Carrier Class Switching

Netzwerk-ReDesign im Landratsamt Bad Homburg, Hochtaunuskreis.

Extreme Networks BlackDiamond 8800er und Summit X450er Serie ermöglichen Carrier Class Switching und „Gigabit to the Edge“ in der Kreisverwaltung.

Modulares Betriebssystem Extreme XOS™ unterstützt Hochverfügbarkeit, Security und Universal Port-Technik.

Das Landratsamt Bad Homburg im Hochtaunuskreis (Hessen) betreibt seit März 2007 ein hochverfügbares Datennetzwerk, basierend auf Aktiven Komponenten des Herstellers Extreme Networks. Vor dem Hintergrund des durchgeführten Netzwerk-ReDesigns beschreibt der Artikel die Funktionsweise und das Featureset der Switchsysteme. Neben der Darstellung der eingesetzten Carrier Class Technologie (BlackDiamond 8800er und Summit X450er Switches) beleuchtet der Bericht insbesondere das breite Featureset des modularen Switch-Betriebssystems *ExtremeXOS*™ (*EXOS*), welches auf den Extreme Networks XOS-Switches einheitlich verfügbar ist.

www.hochtaunuskreis.de

Landratsamt Bad Homburg, Hochtaunuskreis

Der Hochtaunuskreis ist 1972 aus den Landkreisen Obertaunus und Usingen entstanden. Er liegt am Rande des Rhein-Main-Gebietes, dem nach der Bevölkerungsanzahl zweitgrößten Verdichtungsraum der Bundesrepublik, im Zentrum des Landes Hessen und wird begrenzt durch die Landkreise Main-Taunus-Kreis (Südwesten), Rheingau-Taunus-Kreis (Westen), Limburg-Weilburg (Nordwesten), Wetteraukreis (Osten) und der Stadt Frankfurt am Main (Südosten). Mit seinen 13 Städten und Gemeinden hat der Hochtaunuskreis eine Flächengröße von 482,04 km². Insgesamt leben derzeit über 227.000 Menschen im Hochtaunuskreis. Das entspricht einer Bevölkerungsdichte von 471 Einwohnern pro km².

Im Landratsamt Bad Homburg stehen der Bevölkerung rund 700 Mitarbeiter zur Unterstützung in diversen Fachbereichen zur Verfügung. Die Kreisverwaltung ist dabei in entsprechende Geschäftsbereiche strukturiert (Zentrale Dienste, Infrastruktur, Bau und Umwelt, Soziales, Arbeit, Bildung und Schule, Jugend und Freizeit u.a.).

IT-Service bietet Hosting für Städte und Gemeinden

Der Fachbereich IT-Service verantwortet im Landratsamt die informationstechnische Versorgung der Mitarbeiter. Neben den fachspezifischen Applikationen für die diversen Geschäftsbereiche (verteilt auf 120 Server; MS-Windows2003, Linux, Citrix) verwaltet der IT-Service auch die rund 850 Email-Konten für die Mitarbeiter (ca. 10.000 Emails täglich). Darüber hinaus dient der IT-Service als Provider für die 59 öffentlichen Schulen (Projekt Schule digital s.u.) sowie für einen Teil der 13 Städte und Gemeinden im Landkreis. Hier stellt die IT neben den rund 3.000 Email-Konten auch das Hosting der Homepages sowie den Zugriff auf fachspezifische Applikationen zur Verfügung.

Schule digital – Fernwartung aus dem Landratsamt

Im Rahmen des Projekts "Schule digital" wurden seit dem Start im August 2000 rund 4.000 EDV-Anlagen in den 59 öffentlichen Schulen des Landkreises installiert und an die Fernwartung des IT-Services angekoppelt. In die gesamte Technik – Leitungen, Rechner, Bildschirme, Drucker, teilweise auch schon Laptop-Beamer – wurden bislang über 7,5 Millionen Euro investiert. Das Ergebnis kann sich EU-weit sehen lassen. Im Hochtaunuskreis steht ein Computer für acht Schüler zur Verfügung (EU-Forderung: ein PC á 15 Schüler). In den Grundschulen verfügen die Klassenräume über IT-Ecken sowie über einen EDV-Fachraum. In den höheren Schulen stehen mehrere EDV-Fachräume je Schule zur Verfügung.

Kreisverwaltung ist Dienstleister

IT-Service mit Provider-Charakter

Eine Kreisverwaltung ist letztlich ein Dienstleister. Sie stellt ihren Kunden (den Bürgern) spezifische Leistungen zur Verfügung; beispielsweise Führerschein- und KfZ-Zulassungen, Betreuung öffentlicher Schulen oder Soziale Dienste. In Bad Homburg stehen den Bürgern hierfür rund 700 Mitarbeiter in der Kreisverwaltung zur Verfügung, welche in insgesamt neun Geschäftsbereichen vertreten sind. Informationstechnische Dienstleistungen bietet im Hochtaunuskreis der Geschäftsbereich *IT-Service*. Der IT-Service versorgt neben den fachspezifischen Applikationen der Geschäftsbereiche u.a. 120 Server sowie 850 Email-Konten für die Mitarbeiter. Einige Dienstleistungen der Bad Homburger haben im Grunde genommen Provider-Charakter. So werden beispielsweise die 59 öffentlichen Schulen im Kreisgebiet mittels IT-Fernwartung zentral aus dem Landratsamt versorgt

(Projekt *Schule digital*, vgl. Kasten). Auch können die Schulen, Städte und Gemeinden auf einen Web-/ Email-Hosting-Service zugreifen, welcher durch den IT-Service der Kreisverwaltung bereitgestellt wird. Gleiches gilt für die externe Nutzung von fachspezifischen Applikationen (z.B. Geoinformations-system).

Carrier Class Komponenten für Hochverfügbarkeit & Security

Im Hinblick auf das Redesign der Aktiven Komponenten im Netzwerk war insofern von vornherein klar, dass die benötigten Switchsysteme nicht nur der LAN-Ausstattung im eigenen Hause genügen, sondern auch Carrier Class Anforderungen erfüllen müssen, insbesondere im Hinblick auf die Hochverfügbarkeit und die Sicherheit. Ein Netzwerk-Ausfall und damit verbunden eine Trennung von digitalen Resourcen wird in der heutigen Zeit nicht mehr toleriert. De facto sind die meisten Dienste und Applikationen direkt abhängig von einer funktionierenden Netzwerk-Infrastruktur. Vor diesem Hintergrund und nicht zuletzt in Anbetracht des breiten Leistungsspektrums des ExtremeXOS™-Betriebssystems entschieden die Carrier Class- Switches von Extreme Networks das Rennen für sich, basierend auf einem Layer3 Netzdesign.

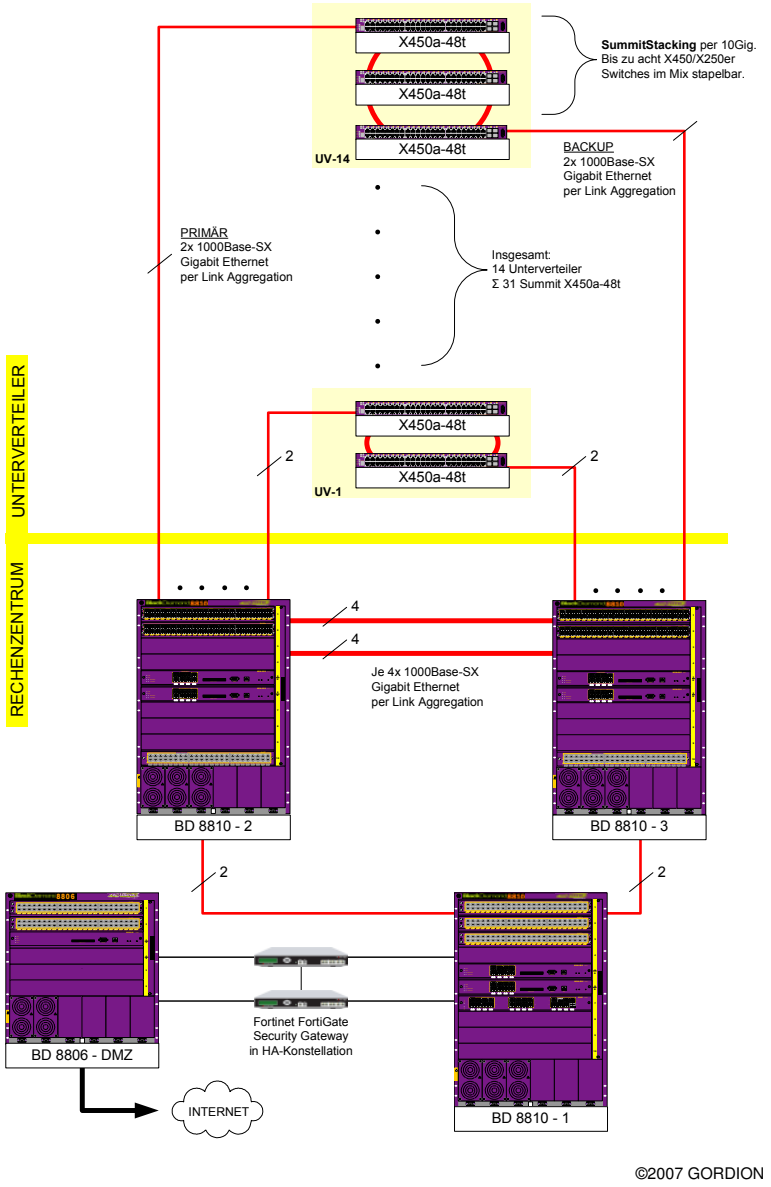


Abb. 1: Layer3 10/100/1000Mbps Ethernet Netzdesign, inkl. Hochverfügbarkeit per ESRP

Layer3 Netzdesign

Netzwerk-Struktur

Die Kreisverwaltung verfügt über eine strukturierte Verkabelung, alle Unterverteiler sind sternförmig mittels Glasfaser angebunden. Den Kern des Ethernet-Netzwerks im Landratsamt bildet ein Hauptverteiler im Rechenzentrum (RZ). Ausgehend von diesem Hauptverteiler sind 14 Unterverteiler mittels Lichtwellenleiter (LWL) redundant per Gigabit Ethernet (2x 1000BaseSX mittels Link Aggregation) angeschlossen (vgl. Abbildung 1).

LWL-Hybrid-Verkabelung unterstützt zukünftige 10Gig-Anbindungen

Neben den Multimode-Glasfasern verfügt der Sekundärbereich zusätzlich auch über Monomodefasern (9/125µm) zu den Unterverteilern. Diese Hybridverkabelung ist durchaus von Vorteil, insbesondere für zukünftige Performancesteigerungen auf den Verbindungen. Bei der Integration von 10Gigabit Ethernet Verbindungen (z.B. mittels *10GBase-LR* Standard) unterstützten die 9µm-Fasern eine unkomplizierte Realisation. Unabhängig von Distanzlimitierungen, welche im Multimodenbereich hinsichtlich des Bandbreitenlängenverhältnis der LWL gegeben sind.

Layer3-Technologie von Extreme Networks

Grundlage des Netzes in der Kreisverwaltung ist ein Layer3-Netzdesign, basierend auf dem IPv4-Netzwerkprotokoll.

Das Design ist ausgelegt für ein IP-Netz pro Unterverteiler und bietet ausreichend Adreßbereiche für eine strukturierte Adreßvergabe:

- Bereich mit festen IPs für PCs
- Bereich mit Endgeräte-IPs, welche per DHCP vergeben werden (PCs, Notebooks, PDAs)
- Bereich mit festen IPs für Drucker
- Bereich mit festen IPs für die Netzwerk-Infrastruktur (Switches)

Abschottung der Unterverteiler gegen Layer2-Netzstörungen

Das Layer3-Konzept beinhaltet IP-Netze pro Unterverteiler und ermöglicht so eine Abschottung der Unterverteiler gegen Layer2-Netzstörungen aus anderen Bereichen. Das Routing erfolgt dabei zentral auf den redundanten Coreswitches. Dies ermöglicht eine einfache Konfiguration und Administration der Edge-Switches und verlagert alle komplexen Konfigurationsinhalte in den Core. Der Einsatz von Etagen-übergreifenden VLANs ist möglich.

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

VLAN-Struktur

Im Netzwerk der Bad Homburger werden portbasierende VLANs eingesetzt. Pro Unterverteiler gibt es ein VLAN sowie ein IP-Netz, welches auf diesem VLAN läuft. Dies ermöglicht eine simple Administration und vereinfacht das „Auffinden“ von Endgeräten im Netzwerk. Die Server sind mittels separatem VLAN im eigenen IP-Netz angeschlossen und befinden sich somit nicht gemeinsam in einer Broadcast-Domäne mit Anwender-PCs. Die Unterverteiler sind auf ein Coreswitch-Paar aufgeteilt (vgl. auch Abbildung 1 auf Seite 2).

Aktive Komponenten

Coreswitches

Der aktive Kern (Core) des Ethernet-Netzwerks im Landratsamt besteht aus drei modularen Coreswitch-Systemen in redundanter Konfiguration. Dies verhindert einen „Single Point of Failure“, welcher einen Totalausfall durch einen einfachen Komponentendefekt bewirken könnte.

Als zentrale Coreswitches fungieren leistungsstarke, modulare Layer3 Carrier Class Systeme von Extreme Networks (vgl. Abbildung 1 auf Seite 2 sowie Abbildung 3 und 4 auf Seite 4). In Bad Homburg sind die BlackDiamond 8800er Switchsysteme im Einsatz (BD8800er), welche pro BD8810er Switch eine Performance von 384Gbps bzw. 48Gbps pro I/O-Slot bereitstellen. Zur Anbindung der Infrastruktur stehen diverse I/O-Module zur Verfügung, darunter 48-Port 10/100/1000T (auch als PoE-Variante verfügbar), 48-Port 1000BaseX (SFP Mini-GBIC-based) sowie 4-Port 10Gig-Module (XFP- , XENPAK-based oder Kupfer), vgl. auch Abbildung 2 unten).

3x BlackDiamond 8810 als Coreswitches

Der BD8810-1 arbeitet als zentrales Default-Gateway für die Kreisverwaltung (Core-Router, vgl. Abbildung 3, Seite 4). Neben dem Email-Server sind hierüber auch externe Lokationen an das Landratsamt angeschlossen (z.B. Veterinäramt). An den Core-Router sind zwei weitere BlackDiamond 8810er Switch-Systeme angebunden (BD8810-2 und BD8810-3, vgl. Abbildung 4, Seite 4), welche als Standort-Switches redundant die Unterverteiler versorgen sowie für die Anbindung der Server zur Verfügung stehen. Zwischen den Standort-Switches ist eine 2x 4Gbps-Verbindung mittels Link Aggregation konfiguriert. Zu den Unterverteilern besteht eine 2Gbps-Verbindung, jeweils per 1000Base-SX.

1x BlackDiamond 8806 als DMZ-Switch

In der „Demilitarized Zone“ (DMZ) nutzt die Kreisverwaltung das BackDiamond 8806er Switch-System als DMZ-Switch.

Module Name	G48Te	G48Pe	G48Ta	G48Xa	G48T	G48P	G48X	MSM-G8X[1]	10G4X	10G4Xa	10G4Ca
10/100/1000 BASE-T ports	48	48 PoE	48	/	48	48 PoE	/	/	/	/	/
1000X Mini-GBIC ports	/	/	/	48	/	/	24	8	/	/	/
10GBASE-X XENPAK ports	/	/	/	/	/	/	/	/	4	4	4
Backplane capacity (Gbps) 2*MSM/1*MSM	24/12	24/12	48/24	48/24	48/24	48/24	48/24	12	48/24	48/24	48/24
Load Sharing Groups	128	128	128	128	128	128	128	128	32	128	128
Jumbo Frame per port	Per Port	Per Port	Per Port	Per Port	Per System	Per System	Per System	Per System	Per System	Per Port	Per Port
Layer 2 MAC FDB	8K per module	8K per module	16K per module	16K per module	16K per module	16K per module	16K per module	16K per module	16K per module	16K per module	16K per module
IPv4 LPM entries	512	512	12K	12K	8K	8K	8K	8K	8K	12K	12K
IPv6 forwarding	Hardware	Hardware	Hardware	Hardware	Software	Software	Software	Software	Software	Hardware	Hardware

©2007 Extreme Networks

Abb. 2: Modultypen der BD8800er Serie. Bis zu 48Gbps Performance pro Modul.

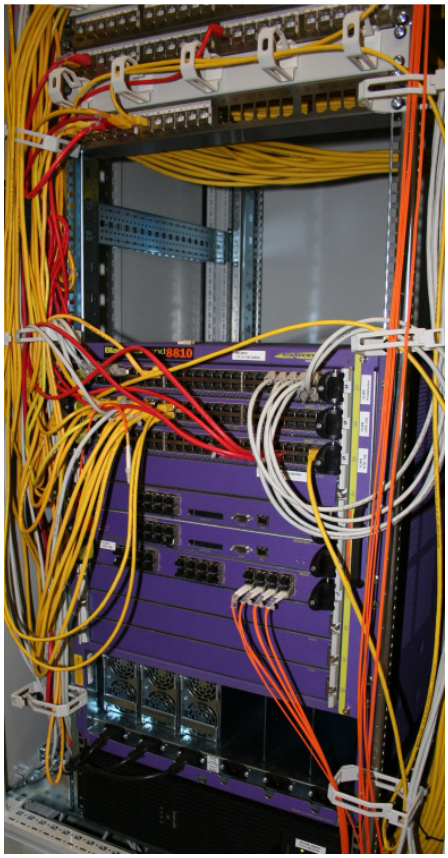


Abb. 3: BlackDiamond 8810-1 im RZ (Core-Router)

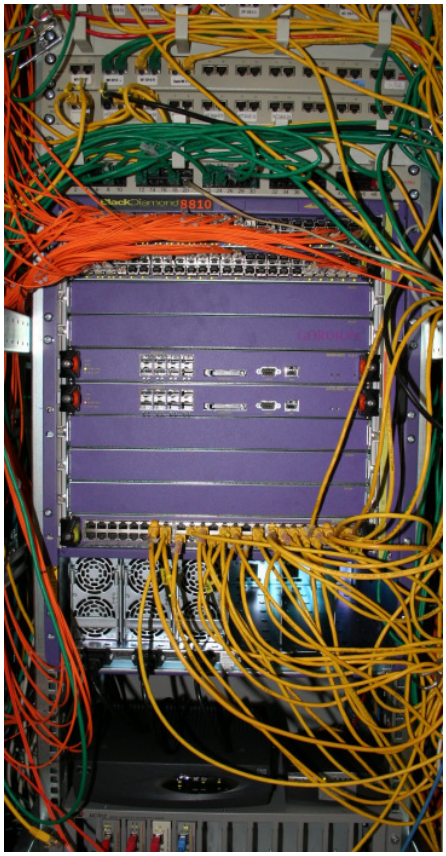


Abb. 4: BlackDiamond 8810-3 im RZ (Standort-Switch)

Der BD8806 ist kleiner als das BD8810er System (vier I/O-Slots anstatt acht), verfügt aber ansonsten über das gleiche Featureset-Spektrum.

Das Landratsamt in Bad Homburg nutzt einen performanten 50Mbps Internet-Zugriff und verwendet den BD8806er zur Versorgung externer Lokationen bzw. als Infrastruktur-Switch für die Bereitstellung von entsprechenden Resourcen: u.a. Webserver, Homepage-Hosting für rund 30 öffentliche Schulen, Versorgung für „Schule digital“ (vgl. Kasten auf Seite 1), sowie fachspezifische Applikationszugriffe für Städte und Gemeinden (z.B. auf das Geoinformationssystem). Ein Fortinet Security Gateway HA-Cluster dient in dieser Konstellation als Firewallsystem (*ASIC*-basiert, Wirespeed Scanning, vgl. Abbildung 7, rechts).

Edgeswitches mit Triple Speed ermöglichen “Gigabit to the Edge”

In den 14 Unterverteilern der Kreisverwaltung steht die SummitX450er-Serie zur Verfügung. Diese Switches sind ebenfalls Carrier Grade-Systeme, verfügen auch über das ExtremeXOS™-Betriebssystem, und ermöglichen einen 10/100/1000Mbit/s TripleSpeed Ethernet Zugriff im Etagenbereich (Edge).

31x SummitX450a-48t als Edge-Switches

An den Core sind insgesamt 14 Unterverteiler redundant mit je zwei Gbps (per Link Aggregation) angeschlossen. Je nach benötigter Portanzahl im Unterverteiler sind die X450er-Switches in 1er-, 2er- oder 3er-Stacks gruppiert. Ein 3er-Stack stellt hierbei 3x 48-Ports mit 10/100/1000T, also 144 Triple Speed Ports aggregiert zur Verfügung. Alle Etagenswitches verfügen über eine redundante Stromversorgung (vgl. Abb.6).

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 und X450er Serie) im Mix gestapelt werden (vgl. Abbildung 5).

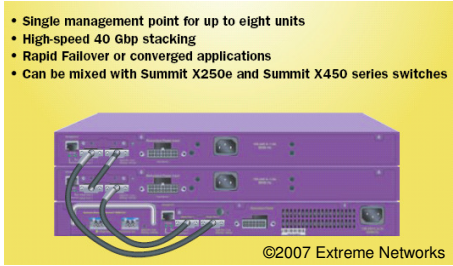


Abb. 5: SummitStacking per 10Gig

Abb. 6: Summit X450a-48t im Unterverteiler (3er Stack, jeweils mit redundanter PSU)

Abb. 7: Fortinet FortiGate HA-Cluster

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.*

Der Hochtaunuskreis setzt in 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™.

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: ESRP, OSPF

Zur Steuerung der redundanten Topologie werden im Landratsamt Bad Homburg 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 des Hochtaunuskreises übernimmt diese Aufgabe das *Extreme Standby Router Protocol* (*ESRP*). *ESRP* steuert die Redundanzen zentral auf den Coreswitches. Das Verfahren ist sowohl für Layer2- als auch für Layer3-Redundanzstrategien geeignet und erfordert nur die Aktivierung des ESRP-Aware-Modes auf den redundant angeschlossenen Etagen-Switches.

ESRP mit Vorteilen gegenüber STP und VRRP

Im Vergleich zu ESRP benötigt die STP/VRRP-Redundanzsteuerung zwei Protokolle: das *Spanning Tree Protocol (STP)* für Layer2- und das *Virtual Router Redundancy Protocol (VRRP)* für die Layer3-Redundanzsteuerung.

Im weiteren Vergleich bedingt Spanning Tree eine Konfiguration des STP-Protokolls auch auf den Etagenswitches. Dies erhöht allerdings den Administrationsaufwand der Switches sowie das Störungspotential der Konstellation im Betrieb. Zudem sind STP und VRRP im Client-VLAN aktiv und können daher durch geeignete Tools PC-seitig beeinflusst werden.

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 Kreisverwaltung wird hierzu das Routingprotokoll *Open Shortest Path First (OSPF)* eingesetzt.

Redundanz-Umschaltung in 3 Sekunden

Im Rechenzentrum bilden die zwei BD8810er Core-Switches ein Redundanz-Paar. Die Redundanz-Umschaltung erfolgt hierbei innerhalb von ca. 3 Sekunden. Auslöser für eine Redundanz-Umschaltung ist entweder ein Link-Down an einem Uplink-Port zu einem Etagen-/ oder Core-Switch oder der Ausfall eines primären Core-Switches. Noch kürzere Umschaltzeiten sind mit *EAPS/VRRP* erreichbar. Diese Redundanzmechanismen ermöglichen Umschaltzeiten unterhalb einer Sekunde.

Abb. 8: Rechenzentrum Hochtaunuskreis

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 12k, 10k, 8800er Serie), im Smart Core- / Gigabit Aggregation-/Distributions-Bereich (BD8800 & X450er Serie) sowie im Edge (Summit X450, X250e 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 im Landratsamt Bad Homburg 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, Multithreating und Memory-Protection. 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 Authorisierung 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 authorisierte Teilnehmer und Geräte Zugang in das Netzwerk erhalten. Alle drei Varianten sind hierbei auf einem Port kombinierbar und können simultan konfiguriert werden.

„Multiple Supplikant"-Unterstützung

Das System ist zudem „Multiple Supplicant"-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.

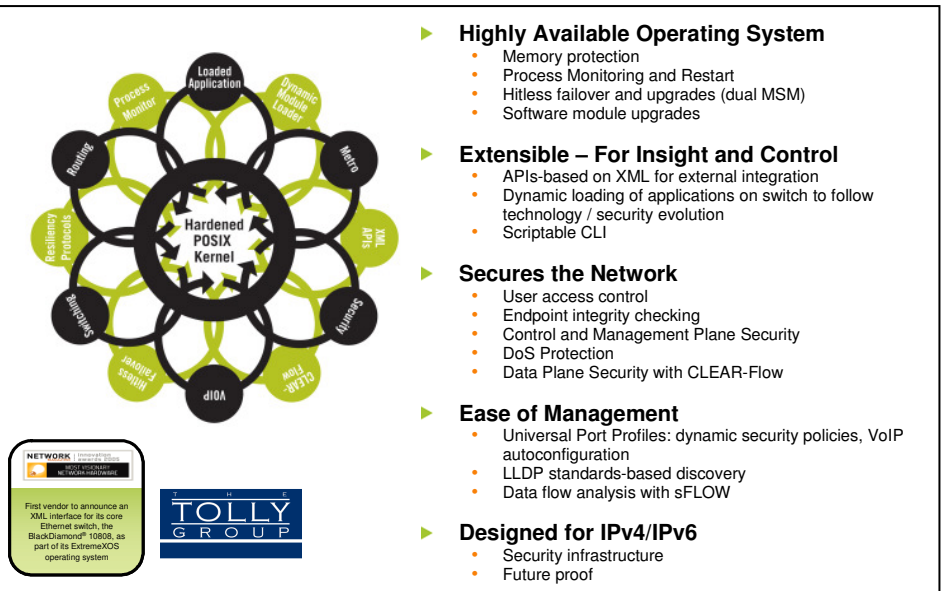


Abb. 9: ExtremeXOS™ Innovationen

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 authorisierte 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 Switch-ASIC in Wirespeed gefiltert werden.

Universal Port

ExtremeXOS™ bietet darüber hinaus 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 Konfiguration des Netzzugangs, abhängig vom angeschlossenen Endgerät bzw. der Tageszeit (Provisioning).

Trigger

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

- Geräteerkennung 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)
- Zeitgesteuerte Auslöser

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-Profile (ASCII / Textdatei) stehen im Switch FLASH-Speicher und somit lokal zur Verfügung.

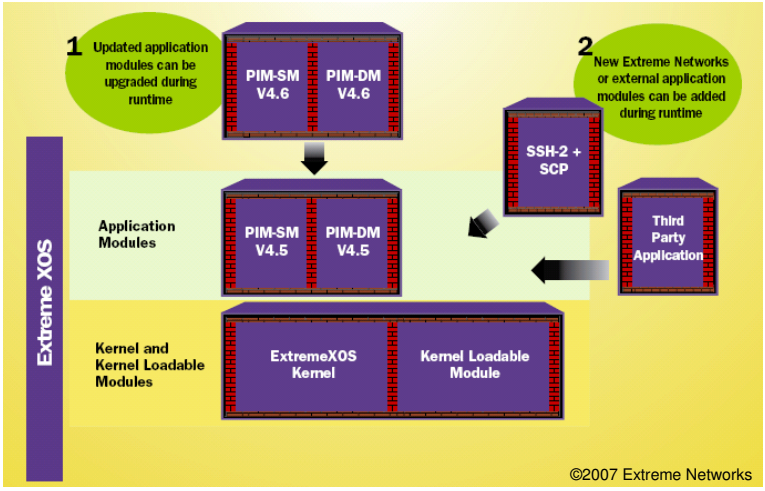


Abb. 10: ExtremeXOS™ — Modulares Design

Verwaltungs-/ Erstellungshilfe

Die Extreme Networks Management-Software *EPICenter*™ stellt einen Universal Port Manager zur Verfügung und ermöglicht eine einfache Administration dieses Featuresets. Eine Management-Station ist für die Anwendung der Profile nicht notwendig.

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 und SNMPv1/2 verwendet 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 ExtremeXOS™-Geräten der aktuellen Generation hardware-basierend integriert und unterstützt (mittels sFlow-Collector ≡ Management-Programm) eine Überwachung des Netzwerks im Hinblick auf Anomalien. Des Weiteren liefert sFlow Daten zur Netzoptimierung, z.B. zu Kommunkations-Beziehungen und zur Protokollverteilung.

Zentrales Management mit EPICenter™

Zur Verwaltung des Netzes nutzt das Landratsamt die Management-Plattform EPICenter™. Die Software basiert auf einer offenen System-Architektur und bietet zahlreiche Features, insbesondere ein Inventory-, Alarm-, Firmware- und Konfigurations-Management. Enthalten ist zudem eine Protokoll-Überwachung (STP, ESRP, EAPS) sowie SNMPv3, SSH-2, HTTPS und LLDP-Unterstützung. Des Weiteren unterstützt EPICenter™ eine schnelle und einfache Konfiguration per Telnet-Makros. Auch die Integration von Sprach-Anwendungen in die Avaya-Plattform und -Managementsysteme sowie eine Wireless-Erkennung und -Verwaltung ist bereits integriert. Ein Policy-Manager unterstützt die Verwaltung von QoS- und ACL-Richtlinien, der integrierte Universal Port Manager hilft bei der Erstellung von Universal Port Profilen. Ein detailliertes *White Paper* ist unter www.gordion.de erhältlich.

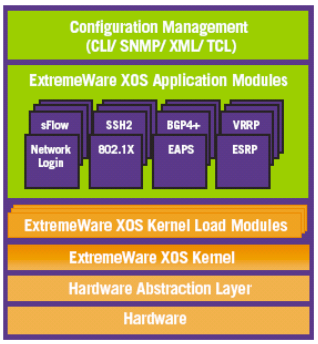
Fazit

Ausgehend vom störungsaversen Layer3-Design im Netzwerk verfügt man im Landratsamt Bad Homburg über Carrier Class Switches mit einem breitem Featurespektrum. Diese unterstützen neben der Versorgung der rund 700 Mitarbeiter insbesondere die Bereitstellung von IT-Dienstleistungen (Hosting, Fernwartung u.a.) für die Städte und Gemeinden im Kreis sowie für das Projekt *Schule digital*. Die Extreme Networks-Lösung mit ihrem modularen EXOS-Betriebssystem hat sich bewährt und hervorragend in das bestehende Netz integriert. Mit Hilfe der Hochverfügbarkeit im Netz (3 Sekunden Umschaltzeit mit ESRP & OSPF, Hitless Failover, partielle Reboots) bietet man den Anwendern einen soliden Zugriff auf die digitalen Resourcen. Darüber hinaus sichert ein adäquates, auf die Bedürfnisse der Kreisverwaltung abgestimmtes Wartungs- und Service-Konzept, die Verfügbarkeit der IT. Die Kreisverwaltung ist gerüstet.

Oliver Lindlar und Thomas Hülsiggensen,
GORDION GmbH

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 X450er Serie
Triple Speed Layer3 Ethernet Switches, mit 24x oder 48x 10/100/1000T, davon 4x shared SFP, inkl. PoE-Varianten, 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.

BlackDiamond 8800er Serie
Modulare Switchsysteme mit 8x (BD8810) bzw. 4x (BD8806) I/O Slots, diverse I/O-Module, inkl. PoE, 48 Gbps Performance pro Slot.

BlackDiamond 12800er Serie
Modulare Switchsysteme mit 4x (BD12804) bzw. 2x (BD12802) I/O Slots, diverse I/O-Module, inkl. CLEAR-Flow, opt. Hierachical QoS, opt. MPLS.

Weitere Informationen:

www.gordion.de

www.extremenetworks.com

www.hochtaunuskreis.de

Copyright ©2008 GORDION GmbH. Alle Rechte vorbehalten. Ausgewiesene Logos, Marken, Firmennamen und Produktdesigns gehören ihren jeweiligen Eigentümern.