

Management-Systeme

Jens-Uwe Winks | winks@cms.hu-berlin.de

SPECTRUM OneClick

ist ein Netzwerkmanagementsystem der Firma CA auf der Grundlage von Java. Es arbeitet Client/Server-basiert mit Tomcat-Server. Damit ist es auf der Client-Seite betriebssystemunspezifisch und erfordert außer Java keine Softwareinstallation. Spectrum erlaubt die Abbildung sehr komplexer Strukturen eines Datennetzes. Die Modellierung geht hinab bis zu einzelnen Ports einer Komponente, den Verbindungen zwischen den Ports verschiedener Geräte und den Darstellungen des Zustands dieser Modelle. Spectrum unterstützt das aktive Abfragen von Netzwerkkomponenten mittels SNMP. So können Informationen direkt ausgelesen werden. Das Spectrum-Managementsystem dient vor allem zum Überwachen der Datenverbindungen und aktiven Komponenten

des HU-Netzes. Es hat außerdem die Aufgabe der Dokumentation der Netzwerktopologie. Es arbeitet herstellerneutral in Bezug auf die verwalteten Netzwerkkomponenten.

Enterasys Netsight Suite

Im LAN-Edge-Bereich werden an der HU fast ausschließlich Geräte der Firma Enterasys eingesetzt. Diese bietet ein eigenes Managementsystem an. Es unterstützt natürlich vor allem Geräte des Herstellers, da dieses System die herstellereigenen SNMP-MIBs bereits implementiert hat. Die Suite besteht aus mehreren Programmteilen, wovon an der HU die Netsight Console, der Inventory-Manager und der Policy-Manager einsetzbar sind. Letzterer wird bisher nicht genutzt.

Eine Übersicht über Systeme für das Management von Datennetzen, die die Netzwerkgruppe des CMS einsetzt, bietet die folgende Abfassung. Es werden Systeme und Tools skizziert, die überwiegend für Netzwerkadministratoren interessant sind. Das Tool Netwatch bietet darüber hinaus unseren Nutzern die Möglichkeit, sich über den Netzwerkzustand zu informieren.

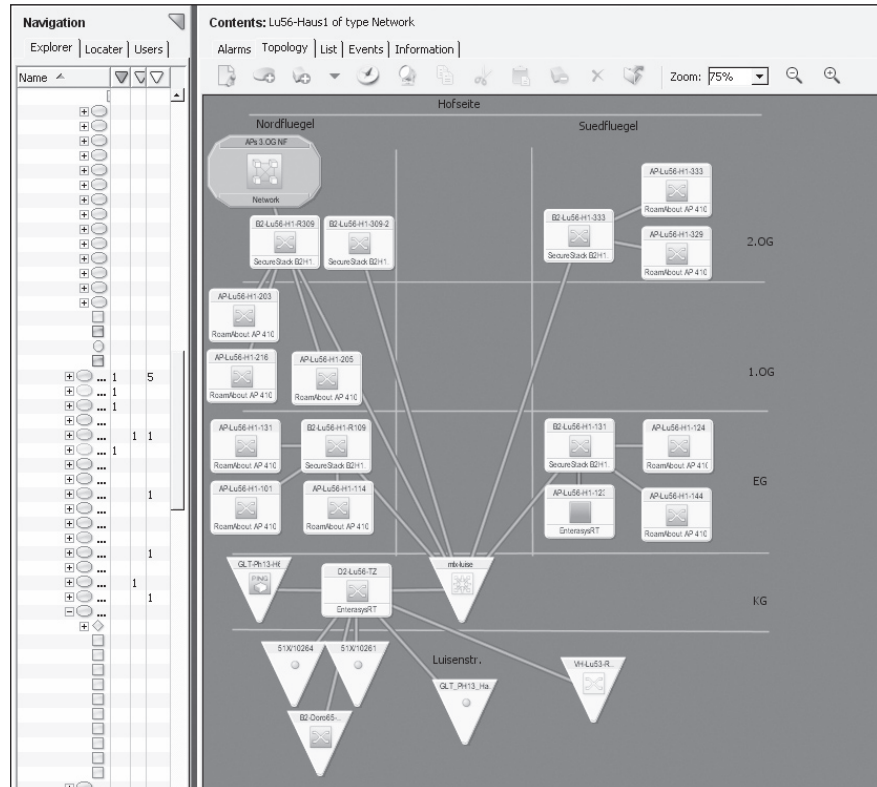


Abb. 1: Ausriß Spectrum OneClick

Netsight setzt Java voraus und arbeitet Client/Server-basiert. Der Client wird als Applet heruntergeladen und ausgeführt.

Netsight Console

Die Console stellt die Grundanwendung der Suite dar. Sie liefert eine Übersicht über alle Geräte und den Status dieser und bietet eine Abfragemöglichkeit bis hinab auf Portebene der Netzwerkgeräte. Die Console verfügt mit ihren Flexitools über eine starke Möglichkeit, nutzerdefinierte Abfragen einzubauen und beinhaltet außerdem bereits eine Vielzahl von vordefinierten Abfragemöglichkeiten.

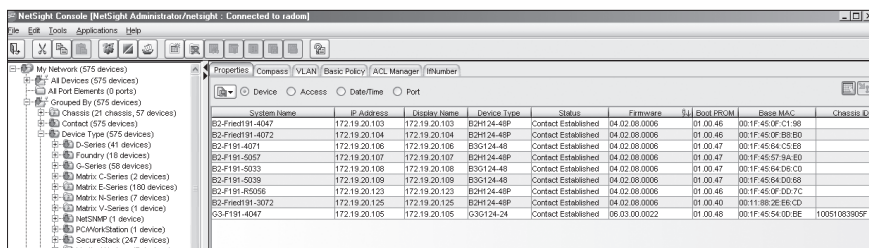


Abb. 2: Ausriß Netsight Console

Die Komponenten lassen sich individuell gruppieren. Dies erhöht die Übersichtlichkeit. Die Sortierung kann parallel auch nach vorgegebenen Kriterien erfolgen – z. B. nach Gerätetyp oder Subnetz. Es gibt eine Topology-Map, welche die grafische Darstellung des Netzwerks und seiner Komponenten erlaubt. Die Flexibilität der Topology-Map ist nicht sehr groß. Sie eignet sich daher vor allem für überschaubare Netze.

Eine wesentlich Stärke der Console ist ihr Compass. Das ist eine Suchfunktion für MAC- oder IP-Adressen. Dabei werden auswählbare Komponenten eines Bereichs abgefragt. Der Clou: Die Console ermittelt und liefert dabei auch Informationen über inaktive Clients.

Netsight Inventory Manager

Der Inventory Manager ist eine Erweiterung der Netsight Console. Er erlaubt Firmware- und Konfigurationsmanagement inklusive eines zeitgesteuerten Backup-Features. Er verfügt über eine Restore-Funktion für die Konfigurationen der Netzwerkgeräte und einen Reset-Manager.

Gerade das Backup-Management ist ein starkes Instrument. Hiermit lassen sich für Geräteklassen Abzüge der Konfiguration für definierte Intervalle automatisch in mehreren Generationen erstellen. Insbesondere beim Einsatz von vielen Netzwerkgeräten ist dies von Vorteil. Beim Ausfall eines Switches lässt sich so beispielsweise die Konfiguration innerhalb von Minuten auf ein Ersatzgerät spielen. Weiterhin bietet das Firmware-Management ein Feature für die effiziente Verwaltung der Softwarestände auf den Geräten. Dazu gehört auch ein Reset-Manager für den gesteuerten Neustart von Komponenten.

Netwatch soll den Nutzern eine Möglichkeit der Netzwerküberwachung bieten. Diese Grafik wird im WWW abgelegt (<http://www.cms.hu-berlin.de/dl/netze/netzintern/netwatch/>) und ist nur aus dem Netz der HU zu erreichen.

Die Abbildung 3 zeigt dabei einen Blick auf das Netz aus einem ganz bestimmten Winkel. Dargestellt werden die Kernnetzrouter des „alten“ HU-Backbones (z. B. CR-ESZ) und die MPLS-Router des neuen 10 Gigabit-Backbones (Bsp.: MLX-ESZ) sowie die an sie angeschlossenen Standorte. In den Standorten sind weitere Router und Switches zusammengefasst. Aus diesen leitet sich der Status der einzelnen Knoten ab (grau, grün, orange, rot). Alle Geräte, die in einem Standort arbeiten, werden tabellarisch angezeigt – durch Anklicken eines entsprechenden Standorts wird die Übersicht wiedergegeben. Die auf diesen Detailseiten einbezogenen WLAN-Accesspoints haben dabei keinen Einfluss auf den Status einer Einrichtung im Hauptbild – ein ausgefallener Accesspoint wirkt sich also nicht auf die Gesamtübersicht aus.

Die beiden Firewall-Cluster an der Außenanbindung des HU-Backbones sind ebenfalls abgebildet, ebenso der dahinter liegenden Router des DFN-Vereins und die des Berliner Wissenschaftsnetzes BRAIN.

Netwatch

Netwatch ist eine Eigenentwicklung des CMS und basiert auf PHP5 und Perl. Es erzeugt eine Grafik mit dem aktuellen Status von Geräten, Standorten und Leitungen zwischen diesen. Benutzt wird dazu SNMP.

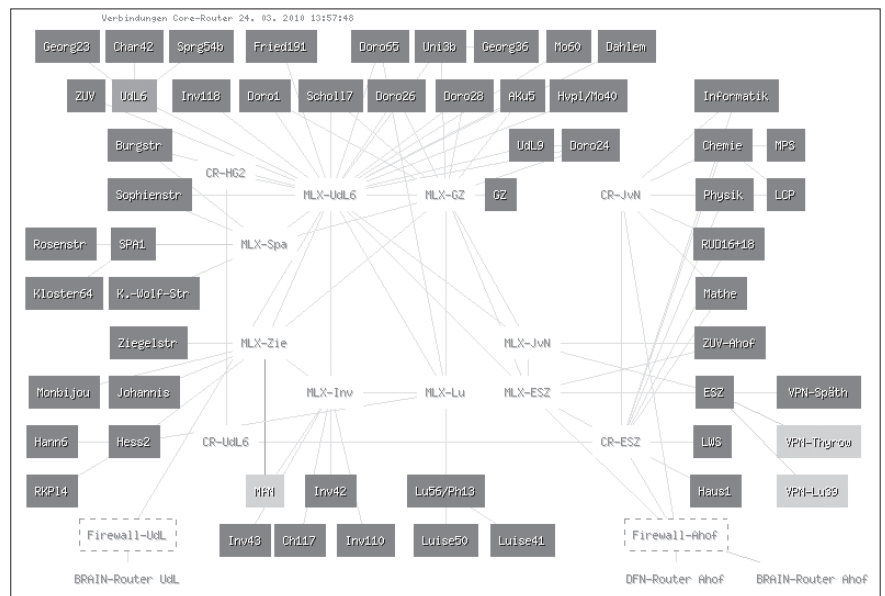


Abb. 3: Netwatch Hauptbild

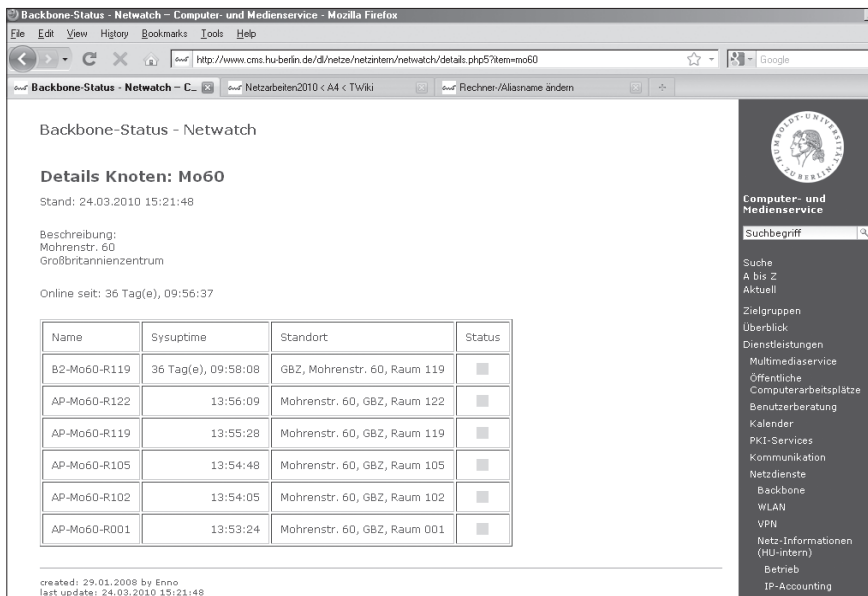


Abb. 4: Ausriß Netwatch Detailansicht

Der Status der Verbindungen zwischen den Standorten und Routern wird durch das Abfragen der entsprechenden Interfaces der beteiligten Netzgeräte ermittelt. Die Verbindung zwischen zwei Knoten kann aus mehreren Leitungen bestehen, die als eine Linie dargestellt werden. Fällt eine Leitung einer solchen Mehrfachverbindung aus, wird die Verbindung in gelber Farbe angezeigt. Bei Komplettausfall oder abgeschalteten Verbindungen erfolgt die Darstellung in Rot. Verbindungen, die nicht geprüft werden, werden in grauer Farbe gemalt.

Die Grafik wird auf einem WWW-Server des CMS in Adlershof erstellt. Dabei werden die Management-Adressen aktiver Komponenten des Netzes abgefragt. Sind diese Adressen nicht erreichbar, werden die Komponenten als nicht in Funktion dargestellt, obwohl sie möglicherweise noch korrekt arbeiten. Ebenso bedeutet die Erreichbarkeit des Management-Interfaces einer Netzkomponente nicht, dass sie störungsfrei funktioniert.

Die Online- und Offline-Zeiten der Standorte und Geräte in der Hauptübersicht werden anhand ihrer Erreichbarkeit ermittelt. Die Laufzeit (SysUptime) einzelner Komponenten wird nur auf den Detailseiten angezeigt. SysUptime und Online-Zeit sind nicht identisch.

Die Benennung der aktiven Netzgeräte auf den Detail-Seiten wird in der Regel wie folgt vorgenommen: *Gerätetyp-*

Standort-Verteiler. Bei älteren Geräten kann auch die Einrichtung anstelle des Standorts aufgeführt sein. Ebenso kann der Gerätetyp fehlen.

Weitere Tools

Ironview

Neben Geräten von Enterasys wird vor allem im Core-Bereich Technik der Firma Brocade (ehemals Foundry) eingesetzt. Dabei handelt es sich um Geräte vom Typ Netiron und Bigiron. Auch Brocade hat ein eigenes Management-Tool: Iron View. Mit diesem lassen sich viele schöne Dinge anstellen: Pflege und Synchronisation von Accesslisten, Analysen im MPLS usw.

Netscreen Security Manager

Der NSM ist ein Tool für das Management der an der HU eingesetzten Firewalls (ISG 1000, ISG 2000, SSG 520) von Juniper. Ohne den NSM wäre es nur schwer möglich, die komplexen Policies und Einstellungen der Firewalls zu verwalten.

SSH

Natürlich arbeiten wir nicht nur mit blinkenden und bunten Oberflächen. Ein Großteil der Routearbeiten mit

der Netzwerktechnik wird im direkten Dialog mit den Geräten erledigt. Dazu wird Secure Shell (SSH) verwendet. Die vielen Management-Tools, so hilfreich, wie sie oft sind, können sich auch mal „irren“. Da ist es schon wichtig, Informationen direkt aus den Komponenten abzufragen oder auch die Konfiguration über SSH zu erledigen. Das geht mitunter sogar schneller.

WLAN-Management

Die Verwaltung und Konfiguration erfolgt auf verschiedenen Ebenen und Stufen. Ein Großteil der Accesspoints, nämlich die von Enterasys, werden mittels OneClick überwacht. Die Konfiguration dieser Geräte (Typ RBT 4102 EU) erfolgt skriptgesteuert. Diese Methode hat sich im Wesentlichen bewährt.

Im Grimm-Zentrum sind ausschließlich Geräte von Siemens (Typ 36xx) verbaut. Diese werden über zwei Controller (C5110) mittels einer WWW-Oberfläche konfiguriert. Für spezielle, zeitabhängige Prozesse erfolgt die Steuerung der Controller aber ebenfalls über Skripte, die mit den Controllern per SSH kommunizieren. Die Überwachung der Siemens-Accesspoints erfolgt über das Controller-Management oder über das allgemein zugängliche WWW-Interface zum WLAN-Status auf dem Server des CMS unter <http://www.cms.hu-berlin.de/dl/netze/wlan/stats/>. Hier sind alle wesentlichen Informationen zusammengefasst, wie beispielsweise die Auslastung, der Status der Radius- und DHCP-Server und die Funktionalität der Accesspoints.