Das Wissensportal

ComConsult Research
IT-Wissen für Ihr Unternehmen

SNMP Versionen 2 und 3

4. Januar 2013 von Dr. Franz-Joachim Kauffels

Teil 65 von 71 aus der Serie "Professionelle Datenkommunikation"
Alle Artikel der Serie "Professionelle Datenkommunikation":

- DC-History (1): die geordneten 70er
- DC-History (2): die wilden 80er
- Übersicht über TCP/IP
- TCP
- IP
- DC-History (3): Rise of the Internet
- Anwendungsunterstützung mit TCP/IP-Protokollen
- Internet-Grundfunktionen (2)
- Internet-Grundfunktionen (1)
- Weiterentwicklung der Web-Achitekturen
- Erweiterungen der Grundkonzepte: Java, HTML 3 und XML
- DC-History (5): E-Business: der aufrechte Gang
- DC-History (4): von der Präsenz zum Profit
- Intranet-Nutzungsphasen
- E-Business Frühindikatoren
- 1:1-Marketing mit dem Internet und Intranets (1)
- Die Wirtschaftlichkeit von Intranets
- 1:1-Marketing mit dem Internet und Intranets (2)
- Spezielle Probleme der Internet/Intranet-Technologie
- Sicherheitsprobleme und -lösungen in Netzen
- Schutz von Objekten in verteilten Umgebungen
- Objekte in vernetzten und verteilten Systemen
- Schwachstellen der Informationssicherheit in Netzen und Absicherungsmaßnahmen bis zur Schicht 5
- Sicherung der Information ab der Datendarstellungsschicht
- Firewall-Systeme
- Transaktionssicherheit
- Verschlüsselungsverfahren
- Protokolle für die Übertragung schützenswerter Daten auf Netzen
- Sicherheitsaspekte in WLANs
- Neue Wege zur WLAN-Sicherheit
- Netzwerk-Management und Betrieb
- Funktionen des integrierten Netzwerk-Managements
- Methoden der Integration von Management-Instrumenten
- Netzwerk-Management Standards
- RMON: Remote Monitoring
- SNMP Versionen 2 und 3
- Web-based Network Management
- Wichtige Netzwerk-Management Produktstrategien
- Wandel der Bedarfsentwicklung im Netzwerk-Management

- Unangenehme Erfahrungen zum Netzwerk-Management
- Privat: Die Zukunft des Netzwerk-, Service- und Anwendungs-Managements
- Unangenehme Erfahrungen zum Netzwerk-Management
- Der Einfluss der Globalisierung

Recht schnell nach seiner Definition nutzten fast alle Netzwerk-Management-Systeme weltweit SNMP. Die Problemstellung war, SNMP sowohl in der Leistung als auch in der Sicherheit zu verbessern. Die SNMP-Erfinder der Internet Engineering Task Force haben Ende 1992/Anfang 1993 eine verbesserte und erweiterte Definition mit dem Namen SMP vorgestellt, die zunächst auf Management-Plattformen mit SNMP koexistieren soll. SMP wurde mit einigen Erweiterungen schnell zu SNMP2. Sicherheitsprobleme führten zu der Definition von SNMP 3.

Die wesentlichen Unterschiede zwischen SNMP und SNMP2 sind folgende:

- SNMP2 benutzt nicht nur UDP/IP, sondern lässt ein ganzes Spektrum von möglichen Transportprotokollen, darunter Appletalk, IPX und OSI-Protokolle.
- Ein Bulk Retrieval Mechanismus sorgt dafür, dass man tabellenartigen Informationen von Agenten mit einem zügigen Protokoll erhalten kann.
- Es gibt Manager-zu-Manager-Kommunikation.
- In Überarbeitung der Vorschläge des Secure SNMP werden Sicherheitsfunktionen angeboten.

SNMP2 verbessert die Operation und Kontrollfunktionen des SET REQUEST. Durch einen Verschlussmechanismus kann eine Management-Station die Konfiguration eines Gerätes durchführen, ohne unterbrochen zu werden. Erst nach Abschluss der Konfiguration wird der Verschlussmechanismus geöffnet.

Die Funktionen für das Auslesen und Übertragen von Tabellen werden in SNMP2 zum ersten Male geschlossen definiert. Es gibt eine für eine Management-Station jetzt auch die Möglichkeit, neue Variablen in einem Agenten zu erzeugen, also eine Teilfunktion der CREATE-Aktion z. B. bei CMIP. Das neue GETBULK-Kommando erlaubt einer Management-Station den gleichzeitigen Empfang eines ganzen Bereiches von Variablen, was bei SNMP mühevoll mit einer leistungsfressenden GET-NEXT-Schleife gemacht werden muss.

SNMP2 definiert einige neue Datentypen, darunter 64-Bit Counter für Ereignisse, einen Datentyp für OSI-Adressen, der das SNMP-Management auch auf OSI-Netze erweitern hilft, und erlaubt in Abhängigkeit vom Kontext sogar die Definition von Subtypen. Dies ist eine Forderung, die die Verfechter des CMIP immer wieder gefordert haben. Ein

SNMP-Agent weist eine Anfrage insgesamt zurück, wenn er bestimmte MIB-Variablen oder Parameter nicht hat. In SNMP2 soll es für diesen Fall Ausnahmebedingungen geben. Außerdem gibt es insgesamt mehr Error-Codes als bei SNMP. Neue Makros erlauben MIB-Erweiterungen in kompilierbarer Form. Früher konnten Erweiterungen bei Kompilierung der MIB verlorengehen.

Mit dem INFORM-Kommando kann eine SNMP2-Management-Station einer anderen SNMP2-Management-Station im Rahmen eines verbindungsorientierten Manager-zu-Manager Kommunikationsdienstes Informationen zukommen lassen und Empfangsbestätigungen anfordern. Dazu gibt es eine neue SNMP2-MIB, die den Informationsaustausch regelt, insbesondere die Art und Weise, in der Ereignisse aufgearbeitet und an andere Management-Stationen verteilt werden. Diese Kommunikation ermöglicht den Aufbau hierarchischer Management-Strukturen.

Ganz besonders wichtig ist jedoch die Loslösung von der TCP/IP- Protokollfamilie. SNMP2 macht die Verwendung des DES-Standards zur Option und nicht zwingend. Dies ist auch dadurch begründet, dass die US-Regierung den Export von DES-verschlüsseltem Source Code lange Zeit verboten hat. Außerdem dürfen Pakete ruhig in veränderter Reihenfolge eintreffen.

Ein wichtiges SNMP2-Ziel ist aber die Rückwärtskompatibilität zu SNMP: die gesamten SNMP-MIB-Definitionen können in SMP weiter benutzt werden. Dies ist wichtig, denn in diesen Definitionen steckt die eigentliche Arbeit, die Netzwerk-Management-Anwendungen sind zweitrangig: dies ist zu vergleichen mit der Situation des Wechsels von einem Textprogramm auf ein anderes: kann man im neuen Programm alle bisher geschriebenen Texte weiterbenutzen und neu bearbeiten, ist es gut, wenn nicht, sollte man ggf. von dem neuen Programm Abstand nehmen. Schließlich sehen die SMP-Dokumente Migrationsstrategien und die Koexistenz von SMP- und SNMP-Lösungen auf einer Workstation vor.

SNMP2 räumt die meisten Kritikpunkte der SNMP-Gegner (und vor allem die der bisherigen SNMP-Benutzer) aus. Zum OSI-Management bleibt letztlich der Unterschied zwischen objektorientiertem (CMIP) und relationalen (SNMP) Ansatz. Für die Lösung praktischer Management-Probleme ist eine allzu lange Diskussion über diese Fragestellungen jedoch unangebracht.

Durch das sogenannte Party-Konzept wird eine Dreistufigkeit der Management-Hierarchie erreicht, da es nicht mehr nur Agenten und NMS gibt, sondern Node Manager, Lokale Manager und Super-Manager. Das führt für den Anwender wiederum dazu, dass er sich diese Hierarchie genauestens überlegen muss. SNMP2 hat drei verschiedene lokale Datenbanken, nämlich für unterstützte Parties, verwaltete Ressourcen und

die Zugriffskontrollvorschriften. Die Formulierung von Zugriffsrechten und Gruppen ist relativ kryptisch. Durch die Notwendigkeit der Prüfung nach Zugehörigkeit zu bestimmten Gruppen, der Einordnung in einen bestimmten Kontext und des Geltungsbereichs der Rechte im Einzelnen ist eine SNMP2-Sendung bzw. ein SNMP2-Empfang zu einer komplexen zusammengesetzten Operation geworden. SNMP2 wurde bislang weder von Herstellern noch von Anwendern akzeptiert. Die Entwicklung wurde eingestellt. Stattdessen gibt es nunmehr einen Vorschlag SNMP3, der zwar Verschlüsselung und Austausch von größeren Datenmengen vorsieht, aber ansonsten auf allzu komplexe Operationen verzichtet. Wir werden sehen, was daraus wird.

SNMP Version 3

Eine wichtige Eigenschaft von SNMP ist es, vor allem in Verbindung mit RMON alle Datenströme sehen zu können, die es gibt. Leider wurde in den Versionen 1 und 2 überhaupt nichts für die Sicherheit getan, was dem Protokoll auch den Spitznamen einbrachte: SNMP: Security is Not My Problem!

SNMP benutzt den Community String zur

- Identifizierung
- Authentifizierung
- Autorisierung
- unverschlüsselt in der SNMP-Nachricht

SNMP hat keine standardisierte Form der Verschlüsselung, das bedeutet:

- keine Authentifizierung: jeder kann SNMP-Messages nachmachen
- keine Vertraulichkeit von Daten: jeder kann das Netz sehen
- keine Integrität: jeder kann die Daten verändern
- keine Autorisierung im laufenden Betrieb

Also hat die IETF genau diese Probleme aufgenommen und sowohl den Verkehr zwischen Agenten und Management Station als auch den Zugang zur Management-Station mit den in den Folgen 30 bis 41 beschriebenen Verfahren abgesichert.

Mittlerweile hatten aber auch alle Hersteller von Plattformen diese Sicherheitsprobleme aufgegriffen. Sicherheit ist nichts, was man statisch einführen kann, sondern die Mechanismen müssen sich permanent auf die Bedrohungen einstellen. Die diesbezüglichen Sicherheitslösungen von den Herstellern werden also von Zeit zu Zeit erneuert, die aus dem Standard selbst eher weniger. So hat sich bis heute SNMP V3 nur wenig verbreitet, die meisten Betreiber setzen auf SNMP V2 und RMON angereichert um aktuelle Sicherheitsmaßnahmen aus den Plattformen.

Bleibt noch ein Problem für die Hersteller, die zwar Geräte und die dazu passenden MIBs anbieten, aber keine übergreifenden Management-Plattformen.

Das Ende des SNMP-Gedankens

Eine wichtige Eigenschaft von SNMP war von Beginn an, dass die MIBs zwar einen standardisierten Teil besitzen, der immer gilt und von allen Plattformen verstanden wird, aber auch einen Teil, der für herstellerspezifische Informationen reserviert ist.

Das haben die Hersteller von Beginn an kräftig benutzt und gleichzeitig relativ kompakte Management-Plattformen für die optimale Steuerung ihrer Geräte aufgesetzt. Das sind zwar keine unternehmensübergreifenden Plattformen, der Gerätepark eines Herstellers lässt sich damit aber prima verwalten. Hersteller haben ja ein Interesse daran, dass ein Kunde möglichst durchgängig ihre Produkte einsetzt.

Der Kunde hatte nun eine Entscheidung zu treffen:

- Einrichtung einer rein standardisierten, übergreifenden Plattform unter Verzicht auf die von einem Hersteller lieferbaren Zusatzfunktionen
- Einrichtung einer herstellerspezifischen Plattform mit allen Funktionen unter Schaffung eines Integrationsproblems in eine übergreifende Plattform

Die meisten Kunden haben zur letzteren Alternative gegriffen. Ein Beispiel für eine solche Plattform wäre Cisco Works. Es unterstützt SNMP und fast unvorstellbar viele Zusatzfunktionen. Es hat einen hohen Sicherheitsstandard und darüber hinaus auch noch den Vorteil, dass man nicht nur LANs oder RZ-Netze, sondern praktisch alle zusammengesetzten Netzformen mit Elementen wie WAN-Strecken und Wireless-Versorgungsbereiche einheitlich damit steuern kann und ein immenses Angebot für die Analyse solcher zusammengesetzten Umgebungen bekommt, solange auf allen benutzten Geräten der Name „Cisco" steht.

Auch Hersteller mit vergleichsweise kleinerem Anteil am weltweiten Umsatz mit Netzkomponenten gehen diesen Weg.

Der ursprüngliche Ansatz von SNMP zum herstellerübergreifenden Management ist dadurch faktisch längst gestorben.

« Teil 64: RMON: Remote MonitoringTeil 66: Web-based Network Management »