

# SONDERDRUCK FÜR



### IP-fähige KVM-Switches

# Schalten und walten

Alle Server des Unternehmens im Zugriff – von überall aus: Moderne IP-fähige KVM-Switches machen dies möglich. Network Computing testete sechs Umschalter der Enterprise-Klasse.

Fragt man Netzwerkadministratoren nach den Vorteilen, die Tastatur/Bildschirm/Maus-Umschalter – Keyboard/Video/Monitor-Switches oder kurz KVM-Switches – bieten, dann wird in der Regel aufgezählt: Platzersparnis beziehungsweise effizientere Nutzung des begrenzten Platzes im Rack sowie Kosteneinsparungen durch reduzierten Stromverbrauch, geringere Wärmeentwicklung und geringere Ausgaben für Equipment. Natürlich ist es auch bequem, alle Server von einem zentralen Arbeitsplatz aus bedienen zu können. Diese Vorteile boten schon die uralten, Druckerumschaltboxen gleichenden, mechanischen und etwas später die ersten elektronisch arbeitenden KVM-Switches. Diese Geräte der ersten und zweiten Generation hatten allerdings auch ihre Probleme, beispielsweise mit neuen Zeigergeräten, fortschrittlicheren Tastaturen und erweiterten Grafikfähigkeiten.

Aber KVM-Switches haben sich natürlich weiterentwickelt und die gerade aufgezählten Nachteile gehören heute weitgehend der Vergangenheit an. Weitgehend deshalb, weil es diese mechanischen Boxen noch immer zu kaufen gibt – aber in Unternehmensnetzwerken sind sie sicher nur in Sonderfällen zu finden. Nahezu alle der für den Einsatz im Unternehmen gedachten KVM-Switches der großen Hersteller kennen diese Probleme nicht mehr. Diese Geräte unterstützen so gut wie jede Hardware- und Betriebssystemplattform, bieten mehr oder weniger komfortable On-

Screen-Displays für Setup und Bedienung, zuverlässige Keep-alive-Funktionen und einfach aufrüstbare Firmware. Und die meisten KVM-Switches, die wir zur Enterprise-Klasse zählen, bieten sogar noch einen Vorteil, den die meisten Administratoren bei ihrer Aufzählung vergessen: sie erlauben nicht nur den Zugriff auf alle Server des Unternehmens von einem zentralen Arbeitsplatz aus, sondern sie erlauben einen solchen Zugriff



von jedem beliebigen Arbeitsplatz aus, sofern dieser Arbeitsplatz über IP mit dem Unternehmensnetzwerk, in das der KVM-Switch eingebunden ist, kommunizieren kann. IP-fähige KVM-Switches ermöglichen dieses kleine Wunder.

Unsere Kriterien zur Testteilnahme waren simpel. Wir baten die großen Hersteller einfach, uns KVM-Switches zur Verfügung zu stellen, die mindestens 16 angeschlossene Computer steuern können, mindestens zwei Benutzern voneinander unabhängigen Zugriff gestatten, IP-fähig sind und sich in ein 19-Zoll-Rack montieren lassen. Zur Teilnahme am Test luden wir die Firmen Adder/Leu-

nig, Aten, Avocent, Belkin, Rose Electronics, Peppercon und Raritan ein. Belkin musste leider absagen, da ihr neuer 16-Port-KVM-Switch zum Testzeitpunkt noch nicht zur Verfügung stand – das System wurde erst zur CeBIT vorgestellt. Rose sagte eine Testteilnahme zu und sandte uns auch Informationen zum in Aussicht gestellten Testgerät, aber das Gerät traf nicht rechtzeitig ein. Damit waren zwar zwei namhafte Hersteller nicht vertreten, aber die Geräte, die wir schließlich erhielten, reflektieren den aktuellen Stand der KVM-Technik trotzdem sehr gut. Von Adder/Leunig erhielten wir einen »Smart-View World SVW4x16«. Aten stellte uns ihren Altusen KH0116 zur Verfügung. Von Avocent erhielten wir gleich zwei verschiedene KVM-Switches, und zwar den »Auto-View 2000R« und den »DSR1010«. Peppercon schickte ihren »0801IP« und Raritan gleich zwei »Paragon II UMT442«.

Wir interessierten uns im Rahmen unseres Real-World-Labs-Tests besonders dafür, ob die Systeme die Anforderungen eines Enterprise-Einsatzes erfüllen. Dazu müssen sie über gute eingebaute Sicherheitsfunktionen verfügen, die Überbrückung großer Entfernungen unterstützen und eine problemlose Steuerung der angeschlossenen Server über das Netzwerk ermöglichen. Die Testsysteme forderten wir mit unterschiedlichen Eingabegeräten und hohen Auflösungen. Wir erzeugten Keep-alive-Testkonditionen und überprüften die On-Screen-Displays und Webschnittstellen auf Bedienungsfreundlichkeit. Alle getesteten KVM-Switches unterstützen KVM-Switch-Grundfunktionen wie Scanning oder Monitoring, auf die wir nachfolgend nicht mehr besonders eingehen werden.



## Peppercon 0801IP

Der 1HE-KVM-Switch von Peppercon gefällt uns auf Anhieb. Zwar handelt es sich beim Modell 0801IP nur um einen 8fach-KVM-Switch, aber da sich das Gerät tatsächlich nur in der Kanalanzahl und im Preis von seinem großen Bruder 1601IP unterscheidet, entschlossen wir uns dazu, es trotzdem mit in den Test zu nehmen. Der 0801IP erwies sich als problemlos einsetzbares Gerät mit einfachem On-Screen-Display und guter, übersichtlicher

der Administrator dazu mit einem Hotkey (2 x Strg-Taste) das On-Screen-Display/Menü (OSD) des Switches auf. Außer zur Konfiguration dient das OSD auch zum Umschalten – das zu steuernde System wird einfach aus der im OSD angezeigten Liste selektiert. Natürlich kann der Administrator benutzerfreundliche Namen für die angeschlossenen Computer konfigurieren, um sich nicht immer daran erinnern zu müssen, welcher Computer an welchem Kanal/Port hängt. Be-

kann der Administrator auf einzelne KVM-Ports beschränken. Auf Wunsch führt der KVM-Switch eine SSL-Verschlüsselung der Konsolendaten mit bis zu 256 Bit durch. Im Switch ist ein eigenes Zertifikatsmanagement integriert. Der oben erwähnte Telnet-Zugriff kann ausgeschaltet werden. Der Zugriff auf den KVM-Switch und die angeschlossenen Computer lässt sich über IP-Adressen steuern. Andere KVM-Switches unterstützen neben dieser IP-Zugriffssteuerung auch eine Zugriffssteuerung über MAC-Adressen, was noch etwas sicherer ist. Selbstverständlich kann der Administrator ein Sitzungs-Timeout konfigurieren und außerdem die maximale Anzahl fehlerhafter Loginversuche vorgeben.

Natürlich erkennt der KVM-Switch ausgeschaltete Computer – das können alle KVM-Switches. Aber der 0801IP kann auch Computer mit Systemfehlern erkennen: Plattenfehler, entfernte Stromkabel beziehungsweise Netzteilfehler, CPU-Controller oder Platinenfehler, Lüfterfehler und RAM-Fehler. Über den Console-Redirection-Service ist ein Reboot angeschlossener Computer und ein Verfolgen des Bootprozesses möglich. Ein System lässt sich auch von einer separaten Partition booten, beispielsweise in eine Diagnoseumgebung.

Der 0801IP ist ein vollständiger, robuster und zuverlässiger KVM-Switch, den wir bei Bedarf sofort selbst einsetzen würden. Der einzige wirkliche Nachteil des 0801IP beziehungsweise des größeren 1601IP ist die Skalierbarkeit. Wir haben leider keine Möglichkeit gefunden, mehrere KVM-Switches miteinander verbinden und über eine einzige IP-Adresse verwalten zu können.

## Avocent AutoView 2000R

Avocents AutoView-2000R ist ein 1HE-16fach-KVM-Switch. Die zu steuernden Computer werden über so genannte AVRIQ-Module mit dem Switch verbunden. Ein AVRIQ-Modul ist ein kleine Plastikgehäuse, das die auf einer Seite über KVM-Kabel hereinkommenden Signale auf ein auf der anderen Seite an einem RJ45-Port angeschlossenes Kategorie-5-Kabel umsetzt. Diese Verwendung von bis zu zehn Meter langem Standard-Ethernet-Kabel hat uns gut gefallen, weniger gut gefallen hat uns allerdings, dass diese Kabel nicht mitgeliefert werden. AVRIQ-Module gibt es für den Anschluss von PCs (PS/2), Sun-Systemen und USB. Der Anschluss serieller Geräte wird ebenfalls unterstützt. Der AutoView ist kaskadierbar und kann auch in Verbindung mit anderen Avocent-KVM-Switches, beispielsweise DSR1010-Systeme, eingesetzt werden. Die maximal unterstützte Portanzahl haben wir allerdings nicht herausfinden können.

Bis auf die Suche nach den notwendigen Kabeln verlief die Inbetriebnahme problemlos. Kabel anschließen, einschalten, fertig. Nach dem Einschalten fiel uns zunächst der recht laute Lüfter des Switches auf. An der am

## Report-Card / interaktiv unter [www.networkcomputing.de](http://www.networkcomputing.de)

### KVM-Switches

Feature	Gewichtung	Adder Smartview World SVW 4x16	Avocent DSR1010	Aten Altusen KH0116 mit CN-6000	Avocent AutoView 2000R	Peppercon 0801IP
Leichtigkeit der Konfiguration/Anwendung	20%	4,5	4,5	4	4	4,5
Direkte Steuerung über große Distanzen	20%	4,5	4	3	3	3
Sicherheitsfeatures	20%	4	4	3,5	3	4
Erweiterbarkeit	20%	4	4	4	4	0
Plattformunterstützung	10%	4	1	4,5	4,5	1
Netzwerkschnittstelle	10%	4	3,5	3	3,5	4
Gesamtergebnis	100%	4,2	3,75	3,65	3,6	2,8
		<b>B+</b>	<b>B-</b>	<b>B-</b>	<b>B-</b>	<b>C</b>

A>=4,3; B>=3,5; C>=2,5; D>=1,5; E<1,5;  
Die Bewertungen A bis C beinhalten in ihren Bereichen + oder -;

Gesamtergebnisse und gewichtete Ergebnisse basieren auf einer Skala von 0 bis 5.

Webschnittstelle. Inbetriebnahme? Server und KVM-Switch über PS/2-KVM-Kabel – bis zu 10 Meter lange Kabel sind erhältlich – miteinander verbinden, Tastatur, Maus und Monitor am KVM-Switch anschließen, Ethernet-Kabel reinstecken und mit Strom versorgen. Über die angeschlossene einzelne Konsole lassen sich dann sofort die angeschlossenen Computer steuern. Wir testeten erfolgreich den Anschluss nicht zuvor heruntergefahrter Computer – eine Aktion, die andere KVM-Switches mit dem Verlust des Maussignals quittierten.

Der KVM-Switch unterstützt an der lokalen Konsole Auflösungen von bis zu 1920 x 1440 bei 60 Hz und über IP Auflösungen von maximal 1280 x 1024 bei 75 Hz mit Autokalibrierung und automatischer Anpassung des Darstellungsfensters an die Bildschirmauflösung des gesteuerten Computers. Für den Anschluss ans Ethernet-Netzwerk steht auf der Geräterückseite eine 10/100-MBit/s-Ethernet-Schnittstelle mit einwandfrei funktionierendem Autosensing der Geschwindigkeit und des Duplexmodus zur Verfügung. Der Zugriff auf den KVM-Switch ist auch per Telnet und über ein an der seriellen Schnittstelle des Switches angeschlossenes externes Modem möglich. Optional lässt sich eine Power-Management-Unit anschließen.

Die Konfiguration des KVM-Switches erfolgt über den Konsolenanschluss oder die Webschnittstelle. An der lokalen Konsole ruft

nutzer der lokalen Konsole können das OSD auch umgehen und das zu steuernde System direkt per Hotkey auswählen.

Die für den Zugriff über IP notwendige IP-Adresse holt sich der 0801IP via BootP/DHCP oder der Administrator konfiguriert eine feste IP-Adresse. Die mit dem KVM-Switch ausgelieferte CD-ROM mit ausführlicher Dokumentation, Treibern und Utilities war leider defekt, was aber nicht weiter schlimm war, denn auch ohne Dokumentation bekamen wir den Switch einschließlich IP-Konfiguration schnell in den Griff – ein Zeichen dafür, wie einfach der 0801IP im täglichen Einsatz ist. Der Vollständigkeit halber haben wir uns den Inhalt der CD-ROM später trotzdem noch von der Peppercon-Web-Site geladen. Die Webschnittstelle des 0801IP ist übersichtlich und einfach navigierbar. Sobald sie für den Zugriff auf das System benutzt werden kann, ist sie das bevorzugte Werkzeug für die Verwaltung und Konfiguration. Außerdem wird über diese Schnittstelle die Firmware aufgerüstet. Beim Zugriff über IP auf einen der am Switch angeschlossenen Computer kommt es durch das Laden eines Applets zu einer kurzen aber vernachlässigbaren Verzögerung. Mehrere Benutzer können simultan an einem Port arbeiten. Der 0801IP enthält eine ganze Reihe von Sicherheitsfeatures. Bis zu 200 Benutzerprofile sind mit individuellen Rechten einzeln definierbar. Benutzerzugriffe

KVM-Switch angeschlossenen lokalen Konsole wird dann durch zweimaliges Drücken der Strg-Taste oder einmaliges Drücken der Printscreen-Taste das OSD des Switches aufgerufen. Diese Schnittstelle nennt sich in Avocent-Sprache »OSCAR« und ist die On-Screen-Konfigurations- und Ereignisprotokollschnittstelle des Systems. Über OSCAR lässt sich zwar das gesamte KVM-System vollständig konfigurieren, empfehlenswert ist jedoch, lediglich aussagekräftige Namen für die angeschlossenen Computer zu vergeben und die restliche Konfiguration über die mitgelieferte Software Avworks durchzuführen.

Der IP-Teil des KVM-Switches ist erstmalig allerdings über ein an der seriellen Schnittstelle des Geräts angeschlossenes Terminal oder einen PC mit Terminalemulation zu konfigurieren. Dies war ebenfalls beim Avocent DSR1010 und beim Adder-Smartview-World der Fall. Wir fragen uns, warum die Hersteller die Switches nicht gleich so vorkonfigurieren, dass sie sich ihre IP-Adresse via DHCP holen. Administratoren, die dies nicht wünschen, können es anschließend ja wieder ändern – in den meisten Umgebungen existieren aber DHCP-Server. Und außerdem: Wenn doch ohnehin schon eine Tastatur, eine Maus und ein Monitor lokal am KVM-Switch angeschlossen sind, warum muss dann die IP-Konfiguration über ein zusätzlich seriell angeschlossenes Terminal erfolgen? Das Setup beziehungsweise die Konfiguration des Autoview ist insgesamt unhandlicher als beim Peppercon-Switch.

An der lokalen Konsole erfolgt die Umschaltung über Oscar oder Hotkeys, bei über IP mit dem KVM-Switch verbundenen Systemen über Avworks, das dazu allerdings erst installiert werden muss. Die Software unterstützt Windows-NT/2000/-XP und Redhat-Linux. Avworks ist keine Browser-, sondern eine eigenständige Anwendung, die ein großes, übersichtliches Fenster zur Verfügung stellt. Die Menü-/Symbolleiste des Programms enthält viele Optionen, darunter Bildschirmaktualisierung, Autoskalierung, manuelle Skalierung, Makroausführung (Strg+Alt-Entf, Alt-Tab, Printscreen) und Sitzungsoptionen, wie Mausskalierung oder Darstellung des lokalen Cursors. Eine Statusübersicht in Avworks listet alle aktiven Videositzungen auf, allerdings nicht die Sitzung, die an der lokalen angeschlossenen Konsole aktiv ist. Die Anwendung stellt einige nützliche Werkzeuge zur Verfügung, beispielsweise Reboot der Switches, Firmwareaufrüstung, Aufrüstung der »AVRIQ«-Firmware, Speichern und Wiederherstellen der Switch-Konfiguration und Benutzerdatenbank.

Die Sicherheitsfeatures des Autoview sind nicht so umfangreich wie beispielsweise die des Peppercon-0801IP, beispielsweise fehlt eine Zugriffssteuerung über IP-Adressen und ein Zertifikatsmanagement. Geboten wird aber eine Benutzerverwaltung. Der Ad-

ministrator konfiguriert für die Benutzer Benutzernamen, Passwörter, Zugriffslevel (Benutzer, Administrator, Appliance-Administrator) und Zugriffsrechte. Der Zugriff auf den KVM-Switch ist durch ein Passwort schützbar. Standardmäßig erfolgt eine Tastatur-/Mausverschlüsselung mit 128-Bit-SSL. Ein Session-Timeout ist einstellbar. Der Autoview sendet auf Wunsch SNMP-Traps, beispielsweise beim Kaltstart, beim Ausfall einer Verbindung, bei Benutzeran- und -abmeldungen und Reboots. Insgesamt stehen mehr als 30 Traps zur Verfügung.

Der Autoview erlaubt einem lokalen Benutzer und zwei so genannten digitalen Benutzern – das sind die, die über IP zugreifen – simultanen Zugriff auch auf verschiedene angeschlossene Computer. Zum Lieferumfang des Autoview gehört eine kurze aber ausreichende Schnellinstallationsanleitung (auch in Deutsch), die restliche Dokumentation steht auf einer CD-ROM als PDF-Datei zur Verfügung.

### Avocent DSR1010

Der DSR1010 sieht äußerlich aus wie der Autoview-2000R, lediglich das Gehäuse des DSR1010 ist schwarz statt hellgrau. Auch der Anschluss der zu steuernden Endgeräte an den Switch erfolgt wie beim Autoview über Kategorie-5-Kabel mit einer Länge von maximal zehn Metern. Die Module zur Umsetzung der KVM-Signale auf Ethernet-Kabel heißen bei diesem System allerdings nicht

werden – aber die hatten wir ja schon für den Test des Autoview herausgesucht. Die IP-Konfiguration erfolgt auch beim DSP1010 via Terminal an der seriellen Schnittstelle. Das Konfigurationsmenü des DSR1010 ist umfangreicher als beim Autoview, denn beim DSR1010 ist beispielsweise die Verbindung zu einem Authentication-Server zu konfigurieren. Die Authentication-Server-Software ist außerdem zu installieren. Im Konfigurationsmenü lassen sich ferner SNMP-Parameter einstellen, Debug-Nachrichten einschalten, ein Passwort für den Zugriff auf den DSR1010 konfigurieren, Firmware-Aufrüstungen durchführen und Factory-Defaults wiederherstellen. Für Konfigurationsarbeiten steht nicht das relativ komfortable Avworks zur Verfügung, dafür aber DS-Software, die zwar auch bequem aber viel komplexer ist.

Der volle Funktions- und Leistungsumfang des DSR1010 erschließt sich dem Administrator oder Benutzer erst mit »DSView«, einem Teil der DS-Software. Dsview zeigt dem Benutzer eine Liste aller Systeme, für die er Zugriffsberechtigungen besitzt. Das System, das der Benutzer zu steuern wünscht, selektiert er einfach aus der Liste. Er kann gleichzeitig auf mehrere Systeme zugreifen, sofern dies der jeweilige KVM-Switch unterstützt – die DS-Software ist vom KVM-Switch unabhängig. Dsview erlaubt unter anderem die Steuerung des selektierten Computers mit Tastatur und Maus, das Senden von Tastenkombinationen durch einfache Klicks auf entsprechende Schaltflächen, das Speichern von Screenshots in Dateien oder in der Zwischenablage und das Ausführen sowie Erzeugen von Tastaturmakros. Alternativ zu Dsview kann der Benutzer Dswebview verwenden, das den Zugriff über Web-Browser erlaubt, aber über weniger Funktionalität als Dsview verfügt.

Für die Konfiguration steht das komfortable Programm »DSAdmin« zur Verfügung. Darin lassen sich unter anderem Zugriffsberechtigungen für die Benutzer pro KVM-Switch und/oder pro KVM-Port konfigurieren. Benutzernamen und Passwörter werden von Windows-NT/2000 übernommen, so dass es hier keine Redundanzen gibt. Die Benutzerberechtigungen verwaltet der »DSAAuthentication-Service«, wiederum ein Teil der DS-Software. Die DS-Software ermöglicht außerdem das Führen eines Event-Logs. Als zusätzliche Sicherheitsmaßnahme kann der Administrator Sitzungs-Timeouts konfigurieren. Die maximale Auflösung an der lokalen Konsole beträgt 1680 x 1280 bei 75Hz, über IP 1280 x 1024 bei 75Hz.

### Raritan Paragon II UMT442

Paragon-II-UMT442 ist eine etwas ausgefallene Lösung, die nahezu vollständig auf Kategorie-5-Verkabelung setzt. Der KVM-Switch UMT442 besitzt 42 Ports für die zu steuernden Computer und vier »lokale« Ports für den Anschluss der steuernden Benutzerstationen.

#### Info

##### Das Testfeld

- ▶ Adder Smartview World SVW4x16
- ▶ Aten Altusen KH0116 mit CN-6000
- ▶ Avocent AutoView 2000R
- ▶ Avocent DSR1010
- ▶ Peppercon o801IP
- ▶ Raritan Paragon II UMT442

mehr »AVRIQ«, sondern »DSRIQ«, aber Unterschiede zwischen den Modulen konnten wir nicht feststellen. DSRIQ-Module gibt es jedenfalls für PS/2-Anschlüsse, Sun, USB und serielle Geräte.

Der DSR1010 besitzt 16 KVM-Ports und unterstützt einen analogen (Direkt-)Benutzer und eine digitale (IP-)Sitzung. Der Anschluss weiterer Legacy-Switches, beispielsweise Outlook-ES- oder Autoview-Switches, ist möglich. In einem kaskadierten System unterstützt jeder Port des DSR1010 bis zu 24 Systeme, womit wir rein rechnerisch auf maximal 384 steuerbare Computer kommen. Für das Setup, die Navigation und das Management steht das vom Autoview-2000R bereits bekannte Oscar zur Verfügung. Die Inbetriebnahme des KVM-Switches ist ebenfalls wie beim Autoview ein kurzer und schmerzloser Prozess. Auch hier fiel negativ auf, dass keine Kategorie-5-Kabel mitgeliefert

nen. Eine solche Benutzerstation besteht aus einer formschönen aktiven Raritan-Komponente, die im Raritan-Jargon tatsächlich schlicht User-Station genannt wird. Die User-Station findet gut Platz unter einem Monitor. Neben dem Monitor schließt der Administrator noch eine Tastatur und eine Maus an und verbindet die User-Station schließlich über herkömmliches Kategorie-5-Kabel mit dem KVM-Switch. Auf diese Weise lassen sich Entfernungen von rund 300 Meter zwischen User-Station und KVM-Switch überbrücken. Der Fairness wegen sei gesagt, dass sich solche Entfernungen durch Einsatz von Extendern auch mit KVM-Switches anderer Hersteller realisieren lassen, und sicher hat man es bei dieser User-Station-/UMT442-Kombination auch mit Extendern zu tun, die gleich in den Geräten eingebaut sind. Die Sache mit den User-Stationen hat natürlich auch den Nachteil, dass zusätzliche Komponenten mit Strom versorgt werden wollen und dass die User-Stationen als solche zusätzliche potenzielle Fehlerquellen darstellen.

Der Anschluss der zu steuernden Computer an den UMT442 erfolgt über so genannte Computer-Interface-Module (CIMs), die auf der einen Seite KVM-Anschlüsse und auf der anderen Seite einen RJ45-Port für den Anschluss eines Ethernet-Kabels besitzen. Diese CIMs sind mit den AVRIQ- oder DSRIQ-Modulen von Avocent vergleichbar. Aber anders als Avocent liefert Raritan die notwendigen Kategorie-5-Kabel gleich mit. CIMs gibt es für PS/2, Sun, USB und serielle Geräte. An die Main-Switching-Unit, also an den UMT442, lassen sich mit Hilfe spezieller Kabel weitere Stacking-Units anschließen. Diese Möglichkeit erlaubt bis zu 128 KVM-Ports pro Switch und über multidimensionale Ausdehnung Tausende Ports. Die Inbetriebnahme des Paragon-II-Systems ist einfach: Alle Kabel anschließen und dann Computer, Switch und User-Stationen einschalten. Auf dem Bildschirm der User-Station erscheint dann ein On-Screen-Menü, in dem einfach über die Pfeiltasten das zu steuernde Gerät selektiert wird. Das On-Screen-Menü ist jederzeit mit einem Hotkey aufrufbar, und der Zugriff darauf lässt sich selbstverständlich durch Benutzernamen-/Passwortkonfiguration schützen.

Die KVM-Switches von Avocent, Aten und Peppercon besitzen auf ihren Vorderseiten eine ganze Reihe von Status-LEDs – nicht so der UMT442. Der UMT442 hat auf der Gerätevorderseite ein zweizeiliges LCD-Display, das unter anderem Statusinformationen anzeigt. Außerdem sind dort einige Funktionstasten für Systemmanagement- und Support-Funktionen untergebracht. Dazu gehören ein Reset auf Factory-Defaults, die Anzeige von Versions- und Seriennummern, verschiedene Testfunktionen, die IP-Adresskonfiguration und der Reset des Ge-

räts. Die Bedienung ist kinderleicht. Über das OSD einer User-Station führt der Benutzer eine Grundkonfiguration durch, in deren Verlauf er einen Gerätenamen, Sitzungs-Timeouts, Operationsmodi (Private, Public-View, PC-Share), Namen für die KVM-Ports beziehungsweise die daran angeschlossenen Computer und IP-Parameter konfiguriert sowie die Verschlüsselung ein- oder ausschaltet. Raritan demonstriert hier, dass sich IP-Parameter auch anders als über ein seriell angeschlossenes Terminal konfigurieren lassen. Das OSD dient auch zur Auswahl des zu steuernden Computers aus einer Computerliste. Unterschiedliche Farben informieren den Benutzer darüber, ob ein Computer angeschlossen und eingeschaltet ist, ein Kanal-

selbst wenn sie für einige dieser Computer keine Zugriffsberechtigung besitzen. Betriebsmodi steuern den Zugriff auf Computer. Im Private-Modus kann immer nur ein Benutzer auf einen spezifischen Computer oder Kanal zugreifen. Der Public-View-Modus erlaubt die Steuerung eines Computers durch einen Benutzer, während alle anderen Benutzer den Bildschirm dieses Computers sehen können. Im PC-Share-Modus ist die Steuerung eines Computers gleichzeitig durch mehrere Benutzer möglich – ein Feature, das sehr zur Erheiterung beitragen kann, wenn vier, fünf Benutzer gleichzeitig die Maus über den Bildschirm jagen.

Bei der Benutzerkonfiguration vergibt der Administrator Benutzernamen, schaltet

## Features

### KVM-Switches

Hersteller Produkt	Adder SmartView World SVW 4x16	Aten Altusen KH 0116 mit CN-6000	Avocent AutoView 2000R	Avocent DSR1010	Peppercon 0801IP	Raritan Paragon II UMT442
Basis-Server-Ports/ max. Server-Ports	16/k.A.	16/512	16/k.A.	16/384	8/8	42/mehrere tausend
Lokale Benutzer	4	1	1	1	1	4
Max. lokale Distanz zwischen Switch und Server (Länge des KVM- bzw. Ethernet-Kabels)	15 Meter	3 Meter	10 Meter	10 Meter	10 Meter	10 Meter
Max. Distanz (mit Extender) zwischen Switch und Konsole	200 Meter	150 Meter	k.A.	k.A.	k.A.	300 Meter
Max. Auflösung für Bildschirm mit KVM	1900 x 1440	1920 x 11440	1680 x 1280	1680 x 1280	1920 x 1440	k.A.
Direkte KVM-Steuerung	●	●	●	●	●	●
TCP/IP-Netzwerkschnittstelle	eingebaut	CN-6000	eingebaut	eingebaut	eingebaut	IP-Reach o. IP-User-Station
Chassis-Controls/Indikatoren	●/●	○/●	○/●	○/●	○/●	●/●
Unterstützte Betriebssysteme	alle	alle	alle	alle	alle	alle
Unterstützung sämtlicher Zeigergeräte	●	●	●	●	●	●
Firmware-Upgrade d. Benutzer	●	●	●	●	●	●
Unterstützung Hot-Adds/-Änderungen	●	●	●	●	●	●
Web	www.adder.com	www.altusen.com	www.avocent.de	www.avocent.de	www.peppercon.de	www.raritan.com

ja = ●; nein = ○; keine Angabe = k.A.

port aktiv und verfügbar ist, ein Kanal gerade von einem anderen Benutzer verwendet wird, ein Kanal zwar nicht für die Steuerung, wohl aber für eine Betrachtung zur Verfügung steht, und ein paar Dinge mehr. Über Benutzerprofile können Benutzer individuell ihre bevorzugten Betriebsparameter einstellen, beispielsweise den Scan-Modus, die Anzeige des ID-Displays, Hotkeys, die Anzeigeposition des OSD und die Taste, mit der sie schnell zum vorangegangenen Kanal zurückspringen können. Der Zugriff auf viele Funktionen des OSDs erfolgt über Funktionstasten. Aber es ist nicht einfach, sich zu merken, welche Funktionstaste wofür gedacht ist.

Im System-Konfigurationsmenü gibt es einige interessante Einstellmöglichkeiten. Dort lässt sich beispielsweise einstellen, ob die Benutzer grundsätzlich immer alle angeschlossenen Computer sehen können,

Administratorprivilegien für einen Benutzer ein oder aus und weist einem Benutzer durch die Eingabe von ID-Nummern Sicherheitsgruppen zu. Damit sind wir bei den Gruppeneinstellungen beziehungsweise Zugriffsrechten angelangt. Hinter den Gruppeneinstellungen verbirgt sich ein kompliziertes aber sehr flexibles System, mit dem Administratoren festlegen, welche Benutzer auf welche Computer zugreifen dürfen. Wir meinen, dass Raritan diese Geschichte etwas übersichtlicher hätte gestalten können/sollen. Um Benutzern Rechte und CPUs Sicherheitsstufen zuzuordnen, weist der Administrator den Benutzern Benutzergruppen mit definierten Rechten und den CPUs Kanalport-Gruppen zu. Jede Gruppe kann mehrfache Benutzer oder CPUs enthalten. Gruppen werden für Benutzer und CPUs jeweils von 00 bis 99 durchnummeriert. Benutzer und Computer

kommunizieren schließlich gemäß festgelegter Gruppen-ID-Regeln miteinander – und die sehen so aus: Benutzer mit der (Default-) Gruppen-ID dürfen beispielsweise auf alle Computer mit den Gruppen-IDs 00 bis 99 zugreifen. Benutzer mit der Gruppen-ID 05 dürfen auf Computer mit den Gruppen-IDs 00, 05 und allen zweistelligen IDs mit 5 als erster Ziffer zugreifen. Jedenfalls erlaubt dieses System beispielsweise, dass Administratoren Computern, die hohe Sicherheit erfordern, CPU-Gruppen-IDs im Bereich von 10 bis 99 zuzuweisen, womit die Computer dann weniger zugreifbar sind als Computer mit den IDs 00 oder 01 bis 99.

Und gerade als wir anfangen wollten, dem Paragon-II-System so richtig auf den Zahn zu fühlen, mussten wir leider aufhören: Das in der Produktdokumentation erwähnte Paragon-Manager-Administrative-Software-Package wurde nicht mitgeliefert. Raritan hatte uns zwar gleich zwei KVM-Switches zur Verfügung gestellt, aber auch im zweiten Paket war die Software nicht zu finden. Auf Raritans Web-Sites stand auch nichts für einen Download zur Verfügung. Problematischer noch: Der UMT442 gestattet zwar grundsätzlich einen Zugriff via IP (Browser), aber dazu benötigt man das ebenfalls nicht gelieferte IP-Reach (ehemals Telereach) oder eine IP-fähige User-Station – wir hatten nur einfache User-Stations. Vermutlich hätten wir die fehlenden Komponenten nach einem Anruf bei Raritan sofort zugestellt bekommen, aber das Raritan-Produkt war das zuletzt von uns getestete und bis zum Redaktionsschluss hätte es niemals geklappt. Und da sich Hardware noch nicht per E-Mail versenden lässt, war an dieser Stelle leider Schluss. Wie sich das Raritan-System in unserem Szenario verhält tragen wir in einem folgenden Artikel nach.

## Aten Altusen KH0116 mit CN-6000 »KVM on the Net«

Sofort waren wir von der schicken Produktverpackung begeistert, aber das interessiert für unseren Test weniger. Der KH0116 ist ein schlichtes, schwarzes Gerät zur Steuerung von 16 PCs. Kaskadierbar über Daisy-Chain-Kabel skaliert das System auf bis zu 512 Ports. Der Anschluss der zu steuernden Computer erfolgt über proprietäre KVM-Kabel von maximal drei Metern Länge. Die Konsole wird entweder direkt am Switch oder an einem Console-Extension-Modul angeschlossen. Dieses Modul ist in etwa vergleichbar mit der Raritan-User-Station, ist aber deutlich kleiner und auch weniger funktionell. Die Verbindung erfolgt auch hier über Kategorie-5-Kabel, aber die maximal überbrückbare Entfernung beträgt lediglich 150 Meter. Eine lokale Konsole kann trotz Verwendung des Extension-Moduls noch angeschlossen bleiben. Beide Konsolen können dann benutzt werden, jedoch nicht si-

multan. Über eine Taste am KVM-Switch lässt sich die Benutzung der Remote-Konsole sperren. Neben diesem Knopf sind auf der Gerätevorderseite noch ein paar Status-LEDs, eine Reset-Taste, der Remote-Konsolen-Port, ein Firmware-Upgrade-Port und eine LCD-Anzeige für die aktiven Stationen untergebracht.

Der KH0116 bietet alle KVM-Switch-Basisfunktionen, darunter Scanning, Skipping – vom aktuellen zum nächsten, zugreifbaren Port –, Hotkey-Umschaltung beziehungsweise -Funktionsauswahl und OSD mit Passwortschutz. Die Auswahl des zu steuernden Systems erfolgt im OSD wie üblich aus einer Liste. Die Namen der in dieser Liste angezeigten Ports sind editierbar. Um eine bessere Übersicht zu erhalten, kann der Benutzer eine Vorauswahl der angezeigten Ports/Computer treffen: alle Ports, nur Ports mit eingeschalteten Computern, nur Quick-View-Ports oder nur Quick-View-Ports mit eingeschalteten Computern. Quick-View umschreibt das Scannen und Betrachten besonders ausgewählter Computer. Die Ports beziehungsweise Computer sind dazu lediglich mit einer Quick-View-Flag zu versehen.

Benutzernamen und Passwörter konfiguriert der Administrator individuell für einen Administrator und bis zu vier Benutzern. Die Benutzerzugriffssteuerung ist schlicht und unterscheidet lediglich zwischen Vollzugriff, nur betrachtenden Zugriff und keinen Zugriff. Firmware-Upgrades erfolgen über ein Windows-Firmware-Upgrade-Utility via mitgeliefertem Firmware-Upgrade-Kabel. Das waren die Basisfunktionen des KVM-Switches. Sicherheitsfeatures sind nur rudimentär vorhanden.

Interessanter wird die Lösung mit der optionalen CN-6000-Box, die IP-Funktionalität liefert. Diese etwa Taschenbuch-große Box wird per Ethernet-Kabel ans Netzwerk angeschlossen. Dann schließt der Benutzer eine Tastatur, eine Maus und einen Monitor an und verbindet die Box schließlich mit Hilfe eines normalen KVM-Kabels mit dem Switch. Am Switch werden dabei die Ports verwendet, die normalerweise die lokale Konsole nutzt – die CN-6000-Box wird damit also gleichzeitig zur lokalen Konsole. Mit der Box wird folgende Software geliefert: ein Administrations-Utility, ein Windows-Client, ein Java-Client und ein Log-Server.

Die Administration und Konfiguration erfolgt – logisch – mit dem Administrations-Utility. Nachdem sich die Box ihre IP-Adresse via BootP/DHCP geholt hat findet das Utility sie und alle anderen Boxen im Subnetz automatisch. Nach der Anmeldung mit Benutzernamen und Passwort kann der Administrator mit der Konfiguration beginnen und zunächst dem Gerät einen einprägsamen Namen geben und anschließend weitere Netzwerkeinstellungen durchführen



oder überprüfen. Über IP-Adresse und/oder MAC-Filter lässt sich einstellen, welche Stationen zugreifen dürfen und welche nicht. Ferner können Administratorzugriffe an eine bestimmte MAC-Adresse gebunden werden. Im Benutzermanagement-Abschnitt lassen sich für

Benutzer Namen, Passwörter und Berechtigungen konfigurieren. Die Berechtigungen beschränken sich allerdings auf eine Konfigurationsberechtigung und eine Berechtigung zum Ausführen des Java-Clients. Weitere Sicherheitseinstellungen sind ein Sitzungs-Timeout, die erlaubte Anzahl von Login-Fehlversuchen, Stealth-Modus/Echo-Modus und ein »Reset on Exit«.

Der Verbindungsaufbau zu einem zu steuernden Computer ist mit dem Windows-Client sehr einfach. Allerdings bietet dieser Client nicht viele Einstellmöglichkeiten oder Optionen. Die Video-Optionen beschränken sich auf Screen-Position, Autosync und RGB-Einstellungen. Der Benutzer kann einige Hotkeys nutzen und einstellen. Im großen und ganzen gibt es am Windows-Client nichts auszusetzen. Der Java-Client verspricht Plattformunabhängigkeit und bietet in etwa die gleiche Funktionalität wie der Windows-Client. Ein Zugriff auf das System zur Konfiguration und Steuerung ist auch via Browser möglich. Die Steuerung eines ausgewählten Computers findet dann aber nicht mehr im Browser statt, sondern aus dem Browser heraus wird entweder der Windows- oder der Java-Client gestartet. Der optional installierbare Log-Server protokolliert alle Ereignisse, die auf ausgewählten CN-6000-Boxen vorkommen, in einer Datenbank.

## Adder/Leunig SmartView World SVC4x16

Der Smartview-World war das einzige System im Testfeld, das im Rack zwei Höheneinheiten beansprucht. Dafür sind in dem großen Gehäuse aber auch eine Menge Funktionen verpackt. Der KVM-Switch bietet 16 Ports für die zu steuernden Computer und 4 Ports für Konsolen. Zwei dieser Konsolenports eignen sich für den Anschluss von Konsolen, die bis zu 200 Meter vom Switch entfernt sein können – dafür benötigt man dann allerdings zusätzlich Adder-Receiver-Units. Solche Receiver-Units standen uns nicht zur Verfügung, wir können uns allerdings vorstellen, dass es sich dabei um Geräte handelt, die mit Raritans User-Station oder Atens Console-Extension-Modul vergleichbar sind. Der Anschluss der zu steuernden Computer erfolgt bei PS/2 über normale KVM-Kabel. Bei Sun und USB sind proprietäre Kabel erforderlich.

Der Smartview erlaubt es dem Administrator, über einen auf der Frontseite untergebrachten Computer-Schalter direkt am

Switch umzuschalten. Die Nummer des eingestellten Ports wird dabei in einem Display angezeigt. Ein zweites Display zeigt die Nummer des Konsolenanschlusses, der den eingestellten Port aktuell nutzt. Mit einem zweiten Schalter kann der Administrator auch durch die vier Konsolenanschlüsse schalten – im Computer-Display sieht er dann die Nummer des jeweils genutzten Kanals/Ports. Vier rote LEDs zeigen Aktivitäten der vier Konsolenanschlüsse an. Wird also beispielsweise an Konsole Nummer 3 die Maus bewegt, dann flackert LED Nummer 3. Es stellt sich die Frage, wozu das wohl gut ist. Gleich zwei grüne LEDs zeigen an, ob der Switch mit Strom versorgt wird, dabei steckt aber nur ein Netzteil im Gerät. Aber gut, vielleicht denkt sich ja der Hersteller was bei redundanten Power-LEDs. Auf der Vorderseite befindet sich dann noch ein IP-Port-Abschnitt mit einer seriellen Schnittstelle für die IP-Grundkonfiguration (dieser lässt sich später für ein externes Modem nutzen), einem RJ45-Port für die Netzwerkverbindung, drei Status-LEDs und einem Reset-Knopf für den IP-Bereich. Rückseitig verfügt der Switch neben den 16 Computerports und 4 Konsolenports noch über eine serielle Schnittstelle, eine Schnittstelle für den Anschluss einer Power-Control-Option, einen Reset-Knopf und den Stromanschluss.

Smartview-KVM-Switches lassen sich kaskadieren. Dazu verbindet der Administrator einfach mindestens einen Computerport eines Switches mit einem Konsolenport eines anderen Switches. Eine solche Kaskadierung darf bis zu vier Ebenen tief reichen. Verbindet der Administrator mindestens zwei Smartview-Units miteinander, dann können diese beiden Systeme synchronisiert arbeiten, was die interessante Anwendung der Mehrfach-Monitor-Verbindung ermöglicht. Um dies zu nutzen, ist die serielle Schnittstelle des ersten, so genannten Master-Switches über ein Synchronisationskabel mit der seriellen Schnittstelle des Slave-Switches zu verbinden. Schaltet der Benutzer nun den Master-Switch um, sendet dieser Switch ein entsprechendes Signal über die serielle Schnittstelle an den Slave-Switch, der daraufhin auf den gleichen Kanal umschaltet. Ein an diesem Kanal des Slave-Switches angeschlossener Monitor zeigt dann das selbe Bild, wie der Monitor am Kanal des Master-Switches.

Die Konfiguration und Umschaltung über eine lokale Konsole erfolgt auch bei die-

sem KVM-Switch über ein OSD. Der Administrator kann im OSD die Sicherheit einschalten, was dazu führt, dass ein Administrator-Passwort verlangt wird. Im Rahmen der Benutzerkonfiguration vergibt der Administrator Benutzernamen, Passworte und Zugriffsrechte. Konfigurierbar sind ein Sitzungs-Timeout und eine automatische Abmeldung. Das Autoscanning-Feature lässt sich auf aktive PCs oder auf die PCs beschränken, die in einer Scan-Liste verzeichnet sind. Wem der Aufruf des OSDs zur Auswahl des zu steuernden Computers aus der Computerliste zu lange dauert, der kann auch direkt per Hotkey die Computer. Der IP-Teil des Smartview pflegt vom Rest des KVM-Switches unabhängige Si-

## Info

### So testete Network Computing

Die KVM-Switches steuerten in unseren Real-World Labs mehrere Server und Arbeitsstationen mit verschiedenen Betriebssystemen, Grafikauflösungen und Eingabegeräten. Unsere Testsysteme liefen unter Windows-2000, Windows-XP, Windows-Millennium, Windows-Server-2003 und Linux in einer 100-MBit/s-Ethernet-Umgebung. Wir testeten, wie leicht sich die Switches in Betrieb nehmen ließen und welche Schritte die erweiterte Konfiguration, dabei besonders die IP-Konfiguration verlangte. Die Switch-Konfiguration führten wir auf verschiedenen Wegen durch, da es natürlich Unterschiede in der Firmware gab. Neben der Benutzerkonfiguration und den Sicherheitseinstellungen modifizierten wir das Setup der Kanäle, wozu auch Tests verschiedener Auflösungen gehörten. Neben der Kompatibilität von Mäusen und Tastaturen testeten wir Keep-alive-Funktionen anhand simulierter Stromausfälle und unterbrochener Verbindungen.

cherheitseinstellungen. Die Grund-IP-Konfiguration erfolgt einmal mehr via seriell angeschlossenen Terminal. Der Administrator stellt dabei ein, wie der Switch seine IP-Adresse erhält (fix oder per Bootp/DHCP), ob eine IP-Zugriffskontrolle durchgeführt werden soll und mit welcher Geschwindigkeit und welchem Duplexmodus das Netzwerk arbeitet. Im Test haben DHCP und Autosensing einwandfrei funktioniert. Den Rest der Konfiguration erledigt der Administrator dann am einfachsten über den Browser. Die Web-

schnittstelle des Smartview ist weitestgehend identisch mit der Webschnittstelle des Peppercon-KVM-Switches, so dass wir darauf nicht weiter eingehen. Wir wissen nicht, wer die Webschnittstelle von wem lizenziert hat, jedenfalls stammen beide Schnittstellen aus einer Hand.

## Fazit

Was die technische Ausstattung betrifft, ist der Smartview-World von Adder das flexibelste und vollständigste System, das noch dazu hoch skaliert. Eine maximale Distanz von 200 Meter mit Adder-Receiver-Unit zwischen Switch und Konsole dürfte für die meisten Einsatzgebiete reichen. Wer größere Distanzen überbrücken muss, kann dies mit IP tun. Der Smartview leistete sich im Test keine Schnitzer. Zwar setzt das System nicht so konsequent auf Ethernet-Verkabelung, wie beispielsweise der Paragon-II oder die beiden Avocent-KVM-Switches, aber dies lässt sich verschmerzen. In der Summe ergibt der Test Referenz für den Smartview-World. Reichen acht beziehungsweise 16 steuerbare Computer aus und ist nicht vorgesehen, zukünftig weitere Computer zu unterstützen, dann tätigt man auch mit einem Peppercon-0801IP oder -1601IP einen guten Kauf. Das Peppercon-Angebot ist also eher für kleinere Umgebungen geeignet, in denen auch nicht mehrere Administratoren gleichzeitig auf unterschiedliche Computer zugreifen können müssen. Die beiden Avocent-KVM-Switches sind bedenkenlos dort einsetzbar, wo es auf Skalierbarkeit ankommt. Geht es um die zentrale Verwaltung mehrerer KVM-Switches, dann eignet sich dank DS-Software besonders der DSR1010. Der DSR1010 bietet auch etwas mehr Sicherheit, als der Autoview-2000R. Der Aten-Altusen-KH0116 bietet als Grundsystem nur wenige Features, eignet sich aber sicher für Shops, die jetzt einen KVM-Switch mit einem lokal angeschlossenen Konsolenplatz benötigen, später aber vielleicht die IP-Fähigkeit ergänzen/nutzen wollen. Das System ist gut skalierbar, aber leider auf PCs (PS/2-Anschlüsse) beschränkt. Den Raritan-Paragon-II-UMT442 haben wir nicht bewertet, weil wir die IP-Fähigkeit nicht testen konnten. Das System besitzt eine Menge guter Features und Eigenschaften, und auch die IP-Talente des Switches sind sicher nicht die schlechtesten – nicht umsonst war ein älteres Paragon-System bis zu diesem Test die Referenz der Network Computing. [ dj ]



LEUNIG GmbH  
Wilhelm-Ostwald-Str. 17  
D 53721 Siegburg, Germany  
Fon: +49 (0) 2241-1766-0  
Fax: +49 (0) 2241-1766-99  
www.leunig.de