ConneXview
Diagnose-Tool für Ethernet-Netzwerke
Häufig gestellte Fragen

7/2007

31008024

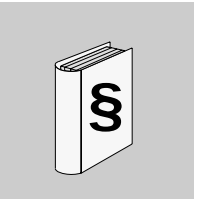
a brand of Schneider Electric

Telemecanique

www.telemecanique.com

Inhaltsverzeichnis

Sicherheitshinweise



HINWEIS

Lesen Sie diese Anweisungen gründlich durch und machen Sie sich mit dem Gerät vertraut, bevor Sie es installieren, in Betrieb nehmen oder warten. Die folgenden Hinweise können an verschiedenen Stellen in dieser Dokumentation enthalten oder auf dem Gerät zu lesen sein. Die Hinweise warnen vor möglichen Gefahren oder machen auf Informationen aufmerksam, die Vorgänge erläutern bzw. 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 macht auf eine möglicherweise gefährliche Situation aufmerksam, die bei Nichtbeachtung **unter Umständen** einen schweren oder tödlichen Unfall oder Beschädigungen an Geräten zur Folge haben kann.

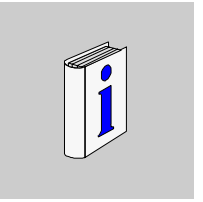
⚠ VORSICHT

VORSICHT macht auf eine möglicherweise gefährliche Situation aufmerksam, die bei Nichtbeachtung **unter Umständen** einen schweren oder tödlichen Unfall oder Beschädigungen an Geräten zur Folge hat.

BITTE BEACHTEN

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

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.

Gültigkeitsbereich

Die in diesem Dokument genannten Daten und Abbildungen sind nicht verbindlich. Wir behalten uns das Recht vor, unsere Produkte entsprechend unserem Grundsatz für kontinuierliche Produktentwicklung zu ändern. Die Informationen in diesem Dokument sind vorbehaltlich eventueller Änderungen und dürfen nicht als Verpflichtung seitens Schneider Electric ausgelegt werden.

Weiterführende Dokumentation

Titel	Referenz-Nummer
ConneXview Referenzhandbuch zum Gerätetyp-Editor	31008028
ConneXview Referenzhandbuch zum Ethernet-Diagnose-Tool	31008032

Produktbezogene Warnhinweise

Schneider Electric übernimmt keinerlei Verantwortung für eventuelle Fehler in diesem Dokument. Wenn Sie Vorschläge für Verbesserungen oder Änderungen haben oder in dieser Publikation Fehler gefunden haben, teilen Sie uns dies bitte mit.

Bei der Installation und Verwendung dieses Produkts müssen alle relevanten staatlichen, regionalen und lokalen Sicherheitsrichtlinien eingehalten werden. Aus Sicherheitsgründen und um die Übereinstimmung mit dokumentierten Systemdaten zu gewährleisten, ist ausschließlich der Hersteller berechtigt, Reparaturen an den Komponenten vorzunehmen.

Befolgen Sie die relevanten Anweisungen, wenn Sie Controller für Anwendungen mit technischen Sicherheitsanforderungen einsetzen.

Unterlassung des Einsatzes von Software von Schneider Electric bzw. für unsere Hardware-Produkte genehmigte Software kann zu Verletzungen, Schäden oder nicht angemessenen Betriebsergebnissen führen.

Nichtbeachtung der auf dieses Produkt bezogenen Warnungen kann zu Verletzungen oder Anlagenschäden führen.

Benutzerkommentar

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

Häufig gestellte Fragen

1

Auf einen Blick

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:

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 Wählverbindung, 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 Alarme 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 Profilinformationen. Wählen Sie dann beispielsweise den Prozessor "Unity Quantum" aus, indem Sie die Datei QCOPROHOST.TYP öffnen. Bearbeiten Sie hier die Schwellwerte und Alarme 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 *lokalen* 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 *lokalen* oder einem *dezentralen* 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 Überwachungsregister-karten 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 Netzwerkzuordnungstopologie. In Netzwerkfeldern können Gerätedaten zu Informationszwecken bearbeiten 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 **Geräteeigenschaften** 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.

Welche Gerätetypen gehören zum Lieferumfang von ConneXview?

Dateiname Gerätetyp	Beschreibung
ATV58Host	Altivar 58-Laufwerk
CEV300Host	CEV30020 Modbus an Ethernet-Bridge
CloudHub	Generischer oder unbekannter Hub
ConneXiumSwitch	499NxS17100/499NxS27100-Schalter
ConneXiumSwitchRM	499NxS17100/499NxS27100 Schalterredundanz-Manager
ConneXiumSwitchSM	499NxS17100/499NxS27100 Schalter-Standby-Manager
DefaultManagedHost	Generischer, verwalteter SNMP-Host
DefaultManagedMBAPHost	Generischer Modbus-TCP-Host
DefaultManagedSwitch	Generischer, verwalteter SNMP-Schalter
DefaultRouter	Generischer Router
DefaultUnmanagedHost	Nicht-SNMP-Host oder -Gerät
DefaultUnmanagedMBAPHost	Nicht-SNMP-Modbus-TCP-Host
DefaultUnmanagedSwitch	Generischer oder nicht verwalteter Schalter
ENTV1Host	Momentum ENT11000/11002
ENTV1Host	Momentum ENT11001
ETY410Host	Premium ETY 410x
ETY510Host	Premium ETY 510x
ETYPortHost	Eingebetteter Premium ETY-Port
ETZHost	Premium ETZ-Gateway
M1EHost	Momentum M1E-Prozessor
NIMHost	Advantys STB-Host
NOEHost	Quantum NOE 771-xx
NWMHost	Quantum FactoryCast HMI
PCoProHost	Premium Unity 5634 CPU
QCoProHost	Quantum Unity 6x1 CPU
TrHost	Generischer Transparent Ready-Host
WMYHost	Premium FactoryCast HMI

Verwenden Sie den Gerätetyp-Editor, um in den Gerätetypdateien zu blättern.

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 Zuggriffssteuerungsrichtlinien 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 *Serveroptionen* den Eintrag **Maximale Größe des Ereignisprotokolls** (tausend Ereignisse) aus: ● 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 Ereignisprotokolldatensätze 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 Netzwerkereignissen 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:	
	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: ● <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:	
	a	Geben Sie den *Namen* des Empfängers ein (maximal 32 Zeichen). **Hinweis:** Dieser Name wird der Liste "Empfänger" im Fenster "E-Mail-Konfiguration" hinzugefügt.
	b	Geben Sie im Feld *E-Mail-Adresse* 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.

Schritt	Aktion
5	Nehmen Sie in den Abschnitten *Kriterien senden* des Dialogfelds "Empfänger hinzufügen" die gewünschten Einstellungen vor. Hier können Sie das Senden von Ereignisnachrichten nach einem oder mehreren der folgenden Kriterien filtern: ● Ereignisschwere ● Netzwerk ● Geräte und Gerätetypen Siehe auch die Online-Hilfe zu ConneXview im Thema zum Hinzufügen von Empfängern für Informationen zur Filterauswahl.
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 *Schwere*, um die Liste zu sortieren, b. Blättern Sie zu den Elementen mit einem *Schwerewert* **Information** **Hinweis:** Elemente, die die Meldung *Alarmüberwachung deaktiviert* auslösen, haben immer den *Schwere*status **Information**.
3	Suchen Sie in der Spalte *Nachricht* nach folgendem Text: ● *Die Werteüberwachung ist deaktiviert.* oder ● *Der Alarm des Standard-Gateway ist deaktiviert.* Wählen Sie ein Gerät aus, auf dass 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: ● die IP-Adresse des Geräts auswählen, damit die statische Eigenschaft *Alarm Standard-Gateway?* zum Bearbeiten angezeigt wird ● in der Eigenschaftenliste nach unten blättern und Werteüberwachungen auswählen, damit das jeweilige Attribut *Überwachung* 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 *S. 44*).

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 *S. 44*). 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:

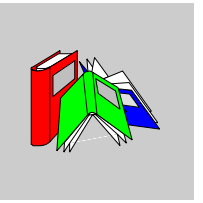
Schritt	Aktion
1	Suchen Sie die Datei "rmi.bat" und doppelklicken Sie darauf. Das Dialogfeld "RMI-Einstellungen" von ConneXview wird aufgerufen.
2	Wählen Sie eine IP-Adresse in der Liste *Adresse für RMI-Server* aus.
3	Klicken Sie auf **OK**. **Hinweis:** Die Änderungen an den Einstellungen für einen 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 *route*, 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 *route* die **Eingabetaste**. Der Befehl wird ausgeführt.	

Glossar



A

Abfrage
Erkennungsmethode, bei der ein Netzwerkverwaltungsgerät bei anderen intelligenten Netzwerkgeräten abfragt, ob diese Daten zu übertragen haben. Nachdem ein Netzwerkgerät den Erhalt dieser Nachricht bestätigt hat, ist es berechtigt, die Übertragung durchzuführen.

Abgeleitete Eigenschaft
Eine dynamische Eigenschaft, die ihren Wert von einer Funktion oder Berechnung erhält, die mit einer oder mehreren SNMP-, Modbus- oder anderen abgeleiteten Eigenschaften durchgeführt wird.

Abonnieren
Das Bekunden von Interesse an verfügbaren Informationen durch ein Gerät. Ein Gerät kann bis zu 2.048 4x-Register von bis zu 64 GDS-Herausgebern abonnieren. Beachten Sie, dass ein Abonnent die gesamte veröffentlichte Netzwerkvariable abonnieren muss, auch wenn nur ein Teil der Registerdaten erforderlich ist.

Adresse des Standard-Gateways
1. Das Gateway in einem Netzwerk, das ein Computer für den Zugriff auf ein anderes Netzwerk verwendet, wenn kein Gateway festgelegt wurde.
2. Der Router in einem Netzwerk mit Subnetzen, der Datenverkehr an ein Ziel außerhalb des Subnetzes des übertragenden Geräts weiterleitet.

Adressserver
In Quantum- und Premium-Kommunikationsmodulen verfügbar, um IP-Adressparameter mit BootP zu Clients zuzuweisen. Darüber hinaus unterstützen die Module Quantum NOE 771-01/11 und Premium ETY 4103/5103 den Austausch defekter Geräte.

Alarm Ein Hinweis auf ein Netzwerkproblem. Es wird ein Alarm ausgelöst, wenn der Wert einer überwachten Geräteeigenschaft folgendes Verhalten aufweist, wobei das Attribut *Schwere* entweder auf **Kritisch** oder auf **Achtung** festgelegt ist:

- Wert überschreitet einen Wert für einen Grenzwertmonitor, oder
- Wert ändert mehr als einen voreingestellten Grenzwert für einen Änderungsmonitor, oder
- Wert ändert sich in oder aus einem Wert aus einer Gruppe voreingestellter Werte für einen Statusmonitor

Änderungsmonitor Ein vorkonfigurierter Alarm-Trigger, der auf Änderungen des Werts einer überwachten Eigenschaft basiert.

Arithmetische Eigenschaft Eine abgeleitete dynamische Eigenschaft, die ihren Wert von einer arithmetischen Funktion erhält (Addition, Subtraktion, Multiplikation oder Division), die mit den Werten von zwei anderen dynamischen Eigenschaften durchgeführt wird.

ARP *Address Resolution Protocol (Adressauflösungsprotokoll).* Das Ethernet-Protokoll, das verwendet wird, um IP-Adressen mit einer MAC-Adresse zu verknüpfen.

Attribut Ein Wert aus einer Gruppe von Feldwerten, die zusammen eine Eigenschaft oder einen Eigenschaftsmonitor definieren.

Auslastungseigenschaft Eine abgeleitete dynamische Eigenschaft, die auf zwei schnittstellenbezogenen Eigenschaften basiert, einer Eingangsmessung und einer Ausgangsmessung, und die den kombinierten Wert als Einheiten/Zeit angibt.

B

Bandbreite Die Kapazität einer Netzwerkverbindung zum Übertragen von Daten. ConneXview überwacht die Bandbreitennutzung, also den Prozentsatz der verwendeten Bandbreite.

Bearbeitungsmodus Der Status von ConneXview mit geöffneter Netzwerkzuordnung, die zur Bearbeitung angezeigt wird.

Biegung Der im Bearbeitungsmodus erstellte Krümmungspunkt in einer Kommunikationsverbindung. Er wurde entweder durch Auswählen einer orthogonalen Struktur oder das manuelle Auswählen und Ziehen einer Kommunikationsverbindung erstellt.

Broadcast Eine Meldung, die an alle Geräte im Netzwerk gesendet wird.

C

Client/Server-Modus Methode zum Installieren und Ausführen von ConneXview als verteilte Softwareanwendung, die aus mindestens zwei einzelnen Komponenten besteht, darunter: 1 Serverkomponente, die über einen NT-Dienst Funktionen ausführt und Informationen bereitstellt, sowie eine oder mehrere Clientkomponenten (von denen eine auf dem Server-PC installiert sein muss), die als dezentrale Benutzeroberflächen fungieren und den NT-Dienst des ConneXview-Servers abonnieren.

Community-Name Der alphanumerische Name einer Zeichenkette, der als Schutzmechanismus verwendet wird, um einer Gruppe von Geräten Lese- oder Schreibzugriff zu gewähren. Für ConneXview ist nur die Community-Zeichenkette "Lesen" erforderlich. Die meisten Anbieter weisen der Community-Zeichenkette "Lesen" als Standardwert *Öffentlich* zu, Sie können diese Zeichenkette für das Gerät aber auch aus Sicherheitsgründen ändern.

CRC (*Cyclical Redundancy Check, Zyklische Redundanzprüfung*) Eine Möglichkeit, mit mathematischen Berechnungen zur Anzahl von Bits in einer Meldung diese auf Fehler zu überprüfen. Die Ergebnisse werden mit den Daten an den Empfänger gesendet. Dieser wiederholt die Berechnung mit den empfangenen Daten. Wenn die beiden Berechnungen unterschiedlich ausfallen, fordert der Empfänger ein erneutes Übertragen vom Absender an.

D

Datagramm Ein einzelnes Datenpaket, auch als Paket bezeichnet, das Daten und eine Kopfzeile mit Adressinformationen enthält. Diese werden über ein Netzwerk von einem Quellgerät an ein Zielgerät geleitet.

DeadBand Der Betrag (in Maßeinheiten) unter (bei hohen Einstellungen) oder über (bei niedrigen Einstellungen) dem Schwellwert, den die überwachte Eigenschaft erreichen muss, bevor der Alarm oder die mit dem Status verknüpfte Meldung gelöscht wird.

Dynamische Eigenschaft Eine Geräte- oder Kommunikationsverbindungseigenschaft, deren Wert nicht konstant ist, sondern sich während der Ausführung dynamisch verändern kann.

E

E/A-Abfragedienst Ein automatischer Client, der für Quantum-, Premium- und Momentum-Plattformen verfügbar ist. Mit der E/A-Abfrage können Lesen-, Schreiben- und Lesen/Schreiben-Halteregister für dezentrale Geräte eingegeben werden. Das Intervall kann in Millisekunden konfiguriert werden. Das Setup der E/A-Abfrage wird in Ihrer Programmieranwendung mit einer Tabelle durchgeführt, und nicht durch das Programmieren logischer Funktionen.

Erkennungs-bereich Die zu erkennenden Geräte sind durch einen Bereich von IP-Adressen definiert. Der Bereich ist festgelegt durch die Subnetzadresse und den Wert der Subnetzmaske, die eine Liste aller Kandidatadressen innerhalb des Subnetzes definiert. Sie können den Bereich manuell einschränken, indem Sie die Start- und/oder Endadressen im Dialogfeld **Subnetz bearbeiten** oder **Subnetz hinzufügen** anpassen.

Ethernet Eine Familie von LAN-Protokollen nach dem Standard IEEE 802.3.

F

Farb-Mapkey Ein Farb-Mapkey verweist auf eine Statusaufzeichnungseigenschaft und setzt den Wert dieser Eigenschaft in Relation zu einem Farbschema. Wenn Sie einen Farb-Mapkey im Überwachungsmodus auswählen, werden alle Geräte und Kommunikationsverbindungen im Netzwerkkarten-Viewer in einer Farbe angezeigt, die den Wert der zugeordneten Eigenschaft angibt.

FDR *Faulty Device Replacement (Austausch defekter Geräte)* Ein Prozess zum einfachen Austauschen eines fehlerhaften Geräts und zum Wiederherstellen der konfigurierten Parameter des ausgetauschten Geräts.

Firewall Ein Router oder eine Workstation mit mehreren Netzwerkschnittstellen, der bzw. die bestimmte Protokolle, Datenverkehrstypen innerhalb dieser Protokolle, Diensttypen und die Richtung des Informationsflusses steuern und einschränken.

FTP *(File Transfer Protocol, Dateiübertragungsprotokoll)* Das für die Dateiübertragung zwischen Geräten zuständige Kommunikationsprotokoll.

G

Gateway

1. Bezieht sich in der Regel auf einen Router. Ein Router ist ein Gerät, das Datenpakete zwischen Netzwerken überträgt. Ein Router ist mindestens mit zwei Netzwerken verbunden, in der Regel zwei LANs oder WANs bzw. einem LAN und dem Netzwerk des Internetdienstanbieters. Router befinden sich an Gateways, also dem Ort, an dem Netzwerke miteinander verbunden werden. Router verwenden Kopfzeilen und Weiterleitungstabellen, um den besten Pfad zum Weiterleiten der Pakete zu ermitteln. Darüber hinaus arbeiten sie mit Protokollen, z. B. ICMP, um miteinander zu kommunizieren und die optimale Verbindung zwischen zwei Hosts zu konfigurieren.
2. Eine Kombination von Hardware und Software, durch die Netzwerke oder Netzwerkgeräte verbunden werden, die sonst nicht miteinander kompatibel wären. Gateways umfassen Packet Assembler/Disassembler (PADs) und Protokollkonverter. Sie werden in den Schichten 5, 6 und 7 des OSI-Modells ausgeführt, also in der Sitzungs-, Darstellungs- bzw. Anwendungsschicht.

Gerät

Die an einem Netzwerkknoten befindliche Hardware. Eine Instanz eines Gerätetyps.

Gerätetyp

Eine im Gerätetyp-Editor erstellte und bearbeitbare Gerätekategorie.

Globale Daten (Dienst)

Bei GDS (Global Data Service, Dienst "Globale Daten") wird die Funktion *Veröffentlichen/Abonnieren in Echtzeit* für ein Gerät verwendet, um eine Tabelle zur Registrierung von Variablen zu veröffentlichen. Daraufhin abonnieren andere Geräte innerhalb dieses Subnetzes die Variablentabelle. Um die Variable mit einem einzigen UDP-Paket gleichzeitig an mehrere Pakete zu verteilen, verwendet der Dienst UDP Multicast. Die Module Quantum NOE 771-01/11 oder Premium ETY 4103/5103 bieten weitere Informationen zu GDS.

Grenzwertmonitor

Ein vorkonfigurierter Alarm-Trigger, der ausgelöst wird, wenn der Wert einer überwachten Eigenschaft den Sollwert erreicht oder überschreitet.

H

Host

Der Endknoten eines Netzwerks, z. B. ein PC, eine SPS, ein E/A-Gerät oder Ähnliches. Ein Host-Gerät enthält keinen Router oder Switch und hat eine ganz andere Funktion.

HTTP *(Hyper Text Transfer Protocol)* Das zum Surfen im Internet erforderliche Kommunikationsprotokoll.

I

ICMP *Internet Control Message Protocol.* Das Internetprotokoll, das Fehler meldet und Informationen zur Datagrammverarbeitung bereitstellt.

IP *Internet Protocol.* Der Teil der TCP/IP-Protokollfamilie, der die Internetadressen von Geräten verfolgt, ausgehende Nachrichten weiterleitet und eingehende Nachrichten erkennt.

IP-Adresse Eine eindeutige 32-Bit-Adresse, die zu TCP/IP-Geräten im Internet zugewiesen wurde. Geschrieben wird sie in vier Oktetten mit Dezimalzahlen, die durch einen Punkt voneinander getrennt sind. Zu einer IP-Adresse gehören eine Netzwerknummer, eine optionale Subnetzwerknummer und eine Gerätenummer. Mit der Netzwerk- und der Subnetzwerknummer werden Nachrichten weitergeleitet und die Gerätenummer dient als spezifische Adresse in einem Netzwerk oder Subnetzwerk. Eine Subnetzmaske ist ein Filter, der die Netzwerknummer von der Subnetzwerknummer trennt.

J

Jabber Netzwerkfehler, der durch eine Schnittstellenkarte verursacht wurde, über die beschädigte Daten in das Netzwerk gelangen.
Auch eine Fehlerbedingung, die dadurch verursacht wurde, dass ein Ethernet-Knoten Pakete übertragen hat, die länger als zulässig sind.

K

Knoten Der Endpunkt eines Netzwerkabschnitts (der z. B. zu einem Host-PC führt) oder ein Schnittpunkt von mehreren Netzwerkpfaden (z. B. der Standort eines Hubs, Switches oder Routers).

Kopfzeile Die Steuerungsinformationen, die an den Anfang einer übertragenen Nachricht eingefügt werden. Sie umfassen wichtige Informationen, wie Paket- oder Blockadresse, Quelle, Ziel, Nachrichtennummer, Länge und Routinganweisungen.

M

MAC-Adresse *Media Access Control Address.* Eine in einem Netzwerk einmalig vergebene 48-Bit-Nummer, die bei Herstellung in jeder Netzwerkkarte oder in jedem Netzwerkgerät programmiert wird.

MBAP *Modbus-Anwendungsprotokoll*. Das TCP/IP-basierte Standardprotokoll, mit dem Master/Slave- bzw. Client/Server-Kommunikationen zwischen intelligenten Geräten in einem Ethernet-Netzwerk verwaltet werden.

MIB *Management-Informationsbasis.* Eine einheitliche akzeptierte hierarchische Datenstruktur mit Objekten, auch Geräteeigenschaften genannt, die ein Gerät in einem SNMP-Netzwerk lesen und in einigen Fällen auch schreiben kann. Die hierarchische Datenstruktur enthält sowohl öffentliche (standardmäßige) als auch private (proprietäre) Verzweigungen.

Modbus Ein Nachrichtenaustauschprotokoll für die Anwendungsschicht. Modbus bietet Client- und Server-Kommunikation zwischen Geräten, die an verschiedene Arten von Bussen oder Netzwerken angeschlossen sind. Modbus bietet viele durch Funktionscodes spezifizierte Dienste.

N

Netzwerkzu-ordnung Die Darstellung eines Netzwerks im Diagramm, entweder im Bearbeitungs- oder im Überwachungsmodus.

NTP *Network Time Protocol* Ein Kommunikationsprotokoll, mit dem die Uhrzeit über ein Netzwerk ausgetauscht und synchronisiert wird.

NWM *Netzwerkzuordnung* Dateierweiterung für eine Netzwerkzuordnungsdatei, die Informationen über alle Geräte in einem Netzwerk, deren Verbindungen untereinander und ihre Einstellungen enthält.

O

OID — *Objektbezeichner.* Eine numerische Sequenz in Dezimalpunktschreibweise, die eindeutig auf ein Objekt in einer MIB verweist und dieses beschreibt. Jedes numerische Segment in der Sequenz beschreibt einen eindeutigen Speicherort in der MIB-Hierarchie und jedes nachfolgende numerische Segment gibt eine Unterverzweigung aus Segmenten höherer Ebene an.

P

Paket — Eine Reihe einzelner Bits, die Daten und Steuerungsinformationen enthalten und für die Übertragung zwischen Knoten formatiert sind. Ein Paket besteht aus einer Kopfzeile mit einem Frame für den Anfang, der Quell- und Zieladresse, Steuerungsdaten, der eigentlichen Nachricht und einem Nachspann mit Fehlern (auch *Frame Check Sequence (Rahmenprüfsumme)* genannt).

Physikalische Schicht — Schicht 1 (die niedrigste Schicht) des OSI-Referenzmodells wird durch den physikalischen Kanal implementiert. Sie bestimmt die Hardwareverbindungen und die Kodierung des Bytestroms zur Übertragung. Diese Schicht ist die einzige, bei der Daten zwischen Netzwerkknoten physikalisch übertragen werden. Die physikalische Schicht isoliert Schicht 2 (die Sicherungsschicht) von mediumabhängigen physikalischen Merkmalen wie Basisband, Breitband oder Glasfaser. Schicht 1 definiert die Protokolle, die Übertragungsmedien und -signale steuern.

Ping — *Packet Internet Groper.* Die Kombination aus einer ICMP-Echoanfrage und deren Antwort wird in IP-Netzwerken verwendet, um festzustellen, ob ein Gerät erreichbar ist und wie lange dies dauert.

Protokollanalysator — Eine Software, die Datenverkehr in einem Ethernet-Netzwerk abfängt und analysiert. Sie ermöglicht das Überwachen der Netzwerkverwendung, das Erkennen des Eindringens in ein Netzwerk sowie das Erfassen von Netzwerkstatistiken.

Q

Quittieren Das Vorhandensein eines Netzwerkalarms zur Kenntnis nehmen. Die Person, die den Alarm quittiert, soll diesen diagnostizieren und das Problem lösen.

R

Router Ein Gerät, das Datenpakete zwischen Netzwerken überträgt. Ein Router ist mindestens mit zwei Netzwerken verbunden, in der Regel zwei LANs oder WANs bzw. einem LAN und dem Netzwerk des Internetdienstanbieters. Router befinden sich an Gateways, also dem Ort, an dem Netzwerke miteinander verbunden werden. Router verwenden Kopfzeilen und Weiterleitungstabellen, um den besten Pfad zum Weiterleiten der Pakete zu ermitteln. Darüber hinaus arbeiten sie mit Protokollen, z. B. ICMP, um miteinander zu kommunizieren und die optimale Verbindung zwischen zwei Hosts zu konfigurieren.

S

Scan Eine nicht intrusive Methode zum Ermitteln aktiver Netzwerkgeräte und ihrer geöffneten Ports.

Sicherungs-schicht Schicht 2 des aus sieben Schichten bestehenden OSI-Referenzmodells für die Kommunikation zwischen Computern in Netzwerken. Diese Schicht definiert Protokolle für Datenpakete und die Art und Weise ihrer Übertragung zu bzw. von den einzelnen Netzwerkgeräten. Es handelt sich um eine Kommunikationsfunktion auf Verbindungsebene mit mittlerer Unabhängigkeit, die sich ganz oben in der physikalischen Schicht befindet und in zwei Unterschichten unterteilt ist: MAC (Medium-Access Control) und LLC (Logical-Link Control).

SMTP *Simple Mail Transfer Protocol* Das gängigste Kommunikationsprotokoll zum Senden und Empfangen von E-Mails in einem Netzwerk.

SNMP *Simple Network Management Protocol.* Das UDP/IP-Standardprotokoll, mit dem Geräte in einem IP-Netzwerk verwaltet werden, darunter Hosts (also Client- oder Server-PCs), Router, Switches und Hubs. ConneXview unterstützt SNMP Version 1.

Standalone-Modus Methode zum Installieren und Ausführen von ConneXview als integrierte Softwareanwendung auf einem einzelnen PC.

Standardeigenschaft Eine SNMP- oder Modbus-Eigenschaft, deren Wert sich dynamisch während der Ausführung ändert.

Start-Modus Der Status von ConneXview ohne geöffnete Netzwerkzuordnung.

Statische Eigenschaft Eine Geräte- oder Kommunikationsverbindungseigenschaft, deren Wert beim Erstellen der Geräte- oder Kommunikationsverbindung festgelegt wird und der sich nicht während der Ausführung dynamisch verändert.

Statusmonitor Ein vorkonfigurierter Alarm-Trigger, der ausgelöst wird, wenn der Wert einer überwachten Eigenschaft dem Mitglied einer Gruppe von festgelegten Sollwerten entspricht oder nicht entspricht.

Subnetz *Subnetzwerk.* Eine Gruppe von Geräten, die dieselbe Netzwerkadresse verwenden. In der Regel ein Segment eines größeren Netzwerks.

Subnetzmaske Ein auf eine IP-Adresse angewendeter Filter, um die Netzwerkadresse von der Host- oder Geräteadresse zu unterscheiden.

T

TCP/IP (*Transmission Control Protocol/Internet protocol*) Eine Protokollfamilie, die Anfang der 70er Jahre von der Advanced Research Projects Agency (ARPA) des US-Verteidigungsministerium entwickelt wurde. Das Ziel bestand darin, verschiedene Arten von Netzwerken und Computern miteinander zu verbinden. TCP/IP bietet nicht denselben Funktionsumfang wie OSI.
TCP/IP ist ein Transport- und Internetprotokoll und stellt praktisch den Netzwerkstandard dar. Die Daten werden meistens über X.25 und Ethernet übertragen und das Protokoll ist eines der wenigen, das als Migrationspfad zu OSI dienen kann. TCP/IP kann in den meisten Umgebungen ausgeführt werden. TCP/IP ist den Schichten drei und vier des OSI-Modells zugeordnet, also der Netzwerk- bzw. Transportschicht.
TCP und IP sind die Standardnetzwerkprotokolle in UNIX-Umgebungen. Sie werden fast immer zusammen implementiert und verwendet.

TFTP *(Trivial File Transfer Protocol)* Eine vereinfachte Form des FTP. Es wird oben im UDP implementiert und bietet keine Sicherheitsfunktionen.

U

Überwachungsmodus Der Status von ConneXview mit geöffneter Netzwerkzuordnung, die zur Netzwerküberwachung in Echtzeit angezeigt wird.

UDP *User Datagram Protocol.* Ein Protokoll für den verbindungslosen Modus, bei dem Meldungen in einem Datagramm an ein Zielgerät gesendet werden. Das UDP-Protokoll ist normalerweise mit dem Internet Protocol (UPD/IP) gepaart.

V

Verbindung *Kommunikationsverbindung.* Eine Netzwerkverbindung zwischen zwei Geräten.

Veröffentlichen Das Bereitstellen und Verteilen von Informationen. Ist bei den Modulen Quantum NOE 771-01/11 und ETY 4103/5103 der Dienst "Globale Daten" (GDS) aktiviert, können sie eine einzelne Multicast-Netzwerkvariable mit bis zu 512 Registern für eine Gruppe von GDS-Abonnenten veröffentlichen. Dies kann in Intervallen des CPU-Scans konfiguriert werden.

X

XWAY Premium-Adressierung im Format {Netzwerkstation} zum Verwenden des Modbus- oder UNI-TE-Protokolls.

Z

Zuordnungseigenschaft *Statusaufzeichnungseigenschaft.* Eine abgeleitete dynamische Eigenschaft, die einem Farb-Mapkey zugeordnet werden kann. Eine Statusaufzeichnungseigenschaft enthält vier benutzerdefinierte Trigger für Schwellwerte (High-High, High, Low, Low-Low). Ein Farb-Mapkey verweist auf eine Statusaufzeichnungseigenschaft und setzt jeden Trigger für Schwellwerte in Relation zu einer Farbe.