

Industrial Ethernet

Der Motorenhersteller DEUTZ AG setzt auf die Carrier Class Technologie von Extreme Networks.

Carrier Class Redundanzmechanismus Ethernet Automatic Protection Switching (EAPS) ermöglicht Hochverfügbarkeit der Netzwerkinfrastruktur mit einer Umschaltzeit unter 100ms.

Modulares Betriebssystem ExtremeXOS™ unterstützt Hochverfügbarkeit, Security, Scripting und Universal Port-Technik.

Die DEUTZ AG mit Hauptsitz in Köln-Porz entwickelt und produziert seit über 140 Jahren Dieselmotoren und setzte schon in den neunziger Jahren auf Ethernet und TCP/IP. Anfang 2010 hat DEUTZ in Köln das Fahrerlose Transportsystem (FTS) als eine der Hauptkomponenten im Material- und Motorenfluss ersetzt (vgl. Box rechts) und dabei auch die Ethernet-basierte Netzwerkinfrastruktur weiter ausgebaut.

Vor dem Hintergrund dieses Industrie-Projektes beschreibt der Artikel die Rahmenbedingungen mit Blick auf die implementierte Netzinfrastruktur und die notwendige Integration älterer Industrieanlagen in moderne Netze. Neben dem Netzdesign und dem Featureset der eingesetzten (Gigabit-) Ethernet-Technik beleuchtet der Bericht zudem den Carrier Class Redundanzmechanismus *Ethernet Automatic Protection Switching (EAPS)*, welcher eine Umschaltzeit von unter 100ms ermöglicht. Des Weiteren beschreibt der Artikel den Aufbau des für die FTS-Kommunikation notwendigen IEEE 802.11a WLAN-Systems und die Funktionalität des innovativen sowie modularen Extreme Networks Switch-Betriebssystems *ExtremeXOS™ (EXOS)*.



Firmenprofil DEUTZ AG

1864 als N.A. Otto & Cie. in Köln gegründet, ist die DEUTZ AG heute die älteste Motorenfabrik der Welt und einer der weltweit führenden unabhängigen Motorenhersteller. Die Kernkompetenzen des Unternehmens liegen in der Entwicklung, Produktion, dem Vertrieb und Service von Dieselmotoren für professionelle Einsätze. Der Full-Line-Motorenspezialist verfügt über eine breite Palette flüssigkeits- und luftgekühlter Motoren in einem Leistungsspektrum von 10 kW bis 500 kW, die in Baumaschinen, Energie-Erzeugungsanlagen, Landmaschinen, Nutz- und Schienenfahrzeugen sowie Schiffen zum Einsatz kommen. DEUTZ Kunden werden von 16 Vertriebsgesellschaften, 12 Vertriebsbüros, 16 Service-Centern und über 800 Vertriebs- und Service-Partnern in mehr als 130 Ländern der Erde betreut.

In der Kölner Montagehalle 40 werden pro Stunde 44 Motoren gefertigt. Mit zwei Montagelinien in bis zu drei Schichten an maximal sechs Tagen in der Woche sowie unter Berücksichtigung von rund 3.800 Varianten. Eine der Hauptkomponenten für diesen hohen Output in der Motorenmontage bildet dabei das Fahrerlose Transportsystem (FTS), welches den automatisierten Transport im Motoren- und Materialfluss gewährleistet.



DEUTZ-Motor TCD 2013 L6 4V
für die industrielle Anwendung

Austausch des FTS und Migration zu TCP/IP mittels SPS-Gateway

Die Kölner Motorenbauer haben Anfang 2010 innerhalb von nur 12 Arbeitstagen das aus dem Jahr 1992 stammende Fahrerlose Transportsystem (FTS, vgl. auch Infobox auf Seite 2) ersetzt. Rahmenbedingungen für die Umstellung auf das neue FTS waren, neben der Realisation einer hochverfügbaren Netzwerk-Infrastruktur (inkl. IEEE 802.11a WLAN), auch die Entwicklung eines dezierten SPS-Gateways, welches zwischen dem proprietären Protokoll *S/NEC AP* und dem herstellerübergreifenden Standard TCP/IP (mit RFC 1006) konvertiert (vgl. Infobox auf Seite 4).

Hochverfügbare Netzwerk-Infrastruktur

Die DEUTZ AG verfügt in der Kölner Produktion über ein hochverfügbares 100/1000 Mbps Ethernet Netzwerk, basierend auf Aktiven Komponenten des Herstellers Extreme Networks. Neben dem modularen und innovativen Betriebssystem der Switches (Seite 7), sorgt hierbei insbesondere der Carrier Class Redundanzmechanismus *EAPS* für die notwendige Hochverfügbarkeit im Netz (S.5).

www.deutz.com

Industrial-IT mit Ethernet & TCP/IP

Das *Industrial-IT* Team des Kölner Motorenherstellers DEUTZ AG betreut die IT-Systemstruktur der Motorenproduktion. Diese umfasst auf der Leitsystemeebene, neben dem Montageleitrechner (MLR) den FTS-Leitrechner (v. *MLR LogOS*), die

Prozessvisualisierung (SICALIS) sowie die Systeme zur Programmierung der Motor-Steuergeräte. Hinzu kommen zahlreiche Systeme u.a. für Warenein- und -ausgang, Montagen, Prüffeld etc. (vgl. Abbildung-1 unten). Mit den Leitsystemen versorgt das Industrial-IT

Team insgesamt 15 Server, 250 PCs und über 100 Steuerungen und Prozessrechner. Der gesamte Produktionsprozess ist nahtlos IT-gesteuert und genau aufeinander abgestimmt. Die Fabrik wurde 1992 in Betrieb genommen und gehört seitdem zu Europas modernsten Montageanlagen.



Martin Feller

Leiter Industrial IT
DEUTZ Montage
Köln-Porz

Martin Feller, Leiter des Industrial-IT Teams, war von Beginn an dabei und entschied sich bereits in den Neunzigern für einen sukzessiven Ausbau der strukturierten Verkabelung und den Einsatz der stan-

dardisierten Ethernet-Technologie. „Es war für uns eine naheliegende Entscheidung, auch bei der jetzigen Ablösung des 18 Jahre alten FTS weiter in Richtung Ethernet und TCP/IP zu investieren“, erläutert Feller.

Die Anbindung an den Montageleitrechner und die Kommunikation zwischen den einzelnen FTS-Komponenten erfolgt nach dem allgemein gebräuchlichen TCP/IP-Standard. Für die Anbindung an die Prozessebene wurde zusätzlich RFC1006 verwendet. Zur Konvertierung des TCP/IP mit RFC1006 zum proprietären SIEMENS Protokoll SINEC AP hat das Team um Martin Feller eine pragmatische Lösung angestrebt und gemeinsam mit SIEMENS entwickelt: ein dezidiertes SPS-Gateway (vgl. Infobox auf Seite 4). „Das Gateway mit der RFC1006-Anbindung erlaubte uns die Anbindung der Prozessebene ohne Anpassung der Anwendungssoftware und damit unproblematische Tests in der Entwicklungsphase des Projektes“ ergänzt Feller.

Fahrerloses Transportsystem (FTS)

Eine der Hauptkomponenten in der Motorenmontage der DEUTZ AG bildet das Fahrerlose Transportsystem (FTS), welches den automatisierten Transport im Motoren- und Materialfluss gewährleistet. Das FTS ist somit das zentrale Transportsystem in der Montagehalle und verfügt über zahlreiche Schnittstellen zu den jeweiligen Montage-Systemen in der Prozessebene, u.a. für Warenein- und -ausgang, Material- und Motorpuffer, Übersetzer Fließmontage und Übergabe Farbgebung (vgl. Abbildung-1 unten).



Das neue FTS in der Kölner Montagehalle wurde von DEUTZ in der Zeit vom 27.12.2009 bis 8.1.2010 gemeinsam mit dem Materialfluß-Systemspezialisten *MLR System GmbH* installiert und in Betrieb genommen. Das neue FTS basiert hierbei auf einer leitdrahtlosen Lasernavigation und unterstützt einen Fahrparcour von rund 6.800m. Insgesamt sind 1.600 Übergabestellen (Ziele) programmiert. Im Einsatz sind 43 frei navigierende Gabelhubwagen (FTS-Fahrzeuge, vgl. Abbildung oben) in drei Varianten für Längs- und Querladegut sowie für den Motorenttransport. Das System leistet bis zu 8.000 Transporte täglich und ist an insgesamt 15 automatische Fördertechnik / Ladesysteme des Material- / Motorenflusses angebunden.

Innerhalb der IT-Systemstruktur der Montage gehört die IT-Steuerung des FTS zu den Leitsystemen der Fabrik (vgl. Abbildung-1 unten). Zur Kommunikation mit den FTS-Fahrzeugen wird ein IEEE 802.11a basiertes Wireless LAN genutzt (5 GHz, 54 Mbps, vgl. auch Infobox auf Seite 7). Nach der Inbetriebnahme des WLANs im Juli 2009 konnten an den Wochenenden die einzelnen Schnittstellen getestet und in Betrieb genommen werden. Hierzu musste jeweils der alte FTS-Leitrechner runtergefahren und die weiterhin benötigten FTS-Module an das neue System angedockt werden. Ebenso die externen Kommunikationspartner (MLR, SICALIS, ...). Ein solcher Vorgang dauerte jeweils 1h und endete mit einem Produktivtest des alten Systems.

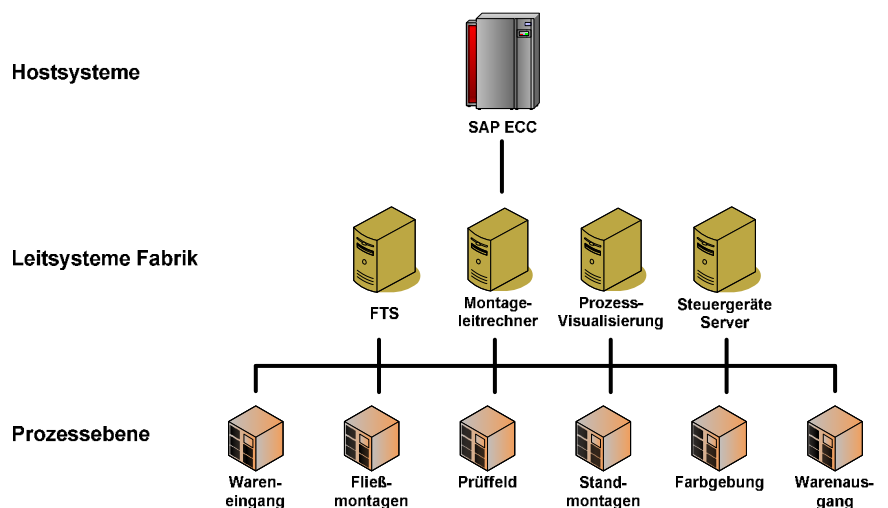


Abbildung-1: IT Systemstruktur – DEUTZ Montage Köln-Porz

© 2009 DEUTZ

Eine wichtige Rahmenbedingung für den reibungslosen Produktionsablauf sowie für den Einsatz des neuen FTS ist eine zuverlässige Netzwerkinfrastruktur. Wir beschreiben nachfolgend zunächst das Netzdesign in der Montagehalle und skizzieren anschliessend den integrierten Carrier Class Redundanzmechanismus EAPS (ab S. 5). Das modular strukturierte Switch-Betriebssystem ExtremeXOS™ unterstützt dabei zusätzlich die Hochverfügbarkeit im Netzwerk (Seite 7).

Layer3 Netzdesign

Netzwerk-Struktur

Die DEUTZ AG verfügt in der Kölner Montagehalle 40 über eine Strukturierte Verkabelung. Alle neun Unterverteiler sind sternförmig mittels Glasfaserkabel angebunden. Den Kern des Ethernet-Netzwerks bildet je ein Hauptverteiler in zwei Rechnerräumen (RR). Ausgehend von diesen Hauptverteilern sind neun Unterverteiler mittels Lichtwellenleiter (LWL) redundant per Gigabit Ethernet (LWL) redundant per Gigabit Ethernet angeschlossen (vgl. Abbildung-2 und -4).

Grundlage des Netzes ist ein Layer3-Netzdesign, basierend auf dem IPv4-Netzprotokoll u. portbasierenden VLANs. Das Routing erfolgt dabei zentral auf den redundanten Coreswitches und ermöglicht somit eine einfache Konfiguration und Administration der Edge-Switches. Die komplexen Konfigurationsinhalte befinden sich im Core.

Zwischen den Coreswitches ist das OSPF Routing-Protokoll im Einsatz. Es wird nur auf den Transfer-VLANs zwischen den Coreswitches genutzt. Hierbei haben ausschließlich die Coreswitches eine direkte Verbindung in die Transfer-VLANs. So ergibt sich keine Möglichkeit der Beeinflussung der Coreswitch-Routing-Tabellen durch Clients oder Server.

Aktive Komponenten

Coreswitches

Der aktive Kern (Core) des Ethernet-Netzes besteht aus je einem Coreswitch-System pro Rechnerraum in redundanter Konfiguration. Dies verhindert einen „Single Point of Failure“, welcher einen Totalausfall durch einen einfachen Komponentendefekt bewirken könnte.

Als zentrale Coreswitches fungieren leistungsstarke Layer3 Carrier Class Systeme von Extreme Networks (vgl. auch die Abbildungen Nr. 2,3 und 4). In beiden Rechnerräumen sind die Summit X450a-24x Switchsysteme im Einsatz, welche pro Switch 24x SFP-based 1000BaseX Ports (inkl. 4x 1000BaseT Combo Ports) bereitstellen. Die Systeme verfügen über eine Performance von 128 Gbps Switchfabric Bandbreite und 95,2 Mpps Frame Forwarding Rate in wirespeed (vgl. auch Abbildung-3 rechts). Die Geräte unterstützen dasselbe Carrier Class Featureset wie die modularen Black Diamond 8800er Switches.

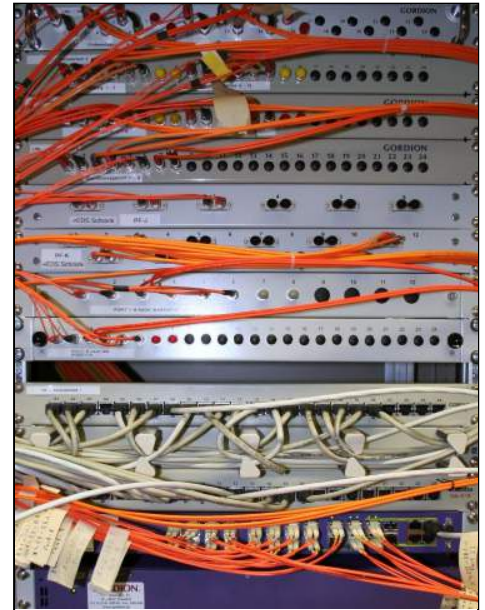


Abbildung-2: Rechnerraum-1 Sternpunkt mit Coreswitch X450a-24x & red. PSU



© 2009 Extreme Networks

Abb.-3: Summit X450a Serie

- 24x SFP-based oder 24/48 Port 10/100/1000T
- inkl. 4x Gigabit Combo Ports
- inkl. 2x XFP-based 10Gig Ports (optional)

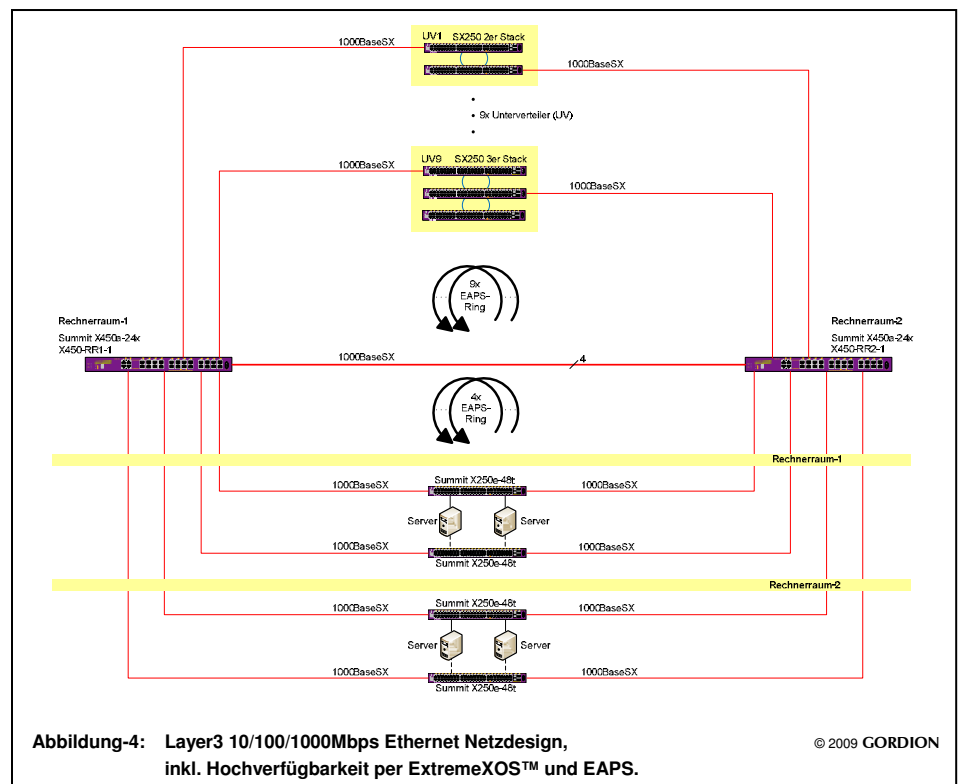
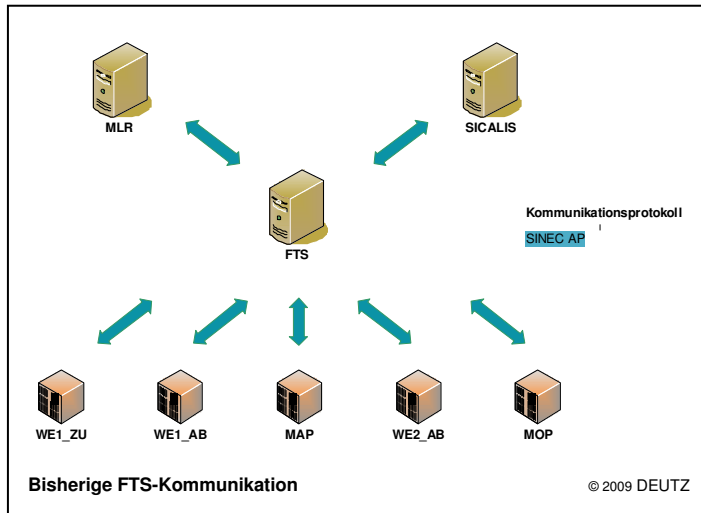


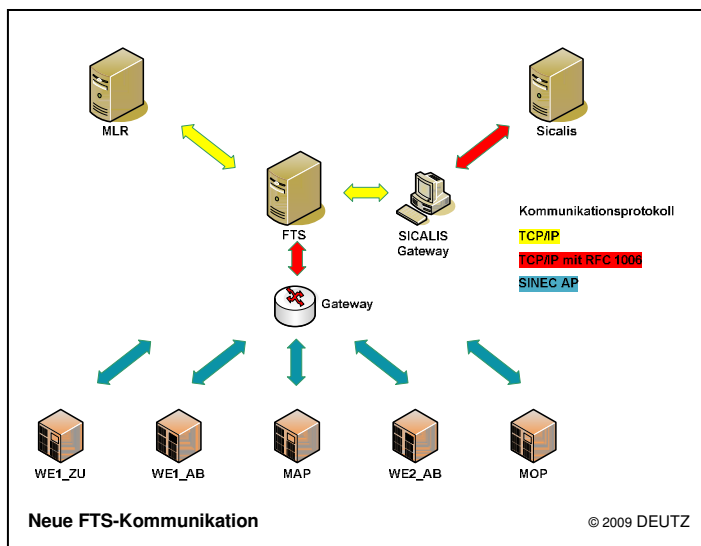
Abbildung-4: Layer3 10/100/1000Mbps Ethernet Netzdesign, inkl. Hochverfügbarkeit per ExtremeXOS™ und EAPS.

FTS-Kommunikation über dezidiertes SPS-Gateway

Die bisherige FTS-Kommunikation zum Montageleitrechner (MLR), zur Prozessvisualisierung (SICALIS) sowie zur Prozessebene (u.a. Warenein- und ausgang, Material- und Motorenpuﬀer) wurde mittels des proprietären SIEMENS-Protokolls SINEC AP realisiert (vgl. Abbildung).



Mit der Einführung des neuen FTS wurde die Anbindung zum Montageleitrechner auf das herstellerübergreifende Standardprotokoll TCP/IP umgestellt, welches auch zur Kommunikation zwischen den einzelnen FTS Komponenten genutzt wird. Die Anbindung an das Prozessvisualisierungssystem SICALIS und an die Prozessebene erfolgt über TCP/IP mit RFC 1006.



Ein von SIEMENS und DEUTZ entwickeltes SPS-Gateway ermöglicht die Konvertierung des proprietären Protokolls SINEC AP zu TCP/IP mit RFC1006 und umgekehrt. Das RFC 1006 ermöglicht bereits auf Treiberebene einen verbindlichen telegramorientierten Datenaustausch auch bei unterschiedlicher Telegrammlänge.

Es mussten keinerlei Anpassungen auf der Prozessebene vorgenommen werden. Weiterhin ermöglicht dieses Verfahren eine zukünftige Migration von S5- auf S7-Steuerungen durch einfache Umparametrierung der Kommunikationsschnittstelle auf dem FTS-Leitrechner.

Edgeswitches ermöglichen mit 10Gig hochperformantes "SummitStacking"

In den neun Unterverteilern der Montagehalle 40 steht die SummitX250er-Serie zur Verfügung (vgl. Abb.-6). Diese Switches sind ebenfalls Layer3-Systeme, verfügen auch über das ExtremeXOS™-Betriebssystem, und ermöglichen einen 10/100Mbit/s DualSpeed Ethernet Zugriff im Unterverteiler-Bereich (Edge).

16x SummitX250e als Edge-Switches

An den Core sind insgesamt neun Unterverteiler redundant mit je ein Gbps angeschlossen. Je nach benötigter Portanzahl im Unterverteiler sind die X250er-Switches in 1er-, 2er- oder 3er-Stacks gruppiert (vgl. Abb.-5 und -7).

SummitStacking

Die Gruppierung der Switches funktioniert per SummitStacking mit einer Performance von zehn Gbps (10Gig). Hierbei erfolgt die Verwaltung des Stacks über eine IP-Adresse. Es können bis zu acht Switches der Summit X250, X450er und X650er-Serie im Mix gestapelt werden (vgl. Abbildung-5).

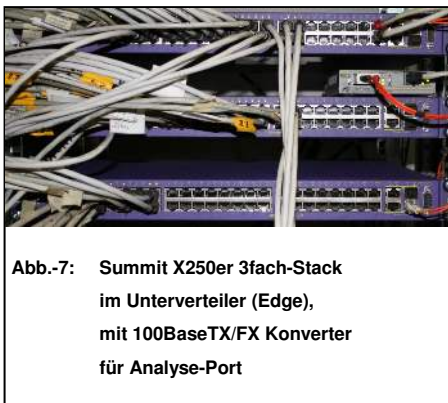
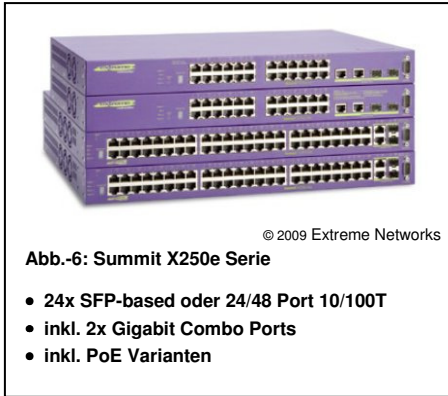
- Single management point for up to eight units
- High-speed 40 Gbps stacking
- Rapid Failover for converged applications
- Can mix Summit X250e, Summit X450 series and Summit X650 series switches



© 2009 Extreme Networks

Abbildung- 5: SummitStack Architektur

Dabei ist die Funktionalität des Stapels auch bei einem eventuellen Ausfall eines Switches gegeben. Bemerkenswert ist die *Local Switching-Funktion* für Non-Master Units sowie die integrierte *Hitless Failover-Funktion*.



Die DEUTZ AG setzt im Core- und Edge-Bereich des Netzwerks auf die Systeme von Extreme Networks. Durch den einheitlichen Einsatz der Extreme Networks-Serie ergeben sich einige Vorteile. Insbesondere das einheitliche Bedienerinterface (CLI und WebGUI) vereinfacht die Administration der Geräte. Denn durchgängig von den Core-, über die Aggregations- / Distributions-Switches bis hin zu den Edge-Komponenten, verfügen die Systeme von Extreme Networks über ein einheitliches Betriebssystem: ExtremeXOS™ (Seite 7).

Die Switches basieren zudem auf einer Carrier Class Hardware und bieten ein attraktives Feature-Set zur Realisierung eines stabilen Netzwerk-Betriebes. Insbesondere im Hinblick auf die Hochverfügbarkeit im Netz, u.a. das *Extreme Standby Router Protocol (ESRP)* und *Ethernet Automatic Protection Switching (EAPS)*.

Hochverfügbarkeit im Netz

Ausfall-Strategie im Core: EAPS, VRRP

Zur Steuerung der redundanten Topologie werden in der Montagehalle verschiedene Mechanismen eingesetzt. Hierbei gibt es folgende Anforderungen:

Erstens: die zwingende Unterdrückung von Netzwerkschleifen zur Verhinderung von Broadcast Storms. Eine Schleife ermöglicht im Gigabit Ethernet das Kreisen von mehreren 1.000 Broadcast-Frames pro Sekunde und blockiert so die Netzwerkkommunikation. In bestimmten Fällen kann ein Broadcaststurm auch einen manuellen Reboot von Endgeräten wie z.B. Printserver erfordern.

Zweitens: die Bereitstellung eines redundanten Default-Gateways für die angeschlossenen Client-/Server-PCs. Die redundante Instanz wird auf einem zweiten Switch konfiguriert und ermöglicht so die Ausfallsicherheit bzw. die Erreichbarkeit des Gateways im Falle einer Störung des Primär- (Layer3-) Switches. Zwingend zu beachten ist jedoch, dass nur eine Instanz aktiv geschaltet ist. Zwei aktive Routing-Interfaces mit der gleichen IP-Adresse führen unweigerlich zu Netzstörungen.

Die Steuerung der redundanten Instanz sowie die Unterdrückung von Netzwerkschleifen wird durch ein geeignetes Protokoll geregelt. Im Netzdesign der DEUTZ AG übernimmt diese Aufgabe der *Ethernet Automatic Protection Switching Mechanismus (EAPS)*.

EAPS mit Zeitvorteilen gegenüber STP

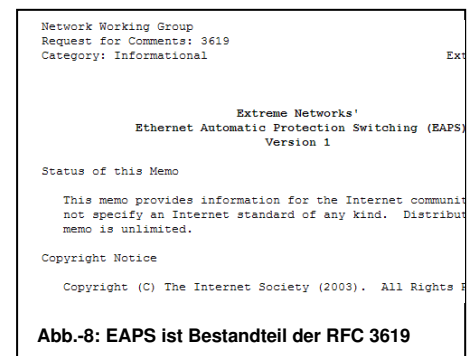
Mit Einsatz von EAPS wird zusätzlich das *Virtual Router Redundancy Protocol (VRRP)* für die Layer3-Redundanz-

steuerung benötigt. VRRP stellt hierbei die Verfügbarkeit des Default-Gateways für die Clients sicher.

Redundanz-Umschaltung unter 100 Millisekunden

Die beiden X450er Core-Switches (je ein Coreswitch pro RR) bilden ein Redundanz-Paar. Das EAPS-Protokoll läuft in einem separaten VLAN. Eine Redundanz-Umschaltung im Störfall erfolgt unter 100ms.

Zur Bekanntgabe der aktiven Routerinterfaces in einer redundanten Konfiguration sind statische Routingeinträge nicht geeignet. Für eine dynamische Aktualisierung der Routingtabellen im Falle einer Änderung ist vielmehr ein dynamisches Routingprotokoll notwendig. Im Netzwerk der DEUTZ AG wird hierzu das Routingprotokoll *Open Shortest Path First (OSPF)* eingesetzt.



EAPS im Detail

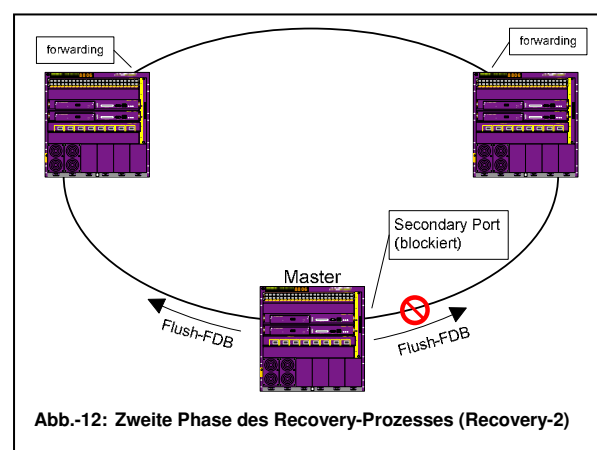
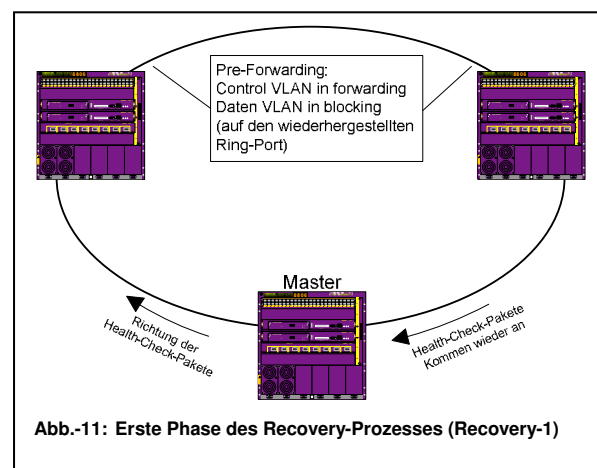
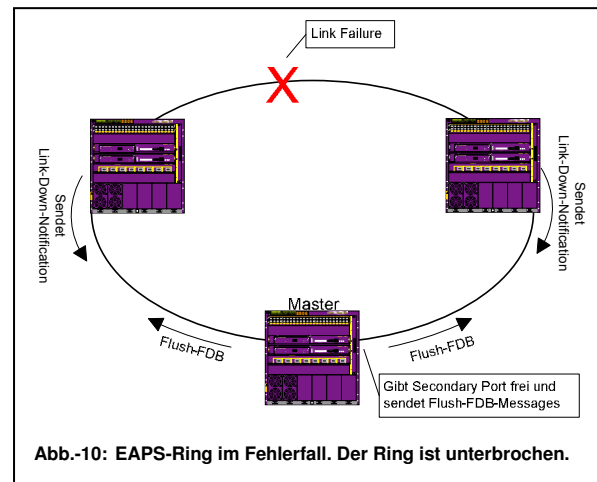
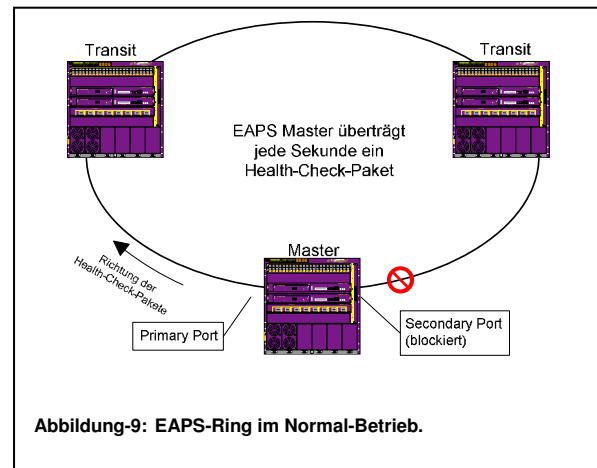
EAPS wurde im Jahre 2000 von Extreme Networks für die Carrier-Netze entwickelt. EAPS ist Bestandteil der RFC 3619 (vgl. Abb.-8 oben) und insbesondere auch für Enterprise-Netze verfügbar. Die realisierbaren Umschaltzeiten von EAPS liegen deutlich unter einer Sekunde. Mit optimalen Rahmenbedingungen liegen die Umschaltzeiten bei 50 Millisekunden (50ms). EAPS gehört damit in die Klasse der „Voice-Grade“ Mechanismen.

Die Redundanzsteuerung erfolgt hierbei über ein separates VLAN mit priorisierter Datenübertragung. Das Steuerungsverfahren ist hierdurch vom „Restnetz“ isoliert. Ein User-Zugriff auf dieses VLAN ist nicht möglich. Die Redundanzsteuerung wird somit nicht durch Störungen aus dem Produktionsnetz beeinflusst. Zusätzliche VLANs für separate Netze werden durch EAPS unterstützt.

Abbildung-9 rechts zeigt exemplarisch einen EAPS-Ring im normalen Betrieb, also ohne akuten Fehler. Der EAPS-Master blockiert den zweiten (secondary) Ringport und verhindert so eine Schleife (Loop) in der redundanten Struktur. Abbildung-10 rechts zeigt einen EAPS-Ring im Fehlerfall. Der Ring ist unterbrochen. Der EAPS-Master schaltet den zweiten (secondary) Ringport frei und ermöglicht so die Überbrückung der Fehlerstelle. Die Unterbrechung im Datenverkehr liegt deutlich unter einer Sekunde und beträgt unter optimalen Rahmenbedingungen lediglich 50 Millisekunden (50ms).

Der Wechsel in den Normalbetrieb erfolgt in zwei Phasen. Abbildung-11 zeigt die erste Phase (Recovery-1). Der unterbrochene Link ist wieder hergestellt und befindet sich im Pre-Forwarding-Modus (es werden nur Daten im EAPS-Control-VLAN weitergeleitet). Der Secondary-Port des EAPS-Master ist immer noch im Forwarding-Mode (also noch nicht blockiert).

In Phase-2 des Recovery-Prozesses (Recovery-2) überträgt der wiederhergestellte Link die Daten-VLANs. Der Secondary-Port am EAPS-Master ist wieder blockiert (Blocked Mode). Das System ist wieder im Normalbetrieb (vgl. Abbildung-12).



Modulares Betriebssystem ExtremeXOS™ unterstützt Hochverfügbarkeit, Security und Universal Port

Eingeführt 2003 auf dem (Carrier-) Switch BlackDiamond 10808, ist das modulare ExtremeXOS™ Betriebssystem heute auf allen Ebenen einer Netzwerk-Infrastruktur verfügbar: im Core (BlackDiamond 20k, 12k, 10k, 8800er Serie), im Smart Core- / Gigabit Aggregation-/Distributions-Bereich (BD8800 & X450er Serie) sowie im Edge (Summit X450, X250e, X350er und X150er Serie).

ExtremeXOS™ ist das erste Switch-Betriebssystem für Enterprise Switches, welches nicht monolithisch, sondern modular aufgebaut ist und somit gänzlich flexibel auf Störungen reagieren kann. Das System verfügt über ein breites Featurespektrum (vgl. Abb. 9 und 10), welches nachfolgend näher beschrieben wird. Ein detailliertes *White Paper* ist unter www.gordion.de erhältlich.



Hochverfügbarkeit

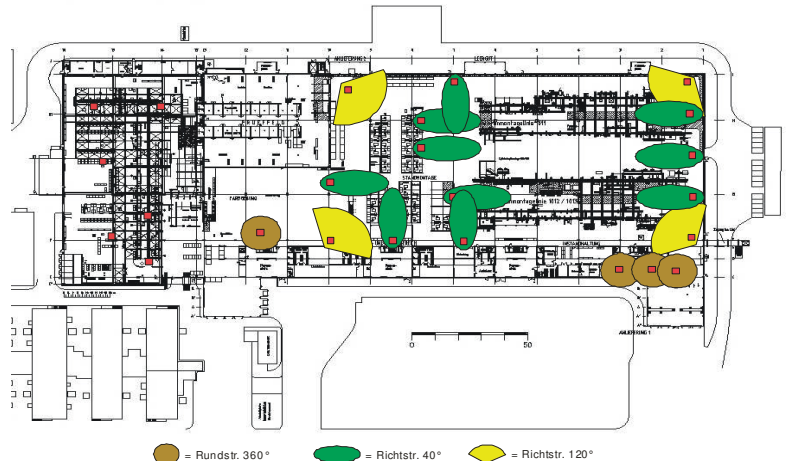
ExtremeXOS™ (EXOS) unterstützt die Hochverfügbarkeit des Netzes bei der DEUTZ AG durch mehrere Eigenschaften, u.a. mit der Möglichkeit eines separaten Reboots von Diensten innerhalb des EXOS sowie durch einen Hitless Failover-Mechanismus.

Partielles Rebooten von Diensten

Das modulare Design von ExtremeXOS™ ermöglicht u.a. ein dynamisches Prozess-Management, Multithreading und Memory-Protection.

5GHz WLAN-Infrastruktur als Kommunikationsplattform zu den FTS-Fahrzeugen

Die leitdrahtlosen und frei navigierenden FTS-Fahrzeuge kommunizieren über eine 5GHz WLAN-Infrastruktur mit den Leitrechnern im Rechenzentrum. Auf einer Fläche von 17.100qm stellt das WLAN sowohl den IEEE 802.11a Standard (5 GHz, 54Mbps, nur für FTS) als auch die IEEE 802.11 b/g Varianten (2.4 GHz, 11 & 54Mbps) zur Verfügung, welche parallel verwendet werden. Das 2.4 GHz-Band wird meist auch von anderen Technologien genutzt (u.a. Bluetooth), so dass das 5 GHz-Band weniger störanfällig und daher für das FTS besser geeignet ist. Zudem stehen im 5 GHz-Bereich mehr nutzbare Kanäle zur Verfügung. Durch den Einsatz von Richtantennen verfügt die Montagehalle über eine optimale Ausleuchtung. Die Ausleuchtung der Halle erfolgte im März 2009.

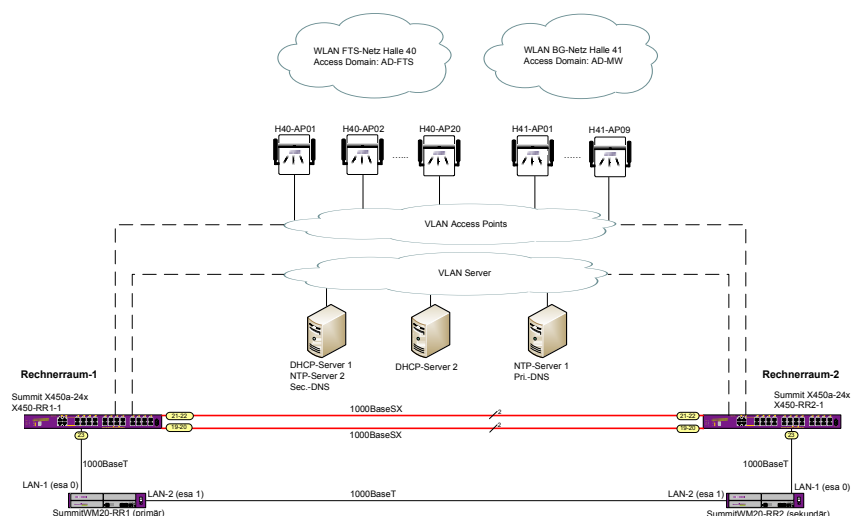


Funkübertragung im a-Standard für FTS

© 2009 DEUTZ

Das WLAN wurde im Juli 2009 in Betrieb genommen. Die Basis der WLAN-Infrastruktur bilden zwei redundant verschaltete Extreme Networks SummitWM-Controller (jeweils 1x pro RR) sowie insgesamt 18 Access Points (APs). Die APs sind hierbei Thin Access Points. Sie erhalten ihre Konfiguration nach Inbetriebnahme über einen IP-Tunnel vom Controller. Mittels Dynamic Radio Management (DRM) sind die Access Points in der Lage, ihre Funkparameter bei Störung einer Funkzelle automatisch anzupassen. Die APs können hierdurch den Ausfall eines benachbarten APs durch Leistungserhöhung kompensieren.

Die Administration des WLANs erfolgt über die Controller. Das WLAN ist in dedizierten Access Domains (separate SSIDs für FTS-WLAN und ein weiteres WLAN-Netz) aufgeteilt. Die Verschlüsselung erfolgt gemäß WPA2/AES bzw. WPA/TKIP. Jedes WLAN-Netz besitzt einen eigenen IP-Adressbereich. Die hochverfügbare WLAN-Controller-basierte Lösung in Kombination mit den Thin Access Points ermöglicht die zentrale Verwaltung und Überwachung des WLAN-Zugriffs.



WLAN-Infrastruktur für FTS

© 2009 GORDION

Es erlaubt das separate Rebooten von Diensten, beispielsweise von Netlogin, EAPS, BGP oder OSPF. Dabei wird jeder Prozess in Echtzeit kontrolliert. Die Möglichkeit von partiellen Reboots bzw. der automatische Restart einzelner Prozesse unterstützt dabei eine höhere Verfügbarkeit des Systems.

Hitless Failover

Innerhalb der BlackDiamond-Systeme sowie in den X250/X450er Stacks unterstützt Hitless Failover sehr schnelle Umschaltzeiten bei Ausfall des Masters. Dies wird durch gezielte Synchronisation der Master-Unit mit dem Backup Node erzielt. Innerhalb der Synchronisation werden beispielsweise Statusinformationen zu Netlogin, PoE, ESRP oder LACP (Link Aggregation Control Protocol) ausgetauscht. Somit müssen diese Informationen bei Ausfall des Masters nicht neu gelernt werden.

Security-Features

Das ExtremeXOS™ Betriebssystem unterstützt neben der Hochverfügbarkeit, u.a. auch nützliche Security-Features, welche im Folgenden kurz skizziert

werden. Im Vordergrund stehen hierbei Funktionen für *Network Login*, *Access Lists (ACLs)*, *Denial of Service-Schutz (DoS)*, *IP- und MAC-Adress Protection*, sowie *Protocol Anomaly Detection*.

Network Login

ExtremeXOS™ ermöglicht eine Autorisierung der User per Network Login. Unterstützt werden drei Varianten zur Zugangskontrolle:

- 802.1x Agent-based Login
- Web-based Login
- MAC-based Login

Durch Verwendung dieser Verfahren wird sichergestellt, dass nur autorisierte Teilnehmer und Geräte Zugang in das Netzwerk erhalten. Alle drei Varianten sind hierbei auf einem Port kombinierbar und können simultan konfiguriert werden.

„Multiple Supplikat“-Unterstützung

Das System ist zudem „Multiple Supplikat“-fähig, d.h. es werden pro Port einzelne Teilnehmer (Benutzer / Endgeräte) authentifiziert und nicht der komplette Port. So wird insbesondere verhindert, dass der komplette Datenverkehr durchgeleitet wird, nachdem

(lediglich) der erste Teilnehmer am Port erfolgreich authentifiziert wurde.

Access Lists (ACLs)

Pro VLAN, Port oder Portgruppe können Access Lists (ACLs) zur Filterung des Datenverkehrs verwendet werden. Basierend auf Layer2/3/4-Informationen ist eine Blockierung unerwünschter Dateninhalte möglich. So können beispielsweise MAC- (Layer2) oder IP-Adressen (Layer3), bzw. Dienste wie Telnet oder FTP (Layer4) gefiltert werden. Darüber hinaus sind ACLs zum Umschreiben (Remapping) der Priorität (IEEE802.1p und DSCP DiffServ Code Point) sowie für Policy based Routing verfügbar.

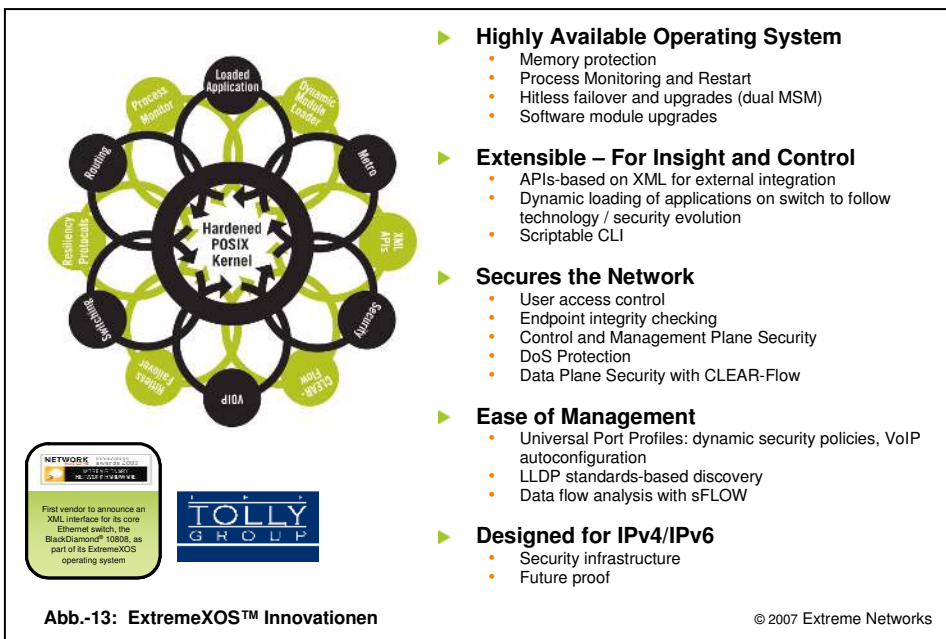
Automatischer Schutz

vor Denial of Service (DoS) Attacken

Die EXOS-basierten Switches sind in der Lage, sich automatisch vor DoS-Attacken zu schützen. Sie erkennen Anomalien beispielsweise in Form von einer ungewöhnlich hohen Anzahl von Paketen in der Input-Queue, erstellen automatisch diesbezüglich ACLs und stoppen den Zugang dieser Pakete zur CPU. Nach einer gewissen Zeitdauer werden diese ACLs automatisch wieder aufgehoben und notfalls wieder reaktiviert, sollte die Attacke andauern. Flankiert wird der DoS-Schutz durch ASIC-basiertes *Longest Prefix Match Routing (LPM)*.

IP- und MAC-Adress Protection

EXOS hat verschiedene Verfahren implementiert, um Attacken mittels gefälschter IP- oder MAC-Adressen zu erschweren. So kann durch das *MAC Adress Security-Feature* die Anzahl der am Port zugelassenen Teilnehmer begrenzt oder statisch vorgegeben werden. Letzteres ermöglicht eine genaue



Zuordnung der erlaubten Teilnehmer am Port. *Trusted DHCP* verhindert den Betrieb nicht zugelassener (rogue) DHCP Server. Zudem behindern mehrere integrierte Features die missbräuchliche Nutzung von IP-Adressen durch nicht autorisierte Stationen (*ARP-Validation*, *Source IP Lockdown*, *Gratuitous-ARP-Protection* sowie *Abschaltung des ARP-Learning-Mechanismus*).

Protocol Anomaly Detection

Die EXOS-Switches der a- und e-Serie erkennen bestimmte Kombinationen im IP- und TCP-Header, welche nicht Bestandteil einer normalen Daten-Kommunikation sind (z.B. illegale TCP Flag-Kombinationen, hervorgerufen durch Netzwerkscanner). Alle durch den Switch erkennbaren Anomalien können im SwitchASIC in wirespeed gefiltert werden.

Konfiguration des Netzzugangs, abhängig vom angeschlossenen Endgerät bzw. der Tageszeit (Provisioning).

Trigger

Aktuell sind folgende Trigger bzw. auslösende Ereignisse in ExtremeXOS™ implementiert:

- Geräte-Erkennung mittels LLDP, z.B. für VoIP-Telefone: angeschlossen / nicht angeschlossen (detect / undetect)
- An/Abmeldung von Endgeräten mittels Netlogin (z.B. 802.1x oder MAC-based)
- Zeit-gesteuerte Auslöser
- Ereignis-gesteuerte Auslöser

Verwaltungs-/ Erstellungshilfe/ Scripting

Die Extreme Networks Management-Software *EPICenter™* stellt einen Universal Port Manager (UPM) sowie einen Skript-Editor zur einfachen Administration dieses Featuresets zur Verfügung. Das Scripting wird auf allen EXOS-Switches unterstützt. Die UPM-Profil und Skripte können auch manuell erstellt werden, z.B. für eine automatisierte Konfiguration der Geräte. Die EXOS-Systeme akzeptieren auch *Tcl/Tk* als Skript-Befehlssprache. Es gibt zudem eine Extreme Networks-Community: www.EtherNation.net. Dort stehen diverse Skripte (Widgets), Infos, Erfahrungen und Beispiele zur freien Verfügung, u.a. ein XML-Software Development Kit (SDK).

Sicheres Management

Zur sicheren Administration der Switches stehen mittels SSH, SCP, HTTPS und SNMPv3 mehrere sichere Kommunikationskanäle zur Verfügung. Als unverschlüsselte Varianten können Telnet, TFTP, HTTP & SNMPv1/2 genutzt werden.

Out-of-Band Management & WebGUI

Alle EXOS-basierten Switches verfügen zudem über einen Ethernet Management-Port für ein sicheres Out-of-Band Management sowie über ein WebGUI-based Device-Management (*ScreenPlay*).

Hardware-based sFlow

sFlow ermöglicht ein kontinuierliches Monitoring von Application Level Datenverkehr, gleichzeitig auf allen Ports. sFlow ist auf den EXOS™-Geräten der aktuellen Generation hardware-basierend integriert und unterstützt (mittels sFlow-Collector ≡ Management-Programm) eine Überwachung des Netzes im Hinblick auf Anomalien. Zudem liefert sFlow Daten zur Netzoptimierung, z.B. zu Kommunikations-Beziehungen und zur Protokollverteilung.

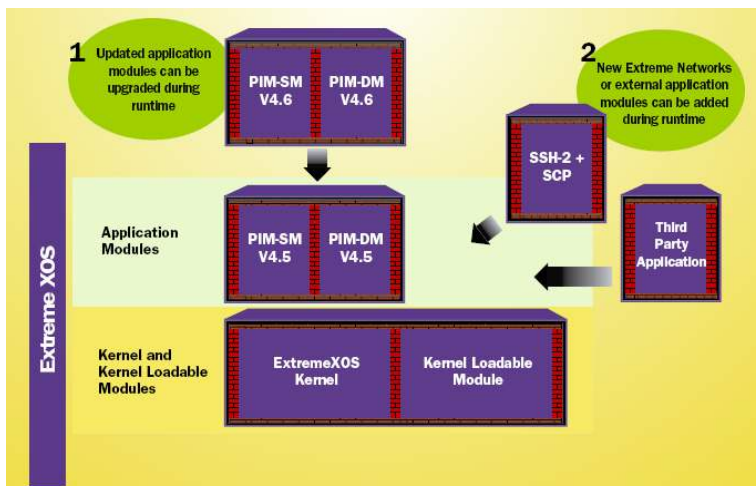


Abb.-14: ExtremeXOS™ — Modulares Design

© 2007 Extreme Networks

Universal Port & Scripting

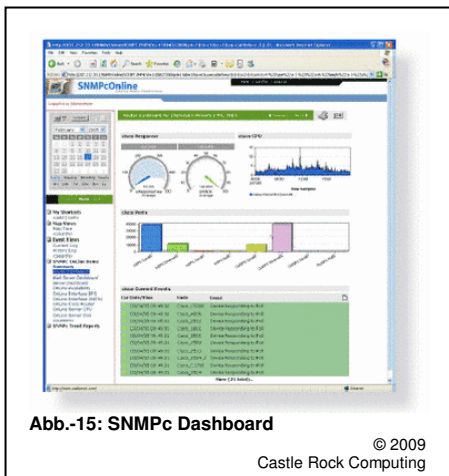
ExtremeXOS™ bietet ab der Edgelizenz das *Universal Port-Featureset*. Universal Port ermöglicht eine User-spezifische Konfiguration der Switch-Ports. Hierbei verwendet Universal Port dynamische Profile, die bei bestimmten Ereignissen (sogenannte Trigger) auf Switch-Ports zum Einsatz kommen. Universal Port ist ein Software-basiertes Feature. Zielsetzung ist die automatische

Dynamische Profile

Das Universal Port Featureset bietet dynamische Profile, welche folgende Portparameter beinhalten können: VLAN, QoS, ACL, PoE und IP-Security (z.B. DoS-Protect). Die Dynamik korreliert hierbei mit dem Inhalt der Profile, welche Variablen enthalten können. Die notwendigen Universal Port-Profil (ASCII / Textdatei) stehen im Switch FLASH-Speicher und somit lokal zur Verfügung.

Management

Für das Management sowie zur SLA-Überwachung des Netzes nutzt das Industrial IT Team von DEUTZ die SNMPc-Lösung von Castle Rock Computing. Im Einsatz sind der *SNMPc Network Manager* in der Enterprise Edition zur Abfrage der Systeme und die *SNMPc Online 2009 Reporting* Lösung zur Darstellung der Reports mittels Webserver (vgl. Abbildung-12).



Hierbei bietet die Lösung zahlreiche private (Hersteller-) und standard (RFC-) basierte MIBs inklusive einem Compiler zur Integration neuer MIBs.



Das Industrial IT-Projektteam der DEUTZ AG in Köln-Porz:
v. l.: Martin Feller (Leiter), Bernd Bärsch, Karl-Heinz Lohoff, Christian Mandt und Sven Hums

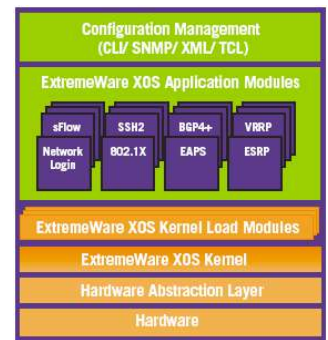
Fazit

Der Ausbau des Netzwerkes und das WLAN wurden frühzeitig und ganzheitlich gemeinsam mit den Ingenieuren von GORDION geplant. Die wesentlichen Komponenten standen bereits im Juli 2009 zur Verfügung und wurden ohne Produktionsstörung in das Gesamtsystem integriert.

„Die installierten Komponenten sind ideal auf die Belange der vorhandenen IT-Systeme zugeschnitten und unterstützen sowohl alte als auch neue Technologien“, bilanziert Teamleiter Martin Feller und blickt dabei auf fast zwei Jahre Projektarbeit zurück. „Wesentliches Merkmal des Redundanz-Konzeptes ist für uns hierbei die extrem schnelle Umschaltzeit der Komponenten, welche auch im möglichen Fall eines Defektes einen reibungslosen Produktionsbetrieb gewährleistet.“

Oliver Lindlar und Thomas Hülsiggensen,
GORDION

ExtremeXOS™ (EXOS) vom Edge bis zum Core



Das modulare Switch-Betriebssystem EXOS ist durchgängig verfügbar, vom Edge bis zum Core. Die X250/X450er-Switches sowie die BlackDiamond-Systeme unterstützen wire-speed IPv4- / IPv6-Routing in Hardware.



Summit X150er (L2) & Summit X250er Serie

Fast Ethernet Switches, mit 24x oder 48x 10/100TX, plus 2x 10/100/1000T (shared SFP), inkl. PoE-Varianten, inkl. Ethernet Out-of-Band Management Port, opt. Red. PSU. Die Summit X250er Serie (Layer3) ist stapelbar per SummitStacking und verfügt zudem über ein 24-Port SFP Fast Ethernet Modell.



Summit X350er (L2) & Summit X450er Serie

Triple Speed Layer3 Ethernet Switches, mit 24x oder 48x 10/100/1000T, davon 4x shared SFP, optional 10Gig, inkl. SummitStacking, inkl. Ethernet Out-of-Band Management Port, opt. Red. PSU. Die X450er Serie verfügt zudem über ein 24-Port SFP Gigabit Ethernet Modell sowie über PoE-Varianten.



Summit X650er Serie

Layer3 10Gigabit Ethernet Switches, mit 24x 10Gig SFP+ oder 24x 10Gig Copper Ports.



BlackDiamond 8800er Serie

Modulare Switchsysteme mit 8x (BD8810) bzw. 4x (BD8806) I/O Slots, diverse I/O-Module (8500er Edge, 8800er Core, 8900 Core, inkl. PoE, bis zu 128 Gbps Performance pro Slot).

Weitere Informationen:

www.gordion.de
www.extremenetworks.com
www.ethernation.net
www.deutz.com

Copyright ©2010 GORDION. Alle Rechte vorbehalten. Ausgewiesene Logos, Marken, Firmennamen und Produktdesigns gehören ihren jeweiligen Eigentümern.