TECHNIK NEWS - NETZWERKMAGAZIN

G46392

Technik NEWS

NOVEMBER 2001

DAS PRAXISNAHE NETZWERKMAGAZIN

N° 11

11. JAHRGANG

thema des monats

KABEL LOS !

Wireless LAN

Drahtlose Technik im Detail

PRAXIS

Business Communications Manager
Teil 1: Basis Konfiguration

AKTUELL

NEWS

THEMA DES MONATS

Wireless LAN

Drahtlose Technik im Detail

Wireless LANs schaffen mehr Freiheit, Flexibilität und Mobilität. Es liegt was in der Luft, denn kabellose Netze offenbaren neue Dimensionen in der Vernetzung von Gebäuden, Abteilungen und Mitarbeitern. Ihr Hauptvorteil ist ihre einfache Installation, weil sie sich schnell und ohne Verkabelungsaufwand konfektionieren lassen.

HOTLINE

PRAXIS

SOLUTIONS

VORSCHAU

impressum

Herausgeber: COMPU-SHACK Electronic GmbH, Ringstraße 56-58, 56564 Neuwied

Telefon: 02631/983-0
Telefax: 02631/983-199
Electronic Mail: TECHNEWS @ COMPU-SHACK.COM

Redaktion: Heinz Bück
Hotline und Patches: Jörg Marx

Verantwortlich für den Inhalt: Heinz Bück

Technische Leitung: Ulf Wolfsgruber

Erscheinungsweise: monatlich 1 Heft

Bezugsquelle: Bezug über COMPU-SHACK Electronic GmbH Abonnementpreis: 119,- DM + MwSt.

Layout und Titelbild: Marie-Luise Ringma

Druck: Görres-Druckerei, Koblenz

Lektorat: Andrea Briel
Anja Dorscheid

Abo-Versand: Wolanski GmbH, Bonn

Wir möchten uns nachträglich bei all denen bedanken, die durch die freundliche Zusammenarbeit das Erscheinen dieser Zeitung ermöglicht haben.

Als Informationsquelle dient uns auch das Internet. Wenn Sie speziell über Ihre Erfahrungen referieren möchten, bieten wir Ihnen dies unter der Rubrik "Hotline" an.

Technik NEWS ONLINE

www.technik-news.de

Selbstverständlich kann COMPU-SHACK die einwandfreie Funktion der vorgestellten Patches und Tips nicht garantieren und übernimmt keinerlei Haftung für eventuell entstehende Schäden.

Patch-CD

NWFTPD3A.exe
NDPCPSP3.exe
275820.exe
270050.exe
BM35SP3.exe
NDSUNIX4.tgz
1839NT.exe
MCSCANNT.zip
DVPGP.dll
BW612.exe
BL6102.x4a
BNT8XVIRUPD_240051.EXE
BNT85OFOFIX_239866.EXE
BNT86OFOFIX_239867.EXE
BNT86SQLFIX_239493.EXE
BNT86SYSFIX_239551.EXE
BE85P00_240250.EXE
B850DV13_239791.EXE
WIN9X_AGENT_239813.EXE

COMPU-SHACK SOLUTION

Solution Service Concept

Partnerprogramm für den IT-Fachhandel

Von Tanja Rübsamen

Die Compu-Shack Solution bietet ihren Fachhandelspartnern jetzt ein einzigartiges Konzept, daß es ihnen ermöglicht, ihr Dienstleistungsspektrum zu erweitern und mehr Umsatz im Service-Bereich zu generieren. In Zeiten fallender Margen bei Hard- und Software wird das Thema Dienstleistungen immer wichtiger. Compu-Shack Kunden können heute exklusiv die Vorteile dieses neuen Partnerprogramms nutzen.

Das Solution Service Concept der Compu-Shack Solution adressiert vor allem Unternehmen im IT-Fachhandel, die neue Geschäftsfelder für sich erschließen wollen, den Wert einer funktionierenden Partnerschaft anerkennen und mit der Sicherstellung von Qualität in der Beratung und Betreuung ihrer Kunden überzeugen möchten. Als Solution Service Partner bieten sie ihren Endkunden nicht nur ein breiteres Dienstleistungsspektrum an, sondern erhalten für ihr Engagement eine attraktive Marge auf jede verkaufte Dienstleistung. Die Solution Service Concept Partner werden im Marketing und bei der Neukunden-Akquise tatkräftig unterstützt. Weiterhin erhalten die teilnehmenden Unternehmen eine exklusive, engagierte Betreuung. Der Fokus des neuen Konzepts liegt auf einer partnerschaftlichen Zusammenarbeit.

Education

Die Compu-Shack Education begleitet Netzwerker auf ihrem Weg zum IT-Experten. Erstklassig ausgebildete Trainer vermitteln in speziellen Trainings im Bereich Networking und Internet aktuellstes Fachwissen, damit Netzwerker, Techniker und Vertriebsmitarbeiter die kniffligen Anforderungen des DV-Alltags meistern können. Als Schulungspartner verschiedener Hersteller bietet die Compu-Shack Education in ihren Seminarzentren in Neuwied, München und Potsdam das Netzwerk-Know How der Technologieführer. Auf alle Trainings erhalten Solution Service Partner attraktive Preisvorteile.

Projekt-Team

Unterstützung rund um die Planung und Realisierung von Netzwerken erhalten die Compu-Shack Fachhandelspartner von den IT-Spezialisten aus Support und Projektberatung. Ob es dabei um Security, Back Office Systeme oder Sprach-Daten-Integration geht, zu jedem Thema verfügt die Compu-Shack Solution über Experten, die speziell ausgebildet wurden und immer auf dem aktuellen Stand der Technik sind. Den IT-Fachhandelpartnern steht dieses Know-how zur Verfügung. Sie können von Compu-Shack Solution die gesamte Projektplanung und -umsetzung erhalten, inklusive Ist-Analyse, Netzwerkdesign, Ressourcenplanung, Bauüberwachung und Dokumentation.
Darüber hinaus erhalten sie Unterstützung bei der Sicherung des reibungslosen Netzwerkbetriebs, oder wenn es darum geht, Netzwerke upzugraden und zu erweitern.

Support-Team

Nach der Planung eines optimalen Systemumfeldes implementiert das Support-Team der Compu-Shack Solution die ausgewählten Komponenten in die vorhandene Netzwerkinfrastruktur, konfiguriert diese nach den gegebenen Anforderungen und begleitet die Kunden durch die Testphase. Diese kompetente Vor-Ort-Unterstützung versetzt den Fachhandel in die Lage, sein Dienstleistungsangebot zu erweitern, und bietet bei Engpässen eine flexible Alternative. Selbstverständlich besteht die Möglichkeit, auch bei einer bestehenden Netzwerklösung auf die Services der Compu-Shack Solution zurückzugreifen, ob in individuellen Workshops, bei Fehleranalysen oder für Remote-Konfigurationen. Solution Service Parnter profitieren von einer breiten Dienstleistungspalette zu attraktiven Konditionen, die von den weitreichenden Synergien aus Distribution und Service bereichert wird.

Ihr Kontakt

Fachhändler, die erweiterte Netzwerkdienstleistungen in Ihr Portfolio aufnehmen möchten, erhalten weitere Informationen zum Solution Service Concept von Tanja Rübsamen unter 02631-983-334 oder per E-Mail an `solution-concept@compu-shack.com`.
In der Heftmitte finden Sie dazu auch auf der TN-Bestellkarte die kostenlose Solution-Broschüre.

Offenes Authentifizierungsnetzwerk

Passport Technologie für universelles Single-Sign-In im Internet erweitert

Microsoft hat eine Reihe von Erweiterungen beim Authentifizierungsservice Passport angekündigt. Die Änderungen bieten Unternehmen, Netzwerkbetreibern, Dienstanbietern und anderen Organisationen die Möglichkeit, Passport im Internet als universelle Single-Sign-On-Lösung zur Bestätigung von Benutzerdaten einzusetzen. Der weit verbreitete Service wird mit der Markteinführung von Windows .NET Server im nächsten Jahr unter anderem Kerberos 5.0 unterstützen.

Die Passport-Unterstützung von Kerberos 5.0, jenem offenen, von der Internet Engineering Taskforce akzeptierten Standard, der auch über Organisations-, System- oder Technologiegrenzen hinweg die sichere und zuverlässige Datenbestätigung gestattet, schafft die Voraussetzung für ein Authentifizierungsnetzwerk zwischen verschiedensten Partnern, das Microsoft gemeinsam mit Unternehmen und Organisationen aus der ganzen Welt realisieren und ausbauen wird. Bei Passport handelt es sich um einen in Websites eingebunden Dienst, der die eindeutige Identifizierung von Internetbenutzern ermöglicht. Er stellt sicher, daß ausschließlich authentifizierte Anwender Kontrolle über den Inhalt und die Weitergabe ihrer persönlichen Informationen im Web erhalten.

Internet Sicherheit

Derzeit wird Passport von weltweit über 165 Millionen Endkunden genutzt. Mit der Unterstützung von Kerberos 5.0 wird der Service aber auch Unternehmen und anderen Organisationen zur Verfügung stehen. Kooperierende Firmen zum Beispiel können Passport dann als einheitlichen Dienst einsetzen, um Online-Transaktionen trotz unterschiedlicher IT-Landschaften oder Bestätigungsprozesse mit optimaler Sicherheit über das Internet abzuwickeln. Ein besonderer Vorteil besteht dabei darin, daß sich Benutzer lediglich einmal zu Beginn einer Arbeitssitzung anmelden müssen. Anschließend werden sie bei allen entsprechenden Vorgängen automatisch über Passport identifiziert. Auch beim Zugriff auf unterschiedliche Websites oder Webservices dient die Single-Sign-On-Lösung Passport als zentraler Authentifizierungsdienst und erhöht dadurch den Komfort für den Internetbenutzer.

Authentifizierung

Die Neuerungen bei Passport bieten Organisationen auf der ganzen Welt die Möglichkeit, gemeinsam mit Microsoft ein Authentifizierungsnetzwerk zu entwickeln. Ähnlich dem Netzwerk für Geldautomaten im Bankensektor wird das System auf einer Reihe allgemeiner technischer und operativer Richtlinien basieren und allen Unternehmen oder Dienstanbietern offen stehen, die diese Standards unterstützen. Neben einer sichereren und effizienteren Kontrolle von Benutzeridentitäten, Profilen und anderen Geschäftsdaten wird das Netzwerk auch zu einer deutlichen Verbesserung der Anwendererfahrung führen. Durch die Vereinheitlichung der unterschiedlichen Authentifizierungsprozesse über Passport können sowohl Unternehmensmitarbeiter als auch Endkunden bequemer und schneller auf gewünschte Internetinhalte zugreifen.

Glasfaserzugang

Einfacher Breitbandanschluß für Heim und Büro

Allied Telesyn stellt eine neue Produktserie zur Medienkonvertierung für Breitbanddienste in Heim und Büro vor. Die Serie AT-FS210 bietet wandmontierbare Zugangs-Switches zur Konvertierung zwischen Ethernet und Fast Ethernet über Kupfer und Glasfaser. Der Benutzer kann seine lokale Desktop-Verbindung direkt in High-Speed-Netzwerke mit großer Bandbreite einbinden und eine Fiber-to-the-Office Lösung realisieren.

Die neuen Zugangs-Switches der Serie FS210 von Allied Telesyn bieten eine praktische Lösung für High-Speed-Netzwerkanbindung. Einfache Zwei-Port-Switches mit der Möglichkeit der Wandmontage dienen als Umwandler zwischen Netzwerkabschnitten unterschiedlicher Geschwindigkeiten und Medien und bringen mehr Flexibilität in den Netzwerkaufbau. Als lokales Verbindungsglied zu High-Speed-Glasfasernetzwerken zielen sie auf den Bedarf kleiner Netzwerke. Die Serie AT-FS210 wird ganz einfach Plug-and-Play installiert.

An die Wand

Das kompakte Chassis zur Wandmontage macht die Geräte zu einer perfekten Ergänzung für einen effektiven High-Speed-Netzwerkzugang. Der Switch wird in den Wandhalter eingeschoben, die Glasfaser-, Kupfer- und Stromversorgungskabel angeschlossen und mit den integrierten Kabelklemmen fixiert. Jeder Switch unterstützt Autonegotiation und bietet einen Full-Duplex-Link zu jedem beliebigen Gerät bei doppelt so viel Bandbreite im Vergleich zu vielen herkömmlichen Half-Duplex-Geräten. Auch MDI/MDIX-Auto-Sensing wird unterstützt, womit die Einbindung in das bestehende Netzwerk in seiner Gesamtheit gewährleistet ist. Die Geräte erfüllen den FCC-Class B Standard. Sie werden mit einer lebenslangen Garantie angeboten, das Netzteil hat 1 Jahr Garantie.

PowerBlade

Media Conversion System

Das PowerBlade Medienkonvertierungssystem auf Chassisbasis bietet modulare Multiprotokoll Lösungen zur High-Density Media Conversion für Service-Provider-Anwendungen, Telekommunikationsgesellschaften und Firmen-LANs. Allied Telesyn bringt eine High-Density-Lösung für die Medienkonversion mit SNMP-Management. Das PowerBlade System nach NEBS-Standard bietet mit seiner technologieübergreifenden Chassis/Blade-Architektur mit 18 Steckplätzen eine Vielzahl von Schnittstellen.

Das PowerBlade System von Allied Telesyn macht die Integration neuer Technologien in eine bestehende Netzwerkstruktur schnell und unkompliziert umsetzbar. Die Konvertereinschübe dienen der Medien- und Geschwindigkeitskonvertierung von Ethernet, Fast Ethernet und Gigabit Ethernet. Mit einfacher Handhabung und redundanten Netzteilen stellt PowerBlade eine Lösung für Enterprise- und Service-Provider-Netzwerke, die Flexibilität und Systemverläßlichkeit erfordern.

Management

Das Management erfolgt mit Hilfe des zusätzlichen SNMP Management Moduls, mit dem der Benutzer über eine grafische Oberfläche den Betrieb aller installierten Einschübe konfigurieren sowie sämtliche Kabelverbindungen überwachen kann. Doch kann das System auch ungemanagt gefahren werden. Das Management Modul kontrolliert den Betrieb der Lüfter sowie die Innentemperatur des Chassis. Das Modul selber besetzt keinen der Steckplätze und schränkt die Zahl der anzuschließenden Kanäle nicht ein. Das PowerBlade System ist auf maximale Redundanz ausgelegt, um aufgabenkritischem und anspruchsvollem Betrieb gerecht zu werden. Es unterstützt den Austausch von Einschüben im laufenden Betrieb und bietet Platz für eine optionale zusätzliche Wechselstromversorgung. Weiterhin ist eine Ausführung mit einem 48V DC Netzteil lieferbar, um die speziellen Anforderungen der Telekommunikationsgesellschaften und Internet Service Provider (ISP) zu erfüllen.

HEWLETT-PACKARD

Einfachheit und Komfort

HP Netserver E200

Einen neuen Server, der auf den Bedarf von kleinen und mittelständischen Unternehmen oder Arbeitsgruppen zugeschnitten ist, stellt Hewlett-Packard mit dem HP Netserver E200 vor. Er zeichnet sich durch Erweiterungsmöglichkeiten, einfache Installation und Bedienung sowie ein ausgesprochen günstiges Preis-Leistungs-Verhältnis aus.

Der HP Netserver E200 arbeitet mit einem 933 MHz oder 1 GHz schnellen Intel Pentium III-Prozessor. Ein 256 KB großer Level-2-Cache und der 133-MHz-Front-Side-Bus sorgen für einen schnellen Zugriff auf den Hauptspeicher. Der E200 wird mit 128 MB RAM ausgeliefert und ist auf 768 MB erweiterbar. Als Netzwerkverbindung dient eine eingebaute 10/100-TX-Netzwerkkarte. Wahlweise kann der neue Server mit IDE- oder SCSI-Festplatten ausgerüstet werden. So wird in der Version mit IDE-Festplatten standardmäßig eine 30-GB-Festplatte ausgeliefert.

Ausbaufähig

Als Erweiterung sind zwei 20-GB-Festplatten lieferbar. Ein CD-ROM-Laufwerk und ein Diskettenlaufwerk sind im Tower-Gehäuse integriert. Für Erweiterungen gibt es vier PCI-Steckplätze, einen PCI/ISA-Steckplatz und sieben Laufwerkseinschübe. Optional wird ein Laufwerksschacht von einem DLT-Bandlaufwerk für die Datensicherung belegt. Die Betreiber können entsprechend ihrem Anwendungsbedarf zwischen den Betriebssystemen MS Windows NT 4.0 Server, MS Windows NT 4.0 Small Business Server, MS Windows 2000 Server, Novell Netware 5.1, Novell Small Business Suite 5, Red Hat Linux 7.1, SuSE Linux 7.0 Professional, Caldera eServer 2.3 und Turbo Linux 6.0 (Rel. 6.02) wählen.

Einstiegs-Server

Der neue HP Netserver E200 eignet sich besonders für Anwender, die über wenig oder kein spezifisches IT-Know-how verfügen - beispielsweise Kanzleien, Handwerksbetriebe oder Praxen - aber auch für Unternehmen, die problemlos und schnell zu installierende Netzwerk-Server benötigen. Um diesen Anwendern die Installation und den Betrieb des neuen Servers so einfach wie möglich zu gestalten, wird der HP Netserver E200 mit einer bootfähigen CD-ROM, einem zuverlässigen Installationsmenü für das Netzwerkbetriebssystem und Installationshilfen für die Netzwerkkomponenten ausgeliefert. Die Wartung erleichtert das mitgelieferte HP Netserver E200-Diagnose-Tool. Hewlett-Packard bietet für ihren neuen Einstiegs-Server 1 Jahr Garantie mit Vor-Ort-Reparatur am nächsten Arbeitstag. Die Gewährleistungen lassen sich über die optionalen HP Supportpacks erweitern.

HEWLETT PACKARD

Preiswert

Procurve Switch 2124

Hewlett-Packard erweitert ihr Netzwerkprogramm. Gleichzeitig mit der Vorstellung des neuen Netzwerk-Switches Procurve Switch 2124 reduziert HP die Preisstruktur für ihre Netzwerkkomponenten um bis zu 17 Prozent.

HP erweitert ihr Netzwerkprogramm um einen neuen Procurve Switch für performantes und zuverlässiges Switching. Für die Switches gilt seitdem auch eine neue Preisstruktur mit einem bis zu 17 Prozent günstigeren Angebot. Der neue HP Procurve 2124 bietet 24 10/100-Mbit-Ports, die in einem 19-Zoll-Gehäuse mit nur einer Höheneinheit untergebracht sind. Kompaktheit und geringe Geräuschentwicklung qualifizieren ihn für den Einsatz in Büroumgebungen. Er ergänzt die vor rund einem Jahr eingeführte Produktreihe mit den HP Procurve Switches 2324 und 2524. Diese Switches erzielen mit ihrer Switch-on-a-chip-ASIC-Technologie eine Bandbreite von bis zu 9,6 Gbps.

Einstiegs-Switch

Anwender erwerben mit dem HP Procurve Switch 2124 einen skalierbaren Einstiegs-Switch, der einen zusätzlichen Steckplatz für einen 100FX-Uplink über einen optionalen Transceiver besitzt. Das Gerät verfügt über die patentierte HP-Technologie Auto-MDIX zur automatischen Kabelerkennung und Fehlerkorrektur bei hohem Rauschpegel. Dies macht die Verwendung von Cross-Over-Kabeln überflüssig und vereinfacht den Anschluß von aktiven Komponenten wie zum Beispiel Netzwerkkarten deutlich. Alle HP Procurve Switches werden mit lebenslanger Garantie, kostenlosen Software-Upgrades und Telefonsupport angeboten.

Für Kupfer und Glasfaser

Neue modulare Gigabit-Switches

Netgear hat die Verfügbarkeit des industrieweit ersten unmanaged 48-Port Modular-Fast-Ethernet-Switch FS750 bekannt gegeben. Weiterhin ist ab sofort ein 24-Port-Variante mit dem FS726 Switch verfügbar. Die neue Switch-Produktfamilie ermöglicht Anwendern die Umstellung zwischen Glasfaser- und Kupferkabelnetzwerken und bietet ihnen die Technologie für den Anschluß an Server oder Netzwerk-Backbones mit Gigabit-Datenraten.

Die FS700-Serie ist die erste Switch-Produktlinie von Netgear mit einer Portdichte dieser Größenordnung und modularen Gigabit-Uplinks. Die Einführung der Modular-Fast-Ethernet-Switches FS750 und FS726 ist ein Angebot einfach zu installierender Netzwerkprodukte für den problemlosen Anschluß kleinerer und mittelständischer Unternehmen an Glasfaser- und/oder Kupfer-Gigabit-Netzwerke. Die FS700-Serie wird zu attraktiven Preisen angeboten und erweitert die Netgear-Produktfamilie von führenden 10/100/1000 MBit/s Ethernet-Netzwerkprodukten, um die Anforderungen kleinerer Geschäftskunden im Hinblick auf Leistung, Qualität und Bedienkomfort zu erfüllen.

SOHO Kunden

Die Netgear-Produktfamilie stellt Small-Business- und Home-Office-Kunden hohe Leistung zu günstigen Preisen zur Verfügung. Das Modell FS750 ist industrieweit der erste unmanaged 48-Port Modular Fast-Ethernet-Switch, der den Anschluß von bis zu 48 10/100 MBit/s-Client-Nutzer an Gigabit-Server und Gigabit-Backbone-Netzwerke mit Glasfaser- und/oder Kupferleitungen ermöglicht. Die beiden modularen Gigabit-Einschübe erlauben bei Bedarf einen flexiblen Anschluß der FS700-Switches an Glasfaser- und/oder Gigabit-Netzwerke, wodurch ein maximaler Investitionsschutz gewährleistet wird. Die 10/100 MBit/s Autosensing-Hochgeschwindigkeitsports der Switches FS726 und FS750 unterstützen die Auto-Uplink-Funktion für einfache Bedienung und automatische Konfiguration. Datenflußsteuerungstechnologie auf der Basis des IEEE 802.3x-Standards verhindert Datenverluste und unterstützt maximale Netzwerkleistung. Unter Verwendung hochentwickelter Chipsätze von Marvell/Galileo gewährleisten die Netgear-Switches FS726 und FS750 störungsfreie Filterung und Weiterleitung des Datenverkehrs mit maximaler Geschwindigkeit. Leicht ablesbare LEDs auf der Frontplatte zeigen den aktuellen Switch-Status an und erleichtern die Behebung von Störungen. Die Netgear-Switches der FS700-Serie erfordern keine Konfiguration und werden mit einem Rackmount-Kit, einer 5-Jahres-Garantie auf das Gerät und einem Netzteil, auf das es 2 Jahre Garantie gibt, geliefert.

Familie komplett

Gigabit-Glasfaser-Ethernet Karte GA 621

Netgear kündigte die Verfügbarkeit ihrer Gigabit-Glasfaser-Ethernet-Karte GA621 an. Damit ist nach der Gigabit-Kupfer-Karte GA622 und dem Gigabit-Kupfer-Ethernet-Switch GS508T die preisgekrönte Gigabit-Familie jetzt um den Bereich Glasfaser erweitert und somit vollständig.

Die Gigabit-Glasfaser-Ethernet-Karte GA621 Netgear läßt mit 1000 Mbps Engpässe in Netzwerken verschwinden. Sie eignet sich besonders für den Einsatz in Servern, die mehrere Fast-Ethernet-Clients betreiben. Die Gigabit-Glasfaser-Ethernet-Karte GA621 unterstützt sowohl den Betrieb mit 64- als auch den mit 32-bit PCI-Bus und ist mit einer umfassenden Treiberbibliothek für alle gängigen Betriebssysteme ausgestattet. Sowohl die Karte als auch die Netgear-Treiber sind auf Spitzenleistung von Servern optimiert. Engpässe werden allenfalls auf den Server bzw. den Backbone zurückverwiesen. Dank Plug-and-Play und umfangreicher Treiberversorgung ist die GA621 in wenigen Minuten eingebaut und einsatzfähig. Somit erfüllt sie die beiden Hauptkriterien für Netzwerkkarten: hoher Durchsatz und einfacher Einbau. Mit der Gigabit-Glasfaser-Ethernet-Karte GA621 erweitert Netgear ihre Gigabit-Familie um das Segment Glasfaser. Waren die Gigabit-Produkte bisher noch aufgrund ihrer Komplexität und hoher Kosten großen Unternehmensnetzen vorbehalten, so hat Netgear ihren Teil dazu beigetragen, daß solche Karten mittlerweile auch für kleinere und mittelgroße Unternehmen und selbst für Heimnetzwerke attraktiv geworden sind.

AVM

ISDN-Kombianlage

FRITZ!X USB v2.0 im Handel

Die neue ISDN-Kombianlage FRITZ!X USB v2.0 von AVM ist im Handel. Die Version 2.0 des vielfachen Testsiegers ist kleiner in den Abmessungen und präsentiert sich in einem neuen Design. Für analoge Endgeräte wurden erweiterte Anschlußmöglichkeiten eingerichtet.

FRITZ!X USB v2.0 kombiniert einen ISDN-Controller mit der Anschlußmöglichkeit für bis zu 4 analoge Geräte in einem neuen kompakten Design und ist damit für den einfachen Einstieg in die ISDN-Leistungsvielfalt ideal geeignet. Auch während des 2-Kanal-Internetsurfens ist FRITZ!X USB für eingehende Anrufe erreichbar. Deutlich erweitert wurden die Anschlußmöglichkeiten für analoge Endgeräte. Mit der Version 2.0 von FRITZ!X USB können analoge Geräte sowohl mit dem in Deutschland bewährten TAE-Stecker als auch mit dem international üblichen Westernstecker oder mit einer vorhandenen Haustelefonverkabelung genutzt werden. FRITZ!X USB v2.0 kann mit den Microsoft-Betriebssystemen Windows Me, 98 und 2000 genutzt werden. Bei Windows XP sind die Treiber für das neue AVM-Produkt bereits auf der Betriebssystem-CD enthalten. Erstmals in dieser Geräteklasse bietet AVM vom Start weg auch CAPI 2.0-Treiber für das Betriebssystem Linux an.

Erweiterte Leistung

Im Zusammenspiel mit FRITZ!X USB v2.0 ist die automatische Zuschaltung des zweiten B-Kanals frei konfigurierbar. So lassen sich sogar während 2-Kanal-Internetverbindungen Anrufe annehmen. In der Grundeinstellung wird der zweite B-Kanal zugeschaltet, sobald die Datenmenge in einem bestimmten Zeitraum einen festgelegten Wert überschreitet. Die größere Bandbreite wird solange genutzt wie die höhere Auslastung besteht. Ist der zweite B-Kanal nicht mehr erforderlich, wird er selbständig abgebaut. Weitere neue Leistungsmerkmale sind eine Anruferliste zur Übersicht eingegangener Calls bei Abwesenheit und "Besetzt bei besetzt", hier erhält ein zweiter Anrufer ein Besetztzeichen. Die neue ISDN-Kombianlage bietet die volle Unterstützung von Fast Internet over ISDN. So läßt sich mittels Datenkompression und ohne zusätzliche Kosten je nach aufgerufener Inter-netseite der Aufbau um bis zu 120 Prozent beschleunigen. Zum Lieferumfang gehört neben der Anlagen- und Konfigurations-Software die neueste Version der Kommunikationssoftware FRITZ! mit dem einfachen und schnellen Internetzugang FRITZ!web, dem PC-Fax FRITZ!fax, dem Softwaretelefon FRITZ!fon, dem Anrufbeantworter FRITZ!vox und dem Dateitransferprogramm FRITZ!-data. FRITZ!X PC, die Produktvariante für die serielle Schnittstelle, ist ebenfalls ab sofort in einer neuen Version 3.0 erhältlich.

INTEL

2 Gigahertz Schwelle

Xeon Prozessoren für Workstations

Intel hat den schnellsten Prozessor der Welt für Hoch-leistungs-Workstations mit Dualprozessoren vorgestellt. Der auf der NetBurst Mikroarchitektur basierende 2 Gigahertz Xeon Prozessor zielt auf die Marktbereiche Hochleistungs- und Midrange-Workstations. Leistungssteigerungen von über 10 Prozent gegenüber bestehenden Xeon basierten Systemen werden erwartet.

Die Intel Xeon Prozessorfamilie wurde im Hinblick auf die Anforderungen an Skalierbarkeit, Verfügbarkeit und Verwaltung im Marktsegment hochleistungsfähiger Workstations entwickelt. Workstations mit Intels neuen Xeon Prozessoren verwenden die Intel NetBurst Mikroarchitektur, um die Rechenleistung für Video, Audio, 3-D Grafik und neueste Internet-Technologien zur Verfügung zu stellen. Die Intel Xeon Prozessor Plattform basiert auf dem leistungsstarken Intel 860 Chipsatz. Dieser Chipsatz unterstützt duale RDRAM Speicherbänke als Ergänzung zum 400 MHz Systembus des Intel Xeon, der einen Datendurchsatz von bis zu 3,2 Gigabyte pro Sekunde ermöglicht. In Zukunft werden höhere Taktfrequenzen und größere Cache-Speicher weiteren Spielraum bei Berechnungen sowie grafisch und I/O-intensiven Arbeitsbelastungen bieten. Nach neuesten Zahlen der Markforschung basierten mehr als 70 Prozent aller im 2. Quartal 2001 ausgelieferten Workstations auf Intel Prozessoren. Im Marktsegment der Mid-Tier- und Highend-Workstations gewinnen auf Intel basierende Workstations weiterhin an Beliebtheit.

Auto-Mobil-Funk

Drahtlose Anwendungen für den Einsatz in Fahrzeugen

Auch Intel stellte jüngst ein neues webbasierendes Programm vor, mit dessen Hilfe Entwickler drahtlose Anwendungen, Dienste und Geräte für den Einsatz in Autos herstellen können. Das Intel Telematics Design Center bietet Telematik-Entwicklern Zugriff auf Programme, Bibliotheken und mehr als 300 Software-Werkzeuge zum Entwerfen von Produkten für den weltweit wachsenden Telematik-Markt.

Bei der Telematik wird die drahtlose Übermittlung von Sprache und Daten im Auto genutzt, um besondere Dienste wie Navigation im Fahrzeug und Notfallhilfe im Straßenverkehr zu ermöglichen. Die steigende Nachfrage nach Telematik-Geräten und Applikationen durch die Verbraucher hat zu einem bedeutenden Interesse von Seiten der Hersteller und Service-Provider geführt. Der Markt zeichnet sich durch ein wachsendes Interesse an sprachaktivierten Telefonen, multimedialer Unterhaltung und der drahtlosen Nutzung regionaler Dienste aus. Das Intel Telematics Design Center unterstützt Hersteller von Telematik-Geräten in den Bereichen Entwicklung und Technik unter Verwendung von Intel StrongARM und XScal basierenden Prozessoren. Ziel sollen Navigationsanwendungen, weitere Internet-Geräte und -Applikationen, freihändig bedienbare Telefone und Multimedia für den Einsatz im Auto sein.

Telematics Design Center

Entwickler, die an Telematik-Entwürfen arbeiten, können seit neuestem auf das Intel Telematics Design Center unter www.intel.com/design/wireless/telematics/designcenter zugreifen. Bei der Benutzung entstehen den Entwicklern keinerlei Kosten. Das Center unterstützt sie mit Tools und Informationen. Diese beinhalten Hardwareentwürfe für umfangreiches Multimedia und freihändig bedienbare Telefone auf Basis der Intel StrongARM und zukünftiger Intel® XScale Prozessoren. Eine Entwurfsunterstützung erfolgt durch die Application Libraries mit Richtlinien für den Hardware-Entwurf und die Software-Entwicklung. Zudem gibt es Software-Werkzeuge für die Programmierung von Flash-Speichern und das Debuggen von Programmen sowie Links zu Downloads von Drittanbietern, deren Tools für Betriebssysteme und Entwicklung von Java Applikationen zugeschnitten sind. Das Telematics Design Center ist Teil des Intel PCA Entwicklernetzwerks für Intels Personal Internet Client Architecture (Intel PCA).

Es bietet Unternehmen Unterstützung in den Bereichen Entwicklung, Technik und Vertrieb. Es richtet sich an Entwickler für Mobiltelefone, Personal Digital Assistants (PDAs) und weiteren mobilen Internet-Geräten sowie -Applikationen basierend auf der Intel PCA. Intel PCA ist eine offene Hardware- und Software-Architektur. Sie soll die Entwicklung von drahtlosen Internet-Geräten und -Anwendungen beschleunigen.

ELSA

Public Spots

Initiative für drahtlosen öffentlichen Internet-Zugang

Unter dem Motto go!wireless startete ELSA eine Initiative zur Einrichtung von Internet-Zugängen an öffentlichen Plätzen über Wireless LAN-Technologien. ELSA setzt diese Funktechnologie bereits seit mehreren Jahren erfolgreich für drahtlose Unternehmens-Netzwerklösungen ein und richtet sich inzwischen mit drahtlosen Netzwerkprodukten auch an Heimanwender.

Technologische Kompetenz und Erfahrung mit dem schnellen und kostengünstigen Funkstandards dienen ELSA jetzt als Basis, um die Verbreitung von Public Spots entscheidend voranzutreiben und dieses Geschäftsfeld frühzeitig zu besetzen. Das Marktpotential liegt laut Gartner-Dataquest bei über 19 Millionen mobilen Nutzern, die im Jahr 2006 regelmäßig Public Access-Dienstleistungen basierend auf Wireless LANs in Anspruch nehmen werden. ELSA demonstrierte in Kooperation mit der Aachener Telefongesellschaft accom drahtlose Datenkommunikation mitten im Aachener Stadtzentrum. Über Zugangspunkte des accom-LWL-Regio-Netzes wird in der historischen Altstadt und in zentralen Bereichen der Innenstadt ein öffentlicher, drahtloser Internetzugang (Public Spot) angeboten. Mit Hilfe der Funkbasisstation ELSA LANCOM Wireless mit Public Access-Funktionalität wird drahtloses Surfen für alle möglich, deren Notebook, PC oder Organizer über eine Wi-Fi-kompatible Funkkarte verfügt. In der Einführungsphase bis Ende diesen Jahres ist der Internet-Zugang sogar kostenlos.

Drahtlos-Zugang

Public Spot-Netzwerke eignen sich insbesondere für Hotels, Flughäfen, Bahnhöfe, Kongreßhallen oder Restaurants, die ihren Gästen per Funknetzwerk drahtlosen Zugang zum Internet ermöglichen wollen. Aber auch für Unternehmen, die ihre Außendienstmitarbeiter drahtlos in das entfernte Firmennetzwerk einbinden wollen. Ziel der jüngsten ELSA go!wireless-Initiative ist die Information und Beratung sowie die Vermittlung qualifizierter Lösungsanbieter und Betreiber von Public Spots. Dienstleistungsbetriebe wie Hotels, Restaurants oder Messegesellschaften, die ihren Gästen per Funknetzwerk den drahtlosen Zugang zum Internet ermöglichen wollen, sowie Anwender erhalten eine geeignete Beratungsplattform. Zur Realisierung von Public Access Netzwerken arbeitet ELSA eng mit führenden Lösungsanbietern und Betreibern zusammen. Als erster Anbieter hat ELSA eine komfortable und sichere Software-Lösung entwickelt, die eine Authentifizierung, Autorisierung und Abrechnung von einzelnen Benutzern ermöglicht.

NetCheckIn

In einem weiteren Pilotprojekt hat ELSA in Zusammenarbeit mit NetCheckIn, einem der ersten Anbieter von drahtlosen Internetzugängen in öffentlichen Bereichen, ein Kongreßhotel in Landshut ausgerüstet. Damit wird der Wunsch vieler Geschäftsreisender erfüllt, im Hotel über einen schnellen, komfortablen und kostengünstigen Internetzugang verfügen zu können. In der Kooperation mit NetCheckIn wurde ein komplettes Betreibermodell erstellt, das für alle Hotels geeignet ist, weil keinerlei Verkabelungen oder Erweiterungen bestehender Systeme, die hohe Kosten verursachen, notwendig sind. NetCheckIn stellt dem Hotel dagegen die gesamte notwendige Infrastruktur zur Verfügung, administriert das System und bietet den Kunden einen umfassenden telefonischen Support. Für die Verbindung mit dem Hotelfunknetz benötigt der Gast lediglich eine Wi-Fi (Wireless Fidelity) kompatible Funkkarte, um während des gesamten Hotelaufenthalts online zu sein. Business Notebooks der neuesten Generation sind bereits mit der entsprechenden Funktechnik ausgestattet. Der Zugang zum Internet erfolgt per Breitbandzugang mit bis zu 1,5 Mbps über eine Standleitung. Im Gegensatz zur Einwahl per Modem oder ISDN Karte bleibt der Kunde ständig mit dem Internet verbunden. Always-On können E-Mails oder Börsenkurse ohne erneute Einwahl ständig empfangen werden.

`www.elsa.de/go-wireless`

Gigabit Ethernet erweitert

GIGAline Switches und 1000Base-T Netzwerkadapter

Die Compu-Shack Production hat ihre Produktfamilie GIGAline um drei Gigabit Ethernet Switches und zwei leistungsfähige 1000Base-T Netzwerkadapter erweitert. Der GIGAline Switch 1008 und die 64-Bit oder 32-Bit Gigabit Netzwerkkarten gewährleisten ein Maximum an Performance und Interoperabilität bei Verwendung vorhandener CAT5 Kupferverkabelung, um Workgroups und Power Usern höchste Performance für ein schnelleres Arbeiten zu ermöglichen. Für den Backbone-Bereich sind neue GIGAline 8000 Switches erhältlich.

Die neuen GIGAline Produkte der Compu-Shack Production bieten zu einem hochinteressanten Preis-Leistungsverhältnis Gigabit Performance für Server, Backbones und Workgroups. Die 32-Bit breitem PCI-Bus der GIGAline 1000Base-T Adapter bieten Power-Usern oder bei Videoübertragungen eine durchsatzintensive Netzwerkverbindung. Die 64-Bit PCI Version empfiehlt sich beim Einsatz in Hochleistungsservern.

Power Switches

Neue Layer 2 Switches bieten zusätzliche Flexibilität in der Auslegung von Netzwerkstrukturen. Der GIGAline1008 bringt als leistungsstarke Workgroup Anbindung mit 8 Auto-Negotiation 100Base-TX Ports und Gigabit-Uplink zur Aufnahme eines 1000Base-T Backbones richtig Schwung in überlastete Netzwerksegmente, und das unter Verwendung von bereits vorhandener CAT5 Kupferverkabelung. Der GIGAline 8000-SX stellt sogar acht Gigabit Ethernet Ports auf Fiberbasis bereit. Diese basiert auf der weit verbreiteten Duplex-SC Anschlußtechnologie. Um eine gebäudeübergreifende Backbone-Anbindung über eine Multimode Glasfaser bereitzustellen, kann auch die Sekundärverkabelung durch die hohe Anzahl der Fiber Ports leicht in Glasfaser ausgeführt werden.

Big Backbone

Um die 1000Base-T Gigabit-Uplinks von durchsatzstarken Workgroup Switches wie dem GIGAline 2024 aufzunehmen und diesen eine direkte Backbone-Anbindung an mehrere hochperformante Server zu gewährleisten, wird der GIGAline 8000-T eingesetzt, mit 8 1000Base-T Ports auch im Workgroup-Bereich, wo 1000Base-T Gigabit für bandbreitenintensive Anwendungen wie simultanes Streamen von Video und Audio oder die Verfügbarkeit von großen Datenmengen realisiert werden soll. Die neuen GIGAline Produkte bieten Dank des großen Adressenspeichers für bis zu 8000 MAC-Einträge ein hohes Maß an Flexibilität und Funktionalität in der Auslegung von Hochgeschwindigkeitsnetzen.

SMB Partner

FaxWare in der neuen NSBS 6

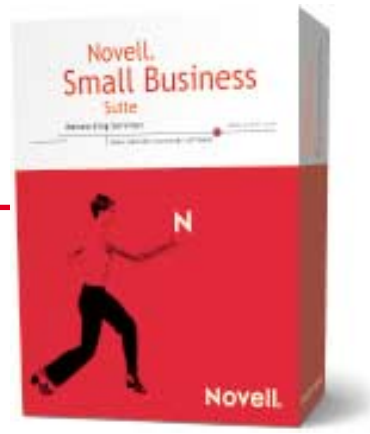
Tobit Software und Novell haben eine Partnerschaft für Novells weltweite Aktivitäten im Bereich kleiner und mittelständischer Unternehmen abgeschlossen. Tobit bringt mit einer speziellen Version ihrer Netzwerkfaxlösung FaxWare eine professionelle Kommunikationslösung in die neue Novell Small Business Suite 6

Als Bestandteil der Small Business Suite 6 wird mit der FaxWare von Tobit Software eine Netzwerkfaxlösung der neuesten Generation ausgeliefert. Die FaxWare ist ein technisch ausgereiftes Produkt, speziell für kleinere und mittelere Unternehmen. Die Novell Small Business Suite 6 wird weltweit vertrieben und enthält die FaxWare in der Version 6.6 als eigenständiges CD-Bestandteil.

Auf Wachstum eingestellt

Bei der Installation der FaxWare wird automatisch die Anzahl der Benutzerlizenzen an die Anzahl der NetWare-User angeglichen. Bis zu 50 Anwender können die Vorteile der unternehmensweiten Faxlösung an ihrem Arbeitsplatz nutzen. Dazu gehören das rationelle Verwalten von Faxen sowie das einfache Erstellen von umfangreichen Faxrundsendungen. Um die Echtheit der Lizenzen zu prüfen, enthält FaxWare zusätzlich einen automatischen Abgleich mit einer Lizenzdatenbank, durch die die Gültigkeit der Version geprüft wird. Tobit FaxWare unterstützt durch diese Zusammenführung die elektronische Kommunikation in einem praktischen Paket. Das gesamte System ist durch ein erweiterbares User-Konto auf steigende Anforderungen ausgerichtetund kommt Anfang November in den Handel.

NOVELL



Komplettlösung für kleine Unternehmen

Novell Small Business Suite 6 für Netzwerk, Kommunikation und Sicherheit

Novell bringt die neue Small Business Suite 6 auf den Markt. Die Netzwerklösung für kleine und mittlere Unternehmen enthält als zentrale Komponenten das Netzwerkbetriebssystem NetWare 6 sowie GroupWise 6 für E-Mail- und Kommunikationsdienste. Im Lieferumfang enthalten sind ZENworks for Desktops 3.2 sowie die Sicherheitslösung Novell BorderManager Enterprise Edition 3.6. Als Partnerprodukte werden Tobit FaxWare, Network Associates VirusScan/NetShield und die Internet-Software Ragula FatPipe mitgeliefert.

Nachdem die NetWare 6 seit Oktober auf dem Markt ist und auch die deutsche Version ab dem 15. November 2001 zur Verfügung stehen wird, kommt ebenfalls im November die Novell Small Business Suite 6 heraus. Sie enthält das Netzwerkbetriebssystem NetWare 6, GroupWise 6 sowie ZENworks for Desktops 3.2 für das Management von Desktops und Applikationen. Die BorderManager Enterprise Edition 3.6 mit Virtual Private Network garantiert mit Authentifizierungs- und Firewall-Funktionen die Vertraulichkeit der Daten in kleinen und mittleren Unternehmen. Die Novell Small Business Suite 6 nutzt die Stärken der aktuellen Novell Technologien, um Unternehmen mit bis zu 50 Anwendern zuverlässige Net Services zur Verfügung zu stellen. Die Lösung ermöglicht diesen kleinen Unternehmen, ihr Nehmensnetz nahtlos und sicher mit dem Internet zu verbinden und über Simplified Install, das Novell Easy Administration Tool (NEAT) und Novell Internet Connection Expert (NICE) effizient zu verwalten.

Komplettlösung

Die Suite ist eine Kombination ausgesuchter Anwendungen, die mit den neuen NetWare 6 Komponenten ausgeliefert wird, um von überall her einen Zugriff auf zentrale Netzwerkressourcen zu ermöglichen. Mit Novell iFolder, iPrint und NetWare Web Access können Anwender Datei-, Druck-, E-Mail- und Verwaltungsfunktionen nutzen. Der Zugriff kann über das Internet von jedem Desktop, über jedes Gerät und an jedem Ort erfolgen. Somit können auch kleinere Unternehmen preiswert an den One Net Technologien Novells partizipieren. Mit der NSBS 6 erhalten sie eine bedienerfreundliche, sichere und extrem zuverlässige Netzwerklösung. Sie bietet zu erschwinglichen Preisen wichtige Zusatzfunktionen wie E-Mail, Datei-Synchronisation und Backup, Internet Printing und den Internet-Zugriff auf Dateien über einen Web-Browser. Außerdem sind die Partnerprodukte Tobit FaxWare, Network Associates VirusScan/NetShield und die Internet-Software Ragula FatPipe im Lieferumfang enthalten.

3COM

Breitband-Internet mit Voice

Office Connect Gateway Familie mit High-Speed DSL Services

Service Provider und ihre Unternehmenskunden können gleichermaßen von den Vorteilen der neuen 3Com OfficeConnect Gateway Produktfamilie profitieren. Die innovativen 3Com DSL Produkte unterstützen Service Provider bei der Schaffung von High-Speed-Internetzugängen und der Nutzung von Voice-Funktionen für Kleinbetriebe, Unternehmensaußenstellen und Telearbeiter.

Die mit zahlreichen Leistungsmerkmalen ausgestattete 3Com DSL-Serie umfaßt bei bewährt einfacher Handhabung die Data und Voice Versionen der 3Com OfficeConnect Gateways ADSL und SHDSL, das 3Com OfficeConnect Gateway Voice Expansion für ADSL und SHDSL sowie den 3Com OfficeConnect Router 612 ADSL. Mit den OfficeConnect Gateways können Service Provider ihren Kunden auf Basis der DSL-Technologie Sprach- und Datendienste über bestehende Telefonleitungen anbieten. Dabei können die Data-Versionen des 3Com OfficeConnect Gateways unter Verwendung der 3Com OfficeConnect Gateway Voice Expansion Einheit jederzeit auf volle Voice-Funktionalität aufgerüstet werden. Provider können mit OfficeConnect Gateway bis zu 12 Telefonleitungen in Festnetzqualität zur Verfügung stellen.

Secure Connections

Unternehmen können mit der DSL-Technologie ihre bisher getrennte Sprach- und Datenkommunikation ohne Qualitätsverlust in einem einzigen High-Speed-Netzwerk zusammenfassen und Kosten einsparen. Virtual Private Networks sorgen dabei für einen komfortablen Informationsaustausch und hohe Datensicherheit. Das 3Com OfficeConnect Gateway ist standardmäßig mit der VPN-Funktionalität ausgestattet, zusätzliche Erweiterungen sind nicht erforderlich.

Voice Connections

Zudem bringt 3Com mit dem OfficeConnect Remote 612 ADSL einen kostengünstigen Daten-Router für Internet/ LAN-Connec-tivity auf den Markt. Die neue Gateway Produktfamilie verfügt neben der Voice-Funktionalität auch über Secure Connections und ist in Verbindung mit anderen LAN-Telefonie-Lösungen von 3Com voll skalierbar. Zudem ist die Kompatibilität zu den Produkten führender DSLAM- sowie Voice Gateway-Anbieter gewährleistet. Die 3Com OfficeConnect Produkte sind seit Oktober auf dem Markt.

Power pur

USV mit Dauerwandler-Technologie

Die Online USV AG bietet Unterbrechungsfreie Stromversorgung mit Dauerwandler-Technologie. Diese bewirkt eine vollständige Entkopplung des Computersystems vom Stromnetz und gewährleistet einen konstanten Spannungsausgang in Sinusform. Selbst extreme Spannungsschwankungen können so keinen Schaden am Rechner, Netzwerk oder an der Peripherie anrichten.

Die Online USV-Serien XANTO S und SR basieren auf der innovativen Online-Doppelwandler-Technologie, die die Abkopplung eines Systems vom Stromnetz ermöglicht. Ein intelligenter Systemmanager prüft automatisch die Verfügbarkeit der Batterieeinheiten und garantiert die hundertprozentige Systemverfügbarkeit und schützt die Batterien vor Über- und Tiefenentladung. Dies wirkt sich positiv auf die Lebensdauer der Batterie aus. Der Schnell-Lademodus lädt die Batterien bei Bedarf in ein bis zwei Stunden wieder auf.

Spektrum bis 20KVA

Das große Leistungsspektrum der Xanto S Serie reicht von 700 bis 10.000 VA im einphasigen Bereich sowie von 10 bis 20 KVA im dreiphasigen Bereich als Standalone-Gerät. Die Modelle der Xanto SR Serie bieten Leistungen zwischen 700 VA und 3.000 VA zum Einbau in ein 19-Zoll-Rack. Durch den Einsatz von Battery-Packs bei den Modellen ab 1 KVA sind Autonomie-Zeiten von über vier Stunden möglich. Alle Modelle verfügen über einen elektronischen Bypass zum Schutz vor Überlastung. Eine Leuchtdioden-Anzeige informiert über Last, Überbrückungszeit und den Zustand der Batterie.

Management

Die Online USV ist serienmäßig mit einer RS 232 Schnittstelle ausgestattet. Für Steckkarten wie beispielsweise RJ-45 Adapter oder potentialfreie Kontakte ist ein entsprechender Einschub vorhanden. Bei den Leistungsstufen 10, 15 und 20 KVA der Reihe Xanto S sorgt der dreiphasige Eingang für eine gleichmäßige Lastaufteilung. Im Preis der XANTO S ist die DataWatch USV- und Netzwerk-Management-Software inbegriffen. DataWatch unterstützt Windows NT, 95, 98 und 2000, Novell Netware, Linux, UNIX, IBM AIX und Sun Solaris. Bei längeren Störungen des Stromnetzes wird der Administrator informiert und ein automatischer Shutdown der Rechner durch die USV eingeleitet. Für alle Geräte der Xanto S und SR Serie gewährleistet der Hersteller zwei Jahre Vollgarantie, bei der Kunden bis zum Morgen des folgenden Arbeitstages ein Austauschgerät erhalten.

Neue Internet Router

Cisco 7300 und 7600 für Multiprotokoll-Routing

Cisco Systems erweitert ihr Produktportfolio um die neuen optischen Router 7300, 7603 und 7606 für Konzerne und Service Provider. Sie sind auf die sehr hohe OC-48-Geschwindigkeit skalierbar und zeichnen sich durch Multiprotokoll-Routing und hohe Verfügbarkeit aus. Die neuen Komponenten sind Bestandteil von Cisco AVVID Architektur zur Übertragung von Sprache, Video und Daten in Netzwerken.

Die neue Cisco 7000 Internet-Router-Familie besteht aus Routern, die mehrere Anwendungen wie Voice-over-IP, Virtual Private Network sowie Layer 7 Content Recognition und Switching simultan auf derselben Plattform bereitstellen. Damit reduzieren sie die Komplexität eines Netzwerks und die Kosten für die Verbindung zu einem LAN. Die Netzinfrastruktur ist durch den modularen Aufbau und die Größe der Router auf die zukünftige Entwicklung eines Unternehmens erweiterbar. Davon profitieren gleichermaßen Konzerne und Service Provider mit modularen und Multiprotokoll-Plattformen, die ein flexibles und breites Angebot an Diensten zur Verfügung stellen.

Express Forwarding

Mit dem Internet Router 7300 hat Cisco einen neues Gerät mit Multiprotokoll-Routing entwickelt, das auf OC-48-Übertragungsraten (Optical Carrier) skalierbar ist. Der Cisco 7300 ist mit einem zentralen Routing-Prozessor (NSE-100) für hohe Leistung ausgestattet und stellt eine Vielzahl an Diensten und Protokollen bereit, die auf dem Cisco IOS System basieren. Der Routing-Prozessor besitzt zwei fest installierte Gigabit Ethernet Ports und ist bei Bedarf mit bis zu vier modularen Schnittstellen erweiterbar. Der R7000 Prozessor arbeitet mit einer Geschwindigkeit von bis zu 450.000 Paketen pro Sekunde. Er wird durch einen PXF IP-Service-Prozessor (Parallel Express Forwarding) von Cisco unterstützt, der wichtige IP-Dienste mit einer Leistung von bis zu 3,5 Millionen Paketen pro Sekunde hardwareseitig beschleunigt. Damit stehen erweiterte Anwendungen wie Quality of Service, Multiprotocol Label Switching (MPLS), Intrusion Detection und Layer 7 Content Switching zur Verfügung. PXF-beschleunigte Software-Dienste wie Centralized CEF (Cisco Express Forwarding), NetFlow v5 und v8, Turbo ACLs (Access Control List), QoS-Klassifizierung und -Markierung und Low Latency Queuing (LLQ) ergänzen die Schnittstellenmodule. Software-Funktionen auf Basis des Cisco IOS sowie die redundante Stromversorgung stellen die Verfügbarkeit des Routers sicher.

OC-48-Geschwindigkeit

Gleichzeitig erweiterte Cisco die 7600 Serie um zwei neue Router. Der Cisco 7603 ist ein kompakter Hochleistungs-Router für den WAN-Zugang. Er besitzt drei Steckplätze. Die Forwarding-Rate beträgt 15 Millionen Pakete pro Sekunde. Die Backplane hat einen Durchsatz von 32 Gbit/s. Während der Cisco 7603 vor allem für große mittelständische Unternehmen oder Außenstellen positioniert ist, die eine hohe Bandbreite zur Zentrale oder zu einem Service Provider benötigen, wurde der Cisco 7606 für den Zugang zum WAN in großen Unternehmen oder für die Verbindung zwischen Datenzentren konzipiert. Die Forwarding-Rate beträgt 30 Millionen Pakete pro Sekunde bei einem gesamten Datendurchsatz von 160 Gbit/s. Der Cisco 7606 wird mit sechs Steckplätzen zur Erweiterung mit modularen Schnittstellen ausgeliefert. Die Cisco Internet Router aus der 7600 Familie sind auf OC-48-Geschwindigkeit skalierbar. Das entspricht einer Übertragungsrate von 2,5 Gbps. Die Router weisen durch redundante Stromversorgung einen hohen Grad an Verfügbarkeit auf und sind für den flexiblen Unternehmenseinsatz im LAN, WAN und MAN (Metropolitan Area Network) geeignet. Die neuen Cisco Router sind ab sofort erhältlich.

neue Anzeige Cisco

...Standleitungskomfort

Service für kleine Unternehmen: Mit einem neuen Softwaremodul, den Server Locator Services for DvISE, ermöglicht Tobit Software das Betreiben einer Quasi-Standleitung trotz wechselnder IP- Adressen. Damit haben auch kleinere Unternehmen oder Home-Offices die Möglichkeit eines ständigen Nachrichtenzugriffs. Voraussetzung ist David 6.6 und eine Always-Online-Verbindung zum Internet, z.B. über eine DSL Flat. Die Server Locator Services for DvISE werden - anders als ursprünglich angekündigt - serienmäßig in David integriert. Der neue Dienst soll mit dem Sevice Pack 2 for DvISE am 12. Oktober 2001 im kostenlosen Download auf der Tobit Web-Site verfügbar sein. Er ermöglicht eine kostengünstige Online-Präsenz in Büros, für die eine echte Standleitung aus Kostengründen bislang kein Thema sein konnte, und sorgt für die ständige Erreichbarkeit eines David Servers trotz wechselnder IP-Adressen. Der Server teilt dabei dem DNS-Server bei Tobit Software regelmäßig seine aktuelle Adresse mit. Erfolgt eine Anfrage über einen Web- oder WAP-Browser, bekommt dieser vom DNS-Server die aktuelle IP-Adresse des David-Servers mitgeteilt. Im Anschluß erfolgt eine automatische Umleitung auf die aktuelle IP, die für den Anfragenden unmerklich stattfindet. In gleicher Weise funktioniert die automatische Umleitung beim Aufruf von Web-Seiten und beim direkten Austausch von E-Mails, ohne Zwischenspeicherung bei einem Provider. Der DNS Server sorgt als die zentrale Auskunftsstelle für den aktuellen Aufenthaltsort eines Servers für dessen ständige Erreichbarkeit. Beim Fernzugriff auf Nachrichten muß zusätzlich das Internet Access Module eingesetzt werden, das den Web- und WAP-Server beinhaltet.

...Flash

Speicher für Mobilte: Intel stellte einen neuen Flash Speicher-Chip vor, der die Leistung von Mobiltelefonen, Personal Digital Assistants und drahtlosen Geräten verbessert. Das 3 Volt Synchronous Intel StrataFlash Memory liest bis zu fünfmal schneller als frühere Generationen des StrataFlash Speichers. Programme werden schneller ausgeführt und der Zugriff auf Daten wird beschleunigt. Im Burst Mode können bis zu 92MB/s vom Speicher übertragen werden. Der neue Speicherbaustein stellt die dritte Generation der Intel Multi-Level Cell (MLC) Technologie dar und wird mit der 0.18-Mikron Prozeßtechnologie gefertigt. Intel führte MLC-Technologie im Jahr 1997 mit der ersten Intel StrataFlash Generation ein. Sie bietet eine preiswerte Lösung für die Ausführung von Code und die Speicherung von Daten in einem Chip. Das Flash Produkt ist die neueste Ergänzung des drahtlosen Produkt-Portfolios von Intel. Es ergänzt die Intel Personal Internet Client Architecture - eine Vorlage für die Entwicklung und Herstellung drahtloser mobiler Kommunikationsgeräte, die über die Möglichkeit der verbalen Kommunikation einen Weg ins Internet eröffnen.

...Multimedia

Klangvolle Ergänzung: Microsoft Plus! für Windows XP, das Ergänzungspaket für das neue Desktop-Betriebssystem von Microsoft enthält zahlreiche Tools, Spiele und Visualisierungen, die die Multimediafähigkeit von Windows XP ausschöpfen und erweitern. Zu den Highlights zählen das Tool Plus! Voice Command, mit dem sich der Windows Media Player per Sprache steuern läßt, und das Tool Plus! Speaker Enhancement, das die Klangqualität vieler Computerlautsprecher deutlich verbessert. Daneben umfaßt das Paket den Plus! Label Maker, mit dem Musikliebhaber eigene CD-Cover gestalten und produzieren können.

...Intelligente Karten

Für PC und Notebook: Netgear kündigte die Verfügbarkeit der autosensing-fähigen PCMCIA Adapter Card FA411 und der CardBus PC Card FA511 für den 10/100 Mbps-Bereich an. Die FA411 erlaubt das Vernetzen von Notebooks, ermittelt automatisch die Netzwerkgeschwindigkeit und benötigt keine weitere Hardware. Ethernet- und Fast-Ethernet-Verbindungen mit 10/100 MBit/s unterstützt auch die FA511. Sie erkennt die Durchsatzraten eines angeschlossenen Hubs oder Switch und stellt sich automatisch auf die höchstmögliche Geschwindigkeit und Duplexbetriebsart ein. Darüber hinaus unterstützt sie Hot-Swap. Mit einem kompakten Design, einfachem Plug ´n Play-Anschluß und 32-Bit-Durchsatz können Anwender die Möglichkeiten der neuesten Notebook-PCs nutzen und mit anspruchsvollen Applikationen und fortschrittlichen Desktop-Technologien Schritt halten.

...Speech Processing

Sprach-Schnittstellen: ELSA und die Philips Speech Processing, führend in der Sprachverarbeitung und Spracherkennung, gaben eine strategische Kooperation bekannt. Ziel ist die gemeinsame Entwicklung von Sprachsteuerungs-Schnittstellen für den Automotive- und Consumer-Markt. Geplant sind Lösungen für Freisprecheinrichtungen, sprachgesteuerte Car-Enter-

tainment-Lösungen, Anwendungen im Bereich Home-Entertainment sowie Lösungen für die Haustechnik und spezielle Steuerungsinstrumente. Während Philips Speech Processing durch die Abteilung Voice Control das notwendige Know-how in integrierter Spracherkennung mit dem hauseigenen Voice Command & Control Softwarepaket - genannt VoConTM - einbringt, wird ELSA in erster Linie seine Kompetenz im Bereich WiFi, Bluetooth und Ethernet-basierte Netzwerke bei der gemeinsamen Entwicklung eines User Interfaces einsetzen. Beide Unternehmen sehen in der Integration von Sprache den entscheidenden Faktor für zukünftige Bedienungsschnittstellen, da Sprache der komfortabelste und - im Automotive-Bereich - auch der sicherste und natürlichste Weg sei, elektronische Geräte mit sich ständig erweiternder Funktionalität effizient zu bedienen.

...Communications

Plattform für Fax-, Voice- und Email: Mit der neuen 3Com NBX Unified Communications Software erhalten Geschäftskunden jetzt einen universellen Nachrichten-Zugang. Sie ermöglicht von herkömmlichen Telefon-Geräten, Web Clients oder PCs aus den Zugriff auf Fax-, Voice- und Email-Nachrichten, von nahezu jedem Kommunikationsmedium aus. Mit der eingebauten Spracherkennung und der Umwandlung von Text in Sprache kann der Anwender Voice- und E-Mails sowie Faxnachrichten anhören und beantworten. Ihre vielfältigen Software-Funktionen für Unified Communications machen die LAN-Telefonie von 3Com zu einer der umfangreichsten Kommunikations-Plattformen. Dabei ist die NBX Software auf die Bedürfnisse des einzelnen Kunden abstimmbar. Die IP PBX-Technologie von 3Com ist universell einsetzbar und unterstützt unter anderem eine vielseitige Medienführung, einfache Verwaltung sowie einen individuellen System-Einsatz wie Spracherkennungsdienste für die Steuerung von "Auto Attendant"-Menüs, integrierte Voice-, Fax- und Email-Nachrichtenspeicher mit benutzerdefinierten Mailbox-Einstellungen oder die Integration und Synchronisation mit Microsoft Outlook und Lotus Notes Multimedia Client mit CTI-Links.

...Gigabit Ethernet

Kupfer- und Glasfaser-Adapter: Allied Telesyn hat eine neue Produktreihe von flexiblen, zuverlässigen, High-Performance-Netzwerkkomponenten vorgestellt, die Gigabit Ethernet Adapter Cards der Serie AT-2930. Diese 10/100/1000 PCI Server-Adapter wurden entwickelt, um die Möglichkeiten von High Bandwidth Servern und Switch-Anbindungen, wie sie in hochentwickelten Netzwerkumgebungen gebräuchlich sind, zu unterstützen. Die hohe Geschwindigkeit der Serie AT-2930 kann das Ansprechverhalten von Anwendungen, die Server-Zuverlässigkeit und die Netzwerk-Skalierbarkeit schnell und preiswert verbessern. Die Serie AT-2930 ist für Kupfer- und Glasfasernetzwerke ausgelegt und ermöglicht sofortige Performance-Steigerungen. Die AT-2930T erfüllt die Anforderungen an das kostengünstigste Upgrade eines bestehenden Kupfer-LAN Backbones. Für Netzwerke, die mittels Glasfaser größere Entfernungen überwinden sollen, bietet die AT-2930SX eine Gigabit-Connectivity bis zu einer Distanz von 2 km.

...Cyber Cop

Network Risk Assessment: PGP Security, ein Geschäftsbereich von Network Associates, präsentierte mit dem neuen Distributed CyberCop Scanner, Version 2.0, das erste Tool zur Risikobewertung von Netzwerken, welches sich auch für Ferninstallationen und Management in verschiedenen Segmenten eignet. CyberCop Scanner 2.0 erlaubt Unternehmen die Kontrolle von geografisch verstreuten Netzwerken. Der Scanner deckt potenzielle Bedrohungen und Sicherheitslöcher auf, bevor Hacker oder Würmer diese ausnutzen können. Zusammen mit dem integrierten McAfee ePolicy Orchestrator (ePO) kontrolliert und prüft der CyberCop Scanner 2.0 die Netzwerke regelmäßig oder bei aktuellem Bedarf auf über 850 verschiedene Bedrohungsszenarien. Die Ergebnisse werden zentral gespeichert. Der Systemadministrator kann den CyberCop Scanner bequem über eine einzige Konsole steuern.

...Smart

Batterie-Management: In der Reihe ihrer Produktfamilie Smart UPS hat APC zwei neue Unterbrechungsfreie Stromversorgungen mit einer Leistung von 1000 VA und 1500 VA herausgebracht. American Power Conversion hat die beiden Geräte mit einem intelligenten Batterie-Management für längere Akku-Lebensdauer ausgestattet. Die beiden Smart UPS 1000 und 1500 verfügen als Standgeräte über acht Ports und lassen sich über die serielle Schnittstelle oder Universal Serial Bus anschließen. Über einen Erweiterungssteckplatz können Boards zur Überprüfung von Umgebungsbedingungen oder zur Netzintegration mittels SNMP oder Telnet nachgerüstet werden. Zum Lieferumfang gehört die APC-eigene Management-Software Powerchute plus, mit der Diagnosen und Einstellungen vorgenommen und die Server bei längeren Stromausfällen automatisch heruntergefahren werden können.

KABELLOS!

Wireless LAN

Drahtlose Technik im Detail

Von Jörg Rech

Wireless LANs schaffen mehr Freiheit, Flexibilität und Mobilität. Es liegt was in der Luft, denn kabellose Netze offenbaren neue Dimensionen in der Vernetzung von Gebäuden, Abteilungen und Mitarbeitern. Ihr Hauptvorteil ist ihre einfache Installation, weil sie sich schnell und ohne Verkabelungsaufwand konfektionieren lassen.

Drahtlose Systeme sind schnell zu installieren, und sie ermöglichen im Handumdrehen den Datenaustausch zwischen den angeschlossenen Wireless Komponenten und den Zugang zum kabelgebundenen Netzwerk. Sie eignen sich hervorragend für eine zeitlich begrenzte Vernetzung, etwa auf Messen, Kongressen oder Workshops. In denkmalgeschützten Gebäuden mit entsprechenden Auflagen dürften sie sogar die einzig praktikable LAN-Technik darstellen. Wir wollen zeigen, wie Wireless LANs technisch umgesetzt sind. Vom Prinzip her stellt die Wireless LAN eine Netzwerktechnologie dar, die sich durch einfachen Aufbau und Implementierung innerhalb eines Netzwerks auszeichnet. Für den richtigen Einsatz eines Wireless LAN´s sollte jedoch ein Netzwerkadministrator nicht nur die verschiedenen Wireless-Komponenten und Netzwerkformen des Wireless LAN's kennen, sondern auch die Funktionsunterschiede zwischen einem drahtlosen und einem drahtgebundenen Netzwerk.

Feinheiten

Oftmals wird einfach behauptet, daß es sich bei Wireless LANs um eine erweiterte Variante des Ethernets handelt. Vergleicht man jedoch die physikalischen Eigenschaften der verwendeten Übertragungsmedien, so stellt man schnell fest, daß ein drahtloses LAN mehr sein muß als ein in die Luft geführtes Ethernet. Alleine durch die Tatsache, daß ein Funkmedium weitaus größeren Störeinflüssen als ein drahtgebundenes Übertragungsmedium unterliegt, müssen beim Wireless LAN technische Finessen greifen, damit diese Einflüsse kompensiert werden können und ein fehlerfreier Datenaustausch gewährleistet werden kann. Des weiteren kann theoretisch jeder, der sich innerhalb der Reichweite eines Wireless LAN´s befindet, auf das genutzte Frequenzband zugreifen oder die Daten abhören. Entsprechende Verfahren müssen deshalb dafür sorgen, daß eine Abgrenzung zwischen unterschiedlichen Systemen gewährleistet wird, ein gerechter Zugriff auf das verwendet Frequenzband sichergestellt ist, und daß die übertragenen Daten nur für autorisierte Teilnehmer zugänglich sind.

Ad hoc

Grundsätzlich gibt es verschiedene Möglichkeiten, ein Wireless LAN aufzubauen. Für den Aufbau eines einfachen Wireless LAN´s reichen vom Prinzip her ein paar Wireless-Netzwerkadapter aus. Die einfachste Form besteht aus zwei Rechnern, in die jeweils ein entsprechender Funkadapter eingebaut ist, die sich innerhalb der Rechnerreichweite befinden und auf demselben Kanal arbeiten. Eine Erweiterung dieser Konstellation ist problemlos möglich, indem ein weiterer Rechner mit Wireless-Netzwerkadaptern innerhalb der Reichweite der beiden anderen Systeme gebracht wird. Das Wireless LAN stellt dabei eine zellulare Struktur dar, bei der jeder Netzwerkadapter eine sogenannte Zelle bildet. Die Rechner, deren Zellen sich überlappen, können alle miteinander kommunizieren und Daten austauschen. In etwa deckt eine Zelle eine ovale Fläche ab, innerhalb der die befindlichen Rechner untereinander Daten austauschen können. Logisch betrachtet bilden die Rechner, die sich innerhalb einer Reichweite befinden, eine gemeinsame Zelle. In der IEEE-Nomenklatur wird die Zelle als Basic Service Set (BSS) bezeichnet. Da die Zelle für sich alleine steht, wird diese Grundform des Wireless LAN´s als Independent Basic Service Set, kurz IBSS oder Ad hoc Netzwerk bezeichnet. Das Ad hoc Netzwerk zeichnet sich dadurch aus, daß für seinen Aufbau vom Prinzip her keinerlei Planung notwendig ist. Die Reichweite eines Ad Hoc Netzwerks ist jedoch auf zirka 30 bis 50 m innerhalb von Gebäuden, außerhalb von Gebäuden auf etwa 300 m und außerdem auf eine geringe Anzahl von Rechnern begrenzt.

Infrastrukturnetzwerk

Neben dieser einfachen Konstellation des Ad hoc Netzwerks gibt es laut IEEE-Standard komplexere Strukturen, die theoretisch unbegrenzt ausgedehnt werden können und eine flächendeckende Versorgung ermöglichen. Um eine solche zu erzielen, können auf die zu versorgende Fläche mehrere BSS plaziert werden, die über ein Verteilungssystem, das als Distribution System, kurz DS, bezeichnet

Abb. 1: Die einfachste Form eines Wireless LAN´s ist das Ad hoc Netzwerk. (Bildquelle: ELSA)

Avaya Wireless

Für den In- und Outdoor-Einsatz

AVAYA bietet mit Ihrer Wireless Reihe ein komplettes Portfolio für die Einrichtung breitbandiger Funkinfrastrukturen im Innen- und Außenbereich, mit dem sich die lokalen Netzwerke mehrerer Gebäude miteinander vernetzen lassen. Die Produkte sorgen für eine schnelle und preiswerte Funkverbindung zu den installierten Datennetzen in Gebäuden oder dem Campus.

Wireless Outdoor Produkte
Im Outdoorbereich können mit Hilfe der AVAYA Wireless Outdoor Router-Familie komplette Standorte über große Distanzen via Funk verbunden werden. Die Outdoor Router ermöglichen entweder Punkt-zu-Punkt- bzw. -Multipunkt-Konstellationen und werden im Service Provider Umfeld sowie zur Anbindung von Außenstellen im Enterprise Bereich eingesetzt. Ein hohes Wachstumspotential liegt im Public Access zur Versorgung von öffentlichen Plätzen in Messezentren, Flughäfen oder Bahnhöfen.

Mehrstufiges Sicherheitssystem
AVAYA bietet neben Netzwerkkarten sowie den AP-I und AP-II Access Point Bridges eine komplette Reihe von WLAN Produkten für den Innen- und Außenbereich. AVAYA Wireless ist ein modulares, funkbasiertes Netzwerksystem, das Übertragungsraten von bis zu 11 Mbps bietet. Alle Komponenten entsprechen dem Standard IEEE 802.11b und sind mit dem Wi-Fi-Siegel der WECA zertifiziert. Interoperabilität mit Produkten anderer Herstellern ist rundum gewährleistet. Die AVAYA Wireless Produktlinie wird mit ihrem mehrstufigen Sicherheitssystem selbst hohen Sicherheitsanforderungen gerecht. Neben der 40- oder 128-Bit-Verschlüsselung können auf dem Access Point Zugangstabellen geführt werden. Diese stellen sicher, daß nur autorisierte Nutzer Zugriff auf das Funknetz erhalten. Zusätzlich erschwert das DSSS-Verfahren das Abhören der Daten über einen herkömmlichen Breitbandempfänger.

Minimale Implementierungsdauer
Mit AVAYA Wireless steht eine preiswerte Alternative zu 10Base-T Hubs zur Verfügung. Der Einsatz der WLAN-Technologie minimiert nicht nur die Implementierungsdauer, sondern vermeidet auch das Risiko einer Neuverkabelung bei Änderungen. Die Wireless Produkte von AVAYA bieten eine hohe Flexibilität. Neue Anwender lassen sich preiswert und schnell an das Unternehmensnetzwerk anbinden. Auch temporäre Arbeitsgruppen können sich ohne großen Aufwand immer wieder neu formieren. So erleichtern diese WLAN-Komponenten die Anpassung an spezifische Geschäftsprozesse im Unternehmen.

wird, verbunden werden. Das DS kann man sich in diesem Fall als eine Art Backbone vorstellen, über den der Datenaustausch zwischen den BSS erfolgt. Beim Aufbau eines DS kommt entweder ein drahtloses oder drahtgebundenes Übertragungsmedium zum Einsatz. Wird ein drahtloses Übertragungsmedium eingesetzt, so spricht man von einem Wireless Distribution System, kurz WDS. Als drahtgebundenes DS kommt in der Regel das Ethernet zum Einsatz. Werden mehrere BSS über ein DS miteinander verbunden, so spricht man von einem Extended Service Set, kurz ESS. Über sogenannte Access-Points wird der Datenaustausch zwischen den BSS und den DS realisiert, wobei pro Zelle ein Access-Point plaziert wird.

Mobilität

Die Access-Points werden beim Aufbau eines Wireless LAN´s so plaziert, daß die zu versorgende Fläche mit überlappenden Zellen bedeckt ist. Auf diese Weise wird es den Anwendern ermöglicht, sich mit ihren Rechnern innerhalb der versorgten Fläche von Zelle zu Zelle zu bewegen, ohne daß die Kommunikation zum Netzwerk abbricht. Durch die Plazierung von Access-Points läßt sich nicht nur die Ausdehnung des Wireless LAN´s erhöhen, sondern auch der Access-Point kann einen Kommunikationsweg zum drahtgebundenen LAN bilden. Auf diese Weise können Ressourcen eines drahtgebundenen Netzwerks, wie Print-Server, Datenbank-Server oder der breitbandige DSL-Zugang innerhalb des Wireless LAN´s genutzt werden.
Werden mehrere Zellen über Access-Points und einen DS miteinander verbunden, so spricht man von dem oben genannten Infrastrukturnetzwerk. Hierbei ist es gleich, ob nur ein Access-Point eine Verbindung zum bestehenden drahtgebundenen Netzwerk schafft, oder mehrere Access-Points über ein DS miteinander verbunden

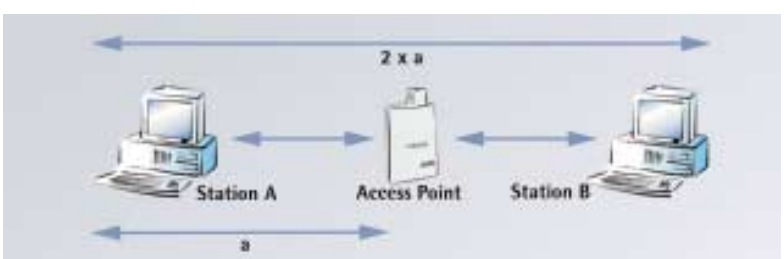
sind und das Wireless LAN für sich alleine steht. Betrachtet man eine Zelle für sich, so kann über die Plazierung eines Access-Points die Ausdehnung der Zelle verdoppelt werden, falls dieser im Zentrum der Zelle steht (siehe Abb. 3).

Standardkonform

Die Idee, eine Netzwerkkommunikation über das Funkmedium zu realisieren, ist eigentlich ein alter Hut. In den Anfängen der Wireless-Ära gab es eine Vielzahl von proprietären Lösungen auf dem Markt. Um jedoch eine breite Akzeptanz dieser Technik durchzusetzen, war ein standardisiertes Verfahren notwendig, das die Interoperabilität zwischen Systemen unterschiedlicher Hersteller sicherstellt. Dieser Aufgabe widmete sich das Institute of Electrical and Electronics Engineers (IEEE). Nachdem eine eigene Arbeitsgruppe gebildet war, wurde im Jahr 1997 der Wireless LAN-Standard 802.11 verabschiedet. Er definierte einen MAC-Layer und drei PHY-Layer, die eine Datenrate von 1 und 2 Mbps zuließen. Der MAC-Layer beinhaltet im wesentlichen das Zugriffsverfahren, Fehlerkorrekturmechanismen und eine Verschlüsselungsmethode, die auf die Bedürfnisse des drahtlosen Mediums zugeschnitten wurden. Auf der PHY-Ebene wurden zwei Verfahren für die Datenübertragung über elektromagnetische Wellen und ein Verfahren für die optische Übertragung im Infrarotbereich implementiert. Bei den Lösungen für die Funkübertragung auf der Basis von elektromagnetischen Wellen kam entweder die FHSS-Technologie (Frequency Hopping Spread Spectrum) oder DSSS-Technologie (Direct Sequence Spread Spectrum) zum Einsatz. Beide Technologien wurden für die Nutzung des 2,4-GHz-Band implementiert. Bei der Lösung im Infrarotbereich wurden die Datenübertragung mittels Licht im Wellenlängenbereich von 850 bis 950 nm definiert, wobei die Information über die sogenannte Pulse Position Modulation (PPM) moduliert wird. Bedingt durch die Tatsache, daß die IR-Lösung nur geringe Reichweiten zuließ und eine Sichtverbindung erforderte, wurde diese Lösung in der Praxis jedoch nie um gesetzt.

Abb.2: Über Access-Points läßt sich ein Infrastrukturnetzwerk aufbauen und das Wireless LAN beliebig ausdehnen (Bildquelle: ELSA).

Abb. 3: Durch die Plazierung eines Access-Points kann die Ausdehnung einer Zelle verdoppelt werden.



IEEE-802.11a, b und h

Im Jahr 1999 erfuhr der Wireless LAN-Standard mit der Verabschiedung des IEEE-802.11a und IEEE-802.11b Standards gleich zwei Erweiterungen, die letztendlich die Realisierung einer höheren Datenrate boten. Der Standard IEEE-802.11a definiert Datenraten von 6, 9, 12, 18, 24, 36 und 54 Mbps im 5-GHz-Band. Anstelle der FHSS- oder DSSS-Technologie wurde hierbei die OFDM-Technologie (Ortogonal Frequency Division Multiplexing) angewendet, um die höheren Datenraten technisch zu realisieren. Derzeit ist jedoch in Europa die Nutzung des 5-GHz-Band für den lizenzfreien Betrieb noch nicht freigegeben. Voraussichtlich wird die Freigabe durch das ETSI Anfang bis

3Com Richtfunklösung

WLAN-Anbindung bis zu 4100 Metern

Mit der Verfügbarkeit ihrer 11 Mbps Wireless Building-to-Building Bridge bringt 3Com inzwischen auch eine kostengünstige Richtfunklösung auf den Markt. Für Unternehmen jeder Größenordnung, deren Augenmerk auf schneller Netzanbindung, einfacher Handhabung und umfassender Funktionalität liegt, ergänzt die 3Com 11 Mbps Wireless Building-to-Building Bridge die umfangreiche 3Com Wireless LAN-Produktfamilie um eine weitere flexible Lösung, ob im Bildungsbereich oder im Gesundheitswesen, ob in Fertigungsumgebungen oder auf Flugplätzen.

Gebäudeverbindungen
Die neue 3Com Bridge ermöglicht die schnelle und kosteneffektive Integration von temporären Netzen, schwierig zu verkabelnden Bauten oder mehreren Gebäuden auf einem Firmengelände. Die Lösung soll dabei nur etwa halb so viel kosten wie existierende Wettbewerbsprodukte. Mit Verbindungen von Punkt zu Punkt oder von einem zu mehreren Punkten ermöglicht die Building-to-Building Bridge den Datentransfer nach dem IEEE 802.11b Standard zwischen zwei oder mehreren Gebäuden gleichzeitig. Mit omnidirektionalen Antennen werden Übertragungsdistanzen von bis zu 1300 Metern, mit direktionalen Antennen von bis zu 4100 Metern erreicht.

Flexibilität und Leistung
Die 3Com 11 Mbps Wireless Building-to-Building Bridge unterstützt sowohl 40bit als auch 128bit WEP-Verschlüsselung. Bei Verwendung von VPN-Protokollen verhält sich die Wireless Bridge transparent. Ein spezielles Encapsulation-Verfahren verhindert dabei Konflikte mit anderen Tunneling-Protokollen. Das Management ist sehr einfach von zentraler Stelle im LAN oder via Internet möglich. Im Lieferumfang der Building-to-Building Bridge sind Antennen und Kabel aufgrund der individuell verschiedenen Anforderungen jedoch nicht inbegriffen.

Breite Palette
3Com bietet eine breite Palette drahtloser Netzwerklösungen. Die WLAN-Produkte entsprechen dem IEEE 802.11 High Rate Standard und sind Wi-Fi zertifiziert. Jeder Access Point unterstützt 63 Funk-Clients gleichzeitig und verfügt über eine Reichweite von rund 100 Metern in Standardumgebungen. Um Funkstörungen auszugleichen, regelt das Dynamic Rate Shifting eine automatische Übertragungsanpassung von 1, 2, 5.5 oder 11 Mbps. Automatic Load Balancing sorgt für optimale Performance, indem es den Datenstrom auf mehrere Access-Points verteilt. Als Sicherheitsbarriere können beim Access Point MAC-Adressen gesperrt werden. Alle Sicherheitsprotokolle, die über Ethernet laufen, sind auch hier möglich, ob IPSec, SSL, DES, 3DES und Anmeldungen an NT-Domänen. Neu ist die Authentifizierung am Radius Server, an den die Access Points über den 3Com Router 400 die relevanten Informationen weitergeben. Dieser gibt dann den Zugriff auf das Netzwerk frei.

Mitte 2002 erteilt werden, wobei noch abzuwarten bleibt, welche Anforderungen sich bezüglich der Aufteilung des Frequenzbandes in Unterbänder oder der maximal zulässigen Sendeleistung ergeben. Bedingt durch diese Tatsache, lassen die Produkte laut IEEE 802.11a bei uns noch auf sich warten.
Derzeitig arbeitet die IEEE 802.11h Gruppe an einer verbesserten Handhabung des laut IEEE 802.11a definierten 5-GHz-Bandes und einer Reduzierung der genutzten Sendeleistung, damit die europäischen Richtlinien erfüllt werden können.
Anders sieht es beim IEEE-802.11b Standard aus, denn hier wurde weiterhin das 2,4-GHz-Band zugrunde gelegt. Durch IEEE-802.11b wurde bei der Nutzung der DSSS-Technologie eine Datenrate von 5,5 und 11 Mbps ermöglicht. In der Regel entsprechen die heutigen Wireless LAN-Produkte dem IEEE 802.11 und 802.11b Standard und unterstützen die Datenraten von 1, 2, 5.5 und 11 Mbps/s.

Frequenzbänder

Der standardkonforme Einsatz von funkbasierten Wireless LANs erfolgt heutzutage im 2,4-GHz-ISM-Band. Bei dem 2,4-GHz-ISM-Band spricht man von ISM-Band (Industrial/ Scientifical/Medical), wobei es sich um ein Frequenzband von 2,4 bis 2,5 GHz handelt, das international für einen gebühren- und genehmigungsfreien Betrieb für industrielle, wissenschaftliche und medizinische Anwendungen lizenzfrei genutzt werden darf. Für den Betrieb eines Wireless LAN´s ist innerhalb des ISM-Bands der Bereich von 2,4 bis 2,4835 GHz vorbehalten. Dieser wird von nationalen Regulierungsbehörden in bestimmte Unterbänder unterteilt, die von Nation zu Nation variieren können. Innerhalb Europas ist das europäische Standardisierungsinstitut für Telekommunikationsangelegenheiten ETSI - das European Telecommuni-

cations Standards Institute - für die Unterteilung des Frequenzbandes zuständig. ETSI hat eine entsprechende Norm veröffentlicht, die sogenannte ETS 300 328 Norm, in der die technischen Voraussetzungen und Zulassungskriterien für Datenfunksysteme im entsprechenden Frequenzband und die Aufteilung in Unterbänder festgelegt wird. Um eine Zulassung für Wireless LAN-Produkte zu erhalten, muß ein Hersteller die Einhaltung der in ETS 300 328 vorgeschriebenen Kriterien durch ein Zeugnis eines unabhängigen und zugelassenen Testlabors oder des Bundesamtes für Post und Telekommunikation (BAPT) nachweisen.

Rechtlich frei

Für den Bereich der Bundesrepublik Deutschland wurde mit der Verfügung 122 im Amtsblatt 14/1997 des Bundesministeriums für Post und Telekommunikation (BMPT) der Betrieb von drahtlosen Datenfunkanlagen ab dem 21. 5. 1997 grundsätzlich neu geregelt. Wireless LANs gelten demnach als nicht öffentliche Einrichtungen, die eingesetzten Systeme müssen lediglich der ETS 300 328 Norm entsprechen. Ist dies gewährleistet, so dürfen die entsprechenden Produkte im Frequenzbereich 2,4 bis 2,4835 GHz ohne weitere Zulassung und auch ohne weitere Gebühren innerhalb der Grundstücksgrenzen betrieben werden. Auf eine formlose schriftliche Mitteilung an das BAPT hin wird eine neu installierte Funkstrecke für die BRD zentral registriert. Kosten entstehen dem Betreiber bei Nutzung des Frequenzbandes von 2,4 bis 2,4835 GHz in diesem Fall nicht.

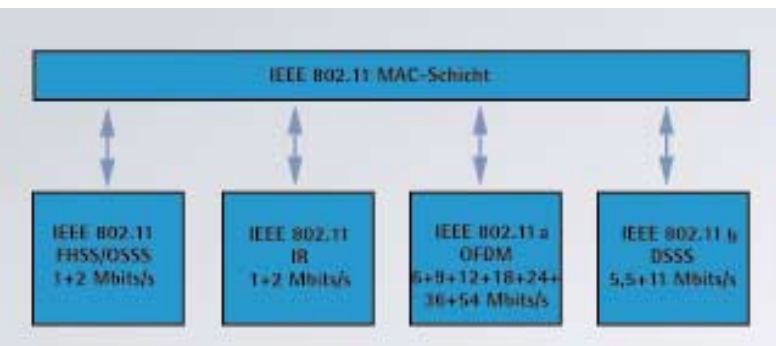
HINWEIS:

Bei einer grundstücksübergreifenden Datenübertragung ist zu beachten, daß zuvor eine formlose und schriftliche Mitteilung an das Referat 122 des BAPTs (Fax: 06131-18-5616, Tel –1229) zu richten ist.

PHY-Schicht

Die Wireless LAN PHY-Schicht ist laut IEEE 802.11 in zwei Teilschichten unterteilt. Die obere wird als Convergence Procedure (PLCP) bezeichnet. Der PLCP stellt eine einheitliche Schnittstelle zwischen der MAC-Schicht und allen darunterliegenden medienabhängigen Schichten dar, die als Physical Medium Dependent, kurz PMD, bezeichnet werden. Der PLCP beschreibt Methoden, um die von der MAC-Schicht übergebenen Daten in ein übertragbares Format zu bringen und die Managementinformationen zwischen der MAC-Schicht und den PMDs auszutauschen. Die einzelnen PMDs für FHSS, DSSS und Infrarot bringen die Daten wiederum in ein für die jeweils angewendete Übertra-gungstechnik geeignetes Format, damit diese über das drahtlose Medium übertragen werden können. Des weiteren stellen die PMDs das Interface zum Übertragungsmedium in Form einer Sende- und Empfangs-Hardware bereit, über das der Datenaustausch zu einem oder mehreren Verbindungspartnern ermöglicht wird. Die Sende- und Empfangs-Hardware ist unter anderem für die Modulation bzw. Demodulation der zu übertragenden Daten zuständig.

Abb. 4: Der Wireless LAN-Standard ist in verschiedene Teilbereiche unterteilt, bei denen unterschiedliche Techniken zum Einsatz kommen und verschiedene Datenraten realisiert werden.



FHSS

Bei der FHSS-Technologie mit Frequency Hopping Spread Spectrum wird das vorhandene Frequenzband in 79 Frequenzunterbänder mit einer Bandbreite von je 1 MHz aufgeteilt. Jedes der 79 Frequenzbänder stellt einen Kanal bereit, der von den Systemen im regelmäßigem Wechsel verwendet wird. Über eine sogenannte Hopping-Sequenz wird festgelegt, wie Sender und Empfänger eines Systems während der Übertragung gleichzeitig zwischen den vorhandenen Kanälen springen. Die Zeitspanne, die die zusammenhängenden Systeme auf einem Kanal verbleiben, sowie der Abstand zwischen zwei nacheinander verwendeten Kanälen ist durch die ETSI festgelegt. Innerhalb Europas darf ein Kanal von den Systemen maximal 400 ms belegt werden, der Abstand zwischen den zwei nacheinander verwendeten Kanälen muß mindestens 6 MHz betragen. Diese Festlegung führt dazu, daß die Systeme 2,5 Kanalwechsel pro Sekunde durchführen müssen. In welcher Reihenfolge die 79 Kanäle genutzt werden wird

XAir Multi

BinTec erweitert die XAir-Palette

Neben ihren etablierten WLAN-Geräten XAir Basic und XAir Professional bietet BinTec mit XAir Multi einen Access Point, bei dem zwei Kanäle auf externe Antennenanschlüsse geführt sind. Beide sind getrennt konfigurierbar, entweder als Access-Point zum kabellosen Anschluß von PCs und Druckern in einer größeren Funkzelle oder als Bridge.

Drahtlos-Szenarien
Mit XAir Multi sind verschieden Szenarien möglich. Dienen beide Kanäle als Access-Point, erfolgt der Anschluß des LANs via Kabel, die Clients - ob PCs, Laptops und Drucker - werden kabellos angeschlossen. Mit den Dipol-Antennen läßt sich eine räumlich große Funkzelle erreichen. Die zwei Kanäle verdoppeln die Anzahl der möglichen Clients, die mit einem Access-Point erreicht werden können.
Ist ein Kanal als Access-Point und einer als Bridge vorgesehen, so erfolgt der LAN-Anschluß der Bridge per Funk. Mit dem Access-Point können hierbei die Clients in einer räumlich großen Funkzelle erreicht werden, etwa um Abteilungen drahtlos an das Firmennetz anzubinden.
Dienen beide Kanäle als 11 MBit/s Bridge, arbeitet die XAir als Relaisstation. Dies bedeutet, daß die Reichweite mit den entsprechenden Antennen verdoppelt werden kann bzw. störende Objekte in der Sichtverbindung umgangen werden können.

XAir Bridge mit 22 Mbps
Ergänzend zur XAir Bridge 11 MBit/s kann jetzt auch die 22 MBit/s Variante angeboten werden. Diese bietet den doppelten Datendurchsatz und ist damit als WLAN Backbone prädestiniert. Die Reichweite bei voller Geschwindigkeit beträgt dabei bis zu 5 km. Hierzu ist aber eine freie Sicht notwendig. Diese High Speed Bridge ist in zwei Versionen erhältlich, als XAir Bridge Set 22 Mpbs Short Range mit einer Reichweite bis 700 m und als Long Range Variante bis zu 5 km. Die Sets werden mit allem benötigten Zubehör ausgeliefert. Hierzu gehören die Kabel, die Antennen und die Access-Points. Damit kann die Bridge in kürzester Zeit eingerichtet werden. Diese Bridge-Lösung ist besonders geeignet, wenn ein hoher Datendurchsatz erforderlich ist. Um dies zu erreichen, werden die beiden vorhandenen Kanäle gebündelt. Dadurch kann eine Bruttodatenrate von 22 MBit/s erreicht werden.

IPSec Lösungen
Für die Datensicherheit sorgt eine 128-Bit Verschlüsselung im WEP Standard. Wem dies nicht genügt, der kann zusätzlich noch die bei BinTec erhältliche IPSec-Lösung einsetzen. Hierzu gibt es verschiedene Varianten von IPSec-Gateways und IPSec-Clients, die die Funkstrecke absolut sicher machen.

über die 79-stellige Hopping-Sequenz festgelegt. Die Hopping-Sequenz kann man somit als ein Hüpfmuster bezeichnen, das die Reihenfolge der Kanalbelegung festlegt.

Grenzen

Zusammenhängende Systeme, die untereinander Daten austauschen sollen, müssen dieselbe Hopping-Sequenz verwenden. Unterschiedliche Systeme verwenden unterschiedliche Hopping-Sequenzen, damit eine Abgrenzung untereinander gewährleistet ist und ein unabhängiger und störungsfreier Betrieb innerhalb eines Empfangsbereiches ermöglicht wird. Werden innerhalb eines Empfangsbereiches unterschiedliche Systeme betrieben, ist es dennoch möglich, daß zufällig zwei Sender zur gleichen Zeit den gleichen Kanal belegen und somit eine Kollision auftritt, die zum Verlust der Daten führt. Doch tritt dies eher selten auf. Bei Kollisionen wird der Datenverlust durch ein wiederholtes Aussenden des kollidierten Frames ausgeglichen.
Damit nun allgemein ein möglichst kollisionsfreier Betrieb gewährleistet werden kann, sind die Hopping-Sequenzen in drei verschiedene Hopping-Sets unterteilt, wobei die angrenzenden Systeme nach Möglichkeit eine Hopping-Sequenz aus einem anderem Hopping-Set verwenden sollen. Durch die Nutzung unterschiedlicher Sequenzen können bis zu 13 unabhängige FHSS-Systeme innerhalb eines Empfangsbereiches arbeiten, ohne daß der Datendurchsatz durch eine Anhäufung von auftretenden Kollisionen merklich reduziert wird.

Modulationsverfahren

Als Modulationsverfahren kommt bei den FHSS-Systemen die Frequenzmodulation zum Einsatz. Dabei wird vom Sender die Frequenz der elektromagnetischen Welle verändert, um

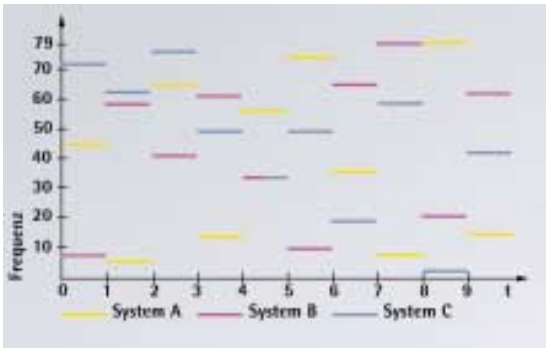


Abb. 5: FHSS-Systeme springen alle 400 ms zwischen unterschiedlichen Kanälen.

dem Empfänger die zu übertragenden Informationen darzustellen. Je nach verwendeter Datenrate von 1 oder 2 Mbps wird entweder die 2GFSK-Modulation - mit 2-Level Gaussian Frequency Shift Keying - oder die 4GFSK-Modulation mit entsprechend 4 Levels angewendet. Bei den FHSS-Systemen werden die Nutzdaten, unabhängig von der verwendeten Datenrate, mit 1 MSymbol pro Sekunde übertragen.

Bei einer Datenrate von 1 Mbps wird die 2GFSK-Modulation verwendet, wobei ein Symbol eine Länge von einem Bit hat. Da pro Zeiteinheit 1 MSymbol übertragen wird, kommt man auf eine Datenrate von 1Mbps: 1MSymbol/s * 1Bit/Symbol. Die beiden möglichen Symbole werden bei dem 2GFSK-Systemen, wie in Tabelle 1 dargestellt, übertragen. Bei einer Datenrate von 2 Mbps wird die 4GFSK-Modulation angewendet, wobei ein Symbol eine Länge von zwei Bits hat, die pro Zeiteinheit übertragen werden. Deshalb kommt man auf eine Datenrate von 2Mbps: 1MSymbol/s * 2Bit/Symbol (vgl. Tabelle 2).

Vor- und Nachteile

Der wesentliche Vorteil, der sich aus der Nutzung der GFSK Modulation ergibt, liegt darin, daß diese Signalübertragung relativ unempfindlich gegenüber Störeinflüssen ist. Denn diese beeinflussen in der Regel die Amplitude des Signals und nicht die Frequenz der elektromagnetischen Welle, weshalb die Nutzinformation bei Störeinflüssen nicht verloren geht.

Ein wesentlicher Nachteil bei den FHSS-Systemen ist, daß die erzielbare Datenrate auf 2 Mbps begrenzt ist. Denn wollte man die Datenrate steigern, so müßte man die Bandbreite der einzelnen Kanäle erhöhen. Dies würde wiederum dazu führen, daß bei einer vorhandenen Gesamtbandbreite die Anzahl der Kanäle reduziert werden würde. Und dies hätte wiederum beim Betrieb verschiedener Systeme zwangsläufig eine Anhäufung möglicher Kollisionen zur Folge und somit einen Verlust des erzielbaren Datendurchsatzes.

Des Weiteren ist das Roaming, das Wandern zwischen verschiedenen Zellen, bei FHSS-Systemen relativ aufwendig. Denn jeder der 79 Kanäle muß abgehört werden, um auf eine Zelle aufspringen zu können. Da ein gleichzeitiges Abhören aller Kanäle unmöglich ist, müssen alle Kanäle nacheinander abgehört werden, was eine lange Wartezeit in Anspruch nehmen kann und eine große Verzögerung beim Wechsel von einer zur anderen Zelle verursacht.

Einen Vorteil stellt die relativ einfache Implementierung eines FHSS-Systems dar, weshalb keine komplexen logischen Bausteine benötigt werden. Dadurch bedingt ist zum einen der Energieverbrauch relativ gering, und zum anderen sind die Kosten für die Erstellung von FHSS-Systemen verhältnismäßig niedrig.

Tabelle 1

Symbol	Center-Frequenz des Kanals
0	– 110KHz bis 160KHz
1	+ 110KHz bis 160KHz

Tabelle 1: Darstellung der Symbole bei der 2GFSK-Modulation

Tabelle 2

Symbol	Center-Frequenz des Kanals
00	– 202,5KHz bis 216KHz
01	– 67,5KHz bis 72KHz
10	+ 202,5KHz bis 216KHz
11	+ 67,5KHz bis 72KHz

Tabelle 2: Darstellung der Symbole bei der 4GFSK-Modulation

DSSS

Bei den Systemen mit Direct Sequence Spread Spectrum, die mit der Ausnahme von Frankreich und Spanien für den Einsatz innerhalb Europas bestimmt sind, wird die vorhandene Bandbreite des ISM-Bands in 13 Kanäle mit jeweils 22 MHz und 30 MHz Abstand zwischen den Kanälen aufgeteilt. Anders als bei den FHSS-Systemen sendet ein DSSS-Sender immer auf demselben Kanal, es findet also kein Kanalwechsel statt.

Cisco Aironet 350

Von Ende zu Ende drahtlos

Cisco Systems bietet mit der Aironet 350 Serie ihre neueste Produktreihe zur drahtlosen Vernetzung mittlerer und großer Unternehmen an. Sie folgt dem IEEE 802.11b Standard und ist die erste vollständige Ende-zu-Ende-Lösung für Wireless LANs. Das Portfolio für die mobile Vernetzung umfaßt Access Points, Bridges und Client Adapter und ist mit minimalem Management-Overhead von kleinen bis zu sehr großen WLAN-Installationen skalierbar.

Mit ihrer neuen Aironet 350 Serie erweitert Cisco ihre Internet Mobile Office Initiative für den einfachen, sicheren und zuverlässigen Internetzugang von zu Hause oder dem Arbeitsplatz aus. Die drahtlosen DSSS- Netzwerke zur mobilen Unternehmenskommunikation bieten flexiblen Netzzugang und Roaming. Mitarbeiter können sich frei bewegen und über eine sichere Verbindung mit 11 Mbps jederzeit auf Daten und Applikationen im Internet und im Intranet des Unternehmens zugreifen.

Security-Framework

Das Security-Framework zur drahtlosen Vernetzung mit der Reihe Cisco Aironet entspricht dem zukünftigen IEEE-802.1x Standard. Unternehmen können mit der Cisco Aironet 350 Serie zum ersten Mal drahtlose Netzsegmente auf Tausende von Anwendern skalieren und mit einem standardisierten und zentralen Security-Management verwalten. Spezielle RADIUS-Funktionen für die Unterstützung der neuen Security-Features der 350er Serie sind in den Cisco Secure Access Control Server (ACS) für Windows NT4 und 2000 v2.6 implementiert worden. Der ACS unterstützt die zentrale Authentifizierung der drahtlosen Aironet-Clients. Er ermöglicht die dynamische Verteilung von Schlüsseln, um jede Verbindung abzusichern und macht das Schlüssel-Management mit Wired Equivalent Privacy (WEP) überflüssig.

Erweiterte Funktionalitäten

Die neue Aironet 350 Serie verfügt über flexible Frequenzbereiche, Load-Balancing, Hot-Standby-Redundanz und Worldmode-Funktionalität. Durch neue Hardware-Features erhalten Wireless LANs nun eine höhere Performance. Um die maximale Reichweite zu erhalten, haben die Client Adapter, Access Points und Bridges eine einstellbare Übertragungsleistung von bis zu 100 Milliwatt. Dadurch kann ein optimaler Abdeckungsbereich eingestellt werden. Die Access Points arbeiten mit einer Inline-Stromversorgung über Ethernet. Sie ist mit dem IEEE-Standardentwurf 802.3a kompatibel und arbeitet mit Cisco-Switches der Serien Catalyst 3524-PWR, Catalyst 4006 und Catalyst 6x00 sowie dem Cisco Inline Power Patch Panel.

Unter der Anwendung der DSSS-Technologie werden die zu übertragenden Daten bei der Übertragung gespreizt. Die Signalspreizung führt dazu, daß im Gegensatz zum schmalbandigen Senden mit hoher Leistung nun über einen größeren Frequenzbereich mit geringerer Sendeleistung gearbeitet wird. Dies hat zur Folge, daß die Energie des ausgesendeten Signals unter dem Strich gleich bleibt. Eventuell schmalbandig auftretende Störeinflüsse können somit nur einen Teil der Information nachhaltig beeinträchtigen, während bei einer schmalbandigen Datenübertragung die komplette Information verloren ginge. Wie resistent die übertragenen Nutzdaten sind, hängt von der Länge des Codes ab, mit dem die Nutzdaten gespreizt werden. Je länger der Code, desto höher ist die Wahrscheinlichkeit, daß die Nutzdaten aus einem gestörten Signal wiedergewonnen werden können. Die Sendeleistung des breitbandigen Signals wird durch die Signalspreizung letztendlich unterhalb der Rauschgrenze gebracht, wodurch angrenzende Systeme weniger gestört werden und die Dichte unterschiedlicher Systeme, bezogen auf eine bestimmte Fläche, erhöht werden kann.

Pseudo Noise Code

Die Spreizung der Nutzdaten erreicht man durch einen Code, der als Pseudo Noise Code (PN-Code) bezeichnet wird. Die Abgrenzung unterschiedlicher Systeme erfolgt durch verschiedene PN-Codes. Sowohl Empfänger als auch Sender müssen denselben PN-Code verwenden, um untereinander Daten austauschen zu können. Weil das Nutzsignal durch die Spreizung im Grundrauschen verschwindet, können sich Systeme mit unterschiedlichen PN-Codes nicht verstehen oder gegenseitig stören. Der PN-Code wird aus einer Chipsequenz mit einer Länge von 2^{n-1} Chips gebildet und wird einfach Modulo-2 (Exklu-

siv-ODER) zum eigentlichen Binärstrom der Nutzdaten addiert. Die Generierung des PN-Codes erfolgt durch spezielle Schieberegister, deren Registeranzahl die Länge des PN-Codes bestimmt. Zum Entschlüsseln der empfangenen Daten wird das Signal vom Empfänger mit demselben PN-Code wieder Modulo-2 addiert. Durch die erneute Addition desselben PN-Codes ergeben sich die ursprünglichen Nutzdaten.

Modulationsverfahren

Bei den DSSS-Systemen kommt als Modulationsverfahren die Phasenmodulation zum Einsatz. Dabei wird zur Darstellung des zu übertragenden Symbols der elektromagnetischen Welle eine unterschiedliche Phase zugeordnet. Bei diesem Modulationsverfahren handelt es sich um die sogenannte Phase Shift Keying-Modulation, kurz PSK.

Je nachdem, welche Datenrate verwendet wird, werden von den DSSS-Systemen unterschiedliche PN-Codes und Varianten der PSK-Modulation genutzt, damit die unterschiedlichen Datenraten erzielt werden können. Bei einer Datenrate von 1 oder 2 Mbps wird für die Signalspreizung der 11-Chip Barker Code mit dem Inhalt 10110111000 angewendet. Werden die Daten mit 1 Mbps übertragen, so hat ein Symbol eine Länge von einem Bit und pro Zeiteinheit wird ein Bit übertragen. Die Datenrate errechnet sich in diesem Fall aus 1 Mbps = 1 MSymbol/s x 1 Bit/Symbol .

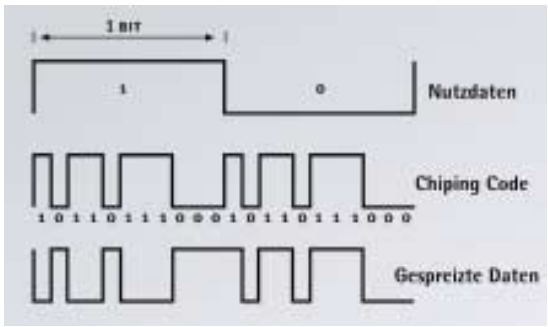


Abb. 6: Bei der DSSS-Technologie werden die Nutzdaten durch einen PN-Code gespreizt.

Bei dem 1Mbps-Betrieb wird für die Modulation die sogenannte Differential Binary Shift Keying Modulation (DBPSK) angewendet. DBPSK stellt eine spezielle Art der Binary Shift Keying Modulation dar, bei der als Bezugspunkt keine Referenzphase, sondern die zuletzt übertragene Phase verwendet wird (vgl. Tabelle 3). Bei einer Datenrate von 2 Mbps wird wiederum mit einer Symbollänge von zwei Bits gearbeitet, und pro Zeiteinheit werden zwei Bit übertragen. Auf diese Weise kommt man auf eine Datenrate von 2 MBit/s, die sich aus 1 MSymbol/s x 2 Bit/Symbol = 2 Mbps errechnen. Arbeiten die DSSS-Systeme mit einer Datenrate von 2 MBit/s, so wird als Modulationsverfahren die sogenannte Differential Quadrature Shift Keying Modulation (DQPSK) genutzt. Bei der DQPSK bestimmt ein Symbol mit der Länge von 2 Bit die Phasenverschiebung (vgl. Tabelle 4).

Complementary Code

Arbeiten die DSSS-Systeme mit einer Datenrate von 5,5 und 11 MBit/s, so wird anstelle des Chip Barker Code ein sogenannter Complementary Code verwendet, der über die sogenannte CCK-Technologie (Complementary Code Keying) gewonnen wird. Bei der Datenrate von 11 Mbps setzt die CCK-Technologie auf ein Codewort auf, das aus 64 komplexen Codewörtern über 6 von 8 Bit der zu übertragenden Nutzinformation ausgewählt wird. Die restlichen 2 Bit der zu übertragenden Nutzinformation werden für die QPSK-Modulation verwendet, über die wiederum das gesamte Symbol moduliert wird. Da man bei den DSSS-Systemen generell mit einer Chiprate von 11 MHz arbeitet, jedoch bei der Datenrate von 5,5 und 11 Mbps anstelle des 11-Bit langen PN-Codes mit 8 Bit langen Codes

Tabelle 3

Symbol (1 Bit)	Änderung der Phasenlage
0	0°
1	180°

Tabelle 3: Darstellung der Symbole bei DSSS-Systemen mit einer Datenrate von 1 MBit/s

Tabelle 4

Symbol (2 Bit)	Änderung der Phasenlage
00	0°
01	90°
10	270°
11	180°

Tabelle 4: Darstellung der Symbole bei DSSS-Systemen mit einer Datenrate von 2 MBit/s

ENTERASYS NETWORKS

Wireless Access Plattform

Sichere Wireless-Lösungen mit Roam About R2

Im Umfeld des Wireless Networking führt Enterasys Networks das User Personalized Network zukünftig neu ein. Es bietet dem Nutzer eines modernen Datennetzwerkes große Vorteile, da dieser immer seine persönliche Arbeitsumgebung vorfindet. Egal über welchen Access-Point oder welchen Switch-Port er sich an einem Netzwerk anmeldet, auf Basis des 802.1 X Standards erfolgt die Zuweisung der Profile und Policies an den jeweiligen Zugangsport und somit die Bereitstellung der nutzerbezogenen Arbeitsumgebung.

Zugangssicherheit
Durch Authentifizierung und anschließende Zuweisung der Nutzerprofile wird die Zugangssicherheit an einem Netz deutlich erhöht. Die neue Access Plattform, der Roam About R2, bietet viele Funktionen an, die das ehedem schon umfangreiche Produktportfolio von Enterasys Networks hervorragend ergänzen und komplettieren. Die Wireless Access Plattform Roam About R2 zeichnet sich durch ihren modularen Aufbau aus, durch den sie alle zukünftigen Wireless Technologien unterstützen kann. Es ist lediglich eine Neuinvestition in die gewünschte Tochterkarte erforderlich und schon ist der Schritt zu einem High Speed Wireless LAN vollzogen. Das bietet Kunden von Enterasys Networks eine hohe Investment Protection, da sie nach einer Investition in einen R2 auch zukünftig neue Wireless Technologien auf einfache Art implementieren können.

Wireless Access Modi
Die neue Access Plattform Roam About R2 unterstützt aus einer Firmware heraus verschiedene Wireless Modi, die einen universellen Einsatz gestatten. Möglich sind Client Betrieb, Point to Point Modus zur Anbindung von remote LANs über eine Wireless Strecke oder auch der Point to Multipoint Mode, wo zukünftig bis zu 100 Remote Lokationen über ein zentrales Gerät zeitgleich angebunden werden können. Herauszuheben ist die volle Kompatibilität zu allen Geräten nach dem Standard 802.11 b, so daß eine leichte Migration zu der Access Plattform Roam About R2 gegeben ist.

Optionen mit Zukunft
Durch den Einsatz der Enterasys Networks VPN Lösungen ist ein vollverschlüsselter, sicherer Betrieb eines Wireless LAN gegeben. Weitere unterstützte Funktionen sind: Telnet, Web Based Management, Management durch SNMP v3 Layer 3 Funktionen (zukünftig) und Quality of Service Funktionen. Hierdurch werden selbst Videoapplikationen im Wireless LAN ermöglicht.

Ein Beitrag von Andreas Richter,
Product Line Manager
Enterasys Networks Germany GmbH

arbeitet, ergibt sich bei diesen Datenraten eine Symbolrate von 1,375 MSymbolen/s (11/8). Die Datenrate von 5,5 Mbps gewinnt man über einen Complementary Code aus 4 Codewörtern mit je 8 Bit, wobei ein Symbol eine Länge von 4 Bits hat. Daraus läßt sich die Datenrate von 5,5 Mbps = 1,375 MSymbol/s * 4 Bit/Symbol errechnen. Bei der Datenrate von 11 Mbps wird der Complementary Code aus 64 Codewörtern mit einer Länge von je 8 Bit gewonnen, wobei ein Symbol eine Länge von 8 Bit hat. Die Datenrate errechnet sich somit über 1,375 MSymbol/s * 8 Bit/Symbol = 11 MBit/s.

Kanalaufteilung

Um mehrere DSSS-Systeme unabhängig voneinander innerhalb eines Empfangsbereiches betreiben zu können, muß die Kanalbelegung der DSSS-Systeme berücksichtigt werden. Laut ETSI ist in Europa mit Ausnahme von Frankreich und Spanien die zur Verfügung stehende Bandbreite des ISM-Bands in 13 Kanäle unterteilt. Die Kanäle haben jeweils eine Bandbreite von 22 MHz und einen Kanalabstand von 30 MHz. Bei den 13 Kanälen beträgt allerdings der Abstand der Center-Frequenzen nur 5 MHz. Demnach überlappen sich die einzelnen Kanäle deutlich. Deshalb muß man berücksichtigen, daß beim Betrieb verschiedener DSSS-Systeme nur bestimmte Kanalgruppierungen innerhalb eines Empfangsbereichs genutzt werden können, ohne daß sich die Kanäle untereinander beeinflussen und Störungen verursacht werden. Bei der vorhandenen Aufteilung des Frequenzbandes können maximal drei DSSS-Systeme innerhalb eines Empfangsbereichs betrieben werden. Dies ist möglich, wenn die Kanäle 1, 7 und 13 verwendet werden, wobei alle andern Kanalgruppierungen jeweils nur den störungsfreien Betrieb von zwei unabhängigen DSSS-Systemen zulassen (vgl. Abb. 7).

DSSS versus FHSS

Im Vergleich zur FHSS-Technologie bietet die DSSS-Technologie, neben der höheren Packungsdichte, mit der Unterstützung von 5.5 und 11 Mbps eine bedeutend höhere Datenrate. Die höhere Datenrate wirkt sich positiv auf die erzielbare Übertragungsgeschwindigkeit aus. Zudem ist die Implementierung des Roaming weitaus einfacher, da die DSSS-Systeme nicht zwischen den Kanälen springen, sondern sich immer nur auf einem bestimmten Kanal bewegen. Das Abhören der Kanäle ist demnach wesentlich einfacher und nimmt bedeutend weniger Zeit in Anspruch. Bedingt durch die höhere Datenrate und die einfachere Umsetzung von Roaming wird bei Wireless LAN heutzutage die DSSS-Technologie bevorzugt verwendet, wobei jüngste Produkte nur noch die DSSS-Technologie unterstützen.

Finessen

Die erzielbare Reichweite der DSSS-Systeme ist von der Datenrate abhängig, wobei sich in einer geschlossenen Umgebung erzielbare Distanzen von 100 m bei 1 und 2 Mbps, von 70 m bei 5.5 Mbps und 30 m bei 11 Mbps ergeben. Die DSSS-Systeme werden dieser Tatsache gerecht, indem sie die verwendete Datenrate nach der jeweiligen Qualität des Empfangssignals und der auftretenden Übertragungsfehler automatischen einstellen. Ist die Empfangsqualität schlecht oder treten Übertragungsfehler auf, so verringern DSSS-Systeme sukzessive ihre Datenrate, bis die Qualität des Empfangssignals für eine fehlerfreie Datenübertragung wieder ausreichend ist. Ist die Empfangsqualität gut und können die Daten wieder fehlerfrei übertragen werden, so wird die Datenrate wieder schrittweise bis auf 11 Mbps erhöht.

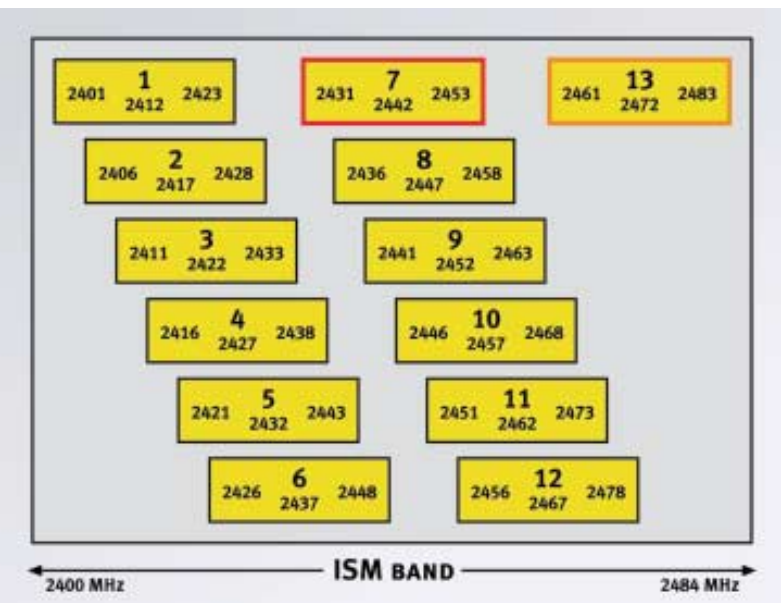
DCF versus PCF

Ein Funkmedium entspricht - wie das Übertragungsmedium der ersten Ethernet Variante - einem Shared Medium. Greifen ungefähr zeitgleich zwei oder mehrere Stationen auf das Funkmedium zu, so tritt eine Kollision auf, die die ausgesendeten Daten unbrauchbar macht. Demnach muß bei einem Wireless LAN über ein geeignetes Zugriffsverfahren dafür gesorgt werden, daß Kollisionen möglichst vermieden werden. Die Umsetzung des Zugriffsverfahrens wird hierbei, wie bei IEEE-Implementierungen üblich, von der MAC-Schicht wahrgenommen. Im Wireless LAN sind zwei Methoden als Zugriffskontrolle definiert, ein dezentralistischer und ein zentralistischer Ansatz. Der dezentralistische Ansatz entspricht dabei der Basiszugriffsmethode und wird als Distribution Coordination Function (DCF) bezeichnet, wobei der zentralistische Ansatz eine erweiterte und optionale Methode darstellt, die als Point Coordination Function (PCF) bezeichnet wird.

CSMA/CA

In Anlehnung an Ethernet wird in der DCF als Zugriffsmethode das Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) verwendet, das ähnlich funktioniert wie die aus der Ethernet-Technologie bekannte Carrier Sense Multiple Access/ Collision Detection (CSMA/CD). Aufgrund der physikalischen Eigenschaft der Funktechnik, bei der eine Station auf einer Frequenz entweder nur Daten senden oder empfangen kann, ist eine Kollisionserkennung (Collision Detection) im herkömmlichen Sinne technisch jedoch nicht möglich. Zudem lassen sich Kollisionen von anderen Störungen auf einem drahtlosen Medium im wesentlichen nicht unterscheiden. Durch diese Gegebenheiten hat man bei dem Wireless-Zugriffsverfahren anstelle der Kollisionserkennung eine Kollisionsvermeidung (Collision Avoidance) implementiert, durch die von vorne herein die Wahrscheinlichkeit für das Auftreten einer Kollision reduziert werden soll.

Abb. 7: Mögliche Kanalbelegung bei DSSS-Systemen.



Die Kollisionsvermeidung wird dabei über eine Reservierung des Übertragungsmediums realisiert, die über einen Timer durchgeführt wird. Dieser wird als Network Allocation Vector (NAV) bezeichnet und definiert fortlaufend den Zeitraum, über den das Übertragungsmedium für die Datenübertragung noch belegt sein wird. Der NAV-Wert wird auf jeder Station verwaltet, erst nachdem der NAV-Wert abgelaufen ist, wird eine Station versuchen, auf das Übertragungsmedium zuzugreifen und bei Bedarf ihre Daten auszusenden.

Medienreservierung

Der NAV-Wert wird auf jeder Station über den Empfang der Frame-Header gebildet, wobei die Zeitangabe im sogenannten Duration/ID Feld eingebettet ist. Da alle Stationen die Frame-Header unabhängig ihrer Adressierung empfangen, können sie ständig ihren NAV-Wert aktualisieren. Die sendende Station kann auf diese Weise das Medium für die benötigte Zeit ihrer Datenübertragung reservieren.
Möchte eine Station Daten übertragen, so prüft sie über das Carrier Sense, ob das Medium frei ist. Ist dies der Fall, so beginnt sie mit der Aussendung ihrer Daten. Sobald alle Stationen den Anfang des Frames, respektive den Frame-Header, empfangen haben, gilt das Medium als eindeutig belegt und die Reservierung für die Dauer der Datenübertragung ist über den NAV-Wert sichergestellt.
Da es jedoch vorkommen kann, daß mehrere Stationen ungefähr zeitgleich versuchen, auf das Medium zuzugreifen, besteht die Möglichkeit, daß sie fälschlicherweise zu der Ansicht gelangen können, daß das Medium frei ist (Multiple Access) und ebenfalls mit der Aussendung der Daten beginnen. Tritt dieser Fall ein, so wird es zwangsläufig zur einer Kollision kommen, durch die die übertragenen Daten unbrauchbar werden und verloren gehen. Da Kollisionen oder andere Störeinflüsse, die die Datenübertragung negativ beeinflussen, nicht ausgeschlossen werden können, wird der erfolgreiche Empfang der Daten durch den Empfänger über die Aussendung einer Empfangsbestätigung (Acknowledgement) bestätigt. Bleibt die Empfangsbestätigung aus, so werden die Daten vom Sender nach einer bestimmten Wartezeit erneut ausgesendet. Generell werden jedoch nur Unicast-Pakete über die Aussendung einer Empfangsbestätigung bestätigt, Broadcast- und Multicast-Pakete werden nicht bestätigt, da es nicht sinnvoll wäre, wenn jeder Empfänger den Empfang bestätigen würde.

Empfangsbestätigung

Nach dem Aussenden der Daten, erwartet eine Station innerhalb eines bestimmten Zeitraums eine Empfangsbestätigung vom Empfänger der Daten. Damit sichergestellt ist, daß die Empfangsbestätigung vom Empfänger ausgesendet werden kann, ohne daß eine andere Station bereits das Übertragungsmedium für die Aussendung ihrer Daten belegt hat, haben die Empfangsbestätigungen bei dem Zugriff auf das Medium eine höhere Priorität. Die Vergabe der Prioritäten wird über verschiedene Mindestabstände zwischen zwei aufeinanderfolgenden

Abb. 8: Zeitlicher Ablauf für die Aussendung eines Frames und die darauffolgende Empfangsbestätigung mit Reservierung des Übertragungsmediums über den NAV-Wert.

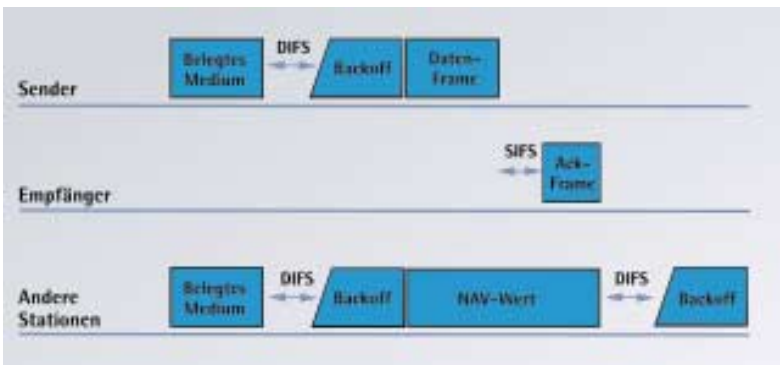


Abb. 9: Durch das Hidden Station Problem kann es zu Kollisionen kommen. (Bildquelle: ELSA)

Frames realisiert, die als Interframe Space (IFS) bezeichnet werden. Laut Standard sind vier verschiedene IFS definiert, die bei der Sicherstellung der Prioritäten verschiedene Funktion haben.

Interframe Spaces

Der Short Interframe Space (SIFS) legt unter anderem den zeitlichen Mindestabstand für ACK-Frames, Clear-to-Send-Frames und die Burst-Folge einer fragmentierten Nachricht fest. SIFS entspricht dabei der Zeitspanne zwischen dem letzten Symbol des vorherigen Frames und dem ersten Symbol, der Präambel, des darauffolgenden Frames.

Der Point (Coordination Function) Interframe Space (PIFS) wird ausschließlich von Stationen verwendet, die im PCF-Modus arbeiten. Über PIFS wird während der PCF sichergestellt, daß für die PCF-Stationen ein bevorzugter Medienzugriff möglich ist. Der Distributed (Coordination Function) Interframe Space (DIFS) wird von Stationen genutzt, die im DCF-Modus arbeiten. DIFS wird für die Aussendung der Daten- und Management-Frames verwendet.

Der Extended Interframe Space (EIFS) wird bei Stationen angewendet, die im DCF-Modus arbeiten. Sollte der PHY bei der Aussendung eines Frames einen Fehler im Frame festgestellt haben, so wird die Aussendung des Frames abgebrochen. Für die anderen Stationen wird nach dem Ablauf der EFIS der Zugriff auf das Medium erlaubt und die Stationen müssen nicht die Zeit abwarten, die ursprünglich als NAV-Wert definiert wurde.

Medienzugriff

Da zeitlich betrachtet die SIFS kürzer als die DIFS sind, haben Frame-Typen, die nach dem Ablauf des Short Interframe Space gesendet werden dürfen, beim Medienzugriff eine höhere Priorität als die Frames, die erst nach Ablauf des DIFS gesendet werden dürfen. So wird sichergestellt, daß ACK-Frames vor Daten-Frames ausgesendet werden dürfen und eine Station grundsätzlich eine Chance hat, ihr ACK-Frame nach dem fehlerfreien Empfang der Daten auszusenden. Damit gewährleistet ist, daß nicht alle Stationen nach dem Ablauf des DIFS zeitgleich versuchen, auf das Medium zuzugreifen, wartet jede Station für sich eine bestimmte Zeit ab, bevor sie eventuell mit der Aussendung der Daten beginnt. Die Wartezeit wird nach dem Zufallsprinzip über den Exponential-Backoff-Algorithmus auf jeder Station erstellt. Die Station, die die kleinste Wartezeit ermittelt hat, greift als erste auf das Medium zu und sendet ihre Daten aus, wodurch für alle anderen Stationen das Medium als belegt und reserviert gilt (vgl. Abb. 8).

Hidden Station Problem

Man spricht von einem Hidden Station Problem, wenn zwei Stationen in der Reichweite zu einer dritten Station stehen, sich jedoch untereinander außerhalb ihrer Reichweite befinden. Denn dann kann es vorkommen, daß sie mit der Datenübertragung zur dritten Station beginnen, obwohl das Übertragungsmedium von der anderen Station bereits belegt ist. In diesem Fall kommt es an der dritten Station zu einer Kollision. Um die Wahrscheinlichkeit zu reduzieren, daß die Daten zweier Stationen kollidieren, die außerhalb ihrer Reichweite zueinander stehen, ist im Standard das RTS/CTS-Verfahren implementiert worden. Eine sendewillige Station schickt ein RTS-Frame (Request-to-Send) aus, um anzukündigen, daß sie Daten aussenden möchte. In dem RTS-Frame wird über das Duration/ID Feld die benötigte Dauer für die Datenübertragung ankündigt. Das RTS-Frame wird von der Zielstation mit einem CTS-Frame (Clear-to-Send) beantwortet, in dem ebenfalls die Dauer für die Datenübertragung bekannt gegeben wird. Die anderen Stationen erhalten auf diese Weise die Reservierung für das Übertragungsmedium und werden darauf ihre eventuell anstehenden Datenaussendungen für die Dauer der Übertragung zurückstellen. Dies reduziert die Wahrscheinlichkeit für eine Kollision, auch wenn Stationen außerhalb ihrer Reichweiten zueinander stehen. Da die RTS/CTS-Frames nur eine geringe Länge haben, würde bei einer Kollision dieser Frames das Übertragungsmedium nur kurzzeitig durch eine Kollision belegt.

Nachdem wir einen Einblick in die PHY-Schichten und in die Basiszugriffsmethode der Wireless LANs geschaffen haben, möchten wir in der nächsten Ausgabe der Technik-News mit der Fragmentierung fortfahren und zeigen, wie die Stationen innerhalb einer Funkzelle aufgenommen werden.

Stand: 09. Oktober 2001

Technik-News Patch-CD November 2001

Empfohlene NovelI-Patches

NetWare

NW 5.1
4PENT.exe
AFNWCGI1.exe
B1CSPJVM.exe
COMX218.exe
DLTTAPE.exe
DS755A.exe
DS877A.exe
DSBROWSE.exe
FP3023A.exe
FP3023S.exe
IDEATA5A.exe
INSTP5X.exe
JSSL11D.exe
MBCMNUP1.exe
N51_NIS1.exe
NAT10.exe
NDP2XP6A.exe
NDPSINF.exe
NESN51B.exe
NICE157.exe
NIPT1.exe
NJCL5A.exe
NLSLSP6.exe
NW51FS1.exe
NW51INST.exe
NW51SP3.exe
NW51UPD1.exe
NW5NWIP.exe
NWFTPD3A.exe
NWOVLY1.exe
NWOVLY2.exe
NWPA5.exe
OS5PT2A.exe
PKISNMAS.exe
PREDS8A.exe
PREEDIRD.exe
RINSTALL.exe
SBCON1.exe
SCMDFLT.exe
SLPINSP3.exe
TCP542U.exe
WBDAV51.exe
NW 5.0
AFNWCGI1.exe
C112BRJ.exe
C112CRJ.exe
CERTSRV.exe
COMX218.exe
DLTTAPE.exe
DS755A.exe
DS877A.exe
DSBROWSE.exe
FP3023A.exe
FP3023S.exe
I20DRV5.exe
IDEATA5A.exe
MBCMNUP1.exe
NAT10.exe
NDP2XP6A.exe
NDPS20P1.exe
NDPSFT1A.exe
NJCL5A.exe
NLSLSP6.exe
NSSNW5A.exe
NW5MCALC.exe
NW5NWIP.exe
NW5PSERV.exe
NW5SP6A.exe
NW5TCP.exe
NWPA5.exe
NWSSO.exe
ODSB.exe
OS5PT2A.exe
PREDS8A.exe
PREEDIRD.exe
SCMDFLT.exe
SLPINSP3.exe
TIMESYNC.exe
VRPNW5A.exe
NW 4.2
DS411T.exe
GROUPFIX.exe
IPG4201.exe
IPGSN10A.exe
LONGNAM.exe
NLSLSP6.exe
NW4SP9.exe
NW4WSOCK.exe
TSANDS.exe
NW 4.11
ATMDRV04.exf
DS411Texe
HSTDEV.exe
I2ODRV4.exe
IPGSN10A.exe
IPX660.exe
LDAP103A.exe
LONGNAM.exe
MIXMOD6.exf
NAT10.exe
NDPS10P2.exe
NLSLSP6.exe
NW4SP9.exe
NWPAUP1A.exe
NWTAPE1.exe
ODI33G.exe
ODIWAN1.exe
RAD102.exe
RADATR.exe
SCMDA.exe
SPXS03A.exe
STRTL8.exe
TSANDS.exe
VRP411a.exe
Tools / DOCs
ADMN519F.exe
CFGRD6B.exe
CONFG9.exe
COPYNLM3.exe
CRON5.exe
DSDIAG1.exe
ETBOX7.exe
HIGHUTIL1.exe
LOADDLL1.exe
NCCUTIL5.exe
NLSDLL.exe
ONSITB8.exe
SCHCMP2.exe
STUFKEY5.exe
TABND2.exe
TBACK3.exe
TBOX7.exe
TCOPY2.exe
TRPMON.exe
UPGRDWZD.exe
ZFSDBPB.exe

NetWare Utilities

NW 5.x/4.x
41DSVU2.exe
C1_FULL.exe
NLSTY2K.exe
NTPRINT.exe

Server Protocol Updates

DHCP SER. 2.0
CSATPXY2.exe
DHCP21R.exe

NLSP-NW 4.10
IPX660.exe

NLSP-NW 3.12
IPX660.exe

NFS 2.3
NFS205.exe
UXP205.exe

TCP/IP
TCPN06.exe

MPR 3.1
MPR31B.exf

NW/IP2.2
NIP199.exe

Client Kits & Updates

Win 95/98 dt.
IPCOST.exe
NDPCPSP3.exe
W9533G.exe

Windows 95/98 engl.
33SP3.exe
NDPCPSP3.exe
W9X33E.exe

Win NT/2000 dt.
243798.exe
264837.exe
270050.exe
275820.exe
IPCOST.exe
NDPCPSP3.exe
WNT48G.exe

Win NT/2000 engl.
243798.exe
264837.exe
270050.exe
275820.exe
48SP3.exe
NDPCPSP3.exe
WNT478E.exe

ZENworks Clients

ZEN for Desktops 3.0
FZD3NAL5.xex
MZFD3SP1.exe
ZD3IDNTY.exe
ZD3RC95.exe
ZD3SCAN2.exe
ZFD3PT3A.exe
ZFD3SITE.exe

ZENworks 2.0
FZD2ABND.exe
FZD2NAL.exe
FZD2NAL1.exe
FZD2ZAPP.exe
ZFD2PT3B.exe
ZFD2SP1.exe
ZFD2TSFX.exe

ZEN 2.0 for Server
ZFS2SP1.exe

ZEN for Networks
ZFN101.exe

Miscellaneous Updates

ManageWise 2.7
MW27SP1.exe
MWNMAUPD.exe

ManageWise 2.5/2.6
MW26SP3.exe
MW26TRD1.exe
MWINOC1K.exe
MWINOC2Kexe
MWNMAUPD.exe
MWNXP26.exe

NW SAA 4.0
NW4SAA.exe
SAA40020.exe

NW SAA 3.0
LANCHK.exe
SAA30020.exe

Cluster Services
CS1SP2.exe
CVSBIND.exe

GroupWise 6.6
GWPDLOCK.exe
NOTES51.exe

eDirectory 8.x
AMW2KP2A.exe
C1UNX85A.exe
DSRMENU4.tgz
MWUNXPFIX.exe
NDSAS3S1.exe
NDSUNIX4.tgz

GroupWise 5.5
CCMLN2.exe
EXCHNT2.exe
G554MLT.exe
G55ESP2M.exe
GW55SP4.exe
GWE2MLFX.exe
MSMPCU.exe
R553AMLT.exe
WINNTWMS.exe
WINNTWMS.exe

Bordermanager 3.5/3.6
ADMATTRS.exe
BM35ADM4.exe
BM35C11.exe
BM35EP1.exe
BM35EP1A.exe
BM35SP3.exe
BM36SP1.exe
BM3CP3.exe
BM3SS02.exe
BM3XC02.exe
BMAS3X01.exe
BMSAMP1.exe
BMTCPE4.exe
BMVPN3Y.exe
PXYAUTH.exe
RADATR3A.exe
VPN35E.exe
WEBLSP1.exe

Empfohlene Microsoft-Patches

Deutsche Updates

Windows 95
D35907.exe
ID4SETUP.exe
MSDUNBD.exe
W95SP1_G.zip
W95Y2KD.exe

Windows 98
O98SECU.exe
Y2KW982G.exe

Windows NT 4.0
DEUQ300972I.exe
ID4SETUP.exe
SP6I386G.exe

Windows 2000
CODEREDSCANNER.exe
ENPACK_WIN2000ADMIN_GER.exe
OUT2KSEC.exe SP1_500I.exe
Q300972_W2K_SP3_X86_DE.exe
Q301625_W2K_SP3_X86_DE.exe
W2KSP2.exf

Exchange 5.5
SP4_550G.exe

Exchange 5.0
SP1S500I.exe

Englische Updates

Windows 95
IE4SETUP.exe
IE4USP.exe
MSDUN13D.exe
W95PLUSD.exe
W95SP1.exe
W95Y2K.exe

Windows 98
Y2KW98_2.exe

IE 5.01
IE5SETUP.exe
Q268465.exe

Windows NT 4.0
IE4USP.exe
IESETUP.exe
MPRI386.exe
PPTPFIXI.exe
RRASFIXI.exe
SP6I386.exf

Windows 2000
ENPACK_WIN2000ADMIN_EN.exe
Q301625_W2K_SP3_X86_EN.exe
W2KSP2.exe

Exchange 2000
Q278523ENGI.exe

Exchange 5.5
SP4_550E.exe

Exchange 5.0
SP2_500I.exe
SP2S500I.exe

Empfohlene BinTec Updates und Patches

Bintec Router Software

Bingo!	**Brick XS/Office**	**Brick XM**	**X4000**	**XCentric**
BGO521.bg	BRK512.xs	BRK511.xm	BL6102.x4a	XC521.xcm
Bingo! Plus/Professional	BRK521xs2	BRK521.xm2	**X3200**	MODULE14.xcm
BGO494.bgp	BRK511P7.XS2	**Brick X.21**	B5501.x3b	**Vicas!**
BrickWare u. Configuration Wizard	**Brick XMP**	BRK495.x21	**X1000/x1200**	VIC494.vc
BW612.exe	BRK521.XP	**Brick XL/XL2**	B5301P06.x1x	**Netracer**
NLMDISK.zip		BRK521.xl		NR494P1.zip

Empfohlene Tobit Updates und Patches

Tobit Produkte für Novell

TimeLAN Novell	**David 6.6**	**DAVID 6.5**	**DAVID 6.0**	
TIMELAN.exe	D66NWSP1.exe	D65SP1NW.exe	D6SP1NM.exe	IHS_NT.exe
Faxware 5.11 für Netware SB 4.2	DVGRAB.nlm	DVVSCA10.exe	DIGITLD.zip	KEDV326.exe
DAVID4.nlm	DVVSCA10.exe	PM_NW.zip	DV4EXSP2.exe	MCSCANNW.zip
Faxware 5.11 für Netware SB 5.0	IVC.dcc		DVVSCA10.exe	PLMSYN10.exe
DAVID5.nlm	POSTMAN.nlm			REPORTER.exe
	WEBACCNW.exf			

Tobit Produkte für Microsoft

Tobit ServTime Win 98	**David 6.6 NT/2000**	**DAVID 6.5 für NTl**	**DAVID 6.0 für NT**	**Tools**
SETUPW98.exe	1839NT.zip	D65SP1NT.exe	D6SP1NT.exe	DCNSETUP.exe
Tobit TimeLAN für NT	D66NTSP1.exe	DV4EXSP2.exe	DVC3PD.dll	DVEXTINF.exe
SETUPNT.exe	DV_WIN.zip	MAPI32.dll	DVVSCA10.exe	DVZMSD.exe
Tobit ServTime für NT	DVGRAB.exe		IHS_NT.exe	KLICKTEL.zip
SERVTIME.exe	DVPGP.dll		KEDV326.exe	SENDMAIL.exe
	IVC.dcc		PLMSYN10.exe	
	MCSCANNT.zip			
	WEBACCNT.exe			

rot	seit unserer letzten Veröffentlichung **neu** hinzugekommen	blau	aus Platzgründen **nicht mehr** auf der CD
		gelb	auf der letzten Service CD
grün	nur noch auf der Technik News **Service-CD**	pink	auf der beiliegenden Novell Sonder-CD

Tobit Updates und Patches neu herausgekommen

1839NT.zip 550 KB

Dieses Download enthält eine aktualisierte Version des Service Layers für den Betrieb unter Windows NT/2000 von Tobit David Version 6.6. Bei der bisherigen Version konnte es in Verbindung mit der Sammelliste oder der Verwendung des PORT-Befehls zu Problemen mit der Client/Server-Verbindung kommen. Die Clients konnten sich nicht mehr am Service Layer anmelden. Das Hotfix braucht nur eingespielt zu werden, wenn die Programm CD vom 12.06.2001 bzw. das Service Pack 1 installiert ist.

Programmversionen:

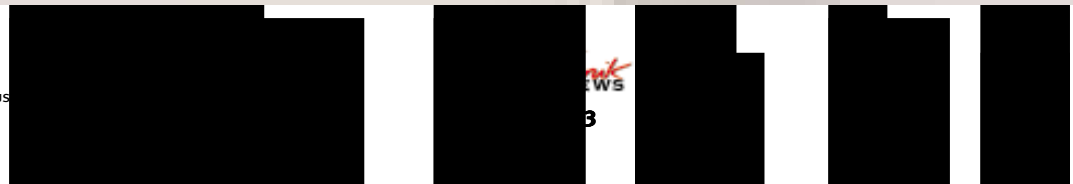
SL.EXE	6.60a	1839
TOBIT32.DLL	6.60a	0121
DAVIDLIB.DLL	6.60a	0153
TGRAPHIC.DLL	.60a	0126

MCSCANNT.zip 600 KB

Dieses Download enthält die aktuelle Version der Scan-Engine für den in DvISE intergrierten Virenscanner. Die aktuelle Engine für den Betrieb unter Windows NT/2000 besitzt die Versionsnummer 4.1.50 und das Dateidatum 26.09.2001. Voraussetzung ihren Einsatz ist die Verwendung aktueller Virensignaturen (mindestens Version 4151).

DVPGP.dll 64 KB

Diese Beta-Version der Tobit PGP Support Library (`dvpgp.dll`) für PGP Version 7.1 verlangt für den Betrieb DvISE ab der Version 6.6. Achtung: Ältere PGP-Versionen als 7.1 werden z.Zt. nicht unterstützt!



Empfohlene Veritas Updates und Patches

Backup Exec 8.5/8.6 — Windows NT und Windows 2000

Installation		
EXV30I03_237919.EXE	29.06.01	ExecView 3.0 Build 152 (englisch)
BNT86I02_237891.EXE	29.06.01	Backup Exec Ver. 8.6 Build 3808 rc5 (dt.)
BNT86I03_237889.EXE	28.06.01	Backup Exec Ver. 8.6 Build 3808 rc5 (engl.)
BNT85SBSFIX_236351.EXE	10.05.01	SBS Seriennr. Fix für BE 8.5 Revision 3572 rc9 (HF23)
RAIDIRECTOR_233163.EXE	14.12.00	RAIDirector Evaluation Version (NLS)
Patches		
BNT8XVIRUPD_240051.EXE	05.09.01	Virus Engine Update Ver.8.0 und 8.5 (alle) (NLS)
BNT85OFOFIX_239866.EXE	30.08.01	OFO Hotfix 31 QLogic Prob. V. 8.5 Build 3572 RC9 (NLS)
BNT86OFOFIX_239867.EXE	30.08.01	OFO Hotfix 7 QL ogic Prob. V. 8.6 Build 3808 RC5 (NLS)
BNT86SQLFIX_239493.EXE	14.08.01	SQL 2000 Hotfix 3 Ver. 8.6 Build 3808 (NLS)
BNT86SYSFIX_239551.EXE	14.08.01	System State Hotfix 10 Ver. 8.6 Build 3808 RC5 (NLS)
BNT85SYSFIX_238549.EXE	30.06.01	System State Sicherungsprobleme v8.5 B.3572 rc9
BNT85CATFIX_238991.EXE	30.06.01	Restore Auswahl Probleme nur v8.5 Build 3572 rc9
BNT86SQLFIX_239007.EXE	30.06.01	SQL 2000 Device not found (dt./engl) nur 8.6 B.3808
BNT86SYSFIX_239027.EXE	30.06.01	System Status Hotfix (dt./engl) nur v8.6 B.3808 rc5
BNT86TSMFIX_239160.EXE	30.06.01	TSM 3.7/TSM 4.1 Unterstüt. (dt./engl) nur v8.6 B.3808 rc5
BNT86CMDFIX_239162.EXE	30.06.01	BEMCD Fix für Cleaning Slot ü. Script. (dt./engl)
BNT85SYSFIX_236381.EXE	10.05.01	8.5 3572 rc9, HF22 System State, Exch. restore, Device Error
BNT85SSOFIX_236423.EXE	08.05.01	8.5 3572 rc9 HF18 SSO Umgebung Drive Offline
MEDIAFIX_234341.EXE	06.02.01	Behebt Fehler “Unrec. Media” für Ver. 8.5 Build 3571(NLS)
POST3571_232826.EXE	10.11.00	Hotfix für Remote Intelligent Desaster Recovery
OFOFIX.EXE	21.02.01	Blue Screen und Initialisierung bei Open File Option
Treiber		
BNT85IDRV29A_237727.EXE	22.06.01	Gerätetreiber R. 20010615 / Autoloader R.29A nur BE 8.5 (dt./engl.)
Agenten		
NWAA191_236656.EXE	18.06.01	NetWare Remote Agent v191 (engl.) behebt Fehler “Acess Denied”
NLS_AGNT_236717.TAR	16.05.01	Unix Agent v5.01 Rel.5030 (deu/engl) behebt Hard Link / NIS Problem
AG9X021_234221.EXE	30.01.01	Windows 9X Agent Version 5.021 (NLS)
AGORACLE_232754.EXE	14.12.00	Oracle Agent Version 5.010 (NLS)
AGOS203.EXE	19.05.00	OS/2 Agent Version 3.203 (NLS)
AGWIN31.EXE	19.05.00	Win 3.1X Agent (NLS)
AGDOS.EXE	19.05.00	DOS Agent Version 3.015 (NLS)
AGMAC500.EXE	10.05.00	Mac Agent Version 5.00 (NLS)
Utilites		
BENTTOOL_232477.EXE	17.01.01	Diagnostik-Utilities für Windows und NetWare

Nur die neusten NW und NT Versionen, nur Intel CPU’s (kein Alpha), nur englisch und deutsch wenn vorhanden.

Backup Exec 8.5 — Für Novell NetWare

Installation		
BE85P00_240250.EXE	17.09.01	Backup Exec für NetWare Version 8.5.194 (NLS)
EXV30I03_237919,EXE	29.06.01	ExecView 3.0 Build 152 (engl.)
B85P00_235814.EXE	12.04.01	Backup Exec für NetWare, Version 8.5.191 (NLS).
EXECV25_231291.EXE	29.08.00	ExecView Version 2.5 mit Pure IP Unterstützung (NLS)
Patches		
BESRVR_2_232776.EXE	07.11.00	BESRVR.NLM V.3.21,behebt Tape Rotation Prob. (engl.)
Treiber		
B850DV13_239791.EXE	12.09.01	Gerätetreiber Set 13 für 8.0 Build 300, 8.5 Build 191 (engl.)
B850DV12_237018.EXE	30.05.01	Gerätetreiber Version 9901N023 (engl.)
NWASPI_232264.EXE	16.10.00	NWASPI.CDM Update Version 3.20 und Version 3.21
Agenten		
WIN9X_AGENT_239813.EXE	28.09.01	Windows 9x Agent V5.019 (NLS) Novell und NT
NLS_AGNT_236717.TAR	16.05.01	Unix Agent v5.01 Rel.5030 (dt./engl) behebt Hard Link / NIS Problem
BEORANW_236814.EXE	21.05.01	Oracle Agent neueste Version (engl.)
WINNTAGT_230560.EXE	28.07.00	Windows NT Version 5.003 (engl.)
WINNTAGT.EXE	19.05.00	Windows NT Agent Version 3.201 (NLS)
AG9X019.EXE	1.08.00	Windows 9x Agent Version 5.019 (NLS)

Empfohlene Veritas Updates und Patches

OS2AGENT.EXE	19.05.00	OS/2 Agent Version 3.204 (engl.)
MACAGENT.EXE	19.05.00	Macintosh Agent Version 4.07 (NLS)
DOSAGENT.EXE	10.05.00	DOS Agent Version 3.015 (NLS)
BEORANW.EXE	08.06.00	Oracle Agent (engl.)
BEWINUPD.EXE	19.05.00	Windows Client (engl.)
Utilities		
ALLTOOLS_235507.EXE	29.03.01	Diagnostik Tools für NetWare Umgebung
BENTTOOL_232477.EXE	17.01.01	Diagnostik Utilitys für Windows und NetWare

Neue Patches in der Übersicht

Veritas Updates und Patches neu herausgekommen

Backup Exec 8.5/8.6 Für Windows NT und 2000

BNT8XVIRUPD_240051.exe (deutsch/englisch)

In dieser Datei ist das Virus Engine Update für Backup Exec für Windows NT und 2000 für alle Buildstände der Versionen 8.0 und 8.5 enthalten (in 8.6 bereits integriert). Zur Installation entpacken Sie am besten Dateien immer in einem temporären Verzeichnis und stoppen alle Backup Exec Dienste!
Benennen Sie die Dateien `Scan.dat`, `Names.dat`, `Clean.dat` und `Mcscan32.dll` aus dem Verzeichnis `\Programme\VERITAS\Backup Exec\NT` um und kopieren Sie die neuen Dateien in den Ordner. Starten Sie anschließend die Backup Exec Dienste wieder und führen Sie im Menü unter Tools den Punkt `Update Virus Protection Files` aus.

BNT85OFOFIX_239866.exe (deutsch/englisch)

Hotfixes müssen generell der Reihenfolge nach eingespielt werden. Dieser ist für die Version 8.5 Build 3572 RC9und trägt die Nummer 31. Wenn die Open File Option (OFO) auf Systemen mit gewissen QLogic Produkten installiert war, kann es zu einem Blue Screen kommen. Der Hotfix muß auf dem Backup Server und den Servern, die mit der Open File Option gesichert werden, eingesetzt werden.
Um diesen Hotfix aus Ihrem temporären Verzeichnis heraus zu installieren, benennen Sie die Datei `Otmlapi.dll` aus `\Programme\VERITAS\Backup Exec\NT` um und kopieren die neue Datei in das Verzeichnis. Außerdem müssen die Dateien `Otman4.sys` und `Otman5.sys` aus `\Winnt\System\Drivers` umbenannt und mit den Dateien aus diesem Hotfix ersetzt werden, anschließend Maschine neu starten.
Ist die Open File Option auf einem entfernten Windows NT/2000 Server installiert, der über den Remote Agent mit OFO gesichert wird, müssen auch hier nach dem Entpacken die Backup Dienste gestoppt werden. Der Remote Agent ist entweder unter `C:\Bentaa` oder `\Programme\VERITAS\Backup Exec\RANT` installiert. Benennen Sie die `Otmlapi.dll` um und kopieren Sie die neue Datei aus diesem Hotfix in das Verzeichnis. In `\Winnt\System32\Drivers` verfahren Sie mit `Otman4.sys` und `Otman5.sys` genauso (Unter Windows 2000 gibt es ggf keine `Otman4.sys`) Starten Sie den Rechner neu.

BNT86OFOFIX_239867.exe (deutsch/englisch)

Dieser Hotfix für die Version 8.6 Build 3808 RC5 trägt die Nummer 7 und behebt Fehler, wenn die Open File Option (OFO) auf Systemen mit gewissen QLogic Produkten installiert wird und es zu Blue Screen kommt. Er muß auf dem Backup Server und den Servern, die mit der Open File Option gesichert werden, eingesetzt werden (wie zuvor).

BNT86SQLFIX_239493.exe (deutsch/englisch)

Dieser Hotfix für die Version 8.6 Build 3808 trägt die Nummer 3 und behebt Fehler auf Systemen, auf denen SQL 2000 mit mehrfach Instanzen läuft, und der Computername und der Instance Name zusammen länger als 15 Zeichen ist, dann kommt es zu einem `Device not found`. Um den Fehler zu beheben, muß dieser Hotfix auf allen Systemen, auf denen Backup Exec SQL sichert, sowie auf dem Medien Server wie gewohnt eingespielt werden. `Bedssql2.dll` unter `\Programme\VERITAS\Backup Exec\NT` wird umbenannt und mit dem Hotfix ersetzt. Anschließend die Dienste wieder straten.
Auf einem Windows 2000 Server, der mit Agent gesichert wird, entpacken Sie wie gewohnt, stoppen den Remote Agent für Windows 2000. Er ist auf `c:\im`

Veritas Updates und Patches neu herausgekommen

Verzeichnis \BENTAA oder Programme\VERITAS\ Backup Exec\RANT zu finden. Benennen Sie Bedssql2.dll um und kopieren Sie die neue Datei. Starten Sie den Remote Agent Dienst neu.

BNT86SYSFIX_239551.exe (deutsch/englisch)

Dieser Hotfix für Version 8.6 Build 3808 RC5 trägt die Nummer 10. Auf Systemen, auf denen das Verzeichnis für alle Benutzer für Standarddokumente und Einstellungen-Ordner verschoben wurden, wird beim System State Backup nicht korrekt gesichert. Umgeleitete Wiederherstellungen des System States geben nicht die korrekte Sysvol Struktur wieder. Es trat ein Dr. Watson während des System State Actice Directory Sicherns auf, wenn das OS nicht die AD Pfadinformationen lieferte. Wurde ein entferntes Sichern des System States durchgeführt, erschien: Unable to open the item _SharedHardlinkData_\0.0.0.-skipped. Und wurde ein lokales System State Backup durchgeführt, erschien: The item \\?\UNC\SERVERS\System?State\Registration DB\Registration DB in use –skipped. Zur Installation benennen Sie die Dateien Bedsnt5.dll und Bengibe.dll um und kopieren Bedsnt5.dll in dieses Verzeichnis. Die Bengine.exe müssen Sie aus dem passenden Sprachenverzeichnis des Hotfixes kopieren. Starten Sie anschließend wieder die Backup Exec Dienste. Auf einem Windows 2000 Server mit Agent installieren Sie wie - oben beschrieben - die Datei Bedsnt5.dll.

Backup Exec Version 8.5 für Novell NetWare

B85P00_240250.exe (deutsch/englisch)

In dieser Datei ist die aktuelle Backup Exec Version 8.5.194 für NetWare enthalten, mit den Einzelkomponenten BEMGR = 8.5.4110.3, BESRVR = 8.5.4112.14, Treiber = 9901N023.1, NLM Client = 8.5.4106, Windows Client = 8.5.4113.190, Windows NT Agent = 5.004, Windows 95 Agent = 5.022, OS2 Agent = 5.000, DOS Agent = 5.000, MAC Agent = 5.00 und Unix Agent = 5.027. Die Version kann auf NetWare 4.11, 4.11 SFT3, 4.11SB, 4.2, 4.2 SB, 5.0, 5.1 und 5SB installiert werden. Kopieren Sie die Datei in ein temporäres Verzeichnis auf den Server und rufen Sie mit Load Sys:\Temp\Beinstl.nlm die Installationsroutine auf. (diverse Beschreibungen in Deutsch vorhanden).

B850DV13_239791.exe (englisch)

In dieser Datei enthalten ist das aktuelle Gerätetreiber Set (13) für die Versionen 7.5 Build M123, 8.0 Build 300, und 8.5 Build 191. Es darf nicht auf anderen Buildständen eingesetzt werden. Fehler wurden behoben und folgende Geräte zusätzlich unterstützt: Adic FastStor mit IBM Ultrium LTO Laufwerken, HP C7200 und HP C7145 mit IBM Ultrium-TD1 Laufwerken. Zur Installation kopieren Sie die Dateien aus dem temporären in das Verzeichnis Sys:\Backupexec\Nlms. Bei der Version 8.5 Build 191 oder neuer reicht das Kopieren der neuen Dateien aus. Bei älteren Versionen muß die Startdatei Sys:\System\Bestart.ncf für dieses Treiber Set noch angepaßt werden. Das Laden des AD_ASPI.nlm muß dort mit Parametern an der richtigen Stelle eingetragen werden. Die Sektion ist:

```
Search add Sys:\Bkupexec\Nlms\
Load AD_ASPI.NLM –N –S -BELOW16=N
Load Bkupexec.NLM –t1 –aa ...
```

(Diese Zeile variiert je nach Installation und muß nicht verändert werden)

Bei einem Controller älterer Generation, der nur DMA im Speicher unterhalb 16 MB unterstützt, darf der Parameter –BELOW16=N nicht angefügt werden. PCI- und die meisten EISA-Kontroller unterstützen DMA oberhalb 16 MB. Sollten Solche Controller können Sie auch an der Ladezeile für das Bpupexec.nlm erkennen, dann gibt es dort einen Schalter –DN anstelle von DY. Wenn Sie nach Ausführen der Bestart.ncf an der Server Konsole die Meldung sehen:

```
Loader cannot find public symbol
NPA_Get_OS_Version
Load file rederenced undefined public
variable
```

muß das NWPA.NLM ebenfalls über die Bestart.ncf geladen werden. Dieses muß mit load NWPA.NLM direkt nach search add Sys:\System\Nlms und vor load AD_ASPI –N -S in der Bestart.ncf eingetragen werden.

WIN9x_AGENT_239813.exe (NLS)

Dieses ist der aktuelle Windows 9x Agent V5.019, der für Novell und NT eingesetzt werden kann. Nach dem Entpacken führen Sie aus dem Verzeichnis für die gewünschten Sprache die Setup.exe aus und folgen den Instruktionen. In den Eigenschaften des Agent in Systemsteuerung Netzwerk kann der Agent konfiguriert werden. Zu beachten ist die Auswahl des Protokolls (SPX/TCP/IP), standardmäßig werden alle lokalen Laufwerke zum Sichern eingerichtet.

NovelI Updates und Patches neu herausgekommen

NWFTPD3A.exe 142 KB

Dieses aktuelle Update für den FTP-Server der Netware Version 5.1 darf nur auf einem Netware Server aufgespielt werden, der über einen installierten FTP-Server verfügt. Weiterhin ist zu beachten, daß das Support Pack 3 der Netware 5.1 bereits vorhanden ist.

NDPCPSP3.exe 908 KB

Support Pack 3 für die NDPS Libaries der aktuellen Novell Clients 3.3 für Windows 95/98 und Version 4.8 für Windows NT/2000. Dieses Update benötigt sowohl auf NT/2000 als auch 95/98 Basis das Support Pack 3 des normalen Clients. Es werden die Dateien `DPLMW32.dll` und `DPLMRW32.dll` erneuert, da die alten Files den Fehler hatten, daß der Default Printer nicht geändert werden konnte, wenn der existierende Drucker kein NDPS-Drucker wart.

275820.exe 285 KB

Dieses Update enthält eine neue Version der Datei `NWFS.sys`, das nur auf einem Novell Client v4.8 (Windows NT/2000) mit Service Pack 3 zu verwenden ist. Die NWFS-Version des Service Pack 3 hat Probleme bei der Verteilung auf eine Workstation über Netware Applikation Launcher. Wird die Datei manuell kopiert, tritt der Fehler nicht auf.

270050.exe 345 KB

Die Updates zu `LOGINW32.dll` und `LGNWNT32.dll` sind nur für die Novell Client Version 4.8 (Windows NT/2000) mit Service Pack 3 geeignet und behebt diverse Client Probleme mit Service Pack 3 und `Grace Login`.

BM35SP3.exe 8950 KB

In dieser Datei befindet sich das Support Pack 3 mit Patches und Updates für die im Novell Bordermanager 3.5. enthaltenen Services. Auch alle älteren Service Packs sind Bestandteil dieses Updates.

NDSUNIX4.tgz 7 KB

Das NDSRepair für den Unix Menü Wrapper in der Version 1.03.03 versetzt Sie - wie das `DSREPAIR.nlm` auf einem NetWare Server - in die Lage, einen NDS-Datenbank-Check auf einem Unix Rechner vorzunehmen.

BinTec Updates und Patches neu herausgekommen

BW612.exe 8204 KB

In diesem Update finden Sie die neueste Version 6.1.2 der BRICK ware for Windows. Es gibt jedoch einige Besonderheiten zu beachten. Zum einen startet die Installation nach dem Entpacken der Installationsdatei nicht mehr selbsttätig, zum anderen kann Ihr BinTec Router nun in eine bestehende HP-Open View-Installation integriert werden. Weiterhin bietet die Brickware 6.1.2 folgende Merkmale:

- Support für die Bintec X-Series, BIANCA/BRICK, BinGO!, XCENTRIC und NetRACER
- SNMP Manager für BIANCA/BRICK und X-Series und PABX-Configuration der XCENTRIC
- DIME Tools: BootP Server, SysLog Daemon, TFTP Daemon, ISDN Tracer, CAPI Tracer
- Remote CAPI 1.1 und 2.0 als 16 und 32 bit DLLs. Multi-BRICK-Support für Windows NT 4 und 98.
- Remote TAPI: Telephony Service Provider 1.4 und 2.0
- Token Authentication Login Program für die Verwendung von SecurID Token Cards für Bintec BRICK XL.
- Configuration Wizard für die Grundkonfiguration von BIANCA/BRICK XS, BinGO!, BinGO! plus und professional, X1000/1200, X4000 und XCENTRIC
- Activity Monitor für die Bintec Router
- Operator Desk, um Bintec XCENTRIC zu administrieren.
- Power Phone: CTI-Software für XCENTRIC
- Voice Mail Box für XCENTRIC
- QoS-Konfiguration auf X4100

BL6102.x4a 1661 KB

Die aktuelle System Software Version 6.1.2 für die Bintec Router X4000 enthält neue Funktionen:

- Vereinfachte Lizenzierung
- Quality of Service jetzt verfügbar
- neue RADIUS Features
- Unterstützung einer Hardware Encryption
- Multiuser WAN-Partner
- Unterstützung des PPPoE Server Mode
- Keepalive für Multi-Protocol HDLC Framing Verbindungen

Sie bringt folgende Änderungen:

- Bridging und X.25 sind jetzt verfügbar
- HP OpenView Compatibility
- IPX wird nicht länger unterstützt
- Konfigurierbare MTU und MRU Werte
- Interface wird geblockt, wenn eine inkonsistente Encryption Konfiguration vorliegt
- neues Activity Monitor Password
- Discarding Link Level Broadcast Packets

Die Bugfixes betreffen:

- RADIUS Fehler wurden behoben
- PPTP: Memory Leakage Removed
- PPPoE Probleme mit Credits
- Probleme mit Multilink PPP bei Cisco 4500
- Data Transfer mit DES oder Blowfish Verschlüsselung
- Portscan Fehler auf Port 1723
- ICMP Fragment unreachable Meldungen
- Probleme mit transparentem ISDN-Login
- RFC Kompatibilität bezüglich CHAP Reauthentication
- Calls durch ein PRI Interface sind jetzt möglich
- DDI Called Party Numbers

X4000 Diagnosen

Teil 4: ISDNLogin Service mit Hilfe eines ISDN-Adapters

Von Hardy Schlink

Nach der SNMP-Shell, den Ping- und Telnet-Optionen haben wir die Diagnosemöglichkeiten von Traceroute und IPX Ping kennengelernt. Außerdem haben wir das Kommando Minipad vorgestellt. Diesmal bemühen wir das ISDNLogin Utility zur Fehlersuche und Diagnose auf dem Workgroup Access Router X4000.

Sicherlich ist es Ihnen auch schon einmal passiert, daß Sie gerade keinen BinTec-Router zur Verfügung hatten, um sich remote auf das entsprechende Gegenüber einwählen zu können, um dort gewisse administrative Aufgaben durchzuführen. Hier existiert eine Lösung, die wir Ihnen anhand eines Beispiels mit einer AVM ISDN-Karte erläutern möchten.

Remote-Login

Voraussetzung für das Remote-Login in einen BinTec Router mit einer ISDN-Karte ist, daß Sie vorher das Incoming Call Answering oder das PABX Menü für den ISDNLogin Service korrekt eingerichtet haben. Hierunter versteht man, daß dem ISDNLogin Service eine eigene Rufnummer zugewiesen wurde, unter der er zu erreichen ist. Unser Beispiel verwendet das Hyperterminal Programm unter Windows 2000 Professional. Das Beispiel kann jedoch auf andere Microsoft Betriebssysteme übertragen werden. Bevor wir mit der

HINWEIS:

CAPI-Treiber für AVM-Karten finden Sie unter `www.avm.de/de/download/index.php3`. Dort gehen Sie auf den FTP-Server und laden sich die zur Ihrer ISDN-Karte gehörigen Treiber. Auf dem FTP-Server finden Sie CAPI-Port Treiber für verschiedene Betriebssysteme.

Konfiguration des Hyperterminals beginnen, muß sichergestellt sein, daß der ISDN-Adapter - in unserem Fall ein AVM B1 - korrekt in das Betriebssystem eingebunden wurde und ordnungsgemäß funktioniert. Weiterhin ist die vorherige Installation des CAPI-Port Treiber für das entsprechende Operatingsystem durchzuführen.

Konfiguration

Starten Sie das Programm Hyperterminal und wählen Sie in der Menüleiste die Option `Datei / Eigenschaften`. Sollten Sie hierbei feststellen, daß der Menüpunkt `Verbinden über` grau hinterlegt und damit nicht anwählbar ist, so besteht noch eine Verbindung des Hyperterminal Programm zu irgendeiner Gegenstelle. In diesem Fall beenden Sie die Verbindung über die Menüleiste `Anrufen / Trennen`. Selektieren Sie die Option `Verbinden über` mit Hilfe des nach unten zeigenden Pfeils rechts in der Leiste. Hierauf erhalten Sie eine Auswahl aller im System bekannten Modems. Darunter fallen auch “Modems”, die mit Hilfe des AVM CAPI-Port Treiber angelegt wurden. Um die Verbindung mit einem BinTec Router herstellen zu können, wählen wir aus der Liste der existierenden Modems den Eintrag `AVM ISDN – ISDN (X.75)` aus. Wir tragen im dafür vorgesehenen Feld die Rufnummer des Routers ein, mit dem eine Verbindung via ISDNLogin Service hergestellt werden soll (vgl. Abb. 1). In dem Register `Einstellungen` oben rechts wird die entsprechende Terminal-Emulation angegeben, in unserem Fall `VT100`. Wir bestätigen die getätigten Einstellungen über den OK-Button.

Verbinden

Um die Anwahl zum einem Remote-Router zu starten, gehen Sie auf die Menüleiste und wählen den Eintrag `Anrufen/Anrufen`. In dem nun erscheinenden Dialogfeld selektieren Sie noch die Option `wählen` und schon wird die Verbindung zum ge-

Abb. 1: Eigenschaften Hyperterminal Modemprofile

wünschten BinTec-Router aufgebaut. Am besten ist es, vorher nochmals die korrekte Rufnummer zu kontrollieren. Beachten Sie, auch eine eventuell nötige Amtsholung der Rufnummer voranzustellen, falls Ihr PC an einer TK-Anlage angeschlossen sein sollte.Nach kurzer Zeit erscheint die Console des Routers in der gleichen Form, wie Sie es vom Zugang via Telnet oder über serielle Schnittstelle bereits gewohnt sind. Das heißt, Sie müssen den entsprechenden Login-Namen und das Paßwort eingeben und befinden sich anschließend auf der Router-Console, von wo aus Sie beispielsweise das Setup-Programm starten können.Beendet wird die Connection entweder durch Angabe des Befehls`exit` auf der Console des Routers oder über die Hyperterminal Menüleiste `Anrufen/Trennen`.

Erlaubnis

Sie werden sich - allein aus Sicherheitsgründen - bestimmt schon gefragt haben, ob jeder, der Ihre Rufnummer kennt, auch den ISDNLogin Service benutzen darf, und sich damit vielleicht unberechtigten Zugang verschaffen könnte. Um diese berechtigten Bedenken zu zerstreuen, kann ich Sie nur darauf hinweisen, daß Sie die Möglichkeit haben, durch Erzeugung eines oder mehrerer Einträge in den ISDN-Tables die Rufnummern selbst festzulegen, die überhaupt in der Lage sind, den ISDNLogin-Service zu benutzen. Konfiguriert werden die Rufnummern in der Tabelle `isdnloginAllowtable`, wo die `RemoteNumber`, und die `StkNumber` des entsprechenden ISDN-Controllers des BinTec-Router anzugeben sind, über den das ISDNLogin erfolgen darf. Sie rufen am Promp X4000:>`isdnloginAllowtable` auf und nehmen die entsprechenden Einträge vor (vgl. Tabelle 1). `Inx:` enthält als Index des ersten Eintrag `00`. Die `StkNumber` erhält für den ISDN-Controller des Routers den Eintrag `-1` (alle ISDN-Stacks). Als`RemoteNumber` wird die erlaubte Rufnummer eingegeben, unter `Screening`: `dont_care`.

TIP:

Am komfortabelsten läßt sich ein solcher Eintrag über den Configuration Manager durchführen. Hierbei handelt es sich um ein SNMP-Tool, welches alle SNMP-Tabellen der Brick grafisch darstellt und somit die Verwaltung der BinTec-Router wesentlich vereinfacht. Der Configuration-Manager ist Bestandteil der BrickWare-Software, die Sie über die URL `www.bintec.de` downloaden können.

Rufnummerkonflikt

An der Compu-Shack Hotline werden wir des öfteren gefragt, warum die Verbindung zwischen einem WAN-Partner der Brick und einem DFÜ Netzwerk Remote-User nicht funktioniert. In diesem Fall erscheint in den Messages des Routers die Meldung, daß die Connection abgebrochen wurde, weil der ISDNLogin Service den Call entgegen genommen hat. Sehr wahrscheinlich wurde hier im Incoming Call Answering des ISDN-Interface für den PPP-Routing und ISDNLogin Dienst die gleiche Rufnummer verwendet und der Bearer bei beiden auf `all` eingestellt. Wenn Sie für die beiden Services nur eine Rufnummer zur Verfügung haben, muß wie eingangs in diesem Artikel erläutert, der ISDNLogin mit dem Bearer `voice` und das PPP-Routing mit dem Bearer `data` konfiguriert werden.

Tabelle 1

Inx	StkNumber(*rw)	RemoteNumber(rw)	RemoteSubaddress(rw)	Screening(-rw)
00	-1	4711		dont_care

Tabelle 1: Einträge in der isdnloginAllowtable

Verteilter Druck

Lokale Drucker an Windows NT/2000 Stationen mit NDPS

Das Printer Gateway in den Novell Distributed Print Services kann jeden auf Line Printer Daemon basierenden Druckdienst, der dem Line Printer Protocol Standard entspricht, verwenden. Wir wollen Ihnen beschreiben, wie über NDPS ein lokal angeschlossener Drucker unter Windows NT/2000 eingesetzt werden kann.

Windows Stationen können ihren lokal angeschlossenen Drucker über LPD/LPR (Line Printer Daemon / Line Printer Protocol) im Netzwerk zur Verfügung stellen. Der Vorteil liegt darin, daß man in einem TCP/IP Netzwerk ohne Nprinter, IPX oder den IPX-Kompatibilitätsmodus arbeiten kann. Denn die Novell Distributed Print Services können über das Novell Printer Gateway die LPD-Druckdienste direkt nutzen. Wir möchten Ihnen zeigen, wie man die LPD-Dienste bei Stationen unter Windows NT 4.0 oder 2000 mit Microsoft TCP/IP Druck Server Diensten dazu einrichtet.

Druckdienste

Als erstes ist zu beachten, daß eine Station, an der ein Drucker angeschlossen ist, am besten mit einer statischen oder permanenten TCP/IP Adresse arbeiten sollte. Wird der Station über DHCP eine TCP/IP Adresse vergeben, ist bei der DHCP-Konfiguration darauf zu achten, daß sie über die verwendete MAC Adresse immer dieselbe TCP/IP Adresse erhält. Mit einer festen Adresse können die LPD-Druckdienste arbeiten. Ändert sich die TCP/IP Adresse, muß der NDPS Druckeragent neu konfiguriert und gestartet werden.

Unter NT 4.0

Zum Installieren der Microsoft TCP/IP Druckdienste auf Windows NT 4.0 Arbeitsstationen oder Servern gehen Sie über `Start/Einstellungen / Systemsteuerung` auf `Netzwerk` und dann auf die Dienste. Verwenden Sie den Punkt `Hinzufügen` und wählen Sie `Microsoft TCP/IP Printing`. Sie bestätigen mit `OK`. Um den Dienst zu installieren, benötigt Windows Zugriff auf die Dateien im Verzeichnis `i386\` auf der Windows NT CD-ROM. Wurde der Dienst hinzugefügt, werden Sie nach Ihrem `OK` dazu aufgefordert, die Station neu zu starten. Nach dem Neustart muß das aktuell verwendete Service Pack wieder installiert werden, da ja nun wieder ältere Dateien von der Original NT CD-ROM auf das System kopiert wurden, und natürlich muß danach auch wieder neu gestartet werden. Öffnen Sie über die Systemsteuerung abermals die Einstellungen für die Dienste und markieren Sie den Microsoft TCP/IP Druckserver Dienst. Damit er beim Starten in Zukunft automatisch aktiviert wird, klicken Sie auf Starttyp und wählen Sie `Automatisch`, dann auf `OK`, um die Einstellungen zu bestätigen. Um den Dienst jetzt ohne Neustart zu aktivieren, können Sie den Startschalter verwenden, wenn Sie den TCP/IP Druck Server Dienst markiert haben. Der Dienststatus muß dann auf `Gestartet` wechseln. Sollte das nicht der Fall sein, überprüfen Sie das Ereignisprotokoll auf diesbezügliche Fehlermeldungen.

Unter Windows 2000

Zur Installation auf Arbeitsstationen mit Windows 2000 Professional oder Windows 2000 Servern müssen die Druckdienste für Unix installiert werden. Öffnen Sie unter der `Systemsteuerung` den Menüpunkt `Software`. Gehen Sie dort auf der linken Seite auf `Windows Komponenten hinzufügen/entfernen` und auf der dann angezeigten Liste nach unten. Sie markieren den Eintrag "`weitere Datei und Druckdienste für das Netzwerk`, gehen auf Details und stellen sicher, daß `Druckdienste für Unix` ausgewählt ist. Nach Ihrem `OK` wird die Windows 2000 CD verlangt. Mit `Fertig stellen` kehren Sie in das Software-Fenster zurück und schlie-

Abb. 1: Eigenschaften des Druckservers

ßen es. Ein Neustart ist unter Windows 2000 zwar in den meisten Fällen nicht notwendig, doch muß auch hier das Service Pack wieder neu installiert werden. Aber dann ist der Neustart fällig.Starten Sie nun unter der `Systemsteuerung`die`Verwaltung` der `Dienste` und stellen Sie dort für den`TCP/IP Druckserver (LPD SVC)` den Starttyp auf`Automatisch`, damit er zukünftig immer mit gestartet wird. Sollte der Dienststatus nicht auf `Gestartet` wechseln, so schauen Sie ins Ereignisprotokoll, um die Ursache zu finden.

Druck für alle

Kommen wir zur Konfiguration, um den Windows Drucker über den Druckserver (LPDSVC) allen Stationen im Netz zur Verfügung zu stellen. Wir werden dazu einen NDPS Druckeragenten anlegen, der auf den Drucker

HINWEIS:

In der Spezifikation des LPD Protokolls (RFC1179) ist festgelegt, das der Druckername keine Leerzeichen enthalten darf, da diese als Abgrenzung für Kommandos verstanden werden. Das bedeutet, daß einer der beiden Namen - der Windows Druckername oder der Freigabename - keine Leerzeichen enthalten darf, damit der TCP/IP Druck-Server Dienst die LPR Anforderung erfolgreich an den Drucker weiterleiten kann.

der Arbeitsstation verweist. Der Microsoft TCP/IP Druckserver Dienst überprüft den Druckernamen der eingehenden LPR Anforderungen mit dem Namen des Druckers, der in Windows installiert und angezeigt wird, z.B. `Lager LaserJet X`. Er ist aber auch einverstanden mit dem Freigabenamen des Druckers, der an der Arbeitsstation installiert ist, z.B. `\\LageristenStation\Lager-Laser`.

Keine Blanks

Die einfachste Methode, um den LPD-Dienst für einen vorhandenen Windows Drucker zu aktivieren, ist eine einfache Freigabe des Druckers an der Arbeitsstation. Gehen Sie dazu über `Start` auf `Drucker` und die Eigenschaften des Freizugebenden Druckers. Sie aktivieren unter`Freigabe` den Punkt `Freigabe als`. Standardmäßig hat der generierte Name immer nur acht Zeichen und enthältkeine Leerzeichen, um ihn mit LPD-Diensten verwenden zu können. Achten Sie bei neu anzulegenden Druckern von vornherein darauf, aber auch dann, wenn Sie den Namen ändern sollten.

Maximal acht

Die LPD Protokoll Spezifikation enthält keine spezifische Grenze über die Länge des Namens, der verwendet wird. Die NDPS Konfiguration für den Dialog mit dem LPR Drucker Namen ist limitiert auf 64 Zeichen. Die Windows Anzeigenamen können sehr lang werden, jedoch gibt es ältere Applikationen, die nicht mit mehr als 30 Zeichen arbeiten können. Der Windows NT Freigabename ist auf 80 Zeichen limitiert. Es kann aber auch noch andere, meist ältere LPR Clients geben, die höchstens mit acht Zeichen arbeiten können. Um die maximale Kompatibilität zu gewährleisten, ist es also in heterogenen Umgebungen am sichersten, Druckernamen generell auf acht Zeichen zu begrenzen. Druckernamen mit 20 Zeichen wurden mit NDPS auf NetWare 5.1 SP2 und Windows NT 4.0 SP6a erfolgreich getestet.

NDPS Agent

Der NDPS Agent, der über das Novell Printer Gateway mit der Windows Arbeitsstation verbunden wird, welche LPR verwendet, kann ein Druckeragent für Controlled Access oder Public Access sein. Von einem Server oder einer Arbeitsstation mit NDPS Unterstützung wird mittels `NWAdmin32.exe` als erstes in dem gewünschtem Container ein NDPS Druckerobjekt erzeugt, indem Sie den Container markieren, mit der rechten Maustaste über `Anlegen NDPS Drucker` auswählen und dann den Namen des Druckers eintragen. Dies ist der NDS-Name des Druckerobjektes und der kann auch Leerzeichen enthalten, im Gegensatz zu den oben erwähnten Windows Drukker- und Freigabenamen. Aber warum sollte er das, wenn es nur Verwirrung stiftet?

NDPS Manager

Als nächstes ist der NDPS Manager auszuwählen, für den Sie den NDPS Druckeragent anlegen möchten. In der Sektion `Gateway Typ` müssen Sie dazu das `Novell Drucker Gateway` auswählen. Im folgenden Dialog `NDPS Drucker Agent konfigurieren`kann unter`Drukker Typ` über `(Generic)PCL` oder`(Generic)PS`die Sprachunterstützung eingestellt werden, die sich allerdings nur auf die Sprache im Banner auswirkt, wenn dieses verwendet wird. Man kann es also auch bei `None` belassen.

Die Standardeinstellung bezüglich des Port Handler Typs kann auf `Novell Port Handler` stehenbleiben. Anschließend muß beim Konfigurieren des`Port Handlers für den Drucker Agent` der Punkt `Remote (LPR on IP)` ausgewählt werden. Im nächsten Dialogfeld muß die IP-Adresse der Arbeitsstation eingetragen werden, oder der DNS-Name der IP-Adresse, die aber dann aufgelöst wird. Deshalb ist es am besten, eine feste IP Adresse zu vergeben, da sonst bei Änderungen neu konfiguriert werden muß. In dem Feld`Drucker Namen` muß der

Windows Druckername eingetragen werden bzw. der Freigabename, wie erwähnt ohne Leerzeichen.

Druckertreiber

An dieser Stelle wartet der NDPS Druckeragentdialog, bis der neue NDPS Druckeragent gestartet ist. Wurde versehentlich doch ein Leerzeichen mit angegeben, wird der Novell Drucker Gateway Port Handler, das `PH.NLM`, sich nicht laden, da es Blanks als falsche Kommandozeilenparameter interpretiert. Ist der NDPS Druckeragent erfolgreich gestartet, erscheint ein Dialogfenster, in dem Sie den verwendeten Druckertreiber für die jeweiligen Betriebssysteme auswählen können.
Von einer Arbeitsstation mit installierter NDPS Unterstützung kann jetzt der neue NDPS Drucker eingerichtet werden. Wurde ein standardmäßiger Druckertreiber für die Windows Version ausgewählt, als der NDPS Druckeragent angelegt wurde, installiert sich der Treiber nun automatisch. Ansonsten werden Sie an dieser Stelle gefragt, welcher Treiber installiert werden soll. Mit dem Ausdruck einer Testseite - über den LPD Dienst von dieser NDPS Client Station an den ausgewählten lokalen Windows Drukker gesendet, ist die Installation abgeschlossen.

Knackpunkte

Wenn der Microsoft TCP/IP Druckserver Dienst an der Arbeitsstation nicht läuft, kann kein Benutzer mit diesen Drucker arbeiten. Es kommt zu einem I/O Error im Druckerstatus des NDPS Managers. Die Auslastung des Servers steigt an, da der Port Handler versucht, die Verbindung zur Arbeitsstation wiederherzustellen. Sollte die Station, an der der Drucker angeschlossen ist, für längere Zeit ausgeschaltet sein, ist es notwendig, den zugeordneten Druckeragenten für diese Zeit auszuschalten.

Spooling

Beachten Sie, daß der LPDSVC Dienst, der auf der Arbeitsstation läuft, den Druckauftrag auch lokal auf dieser Station spoolt. Die Tatsache, daß NDPS den Auftrag erfolgreich über LPR an die Windows Station übertragen hat, bedeutet nicht, daß der Auftrag auch erfolgreich ausgedruckt wurde. Dies ist ein bedeutsamer Unterschied zu der Arbeitsweise von Nprinter, wo der On-Line oder Off-Line Status des Druckers Aufträge daran hindert, den serverseitigen Spooler-Bereich zu verlassen, wenn er nicht gedruckt wurde.
Auch wenn der Druckauftrag lokal auf der Windows Station gespoolt wird, bedeutet das nicht, daß der Auftrag vom Windows Druckertreiber, der sich auf der NT oder Windows 2000 Station mit dem angeschlossenen lokalen Drucker befindet, nochmals verarbeitet wird. Die NDPS Client Arbeitsstation, die den Druckauftrag sendet, benötigt den Druckertreiber, der dem angeschlossenen Drucker entspricht.

Außen vor

Windows 95, 98 und Millennium Edition werden nicht mit einer Unterstützung für den LPD Dienst ausgeliefert. Das bedeutet, daß hieran angeschlossene Drucker nicht standardmäßig als NDPS Drucker verwendet werden können. Jedoch gibt es entsprechende Software von Drittanbietern, die LPD Dienste für diese Windows Versionen vertreiben.

Netware FAQ

Kleine Novell Server Tips

NetWare Client für Windows XP

Novell hatte in der TID 10061913 ursprünglich eine Beschreibung, wie die Installation des Client32 v4.8 unter Windows XP funktioniert. Mittlerweile enthält diese aber nur den Hinweis, daß es noch keinen Client für XP gibt und der öffentliche Betatest des Clients für Windows XP Professional erst Ende Oktober 2001 beginnt. Der Client 4.81 von NetWare 6 verweigert den Betrieb unter Windows XP komplett. Die Home Edition von Windows XP wird nach bisherigen Aussagen gar nicht unterstützt. Zu Ihrer Warnung sei deshalb gleich gesagt: Der folgende Tip dazu wird von Novell nicht supported, und ich kann auch keine Garantie für den fehlerfreien Betrieb in allen Systemumgebungen geben.

Sie sind gewarnt!

1. Download und Entpacken des Client32 v4.8 (optional inkl. Kopieren der SP3 Updatefiles über diese Dateien),
2. unter `Systemsteuerung / Netzwerkverbindungen` rechter Mausklick auf die aktuelle LAN-Verbindung und `Eigenschaften` auswählen,
3. den Install-Button drücken, dann auf die Einstellung `Client` achten und `hinzufügen` auswählen,
4. `Diskette` auswählen und durchsuchen,
5. das `Verzeichnis` mit dem entpackten Client32 v4.8 und dort das Verzeichnis `winnt/i386/nls/english` auswählen und `Öffnen`.
6. Bestätigen Sie die folgende Warnung, daß der `Novell Client for Windows 2000` nicht signiert ist, und die Installation startet.
7. Nach dem Neustart optional Konfigurationsänderungen durchführen
8. Nach Abschluß der Installation kann NDPS und der Workstation Manager mit Hilfe der gleichen Schritte installiert werden, nur daß in Schritt 3 `Dienste` statt `Client` ausgewählt werden muß.

Interna

Teil 5: TCP/IP Debug-Kommandos unter Novell NetWare

Von Jörg Marx

Wir wollten uns für einen möglichen Fehlerfall mit dem IP-Stack der NetWare auseinandersetzen. Nachdem wir das letzte Mal die zahlreichen SET-Parameter der NetWare kennengelernt haben, wenden wir uns als nächstes ihren Debug Kommandos zu.

Die SET-Parameter beinhalten zahlreiche Debug-Befehle, die für die Fehlersuche und -protokollierung von Interesse sind. Die Syntax lautet wie üblich `SET` <command> = <mode>. Wir haben den Wertebereich und den Default jeweils mit angegeben.

`SET TCP IP DEBUG`

Wenn Sie mit dem Parameter `1` das TCP/IP-Debugging aktiv schalten, werden alle ein- und ausgehenden IP-Pakete mit protokolliert. Der Parameter findet Anwendung bei Problemen mit Paket Translation, Filterung und Connections. Da die Informationen direkt über den Netware Console Screen laufen, und das recht zügig, wird eine Auswertung an dieser Stelle sehr schwer. Das das `CONLOG.nlm` zu laden und dann das Debugging zu aktivieren ist ein einfacher Weg, um die Informationen in einer Datei mit zu protokollieren. Mit `UNLOAD CONLOG` schreiben Sie die Datei `CONLOG.log` in das Verzeichnis `SYS:\ETC`, um sie anschließend in Ruhe durchzusehen. (Schalter: `0/1`, Default = 0)

`SET TCP SOCKET DEBUG`

Mit diesem Parameter können Sie RAW Sockets Informationen mitschneiden. Die unterschiedlichen Werte haben folgende Bedeutung. Mode 1 zeigt Basis Informationen an der Server Konsole, Mode 2 schreibt sie zusätzlich auch in die Datei `SYS:\ETC\TCPIP.log`. Mode 3 zeigt erweiterte Informationen an der Server Konsole, Mode 4 schreibt sie zusätzlich auch in die Datei `SYS:\ETC\TCPIP.log`. (Wertebereich: 0 bis 4, Default = 0)

SET TCP TRACE

Um den aktuellen Stand der TCP/IP Connection Table zu erfahren, zeigt Mode 1 Basis Informationen an der Server Konsole an, Mode 2 schreibt sie zusätzlich auch in die Datei `SYS:\ETC\TCPxxxx.log`, wobei `xxxx` beginnend mit `0000` hochgezählt wird. (Wertebereich: 0 bis 4, Default = 0)

Beispiel

Der Befehl `SET TCP TRACE = 2` verlangt Informationen auf der Server-Konsole und schreibt sie im Hintergrund in die Protokolldatei `TCP0000.LOG`. Anschließend führt ein FTP-Request zum NetWare FTP-Server mit der IP-Adresse `193.97.18.100` mit folgender Bildschirmausgabe:

```
c:\win\home\admin>ftp 193.97.18.100
Connected to 193.97.18.100.
220 sjf-ts-paddy FTP server (NetWare v4.11) ready.
User (193.97.18.100:(none)):
331 Password required for (none).
Password:
500 „PASS „: command not understood.
Login failed.
ftp> quit
221 Goodbye.
```

Das Ganze sieht im Log-File anschließend so aus:

```
Output  of  TCP0000.LOG  file:-
Trace started: Wed Mar 21 19:32:40 2001
Tracing 193.97.18.100.21 <–> 193.97.18.1.1129
R 0 ms ––S- SEQ 01A8D1D7 ACK 00000000 LEN 0 WIN 8192 URG 0
S 0 ms -A–S- SEQ 006E37A0 ACK 01A8D1D8 LEN 0 WIN 32768 URG 0
R 56 ms -A–– SEQ 01A8D1D8 ACK 006E37A1 LEN 0 WIN 8760 URG 0
S 0 ms -AP– SEQ 006E37A1 ACK 01A8D1D8 LEN 52 WIN 32768 URG 0
R 112 ms -A–– SEQ 01A8D1D8 ACK 006E37D5 LEN 0 WIN 8708 URG 0
R 1344 ms -AP– SEQ 01A8D1D8 ACK 006E37D5 LEN 13 WIN 8708 URG 0
S 0 ms -AP– SEQ 006E37D5 ACK 01A8D1E5 LEN 35 WIN 32755 URG 0
R 168 ms -A–– SEQ 01A8D1E5 ACK 006E37F8 LEN 0 WIN 8673 URG 0
R 336 ms -AP– SEQ 01A8D1E5 ACK 006E37F8 LEN 7 WIN 8673 URG 0
S 0 ms -AP– SEQ 006E37F8 ACK 01A8D1EC LEN 38 WIN 32748 URG 0
R 168 ms -A–– SEQ 01A8D1EC ACK 006E381E LEN 0 WIN 8635 URG 0
R 2576 ms -AP– SEQ 01A8D1EC ACK 006E381E LEN 6 WIN 8635 URG 0
S 0 ms -AP– SEQ 006E381E ACK 01A8D1F2 LEN 14 WIN 32742 URG 0
S 0 ms -A-R– SEQ 006E382C ACK 01A8D1F2 LEN 0 WIN 32742 URG 0
```

SET TCP ARP DEBUG

Dieser Parameter wird meistens vom Tech-Support von Novell verwendet (Wertebereich ON/OFF, Default = OFF). Es werden ECB-Informationen im Zusammenhang mit ARP-Pakten mitgeschnitten. Benötigt werden sie meist dann, wenn Server-Abends im Zusammenhang mit dem ARP-Prozeß stehen. Ein Auswerten dieser Informationen ist nicht unbedingt von jedem CNE durchzuführen. Das wird an einem Beispiel klar:

`- bind ip ne2000 addr=193.97.18.100`

Die Server-Karte verwendet den NE2000 LAN Treiber:

```
1. Novell NE2000 using Slot 65535, I/O ports 300h to 31Fh, Interrupt 3h, Frame type: ETHERNET_802.2
2. Novell NE2000 using Slot 65535, I/O ports 300h to 31Fh, Interrupt 3h, Frame type: ETHERNET_II
Select board to bind: 2
TCPIP-4.0-112: Bound to board 3 with IP address 193.97.18.100 and mask FF.FF.FF.0.
```

Debug Infos wie folgt:

```
TCPIP:**** ARPNewMapping: Sending ECB *****
ecb_pt=0x20919E0, ueb_data_ln=28, block_ct=0x1ueb_done_anr=0xF1216806,
ueb_done_ctx=0x2718158datablock=0x2091A1C, len=0x1C
IP LAN protocol bound to Novell NE2000
```

SET TCP ECB DEBUG
Wertebereich 0 –4 (default = 0)
Zeigt ECBs bezüglich des IP_SEND bevor Daten gesendet werden. Wird verwendet zur Fehlersuche bei TCP Server Abends und/oder Problemen mit der IP Fragmentation.

SET TCP IPCP DEBUG
Zeigt alle Informationen bezüglich des IPCP-Protokolls. Es dient zur Aushandlung der IP-Parameter auf einer PPP-Verbindung auf einem Netware Server mit Multiprotokoll Router. (Wertebereich 0 bis 4, Default = 0)

SET TCP RIP DEBUG
Hiermit lassen sich TCP/IP RIP-Informationen auf der Server Konsole protokollieren. Mode 1 zeigt RIP-Send Informationen auf der Server Konsole. Im Mode 2 wird der Vorgang durch ein `load conlog` und `unload conlog` zusätzlich in die Datei `SYS:\ETC\CONSOLE.log` geschrieben.
Mode 3 zeigt RIP-Send und -Receive Informationen auf der Server Konsole, während Mode 4 sie wieder in die Logdatei schreibt.
(Wertebereich 0 bis 4, Default = 0)

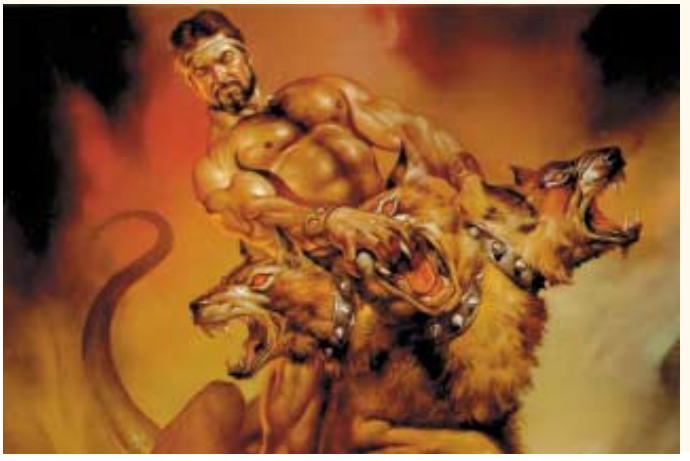
Beispiel

```
TCPIP:RIPSendResponse: ecb_pt 0x26ee158, version 0x1, rif_pt 0x20a0e30, destination 0x0port  0x0
TCPIP:RIPSend with ecb 0x26ee158, version 0x1, rif_pt 0x20a0e30, destination 0x0, port 0x0 (Board 3)
TCPIP:Sending ECB to UDPSendTOIF rif_pt is 0x20a0e30 (Board 3)
TCPIP:RIPSend->UDPSendToIF ecb_pt=0x26EE158, ueb_data_ln=52, block_ct=0x1ueb_done_anr=0xF03C4B70,
ueb_done_ctx=0x50544620datablock=0x26EE194, len=0x34
```

SET TCP WAN DEBUG
Wenn ein WAN-Call über einen Multiprotokoll Router aufgebaut wird, zeigt dieser Befehl alle IP-Informationen auf der Server Konsole an (Wertebereich 0 bis 4, Default =0).

KLEINER TIP ZU KERBEROS

Administrationstools



Es gibt zwei interessante Tools zur Administration von Kerberos v5 erwähnt. Zum einen können Sie mit dem noch aus NT 4.0 Zeiten bekannten Tool Netdom.exe jetzt auch Domänenserver und Trusts überprüfen und transitive Kerberos v5 Trusts zurücksetzen. Neu ist das Tool Kerbtray.exe, mit dem Sie sich Ticketinformationen zum Computer anzeigen lassen können.

Mit ihm kann der Ticketcache ausgelesen und auch gelöscht werden. Das Tool hinterlegt sich als Icon in der Systemicon-Ablage der Startleiste unten rechts.

Bis zum Platzen

Impressionen, Depressionen und Kompressionen

Von Christian Haufe

Gelöschte Dateien auf einem NetWare-Server werden aufbewahrt, solange noch Platz auf dem jeweiligen Volume ist. Ihre Wiederherstellung ist für den Administrator sowie berechtigte Personen über Salvage bis dahin jederzeit möglich. Aus Sicherheits- oder Speicherplatzgründen kann man diese Dateien mit Purge auch ganz löschen. Eigentlich eine feine Sache. Aber es gibt einen Haken, wie immer, wenn der Platz fehlt.

Das NetWare-Datei-System wird mit Dateieinträgen aufbewahrter, gelöschter Files sehr belastet. Das merkt man beim Hochfahren des Servers. Das Mounten dauert eine halbe Ewigkeit. Außerdem wird eine Unmenge Hauptspeicher vergeudet, denn NetWare merkt sich die Dateieinträge in einer Hash-Tabelle im Hauptspeicher. Das kann ältere NetWare-Systeme bis einschließlich 4.2 sogar zum Erliegen bringen, denn der Hauptspeicher wird beim Hochfahren des Servers statisch nach vorprogrammierten Regeln verteilt und reicht unter Umständen irgendwann nicht mehr aus. Ich habe es in diesen Fällen noch nie geschafft, über Änderungen der Server-Parameter einen solchen Server wieder zum Leben zu erwekken. Es half nur noch ein eingeschränkter Start des Servers, z.B. nicht alle Volumes zu mounten oder die `autoexec.ncf` nicht auszuführen. Aus purer Verzweiflung hatten wir in einem kritischen Fall den Server "notgestartet", das Volume `Sys:` auf Band gesichert, dieses weitestgehend gelöscht und "gepurged" und dann vom Band rückgesichert. Doch unglücklicherweise sichert z.B. ARCserve auch gelöschte Dateien, so daß die Mühe von etlichen Stunden für ein Dateivolumen von einigen GB völlig umsonst war.

Die Lösung ist `purge SYS: /A` aus `Toolbox.nlm`: mit `etbox.exe` von `support.novell.com` auszupakken und nach `SYS:SYSTEM` zu kopieren, dann `load toolbox.nlm` einzugeben. In Verbindung mit `cron.nlm` - ebenfalls unter `support.novell.com` zu finden - kann man das Beseitigen gelöschter Dateien vom Server aus sogar automatisieren, z.B. sonntags. Ein `load cron.nlm` mit dem Eintrag `00 06 * * 0 purge SYS: /AD=30` in der Datei `SYS:ETC\crontab` entfernt sonntags früh um 6 Uhr alle vor 30 und mehr Tagen gelöschten Dateien. Ab damit!

Aufräumarbeiten

Traditionell ist ein NetWare-Server stabil und wartungsarm. Dennoch schleichen sich bedingt durch zahlreiche Zusatzprogramme - insbesondere Datensicherung - Unsicherheiten ein. Dieser Effekt wird mit jedem Servicepack noch verschlimmert. Mancher Server ist hängengeblieben, weil Fehlermeldungen der Datensicherung längere Zeit nicht bearbeitet wurden und die Pufferspeicher übergelaufen sind. Zwar wird der Hauptspeicher automatisch alle 15 Minuten aufgeräumt ("defragmentiert" - Garbage-Collection), aber wenn der Platz knapp wird, hilft auch das nichts. Dann muß man den Server halt booten - natürlich immer im unpassenden Moment. Mit dem `cron.nlm` kann man den NetWare-Server z.B. aber auch vorbeugend räumen: dazu Uhrzeit und `restart.ncf` in `SYS:ETC\crontab` eintragen. Ein `restart` sollte mindestens `down` und `restart server` enthalten, z.B. `load cron.nlm` mit dem Eintrag `00 06 * * 0 restart.ncf` in der Datei `SYS:ETC\crontab`.

Depression

Die Kompression auf einem NetWare-Server ist eine feine Sache und durchaus intelligent gelöst. Dennoch gibt es einige Probleme. Das Verzeichnis `SYS:SYSTEM` sollte auf jeden Fall von der Kompression ausgeschlossen sein. Andernfalls kann es unter vorgeblich "mystischen" Umständen passieren, daß ein seit Monaten laufender Server nach einem stromausfallbedingten Neustart wichtige NLMs nicht entpacken kann. Der Reparaturaufwand ist erheblich. Auch habe ich erlebt, daß ein übereifriger Administrator nach Monaten Untätigkeit ein Virenschutzprogramm über den Server laufen ließ. Dieses hat massenweise komprimierte Dateien entpackt und den Server wegen Festplattenmangels zum Absturz gebracht. Die Dekompression kostet auf jeden Fall Zeit. Doch wird es richtig kritisch, wenn die Datei wegen Kapazitätsmangels nicht dekomprimiert auf der Platte abgelegt werden kann, sondern x-mal dekomprimiert werden muß. Einige Systemdateien vertragen das überhaupt nicht. Grundsätzlich sollte während der Kompression, deren Zeit z.B. über `Servman.nlm` bzw. `Monitor.nlm` einstellbar ist - nichts auf dem Server laufen, kein Virenscanner und keine Datensicherung!

Backup Exec in der Version 8.6

Teil 3: Hinweise zum Thema Wiederherstellung

Wir haben die Installation der aktuellen Backup Exec besprochen und Ihnen Tips zur praktischen Anwendung gegeben. Dieses Mal wollen wir Ihnen weitere Hinweise zum Thema Wiederherstellung geben und unter anderem beschreiben, wie ein Resore der Remote Storage Service-Datenbank zu bewerkstelligen ist.

Wenn Windows 2000 auf einem Server installiert worden ist, oder wenn die Remote Storage Service-Datenbank beschädigt oder gelöscht wurde, so muß die RSS-Datenbank wiederhergestellt werden, bevor Dateien vom Offline-Speicher aufgerufen werden können. Die folgenden Dateien werden zum Wiederherstellen der RSS-Datenbank benötigt. Die strukturierten Speicherdateien `RsEng.col`, `RsFsa.col` und `RsSub.col` befinden sich im Unterverzeichnis `%SystemRoot%\System32\RemoteStorage`, die RSS-Engine-Datenbankdateien im Unterverzeichnis `engdb`. Die Dateisystemagent-Datenbankdateien sind im Unterverzeichnis `FsaDb`.

RSS Restore

Backup Exec enthält die Dateien, die zur Wiederherstellung der RSS-Datenbank benötigt werden, wenn eine Gesamtsicherung des Windows 2000-Servers vorgenommen wird. Sie müssen jedoch das Dienstprogramm `RsTore.exe` zum Wiederherstellen der RSS-Engine-Datenbankdateien benutzen. Die Remotespeicher-Engine sichert die Engine-Jet-Datenbankdateien im Unterverzeichnis `engdb` zum Unterverzeichnis `engdb.bak`. Das Dienstprogramm `RsTore.exe` ist ein Teil des Remotespeicher-Produkts und wird zum Wiederherstellen der Jet-Datenbank von den Sicherungsdateien benutzt. Weitere Informationen zu den Remotespeicher-Datenbanken und dem Dienstprogramm RsTore finden Sie im Abschnitt “Remotespeicher” im Server Operations Guide Ihres Microsoft Windows 2000 Server Resource Kit.

Remotespeicher

So stellen Sie Remotespeicher-Datenbankdateien wieder her. Nachdem Sie sichergestellt haben, daß das Medienmanagement-Teilsystem von Backup Exec vollständig auf dem Windows 2000-Server wiederhergestellt wurde, fahren Sie die Remotespeicher-Dienste herunter. Falls dies noch nicht geschehen ist, sollten Sie nun Backup Exec zum Wiederherstellen der BAK-Dateien zum Remotespeicher-Unterverzeichnis in `%systemroot%\system32\remotestorage` benutzen. Öffnen Sie ein Befehlsaufforderungsfenster und wechseln Sie zum Unterverzeichnis `\remotestorage\engdb` und löschen Sie seinen Inhalt. Führen Sie das Dienstprogramm RsTore aus, um den Inhalts des Unterverzeichnisses `engdb` erneut zu erstellen des aus, indem Sie folgende Anweisung eingeben: `RsTore %systemroot%\system32\remotestorage\engdb.bak` Das Subdirectory `engdb.bak` ist der Standort des Sicherungsunterverzeichnisses. Starten Sie die Remotespeicher-Engine-Dienste. Dadurch werden auch die anderen Remotespeicher-Dienste aktiviert. Diese stellen die strukturierten Speicherdaten automatisch wieder her. Der Remotespeicher-Dateisystemagent stellt sicher, daß ein gültiger Auftrag für die verwalteten Datenträger geplant ist, so daß die Dateisystemagent-Datenbanken wiederhergestellt werden können.

Keine IDR bei SBS5.0

Veritas hat in der letzten Zeit ein Problem entdeckt, das eine erfolgreiche Notfallwiederherstellungen eines Microsoft Small Business Server 2000-Systems mit VERITAS Intelligent Disaster Recovery Option evtl. verhindert. Die SBS-Konsole zeigt bei Zugriff nach IDR MMC Snap-In Fehlermeldung an. Das bedeutet nicht, daß die Daten gefährdet sind, sondern vielmehr die Möglichkeit, die Wiederherstellung des Microsoft Small Business Server 2000-Betriebssystems während eines Intelligent Disaster Recovery-Vorgangs zu automatisieren. Veritas rät Benutzern, die Backup Exec-IDR-Funktion nicht für die automatisierte Wiederherstellung von Systemen unter Microsofts Small Business Server 2000 5.0 einzusetzen. Der Backup Exec-IDR-Vorgang für die automatisierte Wiederherstellung eines Systems unter Microsoft SBS 4.5 ist hiervon nicht betroffen.

Clusterquorum schlägt fehl

Die folgende Fehlermeldung tritt evtl. auf, wenn Sie versuchen, das Clusterquorum remote wiederherzustellen: `Beim Abschluß des Vorgangs auf \\System?State trat ein Fehler auf. Die Datenbank für das Clusterquorum konnte nicht wiederhergestellt werden.` Im Ereignisprotokoll des Medienservers finden Sie weitere Informationen. Um das Clusterquorum in einem solchen Fall wiederherzustellen, führen Sie das Befehlszeilendienstprogramm `CLREST.EXE` auf dem wiederhergestellten System aus. Einzelheiten finden Sie im Abschnitt `Wiederherstellen von Daten zu Clustern` des Administratorhandbuchs.

Bekannte Probleme

Dr. Watson bei Exchange 5.0-Client

Bei Dr. Watson während des Auflistens von Mailboxen unter Exchange 5.0-Client, sollten Sie das Exchange 5.0 Client Service Pack 2 installieren, um dieses Problem zu beheben. Sicherungen, die mit Intelligent Image Option in Backup Exec 8.6 für Windows NT und 2000 erstellt wurden, können nicht mit älteren Versionen der Backup Exec oder dem Microsoft-Sicherungs-Applet wiederhergestellt werden. Um Intelligent Image Option für die Notfallwiederherstellung einzusetzen, müssen alle bootfähigen Medien mit Hilfe von Backup Exec 8.6 oder höher erstellt werden.

OFO schlägt bei Whistler fehl

OFO ist mit Windows Whistler einschließlich der Version Beta 2 getestet worden. Das folgende Problem ist beim Aktualisieren von Windows 2000 auf Windows Whistler, auf dem OFO installiert ist, aufgetreten: Bei Sicherungsaufträgen mit OFO, die nach Abschluß der Aktualisierung ausgeführt wurden, erscheint evtl. die Fehlermeldung: `Gerät C:. OFO: Datenträgername ist ungültig oder nicht verfügbar.` Um diesen Fehler zu beheben, sollten Sie die OFO-Komponente von BENT deinstallieren bzw. neu installieren.

HINWEIS:

Zum Problem großer CPU-Belastung durch Winlogon-Prozeß bei der Systemstatuswiederherstellung auf Systemen mit Windows 2000 Service Pack 1 finden Sie Hilfen und aktuelle Details im Microsoft Knowledge Base-Artikel Q272734 (http://support.microsoft.com/support/kb/articles/Q272/7/34.ASP).

RestrictAnonymous

Nicht alle Ressourcen werden bei der Restrict-Anonymous-Einstellung auf Remote Servern aufgeführt Wenn Sie zu Servern wechseln, für die der interaktive Benutzer Rechte besitzt, bei denen jedoch der Registrierungswert `RestrictAnonymous` eingestellt ist, werden einige Ressourcen evtl. nicht aufgeführt. Dies betrifft insbesondere Exchange 2000-Ressourcen, sie werden nicht angezeigt. Es kann sich jedoch auch auf Exchange 5.x- und SQL-Ressourcen auswirken.

Netware FAQ

Kleine Novell Server Tips

REPLACE von NLMs

Zumindest ab NetWare 5.1 ist es möglich, NLMs nicht nur einzeln zu entladen und wieder neu zu laden, sondern mit dem Befehl REPLACE zu "ersetzen". D.h. das bereits geladene - und evtl. nach einem Update veraltete - NLM wird entladen und das neue - bzw. auch die gleiche Version - wird wieder neu geladen.
Dieses Vorgehen bietet sich auch bei Konfigurationsänderungen an, die bei bestimmten Programmen erst nach einem Neustart des Moduls aktiv werden, z.B. DHCP-Server.

FAQs und Facts

Interessante Tips der Deutschen Netware FAQ

Von Stefan Braunstein

Die Deutsche Netware FAQ bietet seit Jahren interessante Tips und eine große Tool-Sammlung rund um Novell NetWare. Stefan Braunstein, der Verwalter der Deutschen Netware FAQ und der Netzwerk-Utility-Sammlung NetwareFiles, liefert Technik-News Lesern eine monatliche Serie seiner Tips und Tricks zu NetWare und zu verwandten Themen.

Policy Manager

Sie sehen einen `PM Status Install` Screen an der Server-Konsole normalerweise nur einmal nach der Installation von NW5SP5. Er ist für Policy Manager Fehlermeldungen zuständig und verschwindet nach dem nächsten Neustart des Servers wieder, wenn der Policy Manager sich richtig registriert hat (siehe Novell TID 10054138). Die möglichen Befehle, mit deren Hilfe Sie weitere Infos über den Policy Manager per Konsole abrufen können, können Sie sich mit `PM HELP` anzeigen lassen. Die Liste ist aber zumindest bei meinem NetWare 5 Server nicht vollständig, wenn ich die Ausgabe mit den möglichen Optionen der genannten TID vergleiche. Vor allem `PM DISPLAY` und `PM STATS` sind interessant, wenn es um die Lizenzverwaltung bei größeren Servern geht.

Die Deutsche Netware FAQ mit ihren wertvollen Tips zu Novell NetWare gibt es auf `www.nwfaq.de`, die große Tool-Sammlung zum Thema unter `www.netwarefiles.de`. Dort finden Sie alle Tools, die hier besprochen werden, und viele andere mehr. Einen direkten Link haben Sie auch über Technik-News online unter `www.technik-news.de`.
Die Texte zu den angesprochenen TIDs (technical information documents) und weitere englischsprachige Informationen zu Fehlern und Fragen finden Sie in der Novell Knowledge Base: `http://support.novell.com/search/kb_index.htm`.

CDROM im Server

In der letzten Ausgabe hatte ich Sie bzgl. des Einsatzes von CD- bzw. DVD-Brennern in einem NetWare Server leider enttäuschen müssen. Doch lassen sich CD- wie auch DVD-Laufwerke relativ problemlos in NetWare Servern einsetzen, um ihren Inhalt allen Benutzern zur Verfügung zu stellen. Sie sollten sich allerdings aus Performance-Gründen überlegen, die komplette CD-ROM auf ein Servervolume zu kopieren. Da die aber schon bei DVD-ROMs erheblich mehr Platz erfordert, hier einige Tips zur korrekten Einbindung.
Für NetWare 3.12, 3.2 und 4.10 ist immer noch der drei Jahre alte Novell Patch `cdup5a.exe` aktuell, den Sie bei Novell und auf der TN-Monats-CD. Eine Weiterentwicklung wird es bei diesen NetWare Versionen aber nicht mehr geben. Für NetWare 3.11 existieren nur sehr alte und fehlerhafte Treiber zur CD-ROM-Unterstützung. Bei allen neueren NetWare Versionen finden sich aktualisierte CDROM.NLMs in den neuesten Support Packs.

HAM Sie alle Treiber?

Achten Sie zunächst darauf, daß kein DOS-Treiber für CD-ROMs auf dem Server geladen ist, weil es sonst Überschneidungen mit dem NetWare-Treiber geben kann. Alle CD-ROM Module unterstützen sowohl SCSI- als auch IDE-CD-ROM, wobei bei letzteren zwingend die mitgelieferten Disk-Treiber im HAM-Standard verwendet werden müssen. Falls Sie noch mit DSK-Treibern - das heißt auch mit SCSI - arbeiten, müssen Sie die Controller-Unterstützung für CD-ROM laden. Diese aktivieren Sie per `LOAD ASPICD`. Bei Netware 3.x muß an dieser Stelle zusätzlich `AFTER311.NLM` per Hand geladen werden.Bei Einsatz von HAM-Treibern sollte deren Unterstützung für CD-ROM bereits beim Laden automatisch mitgeladen werden, wenn ein Laufwerk erkannt wurde. Prüfen Sie mit dem Befehl `MODULES`, ob `IDECD.CDM` bzw. `SCSICD.CDM` vorhanden sind. Jetzt müssen Sie nur noch `NWASPI.CDM` laden, falls dieses nicht bereits für die Streamer-Unterstützung geladen ist. Danach können Sie in beiden Fällen mit `LOAD CDROM` das CD-ROM-Laufwerk aktivieren.

Mind ´n Mount

Mit NetWare 5.x sind Sie jetzt bereits fertig. Sie können jederzeit CDs einlegen und entnehmen. Diese werden automatisch gemountet und wieder dismountet. Bei NetWare 3.x und 4.x können Sie die eingelegte CD-ROM über den Befehl `CD VOLUME LIST` betrachten, mit `CD MOUNT [volume name|volume nummer]` wird die CD-ROM gemountet, mit `CD DISMOUNT` entsprechend wieder dismountet. Vergessen Sie diese Schritte nicht beim Wechseln der CDs! Bei den älteren NetWare Versionen dauert der erste Mountvorgang einer neuen CD-ROM sehr lange und belastet auch den Server. Die normalen Zugriffe und spätere Mountvorgänge sind aber durch das Zwischenspeichern der Verzeichnisinfos recht flott.

Gemappt

Das `CDROM.NLM` von NetWare 3.x und 4.x hat indessen einen Vorteil, mit dem Befehl `CD RENAME` lassen sich Volumes umbenennen. Bei NetWare 5.x können Sie diese Funktionalität nur durch Benutzung des `CDINST. NLM` erreichen, welches zur Installation der NetWare 5.x verwendet wird und das alte `CDROM.NLM` der NW 4.x enthält. Andererseits unterstützt das neue `CDROM. NLM` der NetWare 5.x durch Verwendung der NSS-Module lange Dateinamen auf der CD-ROM und ein sehr schnelles Mounten auch von neu eingelegten CDs. Die neuen CD-Volumes können Sie nun - bei Beachtung des folgenden Tips - wie jedes andere Volume mappen und Benutzern den Zugriff erlauben bzw. verbieten.

Volume nicht angezeigt

Neuerstellte Volumes, vor allem neue CD-Roms, werden nicht automatisch in den NDS Tree eingebunden. `CDROM.NLM` erstellt kein NDS-Objekt für ein neu gemountetes CDROM-Volume.

Laden Sie daher `INSTALL. NLM` bzw. `NWCONFIG. NLM`, wählen Sie dort das Directory-Services Menue aus und dann `upgrade mounted volumes into directory`. Sie müssen sich als Admin anmelden, um die Änderungen in der NDS abzuspeichern. Vergeben Sie anschließend gegebenenfalls mit NWAdmin die gewünschten Zugriffsrechte auf das Volume.

Abb 3: Abfrage des neuen Windows-Paßworts

Keine Fragen, bitte!

Sobald ein neuer Benutzername bei einem NetWare Login an einem Windows 9x Rechner auftaucht, fragt Windows selbst auch nach dem Paßwort (vgl. Abb. 3). Um die Windows Paßwortabfrage zu verhindern, sollten Sie entweder das angebotene Kennwort ganz löschen, das heißt Windows ein leeres Paßwort anbieten, oder mit einem Registry-Eintrag zukünftig dafür sorgen, daß Windows dieses Paßwort gar nicht mehr speichert. Auf keinen Fall jedoch sollten Sie bzw. Ihre Benutzer das Paßwort erneut eintragen. Es wird lokal in der Datei `WINDOWS\username.PWL` gespeichert und ist recht einfach zu knacken. So könnte man ohne großen Aufwand Paßwörter von Admin und anderen Benutzern herausfinden und mißbrauchen. Der Eintrag-Registry lautet: `[HKEY_Local_Machine\Sftware\Microsoft\Windows\CurrentVersion\Policies\Network]` `„DisablePwdCaching“=“1"` `„HideSharePwds“=hex:01,00,00,00,` Alternativ können Sie auch mit `Poledit` unter `lokaler Computer / Netzwerk / Kennwörter` das `disable password ca ching` bzw. `Kennwortver schlüsselung deaktivieren` einstellen und `remote updates` deaktivieren. Außerdem sollte man aus Sicherheitsgründen die bisherigen PWL-Dateien im lokalen Win-dows Verzeichnis löschen, wobei dadurch allerdings auch Paßwörter für DFÜ-Verbindungen, sofern vorhanden, gelöscht werden.

Sie erreichen den Autor Stefan Braunstein über: `www.braunstein.de`.

Abb 1: CD-ROM Unterstützung bei NetWare 5.x

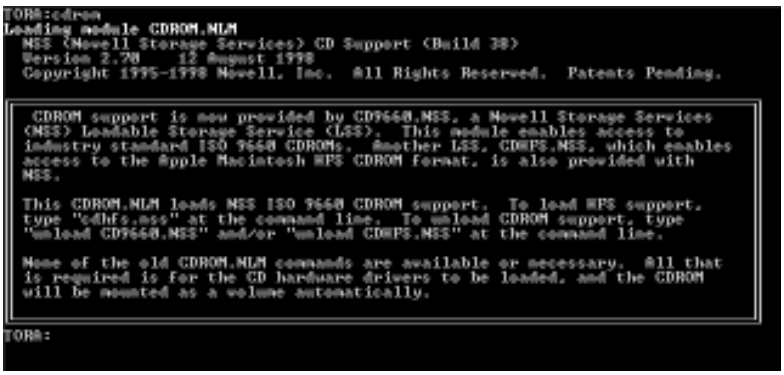
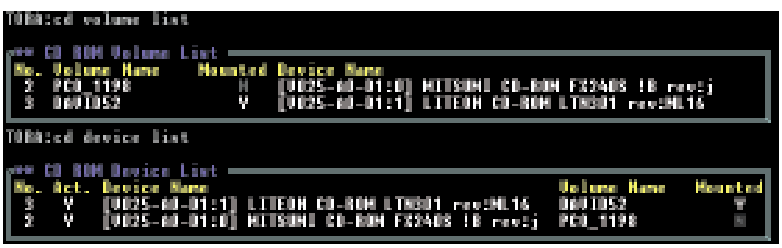


Abb 2: CD-ROM Unterstützung bei NetWare 3.x und 4.x



Business Communications Manager

Teil 1: Installation der Media Bay Modules

Von Hardy Schlink

In der letzten Technik-News haben wir den Business Communications Manager von Nortel Networks ausführlich vorgestellt, einschließlich der verfügbaren Features und Applikationen. Mit dieser Ausgabe starten wir eine neue Serie, in der wir Ihnen deren Einsatz in der Praxis näher bringen möchten. Wir beginnen mit der Installation des BCM und zeigen die erforderlichen Schritte auf, bis die Telefonie zwischen den Systemtelefonen innerhalb des Business Communications Manager funktioniert.

Wenn Sie - wie uns auch - die Kommunikationsvielfalt des Business Communications Manager überzeugt hat und Sie sich entschieden haben, einen solchen Allrounder zu erwerben und einzusetzen, stellen Sie sich natürlich die Frage, wie ein solches Gerät in Betrieb genommen wird. Trotz seiner Komplexität liegen die Hürden gar nicht so hoch. Wir wollen Ihnen am praktischen Beispiel die hierzu notwendigen Schritte im einzelnen erläutern. Eine Installation ist dabei abhängig von der bestellten Konfiguration. Wir gehen in unserem Beispiel von einem System aus, das aus den folgenden Komponenten besteht:

- BCM Chassis
- Software 2.5
- 2 LAN-Adapter
- 1 WAN-Adapter
- 1 Digital Trunk Module E1 (S2M Interface)
- 1 Digital Station Module 16 für den Anschluß von 16 Systemtelefonen.

Im Auslieferungszustand sind im Business Communications Manager die MSC-Card, LAN/WAN Adapter und die Software in der Version 2.5 bereits vorinstalliert. Alles weitere wie der Einbau der einzelnen Module und die Initialisierung des Systems ist Aufgabe des Administrators und sollte in der nun erläuterten Reihenfolge durchgeführt werden.

Media Bay Modules

Zur Installation und Konfiguration der Media Bay Modules sollte Ihnen der sogenannte DS 30 Bus bekannt sein. Dabei handelt es sich um ein internes Bus-System des BCM, dessen Aufgabe es ist, die Kommunikation zwischen den einzelnen Systemkomponenten - wie MSC-Card, LAN/WAN-Adapter, Media Bay Modules etc. - zu ermöglichen.

DS 30 Bus-System

Insgesamt verfügt das DS 30 Bus-System über acht Subsysteme, die bis auf zwei Kanäle den einzelnen Komponenten des Systems zugewiesen werden können. Hierbei gilt es zu beachten, daß die angesprochenen zwei Channels den internen Ressourcen fest zugeordnet sind, und aus diesem Grund nicht mehr den Media Bay Modules zur Verfügung stehen (vgl. Abb. 1). Je nach Konfiguration des DS 30 Bus ist es möglich, entweder fünf oder sechs Kanäle den Media Bay Modules zuzuordnen, hierfür stehen die Begriffe des 2/6 oder 3/5 Split. 2/6 Split meint 2 Channels für interne Ressourcen, 6 für Media Bay Modules, 3/5 Split entsprechend 3 für interne Ressourcen und 5 für die Module.

DIP-Switches

Vor ihrem Einbau müssen die Media Bay Modules über sogenannte DIP-Switches eingestellt werden, um den gewünschten DS 30 Channel zu allokieren. Die DIP-Switches verfügen über 6 Schalter, die sich in die Bereiche `Offset` und `Channel` untergliedern (vgl. Abb. 2). Bestimmte

Module wie das BRI Media Bay Module belegen nur ein Drittel und nicht einen kompletten DS 30 Bus. Hierdurch ist es möglich, drei dieser Module zu installieren, die wiederum nur einen Bus des Systems belegen. Um diese Module im BCM adressieren zu können, verwendet man den sogenannten Offset.
Zur Einstellung des Offsets werden die DIP-Switch Schalter 1 bis 3 verwendet, die Schalter 4 bis 6 dienen der Zuweisung zu einem bestimmten DS 30 Channel. Außerdem wird hier entschieden, welche `Linenumbers` den einzelnen Komponenten zugewiesen werden (vgl. Tab. 1). Die korrekte Einstellung des DIP-Switch Schalter ist also von äußerster Wichtigkeit, da durch Fehlkonfiguration die entsprechenden Module nicht funktionieren.

Initialisierung

Nachdem Sie die Media Bay Modules konfiguriert, in das Chassis eingebaut und den Business Communications Manager mit Strom versorgt haben, fahren wir mit der Initialisierung des Systems fort. Hierbei stehen uns zwei Möglichkeiten zur Auswahl, über die serielle Schnittstelle oder über das LAN-Interface des BCM. In unserem Beispiel wollen wir den Zugriff auf das System über die Ethernet-Schnittstelle verwenden.

Hardware-Profil

Der BCM wird vom Werk aus mit der IP-Adresse `10.10.10.1/255.255.255.0` vorkonfiguriert. Um Zugriff auf das System zu erlangen, verwenden Sie ein Crossover-Kabel zwischen Workstation und BCM und passen Ihren PC dieser IP-Adressierung entsprechend an, z.B. IP-Adresse `10.10.10.2/255.255.255.0`. Nachdem der BCM gebootet hat, können Sie sich über den Befehl `Telnet 10.10.10.1` mit dem Business Communications Manager verbinden. Um sich am System einzuloggen, muß an der Telnet-Console als Benutzername `ee_admin` und als Paßwort `eedge` eingegeben werden, anschließend erscheint das Hauptmenü.
Durch Auswahl der Ziffer `1` gelangen Sie in das Menü `Platform Initialization`. Indem Sie abermals die `1` eingeben, wird das Menü `Hardware Profile` aufgerufen (vgl. Abb. 3). An dieser Stelle müssen Sie für Ihren BCM das entsprechende Hardware-Profil auswählen, welches von der besonderen Hardware-Ausstattung Ihres Geräts abhängig ist.
Verfügt Ihr System über eine MSC-Card, zwei LAN- und einen WAN-Adapter so ist die richtige Wahl hier Profil 3, sind nur die MSC-Card und zwei LAN-Adapter installiert, so muß Profil 4 ausgewählt werden.
Beide Profile sind für die Kommunikation nach europäischen Standards gedacht.

Abb. 1: Das Channel Modell des DS 30 Bus

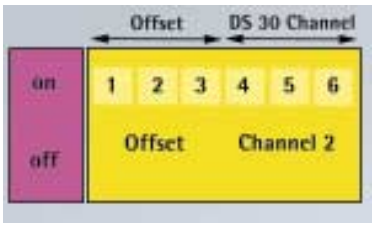


Abb. 2: Bedeutung der Schalter des DIP-Switches

Software Download

Nachdem das entsprechende Hardware-Profil selektiert wurde, findet ein Software-Download von der Festplatte des BCM zur MSC-Card hin statt. Dieser Software-Download sorgt dafür, daß die MSC-Card mit der entsprechenden Core-Software upgedatet wird, damit das System anschließend nach den oben erwähnten europäischen Standards kommunizieren kann.

TIP:

Der Download darf auf keinen Fall beeinträchtigt werden, weder durch Abschalten des BCM oder durch eine Unterbrechung der Stromversorgung. Andernfalls kann es vorkommen, daß sich der BCM nicht mehr initialisieren läßt. Aus diesem Grund ist es zu empfehlen, daß während des Software-Download der Business Communications Manager an ein Notstromgerät angeschlossen wird, um eine absolut sichere Stromversorgung zu garantieren.

Tabelle 1

DS30 Channel	DIP-Switch Einstellung				Zugewiesene Lines		
	1	2	3	4	5	6	
2	on	on	on	on	on	on	211-240
3	on	on	on	on	on	off	181-210
4	on	on	on	on	off	on	151-180
5	on	on	on	on	off	off	121-150
6	on	on	on	off	on	on	91-120
7 *)	on	on	on	off	on	off	61-90

*) Ist das System im 3/5 Split konfiguriert, so ist DS30 Channel 7 nicht verfügbar.

Tabelle 1: DS 30 Channel und Line Numbers

Der Software-Download dauert ca. 45 Minuten. In dieser Zeit dürfen am System keine weiteren Änderungen vorgenommen werden. Die weitere Konfiguration des Business Communications Manager wird nach Abschluß des Downloads mit Hilfe des sogenannten Unified-Managers vorgenommen. Hierbei handelt es sich um ein Web-basierendes Konfigurationstool, welches uns unter anderem verschiedene sogenannte "Setup and Management Wizards" zur Verfügung stellt.

Wizards

Um die "Setup and Management Wizards" zu erreichen, öffnen wir einen Web Browser, z.B. den Microsoft Internet Explorer und geben als URL die Adresse `http://10.10.10.1:6800` an.
Wenn die Haupt-Webpage des Business Communications Manager erscheint, wählen wir die Option `Wizards` und konzentrieren uns zur weiteren Konfiguration des BCM auf den `Quick Start Wizard`. Hierüber werden alle notwendigen Informationen eingetragen, um das System zu initialisieren. Wir erreichen ihn durch Auswahl der entsprechenden Option auf der Webpage `Setup and Management Wizards`. Anschließend öffnet sich ein separates Web-Browser Fenster, wo Sie nach dem Username und dem Paßwort gefragt werden. Als Username wird `supervisor`, als Paßwort `visor` eingegeben, danach wir der Menüpunkt `Quick Start` ausgewählt.

Allgemeine Angaben

Auf der nun erscheinenden Seite mit dem Namen `General` müssen Sie die folgenden allgemeinen Eintragungen tätigen und unter `System Name` den Namen des Business Communications Manager, unter `CallPilot Region` "Germany" und unter `Time Zone` "(GMT+01:00) Brüssel, Berlin, Bern, Rome, Stockholm, Vienna" angeben. Durch Betätigen des Button `Next` gelangen Sie zur nächsten Konfigurationsseite, in der die IP-Adressierung des BCM angepaßt werden kann.

TIP:

Sollte der Web-Browser für die Verwendung eines HTTP-Proxy konfiguriert sein, so entfernen Sie manuell die entsprechenden Einstellungen, da der Zugriff auf die Web-Pages des BCM unter Verwendung eines Proxies nicht funktioniert.

Details

Die nächste Web-Page beinhaltet einige wichtige Detailangaben. `Dect` ist nur dann wichtig, wenn auch ein Dect Media Bay Module zum Einsatz kommt. Unter `Carrier Protocol` ist unbedingt `E1` für Europa anzugeben. Bei `Region` entscheidet `Germany` über die Sprache der Anzeige auf den Telefonen. Nehmen wir als `Template` PBX, so müssen keine weiteren Voreinstellungen durchgeführt werden, im Gegensatz zu `DID`, wo z.B. `DN 221`, `Target Line 241` und `Received Number 221` angegeben werden.
Als `Start DN` wird die erste interne Rufnummer für das System festgelegt. Dies bedeutet, daß die Telefone beginnend mit der Rufnummer `221` adressiert werden: 221, 222, 223, usw. `3/5Split` hängt von der Anzahl der Media Bay Modules ab (siehe oben). Setzen wir `Nortel IP Terminals Registration` auf `On`, sorgen wir dafür, daß IP-Telefone sich registrieren können. Das `Nortel IP Terminals Password` - Default ist 2264 - wird für die Registrierung der IP-Telefone benötigt. `Nortel Term. Auto Assign DNs` sollte auf `Off` stehen, damit Sie selbst entscheiden können, welche Rufnummer das IP-Telefon bekommen soll. Die nächste Seite zeigt uns nun eine Zusammenfassung unserer eingegebenen Informationen an. Durch den Button `Back` erhalten wir die Möglichkeit, sie gegebenenfalls nochmals zu ändern. Durch Selektieren der Option `Apply` wird dann die abschließende Initialisierung des Business Communica-tions Manager durchgeführt.

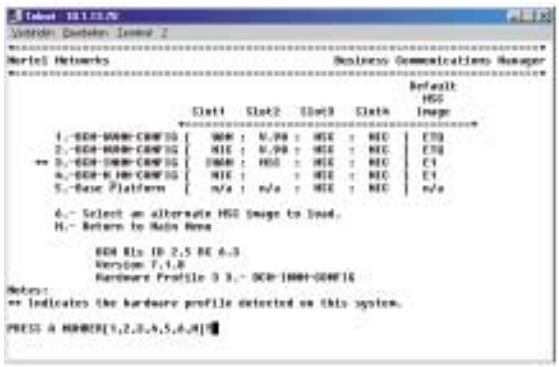
TIP:

Denken Sie daran, nach Abschluß der Initialisierung auch Ihre Workstation an die geänderte IP-Adressierung anzupassen, da ansonsten kein Zugriff mehr auf das System via Web-Browser möglich ist.

Zeitangaben

Die Dauer der Initialisierung kann je nach Konfiguration des Business Communications Manager zwischen 30 Minuten und über eine Stunde dauern. Nachdem dieser Prozeß abgeschlossen ist, sollten wir zunächst noch eine wichtige Änderung am System durchführen, nämlich die korrekte Einstellung der Uhrzeit und des Datums. Diese Aufgabe wird mit dem webbasierenden Tool `Unified Manager` durchgeführt, das über den Configure-Button auf der Main Webpage des BCM ausgeführt wird. Nachdem wir uns im Unified Manager mit dem Username `supervisor` und dem Passwort `visor` wieder angemeldet haben, erscheint die Konfigurationsoberfläche. Hier werden alle

Abb. 3: Menü der Hardware-Profile



weiteren Einstellungen vorgenommen, z.B. die Telefoniefeatures, die Datendienste etc. (vgl. Abb. 5).
Um das Datum und die Uhrzeit korrekt einzustellen, wechseln wir nun auf den Menüpunkt `System / Identification`. Dort finden wir unter anderem die Punkte `Date` und `Time`, die jetzt entsprechend konfiguriert werden. Wichtig ist die richtige Systemzeit allein deshalb, weil sie auf den Telefon-Displays sichtbar wird.

Systemtelefone

Von nun an sind wir in der Lage, mit den angeschlossenen Systemtelefonen interne Anrufe durchzuführen. Sie werden sich jetzt zu Recht fragen, wie denn die Telefone an das System zu installieren sind? Zu diesem Zweck wurden, wie anfangs erwähnt, ein- oder mehrere "Digital Station Media Bay Modules" in den BCM installiert, abhängig von der Anzahl der benötigten Systemtelefone und analogen Devices. Es stehen zwei Module zur Verfügung: DSM 16 und 32 zum Anschluß von bis zu 16 bzw. 32 Systemtelefonen.

DSM 16 Modul

Beim DSM 16 Modul finden wir auf der Vorderseite des Business Communications Manager den sogenannten `Amphenol Connector`, der insgesamt über 25 Adernpaare oder 50 Connectoren verfügt. Für den Anschluß der Systemtelefone und analogen Geräte werden aber nur 16 Adernpaare benutzt (vgl. Tab. 2). Als Gegenpart zum Female Amphenol Connector des DSM 16 Moduls benötigen Sie noch einen Male Connector, dessen Adernpaare wiederum auf ein Patchfeld aufgelegt werden. Somit wird gewährleistet, daß die Verkabelung sich nahtlos in die Infrastruktur des Netzwerkes integriert. Jedes angeschlossene Device benötigt zur Kommunikation mit dem BCM jeweils zwei Adern, die auf dem Patchfeld auf die Pins 4 und 5 aufgelegt werden müssen. Weiterhin ist es wichtig zu wissen, daß es eine physikalische Abhängigkeit zwischen Adernpaar und Rufnummer des Telefons gibt, z.B. verbindet das erste Adernpaar die Rufnummer 221 mit dem daran angeschlossenen Telefon. Hierbei wird vorausgesetzt, daß Sie wie oben beschrieben die `Start DN` im Quick Start Wizard auf `221` festgelegt haben.

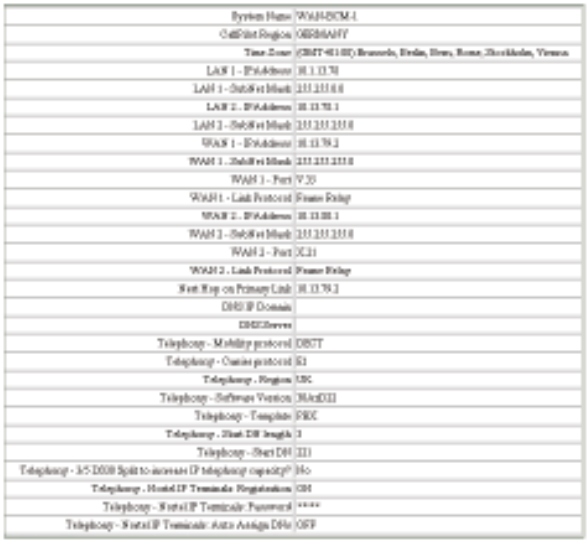


Abb. 4: Zusammenfassung der Information im Quick Start Wizard

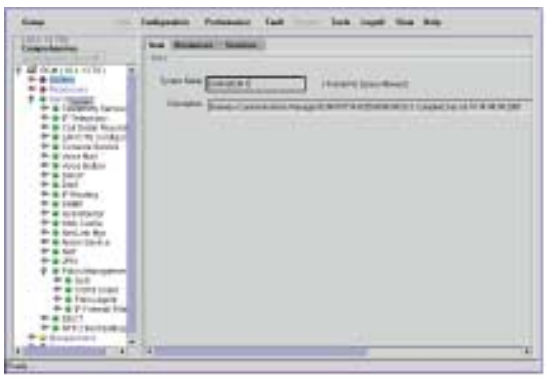
DSM 32 Modul

Die Verdrahtung des DSM 32 Moduls verhält sich im Prinzip genauso wie beim DSM 16, nur stehen hier zum Anschluß der Geräte zwei Amphenol Connectoren zur Verfügung, die jeweils 16, also insgesamt 32 Adernpaare bereitstellen. Damit ist es erforderlich, daß Sie zwei Kabelstränge auf das Patchfeld auflegen, um so die Möglichkeit zu erhalten für 32 Devices eine Kommunikation mit dem BCM zu ermöglichen.
Abschließend müssen wir die Systemtelefone nur noch an ihren Einsatzort aufstellen, und das mitgelieferte Kabel an die entsprechende Buchse des Business Communications Manager anschließen. Nachdem alle benötigten Systemtelefone installiert und der Business Communications Manager gestartet wurde, steht die interne Telefonie zur Verfügung. Wenn Sie nun z.B. von Apparat 222 die Rufnummer 223 wählen, sollte das entsprechende Telefon läuten.

Fazit

Dieser Artikel aus der Praxisserie des Business Communications Manager behandelte die notwendigen Schritte, die erforderlich sind, um das System zu initialisieren und die ersten internen Gespräche führen zu können. Natürlich können Sie auch externe Telefonate mit dem BCM tätigen, die über die sogenannten "Digital Trunk Modules" geroutet werden. Damit der externe Zugriff auf das weltweite Telefonnetz möglich ist, müssen die Module entsprechend konfiguriert werden. Was es hierbei zu beachten gilt, werden wir uns in der nächsten Ausgabe der Technik-News genauer anschauen.

Abb. 5: Die Menüführung des Unified Manager



Novell Modular Authentication Service

Teil 3: Implementierung unterschiedlicher Login-Methoden

Von Johanna Bruder

Bislang haben wir uns in dieser Serie mit der Theorie von NMAS beschäftigt. Wir haben die NMAS-Objekte und deren Bedeutung kennengelernt. Nun können wir dazu übergehen, einzelne Login-Methoden zu implementieren. Wir werden in diesem Artikel die Authentifizierung über ein X509 Zertifikat sowie die Authentifizierung mit Hilfe eines Tokens des Herstellers VASCO, nämlich dem Device Digipass 300, mit NMAS ermöglichen.

Die Implementierung einer Login-Methode erfordert neben der Installation der Methode selber und somit der Installation von SnapIns in die ConsoleOne, einige zusätzliche Schritte. So muß z.B. das einzelne Device in der NDS installiert und dem Benutzer zugeordnet werden. Eventuell muß das Device lokal auf der Workstation installiert werden. Die einzelnen Konfigurationen sind abhängig von dem Device, das Sie in ihrem Unternehmen zur Authentifizierung verwenden möchten.

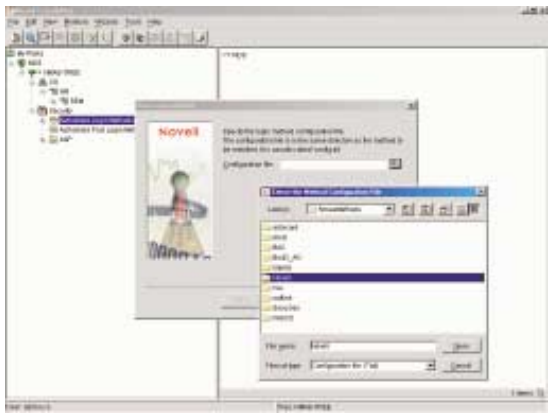
x509 Zertifikat

Möchten Sie NMAS testen, verfügen aber gerade nicht über ein Token oder ein biometric Device? Kein Problem! NMAS bietet Ihnen unter anderem die Möglichkeit, sich mit einem X509 Zertifikat, das Sie z.B. auf einer Diskette speichern können, einzuloggen. Dazu installieren Sie in der NDS die Login-Methode X509 Zertifikat. Anhand dieser einfachen Login-Methode wollen wir zunächst die grundsätzlichen Schritte für die Implementierung einer Methode besprechen.

Installation

Markieren Sie in der ConsoleOne den `Authorized Login Methods` Container und erstellen Sie ein `SAS: NMAS Login Method` Objekt. Im Anschluß daran erscheint das Fenster `New Login Method` und Sie werden aufgefordert, eine Datei `CONFIG.TXT` auszuwählen. Diese Konfigurationsdatei beinhaltet die Einstellungen für die entsprechende Login-Methode. Die Konfigurationsdateien für die meisten Login-Methoden der Hersteller, die NMAS unterstützen (vgl. TN 10/2000) sind auf der NMAS-Installations-CD in dem Verzeichnis NmasMethods abgelegt (vgl. Abb. 1). Für die Installation des X509 Zertifikats wählen Sie die Konfigurationsdatei `CONFIG.TXT` in dem Verzeichnis `Nmas Methods\Novell\X509Cert\`. Nach der Bestätigung der Lizenzbedingungen erscheint ein Fenster wie in Abbildung 2 dargestellt. Dort können Sie lediglich den Namen der Methode ändern. `Vendor` und `Grade` sind vorgegeben und nicht editierbar. Der Grade für diese Art der Authentifizierung ist `Password & Token`. Anschließend wird angezeigt, welche Login-Module in der NDS installiert werden. Schließlich haben Sie die Möglichkeit, außerdem eine Login-Sequenz zu erstellen, die ausschließlich die gerade installierte Methode beinhaltet. Eine Zusammenfassung zeigt, was während der Installation der Login Method durchgeführt bzw. angelegt wurde. In diesem Fall wurden keine SnapIns installiert. Somit muß für die weitere Konfiguration die ConsoleOne nicht neu gestartet werden.

Abb. 1: Wahl der CONFIG.TXT beim Erstellen einer Login-Methode



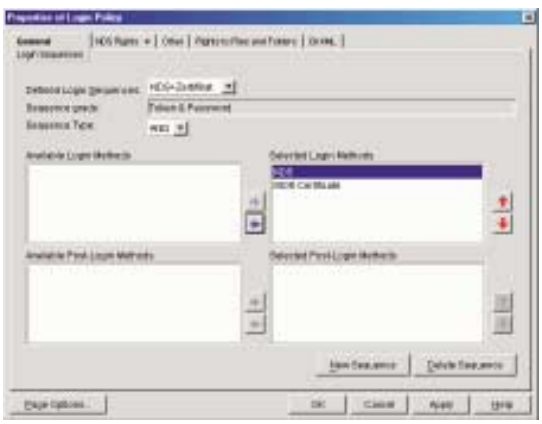
Sequenzen mit mehreren Login-Methoden

Um zu checken, ob nach der Installation der Methode eine Sequenz erstellt wurde, gehen Sie in die Eigenschaften des Login Policy Objekts und wählen den Tab `General Login Sequences`. Dort sollte, wie in Abbildung 3 dargestellt, die Sequenz X509 Certificate erscheinen. Möchten Sie, daß ein Benutzer beim Einloggen zusätzlich zu dem Zertifikat ein Paßwort miteingeben muß, können Sie an der Stelle eine neue Sequenz erstellen, die beide Login-Methoden - NDS und X509 - beinhaltet. Diese Sequenz kann dann ebenfalls vom User beim Login ausgewählt werden. Wählen Sie einfach den Button `New Sequence`, geben Sie der neuen Sequenz einen Namen und ordnen Sie der Sequenz die entsprechenden Login Methoden zu, indem Sie diese von `Available Login Methods` nach `Selected Login Methods` auswählen. Die Reihenfolge der ausgewählten Login-Methoden bestimmt auch die Reihenfolge, in der die einzelnen Methoden beim Einloggen "abgearbeitet" werden müssen. Abbildung 4 zeigt ein Sequenz, die nach einem erfolgreichen Paßwort-Login ein Zertifikat fordert.

Abb. 2: Eigenschaften der X509 Login-Methode

Abb. 3: X509 Certificate Login Sequenz

Abb. 4: Sequenz mit kombinierten Login-Methoden



Benutzerzertifikat

Eine Anforderung an den NetWare Server, auf dem NMAS installiert werden soll, ist der Certificate Server in der Version 2.0. Installieren Sie den ersten Certificate Server in der NDS, wird ein `Certicate Authority` (CA) Objekt in der NDS angelegt. Diese CA kann nun Benutzerzertifikate für Benutzerobjekte in der NDS ausstellen. Im folgenden konzentrieren wir uns auf die Bearbeitungsschritte, die durchgeführt werden müssen, um einem Anwender ein Benutzerzertifikat auf einer Diskette aushändigen zu können.

HINWEIS:

Erklärungen zur Public Key Cryptography (PKI) und Zertifikaten finden Sie im Schwerpunktartikel der TN 4/2000 und den nachfolgenden Praxisbeiträgen zu Encryption. TN 5/2000 behandelte PKI.

TN online: Archiv

In den Eigenschaften eines Benutzerobjekts finden Sie den Punkt `Security – Certificates` oder auch `Sicherheit – Zertifikate`. In diesem Tab können Sie ein Benutzerzertifikat kreieren, das von der CA in dieser NDS signiert wird. Ist das Zertifikat präsent, hat nur noch der Benutzer, auf den das Zertifikat ausgestellt wurde, Zugriff auf den zugehörigen `Private Key`, der zu dem Zertifikat gehört. Selbst der Administrator kann nicht auf den Private Key zugreifen.

TIP:

Besonders einfach kann ein Benutzer sein Zertifikat und den zugehörigen Private Key über das Tool `Certificate Console` aus der NDS exportieren. Die `SETUP.EXE` für dieses Tool befindet sich im Verzeichnis `SYS:\Public\mgmt\ Cert Console`.

Abbildung 5 zeigt den Export eines Benutzerzertifikats inklusive Private Key für das Benutzerobjekt `User` über die `Certificate Console`. Der Benutzer wird aufgefordert, die Datei, die er exportiert, mit einem Paßwort zu versehen.

Login mit Zertifikat

Verfügen Ihre Benutzer nun über ein Zertifikat, das z.B. auf einer Diskette gespeichert ist, und gibt es für diese Login-Methode eine Sequenz, kann der Benutzer diese Sequenz beim Einloggen über einen NMAS-Client auswählen. Er wird dann aufgefordert, das Zertifikat in Form einer PFX-Datei zu lokalisieren. In unserem Beispiel gibt es eine Login Sequenz mit dem Namen`NDS+Zertifikat` (vgl. Abb. 4). Darf der Benutzer diese Sequenz nutzen, d.h. es gibt keine Restriktionen bezüglich dieser Login Sequenz in den Eigenschaften des Benutzerobjekts, so sieht der Login-Vorgang folgendermaßen aus. Der User wählt über den Browser Button `Sequenz` den Eintrag `NDS+Zertifikat` und bestätigt diese Wahl. Dann wird er zunächst - wie gewohnt - nach einem Paßwort gefragt. Wenn dieses mit dem in der NDS übereinstimmt, erscheint der Screen aus Abbildung 6. Der Benutzer muß die Diskette einlegen, den Pfad zu der PFX-Datei sowie das Paßwort für diese Datei angeben. Das war's!

HINWEIS:

Der Benutzer muß beim Einloggen eine Clearance wählen! Tut er das nicht, wird immer die Default Clearance aus den Eigenschaften des Benutzers aktiv, egal welche Sequenz der User zum Authentifizieren gewählt hat.

Zugriffsberechtigungen

Obwohl der Benutzer sich jetzt über das Zertifikat authentisiert hat, dem ja in der NDS der Grade `Password & Token` zugeordnet ist, erscheint nach der Authentifizierung die Graded Authentication Information aus Abbildung 7. Dies bedeutet, daß der Benutzer trotzdem nur den Clearance Level `LoggedIn` hat. Das kommt daher, daß dem Benutzer bislang keine andere Clearance außer LoggedIn, welches die Default Clearance ist, zugeordnet wurde. Mit der Clearance LoggedIn hat der User Lese- und auch Schreibzugriff auf alle Ressourcen, die mit dem Security Label LoggedIn versehen sind. Damit er beim Einloggen die Clearance `Password & Token` wählen kann, müssen Sie als Administrator den Clearance Label in den Eigenschaften des Benutzerobjekts zuordnen. Beim Einloggen kann der User dann die Clearance wählen. Wenn es sich auch dementsprechend einloggt, wird ihm diese Clearance zugeordnet. Welcher Zugriff ihm damit im einzelnen auf Ressourcen gewährt wird, entnehmen Sie dem folgenden Teil dieser Artikelserie.

HINWEIS:

Technische Daten zu den Geräten von VASCO entnehmen Sie der Webseite `www.vasco.com`.

Digipass 300 von VASCO

Der Hersteller VASCO unterstützt NMAS. Es gibt Tokens von VASCO, die eine Authentifizierung in der NDS über NMAS ermöglichen. Für diesen Artikel wurde das Handheld Device Digipass 300 verwendet. Das Gerät ist recht handlich und ähnelt einem Taschenrechner. Es erzeugt einen Zahlencode als Paßwort, der nur für eine kurze Zeit zur Authentifizierung im Netzwerk genutzt werden kann. Diese Lösung basiert auf einer sogenannten "Strong two Factor Authentication". Der Benutzer benötigt zunächst eine PIN, um das Digipass Gerät überhaupt nutzen zu können. Dann erzeugt Device das "One Time Password", das eine Authentifizierung im Netzwerk erlaubt.

Installation

Die Konfigurationsdatei `CONFIG.TXT` für das VASCO Device Digipass 300 wird mit NMAS mitgeliefert. Sie erstellen also im Authorized Login Methods Container ein neues Login Method Objekt und verweisen dabei auf die genannte `CONFIG.TXT` im Verzeichnis `NmasMethods\`

Abb. 5: Export über die Certificate Console

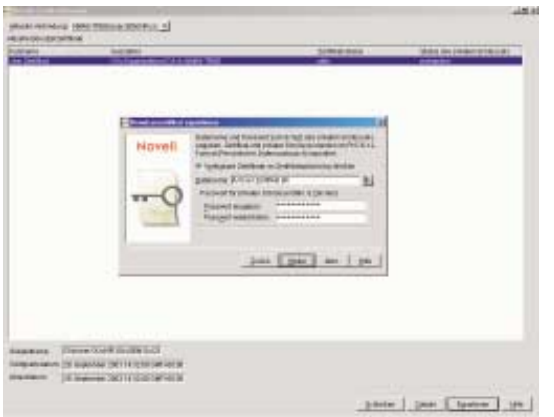


Abb. 6: Aufforderung zum Login mit X.509 Zertifikat

Abb. 7: GAMS Informationen

VASCO\Digipass. Auch hier müssen die Lizenzbedingungen bestätigt und eventuell ein anderer Name für das Login-Method Objekt vergeben werden usw. Bei der Zusammenfassung werden Sie darauf hingewiesen, daß SnapIns installiert wurden und die ConsoleOne neu gestartet werden muß. Außerdem wurde das Schema der NDS erweitert.
So gibt es nun eine Eigenschaft VASCO innerhalb des Benutzerobjekts sowie neue Objekte.

Abb. 8: Vasco Digipass Import Wizard

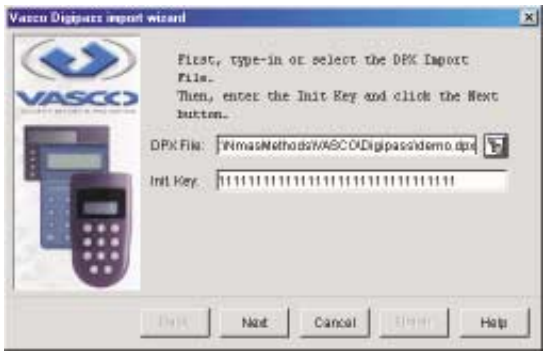


Abb. 9: Eigenschaften des importierten Digipass Objekts

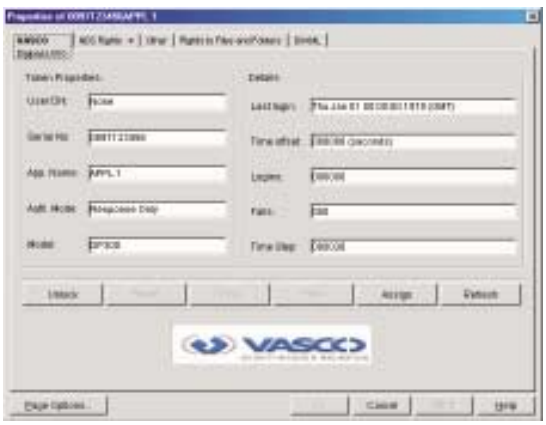


Abb. 10: VASCO Digipass Authentication Screen

Digipass Objekte

Nach dem Neustart der ConsoleOne muß ein vasco DigipassContainer Objekt angelegt werden. In diesen Container legen Sie die vascoDigi pass Token Objekte. Jedes einzelne Handheld Device wird nachher ein Objekt in der NDS haben. In dem neu erstellten Digipass Container erstellen Sie für jedes Handheld Device ein solches vascoDigipassToken Objekt. Beim Generieren dieses Objekts werden Sie aufgefordert, eine DPX-Datei sowie einen Initialisierungs-Key anzugeben (vgl. Abb. 7). Eine DEMO. DPX Datei finden Sie auf der NMAS Installations-CD im Verzeichnis NmasMethods\VASCO\Digipass. Abhängig von der DPX-Datei, die Sie verwenden, haben Sie die Wahl zwischen unterschiedlichen Applikationen, die für ein und dasselbe Device importiert werden sollen. Hierbei handelt es sich um die Art und Weise, wie das Device arbeitet, ob z.B. nach dem Challenge/Response-Verfahren oder nur mit Response. In unserem Beispiel werden wir das Response-Verfahren nutzen. Abbildung 9 zeigt die Eigenschaften des importierten Digipass Objekts.

Benutzer Zuordnung

Das Benutzerobjekt hat eine Eigenschaft VASCO. In dieser Eigenschaft weisen Sie dem Benutzer über den Assign Button ein Digipass-Objekt zu. Jetzt kann ihm das Device ausgehändigt werden, und er kann sich damit in der NDS authentifizieren. Sowohl in der Eigenschaft VASCO des Benutzerobjekts als auch in den Eigenschaften des Digipass Objekts kann das Device getestet, zurückgesetzt und deassoziert werden. Digipass-Objekte, die noch keinem Benutzer zugeordnet sind, erscheinen in der ConsoleOne schwarz. Sobald eine Zuordnung zu einem Benutzerobjekt erfolgt ist, erkennen Sie das an der roten Schriftfarbe.

HINWEIS:

Importieren Sie mehrere Applikationen für ein Device, wird für jede Applikation ein Digipass Objekt in der NDS angelegt. Der Name setzt sich zusammen aus der Serial Number für das Device und dem Applikationsnamen.

Login mit Digipass 300

Der Benutzer kann nun beim Einloggen die Sequenz Digipass, aber auch jede andere Sequenz, die als Kombination mit der Digipass Login-Methode definiert wurde, wählen. Er wird dann über einen Screen wie in Abbildung 10 aufgefordert, ein Paßwort einzugeben, das er wie folgt von seinem Digipass Device erhält: er startet das Gerät, gibt seine vierstellige PIN ein und wählt eine Applikation. In unserem Fall ist es die Applikation 1, für die er die Ziffer 1 eingeben muß, und schon wird eine sechsstellige Zahlenkombination angezeigt, die dann in dem Paßwortfeld der Digipass-Authentisierung eingegeben werden kann. Der Login-Methode Digipass ist ein Grade von Password & Token zugeordnet. Doch kann auch hier natürlich mit Clearances, wie zuvor beschrieben, gearbeitet werden.
In der nächsten Ausgabe werden wir weitere Devices zur Authentifizierung über NMAS besprechen. Wir werden die RSA SecurID Tokens sowie ein Fingerprint Device von Compaq als Login-Methoden in der NDS implementieren und testen.

Schlüssel für die Sicherheit

Teil 7: Implementierung von Kerberos v5 unter Windows 2000

Von Patrick Fell

Mit der Einführung des Standards Kerberos v5 ist Microsoft ein großer Schritt in Richtung einer sicheren Anmeldung und Überprüfung der Benutzercredentials gelungen. Ohne großen administrativen Aufwand läßt sich Kerberos v5 über die Default Domain Policy steuern und konfigurieren. Eine weitere Implementierung, die die Sicherheit Ihres Netzwerks drastisch erhöhen wird und zudem noch die TCO auf lange Sicht reduziert, da neu eingesetzte Dienste Kerberos v5 per Default verwenden werden.

Windows 2000 setzt Kerberos v5 als einen Domänen-Dienst ein und benutzt als Account-Datenbank das Active Directory. Zusätzliche Informationen über die Seacurity Principals werden aus dem Global Catalog gezogen. Das Key Distribution Center (KDC) - um es kurz zu wiederholen - stellt hier jedoch nur zwei Dienste zur Verfügung. Der Authentifizierungs-Dienst gibt die TGTs heraus, damit Session Tickets angefordert werden können, während der Ticket Granting Dienst die Session Tickets für serverspezifische Dienste vergibt.

Security Principals

KDC läuft auf jedem Domänencontroller, genau wie auch der AD-Dienst und wird unter dem Kontext der LSA gestartet. Weder KDC noch AD können somit, auch nicht versehentlich oder durch Mallory, gestoppt werden. Der Security Principal Name für KDC ist `krbtgt`, wie er in der RFC 1510 vorgegeben wird. Das Konto kann nicht gelöscht werden und wird automatisch nach bestimmten Zeiten mit einem neuen Paßwort versehen, ähnlich der Paßwortzuweisung für einen manuell erstellten Trust. Dieses Paßwort wird auch zum Generieren eines Secret Keys zum Ver- und Entschlüsseln von TGTs verwendet. Client Stationen benutzen neben dem Domänennamen auch den Principal-Namen von `krbtgt`, um Nachrichten an den KDC zu adressieren.

Wie bereits erwähnt, wird als Speicherort der Kontendatenbank das Active Directory verwendet. Somit hat der KDC jederzeit Zugriff auf die Objekte und Attribute der Security Principals. Der kryptographische Schlüssel, der die Kommunikation zwischen Clients, Servern und Diensten schützen soll, wird zum Beispiel als Attribut für jedes Benutzer-, Computer und Dienstekonto im AD abgespeichert und nicht, wie viele annehmen, das Paßwort selbst. Das Paßwort wird nur dazu benutzt, um diesen Schlüssel zu erzeugen. Damit Kerberos v5 domänenweit leicht integriert und auch verwaltet werden kann, können einige Optionen über GPOs auf Domänenebene, und nur auf dieser Ebene, konfiguriert werden. Diese Optionen können Sie der Tabelle 1 entnehmen.

Security Support

Unter Windows 2000 benutzen in einer Domäne alle verteilten Dienste das Security Support Provider Interface (SSPI) für ihre Authentifizierung. SSPI stellt die Schnittstelle zwischen dem Security Support Provider (SSP) und der LSA dar. Somit unterstützen auch alle Dienste Kerberos v5 als Protokoll.

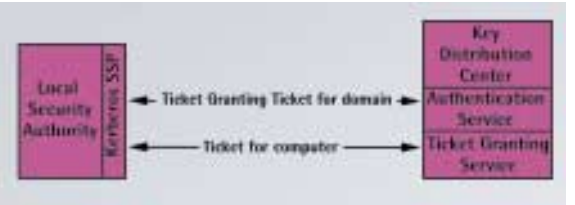
Die Dienste sind:

- Print Spooler Service
- Common Internet File System/ Server Message Blocks (CIFS/SMB)
- remote Dateizugriff
- LDAP-Abfragen ans Active Directory
- DFS (Distributed File System)
- IPSec Host zu Host SA-Authentifizierung (siehe TN Artikel 08/09)
- Reservierungsanfragen für Quality of Service (QoS)
- Intranet Authentifizierung zu einem IIS
- Remote Server- oder Arbeitsplatz verwaltung über RPC (Remote Procedure Call)
- Zertifikatsanfragen an einen Certificate-Server

Initialisierung

Wenn der Kerberos v5 SSP eine Initialisierungsanfrage an den KDC in der Benutzerkontendomäne schickt, muß er einen Domänencontroller für diese Domäne lokalisieren können. Dazu benutzt er den DC-Locator, der einen DNS-Server nach einem gültigen DC und KDC befragt. Der Locator kann jedoch nur KDCs finden, die in AD-Domänen abgespei-

Abb. 1: Kerberos v5 Ticket Exchange (interaktive Anmeldung)



chert sind. Wenn W2K-Maschinen in anderen Kerberos v5-Realms (Kerberos v5-Domänen) laufen, muß der DNS-Name für diesen KDC in der Registry des suchenden PCs abgespeichert werden. Der Kerberos v5 SSP sucht an der entsprechenden Registry-Stelle nach dem DNS Domänennamen des Kerberos v5 Realms und löst den Namen mit Hilfe eines konfigurierten DNS-Servers in die IP-Adresse auf.

Anmeldeprozeß

Schauen wir uns einen kompletten allgemeinen Anmeldeprozeß und eine Anmeldung mit Paßwort unter Windows 2000 an. Der allgemeine Logon-Prozeß kann in drei Schritte unterteilt werden. Der Benutzer fragt zunächst nach dem Zugang zum Tikket Granting Service für die Domäne. Dieser wird durch den AS Exchange zwischen dem Kerberos v5 SSP des anfragenden Computers und des KDCs der Benutzerkontendomäne gewährt. Das Ergebnis ist ein TGT, welches der Benutzer in Zukunft für die Kommunikation mit dem KDC benutzen kann. Als zweites fragt der Benutzer nach einem Ticket für den Remote-Computer. Dieses wird durch den TGS Exchange zwischen dem Kerberos v5 SSP auf dem Computer und dem KDC der Benutzerkontendomäne erstellt. Das Ergebnis ist ein Session Ticket, welches der Benutzer dem Remote-Computer vorweisen kann, um Zugriff zu einem Systemdienst zu erlangen. Als drittes fragt der Benutzer nach dem Zugang zu dem Local System Service auf dem Computer. Dieser wird gewährt, wenn der Kerberos v5 SSP auf dem Computer das Session Ticket der LSA auf der Arbeitsstation präsentiert.

Wenn die Kontendomäne des Computers eine andere ist als die des Users, muß ein zusätzlicher Schritt vollzogen werden. Bevor der Kerberos v5 SSP ein Session Ticket für den Computer anfordern kann, wird der KDC in der Benutzerkontendomäne nach einem TGT befragt, welches den Anforderungen für den KDC in der Computerkontendomäne gerecht wird. Der SSP kann dann das TGT dem KDC in der Computerkontendomäne vorweisen und erhält ein Session Tikket für den Remote-PC.

Paßwort-Anmeldung

Die Paßwort-Anmeldung sieht wie folgt aus. Wenn der Benutzer sich im Netzwerk anmelden möchte, benötigt er ein Benutzerkonto, und die Arbeitsstation, an der die Anmeldung durchgeführt wird, erhält ein Computerkonto. Der Benutzer drückt die Tastenkombination [STRG]+[ALT]+[ENTF]. WinLogon schaltet den Desktop auf eine DLL (`MSGINA.dll`) um, die auch Graphical Identification and Authentication, kurz GINA, genannt wird. Sie sammelt die Anmeldedaten, packt sie in eine Datenstruktur und übergibt diese an WinLogon, das die Daten weiter an die LSA sendet. LSA wandelt das Klartext-Paßwort in eine Secret Key um, indem sie darauf eine Einweg-Hashfunktion anwendet. LSA speichert das Ergebnis im Credentials Cache. Damit die Anmeldeinformationen überprüft werden können und sie sich anmelden kann, benötigt LSA ein TGT, welches Zugang zum TGS ermöglicht, und ein Session Ticket, um Zugang zum lokalen Computer zu erlangen. LSA erhält diese Tickets über den Kerberos v5 SSP, der direkt Nachrichten mit dem KDC der Domäne austauschen kann (siehe Abb. 1). Nach dem Empfang entschlüsselt die LSA das Session Tickets mit dem Secret Key des PCs und extrahiert die Autorisierungsdaten.

Danach wird der Security Account Manager (SAM) befragt, ob der Benutzer Mitglied in irgendwelchen lokalen Security-Gruppen ist, und ob er spezielle Rechte auf der lokalen Station hat. LSA fügt alle aus der Anfrage erhaltenen SIDs den Autorisierungsdaten aus dem Ticket hinzu. Diese letzte Liste wird zum Aufbau des Access Token benutzt, welches zum WinLogon zusammen mit einem Identifier zurückgegeben wird. Der Identifier bestimmt, ob die Anmeldeinformationen korrekt waren. Bei Korrektheit der Informationen startet WinLogon abschließend den ersten Shell-Prozeß (`Explorer.exe`).

Tabelle 1

Policy	Funktion
Erzwungene Einschränkung für Benutzeranmeldung (Enforce user logon restrictions)	Bei Aktivierung wird der KDC jede Anfrage nach einem Session Ticket überprüfen. Dabei wird in der Policy der Eintrag `Log on locally` und `Access this computer from the network` ausgewertet.
Maximale Lebenszeit für ein Serviceticket (Maximum Lifetime for Service Ticket)	Die Lebenszeit des Session Tickets muß größer als 10 Minuten und kleiner als die maximale Lebenszeit für ein Benutzerticket sein. Default ist 10 Stunden.
Maximale Lebenszeit für ein Benutzerticket (Maximum Lifetime for User Ticket)	Bestimmt die maximale Lebenszeit eines TGTs in Stunden. Default ist 10 Stunden.
Maximale Lebenszeit für die Erneuerung eines Benutzertickets (Maximum Lifetime for User Ticket Renewal)	Bestimmt die Erneuerungsrate eines TGTs in Tagen. Default ist 7 Tage.
Maximale Toleranz für die Uhrzeitsynchronisation (Maximum tolerance for computer clock synchronization)	Bestimmt die maximale Toleranz des Zeitunterschiedes zwischen einem Client und einem KDC in Minuten. Default ist 10 Minuten.

Tabelle 1: Optionen über GPOs auf Domänenebene

SOLUTION

compu shack

Windows XP-Trainings

Seminare für eine neue Betriebssystemgeneration

Von Markus Klein

Windows XP Professional, die neue Desktop-Edition von Microsoft, und Windows NET Server, das entsprechende Server-Produkt, repräsentieren eine neue Betriebssystemgeneration. Mit Beginn des bald schon bevorstehenden Jahres 2002 wird die Compu-Shack Education ihr Microsoft Kursprogramm um aktuelle Seminare zum Thema Windows XP Professional und Windows NET Server erweitern. Schon heute möchten wir Ihnen für eine rechtzeitige Planung die neuen XP-Trainings vorstellen, die ab Januar 2002 angeboten werden.

Microsoft Windows XP Professional vereint die Vorteile von Windows 2000 Professional - mit Sicherheit auf der Grundlage von Branchenstandards, Verwaltbarkeit und Zuverlässigkeit - und die besten Funktionen von Windows 98 und Windows Me, insbesondere das Plug ´n Play. Eine vereinfachte Benutzeroberfläche und innovative Support-Services machen es zu einem der anwenderfreundlichsten Desktop-Betriebssysteme für Unternehmen. Ob auf einem Standalone-PC oder im unternehmensweiten Netzwerk implementiert, Windows XP Professional vermag die IT-Produktivität spürbar zu erhöhen. Gleichzeitig wird das neue Betriebssystem die Total Cost of Ownership für Desktops deutlich reduzieren.

Auf Basis von W2K

Administratoren und Techniker können bei Windows XP Professional und Windows NET Server auf ihr Wissen über Windows 2000 aufbauen. Und auch die Unternehmen brauchen im Vorfeld der Bereitstellung keine tiefgreifenden Änderungen an ihrer Infrastruktur vorzunehmen, weder bei der Integration von Windows XP Professional in Windows 2000 Professional, noch beim Austausch von Windows 2000 durch die Kombination von Windows XP Professional und Windows NET Server.

MCSE + XP

Windows XP wird zukünftig als ein weiterer Bestandteil in die Ausbildung zum Microsoft Certified Professional oder Microsoft Certified Systems Engineer integriert sein. Alle, die sich derzeit bereits in einer MCP- bzw. MCSE-Ausbildung befinden, brauchen jedoch zukünftig nicht die

Netzwerk-Know-how: Highlights im November und Dezember 2001

Kursbezeichnung	Kurs-Nr.	Termin	Ort	Preis •	DM
Microsoft Exchange Server 5.5-Concepts & Administration	MS 1026	13.11.-16.11.2001	Neuwied	1.682,15	3.290,-
Updating Support Skills from Win NT 4.0 to Win 2000	MS 1560	19.11.-23.11.2001	Neuwied	1.988,93-	3.890,-
Implementing and Managing Microsoft Exchange 2000	MS 1572	19.11.-23.11.2001	München	1.988,93	3.890,-
Designing Microsoft Exchange 2000 for the Enterprise	MS 1573	28.11.-30.11.2001	Neuwied	1.273,12	2.490,-
		12.12.-14.12.2001	München		
NetWare 6.0 First Class	NV Fclass	26.11.-27.11.2001	Neuwied	510,78	997,47
		05.11.-06.11.2001	Neuwied		
		19.11.-20.11.2001	Potsdam		
		03.12.-04.12.2001	München		
		17.12.-18.12.2001	Neuwied		
		20.12.-21.12.2001	Neuwied		
		10.12.-11.12.2001	Potsdam		
Integrating Novell eDirectory and Windows NT	NV 555	28.11.-30.11.2001	München	1.273,12	2.490,-
Building Scalable Cisco Networks	Cis BSCN	19.11.-23.11.2001	Frankfurt	2.551,35	4.990,-
		10.12.-14.12.2001	Neuwied		
Cisco Sales Essentials Small and Medium Business	Cis CSE-SMB	05.11.-06.11.2001	München	557,31	1.090,-
WatchGuard Firewall & VPN	WG 001	28.11.-30.11.2001	München	1.585,-	3.099,99
		05.12.-07.12.2001	Potsdam		
		10.12.-12.12.2001	Neuwied		
Linux-Grundlagen für Administratoren	Lin Grad	14.11.-16.11.2001	München	1.265,45	2.475,-

Alle im Text und den Terminen genannten Preise verstehen sich zuzüglich der gesetzlichen Mehrwertsteuer

neuen Windows XP Professional bzw. Windows NET Server Prüfungen zu absolvieren, um als MCSE anerkannt zu werden. Die einzelnen Prüfungen werden voraussichtlich von Microsoft parallel angeboten, wodurch für einen längeren Zeitraum keine Update-Prüfungen auf die Kandidaten zukommen werden.

XP-Training

Alle Interessenten, die sich mit der neuen Betriebssystemgeneration beschäftigen möchten, haben ab Januar 2002 die Möglichkeit, das Training "Implementing and Supporting Microsoft Windows XP Professional" (MS 2272) bei Compu-Shack zu besuchen. IT- und Supportspezialisten, die sich mit der neuen Struktur von Windows XP Professional vertraut machen müssen, sind in diesem 5-Tage-Training genau richtig. Dies gilt in besonderem Maße, wenn Helpdesk Unterstützung für Windows XP Professional und Support-Leistungen zum täglichen Arbeitsalltag gehören. Das Seminar berücksichtigt die Unterstützung für die Whistler Server Familie und für Windows XP Lösungen ebenso wie Support für Windows XP Professional in einem Netware- oder Unix-Netzwerk. Zum Inhalt des Seminars MS 2272 gehören:

Inhalt:
- Installation von Windows XP Professional und Upgrade
- Automatisieren von Windows XP Professional
- Installationen über Antwortdateien und Uniqueness Database Files
- Benutzung des System Preparation Tools in Microsoft Windows 2000
- Konfiguration und Verwaltung der Hardware
- Troubleshooting des Bootprozesses und bei anderen Systemausgaben
- Konfiguration für Microsoft Windows Netzwerke
- Desktopumgebung und Benutzerprofile
- Support von TCP/IP
- Fehlerbehebung bei Namensauflösungen
- Konfiguration für Netzwerke mit Novell NetWare und UNIX
- Unterstützung von Remotebenutzern
- Konfiguration für mobiles Computing
- Verwalten von Festplatten
- Konfiguration und Verwalten des Dateisystems
- Überwachen von Resourcen und Performance

Windows-XP Seminare im Jahr 2002

Kursbezeichnung	Kurs-Nr.	Termin	Ort	Preis in •	DM
Implementing	MS 2272	07.01.-11.01.2002	Neuwied	1.988,00	3.888,19
and Supporting		11.03.-15.03.2002	Neuwied		
Microsoft		25.02.-01.03.2002	München		
Windows XP		07.01.-11.01.2002	München		
Professional		25.02.-01.03.2002	München		

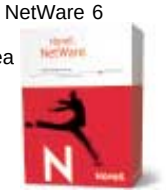
Newcomer im Zeichen der 6

NetWare 6 Upgrade und GroupWise 6 Administration

NetWare 6 baut auf der bewährten Novell Technologie auf und verfügt über neue Merkmale für das Speichermanagement in Netzwerken. Nach der Einführung der Version 6 bietet Compu-Shack Education im kommenden Jahr die aktuellen Novell Upgrade-Trainings an. Im Zeichen der Sechs steht auch das Seminar GroupWise 6 Administration (NV 370). Wir stellen Ihnen die beiden Newcomer-Trainings vor.

Das NetWare 6 Upgrade (NV3000) baut auf fundierten Kenntnissen von Systemadministratoren und Systemverwaltern aus dem Bereich NetWare 5.x auf und bietet den besten und schnellsten Weg, um das vorhandene Wissen von NetWare 5.x auf NetWare 6 zu erweitern. Schon nach 4 Tagen Seminar sind die Teilnehmer in der Lage, ein NetWare 6 Netzwerk mit allen neuen Features wie NSS3, IPP, iFolder oder CIFSzu administrieren. Der Preis für 4 Tage wird 1.682,- • betragen.

Inhalt
- Produktübersicht
- Installation eines NetWare 6 Servers
- Multiprozessorfähigkeit der NetWare 6
- NSS 3.0
- Clustering und Storage Area Network-Technologie
- CIFS Services
- IPP
- Apache Webserver
- iFolder



GW 6 Administration

Systemadministratoren und Supportmitarbeiter, die die effektive Implementierung und Administration von GroupWise 6 erlernen möchten, liegen mit dem Novell Seminar NV 370 genau richtig. Die Teilnehmer bekommen in 5 Tagen einen detaillierten Überblick über die Leistungsfähigkeit von GroupWise 6. Dabei wird ihnen nach der Implementierung eines Basis-Systems auch die Verwaltung komplexer GroupWise Systeme nahegebracht.

Inhalte
- Installation und Konfiguration
- Administration und Instandhaltung
- Installation und Konfiguration des GWIA
- zusätzliche GWIA Eigenschaften
- Erweitern der GroupWise 6 Umgebung
- Verwaltung eines erweiterten Systems
- Installation und Konfiguration des GW 6 Webaccess
- System-Überwachung in einer Webumgebung
- Troubleshooting des GroupWise Net Access und Connectivity

NetWare 6 und GroupWise 6 im Jahr 2002

Kursbezeichnung	Kurs-Nr.	Termin	Ort	Preis in •	DM
NetWare 5 to					
NetWare 6 Upgrade	NV 3000	28.01.-01.02.2002	Neuwied	1.682,-	3.290,-
		04.03.-08.03.2002	Neuwied		
		04.02.-08.02.2002	München		
GroupWise 6					
Administration	NV 370	04.02.-08.02..2002	Neuwied	1.988,-	3.890,-
		11.-03.-15.03.2002	Neuwied		
		11.02.-15.02.2002	München		
		18.03.-22.03.2002	München		

Cluster Services

Advanced Technical Trainings bei Compu-Shack

Die bereits erfolgreich etablierten Advanced Technical Trainings (ATT) von Novell zum Thema Cluster Services werden nun auch von hochqualifizierten Novell Trainingspartnern durchgeführt. Bei Compu-Shack können sich Administratoren und Techniker ab sofort in einem dreitägigen, intensiven Seminar auf Novell Cluster Services schulen lassen, vom 14. bis 16. November in Potsdam und vom 17. bis 19. Dezember in München. Das ATT ist ein technisches Training und richtet sich an Personen, die über hohes technisches Know-How verfügen. Es beinhaltet praktische Laborübungen und ist auf Fehleranaylse und Problembehebung ausgerichtet. Den Teilnehmern werden alle notwendigen Kenntnisse für den optimalen Betrieb komplexer IT-Umgebungen vermittelt. Für diese exklusiven Veranstaltungen ist nur eine begrenzte Anzahl von Plätzen verfügbar. Die Registrierung kann nur über Novell erfolgen! Info unter: `www.education.compu-shack.de`.

Novell Academy

Non Stop Access

Die NetWare 6 ist da. In vertrieblichen und technischen Schulungen setzt Novell dazu auch im November und Dezember ihre etablierte Veranstaltungsreihe unter dem Motto “Non Stop Access” fort. Im Mittelpunkt steht NetWare 6 als moderne eBusiness Plattform für Unternehmen jeder Größe. Das Seminar zeigt die Zukunft mobiler Datenverarbeitung. Auf einem hohen Leistungsniveau vermittelt die Novell Academy das notwendige Wissen zum Thema eBusiness mit NetWare 6. Wertvolle Technische, Vertriebs- und Service Tools unterstützen bei einem schnellen und optimalen Übergang zur die Net Economy. Am 14. November und am 5. Dezember finden in München weitere Eintagesseminare statt. Dabei werden auch die Herausforderungen im Bereich mobiler Benutzer und die Nonstop-Hochverfügbarkeit bei Ausfall von Hardware behandelt. Eine kurze Einführung zeigt auch Novells neueste Net Services Lösungen wie GroupWise oder die Internet-Sicherheitslösung BorderManager. Die Anmeldung erfolgt ausschließlich über `www.novell.de`. Information unter `www.red-alert.compu-shack.com`.

Cisco Solutions

10. Get in CISCOntact

Auf den letzten Stationen der zehnten Get-in-CISCOntact-Tour präsentiert sich Compu-Shack im November in Düsseldorf, Frankfurt und Nürnberg abermals mit professionellen Lösungs-Angeboten für den IT-Fachhandel. Die Cisco Tour bringt komprimiertes Fachwissen für die besonderen Anforderungen des Reseller-Channels, mit neuesten Informationen über Produkte und Trends. Mit ihrem Cisco-Solution-Programm eröffnet Compu-Shack ihren Fachhandelspartnern individuelle Beratung und Know-how-Partnerschaft. Dabei ist Compu-Shack auch für Multivendor-Umgebungen der kompetente Ansprechpartner bei allen Pre-Sales-Angelegenheiten, bei der Projektierung von Netzen und der Planung von Add-on-Funktionen. Als autorisierter Cisco-Trainingspartner warten die Education Center in Neuwied, München und Potsdam mit ihrem breit gefächerten Trainings- und Zertifizierungsangebot auf. Die Compu-Shack Solution stellt mit ihrem Solution Service Concept ein breites, hochqualifizierte Dienstleistungsangebot für den IT Fachhandel bereit. Am 6. November geht die Get-in-CISCOntact-Tour nach Düsseldorf, ist am 7. in Frankfurt und am 8. in Nürnberg. Die Teilnehmergebühr beträgt 99,- DM. Information erteilt das Business Team Cisco über `pm-cisco@compu-shack.com` oder per Telefon unter: 02631-983-453.

First Class Trainings

Bei NetWare 6 in der ersten Reihe

Seit dem letzten Monat ist die NetWare 6 da. Über ihre vielen neuen Features unterrichten seit einigen Wochen die NetWare 6 First Class Trainings. Auch im November gibt es bei Compu-Shack in Neuwied, Potsdam und München weitere Einführungen zur NetWare 6. Diese zweitägigen Seminare bieten einen tiefen Einblick in die Neuerungen. Im Mittelpunkt steht NetWare 6 als moderne E-Business Plattform für Unternehmen jeder Größe. Das Seminar zeigt die Zukunft mobiler Datenverarbeitung. Die Teilnehmergebühr beträgt 999,- DM, für CNEs und Novell PartnerNet Mitglieder 799,- DM. Info unter: `www.education.compu-shack.de`.

Vorschau Technik NEWS

N°12

No 12/2001

Thema des Monats Dezember

GENERATIONSWECHSEL

Windows XP

Die neue Desktop-Betriebssystemgeneration

Von Patrick Fell

Am 25. Oktober war es endlich soweit. Microsoft hatte mit Windows XP Home und Windows XP Professional die nächste Generation ihrer Desktop-Betriebssysteme auf den Markt gebracht. Der weltweite Launch stellte die bis dato größte Windows Marketing-Initiative in der Unternehmensgeschichte von Microsoft dar, mit Investitionen in den ersten vier Monaten der Produkteinführung, die doppelt so hoch sein sollen wie die Gesamtausgaben für den Launch von Windows 95. Die Erwartungen der Kunden sind entsprechend hoch. Mit Einführung der neuen Editionen versprach Microsoft eine gegenüber Windows 2000 Professional nochmals gesteigerte Kombination aus Zuverlässigkeit und Stabilität. Die Home Edition ist dabei auf die Bedürfnisse der Heimanwender ausgerichtet, während Windows XP Professional für den Einsatz in Unternehmen konzipiert. Neue und erweiterte Medientechnologien, die teilweise aus Windows ME und Windows 2000 Professional übernommen wurden, teilweise aber auch vollkommen neu implementiert wurden, sollen die Windows XP Versionen zu den innovativsten Desktop-Betriebssystemen machen, die Microsoft jemals veröffentlicht hat. Gründe genug, uns in der nächsten Ausgabe intensiv mit den entscheidenden Verbesserungen und Neuerungen zu beschäftigen. Denn Windows XP bietet in beiden Editionen nicht nur eine komplett neu überarbeitete Benutzeroberfläche, sondern basiert auf der bislang leistungsfähigsten Microsoft Engine.

Praxis:

Wireless LAN, Teil 1:
Fragmentierung und Anmeldungen von Stationen an einer Funkzelle

Novell Modular Authentication Services, Teil 4:
RSA SecurID Token und Fingerprint Device

Business Communications Manager, Teil 2:
Anbindung an das externe Telefonnetz

Ausgewählte Termine

05.11.-06.11.2001	NetWare 6 First Class Trainings	Neuwied
06.11.2001	Get-in-CISCOntact-Tour	Düsseldorf
07.11.2001	Get-in-CISCOntact-Tour	Frankfurt
08.11.2001	Get-in-CISCOntact-Tour	Nürnberg
12.11.-13.11.2001	NetWare 6 First Class Trainings	München-Haar
14.11.-16.11.2001	Novell Cluster Server Training im Compu-Shack Education Center	Potsdam
15.11.2001	Novell Academy	München
17.11.-19.11.2001	Novell Cluster Server Training im Compu-Shack Education Center	München
19.11.-20.11.2001	NetWare 6 First Class Training	Potsdam
26.11.-27.11.2001	NetWare 6 First Class Training	Neuwied
05.12.2001	Novell Academy	München

Neue Novell CDs und Sales Guides stehen im Technik News Info Channel bereit.

Seit neuestem ist eine Group Wise 6 Demo-CD verfügbar. Sie können die Demos und Trials kostenlos unter www.technik-news.de bestellen.

4. us Novell