



Nways Manager Remote Monitor

# Benutzerhandbuch





Nways Manager Remote Monitor

# Benutzerhandbuch

**Anmerkung**

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter Anhang H, „Hinweise“ auf Seite 211 gelesen werden.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs  
*Nways Manager Remote Monitor - User's Guide*,  
IBM Form SA33-0367-04,  
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

<b>Zu diesem Handbuch</b> . . . . .	xiii
Zur Verwendung dieses Handbuchs . . . . .	xiii
Konventionen in diesem Handbuch . . . . .	xiv
Konventionen zur Benutzerschnittstelle . . . . .	xiv
In diesem Handbuch verwendete Terminologie . . . . .	xv
Nützliche WWW-Sites . . . . .	xv
Nways Management . . . . .	xv
SNMP . . . . .	xv
RMON . . . . .	xv
Verschiedenes . . . . .	xvi
Online-Hilfefunktion . . . . .	xvi
<b>Kapitel 1. Übersicht über Nways Manager Remote Monitor</b> . . . . .	1
Was ist Nways Manager Remote Monitor? . . . . .	1
Nways Manager Remote Monitor zur Überwachung des Netzwerks verwenden . . . . .	2
Wie funktioniert Nways Manager Remote Monitor? . . . . .	2
Übersicht über RMON . . . . .	2
Grundlagen von Nways Manager Remote Monitor . . . . .	4
Unterstützte Arten von Schnittstellen . . . . .	6
<b>Kapitel 2. Nways Manager Remote Monitor starten und konfigurieren</b> . . . . .	7
Übersicht . . . . .	7
Nways Manager Remote Monitor starten . . . . .	7
Das Dialogfenster Device Administration aufrufen . . . . .	9
Einheiten installieren und die Installation überprüfen . . . . .	10
Eine neue Einheit installieren . . . . .	10
Einen Einheiten eintrag ändern . . . . .	11
Einen Einheiten eintrag löschen . . . . .	11
Einen Einheiten eintrag überprüfen . . . . .	12
Grundlegende Einheitsdaten anzeigen . . . . .	13
Device and System Details . . . . .	14
Interfaces . . . . .	14
RMON- und RMON2-Tabellen verwalten . . . . .	15
<b>Kapitel 3. Einheiten von Nways Manager Remote Monitor aus konfigurieren</b> . . . . .	19
Auf Einheitenkonfigurationen zugreifen . . . . .	19
Systemparameter einstellen . . . . .	22
Informationen zu Hardware und Firmware anzeigen . . . . .	22
Eine Einheit zurücksetzen . . . . .	22
RMON2-Funktionalität . . . . .	25
Firmware herunterladen . . . . .	26
IP-Adresse, Teilnetzwerkmaske und Ringnummer einstellen . . . . .	29
IP-Adresse und Teilnetzwerkmaske einstellen . . . . .	29
Ringnummer einstellen . . . . .	30
Serielle Verbindungen herstellen . . . . .	31

Serielle Schnittstellen konfigurieren . . . . .	32
SLIP-Verbindungen konfigurieren . . . . .	33
Statische Leitwege, Standard-Gateway und Echointervall einstellen . . . . .	35
Statische Leitwege einstellen . . . . .	35
Standard-Gateway einstellen . . . . .	36
Echointervall einstellen . . . . .	36
Auf Steuertabellen zugreifen . . . . .	36
Namen von Benutzergemeinschaften festlegen . . . . .	38
Einzelnen Workstations Sicherheitsstufen zuordnen . . . . .	39
Einen Client-Eintrag ändern . . . . .	39
Einen Client-Eintrag löschen . . . . .	39
Benutzergemeinschaften für Alarmnachrichten festlegen . . . . .	40
Namen für Benutzergemeinschaften für Alarmnachrichten festlegen . . . . .	41
Virtuelle Schnittstellen konfigurieren . . . . .	43
Virtuelle Schnittstellen erstellen . . . . .	44
Stufe der Adreßumsetzung einstellen . . . . .	49
Schnittstellen umbenennen . . . . .	51
Benutzerdefinierte Protokolle verwalten . . . . .	52
Protokollverzeichnis anzeigen . . . . .	53
Ein Protokoll hinzufügen . . . . .	54
Ein Protokoll löschen . . . . .	55
Herstellerpräfixe angeben . . . . .	55
<b>Kapitel 4. Hauptfenster von Nways Manager Remote Monitor . . . . .</b>	<b>57</b>
Übersicht . . . . .	57
Beschreibung des Hauptfensters von Nways Manager Remote Monitor . . . . .	57
Menüleiste . . . . .	58
Knopfleiste . . . . .	59
Zusammenfassungsbereich . . . . .	59
Alarmleiste . . . . .	60
Statusleiste . . . . .	60
Hauptfenster anpassen . . . . .	60
Auf mehrere Fenster zugreifen . . . . .	62
Informationen im Hauptfenster lesen . . . . .	62
Hauptfenster anhalten . . . . .	62
Beschreibung der verfügbaren Diagramme . . . . .	63
Diagramme über Nways Manager Remote Monitor ausgeben . . . . .	73
Druckvorgaben einstellen . . . . .	75
<b>Kapitel 5. RMON-Anzeigen verwenden . . . . .</b>	<b>77</b>
Format von Dialogfenstern . . . . .	77
Angepaßte Anzeigen bearbeiten und erstellen . . . . .	78
Dialogfenster Station Select verwenden . . . . .	80
Liste Station ändern . . . . .	81
Statistische Anzeigen . . . . .	84
Tabellarische Darstellung . . . . .	84
Skalendarstellung . . . . .	85
Diagrammdarstellung . . . . .	87

Anzeige Statistics verwenden . . . . .	89
Anzeige Statistics konfigurieren . . . . .	89
Vordefinierte Statistikanzeigen . . . . .	91
Anzeige History verwenden . . . . .	92
Anzeige History konfigurieren . . . . .	92
Vordefinierte Protokollanzeigen . . . . .	95
Anzeige Host verwenden . . . . .	95
Anzeige Host konfigurieren . . . . .	96
Vordefinierte Host-Anzeigen . . . . .	98
Anzeige Matrix verwenden . . . . .	98
Anzeige Matrix konfigurieren . . . . .	99
Anzeige Matrix lesen . . . . .	100
Vordefinierte Matrixanzeigen . . . . .	100
Anzeige Ring Station verwenden . . . . .	101
Anzeige Ring Station konfigurieren . . . . .	101
Vordefinierte Anzeigen . . . . .	102
<b>Kapitel 6. Alarmnachrichten . . . . .</b>	<b>103</b>
Übersicht über Alarmnachrichten . . . . .	103
Alarmnachrichten konfigurieren . . . . .	103
Dialogfenster Stations verwenden . . . . .	107
<b>Kapitel 7. Paketerfassung und Entschlüsselung . . . . .</b>	<b>109</b>
Übersicht über die Anwendungen "Capture" und "Decode" . . . . .	109
Übersicht über die Struktur von Paketen . . . . .	109
Anwendung Capture verwenden . . . . .	110
Erfassungspuffer verwenden . . . . .	110
Neue Erfassungspuffer erstellen . . . . .	111
Einen Erfassungspuffer sichern . . . . .	116
Erfassungspuffer ändern . . . . .	117
Vordefinierte Erfassungspuffer verwenden . . . . .	117
Erfassungspuffer aus einer Datei laden . . . . .	120
Neue Start- und Stoppereignisse erstellen . . . . .	120
Funktion Filter Editor verwenden . . . . .	122
Platzhalterzeichen in Filterschablonen verwenden . . . . .	122
Einen Filter definieren . . . . .	122
Dialogfenster Stations verwenden . . . . .	124
Erfasste Pakete entschlüsseln . . . . .	125
Pakete mit Hilfe der Anwendung Decode erfassen . . . . .	126
Pakete mit Hilfe der Anwendung Decode hochladen . . . . .	127
Filtern nach dem Erfassen . . . . .	127
Funktionen Conversation Trace und Analysis . . . . .	128
Erfasste Pakete sichern und laden . . . . .	130
Pakete sichern . . . . .	130
Erfasste Pakete laden . . . . .	131
<b>Kapitel 8. Zusätzliche Funktionen von Nways Manager Remote Monitor . . . . .</b>	<b>133</b>
Anwendung Address Map . . . . .	133

Funktionen	133
Adreß-Map-Tabellen anzeigen	134
Adressentabelle	134
Eine RMON2-kompatible Einheit verwenden	134
Software RMON2 (ECAM) SmartAgent verwenden	135
Tabelle Duplicate Addresses	136
Anwendung Protocol Distribution	136
Protokollverteilungsdaten anzeigen	136
Protokollverteilungsdaten verwenden	137
Anzeigeoptionen	137
Anwendung Data Export	138
Anwendung Data Collector verwenden	140
Anwendung Collector starten	140
Protokollierungspunkte erstellen	141
Neue Konfigurationen zur Datensammlung erstellen	143
Eine neue Konfiguration für die Anwendung "Collector" hinzufügen	144
Konfigurationen kopieren und ändern	146
Datensammlungen aktivieren und inaktivieren	147
Datensammlung aktivieren	147
CSV-Dateien	148
<b>Anhang A. Integration von NetView für AIX</b>	<b>149</b>
Sonden in IBM NetView einrichten	149
RMON-Anwendungen in IBM NetView verwenden	150
Anwendungen von Nways Manager Remote Monitor starten	151
NetView Tools	152
<b>Anhang B. Integration von OpenView</b>	<b>153</b>
Sonden in HP OpenView einrichten	153
RMON-Anwendungen in HP OpenView verwenden	154
Anwendungen von Nways Manager Remote Monitor starten	155
OpenView-Tools	156
<b>Anhang C. Liste der Protokolle und Protokollentschlüsselungen</b>	<b>157</b>
Entschlüsselungen für RMON-Anwendungen	157
Entschlüsselungen für ECAM-Anwendungen	157
Übersicht über RMON2-Protokolle	161
Vordefinierte RMON2-Protokolle	162
Benutzerdefinierte Protokolle	169
<b>Anhang D. Anwendung Roving Analysis Port und PACMIB</b>	<b>171</b>
Anwendung Roving Analysis Port	171
Status	171
Konfiguration	172
PACMIB-Funktionalität verwenden	176
<b>Anhang E. Variablen in Anzeigen und Anwendungen</b>	<b>179</b>
Statistikvariablen	179



Verfügbare Variablen für Ethernet	179
Verfügbare Variablen für FDDI	180
Statistische Variablen	181
Protokollvariablen	183
Verfügbare Variablen für FDDI	184
Verfügbare Variablen für Token-Ring	184
Host-Variablen	187
Ringstationsvariablen	187
ECAM-Variablen	189
Protokollstatistikvariablen	189
Host-Protokollvariablen	189
Matrixprotokollvariablen	190
<b>Anhang F. Anwendung ECAM (Enterprise Communications Analysis Module)</b>	191
Übersicht über die Anwendung ECAM	191
Software SmartAgent herunterladen	192
Prozedur zum Herunterladen	193
Anwendungen aktivieren	194
Anwendungen inaktivieren	195
Tabelle Auto Boot	196
ECAM starten	197
ECAM-Anzeigen	197
Tabelle (Statistics, Host und Matrix)	197
Skala (Statistics, Host und Matrix)	197
Liniendiagramm (Statistics, Host und Matrix)	198
Balken-, Stapelbalken- und Tortendiagramm (nur Protocol Distribution)	198
Anzeigeoptionen	198
Aktualisierung	199
ECAM-Statistiken erstellen	200
Eine Datenquelle hinzufügen oder ändern	200
Protokollstatistiken	201
Anzeige Protocol Statistics konfigurieren	201
Host-Protokollstatistiken	203
Anzeige Host Protocol Statistics konfigurieren	203
Matrixprotokollstatistiken	205
Anzeige Matrix Protocol Statistics konfigurieren	205
Anwendung Protocol Distribution	206
Anzeige Protocol Distribution konfigurieren	206
Anzeige Protocol Distribution	208
<b>Anhang G. Häufig auftretende Probleme</b>	209
<b>Anhang H. Hinweise</b>	211
Marken	211
<b>Glossar</b>	213

**Antwort** . . . . . 219

---

## Abbildungsverzeichnis

1.	Dialogfenster "Modify Current View" . . . . .	8
2.	Dialogfenster "Device Administration" . . . . .	9
3.	Dialogfenster "Device List Editor" . . . . .	10
4.	Dialogfenster "Device Information" . . . . .	13
5.	Dialogfenster "Table Editor" . . . . .	15
6.	Dialogfenster "Delete Table Entry" . . . . .	17
7.	Dialogfenster "Device Configuration" . . . . .	20
8.	Indezunge "Firmware Download" . . . . .	26
9.	Indezunge "Network" . . . . .	30
10.	Indezunge "Serial Links" . . . . .	31
11.	Indezunge "Routing" . . . . .	35
12.	Indezunge "Community Access" . . . . .	37
13.	Indezunge "Traps" . . . . .	41
14.	Dialogfenster "Virtual Interfaces Editor" . . . . .	44
15.	Dialogfenster "Channel Editor" . . . . .	46
16.	Dialogfenster "Delete Virtual Interface Tables List" . . . . .	48
17.	Dialogfenster "Address Translation" . . . . .	50
18.	Dialogfenster "Edit Interface Description" . . . . .	51
19.	Dialogfenster "Protocol Directory Manager" . . . . .	53
20.	Dialogfenster "New Protocol" . . . . .	54
21.	Hauptfenster von Nways Manager Remote Monitor . . . . .	58
22.	Dialogfenster "Edit Community Name" . . . . .	61
23.	Diagramm "Packet Size Distribution" . . . . .	64
24.	Diagramm "Packet Rates" . . . . .	65
25.	Diagramm "Network Statistics" . . . . .	66
26.	Diagramm "Top 10 Hosts (Packet Rate)" . . . . .	67
27.	Diagramm "Top 10 Hosts (Error Rate)" . . . . .	68
28.	Diagramm "Top 10 Receivers" . . . . .	69
29.	Diagramm "Event Distribution" . . . . .	70
30.	Anzeige "Ring-Status" . . . . .	71
31.	Dialogfenster "Print" . . . . .	73
32.	Beispiel für ein Dialogfenster einer Anzeige . . . . .	77
33.	Dialogfenster "Edit User View" . . . . .	79
34.	Dialogfenster "Station Select" . . . . .	80
35.	Dialogfenster "Station List Editor" . . . . .	82
36.	Tabellarische Darstellung . . . . .	84
37.	Dialogfenster "Dial Reset" . . . . .	86
38.	Diagrammdarstellung . . . . .	87
39.	Beispiel für ein vergleichendes Statistikdiagramm . . . . .	90
40.	Dialogfenster "History Entry Creation" . . . . .	93
41.	Beispiel für die Anzeige "History" in Tabellendarstellung und in Diagrammdarstellung . . . . .	94
42.	Beispiel für die Anzeige "Host" in Skalen- sowie in tabellarischer und in Diagrammdarstellung . . . . .	97
43.	Beispiel für die Anzeige "Matrix" in tabellarischer und in Diagrammdarstellung . . . . .	99

44.	Dialogfenster "Alarms" . . . . .	104
45.	Dialogfenster "Alarm Entry Creation" . . . . .	105
46.	Hysteresesezone . . . . .	106
47.	Dialogfenster "Stations" . . . . .	107
48.	Hauptdialogfenster "Capture" . . . . .	110
49.	Dialogfenster "Edit Packet Capture" . . . . .	111
50.	Dialogfenster "Interfaces" . . . . .	112
51.	Dialogfenster "Start/Stop Event" . . . . .	113
52.	Dialogfenster "Buffer Control" . . . . .	115
53.	Dialogfenster "Buffer Save/Load" . . . . .	118
54.	Dialogfenster "Channel Event Editor" . . . . .	121
55.	Dialogfenster "Filter Editor" . . . . .	123
56.	MAC-Adressen für Ziel und für Quelle eingeben . . . . .	124
57.	Dialogfenster "Decode" . . . . .	125
58.	Knopf "Capture" . . . . .	126
59.	Dialogfenster "Conversation Trace" . . . . .	128
60.	Dialogfenster "File" . . . . .	130
61.	Beispiel für eine Tabelle des Typs "Data Export" . . . . .	138
62.	Dialogfenster "Data Export" . . . . .	139
63.	Hauptdialogfenster der Anwendung "Collector" . . . . .	140
64.	Dialogfenster "Log Configuration Editor" . . . . .	141
65.	Dialogfenster "Device Interrogation Progress" . . . . .	142
66.	Dialogfenster "View Switch Status" . . . . .	172
67.	Dialogfenster "Change Analyzer Port" . . . . .	173
68.	Dialogfenster "Analyzer Port Configuration" . . . . .	174
69.	Dialogfenster "Roving Analysis Configuration" . . . . .	175
70.	Beispiele für Tabellen der Typen "Port to Host" und "Host to Port" . . . . .	177
71.	Dialogfenster "SmartAgent Maintenance" . . . . .	193
72.	Dialogfenster "ECAM Statistics" . . . . .	202
73.	Dialogfenster "ECAM Host" . . . . .	204
74.	Beispiel für ein Diagramm des Typs "Protocol Distribution" mit Datenkennsätzen . . . . .	207

## Tabellen

1.	Wo Sie spezifische Informationen finden	xiii
2.	Hinweissymbole	xiv
3.	Textliche Konventionen	xiv
4.	Konventionen zu Knöpfen in Dialogfenstern	xiv
5.	Indezungen des Dialogfensters "Device Configuration"	21
6.	Product Information	22
7.	Erhaltene und verlorene Konfigurations- und RMON-Daten	23
8.	Erhaltene und verlorene RMON2-Daten	24
9.	Mögliche Gründe für einen TFTP-Fehler	28
10.	Verschiedene Zugriffsebenen (zur Sicherheit)	38
11.	Vordefinierte Kanäle	45
12.	Umkehrknopf	47
13.	Stufen der Adreßumsetzung	51
14.	Knöpfe in der Knopfleiste des Hauptfensters	59
15.	Je nach Verkabelungstyp verfügbare Diagramme	63
16.	Vom Verkabelungstyp abhängige Variablen des Diagramms "Network Statistics"	66
17.	FDDI-Variablen in der Anzeige "Ring Status"	72
18.	Token-Ring-Variablen in der Anzeige "Ring Status"	72
19.	Variablen der Kopfzeile für die Ausgabe	74
20.	Skalendarstellung	85
21.	Menüs der Diagrammdarstellung	88
22.	Vordefinierte Statistikanzeigen	91
23.	Vordefinierte Protokollanzeigen	95
24.	Vordefinierte Host-Anzeigen	98
25.	Spalten der Matrix	100
26.	Vordefinierte Matrixanzeigen	100
27.	Vordefinierte Ringstationsanzeigen	102
28.	Aktivierungsknöpfe	114
29.	Umkehrknopf	114
30.	Beschreibung der vordefinierten Filter	119
31.	Farbcodierungen der Feldarten	124
32.	Anzeigeoptionen	137
33.	Funktionen des Hauptdialogfensters der Anwendung "Collector"	143
34.	CSV-Dateien	148
35.	Optionen der NetView-Tools	152
36.	Optionen der OpenView-Tools	156
37.	Liste mit unterstützten Protokollentschlüsselungen für die einzelnen Protokollfamilien	157
38.	Protokolle, die nur einer Protokollfamilie zugeordnet sind	158
39.	Protokolle, die mehreren Protokollfamilien zugeordnet sind	160
40.	Protokollnamen	162
41.	Vordefinierte Protokolle	164
42.	Erweiterbare Protokolle und Werte für "maxChildren"	169
43.	Unterstützte Karten für 3Com CoreBuilder 5000	176

44.	Verfügbare Statistikvariablen für Ethernet . . . . .	179
45.	Verfügbare Statistikvariablen für FDDI . . . . .	180
46.	Verfügbare statistische Variablen für Token-Ring . . . . .	181
47.	Verfügbare Protokollvariablen für Ethernet . . . . .	183
48.	Verfügbare Protokollvariablen für FDDI . . . . .	184
49.	Verfügbare Protokollvariablen für Token-Ring . . . . .	184
50.	Verfügbare Host-Variablen für Ethernet, Token-Ring und FDDI . . . . .	187
51.	Verfügbare Ringstationsvariablen für Token-Ring . . . . .	187
52.	ECAM-Protokollstatistikvariablen . . . . .	189
53.	ECAM-Host-Protokoll-Variablen . . . . .	189
54.	ECAM-Matrixprotokollvariablen . . . . .	190
55.	ECAM-Anzeigen . . . . .	197
56.	Anzeigeoptionen . . . . .	198

---

## Zu diesem Handbuch

In diesem Handbuch wird Nways Manager Remote Monitor beschrieben. Ferner wird erklärt, wie Sie diese Anwendung verwenden können, um Echtzeit- und Protokollinformationen zu Ihrem Netzwerk zu erhalten.

Eine Beschreibung der Mindestanforderungen für die Systemkonfiguration und der unterstützten Betriebssysteme sowie der mindestens benötigten Agenten-Firmware und Softwareversionen von SmartAgent sind in den Hinweisen zum jeweiligen Release enthalten, die zusammen mit diesem Produkt geliefert werden. In diesen sind auch die aktuellsten Informationen zu Nways Manager Remote Monitor enthalten.

Dieses Handbuch richtet sich an Netzadministratoren. Erfahrung im Umgang mit LAN-Operationen (Local Area Network) wird vorausgesetzt.

---

## Zur Verwendung dieses Handbuchs

In Tabelle 1 wird angegeben, wo Sie spezifische Informationen finden können.

*Tabelle 1. Wo Sie spezifische Informationen finden*

<b>Informationen</b>	<b>Enthalten in</b>
Eine Übersicht über die Anwendungen von Nways Manager Remote Monitor und eine Einführung in den Standard von Remote Monitoring.	Kapitel 1
Informationen zum Kontaktieren und Anzeigen von Netzwerkeinheiten unter Verwendung von Nways Manager Remote Monitor.	Kapitel 2
Informationen zum Ausführen von Einheitenkonfigurationen.	Kapitel 3
Prozeduren zum Konfigurieren des Hauptfensters, zum Öffnen mehrerer Fenster und zum Lesen von Diagrammen im Hauptfenster.	Kapitel 4
Prozeduren zum Sammeln aktueller statistischer Daten zum Netzwerk.	Kapitel 5
Prozeduren zur Überwachung spezifischer Ereignisse im Netzwerk.	Kapitel 6
Prozeduren zum Erfassen von Daten aus dem Netzwerk und zum Ausführen von Paketentschlüsselungen und -analysen.	Kapitel 7
Prozeduren zur Verwendung der folgenden Anwendungen: Address Mapping, Protocol Distribution, Data Export und Data Collector.	Kapitel 8
IBM NetView und Prozeduren zum Integrieren von Nways Manager Remote Monitor und HP OpenView.	Anhang A und Anhang B
Eine Liste mit unterstützten Entschlüsselungen und einer wichtigen Dokumentation sowohl für Anzeigen von RMON als auch für ECAM-Anwendungen.	Anhang C
Prozeduren zur Verwendung von RAP (Roving Analysis Port) und PACMIB.	Anhang D
Eine Liste der in den RMON-Anzeigen und ECAM-Anwendungen verwendeten Variablen.	Anhang E
Prozeduren zum Anzeigen von Statistiken über die Vermittlungsschicht (RMON2/ECAM).	Anhang F
Eine Liste mit häufig auftretenden Problemen.	Anhang G

---

## Konventionen in diesem Handbuch

In Tabelle 2 und Tabelle 3 sind Konventionen aufgeführt, die in diesem Handbuch durchgängig verwendet werden.

---

Tabelle 2. Hinweissymbole

Art	Beschreibung
Anmerkung	Wichtige Funktionen oder Anweisungen.
Achtung	Gefahr eines Systemschadens oder von Datenverlust.

---

Tabelle 3. Textliche Konventionen

Konvention	Beschreibung
Wiedergabe von Befehlen im Text	Diese Schriftbild wird für die Wiedergabe von Befehlen verwendet, die Sie eingeben. Beispiel: SETDefault !0 -IP NETaddr = 0.0.0.0
Tasten	Wenn sich der Text auf spezifische Tasten bezieht, werden diese mit Hilfe ihrer Bezeichnungen angegeben, wie z. B. "die Rückföhrtaste" oder "die Abbruchtaste", oder sie werden als <b>Return</b> oder <b>Esc</b> bezeichnet.  Wenn Sie mehrere Tasten gleichzeitig drücken müssen, werden diese Tasten durch ein Pluszeichen miteinander verbunden wie z. B. in der folgenden Anweisung: "Drücken Sie <b>Ctrl+Alt+Del</b> ".

---

## Konventionen zur Benutzerschnittstelle

Die folgenden Knöpfe werden in Dialogfenstern der Benutzerschnittstelle von Nways Manager Remote Monitor verwendet:

---

Tabelle 4. Konventionen zu Knöpfen in Dialogfenstern

Knopf	Funktion
Apply	Änderungen vornehmen.
Cancel	Änderungen zurücknehmen und zur vorherigen Ebene zurückkehren.
Close	Zur vorherigen Ebene zurückkehren.
Help	Auf die Online-Hilfefunktion zugreifen.
OK	Änderungen vornehmen und zur vorherigen Ebene zurückkehren.



---

## In diesem Handbuch verwendete Terminologie

In diesem Abschnitt werden einige Begriffe und die für sie in diesem Handbuch gültigen Definitionen aufgeführt.

<b>Einheit</b>	Ein Oberbegriff zur Bezeichnung aller Einheiten zum Netzmanagement, wie z. B. Sonden oder Agenten.
<b>Ethernet</b>	Dieser Term bezeichnet Ethernet, 100BASE-FX Ethernet und 100BASE-TX Ethernet (auch als Fast Ethernet bekannt), wenn in diesem Handbuch nicht ausdrücklich etwas anderes gesagt wird.
<b>Firmware</b>	Hierbei handelt es sich um die Software, die in einer Einheit ausgeführt wird.
<b>Sonde</b>	Eine RMON- oder RMON2-fähige Einheit.
<b>Station</b>	Ein Oberbegriff für Workstations und andere Einrichtungen, die in Ihrem Netzwerk installiert sind. Eine alternative Bezeichnung ist "Host".

---

## Nützliche WWW-Sites

Die folgenden WWW-Sites enthalten nützliche Informationen zum Netzbetrieb:

### Nways Management

<http://www.networking.ibm.com/netmgt>

### SNMP

Informationen zu SNMPv2 Working Group:  
<http://snmp.net.cmu.edu/bin/snmpv2>

### RMON

Request for Comment zu RMON:  
<http://ds.internic.net/rfc/rfc1757.txt>

Request for Comment zu RMON2:  
<http://ds.internic.net/rfc/rfc2021.txt>

RMON2-Protokollkennungen:  
<http://ds.internic.net/rfc/rfc2074.txt>

## Verschiedenes

Links zu Informationen zum Netzmanagement:

<http://snmp.cs.utwente.nl>

Home-Page der Internet Engineering Task Force:

<http://www.ietf.cnri.reston.va.us>

Network Management Resource Database:

<http://www.onramp.net/cwk/net-manage.cgi>

---

## Online-Hilfefunktion

Die für Nways Manager Remote Monitor verfügbare Online-Hilfefunktion hilft Ihnen bei der Verwendung von Dialogfenstern und Menüs, beim Ausführen von Prozeduren, beim Interpretieren von Statistiken und bei der Fehlerbehebung in Ihrem Netzwerk.

Auf Hilfe für Nways Manager Remote Monitor kann auf die folgenden drei Weisen zugegriffen werden:

- Mit dem Knopf "Help" in Dialogfenstern
- Über das Hilfemenü (Befehl "Help Contents")
- Über die Knopfleiste

Mit Hilfe des Knopfes "Contents" können Sie auch innerhalb des Hilfesystems nach den benötigten Informationen suchen. Klicken Sie auf **Help On Help**, um Hintergrundinformationen zu erhalten.

---

## Kapitel 1. Übersicht über Nways Manager Remote Monitor

In diesem Kapitel wird Nways Manager Remote Monitor vorgestellt. Das Kapitel enthält die folgenden Abschnitte:

- Was ist Nways Manager Remote Monitor?
- Wie funktioniert Nways Manager Remote Monitor?
- Unterstützte Arten von Schnittstellen

---

### Was ist Nways Manager Remote Monitor?

Nways Manager Remote Monitor besteht aus einer integrierten Menge von Anwendungen, mit deren Hilfe Sie die von mit RMON, ECAM und RMON2 kompatiblen Einheiten im Netzwerk erfaßten Echtzeit- und Protokolldaten anzeigen und untersuchen können.

Sie können Nways Manager Remote Monitor verwenden, um folgende Vorgänge durchzuführen:

- Die aktuelle Leistung von LAN- und WAN-Segmenten überwachen.
- Trends anzeigen. (Im Hauptfenster von Nways Manager Remote Monitor werden kurzfristige Trends angezeigt, während die Anzeige "History" mittel- bis langfristige Trends anzeigt.)
- Anzeichen für aktuelle Problem entdecken (z. B. unregelmäßige Paketgrößen, Fehler und Kollisionen).
- Alarmsignale konfigurieren, um spezifische Ereignisse in einem Segment zu überwachen.
- Pakete mit Hilfe von Filter- und Entschlüsselungsfunktionen erfassen und anzeigen.

In angegebenen Abständen ruft Nways Manager Remote Monitor wichtige Netzwerkdaten von fernen Netzwerkeinheiten auf. Diese Daten werden verarbeitet und im Hauptfenster angezeigt. Über das Hauptfenster können Sie den Zustand eines Segments, seine aktuelle Leistung und aktuelle Trends überwachen. Ferner können Sie weitere Fenster öffnen, um verschiedene Segmente gleichzeitig zu überwachen.

Sie können die RMON-Anzeigen (Views) und -Anwendungen (Applications) von Nways Manager Remote Monitor über das Hauptfenster starten, um eine detaillierte Untersuchung durchzuführen. Im einzelnen können Sie folgendes tun:

- Protokolldaten und statistische Daten anzeigen.
- Alarmbedingungen definieren.
- Den Datenaustausch zwischen Stationen im Netzwerk überwachen.
- Spezifische Pakete erfassen und anzeigen.
- In einem einzigen Diagramm Statistiken aus verschiedenen Segmenten miteinander vergleichen.

Sie können auf weitere Funktionen zugreifen, indem Sie die Software SmartAgent auf kompatible Einheiten herunterladen. Weitere Informationen hierzu sind im Abschnitt „Software SmartAgent herunterladen“ auf Seite 192 enthalten.

## **Nways Manager Remote Monitor zur Überwachung des Netzwerks verwenden**

Sie können das Hauptfenster von Nways Manager Remote Monitor und RMON-Anzeigen zur Überwachung Ihres Netzwerks verwenden. Dabei können Sie Statistiken erstellen, die Ihnen helfen, akute Probleme zu identifizieren und zu lösen.

- Verwenden Sie das Hauptfenster und die Anzeige "Statistics" in regelmäßigen Abständen zur Überprüfung von Netzwerkleistung und -auslastung. Beobachten Sie dabei neu auftretende Probleme und kurzfristige Trends.
- Kombinieren Sie bei spezifischen Problemen die Anzeige "Alarms" und die Anwendung "Capture", um Pakete zu sammeln, die zu einem angegebenen Ereignis geführt haben oder auf dieses gefolgt sind. Verwenden Sie anschließend die Anwendung "Decode" und die Funktion "Conversation Analysis", um die Ursache des Problems festzustellen.
- Verwenden Sie die Anzeigen "Host" und "Matrix", um Informationen zu den am meisten ausgelasteten Stationen im Netzwerk zu erhalten.
- Verwenden Sie die Anzeige "History", um Veränderungen und Trends in den Netzwerkstatistiken im Laufe der Zeit anzuzeigen. Mit Hilfe dieser Informationen können Sie rechtzeitig neue Kapazitäten einplanen und implementieren, bevor die vorhandenen Kapazitäten verbraucht sind.

Mit Hilfe der Anzeige "History" können Sie ferner sporadische Fluktuationen in der Netzwerkbelegung entdecken. Dieses Problem kann möglicherweise gelöst werden, indem vorhandene Netzwerkressourcen erneut konfiguriert werden. Anschließend können Sie eine Kombination aus "Alarms" und "Capture" implementieren, um ein erneutes Auftreten dieses spezifischen Problems schnell zu erkennen.

---

## **Wie funktioniert Nways Manager Remote Monitor?**

In diesem Abschnitt werden einige der grundlegenden Konzepte der fernen Netzüberwachung mit Nways Manager Remote Monitor vorgestellt. Der Abschnitt ist in die folgenden zwei Teile untergliedert:

- Eine Übersicht über die Standards von RMON (Remote Monitoring) und RMON2 und über die der fernen Netzüberwachung zugrundeliegenden Konzepte.
- Eine kurze Beschreibung der von Nways Manager Remote Monitor zur Verfügung gestellten Tools zur Netzwerküberwachung.

## **Übersicht über RMON**

Vor der Entwicklung des RMON-Standards waren Überwachungsanwendungen in der Lage, die Menge an Datenverkehr in eine beliebige oder aus einer beliebigen Einheit in einem LAN zu erkennen, aber sie waren kaum in der Lage, den Datenverkehr im gesamten LAN zu erfassen.

Der RMON-Standard bietet die folgenden Vorteile für die Netzwerküberwachung:

- Er bietet eine effektive und effiziente Möglichkeit, um das Verhalten des gesamten LAN zu überwachen.
- Es handelt sich um einen weitverbreiteten Standard.
- Die Belastung durch die Netzwerküberwachung wird zwischen fernen Einheiten und Managementstationen verteilt.

RMON-Einheiten sammeln Informationen zum Verhalten des Netzwerks und übertragen diese auf Anforderung auf einen Analysestandort. Eine Einheit kann als eigenständige Einheit oder als Agent innerhalb eines Hub, eines Router oder eines Switch eingesetzt werden. RMON-Einheiten weisen folgende Vorteile auf:

- Sie ermöglichen den Mitarbeitern eines Teams eine höhere Effektivität, weil diese von einem zentralisierten Standort aus Informationen von weit auseinanderliegenden LAN-Segmenten sammeln können.
- Sie können fortlaufend Überwachungen durchführen und Informationen sammeln, die sie weiterleiten können, bevor Probleme auftreten. Dadurch wird es Administratoren ermöglicht, beim Management ihres Netzwerks auf eine proaktive Weise zu verfahren.
- Jede ferne Einheit kann Anfragen von verschiedenen Managementanwendungen bearbeiten.

Ein Client stellt RMON-Variablen auf der Einheit ein, um Meßintervalle, überwachte Schwellenwerte und andere Betriebsparameter anzugeben. Die ferne Einheit sammelt und speichert Informationen und leitet sie auf Anfrage an einen Client weiter. Wenn erkannt wird, daß angegebene Bedingungen eingetreten sind, können Einheiten eine SNMP-Alarmnachricht an eine Gruppe von Managementstationen senden. Dadurch wird der Netzadministrator auf eine Situation aufmerksam gemacht, die sofort beachtet werden muß.

### **RMON2-Standard**

RMON2 ist eine Erweiterung des RMON-Standards. RMON2 sammelt Statistiken in den Vermittlungs- und Anwendungsschichten der Protokollgruppe. Durch die RMON2-Funktionalität ermöglicht Nways Manager Remote Monitor dem Benutzer, die Verteilung von Protokollen im Netzwerk anzuzeigen. Ferner wird Adressenzuordnung verwendet, um dem Benutzer zu ermöglichen, Netzadressen im gesamten Netzwerk zu entdecken.

**Anmerkung:** RMON2 (ECAM) ist der IBM Vorgänger des RMON2-Standards.

## Grundlagen von Nways Manager Remote Monitor

Nways Manager Remote Monitor besteht aus folgenden Komponenten:

- Dem Hauptfenster von Nways Manager Remote Monitor
- Funktionen zur Konfiguration
- Analysefunktionen
- Tools

### Das Hauptfenster von Nways Manager Remote Monitor

Über das Hauptfenster können Sie für den Zustand des Netzwerks wesentliche Parameter überwachen. Über die Menüleiste des Hauptfensters haben Sie Zugriff auf alle anderen Funktionen von Nways Manager Remote Monitor. Die Knopfleiste enthält die am häufigsten verwendeten Funktionen.

### Funktionen zur Konfiguration

**Device Configuration** Zum Konfigurieren von Einheiten im Netzwerk.

**Address Translation** Zum Konfigurieren der Art und Weise, wie von Nways Manager Remote Monitor Netzadressen angezeigt werden.

**Protocol Directory** Zum Konfigurieren des Protokollverzeichnisses in einer RMON2-Einheit.

**Roving Analysis Port configuration and status** Zum Konfigurieren von Analyse- und Überwachungsanschlüssen für CoreBuilder-Switches und zum Anzeigen von Statusinformationen für den Switch. Weitere Informationen hierzu sind im Anhang D enthalten.

### Analysefunktionen (RMON-Anzeigen)

**RMON-Anzeige "Statistics"** Die Anzeige "Statistics" zeigt einen Echtzeitbericht über die Aktivitäten des von Ihnen ausgewählten Netzwerksegments an. Diese Anzeige sollten Sie zuerst aufrufen, wenn Sie vermuten, daß in einem bestimmten Segment Probleme auftreten. Mit Hilfe dieser Anzeige können Sie Statistiken zu beliebigen Kombinationen aus Paketen, Byte, Fehlern, Größenverteilungen und Multicasts anzeigen.

**RMON-Anzeige "History"** Mit Hilfe der Anzeige "History" können Sie Daten zu den normalen Trends im Netzwerk sammeln. Nachdem Sie die normalen Aktivitäten Ihres Netzwerks bestimmt haben, können Sie Alarmsignale einstellen, die ausgelöst werden, wenn die Aktivitäten im Netzwerk von der Norm abweichen. Geben Sie mit Hilfe der Anzeige "History" einen Erfassungszeitraum an, und entdecken Sie Trends, die sich über Stunden, Tage oder Monate erstrecken.

**RMON-Anzeige "Host"** Mit Hilfe der Anzeige "Host" können Sie erkennen, welche Knoten sich in Ihrem Netzwerk befinden, in welchem Zustand sie sind und welche Knoten möglicherweise Probleme verursachen. Die Statistik "Host TopN" listet die 50 wichtigsten Stationen nach verschiedenen Kriterien auf.

**RMON-Anzeige "Matrix"** Die Anzeige "Matrix" gibt die Menge an Datenverkehr und die Anzahl der Fehler zwischen Stationen im Netzwerk an. Dadurch können Sie die einzelnen Stationen erkennen, die möglicherweise das Auftreten von Problemen verursachen.

**RMON-Anzeige "Ring Station" (Token Ring)** In dieser Anzeige werden Ringinformationen gesammelt und angezeigt, die sich ausschließlich auf den Token-Ring beziehen. Darin enthalten sind der Status der Station sowie die Zeitpunkte des letzten Einstiegs in das Programm und des letzten Exits.

**Alarms** Die Alarmfunktion ist ein wesentliches Element eines proaktiven Netzwerkmanagements. Sie ermöglicht das Verfolgen des Ablaufs von spezifischen Ereignissen, während diese stattfinden. Sie können Alarmsignale einzeln oder in Verbindung mit den Funktionen "Capture" und "Decode" einsetzen. Sie können sie auch zum Senden von Alarmnachrichten verwenden.

**Anwendungen "Capture" & "Decode"** Verwenden Sie "Capture", um die benötigten Pakete herauszufiltern und zu Analyse Zwecken zu speichern. Verwenden Sie "Decode", um erfaßte Pakete zu entschlüsseln und um alle wichtigen Protokolle in einem leicht zu lesenden Format anzuzeigen. Mit Hilfe von "Conversation Trace Analysis" können Sie den Ablauf der enthaltenen Pakete sowie die Übertragungszeit verfolgen.

**Address Map** Diese Funktion ermöglicht Ihnen das Anzeigen und Exportieren von Adressen der Vermittlungsschicht. Wenn auf die von Ihnen verwendete Einheit die Software ECAM SmartAgent heruntergeladen wurde, können Sie auch doppelte Adressen anzeigen.

**Protocol Distribution** Diese Funktion ermöglicht Ihnen das Anzeigen, Exportieren und Drucken von Protokollverteilungsdaten der Software SmartAgent von RMON2 und RMON2 (ECAM).

**PACMIB** Sie können PACMIB-Daten (Port Address Correlation MIB) aktivieren oder inaktivieren. Durch PACMIB werden Anschluß- und Hostdaten einander zugeordnet, und Anschlußstatistiken werden erstellt. Sie können die Beziehungen zwischen den in dem Segment angezeigten Adressen anhand der Anschlüsse erkennen, aus denen das Segment besteht. Weitere Informationen hierzu sind im Anhang D enthalten.

**"Data Export"-Funktionen** Diese Funktionen ermöglichen Ihnen das Anzeigen und Exportieren von statistischen Gruppen zu "Statistics", "Host", "History" und "Matrix".

## Tools

**Data Collector** Mit Hilfe dieses Tools werden Einheiten im Netzwerk in regelmäßigen Abständen RMON- und RMON2-Daten entnommen. Diese Daten werden in Dateien im CSV-Format (Comma Separated Variable) gespeichert. Verwenden Sie diese Daten in Verbindung mit einem Berichts-Tool.

**Anwendung ECAM** (Diese Anwendung ist nur verfügbar, wenn Sie eine Einheit verwenden, auf die die Software RMON2 (ECAM) SmartAgent heruntergeladen wurde.) Mit Hilfe dieser Anwendung können Sie Protokollstatistiken über mehrere LAN-Segmente sammeln und anzeigen.

Über den ursprünglichen RMON-Standard hinausgehend können Sie auf Netzwerk- und Anwendungsschicht zugreifen und sind Statistiken zu Segmenten, zum Host und zum Datenaustausch für die wichtigsten Protokolle und Anwendungstypen abrufen.

## Unterstützte Arten von Schnittstellen

Die folgenden Arten von Schnittstellen werden gegenwärtig von Nways Manager Remote Monitor unterstützt:

- Ethernet
- 100BASE-TX Ethernet
- 100BASE-FX Ethernet
- FDDI
- LAN-Emulation auf Ethernet (aflane\_8023)
- LAN-Emulation auf einem Token-Ring (aflane\_8025)
- Proprietäre virtuelle LAN-Schnittstellen von IBM (propVirtual)

**Anmerkung:** 100BASE-TX Ethernet, 100BASE-FX Ethernet, aflane\_8023 und propVirtual-Schnittstellen werden als Ethernet-Schnittstellen interpretiert. Wenn keine abweichenden Angaben gemacht werden, umfaßt die Bezeichnung "Ethernet" in diesem Handbuch alle oben genannten Schnittstellen. aflane\_8025-Schnittstellen werden als Token-Ring-Schnittstellen interpretiert. Wenn keine abweichenden Angaben gemacht werden, umfaßt die Bezeichnung "Token-Ring" in diesem Handbuch auch aflane\_8025-Schnittstellen.



---

## Kapitel 2. Nways Manager Remote Monitor starten und konfigurieren

In diesem Kapitel wird erklärt, wie Nways Manager Remote Monitor gestartet wird. Außerdem enthält es Angaben dazu, wie eine Liste der zur Überwachung verfügbaren Einheiten erstellt werden kann. Das Kapitel enthält die folgenden Abschnitte:

- Übersicht
- Nways Manager Remote Monitor starten
- Das Dialogfenster "Device Administration" aufrufen
- Einheiten installieren und die Installation überprüfen
- Grundlegende Einheitendaten anzeigen
- RMON- und RMON2-Tabellen verwalten

---

### Übersicht

Damit Nways Manager Remote Monitor ausgeführt werden kann, müssen Sie eine Liste mit den Einheiten angeben, die Ihr Netzwerk überwachen. Wenn diese Liste vollständig ist, können Sie beginnen, den Zustand des Netzwerks über das Hauptfenster und über die Anzeigen und Anwendungen von Nways Manager Remote Monitor zu überwachen.

Außerdem können jederzeit zusätzliche Konfigurationsvorgänge, wie z. B. das Erstellen von virtuellen Schnittstellen und das Hinzufügen von benutzerdefinierten Protokollen, ausgeführt werden. Weitere Informationen hierzu sind in Kapitel 3, „Einheiten von Nways Manager Remote Monitor aus konfigurieren“ auf Seite 19 enthalten.

---

### Nways Manager Remote Monitor starten

Führen Sie folgenden Befehl aus, um Nways Manager Remote Monitor zu starten:

```
rmon
```

Bei diesem Befehl wird vorausgesetzt, daß Sie das Verzeichnis zu Nways Manager Remote Monitor zu Ihrem Pfad hinzugefügt haben, wie im Anhang G, „Häufig auftretende Probleme“ auf Seite 209 beschrieben.

**Anmerkung:** Informationen zum Starten von Nways Manager Remote Monitor über HP-OpenView und IBM NetView enthält der jeweilige Anhang.

Eine Anzeige für den Systemstart wird eingeblendet. Kurz darauf wird das Hauptfenster von Nways Manager Remote Monitor angezeigt. Das Dialogfenster "Modify View" (Abb. 1) wird angezeigt. Sie werden aufgefordert, die gewünschte Einheit für die Überwachung anzugeben.

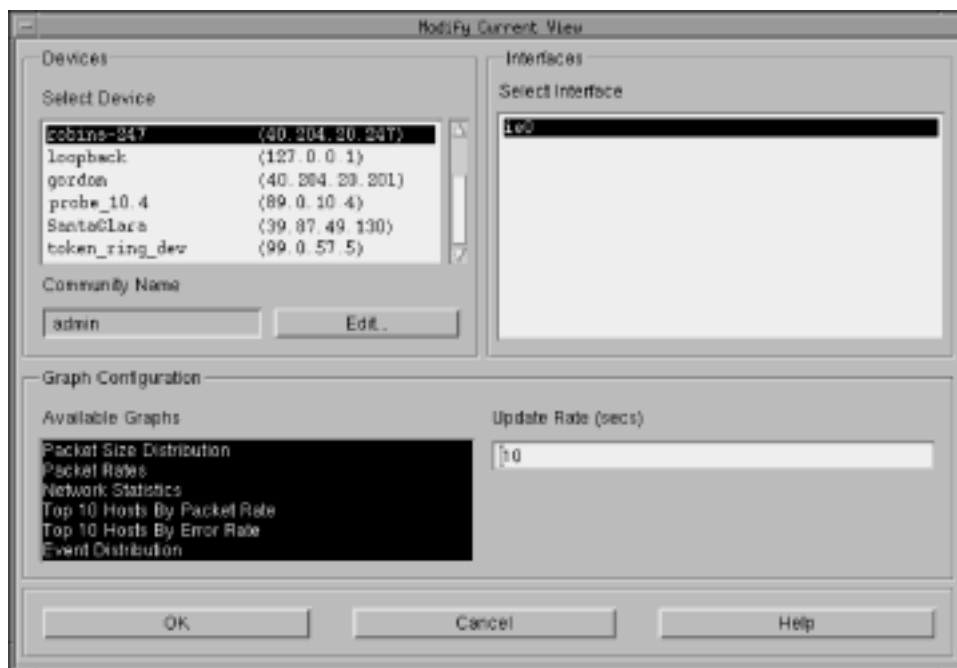


Abbildung 1. Dialogfenster "Modify Current View"

Wählen Sie die benötigte Einheit und die benötigte Schnittstelle in den Bereichen "Device" und "Interface" aus, und klicken Sie das Feld **OK** an, um Details zu der ausgewählten Einheit im Hauptfenster von Nways Manager Remote Monitor anzuzeigen.

Weitere Informationen zum Auswählen von Einheiten sind im Abschnitt „Hauptfenster anpassen“ auf Seite 60 enthalten.

## Das Dialogfenster Device Administration aufrufen

Die Konfiguration aller Einheiten wird über das Dialogfenster "Device Administration" durchgeführt. Wählen Sie den Eintrag **Devices** im Konfigurationsmenü aus, oder klicken Sie den Knopf **Device Administration** in der Knopfleiste an, um dieses Dialogfenster zu öffnen.



Abbildung 2. Dialogfenster "Device Administration"

---

## Einheiten installieren und die Installation überprüfen

Geben Sie an, welche Einheiten von Nways Manager Remote Monitor zur Überwachung des Netzwerks verwendet werden können, indem Sie vom Dialogfenster "Device Administration" aus die angegebenen Schritte durchführen.

### Eine neue Einheit installieren

Gehen Sie wie folgt vor, um eine neue Einheit zu installieren:

1. Klicken Sie die Option **Edit Device List** an, um das in Abb. 3 gezeigte Dialogfenster "Device List Editor" zu öffnen.

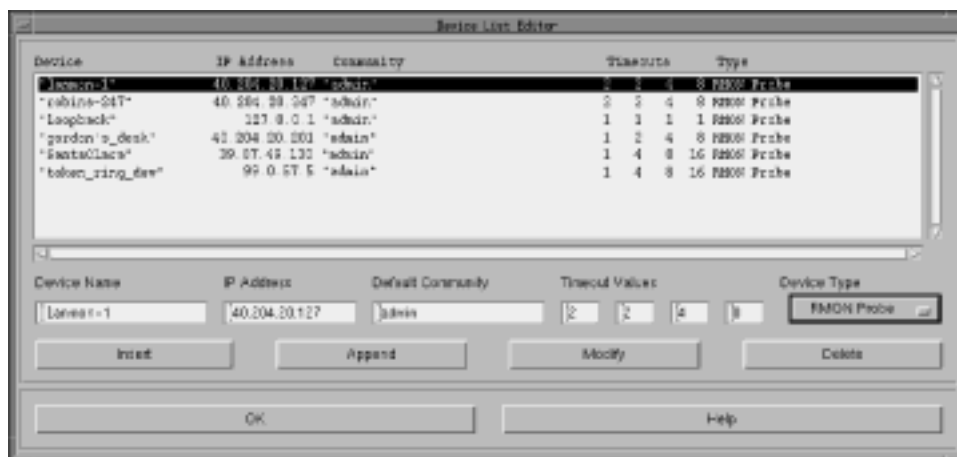


Abbildung 3. Dialogfenster "Device List Editor"

Standardmäßig wird die Einheit ausgewählt, die auch im Dialogfenster "Device Administration" ausgewählt ist.

2. Geben Sie im Feld "Device Name" einen eindeutigen Namen an.
3. Geben Sie die IP-Adresse für die Einheit ein.
4. Im Feld "Default Community" von Nways Manager Remote Monitor wird der standardmäßig eingestellte Name der Benutzergemeinschaft angezeigt, der für den Zugriff auf die ausgewählte Einheit verwendet wird. Bei Bedarf können Sie den Standardnamen ändern.

5. Auch die Werte in der Spalte "Timeout" für den Agenten können bei Bedarf geändert werden. Die Standardwerte sind alle auf 1 Sekunde eingestellt.

Durch die Zeitlimits (Timeouts) werden die Zeiträume bestimmt, während der eine Einheit von Nways Manager Remote Monitor aufgerufen wird, bevor eine Mitteilung angezeigt wird, daß keine Antwort erfolgt. Für die meisten Installationen sind die Standardeinstellungen angemessen. Wenn Ihr Betrieb jedoch über eine langsamere Verbindung stattfindet, wie z. B. über ein serielles Kabel, könnte es ratsam sein, die Werte zu erhöhen, z. B. auf 4, 6, 8 oder 9 Sekunden.

6. Klicken Sie das Feld **Device Type** an und wählen Sie einen angemessenen Typ für die Einheit aus dem verdeckten Menü aus. Im Anhang D sind Informationen zur Verwendung der Funktionen von "Roving Analysis Port" enthalten.
7. Klicken Sie eine der Optionen **Insert** oder **Append** an, um den neuen Eintrag zu der Liste hinzuzufügen. Bei Auswahl von "Insert" wird der neue Eintrag vor der aktuellen Auswahl platziert, bei Auswahl von "Append" wird er angefügt.

Die neue Einheit wird im Bereich "Devices" des Dialogfensters "Device Administration" angezeigt.

### Einen Einheiteneintrag ändern

Gehen Sie wie folgt vor, um einen vorhandenen Einheiteneintrag zu ändern:

1. Wählen Sie einen Eintrag aus dem Dialogfenster "Device List Editor" aus. Details zur ausgewählten Einheit werden in den Feldern unterhalb der Liste angezeigt.
2. Bei Bedarf können Sie jeden beliebigen Eintrag ändern.

**Anmerkung:** An den Namen von Benutzergemeinschaften oder an den Werten für das Zeitlimit vorgenommene Änderungen haben keine Auswirkungen auf aktuelle Anzeigen.

3. Klicken Sie die Option **Modify** an, um die Änderungen vorzunehmen.
4. Klicken Sie das Feld **OK** an, um zum Dialogfenster "Device Administration" zurückzukehren.

### Einen Einheiteneintrag löschen

Gehen Sie wie folgt vor, um einen Einheiteneintrag von Nways Manager Remote Monitor zu löschen:

1. Wählen Sie einen Eintrag aus dem Dialogfenster "Device List Editor" aus. Details zur ausgewählten Einheit werden in den Feldern unterhalb der Liste angezeigt.
2. Klicken Sie die Option **Delete** an, um den Einheiteneintrag zu löschen.

## Einen Einheitseneintrag überprüfen

Wenn Sie überprüfen möchten, ob eine Einheit ordnungsgemäß installiert wurde und ob es möglich ist, Kontakt zu dieser Einheit aufzunehmen, wählen Sie die betreffende Einheit im Dialogfenster "Device Administration" im Bereich "Select Device" aus.

- Bei einem erfolgreichen Versuch wird im Bereich "Interfaces" eine Liste mit den in der Einheit verfügbaren Schnittstellen angezeigt.
- Falls kein Kontakt zu der Einheit aufgenommen werden kann, wird im Bereich "Select Interface" die Nachricht "No response from device" angezeigt. Für diese Nachricht kann eine der folgenden Ursachen vorliegen:
  - Die Einzeldaten zu der Einheit wurden nicht richtig definiert.
  - Aufgrund eines Netzwerkproblems ist die Einheit vorübergehend nicht verfügbar.
  - Die angegebenen Werte für das Zeitlimit sind nicht lang genug, damit ein Kontakt hergestellt werden kann.
  - Der Name der Benutzergemeinschaft verfügt nicht über die benötigten Zugriffsrechte.

Überprüfen Sie, ob die Informationen, die im Dialogfenster "Device List Editor" eingegeben wurden, richtig sind. Versuchen Sie anschließend erneut, Kontakt zu der Einheit aufzunehmen. Mit Hilfe des Dialogfensters "Device Information" können Sie diese Informationen schnell überprüfen. Hinweise hierzu enthält der Abschnitt "Grundlegende Einheitsdaten anzeigen".

Sobald Sie eine Einheit installiert haben und überprüft haben, daß Nways Manager Remote Monitor Kontakt zu der Einheit aufnehmen kann, müssen Sie angeben, welche RMON- und/oder RMON2-Tabellen Sie erstellen möchten. Informationen zum Erstellen dieser Tabellen sind im Abschnitt „RMON- und RMON2-Tabellen verwalten“ auf Seite 15 enthalten.

---

## Grundlegende Einheitendaten anzeigen

Auf eine Zusammenfassung der wichtigsten Informationen zu der Einheit, die gegenwärtig für die Überwachung verwendet wird, kann über das Dialogfenster "Device Administration" zugegriffen werden.

Klicken Sie im Dialogfenster "Device Administration" den Eintrag **Device Information** an. Das Dialogfenster "Device Information" wird angezeigt (siehe Abb. 4).



Abbildung 4. Dialogfenster "Device Information"

Das Dialogfenster ist in die folgenden zwei Bereiche unterteilt:

- Device and System Details
- Interfaces

## Device and System Details

Dieser Bereich enthält den Namen der Einheit, die IP-Adresse, den Namen der Benutzergemeinschaft, den Systemdeskriptor (ein von Herstellern verwendetes Feld zu RMON-Einheiten in freier Form, das grundlegende Informationen zu der Einheit enthält) und den Startzeitpunkt der Überwachung.

## Interfaces

Klicken Sie in der Liste "Select" eine Schnittstelle an, um im Bereich "Details" Details zu der Schnittstelle anzuzeigen.

- Index** Gibt den Index für die ausgewählte Schnittstelle an, der der Schnittstellentabelle für die Einheit entnommen wurde.
- Type** Gibt den Typ der physischen Schnittstelle oder die virtuelle Schnittstelle an.
- MTU** Gibt die Größe (in Byte) des größten Pakets an, das die Schnittstelle verarbeiten kann.
- Speed** Gibt die theoretische Kapazität in Bit pro Sekunde an.
- Physical Address** Gibt die 12stellige MAC-Adresse an.
- "Admin Status" und "Operational Status"** Gibt den gewünschten Status der Schnittstelle an und gibt an, ob die Schnittstelle aktiv ist.
- "In Octets" und "Out Octets"** Gibt die Gesamtzahl der empfangenen und gesendeten Oktette an.

Der Inhalt des Dialogfensters "Device Administration" kann in einer Textdatei gesichert werden. Klicken Sie die Option **Save** an, um das Dialogfenster "File" zu öffnen, und geben Sie einen Dateinamen und eine Adresse an. Klicken Sie das Feld **OK** an, um die Informationen zu sichern, und um zum Dialogfenster "Device Information" zurückzukehren.



---

## RMON- und RMON2-Tabellen verwalten

Für die physischen oder virtuellen Schnittstellen einer Einheit können Sie RMON- und RMON2-Tabellen erstellen und löschen. Sie können auch HostTopN-Tabellen löschen.

1. Wählen Sie eine Einheit aus der Liste "Select Device" aus.
2. Klicken Sie das Feld **Table Editor** an, um wie das in Abb. 5 gezeigte Dialogfenster "Table Editor" zu öffnen.

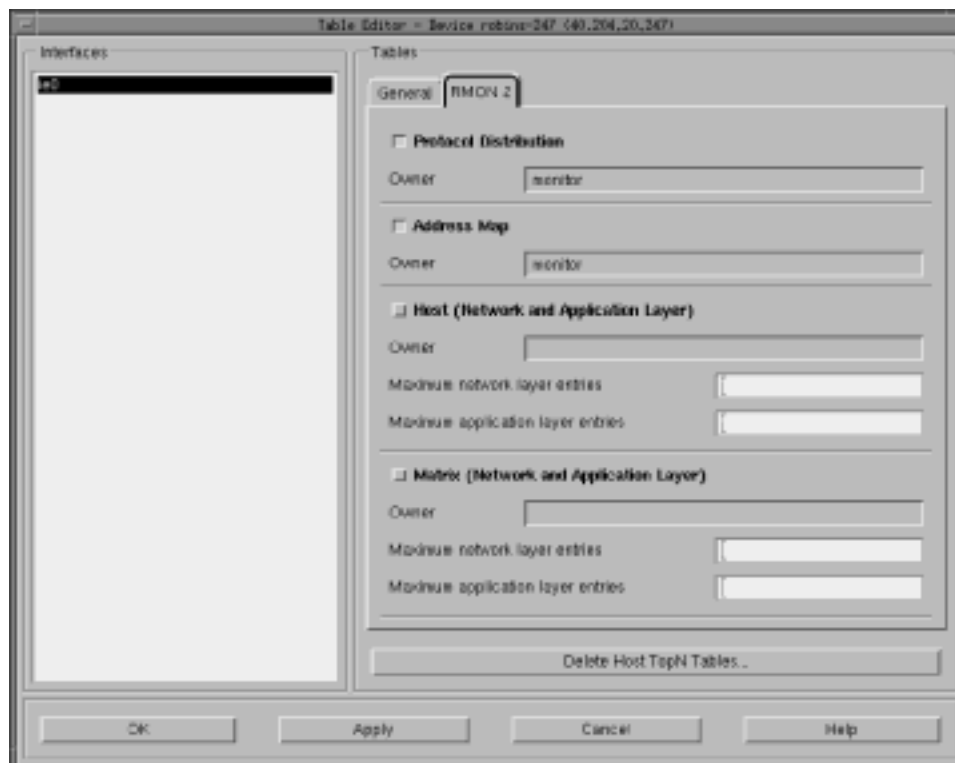


Abbildung 5. Dialogfenster "Table Editor"

3. Wählen Sie im Bereich "Interfaces" eine Schnittstelle aus. Dabei kann es sich um eine physische oder um eine virtuelle Schnittstelle handeln. Informationen zum Erstellen von virtuellen Schnittstellen sind im Abschnitt „Virtuelle Schnittstellen konfigurieren“ auf Seite 43 enthalten.

**Anmerkung:** Wenn Tabelleneinträge in abgeblendet angezeigt werden, sind Sie nicht berechtigt, sie zu erstellen oder zu löschen. Dies ist der Fall, wenn Sie den Namen einer Benutzergemeinschaft verwenden, die über keinen Schreibzugriff auf die Tabellen verfügt, oder wenn bestimmte Tabellen von der Einheit nicht unterstützt werden.

4. Wählen Sie eine der Indexungen "General" oder "RMON2" aus, um die relevanten Tabellen anzuzeigen.

**Anmerkung:**

Wenn Sie RMON2-Tabellen verwenden, wird vorausgesetzt, daß das Protokollverzeichnis bereits vorhanden ist.

Bei der Erstellung der RMON2-Tabellen "Host" und "Matrix" können Sie die Höchstzahl an Einträgen für Netzwerk- und Anwendungsschichten angeben, die von der Einheit erstellt werden soll.

Führen Sie einen der folgenden Schritte aus, um die Tabellen auszuwählen, die Sie verwenden möchten:

- Nehmen Sie die Auswahl eines Tabelleneintrags zurück, wenn Sie eine Tabelle löschen möchten.
- Wählen Sie einen Tabelleneintrag aus, wenn Sie eine Tabelle erstellen möchten.

5. Für bestimmte Diagramme werden von Nways Manager Remote Monitor automatisch HostTopN-Tabellen erstellt. Klicken Sie zum Löschen von HostTopN-Tabelleneinträgen die Option **Delete HostTopN Tables...** an. Dadurch wird das in Abb. 6 gezeigte Dialogfenster "Delete TopN Entries" geöffnet.

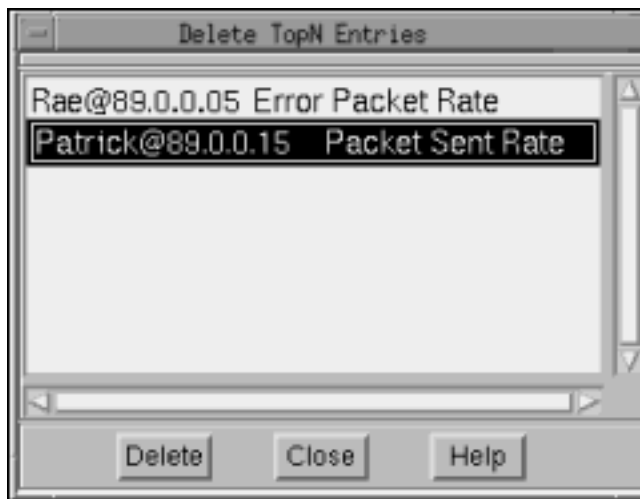


Abbildung 6. Dialogfenster "Delete Table Entry"

- a. Wählen Sie einen Eintrag aus, den Sie löschen möchten.
  - b. Klicken Sie die Option **Delete** an, um den Eintrag dauerhaft aus der Liste zu löschen. Der Eintrag wird sofort gelöscht. Dieser Vorgang kann nicht widerrufen werden. Klicken Sie die Option **Close** an, um zum Dialogfenster "Table Editor" zurückzukehren.
6. Klicken Sie entweder **Apply** oder **OK** an, um im Dialogfenster "Table Editor" vorgenommene Änderungen zu aktivieren. Klicken Sie die Option **Cancel** an, um die Änderungen zu widerrufen oder um eine andere Schnittstelle auszuwählen. Dadurch kehren Sie zum Dialogfenster "Device Administration" zurück.

Sobald Sie die gewünschten Tabellen erstellt haben, können Sie mit Hilfe des Hauptfensters und der RMON-Anzeigen und -Anwendungen beginnen, Ihr Netzwerk zu überwachen.



---

## Kapitel 3. Einheiten von Nways Manager Remote Monitor aus konfigurieren

In diesem Kapitel wird erläutert, wie Sie Einheitenkonfigurationen ausführen können, die über das hinausgehen, was erforderlich ist, damit Nways Manager Remote Monitor Netzwerkeinheiten anzeigen kann. Das Kapitel enthält die folgenden Abschnitte:

- Auf Einheitenkonfigurationen zugreifen
- Systemparameter einstellen
- Firmware herunterladen
- IP-Adresse, Teilnetzwerkmaske und Ringnummer einstellen
- Serielle Verbindungen herstellen
- Statische Leitwege, Standard-Gateway und Echointervall einstellen
- Auf Steuertabellen zugreifen
- Benutzergemeinschaften für Alarmnachrichten festlegen
- Virtuelle Schnittstellen konfigurieren
- Stufe der Adreßumsetzung einstellen
- Schnittstellen umbenennen
- Benutzerdefinierte Protokolle verwalten
- Herstellerpräfixe angeben

---

### Auf Einheitenkonfigurationen zugreifen

Einheiten werden über das Dialogfenster "Device Configuration" konfiguriert. Gehen Sie wie folgt vor, um auf dieses Dialogfenster zuzugreifen:

1. Wählen Sie im Dialogfenster "Device Administration" die Einheit aus, die Sie konfigurieren möchten.

Bei Einheiten, die mehrere Schnittstellen unterstützen, wie z. B. 8272 von IBM, können Sie eine beliebige der aufgelisteten physischen Schnittstellen als IP-Adresse festlegen.

**Anmerkung:** Wenn Sie mehrere IP-Adressen festlegen, müssen Sie sicherstellen, daß sie sich auf verschiedenen Teilnetzwerken befinden.

2. Klicken Sie das Feld **Device Configuration** an, um das in Abb. 7 gezeigte Dialogfenster "Device Configuration" anzuzeigen.

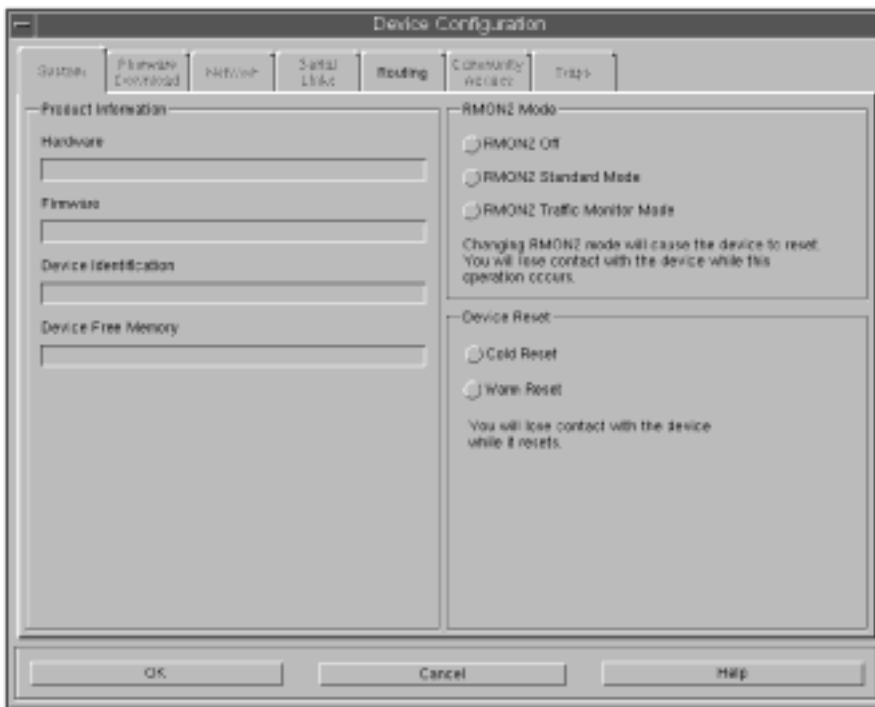


Abbildung 7. Dialogfenster "Device Configuration"

Das Dialogfenster "Device Configuration" enthält die folgenden Indexungen:

*Tabelle 5. Indexungen des Dialogfensters "Device Configuration"*

<b>Indexung</b>	<b>Verwendung</b>
System	<ul style="list-style-type: none"> <li>• Hardware- und Firmwareversionen sowie Einzeldaten zu Einheiten anzeigen.</li> <li>• Eine Einheit mit Kalt- oder Warmstart zurücksetzen.</li> <li>• Den RMON2-Modus auf "Standard" oder auf "Nways Manager-Traffic Monitor" einstellen.</li> <li>• RMON2 aktivieren/inaktivieren.</li> </ul>
Firmware Download	Neue Firmware herunterladen.
Network	Die IP-Adresse, Teilnetzwerkmaske und Ringnummer (nur Token-Ring) für jede Schnittstelle einstellen.
Serial Links	Serielle Verbindungen herstellen. Weitere Informationen hierzu sind im Abschnitt „Serielle Verbindungen herstellen“ auf Seite 31 enthalten.
Routing	Statische Leitwege, Standard-Gateway und Echointervall einstellen.
Community Access	Tabellen zur Zugriffssteuerung konfigurieren.
Traps	Benutzergemeinschaften und Zieladressen für Alarmnachrichten konfigurieren.

---

## Systemparameter einstellen

Verwenden Sie im Dialogfenster "Device Configuration" die Indexzunge "System", um folgende Schritte durchzuführen:

- Informationen zu Hardware und Firmware anzeigen.
- Die Einheit mit Warm- oder Kaltstart in die Grundstellung zurücksetzen.
- Den RMON2-Modus einstellen.

## Informationen zu Hardware und Firmware anzeigen

In Tabelle 6 werden die Inhalte des Bereichs "Product Information" einzeln aufgeführt.

*Tabelle 6. Product Information*

Feld	Funktion
Hardware	Gibt die Platinenüberarbeitung und den Speicher der Einheit an.
Firmware	Gibt die Version der Firmware auf der Einheit an.
Device Identification	Gibt die Kategorie und die MAC-Adresse der Einheit an.
Device Free Memory	Gibt den freien Speicherplatz der Einheit an.

## Eine Einheit zurücksetzen

Wählen Sie im Bereich "Device Reset" eine der Optionen **Warm Reset...** oder **Cold Reset...** aus, um eine Einheit zurückzusetzen. Beide Verfahren zum Zurücksetzen verursachen eine erneute Initialisierung der Einheit. Sie unterscheiden sich jedoch in ihrer Auswirkung auf die Einheit. In Tabelle 7 auf Seite 23 und Tabelle 8 auf Seite 24 werden diese Unterschiede für RMON- und für RMON2-Variablen zusammengefaßt. Beachten Sie die Schlüssel zu den Tabellen.

**Anmerkung:** Vor dem Zurücksetzen der Einheit können Sie in anderen Indexzungen Konfigurationen vornehmen, da das Zurücksetzen erst wirksam wird, wenn Sie im Dialogfenster "Device Configuration" das Feld **OK** anklicken.

**Achtung:** Zwar können Sie durch einen Kaltstart zum Zurücksetzen Konfigurationsdaten schnell löschen und eine Einheit auf die werkseitig vorgenommenen Standardeinstellungen zurücksetzen, aber Sie sollten beachten, daß ein Kaltstart zum Zurücksetzen zum Verlust sowohl von benutzerdefinierten Protokollinformationen als auch von Namen von Benutzergemeinschaften führt.



Tabelle 7 (Seite 1 von 2). Erhaltene und verlorene Konfigurations- und RMON-Daten

<b>Datentyp</b>	<b>Warmstart</b>	<b>Kaltstart</b>
<i>Konfigurationsdaten</i>		
Konfigurationsinformationen zur Einheit (IP-Adresse etc.)	E	E
Echointervall für automatische Erkennung	E	V
RMON2-Modus	E	E
Standard/Traffic-Modus	E	E
TFTP-Server-Adresse	E	E
Dateiname zum Herunterladen	E	E
Datum und Zeit	E	E
Konfigurationsdaten zum seriellen Anschluß	E	E
Tabelleneinträge zum Zugriff von Benutzergemeinschaften	E	VA
Telnet-Kennwort für die Systemkonfiguration	E	V
Tabelleneinträge zum Client	E	VA
<u>Tabelle zur seriellen Verbindung</u>	E	V
Zieltabelle für Alarmnachrichten	E	V
<i>RMON-Daten</i>		
Filtertabelle	E	V
Kanaltabelle	E	V
Steuertabelle zum Erfassen von Puffern	E	V
Protokollsteuertabelle	E	VA
Host-Steuertabelle	E	VA
Matrixsteuertabelle	E	VA
Host-Steuertabelle	E	V
Matrixsteuertabelle	E	V
Host-topN-Tabelle	V	V
Tabelle mit Alarmnachrichten	E	V
Ereignistabelle	E	VA
Erfasste Pakete	V	V
Protokollstatistiken	V	V
Aktuelle Statistiken	VC	VA
Tabellen zur Host-Statistik	V	V
Tabellen zur Matrixstatistik	V	V
Tabellen zur Host-topN-Statistik	V	V
Protokolltabellen	V	V
Tabellen zur Ring-StationD	V	V
Statistiken zur sendestationsorientierten LeitwegwahlD	VC	VA
Steuertabelle zur Ring-StationD	E	VA
Kapselungssteuerung	E	V

Tabelle 7 (Seite 2 von 2). Erhaltene und verlorene Konfigurations- und RMON-Daten

Datentyp	Warmstart	Kaltstart
<b>Schlüssel</b>		
E = Daten bleiben erhalten	A=Wird auf Standardeinstellung zurückgesetzt.	
V= Daten gehen verloren	B=benutzerdefinierte Protokolle	
	C=Steuerungsinformationen bleiben erhalten	
	D=nur Token-Ring	
	E=Gilt nicht für 8271-RMON-Sonden.	

Tabelle 8. Erhaltene und verlorene RMON2-Daten

Datentyp	Warmstart	Kaltstart
Steuertabellen für Adreß-Maps.	E	VA
Adreß-Map-Tabelle	V	V
Steuertabellen zur Protokollzuordnung	E	VA
Protokollzuordnungstabellen	V	V
Steuertabellen für einen Host einer höheren Schicht	E	V
Tabellen für einen Host der Vermittlungsschicht	V	V
Tabellen für einen Host der Anwendungsschicht	V	V
Steuertabellen zur Matrix einer höheren Schicht	E	V
Tabellen zur Matrix einer Vermittlungsschicht	V	V
Tabellen zur Matrix einer Anwendungsschicht	V	V
topN-Steuertabellen zur Matrix einer Vermittlungsschicht	V	V
topN-Tabellen zur Matrix einer Vermittlungsschicht	V	V
topN-Steuertabellen zur Matrix einer Anwendungsschicht	V	V
topN-Tabellen zur Matrix einer Anwendungsschicht	V	V
Benutzerprotokollsteuerung und Objekte	E	V
Benutzerprotokolltabellen	V	V
Protokollverzeichnis	VAB	VA
<b>Schlüssel</b>		
E = Daten bleiben erhalten	A=Wird auf Standardeinstellung zurückgesetzt.	
V= Daten gehen verloren	B=benutzerdefinierte Protokolle bleiben erhalten	

## RMON2-Funktionalität

In Sonden, die DLM-Unterstützung bereitstellen, kann die folgende RMON2-Funktionalität eingerichtet werden:

- Sonden der Tochterkarte HETMAC 8260 von IBM können so konfiguriert werden, daß sie für verschiedene Managementanwendungen die jeweils optimale Tabellengröße verwenden.
- RMON2 kann inaktiviert werden, damit SmartAgent-Software, wie z. B. die Software RMON2 (ECAM) SmartAgent auf der Einheit ausgeführt werden kann.  
RMON2 (ECAM) ist der IBM Vorgänger des RMON2-Standards, der von der Anwendung "Nways Manager - Traffic Monitor" verwendet wird.

**Anmerkung:** Stellen Sie sicher, daß sie die aktuelle Version der Firmware installiert haben, damit Sie über die gesamte RMON2-Funktionalität verfügen.

### Modus einstellen

Der aktuelle Modus der Einheit wird im Dialogfenster "Device Configuration" in der Indexzunge "System" angezeigt. Die Standardeinstellung lautet "Standard Mode".

**Anmerkung:** Bei einer Änderung des Modus wird die Einheit automatisch durch einen Kaltstart zurückgesetzt, damit die Änderungen gültig werden.

Die folgenden drei Modi sind verfügbar:

**Standard Mode** Stellt auf der Einheit die angemessenen Tabellengrößen für die Verwendung mit Nways Manager Remote Monitor oder einer anderen Managementanwendung ein.

**Nways Manager - Traffic Monitor Mode** Stellt auf der Einheit die angemessenen Tabellengrößen für die Verwendung mit "Nways Manager - Traffic Monitor" ein. Sie sollten diesen Modus nur verwenden, wenn Sie über "Nways Manager - Traffic Monitor V1.1" oder eine aktuellere Version verfügen.

**Off** Inaktiviert RMON2. Wenn RMON2 inaktiviert ist, können Sie die Software SmartAgent auf die Einheit herunterladen.

Wenn Sie den Modus ändern und das Feld **OK**, anklicken, wird die Einheit automatisch durch einen Kaltstart zurückgesetzt. Es ist nicht notwendig, die Option **Cold Reset** anzuklicken.

---

## Firmware herunterladen

Verwenden Sie zum Herunterladen von Firmware im Dialogfenster "Device Configuration" die Indexzunge "Firmware Download" (Abb. 8).

Zur Vereinfachung der Einheitenkonfiguration werden Firmware-Dateien auf einem TFTP-Server gespeichert, auf den die Einheiten im Netzwerk zugreifen können. Anschließend können neue Versionen der Firmware vom Server auf die Einheit heruntergeladen werden.

Das Feld "Download Status" im Dialogfenster "Device Configuration" gibt an, ob der letzte von der Einheit vorgenommene Vorgang zum Herunterladen erfolgreich war.

**Anmerkung:** Informationen zum Herunterladen der Software SmartAgent (ECAM) sind im Abschnitt „Software SmartAgent herunterladen“ auf Seite 192 enthalten.



Abbildung 8. Indexzunge "Firmware Download"

**Anmerkung:** Auf dem Server muß TFTP konfiguriert sein. Weitere Informationen sind in den Hinweisen zur Installation und zum jeweiligen Release enthalten.

Gehen Sie zum Herunterladen von Firmware wie folgt vor:

1. Geben Sie im Feld "Download Filename" den Dateinamen der Agenten-Firmware ein. Das in der TFTP-Konfiguration angegebene TFTP-Verzeichnis wird von Nways Manager Remote Monitor als Speicherort für diese Datei verwendet. Im Feld "Download Filename" müssen Sie einen Dateinamen, aber keine Verzeichnisposition angeben.
2. Geben Sie im Feld "Server IP Address" die IP-Adresse des TFTP-Servers ein.
3. Klicken Sie das Feld **OK** an.

Die Einheit wird automatisch zurückgesetzt. Gleichzeitig wird die Verbindung zur Einheit abgebrochen. Dadurch kehren Sie zum Dialogfenster "Device Administration" zurück.

**Anmerkung:** Beim Herunterladen von Firmware wird normalerweise ein Warmstart zum Zurücksetzen vorgenommen. Wenn durch das Herunterladen von Firmware eine Aufrüstung vorgenommen wird, kann möglicherweise aber auch ein Kaltstart zum Zurücksetzen erfolgen.

4. Kehren Sie nach dem Zurücksetzen zum Dialogfenster "Device Configuration" zurück, und überprüfen Sie, ob im Feld "Status" die Einstellung "Success" angezeigt wird.

**Anmerkung:** Wenn durch das Herunterladen ein erneuter Kaltstart verursacht wird, wird im Feld "Status" möglicherweise nicht der richtige Status angezeigt. Bei erfolgreichem Herunterladen der Firmware wird in der Indexzunge "System" im Feld "Firmware" die Version der neuen Firmware angezeigt.

Wenn im Feld "Status" die Einstellung "Failure" angezeigt wird, weist dies möglicherweise auf eines der in Tabelle 9 auf Seite 28 aufgeführten Probleme hin. Überprüfen Sie in diesem Fall den TFTP-Server und führen Sie die Schritte 1 bis 4 erneut durch.

*Tabelle 9. Mögliche Gründe für einen TFTP-Fehler*

<b>Problem</b>	<b>Lösung</b>
Die Datei ist nicht auf dem Server vorhanden.	Kopieren Sie die Datei in das richtige Verzeichnis.
Die Berechtigungen der Datei ermöglichen dem TFTP-Server keinen Zugriff.	Möglicherweise muß die Datei mit globalen Lese-, Schreib- und Ausführungsberechtigungen versehen werden, bevor der Server einen TFTP-Lesevorgang für die Datei ermöglicht. Dies hängt vom Betriebssystem des TFTP-Servers ab. Weitere Informationen hierzu enthält die lokale TFTP-Dokumentation.
Trotz mehrfachen Sendens von Anforderungen reagiert der Server nicht.	Überprüfen Sie, ob die für den TFTP-Server eingegebene IP-Adresse richtig ist.
Die Dateiübertragung wurde abgebrochen.	Dieses Problem kann auftreten, wenn der Server während des Vorgangs zum Herunterladen nicht verfügbar wird. Überprüfen Sie, ob der TFTP-Server verfügbar ist, und wiederholen Sie den Vorgang zum Herunterladen.
Die Einheit ist nicht imstande, Kontakt zum Netzwerk aufzunehmen, oder sie konnte keinen Leitweg zum TFTP-Server finden.	Überprüfen Sie, ob die Einheit gegenwärtig mit dem Netzwerk verbunden ist.  Stellen Sie sicher, daß im Konfigurationssystem der Einheit eine Standard-Gateway-Adresse festgelegt wurde, falls sich der TFTP-Server in einem anderen Teilnetzwerk befindet als die Einheit.
Das TFTP-Herunterladen ist fehlgeschlagen.	Überprüfen Sie, ob Sie über das richtige Firmware-Abbild für die Hardware verfügen.
Der TFTP-Server wurde fälschlicherweise so konfiguriert, daß er als ein bestimmter Benutzer läuft, der auf dem fernen System nicht existiert.	Überprüfen Sie die Konfiguration des TFTP-Servers und des Betriebssystems der Maschine, die als Host für den Server fungiert.

---

## IP-Adresse, Teilnetzwerkmaske und Ringnummer einstellen

Verwenden Sie zum Einstellen der folgenden Parameter im Dialogfenster "Device Configuration" die Indexzunge "Network":

### IP-Adresse und Teilnetzwerkmaske einstellen

Bei Einheiten mit mehreren Schnittstellen können Sie für die meisten physischen Schnittstellen eine IP-Adresse und eine Teilnetzwerkmaske einstellen. Dies gilt auch für serielle Schnittstellen.

Für eine Schnittstelle auf einem 100BASE-TX-Ethernet-Modul, das sich im In-line-Modus befindet, können Sie die IP-Adresse nicht einstellen, weil dieses Modul nicht über eine In-line-Schnittstelle verwaltet werden kann. Auf dieser Einheit müssen Sie für Managementzwecke eine andere Schnittstelle verwenden.

Auf einer virtuellen Schnittstelle können Sie keine IP-Adresse einstellen. (Eine Beschreibung von virtuellen Schnittstellen ist im Abschnitt „Virtuelle Schnittstellen konfigurieren“ auf Seite 43 enthalten.)

Wenn Sie für verschiedene Schnittstellen IP-Adressen festlegen, erhöht sich Ihre Flexibilität bei der Kommunikation mit einer Einheit - wenn auf eine Schnittstelle nicht zugegriffen werden kann, besteht immer noch die Möglichkeit des Zugriffs auf eine andere Schnittstelle. Wenn Sie nicht wissen, welche IP-Adresse Ihnen zugeordnet ist, wenden Sie sich an den zuständigen Netzadministrator.

**Achtung:** Wenn mehrere Schnittstellen auf einer Einheit dasselbe Teilnetzwerk überwachen, kann nur eine dieser Schnittstellen über eine IP-Adresse verfügen. Wenn Sie mehrere IP-Adressen zuordnen möchten, müssen die betreffenden Schnittstellen mit verschiedenen Teilnetzwerken verbunden und für verschiedene Teilnetzwerke konfiguriert sein.

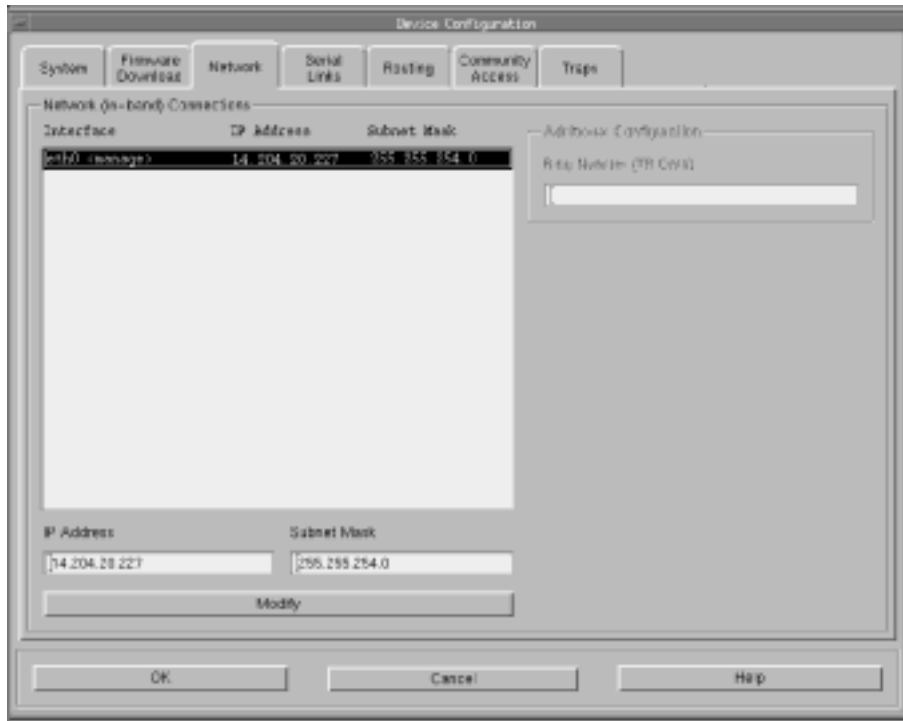


Abbildung 9. Indexzunge "Network"

Gehen Sie wie folgt vor, um die IP-Adresse und die Teilnetzwerkmaske einzustellen:

1. Wählen Sie die erforderliche Schnittstelle aus.
2. Geben Sie im Feld "IP Address" die IP-Adresse für die Einheit oder für die ausgewählte Schnittstelle auf der Einheit ein.
3. Geben Sie im Feld "Subnet Mask" die richtige Teilnetzwerkmaske für die Klasse der IP-Adresse ein.
4. Klicken Sie die Option **Modify** an, damit die neuen Werte gelten.

Nach dem nächsten Zurücksetzen der Einheit werden die neuen Einstellungen für die Einheit wirksam.

## Ringnummer einstellen

Dies ist die Ringnummer für das Token-Ring-Segment, in dem sich die Einheit befindet. Sie wird für Hop-Berechnungen für die sendestationsorientierte Leitwegwahl verwendet.

**Anmerkung:** Möglicherweise wird diese Variable von einigen Sonden nicht unterstützt.

Geben Sie zum Einstellen der Ringnummer im Feld "Ring Number" den erforderlichen Wert ein.



## Serielle Verbindungen herstellen

Verwenden Sie zum Herstellen von seriellen Verbindungen im Dialogfenster "Device Configuration" die Indexzunge "Serial Links" (siehe Abb. 10).

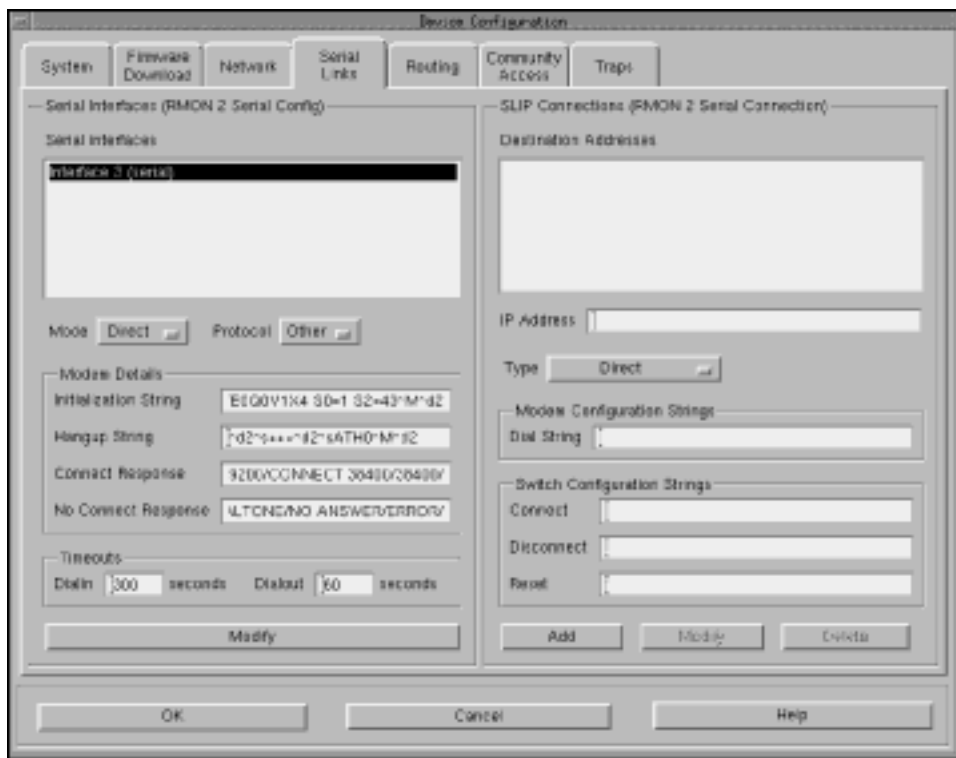


Abbildung 10. Indexzunge "Serial Links"

Diese Indexzunge ist in die folgenden zwei getrennten Bereiche unterteilt:

**Serial Interfaces** Ermöglicht die Konfiguration von seriellen Schnittstellen auf der Einheit.

**SLIP Connections** Ermöglicht die Herstellung von SLIP-Verbindungen zu Managementstationen.

## Serielle Schnittstellen konfigurieren

Die Namen der seriellen Schnittstellen der Einheit werden im Bereich "Serial Interfaces" angezeigt. Diese Einstellung wird auf der Einheit vorgenommen und kann nicht über Nways Manager Remote Monitor geändert werden.

Gehen Sie wie folgt vor, um die seriellen Schnittstellen einer Einheit zu konfigurieren:

1. Wählen Sie den Modus der seriellen Verbindung aus. Die beiden folgenden Modi sind verfügbar:

<b>Direct</b>	Die Einheit wird direkt mit der Managementstation verbunden.
<b>Modem</b>	Für die Verbindung zwischen Einheit und Managementstation wird ein Modem benötigt.

2. Wählen Sie das Protokoll aus, das für die serielle Verbindung verwendet werden soll. Dies Protokoll ist entweder standardmäßig auf "Other" eingestellt oder es kann auf "SLIP" eingestellt werden. Eine Änderung auf die Einstellung "Other" kann nicht vorgenommen werden.
3. Stellen Sie die Einzeldaten zum Modem ("Modem Details") ein. Dabei handelt es sich um die folgenden Daten:

### Initialization String

Diese Steuerzeichenfolge gibt an, wie ein Modem, der an eine serielle Schnittstelle angeschlossen ist, initialisiert werden soll. Wenn Sie den Modus auf "Modem" eingestellt haben, wird die Initialisierung bei jedem Systemstart und nach jeder Beendigung einer Verbindung ausgeführt.

Die folgende Initialisierungszeichenfolge eignet sich für viele Modems:  
~s~MATE0Q0V1X4 S0=1 S2=43~M

### Hangup String

Diese Steuerzeichenfolge gibt an, wie eine Modemverbindung zur seriellen Schnittstelle unterbrochen werden kann. Sie wird nur verwendet, wenn der Modus auf "Modem" eingestellt ist.

Die folgende Zeichenfolge für Auflegen (Hangup String) eignet sich für viele Modems: ~d2~s+++~d2~sATH0~M~d2

### Connect Response

Diese Zeichenfolge enthält Unterzeichenfolgen, die den erwarteten Antwortcode der Modemverbindung und die Rate an zugeordneten Bit pro Sekunde beschreiben. Die Unterzeichenfolgen werden vom ersten Zeichen in der Zeichenfolge begrenzt.

Die folgende Zeichenfolge für Verbindungsantwort (Connect Response) eignet sich für viele Modems: /CONNECT/300/CONNECT 1200/1200/CONNECT 2400/2400/CONNECT 4800/4800/CONNECT 9600/9600/CONNECT 14400/14400/CONNECT 19200/19200/CONNECT 38400/38400/

### No Connect Response

Diese Zeichenfolge enthält Antwortcodes. Sie kann vom einem Modem generiert werden, um den Grund mitzuteilen, warum ein Versuch, eine Verbindung herzustellen, fehlgeschlagen ist. Die Antwortcodes werden vom ersten Zeichen in der Zeichenfolge begrenzt.

Die folgende Zeichenfolge für keine Verbindungsantwort (No Connect Response) eignet sich für viele Modems: /NO CARRIER/BUSY/NO DIALTONE/NO ANSWER/ERROR/

4. Stellen Sie die Zeitlimits (Timeouts) für die seriellen Verbindungen ein.

**Dialin Timeout** Gibt die Länge der Zeit an, während der ankommende Verbindungen inaktiv sein dürfen. Nach Ablauf dieser Zeit wird die Verbindung von der Einheit unterbrochen.

**Dialout Timeout** Gibt die Länge der Zeit an, während der abgehende Verbindungen inaktiv sein dürfen. Nach Ablauf dieser Zeit wird die Verbindung von der Einheit unterbrochen.

Je nach verwendeter Verbindungsart ist es vielleicht ratsam, die Zeitlimits anzupassen. Wenn Sie z. B. eine gebührenfreie Nummer verwenden, können hohe Werte für das Zeitlimit sinnvoll sein.

## SLIP-Verbindungen konfigurieren

Mit Hilfe dieses Bereichs können Sie die Einheit so konfigurieren, daß sie SLIP-Verbindungen zu Managementstationen herstellt.

### Eine SLIP-Verbindung hinzufügen

Führen Sie die folgenden Schritte durch, damit die Einheit eine SLIP-Verbindung zu einer Managementstation herstellt:

1. Geben Sie die IP-Adresse der Station ein, zu der die Verbindung hergestellt werden soll.
2. Wählen Sie eine der folgenden Verbindungsarten aus:

**Direct** Für die Verbindung ist weder ein Modem noch ein Switch erforderlich.

**Modem** Zwischen Einheit und Managementstation befindet sich ein Modem.

**Switch** Zwischen Einheit und Managementstation befindet sich ein Switch.

**Modem and Switch** Für die Verbindung sind sowohl ein Modem als auch ein Switch erforderlich.

Je nach Verbindungsart werden manche Felder abgeblendet angezeigt. Sie müssen die jeweils benötigten Informationen eingeben.

3. Wenn Sie eine Verbindungsart mit Modem oder mit Modem und Switch ausgewählt haben, müssen Sie die Wählzeichenfolge festlegen. Bei dieser handelt es sich um eine Steuerzeichenfolge, die angibt, wie die Rufnummer gewählt werden soll, damit eine Modemverbindung hergestellt wird. Die Zeichenfolge sollte das Präfix und das Suffix der Nummer enthalten.
4. Gehen Sie wie folgt vor, wenn Sie eine Verbindungsart mit Switch oder mit Modem und Switch ausgewählt haben:
  - a. Legen Sie die Verbindungszeichenfolge fest. Bei dieser handelt es sich um eine Steuerzeichenfolge, die angibt, wie eine Daten-Switch-Verbindung hergestellt werden kann.
  - b. Legen Sie die Zeichenfolge für das Trennen der Verbindung fest. Bei dieser handelt es sich um eine Steuerzeichenfolge, die angibt, wie eine Daten-Switch-Verbindung beendet werden kann.
  - c. Legen Sie die Zeichenfolge für Zurücksetzen fest. Bei dieser handelt es sich um eine Steuerzeichenfolge, die angibt, wie ein Daten-Switch im Falle einer Zeitüberschreitung zurückgesetzt werden kann.
5. Klicken Sie zum Hinzufügen des Eintrags die Option **Add** an.

### **Eine SLIP-Verbindung ändern**

Gehen Sie wie folgt vor, um eine vorhandene SLIP-Verbindung zu ändern:

1. Wählen Sie aus der Liste den Namen einer SLIP-Verbindung aus.
2. Ändern Sie bei Bedarf den vorliegenden Namen der Schnittstelle.
3. Klicken Sie die Option **Modify** an.

### **Eine SLIP-Verbindung löschen**

Gehen Sie wie folgt vor, um eine vorhandene SLIP-Verbindung zu löschen:

1. Wählen Sie die IP-Adresse der betreffenden SLIP-Zieladresse aus der Liste aus.
2. Klicken Sie die Option **Delete** an.

---

## Statische Leitwege, Standard-Gateway und Echointervall einstellen

Verwenden Sie zum Einstellen von Standard-Gateway und Echointervall im Dialogfenster "Device Configuration" die Indexzunge "Routing" (siehe Abb. 11).

### Statische Leitwege einstellen

Statische Leitwege werden verwendet, um spezifische Leitwege aufzubauen, die die Einheit verwenden sollte, um andere Netzwerke zu erreichen. Der Standard-Gateway wird dabei außer Kraft gesetzt.

Verwenden Sie zum Erstellen von statischen Leitwegen im Dialogfenster "Device Administration" die Indexzunge "Routing" (siehe Abb. 11).

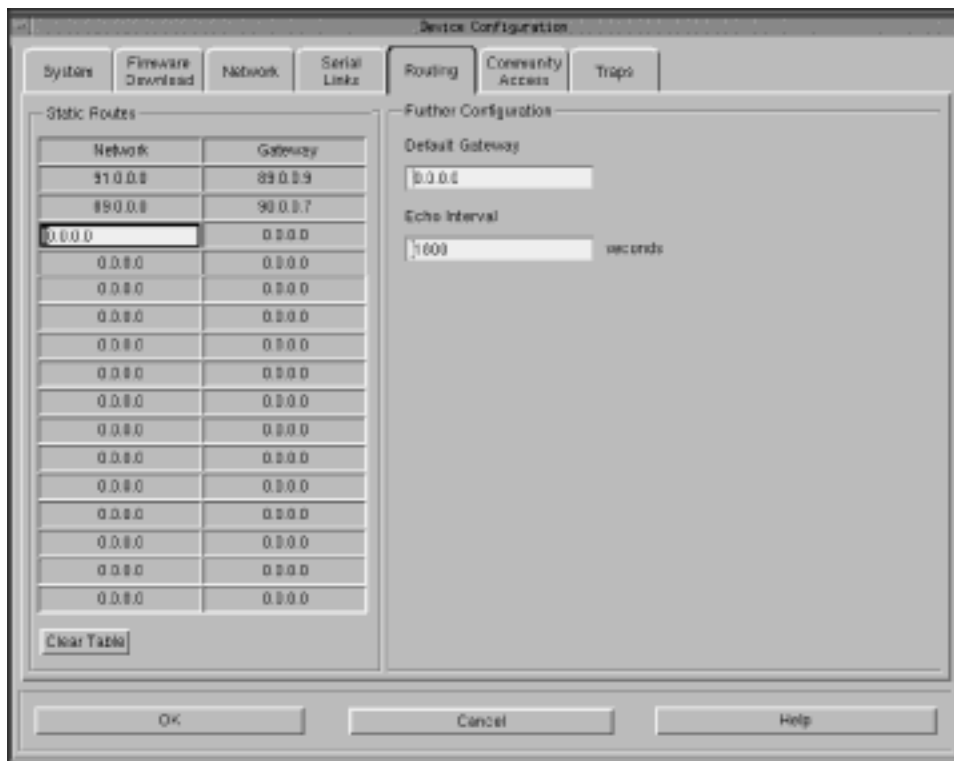


Abbildung 11. Indexzunge "Routing"

Die folgenden Parameter sind verfügbar:

<b>Network</b>	Die IP-Adresse des Zielnetzwerks, z. B. "91.0.0.0".
<b>Gateway</b>	Die Adresse des Router, an den die Pakete gesendet werden sollen, z. B. "89.0.0.9". Dieser Router muß sich im selben Segment befinden wie die Einheit.

1. Klicken Sie die Option **Clear Table** an, um alle Einträge zu statischen Leitwegen in der Tabelle zu löschen. Dadurch werden alle Einträge auf "0.0.0.0" zurückgesetzt.
2. Klicken Sie ein Feld an, und bearbeiten Sie die Werte soweit wie nötig.
3. Die Änderungen werden wirksam, sobald die Einheit zurückgesetzt wurde. Im Abschnitt „Systemparameter einstellen“ auf Seite 22 sind Informationen zum Zurücksetzen einer Einheit über Nways Manager Remote Monitor enthalten.

### Standard-Gateway einstellen

Geben Sie zum Einstellen des Standard-Gateways im Feld "Default Gateway" die IP-Adresse für den Router oder den Gateway ein.

### Echointervall einstellen

Einheiten können so definiert werden, daß sie in regelmäßigen Abständen Ping-Nachrichten an den Standard-Gateway senden. Dadurch kann ein Leitweg zwischen der Einheit und der Managementstation aufrechterhalten werden. Möglicherweise benötigt der Router ein kürzeres Intervall zwischen den Ping-Nachrichten, damit die Einheit in den Leitwegtabellen erhalten bleibt. In diesem Fall kann es notwendig sein, das Echointervall zu ändern.

Geben Sie das Ping-Intervall (in Sekunden) im Feld "Echo Interval" ein. Der Standardwert beträgt 1800 Sekunden. Der Maximalwert beträgt 3600 Sekunden (1 Stunde).

---

### Auf Steuertabellen zugreifen

Mit Hilfe der Indexzunge "Community Access" (Abb. 12 auf Seite 37 ) können Sie für die Namen von Benutzergemeinschaften verschiedene Sicherheitsstufen festlegen. Anschließend können Sie diese Namen den Workstations von spezifischen Endbenutzern zuordnen. Dadurch kann der Zugriff auf den MIB einer Einheit auf eine ausgewählte Menge von Managementstationen bzw. Benutzergemeinschaften begrenzt werden. Durch die Verwendung von mehreren Benutzergemeinschaften kann die Einheit verschiedenen Managementstationen verschiedene Zugriffsebenen zur Verfügung stellen.

**Achtung:** Ein erneuter Kaltstart führt zum Verlust von benutzerdefinierten Protokollinformationen und von Namen von Benutzergemeinschaften.

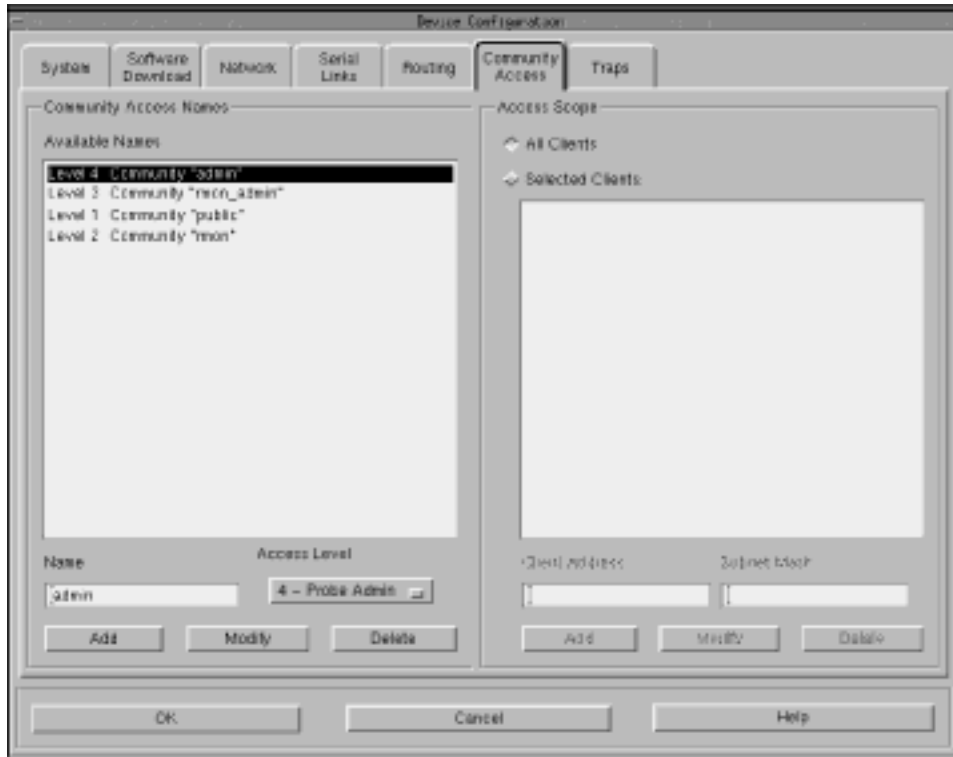


Abbildung 12. Indexzunge "Community Access"

**Anmerkung:** Alle Änderungen, die Sie in der Indexzunge "Community Access" vornehmen, werden sofort auf der konfigurierten Einheit wirksam.

Die Indexzunge ist in die folgenden zwei Bereiche unterteilt:

- Im Bereich "Community Access Names" ist eine Liste mit den Namen der Benutzergemeinschaften und den ihnen jeweils zugeordneten Zugriffsebenen aufgeführt (siehe Tabelle 10 auf Seite 38).
- Der Bereich "Access Scope" enthält eine Liste mit den Stationen, die alle in der Tabelle "Community Access" aufgeführten Namen von Benutzergemeinschaften verwenden können.

## Namen von Benutzergemeinschaften festlegen

Gehen Sie zum Erstellen eines neuen Namens für eine Benutzergemeinschaft mit einer spezifischen Sicherheitsstufe wie folgt vor:

1. Geben Sie im Feld "Name" einen neuen Eintrag ein. Der Name muß eindeutig sein.
2. Legen Sie die Sicherheitsstufe fest, indem Sie den Eintrag **Access Level** anklicken und aus dem verdeckten Menü die gewünschte Stufe auswählen (siehe Tabelle 10).

Tabelle 10. Verschiedene Zugriffsebenen (zur Sicherheit)

Ebene	Beschreibung
1	Lesezugriff auf MIB-II-Objekte (SNMP MIB)
2	Lesezugriff auf MIB-II-, RMON- und RMON2-MIB- sowie Konfigurations-MIB-Objekte. (Mit Ausnahme der Gruppe "Access Control" und der Tabelle "Capture Buffer".)
3	Lesezugriff auf MIB-II-, RMON- und RMON2-MIB- sowie Konfigurations-MIB-Objekte. (Mit Ausnahme der Gruppe "Access Control".) Schreibzugriff auf RMON- und RMON2-MIB- sowie Konfigurations-MIB-Objekte. (Mit Ausnahme der Gruppen "Device Configuration", "Interface" und "Access Control".)
4	Lese- und Schreibzugriff auf alle MIB-II-, RMON- und RMON2-MIB- sowie Konfigurations-MIB-Objekte.

3. Klicken Sie zum Erstellen des Eintrags die Option **Add** an. Standardmäßig ermöglicht Nways Manager Remote Monitor allen Clients die Verwendung des neuen Zugriffsnamens.

Gehen Sie wie folgt vor, um die Einstellungen zu einem vorhandenen Eintrag für den Zugriff einer Benutzergemeinschaft zu ändern:

1. Wählen Sie einen Eintrag aus der Tabelle "Community Access" aus. Die aktuellen Einstellungen werden in den Feldern "Level" und "Community Name" angezeigt.
2. Ändern Sie den Namen oder die Sicherheitsstufe wie oben beschrieben. Klicken Sie anschließend die Option **Modify** an, damit die Änderungen wirksam werden.

Gehen Sie zum Löschen eines vorhandenen Eintrags für den Zugriff einer Benutzergemeinschaft wie folgt vor:

1. Wählen Sie den Eintrag in der Tabelle aus.
2. Klicken Sie die Option **Delete** an.



## Einzelnen Workstations Sicherheitsstufen zuordnen

Im Bereich "Access Scope" wird aufgeführt, welche Clients welche Sicherheitsstufe verwenden können.

Wenn Sie im Bereich "Community Access Names" einen neuen Zugriffsnamen hinzufügen, wird im Bereich "Access Scope" standardmäßig die Einstellung "All Clients" aktiviert.

Gehen Sie wie folgt vor, um einzelnen Workstations die Berechtigung für einen bestimmten Zugriffsnamen zu erteilen:

1. Klicken Sie im Bereich "Access Scope" den Eintrag **Selected Clients** an. Wenn Ihre Workstation den aktuellen Zugriffsnamen der Ebene 4 verwendet, wird die Adresse Ihrer Workstation automatisch in der Liste angezeigt.
2. Geben Sie in den Feldern "Client Address" und "Subnet Mask" die IP-Adresse des Client der Workstation und der Teilnetzwerkmaske ein.
3. Klicken Sie zum Erstellen des Eintrags die Option **Add** an.

**Anmerkung:** Sie können gleichzeitig Gruppen von Clients hinzufügen. Wenn Sie beispielsweise die Client-Adresse "89.56.45.0" und die Teilnetzwerkmaske "255.255.255.0" hinzufügen, bedeutet dies, daß alle Clients im Netzwerk "89.56.45" zum Bereich "Access Scope" hinzugefügt werden.

## Einen Client-Eintrag ändern

Gehen Sie zum Ändern eines Client-Eintrags wie folgt vor:

1. Wählen Sie den Eintrag aus der Liste aus.
2. Ändern Sie bei Bedarf die Werte für die IP-Adresse und die Teilnetzwerkmaske.
3. Klicken Sie die Option **Modify** an.

## Einen Client-Eintrag löschen

Gehen Sie zum Löschen eines vorhandenen Client-Tabelleneintrags wie folgt vor:

1. Wählen Sie den Eintrag aus der Liste aus.
2. Klicken Sie die Option **Delete** an.

---

## Benutzergemeinschaften für Alarmnachrichten festlegen

Wenn auf einer Einheit ein Alarm ausgelöst wird, kann die Einheit Hosts im Netzwerk auf das Ereignis hinweisen, indem sie ihnen ein Paket mit einer SNMP-Alarmnachricht sendet. Nicht alle Workstations im Netzwerk werden über das Ereignis informiert, sondern nur die, für die vorher angefordert wurde, daß sie informiert werden sollen. Sie können steuern, welche Workstations informiert werden, indem Sie jeder Alarmnachricht auf einer Einheit einen Namen und zugleich jedem Namen einer Alarmnachricht eine Liste der zu informierenden Workstations (Benutzergemeinschaft für Alarmnachrichten) zuordnen.

Verwenden Sie zum Festlegen von Benutzergemeinschaften für Alarmnachrichten im Dialogfenster "Device Configuration" die Indexzunge "Traps" (siehe Abb. 13 auf Seite 41).

Die folgenden beiden Möglichkeiten zum Zuordnen von Benutzergemeinschaften für Alarmnachrichten stehen zur Auswahl:

- Jeder neuen Alarmnachricht, die Sie erstellen, wird von Nways Manager Remote Monitor automatisch der Standardname für Benutzergemeinschaften für Alarmnachrichten zugeordnet. Es wird überprüft, daß diese Benutzergemeinschaft auf jeder Einheit, zu der Kontakt aufgenommen wird, vorhanden ist. Ferner werden die Informationen für die Workstation, auf der Nways Manager Remote Monitor ausgeführt wird, zur Benutzergemeinschaft für Alarmnachrichten hinzugefügt.
- Sie können präzise steuern, welche Workstations im Netzwerk Alarmnachrichten von der Einheit erhalten, indem Sie im Dialogfenster "Alarm Entry Creation" im Feld "Trap Destination Community Name" einen anderen Namen für die Benutzergemeinschaft eingeben und die Liste der IP-Zieladressen bearbeiten.

**Anmerkung:** Eine Beschreibung, wie Sie Benutzergemeinschaften für Alarmnachrichten einer Alarmnachricht zuordnen, ist im Abschnitt „Alarmnachrichten konfigurieren“ auf Seite 103 enthalten.

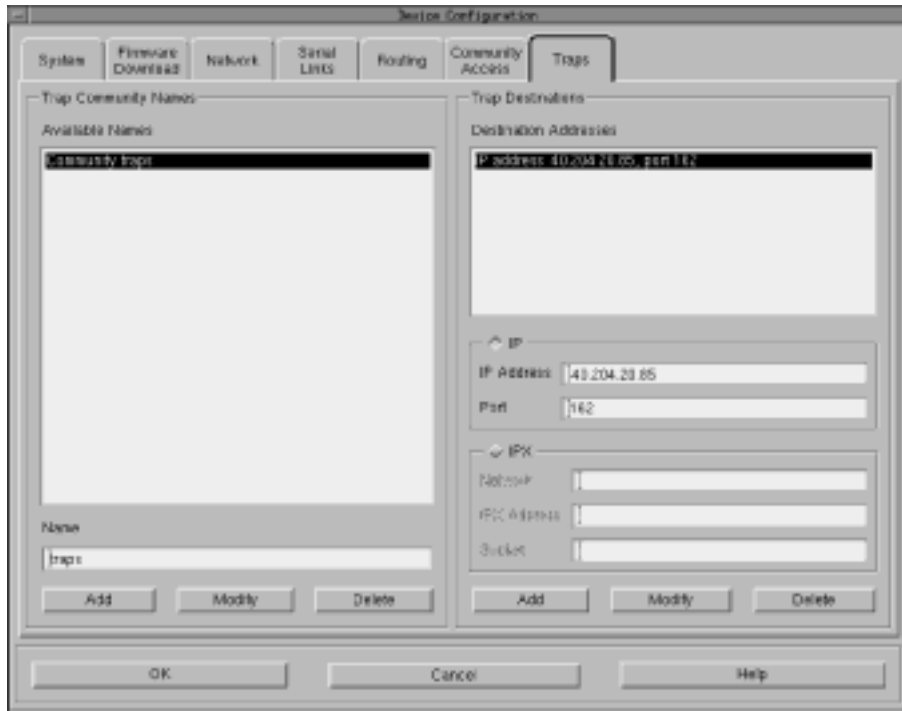


Abbildung 13. Indexzunge "Traps"

## Namen für Benutzergemeinschaften für Alarmnachrichten festlegen

### Namen für Benutzergemeinschaften für Alarmnachrichten hinzufügen

Gehen Sie wie folgt vor, um den Namen einer Benutzergemeinschaft für Alarmnachrichten hinzuzufügen:

1. Geben Sie im Feld "Name" einen eindeutigen Namen ein.
2. Klicken Sie die Option **Add** an. Der Name wird im Bereich "Available Names" angezeigt.

### Namen für Benutzergemeinschaften für Alarmnachrichten ändern

Gehen Sie wie folgt vor, um den Namen einer Benutzergemeinschaft zu ändern:

1. Wählen Sie den Eintrag aus, den Sie ändern möchten. Der Name wird im Feld "Name" angezeigt.
2. Bearbeiten Sie dieses Feld so weit wie erforderlich.
3. Klicken Sie die Option **Modify** an, um die Änderung wirksam zu machen.

## Namen für Benutzergemeinschaften für Alarmnachrichten löschen

Gehen Sie zum Löschen einer Benutzergemeinschaft wie folgt vor:

1. Wählen Sie den Eintrag aus, der gelöscht werden soll.
2. Klicken Sie die Option **Delete** an.

## Zieladressen von Alarmnachrichten ändern

Sie können in der Liste der Ziel-Workstations, die einer Benutzergemeinschaft für Alarmnachrichten zugeordnet ist, Änderungen vornehmen, indem Sie im Bereich "Available Names" die betreffende Benutzergemeinschaft auswählen. Die Zieladressen, die dieser Benutzergemeinschaft zugeordnet sind, werden in der Liste "Destination Addresses" angezeigt. Die Einzelangaben zu den Zieladressen unterscheiden sich je nachdem, ob RMON2 auf der Einheit aktiviert ist oder nicht.

### RMON2 aktiviert

Bei der Zieladresse kann es sich entweder um eine IP- oder um eine IPX-Adresse handeln. Dabei werden die folgenden Einzelangaben angezeigt:

- Für IP:
  - Die IP-Adresse der Ziel-Workstation.
  - Die Anschlußnummer für die Verbindung. Dabei handelt es sich in der Regel um Anschluß 162 (SNMP-Alarmnachrichten).
- Für IPX:
  - Die Netzadresse der Ziel-Workstation.
  - Die IPX-Adresse der Ziel-Workstation.
  - Die Socket-Nummer für die Verbindung

**Anmerkung:** Einige Einheiten unterstützen möglicherweise keine Zieladressen für Alarmnachrichten mit IPX-Adressen. Für solche Einheiten sollten Sie nur Zieladressen für Alarmnachrichten mit IP-Adressen angeben.

### RMON2 inaktiviert

**Anmerkung:** Auf manchen Einheiten können keine Zieladressen für Alarmnachrichten konfiguriert werden, wenn RMON2 inaktiviert ist.

Für jeden Zieladresseneintrag für eine Alarmnachricht wird eine primäre Zieladresse und eine wahlfreie alternative Zieladresse für den Fall, daß kein Kontakt zu der primären Zieladresse aufgenommen werden kann, angegeben. Dabei werden die folgenden Einzelangaben angezeigt:

- Die IP-Adresse der primären Zieladresse.  
Die Schnittstelle auf der Einheit, über die die primäre Zieladresse erreicht werden kann.

- Die IP-Adresse der alternativen Zieladresse (wahlfrei).

Die Schnittstelle auf der Einheit, über die die alternative Zieladresse erreicht werden kann (wahlfrei).

### **Zieladressen für Alarmnachrichten hinzufügen**

Geben Sie die Einzeldaten zur Adresse ein, um eine Ziel-Workstation zur Liste hinzuzufügen. Klicken Sie anschließend die Option **Add** an.

### **Zieladressen für Alarmnachrichten ändern und löschen**

Wählen Sie zum Ändern der Einzelangaben für eine Ziel-Workstation den betreffenden Eintrag aus der Liste "Destination Addresses" aus, ändern Sie die Werte soweit erforderlich, und klicken Sie die Option **Modify** an.

Wählen Sie zum Entfernen einer Ziel-Workstation aus der Liste "Destination Addresses" den betreffenden Eintrag in der Liste aus, und klicken Sie die Option **Delete** an.

---

## **Virtuelle Schnittstellen konfigurieren**

Physische Schnittstellen auf einer Einheit sammeln Daten für Netzwerkparameter, wie z. B. die Gesamtzahl der Pakete, die Gesamtzahl der Fehler etc. Spezifische Pakettypen werden von der Anwendung "Capture" für eine gründlichere Untersuchung aus dem Netzwerk herausgefiltert.

In virtuellen Schnittstellen werden diese Funktionen miteinander vereint, damit die auf der physischen Schnittstelle gesehene Daten Ihren Angaben gemäß gefiltert werden. Beispielsweise kann eine virtuelle Schnittstelle so konfiguriert werden, daß sie nur Statistiken zum WWW-Datenverkehr filtert. Von einer virtuellen Schnittstelle gesammelte Statistiken werden in Standard-RMON- und -RMON2-Tabellen auf der Einheit gespeichert.

Auf virtuellen Schnittstellen können die folgenden RMON- und RMON2-Tabellen nicht konfiguriert sein:

- Adreß-Map
- Protokollverzeichnis
- Token-Ring-Station
- Statistiken zur sendestationsorientierten Leitwegwahl für Token-Ring

**Anmerkung:** Virtuelle Schnittstellen werden von Einheiten in HETMAC 8238 und 8260 von IBM unterstützt. Möglicherweise werden sie auch von Einheiten anderer Hersteller unterstützt. (Weitere Informationen hierzu enthält die Herstellerdokumentation zur Einheit.)

## Virtuelle Schnittstellen erstellen

Geben Sie zum Erstellen einer virtuellen Schnittstelle die Einheit und die physische Schnittstelle an, an die sie angeschlossen werden soll, sowie den Kanal, der verwendet werden soll.

1. Wählen Sie im Dialogfenster "Device Administration" aus der Liste "Devices" eine Einheit aus.
2. Klicken Sie den Eintrag **Virtual Interfaces** an, um das Dialogfenster "Add Virtual Interface Editor" (siehe Abb. 14) zu öffnen.

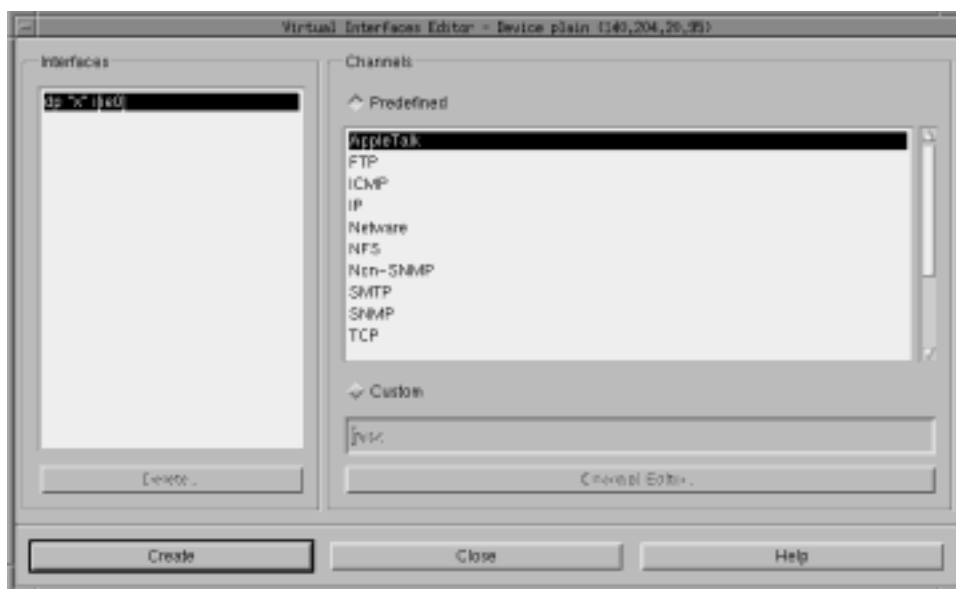


Abbildung 14. Dialogfenster "Virtual Interfaces Editor"

Dieses Dialogfenster ist in die folgenden zwei Bereiche unterteilt:

### Interfaces

Die physische Schnittstelle, der die virtuelle Schnittstelle zugeordnet werden soll.

### Channels

In einem Kanal sind die Angaben zum Filtern von Daten enthalten. Verwenden Sie einen vordefinierten Kanal (je nach Verkabelungstyp der ausgewählten physischen Schnittstelle) oder erstellen Sie einen eigenen angepassten Kanal.

3. Wählen Sie im Bereich "Interfaces" eine physische Schnittstelle auf der Einheit aus.
4. Wählen Sie einen vordefinierten Kanal aus, erstellen Sie einen eigenen angepassten Kanal, oder laden Sie einen gesicherten angepassten Kanal. Weitere Informationen hierzu sind in den Abschnitten „Einen vordefinierten Kanal auswählen“ auf Seite 45 und „Einen angepassten Kanal laden“ auf Seite 47 enthalten.

5. Klicken Sie zum Erstellen der virtuellen Schnittstelle die Option **OK** an. Daraufhin kehren Sie zum Dialogfenster "Device Administration" zurück. Dort wird die neue virtuelle Schnittstelle im Bereich "Interfaces" angezeigt. Die virtuelle Schnittstelle wird als Name der zugeordneten physischen Schnittstelle gefolgt von der Kanalbeschreibung der virtuellen Schnittstelle in runden Klammern angezeigt. Beispiel:

ie0 (IP Source 89.0.0.2).

**Anmerkung:** Informationen zum Hinzufügen von RMON- und RMON2-Tabellen zu virtuellen Schnittstellen sind in Tabelle 7 auf Seite 23 und Tabelle 8 auf Seite 24 enthalten.

### Einen vordefinierten Kanal auswählen

Aktivieren Sie zum Auswählen eines vordefinierten Kanals die Option "Predefined" und wählen Sie einen Eintrag aus der Liste aus.

Die Liste der vordefinierten Kanäle ist je nach Verkabelungstyp der ausgewählten physischen Schnittstelle unterschiedlich.

Tabelle 11. Vordefinierte Kanäle

Kanal	Beschreibung	Verkabelungstyp der physischen Schnittstelle		
		Ethernet	Token-Ring	FDDI
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 außer SNMP-Paketten	■	■	■
SMTP	Übergibt nur SMTP-Pakete	■	■	■
SNMP	Übergibt nur SNMP-Pakete	■	■	■
TCP	Übergibt TCP-Pakete	■	■	■
Telnet	Übergibt nur Telnet-Pakete	■	■	■
UDP	Übergibt UDP-Pakete	■	■	■
WWW	Übergibt nur WWW-Pakete	■	■	■
XNS	Übergibt nur XNS-Pakete	■		
X-Windows	Übergibt nur X-Windows-Pakete	■	■	■

## Einen eigenen angepaßten Kanal erstellen

1. Aktivieren Sie zum Erstellen eines angepaßten Kanals die Option **Custom**.
2. Klicken Sie den Eintrag **Channel Editor...** an, um das in Abb. 15 gezeigte Dialogfenster "Channel Editor" zu öffnen.

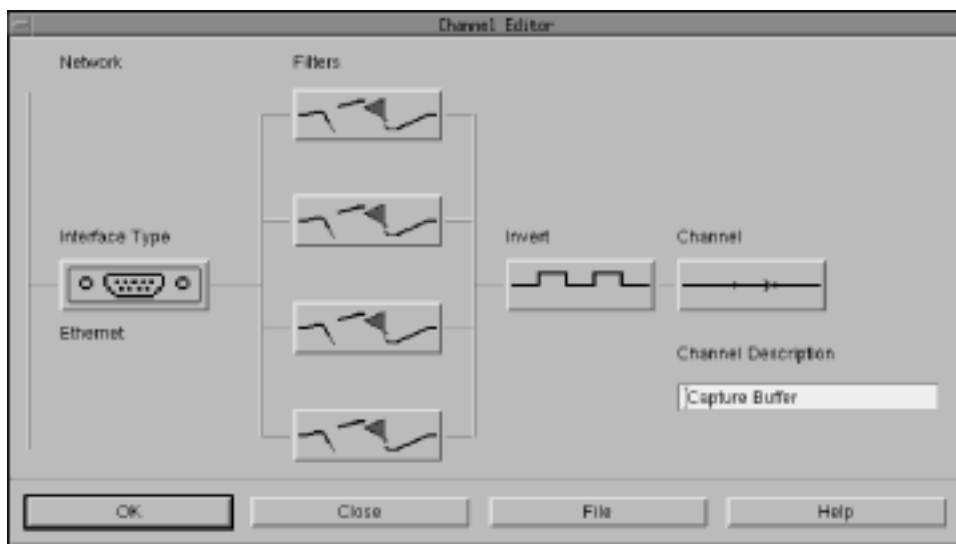


Abbildung 15. Dialogfenster "Channel Editor"




- Anmerkung:** Die Einstellung "Interface Type" wird automatisch auf den Verkabelungstyp der ursprünglichen physischen Schnittstelle gesetzt. Diese Einstellung kann nicht geändert werden.
3. Klicken Sie zum Definieren eines Filters einen der Filterknöpfe an. Dadurch wird das Dialogfenster "Filter Editor" geöffnet. Sie können weitere Filter definieren, indem Sie der Reihe nach weitere Filterknöpfe anklicken. Das Definieren eines Filters wird im Abschnitt „Funktion Filter Editor verwenden“ auf Seite 122 beschrieben. Klicken Sie die Option **OK** an, um zum Dialogfenster "Channel Editor" zurückzukehren.
  4. Der  Umkehrknopf ermöglicht Ihnen, die Logik des Filters wie folgt umzukehren.



Tabelle 12. Umkehrknopf

Umkehrknopf	Beschreibung
	Übergibt die angegebenen Pakete.
	Übergibt alle Pakete außer den angegebenen.

5. Geben Sie im Feld "Channel Description" einen eindeutigen Namen ein.  
 Sie können einen Kanal in einer Datei sichern, so daß er zu einem späteren Zeitpunkt auf eine andere Schnittstelle erneut geladen werden kann. Klicken Sie den Eintrag **File** an, um das Dialogfenster "File Save/Load" zu öffnen.
  - a. Klicken Sie die Option **Save** an.
  - b. Geben Sie im Feld "Selection" einen Dateinamen für diesen Kanal ein.
  - c. Klicken Sie das Feld **OK** an, um die Datei zu sichern und zum Dialogfenster "Channel Editor" zurückzukehren.
6. Klicken Sie zum Erstellen dieses Kanals die Option **OK** an. Daraufhin kehren Sie zum Dialogfenster "Virtual Interface Editor" zurück. Der Name des Kanals wird im Feld "Custom" angezeigt.

### Einen angepaßten Kanal laden

Sie können einen vorher mit der Anwendung "Channel Editor" gesicherten angepaßten Kanal laden oder die Informationen zum Kanal aus gesicherten Auffangpuffern extrahieren, die mit der Anwendung "Capture" erstellt wurden. Durch die Verwendung eines gesicherten Auffangpuffers aus der Anwendung "Capture" können Sie eine virtuelle Schnittstelle mit demselben Profil wie Ihre Paketerfassung erstellen.

1. Klicken Sie die Option **Custom** an.
2. Klicken Sie den Eintrag **Channel Editor...** an, um das Dialogfenster "Channel Editor" zu öffnen.
3. Klicken Sie die Option **File** an, um das Dialogfenster "File Save/Load" zu öffnen.
4. Klicken Sie die Option **Load** an.
5. Suchen Sie die Kanaldatei, und wählen Sie sie aus.
6. Klicken Sie das Feld **OK** an, um die Datei zu laden und zum Dialogfenster "Channel Editor" zurückzukehren. Dort werden die Einzeldaten zur Kanalkonfiguration angezeigt.
7. Klicken Sie im Dialogfenster "Channel Editor" das Feld **OK** an, um diesen angepaßten Kanal zu erstellen und zum Dialogfenster "Virtual Interface" zurückzukehren.

## Virtuelle Schnittstellen löschen

Das Löschen von virtuellen Schnittstellen wird über das Dialogfenster "Virtual Interfaces" durchgeführt.

1. Wählen Sie aus der Liste "Interfaces" die virtuelle Schnittstelle aus, die gelöscht werden soll.
2. Klicken Sie die Option **Delete** an.
3. Das Dialogfenster "Delete Virtual Interfaces Tables List" wird angezeigt (siehe Abb. 16). Sie werden gefragt, ob Sie die virtuelle Schnittstelle und die ihr zugeordneten Tabellen löschen möchten.

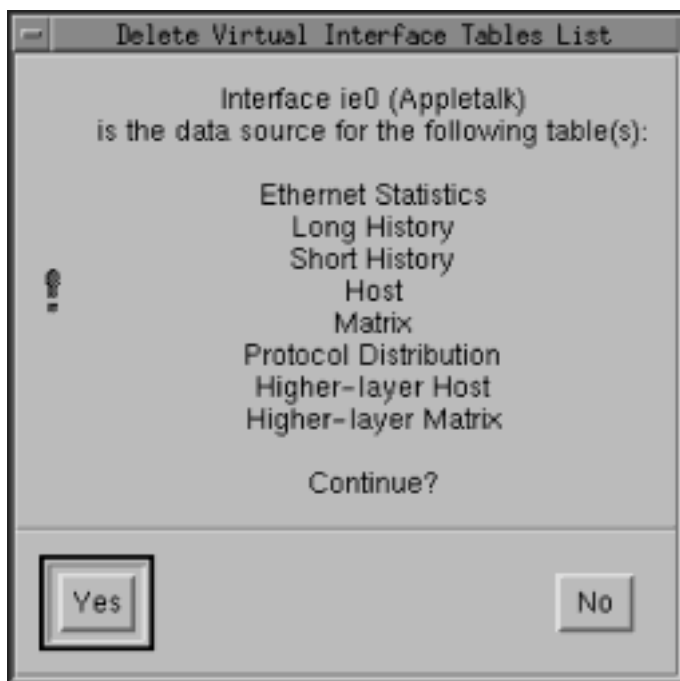


Abbildung 16. Dialogfenster "Delete Virtual Interface Tables List"

**Anmerkung:** Falls es sich bei der virtuellen Schnittstelle um eine gemeinsam benutzte Ressource handelt, sollten Sie sicherstellen, daß sie nicht von anderen Benutzern benötigt wird, bevor Sie sie löschen.

4. Klicken Sie zur Bestätigung das Feld **Yes** an, oder klicken Sie das Feld **No** an, um zum Dialogfenster "Virtual Interfaces" zurückzukehren.

---

## Stufe der Adreßumsetzung einstellen

Durch die Stufe der Adreßumsetzung wird das Format angegeben, das von Nways Manager Remote Monitor verwendet wird, um Stationen im Hauptfenster und in allen stationsbezogenen Anzeigen zu benennen. Wenn Sie diese Einstellung ändern, werden die Änderungen bei der nächsten Aktualisierung in allen geöffneten Anzeigen und Dialogfenstern vorgenommen.

Nways Manager Remote Monitor versucht immer, die höchste angeforderte Stufe anzuzeigen. (Siehe Tabelle 13 auf Seite 51.) Wenn diese nicht verfügbar ist, wird der höchstmögliche Stufenname verwendet. Daher wird in den Diagrammen im Hauptfenster möglicherweise eine Kombination aus verschiedenen Namensstufen angezeigt.

Außerdem können Sie einstellen, wie oft Nways Manager Remote Monitor Informationen zur Adreßumsetzung hochladen soll.

Durch diese Funktion können Sie auch den Zugriff von Nways Manager Remote Monitor auf Ihren Systemnamensservice, wie z. B. NIS, /etc/hosts oder DNS, steuern. Für alle gesehenen Pakete kann die Einheit eine Tabelle der Zuordnungen der MAC-Adressen zu Adressen der Vermittlungsschicht erstellen. Diese Tabelle wird anschließend von Nways Manager Remote Monitor verwendet, um eine beliebige verfügbare Namensumsetzung für die abgerufene Protokolladresse zu erhalten.

**Anmerkung:** Informationen zur Adreßumsetzung werden von jeder Einheit gesammelt, die gegenwärtig im Hauptfenster von Nways Manager Remote Monitor zur Überwachung verwendet wird.

Gehen Sie wie folgt vor, um die Stufe der Adreßumsetzung einzustellen:

1. Wählen Sie im Menü "Configure" den Eintrag **Address Translation** aus, um das in Abb. 17 auf Seite 50 gezeigte Dialogfenster "Address Translation" zu öffnen.

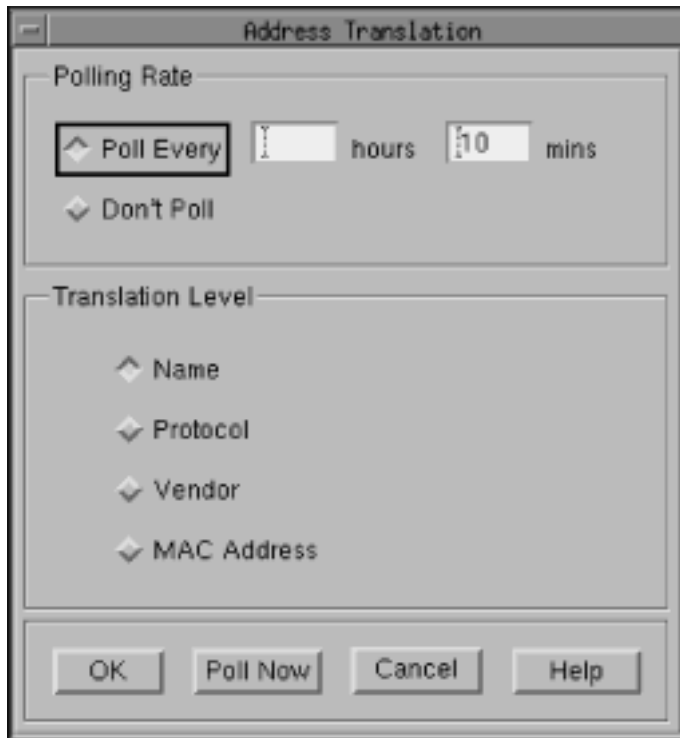


Abbildung 17. Dialogfenster "Address Translation"

2. Aktivieren Sie eine der beiden folgenden Optionen, um einzustellen, wie oft die Informationen zur Umsetzung der Netzadresse von Nways Manager Remote Monitor abgefragt werden sollen:

**Poll Every**                      Aktivieren Sie diese Option, und geben Sie die Häufigkeit der Bereitschaftsabfrage in Stunden und Minuten an. Standardmäßig erfolgt alle 10 Minuten eine Abfrage.

**Don't Poll**                      Aktivieren Sie diese Option, um die Abfragefunktion auszuschalten.

Sie können auch erzwingen, daß Nways Manager Remote Monitor sofort beginnt abzufragen, indem Sie im Dialogfenster unten die Option **Poll Now** anklicken.

**Anmerkung:** Wenn das Feld "Poll Now" abgeblendet ist, bedeutet dies, daß gerade eine Abfrage durchgeführt wird.

3. Klicken Sie eine der Umsetzstufen unter "Translation Levels" an, um die Stufe der Adreßumsetzung einzustellen, die von Nways Manager Remote Monitor nach Möglichkeit angezeigt werden soll.

Die in Tabelle 13 auf Seite 51 aufgeführten folgenden vier Stufen sind verfügbar:

*Tabelle 13. Stufen der Adreßumsetzung*

<b>Stufe</b>	<b>Beschreibung</b>
Name Translation	Hierbei handelt es sich um den der Einheit zugeordneten Namen. Dabei kann es sich um den für die Einheit gefundenen Systemnamen oder um einen beliebigen benutzerdefinierten Namen handeln.
Protocol Address	Hierbei handelt es sich um die der Einheit zugeordnete Protokolladresse (IP, IPX oder DECnet).
Vendor ID	Die ersten sechs Zeichen dieses Namens werden von der in der Datei "vendor.map" enthaltenen Hersteller-ID übernommen. Daran werden die übrigen sechs Ziffern der MAC-Adresse angehängt. Weitere Informationen hierzu sind im Abschnitt „Herstellerpräfixe angeben“ auf Seite 55 enthalten.
MAC Address	Die 12stellige MAC-Adresse wird angezeigt.

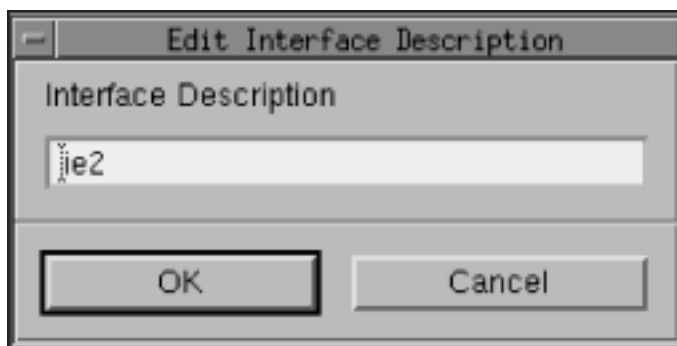
4. Klicken Sie das Feld **OK** an, um die Einstellungen zu sichern und zum Hauptfenster zurückzukehren.

## Schnittstellen umbenennen

Wenn schreibbare Schnittstellenbeschreibungen von einer Einheit unterstützt werden, können Sie den Namen der physischen Schnittstellen auf dieser Einheit über das Dialogfenster "Device Administration" ändern.

Gehen Sie zum Ändern einer Schnittstellenbeschreibung wie folgt vor:

1. Wählen Sie eine Einheit aus der Liste "Devices" aus.
2. Wählen Sie die physische Schnittstelle aus, deren Name in der Liste "Interfaces" geändert werden soll. Bei Auswahl einer virtuellen Schnittstelle wird das Feld "Interface Description" unterhalb der Liste "Interfaces" abgeblendet angezeigt.
3. Klicken Sie den Eintrag **Interface Description** an, um das in Abb. 18 gezeigte Dialogfenster "Edit Interface Description" zu öffnen.



*Abbildung 18. Dialogfenster "Edit Interface Description"*

4. Bearbeiten Sie den Inhalt des Feldes "Interface Description", und klicken Sie das Feld **OK** an.
5. Der neue Name der Schnittstelle wird in der Liste "Interfaces" angezeigt. Dabei werden auch alle der geänderten physischen Schnittstelle zugeordneten virtuellen Schnittstellen aktualisiert. Dadurch kann der neue Name der physischen Schnittstelle zusammen mit dem Kanalnamen der virtuellen Schnittstelle angezeigt werden.
6. Klicken Sie zum Zurücksetzen des Schnittstellennamens auf seine ursprüngliche Beschreibung den Eintrag **Interface Description** an. Dadurch wird das Dialogfenster "Interface Description" geöffnet. Löschen Sie den Inhalt des Feldes "Interface Description" und klicken Sie das Feld **OK** an.

---

## Benutzerdefinierte Protokolle verwalten

Das Protokollverzeichnis ist eine Komponente des RMON2-Standards. Es listet alle Protokolle auf, für die die Einheit Statistiken erstellt. Mit Hilfe von Nways Manager Remote Monitor ist es möglich, das Protokollverzeichnis auf einer RMON2-Einheit anzuzeigen und benutzerdefinierte Protokolle zu erstellen oder zu löschen.

Wenn Sie auf Ihrem Netzwerk angepaßte Protokolle oder Protokollkapselungen verwenden, ermöglicht Ihnen Nways Manager Remote Monitor, diese Protokolle zu definieren und sie zu Ihrem Protokollverzeichnis hinzuzufügen. Dadurch wird die Leistungsfähigkeit der Anzeige "Protocol Distribution" von Nways Manager Remote Monitor verbessert. Informationen zu den von RMON2-kompatiblen Einheiten unterstützten Protokollen sind im Anhang C enthalten.

## Protokollverzeichnis anzeigen

Wählen Sie im Hauptfenster im Menü "Configure" den Eintrag "Protocol Directory" aus. Dadurch wird das Dialogfenster "Protocol Directory Manager" (siehe Abb. 19) geöffnet.

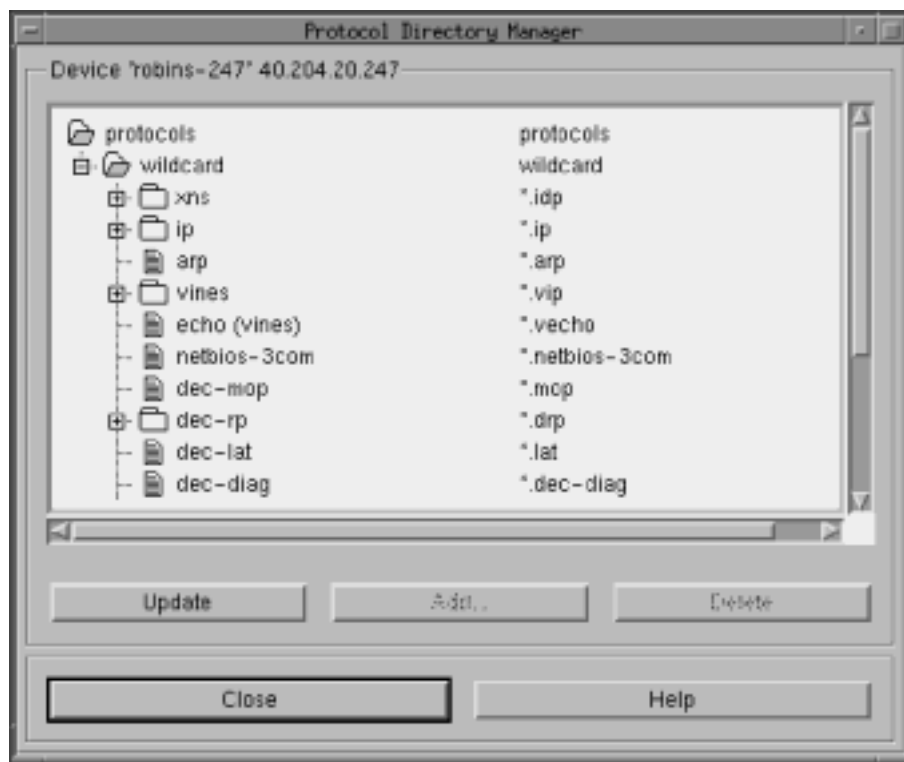


Abbildung 19. Dialogfenster "Protocol Directory Manager"

Im Dialogfenster werden alle Protokolle angezeigt, für die die Einheit Statistiken erstellt.

Diese Anzeige besteht aus zwei Spalten. In der ersten wird die Protokollhierarchie und in der zweiten der vollständige Kapselungspfad für jedes Protokoll angezeigt.

**Anmerkung:** Wenn ein Protokollname zu lang für die Anzeige ist, wird er in abgekürzter Form angezeigt. Klicken und ziehen Sie die Maus am rechten Rand der Spalte, um diese zu erweitern.

## Ein Protokoll hinzufügen

Gehen Sie zum Hinzufügen eines benutzerdefinierten Protokolls wie folgt vor:

1. Klicken Sie im Dialogfenster "Protocol Directory" die Option **Add...** an. Dadurch wird das in Abb. 20 gezeigte Dialogfenster "New Protocol" geöffnet.

**Anmerkung:** Wenn ein Protokoll nicht erweitert werden kann, ist die Option **Add...** inaktiviert. Überprüfen Sie, ob benutzerdefinierte Protokolle von der Einheit unterstützt werden.



Abbildung 20. Dialogfenster "New Protocol"

2. Geben Sie für das gewünschte Protokoll einen Namen und eine Protokollnummer ein. Wenn Sie kein Protokoll hinzufügen können, liegt dafür möglicherweise eine der beiden folgenden Ursachen vor:

- Das Protokoll, das Sie hinzufügen möchten, ist bereits vorhanden.
- Die Einheit verfügt nicht mehr über genügend Speicherkapazitäten. Sie müssen ein Protokoll löschen und einen erneuten Warmstart durchführen, bevor Sie ein weiteres Protokoll hinzufügen können.

**Anmerkung:** Wenn Sie einen erneuten Kaltstart durchführen, gehen alle benutzerdefinierten Protokollinformationen verloren.

3. Klicken Sie das Feld **OK** an, um zum Dialogfenster "Protocol Directory Manager" zurückzukehren.



## Ein Protokoll löschen

Nways Manager Remote Monitor ermöglicht das Löschen von Protokollen, die Sie einer Einheit hinzugefügt haben. Gehen Sie zum Löschen eines Protokolls wie folgt vor:

1. Wählen Sie das betreffende Protokoll im Dialogfenster "Protocol Directory Manager" aus.
2. Klicken Sie die Option **Delete** an. Sie werden aufgefordert, den Löschvorgang zu bestätigen oder abzubrechen.

---

## Herstellerpräfixe angeben

Jede Einheit verfügt über eine eindeutige MAC-Adresse. MAC-Adressen bestehen aus folgenden zwei Teilen: dem Herstellerpräfix und der Seriennummer der Schnittstelle. Das Herstellerpräfix setzt sich aus den ersten sechs Stellen einer MAC-Adresse zusammen. Jedem Hersteller wird vom IEEE ein Block von MAC-Adressen zugeordnet. Der Hersteller ordnet dann jeder hergestellten Einheit eine andere Schnittstellenseriennummer zu.

Bei Lieferung verfügt Nways Manager Remote Monitor über Definitionen der am weitesten verbreiteten Herstellerpräfixe. Beispielsweise wird automatisch erkannt, daß es sich bei einer Einheit mit der MAC-Adresse "08005A000001" um eine IBM Einheit mit der Schnittstellenseriennummer "000001" handelt.

**Anmerkung:** Das Zeichen \$ stellt die Schnittstellenseriennummer in der MAC-Adresse dar.

Verwenden Sie zum Anzeigen vorhandener Herstellerpräfixe einen Texteditor, mit dem Sie die Datei "vendor.map" im Verzeichnis "/usr/LANReMon/rmoncommon/maps" öffnen können. Bearbeiten Sie die Datei "vendor.map" wie folgt, um eigene Herstellerpräfixumsetzungen hinzuzufügen:

1. Gehen Sie an das Ende der Datei "vendor.map".
2. Geben Sie in einer neuen Zeile das gewünschte Herstellerpräfix gefolgt von der Hersteller-ID ein. Die Hersteller-ID muß aus genau sechs Zeichen bestehen, auf die das Zeichen \$ folgt. Falls die Hersteller-ID aus weniger als sechs Zeichen besteht, können Sie sie durch Verwendung von Unterstreichungen auf sechs Zeichen erweitern. Beispiel: 123456 myDev\_\$

In diesem Fall lautet die ursprünglich zugeordnete Zahl "123456". Der Eintrag in der Datei "vendor.map" hat zur Folge, daß alle Einheiten, deren MAC-Adressen mit "123456" beginnen, als "myDev\_" gefolgt von den übrigen sechs Stellen der MAC-Adresse angezeigt werden.

**Anmerkung:** Sie müssen die Anwendung erneut starten, damit die Änderungen in der Datei "vendor.map" wirksam werden.



---

## Kapitel 4. Hauptfenster von Nways Manager Remote Monitor

In diesem Kapitel werden die Informationen im Hauptfenster von Nways Manager Remote Monitor beschrieben. Das Kapitel enthält die folgenden Abschnitte:

- Übersicht
- Beschreibung des Hauptfensters von Nways Manager Remote Monitor
- Hauptfenster anpassen
- Auf mehrere Fenster zugreifen
- Informationen im Hauptfenster lesen
- Diagramme über Nways Manager Remote Monitor ausgeben

---

### Übersicht

Das Hauptfenster von Nways Manager Remote Monitor zeigt wichtige Informationen zur Verwendung eines LAN-Segments und zu Fehlern an. Außerdem werden ausgelöste Alarm- und Statusnachrichten angezeigt. Indem Sie eine physische Schnittstelle auf einer fernen Einheit auswählen, können Sie die Leistung und den Zustand des gesamten überwachten Netzwerksegments anzeigen. Bei Auswahl einer virtuellen Schnittstelle können Sie die Leistung für eine Untergruppe von Netzwerkdaten anzeigen. Sie können Fenster zu anderen Segmenten öffnen, um mehrere Segmente gleichzeitig anzuzeigen. Sie können das Hauptfenster an Ihre Überwachungserfordernisse anpassen, indem Sie auswählen, ob alle Diagramme oder nur eine Auswahl angezeigt werden sollen. Außerdem können Sie Teile der angezeigten Diagramme besonders detailliert anzeigen, indem Sie den betreffenden Teil des Diagramms anklicken.

---

### Beschreibung des Hauptfensters von Nways Manager Remote Monitor

Das Hauptfenster von Nways Manager Remote Monitor ermöglicht Ihnen, die Leistung eines Netzwerksegments zu überwachen und ausgelöste Alarmnachrichten anzuzeigen. Dadurch können Sie auf Änderungen in den Netzwerkbedingungen reagieren. Sie können mehrere Hauptfenster öffnen und dadurch mehrere Segmente gleichzeitig anzeigen.

Das Hauptfenster ist, wie in Abb. 21 auf Seite 58 gezeigt, in die folgenden Bereiche unterteilt:

- Menüleiste
- Knopfleiste
- Zusammenfassungsbereich
- Alarmleiste
- Statusleiste

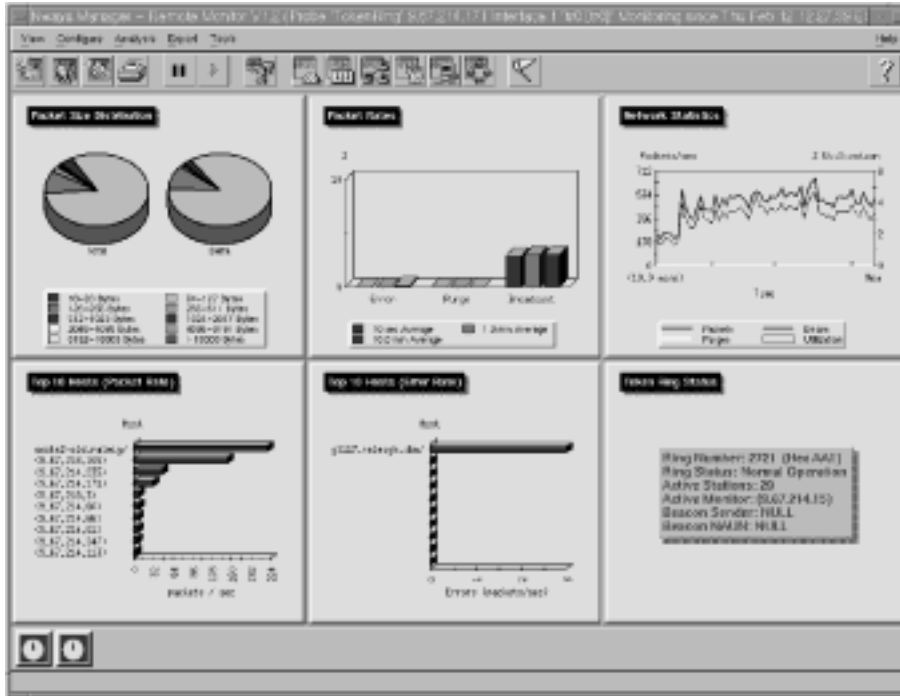


Abbildung 21. Hauptfenster von Nways Manager Remote Monitor

## Menüleiste
















Die Menüleiste oben im Fenster enthält die folgenden Menübefehle:

- |                  |   |
|------------------|---|
| <b>View</b>      | Diese Menüoption wird in erster Linie für Parameter des Hauptfensters benötigt. Sie ermöglicht Anpassungen, Pausen, erneutes Starten und Ausgaben vom aktuellen Hauptfenster aus.   |
| <b>Configure</b> | Über diese Menüoption können Sie auf die Einheitenadministration, die Funktion "Protocol Directory Manager", die Adreßumsetzung und die Funktionalität von "Roving Analyzer Port" zugreifen.  |
| <b>Analysis</b>  | Über diese Menüoption können Sie auf die RMON-Anzeigen ("Statistics", "History", "Host", "Alarms", "Matrix" und "Ring Station") zugreifen. Darüber hinaus erhalten Sie Zugriff auf die Funktionen zum Erfassen, zum Erstellen von Adreß-Maps und zur Protokollverteilung sowie auf die PACMIB-Funktionalität. |
| <b>Export</b>    | Über diese Menüoption können Sie spezifische statistische RMON-Gruppen zur Anzeige auswählen. Hierzu können Sie die Anwendung "Data Export" verwenden.  |
| <b>Tools</b>     | Über diese Menüoption können Sie auf die Anwendung "Data Collection" und auf ECAM-Funktionen zugreifen.   |
| <b>Help</b>      | Diese Menüoption stellt Hilfe zu Nways Manager Remote Monitor bereit.   |

## Knopfleiste

Die Knopfleiste unterhalb der Menüleiste enthält eine Liste der verfügbaren Anwendungen und Anzeigen von Nways Manager Remote Monitor. Wenn Sie die Maus auf einen Knopf setzen, wird auf dem Bildschirm eine Beschreibung des Knopfes angezeigt. Klicken Sie einen Knopf an, um das Dialogfenster der entsprechenden Anwendung aufzurufen. In Tabelle 14 werden die Funktionen der Knöpfe erklärt.

Tabelle 14. Knöpfe in der Knopfleiste des Hauptfensters

Knopf	Funktion	Knopf	Funktion	Knopf	Funktion
	New View (neue Anzeige)		Device Administration (Einheiten-administration)		Print View (Anzeige für die Ausgabe)
	Modify View (Änderungsanzeige)		RMON Statistics (RMON-Statistiken)		Pause main window (Hauptfensteraktionen anhalten)
	Restart View (Neustartanzeige)		RMON History (RMON-Protokoll)		Resume main window (Hauptfenster wieder aufnehmen)
	RMON Ring Station		RMON Host		RMON Matrix
	Anwendung "Capture"		RMON Alarms		Online Help (Online-Hilfefunktion)

## Zusammenfassungsbereich

Die sechs Anzeigen im Zusammenfassungsbereich bilden zusammen den größten Bereich des Hauptfensters. Diese Anzeigen enthalten grafische Darstellungen von wichtigen Statistiken zum Netzwerk. Je nach Verkabelungstyp des überwachten Segments unterscheiden sie sich voneinander.

Im Abschnitt „Beschreibung der verfügbaren Diagramme“ auf Seite 63 wird eine Übersicht über die verschiedenen Diagramme gegeben.

## Alarmleiste

Die Alarmleiste befindet sich unter dem Zusammenfassungsbereich. Wenn Alarmnachrichten auf der überwachten Einheit konfiguriert wurden, werden in dieser Leiste bei Auslösung eines Alarms Alarmsymbole angezeigt. (Eine Beschreibung von Alarmnachrichten ist in Kapitel 6 enthalten.)

## Statusleiste

Auf der Statusleiste werden Statusinformationen zu Alarmnachrichten und Hilfetexte zur Knopfleiste und zu Menüpunkten angezeigt. Setzen Sie den Mauszeiger auf einen Knopf in der Knopfleiste, einen Menüpunkt oder ein Alarmsymbol, damit betreffende Informationen auf der Statusleiste angezeigt werden.

---

## Hauptfenster anpassen

Das Hauptfenster wird über das Dialogfenster "Modify Current View" angepaßt. Über dieses Dialogfenster können Sie folgendes auswählen:

1. Das LAN-Segment, das überwacht werden soll.
2. Die Diagramme, die angezeigt werden sollen.
3. Das Aktualisierungsintervall für die angezeigten Daten.

Gehen Sie zum Anpassen des Hauptfensters wie folgt vor:

1. Wählen Sie im Menü "View" die Option **Modify** aus, oder klicken Sie in der Knopfleiste den Knopf **Modify View** an. Dadurch wird das Dialogfenster "Modify Current View" angezeigt.
2. Wählen Sie das Netzwerksegment aus, das überwacht werden soll, indem Sie die beiden folgenden Schritte durchführen:
  - a. Wählen Sie im Bereich "Devices" eine Einheit aus. Wenn die Einheit kontaktfähig ist, wird im Bereich "Interfaces" eine Liste mit verfügbaren Schnittstellen angezeigt.
  - b. Wählen Sie im Bereich "Interfaces" eine physische oder eine virtuelle Schnittstelle aus. Bei Auswahl einer virtuellen Schnittstelle wird die für diese Schnittstelle konfigurierte Datenuntergruppe überwacht. (Weitere Informationen hierzu sind im Abschnitt „Virtuelle Schnittstellen konfigurieren“ auf Seite 43 enthalten.)
3. Der aktuell verwendete Name für die Benutzergemeinschaft wird im Feld "Community Name" angezeigt. Gehen Sie wie folgt vor, um den Namen der Benutzergemeinschaft zu ändern:
  - a. Klicken Sie die Option **Edit** an. Dadurch wird das in Abb. 22 auf Seite 61 gezeigte Dialogfenster "Edit Community Name" angezeigt.

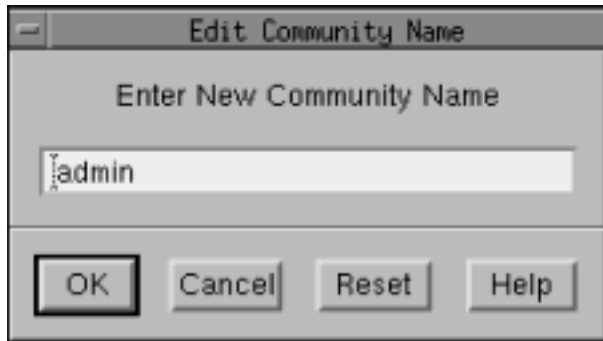


Abbildung 22. Dialogfenster "Edit Community Name"

- 1) Geben Sie den neuen Namen für die Benutzergemeinschaft ein.
  - 2) Klicken Sie das Feld **OK** an, um die Änderungen zu sichern und zum Dialogfenster "Modify Current View" zurückzukehren. Ab sofort wird bei jeder folgenden Kommunikation mit der Einheit der neue Name für die Benutzergemeinschaft verwendet.
  - 3) Falls ein Zurücksetzen auf den in der Datei probe.map enthaltenen Standardnamen für die Benutzergemeinschaft erforderlich wird, öffnen Sie das Dialogfenster "Edit Community Name" und klicken Sie die Option **Reset** an. Klicken Sie das Feld **OK** an, und der auf der Einheit gespeicherte Name für die Benutzergemeinschaft wird verwendet.
4. Wählen Sie die anzuzeigenden Diagramme und das Aktualisierungsintervall wie folgt aus:
- a. Wählen Sie im Bereich "Available Graphs" die Diagramme aus, die angezeigt werden sollen. In der Standardeinstellung werden alle Diagramme ausgewählt. Die Liste der Diagramme ist je nach Verkabelungstyp der ausgewählten Schnittstelle oder Einheit unterschiedlich. Eine Definition der verfügbaren Diagramme ist im Abschnitt „Beschreibung der verfügbaren Diagramme“ auf Seite 63 enthalten.
  - b. Stellen Sie das Intervall ein, mit dem die Diagramme mit neuen Daten aktualisiert werden sollen. Die Angabe erfolgt in Sekunden. Dieses Intervall gilt für alle Diagramme. Der Standardwert beträgt 10 Sekunden.

Klicken Sie das Feld **OK** an, um die vorgenommene Auswahl zu bestätigen. Dadurch, daß das Hauptfenster mit Hilfe von Nways Manager Remote Monitor aktualisiert wird, ist eine Konzentration auf das ausgewählte Netzwerksegment möglich.

---

## Auf mehrere Fenster zugreifen

Sie können sowohl das aktive Fenster über das Dialogfenster "Modify Current View" anpassen, als auch ein neues Fenster zu einem anderen Netzwerksegment anzeigen. Die durchzuführenden Schritte ähneln denen im vorangegangenen Abschnitt, aber Sie müssen eine andere Einheit oder, falls Sie Einheiten mit mehreren Schnittstellen verwenden, eine andere Schnittstelle auf der Einheit auswählen.

1. Wählen Sie im Menü "View" die Option **New** aus, oder klicken Sie in der Knopfleiste den Knopf **New View** an. Dadurch wird das Dialogfenster "Create New View" geöffnet.

Bei Einträgen, die gegenwärtig zur Überwachung in einem Hauptfenster verwendet werden, sind der Name der Einheit und der Schnittstelle mit einem Stern (\*) versehen.

2. Wählen Sie im Bereich "Devices" eine Einheit aus, um das Segment auszuwählen, das überwacht werden soll. Wählen Sie anschließend im Bereich "Interfaces" eine Schnittstelle aus.
3. Der aktuell verwendete Name für die Benutzergemeinschaft wird im Feld "Community" angezeigt. Befolgen Sie die Anweisungen im Abschnitt „Hauptfenster anpassen“ auf Seite 60, um den Namen der Benutzergemeinschaft zu ändern.
4. Wählen Sie die Diagramme und das Aktualisierungsintervall aus, indem Sie die Anweisungen in Schritt 4 des Abschnitts „Hauptfenster anpassen“ auf Seite 60 befolgen.
5. Klicken Sie das Feld **New** an, um ein neues Fenster mit der ausgewählten Konfiguration zu öffnen.

Neue Fenster enthalten dieselbe Funktionalität wie das ursprüngliche Hauptfenster.

---

## Informationen im Hauptfenster lesen

Dieser Abschnitt beschreibt folgendes:

1. Anhalten und erneutes Starten des Hauptfensters.
2. Die unterschiedlichen LAN-Diagramme, die im Hauptfenster angezeigt werden können.

### Hauptfenster anhalten

Sie können das Hauptfenster vorübergehend anhalten und verhindern, daß Datenaktualisierungen angezeigt werden.

**Anmerkung:** Wenn mehrere Fenster geöffnet sind, wird nur das aktuelle Fenster angehalten.



Klicken Sie in der Knopfleiste den Knopf "Pause Main Window" an, oder wählen Sie im Menü "View" die Option "Pause" aus, um die Anzeige des Hauptfensters anzuhalten. Klicken Sie den Knopf "Resume Main Window" in der Knopfleiste an, oder wählen Sie im Menü "View" die Option "Restart" aus, um eine erneute Aktualisierung der Anzeige des Hauptfensters zu starten.

Wenn Sie eine erneute Aktualisierung der Datenanzeige starten, werden die Diagramme am Ende des aktuellen Aktualisierungszeitraums aktualisiert. Dadurch werden alle seit dem Haltepunkt gesammelten Daten berücksichtigt.

**Anmerkung:** Die Datensammlung wird auch bei angehaltenem Hauptfenster fortgeführt.

### Beschreibung der verfügbaren Diagramme

Die Liste der verfügbaren Diagramme ist je nach Verkabelungstyp der ausgewählten Einheit oder, falls Einheiten mit mehreren Schnittstellen verwendet werden, der ausgewählten Schnittstelle unterschiedlich. Die Diagramme sind in Tabelle 15 aufgeführt.

Tabelle 15. Je nach Verkabelungstyp verfügbare Diagramme

Liste der Diagramme	Verkabelungstyp		
	Ethernet	Token-Ring	FDDI
Packet Size Distribution	■	■	■
Packet Rates	■	■	■
Network Statistics	■	■	■
Top 10 Hosts by Packet Rate	■	■	■
Top 10 Hosts by Error Rate	■	■	
Top 10 Receivers			■
Event Distribution	■		
Token Ring Status		■	■

In diesem Abschnitt werden die einzelnen Diagramme definiert. Ferner wird erläutert, wie sie zur Überwachung des Netzwerks verwendet werden können.

## Packet Size Distribution

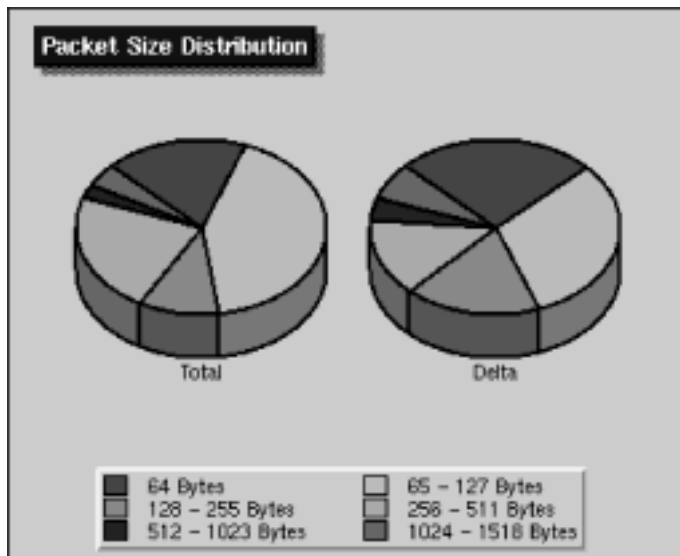


Abbildung 23. Diagramm "Packet Size Distribution"

Mit Hilfe des Diagramms "Packet Size Distribution" (siehe Abb. 23) wird die Zusammensetzung des Datenverkehrs auf dem Netz veranschaulicht. Sie zeigt, ob das Segment viele kleine Pakete überträgt oder ob es durch große Pakete gesättigt ist.

Die Angabe "Total" zeigt den Trend bei den Paketgrößen seit Erstellung der Statistiktabelle an. Die Angabe "Delta" zeigt die Verteilung von Paketgrößen während des letzten untersuchten Zeitraums an.

### Packet Rates bzw. Frame Rates

In Abb. 24 wird ein Beispiel für ein Paketratendiagramm dargestellt.

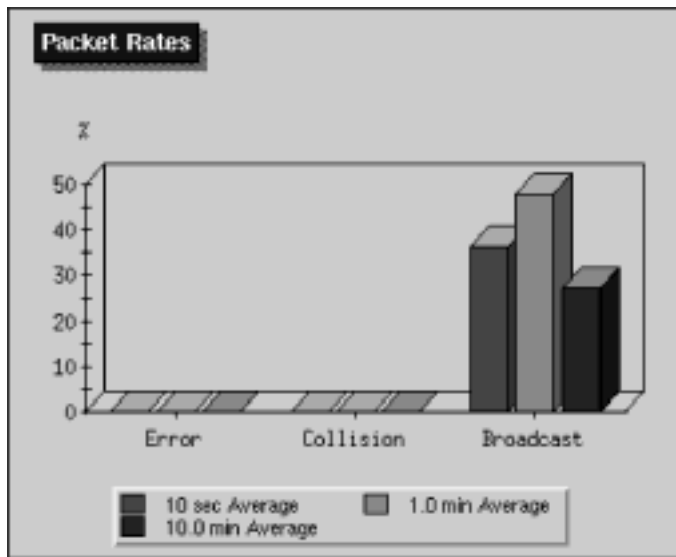


Abbildung 24. Diagramm "Packet Rates"

In den Diagrammen "Packet Rates" und "Frame Rates" wird dargestellt, wie viele Broadcast-Pakete, Fehler, Kollisionen, Freigabeereignisse oder SMT-Rahmen (nur FDDI) im Netzwerk entdeckt wurden. Dadurch kann die Leistung des Netzwerks schnell beurteilt werden. Sowohl die aktuelle als auch die vorausgegangene Netzwerkaktivität wird dargestellt.

## Network Statistics

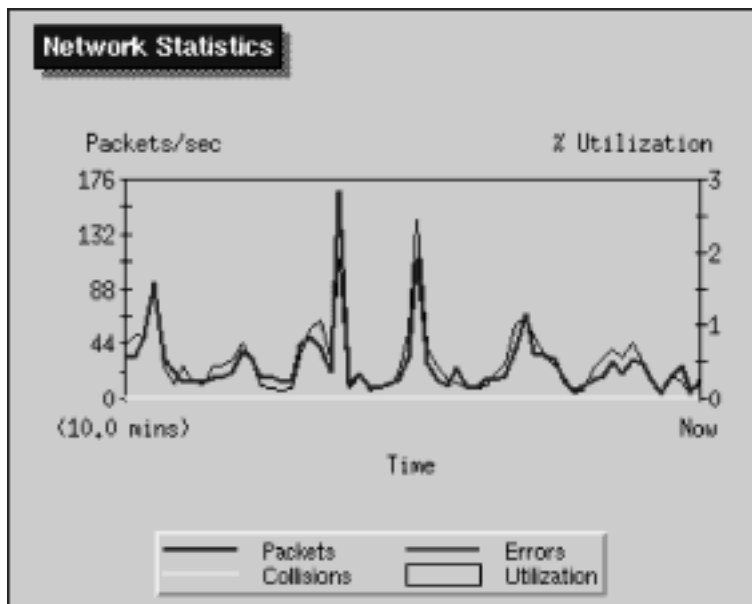


Abbildung 25. Diagramm "Network Statistics"

Im Diagramm "Network Statistics" (siehe Abb. 25) wird die Leistung des Netzwerks während der letzten n Minuten dargestellt (wobei n von der Aktualisierungsfrequenz abhängt). Dadurch können kurzfristige Trends erkannt werden. Durch einen Vergleich der Anzahl an Paketen mit Auslastungsstufen (Utilization) ist es möglich, eine Vorstellung von der Anzahl der üblicherweise im Netzwerk gesehenen Pakete zu erhalten. In Tabelle 16 wird aufgeführt, welche Netzwerkstatistiken für welchen Verkabelungstyp verfügbar sind.

Tabelle 16. Vom Verkabelungstyp abhängige Variablen des Diagramms "Network Statistics"

Variablen	Verkabelungstyp		
	Ethernet	Token-Ring	FDDI
Collisions	■		
Aborts	■	■	■
Packets	■	■	■
Purges		■	
SMT Frames			■
Utilization	■	■	■

## Top 10 Hosts (Packet Rate)

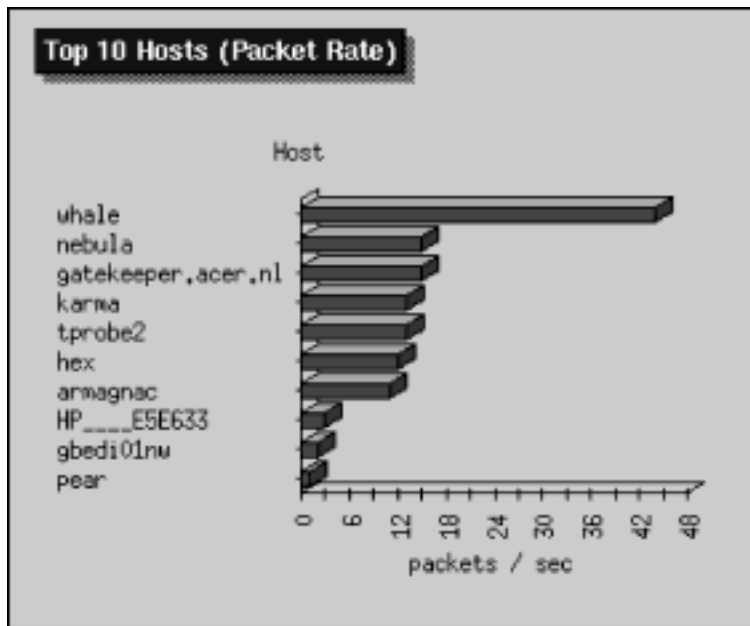


Abbildung 26. Diagramm "Top 10 Hosts (Packet Rate)"

Mit Hilfe des Diagramms "Top 10 Hosts (Packet Rate)" (siehe Abb. 26) werden die aktivsten Hosts im Segment identifiziert. Im Diagramm wird dargestellt, welche Hosts oder Stationen im Netzwerk den meisten Datenverkehr generieren. Das Diagramm ist für Ethernet, Token-Ring und FDDI verfügbar.

Klicken Sie die entsprechende Leiste an, um eine geordnete Liste der Datenaustauschvorgänge für den Host anzuzeigen. Diese Liste zeigt an, ob der Host mit mehreren Stationen hohe Datenmengen austauscht (was möglicherweise lediglich auf eine aktive Station hinweist) oder nur mit ein bis zwei Einheiten (was möglicherweise auf Client/Server-Aktivität hinweist).

## Top 10 Hosts (Error Rate) (Ethernet und Token-Ring)

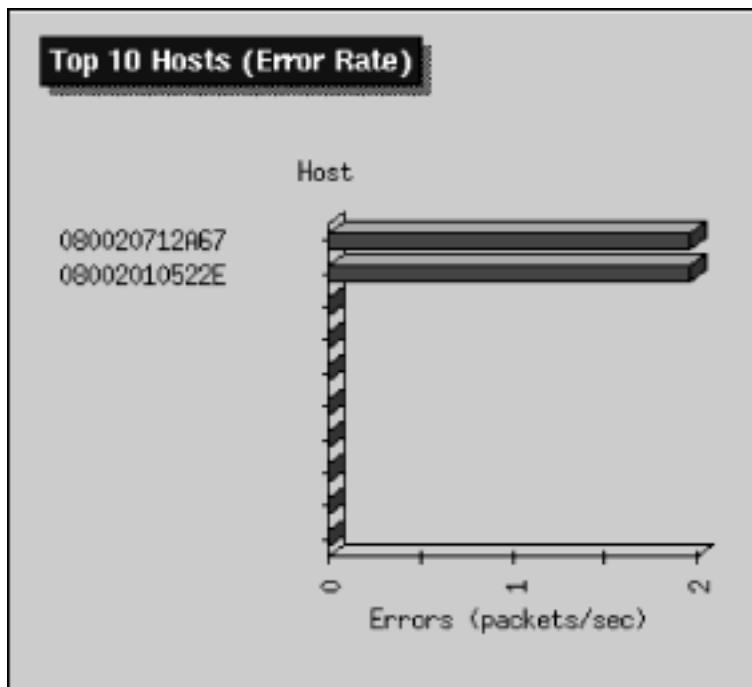


Abbildung 27. Diagramm "Top 10 Hosts (Error Rate)"

Im Diagramm "Top 10 Hosts (Error Rate)" (siehe Abb. 27) wird dargestellt, woher die meisten Fehlerpakete kommen und mit wem die betroffenen Stationen kommunizieren. Das Diagramm ist für Ethernet und für Token-Ring verfügbar.

Klicken Sie eine Leiste auf dem Histogramm an, um detailliertere Informationen zu den möglichen Ursachen für Netzwerkprobleme zu erhalten.

## Top 10 Receivers (FDDI)

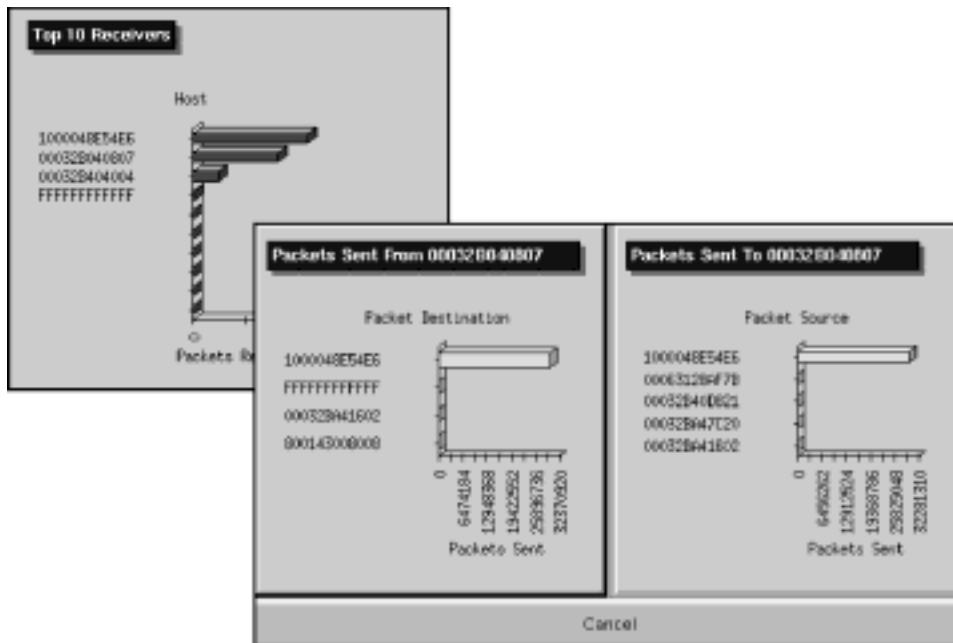


Abbildung 28. Diagramm "Top 10 Receivers"

Für FDDI-Schnittstellen erscheint das Diagramm "Top 10 Receivers" (siehe Abb. 28) anstelle des Diagramms "Top 10 Hosts (Error Rate)", das für Ethernet- und für Token-Ring-Schnittstellen angezeigt wird. In diesem Diagramm werden die zehn wichtigsten Zieladressen für Datenverkehr im Netzwerk angezeigt.

## Event Distribution (Ethernet)

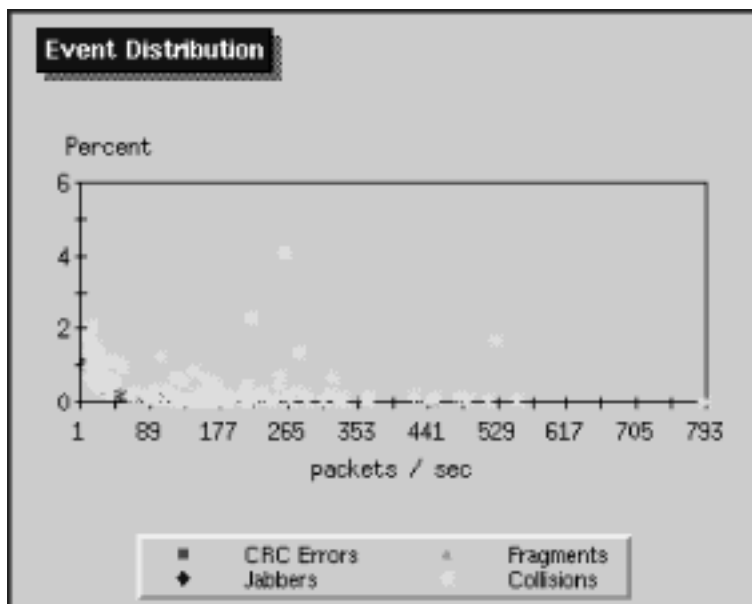


Abbildung 29. Diagramm "Event Distribution"

Das Diagramm "Event Distribution" (siehe Abb. 29) stellt die Beziehung zwischen der Paketrate und den Fehlern, die in einem Segment gesehen werden, dar. Beispielsweise könnte angezeigt werden, daß bei 200 Paketen pro Sekunde 2% aller Pakete Kollisionen sind.



## Ring-Status

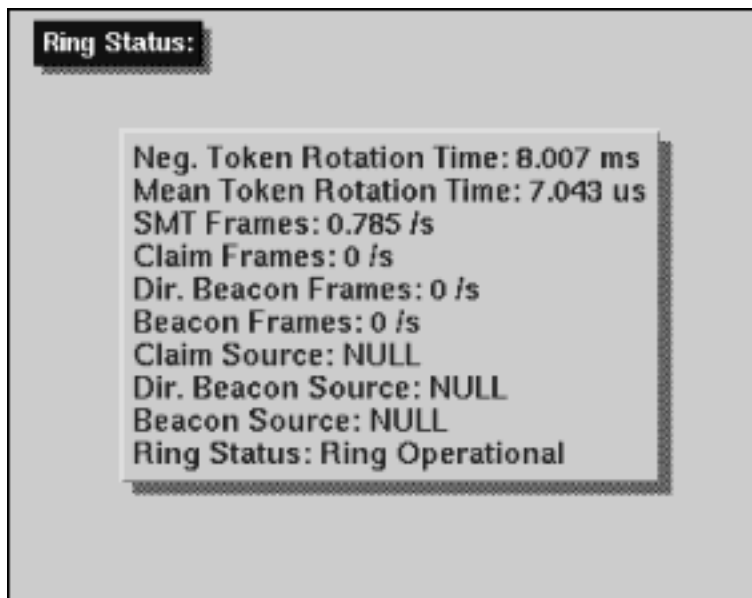


Abbildung 30. Anzeige "Ring-Status"

Die Anzeige "Ring Status" (siehe Abb. 30) enthält eine fortlaufend aktualisierte Zusammenfassung von Ringinformationen für FDDI (siehe Tabelle 17 auf Seite 72) oder Token-Ring (siehe Tabelle 18 auf Seite 72).

Tabelle 17. FDDI-Variablen in der Anzeige "Ring Status"

Variable	Definition
Neg. Token Rotation Time	Die Umlaufdauer, die vom Gewinner des Prozesses zur Senderechanforderung angeboten wird.
Mean Token Rotation Time	Die durchschnittliche Umlaufdauer des Token im letzten Erfassungszeitraum.
SMT Frames	Die Rate der auf diesem Ring gesehenen SMT-Rahmen in Rahmen pro Sekunde.
Claim Frames	Die Rate der auf diesem Ring gesehenen Anforderungsrahmen in Rahmen pro Sekunde.
Dir. Beacon Frames	Die Rate der auf diesem Ring gesehenen übertragenen Beacon-Nachrichten in Rahmen pro Sekunde.
Beacon Frames	Die Rate der auf diesem Ring gesehenen Beacon-Nachrichten in Rahmen pro Sekunde.
Claim Source	Die Adresse des Host, der den letzten Anforderungsrahmen gesendet hat. Dabei handelt es sich um den Gewinner des Prozesses zur Senderechanforderung. Gegenwärtig wird diese Variable nicht unterstützt und mit einem Nullwert angezeigt.
Dir. Beacon Source	Die Adresse des Host, der die letzte übertragene Beacon-Nachricht gesendet hat.
Beacon Source	Die Adresse des Host, der die letzte Beacon-Nachricht gesendet hat.
Ring Status	Der aktuelle Betriebsstatus des FDDI-Rings: <ol style="list-style-type: none"> <li>1. Ring Operational (Ring im Betrieb)</li> <li>2. Non Operational Claim (Bestätigung nicht im Betrieb)</li> <li>3. Non Operational Beacon (Beacon-Nachricht nicht im Betrieb)</li> <li>4. Non Operational Directed beacon (übertragene Beacon-Nachricht nicht im Betrieb)</li> <li>5. Unknown (unbekannt)</li> </ol>

Tabelle 18. Token-Ring-Variablen in der Anzeige "Ring Status"

Variable	Definition
Ring Number	Die Ringnummer dieses Segments.
Ring Status	Der aktuelle Status des gesamten Rings.
Active Stations	Die Anzahl der aktiven Stationen auf dem Ring.
Active Monitor	Die aktuelle aktive Überwachung auf dem Ring.
Beacon Sender	Die letzte Station für den Rundsendebetrieb von Beacon-Rahmen auf den Ring.
Beacon NAUN	Der NAUN (Nearest Active Upstream Neighbor) der letzten Station im Beacon-Betrieb.

---

## Diagramme über Nways Manager Remote Monitor ausgeben

Über das Dialogfenster "Print" können Sie beliebige Diagramme aus Anzeigen, aus Anwendungen und aus dem Hauptfenster in eine Datei oder direkt an den Drucker ausgeben.

Führen Sie zum Öffnen des Dialogfensters "Print" (siehe Abb. 31) einen der folgenden Schritte aus:

- Wählen Sie im Hauptfenster von Nways Manager Remote Monitor im Menü "View" die Option **Print** aus, oder klicken Sie den Knopf **Print View** in der Knopfleiste an.
- Wählen Sie von der Anzeige eines Protokolldiagramms aus im Menü "File" die Option **Print** aus.

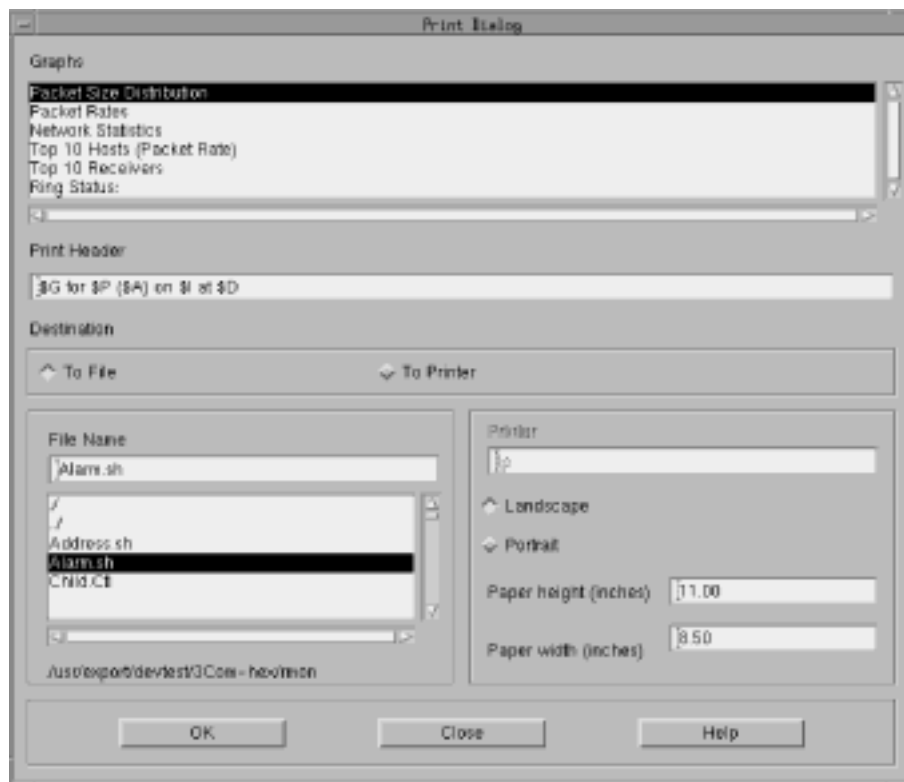


Abbildung 31. Dialogfenster "Print"

**Anmerkung:** Wenn Sie das Dialogfenster "Print" von einer Protokolldiagrammanzeige aus öffnen, wird die Liste "Graphs" nicht angezeigt.

Wenn Sie Diagramme über das Hauptfenster ausgeben, können Sie eine beliebige Kombination von Diagrammen aus dem Bereich "Graphs" auswählen und eine Kopfzeile für die Ausgabe angeben. Gehen Sie dazu wie folgt vor:

1. Wählen Sie im Bereich "Graphs" die Diagramme aus, die ausgegeben werden sollen. Jedes Diagramm wird auf einer eigenen Seite ausgegeben.
2. Im Bereich "Print Header" können Sie die Kopfzeile an Ihre Bedürfnisse anpassen. Geben Sie Ihre Textkombination und die in Tabelle 19 aufgeführten vordefinierten Variablen ein.

**Anmerkung:** Falls der Text der Kopfzeile die Breite des Seitenaufbaus überschreitet, wird er unvollständig ausgedruckt.

Tabelle 19. Variablen der Kopfzeile für die Ausgabe

Variable	Beschreibung
\$A	IP-Adresse der Einheit
\$D	Datum und Zeit
\$G	Datum und Zeit
\$I	Beschreibung der Schnittstelle der Einheit
\$P	Einheitenname

3. Aktivieren Sie zum Sichern der Diagramme in einer Datei das Feld **To File**, und vervollständigen Sie die Angaben im Bereich "File Name".
4. Aktivieren Sie zum Ausdrucken der Diagramme das Feld **To Printer**. Editieren Sie anschließend im Bereich "Printer" die Drucker-ID und den Seitenaufbau.
5. Klicken Sie das Feld **OK** an, um die Nachricht zur angegebenen Datei oder zum Drucker zu senden.

## Druckvorgaben einstellen

Wenn Sie nach einiger Zeit wissen, wofür Sie die Druckfunktion vorrangig einsetzen, ist es nützlich, die im Dialogfenster "Print" angezeigten Standardeinstellungen auf die von Ihnen am häufigsten verwendeten Einstellungen umzustellen. Beispielsweise möchten Sie vielleicht die Zeichenfolge für die Standardkopfzeile auf eine eigene Standardkopfzeile umstellen. Dadurch kann z. B. ein Firmenname oder eine Abteilungsbezeichnung in die Kopfzeile eingefügt werden. Diese Angaben können Sie einstellen, indem Sie die Ressourcendatei zu der betreffenden Anzeige oder Anwendung bearbeiten.

Die folgenden mit einem Stern versehenen Zeilen können in den X-Ressourcendateien "Ecam", "Rmon", "Viewport" und "Proto" bearbeitet werden, die im Verzeichnis /usr/LANReMon/rmon/locale/C/app-defaults enthalten sind.

```
!Default printer commands
*.printCommand: lpr -P
*.paperWidth: 8.5
*.paperHeight: 11.0
*.printerName: lp

! valid paper orientations are - portrait or landscape
*.paperOrientation: landscape

! header formatting
! $G - graph name, $P - device name, $A - probe ip address,
! $D - date and time stamp
*.headerFormat: $G for $P ($A) at $D
```



---

## Kapitel 5. RMON-Anzeigen verwenden

In diesem Kapitel wird erklärt, wie RMON-Anzeigen von Nways Manager Remote Monitor zum Sammeln von vordefinierten oder benutzerdefinierten Daten zum Netzwerk verwendet werden. Das Kapitel enthält die folgenden Abschnitte:

- Format von Dialogfenstern
- Angepaßte Anzeigen bearbeiten und erstellen
- Statistische Anzeigen
- Anzeige "Statistics" verwenden
- Anzeige "History" verwenden
- Anzeige "Host" verwenden
- Anzeige "Matrix" verwenden
- Anzeige "Ring Station" verwenden

---

### Format von Dialogfenstern

Für die meisten Dialogfenster von Anzeigen wird von Nways Manager Remote Monitor ein Standardlayout verwendet. Ein solches ist in Abb. 32 dargestellt.

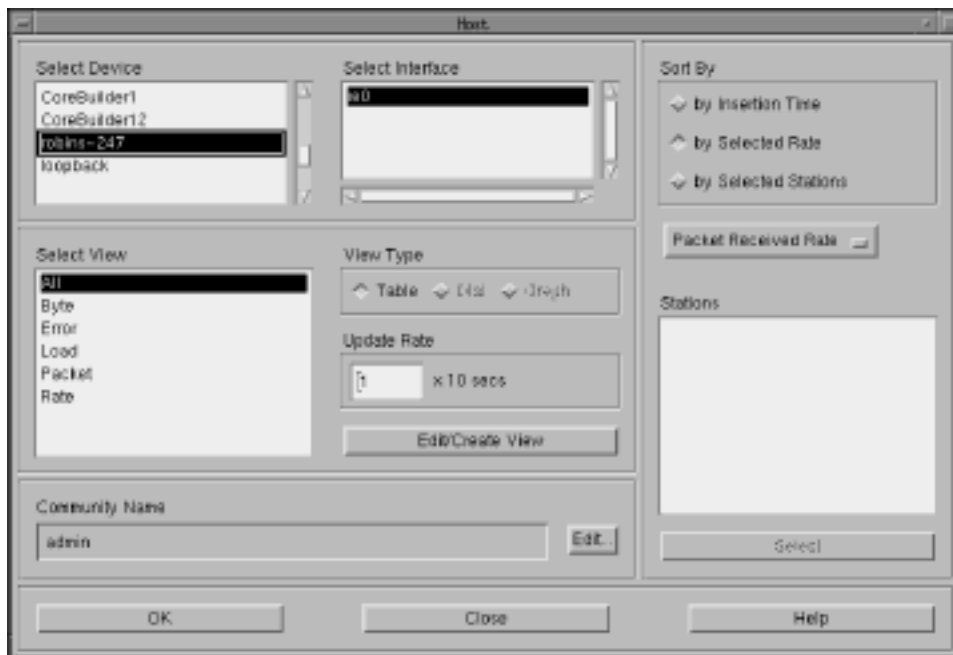


Abbildung 32. Beispiel für ein Dialogfenster einer Anzeige

Alle RMON-Anzeigen ermöglichen Ihnen, aus einer Anzahl von vordefinierten Anzeigen auszuwählen oder mit Hilfe einer Liste von Variablen eine eigene Anzeige zu erstellen. Einige Anzeigen verfügen über zusätzliche Konfigurationsoptionen, mit deren Hilfe zusätzliche Parameter festgelegt werden können. Diese werden jeweils in den entsprechenden Abschnitten beschrieben.

Gehen Sie zum Definieren einer RMON-Anzeige wie folgt vor:

1. Wählen Sie im Bereich "Select Device" eine Einheit aus. Dieser Bereich enthält eine Liste aller konfigurierten Einheiten. (Weitere Informationen hierzu sind im Abschnitt „Einheiten installieren und die Installation überprüfen“ auf Seite 10 enthalten). Bei der hervorgehobenen Einheit handelt es sich um die aktuelle Auswahl.
2. Wählen Sie im Bereich "Select Interface" eine Schnittstelle aus. Dieser Bereich enthält eine Liste mit verfügbaren Schnittstellen (falls auf die ausgewählte Einheit zugegriffen werden kann).
3. Wählen Sie im Bereich "Select View" eine vordefinierte Anzeige aus, oder erstellen Sie eine eigene Anzeige. (Informationen hierzu sind im Abschnitt „Angepaßte Anzeigen bearbeiten und erstellen“ auf Seite 78 enthalten). Durch diese Anzeige wird bestimmt, welche statistischen Elemente angezeigt werden.
4. Geben Sie im Bereich "View Type" eine der folgenden Darstellungsformen für die Anzeige an: "Table" (als Tabelle), "Scale" (als Skala) oder "Graph" (als Diagramm).
5. Geben Sie im Bereich "Update Rate" an, wie oft die Anzeige mit neuen Daten aktualisiert werden soll.
6. Von SNMP-Einheiten im Netzwerk werden Namen für Benutzergemeinschaften verwendet, damit der Zugriff auf Informationen auf der Einheit auf angegebene Gruppen von Workstations begrenzt bleibt. Im Bereich "Community Name" wird der Name für die Benutzergemeinschaft angezeigt, der gegenwärtig für die betreffende Einheit verwendet wird. Klicken Sie die Option **Edit...** an, um den Namen für die Benutzergemeinschaft zu ändern, und befolgen Sie die Anweisungen in Schritt 3 auf Seite 60.

---

## Angepaßte Anzeigen bearbeiten und erstellen

Mit Hilfe von Nways Manager Remote Monitor können Sie neue Datenanzeigen erstellen und bereits vorhandene bearbeiten.

Beispielsweise könnten Sie feststellen, daß von Datei-Servern in Ihrer Fertigungsabteilung häufig kurze Pakete in einem Ethernet-Segment generiert werden. Sie können zum Untersuchen dieser bestimmten Menge statistischer Daten eine angepaßte Anzeige erstellen. In diesem Abschnitt wird erklärt, wie eine "factory short stats" genannte Anzeige erstellt wird.

1. Wählen Sie im Dialogfenster "View" aus der Liste "Select View" eine Anzeige aus.
2. Klicken Sie die Option **Edit/Create View** an, um das in Abb. 33 auf Seite 79 gezeigte Dialogfenster "Edit User View" zu öffnen.





Abbildung 33. Dialogfenster "Edit User View"

3. Geben Sie im Feld "View Name" einen Namen ein. In diesem Fall würden Sie factory short stats eingeben.
4. Klicken Sie die Option **Clear** an, um die vorhandene Menge von statistischen Variablen aus der Liste "Selected Data" zu löschen.
5. Klicken Sie in der Liste "Available Data" die erforderlichen Variablen an, damit sie in die Anzeige aufgenommen werden. Nehmen Sie die Auswahl einer Variable zurück, indem Sie sie erneut anklicken.
6. Für das Beispiel "factory short stats" könnten Sie die folgenden Variablen verwenden:
  - Collisions
  - Too Long
  - Too Short
  - Short + CRC
  - Packets Sent (Utilization)
  - CRC
7. Tragen Sie erforderliche Notizen in das Feld "Comment" ein.
8. Klicken Sie eine der Optionen **Insert** oder **Append** an, um die ausgewählten Daten zur Liste "Selected Data" hinzuzufügen.

Durch die Reihenfolge in der Liste "Selected Data" wird definiert, in welcher Reihenfolge die Kategorien am Bildschirm angezeigt werden. Mit Hilfe der Option **Insert** können Sie einen neuen Eintrag am Anfang der Liste oder vor einem ausgewählten Eintrag in der Liste einfügen. Durch Auswahl der Option **Append** wird der Eintrag am Ende der Liste oder hinter einem ausgewählten Eintrag hinzugefügt.

9. Klicken Sie das Feld **OK** an, um eine angepaßte Datenanzeige zu erstellen und zum Dialogfenster "View" zurückzukehren.

## Dialogfenster Station Select verwenden

Das Dialogfenster "Station Select" wird von den folgenden RMON-Anzeigen verwendet:

- Host
- Matrix
- Ring Station

Mit Hilfe dieses Dialogfensters können Sie Stationen auswählen und vorhandene Stationseinträge ändern. Klicken Sie im Dialogfenster der entsprechenden Anzeige die Option **Select** an, um auf dieses Dialogfenster zuzugreifen.

**Anmerkung:** In den Anzeigen "Host" und "Ring Station" ist die Option **Select** nur dann verfügbar, wenn Sie ausgewählt haben, daß Einträge nach ausgewählten Stationen ("Selected Stations") sortiert werden sollen.

In Abb. 34 ist das Dialogfenster "Station Select" dargestellt.

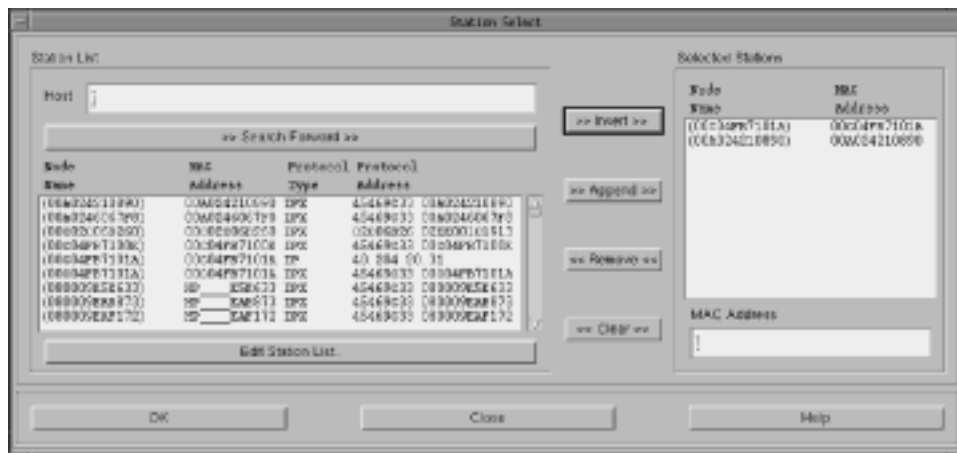


Abbildung 34. Dialogfenster "Station Select"

1. Wählen Sie im Bereich "Station" einen oder mehrere Stationseinträge aus. Klicken Sie anschließend eine der Optionen **Insert** oder **Append** an, um die Stationen zum Bereich "Selected Stations" hinzuzufügen.
  - Die Auswahl einer Station erfolgt durch Anklicken in der Liste. (Durch die rote Suchleiste werden Einträge hervorgehoben, aber nicht ausgewählt.)
  - Geben Sie im Feld "Host" Zeichen oder Ziffern (z. B. die ersten Buchstaben eines Host-Namens oder die ersten Stellen einer MAC-Adresse) ein, um in der Liste "Station" nach einer Station zu suchen. Das erste Vorkommen dieser Zeichenfolge an irgendeiner Position in der Station wird durch eine rote Leiste hervorgehoben. Sie können die Suche eingrenzen, indem Sie weitere Zeichen oder Ziffern hinzufügen.
  - Klicken Sie die Option **>>Search Forward>>** an, um das nächste Vorkommen einer Zeichenfolge zu suchen. Wenn die Zeichenfolge in der Liste nur einmal vorkommt, bleibt die rote Leiste auf dem aktuellen Eintrag. Mit Hilfe der Suchfunktion wird in jeder Spalte der Liste nach dem Inhalt des Feldes "Host" gesucht.
  - Wenn Sie beispielsweise bei der Suche nach einem "Birne" genannten Host im Feld "Host" die Zeichenfolge "Bi" eingegeben haben, wird von der Suchliste möglicherweise zuerst der Host "Biene" hervorgehoben. Klicken Sie die Option **Search Forward** an, um zum nächsten Vorkommen der Zeichenfolge "Bi" zu gelangen, oder grenzen Sie die Suche ein, indem Sie zu der Zeichenfolge im Feld "Host" weitere Zeichen oder Ziffern hinzufügen.
  - Wählen Sie zum Entfernen von Stationen aus der Liste "Selected Stations" die betreffenden Stationen aus, und klicken Sie die Option **Remove** an. Klicken Sie die Option **Clear** an, um den Inhalt der Liste "Selected Stations" zu löschen.
  - Informationen zum Ändern der Liste "Stations" sind im Abschnitt „Liste Station ändern“ auf Seite 81 enthalten.
2. Klicken Sie im Dialogfenster "Station Select" das Feld **OK** an, um die Liste der ausgewählten Stationen zu bestätigen.

### Liste Station ändern

Klicken Sie zum Ändern von Stationseinträgen in der Liste im Dialogfenster "Station Select" die Option **Edit Station List...** an. Dadurch wird das Dialogfenster "Station List Editor" (siehe Abb. 35 auf Seite 82) geöffnet.

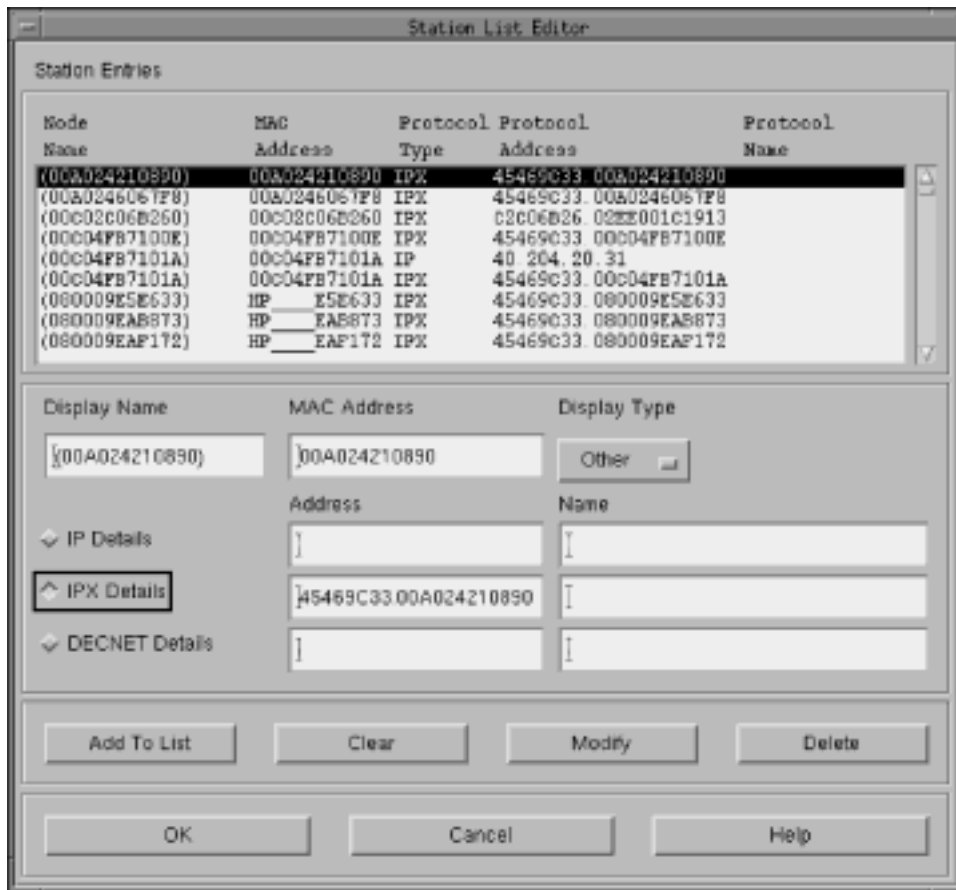


Abbildung 35. Dialogfenster "Station List Editor"

Bekannte Stationen werden im Bereich "Station Entries" alphabetisch nach ihren Anzeigennamen geordnet aufgeführt. Dabei erhalten alle Protokolltypen getrennte Einträge.

Bei der Auswahl eines Stationseintrags werden detaillierte Informationen zu allen Protokollen angezeigt.

Alle verfügbaren Stationen werden von Nways Manager Remote Monitor automatisch aufgeführt. Dennoch kann es erforderlich sein, zu der Liste eine Station hinzuzufügen. Dies kann beispielsweise der Fall sein, wenn Sie eine Einheit verwenden, auf die Sie die Software SmartAgent nicht laden können und die keine RMON2-Einheit ist, oder wenn Sie im Voraus einen Stationseintrag für eine Einheit erstellen möchten, die Sie noch nicht zum Netzwerk hinzugefügt haben.

### **Einen neuen Stationseintrag hinzufügen**

Gehen Sie zum Hinzufügen eines neuen Eintrags wie folgt vor:

1. Klicken Sie die Option **Clear** an, um eine leere Stationsschablone zu erhalten.
2. Geben Sie die MAC-Adresse der Station ein.
3. Aktivieren Sie den entsprechenden Protokollknopf, um die IP-, IPX- oder DEC-Informationen hinzuzufügen. Geben Sie anschließend die Protokolladresse und einen Namen ein.
4. Klicken Sie den Eintrag **Display Type** an, um den Anzeigennamen für die Station auszuwählen, und wählen Sie einen der Einträge "IP", "IPX", "DECnet" oder "Other" aus.
5. Klicken Sie zum Erstellen des neuen Eintrags die Option **Add To List** an.
6. Klicken Sie das Feld **OK** an, um zum Dialogfenster "Station Select" zurückzukehren.

### **Einen Stationseintrag ändern**

Gehen Sie zum Ändern eines Eintrags wie folgt vor:

1. Wählen Sie den Eintrag aus der Liste aus. Alle Protokolleinträge für die jeweilige Station werden in der Liste hervorgehoben.
2. Aktivieren Sie zum Hinzufügen oder Ändern von Protokolleinträgen den entsprechenden Protokollknopf, und ändern Sie die Werte in den Feldern "Address" und "Name".
3. Zum Entfernen eines protokollspezifischen Eintrags für die ausgewählte Station müssen Sie lediglich den Protokollknopf inaktivieren.
4. Klicken Sie die Option **Modify** an, um diese Änderungen zu bestätigen.
5. Klicken Sie das Feld **OK** an, um zum Dialogfenster "Station Select" zurückzukehren.

### **Einen Stationseintrag löschen**

Gehen Sie zum Löschen eines Eintrags wie folgt vor:

1. Wählen Sie den Eintrag aus der Liste aus. Alle Protokolleinträge für die jeweilige Station werden in der Liste hervorgehoben.
2. Klicken Sie die Option **Delete** an.  
**Anmerkung:** Alle Vorkommen von dieser Station für die verschiedenen Protokolltypen werden gelöscht.
3. Klicken Sie das Feld **OK** an, um zum Dialogfenster "Station Select" zurückzukehren.

## Statistische Anzeigen

Von Nways Manager Remote Monitor werden jederzeit mehrere Anzeigen gleichzeitig unterstützt. Bei den verfügbaren Formaten handelt es sich um Tabelle, Skala und Diagramm.

### Tabellarische Darstellung

Bei der tabellarischen Darstellung werden Statistiken in tabellarischer Form angezeigt. Dabei werden die Daten entsprechend den Angaben im Feld "Update Rate" in Echtzeit aktualisiert. (Informationen hierzu sind im Abschnitt „Format von Dialogfenstern“ auf Seite 77 enthalten.) Bei der tabellarischen Darstellung werden keine Deltawerte, sondern absolute Werte angezeigt. Verwenden Sie die Schiebeleisten, um sich durch die Anzeige zu bewegen. In Abb. 36 wird ein Beispiel für eine tabellarische Darstellung gezeigt.

**Anmerkung:** Einträge in der Tabelle "Matrix" werden nicht in Echtzeit aktualisiert. Mit Hilfe des Knopfes **Update** können sie aber manuell aktualisiert werden.

Address	Packets In	Packets Out	Bytes In	Bytes Out	Error Packets	Broadcasts	Multi
IP..._49500	857482	899227	335479770	49632574	1	40768	0
104624481770	25130447	25452763	360819857	2160032485	0	18663	0
3..._282850	985	989	542796	82028	0	1	0
Sun..._90522E	9079903	8443677	699786295	607499218	0	66	0
Sun..._713987	8943199	2679063	526546417	385300836	3	9825	0
3..._840840	3738534	3049033	436626883	1767315078	0	2632877	18656
1029648F232	1932776	1466227	436231374	365762286	0	2997	0
104624728E10	11223803	10364643	987841470	737604824	1	3719	987
Sun..._75133F	146076	3488238	2339392	266755866	0	784	0
10C64F08F7E	1400294	1248713	307891811	86048648	0	3800	300
10E1804359D	98237	332225	4397166	24742945	0	8896	25982
11D82900000	240481	8	19366784	0	0	0	0
3..._1148C4	12889	104336	3397152	25538486	0	96782	0
broadcast	3886133	8	1414482918	0	0	0	0
Sun..._31138E	254003	346298	30371971	75166230	0	32682	0
10C64F08F7E	2506006	2506958	318867875	288854775	0	3941	0

Abbildung 36. Tabellarische Darstellung

Die Tabellen "Host" und "Matrix" enthalten in der oberen linken Ecke außerdem einen Zähler für die Anzahl der Einträge. Die Tabelle "Host" wird genauso oft aktualisiert wie die Daten in der Tabelle. Weitere Informationen hierzu sind in den Abschnitten „Anzeige Host konfigurieren“ auf Seite 96 und „Anzeige Matrix konfigurieren“ auf Seite 99 enthalten.

## Skalendarstellung

In der Skalendarstellung werden Statistiken in Echtzeit angezeigt. Ein gelber Zeiger gibt den aktuellen Wert pro Sekunde an, während ein roter Zeiger den höchsten Wert anzeigt, der seit der Öffnung der Anzeige erreicht wurde. Der rote Bereich, der ungewöhnliche Auslastungsgrade anzeigt, kann vom Benutzer eingestellt werden. Die Zahl unterhalb der Skalen gibt den kumulierten Wert während des überwachten Zeitraums an. In Tabelle 20 wird ein Beispiel für eine Skalendarstellung gezeigt.

Weil sich die Norm von LAN zu LAN unterscheidet, können Sie den Wert des roten Bereichs so anpassen, daß er den Bedürfnissen Ihrer Umgebung entspricht. Möglicherweise möchten Sie die Werte im roten Bereich sogar an die eigenen Schwellenwerte anpassen, die Sie im Feld "Alarms" (siehe Kapitel 6) festgelegt haben. Die Einstellungen für die Skalenschwellenwerte sind für RMON-Anzeigen in der Datei "Rmon" und für ECAM-Anwendungen in der Datei "ECAM" enthalten. (Siehe Anhang F). Beide Dateien sind im Verzeichnis "/usr/LANReMon/rmon/locale/C/app-defaults" enthalten und können mit Hilfe eines beliebigen Texteditors bearbeitet werden.

Tabelle 20. Skalendarstellung



Klicken Sie einen beliebigen Skalanamen an, um das in Abb. 37 auf Seite 86 gezeigte Dialogfenster "Dial Reset" anzuzeigen. In diesem Dialogfenster werden der niedrigste, der höchste und der durchschnittliche Wert in der Skala sowie Werte im roten Bereich angezeigt. Klicken Sie die Option **Reset** an, um die Werte für diese Skala auf 0 zurückzusetzen.

Nach Ablauf des eingestellten Aktualisierungszeitraums werden in der Skala aktualisierte Daten angezeigt.



Abbildung 37. Dialogfenster "Dial Reset"



## Diagrammdarstellung

In der Diagrammdarstellung haben Sie die Auswahl zwischen den folgenden Diagrammtypen: "Bar", "Pie", "Bar 3D", "Line", "Area" und "Scatter". In den ersten drei werden die neuesten statistischen Daten dargestellt. In den anderen werden Statistiken über Trends im Laufe der Zeit dargestellt. Alle Diagramme werden so oft aktualisiert, wie im Feld "Update Rate" angegeben. (Informationen hierzu sind im Abschnitt „Format von Dialogfenstern“ auf Seite 77 enthalten). Die Anzeige "Statistics" ermöglicht Ihnen, vergleichende Statistikdiagramme von verschiedenen Schnittstellen aus zu generieren. In Abb. 38 wird ein Beispiel für eine Diagrammdarstellung gezeigt.

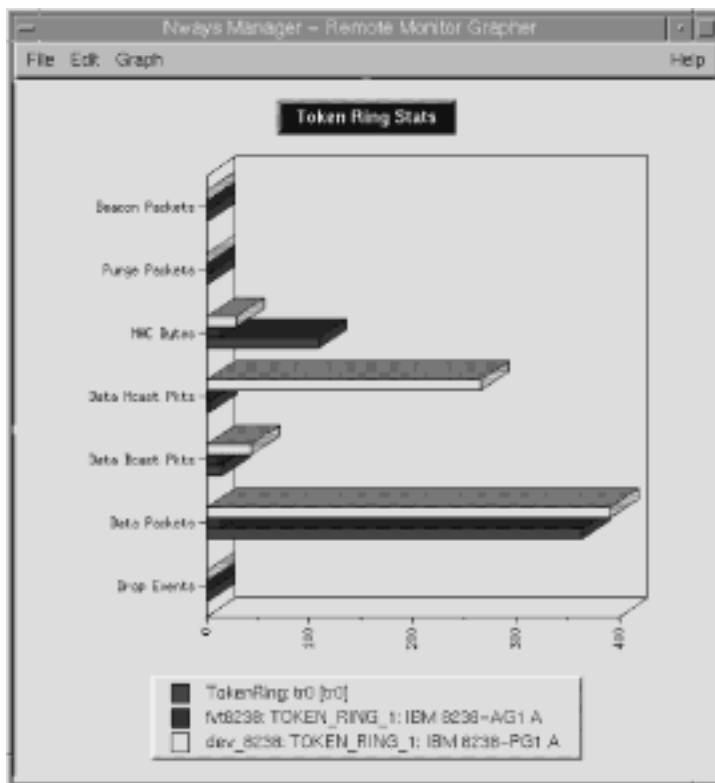


Abbildung 38. Diagrammdarstellung

In Tabelle 21 werden die Menüs aufgeführt, auf die innerhalb der Diagrammdarstellung zugegriffen werden kann.

*Tabelle 21. Menüs der Diagrammdarstellung*

<b>Menü</b>	<b>Option</b>	<b>Beschreibung</b>
File	Print	Gibt den statistischen Inhalt der Anzeige in eine Datei oder an einen Drucker aus.
	Exit	Schließt die Anzeige.
Edit	Transpose*	Schaltet zwischen der Gruppierung von Statistiken nach einem Ausgangspunkt für Stichproben und der Gruppierung nach einer RMON-Variable hin und her.
	Delta Values*	Verwendung absoluter Werte oder veränderlicher Deltawerte.
Graph	Select Columns...	Auswahl, welche Variablen Sie anzeigen möchten.
	Bar*	Zeigt statistische Werte in Echtzeit an. Diese Option ist nützlich beim Vergleich von Statistiken.
	PieA	Zeigt das Verhältnis jeder einzelnen Statistik zum Gesamten an.
	Bar 3DA	Zeigt statistische Werte in Echtzeit an. Diese Option ist nützlich beim Vergleich von Statistiken.
	LineB	Gibt Trends im Laufe der Zeit an. Hebt die Rate an Änderungen im Laufe der Zeit stärker hervor als den Umfang der Änderungen.
	AreaB	Gibt Trends im Laufe der Zeit an. Hebt die Rate an Änderungen im Laufe der Zeit stärker hervor als den Umfang der Änderungen.
	ScatterB	Gibt Trends im Laufe der Zeit an. Hebt die Rate der Änderungen im Laufe der Zeit stärker hervor als den Umfang der Änderungen.

\* Zeigt Protokollstatistiken an.

A Zeigt die neueste Menge von Statistiken an.

B Zeigt Protokollstatistiken an.

---

## Anzeige Statistics verwenden

Die Anzeige "Statistics" zeigt einen Echtzeitbericht über die Aktivitäten des von Ihnen ausgewählten Netzwerksegments an. Diese Anzeige sollten Sie zuerst aufrufen, wenn Sie vermuten, daß in einem bestimmten Segment Probleme auftreten. Mit Hilfe dieser Anzeige können Sie Statistiken zu beliebigen Kombinationen aus Paketen, Byte, Fehlern, Größenverteilungen und Multicasts anzeigen.

## Anzeige Statistics konfigurieren

Verwenden Sie zum Erstellen der Anzeige "Statistics" das Dialogfenster "Statistics". Wählen Sie im Menü "Analysis" erst den Eintrag **RMON Views** und dann den Eintrag **Statistics** aus, um auf das Dialogfenster "Statistics" zuzugreifen, oder klicken Sie in der Knopfleiste den Knopf **RMON Statistics** an.

Diese Anzeige ermöglicht folgendes:

- Statistiken zu einem einzelnen LAN-Segment anzeigen.
- Von mehreren Schnittstellen in verschiedenen LAN-Segmenten gesammelte Statistiken anzeigen und vergleichen.

### Statistiken zu einem einzelnen Segment anzeigen

Gehen Sie zum Anzeigen von Statistiken zu einem einzelnen Segment wie folgt vor:

1. Stellen Sie die grundlegenden Parameter der Anzeige wie im Abschnitt „Format von Dialogfenstern“ auf Seite 77 beschrieben ein.

**Anmerkung:** Statistiken zu einem einzelnen LAN-Segment können als Tabelle, als Skala oder als Diagramm angezeigt werden. (Eine Erklärung der verschiedenen Anzeigearten ist im Abschnitt „Statistische Anzeigen“ auf Seite 84 enthalten.)

2. Klicken Sie zum Aufrufen der Anzeige "Statistics" das Feld **OK** an.

### Zu Vergleichszwecken mehrere Segmentstatistiken anzeigen

Sie können mehrere Kombinationen aus Einheit und Schnittstelle gleichzeitig anzeigen. Die betreffenden Informationen können in einem einzelnen Diagramm angezeigt werden. Dies ist in den folgenden Fällen nützlich:

- Sie möchten Statistiken einsehen, die von verschiedenen Schnittstellen des gleichen Typs auf verschiedenen Einheiten erstellt wurden.
- Sie möchten Statistiken vergleichen, die von mehreren Schnittstellen des gleichen Typs auf einer einzelnen Einheit erstellt wurden.

Gehen Sie zum Anzeigen von Statistiken aus mehreren Segmenten wie folgt vor:

1. Klicken Sie im Bereich "View Type" den Eintrag **Graph** an. (Eine Beschreibung von grafischen Anzeigen ist im Abschnitt „Statistische Anzeigen“ auf Seite 84 enthalten.)
2. Wählen Sie die erforderliche Einheit und die erforderliche Schnittstelle aus, und klicken Sie die Option **Add** an. Die ausgewählten Komponenten werden im Feld "Graph Sample Points" angezeigt. Wiederholen Sie diese Prozedur so oft, bis Sie die benötigte Anzahl an Kombinationen aus Einheit und Schnittstelle hinzugefügt haben.  
**Anmerkung:** Der Verkabelungstyp der ausgewählten Schnittstellen muß identisch sein, z. B. nur Ethernet oder nur FDDI. Außerdem sollten alle Schnittstellen über dieselbe Geschwindigkeit verfügen.
3. Wählen Sie zum Löschen einer einzelnen Kombination aus dem Feld "Graph Sample Points" die betreffende Komponente aus, und klicken Sie die Option **Delete** an. Klicken Sie zum Entfernen aller Komponenten die Option **Clear** an.
4. Konfigurieren Sie die anderen Bereiche wie im Abschnitt „Format von Dialogfenstern“ auf Seite 77 beschrieben.
5. Klicken Sie das Feld **OK** an, um die Anzeige "Statistics" (siehe Abb. 39) aufzurufen.

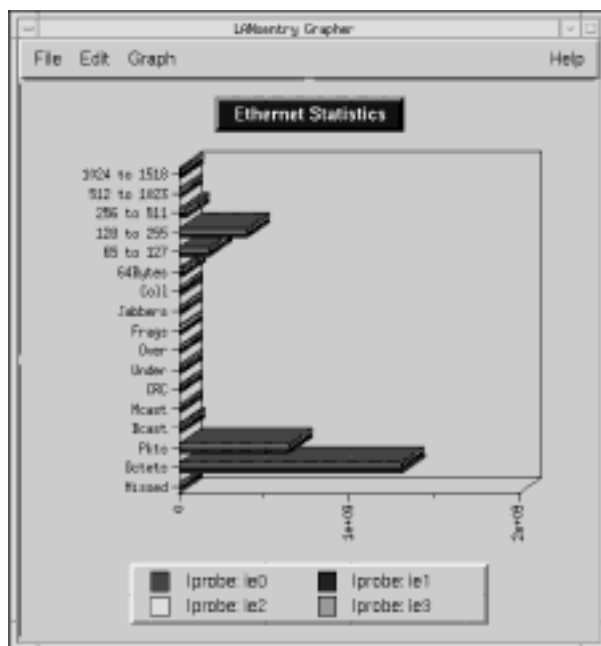


Abbildung 39. Beispiel für ein vergleichendes Statistikdiagramm

## Vordefinierte Statistikanzeigen

In Tabelle 22 werden die für Ethernet, Token-Ring und FDDI verfügbaren Statistikanzeigen beschrieben. Im Anhang E ist eine Liste der in der Anzeige "Statistics" verfügbaren Variablen enthalten.

Tabelle 22. Vordefinierte Statistikanzeigen

Anzeige	Verkabelungstyp			Beschreibung
	Ethernet	Token-Ring	FDDI	
All	■		■	Enthält alle Variablen.
Bytes	■		■	Die Anzahl der Byte, aus denen diese Pakete bestehen (anders ausgedrückt: die Gesamtzahl der Byte des Datenverkehrs in diesem Segment).
Distribution	■	■		Pakete, die für den jeweiligen Verkabelungstyp in spezifische Größenkategorien eingeteilt werden.
Errors	■	■	■	Die Anzahl der im Segment festgestellten Fehler.
Events			■	Ringaufrufe (Ring Polls), Ausgabe von Beacon-Nachrichten (Beacon Events) und Freigabeereignisse (Purge Events) auf dem Ring.
MAC			■	Der gesamte Datenverkehr der MAC-Schicht in einem Segment - Pakete, die Byte dieser Pakete, Beacon-Informationen der MAC-Schicht, verschiedene normale Fehler, die Anzahl der Ringaufrufe usw.
Multicast	■	■		Die Gesamtzahl der fehlerfreien Pakete, die an die Multicast-Adresse übertragen werden. Broadcast-Pakete sind eingeschlossen.
Packets	■	■	■	Die Gesamtzahl der entdeckten Pakete im Netzwerksegment. Fehlerpakete sind eingeschlossen.
Promiscuous			■	Datenverkehr der Datenschicht in einem Segment.
Source Routing			■	Ringnummer, empfangene und gesendete Rahmen, weitergeleitete Rahmen, empfangene und gesendete Oktette, weitergeleitete Oktette, All-Route-Broadcasts und Single-Route-Broadcasts, All-Route-Octets und Single-Route-Octets, lokale LLC-Rahmen und Hop-Zähler.

\*Enthält einige Variablen, die sich nur für eine tabellarische Darstellung eignen. Eine Liste der für FDDI verfügbaren Variablen ist im Anhang E, „Variablen in Anzeigen und Anwendungen“ auf Seite 179 enthalten.

---

## Anzeige History verwenden

Die Anzeige "History" ergänzt die Anzeige "Statistics". Mit Hilfe der Anzeige "History" können Sie Daten zu den normalen Trends in Ihrem Netzwerk sammeln. Nachdem Sie die normalen Aktivitäten Ihres Netzwerks bestimmt haben, können Sie in der Anzeige "Alarms" Alarmsignale einstellen, die ausgelöst werden, wenn die Aktivitäten im Netzwerk von der Norm abweichen. Geben Sie mit Hilfe der Anzeige "History" einen Erfassungszeitraum an und entdecken Sie Trends, die sich über Stunden, Tage, Wochen oder sogar Monate erstrecken.

Protokollinformationen werden in einer Tabelle oder in einem Diagramm angezeigt, die bzw. das Entwicklungen im Laufe der Zeit darstellt. Wenn Sie ein ungewöhnliches Ereignis in der Aktivität des Netzwerks entdecken, klicken Sie einfach den betreffenden Teil des Liniendiagramms an, um herauszufinden, wann das Ereignis stattgefunden hat.

## Anzeige History konfigurieren

Verwenden Sie zum Konfigurieren der Anzeige "History" das Dialogfenster "History". Wählen Sie im Menü "Analysis" erst den Eintrag **RMON Views** und dann den Eintrag **History** aus, um auf das Dialogfenster "History" zuzugreifen, oder klicken Sie in der Knopfleiste den Knopf **RMON History** an.

1. Stellen Sie die grundlegenden Parameter der Anzeige wie im Abschnitt „Format von Dialogfenstern“ auf Seite 77 beschrieben ein.
2. Wählen Sie aus der Liste "History Entries" einen Erfassungszeitraum aus. Führen Sie die folgenden Schritte durch, falls der gewünschte Erfassungszeitraum noch nicht in der Liste "History Entries" angezeigt wird:
  - a. Klicken Sie zum Erstellen eines neuen Erfassungszeitraums die Option **Add** an. Daraufhin wird das in Abb. 40 auf Seite 93 gezeigte Dialogfenster "History Entry Creation" angezeigt.



Abbildung 40. Dialogfenster "History Entry Creation"

- b. Geben Sie an, wie oft und für wie lange (bis zu 1 Stunde) Statistiken im Segment erstellt werden sollen.

Wenn dies einmal pro Stunde erfolgen soll, werden Ereignisse von jedem Punkt des Diagramms in einem stündlichen Intervall wiedergegeben.

- c. Klicken Sie zum Hinzufügen dieses Eintrags das Feld **OK** an.

Jeder Protokolleintrag wird von der Einheit in einer spezifischen Speicherposition, einem Protokollbereich, gespeichert. Die Einheit verfügt nur über eine begrenzte Zahl an Protokollbereichen. Wenn Sie beispielsweise auswählen, daß 8 Stunden lang alle 30 Minuten eine Statistik erstellt werden soll, werden 16 Protokollbereiche gebraucht (pro Stunde 2 Protokollbereiche für jeden Erfassungstyp).

**Anmerkung:** Wenn Sie eine sehr hohe Anzahl von Statistiken angegeben haben, werden Sie möglicherweise von Nways Manager Remote Monitor gewarnt, daß die Einheit nicht über genügend Ressourcen für die Bearbeitung des neuen Eintrags verfügt. Löschen Sie in diesem Fall eine alte Statistik, die Sie nicht mehr benötigen, aus der Liste "History Entries". Erstellen Sie anschließend den Protokolleintrag erneut.

3. Klicken Sie zum Aufrufen der Anzeige "History" das Feld **OK** an.

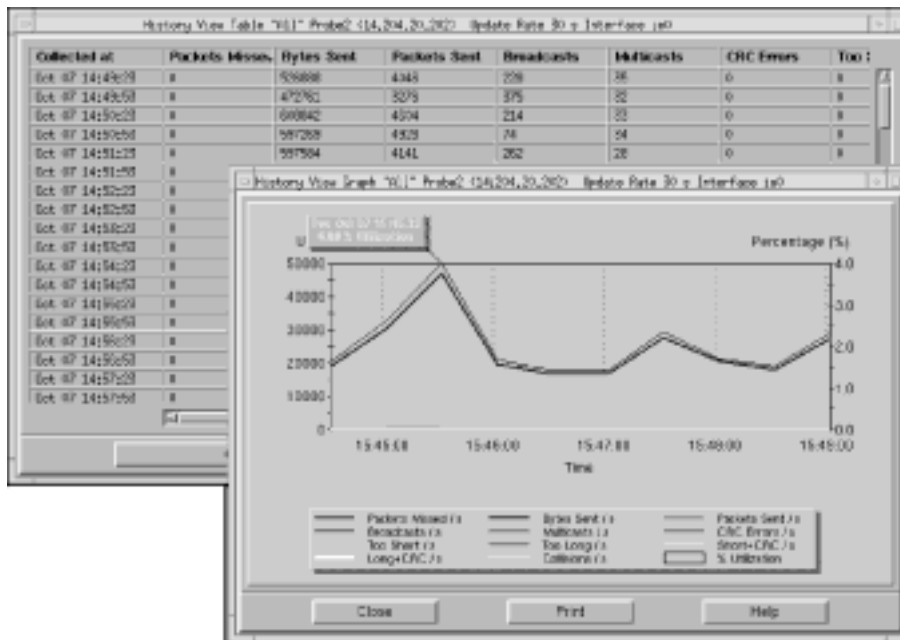


Abbildung 41. Beispiel für die Anzeige "History" in Tabellendarstellung und in Diagrammdarstellung

Eine Beschreibung von tabellarischen Darstellungen ist im Abschnitt „Statistische Anzeigen“ auf Seite 84 enthalten.

Das Fenster "Graph" bietet eine bildliche Darstellung von Protokollereignissen im Laufe der Zeit. Am unteren Ende des Diagramms wird eine Zeitachse angezeigt. Diese verschiebt sich gemeinsam mit dem Diagramm, wenn neue Daten angezeigt werden. Vertikale Rasterlinien markieren die Zeiten, die auf dieser Achse angegeben werden.

Jede Protokollvariable ist farblich kodiert. Ereignisse werden Paketraten und Angaben zur Auslastung im Segment gegenübergestellt. Die Raten der Token-Ring-Auslastung werden mit Hilfe der Schnittstellenübertragungsrate aus der Schnittstellentabelle berechnet. Wenn der Wert nicht verfügbar ist, wird für die Berechnung eine Ringgeschwindigkeit von 16 MB vorausgesetzt.

Wenn Sie herausfinden möchten, wann ein bestimmtes Ereignis im Netzwerk stattgefunden hat, müssen Sie den betreffenden Punkt im Diagramm anklicken. Eine Datenbeschreibungsmarke wird angezeigt. Klicken Sie den Punkt im Diagramm erneut an, um die Datenbeschreibungsmarke zu entfernen.



## Vordefinierte Protokollanzeigen

In Tabelle 23 werden die für Ethernet, Token-Ring und FDDI verfügbaren Protokollanzeigen beschrieben. Im Anhang F, Anwendung ECAM (Enterprise Communications Analysis Module) ist eine Liste der in der Anzeige "History" (Protokollanzeige) verfügbaren Variablen enthalten.

Tabelle 23. Vordefinierte Protokollanzeigen

Anzeige	Verkabelungstyp			Beschreibung
	Ethernet	Token-Ring	FDDI	
All	■		■	Enthält alle Variablen.
Byte	■		■	Die Anzahl der Byte, aus denen die im Segment gesehenen Pakete bestehen (anders ausgedrückt: die Gesamtzahl der Byte des Datenverkehr in diesem Segment).
Error	■	■	■	Die Anzahl der im Segment entdeckten Fehlerpakete.
Events		■		Freigabeereignisse, Ausgaben von Beacon-Nachrichten, Token-Anforderungs-Ereignisse und Ringaufrufe.
Load	■		■	Die Auslastung des Netzwerks in Prozent während dieses Erfassungszeitraums.
Multicast	■		■	Die Gesamtzahl der fehlerfreien Pakete, die an die Multicast-Adresse übertragen werden. Broadcast-Pakete sind eingeschlossen.
Packet	■	■	■	Die Gesamtzahl der entdeckten Pakete im Netzwerksegment. Fehlerpakete sind eingeschlossen.
Size Distribution		■	■	Pakete, die in spezifische Größenkategorien eingeteilt werden.

## Anzeige Host verwenden

Mit Hilfe der Anzeige "Host" können Sie erkennen, welche Knoten sich auf Ihrem Netzwerk befinden, in welchem Zustand sie sind und welche Knoten möglicherweise Probleme verursachen. Beispielsweise kann es sein, daß Sie sich ziemlich sicher sind, daß bei zunehmendem Rundsendebetrieb in einem Segment auch die Anzahl der Fehler auf dem Router zunimmt, Sie aber über keine konkreten Fakten verfügen, die diese Theorie unterstützen.

Die Anzeige "Host" wurde entwickelt, damit Sie bei solchen Problemen Zugriff auf die wesentlichen Informationen erhalten können. Diese Informationen werden von den Host- und von den Host-TopN-RMON-Gruppen zur Verfügung gestellt.

Je nachdem, wie Sie bei Ihren Ermittlungen vorgehen wollen, können die Ergebnisse auf verschiedene Weise geordnet werden. Sie können die folgenden Ordnungsprinzipien heranziehen, um die wesentlichen Informationen hervorzuheben:

- By Insertion Time
- By Selected Rate
- By Selected Station

## Anzeige Host konfigurieren

Verwenden Sie zum Konfigurieren der Anzeige "Host" das Dialogfenster "Host". Wählen Sie im Menü "Analysis" erst den Eintrag **RMON Views** und dann den Eintrag **Host** aus, um auf das Dialogfenster "Host" zuzugreifen, oder klicken Sie in der Knopfleiste den Knopf **RMON Host** an.

- Stellen Sie die grundlegenden Parameter der Anzeige wie im Abschnitt „Format von Dialogfenstern“ auf Seite 77 beschrieben ein.
- Der Bereich **Sort By** ermöglicht Ihnen, die Hosteinträge nach den folgenden drei Kriterien zu ordnen:

**By Insertion Time** Dadurch werden die Hosts in der Reihenfolge aufgeführt, in der sie in der Tabelle "RMON Host" enthalten sind.

**By Selected Rate** Bei Auswahl dieser Option wird die Einstellung "Packet Received Rate" aktiviert. Dabei handelt es sich lediglich um eine Standardeinstellung.

Sie können aus den folgenden Einstellungen auswählen:

- Packet Received Rate (Rate der empfangenen Pakete)
- Packet Sent Rate (Rate der gesendeten Pakete)
- Bytes Received Rate (Rate der empfangenen Byte)
- Bytes Sent Rate (Rate der gesendeten Byte)
- Error Packet Rate (Fehlerpaketrate)
- Broadcast Packet Rate (Rate der Broadcast-Pakete)
- Multicast Packet Rate (Rate der Multicast-Pakete)

**By Selected Station** Bei Auswahl dieser Option wird der Knopf "Select" aktiviert und alle gegenwärtig ausgewählten Stationen werden in der Liste "Stations" angezeigt.

Sie können die Stationen in der Liste ändern, indem Sie die Option "Select" anklicken. Dadurch wird das Dialogfenster "Station Select" geöffnet. Anweisungen zum Hinzufügen, Ändern und Löschen von Stationseinträgen sind in den Erläuterungen zu Abb. 34 auf Seite 80 enthalten.

- Klicken Sie zum Aufrufen der Anzeige "Host" das Feld **OK** an.

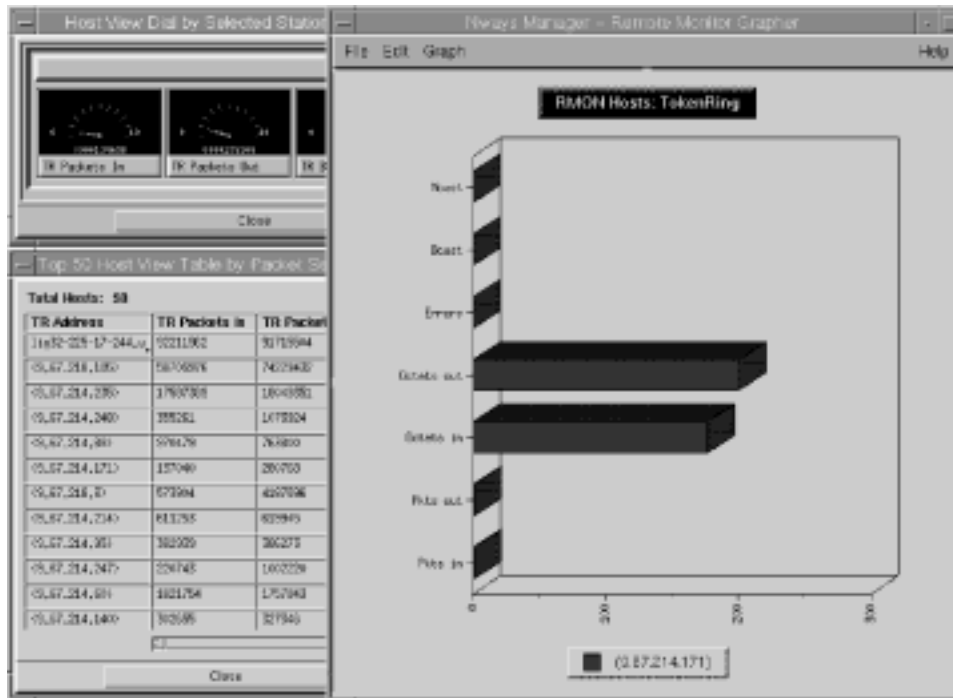


Abbildung 42. Beispiel für die Anzeige "Host" in Skalen- sowie in tabellarischer und in Diagramm-darstellung

Eine Beschreibung von Skalendarstellungen sowie von tabellarischen und von Diagrammdarstellungen ist im Abschnitt „Statistische Anzeigen“ auf Seite 84 enthalten.

Die Gesamtzahl der in der Tabelle aufgeführten Hosts wird unterhalb der Titelleiste angezeigt. Diese Zahl wird zur gleichen Zeit wie die übrige Tabelle aktualisiert. Je nach der ausgewählten Ebene der Adreßumsetzung (Address Translation Level) wird der Host von Nways Manager Remote Monitor in der Spalte "Address" entweder mit seinem Namen, mit seiner Protokolladresse oder mit seiner Mac-Adresse angezeigt. Weitere Informationen hierzu sind im Abschnitt „Stufe der Adreßumsetzung einstellen“ auf Seite 49 enthalten.

## Vordefinierte Host-Anzeigen

In Tabelle 24 werden die für Ethernet, Token-Ring und FDDI verfügbaren Host-Anzeigen beschrieben. Im Anhang G "Anwendung ECAM (Enterprise Communications Analysis Module)" ist eine Liste der in der Anzeige "Host" verfügbaren Variablen enthalten.

Tabelle 24. Vordefinierte Host-Anzeigen

Anzeige	Verkabelungstyp			Beschreibung
	Ethernet	Token-Ring	FDDI	
All	■	■	■	Enthält alle Variablen.
Broadcast		■		Die Anzahl der gesehenen Rundsendungen.
Byte	■	■	■	Die Anzahl der Byte, aus denen die im Segment gesehenen Pakete bestehen (anders ausgedrückt: die Gesamtzahl der Byte des Datenverkehrs in diesem Segment).
Error	■		■	Die Anzahl der im Segment entdeckten Fehlerpakete.
Load	■		■	Die Anzahl der gesehenen Multicasts.
Packet	■	■	■	Die Gesamtzahl der entdeckten Pakete im Netzwerksegment. Fehlerpakete sind eingeschlossen.
Rate	■		■	Die Anzahl der gesehenen Rundsendungen und Multicasts.

## Anzeige Matrix verwenden

Die Anzeige "Matrix" gibt die Menge an Datenverkehr und die Anzahl der Fehler zwischen zwei Stationen im Netzwerk an. Dadurch können Sie die einzelnen Stationen erkennen, die möglicherweise das Auftreten von Problemen verursachen.

Mit Hilfe der Anzeige "Matrix" können Sie folgendes ermitteln:

- Wer mit wem im Netzwerk kommuniziert.
- Wieviel Datenverkehr zwischen zwei Stationen stattfindet.

## Anzeige Matrix konfigurieren

Verwenden Sie zum Konfigurieren der Anzeige "Matrix" das Dialogfenster "Matrix". Wählen Sie im Menü "Analysis" erst den Eintrag **RMON Views** und dann den Eintrag **Matrix** aus, um auf das Dialogfenster "Matrix" zuzugreifen, oder klicken Sie in der Knopfleiste den Knopf **RMON Matrix** an.

1. Stellen Sie die grundlegenden Parameter der Anzeige wie im Abschnitt „Format von Dialogfenstern“ auf Seite 77 beschrieben ein.

**Anmerkung:** In der Liste "Stations" muß mindestens eine Station aufgeführt sein.

2. Klicken Sie im Dialogfenster "Matrix" das Feld **OK** an, um die Anzeige "Matrix" aufzurufen.

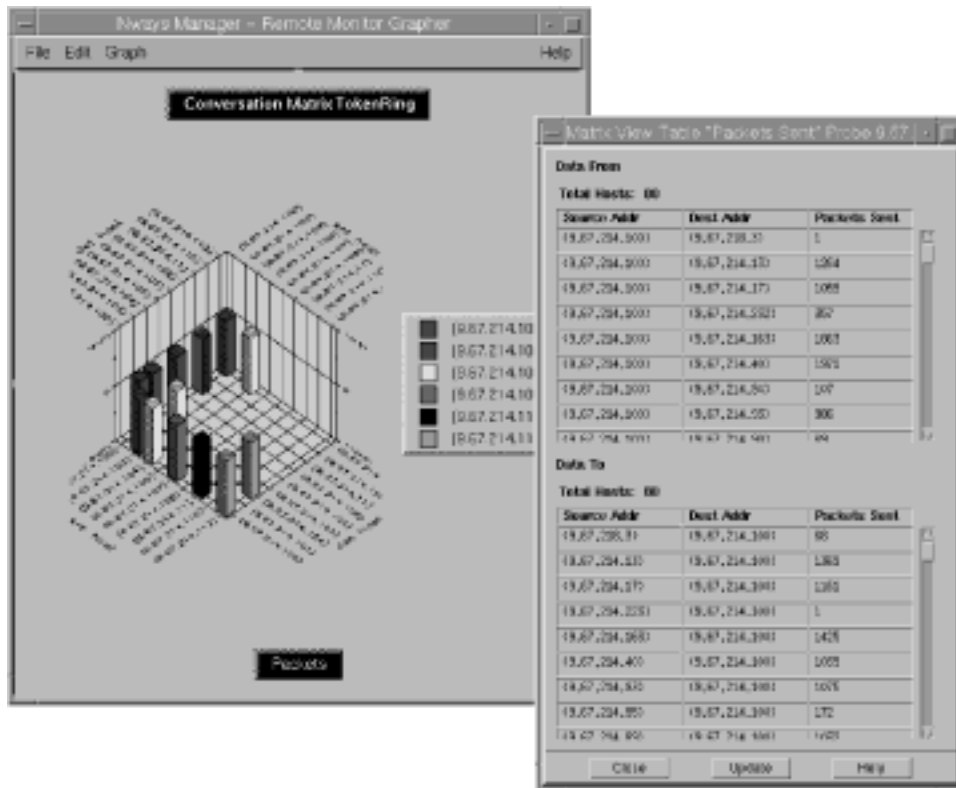


Abbildung 43. Beispiel für die Anzeige "Matrix" in tabellarischer und in Diagrammdarstellung

## Anzeige Matrix lesen

Von Nways Manager Remote Monitor werden alle Hosts angezeigt, die entweder von einer der ausgewählten Stationen Daten empfangen oder an eine der ausgewählten Stationen Daten senden. Die Gesamtzahl der in der Tabelle aufgeführten Hosts wird sowohl für die Tabelle "Data From" als auch für die Tabelle "Data To" angezeigt. Diese Zahl wird zur gleichen Zeit wie die übrige Tabelle aktualisiert. Die Tabelle wird wie in Abb. 43 auf Seite 99 gezeigt im Matrixformat angezeigt. In Tabelle 25 werden die Spalten der Matrix beschrieben.

Tabelle 25. Spalten der Matrix

Spalte	Beschreibung
Source Address	Die Station, die die Daten sendet.
Destination Address	Die Station, an die Daten gesendet werden.
Packets Sent	Die Anzahl der vom Quellsystem gesendeten Datenpakete.
Bytes Sent	Die Anzahl an Byte, aus denen dieses Pakete bestehen.
Error Packets	Die Anzahl der vom Quellsystem generierten Fehlerpakete.

**Anmerkung:** Da die Tabelle "Matrix" nicht automatisch aktualisiert wird, müssen Sie zum Hochladen von Daten von der Einheit die Option **Update** anklicken.

## Vordefinierte Matrixanzeigen

In Tabelle 26 werden die für Ethernet, Token-Ring und FDDI verfügbaren Matrixanzeigen beschrieben. Im Anhang F ist eine Liste der in der Anzeige "Matrix" verfügbaren Variablen enthalten.

Tabelle 26. Vordefinierte Matrixanzeigen

Anzeige	Verkabelungstyp			Beschreibung
	Ethernet	Token-Ring	FDDI	
All	■	■	■	Enthält alle Variablen.
Bytes	■	■	■	Die Gesamtzahl der Byte des Datenverkehrs in diesem Segment.
Errors	■	■	■	Die Anzahl der im Segment entdeckten Fehlerpakete.
Packets	■	■	■	Die Gesamtzahl der entdeckten Pakete im Netzwerksegment. Fehlerpakete sind eingeschlossen.

---

## Anzeige Ring Station verwenden

In der Anzeige "Ring Station" wird eine Tabelle mit Statistiken und Statusinformationen zu jeder Station auf dem Ring generiert. Darin enthalten sind der Status der Station sowie die Zeitpunkte des letzten Einstiegs und des letzten Exits.

Beispielsweise wird jedesmal eine Störung hervorgerufen, wenn eine neue Station in den Ring eingefügt wird. Dies führt zu einem Ringfreigabeereignis, und von der aktiven Überwachung wird ein neues Token ausgegeben. Mit Hilfe der Anzeige "Ring Station" können Sie feststellen, welche Station dies verursacht, und Sie können die aktive Überwachung entdecken, die das neue Token ausgibt.

Die Anzeige "Ring Station" bietet Ihnen die folgenden Möglichkeiten:

- Sie können die Muster des eigenen Token-Rings kennenlernen.
- Sie können erkennen, ob es sich um eingrenzbare oder um nicht eingrenzbare Fehler handelt
- Sie können erkennen, welche Einheiten sich gegenwärtig auf dem Ring befinden.

## Anzeige Ring Station konfigurieren

Verwenden Sie zum Konfigurieren der Anzeige "Ring Station" das Dialogfenster "Ring Station". Wählen Sie im Menü "Analysis" erst den Eintrag **RMON Views** und dann den Eintrag **Ring Station** aus, um auf das Dialogfenster "Ring Station" zuzugreifen, oder klicken Sie in der Knopfleiste den Knopf **RMON Ring Station** an.

1. Stellen Sie die grundlegenden Parameter der Anzeige wie im Abschnitt „Format von Dialogfenstern“ auf Seite 77 beschrieben ein.

**Anmerkung:** Stellen Sie sicher, daß Sie eine Token-Ring-Einheit oder, falls Sie Einheiten mit mehreren Schnittstellen verwenden, eine Einheit auswählen, die eine Token-Ring-Schnittstelle enthält. Dies ist wichtig, weil sich die Statistiken in der Anzeige "Ring Station" nur auf Token-Ring beziehen.

2. Je nachdem, was Sie untersuchen möchten, können Sie die Einträge in der Anzeige "Ring Station" anhand eines der folgenden drei Kriterien anzeigen:

### **By Ring Order**

Dadurch können Sie aktive Stationen auf dem Ring in der Reihenfolge ihrer physischen Verbindung mit dem Ring anzeigen. Dabei wird mit der aktiven Überwachung begonnen.

### By Address

Dadurch werden alle Einheiten angezeigt, die gegenwärtig an den Ring angeschlossen sind oder dies vorher waren.

### By Selected Station

Bei Auswahl dieser Option wird die Option "Select" aktiviert.

Klicken Sie die Option **Select** an, um das Dialogfenster "Station Select" zu öffnen. Anweisungen zum Hinzufügen, Ändern und Löschen von Stationseinträgen sind in der Beschreibung zu Abb. 34 auf Seite 80 enthalten.

3. Wählen Sie im Bereich "View Type" die benötigte Anzeigeart aus. Die tabellarische Darstellung ist immer verfügbar, während die Diagrammdarstellung und die Skalendarstellung nur dann verfügbar sind, wenn "Sort View" auf "By Selected Stations" eingestellt ist.
4. Klicken Sie zum Aufrufen der Anzeige "Ring Station" das Feld **OK** an.

## Vordefinierte Anzeigen

In Tabelle 27 werden die Ringstationsanzeigen beschrieben, die für Token-Ring verfügbar sind. Im Anhang E ist eine Liste mit verfügbaren Variablen enthalten.

Tabelle 27. Vordefinierte Ringstationsanzeigen

Anzeige	Token-Ring	Beschreibung
All	■	Enthält alle Variablen.
Errors	■	Auf dem Ring entdeckte Fehler, einschließlich doppelter Adressen, AC-Fehler und abgebrochener Rahmen.
Events	■	Beinhaltet den letzten NAUN, den Status der Station und die Zeitpunkte des letzten Eintreffens und des letzten Exits.



---

## Kapitel 6. Alarmnachrichten

In diesem Kapitel wird beschrieben, wie Alarmnachrichten auf Nways Manager Remote Monitor konfiguriert werden. Das Kapitel enthält die folgenden Abschnitte:

- Übersicht über Alarmnachrichten
- Alarmnachrichten konfigurieren

---

### Übersicht über Alarmnachrichten

Mit Nways Manager Remote Monitor können Sie Alarmnachrichten für bestimmte Netzwerkereignisse festlegen. Dadurch werden Sie informiert, sobald diese Ereignisse eintreten. Beachten Sie hierzu die folgenden Beispiele:

- Der Router im Netzwerk besitzt die Kapazität zum Weiterleiten von 3000 Paketen pro Sekunde (pps). Es treten jedoch Probleme beim Weiterleiten auf, wenn der obere Bereich der Leistungsfähigkeit erreicht wird. Daher möchten Sie informiert werden, wenn sich die Datenverkehrsrate 3000 pps annähert.
- Das Netzwerk läuft mit einer Rate von 1400 pps. In der Regel gilt eine CRC-Rate von mehr als 1% des Datenverkehrs im Netzwerk als zu hoch. Daher möchten Sie informiert werden, wenn die CRC-Rate 14 pps überschreitet.

Im Laufe der Zeit werden Sie eine Bibliothek mit an Ihre Bedürfnisse angepassten Alarmnachrichten aufbauen.

Sie können Alarmnachrichten einzeln verwenden. Sie können sie aber auch als Start- oder als Stoppereignisse beim Erfassen von Paketen mit Hilfe der Anwendung "Capture" (siehe Kapitel 7) einsetzen. Im ersten Beispiel oben könnten Sie beginnen, jedesmal alle vom Router übertragenen Pakete zu erfassen, wenn die Datenverkehrsrate 2800 Pakete pro Sekunde überschreitet. Wenn sie wieder unter dieses Niveau zurückgeht, könnten Sie die Erfassung beenden.

---

### Alarmnachrichten konfigurieren

Gehen Sie zum Konfigurieren von Alarmnachrichten wie folgt vor:

1. Wählen Sie im Menü "Analysis" den Eintrag **Alarms** aus, oder klicken Sie in der Knopfleiste den Knopf **Alarms** an. Dadurch wird das in Abb. 44 auf Seite 104 gezeigte Dialogfenster "Alarms" geöffnet.



Abbildung 44. Dialogfenster "Alarms"

2. Wählen Sie eine Einheit und eine Schnittstelle aus.

Wenn Sie zum ersten Mal Alarmnachrichten auf dieser Einheit festlegen oder wenn Sie alle vorherigen Alarmnachrichten gelöscht haben, werden in der Liste "Alarm Entries" keine vorhandenen Alarmnachrichten angezeigt. Statt dessen wird die Nachricht "No entries found on that device" angezeigt.

3. Klicken Sie zum Hinzufügen eines neuen Eintrags in die Liste "Alarms" die Option **Add** an. Dadurch wird das in Abb. 45 auf Seite 105 gezeigte Dialogfenster "Alarm Entry Creation" angezeigt.

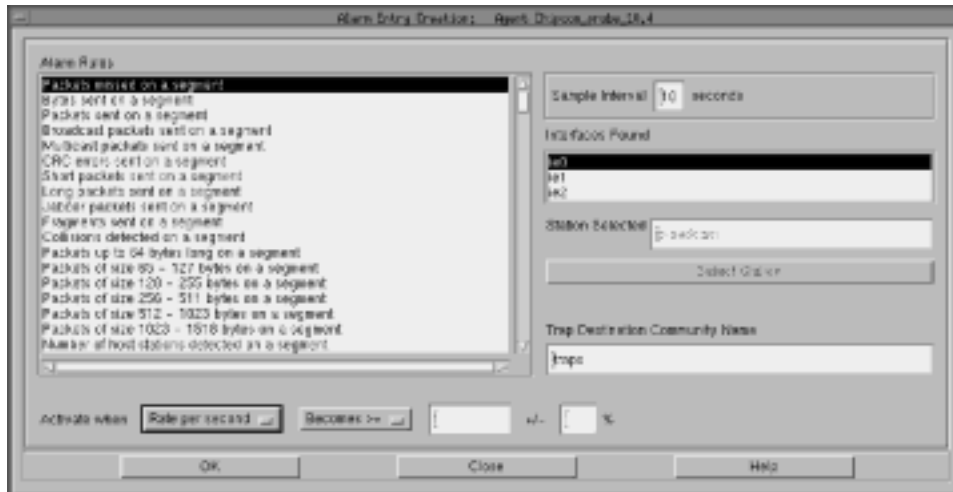


Abbildung 45. Dialogfenster "Alarm Entry Creation"

- Wählen Sie im Bereich "Alarm Rules" den erforderlichen Alarmtyp aus. Die Anzeige "Alarms" bietet eine breite Auswahl an Alarmtypen an. Die Liste "Alarm Rules" unterscheidet sich je nach Typ der verfügbaren Schnittstellen. In der Liste "Interfaces Found" werden die für die ausgewählte Alarmregel (Alarm Rule) zulässigen Schnittstellen aufgeführt. Wählen Sie die benötigte Alarmregel aus.
- Geben Sie im Bereich "Sample Interval" an, wie oft in der Anzeige überprüft werden soll, ob das betreffende Ereignis eingetreten ist.
- Bei Auswahl eines stationsspezifischen Alarmtyps wird die Option "Select Station" aktiviert. Klicken Sie diese Option an, um eine Station auszuwählen. Diese Prozedur wird im Abschnitt „Dialogfenster Stations verwenden“ auf Seite 107 beschrieben.
- Bei Bedarf können Sie den Namen der Benutzergemeinschaft für die Zieladresse der Alarmnachricht (Trap Destination Community Name) ändern. Wenn ein Alarm ausgelöst wird, wird eine SNMP-Alarmnachricht an alle Einheiten gesendet, die dieser Benutzergemeinschaft zugeordnet sind. Weitere Informationen zu Benutzergemeinschaften für Alarmnachrichten sind im Abschnitt „Benutzergemeinschaften für Alarmnachrichten festlegen“ auf Seite 40 enthalten.
- Bei manchen Alarmnachrichten wird zur Vervollständigung der Alarmbeschreibung eine weitere Auswahl von Objekten benötigt. Ein Beispiel hierfür ist ein Alarm auf einem Netzwerk-Hub, der die Anzahl der Pakete zählt, die an einem Anschluß in einer bestimmten Gruppe oder an einem beliebigen Anschluß einer Gruppe gesendet wurden.

Falls zur Vervollständigung der Alarmnachricht weitere Informationen erforderlich sind, wird das Feld "Additional Parameters" aktiviert. Klicken Sie das Feld **Additional Parameters** an, um das Dialogfenster "Alarm Variables" zu öffnen.

Geben Sie Werte für Variablen in den entsprechenden Feldern ein und klicken Sie das Feld **OK** an, um zum Dialogfenster "Alarm Entry Creation" zurückzukehren.

- f. Verwenden Sie den Bereich "Activate When" um anzugeben, wann der Alarm ausgelöst werden soll. Die meisten Alarmtypen sind an die Häufigkeit oder die Rate eines spezifischen Ereignisses gebunden, z. B. darauf, wann die CRC-Rate in einem Segment einen zulässigen Wert überschreitet. Manchmal sind sie auch an einen spezifischen Wert gebunden, z. B. wenn der neue Router die ersten Millionen Pakete weitergeleitet hat .

Mit Hilfe des Bereichs "Activate When" können Sie das Ereignis entweder in bezug auf den Wert der ausgewählten Variable oder in bezug auf die Paketrate für die ausgewählte Variable auswählen.

Für den Wert der Variable können Sie die Bedingung angeben, bei der der Alarm ausgelöst werden soll. Die folgenden drei Bedingungen sind verfügbar:

- Becomes >=** Die Paketrate oder der Wert ist größer-gleich dem angegebenen Wert.
- Becomes <=** Die Paketrate oder der Wert ist kleiner-gleich dem angegebenen Wert.
- Crosses** Die Paketrate oder der Wert unter- oder überschreitet den angegebenen Schwellenwert. Dadurch wird der Alarm nur ausgelöst, wenn der Wert oder die Rate unter- oder überschritten wird, aber nicht, wenn die Rate oder der Wert über oder unter dem Schwellenwert bleibt.

In Abb. 46 gibt die horizontale Linie die überwachte Alarmrate wieder und der schattierte Bereich gibt die angegebene Hysteresezone wieder.

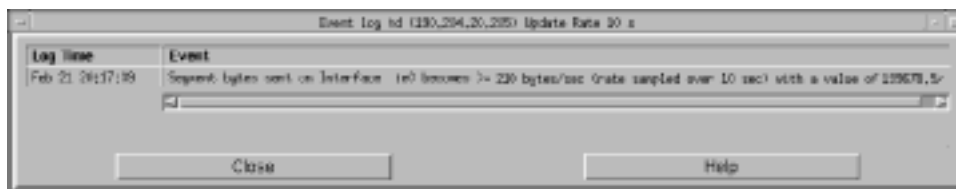


Abbildung 46. Hysteresezone

Die schwarze Linie gibt auf abstrakte Weise die tatsächlichen Netzwerkwerte für die festgelegten Variablen an. Für die drei oben erläuterten Bedingungstypen würden die folgenden Ergebnisse angegeben werden:

- Bei einer als **Becomes >=** angegebenen Alarmnachricht zeigen die Kreise im Diagramm, wann das Ereignis einen Alarm auslösen würde.
- Bei einer als **Becomes <=** angegebenen Alarmnachricht zeigen die Quadrate im Diagramm, wann das Ereignis einen Alarm auslösen würde.

- Bei einer als Crosses <= angegebenen Alarmnachricht zeigen die Kreise und Quadrate im Diagramm, wann das Ereignis einen Alarm auslösen würde.
4. Klicken Sie zum Bestätigen der Alarmeinstellungen im Dialogfenster "Alarm Entry Creation" das Feld **OK** an. Der neue Eintrag wird ab jetzt im Dialogfenster "Alarms" in der Liste "Alarm Entries" angezeigt.
  5. Klicken Sie im Dialogfenster "Alarms" das Feld **OK** an, um diese Alarmbedingung zu definieren. Bei Auslösung eines Alarms wird im Hauptfenster auf der Alarmleiste ein Alarmsymbol angezeigt, und im Ereignisprotokoll (Event Log) wird ein neuer Eintrag angezeigt.

### Dialogfenster Stations verwenden

Mit Hilfe des Dialogfensters "Stations" wird für eine Alarmnachricht eine Station angegeben. In Abb. 47 wird ein Beispiel für ein Dialogfenster "Stations" gezeigt.

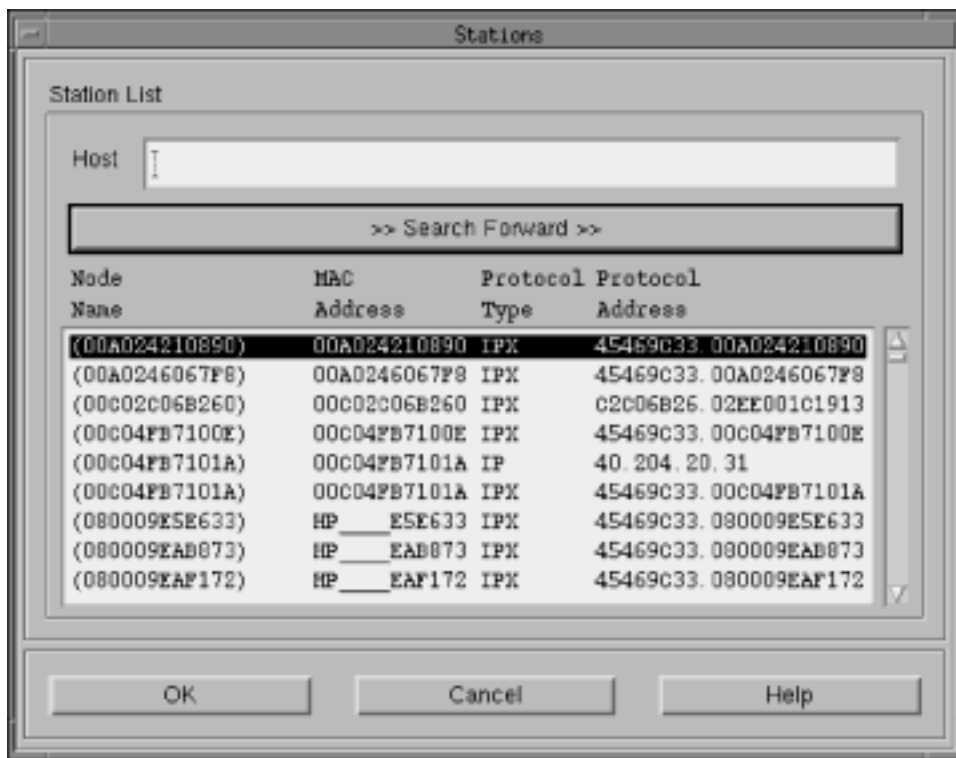


Abbildung 47. Dialogfenster "Stations"

- Geben Sie im Feld "Host" Zeichen oder Ziffern (z. B. die ersten Buchstaben eines Host-Namens oder die ersten Stellen einer MAC-Adresse) ein, um nach einer Station zu suchen. Das erste Vorkommen dieser Zeichenfolge an irgendeiner Position in der Station wird durch eine rote Leiste hervorgehoben. Sie können die Suche eingrenzen, indem Sie weitere Zeichen oder Ziffern hinzufügen.
- Klicken Sie die Option **>>Search Forward>>** an, um das nächste Vorkommen einer Zeichenfolge zu suchen. Wenn die Zeichenfolge in der Liste nur einmal vorkommt, bleibt die rote Leiste auf dem aktuellen Eintrag.

Mit Hilfe der Suchfunktion wird in jeder Spalte der Liste nach dem Inhalt des Feldes "Host" gesucht. Wenn Sie beispielsweise bei der Suche nach einem "Birne" genannten Host im Feld "Host" die Zeichenfolge "Bi" eingegeben haben, wird in der Suchliste möglicherweise zuerst der Host "Biene" hervorgehoben. Klicken Sie die Option **Search Forward** an, um zum nächsten Vorkommen der Zeichenfolge "Bi" zu gelangen, oder grenzen Sie die Suche ein, indem Sie zu der Zeichenfolge im Feld "Host" weitere Zeichen oder Ziffern hinzufügen.

- Die Auswahl einer Station erfolgt durch Anklicken in der Liste. Der hervorgehobene Eintrag wird durch die rote Suchleiste nicht ausgewählt.
- Klicken Sie eines der Felder **OK** oder **Cancel** an, um zum Dialogfenster "Alarm Entry Creation" zurückzukehren.

---

## Kapitel 7. Paketerfassung und Entschlüsselung

In diesem Kapitel wird erklärt, wie die Anwendungen "Capture" (Erfassung) und "Decode" (Entschlüsselung) von Nways Manager Remote Monitor verwendet werden. Das Kapitel enthält die folgenden Abschnitte:

- Übersicht über die Anwendungen "Capture" und "Decode"
- Anwendung "Capture" verwenden
- Erfasste Pakete entschlüsseln

---

### Übersicht über die Anwendungen "Capture" und "Decode"

Durch die Anwendung "Capture" werden Pakete aus dem Netzwerk mit Hilfe von vordefinierten Mustern und von Start- und Stoppbedingungen erfaßt. Sie können eine Bibliothek mit häufig verwendeten Konfigurationskriterien aufbauen, indem Sie die einzelnen Kriterien in einer Datei sichern. Sie können Sie dann bei Bedarf auf derselben Einheit erneut verwenden oder Sie können sie auf verschiedene Einheiten laden.

Die Anwendung "Decode" entschlüsselt alle wichtigen Protokolle und bietet ein geteiltes Fenster, in dem Anzeigen von Paketinhalten in den folgenden drei Detaillierungsebenen angezeigt werden: Ergebnistext, Kopfdaten und tatsächlicher Inhalt des Pakets.

Mit Hilfe der Funktionen "Conversation Trace" und "Analysis" können Sie ein spezifisches Paket anklicken und dadurch alle anderen Pakete des betreffenden Datenaustauschs anzeigen.

### Übersicht über die Struktur von Paketen

Vor dem Definieren von Erfassungspuffern muß die grundlegende Struktur von Netzwerkpaketen bekannt sein.

Pakete bestehen aus zwei Teilen: aus Kopfzeile und aus Daten. Der Kopfbereich enthält den Pakettyp und Protokollinformationen in einem Standardformat. Für diesen Teil des Pakets können Erfassungsfiler verwendet werden. Der Datenbereich verfügt über keine vordefinierte Struktur.

In der Regel enthält der Kopfbereich eines Pakets viele verschiedene Kopfzeilen. Diese stellen die Informationen für die verschiedenen Schichten innerhalb der Protokollhierarchie zur Verfügung. Beim Ausfüllen einer Schablone müssen Sie genügend Kopfdaten zur Verfügung stellen, damit diese Protokollschichten innerhalb eines Pakets identifiziert werden können. Es empfiehlt sich, weitere Informationen der Dokumentation zum jeweiligen Protokoll zu entnehmen.

---

## Anwendung Capture verwenden

Die Konfiguration der Paketerfassung wird über das in Abb. 48 gezeigte Dialogfenster "Capture Application" durchgeführt. Wählen Sie zum Ausführen der Anwendung "Capture" im Menü "Analysis" die Option **Capture** aus, oder klicken Sie in der Knopfleiste den Knopf **Capture** an.



Abbildung 48. Hauptdialogfenster "Capture"

Über dieses Dialogfenster können Sie die folgenden Funktionen ausführen:

- Im Bereich "Device Details" die Einheit auswählen, die Sie zum Erfassen von Paketen verwenden möchten.
- Erfassungspuffer erstellen, ändern und sichern, eigene Puffer aus einer Datei laden oder vordefinierte protokollspezifische Erfassungspuffer verwenden.
- Zum Anzeigen von erfassten Paketen die Anwendung "Decode" starten und eine Trace-Analyse des Datenaustauschs der Paketinhalte durchführen.

---

## Erfassungspuffer verwenden

Unter einem Puffer versteht man den Speicherbereich, der für die Speicherung von aus dem Netzwerk erfassten Paketen angelegt wird.

Im Bereich "Buffer Details" werden die Namen aller vordefinierten Erfassungskriterien angezeigt, die auf der Einheit aktiv sind. Außerdem wird in diesem Bereich definiert, wer über die Puffer verfügen kann.



Ferner enthält die Pufferbeschreibung die folgenden Informationen:

**Slice Size** Gibt die Größe des einem erfaßten Paket zugeordneten Speicherbereichs gefolgt von der Gesamtgröße des Puffers an.

**Buffer Size** Durch das Symbol (S) am Ende der Beschreibungszeile wird außerdem angezeigt, daß der Puffer über genügend Speicherbereich verfügt, um weitere Pakete aufzunehmen. Das Symbol (F) zeigt an, daß der Puffer voll ist.

**Anmerkung:** Die Einheit verfügt nur über eine begrenzte Menge an Ressourcen zur Speicherung von gepufferten Daten. Wenn alle Ressourcen der Einheit von einem der Puffer verbraucht werden, können die anderen Puffer keine erfaßten Pakete speichern. Zum Sparen von Ressourcen können Sie entweder Pakete zerstückeln oder, wie im Abschnitt "Neue Erfassungspuffer erstellen" beschrieben, Puffern Höchstgrößen zuordnen.

### Neue Erfassungspuffer erstellen

Über das Dialogfenster "Edit Packet Capture" können neue Erfassungspuffer erstellt werden. Gehen Sie zum Erstellen neuer Erfassungspuffer wie folgt vor:

1. Klicken Sie im Hauptdialogfenster der Anwendung "Capture" die Option **Add** an, um das in Abbildung 49 gezeigte Dialogfenster "Edit Packet Capture" zu öffnen.

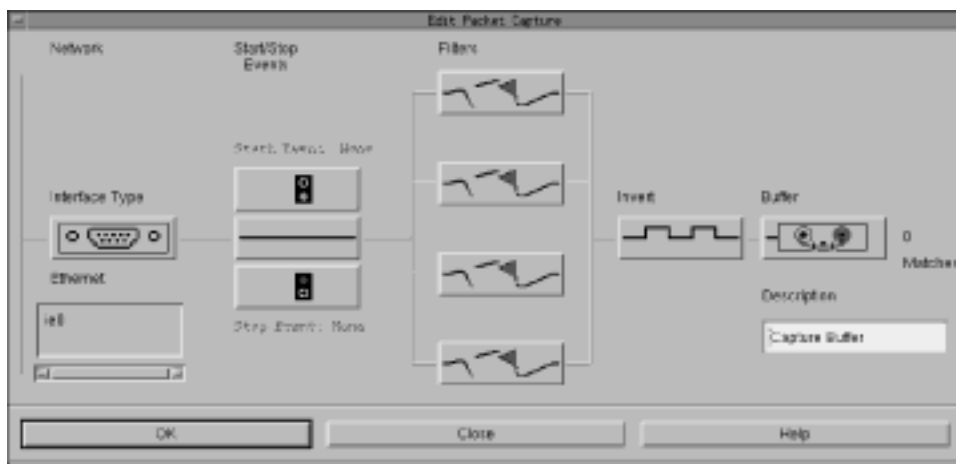


Abbildung 49. Dialogfenster "Edit Packet Capture"

2. Klicken Sie den Eintrag "Interface Type" an, um das in Abbildung 50 gezeigte Dialogfenster "Interface" zu öffnen. Verwenden Sie dieses Dialogfenster, um die Schnittstelle auszuwählen, die für die Paketerfassung verwendet werden soll. Klicken Sie das Feld **OK** an, um zum Dialogfenster "Edit Packet Capture" zurückzukehren.

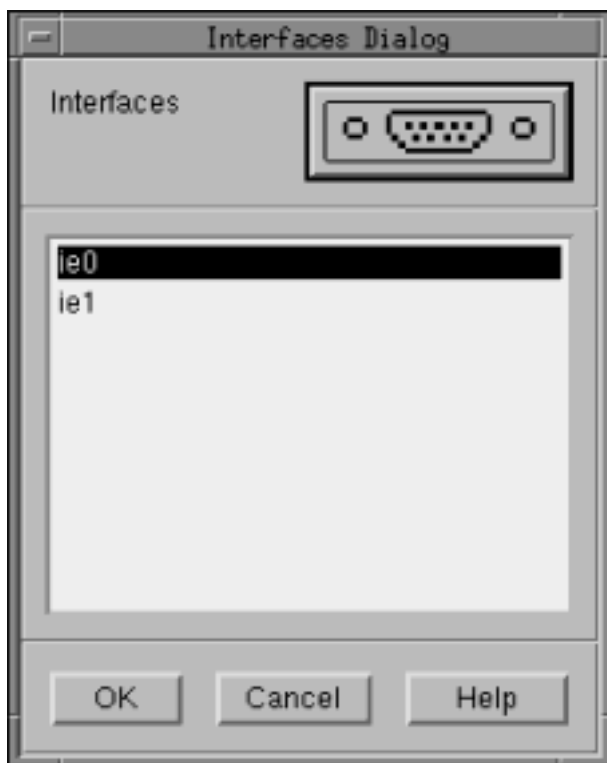


Abbildung 50. Dialogfenster "Interfaces"


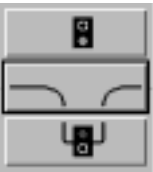


3. Möglicherweise möchten Sie das Erfassen von Paketen jedesmal automatisch starten oder beenden, wenn ein bestimmtes Alarmereignis auftritt (weitere Informationen hierzu sind in Kapitel 6 enthalten) oder wenn eine Gruppe von Paketen einem bestimmten Muster entspricht. Dies wird als Auslöser bezeichnet.
  - a. Gehen Sie wie folgt vor, um ein Auslöserereignis auszuwählen:
  - b. Klicken Sie eine der Optionen **Start Event** or **Stop Event** an, um das in Abb. 51 auf Seite 113 gezeigte Dialogfenster "Start/Stop Event" zu öffnen.



Abbildung 51. Dialogfenster "Start/Stop Event"


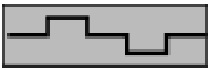
- Wenn Sie eine Alarmnachricht oder ein vorhandenes Ereignis verwenden möchten, müssen Sie dieses lediglich aus der Liste auswählen und das Feld **OK** anklicken.
  - Klicken Sie zum Hinzufügen eines neuen Erfassungsereignisses die Option **Add Capture Event** an. Dadurch wird eines der Dialogfenster "Edit Start Event" oder "Edit Stop Event" angezeigt. Weitere Informationen hierzu sind im Abschnitt „Neue Start- und Stoppereignisse erstellen“ auf Seite 120 enthalten.
  - Wählen Sie ein Erfassungsereignis, das Sie löschen möchten, im Dialogfenster "Start/Stop Event" aus, und klicken Sie die Option **Delete Event** an. Zum Löschen einer Alarmnachricht müssen Sie die Anzeige "Alarms" verwenden.
- c. Klicken Sie zum Aktivieren der Einträge "Start Event" und/oder "Stop Event" den Knopf **Activate** an, der sich zwischen den Knöpfen "Start Event" und "Stop Event" befindet. Dadurch werden, wie in Tabelle 28 auf Seite 114 gezeigt, eines der Ereignisse oder beide aktiviert.

Tabelle 28. Aktivierungsknöpfe

Aktivierungs-knopf	Status	Aktivierungs-knopf	Status
	Kein Start-oder Stoppereignis aktiviert.		Nur Stoppereignis aktiviert.
	Nur Startereignis aktiviert.		Sowohl Start- als auch Stoppereignis aktiviert.

- Klicken Sie einen der **Filter**-Knöpfe an, um anzugeben, auf welchen Pakettyp die Überwachung ausgerichtet ist. Durch Anklicken beliebiger Filterknöpfe können Sie bis zu vier Filter angeben. Detailliertere Informationen hierzu sind im Abschnitt „Funktion Filter Editor verwenden“ auf Seite 122 enthalten.
- Klicken Sie bei Bedarf die Option **Invert** (siehe Tabelle 29) an, um die Logik des Kanals umzukehren.

Tabelle 29. Umkehrknopf

Umkehrknopf	Beschreibung
	Sammelt die angegebenen Pakete.
	Sammelt alle Pakete außer den angegebenen.

6. Klicken Sie die Option **Buffer** an, um anzugeben, wie der Puffer beim Speichern von Paketen vorgehen soll. Das in Abb. 52 gezeigte Dialogfenster "Buffer Control" wird geöffnet.

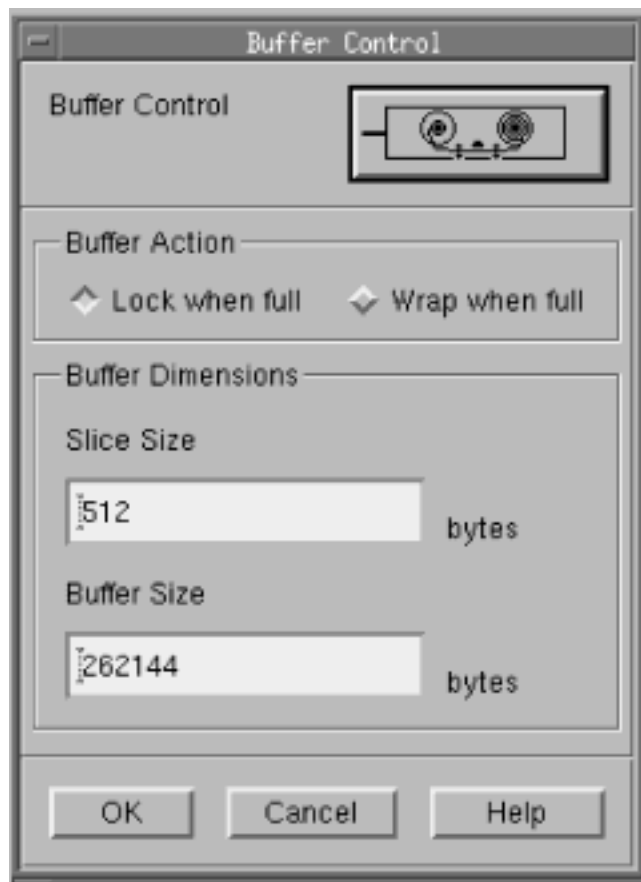


Abbildung 52. Dialogfenster "Buffer Control"

- a. Verwenden Sie die Felder im Dialogfenster "Buffer Control", um anzugeben, wie Pakete in der Einheit gespeichert werden sollen.

<b>Wrap</b>	Pakete werden fortlaufend erfaßt. Bei vollem Puffer werden alte Pakete entfernt.
<b>Lock</b>	Wenn der Puffer voll ist, werden keine Pakete mehr erfaßt.
<b>Slice Size</b>	Gibt den Anteil des Pakets an, der erfaßt werden soll. Je nachdem, wieviele Informationen sie sammeln möchten, sollten Sie ihn so klein wie möglich halten. Stellen Sie jedoch sicher, daß der erfaßte Teil des Pakets groß genug ist, damit die Anwendung "Decode" mit ihm arbeiten kann. Je größer der Anteil des Pakets ist, umso schneller füllt sich der Puffer.
<b>Buffer Size</b>	Hiermit können Sie die Größe des Erfassungspuffers in Byte angeben. Wenn Sie möchten, daß dem Puffer von der Einheit soviel Speicher zugeordnet wird, wie verfügbar ist, stellen Sie diesen Wert auf -1 ein. Dadurch wird in der Liste "Buffers" für den betreffenden Puffer ON DEMAND angezeigt.

- b. Klicken Sie das Feld **OK** an, um zum Dialogfenster "Edit Packet Capture" zurückzukehren.
7. Geben Sie für Ihre Erfassungskonfiguration im Feld "Event Description" einen Namen ein. Wenn Sie sie beispielsweise so eingerichtet haben, daß sie alle TCP/IP-Pakete erfassen soll, könnten Sie sie TCP-Puffer nennen.
8. Klicken Sie das Feld **OK** an, um diesen neuen Erfassungspuffer auf der ausgewählten Einheit zu erstellen.

## Einen Erfassungspuffer sichern

Wenn Sie einen Erfassungspuffer konfiguriert haben und er im Dialogfenster der Anwendung "Packet Capture" (siehe Abb. 48 auf Seite 110) angezeigt wird, können Sie den Puffer in einer Datei sichern und ihn später erneut auf eine beliebige Einheit laden. Gehen Sie zum Sichern eines Erfassungspuffers wie folgt vor:

1. Wählen Sie den Puffereintrag aus der Liste aus.
2. Klicken Sie im Bereich "Buffer Details" den Eintrag **File** an, um das in Abb. 53 auf Seite 118 gezeigte Dialogfenster "Buffer Save/Load" zu öffnen.
3. Klicken Sie die Option **Save** an.
4. Geben Sie im Bereich "Selection" einen Dateinamen ein.
5. Klicken Sie das Feld **OK** an, um die Datei zu sichern, oder klicken Sie die Option **Cancel** an, um sie nicht zu sichern.

## Erfassungspuffer ändern

Sie können vorhandene Erfassungspuffer jederzeit ändern, um sie Ihren Erfordernissen anzupassen. Gehen Sie zum Ändern eines Erfassungspuffers wie folgt vor:

1. Wählen Sie den Puffereintrag aus der Liste aus.
2. Klicken Sie im Bereich "Buffer Details" die Option "Modify" an, um das in Abb. 49 auf Seite 111 gezeigte Dialogfenster "Edit Packet Capture" zu öffnen.
3. Führen Sie ab Schritt 6 die im Abschnitt „Neue Erfassungspuffer erstellen“ auf Seite 111 beschriebene Prozedur durch, um an der aktuellen Erfassungskonfiguration Änderungen vorzunehmen.
4. Klicken Sie im Dialogfenster "Edit Packet Capture" das Feld **OK** an, um die Änderungen zu bestätigen, oder klicken Sie die Option **Cancel** an, um die Änderungen nicht zu bestätigen.

## Vordefinierte Erfassungspuffer verwenden

Von Nways Manager Remote Monitor werden einige vordefinierte protokollspezifische Puffer zur Verfügung gestellt, um die Konfiguration von Erfassungspuffern zu vereinfachen. Die Filterschablonen in diesen Puffern wurden mit den Kopfdaten vorkonfiguriert, die für die einzelnen Protokollschichten erforderlich sind. Diese Puffer können aus einer Datei geladen und anschließend soweit erforderlich geändert werden.

Gehen Sie zum Laden eines vordefinierten Erfassungspuffers wie folgt vor:

1. Klicken Sie im Hauptdialogfenster der Anwendung "Capture" im Bereich "Buffer Details" den Eintrag **File** an, um das in Abb. 53 auf Seite 118 gezeigte Dialogfenster "Buffer Save/Load" zu öffnen.

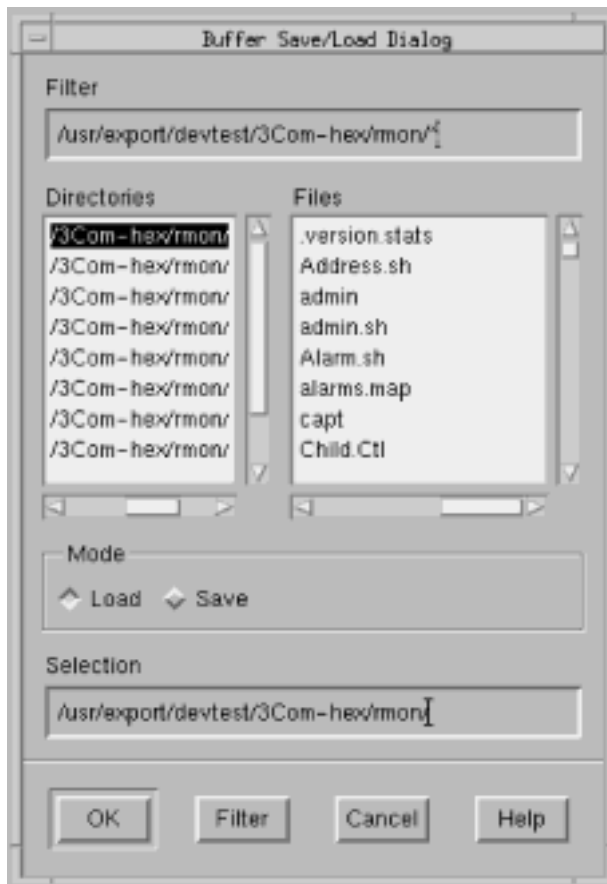


Abbildung 53. Dialogfenster "Buffer Save/Load"

2. Suchen Sie die vordefinierten Puffer, indem Sie einen der folgenden Schritte ausführen:

- Geben Sie im Feld "Filter"
  - /usr/LANReMon/rmon/vi\_chans/\*
  - ein.
- Verwenden Sie die Liste "Directories", um das Verzeichnis
  - /usr/LANReMon/rmon/vi\_chans
  - zu suchen.



3. Wählen Sie aus der Liste "Files" einen vordefinierten Puffer aus. Die Liste mit vordefinierten Filtern ist je nach Verkabelungstyp der ausgewählten physischen Schnittstelle unterschiedlich. Dies wird in Tabelle 30 dargestellt.

Tabelle 30. Beschreibung der vordefinierten Filter

Filter	Verkabelungstyp			Beschreibung
	Ethernet	Token-Ring	FDDI	
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 außer SNMP-Paketen.
SMTP	■	■	■	Übergibt nur SMTP-Pakete.
SNMP	■	■	■	Übergibt nur SNMP-Pakete.
TCP	■	■	■	Übergibt alle TCP-Pakete.
Telnet	■	■	■	Übergibt nur Telnet-Pakete.
UDP	■	■	■	Übergibt alle UDP-Pakete.
WWW	■	■	■	Übergibt nur WWW-Pakete.
XNS	■			Übergibt nur XNS-Pakete.

4. Klicken Sie die Option **Load** an.
5. Klicken Sie das Feld **OK** an, um den Puffer zu laden, oder klicken Sie die Option **Cancel** an, um den Vorgang abubrechen und zum Hauptdialogfenster der Anwendung "Capture" zurückzukehren.

Nachdem Sie das Feld **OK** angeklickt haben, wird der Erfassungspuffer im Bereich "Buffer Details" angezeigt.

Wählen Sie den Erfassungspuffer aus, und klicken Sie im Bereich "Buffer Details" die Option **Modify** an, um das in Abb. 49 auf Seite 111 gezeigte Dialogfenster "Edit Packet Capture" zu öffnen.

6. Führen Sie die im Abschnitt „Neue Erfassungspuffer erstellen“ auf Seite 111 beschriebenen Schritte durch.

### Erfassungspuffer aus einer Datei laden

Wenn Sie einen Erfassungspuffer vorher in einer Datei gesichert haben, können Sie ihn zu einem späteren Zeitpunkt auf eine beliebige Einheit laden. Der Verkabelungstyp der ausgewählten Schnittstelle auf der Zieleinheit muß mit dem Verkabelungstyp der Schnittstelle identisch sein, auf der der Puffer ursprünglich erstellt wurde.

1. Wählen Sie im Bereich "Device" die Einheit aus, auf die der Puffer geladen werden soll.
2. Klicken Sie im Bereich "Buffer Details" den Eintrag **File** an, um das in Abbildung 53 gezeigte Dialogfenster "Buffer Save/Load" zu öffnen.
3. Wählen Sie die Pufferdatei aus, die Sie verwenden möchten.
4. Klicken Sie die Option **Load** an.
5. Klicken Sie das Feld **OK** an, um die Datei zu laden, oder klicken Sie die Option **Cancel** an, um den Vorgang abubrechen.

Der Puffer wird direkt in die Einheit geladen. Wenn dieser Vorgang abgeschlossen ist, wird der Puffereintrag im Hauptdialogfenster der Anwendung "Capture" in der Liste "Buffers" angezeigt.

---

### Neue Start- und Stoppereignisse erstellen

Gehen Sie wie folgt vor, um einen Auslöser zu erstellen, der das Sammeln von Paketen aus dem Netzwerk startet oder beendet:

1. Klicken Sie im Hauptdialogfenster der Anwendung "Capture" die Option **Add** an, um das Dialogfenster "Edit Packet Capture" anzuzeigen.
2. Klicken Sie einen der Einträge **Start Event** oder **Stop Event** an, um die Liste mit verfügbaren Alarmnachrichten und Ereignissen anzuzeigen.
3. Klicken Sie die Option **Add Capture Event** an, um das Dialogfenster "Channel Event Editor" zu öffnen (siehe Abb. 54 auf Seite 121).

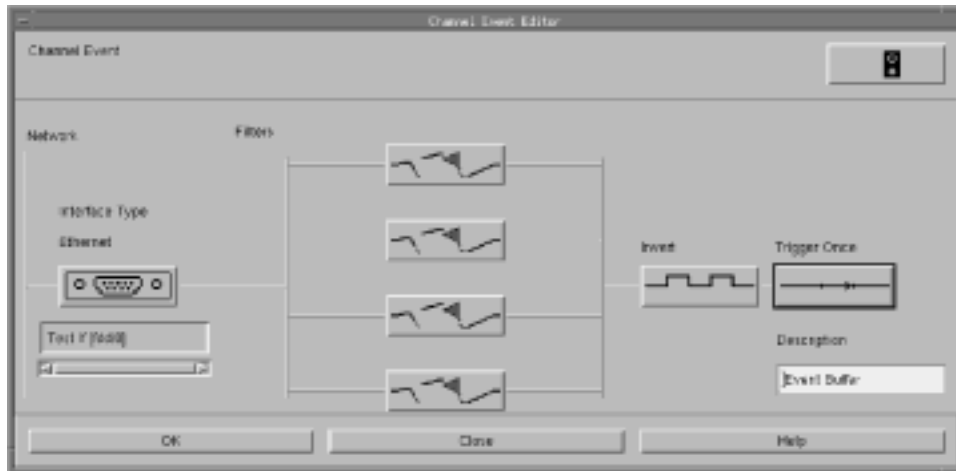


Abbildung 54. Dialogfenster "Channel Event Editor"

Verwenden Sie dieses Dialogfenster, um eine neue Menge von Erfassungskriterien zu erstellen und unter dem eigenen Ereignisnamen zu speichern. Indem Sie Ereignisse auf diese Weise verwenden, können Sie detailliertere Auslösebedingungen definieren, als wenn Sie nur die Funktion "Alarms" verwenden.

4. Klicken Sie den Eintrag "Interface Type" an, um das Dialogfenster "Interfaces" zu öffnen, und geben Sie die Schnittstelle auf der Einheit an, die Sie verwenden möchten

Dabei muß es sich nicht um die Schnittstelle handeln, die für das Erfassen vorgesehen ist. Sie können auf einer Schnittstelle die Überwachung auf ein bestimmtes Paket oder einen bestimmten Pakettyp ausrichten und anschließend auf einer anderen Schnittstelle mit dem Erfassen beginnen.

5. Klicken Sie einen der Filterknöpfe an, um anzugeben, auf welchen Pakettyp die Überwachung ausgerichtet ist. Durch Anklicken beliebiger Filterknöpfe können Sie bis zu vier Filter angeben. Weitere Informationen hierzu sind im Abschnitt „Funktion Filter Editor verwenden“ auf Seite 122 enthalten.
6. Klicken Sie bei Bedarf die Option **Invert** an, um die Logik der ursprünglichen Operation umzukehren.
7. Klicken Sie das Feld "Trigger" an, um Auslösebedingungen zu definieren. "Trigger Once" bedeutet, daß nur ein Ereignis generiert wird. "Trigger Many" bedeutet, daß ein Ereignis jedesmal erzeugt wird, wenn ein Paket durch den Kanal übermittelt wird.
8. Geben Sie im Feld "Description" einen Namen für dieses Ereignis ein.
9. Klicken Sie das Feld **OK** an, um dieses neue Ereignis zu sichern. Es bildet jetzt einen Teil der eigenen Ereignisbibliothek.

---

## Funktion Filter Editor verwenden

Mit Hilfe der Funktion "Filter Editor" können Sie sowohl bestimmte Pakettypen als auch spezifische Pakete erfassen. Sie können bis zu vier Filter angeben, die für jedes Paket gleichzeitig ausgeführt werden.

Im Lieferumfang der Anwendung "Capture" von Nways Manager Remote Monitor sind eine Reihe von sofort einsatzfähigen Protokollschablonen enthalten. Jede dieser Schablonen ist dafür vorgesehen, daß Sie den Pakettyp angeben können, den Sie aus dem Netzwerk filtern möchten. Eine große Bandbreite an Protokollfamilien wird unterstützt.

## Platzhalterzeichen in Filterschablonen verwenden

Beim Ausfüllen von Schablonen können Sie X als Platzhalterzeichen verwenden. Dies könnte beispielsweise nützlich sein, wenn Sie versuchen, alle Pakete im Netzwerk zu erfassen, die von Sun-Workstations ausgegeben wurden. Da Sie wissen, daß alle Produkte von Sun das Herstellerpräfix

080020

in ihrer Mac-Adresse enthalten, können Sie folgendes in das Feld "Source Address" eintragen: 080020XXXXXX.

## Einen Filter definieren

Gehen Sie zum Definieren eines Filters wie folgt vor:

1. Klicken Sie im Dialogfenster "Edit Packet Capture" die Option **Filter** an, um das in Abb. 55 auf Seite 123 gezeigte Dialogfenster "Filter Editor" zu öffnen.

Im Dialogfenster "Filter Editor" wird eine Liste mit Protokollschablonen angezeigt, aus der Sie auswählen können. Die Liste mit Schablonen ist je nach Verkabelungstyp der ausgewählten Schnittstelle unterschiedlich.

**Anmerkung:** Für jede Art von Kopfzeile müssen Sie in den entsprechenden Feldern die relevanten Informationen eingeben. Dadurch wird sichergestellt, daß von Nways Manager Remote Monitor der richtige Pakettyp gefiltert wird.

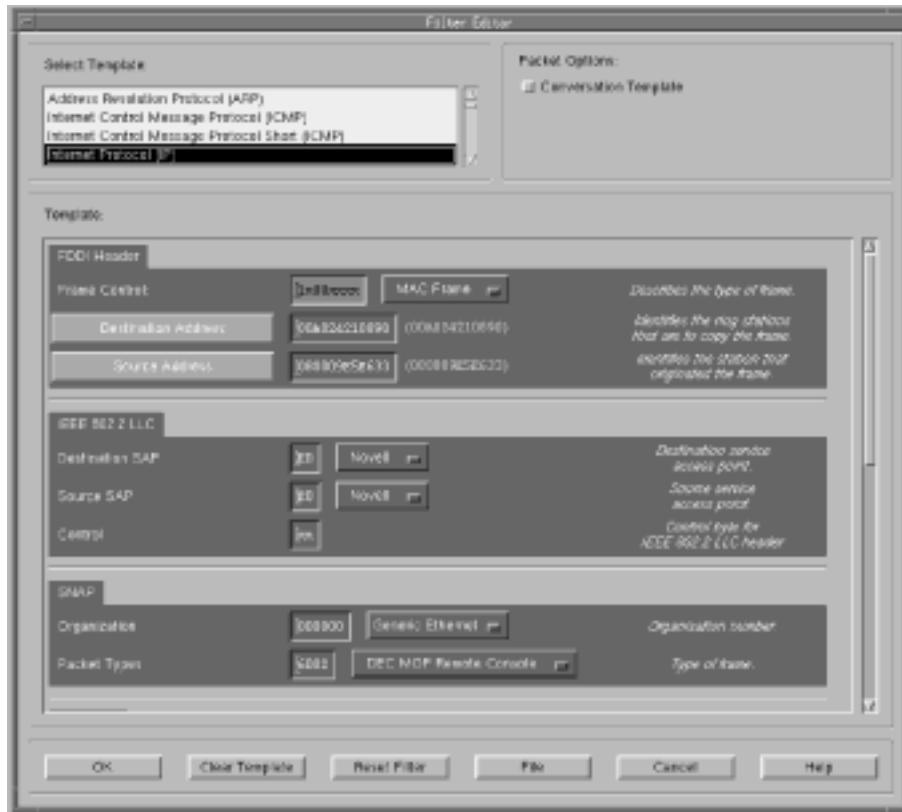


Abbildung 55. Dialogfenster "Filter Editor"

2. Wählen Sie im Bereich "Select Template" die erforderliche Schablone aus.
3. Klicken Sie im Bereich "Packet Options" eines der Dialogfenster **any size** oder **any packets** an, um allgemeine Paketvorgaben einzustellen, wie z. B. die Länge des Pakets oder ob das Paket einen CRC-Fehler aufweist oder wohlgeformt ist. Mit Hilfe eines logischen AND werden die Bedingungen für Größe und für Typ miteinander kombiniert.
4. Die Schablonen stellen Felder für Quellen- und Zieladressen zur Verfügung, damit der Datenverkehr von einer Adresse zur anderen auf Netzwerk- und auf Einheitenebene erfasst werden kann. Wenn jedoch die Option "Conversation Template" aktiviert ist, wird der in beide Richtungen zwischen den angegebenen Punkten stattfindende Datenverkehr von der Anwendung erfasst.

Beispielsweise werden in einer "Internet Protocol"-Schablone im Bereich "Ethernet Header", wie in Abb. 56 auf Seite 124 gezeigt, die MAC-Adressen sowohl für das Ziel als auch für die Quelle eingegeben.

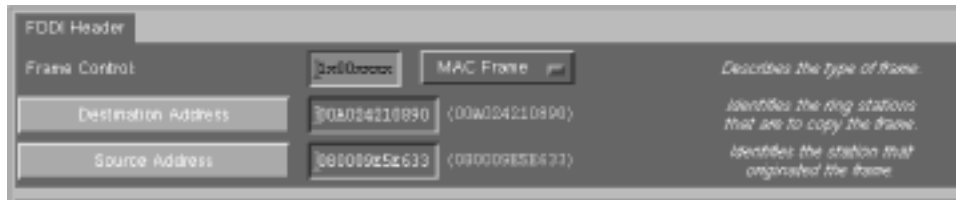


Abbildung 56. MAC-Adressen für Ziel und für Quelle eingeben

Durch die Anwendung wird der Datenverkehr erfaßt, der von der Quellenadresse an die Zieladresse geleitet wird.

**Anmerkung:** Wenn die Option "Conversation Template" aktiviert ist, werden die Adressen in jeder Position in der Filterschablone umgekehrt.

Der Vorgang des Eingebens von Ziel- und Quellenadressen wird von der Anwendung "Capture" vereinfacht, indem eine Liste mit verfügbaren Stationen bereitgestellt wird. Klicken Sie einen der Einträge "Destination Address" oder "Source Address" an, um das Dialogfenster "Stations" zu öffnen. Diese Prozedur wird im Abschnitt „Dialogfenster Stations verwenden“ auf Seite 107 beschrieben.

5. Vervollständigen Sie die Angaben im Dialogfenster "Filter Editor". Die angezeigten Felder unterscheiden sich von Protokoll zu Protokoll. Sie sind farbcodiert wie in Tabelle 31 aufgeführt:

Tabelle 31. Farbcodierungen der Feldarten

Feldart	Farbe
Binär	Grün
Dezimal	Pink
Hexadezimal	Purpurrot

Manche Felder verfügen über ein Dialogfenstermenü, aus dem Sie auswählen können.

6. Klicken Sie das Feld **OK** an, um diesen Filter zu aktivieren.

### Dialogfenster Stations verwenden

Mit Hilfe des Dialogfensters "Stations" wird angegeben, ob es sich bei einer Station um eine Quellen- oder eine Zieladresse handelt. Weitere Informationen hierzu sind im Abschnitt „Dialogfenster Stations verwenden“ auf Seite 107 enthalten.

## Erfaßte Pakete entschlüsseln

Klicken Sie zum Anzeigen der erfaßten Pakete im Hauptdialogfenster der Anwendung "Capture" die Option "Decode" an. Dadurch wird das in Abb. 57 gezeigte Dialogfenster "Decode" geöffnet.

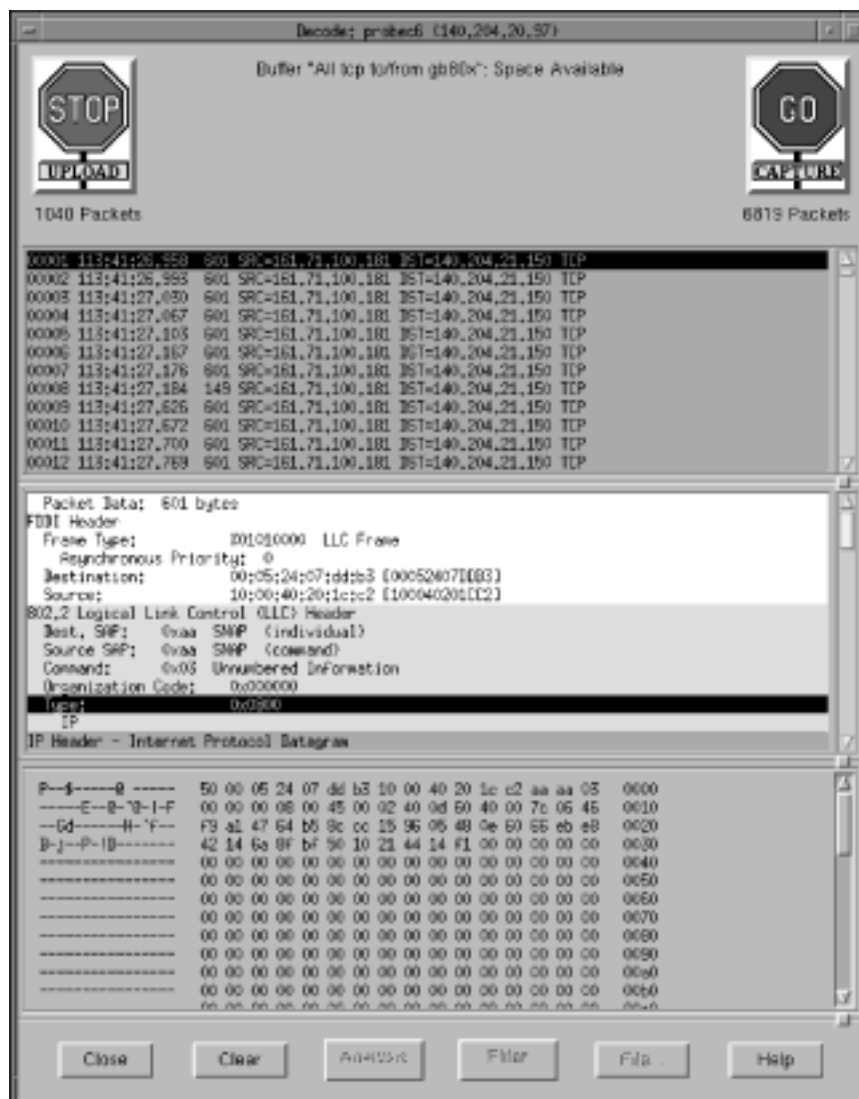


Abbildung 57. Dialogfenster "Decode"

Das Dialogfenster der Anwendung "Decode" ist in drei Anzeigen unterteilt. Dadurch können detaillierte Informationen zu einem Paket angezeigt werden.

- Die obere Anzeige bietet eine Zusammenfassung der Entschlüsselung von Paketen. Wählen Sie in dieser Anzeige das benötigte Paket aus.
- Die mittlere Anzeige bietet eine detaillierte Entschlüsselung des ausgewählten Pakets.
- In der unteren Anzeige wird das ausgewählte Paket im Hexadezimalformat angezeigt.

Zur einfachen Identifikation ist jedes Protokoll farbcodiert. (Eine vollständige Liste mit unterstützten Entschlüsselungen ist im Anhang C enthalten.) Sie können die Größe der einzelnen Anzeigen Ihren Erfordernissen anpassen. Klicken Sie die Größensteuerfelder in der rechten unteren Ecke eines Teilfensters an und ziehen Sie sie, um die Größe einer Anzeige zu ändern.

## Pakete mit Hilfe der Anwendung Decode erfassen

Über dieses Dialogfenster können Sie steuern, wann die Einheit das Erfassen von Paketen starten oder beenden soll und wann die erfaßten Pakete zur Analyse hochgeladen werden sollen. Mit Hilfe des Knopfs "Capture" wird gesteuert, wann die Paketerfassung auf der Einheit gestartet und wann sie gestoppt wird (siehe Abb. 58).



Abbildung 58. Knopf "Capture"

Gehen Sie zum Erfassen von Paketen wie folgt vor:

1. Klicken Sie den Knopf **Go Capture** an, damit Nways Manager Remote Monitor die vorhandenen Pufferinhalte von der Einheit entfernt, alle festgelegten Erfassungsauslöser zurücksetzt und mit dem Erfassen einer völlig neuen Gruppe von Paketen beginnt. Dies hat keine Auswirkungen auf vorher hochgeladene Pakete. Der Knopf springt auf **Stop Capture** um. Unterhalb des Knopfes wird die Gesamtzahl der erfaßten Pakete angezeigt.
2. Klicken Sie den Knopf **Stop Capture** an, um das Erfassen von Paketen zu stoppen.



## Pakete mit Hilfe der Anwendung Decode hochladen

1. Mit Hilfe der Funktion "Upload" kann das Hochladen von Paketen von der Einheit gestartet oder gestoppt werden. Gehen Sie wie folgt vor, um Pakete vom Erfassungspuffer auf einer Einheit hochzuladen: Klicken Sie den Knopf **Go Upload** an. Daraufhin beginnt Nways Manager Remote Monitor, Pakete vom Erfassungspuffer zu der Liste mit geladenen Paketen im Dialogfenster "Decode" hinzuzufügen. Der Knopf springt auf **Stop Upload** um.

Unterhalb des Knopfs "Upload" wird die Anzahl der hochgeladenen Pakete angezeigt. Während sich die Anzahl der von der Anwendung in das Dialogfenster hochgeladenen Pakete erhöht, wird dieser Vorgang veranschaulicht, indem sich die Schiebeleiste im oberen Dialogfenster verkürzt.

2. Klicken Sie den Knopf **Stop Upload** an, um das Hochladen von Paketen von der Einheit zu stoppen.

**Anmerkung:** Falls der Kontakt von Nways Manager Remote Monitor zur Einheit während des Hochladens von Paketen verlorengeht, werden Sie gefragt, ob erneut versucht werden soll, Kontakt zu der Einheit aufzunehmen. Klicken Sie die Option **Retry** an, damit Nways Manager Remote Monitor versucht, erneut Kontakt zur Einheit aufzunehmen. Das Dialogfenster "Retry" wird so lange angezeigt, bis der Kontakt zwischen Nways Manager Remote Monitor und der Einheit hergestellt ist oder Sie den Hochladeversuch abbrechen.

3. Sie können den Inhalt des Dialogfensters "Decode" jederzeit löschen, indem Sie die Option **Clear** anklicken.

---

## Filtern nach dem Erfassen

Nachdem Sie erfasste Pakete hochgeladen haben, können Sie diese Pakete noch stärker filtern, um nach Untermengen der erfassten Daten zu suchen.

1. Klicken Sie im Dialogfenster "Decode" die Option **Filter** an, und wählen Sie die Option **Specify** aus, um das Dialogfenster "Channel Editor" zu öffnen.
2. Die Schnittstellen- und Kanaleinstellungen werden automatisch vorgenommen und können nicht geändert werden.
3. Im Dialogfenster "Channel Editor" können Sie bis zu vier Filter angeben, indem Sie jeweils einen der Filterknöpfe anklicken. Anweisungen zum Definieren eines Filters sind im Abschnitt „Funktion Filter Editor verwenden“ auf Seite 122 enthalten.
4. Klicken Sie bei Bedarf die Option **Invert** an, um die Logik des Kanals umzukehren.
5. Klicken Sie das Feld **OK** an, um mit dem Filtern von Paketen zu beginnen und zum Dialogfenster "Decode" zurückzukehren. In diesem Dialogfenster werden nur Pakete angezeigt, die Ihren Filterspezifikationen entsprechen. Die Anzahl der gefilterten Pakete wird unterhalb der Pufferbeschreibung im Kopfzeilenbereich angezeigt.
6. Klicken Sie den Eintrag **Filter** an, um das nachträgliche Filtern abzubrechen und um zur ursprünglichen Paketanzeige zurückzukehren, und wählen Sie die Option **Reset** aus.

## Funktionen Conversation Trace und Analysis

In manchen Paketanzeigen wird der Datenaustausch zwischen Maschinen im Netzwerk angezeigt. Verwenden Sie die Funktionen "Conversation Trace" und "Analysis", um einen detaillierteren Einblick in diese Anzeigen zu erhalten.

1. Wählen Sie im Dialogfenster "Decode" das gewünschte Paket aus der oberen Anzeige aus.
2. Klicken Sie das Feld **Analysis** an. Dadurch wird die Auswahl einer Ablaufverfolgung des Datenaustauschs mit Zeitmarkierung ermöglicht. Diese Ablaufverfolgung basiert entweder auf den MAC-Adressen oder auf den IP-Adressen.

**Anmerkung:** Der Datenaustausch auf IP-Schicht ist vor allem dann nützlich, wenn sich die IP-Hosts auf verschiedenen Seiten eines Router befinden und sich die MAC-Adresse des Router im Paket befindet.

3. In diesem Fall wird das in der Zusammenfassungsanzeige ausgewählte Paket von Nways Manager Remote Monitor als Schlüssel für den Datenaustausch verwendet, den Sie überwachen möchten. Die Pakete, die an diesem Datenaustausch beteiligt sind, werden herausgefiltert und im in Abb. 59 gezeigten Dialogfenster "Conversation Trace" angezeigt.

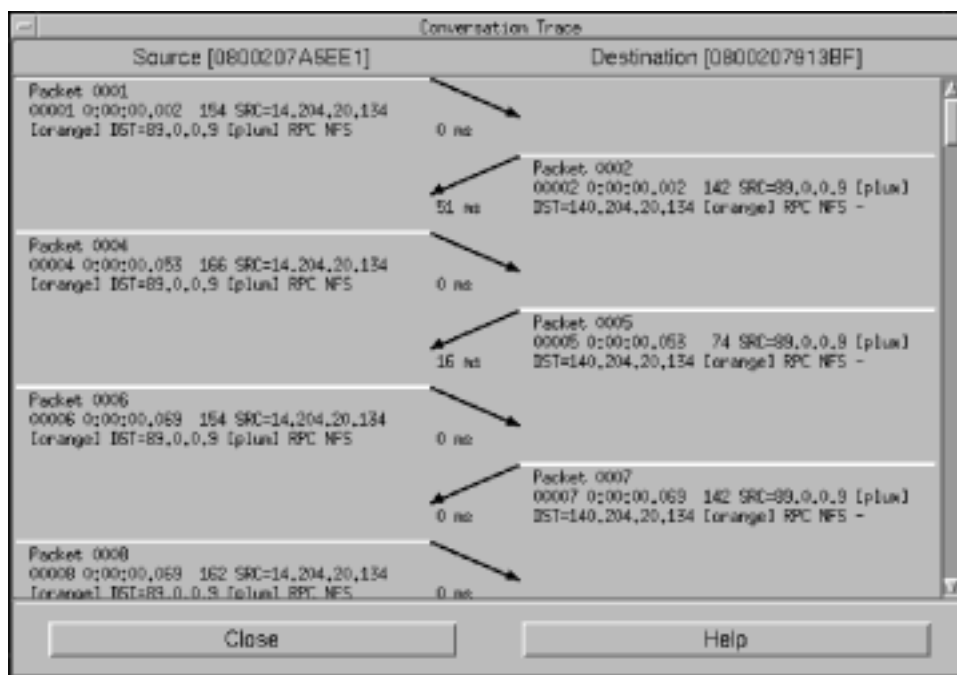


Abbildung 59. Dialogfenster "Conversation Trace"

Im Dialogfenster "Conversation Trace" wird die Beziehung zwischen den am ausgewählten Datenaustausch beteiligten Paketen hervorgehoben. Das Dialogfenster bietet einen Gesamtüberblick über den Datenaustausch.

Die Zeitangaben unterhalb der Pfeile in der Mitte der Anzeige geben die Verzögerungen beim Austausch zwischen Paketen in Millisekunden wieder.

Es ist sinnvoll, auf Pakete zu achten, die von einer Seite wiederholt gesendet werden, bevor die andere Seite antwortet - dies kann auf Überlastungsprobleme hinweisen.

---

## Erfaßte Pakete sichern und laden

Im folgenden Abschnitt wird erläutert, wie erfaßte Pakete gesichert und geladen werden.

### Pakete sichern

Gehen Sie zum Sichern eines erfaßten Pakets wie folgt vor:

1. Klicken Sie den Knopf **File** im Dialogfenster "Decode" (siehe Abb. 57 auf Seite 125) an, um das Dialogfenster "File" zu öffnen. In Abb. 60 wird ein Beispiel für das Dialogfenster "File" gezeigt.

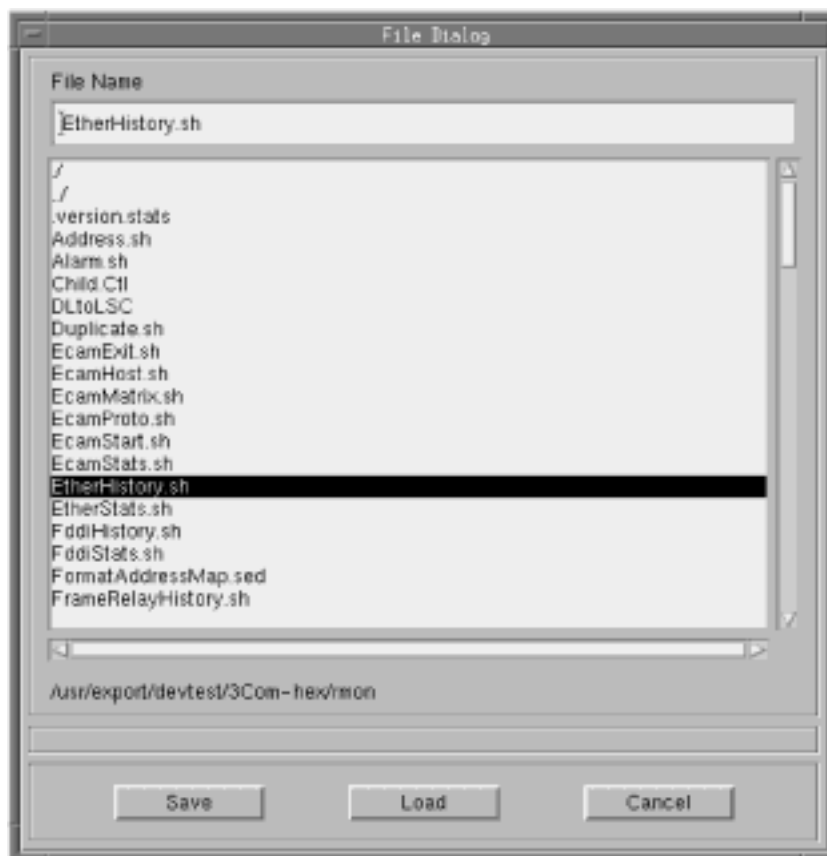


Abbildung 60. Dialogfenster "File"

2. Die Pakete können in den folgenden Dateiformaten gesichert werden:

**Network General Sniffer** Die Ergebnisdatei kann in einen Network General Sniffer geladen werden.

**ASCII** Die Ergebnisdatei kann in einen Texteditor geladen oder gedruckt werden.

**Achtung:** Da ASCII-Dateien sehr groß sein können, müssen Sie sicherstellen, daß Sie über genügend Plattenspeicherplatz verfügen, bevor Sie die Pakete im ASCII-Format sichern.

**W&G DA-30 Capture File** Die Datei kann in einen Wandel & Goltermann DA-30-Analyzer geladen werden.

**Anmerkung:** Auf einem DA-30-Analyzer wird FDDI nicht unterstützt.

**Nways Manager Remote Monitor** Zur weiteren Analyse kann die Datei zurück ins Dialogfenster "Packet Decode" geladen werden.

3. Geben Sie im Bereich "File Name" einen Dateinamen ein, und klicken Sie dann die Option **Save** an.

### **Erfasste Pakete laden**

Wiederholen Sie die oben aufgeführten Schritte, um ein erfaßtes Paket zu laden, das Sie vorher gesichert haben, aber klicken Sie die Option **Load** anstelle der Option **Save** an, wenn Sie bei Schritt 3 angelangt sind. Dadurch können Sie Pakete, die vorher mit dieser Anwendung im Format Nways Manager Remote Monitor gesichert wurden, von einem Network General Sniffer oder einem Wandel & Goltermann DA-30-Analyzer laden.



---

## Kapitel 8. Zusätzliche Funktionen von Nways Manager Remote Monitor

In diesem Kapitel werden die zusätzlichen Funktionen von Nways Manager Remote Monitor beschrieben. Das Kapitel enthält die folgenden Abschnitte:

- Anwendung "Address Map"
- Anwendung "Protocol Distribution"
- Anwendung "Data Export"
- Anwendung "Data Collector" verwenden

Die Anwendungen "Address Map" und "Protocol Distribution" können entweder mit der Software SmartAgent oder mit RMON2 ausgeführt werden. Anweisungen zum Aktivieren von SmartAgent-Anwendungen sind im Abschnitt „Software SmartAgent herunterladen“ auf Seite 192 enthalten. Die Anwendung "Roving Analysis Port" und die Verwendung von PACMIB-Funktionalität werden im Anhang D erläutert.

---

### Anwendung Address Map

In der Anwendung "Address Map" werden Tabellen angezeigt, in denen Zuordnungen von MAC-Adressen und Adressen der Vermittlungsschicht angezeigt werden. Diese Tabellen werden von Nways Manager Remote Monitor zur Umsetzung von Adressen in Namen verwendet. Informationen zur Adreßumsetzung sind im Abschnitt „Stufe der Adreßumsetzung einstellen“ auf Seite 49 enthalten.

Zum Anzeigen dieser Anwendung müssen Sie eine der folgenden Einheiten verwenden:

- Eine RMON2-kompatible Einheit.
- Eine RMON-Einheit, auf der die Software RMON2 (ECAM) SmartAgent geladen ist.

---

### Funktionen

Mit Hilfe der Anwendung "Address Map" können Sie folgendes tun:

- Die Adreß-Map-Tabellen für die aktuelle Einheit anzeigen.
- Die Adreß-Map-Tabelle der Einheit auf doppelte Adressen überprüfen. Dadurch könnte beispielsweise sofort ein Problem im Netzwerkbetrieb erkannt werden, wenn zwei Einheiten dieselbe IP-Adresse aufweisen. Diese Tabelle ist nur dann verfügbar, wenn Sie eine RMON-Einheit verwenden, auf die die Software RMON2 (ECAM) SmartAgent heruntergeladen wurde.

---

## Adreß-Map-Tabellen anzeigen

Gehen Sie zum Anzeigen der Adreß-Map-Tabellen wie folgt vor:

1. Wählen Sie im Menü "Analysis" den Eintrag **Address Map** aus.
2. Wählen Sie einen der Einträge **Address Table** oder **Duplicate Addresses** aus. Adreß-Map-Daten werden daraufhin von der Einheit abgerufen und als Tabelle angezeigt.
3. Klicken Sie die Option **Export** an, um den Inhalt der Tabellen zu exportieren. Dadurch wird das Dialogfenster "Data Export" angezeigt. Weitere Anweisungen sind im Abschnitt „Anwendung Protocol Distribution“ auf Seite 136 enthalten.
4. Klicken Sie zum Schließen der Tabellenanzeige die Option **Close** an.

---

## Adressentabelle

Die Adressentabelle zeigt die Zuordnungen zwischen der MAC-Adresse und der Adresse der Vermittlungsschicht an. Außerdem wird sie für Namensumsetzungen verwendet. Die Anzeige der Tabelle unterscheidet sich, je nachdem, ob Sie eine RMON2-kompatible Sonde oder eine Einheit mit heruntergeladener Software RMON2 (ECAM) SmartAgent verwenden.

---

## Eine RMON2-kompatible Einheit verwenden

Die RMON2-Adreß-Map-Tabelle enthält die folgenden Informationen:

**PhysicalAddress**

Dabei handelt es sich um die MAC-Adresse der Station.

**ProtocolName**

Der Adresstyp.

**NetworkAddress**

Die Netzwerkadresse der Station.

**Interface** Gibt an, welche Schnittstelle zuletzt von dieser Adresse Daten erhalten hat.

**LastChange**

Der Zeitpunkt, an dem dieser Tabelleneintrag zuletzt geändert wurde (seit dem Zeitpunkt, an dem die Einheit zuletzt zurückgesetzt wurde).



---

## Software RMON2 (ECAM) SmartAgent verwenden

Die Adreß-Map-Tabelle der Software RMON2 (ECAM) SmartAgent enthält die folgenden Informationen:

**MacAddress**

Dabei handelt es sich um die MAC-Adresse der Station.

**NetAddrType**

Der Adresstyp.

**ChangeRate**

Jeder Eintrag verfügt über eine Variable für die Änderungsrate, die anzeigt, welche Stationen mehrere Protokolladressen für eine einzige MAC-Adresse aufweisen. Bei Einheiten mit einer hohen Änderungsrate handelt es sich gewöhnlich um Router. Diese werden durch die Angabe RTR= vor der MAC-Adresse gekennzeichnet.

**NetAddress**

Die Netzwerkadresse der Station.

**IsDuplicate**

Listet Stationen auf, bei denen mehreren MAC-Adressen dieselbe Adresse der Vermittlungsschicht zugeordnet wurde. Diese Stationen werden rot markiert. Hierbei handelt es sich gewöhnlich um einen Fehler, der dadurch verursacht wurde, daß jemand zwei Maschinen dieselbe Protokolladresse zugeordnet hat.

**Name**

Der Name der Station.

---

## Tabelle Duplicate Addresses

Diese Tabelle ist nur dann verfügbar, wenn Sie eine RMON-Einheit verwenden, auf die die Software RMON2 (ECAM) SmartAgent heruntergeladen wurde.

Diese Tabelle enthält eine zusammenfassende Liste aller Stationen, die in der Tabelle "Address" als Duplikate gekennzeichnet sind. Mit Hilfe dieser Tabelle sind diese Stationen auf einen Blick zu erfassen.

---

## Anwendung Protocol Distribution

Mit Hilfe der Anwendung "Protocol Distribution" werden die Arten von Datenverkehr angezeigt, die in dem von der ausgewählten Einheit überwachten LAN-Segment auftreten. Mit Hilfe der Anwendung "Protocol Distribution" können Sie folgendes tun:

- Protokollverteilungsdaten in Form einer Tabelle, eines Balkendiagramms oder eines Tortendiagramms anzeigen.
- Den Inhalt eines Diagramms des Typs "Protocol Distribution" in eine Datei oder direkt an den Drucker ausgeben.
- Den Inhalt einer Tabelle des Typs "Protocol Distribution" als Datei im Format ASCII oder CSV in eine andere Anwendung exportieren.

**Achtung:** Zum Anzeigen dieser Anwendung müssen Sie eine der folgenden Einheiten verwenden:

- Eine RMON2-kompatible Einheit.
- Eine RMON-Einheit, auf die die Software RMON2 (ECAM) SmartAgent geladen wurde.

---

## Protokollverteilungsdaten anzeigen

Gehen Sie zum Anzeigen von Protokollverteilungsdaten wie folgt vor:

1. Wählen Sie im Menü "Analysis" zunächst den Eintrag **Protocol Distribution** und anschließend einen der Einträge **Table** oder **Graph** aus. Bei Auswahl des Eintrags "Graph" müssen Sie einen der Diagrammtypen auswählen.
2. Nach einer kurzen Verzögerung werden die Protokollverteilungsdaten von der Einheit geladen und im ausgewählten Format angezeigt.
3. Klicken Sie zum Schließen der Anzeige die Option **Close** an.

---

## Protokollverteilungsdaten verwenden

Mit Hilfe der Anzeige "Protocol Distribution" können Sie folgendes tun:

### Den Inhalt einer Tabellenanzeige exportieren.

Wählen Sie im Menü "Option" die Option **Export** aus. Daten können entweder im Format ASCII oder im Format CSV gesichert werden.

### Den Inhalt einer Diagrammanzeige exportieren.

Wählen Sie im Menü "Option" die Option **Print** aus. Aktivieren Sie die Option **To File**, damit das Diagramm als Postscript-Datei gesichert wird. Weitere Informationen zur Verwendung des Dialogfensters "Print" sind im Abschnitt „Druckvorgaben einstellen“ auf Seite 75 enthalten.

### Diagrammdateien drucken

Wählen Sie im Menü "Option" die Option **Print** aus. Aktivieren Sie die Option **To Printer** und legen Sie die richtigen Druckereinstellungen fest.

### Die angezeigten Daten aktualisieren

Klicken Sie die Option **Update** an.

---

## Anzeigeoptionen

Jede Anzeigeart verfügt über mehrere Optionen. In Tabelle 32 sind die Funktionen aufgeführt, die für die einzelnen Anzeigearten zur Verfügung stehen.

Tabelle 32. Anzeigeoptionen

Anzeigeoptionen	Beschreibung
Export	Mit Hilfe dieser Funktion für tabellarische Darstellungen werden Daten in einer Datei gesichert, so daß sie in andere Anwendungen exportiert oder gedruckt werden können. Die Daten können entweder in einer unstrukturierten Datei im ASCII-Format oder im Dateiformat CSV (Comma Separated Variable) gesichert werden. Bei Auswahl dieser Option wird ein Dialogfenster zum Sichern angezeigt. In diesem Dialogfenster können das Datenformat und der Dateiname angegeben werden.
Print	Diese Funktion für Diagrammdarstellungen ermöglicht, daß Diagramme an einen PostScript-Drucker ausgegeben werden. Bei Auswahl dieser Option wird ein Dialogfenster für die Ausgabe angezeigt. In diesem Dialogfenster können ein Drucker, an den die Daten gesendet werden sollen, oder eine Datei, in der die Daten gesichert werden sollen, sowie das Layout und das Format des Papiers angegeben werden.
Grid On/Off	Mit Hilfe dieser Funktion für Diagrammdarstellungen kann die Darstellung von Rasterlinien in den Diagrammen ein- und ausgeschaltet werden.
Display Style	In Diagrammdarstellungen können die Daten als Balkendiagramm, als Stapelbalkendiagramm oder als Tortendiagramm angezeigt werden. Bei Auswahl einer dieser Optionen wird der Stil der aktuellen Anzeige geändert.

## Anwendung Data Export

Mit Hilfe der Anwendung "Data Export" können Sie eine spezifische RMON-Statistikgruppe auswählen, die Sie anzeigen und in einem der Formate ASCII oder CSV als Datei aus der Einheit exportieren können.

Die folgenden Gruppen sind verfügbar:

<b>Statistics</b>	Ethernet, Token-Ring, FDDI.
<b>History</b>	Ethernet, Token-Ring, FDDI.
<b>Host</b>	Vordefinierte Host-Variablen.
<b>Matrix</b>	Quellen- zu Zieladresse oder Ziel- zu Quellenadresse.

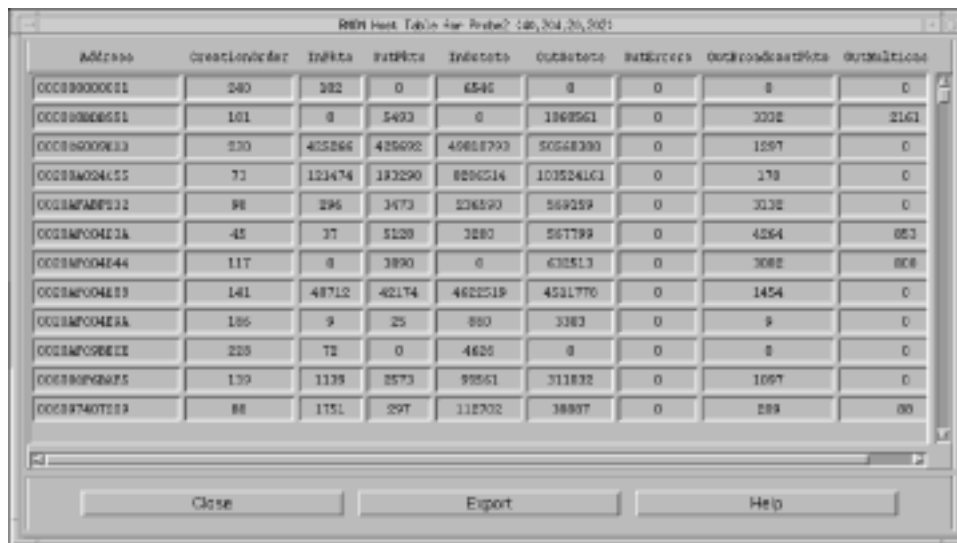
Für die Gruppen "Statistics" und "History" stehen die folgenden Token-Ring-Daten zur Auswahl:

**Token Ring Statistics** Promiscuous, MAC Layer, Source Routing, Ring Station Control und Ring Station Table.

**Token Ring History** Promiscuous und MAC Layer.

Gehen Sie zum Anzeigen von Daten wie folgt vor:

1. Wählen Sie eine Datengruppe aus dem Menü **Export** in der Menüleiste von Nways Manager Remote Monitor aus. Die ausgewählten Daten werden von der Einheit geladen und, wie in Abb. 61 gezeigt, als Tabelle angezeigt.



Address	CreationOrder	InPkts	OutPkts	InErrors	OutErrors	BadPkts	OutBroadcastPkts	OutMulticast
0000000001	240	382	0	6540	0	0	0	0
0000000001	101	0	5403	0	1868561	0	3032	2161
0000000013	230	42286	42502	4061703	5054830	0	1297	0
0000000045	73	121474	183290	820514	103524161	0	178	0
0000000012	98	296	3473	236520	569259	0	3132	0
0000000024	45	37	5128	3280	567799	0	4264	883
0000000044	117	0	3890	0	632513	0	3082	808
0000000018	141	48712	42174	4622519	4531770	0	1454	0
0000000024	186	9	25	880	3383	0	9	0
0000000012	228	72	0	4626	0	0	0	0
0000000025	139	1138	2573	92661	311832	0	1067	0
0000000018	88	1751	297	112702	38807	0	289	80

Abbildung 61. Beispiel für eine Tabelle des Typs "Data Export"

2. Klicken Sie zum Exportieren der in der Tabelle enthaltenen Daten die Option **Export** an. Dadurch wird das Dialogfenster "Data Export" angezeigt. In Abb. 62 wird ein Beispiel für ein Dialogfenster der Anwendung "Data Export" gezeigt.

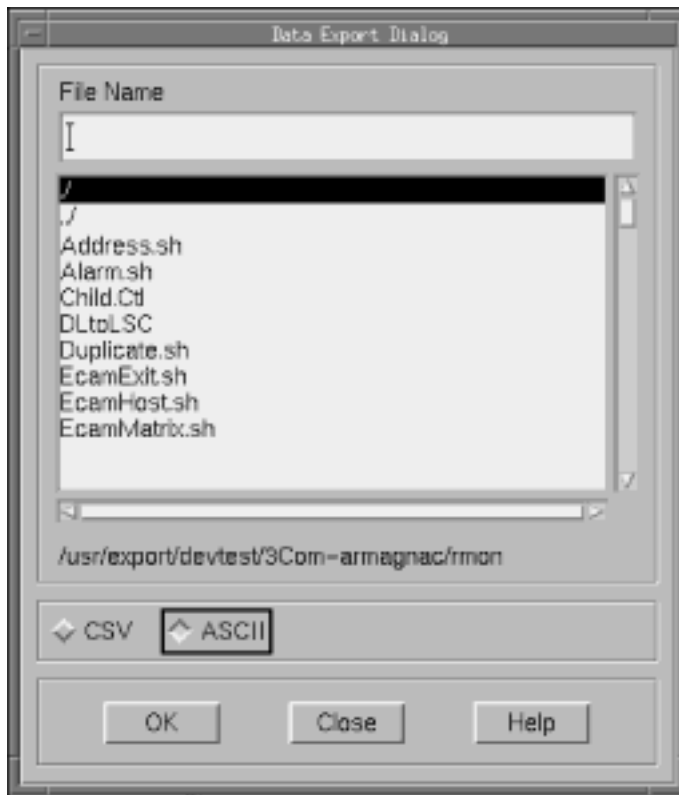


Abbildung 62. Dialogfenster "Data Export"

- a. Geben Sie den Dateinamen ein, und geben Sie den jeweiligen Dateityp an.
  - b. CSV-Dateien können für Berichte im Präsentationsstil und für noch detailliertere Analysen in Datenbanken und Tabellenkalkulationsprogramme eingelesen werden, während ASCII-Dateien in jeden beliebigen Texteditor geladen oder direkt gedruckt werden können.
  - c. Klicken Sie das Feld **OK** an, um die Daten zu exportieren und um zur Tabellenanzeige zurückzukehren.
3. Klicken Sie zum Schließen der Tabellenanzeige die Option **Close** an.

---

## Anwendung Data Collector verwenden

In diesem Abschnitt wird erklärt, wie Sie mit Hilfe der Anwendung "Collector" RMON-Daten von Einheiten im Netzwerk sammeln können.

**Anmerkung:** Die Zugriffsberechtigungen für das Erzeugen und Ändern von Konfigurationen innerhalb der Anwendung "Collector" sind auf eine Benutzer-ID begrenzt.

---

## Anwendung Collector starten

Gehen Sie zum Starten der Anwendung "Collector" wie folgt vor:

1. Wählen Sie den Eintrag **Data Collector** im Menü "Tools" im Hauptfenster von Nways Manager Remote Monitor aus. Öffnen Sie das Hauptdialogfenster der Anwendung "Collector" (siehe Abb. 63).

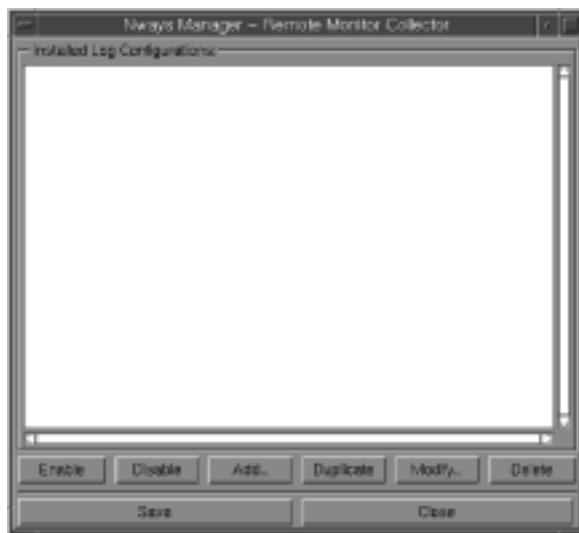


Abbildung 63. Hauptdialogfenster der Anwendung "Collector"

Bevor Sie mit der Datensammlung beginnen können, müssen Sie eine Liste mit Protokollierungspunkten erstellen.

---

## Protokollierungspunkte erstellen

Ein Protokollierungspunkt besteht aus einem Einheitennamen und aus dem Namen und der physischen Nummer jeder Schnittstelle auf der Einheit.

Gehen Sie wie folgt vor, um eine Liste mit Protokollierungspunkten zu erstellen:

1. Klicken Sie im Hauptdialogfenster der Anwendung "Collector" die Option **Add...** an, um das Dialogfenster "Log Configuration Editor" (siehe Abb. 64) zu öffnen.



Abbildung 64. Dialogfenster "Log Configuration Editor"

2. Geben Sie im Feld "Log Name" einen Protokollnamen ein. Unter diesem Namen werden die im Dialogfenster "Log Configuration Editor" erstellten Protokollierungspunkte im Dialogfenster "Installed Log Configurations" angezeigt.
3. Klicken Sie die Option **Update Points...** an, um das Dialogfenster "Device Interrogation Progress" (siehe Abb. 65) anzuzeigen.

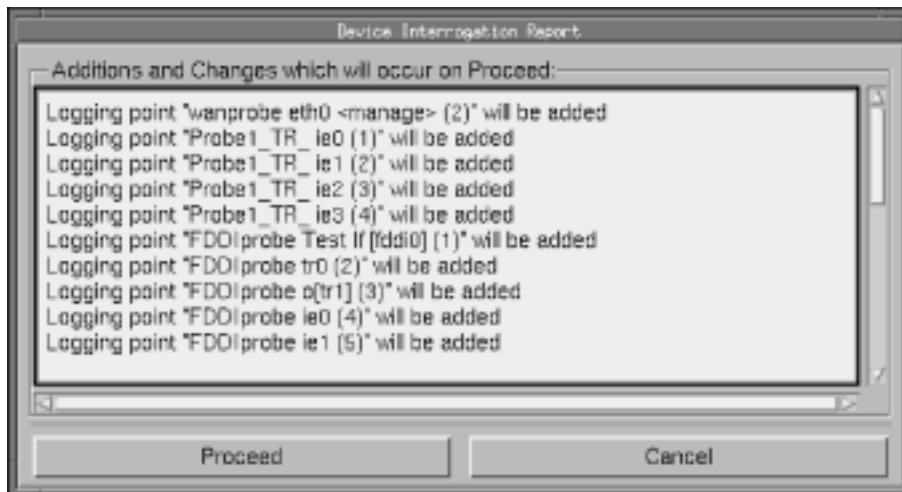


Abbildung 65. Dialogfenster "Device Interrogation Progress"

4. Wählen Sie das Feld **Yes** aus, um den Abfrageprozeß zu starten. Je nach der Anzahl der Einheiten im Netzwerk kann dieser Prozeß einige Minuten in Anspruch nehmen.
5. Die Liste mit Protokollierungspunkten wird erst dann geändert, wenn Sie erneut eine Aktualisierung vornehmen. Der Inhalt der Liste wird dann aktualisiert, indem mit Hilfe der Anwendung "Collector" Einträge mit denen in der Datei probe.map verglichen werden und indem für jede Einheit und für jede Schnittstelle eine neue Abfrage durchgeführt wird.
6. Beim Inhalt der Datei "probe.map" müßte es sich um eine genaue Darstellung des Netzwerks handeln, da diese Datei die von Nways Manager Remote Monitor erstellte Auflistung der Einheiten enthält. Daraus resultiert, daß an der Liste "Available Logging Points" mit Hilfe der Anwendung "Collector" die folgenden Änderungen vorgenommen werden:
  - Wenn eine Einheit oder Schnittstelle nicht mehr in der Datei "probe.map" enthalten ist, wird sie automatisch aus der Liste "Available Logging Points" gelöscht. Wenn Sie beispielsweise eine Einheit aus dem Netzwerk nehmen und sie aus Nways Manager Remote Monitor entfernen, wird diese Einheit bei der nächsten Aktualisierung aus der Liste "Available Logging Points" in der Anwendung "Collector" entfernt.
  - Alle neuen Einträge in der Datei "probe.map" werden der Liste "Available Logging Points" hinzugefügt.



Sobald alle Einheiten von der Anwendung "Collector" verglichen und abgefragt wurden, werden Sie darauf hingewiesen, welche Konfigurationen von Änderungen in der Liste "Available Logging Points" betroffen wären. Eine aus der Liste entfernte Einheit wird auch aus allen Konfigurationen entfernt. Ansonsten werden die Konfigurationen nicht geändert.

7. Klicken Sie zum Implementieren von Änderungen an den Konfigurationen im Dialogfenster "Log Configuration Editor" das Feld **OK** an. Daraufhin kehren Sie zum Hauptdialogfenster der Anwendung "Collector" zurück.
8. Klicken Sie zum Sichern der aktuellen Liste "Available Logging Points" in der Liste "Installed Log Configurations" die Option **Save** an. (Weitere Informationen hierzu sind im Abschnitt „Datensammlung aktivieren“ auf Seite 147 enthalten).

---

## Neue Konfigurationen zur Datensammlung erstellen

Beim Starten der Anwendung "Collector" wird das Hauptdialogfenster der Anwendung geöffnet. In diesem Hauptdialogfenster wird eine Liste mit vorhandenen Konfigurationen (siehe Abb. 63 auf Seite 140) angezeigt. Wenn Sie die Anwendung "Collector" zum ersten Mal verwenden, enthält die Liste noch keine Einträge.

Die über das Hauptdialogfenster verfügbaren Funktionen werden in Tabelle 33 zusammengefasst.

---

*Tabelle 33. Funktionen des Hauptdialogfensters der Anwendung "Collector"*

<b>Funktion</b>	<b>Beschreibung</b>
Enable	Aktiviert die Datensammlung für ausgewählte Konfigurationen bei der nächsten Sicherung.
Disable	Beendet die Datensammlung für ausgewählte Konfigurationen bei der nächsten Sicherung.
Add	Erstellt eine neue Konfiguration.
Duplicate	Kopiert eine oder mehrere ausgewählte Konfigurationen.
Modify	Bearbeitet eine ausgewählte Konfiguration.
Delete	Löscht eine oder mehrere ausgewählte Konfigurationen.
Save	Sichert Änderungen in der Anwendung "Collector" und aktualisiert cron-Eintrag, um die Datensammlung zu starten.
Close	Verläßt die Anwendung "Collector" mit der Auswahlmöglichkeit, die vorgenommenen Änderungen zu sichern oder nicht zu sichern.

## Eine neue Konfiguration für die Anwendung "Collector" hinzufügen

1. Klicken Sie die Option **Add...** an, um das in Abb. 64 auf Seite 141 gezeigte Dialogfenster "Log Configuration Editor" zu öffnen.
2. Geben Sie im Feld "Log Name" einen Namen für diese Datensammlung ein.
3. Die Liste "Selected Logging Points" enthält die gegenwärtig ausgewählten Schnittstellen und Einheiten.
  - a. Gehen Sie zum Hinzufügen von Einträgen aus der Liste "Available Logging Points" wie folgt vor:
    - Wählen Sie einen Eintrag durch Anklicken aus.
    - Halten Sie beim Anklicken von Einträgen in der Liste die **Steuertaste** gedrückt, um mehrere Einträge auszuwählen.
    - Klicken Sie die Option **Add** an.
    - Klicken Sie die Option **Add All** an, um alle verfügbaren Einheiten hinzuzufügen.
    - Gehen Sie zum Entfernen von Einträgen aus der Liste "Selected Logging Points" wie folgt vor:
      - Wählen Sie einen Eintrag durch Anklicken aus.
      - Halten Sie beim Anklicken von Einträgen in der Liste die **Steuertaste** gedrückt, um mehrere Einträge auszuwählen.
      - Klicken Sie die Option **Remove** an.
  - b. Klicken Sie die Option **Remove All** an, um alle verfügbaren Einheiten zu entfernen.
  - c. Klicken Sie zum Aktualisieren der Liste "Available Logging Points" die Option **Update Points...** an. Dieser Prozeß kann einige Zeit in Anspruch nehmen und Auswirkungen auf andere Konfigurationen haben. (Weitere Informationen hierzu sind im Abschnitt „Protokollierungspunkte erstellen“ auf Seite 141 enthalten.)
4. Wählen Sie aus, welche Daten protokolliert werden sollen: Protokoll-, Host- und/oder Matrixdaten.

Protokolldaten werden nur von den Einheiten gesammelt, für die Sie vorher in Nways Manager Remote Monitor eine Anzeige "History" (Protokollanzeige) eingerichtet haben. Weitere Informationen hierzu sind im Abschnitt „Anzeige History verwenden“ auf Seite 92 enthalten.
5. Wählen Sie für die Datenprotokollierung ein Zeitintervall aus. Standardmäßig ist das Protokollintervall (Log Interval) auf eine tägliche Sammlung eingestellt.
6. Verwenden Sie im Dialogfenster im Bereich "Next Collection At" die Zeitleiste, um die genaue Zeit einzustellen, zu der die Sammlung stattfinden soll.

Bei einer einmal täglich stattfindenden Sammlung können Sie die genaue Minute angeben, in der die Sammlung beginnen soll; bei Protokollintervallen von mehr als

einem Tag können Sie sowohl den Tag als auch die Minute für den Start der Sammlung angeben.

**Achtung:** Sie sollten zu keiner Zeit mehr als eine Datensammlung durchführen. Beim Sammelprozeß werden die Daten an allgemeine (nicht an eindeutige) Dateien geschrieben. Wenn mehrere Datensammlungen zur selben Zeit durchgeführt werden, kann dies zu einer Interferenz zwischen den Prozessen führen. Dadurch würden die Daten der Sammlungen ungültig werden.

Wählen Sie eine der folgenden Möglichkeiten zum Einstellen einer neuen Zeit aus:

- Klicken Sie die Schiebeleiste an, und ziehen Sie sie nach links oder nach rechts.
- Klicken Sie einen beliebigen Punkt auf der Schiebeleiste mit der mittleren Maustaste an — dadurch wird der Schiebeknopf auf diesen Punkt versetzt.
- Klicken Sie einen beliebigen Punkt auf der Schiebeleiste mit der linken Maustaste an, und halten Sie die Maustaste gedrückt — dadurch bewegt sich der Schiebeknopf zu diesem Punkt hin.

Während der Schiebeknopf versetzt wird, wird der angezeigte Zeitpunkt für die Sammlung aktualisiert.

7. Klicken Sie das Feld **OK** an, um die Änderungen zu bestätigen und zum Hauptdialogfenster der Anwendung "Collector" zurückzukehren. Durch Anklicken der Option **Cancel** werden alle an der Konfiguration vorgenommenen Änderungen ungültig.

Die neue Konfiguration für die Datensammlung wird im Hauptdialogfenster in der Liste "Installed Log Configurations" angezeigt.

8. Zum Starten von Datensammlung für eine Konfiguration müssen die Änderungen in der Anwendung "Collector" gesichert werden. Weitere Informationen sind in den Abschnitten „Datensammlungen aktivieren und inaktivieren“ auf Seite 147 und „Datensammlung aktivieren“ auf Seite 147 enthalten.

## Konfigurationen kopieren und ändern

Eine weitere Möglichkeit zum Erstellen einer neuen Konfiguration besteht darin, eine vorhandene Konfiguration zu kopieren und dann zu ändern. Gehen Sie dazu wie folgt vor:

1. Wählen Sie eine oder mehrere Konfigurationen für die Datensammlung aus der Liste "Installed Log Configurations" aus, und klicken Sie die Option **Duplicate** an, um eine Kopie der ausgewählten Konfigurationen zu erstellen. Duplikate werden durch Anführungszeichen am Ende des Protokollnamens gekennzeichnet.
2. Wählen Sie eine doppelt vorhandene Konfiguration aus, und klicken Sie die Option **Modify...** an, um das Dialogfenster "Log Configuration Editor" zu öffnen.
3. Befolgen Sie die Anweisungen im Abschnitt „Eine neue Konfiguration für die Anwendung "Collector" hinzufügen“ auf Seite 144, um beliebige Einzeldaten der doppelt vorhandenen Konfiguration zu ändern.
4. Klicken Sie das Feld **OK** an, um die Änderungen zu bestätigen und zum Dialogfenster "Collector Configuration" zurückzukehren. Durch Anklicken der Option **Cancel** werden alle an der Konfiguration vorgenommenen Änderungen ungültig.

Die geänderte Konfiguration für die Datensammlung wird im Hauptdialogfenster in der Liste "Installed Log Configurations" angezeigt.

Zum Starten der Datensammlung für eine Konfiguration müssen die Änderungen in der Anwendung "Collector" gesichert werden. Weitere Informationen sind in den Abschnitten „Datensammlungen aktivieren und inaktivieren“ auf Seite 147 und „Datensammlung aktivieren“ auf Seite 147 enthalten.

## Konfigurationen löschen

Es ist auch möglich, jede beliebige Konfiguration zu löschen, die Sie erstellt haben.

Wenn Sie einen Fehler begehen, indem Sie z. B. die falsche Konfiguration löschen, haben Sie die Möglichkeit, die Anwendung zu verlassen, ohne die Änderungen zu sichern. Wenn Sie die Anwendung "Collector" erneut öffnen, wird die Liste mit Konfigurationen auf den Stand vor der letzten Sicherung zurückgesetzt. Allerdings gehen alle Änderungen verloren, die Sie nach dieser letzten Sicherung vorgenommen haben.

1. Wählen Sie eine oder mehrere Konfigurationen für die Datensammlung aus der Liste "Installed Log Configurations" aus.
2. Klicken Sie die Option **Delete** an.

## Datensammlungen aktivieren und inaktivieren

Durch die Anwendung "Collector" wird Ihnen ermöglicht, eine beliebige Anzahl von Datensammlungen zu definieren. Dabei werden einige Datensammlungen sofort aktiviert, während andere so lange inaktiviert bleiben, bis sie benötigt werden.

### Datensammlungen aktivieren

Beim Hinzufügen von neuen Datensammlungen zur Liste "Installed Log Configurations" werden diese standardmäßig sofort aktiviert. Doppelt vorhandene Konfigurationen werden standardmäßig inaktiviert. Eine aktivierte Konfiguration für die Datensammlung wird durch das Präfix '>>' gekennzeichnet.

Gehen Sie zum Aktivieren einer gegenwärtig inaktiven Konfiguration wie folgt vor:

1. Wählen Sie den betreffenden Eintrag aus der Liste "Installed Log Configurations" aus.
2. Klicken Sie zum Aktivieren der ausgewählten Datensammlung die Option **Enable** aus.

### Datensammlungen inaktivieren

Gehen Sie zum Inaktivieren einer Konfiguration für die Datensammlung wie folgt vor:

1. Wählen Sie die Datensammlung, die inaktiviert werden soll, aus der Liste "Installed Log Configurations" aus.
2. Klicken Sie zum Inaktivieren der ausgewählten Datensammlung die Option **Disable** aus. Das Präfix '>>', das den aktivierten Status des Datensammlungseintrags kennzeichnet, wird entfernt.

## Datensammlung aktivieren

In der Liste "Installed Log Configurations" werden alle Konfigurationen angezeigt, die Sie erstellt haben. Indem Sie die gesamte Konfiguration der Anwendung "Collector" sichern, wird die Datensammlung für alle aktivierten Konfigurationen aktiviert.

- Wenn Sie die Option **Save** oder die Option **Quit** und dann **Save Settings Before Quitting** auswählen, wird von der Anwendung "Collector" für jede aktivierte Konfiguration für die Datensammlung in der Datei crontab ein Eintrag erstellt. Zum angegebenen Zeitpunkt wird von cron das Programm zur Datensammlung ausgeführt.
- Wenn Sie erst die Option **Quit** und anschließend die Option **Quit without Saving** auswählen, gehen alle in der Anwendung "Collector" seit der letzten Sicherung vorgenommenen Änderungen verloren.

## CSV-Dateien

Durch die Anwendung "Collector" werden gesammelte Daten in Dateien im CSV-Format im Verzeichnis `/usr/LANReMon/rmon/LOGDIR` gespeichert. Wenn neue Sammlungen durchgeführt werden, werden neue Daten zu den vorhandenen Dateien hinzugefügt.

In Tabelle 34 sind die dabei erstellten Dateien aufgeführt.

*Tabelle 34. CSV-Dateien*

<b>Dateiname</b>	<b>Beschreibung</b>
hist.csv	Ethernet-Protokolldaten
host.csv	Host-Daten
matrix.csv	Matrixdaten
trml.csv	Token-Ring-Protokolldaten der MAC-Schicht
trp.csv	Token-Ring-Promiscuous-Protokolldaten
fddihist.csv	FDDI-Protokolldaten

Die Größe der CSV-Dateien im Verzeichnis `/usr/LANReMon/rmon/LOGDIR` hängt von der Menge der gesammelten Daten ab. Wenn Sie häufig Sammlungen von großen Datenmengen von vielen Einheiten im Netzwerk durchführen, wird die Größe der CSV-Dateien schnell zunehmen.

---

## Anhang A. Integration von NetView für AIX

In diesem Anhang wird folgendes beschrieben:

- Sonden in IBM NetView einrichten
- RMON-Anwendungen in IBM NetView verwenden

IBM NetView muß installiert worden sein, bevor Nways Manager Remote Monitor installiert wird. Während der Installation findet automatisch eine Integration zwischen Nways Manager Remote Monitor und IBM NetView statt.

Durch die Integration mit NetView können Sie RMON-Einheiten, wie z. B. die IBM RMON-Sonde, in IBM NetView einrichten und anschließend statistische Informationen zum überwachten Segment entweder in einer grafischen oder in einer tabellarischen Darstellung anzeigen.

Außerdem kann über NetView auf alle Funktionen von Nways RMON zugegriffen werden. Dadurch können von NetView aus Anwendungen wie "Packet Capture" und "Decode" verwendet werden.

---

### Sonden in IBM NetView einrichten

Innerhalb von IBM NetView sollte jede Sonde wie folgt für das Segment eingerichtet werden, das sie überwacht:

1. Beim Starten von IBM NetView hat das Erkennungsprogramm möglicherweise die ausgewählte Sonde gefunden und sie als ein generisches Computerobjekt in die Map eingefügt. In diesem Fall muß die Symbolklasse "Net Device" möglicherweise wie folgt in "Analyzer" geändert werden:
  - a. Wählen Sie das Objekt in der Abbildung aus.
  - b. Klicken Sie auf der Menüleiste mit der rechten Maustaste die Option **Change Symbol Type** an.
  - c. Stellen Sie die Symbolklasse "Net Device" auf *Analyzer* ein.
  - d. Stellen Sie die Objektattribute der Sonde wie in Schritt 3 auf Seite 150 beschrieben ein.
2. Falls die IBM Sonden noch nicht erkannt worden sind, müssen Sie den Befehl "ping" verwenden, um die Verbindung der Sonden zum Netzwerk zu überprüfen. Gewöhnlich wird nach einer kurzen Zeit in der Map eine Einheit zur Netzwerkanalyse (die eine IBM Sonde bezeichnet) angezeigt. Wenn die Sonde nicht angezeigt wird, können Sie sie wie folgt manuell hinzufügen:
  - a. Wählen Sie in der Menüleiste die Option **Edit** aus.
  - b. Wählen Sie die Menüoption **Add Object** aus.
  - c. Wählen Sie die Symbolklasse "Net Device" aus.

- d. Wählen Sie einen Analyzer aus, ziehen Sie ihn mit der mittleren Maustaste über die Map, und übergeben Sie ihn.  
Daraufhin wird ein Dialogfenster angezeigt, in dem Sie den der Sonde zugeordneten Namen definieren können. Dabei sollte es sich um den Namen handeln, der in der Systemdatei "/etc/hosts" definiert wurde.
  - e. Stellen Sie die Objektattribute der Sonde wie in Schritt 3 beschrieben ein.
3. Gehen Sie wie folgt vor, um die Objektattribute der Sonde einzustellen:
    - a. Klicken Sie auf der Menüleiste mit der rechten Maustaste die Option **Describe/Modify Object** an. Die folgenden drei Kategorien können eingestellt werden: Capabilities, General Attributes und IP Map.
    - b. Klicken Sie den Eintrag **IP Map** doppelt an, und geben Sie den in der Systemdatei "/etc/hosts" angegebenen Hostnamen ein. Drücken Sie die **Rückschritta**ste, damit die IP-Adresse des Host angezeigt wird. Überprüfen Sie, ob es sich um die richtige Adresse und nicht um eine doppelt vorhandene IP-Adresse handelt. Klicken Sie dann das Feld **OK** an, um die neue Einstellung im Feld "IP Map" zu sichern.
    - c. Klicken Sie den Eintrag **General Attributes** doppelt an, und stellen Sie die Markierung *SNMPSupported* auf **true** ein.
    - d. Wählen Sie aus dem Aktionsfenstermenü "SNMPAgent" eine Einheit für Nways Manager Remote Monitor aus. Wählen Sie als Hersteller (vendor) **IBM** aus.
    - e. Klicken Sie das Feld **OK** an, um die neue Einstellung für den Eintrag "General Attributes" zu sichern.
    - f. Klicken Sie den Eintrag **Capabilities** doppelt an und überprüfen Sie, ob die Markierungen *isAnalyzer* und *isSNMPSupported* beide auf **true** eingestellt sind. Überprüfen Sie anschließend, ob die Informationen zu SNMPAgent und zum Hersteller richtig definiert wurden. Wenn eine der beiden Markierungen nicht gesetzt wurde, sollte der Eintrag **General Attributes** erneut definiert werden.

---

## RMON-Anwendungen in IBM NetView verwenden

Sobald die Einrichtung der Sonden abgeschlossen ist, können Sie Netzwerkstatistiken für die überwachten Segmente anzeigen. Hierzu können Sie die Diagramme von IBM NetView und von Nways Manager Remote Monitor verwenden. Die gesamte von Nways Manager Remote Monitor gebotene Funktionalität kann über IBM NetView gestartet werden.



---

## Anwendungen von Nways Manager Remote Monitor starten

Gehen Sie wie folgt vor, um auf Anwendungen von Nways Manager Remote Monitor zuzugreifen:

1. Wählen Sie eine Sonde aus.
2. Wählen Sie im Hauptmenü den Eintrag "Monitor" aus.
3. Wählen Sie Nways Manager Remote Monitor aus.
4. Wählen Sie eine der Menüoptionen von Nways Manager Remote Monitor aus:

**IBM Tools** Mit dieser Menüoption können Sie alle Anwendungen von Nways Manager Remote Monitor ausführen. Sie können sie einzeln ausführen, indem Sie Anwendungen wie "RMON Segment Statistics", "RMON History View" usw. auswählen, oder Sie können sie zusammen auswählen, indem Sie die Option "RMON Summary Viewport" auswählen, wodurch das Hauptfenster angezeigt wird.

### **NetView Tools**

Über diese Menüoption können verschiedene Diagramme und Tabellen angezeigt werden, die aktuelle von der Sonde erfaßte Informationen enthalten. Diese Menüoptionen sind sowohl für Ethernet als auch für Token-Ring verfügbar. In der Tabelle unten werden sie im einzelnen beschrieben.

### **Stop RMON Tools**

Dient zum Verlassen aller gerade aktiven NetView-Tools.

5. Wenn Sie zu IBM NetView zurückkehren, können Sie entweder das Darstellungsfeld auf Symbolgröße verkleinern, wobei es aktiv bleibt, damit Sie es schnell starten können, wenn Sie es erneut benötigen, oder Sie können den Knopf "Exit" im Hauptdarstellungsfeld verwenden, um Nways Manager Remote Monitor zu beenden.

## NetView Tools

In Tabelle 35 sind die im Menü "NetView Tools" verfügbaren Optionen aufgeführt.

<i>Tabelle 35. Optionen der NetView-Tools</i>	
<b>Optionen</b>	<b>Beschreibung</b>
Ethernet Packet Size Distribution	Die Verteilung des Datenverkehrs für verschiedene Paketgrößen in einem Ethernet-Segment wird grafisch dargestellt.
Ethernet Segment Statistics	Statistiken für verschiedene Pakettypen, einschließlich verschiedener Typen von Fehlerpaketen, Kollisionen, Rundsendungen usw., werden grafisch dargestellt. Diese Option ist nur für Ethernet-Segmente verfügbar.
Token-Ring Packet Size Distribution	Die Verteilung des Datenverkehrs für verschiedene Paketgrößen in einem Token-Ring-Segment wird grafisch dargestellt.
Token-Ring Packet Rate	Statistiken für die LLC-Pakete und die MAC-Pakete werden grafisch dargestellt, und die Rate an gelöschten Ereignissen für ein Token-Ring-Segment wird angezeigt.
Token-Ring MAC Error Rates	Statistiken für verschiedene Fehlertypen in einem Token-Ring-Segment werden grafisch dargestellt. Dies schließt z. B. Informationen wie die Anzahl der Beacon-Pakete oder der Überlastungsfehler ein, die möglicherweise aufgetreten sind.
Token-Ring Routing Statistics	Statistiken zu Leitweginformationen für ein Token-Ring-Segment werden grafisch dargestellt. Dies schließt Informationen zu lokalen LLC-Rahmen, weitergeleiteten Rahmen und SRB-Paketen (Single Route Broadcast) usw. ein.
Token-Ring Hop Statistics	Statistiken für Rahmen, die über mehrere Token-Ring-Segmente geleitet wurden, werden grafisch dargestellt. Dabei werden Statistiken für Pakete mit einer unterschiedlichen Anzahl von Hops angezeigt.
Host Table by Selected Station	Eine Tabelle mit allen Hosts, die von der ausgewählten Sonde gesehen wurden, wird angezeigt. Über diese Tabelle können Sie jeden beliebigen Host auswählen, indem Sie mit der linken Maustaste ein beliebiges Feld in der entsprechenden Zeile anklicken. Dadurch wird ein NetView-Diagramm aufgerufen, in dem die aktuellen Statistiken zu den von diesem Host gesendeten und zu den von diesem Host empfangenen Paketen angezeigt werden. Diese Option ist sowohl für Ethernet- als auch für Token-Ring-Sonden verfügbar.
Matrix Table by Selected Station	Eine Tabelle mit dem gesamten Datenaustausch, der von der ausgewählten Sonde gesehen wurde, wird angezeigt. Sie können jeden beliebigen Datenaustausch zwischen zwei bestimmten Einheiten auswählen, indem Sie mit der linken Maustaste die betreffende Zeile anklicken. Daraufhin wird ein NetView-Diagramm aufgerufen, das den Datenaustausch zwischen den beiden Einheiten anzeigt. Diese Option ist sowohl für Ethernet- als auch für Token-Ring-Sonden verfügbar.

---

## Anhang B. Integration von OpenView

In diesem Anhang wird folgendes beschrieben:

- Sonden in HP OpenView einrichten
- RMON-Anwendungen in HP OpenView verwenden

HP OpenView muß installiert worden sein, bevor Nways Manager Remote Monitor installiert wird. Während der Installation findet automatisch eine Integration zwischen Nways Manager Remote Monitor und HP OpenView statt.

Durch die Integration mit OpenView können Sie RMON-Einheiten, wie z. B. die IBM RMON-Sonde, in HP OpenView einrichten und anschließend statistische Informationen zum überwachten Segment entweder in einer grafischen oder in einer tabellarischen Darstellung anzeigen.

Außerdem kann über OpenView auf die gesamte Funktionalität von Nways Manager Remote Monitor zugegriffen werden. Dadurch können über von OpenView aus Anwendungen wie "Packet Capture" und "Decode" verwendet werden.

---

### Sonden in HP OpenView einrichten

Innerhalb von HP OpenView sollte jede Sonde wie folgt für das Segment eingerichtet werden, das sie überwacht:

1. Beim Starten von HP OpenView hat das Erkennungsprogramm möglicherweise die ausgewählte Sonde gefunden und sie als ein generisches Computerobjekt in die Map eingefügt. In diesem Fall muß die Symbolklasse "Net Device" möglicherweise wie folgt in "Analyzer" geändert werden:
  - a. Wählen Sie das Objekt in der Map aus.
  - b. Klicken Sie auf der Menüleiste mit der rechten Maustaste die Option **Change Symbol Type** an.
  - c. Stellen Sie die Symbolklasse "Net Device" auf **Analyzer** ein.
  - d. Stellen Sie die Objektattribute der Sonde wie in Schritt 3 auf Seite 154 beschrieben ein.
2. Falls die IBM Sonden noch nicht erkannt worden sind, müssen Sie den Befehl "ping" verwenden, um die Verbindung der Sonden zum Netzwerk zu überprüfen. Gewöhnlich wird nach einer kurzen Zeit in der Map eine Einheit zur Netzwerkanalyse (die eine IBM Sonde bezeichnet) angezeigt. Wenn die Sonde nicht angezeigt wird, können Sie sie wie folgt manuell hinzufügen:
  - a. Wählen Sie in der Menüleiste die Option **Edit** aus.
  - b. Wählen Sie die Menüoption **Add Object** aus.
  - c. Wählen Sie die Symbolklasse "Net Device" aus.

- d. Wählen Sie einen Analyzer aus, ziehen Sie ihn mit der mittleren Maustaste über die Map, und übergeben Sie ihn.  
Daraufhin wird ein Dialogfenster angezeigt, in dem Sie den der Sonde zugeordneten Namen definieren können. Dabei sollte es sich um den Namen handeln, der in der Systemdatei "/etc/hosts" definiert wurde.
  - e. Stellen Sie die Objektattribute der Sonde wie in Schritt 3 beschrieben ein.
3. Gehen Sie wie folgt vor, um die Objektattribute der Sonde einzustellen:
    - a. Klicken Sie auf der Menüleiste mit der rechten Maustaste die Option **Describe/Modify Object** an.  
Die folgenden drei Kategorien können eingestellt werden: Capabilities, General Attributes und IP Map.
    - b. Klicken Sie den Eintrag **IP Map** doppelt an, und geben Sie den in der Systemdatei "/etc/hosts" angegebenen Hostnamen ein. Drücken Sie die **Rückschrit-aste**, damit die IP-Adresse des Host angezeigt wird. Überprüfen Sie, ob es sich um die richtige Adresse und nicht um eine doppelt vorhandene IP-Adresse handelt. Klicken Sie dann das Feld **OK** an, um die neue Einstellung im Feld "IP Map" zu sichern.
    - c. Klicken Sie den Eintrag **General Attributes** doppelt an, und stellen Sie die Markierung *SNMPSupported* auf **true** ein.
    - d. Wählen Sie aus dem Aktionsfenstermenü "SNMPAgent" eine Einheit von Nways Manager Remote Monitor aus. Wählen Sie als Hersteller (vendor) **IBM** aus.
    - e. Klicken Sie das Feld **OK** an, um die neue Einstellung für den Eintrag "General Attributes" zu sichern.
    - f. Klicken Sie den Eintrag **Capabilities** doppelt an und überprüfen Sie, ob die Markierungen *isAnalyzer* und *isSNMPSupported* beide auf **true** eingestellt sind. Überprüfen Sie anschließend, ob die Informationen zu SNMPAgent und zum Hersteller richtig definiert wurden. Wenn eine der beiden Markierungen nicht gesetzt wurde, sollte der Eintrag **General Attributes** erneut definiert werden.

---

## RMON-Anwendungen in HP OpenView verwenden

Sobald die Einrichtung der Sonden abgeschlossen ist, können Sie Netzwerkstatistiken für die überwachten Segmente anzeigen. Hierzu können Sie die Diagramme von HP OpenView und Nways Manager Remote Monitor verwenden. Die gesamte von Nways Manager Remote Monitor gebotene Funktionalität kann über HP OpenView gestartet werden.

---

## Anwendungen von Nways Manager Remote Monitor starten

Gehen Sie wie folgt vor, um auf Anwendungen von Nways Manager Remote Monitor zuzugreifen:

1. Wählen Sie eine Sonde aus.
2. Wählen Sie im Hauptmenü den Eintrag "Monitor" aus.
3. Wählen Sie Nways Manager Remote Monitor aus.
4. Wählen Sie eine der Menüoptionen von Nways Manager Remote Monitor aus:

**IBM Tools** Mit dieser Menüoption können Sie alle Anwendungen von Nways Manager Remote Monitor ausführen. Sie können sie einzeln ausführen, indem Sie Anwendungen wie "RMON Segment Statistics", "RMON History View" usw. auswählen, oder Sie können sie zusammen auswählen, indem Sie die Option "RMON Summary Viewport" auswählen, wodurch das Hauptfenster angezeigt wird.

### **OpenView Tools**

Über diese Menüoption können verschiedene Diagramme und Tabellen angezeigt werden, die aktuelle von der Sonde erfaßte Informationen enthalten. Diese Menüoptionen sind sowohl für Ethernet als auch für Token-Ring verfügbar. In der Tabelle der OpenView-Tools unten werden sie im einzelnen beschrieben.

### **Stop RMON Tools**

Dient zum Verlassen aller gerade aktiven Tools von Nways Manager Remote Monitor.

5. Wenn Sie zu HP OpenView zurückkehren, können Sie entweder das Darstellungsfeld auf Symbolgröße verkleinern, wobei es aktiv bleibt, damit Sie es schnell starten können, wenn Sie es erneut benötigen, oder Sie können den Knopf "Exit" im Hauptdarstellungsfeld verwenden, um Nways Manager Remote Monitor zu beenden.

## OpenView-Tools

In Tabelle 36 sind die im Menü "OpenView Tools" verfügbaren Optionen aufgeführt.

<i>Tabelle 36. Optionen der OpenView-Tools</i>	
<b>Optionen</b>	<b>Beschreibung</b>
Ethernet Packet Size Distribution	Die Verteilung des Datenverkehrs für verschiedene Paketgrößen in einem Ethernet-Segment wird grafisch dargestellt.
Ethernet Segment Statistics	Statistiken für verschiedene Pakettypen, einschließlich verschiedener Typen von Fehlerpaketen, Kollisionen, Rundsendungen usw., werden grafisch dargestellt. Diese Option ist nur für Ethernet-Segmente verfügbar.
Token-Ring Packet Size Distribution	Die Verteilung des Datenverkehrs für verschiedene Paketgrößen in einem Token-Ring-Segment wird grafisch dargestellt.
Token-Ring Packet Rate	Statistiken für die LLC-Pakete und die MAC-Pakete werden grafisch dargestellt, und die Rate an gelöschten Ereignissen für ein Token-Ring-Segment wird angezeigt.
Token-Ring MAC Error Rates	Statistiken für verschiedene Fehlertypen in einem Token-Ring-Segment werden grafisch dargestellt. Dies schließt z. B. Informationen wie die Anzahl der Beacon-Pakete oder der Überlastungsfehler ein, die möglicherweise aufgetreten sind.
Token-Ring Routing Statistics	Statistiken zu Leitweginformationen für ein Token-Ring-Segment werden grafisch dargestellt. Dies schließt Informationen zu lokalen LLC-Rahmen, weitergeleiteten Rahmen und SRB-Paketen (Single Route Broadcast) usw. ein.
Token-Ring Hop Statistics	Statistiken für Rahmen, die über mehrere Token-Ring-Segmente weitergeleitet wurden, werden grafisch dargestellt. Dabei werden Statistiken für Pakete mit einer unterschiedlichen Anzahl von Hops angezeigt.
Host Table by Selected Station	Eine Tabelle mit allen Hosts, die von der ausgewählten Sonde gesehen wurden, wird angezeigt. Über diese Tabelle können Sie jeden beliebigen Host auswählen, indem Sie mit der linken Maustaste ein beliebiges Feld in der entsprechenden Zeile anklicken. Dadurch wird ein NetView-Diagramm aufgerufen, in dem die aktuellen Statistiken zu den von diesem Host gesendeten und zu den von diesem Host empfangenen Paketen angezeigt werden. Diese Option ist sowohl für Ethernet- als auch für Token-Ring-Sonden verfügbar.
Matrix Table by Selected Station	Eine Tabelle mit dem gesamten Datenaustausch, der von der ausgewählten Sonde gesehen wurde, wird angezeigt. Sie können jeden beliebigen Datenaustausch zwischen zwei bestimmten Einheiten auswählen, indem Sie mit der linken Maustaste die betreffende Zeile anklicken. Daraufhin wird ein NetView-Diagramm aufgerufen, die den Datenaustausch zwischen den beiden Einheiten anzeigt. Diese Option ist sowohl für Ethernet- als auch für Token-Ring-Sonden verfügbar.

---

## Anhang C. Liste der Protokolle und Protokollentschlüsselungen

In diesem Anhang werden die Protokollentschlüsselungen aufgeführt, die für die RMON-Anzeigen und ECAM-Anwendungen unterstützt werden.

---

### Entschlüsselungen für RMON-Anwendungen

*Tabelle 37. Liste mit unterstützten Protokollentschlüsselungen für die einzelnen Protokollfamilien*

Protokollfamilie	Protokoll
AppleTalk	AARP, ADSP, AEP, AFP, ASP, ATP, DDP, MacIP, MacIP config, 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 (Phrase 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 über TP4
LAN Manager	NetBEUI, NetBIOS, SMB.
LAN Encapsulations	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.

---

### Entschlüsselungen für ECAM-Anwendungen

In diesem Abschnitt werden die Protokolle aufgeführt, die von der Software RMON2 (ECAM) SmartAgent Version 0.21. unterstützt werden. Die Protokolle wurden in zwei Gruppen unterteilt, damit folgendes gezeigt werden kann:

- Die Protokolle, die nur einer Protokollfamilie zugeordnet sind.
- Alle Kapselungen von Protokollen, die mehr als einer Protokollfamilie zugeordnet sind.

**Anmerkung:** Zur besseren Übersichtlichkeit wird jedes Protokoll nur einmal aufgeführt.

Tabelle 38 (Seite 1 von 2). Protokolle, die nur einer Protokollfamilie zugeordnet sind

Protokollfamilie	Protokoll	Beschreibung
Apple Talk 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 Kopfformate
	DDP2	AppleTalk Datagram Delivery Protocol - lange Kopfformate
	NBP	AppleTalk Name Binding Protocol
	RTMP ZIP	AppleTalk Routing Table Maintenance Protocol AppleTalk Zone Information Protocol
Banyan VINES	VINES	Gesamterfassungsgruppe Banyan VINES Internet Protocol
	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
DECnet	DEC	Gesamterfassungsgruppe DECnet*
	DRP	DECnet (Phase IV) Routing Protocol
	LANBridge	Bridge Managing Protocol von Digital
	LAT	DECnet Local Area Transport Protocol
	LAVC/SCA	Local Area Vax Cluster/System Communication Architecture
	MOP PathWorks	DECnet Maintenance Operations Protocol PC to Digital Server Protocol
IBM SNA	SNA	Gesamterfassungsgruppe Systems Network Architecture*
	SNA (Daten)	Endbenutzer- und Netzservicesdaten von SNA
	SNA (Flußsteuerung)	Datenflußsteuerung von SNA
	SNA (Netzsteuerung)	Netzsteuerung von SNA
	SNA (Sitzungssteuerung)	Sitzungssteuerung von SNA



Tabelle 38 (Seite 2 von 2). Protokolle, die nur einer Protokollfamilie zugeordnet sind

Protokollfamilie	Protokoll	Beschreibung
LAN Manager	NetBIOS/NETBEUI	Network Basic Input/Output System
NetWare	IPX NetBIOS/IPX NCP RIP SAP SPX	Internet Packet Exchange IPX-Implementierungen von NetBIOS NCP Netware Core Protocol Routing Information Protocol Service Advertising Protocol Sequenced Packet Exchange
TCP/IP	AFS  ARP DNS FTP GOPHER ICMP IGRP IP LPR/LPD NetBIOS/IP (Datenpaket) NetBIOS/IP (Name) NetBIOS/IP (Sitzung) NeWS NFS NNTP NTP OSPF RCMD REXEC RLOGIN Router RWHO SMTP SOCKS SUNPRC TCP TELNET TFTP UDP WWW X	Andrew File System  Address Resolution Protocol Domain Name Service Protocol File Transfer Protocol Internet-Dokumentensuche und -Abruf Internet Control Message Protocol Inter-Gateway Routing Protocol Internet Protocol* Drucker Datenpaketunterstützung von NetBIOS  Namensunterstützung von NetBIOS  Sitzungsunterstützung von NetBIOS  Network Window Service Network File Service Network News Transfer Protocol Network Time Protocol Open Shortest Path First Remote Command Remote Process Execution Remote Login Lokale Leitwegwahlprozesse (520/udp) Remote Who Simple Mail Transfer Protocol Secure Socket Server SUN Remote Procedure Call Protocol Transmission Control Protocol Network Virtual Terminal Protocol Trivial File Transfer Protocol User Datagram Protocol World Wide Web X Windows

\*Die Software RMON2 (ECAM) SmartAgent versucht, jedes Paket so detailliert wie möglich zu identifizieren. Fragmentpakete können allerdings nicht vollständig klassifiziert werden. Sie werden daher statt dessen in einer Gesamterfassungsklasse gezählt.

*Tabelle 39. Protokolle, die mehreren Protokollfamilien zugeordnet sind*

<b>Protokoll</b>	<b>Beschreibung</b>	<b>Unterstützte Transporte</b>
Notes	Lotus Notes	NETBEUI, NetBIOS/IP (Datenpaket und Sitzung), NetBIOS/IPX, SPX, TCP
SMB	Server Message Block Protocol von Microsoft	IPX, NETBEUI, NetBIOS/IP (Datenpaket und Sitzung), NetBIOS/IPX
SNMP	Simple Network Management Protocol	DDP1, DDP2, IPX, UDP
SNMPTRAP	Simple Network Management Protocol TRAPS	DDP1, DDP2, IPX, UDP

## Übersicht über RMON2-Protokolle

Jeder Eintrag in der Protokollverzeichnistabelle auf einer Einheit stellt ein Protokoll dar, das von der Einheit entschlüsselt und gezählt werden kann. Dabei kann es sich um Standardprotokolle oder um angepaßte Protokolle handeln.

Die Einträge in der Tabelle werden von jedem Protokoll der Datenübertragungsschicht indiziert: zuerst vom Protokoll der MAC-Schicht und dann von jeder Schicht von Kapselungsprotokoll. Beispiele:

ether2	Kennzeichnet das Ethernet-MAC-Protokoll.
ether2.ip	Kennzeichnet IP-Verkehr über Ethernet-MAC-Protokoll.
ether2.ip.udp	Kennzeichnet UDP-Verkehr über IP oder in einem Ethernet-LAN.
ether2.ip.udp.snmp	Kennzeichnet SNMP-Verkehr (Protokoll der Anwendungsschicht) über Ethernet.

Die Protokolle der MAC-Schicht bestehen aus folgendem:

<b>ether2</b>	Kennzeichnet Ethernet II.
<b>llc</b>	Kennzeichnet das Protokoll LLC (802.2).
<b>snap</b>	Kennzeichnet das Protokoll für den Zugriff auf ein Teilnetzwerk.
<b>vsnap</b>	Kennzeichnet das snap zugeordnete Pseudoprotokoll.
<b>wgAssigned</b>	Kennzeichnet die Protokolle, die sich nicht ohne weiteres an das Format der anderen Verzweigungen der Verbindungsschicht anpassen.
<b>anyLink</b>	Kennzeichnet ein mit dem Präfix '*' versehenes Platzhalterzeichenprotokoll, in dem alle Protokolle der Verbindungsschicht anhand ihres Kapselungsprotokolls der Schicht 2 zusammengefaßt werden. Wenn es sich bei dem Kapselungsprotokoll der Schicht 2 um IPX handelt, gilt folgendes Beispiel:  *.ipx $\Xi$ ether2.ipx + llc.ipx + snap.ipx + wgAssigned.ipx

## Vordefinierte RMON2-Protokolle

In diesem Abschnitt werden vordefinierte Protokolle dargestellt, die von IBM Einheiten ab Firmware-Version 4.10 unterstützt werden. Kapselungsprotokolle werden in alphabetischer Reihenfolge aufgeführt, und die Protokolle der MAC-Schicht, über denen sie ausgeführt werden, sind gekennzeichnet. Beispielsweise wird das Protokoll 802.1-bridge als \*.802.1-bridge und llc.802.1-bridge aufgeführt.

Tabelle 40 (Seite 1 von 2). Protokollnamen

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 (kurze und lange 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	File Transfer Protocol Control Port
ftp-data	File Transfer Protocol Data Port
gopher	Internet-Dokumentensuche und -Abruf
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	Datenpaketunterstützung von NetBIOS
nbt_name	Namensunterstützung von NetBIOS
nbt_session	Sitzungsunterstützung von NetBIOS
netbeui	LAN Manager Netbeui Protocol
netbios-IBM	IBM 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

Tabelle 40 (Seite 2 von 2). Protokollnamen

Protokolle	Protokollname
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 Weiterleitungsprozesse (520/udp)
rtmp	AppleTalk Routing Table Maintenance Protocol
rwho	Remote Who
smb	Microsoft Server Message Block Protocol
smtp	Simple Mail Transfer Protocol
sna	Systems Network Architecture
snmp	Simple Network Management Protocol
snmptrap	Simple Network Management Protocol TRAPS
sunrpc	SUN Remote Procedure Call Protocol
tcp	Transmission Control Protocol
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-pep	XNS Packet Exchange Protocol
xns-rip	XNS Routing Information Protocol
xns-spp	XNS Sequenced Packet Protocol
zip	Zone Information Protocol

Tabelle 41 (Seite 1 von 5). Vordefinierte Protokolle

Protokoll der MAC-Schicht						Kapselungsprotokolle
*	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

Tabelle 41 (Seite 2 von 5). Vordefinierte Protokolle

Protokoll der MAC-Schicht						Kapselungsprotokolle
*	ether2.	llc	snap.	vsnap_ether2.	wgAssigned.	
■	■	■	■			ip.ip.udp.nbt_session
■	■	■	■			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

Tabelle 41 (Seite 3 von 5). Vordefinierte Protokolle

Protokoll der MAC-Schicht						Kapselungsprotokolle
*	ether2.	llc	snap.	vsnap_ether2.	wgAssigned.	
■	■	■	■		■	ipx.nov-netbios.notes
■	■	■	■		■	ipx.nov-netbios.smb
■	■	■	■		■	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



Tabelle 41 (Seite 4 von 5). Vordefinierte Protokolle

Protokoll der MAC-Schicht						Kapselungsprotokolle
*	ether2.	llc	snap.	vsnap_ether2.	wgAssigned.	
■	■	■	■			ip.ip.tcp.snmp
■	■	■	■			ip.ip.tcp.snmptrap
■	■	■	■			ip.ip.tcp.telnet
■	■	■	■			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.ccmail
■	■	■	■			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

Tabelle 41 (Seite 5 von 5). Vordefinierte Protokolle

Protokoll der MAC-Schicht						Kapselungsprotokolle
*	ether2.	llc	snap.	vsnap_ether2.	wgAssigned.	
■	■	■	■			ip.udp.ntp
■	■	■	■			ip.udp.printer
■	■	■	■			ip.udp.router
■	■	■	■		■	ipx.nov-pep.nov-watchdog
■	■	■	■		■	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-IBM
■		■				sna
■	■	■	■			vecho
■	■	■	■			vip
■	■	■	■			vip.varp
■	■	■	■			vip.vicp
■	■	■	■			vip.vipc
■	■	■	■			vip.vipc.vipc-dgp
■	■	■	■			vip.vipc.vipc-rdp
■	■	■	■			vip.vrtp
■	■	■	■			vip.vspp

\*Diese Produkte, die über llc ausgeführt werden, werden als "llc.vtr.vecho" etc. angezeigt. Hierbei handelt es sich bei vtr um eine zusätzliche Protokollschicht.

## Benutzerdefinierte Protokolle

**Anmerkung:** Dieser Abschnitt bezieht sich nur auf Version 4.10.

Falls Sie in Ihrem Netzwerk angepaßte Protokolle oder Protokollkapselungen verwenden, möchten Sie diese möglicherweise mit Hilfe einer Managementanwendung wie Nways Manager Remote Monitor in Ihr Protokollverzeichnis aufnehmen.

Wenn Sie auf Ihrer Einheit Firmware der Version 4.10 installiert haben, können Sie mindestens 64 Platzhalterzeichenprotokolle oder 256 andere Protokolle angeben. (Eine Beschreibung des Platzhalterzeichenprotokolls "anyLink" ist in der Liste mit Protokollen der MAC-Schicht im Abschnitt „Übersicht über RMON2-Protokolle“ auf Seite 161 enthalten.) Auf Einheiten, die über höhere Speicherkapazitäten verfügen, können Sie möglicherweise zusätzliche Protokolle angeben.

Von Firmware der Version 4.10 werden einige erweiterbare Protokolle (siehe Tabelle 42) unterstützt. Dabei gibt es folgende Ausnahmen:

- ipx kann durch keinen der Werte 0 oder 17 erweitert werden.
- llc kann nicht durch ungeradzahlige Kindprotokolle erweitert werden.
- nov-sap, nsp, sunrpc, vip, vipc und vsnap sind nicht erweiterbar.

Der Wert "maxChildren" gibt die Gesamtzahl an Kindprotokollen an, die definiert werden können. Diese Berechnung hängt nicht von der verwendeten Kapselung ab. Beispielsweise würden ether2.ip.udp und ip.ip.udp nur als ein Kindprotokoll gezählt werden.

maxChildren				maxChildren			
Protokoll	Gesamt	Vordefiniert	Benutzerdefiniert	Protokoll	Gesamt	Vordefiniert	Benutzerdefiniert
atalk	16	9	7	snap	32	14	18
ether2	32	28	4	tcp	64	22	42
idp	8	5	3	udp	64	17	47
ip	32	7	25	vipc-dgp	4	0	4
ip.ip	16	7	9	vipc-rdp	0	4	
ipx	256	5*	249	vspp	4	0	4
llc	256	8	120**	xns-pep	0	4	
nov-pep	16	11	5	xns-spp	4	0	4
nov-spx	16	0	16				

\*ipx kann durch keinen der Werte 0 oder 17 erweitert werden. \*\*llc kann nicht durch ungeradzahlige Kindprotokolle erweitert werden.



---

## Anhang D. Anwendung Roving Analysis Port und PACMIB

Im Rahmen der Zusammenarbeit zwischen IBM und 3Com wird das Management einiger Überwachungsfunktionen von 3Com von Nways Manager Remote Monitor unterstützt.

Dieser Anhang ist in die folgenden Abschnitte unterteilt:

- Anwendung "Roving Analysis Port"
- PACMIB-Funktionalität verwenden

---

### Anwendung Roving Analysis Port

Mit Hilfe der Anwendung "Roving Analysis Port" können Sie den Status von CoreBuilder-Switches von 3Com im Netzwerk anzeigen. Sie können auf diesen Switches auch Analyzer- und Überwachungsanschlüsse konfigurieren, die Sie zu Zwecken des Netzwerkmanagements zur Überwachung des Datenverkehrs am Anschluß verwenden können. Sie können jedes beliebige an eine CoreBuilder-Einheit von 3Com angeschlossene Netzwerksegment auswählen und seine Aktivität mit Hilfe eines Netzwerk-Analyzers, wie z. B. einer Einheit oder einem Sniffer, überwachen.

Von dieser Anwendung werden nur Switches der CoreBuilder-Produktfamilie von 3Com unterstützt.

### Status

Gehen Sie wie folgt vor, um eine Zusammenfassung der Informationen zum Status von 3Com Corebuilder und von Anschlüssen auf diesem Switch anzuzeigen:

1. Wählen Sie im Hauptfenster von Nways Manager Remote Monitor im Menü "Configure" den Eintrag "RAP Status" aus, um das Dialogfenster "View Switch Status" zu öffnen. (Siehe Abb. 66 auf Seite 172.)
2. In diesem Dialogfenster ist eine Liste mit den Switches im Netzwerk enthalten. (Hierbei handelt es sich um die Einheiten, für die im Dialogfenster "Device List Editor" das Feld "Device Type" auf "3Com CoreBuilder" eingestellt wurde. Weitere Informationen hierzu sind im Abschnitt „Einheiten installieren und die Installation überprüfen“ auf Seite 10 enthalten.)



Abbildung 66. Dialogfenster "View Switch Status"

3. Wählen Sie im Bereich "Select Switch" einen Switch aus, um dessen Status anzuzeigen. Die Informationen zum Switch werden daraufhin im Bereich "Switch Status" angezeigt.

## Konfiguration

Beim Installieren eines Überwachungsanschlusses werden über diesen Anschluß geleitete Daten kopiert und an den Analyseanschluß weitergeleitet. Dabei wird die übliche Paketverarbeitung nicht beeinträchtigt. Sie können diese Funktion verwenden, um den Datenverkehr von einem beliebigen 3Com CoreBuilder-Anschluß zu überwachen, indem Sie eine Einheit an den Analyseanschluß anschließen.

## Einen Analyseanschluß konfigurieren

Die Konfiguration von Analyseanschlüssen sollte dann durchgeführt werden, wenn gerade eine neue Einheit an einen Anschluß auf dem Switch angeschlossen wurde.

1. Wählen Sie im Hauptfenster von Nways Manager Remote Monitor im Menü "Configure" den Eintrag "RAP Configuration" aus.
2. Daraufhin wird das Dialogfenster "Change Analyzer Port" (siehe Abb. 67) angezeigt.

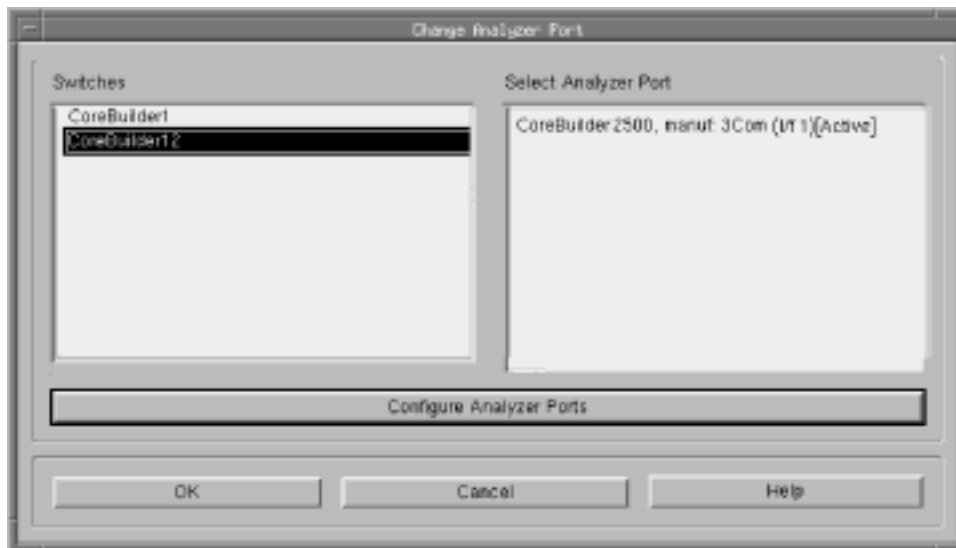


Abbildung 67. Dialogfenster "Change Analyzer Port"

3. Wählen Sie im Bereich "Switches" einen Switch aus. Wenn der ausgewählte Switch verfügbar ist, wird im Bereich "Select Analyzer Port" eine Liste der auf dem Switch vorhandenen Analyseanschlüsse angezeigt. Wenn er nicht verfügbar ist, wird die Nachricht No response from switch angezeigt.
4. Wählen Sie im Bereich "Select Analyzer Port" einen Analyseanschluß aus.  
Anmerkung: Sie sollten nur Anschlüsse auswählen, an die ein Netzwerk-Analyzer angeschlossen ist.
5. Klicken Sie den Eintrag **Configure Analyzer Ports** an, um die aktuelle Konfiguration von Analyseanschlüssen auf dem ausgewählten Switch oder auf anderen verfügbaren Switches zu ändern. Das in Abb. 68 auf Seite 174 gezeigte Dialogfenster "Analyzer Port Configuration" wird angezeigt.

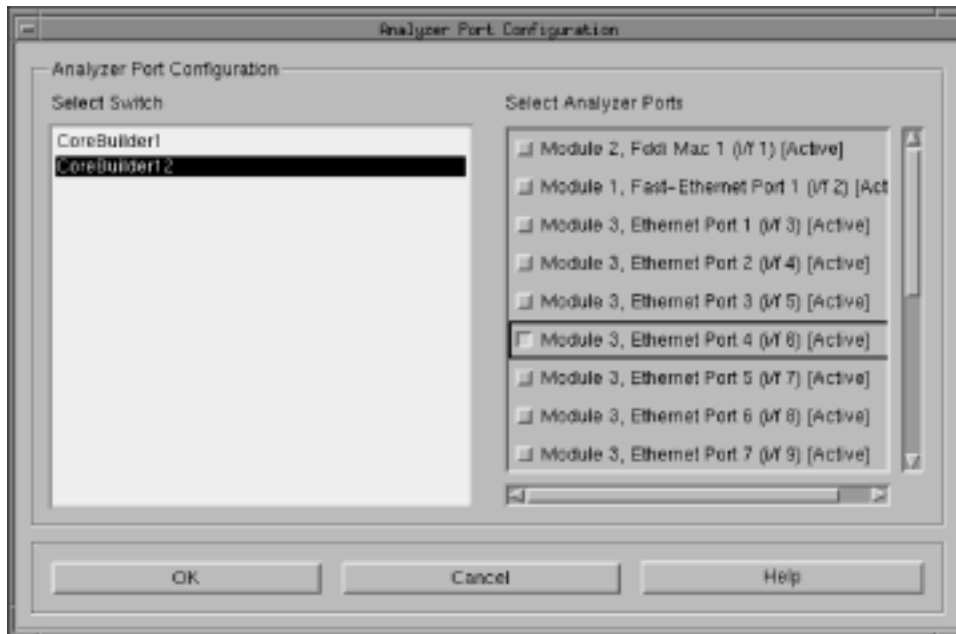


Abbildung 68. Dialogfenster "Analyzer Port Configuration"

- a. Wählen Sie bei Bedarf im Bereich "Select Switch" einen anderen Switch aus. Im Bereich "Select Analyzer Port" wird eine Liste der auf dem Switch vorhandenen Analyseanschlüsse angezeigt. Gegenwärtig als Analyseanschlüsse ausgewählte Anschlüsse werden durch einen dem Anschlußnamen vorangestellten roten Knopf gekennzeichnet.
- b. Aktivieren oder inaktivieren Sie den dem Anschlußnamen vorangestellten Knopf, um Anschlüsse als Analyseanschlüsse auszuwählen oder um die Auswahl zurückzunehmen.  
 Sie sollten nur Anschlüsse auswählen, an die ein Netzwerk-Analyzer angeschlossen ist.
- c. Klicken Sie das Feld **OK** an, um die Änderungen zu sichern und um zum Dialogfenster "Change Analyzer Port" zurückzukehren, oder klicken Sie die Option **Cancel** an, um die Änderungen zu verwerfen.

### Überwachungsanschlüsse konfigurieren

Das Konfigurieren von Überwachungsanschlüssen kann jederzeit durchgeführt werden, wenn sich die Anforderungen an die Überwachung ändern.

1. Klicken Sie das Feld **OK** an, wenn Sie im Dialogfenster "Change Analyzer Port" einen Analyseanschluß ausgewählt haben. Dadurch wird das Dialogfenster "Roving Analysis Configuration" (siehe Abb. 69 auf Seite 175) aufgerufen. Über dieses Dialogfenster können Sie die Anschlüsse definieren, die überwacht werden sollen.



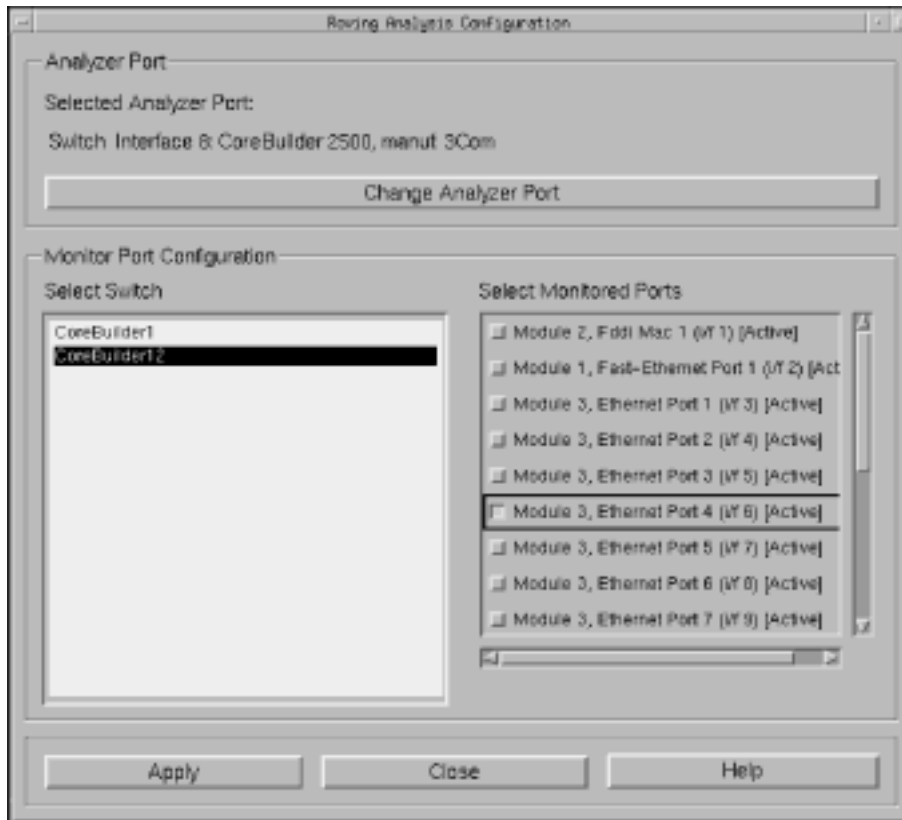


Abbildung 69. Dialogfenster "Roving Analysis Configuration"

- a. Wählen Sie bei Bedarf einen anderen Analyseanschluß aus, an den der Datenverkehr auf dem Überwachungsanschluß kopiert werden soll. Klicken Sie die Option **Change Analyzer Port** an, und befolgen Sie die Anweisungen in Schritt 5 auf Seite 173.
- b. Wählen Sie im Bereich "Select Switch" einen Switch aus, um die Überwachungsanschlüsse auf einem Switch zu definieren. Im Bereich "Select Monitored Ports" wird eine Liste der auf dem Switch vorhandenen Anschlüsse angezeigt. Alle gegenwärtig überwachten Anschlüsse werden blau hervorgehoben, und der dem Anschlußnamen vorangestellte Knopf wird ausgewählt.
- c. Aktivieren oder inaktivieren Sie in der Liste "Selected Monitored Ports" den dem Anschlußnamen vorangestellten Knopf, um einen Anschluß als Überwachungsanschluß auszuwählen oder um die Auswahl zurückzunehmen.
- d. Klicken Sie die Option **Apply** an, um diese Anschlüsse auf dem ausgewählten Switch zu konfigurieren. Daraufhin werden von diesen Anschlüssen gesendete Pakete kopiert und an den Netzwerk-Analyzer auf dem angegebenen Analyseanschluß weitergeleitet.

Weitere Informationen zur Anwendung "Roving Analysis Port" und zur Konfiguration von 3Com CoreBuilder sind in der mit der Einheit 3Com CoreBuilder gelieferten Dokumentation enthalten.

## PACMIB-Funktionalität verwenden

Mit Hilfe von PACMIB (Port Address Correlation MIB) werden Anschluß- und Host-Daten miteinander abgeglichen, und Anschlußstatistiken zu im Netzwerk vorhandenen Einheiten des Typs 3Com CoreBuilder 5000 werden erstellt. Durch Verwendung der Funktion PACMIB kann eine Tabelle mit den MAC-Adressen von Einheiten generiert werden, die mit den einzelnen Anschlüssen auf einem Hub verbunden sind.

Einheiten des Typs 3Com CoreBuilder 5000 mit den in Tabelle 43 aufgeführten Karten werden unterstützt.

<i>Tabelle 43. Unterstützte Karten für 3Com CoreBuilder 5000</i>			
<b>Produkt</b>	<b>Modellnummer</b>	<b>Modul</b>	<b>Version</b>
3Com CoreBuilder 5000 Ethernet Network Monitoring Card	6100-MGT	EMAC	ab 3.0
3Com CoreBuilder 5000 Advanced Ethernet Network Monitoring Card	6100D-AMGT	GEMINI	ab 2.0
3Com CoreBuilder 5000 Token Ring Network Monitoring Card	6200-MGT	TRMAC	ab 3.0

Zum Anzeigen von PACMIB-Daten gibt es die folgenden zwei Möglichkeiten:

- Vom Host zum Anschluß, nach den MAC-Adressen der verbundenen Einheiten sortiert.
- Vom Anschluß zum Host, nach dem Anschluß auf dem Hub sortiert.

Eine Tabelle mit Statistiken zu den einzelnen Anschlüssen kann auch angezeigt werden, indem ein Eintrag in der Tabelle angeklickt wird.

1. Dazu wird von PACMIB die Einheit verwendet, die gegenwärtig zur Überwachung im Hauptfenster verwendet wird. Befolgen Sie bei Bedarf die Anweisungen in Kapitel 4, um eine Einheit und eine Schnittstelle zur Überwachung auszuwählen.
2. Klicken Sie zum Starten von PACMIB für die überwachte Einheit im Hauptfenster von Nways Manager Remote Monitor im Menü "Analysis" den Eintrag "PACMIB" an, und wählen Sie den Eintrag "Enable/Disable" aus.

Wenn PACMIB auf der ausgewählten Einheit aktiviert ist, wird die Einheit zurückgesetzt.

3. Klicken Sie im Dialogfenster "PACMIB Enable/Disable" die Option **Enable** an. Dadurch kehren Sie zum Hauptfenster zurück. Gleichzeitig wird an der Einheit ein Warmstart zum Zurücksetzen durchgeführt.

Eine Beschreibung des Zurücksetzens durch einen Warmstart im Abschnitt „Systemparameter einstellen“ auf Seite 22 enthalten.

- Wählen Sie im Menü "PACMIB" eine der Tabellen "Port to Host" oder "Host to Port" aus, sobald die Einheit zurückgesetzt und die Überwachung im Hauptfenster wiederaufgenommen wurde. In Abb. 70 werden Beispiele für Tabellen der Typen "Port to Host" und "Host to Port" gezeigt.



Abbildung 70. Beispiele für Tabellen der Typen "Port to Host" und "Host to Port"

- Der Inhalt einer PACMIB-Tabelle kann in eine Datei exportiert werden, so daß er in andere Anwendungen exportiert oder ausgedruckt werden kann. Die Daten können in einem der Dateiformate "ASCII unstrukturiert" oder "CSV" gesichert werden. Klicken Sie zum Öffnen des Dialogfensters "File" die Option **Export** an, und geben Sie das Datenformat und den Dateinamen an.
- Klicken Sie zum Schließen einer PACMIB-Tabelle die Option **Exit** an.



---

## Anhang E. Variablen in Anzeigen und Anwendungen

In diesem Anhang sind Definitionen der Variablen enthalten, die in den Anzeigen und Anwendungen von Nways Manager Remote Monitor ausgewählt werden können. Der Anhang enthält die folgenden Abschnitte:

- Statistikvariablen
- Protokollvariablen
- Host-Variablen
- Ringstationsvariablen
- ECAM-Variablen

---

### Statistikvariablen

Die Anzeige "Statistics" enthält die folgenden Variablen für Ethernet-, FDDI- und Token-Ring-Netzwerke.

---

### Verfügbare Variablen für Ethernet

*Tabelle 44. Verfügbare Statistikvariablen für Ethernet*

Bytes Sent	Die Gesamtzahl an Byte, aus denen alle in diesem Segment entdeckten Pakete bestehen.
Broadcasts	An die Rundsendeadresse gesendete fehlerfreie Pakete.
Collisions	Die günstigste Schätzung der Anzahl an Kollisionen in diesem Segment.
CRC Errors	Die Länge eines Pakets ist keine ganzzahlige Anzahl von Oktetten, oder das Paket verfügt über eine fehlerhafte FCS.
Packets Missed	Diese Variable gibt an, wie oft die Sonde einen Mangel an Ressourcen entdeckt hat und dadurch möglicherweise einige Pakete nicht zählen konnte.
Packets Sent	Die Gesamtzahl der in diesem Segment entdeckten Pakete. Fehlerpakete sind eingeschlossen.
Multicasts	An die Multicast-Adresse gesendete fehlerfreie Pakete. Broadcast-Pakete sind nicht eingeschlossen.
Too Long	Länger als 1518 Oktette (einschließlich FCS-Oktette), aber ansonsten wohlgeformt.
Too Short	Kürzer als 64 Oktette (einschließlich FCS-Oktette), aber ansonsten wohlgeformt.
Long + CRC	Zu lang, und ein CRC-Fehler liegt vor.
Short + CRC	Zu kurz, und ein CRC-Fehler liegt vor.
64 Bytes	Pakete mit einer Länge von genau 64 Byte.
65 bis 127 usw.	Es handelt sich um einschließliche Paketgrößen. FCS-Oktette sind eingeschlossen.

## Verfügbare Variablen für FDDI

Tabelle 45. Verfügbare Statistikvariablen für FDDI

Variable	Beschreibung
Beacon-Nachrichten	Die Anzahl der auf dem Ring gesehenen Beacon-Nachrichten.
Beacon Src.*	Die Adresse des Host, der die letzte Beacon-Nachricht gesendet hat.
Broadcasts	An die Rundsendeadresse gesendete fehlerfreie Pakete.
Bytes Sent	Die Gesamtzahl an Byte, aus denen alle auf dem Ring entdeckten Pakete bestehen.
Claim Frames	Die Anzahl der auf dem Ring gesehenen Anforderungsrahmen.
Dir. Beacons	Die Anzahl der auf dem Ring gesehenen weitergeleiteten Beacon-Nachrichten.
Dir. Beacon Src.*	Die Adresse des Host, der die letzte weitergeleitete Beacon-Nachricht gesendet hat.
Errors	Ein Rahmen mit aktivem Fehleranzeiger.
Missed	Diese Variable gibt an, wie oft die Sonde einen Mangel an Ressourcen entdeckt hat und dadurch möglicherweise einige Pakete nicht zählen konnte.
Multicasts	An die Multicast-Adresse gesendete fehlerfreie Pakete (Broadcast-Pakete ausgenommen).
Packets Sent	Die Gesamtzahl der in diesem Ring entdeckten Pakete. Fehlerpakete sind eingeschlossen.
Ring State*	Der aktuelle Betriebsstatus des FDDI-Rings: <ol style="list-style-type: none"> <li>1. Ring Operational</li> <li>2. Non Operation Claim</li> <li>3. Non Operational Beacon</li> <li>4. Non Operational Dir. Beacon</li> <li>5. Unknown</li> </ol>
SMT Frames	Die Anzahl der auf dem Ring gesehenen SMT-Rahmen.
TNEG*	Variable Umlaufdauer des Token (TNEG). Dabei handelt es sich um die TNEG, die beim Prozeß zur Senderechanforderung erfolgreich war.
Tokens	Die Anzahl der Token auf dem Ring.
22 Bytes	Pakete mit einer Länge von genau 22 Byte.
23 to 63 etc.	Es handelt sich um einschließliche Paketgrößen. FCS-Oktette sind eingeschlossen.

\* Eignet sich nicht für Diagrammdarstellungen oder Skalendarstellungen.

## Statistische Variablen

Tabelle 46 (Seite 1 von 3). Verfügbare statistische Variablen für Token-Ring

Variable	Beschreibung
Abort Errors	Die Gesamtzahl der Abbruchbegrenzer, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Beim Versuch, einen Rahmen zu übertragen, wurde von einer Station ein Problem entdeckt.
AC Errors	Die Gesamtzahl der AC-Fehler (Address Copied), die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden.
All Route Bcasts	Die Gesamtzahl an Rundsendungen, die an beliebige Adressen auf einem beliebigen Ring gesendet wurden.
All Route Octets	Die Anzahl der Oktette, aus denen an beliebige und an alle Adressen gesendete Rundsendungen bestehen.
Beacon Events	Die Angabe, wie oft der Ring in einen Status für den Beacon-Betrieb versetzt wird. (Wenn die Quellenadresse eines Beacon-Pakets geändert wird, findet noch keine neue Ausgabe von Beacon-Nachrichten statt.)
Beacon Packets	Die Gesamtzahl der von der Sonde entdeckten MAC-Beacon-Pakete.
Beacon Time	Die Gesamtzeit, während der sich der Ring in einem Status für den Beacon-Betrieb befunden hat.
Burst Errors	Die Gesamtzahl der Trennfehler, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Trennfehler werden oft von einer sehr kurzen Trennung der Verbindung im Kabel oder von einem sehr kurzen Anstieg von elektronischen Störungen (Rauschen) verursacht.
Claim Token Events	Die Angabe, wie oft der Ring in den Token-Anforderungs-Prozeß eingetreten ist.
Claim Token Pkts	Die Gesamtzahl der von der Sonde entdeckten Token-Anforderungs-Pakete.
Congestion Errors	Die Gesamtzahl der Fehler aufgrund von Empfangsüberlastung, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Eine Station hat einen Rahmen empfangen und hat nicht über ausreichenden Pufferbereich verfügt, um ihn zu speichern.
Data Bytes	Die Gesamtzahl an Byte, aus denen alle in diesem Segment entdeckten Promiscuous-Datenpakete bestehen.
Data Packets	Die Gesamtzahl der in diesem Segment entdeckten Promiscuous-Datenpakete.
Data Bcast Pkts	An die Rundsendeadresse gesendete fehlerfreie Pakete. Multicast-Pakete sind nicht eingeschlossen.
Data Mcast Pkts	An die Multicast-Adresse gesendete fehlerfreie Pakete. Broadcast-Pakete sind nicht eingeschlossen.
Drop Events	Diese Variable gibt an, wie oft die Sonde einen Mangel an Ressourcen entdeckt hat und dadurch möglicherweise einige LLC- oder MAC-Pakete nicht zählen konnte.
Error Reports	Die Gesamtzahl der von der Sonde entdeckten Berichtsrahmen für normale Fehler. Normale Fehler sind nicht so gravierend, daß der Ring nicht mehr funktioniert. Folgende Fehler sind normale Fehler: Leitungs- und Trennfehler, interne Fehler, Abbruch- und ACE-Fehler, Fehler durch verlorene Rahmen sowie Token-, Frequenz- und Rahmenkopiefehler.

Tabelle 46 (Seite 2 von 3). Verfügbare statistische Variablen für Token-Ring

Variable	Beschreibung
Frames Copied	Die Gesamtzahl der Rahmenkopiefehler, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. In einer Station wird davon ausgegangen, daß eine andere Station auf dem Ring über dieselbe Adresse verfügt (zumeist kein Problem - weitere Informationen hierzu sind im Glossar enthalten).
Frames In	Die Anzahl der von einem anderen Segment in dieses Segment übertragenen Rahmen.
Frames Out	Die Anzahl der von diesem Segment in ein anderes Segment übertragenen Rahmen.
Frequency Errors	Die Gesamtzahl der Frequenzfehler, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Dabei handelt es sich um einen Fehler in der Ablaufsteuerung, der oft dadurch verursacht wird, daß mehr als 72 Stationen auf dem Ring angeschlossen sind.
Internal Errors	Die Gesamtzahl der internen Adapterfehler, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Dieser Fehler wird oft durch zu große Hitze in einem überlasteten System verursacht.
Line Errors	Die Gesamtzahl der Leitungsfehler, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Dieser Fehler wird in der Regel durch elektronische Störungen (Rauschen) oder durch Kabelfehler verursacht.
Local LLC Frames	Die Gesamtzahl der empfangenen Rahmen, die kein RIF-Feld aufgewiesen haben (oder die ein RIF-Feld aufgewiesen haben, das lediglich die lokale Nummer des Rings eingeschlossen hat) und bei denen es sich nicht um ARB-Rahmen (All Route Broadcast) gehandelt hat.
Lost Frames	Die Gesamtzahl der Fehler durch verlorene Rahmen, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Ein Rahmen wurde von einer Station übertragen und danach von dieser nicht mehr gesehen.
MAC Bytes	Die Gesamtzahl an Byte, aus denen alle in diesem Segment entdeckten MAC-Pakete bestehen.
MAC Packets	Die Gesamtzahl der in diesem Segment entdeckten MAC-Pakete. Fehlerpakete sind eingeschlossen.
NAUN Changes	Die Gesamtzahl der von der Sonde entdeckten NAUN-Änderungen. NAUN-Änderungen treten auf, wenn eine neue Station auf dem Ring geöffnet wird oder wenn eine Station vom Ring genommen wird.
Octets In	Gibt die Anzahl der Oktette an, aus denen von einem anderen Segment an dieses Ringsegment gesendete Rahmen bestehen.
Octets Out	Gibt die Anzahl der Oktette an, aus denen von diesem Ringsegment an ein anderes Segment gesendete Rahmen bestehen.
Octets Through	Gibt die Anzahl der Oktette an, aus denen Rahmen bestehen, die auf dem Weg zur Zieladresse über dieses Ringsegment geleitet werden.
Purge Events	Gibt an, wie oft der Ring von einem normalen Ringstatus in einen Ringfreigabestatus versetzt wird. (Davon ausgeschlossen ist jeder Ringfreigabestatus, der durch einen Token-Anforderungs-Status oder einen Status für den Beacon-Betrieb verursacht wird.)
Purge Packets	Die Gesamtzahl der von der Sonde entdeckten MAC-Pakete für die Ringfreigabe.
Ring Number	Dabei handelt es sich um die numerische Kennung dieses Rings.



Tabelle 46 (Seite 3 von 3). Verfügbare statistische Variablen für Token-Ring

Variable	Beschreibung
Ring Polls	Die Gesamtzahl der von der Sonde entdeckten Ringaufrufereignisse. (Mit anderen Worten: Die Anzahl der von der aktiven Überwachung eingeleiteten Ringaufrufe.)
Sgl Route Bcasts	Die Anzahl der Rundsendungen, die an eine begrenzte Anzahl von Empfängern - in der Regel das lokale Ringsegment - gesendet wurden.
Sgl Route Octets	Die Anzahl der Oktette, aus denen Rundsendungen bestehen, die an eine begrenzte Zahl von Empfängern - in der Regel das lokale Ringsegment - gesendet wurden.
Through Frames	Die Anzahl der Rahmen, die auf dem Weg zur Zieladresse über dieses Ringsegment geleitet werden.
Token Errors	Die Gesamtzahl der Token-Fehler, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Die Benachrichtigung erfolgt über die aktive Überwachung, wenn das Token beschädigt wird.
1 Hop Frames etc.	Die Gesamtzahl der Rahmen, die 1, 2, 3, 4, 5, 6, 7, 8 oder mehr Hops (über Brücken zwischen Ringsegmenten) ausführen, um die Zieladresse zu erreichen.
18 - 63 Bytes etc.	Verteilung der Paketgrößen.

## Protokollvariablen

In der folgenden Tabelle werden die für Ethernet, FDDI und Token-Ring verfügbaren Variablen aufgeführt.

Tabelle 47. Verfügbare Protokollvariablen für Ethernet

Variable	Beschreibung
Broadcasts	An die Rundsendeadresse gesendete fehlerfreie Pakete.
Bytes Sent	Die Gesamtzahl an Byte, aus denen alle in diesem Segment entdeckten Pakete bestehen.
Collisions	Die günstigste Schätzung der Anzahl an Kollisionen in diesem Segment.
CRC Errors	Die Länge eines Pakets ist keine ganzzahlige Anzahl von Oktetten, oder das Paket verfügt über eine fehlerhafte FCS.
Long + CRC	Ein Paket ist zu lang und weist einen CRC-Fehler auf.
Multicasts	An die Multicast-Adresse gesendete fehlerfreie Pakete. Broadcast-Pakete sind nicht eingeschlossen.
Packets Missed	Diese Variable gibt an, wie oft die Sonde einen Mangel an Ressourcen entdeckt hat und dadurch möglicherweise einige Pakete nicht zählen konnte.
Packets Sent	Die Gesamtzahl der in diesem Segment entdeckten Pakete. Fehlerpakete sind eingeschlossen.
Too Long	Länger als 1518 Oktette (einschließlich FCS-Oktette), aber ansonsten wohlgeformt.
Too Short	Kürzer als 64 Oktette (einschließlich FCS-Oktette), aber ansonsten wohlgeformt.
Utilization	Die Auslastung des Netzwerks in Prozent während dieses Erfassungszeitraums.

## Verfügbare Variablen für FDDI

Tabelle 48. Verfügbare Protokollvariablen für FDDI

Variable	Beschreibung
Beacons	Die Anzahl der auf dem Ring gesehenen Beacon-Nachrichten.
Broadcasts	An die Rundsendeadresse gesendete fehlerfreie Pakete.
Bytes Sent	Die Gesamtzahl an Byte, aus denen alle auf dem Ring entdeckten Pakete bestehen.
Claim Frames	Die Anzahl der auf dem Ring gesehenen Anforderungsrahmen.
Dir. Beacons	Die Anzahl der auf dem Ring gesehenen weitergeleiteten Beacon-Nachrichten.
Errors	Ein Rahmen mit aktivem Fehleranzeiger.
Mean TRT	Errechneter Mittelwert für die Zeit eines Token-Umlaufs.
Missed	Diese Variable gibt an, wie oft die Sonde einen Mangel an Ressourcen entdeckt hat und dadurch möglicherweise einige Pakete nicht zählen konnte.
Multicasts	An die Multicast-Adresse gesendete fehlerfreie Pakete (Broadcast-Pakete ausgenommen).
Packets Sent	Die Gesamtzahl der in diesem Ring entdeckten Pakete. Fehlerpakete sind eingeschlossen.
SMT Frames	Die Anzahl der auf dem Ring gesehenen SMT-Rahmen.
TNEG	Variable Umlaufdauer des Token. Dabei handelt es sich um die TNEG, die beim Prozeß zur Senderechanforderung erfolgreich war.
Utilization	Die Auslastung des Netzwerks in Prozent während dieses Erfassungszeitraums.
22 Bytes	Pakete mit einer Länge von genau 22 Byte.
23 to 63 etc.	Es handelt sich um einschließliche Paketgrößen. FCS-Oktette sind eingeschlossen.

## Verfügbare Variablen für Token-Ring

Tabelle 49 (Seite 1 von 3). Verfügbare Protokollvariablen für Token-Ring

Variable	Beschreibung
Abort Errors	Die Gesamtzahl der Abbruchbegrenzer, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Beim Versuch, einen Rahmen zu übertragen, wurde von einer Station ein Problem entdeckt.
AC Errors	Die Gesamtzahl der AC-Fehler (Address Copied), die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden.
Active Stations	Die Anzahl der aktiven Stationen (d. h. der Stationen, die am Ringaufruf teilnehmen) in diesem Ringsegment.
Beacon Events	Die Angabe, wie oft der Ring in einen Status für den Beacon-Betrieb versetzt wird. (Wenn die Quellenadresse eines Beacon-Pakets geändert wird, findet noch keine neue Ausgabe von Beacon-Nachrichten statt.)
Beacon Packets	Die Gesamtzahl der von der Sonde entdeckten MAC-Beacon-Pakete.

Tabelle 49 (Seite 2 von 3). Verfügbare Protokollvariablen für Token-Ring

Variable	Beschreibung
Beacon Time	Die Gesamtzeit, während der sich der Ring in einem Status für den Beacon-Betrieb befunden hat.
Burst Errors	Die Gesamtzahl der Trennfehler, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Trennfehler werden oft von einer sehr kurzen Trennung der Verbindung im Kabel oder von einem sehr kurzen Anstieg von elektronischen Störungen (Rauschen) verursacht.
Claim Token Events	Die Angabe, wie oft der Ring in den Token-Anforderungs-Prozeß eingetreten ist.
Claim Token Packets	Die Gesamtzahl der von der Sonde entdeckten Token-Anforderungs-Pakete.
Congestion Errors	Die Gesamtzahl der Fehler aufgrund von Empfangsüberlastung, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Eine Station hat einen Rahmen empfangen und hat nicht über ausreichenden Pufferbereich verfügt, um ihn zu speichern.
Data Bcast Packets	An die Rundsendeadresse gesendete fehlerfreie Pakete.
Data Bytes	Die Gesamtzahl an Byte, aus denen alle in diesem Segment entdeckten Promiscuous-Datenpakete bestehen.
Data Mcast Packets	An die Multicast-Adresse gesendete fehlerfreie Pakete. Broadcast-Pakete sind nicht eingeschlossen.
Data Packets	Die Gesamtzahl der in diesem Segment entdeckten Promiscuous-Datenpakete.
Drop Events	Diese Variable gibt an, wie oft die Sonde einen Mangel an Ressourcen entdeckt hat und dadurch möglicherweise einige Pakete nicht zählen konnte.
Error Reports	Die Gesamtzahl der von der Sonde entdeckten Berichtsrahmen für normale Fehler. Normale Fehler sind nicht so gravierend, daß der Ring nicht mehr funktioniert. Folgende Fehler sind normale Fehler: Leitungs- und Trennfehler, interne Fehler, Abbruch- und ACE-Fehler, Fehler durch verlorene Rahmen sowie Token-, Frequenz- und Rahmenkopiefehler.
Frames Copied	Die Gesamtzahl der Rahmenkopiefehler, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. In einer Station wird davon ausgegangen, daß eine andere Station auf dem Ring über dieselbe Adresse verfügt (zumeist kein Problem - weitere Informationen hierzu sind im Glossar enthalten).
Frequency Errors	Die Gesamtzahl der Frequenzfehler, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Dabei handelt es sich um einen Fehler in der Ablaufsteuerung, der oft dadurch verursacht wird, daß mehr als 72 Stationen auf dem Ring angeschlossen sind.
Internal Errors	Die Gesamtzahl der internen Adapterfehler, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Dieser Fehler wird oft durch zu große Hitze in einem überlasteten System verursacht.
Line Errors	Die Gesamtzahl der Leitungsfehler, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Dieser Fehler wird in der Regel durch elektronische Störungen (Rauschen) oder durch Kabelfehler verursacht.

Tabelle 49 (Seite 3 von 3). Verfügbare Protokollvariablen für Token-Ring

Variable	Beschreibung
Lost Frames	Die Gesamtzahl der Fehler durch verlorene Rahmen, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Ein Rahmen wurde von einer Station übertragen und danach von dieser nicht mehr gesehen.
MAC Bytes	Die Gesamtzahl an Byte, aus denen alle in diesem Segment entdeckten MAC-Pakete bestehen.
MAC Packets	Die Gesamtzahl der in diesem Segment entdeckten Pakete der MAC-Schicht. Fehlerpakete sind eingeschlossen.
NAUN Changes	Die Gesamtzahl der von der Sonde entdeckten NAUN-Änderungen. NAUN-Änderungen treten auf, wenn eine neue Station auf dem Ring geöffnet wird oder wenn der aktuelle NAUN vom Ring genommen wird.
Purge Events	Gibt an, wie oft der Ring von einem normalen Ringstatus in einen Ringfreigabestatus versetzt wird. (Davon ausgeschlossen ist jeder Ringfreigabestatus, der durch einen Token-Anforderungs-Status oder einen Status für den Beacon-Betrieb verursacht wird.)
Purge Packets	Die Gesamtzahl der von der Sonde entdeckten MAC-Pakete für die Ringfreigabe.
Ring Polls	Die Gesamtzahl der von der Sonde entdeckten Ringaufrufereignisse. (Mit anderen Worten: Die Anzahl der von der aktiven Überwachung eingeleiteten Ringaufrufe.)
Token Errors	Die Gesamtzahl der Token-Fehler, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Die Benachrichtigung erfolgt über die aktive Überwachung, wenn das Token beschädigt wird.
18 - 63 etc.	Es handelt sich um einschließliche Paketgrößen. FCS-Oktette sind eingeschlossen.
Utilization	Die Berechnungen der Token-Ring-Auslastung basieren auf der Verwendung der Variable "ifSpeed" aus der Schnittstellentabelle. Wenn der Wert Null beträgt, wird für die Berechnung eine Ringgeschwindigkeit von 16 Mbps angenommen.

## Host-Variablen

Die folgende Liste mit Variablen ist für die Anzeige "Host" für Ethernet, Token-Ring und FDDI verfügbar.

Tabelle 50. Verfügbare Host-Variablen für Ethernet, Token-Ring und FDDI

Variable	Beschreibung
Packets In	Die Anzahl der im Segment gesehenen Pakete (einschließlich Fehlerpakete), deren Zieladresse diese Station ist.
Packets Out	Die Anzahl der Pakete (einschließlich Fehlerpakete), deren Senden von dieser Station veranlaßt wurde.
Bytes In	Die Gesamtzahl an Byte, aus denen alle an diese Station gesendeten Pakete bestehen.
Bytes Out	Die Gesamtzahl an Byte, aus denen alle Pakete bestehen, deren Senden von dieser Station veranlaßt wurde.
Error Packets	Die Anzahl der Fehlerpakete, deren Generierung von dieser Station veranlaßt wurde.
Broadcasts	Von dieser Station übertragene und an die Rundsendeadresse gesendete fehlerfreie Pakete.
Multicasts	Von dieser Station übertragene und an die Multicast-Adresse gesendete fehlerfreie Pakete. Broadcast-Pakete sind nicht eingeschlossen.

## Ringstationsvariablen

Die folgenden Variablen sind für die Anzeige "Ring Station" für Token-Ring verfügbar.

Tabelle 51 (Seite 1 von 2). Verfügbare Ringstationsvariablen für Token-Ring

Variable	Beschreibung
Last NAUN	Die physische Adresse des letzten bekannten NAUN (Nearest Active Upstream Neighbor) dieser Station.
Station Status	Der Status dieser Station auf dem Ring: entweder aktiv, inaktiv oder erzwungenermaßen vom Ring abgemeldet.
Last Entered	Der letzte Zeitpunkt, an dem diese Station in den Ring eingetreten ist.
Last Exited	Der letzte Zeitpunkt, an dem diese Station den Ring verlassen hat.
Duplicate Address	Gibt an, wie oft diese Station von fehlerhaft doppelten Adressen betroffen war.
In-line Errors	Die Gesamtzahl der Leitungsfehler, die vor dieser Station (upstream) in Fehlerberichts-paketen entdeckt wurden, die von der Sonde entdeckt wurden. Dieser Fehler wird in der Regel durch elektronische Störungen (Rauschen) oder durch Kabelfehler verursacht.
Out-line Errors	Die Gesamtzahl der Leitungsfehler, die nach dieser Station (downstream) in Fehlerberichts-paketen entdeckt wurden, die von der Sonde entdeckt wurden. Dieser Fehler wird in der Regel durch elektronische Störungen (Rauschen) oder durch Kabelfehler verursacht.

Tabelle 51 (Seite 2 von 2). Verfügbare Ringstationsvariablen für Token-Ring

Variable	Beschreibung
Internal Errors	Die Gesamtzahl der internen Adapterfehler, die in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Dieser Fehler wird gewöhnlich durch zu große Hitze in einem überlasteten System verursacht.
Inburst Errors	Die Gesamtzahl der Trennungsfehler, die vor dieser Station (upstream) in Fehlerberichtpaketen entdeckt wurden, die von der Sonde entdeckt wurden. Trennfehler werden gewöhnlich von einer sehr kurzen Trennung der Verbindung im Kabel oder von einem sehr kurzen Anstieg von elektronischen Störungen (Rauschen) verursacht.
Out Burst Errors	Die Gesamtzahl der Trennungsfehler, die nach dieser Station (downstream) in Fehlerberichtpaketen entdeckt wurden, die von der Sonde entdeckt wurden. Trennfehler werden gewöhnlich von einer sehr kurzen Trennung der Verbindung im Kabel oder von einem sehr kurzen Anstieg von elektronischen Störungen (Rauschen) verursacht.
AC Errors	Die Gesamtzahl der vom nächsten aktiven Nachbarn vor dieser Station (downstream) gesendeten Pakete, durch die AC-Fehler (Address Copied) gemeldet werden.
Abort Errors	Die Gesamtzahl der Abbruchbegrenzer, die über diese Station in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden. Dies ähnelt einem internen Fehler, aber in diesem Fall trat der Fehler beim Übertragen eines Rahmens auf.
Lost Frames	Die Gesamtzahl der Fehler durch verlorene Rahmen, die über diese Station in von der Sonde entdeckten Fehlerberichtpaketen mitgeteilt werden.
Congestion Errors	Die Gesamtzahl der Fehler aufgrund von Empfangsüberlastung. Dieser Fehler tritt auf, wenn eine Station einen Rahmen empfangen hat und nicht über ausreichenden Pufferbereich verfügt hat, um ihn zu speichern.
Frame Copied Errors	Die Gesamtzahl der Rahmenkopiefehler, die von dieser Station mitgeteilt wurden. In einer Station wird davon ausgegangen, daß eine andere Station auf dem Ring über dieselbe Adresse verfügt (zumeist kein Problem - weitere Informationen hierzu sind im Glossar enthalten).
Frequency Errors	Die Gesamtzahl der Frequenzfehler, die von dieser Station mitgeteilt wurden. Dieser Fehler wird durch die große Differenz zwischen der Uhr eines Adapters und der Uhr seines NAUN verursacht.
Token Errors	Die Gesamtzahl der Token-Fehler, die von dieser Station mitgeteilt wurden. Der Fehler ähnelt einem Leitungsfehler, aber in diesem Fall ist das Token selbst beschädigt.
In Beacon Errors	Die Gesamtzahl der Beacon-Rahmen, die vor dieser Station (upstream) entdeckt wurden. Weitere Informationen hierzu sind im Glossar enthalten.
Out Beacon Errors	Die Gesamtzahl der Beacon-Rahmen, die nach dieser Station (von der Station, die diese Station als NAUN bezeichnet) entdeckt wurden. Weitere Informationen hierzu sind im Glossar enthalten.
Insertions	Diese Variable gibt an, wie oft die Sonde entdeckt hat, daß sich diese Station in den Ring einfügt.

## ECAM-Variablen

In diesem Abschnitt werden die Variablen beschrieben, die für die Module "Statistics", "Host", "Matrix" und "Protocol Distribution" in der Anwendung ECAM verfügbar sind. Eine Beschreibung der Anwendung ECAM ist im Anhang G enthalten.

## Protokollstatistikvariablen

Im folgenden sind die Variablen aufgeführt, über die alle Statistikprotokolle verfügen.

Tabelle 52. ECAM-Protokollstatistikvariablen

Variable	Beschreibung
Packets	Die Gesamtzahl der im Netzwerk entdeckten Pakete für dieses Protokoll.
Bytes	Die Gesamtzahl an Byte für dieses Protokoll im Netzwerk.
Fragment Packets	Die Gesamtzahl der im Netzwerk entdeckten Fragmentpakete für dieses Protokoll.
Fragment Bytes	Die Gesamtzahl an Byte, aus denen die im Netzwerk entdeckten Fragmentpakete bestehen.
Broadcast Packets	Die Gesamtzahl der an die Rundsendeadresse im Netzwerk übertragenen Pakete für dieses Protokoll.
Broadcast Bytes	Die Gesamtzahl an Byte, aus denen die im Netzwerk entdeckten Broadcast-Pakete bestehen.

## Host-Protokollvariablen

Im folgenden sind die Variablen aufgeführt, über die alle Host-Protokolle verfügen.

Tabelle 53 (Seite 1 von 2). ECAM-Host-Protokoll-Variablen

Variable	Beschreibung
In Packets	Die Gesamtzahl der im Netzwerk entdeckten Pakete dieses Protokolltyps, deren Zieladresse diese Station ist.
Out Packets	Die Gesamtzahl der im Netzwerk entdeckten Pakete dieses Protokolltyps, die von dieser Station gesendet wurden.
In Bytes	Die Gesamtzahl an Byte für dieses Protokoll im Netzwerk, deren Zieladresse diese Station ist.
Out Bytes	Die Gesamtzahl an Byte für dieses Protokoll im Netzwerk, die von dieser Station gesendet wurden.
In Fragment Packets	Die Gesamtzahl der im Netzwerk entdeckten Fragmentpakete für dieses Protokoll, deren Zieladresse diese Station ist.
Out Fragment Packets	Die Gesamtzahl der von dieser Station gesendeten Fragmentpakete für dieses Protokoll im Netzwerk.
In Fragment Bytes	Die Gesamtzahl an Byte, aus denen die im Netzwerk entdeckten Fragmentpakete bestehen, deren Zieladresse diese Station ist.
Out Fragment Bytes	Die Gesamtzahl an Byte, aus denen die im Netzwerk entdeckten Fragmentpakete bestehen, die von dieser Station gesendet wurden.

*Tabelle 53 (Seite 2 von 2). ECAM-Host-Protokoll-Variablen*

<b>Variable</b>	<b>Beschreibung</b>
Out Broadcast Packets	Die Gesamtzahl der an die Rundsendeadresse im Netzwerk übertragenen Pakete für dieses Protokoll, die von dieser Station gesendet wurden.
Out Broadcast Bytes	Die Gesamtzahl an Byte, aus denen diese im Netzwerk entdeckten Broadcast-Pakete bestehen, die von dieser Station gesendet wurden.

## **Matrixprotokollvariablen**

Im folgenden sind die Variablen aufgeführt, über die alle Matrixprotokolle verfügen.

<i>Tabelle 54. ECAM-Matrixprotokollvariablen</i>	
<b>Variable</b>	<b>Beschreibung</b>
Packets	Die Gesamtzahl der im Netzwerk entdeckten Pakete für diesen Datenaustausch und dieses Protokoll.
Bytes	Die Gesamtzahl der im Netzwerk entdeckten Byte für diesen Datenaustausch und dieses Protokoll.
Fragment Packets	Die Gesamtzahl der im Netzwerk entdeckten Fragmentpakete für diesen Datenaustausch und dieses Protokoll.
Fragment Bytes	Die Gesamtzahl der im Netzwerk entdeckten Byte, aus denen die Fragmentpakete für diesen Datenaustausch und dieses Protokoll bestehen.
Broadcast Packets	Die Gesamtzahl der an die Rundsendeadresse im Netzwerk übertragenen Pakete für diesen Datenaustausch und dieses Protokoll.
Broadcast Bytes	Die Gesamtzahl der im Netzwerk entdeckten Byte, aus denen die Broadcast-Pakete für diesen Datenaustausch und dieses Protokoll bestehen.



---

## Anhang F. Anwendung ECAM (Enterprise Communications Analysis Module)

In diesem Kapitel wird beschrieben, wie die bei heruntergeladener Software RMON2 (ECAM) SmartAgent verfügbare Anwendung RMON2 (ECAM) von Nways Manager Remote Monitor verwendet wird. Das Kapitel enthält die folgenden Abschnitte:

- Übersicht über die Anwendung ECAM
- Software SmartAgent herunterladen
- ECAM-Anzeigen
- ECAM-Statistiken erstellen
- Protokollstatistiken
- Host-Protokollstatistiken
- Matrixprotokollstatistiken
- Protokollverteilung

Mit Hilfe von herkömmlichen Protokoll-Analysern und von RMON erhält der Netzwerkmanager einen detaillierten Einblick in ein einzelnes Segment. Mit Hilfe von ECAM kann der Netzmanager zur Fehlerbehebung und für andere Operationen den Datenverkehr zwischen Netzen anzeigen.

Mit dem Begriff "ECAM" wird in diesem Kapitel "RMON2 (ECAM)" bezeichnet.

---

### Übersicht über die Anwendung ECAM

Mit Hilfe der Anwendung ECAM (Enterprise Communications Analysis Module) können Sie Protokollstatistiken und gefilterte Protokollstatistiken erstellen und anzeigen. Über den ursprünglichen RMON-Standard hinausgehend können Sie eine vollständige Datensammlung über alle sieben Schichten durchführen. Darin sind Segment-, Host- und Datenaustauschstatistiken für die wichtigsten Protokolle und Anwendungstypen enthalten. Gesammelte Daten können in einem der Formate ASCII oder CSV exportiert werden.

ECAM-Statistiken können nur von Einheiten gesammelt werden, auf die die Software RMON2 (ECAM) heruntergeladen wurde. Weitere Informationen hierzu sind im Abschnitt „Software SmartAgent herunterladen“ auf Seite 192 enthalten.

---

## Software SmartAgent herunterladen

Die Software SmartAgent kann auf eine Einheit geladen oder von einer Einheit entladen werden, damit zusätzliche Funktionen im Hauptfenster von Nways Manager Remote Monitor verfügbar werden. Die Software kann je nach dem Datentyp, der mit Hilfe der Einheit gesammelt werden soll, bei Bedarf gestartet und gestoppt werden.

Die Software RMON2 (ECAM) SmartAgent ist im Lieferumfang von Nways Manager Remote Monitor enthalten.

- Bei Verwendung einer RMON2-kompatiblen Einheit wird diese Funktionalität standardmäßig vom RMON2-Standard bereitgestellt. In diesem Fall muß die Software nicht heruntergeladen werden. Weitere Informationen hierzu sind im Abschnitt „RMON2-Funktionalität“ auf Seite 25 enthalten.
- Bei Verwendung einer unterstützten RMON-Einheit, die nicht über RMON2-Funktionalität verfügt, müssen Sie die Software RMON2 (ECAM) SmartAgent herunterladen, um diese Funktionalität zu erhalten. In den folgenden Abschnitten wird beschrieben, wie Sie dazu vorgehen müssen.

## Prozedur zum Herunterladen

Verwenden Sie zum Laden und Entladen der Software SmartAgent das in Abb. 71 gezeigte Dialogfenster "SmartAgent Maintenance". Klicken Sie im Dialogfenster "Device Administration" den Eintrag **SmartAgent Administration** an, um auf das Dialogfenster zuzugreifen.

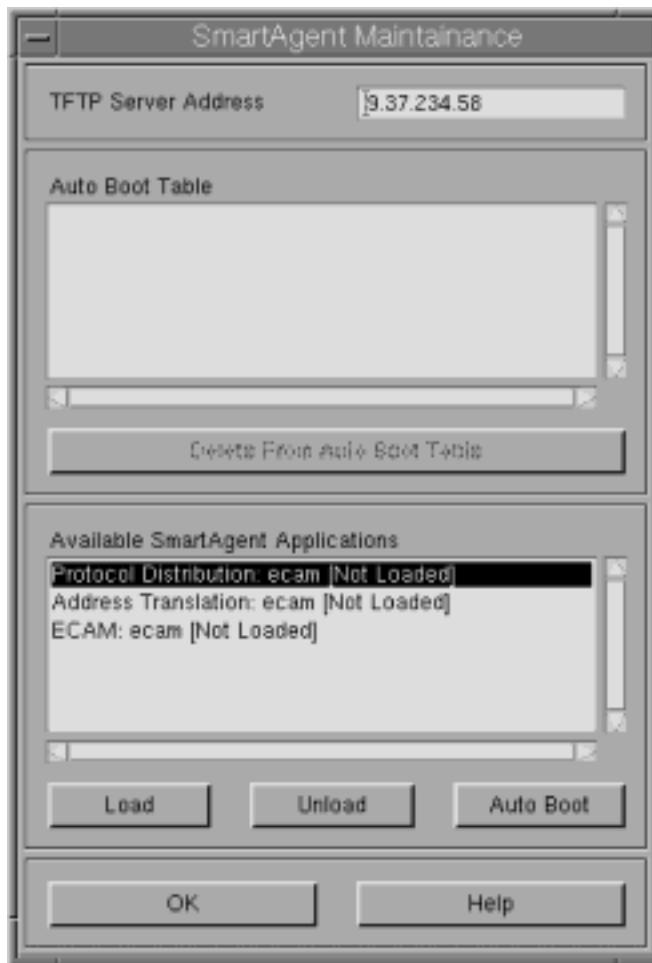


Abbildung 71. Dialogfenster "SmartAgent Maintenance"

Im Bereich "Available SmartAgent Applications" wird eine Liste mit verfügbaren Anwendungen angezeigt. Diese werden mit ihrem Anwendungsnamen gefolgt vom Namen der zugrundeliegenden Software angegeben. Hinter dem Anwendungsnamen wird der Status der Anwendung angezeigt. Wenn die Software für eine der aufgeführten Anwendungen bereits auf die Einheit heruntergeladen wurde, wird der Status [Loaded] gefolgt von der Versionsnummer und der Größe der Anwendung angezeigt.

In Form von # References wird ferner angezeigt, wie oft die jeweilige Software auf die Einheit geladen wurde, ohne daß sie von der Einheit entladen wurde.

## Anwendungen aktivieren

Die Software SmartAgent kann nur geladen werden, wenn ein aktiver TFTP-Server vorhanden ist. Anweisungen zum Starten des TFTP-Servers sind im Abschnitt „Firmware herunterladen“ auf Seite 26 enthalten.

Gehen Sie zum Laden der Software SmartAgent wie folgt vor:

1. Stellen Sie sicher, daß die Software SmartAgent auf dem TFTP-Server verfügbar ist.
2. Ändern Sie bei Bedarf im Bereich "TFTP Server" die Adresse. Standardmäßig wird die Software im Installationsverzeichnis gespeichert, und als Adresse des TFTP-Servers ist die Adresse des Host eingestellt.
3. Wählen Sie im Bereich "Available SmartAgent Applications" eine Anwendung aus. Wenn die Software für diese Anwendung auf die Einheit geladen wird, werden im Hauptfenster alle Anwendungen, denen dieselbe Software zugrundeliegt, als verfügbar angezeigt.
4. Klicken Sie die Option **Load** an. Dadurch wird von der Einheit Kontakt mit dem TFTP-Server hergestellt, und die ausgewählte Software wird geladen, falls sie verfügbar ist. Bei erfolgreichem Laden ändert sich der Status der Anwendung in [Loaded].

Wenn die Einheit die Software nicht laden kann, liegt möglicherweise eine der folgenden Ursachen vor:

- Die ausgewählte Software ist nicht auf dem angegebenen TFTP-Server gespeichert.
- Die Einheit ist nicht mehr verfügbar.
- RMON2 ist immer noch auf der Einheit aktiviert.
- Der TFTP-Server ist nicht verfügbar, oder es wurde eine falsche TFTP-Serveradresse eingegeben.

Überprüfen Sie zur Fehlerbehebung, ob die folgenden Punkte zutreffen, und wiederholen Sie dann die oben beschriebene Prozedur:

- TFTP ist im System aktiviert. (Anweisungen zum Installieren von TFTP im System sind in den Hinweisen zum jeweiligen Release enthalten.)
- RMON2 wurde auf der Einheit inaktiviert.
- Die Software SmartAgent ist im TFTP-Bereich gespeichert.
- Der verwendete Name der Benutzergemeinschaft verfügt über ausreichende Zugriffsberechtigungen. (Weitere Informationen zu Namen von Benutzergemeinschaften sind im Abschnitt „Benutzergemeinschaften für Alarmnachrichten festlegen“ auf Seite 40 enthalten.)
- Die Software SmartAgent wird von der ausgewählten Einheit unterstützt.

Kehren Sie zum Dialogfenster "Device Administration" zurück, falls die Software SmartAgent immer noch nicht geladen werden kann. Versuchen Sie, die Einheit erneut auszuwählen, um zu überprüfen, ob sie verfügbar ist.

## Anwendungen inaktivieren

Gehen Sie zum Inaktivieren von Anwendungen der Software SmartAgent wie folgt vor:

1. Wählen Sie aus der Liste "Available SmartAgent Applications" eine Anwendung aus. Der ausgewählte Eintrag muß den Status [Loaded] aufweisen.

Bei Inaktivierung einer Anwendung werden auch alle anderen Anwendungen inaktiviert, denen dieselbe Software zugrundeliegt.

2. Klicken Sie die Option **Unload** an.

- Wenn die Software zuvor erst einmal in die Einheit geladen wurde, wird der Status der Anwendung auf [Not Loaded] gesetzt.
- Wenn die Software mehr als einmal in die Einheit geladen wurde, wird als Status der Anwendung ebenfalls [Loaded] angezeigt, aber die Zahl unter "References" am Ende des Anwendungseintrags wird um die Zahl 1 verringert. Klicken Sie zum Entladen der Software von der Einheit die Option **Unload** so oft wie erforderlich an, um als Status [Not Loaded] einzustellen.

Wenn als Status weiterhin [Loaded] angezeigt wird und sich die Zahl unter "References" nicht verringert, sollten Sie überprüfen, ob Sie den Namen einer Benutzergemeinschaft mit ausreichender Zugriffsberechtigung verwenden.

## Tabelle Auto Boot

Wenn Sie auf einer Einheit die Software SmartAgent immer benötigen, können Sie die Software in der Tabelle "Auto Boot" für die Einheit registrieren lassen. In der Tabelle "Auto Boot" sind die Namen der Software enthalten, die beim Zurücksetzen durch einen Warmstart der Einheit automatisch geladen werden sollen. Außerdem wird die Adresse des TFTP-Servers angegeben, mit dem die Einheit zum Suchen der Software Kontakt herstellen muß.

### Software in der Tabelle registrieren lassen

Gehen Sie wie folgt vor, um Software in der Tabelle "Auto Boot" registrieren zu lassen:

1. Wählen Sie aus der Liste "Available SmartAgent Applications" eine Anwendung aus.
2. Klicken Sie die Option **Auto Boot** an. Der ursprüngliche Status von registrierter Software wird in der Tabelle "Auto Boot" als [Not Loaded - Idle] angezeigt.

Beachten Sie, daß in der Tabelle "Auto Boot" zwar der Name der Anwendung angezeigt wird, Sie aber lediglich die Software SmartAgent registrieren lassen, die beim nächsten Neustart der Einheit geladen werden soll. Beim Zurücksetzen der Einheit wird die gesamte Funktionalität dieser Software aktiviert.

Bei einem Warmstart zum Zurücksetzen der Einheit wird von dieser versucht, Kontakt mit dem betreffenden TFTP-Server herzustellen, um diese Software zu laden. Bei erfolgreichem Laden wird der Status der Software SmartAgent in der Tabelle "Auto Boot" auf [Autoboot Succeeded] gesetzt.

Bei fehlgeschlagenem Versuch, die Software zu laden, wird die Nachricht [Autoboot Failed] angezeigt.

### Software inaktivieren

Gehen Sie wie folgt vor, um Anwendungen zu inaktivieren und um die Software SmartAgent aus der Tabelle "Auto Boot" zu entfernen:

1. Wählen Sie die betreffende Anwendung aus der Liste "Auto Boot" aus.
2. Klicken Sie in der Tabelle "Auto Boot" die Option **Delete** an.

Die Software ist immer noch für die ihr in der Liste "Available SmartAgent Applications" zugeordneten Anwendungen verfügbar, aber bei einem Neustart der Einheit werden die Anwendungen nicht mehr erneut in die Einheit geladen.

---

## ECAM starten

Wählen Sie im Hauptfenster von Nways Manager Remote Monitor im Menü "Tools" den Eintrag "ECAM Views" aus. Im Menü "ECAM Views" sind die folgenden Optionen enthalten:

- Statistics
- Host
- Matrix
- Protocol

Diese Optionen werden weiter unten in diesem Kapitel beschrieben.

---

## ECAM-Anzeigen

In Tabelle 55 werden die verschiedenen in ECAM verfügbaren Anzeigearten dargestellt.

Tabelle 55. ECAM-Anzeigen

---

Funktion	Tabelle	Skala	Linien- diagramm	Stapel- balken- diagramm	Torten- diagramm	Balken- diagramm
Statistics	■	■	■			
Host	■	■	■			
Matrix	■	■	■			
Protocol				■	■	■
Distribution						

---

Diese verschiedenen Anzeigearten und die für sie verfügbaren Anzeigeeoptionen werden in den folgenden Abschnitten erläutert.

### Tabelle (Statistics, Host und Matrix)

Mit Hilfe der tabellarischen Darstellung können Sie Segment-, Host- und Datenaustauschstatistiken als absolute Werte, als Deltawerte oder als Ratenwerte anzeigen. Die Daten können in einem der Dateiformate ASCII oder CSV gesichert werden.

### Skala (Statistics, Host und Matrix)

Mit Hilfe der Skalendarstellung werden die Änderungsraten für jeden Protokoll Datensatz angezeigt. Für jede der erstellten Statistiken wird eine Skala angezeigt.

## Liniendiagramm (Statistics, Host und Matrix)

Mit Hilfe der Liniendiagrammdarstellung werden die erstellten Statistiken einander gegenübergestellt. Durch Auswahl eines Elements im Schlüssel kann zum Ändern der Skalierung des Diagramms der Wert der ausgewählten Variable mit einem Faktor multipliziert werden. Dadurch können Sie die Anzeige von einzelnen Statistiken hoch- oder abstufen.

## Balken-, Stapelbalken- und Tortendiagramm (nur Protocol Distribution)

In der Balkendiagrammdarstellung werden Daten zur einfachen Analyse in nebeneinander angeordneten vertikalen Balken angezeigt. Die Stapelbalken- und die Tortendiagrammdarstellung können für eine schnelle Bestimmung der relativen Protokollausfälle verwendet werden.

Wenn Sie einen Bereich innerhalb des Diagramms anklicken, wird ein Kennsatz angezeigt, der den Namen des Protokolls angibt. Außerdem gibt er an, welchen Prozentsatz des gesamten im Netzwerk gesehenen Datenverkehrs dieses Protokoll ausmacht. Klicken Sie zum Entfernen des Datenkennsatzes den Bereich erneut an.

## Anzeigeoptionen

Jede Anzeigeart weist einige verfügbare Optionen auf. Die für die einzelnen Anzeigearten bereitgestellten Funktionen werden in Tabelle 56 erläutert.

Tabelle 56 (Seite 1 von 2). Anzeigeoptionen

Anzeigeoptionen	Beschreibung
Export	Mit Hilfe dieser Funktion für tabellarische Darstellungen werden Daten in einer Datei gesichert, so daß sie in andere Anwendungen exportiert oder gedruckt werden können. Die Daten können in einem der Dateiformate ASCII oder CSV (Comma Separated Variable) gesichert werden. Bei Auswahl dieser Option wird ein Dialogfenster für die Datei angezeigt. In diesem Dialogfenster können das Datenformat und der Dateiname angegeben werden.
Print	Diese Funktion für die Anwendung "Protocol Distribution" und für Diagrammdarstellungen ermöglicht, daß Diagramme an einen PostScript-Drucker ausgegeben werden. Bei Auswahl dieser Option wird ein Dialogfenster für die Ausgabe angezeigt. In diesem Dialogfenster können ein Drucker, an den die Daten gesendet werden sollen, oder eine Datei, in der die Daten gesichert werden sollen, sowie das Layout und das Format des Papiers angegeben werden.
Grid On/Off	Mit Hilfe dieser Funktion für die Anwendung "Protocol Distribution" und für Diagrammdarstellungen kann die Darstellung von Rasterlinien in den Diagrammen ein- und ausgeschaltet werden.
Address Display Mode	In den Anzeigen "Host" und "Matrix" werden die Adreßinformationen entweder nach Namen, nach Vermittlungsschichtadresse (Network Layer Address) oder nach MAC-Adresse angezeigt. Durch die Auswahl einer dieser Optionen wird für die folgenden Aktualisierungen definiert, wie die Adressen angezeigt werden sollen.



Tabelle 56 (Seite 2 von 2). Anzeigoptionen

Anzeigoptionen	Beschreibung
Displayed Data Value	In tabellarischen Darstellungen kann das Format der angezeigten Daten geändert werden. Der absolute Wert (Absolute Value), der Deltawert (Delta Value) oder die Rate pro Sekunde (Rate per Second) können angezeigt werden. Durch die Auswahl von dieser Optionen wird für die folgenden Aktualisierungen definiert, wie die Daten angezeigt werden sollen.
Display Style	In Anzeigen des Typs "Protocol Distribution" können die Daten als Balkendiagramm, als Stapelbalkendiagramm oder als Tortendiagramm angezeigt werden. Bei Auswahl einer dieser Optionen wird der Stil der aktuellen Anzeige geändert.

Zum Berechnen des Wertes für "Rate per Second" werden von ECAM die Werte für alle Statistiken bei der letzten Aktualisierung und die aktuellen Werte verwendet. Wenn in einer tabellarischen Darstellung ein neuer Eintrag erstellt wird (z. B. wenn ein bisher nicht gesehenes Protokoll im Netzwerk angezeigt wird), verfügt ECAM über keinen bisherigen Bezugswert. In diesem Fall wird in der gesamten Tabelle standardmäßig der absolute Wert angezeigt. Wenn der Tabelle bei der nächsten Aktualisierung keine neuen Einträge hinzugefügt werden, wird die Tabelle zurückgesetzt, so daß wieder die Rate pro Sekunde angezeigt wird.

## Aktualisierung

Über die im Dialogfenster "Configuration" des Moduls angegebene Aktualisierungsrate hinaus können Sie jederzeit eine Aktualisierung erzwingen, indem Sie die Option **Update** anklicken.

---

## ECAM-Statistiken erstellen

Durch das Erstellen von ECAM-Statistiken erhalten Sie vollkommene Kontrolle über die Datenquelle und die Protokolle, für die Statistiken erstellt werden. Bei der Datenquelle kann es sich um eine der folgenden handeln:

- Physische Schnittstelle
- Virtuelle Schnittstelle
- Erfassungskonfiguration

Beispielsweise können Sie mit einer virtuellen Schnittstelle den Datenverkehr mit einem Netzwerk-Router filtern. Indem Sie ECAM zum Analysieren dieser gefilterten Daten verwenden, können Sie herausfinden, welche Protokolle über den Router gesendet werden. Wenn der Router LANs über einen teuren WAN-Link miteinander verbindet, können Sie mit Hilfe dieser Informationen herausfinden, wer den Link verwendet und zu welchem Zweck. Die Host- und Datenaustauschinformationen können dann als Grundlage für Abrechnungs- und Leistungsanalysen verwendet werden.

## Eine Datenquelle hinzufügen oder ändern

Datenquellen können für alle ECAM-Funktionen auf dieselbe Weise hinzugefügt oder geändert werden.

1. Wählen Sie im Dialogfenster "Configuration" der ECAM-Funktion eine Einheit aus der Liste "Select Device" aus.
2. Klicken Sie die Option **Add** an, um eine neue Datenquelle zu erstellen, oder klicken Sie die Option **Modify** an, um eine Datenquelle zu bearbeiten. Das Dialogfenster "Data Source" wird angezeigt.
3. Wählen Sie aus den in der Liste "Select Interface" aufgeführten verfügbaren Schnittstellen eine physische oder eine virtuelle Schnittstelle aus. Weitere Informationen zu virtuellen Schnittstellen sind im Abschnitt „IP-Adresse und Teilnetzwerkmaske einstellen“ auf Seite 29 enthalten.
4. Alle auf der ausgewählten Schnittstelle verfügbaren Protokolle werden standardmäßig in der Liste "Select Protocols" ausgewählt.
  - Klicken Sie die Option **Clear** an, um die Auswahl aller Protokolle zurückzunehmen.
  - Klicken Sie zum Auswählen aller Protokolle die Option **Select All** an.
  - Klicken Sie den entsprechenden Protokollknopf an, um spezifische Protokolle auszuwählen oder um ihre Auswahl zurückzunehmen.
5. Klicken Sie das Feld **OK** an, um diese Datenquelle zu erstellen, oder klicken Sie die Option **Cancel** an, um die Auswahl abzubrechen und zum Dialogfenster "Configuration" zurückzukehren.

Wenn Sie eine Datenquelle erstellen, wird diese in der Liste "Data Source" in Form des Schnittstellennamens gefolgt von einer Liste mit den ausgewählten Protokollen angezeigt.

---

## Protokollstatistiken

In der Anzeige "Statistics" werden Informationen zu den im Netzwerksegment entdeckten Protokollen gegeben. Für jedes Protokoll wird eine Gruppe von Statistikvariablen überwacht. Einige dieser Variablen gelten für alle Protokolle; bei anderen handelt es sich um spezifische Variablen für ein bestimmtes Protokoll. Eine Liste mit den im Modul "ECAM Statistics" verfügbaren Variablen ist im Abschnitt „ECAM-Variablen“ auf Seite 189 enthalten.

### Anzeige Protocol Statistics konfigurieren

Wählen Sie im Hauptfenster von Nways Manager Remote Monitor im Menü "ECAM" den Eintrag "Statistics" aus, um das Dialogfenster "ECAM Statistics Configuration" zu öffnen.

1. Wählen Sie aus der Liste "Select Device" die Einheit aus, deren Statistiken Sie analysieren möchten.

Wenn die Software RMON2 (ECAM) SmartAgent nicht heruntergeladen ist, wird ein Dialogfenster angezeigt, mit dessen Hilfe die Software geladen werden kann. Erläuterungen zum Laden der Software in die Einheit und zum Entladen der Software von der Einheit sind im Abschnitt „Software SmartAgent herunterladen“ auf Seite 192 enthalten.

2. Wählen Sie aus der Liste "Select Source" die Datenquelle aus, deren Statistiken Sie analysieren möchten. Klicken Sie die Option **Add** an, um eine neue Datenquelle zu erstellen, oder klicken Sie die Option **Modify** an, um eine vorhandene Datenquelle zu ändern. Weitere Informationen hierzu sind im Abschnitt „Eine Datenquelle hinzufügen oder ändern“ auf Seite 200 enthalten.
3. Eine Liste mit den im Dialogfenster "Data Source" angegebenen Protokollen wird im Bereich "View" angezeigt. Die in dieser Anzeige zu verwendende Auswahl kann eingeschränkt werden, ohne daß dies Auswirkungen auf die Liste mit Protokollen hat, die für die ausgewählte Datenquelle konfiguriert wurden.
  - a. Klicken Sie die Option **Edit View...** an, um das Dialogfenster "Protocol Selection" zu öffnen.
  - b. Nehmen Sie die Auswahl beliebiger konfigurierter Protokolle zurück, indem Sie den entsprechenden Protokollknopf anklicken. Protokolle, die nicht für diese Datenquelle konfiguriert wurden, können nicht ausgewählt werden.
  - c. Klicken Sie das Feld **OK** an, um die Änderungen zu sichern, oder klicken Sie die Option **Cancel** an, damit die Änderungen nicht wirksam werden.
4. Die Anzeige "Statistics" kann auf die folgenden drei Arten dargestellt werden: als Tabelle, in Form von Skalen oder in Form von Diagrammen (weitere Informationen hierzu sind in Tabelle 55 auf Seite 197 enthalten). Klicken Sie die benötigte Art der Anzeige (View Type) an.

5. Geben Sie im Bereich "Update Rate" an, wie oft die Anzeigen aktualisiert werden sollen. Diese Option ist nur für Skalendarstellungen und für Diagrammdarstellungen verfügbar. Durch sie wird bestimmt, wie oft die Anzeigen mit neuen Daten aktualisiert werden.

Sie können aber auch eine Aktualisierung mit Daten in der Anzeige "Statistics" erzwingen, indem Sie die Option **Update** anklicken.

6. Klicken Sie das Feld **OK** an, um das in Abb. 72 gezeigte Dialogfenster "Statistics" aufzurufen.

The screenshot shows a dialog window titled "ECAM Statistics for fd00:191:200:18:11:Free fd010 No Automatic Update". It contains a table with the following data:

	ICMP	ARP	SNMP
Packets	17	24	1004
Bytes	1953	1272	134091
Fragment Packets	0	0	0
Fragment Bytes	0	0	0
Broadcast Packets	0	0	0
Broadcast Bytes	0	0	0
Echo Request (Pkts)	8	--	--
Echo Reply (Pkts)	8	--	--
Network Unreachable (Pkts)	0	--	--
Host Unreachable (Pkts)	0	--	--
Port Unreachable (Pkts)	1	--	--
Time Exceeded (Pkts)	0	--	--
Redirect (Pkts)	0	--	--
Other Message (Pkts)	0	--	--
ARP Request (Pkts)	--	24	--

At the bottom of the dialog, there are four buttons: "OK", "Options", "Update", and "Help".

Abbildung 72. Dialogfenster "ECAM Statistics"

Eine Beschreibung der für die Diagrammdarstellung verfügbaren Multiplikatorfunktion ist im Abschnitt „Liniendiagramm (Statistics, Host und Matrix)“ auf Seite 198 enthalten.

---

## Host-Protokollstatistiken

Analog zur Funktion "Statistics" werden von der Funktion "Host" im Netzwerksegment entdeckte Protokollstatistiken überwacht. Allerdings werden Statistiken nicht nur für das Segment, sondern für jeden Host erstellt.

Host-Informationen können als Tabelle oder - für Stationsanzeigen - in Form von Skalen oder Diagrammen angezeigt werden. Durch Informationen zu einzelnen Hosts kann die Leistung spezifischer Protokolle für die jeweilige Einheit überwacht werden.

## Anzeige Host Protocol Statistics konfigurieren

Wählen Sie zum Öffnen des Dialogfensters "ECAM Host Configuration" im Menü "Tools" den Eintrag **ECAM View** aus, und wählen Sie anschließend den Eintrag **Host** aus.

1. Wählen Sie aus der Liste "Select Device" die Einheit aus, deren Host-Protokollstatistiken Sie analysieren möchten.

Wenn die Software RMON2 (ECAM) SmartAgent nicht heruntergeladen ist, wird ein Dialogfenster angezeigt, mit dessen Hilfe die Software geladen werden kann. Erläuterungen zum Laden der Software in die Einheit und zum Entladen der Software von der Einheit sind im Abschnitt „Software SmartAgent herunterladen“ auf Seite 192 enthalten.

2. Wählen Sie aus der Liste "Select Source" die Datenquelle aus, deren Host-Statistiken Sie analysieren möchten. Klicken Sie die Option **Add** an, um eine neue Datenquelle zu erstellen, oder klicken Sie die Option **Modify** an, um eine vorhandene Datenquelle zu ändern. Weitere Informationen hierzu sind im Abschnitt „Eine Datenquelle hinzufügen oder ändern“ auf Seite 200 enthalten.
3. Je nachdem, was Sie überprüfen möchten, können Sie Host-Einträge auf die folgenden verschiedenen Weisen sortieren:

### **By Protocol**

Host-Einträge werden nach ihrem Protokolltyp sortiert (nur im Tabellenformat).

### **By Address**

Host-Einträge werden nach IP-Adressen und anschließend nach Protokoll sortiert (nur im Tabellenformat).

### **By Selected Stations**

Einträge werden nach der angegebenen Station und dann nach Protokoll sortiert (im tabellarischen Format, als Skalen oder im Diagrammformat).

Bei Auswahl der Option "By Selected Stations" wird der Knopf "Select" aktiviert. Klicken Sie zum Öffnen des Dialogfensters "Station Select" die Option "Select" an, und geben Sie die Stationen an, die in der Anzeige enthalten sein sollen. Eine Beschreibung des Prozesses zur Stationsauswahl ist im Abschnitt „Dialogfenster Station Select verwenden“ auf Seite 80 enthalten.

4. Die Anzeige "Host" kann als Tabelle oder - für Anzeigen des Typs "By Selected Station" - in Form von Diagrammen oder Skalen angezeigt werden. Wählen Sie eine Art der Anzeige (View Type) durch Anklicken aus.
5. Geben Sie im Bereich "Update Rate" an, wie oft die Anzeigen aktualisiert werden sollen. Diese Option ist nur für Skalendarstellungen und für Diagrammdarstellungen verfügbar. Durch sie wird bestimmt, wie oft die Anzeigen mit neuen Daten aktualisiert werden.

Sie können aber auch eine Aktualisierung mit Daten in der Anzeige "Host" erzwingen, indem Sie die Option **Update** anklicken.

6. Klicken Sie das Feld **OK** an, um das in Abb. 73 gezeigte Dialogfenster "Host" aufzurufen.

The screenshot shows a dialog window titled "Host Statistics" with a table of network statistics. The table has four columns representing different hosts and several rows representing different types of network traffic. The data is as follows:

	45449c11 80000a5c83	45449c11 80000a5d79	45449c11 80000a5e172	45449c11 80000a5e300
In Packets	41	41	76	8
Out Packets	41	41	76	9
In Bytes	2752	2638	47001	600
Out Bytes	2802	2814	5246	512
In Fragment Packets	0	0	0	0
Out Fragment Packets	0	0	0	0
In Fragment Bytes	0	0	0	0
Out Fragment Bytes	0	0	0	0
Out Broadcast Packets	0	0	0	0

At the bottom of the dialog, there are four buttons: "OK", "Options", "Update", and "Help".

Abbildung 73. Dialogfenster "ECAM Host"

Eine Beschreibung der für die Diagrammdarstellung verfügbaren Multiplikatorfunktion ist im Abschnitt „Liniendiagramm (Statistics, Host und Matrix)“ auf Seite 198 enthalten.

---

## Matrixprotokollstatistiken

Wie von der Funktion "Statistics" werden von der Funktion "Matrix" im Netzwerksegment entdeckte Protokollstatistiken überwacht. Allerdings werden Statistiken nicht für das Segment, sondern für jeden Datenaustausch zwischen Hosts erstellt.

### Anzeige Matrix Protocol Statistics konfigurieren

Wählen Sie zum Öffnen des Dialogfensters "ECAM Matrix Configuration" im Menü "Tools" den Eintrag "ECAM Views" aus, und wählen Sie anschließend den Eintrag "Matrix" aus.

1. Wählen Sie aus der Liste "Select Device" die Einheit aus, deren Statistiken Sie analysieren möchten.

Wenn die Software RMON2 (ECAM) SmartAgent nicht heruntergeladen ist, wird ein Dialogfenster angezeigt, mit dessen Hilfe die Software geladen werden kann. Erläuterungen zum Laden der Software in die Einheit und zum Entladen der Software von der Einheit sind im Abschnitt „Software SmartAgent herunterladen“ auf Seite 192 enthalten.

2. Wählen Sie aus der Liste "Select Source" die Datenquelle aus, deren Statistiken Sie analysieren möchten. Klicken Sie die Option **Add** an, um eine neue Datenquelle zu erstellen, oder klicken Sie die Option **Modify** an, um eine vorhandene Datenquelle zu ändern. Weitere Informationen hierzu sind im Abschnitt „Eine Datenquelle hinzufügen oder ändern“ auf Seite 200 enthalten.
3. Je nachdem, was Sie überprüfen möchten, können Sie Matrixeinträge nach Adresse (By Address) oder nach ausgewählter Station (By Selected Station) sortieren.

**By Address** Host-Einträge werden nach IP-Adressen und anschließend nach Protokoll sortiert (nur im Tabellenformat).

**By Selected Station** Einträge werden nach der angegebenen Station und dann nach Protokoll sortiert (im tabellarischen Format, als Skalen oder im Diagrammformat).

Bei Auswahl der Option "By Selected Station" wird der Knopf "Select" aktiviert. Klicken Sie zum Öffnen des Dialogfensters "Station Select" die Option **Select** an, und geben Sie die Stationen an, die in der Anzeige enthalten sein sollen. Eine Beschreibung des Prozesses zur Stationsauswahl ist im Abschnitt „Dialogfenster Station Select verwenden“ auf Seite 80 enthalten.

4. Die Anzeige "Matrix" kann als Tabelle oder - für Anzeigen des Typs "by Selected Station" - in Form von Diagrammen oder Skalen angezeigt werden. Wählen Sie die erforderliche Art der Anzeige (View Type) aus.

5. Geben Sie im Bereich "Update Rate" an, wie oft die Anzeigen aktualisiert werden sollen. Diese Option ist nur für Skalendarstellungen und für Diagrammdarstellungen verfügbar. Durch sie wird bestimmt, wie oft die Anzeigen mit neuen Daten aktualisiert werden. Sie können aber auch eine Aktualisierung der Daten in der Anzeige "Matrix" erzwingen, indem Sie die Option **Update** anklicken.
6. Klicken Sie zum Aufrufen der Anzeige "Matrix" das Feld **OK** an.

Eine Beschreibung der für die Diagrammdarstellung verfügbaren Multiplikatorfunktion ist im Abschnitt „Liniendiagramm (Statistics, Host und Matrix)“ auf Seite 198 enthalten.

---

## Anwendung Protocol Distribution

Mit Hilfe der Anwendung "Protocol Distribution" wird eine zusammenfassende Anzeige der entdeckten Protokolle bereitgestellt. Bei den Protokollen handelt es sich sowohl um Protokolle, die in einem einzelnen Netzwerksegment entdeckt wurden, als auch um solche, die für einen bestimmten Host spezifisch sind. In der Anzeige wird die relative Verwendung der einzelnen überwachten Protokolle sowohl nach Paket- als auch nach Byte-Rate dargestellt.

Mit Hilfe der Anwendung "ECAM Protocol Distribution" erhalten Sie einen schnellen Überblick über die Protokolle und Anwendungen, die das Netzwerk benutzen, und können sich dann auf die Anwendungen konzentrieren, die von einem bestimmten Host verwendet werden.

## Anzeige Protocol Distribution konfigurieren

Wählen Sie zum Öffnen des Dialogfensters "ECAM Protocol Distribution Configuration" im Menü "Tools" den Eintrag "ECAM Views" aus, und wählen Sie anschließend den Eintrag "Protocol" aus.

1. Wählen Sie aus der Liste "Select Device" die Einheit aus, deren Statistiken Sie analysieren möchten. Wenn die Software RMON2 (ECAM) SmartAgent nicht heruntergeladen ist, wird ein Dialogfenster angezeigt, mit dessen Hilfe die Software geladen werden kann. Erläuterungen zum Laden der Software in die Einheit und zum Entladen der Software von der Einheit sind im Abschnitt „Software SmartAgent herunterladen“ auf Seite 192 enthalten.
2. Wählen Sie aus der Liste "Select Source" die Datenquelle aus, deren Statistiken Sie analysieren möchten. Klicken Sie die Option **Add** an, um eine neue Datenquelle zu erstellen, oder klicken Sie die Option **Modify** an, um eine vorhandene Datenquelle zu ändern. Weitere Informationen hierzu sind im Abschnitt „Eine Datenquelle hinzufügen oder ändern“ auf Seite 200 enthalten.
3. Wählen Sie im Bereich "Calculate Distribution" die Art und Weise aus, wie die Protokollverteilung (Protocol Distribution) berechnet werden soll:

### **By Selected Source**

Die gesamte Protokollverteilung für das überwachte Netzwerk wird angezeigt.

### **By Selected Stations**

Die Protokollverteilung für jede der ausgewählten Stationen wird angezeigt.



Bei Auswahl der Option "By Selected Stations" wird der Knopf "Select" aktiviert. Klicken Sie zum Öffnen des Dialogfensters "Station Select" die Option "Select" an und geben Sie die Stationen an, die in der Anzeige enthalten sein sollen. Eine Beschreibung des Prozesses zur Stationsauswahl ist im Abschnitt „Dialogfenster Station Select verwenden“ auf Seite 80 enthalten.

4. Wählen Sie die die Eingangsdarstellungsweise für die Anzeige "Protocol Distribution" aus - als ein Torten-, Balken- oder Stapelbalkendiagramm. (Weitere Informationen hierzu sind im Abschnitt „ECAM-Anzeigen“ auf Seite 197 enthalten). Die Art der Anzeige kann später im Anzeigefenster über das Menü "Option" geändert werden.
5. Geben Sie im Bereich "Update Rate" an, wie oft die Anzeigen aktualisiert werden sollen.

Sie können aber auch eine Aktualisierung der Daten in der Anzeige "Protocol Distribution" erzwingen, indem Sie die Option **Update** anklicken.

6. Klicken Sie zum Aufrufen der Anzeige "Protocol Distribution" das Feld **OK** an.

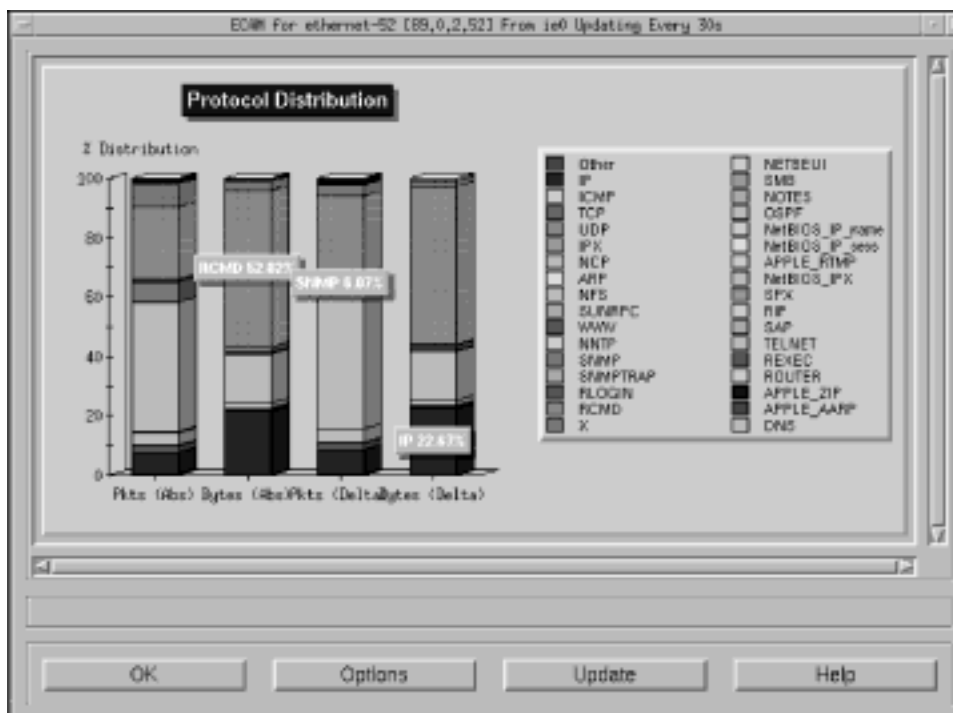


Abbildung 74. Beispiel für ein Diagramm des Typs "Protocol Distribution" mit Datenkennsätzen

## Anzeige Protocol Distribution

In den Diagrammen des Typs "Protocol Distribution" wird der Prozentsatz des gesamten Datenverkehrs im Netzwerk angezeigt, der für jedes ausgewählte Protokoll generiert wird. Die Anzeige wird während des Anzeigens gemäß der in der Anzeige "Protocol Distribution" angegebenen Aktualisierungsrate (Update Rate) automatisch aktualisiert.

Sie können die Daten aber auch zu jedem beliebigen Zeitpunkt aktualisieren, indem Sie die Option **Update** anklicken.

Verwenden Sie zum Umschalten zwischen den Anzeigearten die im Menü "Options" verfügbare Option "Display Style". Erläuterungen zu den über das Menü "Options" verfügbaren Funktionen sind in Tabelle 56 auf Seite 198 enthalten.

Zur einfachen Identifikation ist jedes Protokoll farbcodiert. Außerdem wird durch Anklicken des entsprechenden Teils des Diagramms ein Datenkennsatz für das Protokoll angezeigt, das den Namen des Protokolls und seinen Verteilungsprozentsatz angibt. Klicken Sie das Diagramm erneut an, um den Datenkennsatz zu entfernen.

Bei einem Neustart der Einheit wird ausgewählte Software geladen. Software für die ausgewählten Anwendungen wird auf die Einheit geladen.

---

## Anhang G. Häufig auftretende Probleme

In diesem Abschnitt werden häufig auftretende Probleme und bekannte Mängel von Nways Manager Remote Monitor beschrieben.

### **NMDsc06794**

Bei einer Aufrüstung von Nways Manager Remote Monitor wird während des Installationsprozesses möglicherweise die folgende Warnung angezeigt: "The dcserver is still running. If you continue the installation it will be shut down. Do you want to continue?" Diese Nachricht wird möglicherweise sogar dann angezeigt, wenn ein vollständiger Systemabschluß für Nways Manager Remote Monitor durchgeführt wurde.

**Reaktion:** Der Prozeß "dcserver" wird nie abgebrochen, auch dann nicht, wenn für Nways Manager Remote Monitor ein Systemabschluß durchgeführt wurde. Wenn keine Kopien von Nways Manager Remote Monitor oder von Nways Manager - Traffic Monitor aktiv sind, ist es ungefährlich, dem Installationsprozeß den Abbruch des Prozesses "dcserver" zu erlauben, indem Sie die oben dargestellte Warnung mit "yes" beantworten.

### **NMDsc06879**

Beim Starten von Nways Manager Remote Monitor über OpenView wird die ausgewählte Einheit möglicherweise nicht sofort von Nways Manager Remote Monitor erkannt - Das Dialogfenster "Modify Current View" wird geöffnet, und im Diagramm im Hauptfenster wird die Nachricht "No Device Selected" angezeigt. Dies wird dadurch verursacht, daß von OpenView nicht genügend Informationen zu der Einheit verfügbar gemacht werden, um es Nways Manager Remote Monitor zu ermöglichen, sofort auf die Einheit zuzugreifen.

**Reaktion:** Geben Sie zur Lösung dieses Problems die IP-Adresse der Einheit und den Namen der Benutzergemeinschaft manuell in das Dialogfenster "Device List Editor" ein. Auf dieses Dialogfenster können Sie über das Dialogfenster "Device Administration" zugreifen. Sie müssen diese Einzelangaben nur beim ersten Zugriff von Nways Manager Remote Monitor auf die Einheit hinzufügen.

### **Möglicherweise werden zusätzliche Anzeigefunktionen für die Online-Hilfefunktion aufgerufen**

Unter Umständen wird jedesmal eine neue Anzeigefunktion geöffnet, wenn die Online-Hilfefunktion aus der Anwendung heraus gestartet wird.

**Reaktion:** Beenden Sie alle Anzeigefunktionen der Online-Hilfefunktion, indem Sie in der Menüleiste der Anzeigefunktion die Einträge "File" und "Exit" auswählen.

**Fehler "Error - Can't contact dcserver" oder "bad address" wird beim Starten von Nways Manager Remote Monitor angezeigt**

Dieser Fehler wird von einer Socket-Datei, ".dcserver", hervorgerufen, die sich noch von einer früheren Sitzung her, bei der kein ordnungsgemäßer Systemabschluß durchgeführt wurde oder der Prozeß "dcserver" abgestürzt ist, im Verzeichnis "/tmp" befindet. Nways Manager Remote Monitor wird gestartet, aber es können keine Diagramme zu mehreren Segmenten erstellt werden.

**Reaktion:** Lösen Sie dieses Problem wie folgt:

1. Verlassen Sie Nways Manager Remote Monitor, indem Sie den Eintrag **Exit** anklicken.
2. Ermitteln Sie, ob jemand anderes als der aktuelle Benutzer der Eigner der Socket-Datei ist. Geben Sie dazu den folgenden Befehl ein:

```
ls -l /tmp/.dcserver
```

Wenn jemand anderes der Eigner der Datei ist, sollten Sie sich mit dem Eigner abstimmen, bevor Sie fortfahren.

3. Ändern Sie Ihre Berechtigung in Superuser: su und geben Sie auf die entsprechende Systemanfrage das Kennwort ein.
4. Löschen Sie die Datei .dcserver: rm /tmp/.dcserver
5. Starten Sie Nways Manager Remote Monitor.

**Durch Entfernen von Spalten aus Diagrammen geht die richtige Skalen-/Achsenzuordnung verloren.**

Beim Entfernen von Spalten aus einem Diagramm wird für die Skalen, die auf der Achse des Diagramms angezeigt werden, möglicherweise ein unangemessener Maßstabfaktor festgelegt, so daß die Skalen möglicherweise unleserlich angezeigt werden.

---

## Anhang H. Hinweise

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 und Dienstleistungen in dieser Veröffentlichung bedeuten nicht, daß IBM diese in allen Ländern, in denen es vertreten ist, anbietet. Hinweise auf IBM Programme, Produkte oder Dienstleistungen bedeuten nicht, daß nur diese Programme, Produkte oder Dienstleistungen 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 oder andere Schutzrechte verletzen. Die Verantwortung für den Betrieb der Produkte, Programme oder Dienstleistungen in Verbindung mit Fremdprodukten und Fremddienstleistungen liegt beim Kunden, soweit nicht ausdrücklich solche Verbindungen erwähnt sind.

Für die 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.

---

### Marken

Folgende Namen sind in gewissen Ländern Marken der IBM Corporation:

IBM	Nways	AIX	NetView
-----	-------	-----	---------

UNIX ist eine eingetragene Marke und wird ausschließlich von der X/Open Company Limited lizenziert.

Microsoft, Windows und das Logo von Windows 95 sind Marken der Microsoft Corporation.

Pentium® ist in gewissen Ländern eine Marke oder eine eingetragene Marke der Intel Corporation.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken anderer Unternehmen sein.



---

## Glossar

**Abbruch.** Dies ist dasselbe wie ein interner Token-Ring-Fehler, abgesehen davon, daß die Störung während der Übertragung eines Rahmens aufgetreten ist. Es handelt sich um einen eingrenzbaeren Fehler.

**AC.** Hierbei handelt es sich um das Zugriffssteuerungsfeld (Access Control) in der Rahmenkopfzeile.

**ACE.** Fehler in kopierter Adresse (Address Copied Error). Wenn eine Station diese Meldung ausgibt, deutet dies eher auf ein Problem mit der Station hinter dieser Station hin als auf ein stationsinternes Problem. Normalerweise handelt es sich um eine andere Station im Token-Ring mit der Adresse dieser Station. Es handelt sich um einen eingrenzbaeren Fehler.

**Adapter.** Jede Station eines Token-Ring ist über einen Token-Ring-Adapter mit dem Ring verbunden. Der Adapter verfügt über einen eigenen Mikroprozessor und über eigene Software. Also beeinträchtigt eine ringspezifische Verarbeitung - z. B. die Zuständigkeiten der aktiven Überwachung - nicht die Leistung der Station.

**Aktive Überwachung.** Die nach Belieben gewählte aktive Überwachung ist der für die Generierung des Token zuständige Adapter, wenn es auf einem Token-Ring verloren geht oder beschädigt wird.

**AMP.** (Active Monitor Present) - ein Rahmen-Broadcast, den die aktive Überwachung periodisch auf einem Token-Ring rundsendet, um den Ringaufruf zu starten.

**Anwendungsschicht.** Dies ist die siebte Schicht, der oberste Teil des OSI-Vermittlungsschichtenmodells. Diese Schicht enthält die Benutzer- und Anwendungsprogramme.

**Auslöser.** Ein Auslöser stellt eine Folge von Ereignissen dar, die in einem Netzwerk auftreten können. Wenn diese Ereignisse auftreten, wird ein Alarm ausgelöst.

**Backbone.** Dies ist der Teil eines Netzwerkes, der als primärer Pfad für den Transport von Daten zwischen Netzwerksegmenten verwendet wird.

**Bandbreite.** Dies ist das Informationsvolumen, gemessen in Bit pro Sekunde, das ein Kanal übertragen kann. Die Bandbreite von Ethernet beträgt 10 Mbps, die Bandbreite von Fast Ethernet beträgt 100 Mbps. Die

FDDI-Bandbreite beträgt 100 Mbps. Die Token-Ring-Bandbreite beträgt 4/16 Mbps.

**Beacon-Nachricht.** Wenn auf einem Token-Ring ein Problem auftritt, empfängt eine Station möglicherweise Garbage-Pakete (Fehler in den Signalen des Datenstroms) oder gar nichts (Fehler durch Signalverlust). Diese Station sendet dann eine Beacon-Nachricht, um den Fehlerrahmen zu wiederholen, der die Adresse des Nearest Active Upstream Neighbor (NAUN) enthält. Wenn der NAUN sich im Beacon-Rahmen erkennt, entfernt er sich aus dem Ring und prüft sich selbst. Wenn er einen Fehler entdeckt, den er nicht beheben kann, bleibt er außerhalb des Rings, anderenfalls fügt er sich wieder ein. Wird kein Fehler gefunden, prüft die Beacon-Station sich dann selbst um herauszufinden, ob sie den Fehler verursacht. Die Beacon-Nachricht ist ein Fehler der Stufe 1.

**Bit.** Eine der Ziffern 0 oder 1, wenn sie im binären Numerierungssystem verwendet werden. Acht Bit entsprechen einem Byte.

**Bitübertragungsschicht.** Hierbei handelt es sich um die erste Schicht des OSI-Vermittlungsschichtenmodells. Diese Schicht verwaltet die Übertragung einzelner Daten-Bit über Kabelverbindungen oder irgendeinen Datenträger, der verwendet wird, um Workstations und Peripheriegeräte zu verbinden.

**Byte.** Hier wird die gesamte Bytezahl angegeben, aus denen ein Rahmen besteht - dies umfaßt auch FCS-Oktette.

**Client.** Eine Anwendung, die von Sonden oder Agenten Daten abrufen und anzeigt.

**CRC-Ausrichtungsfehler.** Hierbei handelt es sich um ein Ethernet-Paket mit einer Länge von 64 bis 1518 Oktetten (einschließlich FCS-Oktette) - nicht um eine integrale Zahl von Oktetten gleicher Länge, oder das FCS ist fehlerhaft.

**CSMA/CD-Träger.** Der Begriff bezeichnet den Mehrfachzugriff der Trägerprüfung mit Kollisionserkennung (Carrier Sense Multiple Access with Collision Detection). Dies ist das Ethernet-Protokoll, das jedem Gerät ermöglicht, eigene Datenpakete zu erstellen und zu senden. CSMA/CD wird verwendet, um exzessive Kollisionen zwischen den Paketen zu vermeiden, da sie nur unregelmäßig übertragen werden. Ein CSMA/CD-Gerät sucht zuerst nach anderen Trägern. Wenn es keine anderen

Träger erkennt, erlaubt es dem Datenpaket schließlich, übertragen zu werden. Wenn eine Kollision erkannt wird, stellt das Gerät die Übertragung ein, wartet eine beliebige Zeit lang und beginnt erneut mit der Übertragung.

**Darstellungsschicht.** Hierbei handelt es sich um die sechste Schicht des OSI-Vermittlungsschichtenmodells. Diese Schicht steuert die Formatierung und Umsetzung der Daten.

**Datenpaket (Paket).** Hierbei handelt es sich um eine Folge binärer Ziffern, einschließlich Daten- und Steuerungssignale, die über ein LAN übertragen werden.

**Datenübertragungsschicht.** Hierbei handelt es sich um die zweite Schicht des OSI-Referenzmodells. Diese Schicht ist verantwortlich für die Steuerung des Austauschs von Nachrichten.

**ED.** Endbegrenzer (Ending Delimiter) - es handelt sich um ein bestimmtes Byte, das das Ende eines Rahmens oder Token markiert.

**Eingrenzbarer Fehler.** Dies ist ein Fehler, der genau an einer spezifischen Station oder einem spezifischen Standort in einem Token-Ring ausgemacht werden kann (Informationen finden Sie auch unter 'Nicht eingrenzbarer Fehler').

**Fehler.** Token-Ring definiert 4 Fehlerstufen. Die höchste (oder schwerwiegende) Stufe ist die Beacon-Nachricht. Eine Konkurrenzsituation bei der Überwachung ist die nächste Stufe, gefolgt von der Ringfreigabe. Bei den am wenigsten schwerwiegenden Fehlern - der Stufe 1 - handelt es sich um normale Fehler.

**Fragmentpaket.** Dieser Begriff bezeichnet ein Ethernet-Paket mit einer Länge von weniger als 64 Oktetten (ausschließlich der Rahmen-Bit, aber einschließlich der FCS-Oktette) - nicht eine integrale Anzahl von Paketen gleicher Länge, oder das FCS ist fehlerhaft.

**Freigabe.** Diese tritt im Token-Ring auf und wird nach einer Konkurrenzsituation bei der Überwachung von der aktiven Überwachung gesendet. Ringfreigaberahmen räumen das Ringsegment auf und signalisieren den Beginn des normalen Betriebs. Ein Fehler der Stufe 2.

**Frequenzfehler.** Dieser Fehler tritt auf, wenn das von einem Adapter in einem Token-Ring empfangene Signal - von seinem NAUN - zu sehr von seiner eigenen internen Uhr abweicht. Dies wird häufig dadurch verursacht, daß mehr als 72 Stationen angeschlossen sind, und ist bei 16 Mbps-Arbeitsgängen weiter verbreitet.

Dieser Fehler ist auch als Abweichung bekannt. Es handelt sich hier um einen nicht eingrenzbaren Fehler.

**HDLC.** Bitorientierte Datenübertragungssteuerung (High-Level Data Link Control). Dies ist ein OSI-bitorientiertes Protokoll.

**Hop.** Der Begriff bezeichnet das Überqueren einer Brücke zwischen Token-Rings - eine Anzahl von 1 bis 8. Die Anzahl der Hops und die Hops selbst sind in einer Rahmenkopfzeile gespeichert.

**Host.** Dies ist eine Einheit oder ein Computer in einem IP-Netzwerk, mit dem Ihr System verbunden werden kann.

**ICMP.** Internet Control Message Protocol. Dies ist ein Internet Protocol, das Fehler meldet und andere Informationen liefert, die für die Verarbeitung von IP-Paketen relevant sind.

**IEEE.** Institute of Electrical and Electronics Engineers.

**IETF.** Dies ist die Internet Engineering Task Force, zu deren Zuständigkeiten die Spezifikation von Protokollen und Empfehlung von Internet-Standards über die Anfrage nach Kommentaren (RFC) gehört.

**Interner Fehler.** Es gab ein Problem mit der Herkunftsstation in einem Token-Ring. Es wurde inzwischen behoben. Dieses Problem wird häufig durch Überhitzung in einem überlasteten System verursacht. Es handelt sich um einen eingrenzbaren Fehler.

**Jabber-Paket.** Hierbei handelt es sich um ein Ethernet-Paket mit einer Länge von weniger als 1518 Oktetten (dabei sind Rahmen-Bit ausgeschlossen, aber FCS-Oktette beinhaltet) - es handelt sich nicht um eine integrale Zahl von Paketen gleicher Länge, oder das FCS ist fehlerhaft.

**Kollision.** Es handelt sich hierbei um die günstigste Schätzung der Anzahl an Kollisionen in einem Ethernet-Segment.

**Konkurrenzsituation.** Hier handelt es sich um den Prozeß, der zur Auswahl einer neuen aktiven Überwachung in einem Token-Ring verwendet wird - ausgewählt wird normalerweise die Station mit der niedrigsten Adresse. Es handelt sich um einen Fehler der Stufe 3.

**Kurzes Paket.** Informationen finden Sie unter 'Pakete geringer Länge'.

**Langes Paket.** Informationen hierzu finden Sie unter 'Überlanges Paket'.



**Leitungsfehler.** Im Token-Ring wird ein Paket erkannt, bei dem es sich nicht um eine integrale Anzahl an Oktetten gleicher Länge handelt oder das ein fehlerhaftes FCS aufweist. Normalerweise wird dieser Fehler durch elektronische Störungen (Rauschen) oder durch Kabelprobleme verursacht. Es handelt sich um einen eingrenzbarer Fehler.

**MAC-Rahmen.** Von Token-Ring werden zwei Hauptrahmenarten definiert - Datenrahmen und Ringmanagementrahmen. MAC-Rahmen (Media Access Control) werden verwendet, um die Intaktheit des Netzwerkes zu wahren und bei der Eingrenzung von Fehlern im Netzwerk zu helfen. Mit dem LANServant Manager können Sie sowohl Rahmen der MAC-Schicht (ML-Rahmen) als auch Datenrahmen überwachen (Informationen finden Sie auch unter Token-Rahmen).

**MIB.** Dies ist die Datenbank mit den Managementinformationen (Management Information Base).

**Multicasts.** Hierbei handelt es sich um fehlerfreie Pakete, die an die Adresse für selektives Rundsenden gerichtet sind. Broadcast-Pakete sind ausgeschlossen. Das selektive Rundsenden ist ähnlich dem Rundsenden, arbeitet jedoch in einem begrenzteren Bereich, z. B. werden die Multicasts möglicherweise an alle Brücken eines Rings übertragen.

**Name der Benutzergemeinschaft (Community Name).** Dieser Name ist auch als Community String bekannt. SNMP verwendet Benutzergemeinschaftsnamen, um den Zugriff auf bestimmte Gerätemanagementfunktionen zu begrenzen. Der beim Zugriff auf ein Gerät verwendete Benutzergemeinschaftsname legt fest, auf welche Funktionen zugegriffen werden kann.

**NAUN.** Hierbei handelt es sich um den Nearest Active Upstream Neighbor in einem Token-Ring (Informationen finden Sie unter Beacon-Nachricht).

**Nicht eingrenzbarer Fehler.** Dies ist ein Fehler, der nicht genau an einer spezifischen Station oder einem spezifischen Standort in einem Token-Ring ausgemacht werden kann (Informationen finden Sie auch unter 'Eingrenzbarer Fehler').

**normaler Fehler.** Dies sind Fehler im Token-Ring, die nicht schwerwiegend genug sind, um die Ringfunktion zu stoppen (Fehler der Stufe 1). Es gibt zehn normale Fehler - Leitungs-, Trenn-, Überlastungs-, interne, Abbruch-, ACE-, verlorener-Rahmen-, Token-, Frequenz- und Rahmenkopiefehler. Normale Fehler können eingrenzbar und nicht eingrenzbar sein.

**Oktett.** Dies ist eine digitale Informationseinheit, die acht binäre Ziffern (Bit) umfaßt, die einem Byte entsprechen.

**OSI.** Hierbei handelt es sich um die Open Systems Interconnection, einem Regelwerk, das von der International Standards Organization aufgestellt wurde, um die Aktivitäten zu definieren, die stattfinden müssen, wenn Computer Daten austauschen. In dem OSI-Referenzmodell gibt es sieben Schichten. Jede dieser Schichten enthält einen bestimmten Regelsatz, der an diesem Punkt des Datenaustauschs eingehalten werden muß.

**PACMIB.** Dies ist ein MIB-Abbildungsanschluß zur Anschlußadressenkorrelation (Port Address Correlation) für Host-Daten. Er sammelt Anschlußstatistiken für 3Com CoreBuilder-Geräte im Netzwerk.

**Paket.** Hierbei handelt es sich um eine Informationseinheit, die Daten und Informationen zu Ursprung und Zieladresse enthält und die als Ganzes durch ein Netzwerk geschaltet wird.

**Pakete geringer Länge.** Dies ist ein Ethernet-Paket mit einer Länge von weniger als 64 Oktetten (ausschließlich der Rahmen-Bit aber einschließlich der FCS-Oktette), das ansonsten jedoch wohlgeformt ist.

**PDN.** Öffentliches Datennetzwerk (Public Data Network).

**Protokoll.** Hierbei handelt es sich um einen Satz von Regeln und Verfahren, die den Datenaustausch zwischen zwei datenaustauschenden Systemen regeln.

**Protokollnummer.** Der Begriff bezeichnet die Anschluß- oder Programmnummer, wie sie vom Elternprotokoll definiert ist. Wenn Sie zum Beispiel ein TCP-Kindprotokoll hinzufügen, ist die Protokollnummer die TCP-Anschlußnummer.

**PSTN.** Öffentliches Telefonwählnetzwerk (Public switched telephone network).

**Puffer.** Hierbei handelt es sich um den Speicherbereich, der dem Speicher gefilterter Pakete zugeordnet ist, die vom Netzwerk erfaßt werden. Eine Sonde verfügt nur über begrenzte Ressourcen, um Pufferdaten zu speichern. Wenn einer der Puffer alle Ressourcen der Sonde verbraucht, hält er die anderen Puffer davon ab, Pakete zu speichern. Wenn Sie Ressourcen bewahren wollen, können Sie Pakete in Sektoren aufteilen oder den Puffern maximale Größen zuordnen.

**Rahmen.** Dies ist eine Datenobjektgruppe (sonst als Paket bekannt). Im Token-Ring sind die Rahmen nur drei Byte lang, während die Informationsrahmen über 18000 Byte lang sein können.

**Rahmenkopierfehler.** Dieser Fehler wird von einer Station in einem Token-Ring gemeldet, wenn sie glaubt, daß eine andere Station vielleicht dieselbe Adresse hat. Normalerweise tritt dieser Fehler aufgrund transparenter Brücken auf, die sich in den Ring öffnen. Dies stellt sehr selten ein wirkliches Problem dar. Es handelt sich hier um einen nicht eingrenzenden Fehler.

**REM.** Dies ist die Ringfehlerüberwachung (Ring Error Monitor) im Token-Ring - die funktionale Adresse, an die Fehlermeldungen gerichtet werden.

**Ringaufruf.** Alle Stationen melden alle 7 Sekunden ihre Präsenz im Token-Ring. So werden die Stationen an ihre NAUNs erinnert. Dies ist auch als Nachbarmeldung bekannt.

**Ringfreigabeereignis.** Jedesmal, wenn eine Station sich in einen Token-Ring einfügt, wird eine Unterbrechung verursacht. Dies führt zu einem Ringfreigabeereignis.

**RMON.** Fernüberwachung (Remote MONitoring). Es handelt sich um eine Untergruppe von SNMP MIB II, die Überwachungs- und Verwaltungsfunktionen bietet, indem bis zu zehn verschiedene Informationsgruppen adressiert werden. Sie ist im IETF-Dokument RFC 1757 definiert.

**RMON2.** Hierbei handelt es sich um eine Erweiterung des Funktionsbereichs von RMON, die Protokolle oberhalb der MAC-Schicht einschließt.

**Rundsenden.** Hierbei handelt es sich um alle fehlerfreien Rahmen, die für die Rundsendedresse bestimmt sind, die, mit anderen Worten, an alle Stationen des Netzwerkes gesendet werden. Einige Rundsendebetriebe sind auf das lokale Netzwerk begrenzt und einige Rundsendebetriebe können auch zu anderen Netzwerken gehen.

**SD.** Startbegrenzer (Starting Delimiter) - es handelt sich um ein bestimmtes Byte, das den Anfang eines Rahmens oder Token markiert.

**SMP.** (Standby Monitor Present) - es handelt sich um einen Rahmen, der in einem Token-Ring als Teil der Nachbarmeldung und als Antwort auf einen AMP-Rahmen von einer Ring-Station übertragen wird.

**SMT.** FDDI-Station-Management. Dieses Protokoll soll in einem hochleistungsfähigen Multistationsnetzwerk verwendet werden. Es soll mit Hilfe einer Token-Ring-Architektur und einer Lichtwellenleitertechnik als Übertragungsmedium über Entfernungen von mehreren Kilometern eine Leistung von 100Mbps erbringen.

**Sonde.** Dies ist die Station (oder der Agent), die dafür verantwortlich ist, in einem entfernten Segment Netzwerkdaten zu sammeln und sie an eine zentrale Managementstation (oder Client) weiterzuleiten. Diese Funktion wird normalerweise vom Client konfiguriert und gesteuert.

**Standard-Gateway.** Hierbei handelt es sich um die IP-Adresse eines Gerätes, normalerweise um einen Router oder ein Gateway, an die die Sonde alle Pakete sendet, die nicht für ihr Teilnetzwerk bestimmt sind.

**Station.** Eine mit dem Netzwerk verbundene Maschine - z. B. ein Datei-Server, ein PC, eine Workstation, ein Drucker oder eine Sonde.

**Systemdeskriptor.** Es handelt sich hier um ein unformatiertes Feld auf RMON-Einheiten, das von Herstellern verwendet wird, um grundlegende Informationen zur Einheit zu liefern.

**Teilnetzmaske.** Ein Filtersystem für IP-Adressen. Es definiert den Abschnitt der IP-Adresse, der verwendet wird, um das Teilnetzwerk zu identifizieren. Der restliche Abschnitt wird dazu verwendet, Host-Informationen darzustellen. Die Einheiten und Router verwenden die Maske, um das Teilnetzwerk zu identifizieren, auf dem sich eine Sonde befindet.

**Token-Fehler.** Dieser Fehler wird von der aktiven Überwachung gemeldet, wenn das Token beschädigt wird. Ähnlich einem Leitungsfehler sind auch Token-Fehler nicht eingrenzende Fehler. Bei einer Station, die viele Token-Fehler überträgt, liegt häufig keine Störung vor - es handelt sich dann wahrscheinlich um die aktive Überwachung.

**Token-Rahmen.** Eine Station, die eine Übertragung durchführen möchte, muß zuerst auf das Token zugreifen. Sobald sie fertig ist, sendet sie das Token an den Nachbarn vor dieser Station (downstream), der es wiederum halten oder einfach weiterleiten kann. Token-Rahmen sind 3 Byte lang.

**Transportschicht.** Hierbei handelt es sich um die vierte Schicht des OSI-Vermittlungsschichtenmodells. Sie ist verantwortlich für die Fehlerprüfung und -korrektur und für einen Teil der Nachrichtenflußsteuerung.

**Trennfehler.** Trennfehler wiegen schwerer als Leitungsfehler und werden normalerweise entweder durch eine sehr kurze Unterbrechung des Token-Ring-Kabels verursacht, oder durch das sehr kurze Auftreten von elektronischen Störungen (Rauschen), die nicht schwerwiegend genug waren, um zu einer Beacon-Nachricht zu führen. Es handelt sich um einen eingrenzbaren Fehler.

**Überlanges Paket.** Dies ist ein Ethernet-Paket mit einer Länge von mehr als 1518 Oktetten (einschließlich der FCS-Oktette), das ansonsten jedoch wohlgeformt ist.

**Überlastung.** Die Überlastung wird von einer Station in einem Token-Ring gemeldet, wenn sie einen Rahmen empfängt und nicht den Puffer zur Verfügung hat, den sie zum Speichern benötigt. Da nicht gemeldet wird, wer Daten an diesen Adapter sendet, handelt es sich hier um einen nicht eingrenzbaren Fehler.

**Verlorener Rahmen.** Dieser Begriff wird verwendet, wenn eine Station einen Rahmen um einen Token-Ring

herum überträgt und ihn nicht zurückerhält. Die Meldung wird von der Herkunftsstation ausgegeben. Es handelt sich hier um einen nicht eingrenzbaren Fehler.

**Vermittlungsschicht.** Hierbei handelt es sich um die dritte Schicht des OSI-Referenzmodells. Diese Schicht ist verantwortlich für die Steuerung des Austauschs von Nachrichten.

**Virtuelle Verbindung.** Dies ist ein schaltkreisartiger Service, der von den Softwareprotokollen eines Netzwerkes geliefert wird und der es zwei Endpunkten ermöglicht, Daten so auszutauschen, als wären sie durch einen physischen Schaltkreis verbunden. Netzwerkknoten liefern die Adressierungsinformationen, die in den Paketen benötigt werden, die die Quelldaten zur Zieladresse bringen.

**Weiterleiten.** Hier handelt es sich um den Prozeß des Sendens eines Rahmens über eine Einheit, die über das Intranet arbeitet, an eine Zieladresse.



---

## Antwort

Nways Manager Remote Monitor  
Benutzerhandbuch

IBM Form SH12-4797-00

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.







SH12-4797-00

