

ConneXview

Diagnose-Tool für Ethernet-Netzwerke Häufig gestellte Fragen

Version 2.1

11/2009

Die Informationen in der vorliegenden Dokumentation enthalten allgemeine Beschreibungen und/oder technische Leistungsmerkmale der hier erwähnten Produkte. Diese Dokumentation dient nicht als Ersatz für das Ermitteln der Eignung oder Verlässlichkeit dieser Produkte für bestimmte Verwendungsbereiche des Benutzers und darf nicht zu diesem Zweck verwendet werden. Jeder Benutzer oder Integrator ist verpflichtet, angemessene und vollständige Risikoanalysen, Bewertungen und Tests der Produkte im Hinblick auf deren jeweils spezifischen Verwendungszweck vorzunehmen. Weder Schneider Electric noch deren Tochtergesellschaften oder verbundenen Unternehmen sind für einen Missbrauch der Informationen in der vorliegenden Dokumentation verantwortlich oder können diesbezüglich haftbar gemacht werden. Wenn Sie Verbesserungs- oder Ergänzungsvorschläge haben oder Fehler in dieser Veröffentlichung gefunden haben, benachrichtigen Sie uns bitte.

Dieses Dokument darf ohne entsprechende vorhergehende, ausdrückliche und schriftliche Genehmigung durch Schneider Electric weder in Teilen noch als Ganzes in keiner Form und auf keine Weise, weder anhand elektronischer noch mechanischer Hilfsmittel, reproduziert oder fotokopiert werden.

Bei der Montage und Verwendung dieses Produkts sind alle zutreffenden staatlichen, landesspezifischen, regionalen und lokalen Sicherheitsbestimmungen zu beachten. Aus Sicherheitsgründen und um die Übereinstimmung mit dokumentierten Systemdaten besser zu gewährleisten, sollten Reparaturen an Komponenten nur vom Hersteller vorgenommen werden.

Beim Einsatz von Geräten für Anwendungen mit technischen Sicherheitsanforderungen sind die relevanten Anweisungen zu beachten.

Die Verwendung anderer Software als der Schneider Electric-eigenen bzw. einer von Schneider Electric genehmigten Software in Verbindung mit den Hardwareprodukten von Schneider Electric kann Körperverletzung, Schäden oder einen fehlerhaften Betrieb zur Folge haben.

Die Nichtbeachtung dieser Informationen kann Verletzungen oder Materialschaden zur Folge haben!

© 2009 Schneider Electric. Alle Rechte vorbehalten.

Inhaltsverzeichnis

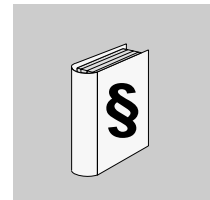


	Sicherheitshinweise	7
	Über dieses Buch	9
Kapitel 1	Häufig gestellte Fragen	11
	Kann ConneXview auf dezentrale Netzwerke zugreifen?	14
	Erkennt ConneXview alle Arten von Ethernet-Ringen?	14
	Kann ConneXview unter Verwendung eines Wireless-Ethernet-Adapters eine Erkennung ausführen?	15
	Können Geräte an den seriellen Anschlüssen eines Gateways bzw. einer Bridge erkannt werden?	15
	Können unterschiedliche Subnetze auf der gleichen Überwachungsregisterkarte erscheinen?	16
	Können in ConneXview für verschiedene Instanzen des gleichen Gerätetyps unterschiedliche Schwellwerte eingestellt werden?	16
	Werden serielle Modbus-Geräte erkannt?	16
	Kann der Editor für die Geräteeigenschaften basierend auf der Firmware-Revision eines Geräts auf "Alarm" eingestellt werden?	17
	Kann der Benutzer Schwellwerte für unterschiedliche Alarme konfigurieren?	17
	Führt ConneXview die Erkennung kontinuierlich durch?	18
	Stellt ConneXview Informationen zu allen Ethernet-Geräten zur Verfügung?	18
	Wie werden drahtlose Verbindungen in ConneXview angezeigt?	18
	Wie stelle ich Änderungen im Netzwerk fest?	19
	Wie erfahre ich die IP-Adresse des ConneXview-Computers?	19
	Wie erfahre ich den Community-Namen eines Geräts?	19
	Wie richte ich SNMP auf einem PC unter Microsoft Windows XP Professional ein?	20
	Wie kann ich Details zu aktiven Modbus-Verbindungen auf einem Gerät finden?	22
	Wie viele Modbus-Meldungen werden vom aktuellen Gerät verarbeitet?	23
	Wie viele Subnetze können gleichzeitig überwacht werden?	23
	Wie viel Datenverkehr generiert ConneXview bei einer Netzwerkerkennung?	24

Wie viel Datenverkehr generiert ConneXview bei einer Netzwerküberwachung?	25
Wie viel Datenverkehr wird von einem verwalteten Gerät generiert? . . .	25
Wie viel Datenverkehr geht in ein verwaltetes Gerät ein?	25
Wie sicher ist ConneXview? Kann ich Informationen auf die Geräte schreiben?	26
Ist ein Gerätetyp ein spezifischer Dateityp? Wo ist er gespeichert?	26
Ist es möglich, die IP-Adresse eines Geräts zu erfahren, das über eine MAC-Adresse erkannt wurde?	27
Ist es möglich, nach Geräten zu suchen?	27
Ist es möglich, die zwischen zwei Geräten ausgetauschten Informationen anzuzeigen?	28
Welches sind die wichtigsten MIB-Objekte?	29
Welche Ports und Protokolle werden von Ethernet-Geräten unterstützt?	30
Welche Sicherheitsfunktionen gehören zum Lieferumfang von ConneXview?	30
Wie entdeckt ConneXview Geräte?	31
Was bedeutet es, wenn Geräte ausschließlich anhand der MAC-Adresse erkannt werden und warum?	31
Was geschieht, wenn ein auf dem lokalen Subnetz erkanntes Gerät für ein anderes Netzwerk konfiguriert ist?	32
Was geschieht, wenn die Geräte auf einem Netzwerk unterschiedliche Community-Namen verwenden?	32
Was ist eine private MIB? Welche Informationen sind in den privaten MIB von Schneider Electric enthalten?	32
Kann ConneXview eine Netzwerkzuordnung auf einem Plotter drucken?	33
Kann ConneXview eine Liste von Alarmmeldungen und Netzwerkereignissen drucken?	34
Speichert ConneXview eine Aufzeichnung der Alarmmeldungen und Netzwerkereignisse?	35
Welche Filterkriterien kann ConneXview mit dem Ereignisprotokollfilter einsetzen?	36
Kann ConneXview bei Netzwerkalarmmeldungen SMS- oder Textnachrichten senden?	37
ConneXview zeigt das Ereignisprotokoll nicht an. Wie kann ich es öffnen?	39
In der Statusleiste in ConneXview erscheint die Meldung "Alarmüberwachung deaktiviert". Was bedeutet das, und wie kann ich sehen, welche Überwachungen deaktiviert sind?	40
Warum sendet mir der E-Mail-Benachrichtigungsdienst von ConneXview E-Mail-Nachrichten weit nach dem Auftreten eines Alarms?	41
Muss ich eine spezielle Konfiguration durchführen, wenn meinem ConneXview-Server- oder -Client-PC mehrere IP-Adressen zugeordnet sind?	42
Welches sind die Mindest-Systemanforderungen für ConneXview v2.1?	44
Wie überträgt man ConneXview-Dateien auf einen anderen PC?	45

Was ist zu tun, wenn der ETY 110WS im Netzplan ohne Verknüpfung erscheint?	46
Wie werden Geräte Dritter integriert und überwacht?	46
Wie wird eine Netzsuche mit einem Drahtlos-Adapter vorgenommen? ..	47
Was tun, wenn ConneXview mein Netz nicht ordnungsgemäß erkennen und darstellen kann?	47
Wie konfiguriere ich SNMP (Simple Network Management Protocol) in Microsoft Windows?	48
Welche Gerätetyp-Dateien sind in ConneXview v2.1 enthalten?	49
Warum verursacht ein Default Gateway (Router) in ConneXview ein Alarmereignis?	51
Was ist ein MIB-Browser und welchen soll ich verwenden?	51
Wie wird ConneXview mit geänderten Typen der installierten Geräte aktualisiert?	51
Welche Dateien werden beim Übertragen von Netz-Plänen oder Aktualisieren/Neuinstallieren von ConneXview transferiert?	52
Wie erhalte ich technische Unterstützung?	52
Glossar	53

Sicherheitshinweise



Wichtige Informationen

HINWEISE

Lesen Sie diese Anweisungen sorgfältig durch und machen Sie sich vor Installation, Betrieb und Wartung mit dem Gerät vertraut. Die nachstehend aufgeführten Warnhinweise sind in der gesamten Dokumentation sowie auf dem Gerät selbst zu finden und weisen auf potenzielle Risiken und Gefahren oder bestimmte Informationen hin, die eine Vorgehensweise verdeutlichen oder vereinfachen.



Erscheint dieses Symbol zusätzlich zu einem Warnaufkleber, bedeutet dies, dass die Gefahr eines elektrischen Schlags besteht und die Nichtbeachtung des Hinweises Verletzungen zur Folge haben kann.



Dies ist ein allgemeines Warnsymbol. Es macht Sie auf mögliche Verletzungsgefahren aufmerksam. Beachten Sie alle unter diesem Symbol aufgeführten Hinweise, um Verletzungen oder Unfälle mit Todesfälle zu vermeiden.

GEFAHR

GEFAHR macht auf eine unmittelbar gefährliche Situation aufmerksam, die bei Nichtbeachtung **unweigerlich** einen schweren oder tödlichen Unfall zur Folge hat.

WARNUNG

WARNUNG verweist auf eine mögliche Gefahr, die – wenn sie nicht vermieden wird – Tod oder schwere Verletzungen **zur Folge haben** kann.

⚠ VORSICHT

VORSICHT verweist auf eine mögliche Gefahr, die – wenn sie nicht vermieden wird – leichte Verletzungen **zur Folge haben** kann.

VORSICHT

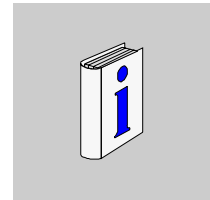
VORSICHT ohne Verwendung des Gefahrensymbols verweist auf eine mögliche Gefahr, die – wenn sie nicht vermieden wird – Materialschäden **zur Folge haben** kann.

BITTE BEACHTEN

Elektrische Geräte dürfen nur von Fachpersonal installiert, betrieben, bedient und gewartet werden. Schneider Electric haftet nicht für Schäden, die durch die Verwendung dieses Materials entstehen.

Als qualifiziertes Personal gelten Mitarbeiter, die über Fähigkeiten und Kenntnisse hinsichtlich der Konstruktion und des Betriebs dieser elektrischen Geräte und der Installationen verfügen und eine Schulung zur Erkennung und Vermeidung möglicher Gefahren absolviert haben.

Über dieses Buch



Auf einen Blick

Ziel dieses Dokuments

Das Dokument beantwortet einige häufig gestellte Fragen (FAQ, Frequently Asked Questions) zum ConneXview-Diagnose-Tool für Ethernet-Netzwerke, version 2.1.

Gültigkeitsbereich

Weiterführende Dokumentation

Titel der Dokumentation	Referenz-Nummer
ConneXview Referenzhandbuch zum Gerätetyp-Editor	31007264 (Englisch), 31008027 (Französisch), 31008028 (Deutsch), 31008029 (Italienisch), 31008030 (Spanisch)
ConneXview Referenzhandbuch zum Ethernet-Diagnose-Tool	31007263 (Englisch), 31008031 (Französisch), 31008032 (Deutsch), 31008033 (Italienisch), 31008034 (Spanisch)

Diese technischen Veröffentlichungen sowie andere technische Informationen stehen auf unserer Website www.schneider-electric.com zum Download bereit.

Benutzerkommentar

Ihre Anmerkungen und Hinweise sind uns jederzeit willkommen. Senden Sie sie einfach an unsere E-mail-Adresse: techcomm@schneider-electric.com.

Häufig gestellte Fragen

1

Übersicht

Hier sind einige häufig gestellte Fragen (FAQ, Frequently Asked Questions) zum ConneXview-Diagnose-Tool für Ethernet-Netzwerke aufgeführt.

Inhalt dieses Kapitels

Dieses Kapitel enthält die folgenden Themen:

Thema	Seite
Kann ConneXview auf dezentrale Netzwerke zugreifen?	14
Erkennt ConneXview alle Arten von Ethernet-Ringen?	14
Kann ConneXview unter Verwendung eines Wireless-Ethernet-Adapters eine Erkennung ausführen?	15
Können Geräte an den seriellen Anschlüssen eines Gateways bzw. einer Bridge erkannt werden?	15
Können unterschiedliche Subnetze auf der gleichen Überwachungsregisterkarte erscheinen?	16
Können in ConneXview für verschiedene Instanzen des gleichen Gerätetyps unterschiedliche Schwellwerte eingestellt werden?	16
Werden serielle Modbus-Geräte erkannt?	16
Kann der Editor für die Geräteeigenschaften basierend auf der Firmware-Revision eines Geräts auf "Alarm" eingestellt werden?	17
Kann der Benutzer Schwellwerte für unterschiedliche Alarmer konfigurieren?	17
Führt ConneXview die Erkennung kontinuierlich durch?	18
Stellt ConneXview Informationen zu allen Ethernet-Geräten zur Verfügung?	18
Wie werden drahtlose Verbindungen in ConneXview angezeigt?	18
Wie stelle ich Änderungen im Netzwerk fest?	19
Wie erfahre ich die IP-Adresse des ConneXview-Computers?	19
Wie erfahre ich den Community-Namen eines Geräts?	19
Wie richte ich SNMP auf einem PC unter Microsoft Windows XP Professional ein?	20

Thema	Seite
Wie kann ich Details zu aktiven Modbus-Verbindungen auf einem Gerät finden?	22
Wie viele Modbus-Meldungen werden vom aktuellen Gerät verarbeitet?	23
Wie viele Subnetze können gleichzeitig überwacht werden?	23
Wie viel Datenverkehr generiert ConneXview bei einer Netzwerkerkennung?	24
Wie viel Datenverkehr generiert ConneXview bei einer Netzwerküberwachung?	25
Wie viel Datenverkehr wird von einem verwalteten Gerät generiert?	25
Wie viel Datenverkehr geht in ein verwaltetes Gerät ein?	25
Wie sicher ist ConneXview? Kann ich Informationen auf die Geräte schreiben?	26
Ist ein Gerätetyp ein spezifischer Dateityp? Wo ist er gespeichert?	26
Ist es möglich, die IP-Adresse eines Geräts zu erfahren, das über eine MAC-Adresse erkannt wurde?	27
Ist es möglich, nach Geräten zu suchen?	27
Ist es möglich, die zwischen zwei Geräten ausgetauschten Informationen anzuzeigen?	28
Welches sind die wichtigsten MIB-Objekte?	29
Welche Ports und Protokolle werden von Ethernet-Geräten unterstützt?	30
Welche Sicherheitsfunktionen gehören zum Lieferumfang von ConneXview?	30
Wie entdeckt ConneXview Geräte?	31
Was bedeutet es, wenn Geräte ausschließlich anhand der MAC-Adresse erkannt werden und warum?	31
Was geschieht, wenn ein auf dem lokalen Subnetz erkanntes Gerät für ein anderes Netzwerk konfiguriert ist?	32
Was geschieht, wenn die Geräte auf einem Netzwerk unterschiedliche Community-Namen verwenden?	32
Was ist eine private MIB? Welche Informationen sind in den privaten MIB von Schneider Electric enthalten?	32
Kann ConneXview eine Netzwerkzuordnung auf einem Plotter drucken?	33
Kann ConneXview eine Liste von Alarmmeldungen und Netzwerkereignissen drucken?	34
Speichert ConneXview eine Aufzeichnung der Alarmmeldungen und Netzwerkereignisse?	35
Welche Filterkriterien kann ConneXview mit dem Ereignisprotokollfilter einsetzen?	36
Kann ConneXview bei Netzwerkalarmmeldungen SMS- oder Textnachrichten senden?	37

Thema	Seite
ConneXview zeigt das Ereignisprotokoll nicht an. Wie kann ich es öffnen?	39
In der Statusleiste in ConneXview erscheint die Meldung "Alarmüberwachung deaktiviert". Was bedeutet das, und wie kann ich sehen, welche Überwachungen deaktiviert sind?	40
Warum sendet mir der E-Mail-Benachrichtigungsdienst von ConneXview E-Mail-Nachrichten weit nach dem Auftreten eines Alarms?	41
Muss ich eine spezielle Konfiguration durchführen, wenn meinem ConneXview-Server- oder -Client-PC mehrere IP-Adressen zugeordnet sind?	42
Welches sind die Mindest-Systemanforderungen für ConneXview v2.1?	44
Wie überträgt man ConneXview-Dateien auf einen anderen PC?	45
Was ist zu tun, wenn der ETY 110WS im Netzplan ohne Verknüpfung erscheint?	46
Wie werden Geräte Dritter integriert und überwacht?	46
Wie wird eine Netzsuche mit einem Drahtlos-Adapter vorgenommen?	47
Was tun, wenn ConneXview mein Netz nicht ordnungsgemäß erkennen und darstellen kann?	47
Wie konfiguriere ich SNMP (Simple Network Management Protocol) in Microsoft Windows?	48
Welche Gerätetyp-Dateien sind in ConneXview v2.1 enthalten?	49
Warum verursacht ein Default Gateway (Router) in ConneXview ein Alarmereignis?	51
Was ist ein MIB-Browser und welchen soll ich verwenden?	51
Wie wird ConneXview mit geänderten Typen der installierten Geräte aktualisiert?	51
Welche Dateien werden beim Übertragen von Netz-Plänen oder Aktualisieren/Neuinstallieren von ConneXview transferiert?	52
Wie erhalte ich technische Unterstützung?	52

Kann ConneXview auf dezentrale Netzwerke zugreifen?

Ja, mit Hilfe von ConneXview können Sie auf dezentrale Netzwerke zugreifen. Standardmäßig erkennt ConneXview die mit lokal konfigurierten Schnittstellen verbundenen Netzwerke. Sie können jedoch auch die Netzwerk-IP-Adresse eines dezentralen Netzwerks eingeben, wenn zu diesem eine Verbindung besteht. ConneXview wurde mit verschiedenen Routern und virtuellen privaten Netzwerken (VPN) getestet.

So überwachen Sie ein dezentrales Netzwerk:

Schritt	Aktion
1	Wählen Sie im Menü Extras die Option Netzwerkerkennung aus.
2	Klicken Sie dann im Dialogfeld Zu erkennende Subnetze auf Hinzufügen .
3	Geben Sie die zu erkennende Netzwerk-IP-Adresse bzw. den Bereich der zu erkennenden IP-Adressen ein. Hinweis: Bei der Erkennung eines dezentralen Netzwerks müssen Sie unbedingt den Router dieses Netzwerks in den IP-Adressbereich einschließen.
4	Löschen Sie eventuell weitere Netzwerke, damit sich nur das dezentrale Netzwerk in der Liste "Parameter zur Netzwerkerkennung" befindet.
5	Klicken Sie auf OK , um mit der Erkennung zu beginnen.

HINWEIS: Wenn für die Erkennung nur ein Teil eines dezentralen Subnetzes ausgewählt ist und der Router sich nicht in diesem IP-Adressbereich befindet, müssen Sie einen zusätzlichen Teil des Subnetzes einschließen, der die IP-Adresse des Routers enthält. Dieser zusätzliche Teil braucht nicht größer als die IP-Adresse des Routers zu sein.

HINWEIS: Abhängig von der verfügbaren Bandbreite zum Erreichen eines dezentralen Netzwerks, wie z. B. eines WAN (Wide Area Network) oder einer Wahlverbindung, müssen Sie möglicherweise eine niedrige Erkennungsrate einstellen. Dies kann vor allem dann erforderlich sein, wenn Sie die Verbindung gemeinsam mit anderen Benutzern oder Diensten verwenden.

Erkennt ConneXview alle Arten von Ethernet-Ringen?

Nicht unbedingt.

ConneXview ist auf den Transparent Ready ConneXium-Ring von Schneider Electric optimiert. Dies wird über die Verwendung eines Identitätsfilters für ConneXium-Schalter erreicht.

Wenn Ihr OEM (Originalgerätehersteller) eine private MIB (Management Information Base) unterstützt, können Sie möglicherweise mit Hilfe des Gerätetyp-Editors ein benutzerdefiniertes Profil erstellen.

Kann ConneXview unter Verwendung eines Wireless-Ethernet-Adapters eine Erkennung ausführen?

Eine Überwachung kann unter Verwendung eines Wireless-Adapters ausgeführt werden; es wird jedoch empfohlen, Erkennungsvorgänge über eine Kabelverbindung auszuführen.

Auch wenn es möglich ist, einen Erkennungsvorgang über einen Wireless-Adapter auszuführen, ist dabei eventuell eine vollständige und erfolgreiche Erkennung gefährdet. Ein Erkennungsvorgang stellt viele Anforderungen an verwaltete Geräte. Der Access-Point einer drahtlosen Verbindung kann die Datenverkehrsmenge möglicherweise nicht verarbeiten. Zu den vielen zu berücksichtigenden Faktoren gehören folgende:

- die Nähe des Adapters zum Wireless-Access-Point
- die Anzahl anderer Geräte, die den Access-Point verwenden
- der Umfang der Broadcast-Aktivität anderer Geräte
- die Latenzzeit erkannter Geräte vor einer Antwort
- die Anzahl an Paketen, die auf Grund von Kollisionen verloren gehen

Wenn auf Grund von Datenstau oder verlorenen Paketen unvollständige Informationen empfangen werden, können die verwalteten Geräte möglicherweise nicht korrekt erkannt werden. Darüber hinaus können ICMP-Ping-Anfragen auf Grund von Datenstau in der drahtlosen Verbindung oder Timeout ausfallen, was dazu führt, dass nicht verwaltete Geräte nicht korrekt aufgezeichnet werden.

Die Überwachung über eine drahtlose Verbindung ist erfolgreicher als eine drahtlose Erkennung, da hier die Gerätetabelle sowie die konfigurierbaren Einstellungen für Wiederholung und Timeout in der Datenbank konfiguriert sind. Wählen Sie für Zugang zu diesen Einstellungen im Editor für Netzwerke **Bearbeiten** → **Netzwerkeinstellungen** aus.

Können Geräte an den seriellen Anschlüssen eines Gateways bzw. einer Bridge erkannt werden?

Nein, SNMP wird nicht für serielle Kommunikation unterstützt.

Eine TCP/IP-SPS kann auf diesen Geräten über das Gateway jedoch eine Abfrage durchführen und unter Verwendung von Logik einen Statuswert in die SPS schreiben. ConneXview kann daraufhin im Gerätetyp-Editor so konfiguriert werden, dass der Statuswert aus der SPS gelesen und eine Statusänderung bekannt gegeben wird, indem der Wert überwacht wird.

Können unterschiedliche Subnetze auf der gleichen Überwachungsregisterkarte erscheinen?

Ja. Auf ein- und derselben Überwachungsregisterkarte können je nach Konfiguration der Subnetzliste im Dialogfeld **Netzwerkerkennung** mehrere Subnetze überwacht werden.

Wenn eine Verbindung zu mehreren Subnetzen besteht und diese in einer Netzwerkzuordnung zusammenfasst sind, können Sie sie gemeinsam in einem Überwachungsfenster überwachen (angenommen, die Subnetze sind in die ursprüngliche Erkennung eingeschlossen).

Wenn Sie getrennte Erkennungsvorgänge ausführen und die einzelnen Subnetze in eigenen Editoren für Netzwerke erstellt und unter einem anderen Netzwerknamen gespeichert werden, müssen Sie hingegen für jedes Subnetz ein eigenes Überwachungsfenster öffnen.

Können in ConneXview für verschiedene Instanzen des gleichen Gerätetyps unterschiedliche Schwellwerte eingestellt werden?

Ja. Wenn sie einmal erkannt sind, können die Schwellwerte für jedes Gerät im Netzwerk (einschließlich Geräte desselben Gerätetyps) eindeutig festgelegt werden.

HINWEIS: Wenn ein Gerät auf dem Netzwerk entfernt und nicht gespeichert wird, in einer folgenden Erkennung jedoch erneut erkannt wird, werden die Schwellwerte auf die globalen Werte zurückgesetzt.

Werden serielle Modbus-Geräte erkannt?

Nein. ConneXview basiert auf SNMP, und SNMP wird nur über Ethernet unterstützt. Serielle Geräte unterstützen SNMP nicht und können deshalb auch nicht über ConneXview erkannt werden.

Kann der Editor für die Geräteeigenschaften basierend auf der Firmware-Revision eines Geräts auf "Alarm" eingestellt werden?

Ja, wenn es sich um Transparent Ready-Geräte von Schneider handelt. Die Firmware-Revisionsebene finden Sie im Ausstattungsprofil der Produkt-MIB unter `profileVersion`.

Wenn Sie Geräte verwenden, die nicht Transparent Ready sind, fügen Sie im ConneXview-Gerätetyp-Editor das Objekt `profileVersion` zum Gerätetyp hinzu. Die SNMP-Objekt-ID in der Schneider-MIB lautet: 1.3.6.1.4.1.3833.1.7.2.0.

Für Firmware-Aktualisierungen besuchen Sie eine der folgenden Websites:

- <http://www.schneider-electric.com>
- <http://eclipse.modicon.com>

Kann der Benutzer Schwellwerte für unterschiedliche Alarmer konfigurieren?

Ja. Wenn Sie im Editor für Netzwerke den Editor für die Geräteeigenschaften öffnen, können Sie die für ein bestimmtes Gerät anzuwendenden Alarmschwellwerte angeben.

Bereits angegebene Schwellwerte für Geräte, die im Editor für Netzwerke schon vorhanden sind, behalten die vorherigen Einstellungen bei. So aktualisieren Sie ein vorhandenes Gerät auf einen neuen Schwellwert:

Schritt	Aktion
1	Geben Sie im Editor für die Geräteeigenschaften manuell den/die Alarmschwellwert(e) für das gewünschte Gerät an.
2	Speichern Sie die Änderungen.
3	Starten Sie die Überwachung des Netzwerks, oder wählen Sie die Registerkarte Überwachung aus, wenn das Netzwerk bereits überwacht wird.
4	Auf die Aufforderung, das überwachte Netzwerk neu zu laden, antworten Sie mit Ja .

Die neuen Alarmschwellwerte sind jetzt wirksam.

Um globale Änderungen für ähnliche Geräte vorzunehmen, verwenden Sie den Gerätetyp-Editor. Öffnen Sie die Datei mit den Profilinformatoren. Wählen Sie dann beispielsweise den Prozessor "Unity Quantum" aus, indem Sie die Datei QCOPROHOST.TYP öffnen. Bearbeiten Sie hier die Schwellwerte und Alarmer für alle Unity Quantum-Prozessoren.

Führt ConneXview die Erkennung kontinuierlich durch?

Nein, ConneXview führt zu Anfang eine Erkennung durch und generiert dann eine Netzwerkzuordnung. Wenn eine erneute Erkennung des Netzwerks ausgeführt werden soll, wählen Sie im Menü **Extras** die Option **Netzwerkerkennung** aus.

Stellt ConneXview Informationen zu allen Ethernet-Geräten zur Verfügung?

Ja, jedoch in unterschiedlichem Ausmaß.

Unterstützt ein Gerät SNMP und wird damit als verwaltetes Gerät betrachtet, sind viele Informationen verfügbar. Unterstützt ein Gerät SNMP nicht, stehen hingegen nur sehr begrenzt Informationen zur Verfügung. ConneXview kann doch Dienst-Ports scannen, um Informationen zu nicht verwalteten Geräten zu erhalten. Der Umfang der von einem Gerät erhaltenen Informationen ist abhängig von:

- der Handhabbarkeit des Geräts bezüglich der Unterstützung von SNMP
- den in den Geräten konfigurierten Netzwerkparametern
- den korrekten Community-Namen während der Erkennung
- den korrekten MIB im Geräteprofil (bei Geräten von Drittanbietern)
- Modbus-TCP-Diensten, die das Gerät möglicherweise unterstützt.

Wie werden drahtlose Verbindungen in ConneXview angezeigt?

Drahtlose Verbindungen werden genau wie fest verdrahtete Verbindungen angezeigt. ConneXview stellt fest, ob eine Verbindung vorhanden ist - unabhängig von ihrer Art.

Wie stelle ich Änderungen im Netzwerk fest?

Mit Hilfe von ConneXview können Sie feststellen, ob Geräte:

- hinzugefügt wurden
- nicht länger verfügbar sind
- verschoben wurden

Um solche Änderungen anzuzeigen, führen Sie eine erneute Erkennung des Netzwerks durch, und klicken Sie dann auf **Anwenden**. ConneXview kennzeichnet Änderungen wie folgt:

- Neue Geräte werden in der Netzwerkzuordnung blau angezeigt.
- Geräte, die während des vorherigen Erkennungsvorgangs, jedoch nicht bei der erneuten Erkennung gefunden wurden, werden im Dialogfeld *Die Geräte wurden nicht gefunden* aufgeführt. Wenn Sie sich dafür entscheiden, sie zu übernehmen, werden sie in der Netzwerkzuordnung rot angezeigt. Sobald Sie im Dialogfeld **Die Geräte wurden nicht gefunden** auf *OK* klicken und das Netzwerk **speichern**, werden Sie nicht wieder benachrichtigt, es sei denn, Sie stellen das Flag *Permanent* im *Editor für die Geräteeigenschaften* auf **True** ein. In diesem Fall werden Sie nach jeder Erkennung benachrichtigt.
- Geräte, die verschoben wurden, werden in der Netzwerkzuordnung gelb angezeigt.

Wie erfahre ich die IP-Adresse des ConneXview-Computers?

Das ConneXview-Symbol repräsentiert den Computer, auf dem ConneXview ausgeführt wird.

Wie erfahre ich den Community-Namen eines Geräts?

Der Community-Name eines Geräts wird im Gerät selbst konfiguriert. Bei Geräten von Schneider Electric wird der Community-Name im Allgemeinen beim Anmelden auf der Webseite "SNMP konfigurieren" angezeigt.

Wenden Sie sich an Ihren Netzwerkadministrator, um den *Lese-Community-Namen* für einen Ethernet-Schalter, -Router, -Computer oder -Server im Dialogfeld für die Erkennung hinzuzufügen, wenn diese Namen festgelegt wurden. Andernfalls werden SNMP-Anfragen seitens ConneXview nicht bestätigt, und das betroffene Gerät wird nach der Erkennung nicht korrekt repräsentiert.

Wählen Sie unter **SNMP Community-Namen** die Option **Hinzufügen** aus, um zusätzliche *Lese-Community-Namen* einzuschließen.

Wie richte ich SNMP auf einem PC unter Microsoft Windows XP Professional ein?

SNMP muss auf einem PC unter Microsoft Windows XP Professional ausgeführt werden, damit ConneXview als verwaltetes Gerät kommunizieren kann.

SNMP wird auf dem mit dem installierten Ethernet-Adapter verbundenen PC als Dienst ausgeführt. Möglicherweise ist Ihre Windows XP-Distributions-CD-ROM erforderlich. Sie können die Unterstützung für den Dienst auch installieren, wenn Ihr IT-Administrator den Ordner "i386" auf Ihrer lokalen Festplatte gespeichert hat. Dieser Ordner enthält komprimierte Quelldateien für das Betriebssystem.

Um SNMP zu installieren, müssen Sie sich am PC als Administrator anmelden.

Schritt	Aktion
1	Gehen Sie zu Startmenü → Einstellungen → Systemsteuerung → Software
2	Wählen Sie Windows-Komponenten hinzufügen/entfernen aus.
3	Markieren Sie in der Liste den Eintrag Verwaltungs- und Überwachungsprogramme , und klicken Sie auf die Schaltfläche Details .
4	Wählen Sie SNMP Simple Network Management Protocol aus.
5	Nehmen Sie die Änderungen an, und legen Sie entweder die Windows XP-CD-ROM ein, oder gehen Sie zum Ordner "i386", um die Installation abzuschließen.

Wenn Ihr Windows XP Professional-PC den in RFC1213 definierten MIB 2-Standard unterstützt, gehen Sie wie folgt vor:

Schritt	Aktion
1	Gehen Sie zu Startmenü → Einstellungen → Systemsteuerung → Verwaltung → Dienste .
2	Doppelklicken Sie in der Liste auf den Eintrag SNMP-Dienst .

Über die Registerkarten und Auswahlmöglichkeiten auf der Eigenschaftenseite können Sie Folgendes verwalten:

- das Starten und Anhalten des SNMP-Dienstes
- die Startoptionen "Automatisch", "Manuell" und "Deaktiviert"
- das zum Anmelden von SNMP als Dienst verwendete Konto
- Wiederherstellungsoptionen bei SNMP-Startproblemen
- SNMP-Agenteneinstellungen für:
 - Kontaktperson
 - Gerätestandort
 - physikalische (MAC-) Objekte
 - IP-Objekte
 - Anwendungsobjekte
 - überwachte End-to-End-Geräte
 - DataLink-Objekte
- das Trap-Ziel, u. a.:
 - den Community-Namen zum Senden des Traps
 - die IP-Adresse der Trap-Empfänger
- Sicherheit - Community-Namen und Berechtigungen:
 - Schreibgeschützt (Standardeinstellung)
 - Benachrichtigen
 - Lesen/Schreiben
 - Lesen/Erstellen

HINWEIS: ConneXview ist ein schreibgeschütztes Diagnose-Tool.

Wie kann ich Details zu aktiven Modbus-Verbindungen auf einem Gerät finden?

Transparent Ready-Geräte von Schneider Electric, die die TFE-MIB von Schneider unterstützen, verfolgen lokale und dezentrale Modbus-TCP-Verbindungen. Um die Anzahl der Verbindungen auf einem Geräts festzustellen, wählen Sie das Gerät in der **Netzwerküberwachung** aus. Zeigen Sie die folgenden Objekte dann im **Geräteeigenschafts-Viewer** an:

Objekt	Definition
port502LocalConn	Zeigt die Anzahl der zurzeit vom <i>lokalen</i> Gerät geöffneten Verbindungen an
port503RemConn	Zeigt die Anzahl der zurzeit von dezentralen Geräten auf diesem Gerät geöffneten Verbindungen an

Die tatsächliche Anzahl der Verbindungen ist die Summe der Werte der beiden oben aufgeführten Objekte.

Um die aktuellen Verbindungen auf einem Gerät anzuzeigen, wählen Sie das Gerät in der **Netzwerküberwachung** aus. Zeigen Sie die folgenden Objekte im **Geräteeigenschafts-Viewer** an:

Objekt	Definition
port502ConnType	Gibt an, ob die Verbindung vom <i>lokalen</i> oder einem <i>dezentralen</i> Gerät geöffnet wurde
port502ConnLocalPort	Zeigt die Nummer des TCP-Ports des lokalen Geräts für jede Verbindungen an
port 502ConnRemAddress	Zeigt die IP-Adresse jedes dezentralen Geräts an
port502ConnRemPort	Zeigt die Nummer des TCP-Ports des dezentralen Geräts für jede Verbindungen an

Wie viele Modbus-Meldungen werden vom aktuellen Gerät verarbeitet?

Transparent Ready-Geräte von Schneider Electric, die die TFE-MIB von Schneider unterstützen, speichern statistische Angaben zu lokalen und dezentralen Modbus-TCP-Meldungen. Diese Statistiken umfassen die Anzahl der gesendeten und empfangenen Modbus-Meldungen.

Um die Anzahl der Meldungen einer bestimmten Verbindung festzustellen, wählen Sie das Gerät in der **Netzwerküberwachung** aus. Zeigen Sie dann die folgenden Objekte im Geräteeigenschafts-Viewer an:

Objekt	Definition
port502ConnMsgInRate	Zeigt die Anzahl der auf dieser Verbindung erhaltenen Modbus-Meldungen an/s.
port502ConnMsgOutRate	Zeigt die Anzahl der von dieser Verbindung gesendeten Modbus-Meldungen an/s.

Wie viele Subnetze können gleichzeitig überwacht werden?

Es können mehrere gleichzeitig Subnetze überwacht werden; die exakte Anzahl ist davon abhängig, wie die Netzwerke erkannt und zusammengesetzt wurden. Wenn beispielsweise eine Verbindung zu mehreren Subnetzen besteht und diese in einer einzigen Netzwerkzuordnung zusammenfasst sind, können Sie sie gemeinsam in einem Überwachungsfenster überwachen.

Wenn Sie getrennte Erkennungsvorgänge ausführen und die einzelnen Subnetze in eigenen Editoren für Netzwerke erstellt und unter einem anderen Netzwerknamen gespeichert werden, müssen Sie hingegen für jedes Subnetz ein eigenes Überwachungsfenster öffnen.

Die Höchstanzahl wird nur von der maximalen Anzahl der Überwachungsregisterkarten auf der Eigenschaftenseite und der Leistungsfähigkeit des Computers, auf dem ConneXview ausgeführt wird, begrenzt.

HINWEIS: Die beste Möglichkeit zur gleichzeitigen Überwachung von mehreren Subnetzen in einem gemeinsamen Fenster besteht darin, die gewünschten Subnetze in den Erkennungsvorgang einzuschließen und im Editor für Netzwerke daraus eine Netzwerkzuordnung zu erstellen.

Wie viel Datenverkehr generiert ConneXview bei einer Netzwerkerkennung?

Der Umfang des Datenverkehrs variiert abhängig von drei Faktoren:

1. der Gesamtanzahl möglicher IP-Adressen im Erkennungsbereich
2. der Gesamtanzahl verwalteter gegenüber nicht verwalteter Geräte
3. der im Dialogfeld **Erkennung** konfigurierten Erkennungsrate.

Beispiel: Sie haben ein Netzwerk der Klasse B (z. B. 172.16.1.0) als Netzwerkadresse und eine 16-Bit-Subnetzmaske (z. B. 255.255.0.0). In diesem Fall sind 16 Bit für Hosts verfügbar. Die Anzahl der potenziellen Hosts ist 65.535 minus 2 (die oben angegebene Netzwerkadresse und die Broadcast-Adresse 172.16.1.255). ConneXview sendet nun eine Ping-Anfrage an alle 65.533 Hosts, um zu sehen, welche antworten. Wenn die Subnetzmaske mit der obigen Netzwerk-IP-Adresse hingegen 24-Bit umfasst (z. B. 255.255.255.0), stehen 8 Bit für Hosts zur Verfügung (254 potenzielle Hosts).

Antwortet ein Gerät auf die Ping-Erkennungsanfrage, gibt ConneXview auf UDP-Port 161 eine SNMP Get-Anfrage an das Gerät aus. Antwortet das Gerät nicht, wiederholt ConneXview die Ping-Anfrage, wobei der Abstand zwischen den Anfragen jedes Mal vergrößert wird.

Für nicht verwaltete Geräte wird jeweils sehr wenig Datenverkehr generiert. Wenn ein Gerät SNMP nicht unterstützt, werden ausschließlich ICMP-Ping-Anfragen und das Scannen von Dienst-Ports wie Modbus und HTTP ausgeführt.

Antwortet ein verwaltetes Gerät auf die Anfrage, führt ConneXview zusätzliche Anfragen nach verfügbaren Objekten auf diesem Gerät durch. Abhängig von der Gesamtanzahl der verfügbaren Objekte ist die Datenverkehrsrate möglicherweise größer.

Die im Dialogfeld **Erkennung** konfigurierte Erkennungsrate erzeugt unterschiedlich viel Datenverkehr. Bei niedriger Erkennungsrate dauert die Erkennung länger, es wird jedoch auch weniger Datenverkehr generiert. Eine hohe Erkennungsrate liefert das Ergebnis schneller, generiert allerdings auch mehr Datenverkehr.

Wie viel Datenverkehr generiert ConneXview bei einer Netzwerküberwachung?

Die Menge an Datenverkehr, die bei einer Überwachung generiert wird, ist konfigurierbar. Wählen Sie hierfür in der Menüleiste **Editor für Netzwerke** die Option **Bearbeiten** → **Netzwerkeinstellungen**.

Die Datenverkehrsmenge ist abhängig von:

- der Anzahl erkannter Geräte
- der Anzahl der erkannten Geräte, die SNMP unterstützen
- der Priorität oder Häufigkeit abgefragter SNMP-Objekte
- der Priorität oder Häufigkeit von Modbus-TCP/IP-Objekten
- der Anzahl erneuter Anfrageversuche, die für SNMP und Modbus-TCP/IP konfiguriert ist
- dem Timeout-Wert zwischen den einzelnen Anfrageversuchen (ein kurzer Timeout entspricht häufigen Anfragen)

Legen Sie weniger Anfrageversuche und einen höheren Timeout-Wert fest, um während der Überwachung weniger Datenverkehr zu generieren.

HINWEIS: Im Dialogfeld "Netzwerkeinstellungen" gibt das Feld *Geschätzte durchschnittliche Auslastung des Netzwerks (KB/Sekunde)* die voraussichtliche Auslastung des Netzwerks durch den ConneXview-PC oder -Server an.

Wie viel Datenverkehr wird von einem verwalteten Gerät generiert?

So zeigen Sie die Datenverkehrsrate (Byte pro Sekunde) an, die von einem Gerät gesendet wird:

Schritt	Aktion
1	Wählen Sie in der Netzwerküberwachung das in der Netzwerkzuordnung abzufragende verwaltete Gerät aus.
2	Wählen Sie das Fenster Überwachte Geräteeigenschaften aus.
3	Blättern Sie nach unten zum Objekt IfOutOctetRate .

Wie viel Datenverkehr geht in ein verwaltetes Gerät ein?

So zeigen Sie die Datenverkehrsrate (Byte pro Sekunde) an, die in dieses Gerät eingeht:

Schritt	Aktion
1	Wählen Sie in der Netzwerküberwachung das in der Netzwerkzuordnung abzufragende verwaltete Gerät aus.
2	Wählen Sie das Fenster Überwachte Geräteeigenschaften aus.
3	Blättern Sie nach unten zum Objekt IfInOctetRate .

Wie sicher ist ConneXview? Kann ich Informationen auf die Geräte schreiben?

ConneXview ist sicher, da das Programm keine Informationen auf Netzwerkgeräte schreibt. ConneXview führt eine eigene Datenbank zu den erkannten bzw. hinzugefügten Geräten und repräsentiert diese in der Netzwerkzuordnungstologie. In Netzwerkfeldern können Gerätedaten zu Informationszwecken bearbeitet werden; diese Daten werden jedoch nicht auf die Geräte geschrieben.

ConneXview liest die in diesen erkannten Geräten gespeicherten Informationen. Während der Erkennung und Überwachung gibt ConneXview SNMP *Get-Lese*-Anfragen aus, jedoch keine *Schreib*-Anfragen.

Ist ein Gerätetyp ein spezifischer Dateityp? Wo ist er gespeichert?

Ja. Der Gerätetyp ist eine Datei: eine Vorlage mit der Dateierweiterung `.TYP`. Diese Dateien befinden sich im ConneXview-Netzwerkordner und können über den Gerätetyp-Editor bearbeitet werden.

Ein Gerätetyp enthält Folgendes:

- allgemeine Informationen
- statische SNMP-Informationen, zum Beispiel zu MIB und Grafiken
- Identitätsfilter für die Zuweisung der Objekt-ID in der Unternehmens-MIB, vorhandene MIB-Variablen oder eine Modbus-Variable
- SNMP-Objekte, die für Schwellwerte und Alarmmeldungen bearbeitet werden können
- Modbus-Informationen zum Lesen von Registern und zum Einstellen von Überwachungen
- abgeleitete Informationen zum Vergleichen von zwei Alarmwerten
- benutzerdefinierte Gruppen von Eigenschaften für rationalisierte, geordnete Überwachung sich ändernder dynamischer Eigenschaftswerte
- Popup-Informationen zum Starten einer Anwendung durch Klicken auf ein Gerät mit der rechten Maustaste

ConneXview verfügt über Gerätetypen für verwaltete und nicht verwaltete MBAP-Geräte und generische Geräte.

Darüber hinaus können Sie Gerätetypen von Drittanbietern definieren.

Ist es möglich, die IP-Adresse eines Geräts zu erfahren, das über eine MAC-Adresse erkannt wurde?

Das ist abhängig vom Gerät. Einige Geräte, z. B. das Quantum NOE, übernehmen eine IP-Adresse auf der Grundlage der Konvertierung hexadezimal-zu-dezimal der vier am wenigsten bedeutenden Byte der MAC-Adresse. Für andere Geräte, z. B. das Premium ETY, sind die ersten beiden Byte als 85.16 definiert, und die letzten zwei Byte werden aus der Konvertierung der beiden am wenigsten bedeutenden Byte der MAC-Adresse abgeleitet.

Wiederum andere Geräte, z. B. Etikettendrucker oder gar Laserdrucker, arbeiten mit dem Data Link Control-Protokoll (DLC), das Daten über das Ethernet überträgt und keine IP-Adresse erfordert.

Ausschließlich anhand einer MAC-Adresse erkannte Geräte treten dann auf, wenn die MAC-Adressentabelle in einem verwalteten Schalter auf ein Gerät auf dem physikalischen Schalter-Port hingewiesen hat.

Ist es möglich, nach Geräten zu suchen?

Es gibt keine spezifische Suchfunktion. Anhand der Funktionen von ConneXview können Sie jedoch Geräte sortieren, was den Prozess der Suche beschleunigt. Öffnen Sie im Editor für Netzwerke bzw. in der Netzwerküberwachung das Fenster **Geräte im Netzwerk**, um die Geräte nach Name, MAC-Adresse oder IP-Adresse zu sortieren.

Wenn Sie ein Geräte im Fenster **Geräte im Netzwerk** auswählen, wird es in der Netzwerkzuordnung markiert. Die Details zu diesem Gerät bzw. seine Verknüpfung werden dann im Fenster **Geräteigenschaften** angezeigt.

Ist es möglich, die zwischen zwei Geräten ausgetauschten Informationen anzuzeigen?

Ja, mit anderen Tools. ConneXview zeigt nur den Status der Modbus-TCP-Verbindung an Port 502 an, der von jedem Gerät, das mit einem anderen kommuniziert, korreliert werden kann.

ConneXview kann die lokalen und dezentralen Verbindungen an Port 502 im Fenster **Überwachte Geräteeigenschaften** in der Netzwerküberwachung angeben. ConneXview kann die zwischen zwei Geräten ausgetauschten spezifischen Informationen nicht decodieren. Hierfür ist ein Packet Sniffer erforderlich.

HINWEIS: Ein Packet Sniffer erfordert im Allgemeinen eine spezifische Netzwerktopologie. Möglicherweise müssen Sie sich diesbezüglich an einen IT-Fachmann wenden.

Ein kostenloser Open-Source-Analyzer ist unter <http://www.ethereal.com> verfügbar.

Laden Sie Ethereal herunter, und installieren Sie das Programm. Stellen Sie eine Verbindung von einem Hub zu dem zu überwachenden Gerät her. Ethereal decodiert dann Modbus-TCP-Meldungen so, dass Sie jede Anfrage und Antwort zwischen allen Geräten sehen, die mit dem überwachten Gerät kommunizieren.

Welches sind die wichtigsten MIB-Objekte?

Die wichtigsten MIB-Objekte beziehen sich auf:

- den Verbindungsstatus
- Fehler
- die Auslastung

Wählen Sie für verwaltete Geräte von Schneider Electric im Überwachungsmodus das Gerät in der Netzwerkzuordnung aus, und öffnen Sie dann das Fenster **Überwachte Geräteeigenschaften**.

Blättern Sie im Fenster **Überwachte Geräteeigenschaften** nach unten, bis die folgenden Ethernet-Fehler angezeigt werden:

- IfInDiscardRate
- IfOutDiscardRate
- IfInErrorRate
- IfOutErrorRate

Diese stehen für Fehler der Ethernet- oder MAC-Ebene.

Für IP-Layer 3-Netzwerkfehler blättern Sie weiter nach unten, bis Folgendes angezeigt wird:

- IpInHdrErrorRate
- IpInDiscardRate
- IpOutDiscardRate
- IpDiscardRate

So werden möglicherweise Broadcast Storms, Pufferüberläufe oder fehlerhafte Geräteübertragung an das überwachte Gerät dargestellt.

Für TCP-Fehler blättern Sie weiter nach unten, bis Folgendes angezeigt wird:

- TcpRetransSegRate
- TcpOutRstRate
- TcpAttemptFails

TCP-Fehler können auf eine Out-of-Socket-Bedingung oder ein dezentrales Gerät ohne Sockets hinweisen, die/das für eine TCP-Verbindung verfügbar ist. Erneute Übertragungen weisen darauf hin, dass das Ziel- oder Peer-Gerät das zuletzt übertragene TCP-Segment nicht bedienen kann.

Für allgemeine Schnittstellenfehler blättern Sie weiter nach unten, bis Folgendes angezeigt wird:

- Schnittstellenauslastung
- Schnittstellenfehlerrate
- Schnittstellen-Bandbreitenauslastung

Diese Fehler weisen auf Überlastung der Schnittstelle auf Grund von zu vielen Meldungen bezüglich Dienst- oder Broadcastverkehr, Verkabelungsproblemen oder einem fehlerhaften Schalter-Port hin.

Welche Ports und Protokolle werden von Ethernet-Geräten unterstützt?

Die von einem Gerät unterstützten Protokolle sind abhängig von den im Gerät ausgeführten Diensten. Um beispielsweise eine eingebettete Webseite wie "Transparent Ready-Geräte von Schneider Electric" zu unterstützen, wird ein Webserverprozess auf dem Gerät ausgeführt, der auf die HTTP-Webseitenanfragen antwortet.

Im Folgenden sind einige von Transparent Ready verwendeten allgemeinen Protokolle und Port-Nummern aufgeführt:

Port	Dienst	Beschreibung
21	FTP	File Transfer Protocol (Dateiübertragungsprotokoll)
23	Telnet	Dezentrale Konsole über TCP/IP
25	SMTP	Simple Mail Transfer Protocol zum Senden von E-Mail
67	BootPS	BootP Server zum Zuweisen von IP-Parametern
68	BootPC	BootP Client zum Anfordern von IP-Parametern
69	TFTP	Trivial File Transfer zum Aktualisieren von Profilen
80	HTTP	Hosting von Webseiten
161	SNMP	Simple Network Management Protocol
502	Modbus TCP	Modbus-Kommunikation

Welche Sicherheitsfunktionen gehören zum Lieferumfang von ConneXview?

ConneXview Version 1.0 umfasst keine eingebetteten Sicherheitsfunktionen wie z. B. Benutzerzugangsprofile mit Kennwortschutz.

Für die Steuerung des Zugriffs auf die ConneXview-Anwendung sollten Sie deshalb die Beschränkung des Zugangs zu dem PC in Betracht ziehen, auf dem die Anwendung installiert ist. Alternativ können Sie die Zugriffssteuerungsrichtlinien und -profile von Microsoft Windows verwenden. Zusätzliche Information zu Zugriffssteuerungsrichtlinien und -profilen finden Sie unter <http://www.microsoft.com>. Diese Verwaltungsfunktion von Windows steuert den Zugriff auf Anwendungen basierend auf der Authentifizierungsebene des Benutzerprofils.

Wie entdeckt ConneXview Geräte?

ConneXview verwendet eine Vielzahl an TCP/IP-Tools zum Erkennen von Geräten. Die Anwendung vergleicht die konfigurierte Netzwerk-IP-Adresse bzw. den Adressbereich, sowie die Subnetzmaske, die entweder für den PC konfiguriert ist, auf dem ConneXview ausgeführt wird, oder vom Benutzer angegeben wurde.

Feststellen von geeigneten Hosts ConneXview stellt die Anzahl geeigneter Hosts fest. ConneXview führt eine Ping-Anfrage für jede Adresse im geeigneten Bereich durch.

Feststellen von verwalteten Geräten An die antwortenden Geräte sendet die Anwendung dann eine SNMP-Get-Anfrage, um ISO-Informationen zu erhalten. Antwortet ein Gerät auf die SNMP-Get-Anfrage, werden weitere Anfragen gesendet, um zusätzliche Informationen zum Gerät zu erhalten.

Feststellen von nicht verwalteten Geräten Antwortet ein Gerät nicht auf eine SNMP-Get-Anfrage, unterstützt es SNMP nicht und benutzt somit nicht den TCP-Port 161 (Listening-Port, der Standard-SNMP-TCP-Dienst-Port).

Feststellen von Modbus-Geräten ConneXview sendet dann Modbus-Anfragen, um festzustellen, ob das betroffene Gerät Modbus unterstützt. Antwortet das Gerät auf die Anfrage, stellt ConneXview fest, ob das Gerät ein verwalteter oder nicht verwalteter MBAP-Host ist.

Feststellen von anderen Geräten Sie können die Zusatzanwendung zu ConneXview, den Gerätetyp-Editor, dazu verwenden, um der Netzwerkzuordnung MIB, Grafiken und andere Gerätefunktionen hinzuzufügen. Siehe auch die Hilfe zum Gerätetyp-Editor für Details zum Hinzufügen von benutzerdefinierten verwalteten und nicht verwalteten Geräten anderer Hersteller.

Was bedeutet es, wenn Geräte ausschließlich anhand der MAC-Adresse erkannt werden und warum?

Der häufigste Grund, warum ein Gerät nur mit einer MAC-Adresse erscheint, ist, dass seine IP-Adresse sich nicht im Erkennungsbereich befindet. Das Gerät kommuniziert jedoch, und seine MAC-Adresse wurde in einem Infrastrukturgerät gefunden.

Andere mögliche Gründe:

- eine auf einem dezentralen Subnetz ausgeführte Erkennung, dessen Router sich nicht im Erkennungsbereich befindet
- ConneXview verfügt nicht über den Community-Namen für diesen Router
- der Router unterstützt SNMP nicht vollständig. In diesem Fall werden die Geräte zweimal angezeigt: einmal nach ihrer IP-Adresse und einmal nach ihrer MAC-Adresse

Was geschieht, wenn ein auf dem lokalen Subnetz erkanntes Gerät für ein anderes Netzwerk konfiguriert ist?

Wenn das Gerät Datenpakete überträgt, wird es ausschließlich als MAC-Adresse angezeigt, da seine IP-Adresse sich nicht im Erkennungsbereich befindet.

Was geschieht, wenn die Geräte auf einem Netzwerk unterschiedliche Community-Namen verwenden?

Wenn Sie eine Erkennung ausführen oder ein Gerät manuell hinzufügen, können Sie auf Wunsch sowohl öffentliche als auch private Community-Namen hinzufügen.

Beim manuellen Hinzufügen eines Geräts können Sie ConneXview mit dem Community-String des Geräts konfigurieren, indem Sie das Gerät auswählen und das Feld **SNMP Community-Name** im Gerätetyp-Editor bearbeiten.

Während der Erkennung probiert ConneXview alle verfügbaren konfigurierten Community-Namen aus, um die richtige Antwort vom Gerät zu erhalten. Die Standardeinstellung umfasst lediglich einen Community-Namen, nämlich *Öffentlich*. Verwendet Ihr Gerät einen anderen Community-Namen, klicken Sie im Dialogfeld **Erkennung** im Abschnitt **Community-Namen** auf **Hinzufügen**.

Wenn nicht der Standard-Community-Name (*Öffentlich*) verwendet wird und der neue Community-Name nicht Teil der Erkennung ist, wird das Gerät als nicht verwaltetes Gerät erkannt, da SNMP-Anfragen von ConneXview von diesem zurückgewiesen werden.

Was ist eine private MIB? Welche Informationen sind in den privaten MIB von Schneider Electric enthalten?

Es gibt zwei Arten von MIB: öffentliche und private.

Informationen aus öffentlichen MIB sind generisch für viele bzw. die meisten Geräte: z. B. die Anzahl an Schnittstellen, gesendete und empfangene Byte, Schnittstellenfehler, Verbindungsstatus usw.

Informationen aus privaten MIB beschreiben die eindeutigen, nicht generischen Funktionen eines Geräts. Die private MIB von Schneider Electric enthält zum Beispiel folgende Informationen:

- E/A-Scanner
- globale Daten
- Modbus Messaging

Diese Funktionen sind nur in Modbus-TCP-Geräten von Schneider Electric zu finden.

Kann ConneXview eine Netzwerkzuordnung auf einem Plotter drucken?

Ja, vorausgesetzt der Treiber für das Drucken in großem Maßstab ist auf Ihrem PC installiert.

Wenn eine Netzwerkzuordnung im Überwachungs- oder Bearbeitungsmodus geöffnet ist, kann ConneXview Folgendes drucken:

- die gesamte Netzwerkzuordnung bzw.
- nur den Teil der Netzwerkzuordnung, der im Viewer oder Editor für die Netzwerkzuordnung sichtbar ist

Eine Netzwerkzuordnung kann wie folgt gedruckt werden:

- als einzelnes Blatt in großem Maßstab. Das Format entspricht einem ausgewählten Prozentanteil der normalen Größe der Netzwerkzuordnung.
- Als mehrere Seiten kleineren Formats, wobei sowohl Höhe als auch Breite des Ausdrucks hinsichtlich einer ausgewählten Anzahl an Seiten ausgedrückt ist.

Siehe auch die Online-Hilfe zu ConneXview im Thema zum Befehl **Drucken**, in dem Sie schrittweise Anweisungen zu den Druckoptionen in ConneXview erhalten.

Kann ConneXview eine Liste von Alarmmeldungen und Netzwerkereignissen drucken?

Ja. Wenn eine Netzwerkzuordnung im Überwachungsmodus geöffnet ist, kann ConneXview gefilterte und sortierte Listen von aktuellen Alarmmeldungen und Ereignisprotokollelementen drucken.

Drucken von aktuellen Alarmmeldungen:

Sie können bestimmen, dass eine Liste von Alarmmeldungen gedruckt wird, die Folgendes enthält:

- alle Alarmmeldungen oder
- nur Alarmmeldungen einer bestimmten Schwere ("Kritisch" oder "Achtung") oder
- nur Alarmmeldungen, die innerhalb ausgewählter Start- und Enddaten und -uhrzeiten auftreten

Sie können die zu druckende Liste aufsteigend oder absteigend nach jedem Feld sortieren, das im Fenster für die aktuellen Alarmmeldungen erscheint.

Drucken von Netzwerkereignissen:

Sie können eine Liste aller oder eines Teils des ConneXview-Ereignisprotokolls drucken. Sie können bestimmen, ob alle Ereignisprotokollelemente in die Liste aufgenommen werden sollen. Alternativ können Sie die auszudruckende Liste durch Anwenden eines oder mehrerer der folgenden Filter beschränken:

- einen Gerätefilter, der die Liste auf Ereignisse beschränkt, die sich auf ein oder mehrere ausgewählte Netzwerkgeräte beziehen
- einen Schwerefilter, der die Liste auf Ereignisse beschränkt, die sich auf ein oder mehrere ausgewählte Schweregrade ("Kritisch", "Achtung", "Information") beziehen
- einen Datumsbereichfilter, der die Liste auf Ereignisse beschränkt, die sich auf ausgewählte Start- und Enddaten und -uhrzeiten beziehen

Sie können die zu druckende Liste aufsteigend oder absteigend nach jedem Feld sortieren, das im Ereignisprotokoll erscheint.

Siehe auch die Online-Hilfe zu ConneXview im Thema zum Befehl "Drucken", in dem Sie schrittweise Anweisungen zu den Druckoptionen in ConneXview erhalten.

Speichert ConneXview eine Aufzeichnung der Alarmmeldungen und Netzwerkereignisse?

Ja. ConneXview fügt dem Ereignisprotokoll jedes Mal, wenn die Überwachung der Geräteeigenschaften eine Alarmmeldung oder ein Informationsereignis auslöst, einen neuen Eintrag hinzu.

ConneXview speichert den Verlauf von Netzwerkereignissen bis zu einer benutzerdefinierten maximalen Ereignisprotokollgröße. Nach Erreichen der maximalen Größe des Ereignisprotokolls fügt ConneXview dem Protokoll ein neues Ereignis hinzu und entfernt gleichzeitig das älteste aufgezeichnete Ereignis aus dem Protokoll.

So konfigurieren Sie die maximale Größe des Ereignisprotokolls:

Schritt	Aktion
1	Wählen Sie in ConneXview Extras → Optionen aus. Das Dialogfeld "Benutzeroptionen" wird geöffnet.
2	Wählen Sie im Abschnitt <i>Serveroptionen</i> den Eintrag Maximale Größe des Ereignisprotokolls (tausend Ereignisse) aus: <ul style="list-style-type: none"> ● 1 ● 10 (Standardeinstellung) ● 100
3	Klicken Sie auf OK , um das Dialogfeld "Benutzeroptionen" zu schließen und die Änderungen zu speichern.

HINWEIS: Das Verringern der maximalen Größe des Ereignisprotokolls wirkt sich nicht nur auf die aktuelle Zuordnung aus, sondern auf alle Zuordnungen, die anschließend in ConneXview geöffnet werden. Eine Verringerung der maximalen Größe des Ereignisprotokolls kann beim darauf folgenden Öffnen einer gespeicherten Netzwerkzuordnung den Verlust von gespeicherten Alarmmeldungen und anderen Netzwerkereignissen zur Folge haben.

Welche Filterkriterien kann ConneXview mit dem Ereignisprotokollfilter einsetzen?

ConneXview wendet benutzerdefinierte Filterkriterien auf das Ereignisprotokoll an. Sie können einen oder beide der folgenden Filter auf Ereignisprotokoll Datensätze anwenden:

- einen Datumsbereichfilter, der die Ereignisprotokollanzeige auf ausgewählte Start- und Enddaten und -uhrzeiten beschränkt
- einen Gerätefilter, der die Ereignisprotokollanzeige auf Ereignisse beschränkt, die sich auf ein ausgewähltes Netzwerkgerät beziehen



So konfigurieren Sie den Ereignisprotokollfilter:

Öffnen Sie das Ereignisprotokollfenster im Überwachungsmodus. Klicken Sie auf die Schaltfläche **Filterdialog öffnen**, die durch Auslassungspunkte markiert ist (...), um das Dialogfenster "Ereignisprotokollfilter" zu öffnen. Hier können Sie die Einstellungen für den Ereignisprotokollfilter konfigurieren.

Siehe auch das Hilfethema *Ereignisprotokollfilter* in ConneXview für schrittweise Anweisungen zur Eingabe der Einstellungen für den Ereignisprotokollfilter.

So schalten Sie den Filter ein und aus:

Klicken Sie auf die Schaltfläche **Filter aktivieren/deaktivieren**. Diese Schaltfläche zeigt eins von zwei Symbolen an (abhängig vom Status des Ereignisprotokollfilters):

- Klicken Sie auf die Schaltfläche  , um den Ereignisprotokollfilter zu aktivieren.
- Klicken Sie auf die Schaltfläche  , um den Ereignisprotokollfilter zu deaktivieren.

Siehe auch das Hilfethema *Ereignisprotokoll* in ConneXview für weitere Informationen zum Ereignisprotokoll und seinen Funktionen.

Kann ConneXview bei Netzwerkalarmmeldungen SMS- oder Textnachrichten senden?

Ja. Der Ereignisbenachrichtigungsdienst von ConneXview sendet bei Netzwerkeignissen E-Mail-Nachrichten an einen vom Benutzer angegebenen SMTP-E-Mail-Server. Dieser Dienst kann auch so konfiguriert werden, dass SMS-Nachrichten (Short Message Service) oder Textnachrichten an vorgesehene Empfänger gesendet werden.

So konfigurieren Sie ConneXview, dass SMS- oder Textnachrichten gesendet werden:

Schritt	Aktion						
1	Wählen Sie Extras → E-Mail-Konfiguration... aus, um das Dialogfeld "E-Mail-Konfiguration" zu öffnen.						
2	Konfigurieren Sie im Dialogfeld "E-Mail-Konfiguration" die folgenden Einstellungen: <table border="1" data-bbox="436 634 1226 878"> <tr> <td>a</td> <td>Geben Sie einen Hostnamen oder eine IP-Adresse für den SMTP-Server ein (maximal 255 Zeichen).</td> </tr> <tr> <td>b</td> <td>Geben Sie die "Von"-Adresse des SMTP-E-Mail-Servers in folgendem Format ein: <Local-Name>@<Domänenname>, wobei: <ul style="list-style-type: none"> ● <Local-Name> maximal 64 Zeichen haben darf ● <Domänenname> maximal 255 Zeichen haben darf </td> </tr> <tr> <td>c</td> <td>Stellen Sie anhand der Drehfelder die Sendedauer (das Intervall zwischen den einzelnen E-Mail-Übertragungen) auf 1 bis 60 Minuten ein.</td> </tr> </table>	a	Geben Sie einen Hostnamen oder eine IP-Adresse für den SMTP-Server ein (maximal 255 Zeichen).	b	Geben Sie die "Von"-Adresse des SMTP-E-Mail-Servers in folgendem Format ein: <Local-Name>@<Domänenname>, wobei: <ul style="list-style-type: none"> ● <Local-Name> maximal 64 Zeichen haben darf ● <Domänenname> maximal 255 Zeichen haben darf 	c	Stellen Sie anhand der Drehfelder die Sendedauer (das Intervall zwischen den einzelnen E-Mail-Übertragungen) auf 1 bis 60 Minuten ein.
a	Geben Sie einen Hostnamen oder eine IP-Adresse für den SMTP-Server ein (maximal 255 Zeichen).						
b	Geben Sie die "Von"-Adresse des SMTP-E-Mail-Servers in folgendem Format ein: <Local-Name>@<Domänenname>, wobei: <ul style="list-style-type: none"> ● <Local-Name> maximal 64 Zeichen haben darf ● <Domänenname> maximal 255 Zeichen haben darf 						
c	Stellen Sie anhand der Drehfelder die Sendedauer (das Intervall zwischen den einzelnen E-Mail-Übertragungen) auf 1 bis 60 Minuten ein.						
3	Klicken Sie auf Hinzufügen.... Das Dialogfeld "Empfänger hinzufügen" wird geöffnet.						
4	Führen Sie im Abschnitt "Empfänger" des Dialogfelds Folgendes aus: <table border="1" data-bbox="436 980 1226 1240"> <tr> <td>a</td> <td>Geben Sie den <i>Namen</i> des Empfängers ein (maximal 32 Zeichen). Hinweis: Dieser Name wird der Liste "Empfänger" im Fenster "E-Mail-Konfiguration" hinzugefügt.</td> </tr> <tr> <td>b</td> <td>Geben Sie im Feld <i>E-Mail-Adresse</i> Ihre Mobiltelefonnummer und die SMSC-Gateway-Adresse des Mobilfunk-Providers in folgendem Format ein: <Nummer>@<SMSC-Gateway-Adresse> Hinweis: Unten finden Sie eine inoffizielle Liste einiger häufiger Mobilfunk-Provider-Gateways. Überprüfen Sie Ihre SMSC-Gateway-Adresse bei Ihrem Mobilfunk-Provider, bevor Sie sie implementieren und sich darauf verlassen.</td> </tr> </table>	a	Geben Sie den <i>Namen</i> des Empfängers ein (maximal 32 Zeichen). Hinweis: Dieser Name wird der Liste "Empfänger" im Fenster "E-Mail-Konfiguration" hinzugefügt.	b	Geben Sie im Feld <i>E-Mail-Adresse</i> Ihre Mobiltelefonnummer und die SMSC-Gateway-Adresse des Mobilfunk-Providers in folgendem Format ein: <Nummer>@<SMSC-Gateway-Adresse> Hinweis: Unten finden Sie eine inoffizielle Liste einiger häufiger Mobilfunk-Provider-Gateways. Überprüfen Sie Ihre SMSC-Gateway-Adresse bei Ihrem Mobilfunk-Provider, bevor Sie sie implementieren und sich darauf verlassen.		
a	Geben Sie den <i>Namen</i> des Empfängers ein (maximal 32 Zeichen). Hinweis: Dieser Name wird der Liste "Empfänger" im Fenster "E-Mail-Konfiguration" hinzugefügt.						
b	Geben Sie im Feld <i>E-Mail-Adresse</i> Ihre Mobiltelefonnummer und die SMSC-Gateway-Adresse des Mobilfunk-Providers in folgendem Format ein: <Nummer>@<SMSC-Gateway-Adresse> Hinweis: Unten finden Sie eine inoffizielle Liste einiger häufiger Mobilfunk-Provider-Gateways. Überprüfen Sie Ihre SMSC-Gateway-Adresse bei Ihrem Mobilfunk-Provider, bevor Sie sie implementieren und sich darauf verlassen.						
5	Nehmen Sie in den Abschnitten <i>Kriterien senden</i> des Dialogfelds "Empfänger hinzufügen" die gewünschten Einstellungen vor. Hier können Sie das Senden von Ereignisnachrichten nach einem oder mehreren der folgenden Kriterien filtern: <ul style="list-style-type: none"> ● Ereignisschwere ● Netzwerk ● Geräte und Gerätetypen <p>Siehe auch die Online-Hilfe zu ConneXview im Thema zum Hinzufügen von Empfängern für Informationen zur Filterauswahl.</p>						

Schritt	Aktion
6	Wenn Sie alle Konfigurationseinstellungen im Dialogfeld "Empfänger hinzufügen" vorgenommen haben, klicken Sie auf OK , um die Änderungen zu speichern und das Dialogfeld zu schließen.
7	Wenn Sie alle Konfigurationseinstellungen im Dialogfeld "E-Mail-Konfiguration" vorgenommen haben, klicken Sie auf OK , um die Änderungen zu speichern und das Dialogfeld zu schließen.

Im Folgenden sind einige Gateway-Provider und ihre SMSC-Gateway-Adressen aufgeführt. Überprüfen Sie Ihre SMSC-Gateway-Adresse bei Ihrem Mobilfunk-Provider, bevor Sie sie implementieren und sich darauf verlassen.

Provider	SMSC-Gateway-Adresse
Alltel	@message.alltel.com
AT&T	@mmode.com
Bell	@txt.bell.ca
Cellular One	@mobile.celloneusa.com
Cingular	@mobile.mycingular.com
Fido	@fido.ca
Nextel	@page.nextel.com
Qwest	@qwestmp.com
Rogers Canada	@pcs.rogers.com
Sprint	@messaging.sprintpcs.com
Suncom	@tms.suncom.com
T-Mobile	@tmomail.net
Verizon	@vtext.net
Virgin Mobile Canada	@vmobile.ca
Virgin Mobile USA	@vmobil.com
Vodacom South Africa	@voda.co.za

ConneXview zeigt das Ereignisprotokoll nicht an. Wie kann ich es öffnen?

Das Ereignisprotokoll ist eine neue Funktion in ConneXview ab Version 2.0. Für Netzwerkzuordnungen, die mit ConneXview Version 1.0 erstellt wurden, wird zunächst kein Ereignisprotokoll angezeigt. Sie können Netzwerkzuordnungen der Version 1.0 jedoch ein Ereignisprotokoll hinzufügen.

So fügen Sie Netzwerkzuordnungen, die in ConneXview, Version 1.0, erstellt wurden, ein Ereignisprotokoll hinzu:

Schritt	Aktion
1	Verwenden Sie ConneXview Version 2.0 (oder höher), und öffnen Sie die betreffende Netzwerkzuordnung aus Version 1.0 im Bearbeitungsmodus.
2	Speichern Sie die Netzwerkzuordnung.
3	Wenn die Netzwerkzuordnung im Überwachungsmodus geöffnet ist, schließen Sie diesen.
4	Öffnen Sie die gespeicherte Netzwerkzuordnung im Überwachungsmodus. ConneXview fügt dem Fenster "Aktuelle Alarmmeldungen" eine Registerkarte "Ereignisprotokoll" hinzu.
5	Klicken Sie auf diese Registerkarte, um sie zu öffnen. Hinweis: Das neu erstellte Ereignisprotokoll enthält nur Elemente, die nach der Erstellung des Ereignisprotokolls auftreten.

In der Statusleiste in ConneXview erscheint die Meldung "Alarmüberwachung deaktiviert". Was bedeutet das, und wie kann ich sehen, welche Überwachungen deaktiviert sind?

Alarmüberwachung deaktiviert zeigt für ein verwaltetes Gerät an, dass entweder:

- das Attribut *Überwachung* einer Werteüberwachung **deaktiviert** ist, während das Attribut *Überwachung* der zugehörigen übergeordneten Eigenschaft **aktiviert** ist, oder
- die statische Eigenschaft *Alarm Standard-Gateway?* des Geräts **deaktiviert** ist

So identifizieren Sie, welche Geräte entsprechend einer dieser Möglichkeiten konfiguriert sind:

Schritt	Aktion
1	Wählen Sie im Bearbeitungs- oder Überwachungsmodus im Menü "Extras" die Option Netzwerk analysieren aus. Das Fenster "Netzwerkanalyse" wird mit einer Liste der Netzwerkfehler angezeigt.
2	Wenn die Liste so lang ist, dass Blättern erforderlich ist, gehen Sie wie folgt vor: a. Klicken Sie auf die Überschrift der Spalte <i>Schwere</i> , um die Liste zu sortieren, b. Blättern Sie zu den Elementen mit einem <i>Schwerewert</i> Information Hinweis: Elemente, die die Meldung <i>Alarmüberwachung deaktiviert</i> auslösen, haben immer den <i>Schwerestatus</i> Information .
3	Suchen Sie in der Spalte <i>Nachricht</i> nach folgendem Text: <ul style="list-style-type: none"> • <i>Die Werteüberwachung ist deaktiviert.</i> oder • <i>Der Alarm des Standard-Gateway ist deaktiviert.</i> Wählen Sie ein Gerät aus, auf das eine dieser Meldungen zutrifft, klicken Sie dann auf Gehe zu , und navigieren Sie zu dem Gerät.
4	(Optional.) Wenn Sie im Bearbeitungsmodus zu einem Gerät navigieren, können Sie den Editor für die Geräteeigenschaften öffnen und Folgendes ausführen: <ul style="list-style-type: none"> • die IP-Adresse des Geräts auswählen, damit die statische Eigenschaft <i>Alarm Standard-Gateway?</i> zum Bearbeiten angezeigt wird • in der Eigenschaftenliste nach unten blättern und Werteüberwachungen auswählen, damit das jeweilige Attribut <i>Überwachung</i> zum Bearbeiten angezeigt wird.

Warum sendet mir der E-Mail-Benachrichtigungsdienst von ConneXview E-Mail-Nachrichten weit nach dem Auftreten eines Alarms?

Ihr SMTP-Server ist die wahrscheinlichste Ursache für die Verzögerung.

ConneXview sendet immer dann, wenn ein Ereignis auftritt, eine E-Mail-Benachrichtigung über Netzwerkereignisse an Ihren SMTP-Server. Wenn der von Ihnen angegebene SMTP-Server jedoch nicht in Betrieb oder ausgelastet ist, ist er möglicherweise nicht in der Lage, die von ConneXview gesendete Nachricht zu empfangen.

ConneXview sendet weiterhin Benachrichtigungen über Netzwerkereignisse, bis der Empfang der Benachrichtigung von Ihrem SMTP-Server bestätigt wird. ConneXview stellt die Ereignisbenachrichtigungen für den Empfänger in eine Warteschlange und führt jede Minute einen neuen Sendeversuch durch, bis die E-Mail erfolgreich gesendet wurde.

Muss ich eine spezielle Konfiguration durchführen, wenn meinem ConneXview-Server- oder -Client-PC mehrere IP-Adressen zugeordnet sind?

Übersicht

Wenn Ihr ConneXview-Server-PC über mehrere IP-Adressen verfügt, müssen Sie eine dieser Adressen als die Adresse auswählen, die von seinen Clients für den Zugriff auf seine dezentralen Objekte verwendet wird. Das Ziel ist die Auswahl einer IP-Adresse, auf die alle ConneXview-Clients des Servers über ihr Standard-Gateway zugreifen können.

Ebenso müssen Sie, wenn Ihr ConneXview-Client-PC über mehrere IP-Adressen verfügt, eine einzige IP-Adresse für den Empfang der ConneXview-Kommunikation festlegen. Wenn Ihr ConneXview-Client-PC (mit mehreren IP-Adressen) eine Verbindung zu einem ConneXview-Server im selben Teilnetz aufbaut, ist keine spezielle Konfiguration erforderlich. Der Client verwendet automatisch die Server-IP-Adresse für dieses Teilnetz. Wenn sich Ihr ConneXview-Client-PC (mit mehreren IP-Adressen) jedoch **nicht** im selben Teilnetz wie der ConneXview-Server befindet, müssen Sie eine der IP-Adressen des Clients für den Empfang von Ereignisbenachrichtigungen auswählen. Das Ziel ist die Auswahl einer IP-Adresse, die der ConneXview-Server-PC über sein Standard-Gateway erreichen kann.

HINWEIS: Verwenden Sie für einen Client oder einen Server mit mehreren IP-Adressen das Tool "rmi.bat", das im Lieferumfang von ConneXview enthalten ist, um eine einzige IP-Adresse für diesen PC auszuwählen (*siehe Seite 43*).

Wenn sich nicht alle Clients im selben Teilnetz befinden, reicht eine einzelne Server-IP-Adresse nicht für alle Clients aus. Für jeden Client, der die ausgewählte Server-IP-Adresse nicht über das Standard-Gateway des Clients erreichen kann, müssen Sie einen persistenten Pfad zur Netzwerk-Routingtabelle des Clients hinzufügen (*siehe Seite 43*). Auf diese Weise kann der dezentrale Client die ausgewählte Server-IP-Adresse erreichen.

Für einen Client-PC (mit mehreren IP-Adressen) müssen Sie, wenn keine seiner IP-Adressen über das Standard-Gateway des Servers vom Server-PC erreicht werden können, einen persistenten Pfad zur Netzwerk-Routingtabelle des Servers hinzufügen (*siehe "Hinzufügen eines persistenten Pfads zu einer PC-Routingtabelle"*). Auf diese Weise kann der Server die ausgewählte Client-IP-Adresse erreichen.

Auswählen einer IP-Adresse

Für Client- oder Server-PCs mit mehreren IP-Adressen müssen Sie eine einzige IP-Adresse für die ConneXview-Kommunikation festlegen. Verwenden Sie hierzu das Tool "rmi.bat", das sich im ConneXview-Ordner befindet. Bei einer Standardinstallation lautet der Pfad zu dieser Datei:

C:\Programme\Schneider Electric\ConneXview\rmi.bat

Gehen Sie folgendermaßen vor, um eine einzige IP-Adresse für einen Client- oder Server-PC mit mehreren IP-Adressen auszuwählen:

Schritt	Aktion
1	Suchen Sie die Datei "rmi.bat" und doppelklicken Sie darauf. Das Dialogfeld "RMI-Einstellungen" von ConneXview wird aufgerufen.
2	Wählen Sie eine IP-Adresse in der Liste <i>Adresse für RMI-Server</i> aus.
3	Klicken Sie auf OK . Hinweis: Die Änderungen an den Einstellungen für einen ConneXview-Server werden erst nach einem Neustart des Servers (über die ConneXview Server-Konsole) übernommen.

Hinzufügen eines persistenten Pfads zu einer PC-Routingtabelle

Gehen Sie folgendermaßen vor, um einen persistenten Pfad zur Netzwerk-Routingtabelle eines PC hinzuzufügen:

Schritt	Aktion
1	Öffnen Sie eine Eingabeaufforderung.
	a Wählen Sie Start → Ausführen . Das Dialogfeld "Ausführen" wird geöffnet.
	b Geben Sie im Dialogfeld "Ausführen" im Feld "Öffnen" cmd ein und klicken Sie dann auf OK . Eine Eingabeaufforderung wird angezeigt.
2	Verwenden Sie in der Eingabeaufforderung den Windows-Befehl <i>route</i> , um einen Pfad zur Netzwerk-Routingtabelle des PC hinzuzufügen. Der folgende Befehl beispielsweise fügt einen persistenten Pfad zum Netzwerk 10.10.10.0 über ein Gateway an der Adresse 192.168.112.2 hinzu: C:\>route -p add 10.10.10.0 mask 255.255.255.0 192.168.112.2
3	Betätigen Sie nach der Eingabe des Befehls <i>route</i> die Eingabetaste . Der Befehl wird ausgeführt.

Welches sind die Mindest-Systemanforderungen für ConneXview v2.1?

ConneXview Stand-alone oder nur Server

Prozessor	Intel 1.2 GHz Pentium 4-CPU oder höher
Systemspeicher	512 MB-RAM
Plattenspeicher	250 MB verfügbare Festplattenkapazität
Betriebssystem	Microsoft Windows 2000 oder XP
Netzadapter	10/100 Ethernet-Adapter, an das Netz über ein Ethernet-Kabel, Kategorie 5e, angeschlossen
Hinweis: Für das Überwachen großer Netze von 250-500 Knoten wird empfohlen, Ihren Prozessor und Speicher zwecks optimaler Systemleistung gegenüber diesen Mindestanforderungen zu ertüchtigen.	

ConneXview Remote Client

Prozessor	Intel 800 GHz Pentium 4-CPU oder höher
Systemspeicher	512 MB-RAM
Plattenspeicher	250 MB verfügbare Festplattenkapazität
Betriebssystem	Microsoft Windows 2000 oder XP
Netzadapter	10/100 Ethernet-Adapter, an das Netz über ein Ethernet-Kabel, Kategorie 5e, angeschlossen

Wie überträgt man ConneXview-Dateien auf einen anderen PC?

Öffnen einer übertragenen ConneXview-Duplikatdatei *.NWM

HINWEIS: Doppelte Gerätetyp-Kennungsfilter sind unzulässig. Es darf nur einen Fall einer Gerätetyp-Kennung geben.

Falls im Netzplan ein neues Gerät existiert (.NWM-Datei) und dieses nicht im Ordner ConneXview Networks ist, dann kann ConneXview die Netzdatei nicht öffnen. Sie erhalten die Fehlermeldung `Unable to create network`. Zum Öffnen der Datei wie folgt vorgehen:

1. Alle fehlenden Gerätetyp-Dateien besorgen.
2. Diese in den ConneXview Networks-Ordner kopieren.
3. Die ConneXview-Anwendung neu starten und versuchen, die Netzdatei erneut zu öffnen.

HINWEIS: Wenn Sie die Parameter der mit der ConneXview-Anwendung installierten Gerätetypen geändert haben und Sie die geänderten Gerätetyp-Dateien nicht in den neuen PC kopieren, dann spiegeln die Standard-Gerätetypen die Standardparameter wieder.

Allgemeine Maßnahmen des Anwenders

- Beim Übertragen der *.NWM-Datei von einem Rechner auf einen anderen folgende Dateitypen mit aufnehmen. Eine Unterlassung kann dazu führen, dass sich die Netzdatei auf dem Zielrechner nicht öffnet.
 - alle geänderten oder neuen (*.typ)-Dateien
 - geänderte oder hinzugefügte MIB-Dateien (*.mib)
 - Grafikdateien (*.GIF/*.JPG)
- Alle geänderten oder neuen Gerätetyp-Dateien und alle zugehörigen Dateien kopieren in den .NETWORKS-Ordner, der sich im Xview-Installationsverzeichnis befindet.
- Entweder in dem ConneXview Gerätetyp-Editor oder in der ConneXview-Anwendung **Analyze Device Types** ablaufen lassen. Damit wird bestätigt, dass alle neuen oder geänderten Gerätetypen von Fehlern frei sind, bevor die mit ConneXview installierten Gerätetypen überschrieben werden. Die erfolgreichen Gerätetypen in den ConneXview-Installationsordner *.dat kopieren.

Was ist zu tun, wenn der ETY 110WS im Netzplan ohne Verknüpfung erscheint?

Derzeit entdeckt ConneXview die ETY110WS im Netzplan ohne Verknüpfung (Anschluss) und zeigt sie an. Dieses geschieht, weil der ETY110WS seine MAC-Adresse nicht korrekt angibt und diesem Gerät keinen Anschluss und Schalter zuordnen kann.

Zum Beheben dieses Problems muss diese Verknüpfung von Hand dem Gerätetyp hinzugefügt werden, der den ETY110WS darstellt.

Wie werden Geräte Dritter integriert und überwacht?

Der ConneXview-Gerätetypeditor gibt Ihnen die Möglichkeit, MIBs anderer Hersteller zu importieren und kundenspezifische Gerätetypen zu erstellen, komplett mit Grafik und SNMP-Objekten. Sprechen Sie den Gerätehersteller an, um eine private MIB für sein Produkt zu erhalten.

HINWEIS: Grafik, die das Gerät abbildet, muss 64x64 Pixel sein, außerdem das *.gif* oder *.jpg*-Format aufweisen.

HINWEIS: Jede Änderung an der Gerätetyp-Bibliothek erfordert einen Neustart der ConneXview-Anwendung.

Das Nachstehende sind öffentliche MIBs, die in ConneXview zur Verfügung stehen.

MIB	Beschreibung
RMON-MIB	RMON-MIB RFC-1271
SNMPv2.MIB	RFC-3418
SNMPv2-TC	RFC-2579 SMIv2
IF-MIB	IETF Schnittstellen MIB RFC-2863
IANAifTYPE-MIB	RFC-1573 IANA Schnittstellen-Identifizierer
IEEE8023-LAG-MIB	IEEE 802.3ad Verbindungsansammlung
RFC-1213	MIB II für TCP/IP
SchneiderTFE	Schneider Transparent Factory Private MIB

Wie wird eine Netzsuche mit einem Drahtlos-Adapter vorgenommen?

HINWEIS: Das Verwenden eines Drahtlos-Adapters während der Netzsuche kann widersprüchliche Ergebnisse liefern. Für beste Ergebnisse ist ein Ethernet-Kabel zu verwenden.

Falls Ihre Anwendung den Einsatz einer drahtlosen Verbindung erfordert, dann wird folgende Vorgehensweise empfohlen:

- Eine niedrige Erfassungsrate wählen
 - im **Network Discovery-Parameter**-Dialog den Steuerschieber für **Discovery Rate** auf Low bringen
- Maximieren Sie die Stärke Ihres drahtlosen Signals in der Nähe des Zugangspunktes
- Im **Advanced Discovery Settings**-Dialog alle Zeitüberwachungs- und Wiederholungsgrenzwerte verdoppeln
 - zum Zugriff auf diesen Dialog die Taste **Advanced ...** im **Network Discovery Parameter**-Dialog drücken

HINWEIS: Für weitere Informationen die Taste **About Discovery** in der **Discovery Progress**-Dialog-Box drücken, die nach dem Aufruf von **Discovery** angezeigt wird.

Was tun, wenn ConneXview mein Netz nicht ordnungsgemäß erkennen und darstellen kann?

- Die Erfassungsrate senken, damit das Gerät auf ConneXview in der **Network Discovery Parameters**-Dialog-Box reagieren kann.
- Überprüfen, ob Sie für den PC, auf dem Xview installiert ist, Verwaltungsrechte haben. Gegebenenfalls müssen Sie Ihren Informationstechnik-Administrator zu Hilfe rufen.
- Überprüfen, ob Sie sämtliche Namen der **Read Community** eingetragen haben, die an Ihrem Netz verwendet werden. Gegebenenfalls müssen Sie Ihren Informationstechnik-Administrator zu Hilfe rufen.
- Falls Sie ein Netz über einen Router oder eine Firewall abfragen oder überwachen, dann prüfen Sie, ob der UDP -Anschluss 161 und der TCP-Anschluss 502 nicht gesperrt sind.
- Falls Sie die Windows Firewall verwenden, dann erstellen Sie eine Regel, die dem UDP 161 und TCP 502-Verkehr den Durchgang durch die Firewall gestattet.
- Überprüfen Sie den LED-Status des gestörten Gerätes und schlagen Sie in der Bedienanweisung für dieses Gerät oder im Transparent Ready User Guide nach (vorhanden auf der ConneXview-Installations-CD.)
- Überprüfen Sie, ob die Firmware auf dem von Schneider Electric und nicht von Schneider Electric verwaltetem Gerät aktuell ist.
- Wenn Sie die IP-Adresse Ihres Netzadapters bei offenem ConneXview geändert haben, dann starten Sie die ConneXview -Anwendung neu.

Wie konfiguriere ich SNMP (Simple Network Management Protocol) in Microsoft Windows?

Microsoft Windows 2000 und XP Professional unterstützen SNMP.

HINWEIS: SNMP ist eine RFC-Spezifikation, die ein Mittel zum Abrufen von Netz-Verwaltungsdaten von Geräten darstellt (nachdem diese erfasst sind), die in Ihrem Netz angesiedelt sind.

SNMP lässt einen PC oder Server, wie SCADA, als ein von SNMP verwaltetes Gerät erscheinen, mit dem Ergebnis, dass intelligenteren Informationen von dem verwalteten Gerät zur Verfügung stehen.

Zum Konfigurieren des SNMP-Dienstes unter Windows XP sind folgende Schritte vorzunehmen. Bitte beachten, dass zum Installieren von SNMP gegebenenfalls Ihre Windows-Installations-CD benötigt wird.

Schritt	Maßnahme
1	auf Start → Settings → Control Panel klicken
2	doppelklicken auf Add/Remove
3	klicken auf Add/Remove Windows Components
4	wählen Sie Management and Monitoring Tools → Details
5	wählen Sie die Simple Network Management Protocol Check-Box, und klicken Sie auf OK
6	klicken Sie auf Next , um SNMP hinzuzufügen
7	klicken Sie auf Finish , um den Windows Component Wizard zu schließen SNMP startet nach der Installation automatisch
<p>Hinweis: Um diesen Vorgang durchführen zu können, müssen Sie ein Mitglied der Gruppe Administrators an Ihrem lokalen Rechner sein, oder es muss die entsprechende Vollmacht auf Sie übertragen worden sein. Wenn der Rechner an eine Domäne angeschlossen ist, dann können Mitglieder der Gruppe Domain Admins gegebenenfalls diesen Vorgang ausführen. Als bewährtes Sicherheitsverfahren ziehen Sie das Verwenden von Run in Betracht, um diesen Vorgang durchzuführen.</p>	

Welche Gerätetyp-Dateien sind in ConneXview v2.1 enthalten?

Die in ConneXview enthaltenen Gerätetyp-Dateien und die Produkte, die sie darstellen, sind im Folgenden aufgeführt.

Dateiname	Produkt
ATV58Host.typ	Altivar ATV58-Umrichter
CEV300Host.typ	174CEV30020 Modbus-zu-Ethernet-Gateway
CloudHub.typ	Generische Wolke zur Darstellung eines nicht erkennbaren Hubs
ConneXium NxS Switch RM.typ	Redundanz-Manager des verwalteten ConneXium 499Nx17100 und 499NxS27100-Switches
ConneXium NxS Switch SM.typ	Ringkopplungs-Standby-Manager des verwalteten ConneXium 499Nx17100 und 499NxS27100-Switches
ConneXium NxS Switch.typ	Verwalteter ConneXium 499NxS17100 und 499NxS27100-Switch
ConneXium Switch.typ	Verwalteter ConneXium TCSESM-Switch im Initialmodus, d. h., nicht für das Hiper-Ring- oder MRP-Protokoll konfiguriert
ConneXium TCSESM Switch.typ	Für Hiper-Ring, aber nicht für Redundanz- oder Standby-Manager konfigurierter, verwalteter ConneXium TCSESM-Switch
ConneXium Switch SM.typ	Ringkopplungs-Standby-Manager des verwalteten ConneXium TCSESM-Switches
ConneXium TCSESM Switch RM.typ	Redundanz-Manager des verwalteten ConneXium TCSESM-Switches
ConneXium MRP.typ	Verwalteter ConneXium TCSESM-Switch mit MRP-Protokoll
ConneXium TCSESM MRP RM.typ	Redundanz-Manager des verwalteten ConneXium TCSESM-Switches mit normalem MRP-Protokoll
DefaultManagedHost.typ	Generisches Endgerät, das SNMP unterstützt
DefaultManagedMbapHost.typ	Generisches Endgerät, das Modbus und SNMP unterstützt
DefaultManagedSwitch.typ	Generisch verwalteter Switch
DefaultRouter.typ	Generischer Netzwerkrouter
DefaultUnmanagedHost.typ	Generisches Endgerät, das Modbus oder SNMP nicht unterstützt
DefaultUnmanagedMbapHost.typ	Generisches Endgerät, das Modbus, aber nicht SNMP unterstützt

Dateiname	Produkt
DefaultUnmanagedSwitch.typ	Generischer Ethernet-Switch, der SNMP nicht unterstützt
ETCHost.typ	Premium EtherNet/IP-Module
EntV1Host.typ	170ENT11000 und 170ENT11002 Kommunikationsadapter für Momentum-E/A- Module
EntV2Host.typ	170ENT11001-Kommunikations-Adapter für Momentum-E/A-Module
Ety410xhost.typ	Premium Ethernet-Adapter TSXETY4102 und TSXETY4103
Ety510xhost.typ	Veraltetes FactoryCast-Modul des Premium Ethernet-Adapters TSXETY5102/5103
EtyPortHost.typ	Premium ETY Port (Ethernet)
ETZHost.typ	Modicon Micro ETZ410/510-Kommunikationsmodul
M1EHost.typ	Momentum PLC 170M1E9x0-20 und 170M1E9x0- 30
M340EGD.typ	M340 Modbus Plus Proxy-Module
NICHost.typ	Advantys STB Ethernet/IP NIM
NIMHost.typ	Advantys STB E/A NIP2212 NIM
NOCHost.typ	Quantum EtherNet/IP-Module
NOEHost.typ	Quantum 140NOE77100/01 Ethernet- und 140NOE77110/11 FactoryCast-Module
NWMHost.typ	Quantum 140NWM100-00 FactoryCast-HMI-Modul
WMY100.typ	Premium FactoryCast HMI-Module
PCoproHost.typ	Unity Premium TSX574624/5634 PLC Ethernet
QCoproHost.typ	Unity Quantum 140CPU651-50/60 PLC Ethernet
TrHost.typ	Generisches Endgerät, das Folgendes unterstützt: <ul style="list-style-type: none"> ● Modbus ● SNMP ● Transparent Ready sowie Dienste, wie: <ul style="list-style-type: none"> ● Web ● Ethernet-E/A-Scanner ● SMTP ● NTP ● Global Data

Warum verursacht ein Default Gateway (Router) in ConneXview ein Alarmereignis?

Manche Geräte von Schneider Electric erfordern, dass ein Gateway-Feld in der Gerätekonfiguration konfiguriert wird, gestatten aber nicht eine Null oder 0.0.0.0. Dadurch sind Sie gezwungen, die konfigurierte IP-Adresse der Geräte einzugeben.

Bei Netzen, in denen ein Default-Gateway (Router) nicht vorhanden ist, wird ein Alarmereignis in ConneXview generiert. Dieses geschieht, weil ConneXview den Wert des Default Gateway kontrolliert und die IP-Adresse des Gateways prüft, um sicherzustellen, dass es sich tatsächlich um ein Default Gateway handelt. Da das Gerät nicht ein Default Gateway ist, wird der Alarm generiert. Zum Unterdrücken dieses Alarms **Default Gateway Alarming** im **Device Property Editor** sperren.

HINWEIS: Alle gesperrten Alarme können dargestellt werden mit Hilfe von **Tools** → **Analyze Network**.

Was ist ein MIB-Browser und welchen soll ich verwenden?

Ein MIB-Browser ist ein Tool zum Abfragen von Geräten bei der Auswahl eines Objekts, auf dem ein Identifizierungsfilter beruhen soll. Ein MIB-Browser ist zweckmäßig, wenn nach SNMP-Geräteobjekten gesucht wird, und die MIB-Objekte, die von anderen, privaten OEM-MIBs zur Verfügung stehen, durchgeblättert werden.

Ein kostenloser MIB-Browser ist von iReasoning, Inc. erhältlich unter:
<http://www.ireasoning.com>

Wie wird ConneXview mit geänderten Typen der installierten Geräte aktualisiert?

Beim Aktualisieren von ConneXview werden alle Objekte, die Sie geändert haben, von der neuen Installation überschrieben. Zu diesen Objekten gehören:

- Standardgrafiken der Gerätetypen
- Alarm-Grenzwerte
- MIBs
- Überwachte Objekte

Es wird empfohlen, dass Sie einen Vorgang **Analyze Device Type** von dem **Device Type Editor** oder vom ConneXview vornehmen und eine Sicherungskopie des geänderten Gerätetyps im Installationsordner **dat** ablegen.

HINWEIS: ConneXview Version 2.0 and darüber sichert automatisch die Gerätetyp- und die Netzdateien. Die Sicherungskopie befindet sich im ConneXview-Programmverzeichnis als Ordner mit bak als Präfix.

Nach dem Aktualisieren von ConneXview kopieren Sie den geänderten Gerätetyp aus dem Ordner **dat** in den Ordner **networks** und starten Sie die Anwendung ConneXview neu.

Welche Dateien werden beim Übertragen von Netz-Plänen oder Aktualisieren/Neuinstallieren von ConneXview transferiert?

Beim Übertragen von Netz-Plänen von einem PC zu einem anderen oder beim Aktualisieren/Neuinstallieren von ConneXview sind folgende Dateien zu exportieren:

- *NWM*
der Netzplan für jedes gesicherte Netz
- *.typ*
alle neuen oder geänderten Gerätetypen einschließlich modifizierter Standard-Gerätetypen
- *.GIF* oder *.JPG*
zu neuen oder geänderten Gerätetypen gehörende Grafik-Dateien

Wie erhalte ich technische Unterstützung?

Wir empfehlen Ihnen, für beste Ergebnisse die Schneider Electric-Gerätefirmware zu aktualisieren. Besuchen Sie <http://www.schneider-electric.com> für Updates oder nehmen Sie mit Ihrem örtlichen Händler oder mit dem Schneider Electric-Vertriebsbüro Verbindung auf.

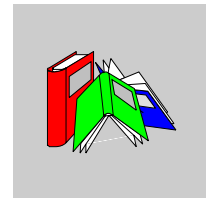
HINWEIS: Ältere Firmwareversionen können bewirken, dass manche Ausgaben auf ConneXview reagieren. Für technische Unterstützung nehmen Sie mit Ihrem Händler oder dem Schneider Electric-Kundendienstzentrum Verbindung auf.

Zur Fehlerbehebung an komplexen Netzen kann Ihr Kundendiensttechniker gegebenenfalls wünschen, zwecks technischer Analyse eine Paket-Erfassungsdatei bereit zu stellen.

HINWEIS: Ein Open Source Freeware-Paketerfassungs-Tool für die Microsoft Windows-Plattform ist erhältlich unter: <http://www.wireshark.org>

Installieren Sie dieses Erfassungs-Tool mit dem zugehörigen WinPcap Promiscuous Mode Driver und sammeln Sie die Paketerfassung, wie von Ihrem Schneider Electric-Kundendienstvertreter angewiesen.

Glossar



A

Abbildungseigenschaft

Zustands-Abbildungseigenschaft. Eine abgeleitete dynamische Eigenschaft, die mit einem Farbkartenschlüssel verknüpft werden kann. Eine Zustands-Abbildungseigenschaft enthält vier anwenderdefinierte Betrags-Grenzwertauslöser (High-High, High, Low, Low-Low). Ein Farbkartenschlüssel zeigt auf eine Zustands-Abbildungseigenschaft und weist jedem Grenzwertauslöser eine Farbe zu.

abgeleitete Eigenschaft

Eine dynamische Eigenschaft, die ihren Wert von einer Funktion oder Berechnung erhält, die an einer oder mehreren Eigenschaften des SNMP, Modbus oder anderen abgeleiteten Eigenschaften vorgenommen wird.

abonnieren

Der Vorgang des erklärten Interesses an einer verfügbaren Information seitens eines Gerätes. Ein Gerät kann insgesamt bis zu 2,048 4x Register von bis zu 64 Global Data-Publizisten abonnieren. Bitte beachten, dass ein Abonnent die gesamte, publizierte und verfügbare Netzvariable abonnieren muss, auch wenn nur ein Teil der Registerdaten benötigt wird.

Adressen-Server

Steht in den Quantum- und Premium-Kommunikationsbausteinen zur Verfügung, um Clients, die BootP verwenden, IP-Adressenparameter zuzuweisen. Zusätzlich unterstützen die Bausteine Quantum NOE 771-01/11 and Premium ETY 4103/5103 Das Ersetzen fehlerhafter Geräte.

Alarm

Ein Anzeichen für ein Netzproblem. Ein Alarm wird angestoßen, wenn der Wert eine überwachten Geräteeigenschaft—deren Atribut *Kritizität* entweder auf **Kritisch eingestellt ist** oder auf **Achtung**:

- überschreitet einen Wert für eine Grenzwertüberwachung oder
- ändert mehr als einen voreingestellten Grenzwert für eine Änderungsüberwachung, oder
- ändert sich von oder zu einer Gruppe voreingestellter Werte für eine Zustandsüberwachung

Änderungsüberwachung

Eine vorkonfigurierte Alarmauslösung aufgrund einer Änderung des Betrags einer überwachten Eigenschaft.

arithmetische Eigenschaft

Eine abgeleitete dynamische Eigenschaft, die ihren Wert von einer arithmetischen Funktion erhält (Addition, Subtraktion, Multiplikation oder Division), welche an den Werten zweier anderer dynamischer Eigenschaften durchgeführt wird.

ARP

Adressen-Auflösungsprotokoll. Das für das Abbilden einer IP-Adresse in eine MAC-Adresse verwendete Ethernet-Protokoll.

Attribut

Eine aus einer Menge von Feldwerten, die zusammen eine Eigenschaft oder eine Eigenschaftsüberwachung definieren.

B

Bandbreite

Die Datenübertragungskapazität einer Netzverbindung. ConneXview überwacht die Bandbreitenausnutzung—den Prozentsatz der Bandbreite, der benutzt wird.

Biegung

Der Punkt einer Kurve in einer Kommunikationsverbindung, der im Edit-Modus entweder durch Wahl einer Form der orthogonalen Anordnung erzeugt wird, oder durch manuelle Wahl und Streckung einer Kommunikationsverbindung.

C

Client-/Server-Modus

Eine Methode zum Installieren und Betreiben von ConneXview als eine verteilte Softwareanwendung, bestehend aus 2 (oder mehr) getrennten Komponenten, zu welchen folgendes gehört: 1 Server-Komponente, über einen NT-Dienst Funktionen ausführt und Informationen liefert, und 1 or mehrere Client-Komponenten—von denen eine auf dem Server-PC installiert sein muss, der als externes GUIs arbeitet und an dem NT service des ConneXview-Servers angemeldet ist.

CRC

(*zyklische Redundanzprüfung*) Eine Methode der Fehlerprüfung in einer Nachricht durch mathematische Berechnungen an der Bitzahl der Nachricht, deren Ergebnisse zusammen mit den Daten an den Empfänger gesendet werden. Der Empfänger wiederholt die Berechnung an den empfangenen Daten. Bestehen Unterschiede der beiden Berechnungen, dann fordert der Empfänger vom Urheber eine Wiederholung der Sendung an.

D

Datagramm

Ein einzelnes Paket von Daten – manchmal als ein Paket bezeichnet – das Daten und einen Nachrichtenkopf mit Adresseninformationen enthält, zur Lenkung von einem Quellengerät über das Netz zu einem Zielgerät.

Datenverbindungs-Schicht

Schicht 2 des siebenlagigen OSI-Referenzmodells für die Kommunikation zwischen Rechnern an Netzen. Diese Schicht definiert Protokolle für Datenpakete und die Art ihrer Übertragung zu und von jedem Gerät am Netz. Es ist eine mediumunabhängige Kommunikationseinrichtung auf Verbindungsebene über der physikalischen Schicht und ist in zwei Unter-Schichten aufgeteilt—Medien-Zugangssteuerung (MAC) und logische Verbindungssteuerung (LLC).

dynamische Eigenschaft

Eine Eigenschaft eines Gerätes oder einer Kommunikationsleitung, deren Wert nicht konstant ist, sondern sich vielmehr im Betrieb dynamisch verändern kann.

E

Edit-Modus

Der Status von ConneXview mit offener und zum Edieren dargestellter Netzkarte

Erfassungsbereich

Die zu erfassenden Geräte sind durch einen Bereich von IP-Adressen definiert. Der Bereich ist durch die Unternetz-Adresse und den Wert der Unternetz-Maske bestimmt, die eine Liste aller in Betracht kommenden Adressen im Unternetz definiert. Sie können den Bereich von Hand einschränken, indem Sie die Startadresse oder/und die Endadresse entweder im **Edit Subnet** oder **Add Subnet** Dialogfeld anpassen.

Ethernet

Eine Familie von Local Area-Netzprotokollen, die unter IEEE 802.3. fallen

F

Farbkartenschlüssel

Ein Farbkartenschlüssel zeigt auf eine Zustands-Abbildungseigenschaft und bringt den Wert dieser Eigenschaft zu einem Farbschema in Beziehung. Das Wählen eines Farbkartenschlüssels im Überwachungsmodus bewirkt, dass der Network Map Viewer jedes Gerät und jede Kommunikationsverbindung in einer Farbe anzeigt, die den Wert der abgebildeten Eigenschaft wiedergibt.

FDR

Austausch fehlerhafter Geräte Ein Vorgang zum leichten Austausch eines Gerätes im Fehlerfall und zum Wiederherstellen der konfigurierten Parameter des vorherigen Gerätes.

Firewall

Ein Router oder eine Workstation mit mehreren Netzschnittstellen, der/die spezifische Protokolle steuert und begrenzt, auch Verkehrstypen innerhalb jedes Protokolls, Dienst-Typen und die Richtung des Informationsflusses.

FTP

(Filetransfer-Protokoll) Das Kommunikationsprotokoll, das den Filetransfer zwischen Geräten ermöglicht.

G

Gateway

1. Typische Übergaben an einen Router. Ein Router ist ein Gerät, das Datenpakete über Netze transportiert. Ein Router ist an mindestens zwei Netze angeschlossen, gewöhnlich an zwei LANs oder WANs oder ein LAN und das Netz seines Internet-Serviceproviders. Router sind an Gateways angeordnet, den Stellen, wo zwei oder mehrere Netze verbunden sind. Router benutzen Nachrichtenköpfe und Durchlasstabelle, um den besten Pfad für den Transport der Pakete zu finden, und sie arbeiten mit Protokollen wie ICMP, um miteinander zu kommunizieren und den besten Weg zwischen beliebigen zwei Hosts zu konfigurieren.

2. Eine Kombination von Hardware und Software, die im Übrigen nicht kompatible Netze oder Netz-Geräte miteinander verbindet. Gateways enthalten Paket-Assembler/Disassembler (pads) und Protocolumsetzer. Gateways arbeiten in den Schichten 5, 6 und 7—der Bearbeitungs-, Darstellungs beziehungsweise Anwendungsschicht—des OSI-Modells.

Gerät

Die an einem Netzknoten befindliche Hardware. Ein Beispiel für einen Gerätetyp.

Gerätetyp

Eine Geräteklasse, die im Device Type Editor erstellt wurde und ediert werden kann.

Globaler Datendienst

Der Globale Datendienst (GDS) arbeitet mit *Echtzeit-Darstellung/Anmeldung* für ein Gerät, um eine variable Registertabell darzustellen. Andere Geräte am selben Unter-Netz melden sich dann an der variablen Tabelle an. Global Data verwendet UDP Multicast, um die Variable gleichzeitig an mehrere Pakete mit nur einem UDP-Paket zu vertweilen. Bezüglich weiterer Einzelheiten zum Global Data Service siehe die Quantum NOE 771-01/11 oder Premium ETY 4103/5103.

H

Hochlauf-Modus

Der Zustand von ConneXview ohne geöffnete Netzkarte.

Host

Ein an ein Netz angeschlossener Endknoten, zum Beispiel ein PC, PLC, E/A-Gerät oder ein ähnliches Gerät. Ein Host-Gerät enthält keinen Router oder Schalter und stellt das Gegenteil von diesen dar.

HTTP

(Hyper Text Transfer Protocol) Das Kommunikationsprotokoll, welches Web Browsing ermöglicht.

I

ICMP

Internetprotokoll für Steuernachrichten. Das Internetprotokoll, das Fehler meldet und Informationen bezüglich Datagramm-Verarbeitung liefert.

IO Scanning Service

Ein automatischer Client, der bei Quantum-, Premium- und Momentum-Plattformen zur Verfügung steht. IO Scanning ermöglicht das Eintragen von Haltereister-Lesevorgängen, Schreibvorgängen und Schreib-/Lesevorgängen an externe Geräte in Zeitabständen, die in Millisekunden konfigurierbar sind. Das Einrichten des IO Scanning erfolgt in Ihrer Programmieranwendung mit Hilfe einer Tabelle anstelle logischer Programmierfunktionen.

IP

Internetprotokoll. Derjenige Teil der TCP/IP Protokollfamilie, der die Internet-adressen von Geräten verfolgt, abgehende Nachrichten lenkt und ankommende Nachrichten erkennt.

IP Adresse

Eine eindeutige 32-Bit-Adresse, die TCP/IP-Geräten am Internet zugewiesen wird, geschrieben als vier Achtergruppen – dargestellt als durch Punkte getrennte Dezimalzahlen. Eine IP-Adresse enthält eine Netznummer, wahlweise eine Unternetz-Nummer und eine Gerätenummer. Die Netz- und die Unternetz-Nummer ermöglichen das Lenken von Nachrichten, die Gerätenummer dient als spezifische Adresse in einem Netz oder Unter-Netz. Eine Subnet-Maske ist ein Filter, das die Netznummern von der Unternetz-Nummer trennt.

J

Jabber

Ein Netzfehler, verursacht durch eine Schnittstellenbaugruppe, die korrumpierte Daten in das Netz einspeist.

Auch ein Fehlerzustand, der von einem Netzknoten verursacht wird, welcher längere Pakete sendet, als zulässig.

K

Knoten

Ein Endpunkt eines Netzabschnitts (der zum Beispiel zu einem Host-PC führt) oder ein Schnittpunkt zweier oder mehrerer Netzpfade (zum Beispiel der Ort einer Buchse, eines Schalters oder Routers).

L

Lasteigenschaft

Eine abgeleitete dynamische Eigenschaft, die auf zwei mit einer Schnittstelle zusammenhängenden beruht – einem Eingangs- und einem Ausgangsmesswert - und deren zusammengefassten Wert als Einheiten/Zeit ausdrückt.

Limit Monitor

Ein vorkonfigurierter Alarmauslöser, der anspricht, wenn der Betrag einer überwachten Eigenschaft den Sollwert erreicht oder überschreitet.

Link

Kommunikationsverbindung. Eine Netzverbindung zwischen zwei Geräten.

LTM E

Der Erweiterungsbaustein des TeSys T-Motormanagement-Systems.

LTM R

Der Steuerbaustein des TeSys T-Motormanagement-Systems.

M

MAC Adresse

Steueradresse für Medienzugriff. Eine 48-Bit-Nummer, die in einem Netz eindeutig ist und in jede Netzbaugruppe oder jedes Gerät bei deren/dessen Herstellung programmiert wird.

MBAP

Modbus-Anwendungsprotokoll. Das auf TCP/IP beruhende Standardprotokoll, das zum Verwalten der Master-Slave/Client-Server- Kommunikation zwischen intelligenten Geräten an einem Ethernet-Netz verwendet wird.

MIB

Management-Informationsbasis. Eine einheitlich anerkannte hierarchische Datenstruktur, die Objekte enthält – manchmal als Geräteeigenschaften bezeichnet – aus welchen ein Gerät in einem SNMP-Netz lesen und, in manchen Fällen, in sie schreiben kann. Die hierarchische Datenstruktur enthält sowohl öffentliche (oder Standard-) Zweige, als auch private (oder Besitzer-) Zweige.

Modbus

Ein Nachrichtenprotokoll der Anwendungsschicht. Modbus ermöglicht Client- und Server-Kommunikation zwischen Geräten, die an unterschiedliche Typen von Bussen oder Netzen angeschlossen sind. Modbus bietet viele Leistungen, die durch Funktions-Codes beschrieben sind.

N

Nachrichtenkopf

Die Steuerinformation, die am Anfang einer zu übertragenden Nachricht eingefügt wird Sie enthält wichtige Informationen, wie die Packet- oder Blockadresse, Quelle, Ziel, Nachrichtennummer, Länge und Routing-Anweisungen.

Name der Menge

Der Name in Form einer alphanumerischen Zeichenfolge, der als Sicherheits-Schutzmechanismus benutzt wird, um den Schreib-/Lese-Zugriff auf eine Gerätegruppe zu gestatten. ConneXview benötigt nur die Zeichenfolge für die Lese-Menge. Die meisten Händler geben der Zeichenfolge der Lese-Menge den Standardwert *Public*, aber Sie können die Zeichenfolge zur Sicherheit am Gerät ändern.

Netzkarte

Eine schematische Darstellung eines Netzes im Edit- oder Überwachungsmodus.

NTP

Netz-Zeitprotokoll Ein Kommunikationsprotokoll, das zum Austausch und Synchronisieren von Zeiten über ein Netz verwendet wird.

NWM

Netzkarte Eine Dateierweiterung für eine Netzkartendatei, die Informationen über alle Geräte an einem Netz, ihre gegenseitigen Verbindungen und Einstellungen enthält.

O**OID**

Objektkennung. Eine dezimale Zahlenfolge mit Punkten, die in eindeutiger Weise einem Objekt in einem MIB zugeordnet ist und die dieses beschreibt. Jedes Zahlensegment in der Folge beschreibt eine eindeutige Lage in der MIB-Hierarchie, wobei jedes folgende Zahlensegment einen Unter-Zweig von Segmente höherer Ebene bezeichnet.

P**Packet Sniffer**

Eine Software, die den Verkehr an einem Ethernet-Netz abfängt und analysiert. Sie kann zur Überwachung der Netz.Nutzung verwendet werden, zum Erkennen von unerlaubten Zugriffen auf das Netz und zum Erfassen und Melden der Netzstatistik.

Paket

Eine Reihe von Bits, die Daten und Steuerinformationen enthalten und für die Übertragung von einem Knoten zum anderen formatiert sind. Sie enthält einen Datenkopf mit Startrahmen, die Ursprungs- und die Zieladresse, Steueraten, die eigentliche Nachricht und einen Dateinachsatz mit Fehler-Steuerdaten (bezeichnet als die *Rahmen-Prüfsequenz*).

Physikalische Schicht

Schicht 1 (die Grundsicht) des OSI-Referenzmodells ist durch den physikalischen Kanal implementiert. Sie steuert Hardwareverbindungen und die Bytestromkodierung für die Übertragung. Es ist die einzige Schicht, die einen physikalischen Transfer von Informationen zwischen Netzknoten beinhaltet. Die physikalische Schicht isoliert Schicht 2 (die Daten-Koppelschicht) von mediumabhängigen physikalischen Merkmalen, wie Grundband-, Breitband- und Lichtleitfaser-Übertragung. Schicht 1 definiert die Protokolle, welche Übertragungsmedien und Signale steuern.

Ping

Paket-Internet-Sucher. Die Kombination einer ICMP-Echoanforderungsnachricht und deren Antwort; wird in IP-Netzen verwendet, um festzustellen, ob ein Netz-Gerät erreichbar ist, und der Zugriffszeit.

Polling

Erfassungsmethode, wobei ein Netzverwaltung ausführendes Gerät andere, bekannte intelligente Netz-Geräte abfragt, ob diese Daten zum Übertragen haben. Der Erhalt dieser Nachricht seitens eines Gerätes berechtigt dieses, daraufhin eine Übertragung zu senden.

Publish

Informationen zugänglich machen und verteilen. Der Quantum NOE 771-01/11 und ETY 4103/5103 mit aktiviertem Global Data Service kann eine einzelne Multicast-Nnetzvariable publizieren, die bis zu 512 registers pro Gruppe von Global Data-Abonenten enthält, konfigurierbar in Zeitabständen einer CPU-Abfrage.

Q

quittieren

Der Vorgang, das Vorhandensein eines Netzalarms zu erkennen. Er bedeutet, dass die Person, die den Alarm quittiert, zur Diagnose übergeht und das Problem löst.

R

Router

Ein Gerät, das Datenpakete über Netze transportiert. Ein Router ist an mindestens zwei Netze angeschlossen, gewöhnlich an zwei LANs oder WANs oder ein LAN und das Netz seines Internet-Serviceproviders. Router sind an Gateways angeordnet, den Stellen, wo zwei oder mehrere Netze verbunden sind. Router benutzen Nachrichtenköpfe und Durchlasstabellen, um den besten Pfad für den Transport der Pakete zu finden, und sie arbeiten mit Protokollen wie ICMP, um miteinander zu kommunizieren und den besten Weg zwischen beliebigen zwei Hosts zu konfigurieren.

S

scan

Eine nicht intrusive Methode zum Erkennen aktiver Netz-Geräte und ihrer offenen Anschlüsse.

Senden

Eine Nachricht, die an alle Geräte an dem Netz ausgegeben wird.

SMTP

Simple mail transfer protocol Das üblichste Kommunikationsprotokoll zum Senden und Empfangen von E-Mail auf einem Netz.

SNMP

Simple network management protocol. Das UDP/IP-Standardprotokoll zum Verwalten von Geräten – einschließlich Hosts (d.h. Client- oder Server-PCs), Router, Schalter und Buchsen - an einem IP-Netz. ConneXview unterstützt SNMP v1.

Stand-alone-Modus

Eine Methode zum Installieren und Betreiben von ConneXview als integrierte Softwareanwendung auf einem einzelnen PC.

Standard-Gatteradresse

1. Das Gatter in einem Netz, das ein Rechner zum Zugriff auf ein anderes Netz benutzt, wenn kein Gatter für die Verwendung vorgegeben ist.
2. In einem Netz, das mit Unter-Netzen arbeitet, der Router, der den Verkehr an einen Bestimmungsort außerhalb des Unter-Netzes des sendenden Gerätes weiter leitet.

Standardeigenschaft

Eine Eigenschaft des SNMP oder Modbus, deren Betrag sich im Laufe der Operationen dynamisch ändert.

Statische Eigenschaft

Die Eigenschaft eines Gerätes oder einer Datenverbindung, deren Wert beim Aufbau des Gerätes oder der Kommunikation eingestellt wird und die sich im Betrieb nicht dynamisch ändert.

T

TCP/IP

(Übertragungs-Steuerprotokoll/Internet-Protokoll) Ein Satz von Protokollen, entwickelt in den frühen Siebzigerjahren von der U.S. Defense Department's Advanced Research Projects Agency (ARPA). Sein Zweck war, Methoden zum Verbinden verschiedener Arten von Netzen und Rechnern untereinander zu entwickeln. TCP/IP hat nicht die Funktionalität, die OSI bietet.

TCP/IP ist ein Transport- und Internet-Arbeitsprotokoll—d.h., der De-facto-Netzwerks-Standard. Es wird allgemein über X.25 und Ethernet-Leitungen verwendet und gilt als eins der wenigen verfügbaren Protokolle, das einen echten Migrationsweg zu OSI bietet. TCP/IP kann in den meisten Umgebungen arbeiten. TCP/IP arbeitet in Schicht Drei und Vier des OSI-Modells (Netz beziehungsweise Transport).

TCP and IP sind die Standard-Netzprotokolle in UNIX-Umgebungen. Sie werden fast immer zusammen implementiert und eingesetzt.

TeSys T

TeSys T ist ein fortschrittliches System für Betrieb und Schutz von Motoren. Es kann gegen alle Motorstörungen schützen: Überlast, Stromspitzen, zu hoher Verbrauch etc.

TsSys T besteht aus:

- dem LTM R
einem Regler, der den Hauptschutz und die Steuerfunktionen übernimmt
- dem LTM E
einem Erweiterungsbaustein, der die Funktionen des Reglers durch Spannungsschutz und Überwachung vervollständigt
- einem Bediener-Steuergerät zum Lesen, Diagnostizieren und Ändern der überwachten Parameter

TFTP

(trivial file transfer protocol) Eine sehr einfache Form des File Transfer Protocol, implementiert auf dem UDP, das keine Sicherheitsmerkmale bietet.

Totband

Der Betrag in Maßeinheiten, unter (bei oberen Einstellungen) oder über (bei unteren Einstellungen) den der Schwellwertbetrag der überwachten Größe gelangen muss, bevor die als Alarm oder Status abgebildete Meldung gelöscht wird.

U

Überwachungs-Modus

Der Status von ConneXview mit offener und zur Echtzeit-Netüberwachung dargestellter Netzkarte

UDP

Anwender-Datagramm-Protokoll. Ein Protokoll im verbindungslosen Modus, in dem Nachrichten in einem Datagramm zu einem Zielgerät übertragen werden. Das UDP-Protokoll ist im typischen Fall mit dem Internet-Protokoll (UDP/IP) gebündelt.

Unter-Netz

Unter-Netz. Eine Gruppe von Geräten mit derselben Netzadresse. Typisch ein Segment eines größeren Netzes.

Unternetz-Maske

Ein Filter, das bei einer IP-Adresse angewendet wird, um die Netzadresse von der Adresse des Host oder des Gerätes zu unterscheiden.

X

XWAY

Premium-Adressierung im Format {Netz, Station} für Verwendung von Modbus- oder UNI-TE-Protokoll-Nachrichtenübertragung.

Z

Zustandsmonitor

Ein vorkonfigurierter Alarmauslöser, der anspricht, wenn der Wert einer überwachten Eigenschaft mit einem Mitglied aus einer Gruppe vorgegebener Sollwerte übereinstimmt oder nicht übereinstimmt.