

SOLUTION GUIDE 2016



SOLUTION GUIDE 2016



20 YEARS OF INNOVATION

1	Extreme Networks – Wir über uns	8
	Kurzprofil	8
	Wer ist Extreme Networks?	8
2	Grundlagen Netzwerk & Security	11
	Verfügbarkeit im Netz	23
	Die Infrastruktur für das Rechenzentrum der Zukunft	35
	Extreme EXOS (Extreme Operation System)	57
	Quality of Service in konvergenten Netzen	59
	Audio-Video-Bridging (AVB)	72
	IP Version 6	75
	SNMP (Simple Network Management Protocol)	79
	Scripting	80
	Universal Port	81
	Identity & Access Control	85
	Extreme Connect	90
	NetFlow, Sflow & IPFIX	94
	Software Defined Networking	96
3	Wireless LAN	99
	Szenarien	99
	Features, Facts und Autoquartett	104
	WLAN High Density & Performance	106
	Sicherung von WLAN Netzen	110
	Voice over WLAN – QoS & Security	111
	Location-Tracking in WLAN Netzen	114
	802.11n – Grundlagen in der Retrospektive	116
	802.11ac – Gigabit WLAN Wave 1 und 2	118
	ExtremeWireless Komponenten	120
	ExtremeWireless Appliances	125
	Befestigungsoptionen	128
4	LAN Komponenten	132
	S-Serie	132
	K-Serie	143
	BDX8	150

BD8000	156
X 770	162
X 670	166
X 670-G2	171
X 620	174
7100-Serie	178
X 480	180
X 460-G2	183
X 450-G2	190
X 440-G2	195
A4-Serie	199
B5-Serie	201
C5-Serie	204
D2-Serie	206
X 430	207
5 Management & Software.....	210
Extreme Management Center	210
Extreme Analytics	224
Extreme Connect	232
ExtremeSDN	235
6 ExtremeCloud.....	237
Was genau ist ein Cloud-Managed Network?	237
Die Vorteile eines Cloud-Managed Network	238
Empfehlungen bei der Evaluierung von Lösungen	239
Zusammenfassung ExtremeCloud	240
7 Technology Solution Partner Program	243
Analytik-Partner	244
Management-Partner	245
Convergence-Partner	246
Security-Partner	248
Data Center & Cloud-Partner	250
Mobility-Partner	251
8 Services	254

Wartung & Support	254
Premier Services Program (PSP)	256
Managed Services	257
Professional Services	258
Extreme Networks Training	259
Extreme Networks Community: The Hub	260
9 Weitere Informationsquellen	261

Der Solution Guide wird herausgegeben von

Extreme Networks GmbH

Solmsstrasse 83, 60486 Frankfurt am Main, Tel.: 069/47860-0

Verantwortlich für die Redaktion:

Marketing / System Engineering Group DACH

Inhalt: Stand 30. Juni 2016

Die Inhalte dieser Netzseite wurden vom Herausgeber und der Redaktion Organisationshandbuch mit größtmöglicher Sorgfalt erarbeitet und implementiert. Dennoch sind Fehler im Bearbeitungsvorgang nicht auszuschließen. Hinweise und Korrekturen senden Sie bitte an die hier aufgeführte Kontaktadresse der Redaktion Solution Guide.

Eine Haftung für die Richtigkeit, Vollständigkeit und Aktualität dieser Netzseite kann trotz sorgfältiger Prüfung nicht uneingeschränkt übernommen werden. Der Herausgeber übernimmt insbesondere keinerlei Haftung für eventuelle Schäden oder Konsequenzen, die durch die direkte oder indirekte Nutzung der angebotenen Inhalte entstehen. Der Herausgeber ist für die zur Nutzung bereit gehaltenen eigenen Inhalte nach den allgemeinen Gesetzen verantwortlich. Von diesen eigenen Inhalten sind Querverweise ("externe Links") auf die von anderen Anbietern bereitgehaltenen Inhalte zu unterscheiden, die allein in der Verantwortung der anderen Anbieter liegen.

Soweit die hier zur Verfügung gestellten Inhalte Rechtsvorschriften, amtliche Hinweise, Empfehlungen oder Auskünfte enthalten, sind sie nach bestem Wissen und unter Beachtung größtmöglicher Sorgfalt erstellt. Etwaige rechtliche Hinweise, Empfehlungen und Auskünfte sind unverbindlich.

Für das bereitgestellte Informationsangebot gilt folgende Haftungsbeschränkung: Extreme Networks haftet nicht für Schäden, die durch die Nutzung oder Nichtnutzung angebotener Informationen entstehen. Für etwaige Schäden, die beim Aufrufen oder Herunterladen von Daten durch Computerviren oder der Installation oder Nutzung von Software verursacht werden, wird nicht gehaftet.

Die auf dieser Netzseite angebotenen Muster und Beispiele stehen im Rahmen der Nutzungs- und Urheberbestimmungen zur Verfügung. Eine Veränderung der Mustervorlagen ist nur mit Genehmigung der Handbuch-Redaktion und auf schriftliche Anfrage erlaubt.

Alle veröffentlichten Inhalte (Texte, Grafiken, Bilder, Layout usw.) unterliegen dem Urheberrecht. Jede vom Urheberrechtsgesetz nicht zugelassene Verwertung bedarf vorheriger schriftlicher Zustimmung der jeweiligen Berechtigten. Dies gilt insbesondere für Bearbeitung, Übersetzung, Vervielfältigung, Einspeicherung, Verarbeitung bzw. Wiedergabe von Inhalten in Datenbanken oder anderen elektronischen Medien und Systemen.

Die kommerzielle Nutzung der hier zur Verfügung gestellten Inhalte kann von der Redaktion auf schriftliche Anfrage hin gestattet werden.

Sehr geehrte Leserin, sehr geehrter Leser,

wie freuen uns, Ihnen die neue Sommerausgabe des Extreme Solution Guide 2016 vorzustellen.

Wieder mal hat sich in unserem Lösungsportfolio einiges verändert. Die zweite Welle des Wireless Standards 802.11ac hat uns Accesspoints mit einer komplett überarbeiteten Hardware beschert. Neue Switchkomponenten für Access und Data Center runden das Portfolio weiter ab. Und auch das Extreme Management Center zeigt sich mit der Version 7 in neuem Outfit.

Bei so vielen Veränderungen ist es natürlich auch an der Zeit, den Solution Guide abzustauben und einer Frischzellenkur zu unterziehen.

In diesem Buch hat das gesamte SE-Team von Extreme Networks in Deutschland Wissen und praktische Erfahrung zusammengetragen, um Ihnen für Ihre Planungsaufgaben ein hilfreiches Kompendium an die Hand zu geben.

Ein Wort zu uns und zu unserem Selbstverständnis als passionierte Netzwerker:

- Customer Experience ist für uns mehr als ein Marketing Buzzword. Customer Experience ist, wenn ein Mitarbeiter IT Ressourcen seines Unternehmens mit derselben Leichtigkeit nutzt, mit der er auch das Licht einschaltet oder den Wasserhahn aufdreht.
- Customer Experience bedeutet aber auch, dass ein Administrator sein Netz wie seine eigene Westentasche kennt, weil ihm Werkzeuge zur Verfügung stehen, die Transparenz und einfache Handhabbarkeit garantieren - egal welche Dimensionen seine Infrastruktur auch in Zukunft annimmt.
- Customer Experience bedeutet, wenn sich ein IT-Verantwortlicher bewusst für einen Partner auf Augenhöhe entscheidet, mit dem er gemeinsam erfolgreich die Herausforderungen angeht.

Das sind ambitionierte Ziele. Doch offenbar sind wir damit ganz gut unterwegs. Wie wir das technisch hinbekommen und was wir anbieten, das erfahren Sie auf den folgenden Seiten.

Wir wünschen Ihnen viel Freude mit diesem Buch

Ihr System Engineer Team von Extreme Networks



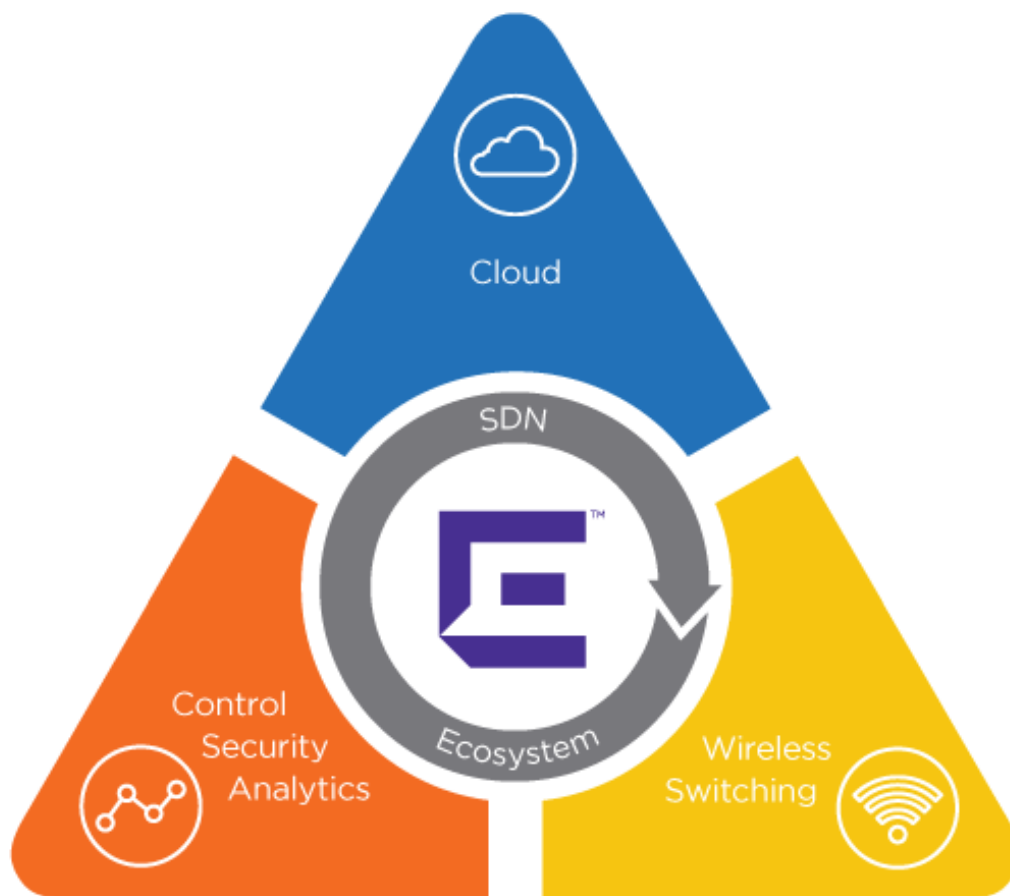
1 Extreme Networks – Wir über uns

Kurzprofil

Extreme Networks ist ein Anbieter von Netzwerklösungen, die durch fortschrittliche Software und Services den IT-Abteilungen dabei helfen, auch die schwierigsten und geschäftskritischsten Herausforderungen im Unternehmensnetzwerk zu meistern. Das Unternehmen mit Firmenzentrale in San Jose, Kalifornien, wurde 1996 gegründet und hat mehr als 20.000 Kunden in über 80 Ländern, darunter sowohl kleine als auch große Organisationen, einschließlich weltweit führender Unternehmen in Branchen wie dem Gesundheits- oder Bildungswesen, der Industrie, dem öffentlichen Bereich oder anderen Märkten.

Wer ist Extreme Networks?

Extreme Networks feiert in diesem Jahr sein 20-jähriges Bestehen. Nach vielen Innovationen im Switching-Bereich haben wir uns jedoch von einem reinen Hardware-Hersteller zu einem Anbieter von umfangreichen, durch Software optimierten, Netzwerklösungen entwickelt – das Portfolio im Kurzüberblick:










- Hochperformante Netzwerkzugangslösungen sowie die entsprechenden Switching-Plattformen, vom Edge bis hin zum Core, LAN und WLAN

- Eine Suite von umfassenden Software-Lösungen, die in einer einheitlichen Managementoberfläche dafür sorgen, dass Sie Ihr Netzwerk ohne größere Aufwände verwalten, absichern und sogar jeden einzelnen User / Applikation im Netzwerk analysieren können.
- Vervollständigung des Portfolios durch die Option der Ausweitung des Netzwerkmanagements in die Cloud.

Über allen Lösungen steht der Begriff ‘Software-Driven Networking’. Dies bedeutet bei Extreme nicht den Einsatz eines Produktes hier und eines Southbound Protokolls dort, sondern steht für eine umfassende SDN Plattform, die sowohl Software als auch Hardware beinhaltet und im Zusammenspiel mit Lösungen von Technologiepartnern für ein Umfeld sorgt, das Ihr Netzwerk in Echtzeit auf die Bedürfnisse Ihrer Nutzer und Applikationen anpassen kann.

Und diese Evolution gab es nicht zufällig. Sie wurde durch unsere Vision getrieben, das Netzwerk zu einem Treiber für bessere Verbindungen zu machen und somit für bessere Geschäftsergebnisse zu sorgen.

Auf die hier kurz beschriebenen Bereiche unseres Portfolios gehen wir in diesem Buch natürlich ausführlich ein. Und wenn Sie ein langjähriger Leser unseres Solution Guides sind, wird Ihnen relativ schnell auffallen, dass manche Produkte und Lösungen nicht mehr den Namen haben, den Sie in der Vergangenheit hatten. Und das ist gewollt, denn wir haben uns im letzten Jahr dazu entschieden, uns von den vielen verschiedenen Markennamen zu verabschieden und diese zu vereinheitlichen und unserem Branding anzupassen. In der nachfolgenden Übersicht sehen Sie die „neuen“ Namen:

Alter Name	Neue Produktfamilie		Neuer Produktname
IdentiFi	ExtremeWireless		Modellbezeichnung AP 3xxx
Summit, Black Diamond	ExtremeSwitching		Modellbezeichnung X450-G2, X8 usw.
S-Serie, K-Serie	ExtremeSwitching		Bleibt bei S-Serie, K-Serie
NetSight	ExtremeManagement		(Extreme) Management Center
NAC und Mobile IAM	ExtremeControl		(Extreme) Access Control
Data Center Manager	ExtremeControl		Data Center Connect
Purview	ExtremeAnalytics		(Extreme) Application Analytics

Unsere Standorte in Deutschland

Dies sind unsere Niederlassungen in Deutschland. Rufen Sie uns an, wenn Sie mehr über uns und unsere Lösungen erfahren möchten. Gerne laden wir Sie ein, unsere Lösungen bei uns in unseren Standorten zu besichtigen. Oder wir kommen zu Ihnen und demonstrieren sie Ihnen „live“.

- Frankfurt: Solmstrasse 83, 60486 Frankfurt am Main
Telefon: +49 (0)69 47860-0, Fax: +49 (0)69 47860-109
- München: Dornacher Strasse 3d, 85622 Feldkirchen
Telefon: +49 (0)89 37427-0, Fax: +49 (0)89 37427-499
- Berlin: Wittestrasse 30 / Haus J, 13509 Berlin
Telefon: +49 (0)30 39979-5, Fax: +49 (0)30 39979-698
- Leipzig: Torgauer Str. 231, 04347 Leipzig
Telefon: +49 (0)341 2710307

Einen vollständigen Überblick über alle Büros und Kontakte weltweit finden Sie unter:
www.extremenetworks.com/contact

2 Grundlagen Netzwerk & Security

Sicherheit – Essentielles zum Einstieg

Sicherheit gehört heute zu den wichtigsten Anforderungen an Netzwerke, die zunehmend zur universellen Plattform für Kommunikation und Geschäftsprozesse in Unternehmen, mithin zur kritischen Ressource, herangewachsen sind. Der Schaden, den Angriffe und digitale Spionage betroffenen Unternehmen zufügen, ist nachhaltig.

Seit der Einführung von Authentisierungsstandards vor 13 Jahren ist aus einem Funktionsmerkmal ein Lösungsportfolio herangewachsen, welches weitaus mehr leistet als eine reine Zugangskontrolle am Netzwerk. Und das ist gut so. Denn die Netzwerksecurity hat sich schon lange aus ihrer Perimeternische herausbewegt und beansprucht nun einen festen Platz in allen Bereichen.

Sicherheit bedeutet, dass ein Unternehmen, ungeachtet aller Einflussfaktoren, handlungsfähig bleibt. Daher umfasst dieses Kapitel nicht nur Authentisierungsmaßnahmen, sondern beschäftigt sich mit Redundanzmechanismen genauso wie Monitoring, Analyse und Rechenzentrumsdesigns.

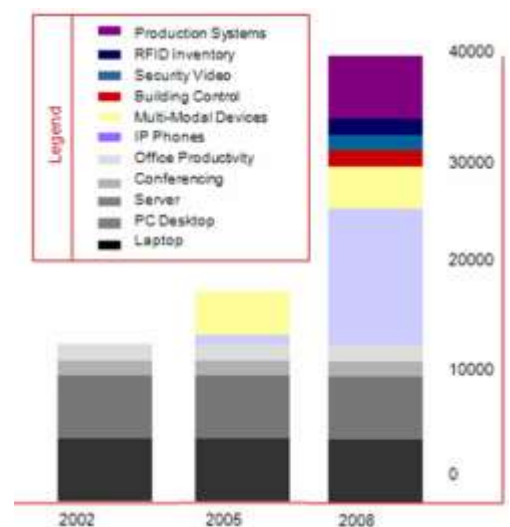
Einige Themenbereiche waren früher eindeutig abgegrenzt und ließen sich klar dem Accessbereich oder dem Rechenzentrumsbetrieb zuordnen. Mittlerweile lassen sich viele Funktionen nicht mehr isoliert betrachten. Daher ist es kein Wunder, wenn manche Technologien in den folgenden Kapiteln mehrfach Erwähnung finden – das erhält den Kontext.

Authentisierung - Der Blick über den Tellerrand

"Warum reden Sie eigentlich immer wieder über Authentisierung?" Diese durchaus berechtigte Frage stellte uns ein Kunde unlängst in einem Workshop. Natürlich, seit der Einführung von Standards wie 802.1x im Jahre 2001 wurde das Thema der Identifikation von Nutzern und Endsystemen immer wieder diskutiert. Und es ist genau die Frage nach dem Warum, welche das Thema lebendig erhält.

Der Ruf nach Sicherheit, also dem Schutz vor unbefugtem Eindringen sowie vor Mißbrauch der zur Verfügung stehenden Ressourcen - das waren die ersten Antriebsmomente. Doch auch, wenn sich alle Beteiligten über die Notwendigkeit dieses Schrittes einig waren, lag die LAN Security in vielen Fällen zugunsten anderer IT Projekte für lange Zeit auf Eis.

Doch, wie von uns bereits vor Jahren angekündigt, sorgte die Eigendynamik der IT für den nächsten Schritt. Das explosive Aufkommen unterschiedlichster, WLAN-fähiger Endgeräte, wie auch die Abbildung bisher separat geführter Dienste



wie VoIP auf die LAN Infrastruktur stellte die Betreiber von Unternehmensnetzen vor neue Herausforderungen.

Der Wandel von Arbeitsprozessen verändert die Struktur von Anlagen und Gebäuden. Die Werkhalle von heute ist - zumindest aus IT Sicht - kein reiner Maschinentaal mehr, sondern ein Konstrukt, in welchem sich Produktionssteuerungen, Telefonie, PCs und ein ganzer Zoo unterschiedlicher tragbarer Endgeräte die gleiche Infrastruktur teilen. Diese - teilweise hochsensiblen - Systeme mittels logischer Separation voreinander zu schützen, ist eine Aufgabe, deren Komplexität mehr und mehr zunimmt.

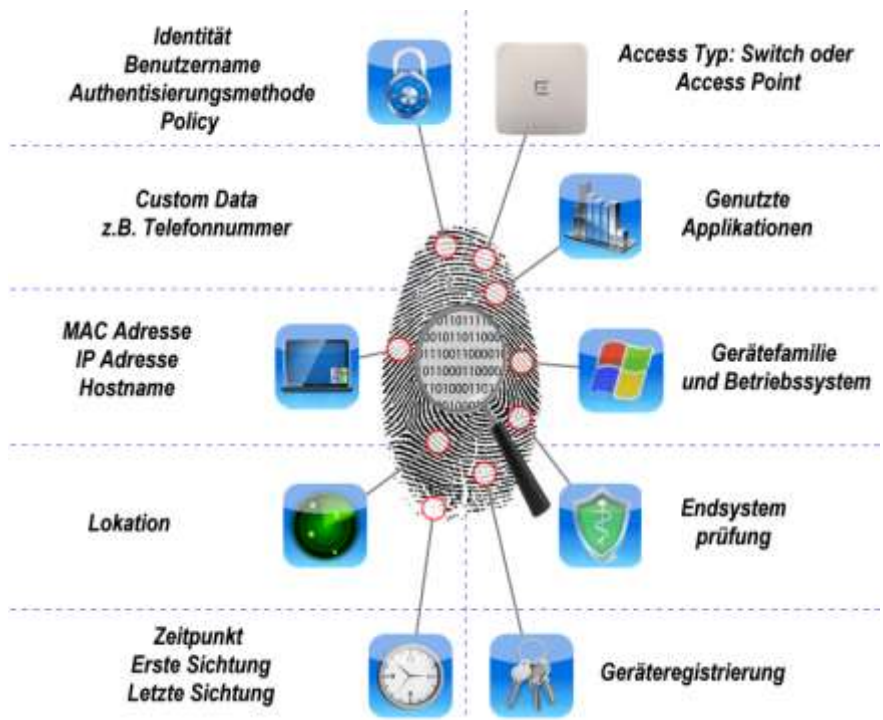


Die Praxis hat gezeigt, dass neben den klassischen PC-basierten Systemen, für die es umfangreiche Sicherheitslösungen gibt, ein breites Feld von Komponenten existiert, bei denen der Einsatz individueller Schutzmaßnahmen nicht möglich (Embedded Systems) oder nicht erlaubt (Medizinische Geräte) ist. Spätestens hier ist die Netzwerkinfrastruktur gefordert, für die nötige Sicherheit zu sorgen.

So waren es schließlich die Netzwerkadministratoren, die das Authentisierungsthema aus der Sicherheitsnische holten und zur Chefsache erklärten.

Konnten Managementsysteme bis dahin zwar Netzwerktopologien darstellen, erweiterte jedoch erst die Network Access Control (NAC) oder Identity & Access Control-Lösung das Blickfeld auf die angeschlossenen Endsysteme und deren Nutzer.

Der Authentisierungsprozess ist dabei nur der erste Schritt. Mit einem komplexen Fingerabdruck liefert NAC hilfreiche Informationen, die das Tagesgeschäft des Administrators ein bißchen leichter gestalten.



Authentifizierungsmethoden – Der technische Ansatz

Mit Access Control haben nur zugelassene Endgeräte aller Art im genehmigten Umfang Zugriff aufs Netzwerk. Anwender an Endgeräten können sich unabhängig von deren Betriebssystem interaktiv authentifizieren. Viele Switches und die meisten Betriebssysteme für PCs und Workstations unterstützen heutzutage den Authentifizierungsstandard IEEE 802.1x.

Allerdings erfordert ein ganzheitlicher Lösungsansatz, dass lückenlos alle Endgeräte im Netz erkannt werden. Dies ist nur möglich, wenn auch alternative Authentifizierungsmethoden zur Verfügung stehen. Dieser Ansatz soll hier detailliert beleuchtet werden.

IEEE 802.1x im Detail

IEEE 802.1x liefert ein komplettes Authentifizierungs-Framework für die portbasierende Zugriffskontrolle. Das Modell umfasst folgende funktionale Rollen:

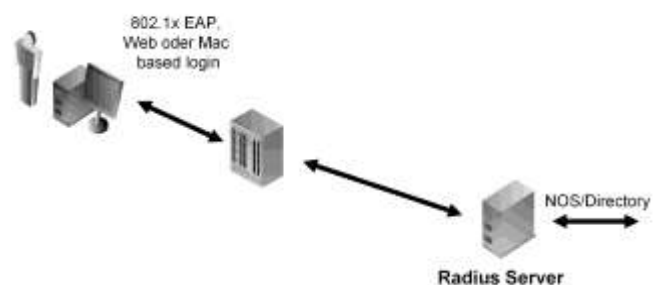
- Supplicant ist das Endgerät, das einen Netzwerkzugang anfordert.
- Authenticator ist das Gerät, das einen Supplicanten authentifiziert und den Netzwerkzugang sperrt oder freigibt.
- Authentication Server ist das Gerät, das den Authentifizierungsdienst im Hintergrund (zum Beispiel RADIUS - Remote Access Dial In User Identification System) bereitstellt

Insbesondere weil Wireless LANs einen sicheren Zugangs- und Verschlüsselungsmechanismus (802.11i und Wireless Protected Access) brauchten, hat sich IEEE 802.1x im WLAN durchgesetzt und wird nun immer öfter auch in herkömmlichen Netzwerken verwendet.

Dabei nutzt 802.1x bestehende Protokolle wie EAP (Extensible Authentication Protocol) und RADIUS, die empfohlen, aber nicht vorgeschrieben sind. 802.1x arbeitet mit Ethernet, Token Ring und IEEE 802.11 zusammen.

Im Standard sind vielfältige Authentifizierungsmechanismen wie Zertifikate, Smart Cards, One-Time-Passwörter oder biometrische Verfahren vorgesehen. EAP garantiert Flexibilität. Das Protokoll erlaubt in der von Microsoft favorisierten Variante für RAS VPN (Remote Access Virtual Private Networks) innerhalb von IPSec/L2TP (IPSecurity, Layer 2 Tunneling Protocol) die einheitliche Authentifizierung eines Nutzers über LAN-, WLAN- und WAN-Infrastrukturen.

Die eigentliche Authentifizierung erfolgt durch die Weiterleitung der EAP-Pakete mittels EAP-RADIUS (RFC 2869) an einen RADIUS-Server. Dieser kann wiederum, je nach Hersteller, Schnittstellen zu Verzeichnisdiensten wie ADS (Active Directory Service) von Microsoft oder



Novell's NDS über LDAP (Lightweight Directory Access Protocol) oder XML sowie Plug-Ins für die Integration von Secure-ID-Cards haben.

Je nach Anforderung und Applikation sind viele EAP-Protokolle geeignet (siehe Tabelle).

Methode		Beschreibung	Dynamisches Key Management
MD5	Klartextübertragung von User Daten; nur selten genutzt	Nein	Nein
PEAP	Einbindung von MS-CHAPv2	Ja	Ja
EAP-TLS	Zertifikatsbasiertes Verfahren, benötigt PKI	Ja	Ja
EAP-TTLS	Aufbau eines verschlüsselten, authentisierten Tunnels zwischen Sender und Empfänger	Ja	Ja

Access Control (NAC) lässt sich also in der Praxis mit bestehenden Authentisierungsinstanzen flächendeckend und benutzerfreundlich realisieren.

Protokolle für die Übertragung von Verschlüsselungsdaten

- **MD5** - Weil die Übertragung unverschlüsselter Authentifizierungsdaten unsicher ist, wird die ursprüngliche Methode MD5 heute nur noch in Ausnahmefällen genutzt.
- **PEAP** (Protected Extensible Authentication Protocol) - Diese gebräuchlichere Microsoft-Variante besitzt im Grunde die schon vorhandenen EAP-TTLS (Tunneled Transport Layer Security Protocol). Auch hier benötigt der Authentifizierungsserver ein Zertifikat und es wird zuerst die Verschlüsselung aufgebaut, bevor eine Identifizierung mit User Name/Passwort stattfindet
- **EAP-TLS - EAP-TLS** (RFC 2716) bietet starke kryptografische Authentifizierungsmethoden des Clients gegenüber dem Netzwerk. Client und Anmeldeserver präsentieren sich gegenseitig kryptografische Zertifikate, um ihre Identität wechselseitig zu beglaubigen. Voraussetzung dafür ist eine PKI (Public Key Infrastructure), die mit dem Directory verbunden ist. Die entsprechenden Zertifikate müssen auf dem Client verfügbar sein und werden in der Regel auf einer Smart Card gespeichert. Zusammen mit einer mehrstelligen PIN-Nummer ist das die optimale Sicherheitslösung.
- **EAP-TTLS** (Tunneled TLS) - EAP-TTLS wurde unter anderem von Funk Software und Certicom aus TLS entwickelt. Der Tunneling-Mechanismus ähnelt einem mit SSL (Secure Socket Layer) verschlüsselten Webserver. Anders als bei EAP-TLS braucht nur der Anmeldeserver ein eindeutiges, digitales Zertifikat, das der Client beim Verbindungsaufbau überprüft.
- **Web Authentifizierung** - Auf Endgeräte externer Mitarbeiter (Gäste, Service Personal, Studenten) können Administratoren nicht zugreifen und sie beispielsweise so konfigurieren, dass eine sichere Authentifizierung möglich ist.

In den Kapiteln über Access Control wird erläutert, welche variablen Möglichkeiten der Betrieb zentraler Registrierungs- und Anmeldeportale bietet.

- **MAC Authentication** - Eine Herausforderung sind Endgeräte ohne standardbasierte Authentisierungsfunktionen, zum Beispiel Drucker, IP Telefone und Industrieanlagen. Authentifizierungsmethoden, die MAC (Media Access Layer)-Adressen verwenden und die automatische Endgeräteklassifizierung durch Protokolle wie CEP (Convergent Endpoint Detection) und LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) sind grundsätzlich eine schwächere Sicherheitsbarriere, da sie sich mit verhältnismäßig einfachen Mitteln kompromittieren lassen. Deshalb reicht es nicht, nur zu entscheiden, ob ein Endgerät zugreifen darf oder nicht. Vielmehr müssen differenziertere Mechanismen her. Die Kombination von Authentisierung und Zugangsregeln (Access Policies) gewährt individuell eingeschränkte Zugangsrechte. Beispielsweise kann man so den Netzzugriff eines Druckers, der sich über eine MAC-Adresse authentifiziert, auf die Kommunikation mit dem zugewiesenen Printserver beschränken. Versucht jemand mit Hilfe dieser MAC-Adresse einen Angriff, ist dessen Erfolg deutlich eingeschränkt.
- **CEP (Convergent Endpoint Detection)** - Mit Telefonerkennung (Phone Detection) erkennt das Netzwerkmanagement automatisch ans Netz angeschlossene IP-Telefone und setzt passende Parameter für Quality of Service. Zum Beispiel kann dessen Datenverkehr via IEEE 802.1p gekennzeichnet und damit höher priorisiert werden als anderer Datenverkehr.
- **LLDP (Link Layer Discovery Protocol, IEEE 802.1ab)** - Wenn sich Netzkomponenten gegenseitig über ihre Identität und Eigenschaften austauschen, optimiert das ihr Zusammenspiel und ermöglicht die Visualisierung von Layer-2-Verbindungen in grafischen Netzwerk-Management-Tools. Die verwendeten proprietären Discovery Protokolle (CDP, EDP) waren aber nur eingeschränkt interoperabel. Deshalb ratifizierte die IEEE 2005 das herstellerunabhängige Link Layer Discovery Protokoll (IEEE 802.1ab). Unterstützen die Netzwerkkomponenten durchgängig LLDP, lässt sich die komplette Layer-2-Netzwerktopologie komplett rekonstruieren und neue Netzwerkkomponenten werden automatisch erkannt. Zudem LLDP ist einfach erweiterbar. Ein Beispiel hierfür ist LLDP-MED. Dieses Protokoll erkennt automatisch Netzwerkeinstellungen von Endgeräten wie VLAN Priorität oder DiffServ-Werte. Dies erleichtert die Integration spezieller Endgerätetypen, beispielsweise von IP Telefonen. Außerdem helfen LLDP-Informationen, Secure-Networks-Policies automatisch zuzuordnen.

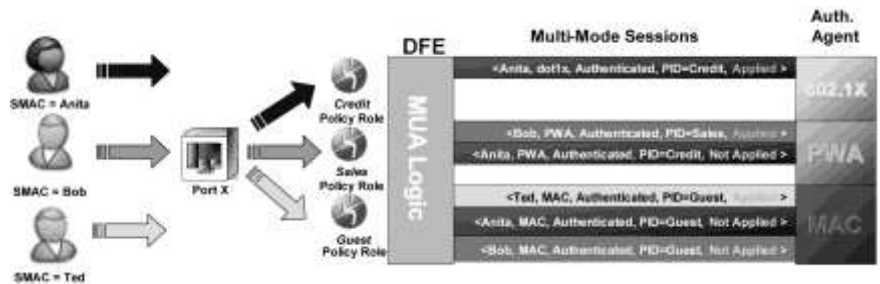
Multiuser Authentication

Als Mitautor der IEEE 802.1x-Standards und Wegbereiter sicherer LANs hat Extreme Networks sehr bald auch bereits existierende Produkte nachträglich mit den erforderlichen Funktionen ausgerüstet.

Diese Strategie reicht zurück bis zur zweiten Generation der Cabletron SmartSwitch-Komponenten aus dem Jahr 1998, welche über die notwendigen Authentifizierungsmöglichkeiten verfügen

In gewachsenen, heterogenen Netzwerken haben meist nicht alle Access-Komponenten Authentifizierungsfeatures. Extreme Switches lösen dieses Problem durch eine integrierte Multiuser-Authentifizierung. Damit können sich auf den Uplinks zahlreiche User individuell authentifizieren.

Bekannte Topologien, aber auch neuartige Fiber-to-the-Office-Konzepte mit simplen Kanal-Switches im Zugangsbereich des Netzes, sind so flächendeckend realisierbar.



Dabei ist zu berücksichtigen, dass die „simplen“ Access-Switches die bei der IEEE-802.1x Anmeldung verwendeten EAPoL (EAP on LAN)-Pakete weiterleiten müssen (EAP-Passthrough). Alle Extreme Access Switches unterstützen diese Funktion. Bei älteren Komponenten anderer Anbieter ist sicherzustellen, dass EAP-Passthrough ebenfalls möglich ist. Manchmal muss dafür das Spanning-Tree-Protokoll deaktiviert oder ähnliche Konfigurationsänderungen vorgenommen werden.

Multi-Method-Authentication

Extreme Switches können mehrere User gleichzeitig auf einem Port authentifizieren und jedem separate Regelwerke zuweisen. Außerdem ist es möglich, verschiedene Authentifizierungsmethoden gleichzeitig auf demselben Port zu betreiben. Normalerweise geht man davon aus, dass jedes Gerät/jeder Anwender sich nur einmal authentifiziert; also der stationäre Anwender an seinem PC über IEEE 802.1x, der Gast mit seinem Laptop über PWA (Port Web Authentication), der Drucker basierend auf MAC-Authentifizierung.

Aber was passiert, wenn der PC gleichzeitig über IEEE 802.1x und MAC-Authentifizierung angemeldet ist und sich die Profile der Authentifizierungsmechanismen widersprechen? Abgesehen davon, dass dann das Security Design und die Zugangsregeln überarbeitet werden sollten, hat Extreme Networks dieses Problem im Griff: Die Anmeldung läuft über sogenannte Authentication Sessions. Hat ein Anwender mehrere dieser Sessions offen, so wird nur eine wirklich genutzt. Bis zu drei Sessions gleichzeitig sind möglich, denn ein User kann über IEEE 802.1x, PWA oder MAC-Authentifizierung angemeldet sein. Die Authentifizierungsmethoden werden nach Prioritätsregeln angewandt. Die vorgegebenen Prioritäten sehen folgendermaßen aus:

- IEEE 802.1x
- Port Web Authentication
- MAC Authentication
- CEP (Convergent Endpoint Detection)

Kommen wir auf unser Beispiel zurück: Ein User hat sich über 802.1x authentifiziert, aber basierend auf seiner MAC-Adresse läuft auch MAC-Authentication im Hintergrund, da beide Methoden auf dem Port aktiviert sind. Da die 802.1x-Session höhere Priorität hat als die MAC-Session, wird diese angewandt und dem Anwender die entsprechende Rolle zugewiesen.

Autorisierung - Regelbasierte Kontrolle

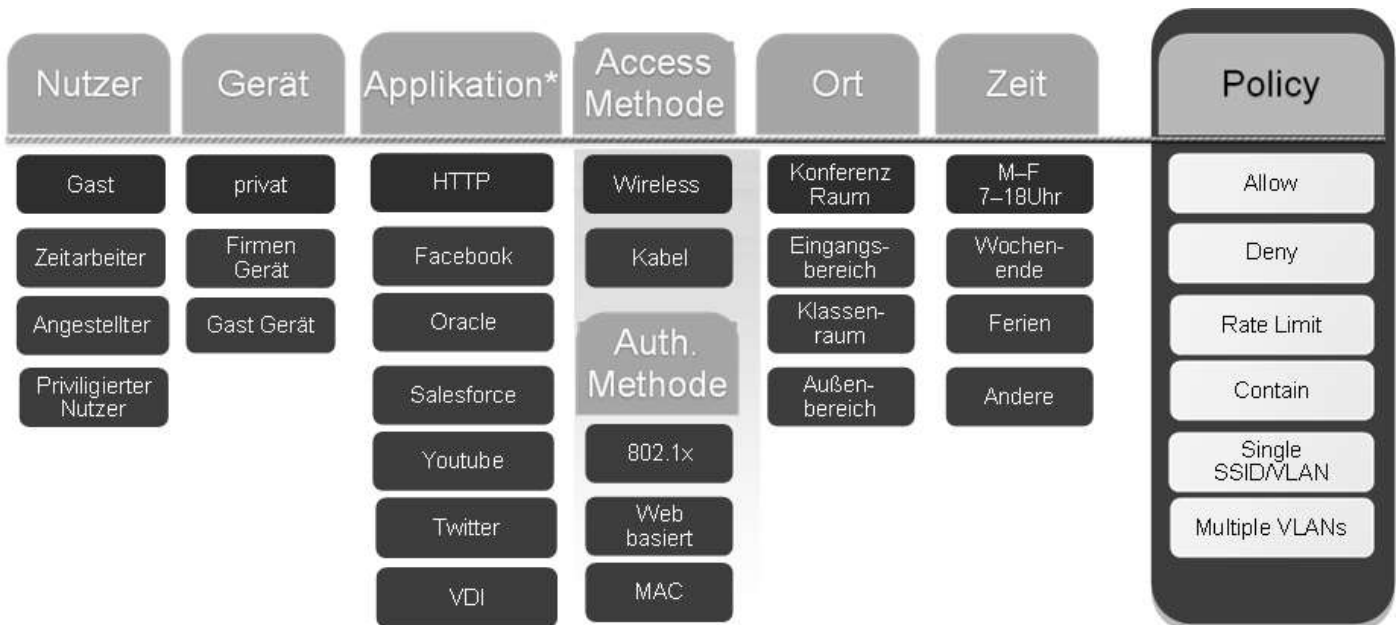
Die Eigenschaften des Fingerabdruckes sind der Schlüssel zu einer regelbasierten Zugriffskontrolle. Verknüpfungen dieser Faktoren bilden in einer klaren Sicherheitsstruktur auch komplexe Modelle ab. Ein Beispiel:

Herr Müller sitzt in seinem Büro an seinem Arbeitsplatz: Sein PC ist mit dem lokalen Netz verbunden und autorisiert, Netzwerkdienste zu nutzen, die für die Arbeit von Herrn Müller notwendig sind. Protokolle wie SNMP, Telnet oder DHCP-Serverdienste werden blockiert.

Das Smartphone von Herrn Müller gehört der Firma. Mit Anmeldedaten von Herrn Müller hat es sich automatisch ins WLAN eingeklinkt, seine Datendienste arbeiten über die Firmeninfrastruktur (WLAN Offload).

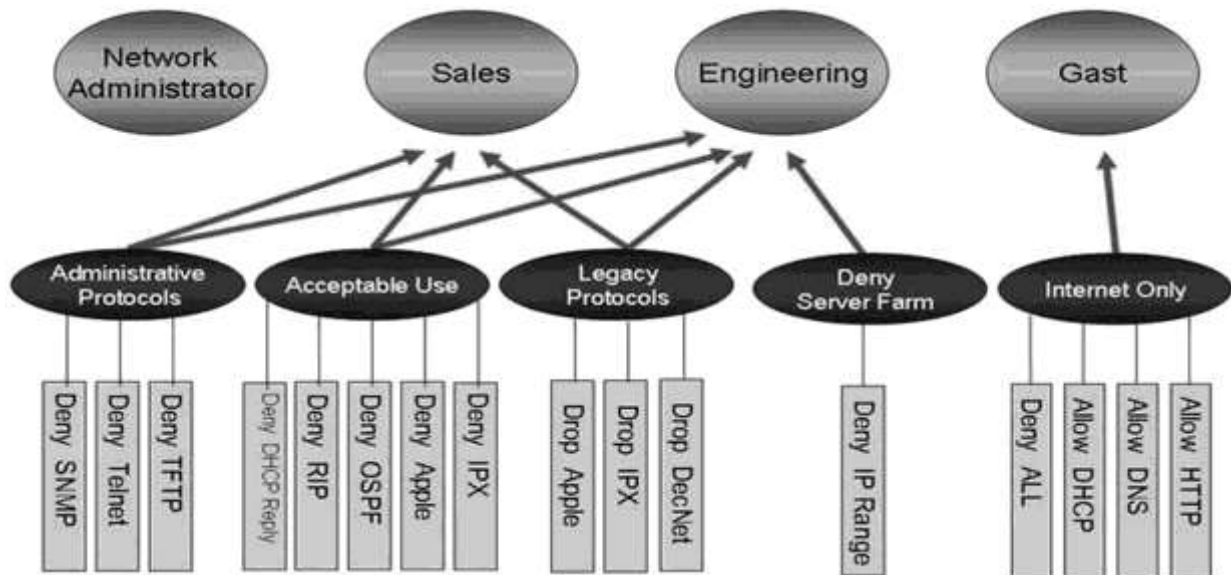
Das Tablet auf dem Schreibtisch ist Herrn Müllers Privateigentum. Er hat sich darauf mit seinen Benutzerdaten angemeldet und erhält dafür einen Zugang zum Internet. Der Zugriff auf lokale Ressourcen ist für private Geräte jedoch nicht freigegeben.

Das hierfür nötige Regelwerk definiert Entscheidungsfaktoren zur Klassifizierung von Benutzer, Endgerät und Diensten und kontrolliert den Zugriff.



Policies

Verteilte Zugriffsinformationen mit Bordmitteln zu pflegen ist für jeden Administrator eine kaum zu bewältigende Herausforderung. Extreme stellte mit dem Control Center Policy Manager schon 2001 ein Werkzeug dafür vor. Damit lassen sich komplexe Regelwerke, unterstützt von einer dreistufigen Hierarchie, baukastenförmig erstellen und verbreiten.



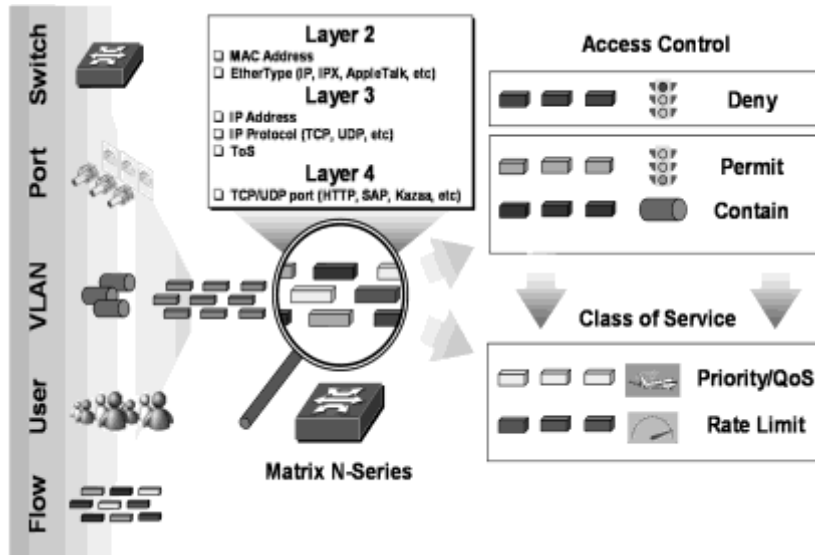
Policies - Hierarchisches Regelwerkzeug

Die oberste Ebene dieser Hierarchie ergibt sich aus der Rolle, die ein Benutzer in der Struktur des Unternehmens spielt. Da diese Rolle bereits anhand der User-Management-Regeln der zentralen Betriebssystemplattform erkennbar ist, liegt es nahe, schon bei der Authentifizierung auf diese Informationen zuzugreifen. Unterhalb dieser Ebene sind Services definiert, die grob beschreiben, was der Benutzer tun darf und was nicht. Sie setzen sich aus einzelnen Regeln zusammen, die den Datenverkehr zunächst nach Kriterien der Layer 2, 3 und 4 klassifizieren.

Passt eine Regel, wird eine zugewiesene Aktion ausgeführt:

- Access Control – Zugriffe zulassen oder verwerfen
- Kennzeichnen des Frames mit einer definierten VLAN-ID
- Veränderung von Parametern zur Servicequalität (QoS)
- Begrenzung der Bandbreite (Rate Limiting, pro Port, Applikations-Flow, Protokoll, Nutzer—IP oder MAC)

Mit dem Policy Manager kann man ein derartiges Konstrukt aus Rollen und Regeln zusammenstellen und per SNMP (Simple Network Management Protocol) an alle Netzwerkkomponenten verbreiten. Dass Zugriffsinformationen im gesamten Access- und Distributionsbereich verfügbar sind, garantiert hierbei Skalierbarkeit.



Granularität der Secure Networks™ Policies

Die Stärke des Policy Enforcement liegt in der Kombination von Authentisierung, Klassifizierung und Kontrolle (siehe Grafik oben). Damit kann man vielfältigen Bedrohungen entgegentreten.

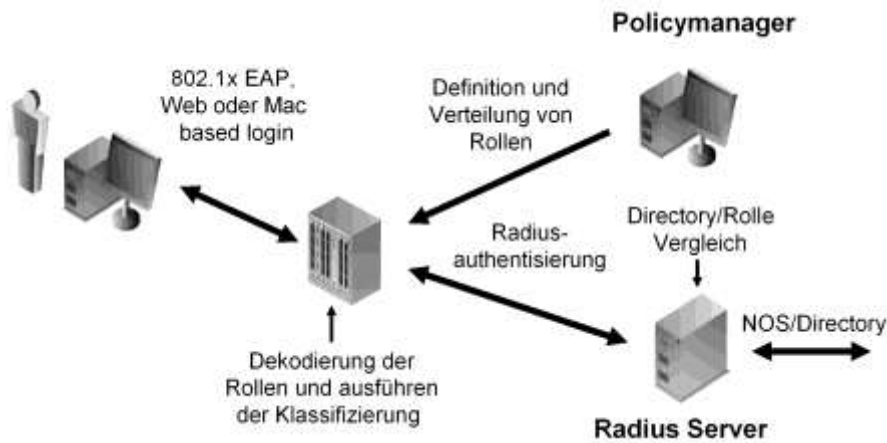
Einige Beispiele:

Risiko	Lösungen
Illegitime DHCP-Server tauchen immer wieder in LANs auf und stören den Betrieb durch Zuweisung eigener IP Adresse	Eine Deny Regel auf SourcePort TCP69 verhindert dies
Port Scanner versuchen das Netz auszuspähen	Das Blockieren des ICMP Protokolls für Standardbenutzer unterbindet Scan Versuche
Rogue Access Points schaffen offene WLAN Zugänge	Auch ein AP muss sich via 802.1x authentifizieren bevor er am Netzverkehr teilnimmt
Priorisierte Protokolle sind anfällig für Packet Flooding	Die Kombination aus Priorisierung und Rate Limiting schützt das Netz
Nicht alle IT Komponenten lassen einen Schutz der Management Ports zu	Layer 4 Regeln filtern Dienste, wie Telnet und SSH, sofern der Benutzer keine Administratorenrolle spielt
Würmer verbreiten sich exzessiv in lokalen Netzen	Für zahlreiche Attacken bietet der Policy Manager vorgefertigte Filterregeln an

MUA+P (Multi-User Authentication and Policy)

Die bisherige Authentifizierungs-Kommunikationskette wird bei MUA+P um die Managementfunktion erweitert, mit deren Hilfe der Administrator Rollen und Regeln verteilt.

Dabei meldet das zentrale Verzeichnis neben der positiven Authentisierungsbestätigung auch die Gruppenmitgliedschaften des Benutzers an den RADIUS-Server zurück. Mit einfachen Filterregeln ermittelt der RADIUS-Server die relevante Gruppe. Anhand ihres Namens weist der Switch jedem Port die richtige Policy zu.



Kombination von Access Control und Policy Enforcement

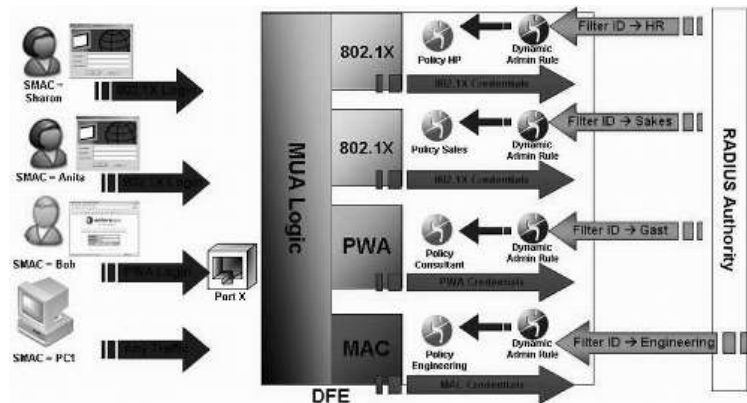
Die Authentisierungsmethode wird also lediglich um eine Filter-ID erweitert. Alle anderen Funktionen führt die verteilte Netzwerkarchitektur selbstständig aus. Das an sich sehr schlanke Standard-RADIUS-Protokoll wird damit zur Grundlage einer hochskalierbaren Gesamtlösung.

Im Kontext heterogener Netze, in denen nicht alle Access-Komponenten Policies unterstützen, müssen sich oft mehrere Benutzer, wie oben beschrieben, an dem selben Port der nachgeschalteten Verteilungsschicht des Netzwerks authentifizieren. Mit den flexiblen Extreme-Switches der S-Serie lässt sich die benutzerabhängige Policy an die jeweils involvierte MAC-Adresse koppeln.

Die folgende Grafik verdeutlicht das Konzept der beschriebenen Distribution Layer Security.

Ihre Vorteile sind:

- Integration Tausender unterschiedlicher Benutzer,
- vielfältige Authentifizierungsmethoden (802.1x, MAC, PWA, CEP...),
- mehrere unterschiedlicher Regelsets (Policies) am selben Uplink-Port.



Dignus est intrare - Complianceprüfung und ihre Folgen

Ein legitimer Nutzer, ein registriertes Endgerät - damit scheint ja alles in Ordnung zu sein. Kommt das Endsystem ohne aktuelle Updates, dafür mit selbstinstallierter Software aus zweifelhafter Quelle an, ist es jedoch durchaus als Sicherheitsrisiko einzustufen.

Die optionale Complianceprüfung des Endgerätes lässt sich mittels eines auf dem Endsystem installierbaren Agenten oder eines Scans über das Netzwerk ausüben.

Zusätzlich geben existierende Mobile Device Managementsysteme Auskunft über die Befindlichkeit eines registrierten WLAN-Gerätes.

Damit kommt ein neues Entscheidungskriterium ins Spiel, welches den Nutzer mitsamt seinem Gerät in eine Quarantänerolle platzieren kann, bevor Schaden entsteht.

Gleichzeitig informiert ihn das System über seine mißliche Lage und gibt Tipps, wie er eigenständig, z.B. durch einen Update seines Gerätes, seine Reputation wiederherstellen kann - ohne den Support kontaktieren zu müssen.

Implementierung - Step by Step

Die längste Reise beginnt mit dem ersten Schritt (Laotse)

Das Leistungsportfolio der Extreme Access Control Lösung bietet ein breites Spektrum von Funktionen und Möglichkeiten an. Entscheidend sind hierbei die verfügbaren technischen Ressourcen sowie die Sicherheitsanforderungen, welche der individuelle Betrieb eines Unternehmensnetzes mit sich bringt.

Eine einfache Inventarisierung und Visualisierung der angeschlossenen Endgeräte bringt bei minimalem Aufwand bereits einen hohen Mehrwert des administrativen Tagesgeschäfts mit sich.

In der nächsten Stufe ist zu entscheiden, wie restriktiv die Auswirkungen des Authentisierungsprozesses sein dürfen. In der Praxis hat sich dabei herausgestellt, dass die Erhaltung der Handlungsfähigkeit gegenüber einer allzu restriktiven Vorgehensweise in den meisten Fällen vorgezogen wird. Bevor ein nicht registriertes Gerät von der Teilnahme am Netzbetrieb komplett ausgeschlossen wird, ist die Bereitstellung rudimentärer Dienste in vielen Fällen sinnvoller, zumal der Administrator auf diese Weise schnell eingreifen kann.

Pauschalaussagen über die optimale Nutzung von Identity & Access Management Lösungen gibt es jedoch nicht. Der erste Schritt bei der Implementierung ist daher, die Arbeitsprozesse und Sicherheitsbedürfnisse eines Unternehmens zu verstehen und auf dieser Basis eine aufwandsgerechte Vorgehensweise festzulegen, deren Zeitplan die Integration von LAN, WLAN, Benutzerverzeichnissen bis hin zur möglichen Integration externer Applikationen definiert.

Management – Mehr als nur Monitoring

Die beste Lösung verliert an Wert, wenn sie durch steigende Komplexität ihrer Struktur nicht mehr verstanden werden kann. Daher ist Netzwerkmanagement Chefsache im Hause Extreme Networks.

Monitoringaufgaben gehen heutzutage weit über die traditionelle Portüberwachung hinaus. Die webbasierte Oberfläche OneView visualisiert, neben dem bereits beschriebenen Fingerprint, Last- und Nutzungsinformationen wie zum Beispiel auch die



momentane Qualität der WLAN-Anbindung eines betroffenen Clients. So lassen sich bereits im First Level Support Problemursachen schnell ermitteln und beheben.

Doch auch im Rechenzentrumsbetrieb gibt das OneView Interface Hilfestellung beim Aufsetzen und Umziehen virtueller und physikalischer Serverkonstrukte. Das dynamische Tracking registriert eine Servermigration, führt VLANs wie auch Regelwerke automatisch nach und leitet aktuelle Informationen auch in das Management des jeweiligen Hypervisors.

Komplexe und vor allem zeitraubende Routineaufgaben werden durch weitgehend automatisierte Prozesse erledigt. Die zeitgesteuerte Sicherung aller Netzwerkkonfigurationen vereinfacht nicht nur den Austausch von Komponenten im Fehlerfall. Die dabei erhobenen Nutzungsstatistiken liefern auch wertvolle Informationen über freie Ressourcen. Ist bekannt, wieviel Prozent der Ports eines Verteilers ungenutzt verbleiben, lassen sich Erweiterungen oder ein Redesign des Netzes präziser planen.

Die Vorhaltung der aktuellen Konfigurationsbibliothek vereinfacht den Austausch defekter Komponenten in Aussenstellen, die nicht von geschultem Administrationspersonal betreut werden. Das Austauschgerät erhält beim Start vom DHCP Server eine Temporäradresse sowie die des zentralen Managementsystemes. Nach der automatischen Kontaktaufnahme ist der Administrator in der Lage, das Gerät per Mausklick mit der passenden Konfiguration zu versorgen.

Auch ein Update aktiver Netzwerkkomponenten lässt sich in einem zeit- und gruppenorientierten Modell vorab festlegen. Selbst in weltweit verteilten Unternehmensnetzen kann eine gezielte Wartungsaktion mit minimalem Aufwand durchgeführt werden.

Extreme Access Control reduziert den Konfigurationsaufwand im Edge-Bereich erheblich, da Zugriffsrechte, VLANs und QoS Parametern einmalig Gerätegruppen zugewiesen werden. Diesen Gruppen zugeordnete Endgeräte werden beim Anschluss automatisch mit den richtigen Ressourcen versorgt. Der Aufwand für Konfigurationsänderungen bei Umzügen und Netzerweiterungen entfällt damit weitgehend.

Analyse - wenn es doch nicht am Netz liegt

"Dein Netz ist zu langsam!" Diese Aussage bringt den Administrator sofort in die Beweispflicht. Und das kann aufwändig werden. Schnell ist geprüft, ob die Topologie stabil ist und die Netzlast sich in einem akzeptablen Rahmen bewegt. Und dann helfen nur noch stichpunktartige Prüfungen, um der Ursache auf den Grund zu gehen. Denn den gesamten Datenverkehr einer Analyse zu unterziehen, ist eine echte Herausforderung.

Schon vor einiger Zeit wurde das Control Center befähigt, Flowinformationen von den Coreswitches entgegenzunehmen und aufzubereiten. Damit war es zumindest möglich,

den gesamten Datenverkehr lückenlos zu analysieren und beispielsweise ressourcenhungrige Clients oder stark ausgelastete Server zu identifizieren.

Doch auch der Netflow Standard hat seine Grenzen. Die Protokolle HTTP und SSL werden beispielsweise von zahlreichen Anwendungen genutzt, was eine differenzierte Auswertung auf Layer 4 nahezu unmöglich macht. An dieser Stelle kommt Extreme Application Analytics ins Spiel. Die selektive Spiegelung des gesamten Datenverkehrs erlaubt eine Analyse bis auf Applikationsebene. Damit sind beispielhaft Antworten auf folgende Fragen möglich:

- Wieviel Volumen beansprucht der Windows Fileservice im Netz?
- Welche cloudbasierten Speicherdienste (Google Drive, Dropbox) werden genutzt?
- Wieviele Nutzer verwenden SAP?

Darüberhinaus werden die Antwortzeiten zwischen Client und Server bzw. zwischen Client- und Serverapplikation ermittelt.

Mit Hilfe dieser Informationen kann eindeutig differenziert werden, ob die gefühlte Geschwindigkeit das Resultat einer überlasteten Netzwerkinfrastruktur oder vielleicht ungünstig verteilter Serverressourcen ist. In jedem Fall können nun klare Maßnahmen zur Behebung getroffen werden.

Hier ein Beispiel aus der Praxis:

Der Betreiber eines WLAN Netzes für 40.000 American Football Fans stellt fest, dass an bestimmten Tagen die Performance auffallend schlecht ausfällt. Ursache sind die wiederkehrenden Patchdays; die automatischen Updates für Android und iOS Endgeräte lassen die Netzlast unverhältnismässig ansteigen. Gezielt werden die Updates unterbunden, in kürzester Zeit ist das Problem behoben - die Fans sind zufrieden.

Verfügbarkeit im Netz

Business ohne IT und Netzwerkinfrastruktur ist heute nicht mehr denkbar. Dementsprechend wichtig ist es, dass das Netzwerk, die darauf laufenden Dienste und die Endgeräte permanent zur Verfügung stehen. Um das zu erreichen, sollte man vor allem auf Standards setzen.

Redundanz

Unter Redundanz in der IT versteht man das doppelte oder mehrfache Vorhandensein gleichartiger oder gleichwertiger Geräte und Funktionen. Über ein Netzwerk operierende Dienste wie VoIP, SAP, etc. sollen dabei weitgehend unbeeinflusst von Ausfällen oder Umstrukturierungen im Netzwerk bleiben. Dafür müssen die einzelnen Schichten der Netzwerkkommunikation einzeln betrachtet und gesichert werden.

Für die eigentliche Sicherung gibt es zwei grundlegende Ansätze: erstens die zu sichernde Komponente so stabil wie möglich zu machen (Verfügbarkeit) und zweitens Redundanz (zum Beispiel in Form eines zweiten Gerätes) aufzubauen. Das Zweitgerät

oder die Ersatzverbindung realisieren im Notfall alle Funktionen der ausgefallenen Komponente. Im Folgenden werden die einzelnen Netzwerkschichten zusammen mit den verfügbaren Redundanzen vorgestellt.

Layer 1 – physikalische Redundanzen

Die physikalische Schicht besteht aus der Hardware der grundlegenden Komponenten: etwa redundante Stromversorgung durch mehrere Netzteile, verbunden mit verschiedenen Versorgungspfaden. Zur Layer-1-Redundanz gehört auch, dass zwei oder mehr gleichartige Netzwerkkomponenten eine gemeinsame Aufgabe übernehmen, wobei sie räumlich oder geografisch voneinander getrennt betrieben werden.

Layer 2 - Datenübertragungsschicht

Auf der Datenübertragungsschicht oder Layer 2 gibt es in Abhängigkeit von der eingesetzten Technologie verschiedene Verfahren, Redundanzen herzustellen - In der Regel durch zusätzliche Leitungen beziehungsweise Übertragungswege in einem Layer-2-Netzwerk (Broadcast Domain). Bei Ethernet ermöglichte erstmals der Spanning-Tree-Algorithmus (STP, IEEE 802.1D) diese Redundanz. Wegen zu hoher Umschaltzeiten bis zu mehreren Sekunden kamen später Weiterentwicklungen wie Rapid Spanning Tree (RSTP) und Multiple Spanning Tree (MSTP) dazu.

Netzwerkinfrastrukturen auf STP Basis spielen heute eine immer kleinere Rolle, da neue Verfahren den Aufbau flexibler und performanter Netzwerke ermöglichen und moderne Applikationen wie IPTV und VoIP eine hohe Umschaltzeit im Fehlerfall nicht tolerieren.

Spanning Tree IEEE 802.1d

Der Spanning-Tree-Algorithmus verhindert Loops auf der Datenübertragungsschicht. Dazu tauschen die Netzwerkkomponenten (Switches) eines Layer-2-Netzwerks untereinander Nachrichten aus, die sich vom normalen Datenverkehr unterscheiden – sogenannte BPDUs (Bridge Protocol Data Unit). Anhand dieser Nachrichten wird dann eine der Komponenten zur Wurzel der Spanning-Tree-Baumstruktur. Alle anderen Komponenten gliedern sich in diese Struktur ein. Pfade, die nicht innerhalb der Baumstruktur liegen (also redundante Pfade) werden dabei ausgeschaltet.

Kommt ein neuer Switch oder Link hinzu oder fällt ein Switch aus, wird diese Baumstruktur neu berechnet. Solange sie nicht vollständig aufgebaut ist, leiten die Switches nur solche Nachrichten weiter, die für den Aufbau der Baumstruktur relevant sind und der normale Datenverkehr im Netzwerk bleibt unterbrochen. Die Neuberechnung der Baumstruktur dauert typischerweise bis zu 60 Sekunden.

Zur Konfiguration von Spanning Tree auf Extreme-Komponenten finden Sie weitere Informationen im EOS bzw. EXOS User Guide.

Rapid Spanning Tree IEEE 802.1w

Um schnellere Konvergenzzeiten als beim Spanning Tree zu ermöglichen, wurde das Rapid Spanning Tree Protocol (RSTP) entwickelt. Prinzipiell wird dabei die Baumstruktur wie bei STP berechnet. Die Nachrichten, welche die Switches austauschen,

enthalten aber mehr Informationen. Außerdem wurde die Verarbeitung der Nachrichten verbessert.

Die wichtigste Neuerung im IEEE 802.1w-Standard (RSTP) besteht darin, einen Port schneller in den Forwarding-Modus zu bringen, in dem normale Datenpakete ausgetauscht werden. Bei STP werden die Ports erst dann aktiviert, wenn der gesamte Baum konvergiert ist. Dieser Standard aktiviert Ports früher. Um das zu erreichen, können Endnutzerports als sogenannte Edge Ports konfiguriert werden. Diese Edge Ports aktivieren sich sofort, wenn der Port angesprochen wird. Außerdem können auch Ports in der Infrastruktur bei Fehlern schneller auf einen alternativen Port in Richtung des Root-Knotens umschalten, da die RSTP-Switche aktiv Rückmeldungen austauschen. In entsprechend konfigurierten Netzwerken sinkt so die Zeit, bis die Baumstruktur nach Fehlern wieder funktioniert, auf wenige hundert Millisekunden.

Multiple Spanning Trees IEEE 802.1s

MST (Multiple Spanning Tree) ist die Erweiterung des RSTP um die Fähigkeit, pro virtuellem LAN (VLAN) genutzt werden zu können.

Mit MST kann man mehrere Spanning-Tree-Instanzen über Trunks hinweg aufbauen. Dabei können in Gruppen zusammengefasste VLANs einzelnen Spanning-Tree-Instanzen zugeordnet werden. Die Topologien der Instanzen sind dabei unabhängig voneinander. Dafür werden die Spanning-Tree-Parameter wie Root-Priorität etc. für jede Instanz angepasst. So verteilt man die Verkehrslast für unterschiedliche-VLAN Gruppen über redundante Layer-2-Wege. MST benutzt dabei MSTP (Multiple Spanning Tree Protocol, IEEE 802.1s).

VLANs gemäß IEEE 802.1Q

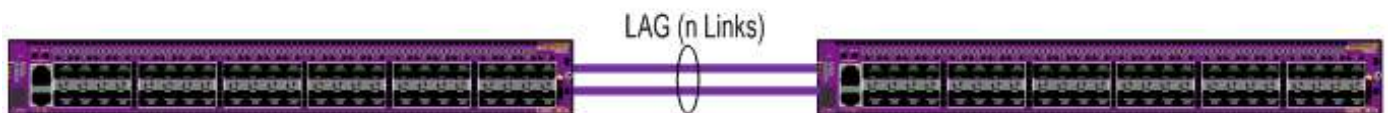
Mit virtuellen LANs (VLANs) kann man die vielen physikalischen Ports eines Switches logisch in Portgruppen unterteilen, die getrennte Broadcast Domains bilden. Der Standard IEEE 802.1Q beschreibt, wie man Daten, die zu einer bestimmten logisch separierten Portgruppe gehören, eindeutig kennzeichnet und sie so markiert an einen anderen Switch transportiert. Der Link, über den diese markierten Pakete transportiert werden, wird auch Trunk genannt. Am Ziel werden die Daten wieder den einzelnen Gruppen zugeordnet und, falls die Gruppen auf diesem Switch ebenfalls existieren, zu den entsprechenden Ports geschickt. So lässt sich eine logische Struktur von Broadcast Domains über eine physikalisch vorgegebene Struktur untereinander verkabelter Switches legen. Dadurch können die Mitarbeiter einer Abteilung mit ihren Rechnern derselben Broadcast Domain zugeordnet werden, obwohl die Abteilung auf verschiedene Gebäude verteilt ist.

Der Standard sieht einen VLAN Adressraum von maximal 4096 verschiedenen VLAN-IDs vor. Davon können die IDs 2 bis 4095 frei vergeben werden. Die ID 1 ist als sogenannte Bridge-ID dafür gedacht, mit Bridges, die keine VLANs unterstützen, kommunizieren zu können.

Eine Erweiterung des VLAN Prinzips stellt der IEEE 802.1ad Standard dar, der neben dem 802.1Q VLAN Tag ein zweites Tag im Header vorsieht. Auch dieses Tag hat einen Adressraum von 4096 möglichen IDs. Mit der Einführung des zweiten Tags ist es möglich, mehr als 4096 Broadcast Domänen zu adressieren ($4096 * 4096$). Dieses doppelte Taggen eines Ethernet Paketes wird auch QinQ, Double-Tagging oder Provider Bridging genannt. Am häufigsten genutzt wird das Double-Tagging in Umgebungen, wo unterschiedliche Dienste (VoIP, IPTV, Data...) an verschiedene, unabhängige Nutzer geliefert werden sollen, etwa im Service Provider Umfeld. Ein Dienst bekommt dann z. B. das 802.1Q Tag 200 für alle Nutzer dieses Dienstes. Die Trennung der Nutzer wird dann über unterschiedliche 802.1ad Tags realisiert.

Link Aggregation IEEE 802.3ad

Oft dienen mehrere physikalische Links zwischen zwei Netzwerkkomponenten der Redundanz. Dann kann man eine Redundant-Port-Lösung auf Layer 1 oder z. B. Spanning Tree als Layer 2 Protokoll einsetzen, um Endlosschleifen (Loops) und damit Broadcast-Stürme zu verhindern.



Eine bessere und gerne genutzte Möglichkeit besteht darin, die physikalischen Links in einem logischen Link zu bündeln und so gleichzeitig Redundanz herzustellen und die Bandbreite zu erhöhen. Alle Extreme-Switches unterstützen diese Link-Aggregation unter dem Standard IEEE 802.3ad. Diese Bündel physikalischer Links können statisch zu einem virtuellen Link (manchmal auch als Trunk bezeichnet) zusammengefasst werden. Besser ist es aber, ein Kontrollprotokoll zu nutzen. Damit lässt sich prüfen, ob die dazugehörigen Links auch korrekt funktionieren und die Switches an beiden Enden der Verbindung dieselben Ports in den virtuellen Link integrieren.

Aktuelle Switches, die nach dem Standard IEEE 802.3ad arbeiten, kommunizieren über ein solches dynamisches Protokoll, dem LACP (Link Aggregation Control Protocol). Dabei entstehen virtuelle Links, die ebenfalls als LAG (Link Aggregation Group), bezeichnet werden. Alle Links einer LAG müssen gleich konfiguriert sein und Full Duplex (also in Hin- und Rückrichtung die gleiche Geschwindigkeit) unterstützen. Der Switch behandelt dann den virtuellen LAG-Port bei der Konfiguration wie einen ganz normalen physikalischen Port. Der LAG-Port kann also zum Beispiel einem VLAN angehören oder als IEEE 802.1q-Trunk definiert werden.

In einem Chassis-basierten System und einem Stack aus mehreren Switches lässt sich ein LAG-Port aus Ports verschiedener Module bilden. Das erhöht die Ausfallsicherheit, denn selbst falls ein ganzes Board ausfällt, bleiben die beiden Chassis-basierten Switches oder Stacks verbunden.

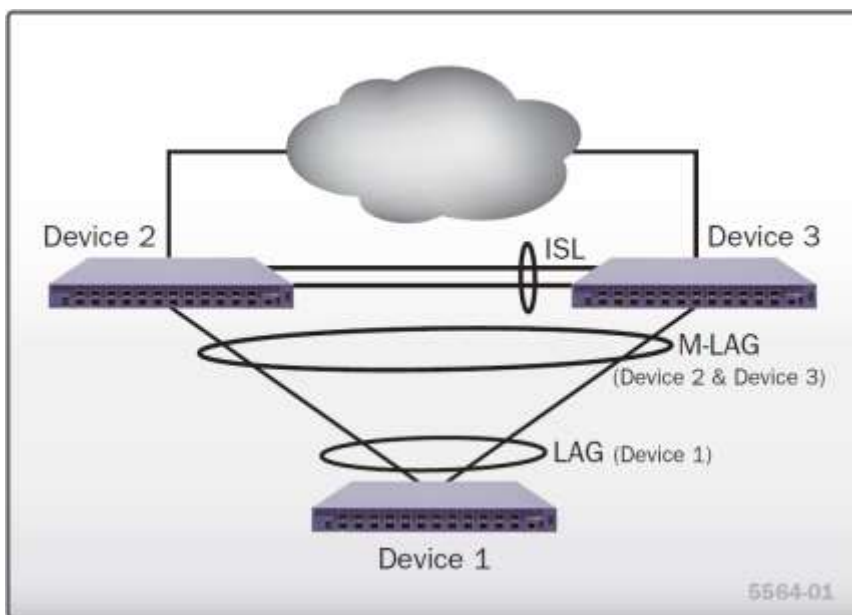
Der Standard IEEE 802.3ad sorgt für Interoperabilität zwischen verschiedenen Herstellern. Sollte es nötig sein, einen Extreme-Switch mit einer Gegenstelle zu

verbinden, die kein LACP unterstützt, kann man den LAG-Port auch statisch konfigurieren. Man verzichtet dann zwar auf das Kontrollprotokoll, das vor Fehlern und Netzproblemen durch Fehlkonfiguration schützt, kann aber trotzdem die Vorteile eines virtuellen, gebündelten Links nutzen.

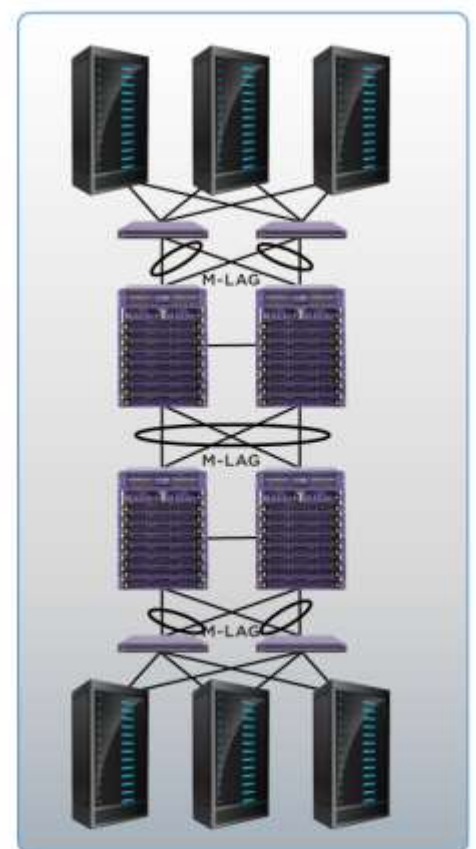
Der Datenverkehr lässt sich mit verschiedenen Methoden bzw. Algorithmen auf die physikalischen Links verteilen, etwa durch ein einfaches auf MAC- oder IP-Adressen basierendes Hashing. Meist sorgt die Analyse von Absender- und Ziel-Adressen für eine ausgewogene Verteilung auf die physikalischen Links. Häufig werden Server mit mehrportigen NIC-Karten über LAG an das Netzwerk gebunden. Kommuniziert der Server nur mit wenigen anderen Komponenten, kann es dazu kommen, dass eine LAG nur teilweise genutzt wird, auch wenn der Server mehr Bandbreite liefern könnte. Das liegt dann daran, dass der verwendete Algorithmus auf Grund der zur Hash-Kalkulation herangezogenen Daten (MAC-, IP-Adressen) immer den gleichen Hashwert errechnet. Abhängig vom Kommunikationsverhalten auf einem Link sollte zur gleichmäßigen Lastverteilung auf alle Ports einer LAG also der passende Algorithmus gewählt werden.

M-LAG - Multiswitch Link Aggregation

Die über LAG/LACP mögliche Link-Redundanz bietet zwar schon eine hohe Verfügbarkeit einer Verbindung, greift aber nicht, wenn einer der LAG Endpunkte ausfällt. Mit Hilfe des M-LAG Protokolls ist es möglich, einen der LAG Endpunkte auf zwei Switche zu verteilen.



Mit der daraus resultierenden Dreiecksbeziehung kann z.B. ein Server, der vier Uplinks zu einer LAG geschaltet hat, redundant an zwei Switche angeschlossen werden. Aus Sicht des Servers ist der Uplink eine normale LAG. Der Datenstrom des Servers wird gemäß seines Verteilungsalgorithmus auf die Links verteilt und vom jeweils angeschlossenen Switch verarbeitet. Bei Ausfall



M-LAG basiertes Netz

eines Switches oder eines Teils der LAG geht lediglich Bandbreite verloren. Ein Verlust der Konnektivität findet nicht statt.

Jedes Gerät, das statische oder dynamische LAGs unterstützt, kann per M-LAG redundant an ein Netz angeschlossen werden – herstellerunabhängig.

Jeder Switch einer M-LAG Beziehung kann seinerseits wieder über zwei nachgeschaltete Switches per M-LAG abgesichert werden (M-LAG Kaskade). Somit kann ein komplettes Netzwerk rein über M-LAG aufgebaut werden.

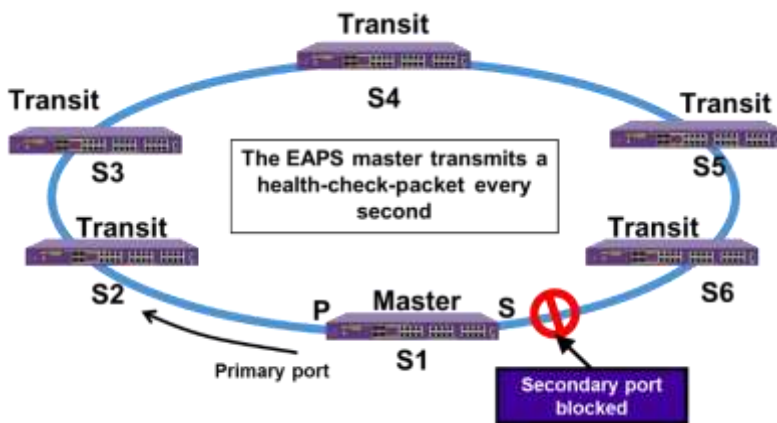
Ringprotokolle EAPS und ERPS

Ein großer Kritikpunkt an STP und RSTP/MSTP ist die sehr hohe Konvergenzzeit im Fehlerfall. Moderne Applikationen wie Video-On-Demand, VoIP, AVB oder iSCSI verlangen Umschaltzeiten von 100ms und weniger.

Extreme Networks hat sich dieser Problematik bereits im Jahr 2000 angenommen und das Protokoll EAPS (Ethernet Automatic Protection Switching) entwickelt (RFC 3619). Entgegen der Forderung des Ethernet Standards, Ringstrukturen zu vermeiden, um Loops zu verhindern, werden bei EAPS bewusst Ethernet Switches zu einem Ring verschaltet. Auf allen Switches des Ringes wird ein sogenanntes Control-VLAN eingerichtet, das dazu dient, „hello“-Pakete zu übertragen. Ein Switch in dem Ring wird zum Master ernannt. Der Master sendet über einen der beiden am Ring beteiligten Ports diese „hello“-Pakete. Kommt das Paket an dem zweiten Ringport an, weiß der Master, dass der Ring physikalisch geschlossen ist. Alle VLANs, die für den Datenverkehr genutzt und von der sogenannten EAPS Domäne geschützt werden,

werden an dem zweiten Ringport des Masters geblockt. Damit ist für diese VLANs der Ring administrativ unterbrochen und die Loop beseitigt.

Besteht ein EAPS Ring ausschließlich aus Extreme Switches, die auf EXOS basieren, können Umschaltzeiten im Fehlerfall von unter 50ms



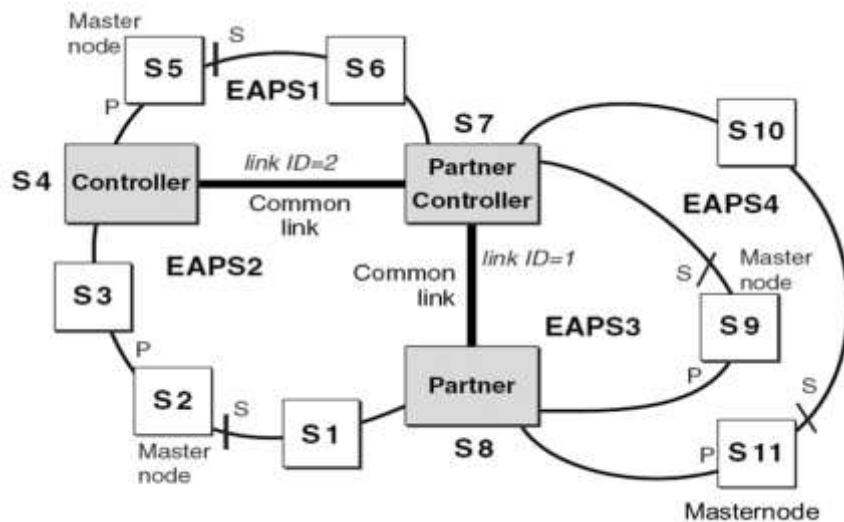
erreicht werden, da die anderen EXOS Switches (Transit Nodes) aktiv an der Fehlererkennung beteiligt sind und den Master informieren, sobald ein Ringport oder Ring-Member ausfällt. Ein EAPS Ring kann aber auch als heterogene Struktur betrieben werden. Solange nicht mehr als ein „Nicht-EAPS“ fähiges Gerät zwischen zwei EXOS Switches platziert ist, steigt im Worst Case lediglich die Umschaltzeit.

EAPS ist unabhängig von der Linkgeschwindigkeit zwischen den Ring-Members, d. h. ein Ring kann aus Teilstrecken unterschiedlichster Geschwindigkeiten aufgebaut werden (100Mbps, 1Gbps, 10Gbps, 40Gbps und 100Gbps).

Sowohl STP als auch EAPS unterbrechen eine erkannte Ringtopologie. Damit ist der Link, an dem die Unterbrechung geschaltet wird, ungenutzt. EAPS ist in der Lage, auf der selben physikalischen Ringstruktur mehrere logische EAPS Ringe zu verarbeiten. Es können für unterschiedliche VLANs verschiedene EAPS Domänen mit eigenen Control-VLANs konfiguriert werden, die auch gegenläufige Verkehrsströme erlauben. Damit kann ein Link, der für einen Teil der VLANs geblockt ist, für andere VLANs geöffnet sein, da diese an einer anderen Stelle im Ring geblockt werden.

EAPS in der Version 2 (EAPsv2) erlaubt sogar eine Kopplung und Verschachtelung von physikalischen Ringen.

Da der RFC 3619 nur von wenigen anderen Herstellern übernommen wurde, gilt EAPS als quasi proprietär. 2009 hat die ITU-T mit dem G.8032 Standard auf Basis von EAPS ein Ringprotokoll verabschiedet, dass von fast allen Herstellern übernommen wurde. 2012 kam G.8032 in der Version 2 auf den Markt und ermöglicht damit die gleichen Ringstrukturen wie EAPS. Im Extreme EXOS wird G.8032 auch ERPS genannt. EAPS und ERPS sind nicht Bit-kompatibel, können aber zusammen arbeiten.



Der Hauptunterschied zwischen EAPS und ERPS ist, dass die Erkennung einer Ringunterbrechung nicht nur über das „hello“-Paket und Meldungen anderer Ring-Teilnehmer erkannt wird, sondern auch über Informationen der Protokolle CFM (Connectivity Fault Management, IEEE 802.1ag) und ITU-T Y.1731 (Ethernet OAM).

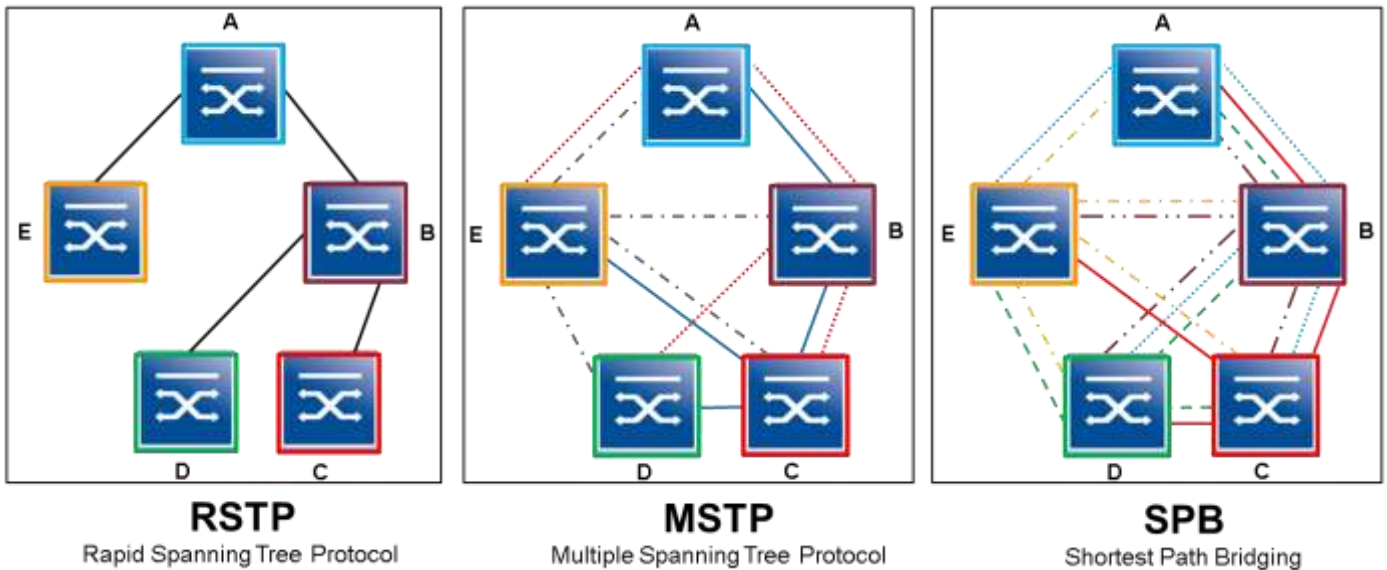
Mit EAPS/ERPS lassen sich STP freie und ausfallsichere Layer2 Netze mit bis zu mehreren tausend Usern aufbauen. Ein EAPS/ERPS Ring kann quasi beliebig viele Switches beinhalten. Die Begrenzung liegt in der steigenden Latenz und damit höheren Umschaltzeit.

Shortest Path Bridging

Shortest Path Bridging (SPB) ist eine Technologie, welche die Konfiguration und den Betrieb von Netzwerken stark vereinfacht. SPB reduziert Bedienungsfehler durch seinen „Zero-touch-Core“ Ansatz und ermöglicht optimale Bandbreitenausnutzung und Lastverteilung via „Shortest-path“ und „Multi-path“-Routing.

Shortest Path Bridging (IEEE 802.1aq) wurde als Ersatz für die älteren Spanning Tree Protokolle (IEEE 802.1D STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP) entwickelt, welche den Verkehr auf allen bis auf einen Netzwerkpfad blockieren. Im Gegensatz dazu ermöglicht IEEE 802.1aq (Shortest Path Bridging SPB), alle Pfade aktiv zu nutzen und

unterstützt viel größere und flexiblere Layer-2 Topologien. Es hat eine kürzere Konvergenzzeit und verfügt über volle Unterstützung der Netzwerkvirtualisierung durch den Einsatz einer Service ID im SPB Netz anstelle von VLAN IDs.



Stark vereinfacht lässt sich Shortest Path Bridging dadurch darstellen, dass jeder Switch in der SPB Domäne den Spanning Tree zu allen anderen Knoten berechnet. Da alle Knoten via IS-IS permanent Daten zur Topologie austauschen, können auch während des Betriebs neue Knoten der Domäne hinzugefügt werden. Von den speziellen Topologiebäumen eines jeden Switches abgesehen, wird ebenfalls noch der sogenannte Common Internal Spanning Tree (CIST) berechnet. Der CIST ist im Grunde nichts anderes als der „normale“ Spanning Tree, der die Abwärtskompatibilität zu älteren Switchen ohne SPB Unterstützung gewährleistet und darüber hinaus auch im Notbetrieb zur Verfügung steht, falls es Probleme mit der SPB Konfiguration geben sollte.

Jeder Switch verfügt so über eine Liste aller potentiellen Ziele im Netz und über welche Pfade die Daten zu versenden sind. Mit diesen Informationen kann jeder Switch dann einen Reverse-Path Forwarding Check durchführen und somit verhindern, dass ein Loop entsteht. Das Wissen, über welchen Weg die Daten gesendet werden, erlaubt auch die vollständige Kompatibilität zu den etablierten IEEE Standards – insbesondere der OAM Suite.

Wie auch bei STP bietet SPB die Möglichkeit zur Gewichtung der einzelnen Verbindungen. Als Besonderheit gilt hier jedoch, dass Verbindungen mit gleichen Kosten nicht einfach abgeschaltet werden, sondern via Equal-Cost Multi-Path eine Möglichkeit zur Lastverteilung über symmetrische Hin- und Rückrouten besteht.

Obwohl SPBM ganze 16 Standard Algorithmen zur Lastverteilung spezifiziert, bietet SPBV leider nur einen an. Extreme bietet hier jedoch auch die Möglichkeit eines weiteren proprietären Algorithmus, um die Lastverteilung über zusätzliche Verbindungen realisieren zu können.

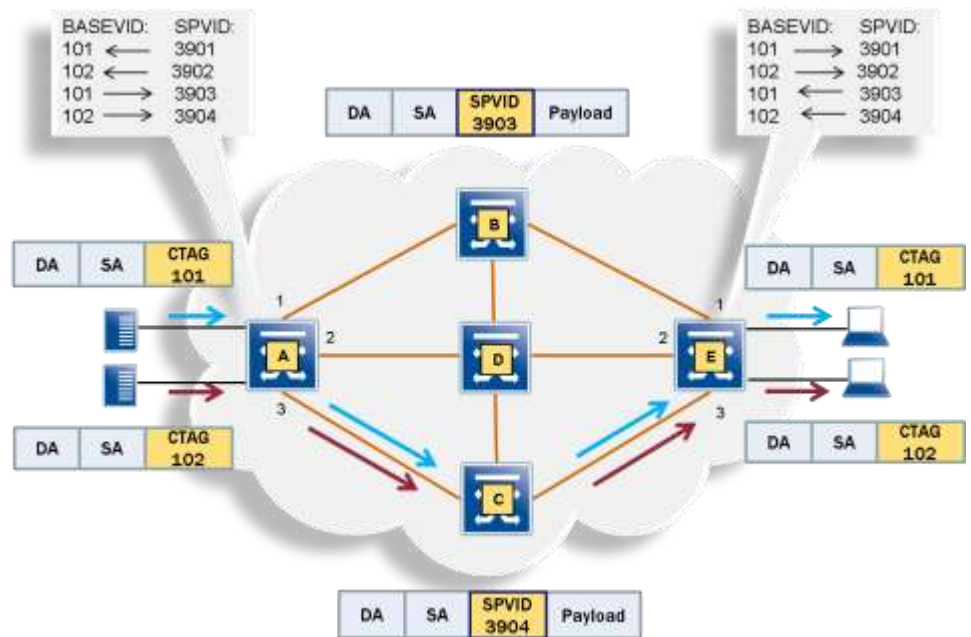
Um all dies nutzen zu können, muss also SPB ankommende Daten markieren können und mit einer Service ID versehen. Im Grunde genommen nicht unähnlich zum Label Switching in MPLS. SPBV benutzt hierfür das VLAN Tag und SPBM eine MAC-in-MAC Einkapsulierung.

Dabei ist zu beachten, dass SPBV kein Q-in-Q verwendet, sondern VLAN Translation. Damit werden ankommende Frames am Rand der SPB Domäne entsprechend dem Ziel und des VLANs mit einer Service-ID versehen, die das bestehende VLAN überschreibt. Wenn die Daten dann die Domäne verlassen, so wird das VLAN Tag wieder „zurück“ getauscht und kann zugestellt werden.

Da SPBV das VLAN Tag zur Identifikation der Service ID benutzt, die wiederum für jeden Switch eindeutig einen Verbindungsbaum zu allen anderen Switchen darstellt, lässt sich somit als Faustregel die Anzahl benötigter VLAN Ids ermitteln: (Anzahl Switche x Anzahl Basis VLANs) + Anzahl Basis VLANs.

Die Basis VLANs müssen zum Schluss noch einmal addiert werden, da der STP-kompatible CIST zwischen den Switchen über das jeweilige Basis VLAN abgebildet ist. Damit ist auch schnell klar, dass SPBV Domänen eher für Bereiche mit einer überschaubaren Anzahl

Switche und VLANs gedacht ist. Letztendlich ist es auch ein Protokoll zur Vermaschung einer grossen Layer2 Domäne. Wem dies nicht reichen sollte, der wird mit SPBM feststellen, dass das Limit von 4096 möglichen Service IDs deutlich auf 16 Millionen angehoben wurde und damit durchaus auch für den Access-Bereich interessant werden wird.



Layer 3 - Netzwerkschicht

Auf der Netzwerkschicht entsteht Redundanz hauptsächlich durch intelligente Routingprotokolle wie OSPF (Open Shortest Path First, RFC 2328), BGP (Border Gateway Protocol) oder MPLS (Multipath Label Switching) und die bessere Erreichbarkeit des Default-Gateways mit VRRP (Virtual Router Redundancy Protocol). Dafür müssen schon auf der Netzwerkebene verschiedene Wege zum selben Ziel vorhanden sein.

Open Shortest Path First

OSPF (RFC 2328) ist ein hierarchisch aufgebautes Link-State-Routingprotokoll und derzeit der de-facto-Standard bei Interior-Gateway-Protokollen, also Protokollen, mit denen Informationen innerhalb einer Organisation ausgetauscht werden. BGP dagegen routet als Exterior-Gateway-Protokoll Daten zwischen autonomen Systemen, also über die Organisationsgrenzen hinaus. BGP kann zwar auch als IGP genutzt werden, findet in der Form aber in der Praxis kaum Verwendung.

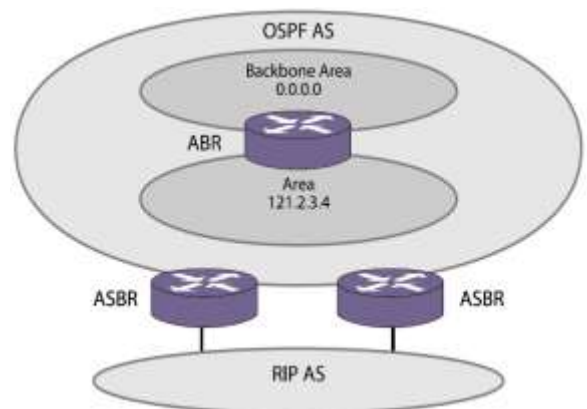
Distance-Vector-Protokolle wie RIP (Routing Information Protocol, inzwischen in Version 2 verfügbar, RFC 2453), sind dafür wegen ihrer schlechten Konvergenzzeiten mittlerweile nur noch selten anzutreffen. Denn Ausfallzeiten bis zu mehreren Minuten sind in heutigen Netzwerken nicht mehr tolerierbar.

Link-State-Protokolle arbeiten eventgesteuert. Informationen über Topologieänderungen werden sofort im gesamten Netz verteilt. Die gesamte Netztopologie ist hier in einer Datenbank gespeichert und alle Router kennen sie. Deswegen können die Router sofort auf Events reagieren und berechnen dann mögliche Ersatzwege. Das führt bei Link-State-Protokollen zu Konvergenzzeiten im Sekundenbereich. Außerdem schonen Link-State-Protokolle, verglichen mit Distance-Vector-Protokollen die Netzwerkressourcen, weil die periodische Verbreitung der gesamten Routinginformationen im gesamten Netz entfällt.

Der hierarchische Ansatz von OSPF macht dieses Routingprotokoll skalierbar. Es eignet sich daher auch für sehr große Netze. Die Hierarchie ist zweistufig: An ein zentrales Backbone-Area (Area ID: 0.0.0.0) sind alle anderen Areas direkt angebunden. Verfahren wie Route Summarization (die Zusammenfassung der zwischen zwei Routern übertragenen Informationen, um die Verarbeitungslast der Router zu verringern) und das Definieren von Areas als Stub Area oder NSSA (Not-So-Stubby Area, RFC 3101) minimieren die Auswirkungen von Topologieänderungen auf das gesamte Netz.

OSPF ist ein offenes Protokoll, das von allen Herstellern unterstützt wird. OSPF schafft Kompatibilität zwischen allen Komponenten. Die schnellen Konvergenzzeiten von wenigen hundert ms (über Fast-Hellos und BFD), die OSPF als Link-State-Protokoll besitzt, sind für heutige Netze unverzichtbar.

Der hierarchische Ansatz unterstützt die OSPF-Implementierung in Netzwerken jeder Größe. Netze mit OSPF-Routing sind mit dem entsprechenden Netzwerk- und Adressdesign einfach zu erweitern. Als modernes Routingprotokoll unterstützt OSPF natürlich VLSM (Variable Length Subnet Mask) und ermöglicht so Optimierungsverfahren wie Route Summarization.



Wegen seiner Allgegenwart wurde OSPF als Routingprotokoll für den IPv4-Nachfolger IPv6 spezifiziert (RFC 2740) und wird deshalb auch in Zukunft nicht aus den Netzwerken wegzudenken sein.

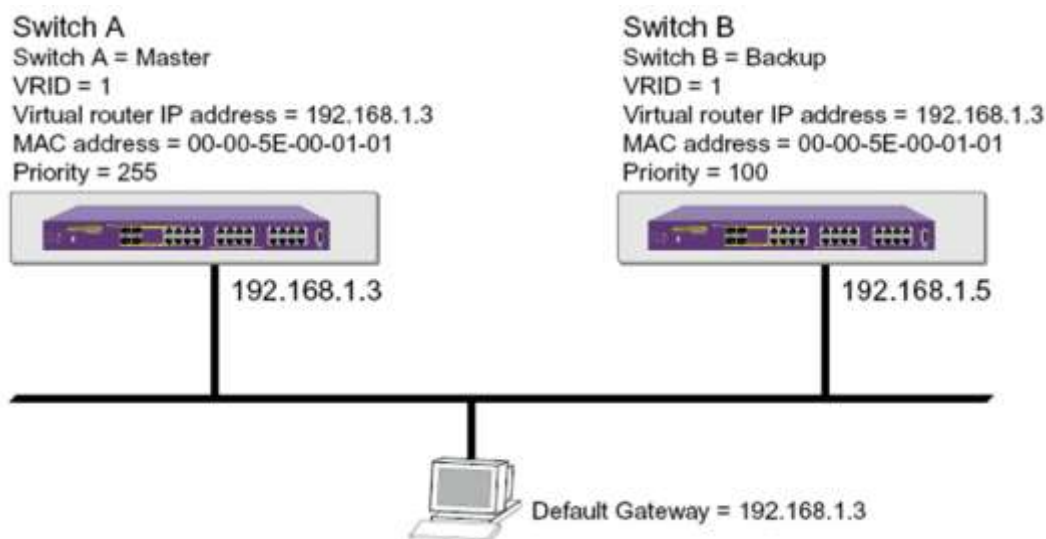
Equal Cost Multi Path (ECMP)

Ein Paket kann in einem gerouteten Netzwerk über unterschiedliche, gleichwertige Pfade ans Ziel gelangen. Bei “Equal Cost Multi Path” werden diese Pfade gleichzeitig zur Lastverteilung genutzt. Redundanz gewährleistet das jedoch nicht. Dafür muss das darunterliegende Routingprotokoll sorgen. Bei Verwendung von ECMP wählt der Router, an dem sich der Pfad gabelt, unterschiedliche Folgestationen (next-hops) für die Pakete. Idealerweise sollten sich die Pakete gleichmäßig auf die beiden gewählten Pfade verteilen. Das wäre mit paketweisem Aufteilen am einfachsten zu realisieren. Dies ist aber in der Regel nicht sinnvoll, da dieses Verfahren unterschiedliche Laufzeiten und Paketreihenfolgen verursachen kann. Meist wird daher versucht, die Pakete flowbasiert aufzuteilen: Pakete, die die selbe Absender-IP und Ziel-IP oder zusätzlich noch die selbe Portadresse haben (Absender-IP+Port/Ziel-IP+Port) gehören zum selben Flow und nehmen den gleichen Weg.

Prinzipiell läuft ECMP in jedem gerouteten Netzwerk. In der Regel beschränken die Routingprotokolle jeweils in ihrer individuellen Metrik, wie viele Pfade gleicher Qualität möglich sind. Allerdings wirkt sich ECMP im Zusammenhang mit L2 Techniken wie VLANs und Virtual Circuits (MPLS) eher negativ aus.

VRRP (Virtual Router Redundancy Protocol)

VRRP (RFC 3768) sorgt für redundante Auslegung des Default-Gateways. Router nutzen untereinander Routing-Protokolle, um die aktuellsten Routing-Informationen auszutauschen. So erfahren sie bei einem Ausfall von Ersatzwegen und nutzen sie dann. Bei sehr vielen Endclients wird dagegen eine statische Router-Adresse als Default-Gateway eingetragen. Doch was geschieht mit ihren Datenpaketen, wenn der Router ausfällt? Selbst wenn es einen Ersatzweg gibt, können die Clients diesen wegen des statischen Eintrags nicht nutzen.



VRRP-Konzept

VRRP behebt dieses Problem durch einen virtuellen Router, dessen IP-Adresse als Default-Gateway auf den Hosts konfiguriert wird.

Die physikalischen, redundanten Router kommunizieren dann über VRRP und handeln aus, wer die Routing-Aufgabe des Default-Gateways übernimmt. Der gewählte Router wird als Master bezeichnet, weitere redundante Router sind Backup-Router. VRRP erkennt jeden Ausfall des Masters und der Backup-Router übernimmt dessen Aufgabe, ohne dass die Clients das merken. Um Probleme bezüglich der ARP (Address Resolution Protocol)-Einträge zu vermeiden, nutzt der virtuelle Router eine für VRRP reservierte MAC Adresse (00-00-5E-00-01-01).

Durch VRRP ist die statische Konfiguration des Default-Gateways auf den Clients kein Single Point of Failure mehr.

Die Konfiguration zweier virtueller Router ermöglicht Lastverteilung zwischen den redundanten Geräten. Man nutzt dazu zwei virtuelle IP-Adressen, für die jeweils einer der Router die Master-Funktion übernimmt. Für die jeweils andere IP-Adresse ist dieser virtuelle Router der Backup-Router. Zusätzlich wird an den Clients eine der beiden IP-Adressen der virtuellen Router als Default-Gateway konfiguriert. Eine gleichmäßige Verteilung lässt sich zum Beispiel mit dem DHCP (Dynamic Host Configuration Protocol) erreichen. Damit sind beide virtuellen Router Default-Gateway. Dieser Ansatz kombiniert Lastverteilung mit Redundanz. Weitere Informationen finden Sie in RFC 2338.

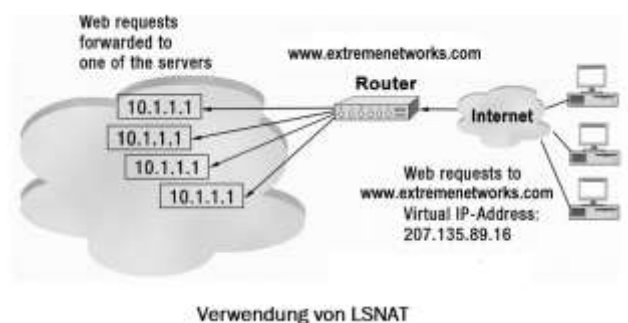
Server Load Balancing

In aktuellen Netzwerkdesigns sorgen meist Protokolle wie VRRP und OSPF bereits für Redundanz. Das gilt allerdings oft nicht für den Anschluss der Server. Um hier Redundanz zu schaffen, braucht man eine zusätzliche Lösung, die eine Netzwerkkomponente bereitstellen muss.

Das Konzept, Server redundant auszulegen, bezeichnet man als SLB (Server Load Balancing) oder LSNAT (Load Sharing Network Address Translation, RFC 2391). Das sorgt für Ausfallsicherheit und mehr Leistung.

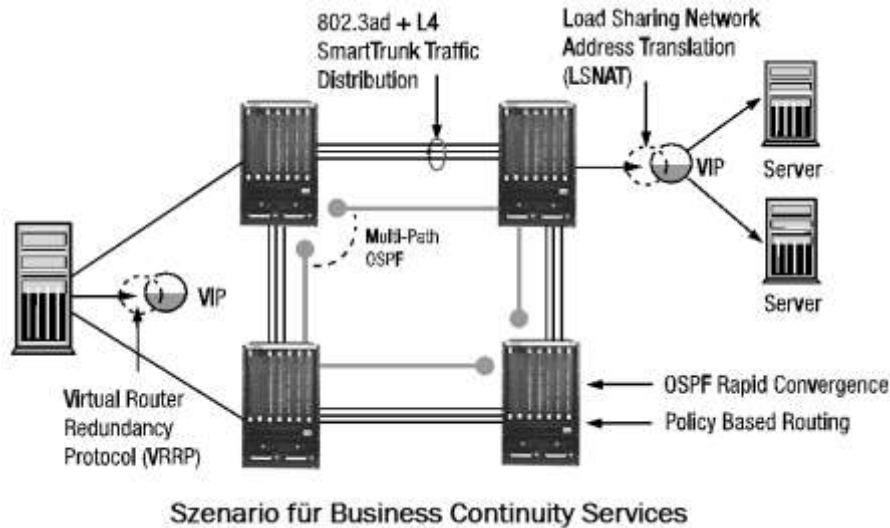
Extreme EOS Produkte verwenden LSNAT. Die Geräte reagieren hierbei auf Anfragen an einen virtuellen Server und setzen diese Anfragen

entsprechend in Abhängigkeit vom angesprochenen Layer-4-Port auf reelle Serveradressen um. Zwischen den physikalischen Servern werden dann die Anfragen mit einem vom Administrator ausgewählten Algorithmus, etwa Round-Robin, Weighted Round-Robin oder Least Weighted Load First, verteilt. Parallel dazu überprüft das System die Verfügbarkeit der Server und verteilt Anfragen beim Ausfall eines Servers auf die verbleibenden Serversysteme.



Das sorgt für hohe Ausfallsicherheit. Das virtuelle Serversystem skaliert sehr gut, da man beliebig viele Server hinzufügen kann. Die Server müssen allerdings auf eine einheitliche Datenstruktur zugreifen, die das Betriebssystem der Server unterstützen muss.

Kombiniert mit den weiter oben beschriebenen Redundanzverfahren, lässt sich so folgendes Szenario realisieren:



In dieser Grafik ist der Zugang des Hosts zum Netz via VRRP redundant ausgelegt; außerdem werden die Anfragen am Ziel, das heißt am Server, per LSNAT verteilt. Wegen des Multi Path Support von OSPF können alle redundanten Wege genutzt werden. Bei einem Defekt sorgt OSPF für sehr kurze Ausfallzeiten. Zwischen den Switchen werden 802.3ad-Trunks gebildet, die mehr Bandbreite liefern und die Redundanz erhöhen.

Die Infrastruktur für das Rechenzentrum der Zukunft

Applikationsverfügbarkeit als Technologietreiber

Mit der Rezentralisierung der Anwendungen im Rechenzentrum und der gleichzeitigen Mobilisierung der Mitarbeiter haben sich die Anforderungen an Rechenzentren geändert. Unternehmen konzentrieren sich heute auf die Erhöhung der Geschäftsmobilität. Dafür ist das Data Center ein Schlüsselfaktor, dem man viel Aufmerksamkeit widmen muss. Heute bestimmen die Anforderungen an die Applikationsverfügbarkeit, wie Anwendungen in Rechenzentren gehostet werden. Bis dahin war es ein langer Weg, in dessen Verlauf sich die meisten Komponenten des Rechenzentrums geändert haben: Server, Storage und Netzwerk-Infrastruktur.

Der übergreifende Trend heißt dabei Virtualisierung. Der erste und sehr wichtige Schritt hin zu einer Evolution des Rechenzentrums war die Servervirtualisierung. Sie versprach Kostensenkungen bei Infrastruktur und Betriebsmitteln, Skalierbarkeit, Flexibilität, mehr Redundanz und schnelleres Recovery nach Störungen,.

Um die möglichen Vorteile der Virtualisierung voll auszuschöpfen, müssen nicht nur Server, sondern auch die übrigen RZ-Komponenten, beispielsweise die Netzwerkinfrastruktur, weiter entwickelt werden. Tatsächlich haben sich die Vernetzungstechniken im Rechenzentrum deshalb ebenfalls verändert. Sie wurden zunächst redundant ausgestaltet. Inzwischen kann man eine skalierbare Fabric in und zwischen Rechenzentren aufbauen.

Drei Trends werden die nächste Generation der Data-Center-Netzwerke prägen:

- Virtualisierungsinitiativen werden auf allen RZ-Ebenen selbstverständlich.
- Die Zahl der Netzwerkebenen sinkt, die Leistung steigt.
- Daten- und Storage-Netze werden vereinigt.

Zukunftsfähige Netzwerkkomponenten müssen alle drei Trends möglichst optimal unterstützen.

Virtualisierung hat die Anforderungen ans RZ-Netz dramatisch geändert. Von Rechenzentrums-Anbietern, die moderne, hoch virtualisierte und dynamische IT-Infrastrukturen betreiben, wird heute ein Maximum an Skalierbarkeit und Performance bei kosteneffizientem und belastbarem Infrastrukturbetrieb verlangt. Denn die überkommenen, hoch segmentierten Data-Center-Netzwerke unterstützten die Schlüsselvorteile der Virtualisierungstechnologie, zum Beispiel Dynamic Virtual Machine Provisioning (vMotion/XenMotion), nicht.

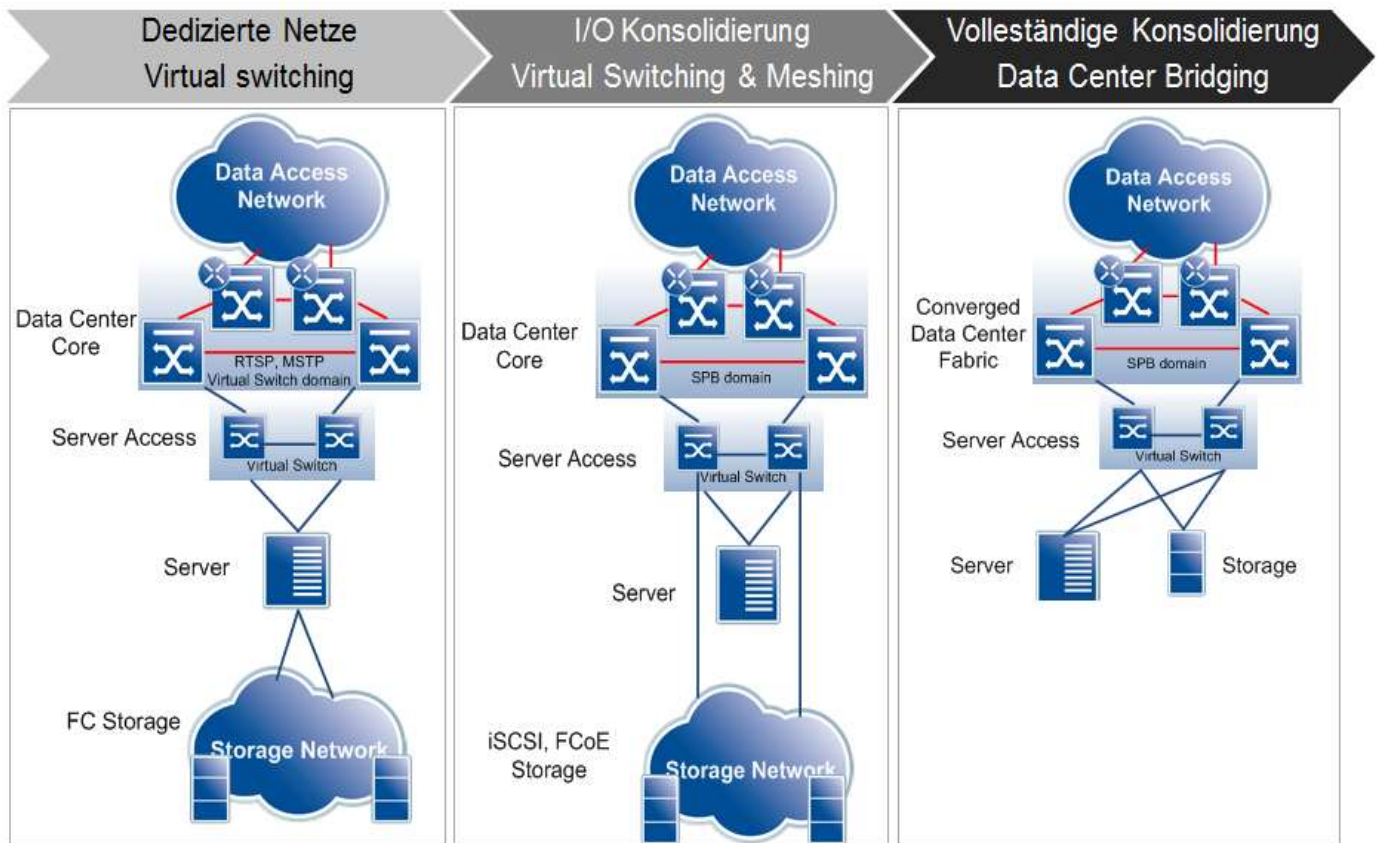
Der heute übliche Wegfall von Netzwerkebenen löst das ursprüngliche Flexibilitätsproblem, bedeutet aber neue Herausforderungen beim Design. Ob den Unternehmen die durch Virtualisierung mögliche Verringerung von Emissions- und Betriebskosten sowie Ausfallzeiten in vollem Umfang zugutekommen werden, hängt sehr von der Architektur der nächsten Rechenzentrumsgeneration ab: Nur bei weniger Schichten im Rechenzentrum werden auch die Kapitalinvestitionen und Betriebskosten sinken. Denn dann braucht man weniger Equipment, was CAPEX (Kapitalausgaben) und OPEX (Betriebsausgaben) verringert. Gleichzeitig steigern kürzere Latenzzeiten auch die Leistung der Anwendungen. Einerseits steigt also die Bandbreite, andererseits verringern weniger Geräte die Topologiekomplexität.

Die kommende SAN-Konvergenz stellt Netzwerke im Datenzentrum vor völlig neue Aufgaben und Gesichtspunkte. Das Thema wird heiß debattiert. Neue Standards wurden je nach SAN-Technologie gerade verabschiedet oder befinden sich in der Ratifizierung. Das wichtigste Argument für Konvergenzkonzepte ist im allgemeinen die Konsolidierung der Infrastruktur: Datenverkehr und Speicher teilen sich dieselbe Infrastruktur und nutzen eine gemeinsame Schnittstelle auf dem Server, was den Ressourcenaufwand verringert. Die erste konvergente SAN-Technologie war iSCSI, derzeit steht Fibre Channel over Ethernet (FCoE) im Mittelpunkt des Interesses.

Dieses Kapitel beschreibt mit der Extreme Networks Data Center Architektur ein Konzept für RZ-Netze der Zukunft, bei dem alle drei aufgeführten Trends berücksichtigt werden.

Die Komponenten von Extreme Networks Data Center

Mit der Architektur von Extreme Networks Data Center können Kunden heutige Rechenzentrums-Netzwerke problemlos in eine einheitliche Fabric migrieren, die alle drei oben genannten Schlüsselanforderungen an die Rechenzentrumsnetze der Zukunft erfüllt.



Die Architektur setzt sich aus folgenden Hauptkomponenten und -merkmalen zusammen:

- **Virtualisierung/Management-automatisierung:** Wenn virtuelle Server (neu) aufgesetzt werden, garantiert sie höchstmögliche Automatisierung aller Managementaufgaben
- **Data Center Bridging:** Die Architektur unterstützt effizient I/O und SAN Konvergenz in der Data Center Fabric.
- **Multipath Switching:** Multipath Switching erhöht die verfügbare Bandbreite und ist gleichzeitig der Weg zu einer redundanten, ausfallsicheren Anbindung von Servern und Blade-Center-Switches.

- **Fabric Core Meshing:** Fabric Core Meshing aggregiert die gesamte Kapazität im Kern der Data Center Fabric und leitet Daten immer über den kürzesten Pfad an ihr Ziel, so dass es dort nur sehr geringe Verzögerungen gibt.
- **Applikations-Awareness:** Die Architektur bietet Applikationstransparenz und -kontrolle in der Data Center Fabric.

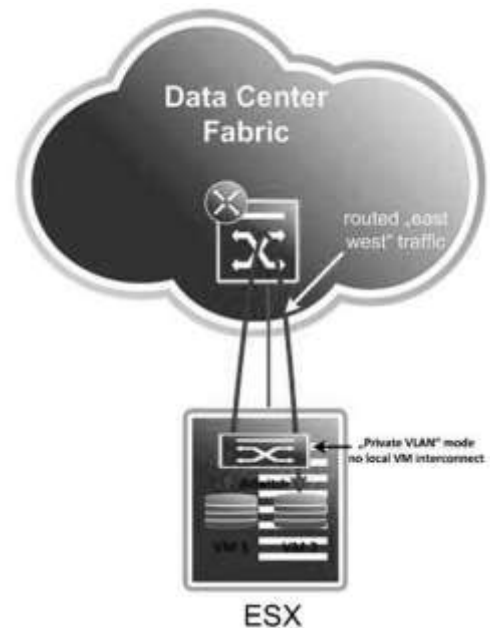
Virtualisierung

Virtualisierung ist der größte Entwicklungsschritt, den Rechenzentrumstechnologien in den vergangenen zehn Jahren vollzogen haben. Durch Server- und Storage-Virtualisierung lassen sich Services heute schnell ändern. Diese Dynamik führt zu neuen Anforderungen an das Netzwerk im Rechenzentrum. Wenn sich Anwender, Endgeräte und Applikationen bewegen oder verändern, ändern sich entsprechend schnell auch Netzwerkkonfigurationen, da Server/VMs zu den physikalischen Maschinen hinzugefügt oder zwischen ihnen bewegt werden.

Um Netzwerkdienste in Echtzeit innerhalb einer virtualisierten Umgebung bereitzustellen und die Kluft zwischen virtueller Maschine und Netzwerk zu überbrücken, hat Extreme Networks seinen Data Center Connect in ExtremeControl integriert. Data Center Connect ist eine leistungsstarke SDN-Lösung. Sie macht das laufende Geschehen in der gesamten Data Center Fabric einschließlich Netzwerkinfrastruktur, Server, Speicher und Anwendungen im physischen und virtuellen Umfeld durchschaubar und ermöglicht es, diese Elemente zu steuern und zu überwachen. Ihr Management wird weitgehend automatisiert.

Um Extreme Data Center Connect zu nutzen, braucht man keine spezielle Software oder Applikation auf dem Hypervisor oder den virtuellen Maschinen. Die Lösung verbindet sich direkt mit dem nativen Hypervisor und dem Hypervisor Management System. Die Steuerung und Überwachung physischer und virtueller Server beeinflusst die Server oder das Betriebssystem nicht. Unternehmen können individuell den Server- oder Hypervisor-Hersteller frei wählen und müssen sich nicht an einen Hersteller binden. Data Center Connect unterstützt alle wichtigen Virtualisierungsplattformen, darunter Citrix XENServer und XENDesktop, Microsoft Hyper-V und VMware vSphere, ESX, vCenter und VMware View.

Extreme Data Center Connect integriert sich in existierende Workflow- und Lifecycle-Tools. So überblickt der Administrator jederzeit virtuelle und physikalische Anlagen und kann physikalische und virtuelle Netzwerke für virtuelle Maschinen automatisch konfigurieren. Die APIs der jeweiligen Hersteller ersetzen arbeitsaufwändige Installationen auf dem Hypervisor. Außerdem veröffentlicht Extreme Networks APIs für



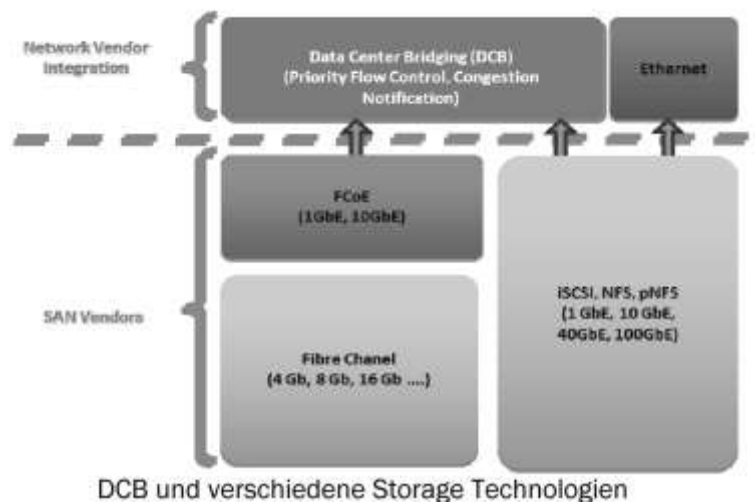
die automatisierte Inventarererkennung und Kontrolle der Hypervisor-Switch-Konfiguration sowie das Management der physikalischen Netzwerkkonfiguration.

Schon heute lässt sich mit Data Center Connect und Fabric Routing dieselbe Funktionalität realisieren. Letzteres erlaubt sogar den Einsatz von PVLAN (Private Virtual LAN)-Konfigurationen auf VMware vSphere Distributed Virtual Switches, um den Datenverkehr zwischen einzelnen virtuellen Maschinen umzuleiten.

Dabei routet der physikalische Switch außerhalb der ESX Servers gleichzeitig als „normaler“ End-of-Row/Top-of-Rack Switch und zwischen den PVLANS. Dadurch kann man den Datenstrom zwischen zwei VMs analysieren, regulieren und (z.B. via NetFlow) exportieren. Mit Extreme Data Center Connect lassen sich diese Systeme zentral und transparent konfigurieren. Alle Daten im Netz werden so einfach sicht- und damit kontrollier- und steuerbar.

Data Center Bridging

Langfristig sollen durch Ethernet als Transportschicht einer „konvergierten“ Data- und Storage-Lösung die Gesamtkosten (TCO = Total Cost of Ownership) sinken. Storage-Vernetzung wird in der Zukunft auf einer einheitlichen konvergierten Netzwerk-Infrastruktur basieren – mit neuen Protokollen und neuer Hardware. Mit dem Ansatz von Extreme Networks kann man schon heute einfach und sehr effizient iSCSI-SAN- oder NFS-NAS (Network Attached Storage)-Umgebungen aufbauen, optimieren und sichern. Damit Storage-Daten entsprechend schnell angesprochen und geliefert werden, erkennt, klassifiziert und priorisiert Extreme Networks hierbei automatisch den IP-SAN-Traffic.



Die IEEE Data Center Bridging (DCB) Task Force, eine Arbeitsgruppe des IEEE 802.1-Standardisierungsgremiums, arbeitet an einer Standardsuite, die Ethernet zur universellen Transportschicht für Server- und Speicherdatenverkehr im Rechenzentrum macht. Besonders wichtig wird dabei Fiber Channel over Ethernet (FCoE) sein. Mit DCB lässt sich ein verlässlicheres, auf Ethernet-Technologie basiertes Netzwerk aufbauen. Es liefert Daten nicht mehr „best effort“, sondern arbeitet verlustfrei (lossless). Engpässe auf Netzwerkschicht 2 handhabt ein solches Netz effizienter als ein traditionelles TCP-basiertes Netz. Dazu kommen Mechanismen zur Kontrolle der einzelnen Datenströme (Flows). Auch wenn traditionelle Storage-Protokolle wie iSCSI und NFS vom DCB profitieren werden, sind sie nicht darauf angewiesen. FCoE dagegen verlangt verlustfreien Betrieb, der sich in einer Multi-Hop Switch-Umgebung nur mit DCB realisieren lässt.

DCB baut hauptsächlich auf drei IEEE Spezifikationen auf:

- **IEEE 802.1Qaz – ETS & DCBX** – Bandbreitenzuweisung an Hauptverkehrsklassen (Priority Groups) plus DCB Management Protokoll
- **IEEE 802.1Qbb – Priority PAUSE** – Wahlweiser Verkehr auf dem Link durch Priority Group PAUSIEREN (dabei werden Pause-Frames an einen Sender geschickt, der so lange keine Daten mehr verschickt und damit die Verbindung entlastet)
- **IEEE 802.1Qau** – Dynamische Engpassbenachrichtigung

Extreme Networks hat diese Standards auf den wichtigsten Data-Center-Plattformen implementiert.

Eine vollständige FCoE-SAN-Konvergenz auf Netzwerken mit DCB wird wohl erst in einigen Jahren umgesetzt werden. IP-SAN-Konvergenz ist allerdings schon heute verfügbar. Zunächst werden die Ein-/Ausgabeaktivitäten des Servers mit der Ethernet Data Fabric konsolidiert. In der zweiten Phase fließt das SAN komplett oder selektiv in die vorhandene Fabric ein.

Die erste Phase reduziert hauptsächlich die Serverkosten, da keine dedizierten HBAs (Host Bus Adapter) mehr nötig sind. Dies spart Server-Energiekosten und verringert den Platzbedarf. Außerdem erleichtert es den Betrieb und spart weitere Kosten, da man weniger Kabelverbindungen zum Server braucht. Auch Switch-Ports werden weniger benötigt. In der zweiten Phase braucht man in der kompletten Fabric weniger Netzwerkgeräte, dafür aber ausgereifte Standards. Deshalb wird es wohl mehrere Jahre beanspruchen, bis dieses Design der Mainstream in Rechenzentren ist.

Multipath Switching

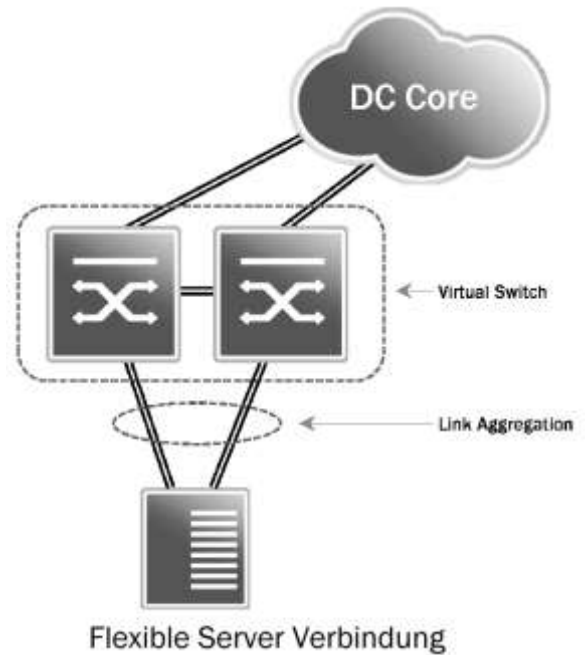
Während in traditionellen Netzwerkdesigns stets Protokolle zum Einsatz kamen, die auf dem Blockieren einzelner Links und dem damit verbundenen Schaffen loopfreier Topologien basierten, sind in heutigen Design Protokolle am Werk, die es ermöglichen sämtliche Links aktiv zu nutzen und dabei auch noch eine optimierte Wegewahl zu gewährleisten.

Die verfügbaren Umsetzungen von Multipath Bridging lassen sich in zwei Gruppen unterteilen:

- Hardwarebasiertes Multipath Switching (Stacking, VSB)
- Protokollbasiertes Multipath Switching (MLAG, TRILL, SPB)

Hardwarebasiertes Multipath Switching

Virtual Switch Bonding bzw. Stacking stattet Data-Center-Architekten beim Data Center Switching mit neuen Werkzeugen aus. Sie erhöhen die Applikationsverfügbarkeit, senken die Antwortzeiten und verbessern und vereinfachen die Edge-Netzwerktopologie. Virtuelles Switching gewinnt in Rechenzentren Akzeptanz. Denn damit sind elastische Serververbindungen möglich, die früher eine manuelle Konfiguration der Server voraussetzten. Heute sehen Server beim virtuellen Switching in ToR (Top of Rack)-Designs zwei physikalische Switche als ein einziges System. Das ermöglicht:



- Automatische Link-Aggregation physikalischer Switches und Server
- Vermaschung von L2-Netzwerk-Uplinks zur Data-Center-Aggregationsebene und den Core-Switches
- Non-Stop-Weiterleitung von Applikationsverkehr, falls eines der Geräte ausfällt.

Extreme Networks löst alle drei Aufgaben. VSB und Stacking führen physikalische Switches zu einem einzigen, logischen Switch zusammen, um die verfügbare Bandbreite zu erhöhen, und vermascht aktiv Server und Switches im Rechenzentrum. VSB und Stacking sind in verschiedenen Chassis der wichtigsten Data-Center-Plattformen verfügbar.

Diese Technologie bietet außerdem:

- automatisierte, Host-spezifische Netzwerk-/Sicherheitsprofile per Virtual Host und Port
- maximale Verfügbarkeit und Ausfalltoleranz
- eine etablierte Technologie mit mehr als drei Millionen Switch- und Routerports im Einsatz

Protokollbasiertes Multipath Switching

Die Anforderungen geschäftskritischer Applikationen verlangen Flexibilität und Performance im gesamten Netzwerk, nicht nur auf einer bestimmten Schicht. Für neue Data-Center-Technologien wie Server-Virtualisierung und FCoE sind mehr denn je „flache“ Layer-2-Netztopologien gefragt. Denn es soll in dem oft hochskalierbaren Dreischichtsystem aus Darstellungsebene, Applikation und Datenbankservern heute jeder immer mit jedem kommunizieren können. Das erfordert eine blockierungsfreie, hochleistungsfähige Netzwerkinfrastruktur mit geringer Latenz.

In den vergangenen Jahren entstanden Netzwerke mit aktiven und passiven Links. Zwar sicherte das ausreichende Redundanz, allerdings kam es bei Änderungen der Netztopologie häufig zu Dienstaussfällen, bis im gesamten Netz die neue logische Konfiguration wieder stimmte. Heute werden viele logische Netztopologien mit Hilfe von Standards wie IEEE 802.1Q-2005 MSTP (Multiple Spanning Tree Protocol) konfiguriert, die mehrere Topologien ermöglichen, so dass alle vorhandenen Links bestmöglich genutzt werden.

Während es MSTP erlaubt, alle Links überhaupt zu nutzen, werden nicht alle Links gleich stark ausgelastet. Das liegt daran, dass die Segmentierung immer noch aktive/redundante Links innerhalb jeder VLAN-Gruppe erlaubt. Netzwerke der nächsten Generation müssen Aktiv/Aktiv-Konfigurationen mit folgenden Eigenschaften unterstützen:

- Sie muss Ausfälle so behandeln, dass nur direkt betroffener Verkehr bei der Wiederherstellung beeinflusst wird
- Alle verfügbaren physikalischen Verbindungen sollen ohne Bandbreitenverlust ausgenutzt werden
- Verbindungen werden nach Ausfall schnell wieder hergestellt
- Broadcast- und Multicast-Verbindungen müssen besonders schnell wieder herstellbar sein

Extreme Networks realisiert diese Anforderungen mit folgenden Technologien:

- Shortest Path Bridging (SPB) – IEEE 802.1aq work group
- Transparent Interconnect of Lots of Links (TRILL) – IETF TRILL work group
- MLAG (Multiple Link Aggregation Groups)

Alle vereinfachen die Netzwerktopologie im Rechenzentrum und vermaschen aktiv Edge und Core in Rechenzentrumsnetzen.

Extreme Networks besitzt viele Patente im Bereich Netzwerk-Fabrics. 1996 stellte Extreme Networks das erste auf Layer 2 vermaschte Ethernet-Netzwerk der Branche vor; eine aktive Vermaschung auf Basis eines intelligenten Router-Protokolls unter der Bezeichnung SecureFast. Als VLSP (VLAN Link State Protocol) diente dabei OSPF (Open Shortest Path First), um die Erreichbarkeit von MAC-Adressen zwischen Netzelementen auszutauschen.

Shortest Path Bridging (SPB)

IEEE SPB nutzt IS-IS (Intermediate System to Intermediate System Protocol) als Routing-Protokoll, um ähnliche Ziele zu erreichen. Das IEEE hat sich offiziell dazu bekannt, alle existierenden und neuen IEEE Standards (besonders die IEEE Data Center Bridging Protokolle, aber auch die bestehenden Managementprotokolle, Ethernet IEEE 802.1ag (OAM), etc.) via IEEE SPB zu unterstützen. IEEE SPB nutzt MAC in-MAC-Encapsulation (IEEE 802.1ah). Dabei wird ein MAC-Header in einen weiteren MAC-

Header verpackt. Dieser Header gehört zum Provider Backbone Bridging Standard. Insgesamt bezeichnet man dieses Vorgehen als SPB-M-Implementierung. TRILL erlaubt verschiedene Pfade (Equal Cost Multipathing) und nutzt selbst ebenfalls verschiedene Pfade für Unicast und Broad-/Multicast.

Extreme Networks Data Center wird anfangs IEEE SPB anwenden, SPB wird per Software-Upgrade auf den wichtigsten Data-Center-Plattformen verfügbar sein und damit CoreFlow2-Technologie realisieren.

SPB baut auf bestehende Layer-2-LANs im Rechenzentrum, die MSTP nutzen, auf und ist deswegen voll dialogfähig, was die Netzwerkflexibilität erhöht. Existierende Infrastrukturen lassen sich mit wenig oder keinen Unterbrechungen auf den IEEE-Standard migrieren.



SPB bringt folgende Vorteile:

- **Plug and Play:** Beim aktiven Vermaschen muss man kaum oder gar nicht konfigurieren.
- **Weniger Sprünge (Hops):** Sind alle Links in der Fabric aktiv, nimmt der Verkehr immer den kürzesten Weg. Die Latenz zwischen Applikationen sinkt.
- **Höher aggregierte Kapazität:** Werden alle Links genutzt und keine blockiert, steigt die Kapazität der Fabric.
- **Skalierbarkeit:** Tausende Switches sind innerhalb einer einzigen Domain möglich.
- **Flexibilität:** Verbindungen, auch für Broad- und Multicasts, lassen sich nach Ausfällen schnell wieder herstellen. Ein Ausfall beeinträchtigt nur den direkt betroffenen Verkehr, nicht direkt betroffener Verkehr läuft einfach weiter.

Besonders für größere Data Center Fabric mit komplexen, ortsübergreifenden Topologien wird SPB zukünftig ein Schlüsselement, um die Vorteile von Virtualisierung und Konvergenz voll zu nutzen. Kleinere Netzwerke brauchen diese Funktion möglicherweise nicht. Da Server und Switches mehr leisten, sinkt die Zahl der Knoten im Datenzentrum dramatisch. Mittelgroße und kleine Infrastrukturen können dann auf komplexe Topologien verzichten.

TRILL

TRILL ist ein Verfahren, bei dem Pakete encapsuliert werden, um somit Data Center Ansprüchen gerecht zu werden. Das Verfahren ähnelt sehr stark dem Shortest Path Bridging (SPB) und Virtual Private LAN Service (VPLS), unterscheidet sich jedoch in einigen Schlüsselbereichen. Ähnlich wie MPLS gilt TRILL als Layer 2½ Protokoll. Aus der Sicht der Endsysteme ist das Netzwerk ein einziges großes und flaches Layer 2 Netzwerk. Innerhalb des Netzwerks werden die Pakete mit Hilfe von Layer 3

Technologien transportiert. Vergleichbar zu SPB und VPLS enthalten Trillpakete das komplette Datenpaket inklusive Header. Daher benötigt TRILL spezielle Edge Networking Devices, sogenannte Rbridges, um sowohl die lokalen MAC/PORT/VLAN Verbindungen als auch die Remote Adressen zu lernen.

TRILL liefert ein flaches Corenetzwerk, welches einfach skaliert und nach Plug and Play Mechanismen konfiguriert wird. Es wird eine hohe Verfügbarkeit und ausgezeichnete Bandbreitennutzung erreicht. TRILL „leiht“ sich Konzepte aus dem Layer 2 Switching und Layer 3 Routing sowie aus dem MAC-in-MAC Bridging und MPLS-VPLS-Tunneling. TRILL benutzt Link-State-Algorithmen um den besten Pfad, basierend auf Link Kosten, zu jedem Punkt im Netzwerk zu berechnen.

MLAG

Das Data Center Netzwerk Modell, welches wir weitestgehend benutzen, besteht aus drei spezifischen Elementen.

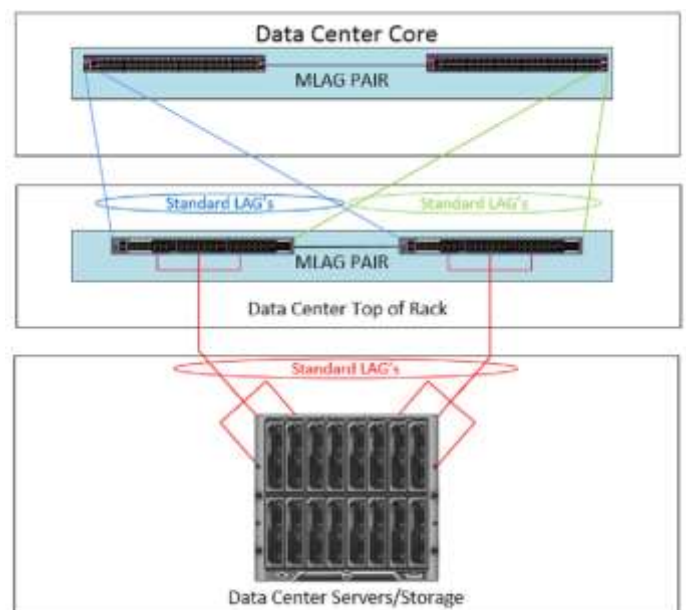
Zunächst Server und Storage Devices, welche sich in den Racks des Data Centers befinden. Diese Elemente sind der einzige Grund dafür, dass das Data Center überhaupt existiert. Irgendwelche Störungen in Konfiguration und Betrieb dieser Geräte führt zwangsläufig zu Störungen des gesamten Geschäftsbetriebs.

Zweiter Bestandteil unseres Modells sind die Top-of-Rack Ethernet Switches, die an die Server und Storageeinheiten angeschlossen sind. Diese Switches liefern den Netzwerkzugang und damit die Konnektivität zum restlichen Netzwerk.

Zu guter Letzt sind es die Data Center Core Switches, die den Sammelpunkt für die Top-of-Rack Switches bilden und es dadurch erlauben, dass alle Server und Storagekomponenten miteinander kommunizieren können.

Dieses Modell bietet die Grundlage für ein hochverfügbares und fehlertolerantes Netzwerk. Um eine maximale Verfügbarkeit zu gewährleisten, verwenden wir eine Technologie namens MLAG (Multiple Link Aggregation Groups). MLAG ist eine Technologie, die es ermöglicht, klassische Link Aggregations Groups (LAG) nicht nur mit dem ursprünglichen Zweck der Bandbreitenerhöhung zu verwenden, sondern auch zur Erhöhung der Verfügbarkeit.

Aufgrund der Einfachheit und Effizienz dieses Mechanismus ist MLAG mittlerweile zum Best-Practice Verfahren im Data Center geworden. Es ist einfach zu konfigurieren und liefert ein kostengünstiges Verfahren, welches normalerweise nur durch deutlich höhere Aufwendungen erzielt werden kann. Darüberhinaus wird MLAG auf dem



kompletten Extreme Networks EXOS Portfolio angeboten. MLAG arbeitet vom kleinsten 8 Port Gigabit Switch (X440-8t) bis hin zum 768 Port 10 Gigabit Switch (X8). Weder Linkgeschwindigkeit noch EXOS Version spielen hier eine Rolle.

Üblicherweise benötigt das Update eines Betriebssystems auf Top-of-Rack Switches einen Reboot, um das neue Betriebssystem zu aktivieren. Während dieses Reboots ist die Verbindung zwischen den Serverkomponenten und der Userzebene nicht möglich. Obwohl dieser Verbindungsverlust geplant werden kann und damit keine Auswirkungen auf das Business hat, ist es dennoch mit sehr viel Aufwand verbunden, alle Server und Stagesystem offline zu nehmen, oder in einen definierten Zustand zu bringen.

Oft wird als Gegenstrategie hierzu ein Stacking verwendet. Die Idee dahinter ist, falls ein Switch „stirbt“, ein anderer im Stackverbund dessen Aufgaben übernehmen kann. Oftmals ist dieses eine sehr valide Strategie. Es gibt jedoch nicht wenige Fälle, in denen der Stack an einem Software- oder Hardwareproblem leidet, welches den kompletten Stack Offline nimmt und dadurch auch sämtliche Server- und Storagekomponenten außer Betrieb setzt.

Im Gegensatz dazu kennen sich MLAG Switche, sind aber nicht in der Form miteinander gekoppelt, wie es bei einem Stackingkonstrukt der Fall ist. Am besten kann man dies mit HA Firewallclustern vergleichen, die in einem Verbund geschaltet sind und miteinander Informationen über den Betriebsstatus austauschen. MLAG Ethernet Switche agieren auf genau die selbe Weise.

Ein weiterer Vorteil ist, dass Server und Storagekomponenten nicht speziell oder proprietär konfiguriert werden müssen, um von der hohen Verfügbarkeit durch MLAG profitieren zu können. Es wird lediglich ein einfaches NIC-Teaming benötigt, um die Verbindung zu MLAG Switchen herzustellen.

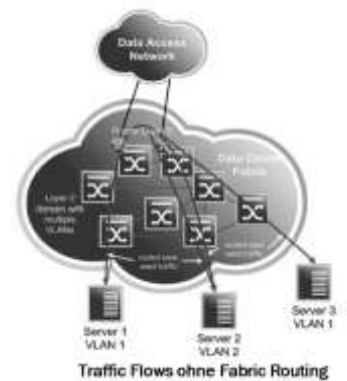
Fabric Core Mesh—Layer 3 Fabric Routing

In der konvergierten Data Center Fabric ist traditionelles Layer-3-Routing häufig problematisch. Denn Servervirtualisierung und FCoE brauchen große und „flache“ Layer-2-Netzwerke, um zu funktionieren und ihr volles Potential zu realisieren. Aber wenn Server auf Subnetze (Server Subnets) verteilt sind, erfolgt die Kommunikation zwischen ihnen mittels Routing. Das führt in Netzen, in denen nur Layer 2 Protokolle (SPB/TRILL/MLAG) implementiert sind, zu Engpässen an den Routerschnittstellen, die sich in herkömmlichen Designs am Edge der Data Center Fabric befinden. Auch traditionelles VRRP (Virtual Router Redundancy Protocol) erlaubt nur ein einziges aktives Default-Gateway auf Layer 3 und schafft damit einen Engpass. Für die Lastverteilung sind solche Konzepte ineffizient und erhöhen die Latenz im Netzwerk. Fabric Routing realisiert verteiltes Routing in Switchen und Routern, die Layer 2 Multipath Switching integrieren. Insgesamt lassen sich so ein maximaler Durchsatz, niedrigste Latenz und optimierte Datenströme, wie es heute verlangt wird, in der Data Center Fabric realisieren.

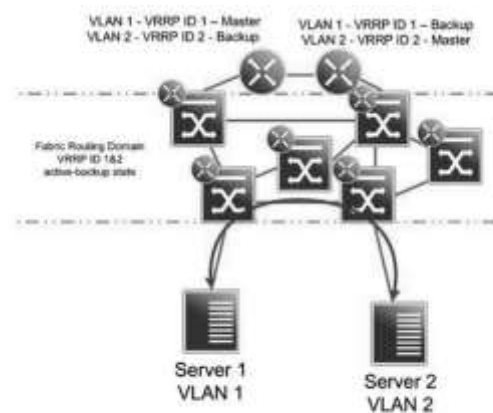
Zum Verständnis: Im Netzwerk unterscheidet man die Verkehrsrichtungen Nord-Süd und Ost-West. Unter Nord-Süd-Verkehr versteht man die Kommunikation zwischen Clients in der Peripherie, etwa in einer Filiale, und dem Rechenzentrum, wo die verwendeten Applikationen gehostet werden, oder umgekehrt. Ost-West-Traffic bezeichnet den Datenverkehr zwischen den Servern innerhalb einer Data Center Fabric.

Extreme Networks Fabric Routing ist primär auf geroutetem Ost-West-Traffic ausgerichtet, baut auf das bekannte VRRP auf und ist damit dialogfähig. Administratoren können ihr vorhandenes Wissen nutzen, um Netze optimal zu implementieren. Fabric Routing als Komponente der Extreme-Architektur ist auch im Campus LAN mit Mehrwert anwendbar.

Im rechten Bild routet der VRRP-Master den Datenverkehr zwischen den Servern in den VLANs 1 und 2 für jedes VLAN/Subnet am Edge der Fabric. In der dargestellten, typischen Installation sind die Server virtualisiert und innerhalb der Fabric mobil. Ein optimaler Pfad oder Ort für die Router lässt sich deshalb nicht festlegen – also werden die Geräte irgendwo im Randbereich des Netzes angeschlossen. Das verdreifacht in diesem Beispiel die Latenz (6 gegenüber 2 Hops), erhöht unnötig die Bandbreiten an fünf zusätzlichen Fabric-Links und begrenzt die aggregierte Routingleistung zwischen zwei VLANs in der Fabric auf einen einzigen Link.



Fabric Routing erweitert VRRP und ist vollständig mit existierenden VRRP-Routern kompatibel. Das VRRP-Auswahlverfahren und das VRRP-Protokoll bleiben unverändert. Beim Fabric Routing per VRRP-Router-ID kann der Extreme Networks Switch/Router den sogenannten „Active-Backup“ übernehmen. Dabei sammelt der Switch/Router jeden Frame, der für diese VRRP-MAC-Adresse bestimmt ist. Dazu gehören Frames in ARP (Address Resolution Protocol)-Antworten vom VRRP Master an die Endsysteme und solche, die für deren Gateway-Adresse oder ein anderes Ziel (falls Proxy-ARP genutzt wird) im spezifischen Subnet bestimmt sind. Fabric Routing bietet in der Data Center Fabric zusammen mit SPB dieselbe Effizienz beim Datenfluss (Shortest Path) auf Layer 2 und Layer 3. Wird die Technologie innerhalb einer Layer 2 Multipath Switching Umgebung genutzt, optimiert das, verglichen mit einer traditionellen VRRP-Konfiguration, die Datenströme.

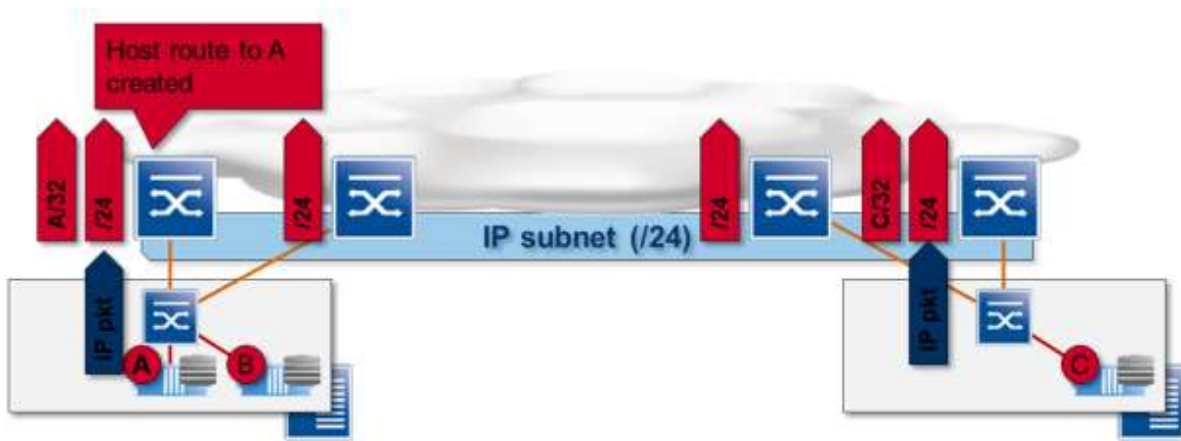


Fabric-Routing-Konfiguration mit multiplen VLANs und VRRP IDs

Data Center Interconnect - Host Routing

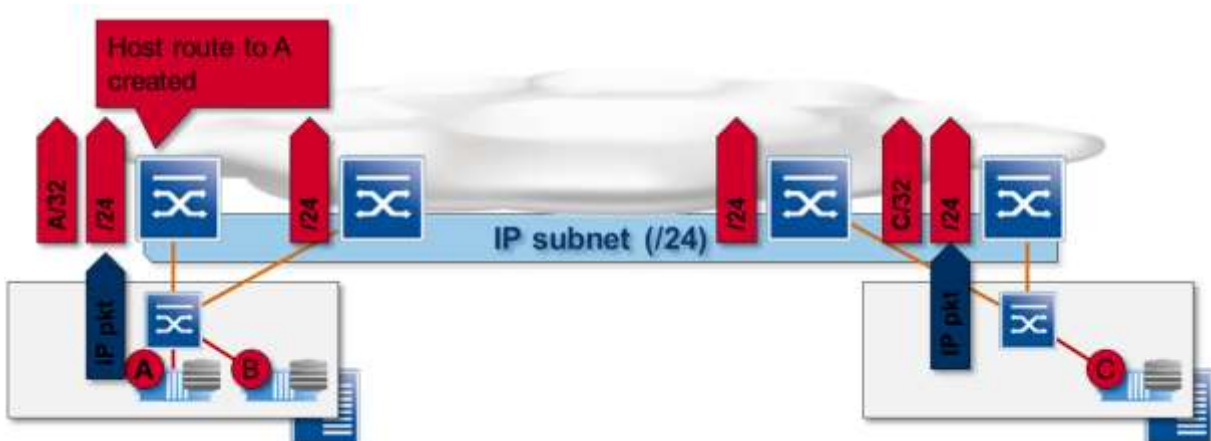
Fabric Routing optimiert den Ost-West-Traffic innerhalb eines verteilten Datenzentrums zwischen virtuellen und mobilen Servern. Doch es gibt ein weiteres Problem: Baut ein externer Client eine Verbindung zu einem Server auf, wird diese Verbindung in aller Regel über jenen Router geleitet, der als letzter Traffic von oder zu dem entsprechenden Ziel gesehen hat. Ist der Server in der Zwischenzeit umgezogen, erfahren dies die Router auf den höheren Netzwerkebenen zu spät; der Datentransport macht also Umwege, erleidet Verzögerungen oder bricht gar zusammen.

Host Routing verhindert das präventiv, indem eine Host-Route mitgeteilt wird, sobald ein Router den Umzug eines Servers erkennt. Damit ist sichergestellt, dass alle eingehenden Datenverbindungen verzögerungsfrei direkt an das richtige Data Center fließen. Das entlastet die Verbindungen zwischen den Rechenzentren. Dabei reicht es schon aus, dass einer der Access Switches ein Paket sieht, um eine OSPF LSA an das Default Gateway zu senden, die als Host-Route vor der Netz-Route Vorrang hat.



Zieht nun ein Server um, so erkennt der angeschlossene Switch die IP-Adresse und schickt ebenfalls eine LSA an das Default Gateway. In dieser kurzen Phase wird zwar nicht der optimale Pfad zum Ziel gewährleistet, allerdings dauert diese nur an, bis der veraltete Routing Eintrag wieder verworfen wurde.

Um Host Routing sicher einsetzen zu können, muss Dynamic ARP Inspection und IP Source Guard auf den Access Switches aktiviert sein. Ansonsten könnte eine Fehlkonfiguration IP-Adressen spoofen und damit die Routing Topologie stören.



Applikations-Awareness

Die meisten heute eingesetzten Netzinfrastrukturkomponenten liefern keine Daten für die Applikationssteuerung und -überwachung. Netzwerke werden typischerweise so implementiert, dass alle Services und Applikationen die gleiche Priorität haben. Üblich sind auch sehr rudimentäre Priorisierungsschemata. Durch verbreitete Virtualisierung, SOA-Architekturen, Cloud Computing und weitergehende Netzwerkkonvergenz entspricht dieses typische Szenario den heutigen Anforderungen nicht mehr. Dies betrifft Access-Netzwerke und Data Center Fabrics. Es ist inzwischen in jedem Bereich des Netzwerks kritisch, Applikationen exakt zu identifizieren, zu steuern und zu überwachen, damit sie wie gewünscht verfügbar sind. Dafür reicht es nicht, den Verkehr auf der Transportschicht zu kontrollieren.

Extreme Networks CoreFlow2-Technologie bietet IT-Administratoren mehr Einblick in kritische Betriebsapplikationen. Sie können diese Anwendungen genauer kontrollieren, um die Dienstgüte zu erreichen, die das Geschäft erfordert. Zu den neuartigen Anwendungen, die CoreFlow2 auf vielen Bereichen ermöglicht, gehören:

- **SAN:** Zugangskontrolle für iSCSI-Ziele mit Granularität für den Initiator und Kontrolle der Bandbreitennutzung für jedes iSCSI-Ziel
- **IP Voice & Video:** QoS und Zugangskontrolle für RTP (Real-Time Transport Protocol)-Mediastreams und Kontrolldaten
- **Cloud:** rollenbasierte Zugangskontrolle für Cloud Dienste wie salesforce.com
- **Bandbreitenüberwachung** für bestimmte Seiten wie youtube.com

Erreicht wird das durch die Kombination von Systemen mit CoreFlow2 Prozessor und Application Analytics. Extreme Application Analytics erlaubt den IT-Administratoren, jeden Teil des Netzwerkes für jede Applikation zu optimieren und Analysedaten bereit zu stellen. Somit verändert das Netzwerk seinen Stellenwert vom bloßen Transportmedium zum strategischen Unternehmensbereich.

Es werden im ganzen Netz verteilte Sonden unterstützt, welche die Antwortzeit von Anwendungen messen. So können IT-Administratoren das Anwendungsverhalten im Netz besser überwachen. Sie können so die vereinbarten SLAs (Service Level Agreements) einhalten, die Verfügbarkeit der Applikationen erhöhen und Fehler schneller finden und beheben.

Zusammenfassung

Data-Center-LANs entwickeln sich stetig weiter. Was gestern funktionierte, kann morgen schon antiquiert sein. Geschäftliche Anforderungen zwingen die IT, Anwendungen auf neue Weise bereitzustellen. In Edge-Computing-Modellen wandern Applikationen vom Netzwerkrand auf virtuelle Desktops im Rechenzentrum. Gleichzeitig entwickeln sich Rechenzentren zu Lieferanten von privaten hybrid Cloud-Services und auch die Integration öffentlich verfügbarer Cloud-Services beginnt bereits. Daten- und Speichernetze konvergieren durch IP-SANs.

Mit offenen Standards hat Extreme Networks bereits heute eine Data-Center-Fabric-Lösung im Angebot. Sie verbessert die Leistung der Anwendungen und erhöht die geschäftliche Mobilität. Denn die Implementierung von virtuellem Switching erhöht die Flexibilität in Rechenzentren und wird sich durch vermaschte Technologien in der gesamten Fabric verbreiten. Extreme Networks stellt hierzu verschiedene Multipath Switching und Routingtechnologien zur Verfügung. Kunden, die Data-Center-Fabric-Architekturen aufbauen wollen, wählen daher mit Extreme Networks einen zukunftssicheren Ansatz.

Physikalische Designs im Data Center

Zwei Grundsatzentscheidungen bestimmen heute das Design von Rechenzentren:

- Die Zahl der Infrastrukturebenen (2-Tier- oder 3-Tier-Architektur)
- Die Switching-Topologie zur Anbindung der Server: In jeder Rackreihe (End-of-Row, EoR) oder in jedem Rack (Top-of-Rack, ToR)

2-Tier oder 3-Tier Design?

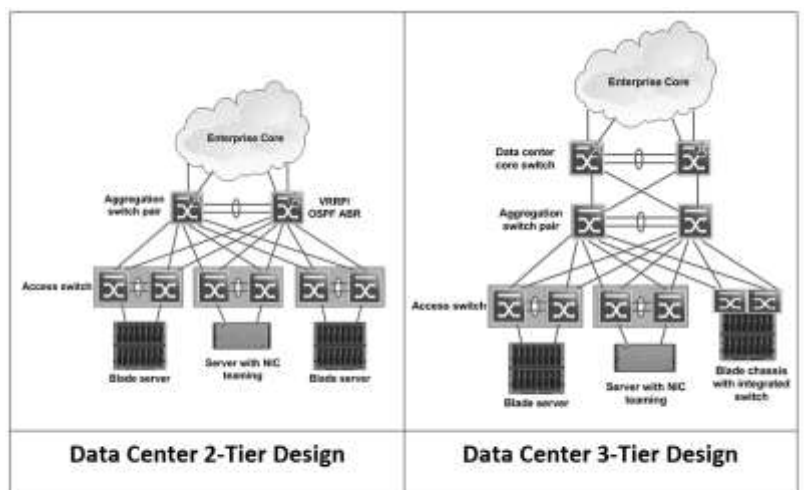
Vereinfacht gesagt geht es dabei um die Frage, ob das Data Center einen eigenen Core-Switch inklusive Routing-Instanz bekommt oder ob es bei Aggregations- und Access-Switches für die Server bleibt.

Jeder der beiden Ansätze hat spezifische Vor- und Nachteile:

Ein 2-Tier-Data-Center bietet meist geringere Latenzzeiten, eine kleinere Überbuchungsrate und die Komponenten lassen sich insgesamt einfacher konfigurieren. Weil weniger Geräte vorhanden sind, wird auch weniger Strom verbraucht, was sich positiv auf die Betriebskosten auswirkt. Nachteilig ist die schlechtere Skalierbarkeit, falls alle Ports der Aggregationsswitche bereits benutzt werden. Die anfangs einfache Verwaltung kann nach Erweiterungen durch neue Switches wieder komplexer werden.

Die hierarchische Struktur eines 3-Tier-Data-Center-Designs ist später sehr gut erweiterbar. Die Aggregations-Uplinks lassen sich weiter konsolidieren, was, wenn später neue Paare hinzugefügt werden, den Aufwand verringert. Die gesteigerte Flexibilität durch die zusätzliche Ebene erhöht jedoch die Verzögerungszeit des Netzwerks. Zudem verbraucht die zusätzlich nötige Hardware mehr Strom und Platz im Data Center.

Die Konsolidierung der Uplinks führt zu mehr Überbuchung von Ports und Bandbreite.



Tier 2 vs Tier 3

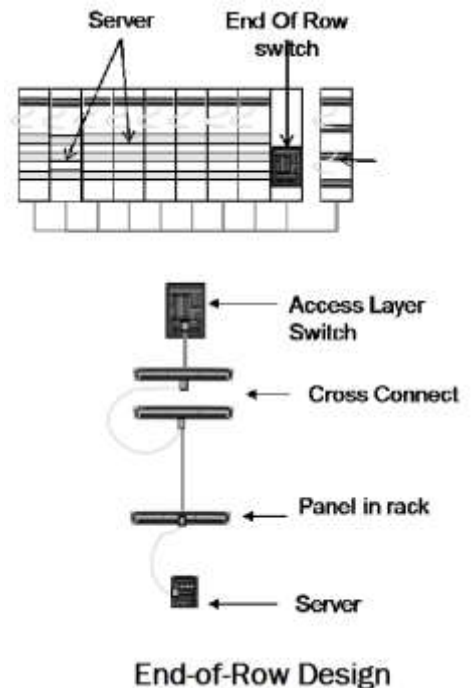
Oft dürfte deshalb ein 2-Tier-Design die bessere Wahl sein. Das „flache“ Netz ist wesentlich leistungsfähiger und entspricht auch den Ansprüchen zukünftiger Storage-Technologien. Ein 3-Tier-Design bietet sich eigentlich nur für sehr große oder in absehbarer Zeit sehr schnell wachsende Rechenzentren an.

End-of-Row versus Top-of-Rack

Die beiden Möglichkeiten zur Anbindung der Access Switches und Server, EoR und ToR, haben ebenfalls individuelle Vor- und Nachteile. Bei EoR-Installationen übernimmt ein Access Switch (Paar) die Anbindung einer ganzen Reihe von Serverracks.

Vorteile des EoR-Designs:

- Server können überall platziert werden und somit Hitzestaus besser vermieden werden.
- Ports werden besser genutzt als bei ToR-Designs.
- EoR spart Platz in Racks, reduziert Strom und Kühlung und verringert die Kapitalkosten.
- Der Managementaufwand sinkt durch weniger Switches.
- Die vorhandene Backplane senkt die Überbuchungsrate.
- Chassis-Switches haben üblicherweise mehr Features und skalieren besser.
- Weniger Switch Hops verursachen eine geringere Latenz.



Nachteile des EoR-Designs:

- Mit der Länge der Rack-Reihe steigt die Komplexität der Verkabelung.

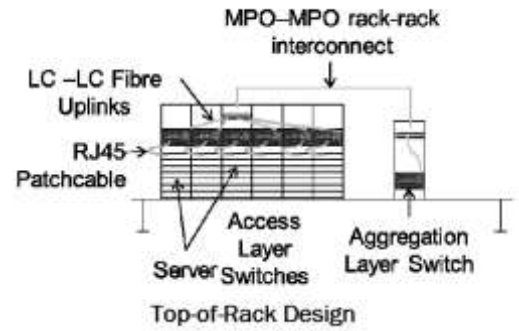
Im Gegensatz dazu steht das Top-of-Rack (ToR) Design. Es sieht einen Switch (oder zwei physikalische Switches, die logisch zu einem virtuellen Switch zusammengefasst sind) pro Rack vor. Dieser Switch konsolidiert die Verkabelung auf Rack-Ebene vor den Aggregationsswitches und erleichtert somit die Kabelführung – jedoch auf Kosten längerer Verzögerungszeiten. Zudem bleiben häufig Ports ungenutzt.

Vorteile des ToR-Designs:

- Vereinfachte Implementierung von Komponenten im Rack.
- Verkabelung ist vermeintlich einfacher und billiger.

Nachteile des ToR-Designs:

- Wechselt die Zahl der Server im Rack, wechselt auch die Zahl der aktiven Switchports, das Sachkapital (Switches) wird nicht ausgenutzt.
- Die Zahl ungenutzter Ports ist höher als beim EoR-Szenario.
- Strom- und Kühlungsanforderungen sind höher als beim EoR-Szenario.
- Bei einem Technologieupdate wird immer ein 1-RU (Rack Unit)-ToR-Switch ausgetauscht.
- ToR verschlechtert tendenziell die Skalierbarkeit, insbesondere durch Überbuchung der Uplinks und zusätzliche Switch-Hops, welche die Latenz erhöhen.

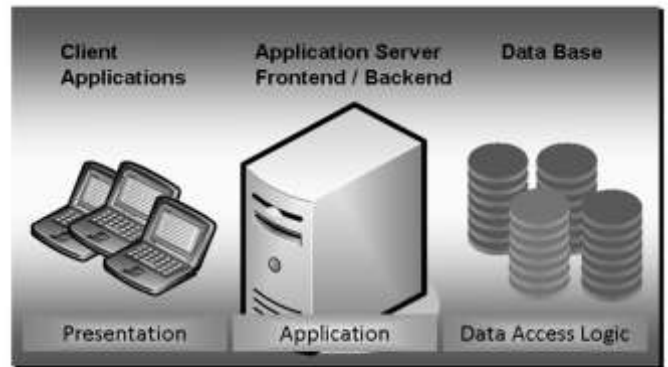


Überbuchung im Design

Die Überbuchung der vorhandenen Ressourcen ist im Access-Bereich üblich und bewährt. Allerdings unterliegt dieser Ansatz im Rechenzentrum vollkommen anderen Voraussetzungen.

Virtualisierungslösungen stellen dieses Prinzip in den Mittelpunkt, damit die vorhandene Hardware möglichst vollständig ausgelastet wird. Dies führt allerdings unweigerlich dazu, dass die Server verglichen mit traditionellen

Infrastrukturen nun wesentlich mehr Daten über jede Schnittstelle übertragen. Um trotzdem den Anforderungen gerecht zu werden, muss das Rechenzentrums-Netzwerk dies kompensieren und zudem die Dynamik einer sich ständig wandelnden Infrastruktur mit „wandernden“ Servern tragen können.



Client – Application - Database

Client – Application - Database

Prinzipiell gibt es drei Funktionsebenen im Data Center: Präsentations-/Web-Server, Anwendungsserver und Datenbankserver. Jede dieser Ebenen hat seine eigenen Verkehrsmuster, verlangt eine andere Übertragungsqualität und stellt spezielle Sicherheitsanforderungen. An sich liegt darin keine ungewöhnliche Anforderung. Neu ist jedoch der Umgang mit den durch Virtualisierung mobilisierten Servern. Zwar kann man Ressourcen nach wie vor manuell statisch zuordnen, das verspielt allerdings den größten Vorteil der Servervirtualisierung und verschlechtert daher erheblich deren Rentabilität. Deshalb sollte man schon bei der Planung eine möglichst geringe Überbuchungsrate auf Down- und Upstream-Links vorsehen und auch den möglichen Ausfall von Links berücksichtigen.

Komplexer wird die Lage durch die Konsolidierung von Daten- und Speichernetz in einer Infrastruktur. Speichernetze erzeugen auf dem Netz sehr viel Last. Sie brauchen spezielle Zeitfenster, in denen die Daten zugestellt werden. Die Parallelisierung von Datenströmen in solchen Netzen führt zu sogenannten „Bursts“, die besonders bei zu großer Überbuchungsrate problematisch sind. Dabei werden große Datenmengen von verschiedenen Stellen im Netz aus versandt und müssen teils gleichzeitig am Ziel ankommen. Um den Puffer am Switch nicht zu überlasten (das bezeichnet man als „Incast Problem“), sollte neben geringen Überbuchungsraten auch darauf geachtet werden, dass die eingesetzten Switches genug Speicherkapazität haben und das Netzwerk solche „Bursts“ abfangen kann. Wenn nicht, können durchaus ganze Transaktionen verloren gehen und die Leistung des Netzes kann drastisch einbrechen.

Logische Designs im Data Center

Ist die richtige Hardware gefunden, fehlt noch ein übergreifendes logisches Design. Auch hier gibt es bereits mehrere Technologievarianten. Wie bei der Hardware ist es sinnvoll, die Bereiche Core und Edge/Access zu unterscheiden.

Protokolldesign der Server-Edge/Access-Switches

Im Außenbereich des Netzes (Edge) kommen verschiedene Hardware oder Software basierende Multipath Bridging Methoden sowie Kombinationen daraus zum Einsatz.

- VSB/Stacking (Hardware-basierend)
- TRILL
- SPB
- MLAG

Protokolldesign der Core-Switches

Die Protokollauswahl für den Core-Bereich sollte sich an den heute üblichen und zukünftigen Standards orientieren. Dabei ist es sinnvoll, schon heute einen späteren Wechsel zu neuen Protokollarchitekturen zu bedenken, so dass dabei kein teures komplettes Redesign nötig wird.

Data-Center-Core-Design heute

Im Kernbereich des Rechenzentrumsnetzes werden heute oft noch MSTP und RSTP eingesetzt. Die Reife der Protokolle und das existierende Know-how der Administratoren spielen bei dieser Entscheidung eine wichtige Rolle. Wichtig ist auch die Kompatibilität der Standards mit den existierenden, nicht selten heterogenen Produkten. Somit werden diese Protokolle als kleinster gemeinsamer Nenner verwendet, um proprietäre oder unübersichtliche Konfigurationen zu vermeiden.

Das Core-Design des Data Center der Zukunft

Heute schon existieren Standards, welche die Vermaschung und Konvergenz von Storage- und Datennetzen optimieren. Technologien wie FCoE (Fibre-Channel over Ethernet) müssen in großräumigen Layer-2-Netzen besonders geringe Latenz aufweisen. Die Netze müssen außerdem flexibel skalierbar, blockierungsfrei und sehr leistungsstark sein, da die Kommunikation jedes Netzelements mit jedem anderen höchste Ansprüche stellt.

Next-Generation-Netzwerke müssen daher eine Aktiv-Aktiv-Konfiguration mit folgenden Eigenschaften unterstützen:

- Eingrenzung von Fehlern, damit nur direkt betroffener Traffic bei der Wiederherstellung verzögert wird
- Schnelle Wiederherstellung von Unicast-, Broadcast- und Multicast-Kommunikation.
- Ausnutzung der kompletten physikalischen Infrastruktur ohne Bandbreitenverluste. Verzögerung und Hops zwischen Servern werden minimiert.
- Schnelles Umschalten bei Verbindungsabbrüchen.

Extreme Networks-Switches bewältigen diese Aufgaben mit DCB (Data Center Bridging) und verschiedenen Multipath Bridging Protokollen (TRILL/SPB/MLAG)

Segmentierung von Load-Sharing im Layer-3-Core

Gerade größere Campusnetze sollten sich in verschiedene Bereiche, etwa Abteilungen, Kunden oder Unternehmen aufteilen lassen. Für Layer-3-Redundanz verwendet man meist die Protokolle OSPF (Open Shortest Path First)-ECMP (Equal-cost Multi-path Routing) oder VRRP (Virtual Router Redundancy Protocol). VRRP hat besonders im Data Center den Nachteil, dass bestehende Links für einen eventuellen Ausfall reserviert werden und nicht aktiv an der Datenübertragung teilnehmen. OSPF-ECMP hingegen bietet ebenfalls Redundanz für den Datenpfad, erlaubt aber auch die gleichzeitige aktive Nutzung aller Verbindungen, um die Last zu verteilen.

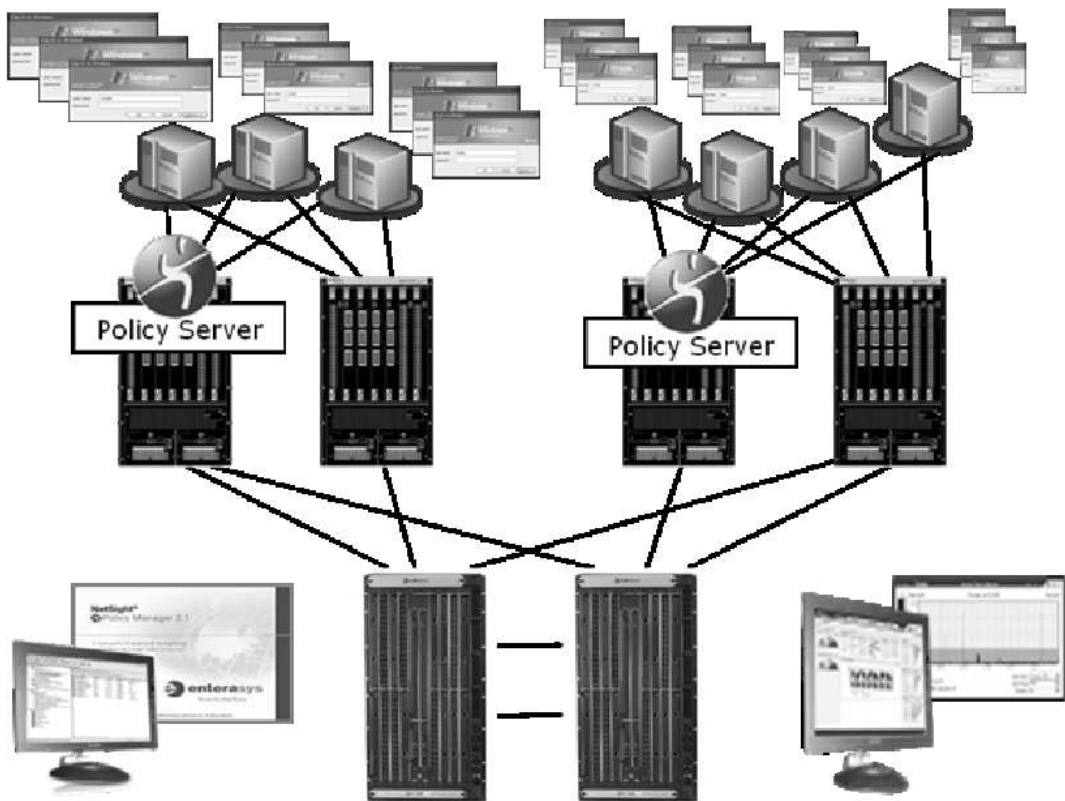
Um mehrere getrennte Routing-Domänen zu schaffen, verwendet man VRF (Virtual Routing and Forwarding). Das vereinfacht eine Installation besonders im Non-Provider-Bereich erheblich. VRF ermöglicht die Konfiguration mehrerer virtueller Routing-Instanzen innerhalb eines physischen Routers. Wie bei einer Implementierung mit MPLS entstehen dabei dedizierte Segmente für kritische Applikationen und Netzbereiche, die Konfiguration ist aber erheblich einfacher.

Virtuelle Welten

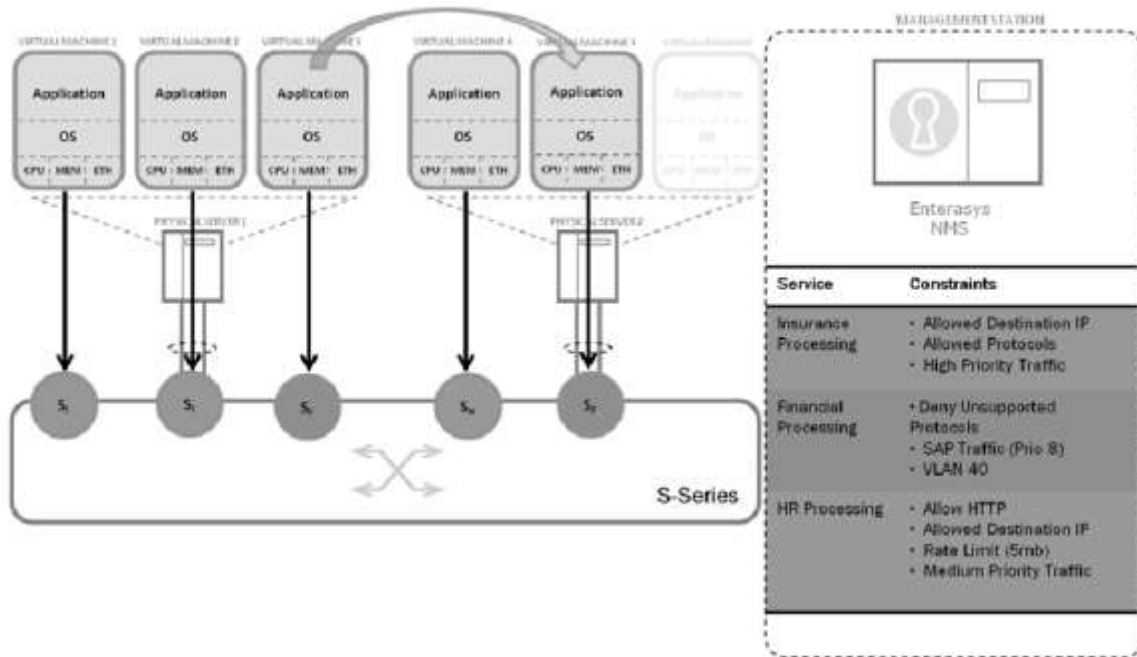
Welches Netzwerkdesign wird einem Data Center im ständigen Wandel gerecht? Extreme Networks bietet Lösungen für zwei Szenarien: Server- und Desktop-Virtualisierung.

Servervirtualisierung

Anhand virtueller Server lässt sich die Vielseitigkeit von Access Control -Integrationen zeigen. Immer mehr Netzwerke beherbergen Cluster und virtuelle Server, weil die dynamische Umverteilung der Software auf die Hardware optimale Auslastung und Flexibilität garantiert. Doch sind die Netzwerke meist nicht flexibel genug und Konfigurationen (z.B. Priorisierung von Daten) müssen manuell angepasst werden.



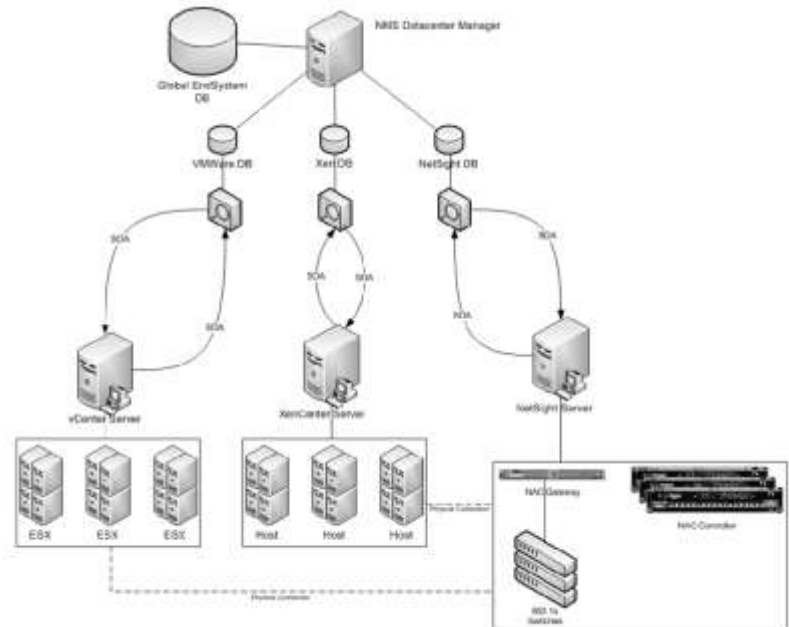
Falls virtuelle Systeme automatisch „umziehen“ – etwa bei einem Hardwareausfall – kompliziert das die Situation. Damit auch das Netzwerk bei Drag-and-Drop-Migrationen mithalten kann, lokalisiert Access Control die Server und vereinfacht es so, Rekonfigurationen im Netzwerk zu automatisieren.



Weitere technische und organisatorische Probleme gibt es in Umgebungen mit virtuellen Switches. So lassen sich die Zuständigkeitsbereiche von System- und Netzwerkadministratoren schwer voneinander abgrenzen.

Aktuelle Virtualisierungssoftware kann mittlerweile einen kompletten Switch auf einem Host abbilden (oder gar auf mehreren Hosts als Distributed Virtual Switch). Dazu gehören wichtige Einstellungen für die Datacenter-Plattform und das Unternehmensnetzwerk. So muss der Administrator VLANs erstellen, routen, protokollieren und analysieren, um so für sichere Kommunikation zwischen virtuellen Maschinen zu sorgen.

Extreme Networks behebt mit Data Center Connect diese Probleme. Dieses offene Framework synchronisiert Informationen zwischen Access Control und der Virtualisierungssoftware. Die aktuelle Version unterstützt VMWare vSphere, Citrix XenCenter und Microsoft Hyper-V. Im einfachsten Fall werden dadurch Detailinformationen zu einer virtuellen Maschine in der Endsystemübersicht des



Management Centers (Name der VM, UUID, etc.) oder Location-Daten innerhalb der Virtualisierungssoftware angezeigt. Dies erleichtert die Identifikation virtueller Maschinen im Netz und hilft dabei, Fehler schnell zu lokalisieren. Darüber hinaus lassen sich beide Seiten – Switchports und virtuelle Maschinen – automatisch konfigurieren. So erlaubt der Datacenter Manager den Aufbau von Identity and Access Control-Endsystemgruppen als (Distributed) Virtual-Switch-Portgroups. Dabei können auch erweiterte Parameter wie VLAN-IDs oder Port Modes (isolated, community, promiscious) eingestellt werden. Die Information darüber, welche VM an eine bestimmte Portgroup angeschlossen ist, dient zur Zuordnung der VMs zu einer Identity and Access Control-Endsystemgruppe. Dabei kann das System so eingestellt werden, dass der Administrator solche Zuordnungen bestätigen muss, bevor sie wirksam werden, um unabsichtliche Fehlkonfigurationen zu vermeiden.

So lassen sich die genannten Probleme elegant lösen. Der Netzwerkadministrator erstellt innerhalb des Management Centers die Regeln und Gruppen für VMs, wählt die VLANs aus und bestimmt, ob der Datenverkehr zwischen den Hosts zunächst über einen physikalischen Switch fließt (z.B. um Flowdaten zu analysieren). Der Systemadministrator schließt seine VM lediglich an eine bereits vorkonfigurierte Portgroup an und muss sich nicht mehr um die Konfiguration des Unternehmensnetzwerks kümmern. Beide Seiten sehen innerhalb ihrer Tools ständig, welche virtuelle Maschine an welchem physikalischen Switch angeschlossen ist und welche Zugangspolicy ihr zugewiesen wurde. Auch die bewährten Identity and Access Control-Mechanismen für die Prüfung und Reparatur virtueller Maschinen stehen weiter

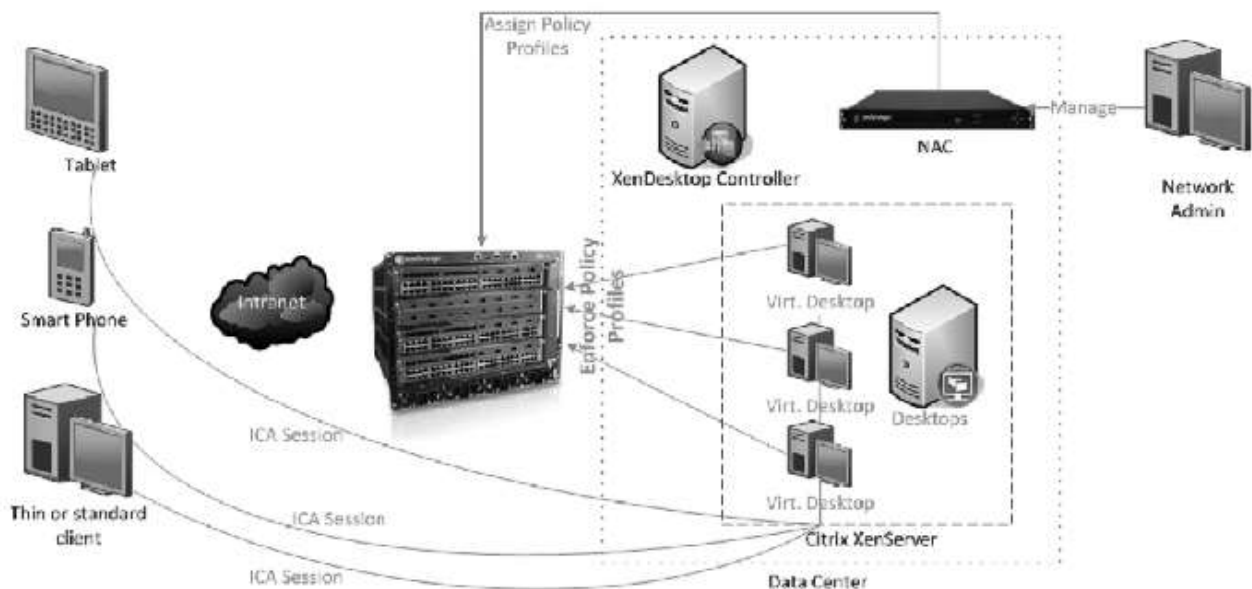
zur Verfügung. Obwohl Access Control eigentlich Endsysteme kontrolliert und nicht Server, kann diese Funktionalität hier dennoch sinnvoll sein, um eine adaptive Netzwerkkumgebung in virtualisierten RZ-Bereichen bereitzustellen.

Desktop Virtualisierung

Auf den ersten Blick unterscheiden sich virtuelle Server und Desktops kaum. Groß sind ihre Differenzen allerdings hinsichtlich der Sicherheit beim Netzwerkzugang.

Mittlerweile haben wir uns daran gewöhnt, dass Desktop-Systeme sich im Netzwerk authentisieren und sogar unterschiedliche Zugriffsprofile erhalten. Im Access-Bereich ist das relativ einfach, da Clients in der Regel an genau einen physikalischen Port angeschlossen werden und somit eindeutig klar ist, wie die Client-Daten durchs Netzwerk fließen.

Bei der Desktop-Virtualisierung greifen jedoch Thin Clients aufs Netz zu. Dazu gehören auch Tablet PCs oder gar Telefone. Die meisten Client-Datenpfade werden auf einige wenige Serverports konsolidiert. Doch es ist extrem schwierig, dort zu unterscheiden, welche Pakete von welchem Benutzer stammen. Traditionelle Verfahren wie Identity & Access Management sind hier unmodifiziert nicht ohne weiteres einsetzbar – umso weniger, je dynamischer sich die Virtual-Desktop-Umgebung verhält. Das Ziel von Virtual-Desktop-Implementierungen ist meist die spontane, automatische Provisionierung von Client-Desktops. Dabei wird der virtuelle Desktop bei Verbindungsaufbau aus einer Vorlage erzeugt. Differenzierte Zugangsprofile sind im Rechenzentrum noch wichtiger als im Access-Bereich, da Clients hier direkt im „Herzen“ des Netzwerks agieren. Sicherheitsverletzungen sind hier sehr riskant.



Extreme Data Center Connect eignet sich für den Einsatz mit den die wichtigsten Desktop-Virtualisierungslösungen am Markt. Data Center Connect erkennt die Zuordnung zwischen Virtual Desktop und entfernten Benutzern und kommuniziert sie an Extreme Access Control

Dank der bei der Extreme Networks Komponenten realisierten Multiuser Authentication werden die einzelnen Flows im Rechenzentrum leicht erkannt und ihnen entsprechend passende Zugangsprofile zugeordnet.

Extreme Data Center Connect Virtual Desktop Integration im Überblick:

- Clients verbinden sich durch sichere, verschlüsselte Tunnel mit dem Virtual Desktop im Data Center. Alle Benutzer haben in der Regel vom Virtual Desktop aus vollen Zugriff auf das Rechenzentrumsnetz.
- Die Netzwerkinfrastruktur kann den Zugriff automatisch nutzer- und desktopspezifisch einschränken. Dazu gehört auch, das Verhalten von Benutzern und Virtual Desktops in der Data Center Infrastruktur für Reports und Troubleshooting zu beobachten.
- Die Zuordnung von Benutzern zu VDs (Virtual Desktops) ist am Citrix XDDC (Desktop Delivery Controller) verfügbar.
- VMware VMView 4.5 unterstützt mit PCoIP (PC over IP) User Authentisierung. Im Rechenzentrum wird dazu 802.1x verwendet.
- Extreme Data Center Connect ermittelt VM-Daten und-Informationen über Remote User und stellt sie der Access Control zur Verfügung
- Extreme Access Control und die Multiuser Authentication identifizieren tausende Benutzer und weisen einzelnen physikalischen Ports individuelle Sicherheitsprofile zu

Extreme EXOS (Extreme Operation System)

Extreme Networks hat das modulare Betriebssystem Extreme EXOS für hochverfügbare, erweiterbare high-performance Netzwerke entwickelt. Seit 2003 hilft dieses Betriebssystem mit seiner Hochverfügbarkeitsarchitektur und Protokollen wie beispielsweise EAPS, Netzwerkausfälle - gerade in kritischen Umgebungen wie z.B CRM - zu verhindern.

Eingebaute Sicherheitsmechanismen beliefern Access Control mit Endpunktüberwachung, Identity Management und Schutz für die Netzwerk-Kontroll- und Management-Strukturen.

Mit EXOS lassen sich die Möglichkeiten des Netzwerkes durch die Integration von spezialisierten Appliances (Security, Application Intelligence) erweitern. Damit erreichen wir Transparenz und Kontrolle über das Netzwerk bis auf Applikations- und Userbene.

Architektur-Highlights

- Ein Betriebssystem für die gesamte Produktpalette
- Speicherschutz für Prozesse
- Selbstheilende Wiederherstellung von Prozessen durch Neustart oder hitless failover

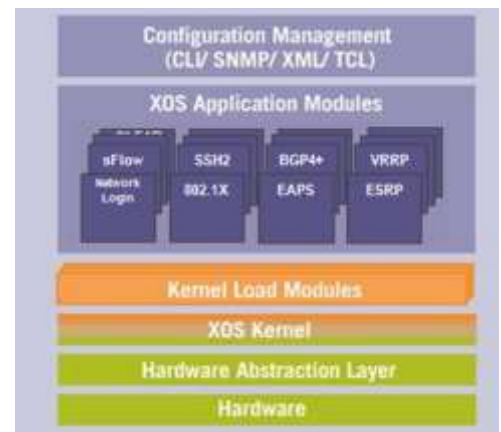
- Dynamisches Nachladen von neuen Funktionen
- Skriptingfähige CLI für Automation und event-gesteuerte Aktionen
- Offene XML APIs zur Integration von Fremdapplikationen
- Dual-stack IPv4 and IPv6 Unterstützung

Hochverfügbare Architektur

- Reduziert Netzwerkausfälle durch Hitless Failover und Software Updates auf Modulebene
- Verhindert Korrumpierung des Systems durch geschützte Speicherbereiche
- Verhindert System Reboots durch selbstheilende Prozesse
- Erweitert Hochverfügbarkeit über Switchgrenzen durch Multi-Switch Link Aggregation Groups
- Integriert Applikationen ins Netzwerk durch ein offenes und sicheres XML-basiertes Application Programming Interface (API)
- Integriert Extreme Networks und fremdentwickelte Applikationen durch ein standardbasierendes POSIX Interface
- Scripting-basierendes Gerätemanagement für einfaches und inkrementelles Ausrollen und Verwalten von Konfigurationen

Integrierte Security

- Kontrolliert den Netzwerkzugriff durch Authentifizierung (Network Login und 802.1x mit multiple User Authentication) sowie Hostkontrolle und Identity Management
- Härtet die Netzwerkinfrastruktur durch Denial-of-Service (DoS) Schutz und IP Security gegen man-in-the-middle und DoS Attacken
- Sicheres Management durch starke Verschlüsselung und Authentifizierung



Ein modulares Betriebssystem

Präemptives Multitasking und Speicherschutz ermöglichen es, dass viele Applikationen, wie beispielsweise Open Shortest Path First (OSPF) und Spanning Tree Protocol (STP), als eigenständige und separate Betriebssystemprozesse laufen, die voneinander geschützt sind. Dieses schafft eine höhere Systemintegrität und hilft, das System gegen DoS-Attacken zu schützen.

EXOS überwacht alle Prozesse und führt bei Bedarf einen Prozessneustart durch. Das modulare Design erlaubt es, falls notwendig, bei individuellen Softwaremodulen einen separaten Softwareupdate durchzuführen (s. Abbildung). Dies umfasst selbstverständlich auch securityrelevante Protokolle wie SSH und SSL.

Weitere Informationen

EXOS ist ein sehr komplexes Thema, schnell wäre damit der Rahmen des Solution Guides als Kompendium gesprengt.

Hier ein paar Tipps zum Stöbern im Netz:

- Das **EXOS Data Sheet** bietet eine übersichtliche Matrix über die einzelnen Features sowie die unterstützenden Hardwareplattformen:

www.extremenetworks.com/product/extremexos-network-operating-system

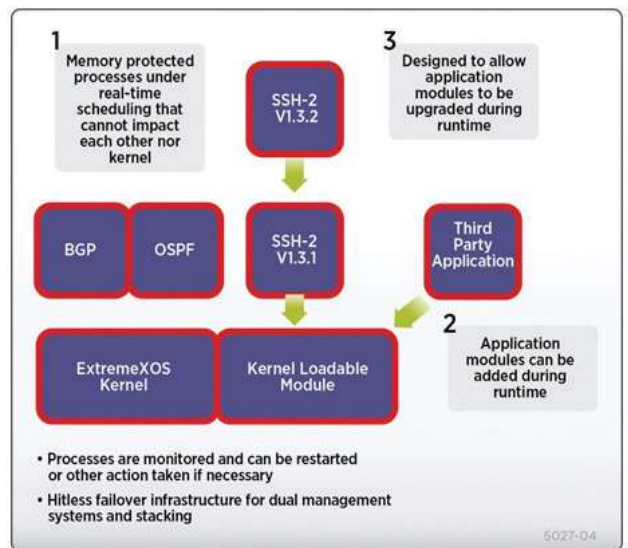
- Möchten Sie sich intensiv mit den Möglichkeiten von EXOS auseinandersetzen? Der aktuelle **User Guide** (Früher: Concepts Guide) erläutert Funktionen und Technologien anschaulich und mit Beispielen:

documentation.extremenetworks.com/exos/EXOS_All/Preface/c_introduction.shtml

Quality of Service in konvergenten Netzen

Die individuelle Kommunikation findet heute auf unterschiedlichste Art und Weise statt. Die technischen Voraussetzungen werden an allen Orten, zu jeder Zeit und immer in guter Qualität erwartet. Das sogenannte Internet der Dinge (Internet of Things, IoT) bringt außerdem eine hohe Anzahl neuer Clients in die Netze, mit jeweils sehr differenzierten Anforderungen an Übertragung, Verfügbarkeit und Sicherheit. Aktuelle LAN Infrastrukturen werden von verschiedensten Diensten und Applikationen genutzt und müssen kontinuierlich den Innovationsprozess eines Unternehmens unterstützen. Sie sind für den zukünftigen Erfolg mitentscheidend. Ziel ist es, dem Nutzer mehr Wissen am richtigen Ort zur richtigen Zeit zur Verfügung zu stellen. Über die digitale Infrastruktur erfolgt die Übertragung von multimedialen Daten. Oft ist dies in Echtzeit gewünscht oder soll mit nur sehr geringen Verzögerungen geschehen, und dies für unterschiedlichste Clients gleichzeitig. Man spricht deshalb auch gerne von einer Multiservice-Infrastruktur. Kann eine LAN Infrastruktur dies leisten, so spricht man von einer konvergenten Multiservice Infrastruktur.

Machen wir eine kurze Bestandaufnahme in aktuellen Installationen. Wir finden PCs, Tablets, Smartphones, Clients der Haustechnik, Telefone, Video- und Sicherheitssysteme vor. So unterschiedlich wie die Clients sind auch die Erwartungen



der genutzten Applikationen. Erwartet wird je nach Art der Applikation eine möglichst hohe oder eine möglichst gleichbleibende Bandbreite, andere wiederum eine sehr kurze Verzögerungszeit. Diese Clients sind wiederum mit einem sehr breiten Spektrum von unterschiedlich schnellen LAN Ports oder per WLAN an die Infrastruktur angeschlossen. Aktuell sind dies 10Mbit/Sek. z.B. für Geräte der Haustechnik und 100Gigabit/Sek. für Server und HPC´s. Auch das Nutzungsverhalten kann sehr unterschiedlich sein, denken Sie beispielsweise an Location Tags, die nur wenige Bytes innerhalb einer Stunde senden. Ein gegenteiliges Verhalten finden wir bei Sicherheitssystemen, wo von jeder Kamera aus ein permanenter Videostream an einen zentralen Server gesendet wird.

Die Hauptmotivation, eine QoS Strategie für die Infrastruktur zu entwickeln, liegt meist darin, jedem Endsystem den bestmöglichen Service zur Verfügung zu stellen und dabei mit vertretbaren Kosten ein Optimum an Effizienz und Kontrolle zu erzielen.

Was ist Quality of Service (QoS)?

QoS ist das Definieren von sogenannten Dienstqualitäten mit den Mitteln oder den Funktionen eines LANs in dessen Transportknoten. Dies können Bandbreiten (fix, variabel oder auch limitiert) oder auch Zeitverzögerungen sein, welche nicht überschritten werden dürfen. Zu diesen Mitteln und Funktionen zählt auch die sehr wichtige Möglichkeit, einzelne Datenpakete zwischenspeichern. Kann man Datenpakete für kurze Zeit speichern, so ergibt sich die Möglichkeit, einzelne zu priorisieren, zu verzögern oder nicht zu übertragen. Diese Speicher werden im Folgenden als Buffer beschrieben. Wie und in welcher Abfolge diese Speicher wieder geleert werden, nennt man Queuing. Auch die unterschiedlichen Queuing-Verfahren werden anschließend vorgestellt. QoS ist demnach das Optimieren der Verkehrscharakteristik eines Netzwerks.

Die Infrastrukturlösungen von Extreme Networks unterstützen den Betreiber mit den notwendigen Werkzeugen wie dem Policymanager (eine weiterführende Beschreibung des Policymanagers finden Sie im Abschnitt „ExtremeControl“).

Wie könnte eine mögliche Herangehensweise aussehen? Bestandsaufnahme und Bedarfsanalyse:

Applikationen

- Welche Applikationen sind im Besonderen zu berücksichtigen z. B.: VoIP?
- Was können die Applikationen signalisieren?
- Welche Applikation soll Vorrang haben, ist das ggf. entscheidend für den Unternehmenserfolg?

Zur Verfügung stehende Hardware:

- Bandbreiten und Links
- Uplinks

- Buffer
- Queues, Anzahl
- Queueing-Verfahren

Was sagt das Netzwerkmanagement?

- Kann das Netzwerkmanagement zu schon bestehenden Engpässen Informationen liefern?
- Welche Komponenten können welche Signalisierungen auf welchen Netzwerk-Layer auswerten?

Wo sind die neuralgischen Punkte in der Infrastruktur?

- Überlastungssituationen entstehen dort, wo sich Verkehrsströme treffen, beispielsweise am Netzwerk Switch oder an Übergängen in ein anderes Medium. Dies kann der Uplink Port zum nächsten Switch/Router oder auch der Übergang von einem kabelbasiertem Netz zu einem Wireless LAN sein.

Ansätze bei der Konzeptionierung

Man unterscheidet bei der Konzeptionierung zwei verschiedene Ansätze - den des statischen QoS und den des dynamischen QoS. Doch wo liegt der Unterschied?

Der statische Ansatz geht davon aus, dass man die genutzten QoS Parameter kennt und die Infrastruktur entsprechend statisch konfiguriert. Unbekannte oder nicht klassifizierte Daten landen im allgemeinen Übertragungspfad (FiFo). Dies gilt meist auch dann, wenn das Endsystem den Standort oder das IP Subnetz ändert. Zu kritischen Situationen kommt es regelmäßig, wenn beispielsweise zwei verschiedene Applikationen oder Endsysteme die selben Dienstparameter nutzen.

Ein dynamisches QoS geht einen etwas anderen Weg. Es stützt seine Transportentscheidungen dabei auf Daten, die eine intelligente Infrastruktur z.B. durch ein Identity & Access Management System (NAC) liefern können. Es wird nur für die Zeit der tatsächlichen Übertragung ein QoS-optimierter Pfad zwischen den beteiligten Endsystemen hergestellt. Danach werden die vorhandenen Ressourcen wieder freigegeben. Dazu aber mehr im Abschnitt „Dynamisches QoS in konvergenten und für Multiservice optimierte Netzen“.

Extreme Networks stellt beide Varianten für seine Kunden zur Verfügung (Ein Beispiel für ein dynamisches QoS Konzept finden Sie im Abschnitt Microsoft Lync Integration und im Abschnitt Datacentermanager).

Realisierungstipps

Entscheidend für den Erfolg der eingeleiteten Maßnahmen ist die genaue Erkennung und Unterscheidung des zu priorisierenden oder zu limitierenden Verkehrs durch die Infrastruktur. Kann eine Applikation signalisieren, welche Dienstqualitäten gewünscht werden, so müssen die Netzwerkkomponenten diese Informationen in ihre Transportentscheidungen mit einbeziehen. Kann dies eine Applikation nicht, so ist es an

der Infrastruktur, diesen Verkehr selbstständig zu markieren (Write/Rewrite). Erfolgreich kann diese Maßnahme nur sein, wenn diese Funktion möglichst nahe am ersten Eingangs-Port oder Access Point zur Verfügung steht. Hier gilt es auch zu prüfen, ob der gesamte Pfad innerhalb des LANs (Ende zu Ende QoS) in der Lage ist, Protokollinformationen auf dem Netzwerk Layer 3 und 4 zu erkennen. Passende Transportoptionen wie die Zuordnung zu den einzelnen Queues und das Gewichten der Buffer sind dann schnell konfiguriert.

Eine Signalisierung unterstützende Applikationen geben sich üblicherweise selbst die höchste Priorität, die größte Bandbreite und geringste Latenz. Dies passt meist nicht zum Gesamt-QoS-Konzept. Deshalb gilt es, wie oben schon erwähnt, deren Datenpakete von einer intelligenten Netzwerkkomponente schon am Eingang über die Rewrite Funktionen in die Spur zu bringen. An den neuralgischen Punkten eines LANs hängt es von der Qualität der gewählten LAN Komponenten ab, wie viele Pakete zwischengespeichert werden können (Buffer), welche Qualität dieser Speicher hat (in hochwertigen Komponenten werden TCAM Speicher eingesetzt) und wie man diesen Speicher verwalten und kontrollieren kann.

Führt ein Vergleich der gewünschten Dienstparameter mit dem aktuellen Status der Auslastung und der eigenen Konfiguration zu Abweichungen, können intelligente Switches und Router diese Parameter ändern (DCB Protokoll Framework) und dies auch dem Endsystem signalisieren. Das Extreme Networks Netzwerkmanagementsystem (Extreme Management Center) unterstützt die Administration bei Konfiguration und Kontrolle (Eine genaue Beschreibung finden Sie im Abschnitt Policymanager).

Ergebnisse einer QoS optimierten konvergenten Multiservice-Infrastruktur

QoS Funktionen stellen den Nutzer gesamtheitliche und garantierte Parameter für den Transport seiner Daten zur Verfügung. Konvergente Netze bieten somit ein hohes Maß an Skalierbarkeit bei geringen Kosten. Sie ermöglichen ein harmonisches Nebeneinander unterschiedlichster Anforderungen zum Wohle und Erfolg des Betreibers, des Unternehmens und der Organisation.

Standards und Funktionen

Extreme Networks hat schon immer darauf geachtet, bestehende Standards zu unterstützen und neue Standards voranzutreiben. Einige wichtige Standards werden im Folgenden beschrieben.

Quality of Service im Netzwerk

Um QoS in heutigen Netzwerken zu verwenden, müssen Dienst- und Service-Qualitätsklassen eingeführt werden. Durch intelligente Switches und Router, welche die entsprechenden Funktionen und Standards unterstützen, sind die Verzögerungszeiten innerhalb eines Netzwerks optimierbar. So erhalten z.B. Sprachpakete auf dem gesamten Übertragungspfad eine höhere Übermittlungspriorität als der tägliche Mail-Verkehr. Die Servicequalität eines Netzwerks wird als Kombination aus

Verzögerungszeit, Bandbreite und Zuverlässigkeit bewertet. Wichtig sind folgende Parameter:

Verzögerungszeit

- Ende-zu-Ende oder Hin- und Rückweg (Round-Trip-Verzögerung)
- Varianz der Verzögerungszeit (Jitter)
- Echtzeit-Möglichkeiten

Bandbreite

- Peak Data Rate (PDR) → Spitzenübertragungsrate
- Sustained Data Rate (SDR) → durchschnittliche Übertragungsrate
- Minimum Data Rate (MDR) → minimale Übertragungsrate

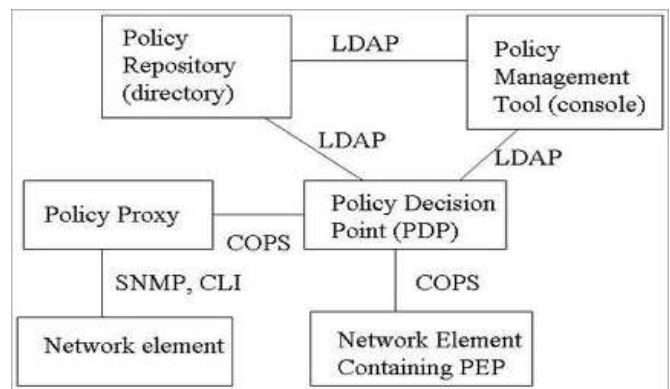
Zuverlässigkeit

- Uptime → Verfügbarkeit in Prozent
- Mean Time Between Failures / Mean Time To Repair (MTBF/MTTR) → mittlere fehlerfreie Laufzeit und mittlere Reparaturdauer
- Fehlerrate und Paketverlustrate

Entscheidend ist es, die im Beispiel genannten VoIP-Dienste zuverlässig bereitzustellen. Nur mit einem Ende-zu-Ende-Ansatz ist das möglich. Effektives Bandbreitenmanagement und eine definierte Servicequalität lassen sich mit IntServ- und DiffServfunktionen umsetzen.

Integrated Services (IntServ)

Die standardisierte Methode Integrated Services (IntServ) basiert auf der Reservierung bestimmter Ressourcen, etwa mit dem RSVP (Resource Reservation Protocol). Hierzu werden bestimmte Bandbreiten für einen Datenstrom (Flow) auf der gesamten Strecke reserviert. Jedes Element in der Übertragungskette muss RSVP verstehen und die Bandbreiten für die entsprechenden Flows reservieren. Weiterhin muss jeder Router diese Informationen dynamisch vorhalten und als sogenannte Soft States ablegen. Das kann bei vielen Flows sehr prozessorintensiv sein.



Die Zugriffskontrolle für die Netzwerkressourcen ist eine weitere Herausforderung. Für RSVP braucht man einen zentralen Policy Server. Schon 1999 entstand die IETF Policy Framework Working Group. Die Resource Admission Policy Working Group der IETF kümmerte sich um die Standardisierung von COPS (Common Open Policy Server). COPS arbeitet mit einer IntServ/RSVP (Integrated Services / Resource Reservation

Protocol)-Umgebung zusammen. Die Kommunikation zwischen PDP (Policy Decision Point) und PEP (Policy Enforcement Point) übermitteln RSVP-/RESV-Anfragen und lässt sie zu. Das Konzept skaliert jedoch wie RSVP leider nicht ausreichend für große Netzwerke, daher gibt es nur wenige COPS Implementierungen. Insgesamt hat sich der Integrated-Services-Ansatz nicht durchsetzen können. Stattdessen wird meist DiffServ verwendet.

Differentiated Services

Differentiated Services (DiffServ) setzen auf OSI-Layer 3 auf. Für DiffServ wird das ToS (Type of Service)-Feld im IP-Header genutzt. Im Gegensatz zu IntServ braucht DiffServ keine Ende-zu-Ende-Signalisierung der Datenflows. Die einzelnen Datenpakete werden zunächst klassifiziert und anschließend entsprechend ihrer Prioritäten über das Netzwerk transportiert. Damit ist es möglich, zwischen bestimmten Dienstklassen (Class of Service, CoS) innerhalb einer DiffServ-Domäne zu differenzieren, um den unterschiedlichen Anforderungen der verschiedenen Applikationen gerecht zu werden.



DSCP Differentiated Services Code Point
ECN Early Congestion Notification

Die Netzwerkkomponenten klassifizieren das Datenpaket und leiten es dann priorisiert weiter. Diese Form der Weiterleitung wird als Per-Hop Forwarding Behavior (PHB) bezeichnet. PHB beschreibt generell die Zuteilung bestimmter Bandbreiten- und Speicherressourcen, sowie die angeforderten Verkehrscharakteristika wie Verzögerungszeit oder Paketverluste. Damit ist eine Differenzierung in verschiedene Dienstklassen möglich.

Als Unterscheidungsmerkmal zwischen den verschiedenen PHB-Weiterleitungsklassen dient der DiffServ Codepoint (DSCP). Er besteht aus den ersten sechs Bit im IPv4-ToS-Feld. In RFC 2474 wurde das ToS-Feld im IPv4-Header in DS (DiffServ)-Feld umbenannt. Damit sind maximal 64 Prioritätsklassen möglich.

Zurzeit sind folgende DSCP-Werte zur Verwendung in LANs definiert:

DSCP dez.	DSCP binär	DSCP hex.	ToS dez.	ToS binär	ToS hex.	Serviceklassen (CoS)
0	000000	0x00	0	00000000	0x00	Best effort
8	001000	0x08	32	00100000	0x20	Class 1
10	001010	0x0a	40	00101000	0x28	Class 1, gold (AF11)
12	001100	0x0c	48	00110000	0x30	Class 1, silver (AF12)
14	001110	0x0e	56	00111000	0x38	Class 1, bronze (AF13)
16	010000	0x10	64	01000000	0x40	Class 2
18	010010	0x12	72	01001000	0x48	Class 2, gold (AF21)
20	010100	0x14	80	01010000	0x50	Class 2, silver (AF22)

22	010110	0x16	88	01011000	0x58	Class 2, bronze (AF23)
24	011000	0x18	96	01100000	0x60	Class 3
26	011010	0x1a	104	01101000	0x68	Class 3, gold (AF31)
28	011100	0x1c	112	01110000	0x70	Class 3, silver (AF32)
30	011110	0x1e	120	01111000	0x78	Class 3, bronze (AF33)
32	100000	0x20	128	10000000	0x80	Class 4
34	100010	0x22	136	10001000	0x88	Class 4, gold (AF41)
36	100100	0x24	144	10010000	0x90	Class 4, silver (AF42)
38	100110	0x26	152	10011000	0x98	Class 4, bronze (AF43)
40	101000	0x28	160	10100000	0xa0	Express forwarding
46	101110	0x2e	184	10111000	0xb8	Expedited forwarding (EF)
48	110000	0x30	192	11000000	0xc0	Control
56	111000	0x38	224	11100000	0xe0	Control

Die Default Klasse ist für nicht speziell klassifizierten Traffic und entspricht damit der IP Precedence 0.

Per Hop Behaviour (PHB)	Diffserv Code Point (DSCP)				IP Precedence
Default	000000				0
Assured Forwarding		Low Drop Probability	Medium Drop Probability	High Drop Probability	
	Class 1	AF11 001010	AF12 001100	AF13 001110	1
	Class 2	AF21 010010	AF22 010100	AF23 010110	2
	Class 3	AF31 011010	AF32 011100	AF33 011110	3
	Class 4	AF41 100010	AF42 100100	AF43 100110	4
Expedited Forwarding	EF101110				5

Die Class Selector (CS) Code Points sind rückwärtskompatibel zu anderen IP-Precedence-Werten.

Expedited Forwarding (EF, RFC 2598) stellt als Klasse geringe Latenzzeiten, wenig Jitter, möglichst keinen Paketverlust und garantierte Bandbreite zur Verfügung.

Assured Forwarding (AF, RFC 2597) hat viele Klassen, um den Datenverkehr zu differenzieren und das PHB mit verschiedenen Paketverlustwahrscheinlichkeiten zu definieren.

Explicit Congestion Notification (ECN)

Die Grundidee hinter der Explicit Congestion Notification ist, dass eine ECN unterstützende Netzwerkkomponente bei Überlastung im Netzwerk Pakete nicht verwirft, sondern stattdessen weiterleitet.

Die Bits 6 und 7 des DSCP-Feldes bilden das sogenannte ECN-Feld (spezifiziert in RFC 3168). Es realisiert Flusskontrolle im IP-Protokoll, wie man sie beispielsweise im WAN-Protokoll Frame Relay mit FECN- und BECN-Bits (Forward/Backward Explicit Congestion Notification) kennt.

Die ECN-Bits sind folgendermaßen definiert:

- Bit 6: ECN-Capable Transport (ECT) Bit
- Bit 7: Congestion Experienced (CE) Bit

Dabei wurde beschlossen, dass nicht nur der binäre Wert 10 (als Kombination von Bit 6 und Bit 7), sondern auch die Kombination 01 ausdrückt, dass ECN unterstützt wird. Es ergibt sich also folgende Bedeutung:

ECT BIT	CE BIT	Bedeutung
0	0	Not-ECT (Not ECN-Capable Transport)
0	1	ECT(1) (ECN-Capable Transport - 1)
1	0	ECT(0) (ECN-Capable Transport - 0)
1	1	CE (Congestion Experienced)

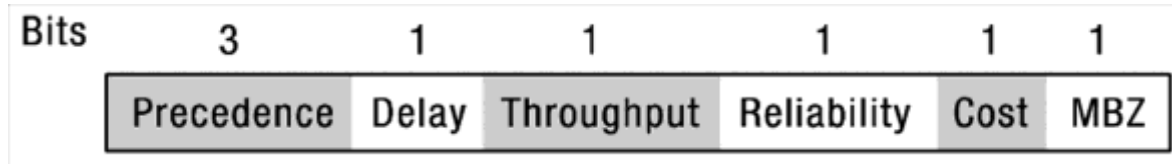
Leitet nun ein Gerät bei Überlastung einzelner Verbindungen Pakete weiter, werden diese mit dem CE Wert markiert, sofern sie schon vorher als ECT gekennzeichnet sind. Diese Information wird an den TCP-Stack weitergegeben, der daraufhin die Fenstergröße in seinem Acknowledge-Paket heruntersetzt. Das veranlasst den Sender, die versandte Datenmenge zu reduzieren.

Zwar ist dieses Konzept gut, dennoch scheint es fraglich, ob es in absehbarer Zeit im Internet genutzt wird. Denn wer auf seinem Rechner bei Überlastung einzelner Links ECN einschaltet und so sein eigenes Datenvolumen reduziert, macht nur mehr Platz für andere, die ECN nicht nutzen. Deren Pakete haben dann freie Fahrt.

Ganz anders ist die Situation in einem Firmennetz, wo man mit regelbasierten Policies durchsetzen kann, dass alle Teilnehmer ECN nutzen. Dort garantiert ECN bei Engpässen eine vernünftige Flusskontrolle.

IP Precedence

Das ToS (Type of Service)-Feld im IPv4 Header ist zwar mittlerweile als DS Feld für die DSCP-Werte umdefiniert, die IP-Precedence Bits in ihrer herkömmlichen Bedeutung werden aber immer noch oft als Alternative zu DSCP genutzt. Die ursprüngliche Definition des ToS-Felds (Länge: 1 Byte = 8 Bits) sieht folgendermaßen aus:



TOS Feld

Mit den drei IP Precedence-Bits kann man dem IP-Paket einen Prioritätswert zwischen 0 und 7 zuweisen:

- 000 (0) - Routine
- 001 (1) - Priority
- 010 (2) - Immediate
- 011 (3) - Flash
- 100 (4) - Flash Override
- 101 (5) - Critical
- 110 (6) - Internetwork Control
- 111 (7) - Network Control

Die beiden höchsten Prioritäten sind für Netzwerk-Traffic reserviert. So schicken zum Beispiel Routingprotokolle ihre Nachrichten meist mit der IP Precedence 6 (Internetwork Control). Verzögerungssensitive Daten wie Sprache werden im Allgemeinen mit der IP-Precedence 5 versandt. Während der Standardwert für normale Daten die IP Precedence 0 ist, kann man mit den verbleibenden Werten von 1-4 den Datenverkehr weiter differenzieren und priorisieren.

Die weiteren Bits des ToS-Feldes könnten über die Latenz, den Durchsatz, die angestrebte Zuverlässigkeit und Kosteninformationen informieren. Das letzte Bit ist noch ungenutzt und musste deswegen auf 0 gesetzt werden (MBZ, Must Be Zero). Routingprotokolle wie OSPF unterstützen zwar laut Definition die Auswertung der ToS-Bits, allerdings gibt es keine Implementierungen, die dies auch wirklich tun.

Bei der Wahl der bisher definierten DSCP-Werte hat man Wert auf Rückwärtskompatibilität gelegt. So wird zum Beispiel VoIP-Traffic mit Expedited Forwarding EF = 101110 versandt, die ersten drei Bits entsprechen also dem IP Precedence Wert 5.

Betrachtet man andere Lösungen für die Festlegung der Servicequalität wie beispielsweise IEEE 802.1p für Ethernet oder die Experimental Bits für MPLS (Multiprotocol Label Switching), finden sich auch hier drei Bits für die Darstellung von Prioritäten. Nutzt man diese QoS-Verfahren, so werden im Allgemeinen die drei IP-Precedence-Bits in die entsprechenden Felder für IEEE 802.1p oder MPLS kopiert.

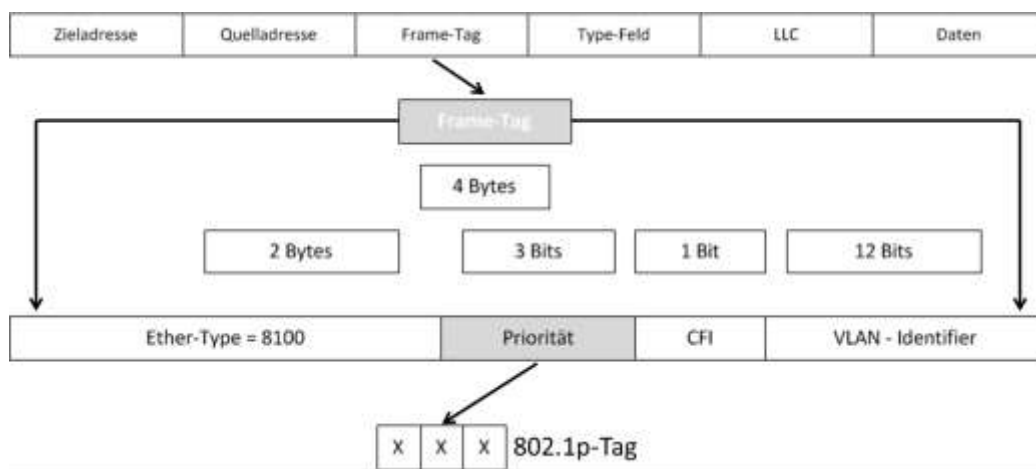
Die Servicequalität mit IP-Precedence-Werten zu definieren ist demnach trotz der neueren Technik mit DSCP-Werten noch aktuell und wird es in absehbarer Zeit auch bleiben. Die Produkte von Extreme Networks Networks unterstützen beide Varianten.

Priorisierung nach IEEE 802.1p

Der Standard IEEE 802.1p ist ein weiterer Ansatz zur Verbesserung der Servicequalität. 802.1p veranlasst, dass bestimmte Datenpakete auf dem Netzwerk priorisiert übertragen werden. Man versieht Datenpakete mit einer Markierung, die entsprechend dem Ende-zu-Ende-Ansatz von jedem Knoten des Übertragungspfades erkannt und entsprechend der Konfiguration für diese Markierung übertragen werden.

Beispiele für diesen Ansatz sind IEEE 802.1p und Differentiated Service (DiffServ).

IEEE 802.1p erweitert IEEE 802.1d:



Ein Markierungssegment (Tag) wird in das Datenpaket eingeschoben. Es ist zwei Byte lang und ermöglicht die Prioritätenvergabe durch drei Bits (entsprechend acht Prioritätsklassen) und die Bildung von Virtuellen LANs (VLANs) nach IEEE 802.1q, was der Priorisierung von Daten auch auf Layer 2 entspricht.

Queuing-Verfahren

Mit DSCP, IP Precedence und IEEE 802.1p lassen sich den Paketen durch Markierungen bestimmte Servicequalitäten zuweisen. Damit der gewählte Service tatsächlich ablaufen kann, braucht man dedizierte Verfahren zum Aufbau und zur Abarbeitung von Warteschlangen (Queuing-Verfahren). Extreme Networks Geräte unterstützen verschiedene Queuing-Methoden wie Strict, Hybrid oder Weighted Round Robin. Dabei existieren für jeden Port mehrere, in Hardware realisierte Queues.

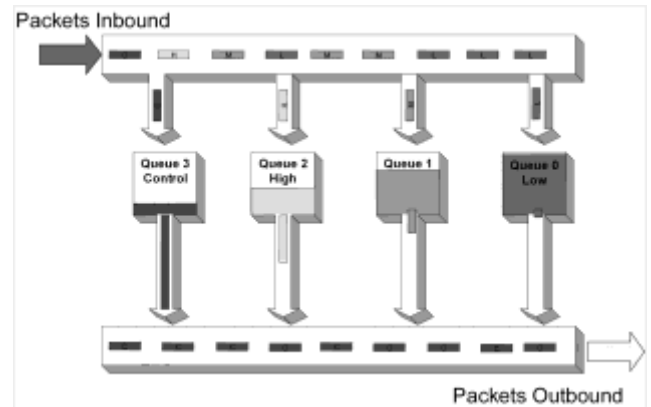
Fifo Queuing

Am einfachsten ist das Fifo (First in, first out)-Queuing: Die Pakete werden in der Reihenfolge auf einen Ausgangsport weitergeleitet, in der sie am Netzwerkknoten empfangen wurden. Dieses Verfahren ist als Vorgabe auf allen Ports aktiv geschaltet und gilt auch für alle Subqueues bei den komplexeren Queuing-Methoden.

Strict Priority Queuing

Beim streng prioritätsgesteuerten (Strict Priority) Queuing werden den verschiedenen Subqueues Prioritäten zugeordnet und diese anschließend streng entsprechend dieser Priorität abgearbeitet. Solange in den Queues der höchsten Priorität Pakete auf Weiterleitung warten, werden diese weitergeleitet. Erst wenn diese Queues geleert sind, wird die Queue mit der nächstniedrigeren Priorität bearbeitet.

So verlassen die Pakete mit der höchsten Priorität das Gerät mit minimaler Verzögerung. Daher wird Strict Priority Queuing gerne für VoIP-Pakete genutzt. Allerdings muss man bei Planung der Priorisierung und Klassifizierung der Pakete sehr vorsichtig sein. Werden zu viele Pakete unangebracht hoch priorisiert, werden Datenströme der unteren Prioritätsklassen nicht mehr weitergeleitet, da die höher eingestuften Pakete die vorhandenen Kapazitäten vollständig verbrauchen.



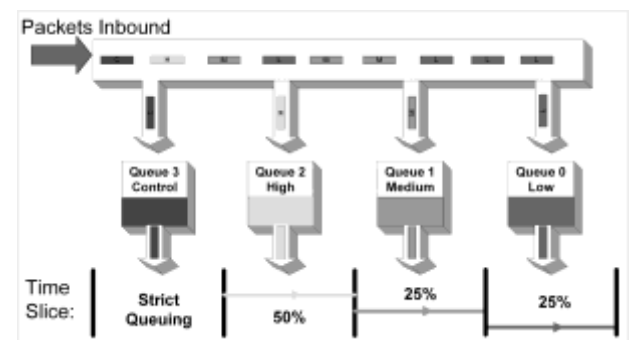
Weighted Round Robin Queuing

Beim Weighted-Round-Robin-Queuing werden die verschiedenen Queues abwechselnd bedient. Um den Traffic unterschiedlich gewichten zu können, erhält jede Queue einen bestimmten Prozentsatz der vorhandenen Kapazität, also ein „Gewicht“ (Weight). Durch eine höhere Gewichtung (einen höheren Prozentsatz) bekommen Pakete der zugehörigen Queue einen besseren Service. Gleichzeitig ist eine gewisse Bandbreite für jede Queue gewährleistet.

Hybrid Queuing

Hybrid Queuing ist eine Mischung von Priority- und Weighted-Round-Robin-Queuing. Es vereinigt Vorteile beider Verfahren. Dabei wird einem Weighted-Round-Robin-Queuing eine Priority-Queue vorgelagert. Letztere wird im Allgemeinen für VoIP-Pakete oder vergleichbaren zeitsensiblen Traffic genutzt.

Da die entsprechenden Pakete normalerweise wenig Bandbreite benötigen, ist die Gefahr einer Vernachlässigung des übrigen Traffics gering. VoIP Pakete werden aber bevorzugt behandelt, um kurze Latenzzeiten zu garantieren. Der übrige Traffic erhält gemäß dem Weighted-Round-Robin-Verfahren die ihm zugestandene Bandbreite.



Rate Limiting und Rate Shaping

Manchmal ist es auch nötig, die von bestimmten Verkehrsarten genutzte Bandbreite zu begrenzen. Dies ist durch strikte Bandbreitenbegrenzung (Rate Limiting) oder das weniger strikte Rate Shaping möglich. Rate Limiting lässt sich für ankommende

(Inbound Rate Limiting) oder ausgehende (Outbound Rate Limiting) Pakete festlegen. Dabei werden die Pakete, die die konfigurierte Rate überschreiten, verworfen. Beim Rate Shaping versucht man den Bandbreitenverbrauch innerhalb der vorgegebenen Rate zu halten, indem Pakete zwischengespeichert werden. Das Verfahren ist daher nur für ausgehenden Traffic sinnvoll.

QoS für Wireless Clients

Wireless Clients unterstützen meist die QoS Parametrierung auf Protokoll-Ebene. Diese entfalten ihre Wirkung aber erst im Access Point und müssen vom Treiber und der Wireless Adapterkarte unterstützt werden. Für diese Luftschnittstelle müssen andere Verfahren eine qualifizierte Übertragung sicherstellen. Hierbei können Funktionen wie Airtime Fairness, Band Steering und Client Load Balancing sehr hilfreich sein.

Airtime Fairness

Airtime Fairness ist eine Besonderheit der ExtremeWireless Lösung. Die garantierte - und in den meisten Fällen auch notwendige Abwärtskompatibilität eines WiFi Netzes - zwingt bei gemischter Nutzung gerade schnelle Clients zu langen Wartezeiten, bis die Übertragung von langsamen 802.11b kompatiblen Clients abgeschlossen ist. Dies wird dadurch verursacht, dass, dem Standard folgend, jeder Client eine bestimmte Anzahl von Paketen senden darf, sobald ihm der Access Point das Senderecht eingeräumt hat.

ExtremeWireless geht einen anderen Weg. Es räumt unter Aufrechterhaltung der Kompatibilität jedem Client ein Zeitfenster ein. Ein 802.11n Client kann damit deutlich mehr Durchsatz erzielen als ein 802.11b Client.

Airtime Fairness wird von allen aktuellen Access Points unterstützt und bedarf dabei keiner Anpassung der WiFi Clients.

Band Steering

Alle aktuellen ExtremeWireless Access Points unterstützen 2 Frequenzbänder gleichzeitig. Daraus ergibt sich die Chance, Clients gleichmäßig auf beiden Frequenzbändern zu verteilen. Grundsätzlich verbinden sich WiFi Clients erst einmal über das 2,4 Ghz Frequenzband mit dem Access Point. Signalisiert ein Client jedoch, dass er in beiden Frequenzbändern arbeiten kann, so obliegt es nun dem Access Point, den Client über das 5Ghz Frequenzband zu verbinden. Hierbei ist keine Unterstützung durch Treiber oder Funktionen der Adapterkarten notwendig. Da die mögliche Distanz zwischen WiFi Client und Access Point im 5 Ghz Band etwas geringer ist, ist eine Anpassung der Access Point Dichte sinnvoll.

Client Load Balancing

Neben einer automatischen Verteilung auf beide Frequenzbänder bietet ExtremeWireless weitere sinnvolle Funktionen zur Optimierung an. Beim Client Load Balancing kümmert sich eine ganze Gruppe von Access Points um die Clients. Es wird eine Gruppe von Access Points definiert, welche gemeinsam eine HF-Zone versorgt. Die Load Balancing Gruppe verteilt alle Clients gleichmäßig auf die Access Points. Andernfalls würde sich ein Client immer zu dem AP verbinden, den er mit dem besten

Pegel empfängt. Dieses qualitativ sehr oberflächliche Verhalten des Clients berücksichtigt nicht die Auslastung des Access Points und dessen Verbindungsverhältnisse. Stark genutzt wird diese Funktion z.B. in Veranstaltungs- und Konferenzhallen und dort, wo die Clientdichte sehr hoch ist oder sein kann.

Wireless Rate Limiting

In den meisten Anwendungsfällen ist eine hohe Bandbreite sehr gewünscht. Es gibt aber auch Anwendungsfälle, denken wir einmal an Hotel- und Freizeitanlagen, wo der allermeiste Verkehr über die Internetanbindung zum Ziel transportiert werden muss. Hier führen die im Verhältnis zur Internetanbindung sehr hohen Bandbreiten der Wireless Lösung regelmäßig zu Überlastungssituationen am Knotenpunkt zum Internet. Da es kaum Einflussmöglichkeiten auf das Verhalten der Clients oder deren Konfiguration gibt, bietet sich hier eine strikte Reglementierung der Bandbreite in beiden Richtungen (Rate Limits) an.

ExtremeWireless hinterlegt in Profilen, wie z.B. „Gast“, mit welcher Bandbreite die Nutzung erfolgen darf. Dabei wird nicht in die HF-Eigenschaften eingegriffen und der Empfang bleibt stabil und sicher.

Für Hotels ist das Bereitstellen von IT-Infrastrukturen für deren Gäste mittlerweile überlebenswichtig, da diese das Erreichen privater und öffentlichen Clouds in guter Qualität als Standard ansehen.

Extreme Networks hat schon immer darauf geachtet, internationale Standards zu unterstützen und an neuen Standards mitzuentwickeln. Das Ziel dabei ist immer, die beste Lösung für den Kunden zu bieten.

Zusammenfassung

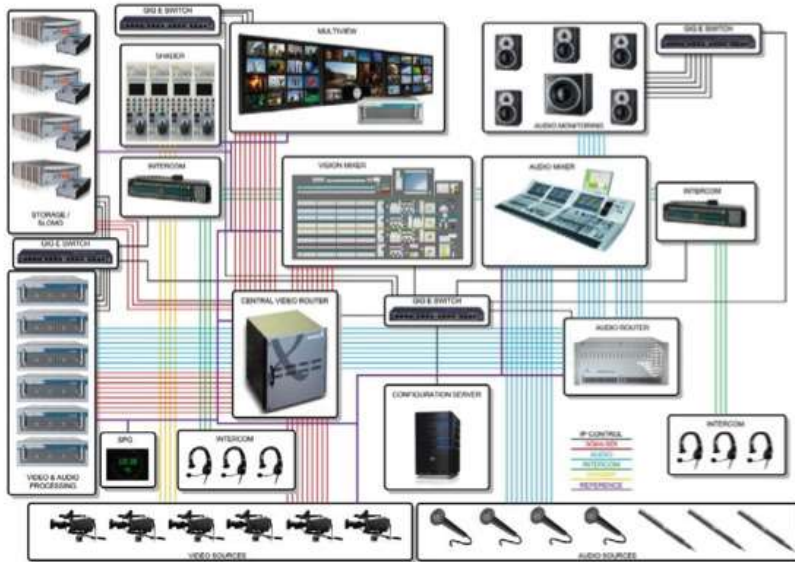
Das Ziel moderner Multiservice-Netze ist es, einer Vielzahl von Applikationen mit höchst unterschiedlichen Anforderungen zuverlässige Übertragungsmöglichkeiten zur Verfügung zu stellen. Extreme Networks kombiniert intelligente Hardware mit hochentwickelten Managementlösungen. Die Extreme Networks Architektur ermöglicht es den Kunden, ihre konvergente Infrastruktur mit minimalem zeitlichen Aufwand und geringen Kosten zu betreiben.

Weitergehende Informationen zum Thema QoS auf Extreme Networks-Komponenten finden Sie unter *Features Guides*:

<https://extranet.extremenetworks.com/downloads/Pages/S.aspx>

Audio-Video-Bridging (AVB)

AVB wurde entwickelt, um das Ethernet für den Einsatz in professionellen Audio- und Video-Umgebungen zu ertüchtigen. Dabei ist dieser Standard nicht wirklich neu. Die IEEE hat AVB bzw. die dazu gehörenden Standards bereits seit März 2011 abschliessend ratifiziert. Dennoch war AVB bis vor kurzem nur wenigen Marktbeobachtern ein Begriff, da es noch keine Produkte gab, die AVB unterstützen.

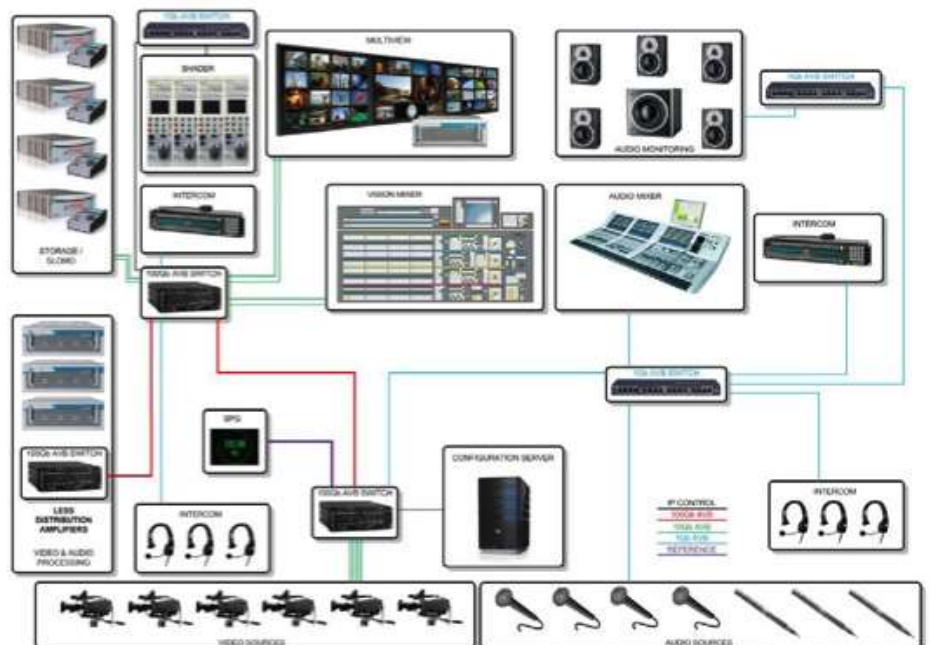


Die Motivation hinter AVB ist, proprietäre, analoge und digitale Verfahren zur Signalübertragung in professionellen Umgebungen durch standardisierte Ethernet Verbindungen zu ersetzen. Das hört sich zunächst nicht besonders spannend an. Tatsächlich jedoch bringt es dem Betreiber einer solchen Lösung enorme Vorteile. Zunächst einmal lässt sich die Verkabelung von z.B. Aufnahmestudios dramatisch vereinfachen. Bisher war für jedes Signal ein dediziertes Kabel vonnöten. Das führte dazu, dass beispielsweise in Konzerthallen enorme Kabelmengen von der Bühne in ein angeschlossenes Aufnahmestudio führen mussten. Diese Verkabelung ist sehr komplex in der Planung, erzeugt hohe Kosten in der Installation, stellt eine enorme Brandlast dar und ist komplett unflexibel. Durch AVB ist es nun möglich, die gesamten Signale auf der Bühne lokal zu bündeln und über eine simple Glasfaserverbindung zum Studio zu übertragen.

Der zweite grosse Vorteil von AVB liegt in der Standardisierung der Übertragung. Wo bisher Signalumsetzer und Konverter benötigt wurden, können über einen einheitlichen Übertragungsstandard Geräte unterschiedlicher Hersteller problemlos miteinander verknüpft werden.

Die Motivation hinter AVB ist, proprietäre, analoge und digitale Verfahren zur Signalübertragung in professionellen Umgebungen durch standardisierte Ethernet Verbindungen zu ersetzen. Das hört sich zunächst nicht besonders spannend an. Tatsächlich jedoch bringt es dem Betreiber einer solchen Lösung enorme Vorteile. Zunächst einmal lässt sich die Verkabelung von z.B.

Aufnahmestudios dramatisch



Zwar gab es auch vor AVB schon Möglichkeiten der digitalen Signalübertragung. Die dazu eingesetzten Verfahren (z.B.: CobraNet oder Dante) sind jedoch rein proprietär und skalieren nicht ausreichend. Somit fallen zum einen Lizenzgebühren an und die Anzahl der zu übertragenden Audiokanäle ist auf 64 (CobraNet) oder 1024 (Dante) beschränkt. AVB kann nun von den Skalierungsstufen des Ethernet profitieren, so dass Übertragungsbandbreiten von bis zu 100 Gbit/s und mehrere tausend Kanäle kein Problem darstellen.

Was ist nun das Neue an AVB? Audio- und Videoübertragungen via Ethernet sind ja nicht wirklich neu. Spätestens seit VoIP und Youtube gehören sie zum Alltag. Allerdings war das klassische Ethernet bisher nicht in der Lage, eine Dienstgüte zu bieten, die den Anforderungen von professionellen Umgebungen gerecht wurde.

Das erste Problem des klassischen Ethernet ist die fehlende Zeitsynchronisierung. Wenn z.B. in einem Stadion die Lautsprecher für Durchsagen ihr Signal via Ethernet erhalten, gibt es keine Möglichkeit zu garantieren, dass alle Lautsprecher das Signal der Quelle auch gleichzeitig erhalten. Ethernet ist nicht deterministisch. Bei AVB werden die beteiligten Endgeräte zeitlich synchronisiert. Insofern haben alle Lautsprecher und die Quelle eine identische Systemzeit. Die vom Standard erlaubte Abweichung liegt hier bei unter 1µs. Die Gesamtverzögerung in einem AVB Netz wird mit 2ms über maximal sieben Hops vorgegeben. Insofern kann die Quelle die Pakete mit einer „Presentation Time“ versehen, die den Zeitpunkt des Signalausgangs vorgibt und somit für eine synchrone Wiedergabe durch alle Lautsprecher sorgt.

Das zweite Problem liegt in der Realisierung von Quality of Service (QoS) im klassischen Ethernet. Die besteht in der Regel aus einer reinen Priorisierung von Paketen. Für eine professionelle Audio- oder Videoübertragung ist dies unter Umständen nicht ausreichend. Dort braucht es eine echte Reservierung von Bandbreite, die dem jeweiligen Signal exklusiv über den gesamten Link zur Verfügung stehen muss. Dafür gab es bisher keinen Standard.

Diese beiden Probleme werden durch AVB gelöst. Im einzelnen werden folgende Standards definiert:

- IEEE 802.1BA: Audio Video Bridging, ist der übergeordnete Standard für AVB
- IEEE 802.1AS: Timing und Synchronisierung von zeitsensitiven Applikationen sorgt für die zeitliche Synchronisierung aller beteiligten Endgeräte mit Hilfe des Generalised Precision Time Protocol (gPTP)
- IEEE 802.1Qat: Stream Reservation Protocol (SRP) / Multiple Stream Reservation Protocol (MSRP), sorgt für die dedizierte Reservierung von Bandbreite
- IEEE 802.1Qav: Forwarding and Queueing von zeitsensitiven Streams (FQTSS), sorgt für das entsprechende QoS
- Zusätzlich gibt es noch eine Erweiterung im IEEE 802.1Q: Multiple Registration Protocol (MRP) / Multiple VLAN Registration Protocol (MVRP), welche dafür sorgt, dass VLAN Informationen über den gesamten Link automatisch signalisiert und konfiguriert werden können.

Die beschriebenen Standards lösen zum einen die Probleme der Zeitsynchronisierung und Bandbreitenreservierung, und zum anderen sorgen sie dafür, dass AVB Umgebungen nahezu selbstkonfigurierend sind. Dies war ein weiteres Ziel bei der Entwicklung des Standards, der vor allem mobilen und oft wechselnden Umgebungen Rechnung trägt. AVB sollte möglichst Plug-and-Play sein.

Die Einsatzszenarien für AVB sind enorm vielfältig. Zunächst gibt es die klassischen Audio-Umgebungen wie Konzertsäle, Aufnahmestudios, Mehrzweckhallen, Kongresszentren, Freizeitparks, Stadien, Schulen, Universitäten usw.

Darüber hinaus gibt es aber auch geplante Einsatzszenarien die deutlich weiter führen. So ist z.B. die Automobilindustrie sehr an AVB interessiert. Die heutigen Bus-Systeme in Fahrzeugen sind ebenfalls proprietär und nicht besonders skalierend. Hier bietet sich Ethernet mit AVB als Möglichkeit zur Steigerung des Funktionsumfanges und für das Bordentertainment an.

Ebenso ist die Flugzeugindustrie an AVB interessiert. Die heutigen In-Seat-Entertainment-Systeme benötigen für jeden Fluggast drei dedizierte Kabel (Video, Audio, Steuerung). Wenn man diese durch ein einziges Ethernet Kabel mit AVB ersetzen kann, ergibt sich auch hier eine Möglichkeit zur Gewichtsreduktion.

Aber auch in ganz klassischen Datennetzen könnte AVB für bestimmte Applikationen durchaus von Interesse sein. Und die Entwicklung ist hier noch nicht an ihrem Ende angelangt.

Getrieben wird der AVB Standard von der AVnu Alliance, einem Industrieforum unterschiedlichster Hersteller aus den Bereichen Audio, Video, Chipherstellung, Automobil, Netzwerk (www.avnu.org). Prominente Beispiele sind Harman, Sennheiser, Yamaha, Biamp, Riedel, Bosch, Broadcom, Marvel, General Motors, Extreme Networks und Cisco Systems.

Die Mitglieder dieser Allianz haben es sich zur Aufgabe gemacht, die Weiterentwicklung von professioneller Audio- und Video-Übertragung über Ethernet in verschiedenen Layern zu betreiben. Stand heute ist der AVB Standard nur für reine Layer 2 Umgebungen vorgesehen. Die Erweiterung auf geroutete Layer 3 Umgebungen ist derzeit noch in der Entwicklung. Diese Einschränkung kommt jedoch in den meisten Anwendungsfällen nicht zum Tragen, da es sich normalerweise um dedizierte Insellösungen handelt.

Nichtsdestoweniger bietet AVB jedoch den zusätzlichen Vorteil einer Konvergenz von klassischen Datendiensten und professionellen Audio-/Video-Streams auf demselben Netz. Per Default sieht der Standard eine Reservierung von 75% der Linkkapazität für AVB Verkehr vor. Dies lässt sich jedoch per Konfiguration verändern.

Die verfügbare Produktlandschaft von AVB fähigen Lösungen ist derzeit noch recht überschaubar. Allerdings haben etliche Hersteller bereits Prototypen vorgestellt und es gibt auch schon einige verfügbare Lösungen.

Erste produktive Umgebungen wurden auch bereits installiert, derzeit hauptsächlich in Audio-Umgebungen. Das liegt zum einen daran, dass es deutlich mehr Audio- als Video-Umgebungen gibt. Zum anderen sind die heute verfügbaren Bandbreiten für hoch auflösende unkomprimierte Video-Signale noch zu niedrig ausgelegt. Wir reden hier über 6-8 Gbit/s pro Signal, so dass hier schon auf 10 Gbit/s Interfaces zurück gegriffen werden muss. Mit der baldigen Einführung von 100 Gbit/s und entsprechender Unterstützung von Kanalbündelung, kann AVB dann auch im professionellen Video-Umfeld die Anforderungen erfüllen.

Extreme Networks unterstützt AVB derzeit auf den Geräten der Serien X430, X440, X440-G2, X450-G2, X460, X460-G2, X670, X670-G2 und X770.

IP Version 6

Das Internet hat sich in den vergangenen Jahren aus einem reinen Datennetzwerk zu einer Multi-Service-Plattform entwickelt. Dies bringt auch neuartige Kommunikationsbeziehungen mit sich, zum Beispiel Peer-to-Peer (P2P)-Vernetzung für Multimedia-Übertragungen oder die Datenversendung über mobile, kabellose Netze.

Der Adressraum des klassischen Internetprotokolls (IPv4) ist höchst unterschiedlich verteilt. So besitzt etwa das Massachusetts Institute of Technology (MIT) in Cambridge/USA ein Netz, in dem sich mit rund 16 Millionen Rechnern mehr Adressen ansprechen lassen als in ganz China. Doch im Web sind gerade einmal 90.000 vom MIT verwendete Adressen zu identifizieren. Zudem steigt die Zahl der Endgeräte exponentiell, so dass der begrenzte Adressraum von IPv4 nicht mehr ausreicht, alle zu versorgen. Obwohl dieser Umstand bereits in den neunziger Jahren erkannt wurde (1992 bildete die IETF eine erste Working-Group) und der erste IPv6 RFC (RFC 1883) bereits 1996 erschien, hat es noch viele Jahre gedauert, bis die ersten Unternehmen und Konzerne über den Einsatz von IPv6 nachdachten.

IPv6 nutzt 128-Bit-Adressen und bietet damit einen viermal so großen Adressraum wie IPv4. Das bedeutet, dass IPv6 unvorstellbare 665.570.793.348.866.943.898.599 Adressen pro Quadratmeter Erdoberfläche bereitstellt. IPv6 dürfte daher in Zukunft die alte Protokollbasis IPv4 in immer mehr Netzen ersetzen. Durch IPv6 lassen sich ganz neue, flexiblere Strukturen zur Verbindung der Knotenpunkte untereinander realisieren. Mit IPv4 werden auch Network Address Translation (NAT) und CIDR (Classless Inter Domain Routing) verschwinden.

Zusätzlich ist wie bei jeder anderen Technologie auch die Sicherheitsfrage zu beantworten. Während IPv4 ursprünglich nur zum einfachen Datenaustausch entwickelt wurde, besitzt IPv6 von Anfang an Sicherheitsfunktionen.

Erweiterter Adressraum im IPv6-Datagrammformat

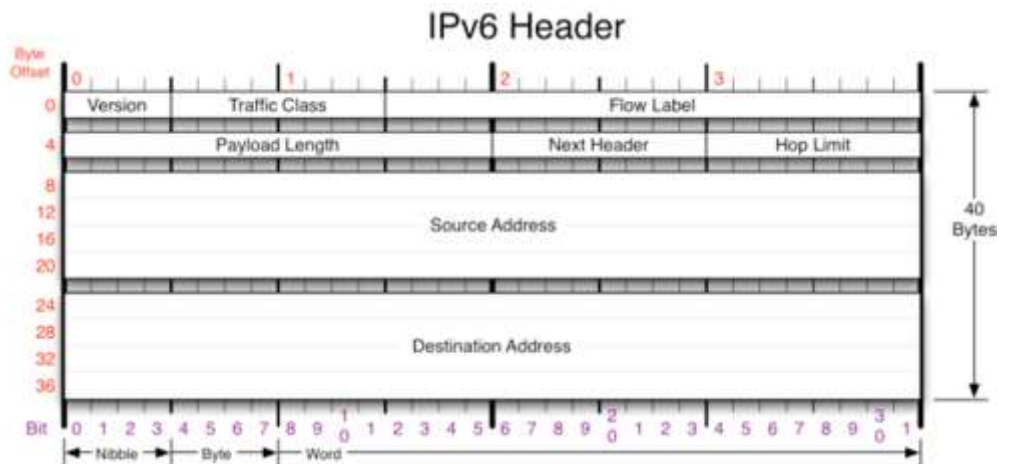
Prinzipiell besteht ein IPv6-Datagramm aus dem Basis-Header, gefolgt von optionalen Zusatzheadern und den Nutzdaten. Dieses „bereinigte“ Header Konzept sorgt für optimierte Routingtabellen und einen besseren Support für Optionen und Erweiterungen.

Besondere Unterschiede zu IPv4 sind:

- Keine Broadcasts
- Kein ARP/RARP
- Kein NAT
- Eingebautes IPSec
- Autokonfiguration/Rekonfiguration OHNE DHCP
- Keine Fragmentierung im Netz (wenn überhaupt dann nur im Source-Host)

IPv6 Basis Header

Der IPv6-Basis-Header ist doppelt so groß wie der IPv4-Header, enthält aber weniger Felder als dieser. Die Adressgröße für die Quell- und Zieladresse wurde von bisher 32 auf nunmehr 128 Bit erweitert.



Erweiterungsheader

Die wichtigste Neuerung von IPv6 besteht in der Möglichkeit, den Basis Header um weitere Header zu erweitern. Diese sollen eine effiziente Datenübertragung und Protokollerweiterungen ermöglichen. Der Basis-Header enthält nur Felder, die unbedingt für die Übermittlung eines Datagramms notwendig sind. Erfordert die Übertragung weitere Optionen, können diese im Erweiterungsheader angegeben werden. Einige IPv6-Merkmale des Protokolls werden nur gezielt eingesetzt, etwa die Fragmentierung von Datagrammen. Im IPv4-Basisheader sind Fragmentierungsfelder vorhanden, obwohl viele IPv4-Datagramme nicht fragmentiert werden müssen. IPv6 gliedert diese in einen Erweiterungsheader aus, der nur dann verwendet wird, wenn das Datagramm fragmentiert werden muss. Dies ist bei IPv6 höchst selten, da hier in der Regel mittels Path MTU (Maximum Transmission Unit) Discovery (RFC 1981) die maximale Paketgröße via ICMPv6 (Internet Control Message Protocol) ausgehandelt wird. Daher sollte IPv6-Fragmentierung nur genutzt werden, wenn Anwendungen ihre Paketgrößen nicht individuell anpassen können.

Vorteilhaft ist, dass Erweiterungsheader neue Funktionen in das Protokoll integrieren. Es genügt, für das Feld „Next Header“ einen neuen Typ und ein neues Header-Format zu definieren. Bei IPv4 müsste hierzu der Header vollständig geändert werden. Derzeit sind sechs optionale Erweiterungsheader definiert. Werden mehrere Erweiterungsheader verwendet, sind sie in einer festen Reihenfolge anzugeben.

IPv6-Erweiterungsheader nach RFC 2460, 2402 und 2406:

Header	Beschreibung
IPv6 & Basis Header	Zwingend erforderlicher IPv6 Basis Header
Optionen für Teilstrecken (Hop-by-Hop Options Header)	Verschiedene Informationen für Router
Optionen für Ziele (Destination Options Header)	Zusätzliche Informationen für das Ziel
Routing (Routing Header)	Definition einer vollständigen oder teilweisen Route
Fragmentierung (Fragment Header)	Verwaltung von Datengrammfragmenten
Authentifizierung (Authentication Header)	Echtzeitsüberprüfung des Senders
Verschlüsselte Sicherheitsdaten (Encapsulating Security Payload Header)	Informationen über den verschlüsselten Inhalt
Optionen für Ziele (Destination Options Header)	Zusätzliche Informationen für das Ziel (für Optionen, die nur vom endgültigen Ziel des Pakets verarbeitet werden müssen)
Header der höheren Schichten (Upper Layer Header)	Header der höheren Protokollschichten (TCP, UDP,...)

In Bezug auf die Sicherheit sind zwei Erweiterungsheader interessant, die für Datenintegrität sorgen:

- **Authentisierung:** Mit Hilfe des Authentication Headers lässt sich die Echtheit eines Paketes prüfen. Er garantiert auch, dass Daten bei der Übertragung unverändert bleiben. Eine Sequenznummer schützt den Empfänger eines Pakets vor Angriffen durch wiederholtes Senden desselben Pakets. Der Authentication Header (AH) liefert dabei dieselbe Sicherheit wie IPv4 zusammen mit IPSec. Bei der Authentisierung unterscheidet man zwei Verfahren: den Transport- und den Tunnelmodus.
- **Verschlüsselte Sicherheitsdaten:** Der ESP (Encapsulating Security Payload)-Header verschlüsselt vertrauliche Daten und garantiert ihre Unversehrtheit. Außerdem schützt ESP wirksam vor sogenannten Data-Replay-Attacks. Wie bei der Authentisierung unterscheidet man bei der Verschlüsselung zwischen Transport- und Tunnelmodus.

Der Transportmodus wird bei der Kommunikation zwischen zwei Rechnern verwendet. Normalerweise kennen sich die Rechner hier nicht oder besitzen keine gültigen Schlüssel für eine Verbindung. Daher müssen beide Rechner bei einem Trust Center

einen One-Session-Key anfordern, der nur für eine begrenzte Zeit gilt. Der IP-Header selbst bleibt beim Transportmodus unverschlüsselt. Deshalb besteht die Gefahr, dass Hacker Informationen darüber erhalten können, wohin ein Rechner Verbindungen aufbaut und wann er wie viele Daten sendet.

Um zwei Firmennetze über öffentliche Leitungen zu verbinden, bietet sich daher der Tunnelmodus an. Hier ist von außen ausschließlich sichtbar, dass die beiden Router kommunizieren, darüber hinaus aber keine weiteren Informationen.

Wird bei einer kompletten Übertragung der Authentifizierungs-Header genutzt, können IPv6-fähige Firewalls sogar die höheren Schichten im Datenpaket überprüfen und somit Pakete sperren oder freischalten.

ICMPv6

ICMPv6 gehört zur IPv6 Protocol Suite. Es dient zur Autokonfiguration unter IPv6. Hier erhalten die Clients automatisch eine IPv6-Adresse.

Auch die Entdeckung benachbarter Stationen läuft über einen bestimmten ICMPv6-Nachrichtentyp. Viele Firewalls filtern allerdings die ICMP-Messages oder blocken sie komplett.

Unter IPv6 müssen aber bestimmte Nachrichtentypen unbedingt zugelassen werden. Daher ist es nötig, bei der Implementierung von IPv6 den Firewalls erhöhte Aufmerksamkeit zu widmen.

Der Autodiscovery Mechanismus ermöglicht es, ohne ARP oder RARP Nachbarschaftsbeziehungen aufzubauen. Dazu werden im ICMPv6 fünf Pakettyten genutzt (s. Abbildung)

Zudem dürfen keine unerlaubten ICMP-Messages vom Zugangspunkt zur Infrastruktur geschickt werden. DHCP- und DNS-Server stecken im Inneren des Netzes und sind meistens bekannt. Daher können diese Pakettyten am Zugangspunkt ausgefiltert werden.

IPv6 Routing und andere Funktionen

Genau wie im IPv4 werden auch im IPv6 Routingprotokolle zur Wegefindung genutzt. Dabei wurden die klassischen Protokolle in Richtung IPv6 erweitert und angepasst. So gibt es ein RIPng/RIP IPv6 (RFC 2080), OSPFv3 (RFC 2740) oder BGP+ (MP-iBGP).

DHCP und DNS sind IPv4 Funktionen, die auch im IPv6 Umfeld die Administration wesentlich erleichtern. Allerdings mussten auch diese Protokolle erweitert werden. DHCPv6 (RFC 3315) verarbeitet IPv6 Adressen und der DNS Dienst muss im IPv6 statt mit A-Records nun mit AAAA-Records umgehen können.

Multicastverkehr im IPv4 wird u.a. über IGMPv3 geregelt. Im IPv6 übernimmt dies das MLDv2 Protokoll (Multicast Listener Discovery).

Type	Message
133	Router Solicitation (RA)
134	Router Advertisement (RA)
135	Neighbor Solicitation (NS)
136	Neighbor Advertisement (NA)
137	Redirect

ICMPv6 Pakettyten

IPv4/IPv6 Übergang

Netze, die noch nicht auf IPv6 umgerüstet wurden, sind Angriffen aus dem Internet stark ausgesetzt, da alle aktuellen Computersysteme bereits mit dem IPv6 Stack ausgeliefert werden. Einige Systeme können nicht einmal mehr rein auf IPv4 arbeiten sondern nutzen den IPv6 Stack im IPv4 Modus. Da der Wechsel von IPv4 zu IPv6 ein langsamer Prozess ist, sind für eine Kommunikation zwischen oder über IPv4 oder IPv6 Tunnel- oder Übersetzungsmechanismen notwendig. Hier die wichtigsten Methoden:

- 4in6/6in4 (Encapsulierung/Tunnel)
- 6to4/6rd (IPv6 Transport über IPv4)
- AYIYA (Anything in Anything)
- Teredo (UDP Encapsulierung, Tunnel)
- DSTM (Dual Stack Transition Mechanism, Übersetzung)
- Carrier Grade NAT (CGN) und Dual Stack Lite (Übersetzung)

Besonders der sogenannte Teredo-Tunnel von Microsoft stellt ein großes Sicherheitsproblem dar. Diese Form eines IPv6 Tunnels funktioniert sogar über NAT Instanzen hinweg. Generell sollte in einem IPv4 Netz jeglicher IPv6 Verkehr an der Firewall unterbunden werden. Dazu muss die Firewall natürlich IPv6 unterstützen.

Der beste Migrationsweg führt über den Dual Stack Ansatz, der den parallelen Gebrauch beider Stacks erlaubt.

IP bleibt IP

IPv6 und IPv4 sind reine Transportprotokolle. Angriffe auf höheren Ebenen, beispielsweise Buffer Overflow oder Angriffe auf Web-Applikationen, sind bei beiden IP-Varianten möglich. Daher braucht man unbedingt zusätzliche Sicherheitsmaßnahmen wie IKE (Internet Key Exchange) aus der IPSec-Protokollsuite oder IEEE 802.1x. Damit lassen sich Attacken wie Flooding (Überflutung mit großen Verkehrsmengen, um einen Zusammenbruch der empfangenden Infrastruktur auszulösen) und Man-in-the-Middle (hier schleicht sich der Angreifer unerkannt in die Kommunikation zwischen zwei Partnern ein, hört mit oder greift selbst ins Kommunikationsgeschehen ein) verhindern und im Netz befindliche, nicht zugelassene Geräte (Rogue Devices) erkennen und entfernen.

SNMP (Simple Network Management Protocol)

SNMP ist das Standard-Netzwerkmanagementprotokoll, um die Konfiguration und Leistungsinformationen entfernter Netzwerkkomponenten auszulesen. SNMPv1 wurde 1988 veröffentlicht und wird noch heute von den meisten am Markt erhältlichen Netzwerkmanagementsystemen verwendet.

Ursprünglich wurde SNMPv1 vor allem entwickelt, um die Ressourcen der Rechner zu schonen. Daher verwendete SNMP zunächst einen reduzierten

Authentifizierungsmechanismus zur Sicherung der Kommunikation: ein einfaches

Klartextpasswort, den Community-String. Ergänzend verwendet man auch heute noch oft auf IP-Adressen basierende Zugangslisten, um den Zugriff für SNMPv1 zu regeln. Da SNMP auf dem verbindungslosen UDP (User Datagram Protocol) aufbaut, ist dies ebenfalls eine Sicherheitslücke: Weil man keinen Handshake für den Aufbau der Verbindung braucht, muss die Absenderadresse des IP-Pakets nicht stimmen.

Mit SNMPv2 wurden einige neue Methoden in das Protokoll integriert, auch die Sicherheitsproblematik lässt sich durch mehrere Ansätze in den Griff bekommen. Allerdings hat sich bisher keiner von ihnen durchgesetzt. Weil die sichere Kommunikation zwischen Managementstation und Netzwerkkomponenten immer wichtiger wird, bietet die aktuelle Version des Protokolls - SNMPv3 - Authentifizierung, Verschlüsselung und Zugriffskontrolle und damit ein komplettes Portfolio von Sicherheitsfunktionen.

SNMPv3 (RFC 2571-2575) definiert verschiedene Sicherheitsmodelle. VACM (View Based Access Control Model) ergänzt die nutzerbasierte Zugriffskontrolle durch die Definition von Views. Die Nutzer erhalten dadurch nur Zugriff auf Teilbereiche der MIB (Management Information Base). Sämtliche Geräte von Extreme Networks und alle Komponenten der Extreme Networks NMS Suite unterstützen SNMPv3.

Scripting

Scripting unterscheidet sich von Batch-Programmierung und Programmierung vor allem dadurch, dass es im Gegensatz zur Batchprogrammierung über gehobene Kontrollfunktionen oder objektorientierte Eigenschaften wie Vererbung verfügt. Als Abgrenzung zu Programmen ist vor allem zu sehen, dass Skripte in einer Interpreterumgebung ausgeführt werden und nicht kompiliert werden müssen. Extreme Networks Switches mit dem Betriebssystem EXOS sind in der Lage, CLI basierte Skripte auszuführen.

CLI basierte Skripte erlauben es, eine Liste von Kommandos zu erstellen, die man manuell mit einem Befehl ausführen kann. Alternativ lassen sich Skripte auch durch das Eintreffen eines bestimmten Events ausführen. Zudem unterstützen CLI basierte Skripte Variablen und Funktionen, so dass man Skripte erstellen kann, die unmodifiziert auf einer Vielzahl von Switchen ausgeführt werden können. Dies vereinfacht das Management der Switches ungemein.

Beispiele für die Anwendungen von Skripten sind unter anderem:

- Automatische Konfigsicherung auf entferntem Managementsystem
- Konfigurationsänderungen, die einen Disconnect erfordern
- Automatischer Healthcheck auf Coresystemen
- Ping basierendes Gatewayfailover

Um ein Skript zu starten, stehen viele Möglichkeiten zur Verfügung:

- Manueller Start auf der Kommandozeile

- Timer basierender Start
- Start basierend auf Ereignissen im Eventlog (z. B.. Port Up)
- Start basierend auf LLDP Events
- Start basierend auf Ereignissen im Zusammenhang mit User Authentifizierung

Besondere Scripts lassen sich im Switch hinterlegen, die entweder beim ersten Start (default.xsf) oder bei jedem Start (autoexec.xsf) ausgeführt werden. Hiermit lassen sich beispielsweise automatische Softwareupdates bei erster Inbetriebnahme von Vorhaltegeräten durchführen. Andere Einsatzzwecke sind das vereinfachte Ausrollen von Geräten in größeren Umgebungen (Initialdialog) oder das Zurückrollen von komplexen Änderungen nach einem Ausfall.

Neben TCL (www.tcl.tk/), welches durch Extreme Networks EXOS seit Version 11.6 unterstützt wird, unterstützt EXOS seit Version 15.5.2 auch die Scriptsprache Python (<https://pypi.python.org/pypi/pexpect/>).

Universal Port

Das Betriebssystem EXOS unterstützt seit der Version 12.0 die Möglichkeit, das Verhalten eines Extreme Switches dynamisch an bestimmte Netzwerkänderungen oder Ereignisse anzupassen. Diese Script Funktion wird im EXOS „Universal Port“ genannt.

Dabei kann das Stecken oder Abziehen eines Netzkabels ein Ereignis sein, auf das der Switch - von einem Universal Port Script gesteuert - reagiert. Das Erreichen eines Schwellwertes, die Erkennung eines VoIP-Telefons, ein User Logon oder Logoff, eine bestimmte Tageszeit oder ein Eintrag im Logfile sind Ereignisse, auf die ein Switch ebenfalls per Universal Port Script reagieren kann.

Ein solches Script wird im EXOS Universal Port Profile genannt (UP Profile). UP Profile führen CLI Kommandos aus und können Variablen benutzen. Der wesentliche Unterschied zu herkömmlichen Scripts ist, dass UP Profile auf Ereignisse reagieren. UP Profile sind Bestandteil einer Switch-Konfiguration.

Zur Erstellung eines solchen Profiles kann der im EXOS eingebaute VI Editor genutzt werden. Allerdings erfreut sich dieser rudimentäre Editor keiner großen Beliebtheit, so dass die meisten Administratoren einen komfortablen grafischen Editor am PC bevorzugen dürften. Das erstellte Profil kann dann per TFTP in den Switch geladen und in die Konfigurationsdatei eingebunden werden.

Pro Switch können bis zu 128 UP Profile erstellt und genutzt werden. Jedes Profil hat eine maximale Größe von 5000 Zeichen.

Praktische Beispiele für den Einsatz von UP Profilen sind:

- Automatische Portkonfiguration in Abhängigkeit vom angeschlossenen Endgerät z.B. einem VoIP-Telefon. Der Port kann in das entsprechende VLAN mit den

passenden QoS Werten geschaltet und mit der korrekten PoE Leistung versorgt werden.

- Security Einstellungen können in Abhängigkeit vom angeschlossenen Gerät bzw. angemeldeten User angepasst werden.
- Ports können zeitgesteuert ein- bzw. ausgeschaltet werden, z. B. nach Büroschluß. PoE gespeiste Ports schalten Ethernet-schaltbare Steckdosenleisten an oder ab.
- Profiltemplates können durch Nutzung von Variablen an unterschiedliche Anforderungen angepasst werden.

UP Profile können entweder statisch oder dynamisch arbeiten. Statische UP Profile entsprechen von ihrer Funktion her einem klassischen Script. Sie werden manuell aufgerufen. Damit läßt sich ein Switch z.B. in einen definierten Zustand schalten.

Dynamische UP Profile liegen im Speicher und werden in Abhängigkeit von Ereignissen abgearbeitet.

Der Befehl **#run upm profile <profile-name> {event <event-name>} {variables <variable-string>}** führt ein dynamisches Profil aus.

Sollen Konfigurationsänderungen, die durch ein UP Profil erzeugt wurden, wieder rückgängig gemacht werden (Rollback), muss ein zweites Profil genutzt oder der Switch gebootet werden, da ein UP Profil per Default im sogenannten Non-Persistent Mode arbeitet. Konfigurationsänderungen durch ein UP Profil werden dabei bei einem Reboot gelöscht und der Switch startet mit der Konfiguration, die vor der Abarbeitung des Profiles gültig war.

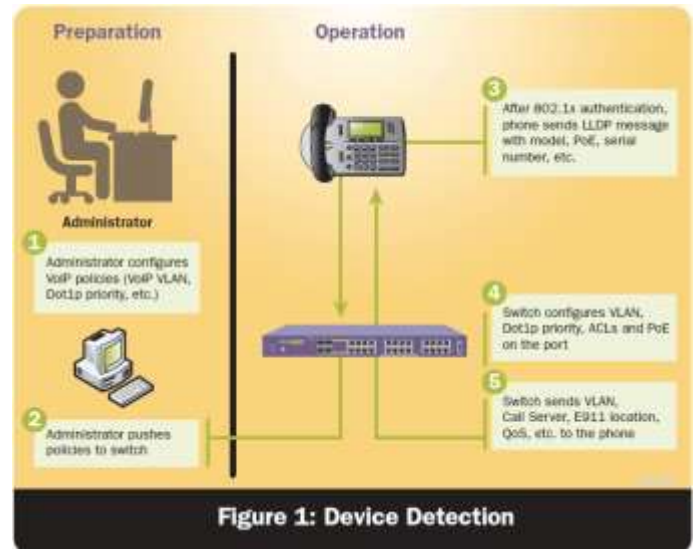
Sollen Konfigurationsänderungen durch ein UP Profil auch nach einem Reboot gültig bleiben und somit dauerhafter Bestandteil der Konfiguration sein, muss die Scriptengine in den Persistent Mode geschaltet werden.

Generell wird zwischen vier Event Trigger bei dynamischen UP Profilen unterschieden:

- Device
- User Authentication (IDAM)
- Time
- Event-Management System

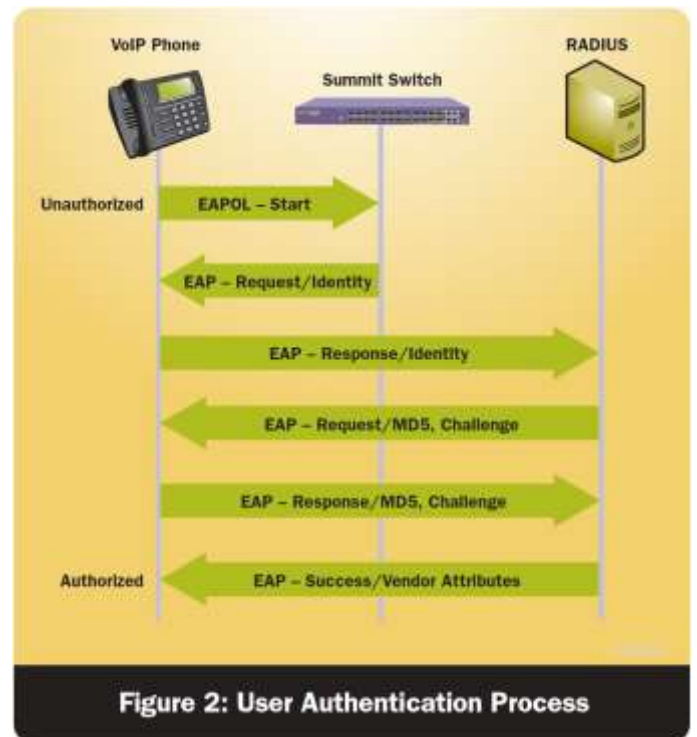
Device Trigger

Dieser Trigger greift immer dann, wenn an einem physikalischen Switchport das Stecken oder Ziehen einer aktiven Verbindung erkannt wird. Zur Erkennung eines solchen Events kann z. B. auf LLDP (IEEE 802.1ab) und LLDP-MED zurückgegriffen werden. Eine weitere Möglichkeit ist das Auswerten neuer Einträge in der Log-Datei. Bei jedem Stecken oder Ziehen einer aktiven Verbindung wird ein entsprechender Eintrag in diese Datei geschrieben. Auf diesen Eintrag kann ein UP Profil reagieren.



User Authentication Trigger

Wenn ein Nutzer oder das entsprechende Endgerät per Network Login erkannt wird, kann dies die Ausführung eines UP Profiles auslösen. Zur Nutzung dieser Funktion ist in der Regel ein RADIUS Server mit entsprechender User und/oder Geräte Datenbank notwendig. Bei kleinen Netzen oder im Filialbetrieb kann auch eine lokale Datenbank im Switch angelegt werden (statisch). Durch die Verwendung von VSAs im RADIUS (Vendor Specific Attributes) kann ein Switch in Abhängigkeit der Nutzer/Geräte Information unterschiedlich konfiguriert werden.



Es gibt drei Network Login Methoden, die den Trigger auslösen können:

- 802.1X
- MAC basiert
- Web basiert

802.1X kann immer dann genutzt werden, wenn das Endgerät mit einer 802.1X Client-Software ausgerüstet werden kann. Ein kleiner Nachteil dabei ist, dass nicht alle Endgeräte 802.1X tauglich sind. Für solche Geräte kann dann der MAC-basierte Trigger genutzt werden, der allerdings keine Informationen über den Nutzer auswerten kann und wegen manipulierbarer MAC Adressen nur eine geringe Sicherheit bietet. Web-basiertes Login liefert über DHCP und optionalen DNS Nutzerinformationen, die als Trigger für UP Profile genutzt werden können.

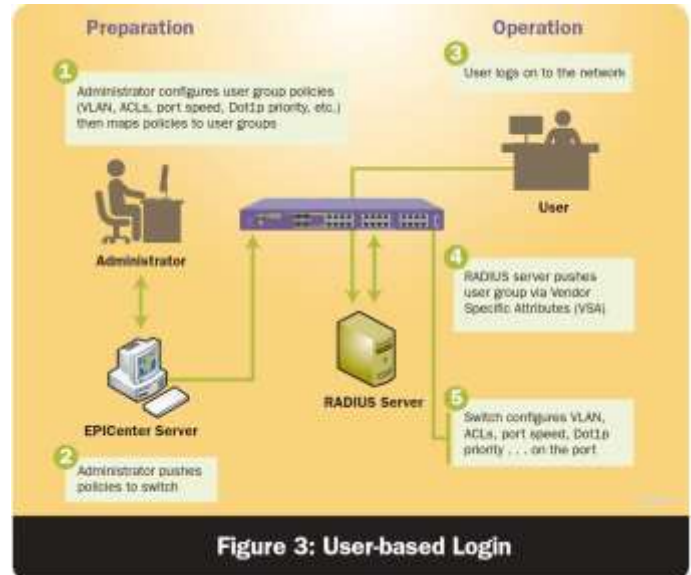


Figure 3: User-based Login

Time Trigger

Der zeitgesteuerte Trigger ist für alle Anwendungen geeignet, die ein zeitlich wiederkehrendes Ereignis nutzen. So kann ein modularer Switch zu einer gegebenen Zeit I/O Module runterfahren bzw. abschalten, um Energie zu sparen oder die Sicherheit im Netz zu steigern. Zu einer zweiten gegebenen Zeit werden die Module dann wieder aktiviert.

```
Create upm profile <profileName>
Create upm timer <timerName>
Configure upm timer <timerName> profile <profileName>
Configure upm timer <timerName> every 3600
```

Figure 4: Example of Periodic Configuration

Ein Zeit-Trigger kann aber auch unabhängig von der aktuellen Uhrzeit in Intervallen (periodisch) ein UP Profil auslösen, z .B. jede Stunde oder alle zwei Tage. Damit können z. B. automatische Konfigurationsbackups erstellt werden.

Ein UP Profil kann aber auch einmalig nach Ablauf einer bestimmten Zeit abgearbeitet werden.

Event-Management System Trigger

Dieser Trigger ist der mächtigste Trigger im EXOS, da hiermit auf fast beliebige Events im Switch reagiert werden kann. Die Nutzung dieses Triggers ist allerdings nur erfahrenen Administratoren empfohlen, da man mit dieser Funktion den Switch ausser Gefecht setzen kann. Richtig angewendet sind aber Szenarien möglich, die sonst nur mit zusätzlicher Hardware oder Software möglich wären.

Um UP Profile nutzen zu können, muss Scripting im EXOS Switch eingeschaltet werden (**#enable cli scripting**).

Die besondere Stärke von UP Profilen ist die Möglichkeit zur Nutzung von Variablen. Damit lassen sich Profile erstellen, die in Abhängigkeit des Variablenwertes unterschiedliche Ergebnisse liefern.

Ein Beispiel dafür wäre das Erkennen eines Nutzers mit seinem Endgerät an einem Port, der z. B. viel Bandbreite belegt (HD Streaming) während ein iSCSI Storage den gleichen Link benötigt. Durch Abfrage der Variablen „Nutzer“, „Port“, „Bandbreite“ kann ein UP Profil entsprechende Porteinstellungen vornehmen, um dem Storage den Vorrang zu geben (höhere QoS Queue).

Es wird unter drei Gruppen von Variablen unterschieden:

- Common Variables (für alle Profile gültig)
Bsp.: `$CLI.USER` = Name des aktuellen CLI Nutzers
- Device Detect Variables (nur für Profile zur Geräteerkennung)
Bsp.: `$EVENT.DEVICE_MAC` = MAC Adresse des angeschlossenen Endgerätes
- User Authentication Variables (nur für Profile zur Nutzererkennung)
Bsp.: `$EVENT.USERNAME` = Name des authentifizierten Nutzers

Identity & Access Control

Mit Access Control bietet Extreme Networks eine BYOD Lösung für durchgängige Sicherheit und volle Kontrolle durch die IT Abteilung, bei bester „Quality of Experience“ für die Endanwender. Extreme Access Control ist die Antwort auf die heutigen Herausforderungen zu Mobility in Enterprise- und Campus-Netzwerken, und bietet Ende-zu-Ende Transparenz und Kontrolle über einzelne Anwender, Geräte und Applikationen, und das in vollem Umfang herstellerübergreifend.

Die Lösung ist aus der Sicht der Administratoren komplett in das Management Center integriert und bietet mit Extreme Connect als Northbound API zusätzliche Erweiterungen und Integrationen.

Bring Your Own Device (BYOD)

Ständig kommen neue mobile Geräte auf den Markt. Ihre Preise fallen, ihre Prozessorleistung steigt und sie konkurrieren bereits mit modernen Laptops und PCs. Die neuen Mobilsysteme erhöhen Flexibilität und Produktivität. Kritische Applikationen und Daten liegen sozusagen „auf der Hand“ - weltweit und jederzeit zugänglich. Viele sehen darin einen Wendepunkt in der Geschichte der traditionellen IT. In jedem Fall bedeutet die explosionsartige Verbreitung dieser Geräte erhebliche Herausforderungen bei der sicheren Verwaltung des Unternehmensnetzes. Derzeit hinkt die Unternehmens-IT diesen Trends hinterher. Denn jedes mobile Gerät bedeutet ein neues Sicherheitsrisiko für das Unternehmensnetz.

Administratoren kennen die Risiken traditioneller Endsysteme wie Laptops und Desktops. Diese Geräte können nur selten eine separate Datenverbindung herstellen, die etablierte physikalische Netzwerkkontrollen und Policies aushebelt. Androids, iPhones, Windows Mobile Devices, Blackberries und verschiedene Tablets allerdings, die im Zug des BYOD (Bring Your Own Device)-Trends in die Unternehmensnetze einziehen, haben unter Umständen gleichzeitig 3G- oder WiFi-Verbindungen zu ungesicherten Netzwerken wie dem Internet und zu Unternehmensnetzen.

Ohne eine agentenbasierte Mobile Device Management (MDM)-Lösung erfährt der Administrator kaum Details zum mobilen Gerät und seinem Verhalten im Netz. Er weiß weder, ob es „gesund“ noch wie sicher es ist. Doch selbst MDM-Produkte sind keine perfekte Lösung. Denn viele MDM-Lösungen erkennen nicht, wie ein Gerät und der darauf geladene MDM-Agent mit dem Managementsystem kommunizieren, sie wissen also beispielsweise nicht, wo das Gerät ans Netz angebunden ist, ob also beispielsweise ein Telefon direkt am Unternehmensnetz hängt oder nicht. Vielmehr befassen sie sich vor allem mit dem offenen Kanal zwischen dem Managementsystem und dem betreffenden Gerät.

Außerdem verwalten MDM-Lösungen nur Geräte, auf die ein Softwareagent geladen wurde - andere auch dann nicht, wenn sie sich mit dem Netz verbinden wie in BYOD (Bring Your Own Device)-Umgebungen üblich: Bei BYOD gewähren Organisationen den mobilen Geräte ihrer Mitarbeiter oder von Dritten Zugriff auf das Firmennetz. Das ist eine ernste Herausforderung für Netzwerksicherheit, Anwendungen und Daten.

Die ganzheitliche Herangehensweise von Extreme Access Control bewältigt diese Herausforderung. Das System erkennt, authentifiziert und bewertet die Sicherheit individueller Mobilsysteme ganz oder teilweise durch die Integration mit bestimmten MDM-Lösungen.

Auf Basis der Bewertung werden den Geräten unabhängig von der Mobilstrategie des Anwenderunternehmens intelligente Policies zugewiesen.

Die Identity and Access Control-Funktionen im Detail:

- **Mobile Device Identification:** Identifizierung von mobilen Geräten, so dass gerätespezifische Richtlinien entwickelt und zugewiesen werden können. Administratoren in Organisationen, die ein BYOD-Konzept umsetzen, identifizieren so mit oder ohne MDM-Lösung schneller unbekannte oder verbotene Geräte und können gerätespezifische Policies erstellen und zuweisen.
- **Mobile Device Authentication:** Authentifizierung von mobilen Geräten am Netzwerkzugangspunkt und Weiterleitung von unbekanntem oder möglicherweise unsicheren Geräten an das eigene interne (oder externe) Captive Portal. So lässt sich BYOD realisieren, ohne die Sicherheit im Netz zu gefährden.
- **Mobile Device Assessment:** Die integrierte, interne Assessment-Engine ist in der Lage, mit bestimmten MDM-Lösungen zu kooperieren. Das steigert Übersicht und Kontrolle hinsichtlich am Netz befindlicher Mobilgeräte. MDM-Lösungen arbeiten geräte-zentrisch, wobei Mobilgeräte sehr unterschiedliche Funktionen bieten. Das ergibt Sicherheitsherausforderungen, die sich durch die Integration mit Extreme Access Control bewältigen lassen. Denn so „weiß“ Identity and Access Control, ob das Gerät verwaltet wird und kennt Status und Sicherheit des Geräts am Netzzugang. Administratoren können auf diese Weise bekannten Geräten mit einem durch das MDM-System festgestellten, zweifelhaften Gesundheits- oder Sicherheitsstatus, den Zugriff verweigern.

Identity and Access Control-Funktionen ermöglichen es einer Organisation, BYOD erfolgreich auch ohne MDM-System zu implementieren, vor allem, wenn sie keine gemanagten mobilen Geräte haben. Administratoren können durch die Kombination von Geräteprofilen und einer Registrierung Geräte identifizieren und bereitstellen, ohne in eine MDM-Lösung zu investieren. Organisationen, die mobile Endgeräte noch besser überwachen und bewerten wollen, können das durch die Integration von MDM in das Extreme Management Center realisieren. Diese Lösung erfasst neben der bloßen Existenz der Geräte auch deren Gesundheitszustand.

Mobile Devices und Virtual Desktop Infrastructure (VDI)

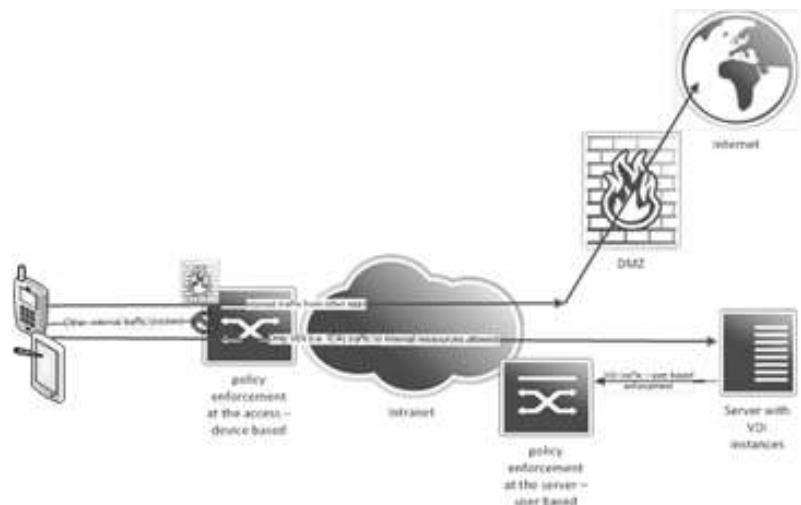
Bei der Betrachtung einer mobilen Geräte Strategie für die Organisation, gibt es noch eine weitere Option für eine einzigartige Daten- und Anwendungssicherheit. Dies ist die Virtual Desktop Infrastructure (VDI) von Anbietern wie Microsoft, Citrix und Vmware. In einem solchen Szenario sind alle Daten und Anwendungen an einem zentralen Ort, auf welchen das Gerät Remote über eine virtuelle Schnittstelle zugreift. In Kombination mit Extreme Mobile IAM verwendet, kann eine Organisation

- den Zugriff für mobile Endgeräte im Unternehmensnetzwerk auf VDI Nutzung beschränken.
- nutzerbasierte Policies für die VDI-Session im Rechenzentrum durchsetzen.
- allen anderen Verkehr zu externen Ressourcen (z. B. ein Internet-Proxy) routen.

Durch den Einsatz Access Control zusammen mit einer VDI-Lösung werden kritische geschäftliche Daten niemals auf dem mobilen Gerät gespeichert. Sie werden immer innerhalb des Rechenzentrums bleiben, wo sie nur angesehen und mit VDI-Technologie für den Remote Zugriff geändert werden können.

Andere Anwendungen können nicht auf diese Daten zugreifen

und wenn der Mitarbeiter das Unternehmensareal verlässt, können die Daten nicht mitgenommen werden. Der Mitarbeiter kann andere Anwendungen nutzen, um vollen Nutzen aus dem Funktionsumfang des Geräts zu haben, ohne dabei die Sicherheitsrichtlinien des Unternehmens zu verletzen. All dies wird unter Verwendung von leistungsstarken Extreme Policies erreicht, die direkt am Netzzugang des mobilen Geräts durchgesetzt werden – dem ExtremeWireless Access Point. Natürlich ist diese Lösung voll in die Extreme Identity and Access Control-Lösung integriert und bietet somit den vollen Umfang an Funktionalitäten, wie zentrales End-System-Management, Gerätetyp-Profilung, Standort-bestimmung, Gast-Zugang, etc.



MDM – Mobile Device Management

Die Anforderungen an Verfügbarkeit, Bandbreite, Sicherheit und Zugangskontrolle der WLAN Infrastruktur steigen rasant an. Das liegt an verschiedenen Faktoren. Zu den wichtigsten gehören die explosionsartige Verbreitung mobiler Endgeräte unterschiedlicher Hersteller mit verschiedenen Betriebssystemen, der große Bedarf an persönlichen und berufsbezogenen Applikationen und die steigenden Bandbreitenanforderungen durch Video, Voice und andere Daten.

Extreme Networks Mobile Identity and Access Management (Mobile IAM) verwendet einen einzigartigen Ansatz, um dieser Herausforderung gerecht zu werden: die Integration zwischen Extreme Networks IAM und einer MDM (Mobile Device Management)-Lösung. So erhält IAM mehr Einblick in Zustand und Konfiguration der mobilen Endgeräte und erweitert dadurch die Entscheidungsbasis für die Zuweisung von Netzwerkregeln (Policies).

Wie funktioniert eine MDM-Lösung?

Die meisten MDM-Lösungen nutzen derzeit eine Agenten-/Server-Architektur. Auf jedes mobile Gerät wird eine Software (Agent) aufgespielt. Sie liest genaue Informationen zu dem jeweiligen Gerät aus und leitet sie an einen zentralen Managementserver weiter. Zu diesen Informationen gehören unter anderem:

- Betriebssystem
- Gerätetyp
- Telekommunikationsinformationen wie die IMEI (International Mobile Equipment Identity), Telefonnummer, Netzbetreiber, etc.,
- Sicherheitszustand:
 - Verschlüsselungsstatus
 - Wipe Status (wurde das Gerät gelöscht?)
- Jailbroken-Status
- installierte Applikationen
- GPS-Informationen
- Sicherheitszustand der Unternehmensdaten auf dem Gerät
- Inventarisierungsinformationen:
 - Seriennummer
 - MAC-Adresse

Diese Daten werden für viele Unternehmen und Einrichtungen, die ein striktes Management mobiler Geräte vorschreiben, etwa Regierungsbehörden oder Krankenhäuser, immer wichtiger.

Was eine MDM Lösung nicht leistet

Auch wenn eine MDM-Lösung eingesetzt wird, braucht man für ein sicheres Netz eine Netzwerkzugangskontrolle für nicht gemanagte Gastgeräte und unregistrierte Geräte, die sich mit dem eigenen WLAN verbinden. Unerwünschte Geräte zu blockieren und Gastzugänge korrekt zu unterstützen, indem Gäste und Gastgeräte registriert und authentifiziert werden, gehört zu den zentralen Aufgaben der Mobile-IAM Lösung. Die MDM-Lösung ergänzt Extreme Access Control und übernimmt speziell die Verwaltung der gemanagten mobilen Endgeräte. Sie kontrolliert aber nicht, welche Geräte überhaupt Zugriff auf das Unternehmensnetzwerk erhalten und welche ausgeschlossen bleiben.

Beispielszenario-1:

Auf einem Gerät, das kompromittiert wurde, ist eine bösartige Applikation installiert. Die MDM-Management Lösung kennzeichnet dieses Gerät als gefährlich, allerdings hat das keinen Einfluss darauf, ob das Gerät ins Netz darf. Solange der Benutzer die WLAN-Zugangsdaten kennt, kann er sich auch mit dem WLAN verbinden.

Beispielszenario-2:

Der Geschäftsführer eines Unternehmens greift mit iPhone und WLAN auf unternehmenskritische Daten zu. Diese Daten bleiben nach beendeter Verbindung unter Umständen unverschlüsselt im Cache des iPhones. Sollte das iPhone verloren gehen oder gestohlen werden und wird es nicht von einer MDM-Lösung kontrolliert, kann Access Control beim nächsten Verbindungsaufbau zum WLAN überprüfen, ob das Gerät im MDM hinterlegt ist – falls nicht, kann man

- den Netzzugang so lange einschränken, bis das Gerät registriert ist und unter der Kontrolle der MDM-Lösung steht,
- einen einfach zu bedienenden Zugang für die Registrierung bei der MDM-Lösung realisieren,
- den Netzwerkzugang erlauben, sobald die MDM-Lösung festgestellt hat, dass das Gerät verwaltet wird und seine Daten gesichert sind.

Warum sich MDM und Access Control optimal ergänzen

MDM-Lösungen erfassen detailliert die Daten von Endgeräten und bestimmen genau, welche Applikationen und Konfigurationen auf ihnen erlaubt sind. Sie können Geräte-Policies jedoch nicht in Netzwerkzugangsregeln umsetzen.

Extreme Access Control nutzt die Geräteinformationen aus dem MDM, um die Netzwerksicherheitsrichtlinien auf alle mobilen Geräte anzuwenden:

- Positive Regeln: Stuft MDM ein Gerät als sicher ein, gewährt es diesem Gerät Netzwerkzugang. Andernfalls kann es das Gerät in eine Sicherheitszone verschieben, in der es keinen Schaden anrichten kann.
- Negative Regeln: Ist ein Gerät dem MDM nicht bekannt, wird es als unsicher oder als Gast eingestuft. Es wird auf eine Registrierungsseite in einer Sicherheitszone umgeleitet.

Zusätzlich realisiert Access Control eine globale Sicht des Netzwerks unabhängig vom Betriebssystem über alle Endsysteme in LAN und WLAN hinweg. Der Administrator kann somit jederzeit nachvollziehen, wer und was mit dem Netzwerk verbunden ist oder war und welche Sicherheitsregeln jedem Gerät zugewiesen wurden.

Extreme Connect

Mit Extreme Connect (vormals „OneFabric Connect API“) bietet der Management Center Server die Möglichkeit, andere Managementsysteme, wie VoIP-Systeme, Palo Alto, iBoss, Microsoft SCCM, eigene Datenbanken, etc. zu integrieren. Dies ermöglicht Vorteile im Betrieb und Troubleshooting, wenn z. B. erweiterte Geräteinformationen (z. B. Telefonnummer, Hardwaretyp, Softwarestand, Kostenstelle, etc.) aus externen System oder Datenbanken in Access Control importiert werden. Des Weiteren können Endgeräte durch solche Informationen auch automatisiert in eine entsprechende Autorisierungsgruppe provisioniert werden, um somit einen großen Rollout von Access Control zu unterstützen, bzw. im täglichen Betrieb neu beschaffte Systeme automatisiert zu autorisieren oder veraltete/verlorene/gestohlene Systeme automatisiert zu blocken.

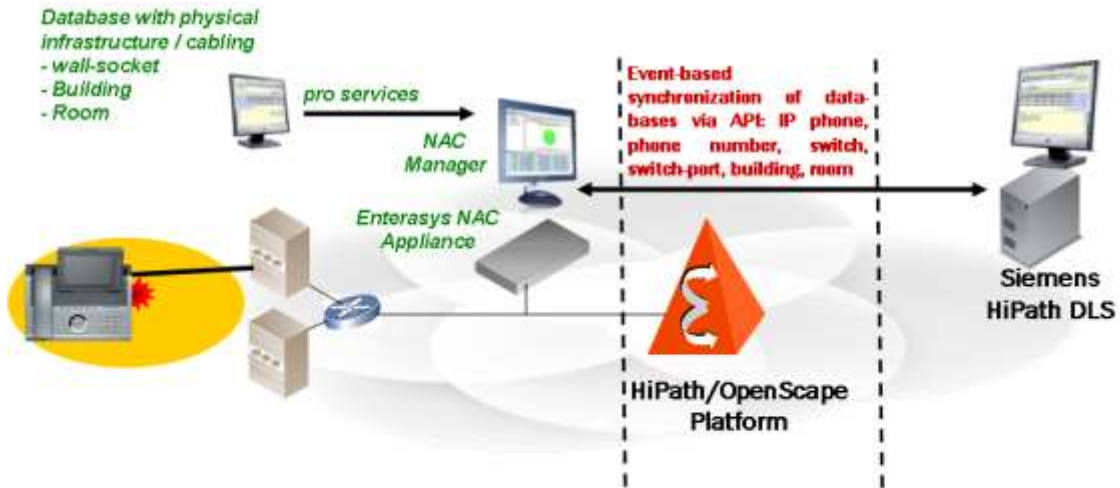
Die folgende Grafik zeigt erweiterbare Endsystem-Informationen, die über Extreme Connect aus dem Microsoft System Center Configuration Manager und Palo Alto gewonnen wurden.

Custom 3	Top Applications
Netbios Name=PZANELLA-WS2; User=; OS=Microsoft Windows 7 Enterprise (Service Pack 1); Manufacturer=Dell Inc. Model=Latitude E6400; PATH=\\MASCC...	web-browsing
Netbios Name=SMCROY-WS; User=CTRON\smcroy; OS=Microsoft Windows 7 Enterprise (Service Pack 1); Manufacturer=Dell Inc. Model=Latitude D620; PATH...	web-browsing
Netbios Name=JKNAPP-WS; User=CTRON\jknapp; OS=Microsoft Windows 7 Enterprise (Service Pack 1); Manufacturer=Dell Inc. Model=Latitude E6520; PATH...	web-browsing
Netbios Name=DESOUZA-WS; User=CTRON\desousa; OS=Microsoft Windows 7 Enterprise (Service Pack 1); Manufacturer=Dell Inc. Model=Latitude D620; PAT...	web-browsing
Netbios Name=DDULAC-WS; User=CTRON\ddulac; OS= (); Manufacturer=Dell Inc. Model=Latitude E6410; PATH=\\MASCCM1\root\sms\site_AND:SMS_R_Syst...	web-browsing
Netbios Name=JHARDIMAN-WS; User=CTRON\jhardiman; OS=Microsoft Windows 7 Enterprise (Service Pack 1); Manufacturer=Dell Inc. Model=Latitude E4310...	web-browsing
Netbios Name=LWESTON-WS1; User=CTRON\lweston; OS=Microsoft Windows 7 Enterprise (Service Pack 1); Manufacturer=Dell Inc. Model=Latitude E6520; P...	web-browsing
Netbios Name=DYEE-WS; User=CTRON\dyee; OS=Microsoft Windows 7 Enterprise (Service Pack 1); Manufacturer=Dell Inc. Model=Latitude E6510; PATH=\\M...	web-browsing
Netbios Name=JHARTFOR-WS1; User=CTRON\jhartfor; OS=Microsoft Windows 7 Enterprise (Service Pack 1); Manufacturer=Dell Inc. Model=Latitude D620; PA...	web-browsing
Netbios Name=LSELHI-WS; User=CTRON\Lilia.Selhi; OS= (); Manufacturer=Dell Inc. Model=Latitude E6400; PATH=\\MASCCM1\root\sms\site_AND:SMS_R_Sys...	web-browsing
Netbios Name=CMCTAGUE-WS1; User=CTRON\cmctague; OS=Microsoft Windows 7 Enterprise (Service Pack 1); Manufacturer=Dell Inc. Model=Latitude E6500...	web-browsing
Netbios Name=CARRIER-XP; User=CTRON\carrier; OS=Microsoft Windows XP Professional (Service Pack 3); Manufacturer=Dell Inc. Model=Latitude D630; PAT...	web-browsing

Dazu bietet Extreme Networks heute schon bestehende Integrationen, aber auch einen Professional Service, um individuelle Integrationen umzusetzen, an. Zukünftig ist geplant, unseren Kunden und Partnern ein dokumentiertes SDK für die XML/SOAP-basierte API des Control Centers anzubieten.

Automated VoIP Deployment

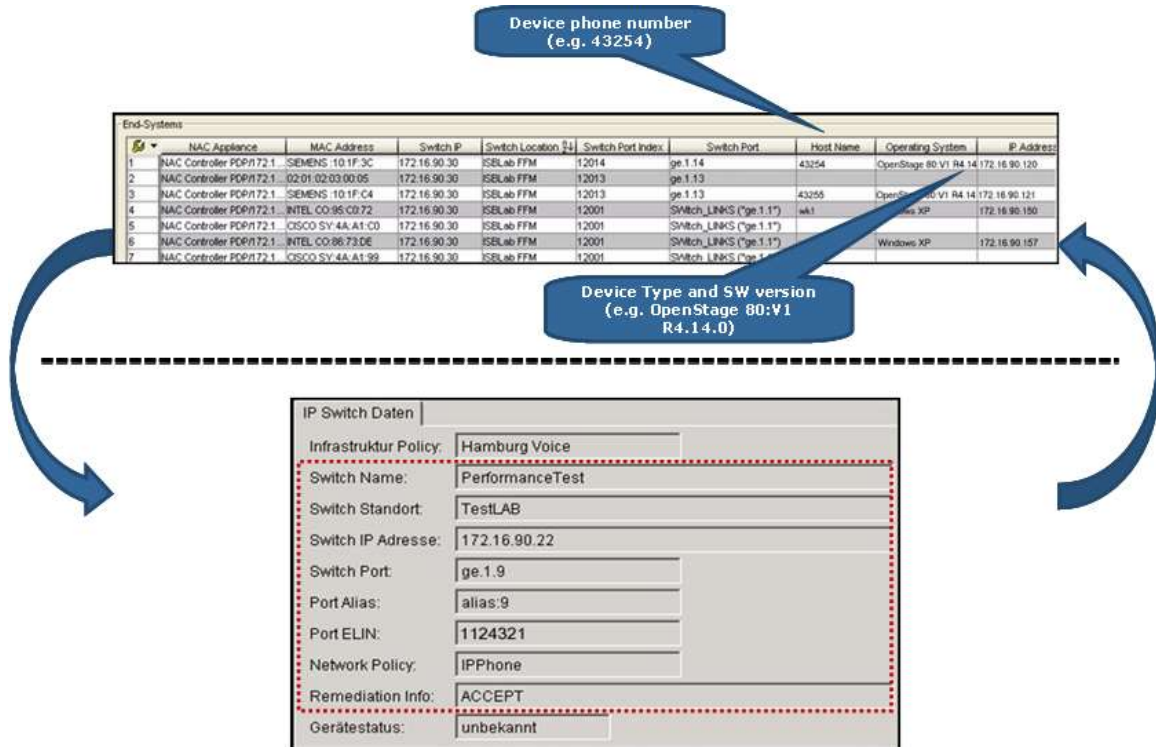
Beim Automated VoIP Deployment handelt es sich um die Verknüpfung der Daten des Extreme Access Control und der Unify DLS Server. Es handelt sich also um eine bidirektionale Integration zwischen den Webservices beider Dienste, die sowohl Infrastrukturdaten an den DLS als auch VoIP Endgeräte Informationen an das Management Center sendet.



Phone number	Phone IP Address	Phone MAC Address	Switch-name	Switch IP Address	Switch-port	Building	Room	Wall jacket	Phone Software
12345	10.1.1.10	xx-yy-yy-zz-aa	Access 1	10.9.9.8	fe.0.15	B. A	130	3	4.2.4
34567	10.1.1.18	aa-bb-cc-dd-ee-ff	Access 2	10.9.9.9	fe.1.8	B. B	241	1	4.2.4
56789	10.1.1.25	ab-cd-ef-gh-ij-h	Access 3	10.9.9.10	fe.2.21	B. A	412	2	4.2.2

SOA basierte Integration von Access Control und VoIP Device Management

Das Zusammenspiel aus Access Control und VoIP Infrastruktur erlaubt neben dem typischen Asset Tracking auch umfassendere Location Services, wie zum Beispiel eine automatisierte Rufumleitung, je nach Standort. Auch können spezielle Konfigurationen „location based“ automatisiert an ein Telefon weitergegeben werden. Dies können einfache Dinge wie eine Raumbezeichnung sein oder durchaus komplexe Stammdaten in Abhängigkeit zur jeweiligen Autorisierung (je nach Leistungsumfang der Telefone).



Damit ist eine ähnliche Dynamik erreichbar, wie man sie schon von zentralen Nutzerprofilen auf Desktop PCs kennt, die eine optimale Nutzung der gesamten Telefonie unter Einsatz von minimalem administrativem Aufwand erlaubt.

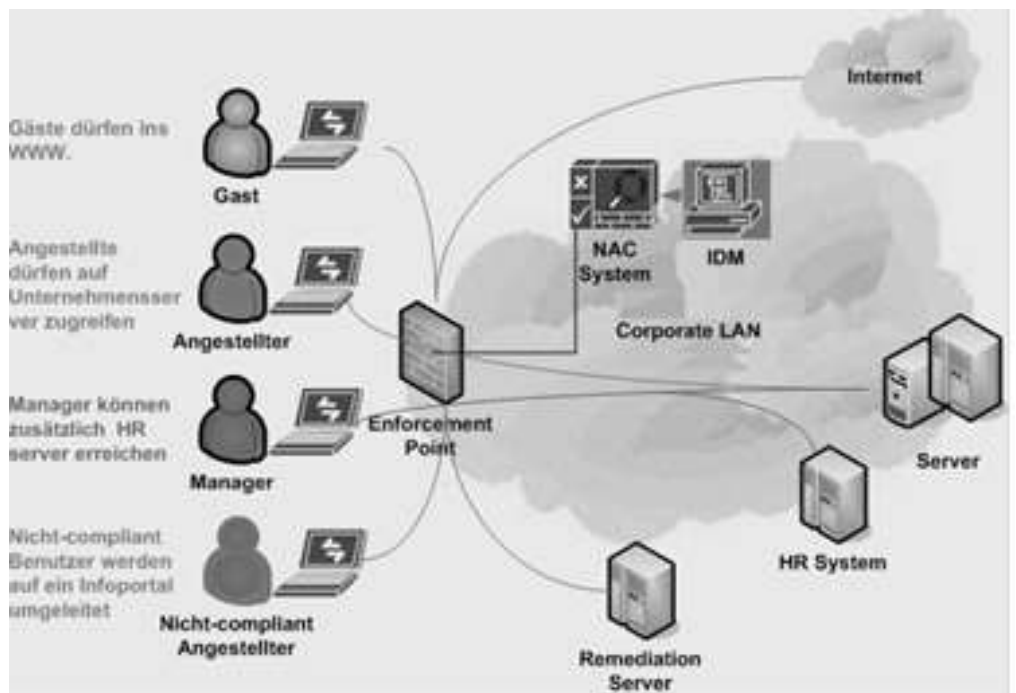
Location und Status Tracking

Alle gewonnenen Informationen werden auf dem Management Center in einer zentralen, offenen SQL Datenbank abgelegt und stehen somit über Standardschnittstellen zur Verfügung. So können automatisierte Benachrichtigungen über Zustandsänderungen per eMail versendet oder weitere Systeme über **Statuswechsel informiert** werden. Die neue „Notification Engine“ unterstützt dabei mit der Einrichtung von Benachrichtigungsoptionen, Filtern und frei konfigurierbaren Nachrichteninhalten. Diese Funktionalität ermöglicht die Automatisierung von Umzugsmeldungen im Netzwerk und reduziert den administrativen und finanziellen Aufwand erheblich. Natürlich können umgekehrt auch Konfigurationsdaten über einfache Schnittstellen erstellt oder geändert und damit ebenfalls automatisierte Aktualisierungen der Access Control Konfiguration durch externe Systeme vorgenommen werden.

Da in der Control Center Datenbank die Daten für alle Endsysteme bei der Anmeldung hinterlegt werden, kann jeder Benutzer im Netzwerk in Sekundenbruchteilen lokalisiert werden. Diese Informationen dienen dem NMS Console Compass sowie dem Automated Security Manager zum Suchen und können auch zur Realisierung einer E911 Notrufortung verwendet werden.

Identity und Access Management

Besonders deutlich wird das Zusammenspiel der vorliegenden Infrastrukturdaten in Kombination mit offenen Schnittstellen zur Ein- und Ausgabe von Daten am Beispiel einer IAM (Identity und Access Management) Integration. Hierbei werden sowohl Infrastrukturdaten (beispielsweise ein Umzug in ein anderes Gebäude) an einen IAM Server sofort weitergeleitet als auch Richtlinien (z. B. Stellenwechsel oder Kündigung eines Mitarbeiters) vom IAM Server an die Access Control Konfiguration weitergegeben.



Dies führt zu einer optimalen Verzahnung aus Richtlinienvergabe (IAM) und Kontrollinstanz (NAC), die automatisiert und mit überschaubaren Betriebskosten bei der Einhaltung von Betriebsprozessen unterstützt und ein Maximum an Sicherheit gewährleistet.

Produkte und Lizenzen

Um eine Access Control Lösung aufzubauen, benötigt man in der Basis mindestens zwei Komponenten: Extreme Management Center und ein oder mehrere Access Control Engines (auch als Gateways bezeichnet). Folgende Tabelle zeigt alle derzeit verfügbaren Access Control Produkte und Lizenzen:

Produkt / Lizenz	Beschreibung
IA-A-20	Physische Identity & Access Appliance (Hardware), unterstützt 3000 bis 6000 Endsysteme (abhängig von den verwendeten Optionen). Zusätzlich IA-ES Lizenz erforderlich.
IA-A-300	Physische Identity & Access Appliance (Hardware), unterstützt 6000 bis 12000 Endsysteme (abhängig von den verwendeten Optionen). Zusätzlich IA-ES Lizenz erforderlich.
virtuelle Appliances	die Verwendung virtueller Identity & Access Appliances ist in den NMS Advanced Lizenzen enthalten.
IA-ES-1K	Enterprise Lizenz für das Managen von bis zu 1.000 Endsystemen. Dazu wird eine entsprechende NMS Advanced Lizenz benötigt (NMS-ADV-XXX). Hierbei kann der Kunde so viele physische oder virtuelle NAC Appliances installieren, wie er benötigt, solange er die Anzahl von 1.000 Endsysteme nicht überschreitet. Das kombinieren mehrerer IA-ES Lizenzen ist möglich.
IA-ES-3K	Enterprise Lizenz für das Managen von bis zu 3.000 Endsystemen. Sonst wie IA-ES-1K
IA-ES-12K	Enterprise Lizenz für das Managen von bis zu 12.000 Endsystemen. Sonst wie IA-ES-1K
IA-PA-3K	Posture Assessment Lizenz für das Managen von bis zu 3.000 Endsystemen. Beinhaltet die Möglichkeit, sowohl agentenbasiertes, als auch netzwerkbasieretes Assessment durchzuführen. Sonst wie IA-ES-1K
IA-PA-12K	Posture Assessment Lizenz für das Managen von bis zu 12.000 Endsystemen. Beinhaltet die Möglichkeit, sowohl agentenbasiertes, als auch netzwerkbasieretes Assessment durchzuführen. Sonst wie IA-ES-1K

Die Anzahl der benötigten Identity & Access Appliances richtet sich nach der Anzahl der im Netz vorhandenen Endsysteme (=MAC Adressen) und die Anforderungen an die Redundanz dieser Lösung.

NetFlow, Sflow & IPFIX

Übersicht

Neben weiteren Verfahren sind NetFlow, sFlow und IPFIX weit verbreitet, um Verkehrsströme und Statistiken in Netzwerkkomponenten wie Switches und Routern zu sammeln und an eine oder mehrere externe Sammelstellen, die Kollektoren, zu senden.

Anwendungszwecke für Flow Export sind z. B.:

- Fehlersuche (z. B. durch das Auffinden ungewöhnlicher Datenraten bestimmter Anwendungen)
- Verkehrsflusskontrolle (z. B. durch ständiges Überwachen der ausgehenden Datenströme pro Switchport. Bei Überlastsituationen können die Applikationen erkannt werden, die höher oder niedriger priorisiert werden müssen)
- Sicherheit und Zugangskontrolle (durch Erkennen von Anomalien und unbekanntem Datenquellen im Netzwerk)
- Statistiken und Abrechnung (z. B. zur Netznutzung einzelner IP Endgeräteadressen oder IP Adressbereiche)

Das Modell ist bei allen Flow Export Protokollen das selbe: Ein Agent sammelt Flows auf dedizierten Probes, Switches oder Routern und exportiert diese in genau definierten Formaten an einen Kollektor. Dieser Kollektor analysiert und interpretiert die Flow Records und bietet in der Regel eine grafische Benutzeroberfläche zum Darstellen und Auswerten.

Was versteht man unter einem Flow?

Ein Flow ist nach gängigen Definitionen eine Folge von unidirektionalen Paketen mit gleichen Eigenschaften. Für IP Pakete nach NetFlow v5 sind diese Eigenschaften z. B.:

- Absender IP Adresse
- Ziel IP Adresse
- Absender Port für UDP oder TCP
- Ziel Port für UDP oder TCP, type und code für ICMP
- IP Protokolltyp
- Eingehendes Interface (ifindex)
- IP Type of Service

Flow record

Die Informationen aller zu einem Flow gehörenden Pakete werden also durch den Agenten gesammelt und als flow record an den Kollektor exportiert. Während sich bei NetFlow v5 die Inhalte des flow record auf IPv4 Header- und Routing-Informationen beschränkten, wurde mit NetFlow v9 ein dynamisches flow record Format eingeführt. Über ein frei definierbares Template werden die Inhalte festgelegt, die ein Agent dem Kollektor übermittelt. Zusätzlich zu den flow records wird nun also das Template Format in regelmäßigen Abständen vom Agenten zum Kollektor übermittelt. Durch

dieses offene Format können nun beliebige Zusatzinformationen wie IPv6 Adresse, MAC Adresse, VLAN ID, MPLS tag o.ä. in den flow records übermittelt werden.

Mit zunehmender Verbreitung von Flow Export Technologien und NetFlow wurde der Wunsch nach einem standardisierten Verfahren größer. Mit IPFIX (IP Flow Information eXport) wurde durch die IETF ein solcher Standard geschaffen. Da IPFIX quasi eine Weiterentwicklung von NetFlow v9 ist, wird gelegentlich auch von NetFlow v10 gesprochen.

sFlow ist ein weiterer Industriestandard, der von vielen Netzwerkkomponenten unterstützt wird. Neben Paketstatistiken liefert sFlow auch Portstatistiken.

Sampled, Unsampled, Any Port – Any Time

Wie unterscheiden sich nun die Technologien und Implementierungen in der Praxis?

sFlow arbeitet mit statistischen Verfahren, um Stichproben der übertragenen Datenpakete zu erfassen. Das macht sFlow skalierbar und es ist relativ einfach auf einer Vielzahl von Hardwareplattformen anwendbar. Als Nachteil muss jedoch genannt werden, dass nicht alle Pakete erfasst werden und je nach sampling interval die Aussagekraft der Statistiken variiert. Gerade wenn flow records für Sicherheitsanwendungen verwendet werden sollen, geht man mit sFlow große Kompromisse ein.

NetFlow bietet sowohl sampled als auch unsampled als Erfassungsmethode an. Aber warum sollte dann jemand unsampled auswählen? Ein Grund kann z. B. ein begrenzter Speicherplatz für die NetFlow Tabelle im Switch/Router sein. Traditionelle, paketbasierende Switches müssen die Flow-Zugehörigkeit aus einzelnen Paketen mit gleichen Eigenschaften (s. o.) erkennen und diesen flow im cache zwischenspeichern. Dafür steht je nach Gerätetyp selbst bei Core-Switches u.U. nur Platz für 128k bis 1M flows bereit. Kommt man an die Grenze dieser Tabellen, gibt es zwei Möglichkeiten:

- Einschränken der zu erfassenden Flows, z. B. Beschränken auf bestimmte Interfaces
- Sampling und damit „unterdrücken“ von Paketen mit den unter sFlow genannten Nachteilen

CoreFlow2 basierende Systeme unterliegen in dieser Hinsicht keinen Beschränkungen. Da die Weiterleitungs-Entscheidung nicht auf Paket-, sondern auf Flow-Basis erfolgt, werden auch die Flow-Informationen nicht im Cache, sondern direkt im ASIC vorgehalten. Systeme wie die Extreme Networks S-Serie oder K-Serie sind dadurch in der Lage, unsampled NetFlow von jedem Port zu jeder Zeit als flow record zu exportieren.

Flow Kollektoren

Als Flow Kollektor bietet Extreme Networks zwei Möglichkeiten:

- ExtremeSecurity Information and Event Manager (sFlow, NetFlow, IPFIX)
- Control Center (Netflow, IPFIX)

Neben dem Monitoring der reinen Flows und statistischer Aufbereitung in OneView kann durch Application Analytics das Flow Monitoring auf eine Applikationsanalyse erweitert werden. Mehr dazu in den entsprechenden Kapiteln.

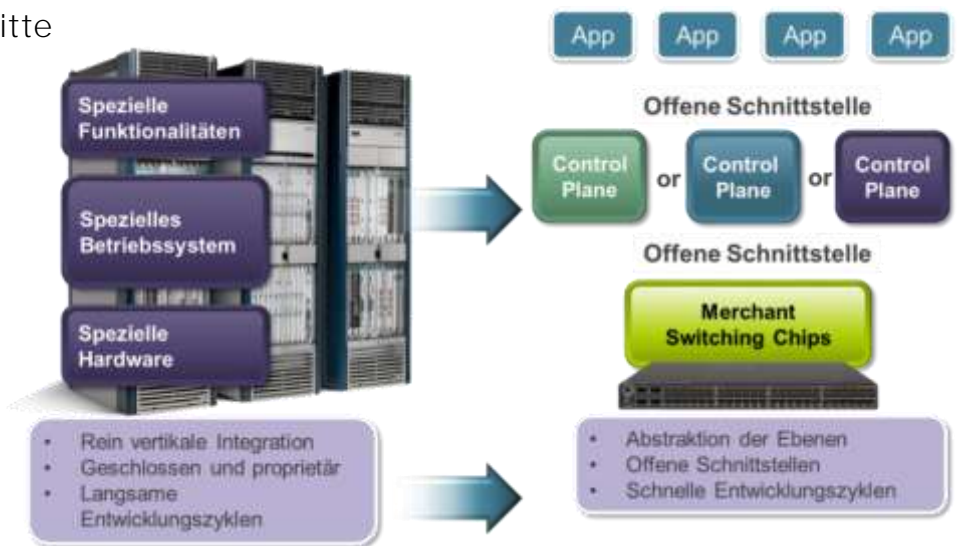
Kompatibilität

sFlow verwendet ein fest vorgeschriebenes Format für die flow records, das nicht mit NetFlow/IPFIX kompatibel ist. NetFlow v9 und IPFIX flow records können durch das offene template Format frei definiert werden. Damit ist es den Anbietern von Switches und Routern mit NetFlow Unterstützung möglich, flow records so zu definieren, dass diese den IPFIX Vorgaben entsprechen. Das gleiche gilt natürlich umgekehrt. In der Praxis wird auf den Netzwerkkomponenten über cli Befehle konfiguriert, ob im NetFlow v9 oder IPFIX Format exportiert wird. Die Kollektoren unterstützen in der Regel beide Varianten.

Software Defined Networking

Unter Software Defined Networking (SDN) versteht man im Wesentlichen die Einführung von Abstraktionsebenen in Netzwerk-Komponenten und weiterführend eine Trennung der Control Plane von der Data Plane.

Entstanden ist diese Idee Mitte der 2000er Jahre an der Stanford University. Im Rahmen der dortigen Forschungsprojekte entwickelte man unter anderem neue Ansätze für Routingprotokolle. Diese neuen Protokolle in einem produktiven Netz zu testen erwies sich als enorm schwierig. Die



vorhandenen Netzwerksysteme liessen sich aufgrund ihrer proprietären Hardware und ihrer proprietären Betriebssysteme nicht mit den neuen Protokollen betreiben. Daher entwickelte man ein Modell, welches sich an der Abstraktion der Computerindustrie in den 1980er Jahren orientierte. Dort hatte es durch den Einzug des Personal Computers einen radikalen Paradigmenwechsel gegeben. Statt proprietärer Mainframe Systeme, gab es nun Computer, welche mit standartisierten Schnittstellen arbeiteten. Somit war es möglich, jede Hardware mit jedem Betriebssystem zu betreiben, vorausgesetzt dass die jeweiligen Schnittstellen unterstützt werden. Ähnliches soll nun auch bei Netzwerk-Komponenten erfolgen.

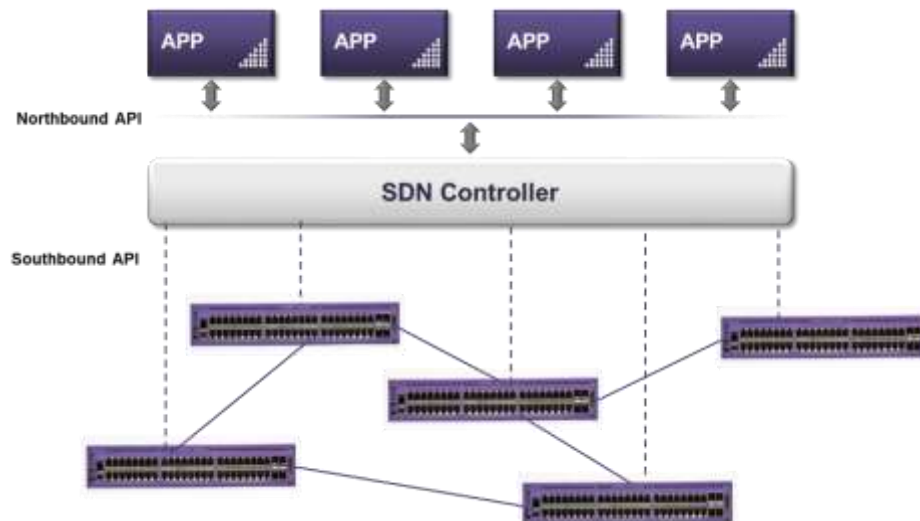
Die Trennung der verschiedenen Ebenen ermöglicht es auf Basis der standartisierten Schnittstellen, eine Interoperabilität zwischen verschiedenen Komponenten zu schaffen. Die unterste Ebene ist die Hardware oder Data Plane. Sie ist für das reine

Forwarding auf Basis von definierten Policies oder Flows zuständig. Die Data Plane trifft keine Entscheidungen, sondern ist sozusagen das ausführende Organ.

Über der Data Plane sitzt die Control Plane. Die Control Plane ist sozusagen das Netzwerk Betriebssystem. Sie trifft die Entscheidungen und definiert die Flows, die im Netzwerk erlaubt und nötig sind. Die Control Plane kommuniziert mit der Data Plane über die so genannte Southbound API als Schnittstelle. Vielfach wird die Control Plane in SDN Umgebungen auch einfach als Controller bezeichnet. Vor allem, wenn es sich um eine einzige zentrale Instanz handelt.

Nach oben hin kommuniziert die Control Plane oder der Controller über das so genannte Northbound API mit den Applikationen. Dabei können auch klassische Router Funktionalitäten wie OSPF oder BGP als Applikationen betrachtet werden.

Die Architektur eines SDN Netzes stellt sich also wie folgt dar:



Warum nun der ganze Aufwand? Schliesslich haben wir mit dezentralen Control Planes in den letzten Jahren ganz hervorragende und leistungsfähige Netze betrieben. Was ist also die Motivation hinter der Zentralisierung?

Die Anforderungen an die Netze haben sich in den letzten Jahren grundlegend geändert. Heutige Netze sind bei weitem komplexer als sie es noch vor einigen Jahren waren. Es gibt bei weitem mehr Applikationen mit unterschiedlichen Anforderungen. Durch die zunehmende Virtualisierung in den Bereichen Server, Desktop und Storage müssen Netze heute flexibler sein. Die erwartete Dienstgüte verbunden mit gestiegenen Anforderungen an die Sicherheit bedeutet einen deutlich höheren Konfigurationsaufwand als in der Vergangenheit. Clouddienste verlangen die Provisionierung von virtuellen Maschinen im Netz. Gleichzeitig sehen sich jedoch nahezu alle Netzbetreiber mit dem Problem mangelhafter Ressourcen und Budgets konfrontiert. Alles in allem können wir derartigen Anforderungen nur durch einen steigenden Grad von Automatisierung begegnen. Dabei ist die dezentrale Control Plane kein optimaler Ansatz mehr. In einem klassischen Netz muss jede Komponente einzeln konfiguriert werden, da sie jeweils für sich eine autonome Instanz darstellt. Das führt zu enormem Aufwand und langsamen Reaktionsgeschwindigkeiten. Eine Automatisierung

kann hier Abhilfe schaffen. In diesem Zuge ist eine zentrale Control Plane natürlich eindeutig im Vorteil. Es gibt eine zentrale Instanz, die das gesamte Netzwerk kontrolliert. Also müssen etwaige Änderungen auch nur noch an einer Stelle vorgenommen werden.

Darüber hinaus bietet der zentrale Controller auch noch andere Vorteile. Zunächst einmal handelt es sich hier um ein Stück Software und die Entwicklungszyklen sind bei Software deutlich kürzer als in der Hardware. Somit können neue Funktionalitäten schneller implementiert werden. Ausserdem können neue Funktionen und Services auf einem Klon des Controllers vorab umfangreich getestet werden, bevor sie ihren Weg in die Produktionsumgebung finden. Darüber hinaus kann die konsequente Umsetzung eines solchen Modells auch die Fehlersuche deutlich vereinfachen. Vorausgesetzt, dass alle Entscheidungen zentral vom Controller getroffen werden und dass die Southbound API verlässlich umgesetzt wurde, können etwaige Fehler nur noch im Controller selbst auftreten. Alle Informationen zur Fehlersuche sind also auch an einer zentralen Stelle verfügbar.

Soviel zur Theorie der reinen Lehre von SDN. In der Praxis haben sich jedoch einige Punkte ebendieser als nicht sehr praktikabel und nicht skalierbar herausgestellt. So findet man heute im Markt überwiegend einen hybriden Ansatz, bei dem der Switch weiterhin eine eigene Control Plane behält. Diese kann jedoch von einem zentralen Controller gesteuert werden. Das erleichtert zum einen die Migrationsszenarien von der klassischen Technologie hin zu einer SDN Architektur. Zum anderen entlastet es den zentralen Controller. Es gibt zum Beispiel keinen zwingenden Grund, warum das Hashing für Link Aggregation Groups nicht im Switch selbst, sondern im Controller vorgenommen werden sollte. Genau so ist das Scheduling der QoS Queues eine Aufgabe, die lokal vom Switch übernommen werden sollte. Der Switch braucht also auch weiterhin eine gewisse Intelligenz. Der Controller ist bezüglich der Umsetzung seiner Steuerungsbefehle und Flow Einträge agnostisch. Eine Link Aggregation Group wird beispielsweise einfach als eine Punkt-zu-Punkt-Verbindung mit mehrfacher Kapazität zum Controller gemeldet. Durch welchen der physischen Links das Paket letztlich übertragen wird, ist dem Controller egal. Das kann der Switch lokal entscheiden.

Bezüglich der Southbound API des Controllers haben sich im Markt zwei Konsortien als federführend erwiesen. Das ist zum einen die Open Network Foundation (www.opennetworking.org) und zum anderen die Open Daylight Foundation (www.opendaylight.org). Beides sind Zusammenschlüsse mehrerer namhafter Hersteller, welche sich des Protokolls OpenFlow als Southbound API annehmen.

Weitere mögliche Southbound APIs und die konkrete Umsetzung und Integration mit der Applikationswelt werden im Kapitel Management behandelt. Am Ende dieses Buches werden wir auf unsere Lösungspartnerschaften eingehen. Und schliesslich ist eine gute Kommunikation in Partnerschaftsfragen das A und O.

3 Wireless LAN

Nichts bewegt sich schneller als das Licht – ausgenommen die technische Entwicklung im Wireless LAN. Mit dem enormen Geschwindigkeitszuwachs geht simultan eine Durchdringung aller Bereiche des Lebens einher. Das verändert tatsächlich die Art wie wir arbeiten, lernen und kommunizieren. Es gehört mittlerweile zu den Selbstverständlichkeiten des Lebens, zu jedem Zeitpunkt vernetzt zu sein; eine Grundversorgung wie fließend Wasser oder elektrische Beleuchtung. Wie sehr wir uns schon daran gewöhnt haben fällt erst auf, wenn diese Verfügbarkeit plötzlich fehlt.

Diese hektischen Entwicklungssprünge stellen für uns – in der Rolle als Hersteller – eine echte Herausforderung dar. Sobald neue Chipsätze den nächsten Quantensprung beherrschen, sind unsere Entwickler schon dabei, die nächste Generation aktiver WLAN Komponenten zu entwerfen.

Derartig kurze Produktvorstellungszyklen sind nicht immer willkommen. Planer und Einkäufer fühlen sich eher verunsichert. Wie sicher ist die Investition der letzten Jahre? Kann ich heute noch – wie früher – technologischen Vorsprung einkaufen? Wie deckt sich mein reales Bedarfsprofil mit immer leistungsfähigeren Lösungsangeboten?

Die Antwort darauf kann nicht pauschal erfolgen. Betrachten wir daher zunächst ein paar Szenarien, die aufzeigen, wie unterschiedlich die Anforderungsperspektiven für Wireless LAN sein können.

Szenarien

Oder: Wieviel WLAN solls denn sein?

Zählen Sie doch mal nach...wieviele WLAN taugliche Gerätschaften tragen Sie tagsüber so bei sich? Laptop, Tablet, Smartphone? Analysten beziehen sich gerne auf alle drahtlosen Medien; Smartwatches und Fitnessarmbänder – die Blockbuster auf den großen Consumermessen – sind dabei nur der Anfang. Vom appgesteuerten Hörgerät über den überwachten Herzschrittmacher bis hin zur automatischen Insulinpumpe – bereits heute liegen zahlreiche Ideen in den Schubladen der Entwickler und warten auf profitable Anwendungsszenarien.

Und dann ist da natürlich noch eines der meiststrapazierten Schlagworte des Jahres 2016. Hinter Industrie 4.0 – gerne auch unter IoT firmierend – steckt eine ganze Reihe von Lösungen, die teilweise brandneu sind, manchmal jedoch auch schon einige Jahre eingesetzt werden.

Der beliebteste – weil am einfachsten zu vermittelnde - Aspekt aktueller WLAN Standards, die Bandbreite, deckt tatsächlich nur einen Randbereich der Erwartungen ab. „Harte Fakten“ wie 1,7 Gigabit pro Sekunde sagen in Wirklichkeit nur wenig über die Qualität eines drahtlosen Netzwerkes aus.

Fast jedes Praxisszenario fordert eine WLAN Lösung auf andere Weise heraus. Schauen wir uns diese doch einmal näher an:

Angewandter Flurfunk – WLAN im Büro

Eigentlich sind die Anforderungen an das drahtlose Netz im normalen Bürobetrieb gar nicht so dramatisch. Einfach ausgedrückt: Das Ziel ist erreicht, wenn kein Nutzer sich der Tatsache bewusst ist, dass kein Patchkabel seine Arbeit behindert, sein Smartphone immer die aktuellen Termine kennt und das private Tablet genauso selbstverständlich in die Arbeit einbezogen werden kann, wie zuhause auch.

Bandbreite spielt dabei eine geringere Rolle als eine flächendeckende Erreichbarkeit auch in der letzten Ecke des Büros. Kostengünstige Accesspoints in einer Vermaschungsdichte, die auch mal einen Geräteausfall kompensieren kann, sind hier das Mittel der Wahl. Dabei nehmen wir von altgewohnten Szenarien Abschied, bei denen wenige APs auf dem Gang die anliegenden Büros mitversorgt haben.

Sinnvoller ist mittlerweile eine Platzierung an den Punkten höchsten Bandbreitenkonsumes – innerhalb der Büros. Auf dem Gang wird selten aktiv gearbeitet, eine Basisversorgung ist jedoch angebracht, um die mobilen Geräte jederzeit online zu halten.

Alles nur geCLOUD – Die Einstiegslösung

Auch in einem kleinen Unternehmen kann die Anzahl genutzter Accesspoints schnell zunehmen. Und ein zentrales Management, welches alle Standorte und aktiven Systeme visualisiert und überwacht, vereinfacht den Tagesbetrieb signifikant.

Die Inbetriebnahme erfolgt denkbar einfach. Ein frisch installierter Accesspoint etabliert einen Tunnel zu seiner vordefinierten Controllerappliance - diese residiert auf einer deutschen ExtremeCloud-Plattform in Frankfurt am Main. Die gegenseitige Authentisierung von Accesspoint und Controller erfolgt per Zertifikat.

Über ein gesichertes Webinterface verschafft sich der Administrator Übersicht über die Betriebs- und Nutzungsdaten aller registrierten Komponenten und Endgeräte.

Der Fokus liegt auf der einfachen Bedienbarkeit. Ein Bausteinsystem verbindet Standorte, APs, Networks und Regelwerke zu einem flexiblen, sicheren Konstrukt.



Anmelde- und Nutzungsdaten verlassen in keinem Fall das lokale Netz. Der Zugriff wird durch standardisierte Schlüssel definiert. Und mit wenigen Handgriffen lässt sich die RADIUS Instanz eines lokalen Servers oder NAS zur individuellen Authentisierung einrichten.

Einstiegslösungen wie ExtremeCloud wachsen mit dem Unternehmen mit. Entscheide ich als Betreiber, mein WLAN Management künftig selbst in die Hand zu nehmen, so lassen sich die bereits angeschafften Accesspoints reibungslos in ein lokales Controllerszenario einbinden. Reboot genügt!

Home far from Home – Außenstandorte und Homeoffices

Kleine Außenbüros, die manchmal nur für begrenzte Zeit betrieben werden, sollten nach Möglichkeit mit minimalem Aufwand einzurichten sein.

Mit einem funktionierenden Internetzugang als Voraussetzung baut ein leistungsfähiger Accesspoint selbständig einen verschlüsselten Tunnel zum zentralen WLAN Controller des Unternehmens auf. Von diesem Moment an können die Mitarbeiter am Außenstandort die gleichen Dienste nutzen, wie sie auch in der Zentrale zur Verfügung stehen. Lediglich Latenzen und Bandbreitenlimits der Internetanbindung setzen dieser Methode Grenzen. Automatische Verschlüsselung und zentrale Authentisierungsinstanzen garantieren ein Sicherheitslevel ohne zusätzliche Sicherheitsmaßnahmen. Clientprobleme, aber auch physische Störeinflüsse, werden innerhalb des zentralen Managements schnell erkannt und lokalisiert.

Zwischen Regalen und Paletten – Drahtlose Logistik

Der Lagerbetrieb mit mobilen Terminals hat WLAN schon sehr früh als Medium der Wahl erkannt. Hier steht ständige Erreichbarkeit im Vordergrund; das Datenaufkommen fällt meist eher gering aus.

In der Praxis stellt so ein Lagerbereich mit fluktuierendem Regalbestand und ständig wechselnden Palettenstapeln eine echte Herausforderung an die Regelalgorithmen eines controllergesteuerten WLAN-Verbundes. Besonders beliebt: Bewegliche Hochregale, bei denen sich die Umgebungsbedingungen in kürzester Zeit dramatisch verändern.

Hier zieht WLAN alle Steuerungsregister. MIMO-Technologie nutzt neben den direkt eingehenden auch reflektierte Funkwellen, um auch in schwierigen räumlichen Umfeld mit optimal aufbereiteten Signalen Datenverbindungen sicher aufrechtzuerhalten.

Aber auch Leistungsparameter müssen immer wieder automatisch nachgeregelt werden, um ständig wechselnde Dämpfungs- und Reflektionsfaktoren auszugleichen.

Der Logistikbereich gehört zu den neuralgischen Punkten eines Unternehmens. Ohne reibungslose Abfertigung kommt der – oft sehr zeitkritisch konzipierte – Gesamtprozess schnell zum Stehen. Robuste Hardware und zuverlässige Software muss hier Hand in Hand gehen. Dazu gehören aufwändige Zertifizierungen, welche die Standardkonformität unserer Lösungen sichern. Angesichts einer unüberschaubaren Vielzahl von Clients wird dies zunehmend wichtiger.

High Density – Vom Hörsaal bis zum Stadion

Glaukt man den Analysten, so werden in den nächsten drei Jahren weltweit 7 Milliarden neue WLAN-Endgeräte ausgeliefert. Ein Hochschuladmin brachte es auf den Punkt: „Das letzte Weihnachtsfest hat uns 30% mehr WLAN Endgeräte beschert!“

Es sind also nicht nur die chronisch überfüllten Hörsäle, sondern auch die zunehmende technische Ausstattung der Nutzer, die dem Netz immer mehr abverlangt. In der nächstgrößeren Dimension sprechen wir von Kongresszentren und Sportstadien – letztere mit mehreren 10.000 Nutzern.

Wie gehen wir damit um? Nun, hier können die neuen Standards 802.11ac die Muskeln spielen lassen. Kleine Zellenkonstrukte mit grossen Bandbreitenkapazitäten sind hier gefragt. Neue Modulationsarten und Multiuser-MIMO nutzen die verfügbare Luftschnittstelle in diesem geringen Radius weitaus effizienter aus, als das früher notwendig war.

Das ist gut so, denn die Dichte der installierten Accesspoints lässt sich, bedingt durch die Frequenzbänder, nicht beliebig erhöhen. Hier ist eine präzise Feintuning notwendig, um Interferenzen zwischen indirekt benachbarten Zellen mit gleichem Kanal zu vermeiden. Doch auch kreative Methoden sind gefragt. War früher eine solide Betonwand für den WLAN Planer eher ein Ärgernis, so freut sich dieser nun über eine willkommene Abschirmung, die sein Funkzellenkonzept bereichert.

Offenen Stadien und großen Räumlichkeiten fehlen diese natürlichen Barrieren. In solchen Szenarien werden Accesspoints nicht nur an der Decke, sondern auch unter Tribünen angebracht. Hier agieren die Besucher selbst als Dämpfungselement und reduzieren die WLAN Bereiche auf das gewünschte Maß.

High Density Szenarien bringen eine ganze Menge Einflußfaktoren ins Spiel. Der Betrieb eines solch komplexen Netzes erfordert ein leistungsfähiges Monitoring, welches nicht nur Fehlersituationen schnell erkennt und Korrekturen erlaubt. Die Darstellung von Applikationsnutzung und Latenzwerten geben realistisch wieder, welche „Nettoleistung“ die Infrastruktur gerade hergibt. User Experience ist hier ein – im englischsprachigen Raum gerne genutzter – Begriff. Den Nutzer interessiert nicht die Technologie, die hinter allem steht. Er möchte „sein“ Internet haben. Im Hörsaal oder im Sportstadion – und das so einfach, wie zuhause. Die Einflußfaktoren zu verstehen und zu steuern, um nach außen hin eine Infrastruktur bereitzustellen, die sich reibungslos nutzen lässt, das ist der Trick. Zahlreiche Sporteinrichtungen bieten mittlerweile Dienste auf Extreme Wireless Plattformen an. Vom Fanportal über Videostreaming bis hin zu lokalen Webshops. Die wachsende Ausbreitung spricht für sich.

Die vernetzte Schwester – Wireless im Krankenhaus

Hier wird es ernst. Wenn Vitalmonitore, Patienten-Informationssysteme und Telefonie ganz selbstverständlich WLAN als Medium nutzen, ist das schon ein Vertrauensbeweis in diese Technologie. Ausfälle gefährden hier Gesundheit und Leben der Patienten.

Verfügbarkeit ist hier der Schlüsselfaktor. Die vorausschauende Platzierung von Accesspoints ist das A und O. Selbst wenn eine Komponente ausfällt, können benachbarte Accesspoints die Lücke automatisch schliessen. Probe Suppression Mechanismen optimieren die Endsysteme zu effizientem Roaming und damit der bestmöglichen Verbindung. Zahlreiche Kliniken haben WLAN als Plattform für VoIP Telefonie gewählt – einen besseren Beweis für gute Quality of Service und reibungsloses Handover gibt es kaum.

Schon heute unterstützen Krankenhausinformationssysteme mit digitalen Krankenakten die Visite. Die Einbindung bildgebender Systeme über Wireless wird den

Bandbreitenbedarf künftig erhöhen. Auch hier stellen die neuen Standards mit ihren grösseren Übertragungsraten die Basis für die nächste Generation von RIS- und PACS-Lösungen bereit.

Nicht zu unterschätzen sind Chancen, Mehrwerte und Anforderungen des Patientennetzes. Ein Krankenhausaufenthalt ist ohnehin kein Zuckerschlecken. Dabei weitgehend von Kontakten und Informationsquellen ausgeschlossen zu sein, macht es nicht leichter. Der Kontakt nach außen unterstützt in vielen Fällen den Genesungsprozess. Ein Grund mehr, die Möglichkeiten des WLAN dahingehend auszuloten.

Der Sicherheitsaspekt darf dabei auch nicht außer Acht gelassen werden. Robuste Authentisierungsmethoden, klare Separierung auf logischer Ebene und eine Bandbreitenkontrolle, die betriebskritischen Prozessen stets ausreichende Ressourcen sichert, sind wichtige Elemente einer Sicherheitsstrategie im Gesundheitswesen.

Das WLAN im Krankenhaus erfordert die Betrachtung aller Aspekte - von Verfügbarkeit über Bandbreite bis zur Sicherheit. Das ist für uns nicht neu, und wir stehen auch für die nächste Entwicklungsgeneration mit Ideen, Technologie und soliden Standards bereit.

Was kommt als nächstes?

Zunächst ist WLAN ja nicht die einzige drahtlose Technik. Je nach Anwendungsbereich Bandbreite und Distanz gibt es zahlreiche Technologien, von denen jede ihre Daseinsberechtigung hat. Und die wachsen nun immer weiter zusammen.

Accesspoints der nächsten Generation werden für manche Anwendungsbereiche kleiner ausfallen, dichter platziert und unterstützen neben 802.11ac auch Technologien wie Bluetooth Low Energy und Zigbee.

Hotspot 2.0, basierend auf dem IEEE 802.11u Standard, löst zwei Probleme auf einmal. Stellen Sie sich vor, Sie betreten ein Gebäude - und Ihr Smartphone klinkt sich automatisch in das lokal bereitgestellte Gast WLAN ein. Ohne Registrierung, ohne Papiervoucher mit Passwörtern, die sich nicht mal ein Zahlenkünstler merken kann. Hotspot 2.0 authentisiert sie mit den Zugangsdaten „Ihrer“ Telefongesellschaft.

Das Ergebnis ist eine Win-Win-Win Situation. Der Endnutzer roamt mühelos aus einem, möglicherweise stark belasteten Mobilfunknetz in die robuste WLAN Umgebung seines Gastgebers. Dieser bietet einen Gastzugang ohne Aufwände für die Registrierung. Und der Mobilfunkbetreiber entlastet mit dieser Maßnahme sein Netz. Trotz aller Einfachheit findet eine eindeutige Authentisierung statt. In Zeiten einer - nach wie vor unscharf definierten - Störerhaftungsregelung ist auch dies von Vorteil.

WLAN wird unsere Umwelt immer stärker durchdringen. Von Bürobereichen, die mit wenigen Ausnahmen nur noch Wireless betrieben werden über öffentliche Bereiche in denen die einschlägige Mobilfunkausleuchtung zunehmend durch lokale Accesspoints ergänzt werden.

Neue Standards wie 802.11ax und ay weisen schon auf Technologien hin, die 10Gbps und mehr ermöglichen. Was sich hier in welchem Bereich durchsetzen wird, lässt sich

heute noch nicht ermessen. Die Erfahrung zeigt, dass allein die Jagd nach immer höheren Übertragungsraten im Wireless LAN nicht mal die halbe Miete abdeckt.

Die Fähigkeit, IT Dienste auf drahtlosen Medien sicher und zuverlässig abzubilden, ist nach wie vor der entscheidende Faktor auf dem Weg zur praktischen WLAN Integration. Genug der Visionen - werden wir konkret:

Features, Facts und Autoquartett

Architektonisches - Evolution der Controller

Seit vielen Jahren beschreibt der Solution Guide nun schon die Entwicklungen drahtloser Systeme. Dass traditionelle Stand-alone Accesspoints nur noch im häuslichen Umfeld einsetzbar sind und im Enterprisebereich durch controllerbasierte Lösungen abgelöst wurden, soll nur noch der Vollständigkeit halber erwähnt werden.

Auch die Definition des Thin Accesspoint als „intelligente Antenne“ hat sich in den meisten Fällen überholt. Stark zentralisierte Konzepte haben, wenn es um Skalierbarkeit und Ausfallsicherheit geht, mittlerweile so viele Schwachpunkte entwickelt, dass eine balancierte Verteilung von Intelligenz und Leistungsfähigkeit eindeutig die bessere Lösung darstellt.

Um Mißverständnissen vorzubeugen - diese Konzepte waren zu ihrer Zeit durchaus gut und richtig. Aber Evolution bedeutet auch immer, dass sich die Rahmenbedingungen ändern. Zu Zeiten als ein Accesspoint noch 11 oder 54 Mbps auf der Luftschnittstelle transportierte, war es durchaus legitim dieses Datenvolumen in den Controller zu tunneln. Aber lassen Sie heute mal zweitausend 802.11ac Accesspoints auf eine Appliance los...

Die Technologie bietet heute einfach andere Möglichkeiten. Es gibt nicht mehr das ausschließliche „entweder tunneln oder local breakout“. Die Steuerung des Datenverkehrs lässt sich mittlerweile anhand von Regelwerken dynamisch ändern.

Und das schafft ganz neue Möglichkeiten. Typische Funktionen einer WLAN Switching Lösung sind z.B.:

- Automatische Kanalwahl
- Automatische Regelung der Sendeleistung
- Loadbalancing zwischen den APs
- Verarbeiten von Gebäude/ Geländeplanen, um die Funkausbreitung/ Clients/ RFID-Tags/ Fremd-APs visuell darzustellen
- Verkürztes, subnetübergreifendes Roaming
- Automatisiertes Erkennen, Lokalisieren und Bekämpfen von Fremd-APs und Clients
- Zentralisierte Planung, Deployment, Reporting & Alarmierung

Durch die ExtremeWireless Fit AP Architektur bleibt ein grosser Anteil der Intelligenz in den APs erhalten. Dies ermöglicht dezentrales Traffic-Forwarding direkt am AP mit allen nötigen Parametern wie z. B QoS, Ratelimit, ACLs usw. und eliminiert das Nadelöhr am Controller.

Sites - The Art of Survival




Kein Planungsgespräch ohne diese Frage: „Was passiert in einer Außenstelle, wenn die Verbindung zum WLAN-Controller unterbrochen ist?“ Nun, um die Handlungsfähigkeit der Mitarbeiter zu definieren, muss erst einmal geklärt werden, welche Arbeits- und Kommunikationsprozesse überhaupt noch möglich sind, wenn die WAN Verbindung gekappt ist. Ohne Rechenzentrum – oder Cloud – dürften die meisten Dienste auch nicht mehr zur Verfügung stehen. Die Frage nach einem funktionierenden WLAN ist damit gegenstandslos.

Trotzdem – welche Optionen sind denn noch verfügbar?

Zunächst lassen sich APs in sogenannten Sites zusammenfassen. Diese Überlebensgemeinschaften kommunizieren untereinander; das dient Funktionen wie Band Steering und Load Sharing. Aber auch bereits eingebuchte und authentifizierte Endgeräte können innerhalb einer Site von AP zu AP weitergereicht werden, ohne dass eine Autorisierung vom Controller notwendig ist. Wer schon im Netz ist, kann also weiterarbeiten. Vor Ort bereitgestellte, autonome RADIUS Dienste können von den Site APs direkt angesprochen werden. Damit wäre auch eine dezentrale Authentisierung möglich. Wer diesen Aufwand scheut, legt sich eine Notfall-SSID an, deren Zugang über einen Private Shared Key erfolgt. Dieser liegt im Filialtresor und wird auch nur im Störfall mitgeteilt.

Das Beste aus zwei Welten

Diese Architektur verbindet die Autonomie einer Thick AP Architektur mit dem Komfort Thin AP Architektur. Nachdem auch die Cloudarchitekturen von dieser Symbiose profitieren liegt Extreme Networks hier voll im Trend.

	<p>FAT AP Architektur</p> <p>Intelligenz und Management direkt auf den Access Points</p>
	<p>Split MAC / Thin AP Architektur</p> <p>Splitted MAC-Funktionen zwischen AP und Controller (Encryption, QoS, RF Management)</p> <p><i>(Skaliert nicht in großen Umgebungen)</i></p>
	<p>Fit AP Architektur</p> <p>Dezentrales Policy-Enforcement (Encryption, QoS, RF Management)</p> <p>Zentralisiertes Management und Kontrolle</p>

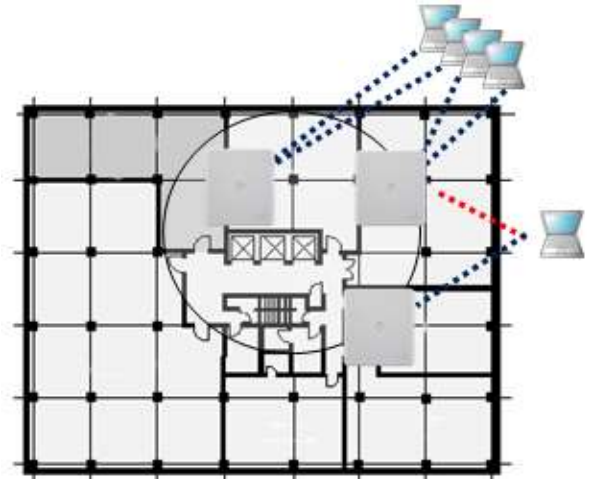
WLAN High Density & Performance

Die Analysten erwarten in den nächsten 3 Jahren die Auslieferung von 7 Milliarden WLAN fähigen Endgeräten. Und nicht nur technikaffine Menschen tragen mehr als eine funktaugliche Komponente mit sich herum. Laptop, Smartphone, Tablet...Tendenz: Steigend. Höchste Zeit, dass wir uns mit High Density Szenarien genauso auseinandersetzen, wie mit den gesteigerten Bandbreiten, welche die neuen Standards bieten.

Sehen wir uns zunächst mal die unterschiedlichen Techniken an:

Load Balancing & Band Steering

Load Balancing verteilt Clients über eine definierte Anzahl von APs. Das stellt sicher, dass ein einziger Accesspoint oder Kanal nicht überlastet wird, während andere weitgehend ungenutzt bleiben. Voraussetzung ist, dass sich die APs gegenseitig auf der Luftschnittstelle sehen. Typischerweise wird dieses Feature in großen Besprechungsräumen, Bibliotheken oder Hörsälen eingesetzt.



Das 5GHz Band hat nicht die gleiche Reichweite, bietet mit zahlreichen überlappungsfreien Kanälen und weitaus mehr Bandbreite die bessere Alternative zum bisher genutzten ISM Frequenzbereich.

Viele Endgeräte arbeiten heute schon im 5GHz Band. Das sogenannte Band Steering erkennt die Dual Band Fähigkeit eines Clients und assoziiert ihn bevorzugt über das 5GHz Radio eines Access Points. Damit wird das 2,4GHz ISM Band idealerweise nur noch von Geräten genutzt, denen diese Alternative nicht offensteht.

Voraussetzung für diese Maßnahme ist eine flächendeckende Ausleuchtung im 5GHz Band, um Verbindungsabbrüchen vorzubeugen. In Kombination maximieren beide Methoden die Effizienz und den Durchsatz des Gesamtsystems.

Single SSID Design

Die Vielzahl an Applikationen und Endsystemen in heutigen WLAN-Netzen kann nicht mehr durch zusätzliche SSIDs Domänen umgesetzt werden. Durch die Möglichkeit, userbezogene Policies mit allen nötigen Parametern (VLAN, ACL, Topologie, Ratelimit, QoS) zu vergeben, wird dies beim Single SSID Design innerhalb der SSID gelöst. Dadurch ergeben sich folgende Vorteile:

- Per User Topologie, QoS, Ratelimit und ACL
- weniger SSIDs nötig – einfachere Konfiguration der Clients
- einfacheres Durchsetzen von Security-Policies, da weniger SSIDs zu schützen sind
- Bessere Performance in der Luft – da weniger Beacons

Besonders durch das Minimieren der Beacons steigt die Performance in der Luft erheblich:

Beispiel mit 6 SSID per AP – 3 APs im gleichen Bereich:			Gleiches Netzwerk mit nur 3 SSIDs per AP:		
Beacon Datenrate	Channel	Bandbreitennutzung	Beacon Datenrate	Channel	Bandbreitennutzung
1 Mbps	25.92%		1 Mbps	12.96%	
2 Mbps	12.96%		2 Mbps	6.48%	
5.5 Mbps	4.71%		5.5 Mbps	2.36%	
11 Mbps	2.36%		11 Mbps	1.18%	
6 Mbps (802.11a/g)	4.32%		6 Mbps (802.11a/g)	2.16%	
12 Mbps (802.11a/g)	2.16%		12 Mbps (802.11a/g)	1.08%	

Denken Sie auch daran, dass die Rückwärtskompatibilität zu dem alten Standard 802.11b nur zu dem Preis einer auf 1Mbps reduzierten Datenrate der Beacons zu haben ist. Geräte, die ausschließlich diesen Standard unterstützen, finden sich manchmal in Produktionsanlagen, vereinzelt auch im Logistikbereich eines Unternehmens.

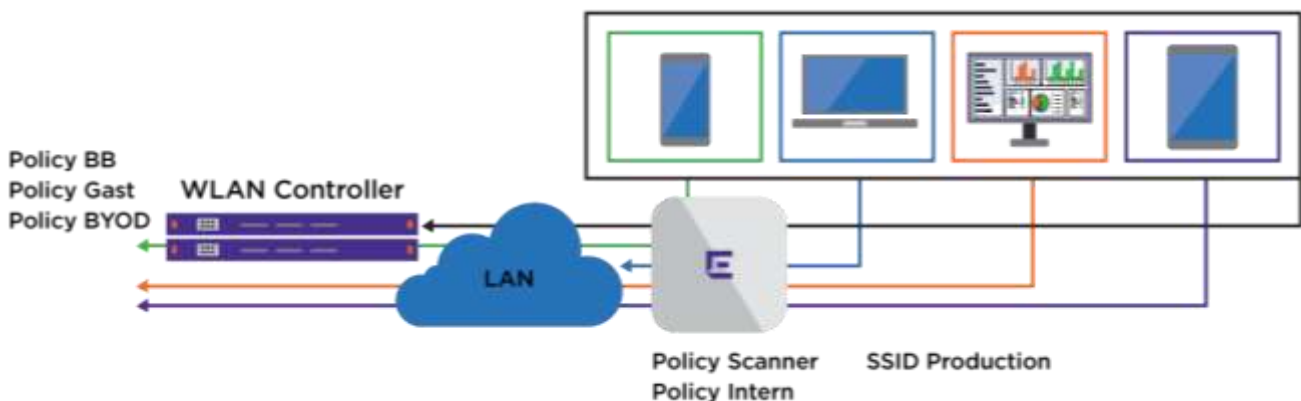
In der Verwaltungszone einer Organisation sollten diese betagten Systeme nicht mehr auftauchen. Werfen Sie doch mal einen Blick auf den Clientreport Ihres Controllers. Sind hier keine Endsysteme mehr über 802.11b eingebucht, deaktivieren Sie diesen Standard und entlasten damit die Luftschnittstelle in dieser Zone.

Jedes bißchen hilft...

Mit Policies verteilt bereits der Access Point die an eine SSID angedockten Endsysteme gemäß der Regelanweisungen. Und das sind nicht nur die üblichen Verdächtigen wie Layer 2/3/4-basierte Filter, auch die Weiterleitung an unterschiedliche Topologien wird hier eingesteuert.

Mit der neuesten Software ist ExtremeWireless darüberhinaus in der Lage, die aus Analytics ermittelten Applikationsfingerprints als Regelfilter festzulegen. (Siehe auch Kapitel Extreme Analytics)

Prinzipschaubild:



Airtime Fairness

Obwohl die Anzahl der installierten 11n/ac-APs stetig steigt, findet man auf der Client-Seite fast immer noch bunt gemischte Umgebungen, in denen Endgeräte unterschiedlichster Generationen auf die gleiche Infrastruktur zugreifen. Durch den bestehenden Zugangsmechanismus wird jedem Client, unabhängig von der

Geschwindigkeit, mit der er verbunden ist, erlaubt, die gleiche Anzahl an Paketen zu versenden. Bei gemischten Clientzugangstechnologien (11n vs .11a/b/g) führt dies dazu, dass z.B. ein 11b Client den Kanal erheblich länger belegt als ein 11n Client. In der Summe wird dadurch der Gesamtdurchsatz der Funkzelle stark vermindert. Dieses Verhalten wird als Packet Fairness bezeichnet.

Durch Ändern dieses Verhaltens von Packet Fairness auf Airtime Fairness, bei dem jedem Client die gleiche Sendezeit eingeräumt wird, wird der Gesamtdurchsatz der Funkzelle gesteigert.

Client Mix	Effective Bandwith (Mbps)	
	Packet Fairness	Airtime Fairness
11a @ 6 Mbps	4.5	1.5
11a @ 24 Mbps	4.5	6
11n HT20 @ 104 Mbps	4.5	26
11n HT40 @ 240 Mbps	4.5	60
Total Throughput	18.0	93.5

Ratelimit & QoS

Da sich die in einer Funkzelle eingeloggten Clients die Bandbreite und Sendezeit dieser Zelle teilen, ist es höchst effizient, mit Ratelimits & QoS den Zugriff auf die Zelle je nach Nutzer (z. B. Gäste vs. internen Clients) zu steuern. Dadurch ist es möglich, die limitierte Kapazität nutzer- bzw applikationsbezogen effizient zu verteilen.

Erhöhen der Minimum-Basic-Rate:

Management- sowie Multicast-Frames werden mit der geringstmöglichen Geschwindigkeit übertragen, damit sichergestellt wird, dass der Traffic auch von allen Clients erreicht wird. In einem gut ausgeleuchteten Areal erreicht jeder Client eine solide Bandbreitenversorgung. Die MBR von einem auf solide 12 bit zu erhöhen, sollte hier möglich sein und schafft wieder mal etwas mehr Luft auf der Schnittstelle.

Performance-Tuning für Multicast-Verkehr:

Die gestiegene Nutzung von Video-over-WLAN & Zero-Config-Protokollen wie Bonjour, UpnP und LLNMR führt zu einem erheblich größeren Anteil an Multicast-Traffic innerhalb eines WLANs. Da Multicast-Traffic immer mit der Minimum-Basic-Rate versendet wird, kann dies zu Performance-Engpässen führen. Daher wird folgender Umgang mit Multicast-Traffic empfohlen:

- Multicast-Filterung @ AP
- Multicast zu Unicast Umwandlung
- Proxy ARP @ AP
- Anpassbare Multicast Senderate

Best Practise Radio Konfiguration:

Nicht ohne Grund gibt es zahlreiche Einstellungen und Optionen, um eine WLAN Infrastruktur feinzutunen. Das Büroumfeld stellt andere Anforderungen als eine Lagerzone - hatten wir ja schon beleuchtet.

Für den Einstieg lässt sich ein WLAN mit einer soliden Grundeinstellung wie dieser betreiben:

Radio 1	Radio 2
<ul style="list-style-type: none"> • Radio Mode: a/n/ ac • Channel Width: 40MHz (80 Mhz bei 11ac APs) • Guard Interval: Short • ATPC: Enabled • Max Power: 20 dBm • Min Power: 0dBm • Protection Mode: Disabled • 40MHz Protection Mode: None • Aggregate MSDUs: Disabled • Aggregate MPDUs: Enabled (Disabled for Voice) • ADDBA Support: Enabled (Disabled for Voice) <p>Zusätzlich bei AP37xx:</p> <ul style="list-style-type: none"> • Enable LDPC • Enable STBC • Enable TXBF 	<ul style="list-style-type: none"> • Radio Mode: b/g/n (b ausschalten, wenn keine 11b Devices mehr vorhanden) • Channel Width: 20MHz • ATPC: Enabled • Max Tx Power: 20 dBm • Min Tx Power: 0 dBm • Protection Mode: Disabled • 40MHz Protection Mode: None • Aggregate MSDUs: Disabled • Aggregate MPDUs: Enabled (Disabled for Voice) • ADDBA Support: Enabled (Disabled for Voice) <p>Zusätzlich, wenn Abdeckung gegeben:</p> <ul style="list-style-type: none"> • Erhöhen der min. Basic-Rate (2, 5,5 oder auch 11 Mbps) • Erhöhen der 802.11g/ a min. Basic-Rates (12 oder auch 24 Mbps) <p>Zusätzlich bei AP37xx:</p> <ul style="list-style-type: none"> • Enable LDPC • Enable STBC • Enable TXBF
VNS Configuration	
<p>Global Settings->Wireless QoS->Flexible Client Access</p> <ul style="list-style-type: none"> • Fairness Policy: 100% Airtime <p>WLAN Services->Privacy</p> <ul style="list-style-type: none"> • “None”, “WPA v.2” oder “WPA-PSK v.2” <p>WLAN Services->QoS</p> <ul style="list-style-type: none"> • WMM: Enabled • Flexible Client Access: Enabled 	

Sicherung von WLAN Netzen

Lassen Sie uns über WEP nur soviel sagen: Ja, das war einmal ein Sicherheitsstandard, der wegen seiner Angreifbarkeit schon seit langem geächtet ist und keinesfalls mehr eingesetzt werden sollte. Zwischenstandards wie WPA sind mittlerweile auch obsolet.

Das Thema Sicherheit im Wireless LAN ist nach langer Diskussion nun final gelöst: Der Standard 802.11i (auch WPA2 genannt) ist verabschiedet und bietet für alle existierenden Sicherheitslücken innerhalb der 802.11 Familie eine adäquate Lösung. Die Authentifizierung via 802.1x (Port Based Authentication) und dessen gängige Methoden EAP-TLS, PEAP und EAPTTLS (zertifikats- und passwortbasiert) stellen neben der eigentlichen Authentifizierung die Basis für das Key Management dar. Die Verschlüsselung ist 128-Bit AES (Advanced Encryption Standard) -basiert. Die Integrität von Daten und Header wird durch CCM (CCM = Counter Mode Encryption mit CBC-MAC) gewährleistet. Replay Attacks werden durch ein IV (Initialization Vector) Sequencing mit 48 Bit IV verhindert.

Nach dem Credo der Sicherheitsexperten (Verfügbarkeit, Vertraulichkeit, Integrität) ist neben dem Schutz vor unbefugtem Eindringen und Mitlesen vor allem der kontinuierliche Betrieb alles andere als trivial. Fremde APs sowie WLAN-fremde Störungen beeinflussen die Übertragungsqualität auf einzelnen Kanälen oder im gesamten Frequenzband. Mangelhaft geschirmte Mikrowellenöfen oder DECT-Stationen sind, neben einem mangelhaft getunten Nachbar-WLAN, häufige Ursachen. Aber auch in Produktionshallen stören Maschinen oder sogar Großraumleuchten mit ihren Interferenzen das unbeschwertere Arbeiten über WLAN.

Je nach Einstellung scannen Accesspoints automatisch die selbst genutzten Kanalbereiche der APs nach anderen Geräten, die im selben RF-Band arbeiten. Dadurch werden fremde Sender wie auch die zum eigenen Netz gehörenden APs erkannt. Alle fremden Sender stellen potentielle Rogues (Schurken) dar. Hierbei ist eine automatische Unterscheidung zwischen „Interfering AP“, „Rogues“ und „Ad-hoc Clients“ wichtig.

Ein Interfering AP wird auf der RF-Schnittstelle von den APs gesehen. Dieser hat jedoch keine Verbindung über die LAN Schnittstelle ins eigene Netz und stellt daher nur eine Störung auf der Funkseite dar. Meist sind dies Netze in benachbarten Gebäuden oder interne, unabhängige WLANs. Ein Rogue AP hingegen hat auch eine Verbindung über die LAN Schnittstelle ins eigene Netz und stellt damit ein erhöhtes Sicherheitsrisiko dar, da sich über diesen AP auch fremde Clients in das interne Netz einloggen können. Ad-hoc Clients kommunizieren direkt miteinander ohne Verbindung zum eigentlichen Netzwerk. Dies stellt ähnlich wie die Interfering APs kein direktes Sicherheitsrisiko dar, allerdings werden sie als Störung auf der Funkseite erkannt.

Die Allianz aus AP und Controller kategorisiert diese Störquellen und ergreift optional Gegenmaßnahmen, Anbandelversuche von WLAN Clients mit einem Rogue AP zu vereiteln. Das WLAN Konstrukt simuliert dabei den Rogue AP und beendet die ungute

Liaison mit eigens gesendeten Disassociation Frames. Die Clients klinken sich aus und können sich auch nicht mehr fehlerfrei verbinden.

Mit Hilfe von Gebäudeplänen und Triangulation lassen sich Rogue APs lokalisieren, und neutralisieren.

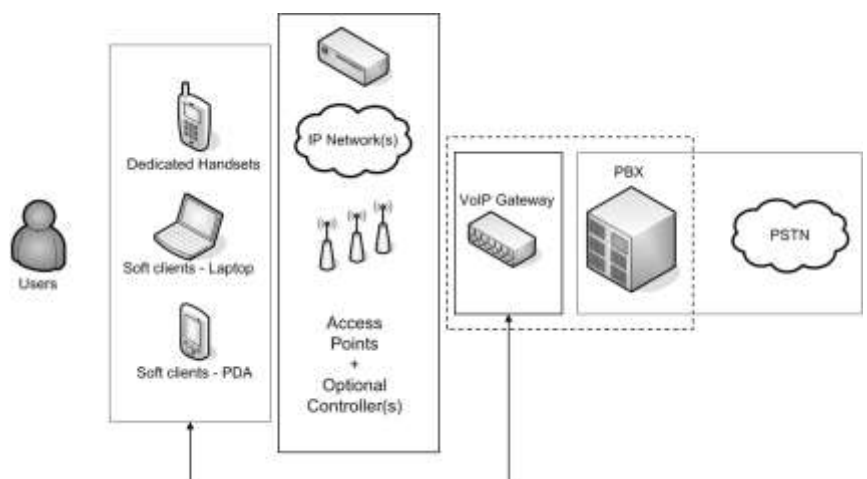
Voice over WLAN – QoS & Security

Die Zugriffsmethode für WLANs basiert derzeit meist noch auf CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Damit können keine QoS Merkmale geliefert werden.

Der IEEE 802.11e Standard beschreibt einige Erweiterungen, um diese Merkmale in einer WLAN Umgebung zu ermöglichen. Einige Unterfunktionen dieses Wireless Standards werden als WiFi Multimedia (WMM) vermarktet.

WMM eignet sich vor allem für Video- und Sprachübertragungen. Für den Kanalzugriff (Medium Access Control - MAC) sind in IEEE 802.11 zwei Verfahren spezifiziert worden: Die Distributed Coordination Function (DCF) ist ein verteilter, zufallsgesteuerter Zugriffsmechanismus (Carrier Sense Multiple Access with Collision Avoidance, kurz: CSMA/CA), der einen Best-Effort-Dienst liefert. Die Point Coordination Function (PCF) ist ein zentral gesteuerter Mechanismus, bei dem die beteiligten Stationen in regelmäßigen Abständen durch einen Master (typischerweise ein Access Point) per Polling ein Senderecht erhalten. Auf diese Weise kann für die beteiligten Stationen eine gewisse Bandbreite zugesichert werden. Die Implementierung der DCF ist in IEEE 802.11 zwingend vorgeschrieben, die Realisierung der PCF ist jedoch nur als optional klassifiziert. Daher ist es nicht verwunderlich, dass in allen bekannten

Implementierungen lediglich die DCF umgesetzt wurde. Da DCF zufallsgesteuert in einem Shared Medium wie Wireless LAN arbeitet, ist bei dieser Technik jedoch keine Bandbreitengarantie möglich – die Latenzzeit kann stark schwanken (Jitter), was für VoIP sehr negative Auswirkungen auf die Sprachqualität hat.



Komponenten einer VoWLAN-Lösung

Aus den oben genannten Gründen verwenden die meisten VoWLAN-Phone Hersteller eine Kombination aus standardbasierten und proprietären Mechanismen, um ein schnelles Hand-Over von AP zu AP zu ermöglichen. Das Ziel dieses Roamingvorganges ist es, ein für den Anwender nicht merkbares Wechseln der Funkzelle zu ermöglichen.

Bei den heute am meisten verwendeten Codecs G.711 und G.729 beträgt die maximal zu akzeptierende Roamingzeit ca. 50ms.

Class	Applications	Traffic	Latency Delay	Packet Loss Sensitivity
Background	FTP Email	Bidirectional/Asymmetric Variable Pkts	Unbounded <5-10s	Low
Interactive	Web Telnet	Bidirectional/Asymmetric Variable Pkts	Tolerable <1s	Low
Fast Interactive	Video Gaming	Bidirectional/Asymmetric Variable Pkts	Tolerable <100ms	High
Non-RT Streaming	VOD Cable TV	Unidirectional Large Pkts / Multicast	Bounded <5s	Low
RT Streaming	IP TV	Unidirectional Large Pkts / Multicast	Bounded <1s	High
Conversational	VoIP Video Phone Internet Game	Bidirectional Small Pkts (VoIP, Gaming) Large Pkts	Strict & Low <50ms	High

Als Roaming-Vorbereitung eines VoWLAN-Clients ist es nötig, dass dieser die APs in seinem Sendebereich kennt. Um dies umzusetzen, senden die Clients Probe-Requests. Manche VoWLAN-Clients können so konfiguriert werden, dass nur bestimmte Kanäle (1,6,11) gescannt werden. Oder es werden spezielle Elemente in den AP Beacons verwendet, um die Scangeschwindigkeit zu verbessern. Ebenso können manche Endgeräte so eingestellt werden, dass sie das Scannen erst bei Erreichen eines bestimmten Schwellenwerts beginnen. Dieser liegt meist bei -65 bis -70dBm. Diese Funktionen verbessern die Akkulaufzeiten und sorgen für ein schnelleres Roaming. Eine der größten Hürden in Bezug auf schnelles Roaming beim Ausrollen von VoWLAN-Lösungen sind die Verschlüsselungstechniken. Das beste Roamingverhalten wird bei unverschlüsseltem Verkehr oder mit WEP mit unter 8ms erreicht. Dieser Wert umfasst die Zeitspanne vom letzten erfolgreich gesendeten Paket auf dem alten AP bis zu dem ersten erfolgreich gesendeten Paket auf dem neuen AP.

Durch die Einführung von 802.11i wurde die Sicherheit in WLAN-Netzen drastisch erhöht, speziell auf 802.1x-basierende Implementierungen, allerdings auf Kosten eines schnellen Roamingvorgangs. Durch die Einbeziehung eines RADIUS Servers bei diesem Standard innerhalb jedes Authentifizierungsvorgangs werden die Roamingzeiten auf 50-200ms erhöht. Selbst unter besten Voraussetzungen mit einem lokalen, nicht unter Last stehenden RADIUS Server, werden sehr schnell die gewünschten 50ms

überschritten. Dies wird durch den Einsatz von WPA-PSK umgangen. Beide dazugehörigen Standards, WPA-PSK und WPA2-PSK, erreichen fast ein ähnliches Sicherheitsniveau wie die 802.1x-Implementierung, jedoch ohne Einbeziehung einer RADIUS Abfrage. Zusätzlich zu den einfachen Verfahren ohne Verschlüsselung oder WEP wird jedoch bei jedem Roamingvorgang die Erzeugung von Keys vorgenommen. Dieser Vorgang führt zu einer Verzögerung von weniger als 7ms bei WPA-PAS und 5ms bei WPA2-PSK. Dies führt in der Summe zu Gesamtroamingzeiten von 13-15ms. Das ist eine erhebliche Verbesserung gegenüber Verfahren, die einen RADIUS Server ansprechen.

Allerdings ergeben sich durch den Einsatz von WPA-PSK auch einige Nachteile. So ist diese Technologie, wie alle Preshared-Key-Technologien, anfällig gegenüber Wörterbuchattacken, sobald ein einfacher Verschlüsselungskey gewählt wurde. Weiterhin ist das Ändern des Keys auf den Endgeräten meist mit einem Konfigurationsaufwand auf jedem Endgerät verbunden. Diese Punkte treffen für eine auf RADIUS Abfrage basierende Technologie nicht zu. Um die zusätzlich benötigten schnellen Roamingvorgänge für VoWLAN umsetzen zu können, wurden zwei neue Technologien entwickelt: OKC und Pre-Authentication.

Opportunistic Key Caching (OKC) verteilt den Key, den ein WLAN-Phone bei der ersten RADIUS Abfrage (für gewöhnlich beim Einschalten) erhält, auf alle APs, die den Service beinhalten. Bei einem Roamingvorgang ist es nun nicht mehr nötig, den RADIUS Server abzufragen, da sich der passende PMK bereits auf den APs befindet. Dadurch ergeben sich Roamingzeiten wie bei der PSK-Variante mit den Security-Vorteilen einer RADIUS Infrastruktur. Allerdings wird das Sicherheitsniveau einer vollen 802.11i Implementierung nicht erreicht, da der gleiche PMK auf alle APs verteilt und für die Authentifizierung und Verschlüsselung benutzt wird. 802.11i fordert jeweils einen neuen PMK per Session pro AP. Zur Zeit gibt es noch wenige Endgeräte, die OKC unterstützen.

Pre-Authentication ist eine Lösung, die eine volle RADIUS Abfrage an jedem AP benutzt. Dieser Vorgang, der mithilfe des Roamings stattfindet, ist erheblich zeitsparender. Mit Pre-Authentication führt das Endgerät eine vollwertige RADIUS basierende Authentifizierung beim erstmaligen Verbinden mit einem AP durch. Danach scannt das Endgerät nach jedem AP in der Umgebung mit der selben ESSID (aber anderen BSSID) und nutzt seine existierende Verbindung zur Infrastruktur, um eine vollwertige RADIUS Authentifizierung an den umgebenden APs durchzuführen, bevor der Roamingvorgang stattfindet. Der PMK wird sowohl von dem AP als auch Endgerät für eine spätere Benutzung vorgehalten. Bei einem Roamingvorgang wird über diesen Key ein Sessionkey je AP generiert. Der Zeitaufwand hierfür ist vergleichbar mit dem bei WPA-PAK. Pre-Authentication ist anfällig gegenüber Infrastrukturen mit hoher AP-Dichte und sehr mobilen Endgeräten. Dies kann zu Situationen führen, bei denen ein Roamingvorgang stattfindet, bevor die Pre-Authentication durchgeführt wurde. Die Technologie gilt als sicherer als OKC, ist aber erst auf wenigen Endgeräten verfügbar.

Load Balancing in VoWLAN-Umgebungen wird durch eine von mehreren Call Admission Control (CAC) Funktionen erreicht. Extreme Networks WLAN benutzt hierzu

TSPEC, wobei ein Endgerät eine Traffic-SPECification (TSPEC) erstellt und diese an den AP sendet. Dieser reserviert die angekündigte Menge an Up- und Down-Stream Bandbreite. Die Implementierung erlaubt es, Limits für neue und bestehende Roaming-Verbindungen zu setzen. Weiterhin können Bandbreitenreservierungen in unabhängigen Klassen gemacht werden, in denen z. B. Voice eine höhere Priorität bekommt als Video. Die Implementierung beim Extreme Networks WLAN geht sogar soweit, dass spezielle Aktionen definiert werden können, sobald die angekündigte Up- und Down-Stream Bandbreite überschritten wird, was auf einer per SSID-Basis geschieht.

Location-Tracking in WLAN Netzen

Eine weitere Technologie, die erst durch WLAN Switching ermöglicht wurde, sind Location Based Services. Mit Hilfe dieser Technologie können Geräte geortet werden, die ein WLAN Radio besitzen (Notebooks, VoWLAN Phones) sowie dedizierte Location Tags, in denen z.B. Panic-Buttons und Bewegungssensoren integriert sind. Diese können an wichtigen Gütern, z.B. mobilen Infusionspumpen im Krankenhausbereich oder an Staplern in der Logistik, befestigt werden. Durch die lokationsbezogenen Daten kann sehr einfach eine Prozessoptimierung durchgeführt werden, wie beispielsweise standortabhängige Disponierung von Staplern im Logistikbereich.

Für die Ortung selbst werden verschiedene Technologien eingesetzt:

- **Anwesenheit:** Ein Tag sendet zyklisch oder bei Bewegung ein kurzes Signal. So wird sichergestellt, dass immer die aktuelle Lokation angezeigt wird.
- **Echtzeit:** Ein Client/Tag wird gezielt vom User/System abgefragt und die aktuelle Lokation zurückgemeldet.
- **Lokationsbezogen:** Ein Tag wird bei Passieren einer bestimmten Lokation über einen so genannten Exiter gezwungen, seine Lokation an das System zu melden.

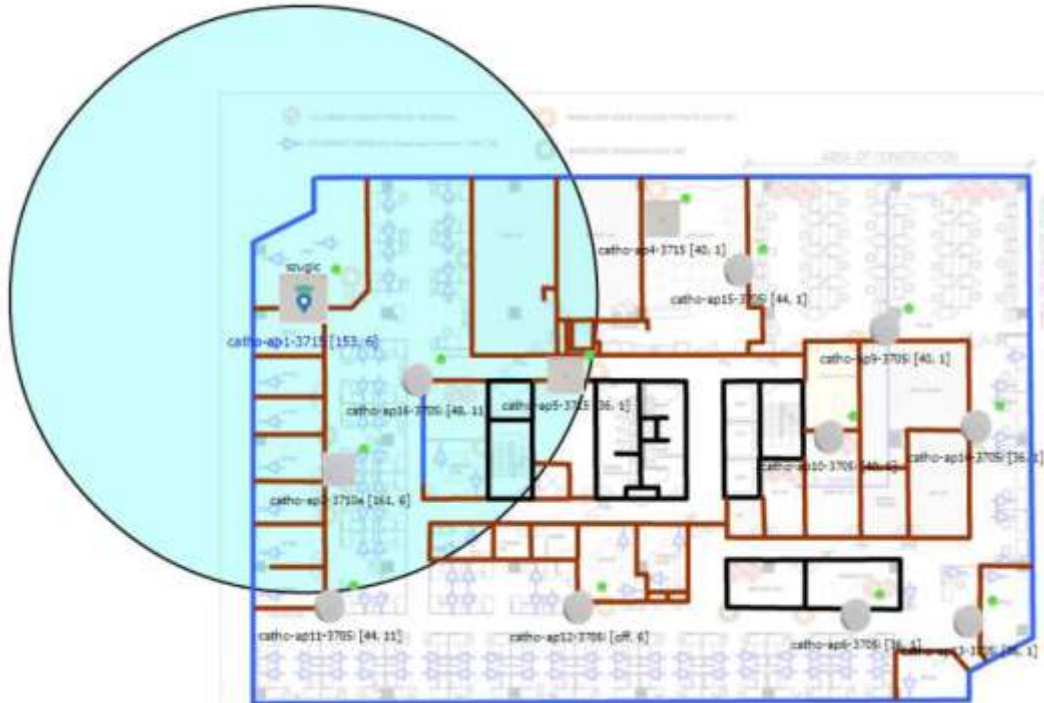
Weiterhin gibt es verschiedene Ortungsmethoden:

AP Connection und RSSI-Wert

- Zur Lokationsbestimmung wird die Client Sendestärke verwendet
- Bekannte AP Lokationen und Client RSSI-Werte ermöglichen Distanzangaben
- Ab einer Anzahl von 3 Distanzwerten (APs) kann die Lokation per Triangulation genau bestimmt werden
- RF-Hindernisse können die Qualität der Werte beeinflussen
- Folgende Faktoren können die Werte verbessern:
 - Anzahl der APs, die den Client sehen
 - Geometrie der APs
 - Qualität des RF-Models des Gebäudeplans

Die abgedruckten Bilder aus dem Extreme Management Center zeigen die Lokalisierungsmöglichkeiten der einfachen RSSI Umkreislokation sowie die „Wahrscheinlichkeitswolke“ aus der Triangulation heraus.

Cell of Origin



Triangulation: Good location



Serverbasierendes Pattern Matching

- Das von mehreren APs gesehene RSSI-Pattern eines Clients wird als eindeutiger „Fingerabdruck“ klassifiziert
- Hat ein weiterer Client den selben RSSI-Pattern, ist er an der gleichen Lokation
- Client Sendestärke ist hierbei nicht relevant
- kein RF-Model des Gebäudes notwendig

ExtremeWireless ermöglicht Location Tracking über die hier genannten Methoden. Als Frontend-Applikation kann NMS-ADV eingesetzt werden. Weiterhin ist ab der Version 9.15 ein zyklisches Abfragen von Clientlokationen via XML/PHP-Script möglich, um damit weitere Applikationen zu versorgen.

Das Extreme Management Center fasst ab Version 7 die Location Tracking Informationen zentral zusammen und tauscht sie über die ExtremeConnect API mit anderen Applikationen aus.

802.11n – Grundlagen in der Retrospektive

Der in 2008 ratifizierte Standard 802.11n hat einige Änderungen und Verbesserungen in die WLAN Technologie gebracht, auf die in dem Folgestandard 802.11ac aufgebaut wird. Aus technischer Sicht sind dies 3 Hauptkomponenten:

Multiple Input Multiple Output (MIMO) Technologie

Bei 11a/b/g wurde bisher die gesamte Datenmenge über eine Antenne gesendet und empfangen. Mit der MIMO Technologie wird der Datenstrom über einen Splitter auf zwei oder mehr Sende-/Empfangsantennen aufgeteilt.

Die Anordnung der Antennen auf den WLAN Komponenten ist so gestaltet, dass die Ausbreitung des Funksignals räumlich versetzt erfolgt und es so zu keinen gegenseitigen Störungen bei der Übertragung kommt. Während erste WLAN Technologien Reflexionen eher als Problem erlebten, nutzt MIMO diese bewusst und erreicht dadurch einen erhöhten Durchsatz, sowie auch eine robustere Kommunikation.

Kanalbündelung

Der einfachste Weg, um den Durchsatz in einem WLAN Netz zu erhöhen, ist die Verdopplung des genutzten Frequenzbandes. 11n nutzt dies, um 2 benachbarte 20 Mhz-Kanäle zusammen zu fassen. Diese Technologie ist am effektivsten im 5 Ghz Bandbereich, in dem 19 überlappungsfreie 20 Mhz-Kanäle zur Verfügung stehen. Im 2,4 Ghz-Bereich ist diese Technik weniger effektiv, da bereits mit der alten Technologie nur 3 überlappungsfreie Kanäle verfügbar sind. Kanalbündelung reduziert dies auf einen Kanal, was einen professionellen Einsatz in MultiAP-Topologien ausschließt.

Packet Aggregation

Bei konventionellen WLAN Techniken ist der Overhead für den Transport eines Frames fix, unabhängig von dessen Größe. 11n erlaubt die Verkettung von Nutzdatenframes zu

einem einzigen Sende-Frame. Dadurch können mehrere Pakete mit den Overhead-Kosten eines einzigen Pakets gesendet werden. Die Effektivität dieser Technologie ist je nach Anwendung verschieden. Besonders groß ist der Vorteil z. B. bei großen Filetransfers - Echtzeitanwendungen wie Voice oder Video profitieren nicht davon.

802.11n - Mehrwerte

Erhöhte Kapazität

Bei 11n wird die Kapazität einer WLAN Zelle von 14-22 Mbps bei 11a/g auf 100-200 Mbps erhöht. Verteilt auf mehrere User pro Zelle sind damit Geschwindigkeiten von bis zu 100 Mbps pro User möglich, was sich in der Praxis in einer größeren Bandbreite für mehr User zeigen wird.

Erhöhte Reichweite

Durch die MIMO Technologie und das bewusste Arbeiten mit Reflexionen durch die räumlich versetzte Funkausbreitung der Funkwellen wird die Reichweite je AP erhöht. Die Datenrate reduziert sich mit steigendem Abstand vom AP zum Client weniger als bei den bisherigen Technologien und erreicht somit eine größere Abdeckung mit weniger APs.

Höhere Verfügbarkeit / Robustheit

Die Performance bisheriger Technologien konnte bereits durch Verlagerung oder Änderungen in der Umgebung (Schließen einer Tür, veränderte Raumeinrichtung) stark beeinträchtigt werden. Die MIMO Technologie trägt dazu bei, mit mehreren aktiven Antennen die Robustheit und Verfügbarkeit erhöhen.

Design

Durch die Abwärtskompatibilität von 802.11n mit a/b/g wird auch die Performance in einer 11n-Funkzelle auf die Geschwindigkeit der bisherigen Technologien verringert. Der größte Teil der bisherigen WLAN Clients arbeitet im 2,4 Ghz-Bereich. Durch die Einschränkung bei der Kanalbündelung in diesem Frequenzband und einer oft geforderten Unterstützung bereits bestehender WLAN Clients wird 11n im 2,4 Ghz-Bereich noch oft in einem Kompatibilitätsmodus betrieben. Der 5 GHz-Bereich spielt hingegen mit dem breiteren Kanalspektrum Funktionen wie Kanalbündelung voll aus. Abwandlungen dieses Designs können je nach Anforderungen und Randbedingungen auftreten, so z. B. wenn man komplett neue WLAN Netze (Access Points & Clients unterstützen 11n) aufbaut (Greenfield) oder wenn ein komplett unabhängiges 11n-Netz zu einem bestehenden 802.11a/b/g Netz aufgebaut wird (Overlay).

802.11ac – Gigabit WLAN Wave 1 und 2

Haben Sie den letzten Abschnitt genau gelesen? Gut. Denn auf diesen Grundlagen baut 802.11ac auf. Schneller, höher, weit....nein. Nicht weiter. Nach wie vor begrenzen die Regulierungsbehörden dieses Planeten die Ambitionen der WLAN Hersteller, HF-Komponenten der APs immer leistungsfähiger zu dimensionieren.

Und das ist sogar gut. Denn mit 802.11ac wird das Betreiben kleiner Funkzellen zum kritischen Faktor, um die zugesicherten Bandbreiten auch praktisch zu erreichen.

Aber schauen wir uns doch zunächst die Techniken an, mit denen der Performancezuwachs erzielt wird:

Höhere Datenraten: Potential für Gigabit- und Multi-Gigabit-Geschwindigkeiten - im Vergleich zu maximal 450Mbps mit 11n (per Funk)

Client	MIMO Spatial Streams	20 MHz Channel (Mbps)	40 MHz Channel (Mbps)	80 MHz Channel (Mbps)
11ac	1x1:1	86,7	200	433,3
	2x2:2	173,4	400	866,6
	3x3:3	260	600	1300
	4x4:4	346,8	800	1733,3
11n	1x1:1	72,2	150	N/A
	2x2:2	144,4	300	N/A
	3x3:3	216,7	450	N/A
11abg	a/g	54	N/A	N/A
	B	11	N/A	N/A

Mit 8 Spatial Streams definiert der Standard eine maximalbandbreite von 6,9Gbps.

Breitere Kanäle: Der Standard erlaubt - verglichen mit 20MHz und 40MHz bei 11n - Kanalbündelungen bis 80 bzw. 160MHz. In der Praxis führt dies zu kontroversen Diskussionen. Im privaten Consumerbereich ist die Nutzung des gesamten Kanalspektrums durchaus legitim - sofern der Nachbar nicht auf die gleiche Idee gekommen ist. Dann kann sich die Nettobandbreite aufgrund der Interferenzen rapide reduzieren.

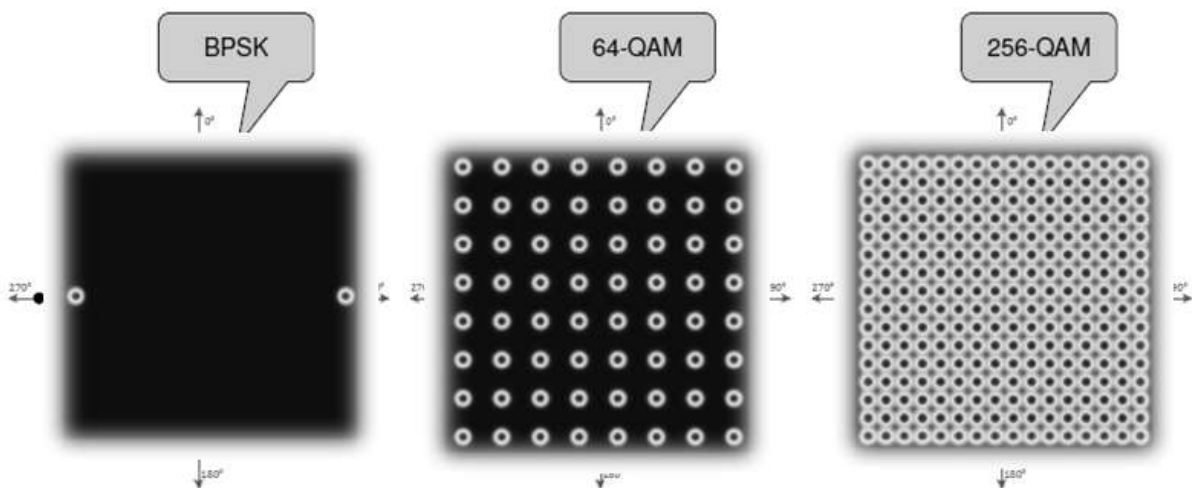
Das professionelle Unternehmensnetz besteht jedoch aus einer zwei- bis dreidimensionalen Matrix aus benachbarten Access Points. Hier ist ein Kanalplan

erforderlich, welcher den gegenseitigen Einfluss auf einem Minimum hält. In einem entsprechend dicht gesetzten WLAN kann die grössere Kanalvarianz gegenüber höherer Kanalbandbreite von Vorteil sein.

Zusätzliche Spatial Streams: Bis zu 8 Spatial Streams werden vom 11ac Standard unterstützt. Momentan verfügbare Hardware bietet 4 Spatial Streams an. Bisher verfügen nur wenige Endsysteme über vier Antennen, dieses Feature ist eher auf die Zukunft ausgerichtet.

Multi-User MIMO umschreibt die Fähigkeit, mehrere Stationen auf dem gleichen Kanal zur gleichen Zeit zu bedienen - im Vergleich zu maximal einer Station bei 11n. Diese vielversprechende Technologie nutzt das bestehende Shared Medium wesentlich effizienter.

Höhere Modulationsverfahren: Das folgende Bild macht es deutlich - BPSK kannte für den Urstandard 802.11 zwei Zustände: 0 und 1. Bei 11n überträgt die sogenannte Quadraturamplitudenmodulation 64 Symbole pro Übertragungsschritt. 11ac sattelt hier noch mit 256 Symbolen noch kräftig drauf.



Einerseits sorgt dies für eine gesteigerte Übertragungsrates. Andererseits wird die Aufbereitung des Signales ungleich kniffliger. Um diese Modulationsart fehlerfrei nutzen zu können, muss der WLAN Client die Distanz zum AP signifikant verringern.

Durch die kürzeren Sendesignale lässt sich der Energieverbrauch bis zu 40% reduzieren. Gute Nachrichten für alle mobilen Geräte die - bei gesteigerter Geschwindigkeit - in einem optimierten Netz nun auch mit längeren Akkulaufzeiten glänzen können.

Ganz nebenbei: Die neueste AP Generation unterstützt 256-QAM auch im 2,4GHz Band. Das steigert die Nettodatenrate nochmal von 600 auf 800 Mbps.

Der Blick nach vorne

WLAN Client-Karten mit 11ac werden bereits seit Anfang 2013 geliefert. Extreme Networks hat bereits heute ein vollständiges Portfolio von verschiedensten 11ac APs, um alle Anforderungen optimal abzudecken. Mag das über WLAN transportierte





Datenvolumen auch in den nächsten Jahren massiv ansteigen; aktuelle Controller sind in der Lage, diesen Verkehr zentral wie auch dezentral ins LAN einzuspeisen – die Skalierung ist sichergestellt.

Bei heutigen Planungen empfehlen wir das 5 Ghz Band mit zu berücksichtigen, um zukünftig einfach und ohne weitere Planungsschritte auf 11ac migrieren zu können. Die neuen 11ac WLAN-Clients sind abwärtskompatibel zu 11n, so dass ein sanfter Übergang sichergestellt ist. 802.11ac-fähige Komponenten haben sich im Markt etabliert, Investitionen in 11n Hardware bieten mittlerweile keinerlei funktionale oder monetäre Vorteile mehr.

ExtremeWireless Komponenten

Die zentral koordinierte Architektur von ExtremeWireless ermöglicht den Betrieb mobiler Anwendungen - einfach, sicher, kosteneffizient und mit hoher Verfügbarkeit.

Neue Anwendungen lassen sich damit ohne zusätzliche Investitionen in die Infrastruktur integrieren. Die Intelligenz und Flexibilität des Verbundes aus leistungsfähigem AP und zentralem Controlling sorgt für Betriebssicherheit und hohe Dienstgüte. Die Lösungen basieren auf Komponenten, die im weiteren Verlauf beschrieben werden:

		
Access Points	Appliances	Management
		
<ul style="list-style-type: none"> • Semiautonome APs • Custom Design • Hohe Sicherheit: WPA2, WIDS/WIPS, AAA, Forensik • 2x HD Video-Performance • Optimierte Antennen für bessere Funkabdeckung • GbE Ports – Kein Bottleneck • Hohe Energieeffizienz, geringer Stromverbrauch 	<ul style="list-style-type: none"> • Physikalische & virtuelle Appliances • HA ohne Unterbrechung • Flexible SFP+ (1G/10G) • Verschlüsselungs-Beschleuniger in Hardware • Unterstützung von bis zu 2.000 APs und 32.000 User / Appliance 	<ul style="list-style-type: none"> • Visibilität, Kontrolle & Automatisierung • Policy-basiertes System für WLAN und LAN • Aurtomatisches RF-Management & Spectrum-Analyse • Single SSID-Design

Individuelle WLAN-Topologien, –Designs und –Parameter für die sehr unterschiedlichen und komplexen Anforderungen der einzelnen Kunden an Verfügbarkeit, Sicherheit, Verkehrsoptimierung und Dienstgüte heutiger Netze sind mit ExtremeWireless möglich. Dieses wird durch die VNS (Virtual Network Service)-Architektur erreicht, die von allen WLAN-APs (Access Points) unterstützt wird. Die WLAN-Komponenten lassen sich direkt über das Webinterface des Controllers oder zentral über die Extreme Managementplattform administrieren. Hier stehen auch Dashboardvisualisierung, Etagenpläne mit Heatmapfunktion und ein umfangreiches Reporting zur Verfügung. Ein Gastzugang inklusive Captive Portal und Accountverwaltung wird direkt auf Controllerebene unterstützt. Für eine einheitliche Gästelösung, die den WLAN- und LAN-Zugang unterstützt, bildet Extreme Control mit flächendeckender Network Access Control die gemeinsame Ebene.




ExtremeWireless Access Points

Die ExtremeWireless Architektur setzt neben den Controllern auf die Eigenintelligenz der Access Points. Datenverkehr kann so – unabhängig von einer zentralen Instanz – mit allen nötigen Steuermechanismen wie QoS, Ratelimit oder ACLs benutzerspezifisch ins LAN eingespeist werden. Dieses Konzept semiautonomer Access Points schafft zusätzliche Flexibilität und vermeidet, dass in natürlich wachsenden WLAN Ökosystemen der Controller zum Flaschenhals mutiert.

Aus dieser weitgehenden Unabhängigkeit hat sich die ExtremeCloud Lösung entwickelt, die später im Detail beschrieben wird.

Hier zunächst eine Vergleichsübersicht der unterschiedlichen Gruppen.

Indoor Access Points

AP 3935i/e	AP 3825i/e	AP 3805i/e
Ultra-Performance + HA	High-Performance	Viele Features
<ul style="list-style-type: none"> • 11ac Wave 2, 11abgn, 4x4:4 MIMO • Cloud-Ready • 802.3at & 802.3af (Stromsparmmodus) • Mesh, Policy, QoS • WIDS, WIPS, Spectrum-Analyse • 2,5 Gbps • 90.000 pps • 2x E/N mit Active/Active und Active/Passive 	<ul style="list-style-type: none"> • 11ac, 11abgn, 3x3:3 MIMO • Dual-Radio • 802.3at & 802.3af (Stromsparmmodus) • Mesh, Policy, QoS • WIDS, WIPS, Spectrum-Analyse • 1,75 Gbps • 75.000 pps • 2x E/N mit Active/Active und Active/Passive 	<ul style="list-style-type: none"> • 11ac, 11abgn, 2x2:2 MIMO • Dual-Radio • 802.3af PoE • Mesh, Policy, QoS • WIDS, WIPS, Spectrum-Analyse • 1,16 Gbps • 40.000 pps • Rauchmelderdesign
		

ExtremeWireless 3805 Indoor Access Point

Der AP3805i/e ist ein funktionsreicher 802.11ac/abgn Access Point. Speziell entwickelt, um sich harmonisch in Büroräume, Klassenzimmer, oder Hotel-Umgebungen einzufügen, eignet sich AP3805i/e besonders gut, um sichere WLAN-Konnektivität in mitteldichten Umgebungen bereitzustellen.



Mit zwei Radios, je zwei Antennen und zwei Spatial Streams verfügt das Modell über eine max. Performance von 1.17 Gbps über die WLAN- und bis zu 40.000 Pakete pro Sekunde über die LAN-Schnittstelle.

Der AP 3805i/e wird mit den fortschrittlichsten, derzeit erhältlichen, 11ac-Eigenschaften geliefert. Dazu gehören dynamisches Funk-Management, Beamforming, Spektrumanalyse mit Störungserkennung und Klassifizierung, Selbstreparatur und AP-Vermaschung sowie rollenbasierte Authentifizierung und Autorisierung. Unter Volllast verbraucht das Gerät maximal 9 Watt. Extreme Networks liefert den AP mit lebenslanger Garantie (Extreme Networks Lifetime Warranty). Die internen Antennen des 3805i besitzen produzieren ein weitgehend kugelförmiges Abstrahlprofil. Dies begünstigt die einfache Decken- oder Wandmontage ohne zusätzliche Montageeinrichtungen oder andere Optionen. Erfordert das Umfeld besondere Massnahmen empfiehlt sich der Einsatz des Modells AP3805e mit zusätzlichen, externen Antennen.

ExtremeWireless 3801 Indoor Access Point

Eine Sondervariante des AP3805i ist sein, in Funktion und Aussehen nahezu identischer kleiner Bruder, der AP3801. Dieser 802.11ac/abgn Access Point nutzt ebenfalls die neueste Advanced-11ac-Funktechnologie. Auch er basiert auf einer 2x2:2 Plattform. Als „Single Radio“ Access Point, unterstützt der AP3801 jedoch wahlweise das 2.4GHz- oder das 5GHz-Frequenzspektrum.

Der AP 3801 ist für ein sehr günstiges Preissegment konzipiert und bietet damit den LowCost Einstieg in die Welt von 802.11ac.

Vor die Entscheidung für dieses Modell sollten jedoch klare Überlegungen hinsichtlich des geplanten Umfeldes getroffen werden. Ein reinrassiges 2,4GHz Modell ist, nach heutigem Stand keine Option mehr. Das ISM Band wird von zahlreichen Anwendungen regelrecht zugemüllt. Aktuelle Clientsysteme unterstützen meist beide Frequenzbänder. Daher sollte der Weg zu 5GHz nicht verbaut werden.

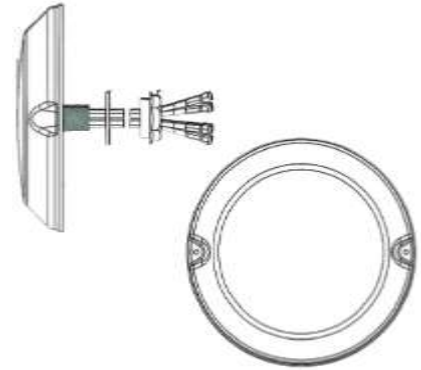
Der logische Schritt zu einer ausschliesslichen 5GHz Infrastruktur ist sehr konsequent, berücksichtigt jedoch nicht die Vielfalt noch bestehender Systeme. Gerade der Logistik- und Fertigungsbereich beinhaltet zahlreiche Komponenten die auf 2,4GHz Unterstützung angewiesen sind.

ExtremeWireless 3825 Indoor Access Point

Der Indoor AP3825 eignet sich speziell für Installationen mit hoher Nutzerdichte, in denen auch breitbandige Video- und verzögerungssensitive Sprachanwendungen übertragen werden. Das Modell AP3825i lässt sich durch seine integrierte Matrix von sechs Antennen einfach installieren und ist dabei ebenso unauffällig wie sein Vorgänger, der AP3715.



Der AP3825e verfügt über sechs RP-SMA Antennenanschlüsse für das 2.4GHz- bzw. 5GHz-Band. Neben den klassischen „Hörnchen“ steht ein Portfolio von Multifeedantennen mit Rundstrahl- oder Richtcharakteristik für den Einsatz in besonderen Umgebungen bereit. Eine solche Antenne wird über 3 bzw. 6 Anschlussleitungen mit den Ausgängen des AP verbunden.



Die Stromversorgung erfolgt regulär über PoE gemäss dem Standard IEEE 802.3af alternierend an einem der beiden LAN Ports. Ein Anschluss zur lokalen Stromversorgung ist ebenfalls vorhanden. In der Praxis gestaltet sich diese durch den Verlegeaufwand der Netzspannungsversorgung recht aufwändig; PoE hat sich hier eindeutig als die bessere Lösung etabliert.

Extreme Networks liefert den AP mit lebenslanger Garantie (Extreme Networks Lifetime Warranty). Die AP3825-Serie unterstützt alle 11ac Wave1 Wi-Fi-Technologien: dynamisches Funkmanagement, Spektrumanalyse mit Störungsklassifizierung und -vermeidung, Selbstreparatur und Vermaschung sowie rollenbasierte Authentifizierung und Autorisierung. Die 3x3:3 AP- Plattform verfügt über eine max. Performance von 1.7 Gbps über die WLAN- und bis zu 75.000 Pakete pro Sekunde über die LAN-Schnittstelle. Umfassende Antennenoptionen sorgen für flexible Einsatzmöglichkeiten des AP3825e.

Über eine zweite Ethernet-Schnittstelle kann eine redundante Anbindung inkl. Lastausgleich an den Access-Switch-Bereich erfolgen.

ExtremeWireless 3935 Indoor Access Points

Zum Ende des Jahres 2015 wurde bei Extreme Networks die zweite Welle des 802.11ac Standards angekündigt. 8 Antennen für zwei Radios, 4 Spatial Streams in MU MIMO Technologie – das sind nur die einfachen Eckdaten, mit denen der neue AP punktet. Das robust anmutende Gerät lässt mit 1,7Kg Gewicht vermuten, dass hier einiges an Leistung verbaut ist. Gute 20% mehr Durchsatz für bis zu 480 Userpositionieren den 3935 an die Spitze des High Density Bereiches. Die zweite Welle bringt neben MU-MIMO neue Modulationsverfahren (QAM256) und breitere Kanalbündel mit – wichtige Werkzeuge um künftige Anforderungen zu erfüllen.






Wie die anderen Modelle der Extreme Wireless AP-Familie wird auch dieser Accesspoint mit internen Antennen bzw. externen Anschlüssen angeboten. Multifeedantennen decken mit ihrer Rundstrahl bzw. Richtcharakteristik die verschiedensten Szenarien ab.

Spezifikationen und Bestellinformationen zu Indoor APs finden Sie unter:

www.extremenetworks.com/products/wireless

Outdoor Access Points

AP 3965i	AP 3965e	AP 3865e
High-Performance + HA	High-Performance + HA	
<ul style="list-style-type: none"> • 11ac Wave 2, 11abgn, 4x4:4 MIMO • Cloud-Ready • Dual-Radio • 802.3at PoE • Mesh, Policy, QoS • WIDS, WIPS, Spectrum-Analyse • 2,5 Gbps • 90.000 pps • 2x E/N mit Active/Active und Active/Passive • IP67/NEMA6 • Integrierte Antennen 	<ul style="list-style-type: none"> • 11ac Wave 2, 11abgn, 4x4:4 MIMO • Dual-Radio • 802.3at PoE • Mesh, Policy, QoS • WIDS, WIPS, Spectrum-Analyse • 2,5 Gbps • 90.000 pps • 2x E/N mit Active/Active und Active/Passive • IP67/NEMA6 • Externe Antennen 	<ul style="list-style-type: none"> • 11ac, 11abgn, 3x3:3 MIMO • Dual-Radio • 802.3at PoE • Mesh, Policy, QoS • WIDS, WIPS, Spectrum-Analyse • 1,75 Gbps • 75.000 pps • Rauchmelderdesign • 2x E/N mit Active/Active und Active/Passive • IP67/NEMA6 • Externe Antennen
		

ExtremeWireless 3865e Outdoor Access Point

Der AP3865e ist, als Vorläufer des neuen AP3965 - ein Hochleistungs-802.11ac/abgn Outdoor AP. Er stellt die drahtlose Mobilität in Außenbereichen und Umgebungen mit harten Witterungseinflüssen wie Lagerhallen, Minen, Fabriken und Stadien bereit. Der AP3865e wird standardmäßig mit sechs Antennen N-Type Antennenanschlüssen mit integrierten Blitzschutz geliefert. Der AP wird via 802.3at PoE (Power over Ethernet) oder über ein optionales, externes und outdoortaugliches Netzteil mit Strom versorgt.



Auch der AP3865e unterstützt alle neuen 1st Wave-11ac Wi-Fi-Technologien: dynamisches Funkmanagement, Spektrumanalyse mit Störungsklassifizierung und -vermeidung, Selbstreparatur und Vermaschung sowie rollenbasierte Authentifizierung und Autorisierung. Die 3x3:3 AP-Plattform verfügt über eine maximale Performance von bis zu 1,75 Gbps über die WLAN- und bis zu 75.000 Pakete pro Sekunde über die

LAN-Schnittstelle. Umfassende Antennenoptionen sorgen für flexible Einsatzmöglichkeiten des AP3865e.

ExtremeWireless 3865i Outdoor Access Points

Weitgehend baugleich mit dem 3865e wird der AP3865i standardmäßig mit einer integrierten Matrix aus sechs Antennen geliefert. Auch die AP3865-Serie unterstützt alle Advanced-11n/ac Wi-Fi-Technologien: dynamisches Funkmanagement, Spektrumanalyse mit Störungsklassifizierung und -vermeidung, Selbstreparatur und Vermaschung sowie rollenbasierte Authentifizierung und Autorisierung.

Die 3x3:3 AP-Plattform verfügt über eine maximale Performance von bis zu 900 Mbps über die WLAN- und bis zu 60.000 Pakete pro Sekunde über die LAN-Schnittstelle. Umfassende Antennenoptionen sorgen für flexible Einsatzmöglichkeiten mit Rundstrahl- bzw. Richtcharakteristiken.

ExtremeWireless 3965 Outdoor Access Points

Mit der Vorstellung des AP3965 schwappt die zweite Welle von 802.11ac in die Outdoorzone. Ein Array aus 8 integrierten Antennen vereinfacht die Montage des -i Modells. Für komplexere Anwendungsszenarien lässt sich der AP3965e mit einem breiten Spektrum von Rundstrahl- und Richtantennen ausrüsten. Der AP3965e bietet acht Reverse Polarity-SMA-Anschlüsse, getrennt für 2.4GHz- und 5GHz. Die APs werden via 802.3at PoE (Power over Ethernet) mit Strom versorgt.



Auch die AP3865-Serie unterstützt alle Advanced-11n/ac Wi-Fi-Technologien: dynamisches Funkmanagement, Spektrumanalyse mit Störungsklassifizierung und -vermeidung, Selbstreparatur und Vermaschung sowie rollenbasierte Authentifizierung und Autorisierung. Die 4x4:4 AP-Plattform verfügt über eine maximale Performance von bis zu 2,5 Gbps über die WLAN- und bis zu 90.000 Pakete pro Sekunde über die LAN-Schnittstelle. Umfassende Antennenoptionen sorgen für flexible Einsatzmöglichkeiten mit Rundstrahl- bzw. Richtcharakteristiken.

Spezifikationen und Bestellinformationen zu Outdoor APs finden Sie unter:

www.extremenetworks.com/products/wireless

ExtremeWireless Appliances

Aktuell umfasst das ExtremeWireless Hardwareportfolio drei Controllermodelle, welche alle mit selber Funktionalität ausgestattet sind. Sie unterscheiden sich lediglich in der Hardware und in der Anzahl der unterstützten APs.

Paarweise im Hochverfügbarkeitsmodus gekoppelt, erreichen die Controller eine Resilienz gegenüber Störeinflüssen, welche den Betrieb kritischer Anwendungen sicherstellt. Angeschlossene APs wechseln reibungslos von einer Primär- zu einer Backup-Appliance. Dies ist optimal für hochverfügbare VoWLAN-Umgebungen, denn es kommt selbst dann zu keiner Gesprächsunterbrechung, wenn eine Appliance

ausfallen sollte. Zusätzliche Lizenzen für die Backup- Appliance sind nicht erforderlich. Mit dem richtigen WLAN-Design kann auch bei vollständigem Ausfall der Appliances weiterhin ein WLAN-Service angeboten werden, der selbst beim Reboot des APs, zusätzlich zu einem Ausfall der Appliance, funktioniert.

Mitgeliefert wird der Extreme Networks-Assistent für die Konfiguration der WLAN-Infrastruktur. Zusätzlich zu den Appliances und Lizenzen für die gewünschte Menge an APs, wird pro Hardwareappliance ein „Regulatory Domain Key“ bestellt, um die gesetzlichen Bestimmungen hinsichtlich Leistung und Kanalwahl einzuhalten. In Europa ist dies „WS-CTLREGxP-ROW“, bei der virtuellen Appliance „WS-V2110-x-ROW“.

ExtremeWireless Appliances		
C35	V2110	C5210
Entry-Level	Virtualisiert	Mid/High-End
<ul style="list-style-type: none"> • 50-125 Access Points • 250 APs im HA-Modus • 4 GE Interfaces • GE Mgmt Port • 2.000 User • 4.000 User im HA-Modus • Lifetime Warraty 	<ul style="list-style-type: none"> • VMware ESXi 5.1 • Hyper-V • 8-250 Access Points • 500 APs im HA-Modus • 2 GE Interfaces • GE Mgmt Port • 4.096 User • 8.192 User im HA-Modus 	<ul style="list-style-type: none"> • 100-1.000 Access Points • 2.000 APs im HA-Modus • HW Crypto Beschleuniger • 2 SFP+ Interfaces • 2 GE Interfaces • GE Mgmt Port • 16.000 User • 32.000 User im HA-Modus

Elastic V2110: System Limits

Als sogenannte „Elastic Appliance“ lässt sich der virtuelle Controller V2110, mit abgestuften Ressourcen der bereitgestellten virtuellen Plattform ausstatten. So ergeben sich 3 Skalierungsvarianten mit unterschiedliche hohen Eckdaten für die Anzahl von Accesspoints und Benutzern.

Configuration	Small	Medium	Large
Host Resources	2 CPU 1 GB RAM 25 GB HDD	4 CPU 2 GB RAM 25 GB HDD	8 CPU 4 GB HDD 25 GB HDD
System Limits			
AP Capacity	100	500	1050
Local AP	50	250	525
High Availability	50	250	525
User Capacity	1024	4096	8192
Standalone Users	512	2048	4096
High Availability	512	2048	4096
Max Number of WLAN Services/VNS	32	128	256
Max Number of Active WLAN services	16	64	128
Max Number Topologies	32	128	256
Max Number Policies/Roles	128	512	1024

Spezifikationen und Bestellinformationen unter www.extremenetworks.com/products/wireless

ExtremeWireless Radar

Ab der AP37xx-Serie aufwärts sind die erweiterte Spektrumanalyse, Funkmanagement und Funktionen für Eindringerschutz und -vorbeugung (IDS & IPS) verfügbar. So kann die Lösung proaktiv auf Änderungen im Funkspektrum und Angriffe reagieren. Das steigert Verfügbarkeit und Security der Gesamtlösung.

Zu ExtremeWireless Radar gehören folgende Komponenten:

- **ExtremeWireless Radar RF Security:** Alle 37/38/39XX-APs unterstützen WIPS/WIDS (Wireless IDS/IPS). Die 3705 und 3710 Access Points bieten kanalintegrierte IDS&IPS auf allen Kanälen, die der AP gerade für den WLAN-Service nutzt, ohne die Versorgung der Clients dadurch zu stören oder zu unterbrechen. Alle APs der 3710/15 sowie der 38/39XX Serien können darüber hinaus mit Hilfe der Guardian Funktion in einen Sensor umgewandelt werden. Dieser sichert dann gleichzeitig alle Kanäle und Bänder.
- **ExtremeWireless Funk-Management:** Dynamisches Radio Management (DRM) arbeitet unabhängig auf jedem Funkmodul. Es passt Kanal- und Sendeleistungsparameter automatisch und dynamisch der Funkumgebung an, um den Empfang zu optimieren. DRM ist unabhängig von der Radar-Lizensierung auf allen APs kostenfrei verfügbar.
- **ExtremeWireless Radar RF Fingerprinting:** Alle 37/38/39XX-APs unterstützen hardwarebasiertes Spektrum Fingerprinting. Das bedeutet, dass Funkrauschen oder Störungen von anderen Funksystemen wie etwa Mikrowellen, Bluetooth- oder Video-Brücken erkannt und identifiziert werden. Sobald die APs eine Interferenz detektieren, verschiebt das Controller-System den AP manuell oder automatisiert

auf einen störungsfreien Kanal. Das sichert den Clients permanent hohe Empfangsqualität. Für diese Funktion ist je eine Radar-Lizenz je AP, der dieses Feature nutzen soll, nötig.

- **ExtremeWireless Radar Reporting:** Radar Reporting wird auf den Controllern konfiguriert. Überwachung und Berichte (Reporting & Monitoring) sind via Controller WebGUI oder das ExtremeManagementCenter möglich.

Bestellinformationen ExtremeWireless Radar:

Radar Capacity Upgrades	
WS-RADAR-1	Radar capacity for C25 and V2110. Adds Radar capacity for 1 access point.
WS-RADAR-16	Radar capacity for C25 and V2110. Adds Radar capacity for 16 access points.
WS-RADAR-25	Radar capacity for C4110, C5110 and C5210. Adds Radar capacity for 25 access points.
WS-RADAR-100	Radar capacity for C5210. Adds Radar capacity for 100 access points.

ExtremeWireless Management (WM)

Das zentrale Management der Wireless Lösung ist Bestandteil der ExtremeControl Plattform. Informationen hierzu finden Sie im Kapitel Management und Software.

ExtremeWireless Antennen

Bei den externen Antennen ist zu beachten, dass sie für die Zuständigkeitsbereiche der FCC (Federal Communications Commission) in den USA und des ETSI (European Telecommunications Standards Institute) in Europa zertifiziert sind. Diese Information findet sich in den Datenblättern der Accesspoints.

Wie bereits erwähnt: Mit strengen Richtlinien schränken die Regulierungsbehörden die Leistungsmöglichkeiten im Bereich WLAN stark ein. Mit einer immer stärkeren Ausbreitung drahtloser Netze im privaten wie auch im geschäftlichen Bereich ist dies im Sinne eines störungsfreien Nebeneinanders.

Beachten Sie der Auswahl der Antennen für Ihren Accesspoint das jeweils aktuelle Datenblatt. So können Sie sicher gehen, dass Ihre Kombination AP/Antenne optimal abgestimmt ist.

In unserer Onlinebibliothek finden Sie unter

<http://extremenetworks.com/support/documentation/> den External Antenna Site Preparation and Installation Guide.

Befestigungsoptionen

Die Frage klingt trivial, aber wie wird so ein Access Point eigentlich montiert? Welche Befestigungsvarianten gibt es und muss ich beim Tausch gegen ein neueres Gerät auch wieder bohren? Müssen hundert APs an Stellen montiert oder getauscht werden, an die sich ein Mensch mit Höhenangst garnicht erst wagt, bekommen diese Fragen ein ganz anderes Gewicht.

Da hierzu immer wieder Anfragen kommen, haben wir diese Themen in einem eigenen Absatz zusammengefasst.

AP3935

Die Wandbefestigung erfolgt einfach über Langlöcher. Schrauben und Dübel werden mitgeliefert. Bohrungen sind in einem Horizontalabstand von 113 mm zu setzen. Eine Bohrschablone wird mitgeliefert.

Dieses einfache Konzept ist für die Deckenmontage natürlich nicht empfehlenswert, da keine Sicherung den AP gegen unbeabsichtigtes Verschieben schützt.

Eine gesicherte Montage für Wand und Decke ist mit dem optionalen Wall Mount Kit (WS-MBI-WALLO3 Wall mounting bracket) möglich.

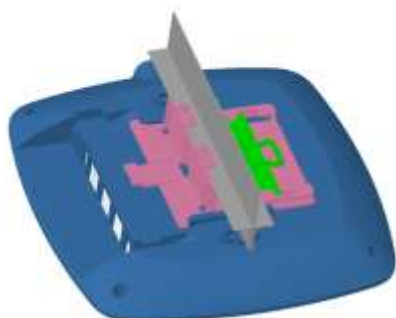


Die markierten Profilbolzen rasten zuverlässig in die Langlöcher des Metallgussgehäuses ein.

Mittels einer Schraubverbindung wird der AP gesichert. Zusätzlich kann ein Kensington Schloss angebracht werden.



Eine mitgelieferte Halterung ermöglicht die Befestigung des AP an den Halteschienen abgehängter Decken. Die dreistufige Verstellmöglichkeit passt das System an Schienenbreiten von 9 bis 39 mm an.



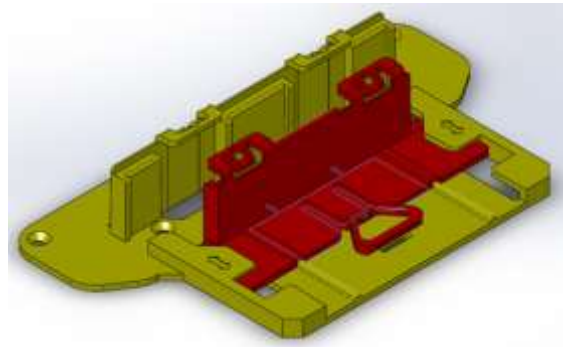
AP3825



Auch der AP3825 verfügt über eine einfache Aufhängung mit zwei Langlöchern. Schrauben und Dübel werden mitgeliefert.

Eine Halterung für Schienenprofile abgehängter Decken wird auch hier mitgeliefert (siehe Foto). Die Normbreite beträgt 27mm.

Nicht alle Schienen entsprechen dieser Norm, der optionale Adapter WS-MBI-DCU01 passt sich an Schienenbreiten von 14, 24 und 38mm an.



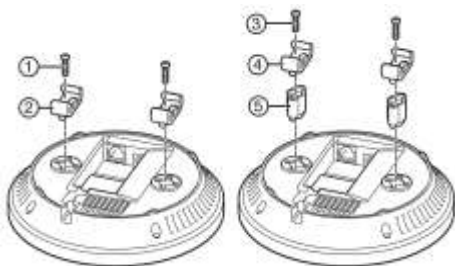
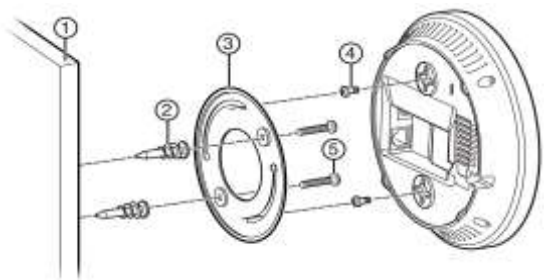
Darüberhinaus ist eine Wandhalterung mit Kensington Schloss verfügbar.

Bestellnr: WS-MBI-WALL01

AP3801/3805

Ergänzend soll auch die Montage der AP Modelle 3805 und 3801 beschrieben werden.

Die mitgelieferte Montageplatte ermöglicht das einfache Anbringen des Accesspoints an Decken oder Wänden.

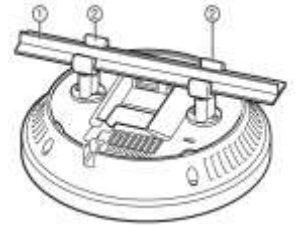


Klemmen und Abstandshalter für die Schienenmontage an abgehängten Decken sind ebenfalls Bestandteil des Lieferumfangs.

Hier ein Beispielschema für die Deckenmontage (Genaue Daten entnehmen Sie bitte den Installation Guides im Extranet).

Als robustere Ausführung kann das Mount Kit WS-MBI-WALL02 zusätzlich bestellt werden.

Nachdem bestehende Accesspoints vom Typ AP26xx sukzessive ausgetauscht werden, stellt sich in manchen Fällen auch die Frage nach der Bohrlochkompatibilität.



Das klingt trivial, hat jedoch z.B. im Krankenhausumfeld durchaus Bedeutung, denn in keimfreier Umgebung werden Bohr- und Stemmarbeiten nicht gerne gesehen.

Die Befestigungslöcher passen zu denen des AP26xx wie auch 36xx. Damit steht einem Austausch gegen den AP3805 nun garnichts mehr im Wege. Die, auffällig zahlreichen, Bohrungen schaffen Kompatibilität zu allen gängigen APs am Markt.

4 LAN Komponenten



Dieses Kapitel führt Sie durch das Extreme Networks Portfolio vom kostengünstigen 8-Port Kompaktswitch bis hin zu den Hochleistungschassis für maximale Anforderungen. Die folgende Übersicht unserer aktiven Netzwerkkomponenten soll Ihnen als Planungshilfe dienen.

S-Serie




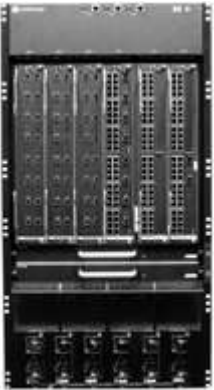
Die S-Serie ist die High End Produktlinie mit Switching-, Routing- und Security-Funktionen für alle Anwendungsbereiche im LAN, vom Datacenter über Core bis zum Access. Mit 3 standalone Systemen sowie 5 Chassis-Typen mit 1, 3, 4, 6 und 8 Slots und einer verteilten Architektur, einer hohen Skalierbarkeit mit einer Backplane Kapazität von aktuell bis zu 9,5 Terabit/s und „pro Slot“ Durchsatz von 80/160/320 Gbit/s, ist die S-Serie eine zukunftssichere Investition. Die Möglichkeiten gehen heute von 10/40 Gigabit Ethernet bis hin zu 100 Gigabit Ethernet in der Zukunft.

Alle Systeme der S-Serie auf einen Blick:

	SSA 130	SSA180	S1	S3	S4	S6	S8
Chassis-Slots	-	-	1	3	4	6	8
Switching-Kapazität Gesamtsystem (Gbps)	40	120	320	360	1280	1920	2560
Switching-Durchsatz Gesamtsystem (Mpps)	30	90	240	360	960	1440	1920
Gesamte Backplane-Kapazität (Gbps)	-	-	320	525	3000	7000	9500
10/100/1000BASE-TX Class 3 PoE Ports pro System (maximal)	48	48 (no PoE)	72	216	288	432	576
1000BASE-X SFP (MGBIC) Ports Pro System (maximal)	-	48	72	180	288	432	576
10GBASE-X SFP+ Ports pro System (maximal)	4	4	24	96	112	168	232
40GBase-X QSFP+ Ports pro System (maximal)	-	-	6	-	24	36	48

Bei der S-Serie handelt es sich um eine Weiterentwicklung der N-Serie, die alle Funktionen der N-Serie mit identischer Software realisiert, plus weitere Funktionen wie DCB, SPB, MPLS, Ipv6, MAC Sec* (Hardware ready) sowie die Möglichkeit der Applikationsklassifizierung in Hardware bietet. In der zweiten Generation der S-Module steht eine Kapazität von 2,56 Tbps und 1920 Mpps zur Verfügung (in einem S8 Chassis). Damit können bis zu 576 Gigabit Ethernet, 232 10 Gigabit Ethernet oder 48 40 Gigabit Ethernet Ports via SFP+/QSFP realisiert werden.

Weitere Portdichtenerhöhungen werden folgen. Alle 10/100/1000 Module sind von Hause aus High Power PoE+ 802.3at fähig. Der PoE Betrieb wird über zusätzliche, modulare Stromversorgungen mit bis zu 16KW Leistungsbudget sichergestellt.

	
<p>SSA</p>	<p>S1</p>
	
<p>S3</p>	<p>S4</p>
	
<p>S6</p>	<p>S8</p>

Architektur

Die Extreme S-Serie Chassis nutzen sowohl (Switch-)Fabric-based als auch Fabricless Architekturen. Die S4 und S8 Chassis nutzen die Fabric-based Variante mit mehreren High Speed Links zwischen den I/O Modulen und den jeweiligen Fabric- Komponenten.

Währenddessen ist das S3 Chassis Fabric-less für den Einsatz im Access Bereich optimiert. Mindestens ein I/O Fabric Modul muss in einem S4 oder S8 Chassis eingesetzt werden, für den vollen Systemdurchsatz sind jedoch 2 I/O Fabric Module im Loadsharing notwendig. Damit werden dann bis zu 2560 Gbps Switching und HA Funktionen realisiert. Im S8 Chassis ist sogar der Einsatz einer dritten I/O Fabric zur Steigerung der Gesamtverfügbarkeit und Erhöhung der Redundanz möglich. Extreme S-Serie I/O Module sind hoch performante, voll ausgestattete Switches in einem verteilten Switch-System mit Management- und Routing Funktionen, die vom jeweiligen On-Board Prozessorsystem übernommen werden. Die flowbasierten CoreFlow2 ASICs formen zusammen mit den Prozessorsystemen ein sehr flexibles, skalierbares und hoch-performantes Gesamtsystem mit wesentlich höherer Prozessorleistung als vergleichbare Systeme. I/O Fabric und I/O Modules sind mit vielen unterschiedlichen Interface-Typen und Portdichten verfügbar, um alle möglichen Netzwerkdesigns optimal abzubilden: von 10/100/1000BASE-TX, 1000BASE-X SFP bis zu 10G BASE-X SFP+ und 40G Base-X QSFP. Die SFP+ Ports können auch SFP´s aufnehmen, die SFP Ports auch 100FX SFP´s. Alle Triple Speed I/O Kupfer Module sind PoE-enabled. Viele I/O Modules haben ein oder zwei sogenannte Option-Module, die weitere Konfigurationsflexibilität im Bereich Media und Portdichte bieten. Dies resultiert in einfacheren und kostengünstigeren Designs.

Extreme CoreFlow2

Mit der Extreme CoreFlow2 Technologie bietet Extreme die Schlüsselfunktion für die Flusssteuerung von Applikationsdaten als auch für die Datenzugriffskontrolle. Die Extreme CoreFlow2 ASIC Technologie wurde über die letzten 15 Jahre stetig weiterentwickelt. Das patentierte ASIC Design hat eine Kapazität, um bis zu 64 Millionen Flows pro System zu verarbeiten. Dabei unterstützt der flexibel programmierbare ASIC die Klassifizierung, Sichtbarkeit und Kontrolle des Applikationsflusses in Line-Rate-Geschwindigkeit.

CoreFlow2 bietet die Möglichkeit, die Klassifikation von Datenverkehr zwischen Layer-2 und Layer-7 durchzuführen. Stand heute wird anhand NMS Policies der Datenfluss zwischen Layer-2 und Layer-4 gesteuert. Unter dem gemeinsamen Einsatz von Access Control und Policies können Endsystemen und auch Servern anhand ihrer Identifikation (802.1x, MAC etc.) dynamisch Kommunikationsregeln in einem LAN zugeordnet bzw. durchgesetzt werden.

Mögliche Anwendungsszenarien für die von CoreFlow2 gebotenen Policies:

- iSCSI
 - Zugriffskontrolle nur iSCSI Initiatoren
 - Überwachung der Netzwerkbandbreite pro iSCSI Target
- RTP
 - Spezifizierte Zugriffssteuerung anhand von Audio und Video Codec

- zukünftige Features auf Basis von http
 - Zugriffskontrolle auf Cloud Service wie z. B.. www.salesforce.com
 - Bandbreitenüberwachung (z. B..www.youtube.com)

Der flexibel programmierbare CoreFlow2 ASIC bietet nicht nur eine Application Awareness, ferner bietet er die Möglichkeit, auch zukünftige Features und Standards als Software Upgrade auf dem Switch einzuspielen. Der Extreme CoreFlow2 ASIC kommt auf Data Center, Distribution und Core Router Fabric Einschüben der S-Serie zum Einsatz. Die wichtigsten neuen Standards, die auf diese Weise Feature-Unterstützung auf der S-Serie erhalten sollen, sind:

Access/Edge I/O Module

Diese Module sind für den Einsatz im User-Access und der Peripherie optimiert. Die Access/Edge I/O Module ermöglichen es, durch die am Markt einzigartige Flex-Edge Technologie, bandbreitenhungrigen Workstations selektiv nicht-überbuchte, line-rate Datendienste zur Verfügung zu stellen, um damit sensitive Daten in allen Situationen sicher zu übertragen. Sie unterstützen bei der Authentifizierung und Policy Zuweisung bis zu 512 Nutzer pro Modul und 8 authentifizierte Nutzer pro Port, verglichen mit den Core/Distribution Modulen, die bis zu 1.024 User/Devices pro Modul und keine Restriktion pro Port haben. Falls ein Access Modul mehr Nutzer benötigt, kann mit der Upgrade Lizenz (S-EOS-PPC) auf die gleichen Limits wie die Core/Distribution Module erweitert werden. Alle S-Serie Triple Speed I/O Module unterstützen PoE als Standard, keine weiteren Hardware oder Software Upgrades sind erforderlich - nur entsprechende PoE Power Supplies sind dem Chassis hinzuzufügen. Die Access Module sind bei den Routing Funktionen limitiert und bieten im Gegensatz zu den anderen Module keine *BGPv4, *IS-IS für IPv4 & IPv6, *VRF, NAT, LSNAT, TWCB Funktionen, jedoch ein Upgrade auf VRF mittels S-EOS-L3- ACCESS. *(Funktionen mit * sind nicht im ersten Release vorhanden, bitte erfragen Sie die Verfügbarkeit bei Extreme und lassen Sie diese bestätigen)*

Distribution, Core und Data Center I/O Module

Eine Reihe von S-Serie I/O Modulen sind für die Bereiche mit höchsten Anforderungen designed, die fortlaufend hohe Datenraten aufweisen. Gigabit und 10 Gigabit Ethernet Module mit Line Rate Forwarding und erweiterten Traffic Management Mechanismen sowie extrem große Packet-Buffer erlauben maximale Netzwerk-Performance.

Distribution, Core und Data Center I/O Module sind optimiert für den Einsatz im Core und Data Center Bereich. Die Media Flexibilität ist auch bei diesen Modulen gegeben. Hier gibt es auch Upgrade Möglichkeiten für weitere Core Routingprotokolle (Stichwort *MPLS, *VPLS und *Tunneling/GRE in Zukunft via SEOS- L3-ACCESS).

High Availability Upgrade (HAU)

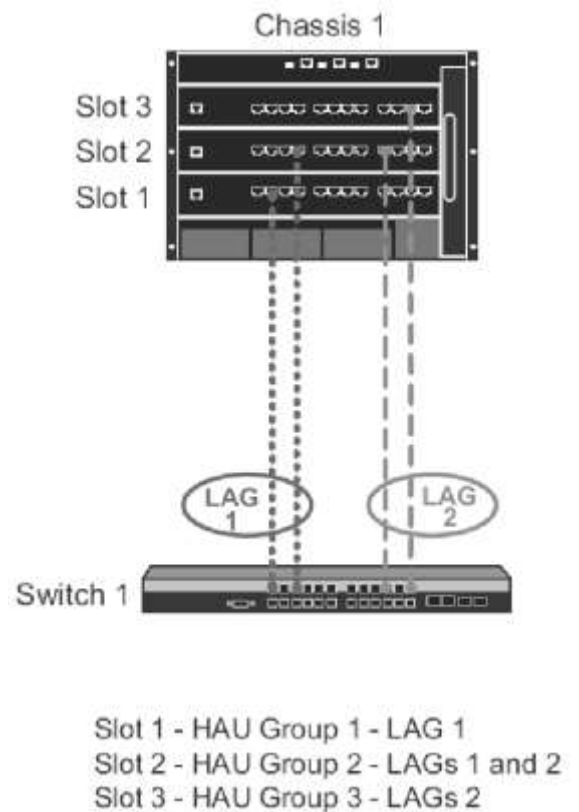
High Availability Firmware Upgrade (HAU) ist eine S-Serie Funktion, die ein Firmware Update eines S-Serie Chassis oder S-Serie VSB über einen Rolling Mechanismus bereitstellt.

Der Funktionsunterschied des High Availability Update (HAU) zu einem Standard Update ist, dass bei einem Standard Update alle Module eines Chassis Systems gleichzeitig einen Software Neustart durchführen und dabei die neue Software geladen wird. Hierbei werden alle Datenverbindungen deaktiviert und alle Services, die an diesem Chassis angebunden sind, unterbrochen.

Bei dem HAU Software Update wird ein Rolling Update Prozess in einem Chassis genutzt. Die Module werden sequenziell neu gestartet und dabei wird nach und nach die neue Software geladen. Das S-Serie Chassis nutzt hierbei vordefinierte Gruppen, welche sequenziell gebootet werden. Der Vorteil hierbei ist, dass ein Großteil des S-Serie Chassis weiterhin ohne Einschränkungen aktive Netzwerkdaten bearbeitet. Unterbrechungen gibt es nur bei Chassis Elementen, die neu gestartet werden und bei denen eine neue Software geladen wird.

Die Gruppenelemente sind in der Grundkonfiguration so definiert, dass sich jeder S-Serie Systemslot in einer Gruppe befindet. Bei einem Update eines S4, der 4 Module haben kann, welche sequenziell neu gestartet werden, sind also 4 Module-Neustarts notwendig, um final die neue Software zu aktivieren.

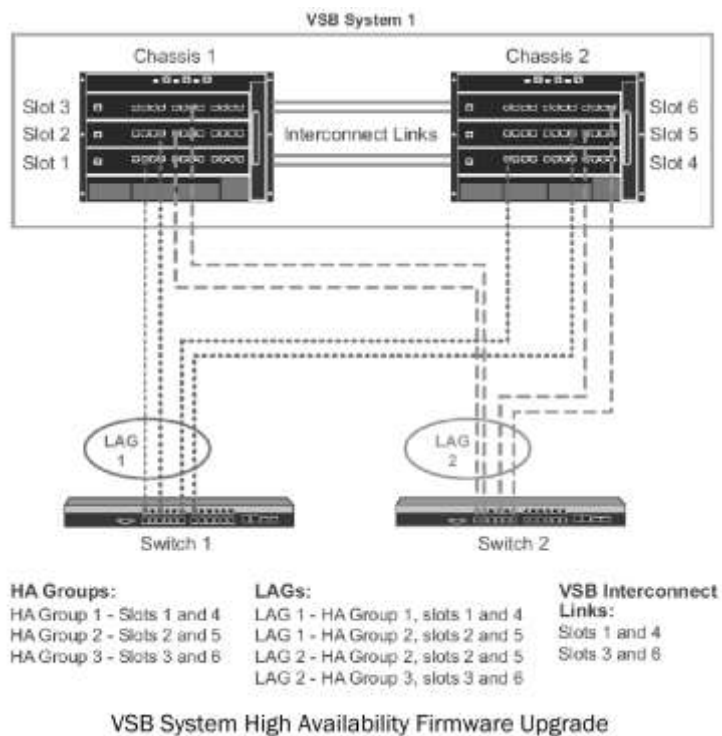
Der Administrator hat die Möglichkeit die Gruppen der einzelnen Slots eines Chassis manuell neu zu definieren und dabei eine schnellere Update Sequenz zu erreichen. So können 2 oder in einem VSB alle Systemslots eines Chassis in einer Gruppe zusammengefasst werden. Ein Update der vordefinierten Gruppen wird endgültig die aktiven und neu zu startenden Systemslots/Gruppen definieren.



Das Neustarten der Gruppen - also der Slots - kann mit einem zusätzlichen Delay definiert werden, so dass der Administrator die neu gestarteten Systemkomponenten kontrollieren und das Update auch, wenn notwendig, manuell stoppen kann. Hierzu ist der Update-Delay zu verändern. Der High Availability Update Prozess kann nicht nur für Updates, sondern auch für Downgrades genutzt werden. So ist dem Administrator weiterhin eine flexible Software Up-/Downgrade Möglichkeit gegeben.

Die Software erkennt anhand eines internen Upgradeschlüssels, ob ein HAU Update von Version A nach

Version A.xx freigegeben ist. Eine solche Freigabe berücksichtigt Abhängigkeiten zwischen den Versionen und ist auch in den jeweils aktuellen Release Notes dokumentiert. Der HAU Update Prozess ist primär für Minor Release Changes und Release Patches definiert.



EEE Energy Efficient Ethernet

Im Netzwerk und speziell im Data Center steigt der Datendurchsatz täglich. Um diesem Zustand Rechnung zu tragen, werden heutige Netzwerkumgebungen von 1G Interfaces auf 10G oder 40G Interface aufgerüstet. Für den Betrieb der schnelleren Datenschnittstellen benötigt man Hardware (Phy), die wiederum mehr Strom benötigt, um den Betrieb zu erhalten, selbst wenn keine Daten über das Interface gehen. Dadurch steigt der Energieverbrauch in Rechenzentren durch die Hardware und die benötigte Kühlung. Um dem entgegen zu wirken wurden Mechanismen wie EEE entwickelt. Energy Efficient Ethernet beschreibt eine Reihe von Erweiterungen des Ethernet-Standards für Rechnernetze, die eine Reduzierung des Stromverbrauchs in Phasen geringer oder keiner Aktivität bewirken. Der IEEE Standard für EEE ist 802.3az

Im Normalfall bleiben Ethernet-ICs in den betreffenden Geräten auch dann aktiv, wenn aktuell kein Datenverkehr stattfindet. Zur Verringerung des Energiebedarfs kann in diesem Fall das Interface in einen sparsamen Schlafmodus versetzt werden. Bei einer anstehenden Datenübertragung wird der Port durch ein Wecksignal wieder in den aktiven Zustand versetzt. Damit eine Einsparung erzielt wird, müssen sämtliche beteiligten Komponenten diese im Standard vorgesehenen Funktionen beherrschen.

Für die S-Serie gibt es I/O Module, die EEE auf ihren Ports unterstützen. Damit lässt sich die Energie Effizienz der Systeme erweitern.

I/O Fabric and I/O Modul Spezifikationen

	S130 Class I/O Modules		S140 I/O Modules			
Network Applications	Wiring Closet, Distribution Layer, Small Network Core		Distribution Layer, Server Aggregation, Data Center Core, Enterprise			
Part Number	ST4106-0248	SG4101-0248	ST2206-0848A	SG2201-0848	SK2008-0832	SK2009-0824
Used in	S3/S4/S6/S8 Chassis	S3/S4/S6/S8 Chassis	S3/S4/S6/S8 Chassis	S3/S4/S6/S8 Chassis	S3/S4/S6/S8 Chassis	S3/S4/S6/S8 Chassis
Port Type	RJ45	SFP	RJ45	SFP	SFP+	10GBase-T
Port Quantity	48	48	48	48	32	24
Port Speed	10/100/1000 Mbps	1000 Mbps	10/100/1000 Mbps	1000 Mbps	10 Gbps	10 Gbps
PoE Support	802.3af, 802.3at	-	802.3af, 802.3at	-	-	-
Option Module Slots	1, (Type1)	1, (Type1)	2, (Type 2)	2, (Type 2)	-	-
Module Throughput	30 Mpps	30 Mpps	120 Mpps	120 Mpps	120 Mpps	120 Mpps
I/O Switching Capacity	40 Gbps	40 Gbps	160 Gbps	160 Gbps	160 Gbps	160 Gbps

	S180 I/O Modules		
Network Applications	Distribution Layer, Server Aggregation, Data Center Core, Enterprise		
Part Number	SK8008-1224	SK8009-1224	SL8013-1206A
Used in	S4/S6/S8 Chassis	S4/S6/S8 Chassis	S4/S6/S8 Chassis
Port Type	SFP+	10GBase-T	QFSP+
Port Quantity	24	24	6
Port Speed	10 Gbps	10 Gbps	40 Gbps
PoE Support	-	-	-
Option Module Slots	-	-	-
Module Throughput	240 Mpps	240 Mpps	240 Mpps
I/O Switching Capacity	320 Gbps	320 Gbps	320 Gbps

I/O Fabric Modul Spezifikationen

	S130 Class Fabric Mod.	S180 Class I/O Fabric Modules				
	Wiring Closet, Distribution Layer, Small Network Core	Distribution Layer, Server Aggregation, Data Center Core, Enterprise				
Part Number	ST4106-0248-F6	ST8206-0848-F8A	SG8201-0848-F8	SK8008-1224-F8	SK8009-1224-F8	SL8013-1206-F8A
Used in	S1/S4/S6/S8 Chassis	S1/S4/S6/S8 Chassis	S1/S4/S6/S8 Chassis	S1/S4/S6/S8 Chassis	S1/S4/S6/S8 Chassis	S1/S4/S6/S8 Chassis
Port Type	RJ45	RJ45	SFP	SFP+	10GBase-T	QSFP+
Port Quantity	48	48	48	24	24	6
Port Speed	10/100/1000 Mbps	10/100/1000 Mbps	1000 Mbps	10 Gbps	10 Gbps	40 Gbps
PoE Support	802.3af, 802.3at	802.3af, 802.3at	-	-	-	-
Option Module Slots	1, (Type 2)	2, (Type 2)	2, (Type 2)	-	-	-
Module I/O Throughput	45 Mpps	120 Mpps	120 Mpps	240 Mpps	240 Mpps	240 Mpps
I/O Switching Capacity	60 Gbps	160 Gbps	160 Gbps	320 Gbps	320 Gbps	320 Gbps
Fabric Throughput (Single)	480 Mpps	960 Mpps	960 Mpps	960 Mpps	960 Mpps	960 Mpps

Chassis Modellinformationen:

Part Number	Description
S8 Chassis	
S8-Chassis	S-Series S8 Chassis and fan trays (Power supplies ordered separately)
S8-Chassis-POE4	S-Series S8 Chassis and fan trays with 4 bay PoE subsystem (System and PoE Power supplies ordered separately)
S8-Chassis-POE8	S-Series S8 Chassis and fan trays with 8 bay PoE subsystem (System and PoE Power supplies ordered separately)
S8-POE-8BAY-UGK	S-Series 8 bay PoE upgrade kit for the S8 (PoE Power supplies ordered separately)

S8-POE-4BAY-UGK	S-Series 4 bay PoE upgrade kit for the S8 (PoE Power supplies ordered separately)
S8-Midmount-Kit	S-Series S8 Chassis 19" midmount installation rack kit can be used with all S8 chassis types
S6 Chassis	
S6-Chassis	S-Series S6 Chassis and fan trays. Front to back cooling. (Power supplies ordered separately)
S6-Chassis-POE4	S-Series S6 Chassis and fan tray with 4 bay POE subsystem. Front to back cooling. (System and POE power supplies ordered separately)
S6-Midmount-Kit	S-Series S6 Chassis 19" midmount installation rack kit, can be used with all S6 Chassis types
S6-FAN	S-Series Fan Tray (For use w/ S6)
S4 Chassis	
S4-Chassis	S-Series S4 Chassis and fan tray (Power supplies added separately)
S4-Chassis-POE4	S-Series S4 Chassis and fan tray with 4 bay PoE subsystem (System and PoE Power supplies ordered separately)
S4-POE-4BAY-UGK	S-Series 4 bay PoE upgrade kit for the S4 (PoE Power supplies ordered separately)
S4-Midmount-Kit	S-Series S4 Chassis 19" midmount installation rack kit, can be used with all S4 Chassis types
S3 Chassis	
S3-Chassis-A	S-Series S3 Chassis and fan tray (Power supplies ordered separately)
S3-Chassis-POEA	S-Series S3 Chassis and Fan Tray with 4 bay PoE subsystem (System and PoE Power supplies ordered separately)
S3-POE-4BAY-UGK	S-Series 4 bay PoE upgrade kit for the S3 (PoE Power supplies ordered separately)
S3-Midmount-Kit	S-Series S3 Chassis 19" midmount installation rack kit, can be used with all S3 Chassis types
S1-Chassis	
S1-Chassis-A	S-Series S1 Chassis and fan tray. Compatible with Fabric Modules only. (SSA 1000W Power supplies ordered separately)
S1-Mount-Kit	S-Series S1 Chassis 19" accessory mounting kit. Supports midmount and rail kit installation options for 2 and 4 post racks, can be used with the S1 chassis.
S1-FAN-A	S1 Chassis fan tray, Spare (For use w/S1)
Power Supplies and Fans	
S-AC-PS	S-Series AC power supply, 20A 100-240 VAC input (1200W/1600W) (For use w/S3/S4/S6/S8)
S-AC-PS-15A	S-Series AC power supply, 15A, 100-240 VAC input, (930W/1600W) (For use w/S3/S4/S6/S8)
S-POE-PS	S-Series POE power supply, 20A, 100-240 VAC input, (1200/2000 W) (For Use in 4/8 Bay PoE power subsystems)

S-DC-PS	S-Series 48-60v DC Power Supply (For Use w/ S3/S4/S6/S8) (1200W)
S-FAN	S-Series Fan Tray (For use w/ S3/S4/S8)

I/O und I/O Fabric Modulinformationen

Part Number	Description
S130 I/O Fabric Modules	
ST4106-0348-F6	S-Series I/O-Fabric S130 Class Module, 1280Gpbs Load Sharing -48Ports 10/100/1000Base-TX via RJ45 with PoE (802.3at) and one Type2 option slot (used in S1/S4/S6/S8)
S130 I/O Modules	
ST4106-0248	S-Series I/O S130 Class Module - 48 Ports 10/100/1000BASE-T via RJ45 with PoE (802.3at) and one Type1 option slot (Used in S3/S4/S6/S8)
SG4101-0248	S-Series I/O S130 Class Module - 48 Ports 1000BASE-X ports via SFP and one Type1 option slot (Used in S3/S4/S6/S8)
S140 I/O Modules	
ST2206-0848	S-Series S140 I/O Module - 48 Ports 10/100/1000BASE-TX via RJ45 with PoE (802.3at) and two Type2 option slot (Used in S3/S4/S6/S8)
SG2201-0848	S-Series S140 I/O Module - 48 Ports 1000BASE-X ports via SFP and two Type2 option slot (Used in S3/S4/S6/S8)
SK2008-0832	S-Series S140 Class I/O Module - 32 Ports 10GBASE-X via SFP+ (Used in S3/S4/S6/S8)
SK2009-0824	S-Series S140 Class I/O Module -24 Ports 10GBASE-T via RJ45 (Used in S3/S4/S6/S8)
S180 I/O Fabric Modules	
SL8013-1206-F8A	S-Series S180 Class I/O-Fabric Module, Load Sharing - 6 Ports 40GBASE-X Ethernet via QSFP, 4 ports VSB via SFP+ (Used in S1/S4/S6/S8)
SKL8008-0810-F8	S-Series S180 Class I/O-Fabric Module Load Sharing - 8 Ports 10GBASE-X via SFP+ and 2 ports 40GBASE-X Ethernet via QSFP+ (Used in S1A/S4/S6/S8)
SK8208-0808-F8	S-Series S180 Class I/O - Fabric Module, Load Sharing - 8 Ports 10GBASE-X via SFP+ and two Type2 option slots (Used in S1A/S4/S6/S8)
SK8008-1224-F8	S-Series S180 Class I/O-Fabric Module, Load Sharing - 24 Ports 10GBASE-X via SFP+, 4 ports VSB via SFP+ (Used in S1/S4/S6/S8)
SK8009-1224-F8	S-Series S180 Class I/O-Fabric Module, Load Sharing - 24 Ports 10GBASE-T via RJ45, 4 ports VSB via SFP+ (Used in S1/S4/S6/S8)
ST8206-0848-F8A	S-Series S180 Class I/O-Fabric Module, Load Sharing - 48 Ports 10/100/1000BASE-T via RJ45 with PoE (802.3at) and two Type2 option slots (Used in S1/S4/S6/S8)
SG8201-0848-F8	S-Series S180 Class I/O-Fabric Module, Load Sharing - 48 Ports 1000BASE-X via SFP and two Type2 options slots (Used in S1/S4/S6/S8)
S180 I/O Modules	
SL8013-1206A	S-Series S180 Class I/O Module - 6 Ports 40GBASE-X Ethernet via QSFP, VSB expansion slot (Used in S4/S6/S8)
SK8008-1224	S-Series S180 Class I/O Module -24 Ports 10GBASE-X via SFP+, VSB expansion slot (Used in S4/S6/S8)

SK8009-1224	S-Series S180 Class I/O Module -24 Ports 10GBASE-T via RJ45, VSB expansion slot (Used in S4/S6/S8)
Option Modules	
SOK2208-0102	S-Series Option Module (Type1) - 2 10GBASE-X Ethernet ports via SFP+ (Compatible with Type1 & Type2 option slots)
SOK2208-0104	S-Series Option Module (Type1) - 4 10GBASE-X Ethernet ports via SFP+ (Compatible with Type1 & Type2 option slots)
SOK2208-0204	S-Series Option Module (Type2) - 4 10GBASE-X Ethernet ports via SFP+ (Compatible with Type2 option slots)
SOK2209-0204	S-Series Option Module (Type2) - 4 10GBASE-T RJ45 ports with PoE+ Support (Compatible with Type2 option slots)
SOG2201-0112	S-Series Option Module (Type1) - 12 1000BASE-X ports via SFP (Compatible with Type1 & Type2 option slots)
SOT2206-0112	S-Series Option Module (Type1) - 12 Ports 10/100/1000BASE-TX via RJ45 with PoE (802.3at) (Compatible with Type1 & Type2 option slots)
SOTK2268-0212	S-Series Option Module (Type2) - 10 Ports 10/100/1000BASE-T via RJ45 with PoE and 2 ports 10GBASE-X via SFP+ (Compatible with Type2 option slots)
SOGK2218-0212	S-Series Option Module (Type2) - 10 Ports 1000BASE-X via SFP and 2 ports 10GBASE-X via SFP+ (Compatible with Type2 option slots)
SOV3208-0202	S-Series Option Module (Type2) - 2 port VSB Option Module (Compatible with Type2 option slots on S140/S180 modules only)
Expansion Module	
SOV3008-0404	S-Series VSB Expansion Module - 4 port VSB Module (Compatible with S180 Class 10Gb/40Gb I/O modules only)

SSA & Lizenzmodellinformationen

Part Number	Description
SSA S130 (S-Series Stand Alone)	
SSA-T4068-0252	S-Series Stand Alone (SSA) - S130 Class - 48 Ports 10/100/1000BASE-T via RJ45 with PoE (802.3at) and 4 10GBASE-X Ethernet ports via SFP+ (Power supplies not included - Please order separately)
SSA-AC-PS-625W	S-Series Standalone (SSA S130 Class) - AC power supply, 15A, 100-240VAC input, (625W)
SSA-AC-PS-1000W	S-Series Standalone (SSA S130 Class) and S1-Chassis - AC and POE power supply, 15A, 110-240VAC input, (1000/1200W)
SSA-FAN-KIT	S-Series Stand Alone (SSA S130 Class) - Replacement fan assembly (Single Fan)
SSA S180 (S-Series Stand Alone)	
SSA-T8028-0652	S-Series S180 Class Standalone (SSA) - 48 Ports 10/100/1000BASE-T via RJ45 and 4 ports 10GBASE-X via SFP+, Front to Back cooling (Power supplies not included - Please order separately)

SSA-G8018-0652	S-Series S180 Class Standalone (SSA) - 48 Ports 1000BASE-X via SFP and 4 ports 10GBASE-X via SFP+, Front to Back cooling (Power supplies not included - Please order separately)
SSA-FB-MOUNTKIT	Optional Rack Mount Kit for the SSA 'Front to Back' models.
SSA-FB-AC-PS-A	S-Series Standalone (SSA Front to Back) - AC power supply, 15A, 100-240VAC input, I/O side exhaust
SSA-FB-AC-PS-B	S-Series Standalone (SSA Front to Back) - AC power supply, 15A, 100-240VAC input, I/O side intake
SSA-FB-FAN	S-Series Standalone (SSA Front to Back) - Spare fan tray assembly
Optional Licenses	
S-EOS-L3-S130	S-Series Advanced Routing License (For use on S130 Class Modules) (Enables VRF, BGP, Tunneling)
S-EOS-PPC	S-Series Per Port User Capacity License Upgrade (For use on S130 Class Modules)
S-EOS-VSB	S-Series Multi-slot Virtual Switch Bonding License Upgrade (For use on S130/S140 Class Modules)
SSA-EOS-VSB	S-Series SSA Virtual Switch Bonding License Upgrade (For use on SSA Only)
SSA-EOS-2XUSER	SSA180 double user capacity license
S1-EOS-VSB	S-Series S1 Chassis Virtual Switch Bonding License Upgrade (For use on S1-Chassis-A /S1-Chassis Only)

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/s-series

K-Serie

Überblick

Die Extreme K-Serie ist die kosteneffizienteste, modulare Switching-Lösung mit Flowbasierter ASIC Technologie auf dem Markt. Durch den Coreflow 2 Asic ist die K-Serie in der Lage, ein außergewöhnliches Maß an Performance, Netzwerkkontrolle und Datentransparenz zur Verfügung zu stellen. Die K-Serie bietet als einziger Switch seiner Klasse unsampled Netflow Daten auf allen Ports und somit eine hohe Datentransparenz ohne Einbußen bei der Performance.



Die K-Serie ist ein Switch für den Netzwerk Edge und small Enterprise Core Bereich, mit dem umfangreichen Feature-Satz eines großen Core Switches. Entwickelt, um die wachsenden Anforderungen durch neue Applikationen und Services zu erfüllen, ist die

K-Serie eine ideale Lösung für verschiedenste Bereiche der Netzwerk-Infrastruktur. Sie macht das Nutzer-, Service- und Applikationsverhalten im Detail durchschaubar und ermöglicht so genaue Kontrolle und Steuerung. Dadurch lassen sich Schlüsseltechnologien wie Unified Communications und kritische Betriebsapplikationen wie CRM und SAP optimieren. Ihre Funktionsvielfalt empfiehlt die Systeme Extreme K6 und K10 als extrem kosteneffiziente Switches mit hoher Portdichte.

Die Extreme K-Serie Switches sind in den folgenden Ausführungen verfügbar:

- 6-Slot-Chassis mit maximal 144 Triple-Speed Edge-Ports und vier 10Gb-Uplinks
- 10-Slot-Chassis mit maximal 216 Triple Speed Edge Ports und acht 10Gb-Uplinks

Die K-Serie unterstützt bis zu 12 10Gb-Uplinks. 4 x SFP+ Ports stehen auf den Fabric Cards zur Verfügung und bis zu 8 weitere SFP* Ports können über I/O-Module erweitert werden.

Die K-Serie implementiert eine hochleistungsfähige flowbasierte Switching-Architektur, mit der sich individuelle Nutzer- und Applikationskonversationen intelligent managen lassen. Die Geräte können weit mehr als reines Switching, das hauptsächlich VLANs, ACLs und Ports zur Implementierung rollenbasierter Zugangskontrolle umfasst. Sicherheitspolicies und -rollen setzen sie mit Wire Speed durch. Datenverkehr wird klassifiziert und priorisiert. Alle Ein-/Ausgabemodule bieten höchste Servicequalität für kritische Applikationen wie Sprache und HD-Video, sogar in Zeiten hoher Netzwerk-Verkehrbelastung. Gleichzeitig verhindern sie DoS (Denial-of-Service)-Attacken und Malware-Übertragungen.

Nutzeridentifikation und Rollenkonzepte gewährleisten, dass jeder einzelne Anwender auf seine betriebskritischen Applikationen zugreifen kann, egal von wo aus er sich mit dem Netzwerk verbindet. Die K-Serie inspiziert Pakete im Detail und ermöglicht die Definition umfangreicher Regelwerke. Dadurch lassen sich Sicherheitsbedrohungen intelligent aufspüren. Das System reagiert dann automatisch auf entsprechende Bedrohungen. Die Zuverlässigkeit und die Qualität der Nutzererfahrung steigen.

Ein wichtiges Merkmal der K-Serie ist ihre Fähigkeit, NetFlow-Daten mit Leitungsgeschwindigkeit zu sammeln. Das bedeutet absolute Transparenz hinsichtlich der Nutzung der Netzwerkressourcen durch Anwender und Applikationen. Die Enterprise-Switches der Extreme K- und S-Serie unterstützen Multi-User und Multi-Method-Authentisierung für mehrere 100 User auf jedem Port. Das ist absolut essenziell, wenn Geräte wie IP Telefone, Computer, Drucker, Kopierer, Sicherheitskameras, Barcodeleser und virtuelle Maschinen an das Netzwerk angeschlossen werden.

Hardwarebasierte, hochverfügbare Funktionen

Die K-Serie enthält viele Standard-Hochverfügbarkeits-Funktionen, die in der Hardware implementiert sind. Daher eignet sie sich für betriebskritische Umgebungen, die ununterbrochen (24/7) verfügbar sein müssen.

Im Einzelnen sichern folgende Funktionen und Eigenschaften der K-Serie die Hochverfügbarkeit:

- passive Chassis-Backplane
- redundante Lüftermodule, die im laufenden Betrieb austauschbar sind
- redundante Stromversorgungen mit Lastverteilung, die im laufenden Betrieb austauschbar sind

Verteilte, flowbasierte Architektur

Für granulare Transparenz und Verkehrsmanagement ohne Leistungseinbußen verwendet die Extreme K-Serie eine verteilte, flowbasierte Architektur. Sie garantiert, dass die ersten Pakete eines Datenstroms zwischen zwei Endpunkten durch die Multilayer-Klassifizierungsmaschine in den I/O- und den I/O-Fabric-Modulen des Switches verarbeitet werden. Sie identifizieren die Rolle des Absenders, bestimmen die anzuwendenden Regelsätze, prüfen die Pakete und definieren die Maßnahme zur Weiterleitung. Nachdem ein Datenstrom identifiziert wurde, handhaben die Extreme-ASICs die nachfolgenden Pakete dieses Flows automatisch und ohne weitere Verarbeitung. Die Extreme K-Serie kann damit jeden Datenstrom sehr detailliert auf der gesamten Transportstrecke steuern und überwachen.

Multi-User / Method Authentifizierung und Policy

Mit Authentifizierung verwalten Unternehmen den Netzwerkzugang und machen Nutzer und Geräte mobil. Authentifizierung schafft Überblick darüber, wer oder was mit dem Netzwerk verbunden ist und vermittelt jederzeit Wissen darüber, wo sich diese Verbindung befindet. Die Module der Extreme K-Serie unterstützen Multi Method Authentifizierung. Dazu gehören die 802.1x-Authentifizierung, die MAC-Authentifizierung (für die Identifizierung der Geräte am Netz über die MAC-Adresse) sowie die webbasierte Authentifizierung (PWA, Port Web Authentifizierung - dabei stellt der Browser Nutzernamen und Password bereit).

CEP (Convergence End Point): Mehrere VoIP-Telefone unterschiedlicher Lieferanten werden identifiziert und authentifiziert. Das erhöht die Flexibilität von Unternehmen, die Zugangskontroll-mechanismen in ihrer Infrastruktur implementieren möchten.

Weiterhin unterstützt die K-Serie Multiuser Authentifizierung. Damit lassen sich mehrere Nutzer und Geräte an den selben physikalischen Ports anbinden, trotzdem kann man jeden Anwender und jedes Gerät individuell mit einer Multi-Method Option (802.1x, MAC, PWA oder CEP) authentifizieren. Der Hauptvorteil des Verfahrens liegt in der Autorisierung mehrerer Nutzer, entweder durch dynamische Policies oder VLAN-Zuweisung an jeden authentifizierten Nutzer. Derartige dynamische Policies bezeichnet man als Multiuser Policy. Multiuser-Portfähigkeiten lassen sich bei der K-Serie pro Port, pro I/O Modul und pro Multi-Slot System festlegen.

Multiuser Authentifizierung und Policy können Sicherheitsdienste auf Nutzer anwenden, die über ungemanagte Geräte, Switches/Router anderer Hersteller, VPN-Konzentratoren oder WLAN-Access-Points am Edge mit dem Netzwerk verbunden sind.

Authentifizierung bietet Sicherheit, Priorität und Bandbreitenkontrolle bei gleichzeitigem Schutz bestehender Netzwerkinvestitionen.

Dynamische, flowbasierte Paketklassifizierung

Ein weiteres einzigartiges Feature der K-Serie ist die nutzerbasierte Multilayer Paketklassifizierung/Servicequalität. Da in den heutigen Infrastrukturen viele Netzwerkanwendungen eingesetzt werden, reicht eine traditionelle Multilayer-Paketklassifizierung nicht mehr, um den zeitgemäßen Transport betriebskritischer Applikationen zu garantieren. Bei der K-Serie ordnet die nutzerbasierte Multilayer-Paketklassifizierung Datenströme nach Pakettyp, Nutzerrolle im Netzwerk und nutzerspezifischer Policy. So lassen sich Pakete basierend auf eindeutigen Zuordnungen, wie „All User“, „User Groups“ und „Individual User“, klassifizieren. Netzwerkvertraulichkeit, Integrität und Verfügbarkeit kann man so besser sicherstellen und managen.

Netzwerktransparenz durch präzise NetFlow Daten

NetFlow stellt auf den Switchports der K-Serie Netzwerk-Performance-Management und Sicherheitsfunktionen bereit, ohne die Switching- und Routing-Performance zu verringern, und das ohne den Zukauf teurer Tochterkarten für jedes Modul. Extreme NetFlow überwacht, anders als typische statistische Stichprobentechniken oder restriktive applikationsbasierte Implementierungen, jedes Paket in jedem Datenstrom. Durch dieses nicht gesampelte Echtzeit-NetFlow-Monitoring ist stets genau bekannt, welcher Verkehr genau durchs Netz fließt. Taucht etwas Ungewöhnliches auf, erfasst NetFlow es und man kann sofort einschreiten. Zusätzlich kann man NetFlow für Kapazitätsplanungen nutzen. Netzwerkmanager überwachen und verstehen damit Verkehrsflüsse und -volumen im Netzwerk und sehen, wo das Netzwerk rekonfiguriert oder erweitert werden muss. Dass die Administratoren Upgrades genau planen können, spart Zeit und Geld.

Feature-Zusammenfassung

- Multilayer Paketklassifizierung: Kenntnis der Datenströme und ihre genaue Steuerung für zielgenaue Bereitstellung kritischer Applikationen an spezifische Nutzer
 - Nutzer-, Port- und Geräteebene (Paketklassifizierung auf Layer 2 bis 4)
 - QoS-Mapping für priorisierte Warteschlangen (Queues) (802.1p & IP ToS (Type of Service)/DSCP (Differentiated Services Code Point) für bis zu acht Queues pro Port)
 - Mechanismen für den Aufbau mehrerer gleichzeitiger Queues (SPQ (Strict priority Queuing), WFQ (Weighted Fair Queuing), WRR (Weighted Round Robin Queuing) und Hybrid)
 - Granulares QoS/Rate Limiting
 - VLAN für Policy Mapping
- Switching/VLAN Services – bietet hohe Performance Konnektivität, Aggregation und schnelle Recovery-Services

- Umfangreiche Industriestandard-Compliance (IEEE und IETF)
- Inbound- und Outbound-Bandbreitenkontrolle per Flow
- VLAN-Serviceunterstützung
- Link Aggregation (IEEE 802.3ad)
- Multiple Spanning Trees (IEEE 802.1s)
- Schnelle Rekonfiguration von Spanning Trees (IEEE 802.1w)
- Provider Bridges (IEEE 802.1ad), Q-in-Q Ready
- Flow Setup Throttling
- Verteiltes IP Routing – bietet dynamische Verkehrsoptimierung, Broadcast Eindämmung und effizientere Netzwerkausfallsicherheit
 - Zu den Standard-Routing-Features gehören statische Routen, RIPv1/ RIPv2, Ipv4 und Multicast Routing Unterstützung (DVMRP, IGMP v1/v2/v3), Policy-basiertes Routing und Route Maps, VRRP
 - Zu den lizenzierten Routing-Features gehören OSPF v1/v2, PIM-SM und Ipv6
 - Erweiterte ACLs
- Sicherheit (Nutzer, Netzwerk und Management)
 - Nutzersicherheit
 - Authentifizierung (802.1x, MAC, PWA+ und CEP), MAC (statisch und dynamisch) Port Locking
 - Multiuser Authentifizierung / Policies
 - Netzwerksicherheit
 - Einfache und erweiterte ACLs
 - Policy-basierte Sicherheitsservices (Beispiel: Spoofing, nicht unterstützter Protokollzugang, Intrusion Prevention, DoS-Attacken-Limitierung)
 - Management-Sicherheit
 - Sicherer Zugang zur K-Serie via SSH, SSL, SNMP v3
- Management, Kontrolle und Analyse – bietet modernisierte Werkzeuge, um Netzwerkverfügbarkeit und -zustand zu bewahren
 - Konfiguration
 - Industriestandard CLI und Web-Management Unterstützung
 - Multiple Firmware-Images mit editierbaren Konfigurationsdateien
 - Netzwerkanalyse
 - SNMP v1/v2/v3, RMON (9 Gruppen) und SMON (RFC 2613) VLAN und Stats
 - Port/VLAN Spiegelung (1-to-1, 1-to-many, many-to-many)
 - Nicht gesampleter NetFlow auf jedem Port ohne Einfluss auf System Switching- und Routing-Performance
 - Automatisiertes Set-Up und Rekonfiguration

- Ersatz-I/O Module übernehmen automatisch die Konfiguration von ausfallenden Modulen

Viele zusätzliche Funktionen und Eigenschaften der K-Serie – einige Beispiele:

- NetFlow – für Echtzeit-Transparenz, Applikationsprofiling und Kapazitätsplanungen
- LLDP-MED (Link Layer Discovery Protocol für Medien-Endpunkt- Geräte) - verbessert VoIP-Umgebungen
- Flow Setup Throttling (FST) –effektive Vorbelegung und Schutz vor DoS Attacken
- Web Cache Redirect – erhöht WAN- und Internet-Bandbreiteneffizienz
- Node & Alias Location – verfolgt Nutzer- und Gerätelokation automatisch und verbessert die Produktivität des Netzwerkmanagement und die Fehlerisolation
- Port Protection Suite – bewahrt Netzwerkverfügbarkeit durch Sicherung eines guten Verhaltens von Protokollen und Endgeräten
- Flex-Edge-Technologie –erweitertes Bandbreitenmanagement und -zuweisung für anfragende Access / Edge Geräte

Jedes Gerät der K-Serie bietet hohe Netzwerkperformance, Management- und Sicherheitsfeatures via NetFlow, ohne die Switching- oder Routingleistung zu beeinflussen. Auch teure Tochterkarten für jedes Blade sind unnötig. Die K-Serie verfolgt jedes Paket in jedem Datenstrom – im Gegensatz zu den statistischen Stichprobentechniken andere Produkte auf dem Markt. Das liegt an den maßgeschneiderten Extreme-ASICs, die NetFlow-Statistiken für jedes Paket in jedem Flow sammeln, ohne dass die Leistung sinkt.

Flow Setup Throttling (FST) ist eine Funktion für vorbeugende Aktionen gegen Zero-Day- und Denial of Service (DoS)-Attacken, bevor sie das Netzwerk beeinträchtigen können. FST bekämpft die Auswirkungen solcher Angriffe, indem die Funktion direkt die Zahl neuer oder existierender Datenströme an jedem individuellen Switchport begrenzt. Sie kontrolliert, wie viele Flows eintreffen und misst, wann die maximal erwünschte Flow-Zahl erreicht ist.

Im Netzwerkbetrieb kostet es viel Zeit, ein Gerät zu lokalisieren oder herauszufinden, wo genau ein Nutzer angebunden ist. Dies ist besonders wichtig, wenn man auf Sicherheitsverletzungen reagiert. Die Module der Extreme K-Serie lesen den Netzverkehr komplett mit, sobald Pakete den Switch passieren und verfolgen dabei automatisch auch die Standortinformationen von Nutzern und Geräten. Mit diesen Informationen, etwa der MAC-Adresse einer Station oder dem Layer-3-Alias (IP Adresse, IPX Adresse, etc.) wird dann die Node/Alias-Tabelle bestückt. Die Managementtools der Extreme NMS Suite nutzen dann diese Informationen, um schnell die Switch- und Port-Nummer jeder IP Adresse zu ermitteln und bei einer Sicherheitslücke Maßnahmen gegen dieses Gerät zu ergreifen. Diese Node- und Alias-Funktionalität – die derzeit nur Extreme bietet - hilft, Probleme statt in Stunden innerhalb von Minuten genau zu orten.

Für Organisationen, die UC (Unified Communications) einsetzen wollen, bietet die K-Serie Policy-basierte Automation. Die Systeme unterstützen mehrere standardbasierte Erkennungsmethoden, inklusive LLDP-MED, SIP (Session initiation Protocol) und H.323, um UC-Dienste für IP Telefone aller großen Hersteller automatisch zu erkennen und bereitzustellen. IP-Clients werden durch die Switches der K-Serie ohne Administrationsaufwand mobil. Zieht ein IP Telefon um oder wählt sich andernorts ins Unternehmensnetzwerk ein, wandern alle VoIP-, Sicherheits- und Prioritätseinstellungen automatisch mit. Dasselbe gilt für Ergänzungen und Änderungen des Netzes.

Ports lassen sich mit den Geräten der K-Serie vielfältig und umfassend schützen. Zu den Portschutzfunktionen gehören zum Beispiel SPANguard und MACLock. SPANguard erkennt unautorisierte Bridges im Netz, MACLock weist einer MAC Adresse einen spezifischen Port zu, auf andere Ports hat sie keinen Zugriff. Weitere Möglichkeiten sind Link Flap, Broadcast-Unterdrückung und Spanning-Tree-Loop-Schutz - alles Funktionen zur Verhinderung von Fehlkonfigurationen und Protokollfehlern.

Die Flex-Edge-Technologie der Extreme K-Serie klassifiziert Datenströme mit Leitungsgeschwindigkeit für alle Zugangsports. Dabei erhalten Steuer- und Überwachungsdaten sowie hochpriorisierter Verkehr garantiert Vorrang vor anderen Datenströmen. Die diesbezüglichen Regeln werden in einer übergreifenden Policy (Extreme Policy Overlay) festgelegt. Außerdem kann auch jedem authentifizierten Nutzer an jedem Port, den der Administrator dafür bestimmt, priorisierte Bandbreite zugewiesen werden. Flex-Edge Technologie ist ideal für den Einsatz in Schaltschränken und Verteilerpunkten, die oft veraltet sind. Das kann zu Netzwerkengpässen führen, die wiederum in Topologieänderungen und zufälligen Paketausschüssen resultieren können. Flex Edge verhindert solche Störungen.

Komponenten

Part Number	description
K6 Chassis	
K6-Chassis	K-Series 6 Slot Chassis and Fan Tray
K6-FAN	K6 Fan Tray - Spare
K6-MID-KIT	K6 Mid-Mount Kit
K10 Chassis	
K10-Chassis	K-Series 10 Slot Chassis and Fan Tray
K10-FAN	K10 Fan Tray - Spare
K10-MID-KIT	K10 Mid-Mount Kit
Power Supplies and Accessories	
K-AC-PS	K-Series Power Supply, 15A, 100-240VAC input, (600W system, 400/800W POE)
K-POE-4BAY	K-Series External 4 Bay Power Shelf
K-POE-4BAY-RAIL	Mounting Kit for K-POE-4BAY

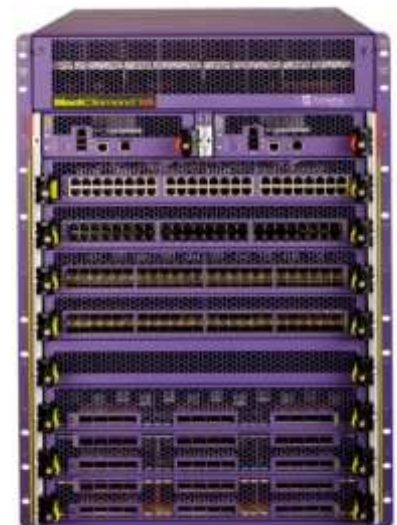
K-POE-CBL-2M	K-Series PoE Power to K Chassis Cable - 2M
I/O Fabric Modules	
KK2008-0204-F2	K10 Management/Fabric Module (4) 10GB via SFP+
KK2008-0204-F2G	K10 Management/Fabric Module (4) 10GB via SFP+(TAA Compliant)
KK2008-0204-F1	K6 Management/Fabric Module (4) 10GB via SFP+
KK2008-0204-F1G	K6 Management/Fabric Module (4) 10GB via SFP+(TAA Compliant)
I/O Modules	
KT2006-0224	K-Series (24) Port 10/100/1000 802.3at RJ45 PoE IOM
KT2006-0224-G	K-Series (24) Port 10/100/1000 802.3at RJ45 PoE IOM (TAA Compliant)
KT2010-0224	K-Series (24) Port 10/100/1000 802.3at Mini-RJ21 PoE IOM
KT2010-0224-G	K-Series (24) Port 10/100/1000 802.3at Mini-RJ21 PoE IOM (TAA Compliant)
KG2001-0224	K-Series (24) Port 1Gb SFP IOM
KG2001-0224-G	K-Series (24) Port 1Gb SFP IOM (TAA Compliant)
KK2008-0204	K-Series (4) Port 10Gb SFP+ IOM
Licenses	
K-EOS-L3	Advanced Routing License (OSPF, VRF, PIM-SM)
K-EOS-PPC	K-Series Per Port User Capacity License Upgrade

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/k-series

BDX8

Aktuelle Rechenzentren verlangen heute nach hochgradig virtualisierter, konvergenter und hoch-skalierbarer Infrastruktur. Integration unterschiedlicher Benutzergruppen, Trennung von Klienten und Cloud Computing Applikationen erfordern einfach zu betreibende und dennoch hoch virtualisierte Netzwerkkumgebungen, die in sogenannten Fabric-Lösungen implementiert werden. Erweiterbarkeit, Hochverfügbarkeit und hohe Durchsatzraten werden hier selbstverständlich. Die Extreme Networks Open Fabric Lösung, im Kernbereich dargestellt durch das Flaggschiff des Portfolios, den X8, bietet unterbrechungsfreie Konnektivität durch ein übersichtliches, skalierbares und zentral verwaltbares Netzwerk.



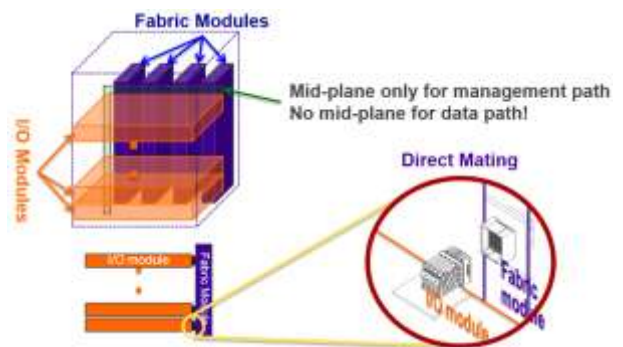
Der X8 ist das Kernstück der Lösung für sehr große Data-Center Betreiber (Cloud Lösungen), High Performance Computing (HPC), große Enterprise Umgebungen und Internet Exchange Points (IXP) und liefert hochperformante und –skalierbare, überbuchungsfreie Netze für Anschluß-Geschwindigkeiten von 100 MbE bis 100 GbE vom Access bis zum Core. All das in kompakter Bauweise, die es ermöglicht, bis zu 3 Systeme in einem Netzwerkschrank unterzubringen. Die hohe Portdichte des X8 ermöglicht den Verzicht auf teure und komplexe Multilayer Netzarchitekturen, die durch große Anzahlen von aktiven Verbindungen zwischen den Systemen, überbuchte Zwischenebenen und dadurch zusätzliche Latenzen weitere Nachteile für den Betrieb mit sich bringen. Durch das energiesparende Hardware Design eignet er sich ideal für den Einsatz in energiekritischen Umgebungen und unterstützt so bei der Optimierung der Betriebskosten.

“Cloud Scale“ Switching

Die X8 bieten entweder 10,24 oder 20,48 Tbps (Terabit per seconds) Switching Durchsatz und unterstützen bis zu 384 100/1000/10000 MbE RJ45 (oder alternativ 1GbE SFP), 768 10GbE SFP+, 192 40GbE QSFP+ oder 32 100GbE CFP2 blockierungsfreie Ports in einem Chassis. Dies ermöglicht Portdichten bis zu 1.152 1GbE / 2.304 10GbE / 576 40GbE oder 96 100GbE Ports, selbstverständlich auch in gemischter Portbestückung, in einem 19“ Netzwerkschrank.

Effizientes Hardware Design

Das intelligente Hardware Design des X8 nutzt die direkte orthogonale Verbindung der frontseitig eingeschobenen Anschlußmodule zu den von der Rückseite bestückten Switch Fabric Modulen und verzichtet auf Durchsatz begrenzende Backplane bzw. Midplane Baugruppen. Der X8 ermöglicht zurzeit bis zu 1,28 TBits unidirektionale Switching Bandbreite pro Slot, die gewählte Architektur ermöglicht zukünftig jedoch weiteres Wachstum.



Integrierte skalierbare Servervirtualisierung

Die X8 Serie nutzt das modulare Extreme EXOS Betriebssystem und bietet damit eine skalierbare Plattform für virtualisierte Umgebungen. Das System unterstützt bis zu 128.000 (zukünftig bis zu 1 Mio.) virtuelle Maschinen verteilt auf bis zu 768 angeschlossene Server pro Chassis und ermöglicht so hochintegrierte virtuelle Lösungen.

Das EXOS stellt hierbei die hochperformante Steuerungsebene dar und vereinfacht dabei die Netzwerkinstallation und den Betrieb durch virtualisierungs-unterstützende Funktionalitäten wie EXOS Network Virtualization (XNV™) und Extreme Networks Direct Attach™. XNV erlaubt die automatisierte Provisionierung virtueller Port Profile (VPP) mit Regelwerken für virtuelle Server Umgebungen unter Einbeziehung der jeweiligen Hypervisorinstanzen und bietet hierdurch eine vereinfachte Verwaltung für

die virtuellen Serverinstanzen. Der Umzug eines virtuellen Servers von einer physikalischen Ressource auf eine andere führt dadurch zur automatischen Anpassung der assoziierten Switch Port Konfiguration.

Direct Attach™ unterstützt Rechenzentrumsbetreiber bei der Vereinfachung der Netzwerkinfrastruktur durch die Eliminierung der virtuellen Switches in den virtuellen Server Umgebungen. Unterschiedliche Funktionen, wie Multi-Chassis Link Aggregation (M-LAG) und „Port Isolation“, erlauben ein flacheres, weniger hierarchisches Design der Network Fabric für hochskalierte, durch unterschiedliche Benutzergruppen genutzte Rechenzentren. Somit kann man auf dedizierte funktionsbezogene Netze und den Einsatz des Spanning Tree Protokolls (STP) verzichten.

Zuverlässigkeit für konvergente Storage-Anbindungen

Der X8 ist die optimale Lösung für hochperformante Storage Applikationen wie Server Replizierung, Data-Center Disaster Recovery und High Performance Compute Cluster (HPC) Anwendungen. Die X8 Serie unterstützt IEEE Data Center Bridging (DCBx) für IP basierte Storage Anwendungen wie iSCSI, NFS oder CIFS über ein konvergentes Netzwerk. Durch die IEEE kompatible Implementation von verlustfreiem (Lossless) Ethernet mit Priority Flow Control (PFC) und Enhanced Transmission Selection (ETS), können diese Storage Protokolle priorisiert, mit garantierter Bandbreite verarbeitet und verlustfrei transportiert werden.

Die X8 Serie eignet sich zusätzlich für den Transport von Fiber Channel over Ethernet (FCoE) und stellt so eine kostengünstige Alternative zur Anbindung von Speichersystemen über hochperformante 10 GbE und 40 GbE Schnittstellen dar.

Low Latency für schnellere Antwortzeiten

Low Latency Applikationen wie High Performance Computing (HPC) oder High Frequency Trading (HFT) erfordern sehr kurze Latenzzeiten in der eingesetzten Infrastruktur. Die X8 Serie eignet sich durch ihre Latenz von 2,3 Mikrosekunden vom Eingangs- zum Ausgangsport auch modulübergreifend hervorragend für ein solches „Fabric-in-a-Box“ Szenario. In Designs mit angeschlossenen X670/X770 Systemen als Top-of-Rack Systeme, erreicht dieses „Open Fabric“ Design Latenzen unter 3 Mikrosekunden. Die Latenz innerhalb eines Modules erreicht dabei Werte von unter 1 Mikrosekunde.

Die steigende Anzahl von mobilen Netzteilnehmern und der Anstieg von zentral gehosteten Applikationen im Rechenzentrum führen zu ständig steigendem Verkehrsaufkommen innerhalb des Rechenzentrums (East-West-Traffic) und beim Verkehr vom Rechenzentrum in Richtung des Anwenders (North-South-Traffic). Die Gesamtlatenz für die Anwendung resultiert aus der Addition der Latenzen für die Verarbeitung der Daten (Compute), den Zugriff auf den Datenbestand (Storage) und den eigentlichen Daten-Transport (Transmission). Hierbei ist die niedrige Latenz der X8 Systeme ein wichtiger Baustein für die Zufriedenheit der Anwender und optimiert die gesamte Antwortzeit der eingesetzten Applikationen.

Netzwerkmanagement durch Software Defined Networking (SDN)

Software Defined Networking (SDN) ist der revolutionäre Ansatz für das Design und den Betrieb zukünftiger Netze. SDN vereinfacht die Virtualisierung, Visualisierung, Optimierung und die Verwaltung (Orchestration) von Netzwerk, Rechenleistung und Speicherverwaltung aus einer einzigen granularen Kommando- und Kontrollinstanz heraus.

Die X8 Serie unterstützt den OpenFlow Standard für SDN Controller auf Open Source Basis oder von Drittherstellern und stellt eine komplette SDN Netzwerk Lösung dar. Sie erlauben es Anwendern, SDN effizient auf einer programmierbaren und skalierbaren Fabric Plattform zu implementieren.

Zusätzlich unterstützt die X8 Serie das OpenStack Neutron Plugin für den Betrieb von Cloudlösungen. Sie können in hybriden Ansätzen gleichzeitig für SDN und herkömmliche Anwendungsszenarien genutzt werden. Standardapplikationen und selbsterstellte Programme können hierbei für den Netzwerkbetrieb, Verkehrskontrolle (Traffic Engineering), Quality-of-Service, Qualitätsmanagement (SLA Management), Überwachung (Monitoring), Analyse (Analytics), Virtualisierung oder weitergehende Anwendungen zum Einsatz kommen.

Hochskalierbare Routing-Instanzen

Zukünftig wird die X8 Serie zwei Varianten von Einschubmodulen unterstützen: die bereits verfügbaren non-XL-Module für hohe Portdichten, niedrige Latenz für mittelgroße Ausbaustufen im Access, Distribution oder Core Bereich und die geplanten XL-Module für hoch skalierbare Core und Übergangsszenarien mit großen Layer-2 und Layer-3 Tabellen. Hierbei werden bis zu 1 Million Layer-2/Layer-3 Einträge in den 40 GbE und 100 GbE Einschüben unterstützt (Verfügbarkeit geplant). Damit kann der X8 in Bereichen eingesetzt werden, die bisher durch deutlich teurere traditionelle Layer-3 Systeme im Data-Center Core erforderten.

Die XL- und non-XL-Varianten der Module können in einem Chassis ohne Einschränkung kombiniert betrieben werden, so dass nicht nur das Netzwerkdesign durch Konzentration auf wenige Komponenten vereinfacht werden kann, sondern auch die Implementierungs- und Betriebskosten optimiert werden. Die XL-Serien-Module können hierbei für hochskalierte Edge Anwendungen mit großer Anzahl von angeschlossenen Hostsystemen oder benötigten Access Control Listen (ACLs) eingesetzt werden, wie dies zum Beispiel bei Hosting Providern oder Cloud Dienstleistern der Fall ist. Die 40 GbE und 100 GbE Module unterstützen hierfür das aufteilen der Ports in 4 bzw. 10 10 GbE Ports für hochskalierbare Anforderungen, die hohe Portdichten erfordern.

Data-Center zu Data-Center Verbindung

Die X8 Systeme wurden als Systeme für die gemeinsame Nutzung für Data-Center Core und Data-Center Anbindungssystem designed. Hierfür stehen 10 GbE SFP+ und 100 GbE CFP2 Module für große Glasfaser-Distanzen zur Verfügung, die bis zu 80 km bzw. 10 km Entfernung überbrücken können. Die kommenden X8 XL-Module werden auch

sehr große Routing Tabellen und MPLS Skalierungen unterstützen und eliminieren damit den Bedarf an teuren Routing Systemen.

Die X8 Systeme bieten durch Virtual Private LAN Service (VPLS) Virtual Machine Mobilität über active/active Data-Center Grenzen hinweg. Virtuelle Routing (VR) Instanzen ermöglichen die logische Aufteilung der X8 Core Systeme in kleinere Einheiten, die den einzelnen VPLS Diensten für die komplette Isolierung der Dienste und der kundenbezogenen Instanzen zugeordnet werden können und so eine Nutzung für mehrere Anwendungsgruppen oder Kunden Ende-zu-Ende implementierbar machen.

Hochverfügbarkeit und Service Absicherung

Die heutigen Data-Center und Service Provider Netzwerke stellen hohe Anforderungen an die Verfügbarkeit der Komponenten. Netzwerkausfälle sind hier nicht tolerierbar, da dies zur Nichtverfügbarkeit angebotener Dienste führt und Kunden dies nicht mehr akzeptieren. Designed für den Einsatz in Tier-3 und Tier-4 Data-Centern und Service Provider Netzen verzichtet der X8 auf Single-Point-of-Failure im Hardware Design. Getrennte Control und Data Planes, redundante Management Module, N+1 redundante Switching-Fabric Einschübe und N+1 redundante Lüfter und Netzteile bieten den höchsten Grad an Redundanzen im Chassis. Die Netzteile verfügen ebenfalls über redundante Kontrollinstanzen und die Systeme lassen sich Phasen-redundant für höchste Ausfallsicherheit betreiben.



BlackDiamond X8 Chassis
Rückansicht mit Fabric Modulen

Auf Betriebssystemebene liefert das modulare EXOS die entsprechenden Hochverfügbarkeitsfunktionen und verfügt über Echtzeitmonitoring der individuellen Prozesse. Sollte unerwarteterweise ein Software Prozess nicht mehr verfügbar bzw. ansprechbar sein, wird dieser vom System automatisch neu gestartet, ohne das restliche System zu beeinflussen. Die X8 Serie verfügt über zahlreiche Hochverfügbarkeitsfunktionen wie In-Service-Software-Upgrades (ISSU) zur unterbrechungsfreien Aktivierung von Software Patches und Multi-Chassis Link Aggregation (M-LAG).

Optimierte Betriebskosten für bessere Total-Cost-of-Ownership (TCO)

Die X8 Serie wurde für effektive Kühlung und platzoptimierte Einsatzszenarien entwickelt. Die Leistungsaufnahme pro 10 GbE Port beträgt im Vollausbau maximal 5,6 Watt und wird neben dem gewählten Hardwareaufbau mit durchgängigen Lüftungswegen durch die temperaturabhängige Lüftersteuerung unterstützt. Somit wird ein sparsamer Betrieb in klimatechnisch kritischen Umgebungen ermöglicht und ein erhebliches Sparpotenzial beim Stromverbrauch erzielt.

Zusammenfassung

- High Density 1/10GbE, 40GbE und 100GbE Switch

- 768 Ports 10GbE pro Switch, bis zu 2.304 Ports pro Netzwerkschrank
- 384 Ports 100/1000/10000MbE RJ45 oder 1/10GbE SFP(+) pro Switch, bis zu 1.152 Ports pro Netzwerkschrank (using 10GbE)
- 192 Ports 40GbE QSFP+ pro Switch, bis zu 576 Ports pro Schrank
- 32 Ports 100GbE CFP2 pro Switch, bis 96 Ports pro Schrank
- Orthogonale Architektur mit 20.48Tbps Switching Kapazität
- 2.3 µSec Port-zu-Port Latenz fabricübergreifend, sub-µSec auf einem Modul
- High-scale Enterprise Routing mit zukünftig bis zu 1 Mio Hardware Einträgen L2/L3
- Software Defined Networking mit OpenFlow 1.3 und OpenStack Unterstützung
- Enterprise und IXP fokussierter MPLS Support
- Converged Fabric für zuverlässige IP-basierte SAN Anbindung und FCoE Transit Verkehr
- Niedriger Stromverbrauch von 5.6 Watt pro 10GbE für optimiertes Total Cost of Ownership

Bestellhinweise

Bestellnummer	Produktbezeichnung	Beschreibung
48001	BDX8-AC	BlackDiamond X8 Serie Chassis mit 8 Einschubslots. Das Chassis enthält die 5 zum Betrieb benötigten Lüfter Baugruppen. Power Supplies und Blank Panels für nicht benutzte Einschubslot müssen separat bestellt werden
48021	BDX-MM1	Management Module 1 für die BlackDiamond X Serie. Benötigt wird mindestens 1 MM1 Module, 2 Modules werden für optionale 1+1 Redundanz benötigt
48032	BDXA-FM10T	2,56Tbps Fabric Module für BlackDiamond X Chassis. Es werden 3 Module für überbuchungsfreien Durchsatz benötigt, das vierte Modul ermöglicht volle N+1 Redundanz bei voller 10Tbps Performanz
48031	BDXA-FM20T	5,12Tbps Fabric Module für BlackDiamond X Chassis. Es werden 3 Module für überbuchungsfreien Durchsatz benötigt, das vierte Modul ermöglicht volle N+1 Redundanz bei voller 10Tbps Performanz
48040	BDXA-10G48T	48-Port 10GBASE-T RJ45 Module für die BlackDiamond X Serie. Bis zu 8 Module werden pro Chassis unterstützt. Es stehen damit bis zu 384 wirespeed 100/1000/10000MbE (10GbE) Kupfer Ports zur Verfügung. Das Modul wird von den 2,56 oder 5,12Tbps Fabric Modules unterstützt
48041	BDXA-10G48X	48-Port 10GBASE-X SFP+ Module für die BlackDiamond X Serie. Bis zu 8 Module werden pro Chassis unterstützt. Es stehen damit bis zu 384 wirespeed 1000/10000 Base-X SFP+ Ports zur Verfügung. Das Modul wird von den 2,56 oder 5,12Tbps Fabric Modules unterstützt. Optiken und Kabel sind optional erhältlich
48046	BDXA-40G12X	12-Port 40GBASE-X QSFP+ Module für die BlackDiamond X Serie. Bis zu 8 Module werden pro Chassis unterstützt. Es stehen damit bis zu 96 wirespeed 40 GbE Ports oder 384 wirespeed 10 GbE Ports zur Verfügung.

		Das Modul wird von den 2,56 oder 5,12Tbps Fabric Modules unterstützt. Optiken und Kabel sind optional erhältlich
48047	BDXA-40G12X-XL	12-Port 40GBASE-X QSFP+ Module für die BlackDiamond X Serie, wie oben beschrieben. Erweiterte Kapazitäten mit bis zu 1 Mio TCAMS für den Einsatz in komplexen Szenarien.
48051	BDXA-40G24X	24-Port 40GBASE-X QSFP+ Module für die BlackDiamond X Serie. Bis zu 8 Module werden pro Chassis unterstützt. Es stehen damit bis zu 192 wirespeed 40 GbE Ports oder 768 wirespeed 10 GbE Ports zur Verfügung. Das Modul wird von den 5,12Tbps Fabric Modules unterstützt. Optiken und Kabel sind optional erhältlich
48061	BDXB-100G4X	4-Port 100GBASE-X CFP2 Module für die BlackDiamond X Serie. Bis zu 8 Module werden pro Chassis unterstützt. Es stehen damit bis zu 32 wirespeed 100 GbE Ports oder 320 wirespeed 10 GbE Ports zur Verfügung. Das Modul wird von den 2,56 oder 5,12Tbps Fabric Modules unterstützt. Optiken und Kabel sind optional erhältlich
48062	BDXB-100G4X-XL	4-Port 100GBASE-X CFP2 Module für die BlackDiamond X Serie, wie oben beschrieben. Erweiterte Kapazitäten mit bis zu 1 Mio TCAMS für den Einsatz in komplexen Szenarien.
48011	BDX-PSU-AC2500	2500W 230V AC Power Supply für BlackDiamond X Serie Chassis. Es werden maximal 4 für volle Bestückung benötigt. Bis zu 8 Netzteile werden pro BDX8 Chassis unterstützt.
48018	BDX-IO-BLANK-E	Blank Panel für BlackDiamond X Serie Chassis. Diese Panels sichern die korrekte Systembelüftung in ungenutzten Einbauplätzen.

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/blackdiamond-x-series

BD8000

Die 8800 Serie ist eine flexible Lösung für Anwendungsfälle in den Bereichen Enterprise Core und Aggregation, chassisbasierender Access, Data-Center und Service-Provider Netzwerke. Hierfür stehen unterschiedliche Interfacemodule in skalierbarer Leistungsfähigkeit und Portdichte zur Verfügung, die Gigabit Ethernet (GbE), Power over Ethernet (PoE), 10 GbE und 40 GbE Schnittstellen bieten. Man kann bei den Einschubmodulen aus drei unterschiedlichen Leistungsklassen wählen und damit passend auf alle gestellten Anforderungen reagieren. Durch die Verfügbarkeit von Modulen mit hohen Portdichten können in vielen Fällen Netzwerkebenen konsolidiert und somit eine vereinfachte Netzstruktur und ein optimiertes Netzwerk Design erreicht werden.

Mit den Modulen der 8900-xl Serie eignet sich das System auch für Service Provider, die konvergente Dienste für ihre Kunden anbieten und hierfür sehr umfangreiche Adressspeicherkapazitäten im System benötigen. Die vollständige Unterstützung von IPv4 und IPv6 auf OSI Layer 2-4 unterstützt die Netzwerkadministratoren beim

Auflösen von Engpässen im Netzwerk und bei der Aggregation von Hochgeschwindigkeitsverbindungen. Im Accessbereich stellt das System eine optimierte Lösung für anspruchsvolle Anwendungen in den Bereichen Voice-over-IP, Video, Multicast und konvergenten LAN / WLAN Infrastrukturen dar.

Einsatzbereiche:

- Hochperformanter Core Switch für mittelgroße und große Netze
- Skalierbarer und hochverfügbarer Metro Service Provider Core
- High-Density Core oder End-of-Row System für Data-Center und High Performance Compute Cluster (HPCC)
- Kostengünstiges Chassis System für den Netzwerk Access Bereich

Chassis Varianten

Die 8800 Serie ist in zwei Chassis Varianten Verfügbar. Der d 8810 verfügt über 10 Einschubslots, von denen acht für Netzwerkinterface-Karten zur Verfügung stehen. Jeweils die beiden mittleren Slots sind für den Einbau der Management Switch Module (MSM) vorgesehen. Hierbei wird ein Modul für den Betrieb, das zweite für die Schaffung der Redundanz benötigt.

Hochverfügbarkeit

Die 8800 Plattform bietet umfangreiche Funktionen im Bereich der Hochverfügbarkeit auf Hardware und auf Software Ebene. Als Betriebssystem kommt das modulare EXOS zum Einsatz, das diese Funktionen unterstützt und um softwarebasierte Funktionalitäten erweitert.

Redundantes Hardware Design durch modulares Management

Die 8800 Serie unterstützt optional den Einsatz von redundanten Management Modulen, die im Fehlerfall den Ausfall eines Management Switch Moduls (MSM) automatisch erkennen und den Betrieb durch die Aktivierung des redundanten Management Switch Moduls unterbrechungsfrei gewährleisten (MSM Takeover). Es stehen drei unterschiedliche Varianten von MSM Modulen zur Verfügung. Hierbei bieten die Einstiegsmodelle MSM-24 eine Switching Bandbreite von 24 Gbps pro Slot. Die MSM-24 Module arbeiten im Cold-Standby Betrieb, d. h. das System wird bei Ausfall des primären MSM Moduls neu gestartet. Die MSM-48 Module arbeiten hier im Hot-Standby und Load Sharing Betrieb und stellen dann im Loadsharing 48 Gbps je Slot zur Verfügung. Bei Ausfall des MSM-48 Moduls bleibt das System voll funktionsfähig, die Management Funktion des MSM Moduls bietet dann volle Redundanz. Die Switchingfabric des ausgefallenen MSM Moduls steht dann unter Umständen nicht mehr zur Verfügung, wodurch sich die zur Verfügung stehende Bandbreite je Slot auf 24 Gbps minimiert.

Für die MSM-128 Module gilt das gleiche Verhalten wie für die MSM-48 Module, jedoch stehen im Betrieb mit 2 MSM-128 Modulen für die 8900 Serien Module bis zu 160 Gbps im 8806 Chassis oder 80 Gbps im 8810 Chassis zur Verfügung.

Skalierbare Leistung

Die 8800 Interface Einschubmodule stehen in drei Leistungsklassen zur Verfügung:

- **8500 Serie Module:** 48-Port 10/100/1000 Base-T (optional mit PoE) oder 24-Port 1000-Base-X mit SFP Ports, 24 Gbps je Slot
- **8800 Serie Module:** 4 oder 8-Port 10 GbE mit XFP Ports, 24- oder 48-Ports 1000Base-X mit SFP Ports und 48-Ports 10/100/1000Base-T (optional mit PoE) mit 24 Gbps je Slot bei Verwendung einer MSM, 48 Gbps je Slot bei Nutzung von 2 MSM Einschüben
- **8900 Serie Module:** 8 Port 10 GbE mit XFP Ports, 24 Port 10 GbE mit SFP Ports, 48 Ports GbE mit 10/100/1000Base-T oder 1000Base-X in SFP Variante, 96 Port GbE mit MRJ21 Telco Technologie oder 6 Port 40 GbE mit QSFP+ Ports. Die Module der – xl Serie verfügen über externen TCAM Speicher und unterstützen bis zu 512.000 MAC/IP Adress-Einträge.

Passives Chassis Design

Die 8800 Serie verfügt über eine passive Backplane, ergänzt durch isolierte Control- und Data-Planes, redundante Lüfter- und Netzteilsteuerungsmodule und unterschiedliche Sensoren, die auf geänderte Umgebungsveränderungen wie Temperaturschwankungen reagieren und den Administrator informieren, bevor dies Auswirkung auf die Verfügbarkeit des Systemes hat.

Redundante Netzteile im Loadsharing Betrieb

Die 8800 Serie unterstützt bis zu 6 interne, im Betrieb tauschbare Netzteile, die im Loadsharing betrieben werden. Drei Netzteile reichen in Vollbestückung im 1/10 GbE Ausbau zum Erreichen einer 2+1 Redundanz. Zusätzlich stehen 3 Netzteile zur Unterstützung von Power-over-Ethernet (PoE) zur Verfügung.

Redundante Lüfter im Betrieb

Die Kühlung wird mit 9 (Modell 8810) bzw. 6 Lüftern (Modell 8806) gewährleistet. Diese sind auf einer Lüfterbaugruppe montiert, die im Betrieb unterbrechungsfrei getauscht werden kann.

Modulares Netzwerk Betriebssystem Extreme EXOS

Das Betriebssystem EXOS bietet sehr umfangreiche Features zur Bereitstellung von Netzredundanz im Bereich Layer-2 und im Bereich Layer-3. Im Layer-2 stehen Funktionen wie dynamischer und statischer Link Aggregation (802.3AD) MLAG (Multiswitch Link Aggregation), EAPS (Ethernet Automated Protection Switching), Standard Spanningtree (IEEE 802.1d/w), MSTP (IEEE 802.1s), PVST+ (Per Vlan Spanningtree) oder Ethernet Ring Protection Switching nach ITU G.8032 (ERPS) zur Verfügung. Im Layer-3 wird dies ergänzt durch Funktionen wie VRRP (Virtual Router Redundancy Protocol), OSPF ECMP (Open Shortest Path First mit Equal Cost Multi Path) oder ESRP (Extreme Standby Router Protocol™), die das dynamische Anpassen von Routing Informationen oder redundanten Wegen bereitstellen.

Verkehrsteuerungsmöglichkeiten durch hardwarebasierte Line-rate ACLs im Layer-2, -3 & 4 werden ebenso unterstützt wie die automatische Erkennung von Endgeräten mit Zuweisung von Benutzerprofilen über Protokolle wie LLDP, CDP (Cabletron Discovery Protokoll) oder basierend auf Netzwerklogin Funktionen (Netlogin).

EXOS bietet für den Access Bereich weitreichende Sicherheitsfunktionen wie Multi-User-/Multi-Suppliant-Authentisierung per MAC-Adresse, 802.1x oder Web-Portal mit dynamischer VLAN und Nutzerprofil Zuweisung mit ACL und QoS Parametrierung, die das System auch dort sinnvoll einsetzbar machen. Kerberos Snooping zum Monitoring des Benutzerlogin am Active Directory steht ebenfalls zur Verfügung.

Überzeugende Portdichten

Die 8800 Serie mit den 8900-xl oder -xm Serie Modulen bietet mit bis zu 196 10 GbE Ports, 776 GbE Kupfer Ports, 384 GbE SFP Ports oder 48 40 GbE Ports in einem 14,5 HE Chassis eine ausgezeichnete Portdichte für heutige Anforderungen.

Zusammenfassung

- Redundantes hochverfügbares Chassis System
- High-Density Gigabit, 10 Gigabit und 40 Gigabit Ethernet Switch
- Modulares Extreme EXOS Operating System (OS) für unterbrechungsfreien Netzwerkbetrieb
- Ethernet Automatic Protection Switching (EAPS) als Netzwerkredundanz Protokoll
- Sehr große Switching Kapazität mit bis zu 2,840 Mpps
- Unterstützung konvergenter Voice-over-IP (VoIP) Implementationen mit automatischer Provisionierung der Ports
- Flexible Anschluß Optionen für vielfältigste Anwendungen
- Effizientes Design für optimierten Stromverbrauch und niedrigen Kühlungsbedarf
- Tunable Dense Wavelength Division Multiplexing (DWDM) Optiken für optimale Nutzung der Glasfaser Infrastruktur
- Universal Port für die Einrichtung dynamischer Security Profile für das anwendungsoptimierte Netzwerk
- Threat Erkennung und Bekämpfung mit Hilfe der CLEAR-Flow Security Rules Engine
- Common Criteria EAL3+ Certified

	<p>8806 Chassis</p>
	<p>8810 Chassis</p>
	<p>MSM Modul</p>
	<p>S-10G1Xc Modul</p>
	<p>S-10G2Xc Modul</p>
	<p>S-G8Xc Modul</p>
	<p>8900-10G24X-c Modul</p>
	<p>8900-40G6X-xm Modul</p>
	<p>8900-xl Module</p>
	<p>8800-G48Xc Modul</p>

Bestellinformationen

Bestellnummer	Produktbezeichnung	Beschreibung
41011	10-Slot Chassis	BlackDiamond 8810 10-Slot Chassis mit Lüfter Modul
41012	6-Slot Chassis	BlackDiamond 8806 6-Slot Chassis mit Lüfter Modul
60020	700W/1200W 100-240V PSU	BlackDiamond 8800 700W/1200W 100-240V Netzteil
41050	600W/900W PSU	BlackDiamond 8806 600W/900W 100-240V Netzteil
60021	1200W -48V DC PSU	BlackDiamond 10808/BlackDiamond 8800 1200W - 48V DC Netzteil
Management Modules BlackDiamond 8900-Series		
41231	8900-MSM128	BlackDiamond 8900 Management Switch Module mit Erweiterungsslot für ein MSM Uplink Modul
Management Modules BlackDiamond 8800 c-Series		
41213	MSM-48c	BlackDiamond 8800 Management Switch Module mit Erweiterungsslot für ein MSM Uplink Modul
Management Modules BlackDiamond 8500-Series		
41251	8500-MSM24	BlackDiamond 8500 Management Switch Module mit Erweiterungsslot für ein MSM Uplink Modul
I/O Modules BlackDiamond 8900-xl/xm Series		
41711	8900-40G6X-xm	BlackDiamond 8900-xm 6-Port 40GBASE-X Modul mit QSFP+ Ports
41631	8900-10G8X-xl	BlackDiamond 8900 8-Port 10GBASE-X Modul mit XFP Ports
41531	8900-G48T-xl	BlackDiamond 8900 48-Port 10/100/1000BASE-T RJ-45 Modul, optional erweiterbar auf PoE 802.3af per PoE card (S-PoE)
41521	8900-G48X-xl	BlackDiamond 8900 48-Port 1000BASE-X Modul mit SFP Ports
I/O Modules BlackDiamond 8900-Series		
41632B	8900-10G24X-c	BlackDiamond 8900 24-Port 10GBASE-X SFP+ Modul
41532	8900-G96T-c	BlackDiamond 8900 96-port 10/100/1000BASE-T MRJ-21
I/O Modules BlackDiamond 8800 c-Series Modules		
41516	G48Te2	BlackDiamond 8800 48-port 10/100/1000BASE-T RJ-45 Modul, optional erweiterbar auf PoE 802.3af per PoE card (S-PoE)
41517	G48Tc	BlackDiamond 8800 48-port 10/100/1000BASE-T RJ-45 Modul, optional erweiterbar auf PoE 802.3af per PoE card (S-PoE)
41543	G24Xc	BlackDiamond 8800 24-Port 1000BASE-X Modul mit SFP
41544	G48Xc	BlackDiamond 8800 48-Port 1000BASE-X Modul mit SFP

41614	10G4Xc	BlackDiamond 8800 4-Port 10GBASE-XFP Modul mit XFP
41615	10G8Xc	BlackDiamond 8800 8-Port 10GBASE-XFP Modul mit XFP
I/O Modules BlackDiamond 8500-Series Modules		
41551	8500-G48T-e	BlackDiamond 8500 48-Port 10/100/1000BASE-T RJ-45 Modul, optional erweiterbar auf PoE 802.3af per PoE card (S-PoE)
41561	8500-G24X-e	BlackDiamond 8500 24-port 1000BASE-X SFP
MSM-Uplink Module		
41821	S-G8Xc	BlackDiamond 8800 8-Port 1G SFP Add-On Einschub für MSM
41822	S-10G1Xc	BlackDiamond 8800 1-port 10G XFP Add-On Einschub für MSM
41823	S-10G2Xc	BlackDiamond 8800 2-port 10GBASE-X SFP+ Add-On Einschub für MSM
41811	S-PoE	BlackDiamond 8800 PoE Add-On Einschub für RJ45 Module

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/blackdiamond-8800-series

X 770

Die X770-32q Produkt Familie liefert hohe 40 Gigabit Portdichten im kompakten 1 Höheneinheiten Format. Die Systeme sind Layer-2 und Layer-3 fähig (optional) und zeichnen sich durch sehr geringe Latenzzeiten aus. Sie unterstützen IPv4, IPv6 und Multicast Routing und eignen sich dadurch als Data-Center Aggregations- und Core Systeme.



Summit X770-32q Frontansicht



Summit X770-32q Rückansicht mit bestückten AC Netzteilen

Die X770 unterstützen das gleiche modulare und robuste Extreme EXOS® Netzwerk-Betriebssystem wie die anderen Extreme Networks Produkte und ermöglichen damit ein durchgängiges Betriebssystem mit einheitlichem Funktionsumfang in allen Bereichen des Netzes. Die X770-32q verfügen über 32x 40 GbE Ports die wahlweise QSFP+ Einschubmodulen, passiven oder aktiven QSFP+ Kabeln bestückt werden können. 24 der 32 zur Verfügung stehenden 40 GbE Ports können per Konfiguration für die Nutzung als 4 x 10 GbE Port aufgesplittet werden. Die verbleibenden 8 40 GbE Ports können ebenfalls als ein 10 GbE Port konfiguriert werden. Damit stehen dann bis

zu 104 10 Gigabit Ports in der kompakten Bauhöhe von 1 Höheneinheit zur Verfügung. Alternativ können bis zu 8 Ports 40 GbE und 96 Ports mit 10 GbE genutzt werden. Die X770 liefern hierbei bis zu 1904 Mpps Forwarding Rate und 2.560 GBps Switching Bandbreite.

High-Performance Stacking

Die X770 Systeme unterstützen folgende Stacking Methoden:

- SummitStack-V
- SummitStack-V160
- SummitStack-V320

SummitStack-V – flexibles Stacking über 10 GbE

Die SummitStack-V Funktion des EXOS Betriebssystems unterstützt die Nutzung von 2 10 GbE Ports als Stacking Ports. Hierfür werden die Ports 103 & 104 im 10 GbE Modus für Stacking verwendet. Durch den Einsatz von Standard Verkabelung wird die Komplexität bei der Planung und Inbetriebnahme von gestackten Systemen reduziert. SummitStack-V® ist kompatibel mit den X440, X460, X460-G2, X480, X670, X670V und X670-G2 Switches, die in der gleichen Version des Betriebssystems EXOS verfügbar sind.

SummitStack-V160/V320 – Flexibles Stacking über 40 Gigabit Schnittstellen

Die X770-32q können auch per 40 GbE QSFP+ Schnittstelle gestackt werden. Stacking kann hierbei über passive Kupfer Kabel (bis 5m), vorkonfektionierte aktive Glasfaser Kabel (bis 100m) oder über die QSFP+ Standard Optiken bis zu 10 km erfolgen. Diese Flexibilität in der Stacking Technologie ermöglicht eine optimale Nutzung als Unternehmens-Core-Ausstattung oder als Top-of-Rack System im Rechenzentrum, das schrankübergreifende Systeme ermöglicht. Hierbei stehen zwei unterschiedliche Geschwindigkeiten zur Auswahl: 160 Gbps und 320Gbps. Beim SummitStack-V160 werden die physikalischen Ports 31 & 32 genutzt, beim SummitStack-V320 werden 4 Ports (Port 29-32) verwendet.

Intelligentes Switching

Die X770 eignen sich hervorragend für den Einsatz als Layer-2 System und ermöglichen durch Funktionen wie „Policy-Based-Switching und -Routing“, Provider Bridging, ein- und ausgehende Accesslisten, Bandbreiten Regulierung in 8 kbps Stufen ein- und ausgehend sowie das komplette IPv4 und IPv6 Routing auch den Einsatz in komplexen und anspruchsvollen Unternehmensnetzwerken.

1588 Precision Time Protocol (PTP)

Die X770 liefern optional bei Bedarf Boundary Clock (BC), Transparent Clock (TC), und Ordinary Clock (OC) für Applikationen, die synchronisierte Phasen und Frequenzen auf Netzwerkebene erfordern, um Synchronität im Bereich von Millisekunden erfordern. Die gegebenenfalls erforderlichen Anschlüsse hierfür sind rückseitig vorhanden.

Low Latency Switching für Cluster Computing

Der Chipsatz der X770 unterstützt sogenanntes Cut-Through-Switching, dabei werden eingehende Pakete bereits zum Ausgangsport befördert, bevor das Paket vollständig im Switch angekommen ist. Dies ermöglicht Latenzzeiten kleiner als 600ns und eignet sich besonders für den Einsatz in latenzkritischen Cluster Netzwerken.

Green Design – Energieoptimiertes Design mit flexiblen Kühlungsoptionen

Die X770 Serie wurde energieoptimiert und umweltverträglich gestaltet. Der Energieverbrauch ist durch das energiesparende Design in allen Lastzuständen äußerst effektiv. Der Einsatz hocheffizienter Netzteile minimiert die entstehende Verlustleistung und vermindert dadurch die Entstehung unnötiger Abwärme. Zudem bietet die Serie AC und DC Netzteile als Option.

Designed für den Einsatz in großen Unternehmensnetzen & Cloud-Rechenzentren

Die X770-32q unterstützen viele Funktionen, die sie sich besonders für den Einsatz in Rechenzentren und Cloudlösungen empfehlen:

- Direct Attach (VEPA)
- EXOS Network Virtualization (XNV)
- Data Center Bridging (DCB)
- Priority Flow Control (PFC)
- Virtuelle Router Instanzen (VR)

MPLS – Multi Protocol Label Switching

Für Einsatzszenarien im Bereich von Carrier Ethernet Lösungen unterstützt die X770 Serie MPLS LSP basiertes Layer-3 Forwarding und hierarchisches VPLS (H-VPLS) für den Aufbau von transparenten LAN Diensten durch den Netzbetreiber. Mit Hilfe von H-VPLS kann der Netzbetreiber Layer-3 Netze durch Layer-3 Core Netzwerke erweitern und regionale VPLS Dienste miteinander verbinden.

Hochverfügbarkeitsfunktionalitäten

- Ethernet Automatic Protection Switching (EAPS)
- Ethernet Ring Protection Switching (G.8032 /ERPS)
- Spanningtree und Rapid Spanningtree Protokolle (IEEE 802.1d, IEEE 802.1w, MSTP und PVST+)
- Virtual Router Redundancy Protocol (VRRPv2/v3)
- Extreme Standby Router Protocol™ (ESRP)
- Equal Cost Multipath (ECMP)
- Link Aggregation mit LACP(802.3AD)
- Multiswitch Link Aggregation (MLAG)

Bestellhinweise

Die X770-32q werden generell bestückt mit redundanten Power Supplies und Lüfter Modulen als Bundle verpackt geliefert. Hierbei stehen Bundles für Front-to-Back (kühle Seite 164 von 264

Luft wird an den Ethernetports an der Front ins Gehäuse gesaugt und an der Rückseite abgegeben) und Back-to-Front (kalte Luft wird auf der Rückseite angesaugt und an der Frontseite mit den Ethernetports abgegeben) Lüftungsrichtung zur Verfügung. Für den Betrieb mit Gleichstrom-Versorgung stehen ebenfalls Bundles mit Front-to-Back- oder Back-To-Front-Kühlungsrichtung und Bundles mit gemischter AC & DC-Power Supply Bestückung zur Verfügung.

Bestellnummer	Produktbezeichnung	Beschreibung
17701	Summit X770-32q-FB-AC	32 40GBASE-X QSFP+ Ports (ohne Optiken) , ExtremeXOS Advanced Edge Lizenz, 2 Front-to-Back 550W AC Netzteile, 5 Front-to-Back Lüfter
17702	Summit X770-32q-BF-AC	32 40GBASE-X QSFP+ Ports (ohne Optiken) , ExtremeXOS Advanced Edge Lizenz, 2 Back-to-Front 550W AC Netzteile, 5 Back-to-Front Lüfter
17703	Summit X770-32q-FB-DC	32 40GBASE-X QSFP+ Ports (ohne Optiken) , ExtremeXOS Advanced Edge Lizenz, 2 Front-to-Back 550W DC Netzteile, 5 Front-to-Back Lüfter
17704	Summit X770-32q-BF-DC	32 40GBASE-X QSFP+ Ports (ohne Optiken) , ExtremeXOS Advanced Edge Lizenz, 2 Back-to-Front 550W DC Netzteile, 5 Back-to-Front Lüfter
17705	Summit X770-32q-FB-MIX	32 40GBASE-X QSFP+ Ports (ohne Optiken) , ExtremeXOS Advanced Edge Lizenz, 1 Front-to-Back 550W AC Netzteil, 1 Front-to-Back 550W DC Netzteil, 5 Front-to-Back Lüfter
17706	Summit X770-32q-BF-MIX	32 40GBASE-X QSFP+ Ports (ohne Optiken) , ExtremeXOS Advanced Edge Lizenz, 1 Back-to-Front 550W AC Netzteil, 1 Back-to-Front 550W DC Netzteil, 5 Back-to-Front Lüfter
10925	Summit 550W AC PSU FB	550W AC Netzteil für Summit Systeme, Front-to-Back Lüftungsrichtung
10926	Summit 550W DC PSU FB	550W DC Netzteil für Summit Systeme, Front-to-Back Lüftungsrichtung
10927	Summit 550W AC PSU BF	550W AC Netzteil für Summit Systeme, Back-to-Front Lüftungsrichtung
10928	Summit 550W DC PSU BF	550W DC Netzteil für Summit Systeme, Back-to-Front Lüftungsrichtung
17111	Summit X670 Lüfter Modul FB	Lüfter Modul für Summit X670 & X770 Systeme, Front-to-Back Lüftungsrichtung
17112	Summit X670 Lüfter Modul BF	Lüfter Modul für Summit X670 & X770 Systeme, Back-to-Front Lüftungsrichtung

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/summit-x770-series-2/

X 670

Die X670 Produktfamilie liefert hohe 10 Gigabit und 40 Gigabit Portdichten im kompakten 1 Höheneinheiten Format. Die X670 Systeme sind Layer-2 und Layer-3 fähig (optional) und zeichnen sich durch geringe Latenzzeiten aus. Sie unterstützen IPv4, IPv6 und Multicast Routing und eignen sich dadurch als Aggregations- und Core Systeme. Die X670 unterstützen das gleiche modulare und robuste Extreme EXOS® Netzwerk-Betriebssystem wie die anderen Extreme Networks Produkte und ermöglichen damit ein durchgängiges Betriebssystem mit einheitlichem Funktionsumfang in allen Bereichen des Netzes.

Die X670 Serie steht in 3 Ausführungen zur Verfügung:

- **X670-48x** – Der X670-48x verfügt über 48 SFP+ Ports, die wahlweise mit 1GbE SFP oder 10 GbE SFP+ Einschüben bestückt werden können und verfügt über 2 rückseitige Netzteilbauplätze.
- **X670V-48x** – Der X670V-48x bietet 48 SFP+ Ports, die wahlweise mit 1GbE SFP oder 10 GbE SFP+ Einschüben bestückt werden können. Zusätzlich besteht auf der Rückseite die Möglichkeit ein VIM-Erweiterungsmodul einzubauen und damit 4 Ports 40 GbE zusätzlich zu erhalten.
- **X670V-48t** – Der X670V-48t bietet 48 10GBase-T Ports, die triplespeed fähig implementiert sind und wahlweise mit 100 Mbit/s, 1 GBit/s oder 10 GBit/s betrieben werden können. Zusätzlich besteht auf der Rückseite die Möglichkeit ein VIM-Erweiterungsmodul einzubauen und damit 4 Ports 40 GbE zusätzlich zu erhalten. Die 10 GBase-T Ports 45-48 sind hierbei als Combo Ports ausgeführt und können alternativ mit SFP+ Modulen bestückt werden.

Die 40 Gigabit Ethernet Ports des optionalen VIM4-40G4X Modules sind zur Aufnahme der QSFP+ Optiken oder vorkonfektionierter Kupfer oder Glasfaserkabel geeignet.

Die einzelnen 40 GbE Ports können per Software Konfiguration für die unterschiedlichen Anwendungen eingestellt werden:

- Nutzung als nativer 40 Gigabit Uplink
- Nutzung als 4 x 10 GbE Port aufgesplittet
- Nutzung als SummitStack-V80/V160 oder -V320 Port

High-Performance Stacking

Die X670 Systeme unterstützen vier unterschiedliche Stacking Methoden:

- SummitStack-V
- SummitStack-V80
- SummitStack-V160
- SummitStack-V320

SummitStack-V – flexibles Stacking über 10 GbE

Die SummitStack-V Funktion des EXOS Betriebssystems unterstützt die Nutzung von 2 der nativen 10 GbE Ports auf der Frontseite der X670 Modelle als Stacking Ports über Standard SFP+ Kabel oder Optiken. So werden Entfernungen von bis zu 40 km als Stacking Verbindung überbrückt. Durch den Einsatz von Standard Verkabelung wird die Komplexität bei der Planung und Inbetriebnahme von gestackten Systemen reduziert. SummitStack-V® ist kompatibel mit X440, X460, X460-G2, X480, X670, X670V, X670-G2 und X770 Switches, die in der gleichen Version des Betriebssystems EXOS verfügbar sind.

SummitStack-V80/V160/V320 – Flexibles Stacking über 40 Gigabit

Die X670V-48x und X670V-48t können beim Einsatz des optionalen VIM4-Modules zusätzlich über die rückseitigen 40 GbE QSFP+ Schnittstellen des VIM Modules gestackt werden. Hierbei stehen drei unterschiedliche Geschwindigkeiten zur Auswahl: 80 Gbps, 160 Gbps und 320 Gbps. Stacking kann hierbei über passive Kupfer Kabel (bis 5m), vorkonfektionierte aktive Glasfaser Kabel (bis 100m) oder über die QSFP+ Standard Optiken bis zu 10 km erfolgen. Diese Flexibilität in der Stacking Technologie ermöglicht eine optimale Nutzung als Unternehmens-Core-Ausstattung oder Top-of-Rack System im Rechenzentrum, das schrankübergreifende Systeme ermöglicht.

Intelligentes Switching

Die X670 eignen sich hervorragend für den Einsatz als Layer-2 System und ermöglichen durch Funktionen wie „Policy-Based-Switching und -Routing“, Provider Bridging, ein- und ausgehende Accesslisten, Bandbreiten Regulierung in 8 kbps Stufen ein- und ausgehend sowie das komplette IPv4 und IPv6 Routing auch den Einsatz in komplexen und anspruchsvollen Unternehmensnetzwerken.

Audio Video Bridging (AVB)

Audio Video Bridging ermöglicht zuverlässige Audio- und Video-Übertragung in Echtzeit, basierend auf Ethernet Netzwerk Infrastruktur. Die AVB Technologie bietet die entsprechenden Quality-of-Service und Multicast Funktionen, um die Anforderungen von zeitsensitiven und latenzkritischen Applikationen zu erfüllen. Die Systeme der X670 Serie unterstützen diesen IEEE 802.1 Standard.

Low Latency Switching für Cluster Computing

Der Chipsatz der X670 unterstützt sogenanntes Cut-Through-Switching, dabei werden eingehende Pakete bereits zum Ausgangsport befördert, bevor das Paket vollständig im Switch angekommen ist. Dies ermöglicht Latenzzeiten kleiner 1 ms und eignet sich besonders für den Einsatz in latenzkritischen Cluster Netzwerken.

Green Design – Energieoptimiertes Design mit flexiblen Kühlungsoptionen

Die X670 Serie wurde energieoptimiert und umweltverträglich gestaltet. Der Energieverbrauch ist durch das energiesparende Design in allen Lastzuständen äußerst effektiv. Der Einsatz hocheffizienter Netzteile minimiert die entstehende Verlustleistung

und vermindert dadurch die Entstehung unnötiger Abwärme. Die X670 Serie bietet AC und DC Netzteile als Option.

Designed für den Einsatz in Cloud Rechenzentren

Die Systeme der X670 Serie unterstützen viele Funktionen, wodurch sie sich besonders für den Einsatz in Rechenzentren und Cloudlösungen eignen:

- Direct Attach (VEPA)
- EXOS Network Virtualization (XNV)
- Data Center Bridging (DCB)
- Priority Flow Control (PFC)
- Virtuelle Router Instanzen (VR)

MPLS – Multi Protocol Label Switching

Für Einsatzszenarien im Bereich von Carrier Ethernet Lösungen unterstützt die X670 Serie MPLS LSP basiertes Layer-3 Forwarding und hierarchisches VPLS (H-VPLS) für den Aufbau von transparenten LAN Diensten durch den Netzbetreiber. Mit Hilfe von H-VPLS kann der Netzbetreiber Layer-3 Netze durch Layer-3 Core Netzwerke erweitern und regionale VPLS Dienste miteinander verbinden.

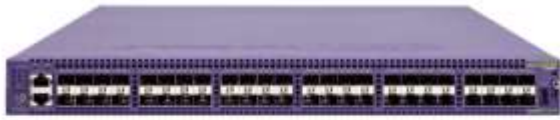
Hochverfügbarkeitsfunktionalitäten

- Ethernet Automatic Protection Switching (EAPS)
- Ethernet Ring Protection Switching (G.8032 /ERPS)
- Spanningtree und Rapid Spanningtree Protokolle (IEEE 802.1d, IEEE 802.1w, MSTP und PVST+)
- Virtual Router Redundancy Protocol (VRRPv2/v3)
- Extreme Standby Router Protocol™ (ESRP)
- Equal Cost Multipath (ECMP)
- Link Aggregation mit LACP (802.3AD)
- Multiswitch Link Aggregation (MLAG)

Bestellhinweise

Die X670 Systeme in SFP+ Ausführung (X670-48x & X670V-48x) werden ohne Power Supplies geliefert. Diese sind separat zu bestellen, hierbei wird ein Netzteil für den Betrieb und ein zweites für eine eventuelle Redundanz benötigt. Es stehen Versionen für Front-to-Back (kühle Luft wird an den SFP+-Ports an der Front ins Gehäuse gesaugt und an der Rückseite abgegeben) und Back-to-Front (kalte Luft wird auf der Rückseite angesaugt und an der Frontseite mit den SFP+Ports abgegeben) Lüftungsrichtung zur Verfügung. Die Lüftungsrichtung darf innerhalb eines Switch Systemes nicht gemischt werden.

Die X670V-48t Modelle werden immer mit 2 Netzteilen bestückt geliefert, hierbei ist bei der Bestellung die Lüftungsrichtung (Front-to-Back oder Back-to-Front) sowie die Version der Netzteile auszuwählen (AC, DC oder MIX – gemischt je ein AC und ein DC Netzteil)



Summit X670-48x
Frontansicht



Summit X670V-48x
Frontansicht



Summit X670V-48t
Frontansicht



Summit X670 Rückansicht ohne VIM4
Einschubmodul



Summit X670 Rückansicht mit
eingebautem VIM4 Einschubmodul

Bestellnummer	Produktbezeichnung	Beschreibung
17101	Summit X670V-48x-FB	48 10GBASE-X SFP+ Ports, rückseitiger VIM4 Einschubslot (unbestückt) , ExtremeXOS Advanced Edge Lizenz, 2 Netzteil Einschubplätze (unbestückt), Front-to-Back Lüftungsrichtung, 3 Lüftereinschubmodule enthalten
17102	Summit X670V-48x-BF	48 10GBASE-X SFP+ Ports, rückseitiger VIM4 Einschubslot (unbestückt) , ExtremeXOS Advanced Edge Lizenz, 2 Netzteil Einschubplätze (unbestückt), Back-to-Front Lüfter
17103	Summit X670-48x-FB	48 10GBASE-X SFP+ Ports, ExtremeXOS Advanced Edge Lizenz, 2 Netzteil Einschubplätze (unbestückt), Front-to-Back Lüfter
17104	Summit X670-48x-BF	48 10GBASE-X SFP+ Ports, ExtremeXOS Advanced Edge Lizenz, 2 Netzteil Einschubplätze (unbestückt), Back-to-Front Lüfter
17201	Summit X670V-48t-FB-AC	48 10GBASE-T Ports, 4 10GBASE-X Ports (alternativ zu 4 der 10 GBase-T Ports nutzbar, unbestückt), rückseitiger VIM4 Einschubslot (unbestückt), ExtremeXOS Advanced Edge Lizenz, 2 Front-to-Back 550W AC Netzteile, Front-to-Back Lüfter Module
17202	Summit X670V-48t-BF-AC	48 10GBASE-T Ports, 4 10GBASE-X Ports (alternativ zu 4 der 10 GBase-T Ports nutzbar, unbestückt), rückseitiger VIM4 Einschubslot (unbestückt), ExtremeXOS Advanced Edge

		Lizenz, 2 Back-to-Front 550W AC Netzteile, Back-to-Front Lüfter Module
17203	Summit X670V-48t-FB-DC	48 10GBASE-T Ports, 4 10GBASE-X Ports (alternativ zu 4 der 10 GBase-T Ports nutzbar, unbestückt), rückseitiger VIM4 Einschubslot (unbestückt), ExtremeXOS Advanced Edge Lizenz, 2 Front-to-Back 550W DC Netzteile, Front-to-Back Lüfter Module
17204	Summit X670V-48t-BF-DC	48 10GBASE-T Ports, 4 10GBASE-X Ports (alternativ zu 4 der 10 GBase-T Ports nutzbar, unbestückt), rückseitiger VIM4 Einschubslot (unbestückt), ExtremeXOS Advanced Edge Lizenz, 2 Back-to-Front 550W DC Netzteile, Back-to-Front Lüfter Module
17205	Summit X670V-48t-FB-MIX	48 10GBASE-T , 48 10GBASE-T , 4 10GBASE-X (unpopulated and shared with 4 ports of the 48 10GBase-T ports), one VIM4 slot (unpopulated), ExtremeXOS Advanced Edge License, 1 Front-to-Back 550W AC power supply, 1 Front-to-Back 550W DC power supply, Front-to-Back airflow fans Front-to-Back airflow fans
17206	Summit X670V-48t-BF-MIX	48 10GBASE-T , 4 10GBASE-X (unpopulated and shared with 4 ports of the 48 10GBase-T ports), one VIM4 slot (unpopulated), ExtremeXOS Advanced Edge License, 1 Back-to-Front 550W AC power supply, 1 Back-to-Front 550W DC power supply, Back-to-Front airflow fans 550W DC power supply, Front-to-Back airflow fans Front-to-Back airflow fans
10925	Summit 550W AC PSU FB	550W AC Power Supply module for Summit switches, Front-to-Back airflow
10926	Summit 550W DC PSU FB	550W DC Power Supply module for Summit switches, Front-to-Back airflow
10927	Summit 550W AC PSU BF	550W AC Power Supply module for Summit switches, Back-to-Front airflow
10928	Summit 550W DC PSU BF	550W DC Power Supply module for Summit switches, Back-to-Front airflow
17111	Summit X670 fan module FB	Fan module for Summit X670 series switches, Front-to-Back airflow, spare
17112	Summit X670 fan module BF	Fan module for Summit X670 series switches, Back-to-Front airflow, spare

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/summit-x670-series

X 670-G2

Die X670-G2 Produkt Familie liefert hohe 10 Gigabit und 40 Gigabit Portdichten im kompakten 1 Höheneinheiten Format. Die X670-G2 Systeme sind Layer-2 und Layer-3 fähig (optional) und zeichnen sich durch sehr schnelle Latenzzeiten aus. Sie unterstützen IPv4, IPv6 und Multicast Routing und eignen sich dadurch als Aggregations- und Core Systeme.



Die X670-G2 Familie unterstützt das gleiche modulare und robuste Extreme EXOS® Netzwerk-Betriebssystem wie die anderen Extreme Networks Produkte und ermöglicht damit ein durchgängiges Betriebssystem mit einheitlichem Funktionsumfang in allen Bereichen des Netzes.

Die X670-G2 Serie wird in 2 Ausführungen angeboten:

- Der X670-G2-48x-4q verfügt über 48 SFP+ Ports, die wahlweise mit 1GbE SFP oder 10 GbE SFP+ Einschüben bestückt werden können. Zusätzlich stehen frontseitig vier 40 Gigabit Ethernet Ports für die Nutzung per QSFP+ Modul zur Verfügung. Diese 40 GbE Ports können per Konfiguration für die Nutzung als 4 x 10 GbE Port aufgesplittet werden.
- Der X670-G2-72x bietet 72 SFP+ Ports, die wahlweise mit 1GbE SFP oder 10 GbE SFP+ Einschüben bestückt werden können und bietet so eine sehr hohe Portdichte im Bereich 10 Gigabit Ethernet.

High-Performance Stacking

Die X670-G2 Systeme unterstützen vier unterschiedliche Stacking Methoden:

- SummitStack-V
- SummitStack-V160
- SummitStack-V80
- SummitStack-V320

SummitStack-V – flexibles Stacking über 10 GbE

Die SummitStack-V Funktion des EXOS Betriebssystems unterstützt die Nutzung von 2 der nativen 10 GbE Ports auf der Frontseite der X670 Modelle als Stacking Ports über Standard SFP+ Kabel oder Optiken. So werden Entfernungen von bis zu 40 km als Stacking Verbindung überbrückt. Durch den Einsatz von Standard Verkabelung wird die Komplexität bei der Planung und Inbetriebnahme von gestackten Systemen reduziert. SummitStack-V® ist kompatibel mit X440, X460, X460-G2, X480, X670, X670V, X670-G2 und X770 Switches, die in der gleichen Version des Betriebssystems EXOS verfügbar sind.

SummitStack-V80/V160/V320 – Flexibles Stacking über 40 Gigabit Schnittstellen

Die X670-G2-48x-4q können zusätzlich über die frontseitigen 40 GbE QSFP+ Schnittstellen gestackt werden. Hierbei stehen drei unterschiedliche Geschwindigkeiten zur Auswahl: 80Gbps, 160 Gbps und 320Gbps. Stacking kann hierbei über passive Kupfer Kabel (0,5-1m), vorkonfektionierte aktive Glasfaser Kabel (bis 100m) oder über die QSFP+ Standard Optiken bis zu 10 km erfolgen. Diese Flexibilität in der Stacking Technologie ermöglicht eine optimale Nutzung als Unternehmens-Core-Ausstattung oder Top-of-Rack System im Rechenzentrum, das schrankübergreifende Systeme ermöglicht.

Intelligentes Switching

Die X670-G2 eignen sich hervorragend für den Einsatz als Layer-2 System und ermöglichen durch Funktionen wie „Policy-Based-Switching und -Routing“, Provider Bridging, ein- und ausgehende Accesslisten, Bandbreiten Regulierung in 8 kbps Stufen ein- und ausgehend sowie das komplette IPv4 und IPv6 Routing auch den Einsatz in komplexen und anspruchsvollen Unternehmensnetzwerken.

1588 Precision Time Protocol (PTP)

Die X670-G2 liefern optional bei Bedarf Boundary Clock (BC), Transparent Clock (TC), und Ordinary Clock (OC) für Applikationen, die synchronisierte Phasen und Frequenzen auf Netzwerkebene und Synchronität im Bereich von Millisekunden erfordern.

Audio Video Bridging (AVB)

Audio Video Bridging ermöglicht zuverlässige Audio und Video Übertragung in Echtzeit basierend auf Ethernet Netzwerk Infrastruktur. Die AVB Technologie bietet die entsprechenden Quality-of-Service und Multicast-Funktionen, um die Anforderungen von zeitsensitiven und latenzkritischen Applikationen zu erfüllen. Die Systeme der X670-G2 Serie unterstützen diesen IEEE 802.1 Standard.

Low Latency Switching für Cluster Computing

Der Chipsatz der X670-G2 unterstützt sogenanntes Cut-Through-Switching, dabei werden eingehende Pakete bereits zum Ausgangsport befördert, bevor das Paket vollständig im Switch angekommen ist. Dies ermöglicht Latenzzeiten kleiner 600 ns und eignet sich besonders für den Einsatz in latenzkritischen Cluster Netzwerken.

Green Design – Energieoptimiertes Design mit flexiblen Kühlungsoptionen

Die X670-G2 Serie wurde energieoptimiert und umweltverträglich gestaltet. Der Energieverbrauch ist durch das energiesparende Design in allen Lastzuständen äußerst effektiv. Der Einsatz hocheffizienter Netzteile minimiert die entstehende Verlustleistung und vermindert dadurch die Entstehung unnötiger Abwärme. Die X670-G2 Serie bietet AC und DC Netzteile als Option.

Designed für den Einsatz in Cloud-Rechenzentren

Die X670-G2 unterstützen viele Funktionen, wodurch sie sich besonders für den Einsatz in Rechenzentren und Cloudlösungen eignen:

- Direct Attach (VEPA)
- EXOS Network Virtualization (XNV)
- Data Center Bridging (DCB)
- Priority Flow Control (PFC)
- Virtuelle Router Instanzen (VR)

MPLS – Multi Protocol Label Switching

Für Einsatzszenarien im Bereich von Carrier Ethernet Lösungen unterstützt die X670-G2 Serie MPLS LSP basiertes Layer-3 Forwarding und hierarchisches VPLS (H-VPLS) für den Aufbau von transparenten LAN Diensten durch den Netzbetreiber. Mit Hilfe von H-VPLS kann der Netzbetreiber Layer-3 Netze durch Layer-3 Core Netzwerke erweitern und regionale VPLS Dienste miteinander verbinden.

Hochverfügbarkeitsfunktionalitäten

- Ethernet Automatic Protection Switching (EAPS)
- Ethernet Ring Protection Switching (G.8032 /ERPS)
- Spanningtree und Rapid Spanningtree Protokolle (IEEE 802.1d, IEEE 802.1w, MSTP und PVST+)
- Virtual Router Redundancy Protocol (VRRPv2/v3)
- Extreme Standby Router Protocol™ (ESRP)
- Equal Cost Multipath (ECMP)
- Link Aggregation mit LACP(802.3AD)
- Multiswitch Link Aggregation (MLAG)

Bestellhinweise

Die X670-G2 Systeme werden generell ohne Power Supplies und Lüfter-Module geliefert. Diese sind separat zu bestellen. Hierfür stehen Versionen für Front-to-Back (Kühle Luft wird an den Ethernetports an der Front ins Gehäuse gesaugt und an der Rückseite abgegeben) und Back-to-Front (Kalte Luft wird auf der Rückseite angesaugt und an der Frontseite mit den Ethernetports abgegeben) Lüftungsrichtung zur Verfügung. Die Lüftungsrichtung darf innerhalb eines Switch Systemes nicht gemischt werden.



Summit X670-G2-72x
Frontansicht



Summit X670-G2-48x-4q
Frontansicht



Summit X670-G2-72x
Rückansicht bestückt



Summit X670-G2-48x-4q
Rückansicht unbestückt

Bestellnummer	Produktbezeichnung	Beschreibung
17300	Summit X670-G2-72x-Base-Unit	72 10GBASE-X SFP+ Ports frontseitig, ExtremeXOS Advanced Edge Lizenz, 2 unbestückte Netzteilplätze und 5 unbestückte Lüftereinbauplätze
17310	Summit X670-G2-48x-4q-Base-Unit	48 10GBASE-X SFP+ Ports und 4 40GBASE-X QSFP+ Ports frontseitig, ExtremeXOS Advanced Edge Lizenz, 2 unbestückte Netzteilplätze und 3 unbestückte Lüftereinbauplätze
10925	Summit 550W AC PSU FB	550W AC Netzteil für Summit Systeme, Front-to-Back Lüftungsrichtung
10926	Summit 550W DC PSU FB	550W DC Netzteil für Summit Systeme, Front-to-Back Lüftungsrichtung
10927	Summit 550W AC PSU BF	550W AC Netzteil für Summit Systeme, Back-to-Front Lüftungsrichtung
10928	Summit 550W DC PSU BF	550W DC Netzteil für Summit Systeme, Back-to-Front Lüftungsrichtung
17111	Summit X670 Lüfter Modul FB	Lüfter Modul für Summit X670 & X770 Systeme, Front-to-Back Lüftungsrichtung
17112	Summit X670 Lüfter Modul BF	Lüfter Modul für Summit X670 & X770 Systeme, Back-to-Front Lüftungsrichtung

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/summit-x670-series

X 620

Top of Rack vs End of Row – diese Diskussion endete in der Vergangenheit meist in einem Dilemma. Denn so sauber eine – auf jeden Schrank reduzierte – Verkabelung die Ästhetik im Rechenzentrum fördert; die Investition in zwei redundante 48 Port Switches per Schrank gestaltet sich selten effizient. Mit der neuen Switchfamilie X620 lassen sich ToR-Lösungen bei geringeren Kosten sauber etablieren. Und auch für Betreiber kleinerer Infrastrukturen sind 10G nun eine Perspektive.



Die X620 Produkt Familie liefert 10 Gigabit Ports im kompakten 1 Höheneinheiten Format. Die Systeme sind Layer-2 und Layer-3 fähig und zeichnen sich durch sehr schnelle Latenzzeiten aus. Sie unterstützen IPv4, IPv6 und Multicast Routing. Durch Portanzahl sowie Software- und Hardware-Eigenschaften eignet sich die X620 Serie

ideal für den LAN Edge Bereich, kleinere Storage Netzwerke, aber auch kleinere Datacenter.

Dabei unterstützt die X620 Familie das gleiche modulare und robuste Extreme 21.x EXOS® Netzwerk-Betriebssystem wie die anderen Extreme Networks Produkte und ermöglicht damit ein durchgängiges Betriebssystem mit einheitlichem Funktionsumfang in allen Bereichen des Netzes.

Die X620 Serie wird aktuell in 4 Ausführungen angeboten:

- Der **X620-10x** verfügt über 10 SFP+ Ports, die wahlweise mit 100/1000Mbit Kombo, 1Gbit oder 10Gbit Optiken bestückt werden können.
- Der **X620-8t-2x** verfügt über 8 Kupfer Ports für 100Mbit/1Gbit/10Gbit (FullDuplex) und 2 SFP+ Ports, die wahlweise mit 100/1000Mbit Kombo, 1Gbit oder 10Gbit Optiken bestückt werden können.
- Der **X620-16x** verfügt über 16 SFP+ Ports, die wahlweise mit 100/1000Mbit Kombo, 1Gbit oder 10Gbit Optiken bestückt werden können.
- Der **X620-16t** verfügt über 12 Kupfer Ports für 100Mbit/1Gbit/10Gbit (FullDuplex) und 4 1Gb/10GBASE-T / 10Gb SFP+ combo ports.

High-Performance Stacking

Die X620 Systeme unterstützen SummitStack-V über die 10Gbit/s SFP+ Ports

SummitStack-V – flexibles Stacking über 10 GbE

Die SummitStack-V Funktion des EXOS Betriebssystems unterstützt die Nutzung von 2 der nativen 10 GbE Ports auf der Frontseite der X620 Modelle als Stacking Ports über Standard SFP+ Kabel oder Optiken. So werden Entfernungen von bis zu 40 km als Stacking Verbindung überbrückt. Durch den Einsatz von Standard Verkabelung wird die Komplexität bei der Planung und Inbetriebnahme von gestackten Systemen reduziert. SummitStack-V® ist kompatibel mit X440-G2, X450-G2, X460-G2, X670-G2 und X770 Switches, die in der gleichen Version des Betriebssystems EXOS verfügbar sind.

Intelligentes Switching

Die X620 eignen sich hervorragend für den Einsatz als Layer-2 System und ermöglichen durch Funktionen wie „Policy-Based-Switching und -Routing“, Provider Bridging, ein- und ausgehende Accesslisten, Bandbreiten Regulierung in 8 kbps Stufen ein- und ausgehend sowie IPv4 und IPv6 Routing bis zu den Advanced Edge Funktionen den Einsatz als LAN Edge Switch, in kleineren Storage Netzwerken oder auch in kleineren Datacentern.

Audio Video Bridging (AVB)

Audio Video Bridging ermöglicht zuverlässige Audio und Video Übertragung in Echtzeit basierend auf Ethernet Netzwerk Infrastruktur. Die AVB Technologie bietet die entsprechenden Quality-of-Service und Multicast-Funktionen, um die Anforderungen

von zeitsensitiven und latenzkritischen Applikationen zu erfüllen. Die Systeme der X620 Serie unterstützen diesen IEEE 802.1 Standard optional durch eine Feature Lizenz.

Limited Lifetime Warranty

Die X620 Serie überzeugt durch niedrige Unterhaltskosten, da die Geräte über limited lifetime warranty mit Advanced Hardware Replacement (eAHR-2) verfügen.

Green Design – Energieoptimiertes Design mit flexiblen Kühloptionen

Die X620 Serie wurde energieoptimiert und umweltverträglich gestaltet. Der Energieverbrauch ist durch das energiesparende Design in allen Lastzuständen äußerst effektiv. Alle Kupfer Ports erfüllen die Anforderungen des Energy Efficient Ethernet (EEE) nach IEEE 802.3az. Der Einsatz hocheffizienter Netzteile minimiert die entstehende Verlustleistung und vermindert dadurch die Entstehung unnötiger Abwärme. Die 16-Port Varianten der X620 Serie bieten AC und DC Netzteile als Option.

Erweiterter Temperaturbereich

Die X620 Serie ist für den Einsatz bei Umgebungstemperaturen von 0 – 50°C konzipiert und kann dadurch 10Gbit/s Anschlüsse auch unter erschwerten Bedingungen bereitstellen.

Hochverfügbarkeitsfunktionalitäten

- Ethernet Automatic Protection Switching (EAPS)
- Ethernet Ring Protection Switching (G.8032 /ERPS)
- Spanningtree und Rapid Spanningtree Protokolle (IEEE 802.1d, IEEE 802.1w, MSTP und PVST+)
- Virtual Router Redundancy Protocol (VRRPv2/v3)
- Extreme Standby Router Protocol™ (ESRP)
- Equal Cost Multipath (ECMP)
- Link Aggregation mit LACP(802.3AD)
- Multiswitch Link Aggregation (MLAG)

Bestellhinweise

Die X620 Systeme werden in den 16 Port Varianten generell ohne Power Supplies und Lüfter-Module geliefert. Diese sind separat zu bestellen. Hierfür stehen Versionen für Front-to-Back (Kühle Luft wird an den Ethernetports an der Front ins Gehäuse gesaugt und an der Rückseite abgegeben) und Back-to-Front (Kalte Luft wird auf der Rückseite angesaugt und an



Frontansicht X620-16x (oben) und X620-16t (unten)



Rückansicht X620-16x / -16t mit 1 Powersupply



Frontansicht X620-8t-2x (oben) und X620-10x (unten) (unten)



Rückansicht X620-8t-2x / -10x

der Frontseite mit den Ethernetports abgegeben) Lüftungsrichtung zur Verfügung.

Die Lüftungsrichtung darf innerhalb eines Switch Systemes nicht gemischt werden. Die 10 Port Varianten werden mit fest eingebauten Power Supplies und Side-to-Side Lüftung ausgeliefert. Über die externen Geräte RPS-150XT oder EPS-C2 kann eine redundante Stromversorgung realisiert werden. Alle Ports der X620 Serie arbeiten ausschließlich im Full-Duplex Modus.

Bestellnummer	Produktbezeichnung	Beschreibung
17401	X620-16x-Base	16 100Mb/1Gb/10GBASE-X SFP+ ports frontseitig, 2 unbestückte Netzteilplätze und 1 unbestückter Lüftereinbauplatz , ExtremeXOS Edge Lizenz
17402	X620-16t-Base	12 100Mb/1Gb/10GBASE-T ports mit EEE, 4 100Mb/1Gb/10GBASE-T mit EEE als Kombo mit 4 1Gb/10GBASE-X SFP+ ports, 2 unbestückte Netzteilplätze und 1 unbestückter Lüftereinbauplatz , ExtremeXOS Edge Lizenz
10945	Summit X620 Lüfter Modul FB	Lüfter Modul für Summit X620 16 Port Systeme, Front-to-Back Lüftungsrichtung
10946	Summit X620 Lüfter Modul BF	Lüfter Modul für Summit X620 16 Port Systeme, Back-to-Front Lüftungsrichtung
10930A	Summit 300W AC PSU XT	300W AC Netzteil für Summit Systeme, Front-to-Back Lüftungsrichtung
10943	Summit 300W AC PSU BF	300W AC Netzteil für Summit Systeme, Back-to-Front Lüftungsrichtung
10933	Summit 300W +24V/-48V DC PSU FB	300W DC Netzteil für Summit Systeme, Front-to-Back Lüftungsrichtung
10944	Summit 300W +24V/-48V DC PSU BF	300W DC Netzteil für Summit Systeme, Back-to-Front Lüftungsrichtung
17404	X620-10x-Base	10 100Mb/1Gb/10GBASE-X SFP+ ports, integrierte power supply und Lüfter, ExtremeXOS Edge Lizenz
17405	X620-8t-2x-Base	8 100Mb/1Gb/10GBASE-T ports mit EEE, 2 1Gb/10GBASE-X SFP+ ports, integrierte power supply und Lüfter, ExtremeXOS Edge Lizenz

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/summit-x620-series

7100-Serie

Die Extreme 7100-Serie ist eine Familie von Switches mit einer hohen Dichte von performanten 1 Gigabit und 10 Gigabit Ports für Server Anbindungen. Die 7100 - Serie ist ideal für den Einsatz in modernen Rechenzentren und hochperformantem LAN Edge Anwendungsbereichen geeignet. Die 7100-Serie bietet eine sinnvolle Lösung für die hohen Bandbreitenanforderungen mit niedrigen Latenzzeiten in den heutigen Netzwerkumgebungen.



Extreme 7100 - Hohe Portdichte

Extreme bietet mit den Switchen der 7100er Serie eine Lösung mit unterschiedlicher Portbestückung zum flexiblen Einsatz in der Server Umgebung. Es stehen Modelle mit SFP, SFP+ und/oder 10GBASE-T zu Verfügung. Für den Uplink sind die Switche mit 40 Gigabit Ports mit QSFP Optik ausgestattet. Durch den Einsatz von „Direct Attach“ Kabeln für Gigabit, 10 Gigabit und 40 Gigabit können alle Arten von Verbindungen kostengünstig realisiert werden. Bis zu 64 Ports mit 10 Gigabit in „line rate“ Geschwindigkeit in einer Rack Höheneinheit minimieren den Platzbedarf für Top of Rack Switches (ToR) und maximieren den verfügbaren Platz für Server in Rechenzentren. Die Lüftung der Switches kann Front to Back oder Back to Front konfiguriert werden und unterstützt die modernen Klimakonzepte in Rechenzentren (Kaltgangeinhausung).



Extreme 7100 - Zuverlässigkeit und Verfügbarkeit

Für eine hohe Verfügbarkeit der Systeme sind alle 7100er Switches mit redundanten, im laufenden Betrieb wechselbaren, Power Supplies und Lüfter Modulen ausgestattet. Über Extreme Virtual Switch Bonding (VSB) können bis zu 8 Systeme zu einem virtuellen System verbunden werden, um eine Hardware Redundanz ohne Ausfallzeiten bei Störungen zu erreichen.

Die 7100-Serie ist ein integraler Bestandteil der Netzwerk-Architektur von Extreme. Diese unterstützt Unternehmen dabei, einen unkomplizierten und einheitlichen Netzwerkzugang in immer stärker virtualisierten Umgebungen zu realisieren.

Die Architektur bietet über Ihre Monitor Funktionalität eine transparente Sicht auf das Netzwerk, welche virtuelle Maschinen bei Inbetriebnahme und Bewegung innerhalb der Server Struktur darstellbar macht. DCB (Data Center Bridging) als Feature unterstützt die Konvergenz zwischen LAN und Storage-Daten. Mit der höheren aggregierten Kapazität können Data Center effektiv skalieren – ohne Kompromisse bei Latenz- und Verfügbarkeitsanforderungen. Die Integration in das Management mit ExtremeControl automatisiert viele Administrationsvorgänge. So wird im Detail bei laufendem Betrieb durchschaubar, wie kritische Ressourcen des Rechenzentrums funktionieren. Und diese Ressourcen lassen sich steuern – vom Edge über den Core bis ins Data Center. Bandbreiten und Prioritäten sind zentral bereitstellbar. Das garantiert eine einheitliche, umfassende Netzwerkkonfiguration.

Extreme 7100 - Zusammenfassung

- Hoch performanter 1/10G Switch für DataCenter und Advanced Edge/Distribution Bereich
- Bis zu 4 x 40 Gigabit Uplink über QSFP Interfaces pro Switch. Bis zu 64 x 10 Gig Ports wire speed pro Switch
- Stacking über VSB von bis zu 8 Switches
- Vollständig Managebar über Extreme Control Center
- Hochverfügbarkeit durch Redundanzen in Stromversorgung, redundante Lüfter und VSB.
- Unterstützung von dynamische Rollen basierenden Policies
- Umfangreiche QoS Möglichkeiten für Einsatz in Multimedia Anwendungen
- Multimethod Authentifizierung am Port. Sicherer Netzwerk Zugang durch Web, 802.1x, und MAC Address Authentication
- Multiuser Authentifizierung (Bis zu 512 Endgeräte) pro Port
- IGMP v1/v2/v3 - MLD v1/v2
- Data Center Bridging
 - Priority Flow Control (PFC), Enhanced Transmission Selection (ETS), Congestion Notification (CN), Application Priority, DCBx
- Routing
 - L3 Unicast and Mcast Routing – Static, OSPFv2, OSPFv3, VRRP, PIM-SM, DVMRP
- Shortest Path Bridging

Extreme 7100 - Varianten

Die 10G Switches der 7100er Serie gibt es in den folgenden Varianten

Produktbezeichnung	Beschreibung
7148	48 Ports 1/10Gb SFP+ mit 4 10/40Gb QSFP+ Ports
7124	24 Ports 1/10Gb SFP+ mit 4 10/40Gb QSFP+ Ports
7148T	48 Ports 1/10GBASE-T mit 4 10/40Gb QSFP+ Ports
7124T	24 Ports 1/10GBASE-T mit 4 10/40Gb QSFP+ Ports
7148G	48 Ports 10/100/1000Mb RJ45 mit PoE, 2 1/10Gb SFP+ und 2 10/40Gb QSFP+ Ports
7124G/24	24 Ports 10/100/1000Mb mit PoE, 2 1/10Gb SFP+ und 2 10/40Gb QSFP+ Ports

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/7100-series-2

X 480

Die X480 Switch Serie ist ein vielseitiges und sehr leistungsfähiges Ethernet Switching System, das speziell für den Einsatz in Rechenzentren, Aggregationsebenen in Unternehmensnetzen und in



Carrier Netzwerken designed wurde. Die X480 bieten einige Funktionen, die speziell hier zum Einsatz kommen, darunter vor allem eine extrem hohe Skalierbarkeit.

Mit bis zu 48 Gigabit Ethernet Ports je System und der flexiblen SummitStack® Technologie für Stacks aus bis zu 8 Teilnehmern in unterschiedlichsten Varianten von 10 Gbps (SummitStack-V®) bis zu 320 Gbps (SummitStack-V320®) können bis zu 384 Gigabit Ethernet Ports und bis zu 64 10 Gigabit Ethernet Ports in einem System realisiert werden.

Den immer weiter steigenden Anforderungen an heutige Netzwerke werden die X480 Systeme durch hoch skalierbare Layer-2/Layer-3 Forwarding Tabellen mit bis zu 512.000 MAC Adress-Einträgen oder bis zu 512.000 IPv4 LPM Einträgen sowie der Unterstützung von MPLS/H-VPLS gerecht. Auch im Bereich der Netzwerksicherheit zeichnen sich die X480 durch ihre Skalierbarkeit von bis zu 60.000 Access Control Listen (ACLs) aus.

Hierdurch eignet sich der X480 besonders für den Einsatz in Rechenzentren, Aggregationsebenen und natürlich auch in Carrier Netzwerken. Dies wird durch die Verfügbarkeit von 230V AC und 48V DC Netzteilen unterstützt. Die X480 Systeme unterstützen 10 GbE Optiken in XFP Bauform und ermöglichen dadurch den flexiblen

Einsatz von 10GBase-SR, -LR, -ER, -ZR und konfigurierbaren DWDM (Dense Wavelength Division Multiplexing) Optiken, die durch ihre einstellbaren Lichtfarben flexible Netzwerkdesigns auf Glasfaser-Basis ermöglichen. Zusätzlich wird DDMI (Digital Diagnostics Monitoring Interface) für die Überwachung von Kabelstrecken unterstützt.

Die X480 Systeme werden mit dem Netzwerk-Betriebssystem Extreme EXOS® betrieben, dem gleichen modularen Betriebssystem, das auf allen Systemen zum Einsatz kommt und so Hochverfügbarkeit und einfache Handhabung durch ein einheitliches System garantiert.

Haupteinsatzbereiche

- Top-of-Rack System für den Anschluß GbE basierender Server im Data-Center
- Hoch performanter Core Switch in kleinen und mittelgroßen Netzwerken
- Hoch performanter Gigabit Aggregationsswitch in klassischen 3 Ebenen Netzwerken (Core/Aggregation/Access)
- Aggregationsswitch in Carrier Netzwerken für die Zusammenführung von DSLAM oder CMTS Systemen

High-Performance Switching und Routing Plattform

Die X480 sind in drei Bauformen lieferbar:

- 24 Port Gigabit Ethernet plus 2 Port 10 GbE Uplink (X480-24x). Es stehen 24 SFP basierte Anschlußports zur Verfügung. 12 dieser Ports sind als Combo-Ports ausgeführt und können alternativ mit Kupfer-Anschluß betrieben werden
- 48 Port Gigabit Kupfer (X480-48t). Hiervon sind 4 Ports als Combo Ports ausgeführt und können alternativ mit Glas-Anschluß betrieben werden
- 48 Port Gigabit Glas (SFP) (X480-48x)

Alle Systeme verfügen über eine non-blocking Architektur und verarbeiten den Netzwerkverkehr in voller Leitungsgeschwindigkeit auch in Richtung des rückseitigen VIM-2 Einbauplatzes (Versatile Interface Module-2), für den folgende Einschuboptionen zur Verfügung stehen:

- 4-Port 10 Gigabit Ethernet Modul (VIM2-10G4X)
- 4-Port 40 Gigabit Ethernet Modul (VIM3-40G4X)
- 2-Port SummitStack Modul (VIM2-SummitStack)
- 2-Port SummitStack128 Modul (VIM2-SummitStack128)
- 2-Port SummitStack-V80 Modul (VIM2-SummitStack-V80)

Hochverfügbarkeit

- Modulares EXOS® Betriebssystem für hochverfügbaren Netzbetrieb

- Ethernet Automatic Protection Switching (EAPS) Protokoll für ultrakurze Umschaltzeiten im Redundanzfall (<50ms)
- Redundantes, internes Netzteil im Betrieb tauschbar
- Im Betrieb tauschbarer Lüftereinschub

X480 - Zusammenfassung

- Gigabit Ethernet Plattform für höchste Layer-2 und Layer-3 Skalierbarkeit
- Unterstützung Carrier Funktionalitäten wie MPLS/VPLS in hohen Skalierungen
- XFP Optiken für Carrier Anwendungen
- Modularer Erweiterungsslot für Stacking, zusätzliche 10 Gigabit Ports oder 40 GBase-X Fähigkeit für Uplinks oder Stacking



Bestellnummer	Produktbezeichnung	Beschreibung
16301	Summit X480-48t	48 Ports 10/100/1000BASE-T, davon 4 Ports alternativ nutzbar als 100/1000BASE-X SFP Einschub (shared Ports), ein VIM-2 Einschubplatz rückseitig, 2 unbestückte Netzteilbauplätze, ExtremeXOS Advanced Edge Lizenz
16303	Summit X480-24x	24 Ports 100/1000BASE-X unpopulated SFP, davon 12 Ports alternativ nutzbar als 10/100/1000BASE-T (shared Ports), 2 unbestückte XFP Ports, ein VIM-2 Einschubplatz rückseitig, 2 unbestückte Netzteilbauplätze, ExtremeXOS Advanced Edge Lizenz
16304	Summit X480-48x	48 Ports 100/1000BASE-X SFP, ein VIM-2 Einschubplatz rückseitig, 2 unbestückte Netzteilbauplätze, ExtremeXOS Advanced Edge Lizenz
16311	VIM2-SummitStack	VIM2-SummitStack, 2 SummitStack Stacking Ports
16312	VIM2-10G4X	VIM2-10G4X, 4 10GBASE-X XFP Ports
16313	VIM2-SummitStack128	VIM2-SummitStack128, 2 x 64G Stacking Ports
16315	VIM2-SummitStack-V80	VIM2-SummitStack-V80, 2 x 40G Stacking Ports
17121	VIM3-40G4X	40 Gigabit Ethernet Modul, 4 40GBASE-X QSFP+ Ports

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/summit-x480-series/

X 460-G2

Die Systeme der X460-G2 Serie basieren auf dem Netzwerkbetriebssystem



Extreme EXOS®, dem ausgereiften Betriebssystem für höchste Netzwerkverfügbarkeit, Managebarkeit und effizienten Netzwerkbetrieb. Jedes Switch Modell ist mit non-blocking Hardware ausgestattet und ermöglicht den plattformübergreifenden Einsatz eines einheitlichen Betriebssystems in allen Bereichen des Netzwerkes.

Die X460-G2 Switche eignen sich durch ihre Unterstützung von Energy Efficient Ethernet (EEE – IEEE 802.3az) als energieeffiziente Netzwerk-Access Switching Systeme und unterstützen PoE+ nach IEEE 802.3at zum Betrieb von Power-over-Ethernet Endgeräten. Weitere Anwendungsgebiete für die X460-G2 Serie ist der Aggregationsbereich klassischer Unternehmensnetzwerke oder der Einsatz im Bereich „Aktiver Ethernet Access“ als Aggregationsswitch für DSLAMs oder CMTS Systeme.

Die X460-G2 eignen sich zusätzlich für den Einsatz als Top-of-Rack Systeme im Bereich moderner, hochintegrierter Rechenzentrumsinstallationen durch die Verfügbarkeit von Funktionen wie XNV™ (EXOS Network Virtualization) als zentrale Lösung zur Unterstützung und Inventarisierung von Virtuellen Maschinen (VM), mit Lokalisierung und Provisionierung von virtuellen Server Landschaften. Sie bieten Funktionen wie VEPA (Virtual Ethernet Port Aggregator) zur Eliminierung virtueller Switches (Direct Attach™), um die CPU virtueller Server Umgebungen zu entlasten und dadurch die Systemperformance zu verbessern. Sehr hohe Skalierbarkeit im Bereich Layer-2/Layer-3 Adressen stehen hier ebenso im Fokus wie das branchenweit führende Stacking System mit unterschiedlichen Geschwindigkeiten und Entfernungs- bzw. Längenoptionen, das sich perfekt für die Bildung von schrankinternen sowie schrankübergreifenden Stack Systemen eignet.

Umfangreiche Sicherheitsfunktionen

- Unterstützung von Benutzer- und Identitäts-Management mit dynamischen Rollen und darauf basierenden Regelwerken (Policies).
- Automatische Anpassung der Portkonfiguration durch Erkennung des angeschlossenen Endgerätes und automatisierte Provisionierung (Universal Port Funktion).
- Erkennung von Angriffsszenarien, Fehlverhalten und Störungen sowie automatisierte Reaktion auf solche Szenarien durch die integrierte CLEAR-Flow Sicherheitstechnologie
- Schutz vor Denial of Service (DoS) Angriffen und IP Sicherheitstechnologien zur Abwehr von Man-in-the-Middle Angriffen und zum Schutz der Netzwerkinfrastruktur.
- Sicherer Netzwerk Zugang durch Web, 802.1x, und MAC Adressen Authentisierung
- Gleichzeitige Multimethod-Authentisierung am Access-Port
- Multiuser Authentisierung

Flexible Systemvarianten

Die X460-G2 Serie ist in verschiedenen Ausführungen verfügbar: Die X460-G2 24 Port 10/100/1000Base-T Varianten verfügen über 4 Shared Gigabit SFP Ports (1 GBase-T oder 1 GBase-X nutzbar) und zusätzlich 4 dedizierte Gigabit SFP Ports und können dadurch mit bis zu 8 Optiken bestückt werden, während zusätzlich 20 Ports Gigabit 1 GBase-T mit oder ohne PoE zur Verfügung stehen. Die X460-G2-24t-GE4 Systeme stellen bis zu 12 SFP Ports mit 1 Gigabit zur Verfügung (4x Shared Ports, 8x dedizierte SFP Ports)

Alle Modelle verfügen über 4 SFP+ Ports mit 10 GbE (X460-xxx-10GE4 alle Modelle) oder 4 SFP 1 GbE Ports (X460-xxx-GE4 Modelle), die frontseitig verfügbar sind. Zusätzlich verfügen alle Modelle über einen optional bestückbaren VIM Slot auf der Rückseite, der mit unterschiedlichen Modulen bestückbar ist. Hierfür stehen z. B. VIM Module mit 2 10GbE Ports in Kupfer oder SFP+ Technik zur Verfügung, so dass insgesamt bis zu 6 10 GbE Schnittstellen genutzt werden können.

Alternativ kann der VIM Slot mit einem 2 Port 40 GbE Interface bestückt werden, welches für Highspeed Uplinks mit 40 GbE oder für die SummitStack® Technologie genutzt werden kann.

Hochperformantes Stacking wird in dieser Serie mit bis zu 8 Systemen unterstützt und kann auch in gemischten Varianten mit SummitStack, SummitStack-V und SummitStack-V160 betrieben werden.

SummitStack – Stacking über CX4 Kupferverbindungen

Die X460-G2 unterstützen über die optionalen VIM-2ss Module auch Stacking über die klassische SummitStack Technologie und sind damit kompatibel zu den Systemen der X440, X460 und X480 Serie, die in der gleichen Version des Betriebssystems EXOS verfügbar sind.

SummitStack-V – flexibles Stacking über 10 GbE

Die SummitStack-V Funktion des EXOS Betriebssystems unterstützt die Nutzung von 2 der nativen 10 GbE Ports auf der Frontseite der X460-G2-10GE4 Modelle als Stacking Ports über Standard SFP+ Kabel oder Optiken und ermöglicht so, Entfernungen bis zu 40 km als Stacking Verbindung zu überbrücken. Dies erfordert eine direkte Verbindung zwischen den 10 GbE Stacking Ports. Durch den Einsatz von Standard Verkabelung wird die Komplexität bei der Planung und Inbetriebnahme von gestackten Systemen reduziert. SummitStack-V® ist kompatibel mit X440, X460, X460-G2, X480, X670, X670V, X670-G2 und X770 Switch Serien, die in der gleichen Version des Betriebssystems EXOS verfügbar sind.

Hinweis I: Stacking wird auf den 10 GbE VIM Modulen zu Beginn der Auslieferung der X460-G2 Systeme nicht unterstützt.

Hinweis II: Die 1 GbE SFP Ports an der Frontseite der X460-G2-GE4 Systeme sind nicht für Stacking nutzbar.

SummitStack-V160 – Stacking mit 40 GbE Schnittstelle

Für Einsatzszenarien mit sehr hohen Anforderungen an die Stacking Bandbreite können die X460-G2 Systeme mit Hilfe des VIM-2q Einschubmodules mit 160 Gbps Stacking ausgestattet werden.

Die SummitStack-V160 Option kann über passive Kupferkabel bis 3m Länge überbrücken, über fertig konfektionierte Glasfaserkabel bis 100m oder über Standard QSFP+ Optiken bis 10km.

Mit dem SummitStack-V160 bieten die SummitStack X460-G2 eine äußerst flexible und leistungsfähige Stacking Option für den Einsatz im Rechenzentrum, um eine virtualisierte Netzwerkumgebung auch schrankübergreifend zur Verfügung zu stellen.

SummitStack-V160® ist kompatibel mit den X460-G2, X480, X670V, X670-G2 und X770 Switch Serien, die in der gleichen Version des Betriebssystems EXOS verfügbar sind.

Intelligentes Switching und die Unterstützung von MPLS

Die X460-G2 eignen sich hervorragend für den Einsatz als Layer-2 Systeme und ermöglichen durch Funktionen wie „Policy-Based-Switching und -Routing“, Provider Bridging, ein- und ausgehende Accesslisten, Bandbreitenregulierung in 8 kbps Stufen ein- und ausgehend sowie das komplette IPv4 und IPv6 Routing auch den Einsatz in komplexen und anspruchsvollen Unternehmensnetzwerken.

Für Einsatzszenarien im Bereich von Carrier Ethernet Lösungen unterstützt die X460-G2 Serie MPLS LSP basiertes Layer-3 Forwarding und hierarchisches VPLS (H-VPLS) für den Aufbau von transparenten LAN Diensten durch den Netzbetreiber. Mit Hilfe von H-VPLS kann der Netzbetreiber Layer-3 Netze durch Layer-3 Core Netzwerke erweitern und regionale VPLS Dienste miteinander verbinden.

Power over Ethernet (IEEE 802.3at PoE-plus)

IEEE 802.3af PoE (Power-over-Ethernet) ist in vielen Einsatzbereichen der Netzwerke heute für die Stromversorgung von Voice-Over-IP Endgeräten, WLAN Access Points oder Sicherheitssystemen wie IP-basierte Kameras unverzichtbar. Portextender wie der Extreme Networks ReachNXT™ 100-8T nutzen ebenfalls die Spannungsversorgung durch PoE und vereinfachen so die Installation, den Betrieb und reduzieren dadurch die Betriebskosten für das Netzwerk. Der aktuellere IEEE 802.3at PoEplus Standard erweitert diese Einsatzszenarien durch die Möglichkeit bis zu 30 Watt je Port an Leistung zur Verfügung zu stellen. Dies erfolgt nach erfolgreicher Aushandlung der Parameter über das LLDP Protokoll. Die X460-G2 POE Systeme liefern PoEplus nach 802.3at Standard. Für die Nutzung von PoE stehen 2 unterschiedliche Netzteil-Varianten zur Verfügung. Das 715W PoE AC Netzteil liefert bis zu 500 Watt PoE Leistung, bei Betrieb mit 2 Netzteilen stehen bis zu 1.031 Watt PoE Leistung zur Verfügung. Als zweite Option gibt es die 1100W PoE AC Netzteile, von denen ein einzelnes 850W PoE-Plus Budget bietet. Bei Bestückung mit zwei dieser Netzteile kann 1668W PoE-Plus Leistung genutzt werden.

1588 Precision Time Protocol (PTP)

Die X460-G2 liefern optional bei Bedarf Boundary Clock (BC), Transparent Clock (TC), und Ordinary Clock (OC) für Applikationen, die synchronisierte Phasen und Frequenzen auf Netzwerkebene erfordern, um Synchronität im Bereich von Millisekunden erfordern.

Audio Video Bridging (AVB)

Audio Video Bridging ermöglicht zuverlässige Audio und Video Übertragung in Echtzeit, basierend auf Ethernet Netzwerk Infrastruktur. Die AVB Technologie bietet die entsprechenden Quality-of-Service und Multicast Funktionen, um die Anforderungen von zeitsensitiven und latenzkritischen Applikationen zu erfüllen. Die Systeme der X460-G2 Serie unterstützen diesen IEEE 802.1 Standard.

Leistungsdaten

- 48-Port und 28-Port Modelle verfügbar
- 2 Bauformen: 4 Port SFP+ 10 GbE oder 4 Port SFP 1 GbE Uplink auf der Front
- Alle Versionen liefern full-duplex non-blocking Geschwindigkeit in allen Portbestückungen
- Kupfer RJ45, Optische SFP und PoEplus Versionen verfügbar
- Optionale 10 GbE SFP+ oder 10 GbE 10 GBase-T Uplink Module zum Einbau auf der Rückseite
- Optionales 2 Port 40 GbE Modul für bandbreiten intensive Anbindung oder hochperformanten Stacking mit SummitStack-V160
- 40 Gbps Stacking über die Front Ports der 10GE Varianten
- Latenz kleiner 4 Microsekunden (für 64 Byte Pakete)
- 96k (98.304) Layer-2 / MAC Adress Einträge in Hardware
- 12k (12.288) IPv4 LPM Einträge
- 6k (6.144) IPv6 LPM Einträge
- 4096 VLAN/VMANs
- Jumbo Frame Support bis maximal 9216 Byte Paketgröße
- 128 Linkaggregate Gruppen mit bis zu 32 physikalischen Ports je Gruppe
- Eingangs- und Ausgangs-Bandbreitenbegrenzung
- 8 Quality of Service Klassen per Port in Hardware (8 Hardware Queues)
- Bandbreitenbegrenzung am Ausgangsport pro Port und Queue
- Granulare Bandbreitenbegrenzung in Schritten von 8 kbps
- Voll-Duplex Unterstützung an allen Ports - Halb-Duplex Betrieb wird nicht unterstützt

X460-G2 – Zusammenfassung

- Flexibler 24- bzw. 48 Port Gigabit Switch mit 4 1 GbE oder 10 GbE Uplink Ports
- PoEplus Versionen mit bis 1668 Watt PoE Leistung
- Leistungsfähige Layer-2 und Layer-3 Plattform

- Modularer Erweiterungsslot mit optionalen SummitStack Ports, 10 GBase-T oder 40 GBase-X Ports
- Energy Efficient Ethernet - IEEE 802.3az
- Unterstützung von Synchronem Ethernet nach ITU G.8232 und Precision Timing Protocol nach IEEE 1588 PTP
- Hardware Unterstützung von ITU Y.1731 OAM Messfunktionen

Bestellhinweise

Die X460-G2 Systeme werden generell ohne Power Supplies und Lüfter-Module geliefert. Diese müssen separat bestellt werden. Hierfür stehen Versionen für Front-to-Back (kühle Luft wird an den Ethernetports an der Front ins Gehäuse gesaugt und an der Rückseite abgegeben) und Back-to-Front (kalte Luft wird auf der Rückseite angesaugt und an der Frontseite mit den Ethernetports abgegeben)

Lüftungsrichtungen zur Verfügung. Die Lüftungsrichtung darf innerhalb eines Switch Systemes nicht gemischt werden. Optionale Module wie das VIM Modul und das Timing Modul für den Einbau auf der Rückseite sind als separate Einschubmodule zusätzlich orderbar.



Summit ® X460-G2-GE4



Summit ® X460-G2-10GE4



Optionale Einschubmodule für X460-G2



Rückansicht X460-G2 Systeme
(voll bestückt)

Bestellnummer	Produktbezeichnung	Beschreibung
16701	X460-G2-24t-10GE4	24 10/100/1000BASE-T Ports, 8 100/1000BASE-X unbestückte SFP Ports (davon 4 SFP Ports die alternativ als 4 10/100/1000BASE-T Ports genutzt werden können), 4 1000/10GBaseX unbestückte SFP+ Ports, rückseitiger VIM Slot (unbestückt), rückseitiger Einbauplatz für Timing Modul (unbestückt), 2 unbestückte Netzteil Einschubplätze, Einschubplatz für Lüftermodul (unbestückt)
16702	X460-G2-48t-10GE4	48 10/100/1000BASE-T Ports, 4 1000/10GBaseX unbestückte SFP+ Ports, rückseitiger VIM Slot (unbestückt), rückseitiger Einbauplatz für Timing Modul (unbestückt), 2 unbestückte

		Netzteil Einschubplätze, Einschubplatz für Lüftermodul (unbestückt)
16703	X460-G2-24p-10GE4	24 10/100/1000BASE-T Ports mit PoE-plus, 8 100/1000BASE-X unbestückte SFP Ports (davon 4 SFP Ports die alternativ als 4 10/100/1000BASE-T Ports genutzt werden können), 4 1000/10GBaseX unbestückte SFP+ Ports, rückseitiger VIM Slot (unbestückt), rückseitiger Einbauplatz für Timing Modul (unbestückt), 2 unbestückte Netzteil Einschubplätze, Einschubplatz für Lüftermodul (unbestückt)
16704	X460-G2-48p-10GE4	48 10/100/1000BASE-T Ports mit PoE-plus, 4 1000/10GBaseX unbestückte SFP+ Ports, rückseitiger VIM Slot (unbestückt), rückseitiger Einbauplatz für Timing Modul (unbestückt), 2 unbestückte Netzteil Einschubplätze, Einschubplatz für Lüftermodul (unbestückt)
16705	X460-G2-24x-10GE4	24 100/1000BASE-X Ports, 8 10/100/1000BASE-T Ports (davon 4 SFP Ports die alternativ als 4 10/100/1000BASE-T Ports genutzt werden können), 4 1000/10GBaseX unbestückte SFP+ Ports, rückseitiger VIM Slot (unbestückt), rückseitiger Einbauplatz für Timing Modul (unbestückt), 2 unbestückte Netzteil Einschubplätze, Einschubplatz für Lüftermodul (unbestückt)
16706	X460-G2-48x-10GE4	48 100/1000BASE-X Ports, 4 1000/10GBaseX unbestückte SFP+ Ports, rückseitiger VIM Slot (unbestückt), rückseitiger Einbauplatz für Timing Modul (unbestückt), 2 unbestückte Netzteil Einschubplätze, Einschubplatz für Lüftermodul (unbestückt)
16716	X460-G2-24t-GE4	24 10/100/1000BASE-T Ports, 8 100/1000BASE-X unbestückte SFP Ports (davon 4 SFP Ports die alternativ als 4 10/100/1000BASE-T Ports genutzt werden können), 4 1GBaseX unbestückte SFP Ports, rückseitiger VIM Slot (unbestückt), rückseitiger Einbauplatz für Timing Modul (unbestückt), 2 unbestückte Netzteil Einschubplätze, Einschubplatz für Lüftermodul (unbestückt)
16717	X460-G2-48t-GE4	48 10/100/1000BASE-T Ports, 4 1GBaseX unbestückte SFP Ports, rückseitiger VIM Slot (unbestückt), rückseitiger Einbauplatz für Timing Modul (unbestückt), 2 unbestückte Netzteil Einschubplätze, Einschubplatz für Lüftermodul (unbestückt)
16718	X460-G2-24p-GE4	24 10/100/1000BASE-T Ports mit PoE-plus, 8 100/1000BASE-X unbestückte SFP Ports (davon 4 SFP Ports die alternativ als 4 10/100/1000BASE-T Ports genutzt werden können), 4 1GBaseX unbestückte SFP Ports, rückseitiger VIM Slot (unbestückt), rückseitiger Einbauplatz für Timing Modul (unbestückt), 2 unbestückte Netzteil Einschubplätze, Einschubplatz für Lüftermodul (unbestückt)
16719	X460-G2-48p-GE4	48 10/100/1000BASE-T Ports mit PoE-plus, 4 1GBaseX unbestückte SFP Ports, rückseitiger VIM Slot (unbestückt),

		rückseitiger Einbauplatz für Timing Modul (unbestückt), 2 unbestückte Netzteil Einschubplätze, Einschubplatz für Lüftermodul (unbestückt)
16710	Summit X460-G2 VIM-2q	Optionales VIM Modul (Virtual Interface Module) zum Einbau im rückseitigen VIM Slot der Summit® X460-G2 Systeme. Bietet 2 Ports 40GBase-X für den die Aufnahme von QSFP+ Modulen (unbestückt).
16711	Summit X460-G2 VIM-2x	Optionales VIM Modul (Virtual Interface Module) zum Einbau im rückseitigen VIM Slot der Summit® X460-G2 Systeme. Bietet 2 Ports 1000/10GBase-X für den die Aufnahme von SFP+ Modulen (unbestückt).
16712	Summit X460-G2 VIM-2t	Optionales VIM Modul (Virtual Interface Module) zum Einbau im rückseitigen VIM Slot der Summit® X460-G2 Systeme. Bietet 2 Ports 10GBase-T.
16713	Summit X460-G2 VIM-2ss	Optionales VIM Modul (Virtual Interface Module) zum Einbau im rückseitigen VIM Slot der Summit® X460-G2 Systeme. Bietet 2 Ports 10GBase-CX4 SummitStack
16715	Summit X460-G2 TM-CLK	Optionales Timing Module für den Einbau in den dafür vorgesehenen rückseitigen Einbauplatz der Summit® X460-G2 um hardware basiertes SyncE und 1588 PTP Clocking zu ermöglichen. Bietet 2 Mini-BNC Anschlüsse für die Anbindung des externen Taktes
10941	Summit 1100W AC PSU FB	PoE 1100 Watt AC Netzteil für die Summit X460-G2-POE Switch mit Front-to-Back Lüftungsrichtung
10942	Summit 1100W AC PSU BF	PoE 1100 Watt AC Netzteil für die Summit X460-G2-POE Switch mit Back-to-Front Lüftungsrichtung
10951	Summit 715W AC PSU FB	PoE 715 Watt AC Netzteil für die Summit X460-G2-POE Switch mit Front-to-Back Lüftungsrichtung
10952	Summit 715W AC PSU BF	PoE 715 Watt AC Netzteil für die Summit X460-G2-POE Switch mit Back-to-Front Lüftungsrichtung
10930A	Summit 300W AC PSU XT	300W AC Netzteil für die nicht POE Versionen der Summit X460-G2 und X460 und der E4G-400 Switch Serien - Erweiterter Temperaturbereich von -10 bis +50 Grad Celsius - Front-to-Back Lüftungsrichtung
10943	Summit 300W AC PSU BF	300W AC Netzteil für die nicht POE Versionen der Summit X460-G2 - Back-to-Front Lüftungsrichtung

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/summit-x670-series/

X 450-G2

Nach dem erfolgreichen Start der zweiten X460 Generation ist es an der Zeit, einen Nachfolger für das bewährte Arbeitspferd Securestack B5/C5 vorzustellen.



Mit dem Modell X450-G2 wird das Portfolio um einen schnörkellosen Access Switch für den professionellen und kosteneffizienten Einsatz erweitert.

Während das Portfolio des X460-G2 zahlreiche Kupfer/Glaskombinationen für den flexiblen Bau kleiner Core- und Distributionbereiche aufweist, konzentriert sich die Modellreihe X450-G2 auf die Versorgung von Netzwerkclients und Accesspoints über 10/10/1000BaseTX. Auf zusätzliche Erweiterungsmodule wurde bewusst verzichtet, um diese geradlinige Konzeption nicht zu durchbrechen.

Das Portfolio des X450-G2 stellt sich mit 24 bzw. 48 User Ports sowie Modellen mit und ohne Power over Ethernet Unterstützung auf.

Rückmeldungen aus dem Feld bestätigen: Entgegen theoretischer Annahmen liegt die praktische Verkehrslast in weiten Bereichen des Access nach wie vor weit unterhalb der Erwartungen. Nicht jeder Uplink bedarf also zwingend einer 10G Anbindung – aus diesem Grund werden alle X450-G2-Modelle alternativ mit 1 bzw. 10G Uplinks angeboten.

Leistungseffizienz und Power over Ethernet

Die X450-G2 Switches stellen sich durch ihre Unterstützung von Energy Efficient Ethernet (EEE – IEEE 802.3az) einen zusätzlichen Effizienzfaktor beim Aufbau energieoptimierter Systeme dar.

Technologien wie Wireless und Voice over IP liegen als Technologie voll im Trend. In der Planungsphase sollte daher auf jeden Fall über Power over Ethernet im Accessbereich nachgedacht werden. Hier kommt es auf die sinnvolle Dimensionierung an um Leistungsaufnahme, Wärmeabgabe und Anschaffungskosten in einem akzeptablen Rahmen zu halten.

Die PoE Modelle des X450-G2 nehmen bis zu zwei Stromversorgungsmodule auf und liefern damit ein Powerbudget zwischen 500 und 1440 Watt. Diese Skalierungsvarianz erlaubt nicht nur ein kostengünstiges Konzept, damit lassen sich auch planbare Rahmenbedingungen für die Klimatisierung und USV-Versorgung von Etagenverteilern setzen.

Die Luftkühlung des X450-G2 erfolgt von der Front- zur Rückseite hin. Diese Gerätefamilie ist nicht für den Einsatz als Serverswitch positioniert, daher entfällt die, für Serverumfelder typische, Back-to-Front Kühloption.

Stackingvarianten

Alle Komponenten der Summit-Stackfamilie lassen sich mit bis zu acht Systemen unter einem gemeinsamen Management fusionieren. Hierzu werden zwei unterschiedliche Technologien genutzt:

Die SummitStack-V-Option wird von nahezu allen Modellen unterstützt. Mit der Nutzung standardisierter 10 Gigabit Schnittstellen lassen sich beliebige Ringtopologien auf Distanzen von bis zu 40 KM abbilden. Jeweils zwei der eingebauten SFP+ Interfaces der X450-G2xx-10GE4 lassen sich pro Switch zum Stacking nutzen.

Grössere Bandbreitenanforderungen werden auf dem X450-G2 mittels zweier dedizierter SummitStack-V82-ports erfüllt. Diese lassen sich mit standardisierten QSFP-Kupferleitungen über eine maximale Distanz von 7m per Segment verbinden.

Betriebssystem

Die Systeme der X450-G2 Serie gewährleisten mit dem durchgängig etablierten Netzwerkbetriebssystem EXOS®, höchste Netzwerkverfügbarkeit, Managebarkeit und einen effizienten Netzbetrieb. Jedes Switch Modell ist mit non-blocking Hardware ausgestattet und ermöglicht den plattformübergreifenden Einsatz eines einheitlichen Betriebssystems in allen Bereichen des Netzwerkes.

Sicherheit

Zusammen mit dem Modell X450-G2 wurde die Version 16.1 des Betriebssystems freigegeben. Damit ist der nächste Integrationsschritt getan: Die „Purple“-Switchingfamilie lässt sich nun auch über Extreme Identity & Access Control flächendeckend mit Regelwerken versorgen. Damit sind auch gewachsene heterogene Modellstrukturen im Tagesgeschäft einfacher zu handhaben.

Weitere Leistungsmerkmale im Bereich Security sind:

- Sicherer Netzwerk Zugang durch Web, 802.1x, und MAC Adressen Authentisierung
- Gleichzeitige Multimethod-Authentisierung am Access-Port
- Multiuser Authentisierung
- Automatische Anpassung der Portkonfiguration durch Erkennung des angeschlossenen Endgerätes und automatisierte Provisionierung (Universal Port Funktion).
- Erkennung von Angriffsszenarien, Fehlverhalten und Störungen sowie automatisierte Reaktion auf solche Szenarien durch die integrierte CLEAR-Flow Sicherheitstechnologie
- Schutz vor Denial of Service (DoS) Angriffen und IP Sicherheitstechnologien zur Abwehr von Man-in-the-Middle Angriffen und zum Schutz der Netzwerkinfrastruktur.

Audio Video Bridging (AVB)

Audio Video Bridging ermöglicht zuverlässige Audio und Video Übertragung in Echtzeit, basierend auf Ethernet Netzwerk Infrastruktur. Die AVB Technologie bietet

die entsprechenden Quality-of-Service und Multicast Funktionen, um die Anforderungen von zeitsensitiven und latenzkritischen Applikationen zu erfüllen. Die Systeme der X450-G2 Serie unterstützen diesen IEEE 802.1 Standard.

Leistungsdaten

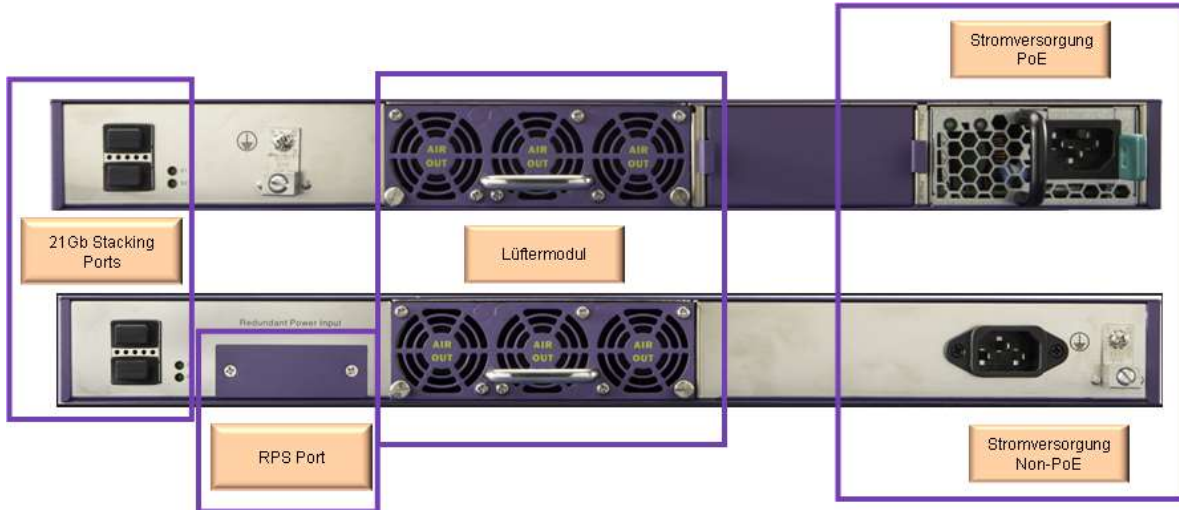
- 48-Port und 28-Port Modelle verfügbar
- 2 Bauformen: 4 Port SFP+ 10 GbE oder 4 Port SFP 1 GbE Uplink auf der Front
- Alle Versionen liefern full-duplex non-blocking Geschwindigkeit in allen Portbestückungen
- 40 Gbps Stacking über die Front Ports der 10GE Varianten
- SummitStack-V82 Stacking über die QSFP+ Ports an der Rückseite
- Latenz kleiner 4 Microsekunden (für 64 Byte Pakete)
- 68k (98.304) Layer-2 / MAC Adress Einträge in Hardware
- 16k (12.288) IPv4 LPM Einträge
- 256 (6.144) IPv6 LPM Einträge
- 4094 VLAN/VMANs
- Jumbo Frame Support bis maximal 9216 Byte Paketgröße
- 128 Linkaggregate Gruppen mit bis zu 32 physikalischen Ports je Gruppe
- Eingangs- und Ausgangs-Bandbreitenbegrenzung
- 8 Quality of Service Klassen per Port in Hardware (8 Hardware Queues)
- Bandbreitenbegrenzung am Ausgangsport pro Port und Queue
- Granulare Bandbreitenbegrenzung in Schritten von 8 kbps
- Voll-Duplex Unterstützung an allen Ports - Halb-Duplex Betrieb wird nicht unterstützt
- Volle Unterstützung durch Extreme Control Center inkl. Policy Support ab Version 6.3

Bestellhinweise

Die X450-G2 Systeme werden generell ohne Lüfter Modul geliefert. Diese sind also bei der Bestellung besonders zu berücksichtigen.

Die Non-PoE Modelle bieten eine fest montierte Stromversorgung sowie einen Anschluss für die externen Redundanzstromversorgungen STK-RPS-150 bzw. EPS-C2.

PoE-unterstützende Komponenten weisen zwei Einbauplätze für die Installation modularer Stromversorgungen mit 715 bzw. 1100W Nennleistung auf. Auch diese sind gesondert zu bestellen.



Wie bei allen Produkten aus dem Hause Extreme Networks Anschlussleitungen für Stromversorgungen optional geliefert. Dies erlaubt sowohl die flexible Anpassung an regionale Steckernormen als auch die Wiederverwendung bestehender Schrankverkabelungen.

Komponentenübersicht

Bestellnummer	Produktbezeichnung	Beschreibung
16172	X450-G2-24t-GE4-Base	Summit X450-G2 24 10/100/1000BASE-T, 4 SFP 2 21Gbps Stackports, eingebaute Stromversorgung, 1 RPS Port, Einbauplatz für Lüfter
16173	X450-G2-24p-GE4-Base	Summit X450-G2 24 10/100/1000BASE-T, 4 SFP, POE+ 2 21Gbps Stackports, 2 Einbauschächte für Stromversorgung, Einbauplatz für Lüfter
16174	X450-G2-48t-GE4-Base	Summit X450-G2 48 10/100/1000BASE-T, 4 SFP 2 21Gbps Stackports, eingebaute Stromversorgung, 1 RPS Port, Einbauplatz für Lüfter
16175	X450-G2-48p-GE4-Base	Summit X450-G2 48 10/100/1000BASE-T, 4 SFP, POE+, 2 21Gbps Stackports, 2 Einbauschächte für Stromversorgung, Einbauplatz für Lüfter
16176	X450-G2-24t-10GE4-Base	Summit X450-G2 24 10/100/1000BASE-T, 4 SFP+ 2 21Gbps Stackports, eingebaute Stromversorgung, 1 RPS Port, Einbauplatz für Lüfter
16177	X450-G2-24p-10GE4-Base	Summit X450-G2 24 10/100/1000BASE-T 4 SFP+ POE+ 2 21Gbps Stackports, 2 Einbauschächte für Stromversorgung, Einbauplatz für Lüfter
16178	X450-G2-48t-10GE4-Base	Summit X450-G2 48 10/100/1000BASE-T, 4 SFP+ unpopulated SFP+, two 21Gb stacking ports, 1 Fixed AC PSU, 1 RPS port, fan module slot (unpopulated), ExtremeXOS Edge license
16179	X450-G2-48p-10GE4-Base	Summit X450-G2 48 10/100/1000BASE-T, 4 SFP+ , POE+ 2 21Gbps Stackports, 2 Einbauschächte für Stromversorgung, Einbauplatz für Lüfter

10945	Summit X460/X450-G2 fan module FB	Lüftermodul für alle Modelle der X450-G2 Serie
10941	Summit 1100W PoE AC PSU FB	1100 Watt AC Stromversorgungsmodul für Summit X450-G2 PoE Switches, Front-to-Back Belüftung
10931	Summit 750W AC PSU	AC Power Supply module for EPS-C2 Chassis
STK-RPS-150PS	150W Non-PoE RPS	150 watt non-PoE redundant power supply for A, B, C and X450-G2 switches
STK-RPS-150CH2	Einbaurahmen	19" Einbaurahmen für 2 Stromversorgungsmodule STK-RPS-150PS
STK-RPS-150CH8	Einbaurahmen	19" Einbaurahmen für 2 Stromversorgungsmodule STK-RPS-150PS
10936	EPS-C2	External Power System Chassis 2. Accepts up to three Summit 750W AC PoE PSU 48V power supplies. Accepts up to 3 EPS-CBL-2x7 or up to 1 EPS-CBL-2x9 cables
10939	EPS-CBL-2x7	External Power System Cable (1M) that connects EPS to any Summit X440 for providing redundant DC power
16190	Summit X450-G2 Edge to Advanced Edge Lic	ExtremeXOS Advanced Edge License for Summit X450 series switches
11011	Direct Attach Feature Pack	Direct Attach Feature Pack
16200	Summit X450-G2 OpenFlow FeaturePack	ExtremeXOS SDN - OpenFlow Feature Pack for Summit X450 series switches
16169	X450-G2 Multimedia(AVB) Feature Pack	ExtremeXOS Multimedia Service (Audio Video Bridging) Feature Pack for Summit X450 series switches
16190	Summit X450-G2 Edge to Advanced Edge Lic	ExtremeXOS Advanced Edge License for Summit X450 series switches
11011	Direct Attach Feature Pack	Direct Attach Feature Pack
16200	Summit X450-G2 OpenFlow FeaturePack	ExtremeXOS SDN - OpenFlow Feature Pack for Summit X450 series switches
16169	X450-G2 Multimedia(AVB) Feature Pack	ExtremeXOS Multimedia Service (Audio Video Bridging) Feature Pack for Summit X450 series switches

Weitere Informationen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/summit-x450-g2-series

X 440-G2

Die Extreme Networks X440-G2 Serie stellt die Intelligenz und Verfügbarkeit des Extreme EXOS® Netzwerk-Betriebssystems bis zum konvergenten Access Bereich zur Verfügung. Die X440-G2 ermöglichen den Einsatz granularer Quality-Of-Service (QoS) Strukturen, Stackingfunktion, Hochverfügbarkeit, Benutzerauthentisierung und Sicherheitsfunktionen in einem kompakten, kostengünstigen Access Switch System.

Standardisiertes PoE/PoE+ (802.3af / 802.3at) ermöglicht den flächendeckenden Einsatz der X440-G2 Serie zur Unterstützung von konvergenten Endgeräten wie IP Telefone, WLAN Antennen (Wireless Access Points) oder Sicherheitseinrichtungen wie Videoüberwachungsanlagen oder Gebäudeleittechnik. Mit optionalen, externen Stromversorgungseinheiten lassen sich Redundanz und Power Budget selektiv und kostengünstig erhöhen.

Mit ihrer hohen Portdichte, niedrigen Latenz, der vollen Switching Bandbreite der 10/100/1000 Ethernet Ports, den dedizierten 10 Gigabit Stacking Ports und der kompakten Bauform in einer Höheneinheit (1 RU) stellen die X440-G2 eine kosteneffektive Lösung für den Netzwerkaccess Bereich dar. Die Verfügbarkeit von optionalen, redundanten Netzteilen, die Hardwareunterstützung von IPv4 und IPv6 sowie die umfangreichen Funktionalitäten im Bereich Layer-2 bis Layer-4 bestätigen dies.

Flexible Port Konfiguration

Alle Modelle sind mit 4 SFP 1 GbE Ports ausgestattet. Die Ports befinden sich an der Front- beziehungsweise Rückseite des jeweiligen X440-G2 Modells. Die meisten Modelle erlauben ein Lizenzupgrade dieser Ports auf SFP+ für eine Uplinksgeschwindigkeit von 10Gbps. In der nachfolgenden Komponentenübersicht werden die



Modelle benannt, die per Lizenz hochrüstbar sind. Die X440-G2 unterstützen das modulare und robuste EXOS® 21.x Netzwerkbetriebssystem wie die anderen Extreme Networks Produkte der zweiten Generation und ermöglichen damit ein durchgängiges Betriebssystem mit einheitlichem Funktionsumfang in allen Bereichen des Netzes.

Role Based Policy

Authentisierungsprozesse mit Regelwerken zu kombinieren, hat im Hause Extreme Networks schon lange Tradition. Logisch, dass die Access-Switches aller Leistungsklassen diese Methodik unterstützen. So lassen sich Anwendungen und Dienste wahlweise der Identität von Benutzer und Endgerät anhand der MAC Adresse, über 802.1x Authentisierung oder per Web-Login zuweisen.

In Kombination mit der Network Access Control Lösung und dem zentral orientierten Policy Management wird ein durchgängiges Sicherheits- und Administrationskonzept flächendeckend ausgerollt. Diese standardisierte Vorgehensweise hält administrative

Aufwände im angemessenen Rahmen und skaliert reibungslos. Funktionale Benutzer- oder Gerätegruppen bilden eine Entscheidungsmatrix für den strukturierten Zugriff auf Dienste und Ressourcen.

ExtremeCloud™ Management

Mit der ExtremeCloud Management Lösung können Wireless (AP) & Netzwerk Komponenten (Switches) zentral über eine Web Applikation verwaltet & konfiguriert werden. Nach der Montage beziehen die Komponenten selbständig eine IP Adresse und nehmen über eine gesicherte Verbindung zu einer, in Deutschland residenten Cloudinstanz auf. Einstellungen und Überwachung werden nun - unternehmensweit - über das mandantenfähige Webmanagement vorgenommen.

Weitere Information über die ExtremeCloud Services finden Sie in diesem Buch sowie unter <http://extremenetworks.com/product/extremecloud> auf unserer Website

Vereinfachte Inbetriebnahme und unkomplizierter Netzwerkbetrieb

- Modulares EXOS® Betriebssystem als netzwerkweit einheitliches Betriebssystem
- Automatische Anpassung der Portkonfiguration durch Erkennung des angeschlossenen Endgerätes und automatisierte Provisionierung (Universal Port)
- Optionaler Einsatz von Widgets und Skripting Funktionen (TCL oder Python) für automatisierten Betrieb und dynamische Anpassung
- Unterstützung von CDP/LLDP/LLDP-MED für automatisiertes Endgerätemanagement
- Zero touch & Zero touch plus support. Vorteil des "Zero-Touch Deployment" ist eine vollständig automatisierte Erstkonfiguration, welche keine Interaktion erfordert. Zentral bereitgestellte Konfigurationsimages auf einem RADIUS oder ExtremeManagement Server reduzieren den administrativen Aufwand zusätzlich. Mit der automatisierten Installation von Betriebssystem und Konfiguration lassen sich Wartungs- und Supporteinsätze essentiell vereinfachen.

Hochverfügbarkeit

- Ethernet Automatic Protection Switching (EAPS) Hochverfügbarkeitsprotokoll
- SummitStack-V™ - Hoch verfügbare High Speed Stack über 10 Gigabit SFP+ Ports mit Optiken bis 40 km
- Externe Power Supplies für redundante Stromversorgung: EPS-C2 für die Absicherung von bis zu 5 X440 Systemen, RPS-500p & RPS-150 XT für die Absicherung eines einzelnen X440 Systemes
- Non-POE Varianten sind auch mit Gleichspannungsstromversorgung lieferbar

High-Performance

- Hohe Bandbreite, Non-Blocking Architektur
- Quality of Service (QoS) mit erweiterten Traffic Management Funktionen
- Automatische Provisionierung via Universal Port Funktion
- Umfangreiche Netzwerkmanagement Funktion
- 12, 24 oder 48-port Gigabit Ethernet (GbE) Varianten in 1 Höheneinheit (1RU)

- SummitStack-V® mit 40 Gbps Geschwindigkeit
- Optional 10 Gigabit Ethernet (10GbE) Uplinks via Lizenz zu aktivierbar

Sicherheitsfunktionen

- Umfangreiche MAC und IP Adressen Sicherheitsfunktionen für die Erkennung von zahlreichen Angriffsszenarien (z. B.. Man-in-the-Middle Attacken)
- Universal Port Funktion mit dynamischer Zuordnung von Sicherheitsprofilen für die Errichtung granularer Sicherheitskonzepte
- Sicherer Netzwerkzugang durch Web, 802.1x, und MAC Adressen Authentisierung
- Multimethod-Authentisierung an den Access-Ports
- Multiuser Authentisierung
- Role Base Policy

X440-G2 - Zusammenfassung

- Hochperformanter 10/100/1000 Base-T Switch für Access Bereich
- Hardware Varianten mit 12, 24 und 48- Ports 10/100/1000 Base-T verfügbar
- 4x1 Gigabit Uplink upgradebar via Lizenz auf 10 GB.
- Stacking Support SummitStack-V
- Role Based Policy
- PoE 802.3at auf den PoE fähigen Varianten über alle Kupfer Ports
- Umfangreiche QoS Möglichkeiten für Einsatz in Multimedia Anwendungen
- Sicherer Netzwerk-Zugang durch Web, 802.1x, und MAC Adressen Authentisierung
- Gleichzeitige Multimethod-Authentisierung am Access-Port
- Multiuser Authentisierung
- EXOS Edge Lizenz für volle Layer-2 Funktion incl. Spanningtree, EAPS, Link Aggregation sowie Layer-3 Funktionen mit statischem Routing und RIP
- Optionale Advanced Edge Lizenz für Freischaltung dynamischer Routingprotokolle OSPFv2, OSPFv3 und PIMv4/v6 für 4 aktive Interfaces
- Optionale AVB Unterstützung
- Optional SDN
- Managebar über Extreme Control Center und voll integrierbar in Identity & Access Control
- Investitionsschutz via Lifetime Garantie
- Extreme Cloud Fähig (ausgewählte Modelle)

X440-G2 – Bestellinformationen

Bestellnummer	Produktbezeichnung	Beschreibung
16530	Summit X440-G2-12t-10GE4	12 Port 10/100/1000BASE-T, 4 dedizierte 1GbE SFP Uplink upgradbar auf 10GbE SFP+ Ports, SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz.
16531	X440-G2-12p-10GE4	12 Port 10/100/1000BASE-T POE+ fähig, 4 dedizierte 1GbE SFP Ports upgradbar auf 10GbE SFP+ Ports, SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz.
16532	X440-G2-24t-10GE4	24 Port 10/100/1000BASE-T, 8 SFP combo Ports davon 4 dedizierte 1GbE SFP Ports + 4 dedizierte 1GbE SFP Ports upgradbar auf 10GbE SFP+ Ports, SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz
16533	X440-G2-24p-10GE4	24 Port 10/100/1000BASE-T POE+ fähig, 8 SFP combo Ports davon 4 dedizierte 1GbE SFP Ports + 4 dedizierte 1GbE SFP Ports upgradbar auf 10GbE SFP+ Ports, SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz
16534	X440-G2-48t-10GE4	48 Port 10/100/1000BASE-T, 8 SFP combo Ports davon 4 dedizierte 1GbE SFP Ports + 4 dedizierte 1GbE SFP Ports upgradbar auf 10GbE SFP+ Ports, (2 combo/2 non-combo), 2 1GbE BASE-T combo Ports upgradbar auf 10GbE, SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz
16535	X440-G2-48p-10GE4	48 Port 10/100/1000BASE-T POE+, 8 SFP combo Ports davon 4 dedizierte 1GbE SFP Ports + 4 dedizierte 1GbE SFP Ports upgradbar auf 10GbE SFP+ Ports, (2 combo/2 non-combo), 2 1GbE BASE-T combo Ports upgradbar auf 10GbE, SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz
16536	X440-G2-24t-10GE4-DC	24 Port 10/100/1000BASE-T POE+, 8 SFP combo Ports davon 4 dedizierte 1GbE SFP Ports + 4 dedizierte 1GbE SFP Ports upgradbar auf 10GbE SFP+ Ports, (2 combo/2 non-combo), 2 1GbE BASE-T combo Ports upgradbar auf 10GbE, SummitStack-V® support. Ein internes DC PSU, ExtremeXOS Edge Lizenz
16537	X440-G2-48t-10GE4-DC	48Port 10/100/1000BASE-T POE+, 8 SFP combo Ports davon 4 dedizierte 1GbE SFP Ports + 4 dedizierte 1GbE SFP Ports upgradbar auf 10GbE SFP+ Ports, 1 internes 230V Netzteil, ExtremeXOS Edge Lizenz, Anschlußport für externes redundantes Netzteil
16538	X440-G2-24x-10GE4	24 100/1000BASE-X SFP Ports, davon 8 Gigabit Combo Ports (4 RJ45 Ports geshared mit 100/1000BASE-X Ports) + 4 dedizierte 1GbE SFP Ports upgradbar auf 10GbE SFP+ Ports, SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz

A4-Serie

Überblick

Die Extreme A-Serie bietet leistungsstarke, schnelle Enterprise-Class Edge Switches mit einer Switching-Kapazität von bis zu 17,6 Gbps. Die Serie beinhaltet Switches mit bis zu 48 Ethernet Ports 10/100 Base-T oder 24 100Base-FX-Ethernet-Ports und 4 Gigabit-Ethernet-Uplink-Ports. Die A4-Serie bietet Multi-Layer-QoS und Prioritätsqueuing für unterschiedliche Dienste. Durch robuste QoS-



Eigenschaften eignet sich der A4 besonders für integrierte Multimedia-Netzwerke mit VoIP und Video sowie datenintensive Anwendungen. In Verbindung mit seiner Non-blocking Layer-2-Switching-Architektur stellt der intelligente Queuing-Mechanismus des A4 sicher, dass geschäftskritische Anwendungen vorrangigen Zugriff auf Netzwerk-ressourcen erhalten. Der Switch garantiert durch seine Authentifizierungs- und Sicherheits-Features auf Port- oder User-Ebene ein sicheres Netzwerk. Pro Port können 2 Endgeräte (z. B. PC und VoIP Telefon) authentifiziert und mit dynamischen Regelwerk versehen werden. Die A4 Serie unterstützt rollenbasierte dynamische Policies. Die Authentifizierung erfolgt via IEEE 802.1x oder MAC Adresse.

Zuverlässigkeit und Verfügbarkeit

Redundanz und Fehlerschutz – die Grundvoraussetzungen für ein zuverlässiges Netz - realisiert der A4-Switch durch automatisierte Fehler- und Recovery-Leistungen. Über Stacking können bis zu 8 Switches in einem Verbund betrieben werden und stellen eine Gesamtkapazität von bis zu 140,8 Gbps über bis zu 384 10/100 Ethernet Ports zur Verfügung. Das Closed-Loop-Stacking des A4 nutzt bidirektionale Switchverbindungen, damit auch bei Fehlern auf der physikalischen Ebene der Switches die Verbindungen im virtuellen Switch erhalten bleiben. Der Switch arbeitet im Stack mit Wire Speed, ist skalierbar und eignet sich besonders für breitbandintensive und verzögerungssensitive Applikationen. Die A4 Serie unterstützt Link-Aggregation mit bis zu acht Ethernet Links pro Link Aggregation Group. Diese LAGs lassen sich innerhalb eines Stacks über mehrere Switches verteilen, dies vermeidet eine Unterbrechung der Datenkommunikation aufgrund von Fehlern auf Switchlevel. Externe Power Supply Module stellen optional die Stromversorgung der A4 Serie sicher.

Investitionsschutz

Der A4 ist ein kosteneffizienter, stackbarer Switch für den Access Bereich mit umfangreichem Featureset. Für alle Switches der A-Serie gilt die Extreme Networks Lifetime Garantie. Zum Garantieumfang gehören der Vorabaustausch der Hardware im Fehlerfall, Firmware-Upgrades und Telefonsupport.

Zusammenfassung

- Hoch performanter 10/100-BaseT stackable Switch
- Kostengünstiger Switch für FTTX Anwendungen mit 24 Ports 100Base-FX
- Vollständig Managebar über Extreme Control Center
- Hochverfügbarkeit durch Redundanzen in Stromversorgung und Stacking
- Unterstützung von dynamische Rollen basierenden Policies
- Umfangreiche QoS Möglichkeiten für Einsatz in Multimedia Anwendungen
- PoE 802.3af
- Sicherer Netzwerkzugang durch Web, 802.1x, und MAC Address Authentication
- Multiuser Authentifizierung (PC + VoIP Telefon) pro Port
- Investitionsschutz via Lifetime Garantie

Extreme A4 -Varianten

Modell	Beschreibung
A4H124-24	24 x 10/100, (2) SFP Ports, (2) 10/100/1000 stacking/uplink RJ45 ports, Ext RPS
A4H124-24P	24 x 10/100 PoE (.af), (2) SFP Ports, (2) 10/100/1000 stacking/uplink RJ45 ports, Ext RPS
A4H124-48	48 x 10/100, (2) SFP Ports, (2) 10/100/1000 stacking/uplink RJ45 ports, Ext RPS
A4H124-48P	48 x 10/100 PoE (.af), (2) SFP Ports, (2) 10/100/1000 stacking/uplink RJ45 ports, Ext RPS
A4H124-24FX	24 x 100Base-FX, (2) SFP Ports, (2) 10/100/1000 stacking/uplink RJ45 ports, Ext RPS
A4H254-8F8T	8 x 100Base-FX plus 8 x 10/100, (2) SFP ports, (2) 10/100/1000 stacking/uplink RJ45 ports, Ext RPS

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/a-series

B5-Serie

Zusammenfassung

Die Extreme B-Serie bietet kostengünstige, leistungsstarke Gigabit Ethernet Edge Switchkomponenten für den Enterprise Bereich mit einer Switching-Kapazität von bis zu 184 Gbps. Das Gerät eignet sich besonders für bandbreitenintensive und verzögerungssensitive Applikationen. Damit ist der B5 erste Wahl für Umgebungen mit hohen Dichten an 10/100/1000-Ethernet-Ports im Access- und Distributions-Bereich. Die B5 Serie bietet



grundlegende Routing-Eigenschaften, in Form von RIP, statisches IPv4-Routing und IPv6-Management-Support. Das Gerät unterstützt bis zu 48 10/100/1000Mbps-Ethernet-Ports und 4x Gigabit- bzw. 2x Gigabit + 2x 10-Gigabit-Ethernet-Uplink-Ports.

Über Stacking können bis zu 8 B5 Switches im Verbund betrieben werden. Ein virtueller Switch mit bis zu 384 10/100/1000-Mbps-Ethernet-Ports sowie 32 Gigabit-Ethernet- oder 16 10-Gigabit-Ethernet-Uplink-Ports und einer Switching Kapazität von bis zu 1,5 Tbps Kapazität kann so dargestellt werden. Der Switch arbeitet im Stack mit Wire Speed und ist skalierbar. Die B5 Serie unterstützt Link-Aggregation mit bis zu acht Ethernet Links pro Link Aggregation Group. Diese LAGs lassen sich innerhalb eines Stacks über mehrere Switches verteilen, dies vermeidet eine Unterbrechung der Datenkommunikation aufgrund von Fehlern auf Switchlevel. Externe Power Supply Module stellen optional die Stromversorgung der B5 Serie sicher.

Extreme B5 – QoS

Umfangreiche Features im QoS (Quality of Service) empfehlen die Switchmodelle B5 für integrierte Multimedia-Netzwerke mit VoIP und Video sowie alle datenintensiven Anwendungen. Die Authentifizierungs- und Sicherheitsfeatures des B5 schützen das Netzwerk vor Angriffen von innen und außen. Pro Port können bis zu 4 Endgeräte oder Benutzer über MAC, 802.1x oder Web based authentifiziert und sicher ins Netzwerk geleitet werden.

Für jeden authentifizierten User können granular konfigurierbare Regelwerke zugewiesen werden. Die rollenbasierten Regelwerke, sog. Policies, können neben VLAN Zuordnung auch QoS Merkmale und Layer 4 basierte Zugriffsrechte beinhalten. Policies kann man pro Anwender oder auch statisch pro Port definieren. Mit Hilfe von Extreme Identity & Access Control oder über das Command-Line-Interface können Netzwerk-administratoren für operative Gruppen von Endgeräten oder Nutzern (Drucker, VoIP Telefone, Mitarbeiter, Geschäftsführung ...) im Unternehmen individuelle Rollen oder Profile erstellen und im Netzwerk ausrollen. Das leistungsfähige rollenbasierte Managementkonzept ermöglicht Hunderte individueller Policies. Diese gestatten eine sehr detaillierte Definition des Netzwerkzugangs und der

Nutzungsrechte für die verschiedenen Nutzer und Applikationen im Netzwerk. Dadurch lässt sich die Nutzung der Netzwerkressourcen genau an Geschäftszielen und Prioritäten ausrichten.

Extreme B5 - Zuverlässigkeit und Verfügbarkeit

Die Geräte der B-Serie bieten bei nur einer Höheneinheit (1U) im Rack eine hohe Port-Dichte. Sie entsprechen den gestiegenen Anforderungen in Sachen Energieeffizienz und Umweltfreundlichkeit. Der Switch verfügt über eine extreme Toleranz gegenüber hohen Umgebungstemperaturen und sorgt somit für einen geringen Stromverbrauch. Ihre hochskalierbare Architektur und die lebenslange Garantie machen die B5-Switche zu einer zukunftsfähigen Investition.

Redundanz und Fehlerschutz - Grundvoraussetzungen für ein zuverlässiges Netz - realisiert der B5-Switch durch automatisierte Fehler- und Recovery-Leistungen. Über Stacking können bis zu 8 Switche in einem Verbund betrieben werden und stellen eine Gesamtkapazität von mehr als 1,4 Tbps über bis zu 384 10/100/1000 Base-T Ethernet Ports zur Verfügung. Das Closed-Loop-Stacking nutzt bidirektionale Switchverbindungen, damit auch bei Fehlern auf der physikalischen Ebene der Switche die Verbindungen im virtuellen Switch erhalten bleiben. Der Switch arbeitet im Stack mit Wire Speed, ist skalierbar und eignet sich besonders für brandbreitenintensive und verzögerungssensitive Applikationen. Die B5 Serie unterstützt Link-Aggregation mit bis zu acht Ethernet Links pro LAG. Die LAG'S können innerhalb eines Stacks über mehrere Switche verteilt werden. Dadurch kann eine Unterbrechung der Datenkommunikation aufgrund von Fehlern auf Switchlevel vermieden werden. Die Stromversorgung der B5 Serie Switche kann über externe redundante Power Supplies abgesichert werden.

Extreme B5 - Zusammenfassung

- Hochperformanter 10/100/1000 Base-T Stackable Switch für Access und Distribution Bereich
- Bis zu 2 x 10 Gigabit Uplink über SFP+ Interfaces
- 48 Gig Stacking Bandbreite
- Vollständig managebar über Extreme Control Center
- Hochverfügbarkeit durch Redundanzen in Stromversorgung und Stacking von Switchen.
- Unterstützung von dynamische Rollen basierenden Policies
- Umfangreiche QoS Möglichkeiten für Einsatz in Multimedia Anwendungen
- PoE 802.3at auf allen PoE fähigen B5 Varianten über alle Kupfer Ports
- Multimethod-Authentifizierung am Port. Sicherer Netzwerk Zugang durch Web, 802.1x, und MAC Address Authentication
- Multiuser Authentifizierung (Bis zu 4 Endgeräte) pro Port
- Investitionsschutz durch Lifetime Garantie

Extreme B5 – Varianten

Modell	Beschreibung
B5G124-24	(24) 10/100/1000 RJ45 ports, (4) combo SFP ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports
B5G124-24P2	(24) 10/100/1000 PoE (.at + .af) RJ45 ports, (4) combo SFP ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports
B5G124-48	(48) 10/100/1000 RJ45 ports, (4) combo SFP ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports
B5G124-48P2	(48) 10/100/1000 PoE (.at + .af) RJ45 ports, (4) combo SFP ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports
B5K125-24	(24) 10/100/1000 RJ45 ports, (2) combo SFP ports, (2) 10GE ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports + (2) 10GE ports
B5K125-24P2	(24) 10/100/1000 PoE (.at + .af) RJ45 ports, (2) combo SFP ports, (2) 10GE ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports + (2) 10GE ports
B5K125-48	(48) 10/100/1000 RJ45 ports, (2) combo SFP ports, (2) 10GE ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports + (2) 10GE ports
B5K125-48P2	(48) 10/100/1000 PoE (.at + .af) RJ45 ports, (2) combo SFP ports, (2) 10GE ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports + (2) 10GE ports

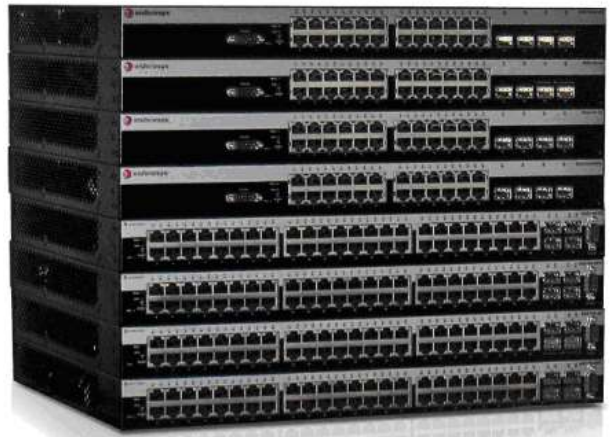
Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/b-series

C5-Serie

Überblick

Bei der Extreme C5 Serie handelt es sich um hochperformante und kostengünstige Gigabit Ethernet Switches für den Enterprise Bereich mit dynamischem IPv4 und IPv6 Routing, IEEE 802.3at PoE+, hohen Portdichten, flexiblen 10 Gigabit Ethernet Optionen und einer Switching-Kapazität von bis zu 264 Gbps. Der C5 eignet sich besonders für hochkomplexe Netzwerkkomplexe im Distribution, Core und Server Bereich. Gegenüber der B5 Serie bietet der Switch einen erweiterten



Funktionsumfang für dynamisches Routing sowie eine höhere Skalierbarkeit im Bereich der Authentifizierung und Autorisierung.

Die C5 Serie bietet vollen Routing Support für IPv4 und IPv6. Das Gerät unterstützt bis zu 48 10/100/1000 Mbps-Ethernet-Ports und 4x Gigabit- bzw. 2x Gigabit + 2x 10-Gigabit-Ethernet-Uplink-Ports.

Über Stacking können bis zu 8 x C5 (24 und 48 Port Varianten) Switches im Verbund betrieben werden. Ein virtueller Switch mit bis zu 384 10/100/1000 Mbps-Ethernet-Ports sowie 32 Gigabit-Ethernet- oder 16 10-Gigabit-Ethernet-Uplink-Ports und einer Switching Kapazität von bis zu 2,1 Tbps kann so dargestellt werden. Der Switch arbeitet im Stack mit Wire Speed, ist skalierbar und eignet sich besonders für brandbreitenintensive und verzögerungssensitive Applikationen. Die C5 Serie unterstützt Link-Aggregation mit bis zu acht Ethernet Links pro Link Aggregation Group. Diese LAGs lassen sich innerhalb eines Stacks über mehrere Switches verteilen, dies vermeidet eine Unterbrechung der Datenkommunikation aufgrund von Fehlern auf Switchlevel.

Extreme C5 – QoS

Zusätzlich zu den Features der B5 Serie, können auf den C5 Switches bis zu 8 Endgeräte oder Benutzer über MAC, 802.1x oder Web-based authentifiziert und sicher ins Netzwerk geleitet werden. Dadurch können auch vorgeschaltete unmanaged Mini-Office oder Kabel-Einbau Switches in ein Sicherheitskonzept mit dedizierter Zugriffskontrolle integriert werden. Die sichere Authentifizierung und Policy Vergabe wird in die zweite Ebene des Netzwerkes verlegt und garantiert auch beim Einsatz von kostengünstigen Front End Port Switches ein sicheres und flexibles Netzwerk.

Extreme C5 - Zuverlässigkeit und Verfügbarkeit

Wie die B5 Serie bieten die C5 Switches bei nur einer Höheneinheit (1U) im Rack eine hohe Port-Dichte. Durch Stacking kann eine performante und redundante Hardware Plattform geschaffen werden. Die Stromversorgung der C5 Serie Switches kann über

externe redundante Power Supplies abgesichert werden. Für die Modelle der C5 Serie erhöht die redundante Stromversorgung im Normalbetrieb zusätzlich die mögliche Leistungsabgabe für PoE-Ports.

Extreme C5 - Zusammenfassung

- Hochperformanter 10/100/1000 Base-T Stackable Switch für Distribution und Core Bereich
- Modelle mit SFP für FTTx Topologien sind verfügbar
- Advanced Routing IPv4 und IPv6
- Multicast Routing IPv4 und IPv6
- Bis zu 2 x 10 Gigabit Uplink über SFP+ Interfaces pro Switch. Bis zu 16 x 10Gig Ports pro Stack
- 128 Gig Stacking Bandbreite
- Vollständig Managebar über Extreme Control Center
- Hochverfügbarkeit durch Redundanzen in Stromversorgung und Stacking von Switchen
- Unterstützung von dynamische Rollen basierenden Policies
- Umfangreiche QoS Möglichkeiten für Einsatz in Multimedia Anwendungen
- PoE 802.3at auf allen PoE fähigen C5 Varianten über alle Kupfer Ports. Redundantes Power Supply liefert zusätzliche PoE Power für Redundanz oder additiv.
- Multimethod Authentifizierung am Port. Sicherer Netzwerkzugang durch Web, 802.1x, und MAC Address Authentication
- Multiuser Authentifizierung (Bis zu 8 Endgeräte) pro Port
- Investitionsschutz via Lifetime Garantie

Extreme C5 – Varianten

Modell	Beschreibung
C5G124-24	(24) 10/100/1000 RJ45 ports, (4) combo SFP ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports
C5G124-24P2	(24) 10/100/1000 PoE (.at + .af) RJ45 ports, (4) combo SFP ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports
C5G124-48	(48) 10/100/1000 RJ45 ports, (4) combo SFP ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports
C5G124-48P2	(48) 10/100/1000 PoE (.at + .af) RJ45 ports, (4) combo SFP ports, (2) dedicated high-speed dedicated stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports
C5K125-24	(24) 10/100/1000 RJ45 ports, (2) combo SFP ports, (2) SFP+, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports + (2) 1GE or 10GE SFP+ ports
C5K125-24P2	(24) 10/100/1000 PoE (.at + .af) RJ45 ports, (2) combo SFP ports, (2) SFP+, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports + (2) 1GE or 10GE SFP+ ports

C5K125-48	(48) 10/100/1000 RJ45 ports, (2) combo SFP ports, (2) SFP+, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports + (2) 1GE or 10GE SFP+ ports
C5K125-48P2	(48) 10/100/1000 PoE (.at + .af) RJ45 ports, (2) combo SFP ports, (2) SFP+, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports + (2) 1GE or 10GE SFP+ ports
C5K175-24	(24) SFP, (2) SFP+ ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) SFP, (2) 1GE or 10GE SFP+ ports

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/c-series

D2-Serie

Überblick

Der Extreme D2 Switch ist ein hochperformanter Switch mit hoher Temperaturtoleranz und niedriger Geräuschentwicklung, geeignet für den Einsatz in Büro-, Konferenz- oder Schulungsräumen.

Durch seine hohe Temperaturtoleranz arbeitet der Switch bis zu einer Außentemperatur von 40° Celsius (35° mit PoE) ohne Lüftereinsatz. Die D-Serie eignet sich dadurch für den Einsatz in geräuschsensiblen Umgebungen



Der D2 Switch bietet 10 x 10/100/1000Mbps-Ethernet-Ports und 2 Combo Ports 10/100/1000 Base T und SFP. Es gibt Varianten - mit und ohne PoE 802.3af - für die Versorgung von WLAN Access Points oder VoIP Telefonen. Die D2 Serie besitzt die Möglichkeit für 2 externe Stromversorgungsmodule zur redundanten Versorgung.

Die Switches der Serie sind vielfältig montierbar. Es gibt Montagekits für die Wand- oder Deckenmontage. Abschließbare Untertisch-Montagekits für den Einsatz in Schulungsräumen oder öffentlichen Umgebungen sind ebenfalls lieferbar. Für den Einsatz im Rack bietet Extreme ein Kit zur Installation zweier D2s nebeneinander an.

Die D-Serie unterstützt analog zur B-Serie alle SecureNetworks™ Features.

Zusammenfassung

- Hochperformanter 10/100/1000 Base-T Workgroup Switch für Access Bereich
- Geräuscharm durch temperatur gesteuerte Lüfter. Lüfter arbeiten erst ab 40°C Außentemperatur (35°C mit PoE)
- Information-LEDs auf Front- und Oberseite des Switches für verschiedene Einbauoptionen.
- Montagekits für Wand-, Decken- und Untertischmontage.
- Abschließbares Container-Montagekit zum Einbau in sensiblen Bereichen.

- Vollständig managebar über Extreme Control Center
- Hochverfügbarkeit durch Stromversorgungsredundanzen
- Unterstützung dynamischer, rollenbasierender Policies
- Umfangreiche QoS Möglichkeiten zum Einsatz in Multimedia Anwendungen
- PoE 802.3af auf allen PoE fähigen D2 Varianten über alle Kupfer Ports
- Dynamisch verwaltetes Power Budget (100W)
- Multimethod Authentifizierung am Port. Sicherer Netzwerkzugang durch Web, 802.1x, und MAC Address Authentication
- Multiuser Authentifizierung mit bis zu 2 Endgeräten pro Port
- Investitionsschutz via Lifetime Garantie

Extreme D2 – Varianten

Modell	Beschreibung
D2G124-12	12 X 10/100/1000 FIXED CONFIG L2 SWITCH & POWER BRICK
D2G124-12P	12 X 10/100/1000 FIXED POE L2 SWITCH & POWER BRICK

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

<https://extranet.extremenetworks.com/downloads/pages/D.aspx>

X 430

Die Extreme Networks X430 Serie von Standalone Gigabit Ethernet Switchen bietet Layer-2 Access-Konnektivität für Enterprise Kunden, Filialunternehmen und KMU Kunden. Die X430 Serie ist als 28- oder 52-Port 10/100/1000 Mbps



System oder als 8- oder 24- Port Modell mit 10/100/1000 Mbps und IEEE 802.3at PoE Unterstützung verfügbar. Alle Modelle sind ideal für die Implementierung von konvergenten Netzwerken für Sprache/Unified Communications, Wireless Mobility sowie Multimedia und Multicast Streaming Netzwerke geeignet und stellen somit Grundbausteine des Extreme Networks Open Fabric Edge Netzwerkes dar.

Die X430 Serie vereinfacht den Betrieb von Netzwerken durch die Nutzung von Extreme EXOS, einem modularen Betriebssystem (OS), das auf allen Extreme Networks Ethernet Switching Systemen eingesetzt wird. EXOS ermöglicht Netzwerkbetreibern und Administratoren den Aufbau und Betrieb von sicheren und hochverfügbaren Netzwerken und unterstützt dies durch vereinfachtes Management, operative Effizienz und niedrige Gesamtbetriebskosten (TCO - Total Cost of Ownership)

Quality of Service

Die X430 unterstützen Policy-basiertes Quality-of-Service (QoS) mit erweiterten Traffic-Management Funktionalitäten auf Layer-2 bis Layer-4 für den Einsatz in

konvergenten Anwendungsumgebungen. Sie bieten 8 hardwarebasierte QoS Queues und unterstützen granulares Bandbreitenmanagement (8kbps-1Mbps). Dies ermöglicht den Aufbau zuverlässiger Netze für den Transport von Daten-, Sprach- und Video-Anwendungen.

Die Authentisierungs- und Sicherheitsfeatures des EXOS schützen das Netzwerk vor Angriffen von innen und außen. Pro System können bis zu 1024 Endgeräte oder Benutzer über MAC, 802.1x oder Web-based authentifiziert und sicher ins Netzwerk geleitet werden.

Zuverlässigkeit und Verfügbarkeit

Die X430 Serie bietet auf einer Höheneinheit mit einer Bautiefe von ca. 25 cm und einem geräuscharmen Betrieb ideale Voraussetzungen für Installationen im offenen Office-Bereich oder in kleineren Wandschränken. Die Systeme bieten bis zu 4 SFP basierende 100/1000BASE-X Uplink-Ports an der Front (SFPs sind optional erhältlich), das 8-Port PoE+ Modell bietet zwei zusätzliche SFP Uplink-Ports. Diese zusätzlichen Ports können für die hochperformante Anbindung an Core- bzw. Distributionssysteme als Link-Aggregate eingesetzt werden.

X430 - Zusammenfassung

- Hochperformanter 10/100/1000 Base-T Switch für Access Bereich
- Bis zu 4 x 1 Gigabit Uplink über dedizierte SFP Interfaces
- PoE 802.3at auf den PoE fähigen Varianten über alle Kupfer Ports
- Umfangreiche QoS Möglichkeiten für Einsatz in Multimedia Anwendungen
- Sicherer Netzwerkzugang durch Web, 802.1x, und MAC Adressen Authentisierung
- Multimethod Authentisierung an den Access-Ports incl. Multiuser Authentisierung
- EXOS L2 Edge Lizenz für volle Layer-2 Funktion incl. Spanningtree, EAPS, Link Aggregation und LLDP
- Optionale AVB Unterstützung
- Managebar über Extreme Control Center
- Investitionsschutz durch Lifetime Garantie



Summit X430-8p



Summit X430-24p



X430-24t



X430-48t

X430 - Bestellinformation

Bestellnummer	Produktbezeichnung	Beschreibung
16515	Summit X430-8p	8 Ports 10/100/1000BASE-T PoE+ und 2 dedizierte 1000BASE-X SFP Uplink Ports, internes 230V Netzteil, ExtremeXOS L2 Edge license
16517	Summit X430-24p	24 Ports 10/100/1000BASE-T mit PoE+ nach 802.3at Standard und 4 dedizierte 1000BASE-X SFP Uplink Ports. internes 220V Netzteil, ExtremeXOS L2 Edge license
16516	Summit X430-24t	24 Port 10/100/1000BASE-T und 4 dedizierte 1000BASE-X SFP Uplink Ports, internes 220V Netzteil, ExtremeXOS L2 Edge license
16518	Summit X430-48t	48 Port 10/100/1000BASE-T und 4 dedizierte 1000BASE-X SFP Uplink Ports, internes 220V Netzteil, ExtremeXOS L2 Edge license

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

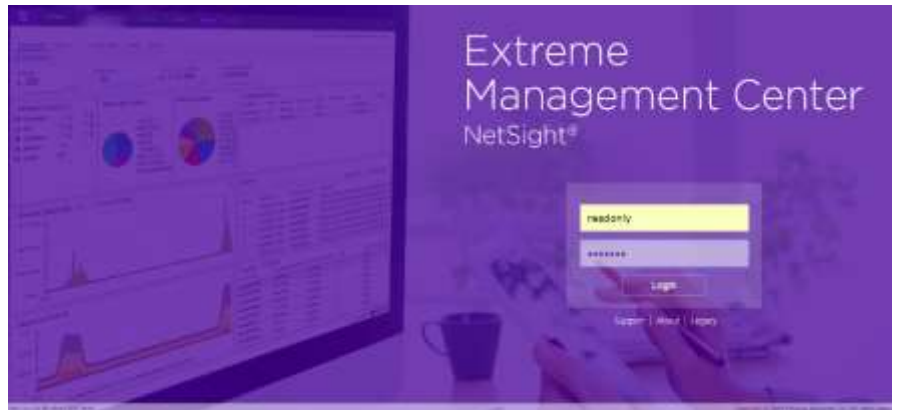
www.extremenetworks.com/product/summit-x430-series/

5 Management & Software



Extreme Management Center

Mit der der Erstaufgabe von OneView als Oberfläche in NetSight hat Extreme Networks einen Trend gestartet, der sich in der Version 7.x nun konsequent fortsetzt. Ziel ist die Migration der Managementoberfläche JBoss Java Applets hin zur webbasierten Umgebung ohne Versionsabhängigkeiten.



Extreme Management Center (aka OneView™)

Schon in der aktuellen Version finden sich Informationen und Funktionen der einzelnen Anwendungen wieder. So findet sich die Console und der Inventory Manager mit all ihren Funktionen im Reiter „Network“ wieder. Auch Policy Manager, WLAN Manager und Purview sind in der aktuellen Version integriert und werden bis zum nächsten Major-Release vollständig abgebildet sein. Natürlich gibt es immer noch die Möglichkeit, die bekannten Applets auch aus dieser Umgebung heraus zu starten.

Mit diesem Wandel ist auch ein Wechsel von NetSight als Produktname hin zu Extreme Management Center (EMC) verbunden.

Extreme Management Center ist eine Management Plattform, die entwickelt wurde um den heutigen Anforderungen gerecht zu werden, Netzwerke zu kontrollieren, konfigurieren und zu verwalten. Extreme Management Center bietet umfassende Managementunterstützung für sämtliche Komponenten und Lösungen von Extreme Networks. Auch Komponenten anderer Hersteller lassen sich in Extreme Management Center implementieren um eine zentrale Plattform zu bieten, die alle Komponenten einer Netzwerkkumgebung darstellen kann. EMC ermöglicht einen Blick über Ports VLAN's und SSID hinweg auf den Enduser.

Infrastruktur Management, Kontrolle und Verwaltung

Network/Wireless

Der Network und Wireless Tab beim EMC wird für das Management und zur Verwaltung der physischen Netzinfrastruktur benutzt. Über diese Bereiche lassen sich alle aktiven Komponenten von Extreme (Wired und Wireless) und auch von 3rd-Party

Herstellern konfigurieren, verwalten und überwachen. Der Network Tab ist in verschiedene Untergruppen aufgeteilt:

Dashboard

Das Dashboard bietet einen schnellen Überblick über die Netzwerkumgebung. Verschiedene Graphiken zeigen den Zustand der kompletten Infrastruktur (Wired und Wireless) und geben Anhaltspunkte über die aktuelle Performance aller Netzbestandteile. Alle Dashboards können über den Report Designer angepasst werden, um dem Administrator die Informationen zu Verfügung zu stellen, die für ihn wichtig sind.



Network Dashboard

- 1) Infos zu aktiven LAN Komponenten: Zeigt die Liste der am wenigsten verfügbaren aktiven Komponenten im Netzwerk, die Switches mit höchsten CPU Auslastung und die Switch Interfaces mit der höchsten Port Auslastung.
- 2) Infos zu WLAN: Zeigt den Status und die Verfügbarkeit von Controllern, AP's und Clients. Zeigt Bandbreitennutzung von Controllern und AP's und zeigt die Anbindung und Verteilung von Clients im WLAN.
- 3) Infos zu Alarmen: Zeigt die aktuellen kritischen Alarme zu Elementen im Netzwerk und die Systeme mit der höchsten Auslastung.

Devices

Dieser Bereich liefert eine umfassende Übersicht über die Netzwerkinfrastruktur. Die Darstellung der aktiven Netzwerkkomponenten wird sowohl in tabellarischer als auch in graphischer Ansicht zur Verfügung gestellt. Die Komponenten lassen sich je nach Bedarf gruppieren oder nach Parametern sortieren. Neben den automatisch angebotenen Sortierungen nach Device Typ, Lokation, IP- Subnetzen und hinterlegten Kontaktinformationen kann der Administrator zusätzliche Systemgruppen nach seinen Bedürfnissen konfigurieren.

Neben der tabellarischen Darstellung stellt EMC eine graphische Topologie-Darstellung über MAPs mit aktiver Linkerfassung zur Verfügung. Bei dieser Topologie-Map können Gebäudepläne oder logische Pläne als Hintergrund zur besseren Orientierung unterlegt werden.

Über die Maps kann sowohl die LAN als auch die WLAN-Infrastruktur des Netzes dargestellt werden. Der Administrator kann eigene Gebäudepläne als Bilder importieren, in denen er die Netzwerkkomponenten und WLAN-APs frei platzieren kann. Die Gerätesymbole auf den Karten sind interaktiv – ein Klick direkt auf eines der Symbole führt zur detaillierteren Ansicht aller verfügbaren Geräteinformationen. Sucht man nach einem Gerät oder Benutzer, markiert das System in der Karte die Komponente bzw. den AP, mit dem das gesuchte Element aktuell verbunden ist. EMC bietet über die Triangulation der Empfangsstärke eines Endsystems von drei APs eine noch genauere Lokalisierung. Enthalten sind auch sogenannte „Heat Maps“ für die Analyse der WLAN-Ausleuchtung.

EMC bietet umfassende Möglichkeiten zur Geräteerfassung bis hin zur automatischen Erkennung und Konfiguration von neuen aktiven Komponenten über Zero Touch Provisioning. Durch ZTP+ können neu installierte Extreme Komponenten automatisch erkannt, auf den neuesten Firmwarestand gebracht und mit einer vollständigen Konfiguration versehen werden. Dies erleichtert die Integration neuer Systeme in ein bestehendes Netzwerk und automatisiert die aufwendige Grundkonfiguration von standardisierten Parametern wie SNMP Credentials, Admin Passwörter, Management VLANs usw. Dies spart Zeit bei der Installation und Einrichtung von neuen Geräten.

Für jede aktive Komponente lassen sich auch detaillierte Ansichten aufrufen, die erweiterte Informationen über das Gerät zur Verfügung stellen und zur Konfiguration einzelner Komponenten genutzt werden können. Je nach Art des Gerätes sind Detailinformationen zu dem System selbst inklusive Power und FAN Status wie auch zu den Interfaces, Porteeinstellungen, Alarmen, VLAN's, MLAG, etc. abrufbar. Über die Detailansicht kann das Gerät auch konfiguriert werden. Neben der Konfiguration von VLAN's, oder MLAG können aus dem System heraus Scripte ausgeführt oder Konfigurationsfiles abgespeichert/aufgespielt werden. Aus den detaillierten Geräteansichten kann der Administrator auf Betriebsstatus und Auslastungsdaten zugreifen. Auch die aus Network Access Control bekannten adaptierbaren Managementsichten (Flexviews) lassen sich direkt aus der Geräteansicht von Oneview aufrufen.

Firmware/Archives

Die Inventarisierung aller Komponenten gehört heute zu den großen Herausforderungen in Unternehmen. Dies gilt nicht nur für die IT, sondern für alle Geschäftsbereiche. Mit Hilfe des Firmware und Archives Tab lassen sich Informationen über die IT-Komponenten (Switches, Router, Wireless-Controller,...) schnell und einfach katalogisieren.

Es können der Hardwaretyp und die jeweilige Seriennummer jeder IT-Komponente, die eingesetzten Firmware-Versionen, die Speicherausstattung oder aktuelle Konfigurationen ausgelesen, zentral abgelegt und verwaltet werden. Ältere Firmware-Versionen können automatisch aktualisiert werden. Konfigurationen werden regelmäßig zeitgesteuert gespeichert und archiviert. Das Management Center bietet die Möglichkeit, verschiedene Versionen von Konfigurationen einer Komponente miteinander zu vergleichen. Veränderungen oder neue Einträge werden hierbei farblich gekennzeichnet und ermöglichen so ein effektives Change Management. Es unterstützt die IT bei der Bearbeitung von RMA und der Verwaltung von Wartungsverträgen. Dies vereinfacht die Verwaltung und senkt die Betriebskosten erheblich.

Wireless

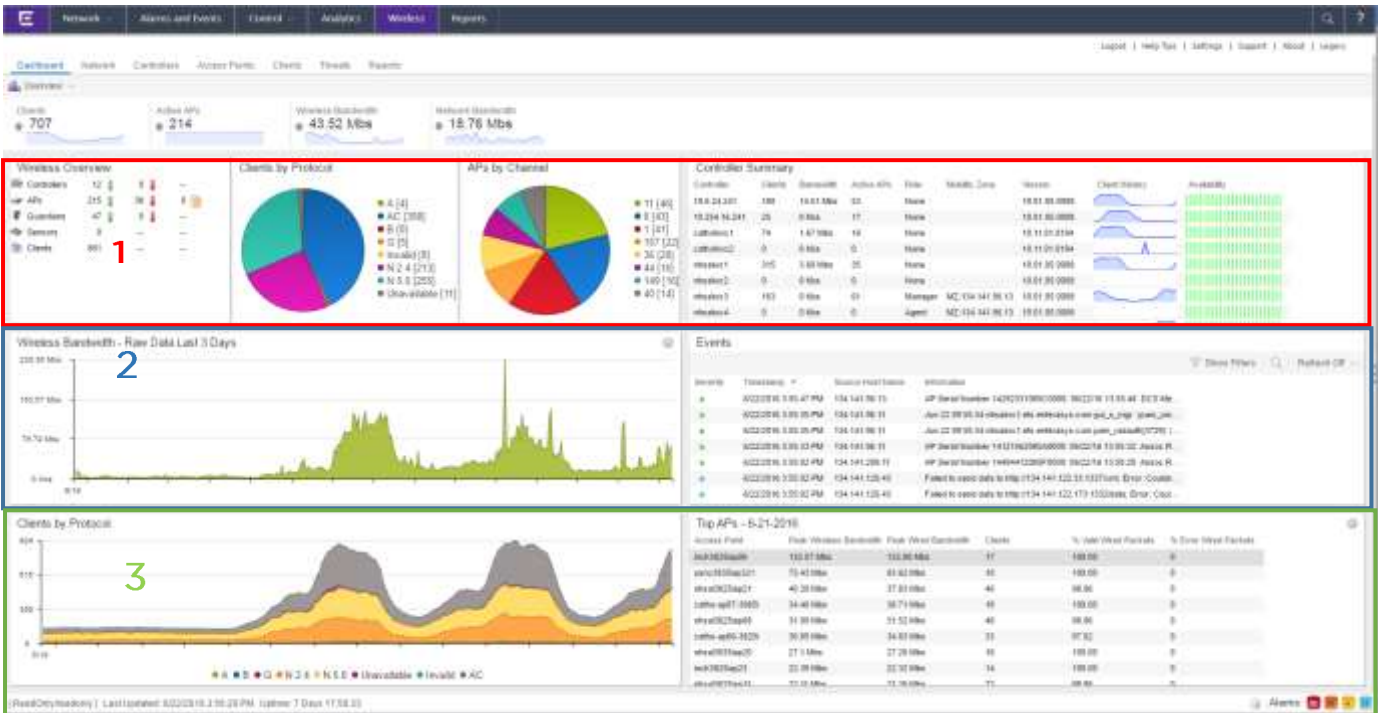
Mit dem Wireless Tab komplettiert Extreme Networks seinen Ansatz eines ganzheitlichen Netzwerkmanagements. Es lassen sich LAN und WLAN durch eine einzige Managementplattform administrieren.

Der Zugang zu allen Informationen erfolgt über den Reiter „Wireless“ und das Dashboard wird angezeigt.



Oberhalb befindet sich eine Information- / Status Zeile. Hier bekommt der Anwender einen schnellen Überblick über den Status und die Leistung der gesamten Wireless-Infrastruktur. In entsprechenden Graphen wird die Anzahl der Clients, der Access Points, sowie die genutzte Bandbreite in der WLAN und LAN Umgebung angezeigt. Im darunterliegenden Dashboard stellt sich übersichtlich die Verfügbarkeit, die Last und der Status der Controller, die jüngsten Ereignisse aus der drahtlosen Infrastruktur und Statistiken zu den am stärksten belasteten APs dar.

Dashboard:



- 1) Infrastruktur Anzeige: Überblick über aktive und installierte Controller und APs mit einem Kuchendiagramm zur Auslastung der einzelnen Endgeräte nach ihrem Verbindungsprotokoll. Auch wird die Verteilung der APs auf die einzelnen Kanäle und eine Verfügbarkeit und Auslastung aller WLAN Controller angezeigt.
- 2) Wireless Anzeige: Auslastung der WLAN Bandbreite und Übersicht der zuletzt aufgetretenen Events.
- 3) Endsystem Anzeige: Darstellung der Endsysteme pro Verbindungsprotokoll und Top APs nach Bandbreite, Endsystemen oder Paketen im Wired-Bereich (wählbare Sortierung)

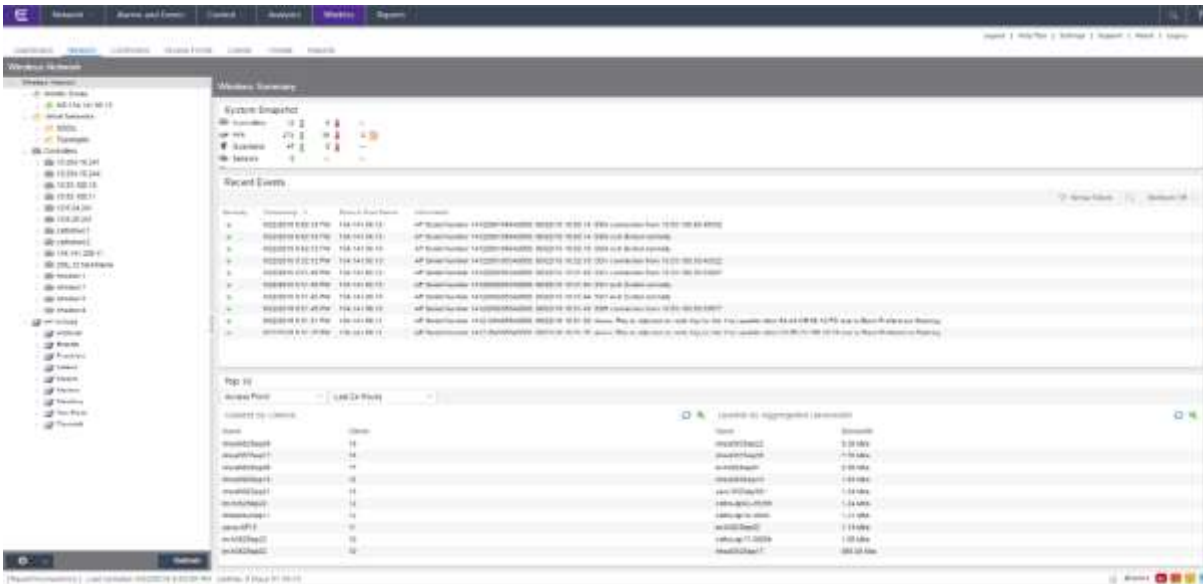
Alle Dashboard Anzeigen können im Report Designer geöffnet und angepasst werden. Somit bekommt jeder Anwender exakt das Anzeigefenster, welches ihn mit den benötigten Informationen versorgt.

Das Dashboard liefert somit die Informationen, die eine IT Abteilung in die Lage versetzt, schnell und effektiv auf Störungen zu reagieren, ohne zeitintensiv eine Fehlersuche in vielen Management-Oberflächen zu betreiben.

Natürlich steht neben der Weboberfläche weiterhin die Oberfläche des Controllers zur Verfügung. Hier können in der gewohnten Umgebung Einstellungen getroffen sowie Konfigurationen erstellt und angepasst werden.

Das Extreme Management Center ist ein umfangreiches Tool, welches IT Administratoren in die Lage versetzt, nicht reaktiv zu handeln, sondern proaktive Entscheidungen für die Zukunft des Netzwerks und die Zukunft des Unternehmens zu treffen.

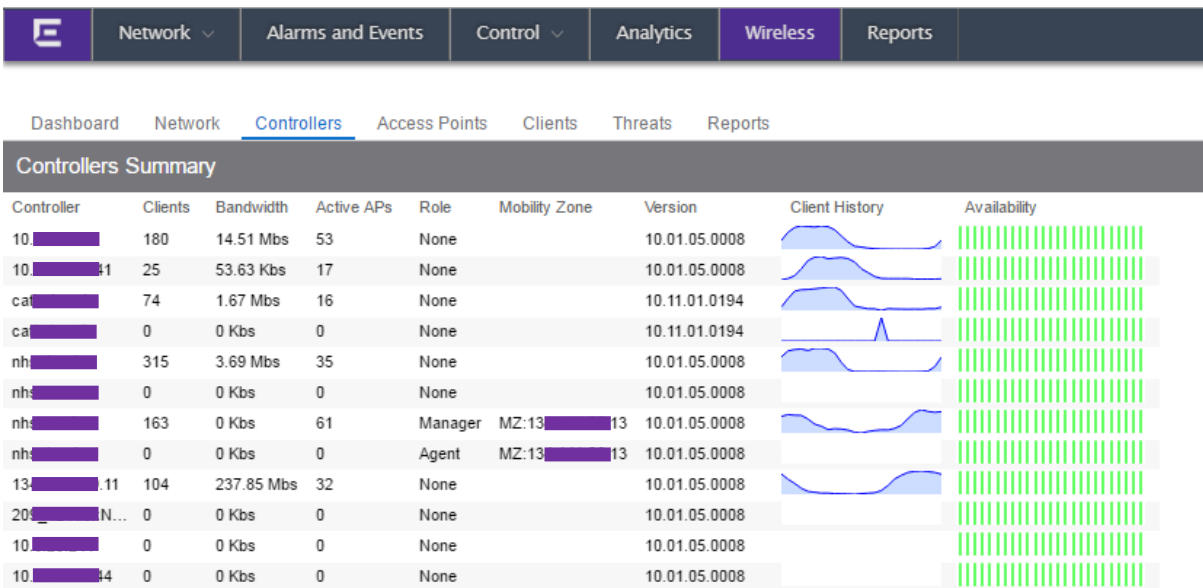
Network



Der Network Bereich informiert über Mobility Zonen, angelegte VNS und installierte Controller sowie angelegte AP Groups, welche in der Regel den Lokationen entsprechen. Hier werden Daten korreliert oder auf einzelne SSID, Controller oder Gruppen heruntergebrochen dargestellt. Dem Anwender wird eine übersichtliche Darstellung der installierten WLAN Umgebung dargestellt.

Neben der rein informativen Darstellung befinden sich links unten zwei Buttons. Ein Refresh Button, um die Anzeige zu aktualisieren, und ein Setup Button. Mittels des Setup Buttons gelangt der Anwender in die Multi-Controller Konfiguration und kann nun komfortabel Veränderungen in der Konfiguration vornehmen. Die Auswahlmenüs sind direkt mit den entsprechenden Seiten in der Konfiguration des Controllers verlinkt.

Controller



In Listenform werden alle installierten Controller dargestellt. Neben der IP und der aktuellen Auslastung (Anzahl Endsysteme und genutzte Bandbreite) sieht man auch die Anzahl der APs, die verwendete Firmware Version, eine Anzeige der Historie des

Controllers sowie eine Information der Verfügbarkeit. Dies bietet schnell einen Überblick über geleistete SLAs und zeigt im Störfall einen inaktiven Controller auf. Durch Auswahl eines Controllers öffnet sich ein neuer Reiter mit detaillierteren Informationen zu dem Controller, den APs (local und foreign im HA-Fall) und den Endsystemen.

Access Points & Clients

Entsprechend der Hierarchie steht neben dem Reiter mit den Controllern jeweils einen Reiter für die Access Points sowie für die Endsysteme im WLAN Umfeld zur Verfügung. Die Tabellen in diesen Reitern können nach den verschiedensten Kriterien sortiert und durchsucht werden. Das Auffälligste Kriterium ist der Status. Hier kann man über die Farbe (grün = verfügbar, rot = nicht verfügbar) schnell erkennen, ob seine WLAN Umgebung funktioniert oder eine Störung vorliegt. Bei den Access Points kann schnell erkannt werden, an welchen Controller diese gebunden sind und bei den Endsystemen, an welchem AP diese hängen.

Threats

Timestamp	Event Type	Threat Type	Start Time	AP Name	Additional Details
6/22/2016 4:00:12 PM	Inactive	Microwave	6/22/2016 4:00:12 PM	ukred3825ap01	frequency=2417
6/22/2016 4:00:07 PM	Inactive	Phone	6/22/2016 4:00:07 PM	ukred3825ap01	frequency=2452
6/22/2016 4:00:03 PM	Active	Phone	6/22/2016 4:00:03 PM	ukred3825ap01	frequency=2472
6/22/2016 4:00:01 PM	Active	Microwave	6/22/2016 4:00:01 PM	ukred3825ap01	frequency=2472
6/22/2016 3:59:58 PM	Inactive	Phone	6/22/2016 3:59:58 PM	ukred3825ap01	frequency=2427
6/22/2016 3:59:55 PM	Active	Constant Wave	6/22/2016 3:59:55 PM	fpap3825i-gAP6	frequency=2432
6/22/2016 3:59:54 PM	Active	Bluetooth Headset	6/22/2016 3:59:54 PM	ukred3825ap01	frequency=2432
6/22/2016 3:59:53 PM	Active	Microwave	6/22/2016 3:59:53 PM	ukred3825ap04	frequency=2442
6/22/2016 3:59:49 PM	Inactive	Bluetooth Headset	6/22/2016 3:59:49 PM	nhsa0825gap2	frequency=2437
6/22/2016 3:59:48 PM	Inactive	Microwave	6/22/2016 3:59:48 PM	ukred3825ap04	frequency=2472
6/22/2016 3:59:46 PM	Inactive	Bluetooth Headset	6/22/2016 3:59:46 PM	defa3825gap1	frequency=2467
6/22/2016 3:59:44 PM	Inactive	Microwave	6/22/2016 3:59:44 PM	ukred3825ap01	frequency=2457
6/22/2016 3:59:40 PM	Active	Bluetooth Headset	6/22/2016 3:59:40 PM	ukred3825ap04	frequency=2462
6/22/2016 3:59:40 PM	Active	Bluetooth Headset	6/22/2016 3:59:40 PM	ukred3825ap04	frequency=2442
6/22/2016 3:59:34 PM	Inactive	Phone	6/22/2016 3:59:34 PM	ukred3825ap04	frequency=2412
6/22/2016 3:59:30 PM	Inactive	Video Bridge	6/22/2016 3:59:30 PM	ukred3825ap04	frequency=2467
6/22/2016 3:59:29 PM	Active	Microwave	6/22/2016 3:59:29 PM	defa3825gap1	frequency=2442
6/22/2016 3:59:23 PM	Inactive	Phone	6/22/2016 3:59:23 PM	ukred3825ap01	frequency=2422
6/22/2016 3:59:21 PM	Active	Video Bridge	6/22/2016 3:59:21 PM	ukred3825ap10	frequency=2432
6/22/2016 3:59:20 PM	Active	Bluetooth Stereo	6/22/2016 3:59:20 PM	ukred3825ap10	frequency=2442
6/22/2016 3:59:20 PM	Active	Microwave	6/22/2016 3:59:20 PM	defa3825gap1	frequency=2447
6/22/2016 3:59:18 PM	Active	Phone	6/22/2016 3:59:18 PM	ukred3825ap04	frequency=2447
6/22/2016 3:59:16 PM	Active	Microwave	6/22/2016 3:59:16 PM	usca-AP16	frequency=2417
6/22/2016 3:59:16 PM	Active	Microwave	6/22/2016 3:59:16 PM	usca-AP18	frequency=2412
6/22/2016 3:59:12 PM	Active	Microwave	6/22/2016 3:59:12 PM	ukred3825ap01	frequency=2417
6/22/2016 3:59:10 PM	Inactive	Bluetooth Headset	6/22/2016 3:59:10 PM	ukred3825ap01	frequency=2462
6/22/2016 3:59:09 PM	Inactive	Phone	6/22/2016 3:59:09 PM	ukred3825ap01	frequency=2472

Threats sind Störungen. Störungen sind negative Einflüsse auf die WLAN Ausbreitung und die den Endsystemen zur Verfügung stehende Bandbreite. Somit haben Threats einen direkten Einfluss auf die sogenannte „User-Experience“, die Anwender-Zufriedenheit.

Die Wireless Infrastruktur und das zugehörige Management sind darauf ausgelegt, genau diese Anwender-Erfahrung zu optimieren. Daher legt Extreme Wireless einen Schwerpunkt auf schnelle Fehlerbeseitigung im Störfall und umfangreiche Analysemöglichkeiten im

Normalbetrieb, um negative Einflüsse zu identifizieren und ggf. zu umgehen.

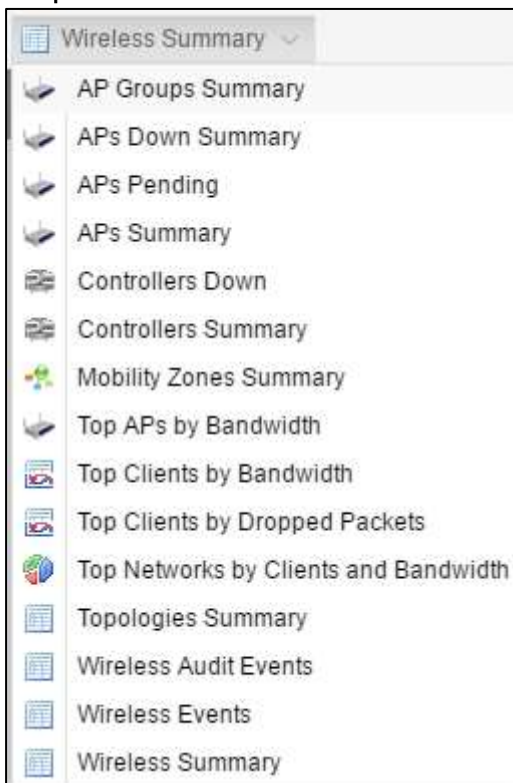
Extreme Wireless Access Points verfügen hierzu über die Funktion, im entsprechenden Kanal eine Radar Funktion auszuüben. Radar heißt aktive Suche nach Störeinflüssen. Befindet sich im direkten Umfeld ein Röntgensystem, eine Mikrowelle oder überlagernde BlueTooth Systeme? Wird das Signal durch andere Access Points negativ beeinflusst? Auch können die Access Points so konfiguriert werden, dass diese das

gesamte Frequenzband scannen. In diesem Fall senden diese jedoch keine SSID mehr aus. Ihre gesamte Empfangsleistung wird zur Analyse der Umgebung genutzt.

Jede erkannte Störung (Signaturen zur Erkennung sind auf dem AP vorgeladen) wird an den Controller gemeldet. Über diesen Tab werden alle Threats, Threat Events, Interference und Interference Events mit Zeitstempel und Typ sowie meldender AP und die beeinflusste Frequenz angezeigt.

Sollen aus diesen Threats entsprechende Aktionen abgeleitet werden, so ist dies im Controller zu definieren.

Reports



Wie auch in den anderen Bereichen des Tools bietet Extreme eine Auswahl an vorgefertigten Reports zur Analyse und Dokumentation der WLAN Umgebung.

Neben den Top N und Summary Reports findet sich hier ein Report zu APs, welche noch nicht in die Installation integriert wurden. Diese APs stehen auf „Pending“.

Viele dieser Reports bieten die Möglichkeit eines Exports in andere Systeme und Tools. Das angebotene .csv-Format eignet sich hierfür hervorragend.

Im weiteren Verlauf dieses Dokuments wird intensiver auf den Bereich Reports, Erstellung und Anpassung eingegangen.

Alarms

Beim Alarm Tab des Extreme Management Centers laufen alle Alarmer zu Geräten und Systemen, Logs und Events zusammen. Alarmer zur Netzwerkinfrastruktur können aus vielen Quellen stammen und viele Themen behandeln. Hierzu gehören SNMP-Traps, Syslog-Dateien von Switches, Benachrichtigungen des Controllers über eine Bedrohung im WLAN, Meldungen über Kommunikationsprobleme mit einem zu überwachenden Gerät, etc. Für jeden Alarm werden verschiedene Parameter (z. B. seine Kritikalität, seine Quelle, die Meldung respektive ihrem Inhalt, Uhrzeit, etc.) protokolliert.

Alarmer kann der Administrator manuell quittieren, oder das System hebt diese automatisch durch ein folgendes Event wieder auf. Die Funktion schreibt auch alle internen Events und Audit-Meldungen der Management Center Module mit und macht sie damit auswertbar.

Jeder Alarm kann eine Aktion auslösen. Diese reicht von einem einfachen Weiterleiten per Syslog, Trap oder E-Mail bis zur Informationsverbreitung über soziale Netzwerke.

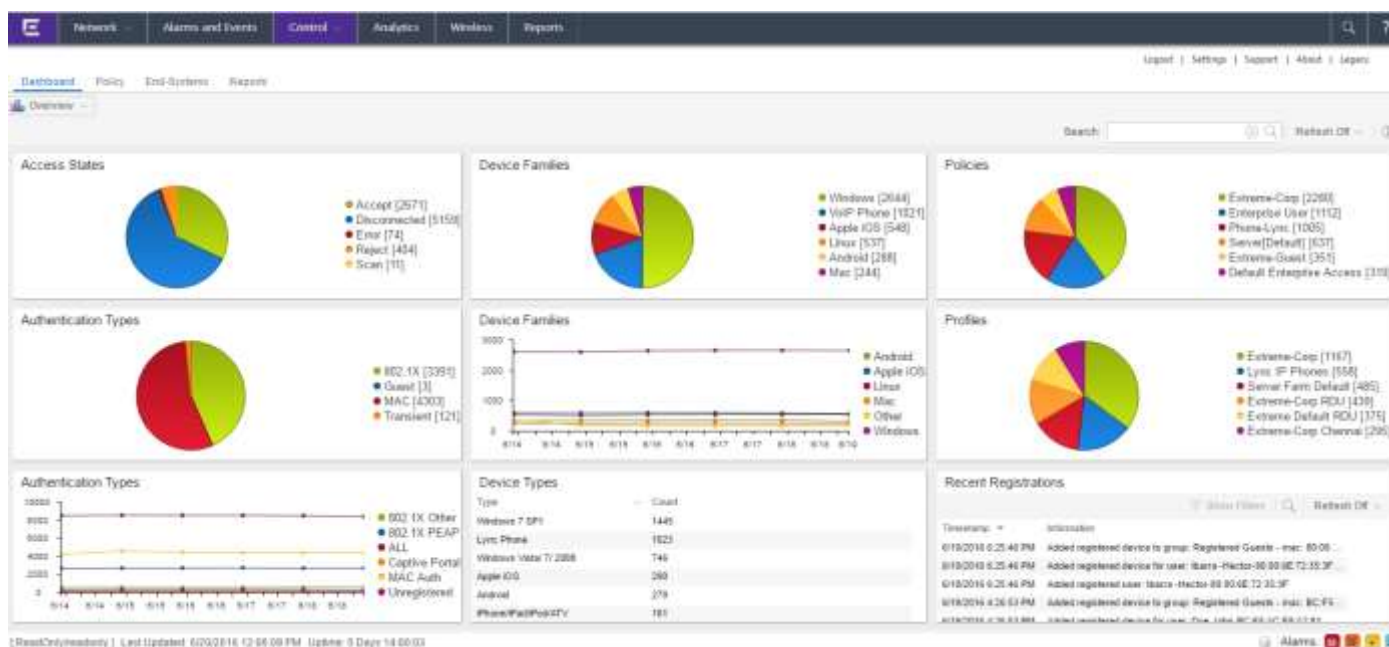
Doch auch eigens erstellte Skripte und Batchabläufe lassen sich mit Alarmparametern versorgen und automatisch starten.

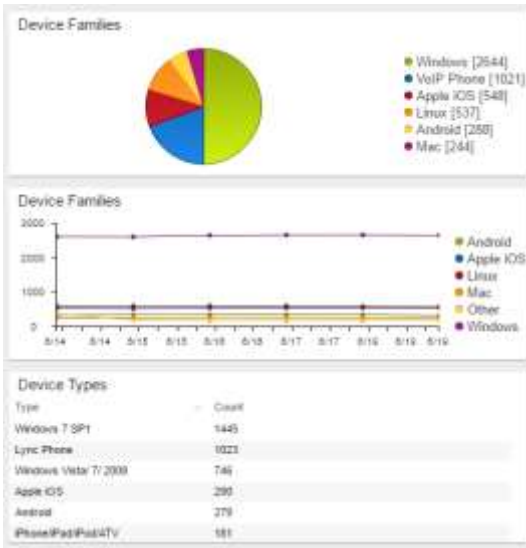
Über den Alarms Configuration Tab sind dynamische und automatisierte Reaktionen auf kritische Events möglich. Es ist nicht mehr notwendig, einen Mitarbeiter abzustellen, der ständig die IDS-Konsole überwacht und bei einem Angriff sofort reagiert. Logfile Einträge oder Netzevents (Traps) können automatisch den Admin informieren und gefährdete Systeme vom Netz nehmen.

Control

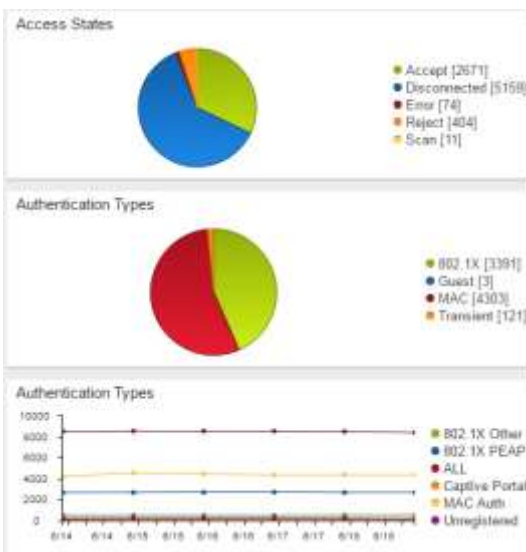
Über den Control Tab wird das Management der im Netzwerk befindlichen Endgeräte ermöglicht. Der Control tab beinhaltet sowohl die Extreme Access Lösung (NAC) als auch die Verwaltung der Extreme-eigenen Policy Lösung. Access Control enthält Informationen zu den am Netz angeschlossenen und authentisierten Endgeräten und Benutzern. Basis der Anzeige sind die bei der Authentisierung gewonnenen Daten der Access Control Lösung. Hier finden sich hier zahlreiche Daten, die tägliche Arbeiten und eine langfristige Netzplanung deutlich erleichtern. Das Datenmaterial reicht von einem globalen Überblick über alle im Netz befindlichen Gerätetypen (z. B. Windows, iPhone, Android, etc.) bis hin zu sehr detaillierten endgerätbezogenen Informationen für das Troubleshooting (z. B. MAC-Adresse, IP, angemeldeter User, Hostname, AP oder Switchport, an dem das Gerät aktuell angeschlossen ist etc.). Zu jedem Endgerät werden Anmeldedaten chronologisch archiviert. Bei eingeschaltetem Assessment werden auch diese Daten archiviert und zur Auswertung bereitgestellt.

Dashboard:





Das Dashboard liefert einen schnellen Überblick über alle Endgeräte und deren Authentisierungsstatus. Dieser Überblick hilft zu erkennen, welche Endgeräte aktiv oder inaktiv sind. Mit einem Blick kann man Geräte identifizieren, die Probleme bei der Anmeldung haben. Das Dashboard gibt auch ein besseres Bild darüber ab, wie sicher oder unsicher die Anmeldung der Endgeräte im Unternehmen ist, indem es aufzeigt, wie die einzelnen Geräte angemeldet sind (802.1x, MAC, etc.)



Der implementierte Fingerprinting Mechanismus ermöglicht eine Erkennung des Gerätetyps. Die Darstellung der Endgeräte Typen und deren Betriebssystem hilft beim Analysieren der Netzinformationen über einen anderen Ansatz. So beispielsweise beim Sortieren der Endgeräte nach Betriebssystem (Apple, Windows, Iphones, Androids, usw.) über einen Mausklick. Durch die Erkennung wird das einfache Auffinden von Systemen, die nicht in das Netz gehören, ermöglicht.



Beim Einsatz von Policies wird jedes erfasste Endgerät nach Policy und Profile sortiert dargestellt. Dies ermöglicht eine einfache Zuordnung, wie viele Endgeräte als Angestellter, Drucker, Gast, usw. angemeldet sind. Das ermöglicht eine schnelle Zuordnung von Systemen innerhalb des Firmennetzes.

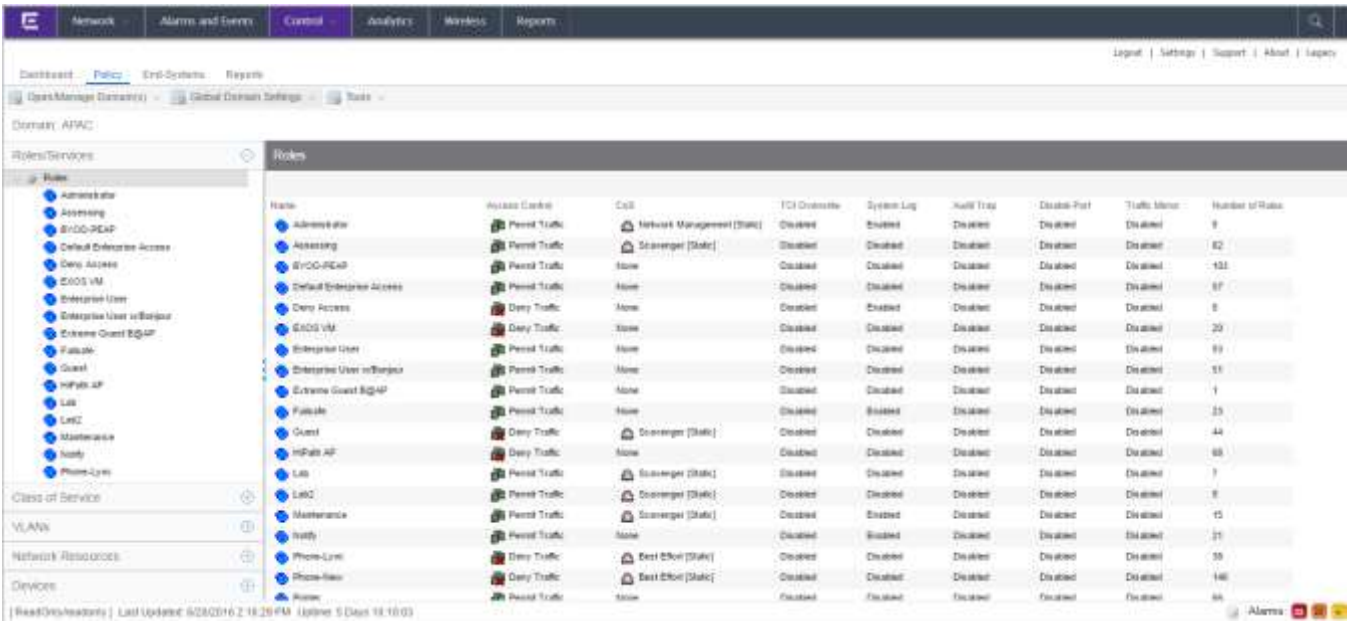
Weitere Dashboards zeigen Informationen über den Zustand der Access Control Systeme und der Assessment Lösung. Bei Implementation des Data Center Managements über Extreme Connect steht ein zusätzliches Dashboard zur Verfügung, welches Informationen über das virtuelle Data Center

zusammenfasst.

Policy

Über den Policy Tab können Anwender das Potential der Netzwerk-Policies, eines rollenbasierten Regelwerks, nutzen. Über Policies erstellt die IT-Administration gezielt vorformulierte Regeln für Netzzugang und -nutzung auch nicht-technischen Mitarbeitern in deren Arbeitsumgebung zur Verfügung. Dieses zentral konfigurierte Regelwerk kann Endgeräte/Nutzer bezogen angewandt werden. Basierend auf Nutzer, Endgerätetyp, Zeitpunkt der Anmeldung oder Ort der Anmeldung können

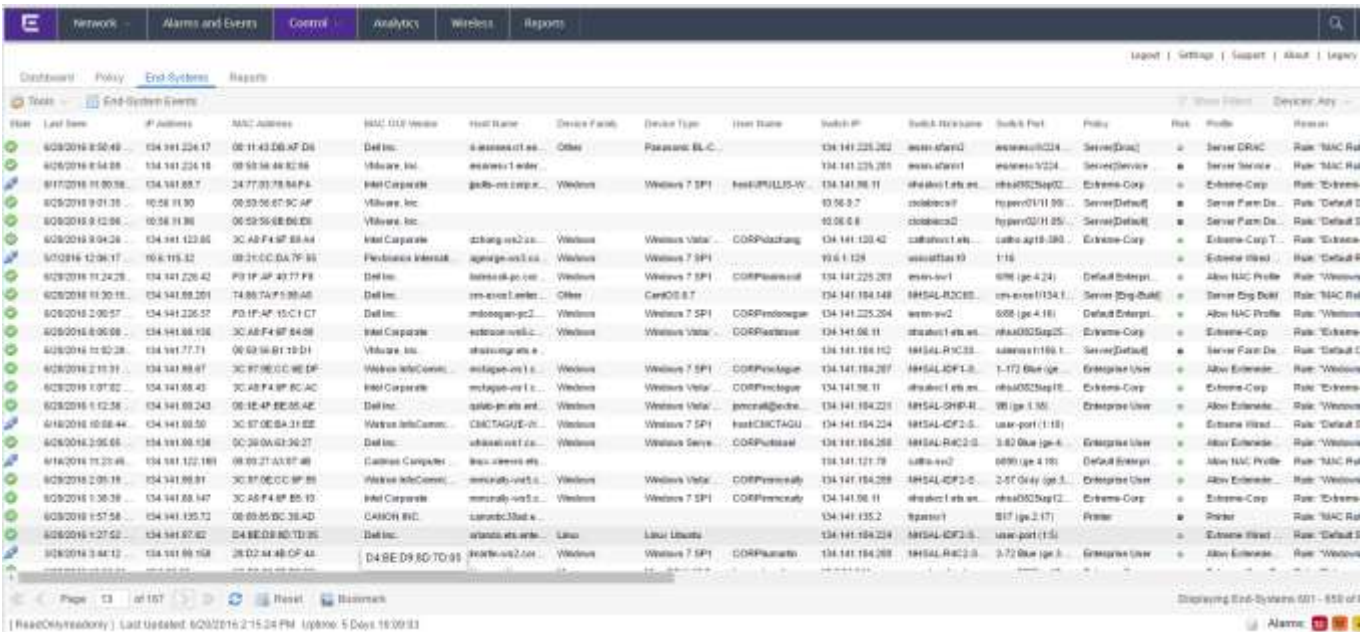
unterschiedliche Regelwerke/Policies dem Endsystem dynamisch zugeordnet oder verändert werden.



Beispielsweise kann so ein Trainer oder Lehrer über die Webschnittstelle mit einem Klick den Internet-Zugang für seine Schulungsteilnehmer ein- und ausschalten. Oder ein neu angeschaffter Drucker wird bei der Installation im Netz automatisch erkannt und mit den ihm zugeordneten Zugriffsregeln und ACLs versehen.

Da die Anwendung der Regeln und teilweise auch ihre Erstellung an geschulte Anwender delegiert werden kann, konzentrieren sich die IT-Abteilung auf wichtigere Aufgaben.

Endsystems:



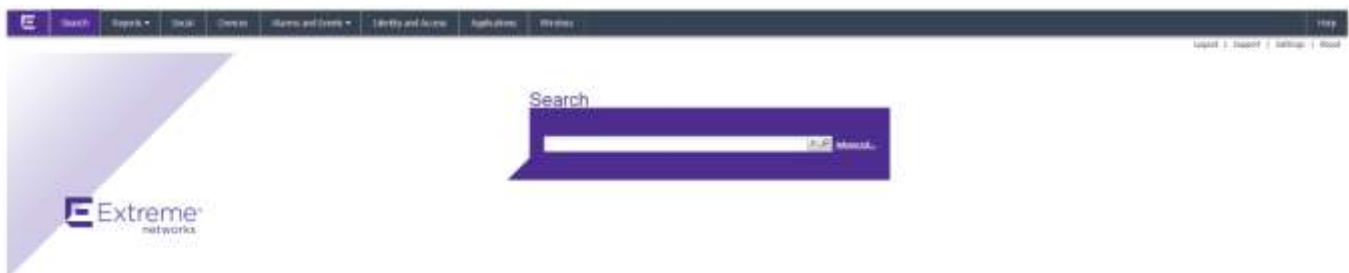
Der Endsystem Tab zeigt die Liste der über Extreme Access Control erkannten Endgeräte. Access Control ist eine komplett Standard-basierte, Multi-Vendor-Interoperable Network Access Control-Lösung für drahtgebundenes Netz, Wireless

LAN und VPN-Benutzer. Neben der eigentlichen Authentisierung / Zugangskontrolle (pre-connect), können auch im laufenden Betrieb Sicherheits-Scans durchgeführt werden (post-connect). Die Extreme Access Control Engines bzw. Virtual Appliances werden über das Extreme Management Center konfiguriert und betrieben. IT-Administratoren steht dadurch eine Lösung zur Verfügung, die gewährleistet, dass nur die richtigen Anwender Zugriff auf die richtigen Daten vom richtigen Ort und zur richtigen Zeit haben. Konfiguriert werden können unter anderem Uhrzeit, Ort, Authentifizierungsarten, Geräte- und Betriebssystemtyp sowie Endgeräte und Anwendergruppen.

Extreme Access Control kann zur Überwachung der Einhaltung von Sicherheitsrichtlinien genutzt werden. Sogenannte „Health-Checks“ bieten (eventgesteuert oder zyklisch) detaillierte Informationen über den Sicherheitszustand eines oder aller Endsysteme im gesamten Netzwerk. Anwendungsverstöße oder falsche Patchlevel werden identifiziert und können automatisiert oder durch manuellen Eingriff behoben werden. Zusätzlich werden alle Anmelungsverfahren in einer Datenbank protokolliert. Dies bietet die Möglichkeit, jederzeit eine Netzwerk-Inventarliste zu generieren. Es ist das zentrale Tool, um IT Administratoren die Kontrolle über das verwaltete Netzwerk zurückzugeben.

Search

Um Endgeräte einfach und schnell zu lokalisieren gibt es eine Suchmaske. Die Eingabemaske der Suchmaske ist einfach und benutzerfreundlich gestaltet. Ein freies Textfeld ist der Einstieg zur umfassenden Suche. Über diese kann man intuitiv nach Endgeräten (z. B. MAC-Adresse, IP, etc.), Benutzern, APs, Switches, etc. suchen. Die Suchergebnisse werden grafisch aufbereitet und dargestellt.

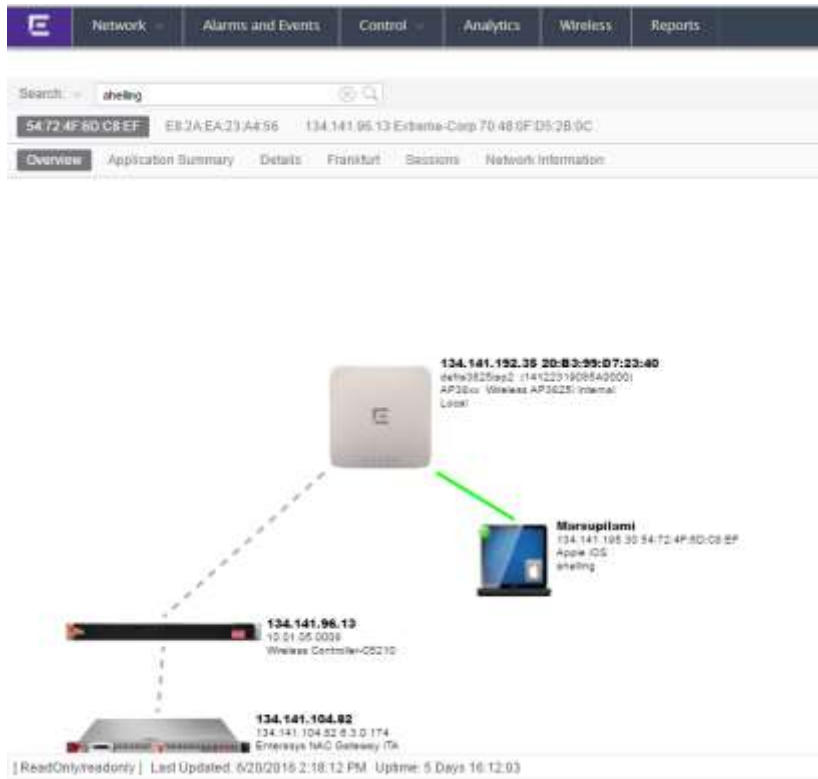


Zentrale Suchfunktion zu allen Geräten, Benutzern etc.

Die Grafiken, die als Suchergebnis entstehen, sind interaktiv und zeigen die aktuellen Informationen zu dem abgefragten Enduser/Endgerät. Mit ihnen lassen sich effizient und einfach Geräte- und Benutzerinformationen anzeigen, Netzwerkstörungen schnell lokalisieren und entsprechend zügig bearbeiten. Über die gemeinsame Datenbank der Control Lösung, Analytics und des Managements der aktiven Komponenten, ist das Extreme Management Center in der Lage, eigenständig Informationen aus verschiedenen Quellen im Kontext darzustellen. Verschiedene Graphiken zeigen die Informationen in einer leicht zu verstehenden Form da und vereinfachen die Orientierung. In Folge einige Beispiele:

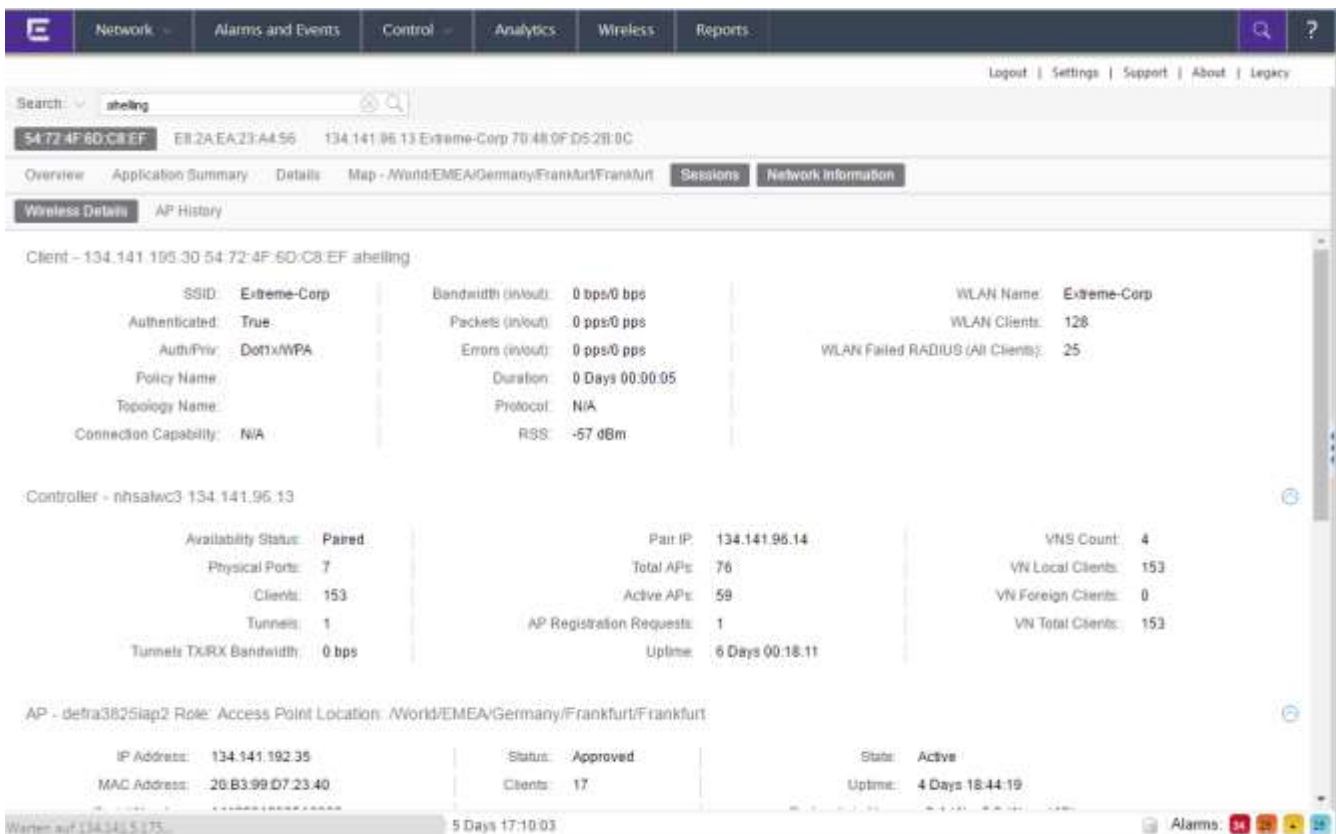
Overview

Der Overview ist eine Graphische Darstellung der Netztopology für das gesuchte Endgerät. Mit rechtecklick auf die Systeme können weitere Informationen abgerufen werden.



Suchergebnis für einen über WLAN angekoppelten Mitarbeiterlaptop

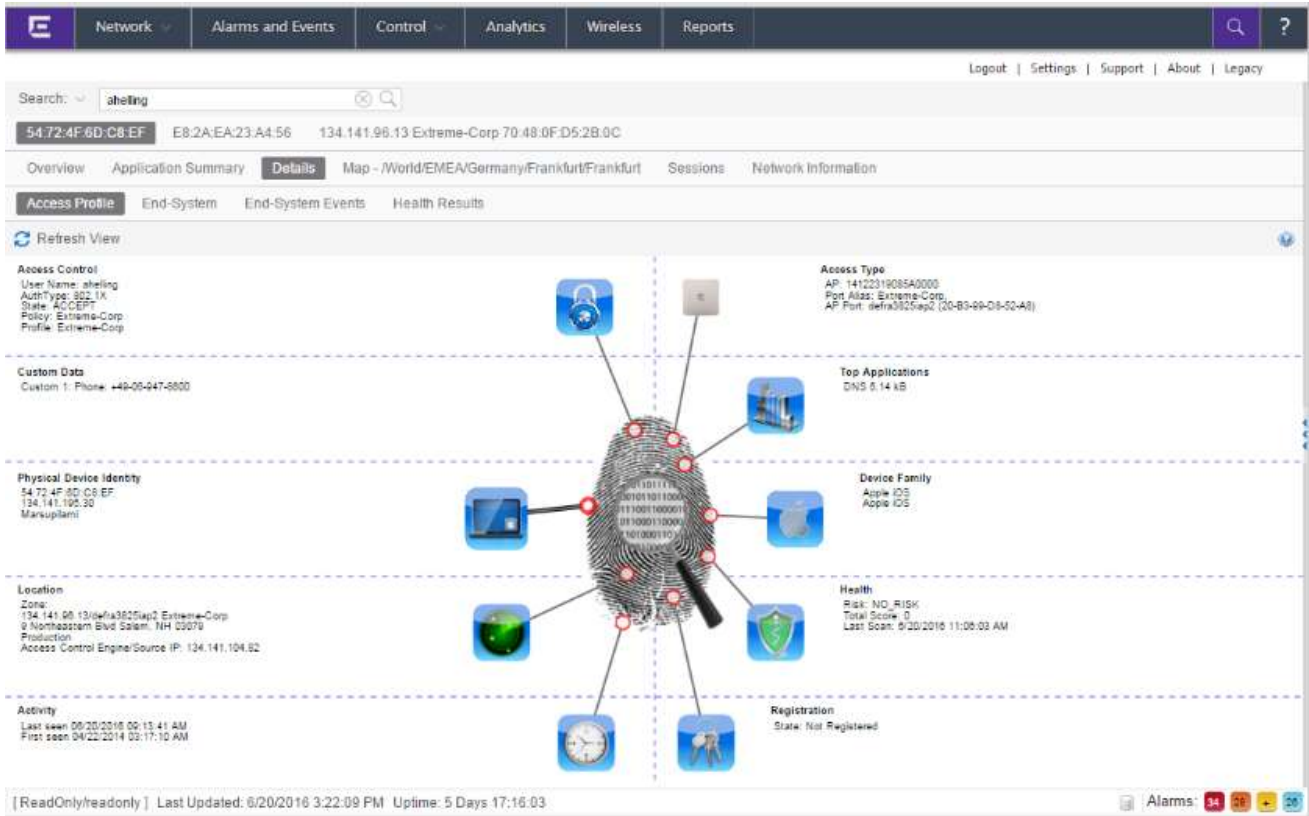
Network Details



Abhängig davon, ob das Endgerät über LAN oder WLAN angebunden ist, werden Status der Netzinfrastruktur und statistische Daten der Anbindung zur Verfügung gestellt.

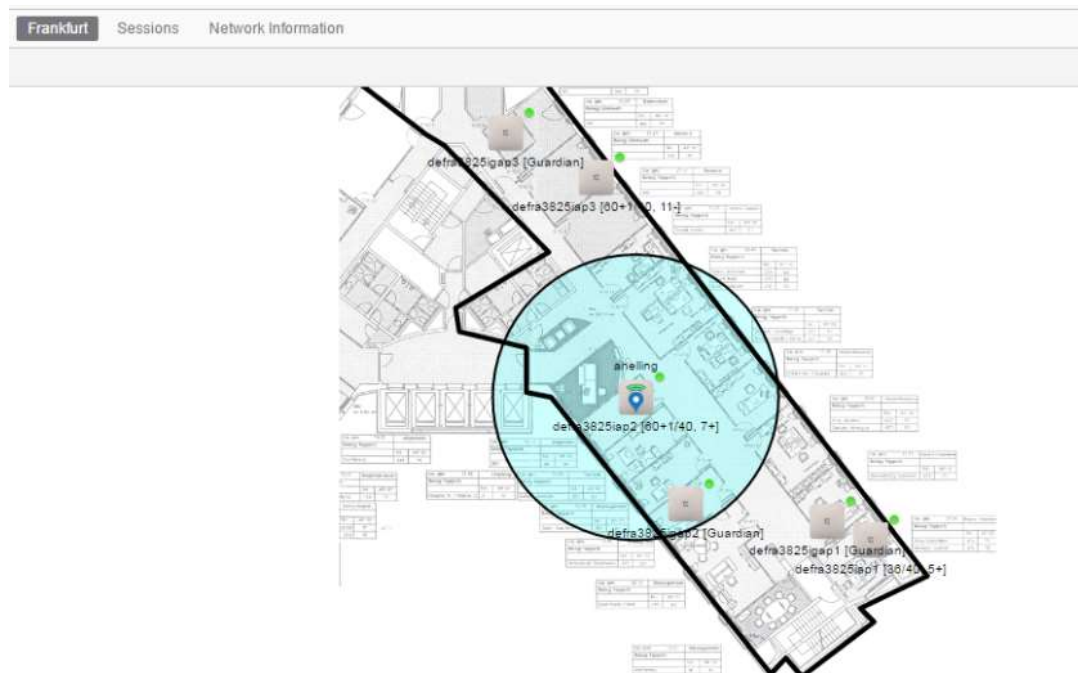
Details

Der Device Fingerprint zeigt gesammelte Details zu dem gesuchten Endgerät. Durch Mausklick in die einzelnen Bereiche werden tiefere Informationen zur Verfügung gestellt.

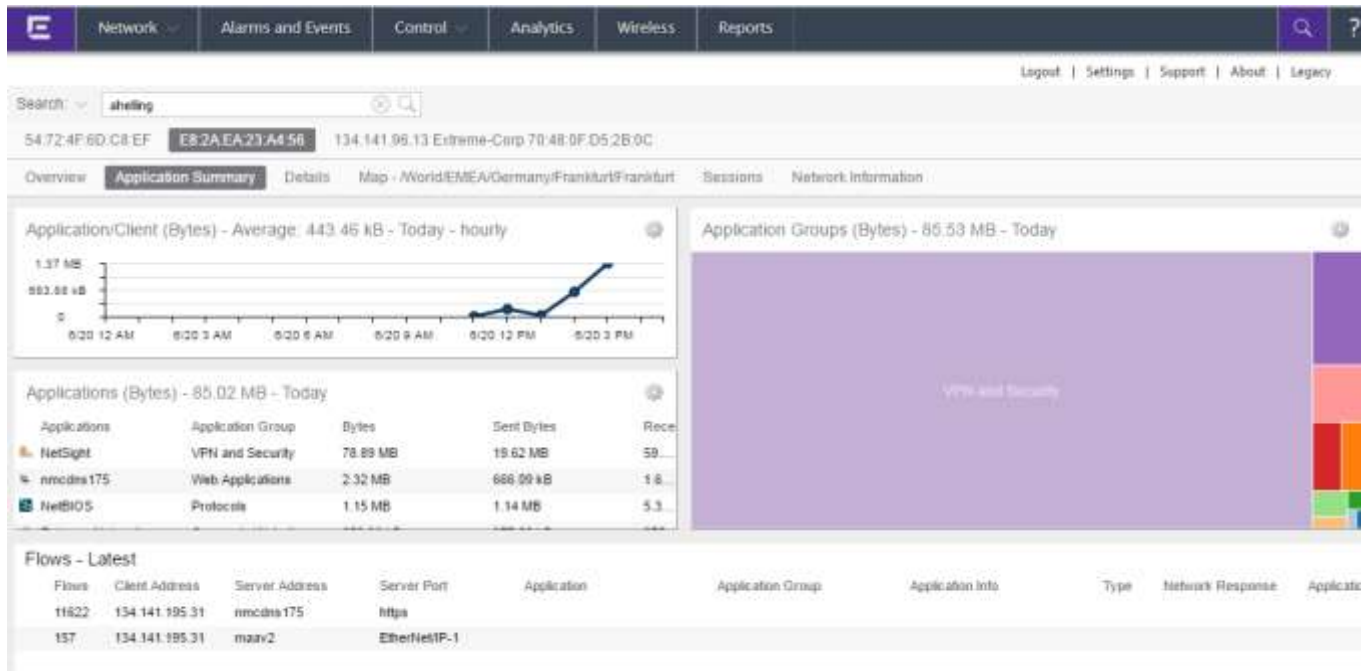


Map

Über die Map Darstellung wird das gesuchte Endgerät direkt auf den hinterlegten Karten lokalisiert und dargestellt.



Application Summary



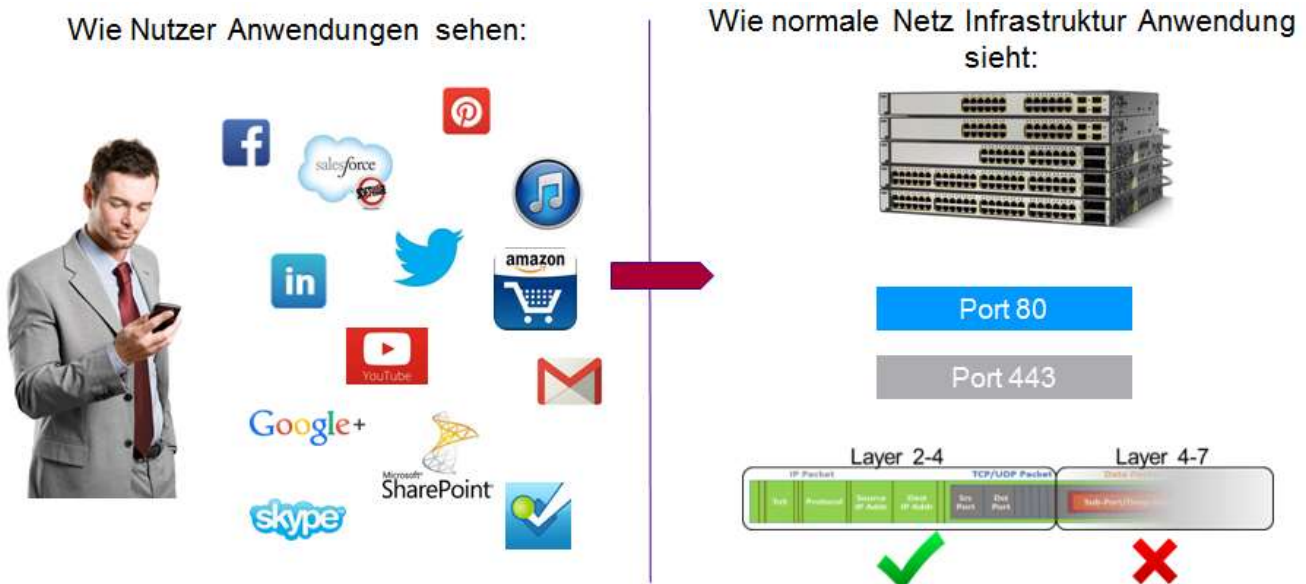
Wenn Extreme Analytics in die Lösung integriert ist, werden Endgeräte-spezifische Applikationsdaten graphisch dargestellt. Dies ermöglicht eine Sicht auf die Applikationsnutzung des ausgewählten Endgeräts

Durch die Möglichkeit des Administrators, mit wenigen Mausklicks auf die wichtigsten Informationen zu Geräten, Benutzern und Infrastruktur zugreifen zu können, steigt die Effizienz seiner Tätigkeiten und er hat mehr Zeit für Aufgaben außerhalb der täglichen Routine.

Extreme Analytics

Übersicht

Extreme Analytics (vormals Purview) ist eine netzwerkbasierende Applikationsanalyse- und Optimierungslösung, die Anwendungsdaten sammelt und analysiert, um Informationen über laufende Applikationen, Nutzerverhalten, räumliche Verteilung der Daten und im Netzwerk aktive Geräte darzustellen. Analytics nutzt die patentierte Coreflow2™ ASIC Technologie von Extreme, macht dadurch die Nutzung von Applikationen in Netzwerken sichtbar und hilft Unternehmen damit gleich in vierfacher Hinsicht: Qualitätssteigerung für Anwender, die Applikationen und Services im Netzwerk nutzen; Verstehen von Nutzerverhalten; Verbesserung der Applikations-Performance; Schutz gegen den nicht autorisierten oder schadhafte Einsatz von Applikationen.



Mithilfe von Analytics können IT-Abteilungen nun signifikante Verbesserungen bei den unternehmenskritischen technologischen Anwendungen erzielen.

In der heutigen hochvernetzten und reizüberfluteten Welt wird es immer schwieriger, Nutzerverhalten zu erfassen, das Nutzererlebnis im Bereich mobiler Kommunikation sowie Social Media zu verbessern und dabei die Zuverlässigkeit des unternehmenskritischen Netzwerks zu gewährleisten. Application Analytics löst diese komplexen Anforderungen durch die Integration von Netzwerkdaten, die einen Kontext zwischen Nutzern, Geräten, Standorten und verwendeten Applikationen herstellen. Netzwerkdaten werden erfasst und anschließend kumuliert, analysiert, gekennzeichnet und korreliert, um dann entsprechende Reports zu liefern. Somit schließt sich die Lücke zwischen Netzwerk-Management, Security und Business Analytics durch eine einheitliche, integrierte Sichtweise. Das hilft Unternehmen dabei, die Qualität für Anwender zu steigern, den wachsenden Anforderungen von Nutzern zu entsprechen und die Applikations-Performance zu steigern. Die Lösung kann in bestehenden oder neuen Netzwerken mit Switchen und/oder WLAN Access Points von Extreme Networks oder jedem anderen Anbieter eingesetzt werden. Applikationsdaten werden über das gesamte Netzwerk hinweg gesammelt, analysiert und optimiert. Dies beinhaltet Daten aus kabellosen und -gebunden Netzen sowie aus Core und Data Center.

Vorteile der Lösung im Überblick

- Business Analytics – Analyse der Nutzung von Applikationen und deren Reaktionszeiten.
- IT-Netzwerk-Management – Schnellere Problemlösung durch Erfassen der Applikations- und Netzwerk-Performance sowie Optimierung des Netzwerkdesigns für ein verbessertes Nutzererlebnis.
- Netzwerksicherheit – Identifizierung von nicht autorisierten und schadhafte Applikationen zur Einhaltung von Compliance-Richtlinien.

- In Verbindung mit der Extreme Access Control Lösung steigert Application Analytics die Effizienz der IT durch noch umfassendere Analysefunktionen, die Benutzernamen, Standort, Gerätetyp, Netzwerkrichtlinien und vieles mehr beinhalten.
- Application Analytics basiert auf der patentierten CoreFlow2™ ASIC Technologie, die den Zugriff auf Anwendungsnutzungsdaten während ihrer Übertragung im Netzwerk ermöglicht.
- Bereits bei der Einführung unterstützt Application Analytics über 13.000 Applikations-Profile. Dazu gehören die Bereiche Enterprise CRM, ERP, HCM, Storage, Internet, Collaboration, Email, Soziale Netzwerke und Gaming.

Architektur

Die Application Analytics Lösung ist aus vier Elementen aufgebaut.

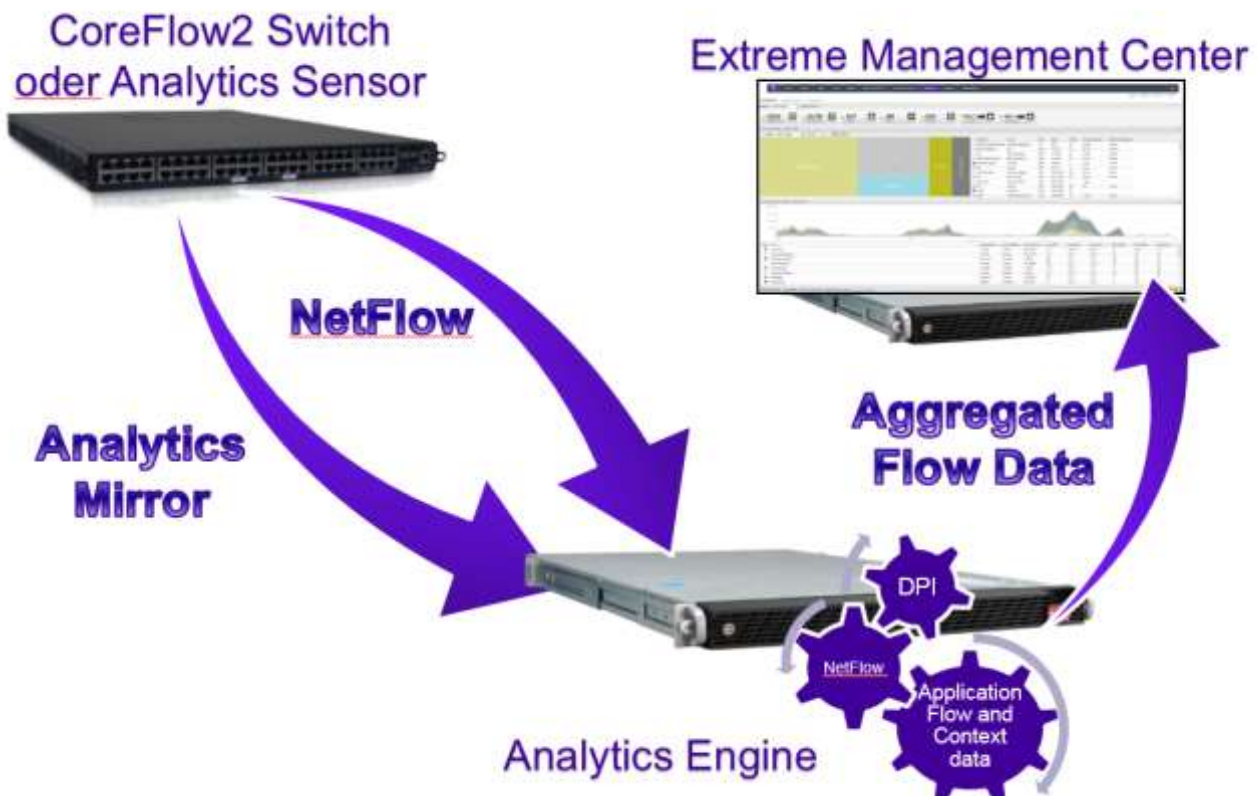
- Die **Application Analytics Engine**, die sowohl als virtuelle Maschine für VMware oder als Hardware Appliance zur Verfügung steht.
- **Management Center**
- Eine Netzwerk-Infrastruktur, die **unsampled Netflow** Daten und Traffic Mirror Funktionalität in Echtzeit liefert. Hierbei kommt der CoreFlow2 Asic in den Extreme Switchen der S-, und K-Serie sowohl als auch Network Sensoren, Extreme WLAN und bestimmte Summit Switche von Extreme zum Einsatz
- Die notwendigen **Lizenzen** um die einzelnen Elemente zu betreiben (Control Center, Flow-Lizenzen, usw.)



Die Application Analytics Engine empfängt Netflow Records und einen korrespondierenden Daten Satz aus dem Traffic Mirror für die Analyse. Mit beiden Informationssätzen korreliert die Engine die Netflow Statistiken, die ihr die Informationen über Teilnehmer des Daten-Flows und über Menge und Art der Daten liefern mit den Applikations-Informationen, die ihr über den korrespondierten Datensatz zur Verfügung gestellt werden. Diese Daten werden zusammengefasst und dem Management Center für graphische Darstellung und Speicherung der Informationen übergeben.

Durch den Einsatz der einzigartigen CoreFlow2 Architektur von Extreme (S-, K-Serie und Application Analytics Sensor), der Extreme WLAN Lösung oder X460-G2 Switche für den Access Bereich ist Application Analytics eine Lösung für Netzwerk-Infrastrukturen mit hoher Datendurchsatz-Rate im Core und Data Center Bereich, in dem sowohl die Verarbeitung von Daten aus einer Multi-Gigabit Umgebung - ohne Einsatz von kostenintensiverer Hardware - ermöglicht wird, als auch eine Entkopplung von Switch und Application Intelligence ermöglicht wird. Die CoreFlow2 Technologie liefert drei nötige Funktionen:

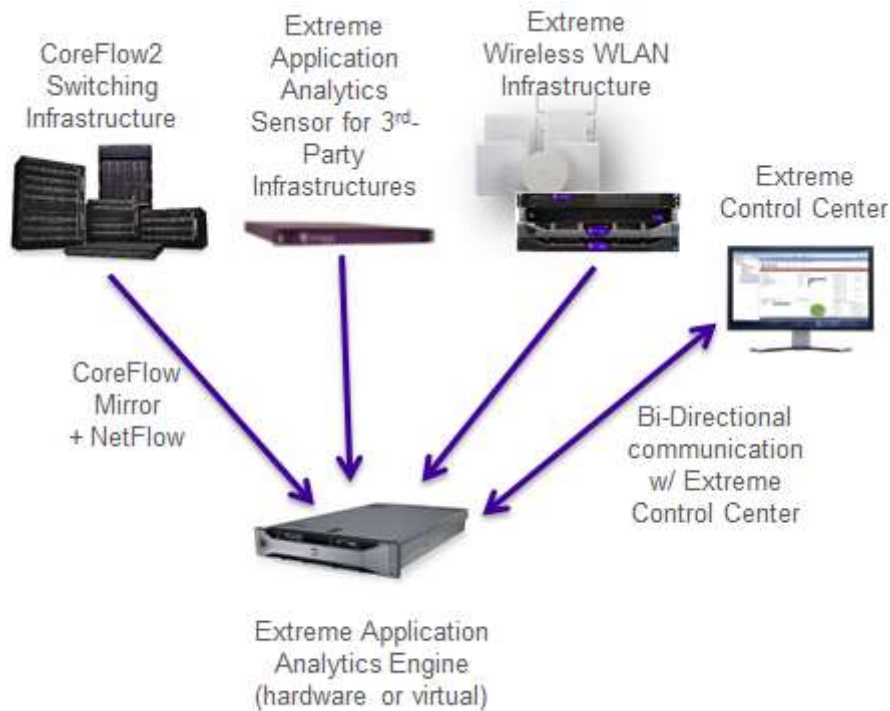
- **Unsampled Netflow:** Die CoreFlow2 Architektur erlaubt die Lieferung von unsampled Netflow Daten, unabhängig von Anzahl und Bandbreite der Datenschnittstelle und ohne Beeinträchtigung der Switch Performance des Systems. Dadurch ist eine akkurate statistische Erfassung der Verkehrsbeziehungen möglich
- **MirrorN Feature:** Das MirrorN Feature in Extreme-Geräten mit CoreFlow2 Technologie ermöglicht es, eine Policy zu erstellen, die nur die ersten 15-30 (N) Pakete einer Datenverbindung (Flow) auf einen Mirror Port spiegelt. Über diese Policy werden nur die notwendigen Informationen über eine Datenverbindung an die Application Analytics Engine gesendet. Dadurch wird die Menge der zu analysierenden Daten auf die relevanten Informationen zur Applikationsidentifizierung eingegrenzt.
- **Remote Mirroring über GRE L2 Tunneling:** Über Remote Mirroring kann eine einzelne Application Analytics Engine die Daten von mehreren Switchen oder Flow Sensoren bearbeiten, ohne direkt mit Ihnen verbunden zu sein.



Aufbau und Bestandteile der Application Analytics Lösung

Die Flow-Information und der Mirror-N kann auch über folgende Extreme Komponenten zur Verfügung gestellt werden: Extreme WLAN Lösung und Extreme X460-G2 Switch.

Extreme Analytics kann somit in verschiedensten Einsatzszenarien verwendet werden. Application Analytics hilft der IT Administration, Entscheidungen zu treffen und gibt Ihnen hilfreiche Informationen zu Situationen, denen Sie in ihrer täglichen Arbeit gegenüber stehen. Im Folgenden ein paar Beispiele, wie die Lösung eingesetzt werden kann, um häufige Probleme in Netzwerken zu lösen.



Data Center Performance Analyse

Um die optimale Auslastung der vorhandenen Netzwerk-Ressourcen zu erreichen, ist es oft sinnvoll, Anwendungen an unterschiedliche physikalische Lokationen zu verteilen. Aus Gründen der Performance oder aus Wartungsgründen müssen virtuelle Applikationsserver im Netzwerk verschoben werden. Vor diesen Aktionen ist es sinnvoll und notwendig festzustellen, wie die Anwendungen von End Usern genutzt werden und in welchen räumlichen Lokationen wie viele User auf die Anwendungen zugreifen. Zusätzlich ist es wichtig zu wissen, in welchem Zeitraum die wenigsten User auf dieser Anwendung arbeiten, um den Termin des Umzugs oder der Wartung festzulegen.

Application Analytics bietet hier die Möglichkeit, den Datenverkehr auf räumliche Verteilung und Nutzerverhalten zu analysieren und über die OneView Oberfläche des Management Centers darzustellen. Anhand der Informationen aus den einfach verständlichen Graphen lässt sich ablesen, zu welcher Zeit ein Umzug der Anwendung am wenigsten Nutzer betrifft und wo der beste Standort für die Anwendung ist.

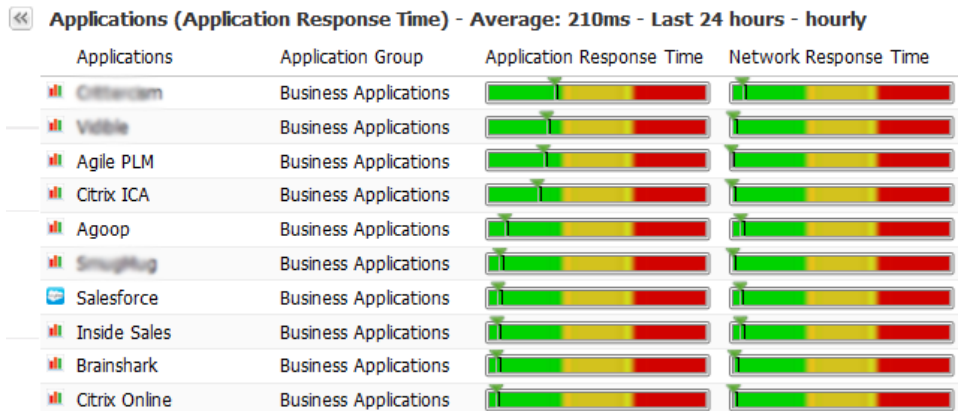


Darstellung von User pro Zeit und Applikation

Application-Response vs. Network-Response

Die meisten Fehlermeldungen von Endanwendern sind in ihren Aussagen zu diffus, um eine schnelle Problemanalyse zu ermöglichen. Eine Aussage wie „Das Netzwerk ist langsam“ lässt keine Rückschlüsse darauf zu, wo die tatsächliche Störung des Datenverkehrs zu finden ist. Für den Administrator ist es oft schwer heraus zu finden, ob das Problem am Endgerät/dem Nutzer, der Netzwerk-Infrastruktur oder der Anwendung liegt, die der End User benutzen möchte.

Application Analytics bietet hier im Zusammenspiel mit Extreme Access Control eine Anzahl von Informationen, die eine Eingrenzung und Lösung des Nutzerproblems



beschleunigen und ermöglichen. Sie kann bis auf das Nutzer-Level die Antwortzeiten einzelner Anwendungen sowohl auf Netzwerkebene, als auch auf Anwendungsebene darstellen. Es können z. B. Analysen über Netzwerk-Antwortzeiten in Relation zu Anwendungs-Antwortzeiten durchgeführt werden. Dies kann auf einer zeitlichen Basis oder auf den Nutzer spezifisch dargestellt werden.

Erkennung von schädlichen Applikationen

Neue Sicherheitsbestimmungen verlangen von einem Administrator immer umfangreichere Maßnahmen, um Anwendungen zu sperren oder den Gebrauch von nicht erlaubten Anwendungen zu erkennen. Application Analytics ermöglicht es zu analysieren, welche Anwendungen im Netzwerk aktiv sind und gegebenenfalls von



welcher Nutzergruppe diese Anwendungen eingesetzt werden. Werden Applikationen benutzt, die für spezifische Bereiche/Usergruppen nicht freigegeben sind? Sind nicht erlaubte Anwendungen im Netzwerk aktiv?

Überwachung von Anwendungs Roll-Out und Nutzung von lizenzierten Anwendungen

Application Analytics ist ein nützliches Hilfsmittel, um heraus zu finden, wie eine neue Anwendung vom Nutzer angenommen wird. Bei vielen IT-Abteilungen geht man davon aus, das ein Software Projekt abgeschlossen ist, wenn man die Anwendung jedem Nutzer zur Verfügung gestellt hat. Ob die neue Anwendung wirklich vom Endnutzer angenommen, kann nicht überprüft werden. Hier hilft Application Analytics. Man kann sehr einfach darstellen, wie viele Nutzer, wie häufig eine Anwendung nutzen und von welchen Arbeitsgruppen/Lokationen auf diese Anwendung zugegriffen wird.

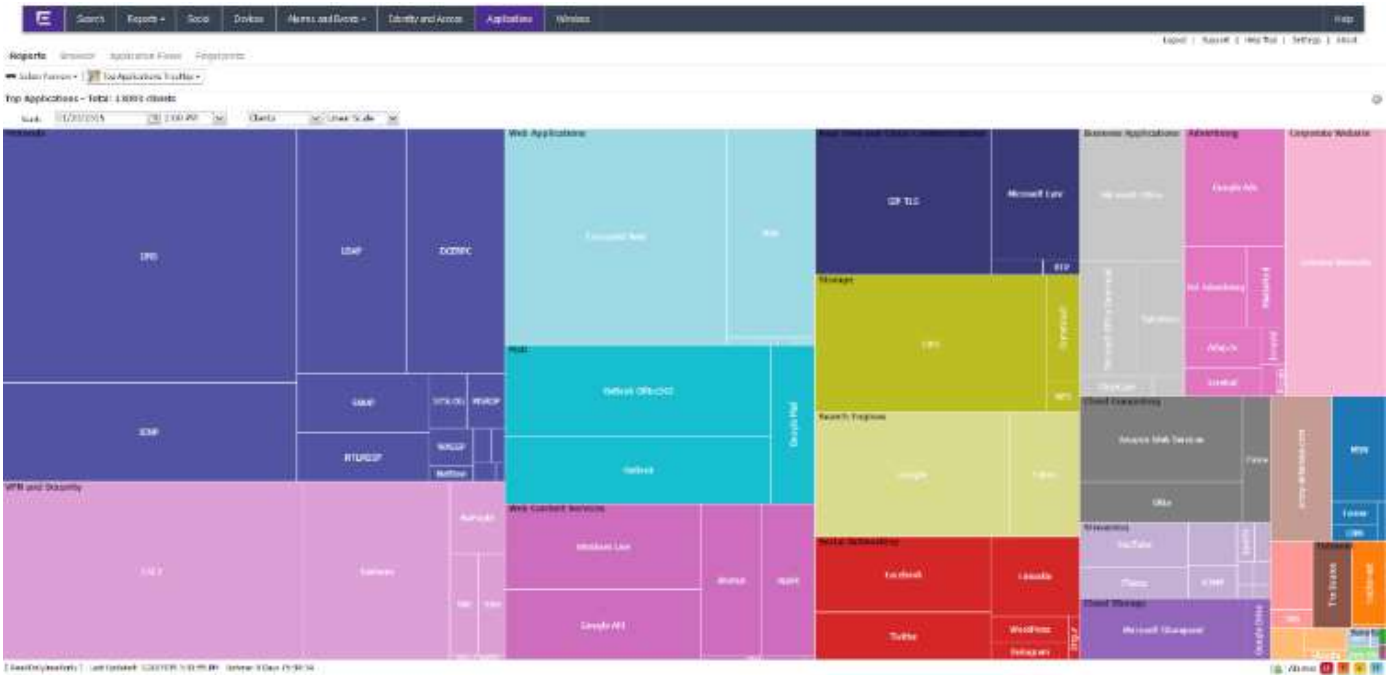
Application/Client (Flows) - 148357 flows - Last hour

Application	Client	Application Group	Flows	Outbound Flows	Inbound
ClearCase	ntcde-ws1.corp.extr...	Business Applications	51893	25942	25951
Encrypted Web	134.141.1.138	Web Applications	24208	12204	12004
Extreme Networks	134.141.168.114	Corporate Website	14255	14255	0
Microsoft SQL Server	jenap-ws.corp.extr...	Databases	8574	4287	4287
Microsoft SQL Server	elstour-ws.corp.extr...	Databases	8521	4321	4200
LDAP	134.141.20.182	Protocols	8330	4168	4162
Microsoft SQL Server	delcemo-pc.corp.ex...	Databases	8264	4132	4132
Microsoft SQL Server	chf-ws1.corp.extre...	Databases	8146	4073	4073
Microsoft SQL Server	monney-ws1.corp.e...	Databases	8132	4066	4066
nmcdrn175	noc-display.ets.ente...	Web Applications	8034	4020	4014

Zusammenfassung

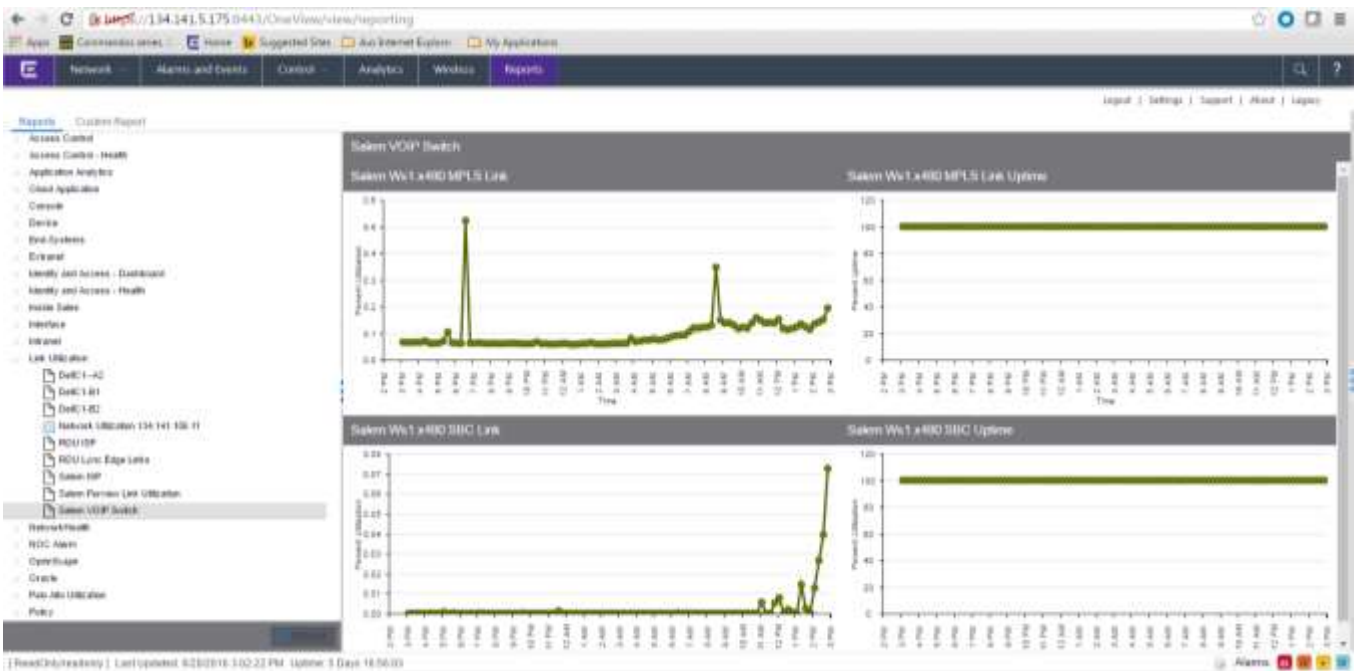
- Intuitive Dashboards und Reporting
 - Überblick aller Applikationen, Bandbreitennutzung, Clients, Flows sowie Performance des Netzwerks und der Applikationen
 - Spezifische Dashboards
- Durchgängige Beobachtung von Applikationen im gesamten Netzwerk
 - Von Edge über Data Center und Core zum Internet
- Offene & anpassbare Applikationsdaten und -profile
 - Akkurat durch Signaturen & Heuristik
 - Mehr als 13.000 Daten für mehr als 7.000 Applikationen sofort verfügbar
 - Hinzufügen von eigenen Applikationsprofilen möglich
- Detaillierte Informationen über Nutzung und Performance von Applikationen
 - pro Applikation, User, Gerätetyp, Ort, etc.
- Kontextuelle Information der Applikationen
 - Nutzer, Profil, Ort, Zeit, Gerät & mehr
- Applikation und Netzwerk Performance Tracking
- Netzwerkübergreifend

- Decodierung von Applikation – unabhängig vom Port
- Eine einzige Architektur für Access, Distribution, Core, Data Center, übergreifend
- Tbit/s Geschwindigkeiten und Skalierung bis zu Millionen von Flows ohne die Switch-Performance zu beeinträchtigen



Reports

Da Reports und Berichte über den Zustand einzelner Bereiche eines Netzwerkes von entscheidender Wichtigkeit für den Betrieb und die Pflege heutiger Datennetzwerke sind, stellt das Extreme Management Center eine umfassende Reporting Funktion zur Verfügung.



Im Reporting-Bereich bekommt man Auswertungen basierend auf Echtzeitdaten und Auswertungen der Daten der Geräte-Historie der überwachten Infrastruktur. Aus den zusammenfassenden Ansichten und Reports kann in die einzelnen Events

hineingesehen werden. Das umfassende Ad-Hoc Reporting von OneView übernimmt alle verfügbaren Parameter in die Reportauswahl. Es stehen Reports zu Switches, Interfaces, der Extreme Networks WLAN-Lösung, Access Control, Management Center Server und NetFlow zur Verfügung.

Zusätzlich können über den Report Designer eigene Reports erstellt werden und in graphische Dashboards zusammengestellt werden. Alle vorhandenen Dashboards können individualisiert und angepasst werden. Somit kann jeder Administrator die Oberflächen einfach und intuitiv anpassen, um die wichtigen Informationen jederzeit abrufbar zu haben.

Extreme Connect

Überblick

Extreme Connect ist eine Schnittstelle zur Anwendungsprogrammierung (API). Über die offene, programmierbare und zentral verwaltete API können externe Anwendungen mit dem Management Center kommunizieren und Daten austauschen. Mit der Connect API ist es möglich, die verschiedenen Geschäftsprozesse eines Unternehmens zu synchronisieren und über eine gesamtheitliche Management-Oberfläche zu verwalten.

Als Resultat erreicht man:

- **Zentralisierte Verwaltung und Kontrolle** des Netzwerks und von Systemen anderer Hersteller über ExtremeControl
- **Programmierbarkeit** der Virtualisierung und Anwendungsintegration mit Extreme Connect
- **Offene XML/SOAP-basierte API**, die über Extreme Connect bereitgestellt wird

Mit der Extreme Connect API können Unternehmen viele Systeme und Anwendungen über ExtremeManagement integrieren. Extreme Networks hat eine Reihe vordefinierter Integrationen entwickelt, die eine programmatische Kontrolle von VM, MDM, Webfilter- und Firewall-Systemen ermöglichen. Darüber hinaus besteht jederzeit die Option für kundenspezifische Integrationen. Kunden können außerdem ihre eigenen Integrationen einfach und problemlos über die offene, XML/SOAP-basierte API entwickeln.

Anwendungen

Die Extreme Connect API erleichtert die Automatisierung einer breiten Palette von Netzwerkfunktionen. Mithilfe der API können Administratoren

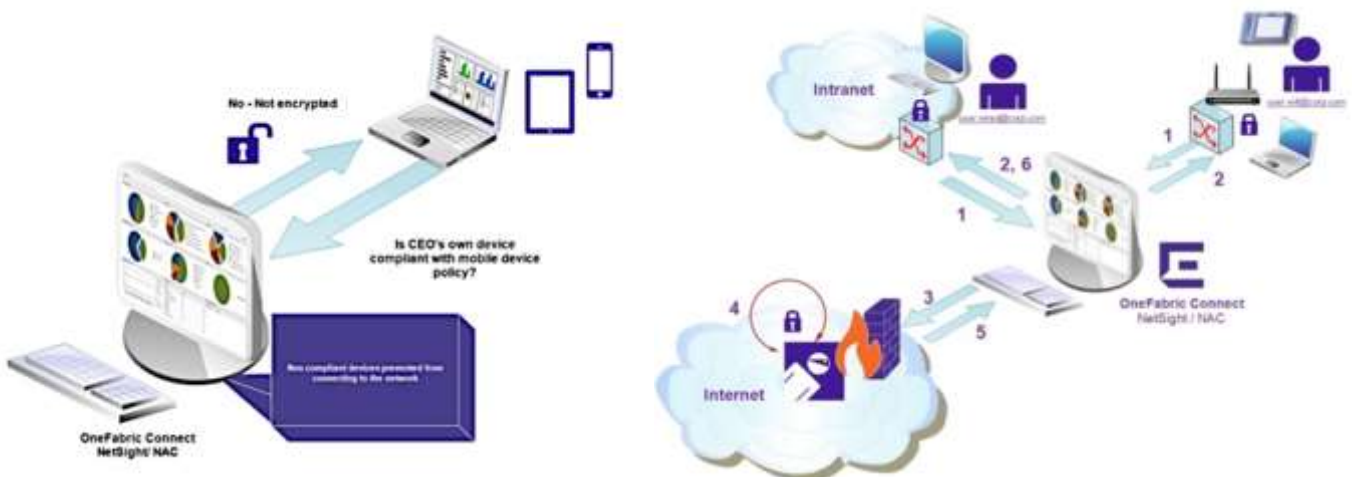
- Richtlinien für physische und virtuelle Endsysteme überall im Netzwerk festlegen, abfragen und/oder modifizieren
- Richtlinien für Nutzer im Netzwerk festlegen, erhalten und/oder modifizieren
- Richtlinien für Nutzer- und Endsystem-Anmeldungen im Netzwerk festlegen, erhalten und/oder modifizieren

- Informationen über Nutzer und Endsysteme festlegen, erhalten und/oder modifizieren, einschließlich Ort, Gerätetyp, Zeitstempel, Asset-Informationen, Integrität und Sicherheitsstatus
- eine Liste aller Netzwerkgeräte anlegen und/oder erhalten
- neue Gastnutzer im Netzwerk anlegen
- auf Berichtsdaten zugreifen

Diese Funktionen lassen sich für die Automatisierung oder Programmierung einer beliebigen Anzahl von Vorgängen in der Anwendungsdomäne nutzen.

Dazu gehören:

- **Geräteortung** – Informationen über Switch-Port- oder AP-Verbindungsunkte von allen Endsystemen
- **Bestandsverwaltung** – Inventarisierung aller ans Netz angeschlossenen Systeme auf Knopfdruck
- **Virtualisierung und Orchestrierung** – Automatisierung von Regelwerkszuweisung (QoS, VLAN, BW, Filter usw.) auf Port Basis.
- **Compliance** – Erfassung von nicht autorisierten Netzzugriffen durch Fremdgeräte (z. B. Black- und White-Listen für Endgeräte)
- **Hospitality** – Gastzugang über Wired und Wireless nach Firmenrichtlinien (Policies)



Integrationsbeispiele für die ExtremeConnect API

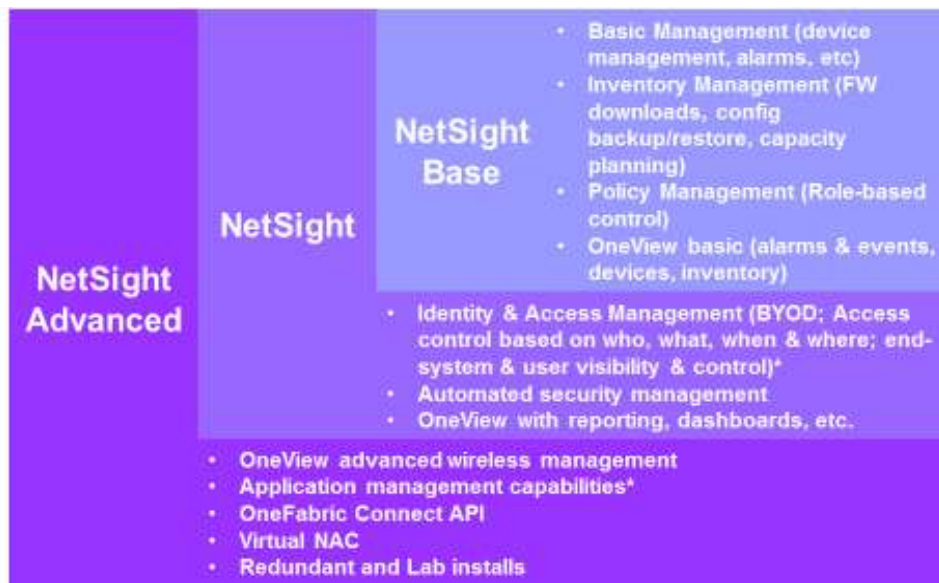
Vorteile:

- **Neue Services, Innovation und Flexibilität** – eine offene Northbound-API ermöglicht Innovation bei Technologie-/Integrationspartnern und Kunden für ein außergewöhnlich leistungsfähiges Netzwerk.
- **Erstklassige Anwendererfahrung und Skalierbarkeit** – das Netzwerk erkennt Applikationen und Flows und lässt sich an aktuelle und zukünftige Anforderungen bedarfsgerecht anpassen.

- **Einfache Handhabung** – vollständig zentralisierte Verwaltung und Kontrolle aller Geräte, Nutzer und Anwendungen über das komplette Netzwerk hinweg
- **Verbesserte Orchestrierung und Effizienz** – die Speicher-, Rechen- und Netzwerkressourcen sind komplett aufeinander abgestimmt und erlauben so die automatisierte Bereitstellung neuer Services.
- **Netzwerkbasierter Business Intelligence und Kontrolle** – erkennt nicht nur, welche Geschäftsanwendungen von wem, wo und wann genutzt werden, sondern ermöglicht auch die Optimierung und stärkere Auslastung des bestehenden Netzwerks

Lizenzierung von Extreme Management Center

ExtremeManagement (vormals NetSight) wird in drei Ausstattungsstufen angeboten:



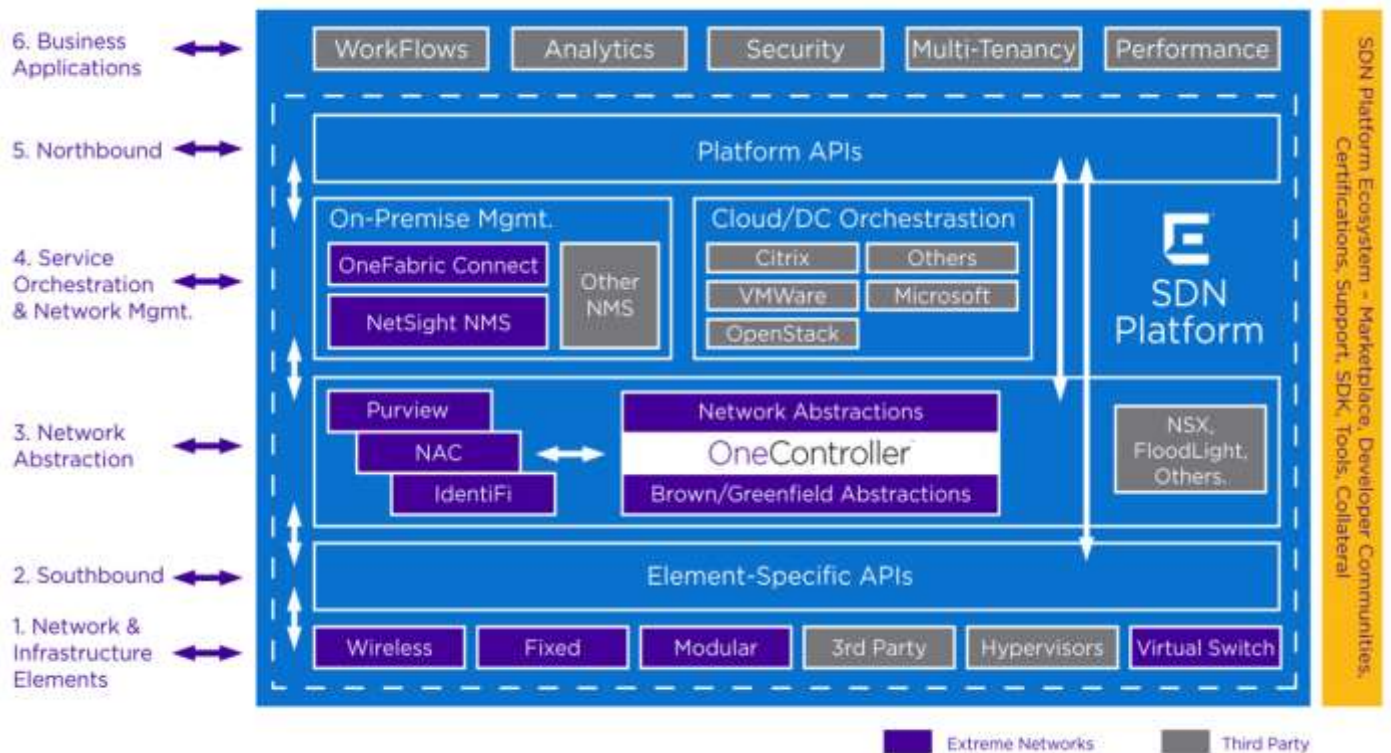
- **NMS-BASE:** Dieses Basispaket umfasst Network Control, Policy Manager (PM), Inventory Manager (IM) und einige Basisfunktionen von OneView. Maximal drei Benutzer können sich gleichzeitig am Management anmelden.
- **NMS:** Dieses Standardpaket umfasst die Module NMS-BASE plus Automated Security Manager (ASM), Access Control Manager (NAC) und OneView. Bis zu 25 Benutzer können sich gleichzeitig anmelden.
- **NMS-ADV:** Dieses umfangreichste Paket enthält alle Module des NMS-Pakets. Zusätzlich lassen sich zukünftige Application-Intelligence-Appliances und erweiterte WLAN-Features in OneView nutzen (Heat Maps, Triangulation, etc.). Außerdem kann man auf die Webservice-Schnittstelle von Management Center (SDK Connect) zugreifen. Die NMS-ADV lizenziert automatisch 500 Endsysteme für Extreme Access Control sowie eine Basiskapazität von 3000 Flows/min für Application Analytics.

	Devices	APs
NMS-xxx-5	5	50
NMS-xxx-10	10	100
NMS-xxx-25	25	250
NMS-xxx-50	50	500
NMS-xxx-100	100	1000
NMS-xxx-250	250	2500
NMS-xxx-500	500	5000
NMS-xxx-U	U	U

Die Lizenzpreise aller drei Pakete staffeln sich nach der Anzahl der verwalteten SNMP-Geräte (z. B. Switch, Wireless Controller, etc.) und APs. Für den in Network Control enthaltenen Wireless Manager braucht man keine separaten Lizenzen für den Wireless Controller. Berücksichtigt werden lediglich die vom Controller verwalteten Thin-APs.

ExtremeSDN

In Kapitel 1 haben wir uns bereits mit den Grundlagen von SDN beschäftigt. Im Folgenden soll nun die Umsetzung von Extreme Networks in Form der SDN Control Engine (vormals OneController) beschrieben werden. Das Schaubild stellt die verschiedenen Schichten der Lösung dar:



1. Netzwerkinfrastruktur

Die SDN Control Engine ist dafür konzipiert, jegliche Form von Netzwerkinfrastruktur zu betreiben, solange sie über die Unterstützung eines der vorhandenen Southbound API verfügt.

2. Southbound API

Als Southbound API können SNMP, Netconf, XML oder OpenFlow zum Einsatz kommen.

3. Netzwerk-Abstraktion

Die Abstraktionsebene wird durch einen Open Daylight Controller realisiert, welcher das OpenFlow API und ein OpenStack Plug-in zur Verfügung stellt.

4. Service Orchestrierung und Netzwerkmanagement

In der Netzwerkmanagement-Ebene kommt das Control Center mit allen seinen bekannten Schnittstellen zum Tragen.

5. Northbound API

Das Northbound API wird durch Extreme Connect realisiert.

6. Applikationen

In der Applikationsebene finden sich sämtliche Integrationen aus dem Technical Solution Partner Program

Was sind nun die Besonderheiten der SDN Control Engine?

Durch die Unterstützung mehrerer Southbound APIs ist die SDN Control Engine deutlich flexibler als alle anderen am Markt verfügbaren Controller. Das wirkt sich vor allem positiv auf den Betrieb in heterogenen Umgebungen aus. Solange die Komponenten der Infrastruktur mindestens eine der vorhandenen Schnittstellen unterstützen, können sie mit der SDN Control Engine betrieben werden. Gleichzeitig gibt es eine nahtlose Integration mit dem Management Center, Access Control und Application Analytics. Insofern steht das gesamte Funktionalitätenspektrum von Netzwerkmanagement, Policy-basiertem Netzwerkzugang und Applikationsanalyse auch der Engine zur Verfügung. Die Schnittstelle zu den Applikationen stellt das Northbound API von Extreme Connect dar. So kann die SDN Control Engine von den bereits bestehenden Applikationsintegrationen aus dem Technical Solutions Partner Program profitieren. Dadurch lässt sich ein vereinheitlichter Betrieb der Netzwerkinfrastruktur mit den verschiedenen Middleware Lösungen anderer Hersteller gewährleisten und die SDN Control Engine wird zur zentralen Steuerungsinstanz.

Im Rahmen der Mitgliedschaft in der Open Daylight Foundation wird Extreme Networks die SDN Control Engine in Zukunft weiter ausbauen. Durch Integration weiterer Applikationen wird der Mehrwert für den Netzwerk Betreiber kontinuierlich gesteigert werden.

6 ExtremeCloud



Kein Unternehmen kommt heute noch ohne eine angemessene IT-Infrastruktur aus. Die Lücke zwischen gewachsenen Plug-and-Pray Netzwerken und professionellen Strukturen mit Monitoring und zentralem Management lässt sich nun auf vernünftige Weise schliessen.

ExtremeCloud ist die einfach konzipierte, cloudbasierte Netzwerk-Management-Lösung von Extreme Networks für den Betrieb von LAN- und WLAN Komponenten. Das beginnt bereits mit der Inbetriebnahme. Im Bestellprozess werden die Komponenten einem Kundenaccount zugewiesen. Nach der Montage ist die einzige Voraussetzung, Switch oder Accesspoint mit einem Netzwerk zu verbinden. Der automatische Bezug von IP-Adresse und Gateway per DHCP ermöglicht dem Switch über einen handelsüblichen Internetrouter Kontakt mit der – in Frankfurt am Main residierenden – Cloudinstanz eine gesicherte Verbindung aufzubauen.

Über ein standardisiertes Webportal ist der Administrator nun in der Lage, seine Komponenten in allen Geschäftsstellen zu überwachen und Einstellungen vorzunehmen.

Die nach Standorten und Netzen geordnete Administration erlaubt eine regelbasierte Konfiguration. Beispielsweise wird so die Einstellung einer WLAN Instanz auf allen zugewiesenen Accesspoints angewandt. Stereotype Routineprozeduren fallen weg.

Die Durchgängigkeit der Administration reduziert Konfigurationsfehler und Ausnahmen, welche sich im Nachhinein manchmal als fatale Sicherheitslücken herausstellen.

Was genau ist ein Cloud-Managed Network?

Durch Cloud-Managed Networks werden die Vorteile der Cloud in das Unternehmensnetzwerk übertragen. Sie liefern Bedienerfreundlichkeit sowie kostengünstiges Netzwerkmanagement. Ursprünglich war dieses Netzwerkmanagement in der Cloud auf Wireless-Access Points beschränkt, wurde aber inzwischen auch auf Switches erweitert, um somit eine vollwertige Alternative zu den vor Ort („on premise“) verwalteten Netzwerken zu haben. Mit dem Netzwerkmanagement in der Cloud wird die Verwaltung und der Verkehr auf Controller-Ebene von der Cloud gehostet, der Verkehr auf Datenebene und die Geräte selbst (Access Points und Switches) verbleiben vor Ort. Es ist sehr wichtig, dass die Daten vor Ort verbleiben, denn dadurch wird den Unternehmen erlaubt, ihre hochgradige Sicherheit und die Steuerung ihrer Daten beizubehalten.

Cloud-Managed Networks basieren auf einer mandantenfähigen Architektur des in der Cloud ansässigen Controllers. Dies erlaubt die gleichzeitige Bedienung mehrerer Kunden ohne Daten- oder Management-Überlappung. Physische und virtuelle Cloud-basierte Netzwerkressourcen passen sich an die Netzwerkexpansion oder -kontraktion an, die auf der individuellen Kundenanforderung basiert. Üblicherweise werden Cloud-Lösungen als eine Art Abonnement angeboten – ein Preis-Modell für die Services, die in der Cloud gehostet werden, zusätzlich zum Kauf oder zur Miete der Geräte vor Ort. Schulen, kleine und mittelgroße Unternehmen, Kliniken, Hotels, Restaurants, Einzelhandelsläden und Firmen mit Niederlassungen und Heimbüros können große Vorteile durch die Nutzung des Netzwerkmanagements in der Cloud erlangen. Gerade kleinere und entfernte Standorte verfügen oft nicht über ausreichende IT vor Ort, um Support für die traditionellen Lösungen zu bieten.

Die Vorteile eines Cloud-Managed Network

Das Ziel eines Cloud-Managed Networks ist es, die Bereitstellung, die Verwaltung und die Steuerung der Geräte der Netzwerkinfrastruktur - so wie Wireless Access Points und Switches - sehr einfach zu machen und sowohl Betriebskosten als auch Anschaffungskosten zu reduzieren.

Es gibt viele Vorteile durch die Nutzung eines Cloud-Managed Networks für Ihr Unternehmen:

- Es werden keine WLAN-Controller vor Ort benötigt. Die Funktionalität der Steuerungs- und Verwaltungsebene wird in der Cloud abgebildet. Dies bedeutet, dass Sie keine Controller mehr an mehreren Standorten für eine Multi-Site-Installation bereitstellen müssen. Das Management ist zentralisiert, während die Access Points leicht über verschiedene Regionen verteilt werden können. Zusätzliche Controller haben oft Ihre Grenzen bezüglich der Anzahl von APs, die sie verwalten können. Ein Cloud-Managed Network beseitigt diese Einschränkungen und kann fast unbegrenzt erweitert werden.
- Einfach zu implementieren, zu nutzen und zu verwalten. Cloud-Managed Networks sind ideal für geographisch verstreute Unternehmen mit ein paar, Hunderten oder sogar Tausenden von Standorten. Die Cloud liefert einen einzigen Verwaltungspunkt, der mittels Internet-Konnektivität von überall aus verfügbar ist, unabhängig von dem Ort, an dem sich das IT-Team befindet.
- Sie brauchen sich nicht mehr über Softwareaktualisierungen zu sorgen. Mit dem Netzwerkmanagement in der Cloud werden die Updates von der Cloud an die Access Points und Switches vor Ort übertragen. Dadurch verringert sich das Risiko und die Belastung der IT.
- Das Cloud-Managed Network liefert Flexibilität und unmittelbare Skalierbarkeit. Der Access Point oder Switch kann schnell mit Änderungen versorgt werden, die in einzelnen oder Multigeräten sofort wirksam werden. Die IT kann schnell eine neue

Niederlassung oder ein entferntes Büro in das Unternehmensnetzwerk einbinden, ohne geschultes Personal dorthin schicken zu müssen. Der Access Point oder Switch wird einfach in Betrieb genommen, entdeckt automatisch und sicher seine Konfigurationsdatei in der Cloud und beginnt zu arbeiten.

- **Reduzierte Anschaffungskosten:** Mit dem Netzwerkmanagement in der Cloud wird die Notwendigkeit beseitigt, Netzwerk-Appliances für die Installation vor Ort zu kaufen, bereitzustellen, zu warten, zu sichern und zu lokalisieren, wodurch die Anschaffungskosten gesenkt werden.
- **Der Ausbau des Netzwerks folgt der Regel „Pay as you grow“.** Sie kaufen nur das, was Sie benötigen.
- **Reduzierte Betriebskosten:** Mit Hilfe von Cloud-Managed Networks braucht sich die IT nicht mehr über die Netzwerkmanagement-Plattform vor Ort, die Softwareaktualisierungen oder den Einsatz von IT-Ressourcen an entfernten Standorten für Installationen und Fehlerbehebung zu sorgen. Es gibt außerdem weniger Wartungsarbeiten und Überstunden. Die Softwareverwaltung erfolgt in der Cloud.
- **Mit einem Cloud-Managed Network brauchen Sie nicht ein IT-Experte zu sein.** Inbetriebnahme und Einsatz sind sehr leicht zu handhaben.

Empfehlungen bei der Evaluierung von Lösungen

Wie bei jedem Projekt, sollte man zunächst gut planen. Ein Cloud-Managed Network kann eine große Ersparnis für die Gesamtkosten bedeuten, jedoch in manchen Fällen auch die Gesamtkosten einer on-premise Lösung übertreffen. Stellen Sie also sicher, dass Sie richtig kalkuliert haben. Vergleichen Sie sorgfältig die erwartete Produktlebensdauer von den vor Ort verwalteten gegenüber Cloud-verwalteten Implementierungen. Die Gesamtkostenrechnung sollte die Anzahl von Cloud-Geräten, die Abonnementgebühren, die Größe und die Anforderungen Ihres Unternehmens, das verfügbare geschulte IT-Personal, die Nutzeranforderungen, die Integration in die vorhandene Infrastruktur, die Anwendungen und die Benutzer berücksichtigen. Bei größeren, geographisch verteilten Unternehmen sollte man die Vorteile der Funktionalität, wie leichte Bedienbarkeit sowie Bereitstellung und Verwaltung von Zero-Touch-Geräten ebenfalls intensiv betrachten, anstatt nur die Gesamtkosten der Geräte vor Ort zu berücksichtigen.

Eine weitere Option ist es, mit einem Cloud-Managed Network zu starten und dann im Falle einer Vergrößerung des Unternehmens in ein Vor-Ort verwaltetes Modell zu wechseln. Vergewissern Sie sich also, dass die gewählte Hardware über die Flexibilität verfügt, von einer Cloud- zu einer on-premise Lösung überzugehen, ohne dabei ausgetauscht werden zu müssen.

Zusammenfassung ExtremeCloud



- Einfache Inbetriebnahme von Wired & Wireless Komponenten
- Skalierung - Die Netzwerk Infrastruktur wächst mit den Geschäftsprozessen
- Investitionsschutz - Die Cloud Komponenten werden automatisch & zentral aktualisiert. Dies gewährleistet, daß alle Netzwerk Komponenten immer auf den neuesten Softwarestand sind.
- Zero-Touch provisioning - automatisierte Bereitstellung & Konfiguration
- Einfache Verwaltung & schnellere Problemanalyse über Standortgrenzen hinweg durch cloudbasierte Transparenz und Kontrolle.
- Adaptive Architektur zur Reduzierung der Komplexität und Optimierung der Infrastruktur
- Personalisierte Services - Flexible Definition & Konfiguration von Administratorprofilen. Dadurch ist die personalisierte Sicherheit gewährleistet.
- Einfache Web-basierende Grafik Oberfläche
- Firewall freundlich - keine spezielle Konfiguration erforderlich
- Die Kommunikation von den Netzwerkkomponenten zum Cloud Controller ist sicher (Secure Socket Layer (SSLv3))
- Die Netzwerkkomponenten in der Cloud werden Out-of-band verwaltet.
- RADIUS Dienste lassen sich zentral oder Standortbezogen anbinden
- Der Cloud Service steht redundant weltweit zur Verfügung
- Gastzugang

Extreme Cloud - Bestellinformationen für Access Points & Switches

Bestellnummer	Produktbezeichnung	Beschreibung
31012	AP3935i - FCC	Für folgende Länder frei gegeben US, Puerto Rico & Columbien - Dual band Dual Radio 802.11ac/abgn, 4x4:4 MIMO Indoor Wave 2 Access Point mit acht internen Antennen.
31013	AP3935i - ROW	Freigegeben für die EU & Rest-of-World (Landesertifizierung überprüfen) - Dual band Dual Radio 802.11ac/abgn, 4x4:4 MIMO Indoor Wave 2 Access Point mit acht internen Antennen.
31016	AP3965i - FCC	Für folgende Länder frei gegeben US, Puerto Rico & Columbien - Dual band Dual Radio 802.11ac/abgn, 4x4:4 MIMO Outdoor Wave 2 Access Point mit acht internen Antennen.
31017	AP3965i - ROW	Freigegeben für die EU & Rest-of-World (Landesertifizierung überprüfen) - Dual band Dual Radio 802.11ac/abgn, 4x4:4 MIMO Outdoor Wave 2 Access Point mit acht internen Antennen.
30912	AP3805i - FCC	Für folgende Länder frei gegeben US, Puerto Rico & Columbien - Dual band Dual Radio 802.11ac/abgn, 2x2:2 MIMO Indoor Wave 1 Access Point mit vier internen Antennen.
30913	AP3805i - ROW	Freigegeben für die EU & Rest-of-World (Landesertifizierung überprüfen) - Dual band Dual Radio 802.11ac/abgn, 2x2:2 MIMO Indoor Wave 1 Access Point mit vier internen Antennen.
16530	X440-G2-12t-10GE4	12 Port 10/100/1000BASE-T, 4 dedizierte 1GbE SFP Uplink upgradbar auf 10GbE SFP+ Ports, SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz.
16531	X440-G2-12p-10GE4	12 Port 10/100/1000BASE-T POE+ fähig, 4 dedizierte 1GbE SFP Ports upgradbar auf 10GbE SFP+ Ports, SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz.
16532	X440-G2-24t-10GE4	24 Port 10/100/1000BASE-T, 8 SFP combo Ports davon 4 dedizierte 1GbE SFP Ports + 4 dedizierte 1GbE SFP Ports upgradbar auf 10GbE SFP+ Ports, SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz.
16533	X440-G2-24p-10GE4	24 Port 10/100/1000BASE-T POE+ fähig, 8 SFP combo Ports davon 4 dedizierte 1GbE SFP Ports + 4 dedizierte 1GbE SFP Ports upgradbar auf 10GbE SFP+ Ports, SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz.
16534	X440-G2-48t-10GE4	48 Port 10/100/1000BASE-T, 8 SFP combo Ports davon 4 dedizierte 1GbE SFP Ports + 4 dedizierte 1GbE SFP Ports upgradbar auf 10GbE SFP+ Ports, (2 combo/2 non-combo), 2 1GbE BASE-T combo Ports upgradbar auf 10GbE,

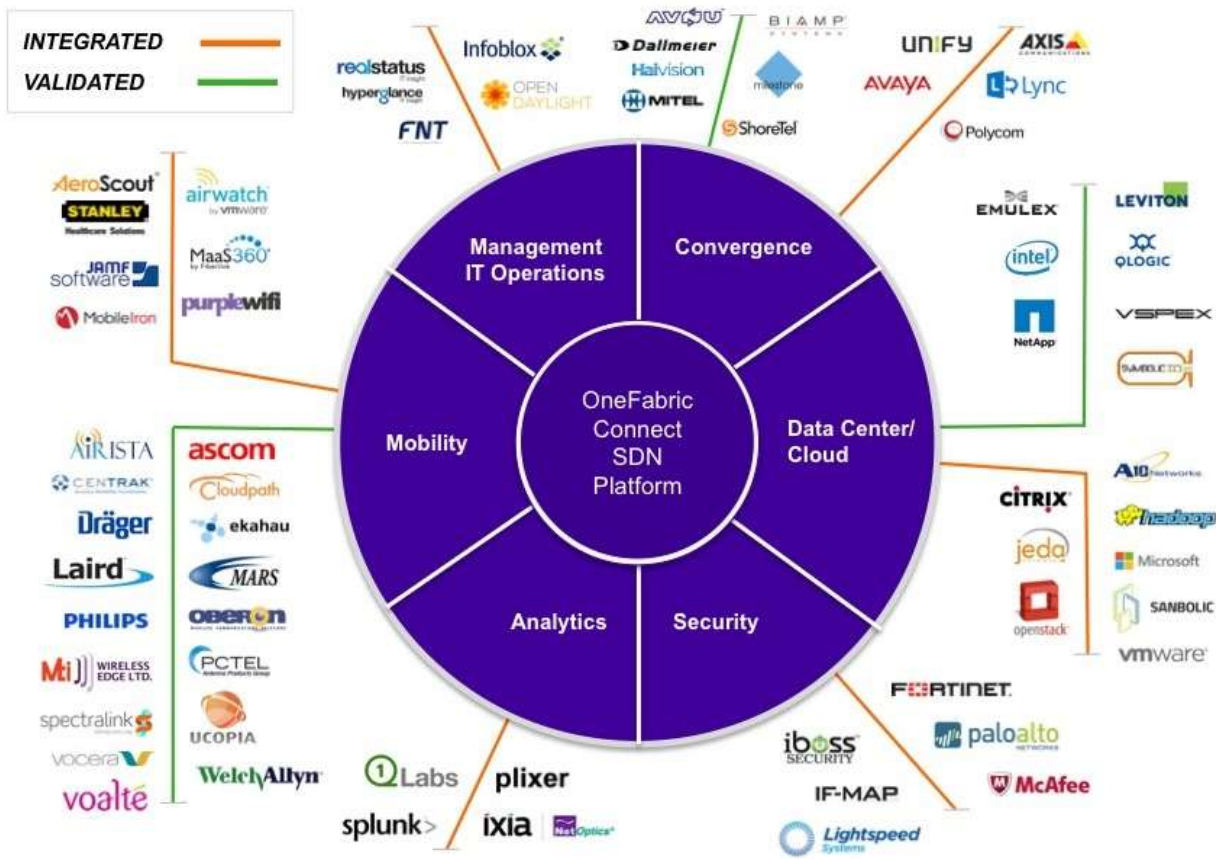
		SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz
16535	X440-G2-48p-10GE4	48 Port 10/100/1000BASE-T POE+, 8 SFP combo Ports davon 4 dedizierte 1GbE SFP Ports + 4 dedizierte 1GbE SFP Ports upgradbar auf 10GbE SFP+ Ports, (2 combo/2 non-combo), 2 1GbE BASE-T combo Ports upgradbar auf 10GbE, SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz
17401	X620-16x-Base	X620 16 100Mb/1Gb/10GBASE-X SFP+ Ports, 2 Power Supply Einschübe, 1 Lüfter Einschub, ExtremeXOS Edge Lizenz
10945	Fan Module FB	Lüfter für X620-16x, Front to Back airflow
10946	Fan Module BF	Lüfter für X620-16x, Back to Front airflow
10930A	300W AC PSU XT	300W AC 230V Netzteil für X620-16x, Front to Back airflow
10943	300W AC PSU BF	300W AC 230V Netzteil für X620-16x, Back to Front airflow
10933	300W +24V/-48V DC PSU	300W DC 48V Netzteil für X620-16x, Front to Back airflow
10944	300W DC PSU BF	300W DC 48V Netzteil für X620-16x, Back to Front airflow

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

<http://learn.extremenetworks.com/rs/641-VMV-602/images/ExtremeCloud-DS.pdf>

7 Technology Solution Partner Program

Extreme Networks kooperiert mit weltweit führenden Technologie-Anbietern, um innovative Lösungen auf den Markt zu bringen, die die realen Probleme für zukunftsorientierte IT-Organisationen lösen. Das Extreme Networks Technology Solution Partner (TSP)-Programm basiert auf der Extreme Networks SDN-Plattform und bietet ein offenes, standardbasiertes Umfeld aus verschiedenen Anbietern, das die Einführung neuer und einzigartiger Funktionen von marktführenden Technologieanbietern vereinfacht.



EXTREME NETWORKS - TECHNOLOGY SOLUTION PARTNERS

Im Rahmen des Technology Solution-Partnerprogramms können Extreme Networks-Channelpartner außerdem strategische Kundenbeziehungen aufbauen, indem sie differenzierte Lösungen bereitstellen und ihre Kunden dabei unterstützen, eine höhere Anwendungs- und Netzwerkperformance zu erzielen, Kosten zu reduzieren und Prozesse zu optimieren.

Im folgenden Abschnitt wird eine Auswahl der gemeinsam unterstützten Lösungen erläutert.

Analytik-Partner

IXIA

IXIA bietet Netzwerktransparenz und Sicherheitslösungen, die für Unternehmen und Service Provider eine einzelne Ressource darstellen, um sich mit allen Anforderungen an Transparenz für Anwendungen und Netzwerken befassen zu können. Die Integration in die Extreme Application Analytics -Anwendung ermöglicht eine netzwerkgestützte Anwendungsanalyse und -optimierung, die den jeweiligen Kontext mit einbezieht – d. h. Anwender, Geräte, Standorte und Applikationen – und bisher ungekannte Einsichten in die Performance bereitstellt.

Nexthink

Die Extreme Networks Integration mit der Nexthink End-user IT Analytics Plattform liefert Visibilität in alle Facetten einer IT-Umgebung, inclusive User, Geräte, Elemente der Infrastruktur, Applikationen und vieles mehr. Gemeinsam ermöglichen die umfassenden Analytics-Tools von Extreme und Nexthink der IT, ihre Ressourcenzuordnung zu optimieren und tiefe Einblicke in aussagekräftige Nutzungs- und Performancemuster zu bekommen.

Plixer International

Das NetFlow-Analysetool Scrutinizer von Plixer International Inc. ist in das Extreme Management Center integriert und unterstützt BYOD-Installationen zur Erhöhung der Transparenz und Kontrolle von verbundenen Geräten. Im Rahmen der Überprüfung von Sicherheitsrichtlinien von Endknoten vor deren Zulassung sowie der Richtliniendurchsetzung nach der Zulassung gibt Extreme Access Control die Anmeldeinformationen von Anwendern an Scrutinizer weiter, um detaillierte Geräteinformationen für IT-Administratoren bereitzustellen.

Qlabs

Die Extreme Networks-Integration mit der IBM QRadar Security Intelligence Platform bietet Netzwerksicherheit durch flowbasierte Technologien, um interne oder externe Bedrohungen unabhängig vom Standort oder der Art des Zugriffs zu identifizieren, ins Visier zu nehmen und zu beseitigen. Die jeweiligen Stärken der beiden Organisationen bei der signatur- und verhaltensbasierten Erkennung bieten Unternehmen eine detaillierte Netzwerkansicht, identifizieren den Ursprung eines Angriffs und stellen leistungsfähige Lösungen bereit, die Bedrohungen isolieren und eliminieren, bevor Geschäftsaktivitäten davon betroffen sind.

Splunk

Die Integration von Extreme Management Center mit Splunk liefert Ereignismeldungen an den Splunk-Datenkollektor aus, u. a. mit Details zu Endgeräten und granularen Statistiken mit dem Schwerpunkt auf Identity and Access Control-Services und Netzwerknutzung. Außerdem stellt die Extreme EXOS-App für Splunk Informationen über Netzwerkswitches unter dem EXOS Network Operating System bereit; Administratoren können auf diese Weise Möglichkeiten zur Optimierung der

Netzwerkleistung schnell erkennen, da Protokollanalysen einfacher durchzuführen sind und weniger Zeit für die manuelle Analyse von Switchprotokollen zur Rekonstruktion von Netzwerkereignissen aufgewendet werden muss. Die erstellten Analysen können anschließend exportiert und beispielsweise an Netzwerkarchitekten, den technischen Support sowie an IT-Manager weitergegeben werden.

Management-Partner

FNT

Durch die FNT Command-Integration in Extreme Connect können Organisationen die Unterstützung, Transparenz und Steuerung von Netzwerken verbessern. Extreme Management Center importiert aus FNT Command automatisch Infrastrukturdaten darüber, welcher aktive Switch-Port mit welchem passiven Steckfeld verbunden ist, sowie über seinen physischen Standort (Gebäude, Etage, Raum, Steckfeldnummer usw.). Das Management Center pflegt diese Daten anschließend für jedes verwaltete Endgerät ein, sodass sie einfach abzurufen und zu durchsuchen sind, und ermöglicht somit einen standortbasierten Support für jedes Gerät im Netzwerk sowie eine vereinfachte Fehlerbehebung bei Netzwerkproblemen.

IF-MAP

Die Integration von Extreme Management Center-Standortinformationen mit InfoBlox IF-MAP Server stellt eine elegante Lösung dar, die physische Zugriffskontrollen und Netzwerkauthentifizierung miteinander kombiniert. Extreme Management Center verwendet Informationen aus InfoBlox, um das Netzwerkmanagement und Reporting zu optimieren, indem SCCM-verwaltete Geräte wie Kartenlesegeräte und Tastaturen bzw. Tastenfelder für die physische Zugriffskontrolle automatisch erkannt werden, entsprechende Konnektivitäts- und Sicherheitsprofile zugewiesen werden und Administratoren ermöglicht wird, auf Extreme Networks OneView-Berichte zuzugreifen und detaillierte Netzwerkdaten über alle SCCM-verwalteten Geräte zu erhalten. Diese Integration erhöht die Sicherheit, Überschaubarkeit und Performance von vernetzten Ressourcen, Endgeräten und Anwendungen.

Real Status Hypergance

Real Status Hypergance ist die erste IT-Modellierungs- und Visualisierungslösung, die umfangreiche 3D-Ansichten der gesamten End-to-End Infrastructure liefert und somit den IT-Abteilungen bei der Fehlersuche, -behebung und -prävention hilft. Hypergance verbindet sich über die OpenStack API in OpenStack Umgebungen und erstellt eine Topologie basierend aus den Daten. Desweiteren werden Router und Netzwerke hinzugefügt und dynamisch angepasst, wodurch die gesamte OpenStack Umgebung in einer einzigen Ansicht dargestellt wird.

OpenDaylight

OpenDaylight ist ein durch die Community entwickeltes und von der Netzwerkbranche unterstütztes Framework für eine schnellere Übernahme und Förderung von Innovationen, die Reduzierung von Risiken und einen transparenteren Ansatz für

Software-Defined Networking. Extreme Networks ist Mitglied des OpenDaylight Projects, einer durch die Community entwickelten und unterstützten Open-Source-Plattform mit dem Ziel, die Entwicklung von Software-Defined Networking (SDN) und der Network Functions Virtualization (NFV) voranzutreiben und der Branche eine quelloffene, gemeinsame Plattform für SDN und NFV zu bieten.

Convergence-Partner

Microsoft Skype for Business

Die Integration von Microsoft Skype for Business durch Extreme umfasst die Wired-, Wireless- und SDN-Zertifizierung, Lync-Konnektivitätsanalysen aus der Application Analytics Engine und die End-to-End-QoS für Lync-Video- und -Audioanwendungen.

AXIS

Extreme Networks integriert Ethernet-Switches für IP-basierte Netzwerk-Videolösungen von Axis Communications; dazu gehören IP-Kameras, Videomanagementsysteme (VMS) und Videoencoder. Die gemeinsame Lösung senkt die Kosten für Videoüberwachungsnetzwerke durch einfachere Installationsvorgänge, einen vereinfachten Support und eine optimierte Kommunikation mit weit entfernten Endknoten. Darüber hinaus können Netzwerkadministratoren Abweichungen der Bitrate einzelner Videostreams oder Standbilder unmittelbar identifizieren und die administrative Steuerung für das IT- und Sicherheitspersonal innerhalb desselben Switches voneinander trennen.

Avaya

Extreme Networks stellt Avaya-Umgebungen automatisierte Tools zur Verwaltung ihrer IP-Kommunikation zur Verfügung. Unsere belastbaren Enterprise und Metro-Area Ethernet Netzwerke bieten Avaya-Kunden eine offene Alternative zu proprietären Netzwerken und somit eine Verlängerung der Lebensdauer ihrer Infrastruktur-Investitionen.

AVnu

AVnu-zertifizierte AVB Ethernet-Switches von Extreme Networks liefern Video- und Audioinhalte in professioneller Qualität über Ethernet-Netzwerke aus und ermöglichen Rundfunkanstalten die Einrichtung von effizienteren und kostengünstigeren Workflows für Studio- und Liveproduktionen. Stackbare Switches der Extreme Networks X440-Serie sind die ersten Ethernet-Switches mit vollständiger AVnu-Zertifizierung und stellen für die AVnu Alliance einen großen Schritt auf dem Weg zu ihrem Ziel dar, das Angebot professioneller Audio-/Videoinhalte weiterzuentwickeln, indem die Verbreitung des IEEE 802.1 Audio Video Bridging (AVB) und ähnlicher Standards über verschiedene Link-Layer für Netzwerke vorangetrieben wird. AVnu erstellt umfassende Testverfahren und -prozesse, um die Interoperabilität von A/V-Geräten in Netzwerken sicherzustellen, und trägt dadurch dazu bei, A/V-Streams in einer möglichst hohen Qualität erleben zu können.

Biamp Systems

Extreme Networks stellt auf die Bedürfnisse von Unternehmen zugeschnittene Switches für kommerziell eingesetzte Audiolösungen von Biamp Systems bereit, die ein hohes Maß an Qualität, einfache Handhabung und Skalierbarkeit für professionelle A/V-Umgebungen bieten. Der Einsatz von Extreme Networks AVB-Switches (Audio Video Bridging) bietet Organisationen aufgrund der bahnbrechenden Performance und dem Erweiterungspotential einen enormen Mehrwert; dazu gehören modulare und skalierbare I/Os, DSPs, vernetzte Endknoten sowie ein skalierbares Backbone für digitale Medien. Kunden profitieren dabei von vollständig interoperablen und getesteten AVB-Lösungen, die eine hervorragende Ausfallsicherheit, niedrigere Betriebskosten, Netzwerk-konvergenz für alle Medien und standardbasierte Entwürfe für eine vereinfachte Integration bieten.

Haivision

Haivision liefert End-to-End Video-Streaming Lösungen für sichere Enkodierung, Aufnahme, Verwaltung, Publizierung und Distribution von Video-Content. Live oder On-Demand werdeneiner größeren Internet-Audienz somit über dedizierte Netzwerke Haivisions Video-Streaming Lösungen für eine Reihe von Anwendungen wie beispielsweise Enterprise Communications, Skills Training & Assessment sowie unternehmenskritische Intelligence, Surveillance und Reconnaissance (ISR) Abläufe zur Verfügung gestellt.

Unify

Unify entwickelt, installiert und verwaltet Lösungen für Unified Communications (UC), Sicherheit und professionelle Managed Services. Zwischen Extreme Networks und Unify besteht eine Partnerschaft zur Förderung der Interoperabilität, um hochperformante Lösungen im Bereich Unified Communications für Unternehmen bereitstellen zu können.

Milestone Systems

Milestone Systems bietet IP-basierte Videoüberwachungs- und Videoverwaltungssoftware (Video-Management-Software, VMS), die auf offenen Architekturen basieren und mit mehr IP-Kameras, Encodern und digitalen Videorecordern kompatibel sind als jedes andere vergleichbare System. Milestones offene Plattform ermöglicht Organisationen die Integration mit den besten heutzutage verfügbaren Analytik- und Businesslösungen, so dass Innovationen vorangetrieben werden können. Die Partnerschaft zwischen Milestone und Extreme Networks erhöht die Effizienz im Bereich End-to-End-Physical Security.

Mitel

Extreme Networks und Mitel stellen IP-basierte End-to-End-Lösungen für die Sprachübertragung und die dafür benötigte Netzwerkinfrastruktur bereit. Durch Extreme Networks flexible Hochleistungsswitches und VoIP-Lösungen von Mitel können Organisationen von den Vorteilen eines paketvermittelten Netzwerks

profitieren, ohne Einbußen bei der Performance und Ausfallsicherheit hinnehmen zu müssen.

ShoreTel

Extreme Networks und ShoreTel bieten eine konvergierte Übertragung von Sprache und Daten über eine einfach bereitzustellende, interoperable VoIP-Netzwerklösung, die auf Hochleistungsswitches, Netzwerkmanagement sowie Voice-Switches und Telefonen von ShoreTel ausgerichtet ist. Extreme-Switches bieten ein hohes Niveau an Verfügbarkeit und Ausfallsicherheit für VoIP, während im Management Center, der Anwendung für das Management, eine Gesamtansicht des Netzwerks bereitgestellt wird, in der Änderungen an der Konfiguration schnell und einfach umgesetzt werden können.

Dräger

Dräger ist ein international führendes Unternehmen der Medizin- und Sicherheitstechnik. Das Produktprogramm des Unternehmensbereichs Medizintechnik umfasst Anästhesiearbeitsplätze, Beatmungsgeräte für Intensivmedizin, Intensiv- und Transportbeatmung sowie Wärmetherapie für Neugeborene. Patientenmonitoring, IT-Lösungen und Gasmanagementsysteme runden das Angebot ab.

Philips

In der Philips Sparte Healthcare arbeiten weltweit rund 33.000 Mitarbeiterinnen und Mitarbeiter in den Segmenten: Bildgebende Systeme, Gesundheitslösungen für Zuhause, Kundendienstleistungen, Gesundheits-IT sowie Ultraschall & Überwachungssysteme.

Polycom

Die Integration von Extreme Connect und Polycom CMA Management Application ermöglicht eine automatische Erkennung von Polycom-Geräten und weist entsprechende Konnektivitäts- und Sicherheitsprofile zu. Netzwerkadministratoren greifen auf einen OneView-Bericht zu, der detaillierte Netzwerkinformationen zu allen Polycom-Geräten liefert, u. a. Typ und Status, über das gesamte Netzwerk hinweg.

Security-Partner

Palo Alto Networks

Extreme Networks erweitert die Palo Alto Next Generation Firewall-Richtlinien für die Anwendung innerhalb eines Unternehmensnetzwerks, um Bedrohungen zu entschärfen, die innerhalb der Firewall entstehen, und weist Anwender-zu-IP-Adressen dynamisch zu, während sich drahtlose und -gebundene Geräte mit dem Netzwerk verbinden und es verlassen. Dadurch wird eine niedrigere Fehlerquote bei der Richtliniendurchsetzung und Erstellung von Berichten erreicht.

Fortinet

Fortinet stellt schnelle, sichere, mandantentaugliche Cloud-Netzwerke für moderne große Unternehmen und Cloud Service Provider bereit. Extreme Networks Switches und FortiGate-Securityappliances von Fortinet bieten sowohl Unified Threat Management als auch spezialisierte Sicherheitslösungen zum Schutz vor hochentwickelten Netzwerk- und inhaltsbasierten Bedrohungen.

iBoss

Die Extreme Access Control-Integration mit der iBoss-Internetfilterlösung bietet die Möglichkeit, mehrere physische Standorte innerhalb des Netzwerks zu definieren und Endgeräten an diesen Standorten unterschiedliche Zugriffsprofile und Internetfiltersätze zuzuweisen. Diese Integration ermöglicht iBoss darüber hinaus die Zuweisung von Internetfiltern an Geräte, die normalerweise nicht in Active Directory authentifiziert werden, u. a. iOS-Geräte und Android-Geräte.

Lightspeed Systems

Die Integration von Lightspeed Systems Webfilter und Extreme Access Control stellt Single-Sign-On-Funktionen (SSO) sowie eine vereinfachte Netzwerkverwaltung bereit, die Webfilterrichtlinien mit granularer Transparenz für Endgeräte und der Kontrolle von Anwendern bzw. Geräten kombiniert. Diese einheitliche Managementlösung ermöglicht eine tiefgreifende Transparenz und Kontrolle darüber, auf was Studenten, die Lehrerschaft und Angestellte zugreifen können, und bietet jeweils bestimmte Berechtigungen für einzelne Ressourcen und Systeme.

McAfee

Extreme Access Control integriert Daten von McAfee ePO, um den Status aller Geräte bewerten zu können, die mit dem LAN- oder WLAN-Netzwerk verbunden sind. Für Geräte mit veralteten McAfee-Signaturen löst Access Control über ePO ein Update des Clients aus und stellt damit sicher, dass alle Geräte auf dem neuesten Stand sind. Geräte mit veralteten Signaturen können auch unter Quarantäne gestellt werden, um andere Geräte und Services innerhalb des Netzwerks zu schützen. Daten auf von McAfee ePO verwalteten Geräten werden außerdem innerhalb der Extreme Access Control-Lösung mit zusätzlichen Informationen angereichert; dazu gehören Betriebssystem bzw. Gerätetyp, Anwendername, Zeitstempel des letzten Updates, aktuelle DAT-Version und Name des Geräts.

InfoBlox

Die Extreme Networks-Integration mit InfoBlox IF-MAP automatisiert Updates der Configuration Management Database (CMDB), indem neue Geräte, die sich mit dem Netzwerk verbinden, erkannt und authentifiziert werden, und InfoBlox IF-MAP Server automatisch mit den Daten des jeweiligen Endgeräts aktualisiert wird. Der InfoBlox-Server aktualisiert anschließend die CMDB; dadurch wird garantiert, dass alle Anwendungen, die den IF-MAP-Server verwenden, aktuelle und vollständige Informationen erhalten, und sichergestellt, dass die CMDB jederzeit korrekte Daten enthält. Extreme Control Center versorgt InfoBlox IF-MAP Server mit verschiedenen

Informationen, u. a. dem physischen Standort des Endgeräts, der MAC-Adresse, der IP-Adresse, dem Hostnamen und dem Betriebssystem, und ermöglicht IT-Administratoren damit, das Netzwerk besser zu verwalten und zu sichern.

Data Center & Cloud-Partner

A10 Networks

A10 Networks – Die Integration von Extreme Networks mit A10 optimiert den Nord/Süd Datenfluss in Data Center Interconnect (DCI) Szenarien. Dies geschieht durch VM und Topologie-Awareness und verbessert die Data Center Security durch Distributed Threat Response gegen suspekta Server-Threats. Die Ressourcenoptimierung von A10 kann zudem in die Extreme Networks SDN Plattform integriert werden

Sanbolic

Die Integration von Sanbolic SDx Management mit der Extreme Networks SDN Plattform schafft eine hyper-konvergente Infrastruktur, welche die Verfügbarkeit, Load-Balancing sowie das Nutzererlebnis einer virtuellen Anwendung an mehreren Standorten oder aber in der Cloud verbessert.

Citrix

Citrix Systems und Extreme Networks stellen eine offene und integrierte Virtualisierungsumgebung zur Verfügung, welche es den Betreibern eines Data Centers erlaubt, Netzwerkfunktionen zu optimieren und zu automatisieren. Durch die Kombination von Extreme Data Center Connect und der Citrix XenServer Virtualisierungsplattform können Anwendungen leichter durch das Netzwerk integriert und verwaltet werden. Die Extreme Networks Virtualisierungs- und Cloud-Architektur unterstützt Virtualisierung auf der Netzwerkebene – das beinhaltet Management, Reporting und Konfiguration durch “Zero-Touch” Management und Mobilität zwischen Server und Netzwerk für vollständige Transparenz und Synchronisation der virtuellen Serverumgebung mit dem Netzwerk. Durch diesen offenen Ansatz können XenServer Kunden ihre Server-Virtualisierung sehr eng in das Netzwerk integrieren und schaffen somit eine nahtlose mobile VM Nutzung im Data Center.

EMC VSPEX

Extreme Networks liefert als Teil der EMC VSPEX Infrastruktur branchenweit führende Geschwindigkeit, geringe Latenzzeit und Unterstützung von Virtualisierung für Cloud Networking. Mit der Extreme Networks VSPEX-validierten Technologie können Channel Partner, VARs und Distributoren Mehrwerte zur Verfügung stellen, welche Disaster Recovery, Business Continuity, Business Productivity und IT Edge-Lösungen beinhalten. Durch eine integrierte Lösungsarchitektur bekommen Unternehmen vereinfachte Einsatzmöglichkeiten, vorhersehbare Performance sowie Flexibilität der Lösung.

Apache Hadoop

Die Interoperabilitätspartnerschaft von Extreme Networks und Apache Hadoop hilft Kunden, wertvolle Informationen nutzbar zu machen und die Geschwindigkeit, in der

Daten analysiert werden können, drastisch zu erhöhen. Die gemeinsame Lösung wurde geschaffen, um Engpässe in traditionellen Netzwerken zu verringern und bessere und schnellere Geschäftsentscheidungen treffen zu können.

Microsoft

Die Integration von Extreme Data Center Connect mit Microsoft Hyper-V 2012 R ermöglicht vereinfachte Workflows zur Konfiguration und zum Einsatz von VMs in Hypervisor oder physikalischen Netzwerken. Dadurch wird die Synchronisation von virtuellen und physischen Netzwerkkonfigurationen verbessert und gleichzeitig eine hohe Anzahl von mobilen VMs mit individuellen Endsystemprofilen unterstützt. Extreme Networks OneView liefert tiefe Einblicke in Data Center Umgebungen und Leistungen, inklusive Echtzeit-Visibilität in alle Data Center Server (inklusive VMs), Hypervisor-Server und klassische Server. Zeitbezogene Reports zeigen eine Vielzahl von Daten, wie Anzahl der virtuellen Maschinen, Hypervisor-Servern und klassischen Servern.

VMware

Die Integration von Extreme Data Center Connect und VMware vSphere 5.5 automatisiert die Konfiguration und den Einsatz von VMs sowohl im Hypervisor als auch im physikalischen Netzwerk. Die Vorteile sind eine verbesserte Synchronisation der virtuellen und physikalischen Netzwerke, Unterstützung von VM-Mobilität mit individuellen Profilen pro Endsystem, erweitertes Reporting über VM und Hypervisor Verteilung, sowie Integration in native VM Konfigurationen. Zudem liefert Extreme Networks OneView tiefe Einblicke in Data Center Umgebungen und Performance, inklusive Echtzeit-Visibilität in alle Data Center Server (inklusive VMs) Hypervisor-Server und klassische Server. Zeitbezogene Reports zeigen eine Vielzahl von Daten wie Anzahl der virtuellen Maschinen, Hypervisor-Servern und klassischen Servern.

Mobility-Partner

Airwatch

Die Extreme Networks Integration mit AirWatch von VMware ermöglicht die Kontrolle darüber, welche Geräte sich zu welchem Grad im Netzwerk befinden und welche Verbindungsart in Form von Bandbreite diese bekommen. Zudem wird der Netzwerkverkehr gefiltert, VLANs zugewiesen, MDM umgesetzt und vieles mehr.

AeroScout

AeroScout hilft Kunden, die Leistungsfähigkeit von WLANs zu steigern, indem sie die Lokation, Kondition und Status von mobile Geräten und Personen tracken und verwalten. Durch die Integration von AeroScout und Extreme Access Control können IT-Manager ihre kabellosen und kabelgebundenen Geräte und Applikationen aus einer Konsole heraus verwalten und kontrollieren.

Maas360

Die Integration von Extreme Access Control und Fiberlink Communications MaaS360 beinhaltet verbesserte Netzzugangskontrolle, Sicherheit und vereinfachtes Geräte-Management. Die Lösung ermöglicht der Unternehmens-IT das Sammeln von als persönlichen erkennbaren Informationen auf dem Smartphone oder Tablet zu blockieren und erlaubt somit den Administratoren die Wahl, welche Privacy-Einstellungen sie implementieren möchten.

JAMF

Die Integration von JAMF Casper Suite und Extreme Access Control bietet automatisiertes Risk-Assessment, Onboarding und Provisionierung von BYOD Geräten und somit den IT Abteilungen die Möglichkeit, das Troubleshooting zu verbessern, Nutzer-Transparenz zu erlangen und Gastgeräte mit Informationen wie Sponsor, Lokation, verbundener Access Point bzw. Switch, Applikationen im Einsatz sowie Gerätetyp und weitere Details zu sehen.

MobileIron

Die gemeinsame Lösung von MobileIron und Extreme Access Control liefert IT-Leitern einen ganzheitlichen und detaillierten Ansatz für durchgängiges Policy-Management, Zugangskontrolle, Compliance-Monitoring und Reporting über alle Netzwerkebenen und -endpunkte hinweg. Durch die Integration in Extreme Access Control entstehen zudem zusätzliche On-Boarding Methoden für BYOD Umgebungen, erweiterte Netzwerksecurity durch das Hinzufügen von MDM-Daten zu den Netzwerkzugangsregeln und vieles mehr.

Purple WiFi

Purple WiFi stellt cloud-basierte WiFi Analytics und lokationsbasierte Dienste für Echtzeit-Daten und Reporting zur Verfügung. So liefert Purple WiFi speziell Veranstaltungsorten ein nie dagewesenes Level an Einblicken in das Nutzerverhalten und bietet somit Möglichkeiten, sich mit diesen direkt und gezielt auseinanderzusetzen. Integriert mit Extreme Application Analytics bietet die Lösung durch das Netzwerk granulare Einblicke in das Nutzerverhalten. Purple WiFi stellt außerdem demografische Daten der Nutzer auf dem Purple-Portal zur Verfügung, durch welches man versteht, wer, wann, wie lange den Hotspot nutzt und wie alt die entsprechenden Nutzer sind, welches Geschlecht sie haben und viele weitere verwertbare Informationen, welche die Nutzer über ihre sozialen Netzwerke anbieten.

Ascom

Die zertifizierte Partnerschaft von Extreme Networks und Ascom ermöglicht die Bereitstellung von nahtloser, end-to-end Wireless-Telefonie und Messaging-Systemen im Unternehmen.

Ekahau

Ekahau Site Survey (ESS) bietet IT-Managern, Administratoren und Wireless-Experten die optimale Lösung für den Entwurf und die Überprüfung sämtlicher 802.11a/b/g/n-

Wi-Fi-Netzwerke sowie für deren Fehlerbehebung. Bei ESS handelt es sich um ein softwarebasiertes Tool zur Netzwerkvisualisierung, das auf einem Standardlaptop mit unterstütztem WLAN-Adapter ausgeführt werden kann. Zwischen Ekahau und Extreme besteht eine interoperable Partnerschaft zur schnellen und effizienten Erstellung von WLAN-Netzwerken für eine bessere Quality of Experience für Kunden.

Ucopia

Ucopia bietet Zugriffssicherheit und Mobilitäts-Management-Lösungen für drahtlose und kabelgebundene Netzwerke. Diese Lösungen für kleine und große Unternehmen, Hotels, Bildungseinrichtungen, Krankenhäuser oder auch Verwaltungen, ermöglicht mobilen Nutzern die sichere und bequeme Verbindung zum Netzwerk.

8 Services

Netzwerke sind für Unternehmen eine effektive und effiziente Kommunikations- und Informationsbasis. Sie bilden sozusagen ihr Nervensystem. Deshalb werden Service, Support und Training der IT-Mitarbeiter immer wichtiger, um Netzwerke flexibel genug zu machen, damit sie sich den immer schneller verändernden Anforderungen an Unternehmen anpassen können. Ein Netzwerk kann sehr schnell neue Funktionen anbieten, wenn Hard- und Softwareprodukte, Service und Support, Training und Professional Services konzeptionell aufeinander abgestimmt sind. Weil immer mehr Funktionen, kritische Daten, organisations- oder kommunikationsrelevante Anwendungen aufs Netz verlagert werden oder übers Netz arbeiten, ist dessen Verfügbarkeit für das Funktionieren der Geschäftsabläufe essentiell. Daher zielen sämtliche administrativen Aktivitäten darauf, optimale Netzwerkverfügbarkeit sicherzustellen. Service, Support und Training spielen hierbei eine Schlüsselrolle.

Dazu gehören auch Wartungskonzepte, die sich an den individuellen Unternehmensanforderungen orientieren. Grundbausteine wie Telefonsupport, Firmware-Upgrades oder ein Vorabtausch sollten auf die gesamte Netzwerk- und Security-Infrastruktur abgestimmt sein. So lässt sich sicherstellen, dass das Netz bei Beeinträchtigungen in kürzester Zeit wieder funktioniert.

Je komplexer das Netzwerk wird, desto wichtiger wird eine richtige Kombination aus verschiedenen Services zum Schutz Ihrer Investitionen und Ressourcen.

Wartung & Support

Premier Services

Managed Services

Professional Services

Aussagekräftige Analytik. Zuverlässigkeit. Skalierbarkeit. Flexibilität.

Wartung & Support

Die Netzwerke von Gestern sind nicht dafür geschaffen, die Anforderungen der heutigen Applikationen, Analytics und Services von BYOD, IoT, Big Data und Cloud-Initiativen zu meistern, geschweige denn mit der Komplexität, die sie mit sich bringen, fertig zu werden. Die softwarebasierten Mobility- und BYOD-Lösungen von Extreme arbeiten auch in den anspruchsvollsten Umgebungen fehlerfrei. Gleichzeitig können sie die Betriebskosten senken, das Nutzererlebnis verbessern, mobile Initiativen ermöglichen und die Sicherheit steigern. Flexibilität, Effizienz und Wettbewerbsfähigkeit der Unternehmen sind das Resultat.

Ihr Netzwerk läuft 24x7. Obwohl Ihre Support-Mitarbeiter es unterstützen, braucht Ihr Team einen Ansprechpartner, wenn technische Fragen auftreten. Services von Extreme ergänzen das firmeninterne Wissen über die Netzwerkressourcen durch tiefgehendes technisches Produktwissen, wie es nur der Hersteller liefern kann. Es gibt Support-Level für jeden Bedarf - vom 24x7 Telefonsupport bis zu vier Stunden Vor-Ort-Reaktionszeit. Über SupportNet greifen Sie auf unsere Experten zu und bekommen tiefgehende Troubleshooting-Informationen und Antworten auf Ihre technischen Fragen. Unsere Experten beraten Sie bei einem kostenfreien Anruf, oder wenn Sie unser Online-Websupport-Portal besuchen. Diese komfortable Supportoption von Extreme Networks bietet eine sinnvolle Erweiterung Ihrer Gewährleistung.

Extreme Services - Leistungsumfang

- **24x7 Telefonsupport:** Unbegrenzter, jederzeit verfügbarer und kostenfreier Zugang zu unserem 100% internen Support Center.
- **Firmware Updates und Upgrades:** Laden Sie online wertvolle Firmware-Updates und Upgrades von unserer Webseite herunter.
- **Software und Secure Network Appliance Support:** Sofortiger Zugang zu neuen Releases garantiert, dass Ihre Applikationssoftware und Sicherheitsanwendungen immer auf dem neusten Stand sind und mit Hochleistung arbeiten.
- **Web-Support:** Nutzen Sie die Vorteile des 24x7-Web-Supports, um allgemeine Fragen mit Hilfe unserer Knowledgebase zu klären und in technischen Dokumentationen zu recherchieren.
- **Ersatzteile:** Vorabaustausch defekter Produkte innerhalb einer vereinbarten Zeitspanne (Lieferoptionen 4 Stunden / gleicher Werktag / nächster Werktag, auch als 7x24-Stunden-Servicelevel erhältlich) von globalen Lagern aus.
- **Techniker vor Ort:** Von Extreme Networks zertifizierte Techniker helfen, wenn nötig, Netzwerkfehler zu diagnostizieren, die Logistik vor Ort zu managen und bei technischen Eskalationen die Verbindung zu Produkt-Ingenieuren herzustellen. Mögliche Service-Levels: 4 Stunden / gleicher Werktag / nächster Werktag /rund um die Uhr.

Vorteile von Extreme Services

- Unsere Kompetenz:
 - 94% aller Anfragen werden von unserem Support-Team beim ersten Kontakt gelöst
 - 9 von 10 Kunden sind mit dem Support von Extreme Networks sehr zufrieden
 - 100% internes Service Center
- Netzwerkverfügbarkeit und Produktivität: Mit Extreme Services minimieren Sie die Auswirkungen eines ungeplanten Ausfalls und erhöhen die Mitarbeiterproduktivität.
- Optimierte Betriebskosten: Wahrscheinlich übersteigen die Betriebskosten Ihrer Technikumgebung über den Lebenszyklus der Produkte deren Einkaufspreis. Mit Extreme Services senken Sie die Betriebskosten und sichern eine lange Lebensdauer des Netzes.

Übersicht des kompletten Service Supports

Support Offering	Global Technical Assistance Center (24x7x365)	eSupport (24x7x365)	Advanced Hardware Replacement	Onsite Services	Return & Replace (10 Business Days, After Receipt at Factory)
Software & TAC	✓	✓			
Return & Replace	✓	✓			✓
NBD AHR	✓	✓	Next Business Day		
NBD Onsite	✓	✓	Next Business Day	M - F (8 x 5)	
4-Hour AHR	✓	✓	4 Hours		
4-Hour Onsite	✓	✓	4 Hours	24 x 7	
Software Subscription	✓	✓			

Warum Extreme Services?

Extreme Networks ist der Überzeugung, dass anspruchsvoller Service und Support kritisch für die gesamte Netzwerkverfügbarkeit ist. Deswegen komplettiert unser Services-Portfolio mit seinen innovativen und flexiblen Service- und Support-Angeboten Ihre Lösung. Extreme Services-Kunden profitieren davon, dass 94% aller Anfragen schon beim Erstkontakt durch unser internes Support-Center-Team gelöst werden. Unsere Support-Center-Techniker haben im Durchschnitt über 8,5 Jahre technische Erfahrung mit Extreme Networks-Lösungen gesammelt. Extreme Services bietet alle Support-Services, die Unternehmen in der Nutzungsphase für hochverfügbare Netze und Services brauchen – online, vor Ort und per Telefon.

Premier Services Program (PSP)

Extreme Networks bietet mit dem Premier Service Program einen proaktiven Service an, der sich individuellen Kundenbedürfnissen anpasst und Fokus auf Ihr Netzwerk legt:

- **Ressourcen:** Support-Techniker und Program-Manager
- **Expertise:** Optimierungsempfehlungen, Service-Support vor Ort (Premier Gold und Premier Platinum) und individuelle Service-Eskalation
- **Proaktiver Service:** proaktive Empfehlungen für Software Updates, um Problemen vorzubeugen und die Performance zu maximieren
- **Der Mehrwert von Premier:** regelmäßige Besprechungen der Cases, Überprüfung der Netzwerke und regelmäßiger Wartungsprozess

Level von Premier Services

Bronze	Silver	Gold	
Geringe Netzwerk-Komplexität	Mittlere Netzwerk-Komplexität	Hohe Netzwerk-Komplexität	
			Regional Designated Technical Support Engineers
			Upgrade Management + Lab Validation Hardware und Software
			Customer Entitlement & Asset Management
			Vier oder Acht Tage Onsite Support pro Jahr mit PM oder PSE
			Network Assessment Einmal im Jahr mit PSE
			Zwei oder Vier Service History Reviews pro Jahr und remote mit PM
			Dedizierter Program Manager (PM) Bis zu 5 Stunden pro Woche
			Code Review und Knowledge Transfer halbjährlich mit PSE
			Case Management zwewöchentliche Calls mit PSE
			Dedizierter Premier Services Engineer (PSE)

Managed Services

Extreme Networks bietet neben ExtremeWorks Wartungsleistungen und dem Premier Services Program auch eine Extreme Networks Managed Services Option an. Denn mit all den cloud-basierten Applikationen, den großen Datenmengen, die das Netzwerk belasten, stellt sich zwangsläufig die Frage, wie proaktiv Sie heute die maximale Verfügbarkeit Ihres Netzes garantieren können? Wenn Sie zudem mehrere Lokationen haben und zentrale Sichtbarkeit und Kontrolle über das Netz behalten wollen, dann kann ExtremeWorks Monitoring Plus, wo wir Ihnen ein cloud basiertes Tool an die Hand geben, jederzeit und überall den Sicherheitsstatus, die aktuelle Performance und Gesundheit Ihres Netzes darstellen. Bei der ExtremeWorks Response Plus Option werden wir hier sogar proaktiv tätig und beheben eventuell auftretende Probleme proaktiv und entsprechend der vereinbarten SLAs.

Vorteile von Network Managed Services:

- Entlastung Ihrer IT-Mitarbeiter: Managed Services übernimmt das Monitoring und Management Ihres Netzwerkes
- Einsparung von Zeit- und Geldressourcen durch Trainings für die IT-Mitarbeiter und Neueinstellungen
- Managed Services stellt eine flexible und kostengünstige Netzwerk-Lösung bereit inklusive Support des Extreme Networks-Equipments

Extreme Managed Services Angebote:

	MonitoringPLUS	ResponsePLUS
24x7 Service Desk	X	X
Advanced Monitoring System (H-P-S)	X	X
Proaktive Problemerkennung	X	X
Webportal mit Dashboards	X	X
Service Reporting	X	X
Config Backup	X	X
Asset Management	X	X
Service Review		X
Service Manager		X
Network Operation (Problembehebung)		X

Professional Services

Netzwerke und die damit verbundene Sicherheit stehen mehr als andere Dienste im Blickpunkt von Unternehmen, da sie die universelle Plattform für Kommunikation und Geschäftsprozesse bilden. Um den Unternehmensanforderungen gerecht zu werden, bietet Extreme Networks ein umfassendes Portfolio an Dienstleistungen wie Beratung, Planung & Design, Assessments, Implementierung oder auch Projektmanagement an. Die Leistungen werden durch Systemspezialisten, basierend auf Best Practices, erbracht. Auch die permanente Vor-Ort Unterstützung durch einen ‘Resident Onsite Engineer’ ist Bestandteil des Leistungsumfangs.

Wir stellen unsere Expertise zur Verfügung, wenn Sie diese benötigen. Extreme Networks bietet umfassende professionelle Dienstleistungen an, um vorhandenes technisches Know-how -in Bezug auf das gesamte Lösungsportfolio- zu ergänzen und eventuelle Personalengpässe auszugleichen. Das Professional Services Team kann beispielsweise bei folgenden Anforderungen mit einbezogen werden:

- Planung und Design von Extreme Lösungen
- Bei der Implementierung des Extreme Networks-Lösungsportfolios
- Integration neuer Technologien
- Durchführung von Analysen/Network Health-Checks
- bei Bedarf eines ‘Resident Onsite Engineers’ zur Erbringung umfassender Services in Verbindung mit dem Lösungsportfolio von Extreme.

Weitere Informationen finden Sie auch auf:

<http://extremenetworks.com/support/professional-services/>

Extreme Networks Training

Unsere Schulungsprogramme sind auf Lernziele ausgerichtet, die für die Anwendung bestimmter Technologien und für die Konzeption von Infrastrukturen entscheidend sind. Neben einer Reihe von virtuellen On-Demand und Live-Trainings bieten wir auch Trainings in verschiedenen Lokationen in Deutschland an.

- Live-Trainings in virtuellem oder klassischem Trainingsformat im Klassenraum
- Ausgezeichnete „Hands-on“ Lab-Umgebung
- Über 20 Technologie-, Produkt- und Lösungsbasierte Kurse stehen zur Auswahl
- Einfacher Teilnahme-Prozess in kleinen Trainingseinheiten
- Weitere Informationen sowie Termine und Lokationen unter www.extremenetworks.com/education/courses

Überblick der aktuell verfügbaren Extreme Trainings:















Durch Extreme Technical Training werden Sie mit der Extreme Technologie vertraut und lernen, Extreme Lösungen zu betreiben. Eine Auswahl der verfügbaren Kurse:	
Switching & Routing:	Netzwerkmanagement & Security
• ExtremeXOS Fundamentals	• Extreme Application Analytics
• ExtremeXOS Switching & Routing	• High-Density Environments
• IPv6 Networking	• Extreme Management Center Boot Camp
• ExtremeEOS Fundamentals	• Extreme Policy
• ExtremeEOS Switching & Routing	• Extreme Access Control (NAC)
• Switching & Routing Boot Camp (EXOS & EOS)	• Security Information & Event Management (SIEM)
• ECA Networking Hands-On Lab	Wireless LAN
• Advanced Routing	• Extreme Wireless

Extreme Networks Community: The Hub

The HUB ist eine Online-Plattform, auf der sich Extreme Networks-Interessierte untereinander austauschen, Feedback und Ideen teilen können und Lösungen gemeinsam gesucht werden können. Nähere Informationen, Tipps und Guidelines zum HUB sind unter folgendem Link zu finden:

<https://community.extremenetworks.com/extreme>

The Hub: Diskussions-Kategorien

Products	Technical Discussions	Technical Discussions
 ExtremeXOS	 Switching & Network	 Training
 EOS	 Network	 Regional User
 IdentiFi	 General	 General
 NetSight	 Security	 All Things E-
 SummitWM	 Scripting	Und viele weitere Themen ...

9 Weitere Informationsquellen

Die Halbwertszeit von Information im Bereich IT ist schon seit langem erschreckend kurz. Alleine schon wegen der großen Akzeptanz unserer Kunden planen wir auch eine gedruckte Form dieser Ausgabe.

Zusätzlich geben wir in diesem Kapitel einige Tipps, an welchen Stellen im Netz Sie weiterstöbern können, um mehr über unser Unternehmen und unsere Lösungen zu erfahren.

Corporate Homepage

Unsere internationale Webpräsenz erreichen Sie unter der URL www.extremenetworks.com. Von dort gelangen Sie auch zur deutschen Microsite, die seit März 2015 bereitsteht.

Extranet

Registrieren Sie sich unverbindlich als Endkunde bzw. Vertriebspartner auf unserem Extranet extranet.extremenetworks.com. Hier haben Sie Zugriff auf Handbücher, Funktionsbeschreibungen und Software. Hier können Sie zu Testzwecken auch eigene Evaluationslizenzen generieren.

Consultants und Planungsbüros

Technische Dokumente für die Planung von Ausschreibungen finden Sie unter der URL bit.ly/extreme-planer. Bitte registrieren Sie sich für den Zugang bei ralf.klockewitz@extremenetworks.com

Hintergrundinformationen

Unter der URL www.extremenetworks.com/resources finden Sie eine Auswahl von Case Studies, Webinaren, Whitepapers und anderen Dokumenten zur Veranschaulichung unserer Lösungen.

Videos

Ein Film sagt mehr als tausend Worte. Schauen Sie unseren Technikern bei Youtube über die Schulter: bit.ly/extreme-how-to. Hier werden grundlegende Funktionen mit eingängigen HowTo Videos erläutert

Training

Informieren Sie sich über unser Trainingsangebot. Wir bieten Zertifizierungstrainings für unser gesamtes Lösungsportfolio an. Auf Ihren Wunsch hin halten wir Schulungen gerne auch bei Ihnen vor Ort und passen die Inhalte Ihrem Bedarf an. bit.ly/extreme-trainings

Web Based Trainings sind hervorragend geeignet, um einen fundierten Einstieg in neue Themen zu erhalten. Suchen Sie das Thema Ihres Interesses und den Zeitpunkt für das Training selbst aus. bit.ly/extreme-wbt-trainings

GTAC Knowledgebase

Die Extreme GTAC Knowledgebase stellt eine umfangreiche Sammlung von technischen Informationen und Artikeln zur Verfügung. Diese stehen beim täglichen Umgang mit Produkten sowie Lösungen von Extreme mit einer Vielzahl von Hinweisen, Empfehlungen und Hilfestellungen mit Rat und Tat zur Seite. Die Informationsvielfalt wird kontinuierlich erweitert, eine konsequente Nutzung der Knowledgebase wird empfohlen.

GTAC Knowledge Home: <https://gtacknowledge.extremenetworks.com/>

Danksagung

Schon seit über zehn Jahren dient der Solution Guide unseren Kunden als Planungshilfe und Nachschlagewerk. Nicht nur technisches Know-How, sondern auch das praktische Wissen darüber, welche Themen im Feld von Interesse sind, unterscheiden dieses Buch von anderen Dokumenten. Vor allem die Bereitschaft jedes Einzelnen, mit einem eigenen Beitrag zusätzliche Zeit in dieses Projekt zu investieren, machen den Charme des Solution Guides aus.

Daher ein besonderes Dankeschön an:

Markus Altmann

Alexander Eichholz

Karin Denk

Fred Götz

Olaf Hagemann

Andreas Helling

André Herkenrath

Efthymios Christodoulakis

Ralf Klockewitz

Stephan Krock

Marco Mautone

Jan Heinbokel

Heribert Rehart



Extreme®

Connect Beyond the Network

Extreme Networks GmbH

Solmsstr. 83
60486 Frankfurt am Main
Tel.: +49 69 47860-0
Fax: +49 69 47860-109

Dornacher Str. 3d
85622 Feldkirchen (München)
Tel.: +49 89 37427-0
Fax: +49 89 37427-499

Wittestr. 30, Haus J
13509 Berlin
Tel.: +49 30 399 795

Torgauer Str. 231
04347 Leipzig
Tel.: +49 341 271 03 07

[HTTP://DE.EXTREMENETWORKS.COM](http://de.extremenetworks.com)