second)
- Usage by media (Asynchronous, ISDN, X.25, or other)

This chapter covers the following topics:

- "Preparing for Trend Analysis" on page 36
- "Displaying Trend Analysis Data" on page 37
- "Interpreting Trend Analysis Data" on page 39
- "Saving Trend Analysis Data" on page 53
- "Outputting Trend Analysis Data" on page 54

Preparing for Trend Analysis

Trend analysis enables you to monitor resource usage, proactively distribute resource utilization, and perform capacity planning. To effectively use this ConnectView feature, ensure that

- Audit trail files or archived files are available
- Server and workstation software is running
- An effective display period is used

Maintaining Audit Trail and Archive Files

Before displaying trend analysis data, ensure that the audit trail option is enabled and sufficient data has been recorded. Trend analysis data can be viewed only after the remote access software has recorded data in the current server's audit trail file, or there is access to data stored in an archived file. The audit trail file and/or archived files must be available before any trend analysis data can be displayed.

Because ConnectView uses the remote Btrieve client to access audit trail records, you must have READ/SCAN rights to the server's SYS:\SYSTEM\CSLIB directories in which the audit trail file and archived files are stored.

Important Ensure that only the audit trail file and archived files for the Novell® Internet Access Server 4.1 are used. ConnectView will not display data from other files.

Ensuring That Server and Workstation Software Is Running

For ConnectView to display trend analysis data, ensure that the following NetWare® Loadable ModuleTM (NLMTM) files are loaded on the managed server:

- BSPXCOM.NLM
- NCMA.NLM (NetWare ConnectTM Management Agent)
- SNMP.NLM (NetWare SNMP Agent)

Also, ensure that BREQUEST.EXE is running on the ConnectView workstation.

Planning for Data Display

Because accessing large amounts of data could require a substantial period of time and trend analysis graphs are not scrollable horizontally, plan the display of data in manageable amounts. For example, displaying trend analysis data from 8 a.m. to 5 p.m. in hourly intervals for one day or displaying data in daily intervals for 30 days results in manageable displays of data. However, displaying data in hourly intervals for a large number of days (60, for example) could result in long delays in data processing and data that is difficult to view.

If you are accessing large amounts of data in the current audit trail file and/or archived files, displaying trend analysis data could require a substantial amount of time and memory. Also, if low memory conditions occur and Windows is configured to swap data to disk, this could increase the amount of time required to process the data.

ConnectView enables you to display different views of the same data within one window, so you can analyze data from the same trend analysis category in a variety of ways. Refer to “Using the Trend Analysis Split Window” on page 38 for more information.

Displaying Trend Analysis Data

To access a Trend Analysis Data window, select a server in the View All window or a View window, or select a server name in the Server drop-down combo box in the left corner of the Tool Bar. Then, either click the Trend Analysis icon in the Tool Bar or choose Server > View Trend Analysis. ConnectView prompts you for starting and ending dates and then opens the Trend Analysis window for the specified period.

Note

Connections that terminate while the audit trail option is disabled and connections that terminate beyond the end date of the display period are not included in trend analysis data.

You can also open multiple views of the Trend Analysis window for the same server and the same display period by selecting the opened Trend Analysis window and choosing Window > New.

Important

If you are accessing large amounts of data in the current audit trail file and/or archived files, displaying trend analysis data could require a substantial amount of time and memory. Also, if low memory conditions occur and Windows is configured to swap data to disk, this could increase the amount of time required to process the data.

For sample Trend Analysis windows and explanations, see “Interpreting Trend Analysis Data” on page 39

Setting the Trend Analysis Display Options

When you are viewing trend analysis data, ConnectView enables you to customize the display of data with several display options. These options appear in the Trend Analysis Display Options dialog box. The available options vary depending on which trend analysis category is selected.

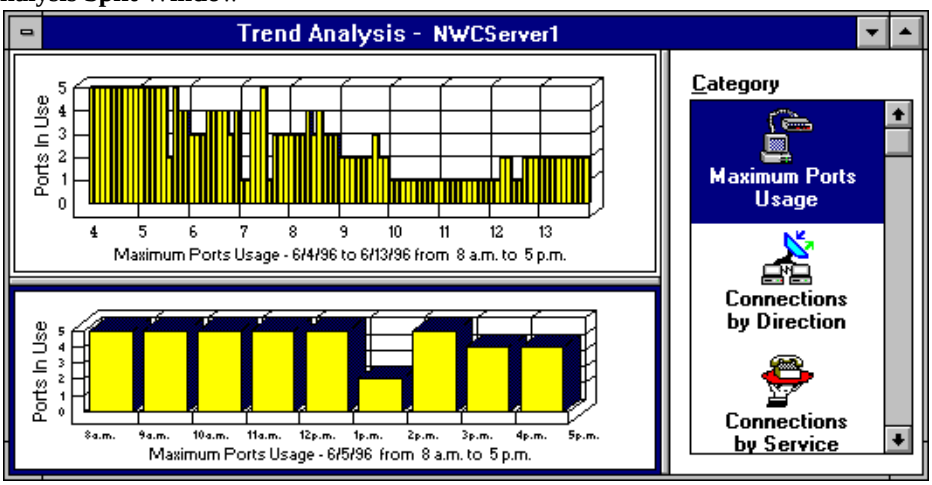
To access the Dialog boxes:Trend Analysis Display OptionsTrend Analysis Display Options dialog boxTrend Analysis Display Options dialog box, ensure that a Trend Analysis window is open and the desired graph is selected. Choose View > Display Options (F4). ConnectView opens the Trend Analysis Display Option dialog box. Specify the desired options and click the OK button.

Using the Trend Analysis Split Window

ConnectView enables you to display two views of data from the same trend analysis category within one window, so you can easily compare data from the same category for different intervals.

To display a split trend analysis window, position the cursor over the upper gray border of the window (just under the Title Bar) until it changes shape to parallel lines with two arrows. Press and hold the left mouse button. Drag the border to the desired position and release the mouse button. Click the icon for the desired category. Figure 3-1 shows an example split window with maximum port usage data.

Figure 3-1
Trend Analysis Split Window



To limit the data display in either graph, select the desired graph. A dark border appears around the selected graph. Choose View > Display Options (F4). ConnectView opens the Trend Analysis Display Options dialog box for the selected graph.

Note

If the Category list box is in focus and you have split windows, a dialog box appears so you can specify to which graph to apply the display options.

Interpreting Trend Analysis Data

This section contains sample Trend Analysis windows to help you interpret and analyze the trend analysis data you collect.

Note

The grace period or minimum connection duration needed for a connection to be included as trend analysis data can be set in the Grace Period page of the Preferences dialog box. To access this dialog box, choose File > Preferences. By default, the grace period is set at 30 seconds.

Maximum Ports Usage Graphs

Maximum ports usage graphs show the maximum number of ports in use simultaneously during the display period to enable you to monitor port utilization, perform capacity planning, and evenly distribute port usage across Novell Internet Access Server 4.1 servers running the remote access software.

To obtain this data, ConnectView checks the recorded status of each port for each minute of the display period. If a port was accessed during a minute, ConnectView counts the port as used during that minute. Then, ConnectView compares the number of ports used during each minute for a 60 minute interval and selects the highest value as the maximum port usage for that hour. This process is repeated for each hour of the display period. The highest hourly value within a 24 hour period is then used as the daily maximum port usage.

Note

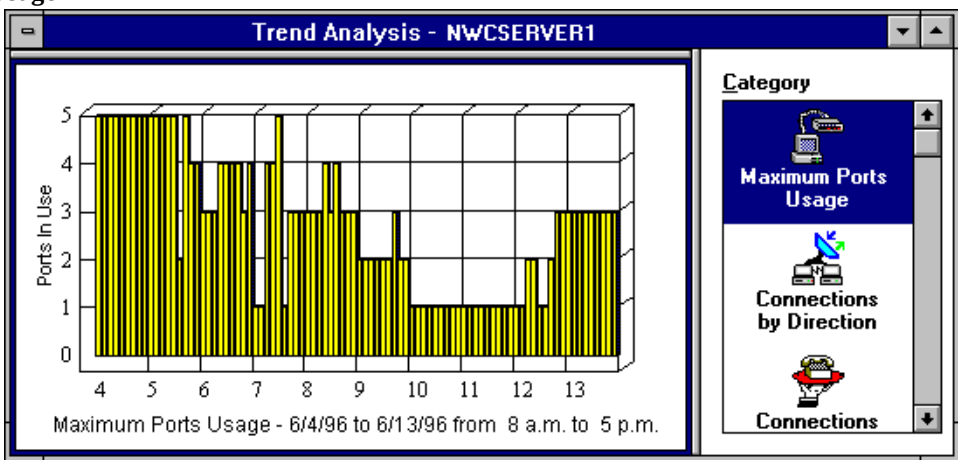
Because it is unlikely a port will be used more than once per minute, ConnectView uses a minute interval to check for port usage. If a port happens to be used more than once during a minute, the port usage data will be inaccurate. Also, ConnectView considers only complete connections, so if a port is in use when the port usage data is calculated, it will not be counted.

If a port is accessed more than once per minute, ConnectView counts it as being used only once during the minute interval.

To display maximum ports usage data, click the Maximum Ports Usage icon in the Category list box. By default, data is displayed at hourly intervals from 8 a.m. to 5 p.m. for each day for the specified dates.

Figure 3-2 shows a sample Trend Analysis window for ports usage on server NWCServer1. To change the time of day and display interval, ensure the desired graph is selected and choose View > Display Options (F4).

Figure 3-2
ExampleTrend Analysis Windowfor Maximum Ports Usage



From this example, you can see that the maximum ports usage on the server NWCServer1 is displayed from 8:00 a.m. to 5:00 p.m for 10 days (6/4/96 to 6/

13/96). This data indicates that a maximum of five ports were in use simultaneously on 6/4. Only one port was used on 6/10 and 6/11. If the remote access software is licensed for eight ports, this data suggests that port utilization is greater than 50 percent of the available port licenses for more than two days.

Note

Maximum ports usage does not reflect the number of sessions using the ports.

Setting Display Options for Maximum Ports Usage, Connections by Direction, Connections by Service, and Connection Attempts Graphs

When you are viewing maximum ports usage, connections by direction, connections by service, and connection attempts data, ConnectView enables you to customize the display of data within the originally specified start and end dates by changing the

- Start date
- Number of days for which data is displayed
- Time of day for which data is displayed (individual hours or all day [24 hours])
- Interval by which data is displayed (hourly or daily)
- Graph style

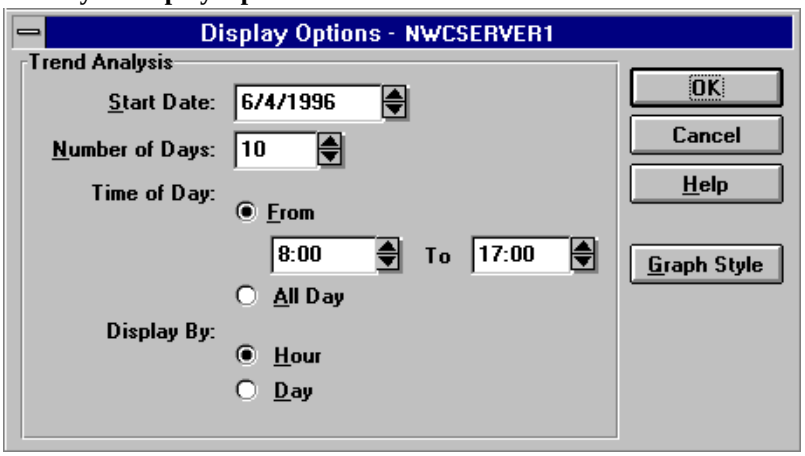
Important

Displaying connection data by hour shows the number of connections that were established during the displayed hours. If a connection crosses hours, the connection will be counted in each hourly interval that it crosses. In this case, the total number of connections could exceed the total when the data is displayed by a daily interval.

To access the Trend Analysis Display Options dialog box, ensure that the desired graph is selected and choose View > Display Options (F4). ConnectView opens the Trend Analysis Display Option dialog box, shown in Figure 3-3 .

Figure 3-3

Example Trend Analysis Display Options



Specify the desired options and click the OK button.

Connections by Direction Graphs

Connections by Direction graphs help you determine the number of dial-in, dial-out, and dialback connections made during a specified period, monitor resource usage, and evenly distribute dial-in, dial-out, and dialback users for more efficient performance.

ConnectView counts the number of valid dial-in, dial-out, and dialback connections that occurred during each hour of the display period. The hourly totals for each twenty-four hour period within the display period are then added together for the daily totals. For a connection to be valid for this trend analysis category, both a start connection record and an end connection record must be found within the display period.

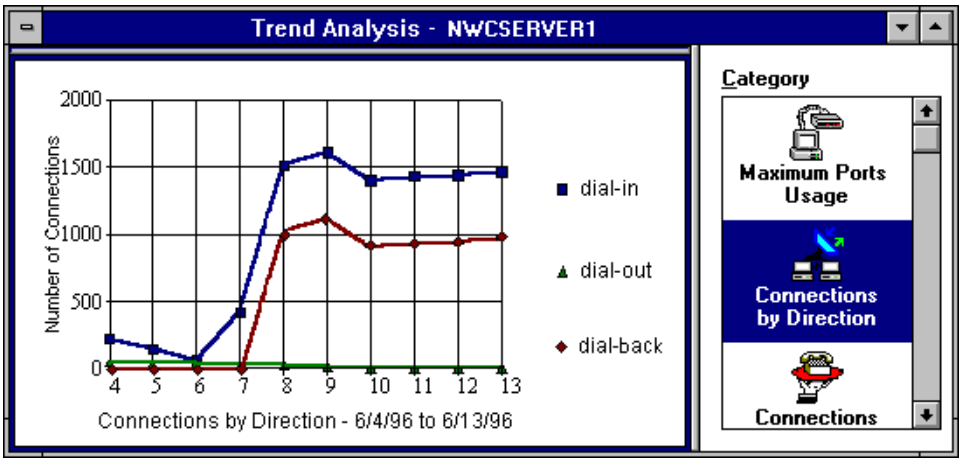
Important

Within the same display period, the number of valid connections for this category might not match the number of valid connections for the Connections by Service, Connection Attempts, and Connection Duration categories. Connection Direction graphs require both a start connection record and an end connection record within the display period. These other categories require that valid connections have only an end connection record within the display period.

To display connections-by-direction data, click the Connections by Direction icon in the Category list box. By default, this graph shows the number of connections by direction on a daily interval.

Figure 3-4 shows a sample Trend Analysis window with connections by direction data.

Figure 3-4
Example Trend Analysis Windowfor Connections by Direction



In this example, you can see the number of dial-in, dial-out, and dialback connections made between 6/4/96 and 6/13/96 on server NWCServer1. This data indicates that approximately 1,500 dial-in connections and 1,000 dialback connections were made each day between 6/8 and 6/13, while there were few dial-out connections during the display period.

To change the display options for connections by direction data, choose View > Display Options (F4). For an example Display Options dialog box, see Figure 3-3 on page 42 .

Connections by Service Graphs

Connections by Service graphs provide data to enable you to track service usage and proactively plan for service expansion.

ConnectView counts the number of valid connections for each service that occurred during each hour of the display period. The hourly totals for each twenty-four hour period within the display period are then added together for the daily totals. For a connection to be valid for this trend analysis category, only an end connection record must be found within the display period.

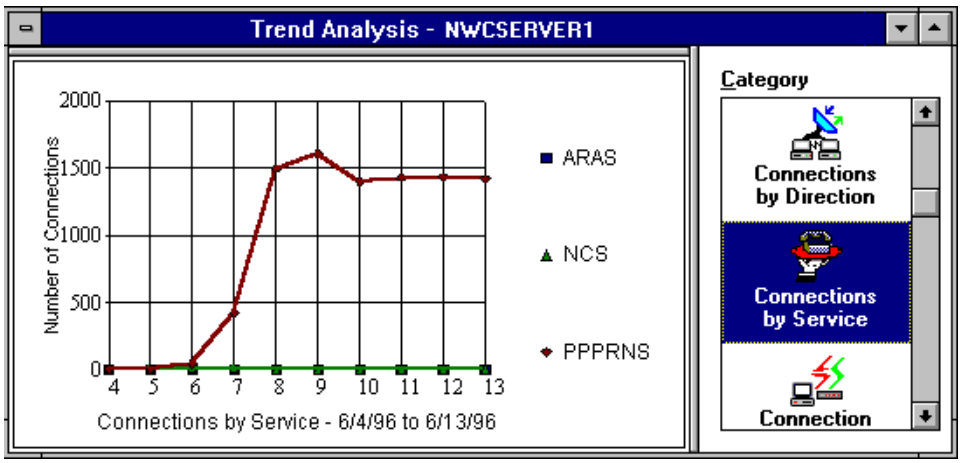
Important

Within the same display period, the number of valid connections for this category might not match the number of valid connections for the Connections by Direction, Traffic Statistics, and Usage by Media categories. Connections by Service graphs require only an end connection record within the display period. These other categories require that valid connections have both a start connection record and an end connection record within the display period.

To display connections-by-service data, click the Connection by Service icon in the Category list box. By default, this graph displays the daily number of connections by service.

Figure 3-5 shows a sample Trend Analysis window with connections by service data.

Figure 3-5
Example Trend Analysis Windowfor Connections by Service



In this example, you can see that connections were made using the PPPRNS service from 6/6/96 to 6/13/96 on the server NWCServer1. No AppleTalk Remote Access Services (ARAS) or NASI™ Connection Service (NCS) connections occurred throughout the period.

Note

The remote access services that are configured and loaded on the server or recorded in the audit trail file appear in this graph.

To change the display options for connections by service data, ensure the desired graph is selected and choose View > Display Options (F4). For an example Display Options dialog box, see Figure 3-3 on page 42 .

Connection Attempts Graphs

Connection attempts graphs show the number of normal connections, abnormal connections, dial-out failures, and login failures on a server. These graphs help you monitor how successful users are in establishing their connections and assess connection and security problems during this period. Table 3-1 describes the connection attempt categories.

Table 3-1 Connection Attempt Categories

Connection Category	Description
Normal Connection	Successful dial-in, dial-out, and dialback connections that terminated in an orderly fashion.
Abnormal Connection	Connections that were terminated in a disorderly fashion, without user initiation. Possible causes are line failure, transmission error, maximum idle time or user connection time exceeded limit, port or session reset by administrator, or service or driver unloaded.
Dial-out Failure	Dial-out or dialback connection failed. Possible causes are that the number was busy, port or service was unavailable, or access was restricted.
Login Failure	User login attempt failed. Possible causes are invalid username or password, unauthorized NetWare or remote access software access, or that the login was disabled.

Important

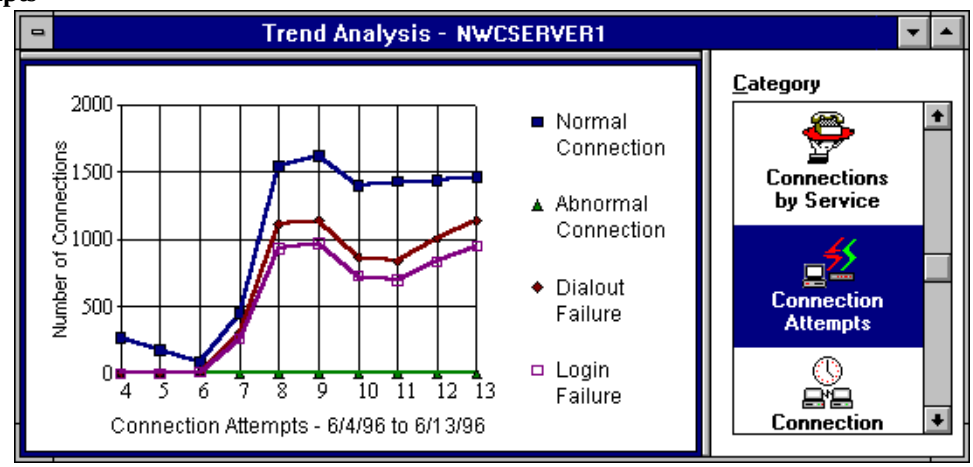
Within the same display period, the number of valid connections for this category might not match the number of valid connections for the Connections by Direction, Traffic Statics, and Usage by Media categories. Connection Attempts graphs require only an end connection record within the display period. These other categories require that valid connections have both a start connection record and an end connection record within the display period.

To display connection attempts data, click the Connection Attempts icon in the Category list box. The connection attempts graph shows daily connection attempts from the specified start date to the specified end date.

Figure 3-6 shows a sample Trend Analysis window with connection attempts data.

Figure 3-6

Example Trend Analysis Windowfor Connection Attempts



In this example, you can see that there were approximately 1,500 successful connections each day between 6/8/96 and 6/13/96 on the server NWCServer1. Also, notice that during this period a number of dial-out failures and login failures occurred. There were no abnormal connections during the display period.

To change the display options for connection attempts data, ensure that the desired graph is selected and choose View > Display Options (F4). For an example Display Options dialog box, see Figure 3-3 on page 42 .

Connection Duration Graphs

Connection duration graphs enable you to track connection durations and patterns in connection durations. This data can help you to set duration standards and monitor the amount of time users are connected to the remote access software.

For each day of the display period, ConnectView counts the number of connections with connected times within each duration interval. Connection times are calculated in seconds and then converted to minutes. The number of connections within each connection duration interval provides the daily totals. For a connection attempt to be valid for this trend analysis category, only an end connection record must be found within the display period.

Important

Within the same display period, the number of valid connections for this category might not match the number of valid connections for the Connections by Direction, Traffic Statics, and Usage by Media categories. Connection Duration graphs require only an end connection record within the display period. These other categories require that valid connections have both a start connection record and an end connection record within the display period.

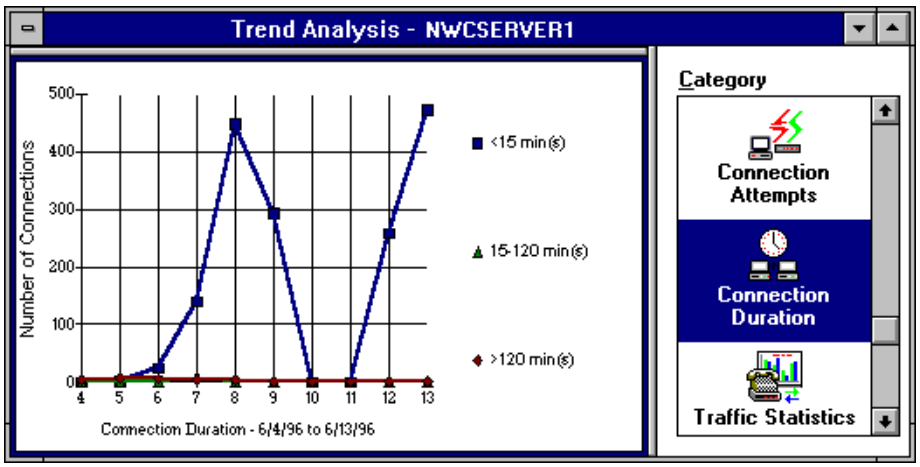
To display connection duration data, click the Connection Duration icon in the Category list box.

Note

This data can be viewed only on a daily basis.

Figure 3-7 shows a sample Trend Analysis window with connection duration data. By default, this graph shows the number of connections established for less than 15 minutes, between 15 and 120 minutes (2 hours), and more than 120 minutes. Also, data is displayed daily from the specified start date to the specified end date.

Figure 3-7
Example Trend Analysis Windowfor Connection Duration



In this example, you can see the duration of connections between 6/4/96 and 6/13/96 on the server NWCServer1. This data indicates that almost all connections were established for less than 15 minutes.

Setting Display Options for Connection Duration Graphs

When you are viewing connection duration data, ConnectView enables you to customize the display of data within the originally specified start and end dates by changing the

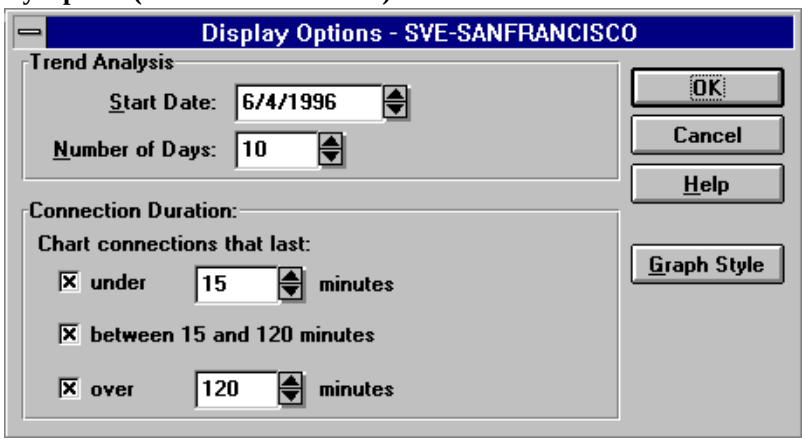
- Start date
- Number of days for which data is displayed
- Under (less than) duration setting
- Over (greater than) duration setting
- Graph style

Note

This data can be displayed only in daily intervals.

To access the Trend Analysis Display Options dialog box, ensure that a connection duration graph is selected and choose View > Display Options (F4). ConnectView opens the Trend Analysis Display Options dialog box, shown in Figure 3-8 . Specify the desired options and click the OK button.

Figure 3-8
Example Display Options(Connection Duration)



Traffic Statistics Graphs

Traffic statistics graphs help you monitor traffic patterns, anticipate periods of heavy or light traffic, and more evenly distribute traffic across your remote access servers.

These graphs show the number of connections in groups of the average traffic patterns. Traffic consists of the number of kilobytes or kilopackets sent and received per second. To determine the level of traffic, the total number of bytes or packets is divided by the number of seconds in the connection duration. The resultant rates of traffic are then grouped according to intervals. For a connection to be valid for this trend analysis category, both a start connection record and an end connection record must be found within the display period.

Important

Within the same display period, the number of valid connections for this category might not match the number of valid connections for the Connections by Service, Connection Duration, and Connection Attempts categories. Traffic Statistics graphs require both a start connection record and an end connection record within the display period. These other categories require that valid connections have only an end connection record within the display period.

By default, the traffic intervals start at 0.1 KBps (100 bytes) and continue for 10 intervals. The display options allow you to adjust these intervals and display values and to display data for Kilopackets sent and received.

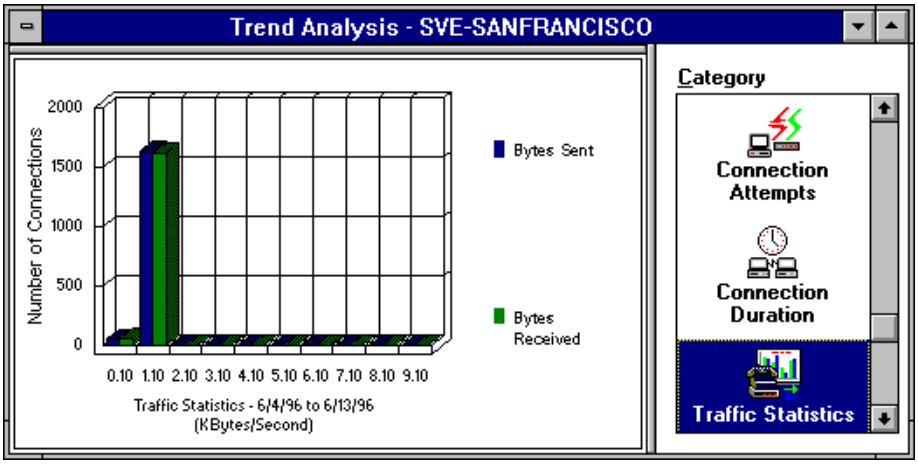
Note

This data can be displayed only in daily intervals.

To display traffic statistics, click the Traffic Statistics icon in the Category list box.

Figure 3-9 shows a sample Trend Analysis window with traffic statistics data.

Figure 3-9
Example Trend Analysis Windowfor Traffic Statistics



In this example, you can see that all connections between 6/4/96 and 6/13/96 on the server NWCServer1 had less than 2 KBps of traffic.

Setting Display Options for Traffic Statistics

When viewing traffic statistics data, you can customize the display of data based on the originally specified start and end dates by changing the

- Start date
- Number of days for which data is displayed
- Traffic statistics
- Starting interval
- Interval size
- Number of intervals

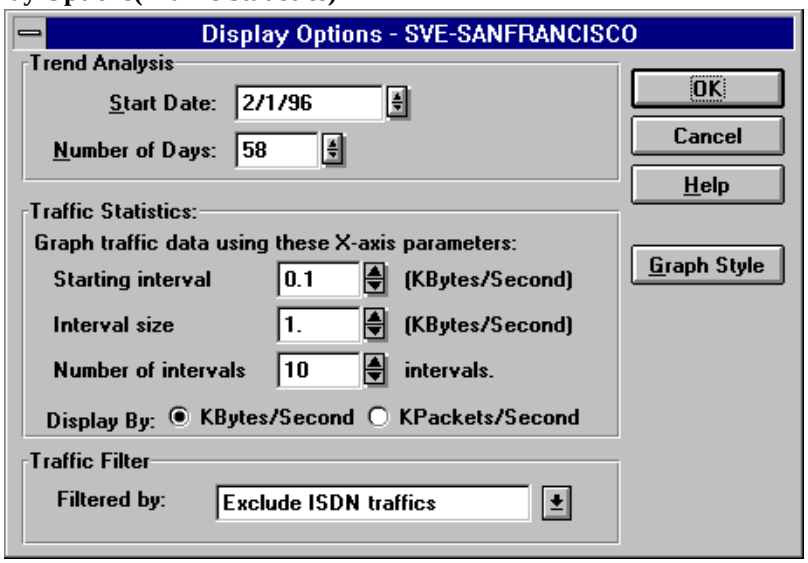
- Data display for kilobytes per second (KBytes/Second) or kilopackets per second (KPackets/Second)
- Traffic filter (ISDN only, ISDN and others, non-ISDN only)
- Graph style

Note

This data can be displayed only in daily intervals.

To access the Trend Analysis Display Options dialog box, ensure that a traffic statistics graph is selected and choose View > Display Options (F4). ConnectView opens the Trend Analysis Display Option dialog box, shown in Figure 3-10 . Specify the desired options and click the OK button

Figure 3-10
Example Display Options(Traffic Statistics)



Usage by Media Graphs

Usage by media graphs help you monitor media usage, analyze media usage patterns, and distribute media utilization across your remote access servers.

These graphs contain pie charts that show the percentage of data traffic and the percentage of connections by media groups. Media groups are defined as analog, ISDN, X.25, and other. Other refers to remote access connections that use a media type different from those listed.

Note Media type is not supported by NetWare Connect 2.0 servers. Connections to NetWare Connect 2.0 servers will show the media type as other.

ConnectView counts the amount of traffic in kilobytes and the number of connections for each media type for each day of the display period. The resultant totals are then divided by the total amount of traffic and the total number of connections, respectively. For a connection to be valid for this trend analysis category, both a start connection record and an end record must be found within the display period.

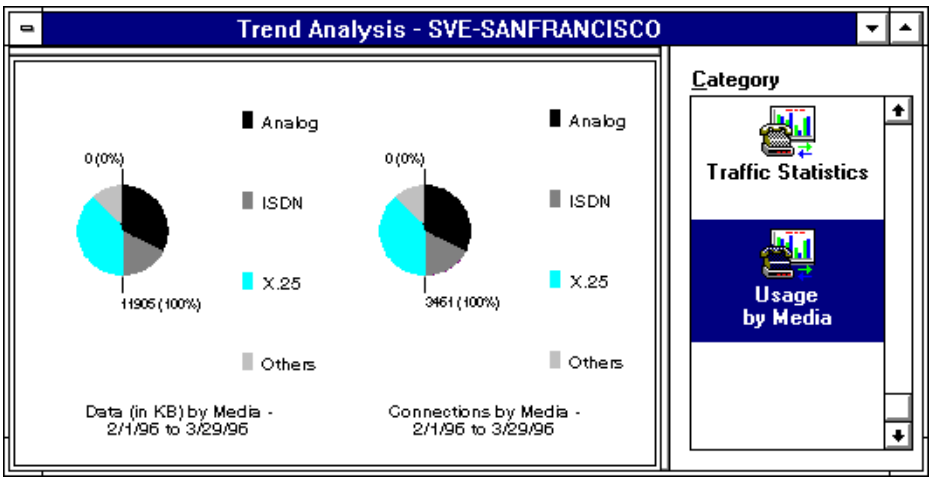
Important Within the same display period, the number of valid connections for this category might not match the number of valid connections for the Connections by Service, Connection Duration, and Connection Attempts categories. Usage by Media graphs require both a start connection record and an end connection record within the display period. These other categories require that valid connections have only an end connection record within the display period.

To display media usage data, click the Usage by Media icon in the Category list box.

Note This data can be displayed only in daily intervals. You can choose View > Display Options to adjust the dates of the displayed data.

Figure 3-11 shows a sample Trend Analysis window with usage by media data.

Figure 3-11
Example Trend Analysis Windowfor Usage by Media



In this example, you can see that most data traffic (40%) on the server San Francisco during the period 2/1/97 to 3/29/97 was analog traffic. Also, most connections (40%) were established for analog connections.

Note

Because the numerical values for traffic and connections are displayed in the graphs, the hot graph feature is disabled for this trend analysis category.

Saving Trend Analysis Data

ConnectView enables you to save trend analysis data to a file so that you can view trend analysis graphs independent of the server's audit trail and archived files.

To save trend analysis data, open the Trend Analysis window for the desired period and choose File > Save Trend Analysis. ConnectView prompts you for a path and filename and then saves the data for the specified period to a trend analysis file. Trend analysis files have a .TAD extension.

To access a previously saved trend analysis file, choose File > Open Trend Analysis. The File Open dialog box appears. Specify the desired trend analysis file (file with a .TAD extension) and click OK. ConnectView opens the Trend Analysis window and displays the saved data.

Note Use the DOS command or Windows File Manager to delete trend analysis files.

Outputting Trend Analysis Data

ConnectView enables you to print the graphs from any Trend Analysis window, copy the trend analysis graph in bit map or text format to the Windows clipboard, or export trend analysis data in tab-delimited format. This capability allows you to create and maintain trend analysis records for detailed reports and analyses.

Copying Trend Analysis Data

To copy graphs from a Trend Analysis window in text or bit map format, select the category you wish to copy. A dark border appears around the selected graph. Choose Edit > Copy. ConnectView prompts you to choose graph or bit map format. Select the desired format and click OK.

ConnectView copies the graph data in the specified format to the Windows clipboard. You can then paste the text or bit map into other applications.

Printing Trend Analysis Data

To print a graph from a Trend Analysis window, select the category you wish to print. A dark border appears around the selected graph. Choose File > Print. ConnectView prints the selected graph.

Important To print graphs, some printers could require configuration changes.

Exporting Trend Analysis Data

To export trend analysis data, select the trend analysis category you wish to export. A dark border appears around the selected graph. Choose File > Export. ConnectView prompts you to specify a filename and path. Specify the desired path and click the OK button.

ConnectView exports data in tab-delimited format to the specified file. You can then import the data into other applications for additional analysis.

Chapter 4 *Setting Up Accounting Profiles and Generating Billing Charges*

ConnectViewTM enables you to create a basic accounting system for remote access software users. This accounting system enables you to compose a billing formula, enter charge rates, view sample charges for verification, assign accounting profiles and account numbers to users, and generate billing charges and display them.

An accounting profile contains the specified billing formula and the specified rate tables used to calculate accounting charges. ConnectView allows you to set up multiple accounting profiles based on your users and network needs and apply these profiles to users.

By default, the DEFAULT.NCP accounting profile is assigned to all users (<DEFAULT >). Although you still need to specify a billing formula and enter rates for this profile, you have to create new accounting profiles only for nondefault users. Accounting data can be displayed by username or account number. This data can then be displayed in a table or report format, copied or printed, and exported.

This chapter covers the following topics:

- "Preparing for Accounting" on page 56
- "Understanding How Accounting Data Is Calculated" on page 57
- "Setting Up Accounting Profiles" on page 61
- "Assigning Accounting Profiles and Account Numbers to Users" on page 74
- "Displaying Billing Charges" on page 78
- "Printing, Copying, and Exporting Accounting Data" on page 87

Preparing for Accounting

The ConnectView accounting feature allows you to create account profiles with specific billing formulas and rates, apply profiles to users, and generate accounting data in accounting log and accounting report format. To effectively use this feature, ensure that

- Audit trail file and/or archived files are available
- Server and workstation software is running
- Data processing and display requirements are considered

Maintaining Audit Trail and Archive Files

Before starting the accounting process, ensure the audit trail option is enabled and sufficient data has been recorded. Accounting data can be viewed only if there is data recorded in the current server's audit trail file or there is access to data stored in archived files. The audit trail file and/or archived files must be available for the specified billing period to display accounting data.

Because ConnectView uses the remote Btrieve client to access audit trail records, you must have Read/Scan rights to the server's SYS:\SYSTEM\CSLIB directories where the audit trail file and archived files are stored.

Important

Ensure that only the audit trail file and archived files from Novell® Internet Access Server 4.1 or NetWare® ConnectTM 2.0 are used. ConnectView will not display data from other files.

Ensuring Server and Workstation Software Is Running

For ConnectView to process accounting data, ensure the following NetWare Loadable ModuleTM (NLMTM) files are loaded on the managed server:

- BSPXCOM.NLM
- NCMA.NLM (NetWare Connect Management Agent)
- SNMP.NLM (NetWare SNMP Agent)

Also, ensure that BREQUEST.EXE is running on the ConnectView workstation.

Planning for Data Processing and Display Requirements

Because processing and displaying large amounts of accounting data could require a substantial period of time, plan to process and display data in manageable periods of time. Extremely large amounts of audit trail data and slow network connections will increase the amount of time required to process and display the data.

Also, large amounts of audit trail data from the current or archived audit trail files could also require a substantial amount of memory. If low memory conditions occur and Windows is configured to swap data to disk, this could increase the amount of time required to process and display accounting data.

Note To improve display times and data interpretation, ConnectView allows you to customize the display of data in the Accounting Report window. See"Customizing the Accounting Report" on page 85 for more information.

Understanding How Accounting Data Is Calculated

To calculate billing charges, ConnectView

- Matches start connection records with end connection records to determine the valid connections that occurred during the billing period.
- Applies the rates from the rate tables to the hourly intervals of the connection durations.

The following sections explain how accounting data is calculated in more detail.

Matching Start Connection and End Connection Records

ConnectView determines valid connections within the specified billing period by matching start connection records and end connection records.

If both a start connection record and an end connection record are found within the billing period for the same connection ID, ConnectView logs the connection as valid. Otherwise, ConnectView considers the connection incomplete and does not use the connection in the accounting process.

If a start connection record is found, but a matching end connection record cannot be located within the specified billing period, ConnectView searches for the end connection record one day beyond the end date of the billing period. If the matching end connection record is found within this 1-day buffer, ConnectView logs the connection as valid. If the matching end connection record is not found during the one day buffer, ConnectView considers the connection invalid and logs the connection in the Discarded Connections dialog box.

Note

Checking for end connection records during this 1-day buffer helps eliminate incomplete connections that might occur when connections are started near the end of the billing period.

If an end connection record without a matching start connection record is found within the specified billing period, ConnectView considers the connection invalid and logs the end connection record in the Discarded Connections dialog box. Logging the unmatched end connection records avoids duplicating billing and invalid connections across billing periods.

Note

The grace period, by default set to 30 seconds, determines the minimum connection duration required for a connection to be valid.

The following table summarizes the process of determining valid connections for a connection that began on 3/1/96 at 8:00 a.m. and ended at 3/4/96 at 3:00 p.m.

Billing Period	Accounting Result
3/1/96 to 3/4/96	Valid Connection The connection is included in the accounting data, because both the start time and the end time are within the billing period.
3/1/96 to 3/3/96	Valid Connection The connection is included in the accounting data, because the start time is within the billing period and the end time is outside the billing period by less than one day.

Billing Period	Accounting Result
3/1/96 to 3/2/96	Invalid Connection. The connection is counted as an incomplete connection, because the start time is within the billing period, but the end time is outside the billing period by more than one day. The start connection record is logged in the Disacarded Connections dialog box.
3/2/96 to 3/2/96	Invalid Connection The connection is not included in the accounting data, because neither the start time nor the end time is within the billing period.
3/2/96 to 3/4/96	Invalid Connection The connection is not included in the accounting data and is not counted as an incomplete connection, because the start time is outside the billing period, even though the end time is within the billing period. The end connection record is logged in the Discarded Connections dialog box.

Applying Rates to Connection Durations

After the valid connections are determined, ConnectView applies the billing rates from the assigned accounting profiles to the connection durations.

For charges based on the rate per minute, ConnectView determines the amount of time in seconds that applies to each hourly interval within the connection duration. Next, ConnectView checks the hourly rates in the assigned accounting profile and applies the rates. The cost of each hourly interval is then added together to equal the total charge for the connection.

For charges based on rate per connection and overhead rate, ConnectView checks the assigned accounting profile for rates and charges, determines the connected time in seconds for each hourly interval of the billing period, and applies the assigned rates. The costs of each hourly interval are then added together to equal the total charge for the connection.

The following connection example illustrates this process.

Connected Time	Hourly Intervals	Rates per Minute	Rates per Second	Connected Seconds per Interval	Total Charges
3:30:35 p.m.– 5:30:10 p.m.	3:00–3:59 4:00–4:59 5:00–5:59	0.60 0.60 0.50	0.01 0.01 0.008	1765 3600 1790	1765 x .01 = 17.65 3600 x .01 = 36.00 1790 x .008 = 14.32 Total Charge = $67.97
09:00:10 a.m.– 09:54:31 a.m.	9:00–9:59	0.30	0.005	3281	3281 x .005 = 16.40 Total Charge = 16.40
11:30:15 a.m.– 2:45:03 p.m.	11:00–11:59 12:00–12:59 1:00–1:59 2:00–2:59	0.85 0.85 0.85 0.85	0.01 0.01 0.01 0.01	1815 3600 3600 2703	1815 x .01 = 18.15 3600 x .01 = 36.00 3600 x .01 = 36.00 2703 x .01 = 27.03 Total Charge = 117.18

Important

Baud rate and port name rates assigned in accounting profiles do not apply to NCS dial-out and AIOPAD connections. NCS and AIOPAD do not report the baud rate used during these connections.

Handling Invalid Connections and Duplicate Connection IDs

Invalid connections are connections for which ConnectView can find only one connection record, but cannot locate the matching start or end connection record.

ConnectView automatically checks for end connection records up to one day after the end date of the billing period. If a matching end connection record is found in the one day after the billing period end data, ConnectView logs the connection as valid and includes the connection in accounting data for the specified billing period. If the matching end connection record is not found, ConnectView counts the connection as invalid. Invalid connections are not included in the accounting data for the specified period, but they are logged in the Invalid Connections dialog box.

Note

Because of the checking one day beyond the end date of the billing period and to avoid duplicate billing, ConnectView discards any end connection records for which a matching start connection record cannot be found.

Duplicate connection IDs occur when a new connection record contains the same connection ID as an existing connection record of the same type. When this occurs, ConnectView displays a warning message and allows you to terminate or continue the accounting process.

If the accounting process is continued, ConnectView cannot guarantee the integrity of the accounting data.

Setting Up Accounting Profiles

Accounting profiles define how charges will be calculated with a billing formula and rates. First, specify the desired billing formula (Step 1). Then enter the desired rates (Step 2). After the billing formula and rates have been entered, view sample charges to verify that the formula and rates are correct (Step 3).

A billing formula can be based on one or more of the following categories

- Rate per minute based on connection duration

  Length of the connection multiplied by the rate per minute, based on:

  - Time-of-day

    Intervals of 60 minutes from 0:00 a.m. to 11:59 p.m., for each day of the week and holidays

  - Baud rate

    Connection speeds in bits per second (bps)

  - Port

    Port names and available speeds

  - Services

    Remote access services available on the current server

- Rate per connection

  Rate for each connection based on baud rate, service, or port

- Overhead Rate

A flat-rate charge applied to the users assigned to the profile with valid remote access software connections. A check box is available to apply this charge to all users assigned to the profile, including those without valid connections.

After the billing formula and rates are specified, accounting profiles are saved as files with .NCP extensions. Accounting profiles can be saved locally or on a network drive. You can then assign users to the saved profiles.

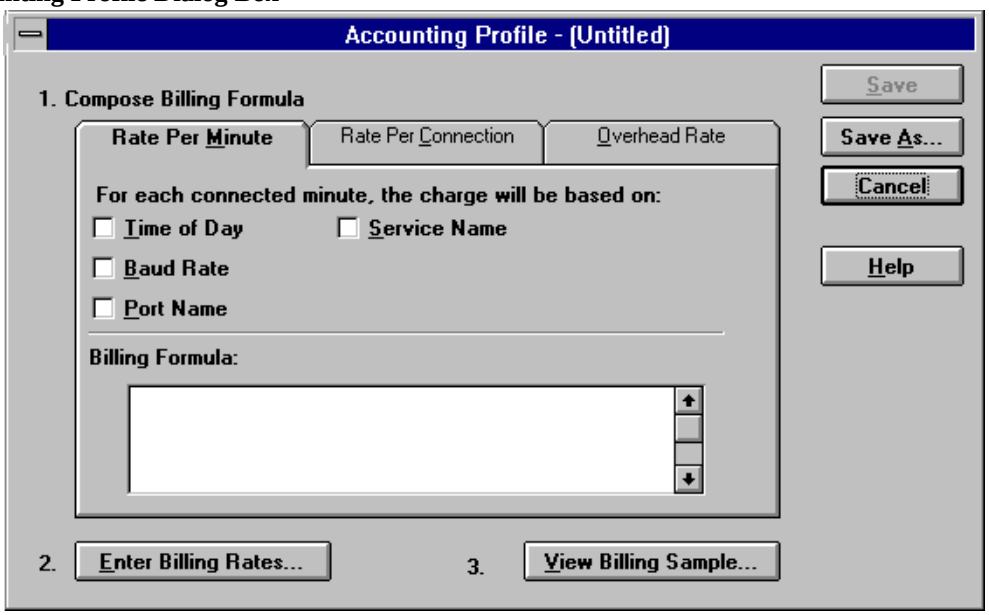
Note

To delete unwanted accounting profiles, use the DOS command or Windows File Manager.

You can create multiple accounting profiles and apply them to different users as necessary. By default, ConnectView creates an accounting profile called DEFAULT.NCP, with no billing formula or rates. This default accounting profile is assigned to all users. However, you must specify the desired billing formula and enter the billing rates to generate meaningful charges.

To access the Accounting Profile dialog box, select a server icon in the View All window or a View window, or select a server name in the Server drop-down combo box in the left corner of the Tool Bar. Then, choose Accounting > Create Profile or, if an accounting profile has already been saved, Accounting > Edit Profile. ConnectView opens the Accounting Profile dialog box, shown in Figure 4-1 .

Figure 4-1
Accounting Profile Dialog Box



In this dialog box, you can use the tab buttons to specify the desired billing formula. The current billing formula appears in the lower section of this dialog box.

Note

The display in the Billing Formula list box changes as you select or deselect the desired charges, but cannot be edited.

ConnectView enables you to create or change billing formulas based on rate tables for time of day, baud rate, port, and service, as well as an overhead rate.

Setting the Rate per Minute Charge

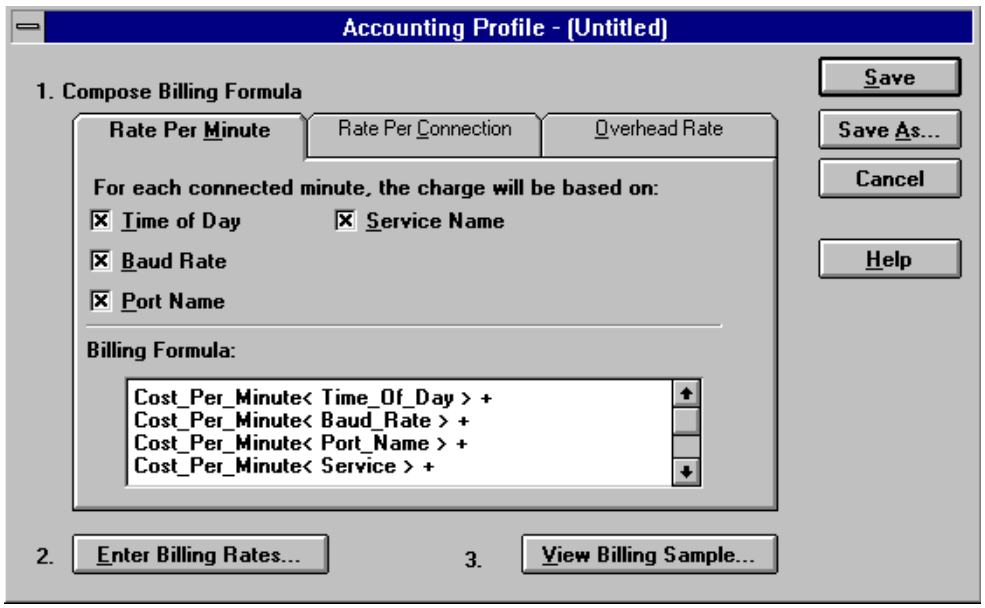
Rate per minute is a charge applied to users based on any or all of the following costs:

- Time of day the connection was made
- Baud rate or connection speed
- Individual port accessed

- Remote access service used

To access the Rate Per Minute settings, click the Rate Per Minute tab button in the Accounting Profile dialog box. ConnectView displays the rate per minute options, shown in Figure 4-2 .

Figure 4-2
Account Profile Dialog Boxwith Rate Per Minute Options



Click the desired check boxes for the rate tables you want to use. Click a tab button to display additional billing formula options.

To close this dialog box and accept all changes, click the Save or Save As button. To close this dialog box without applying any changes, click the Cancel button.

Note

To enter rates for the rate per minute based on baud rate, port name, time of day, and type of service, click the Enter Billing Rates button (Step 2) and then click the desired tab buttons.

Setting the Rate per Connection Charge

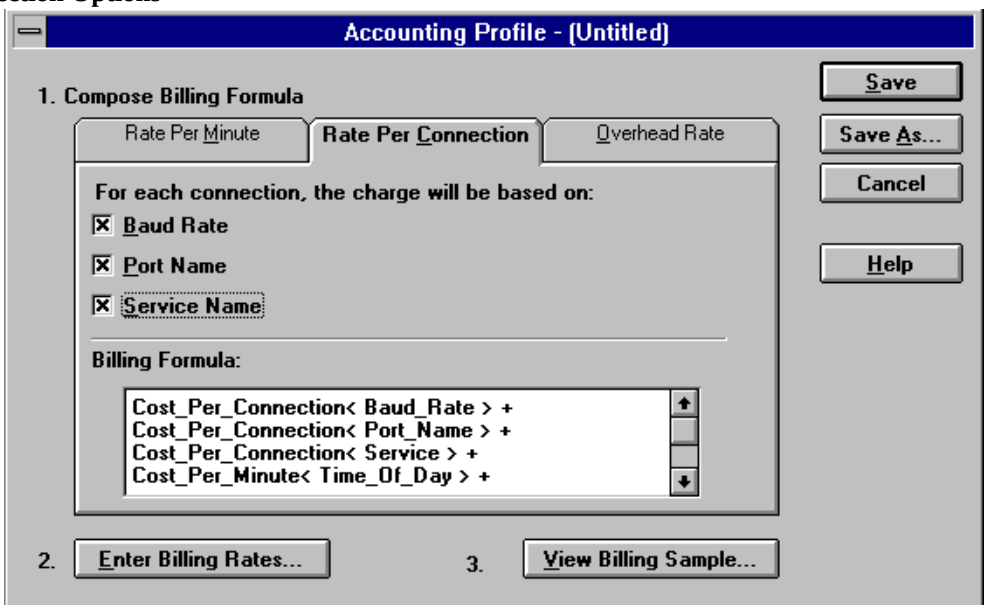
Rate per connection is a flat-rate charge based on any or all of the following:

- Baud rate of the connection
- Individual port and connection speed used in the connection
- Remote access service used for the connection

This rate is applied to all users each time they connect to the current remote access software, regardless of the duration of the connection.

To access the Rate Per Connection settings, click the Rate Per Connection tab button in the Accounting Formula dialog box. ConnectView displays the rate per connection options, shown in Figure 4-3 .

Figure 4-3
Accounting Profile Dialog Boxwith Rate per Connection Options



Click the desired check boxes for the rate tables you want to use.

To close this dialog box and accept all changes, click the Save or Save As button. To display additional billing formula options, click a tab button. To close this dialog box without applying any changes, click the Cancel button.

Note

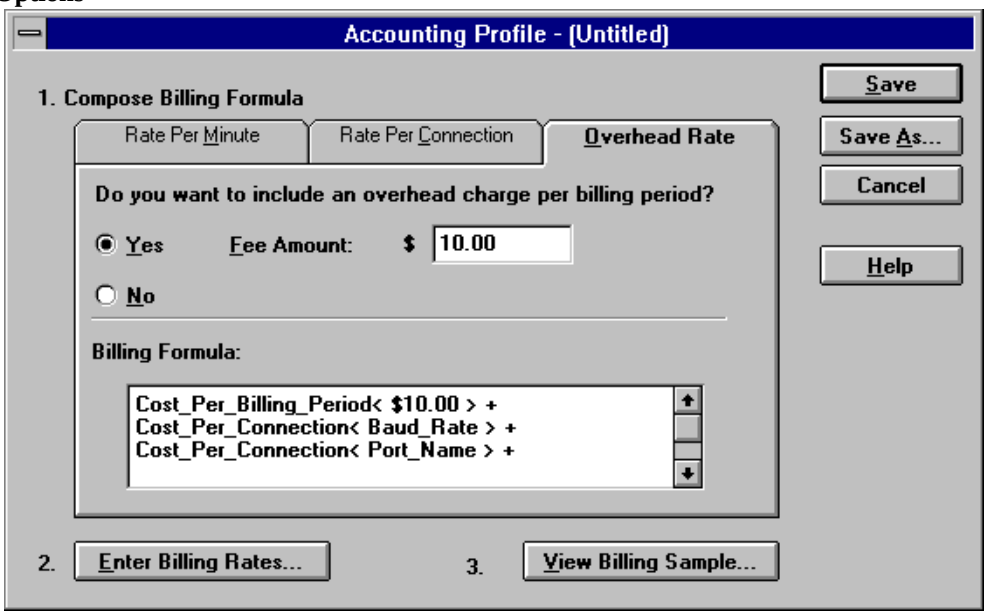
To enter rates for the rate per connection based on baud rate, port name, and type of service, click the Enter Billing Rates button (Step 2) and then click the desired tab buttons.

Setting the Overhead Rate Charge

Overhead rate is a flat-rate charge applied to all remote access software users assigned to the profile during the specified billing period. Alternatively, this charge can be applied to all users assigned to the profile, including those without valid remote access connections during the billing period.

To enter a rate per billing period, click the Overhead Rate tab button. ConnectView displays the overhead rate options, shown in Figure 4-4 .

Figure 4-4
Accounting Profile Dialog Boxwith Overhead Rate Options



If you want to use a flat-rate access fee or rate per billing period charge, click the Yes radio button and enter the desired charge.

Note

Rates must begin with an integer, for example 0.50 or 1.20. A leading decimal point will not be accepted.

To close this dialog box and accept all changes, click the OK button. To display additional billing formula options, click a tab button. To close this dialog box without applying any changes, click the Cancel button.

Entering Billing Rates

ConnectView enables you to enter rates (Step 2) for any or all of the following:

- Time of day for 24-hour intervals for each day and holiday
- Baud rates by connection speeds on a per minute or per connection basis
- Individual ports by port speeds on a per minute or per connection basis
- Remote access services on a per minute or per connection basis

Note Time of day and holiday rates apply only to the rate per minute billing formula.

Important Because NCS cannot report the baud rate used for its dial-out connections, baud rate and port name charges do not apply to NCS dial-out connections. Because an AIOPAD port cannot report the baud rate used for its connections, the rates specified in the baud rate and port name rate tables do not apply to these connections.

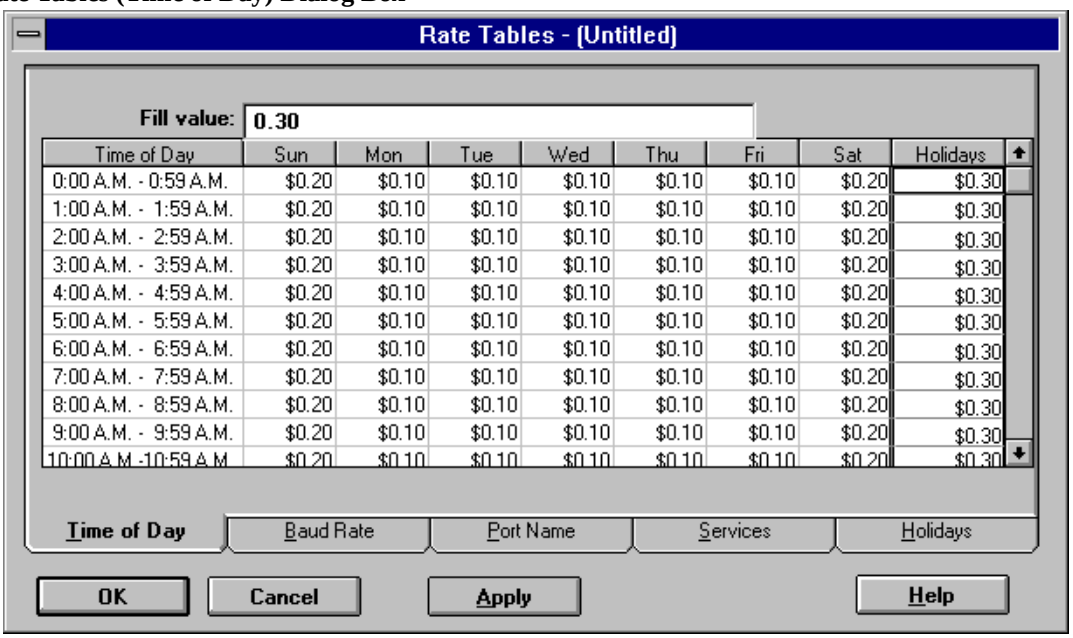
Setting Up a Time of Day Rate Table

Time of day rate tables can be used to specify different costs per minute based on the hour of the day, the day of the week, and whether or not it is a holiday.

To set up a time of day rate table, click the Enter Billing Rates button in the Accounting Profile dialog box. ConnectView displays the Time of Day rate table and the tab buttons for additional rate tables, shown in Figure 4-5 .

Figure 4-5

Rate Tables (Time of Day) Dialog Box



The example Time of Day rate table lists the time in hourly intervals from 0:00 a.m. to 23:59 p.m., and charges for each interval for each day of the week.

Enter the desired rates.

Note

To enter the same amount in multiple cells, highlight the desired cells and enter the desired rate in the Fill value edit box. Click the Apply button. This fills the highlighted cells with the entered rate. Rates must begin with an integer, for example 0.50 or 1.20. A leading decimal point will not be accepted.

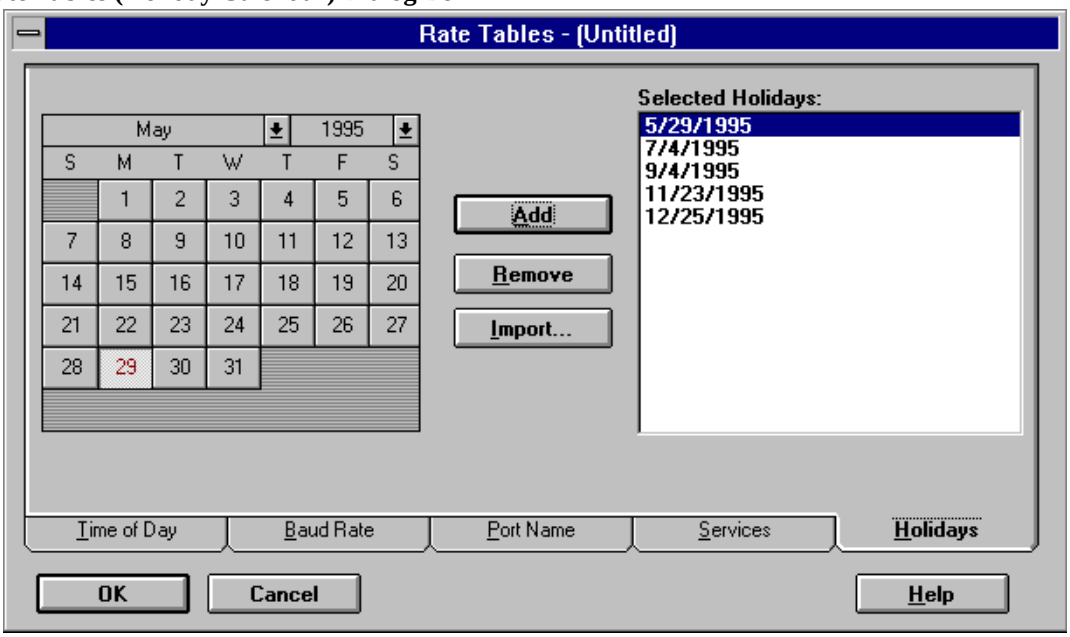
Also, enter additional rates that apply to holidays under the Holidays column. The Holidays column is the far right column.

Setting Holidays

When specifying time of day rates, ConnectView enables you to specify holidays of the year to receive special rates. When a connection occurs on a day assigned to be a holiday, holiday rates are used in place of any other rates. Enter the desired holiday rates in the Holidays column in the Time of Day rate table.

Click the Holidays tab button. ConnectView displays the holiday calendar in the Rate Tables dialog box, shown in Figure 4-6 .

Figure 4-6
Rate Tables (Holiday Calendar) Dialog Box



To include dates as holidays, either double-click them in the calendar or select the desired holiday dates and click the Add button. To remove dates as holidays, either double-click them in the Selected Holidays list or select any unwanted dates and click the Remove button.

To copy holiday settings from a previously saved profile, click the Import button. Importing holidays from another profile replaces the current holiday settings with the imported settings.

To close this dialog box and apply the holiday changes, click the OK button. To display additional accounting profile options, click a tab button.

Setting Up a Baud Rate Table

ConnectView enables you to create a rate table based on cost per minute or cost per connection for baud rates used for a connection (connection speeds).

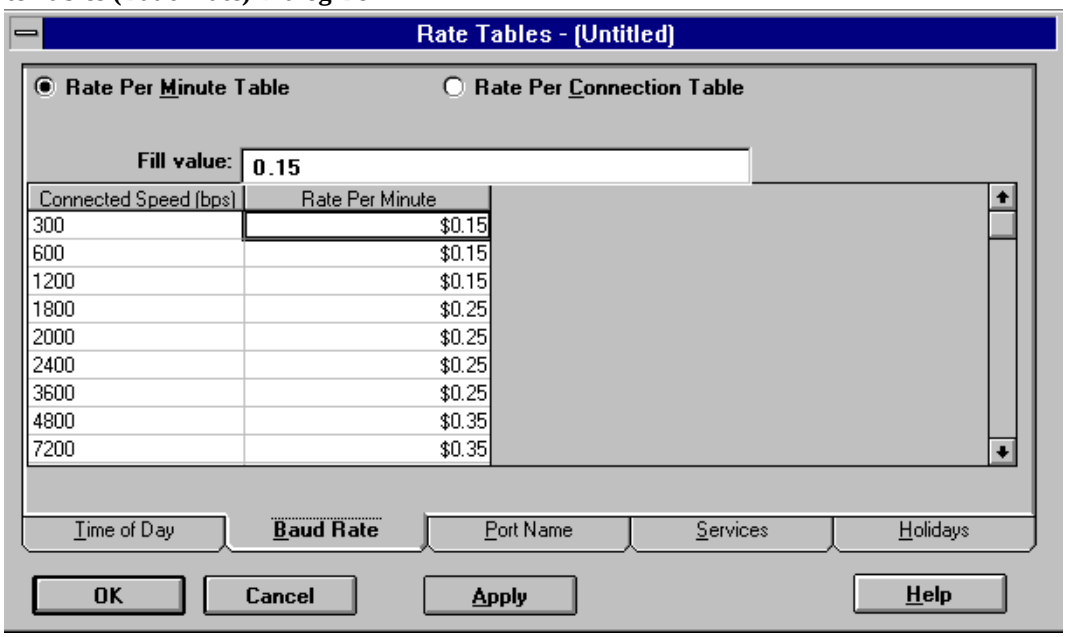
Note

Because an AIOPAD port cannot report the baud rate used for its connections, the rates specified in the baud rate or port name rate tables do not apply to these connections. Also, because NCS cannot report the baud rate used for its dial-out connections, baud rate and port name charges do not apply to NCS dial-out connections.

To create a rate table for baud rates, click the Baud Rate tab button. ConnectView displays the rates in the Rate Tables (Baud Rate) dialog box, shown in Figure 4-7 .

Figure 4-7

Rate Tables (Baud Rate) Dialog Box



Click the Rate Per Minute Table or Rate Per Connection Table radio button and enter the desired rates for the connection speeds in the rate column.

Note

To enter the same amount in multiple cells, highlight the desired cells and enter the desired rate in the Fill value edit box. Click the Apply button. This fills the highlighted cells with the entered rate. Rates must begin with an integer, for example 0.50 or 1.20. A leading decimal point will not be accepted.

To close this dialog box and apply all rate changes, click the OK button. To display additional accounting profile options, click another tab button.

Setting Up a Port Rate Table

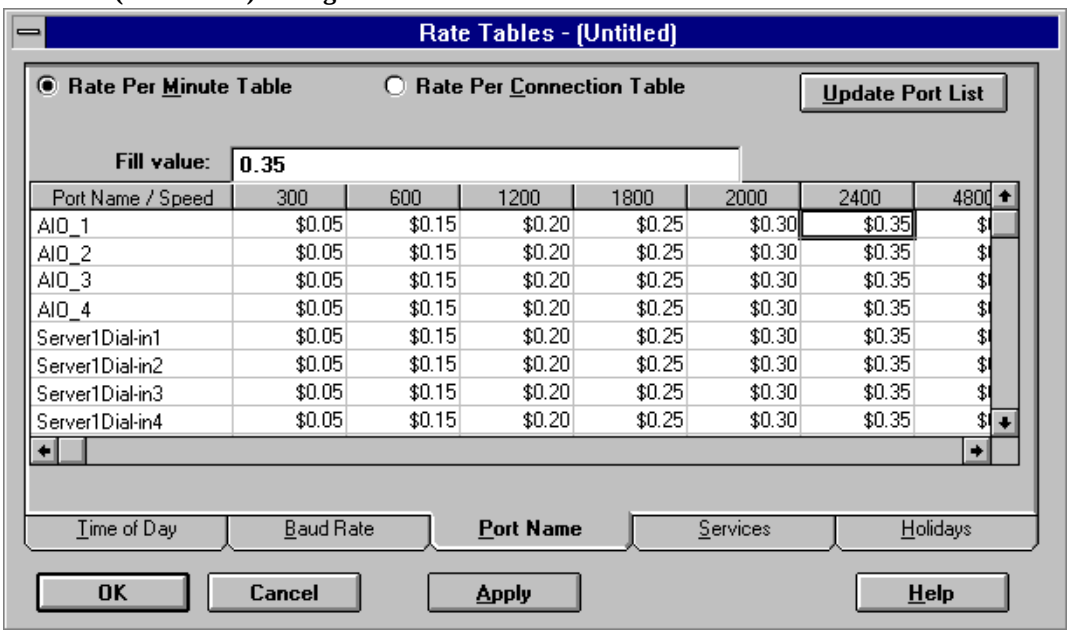
ConnectView enables you to create a rate table based on cost per minute or cost per connection for individual port access on the current server.

Note

Because an AIOPAD port cannot report the baud rate used for its connections, the rates specified in the baud rate or port name rate tables do not apply to these connections. Also, because NCS cannot report the baud rate used for its dial-out connections, baud rate and port name charges do not apply to NCS dial-out connections.

To create a rate table for the ports, click the Port Name tab button. ConnectView displays the rates for the different speed on a port in the Rate Tables (Port Name) dialog box, shown in Figure 4-8 .

Figure 4-8
Rate Tables (Port Name) Dialog Box



Click either the Cost Per Minute Table or Cost Per Connection radio button and enter the desired rates for each port and port speed. To update the list of available ports to match the available ports on the current server, click the Update Port List button.

Note

To enter the same amount in multiple cells, highlight the desired cells and enter the desired rate in the Fill value edit box. Click the Apply button. This fills the highlighted

cells with the entered rate. Rates must begin with an integer, for example 0.50 or 1.20. A leading decimal point will not be accepted.

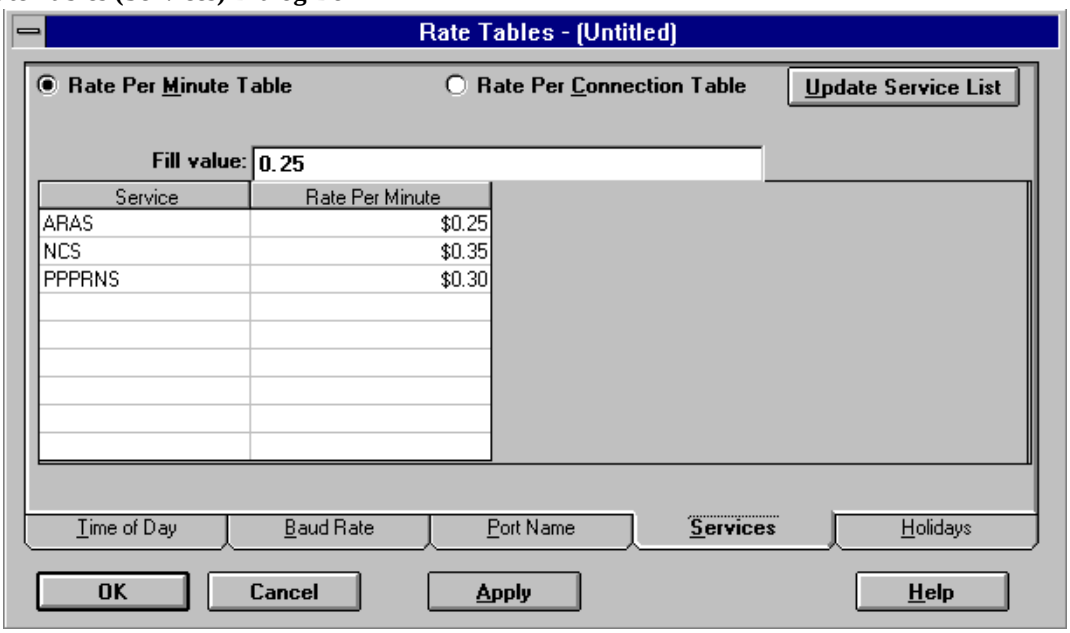
To close this dialog box and apply all rate changes, click the OK button. To display additional accounting profile options, click another tab button.

Setting Up a Service Rate Table

ConnectView enables you to create a rate table based on cost per minute or cost per connection for each remote access service on the current server.

To create a rate table for the supported services, click the Services tab button. ConnectView displays the service rates in the Rate Tables (Services) dialog box, shown in Figure 4-9 .

Figure 4-9
Rate Tables (Services) Dialog Box



Click the Rate Per Minute Table or the Rate Per Connection Table radio button and enter the desired rates in the rate column. To update the list of available services on the current server, click the Update Service List button.

Note

To enter the same amount in multiple cells, highlight the desired cells and enter the desired rate in the Fill value edit box. Click the Apply button. This fills the highlighted

cells with the entered rate. Rates must begin with an integer, for example 0.50 or 1.20. A leading decimal point will not be accepted.

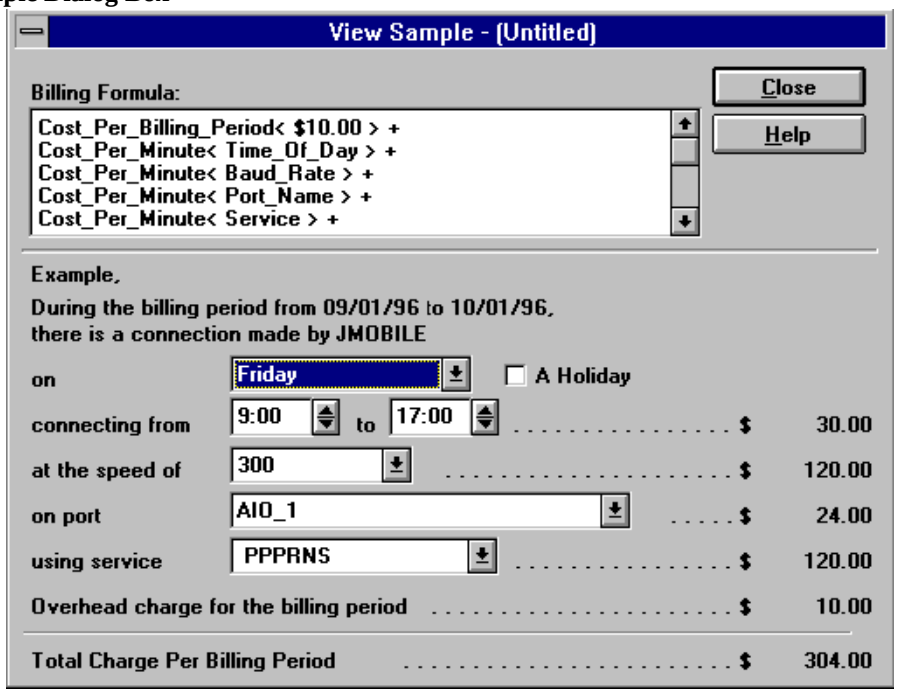
To close this dialog box and apply all rate changes, click the OK button. To display additional accounting profile options, click another tab button.

Viewing Sample Billing Charges

ConnectView allows you to view sample billing charges based on the current billing formula, so that you can quickly evaluate the specified billing formula and the specified rates.

To access the View Sample dialog box, click the View Sample button in the right side of the Accounting Profile dialog box. ConnectView opens the View Sample dialog box, shown in Figure 4-10 .

Figure 4-10
View Sample Dialog Box



Use the spin controls to change the time of day, click the A Holiday check box to specify holiday charges, and use the combo boxes to select a connection time, baud rate, port, and/or service. ConnectView displays sample billing

charges based on the current billing formula and rate tables. The current billing formula is displayed in the upper section of the dialog box.

Important

Remote Node Service (RNS) connections that fail to log in could be included in the billing charges because a start and end record could still be logged. Because NCS cannot report the baud rate used for its dial-out connections, baud rate and port name charges do not apply to NCS dial-out connections. Also, because an AIOPAD port cannot report the baud rate used for its connections, the rates specified in the baud rate or port name rate tables do not apply to AIOPAD connections.

To close this dialog box, click the Close button.

Assigning Accounting Profiles and Account Numbers to Users

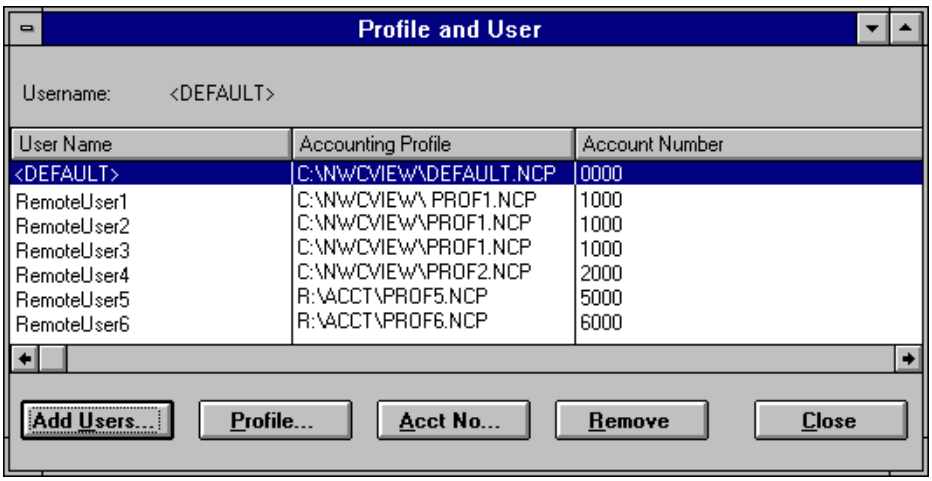
ConnectView enables you to assign users to the saved accounting profiles in the Profile and User window.

To assign users to your accounting profiles, choose Accounting > Assign Profile to Users. ConnectView opens the Profile and User window, shown in Figure 4-11 .

Note

By default, ConnectView creates the DEFAULT.NCP profile with account number 0000 and assigns this profile to all users (<DEFAULT>). This profile does not initially contain any billing formula or rates. The profile can be modified using Accounting > Edit Profile, but cannot be removed from the Profile and User window.

Figure 4-11
Profile and User Window



Note

No charges are applied for accounting profiles that are unavailable or cannot be found.

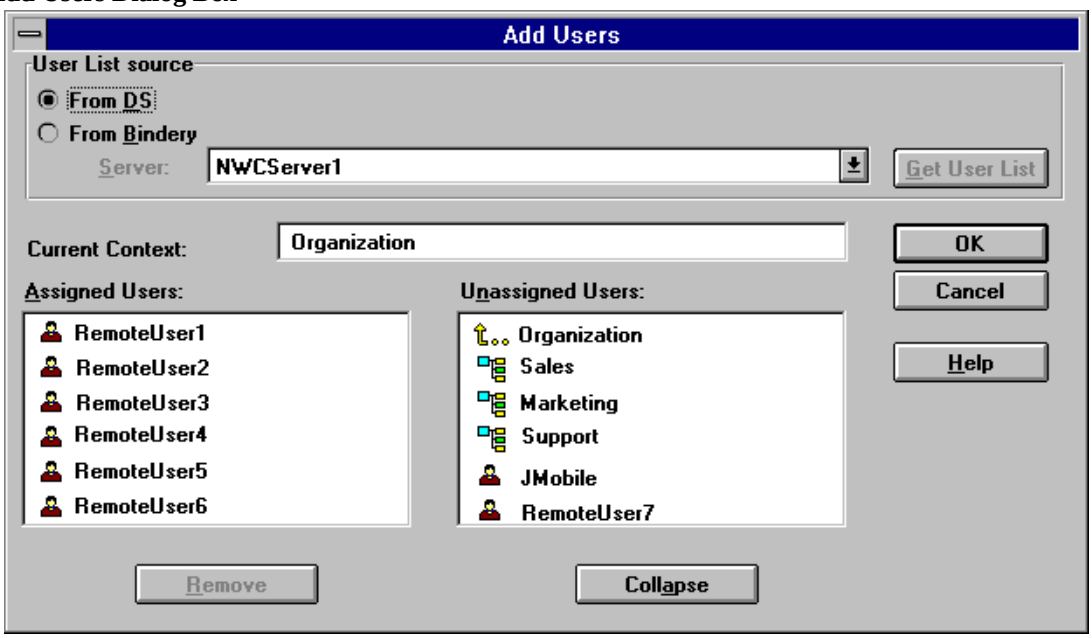
Adding Users and Removing Users from a Profile Assignment

You might want to assign users to different accounting profiles to enable you to apply different billing charges to different users.

To select users, click the Add Users button. ConnectView opens the Add Users dialog box, shown in Figure 4-12 .

Figure 4-12

Add Users Dialog Box



To select users from the current Novell Directory Services™ (NDS™) tree, click the From DS radio button in the User List Source section. Then, either double-click the desired usernames in the Assigned Users list box or select the desired context or usernames in the Unassigned Users list box and click the Add button.

Note

If you assign accounting profiles using the bindery username jsmith, then record transactions using the complete NDS context (jsmith.eng.xyzcorp) the transactions will not match the bindery username (jsmith) assigned to the accounting profile and the default accounting profile will be used. NDS usernames are different than bindery usernames.

You can either double-click the objects or use the Collapse/Expand button to browse the tree and select the desired users. You can use the arrow buttons to navigate the tree.

Note

To select multiple users, press and hold the left mouse button while dragging the selection over the desired usernames or press and hold Ctrl while clicking the usernames. Selecting multiple users is not possible when you select users from an NDS tree.

To remove users, select the desired usernames in either the Profile and User window or the Assigned Users list box and click the Remove button.

When the desired users have been selected, click the OK button to close this dialog box and add or remove the users to the Profile and User window. To close this dialog box without applying any changes, click the Cancel button.

Selecting an Accounting Profile

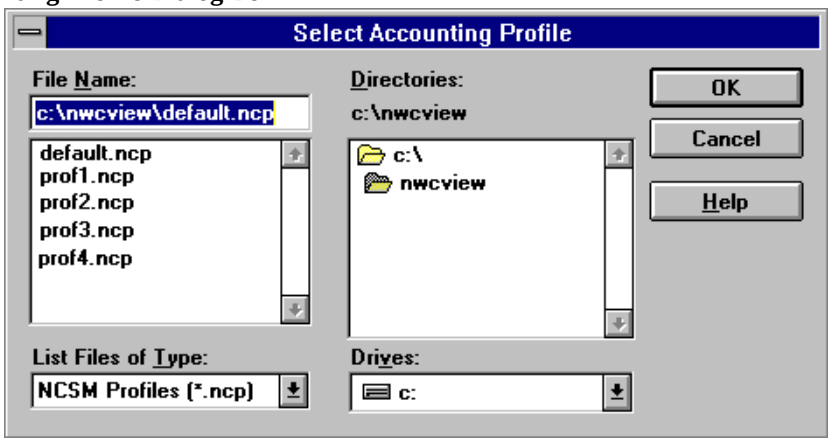
To select a different accounting profile for a user, select the desired usernames and click the Profile button.

Note

To select multiple users, press and hold the left mouse button while dragging the selection over the desired usernames or press and hold Ctrl while clicking the usernames.

ConnectView opens the Select Accounting Profile dialog box, shown in Figure 4-13 .

Figure 4-13
Select Accounting Profile Dialog Box



Use the file options to specify the desired drive, path, and accounting profile filename. By default, accounting profiles are stored in the \NWCVIEW directory.

To apply the accounting profile to the selected users, click the OK button. To close this dialog box without applying the profile, click the Cancel button.

Setting Up Account Numbers

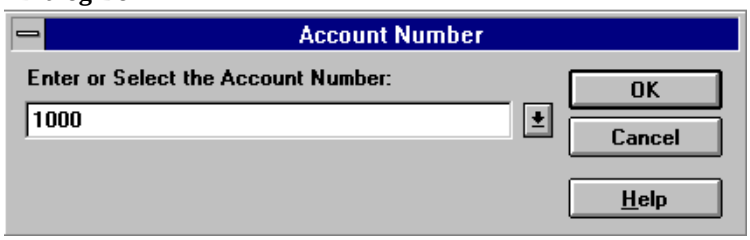
To set up or change the account number assigned to a user, select the desired usernames and click the Acct No button.

Note

To select multiple users, press and hold the left mouse button while dragging the selection over the desired usernames or press and hold Ctrl while clicking the usernames.

ConnectView opens the Account Number dialog box, shown in Figure 4-14 .

Figure 4-14
Account Number Dialog Box



Enter the desired account number and click the OK button. Account numbers can be up to 38 alphanumeric characters, including mixed case and special characters. ConnectView applies the entered account number to the selected users.

To close this dialog box without applying the account number, click the Cancel button.

Displaying Billing Charges

ConnectView enables you to generate and display billing charges based on the accounting profiles assigned to users and remote access usage.

Important

The audit trail file and/or archived files must be available for the display period to display accounting data. Also, ensure that the BSPXCOM.NLM file is loaded on the managed servers and the BREQUEST.EXE program file is running on the ConnectView workstation.

Only connections that begin and terminate during the display period (connections that have both a valid start record and end record) are considered in accounting data. RNS connections that fail to log in might be included in the billing charges because a start record and end record might still be logged.

Because NCS cannot report the baud rate used for its dial-out connections, baud rate and port name charges do not apply to the NCS dial-out connections. Also, because a connected speed is not available for connections using an AIOPAD port, the rates specified in the baud rate and port name rate tables do not apply to AIOPAD connections.

Note

Connections with a duration less than the grace period, the minimum connection duration, are not included in accounting data. By default, the grace period is set to 30 seconds. To change the grace period, choose File > Preferences and click the Grace Period tab button.

After accounting profiles are assigned and connection data is available, accounting data can be displayed in an accounting log, with data listed by username or account number or in an accounting report.

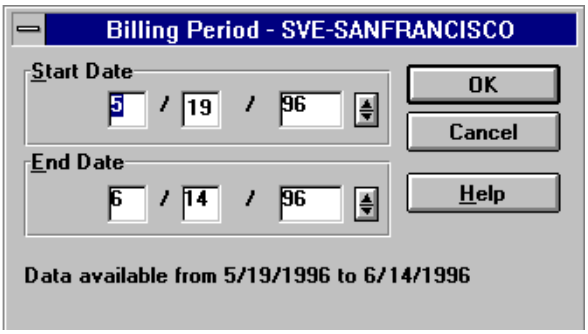
Important

If you are accessing large amounts of data in the current audit trail file and/or archived files, displaying accounting data could require a substantial amount of time and memory. This is escpecially so if low memory conditions occur and Windows begins to swap data to disk, increasing the amount of time required to process the data. In extremely low memory conditions, you might not be able to complete the operation.

Specifying a Billing Period and Accessing the Accounting Log Window

To access accounting data, select the desired server icon in the View All window or a View window, or select the desired server name in the Server combo box in the left corner of the Tool Bar. Then, either click the Accounting icon or choose Accounting > View Billing Charges by User Name. ConnectView opens the Billing Period dialog box, shown in Figure 4-15 .

Figure 4-15
Billing PeriodDialog Box



Enter the desired Start and End dates and click the OK button.

Note

Connections that are started before the billing period start date and continue past the billing period end date (span the entire specified billing period), and connections that do not start within the billing period but end within the billing period are not displayed as incomplete connections and are not included in accounting data.

By default, start and end dates are determined by the available audit trail and archived files.

To check for connections that started during the specified billing period but last beyond the end date (a start connection record is found, but not a matching end connection record), ConnectView checks for end records up to one day after the billing period. If an end connection record that matches a start connection record is found, ConnectView includes the connection in the accounting data. If not, ConnectView counts it as incomplete.

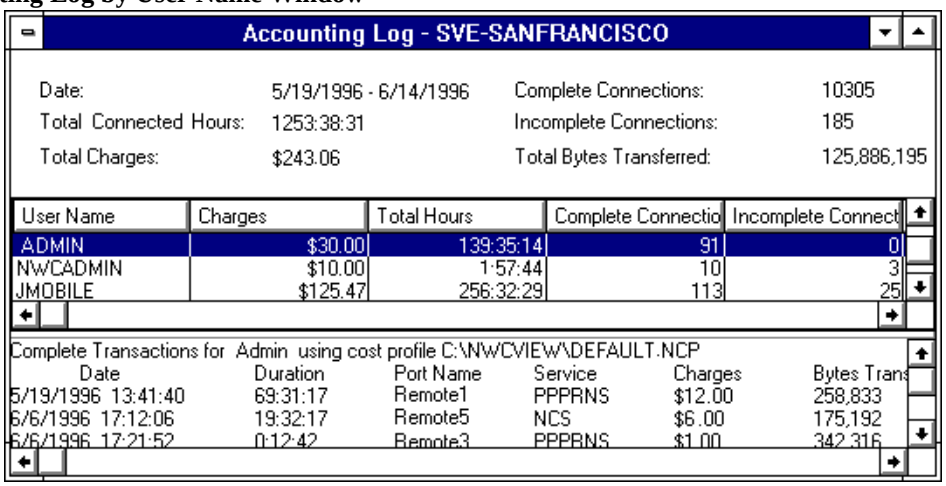
Because of this one day checking and to avoid duplicate billing, ConnectView discards any end connection records for which a matching start connection record cannot be found. The following table summarizes this accounting process for a connection that begins on 3/1/96 at 8:00 a.m. and ends on 3/4/96 at 3:00 p.m.

Billing Period	Accounting Result
3/1/96 to 3/4/96	Included. The connection is included in the accounting data, because both the start time and the end time are within the billing period.
3/1/96 to 3/3/96	Included. The connection is included in the accounting data, because the start time is within the billing period and the end time is outside the billing period by less than one day.
3/1/96 to 3/2/96	Incomplete connection. The connection is counted as an incomplete connection, because the start time is within the billing period, but the end time is outside the billing period by more than one day.

Billing Period	Accounting Result
3/2/96 to 3/2/96	Not included. The connection is not included in the accounting data, because neither the start time nor the end time is within the billing period.
3/2/96 to 3/4/96	Not included. The connection is not included in the accounting data and is not counted as an incomplete connection, because the start time is outside the billing period, even though the end time is within the billing period.

ConnectView opens the Accounting Log window with data for the specified date. Figure 4-16 shows an example Accounting Log window with data displayed by user ID.

Figure 4-16
Accounting Log by User Name Window



From this example, you can see that the Accounting Log window is divided into three sections. The top section contains billing period summaries, the middle section shows totals by user ID, and the bottom section lists the completed transactions associated with the selected user.

Important

The Accounting Log window can display data for up to 8,000 user IDs for the specified billing period. However, this display limitation does not apply to copying, printing, or exporting accounting data.

Displaying Accounting Data for Specific Users

ConnectView enables you to limit the data displayed in the Accounting Log window by usernames, account numbers, and dates within the display period.

To limit the display of accounting data, with the Accounting Log window open, choose View > Display Options (F4). ConnectView opens the Accounting Log By Users Display Options dialog box.

Specify the desired dates. These dates cannot exceed the dates and times specified for the accounting display period.

Then, select the desired usernames in the Available Users list and click Add. The usernames appear in the Selected Users list.

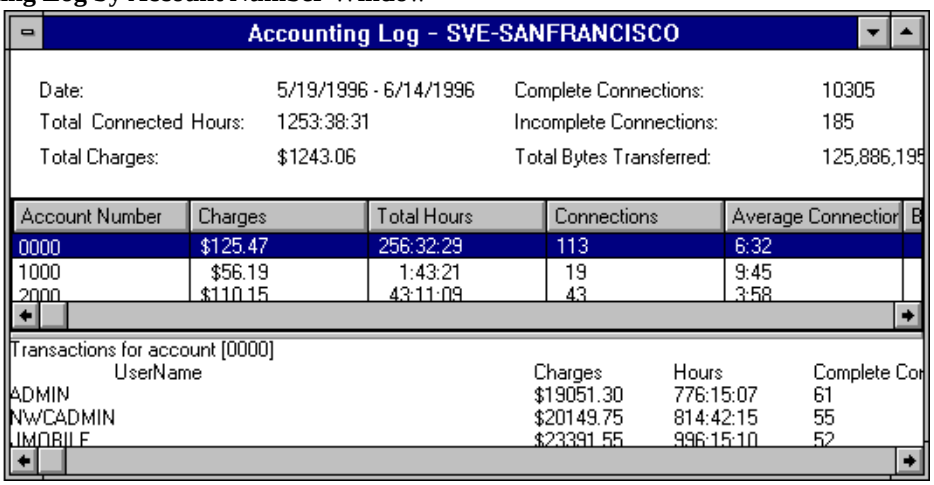
Click OK to limit the data displayed in the Accounting Log window to specified options. Click Cancel to close this dialog box without changing the data in the Accounting Log window.

Displaying Accounting Data by Account Number

To display accounting data by account number, first open the Accounting Log window with data displayed by user ID. This is the default view of the accounting log. When this window is open, the command changes to Accounting > View Billing Charges by Account Number. Choose this command. ConnectView displays accounting data by account number.

Figure 4-17 shows an example Accounting Log window for the period from 5/19/96 to 6/14/96, with data by account number.

Figure 4-17
Accounting Log by Account Number Window



From this example, you can see that the Accounting Log window is divided into three sections. The top section contains billing period summaries; the middle section shows connections by account number; and the bottom section lists the users assigned to the selected account number along with data for each user.

Important

The Accounting Log window can display up to 8,000 user IDs for the specified billing period. However, this display limitation does not apply to copying, printing, or exporting accounting data.

To switch back to displaying accounting data by user ID, choose Accounting > View Billing Charges by User Name.

Displaying Accounting Data for Specific Account Numbers

ConnectView enables you to limit the data displayed in the Accounting Log window account numbers and dates within the original display period.

To limit the display of accounting data, with the Accounting Log window open, choose View > Display Options (F4). ConnectView opens the Accounting Display By Account Number Options dialog box.

Specify the desired dates. These dates cannot exceed the dates and times specified for the original accounting display period.

Select the desired account numbers in the Available Acccounts list and click Add. The account numbers appear in the Selected Accounts list.

Click OK to limit the data displayed in the Accounting Log window to specified options. Click Cancel to close this dialog box without changing the data in the Accounting Log window.

Accessing the Accounting Report Window

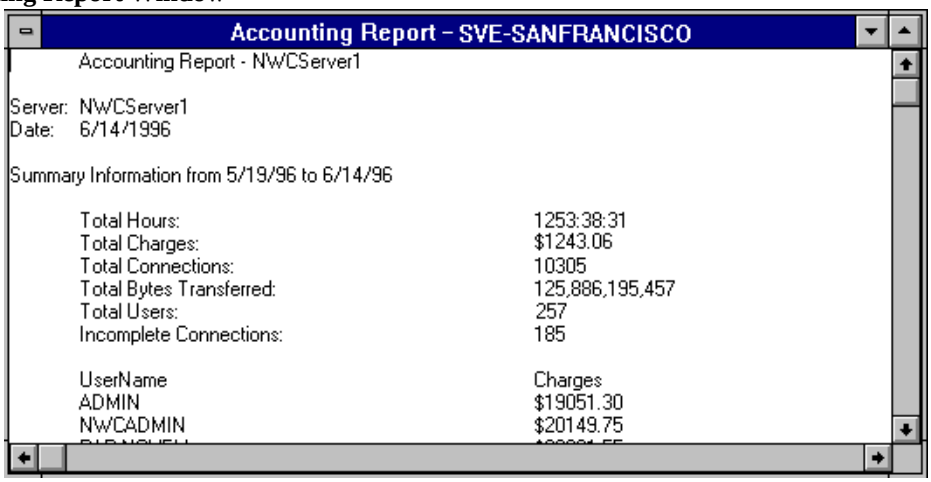
You can use the Accounting Report window to display accounting totals and daily connections in report format.

To display accounting data in report format, ensure the desired server is selected and from any window choose File > Generate Report > Accounting. The Billing Period dialog box appears so you can enter start and end dates. For a description of the Billing Period dialog box, see Figure 4-15 on page 79 .

Enter the desired dates and click OK.

ConnectView opens the Accounting Report window shown in Figure 4-18 .

Figure 4-18
Accounting Report Window



From this example, you can see an Accounting Report window with data for connections made between 5/19/96 and 6/14/96.

Important The Accounting Report window can display up to 32,000 lines of data for the specified billing period. However, this display limitation does not apply to copying, printing, or exporting accounting data.

Customizing the Accounting Report

ConnectView allows you to specify which information appears in the Accounting Report window and in what order the data columns appear.

To customize the data display in the Accounting Report window, choose File > Report Preferences and click the Accounting tab button. The Report Preferences dialog box appears with the options for the Accounting Report window.

By default, the Accounting Report includes summary information, user totals, account totals, and connection information. The following table shows the default fields for the user totals and connection information.

User Totals	Username, charges, hours, dial-in hours, dial-out hours, dial-in charge, dial-out charge, complete connections, discarded connections, account number, account profile, bytes transferred
Connection Information	Server name, date, username, hours, port name, baud rate, service, dial type, charges, bytes transferred, phone number

Clear the check boxes for the data you do not want to appear in the report.

To change the order of the detailed information, select the desired field and click the Up or Down button.

To save your changes, click the OK button. The changes take effect the next time the Accounting Report window is opened and remain in effect until these options are changed. To close this dialog box without applying the changes, click the Cancel button.

Displaying Incomplete Connections and Connections with Duplicate IDs

Incomplete connections are connections for which ConnectView can find a start connection record but cannot locate the related end connection record. Incomplete connections could be due to one of the following:

- Server was down.
- Audit trail recording was disabled or unavailable after the connection was established.
- Connection was disconnected beyond the end date of the display period.
- Connection is ongoing or the connection was disconnected and an end of connection record could not be generated.

Note

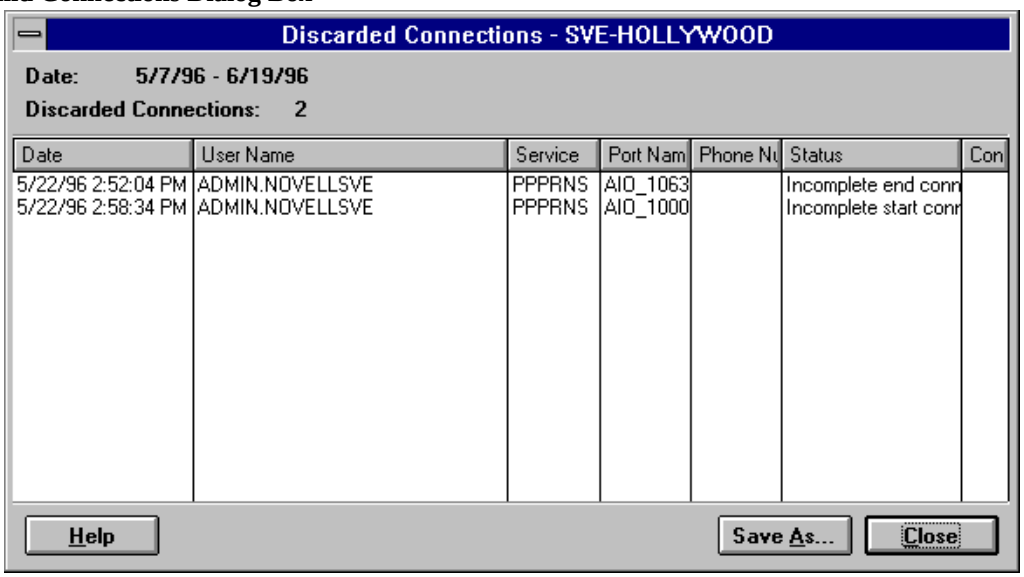
ConnectView automatically checks for end connection records up to one day after the end date of the billing period. If an end connection record that matches a start connection record is found in the day after the billing period end date, ConnectView includes the connection in the accounting data. If the matching end connection record is not found, ConnectView counts it as incomplete. Because of this one day checking and to avoid duplicate billing, ConnectView considers any end connection records for which a matching start connection record cannot be found as incomplete connections.

Duplicate connection IDs occur when a new connection record contains the same connection ID as an existing connection record of the same type. When this occurs, ConnectView displays a warning message and allows you to terminate or continue the accounting process. If the accounting process is continued, ConnectView cannot guarantee the integrity of the accounting data.

To display the incomplete connections and connection records with duplicate connection IDs, with the Accounting Log window open, choose Accounting > View Invalid Connections.

ConnectView opens the Invalid Connections dialog box, shown in Figure 4-19 .

Figure 4-19
Invalid Connections Dialog Box



From this example, you can see there were two invalid connections during the current billing period. These connections are not included in the accounting data.

Note

Connections that are started before the billing period start date and continue past the billing period end date (span the entire specified billing period) are not displayed as discarded connections and are not included in accounting data.

Printing, Copying, and Exporting Accounting Data

ConnectView enables you to copy, print, and export accounting data.

Important

The amount of accounting data that can be output is not limited to the display limitations of 8,000 user IDs or account numbers in the Accounting Log window and 32,000 lines of data in the Accounting Report window.

This capability allows you to create and maintain comprehensive accounting records.

Important

If you are accessing large amounts of data in the current audit trail file and/or archived files, generating accounting data could require a substantial amount of time and memory. This is especially so if low memory conditions occur and Windows begins to

swap data to disk, increasing the amount of time required to process the data. In extremely low memory conditions, you might not be able to complete the operation.

Copying Accounting Data

To copy accounting data, open the desired Accounting Log or Accounting Report window and choose Edit > Copy. ConnectView copies the displayed data to the Windows clipboard. You can then paste this data into other applications.

Printing Accounting Data

To print accounting data, open the desired Accounting Log or Accounting Report window and choose File > Print. ConnectView prints the data from the opened window.

Exporting Accounting Data

To export accounting data in tab-delimited format, open the Accounting Report window for the desired period and choose File > Export. ConnectView prompts you for a filename and then exports the data from the opened Accounting Report window to the specified file in tab-delimited format.

Appendix

A *Running with ManageWise*

This appendix explains how to install and run ConnectViewTM on workstations with ManageWise® installed.

Important ConnectView does not install on workstations with ManageWise 1.0.

This appendix covers

- "Installing with ManageWise" on page 89
- "Using ManageWise SNMP Options" on page 92
- "Starting from ManageWise" on page 92

Installing with ManageWise

When installing ConnectView with ManageWise, ensure that the following requirements are met:

Important ConnectView does not support the Simple Network Management Protocol (SNMP) over IP.

- ManageWise software and workstation requirements
- ConnectView product diskettes
- 8 MB of RAM in addition to the ManageWise requirement
- 4 MB of disk space in addition to the ManageWise requirement

Important Because ManageWise can run with multiple Windows applications, refer to the ManageWise documentation to ensure that you have sufficient DOS memory and Windows resources to run ConnectView. If you are low on DOS memory, you might not be able to launch ConnectView. You might also be unable to open numerous windows if you are low on Windows resources.

Before installing ConnectView, perform the following tasks:

1. **Ensure that ManageWise is installed.**

   ConnectView can also run as a standalone application if ManageWise is unavailable.

Warning

If the install mode does not match the runtime environment, ConnectView displays a warning message and exits the installation. The install mode does not match the runtime environment if ConnectView was installed as a standalone application but the workstation is running with ManageWise, or ConnectView was installed with ManageWise but the workstation is running without ManageWise.

2. **Close ManageWise and exit any ManageWise applications.**

3. **Insert the Novell® Internet Access Server 4.1 CD-ROM in the workstation's CD-ROM drive.**

4. **Choose File > Run from the Program Manager menu to run the ConnectView SETUP.EXE program from Windows.**

   See your Windows documentation for details about running applications within Windows.

5. **Follow the installation program's directions.**

   The installation program displays a series of windows with dialog boxes that guide you through the installation process. Although the dialog boxes are self-explanatory, when responding to them you should be aware of the following information:

   - ConnectView is installed in \MW\NMS\BIN.

     This directory also contains the NWCVIEW.TXT file and is the default location for trend analysis files (files with .TAD extension) and accounting profiles (files with .NCP extension).

   - You can exit the installation program anytime; simply click the Exit button. A message appears to confirm the canceling of the installation.

   - When running with ManageWise, ConnectView allows you to display all servers running the remote access software as Novell Internet Access 4.1 server icons in the ManageWise maps. If you do not wish the servers running the remote access software to appear as Novell Internet Access Server 4.1 server icons in your

ManageWise maps, select the No radio button on the Welcome screen.

Important

If you choose the option to display server icons, be sure to run the NetExplorerTM program to ensure that the ManageWise maps are updated.

- ConnectView enables you to specify to which directory the Btrieve v6.15 files are copied. By default, the Btrieve files are copied to the \WINDOWS directory. If you wish to copy the files to a different directory, click the Btrieve Directory button in the Welcome screen and specify the desired location.
- If any ConnectView files already exist on the target location, ConnectView lists the installation files and the existing files with check boxes for each file. If you wish to override this, click the check boxes for the desired version of the displayed files.

Note

If an older version of the WLIBSOCK.DLL file exists on your workstation, ConnectView displays a warning message.

- ConnectView enables you to edit your AUTOEXEC.BAT file to load BREQUEST.EXE and SHARE. If you change this file, the current file is saved as AUTOEXEC.SAV. If you do not change this file, the file with changes suggested by ConnectView is saved as AUTOEXEC.NEW.
- When viewing the AUTOEXEC.BAT file, click the Warning Alerts button if you want to view a display of possible conflicts with files existing in multiple locations. ConnectView also suggests corrective actions to avoid these conflicts.

6. **If your AUTOEXEC.BAT file has changed, reboot your system. Otherwise, restart MS Windows.**

   If you changed your AUTOEXEC.BAT to load BREQUEST.EXE after the NetWare shell and before MS Windows or for any other reason, reboot your system before you start ConnectView. Otherwise, bring down MS Windows, ensure that BREQUEST.EXE is loaded after the NetWare shell, and restart Windows before you start ConnectView. If you choose to return to Windows, ensure that the proper action is taken before you attempt to start ConnectView.

7. **Check the ConnectView file NWCVIEW.TXT for product notes.**

   ConnectView provides the NWCVIEW.TXT file for product notes and last-minute feature changes. This file is stored in \MW\NMS\BIN. To

access this file at any time, use the Microsoft Notepad or any similar text editor.

Using ManageWise SNMP Options

If ConnectView is installed with ManageWise, ConnectView utilizes the SNMP engine in ManageWise and does not install the SNMP files on your workstation.

You can use the ManageWise command Configure > Global Preferences > SNMP Options to configure global community strings on your workstation for all Novell Internet Access 4.1 servers running the remote access software. In addition, ManageWise offers secure SNMP over NCP. This encapsulates an SNMP PDU in a NetWare Core Protocol™ (NCP™) packet. You can also use the ManageWise SNMP Options dialog box to configure SNMP over NCP separately for GET and SET requests on individual servers. If this option is used, a login dialog box for either the Novell Directory Services™ (NDS™) program or Bindery login information appears before an SNMP GET or SET operation is performed.

Starting from ManageWise

You can start ConnectView from ManageWise in the following ways:

- Choose Tools > ConnectView from the ManageWise Menu Bar.

  ConnectView opens the application and displays the View All window with a list of the available servers.

- Double-click a Novell Internet Access 4.1 server icon in a ManageWise map.

  ConnectView opens the application and displays the View All window with a list of the available servers and a View window for the selected server.

Appendix B *Understanding SNMP Management and Security*

This appendix explains how ConnectViewTM uses the Simple Network Management Protocol (SNMP) to manage and monitor Novell® Internet Access 4.1 servers running remote access software.

Important ConnectView does not support SNMP over IP.

The appendix covers:

- "Understanding SNMP Management" on page 93
- "Understanding ConnectView Security" on page 94
- "Setting Workstation SNMP Security" on page 95
- "Viewing Audit Trail, Alerts, Trend Analysis, and Accounting Data" on page 95

Understanding SNMP Management

ConnectView uses a combination of SNMP and remote Btrieve client to manage your remote access servers. To implement the SNMP connectionless management protocol, each server running the remote access software contains the Remote Access Management Agent (RAMA) and NetWare® SNMP Agent (SNMP.NLM). The Remote Access Management Agent registers the IDs of the NetWare ConnectTM objects it manages with the SNMP Agent. When a request is received for data, the SNMP agent forwards the request to the RAMA service, which processes the request and returns the information to the SNMP Agent. The SNMP Agent then returns the data to ConnectView.

Important Ensure that the most up-to-date versions of NCMA.NLM and SNMP.NLM are loaded on the managed servers.

ConnectView copies the necessary SNMP files to your workstation. This includes the WLIBSOCK.DLL file. If a different version of this file exists on your workstation, ConnectView displays a warning message.

However, ConnectView does not install the Novell TCP/IP stack and does not support SNMP over IP.

Important ConnectView SNMP options are available only when ConnectView is run in standalone mode.

Understanding ConnectView Security

ConnectView uses SNMP to retrieve data with GET requests and to control the remote access software with SET requests. These management operations affect a large number of windows and are dependent on the SNMP community string settings on each managed server and the ConnectView workstation.

On the server side, you can set the desired community strings on the command line either when you are loading SNMP.NLM or through the NIASCFG utility.

Important By default, SNMP.NLM on your servers grants public access to the MonitorCommunity (monitor=public) but disables access to the ControlCommunity.

Table 2-1 describes the server SNMP community strings.

Table 2-1 Server SNMP Community Strings

Community String	Description
MonitorCommunity	Controls security for the read-only GET and GET NEXT operations. The default is *public* .
ControlCommunity	Controls security for the read-write SET operations. By default, this operation is disabled.
TrapCommunity	Controls security for receiving SNMP-trap messages. The default is *public* .

Important The ConnectView use of community strings follows SNMP v1 security.

Setting Workstation SNMP Security

Your workstation's community string settings must match the community string settings on the managed servers. By default, ConnectView sets the workstation community strings to public (monitor=public control=public).

To configure workstation community strings for each server, choose *File* > *Preferences* and click the SNMP Options tab button. This dialog box also contains options for SNMP time-out and retry values.

Important

ConnectView does not support SNMP over the NetWare Core Protocol™ (NCP™) or SNMP over IP. An SNMP workstation can still access the Management Information Base (MIB) objects using the MIB browser over an IP stack.

Viewing Audit Trail, Alerts, Trend Analysis, and Accounting Data

ConnectView uses the remote Btrieve client to access records stored in the server-based audit trail log file for the Trend Analysis, Accounting, Audit Trail, and Alerts windows. To display this data, users must have READ/SCAN rights to the server and SYS:\SYSTEM\CSLIB directories and files.

For users already logged in to a Novell Directory Services™ (NDS™) tree, ConnectView attempts background authentication the first time an Accounting, Trend Analysis, Audit Trail, or Alerts window is opened. If the authentication is successful, ConnectView displays the data. If the authentication is unsuccessful, ConnectView displays a Bindery login box. The user must enter a valid username and password to display the data. Subsequent access to servers in the same NDS tree will occur without a login prompt.

For users not logged into an NDS tree, ConnectView displays a Bindery login box. The user must enter a valid username and password before the data will be displayed.