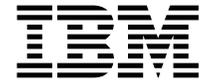


Nways Remote Monitor für Windows NT

Benutzerhandbuch

Version 2.0



Nways Remote Monitor für Windows NT

Benutzerhandbuch

Version 2.0

Anmerkung

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten Sie die allgemeinen Informationen unter Anhang H, „Bemerkungen“ auf Seite 193 lesen.

Dritte Ausgabe (Juli 1999)

Diese Ausgabe gilt für Version 2 von Nways Remote Monitor.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
Nways Remote Monitor for Windows NT - User's Guide
IBM Form SA27-4195-02,
herausgegeben von International Business Machines Corporation, USA
© Copyright International Business Machines Corporation 1999

© Copyright IBM Deutschland Informationssysteme GmbH 1999

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW NLS Center
Kst. 2877
Juli 1999

Inhaltsverzeichnis

Zu diesem Handbuch	xv
Zielgruppe	xv
Neue Funktionen in diesem Release	xv
Konventionen	xvi
Terminologie	xvi
Übersicht über Nways Remote Monitor	1
Einführung in Nways Remote Monitor	1
Nways Remote Monitor zum Netzwerkmanagement verwenden	2
Grundlageninformationen	2
RMON-Übersicht	3
Grundlagen von Nways Remote Monitor	4
Neue Funktionen in diesem Release	6
Mit der Schnittstelle von Nways Remote Monitor arbeiten	7
Viewman-Schnittstelle	7
Menüleiste	8
Funktionsleiste	8
Zusammenfassungsbereich	8
Alarmleiste	8
Statusleiste	8
Rmonview-Schnittstelle	9
Dialog "... View"	9
Rmonview-Hauptfenster	10
Funktionsleiste	13
Anwendungsanzeigebereich	14
Statusleiste	16
Collector-Schnittstelle	16
Menüleiste	17
Statusprotokoll	17
Statusleiste	17
Reporter-Schnittstelle	18
Optionen im Hauptfenster	18
Optionen in der Menüleiste	19
Sonden definieren	21
Dialog "Device Configuration" öffnen	21
Über Viewman	21
Über Collector und Translator	21
Über das Menü "Start" von Windows NT	21
Sonden definieren	22
Sonden verwalten	24
Hardware- und Firmware-Versionen	26
Firmware herunterladen	26
Datum/Zeit und Echointervall	27

IP-Adresse, Teilnetzmaske und Standard-Gateway	28
Sonden zurücksetzen	29
Zugriffssteuerungstabellen	32
Dialog "Access Control" öffnen	32
Alarmnachricht-Benutzergemeinschaften	34
Dialog "Trap Control" öffnen	35
Statische Leitwege definieren	36
PACMIB aktivieren und inaktivieren	37
RMON2-Modus definieren	38
Virtuelle Schnittstellen konfigurieren	39
Virtuelle Schnittstellen erstellen	39
Virtuelle Schnittstellen löschen	42
RMON- und RMON2-Tabellen verwalten	43
RMON2-(ECAM)-SmartAgent-Firmware verwalten	44
Dialog "SmartAgent Maintenance" öffnen	45
Benutzerdefinierte Protokolle verwalten	48
Protokollverzeichnis anzeigen	48
Protokolle hinzufügen	49
Protokolle löschen	49
RMON2-Tabellen für Protokolle aktualisieren	50
Stationsnamen definieren	53
Stationen automatisch erkennen	53
SmartAgent-Sonden	53
RMON2-Sonden	54
Translator starten	54
Menü "Start"	54
Translator-Hauptfenster	54
Daten importieren	56
Datensammlungen starten	57
Datensammlungen stoppen	59
Datensammlungen löschen	59
Stationen manuell einrichten	60
Namenumsetzungsebene definieren	62
Lieferantenpräfixe angeben	63
Viewman	65
Viewman starten	66
Das Hauptfenster konfigurieren	66
Viewman-Diagramme	68
Diagramm "Packet Size Distribution"	69
Diagramm "Packet Rates"	70
Diagramm "Network Statistics"	71
Diagramm "Top 10 Hosts by Packet Rate"	72
Diagramm "Top 10 Hosts by Error Rate" (Ethernet und Token-Ring)	73
Diagramm "Top 10 Receivers" (FDDI)	73
Diagramm "Event Distribution" (Ethernet)	74
Diagramm "Ring Status" (FDDI und Token Ring)	74

Rmonview und RMON-Anwendungen	77
Rmonview starten	78
RMON-Anwendungen starten	78
Rmonview	78
Viewman	79
RMON-Anwendungen konfigurieren	80
Anzeigen erstellen und editieren	80
Statistikanzeige (Statistics View)	82
"Statistics View" konfigurieren	82
Protokollanzeige (History View)	84
"History View" konfigurieren	84
Host-Anzeige (Host View)	87
"Host View" konfigurieren	87
Matrixanzeige (Matrix View)	90
"Matrix View" konfigurieren	91
Ringstationsanzeige (Ring Station View)	92
"Ring Station View" konfigurieren	93
Alarmanzeige (Alarms View)	94
"Alarms View" konfigurieren	95
Adreßumsetzungsanzeige (Address Translation View)	98
Tabellenarten in Address Translation	99
Adreßumsetzungstabellen anzeigen	100
Protokollverteilung (Protocol Distribution) anwenden	101
Anzeigearten in Protocol Distribution	101
Tabellen in Protocol Distribution anzeigen	102
Packet Capture und Decode	103
Capture starten	103
Viewman	103
Menü "Start"	104
Capture konfigurieren	104
Puffer verwenden	104
Neue Puffer für Capture erstellen	105
Erfassungspuffer ändern	109
Erfassungspuffer aus einer Datei laden	110
Neue Start- und Stoppereignisse erstellen	110
Filtereditor verwenden	112
Verfügbare Filterschablonen	114
Decode starten	116
Capture	116
Den Erfassungspuffer einer Sonde anzeigen	116
Einen gespeicherten Puffer anzeigen	116
Erfaßte Pakete lesen	116
Sondenerfassungspuffer laden	117
Conversation Trace and Analysis	118
Erfaßte Pakete speichern und laden	119
Pakete speichern	119
Pakete laden	119

Collector	121
Collector starten	122
Viewman	122
Menü "Start"	122
Datenquellen konfigurieren	123
Adreßumsetzungsebene einstellen	123
Datensammlungen definieren	125
Eine neue Konfiguration hinzufügen	126
Konfigurationen ändern	128
Datensammlung stoppen	128
Datensammlung starten	129
Speicher für gesammelte Daten	129
Collector beenden	129
Reporter	131
Reporter starten	132
Viewman	132
Menü "Start"	132
Berichtsdatenbank auswählen	133
Eine neue Datenbank erstellen	133
Eine vorhandene Datenbank öffnen	133
Daten importieren	134
Datenbankinhalt anzeigen	135
Berichte auswählen und generieren	136
Berichte auswählen	136
Berichtsparameter auswählen	137
Gespeicherte Berichte laden	141
Datenmanagement	143
Daten verwalten	143
Beispiele für die Zusammenfassung	144
Daten zusammenfassen	146
Daten löschen	147
Daten archivieren	148
Daten archivieren	148
Auf archivierte Daten zugreifen	148
Anwendungsdatenbank komprimieren und reparieren	149
Anwendungsdatenbank komprimieren	149
Anwendungsdatenbank reparieren	150
Anhang A. Liste der Protokolldecodierungen	151
Anhang B. Anwendungsvariablen	153
Variablen für Statistics	153
Auf Ethernet verfügbare Variablen	153
Auf FDDI verfügbare Variablen	154
Auf Token-Ring verfügbare Variablen	155

Variablen für History	158
Auf Ethernet verfügbare Variablen	158
Auf FDDI verfügbare Variablen	159
Auf Token-Ring verfügbare Variablen	160
Variablen für Hosts	162
Variablen für Ring Station	163
Anhang C. Leistungsrichtlinien	165
Anhang D. Inhalt der CSV-Dateien	167
Protokolldateiformat	168
Host-Dateiformat	169
Matrixdateiformat	170
MAC-Schichtprotokolldaten für Token-Ring	171
Sonstige Protokolldaten für Token-Ring	173
Anhang E. Berichtsbeschreibungen	175
Beispiel für ein Histogramm	178
Beispiel für eine Liniengrafik	178
Anhang F. HTML-Berichtsschablonen anpassen	179
Standardschablone anpassen	179
HTML-Standardschablone	180
Anhang G. RMON2- und ECAM-Protokolle	181
ECAM-Anwendungsdecodierungen	181
RMON2-Protokollübersicht	184
Vordefinierte RMON2-Protokolle	185
Anhang H. Bemerkungen	193
Marken	194
Glossar	195
Index	199
Antwort	201

Abbildungsverzeichnis

1.	Viewman-Hauptfenster	7
2.	Rmonview-Hauptfenster	10
3.	Statistikanzeigen in Rmonview	14
4.	Collector-Hauptfenster	16
5.	Reporter-Hauptfenster	18
6.	Dialog "Probe List Editor"	22
7.	Dialog "Agent Maintenance"	25
8.	Firmware herunterladen	26
9.	Datum/Zeit und Echointervall	27
10.	IP-Adresse, Teilnetzmaske und Standard-Gateway	28
11.	Dialog "Access Control"	32
12.	Dialog "Trap Control"	35
13.	Dialog "Static Routing Table"	36
14.	Dialog "Edit Routing Entry"	37
15.	PACMIB aktivieren und inaktivieren	37
16.	Dialog "RMON2 Config"	38
17.	Dialog "Reset Confirmation"	39
18.	Dialog "Create Virtual Interfaces"	40
19.	Dialog "Channel"	41
20.	Dialog "RMON Tables"	43
21.	Dialog "RMON2 Table Management"	43
22.	Dialog "SmartAgent Maintenance"	45
23.	Dialog "Protocol Directory"	48
24.	Dialog "User Defined Protocol"	49
25.	Beispiel für den Dialog "Protocol Properties"	50
26.	Beispiel für den Protokollkonfigurationsdialog	51
27.	Menü- und Funktionsleiste von Nways Remote Monitor	54
28.	Translator-Hauptfenster	55
29.	Dialog "Import Host Map file"	57
30.	Dialog "Data Collection Configurations"	57
31.	Dialog "Data Collection Editor"	58
32.	Dialog "Station List Edit"	60
33.	Dialog "Add Station"	61
34.	Dialog "Edit Station"	61
35.	Dialog "Set Translation Level"	63
36.	Viewman	66
37.	Menü "View"	66
38.	Dialog "Display Options"	67
39.	Diagramm "Packet Size Distribution" für Token-Ring	69
40.	Diagramm "Packet Rates" für Token-Ring	70
41.	Diagramm "Network Statistics" für Token-Ring	71
42.	Diagramm "Top 10 Hosts by Packet Rate" für Ethernet	72
43.	Diagramm "Top 10 Hosts by Error Rate" für Ethernet	73
44.	Diagramm "Event Distribution" für Ethernet	74
45.	Diagramm "Ring Status" für Token-Ring	74

46.	Anwendung über Rmonview öffnen	78
47.	Viewman-Menüleiste und -Funktionsleiste	79
48.	Beispiel für den Dialog oder die Anwendungsanzeige	80
49.	Dialog "Edit User View"	81
50.	Dialog "Statistics View"	82
51.	Dialog "History View"	84
52.	Dialog "History Entry Creation"	86
53.	Dialog "Host View"	87
54.	Dialog "Station Select"	89
55.	Matrix View	91
56.	Dialog "Ring Station View"	93
57.	Dialog "Alarms View"	95
58.	Dialog "Alarm Creation"	96
59.	Alarmaktivierung angeben	97
60.	Hysterese-Zone	98
61.	Aktuelle Einheit in Viewman anzeigen	100
62.	Rmonview	100
63.	Aktuelle Einheit in Viewman anzeigen	102
64.	Rmonview	102
65.	Viewman-Menüleiste und -Funktionsleiste	103
66.	Hauptdialog "Capture Application"	104
67.	Dialog "Edit Packet Capture"	105
68.	Dialog "Configure Interface"	106
69.	Dialog "Start Events"	106
70.	"Start Event" aktiv	107
71.	"Stop Event" aktiv	107
72.	"Start Event" und "Stop Event" aktiv	107
73.	Dialog "Buffer Control"	108
74.	Dialog "Edit Start Event"	111
75.	Dialog "Edit Filter"	112
76.	Anzeige "Packet Decode"	116
77.	Anzeige "Conversation Trace" für IP	118
78.	Viewman -Menüleiste und -Funktionsleiste	122
79.	Collector-Hauptfenster	122
80.	Gemischte Adreßumsetzungsebenen in Reporter	124
81.	Dialog "Set Translation Level"	124
82.	Dialog "Data Collection Configurations"	125
83.	Dialog "Data Collection Editor"	126
84.	Reporter-Hauptfenster	132
85.	Dialog "New Database File"	133
86.	Dialog "Open Database File"	134
87.	Dialog "Import Files"	134
88.	Dialog "Summary Data"	135
89.	Dialog "Report Configuration"	136
90.	Report Configuration	137
91.	Dialog "Report Configuration"	138
92.	Berichtsausgabeoptionen auswählen	138
93.	Indexzunge "Preview"	140

94.	Gespeicherte Berichte laden	141
95.	Dialog "Page Setup"	142
96.	Mehrere Datensätze zusammenfassen	144
97.	Ursprüngliche Datensammlungen	144
98.	Nach der ersten Zusammenfassung	145
99.	Nach der zweiten Zusammenfassung	145
100.	Dialog "Data Management"	146

Tabellen

1.	Textkonventionen	xvi
2.	Rmonview-Tools	13
3.	Beibehaltene und verlorene RMON-Daten	30
4.	Beibehaltene und verlorene RMON2-Daten	31
5.	Sicherheitsstufen	33
6.	Vordefinierte Kanäle (Filter)	41
7.	Knopf "Invert"	42
8.	Namenumsetzungsebenen	62
9.	Verfügbare Diagramme nach Datenträgertyp	68
10.	Diagrammvariablen für "Packet Rate" nach Datenträgertyp	70
11.	Diagrammvariablen für "Network Statistics" nach Datenträgertyp	71
12.	Variablen für "Ring Status" für FDDI	75
13.	Variablen für "Ring Status" für Token-Ring	75
14.	Vordefinierte Statistikanzeigen	83
15.	Vordefinierte Protokollanzeigen	85
16.	Vordefinierte Host-Anzeigen	88
17.	Vordefinierte Matrixanzeigen	92
18.	Vordefinierte Token-Ring-Anzeigen	94
19.	Anzeige "Address Translation"	99
20.	Anzeige "Protocol Distribution"	101
21.	Knopf "Invert"	108
22.	Filterschablonen nach Datenträgertyp der Schnittstelle	114
23.	Dateiformate für Packet Decode	119
24.	Von Collector erstellte CSV-Dateien	129
25.	Liste der unterstützten Protokolldecodierungen nach Protokollfamilie	151
26.	Auf Ethernet verfügbare Variablen für Statistics	153
27.	Auf FDDI verfügbare Variablen für Statistics	154
28.	Auf Token-Ring verfügbare Variablen für Statistics	155
29.	Auf Ethernet verfügbare Variablen für History	158
30.	Auf FDDI verfügbare Variablen für History	159
31.	Auf Token-Ring verfügbare Variablen für History	160
32.	Auf Ethernet, FDDI und Token-Ring verfügbare Variablen für Hosts	162
33.	Auf Token-Ring verfügbare Variablen für Ring Station	163
34.	Beispiel für Verarbeitungszeiten in Reporter	165
35.	Von Collector erstellte CSV-Dateien	167
36.	Inhalt der CSV-Datei für Protokolldaten	168
37.	Inhalt der CSV-Datei für Host-Daten	169
38.	Inhalt der CSV-Datei für Matrixdaten	170
39.	Inhalt der CSV-Datei für MAC-Schichtprotokolldaten für Token-Ring	171
40.	Inhalt der CSV-Datei für sonstige Protokolldaten für Token-Ring	173
41.	Protokollberichte	175
42.	Host-Berichte	176
43.	Matrixberichte	177
44.	Nicht editierbare HTML-Kommentare	179
45.	Protokolle, die einer Protokollfamilie zugeordnet werden	181

46.	Verfügbare Statistikvariablen zu Ethernet	185
47.	Vordefinierte Protokolle - Protokolle der MAC-Schicht	188

Zu diesem Handbuch

In diesem Handbuch wird IBM Nways® Remote Monitor für Windows NT® (Nways Remote Monitor) beschrieben und erklärt, wie Sie mit dieser Anwendung statistische Daten und Protokollinformationen für Ihr Netzwerk sammeln und überwachen können.

Wenn die zum Lieferumfang dieses Produkts gehörende Informationsdatei vom Inhalt dieses Handbuchs abweicht, ist die Informationsdatei maßgeblich.

In der zum Lieferumfang dieses Produkts gehörenden Informationsdatei finden Sie Informationen zur minimalen Systemkonfiguration und zu unterstützten Betriebssystemen sowie zu den minimalen Sonden-Firmware- und SmartAgent-Softwareversionen.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die für die Überwachung und Verwaltung von Netzwerksegmenten mit Hilfe von Nways Remote Monitor für Windows NT verantwortlich sind.

Neue Funktionen in diesem Release

Dieses Release von Nways Remote Monitor für Windows NT bietet folgende neue Funktionen:

- Unterstützung für RMON2-Adreßumsetzung (Address Translation) und -Protokollverteilung (Protocol Distribution)
- Anpassung des Viewman-Hauptfensters und Aktivierung bzw. Inaktivierung bestimmter Diagramme
- Anzeige mehrerer Viewman-Hauptfenster
- Definition benutzerdefinierter Protokolle mit Hilfe des RMON2-Protokollverzeichnismanagers (Protocol Directory Manager)
- Generierung HTML-basierter Berichte in Nways Remote Monitor Reporter

Konventionen

Tabelle 1 listet die Konventionen auf, die in diesem Handbuch verwendet werden.

Tabelle 1. Textkonventionen

Konvention	Beschreibung
In einer besonderen Schriftart dargestellter Text	Dieses Schriftbild wird zur Darstellung von Nachrichten und Anzeigen verwendet, die am Bildschirm Ihres Terminals angezeigt werden, z. B.: NetLogin:
Als Befehl dargestellter Text	Dieses Schriftbild wird zur Darstellung von Befehlen verwendet, die Sie eingeben, z. B.: SETDefault !0 -IP NETaddr = 0.0.0.0
Tasten	Wenn bestimmte Tasten im Text erwähnt werden, werden sie mit ihrer Bezeichnung verwendet, wie „die Rückföhrtaste“ oder „ die Abbruchtaste“ oder als Eingabe oder Esc angezeigt. Wenn mehrere Tasten gleichzeitig gedrückt werden müssen, werden Sie mit einem Pluszeichen (+) verbunden, z. B.: Drücken Sie Strg+Alt+Entf.
<i>Kursivdruck</i>	<i>Kursivdruck</i> wird zum Hervorheben <i>neuer Begriffe</i> verwendet.

Terminologie

In diesem Abschnitt werden mehrere in diesem Handbuch verwendete Begriffe mit ihren Definitionen aufgelistet.

Einheit, Agent oder Sonde	Generischer Begriff für in Ihrem Netzwerk installierte RMON-Sonden oder -Agenten.
Ethernet	Bezieht sich sowohl auf Ethernet als auch auf Fast Ethernet, sofern in diesem Handbuch nicht anders angegeben.
Firmware	In einer Einheit aktive Software, mitunter auch als Agenten- bzw. Sondensoftware bezeichnet.
Station	Generischer Begriff für in Ihrem Netzwerk installierte Workstations oder andere Netzwerkeinheiten; auch als Host bezeichnet.

Übersicht über Nways Remote Monitor

In diesem Kapitel wird Nways Remote Monitor für Windows NT (Nways Remote Monitor) vorgestellt. Das Kapitel ist in zwei Hauptabschnitte unterteilt:

- Einführung in Nways Remote Monitor

In diesem Abschnitt erhalten Sie eine kurze Übersicht über Nways Remote Monitor, seine Komponentenanwendungen und Funktionen sowie seine Vorzüge für das Netzwerkmanagement.

- Grundlageninformationen

In diesem Abschnitt erhalten Sie einen Überblick über den RMON-Standard sowie eine Einführung in die Funktionsweise von Nways Remote Monitor in Verbindung mit RMON.

- Nways Remote Monitor - Grundlagen
- Neue Funktionen in diesem Release

Einführung in Nways Remote Monitor

Nways Remote Monitor besteht aus integrierten Anwendungen, die Sie zum Anzeigen und Untersuchen der Echtzeit- und Protokolldaten verwenden können, die mit RMON-kompatiblen Einheiten im Netzwerk erfaßt wurden. Sie können diese Einheiten auch über Nways Remote Monitor konfigurieren und steuern.

Sie können Nways Remote Monitor für folgende Aufgaben einsetzen:

- Überwachung der aktuellen Leistung von Netzwerksegmenten
- Anzeige von Trends über die Zeit (Viewman, das Nways Remote Monitor-Hauptfenster, zeigt die kurzfristigen Trends an, während die Anwendung History mittel- bis langfristige Trends aufzeigt)
- Erkennung von Anzeichen aktueller Probleme (z. B. unregelmäßige Paketgrößen, Fehler und Kollisionen)
- Konfiguration von Alarmnachrichten zur Überwachung spezifischer Ereignisse in einem Segment und zur Erfassung und Anzeige von Paketen mit Filter- und Decodierfunktionen

In festgelegten Intervallen fragt Nways Remote Monitor ferne Netzwerksonden ab, um die wichtigsten Netzwerkdaten abzurufen, die es dann verarbeitet und dynamisch im Hauptfenster anzeigt. Über Viewman können Sie die den korrekten Betrieb eines Segments, dessen aktuelle Leistung und die neuesten Trends überwachen.

Für eine detaillierte Untersuchung können Sie die RMON- und RMON2-Anwendungen von Nways Remote Monitor über Viewman oder unabhängig über Ihre Systemsoftware starten. Mit diesen Anwendungen können Sie statistische Daten und Protokollinformationen anzeigen, Alarmbedingungen definieren, Datenaustausch zwischen Stationen im Netzwerk überwachen und bestimmte Pakete erfassen und anzeigen.

Weitere Anwendungen können durch Herunterladen der SmartAgent-Software auf die Sonden hinzugefügt werden. Diese Software kann dann entladen werden, wenn die Anwendungen nicht mehr benötigt werden. SmartAgent-Software kann auch in der Autostart-Tabelle einer Sonde registriert werden, so daß die Sonde versucht, die Software erneut zu laden, wenn sie neu gestartet wird.

Nways Remote Monitor zum Netzwerkmanagement verwenden

Viewman und die RMON-Anwendungen können einzeln oder gemeinsam für proaktives Netzwerkmanagement verwendet werden. Dabei werden statistische Daten gesammelt, um Probleme frühzeitig erkennen und auf sie reagieren zu können.

- Mit Viewman und der Anwendung Statistics können Sie in regelmäßigen Abständen die Leistung und die Auslastung des Netzwerks prüfen, um auftretende Probleme und kurzfristige Trends sofort zu erkennen.
- Bei spezifischen Problemen kombinieren Sie die Anwendungen Alarms und Capture, um Pakete zu erfassen, die zu einem angegebenen Ereignis führen oder darauf folgen. Verwenden Sie dann die Anwendung Decode und Conversation Trace and Analysis, um die Ursache des Problems herauszufinden.
- Mit den Anwendungen Hosts und Matrix können Sie Informationen zu den am meisten ausgelasteten Stationen in Ihrem Netzwerk erhalten.
- Verwenden Sie die Anwendung History, um die Schwankungen und Trends in der Netzwerkstatistik über einen bestimmten Zeitraum anzuzeigen. Durch diese Informationen haben Sie die Möglichkeit, neue Kapazitäten einzuplanen und zu implementieren, bevor die aktuelle Kapazität erschöpft ist.
- Die Anwendung History kann Ihnen auch beim Erkennen gelegentlicher Schwankungen in der Netzwerknutzung helfen, die durch eine Neukonfiguration vorhandener Netzwerkressourcen behoben werden können. Sie können dann eine Kombination von Alarms und Capture implementieren, um darauf zu achten, ob dieses Problems erneut auftritt.

Grundlageninformationen

In diesem Abschnitt werden einige der grundlegenden Konzepte der fernen Netzwerküberwachung mit Hilfe von Nways Remote Monitor eingeführt. Der Abschnitt ist in zwei Abschnitte unterteilt. Der erste Abschnitt bietet eine Übersicht der Standards RMON und RMON2 sowie Überlegungen zur fernen Netzwerküberwachung. Der zweite Abschnitt bietet eine kurze Beschreibung der Tools und Methoden von Nways Remote Monitor für das Verwalten des Netzwerks.

RMON-Übersicht

Vor dem RMON-Standard konnten Managementanwendungen den Datenverkehr zu und von jeder Einheit in einem LAN abrufen, nicht jedoch Informationen zum gesamten Datenverkehr im LAN sammeln. Der RMON-Standard bietet eine effektive und effiziente Möglichkeit zur Überwachung des Verhaltens des gesamten LAN und verringert gleichzeitig den allgemeinen Systemaufwand auf fernen Sonden und auf Managementstationen.

RMON-Sonden sind intelligente, ferngesteuerte Einheiten, die Informationen zum Netzwerkverhalten sammeln und diese auf Abruf an einen Analysestandort übertragen. Eine Sonde kann als eigenständige Einheit oder als Agent in einem Hub, Router oder Switch eingesetzt werden. Die Verwendung von RMON-Sonden steigert die Effizienz der Mitarbeiter, weil diese an einem zentralen System bleiben und gleichzeitig Informationen von weit verteilten LAN-Segmenten sammeln können. Ein weiterer Vorteil ferner Sonden besteht darin, daß sie auch eine kontinuierliche Überwachung ermöglichen und dabei Informationen sammeln und diese weiterleiten, bevor Probleme auftreten, so daß die Administratoren ihre Netzwerke proaktiv verwalten können.

Jede ferne Sonde kann Anfragen von mehreren Managementanwendungen ausführen. Eine Managementanwendung, wie Nways Remote Monitor, wird typischerweise auf der Netzwerkmanagementstation ausgeführt. Durch die Verwendung einer Managementanwendung können Netzwerkadministratoren, die für bestimmte Aspekte des Netzwerkbetriebs verantwortlich sind, die Funktionen der Sonde nutzen, um ihre eigenen Datenanforderungen zu erfüllen.

Die Managementanwendung definiert die entsprechenden Variablen der RMON-Managementinformationsdatenbank (MIB - Management Information Base) für Meßintervalle, überwachte Schwellenwerte und andere Verarbeitungsparameter. Die ferne Sonde sammelt und speichert Informationen und liefert diese auf Anfrage an die Managementanwendung. Sonden können auch eine SNMP-Alarmnachricht an eine Gruppe von Managementstationen senden, wenn bestimmte Bedingungen festgestellt wurden, und so den Netzwerkadministrator über eine kritische Situation informieren, die sofort behoben werden muß.

RMON2-Standard

RMON2 ist eine Erweiterung des RMON-Standards. RMON2 sammelt statistische Daten in der Vermittlungs- und der Anwendungsschicht der Protokollgruppe. Nways Remote Monitor verwendet RMON2-Funktionalität, um dem Benutzer das Anzeigen der Verteilung von Protokollen im Netzwerk zu ermöglichen. Das Produkt verwendet darüber hinaus auch Adreßzuordnung, damit der Benutzer Netzwerkadressen im gesamten Netzwerk erkennen kann.

Mit statistischen RMON2-Daten ist ersichtlich, welche Stationen miteinander Daten austauschen und welche Anwendungen verwendet werden. Mit ihnen kann der Netzwerkmanager die Leistung aktueller Netzwerkressourcen besser optimieren und Client/Server- und Wählnetzwerkumgebungen besser verwalten.

Grundlagen von Nways Remote Monitor

Nways Remote Monitor besteht aus den folgenden Anwendungen:

- | | |
|--------------------|---|
| Viewman | Diese Anwendung besteht aus einem Hauptfenster, in dem Sie die wichtigsten Parameter für den Netzwerkbetrieb überwachen können. Sie können auch alle anderen Anwendungen von hier aus starten. |
| Config | Diese Anwendung wird zum Definieren der Adreßumsetzungsebenen und zum Bearbeiten der Stationsinformationsliste verwendet. Sie kann von Viewman, Translator, Collector und vom System aus gestartet werden. |
| Translator | Diese Anwendung sammelt Stationsinformationen von jeder Sonde, auf der ECAM-(RMON2-)SmartAgent-Software geladen ist. Die sich ergebende Adreßumsetzungstabelle bietet Stationsinformationen für alle anderen Anwendungen von Nways Remote Monitor. |
| Capture | Diese Anwendung erfaßt Pakete beim Zutreffen bestimmter Alarmbedingungen und läßt Sie nur die von Ihnen benötigten Pakete ausfiltern und sie für die Analyse speichern. |
| Decode | Diese Anwendung decodiert erfaßte Pakete und zeigt alle wichtigen Protokolle in leicht lesbarem Format an. Verwenden Sie anschließend Conversation Trace and Analysis, um die Komponentenpakete zusammen mit ihren Übertragungszeiten zu protokollieren. |
| Reporter | Diese Anwendung ist ein Tool zur Datensammlung und Berichterstellung, das ideal für kleinere Netzwerke oder zum Erstellen von Berichten zu einer beschränkten Anzahl von RMON-Einheiten in einer größeren Netzwerkumgebung ist. Sie besteht aus zwei Hauptkomponenten, Collector und Reporter, die einen optimierten Ansatz zum Sammeln wichtiger statistischer Daten und zum Erstellen wertvoller Netzwerkberichte bieten.

Collector und Reporter arbeiten in Verbindung mit Nways Remote Monitor und der IBM Familie von RMON-Ethernet-, -Fast-Ethernet- und -Token-Ring-Sonden sowie anderen RMON-kompatiblen Ethernet-, Fast-Ethernet- und Token-Ring-Einheiten im Netzwerk. |
| SmartAgents | SmartAgents können jederzeit von einer Sonde geladen oder entladen werden, um RMON2-ähnliche Anwendungen zu bieten. |

Rmonview	Diese Anwendung besteht aus neun RMON-Anwendungen: Statistics, History, Hosts, Alarms, Matrix, Ring Station, Protocol Distribution, Address Translation sowie dem Rmonview-Fenster, in dem diese Anwendungen angezeigt werden.
Statistics	Diese Anwendung zeigt statistische Segmentdaten zu jeder Kombination von Paketen, Byte, Fehlern und Größenverteilung oder selektivem Rundsenden an. Die Daten werden in Echtzeit aktualisiert.
History	Diese Anwendung gibt eine Stichprobenperiode und punktuelle Trends über Stunden, Tage, Wochen und sogar Monate an.
Hosts	Diese Anwendung zeigt detaillierte Informationen zu den Hosts in einem Segment an.
Alarms	Diese Anwendung überwacht spezifische Ereignisse im Netzwerk bei ihrem Auftreten. Verwenden Sie Alarms allein oder in Verbindung mit Capture.
Matrix	Diese Anwendung stellt fest, welche Hosts untereinander im Netzwerk Daten austauschen und wieviel Datenverkehr zwischen ihnen fließt. Sie gibt Stationen an, die möglicherweise Probleme verursachen.
Ring Station (Token-Ring)	Diese Anwendung zeigt Ringinformationen nur für einen Token-Ring an, einschließlich Stationsstatus und die Zeit des letzten Eintritts und des letzten Verlassens.
Protocol Distribution	Diese Anwendung zeigt die Protokollverteilung als Tabelle, Balkendiagramm oder Tortendiagramm an.
Address Translation	Diese Anwendung zeigt eine Tabelle mit der Zuordnung zwischen der MAC-Adresse und der Vermittlungsschicht an.

Neue Funktionen in diesem Release

Dieses Release von Nways Remote Monitor für Windows NT bietet folgende neue Funktionen:

- Unterstützung für RMON2-Adreßumsetzung (Address Translation) und -Protokollverteilung (Protocol Distribution)
- Anpassung des Viewman-Hauptfensters und Aktivierung oder Inaktivierung bestimmter Diagramme
- Anzeige mehrerer Viewman-Hauptfenster
- Definition benutzerdefinierter Protokolle mit dem RMON2-Protokollverzeichnismanager (Protocol Directory Manager)
- Generierung HTML-basierter Berichte in Nways Remote Monitor Reporter

Mit der Schnittstelle von Nways Remote Monitor arbeiten

In diesem Kapitel werden folgende Schnittstellen beschrieben:

- Viewman und Rmonview

Viewman und Rmonview bestehen jeweils aus einem Hauptfenster, in dem Sie weitere Anwendungen von Nways Remote Monitor starten können. Viewman ist eine eigenständige Überwachungsanwendung, Rmonview wird dagegen einfach als Start- und Anzeigebereich für die RMON-Anwendungen von Nways Remote Monitor verwendet und führt nicht selbst Überwachungen oder Statistiksammlungen durch.

- Collector und Reporter

In diesen Abschnitte werden die Schnittstellen für Collector und Reporter beschrieben.

Viewman-Schnittstelle

Viewman besteht aus einem Hauptfenster, in dem Sie die Leistung eines LAN-Segments überwachen können. Sie können auch alle anderen Anwendungen von Nways Remote Monitor und RMON2/SmartAgent-Anwendungen in diesem Fenster starten.

Das Hauptfenster ist in fünf Bereiche unterteilt (siehe Abb. 1):

- Menüleiste
- Funktionsleiste
- Zusammenfassungsbereich
- Alarmbereich
- Statusleiste

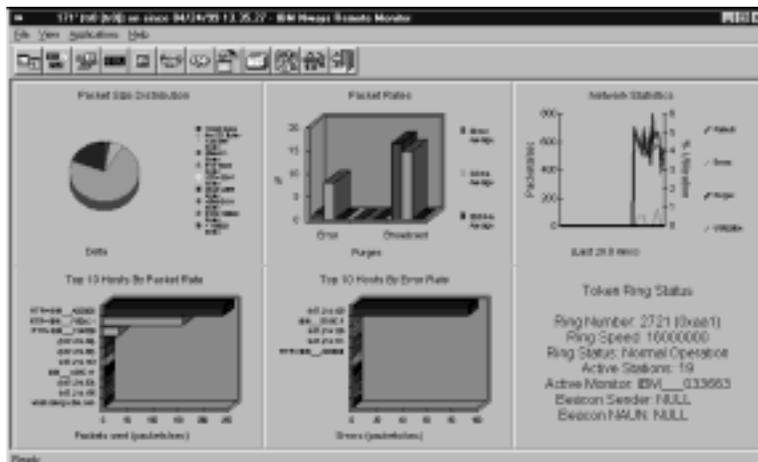


Abbildung 1. Viewman-Hauptfenster

Menüleiste

Die Menüleiste am oberen Fensterrand enthält die folgenden Menüoptionen:

File	Der Befehl New öffnet ein neues Viewman-Hauptfenster.
View	Über dieses Menü können Sie die Anzeige eines Bereichs im Hauptfenster aktivieren oder inaktivieren, die angezeigten Daten aktualisieren, die Diagramme für die Anzeige im Zusammenfassungsbereich auswählen oder mit der Option Device Options das zu überwachende LAN-Segment auswählen.
Applications	In diesem Menü können Sie alle Anwendungen von Nways Remote Monitor starten, einschließlich des Dialogs Device Configuration .
Help	Dieses Menü bietet Zugriff auf die Hilfe zu Viewman und zur umfassenden Online-Hilfefunktion von Nways Remote Monitor.

Funktionsleiste

Die Funktionsleiste unterhalb der Menüleiste zeigt eine Teilliste der verfügbaren Anwendungen von Nways Remote Monitor an. Klicken Sie einen Knopf an, um den entsprechenden Anwendungsdialog zu starten. Die Funktionsleiste enthält auch einen Knopf **Exit**, mit dem Sie Viewman verlassen können.

Zusammenfassungsbereich

Die sechs Felder des Zusammenfassungsbereichs stellen den größten Teil des Hauptfensters dar. Diese Felder enthalten grafische Darstellungen der wichtigsten statistischen Netzwerkdaten und sind je nach Datenträgertyp des überwachten Segments unterschiedlich.

Eine Beschreibung der unterschiedlichen Diagramme finden Sie in „Viewman-Diagramme“ auf Seite 68.

Alarmleiste

Die Alarmleiste befindet sich unter dem Zusammenfassungsbereich. Alarmsymbole in dieser Leiste werden rot dargestellt, sobald ein Alarm ausgelöst wird. Wenn Sie den Mauszeiger auf ein Alarmsymbol setzen, wird eine Alarmstatusnachricht in der Statusleiste angezeigt.

Statusleiste

Die Statusleiste unterhalb der Alarmleiste zeigt Systemnachrichten und Alarmstatusinformationen an.

Rmonview-Schnittstelle

Rmonview ist die RMON-Anzeige von Nways Remote Monitor. Alle RMON-Anwendungen können vom Rmonview-Fenster aus gestartet werden. Die Anwendungen verwenden dieses Fenster auch zur Anzeige von Daten (siehe „Rmonview und RMON-Anwendungen“ auf Seite 77). Jede Anwendung öffnet ein neues Fenster im Anzeigebereich von Rmonview. Es gibt keine Beschränkung bezüglich der Anzahl der gleichzeitig geöffneten Anwendungsfenster. Rmonview kann auf Symbolgröße verkleinert werden, so daß es im Hintergrund aktiv ist.

Dialog "... View"

Dieser Dialog wird angezeigt, wenn Sie eine neue Rmonview-Anwendung starten. Mit ihm können Sie die RMON-Sonde und -Schnittstelle für die Anwendung zum Analysieren und Anzeigen auswählen. Über diesen Dialog können Sie auch die Statistikelemente auswählen, die die Anwendung anzeigen soll. Mit diesen Optionen können Sie die Anwendungsanzeige anpassen. Einige der Abschnitte dieses Dialogs sind hier beschrieben. Ausführlichere Informationen finden Sie in „RMON-Anwendungen konfigurieren“ auf Seite 80.

Probe	Dieser Bereich enthält eine Liste aller konfigurierten Sonden (siehe „Sonden definieren“ auf Seite 21). Die hervorgehobene Sonde ist die aktuelle Auswahl. Klicken Sie eine Sonde an, um sie auszuwählen.
Interface	In diesem Bereich wird eine Liste verfügbarer Schnittstellen angezeigt, wenn auf die ausgewählte Sonde zugegriffen werden kann. Klicken Sie eine Schnittstelle an, um sie auszuwählen.
View	Wählen Sie eine vordefinierte Anzeige aus, oder erstellen Sie Ihre eigene Anzeige. Diese Anzeige bestimmt, welche Statistikelemente angezeigt werden.
Update Rate	Geben Sie an, wie oft die Anzeige mit neuen Daten aktualisiert werden soll.
Community String	SNMP-Einheiten im Netzwerk verwenden diese Zeichenfolge, um den Zugriff auf die Sonde einzuschränken. Diese kann für jede Sonde geändert werden (siehe „Benutzergemeinschafts-Zugriffsnamen“ auf Seite 33).
OK, Close, Help	<ul style="list-style-type: none">• Klicken Sie OK an, um die in diesem Dialog vorgenommenen Auswahlen zu implementieren.• Klicken Sie Close an, um Ihre Auswahlen zu verwerfen und zur vorhergehenden Ebene zurückzukehren.• Klicken Sie Help an, um den Online-Hilfetext aufzurufen.

Menüleiste

Der Inhalt der Menüleiste am oberen Fensterrand hängt davon ab, ob RMON-Daten angezeigt werden.

File

New	Bietet Zugriff auf alle RMON-Anwendungen. Wenn Sie eine RMON-Anwendung in diesem Menü auswählen, wird der Konfigurationsdialog der Anwendung gestartet.
Open	Öffnet bereits gespeicherte RMON-Anwendungsanzeigen. Diese Option ist auch über die Funktionsleiste verfügbar.
Close	Schließt die aktuell ausgewählten RMON-Anwendungsanzeigen.
Save, Save As	Speichert die Konfigurationsanzeige des aktuellen Anwendungsfensters in einer Datei.
Print Graphic	Druckt den aktuellen Dialog auf dem Standarddrucker Ihres Systems.
Print Setup	Legt die Druckmerkmale der aktuellen zu druckenden Anzeige fest.
Export	Exportiert den Inhalt der angezeigten Tabellen in ASCII- oder CSV-Dateien.
Recent File	Listet die zuletzt gespeicherten Anwendungsanzeigen auf. Wählen Sie den Dateinamen aus, um die entsprechende Anwendung zu starten. Wenn die Option Recent File abgeblendet ist, gibt es keine gespeicherten Anzeigen.
Exit	Beendet Rmonview.

View

Toolbar	Blendet die Funktionsleiste im Anwendungsfenster ein und aus.
Status Bar	Blendet die Statusleiste im Anwendungsfenster ein und aus.
Graph Only, Graph and Table, Table Only	Konfiguriert die Anwendungsanzeige so um, daß nur das Diagramm, nur die Tabelle oder Tabelle und Diagramm gleich groß angezeigt werden. Sie können auch die Größe der Bereiche anpassen, indem Sie den mittleren Trennbalken mit der Maus nach links oder rechts ziehen. Diese Optionen sind auch über die Funktionsleiste verfügbar.

	Clear Flags	Wenn Sie Daten in einem Diagramm anklicken, wird eine Markierung angezeigt, die das genaue Datum und die genaue Uhrzeit der Erfassung der ausgewählten Daten, eine Variablenbeschreibung und den Wert für diese Variable angibt. Dieser Menüpunkt löscht alle Markierungen aus einem Diagramm.
	Pause Graph, Resume Graphing	Aktiviert und inaktiviert die Aktualisierung von Daten im Diagramm. Wenn Automatic Upload aktiv ist oder die Option Manual Update ausgewählt ist, werden die Daten noch von der Sonde hochgeladen, die Anzeige im Diagrammbereich wird jedoch erst aktualisiert, wenn die Option Resume Graphing ausgewählt wird.
Options	Display Graph	Blendet das Diagramm in der ausgewählten Anzeige ein und aus.
	Automatic Upload	Wenn diese Option aktiviert ist, werden neue Daten in dem im Konfigurationsdialog der Anzeige angegebenen Intervall hochgeladen.
	Manual Upload	Wenn diese Option aktiviert ist, wird das automatische Hochladen inaktiviert. Neue Daten werden erst hochgeladen, wenn Sie den Knopf Manual Update anklicken.
	Line Width	Gibt die Breite der Linien in Liniengrafiken an.
	Table Control	Öffnet ein Dialogfenster, in dem Sie die Optionen für Größe und Umbruch für die aktive Anzeigentabelle der Anwendung einstellen können.
	Graphed Values	Legt den Wert für das Diagramm fest. Sie können entweder die Werte für die Änderung über das angegebene Zeitintervall (Delta) oder die absoluten Gesamtwerte seit dem Starten der Sonde auswählen.
Update		Über dieses Menü können Sie eine Aktualisierung der Anwendungsanzeige erzwingen.
Window		Dieses Menü enthält die Standardfunktionen von Microsoft® Windows zum Arbeiten mit Fenstern.
Help		Dieses Menü bietet Zugriff auf die umfassende Online-Hilfefunktion von Nways Remote Monitor.

Funktionsleiste

Die Funktionsleiste enthält die in Tabelle 2 beschriebenen Knöpfe.

Tabelle 2. Rmonview-Tools

Tool	Beschreibung
 Open	Öffnet eine gespeicherte Anwendungsdatei zur Anzeige.
 Save	Speichert den Inhalt der aktuellen Anzeige in einer Datei.
 Print Graph	Druckt die aktuelle Anzeige auf dem Standarddrucker Ihres Systems.
 Display Event Data	Blendet die Diagrammanzeige ein und aus.
 Resume Graphing	Setzt die grafische Darstellung fort.
 Pause Graph	Unterbricht die grafische Darstellung.
 Automatic Upload	Bewirkt, daß neue Daten im angegebenen Aktualisierungsintervall hochgeladen werden (sofern aktiviert).
 Manual Upload	Inaktiviert das automatische Hochladen (sofern aktiviert). Neue Daten werden erst hochgeladen, wenn Sie den Knopf Manual Update anklicken.
 Manual Update	Erzwingt in Verbindung mit dem Tool Manual Upload eine neue Aktualisierung im Konfigurationsdialog der Anwendung.
 Graph Only	Ändert die Größe des Anwendungsfensters so, daß nur das Diagramm angezeigt wird.
 Table & Graph	Ändert die Größe des Anwendungsfensters so, daß das Diagramm und die Tabelle angezeigt werden.
 Table Only	Ändert die Größe des Anwendungsfensters so, daß nur die Tabelle angezeigt wird.

Die Funktionsleiste enthält auch zwei weitere Funktionen:

Diagrammliste Mit dieser Liste können Sie das Format der aktuellen Diagrammanzeige auswählen oder ändern. Folgende Anzeigeformate sind verfügbar: **Line Graph**, **3D Tape**, **Log/Lin**, **Histogram** und **Pie**.

Lade-/Aktualisierungsstatus

Dieses Feld zeigt Statusnachrichten zum Hochladen und Aktualisieren an.

Anwendungsanzeigebereich

Die RMON- und RMON2/Smart-Agent-Anwendungsfenster werden in diesem Bereich angezeigt. In diesem Bereich kann gleichzeitig eine beliebige Anzahl von Anwendungsfenstern geöffnet sein. Mit den Optionen im Menü **Window** und den Standardknöpfen zum Maximieren, Minimieren und Schließen oben rechts in jedem Anwendungsfenster können Sie die Fensteranzeige steuern.

Statistikanzeigen

Rmonview unterstützt mehrere Fenster in seinem Anzeigebereich. Alle Anwendungen verwenden ein Standardformat.

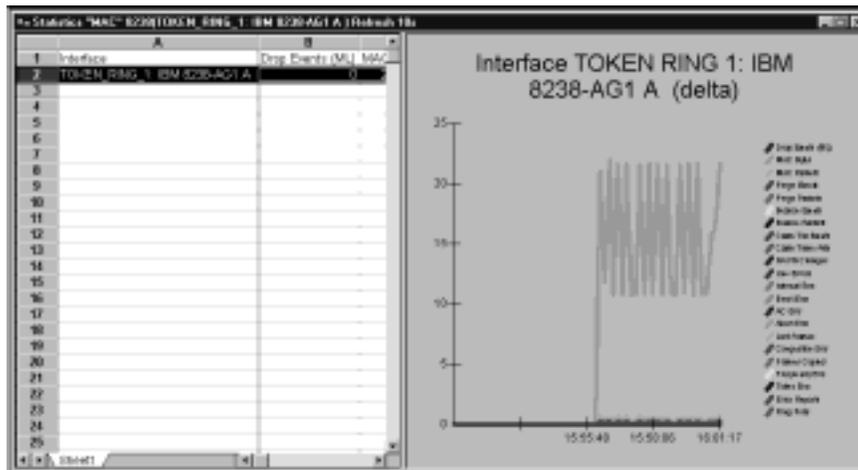


Abbildung 3. Statistikanzeigen in Rmonview

Die Anzeige ist in zwei Bereiche aufgeteilt:

Tabelle

Statistische Daten werden in Tabellenform im linken Bereich der Anzeige dargestellt. Gehen Sie wie folgt vor, um Einträge für die grafische Darstellung auszuwählen:

- Stellen Sie einzelne Variablen durch Auswahl einer einzelnen Zelle in der Tabelle grafisch dar.
- Stellen Sie mehrere benachbarte Variablen in einer Zeile oder Spalte grafisch dar, indem Sie die erste Zelle anklicken und bei gedrückter Umschalttaste die letzte benachbarte Zelle anklicken.
- Stellen Sie mehrere nicht benachbarte Variablen grafisch dar, indem Sie bei gedrückter Taste **Strg** die einzelnen Zellen anklicken.
- Stellen Sie die Einträge in einer gesamten Zeile oder Spalte grafisch dar, indem Sie den Zeilen- oder Spaltenkopf auswählen.

Diagramm

Eine grafische Darstellung der ausgewählten Daten befindet sich im rechten Bereich der Anzeige. Klicken Sie die Daten im Diagramm an, um eine Markierung anzuzeigen, die das genaue Erfassungsdatum der statistischen Daten mit Uhrzeit, die Art der Statistik und den exakten Wert angibt. Wenn Sie diese Markierungen entfernen wollen, klicken Sie den Menüpunkt **Clear Flags** im Menü **View** an.

Verwenden Sie die Knöpfe **Graph Only**, **Table and Graph** und **Table Only** in der Funktionsleiste oder die entsprechenden Optionen im Menü **View**. Wenn Sie die Größe der Anzeige ändern wollen, klicken Sie den Trennbalken in der Mitte mit der Maus an, und ziehen Sie ihn nach links oder rechts.

Statusleiste

Die Statusleiste befindet sich am unteren Rand des Hauptfensters. Sie zeigt Systemnachrichten an.

Collector-Schnittstelle

In diesem Abschnitt wird die Schnittstelle für Collector beschrieben. Wie Collector gestartet werden kann, ist in „Collector“ auf Seite 121 beschrieben. Das Hauptfenster ist in drei Bereiche unterteilt:

- Menüleiste
- Statusprotokoll
- Statusleiste

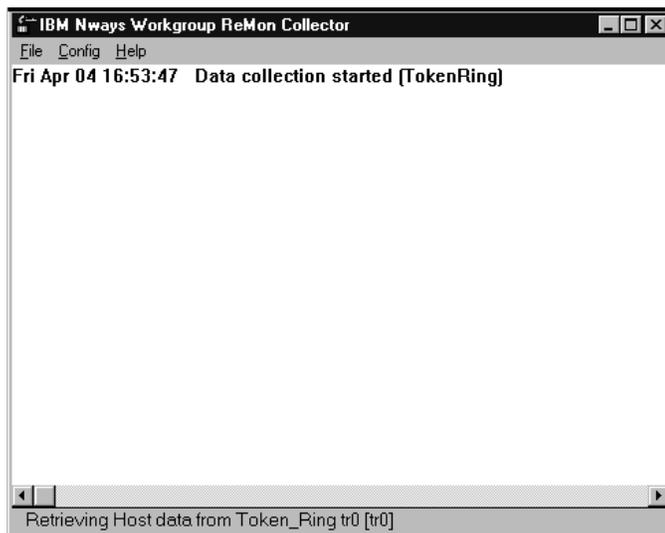


Abbildung 4. Collector-Hauptfenster

Das Hauptfenster zeigt das Statusprotokoll für alle aktuellen Datensammlungskonfigurationen an. Die Statusleiste am unteren Fensterrand bietet Echtzeit-Rückmeldungen, z. B. wann die nächste Datensammlung beginnen wird.

Menüleiste

Folgende Menüoptionen sind in diesem Fenster verfügbar:

File

- Save** Speichert den Inhalt des Statusprotokolls, um eine Aufzeichnung der durchgeführten Datensammlungen zu führen.
- Print** Druckt den Inhalt des Statusprotokolls.
- Exit** Beendet Collector.

Config

- Data Collections**
Erlaubt das Erstellen, Ändern und Löschen von Konfigurationen.
- Address Translation Level**
Ermöglicht das Auswählen der Ebene von Adreßinformationen, die Collector für Einheiten und das bevorzugte Protokoll erkennen soll.
- RMON Devices** Bietet Zugriff auf den Dialog **Device Configuration**, der auch über die Viewman- und Translator-Hauptfenster sowie als eigenständige Anwendung von Ihrer Systemsoftware aus aufgerufen werden kann. In diesem Dialogfenster können Sie die Liste der im Netzwerk verfügbaren RMON-kompatiblen Einheiten definieren.

Help

- Contents** Startet die Online-Hilfefunktion von Remote Monitor.
- About Collector**
Zeigt die Versionsinformationen und den Copyrightvermerk an.

Statusprotokoll

Das Statusprotokoll nimmt den größten Bereich im Hauptfenster ein. Während der Datensammlung werden in diesem Bereich Statusnachrichten angezeigt. Wenn der Bereich mit Nachrichten gefüllt ist, können Sie durch das Protokoll nach oben und unten blättern. Der Inhalt des Protokolls kann über die Optionen im Menü **File** in einer Datei gespeichert oder ausgedruckt werden.

Statusleiste

Die Statusleiste befindet sich am unteren Rand des Hauptfensters. Sie zeigt den Status der aktuellen oder nächsten Sammlung an.

Reporter-Schnittstelle

In diesem Abschnitt werden die Schnittstellen für Reporter beschrieben. Wie Reporter gestartet werden kann, ist in „Reporter“ auf Seite 131 beschrieben. Reporter besteht aus einem Hauptfenster in der Microsoft Access-Datenbankumgebung.



Abbildung 5. Reporter-Hauptfenster

Optionen im Hauptfenster

Folgende Funktionen sind im Reporter-Hauptfenster verfügbar:

New Database	Erstellt eine neue Berichtsdatenbank.
Open Database	Öffnet eine vorhandene Berichtsdatenbank.
Import	Importiert den Inhalt von CSV-Dateien, die in Collector erstellt wurden, in eine Datenbank.
Data Management	Faßt Daten regelmäßig zusammen oder löscht Daten.
Data Summary	Zeigt eine Zusammenfassung der aktuellen Datenbank an.
Report	Generiert Berichte aus der aktuellen Datenbank.
Open Report	Lädt einen gespeicherten Bericht zum Drucken.
Exit	Schließt die Anwendung.

Optionen in der Menüleiste

Folgende Menüoptionen sind in der Menüleiste für Reporter verfügbar:

File

New Database Erstellt eine neue Berichtsdatenbank aus vorhandenen CSV-Dateien.

Open Database Öffnet eine vorhandene Berichtsdatenbank.

Close Database

Schließt die aktuelle Datenbank.

Exit Schließt die Datenbankumgebung.

Wenn Sie eine Vorschau eines Berichts anzeigen (siehe Seite 139) oder einen vorhandenen Bericht geladen haben (siehe Seite 141), sind darüber hinaus die folgenden Optionen verfügbar:

Print Druckt den aktuellen Bericht.

Print Setup Ändert die aktuelle Druckereinrichtung.

Window Ordnet Fenster nebeneinander, überlappend oder in spezieller Reihenfolge an.

Help Zeigt die Versionsinformationen und den Copyrightvermerk an.

Sonden definieren

Sie müssen eine Liste der zum Einsatz verfügbaren Sonden angeben, damit Nways Remote Monitor betriebsbereit ist. Wenn dies abgeschlossen ist, können Sie sofort beginnen, Ihr Netzwerk über Viewman und die Anwendungen von Nways Remote Monitor zu überwachen.

Weitere Konfigurationsvorgänge, wie das Erstellen virtueller Schnittstellen und das Hinzufügen benutzerdefinierter Protokolle, können jederzeit durchgeführt werden.

Dieses Kapitel ist in die folgenden Abschnitte unterteilt:

- Dialog "Device Configuration" öffnen
- Sonden definieren
- Sonden verwalten
- PACMIB aktivieren und inaktivieren
- RMON2-Modus definieren
- Virtuelle Schnittstellen konfigurieren
- RMON- und RMON2-Tabellen verwalten
- RMON-(ECAM)-SmartAgent-Firmware verwalten
- Benutzerdefinierte Protokolle verwalten
- RMON2-Tabellen für Protokolle aktualisieren

Dialog "Device Configuration" öffnen

Der Dialog **Device Configuration** kann wie folgt geöffnet werden:

Über Viewman

Zum Öffnen des Dialogs **Device Configuration** klicken Sie  in der Funktionsleiste an, oder wählen Sie **Config** in der Menüleiste der Anwendung aus.

Über Collector und Translator

Wählen Sie **RMON Devices...** im Menü **Config** in der Menüleiste des Hauptfensters der Anwendung aus.

Über das Menü "Start" von Windows NT

Wählen Sie die Programmgruppe **IBM Nways ReMon** im Menü **Start** und anschließend **Config** aus.

Die Einheitenkonfiguration von Nways Remote Monitor wird vollständig in diesem Dialog durchgeführt.

Sonden definieren

Sie können angeben, welche Sonden Nways Remote Monitor zur Überwachung des Netzwerks verwenden soll. Führen Sie dazu die folgenden Schritte im Dialog **Device Configuration** aus:

1. Klicken Sie **Probes** an, um den Dialog **Probe List Editor** zu öffnen. Standardmäßig ist die erste Sonde in der Liste ausgewählt.

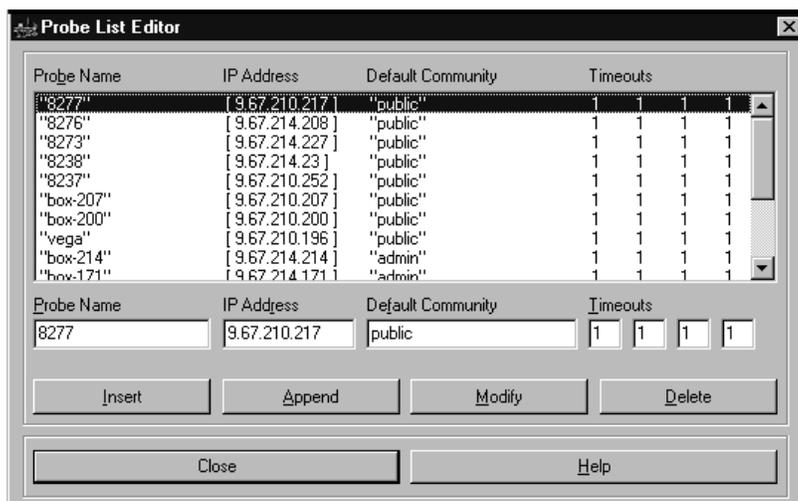


Abbildung 6. Dialog "Probe List Editor"

2. Gehen Sie wie folgt vor, um eine neue Sonde zu definieren:
 - a. Geben Sie im Feld **Probe Name** einen eindeutigen Namen ein.
 - b. Geben Sie im Feld **IP Address** die IP-Adresse für die Sonde im Format n.n.n.n ein. Dabei steht n für eine Dezimalzahl zwischen 0 und 255. Eine IP-Adresse sieht zum Beispiel folgendermaßen aus: 192.128.40.120. Wenn Sie nicht sicher sind, welche IP-Adresse der Sonde zugeordnet ist, wenden Sie sich an Ihren Netzwerkadministrator.
 - c. Ändern Sie in **Default Community** gegebenenfalls den Namen der Benutzergemeinschaft. Das Definieren der Zugriffstabellen für die Benutzergemeinschaft wird in „Zugriffssteuerungstabellen“ auf Seite 32 beschrieben.
 - d. Ändern Sie gegebenenfalls unter **Timeouts** die Zeitlimitüberschreitungswerte für die Sonde. Alle Werte sind standardmäßig auf 1 Sekunde eingestellt. Die Zeitlimitüberschreitungswerte bestimmen die Intervalle, in denen Nways Remote Monitor eine Sonde abfragt, bevor es meldet, daß sie nicht antwortet. Die Standardwerte sind für die meisten Installationen geeignet. Wenn Sie jedoch ein serielles Kabel oder eine langsame Verbindung verwenden, ist die Antwortzeit länger. In diesem Fall könnten Sie die Werte beispielsweise auf 1, 2, 3 und 4 Sekunden erhöhen.
 - e. Klicken Sie **Insert** oder **Append** an, um den neuen Eintrag in die Liste aufzunehmen.

Wenn Sie einen Eintrag ausgewählt haben, wird dieser mit **Insert** vor dem aktuell ausgewählten Eintrag eingefügt; mit **Append** wird er nach der aktuellen Auswahl eingefügt.

3. Gehen Sie wie folgt vor, um einen vorhandenen Sondeneintrag zu ändern:
 - a. Klicken Sie einen vorhandenen Eintrag in der Liste an. Die Einzelangaben zur ausgewählten Sonde werden in den Feldern unter der Sondenliste angezeigt.
 - b. Ändern Sie einen oder mehrere dieser Einträge gemäß der Beschreibung in Schritt 2 auf Seite 22 oben.
 - c. Klicken Sie **Modify** an, um diese Änderungen anzuwenden.

4. Klicken Sie **Close** an, um zum Dialog **Device Configuration** zurückzukehren.

Die neue Sonde wird im Bereich **Select Probe** des Dialogs **Device Configuration** angezeigt.

5. Wenn Sie prüfen wollen, ob die Sonde korrekt definiert wurde und ob eine Verbindung zu ihr hergestellt werden kann, wählen Sie die Sonde durch Anklicken im Bereich **Select Probe** aus.
 - a. Wenn eine Verbindung zu ihr hergestellt werden kann, wird eine Liste der verfügbaren Schnittstellen der Sonde im Bereich **Select Interface** angezeigt.
 - b. Wenn keine Verbindung zur Sonde hergestellt werden kann, wird die Nachricht `Unavailable` in der Liste **Select Interface** angezeigt. Diese Nachricht kann auf folgende Probleme hinweisen:
 - Sie haben die Einzelangaben für die Sonde nicht korrekt angegeben.
 - Die Sonde ist aufgrund eines Netzwerkproblems vorübergehend nicht verfügbar.
 - Die angegebenen Zeitlimitüberschreitungswerte sind nicht groß genug, um eine Verbindung zur Sonde herzustellen.
 - Die angegebene Benutzergemeinschaft hat nicht die benötigten Zugriffsrechte.

Prüfen Sie, ob die im Dialog **Probe List Editor** eingegebenen Informationen korrekt sind, und versuchen Sie erneut, eine Verbindung zur Sonde herzustellen.

Sobald Sie diese Schritte ausgeführt haben, können Sie Ihr Netzwerk sofort über das Hauptfenster (siehe Viewman) und die Anwendungen von Nways Remote Monitor (siehe Rmonview und RMON-Anwendungen sowie Packet Capture und Decode) überwachen.

Sie können auch jederzeit weitere Konfigurationsschritte für die fernen Sonden vornehmen. Diese werden in den folgenden Abschnitten behandelt.

Sonden verwalten

Für IBM 8250 Ethernet Probe und IBM 8260 High-End Token-Ring Media Access Daughter Card können Sie die folgenden Informationen aus dem Dialog **Agent Maintenance** anzeigen und konfigurieren:

- Sie können die Hardware- und Firmware-Versionen anzeigen und neue Firmware herunterladen.
- Sie können Datum und Uhrzeit sowie das Echointervall anzeigen und definieren.
- Sie können die PACMIB-Verfügbarkeit anzeigen und definieren.
- Sie können die RMON2-Verfügbarkeit anzeigen und definieren.
- Sie können die IP-Adresse, die Teilnetzmaske und den Standard-Gateway einer Sonde anzeigen und definieren.
- Sie können eine Sonde mit Kalt- oder Warmstart zurücksetzen.
- Sie können Zugriffssteuerungstabellen anzeigen und konfigurieren.
- Sie können Alarmnachricht-Benutzergemeinschaften anzeigen und konfigurieren.

Dieser Abschnitt gilt nur für RMON-Agenten, die die MIB „Aspen“ implementieren.

Gehen Sie wie folgt vor, um den Dialog **Agent Maintenance** zu öffnen:

1. Wählen Sie im Dialog **Device Configuration** die gewünschte Sonde aus.
2. Bei Sonden, die mehrere Schnittstellen unterstützen, wie z. B. IBM 8250 Ethernet RMON Probe und IBM 8250 High-End Ethernet Media Access Daughter Card, können Sie die IP-Adresse für jede beliebige der aufgeführten physikalischen Schnittstellen definieren.

Wählen Sie eine Schnittstelle durch Anklicken in der Liste **Select Interface** aus.

Sie können die IP-Adressen für virtuelle Schnittstellen nicht definieren. (Eine Beschreibung virtueller Schnittstellen finden Sie in „Virtuelle Schnittstellen konfigurieren“ auf Seite 39.)

3. Klicken Sie **Admin** an. Sie werden aufgefordert, den Benutzergemeinschaftsnamen der Sicherheitsstufe 4 anzugeben, um auf die Konfigurationsdaten der ausgewählten Sonde zugreifen zu können. (Eine Erklärung der Benutzergemeinschaftsnamen finden Sie in „Zugriffssteuerungstabellen“ auf Seite 32.)

Wenn Sie auf den Dialog **Agent Maintenance** zugreifen wollen, müssen Sie einen Benutzergemeinschaftsnamen der Sicherheitsstufe 4 haben (die Stufen sind in Tabelle 5 auf Seite 33 definiert). Wenn Sie diesen Namen vergessen, müssen Sie über ein direkt an die Sonde angeschlossenes Terminal einen Kaltstart der Sonde ausführen.

4. Klicken Sie **OK** an. Der Dialog **Agent Maintenance** wird geöffnet.

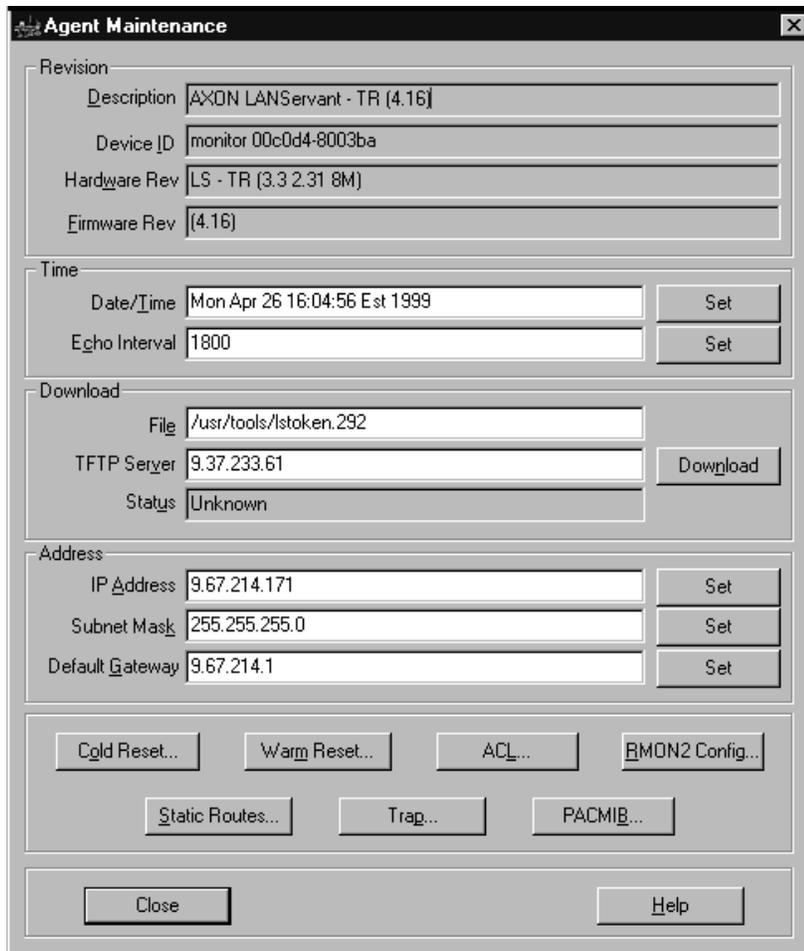


Abbildung 7. Dialog "Agent Maintenance"

Hardware- und Firmware-Versionen

Der erste Bereich im Dialog **Agent Maintenance** gibt die Sondenkennung an. Die aktuellen Hardware- und Firmware-Stufen werden in den Feldern **Hardware Rev** und **Firmware Rev** angezeigt.

Firmware herunterladen

Zur Vereinfachung der Sondenadministration werden Firmware-Dateien im allgemeinen auf einem TFTP-Server gespeichert, auf den die Sonden im Netzwerk zugreifen können. Neue Versionen der Firmware können einfach und schnell von diesem Server auf die Sonde heruntergeladen werden. Das Herunterladen der SmartAgent-(ECAM)-Firmware wird über den Dialog **Agent Maintenance** eingeleitet. Weitere Informationen finden Sie in „RMON2-(ECAM)-SmartAgent-Firmware verwalten“ auf Seite 44.

Das Feld **Status** im Dialog **Agent Maintenance** zeigt den Erfolg des letzten Herunterladens durch Nways Remote Monitor an.

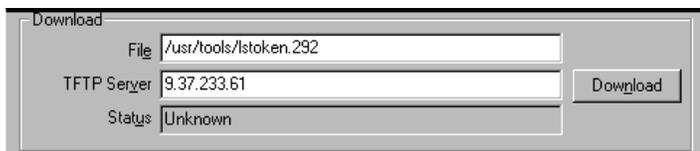


Abbildung 8. Firmware herunterladen

1. Bevor Sie neue Firmware herunterladen können, muß ein TFTP-Server aktiv sein. Wählen Sie die Programmgruppe **IBM Nways ReMon** im Menü **Start** und anschließend **TFTP** aus, um den mit Nways Remote Monitor mitgelieferten TFTP-Server zu starten. Der TFTP-Server wird gestartet, wenn die Workstation bootet, auf der Nways Remote Monitor installiert ist.
2. Geben Sie im Feld **File** im Bereich **Download** den Dateinamen der Agenten-Firmware ein. Nways Remote Monitor verwendet das Installationsverzeichnis als Speicherplatz für diese Datei. Sie müssen im Feld **File** keine Verzeichnisposition angeben.
3. Geben Sie im Feld **TFTP Server** die IP-Adresse des gewünschten TFTP-Servers ein.
4. Klicken Sie **Download** an, um die neue Firmware-Version auf die Sonde herunterzuladen. Die Sonde wird automatisch mit einem Kaltstart zurückgesetzt. In dieser Zeit besteht keine Verbindung zur Sonde, und Sie kehren automatisch zum Dialog **Device Configuration** zurück. Wenn die Sonde erneut gestartet wurde, kehren Sie zum Dialog **Agent Maintenance** zurück, und prüfen Sie, ob das Feld **Status** auf den Wert **Success** gesetzt ist. Wenn das Feld **Status** den Wert **Failure** anzeigt, prüfen Sie, ob der TFTP-Server aktiv und korrekt konfiguriert ist, und wiederholen Sie Schritt 1 bis 3.

Datum/Zeit und Echointervall

Datum-/Zeiteinstellungen

Bei Sonden mit einem Taktgeber können Sie das Datum und die Uhrzeit der Sonde über den Dialog **Agent Maintenance** einstellen.

Bei Sonden ohne Taktgeber können Sie weder Datum noch Uhrzeit eingeben. In diesem Fall wird im Feld **Date/Time** die Nachricht **Unavailable** angezeigt.

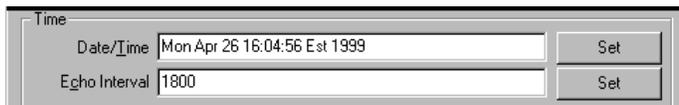


Abbildung 9. Datum/Zeit und Echointervall

1. Geben Sie im Feld **Date/Time** das Datum und die Uhrzeit in folgendem Format ein:

Tag	Erste drei Buchstaben des (englischen) Wochentags: Mon, Tue, Wed, Thu, Fri, Sat, Sun.
Monat	Erste drei Buchstaben des (englischen) Monats: Jan, Feb, Mar, Apr usw.
Datum	Zweistelliges Datum: 01, 02, 03 usw.
Zeit	Stunden:Minuten:Sekunden.
Zeitzone	BST, EST, GMT oder andere.
Jahr	Vierstellige Jahreszahl: 1996, 2000 u. ä.

2. Klicken Sie **Set** rechts neben dem Feld **Date/Time** an, um das neue Datum und die neue Uhrzeit auf die Sonde anzuwenden.

Echointervall

Sonden können so eingestellt sein, daß sie in regelmäßigen Abständen eine PING-Nachricht an den Standard-Gateway senden (siehe „Standard-Gateway“ auf Seite 29). Wenn Ihr Router ein kürzeres oder längeres Intervall zwischen den einzelnen PING-Nachrichten benötigt, um die Sonde in seinen Leitwegtabellen zu führen, müssen Sie das Echointervall ändern.

1. Geben Sie im Feld **Echo Interval** das PING-Intervall in Sekunden ein. Die Standardeinstellung ist 1800 Sekunden.
2. Klicken Sie **Set** rechts neben dem Feld **Echo Interval** an, um das neue Intervall auf die Sonde anzuwenden.

IP-Adresse, Teilnetzmaske und Standard-Gateway

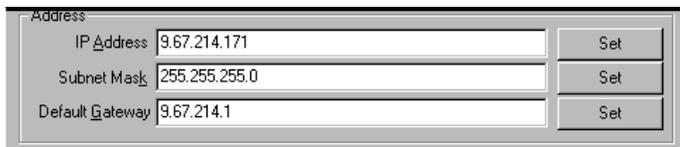
IP-Adresse und Teilnetzmaske

Bei Einheiten mit mehreren Schnittstellen können Sie für jede physische Schnittstelle eine IP-Adresse und eine Teilnetzmaske definieren. Die Schnittstelle wird im Dialog **Device Configuration** ausgewählt (siehe „Dialog "Device Configuration" öffnen“ auf Seite 21).

Wenn Sie eine virtuelle Schnittstelle oder eine Schnittstelle ausgewählt haben, für die keine IP-Adresse oder Teilnetzmaske definiert werden kann, bleiben diese Felder leer und können nicht editiert werden. Durch das Definieren von IP-Adressen für die unterschiedlichen Schnittstellen erhalten Sie größere Flexibilität für die Kommunikation mit einer Sonde. Wenn eine Schnittstelle nicht verfügbar ist, kann dennoch eine andere Schnittstelle verfügbar sein. Wenn Sie nicht sicher sind, welche IP-Adressen der Sonde zugeordnet sind, wenden Sie sich an Ihren Netzwerkadministrator.

Wenn mindestens zwei Schnittstellen auf einer Sonde dasselbe Teilnetzwerk überwachen, muß jede Schnittstelle mit einer anderen IP-Adresse konfiguriert sein.

Die Teilnetzmaske ist ein Filtersystem für IP-Adressen. Sie definiert den ersten Teil der IP-Adresse, der zur Bezeichnung des Netzwerks verwendet wird. Der Rest der Adresse stellt Host-Informationen dar. Einheiten und Router verwenden die Maske zur Bezeichnung des Teilnetzwerks, in dem sich eine Sonde befindet.



Address	
IP Address	9.67.214.171
Subnet Mask	255.255.255.0
Default Gateway	9.67.214.1

Abbildung 10. IP-Adresse, Teilnetzmaske und Standard-Gateway

1. Gehen Sie wie folgt vor, um die IP-Adresse zu definieren:
 - a. Geben Sie im Feld **IP Address** die IP-Adresse für die Sonde oder für die ausgewählte Schnittstelle der Sonde ein.
IP-Adressen haben das Format $n.n.n.n$. Dabei steht n für eine Dezimalzahl zwischen 0 und 255. Eine IP-Adresse sieht zum Beispiel folgendermaßen aus:
91.1.1.9.
 - b. Wenn Sie eine neue IP-Adresse anwenden wollen, klicken Sie **Set** rechts neben dem Feld **IP Address** an.
2. Gehen Sie wie folgt vor, um die Teilnetzmaske zu definieren:
 - a. Geben Sie im Feld **Subnet Mask** eine geeignete Teilnetzmaske für die Klasse von IP-Adressen ein. Weitere Informationen erhalten Sie von Ihrem Systemadministrator.
 - b. Klicken Sie **Set** rechts neben dem Feld **Subnet Mask** an, um die neue Teilnetzmaske anzuwenden.

Standard-Gateway

Der Standard-Gateway ist die IP-Adresse einer Einheit, normalerweise eines Routers oder Gateways, zu der die Sonde alle Pakete überträgt, die nicht für ihr eigenes Teilnetzwerk bestimmt sind.

Sie können auch über die Option **Static Routes** bis zu 16 Leitwege zu anderen Teilnetzen definieren (siehe „Statische Leitwege definieren“ auf Seite 36).

1. Geben Sie im Feld **Default Gateway** die IP-Adresse für den Router oder den Gateway ein.
2. Klicken Sie **Set** rechts neben dem Feld **Default Gateway** an, um die neue Einstellung anzuwenden.

Sonden zurücksetzen

Sie können Sonden mit einem Warm- oder Kaltstart zurücksetzen. Bei beiden wird die Sonde neu initialisiert. Sie wirken sich jedoch unterschiedlich auf die Sonde aus. Diese Unterschiede werden für die RMON- und RMON2-Variablen in Tabelle 3 auf Seite 30 und Tabelle 4 auf Seite 31 zusammengefasst. Informationen werden beibehalten, gesammelte statistische Daten, die im Arbeitsspeicher der Sonde gespeichert sind, gehen jedoch verloren.

Mit Warmstart zurücksetzen

Wenn Sie eine Sonde mit einem Warmstart zurücksetzen, werden alle grundlegenden und erweiterten Konfigurationsdaten beibehalten, gesammelte statistische Daten, die im Arbeitsspeicher der Sonde gespeichert sind, gehen jedoch verloren.

Mit Kaltstart zurücksetzen

Wenn Sie eine Sonde mit einem Kaltstart zurücksetzen, gehen alle Netzwerkmanagementinformationen verloren. Hiervon ausgenommen sind lediglich die grundlegenden Konfigurationsdaten wie IP-Adresse, Teilnetzmaske und Standard-Gateway, die im EEPROM gespeichert sind.

Mit einer Rücksetzung mit Kaltstart können Sie die Konfigurationsdaten schnell löschen und die Einheit auf die Werkseinstellungen zurücksetzen. Eine derartige Rücksetzung führt zum Verlust der benutzerdefinierten Protokollinformationen.

Wenn Sie eine Sonde mit Warm- oder Kaltstart zurücksetzen wollen, klicken Sie **Warm Reset...** bzw. **Cold Reset...** in der Funktionsleiste unten im Dialog **Agent Maintenance** an. Sie kehren automatisch zurück zum Dialog **Device Configuration**. Während der Rücksetzung ist die Sonde vorübergehend nicht verfügbar.

Bei beiden Arten der Rücksetzung wird die Sonde neu initialisiert. Sie wirken sich jedoch unterschiedlich auf die Sonde aus. Diese Unterschiede werden für die RMON- und RMON2-Variablen in Tabelle 3 auf Seite 30 und Tabelle 4 auf Seite 31 zusammengefasst.

Tabelle 3 (Seite 1 von 2). Beibehaltene und verlorene RMON-Daten

Datentyp	Rück- setzen mit Warmstart	Rücksetzen mit Kaltstart
Sondenkonfigurationsdaten (IP-Adresse usw.)	B	B
TFTP-Server-Adresse	B	B
Dateiname für Herunterladen	B	B
Datum und Zeit	B	B
Konfigurationsdaten für seriellen Anschluß	B	B
Filtertabelle	B	V
Kanaltabelle	B	V
Steuertabelle für Capture-Puffer	B	V
History-Steuertabelle	B	V ^a
Host-Steuertabelle	B	V ^a
Matrixsteuertabelle	B	V ^a
N oberste Einträge der Host-Tabelle	V	V
Alarmtabelle	B	V
Ereignistabelle	B	V ^a
Tabelleneinträge für Benutzergemeinschaftszugriff	B	V ^a
Client-Tabelleneinträge	B	V ^a
Tabelle für seriellen Anschluß	B	V
Alarmnachrichtzieltabelle	B	V
Erfasste Pakete	V	V
Historische Statistik	V	V
Aktuelle Statistik	V ^c	V ^a
Host-Statistiktabellen	V	V
Matrixstatistiktabellen	V	V
N oberste Einträge der Host-Statistiktabellen	V	V
Protokolltabellen	V	V
Tabelle der Stationen im Ring ^d	V	V
Quellenleitwegstatistik ^d	V ^c	V ^a
Steuertabelle der Stationen im Ring ^d	B	V ^a

Tabelle 3 (Seite 2 von 2). Beibehaltene und verlorene RMON-Daten

Datentyp	Rück- setzen mit Warmstart	Rücksetzen mit Kaltstart
Anmerkung:		
	B Daten beibehalten	
	V Daten verloren	
	a Rückkehr zu Standardwerten	
	b Benutzerdefinierte Protokolle beibehalten	
	c Steuerinformationen beibehalten	
	d Nur Token-Ring	

Tabelle 4. Beibehaltene und verlorene RMON2-Daten

Datentyp	Rück- setzen mit Warmstart	Rücksetzen mit Kaltstart
Steuertabellen für Adreßzuordnung	B	√a
Adreßzuordnungstabelle	V	V
Steuertabellen für Protokollverteilung	B	√a
Protokollverteilungstabellen	V	V
Host-Steuertabellen in höheren Schichten	B	V
Host-Tabellen in der Vermittlungsschicht	V	V
Host-Tabellen in der Anwendungsschicht	V	V
Matrixsteuertabellen in höheren Schichten	B	V
Matrixtabellen in der Vermittlungsschicht	V	V
N oberste Einträge der Matrixsteuertabellen in der Vermittlungsschicht	V	V
N oberste Einträge der Matrixtabellen in der Vermittlungsschicht	V	V
N oberste Einträge der Matrixsteuertabellen in der Anwendungsschicht	V	V
N oberste Einträge der Matrixtabellen in der Anwendungsschicht	V	V
Benutzerprotokollsteuerung und -objekte	B	V
Benutzerprotokolltabellen	V	V
Protokollverzeichnis	√a,b	√a

Zugriffssteuerungstabellen

Über das Fenster **Access Control** können Sie Namen für den Benutzergemeinschaftszugriff mit den geeigneten Sicherheitsstufen definieren und diese Namen dann bestimmten Endbenutzer-Workstations zuordnen. Dadurch können Sie den Zugriff auf die MIB einer Sonde auf die ausgewählte Gruppe oder Benutzergemeinschaft von Managementstationen einschränken. Durch die Verwendung mehrerer Benutzergemeinschaften kann die Sonde unterschiedliche Ebenen für unterschiedliche Managementstationen bieten. Bei jedem Versuch eines Benutzers, eine kritische Funktion mit Nways Remote Monitor auszuführen, muß der Benutzer zuerst einen Benutzergemeinschaftsnamen der entsprechenden Sicherheitsstufe angeben.

Dialog "Access Control" öffnen

Klicken Sie **ACL...** im Dialog **Agent Maintenance** (Abb. 7) an, um den Dialog **Access Control** zu öffnen.

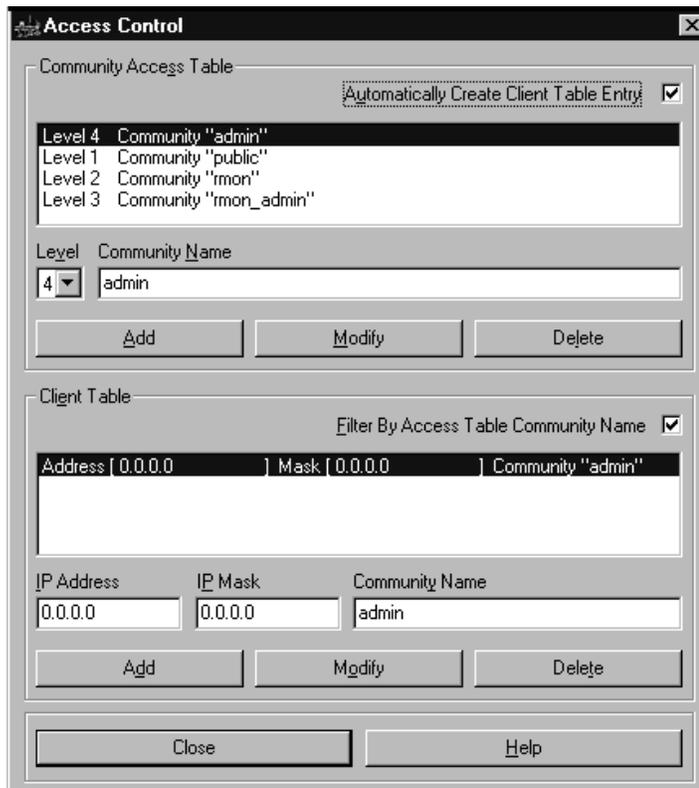


Abbildung 11. Dialog "Access Control"

Alle Änderungen in den Tabellen für Benutzergemeinschaftszugriff und den Client-Tabellen werden sofort wirksam.

Benutzergemeinschafts-Zugriffsnamen

Gehen Sie wie folgt vor, um einen neuen Benutzergemeinschafts-Zugriffsnamen mit einer bestimmten Sicherheitsstufe zu definieren:

Wenn Nways Remote Monitor automatisch einen Eintrag in der Client-Tabelle für diesen neuen Eintrag erzeugen soll, aktivieren Sie die Option **Automatically Create Client Table Entry** oben rechts im Dialog. Sie können den Eintrag auch jederzeit manuell zur Client-Tabelle hinzufügen (siehe „Sicherheitsstufen für bestimmte Endbenutzer-Workstations“ auf Seite 34).

1. Wählen Sie die Sicherheitsstufe aus, indem Sie **Level** anklicken und die gewünschte Stufe aus der verdeckten Liste auswählen (siehe Tabelle 5).

Tabelle 5. Sicherheitsstufen

Stufe	Beschreibung
1	Lesezugriff auf MIB-II-Objekte (SNMP MIB)
2	Lesezugriff auf MIB-II-, RMON-MIB- und Konfigurations-MIB-Objekte, mit Ausnahme der Zugriffssteuerungsgruppe und der Capture-Puffertabelle
3	Lesezugriff auf MIB-II-, RMON-MIB- und Konfigurations-MIB-Objekte, mit Ausnahme der Zugriffssteuerungsgruppe Schreibzugriff auf RMON-MIB- und Konfigurations-MIB-Objekte, mit Ausnahme der Gruppen für Sondenadministration, Schnittstellen und Zugriffssteuerung
4	Lese- und Schreibzugriff auf alle MIB-II-, RMON-MIB- und Konfigurations-MIB-Objekte

- a. Geben Sie den neuen Wert in das Feld **Community Name** ein, um den neuen Benutzergemeinschaftsnamen zu definieren. Der Name muß eindeutig sein.
 - b. Klicken Sie **Add** an, um diesen neuen Eintrag zu erstellen.
2. Gehen Sie wie folgt vor, um die Einstellungen für einen vorhandenen Benutzergemeinschafts-Zugriffseintrag zu ändern:
 - a. Klicken Sie einen vorhandenen Eintrag in der Liste **Community Access Table** an. Die aktuellen Einstellungen werden in den Feldern **Level** und **Community Name** angezeigt.
 - b. Ändern Sie die Sicherheitsstufe wie oben beschrieben, und klicken Sie anschließend **Modify** an, damit die Änderung wirksam wird.
 - c. Ändern Sie den Benutzergemeinschaftsnamen wie oben beschrieben, und klicken Sie anschließend **Modify** an, damit die Änderung wirksam wird.
 3. Wenn Sie einen vorhandenen Eintrag löschen wollen, wählen Sie einfach den Eintrag in der Tabelle aus, und klicken Sie **Delete** an.

Sicherheitsstufen für bestimmte Endbenutzer-Workstations

1. Standardmäßig werden alle Einträge in der Client-Tabelle angezeigt. Wenn Sie den Inhalt der Client-Tabelle filtern wollen, so daß nur die Einträge der Client-Tabelle für den ausgewählten Eintrag in der Benutzergemeinschafts-Zugriffstabelle angezeigt werden, klicken Sie den Knopf **Filter by Community Access Table** über der Client-Tabelle an.
2. Gehen Sie wie folgt vor, um einen neuen Eintrag zur Client-Tabelle hinzuzufügen:
 - a. Geben Sie die IP-Adresse und die Teilnetzmaske der Workstation in den Feldern **IP Address** und **IP Mask** ein.
 - b. Geben Sie einen eindeutigen Benutzergemeinschaftsnamen im Feld **Community Name** ein.
 - c. Klicken Sie **Add** an, um diesen neuen Eintrag zu erstellen.
3. Wenn Sie einen Eintrag der Client-Tabelle ändern wollen, ändern Sie die Werte für die IP-Adresse und die Teilnetzmaske, und klicken Sie **Modify** an.
4. Wenn Sie einen Eintrag der Client-Tabelle löschen wollen, wählen Sie einfach den Eintrag aus, und klicken Sie **Delete** an.

Alarmnachricht-Benutzergemeinschaften

Wenn ein Alarm auf einer Sonde ausgelöst wird, kann die Sonde weitere Hosts im Netzwerk mit einem SNMP-Alarmnachrichtpaket über dieses Ereignis informieren. Über dieses Ereignis werden nicht alle Workstations in Ihrem Netzwerk informiert, sondern nur die Workstations, die zuvor die Information angefordert haben. Dies wird dadurch gesteuert, daß jedem Alarm auf einer Sonde eine Alarmnachricht-Benutzergemeinschaft und jeder Alarmnachricht-Benutzergemeinschaft eine Liste der zu informierenden Workstations zugeordnet wird.

Es gibt zwei Methoden zum Zuordnen von Alarmnachricht-Benutzergemeinschaften:

- Nways Remote Monitor ordnet jedem neu erstellten Alarm automatisch traps als Standard-Benutzergemeinschaftsnamen zu. Nways Remote Monitor prüft, ob diese Benutzergemeinschaft auf einer der Sonden vorhanden ist, zu denen es eine Verbindung herzustellen versucht, und fügt die Informationen für die Workstation, auf der es ausgeführt wird, zu den Alarmnachricht-Benutzergemeinschaften hinzu.
- Sie können einen anderen Benutzergemeinschaftsnamen im Bereich **Trap Configuration** des Dialogs **Alarm Creation** eingeben und die Namen der Alarmnachricht-Benutzergemeinschaften auf der Sonde editieren. Im Dialog **Trap Control** können Sie genau steuern, welche Workstations in Ihrem Netzwerk Alarmereignisse von der fraglichen Sonde erhalten.

Die Zuordnung von Alarmnachricht-Benutzergemeinschaften zu einem Alarm wird in „Alarmanzeige (Alarms View)“ auf Seite 94 beschrieben.

Dialog "Trap Control" öffnen

Klicken Sie im Dialog **Agent Maintenance** (Abb. 7) die Option **Trap...** unten im Fenster an, um den Dialog **Trap Control** zu öffnen.

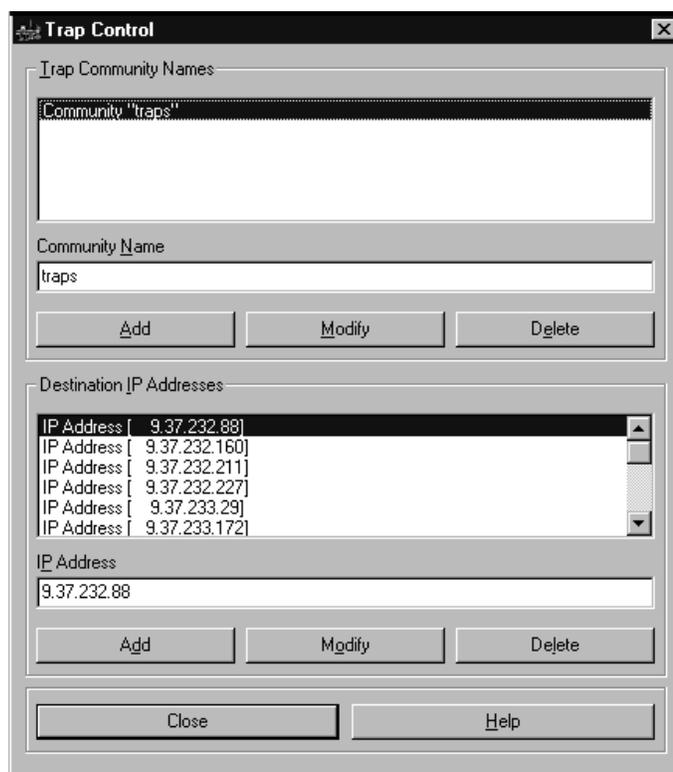


Abbildung 12. Dialog "Trap Control"

Alarmnachricht-Benutzergemeinschaftsnamen

1. Wenn Sie eine Alarmnachricht-Benutzergemeinschaft erstellen wollen, geben Sie einen eindeutigen Namen im Feld **Community Name** unter der Liste **Trap Community Names** ein, und klicken Sie **Add** an.
2. Wenn Sie einen Benutzergemeinschaftsnamen ändern wollen, klicken Sie den gewünschten Eintrag an. Dieser wird dann im Feld **Community Name** angezeigt. Editieren Sie dieses Feld, und klicken Sie **Modify** an, damit die Änderung wirksam wird.
3. Wenn Sie eine Benutzergemeinschaft löschen wollen, klicken Sie den Eintrag und anschließend **Delete** an.

IP-Zieladressen

Gehen Sie wie folgt vor, um die Liste der IP-Adressen der Workstations zu ändern, die einer Benutzergemeinschaft zugeordnet sind:

1. Wählen Sie eine Benutzergemeinschaft durch Anklicken in der Liste **Trap Community Names** aus. Eine Liste vorhandener IP-Adressen für diese Benutzergemeinschaft wird in der Liste **Destination IP Addresses** angezeigt.
2. Wenn Sie eine Ziel-Workstation hinzufügen wollen, geben Sie die IP-Adresse der Workstation im Feld **IP Address** ein, und klicken Sie **Add** an.
3. Wenn Sie eine IP-Adresse für eine Ziel-Workstation ändern wollen, klicken Sie den gewünschten Eintrag an, und ändern Sie den Wert im Feld **IP Address**. Klicken Sie anschließend **Modify** an.
4. Wenn Sie eine Ziel-Workstation von einer Benutzergemeinschaft löschen wollen, klicken Sie die IP-Adresse der Workstation und anschließend **Delete** an.

Statische Leitwege definieren

Statische Leitwege werden verwendet, um bestimmte Leitwege einzurichten, die die Sonde zur Kommunikation mit anderen Netzwerken verwenden soll. Dabei wird der Standard-Gateway umgangen (siehe „Standard-Gateway“ auf Seite 29). Auf jeder Sonde können bis zu 16 statische Leitwege definiert werden.

1. Klicken Sie **Static Routes...** im Dialog **Agent Maintenance** (Abb. 7 auf Seite 25) an, um den Dialog **Static Routing Table** zu öffnen.

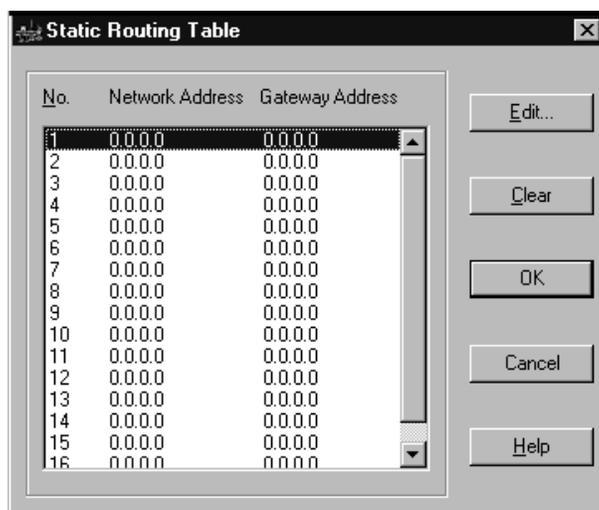


Abbildung 13. Dialog "Static Routing Table"

2. Wenn Sie den Inhalt des Dialogs **Static Routing Table** zurücksetzen wollen, klicken Sie **Clear** an. Alle Werte werden auf 0.0.0.0 gesetzt.
3. Klicken Sie einen statischen Leitweg an, um ihn auszuwählen.

4. Klicken Sie **Edit** an, um den Dialog **Edit Routing Entry** zu öffnen.

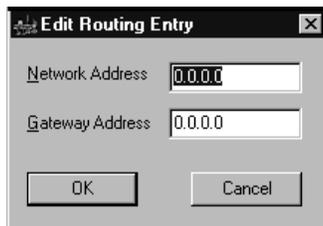


Abbildung 14. Dialog "Edit Routing Entry"

- Die Netzwerkadresse ist die IP-Adresse des Zielnetzwerks, z. B. 91.0.0.0.
 - Die Gateway-Adresse ist die Adresse des Routers, zu dem die Pakete gesendet werden sollen, z. B. 89.0.0.9. Dieser Router muß sich im selben Netzwerk befinden wie die Sonde.
5. Klicken Sie ein Feld an, und editieren Sie die Werte nach Bedarf.
 6. Klicken Sie **OK** an, um die neue Einstellung zu speichern und zum Dialog **Static Routing Table** zurückzukehren.
 7. Wiederholen Sie Schritt 2 bis 6, bis Sie fertig sind.
 8. Klicken Sie **OK** an, um zum Dialog **Agent Maintenance** zurückzukehren.

PACMIB aktivieren und inaktivieren

PACMIB (Port Address Correlation MIB) ordnet den Hosts Anschlüsse zu und sammelt statistische Anschlußdaten für in Ihrem Netzwerk unterstützte Einheiten. Mit PACMIB können Sie unter Verwendung von **Host View** von Rmonview statistische Daten für Anschlüsse und Einschubmodule auf einem Host sammeln.

1. Klicken Sie den Knopf **PACMIB** im Dialog **Agent Maintenance** (Abb. 7) an, um den Dialog **PACMIB Support** zu öffnen.

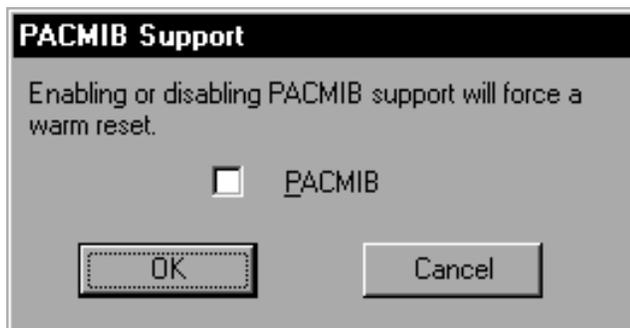


Abbildung 15. PACMIB aktivieren und inaktivieren

2. Wenn PACMIB auf der aktuellen Einheit aktiviert ist, ist das Markierungsfeld **PACMIB** ausgewählt. Wenn Sie PACMIB inaktivieren wollen, klicken Sie das Markierungsfeld **PACMIB** an, um die Auswahl zurückzunehmen. Wenn PACMIB auf der aktuellen Einheit inaktiviert ist, ist das Markierungsfeld **PACMIB** nicht ausgewählt. Wenn Sie PACMIB aktivieren wollen, wählen das Markierungsfeld **PACMIB** aus.
3. Klicken Sie **OK** an, um Ihre Änderungen zu aktivieren und die Einheit zurückzusetzen. Sie kehren zum Dialog **Device Configuration** zurück. Während der Rücksetzung ist die Einheit nicht verfügbar.
4. Wenn die Einheit wieder verfügbar ist, können Sie die Host-Anzeige verwenden, um statistische Daten für Anschlüsse und Einschubmodule für unterstützte Einheiten zu sammeln.

RMON2-Modus definieren

Sie können RMON2-kompatible Sonden konfigurieren, um die optimalen Tabellengrößen für unterschiedliche Anwendungen zu nutzen. Sie können RMON2 auch inaktivieren, so daß die Sonde SmartAgent-Software wie z. B. RMON2 (ECAM) SmartAgent ausführen kann. ECAM ist ein Vorläufer des RMON2-Standards.

Gehen Sie wie folgt vor, um den RMON2-Modus zu definieren:

1. Klicken Sie **RMON2 Config** im Dialog **Device Configuration** an, um den Dialog **RMON2 Config** zu öffnen (siehe Abb. 16).

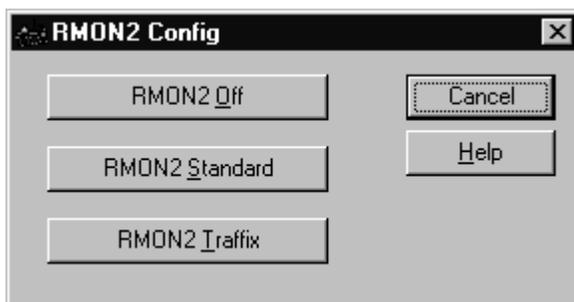


Abbildung 16. Dialog "RMON2 Config"

2. Wählen Sie eine der folgenden Einstellungen aus:

- RMON2 Off

Klicken Sie **RMON2 Off** an, um RMON2 zu inaktivieren. Sie sollten diese Einstellung für Anwendungen auswählen, die SmartAgent-Software verwenden.

- RMON2 Standard

Sie sollten diesen Modus auswählen, um die Fehlerbehebungsfunktionalität von RMON2 zu optimieren.

- RMON2 Traffic

Bei diesem Modus wird den Verkehrsüberwachungsfunktionen mehr Speicher zugewiesen, d. h. Traffic Monitor wird optimiert.

Anmerkung: IBM Nways Traffic Monitor wird derzeit nicht für Windows NT bereitgestellt.

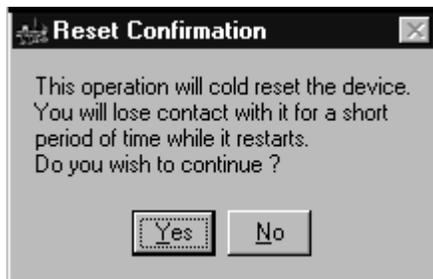


Abbildung 17. Dialog "Reset Confirmation"

3. Wenn Sie **Yes** anklicken, führt die Sonde eine Rücksetzung mit Kaltstart aus, und Ihre Änderungen werden angewendet.

Virtuelle Schnittstellen konfigurieren

Die physischen Schnittstellen einer Sonde können bestimmte Datengruppen für die Messung der Netzwerküberprüfungsparameter sammeln, z. B. Gesamtanzahl der Pakete, Gesamtanzahl der Fehler usw. Mit Capture können physische Schnittstellen auch bestimmte Pakettypen aus dem Netzwerk zur Untersuchung des Inhalts dieser Pakete filtern.

Mit virtuellen Schnittstellen können Sie jedoch diese Filter- und Meßfunktionen kombinieren. Virtuelle Schnittstellen sind Kopien einer physischen Schnittstelle einer Sonde und werden zum Filtern der Daten auf der physischen Schnittstelle gemäß Ihren Filterkriterien verwendet. Sie könnten z. B. eine virtuelle Schnittstelle konfigurieren, um nur statistische Daten zum WWW-Datenverkehr zu filtern. Statistische Daten, die von einer virtuellen Schnittstelle gesammelt werden, werden in RMON-Standardtabellen auf der Sonde gespeichert.

Virtuelle Schnittstellen erstellen

Wenn Sie eine virtuelle Schnittstelle erstellen wollen, müssen Sie die Sonde und die physische Schnittstelle, zu der sie gehören soll, den verwendeten Filter sowie die RMON-Tabellen angeben, in denen die gefilterten Daten gespeichert werden sollen.

1. Wählen Sie im Dialog **Device Configuration** die Sonde, für die Sie die virtuelle Schnittstelle erstellen wollen, durch Anklicken in der Liste **Select Probe** aus.
2. Wählen Sie die physische Schnittstelle aus, der die neue virtuelle Schnittstelle zugeordnet werden soll. Sie können diese Auswahl später im Dialog **Create Virtual Interfaces** ändern.

3. Klicken Sie **Add...** an, um den Dialog **Create Virtual Interfaces** zu öffnen.

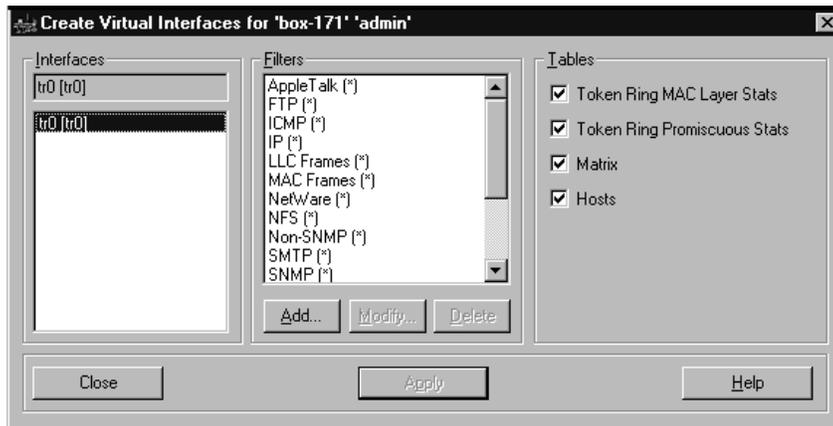


Abbildung 18. Dialog "Create Virtual Interfaces"

Dieser Dialog ist in drei Bereiche unterteilt::

Interfaces Wählen Sie die physische Schnittstelle aus, der die neue virtuelle Schnittstelle zugeordnet werden soll.

Filters Fügen Sie einen Filter gemäß dem Datenträgertyp der ausgewählten physischen Schnittstelle hinzu, oder wählen Sie einen vordefinierten Filter aus.

Tables Geben Sie an, welche RMON-Tabellen der virtuellen Schnittstelle zugeordnet werden sollen.

RMON2-Tabellen können mit dem Knopf **RMON2 Tables** im Dialog **Device Configuration** ausgewählt werden, sobald die Schnittstelle erstellt wurde.

4. Wählen Sie eine physische Schnittstelle für die Sonde durch Anklicken in der Liste **Interfaces** aus. Die virtuelle Schnittstelle wird der ausgewählten physischen Schnittstelle zugeordnet. Alle Änderungen, die Sie an der physischen Schnittstelle vornehmen, z. B. am Namen, werden in der virtuellen Schnittstelle repliziert.
5. Wenn Sie einen vordefinierten Filter auswählen wollen, klicken Sie einen vorhandenen Eintrag in der Liste an. Die Liste der vordefinierten Filter ändert sich in Abhängigkeit vom Datenträgertyp der ausgewählten physischen Schnittstelle.
6. Wenn Sie Ihre eigenen Filter zur Verwendung mit dieser oder einer anderen Schnittstelle erstellen wollen, klicken Sie **Add...** an, um den Dialog **Channel** zu öffnen.

Tabelle 6. Vordefinierte Kanäle (Filter)

Kanal	Beschreibung	Datenträgertyp der physischen Schnittstelle		
		Ethernet	FDDI	Token-Ring
AppleTalk	Übergibt nur AppleTalk-Pakete	■	■	■
FTP	Übergibt nur FTP-Pakete	■	■	■
ICMP	Übergibt nur ICMP-Pakete	■	■	■
IP	Übergibt nur IP-Pakete	■	■	■
LLC Frames	Übergibt nur LLC-Pakete			■
MAC Frames	Übergibt nur MAC-Pakete			■
NetWare	Übergibt nur NetWare-Pakete	■	■	■
NFS	Übergibt nur NFS-Pakete	■	■	■
Non-SNMP	Übergibt alle Pakete mit Ausnahme von SNMP	■	■	■
SMTP	Übergibt nur SMTP-Pakete	■	■	■
SNMP	Übergibt nur SNMP-Pakete	■	■	■
TCP	Übergibt alle TCP-Pakete	■	■	■
Non-SNMP	Übergibt alle Pakete mit Ausnahme von SNMP	■	■	■
SMTP	Übergibt nur SMTP-Pakete	■	■	■
SNMP	Übergibt nur SNMP-Pakete	■	■	■
Telnet	Übergibt nur Telnet-Pakete	■	■	■
UDP	Übergibt alle UDP-Pakete	■	■	■
WWW	Übergibt nur WWW-Pakete	■	■	■
XNS	Übergibt nur XNS-Pakete	■		
X-Windows	Übergibt nur X-Windows-Pakete	■	■	■

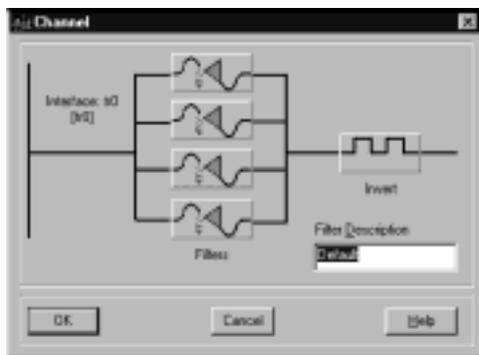


Abbildung 19. Dialog "Channel"

- a. Sie können bis zu vier Unterfilter aufnehmen. Zum Definieren eines Filters klicken Sie einen der Filterknöpfe  an. Der Dialog **Edit Filter** wird geöffnet.
Das Definieren eines Filters wird in „Filtereditor verwenden“ auf Seite 112 beschrieben. Klicken Sie **OK** an, um zum Dialog **Channel** zurückzukehren.
- b. Mit dem Knopf **Invert** können Sie die Logik des Filters umkehren. Wenn Sie z. B. derzeit alle TCP-Pakete erfassen, klicken Sie einfach diesen Knopf an, um alle Pakete mit Ausnahme von TCP-Paketen zu erfassen.

Tabelle 7. Knopf "Invert"

Stufe	Beschreibung
	Sammelt die angegebenen Pakete.
	Sammelt alles mit Ausnahme der angegebenen Pakete.

- c. Klicken Sie **OK** an, um diesen Filter zu erstellen. Sie kehren zurück zum Dialog **Create Virtual Interfaces**. Der neue Filter ist automatisch ausgewählt.
7. Wählen Sie die Tabellen aus, die Sie erstellen wollen, indem Sie die Markierungsfelder für diese Tabellen anklicken. Sie können Tabellen auch später im Dialog **RMON Tables** auswählen (siehe „RMON- und RMON2-Tabellen verwalten“ auf Seite 43).
8. Wenn Sie die virtuelle Schnittstelle erstellen wollen, klicken Sie **Apply** an. Ein Nachrichtenfenster wird geöffnet, in dem bestätigt wird, daß die virtuelle Schnittstelle erstellt wurde.
9. Wiederholen Sie Schritt 3 bis 7, um die erforderliche Anzahl von Schnittstellen zu erstellen. Wenn Sie zum Dialog **Device Configuration** zurückkehren, wird die neue virtuelle Schnittstelle in der Liste **Select Interface** angezeigt. Die virtuelle Schnittstelle wird als Name der zugehörigen physischen Schnittstelle gefolgt von der Filterbeschreibung in Klammern angezeigt. Beispiel: ie0 (All IP Packets).

Virtuelle Schnittstellen löschen

Das Löschen von virtuellen Schnittstellen erfolgt über den Dialog **Device Configuration**.

1. Wählen Sie in der Liste **Select Probe** die Sonde, von der die virtuelle Schnittstelle gelöscht werden soll, durch Anklicken aus.
2. Wählen Sie in der Liste **Select Interface** die Schnittstelle, von der die virtuelle Schnittstelle gelöscht werden soll, durch Anklicken aus.
3. Klicken Sie **Delete** an.
4. Wenn Sie eine virtuelle Schnittstelle ausgewählt haben, der RMON-Tabellen zugeordnet sind, werden Sie aufgefordert, den Löschvorgang zu bestätigen. Klicken Sie **Yes** an, um fortzufahren, oder **No**, um die virtuelle Schnittstelle unverändert zu lassen.

RMON- und RMON2-Tabellen verwalten

Sie können die RMON-Tabellen für eine physische oder virtuelle Schnittstelle einer Sonde im Dialog **Device Configuration** anzeigen und zurücksetzen.

1. Wählen Sie eine Sonde durch Anklicken in der Liste **Select Probe** aus.
2. Klicken Sie **RMON Tables...** an, um den Dialog **RMON Tables** zu öffnen, *beziehungsweise* klicken Sie **RMON2 Tables...** an, um den Dialog **RMON2 Table Management** zu öffnen.

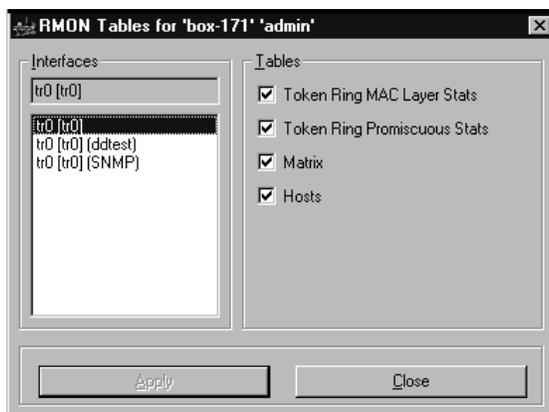


Abbildung 20. Dialog "RMON Tables"

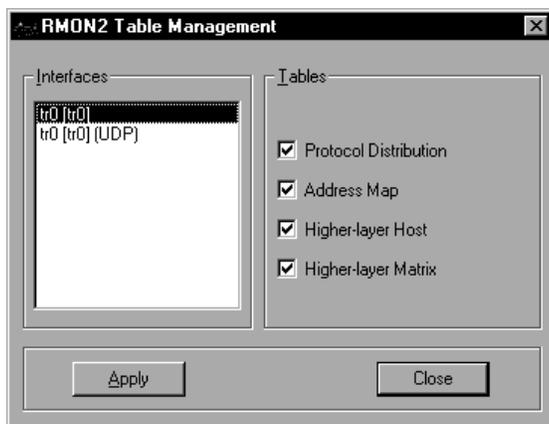


Abbildung 21. Dialog "RMON2 Table Management"

3. Wählen Sie die Schnittstelle, für die Sie die aktuellen RMON-Tabellen anzeigen wollen, durch Anklicken in der Liste **Interfaces** aus. Dies kann eine physische oder virtuelle Schnittstelle sein.
4. Wenn Sie aus einer aktiven Tabelle alle gesammelten statistischen Daten entfernen wollen, klicken Sie die entsprechenden Markierungsfelder an, um sie zu inaktivieren, und klicken Sie dann **Apply** an.
5. Wenn Sie statistische Daten für eine inaktive Tabelle sammeln wollen, klicken Sie die entsprechenden Markierungsfelder an, um sie zu aktivieren, und klicken Sie **Apply** an.
6. Klicken Sie **Close** an, um zum Dialog **Device Configuration** zurückzukehren.

Anmerkung: Wenn Sie **Close** auswählen, ohne zuerst **Apply** ausgewählt zu haben, werden die Änderungen nicht wirksam.

RMON2-(ECAM)-SmartAgent-Firmware verwalten

SmartAgent-Firmware kann jederzeit von einer Sonde geladen werden, um die Funktionalität zu bieten, und wieder von ihr entladen werden. Die Firmware kann je nach Datentyp, den Sie mit der Sonde sammeln wollen, nach Bedarf gestartet und gestoppt werden.

Sie können die SmartAgent-Firmware auch in der Autostart-Tabelle einer Sonde registrieren, so daß die Firmware beim Neustart von der Sonde geladen wird.

Wenn Sie eine RMON2-kompatible Sonde verwenden, bietet der RMON2-Standard Informationen für die meisten Anwendungen, so daß Sie die Firmware nicht herunterladen müssen. Zum Herunterladen der SmartAgent-Firmware müssen Sie RMON2 auf der Sonde inaktivieren. Weitere Informationen finden Sie in „RMON2-Modus definieren“ auf Seite 38.

Dialog "SmartAgent Maintenance" öffnen

Das Laden und Entladen der SmartAgent-Firmware erfolgt über den Dialog **SmartAgent Maintenance**. Klicken Sie **SmartAgents...** im Dialog **Device Configuration** an, um den Dialog **SmartAgent Maintenance** zu öffnen.



Abbildung 22. Dialog "SmartAgent Maintenance"

Ein Element der SmartAgent-Firmware kann die Grundlage für mehr als eine Anwendung sein. Wenn Sie eine Anwendung auswählen, wird die zugrundeliegende Firmware in die Sonde geladen, so daß *alle Anwendungen* für diese Firmware in Viewman und Rmonview verfügbar sind.

Anwendungen aktivieren

1. Bevor Sie SmartAgent-Firmware herunterladen können, muß ein TFTP-Server aktiv sein. Anweisungen zum Starten des mit Nways Remote Monitor mitgelieferten TFTP-Servers finden Sie in „Firmware herunterladen“ auf Seite 26.
2. Standardmäßig wird die Firmware im Installationsverzeichnis von Nways Remote Monitor gespeichert, und die Adresse des TFTP-Servers wird auf die Adresse Ihres PCs eingestellt. Ändern Sie gegebenenfalls die Adresse im Feld **Address** im Bereich **TFTP Server**.
3. Die Liste der verfügbaren Anwendungen wird als Anwendungsname gefolgt vom Namen der zugrundeliegenden Firmware angezeigt.

Dies sind Anwendungen, die über Viewman oder Rmonview ausgeführt werden können — sie stellen nicht die auf dem TFTP-Server gespeicherte Firmware dar.

Der Status einer Anwendung wird hinter dem Anwendungsnamen angezeigt. Wenn die Firmware für eine der aufgelisteten Anwendungen bereits auf die Sonde heruntergeladen ist, wird der Status [Loaded] gefolgt von der Versionsnummer und der Größe angezeigt.

Wie oft diese Firmware auf die Sonde geladen wurde, ohne entladen zu werden, wird unter **# References** angezeigt.

Wählen Sie eine Anwendung aus der Liste **Available SmartAgent Apps** aus.

Wenn die zugrundeliegende Firmware für diese Anwendung auf die Sonde geladen ist, sind alle Anwendungen, die auf derselben Firmware basieren, ebenfalls im Hauptfenster verfügbar.

4. Klicken Sie **Load** an. Die Sonde stellt eine Verbindung zum TFTP-Server her und lädt die ausgewählte Firmware, sofern diese verfügbar ist. Wenn dieser Vorgang erfolgreich ist, wird der Status der Anwendung in [Loaded] geändert.

Wenn die Sonde die Firmware nicht laden kann, kann dies folgende Ursachen haben:

- Der TFTP-Server ist nicht verfügbar, oder die Adresse des TFTP-Servers wurde falsch eingegeben.
- Die ausgewählte Firmware ist nicht auf dem angegebenen TFTP-Server gespeichert.
- Die Sonde ist nicht mehr verfügbar.
- RMON2 ist noch auf der Sonde aktiviert. Weitere Informationen finden Sie in „RMON2-Modus definieren“ auf Seite 38.

Prüfen Sie die einzelnen Angaben für den Server, und versuchen Sie es erneut. Wenn die Firmware immer noch nicht geladen werden kann, kehren Sie zum Dialog **Device Configuration** zurück, und wählen Sie die Sonde aus, um sicherzustellen, daß sie verfügbar ist.

Anwendungen inaktivieren

1. Wählen Sie die nicht mehr erforderliche Anwendung durch Anklicken in der Liste **Available SmartAgent Apps** aus. Sie müssen einen Eintrag mit dem Status [Loaded] auswählen.

Denken Sie daran, daß eine Reihe von Anwendungen dieselbe zugrundeliegende Firmware haben kann. Wenn Sie eine Anwendung inaktivieren, werden auch alle anderen Anwendungen inaktiviert, die auf derselben Firmware basieren.

2. Klicken Sie **Unload** an. Der Status der Anwendung wird in [Not Loaded] geändert.

Autostart-Tabelle

Wenn einige Anwendungen ständig erforderlich sind, können Sie die zugrundeliegende Firmware in der Autostart-Tabelle der Sonde registrieren. Die Autostart-Tabelle enthält die Namen der Firmware, die automatisch geladen werden soll, wenn ein Warmstart oder ein Neustart der Sonde durchgeführt wird.

1. Gehen Sie wie folgt vor, um die zugrundeliegende Firmware in der Autostart-Tabelle zu registrieren:
 - a. Klicken Sie eine Anwendung in der Liste **Available SmartAgent Apps** an.
 - b. Klicken Sie **AutoBoot** an. Die Firmware wird der Liste **Auto Boot Table** mit einem Anfangsstatus von [Not Loaded - Idle] hinzugefügt.

Obwohl der Anwendungsname in der Tabelle angezeigt wird, registrieren Sie tatsächlich die zugrundeliegende Firmware. Wenn die Sonde erneut gestartet wird, sind alle Anwendungen für diese Firmware in Viewman und Rmonview verfügbar.

Wenn die Sonde erneut gestartet wird, versucht sie, eine Verbindung zum entsprechenden TFTP-Server herzustellen, um die Firmware zu laden. Wenn dieser Vorgang erfolgreich ist, wird der Status der Firmware in der Autostart-Tabelle in [Autoboot Succeeded] geändert.

Wenn der Versuch, die Firmware zu laden, nicht erfolgreich war, wird die Nachricht [Autoboot failed] angezeigt.

2. Gehen Sie wie folgt vor, um Anwendungen zu inaktivieren und SmartAgent-Firmware aus der Autostart-Tabelle zu entfernen:
 - a. Wählen Sie die Anwendung in der Liste **Auto Boot Table** aus.
 - b. Klicken Sie **DELETE** an.

Die Firmware ist noch für die zugeordneten Anwendungen in der Liste **Available SmartAgent Apps** verfügbar. Die Anwendungen können jedoch nicht mehr in Viewman verwendet werden, wenn die Sonde erneut gestartet wird.

Protokolle hinzufügen

Gehen Sie wie folgt vor, um ein benutzerdefiniertes Protokoll hinzuzufügen:

- Klicken Sie **Add...** im Dialog **Protocol Directory** an, um den Dialog **User Defined Protocol** (siehe Abb. 24) zu öffnen.

Wenn ein Protokoll nicht erweitert werden kann, ist der Knopf **Add...** inaktiviert.

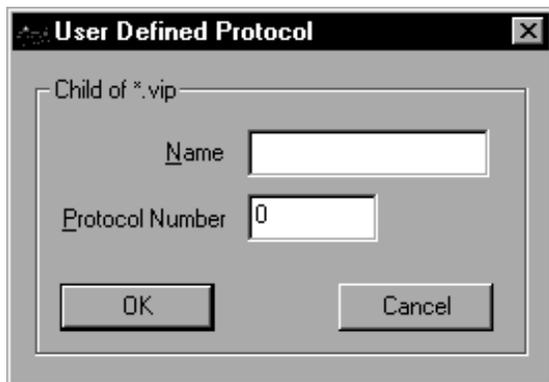


Abbildung 24. Dialog "User Defined Protocol"

- Geben Sie einen Namen und eine Protokollnummer für das gewünschte Protokoll ein. Wenn Sie kein Protokoll hinzufügen können, kann dies folgende Ursachen haben:
 - Das Protokoll, das Sie hinzuzufügen versuchen, ist bereits vorhanden.
 - Sie haben versucht, ein Protokoll zu erweitern, das nicht erweitert werden kann, d. h. der Knopf **Add...** ist inaktiviert.
 - Die Sonde unterstützt keine benutzerdefinierten Protokolle, d. h. der Knopf **Add...** ist inaktiviert.
 - Die Sonde hat keinen freien Speicher mehr. Sie müssen ein Protokoll löschen und einen Warmstart der Sonde ausführen, bevor Sie ein weiteres Protokoll hinzufügen können.

Wenn Sie einen Kaltstart durchführen, gehen alle benutzerdefinierten Informationen verloren.

- Klicken Sie **OK** an, um zum Dialog **Protocol Directory** zurückzukehren.

Protokolle löschen

Mit Nways Remote Monitor können Sie Protokolle löschen, die Sie zur Sonde hinzugefügt haben. Gehen Sie wie folgt vor, um ein benutzerdefiniertes Protokoll zu löschen:

1. Wählen Sie das gewünschte Protokoll im Dialog **Protocol Directory** aus.
2. Klicken Sie **Delete** an.

RMON2-Tabellen für Protokolle aktualisieren

Mit Nways Remote Monitor können Sie die RMON2-Tabellen für ein bestimmtes Protokoll oder für einen bestimmten Protokolleintrag und alle untergeordneten Protokolle aktualisieren.

Wählen Sie **Properties** aus, um die RMON2-Tabellen für ein bestimmtes Protokoll zu aktualisieren. Dieser Dialog zeigt den vollständigen Namen des Protokolls an und gibt auch an, ob das Protokoll erweitert werden kann. Gehen Sie wie folgt vor, um das Protokoll zu aktualisieren:

1. Wählen Sie das Protokoll im Dialog **Protocol Directory** aus.
2. Klicken Sie den Knopf **Properties** an.
3. Wählen Sie die erforderlichen RMON2-Tabellen aus.
4. Klicken Sie **OK** oder **Cancel** an, um zum Dialog **Protocol Directory** zurückzukehren.

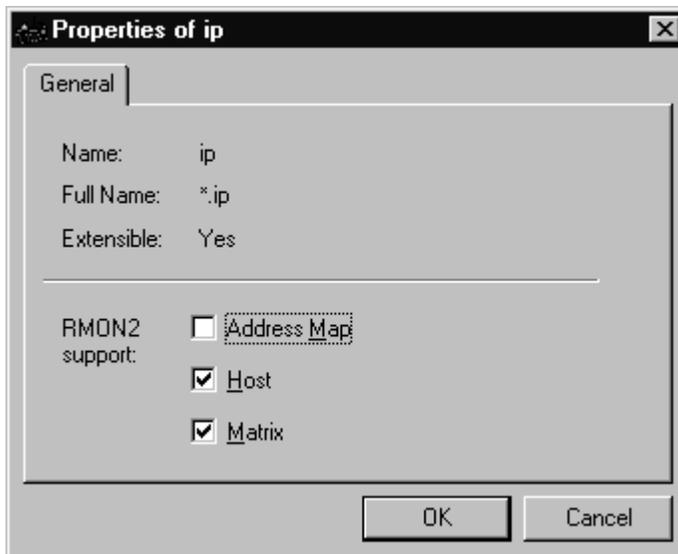


Abbildung 25. Beispiel für den Dialog "Protocol Properties"

Wählen Sie **Configure** aus, um die RMON2-Tabellen für ein bestimmtes Protokoll und die untergeordneten Protokolle zu aktualisieren. Gehen Sie wie folgt vor, um den Protokollbaum zu aktualisieren:

1. Wählen Sie die höchste Ebene des erforderlichen Protokollbaums im Dialog **Protocol Directory** aus.
2. Klicken Sie den Knopf **Configure** an.
3. Wählen Sie die erforderlichen RMON2-Tabellen aus.
4. Klicken Sie **OK** oder **Cancel** an, um zum Dialog **Protocol Directory** zurückzukehren.

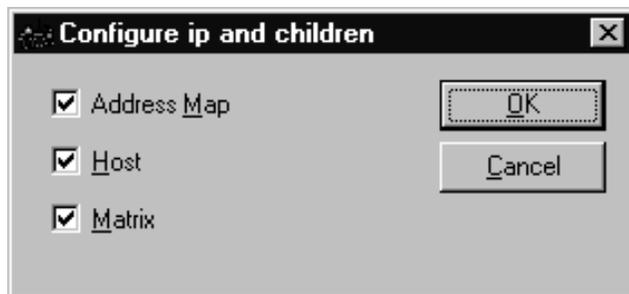


Abbildung 26. Beispiel für den Protokollkonfigurationsdialog

Stationsnamen definieren

Informationen zu den Stationen in Ihrem Netzwerk können auf zwei Arten hinzugefügt werden:

- Automatisch von Sonden über Nways Remote Monitor Translator gesammelt
Eine RMON2-Sonde oder eine Sonde mit SmartAgent-Firmware kann Informationen zu den Stationen in Ihrem Netzwerk sammeln. Diese Informationen können in regelmäßigen Abständen von Nways Remote Monitor Translator gesammelt werden.
- Manuell über den Dialog **Station List Edit** hinzugefügt
Die Ebene der Stationsadresse, die in den Anwendungen von Nways Remote Monitor angezeigt werden sollte, kann über Translator und den Dialog **Device Configuration** definiert werden.

In diesem Kapitel werden folgende Themen behandelt:

- Stationen automatisch erkennen
- Translator starten
- Stationen manuell einrichten
- Namensumsetzungsebene definieren
- Lieferantenpräfixe angeben

Stationen automatisch erkennen

Eine korrekt konfigurierte Sonde erstellt automatisch eine Tabelle, die für Einheiten, die im Netzwerk Daten austauschen, eine MAC-Adresse einer Vermittlungsschichtadresse zuordnet. Translator, eine Anwendung von Nways Remote Monitor, kombiniert die Adreßtabellen von mehreren Sonden in einer einzigen Adreßumsetzungstabelle. Diese Tabelle bietet Stationsadreßinformationen für alle anderen Anwendungen von Nways Remote Monitor.

Die folgenden beiden Arten von Sonden erstellen eine Adreßtabelle.

SmartAgent-Sonden

SmartAgent-Firmware wird zusammen mit Nways Remote Monitor ausgeliefert. Wenn diese SmartAgent-Firmware auf eine Sonde heruntergeladen ist, erstellt die Sonde automatisch die Adreßtabelle. Anweisungen zum Laden der SmartAgent-Firmware auf Sonden finden Sie in „RMON2-(ECAM)-SmartAgent-Firmware verwalten“ auf Seite 44.

RMON2-Sonden

RMON2-Sonden müssen so konfiguriert werden, daß sie die Adreßtabelle erstellen.

1. Öffnen Sie den Dialog **Device Configuration** (siehe „Dialog "Device Configuration" öffnen“ auf Seite 21).
2. Wählen Sie in diesem Dialog die Option **RMON2 Tables...** aus.
3. Aktivieren Sie das Markierungsfeld **Address Map** im Dialog **RMON2 Table Management**.
4. Wählen Sie **Apply** aus, damit alle Änderungen auf die Sonde angewendet werden.
5. Wählen Sie **Close** aus, um den Dialog zu schließen.

Anmerkung: Wenn Sie **Close** auswählen, ohne zuerst **Apply** ausgewählt zu haben, werden die Änderungen nicht wirksam.

Translator starten

Translator kann von Viewman, dem Nways Remote Monitor-Hauptfenster, oder von Ihrer Systemsoftware aus gestartet werden.

1. Klicken Sie in Viewman  an, oder wählen Sie **Translator** im Menü **Applications** aus.



Abbildung 27. Menü- und Funktionsleiste von Nways Remote Monitor

Menü "Start"

Wählen Sie die Programmgruppe **IBM Nways ReMon** im Menü **Start** und anschließend **Translator** im Menü **Applications** aus.

Translator-Hauptfenster

Das Translator-Hauptfenster ist in drei Bereiche unterteilt:

- Menüleiste
- Statusprotokoll
- Statusleiste

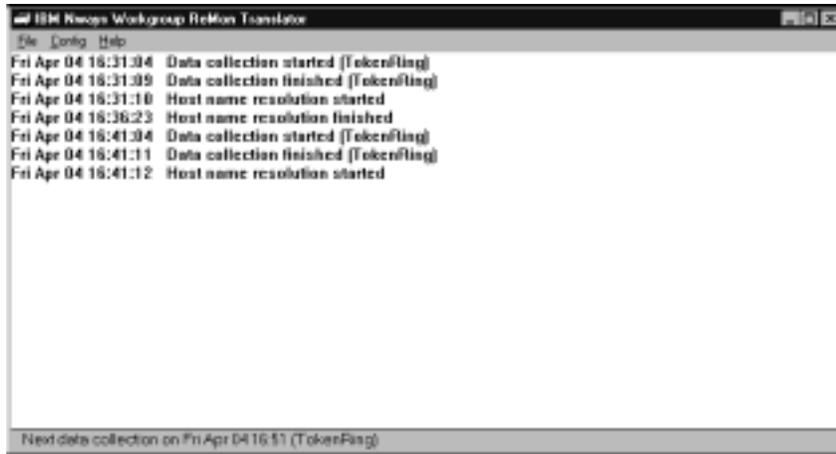


Abbildung 28. Translator-Hauptfenster

Menüleiste

Die Menüleiste am oberen Fensterrand bietet Zugriff auf folgende Funktionen:

File

Import	Lädt Stationsinformationen von Nways LAN Remote Monitor für Windows.
Save Status Log	Speichert den Inhalt des Statusprotokollbereichs im Hauptfenster in einer ASCII-Datei.
Print Status Log	Druckt den Inhalt des Statusprotokolls.
Exit	Schließt die Anwendung.

Config

Data Collections	Startet den Dialog Data Collection Configurations , in dem Sie Datensammlungen hinzufügen, ändern oder löschen können.
Translation Level	Ermöglicht das Definieren der Anzeigeebene von Stationsnamen, die für alle stationsbezogenen Ansichten von Nways Remote Monitor verwendet werden. Diese Funktion wird in „Namenumsetzungsebene definieren“ auf Seite 62 beschrieben.

Host Name Resolution	Wenn diese Option ausgewählt ist, versucht Translator, einen Host-Namen für jede gefundene IP-Adresse mit dem auf Ihrem PC konfigurierten Prozeß zum Suchen von Host-Namen (z. B. DNS) zuzuordnen.
RMON Devices	Bietet Zugriff auf den Dialog Device Configuration (siehe „Dialog "Device Configuration" öffnen“ auf Seite 21). Definiert die Liste der im Netzwerk verfügbaren RMON-kompatiblen Einheiten.

Help

Contents	Öffnet das Online-Hilfesystem von Nways Remote Monitor.
About Translator	Zeigt die Versionsinformationen und den Copyrightvermerk an.

Statusprotokoll

Das Statusprotokoll nimmt den größten Bereich im Hauptfenster ein. Während der Datensammlung werden in diesem Bereich Statusnachrichten angezeigt. Wenn der Bereich mit Nachrichten gefüllt ist, können Sie durch das Protokoll nach oben und unten blättern. Der Inhalt des Protokolls kann über die entsprechenden Optionen im Menü **File** in einer Datei gespeichert oder ausgedruckt werden.

Statusleiste

Die Statusleiste befindet sich am unteren Rand des Hauptfensters. Sie zeigt den Status der aktuellen oder nächsten Sammlung an.

Daten importieren

Wenn Sie von Nways LAN Remote Monitor für Windows erweitert haben, können Sie die Stationsinformationen aus der Datei `Host.Map` der älteren Version in Translator importieren. Sie müssen also stationspezifische Informationen nicht neu eingeben.

1. Wählen Sie **Import** im Menü **File** aus. Der Dialog **Import Host Map file** wird geöffnet.

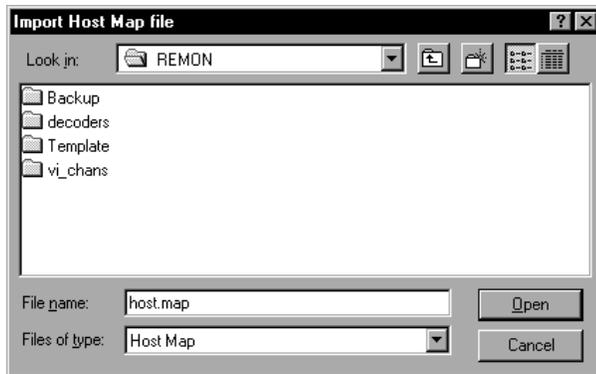


Abbildung 29. Dialog "Import Host Map file"

- Suchen Sie die Datei Host.Map, und klicken Sie **Open** an, um den Inhalt dieser Datei zu importieren.

Sie kehren zum Hauptfenster zurück. Am Ende der Statusleiste wird der Status **Importing** angezeigt. Diese Statusnachricht wird nicht mehr angezeigt, wenn der Import abgeschlossen ist.

Datensammlungen starten

Wenn Sie die Sammlung von Stationsinformationen starten wollen, müssen Sie eine Sammlungskonfiguration definieren, die angibt, von welchen Sonden und Schnittstellen Daten und welcher Datentyp gesammelt werden soll.

- Wählen Sie im Translator-Hauptfenster **Data Collections...** im Menü **Config** aus, um den Dialog **Data Collection Configurations** zu öffnen.

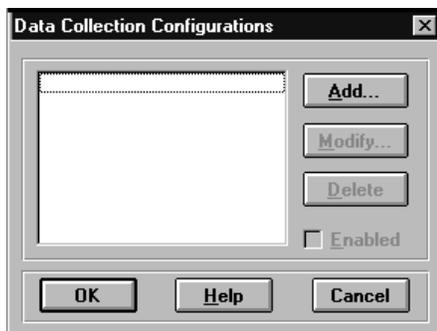


Abbildung 30. Dialog "Data Collection Configurations"

In diesem Dialog können Sie neue Sammlungskonfigurationen erstellen, indem Sie eine Konfiguration hinzufügen oder eine vorhandene Konfiguration ändern.

- Wenn Sie eine Konfiguration hinzufügen wollen, klicken Sie **Add...** an, um das Fenster **Data Collection Editor** zu öffnen.

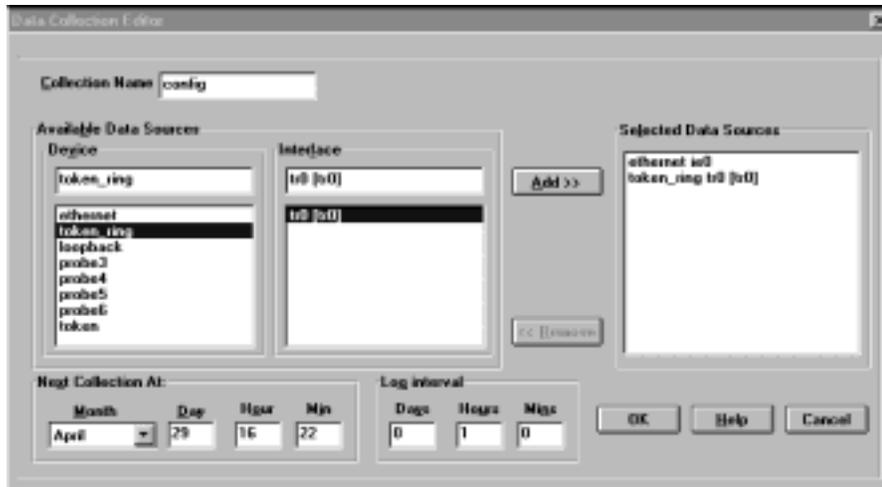


Abbildung 31. Dialog "Data Collection Editor"

3. Geben Sie einen eindeutigen Namen für diese Sammlung im Feld **Collection Name** ein.

- Klicken Sie die entsprechenden Einträge in den Listen **Device** und **Interface** an, um eine Sonde und eine Schnittstelle auszuwählen. Klicken Sie anschließend **Add>>** an.
- Gehen Sie wie folgt vor, wenn Sie mehrere Sonden auswählen wollen:
 - a. Führen Sie eine der folgenden Aktionen aus:
 - Klicken Sie bei gedrückter Taste **Strg** jede gewünschte Sonde in der Liste **Device** an.
 - Klicken Sie die erste Sonde an, und ziehen Sie sie mit der Maus zur letzten Sonde.
 - Klicken Sie die erste Sonde an, und klicken Sie bei gedrückter Umschalttaste die letzten Sonde an.
 - b. Klicken Sie **Add>>** an. Alle Schnittstellen der ausgewählten Sonden werden hinzugefügt.

*Wenn mehrere Sonden ausgewählt sind, werden standardmäßig alle verfügbaren Schnittstellen ausgewählt. Wenn Sie eine RMON2-kompatible Einheit verwenden, werden die Daten automatisch von allen Schnittstellen der Einheit gesammelt. Wenn Sie eine RMON-Einheit verwenden, auf der RMON2 (ECAM) SmartAgent geladen ist, müssen Sie eine Schnittstelle aus der Liste **Interface** auswählen.*

- Wenn Sie die Auswahl von Einträgen zurücknehmen wollen, klicken Sie einen Eintrag an, oder verwenden Sie eine der in Schritt 3 beschriebenen Verfahren zur Auswahl mehrerer Einträge. Klicken Sie anschließend **<<Remove** an.
- Stellen Sie im Bereich **Next Collection At** das Datum und die exakte Uhrzeit für den Start der Datensammlung ein.

- Stellen Sie im Bereich **Log Interval** die Häufigkeit ein, mit der nachfolgende Sammlungen erfolgen sollen. Standardmäßig ist diese Option auf stündliche Sammlung eingestellt.
 - Klicken Sie **OK** an, um diese Sammlungskonfiguration zu erstellen.
4. Wenn eine Sammlungskonfiguration erstellt wird, wird automatisch das Markierungsfeld **Enabled** im Dialog **Data Collection Configurations** aktiviert. Wenn Sie die Datensammlung für eine Konfiguration aktivieren wollen, klicken Sie einfach **OK** im Dialog **Data Collection Configurations** an, um Ihre Änderungen zu speichern und zum Translator-Hauptfenster zurückzukehren.

Der Zeitpunkt der nächsten geplanten Sammlung wird in der Statusleiste am unteren Rand des Hauptfensters angezeigt. Ein Protokoll der Datensammlungen wird im Statusprotokollbereich im Hauptfenster geführt.

Datensammlungen stoppen

Wenn Sie die Datensammlung für eine Konfiguration stoppen wollen, können Sie sie entweder inaktivieren oder löschen.

1. Wählen Sie im Translator-Hauptfenster **Data Collections...** im Menü **Config** aus, um den Dialog **Data Collection Configurations** (siehe Abb. 30 auf Seite 57) zu öffnen.
2. Gehen Sie wie folgt vor, um die Datensammlung für eine Konfiguration zu inaktivieren:
 - a. Wählen Sie die Konfiguration durch Anklicken aus.
 - b. Klicken Sie das Markierungsfeld **Enabled** an, um es zu inaktivieren.
 Wenn Sie die Sammlung später wieder aktivieren wollen, klicken Sie einfach erneut das Markierungsfeld **Enabled** an.
3. Gehen Sie wie folgt vor, um eine Konfiguration endgültig zu löschen:
 - a. Wählen Sie die gewünschte Konfiguration durch Anklicken aus.
 - b. Klicken Sie **Delete** an.
4. Zum Speichern Ihrer Änderungen klicken Sie **OK** an.

Datensammlungen löschen

Führen Sie folgende Schritte aus, um eine Datensammlungskonfiguration endgültig zu löschen:

1. Wählen Sie die gewünschte Konfiguration durch Anklicken aus.
2. Klicken Sie **Delete** an.
3. Zum Speichern Ihrer Änderungen klicken Sie **OK** an. Wenn Sie Ihre Änderungen rückgängig machen wollen, klicken Sie **Cancel** an.

Stationen manuell einrichten

Sie können mit dem Dialog **Station List Edit** Einträge in der Translator-Tabelle hinzufügen oder ändern, möglicherweise um eine Station einzurichten, bevor sie zum Netzwerk hinzugefügt wird, oder um einen neuen Namen für eine vorhandene Station hinzuzufügen.

1. Der Dialog **Station List Edit** wird über den Dialog **Device Configuration** gestartet (siehe „Dialog "Device Configuration" öffnen“ auf Seite 21).
2. Klicken Sie **Stations...** im Dialog **Device Configuration** an.

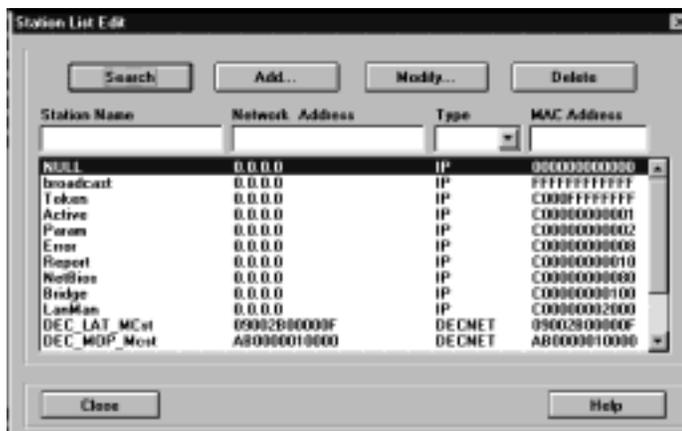


Abbildung 32. Dialog "Station List Edit"

Folgende Werte werden für jede Station angezeigt:

- Station Name** Ein benutzerdefinierter Name oder ein von Translator über den auf Ihrem PC konfigurierten Prozeß zum Suchen von Host-Namen erkannter Name.
- Network Address** Die Netzwerkadresse dieser Station.
- Type** Entweder IP, IPX, DECnet, SNA, AppleTalk oder VINES.
- MAC Address** Die 12stellige MAC-Adresse der Station.

3. Der Dialog **Station List Edit** enthält eine Suchfunktion, mit der Sie nach einer beliebigen Zeichenfolge in einem der verfügbaren Felder suchen können.
 - a. Wenn Sie nach einer bestimmten Zeichenfolge suchen wollen, geben Sie einen Wert in das Feld **Station Name**, **Network Address** oder **MAC Address** ein, oder wählen Sie einen Netzwerktyp aus. Klicken Sie dann **Search** an. Alle übereinstimmenden Einträge werden in der Stationsliste angezeigt.

- b. Verwenden Sie einen Stern (*) als Platzhalterzeichen, wenn Sie eine Zeichenfolge eingeben, und klicken Sie **Search** an. Wenn Sie z. B. **1127.40.*.*** im Feld **Network Address** eingeben, wird jede Station, deren Netzwerkadresse mit 127.40. beginnt, in der Stationsliste angezeigt.
 - c. Wenn Sie alle Stationseinträge anzeigen wollen, lassen Sie die Felder **Station Name**, **Network Address**, **MAC Address** und **Type** leer, und klicken Sie **Search** an. In der Stationsliste werden dann alle Einträge angezeigt.
4. Wenn Sie eine neue Station hinzufügen wollen, klicken Sie **Add** an, um den Dialog **Add Station** zu öffnen.



Abbildung 33. Dialog "Add Station"

- a. Geben Sie neue Werte in den Feldern **Station Name**, **Network Address** und **MAC Address** ein.
 - b. Wählen Sie einen Typ aus der verdeckten Liste **Type** aus.
 - c. Klicken Sie **OK** an, um diese neue Station zu erstellen. Sie kehren zurück zum Dialog **Station List Edit**.
5. Gehen Sie wie folgt vor, um eine Station zu ändern:
 - a. Klicken Sie den Eintrag in der Stationsliste und anschließend **Modify...** an, um den Dialog **Edit Station** zu öffnen.

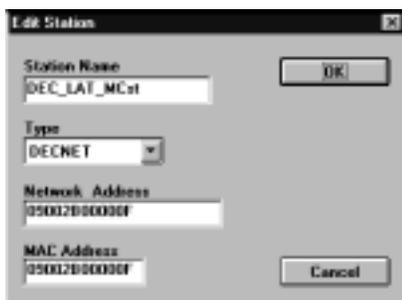


Abbildung 34. Dialog "Edit Station"

- b. Editieren Sie nach Bedarf die Werte in den jeweiligen Feldern.
 - c. Klicken Sie **OK** an, um Ihre Änderungen zu bestätigen.
6. Gehen Sie wie folgt vor, um eine Station zu löschen:
- a. Klicken Sie den Eintrag in der Stationsliste an.
 - b. Klicken Sie **Delete** an.
7. Klicken Sie **Close** an, um zum Hauptfenster zurückzukehren.

Namenumsetzungsebene definieren

Vier Namenumsetzungsebenen sind in Nways Remote Monitor verfügbar.

Diese Ebenen sind in Tabelle 8 beschrieben:

Tabelle 8. Namenumsetzungsebenen

Ebene	Beschreibung
Name Translation	Der Name, der der Einheit zugeordnet ist. Es kann der für die Einheit gefundene Systemname oder ein beliebiger benutzerdefinierter Name sein.
Protocol Address	Die Protokolladresse für die Einheit.
Vendor ID	Die ersten 6 Zeichen dieses Namens, übernommen von der Lieferanten-ID in der Datei Vendor.Map, gefolgt von den letzten 6 Ziffern der MAC-Adresse (siehe „Lieferantenpräfixe angeben“ auf Seite 63).
MAC Address	Die 12stellige MAC-Adresse.

Nways Remote Monitor versucht, einen Wert für die ausgewählte Ebene anzuzeigen. Wenn ein Wert nicht verfügbar ist, wird die nächste Ebene angezeigt, usw. Als Ergebnis kann eine Mischung aus unterschiedlichen Namensebenen angezeigt werden.

Sie können über den Dialog **Set Translation Level** auswählen, welche Adreßebenen Nways Remote Monitor versuchen soll, in allen stationsbezogenen Ansichten anzuzeigen. Sie können auch Ihr bevorzugtes Netzwerkprotokoll festlegen.

1. Der Dialog **Set Translation Level** kann über Remote Monitor Translator und auch über den Dialog **Device Configuration** aufgerufen werden.
 - Wählen Sie im Translator-Hauptfenster **Translation Level** im Menü **Config** aus.
 - Klicken Sie **Translation...** im Dialog **Device Configuration** an.

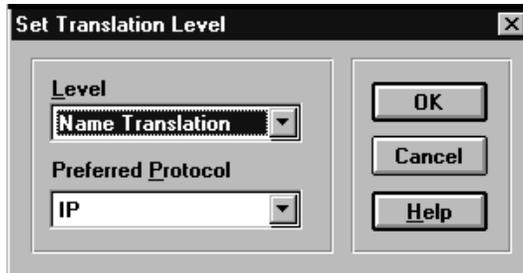


Abbildung 35. Dialog "Set Translation Level"

2. Wenn Sie die Ebene der Adreßumsetzung definieren wollen, die Nways Remote Monitor versuchen soll anzuzeigen, wählen Sie entweder **Name Translation**, **Protocol Address**, **Vendor ID** oder **MAC Address** in der verdeckten Liste **Level** aus.
3. Wenn Sie in **Preferred Protocol** das bevorzugte Protokoll festlegen wollen, wählen Sie **IP**, **IPX**, **DECnet**, **AppleTalk**, **VINES** oder **SNA** in der verdeckten Liste aus. Das bevorzugte Protokoll gibt an, welche Protokolladresse oder welcher Name angezeigt werden soll, wenn eine bestimmte MAC-Adresse mehr als eine Netzwerkadresse hat.
4. Klicken Sie **OK** an, um die neue Einstellung zu speichern.

Die neue Ebene wird in Viewman oder in jeder stationsspezifischen Anwendungsanzeige bei der nächsten Aktualisierung angezeigt.

Lieferantenpräfixe angeben

Jedes Gerät hat unabhängig von seinem Herstellungsort eine eigene, eindeutige MAC-Adresse. Damit dies möglich ist, wird jedem Lieferanten ein Adressenblock zugeordnet. Der Lieferant ordnet dann jeder hergestellten Einheit eine andere Adresse zu. Jede Adresse, die beispielsweise mit der Zeichenfolge 0004AC beginnt, ist eine IBM Einheit. In Nways Remote Monitor sind bereits die wichtigsten Lieferantenpräfixe definiert. Wenn Sie diese anzeigen wollen, öffnen Sie die Datei `Vendor.Map` im Installationsverzeichnis. Ein typischer Eintrag in der Datei `Vendor.Map` sieht folgendermaßen aus:

```
0004AC      IBM_$
```

Immer, wenn Nways Remote Monitor eine Adresse wie z. B. 0004AC123456 sieht, zeigt es die Adresse als `IBM_123456` an. Dies erleichtert die Identifikation der Einheiten.

Wenn Sie eigene Lieferantennamen in der Datei `Vendor.Map` hinzufügen wollen, editieren Sie einfach die Datei mit einem Texteditor, z. B. **Editor** oder **Write**.

Viewman

Das Viewman-Hauptfenster ermöglicht eine einfache Prüfung eines LAN-Segments, bei der Hauptfehler und Belegungsinformationen angezeigt werden. Weiterhin werden Alarmpositionen und Statusnachrichten angezeigt.

Wenn Sie eine physische oder virtuelle Schnittstelle einer fernen Sonde auswählen, können Sie Leistung und Zustand des überwachten Netzwerksegments anzeigen.

Die im Hauptfenster angezeigten Diagramme variieren je nach Datenträgertyp der ausgewählten Schnittstelle. Sie können Teile der angezeigten Diagramme anklicken, um weitere Details anzuzeigen.

Eine Beschreibung des Viewman-Hauptfensters finden Sie in „Mit der Schnittstelle von Nways Remote Monitor arbeiten“ auf Seite 7.

In diesem Kapitel finden Sie die folgenden Abschnitte:

- Viewman starten
- Das Hauptfenster konfigurieren
- Viewman-Diagramme

Viewman starten

Wenn Sie Viewman starten wollen, wählen Sie die Programmgruppe **IBM Nways ReMon** im Menü **Start** und anschließend **Viewman** aus.

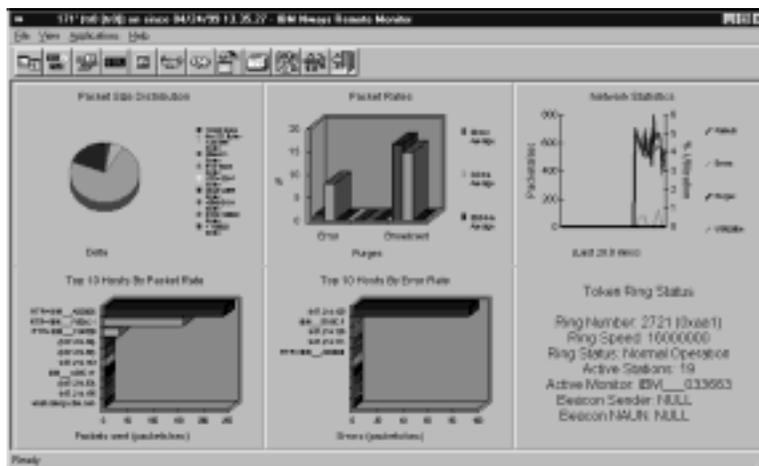


Abbildung 36. Viewman

Das Hauptfenster konfigurieren

Die gesamte Konfiguration des Hauptfensters wird über das Menü **View** ausgeführt. Die Funktionsleiste, Statusleiste und der Fensterbereich mit der Alarmleiste können angezeigt oder verdeckt werden.

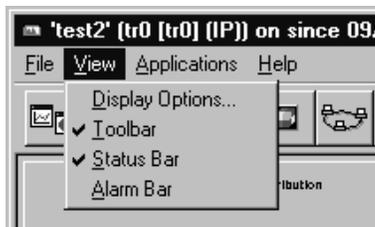


Abbildung 37. Menü "View"

Über Viewman **Display Options** können Sie folgendes konfigurieren:

- Zu überwachende LAN-Segmente
 - Die Aktualisierungsrate der angezeigten Daten
 - Die Auswahl der Grafikanzeigen
1. Wählen Sie *Display Options...* im Menü *View* aus, um den Dialog **Display Options** zu öffnen.

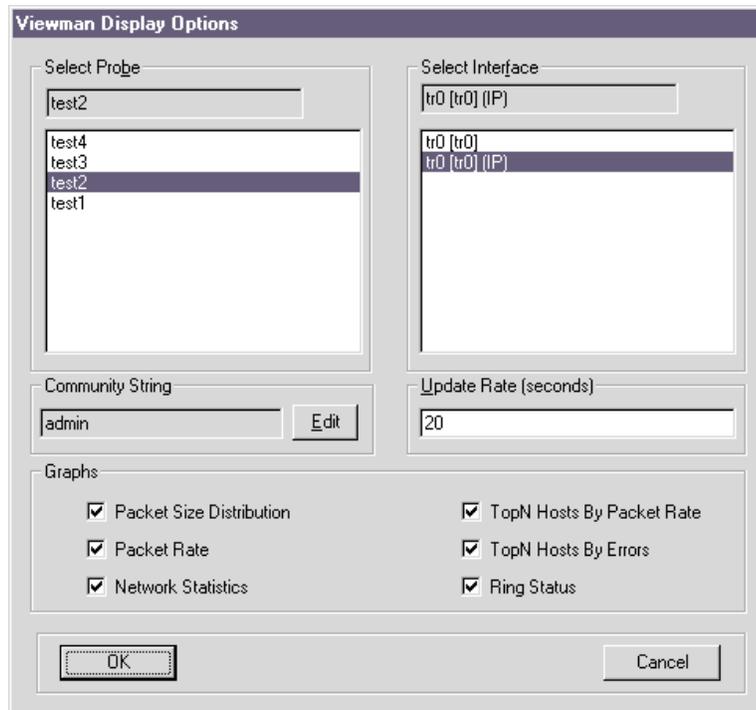


Abbildung 38. Dialog "Display Options"

2. Wählen Sie das zu überwachende Netzwerksegment aus:
 - a. Klicken Sie die Sonde in der Liste *Select Probe* an. Wenn die Sonde verfügbar ist, werden in der Liste **Select Interface** die verfügbaren Schnittstellen der Sonde angezeigt.
 - b. Wählen Sie eine physische oder virtuelle Schnittstelle durch Anklicken aus der Liste aus. Wenn Sie eine virtuelle Schnittstelle auswählen, überwachen Sie die Datenuntergruppe, die für diese Schnittstelle konfiguriert wurde (siehe „Virtuelle Schnittstellen konfigurieren“ auf Seite 39).
3. Die Zeichenfolge für die Benutzergemeinschaft, die derzeit verwendet wird, wird im Feld *Community String* angezeigt. Gehen Sie wie folgt vor, um diese Zeichenfolge zu ändern:
 - a. Klicken Sie **Edit** an, um den Dialog **Edit Community** zu öffnen.
 - b. Geben Sie die neue Zeichenfolge für die Benutzergemeinschaft ein.
 - c. Klicken Sie **OK** an, um Ihre Änderungen zu speichern und zum Dialog **Display Options** zurückzukehren. In zukünftigen Übertragungen von und zu der Sonde wird die neue Zeichenfolge für die Benutzergemeinschaft verwendet. Klicken Sie **Cancel** an, um Ihre Änderungen zu verwerfen.

4. Geben Sie im Feld **Update Refresh** die Aktualisierungsrate in Sekunden an, in der die Diagramme mit neuen Daten aktualisiert werden sollen.
5. Geben Sie an, welche Diagramme im Viewman-Hauptfenster angezeigt werden sollen, indem Sie die gewünschten Diagramme auswählen bzw. die Auswahl zurücknehmen. In der Standardeinstellung werden alle Diagramme angezeigt. Informationen zur Verfügbarkeit von Diagrammen finden Sie in „Viewman-Diagramme“.
6. Klicken Sie **OK** an, um Ihre Auswahl zu bestätigen, so daß Viewman eine Aktualisierung mit den ausgewählten Netzwerksegmenten vornehmen kann.

Viewman-Diagramme

Die Liste der verfügbaren Diagramme ändert sich, je nach dem Datenträgertyp der ausgewählten Sonde bzw. bei Sonden mit Mehrfachschnittstellen nach der ausgewählten Schnittstelle.

In diesem Abschnitt finden Sie eine Definition der einzelnen Diagramme und ihrer Verwendungsmöglichkeit für die Netzwerküberwachung.

Tabelle 9. Verfügbare Diagramme nach Datenträgertyp

Diagrammliste	Datenträgertyp		
	Ethernet	FDDI	Token-Ring
Packet Size Distribution	■	■	■
Packet Rates	■	■	■
Network Statistics	■	■	■
Top 10 Hosts By Packet Rate	■	■	■
Top 10 Hosts By Error Rate	■		■
Top 10 Receivers on FDDI		■	
Event Distribution	■		
Ring Status		■	■

Diagramm "Packet Size Distribution"

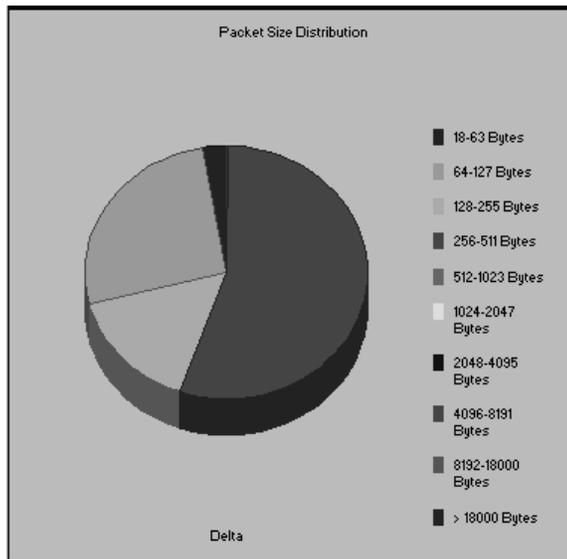


Abbildung 39. Diagramm "Packet Size Distribution" für Token-Ring

Das Diagramm **Packet Size Distribution** veranschaulicht auf einfache Weise, wie der gesamte Datenverkehr Ihres Netzwerks aufgebaut ist. In der Regel werden Paketgröße, den Anteil großer und kleiner Pakete am Datenverkehr und weitere Informationen angezeigt. Das Diagramm wird als Variation oder *Delta* über den letzten Erfassungszeitraum dargestellt.

Diagramm "Packet Rates"

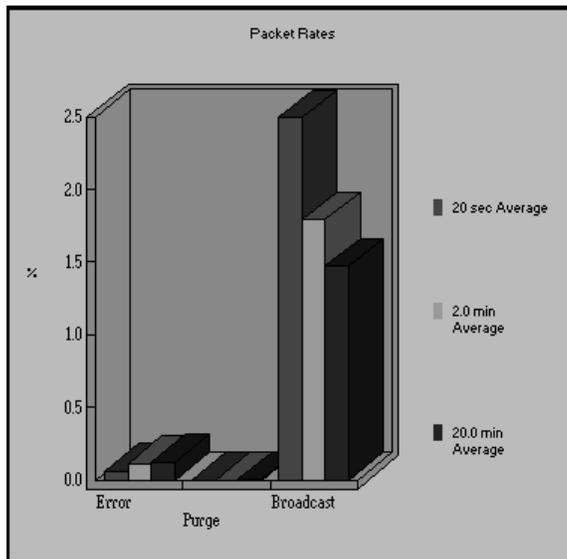


Abbildung 40. Diagramm "Packet Rates" für Token-Ring

Das Diagramm **Packet Rates** zeigt Ihnen auf einen Blick, wieviele Rundsendepakete, Fehler, Kollisionen, SMT-Rahmen oder Freigaben im Netzwerk festgestellt wurden, und ermöglicht Ihnen somit jederzeit eine schnelle Beurteilung der Netzwerkleistung. Sie können sehen, was im aktuellen und in früheren Berichtszeiträumen passierte.

Tabelle 10. Diagrammvariablen für "Packet Rate" nach Datenträgertyp

Variablen	Datenträgertyp		
	Ethernet	FDDI	Token-Ring
Broadcasts	■	■	■
Collisions	■		
Errors	■	■	■
Purges			■
SMT Frames		■	

Diagramm "Network Statistics"

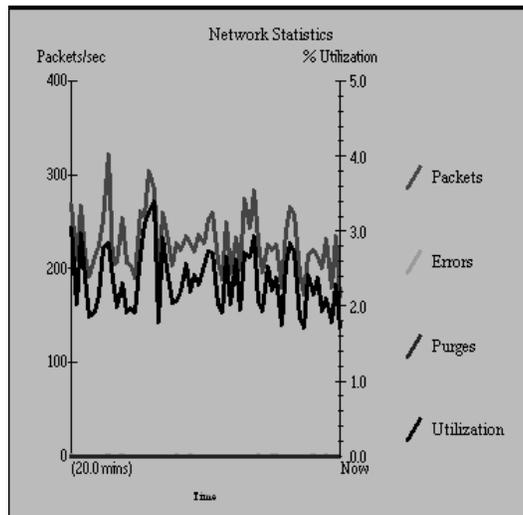


Abbildung 41. Diagramm "Network Statistics" für Token-Ring

Das Diagramm **Network Statistics** stellt Pakete, Fehler, Kollisionen, SMT-Rahmen, Freigaben und Netzwerkauslastung in Form einer Zeitliniengrafik dar. Es vergleicht Spitzen im Datenverkehr mit Spitzen im Fehler-, Freigabe- oder Kollisionsaufkommen und ermöglicht so eine schnelle Beurteilung des Netzwerkzustands.

Tabelle 11. Diagrammvariablen für "Network Statistics" nach Datenträgertyp

Variablen	Datenträgertyp		
	Ethernet	FDDI	Token-Ring
Collisions	■		
Errors	■	■	■
Packets	■	■	■
Purges			■
SMT Frames		■	
Utilization	■	■	■

Diagramm "Top 10 Hosts by Packet Rate"

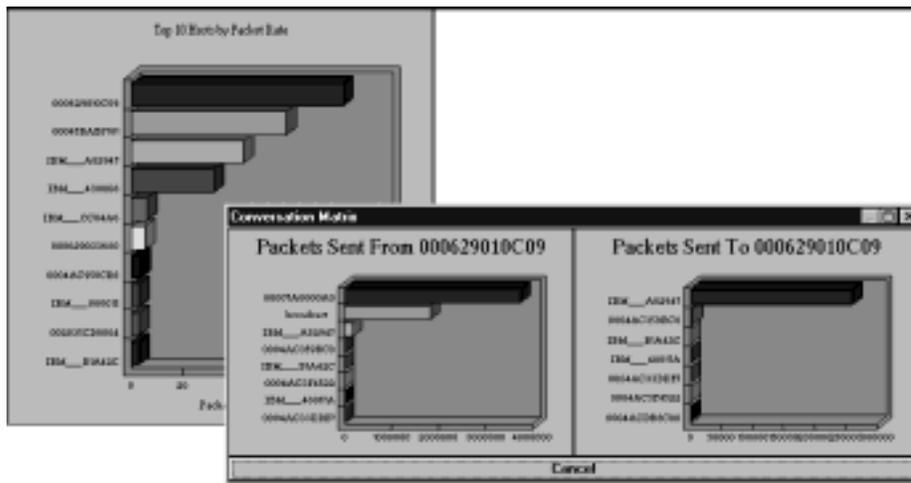


Abbildung 42. Diagramm "Top 10 Hosts by Packet Rate" für Ethernet

Welche Hosts oder Stationen des Netzwerks sind für den meisten Datenverkehr verantwortlich? Wenn es an einer bestimmten Station ein Unterbrechung gibt, oder wenn Sie herausfinden wollen, mit wem sie gerade verbunden ist, klicken Sie einfach den entsprechenden Balken des Histogramms an, um eine Detailanzeige aufzurufen.

Diagramm "Top 10 Hosts by Error Rate" (Ethernet und Token-Ring)

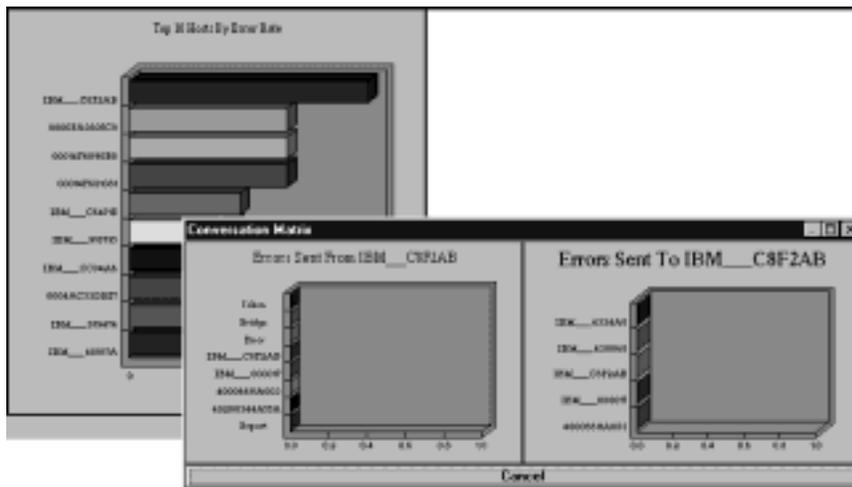


Abbildung 43. Diagramm "Top 10 Hosts by Error Rate" für Ethernet

Dieses Diagramm gibt es für Ethernet und Token-Ring. Es enthält die folgenden Informationen:

- Herkunft der meisten Fehlerpakete
- Andere Stationen, mit denen die betreffenden Stationen noch verbunden sind

Klicken Sie den entsprechenden Balken an, um einen Bericht über den möglichen Verursacher von Netzwerkproblemen aufzurufen.

Diagramm "Top 10 Receivers" (FDDI)

Diese FDDI-spezifische Anzeige ersetzt die Anzeige **Top 10 Hosts by Error Rate** für Ethernet- und Token-Ring-Schnittstellen. Sie sehen hier auf einen Blick die 10 Ziel-Hosts oder Ziel-Stationen mit dem höchsten Anteil am Datenverkehr im Netzwerk. Klicken Sie einen Balken des Histogramms an, um abzufragen, wer mit diesen Stationen verbunden ist.

Diagramm "Event Distribution" (Ethernet)

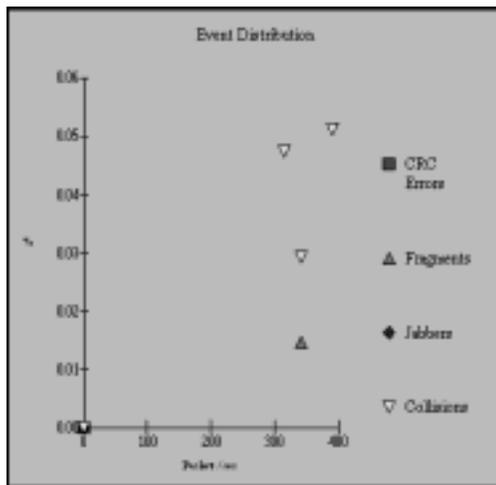


Abbildung 44. Diagramm "Event Distribution" für Ethernet

Verfolgen Sie Trends in Ethernet, indem Sie Cluster suchen. Ist es z. B. möglich, daß sich Fehler häufen, sobald der Datenverkehr eine bestimmte Grenze überschreitet?

Diagramm "Ring Status" (FDDI und Token Ring)

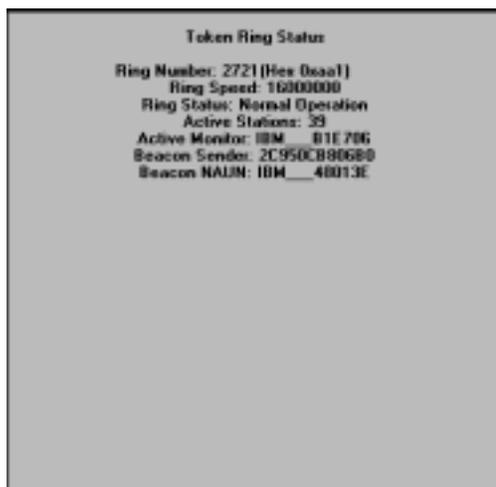


Abbildung 45. Diagramm "Ring Status" für Token-Ring

Die Anzeige **Ring Status** gibt eine konstant aktualisierte Zusammenfassung der Ring-Informationen entweder für FDDI (Tabelle 12) oder Token-Ring (Tabelle 13).

Tabelle 12. Variablen für "Ring Status" für FDDI

Variable	Definition
Neg. Token Rotation Time	Vom Gewinner der Senderechanforderung angebotene Umlaufdauer des Tokens.
Mean Token Rotation Time	Durchschnittliche Umlaufdauer des Tokens in der letzten Stichprobenperiode.
SMT Frames	In diesem Ring gezählte Rate der SMT-Rahmen in Rahmen pro Sekunde.
Claim Frames	In diesem Ring gezählte Rate der Bestätigungsrahmen in Rahmen pro Sekunde.
Dir. Beacon Frames	In diesem Ring gezählte Rate der Rahmen mit Beacon-Nachrichten in Rahmen pro Sekunde.
Beacon Frames	In diesem Ring gezählte Rate der Beacon-Nachrichten in Rahmen pro Sekunde.
Dir. Beacon Source	Adresse des Hosts, der die letzte übertragene Beacon-Nachricht gesendet hat.
Beacon Source	Adresse des Hosts, der die letzte Beacon-Nachricht gesendet hat.
Ring Status	Aktueller Betriebsstatus des FDDI-Rings: <ol style="list-style-type: none"> 1. Ring Operational 2. Non-Operational Claim 3. Non-Operational Beacon 4. Non-Operational Directed Beacon 5. Unknown

Tabelle 13. Variablen für "Ring Status" für Token-Ring

Variable	Definition
Ring Number	Die Ringnummer dieses Ringsegments.
Ring Status	Der aktuelle Gesamtstatus des Rings.
Active Stations	Die Anzahl aktiver Stationen im Ring.
Active Monitor	Der aktuelle aktive Monitor im Ring.
Beacon Sender	Die letzte Station, die Rahmen mit Beacon-Nachrichten an den Ring übertragen hat.
Beacon NAUN	Die NAUN (Nearest Active Upstream Neighbor) der letzten Station mit Beacon-Betrieb.

Rmonview und RMON-Anwendungen

RMON-Anwendungen von Nways Remote Monitor werden für die Sammlung von vordefinierten oder benutzerdefinierten Netzwerkdaten verwendet. Die Anwendungen können über Viewman gestartet werden, es ist aber auch möglich, sie unabhängig über Rmonview zu starten. Wenn eine Anwendung über Viewman gestartet wird, wird auch Rmonview automatisch gestartet und die Anwendung wird in Rmonview im Anzeigebereich für Anwendungen angezeigt.

Dieses Kapitel enthält die folgenden Abschnitte:

- Rmonview starten
- RMON-Anwendungen starten
 - über Rmonview
 - über Viewman
- RMON-Anwendungen konfigurieren
- Anzeigen erstellen und editieren
 - Statistikanzeige (Statistics View)
 - Protokollanzeige (History View)
 - Host-Anzeige (Host View)
 - Matrixanzeige (Matrix View)
 - Ringstationsanzeige (Ring Station View)
 - Alarmanzeige (Alarms View)
- Adreßumsetzungsanzeige (Address Translation View)
- Protokollverteilung (Protocol Distribution) anwenden

Eine Beschreibung des Hauptfensters von Rmonview finden Sie in „Mit der Schnittstelle von Nways Remote Monitor arbeiten“ auf Seite 7.

Rmonview starten

Wenn Sie Rmonview starten wollen, wählen Sie die Programmgruppe *IBM Nways ReMon* im Menü **Start** und anschließend *Rmonview* aus.

RMON-Anwendungen starten

Sie können eine Anwendung über Rmonview oder Viewman starten. Alle gestarteten Anwendungen werden in Rmonview im Anzeigebereich für Anwendungen angezeigt.

Rmonview

Gehen Sie wie folgt vor, um eine Anwendung über Rmonview zu öffnen:

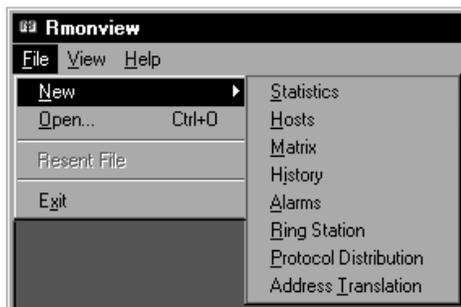


Abbildung 46. Anwendung über Rmonview öffnen

1. Wählen Sie *New* im Menü **File** aus.
2. Wählen Sie die gewünschte Anwendung aus. Nun wird der Dialog für die jeweilige Anwendungsanzeige bzw. der Dialog **Sample Point Selection** geöffnet, in dem Sie die Anwendung konfigurieren können.

Viewman

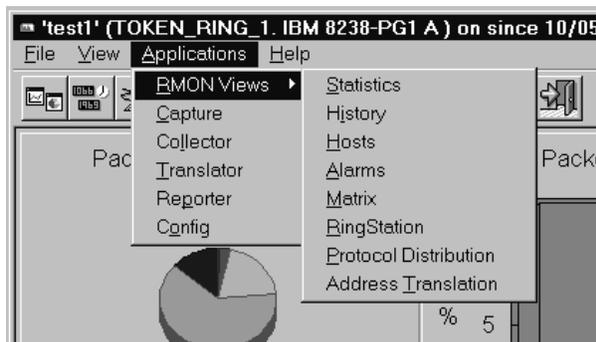
Verwenden Sie eine der folgenden Möglichkeiten, um eine RMON-Anwendung über Viewman zu öffnen:

- Wenn es für die gewünschte Anwendung einen eigenen Knopf in der Funktionsleiste gibt, verwenden Sie diesen. Es gibt Knöpfe für die folgenden Anwendungen: **Statistics, Hosts, Matrix, History, Alarms** und **Ring Station**.



Abbildung 47. Viewman-Menüleiste und -Funktionsleiste

- Wählen Sie **RMON Views** im Menü **Applications** aus. Wählen Sie anschließend die gewünschte Anwendung aus.



Wenn Sie **Statistics, Hosts, Matrix, History, Alarms** oder **Ring Station** auswählen, wird der Dialog für die entsprechende Anwendungsanzeige geöffnet.

Wenn Sie **Protocol Distribution** oder **Address Translation** auswählen, wird die in Viewman angezeigte Einheit automatisch als Ausgangspunkt für Stichproben ausgewählt.

Anmerkung: Diese Vorauswahl eines Ausgangspunkts für Stichproben wird nur getroffen, wenn RMON2-(ECAM)-Anwendungen über Viewman gestartet werden. Rmonview zeigt den Dialog **Sample Point Selection** an, damit Sie eine Einheitenschnittstelle auswählen können.

RMON-Anwendungen konfigurieren

In diesem Abschnitt finden Sie die Prozeduren zum Erstellen und Editieren von Anzeigen.

Für die Anwendungen **Statistics**, **History**, **Hosts**, **Matrix** und **Ring Station** (Token-Ring) stehen Ihnen eine Reihe vordefinierter Anzeigen zur Verfügung. Sie können aber auch Ihre eigenen Anzeigen anhand von Variablenlisten erstellen. Nachfolgend finden Sie eine Anleitung zum Erstellen und Editieren von Anzeigen. Die Prozedur ist für alle genannten Anwendungen identisch.

Anzeigen erstellen und editieren

Gehen Sie wie folgt vor, um eine neue Anzeige zu erstellen oder eine bereits vorhandene zu editieren:

1. Starten Sie die entsprechende Anwendung, wie in „RMON-Anwendungen starten“ auf Seite 78 beschrieben.

Daraufhin wird der jeweilige Dialog **View** für die Anwendung geöffnet. Im Anschluß an diesen Abschnitt finden Sie eine vollständige Beschreibung der einzelnen Anwendungsanzeigen.



Abbildung 48. Beispiel für den Dialog oder die Anwendungsanzeige

2. Wählen Sie eine Sonde und eine Schnittstelle aus.
3. Wählen Sie eine Anzeige in der Liste **View** aus. Die Liste sieht je nach Anwendung und Datenträgertyp der ausgewählten Schnittstelle unterschiedlich aus.

4. Klicken Sie **Edit/Create View** an, um den Dialog **Edit User View** zu öffnen.

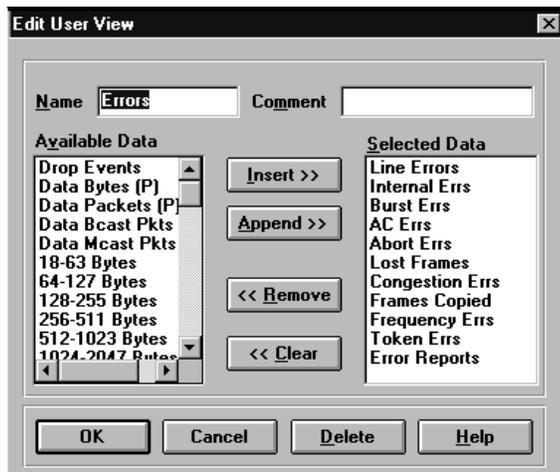


Abbildung 49. Dialog "Edit User View"

5. Ändern Sie gegebenenfalls den im Feld *Name* angegebenen Namen. In das Feld *Comment* können Sie einen zusätzlichen Kommentar eingeben.
6. Klicken Sie gegebenenfalls **<<Clear** an, um die Variablen aus der Liste **Selected Data** zu löschen.
7. Klicken Sie eine Variable in der Liste *Available Data* an, um diese auszuwählen, bzw. die Auswahl wieder zurückzunehmen. Die Variablenliste enthält je nach Datenträgertyp der ausgewählten Schnittstelle unterschiedliche Variablen.
8. Klicken Sie **Insert>>** oder **Append>>** an, um die Auswahl zur Liste **Selected Data** hinzuzufügen. Damit definieren Sie die Reihenfolge, in der die Kategorien auf dem Bildschirm angezeigt werden.
 - a. Mit *Insert>>* fügen Sie den neuen Eintrag am Anfang der Liste bzw. vor dem in der Liste ausgewählten Eintrag hinzu.
 - b. Mit *Append>>* hängen Sie den neuen Eintrag an das Ende der Liste bzw. an den in der Liste ausgewählten Eintrag an.
9. Klicken Sie **OK** an, um die Anzeige zu speichern und zum Dialog der entsprechenden Anwendungsanzeige zurückzukehren.

Statistikanzeige (Statistics View)

Während eine Sonde mit einem fernen Segment Ihres Netzwerks verbunden und eingeschaltet ist, sammelt sie statistische Daten über alle Aktivitäten dieses Segments. Dazu gehören auch korrekte und fehlerhafte Pakete. Nways Remote Monitor stellt Statistiken auf zwei Arten grafisch dar: Entweder werden die Änderungen innerhalb eines bestimmten Zeitintervalls erfaßt oder es wird die Gesamtstatistik seit Aktivierung der Sonde angezeigt.

*Wenn Sie prüfen wollen, welche dieser Werte grafisch dargestellt werden können, wählen Sie **Graphed Values** im Menü **Options** im RMON-Hauptdialog aus.*

Statistische Daten werden bevorzugt pro Segment geführt, statt pro Station. Damit erreichen Sie die Anzeige auf höherer Ebene und können Aktivitätsspitzen eines Segments hervorheben.

"Statistics View" konfigurieren

1. Starten Sie den Dialog **Statistics View**, wie in „RMON-Anwendungen starten“ auf Seite 78 beschrieben.



Abbildung 50. Dialog "Statistics View"

2. Klicken Sie in der Liste **Probe** die Sonde an, deren statistische Daten Sie analysieren wollen. Wenn die Sonde verfügbar ist, werden in der Liste **Interface** die Schnittstellen der Sonde angezeigt.
3. Klicken Sie den Namen einer Schnittstelle in der Liste **Interface** an, um auf die Daten in einem der LAN-Segmente zuzugreifen, die von der Sonde überwacht werden.

4. Wählen Sie im Bereich **View** eine der vordefinierten oder eine der von Ihnen definierten Anzeigen aus.

a. Die Liste der vordefinierten Anzeigen ändert sich in Abhängigkeit vom Datenträgertyp der ausgewählten Schnittstelle. Tabelle 14 beschreibt die für Ethernet und FDDI verfügbaren Statistikanzeigen.

Tabelle 14. Vordefinierte Statistikanzeigen

Anzeige	Daten-trägertyp	Beschrei-bung	Ethernet	FDDI
All	■	■		Enthält alle für den Datenträgertyp relevanten Variablen.
Bytes	■	■		Die Anzahl Byte, aus denen die Pakete bestehen (d. h. alle Byte, die in diesem Segment versendet wurden).
Distribution	■	■	■	Pakete, die nach ihrer Größe in verschiedene Kategorien eingeordnet werden.
Errors	■	■	■	Die Anzahl der im Segment festgestellten Fehler.
Events			■	Ringaufrufe, Beacon-Nachrichten und Löschereignisse im Ring.
MAC			■	Der gesamte Datenverkehr der MAC-Schicht eines Segments-Pakets, Byte der Pakete, Beacon-Nachrichten der MAC-Schicht, verschiedene normale Fehler, die Anzahl Ringaufrufe usw.
Multicast	■	■		Die Gesamtanzahl fehlerfreier Pakete, die an die Adresse mit Unterstützung für selektives Rundsenden gesendet wurden (einschließlich Rundsendepakete).
Packets	■	■	■	Die Gesamtzahl der im Netzwerk festgestellten Pakete (einschließlich Fehlerpakete).
Source Routing			■	Ringnummer, ein-, aus- und durchgehende Rahmen und Oktette, alle Rundsendebetriebe über (einen) Leitweg und Oktette, lokale LLC- und Hop-Rahmen.

b. Anleitungen zum Erstellen Ihrer eigenen Anzeige finden Sie in „Anzeigen erstellen und editieren“ auf Seite 80.

Angenommen, Sie hätten ständig wiederkehrende Probleme mit kurzen Paketen, die auf einem Ethernet-Segment von Datei-Servern auf Produktionsebene generiert werden. Anstatt nun immer wieder dieselbe Anzeige für die

Analyse dieser speziellen statistischen Daten zu definieren, könnten Sie eine Anzeige erstellen.

Geben Sie in das Feld *View Name* den Namen `short stats` ein. Wählen Sie anschließend die Variablen `Short+CRC` und `Too Short` aus. Klicken Sie **OK** an, um die neue Anzeige zu erstellen und auszuwählen.

5. Geben Sie die Aktualisierungsrate in Schritten von 10 Sekunden in das Feld *Update Rate* ein. Damit legen Sie fest, in welchen Intervallen die Anzeige mit neuen Daten aktualisiert wird. Eine 1 steht für 10 Sekunden, 2 für 20 Sekunden und so weiter.
6. Im Bereich **Community String** zeigt Nways Remote Monitor die Zeichenfolge für die Benutzergemeinschaft an, die der ausgewählten Sonde zugeordnet ist. Dies wird im Detail in „Zugriffssteuerungstabellen“ auf Seite 32 beschrieben.
7. Klicken Sie **OK** an, um Statistics zu starten.

Protokollanzeige (History View)

Mit History wird Statistics vervollständigt. Mit History können Sie die statistischen Daten eines breiteren Bereichs erfassen und Trends über Stunden, Tage, Wochen und sogar Monate verfolgen. Wenn Sie Intervalle wie „alle 30 Sekunden“ oder „einmal in der Stunde“ angeben, können Sie die Netzwerkaktivität über einen längeren Zeitraum beobachten. Wenn Sie ungewöhnliche Spitzen oder Einbrüche in der Netzwerkaktivität in der Protokollanzeige feststellen, brauchen Sie den betreffenden Teil des Liniendiagramms nur anzuklicken, um den Zeitpunkt dieses Ereignisses festzustellen.

"History View" konfigurieren

1. Starten Sie den Dialog **History View** wie in „RMON-Anwendungen starten“ auf Seite 78 beschrieben.

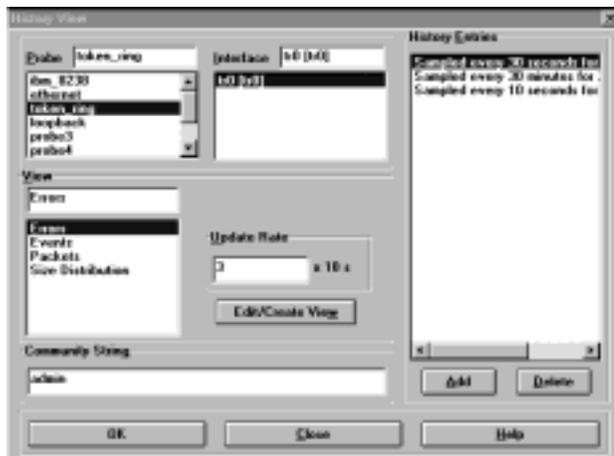


Abbildung 51. Dialog "History View"

2. Klicken Sie in der Liste **Probe** die Sonde an, deren Protokolldaten Sie analysieren wollen. Wenn die Sonde verfügbar ist, werden in der Liste **Interface** die Schnittstellen der Sonde angezeigt.
3. Klicken Sie den Namen einer Schnittstelle in der Liste *Interface* an, um auf die Daten in einem der LAN-Segmente zuzugreifen, die von der Sonde überwacht werden.
4. Wählen Sie im Bereich *View* eine der vordefinierten oder eine der von Ihnen definierten Anzeigen aus.
 - a. Die Liste der vordefinierten Anzeigen ändert sich in Abhängigkeit vom Datenträgertyp der ausgewählten Schnittstelle. Tabelle 15 beschreibt die für Ethernet und FDDI verfügbaren Protokollanzeigen.

Tabelle 15. Vordefinierte Protokollanzeigen

Anzeige	Daten-trägertyp	Beschrei-bung	Ethernet	FDDI
All	■	■		Enthält alle für den Datenträgertyp relevanten Variablen.
Bytes	■	■		Die Anzahl Byte, aus denen die Pakete bestehen (d. h. alle Byte, die in diesem Segment versendet wurden).
Errors	■	■	■	Die Anzahl der im Segment festgestellten Fehler.
Events			■	Freigabeereignisse, Beacon-Ereignisse, Bestätigungs-Token-Ereignisse und Ringaufrufe.
Load	■	■		Der Prozentsatz der Netzwerkauslastung im Berichtszeitraum.
Multicast	■	■		Die Gesamtanzahl fehlerfreier Pakete, die an die Adresse mit Unterstützung für selektives Rundsenden gesendet wurden (einschließlich Rundsendepakete).
Packets	■	■	■	Die Gesamtzahl der im Netzwerk festgestellten Pakete (einschließlich Fehlerpakete).
Size Distribution		■	■	Pakete, die nach ihrer Größe in verschiedene Kategorien eingeordnet werden.

- b. Anleitungen zum Erstellen Ihrer eigenen Anzeige finden Sie in „Anzeigen erstellen und editieren“ auf Seite 80.
5. Geben Sie im Bereich *Update Rate* an, wie oft die Anzeigen aktualisiert werden. Damit legen Sie fest, in welchen Intervallen die Anzeige mit neuen Daten aktualisiert wird. Der Standardwert wird von dem ausgewählten Protokoll übernommen.

6. Wählen Sie das gewünschte Stichprobenintervall aus der Liste *History Entries* durch Anklicken aus.
7. Klicken Sie **Add** an, um ein neues Stichprobenintervall zu erstellen, wenn das gewünschte Intervall noch nicht in der Liste *History Entries* angezeigt wird. Der Dialog **History Entry Creation** wird geöffnet.

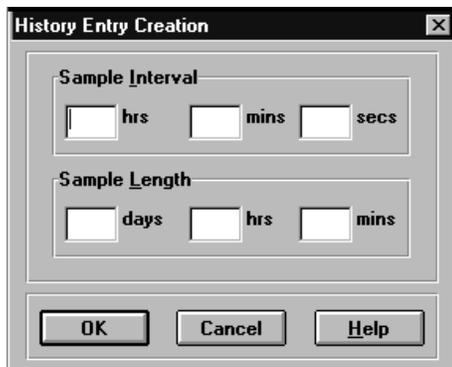


Abbildung 52. Dialog "History Entry Creation"

- a. Geben Sie in den Feldern *Sample Interval* an, wie oft statistische Daten im Segment erfaßt werden sollen.
 Wenn Sie das Intervall „einmal pro Stunde“ angeben, steht jeder Punkt des Diagramms für Ereignisse, die in stündlichen Intervallen eingetreten sind. Das heißt, obwohl zwei Ereignisse im Diagramm unmittelbar aufeinander folgen, liegt tatsächlich doch eine zeitliche Verzögerung von einer Stunde dazwischen.
- b. In den Feldern *Sample Length* geben Sie die Dauer der Stichprobenentnahme an.
- c. Klicken Sie **OK** an, um den neuen Eintrag zu speichern.

*Wenn Sie sehr viele Stichproben angegeben haben, werden Sie unter Umständen von Nways Remote Monitor gewarnt, daß die Sonde diesen Eintrag nicht bearbeiten kann, da ihr keine ausreichenden Ressourcen zur Verfügung stehen. Löschen Sie in diesem Fall eine alte Stichprobe, die Sie nicht länger brauchen, aus der Liste **History Entries**.*

8. Im Bereich *Community String* zeigt Nways Remote Monitor die Zeichenfolge für die Benutzergemeinschaft an, die der ausgewählten Sonde zugeordnet ist. Dies wird im Detail in „Zugriffssteuerungstabellen“ auf Seite 32 beschrieben.
9. Klicken Sie **OK** an, um History zu starten.

Host-Anzeige (Host View)

Beim Netzwerkmanagement und der Fehlerbehebung muß ein Manager oft viel Zeit darauf verwenden herauszufinden, welche Beziehung zwischen einzelnen Ereignissen besteht. So sind Sie sich z. B. ziemlich sicher, daß mit der Erhöhung der Rundsende-rate eines Segments auch die Fehlerzahl auf dem Router ansteigt. Es ist jedoch oft sehr schwer, die für diese Theorie erforderlichen Beweise zu erbringen.

Host wurde entwickelt, um Ihnen dabei zu helfen, auf die entsprechenden Informationen zuzugreifen, um genau diesen Problemen auf die Spur zu kommen. Die Informationen werden von den Gruppen **Host** und **Host Top N RMON** dargestellt.

Je nachdem, welche Nachforschungsmethode Sie bevorzugen, können die Ergebnisse unterschiedlich sortiert werden, so daß die herausragenden Informationen gleich hervorgehoben werden:

- Nach der Einfügezeit (Insertion Time)
- Nach der ausgewählten Rate (Selected Rate)
- Nach den ausgewählten Stationen (Selected Stations)

Wurde auf der ausgewählten Sonde PACMIB aktiviert, können Sie auch statistische Daten zu Anschlüssen und Steckplätzen sammeln. Siehe „PACMIB aktivieren und inaktivieren“ auf Seite 37.

"Host View" konfigurieren

1. Starten Sie den Dialog **Host View** wie in „RMON-Anwendungen starten“ auf Seite 78 beschrieben.

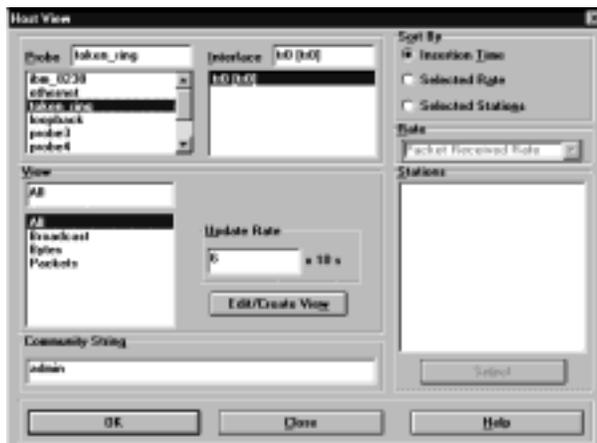


Abbildung 53. Dialog "Host View"

2. Klicken Sie in der Liste **Probe** die Sonde an, deren statistische Daten Sie analysieren wollen. Wenn die Sonde verfügbar ist, werden in der Liste **Interface** die Schnittstellen der Sonde angezeigt.
3. Klicken Sie den Namen einer Schnittstelle in der Liste *Interface* an, um auf die Daten in einem der LAN-Segmente zuzugreifen, die von der Sonde überwacht werden.
4. Wählen Sie im Bereich *View* eine der vordefinierten oder eine der von Ihnen definierten Anzeigen aus.
 - a. Die Liste der vordefinierten Anzeigen ändert sich in Abhängigkeit vom Datenträgertyp der ausgewählten Schnittstelle. Tabelle 16 beschreibt die für Ethernet und FDDI verfügbaren Host-Anzeigen.

Tabelle 16. Vordefinierte Host-Anzeigen

Anzeige	Daten-trägertyp	Beschrei-bung	Ethernet	FDDI
All	■	■	■	Enthält alle für den Datenträgertyp relevanten Variablen.
Broadcast			■	Die Anzahl der gezählten Rundsendebetriebe.
Bytes	■	■	■	Die Anzahl Byte, aus denen die Pakete bestehen (d. h. alle Byte, die in diesem Segment versendet wurden).
Errors	■	■		Die Anzahl der im Segment festgestellten Fehler.
Load	■	■		Der Prozentsatz der Netzwerkauslastung im Berichtszeitraum.
Packets	■	■	■	Die Gesamtzahl der im Netzwerk festgestellten Pakete (einschließlich Fehlerpakete).
Rate	■	■		Die Anzahl der Rundsendebetriebe und der Betriebe mit Unterstützung für selektives Rundsenden.

- b. Anleitungen zum Erstellen Ihrer eigenen Anzeige finden Sie in „Anzeigen erstellen und editieren“ auf Seite 80.

5. Geben Sie im Bereich *Update Rate* an, wie oft die Anzeigen aktualisiert werden. Damit legen Sie fest, in welchen Intervallen die Anzeige mit neuen Daten aktualisiert wird.
6. Je nach Ihrer Nachforschungsmethode, das heißt, abhängig von Ihrer verfolgten Theorie, können Sie die Host-Einträge unterschiedlich sortieren:
 - a. Wenn Sie nach Zeit sortieren wollen, klicken Sie **Insertion Time** an. Dies entspricht der Reihenfolge, in der die Sonde die Stationen des Netzwerks erfaßt.
 - b. Wenn Sie nach einer ausgewählten Rate sortieren wollen, klicken Sie **Selected Rate** an. Nun ist die Liste *Packet Received Rate* aktiv. Hierbei handelt es sich jedoch nur um einen Standardwert. Klicken Sie das Aktionsfenstermenü an, und wählen Sie eine der folgenden Optionen aus: **Packet Received Rate, Packet Sent Rate, Bytes Received Rate, Bytes Sent Rate, Error Packet Rate, Broadcast Packet Rate** und **Multicast Packet Rate**.
 - c. Wenn Sie nach Stationen sortieren wollen, klicken Sie **Selected Stations** an. Nun ist der Knopf *Select* aktiv, und alle derzeit ausgewählten Stationen werden in der Liste *Stations* angezeigt.

Sie können die in der Liste angezeigten Stationen ändern, indem Sie **Select** anklicken, um den Dialog **Station Select** zu öffnen.



Abbildung 54. Dialog "Station Select"

Der erste Teil des Dialogs ist ähnlich angelegt wie der Station List Editor. Die Suchfunktion definiert die Liste mit den anzuzeigenden Stationen. Sie können auch Stationseinträge hinzufügen, ändern und löschen. Diese Funktionen sind in „Stationen manuell einrichten“ auf Seite 60 beschrieben.

Im zweiten Teil des Dialogs können Sie Stationen auswählen, die in die Host-Anzeige aufgenommen werden sollen.

- Wählen Sie Einzel- oder Mehrfachstationen aus der Stationsliste aus. Klicken Sie danach **Add...** an, damit die Stationen zur Liste *Select Stations* hinzugefügt werden.
- Wenn Sie Stationen aus der Liste *Select Stations* entfernen wollen, wählen Sie mindestens eine Station aus, und klicken Sie anschließend **Delete** an.
- Klicken Sie **OK** an, um zum Dialog **Host View** zurückzukehren.

7. Im Bereich *Community String* zeigt Nways Remote Monitor die Zeichenfolge für die Benutzergemeinschaft an, die der ausgewählten Sonde zugeordnet ist. Dies wird im Detail in „Zugriffssteuerungstabellen“ auf Seite 32 beschrieben.

8. Klicken Sie **OK** an, um die Host-Tabellenanzeige zu starten.

Matrixanzeige (Matrix View)

Wenn sich ein Netzwerkmanager bis zur Wurzel eines bestimmten Problems vorgearbeitet hat, ist es unter Umständen erforderlich, eine Analyse von Station zu Station durchzuführen.

Mit Matrix können Sie folgendes prüfen:

- Wer im Netzwerk mit wem kommuniziert
- Wie hoch der Datenverkehr zwischen zwei Stationen ist
- Ob der Datenverkehr zwischen zwei Stationen fehlerfrei oder fehlerhaft ist

In der Regel verwenden Sie diese Anwendung, um einzelne Stationen zu überprüfen, die unter Umständen für Fehler verantwortlich sind, die innerhalb eines bestimmten Segments auftreten.

Wenn Sie Trendänderungen an Stationen in einem Token-Ring analysieren wollen, sollten Sie **Ring Station** verwenden.

"Matrix View" konfigurieren

1. Starten Sie den Dialog **Matrix View** wie in „RMON-Anwendungen starten“ auf Seite 78 beschrieben.

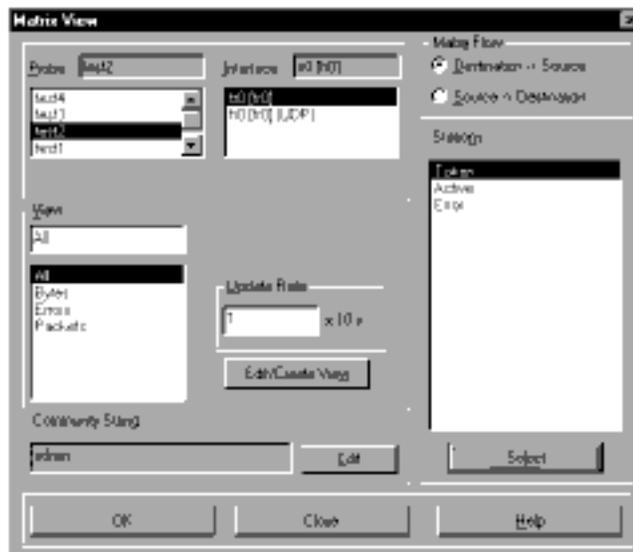


Abbildung 55. Matrix View

2. Klicken Sie in der Liste **Probe** die Sonde an, deren statistische Daten Sie analysieren wollen. Wenn die Sonde verfügbar ist, werden in der Liste **Interface** die Schnittstellen der Sonde angezeigt.
3. Klicken Sie den Namen einer Schnittstelle in der Liste *Interface* an, um auf die Daten in einem der LAN-Segmente zuzugreifen, die von der Sonde überwacht werden.
4. Wählen Sie im Bereich *View* eine der vordefinierten oder eine der von Ihnen definierten Anzeigen aus.
 - a. Die Liste der vordefinierten Anzeigen ändert sich in Abhängigkeit vom Datenträgertyp der ausgewählten Schnittstelle. Tabelle 17 beschreibt die für Ethernet und FDDI verfügbaren Matrixanzeigen.

Tabelle 17. Vordefinierte Matrixanzeigen

Anzeige	Daten-trägertyp	Beschrei-bung	Ethernet	FDDI
All	■	■	■	Enthält alle für den Datenträgertyp relevanten Variablen.
Bytes	■	■	■	Die Anzahl Byte, aus denen die Pakete bestehen (d. h. alle Byte, die auf diesem Segment versendet wurden).
Errors	■	■	■	Die Anzahl der im Segment festgestellten Fehler.
Packets	■	■	■	Die Gesamtzahl der im Netzwerk festgestellten Pakete (einschließlich Fehlerpakete).

- b. Anleitungen zum Erstellen Ihrer eigenen Anzeige finden Sie in „Anzeigen erstellen und editieren“ auf Seite 80.
5. Geben Sie im Bereich *Update Rate* an, wie oft die Anzeigen aktualisiert werden. Damit legen Sie fest, in welchen Intervallen die Anzeige mit neuen Daten aktualisiert wird.
6. Klicken Sie in der Liste **Stations** die Stationen an, die Sie überprüfen wollen.
Sie können die in der Liste angezeigten Stationen ändern, indem Sie **Select** anklicken, um den Dialog **Station Select** zu öffnen. Dieser Dialog wird in „Host-Anzeige (Host View)“ auf Seite 87 ausführlich beschrieben.
7. Im Bereich *Community String* zeigt Nways Remote Monitor die Zeichenfolge für die Benutzergemeinschaft an, die der ausgewählten Sonde zugeordnet ist. Dies wird im Detail in „Zugriffssteuerungstabellen“ auf Seite 32 beschrieben.
8. Klicken Sie **OK** an, um die Matrixanzeige zu starten.

Ringstationsanzeige (Ring Station View)

Für die effektive Verwaltung eines Token-Rings muß ein Netzwerkmanager in der Lage sein, auch die subtilsten Beziehungen zwischen scheinbar zusammenhanglosen Ereignissen im Ring zu analysieren. Bestimmte Ereignisse im Token-Ring können zu speziellen und schließlich erkennbaren Verhaltensmustern zwischen Stationen führen.

Ein ganz simples Beispiel ist es, wenn eine Station jedesmal, wenn sie sich in den Ring einfügt, eine Unterbrechung auslöst. Das wiederum führt zu einem Ringfreigabeereignis, so daß vom aktiven Monitor ein neues Token abgesetzt wird. Mit Ring Station können Sie herausfinden, wer die Unterbrechung auslöst, und wer als aktiver Monitor das neue Token absetzt.

Mit Ring Station haben Sie die folgenden Möglichkeiten:

- Sie lernen, Muster in Ihrem eigenen Token-Ring aufzuspüren.
- Sie können sich auf eingrenzbare und nicht-eingrenzbare Fehler konzentrieren.
- Sie können feststellen, wer gerade im Ring aktiv ist.

"Ring Station View" konfigurieren

1. Starten Sie den Dialog **Ring Station View** wie in „RMON-Anwendungen starten“ auf Seite 78 beschrieben.



Abbildung 56. Dialog "Ring Station View"

2. Klicken Sie in der Liste **Probe** eine Token-Ring-Sonde oder eine Sonde an, die eine Token-Ring-Schnittstelle unterstützt. Wenn die Sonde verfügbar ist, werden in der Liste **Interface** die Schnittstellen der Sonde angezeigt.
3. Klicken Sie den Namen einer Schnittstelle in der Liste **Interface** an, um auf die Daten in einem der LAN-Segmente zuzugreifen, die von der Sonde überwacht werden.
4. Wählen Sie im Bereich **View** eine der vordefinierten oder eine der von Ihnen definierten Anzeigen aus.
 - a. Tabelle 18 beschreibt die verfügbaren Token-Ring-Anzeigen.

Tabelle 18. Vordefinierte Token-Ring-Anzeigen

Anzeige	Beschreibung
All	Enthält alle Variablen.
Errors	Die Anzahl der im Segment festgestellten Fehler.
Events	Hierzu gehören die letzte bekannte NAUN (Nearest Active Upstream Neighbor), der Status der Station im Ring, der Zeitpunkt des letzten Eintritts der Station in den Ring sowie der Zeitpunkt des letzten Austritts der Station aus dem Ring.

- b. Anleitungen zum Erstellen Ihrer eigenen Anzeige finden Sie in „Anzeigen erstellen und editieren“ auf Seite 80.
 5. Geben Sie im Bereich *Update Rate* an, wie oft die Anzeigen aktualisiert werden. Damit legen Sie fest, in welchen Intervallen die Tabelle mit neuen Daten aktualisiert wird.
 6. Je nach Ihren Nachforschungsmethoden können Sie die Einträge in Ring Station unterschiedlich sortieren.
 - Wenn Sie die Stationen nach ihrer Ringreihenfolge sortieren wollen, klicken Sie *Ring Order* an. Nun werden die aktiven Stationen des Rings in der Reihenfolge ihrer physischen Verbindung zum Ring angezeigt. Die erste Station ist der aktive Monitor (Active Monitor).
 - Wenn Sie die Stationen nach ihrer Adresse sortieren wollen, klicken Sie **Address** an.
 - Wenn Sie die Stationen nach ihrem Stationsnamen sortieren wollen, klicken Sie **Selected Station** an. Nun ist der Knopf *Select* aktiv.
- Wenn eine gewünschte Station nicht in der Liste angezeigt wird, klicken Sie **Select** an, um den Dialog **Station Select** zu öffnen. Dieser Dialog wird in „Host-Anzeige (Host View)“ auf Seite 87 ausführlich beschrieben.
7. Im Bereich *Community String* zeigt Nways Remote Monitor die Zeichenfolge für die Benutzergemeinschaft an, die der ausgewählten Sonde zugeordnet ist. Dies wird im Detail in „Zugriffssteuerungstabellen“ auf Seite 32 beschrieben.
 8. Klicken Sie **OK** an, um die Token-Ring-Anzeige zu starten.

Alarmanzeige (Alarms View)

Da ein großer Teil des Netzwerkmanagement darin besteht, bestimmte Ereignisse im Netzwerk zu überwachen, ermöglicht es Ihnen Nways Remote Monitor, diese Ereignisse bereits im voraus anzugeben, um Sie dann über deren Eintreten zu informieren. Diese Ereignisse werden *Alarm* genannt.

Betrachten Sie die folgenden Beispiele:

- Der Router Ihres Netzwerks kann bis zu 3000 Pakete pro Sekunde (pps) weiterleiten.

Da er jedoch offensichtlich Probleme bekommt, wenn er bis an seine Höchstleistungsgrenze gehen muß, wollen Sie informiert werden, sobald sich der Datenverkehr der Rate von 3000 pps nähert.

- Ihr Netzwerk ist mit einer Rate von 1400 pps aktiv. In der Regel ist eine CRC-Rate (zyklische Blockprüfung) von mehr als 1% Datenaustausch auf dem Netzwerk übertrieben, so daß Sie informiert sein wollen, sobald die CRC-Rate die Grenze von 14 pps übersteigt.

Im Laufe der Zeit werden Sie Ihre eigene Alarmbibliothek mit speziellen, an Ihr Netzwerk angepaßten Alarmen erstellen.

Sie können einen Alarm nicht nur als Alarm, sondern auch als Start- oder Stoppereignis bei der Paketerfassung mit Capture verwenden (siehe „Packet Capture und Decode“ auf Seite 103). Im ersten Beispiel könnten Sie die Erfassung der übertragenen Pakete *starten*, wenn die Übertragungsrates über 2800 pps steigt, und die Erfassung wieder *stoppen*, wenn dieser Wert wieder unterschritten wird. Wenn Sie Alarms und Capture auf diese Weise miteinander kombinieren, erhalten Sie leistungsfähige Management- und Fehlerbehebungsanwendungen.

"Alarms View" konfigurieren

1. Starten Sie den Dialog **Alarms View** wie in „RMON-Anwendungen starten“ auf Seite 78 beschrieben.



Abbildung 57. Dialog "Alarms View"

2. Klicken Sie in der Liste **Probe** die Sonde an, deren statistische Daten Sie analysieren wollen. Wenn die Sonde verfügbar ist, werden in der Liste **Interface** die Schnittstellen der Sonde angezeigt.

3. Klicken Sie den Namen einer Schnittstelle in der Liste *Interface* an, um auf die Daten in einem der LAN-Segmente zuzugreifen, die von der Sonde überwacht werden.
4. Wenn Sie zum ersten Mal einen Alarm für die betreffende Sonde einstellen, oder wenn Sie alte Alarme gelöscht haben, enthält die Liste *Alarm Entries* keine Einträge.
5. Wenn Sie einen neuen Eintrag hinzufügen wollen, klicken Sie **Add...** an, um den Dialog **Alarm Creation** zu öffnen.



Abbildung 58. Dialog "Alarm Creation"

- a. Klicken Sie in der Liste *Select Alarm Rule* die Art Alarm an, die Sie aktivieren wollen. Die Liste enthält je nach Datenträgertyp der ausgewählten Schnittstelle unterschiedliche Alarmregeln.
- b. Geben Sie im Bereich *Sample Interval Configuration* an, wie oft die Anwendung eine Überprüfung auf dieses Ereignis durchführen soll.
- c. Für einige Alarme ist es erforderlich, eine weitere Objektauswahl zu treffen, um die Alarmbeschreibung zu vervollständigen. Ein Beispiel ist ein Alarm auf dem Hub eines Netzwerks, der die Anzahl der Pakete zählt, die an einem Anschluß einer bestimmten Gruppe oder an einem beliebigen Anschluß einer Gruppe gesendet werden.

Klicken Sie gegebenenfalls **More...** an, um den Dialog **Alarm Variables** zu öffnen und Werte in die entsprechenden Felder einzugeben.

- d. Wenn Sie eine stationsspezifische Alarmart ausgewählt haben, ist der Knopf *Select* aktiv. Klicken Sie diesen Knopf an, um den Dialog **Station Select** zu öffnen. Dieser Dialog wird in „Host-Anzeige (Host View)“ auf Seite 87 ausführlich beschrieben.
- e. Ändern Sie gegebenenfalls den Namen unter *Trap Configuration Community*. Weitere Informationen zu Alarmnachricht-Benutzergemeinschaften finden Sie in „Alarmnachricht-Benutzergemeinschaften“ auf Seite 34.
- f. Im Bereich *Activate The Alarm When The...* können Sie angeben, wann der Alarm ausgelöst werden soll. Die meisten Alarmarten sind auf die Frequenz oder Rate eines speziellen Ereignisses ausgerichtet, z. B. wenn die CRC-Rate auf einem Segment eine akzeptable Stufe übersteigt. Manchmal geht es auch um einen bestimmten Wert, z. B. wenn Ihr neuer Router seine erste Million Pakete weitergeleitet hat.

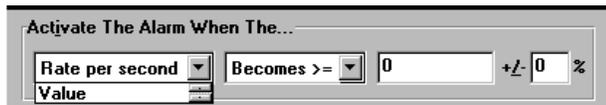


Abbildung 59. Alarmaktivierung angeben

Im Bereich *Activate The Alarm When* können Sie das Ereignis nach dem Wert der ausgewählten Variablen oder der Paketrate auswählen.

Für den Variablenwert können Sie die Bedingung angeben, unter der ausgelöst werden soll. Es gibt drei Bedingungen:

Becomes >=

Die Paketrate oder der Wert ist größer-gleich einem bestimmten Wert.

Becomes <=

Die Paketrate oder der Wert ist kleiner-gleich einem bestimmten Wert.

Crosses:

Die Paketrate oder der Wert unter- oder überschreitet den angegebenen Schwellenwert. Hier wird nur ausgelöst, wenn der Wert oder die Rate über- oder unterschritten wird, nicht wenn der Wert kleiner-gleich oder größer-gleich dem angegebenen Schwellenwert bleibt.

Um die Alarmbedingungen noch besser zu steuern, können Sie um den angegebenen Wert eine Hysterese-Zone legen. Damit erweitern Sie die Flexibilität des Auslöserwerts, indem Sie eine Prozentgrenze von plus oder minus des Werts angeben.

In Abb. 60 auf Seite 98 stellt die horizontal Linie die überwachte Alarmrate dar, die schraffierte Fläche ist die angegebene Hysterese-Zone.

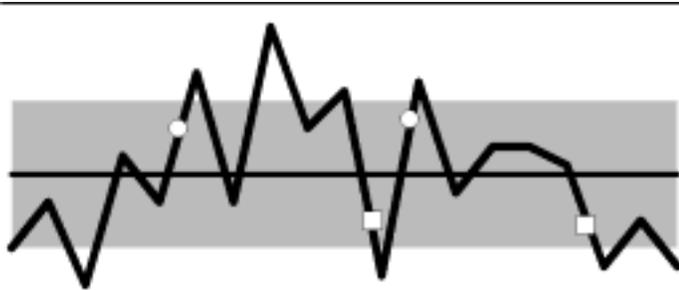


Abbildung 60. Hysterese-Zone

- Die schwarze Linie stellt die tatsächlichen Netzwerkwerte der Variableneinstellung dar. Für die oben genannten drei Bedingungen sind die folgenden Ergebnisse möglich:
- Wenn der Alarm als *Becomes >=* angegeben ist, würde das Ereignis da ausgelöst, wo im Diagramm die Kreise dargestellt sind.
- Wenn der Alarm als *Becomes <=* angegeben ist, würde das Ereignis da ausgelöst, wo im Diagramm die Quadrate dargestellt sind.
- Wenn der Alarm als *Crosses* angegeben ist, würde das Ereignis sowohl bei den Kreisen als auch bei den Quadraten im Diagramm ausgelöst.

Klicken Sie **OK** an, um den Eintrag zu speichern und zur Alarmanzeige zurückzukehren.

6. Klicken Sie **OK** im Dialog **Alarms View** an, um die neue Alarmbedingung zu speichern.

Adreßumsetzungsanzeige (Address Translation View)

Mit Address Translation kann die Sonde eine Tabelle kompilieren, in der die MAC-Adressen den Vermittlungsschichtadressen zugeordnet sind.

Die Sonde kann auch nach doppelten Vermittlungsschichtadressen im Netzwerk suchen. Damit könnte ein Netzwerkbetriebsproblem sofort erkannt werden, wenn z. B. zwei Einheiten dieselbe IP-Adresse haben.

Address Translation wird im Fenster **Rmonview** angezeigt. Sie müssen eine der folgenden Einheiten verwenden, um diese Anwendung anzuzeigen:

- Eine RMON2-fähige Einheit
- Eine RMON2-Einheit, auf der die RMON2-(ECAM)-SmartAgent-Software geladen ist

Tabellenarten in Address Translation

Die Tabellenanzeige unterscheidet sich leicht, je nach dem, ob Sie eine RMON2-fähige Einheit oder eine RMON-Einheit mit aktivierter RMON2-(ECAM)-SmartAgent-Software verwenden. Eine Beschreibung dieser Unterschiede finden Sie in Tabelle 19.

Tabelle 19. Anzeige "Address Translation"

Anzeigefunktion	RMON2-Einheit	SmartAgent-Software
Change Rate Variable	nein	ja
Last Changed Variable	ja	nein
Sorts by Duplicate Menu Option	nein	ja

Die Variable **Change Rate Variable** gibt an, welche Stationen mehrere Vermittlungsschichtadressen für eine einzige MAC-Adresse haben. Einheiten mit einer hohen Änderungsrate sind in der Regel Router und vor der MAC-Adresse mit RTR= gekennzeichnet.

Die Variable **Last Changed Variable** gibt an, wann die Sonde zuletzt eine Änderung bei der Zuordnung der Vermittlungsschichtadresse und der MAC-Adresse feststellte. Mit diesem Wert können Sie doppelte Adressen ermitteln. Wurden Adressen dupliziert, ändert sich dieser Wert ständig.

In der Spalte **Duplicate Adresses** sind Stationen aufgelistet, wo mehr als eine MAC-Adresse derselben Vermittlungsschichtadresse zugeordnet wurde. Dies gilt in der Regel als Fehler, der entstehen kann, wenn ein und dieselbe Protokolladresse an zwei Maschinen vergeben wird. Die Symptome sind meist schwer zu verfolgen und unvorhersehbar.

Gehen Sie wie folgt vor, um doppelte Adressen aufzuspüren:

- RMON2-fähige Einheiten
Wählen Sie *Sort By* im Menü **View** aus. Wählen Sie *Last Changed* aus. Die Adressen, die zuletzt geändert wurden, sind wahrscheinlich doppelt vorhanden.
- RMON-Einheit mit RMON2-(ECAM)-SmartAgent-Software
Wählen Sie *Sort By* im Menü **View** aus. Wählen Sie *Duplicates* aus. Doppelte Adressen sind mit *true* gekennzeichnet.

Adreßumsetzungstabellen anzeigen

Sie können Address Translation über das Viewman-Hauptfenster oder über Rmonview starten.

Über Viewman

- Wählen Sie im Menü *Applications* erst **RMON views...** und anschließend **Address Translation** aus. Die aktuelle Einheit, deren Schnittstelle in Viewman angezeigt wird, wird automatisch als Ausgangspunkt für Stichproben für die Anwendung ausgewählt („RMON-Anwendungen starten“ auf Seite 78).



Abbildung 61. Aktuelle Einheit in Viewman anzeigen

Über Rmonview

- Wählen Sie **New** im Menü *File* in Rmonview und anschließend **Address Translation** aus.
- Wählen Sie im Dialog **Sample Point Selection** eine Einheit und eine Schnittstelle aus.
- Wählen Sie **OK** aus, um die Daten von der Sonde abzurufen und als Tabelle im Anzeigefenster von Rmonview anzuzeigen. Sie können mehrere Tabellen gleichzeitig anzeigen.

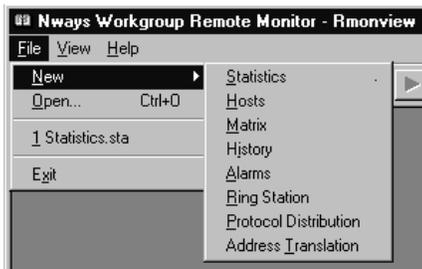


Abbildung 62. Rmonview

Protokollverteilung (Protocol Distribution) anwenden

In Protocol Distribution werden die von der ausgewählten Sonde überwachten verschiedenen Arten des Datenverkehrs im Netzwerksegment dargestellt. In Protocol Distribution haben Sie die folgenden Möglichkeiten:

- Sie können die Protokollverteilungsdaten als Tabelle, Balkendiagramm oder Kreisdiagramm anzeigen.
- Sie können den Inhalt einer Protokollverteilungstabelle als HTML-Tabelle, Excel-Datei oder Textdatei mit durch Tabulatorzeichen getrennten Spalten in eine andere Anwendung exportieren.
- Sie können den Inhalt eines Protokollverteilungsdiagramms in einer Datei oder direkt auf einem Drucker ausdrucken.

Protocol Distribution wird im Fenster **Rmonview** angezeigt. Sie müssen eine der folgenden Einheiten verwenden, um diese Anwendung anzuzeigen:

- Eine RMON2-fähige Einheit
- Eine RMON-Einheit mit geladener RMON2-(ECAM)-SmartAgent-Software

Anzeigearten in Protocol Distribution

Die Anzeige in Protocol Distribution unterscheidet sich leicht, je nach dem, ob Sie eine RMON2-fähige Einheit oder eine RMON-Einheit mit aktivierter RMON2-(ECAM)-SmartAgent-Software verwenden. Eine Beschreibung dieser Unterschiede finden Sie in Tabelle 20.

Tabelle 20. Anzeige "Protocol Distribution"

Anzeigefunktion	RMON2-Einheit	SmartAgent-Software
Set number of protocols for display	ja	nein
Sort table display by packets/bytes	ja	nein
Set Rmonview Update Rate	ja	nein
Display different views simultaneously	ja	nein

- Wenn Sie die Anzahl der anzuzeigenden Protokolle angeben wollen (nur für die grafische Anzeige), wählen Sie **TopN** im Menü *Edit* aus. Die ersten 10 Protokolle werden standardmäßig angezeigt.
- Wenn Sie eine Tabellenanzeige nach Paketen oder Byte sortieren wollen, wählen Sie **Sort by** im Menü *View* und anschließend die gewünschte Anzeigeart aus. Wenn Sie eine grafische Anzeige nach Paketen oder Byte anzeigen wollen, wählen Sie **Packets** oder **Bytes** im Menü *View* aus.
- Wenn Sie die Aktualisierungsrate für Rmonview einstellen wollen, wählen Sie **Update Rate** im Menü *Edit* aus.
- Wenn Sie unterschiedliche Anzeigen gleichzeitig anzeigen wollen, wählen Sie **New** im Menü *View* und anschließend **Table** oder **Graph** aus.
- Wenn Sie Daten exportieren wollen, wählen Sie **Export** im Menü *File* aus. Der Menüpunkt **Export** ist nur in der Tabellenanzeige aktiv.

Tabellen in Protocol Distribution anzeigen

Sie können Protocol Distribution über das Viewman-Hauptfenster oder über Rmonview starten.

Über Viewman

- Wählen Sie im Menü *Applications* erst **Rmon views...** und anschließend **Protocol Distribution** aus. Die aktuelle Einheit, deren Schnittstelle in Viewman angezeigt wird, wird automatisch als Ausgangspunkt für Stichproben für die Anwendung ausgewählt („RMON-Anwendungen starten“ auf Seite 78).



Abbildung 63. Aktuelle Einheit in Viewman anzeigen

Über Rmonview

- Wählen Sie **New** im Menü *File* in Rmonview und anschließend **Protocol Distribution** aus.
- Wählen Sie im Dialog **Sample Point Selection** eine Einheit und eine Schnittstelle aus.

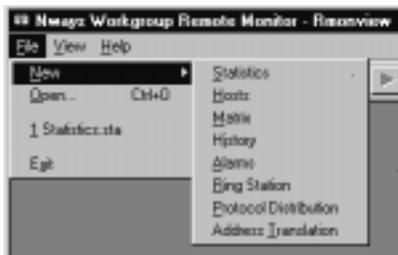


Abbildung 64. Rmonview

- Wählen Sie **OK** aus, um die Daten von der Sonde abzurufen und als Diagramm im Anzeigefenster von Rmonview anzuzeigen. Sie können mehrere Tabellen und Diagramme gleichzeitig anzeigen. Wenn Sie die Anzeige in eine Tabelle umwandeln wollen, damit Sie die Daten exportieren können, wählen Sie **New** im Menü *View* und anschließend *Table* aus.

Packet Capture und Decode

Auf der Basis des *Filter*prinzips erfaßt Capture Pakete im Netzwerk anhand von vordefinierten Mustern und Start- und Stoppbedingungen. Anschließend werden alle wichtigen Protokolle von Decode decodiert und die Paketinhalte in einem geteilten Fenster in drei Detaillierungsebenen angezeigt: Ergebnistext, Kopfdaten und tatsächlicher Paketinhalt.

Mit der einzigartigen **Conversation Trace and Analysis** können Sie ein bestimmtes Paket anklicken, so daß alle anderen an der betreffenden Übertragung beteiligten Pakete mit ihren Übertragungszeiten angezeigt werden. Damit kommen Sie schnell und einfach Verzögerungen und Übertragungsproblemen auf die Spur.

Wenn Sie Ihre Konfigurationseinstellungen in einer Datei speichern, können Sie eine Bibliothek für häufig verwendete Konfigurationen anlegen, und diese Konfigurationen für eine oder mehrere Sonden immer wieder verwenden.

In diesem Kapitel finden Sie die folgenden Abschnitte:

- Capture starten
- Capture konfigurieren
- Puffer verwenden
- Neue Start- und Stoppereignisse erstellen
- Filtereditor verwenden
- Decode starten
- Erfaßte Pakete lesen
- Conversation Trace and Analysis
- Erfaßte Pakete speichern und laden

Capture starten

Capture kann über Viewman oder unabhängig über das Menü **Start** gestartet werden.

Viewman

Wenn Sie Capture über Viewman starten wollen, klicken Sie  in der Funktionsleiste an, oder wählen Sie **Capture** im Menü **Applications** aus.



Abbildung 65. Viewman-Menüleiste und -Funktionsleiste

Menü "Start"

Wählen Sie die Programmgruppe **IBM Nways ReMon** im Menü **Start** und anschließend **Capture** aus.

Capture konfigurieren

Capture wird im Hauptdialog konfiguriert.

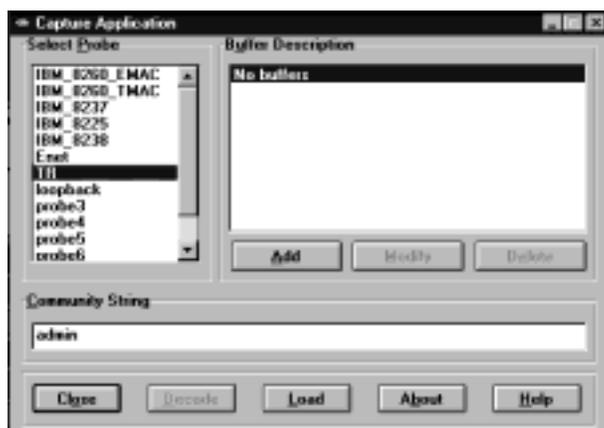


Abbildung 66. Hauptdialog "Capture Application"

1. Klicken Sie in der Liste **Select Probe** die Sonde an, die Sie für die Paketerfassung verwenden wollen.
2. Erstellen, ändern und speichern Sie die Puffer für die Erfassung, oder laden Sie bereits vorhandene Puffer aus einer Datei. Genauere Angaben finden Sie in „Puffer verwenden“.
3. Mit Packet Decode können Sie erfaßte Pakete anzeigen und den Ablauf des Paketinhalts verfolgen.

Puffer verwenden

Ein *Puffer* ist der Speicherbereich, der dem Speicher für gefilterte Pakete zugewiesen wird, wenn diese im Netzwerk erfaßt werden.

Vorhandene Puffer für die ausgewählte Sonde sind im Bereich *Buffer Description* des Hauptdialogs aufgelistet. In diesem Bereich werden die Namen aller vordefinierten, für die Sonde aktiven Erfassungsbedingungen mit ihren jeweiligen Eigentümern angezeigt.

Darüber hinaus können Sie **Buffer Description** die folgenden Informationen entnehmen:

- Slice Size** Zeigt die Größe des zugewiesenen Speicherbereichs eines jeden erfaßten Pakets, gefolgt von der Gesamtpuffergröße.
- Buffer Space** Sie können erkennen, ob der Puffer noch verfügbaren Speicherbereich für weitere Pakete hat oder ob er voll ist. Ist noch Platz vorhanden, steht am Ende der Pufferbeschreibung das Symbol (S), ist er voll, wird das Symbol (F) angezeigt.

Die Sonde hat nur begrenzte Ressourcen für die Aufnahme von Pufferdaten. Wenn ein Puffer alle Ressourcen der Sonde verbraucht, müssen die anderen Puffer die Paketerfassung beenden. Wie in 7 auf Seite 108 beschrieben, können Sie Pakete aufteilen oder den Puffern maximale Größen zuordnen, um Ressourcen zu sparen.

Neue Puffer für Capture erstellen

Neue Erfassungspuffer erstellen Sie im Fenster **Edit Packet Capture**.

1. Klicken Sie im Hauptdialog *Add* an, um das Fenster **Edit Packet Capture** zu öffnen.

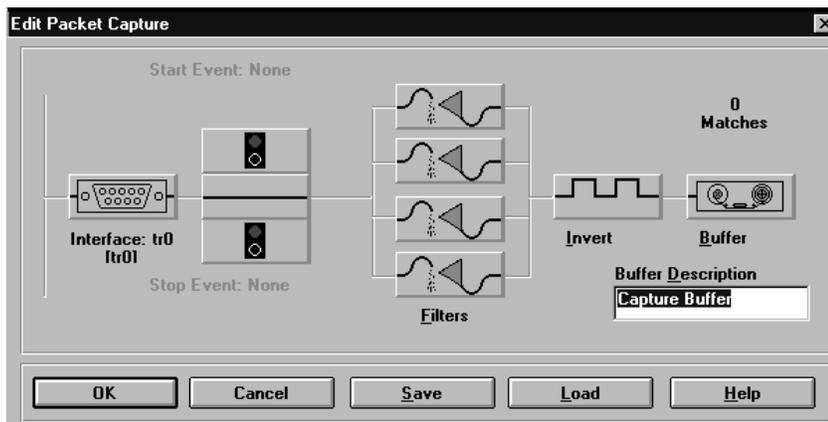


Abbildung 67. Dialog "Edit Packet Capture"

2. Klicken Sie  an, um den Dialog **Configure Interface** zu öffnen. Verwenden Sie diesen Dialog, um die Schnittstelle auszuwählen, die für die Paketerfassung verwendet werden soll.

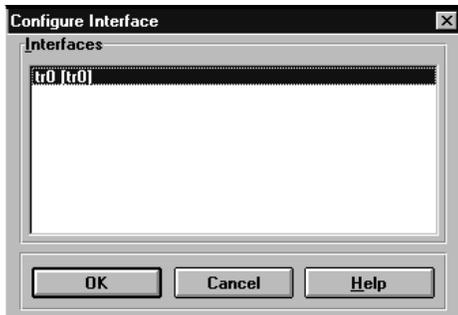


Abbildung 68. Dialog "Configure Interface"

- a. Klicken Sie die zu verwendende Schnittstelle an.
 - b. Klicken Sie **OK** an, um zum Dialog **Edit Packet Capture** zurückzukehren.
3. Unter Umständen ist es sinnvoll, die Paketerfassung automatisch zu starten, wenn ein bestimmtes Alarmereignis eintritt (weitere Informationen siehe „Alarmanzeige (Alarms View)“ auf Seite 94), oder wenn ein Paket einem bestimmten Muster entspricht. Ein solches Ereignis nennt man *Auslöser*.
- a. Klicken Sie das Symbol zum Starten eines Ereignisses () an, um eine Liste mit den verfügbaren Alarmen und Ereignissen aufzurufen. Der Dialog **Start Events** wird angezeigt.



Abbildung 69. Dialog "Start Events"

- b. Wenn Sie einen Alarm oder ein vorhandenes Ereignis verwenden wollen, klicken Sie dieses einfach an, um es auszuwählen, und klicken Sie anschließend **OK** an.
- c. Wenn Sie einen neuen Auslöser hinzufügen wollen, klicken Sie **Add** an. Weitere Informationen finden Sie in „Neue Start- und Stoppereignisse erstellen“ auf Seite 110.

- d. Wenn Sie das Startereignis aktivieren wollen, klicken Sie den *Aktivierungsschalter* () an. Der Schalter verändert sich, und zeigt damit an, daß der Startauslöser nun aktiv ist.

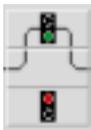


Abbildung 70. "Start Event" aktiv

4. Umgekehrt kann es auch sein, daß Sie unter bestimmten Netzwerkbedingungen die Paketerfassung stoppen wollen. Damit können Sie prüfen, was in Ihrem Netzwerk vorgefallen ist, bevor das Ereignis eintrat.
- a. Klicken Sie das Symbol zum Stoppen eines Ereignisses () an, um eine Liste mit den verfügbaren Alarmen und Ereignissen aufzurufen. Der Dialog **Stop Events** wird angezeigt.
- b. Befolgen Sie die in Schritt 3 auf Seite 106 genannten Anweisungen, um einen Alarm oder ein Ereignis auszuwählen oder ein neues Stoppereignis zu erstellen. Klicken Sie anschließend **OK** an, um zum Dialog **Edit Packet Capture** zurückzukehren.
- c. Wenn Sie nur dieses Stoppereignis aktivieren wollen, klicken Sie den *Aktivierungsschalter* () an, bis nur noch das Stoppereignis aktiv ist.



Abbildung 71. "Stop Event" aktiv

- d. Wollen Sie sowohl das Start- als auch das Stoppereignis aktivieren, klicken Sie den *Aktivierungsschalter* () an, bis beide Ereignisse als aktiv angezeigt werden.



Abbildung 72. "Start Event" und "Stop Event" aktiv

5. Klicken Sie einen der Knöpfe *Filters* () an, um anzugeben, welcher Pakettyp überwacht werden soll. Genauere Angaben finden Sie in „Filtereditor verwenden“ auf Seite 112.
6. Der Knopf *Invert* () ermöglicht die Umkehrung der ausgewählten Logik. Wenn Sie zum Beispiel derzeit alle TCP-Pakete erfassen, brauchen Sie nur diesen Knopf anzuklicken, und schon werden alle anderen Pakete mit Ausnahme der TCP-Pakete erfaßt.

Tabelle 21. Knopf "Invert"

Knopf "Invert"	Beschreibung
	Erfaßt die angegebenen Pakete.
	Erfaßt alle Pakete, nur nicht die angegebenen.

7. Klicken Sie  an, um anzugeben, wie sich der Puffer beim Speichern der Pakete verhalten soll. Der Dialog **Buffer Control** wird angezeigt.



Abbildung 73. Dialog "Buffer Control"

Verwenden Sie die Felder im Dialog **Buffer Control**, um anzugeben, wie die Pakete auf der Sonde gespeichert werden sollen.

Wrap When Full Bedeutet, daß die Pakete kontinuierlich erfaßt werden, wobei alte Pakete gelöscht werden, wenn der Puffer voll ist.

Lock When Full Bedeutet, daß die Erfassung gestoppt wird, wenn der Puffer voll ist.

- Slice Size** Gibt an, welcher Paketanteil erfaßt werden soll. Je nach dem, wieviele Informationen Sie sammeln wollen, sollten Sie diese Angabe so gering wie möglich halten. Je größer die Sektorgröße, desto schneller wird der Puffer voll.
- Buffer Size** Hier können Sie die Größe des Erfassungspuffers in Byte angeben. Wenn die Sonde soviel Speicher wie möglich zuordnen soll, geben Sie den Wert -1 an. Danach wird der Puffer in der Liste **Buffer Description** als Bedarfspuffer (ON DEMAND) angegeben.

8. Klicken Sie **OK** an, um zum Dialog **Edit Packet Capture** zurückzukehren.
9. Geben Sie in das Feld **Buffer Description** einen Namen für Ihre Erfassungskonfiguration ein. Wenn Sie z. B. eine Konfiguration für die Erfassung von TCP/IP-Paketen eingerichtet haben, könnten Sie diese **TCP-Puffer** nennen.
10. Sie können diese Erfassungspuffer in einer Datei speichern und diese nach Bedarf für andere Sonden wieder laden und verwenden. Klicken Sie **Save** an, um den Dialog **Save As** zu öffnen. Geben Sie einen Dateinamen ein, und klicken Sie anschließend **Save** an, um den Erfassungspuffer zu speichern und zum Dialog **Edit Packet Capture** zurückzukehren.
11. Klicken Sie **OK** an, um den neuen Erfassungspuffer zur Liste **Buffer Description** des Hauptdialogs hinzuzufügen.

Erfassungspuffer ändern

Sie können vorhandene Erfassungspuffer jederzeit ändern, um diese an Ihre Erfordernisse anzupassen.

Gehen Sie wie folgt vor, um einen Erfassungspuffer zu ändern:

1. Klicken Sie einen Puffer in der Liste *Buffer Description* an, um diesen auszuwählen.
2. Klicken Sie **Modify** im Bereich *Buffer Description* an, um den Dialog **Edit Packet Capture** zu öffnen.
3. Befolgen Sie die in „Neue Puffer für Capture erstellen“ auf Seite 105 beschriebenen Anweisungen zum Ändern und Speichern der Erfassungskonfiguration.
4. Klicken Sie **OK** im Dialog **Edit Packet Capture** an, um Ihre Änderungen zu speichern.

Erfassungspuffer aus einer Datei laden

Wenn Sie bereits einen Erfassungspuffer in einer Datei gespeichert haben, können Sie diesen zu einem späteren Zeitpunkt für jede beliebige Sonde laden. Sie können auch virtuelle Schnittstellenfilter laden (siehe „Virtuelle Schnittstellen konfigurieren“ auf Seite 39). Der Datenträgertyp der ausgewählten Schnittstelle der Zielsonde muß mit dem Datenträgertyp der Originalschnittstelle, auf der der Puffer oder Filter erstellt wurde, identisch sein.

Gehen Sie wie folgt vor, um einen Puffer oder Filter aus einer Datei zu laden:

1. Wählen Sie im Capture-Hauptdialog aus der Liste *Select Probe* eine Sonde aus.
2. Klicken Sie **Add** an, um den Dialog **Edit Packet Capture** zu öffnen.
3. Klicken Sie **Load** an, um den Dialog **Open** zu öffnen.
4. Wählen Sie die Datei mit dem Erfassungspuffer oder den virtuellen Schnittstellenfilter aus, der geladen werden soll, und klicken Sie **Open** an. Der Datenträgertyp des ausgewählten Puffers oder Filters muß mit dem Datenträgertyp der ausgewählten Schnittstelle der Zielsonde identisch sein.

Die vordefinierten virtuellen Schnittstellenfilter sind im Unterverzeichnis vi_chans gespeichert. Die verschiedenen Datenträgertypen sind mit ihrer Dateierweiterung gekennzeichnet: .eth für Ethernet und Fast Ethernet, .fdd für FDDI und .tok für Token-Ring.

5. Der ausgewählte Erfassungspuffer wird geladen. Anschließend kehren Sie zum Dialog **Edit Packet Capture** zurück. Wenn Sie noch Änderungen an den Puffereinstellungen vornehmen und speichern wollen, befolgen Sie die Anweisungen in „Neue Puffer für Capture erstellen“ auf Seite 105.
6. Klicken Sie **OK** an, um den Erfassungspuffer auf der ausgewählten Sonde zu erstellen, und zum Capture-Hauptdialog zurückzukehren.

Neue Start- und Stoppereignisse erstellen

Vermutlich wollen Sie beim Eintritt bestimmter Netzwerkbedingungen die Paketerfassung starten oder stoppen. Ein solches Ereignis nennt man *Auslöser*.

Gehen Sie wie folgt vor, um einen Auslöser zu erstellen:

1. Klicken Sie im Dialog **Edit Packet Capture** das Symbol zum Starten eines Ereignisses () oder zum Stoppen eines Ereignisses () an, um eine Liste mit den verfügbaren Alarmen und Ereignissen aufzurufen.
2. Klicken Sie **Add** an, um den Dialog **Edit Start Event** bzw. den Dialog **Edit Stop Event** aufzurufen.

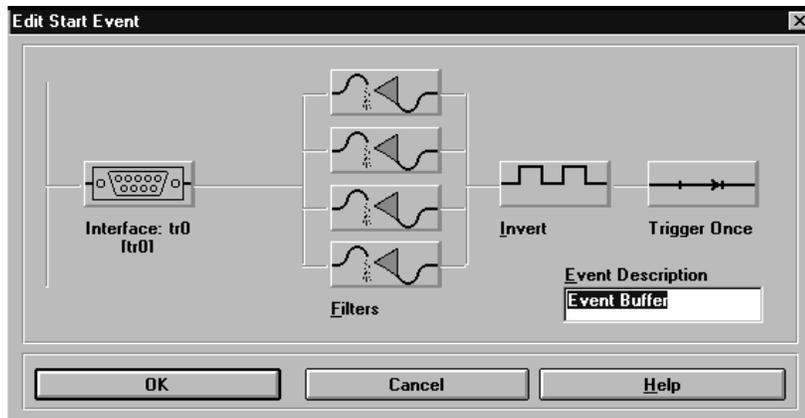


Abbildung 74. Dialog "Edit Start Event"

Verwenden Sie diesen Dialog, um neue Erfassungskriterien zu erstellen und unter einem eigenen Ereignisnamen zu speichern. Wenn Sie Ereignisse auf diese Weise verwenden, können Sie in Ihrer Konfiguration genauere Auslöserbedingungen angeben, als es nur mit Alarmen möglich wäre.

3. Klicken Sie  an, um den Dialog **Configure Interface** (Abb. 68 auf Seite 106) zu öffnen und die Schnittstelle der Sonde anzugeben, die Sie verwenden wollen.

Dabei muß es sich nicht unbedingt um dieselbe Schnittstelle handeln wie die, auf der Sie die Erfassung durchführen wollen — Sie können also auf einer Schnittstelle nach einem bestimmten Paket oder Pakettyp suchen und dann die Erfassung auf einer anderen starten.

4. Klicken Sie einen der Knöpfe *Filters* () an, um anzugeben, welcher Pakettyp überwacht werden soll. Eine genaue Beschreibung finden Sie in „Filtereditor verwenden“ auf Seite 112 später in diesem Kapitel.
5. Klicken Sie gegebenenfalls  an, um die Logik der ursprünglichen Operation umzukehren. Genauere Angaben finden Sie in „Neue Puffer für Capture erstellen“ auf Seite 105.
6. Der Auslöserknopf () ist in der Standardeinstellung auf ein einmaliges Auslösen gestellt. Wenn Sie jedesmal auslösen wollen, wenn ein Paket die vorgegebenen Bedingungen erfüllt, klicken Sie den Kopf an, bis der Status „mehrmals auslösen“ () erreicht ist.
7. Geben Sie einen eindeutigen Namen für dieses Ereignis in das Feld **Event Description** ein.
8. Klicken Sie **OK** an, um das neue Ereignis zu speichern. Es gehört nun zu Ihrer eigenen Ereignisbibliothek.

Filtereditor verwenden

Nways Remote Monitors Capture wird zusammen mit einer ganzen Reihe vordefinierter und einsatzbereiter Protokollschablonen ausgeliefert. Jede dieser Schablonen ist so ausgelegt, daß Sie schnell den aus dem Netzwerk zu filternden Pakettypp angeben können. Es werden viele Protokollfamilien unterstützt. Wählen Sie die Schablone nach den zu erfassenden Paketen aus.

Mit dem Filtereditor können Sie alles erfassen oder überwachen, angefangen von einem bestimmten Pakettypp bis hin zu einem ganz speziellen Paket. Darüber hinaus können Sie bis zu vier Filter gleichzeitig einsetzen.

Gehen Sie wie folgt vor, um den Filtereditor zu verwenden:

1. Klicken Sie einen der Knöpfe *Filters* () im Dialog **Edit Packet Capture** an, um den Dialog **Edit Filter** zu öffnen.

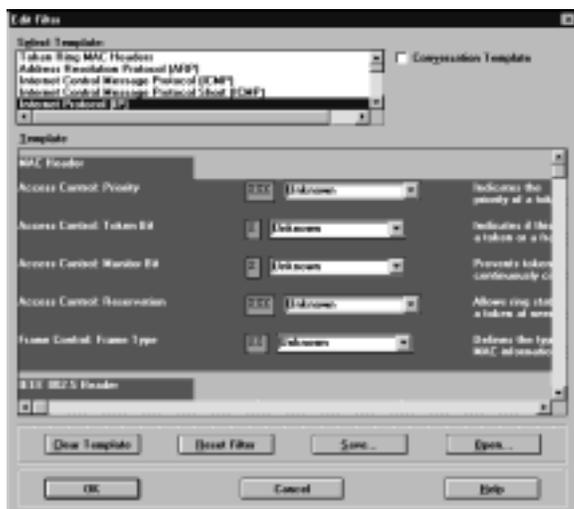


Abbildung 75. Dialog "Edit Filter"

Der Dialog **Edit Filter** enthält verschiedene Protokollschablonen, aus denen Sie wählen können. Die Liste enthält je nach Datenträgertyp der ausgewählten Schnittstelle unterschiedliche Schablonen.

Sie müssen die Felder für alle Kopfzeilenarten ausfüllen. Damit wird gewährleistet, daß Nways Remote Monitor den richtigen Pakettypp filtert. Siehe „Verfügbare Filterschablonen“ auf Seite 114.

2. Wählen Sie die gewünschte Schablone aus der Liste *Select Template* aus. Siehe „Verfügbare Filterschablonen“ auf Seite 114.

3. Die Schablonen enthalten Felder mit Quelle und Ziel für die Erfassung des Datenverkehrs von einer Adresse zur anderen auf Netzwerk- und Einheitenebene. Wenn Sie jedoch die Option *Conversation Template* in der rechten oberen Ecke des Dialogs aktivieren, wird der Datenverkehr in *beiden* Richtungen zwischen den angegebenen Punkten erfaßt.

*Wenn die Option **Conversation Template** aktiviert ist, wird die Übertragung zwischen den Quell- und Zielfeldern an jedem Punkt einer Schablone in beiden Richtungen erfaßt.*

4. Capture vereinfacht den Eingabeprozess für Quell- und Zieladressen, denn es bietet Ihnen eine Liste mit allen verfügbaren Stationen.

Klicken Sie **Destination Address** oder **Source Address** an, um den Dialog **Station Select** zu öffnen. Sie finden eine genaue Beschreibung der Schritte zum Suchen, Hinzufügen, Ändern und Auswählen in diesem Dialog in „Stationen manuell einrichten“ auf Seite 60. Wenn Sie eine Station ausgewählt haben, klicken Sie **OK** an, um zum Filtereditor zurückzukehren.

5. Klicken Sie die Dialogfenster *Any Size* oder *Any Packets* an, um allgemeine Paketvorgaben zu definieren, z. B. die Paketlänge, ob das Paket einen CRC-Fehler hat oder fehlerfrei ist. Die Bedingungen für Größe und Typ werden mit dem logischen AND verbunden.

6. Machen Sie alle erforderlichen Angaben. Die angezeigten Felder sind von Protokoll zu Protokoll unterschiedlich und haben eine Farbcodierung. Die Farben verweisen auf die Art der Werte, die in ein Feld eingegeben werden müssen. So werden zum Beispiel Binär-, Dezimal- oder Hexadezimalwerte mit den Farben grün, lachs bzw. purpurrot angegeben.

In einigen Fällen gibt es für das Feld ein Dialogfenster, in dem Sie einen vorgegebenen Wert durch Anklicken auswählen können.

Beim Ausfüllen einer Schablone können Sie das Zeichen X als Platzhalterzeichen verwenden. Stellen Sie sich vor, Sie beabsichtigen, alle von Sun®-Workstations gesendeten Pakete in Ihrem Netzwerk zu erfassen. Da Sie wissen, daß alle Produkte von Sun das Lieferantenpräfix 080020 in ihrer MAC-Adresse haben, könnten Sie den Wert 080020XXXXXX in das Feld für die Quelladresse eingeben.

7. Klicken Sie **OK** an, um den Filter zu aktivieren.

Verfügbare Filterschablonen

Tabelle 22 enthält eine nach dem Datenträgertyp der Schnittstelle sortierte Liste der verfügbaren Filterschablonen.

Tabelle 22 (Seite 1 von 2). Filterschablonen nach Datenträgertyp der Schnittstelle

Anzeige	Datenträgertyp		
	Ethernet	FDDI	Token-Ring
IEEE 802.3	■		
Ethernet LLC	■		
FDDI Header		■	
Token-Ring MAC Headers			■
Address Resolution Protocol (ARP)	■	■	■
Internet Control Message Protocol (ICMP)	■	■	■
Internet Control Message Protocol Short (ICMP)	■	■	■
Internet Protocol (IP)	■	■	■
Internet Protocol Short (IP)	■	■	■
Transport Control Protocol (TCP)	■	■	■
Transport Control Protocol Short (TCP)	■	■	■
User Datagram Protocol (UDP)	■	■	■
User Datagram Protocol Short (UDP)	■	■	■
Novell NetWare Internet Packet Exchange (IPX)	■	■	■
Novell NetWare Internet Packet Exchange 802.2 (IPX)	■	■	■
Novell NetWare Internet Packet Exchange SNAP (IPX)	■		
Novell NetWare Sequenced Packet Exchange (SPX)	■	■	■
Novell NetWare Sequenced Packet Exchange 802.2 (SPX)	■	■	■
Novell NetWare Sequenced Packet Exchange SNAP (SPX)	■		
Reverse Address Resolution Protocol (RARP)	■	■	■
Raw Data	■	■	■
Sub-Network Access Protocol (SNAP)	■	■	■
Xerox Routing Information Protocol (RIP)	■	■	■
Xerox Internet Datagram Protocol (IDP)	■	■	■
Xerox Error Protocol	■	■	■
Xerox Sequence Packet Protocol (SPP)	■	■	■

Tabelle 22 (Seite 2 von 2). Filterschablonen nach Datenträgertyp der Schnittstelle

Anzeige	Datenträgertyp		
	Ethernet	FDDI	Token-Ring
Banyan VINES Internet Protocol (IP)	■	■	■
Banyan VINES Routing Update Protocol (RTP)	■	■	■
Banyan VINES Address Resolution Protocol (ARP)	■	■	■
Banyan VINES Internet Control Protocol (ICP)	■	■	■
Banyan VINES Interprocess Communications Protocol Short (IPC)	■	■	■
Banyan VINES Interprocess Communications Protocol (ICP)	■	■	■
Banyan VINES Sequence Packet Protocol (SPP)	■	■	■
AppleTalk Address Resolution Protocol (AARP)	■	■	■
AppleTalk Short Datagram Delivery Protocol (DDP)	■	■	■
AppleTalk Long Datagram Delivery Protocol (DDP)	■	■	■
AppleTalk Transaction Protocol (ATP)	■	■	■
AppleTalk Sessions Protocol (ASP)	■	■	■
AppleTalk Filing Protocol (AFP)	■	■	■
DECnet Local Area Transport (LAT)	■	■	■
DECnet Network Services Protocol (NSP)	■	■	■
DECnet Maintenance Operations Protocol (MOP)	■	■	■
IBM Systems Network Architecture (SNA)	■	■	■
OSI End System to Intermediate System (ESIS)	■	■	■
OSI Intermediate System to Intermediate System (ISIS)	■	■	■
OSI Connectionless-Mode Network Service (CLNS)	■	■	■
OSI Transport Protocol (TP)	■	■	■

Decode starten

Sie können Decode entweder über den Capture-Hauptdialog starten, oder Sie wählen die Programmgruppe *IBM Nways Remote Monitor* im Menü **Start** und anschließend **Decode** aus.

Capture

Im Capture-Hauptdialog starten Sie Decode, um entweder den Erfassungspuffer einer Sonde oder aber den Inhalt eines gespeicherten Puffers anzuzeigen.

Den Erfassungspuffer einer Sonde anzeigen

1. Klicken Sie die Sonde in der Liste *Select Probe* an. Nun werden die Erfassungspuffer der ausgewählten Sonde in der Liste *Buffer Description* angezeigt.
2. Klicken Sie einen Erfassungspuffer an, um diesen auszuwählen.
3. Klicken Sie **Decode** an, um Decode zu starten und den Inhalt des ausgewählten Puffers anzuzeigen.

Einen gespeicherten Puffer anzeigen

1. Klicken Sie **Load** an, um Decode zu starten.
2. Nun wird automatisch der Dialog **Open** angezeigt. Verwenden Sie diesen Dialog, um nach der Datei zu suchen, die den gewünschten Puffer enthält, und diese auszuwählen.
3. Klicken Sie **Open** an, um die Datei zu öffnen.

Erfaßte Pakete lesen

Im Packet Decode-Hauptfenster können beliebig viele Erfassungspuffer gleichzeitig angezeigt werden. Abb. 76 zeigt ein Beispiel für die Anzeige eines Puffers.

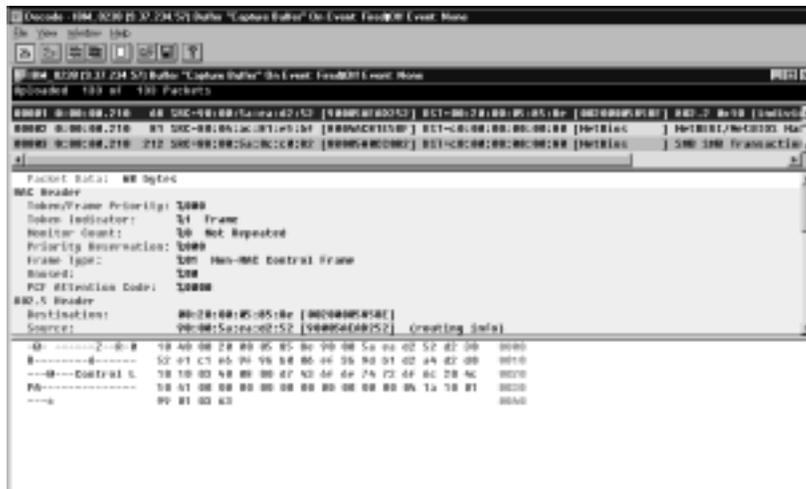


Abbildung 76. Anzeige "Packet Decode"

Die Anzeige ist dreigeteilt, so daß möglichst viele Informationen zu einem Paket angezeigt werden können.

In der oberen Anzeige können Sie das Paket auswählen, zu dem Sie genauere Informationen wünschen. Wählen Sie das Paket durch Anklicken aus.

- Die mittlere Anzeige enthält *Detailinformationen* zum ausgewählten Paket.
- In der unteren Anzeige wird das ausgewählte Paket *hexadezimal* dargestellt.

Jedes Protokoll ist mit einer Farbcodierung ausgestattet, so daß eine einfache und schnelle Identifikation möglich ist. (Eine vollständige Liste der unterstützten Decodierungen finden Sie in Anhang A, „Liste der Protokolldecodierungen“ auf Seite 151.)

Sie können die Größe der einzelnen Anzeigen verändern, um diese an Ihre Bedürfnisse anzupassen. Sie brauchen hierzu nur den unten in der jeweiligen Anzeige befindlichen Balken anzuklicken und zu ziehen.

Wenn Sie  anklicken, wird die aktuelle Anzeige gelöscht.

Sondenerfassungspuffer laden

Gehen Sie wie folgt vor, um Pakete vom Erfassungspuffer einer Sonde zu erfassen, zu laden und anzuzeigen:

1. Klicken Sie gegebenenfalls  an, um die aktuelle Anzeige zu löschen.

2.  steuert das Starten und Stoppen der Erfassung auf der Sonde.

Wenn Sie die Paketerfassung starten, *löscht* Nways Remote Monitor die vorhandenen Pufferinhalte aus der Sonde, stellt gegebenenfalls die Auslöser erneut ein und startet mit der Erfassung neuer Pakete.

3.  steuert das Laden von Paketen vom Erfassungspuffer der Sonde.

Wenn Sie das Laden von Paketen starten, *hängt* Nways Remote Monitor Pakete vom Erfassungspuffer an die in der Decode-Anzeige geladenen *vorhandenen* Pakete an. Wenn Sie die Anzeige löschen und eine vollständig neue Anzeige laden

wollen, klicken Sie erst , um die Anzeige zu löschen, und anschließend  an.

Die Anzahl der geladenen Pakete und die Gesamtzahl erfaßter Pakete im Puffer werden unterhalb der Funktionsleiste angezeigt. Sie können den Ladevorgang von mehr und mehr Paketen in die Anzeige verfolgen, indem Sie beobachten, wie sich die Schiebeleiste der oberen Anzeige während dieses Vorgangs verkürzt.

Conversation Trace and Analysis

Einige Pakete zeigen den Datenaustausch zwischen Maschinen des Netzwerks. Mit Conversation Trace and Analysis können Sie diese Anzeigen noch weiter detaillieren.

1. Klicken Sie ein Paket in der oberen Anzeige von Packet Decode an, um dieses auszuwählen.
2. Klicken Sie entweder  für den MAC-Dialog-Trace oder  (grün hervorgehoben) für den IP-Trace an. Mit diesen Trace-Funktionen können Sie einen mit Zeitmarke versehenen Trace des Datenaustauschs erstellen, der entweder auf den MAC- oder IP-Adressen der Hosts des ausgewählten Pakets basiert.

Der Datenaustausch auf IP-Schicht ist vor allem dann sinnvoll, wenn sich Ihre IP-Hosts auf unterschiedlichen Seiten eines Routers befinden und sich die MAC-Adresse des Routers auch im Paket befindet.

3. Nways Remote Monitor verwendet in diesem Fall das ausgewählte Paket als Schlüssel zu dem zu überwachenden Datenaustausch. Die an diesem Datenaustausch beteiligten Pakete werden herausgefiltert und in einer Anzeige für den Datenaustausch angezeigt.



Abbildung 77. Anzeige "Conversation Trace" für IP

In dieser Anzeige wird die Beziehung zwischen Paketen des ausgewählten Datenaustauschs hervorgehoben. Sie können daran die Gesamtform des Datenaustauschs erkennen.

Achten Sie besonders darauf, ob Pakete von einer Seite mehrmals gesendet wurden, bevor die andere Seite reagierte. Dies kann ein Zeichen für Überlastung sein. Achten Sie auch darauf, ob es längere Verzögerungszeiten gab, in denen keine Pakete gesendet wurden. Das kann bedeuten, daß eine Seite auf eine Antwort wartet, die vielleicht schon verloren ging.

Erfaßte Pakete speichern und laden

In den folgenden Abschnitten finden Sie eine Beschreibung zum Speichern und Laden von Paketen.

Pakete speichern

Gehen Sie wie folgt vor, um ein Paket zu speichern:

1. Wenn Sie die geladenen Pakete in einer Datei speichern wollen, klicken Sie



an, um den Dialog **Save As** zu öffnen.

2. Geben Sie einen Dateinamen und eine Speicherposition an.
3. Wählen Sie das Dateiformat aus, in dem Sie die Pakete speichern wollen (Tabelle 23).

Tabelle 23. Dateiformate für Packet Decode

Format	Zur Verwendung mit
IBM-Dateien (*.3co)	Packet Decode
Sniffer-Dateien (*.snf)	Network General Sniffer
Sniffer-Dateien (*.enc)	Network General Sniffer
Sniffer-Dateien (*.trc)	Network General Sniffer
DA30 Capture-Dateien (*.d30)	Wandel & Goltermann DA-30 Analyzer
ASCII (*.asc)	Für jeden beliebigen Texteditor oder Drucker

4. Klicken Sie **Save** an.

Pakete laden

Befolgen Sie die folgenden Schritte, um ein gespeichertes Paket zu laden. Sie können Packet Decode-Anwendungsdateien im Format *IBM* laden, sowie Dateien, die mit Network General Sniffer oder Wandel & Goltermann DA-30 Analyzer erstellt wurden.

1. Wenn Sie ein gespeichertes Paket laden wollen, klicken Sie  an, um den Dialog **Open** zu öffnen.
2. Suchen Sie nach der Datei, die den gewünschten Puffer enthält, und wählen Sie diese aus.
3. Klicken Sie **Open** an.

Collector

Mit Collector können Sie RMON-Protokoll-, Host- und Matrixdaten der Einheiten in Ihrem Netzwerk erfassen, diese Daten in Dateien speichern und damit Berichte über die Netzwerkaktivität erstellen.

Sie können genau angeben, welche Sonden und Schnittstellen abgefragt werden sollen, die zu protokollierenden Daten auswählen und angeben, wann und wie oft die Erfassung durchgeführt werden soll. Diese Informationen werden als *Konfiguration* bezeichnet. Es werden mehrere Konfigurationen unterstützt. Die gesammelten Daten werden in CSV-Dateien (Comma Separated Variables, durch Komma getrennte Variablen) gespeichert und können in eine Datenbank importiert und zur Berichtserstellung verwendet werden.

Collector sammelt die Protokolldaten derjenigen RMON-Sonden, deren Protokollanzeige konfiguriert wurde. Wenn für eine Sonde keine Protokollanzeige konfiguriert wurde, können für die betreffende Sonde auch keine Protokolldaten erfaßt werden.

Protokollanzeigen werden in History konfiguriert, der Zugriff erfolgt über das Nways Remote Monitor-Hauptfenster.

In Collector können Sie folgendes angeben:

- Von welchen Schnittstellen welcher Sonden Daten gesammelt werden sollen
- Welche Daten gesammelt werden sollen
- Wie oft die Daten gesammelt werden sollen
- Zu welchem Zeitpunkt die Daten gesammelt werden sollen

Die Daten werden gespeichert und können in die Reporter-Datenbank importiert werden.

In diesem Kapitel wird erläutert, wie Sie eine Datensammlung für RMON-Protokoll-, Host- und Matrixdaten der Einheiten in Ihrem Netzwerk anlegen.

Bei der Datensammlung sind die folgenden Schritte auszuführen:

- Collector starten
- Datenquellen konfigurieren
- Adreßumsetzungsebene einstellen
- Datensammlungen anlegen
- Datensammlung starten
- Collector beenden

Collector starten

Collector kann über Viewman oder unabhängig über das Menü **Start** gestartet werden.

Viewman

Wenn Sie Collector über Viewman starten wollen, klicken Sie  in der Funktionsleiste an, oder wählen Sie Capture im Menü **Applications** aus.



Abbildung 78. Viewman -Menüleiste und -Funktionsleiste

Menü "Start"

Wählen Sie die Programmgruppe *IBM Nways ReMon* im Menü **Start** und anschließend *Capture* aus.

Nun wird das Collector-Hauptfenster geöffnet.



Abbildung 79. Collector-Hauptfenster

Datenquellen konfigurieren

Wenn Collector das erste Mal ausgeführt wird, wird anhand der Datei PROBE.MAP eine Liste der RMON-fähigen Einheiten des Netzwerks generiert. Die Liste enthält den Einheitennamen sowie den Namen und die physische Nummer der einzelnen Schnittstellen der betreffenden Einheit. Gegebenenfalls können Sie weitere Netzwerkeinheiten von Collector aus hinzufügen.

Öffnen Sie das Collector-Hauptfenster, und gehen Sie wie folgt vor:

1. Wählen Sie *RMON Devices* im Menü *Config* aus, um den Dialog **Device Configuration** zu öffnen (siehe „Dialog "Device Configuration" öffnen“ auf Seite 21).

Die RMON-Einheiten, die bereits in Nways Remote Monitor konfiguriert wurden, werden in der Liste *Select Probe* angezeigt.

2. Weitere Informationen zur Konfiguration von RMON-Einheiten finden Sie in „Sonden definieren“ auf Seite 21.

Adreßumsetzungsebene einstellen

Die ausgewählte Adreßumsetzungsebene legt fest, welche Einheitenadressinformationen in den Hosttabellen und den in Reporter generierten Berichten angezeigt werden.

Standardmäßig versucht Collector, die höchstmögliche verfügbare Adreßumsetzungsebene zu erreichen. Wenn Sie vorher Translator (siehe „Sonden definieren“ auf Seite 21) ausgeführt haben, kann Collector sogar Einheitenadressen in Netzadressen oder Stationsnamen umsetzen.

Wenn Sie eine Umsetzungsebene auswählen, sucht Collector zuerst auf dieser Ebene nach einer Adresse, bevor er die restlichen Ebenen der Reihe nach durchsucht. Wenn Sie z. B. *Vendor ID* auswählen, sucht Collector erst nach dieser Ebene, und sucht erst, wenn er nichts findet, nach *MAC address*. Er sucht jedoch nicht nach *Name Translation* oder *Protocol Address*.

Dadurch kann es bei der Berichterstellung in Reporter zu einer Mischung aus Namen, Lieferanten-IDs, Protokoll- und MAC-Adressen für die ausgewählten Hosts kommen. Ein Beispiel dazu finden Sie in Abb. 80.

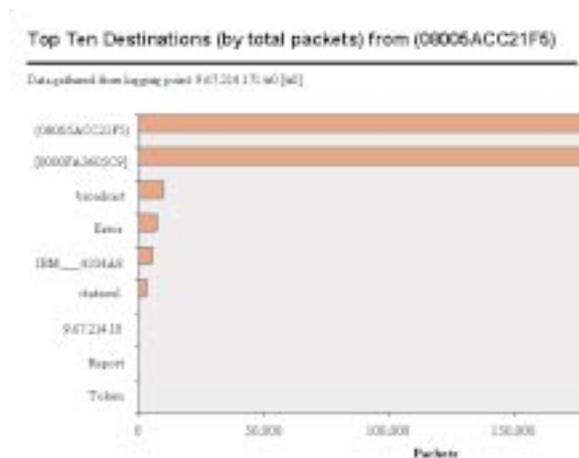


Abbildung 80. Gemischte Adreßumsetzungsebenen in Reporter

1. Wählen Sie aus dem Dialog *Device Configuration* die Option *Translation* aus, um den Dialog **Set Translation Level** zu öffnen.

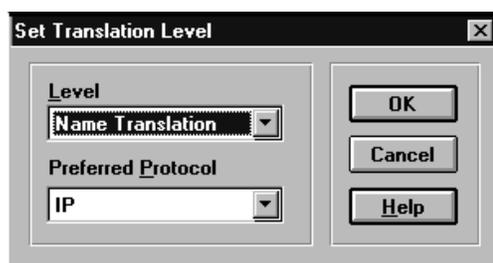


Abbildung 81. Dialog "Set Translation Level"

2. Wählen Sie eine Ebene oder ein Protokoll in den Aktionsfenstermenüs aus.
 - Es stehen die folgenden Ebenen zur Verfügung: *Name Translation*, *Protocol Address*, *Vendor ID* oder *MAC Address*. Standardmäßig wird die Ebene *Name Translation* ausgewählt.
 - Es stehen die folgenden bevorzugten Protokolle zur Verfügung: *IP*, *IPX*, *DECnet*, *AppleTalk*, *VINES* oder *SNA*. *IP* ist die Standardeinstellung.
3. Klicken Sie **OK** an, um eventuell vorgenommene Änderungen zu bestätigen.

Datensammlungen definieren

Datensammlungen werden im Dialog **Data Collection Configurations** angelegt. In einer Datensammlung wird definiert, welche Daten von welchen RMON-Einheiten zu erfassen sind. Ein Beispiel für das typische Ergebnis einer Verarbeitung der gesammelten Daten finden Sie in Anhang C, „Leistungsrichtlinien“ auf Seite 165.

Wenn Sie diesen Dialog öffnen wollen, müssen Sie *Data Collections* im Menü *Config* im Collector-Hauptfenster auswählen.

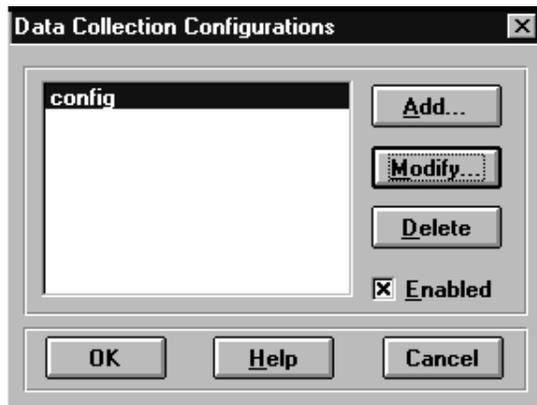


Abbildung 82. Dialog "Data Collection Configurations"

Wenn Sie diesen Dialog zum ersten Mal öffnen, ist er noch leer.

Eine neue Konfiguration hinzufügen

Gehen Sie wie folgt vor, um eine neue Konfiguration für eine Datensammlung hinzuzufügen:

1. Klicken Sie im Dialog **Data Collection Configurations** die Option **Add** an, um das Fenster **Data Collection Editor** anzuzeigen.



Abbildung 83. Dialog "Data Collection Editor"

2. Geben Sie einen eindeutigen Namen in das Feld *Collection Name* ein. Der Standardwert ist *config*.
3. Wählen Sie die Einheiten und physischen Schnittstellen aus, von denen Daten zu erfassen sind:
 - a. Wenn Sie nur eine Einheit und eine physische Schnittstelle auswählen wollen, klicken Sie den gewünschten Eintrag in den Listen *Device* und *Interface* an.
Wenn eine Einheit und eine physische Schnittstelle ausgewählt wurden, werden diese in den Feldern oberhalb der Listen *Device* und *Interface* angezeigt.
 - b. Wenn Sie mehrere Einheiten auswählen wollen, klicken Sie bei gedrückter Taste **STRG** die gewünschten Einheiten an. Wenn Sie mehrere direkt aufeinander folgende Einheiten auswählen wollen, halten Sie die **Umschalttaste** gedrückt und klicken erst die erste Einheit und anschließend die letzte Einheit an.

Bei der Auswahl mehrerer Einheiten ist das Feld **Interface** abgeblendet, und es werden automatisch *alle* Schnittstellen der betreffenden Einheiten ausgewählt. Auch die Felder oberhalb der Listen *Device* und *Interface* sind abgeblendet.

- c. Klicken Sie **Add** an, damit die Schnittstellen in der Liste *Selected Data Sources* angezeigt werden.
4. Gehen Sie wie folgt vor, um in der Liste *Selected Data Sources* ausgewählte Einträge zurückzunehmen:
 - a. Wählen Sie einen oder mehrere Einträge aus. Gehen Sie hierzu wie oben beschrieben vor.
 - b. Klicken Sie **Remove** an.

5. Im Bereich *Tables* sind standardmäßig alle Tabellen ausgewählt. Nun können Sie nach Belieben auswählen bzw. die Auswahl zurücknehmen.

Von Ihrer getroffenen Auswahl hängt es ab, welche Berichte Sie später erstellen können. Wenn Sie die Auswahl der *Protokoll-, Host- oder Matrix*tabellen zurücknehmen, werden für diese Option keine Daten erfaßt. Das heißt, die in Reporter aufgelisteten Berichte können nicht erstellt werden. (Eine Liste der Berichte, die für den jeweiligen Datentyp erstellt werden können, finden Sie in Anhang E, Berichtsbeschreibungen.)

Es werden nur Protokolldaten von denjenigen Sonden gesammelt, für die Sie vorher eine Protokollanzeige in Nways Remote Monitor definiert haben.

6. Geben Sie Datum und Zeit für die nächste Datensammlung in den Bereich *Next Collection At* ein. Der Standardwert ist das aktuelle Datum und die aktuelle Uhrzeit.
7. Für die Frequenz der Datensammlungen geben Sie die Anzahl der Tage, Stunden und Minuten in den Bereich *Log Interval* ein. Der Standardwert ist eine Stunde.
8. Die gesammelten CSV-Dateien werden im unter *Log Directory* angegebenen Protokollverzeichnis gespeichert. In der Standardeinstellung ist hierfür das Installationsverzeichnis angegeben. Wenn Sie ein anderes Verzeichnis auswählen wollen, klicken Sie **Browse...** an.

Bei jeder Datensammlung wird mindestens eine CSV-Datei gespeichert. Sie können die Ergebnisse unterschiedlicher Datensammlungen voneinander trennen, indem Sie für jede Datensammlung ein eigenes Protokollverzeichnis angeben.

9. Wenn Sie die Konfiguration speichern wollen, klicken Sie **OK** an. Daraufhin kehren Sie zum Dialog **Data Collection Configurations** zurück, in dem nun die neue Konfiguration angezeigt wird und *Enabled* ausgewählt ist. Die Datensammlung für diese Konfiguration wird jedoch erst gestartet, wenn Sie zum Hauptdialog zurückkehren.

Konfigurationen ändern

Gehen Sie wie folgt vor, um eine Erfassungskonfiguration zu ändern:

1. Wählen Sie im Dialog **Data Collection Configurations** eine Konfiguration aus.
2. Klicken Sie **Modify** an, um das Fenster **Data Collection Editor** zu öffnen.
3. Befolgen Sie zum Ändern der Konfigurationsdaten die Anweisungen in „Eine neue Konfiguration hinzufügen“ auf Seite 126.
4. Klicken Sie **OK** an, um Ihre Änderungen zu speichern und zum Dialog **Data Collection Configurations** zurückzukehren. Klicken Sie **Cancel** an, wenn Sie Ihre Änderungen wieder verwerfen wollen.

Wenn sich noch alte CSV-Dateien im ausgewählten Verzeichnis befinden, werden Sie gefragt, ob Collector diese löschen soll. Wenn sie nicht gelöscht werden, werden die geänderten Daten an diese Dateien angehängt. Nachdem eine CSV-Datei in Reporter importiert wurde, kann sie ruhig gelöscht werden.

Datensammlung stoppen

Wenn Sie die Datensammlung für eine Konfiguration stoppen wollen, können Sie diese entweder inaktivieren oder löschen.

Konfiguration inaktivieren

Gehen Sie wie folgt vor, um die Datensammlung für eine Konfiguration zu inaktivieren:

1. Wählen Sie die Konfiguration aus, für die die Datensammlung inaktiviert werden soll.
2. Nehmen Sie die Auswahl *Enabled* zurück.
3. Klicken Sie **OK** an, um die Änderung zu speichern.

Wollen Sie die Datensammlung erneut starten, können Sie jederzeit **Enabled** wieder auswählen.

Konfiguration löschen

Wenn Sie Konfigurationen löschen wollen, sollten Sie dies in den Perioden zwischen den Datensammlungen tun.

Gehen Sie wie folgt vor, um eine Konfiguration endgültig zu löschen:

1. Wählen Sie die zu löschende Konfiguration aus.
2. Klicken Sie **Delete** an.
3. Wiederholen Sie gegebenenfalls die ersten beiden Schritte.

Wenn Sie versehentlich eine Konfiguration gelöscht haben, klicken Sie sofort **Cancel** an, um den Dialog **Data Collection Configurations** zu verlassen, ohne die Änderungen zu speichern. Wenn Sie **Config** erneut auswählen, wird die Konfiguration wieder angezeigt. Es werden jedoch auch alle anderen Änderungen, die Sie am Dialog **Data Collection Configurations** vorgenommen haben, wieder zurückgenommen.

4. Klicken Sie **OK** an, um eventuell vorgenommene Änderungen zu bestätigen.

Datensammlung starten

Nachdem Sie im Dialog **Data Collection Configurations** die Option *OK* angeklickt haben und zum Hauptfenster zurückgekehrt sind, wird die nächste Datensammlung automatisch zum angegebenen Datum und Zeitpunkt gestartet.

Speicher für gesammelte Daten

Die gesammelten Daten werden in CSV-Dateien in dem Verzeichnis gespeichert, das Sie im Fenster **Data Collection Editor** angegeben haben (siehe „Eine neue Konfiguration hinzufügen“ auf Seite 126). Bei weiteren Datensammlungen werden die neuen Daten an die vorhandenen Dateien *angehängt*. Die für die verschiedenen Tabellen erstellten Dateien finden Sie in Tabelle 24.

Tabelle 24. Von Collector erstellte CSV-Dateien

Dateiname	Beschreibung	Ausgewählte Tabelle
hist.csv	Ethernet-Protokolldaten	Protokoll
host.csv	Host-Daten	Host
matrix.csv	Matrix-Daten	Matrix
trml.csv	MAC-Schichtprotokolldaten für Token-Ring	Protokoll
trp.csv	Sonstige Protokolldaten für Token-Ring	Protokoll

Eine Beschreibung der Inhalte dieser fünf CSV-Dateiformate finden Sie in „Berichte auswählen und generieren“ auf Seite 136.

Die Größe der CSV-Dateien im Verzeichnis hängt von der gesammelten Datenmenge ab. Wenn Sie häufige Datensammlungen mit großen Datenmengen von vielen Netzwerkeinheiten angegeben haben, wird die Größe der CSV-Dateien schnell ansteigen.

Anschließend können die CSV-Dateien für die Berichtserstellung in Reporter importiert werden (siehe „Berichte auswählen und generieren“ auf Seite 136).

Nachdem die Daten dieser Dateien in die Reporter-Datenbank importiert wurden, sind sie nicht mehr länger für Collector erforderlich. Deshalb ist es ratsam, diese Dateien nach dem Import in Reporter regelmäßig zu löschen. Aus Sicherheitsgründen sollten Sie vor dem Löschen der Dateien jedoch eine Sicherheitskopie anlegen oder die Dateien archivieren.

Collector beenden

In der Regel sollte Collector stets im Hintergrund aktiv sein. Wenn Sie Collector aber doch einmal beenden müssen, z. B. um einen Neustart des Systems auszuführen, wählen Sie *Exit* im Menü *File* aus. Wenn Sie Collector erneut starten, wird auch die Datensammlung erneut gestartet.

Reporter

Mit Reporter können Sie in der Berichtsdatenbank über einen beliebigen Zeitraum erfaßte Protokollberichte erstellen.

Die bei der Datensammlung von Collector erstellten Dateien werden in Reporter importiert, wo sie in einer Berichtsdatenbank gespeichert werden. Anschließend können Sie verschiedene Berichte mit diesen Daten erstellen lassen, diese sofort drucken oder in einer Datei speichern und später drucken. Sie können die Berichte auch vor dem Drucken anzeigen. Mit der Datenmanagementfunktion können Sie die Daten in der Datenbank zusammenfassen oder löschen.

Dieses Release von Reporter enthält eine Laufzeitversion der relationalen Datenbank-anwendung Microsoft Access für Windows® Version 8.0.

Wenn Sie Microsoft Access Version 8.0 besitzen und bereits Erfahrung mit diesem Produkt haben, können Sie die in Reporter enthaltenen Berichte anpassen. Genauere Anweisungen hierzu entnehmen Sie bitte Ihrem Microsoft Access Benutzerhandbuch. Es ist jedoch nicht erforderlich, Microsoft Access zu kaufen, um Reporter zu verwenden.

In Reporter können Sie folgendes angeben:

- Welche Daten in die Datenbank importiert werden sollen
- Welche Berichte erstellt werden sollen

Diese Berichte können Sie drucken oder speichern.

Zu den Hauptmerkmalen von Reporter gehören:

- Erfassung von RMON-Protokoll-, Host- und Matrix-Daten
- Unterstützung von Ethernet-, Fast Ethernet- und Token-Ring RMON-Einheiten
- Flexible Datensammlung, die Ihnen die folgenden Möglichkeiten bietet:
 - Angabe von mehreren Einheiten
 - Angabe von Einheitengruppen
 - Angabe von mehreren Schnittstellen einer einzigen Einheit
- Einfach zu konfigurierende Datensammlung
- Passive RMON-Datensammlung von Einheiten
- Unterstützung der Trendermittlung von RMON-Daten über längere Zeiträume mit Hilfe von Protokollen
- Erstellung folgender Berichte:
 - Für RMON-Protokoll-, Host- und Matrix-Daten
 - Für eine einzelne Schnittstelle einer Einheit oder für alle Protokollierungspunkte einer Datensammlung
 - Für einen oder mehrere Hosts
 - Für einen bestimmten Zeitraum

- Steuerung des Datenbankinhalts mit der Datenmanagementfunktion, während Datenbestand wächst

In diesem Kapitel finden Sie Anweisungen zum Erstellen von Berichtsdatenbanken, aus denen verschiedene Berichte generiert werden können.

Hierzu sind die folgenden Schritte erforderlich:

- Berichtsdatenbank auswählen
- Daten aus den in Collector erstellten CSV-Dateien importieren
- Datenbankinhalt anzeigen
- Berichte auswählen und generieren
- Gespeicherte Berichte laden

Reporter starten

Reporter kann über Viewman oder unabhängig über das Menü **Start** gestartet werden.

Viewman

Wenn Sie Reporter über Viewman starten wollen, klicken Sie  in der Funktionsleiste an, oder wählen Sie Reporter im Menü **Applications** aus.

Menü "Start"

Wählen Sie die Programmgruppe *IBM Nways ReMon* im Menü **Start** und anschließend **Reporter** aus.

Nun wird das Reporter-Hauptfenster geöffnet.



Abbildung 84. Reporter-Hauptfenster

Berichtsdatenbank auswählen

Bevor Sie die Daten aus den von Collector erstellten CSV-Dateien importieren können, müssen Sie angeben, welche Datenbank Reporter verwenden soll.

- Wenn Sie Reporter das erste Mal verwenden, müssen Sie eine neue Datenbank erstellen.
- Wenn Sie Reporter später wieder öffnen, wird die zuletzt verwendete Datenbank automatisch geöffnet. Der Name dieser Datenbank wird im Hauptfenster unten links unter *Current Database* angezeigt.

Eine neue Datenbank erstellen

Gehen Sie wie folgt vor, um eine neue Datenbank zu erstellen:

1. Klicken Sie im Hauptfenster **New Database** an. Damit öffnen Sie den Dialog **New Database File**.

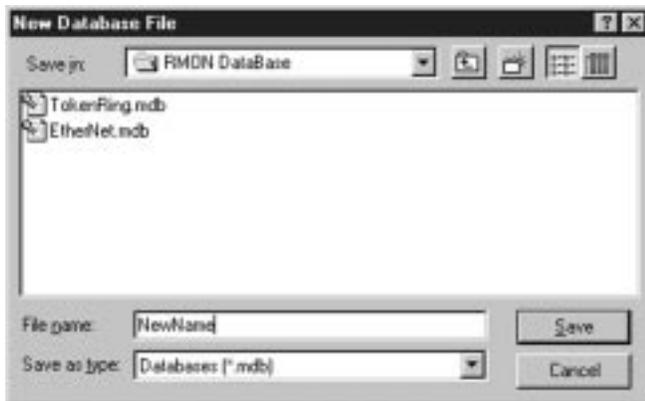


Abbildung 85. Dialog "New Database File"

2. Geben Sie den gewünschten Dateinamen ein. Das Suffix `.mdb` für den Dateityp wird automatisch hinzugefügt.
3. Klicken Sie **Save** an, um die neue Datenbank zu speichern.

Wenn Sie zum Hauptfenster zurückkehren, wird der Name der neuen Datenbank unter *Current Database* als aktuelle Datenbank angezeigt.

Eine vorhandene Datenbank öffnen

Gehen Sie wie folgt vor, um eine vorhandene Datenbank zu öffnen:

1. Klicken Sie im Hauptfenster **Open Database** an. Damit öffnen Sie den Dialog **Open Database File**, in dem alle verfügbaren `.mdb`-Dateien angezeigt werden.



Abbildung 86. Dialog "Open Database File"

2. Wählen Sie die gewünschte Datenbank aus.
3. Klicken Sie **Open** an, um die ausgewählte Datenbank zu öffnen.

Wenn Sie zum Hauptfenster zurückkehren, wird der Datenbankname unter *Current Database* als aktuelle Datenbank angezeigt.

Daten importieren

Wenn Sie zu verwendende Berichtsdatenbank ausgewählt haben, können Sie Daten aus den von Collector erstellten CSV-Dateien in die ausgewählte Datenbank importieren. Wenn Sie eine bereits vorhandene Datenbank ausgewählt haben, werden die neuen Daten an die Datenbank angehängt.

Richtlinien zur Datenbankpflege finden Sie in Anhang C, „Leistungsrichtlinien“ auf Seite 165.

Gehen Sie wie folgt vor, um Daten zu importieren:

1. Klicken Sie im Hauptfenster **Import** an. Damit öffnen Sie den Dialog **Import Files**.



Abbildung 87. Dialog "Import Files"

2. Stellen Sie fest, in welchem Collector-Verzeichnis sich die von Collector erstellten .csv-Dateien befinden.
3. Wenn Sie eine beliebige .csv-Datei in der Liste auswählen, werden *alle* verfügbaren .csv-Dateien ausgewählt.
4. Klicken Sie **OK** an, um die Dateien zu importieren, oder **Cancel**, um den Import abzubrechen. Wenn Sie **Open** anklicken, werden alle verfügbaren .csv-Dateien zur aktuellen Datenbank hinzugefügt.

Nun können Sie den Datenbankinhalt anzeigen oder anfangen, Berichte zu generieren.

Datenbankinhalt anzeigen

Sie können eine Zusammenfassung des Inhalts einer Reporter-Datenbank mit den folgenden Informationen anzeigen:

- Der von der Datenbank erfaßte Zeitraum. Das erste und letzte Datum, an dem Daten gesammelt wurden.
- Der Zustand der Daten. Ob die Daten täglich oder wöchentlich zusammengefaßt wurden oder nicht (eine Definition der Konsolidierung finden Sie in „Anwendungsdatenbank komprimieren“ auf Seite 149 und „Datenmanagement“ auf Seite 143).

Gehen Sie wie folgt vor, um eine Zusammenfassung der Daten anzuzeigen:

1. Klicken Sie im Hauptfenster **Data Summary** an, um den Dialog **Summary Data** zu öffnen.
2. Nun wird eine Zusammenfassung der Datenbankdaten angezeigt.



Abbildung 88. Dialog "Summary Data"

Abb. 88 zeigt eine Beispieldatenbank mit Daten aller Datentypen, die im Laufe eines Jahres gesammelt und zusammengefaßt wurden.

Wie im obigen Beispiel können in der Zusammenfassung in den Datenbalken Lücken auftreten. Diese können aufgrund von Änderungen in der Konfiguration der verwendeten Datensammlung oder an den Netzwerkeinheiten entstehen.

3. Klicken Sie **OK** an, um zum Hauptfenster zurückzukehren.

Berichte auswählen und generieren

Berichte zu den in der Reporter-Datenbank enthaltenen Daten werden mit Hilfe des Dialogs **Report Configuration** generiert. Wenn Sie diesen Dialog öffnen wollen, klicken Sie im Reporter-Hauptfenster **Report** an.

In diesem Dialog haben Sie die folgenden Möglichkeiten:

- Sie können auswählen, welche Berichte für alle oder bestimmte Protokollierungspunkte und Hosts generiert werden sollen.
- Sie können den Berichtszeitraum festlegen.
- Sie können eine Voranzeige des Berichts aufrufen.
- Sie können ausgewählte Berichte drucken und/oder als Datei speichern.
- Sie können Berichte im HTML-Format speichern.

Wenn Sie Berichte definieren wollen, müssen Sie den Bericht, die Protokollierungspunkte für die Ausgabe, den Berichtszeitraum und, falls zutreffend die Hosts, für die die Daten angezeigt werden sollen, auswählen.

Wenn Sie auf allen erforderlichen Seiten die entsprechenden Einstellungen vorgenommen haben, klicken Sie **OK** an, um die Berichtsgenerierung zu starten, die eingestellte Konfiguration zu sichern und den Dialog zu verlassen. Klicken Sie **Cancel** an, wenn Sie Ihre Änderungen wieder verwerfen und den Dialog verlassen wollen.

Berichte auswählen

1. Klicken Sie im Dialog **Report Configuration** die Indexzunge *Select Reports* an, um diese Seite zu öffnen.
2. Klicken Sie *All* an, um alle Berichte auszuwählen, oder wählen Sie einen oder mehrere Berichte einzeln aus.
3. Klicken Sie *None* an, um eine bereits getroffene Auswahl wieder zurückzunehmen.

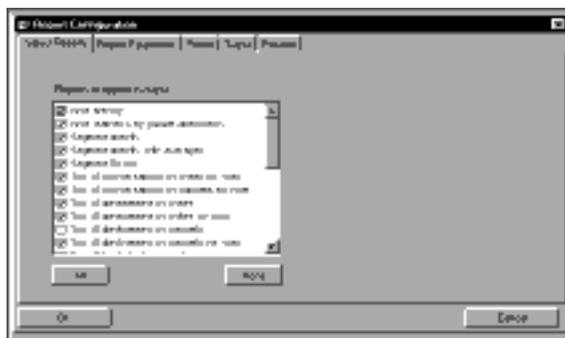


Abbildung 89. Dialog "Report Configuration"

Berichtsparameter auswählen

1. Klicken Sie im Dialog **Report Configuration** die Indexzunge *Report Parameters* an, um diese Seite zu öffnen.
2. Klicken Sie **Use same parameters for all reports** an, wenn Sie dieselben Optionen für alle Berichte verwenden wollen.
3. Vervollständigen Sie die Optionen für die einzelnen Berichte, die Sie auf der Seite **Select Reports** ausgewählt haben, und die nun in den Listenfenstern **Per Segment Reports** bzw. **Per Host Reports** angezeigt werden.
 - Für **Per Segment Reports** gilt:
 - a. Wählen Sie die Protokollierungspunkte aus dem Listenfenster **Per Segment Reports** aus.
 - b. Geben Sie, falls zutreffend, den Namen des Alarmauslösers in das Feld **Alarm Trigger** ein.
 - Für **Per Host Reports** gilt:
 - a. Wählen Sie entweder *Use all logging points* oder *Use single logging point* im Bereich **Per Host Reports** aus.
 - b. Wählen Sie die Hosts für den Bericht aus dem Listenfenster aus.

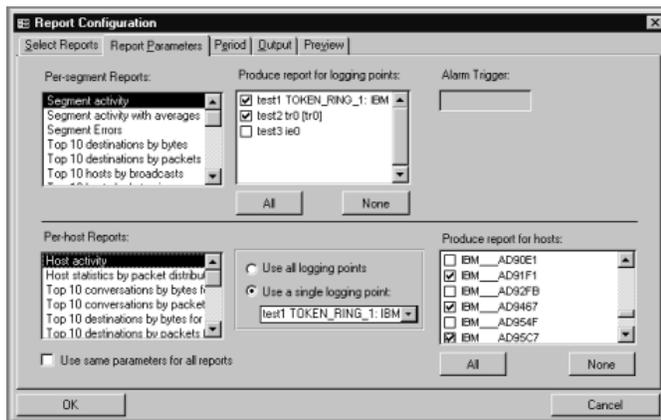


Abbildung 90. Report Configuration

Berichtszeitraum

Wenn Sie nichts anderes angeben, wird der gesamte Erfassungszeitraum der Datenbank für die Berichte verwendet.

Gehen Sie wie folgt vor, um einen Berichtszeitraum anzugeben:

1. Klicken Sie im Dialog **Report Configuration** die Indexzunge *Period* an, um diese Seite zu öffnen.

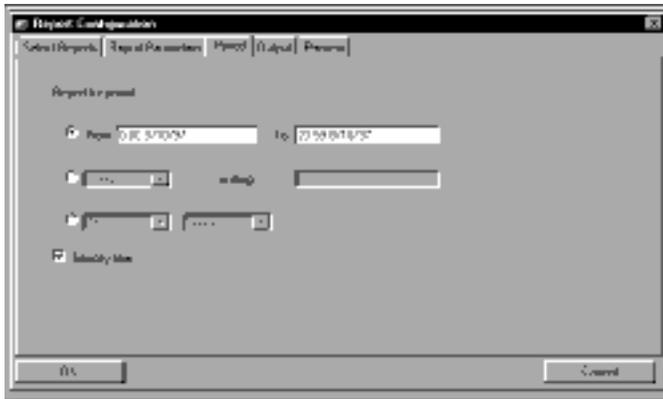


Abbildung 91. Dialog "Report Configuration"

2. Klicken Sie einen der Radioknöpfe an, um eine der folgenden drei Möglichkeiten auszuwählen:

- Ein bestimmtes Start- und Enddatum
- Den Zeitraum einer Woche, eines Monats oder eines Jahres, der an einem bestimmten Datum endet
- Einen allgemeinen Zeitraum, z. B. diese Woche oder vergangenen Monat

Wenn Sie das Markierungsfeld **Specify time** ausgewählt haben, können Sie für die ersten beiden Optionen auch eine bestimmte Zeit für das Start- und Enddatum eingeben.

3. Geben Sie den gewünschten Berichtszeitraum ein.

Berichtsausgabeoptionen auswählen

Wenn Sie die Ausgabeoptionen ändern wollen, wählen Sie die Indexzunge **Output** aus. Nun wird die zugehörige Seite angezeigt.

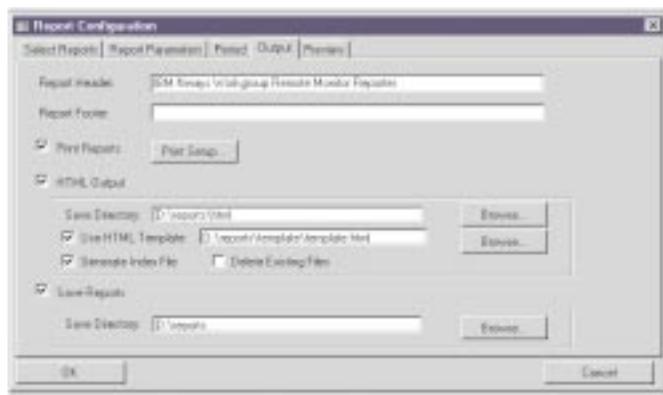


Abbildung 92. Berichtsausgabeoptionen auswählen

Kopf-/Fußzeilen:

1. Geben Sie den Text für die Kopf- bzw. Fußzeile des Berichts in die Felder **Report Header** bzw. **Report Footer** ein.

Berichte drucken:

1. Wählen Sie das Markierungsfeld *Print* aus, wenn Sie die Berichte nach dem Generieren drucken wollen.
2. Wählen Sie *Print Setup* aus, um den Dialog **System Printer Setup** zu öffnen.

Berichte speichern:

1. Wählen Sie das Markierungsfeld *Save Reports* aus, und geben Sie anschließend die Informationen zur Verzeichnisposition der gespeicherten Dateien ein. Mit dem Knopf *Browse* können Sie nach Verzeichnissen suchen. Reporter erstellt die Dateien automatisch im ausgewählten Verzeichnis und vergibt Dateinamen.

HTML-Berichte:

1. Wählen Sie das Markierungsfeld *HTML Output* aus, wenn Sie die Berichte nach dem Generieren in HTML-Dateien speichern wollen.
2. Geben Sie die Verzeichnisposition der HTML-Berichte ein. Mit dem Knopf *Browse* können Sie nach Verzeichnissen suchen. Reporter erstellt die Dateien automatisch im ausgewählten Verzeichnis und vergibt Dateinamen.
3. Wählen Sie *Use HTML Template:* aus, wenn Sie Ihre Schablonendatei für die Erstellung der HTML-Dateien verwenden wollen. Geben Sie den Namen und die Verzeichnisposition dieser Datei ein. Mit dem Knopf *Browse* können Sie nach der Datei suchen. Weitere Informationen finden Sie in Anhang F, „HTML-Berichtsschablonen anpassen“ auf Seite 179.

Speichern Sie Ihre Schablonen nicht im selben Verzeichnis wie die HTML-Berichte, weil sie sonst gelöscht werden, wenn Sie die Option **Delete Existing Files** auswählen.

4. Wählen Sie *Generate Index File* aus, wenn Sie eine Index-Seite mit HTML-Links, die auf die einzelnen Berichte verweisen, erstellen wollen.
5. Wählen Sie *Delete Existing Files* aus, wenn Sie früher erstellte HTML-Berichte überschreiben wollen.

Voranzeige

Sie haben die Möglichkeit, Berichte vor dem Drucken oder Speichern anzuzeigen. Dann können Sie die Berichte drucken oder speichern und später drucken (oder beides).

Wenn Sie im Dialog **Report Configuration** den Knopf **OK** anklicken, ohne die Optionen zum Drucken oder Speichern zu ändern, wird die zuletzt eingestellte Konfiguration angewendet.

Gehen Sie wie folgt vor, um eine Voranzeige durchzuführen:

1. Wählen Sie im Dialog **Report Configuration** die Indexzunge *Preview* aus, um diese Seite zu öffnen.

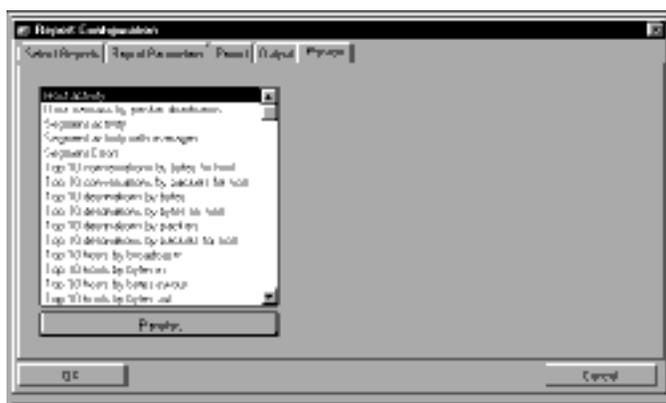


Abbildung 93. Indexzunge "Preview"

2. Wählen Sie einen der Berichte, die Sie vorher auf der Seite **Select Reports** ausgewählt haben, aus der angezeigten Liste aus.
3. Klicken Sie **Preview** an, um die Berichtsgenerierung zu starten. Der Bericht wird in der Voranzeige angezeigt.
4. Nun haben Sie die folgenden Möglichkeiten:

- **Schließen**

Klicken Sie das x in der oberen rechten Ecke des Anzeigefensters an.

- **Drucken**

Wählen Sie *File* aus der Menüleiste aus, und wählen Sie anschließend *Print* aus. Der Dialog **Page Setup** wird angezeigt. Wenn Sie **OK** anklicken, wird der Bericht gedruckt, mit **Cancel** verlassen Sie den Dialog.

- **Druckeinstellungen**

Wählen Sie *File* aus der Menüleiste aus, und wählen Sie anschließend *Print Setup* aus. Der Dialog **Page Setup** wird angezeigt. Mit diesem Dialog können Sie die Seitenränder, die Ausrichtung und die Spaltenanordnung ändern.

Wenn Sie die Ausgabeinheit ändern wollen, klicken Sie erst die Indexzunge *Page*, danach **Use Specific Printer** und anschließend **Printer** an. Klicken Sie **OK** an, um die vorgenommenen Änderungen zu speichern, oder **Cancel**, um diese wieder zu verwerfen.

Gespeicherte Berichte laden

Jeder gespeicherte Bericht kann zu einem späteren Zeitpunkt gedruckt werden. Gehen Sie wie folgt vor, um einen gespeicherten Bericht zur Ansicht oder zum Drucken erneut zu laden:

1. Klicken Sie im Hauptfenster **Open Report** an, um den Dialog **Open Report** zu öffnen.
2. Wählen Sie den Bericht aus, den Sie drucken oder anzeigen wollen, und klicken Sie **Open** an.

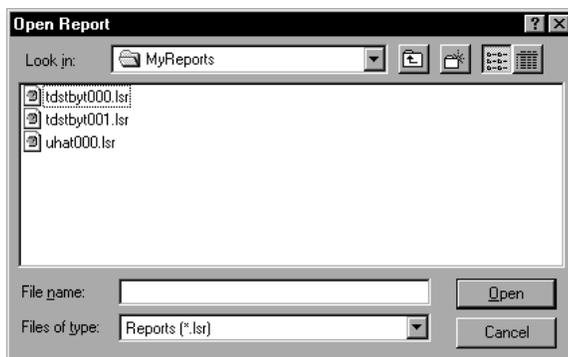


Abbildung 94. Gespeicherte Berichte laden

3. Wenn ein Bericht in der Voranzeige angezeigt wird, haben Sie die folgenden Möglichkeiten:
 - **Schließen**
Klicken Sie das **x** in der oberen rechten Ecke des Anzeigefensters an.
 - **Drucken**
Wählen Sie **File** aus der Menüleiste aus, und wählen Sie anschließend **Print** aus. Der Dialog **Page Setup** wird angezeigt. Wenn Sie **OK** anklicken, wird der Bericht gedruckt, mit **Cancel** verlassen Sie den Dialog.
 - **Druckeinstellungen**
Wählen Sie **File** aus der Menüleiste aus, und wählen Sie anschließend **Print Setup** aus. Der Dialog **Page Setup** wird angezeigt. Mit diesem Dialog können Sie die Seitenränder, die Ausrichtung und die Spaltenanordnung ändern. Wenn Sie die Ausgabeinheit ändern wollen, klicken Sie erst die Indexzunge **Page**, danach **Use Specific Printer** und anschließend **Printer** an. Klicken Sie **OK** an, um die vorgenommenen Änderungen zu speichern, oder **Cancel**, um diese wieder zu verwerfen.

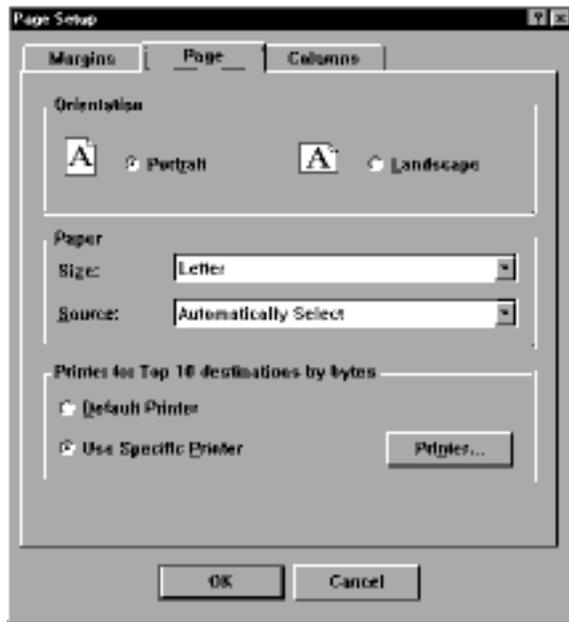


Abbildung 95. Dialog "Page Setup"

Datenmanagement

Wenn Sie häufig Datensammlungen in Ihrem Netzwerk über einen längeren Zeitraum durchführen, hat das zwei Auswirkungen:

- Ältere Daten sind veraltet oder möglicherweise nicht mehr mit einem solchen Detaillierungsgrad erforderlich.
- Die Reporter-Datenbank kann zu groß werden, so daß Reporter länger braucht, um seine Tasks auszuführen.

Ein regelmäßiges Datenmanagement kann diese Probleme beheben.

Die in Collector erstellten CSV-Dateien müssen ebenfalls verwaltet werden, weil sie schnell die Festplatte füllen (siehe Anhang C, „Leistungsrichtlinien“ auf Seite 165).

In diesem Kapitel werden folgende Themen behandelt:

- Daten verwalten
- Daten zusammenfassen
- Daten löschen
- Daten archivieren

Daten verwalten

Beim Speichern von Daten, die Sie im Lauf der Zeit gesammelt haben, belegt Ihre Datenbank immer mehr Plattenspeicherplatz. Die Geschwindigkeit, mit der sie wächst, hängt von der Unterteilung der gesammelten Daten ab.

Eine hohe Unterteilung führt zu häufigen Datensammlungen und daher zu mehr erforderlichem Plattenspeicherplatz.

Reporter kann Daten durch Berechnung von Tages- oder Wochenmitteln der ursprünglichen Daten zusammenfassen. Die ursprünglichen Daten in der Datenbank werden dann *automatisch gelöscht*. Auf diese Weise behalten Sie das Wesentliche Ihrer ursprünglich gesammelten Daten und benötigen doch viel weniger Plattenspeicherplatz.

Bei der *Konsolidierung* werden mehrere Datensätze in einem einzigen Datensatz komprimiert, indem der Mittelwert der Daten gebildet wird. Eine weniger detaillierte Unterteilung bewirkt, daß die zusammengefaßten Daten besser für die Trendermittlung und die Ermittlung von Vergleichsdaten, die Durchschnittswerte verwenden, als für die kurzfristige Fehlerbehebung geeignet sind, die mehr Detailinformationen benötigt.

Daten, die zu Tagesmitteln zusammengefaßt wurden, können weiter zu Wochenmitteln zusammengefaßt werden, usw.

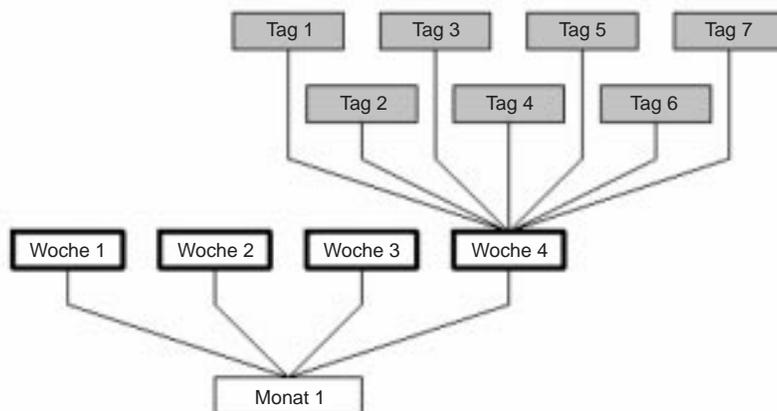


Abbildung 96. Mehrere Datensätze zusammenfassen

Mit der Datenzusammenfassungsfunktion (siehe „Datenbankinhalt anzeigen“ auf Seite 135) können Sie sehen, ob die Daten bereits zusammengefaßt sind.

Beispiele für die Zusammenfassung

Die folgenden Abbildungen zeigen Daten über denselben Zeitraum, allerdings jeweils mit einem anderen Alter der Daten.

1. In der ursprünglichen Form gibt es viel mehr Variation im Zeitgraphen:

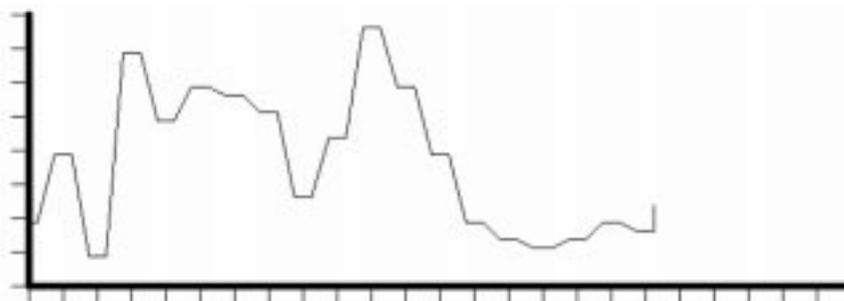


Abbildung 97. Ursprüngliche Datensammlungen

2. Wenn die Daten eine Woche alt sind, werden sie zu Tagesdatensätzen zusammengefaßt. Der Zeitgraph wird glatter, behält jedoch einige Spitzen und Senken:

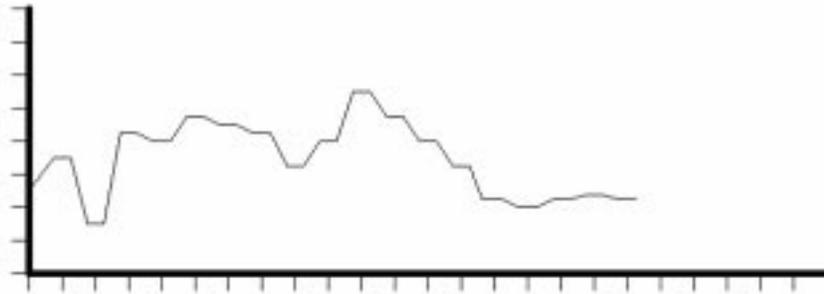


Abbildung 98. Nach der ersten Zusammenfassung

3. Nach einem Monat werden die Tagesdatensätze weiter zusammengefaßt. Der Zeitgraph wird noch glatter:

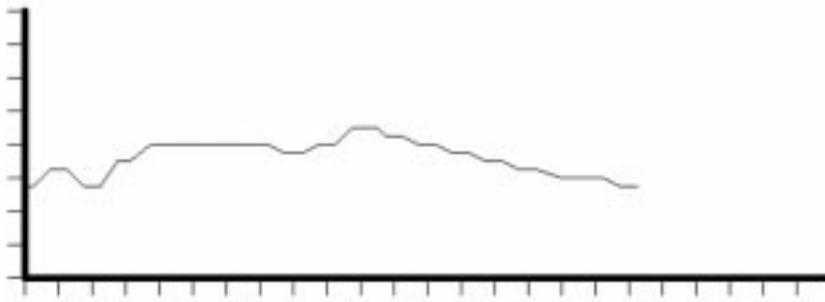


Abbildung 99. Nach der zweiten Zusammenfassung

Wenn die Zusammenfassung fortgesetzt wird, wird der Zeitgraph immer glatter. Er zeigt dann immer mehr den Gesamttrend an und bietet immer weniger Informationen zu periodischen Schwankungen.

Sobald Daten zusammengefaßt sind, kann dieser Prozeß nicht wieder umgekehrt werden. Es kann deshalb wünschenswert sein, eine Kopie der Datenbank zu behalten (siehe „Daten archivieren“ auf Seite 148).

Daten zusammenfassen

Klicken Sie im Reporter-Hauptfenster **Data Management** an, um den Dialog **Data Management** zu öffnen.

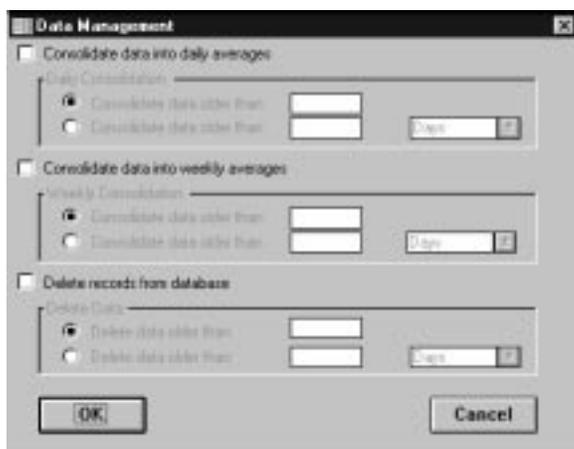


Abbildung 100. Dialog "Data Management"

Gehen Sie wie folgt vor, um Daten in der Reporter-Datenbank zusammenzufassen:

1. Wählen Sie entweder **Consolidate data into daily averages** oder **Consolidate data into weekly averages** aus.
2. Gehen Sie wie folgt vor, um bei beiden Optionen jeweils anzugeben, welche Daten zusammengefaßt werden sollen:
 - a. Klicken Sie den Knopf **Consolidate data older than** an, und geben Sie ein Datum im Textfeld im Format tt:mm:jj ein.
 - b. Klicken Sie den zweiten Knopf **Consolidate data older than** an. Geben Sie eine bestimmte Anzahl von Tagen, Wochen oder Monaten im Textfeld ein, und wählen Sie dann einen Zeitraum aus der verdeckten Liste aus.
3. Klicken Sie **OK** an, um zum Hauptfenster zurückzukehren. Reporter startet die Zusammenfassung. Klicken Sie **Cancel** an, um die Zusammenfassung abzubrechen.

Daten löschen

Sie müssen möglicherweise Daten löschen, z. B. wenn Sie Ihr Netzwerk neu konfiguriert haben. Wenn Sie Daten löschen, werden diese endgültig aus der ausgewählten Datenbank gelöscht. Sie müssen sicher sein, daß Sie die Daten nicht mehr benötigen, bevor Sie sie löschen.

Das Löschen von Daten unterscheidet sich vom Zusammenfassen von Daten. Wenn Daten aus der Datenbank gelöscht werden, stehen sie für zukünftige Zusammenfassungen nicht mehr zur Verfügung.

Wenn Sie sich nicht sicher sind, ob Sie die Daten möglicherweise noch benötigen, gehen Sie nach einer der folgenden Methoden vor:

- Erstellen Sie zuerst eine Sicherungskopie der Datenbank in einem sicheren Verzeichnis, so daß die Daten nicht endgültig verloren sind (siehe „Daten archivieren“ auf Seite 148).
- Verwenden Sie statt der Löschfunktion die Zusammenfassungsfunktion. Auf diese Weise werden die ursprünglichen Daten durch Tages- oder Wochenmittel ersetzt.

Gehen Sie wie folgt vor, um Daten aus der Reporter-Datenbank zu löschen:

1. Klicken Sie im Reporter-Hauptfenster **Data Management** an, um den Dialog **Data Management** zu öffnen (siehe Abb. 100).
2. Wählen Sie **Delete records from database** aus.
3. Verwenden Sie eine der folgenden Methoden, um den Zeitpunkt anzugeben, ab dem das Löschen erfolgen soll:
 - a. Klicken Sie zuerst den Knopf **Delete data older than** an, und geben Sie ein Datum im Textfeld im Format `tt:mm:jj` ein.
 - b. Klicken Sie den zweiten Knopf **Delete data older than** an. Geben Sie eine bestimmte Anzahl von Tagen, Wochen oder Monaten im Textfeld ein, und wählen Sie dann einen Zeitraum aus der verdeckten Liste aus.
4. Klicken Sie **OK** an, um zum Hauptfenster zurückzukehren. Reporter startet den Löschvorgang. Klicken Sie **Cancel** an, um das Löschen von Daten abzubrechen.

Daten archivieren

Nach einer gewissen Zeit möchten Sie möglicherweise den gesamten Inhalt einer Datenbank archivieren und von Collector gesammelte Daten in eine neue Datenbank importieren.

Daten archivieren

1. Importieren Sie ab einem geeigneten Zeitpunkt keine Daten mehr in die aktuelle Datenbank, z. B. am Ende einer Woche oder eines Monats.
2. Speichern Sie die Datenbank an einer sicheren Position.
3. Erstellen Sie eine neue Datenbank (siehe „Eine neue Datenbank erstellen“ auf Seite 133).
4. Importieren Sie von Collector gesammelte Daten in die neue Datenbank.

Wenn Sie den für die archivierten Datenbanken benötigten Plattenspeicherplatz verringern wollen, fassen Sie die in der Datenbank enthaltenen Daten zusammen (siehe „Daten zusammenfassen“ auf Seite 146).

Auf archivierte Daten zugreifen

1. Klicken Sie **Open Database** im Reporter-Hauptfenster an, um den Dialog **Open Database File** zu öffnen.
2. Wählen Sie die alte Datenbank aus.

Sie können jetzt Berichte von diesen alten Daten generieren (siehe „Berichte auswählen und generieren“ auf Seite 136).

Sie müssen die archivierte Datenbank schließen und die neue Datenbank auswählen, bevor Sie neue Daten importieren können.

Anwendungsdatenbank komprimieren und reparieren

Reporter verwendet zwei Arten von Datenbanken:

- Eine benutzerdefinierte Berichtsdatenbank für importierte Daten
Diese wird einfach zum Speichern von Daten verwendet. Sie enthält die gesammelten Daten, die Sie in Reporter importiert haben.
- Eine Anwendungsdatenbank für das Reporter-Programm
Diese heißt `1sr97.mdb`. Sie enthält die Benutzerschnittstelle und die vollständige Funktionalität von Reporter.

Dieses Kapitel befaßt sich mit der Anwendungsdatenbank.

Die Anwendungsdatenbank wird mit der Zeit größer oder möglicherweise beschädigt. Reporter enthält zwei weitere Programme für die folgenden Aufgaben:

- Komprimieren der Anwendungsdatenbank
- Reparieren der Anwendungsdatenbank

Anwendungsdatenbank komprimieren

Wenn Sie mit Reporter arbeiten und Daten löschen, kann die Anwendungsdatenbank fragmentiert werden, so daß sie den Plattenspeicherplatz nicht mehr effizient nutzt. Beim Komprimieren wird eine Kopie der Datenbank erstellt, bei der die gespeicherte Datenbankdatei auf der Platte neu angeordnet wird. Eine Komprimierung sollte wöchentlich ausgeführt werden.

Stellen Sie sicher, daß auf Ihrer Platte ausreichend Platz für die ursprüngliche Datenbank und eine temporäre Kopie der Datenbank vorhanden ist. Die Komprimierung wird abgebrochen, wenn nicht ausreichend Plattenspeicherplatz verfügbar ist.

Sie müssen Reporter schließen, bevor Sie versuchen, die Anwendungsdatenbank zu komprimieren.

Gehen Sie wie folgt vor, um die Anwendungsdatenbank zu komprimieren:

1. Schließen Sie Reporter.
2. Wählen Sie die Programmgruppe **IBM Nways ReMon** im Menü **Start** und anschließend **Compact Application Database** aus.

Die Anwendungsdatenbank wird automatisch komprimiert.

Anwendungsdatenbank reparieren

Wenn die Reporter-Anwendungsdatenbank beschädigt wird, z. B. durch einen Stromausfall, kann sie repariert werden.

Sie müssen Reporter schließen, bevor Sie versuchen, die Datenbank zu reparieren.

Gehen Sie wie folgt vor, um die Anwendungsdatenbank zu reparieren:

1. Schließen Sie Reporter.
2. Wählen Sie die Programmgruppe **IBM Nways ReMon** im Menü **Start** und anschließend **Repair Application Database** aus.

Die Datenbank wird automatisch repariert.

Anhang A. Liste der Protokolldecodierungen

In diesem Anhang werden die für die RMON-Anwendungen in diesem Release unterstützten Protokolldecodierungen (Tabelle 25) aufgeführt.

Tabelle 25. Liste der unterstützten Protokolldecodierungen nach Protokollfamilie

Protokollfamilie	Protokolle
AppleTalk Phase I & II	AARP, ADSP, AEP, AFP, ASP, ATP, DDP, MacIP, MacIP-Konfiguration, NBP, PAP, RTMP, ZIP
TCP/IP	AppleTalk in Cayman-IP-Tunnel, ARP, AURP (IPTALK-Leitweginformationen), BootP, DNS, EGP, FTP, ICMP, IGMP, IP, IPTALK (AppleTalk in IP-Tunnel), LPR/LPD, NetBIOS (TCP), NFS, OSPF, POP, RARP, RIP, RIP2, RLOGIN, RPC, RSH, SMTP, SNMP, TCP, Telnet, TFTP, UDP
DECNet (Phase IV & V)	Control, DRP, NSP, LAT, MOP, SCP
Novell NetWare	IPX, NCP, RIP, SAP, SNMP (über IPX), SPX
Banyan VINES	ARP, Echo, ICP, IPC, RTP, SPP
IBM SNA	DLC, XID (TH, RH, RU)
Xerox XNS	Echo, Error, PEP, RIP, SPP
ISO	CLNP, ESIS, ISIS, LLC 1 & 2, TP0 bis TP4
LAN Manager	NetBEUI, NetBIOS, SMB
LAN-Kapselungen	Ethernet Typ II, IEEE 802.1, IEEE 802.2, IEEE 802.3, IEEE 802.5, LLC1, LLC2, LSAP, MAC, SNAP, Spanning Tree
FDDI	LLC, MAC, SMT

Anhang B. Anwendungsvariablen

Dieser Anhang enthält Definitionen der Variablen, die in den folgenden Anwendungen ausgewählt werden können:

- Statistics
- History
- Hosts
- Matrix
- Ring Station

Variablen für Statistics

Statistics bietet die folgenden Variablen auf Ethernet, FDDI und Token-Ring.

Auf Ethernet verfügbare Variablen

Tabelle 26. Auf Ethernet verfügbare Variablen für Statistics

Variable	Beschreibung
Bytes Sent	Die Gesamtanzahl von Byte, aus denen alle auf diesem Segment erkannten Pakete bestehen.
Broadcasts	Fehlerfreie Pakete, die an die Rundsendeadresse gerichtet sind.
Collisions	Beste Schätzung der Anzahl der Kollisionen auf diesem Segment.
CRC Errors	Ein Paket ist nicht eine ganze Zahl von Oktetten lang oder hat eine fehlerhafte Rahmenprüfbitfolge.
Missed	Anzahl der durch die Sonde erkannten Ressourcenmängel, wodurch die Sonde möglicherweise Pakete nicht gezählt hat.
Packets Sent	Gesamtanzahl von auf diesem Segment erkannten Paketen, einschließlich Fehlerpakete.
Multicasts	Fehlerfreie Pakete, die an die Adresse für selektives Rundsenden gerichtet sind. Schließt Rundsendepakete nicht ein.
Too Long	Länger als 1518 Oktette (einschließlich Rahmenprüfbitfolge-Oktette), aber ansonsten fehlerfrei.
Too Short	Kürzer als 64 Oktette (einschließlich Rahmenprüfbitfolge-Oktette), aber ansonsten fehlerfrei.
Long + CRC	Zu lang und Prüfsummenfehler.
Short + CRC	Zu kurz und Prüfsummenfehler.
64 Bytes	Pakete genau 64 Byte lang.
65 to 127, usw.	Paketgrößen sind inklusiv und enthalten Rahmenprüfbitfolge-Oktette.

Auf FDDI verfügbare Variablen

Tabelle 27. Auf FDDI verfügbare Variablen für Statistics

Variable	Beschreibung
Beacons	Anzahl der im Ring sichtbaren Beacon-Nachrichten.
Beacon Src.	Adresse des Host, der die letzte Beacon-Nachricht gesendet hat.
Broadcasts	Fehlerfreie Pakete, die an die Rundsendeadresse gerichtet sind.
Bytes Sent	Gesamtanzahl von Byte, aus denen alle in diesem Ring erkannten Pakete bestehen.
Claim Frames	Anzahl der im Ring sichtbaren Bestätigungsrahmen.
Dir. Beacons	Anzahl der im Ring sichtbaren gerichteten Beacon-Nachrichten.
Dir. Beacon Src.	Adresse des Host, der die letzte gerichtete Beacon-Nachricht gesendet hat.
Errors	Rahmen mit gesetztem Fehleranzeiger.
Missed	Anzahl der durch die Sonde erkannten Ressourcenmängel, wodurch die Sonde möglicherweise Pakete nicht gezählt hat.
Multicasts	Fehlerfreie Pakete, die an die Adresse für selektives Rundsenden gerichtet sind. Schließt Rundsendepakete nicht ein.
Packets Sent	Gesamtanzahl von in diesem Ring erkannten Paketen, einschließlich Fehlerpakete.
Ring State	Aktueller Betriebsstatus des FDDI-Rings: <ol style="list-style-type: none"> 1. Ring Operational 2. Non-Operational Claim 3. Non-Operational Beacon 4. Non-Operational Dir. Beacon 5. Unknown
SMT Frames	Anzahl der im Ring sichtbaren SMT-Rahmen.
TNEG	Variable Umlaufdauer des Tokens (Negotiated Token Rotation Time; TNEG). Dies ist die TNEG, die bei der Senderechanforderung erfolgreich war.
Tokens	Anzahl der Token im Ring.
22 Bytes	Pakete genau 22 Byte lang.
23 to 63, usw.	Paketgrößen sind inklusiv und enthalten Rahmenprüfbitfolge-Oktette.

Auf Token-Ring verfügbare Variablen

Tabelle 28 (Seite 1 von 3). Auf Token-Ring verfügbare Variablen für Statistics

Variable	Beschreibung
Abort Errors	Gesamtanzahl von Abbruchbegrenzern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Von einer Station wurde beim Versuch, einen Rahmen zu übertragen, ein Problem erkannt.
AC Errors	Gesamtanzahl von ACE-Fehlern (Address Copied Error) in Fehlerberichtspaketen, die von der Sonde erkannt werden.
All Route Bcasts	Anzahl der an beliebige Adressen in allen Ringen ausgegebenen Rundsendenachrichten.
All Route Octets	Anzahl der Oktette, aus denen an beliebige Adressen in allen Ringen ausgegebenen Rundsendenachrichten bestehen.
Beacon Events	Gesamtanzahl der Wechsel des Rings in einen Beacon-Betriebsstatus (die Änderung der Quellenadresse eines Beacon-Pakets stellt kein neues Beacon-Ereignis dar).
Beacon Packets	Gesamtanzahl von Beacon-MAC-Paketen, die von der Sonde erkannt werden.
Beacon Time	Gesamtzeit, während der sich der Ring in einem Beacon-Betriebsstatus befand.
Burst Errors	Gesamtanzahl von Trennfehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Oft verursacht durch eine sehr kurze Trennung im Kabel oder eine sehr kurze Spitze des elektronischen Rauschens.
Claim Token Events	Anzahl der Wechsel des Rings in den Bestätigungs-Token-Prozess.
Claim Token Pkts	Gesamtanzahl von Bestätigungs-Token-Paketen, die von der Sonde erkannt werden.
Congestion Errors	Gesamtanzahl von Fehlern aufgrund von Empfangsüberlastung in Fehlerberichtspaketen, die von der Sonde erkannt werden. Eine Station empfing einen Rahmen und hatte keinen ausreichenden Puffer, um ihn zu speichern.
Data Bytes	Gesamtanzahl von Byte, aus denen alle auf diesem Segment erkannten sonstigen Datenpakete bestehen.
Data Packets	Gesamtanzahl von sonstigen Datenpaketen, die auf diesem Segment erkannt werden.
Data Bcast Pkts	Fehlerfreie Pakete, die an die Rundsendeadresse gerichtet sind. Schließt Pakete für selektives Rundsenden nicht ein.
Data Mcast Pkts	Fehlerfreie Pakete, die an die Adresse für selektives Rundsenden gerichtet sind. Schließt Rundsendepakete nicht ein.
Drop Events	Anzahl der durch die Sonde erkannten Ressourcenmängel, wodurch die Sonde möglicherweise LLC- oder MAC-Pakete nicht gezählt hat.
Error Reports	Gesamtanzahl von normalen Fehlerberichtsrahmen, die von der Sonde erkannt werden. Normale Fehler sind oft nicht schwerwiegend genug, um den Betrieb des Rings zu unterbrechen. Sie umfassen Leitungsfehler, Trennfehler, interne Fehler, Abbruchfehler, ACE-Fehler (Address Copied Error), Fehler aufgrund verlorener Rahmen, Token-Fehler, Frequenzfehler und Rahmenkopiefehler (Frame Copied Error).

Tabelle 28 (Seite 2 von 3). Auf Token-Ring verfügbare Variablen für Statistics

Variable	Beschreibung
Frames Copied	Gesamtanzahl von Rahmenkopierfehlern (Frame Copied Error) in Fehlerberichtspaketen, die von der Sonde erkannt werden. Eine Station glaubt, daß eine andere Station im Ring dieselbe Adresse hat (<i>normalerweise</i> kein Problem — siehe „Glossar“ auf Seite 195).
Frames In	Anzahl der Rahmen, die in diesem Ringsegment von einem anderen Segment eingehen.
Frames Out	Anzahl der Rahmen, die von diesem Ringsegment an ein anderes übergeben werden.
Frequency Errors	Gesamtanzahl von Frequenzfehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Ein Taktungsfehler, der oft durch den Anschluß von mehr als 72 Stationen an den Ring verursacht wird.
Internal Errors	Gesamtanzahl von internen Adapterfehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Oft verursacht durch Überhitzung in einem überlasteten System.
Line Errors	Gesamtanzahl von Leitungsfehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Normalerweise verursacht durch elektronisches Rauschen oder Kabelprobleme.
Local LLC Frames	Gesamtanzahl von empfangenen Rahmen, die kein RIF-Feld hatten (bzw. ein RIF-Feld hatten, das nur die Nummer des lokalen Rings umfaßt) und keine Rahmen für Rundsendebetrieb über alle Leitwege waren.
Lost Frames	Gesamtanzahl von Fehlern aufgrund verlorener Rahmen in Fehlerberichtspaketen, die von der Sonde erkannt werden. Eine Station übertrug einen Rahmen, der nicht mehr zu ihr zurückkam.
MAC Bytes	Gesamtanzahl von Byte, aus denen alle auf diesem Segment erkannten MAC-Pakete bestehen.
MAC Packets	Gesamtzahl der in diesem Segment erkannten MAC-Pakete, einschließlich Fehlerpakete.
NAUN Changes	Gesamtanzahl der von der Sonde erkannten NAUN-Änderungen (Nearest Active Upstream Neighbor), verursacht dadurch, daß eine neue Station im Ring betriebsbereit wird oder eine Station sich selbst aus dem Ring entfernt.
Octets In	Anzahl der Oktette, aus denen die Rahmen bestehen, die in diesem Ringsegment von einem anderen Segment eingehen.
Octets Out	Anzahl der Oktette, aus denen die Rahmen bestehen, die von diesem Ringsegment an ein anderes übergeben werden.
Octets Through	Anzahl der Oktette, aus denen die Rahmen bestehen, die auf dem Weg zur Zieladresse dieses Ringsegment durchlaufen.
Purge Events	Gesamtanzahl der Wechsel des Rings aus dem normalen Ringstatus in einen Ringfreigabestatus (schließt jeden Ringfreigabestatus aus, der als Ergebnis eines Bestätigungs-Token- oder eines Beacon-Betriebsstatus auftritt).
Purge Packets	Gesamtanzahl von Ringfreigabe-MAC-Paketen, die von der Sonde erkannt werden.
Ring Number	Numerische Kennung dieses Rings.

Tabelle 28 (Seite 3 von 3). Auf Token-Ring verfügbare Variablen für Statistics

Variable	Beschreibung
Ring Polls	Gesamtanzahl von Ringaufrufereignissen, die von der Sonde erkannt werden (d. h. Anzahl der Ringaufrufe, die vom aktiven Monitor eingeleitet wurden).
Sgl. Route Bcasts	Anzahl der an eine bestimmte Anzahl von Empfängern ausgegebenen Rundsendenachrichten — normalerweise das lokale Ringsegment.
Single Route Oct.	Anzahl der Oktette, aus denen die an eine bestimmte Anzahl von Empfängern ausgegebenen Rundsendenachrichten bestehen — normalerweise das lokale Ringsegment.
Through Frames	Anzahl der Rahmen, die auf dem Weg zur Zieladresse dieses Ringsegment durchlaufen.
Token Errors	Gesamtanzahl von Token-Fehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Gemeldet vom aktiven Monitor, wenn das Token beschädigt wird.
1 Hop Frames usw.	Gesamtanzahl von Rahmen, die mit 1, 2, 3, 4, 5, 6, 7, 8 oder mehr als 8 Hops (über Brücken zwischen Ringsegmenten) ihre Zieladresse erreichen.
18 to 63 Bytes usw.	Paketgrößen sind inklusiv und enthalten Rahmenprüfbitfolge-Oktette.

Variablen für History

In den folgenden Tabellen sind die auf Ethernet, FDDI und Token-Ring verfügbaren Variablen aufgelistet.

Auf Ethernet verfügbare Variablen

Tabelle 29. Auf Ethernet verfügbare Variablen für History

Variable	Beschreibung
Broadcasts	Fehlerfreie Pakete, die an die Rundsendeadresse gerichtet sind.
Bytes Sent	Die Gesamtanzahl von Byte, aus denen alle auf diesem Segment erkannten Pakete bestehen.
Collisions	Beste Schätzung der Anzahl der Kollisionen auf diesem Segment.
CRC Errors	Ein Paket ist nicht eine ganze Zahl von Oktetten lang oder hat eine fehlerhafte Rahmenprüfbitfolge.
Long + CRC	Zu lang und Prüfsummenfehler.
Multicasts	Fehlerfreie Pakete, die an die Adresse für selektives Rundsenden gerichtet sind. Schließt Rundsendepakete nicht ein.
Packets Missed	Anzahl der durch die Sonde erkannten Ressourcenmängel, wodurch die Sonde möglicherweise Pakete nicht gezählt hat.
Packets Sent	Gesamtanzahl von auf diesem Segment erkannten Paketen, einschließlich Fehlerpakete.
Short + CRC	Zu kurz und Prüfsummenfehler.
Too Long	Länger als 1518 Oktette (einschließlich Rahmenprüfbitfolge-Oktette), aber ansonsten fehlerfrei.
Too Short	Kürzer als 64 Oktette (einschließlich Rahmenprüfbitfolge-Oktette), aber ansonsten fehlerfrei.
Utilization	Prozentsatz der Netzwerkkapazität zum Zeitpunkt dieser Stichprobenperiode.

Auf FDDI verfügbare Variablen

Tabelle 30. Auf FDDI verfügbare Variablen für History

Variable	Beschreibung
Beacons	Anzahl der im Ring sichtbaren Beacon-Nachrichten.
Broadcasts	Fehlerfreie Pakete, die an Rundsendeadresse gerichtet sind.
Bytes Sent	Gesamtanzahl von Byte, aus denen alle in diesem Ring erkannten Pakete bestehen.
Claim Frames	Anzahl der im Ring sichtbaren Bestätigungsrahmen.
Dir. Beacons	Anzahl der im Ring sichtbaren gerichteten Beacon-Nachrichten.
Errors	Rahmen mit gesetztem Fehleranzeiger.
Mean TRT	Errechnete mittlere Zeit, während der ein Token umläuft.
Missed	Anzahl der durch die Sonde erkannten Ressourcenmängel, wodurch die Sonde möglicherweise Pakete nicht gezählt hat.
Multicasts	Fehlerfreie Pakete, die an die Adresse für selektives Rundsenden gerichtet sind. Schließt Rundsendepakete nicht ein.
Packets Sent	Gesamtanzahl von in diesem Ring erkannten Paketen, einschließlich Fehlerpakete.
SMT Frames	Anzahl der im Ring sichtbaren SMT-Rahmen.
TNEG	Variable Umlaufdauer des Token (Negotiated Token Rotation Time; TNEG). Dies ist die TNEG, die bei der Senderechanforderung erfolgreich war.
Utilization	Prozentsatz der Netzwerkkapazität zum Zeitpunkt dieser Stichprobenperiode.
22 Bytes	Pakete genau 22 Byte lang.
23 to 63 usw.	Paketgrößen sind inklusiv und enthalten Rahmenprüfbitfolge-Oktette.

Auf Token-Ring verfügbare Variablen

Tabelle 31 (Seite 1 von 2). Auf Token-Ring verfügbare Variablen für History

Variable	Beschreibung
Abort Errors	Gesamtanzahl von Abbruchbegrenzern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Von einer Station wurde beim Versuch, einen Rahmen zu übertragen, ein Problem erkannt.
AC Errors	Gesamtanzahl von ACE-Fehlern (Address Copied Error) in Fehlerberichtspaketen, die von der Sonde erkannt werden.
Active Stations	Anzahl der aktiven Stationen in diesem Ringsegment, d. h. die Stationen, die am Ringaufruf teilnehmen.
Beacon Events	Gesamtanzahl der Wechsel des Rings in einen Beacon-Betriebsstatus (die Änderung der Quellenadresse eines Beacon-Pakets stellt kein neues Beacon-Ereignis dar).
Beacon Packets	Gesamtanzahl von Beacon-MAC-Paketen, die von der Sonde erkannt werden.
Beacon Time	Gesamtzeit, während der sich der Ring in einem Beacon-Betriebsstatus befand.
Burst Errors	Gesamtanzahl von Trennfehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Oft verursacht durch eine sehr kurze Trennung im Kabel oder eine sehr kurze Spitze des elektronischen Rauschens.
Claim Token Events	Anzahl der Wechsel des Rings in den Bestätigungs-Token-Prozeß.
Claim Token Packets	Gesamtanzahl von Bestätigungs-Token-Paketen, die von der Sonde erkannt werden.
Congestion Errors	Gesamtanzahl von Fehlern aufgrund von Empfangsüberlastung in Fehlerberichtspaketen, die von der Sonde erkannt werden. Eine Station empfing einen Rahmen und hatte keinen ausreichenden Puffer, um ihn zu speichern.
Data Bcast Packets	Fehlerfreie Pakete, die an die Rundsendeadresse gerichtet sind.
Data Bytes	Gesamtanzahl von Byte, aus denen alle auf diesem Segment erkannten sonstigen Datenpakete bestehen.
Data Mcast Packets	Fehlerfreie Pakete, die an die Adresse für selektives Rundsenden gerichtet sind. Schließt Rundsendepakete nicht ein.
Data Packets	Gesamtanzahl von sonstigen Datenpaketen, die auf diesem Segment erkannt werden.
Drop Events	Anzahl der durch die Sonde erkannten Ressourcenmängel, wodurch die Sonde möglicherweise Pakete nicht gezählt hat.
Error Reports	Gesamtanzahl von normalen Fehlerberichtsrahmen, die von der Sonde erkannt werden. Normale Fehler sind oft nicht schwerwiegend genug, um den Betrieb des Rings zu unterbrechen. Sie umfassen Leitungsfehler, Trennfehler, interne Fehler, Abbruchfehler, ACE-Fehler (Address Copied Error), Fehler aufgrund verlorener Rahmen, Token-Fehler, Frequenzfehler und Rahmenkopiefehler (Frame Copied Error).

Tabelle 31 (Seite 2 von 2). Auf Token-Ring verfügbare Variablen für History

Variable	Beschreibung
Frames Copied	Gesamtanzahl von Rahmenkopiefehlern (Frame Copied Error) in Fehlerberichtspaketen, die von der Sonde erkannt werden. Eine Station glaubt, daß eine andere Station im Ring dieselbe Adresse hat (normalerweise kein Problem — siehe „Glossar“ auf Seite 195).
Frequency Errors	Gesamtanzahl von Frequenzfehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Ein Taktungsfehler, der oft durch den Anschluß von mehr als 72 Stationen an den Ring verursacht wird.
Internal Errors	Gesamtanzahl von internen Adapterfehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Oft verursacht durch Überhitzung in einem überlasteten System.
Line Errors	Gesamtanzahl von Leitungsfehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Normalerweise verursacht durch elektronisches Rauschen oder Kabelprobleme.
Lost Frames	Gesamtanzahl von Fehlern aufgrund verlorener Rahmen in Fehlerberichtspaketen, die von der Sonde erkannt werden. Eine Station übertrug einen Rahmen, der nicht mehr zu ihr zurückkam.
MAC Bytes	Gesamtanzahl von Byte, aus denen alle auf diesem Segment erkannten MAC-Pakete bestehen.
MAC Packets	Gesamtzahl der in diesem Segment erkannten Pakete der MAC-Schicht (einschließlich Fehlerpakete).
NAUN Changes	Gesamtanzahl der von der Sonde erkannten NAUN-Änderungen (Nearest Active Upstream Neighbor), verursacht dadurch, daß eine neue Station im Ring betriebsbereit wird oder die aktuelle NAUN sich selbst aus dem Ring entfernt.
Purge Events	Gesamtanzahl der Wechsel des Rings aus dem normalen Ringstatus in einen Ringfreigabestatus (schließt jeden Ringfreigabestatus aus, der als Ergebnis eines Bestätigungs-Token- oder eines Beacon-Betriebsstatus auftritt).
Purge Packets	Gesamtanzahl von Ringfreigabe-MAC-Paketen, die von der Sonde erkannt werden.
Ring Polls	Gesamtanzahl von Ringaufrufereignissen, die von der Sonde erkannt werden (d. h. Anzahl der Ringaufrufe, die vom aktiven Monitor eingeleitet wurden).
Token Errors	Gesamtanzahl von Token-Fehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Gemeldet vom aktiven Monitor, wenn das Token beschädigt wird.
18 to 63 usw.	Paketgrößen sind inklusiv und enthalten Rahmenprüfbitfolge-Oktette.
Utilization	Token-Ring-Auslastungsberechnungen beruhen auf der Verwendung der Variablen <code>ifSpeed</code> aus der Schnittstellentabelle. Wenn der Wert 0 ist, wird eine Ringgeschwindigkeit von 16 Mbps für die Berechnung angenommen.

Variablen für Hosts

In der folgenden Variablenliste sind die auf Ethernet, FDDI und Token-Ring verfügbaren Variablen für Hosts aufgelistet.

Tabelle 32. Auf Ethernet, FDDI und Token-Ring verfügbare Variablen für Hosts

Variable	Beschreibung
Packets In	Anzahl der im Segment sichtbaren Pakete für diese Station, einschließlich Fehlerpakete.
Packets Out	Anzahl der Pakete, für deren Senden diese Station verantwortlich war, einschließlich Fehlerpakete.
Bytes In	Gesamtanzahl von Byte, aus denen alle für dieses Segment bestimmten Pakete bestehen.
Bytes Out	Gesamtanzahl von Byte, aus denen alle von diesem Segment zu sendenden Pakete bestehen.
Error Packets	Anzahl der Fehlerpakete, für deren Generierung diese Station verantwortlich war.
Broadcasts	Fehlerfreie Pakete, die von dieser Station an die Rundsendeadresse gerichtet sind.
Multicasts	Fehlerfreie Pakete, die von dieser Station an die Adresse für selektives Rundsenden gerichtet sind. Schließt Rundsendepakete nicht ein.

Variablen für Ring Station

Die folgenden Variablen sind für Ring Station verfügbar auf Token-Ring.

Tabelle 33 (Seite 1 von 2). Auf Token-Ring verfügbare Variablen für Ring Station

Variable	Beschreibung
Last NAUN	Physische Adresse der letzten bekannten NAUN (Nearest Active Upstream Neighbor) dieser Station.
Station Status	Status dieser Station im Ring — entweder aktiv, inaktiv oder vom Ring erzwungenermaßen abgemeldet.
Last Entered	Zeitpunkt des letzten Eintritts dieser Station in den Ring.
Last Exited	Zeitpunkt des letzten Austritts dieser Station aus dem Ring.
Duplicate Address	Anzahl der durch diese Station erkannten Fehler aufgrund einer doppelten Adresse.
In-line Errors	Gesamtanzahl von oberhalb dieser Station erkannten Leitungsfehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Normalerweise verursacht durch elektronisches Rauschen oder Kabelprobleme.
Out-line Errors	Gesamtanzahl von unterhalb dieser Station erkannten Leitungsfehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Normalerweise verursacht durch elektronisches Rauschen oder Kabelprobleme.
Internal Errors	Gesamtanzahl von internen Adapterfehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Normalerweise verursacht durch Überhitzung in einem überlasteten System.
Inburst Errors	Gesamtanzahl von oberhalb dieser Station erkannten Trennfehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Normalerweise verursacht durch eine sehr kurze Trennung im Kabel oder eine sehr kurze Spitze des elektronischen Rauschens.
Out Burst Errors	Gesamtanzahl von unterhalb dieser Station erkannten Trennfehlern in Fehlerberichtspaketen, die von der Sonde erkannt werden. Normalerweise verursacht durch eine sehr kurze Trennung im Kabel oder eine sehr kurze Spitze des elektronischen Rauschens.
AC Errors	Gesamtanzahl von ACE-Fehlern (Address Copied Error) in Fehlerberichtspaketen, die vom NADN dieser Station gesendet wurden.
Abort Errors	Gesamtanzahl von Abbruchbegrenzern, die von dieser Station in Fehlerberichtspaketen gemeldet wurden, die von der Sonde erkannt wurden. Ähnlich einem internen Fehler. In diesem Fall trat der Fehler jedoch beim Übertragen eines Rahmens auf.
Lost Frames	Gesamtanzahl von Fehlern aufgrund verlorener Rahmen, die von dieser Station in Fehlerberichtspaketen gemeldet wurden, die von der Sonde erkannt wurden.
Congestion Errors	Gesamtanzahl von Fehlern aufgrund von Empfangsüberlastung. Verursacht, wenn eine Station einen Rahmen empfängt und keinen ausreichenden Puffer hat, um ihn zu speichern.

Tabelle 33 (Seite 2 von 2). Auf Token-Ring verfügbare Variablen für Ring Station

Variable	Beschreibung
Frame Copied Errors	Gesamtanzahl von Rahmenkopiefehlern (Frame Copied Errors), die von dieser Station gemeldet wurden. Eine Station glaubt, daß eine andere Station dieselbe Adresse hat (<i>normalerweise</i> kein Problem — siehe „Glossar“ auf Seite 195).
Frequency Errors	Gesamtanzahl von Frequenzfehlern, die von dieser Station gemeldet wurden. Verursacht durch große Unterschiede zwischen einem Adaptertaktgeber und dem NAUN-Taktgeber.
Token Errors	Gesamtanzahl von Token-Fehlern, die von dieser Station gemeldet wurden. Ähnlich einem Leitungsfehler. In diesem Fall wurde jedoch das Token selbst beschädigt.
In Beacon Errors	Gesamtanzahl von Beacon-Rahmen, die oberhalb von dieser Station erkannt wurden (siehe „Glossar“ auf Seite 195).
Out Beacon Errors	Gesamtanzahl von Beacon-Rahmen, die unterhalb von dieser Station erkannt wurden (durch die Station, die diese Station als NAUN benennt) (siehe „Glossar“ auf Seite 195).
Insertions	Anzahl der durch die Sonde erkannten Eintritte dieser Station in den Ring.

Anhang C. Leistungsrichtlinien

In diesem Anhang wird ein typischer Fall der Datensammlung und des Datenimports in eine Reporter-Datenbank beschrieben, aus der die Daten zusammengefaßt und Berichte erzeugt werden. Tabelle 34 zeigt ein Beispiel für die Dauer jedes Vorgangs, um Ihnen eine Vorstellung davon zu geben, wie Sie Ihre Sammlungs- und Berichtszeitpläne einrichten sollten.

Im allgemeinen steigen die Zeiten für jeden Arbeitsgang proportional zur erfaßten Datenmenge. Die Leistung wird auch stark vom Prozessor des PCs und dem verfügbaren Hauptspeicher beeinflusst. Die Leistungszeiten im Beispiel stammen aus einem einzelnen Ethernet-Segment mit einem PC mit einem 120-MHz-Pentium®-Prozessor und 16 MB RAM.

Die Datensammlung wurde in Collector so definiert, daß sie 2 Tage dauert und alle Tabellen stündlich von einer einzigen SONDENSCHNITTSTELLE sammelt. Die Protokolleinträge wurden alle 30 Sekunden und alle 30 Minuten erfaßt. Es gab 162 Hosts und 1489 Datenaustauschvorgänge im Segment. Am Ende der Sammlungsphase waren 6 150 050 Byte Daten erfaßt und im CSV-Format auf Platte gespeichert.

Die Dateien waren dann zum Import in eine Reporter-Datenbank bereit. Es gibt verschiedene einzelne Operationen, die in Reporter für die Daten ausgeführt werden können. Diese Operationen werden in in Tabelle 34 dargestellt.

Tabelle 34. Beispiel für Verarbeitungszeiten in Reporter

Operation	Aktion	Zeit
Import	Importiert Dateien in eine leere Datenbankdatei.	9 Min. 37 Sek.
Save Reports	Generiert einen Bericht jedes Typs und speichert ihn in einer Datei.	5 Min. 37 Sek.
Print Reports	Generiert einen Bericht jedes Typs und sendet ihn an den Drucker.	11 Min. 10 Sek.
Consolidate data into daily averages	Faßt alle Daten in der Datenbank zu Tagesmitteln zusammen.	12 Min. 26 Sek.
Consolidate data into weekly averages	Faßt alle Daten in der Datenbank zu Wochenmitteln zusammen.	10 Min. 48 Sek.
Delete	Löscht alle Einträge aus der Datenbank.	8 Min. 12 Sek.

Sobald die CSV-Dateien in eine Reporter-Datenbank importiert wurden, sind sie nicht mehr erforderlich und sollten gelöscht werden, um Plattenplatz freizugeben.

Anhang D. Inhalt der CSV-Dateien

Collector erstellt die folgenden Dateien im CSV-Format für die Datenerfassung.

Tabelle 35. Von Collector erstellte CSV-Dateien

Dateiname	Beschreibung
hist.csv	Ethernet-Protokolldaten
host.csv	Host-Daten
matrix.csv	Matrix-Daten
trml.csv	MAC-Schichtprotokolldaten für Token-Ring
trp.csv	Sonstige Protokolldaten für Token-Ring

Der Inhalt dieser Dateien wird in den folgenden Abschnitten erläutert. Bitte berücksichtigen Sie bei der Interpretation der Dateiinhalte die folgenden Hinweise.

1. TimeIndex wird in Protokolltabellen und anderen Tabellen unterschiedlich interpretiert. In Protokolltabellen (hist.csv, trml.csv und trp.csv) verweist TimeIndex auf den *Start* eines Intervalls, das heißt, das Intervall endet bei (TimeIndex + dTimeIndex). In Host- und Matrixtabellen verweist TimeIndex auf das *Ende* eines Intervalls, das heißt, das Intervall beginnt bei (TimeIndex - dTimeIndex).
2. In Host- und Matrixtabellen wird selten ein absoluter Wert verwendet, da die Werte ständig steigen. In der Regel sind hier die Deltawerte wichtiger.
3. Der Feldname Probe verweist auf die Datenquelle (siehe „Datenquellen konfigurieren“ auf Seite 123) und die Schnittstellenummer. Deshalb ist es nicht erforderlich das Feld Index zu verwenden, um die einzelnen Schnittstellen einer Sonde mit mehreren Schnittstellen zu unterscheiden.

Protokolldateiformat

Der Inhalt der CSV-Datei, die Collector für Protokolldaten erstellt, ist in Tabelle 36 abgebildet.

Tabelle 36. Inhalt der CSV-Datei für Protokolldaten

Feldname	Beschreibung
Probe	Name des Protokollierungspunkts, an dem dieser Eintrag erfaßt wurde
TimeIndex	Startdatum und -zeitpunkt des Erfassungsintervalls
HistoryIndex	Identifikationsnummer der Protokollstudie, zu der dieser Eintrag gehört
Index	Schnittstelle, von der die Daten erfaßt wurden
SampleIndex	Identifikationsnummer des Eintrags innerhalb einer bestimmten Protokollstudie
IntervalStart	Startzeit des Intervalls (im Format sysUpTime)
DropEvents	Anzahl der in diesem Intervall von der Sonde gelöschten Pakete
Octets	Anzahl der in diesem Intervall gezählten Byte
Pkts	Anzahl der in diesem Intervall gezählten Pakete
BroadcastPkts	Anzahl der in diesem Intervall gezählten Rundsendepakete
MulticastPkts	Anzahl der in diesem Intervall gezählten Pakete mit Unterstützung für selektives Rundsenden
CRCAIalignErrors	Anzahl der in diesem Intervall gezählten CRC-Fehler
UndersizePkts	Anzahl der in diesem Intervall gezählten zu kleinen Pakete (< 64 Byte)
OversizePkts	Anzahl der in diesem Intervall gezählten zu großen Pakete (> 1518 Byte)
Fragments	Anzahl der in diesem Intervall gezählten Fragmente (Pakete < 64 Byte mit CRC-Fehler)
Jabbers	Anzahl der in diesem Intervall gezählten Pakete > 1518 Byte mit CRC-Fehler (Jabbers)
Collisions	Anzahl der in diesem Intervall gezählten Kollisionen
Utilization	Die durchschnittliche Segmentauslastung in diesem Intervall (auf einer Skala von 0 bis 10000)
dTimeIndex	Länge dieses Zeitintervalls (in Sekunden)

Host-Dateiformat

Der Inhalt der CSV-Datei, die Collector für Host-Daten erstellt, wird in Tabelle 37 beschrieben.

Tabelle 37. Inhalt der CSV-Datei für Host-Daten

Feldname	Beschreibung
Probe	Name des Protokollierungspunkts, an dem dieser Eintrag erfaßt wurde
TimeIndex	Datum und Zeitpunkt, zu dem dieser Eintrag von der Sonde erfaßt wurde
Address	Adresse des Hosts, auf den dieser Eintrag verweist
CreationOrder	Reihenfolge der Host-Erstellung in der RMON-Host-Tabelle
Index	Schnittstelle, von der die Daten gesammelt wurden
InPkts	Summe aller vom Host empfangenen Pakete
OutPkts	Summe aller vom Host gesendeten Pakete
InOctets	Summe aller vom Host empfangenen Byte
OutOctets	Summe aller vom Host gesendeten Byte
OutErrors	Summe aller vom Host gesendeten fehlerhaften Pakete
OutBroadcastPkts	Summe aller vom Host gesendeten Rundsendepakete
OutMulticastPkts	Summe aller vom Host gesendeten Pakete mit Unterstützung für selektives Rundsenden
dInPkts	Summe aller Pakete, die der Host seit der letzten Datensammlung empfangen hat
dOutPkts	Summe aller Pakete, die der Host seit der letzten Datensammlung gesendet hat
dInOctets	Summe aller Byte, die der Host seit der letzten Datensammlung empfangen hat
dOutOctets	Summe aller Byte, die der Host seit der letzten Datensammlung gesendet hat
dOutErrors	Summe aller fehlerhaften Pakete, die der Host seit der letzten Datensammlung gesendet hat
dOutBroadcastPkts	Summe aller Rundsendepakete, die der Host seit der letzten Datensammlung gesendet hat
dOutMulticastPkts	Summe aller Pakete mit Unterstützung für selektives Rundsenden, die der Host seit der letzten Datensammlung gesendet hat
dTimeIndex	Zeit (in Sekunden) zwischen der aktuellen und der letzten Datensammlung

Matrixdateiformat

Der Inhalt der CSV-Datei, die Collector für Matrixdaten erstellt, wird in Tabelle 38 beschrieben.

Tabelle 38. Inhalt der CSV-Datei für Matrixdaten

Feldname	Beschreibung
Probe	Name des Protokollierungspunkts, an dem dieser Eintrag erfaßt wurde
TimeIndex	Datum und Zeitpunkt, zu dem dieser Eintrag von der Sonde erfaßt wurde
SourceAddress	Quellenadresse des Datenaustauschs
DestAddress	Zieladresse des Datenaustauschs
Index	Schnittstelle, von der die Daten gesammelt wurden
Pkts	Summe aller Pakete des Datenaustauschs
Octets	Summe aller Byte des Datenaustauschs
Errors	Summe aller Fehler des Datenaustauschs
dPkts	Anzahl der Pakete, die während des Datenaustauschs seit der letzten Datensammlung gesendet wurden
dOctets	Anzahl der Byte, die während des Datenaustauschs seit der letzten Datensammlung gesendet wurden
dErrors	Anzahl der Fehler, die während des Datenaustauschs seit der letzten Datensammlung aufgetreten sind
dTimeIndex	Zeit (in Sekunden) zwischen der aktuellen und der letzten Datensammlung

MAC-Schichtprotokolldaten für Token-Ring

Der Inhalt der CSV-Datei, die Collector für MAC-Schichtprotokolldaten für Token-Ring erstellt, wird in Tabelle 39 beschrieben.

Tabelle 39 (Seite 1 von 2). Inhalt der CSV-Datei für MAC-Schichtprotokolldaten für Token-Ring

Feldname	Beschreibung
Probe	Name des Protokollierungspunkts, an dem dieser Eintrag erfaßt wurde
TimeIndex	Startdatum und -zeitpunkt des Erfassungsintervalls
HistoryIndex	Identifikationsnummer der Protokollstudie, zu der dieser Eintrag gehört
Index	Schnittstelle, von der die Daten gesammelt wurden
SampleIndex	Identifikationsnummer des Eintrags innerhalb einer bestimmten Protokollstudie
IntervalStart	Startzeit des Intervalls (im Format sysUpTime)
DropEvents	Anzahl der in diesem Intervall von der Sonde gelöschten Pakete
MacOctets	Anzahl der in diesem Intervall in MAC-Paketen gezählten Oktette
MacPkts	Anzahl der in diesem Intervall gezählten MAC-Pakete
RingPurgeEvents	Anzahl der Wechsel des Rings vom normalen Status in den Ringfreigabestatus in diesem Intervall
RingPurgePkts	Anzahl der in diesem Intervall gezählten Ringfreigabe-MAC-Pakete
BeaconEvents	Anzahl der Wechsel des Rings von einem Beacon-Betriebsstatus in einen Nicht-Beacon-Betriebsstatus in diesem Intervall
BeaconTime	Zeitdauer, in der sich der Ring in diesem Intervall im Beacon-Betrieb befunden hat
BeaconPkts	Anzahl der in diesem Intervall gezählten MAC-Pakete mit Beacon-Nachrichten
MCEvents	Anzahl der Wechsel des Rings in den Bestätigungs-Token-Status in diesem Intervall
ClaimTokenPkts	Anzahl der in diesem Intervall gezählten MAC-Pakete mit Bestätigungs-Token
NAUNChanges	Anzahl der in diesem Intervall festgestellten NAUN-Änderungen
LineErrors	Anzahl der in diesem Intervall aufgezeichneten Leitungsfehler
InternalErrors	Anzahl der in diesem Intervall aufgezeichneten internen Adapterfehler
BurstErrors	Anzahl der in diesem Intervall aufgezeichneten Trennfehler
ACErrors	Anzahl der in diesem Intervall aufgezeichneten ACE-Fehler (Address Copied Error)

Tabelle 39 (Seite 2 von 2). Inhalt der CSV-Datei für MAC-Schichtprotokolldaten für Token-Ring

Feldname	Beschreibung
AbortErrors	Anzahl der in diesem Intervall aufgezeichneten Abbruchbegrenzer
LostFrameErrors	Anzahl der in diesem Intervall aufgezeichneten Fehler aufgrund verlorener Rahmen
CongestionErrors	Anzahl der in diesem Intervall aufgezeichneten Überlastungen
FrameCopiedErrors	Anzahl der in diesem Intervall aufgezeichneten Rahmenkopiefehler (Frame Copied Error)
FrequencyErrors	Anzahl der in diesem Intervall aufgezeichneten Frequenzfehler
TokenErrors	Anzahl der in diesem Intervall aufgezeichneten Token-Fehler
SoftErrorReports	Anzahl der in diesem Intervall aufgezeichneten normalen Fehler
RingPollEvents	Anzahl der in diesem Intervall festgestellten Ringaufrufereignisse
ActiveStations	Die maximale Anzahl aktiver Stationen, die von der Sonde in diesem Intervall festgestellt wurden
dTimeIndex	Länge dieses Zeitintervalls (in Sekunden)

Sonstige Protokolldaten für Token-Ring

Der Inhalt der CSV-Datei, die für sonstige Protokolldaten für Token-Ring erstellt wird, wird in Tabelle 40 beschrieben.

Tabelle 40 (Seite 1 von 2). Inhalt der CSV-Datei für sonstige Protokolldaten für Token-Ring

Feldname	Beschreibung
Probe	Name des Protokollierungspunkts, an dem dieser Eintrag erfaßt wurde
TimeIndex	Startdatum und -zeitpunkt des Erfassungsintervalls
HistoryIndex	Identifikationsnummer der Protokollstudie, zu der dieser Eintrag gehört
Index	Schnittstelle, von der die Daten erfaßt wurden
SampleIndex	Identifikationsnummer des Eintrags innerhalb einer bestimmten Protokollstudie
IntervalStart	Startzeit des Intervalls (im Format sysUpTime)
DropEvents	Anzahl der in diesem Intervall von der Sonde gelöschten Pakete
Octets	Anzahl der in diesem Intervall in Nicht-MAC-Paketen gezählten Byte
Pkts	Anzahl der in diesem Intervall gezählten Nicht-MAC-Pakete
DataBroadcastPkts	Anzahl der in diesem Intervall gezählten Nicht-MAC-Rundsendepakete
DataMulticastPkts	Anzahl der in diesem Intervall gezählten Nicht-MAC-Pakete mit Unterstützung für selektives Rundsenden
Pkts18to63Octets	Anzahl der in diesem Intervall gezählten Nicht-MAC-Pakete von 18 bis 63 Oktett
Pkts128to255Octets	Anzahl der in diesem Intervall gezählten Nicht-MAC-Pakete von 128 bis 255 Oktett
Pkts256to511Octets	Anzahl der in diesem Intervall gezählten Nicht-MAC-Pakete von 256 bis 511 Oktett
Pkts512to1023Octets	Anzahl der in diesem Intervall gezählten Nicht-MAC-Pakete von 512 bis 1023 Oktett
Pkts1024to2047Octets	Anzahl der in diesem Intervall gezählten Nicht-MAC-Pakete von 1024 bis 2047 Oktett
Pkts2048to4095Octets	Anzahl der in diesem Intervall gezählten Nicht-MAC-Pakete von 2048 bis 4095 Oktett
Pkts4096to8191Octets	Anzahl der in diesem Intervall gezählten Nicht-MAC-Pakete von 4096 bis 8191 Oktett
Pkts8192to18000Octets	Anzahl der in diesem Intervall gezählten Nicht-MAC-Pakete von 8192 bis 18 000 Oktett

Tabelle 40 (Seite 2 von 2). Inhalt der CSV-Datei für sonstige Protokolldaten für Token-Ring

Feldname	Beschreibung
PktsGT18000Octets	Anzahl der in diesem Intervall gezählten Nicht-MAC-Pakete, die größer waren als 18 000 Oktett
dTimeIndex	Länge dieses Zeitintervalls (in Sekunden)

Anhang E. Berichtsbeschreibungen

In diesem Anhang werden die in Reporter verfügbaren Berichte beschrieben und Beispiele für die verschiedenen von der Anwendung generierten Diagramme angegeben.

Reporter enthält die folgenden Berichte für Protokoll-, Host- und Matrixdaten. Berichtart: L = Liniengrafik und H = Histogramm.

Tabelle 41. Protokollberichte

Berichtstitel	Art	Beschreibung
Segment Activity	L	Paketgeschwindigkeit des Segments
Segment Activity with Averages	L	Paketgeschwindigkeit des Segments mit Durchschnitts- und Standardabweichungen
Segment Errors	L	Kollisionen und Summe der Fehler für Ethernet-Isolation und Summe der Fehler für Token-Ring
Utilization Summary with Broadcast Packets	L	1. Segmentauslastung
	L	2. Geschwindigkeit von Rundsendepaketen und allen Paketen
Utilization Summary with Alarm Triggers	L	Auslastung, bei der die Auslastungsstufe den angegebenen Alarmauslöser überschreitet

Tabelle 42. Host-Berichte

Berichtstitel	Art	Beschreibung
Host Activity	L	Paket, das pro Sekunde an jeden ausgewählten Host gesendet wird
Host Statistics by Packet Distribution	H H	1. Gesamtzahl der gesendeten und empfangenen Pakete, Fehler, Rundsendenachrichten und Nachrichten für selektives Rundsenden 2. Die 10 Hosts mit den meisten Kontakten zu dieser Station
Top 10 Hosts by Broadcasts	H	Die 10 Sender, die die meisten Rundsendepakete gesendet haben
Top 10 Hosts by Bytes In	H	Die 10 Empfänger, die die meisten Byte empfangen haben
Top 10 Hosts by Bytes In + Out	H	Die 10 Hosts, die die meisten Byte empfangen und versendet haben
Top 10 Hosts by Bytes Out	H	Die 10 Sender, die die meisten Byte gesendet haben
Top 10 Hosts by Errors	H	Die 10 Sender, die die meisten fehlerhaften Pakete gesendet haben
Top 10 Hosts by Multicasts	H	Die 10 Sender, die die meisten Pakete mit Unterstützung für selektives Rundsenden gesendet haben
Top 10 Hosts by Packets In	H	Die 10 Empfänger, die die meisten Pakete empfangen haben
Top 10 Hosts by Packets In + Out	H	Die 10 Hosts, die die meisten Pakete empfangen und versendet haben
Top 10 Hosts by Packets Out	H	Die 10 Sender, die die meisten Pakete gesendet haben

Tabelle 43. Matrixberichte

Berichtstitel	Art	Beschreibung
Top 10 Conversations by Bytes for Host	H	Die 10 Stationen mit den meisten Kontakten zum ausgewählten Host (nach Byte)
Top 10 Conversations by Packets for Host	H	Die 10 Stationen mit den meisten Kontakten zum ausgewählten Host (nach Paketen)
Top 10 Destinations by Bytes	H	Die 10 Empfänger, die die meisten Byte empfangen haben
Top 10 Destinations by Bytes for Host	H	Die 10 Empfänger, die vom ausgewählten Host die meisten Byte empfangen haben
Top 10 Destinations by Packets	H	Die 10 Empfänger, die die meisten Pakete empfangen haben
Top 10 Destinations by Packets for Host	H	Die 10 Empfänger, die vom ausgewählten Host die meisten Pakete empfangen haben
Top 10 Sources by Bytes	H	Die 10 Sender, die die meisten Byte gesendet haben
Top 10 Sources by Bytes for Host	H	Die 10 Sender, die die meisten Byte zum ausgewählten Host gesendet haben
Top 10 Sources by Packets	H	Die 10 Sender, die die meisten Pakete gesendet haben
Top 10 Sources by Packets for Host	H	Die 10 Sender, die die meisten Pakete zum ausgewählten Host gesendet haben

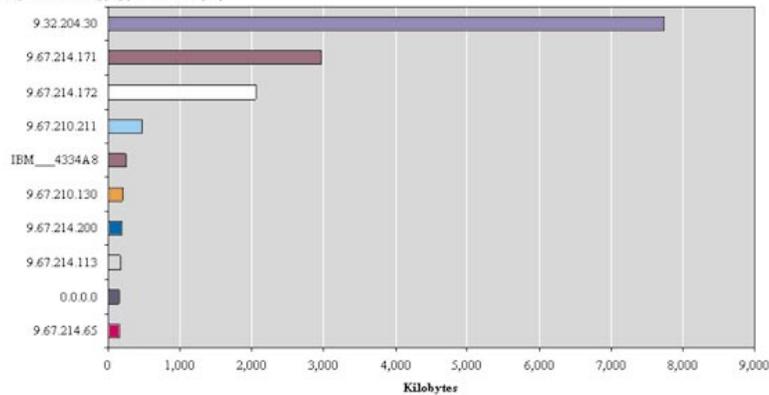
Beispiel für ein Histogramm

IBM Nways Workgroup Remote Monitor

Top 10 Hosts by Bytes In

Monday, January 12, 1998 - Tuesday, January 13, 1998

Data gathered from logging point: test2 tr0 [tr0]



Beispiel für eine Liniengrafik

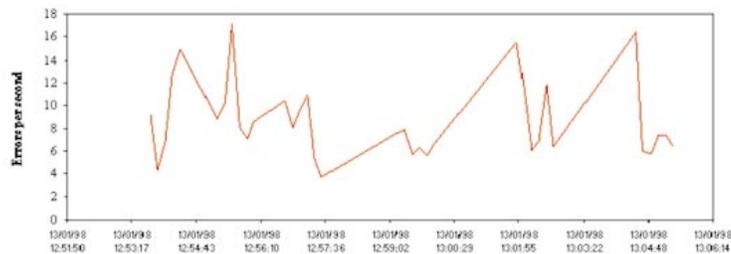
IBM Nways Workgroup Remote Monitor

Segment Errors

Monday, January 12, 1998 - Tuesday, January 13, 1998

test2 tr0 [tr0]

Logging point test2 tr0 [tr0], history 42 sampling every 10s between 13 Jan 98 12:53:26 and 13 Jan 98 13:05:15



Anhang F. HTML-Berichtsschablonen anpassen

In diesem Anhang werden die folgenden Elemente beschrieben:

- Standardschablone anpassen
- HTML-Standardschablone

Standardschablone anpassen

Wenn Reporter Berichte im HTML-Format speichert, verwendet es die HTML-Standardschablone TEMPLATE.HTML. Sie können die Standardschablone an Ihre firmentypischen Berichte anpassen und firmenspezifische Informationen hinzufügen. Die nicht editierbaren Bereiche dieser Schablone sind mit HTML-Kommentaren gekennzeichnet, z. B. `<!--AccessTemplate_Body-->`. Diese Kommentare werden in der Endausgabe durch die in Tabelle 44 angegebenen Informationen ersetzt.

Tabelle 44. Nicht editierbare HTML-Kommentare

HTML-Kommentar	In diesem Bereich wird folgende Information angezeigt
<code><!--AccessTemplate_Title--></code>	Der Berichtstitel
<code><!--AccessTemplate_Body--></code>	Der Hauptteil des Berichts
<code><!--AccessTemplate_FirstPage--></code>	Eine Verbindung zur ersten Seite des Berichts
<code><!--AccessTemplate_PreviousPage--></code>	Eine Verbindung zur vorherigen Seite des Berichts
<code><!--AccessTemplate_NextPage--></code>	Eine Verbindung zur nächsten Seite des Berichts
<code><!--AccessTemplate_LastPage--></code>	Eine Verbindung zur letzten Seite des Berichts
<code><!--LSRTemplate_Index--></code>	Eine Verbindung zu der Seite, auf der sich der Index befindet (in der Regel index.html)

Wie bei allen HTML-Dokumenten werden die Berichte je nach dem verwendeten Browser unterschiedlich angezeigt.

Standardwerte für die Formatierung sind von Microsoft Access vorgegeben. Diese befinden sich in `<!--AccessTemplate_Body-->` und können nicht editiert werden.

HTML-Standardschablone

Der Inhalt dieser Schablone wird unten angezeigt:

```
<HTML>

<!--Set page title to report title-->
<TITLE><!--AccessTemplate_Title--></TITLE>

<!--Set the background colour to white-->
<BODY BGCOLOR="#FFFFFF">

<!--Insert the main report body here-->
<!--AccessTemplate_Body-->

<!--This rule ensures that the spacing is correct in all browsers-->
<HR noshade size=0 width=0>

<!--At the bottom of the page, place links to other pages in the report-->
<TABLE BORDER=0 WIDTH=718>
<TR >
<TD ALIGN=LEFT >
<FONT SIZE=2 FACE="Arial" COLOR=#000000>
<A HREF=<!--AccessTemplate_FirstPage--> >First</A>
<A HREF=<!--AccessTemplate_PreviousPage--> >Previous</A>
<A HREF=<!--AccessTemplate_NextPage--> >Next</A>
<A HREF=<!--AccessTemplate_LastPage--> >Last</A>
</FONT>

<!--In the bottom right-hand corner, place a link to the Index page-->
<TD ALIGN=RIGHT >
<FONT SIZE=2 FACE="Arial" COLOR=#000000>
<A HREF=<!--LSRTemplate_Index--> >Index</A>
</FONT>
</TR>
</TABLE>

</BODY>
</HTML>
```

Anhang G. RMON2- und ECAM-Protokolle

Dieser Anhang enthält die folgenden Abschnitte:

- ECAM-Anwendungsdecodierungen
- RMON2-Protokollübersicht
- Vordefinierte RMON2-Protokolle

ECAM-Anwendungsdecodierungen

In diesem Abschnitt finden Sie eine Auflistung der von der RMON2-(ECAM)-SmartAgent-Software Version 0.21 unterstützten Protokolle. Die Protokolle wurden in den folgenden beiden Tabellen in Gruppen zusammengefaßt:

- Protokolle, die nur einer Protokollfamilie zugeordnet werden.
- Alle Protokollkapselungen, die mehr als einer Protokollfamilie zugeordnet werden.

Aus Gründen der Übersichtlichkeit wird jedes Protokoll nur einmal aufgeführt.

Tabelle 45 (Seite 1 von 3). Protokolle, die einer Protokollfamilie zugeordnet werden

Protokollfamilie	Protokoll	Beschreibung
AppleTalk Phase I & II	AARP	AppleTalk Address Resolution Protocol
	ADSP	AppleTalk Data Stream Protocol
	AEP	AppleTalk Echo Protocol
	ATP	AppleTalk Transaction Protocol
	DDP1	AppleTalk Datagram Delivery Protocol (kurze Kopfzeilen)
	DDP2	AppleTalk Datagram Delivery Protocol (lange Kopfzeilen)
	NBP	AppleTalk Name Binding Protocol
	RTMP	AppleTalk Routing Table Maintenance Protocol
Banyan VINES	ZIP	AppleTalk Zone Information Protocol
	VINES	Gesamterfassungsgruppe „Banyan VINES Internet Protocol“ (siehe Anmerkung auf Seite 183)
	VINES (ARP)	Banyan VINES Address Resolution Protocol
	VINES (ICP)	Banyan VINES Internet Control Protocol
	VINES (IPC)	Banyan VINES InterProcess Communications Protocol
	VINES (RTP)	Banyan VINES Routing Update Protocol
	VINES (SPP)	Banyan VINES Sequenced Packet Protocol

Tabelle 45 (Seite 2 von 3). Protokolle, die einer Protokollfamilie zugeordnet werden

Protokollfamilie	Protokoll	Beschreibung
DECnet	DEC	DECnet-Gesamterfassungsgruppe (siehe Anmerkung auf Seite 183)
	DRP	DECnet (Phase IV) Routing Protocol
	LANBridge	Digital's Bridge Management Protocol
	LAT	DECnet Local Area Transport Protocol
	LAVC/SCA	Local Area Vax Cluster/System Communication Architecture
	MOP	DECnet Maintenance Operations Protocol
	PathWorks	PC-zu-Digital-Server-Protokoll
IBM SNA	SNA	Gesamterfassungsgruppe „Systemnetzwerkarchitektur“ (siehe Anmerkung auf Seite 183)
	SNA (data)	SNA End User and Network Services Data
	SNA (flow control)	SNA Data Flow Control
	SNA (network control)	SNA Network Control
	SNA (session control)	SNA Session Control
LAN Manager	NetBIOS/NETBEUI	Network Basic Input/Output System
NetWare	IPX	Internet Packet Exchange
	NetBIOS/IPX	IPX-Implementierungen von NetBIOS
	NCP	NetWare Core Protocol
	RIP	Routing Information Protocol
	SAP	Service Advertising Protocol
	SPX	Sequenced Packet Exchange

Tabelle 45 (Seite 3 von 3). Protokolle, die einer Protokollfamilie zugeordnet werden

Protokollfamilie	Protokoll	Beschreibung
TCP/IP	AFS	Andrew File System
	ARP	Address Resolution Protocol
	DNS	Domain Name Service Protocol
	FTP	File Transfer Protocol
	GOPHER	Internet Document Search and Retrieval
	ICMP	Internet Control Message Protocol
	IGRP	Inter-Gateway Routing Protocol
	IP	Internet Protocol
	LPR/LPD	Drucker
	NetBIOS/IP (datagram)	NetBIOS Datagram Support
	NetBIOS/IP (name)	NetBIOS Name Support
	NetBIOS/IP (session)	NetBIOS Session Support
	NeWS	Network Window Service
	NFS	Network File Service
	NNTP	Network News Transfer Protocol
	NTP	Network Time Protocol
	OSPF	Open Shortest Path First
	RCMD	Remote Command
	REXEC	Remote Process Execution
	RLOGIN	Remote Login
	Router	Lokale Routing-Prozesse (520/udp)
	RWHO	Remote Who
	SMTP	Simple Mail Transfer Protocol
	SOCKS	Secure Socket Server
	SUNPRC	SUN Remote Procedure Call Protocol
	TCP	Transmission Control Protocol
	TELNET	Network Virtual Terminal Protocol
	TFTP	Trivial File Transfer Protocol
	UDP	User Datagram Protocol
	WWW	World Wide Web
	X	X Windows

Anmerkung: Die RMON2-(ECAM)-SmartAgent-Software versucht, jedes Paket so detailliert wie möglich zu identifizieren. Da es jedoch nicht möglich ist, fragmentierte Pakete vollständig einzuordnen, werden diese in einer sogenannten Gesamterfassungsklasse gezählt.

RMON2-Protokollübersicht

Jeder Eintrag in der Protokollverzeichnisstabelle einer Einheit steht für ein Protokoll, das von der Einheit decodiert und gezählt werden kann. Dabei kann es sich um Standard- oder benutzerdefinierte Protokolle handeln.

Die Einträge in der Tabelle sind nach dem jeweiligen Protokoll der Datenübertragungsschicht indexiert: das erste ist das Protokoll der MAC-Schicht, anschließend folgt die jeweilige Stufe des eingebundenen Protokolls. Beispiel:

ether2	gibt das Ethernet MAC-Protokoll an.
ether2.ip	gibt an, daß IP über das Ethernet MAC-Protokoll aktiv ist.
ether2.ip.udp	gibt an, daß UDP über IP auf einem Ethernet LAN aktiv ist.
ether2.ip.udp.snmp	gibt an, daß das Protokoll SNMP auf Anwendungsebene über Ethernet aktiv ist.

Es gibt die folgenden Protokolle der MAC-Schicht:

ether2	Ethernet II.
llc	Protokoll LLC (802.2).
snap	Abkürzung für Sub-Network Access Protocol.
vsnap	das snap zugeordnete Pseudo-Protokoll.
wgAssigned	gibt die Protokolle an, die sich nicht so einfach einem der Formate der anderen Verbindungsschichtzweige zuordnen lassen.
*	Steht für ein Protokollpräfix in Form eines Platzhalterzeichens, das alle Verbindungsschichtprotokolle nach ihrem zweiten eingebundenen Protokoll zusammenfaßt. Im nachfolgenden Beispiel ist IPX das eingebundene Protokoll der zweiten Stufe: * .ipx = ether2.ipx + llc.ipx + snap.ipx + wgAssigned.ipx

Vordefinierte RMON2-Protokolle

In diesem Abschnitt finden Sie Beispiele für vordefinierte Protokolle. Die eingebundenen Protokolle sind alphabetisch aufgelistet, die Protokolle der MAC-Schicht über die sie aktiv sind, sind markiert. Das Protokoll 802.1-bridge wird z. B. unter *.802.1-bridge und llc.802.1-bridge aufgeführt.

Tabelle 46 (Seite 1 von 3). Verfügbare Statistikvariablen zu Ethernet

Protokolle	Protokollname
802.1-bridge	802.1D Bridge Spanning Tree Protocol
aarp	AppleTalk Address Resolution Protocol
adsp	AppleTalk Data Stream Protocol
aep	AppleTalk Echo Protocol
arp	Address Resolution Protocol
atalk	AppleTalk Datagram Delivery Protocol (mit kurzen und langen Kopfzeilen)
atp	AppleTalk Transaction Protocol
bootpc	Bootstrap Protocol Client
bootps	Bootstrap Protocol Server
ccmail	Lotus® cc-Mail Protocol
dec-diag	DEC Diagnostic Protocol
dns	Domain Name Service Protocol
drp	DECnet (Phase IV) Routing Protocol
ftp	FTP-Steueranschluß
ftp-data	File Transfer Protocol Data Port
gopher	Internet Document Search and Retrieval
icmp	Internet Control Message Protocol
idp	XNS Internet Datagram Protocol
igrp	Inter-Gateway Routing Protocol
ip	Internet Protocol
ipx	Internet Packet Exchange
nbp	AppleTalk Name Binding Protocol
lat	DECnet Local Area Transport Protocol
lavc	Local Area Vax Cluster
mop	DECnet Maintenance Operations Protocol
nbt_data	NetBIOS Datagram Support
nbt_name	NetBIOS Name Support
nbt_session	NetBIOS Session Support
netbeui	LAN Manager Netbeui Protocol

Tabelle 46 (Seite 2 von 3). Verfügbare Statistikvariablen zu Ethernet

Protokolle	Protokollname
netbios-3com	3Com Netbios Protocol
news	Network Window Service
nfs	Network File Service
nntp	Network News Transfer Protocol
notes	Lotus Notes® Protocol
nov-bcast	Novell Broadcast Protocol
nov-diag	Novell Diagnostic Protocol
nov-echo	Novell Echo Protocol
nov-error	Novell Error-Handler Protocol
nov-ncp	Novell Netware Core Protocol
nov-netbios	Novell Network Basic Input/Output System
nov-pep	Novell Packet Exchange Protocol
nov-rip	Novell Routing Information Protocol
nov-sap	Novell Service Advertising Protocol
nov-sec	Novell Security Protocol
nov-spx	Novell Sequenced Packet Exchange
nov-watchdog	Novell Watchdog Protocol
nsp	DECnet Network Services Protocol
ntp	Network Time Protocol
ospf	Open Shortest Path First
pop3	Post Office Protocol Version 3
printer	Drucker
rcmd	Remote Command
rexec	Remote Process Execution
rlogin	Remote Login
router	Lokale Routing-Prozesse (520/udp)
rtmp	AppleTalk Routing Table Maintenance Protocol
rwho	Remote Who
smb	Microsoft Server Message Block Protocol
smtp	Simple Mail Transfer Protocol
sna	Systemnetzwerkarchitektur
snmp	Simple Network Management Protocol
snmptrap	Simple Network Management Protocol TRAPS
sunrpc	SUN Remote Procedure Call Protocol
tcp	Transmission Control Protocol

Tabelle 46 (Seite 3 von 3). Verfügbare Statistikvariablen zu Ethernet

Protokolle	Protokollname
telnet	Network Virtual Terminal Protocol
tftp	Trivial File Transfer Protocol
udp	User Datagram Protocol
varp	Banyan VINES Address Resolution Protocol
vecho	Banyan VINES Data Link Level Echo Protocol
vicp	Banyan VINES Internet Control Protocol
vip	Banyan VINES Internet Protocol
vipc	Banyan VINES InterProcess Communications Protocol
vipc-dgp	Banyan VINES Unreliable Datagram Protocol
vipc-rdp	Banyan VINES Reliable Datagram Protocol
vrtp	Banyan VINES Routing Update Protocol
vspp	Banyan VINES Sequenced Packet Protocol
www-http	World Wide Web HTTP
X	X Windows
xns-echo	XNS Echo Protocol
xns-error	XNS Error-Handler Protocol
xns-peg	XNS Packet Exchange Protocol
xns-rip	XNS Routing Information Protocol
xns-spp	XNS Sequenced Packet Protocol
zip	Zone Information Protocol

Tabelle 47 (Seite 1 von 5). Vordefinierte Protokolle - Protokolle der MAC-Schicht

Eingebundene Protokolle	*	ether2.	llc.	snap.	vsnap_ether2.	wgAssigned.
802.1-bridge	√		√			
aarp	√	√		√		
arp	√	√		√		
atalk	√	√		√	√	
atalk.adsp	√	√		√	√	
atalk.aep	√	√		√	√	
atalk.atp	√	√		√	√	
atalk.atp.zip	√	√		√	√	
atalk.nbp	√	√		√	√	
atalk.rtmp	√	√		√	√	
atalk.snmp	√	√		√	√	
atalk.snmptrap	√	√		√	√	
atalk.zip	√	√		√	√	
dec-diag	√	√		√		
drp	√	√		√		
drp.nsp	√	√		√		
idp	√	√		√		
idp.xns-echo	√	√		√		
idp.xns-error	√	√		√		
idp.xns-pep	√	√		√		
idp.xns-rip	√	√		√		
idp.xns-spp	√	√		√		
ip	√	√	√	√		
ip.icmp	√	√	√	√		
ip.igrp	√	√	√	√		
ip.ip	√	√	√	√		
ip.ip.icmp	√	√	√	√		
ip.ip.igrp	√	√	√	√		
ip.ip.opsf	√	√	√	√		
ip.ip.udp.ccmal	√	√	√	√		
ip.ip.udp.dns	√	√	√	√		
ip.ip.udp.nbt_data	√	√	√	√		
ip.ip.udp.nbt_data.smp	√	√	√	√		
ip.ip.udp.nbt_name	√	√	√	√		
ip.ip.udp.nbt_session	√	√	√	√		

Tabelle 47 (Seite 2 von 5). Vordefinierte Protokolle - Protokolle der MAC-Schicht

Eingebundene Protokolle	*	ether2.	llc.	snap.	vsnap_ether2.	wgAssigned.
ip.ip.udp.nbt_session.smp	√	√	√	√		
ip.ip.udp.notes	√	√	√	√		
ip.ip.udp.ntp	√	√	√	√		
ip.ip.udp.printer	√	√	√	√		
ip.ip.udp.router	√	√	√	√		
ip.ip.udp.rwho	√	√	√	√		
ip.ip.udp.snmp	√	√	√	√		
ip.ip.udp.snmptrap	√	√	√	√		
ip.ip.udp.sunrpc	√	√	√	√		
ip.ip.udp.sunrpc.nfs	√	√	√	√		
ip.ip.udp.tftp	√	√	√	√		
ip.ospf	√	√	√	√		
ip.tcp	√	√	√	√		
ip.tcp.X	√	√	√	√		
ip.tcp.ccmall	√	√	√	√		
ip.tcp.dns	√	√	√	√		
ip.tcp.ftp	√	√	√	√		
ip.tcp.ftp-data	√	√	√	√		
ip.tcp.gopher	√	√	√	√		
ip.tcp.nbt_data	√	√	√	√		
ip.tcp.nbt_data.smb	√	√	√	√		
ip.tcp.nbt_name	√	√	√	√		
ip.tcp.nbt_session	√	√	√	√		
ip.udp.rwho	√	√	√	√		
ip.udp.snmp	√	√	√	√		
ip.udp.snmptrap	√	√	√	√		
ip.udp.sunrpc	√	√	√	√		
ip.udp.sunrpc.nfs	√	√	√	√		
ip.udp.tftp	√	√	√	√		
ipx	√	√	√	√		√
ipx.nov-echo	√	√	√	√		√
ipx.nov-error	√	√	√	√		√
ipx.nov-netbios	√	√	√	√		√
ipx.nov-netbios.notes	√	√	√	√		√
ipx.nov-netbios.smb	√	√	√	√		√

Tabelle 47 (Seite 3 von 5). Vordefinierte Protokolle - Protokolle der MAC-Schicht

Eingebundene Protokolle	*	ether2.	llc.	snap.	vsnap_ether2.	wgAssigned.
ipx.nov-pep	✓	✓	✓	✓		✓
ipx.nov-pep.nov-bcast	✓	✓	✓	✓		✓
ipx.nov-pep.nov-diag	✓	✓	✓	✓		✓
ipx.nov-pep.nov-netbios	✓	✓	✓	✓		✓
ipx.nov-pep.nov-netbios.notes	✓	✓	✓	✓		✓
ipx.nov-pep.nov-netbios.smb	✓	✓	✓	✓		✓
ipx.nov-pep.nov-rip	✓	✓	✓	✓		✓
ipx.nov-pep.nov-sap	✓	✓	✓	✓		✓
ipx.nov-pep.nov-sap.notes	✓	✓	✓	✓		✓
ipx.nov-pep.nov-sap.nov-ncp	✓	✓	✓	✓		✓
ipx.nov-pep.nov-sec	✓	✓	✓	✓		✓
ip.ip.tcp	✓	✓	✓	✓		
ip.ip.tcp.X	✓	✓	✓	✓		
ip.ip.tcp.ccmil	✓	✓	✓	✓		
ip.ip.tcp.dns	✓	✓	✓	✓		
ip.ip.tcp.ftp	✓	✓	✓	✓		
ip.ip.tcp.ftp-data	✓	✓	✓	✓		
ip.ip.tcp.gopher	✓	✓	✓	✓		
ip.ip.tcp.nbt_data	✓	✓	✓	✓		
ip.ip.tcp.nbt_data.smb	✓	✓	✓	✓		
ip.ip.tcp.nbt_name	✓	✓	✓	✓		
ip.ip.tcp.nbt_session	✓	✓	✓	✓		
ip.ip.tcp.nbt_session.smb	✓	✓	✓	✓		
ip.ip.tcp.news	✓	✓	✓	✓		
ip.ip.tcp.nntp	✓	✓	✓	✓		
ip.ip.tcp.notes	✓	✓	✓	✓		
ip.ip.tcp.pop3	✓	✓	✓	✓		
ip.ip.tcp.printer	✓	✓	✓	✓		
ip.ip.tcp.rcmd	✓	✓	✓	✓		
ip.ip.tcp.rexec	✓	✓	✓	✓		
ip.ip.tcp.rlogin	✓	✓	✓	✓		
ip.ip.tcp.smtp	✓	✓	✓	✓		
ip.ip.tcp.snmp	✓	✓	✓	✓		
ip.ip.tcp.snmptrap	✓	✓	✓	✓		
ip.ip.tcp.telnet	✓	✓	✓	✓		

Tabelle 47 (Seite 4 von 5). Vordefinierte Protokolle - Protokolle der MAC-Schicht

Eingebundene Protokolle	*	ether2.	llc.	snap.	vsnap_ether2.	wgAssigned.
ip.ip.tcp.www-http	√	√	√	√		
ip.ip.udp	√	√	√	√		
ip.ip.udp.X	√	√	√	√		
ip.ip.udp.bootpc	√	√	√	√		
ip.ip.udp.bootps	√	√	√	√		
ip.tcp.nbt_session.smb	√	√	√	√		
ip.tcp.news	√	√	√	√		
ip.tcp.nntp	√	√	√	√		
ip.tcp.notes	√	√	√	√		
ip.tcp.pop3	√	√	√	√		
ip.tcp.printer	√	√	√	√		
ip.tcp.rcmd	√	√	√	√		
ip.tcp.rexec	√	√	√	√		
ip.tcp.rlogin	√	√	√	√		
ip.tcp.smtp	√	√	√	√		
ip.tcp.snmp	√	√	√	√		
ip.tcp.snmptrap	√	√	√	√		
ip.tcp.telnet	√	√	√	√		
ip.tcp.www-http	√	√	√	√		
ip.udp	√	√	√	√		
ip.udp.X	√	√	√	√		
ip.udp.bootpc	√	√	√	√		
ip.udp.bootps	√	√	√	√		
ip.udp.cmail	√	√	√	√		
ip.udp.dns	√	√	√	√		
ip.udp.nbt_data	√	√	√	√		
ip.udp.nbt_data.smb	√	√	√	√		
ip.udp.nbt_name	√	√	√	√		
ip.udp.nbt_session	√	√	√	√		
ip.udp.nbt_session.smb	√	√	√	√		
ip.udp.notes	√	√	√	√		
ip.udp.ntp	√	√	√	√		
ip.udp.printer	√	√	√	√		
ip.udp.router	√	√	√	√		
ipx.nov-pep.nov-watchdog	√	√	√	√		√

Tabelle 47 (Seite 5 von 5). Vordefinierte Protokolle - Protokolle der MAC-Schicht

Eingebundene Protokolle	*	ether2.	llc.	snap.	vsnap_ether2.	wgAssigned.
ipx.nov-pep.smb	√	√	√	√		√
ipx.nov-pep.snmp	√	√	√	√		√
ipx.nov-pep.snmptrap	√	√	√	√		√
ipx.nov-rip	√	√	√	√		√
ipx.nov-spx	√	√	√	√		√
lat	√	√		√		
lavc	√	√		√		
mop	√	√		√		
netbeui	√	√	√			
netbeui.notes	√	√	√			
netbeui.smb	√	√	√			
netbios-3com	√	√				
sna	√	√	√*			
vecho	√	√	√*	√		
vip	√	√	√*	√		
vip.varp	√	√	√*	√		
vip.vicp	√	√	√*	√		
vip.vipc	√	√	√*	√		
vip.vipc.vipc-dgp	√	√	√*	√		
vip.vipc.vipc-rdp	√	√	√*	√		
vip.vrtp	√	√	√*	√		
vip.vsp	√	√	√*	√		

Anhang H. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich.

Hinweise auf IBM Produkte, Programme oder Dienstleistungen in dieser Veröffentlichung bedeuten nicht, daß IBM diese in allen Ländern, in denen IBM vertreten ist, anbietet. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb der Produkte in Verbindung mit Fremdprodukten liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich von IBM bestätigt sind.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf englisch formuliert werden.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekanntgegeben. IBM kann jederzeit ohne Vorankündigung Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in dieser Veröffentlichung auf Web-Sites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Web-Sites dar. Das über diese Web-Sites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Web-Sites geschieht auf eigene Verantwortung.

Marken

Folgende Namen sind in gewissen Ländern Marken der IBM Corporation:

IBM

Nways

Microsoft, Windows, Windows NT und die Logos von Windows 95 und Windows 98 sind Marken der Microsoft Corporation.

Pentium ist in gewissen Ländern eine eingetragene Marke der Intel Corporation.

Sun ist in gewissen Ländern eine eingetragene Marke von Sun Microsystems, Inc.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken anderer Unternehmen sein.

Glossar

Abbruch (Abort). Entspricht einem internen Token-Ring-Fehler mit dem Unterschied, daß der Fehler während der Übertragung eines Rahmens auftritt. Ein *eingrenzbarer* Fehler.

AC. Feld für Zugriffssteuerung (Access Control) im Kopfbereich eines Rahmens.

ACE. Abkürzung für *Address Copied Error* (Fehler aufgrund kopierter Adresse). Wenn eine Station diese Meldung anzeigt, liegt der Fehler zumeist bei einer übergeordneten Station des Token-Rings mit der Adresse dieser Station. Ein *eingrenzbarer* Fehler.

Adapter (Adapter). Die Stationen in einem Token-Ring sind über einen Token-Ring-Adapter mit dem Ring verbunden. Der Adapter besitzt einen eigenen Mikroprozessor und eigene Software. Ringspezifische Funktionen, beispielsweise die Aufgaben des aktiven Monitors, beeinträchtigen daher die Leistung einer Station nicht.

Aktiver Monitor (Active Monitor). Beliebig ausgewählter, für das Generieren eines verlorenen oder in einem Token-Ring beschädigten *Tokens* verantwortlicher *Adapter*.

AMP. Abkürzung für *Active Monitor Present* (Aktiver Monitor vorhanden). Regelmäßig vom aktiven Monitor eines Token-Rings gesendeter Rahmen zum Starten des *Ringaufrufs*.

Beacon-Nachricht (Beacon). Tritt in einem Token-Ring ein Fehler auf, empfängt eine Station möglicherweise unbrauchbare Pakete (Störung des Zufuhrsignals) oder überhaupt nichts mehr (Signalverlust). Diese Station sendet dann im Rundsendebetriebs eine Beacon-Nachricht und wiederholt dabei den Fehlerrahmen mit der NAUN-Adresse (Nearest Active Upstream Neighbor). Wenn die NAUN sich in dem Rahmen mit der Beacon-Nachricht erkennt, entfernt sie sich aus dem Ring und führt einen Selbsttest durch. Stellt sie einen Fehler fest, den sie nicht beheben kann, bleibt sie außerhalb des Rings. Ansonsten begibt sie sich wieder in den Ring. Tritt kein Fehler auf, prüft die Station, die die Beacon-Nachricht gesendet hat, mit einem Selbsttest, ob sie den Fehler verursacht hat. Beacon-Betrieb ist ein Fehler der Stufe 1.

Byte (Bytes). Gesamtlänge eines Rahmens in Byte einschließlich FCS-Oktetten (Frame Checking Sequence - Rahmenprüfbitfolge).

CRC-Ausrichtungsfehler (CRC Align Error).

Ethernet-Paket mit einer Gesamtlänge zwischen 64 und 1518 Oktett (einschließlich FCS-Oktetten), ohne integrale Oktettanzahl oder mit fehlerhafter Rahmenprüfbitfolge.

ED. Abkürzung für *Ending Delimiter* (Endbegrenzer). Abgrenzendes Byte zur Markierung eines Rahmen- oder Token-Endes.

Eingrenzbarer Fehler (Isolating Error). Fehler, der auf eine bestimmte Station oder Position im Token-Ring zurückgeführt werden kann (siehe auch *Nicht eingrenzbarer Fehler*).

FCS. Abkürzung für *Frame Check Sequence* (Rahmenprüfbitfolge). Eine Art Kontrollsumme. Ein Fehler bedeutet, daß die Kontrollsumme nicht mit dem Inhalt des Rahmens übereinstimmt.

Fehler (Errors). In einem Token-Ring sind 4 Fehlerstufen definiert. Die höchste (schwerwiegendste) Fehlerstufe ist der *Beacon-Betrieb*. Die zweithöchste Stufe ist eine *Monitorkonkurrenzsituation*, danach folgt *Ringfreigabe*. Am geringfügigsten sind Fehler der Stufe 1 – sogenannte *normale Fehler*.

Fragmentpaket (Fragment Packet). Ethernet-Paket mit einer Länge von unter 64 Oktett (ohne Rahmenbits, aber mit FCS-Oktetten), ohne integrale Paketanzahl oder mit fehlerhafter Rahmenprüfbitfolge.

Freigabe (Purge). Wird im Token-Ring vom *aktiven Monitor* nach einer *Konkurrenzsituation* bei der Überwachung gesendet. Ringfreigaberahmen bereinigen das Ringsegment und geben das Signal zur Wiederaufnahme des Normalbetriebs. Ein Fehler der Stufe 2.

Frequenzfehler (Frequency Error). Tritt auf, wenn ein Adapter im Token-Ring ein Signal von seiner NAUN empfängt, das von seinem internen Takt zu stark abweicht. Wird oft durch das Verbinden mit mehr als 72 Stationen und bei 16 MB-Verarbeitung verursacht. Wird auch als *Abweichung* bezeichnet. Ein *nicht eingrenzbarer* Fehler.

Hop (Hop). Das Überqueren einer Brücke zwischen Token-Rings. Eine Zahl zwischen 1 und 8. Die Anzahl der Hops und der Hop selbst werden in der Kopfzeile eines Rahmens gespeichert.

Interner Fehler (Internal Error). Früheres Problem auf der Ursprungsstation eines Token-Rings, wurde inzwischen behoben. Oft durch Überbelastung eines Systems verursacht. Ein *eingrenzbarer* Fehler.

Jabber-Paket (Jabber Packet). Ethernet-Paket mit einer Länge von mehr als 1518 Oktett (ohne Rahmenbits, aber mit FCS-Oktetten), ohne integrale Oktettanzahl oder mit fehlerhafter Rahmenprüfbitfolge.

Kollision (Collision). Beste Schätzung der Anzahl der Kollisionen in einem Ethernet-Segment.

Konkurrenzsituation (Contention). Prozeß zur Auswahl eines neuen *aktiven Monitors*. Gewöhnlich wird die Station mit der niedrigsten Adresse ausgewählt. Ein *Fehler* der Stufe 3.

Kurzes Paket (Short Packet). Siehe *Paket geringer Länge*.

Langes Paket (Long Packet). Siehe *Überlanges Paket*.

Leitungsfehler (Line Error). Paket im Token-Ring mit einer Länge ohne integrale Oktettanzahl oder mit fehlerhafter Rahmenprüfbitfolge. Zumeist von elektronischem Rauschen oder Kabelproblemen verursacht. Ein *eingrenzbarer* Fehler.

MAC-Rahmen (MAC Frames). In einem Token-Ring gibt es zwei Hauptrahmenarten: Datenrahmen und Ringmanagementrahmen. MAC-Rahmen (*Media Access Control* - Datenträgerzugriffssteuerung) werden zur Pflege des Netzwerks und Fehlereingrenzung im Netzwerk verwendet. Mit dem LANServant-Manager können Sie sowohl ML-Rahmen (MAC Layer Frame) als auch Datenrahmen überwachen (siehe auch *Token-Rahmen*).

NAUN. Nächste aktive übergeordnete Station (Nearest Active Upstream Neighbor) in einem Token-Ring (siehe *Beacon-Nachricht*).

Nicht eingrenzbarer Fehler (Non-isolating Error). Fehler, der *nicht* auf eine bestimmte Station oder Position im Token-Ring zurückgeführt werden kann (siehe auch *Eingrenzbarer Fehler*).

Normaler Fehler (Soft Error). Fehler in einem Token-Ring, die nicht schwerwiegend genug sind, um die Funktionsfähigkeit des Rings zu stoppen (Fehler der Stufe 1). Es gibt 10 normale Fehler: Leitungsfehler, Trennfehler, Überlastung, interne Fehler, Abbruch, ACE-Fehler, Fehler aufgrund verlorener Rahmen, Token-Fehler,

Frequenzfehler und Rahmenkopiefehler (Frame Copied Error). Normale Fehler können eingrenzbar oder nicht eingrenzbar sein.

Pakete (Packets). Die Gesamtzahl der in einem Segment gefundenen Pakete (einschließlich Fehlerpakete).

Paket geringer Länge (Undersize Packet). Ein Ethernet-Paket mit einer Länge unter 64 Oktett (ohne Rahmenbits, aber mit FCS-Oktetten), ansonsten aber fehlerfrei.

Rahmen (Frame). Datensammlung (auch als *Paket* bezeichnet). In einem Token-Ring sind Token-Rahmen nur 3 Byte lang, Informationsrahmen dagegen können mehr als 18 000 Byte lang sein.

Rahmenkopiefehler (Frame Copy Error). Wird von einer Station des Token-Rings gemeldet, die annimmt, daß eine andere Station dieselbe Adresse haben könnte. Ursache dafür sind in der Regel *transparente Brücken*, die zum Ring hin geöffnet werden. Dies ist nur selten ein wirkliches Problem. Ein *nicht eingrenzbarer* Fehler.

REM. Abkürzung für *Ring Error Monitor* (Ringfehlermonitor). Funktionale Adresse in einem Token-Ring, an die Fehlermeldungen gerichtet werden.

Ringaufruf (Ring Poll). Sämtliche Stationen melden alle 7 Sekunden ihr Vorhandensein im Token-Ring. Dadurch sind die Stationen stets über ihre NAUNs informiert. Wird auch als *Nachbarmeldung* bezeichnet.

Rundsendebetrieb (Broadcast). Alle *fehlerfreien* Rahmen, die für die Rundsendeadresse bestimmt sind, d. h. an alle Stationen des Netzwerks gesendet werden. Bestimmte Rundsendenachrichten sind auf das lokale Netzwerk beschränkt, andere können auch in andere Netzwerke gesendet werden.

SD. Abkürzung für *Starting Delimiter* (Anfangsbegrenzer). Abgrenzendes Byte zur Markierung eines Rahmen- oder Token-Anfangs.

SMP. Abkürzung für *Standby Monitor Present* (Bereitschaftsmonitor vorhanden). Von einer Station im Token-Ring übertragener Rahmen als Antwort auf einen AMP-Rahmen im Zuge der Nachbarmeldung.

Sonde (Probe). Station (oder *Agent*). Sammelt Netzwerkdaten auf einem fernen Segment und gibt sie an eine zentrale Managementstation (oder einen *Client*) weiter. Wird in der Regel vom Client konfiguriert und gesteuert.

Station (Station). Jede mit dem Netzwerk verbundene Maschine, z. B. ein Datei-Server, PC, Drucker, eine Workstation oder eine Sonde.

Token-Fehler (Token Error). Wird vom aktiven Monitor gemeldet, wenn der Token beschädigt wird. Ähnlich wie ein Leitungsfehler ist auch ein Token-Fehler nicht eingrenzbar. Eine Station, die viele Token-Fehler überträgt, ist oft nicht fehlerhaft - wahrscheinlich wird der Fehler durch den aktiven Monitor verursacht.

Token-Rahmen (Token Frame). Wenn eine Station einen Token übertragen will, muß sie ihn zuvor bestätigen. Nach der Bestätigung sendet sie den Token an die untergeordnete Nachbarstation, die ihn behalten oder einfach weitergeben kann. Token-Rahmen haben eine Länge von 3 Byte.

Trennfehler (Burst Error). Schwerwiegender als ein Leitungsfehler. Ein Trennfehler wird gewöhnlich durch eine kurze Verbindungsunterbrechung des Token-Ring-Kabels oder ein kurzzeitig erhöhtes elektronisches Rauschen verursacht, was jedoch nicht stark genug ist, um den *Beacon-Betrieb* herbeizuführen. Ein *eingrenzbarer* Fehler.

Überlanges Paket (Oversize Packet). Ein Ethernet-Paket mit einer Länge von mehr als 1518 Oktett (mit FCS-Oktetten), ansonsten aber fehlerfrei.

Überlastung (Congestion). Wird von einer Station des Token-Rings gemeldet, die nicht genügend Pufferspeicher hat, um einen empfangenen Rahmen zu speichern. Da nicht gemeldet wird, wer diesen Adapter überlastet, ist dies ein *nicht eingrenzbarer* Fehler.

Unterstützung für selektives Rundsenden (Multicast). *Fehlerfreie* Pakete, die an die Adresse für selektives Rundsenden übertragen werden. Bezieht sich nicht auf Rundsendepakete. Im selektiven Rundsendebetrieb übertragene Pakete sind den im Rundsendebetrieb übertragenen Paketen vergleichbar, gelten jedoch für einen beschränkten Bereich: sie können z. B. an alle Brücken eines Rings übertragen werden.

Verlorener Rahmen (Lost Frame). Wenn eine Station einen Rahmen im Token-Ring überträgt und nicht zurückbekommt. Wird von der Ursprungsstation gemeldet. Ein *nicht eingrenzbarer* Fehler.

Index

A

- Address Translation View 98
- Adreßumsetzungstabellen 100
- Alarmnachricht-Benutzergemeinschaften
 - IP-Zieladressen 36
 - Namen 35
 - Steuerungsdialog 35
- Alarms View 94
- Anwendungsvariablen
 - History 158
 - Hosts 162
 - Ring Station 163
 - Statistics 153
- Anzeigen
 - Adreßumsetzung 98
 - Alarm 94
 - editieren 80
 - erstellen 80
 - Host 87
 - Matrix 90
 - Protokoll 84
 - Statistik 82
 - Token-Ring 92

B

- Benutzergemeinschafts-Zugriffsnamen 33
- Berichte
 - auswählen und generieren 136
 - Berichtszeitraum 137
 - Beschreibungen 175
 - drucken 140, 141
 - HTML 139
 - HTML-Schablonen 179
 - Kopf- und Fußzeilen 139
 - laden, gespeicherte 141
 - Parameter 137
 - speichern 139
 - Voranzeige 139
- Berichtsschablonen, HTML 179

C

- Capture
 - konfigurieren 104

Capture (*Forts.*)

- Pakete lesen 116
- Puffer 104
- Start- und Stoppereignisse 110
- starten 103

Collector

- Adreßumsetzungsebene 123
- beenden 129
- Datensammlung, starten 129
- Datensammlung, stoppen 128
- Datensammlungen, anlegen 125
- konfigurieren, Datenquellen 123
- Schnittstelle 16
- starten 122
- Übersicht 121

Conversation Trace and Analysis 118

CSV-Dateien

- Host-Format 169
- MAC-Schichtprotokolldaten für Token-Ring 171
- Matrixformat 170
- Protokollformat 168
- sonstige Protokollaten für Token-Ring 173

D

Daten

- archivieren 148
- löschen 147
- Sammlungen, anlegen 125
- verwalten 143
- zusammenfassen 146

Datenbank

- anzeigen 135
- auswählen 133
- Berichte 136
- erstellen 133
- importieren 134
- komprimieren 149
- öffnen 133
- reparieren 150

Datensammlung

- ändern, Konfigurationen 128
- Datum-/Zeiteinstellungen 27
- importieren 56
- löschen 59
- starten 57, 129

Datensammlung (*Forts.*)
stoppen 59, 128
Decode
Conversation Trace and Analysis 118
ECAM-Anwendung 181
lesen, erfaßte Pakete 116
starten 116
Diagramme
Event Distribution 74
Network Statistics 71
Packet Rates 70
Packet Size Distribution 69
Ring Status 74
Top 10 Hosts by Error Rate 73
Top 10 Hosts by Packet Rate 72
Top 10 Receivers 73

E

ECAM-Anwendungsdecodierungen 181
Ereignisse, Start und Stopp 110
Erfaßte Pakete
konfigurieren 104
lesen 116
Puffer 104
speichern und laden 119
Start- und Stoppereignisse 110
starten 103
Erfaßtes Paket
speichern und laden 119

F

Filtereditor
Schablonen 114
verwenden 112
Firmware
herunterladen 26
Versionen 26
Format, Dialog 9
Funktionsleiste 13

H

Hardware, Versionen 26
History View 84
Host View 87
HTML-Berichtsschablonen 179
Hysterese-Zone 98

I

IP-Adresse 28

K

Kaltstart, zurücksetzen 29
Konfigurieren, virtuelle Schnittstellen 39

L

Leistungsrichtlinien 165
Lieferantenpräfixe 63

M

Marken 194
Matrix View 90
Menüleiste
Rmonview 11, 17
Translator 55
Viewman 8

N

Namenumsetzungsebene 62
Network Statistics 71
Nways Remote Monitor
Grundlagen 4
Grundlageninformationen 2
Übersicht 1
verwenden 2
Nways Remote Monitor, Schnittstelle 7

P

Packet Capture
konfigurieren 104
lesen 116
Puffer 104
speichern und laden 119
Start- und Stoppereignisse 110
starten 103
Packet Capture und Decode 103
Packet Decode
Conversation Trace and Analysis 118
lesen, erfaßte Pakete 116
starten 116
PACMIB aktivieren und inaktivieren 37

- Paket
 - Größenzuordnung 69
 - Raten 70
- Protocol Distribution
 - anzeigen, Tabellen 102
 - starten, Anzeige 101
 - verwenden 101
- Protokolldecodierungen 151
- Protokolle
 - benutzerdefiniert 48
 - Decodierungen 151
 - hinzufügen 49
 - löschen 49
 - RMON2 und ECAM 181
 - RMON2-Tabellen aktualisieren 50
 - Verzeichnis 48
- Puffer
 - ändern, Capture 109
 - erstellen, neue für Capture 105
 - laden, Capture 110
 - verwenden 104

R

- Reporter
 - anzeigen, Datenbank 135
 - auswählen, Datenbank 133
 - generieren, Berichte 137
 - importieren, Daten 134
 - komprimieren, Datenbank 149
 - reparieren, Datenbank 150
 - Schnittstelle 18
 - starten 132
 - Übersicht 131
- Ringstationsanzeige 92
- RMON
 - Address Translation View 98
 - Alarms View 94
 - Host View 87
 - konfigurieren 80
 - Matrix View 90
 - Protokollanzeigen 84
 - Ring Station View 92
 - starten, Anwendungen 78
 - Statistics View 82
 - Übersicht 3
- RMON/RMON2-Tabellen 43
- RMON2- und ECAM-Protokolle 181
- RMON2-Modus definieren 38

- RMON2-Protokolle
 - aktualisieren, Tabellen 50
 - Übersicht 184
 - vordefiniert 185
- Rmonview
 - Anwendungsanzeigebereich 14
 - Format, Dialog 9
 - Funktionsleiste 13
 - Menüleiste 11, 17
 - Schnittstelle 9
 - starten 78
 - starten, Anwendungen 78

S

- Schnittstellen
 - Collector 16
 - Reporter 18
 - Rmonview 9
 - Viewman 7
- SmartAgent-Firmware
 - aktivieren 46
 - Autostart-Tabelle 47
 - inaktivieren 47
 - SmartAgent Maintenance, Dialog 45
 - verwalten 44
- Sonden
 - Alarmnachricht-Benutzergemeinschaften 34
 - benutzerdefinierte Protokolle 48
 - definieren 22
 - Device Configuration 21
 - IP-Adresse 28
 - PACMIB 37
 - RMON2 54
 - SmartAgent 53
 - Standard-Gateway 29
 - statische Leitwege 36
 - Teilnetzmaske 28
 - verwalten 24
 - virtuelle Schnittstellen 39
 - Zugriffssteuerungstabellen 32
 - zurücksetzen 29
- Standard-Gateway 29
- Start- und Stoppereignisse 110
- Stationen
 - automatische Erkennung 53
 - Lieferantenpräfixe 63
 - manuelle Einrichtung 60
 - Namenumsetzungsebene 62
 - starten, Translator 54

Stationsnamen definieren 53
Statische Leitwege definieren 36
Statistics View 82

T

Teilnetzmaske 28
Translator
 Hauptfenster 54
 Menüleiste 55
 starten 54

U

Unterteilung 143

V

Variablen
 History 158
 Hosts 162
 Ring Station 163
 Statistics 153
Verwalten, Daten 143
Viewman
 Diagramme 68
 konfigurieren 66
 Menüleiste 8
 starten 66
 starten, Anwendungen 79
Viewman-Schnittstelle 7
Virtuelle Schnittstellen
 erstellen 39
 konfigurieren 39
 löschen 42
 vordefinierte Kanäle 41

W

Warmstart, zurücksetzen 29

Z

Zugriff
 Benutzergemeinschafts-Zugriffsnamen 33
 Sicherheitsstufen 34
 Steuerungstabellen 32
Zurücksetzen, Sonden 29

Antwort

Nways Remote Monitor für Windows NT
Benutzerhandbuch

IBM Form SA12-4796-00

Anregungen zur Verbesserung und Ergänzung dieser Veröffentlichung nehmen wir gerne entgegen.
Bitte informieren Sie uns über Fehler, ungenaue Darstellungen oder andere Mängel.

Senden Sie Ihre Anregungen bitte an die angegebene Adresse.

IBM Deutschland
Informationssysteme GmbH
SW NLS Center

70548 Stuttgart

Kommentare:

Zu Ihrer weiteren Information:

Zur Klärung technischer Fragen sowie zu Liefermöglichkeiten und Preisen wenden Sie sich bitte entweder an Ihre *IBM Geschäftsstelle*, Ihren *IBM Geschäftspartner* oder Ihren *Händler*. Unsere Telefonauskunft „**Hallo IBM**“ (Telefonnr.: 0180 3/31 3233) steht Ihnen ebenfalls zur Klärung allgemeiner Fragen zur Verfügung.



SA12-4796-00

