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
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

Seite 4 von 264
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 (11)

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.


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.


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 Resourcen 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:

<table>
<thead>
<tr>
<th>Alter Name</th>
<th>Neue Produktfamilie</th>
<th>Neuer Produktnamen</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdentiFi</td>
<td>ExtremeWireless</td>
<td>Modellbezeichnung AP 3xxx</td>
</tr>
<tr>
<td>Summit, Black Diamond</td>
<td>ExtremeSwitching</td>
<td>Modellbezeichnung X450-G2, X8 usw.</td>
</tr>
<tr>
<td>S-Serie, K-Serie</td>
<td>ExtremeSwitching</td>
<td>Bleibt bei S-Serie, K-Serie</td>
</tr>
<tr>
<td>NetSight</td>
<td>ExtremeManagement</td>
<td>(Extreme) Management Center</td>
</tr>
<tr>
<td>NAC und Mobile IAM</td>
<td>ExtremeControl</td>
<td>(Extreme) Access Control</td>
</tr>
<tr>
<td>Data Center Manager</td>
<td>ExtremeControl</td>
<td>Data Center Connect</td>
</tr>
<tr>
<td>Purview</td>
<td>ExtremeAnalytics</td>
<td>(Extreme) Application Analytics</td>
</tr>
</tbody>
</table>
Unsere Standorte in Deutschland

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

Sie erreichen uns per ...

- Telefon: +49 (0) 69 478 60-0
- Email: info.de@extremenetworks.com
- Twitter: @EXTR_DE
- Facebook: ExtremeNetworksDE

Unsere Standorte:

- Frankfurt: Solmstr. 83, 60486 Frankfurt am Main
- München: Dornacher Str. 3d, 85622 Feldkirchen
- Berlin: Wittestr. 30 / Haus J, 13509 Berlin
- Leipzig: Torgauer Str. 231, 04347 Leipzig
- Zürich: Leutschenbachstr. 95, 8050 Zürich (CH)

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 Rechenzentrumserigns.


Authentisierung - Der Blick über den Tellerrand

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 Evidenzah of 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.


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 (IP Security, 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

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

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.
- **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.


- **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.


**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 Authentisierungsmöglichkeiten verfügen.


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


**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-Authentication.

Aber was passiert, wenn der PC gleichzeitig über IEEE 802.1x und MAC-Authentication 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, Netzwerkdiensste 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 Resourcen 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

**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)

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:

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

**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 selbsttätig aus. Das an sich sehr schlange 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 platzen 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 Resourcen 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 Problemläufe schnell ermitteln und beheben.

Doch auch im Rechenzentrumbetrieb gibt das OneView Interface Hilfestellung beim Aufsetzen und Umziehen virtueller und physischer 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.


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.


**Analyse - wenn es doch nicht am Netz liegt**

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?
- Wie viele 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 sichern Komponeente so stabil wie möglich zu machen (Verfügbarkeit) und zweitens Redundanz (zum Beispiel in Form eines zweiten Gerätes) aufzubauen. Das Zweitgerät

---

\[Extrem Networks – Solution Guide 2016\]

Seite 23 von 264
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

Layer 2 - Datenübertragungsschicht

Spanning Tree IEEE 802.1d
Der Spanning-Tree-Algorithmus verhindert Loops auf der Datenübertragungsschicht. Dazu tauschen die Netzwerkkomponenten (Switche) 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 Switche 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.


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 Switche austauschen,
enthalt aber mehr Informationen. Außerdem wurde die Verarbeitung der Nachrichten verbessert.


**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.


**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 Switchte 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.

**Link Aggregation IEEE 802.3ad**

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


Aktuelle Switche, 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 Switche 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 Switche 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.


**M-LAG – Multiswitch Link Aggregation**


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

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


**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).


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 Switchen 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.


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).


**Shortest Path Bridging**


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.


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 Enkapsulierung.

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 wiederrum für jeden Switch eindeutig einen Verbindungsbaukasten zu allen anderen Switches darstellt, lässt sich somit als Faustregel die Anzahl benötigter VLAN IDs ermitteln: (Anzahl Switches x Anzahl Basis VLANs) + Anzahl Basis VLANs.


**Layer 3 - Netzwerkschicht**

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.


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 Verarbeitungszeit 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.


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)**


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 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.


**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.

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 Schlüsselsfaktor, 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.

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 Performace 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**

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.


Extreme Data Center Connect integriert sich in existierende Workflow- und Lifecycle-Tools. So überblickt der Administrator jederzeit virtuelle und physische 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 Inventarerkennung 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.


**Data Center Bridging**


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.


**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 Weggewahl 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 Switche 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 Switche 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

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.


**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 802.1aq (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-

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.


**TRILL**


**MLAG**

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


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

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

Dieses Modell bietet die Grundlage für ein hochverfügbares und fehler tolerantes 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.


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**


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 Brandbreiten an fünf zusätzlichen Fabric-Links und begrenzt die aggregierte Routingleistung zwischen zwei VLANs in der Fabric auf einen einzigen Link.

**Data Center Interconnect - Host Routing**


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**


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 Bandbreitenutztung 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


Es werden im ganzen Netz verteilte Sonden unterstützt, welche die Antwortzeit von Anwendungen messen. So können IT-Administratoren das Verhaltensverhalten 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**

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 Latenzziten, 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 Aggregationsswitches 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.

**End-of-Row versus Top-of-Rack**


**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 Switch.
- Die vorhandene Backplane senkt die Überbuchungsraten.
- Chassis-Switche 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 Switche, die logisch zu einem virtuellen Switch zusammengefasst sind) pro Rack vor. Dieser Switch konsolidiert die Verkabelung auf Rack-Ebene vor den Aggregationsswitchen 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


Client – Application – Database


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

Das Core-Design des Data Center der Zukunft
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.

**Server-Virtualisierung**

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.


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**


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)**


**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-basierted Application Programming Interface (API)
• Integriert Extreme Networks und fremdentwickelte Applikationen durch ein standardbasierendes POSIX Interface
• Scripting-basierendes Geräteverwalten 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
• Sicherem Management durch starke Verschlüsselung und Authentifizierung

Ein modulares Betriebssystem
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](http://www.extremenetworks.com/product/extremexos-network-operating-system)


**Quality of Service in konvergenten Netzen**


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

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)?**

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

Seite 60 von 264
- 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.


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 prioritierenden 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.


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**


**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 Übermittlungsriorität 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


**Integrated Services (IntServ)**


**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.

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:

<table>
<thead>
<tr>
<th>DSCP dez.</th>
<th>DSCP binär</th>
<th>DSCP hex.</th>
<th>ToS dez.</th>
<th>ToS binär</th>
<th>ToS hex.</th>
<th>Serviceklassen (CoS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>000000</td>
<td>0x00</td>
<td>0</td>
<td>00000000</td>
<td>0x00</td>
<td>Best effort</td>
</tr>
<tr>
<td>8</td>
<td>001000</td>
<td>0x08</td>
<td>32</td>
<td>00100000</td>
<td>0x20</td>
<td>Class 1</td>
</tr>
<tr>
<td>10</td>
<td>001100</td>
<td>0x0a</td>
<td>40</td>
<td>00110000</td>
<td>0x28</td>
<td>Class 1, gold (AF11)</td>
</tr>
<tr>
<td>12</td>
<td>001110</td>
<td>0x0c</td>
<td>48</td>
<td>00111000</td>
<td>0x30</td>
<td>Class 1, silver (AF12)</td>
</tr>
<tr>
<td>14</td>
<td>001111</td>
<td>0x0e</td>
<td>56</td>
<td>00111100</td>
<td>0x38</td>
<td>Class 1, bronze (AF13)</td>
</tr>
<tr>
<td>16</td>
<td>010000</td>
<td>0x10</td>
<td>64</td>
<td>01000000</td>
<td>0x40</td>
<td>Class 2</td>
</tr>
<tr>
<td>18</td>
<td>010100</td>
<td>0x12</td>
<td>72</td>
<td>01010000</td>
<td>0x48</td>
<td>Class 2, gold (AF21)</td>
</tr>
<tr>
<td>20</td>
<td>011000</td>
<td>0x14</td>
<td>80</td>
<td>01100000</td>
<td>0x50</td>
<td>Class 2, silver (AF22)</td>
</tr>
</tbody>
</table>
Die Default Klasse ist für nicht speziell klassifizierten Traffic und entspricht damit der IP Precedence 0.

<table>
<thead>
<tr>
<th>Per Hop Behaviour (PHB)</th>
<th>Diffserv Code Point (DSCP)</th>
<th>IP Precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>000000</td>
<td>0</td>
</tr>
<tr>
<td>Assured Forwarding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low Drop Probability</td>
<td>AF11001010</td>
<td>1</td>
</tr>
<tr>
<td>Medium Drop Probability</td>
<td>AF12001100</td>
<td></td>
</tr>
<tr>
<td>High Drop Probability</td>
<td>AF13001110</td>
<td></td>
</tr>
<tr>
<td>Class 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class 2</td>
<td>AF21001010</td>
<td>2</td>
</tr>
<tr>
<td>Class 3</td>
<td>AF31001010</td>
<td>3</td>
</tr>
<tr>
<td>Class 4</td>
<td>AF41001010</td>
<td>4</td>
</tr>
<tr>
<td>Expedited Forwarding</td>
<td>EF101110</td>
<td>5</td>
</tr>
</tbody>
</table>

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 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:

<table>
<thead>
<tr>
<th>ECT BIT</th>
<th>CE BIT</th>
<th>Bedeutung</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Not-ECT (Not ECN-Capable Transport)</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>ECT(1) (ECN-Capable Transport - 1)</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>ECT(0) (ECN-Capable Transport - 0)</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>CE (Congestion Experienced)</td>
</tr>
</tbody>
</table>

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: 1Byte = 8 Bits) sieht folgendermaßen aus:

<table>
<thead>
<tr>
<th>Bits</th>
<th>Precedence</th>
<th>Delay</th>
<th>Throughput</th>
<th>Reliability</th>
<th>Cost</th>
<th>MBZ</th>
</tr>
</thead>
</table>

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 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.

**Priorisierung nach IEEE 802.1p**


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**


**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 Netzwerkzweigempfangen 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.


**Weighted Round Robin Queuing**

**Hybrid Queuing**

**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

Airtime Fairness

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

Client Load Balancing

**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.


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**


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

[https://extranet.extremenetworks.com/downloads/Pages/S.aspx](https://extranet.extremenetworks.com/downloads/Pages/S.aspx)
Audio-Video-Bridging (AVB)


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.
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.


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.


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.


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 Linkskapazität 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.


**IP Version 6**


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**

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**


IPv6-Erweiterungsheader nach RFC 2460, 2402 und 2406:

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

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


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

---

Extreme Networks – Solution Guide 2016

Seite 77 von 264
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**


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


**IPv6 Routing und andere Funktionen**


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


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


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

**IP bleibt IP**


**SNMP (Simple Network Management Protocol)**


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


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**


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 Script 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


Neben TCL (http://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


Dabei kann das Stecken oder Abziehen eines Netzwerkkabels 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.


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 Profile unterschieden:

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

**User Authentication Trigger**

Es gibt drei Network Login Methoden, die den Trigger auslösen können:
- **802.1X**
- **MAC basiert**
- **Web basiert**

**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.


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.

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)**


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)-Umgaben üblich: Bei BYOD gewährten 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 Devices und Virtual Desktop Infrastructure (VDI)

- 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.

MDM – Mobile Device Management


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

**Beispielszenario-1:**

**Beispielszenario-2:**
Der Geschäftsführer eines Unternehmens greift mit iPhone und WLAN auf unternehmenskritische Daten zu. Diese Daten bleiben nach beendetem 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**


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**


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

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.
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**

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**
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:

<table>
<thead>
<tr>
<th>Produkt / Lizenz</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtuelle Appliances</td>
<td>die Verwendung virtueller Identity &amp; Access Appliances ist in den NMS Advanced Lizenzen enthalten.</td>
</tr>
<tr>
<td>IA-ES-3K</td>
<td>Enterprise Lizenz für das Managen von bis zu 3.000 Endsystemen. Sonst wie IA-ES-1K</td>
</tr>
<tr>
<td>IA-ES-12K</td>
<td>Enterprise Lizenz für das Managen von bis zu 12.000 Endsystemen. Sonst wie IA-ES-1K</td>
</tr>
<tr>
<td>IA-PA-3K</td>
<td>Posture Assessment Lizenz für das Managen von bis zu 3.000 Endsystemen. Beinhaltet die Möglichkeit, sowohl agentenbasiertes, als auch netzwerkbasieres Assessment durchzuführen. Sonst wie IA-ES-1K</td>
</tr>
<tr>
<td>IA-PA-12K</td>
<td>Posture Assessment Lizenz für das Managen von bis zu 12.000 Endsystemen. Beinhaltet die Möglichkeit, sowohl agentenbasiertes, als auch netzwerkbasieres Assessment durchzuführen. Sonst wie IA-ES-1K</td>
</tr>
</tbody>
</table>

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 Verkehrsstrome 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 unbekannten Datenquellen im Netzwerk)
- Statistiken und Abrechnung (z. B. zur Netznutzung einzelner IP Endgerätederessen oder IP Adressbereiche)


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


**Sampled, Unsamped, Any Port – Any Time**

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


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


**Flow Kollektoren**

Als Flow Kollektor bietet Extreme Networks zwei Möglichkeiten:

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

**Kompatibilität**


**Software Defined Networking**


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


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:

![SDN Architektur](image)

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?

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.


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.


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 soll es denn sein?


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 garnicht 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.


Sinnvoller ist mittlerweile eine Plazierung 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.


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.


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 Pallettenstäben 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.


High Density – Vom Hörsaal bis zum Stadion
Glaubt 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.

Das ist gut so, denn die Dichte der installierten Accesspoints lässt sich, bedingt durch die Frequenzbänder, nicht beliebig erhöhen. Hier ist ein präzises 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.


Die vernetzte Schwester – Wireless im Krankenhaus

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.


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?**


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 klingt sich automatisch in das lokal bereitgestellte Gast WLAN ein. Ohne Registrierung, ohne Papiervoucher mit Passwörtern, die sich nicht mal ein Zahlenkünstler merken kann.


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 10 Gbps und mehr ermöglichen. Was sich hier in welchem Bereich durchsetzen wird, lässt sich...

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**


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

**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?

**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.

<table>
<thead>
<tr>
<th>Architektur</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FAT AP Architektur</strong></td>
<td>Intelligenz und Management direkt auf den Access Points</td>
</tr>
<tr>
<td><strong>Split MAC / Thin AP Architektur</strong></td>
<td>Splitted MAC-Funktionen zwischen AP und Controller (Encryption, QoS, RF Management) (Skaliert nicht in großen Umgebungen)</td>
</tr>
<tr>
<td><strong>Fit AP Architektur</strong></td>
<td>Dezentrales Policy-Enforcement (Encryption, QoS, RF Management) Zentralisiertes Management und Kontrolle</td>
</tr>
</tbody>
</table>

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 überlappenden Kanälen und weitaus mehr Bandbreite die bessere Alternative zum bisher genutzten ISM Frequenzbereich.


**Single SSID Design**


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:

<table>
<thead>
<tr>
<th>Beacon Datenrate</th>
<th>Channel Bandbreitenutzung</th>
<th>1 Mbps</th>
<th>2 Mbps</th>
<th>5.5 Mbps</th>
<th>11 Mbps</th>
<th>6 Mbps (802.11a/g)</th>
<th>12 Mbps (802.11a/g)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Mbps</td>
<td>25.92%</td>
<td>12.96%</td>
<td>4.71%</td>
<td>2.35%</td>
<td>4.32%</td>
<td>2.16%</td>
<td></td>
</tr>
<tr>
<td>2 Mbps</td>
<td>12.96%</td>
<td>6.48%</td>
<td>2.36%</td>
<td>1.18%</td>
<td>2.16%</td>
<td>1.08%</td>
<td></td>
</tr>
</tbody>
</table>

Denken Sie auch daran, dass die Rückwärtskompatibilität zu dem alten Standard 802.11b nur zu dem Preis einer auf 1 Mbps 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 Luftschmittstelle 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 Sendezzeit eingeräumt wird, wird der Gesamtdurchsatz der Funkzelle gesteigert.

<table>
<thead>
<tr>
<th>Client Mix</th>
<th>Effective Bandwith (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Packet Fairness</td>
</tr>
<tr>
<td>11a @ 6 Mbps</td>
<td>4.5</td>
</tr>
<tr>
<td>11a @ 24 Mbps</td>
<td>4.5</td>
</tr>
<tr>
<td>11n HT20 @ 104 Mbps</td>
<td>4.5</td>
</tr>
<tr>
<td>11n HT40 @ 240 Mbps</td>
<td>4.5</td>
</tr>
<tr>
<td>Total Throughput</td>
<td>18.0</td>
</tr>
</tbody>
</table>

**Ratelimit & QoS**
Da sich die in einer Funkzelle eingeloggten Clients die Bandbreite und Sendezzeit 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:**

**Performance-Tuning für Multicast-Verkehr:**
Die gestiegene Nutzung von Video-over-WLAN & Zero-Config-Protokollen wie Bonjour, UpnP und LLMNR 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:

<table>
<thead>
<tr>
<th>Radio 1</th>
<th>Radio 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Radio Mode: a/n/ ac</td>
<td>• Radio Mode: b/g/n (b ausschalten, wenn keine 11b Devices mehr vorhanden)</td>
</tr>
<tr>
<td>• Channel Width: 40MHz (80 Mhz bei 11ac APs)</td>
<td>• Channel Width: 20MHz</td>
</tr>
<tr>
<td>• Guard Interval: Short</td>
<td>• ATPC: Enabled</td>
</tr>
<tr>
<td>• ATPC: Enabled</td>
<td>• Max Tx Power: 20 dBm</td>
</tr>
<tr>
<td>• Max Power: 20 dBm</td>
<td>• Min Tx Power: 0 dBm</td>
</tr>
<tr>
<td>• Min Power: 0dBm</td>
<td>• Protection Mode: Disabled</td>
</tr>
<tr>
<td>• Protection Mode: Disabled</td>
<td>• 40MHz Protection Mode: None</td>
</tr>
<tr>
<td>• 40MHz Protection Mode: None</td>
<td>• Aggregate MSDUs: Disabled</td>
</tr>
<tr>
<td>• Aggregate MSDUs: Disabled</td>
<td>• Aggregate MPDUs: Enabled (Disabled for Voice)</td>
</tr>
<tr>
<td>• Aggregate MPDUs: Enabled (Disabled for Voice)</td>
<td>• ADDBA Support: Enabled (Disabled for Voice)</td>
</tr>
<tr>
<td>• ADDBA Support: Enabled (Disabled for Voice)</td>
<td>Zusätzlich bei AP37xx:</td>
</tr>
<tr>
<td></td>
<td>• Enable LDPC</td>
</tr>
<tr>
<td></td>
<td>• Enable STBC</td>
</tr>
<tr>
<td></td>
<td>• Enable TXBF</td>
</tr>
<tr>
<td>Zusätzlich bei AP37xx:</td>
<td>Zusätzlich, wenn Abdeckung gegeben:</td>
</tr>
<tr>
<td>• Erhöhen der min. Basic-Rate (2, 5,5 oder auch 11 Mbps)</td>
<td>• Erhöhen der 802.11g/ a min. Basic-Rates (12 oder auch 24 Mbps )</td>
</tr>
<tr>
<td>• Erhöhen der 802.11g/ a min. Basic-Rates (12 oder auch 24 Mbps )</td>
<td>Zusätzlich bei AP37xx:</td>
</tr>
<tr>
<td></td>
<td>• Enable LDPC</td>
</tr>
<tr>
<td></td>
<td>• Enable STBC</td>
</tr>
<tr>
<td></td>
<td>• Enable TXBF</td>
</tr>
</tbody>
</table>

**VNS Configuration**

**Global Settings->Wireless QoS->Flexible Client Access**
- Fairness Policy: 100% Airtime

**WLAN Services->Privacy**
- “None”, “WPA v.2” oder “WPA-PSK v.2”

**WLAN Services->QoS**
- 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.


Nach dem Credo der Sicherheitsexperten (Verfügbarkeit, Vertraulichkeit, Integrität) ist neben dem Schutz vor unbefugtem Eindringen und Mithören vor allem der kontinuierliche Betrieb alles andere als trivial. Fremde APs sowie WLAN-fremde Störungen beeinflussen die Übertragungsqualität auf einzelne Kanäle 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 unbeschwert e 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.


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

Mit Hilfe von Gebäudeplanen 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, zufallsgesteueter 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.

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


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.


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 all APs verteilt und für die Authentifizierung und Verschlüsselung benutzt wird. 802.11i fordert jeweils einen neuen PMK per Session pro AP. Zurzeit gibt es noch wenige Endgeräte, die OKC unterstützen.


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

**Location-Tracking in WLAN Netzen**


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.
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


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

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


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)

<table>
<thead>
<tr>
<th>Client</th>
<th>MIMO Spatial Streams</th>
<th>20 MHz Channel (Mbps)</th>
<th>40 MHz Channel (Mbps)</th>
<th>80 MHz Channel (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11ac</td>
<td>1x11</td>
<td>86,7</td>
<td>200</td>
<td>433,3</td>
</tr>
<tr>
<td></td>
<td>2x2:2</td>
<td>173,4</td>
<td>400</td>
<td>866,6</td>
</tr>
<tr>
<td></td>
<td>3x3:3</td>
<td>260</td>
<td>600</td>
<td>1300</td>
</tr>
<tr>
<td></td>
<td>4x4:4</td>
<td>346,8</td>
<td>800</td>
<td>1733,3</td>
</tr>
<tr>
<td>11n</td>
<td>1x11</td>
<td>72,2</td>
<td>150</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>2x2:2</td>
<td>144,4</td>
<td>300</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>3x3:3</td>
<td>216,7</td>
<td>450</td>
<td>N/A</td>
</tr>
<tr>
<td>11abg</td>
<td>a/g</td>
<td>54</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>11</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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 Seite 118 von 264
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.

![BPSK, 64-QAM, 256-QAM](image)

Einerseits sorgt dies für eine gesteigerte Übertragungsrate. 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:

<table>
<thead>
<tr>
<th>Access Points</th>
<th>Appliances</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌊 Semiautonome APs</td>
<td>🌊 Physikalische &amp; virtuelle Appliances</td>
<td>🌊 Visibilität, Kontrolle &amp; Automatisierung</td>
</tr>
<tr>
<td>🌊 Custom Design</td>
<td>🌊 HA ohne Unterbrechung</td>
<td>🌊 Policy-basiertes System für WLAN und LAN</td>
</tr>
<tr>
<td>🌊 Hohe Sicherheit: WPA2, WIDS/WIPS, AAA, Forensik</td>
<td>🌊 Flexible SFP+ (1G/10G)</td>
<td>🌊 Automatisches RF-Management &amp; Spectrum-Analyse</td>
</tr>
<tr>
<td>🌊 2x HD Video-Performance</td>
<td>🌊 Verschlüsselungs-Beschleuniger in Hardware</td>
<td>🌊 Single SSID-Design</td>
</tr>
<tr>
<td>🌊 Optimierte Antennen für bessere Funkabdeckung</td>
<td>🌊 Unterstützung von bis zu 2.000 APs und 32.000 User / Appliance</td>
<td>🌊</td>
</tr>
</tbody>
</table>

**ExtremeWireless Access Points**


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**

<table>
<thead>
<tr>
<th>Ultra-Performance + HA</th>
<th>High-Performance</th>
<th>Viele Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AP 3935i/e</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11ac Wave 2, 11abgn, 4x4:4 MIMO</td>
<td>11ac, 11abgn, 3x3:3 MIMO</td>
<td>11ac, 11abgn, 2x2:2 MIMO</td>
</tr>
<tr>
<td>Cloud-Ready</td>
<td>Dual-Radio</td>
<td>Dual-Radio</td>
</tr>
<tr>
<td>802.3at &amp; 802.3af (Stromsparmodus)</td>
<td>802.3at &amp; 802.3af (Stromsparmodus)</td>
<td>802.3af PoE</td>
</tr>
<tr>
<td>Mesh, Policy, QoS</td>
<td>Mesh, Policy, QoS</td>
<td>Mesh, Policy, QoS</td>
</tr>
<tr>
<td>WIDS, WIPS, Spectrum-Analyse</td>
<td>WIDS, WIPS, Spectrum-Analyse</td>
<td>WIDS, WIPS, Spectrum-Analyse</td>
</tr>
<tr>
<td>2,5 Gbps</td>
<td>1,75 Gbps</td>
<td>1,16 Gbps</td>
</tr>
<tr>
<td>90.000 pps</td>
<td>75.000 pps</td>
<td>40.000 pps</td>
</tr>
<tr>
<td>2x E/N mit Active/Active und Active/Passive</td>
<td>2x E/N mit Active/Active und Active/Passive</td>
<td>Rauchmelderdesign</td>
</tr>
</tbody>
</table>
**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 Spacial 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.


**ExtremeWireless 3801 Indoor Access Point**


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


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.


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.


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 17Kg 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.

Spezifikationen und Bestellinformationen zu Indoor APs finden Sie unter: www.extremenetworks.com/products/wireless

### Outdoor Access Points

<table>
<thead>
<tr>
<th>AP 3965i</th>
<th>AP 3965e</th>
<th>AP 3865e</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High-Performance + HA</strong></td>
<td><strong>High-Performance + HA</strong></td>
<td><strong>High-Performance + HA</strong></td>
</tr>
<tr>
<td>• 11ac Wave 2, 11abgn, 4x4:4 MIMO</td>
<td>• 11ac Wave 2, 11abgn, 4x4:4 MIMO</td>
<td>• 11ac, 11abgn, 3x3:3 MIMO</td>
</tr>
<tr>
<td>• Cloud-Ready</td>
<td>• Dual-Radio</td>
<td>• Dual-Radio</td>
</tr>
<tr>
<td>• Dual-Radio</td>
<td>• 802.3at PoE</td>
<td>• 802.3at PoE</td>
</tr>
<tr>
<td>• 802.3at PoE</td>
<td>• Mesh, Policy, QoS</td>
<td>• Mesh, Policy, QoS</td>
</tr>
<tr>
<td>• Mesh, Policy, QoS</td>
<td>• WIDS, WIPS, Spectrum-Analyse</td>
<td>• WIDS, WIPS, Spectrum-Analyse</td>
</tr>
<tr>
<td>• WIDS, WIPS, Spectrum-Analyse</td>
<td>• 2,5 Gbps</td>
<td>• 175 Gbps</td>
</tr>
<tr>
<td>• 2,5 Gbps</td>
<td>• 90.000 pps</td>
<td>• 75.000 pps</td>
</tr>
<tr>
<td>• 90.000 pps</td>
<td>• 2x E/N mit Active/Active und Active/Passive</td>
<td>• Rauchmelderdesign</td>
</tr>
<tr>
<td>• 2x E/N mit Active/Active und Active/Passive</td>
<td>• IP67/NEMA6</td>
<td>• 2x E/N mit Active/Active und Active/Passive</td>
</tr>
<tr>
<td>• IP67/NEMA6</td>
<td>• Externe Antennen</td>
<td>• IP67/NEMA6</td>
</tr>
<tr>
<td>• Integrierte Antennen</td>
<td></td>
<td>• Externe Antennen</td>
</tr>
</tbody>
</table>

### 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 175 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**


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.


Spezifikationen und Bestellinformationen zu Outdoor APs finden Sie unter: [www.extremenetworks.com/products/wireless](http://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

<table>
<thead>
<tr>
<th>C35</th>
<th>V2110</th>
<th>C5210</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entry-Level</strong></td>
<td><strong>Virtualisiert</strong></td>
<td><strong>Mid/High-End</strong></td>
</tr>
<tr>
<td>50-125 Access Points</td>
<td>VMware ESXi 5.1</td>
<td>100-1000 Access Points</td>
</tr>
<tr>
<td>250 APs im HA-Modus</td>
<td>Hyper-V</td>
<td>2.000 APs im HA-Modus</td>
</tr>
<tr>
<td>4 GE Interfaces</td>
<td>8-250 Access Points</td>
<td>HW Crypto Beschleuniger</td>
</tr>
<tr>
<td>GE Mgmt Port</td>
<td>500 APs im HA-Modus</td>
<td>2 SFP+ Interfaces</td>
</tr>
<tr>
<td>2.000 User</td>
<td>2 GE Interfaces</td>
<td>2 GE Interfaces</td>
</tr>
<tr>
<td>4.000 User im HA-Modus</td>
<td>GE Mgmt Port</td>
<td>GE Mgmt Port</td>
</tr>
<tr>
<td>* Lifetime Warraty</td>
<td>4.096 User</td>
<td>4.096 User</td>
</tr>
<tr>
<td></td>
<td>8.192 User im HA-Modus</td>
<td>8.192 User im HA-Modus</td>
</tr>
</tbody>
</table>

Elastic V2110: System Limits

Als sogenannte „Elastic Appliance“ lässt sich der virtuelle Controller V2110, mit abgestuften Resourcen der bereitgestellten virtuellen Plattform ausstatten. So ergeben sich 3 Skalierungsvarianten mit unterschiedliche hohen Eckdaten für die Anzahl von Accesspoints und Benutzern.
Spezifikationen und Bestellinformationen unter www.extremenetworks.com/products/wireless

**ExtremeWireless Radar**

Zu ExtremeWireless Radar gehören folgende Komponenten:


- **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 ExtremeMangementCenter möglich.

**Bestellinformationen ExtremeWireless Radar:**

<table>
<thead>
<tr>
<th>Radar Capacity Upgrades</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-RADAR-1</td>
<td>Radar capacity for C25 and V2110. Adds Radar capacity for 1 access point.</td>
</tr>
<tr>
<td>WS-RADAR-16</td>
<td>Radar capacity for C25 and V2110. Adds Radar capacity for 16 access points.</td>
</tr>
<tr>
<td>WS-RADAR-100</td>
<td>Radar capacity for C5210. Adds Radar capacity for 100 access points.</td>
</tr>
</tbody>
</table>

**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.


**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**


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-WALL03 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.

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 Schienenausführung an abgehängten Decken sind ebenfalls Bestandteil des Lieferumfanges.
Hier ein Beispielschema für die Deckenmontage (Genaue Daten entnehmen Sie bitte den Installation Guides im Extranet).

Als robuster 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.

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**


**Alle Systeme der S-Serie auf einen Blick:**

<table>
<thead>
<tr>
<th></th>
<th>SSA 130</th>
<th>SSA 180</th>
<th>S1</th>
<th>S3</th>
<th>S4</th>
<th>S6</th>
<th>S8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis-Slots</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Switching-Kapazität Gesamtsystem (Gbps)</td>
<td>40</td>
<td>120</td>
<td>320</td>
<td>360</td>
<td>1280</td>
<td>1920</td>
<td>2560</td>
</tr>
<tr>
<td>Switching-Durchsatz Gesamtsystem (Mpps)</td>
<td>30</td>
<td>90</td>
<td>240</td>
<td>360</td>
<td>960</td>
<td>1440</td>
<td>1920</td>
</tr>
<tr>
<td>Gesamte Backplane-Kapazität (Gbps)</td>
<td>-</td>
<td>-</td>
<td>320</td>
<td>525</td>
<td>3000</td>
<td>7000</td>
<td>9500</td>
</tr>
<tr>
<td>10/10/1000BASE-TX Class 3 PoE Ports pro System (maximal)</td>
<td>48</td>
<td>48</td>
<td>72</td>
<td>216</td>
<td>288</td>
<td>432</td>
<td>576</td>
</tr>
<tr>
<td>1000BASE-X SFP (MGBIC) Ports Pro System (maximal)</td>
<td>-</td>
<td>48</td>
<td>72</td>
<td>180</td>
<td>288</td>
<td>432</td>
<td>576</td>
</tr>
<tr>
<td>10GBASE-X SFP+ Ports pro System (maximal)</td>
<td>4</td>
<td>4</td>
<td>24</td>
<td>96</td>
<td>112</td>
<td>168</td>
<td>232</td>
</tr>
<tr>
<td>40GBase-X QSFP+ Ports pro System (maximal)</td>
<td>-</td>
<td>-</td>
<td>6</td>
<td>-</td>
<td>24</td>
<td>36</td>
<td>48</td>
</tr>
</tbody>
</table>

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.

**Architektur**


**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.


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
  o Zugriffskontrolle auf Cloud Service wie z. B. www.salesforce.com
  o 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

Distribution, Core und Data Center I/O Module

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.


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.


**EEE Energy Efficient Ethernet**

Im Netzwerk und speziell im Data Center steigt der Datendurchsatz täglich. Um diesem Zustand Rechnung zu tragen, werden heutige Netzwerkeinstellungen 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


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

<table>
<thead>
<tr>
<th>Network Applications</th>
<th>S130 Class I/O Modules</th>
<th>S140 I/O Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Part Number</strong></td>
<td>ST4106-0248</td>
<td>ST2206-0848A</td>
</tr>
<tr>
<td></td>
<td>SG4101-0248</td>
<td>SG2201-0848</td>
</tr>
<tr>
<td><strong>Used in</strong></td>
<td>S3/S4/S6/S8 Chassis</td>
<td>S3/S4/S6/S8 Chassis</td>
</tr>
<tr>
<td><strong>Port Type</strong></td>
<td>RJ 45</td>
<td>RJ 45</td>
</tr>
<tr>
<td></td>
<td>SFP</td>
<td>SFP</td>
</tr>
<tr>
<td></td>
<td>SFP</td>
<td>SFP+</td>
</tr>
<tr>
<td></td>
<td>10GBase-T</td>
<td></td>
</tr>
<tr>
<td><strong>Port Quantity</strong></td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>24</td>
</tr>
<tr>
<td><strong>Port Speed</strong></td>
<td>10/100/1000 Mbps</td>
<td>100 Mbps</td>
</tr>
<tr>
<td></td>
<td>100 Mbps</td>
<td>10 Gbps</td>
</tr>
<tr>
<td></td>
<td>10 Gbps</td>
<td>10 Gbps</td>
</tr>
<tr>
<td><strong>PoE Support</strong></td>
<td>802.3af, 802.3at</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>802.3af, 802.3at</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Option Module Slots</strong></td>
<td>1, (Type 1)</td>
<td>2, (Type 2)</td>
</tr>
<tr>
<td></td>
<td>2, (Type 2)</td>
<td>-</td>
</tr>
<tr>
<td><strong>Module Throughput</strong></td>
<td>30 Mpps</td>
<td>120 Mpps</td>
</tr>
<tr>
<td></td>
<td>120 Mpps</td>
<td>120 Mpps</td>
</tr>
<tr>
<td></td>
<td>120 Mpps</td>
<td>120 Mpps</td>
</tr>
<tr>
<td><strong>I/O Switching Capacity</strong></td>
<td>40 Gbps</td>
<td>160 Gbps</td>
</tr>
<tr>
<td></td>
<td>40 Gbps</td>
<td>160 Gbps</td>
</tr>
<tr>
<td></td>
<td>160 Gbps</td>
<td>160 Gbps</td>
</tr>
<tr>
<td></td>
<td>160 Gbps</td>
<td>160 Gbps</td>
</tr>
</tbody>
</table>

## S180 I/O Modules

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

Seite 138 von 264
### I/O Fabric Modul Spezifikationen

<table>
<thead>
<tr>
<th>S130 Class Fabric Mod.</th>
<th>S180 Class I/O Fabric Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wiring Closet, Distribution Layer, Small Network Core</td>
<td>Distribution Layer, Server Aggregation, Data Center Core, Enterprise</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part Number</th>
<th>ST4106-0248-F6</th>
<th>ST8206-0848-F8A</th>
<th>SG8201-0848-F8</th>
<th>SK8008-1224-F8</th>
<th>SK8009-1224-F8</th>
<th>SL8013-1206-F8A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Type</td>
<td>RJ 45</td>
<td>RJ 45</td>
<td>SFP</td>
<td>SFP+</td>
<td>10GBase-T</td>
<td>QSFP+</td>
</tr>
<tr>
<td>Port Quantity</td>
<td>48</td>
<td>48</td>
<td>48</td>
<td>24</td>
<td>24</td>
<td>6</td>
</tr>
<tr>
<td>Port Speed</td>
<td>10/100/1000 Mbps</td>
<td>10/100/1000 Mbps</td>
<td>1000 Mbps</td>
<td>10 Gbps</td>
<td>10 Gbps</td>
<td>40 Gbps</td>
</tr>
<tr>
<td>PoE Support</td>
<td>802.3af, 802.3at</td>
<td>802.3af, 802.3at</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Option Module Slots</td>
<td>1, (Type 2)</td>
<td>2, (Type 2)</td>
<td>2, (Type 2)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Module I/O Throughput</td>
<td>45 Mpps</td>
<td>120 Mpps</td>
<td>120 Mpps</td>
<td>240 Mpps</td>
<td>240 Mpps</td>
<td>240 Mpps</td>
</tr>
<tr>
<td>I/O Switching Capacity</td>
<td>60 Gbps</td>
<td>160 Gbps</td>
<td>160 Gbps</td>
<td>320 Gbps</td>
<td>320 Gbps</td>
<td>320 Gbps</td>
</tr>
<tr>
<td>Fabric Throughput (Single)</td>
<td>480 Mpps</td>
<td>960 Mpps</td>
<td>960 Mpps</td>
<td>960 Mpps</td>
<td>960 Mpps</td>
<td>960 Mpps</td>
</tr>
</tbody>
</table>

### Chassis Modellinformationen:

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S8-Chassis</td>
<td>S-Series S8 Chassis and fan trays (Power supplies ordered separately)</td>
</tr>
<tr>
<td>S8-Chassis-POE4</td>
<td>S-Series S8 Chassis and fan trays with 4 bay PoE subsystem (System and PoE Power supplies ordered separately)</td>
</tr>
<tr>
<td>S8-Chassis-POE8</td>
<td>S-Series S8 Chassis and fan trays with 8 bay PoE subsystem (System and PoE Power supplies ordered separately)</td>
</tr>
<tr>
<td>S8-POE-8BAY-UGK</td>
<td>S-Series 8 bay PoE upgrade kit for the S8 (PoE Power supplies ordered separately)</td>
</tr>
<tr>
<td>Model</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>S8-POE-4BAY-UGK</td>
<td>S-Series 4 bay PoE upgrade kit for the S8 (PoE Power supplies ordered separately)</td>
</tr>
<tr>
<td>S8-Midmount-Kit</td>
<td>S-Series S8 Chassis 19” midmount installation rack kit can be used with all S8 chassis types</td>
</tr>
<tr>
<td><strong>S6 Chassis</strong></td>
<td></td>
</tr>
<tr>
<td>S6-Chassis</td>
<td>S-Series S6 Chassis and fan trays. Front to back cooling. (Power supplies ordered separately)</td>
</tr>
<tr>
<td>S6-Chassis-POE4</td>
<td>S-Series S6 Chassis and fan tray with 4 bay POE subsystem. Front to back cooling. (System and PoE power supplies ordered separately)</td>
</tr>
<tr>
<td>S6-Midmount-Kit</td>
<td>S-Series S6 Chassis 19” midmount installation rack kit, can be used with all S6 Chassis types</td>
</tr>
<tr>
<td>S6-FAN</td>
<td>S-Series Fan Tray (For use w/ S6)</td>
</tr>
<tr>
<td><strong>S4 Chassis</strong></td>
<td></td>
</tr>
<tr>
<td>S4-Chassis</td>
<td>S-Series S4 Chassis and fan tray (Power supplies added separately)</td>
</tr>
<tr>
<td>S4-Chassis-POE4</td>
<td>S-Series S4 Chassis and fan tray with 4 bay PoE subsystem (System and PoE Power supplies ordered separately)</td>
</tr>
<tr>
<td>S4-POE-4BAY-UGK</td>
<td>S-Series 4 bay PoE upgrade kit for the S4 (PoE Power supplies ordered separately)</td>
</tr>
<tr>
<td>S4-Midmount-Kit</td>
<td>S-Series S4 Chassis 19” midmount installation rack kit, can be used with all S4 Chassis types</td>
</tr>
<tr>
<td><strong>S3 Chassis</strong></td>
<td></td>
</tr>
<tr>
<td>S3-Chassis-A</td>
<td>S-Series S3 Chassis and fan tray (Power supplies ordered separately)</td>
</tr>
<tr>
<td>S3-Chassis-POE4</td>
<td>S-Series S3 Chassis and Fan Tray with 4 bay PoE subsystem (System and PoE Power supplies ordered separately)</td>
</tr>
<tr>
<td>S3-POE-4BAY-UGK</td>
<td>S-Series 4 bay PoE upgrade kit for the S3 (PoE Power supplies ordered separately)</td>
</tr>
<tr>
<td>S3-Midmount-Kit</td>
<td>S-Series S3 Chassis 19” midmount installation rack kit, can be used with all S3 Chassis types</td>
</tr>
<tr>
<td><strong>S1 Chassis</strong></td>
<td></td>
</tr>
<tr>
<td>S1-Chassis-A</td>
<td>S-Series S1 Chassis and fan tray. Compatible with Fabric Modules only. (SSA 1000W Power supplies ordered separately)</td>
</tr>
<tr>
<td>S1-Mount-Kit</td>
<td>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.</td>
</tr>
<tr>
<td>S1-FAN-A</td>
<td>S1Chassis fan tray, Spare (For use w/ S1)</td>
</tr>
<tr>
<td><strong>Power Supplies and Fans</strong></td>
<td></td>
</tr>
<tr>
<td>S-AC-PS</td>
<td>S-Series AC power supply, 20A 100-240 VAC input (1200W/1600W) (For use w/ S3/S4/S6/S8)</td>
</tr>
<tr>
<td>S-AC-PS-15A</td>
<td>S-Series AC power supply, 15A, 100-240 VAC input, (930W/1600W) (For use w/ S3/S4/S6/S8)</td>
</tr>
<tr>
<td>S-POE-PS</td>
<td>S-Series POE power supply, 20A, 100-240 VAC input, (1200/2000 W) (For Use in 4/8 Bay PoE power subsystems)</td>
</tr>
</tbody>
</table>
### I/O und I/O Fabric Modulinformationen

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>S130 I/O Fabric Modules</strong></td>
<td></td>
</tr>
<tr>
<td>ST4106-0348-F6</td>
<td>S-Series I/O-Fabric S130 Class Module, 1280Gpbs Load Sharing -48Ports 10/100/1000Base-TX via RJ 45 with PoE (802.3at) and one Type2 option slot (used in S1/S4/S6/S8)</td>
</tr>
<tr>
<td><strong>S130 I/O Modules</strong></td>
<td></td>
</tr>
<tr>
<td>ST4106-0248</td>
<td>S-Series I/O S130 Class Module - 48 Ports 10/100/1000BASE-T via RJ 45 with PoE (802.3at) and one Type1 option slot (Used in S3/S4/S6/S8)</td>
</tr>
<tr>
<td>SG4101-0248</td>
<td>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)</td>
</tr>
<tr>
<td><strong>S140 I/O Modules</strong></td>
<td></td>
</tr>
<tr>
<td>ST2206-0848</td>
<td>S-Series S140 I/O Module - 48 Ports 10/100/1000BASE-T via RJ 45 with PoE (802.3at) and two Type2 option slot (Used in S3/S4/S6/S8)</td>
</tr>
<tr>
<td>SG2201-0848</td>
<td>S-Series S140 I/O Module - 48 Ports 1000BASE-X ports via SFP and two Type2 option slot (Used in S3/S4/S6/S8)</td>
</tr>
<tr>
<td><strong>S180 I/O Fabric Modules</strong></td>
<td></td>
</tr>
<tr>
<td>SL8013-1206-F8A</td>
<td>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)</td>
</tr>
<tr>
<td>SKL8008-0810-F8</td>
<td>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)</td>
</tr>
<tr>
<td>SK8208-0808-F8</td>
<td>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)</td>
</tr>
<tr>
<td>SK8008-1224-F8</td>
<td>S-Series S180 Class I/O-Fabric Module, Load Sharing - 24 Ports 10GBASE-X via SFP+, 4 ports VSB via SFP+ (Used in S1A/S4/S6/S8)</td>
</tr>
<tr>
<td>SK8009-1224-F8</td>
<td>S-Series S180 Class I/O-Fabric Module, Load Sharing - 24 Ports 10GBASE-T via RJ 45, 4 ports VSB via SFP+ (Used in S1A/S4/S6/S8)</td>
</tr>
<tr>
<td>ST8206-0848-F8A</td>
<td>S-Series S180 Class I/O-Fabric Module, Load Sharing - 48 Ports 10/100/1000BASE-T via RJ 45 with PoE (802.3at) and two Type2 option slots (Used in S1/S4/S6/S8)</td>
</tr>
<tr>
<td>SG8201-0848-F8</td>
<td>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)</td>
</tr>
<tr>
<td><strong>S180 I/O Modules</strong></td>
<td></td>
</tr>
<tr>
<td>SL8013-1206A</td>
<td>S-Series S180 Class I/O Module - 6 Ports 40GBASE-X Ethernet via QSFP, VSB expansion slot (Used in S4/S6/S8)</td>
</tr>
<tr>
<td>SK8008-1224</td>
<td>S-Series S180 Class I/O Module - 24 Ports 10GBASE-X via SFP+, VSB expansion slot (Used in S4/S6/S8)</td>
</tr>
</tbody>
</table>
### Option Modules

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SK8009-1224</td>
<td>S-Series S180 Class I/O Module - 24 Ports 10GBASE-T via RJ45, VSB expansion slot (Used in S4/S6/S8)</td>
</tr>
<tr>
<td>SOK2208-0102</td>
<td>S-Series Option Module (Type1) - 2 10GBASE-X Ethernet ports via SFP+ (Compatible with Type1&amp;Type2 option slots)</td>
</tr>
<tr>
<td>SOK2208-0104</td>
<td>S-Series Option Module (Type1) - 4 10GBASE-X Ethernet ports via SFP+ (Compatible with Type1&amp;Type2 option slots)</td>
</tr>
<tr>
<td>SOK2208-0204</td>
<td>S-Series Option Module (Type2) - 4 10GBASE-X Ethernet ports via SFP+ (Compatible with Type2 option slots)</td>
</tr>
<tr>
<td>SOK2209-0204</td>
<td>S-Series Option Module (Type2) - 4 10GBASE-T RJ45 ports with PoE+Support (Compatible with Type2 option slots)</td>
</tr>
<tr>
<td>SOG2201-0112</td>
<td>S-Series Option Module (Type1) - 12 1000BASE-X ports via SFP (Compatible with Type1&amp;Type2 option slots)</td>
</tr>
<tr>
<td>SOT2206-0112</td>
<td>S-Series Option Module (Type1) - 12 Ports 10/100/1000BASE-TX via RJ 45 with PoE (802.3at) (Compatible with Type1&amp;Type2 option slots)</td>
</tr>
<tr>
<td>SOTK2268-0212</td>
<td>S-Series Option Module (Type2) - 10 Ports 10/100/1000BASE-T via RJ 45 with PoE and 2 ports 10GBASE-X via SFP+ (Compatible with Type2 option slots)</td>
</tr>
<tr>
<td>SOGK22B-0212</td>
<td>S-Series Option Module (Type2) - 10 Ports 1000BASE-X via SFP and 2 ports 10GBASE-X via SFP+ (Compatible with Type2 option slots)</td>
</tr>
<tr>
<td>SOV3208-0202</td>
<td>S-Series Option Module (Type2) - 2 port VSB Option Module (Compatible with Type2 option slots on S140/S180 modules only)</td>
</tr>
<tr>
<td>SOV3008-0404</td>
<td>S-Series VSB Expansion Module - 4 port VSB Module (Compatible with S180 Class 10Gb/40Gb I/O modules only)</td>
</tr>
</tbody>
</table>

### SSA & Lizenzmodellinformationen

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSA S130 (S-Series Stand Alone)</td>
<td>S-Series Stand Alone (SSA) - S130 Class - 48 Ports 10/100/1000BASE-T via RJ 45 with PoE (802.3at) and 4 10GBASE-X Ethernet ports via SFP+ (Power supplies not included - Please order separately)</td>
</tr>
<tr>
<td>SSA-AC-PS-625W</td>
<td>S-Series Standalone (SSA S130 Class) - AC power supply, 15A, 100-240VAC input, (625W)</td>
</tr>
<tr>
<td>SSA-AC-PS-1000W</td>
<td>S-Series Standalone (SSA S130 Class) and S1-Chassis - AC and POE power supply, 15A, 100-240VAC input, (1000/1200W)</td>
</tr>
<tr>
<td>SSA-FAN-KIT</td>
<td>S-Series Stand Alone (SSA S130 Class) - Replacement fan assembly (Single Fan)</td>
</tr>
<tr>
<td>SSA S180 (S-Series Stand Alone)</td>
<td>S-Series S180 Class Standalone (SSA) - 48 Ports 10/10/1000BASE-T via RJ 45 and 4 ports 10GBASE-X via SFP+, Front to Back cooling (Power supplies not included - Please order separately)</td>
</tr>
</tbody>
</table>
### Optional Licenses

<table>
<thead>
<tr>
<th>License Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-EOS-L3-S130</td>
<td>S-Series Advanced Routing License (For use on S130 Class Modules) (Enables VRF, BGP, Tunneling)</td>
</tr>
<tr>
<td>S-EOS-PPC</td>
<td>S-Series Per Port User Capacity License Upgrade (For use on S130 Class Modules)</td>
</tr>
<tr>
<td>S-EOS-VSB</td>
<td>S-Series Multi-slot Virtual Switch Bonding License Upgrade (For use on S130/S140 Class Modules)</td>
</tr>
<tr>
<td>SSA-EOS-VSB</td>
<td>S-Series SSA Virtual Switch Bonding License Upgrade (For use on SSA Only)</td>
</tr>
<tr>
<td>SSA-EOS-2XUSER</td>
<td>SSA-S180 double user capacity license</td>
</tr>
<tr>
<td>S1-EOS-VSB</td>
<td>S-Series S1 Chassis Virtual Switch Bonding License Upgrade (For use on S1-Chassis-A / S1-Chassis Only)</td>
</tr>
</tbody>
</table>

### K-Serie

**Überblick**


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

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.


**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**

**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.


Authentifizierung bietet Sicherheit, Priorität und Bandbreitenkontrolle bei gleichzeitigem Schutz bestehender Netzwerkinvestitionen.

**Dynamische, flowbasierte Paketklassifizierung**

**Netzwerktransparenz durch präzise NetFlow Daten**

**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 Queing), 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
o Umfangreiche Industriestandard-Compliance (IEEE und IETF)

o Inbound- und Outbound-Bandbreitenkontrolle per Flow

o VLAN-Serviceunterstützung

o Link Aggregation (IEEE 802.3ad)

o Multiple Spanning Trees (IEEE 802.1s)

o Schnelle Rekonfiguration von Spanning Trees (IEEE 802.1w)

o Provider Bridges (IEEE 802.1ad), Q-in-Q Ready

o Flow Setup Throttling

- Verteiltes IP Routing – bietet dynamische Verkehrsoptimierung, Broadcast Eindämmung und effizientere Netzwerkausfallsicherheit

  o Zu den Standard-Routing-Features gehören statische Routen, RIPv1/2, IPv4 und Multicast Routing Unterstützung (DVMRP, IGMP v1/v2/v3), Policy-basiertes Routing und Route Maps, VRRP

  o Zu den lizenzierten Routing-Features gehören OSFP v1/v2, PIM-SM und IPv6

  o Erweiterte ACLs

- Sicherheit (Nutzer, Netzwerk und Management)

  o Nutzersicherheit

    - Authentifizierung (802.1x, MAC, PWA+ und CEP), MAC (statisch und dynamisch) Port Locking

    - Multiuser Authentifizierung / Policies

  o Netzwerksicherheit

    - Einfache und erweiterte ACLs

    - Policy-basierte Sicherheitsservices (Beispiel: Spoofing, nicht unterstützter Protokollzugang, Intrusion Prevention, DoS-Attacken-Limitierung)

    - Management-Sicherheit

  o Sicherer Zugang zur K-Serie via SSH, SSL, SNMP v3

- Management, Kontrolle und Analyse – bietet modernisierte Werkzeuge, um Netzwerkverfügbarheit und -zustand zu bewahren

  o Konfiguration

    - Industriestandard CLI und Web-Management Unterstützung

    - Multiple Firmware-Images mit editierbaren Konfigurationsdateien

  o 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

  o 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


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.


**Komponenten**

<table>
<thead>
<tr>
<th>Part Number</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>K6 Chassis</strong></td>
<td></td>
</tr>
<tr>
<td>K6-Chassis</td>
<td>K-Series 6 Slot Chassis and Fan Tray</td>
</tr>
<tr>
<td>K6-FAN</td>
<td>K6 Fan Tray - Spare</td>
</tr>
<tr>
<td>K6-MID-KIT</td>
<td>K6 Mid-Mount Kit</td>
</tr>
<tr>
<td><strong>K10 Chassis</strong></td>
<td></td>
</tr>
<tr>
<td>K10-Chassis</td>
<td>K-Series 10 Slot Chassis and Fan Tray</td>
</tr>
<tr>
<td>K10-FAN</td>
<td>K10 Fan Tray - Spare</td>
</tr>
<tr>
<td>K10-MID-KIT</td>
<td>K10 Mid-Mount Kit</td>
</tr>
<tr>
<td><strong>Power Supplies and Accessories</strong></td>
<td></td>
</tr>
<tr>
<td>K-AC-PS</td>
<td>K-Series Power Supply, 15A, 100-240VAC input, (600W system, 400/800W POE)</td>
</tr>
<tr>
<td>K-POE-4BAY</td>
<td>K-Series External 4 Bay Power Shelf</td>
</tr>
<tr>
<td>K-POE-4BAY-RAIL</td>
<td>Mounting Kit for K-POE-4BAY</td>
</tr>
</tbody>
</table>
### I/O Fabric Modules

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KK2008-0204-F2</td>
<td>K10 Management/Fabric Module (4) 10GB via SFP+</td>
</tr>
<tr>
<td>KK2008-0204-F2G</td>
<td>K10 Management/Fabric Module (4) 10GB via SFP+(TAA Compliant)</td>
</tr>
<tr>
<td>KK2008-0204-F1</td>
<td>K6 Management/Fabric Module (4) 10GB via SFP+</td>
</tr>
<tr>
<td>KK2008-0204-F1G</td>
<td>K6 Management/Fabric Module (4) 10GB via SFP+(TAA Compliant)</td>
</tr>
</tbody>
</table>

### I/O Modules

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KT2006-0224</td>
<td>K-Series (24) Port 10/100/1000 802.3at RJ 45 PoE IOM</td>
</tr>
<tr>
<td>KT2006-0224-G</td>
<td>K-Series (24) Port 10/100/1000 802.3at RJ 45 PoE IOM (TAA Compliant)</td>
</tr>
<tr>
<td>KT2010-0224</td>
<td>K-Series (24) Port 10/100/1000 802.3at Mini-RJ 21PoE IOM</td>
</tr>
<tr>
<td>KT2010-0224-G</td>
<td>K-Series (24) Port 10/100/1000 802.3at Mini-RJ 21PoE IOM (TAA Compliant)</td>
</tr>
<tr>
<td>KG2001-0224</td>
<td>K-Series (24) Port 1Gb SFP IOM</td>
</tr>
<tr>
<td>KG2001-0224-G</td>
<td>K-Series (24) Port 1Gb SFP IOM (TAA Compliant)</td>
</tr>
<tr>
<td>KK2008-0204</td>
<td>K-Series (4) Port 1Gb SFP+ IOM</td>
</tr>
</tbody>
</table>

### Licenses

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>K-EOS-L3</td>
<td>Advanced Routing License (OSPF, VRF, PIM-SM)</td>
</tr>
<tr>
<td>K-EOS-PPC</td>
<td>K-Series Per Port User Capacity License Upgrade</td>
</tr>
</tbody>
</table>

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

[www.extremenetworks.com/product/k-series](http://www.extremenetworks.com/product/k-series)

**BDX8**

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 Verzug 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 RJ 45 (oder alternativ 1GbE SFP), 768 10GbE SFP+, 192 40GbE QSFP+ oder 32 100GbE CFP2 blockierungsfreie Ports in einem Chassis. Dies ermöglicht Portdichten bis zu 1152 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 128 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 1Mio.) 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 virtualisierungsunterstützende 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.


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 garantiert 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

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)


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**


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 100/100/10000MbE RJ 45 oder 10Gbe SFP(+) pro Switch, bis zu 1152 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 1Mio Hardware Einträgen L2/L3
- Software Defined Networking mit OpenFlow 13 und OpenStack Unterstützung
- Enterprise und IXP fokuserter 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**

<table>
<thead>
<tr>
<th>Bestellnummer</th>
<th>Produktbezeichnung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>48001</td>
<td>BDX8-AC</td>
<td>BlackDiamond X8 Serie Chassis mit 8 Einschubslots. Das Chassis enthält die 5 zum Betrieb benötigten Lüfter Baugruppen. Power Supplys und Blank Panels für nicht benutzte Einschubslot müssen separat bestellt werden</td>
</tr>
<tr>
<td>48021</td>
<td>BDX-MM1</td>
<td>Management Module 1 für die BlackDiamond X Serie. Benötigt wird mindestens 1 MM1 Module, 2 Modules werden für optionale 1+1 Redundanz benötigt</td>
</tr>
<tr>
<td>48032</td>
<td>BDXA-FM10T</td>
<td>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 Performance</td>
</tr>
<tr>
<td>48031</td>
<td>BDXA-FM20T</td>
<td>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 Performance</td>
</tr>
<tr>
<td>48040</td>
<td>BDXA-10G48T</td>
<td>48-Port 10BASE-T RJ 45 Module für die BlackDiamond X Serie. Bis zu 8 Module werden pro Chassis unterstützt. Es stehen damit bis zu 384 wirespeed 100/100/10000 MbE (10Gbe) Kupfer Ports zur Verfügung. Das Modul wird von den 2,56 oder 5,12Tbps Fabric Modules unterstützt</td>
</tr>
<tr>
<td>48041</td>
<td>BDXA-10G48X</td>
<td>48-Port 10BASE-X SFP+ Module für die BlackDiamond X Serie. Bis zu 8 Module werden pro Chassis unterstützt. Es stehen damit bis zu 384 wirespeed 100/1000 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</td>
</tr>
<tr>
<td>48046</td>
<td>BDXA-40G12X</td>
<td>12-Port 40BASE-X QSFP+ Module für die BlackDiamond X Serie. Bis zu 8 Module werden pro Chassis unterstützt. Es stehen damit bis zu 96 wirespeed 40GbE Ports oder 384 wirespeed 10 Gbe Ports zur Verfügung.</td>
</tr>
</tbody>
</table>
Das Modul wird von den 2,56 oder 5,12Tbps Fabric Modules unterstützt. Optiken und Kabel sind optional erhältlich.

<table>
<thead>
<tr>
<th>Code</th>
<th>Modul</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>48047</td>
<td>BDXA-40G12X-XL</td>
<td>12-Port 40GBASE-X QSFP+ Module für die BlackDiamond X Serie, wie oben beschrieben. Erweiterte Kapazitäten mit bis zu 1Mio TCAMS für den Einsatz in komplexen Szenarien.</td>
</tr>
<tr>
<td>48061</td>
<td>BDXB-100G4X</td>
<td>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.</td>
</tr>
<tr>
<td>48062</td>
<td>BDXB-100G4X-XL</td>
<td>4-Port 100GBASE-X CFP2 Module für die BlackDiamond X Serie, wie oben beschrieben. Erweiterte Kapazitäten mit bis zu 1Mio TCAMS für den Einsatz in komplexen Szenarien.</td>
</tr>
<tr>
<td>48011</td>
<td>BDX-PSU-AC2500</td>
<td>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.</td>
</tr>
</tbody>
</table>

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:
www.extremenetworks.com/product/blackdiamond-x-series

**BD8000**


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**

**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**

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 1000-Base-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


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 den 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).


**Überzeugende Portdichten**

### 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
- Common Criteria EAL3+ Certified
<table>
<thead>
<tr>
<th>8806 Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>8810 Chassis</td>
</tr>
<tr>
<td>MSM Modul</td>
</tr>
<tr>
<td>S-10G1Xc Modul</td>
</tr>
<tr>
<td>S-10G2Xc Modul</td>
</tr>
<tr>
<td>S-G8Xc Modul</td>
</tr>
<tr>
<td>8900-10G24X-c Modul</td>
</tr>
<tr>
<td>8900-40G6X-xm Modul</td>
</tr>
<tr>
<td>8900-xl Module</td>
</tr>
<tr>
<td>8800-G48Xc Modul</td>
</tr>
</tbody>
</table>
### Bestellinformationen

<table>
<thead>
<tr>
<th>Bestellnummer</th>
<th>Produktbezeichnung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>41011</td>
<td>10-Slot Chassis</td>
<td>BlackDiamond 8810 10-Slot Chassis mit Lüfter Modul</td>
</tr>
<tr>
<td>41012</td>
<td>6-Slot Chassis</td>
<td>BlackDiamond 8806 6-Slot Chassis mit Lüfter Modul</td>
</tr>
<tr>
<td>60020</td>
<td>700W/1200W 100-240V PSU</td>
<td>BlackDiamond 8800 700W/1200W 100-240V Netzteil</td>
</tr>
<tr>
<td>41050</td>
<td>600W/900W PSU</td>
<td>BlackDiamond 8806 600W/900W 100-240V Netzteil</td>
</tr>
<tr>
<td>60021</td>
<td>1200W -48V DC PSU</td>
<td>BlackDiamond 8808/BlackDiamond 8800 1200W -48V DC Netzteil</td>
</tr>
<tr>
<td>41231</td>
<td>8900-MSM128</td>
<td>BlackDiamond 8900 Management Switch Module mit Erweiterungsflot für ein MSM Uplink Modul</td>
</tr>
<tr>
<td>41213</td>
<td>MSM-48c</td>
<td>BlackDiamond 8800 Management Switch Module mit Erweiterungsflot für ein MSM Uplink Modul</td>
</tr>
<tr>
<td>41251</td>
<td>8500-MSM24</td>
<td>BlackDiamond 8500 Management Switch Module mit Erweiterungsflot für ein MSM Uplink Modul</td>
</tr>
<tr>
<td>41711</td>
<td>8900-40G6X-xm</td>
<td>BlackDiamond 8900-xm 6-Port 40GBASE-X Modul mit QSFP+ Ports</td>
</tr>
<tr>
<td>41631</td>
<td>8900-10G8X-xl</td>
<td>BlackDiamond 8900 8-Port 10GBASE-X Modul mit XFP Ports</td>
</tr>
<tr>
<td>41531</td>
<td>8900-G48T-xl</td>
<td>BlackDiamond 8900 48-Port 10/100/1000BASE-T RJ-45 Modul, optional erweiterbar auf PoE 802.3af per PoE card (S-PoE)</td>
</tr>
<tr>
<td>41521</td>
<td>8900-G48X-xl</td>
<td>BlackDiamond 8900 48-Port 1000BASE-X Modul mit SFP Ports</td>
</tr>
<tr>
<td>41632B</td>
<td>8900-10G24X-c</td>
<td>BlackDiamond 8900 24-Port 10GBASE-X SFP+Modul</td>
</tr>
<tr>
<td>41532</td>
<td>8900-G96T-c</td>
<td>BlackDiamond 8900 96-port 10/100/1000BASE-T MRJ-21</td>
</tr>
<tr>
<td>41516</td>
<td>G48Te2</td>
<td>BlackDiamond 8800 48-port 10/100/1000BASE-T RJ-45 Modul, optional erweiterbar auf PoE 802.3af per PoE card (S-PoE)</td>
</tr>
<tr>
<td>41517</td>
<td>G48Tc</td>
<td>BlackDiamond 8800 48-port 10/100/1000BASE-T RJ-45 Modul, optional erweiterbar auf PoE 802.3af per PoE card (S-PoE)</td>
</tr>
<tr>
<td>41543</td>
<td>G24Xc</td>
<td>BlackDiamond 8800 24-Port 1000BASE-X Modul mit SFP</td>
</tr>
<tr>
<td>41544</td>
<td>G48Xc</td>
<td>BlackDiamond 8800 48-Port 1000BASE-X Modul mit SFP</td>
</tr>
<tr>
<td>I/O Modules BlackDiamond 8500-Series Modules</td>
<td>I/O Modules BlackDiamond 8500-Series Modules</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>4151 8500-G48T-e</td>
<td>BlackDiamond 8500 48-Port T/100/1000BASE-T RJ -45 Modul, optional erweiterbar auf PoE 802.3af per PoE card (S-PoE)</td>
<td></td>
</tr>
<tr>
<td>41561 8500-G24X-e</td>
<td>BlackDiamond 8500 24-port 1000BASE-X SFP</td>
<td></td>
</tr>
<tr>
<td>MSM-Uplink Module</td>
<td>MSM-Uplink Module</td>
<td></td>
</tr>
<tr>
<td>41B21 S-G8Xc</td>
<td>BlackDiamond 8800 8-Port 1G SFP Add-On Einschub für MSM</td>
<td></td>
</tr>
<tr>
<td>41B22 S-DG1Xc</td>
<td>BlackDiamond 8800 1-port DG XFP Add-On Einschub für MSM</td>
<td></td>
</tr>
<tr>
<td>41B23 S-DG2Xc</td>
<td>BlackDiamond 8800 2-port DGBASE-X SFP+Add-On Einschub für MSM</td>
<td></td>
</tr>
<tr>
<td>41B11 S-PoE</td>
<td>BlackDiamond 8800 PoE Add-On Einschub für RJ 45 Module</td>
<td></td>
</tr>
</tbody>
</table>


**X 770**


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 Hoheneinheit 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**

**SummitStack-V160/V320 – Flexibles Stacking über 40 Gigabit Schnittstellen**

**Intelligentes Switching**

**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 gegebenfalls 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

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

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

<table>
<thead>
<tr>
<th>Bestellnummer</th>
<th>Produktbezeichnung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>17701</td>
<td>Summit X770-32q-FB-AC</td>
<td>32 40GBASE-X QSFP+ Ports (ohne Optiken) , ExtremeXOS Advanced Edge Lizenz, 2 Front-to-Back 550W AC Netzteile, 5 Front-to-Back Lüfter</td>
</tr>
<tr>
<td>17702</td>
<td>Summit X770-32q-BF-AC</td>
<td>32 40GBASE-X QSFP+ Ports (ohne Optiken) , ExtremeXOS Advanced Edge Lizenz, 2 Back-to-Front 550W AC Netzteile, 5 Back-to-Front Lüfter</td>
</tr>
<tr>
<td>17703</td>
<td>Summit X770-32q-FB-DC</td>
<td>32 40GBASE-X QSFP+ Ports (ohne Optiken) , ExtremeXOS Advanced Edge Lizenz, 2 Front-to-Back 550W DC Netzteile, 5 Front-to-Back Lüfter</td>
</tr>
<tr>
<td>17704</td>
<td>Summit X770-32q-BF-DC</td>
<td>32 40GBASE-X QSFP+ Ports (ohne Optiken) , ExtremeXOS Advanced Edge Lizenz, 2 Back-to-Front 550W DC Netzteile, 5 Back-to-Front Lüfter</td>
</tr>
<tr>
<td>17705</td>
<td>Summit X770-32q-FB-MIX</td>
<td>32 40GBASE-X QSFP+ Ports (ohne Optiken) , ExtremeXOS Advanced Edge Lizenz, 1 Front-to-Back 550W AC Netzeil, 1 Front-to-Back 550W DC Netzeil, 5 Front-to-Back Lüfter</td>
</tr>
<tr>
<td>17706</td>
<td>Summit X770-32q-BF-MIX</td>
<td>32 40GBASE-X QSFP+ Ports (ohne Optiken) , ExtremeXOS Advanced Edge Lizenz, 1 Back-to-Front 550W AC Netzeil, 1 Back-to-Front 550W DC Netzeil, 5 Back-to-Front Lüfter</td>
</tr>
<tr>
<td>10925</td>
<td>Summit 550W AC PSU FB</td>
<td>550W AC Netzteil für Summit Systeme, Front-to-Back Lüftungsrichtung</td>
</tr>
<tr>
<td>10926</td>
<td>Summit 550W DC PSU FB</td>
<td>550W DC Netzteil für Summit Systeme, Front-to-Back Lüftungsrichtung</td>
</tr>
<tr>
<td>10927</td>
<td>Summit 550W AC PSU BF</td>
<td>550W AC Netzteil für Summit Systeme, Back-to-Front Lüftungsrichtung</td>
</tr>
<tr>
<td>10928</td>
<td>Summit 550W DC PSU BF</td>
<td>550W DC Netzteil für Summit Systeme, Back-to-Front Lüftungsrichtung</td>
</tr>
<tr>
<td>17111</td>
<td>Summit X670 Lüfter Modul FB</td>
<td>Lüfter Modul für Summit X670 &amp; X770 Systeme, Front-to-Back Lüftungsrichtung</td>
</tr>
<tr>
<td>17112</td>
<td>Summit X670 Lüfter Modul BF</td>
<td>Lüfter Modul für Summit X670 &amp; X770 Systeme, Back-to-Front Lüftungsrichtung</td>
</tr>
</tbody>
</table>

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

X 670


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 Netzteileinbauplätze.


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

SummitStack-V80/V160/V320 – Flexibles Stacking über 40 Gigabit

Intelligentes Switching

Audio Video Bridging (AVB)

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 Latenzzzeiten kleiner 1ms 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**

**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 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)

<table>
<thead>
<tr>
<th>Bestellnummer</th>
<th>Produktbezeichnung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>17101</td>
<td>Summit X670V-48x-FB</td>
<td>48 10GBASE-X SFP+Ports, rückseitiger VIM4 Einschubslot (unbestückt), ExtremeXOS Advanced Edge Lizenz, 2 Netzteil Einschubplätze (unbestückt), Front-to-Back Lüftungsrichtung, 3 Lüftereinschubmodule enthalten</td>
</tr>
<tr>
<td>17102</td>
<td>Summit X670V-48x-BF</td>
<td>48 10GBASE-X SFP+Ports, rückseitiger VIM4 Einschubslot (unbestückt), ExtremeXOS Advanced Edge Lizenz, 2 Netzteil Einschubplätze (unbestückt), Back-to-Front Lüfter</td>
</tr>
<tr>
<td>17103</td>
<td>Summit X670-48x-FB</td>
<td>48 10GBASE-X SFP+Ports, ExtremeXOS Advanced Edge Lizenz, 2 Netzteil Einschubplätze (unbestückt), Front-to-Back Lüfter</td>
</tr>
<tr>
<td>17104</td>
<td>Summit X670-48x-BF</td>
<td>48 10GBASE-X SFP+Ports, ExtremeXOS Advanced Edge Lizenz, 2 Netzteil Einschubplätze (unbestückt), Back-to-Front Lüfter</td>
</tr>
<tr>
<td>17201</td>
<td>Summit X670V-48t-FB-AC</td>
<td>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</td>
</tr>
<tr>
<td>17202</td>
<td>Summit X670V-48t-BF-AC</td>
<td>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</td>
</tr>
<tr>
<td>Artikelkennung</td>
<td>Produktbeschreibung</td>
<td>Spezifikationen</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>17203</td>
<td>Summit X670V-48t-FB-DC</td>
<td>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</td>
</tr>
<tr>
<td>17204</td>
<td>Summit X670V-48t-BF-DC</td>
<td>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</td>
</tr>
<tr>
<td>17205</td>
<td>Summit X670V-48t-FB-MIX</td>
<td>48 10GBase-T , 48 10GBase-T , 4 10GBase-X (unpopuliert und shared with 4 ports of the 48 10GBase-T ports), one VIM4 slot (unpopuliert), 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</td>
</tr>
<tr>
<td>17206</td>
<td>Summit X670V-48t-BF-MIX</td>
<td>48 10GBase-T , 4 10GBase-X (unpopuliert and shared with 4 ports of the 48 10GBase-T ports), one VIM4 slot (unpopuliert), 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</td>
</tr>
<tr>
<td>10925</td>
<td>Summit 550W AC PSU FB</td>
<td>550W AC Power Supply module for Summit switches, Front-to-Back airflow</td>
</tr>
<tr>
<td>10926</td>
<td>Summit 550W DC PSU FB</td>
<td>550W DC Power Supply module for Summit switches, Front-to-Back airflow</td>
</tr>
<tr>
<td>10927</td>
<td>Summit 550W AC PSU BF</td>
<td>550W AC Power Supply module for Summit switches, Back-to-Front airflow</td>
</tr>
<tr>
<td>10928</td>
<td>Summit 550W DC PSU BF</td>
<td>550W DC Power Supply module for Summit switches, Back-to-Front airflow</td>
</tr>
<tr>
<td>17111</td>
<td>Summit X670 fan module FB</td>
<td>Fan module for Summit X670 series switches, Front-to-Back airflow, spare</td>
</tr>
<tr>
<td>17112</td>
<td>Summit X670 fan module BF</td>
<td>Fan module for Summit X670 series switches, Back-to-Front airflow, spare</td>
</tr>
</tbody>
</table>

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:
www.extremenetworks.com/product/summit-x670-series
X 670-G2


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-V80
- SummitStack-V160
- SummitStack-V320

SummitStack-V – flexibles Stacking über 10 GbE

SummitStack-V80/V160/V320 – Flexibles Stacking über 40 Gigabit Schnittstellen

Intelligentes Switching

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)

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
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

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
<table>
<thead>
<tr>
<th>Bestellnummer</th>
<th>Produktbezeichnung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>17300</td>
<td>Summit X670-G2-72x-Base-Unit</td>
<td>72 10GBASE-X SFP+ Ports frontseitig, ExtremeXOS Advanced Edge Lizenz, 2 unbestückte Netzteilplätze und 5 unbestückte Lüftereinaubplätze</td>
</tr>
<tr>
<td>17310</td>
<td>Summit X670-G2-48x-4q-Base-Unit</td>
<td>48 10GBASE-X SFP+ Ports und 4 40GBASE-X QSFP+ Ports frontseitig, ExtremeXOS Advanced Edge Lizenz, 2 unbestückte Netzteilplätze und 3 unbestückte Lüftereinaubplätze</td>
</tr>
<tr>
<td>10925</td>
<td>Summit 550W AC PSU FB</td>
<td>550W AC Netzteil für Summit Systeme, Front-to-Back Lüftungsrichtung</td>
</tr>
<tr>
<td>10926</td>
<td>Summit 550W DC PSU FB</td>
<td>550W DC Netzteil für Summit Systeme, Front-to-Back Lüftungsrichtung</td>
</tr>
<tr>
<td>10927</td>
<td>Summit 550W AC PSU BF</td>
<td>550W AC Netzteil für Summit Systeme, Back-to-Front Lüftungsrichtung</td>
</tr>
<tr>
<td>10928</td>
<td>Summit 550W DC PSU BF</td>
<td>550W DC Netzteil für Summit Systeme, Back-to-Front Lüftungsrichtung</td>
</tr>
<tr>
<td>17111</td>
<td>Summit X670 Lüfter Modul FB</td>
<td>Lüfter Modul für Summit X670 &amp; X770 Systeme, Front-to-Back Lüftungsrichtung</td>
</tr>
<tr>
<td>17112</td>
<td>Summit X670 Lüfter Modul BF</td>
<td>Lüfter Modul für Summit X670 &amp; X770 Systeme, Back-to-Front Lüftungsrichtung</td>
</tr>
</tbody>
</table>

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:
www.extremenetworks.com/product/summit-x670-series

**X 620**


ideal für den LAN Edge Bereich, kleinere Storage Netzwerke, aber auch kleinere Datacenter.

Dabei unterstützt die X620 Familie das gleiche modulare und robuste Extreme 21x 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**


**Intelligentes Switching**


**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

**Limited Lifetime Warrenty**
Die X620 Serie überzeugt durch niedrige Unterhaltskosten, da die Geräte über limited lifetime warrenty mit Advanced Hardware Replacement (eAHR-2) verfügen.

**Green Design – Energieoptimiertes Design mit flexiblen Kühlungsoptionen**

**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
der Frontseite mit den Ethernetports abgegeben) Lüftungsrichtung zur Verfügung.


<table>
<thead>
<tr>
<th>Bestellnummer</th>
<th>Produktbezeichnung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>17401</td>
<td>X620-16x-Base</td>
<td>16 100Mb/1Gb/10GBASE-X SFP+ ports frontseitig, 2 unbestückte Netzteilplätze und 1 unbestückter Lüftereinbauplatz, ExtremeXOS Edge Lizenz</td>
</tr>
<tr>
<td>17402</td>
<td>X620-16t-Base</td>
<td>12 100Mb/1Gb/10GBASE-T ports mit EEE, 4 100Mb/1Gb/10GBASE-T mit EEE als Combo mit 4 1Gb/10GBASE-X SFP+ ports, 2 unbestückte Netzteilplätze und 1 unbestückter Lüftereinbauplatz, ExtremeXOS Edge Lizenz</td>
</tr>
<tr>
<td>10945</td>
<td>Summit X620 Lüfter Modul FB</td>
<td>Lüfter Modul für Summit X620 16 Port Systeme, Front-to-Back Lüftungsrichtung</td>
</tr>
<tr>
<td>10946</td>
<td>Summit X620 Lüfter Modul BF</td>
<td>Lüfter Modul für Summit X620 16 Port Systeme, Back-to-Front Lüftungsrichtung</td>
</tr>
<tr>
<td>10930A</td>
<td>Summit 300W AC PSU XT</td>
<td>300W AC Netzteil für Summit Systeme, Front-to-Back Lüftungsrichtung</td>
</tr>
<tr>
<td>10943</td>
<td>Summit 300W AC PSU BF</td>
<td>300W AC Netzteil für Summit Systeme, Back-to-Front Lüftungsrichtung</td>
</tr>
<tr>
<td>10933</td>
<td>Summit 300W +24V/-48V DC PSU FB</td>
<td>300W DC Netzteil für Summit Systeme, Front-to-Back Lüftungsrichtung</td>
</tr>
<tr>
<td>10944</td>
<td>Summit 300W +24V/-48V DC PSU BF</td>
<td>300W DC Netzteil für Summit Systeme, Back-to-Front Lüftungsrichtung</td>
</tr>
<tr>
<td>17404</td>
<td>X620-10x-Base</td>
<td>10 100Mb/1Gb/10GBASE-X SFP+ ports, integrierte power supply und Lüfter, ExtremeXOS Edge Lizenz</td>
</tr>
<tr>
<td>17405</td>
<td>X620-8t-2x-Base</td>
<td>8 100Mb/1Gb/10GBASE-T ports mit EEE, 2 1Gb/10GBASE-X SFP+ ports, integrierte power supply und Lüfter, ExtremeXOS Edge Lizenz</td>
</tr>
</tbody>
</table>

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

www.extremenetworks.com/product/summit-x620-series
**7100-Serie**


**Extreme 7100 - Hohe Portdichte**


**Extreme 7100 - Zuverlässigkeit und Verfügbarkeit**

Für eine hohe Verfügbarkeit der Systeme sind alle 7100er Switches sind 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.


**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.icher 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:

<table>
<thead>
<tr>
<th>Produktbezeichnung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>7148</td>
<td>48 Ports 1/10Gb SFP+ mit 4 10/40Gb QSFP+ Ports</td>
</tr>
<tr>
<td>7124</td>
<td>24 Ports 1/10Gb SFP+ mit 4 10/40Gb QSFP+ Ports</td>
</tr>
<tr>
<td>7148T</td>
<td>48 Ports 1/10GBASE-T mit 4 10/40Gb QSFP+ Ports</td>
</tr>
<tr>
<td>7124T</td>
<td>24 Ports 1/10GBASE-T mit 4 10/40Gb QSFP+ Ports</td>
</tr>
<tr>
<td>7148G</td>
<td>48 Ports 1/10/1000Mb Rj 45 mit PoE, 2 1/10Gb SFP+ und 2 10/40Gb QSFP+ Ports</td>
</tr>
<tr>
<td>7124G/24</td>
<td>24 Ports 1/10/1000Mb mit PoE, 2 1/10Gb SFP+ und 2 10/40Gb QSFP+ Ports</td>
</tr>
</tbody>
</table>


**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

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

<table>
<thead>
<tr>
<th>Bestellnummer</th>
<th>Produktbezeichnung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>16301</td>
<td>Summit X480-48t</td>
<td>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 Netzteileinbauplätze, ExtremeXOS Advanced Edge Lizenz</td>
</tr>
<tr>
<td>16303</td>
<td>Summit X480-24x</td>
<td>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 Netzteileinbauplätze, ExtremeXOS Advanced Edge Lizenz</td>
</tr>
<tr>
<td>16304</td>
<td>Summit X480-48x</td>
<td>48 Ports 100/1000BASE-X SFP, ein VIM-2 Einschubplatz rückseitig, 2 unbestückte Netzteileinbauplätze, ExtremeXOS Advanced Edge Lizenz</td>
</tr>
<tr>
<td>16311</td>
<td>VIM2-SummitStack</td>
<td>VIM2-SummitStack, 2 SummitStack Stacking Ports</td>
</tr>
<tr>
<td>16312</td>
<td>VIM2-10G4X</td>
<td>VIM2-10G4X, 4 10GBASE-X XFP Ports</td>
</tr>
<tr>
<td>16313</td>
<td>VIM2-SummitStack128</td>
<td>VIM2-SummitStack128, 2 x 64G Stacking Ports</td>
</tr>
<tr>
<td>16315</td>
<td>VIM2-SummitStack-V80</td>
<td>VIM2-SummitStack-V80, 2 x 40G Stacking Ports</td>
</tr>
<tr>
<td>17121</td>
<td>VIM3-40G4X</td>
<td>40 Gigabit Ethernet Modul, 4 40GBASE-X QSFP+ Ports</td>
</tr>
</tbody>
</table>

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:
www.extremenetworks.com/product/summit-x480-series/


Die X460-G2 eignen sich zusätzlich für den Einsatz als Top-of-Rack Systeme im Bereich moderner, hochintegrierter Rechenzentruminstallationen 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 Switche (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

- 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 (1GBase-T oder 1GBase-X nutzbar) und zusätzlich 4 dedizierte Gigabit SFP Ports und können dadurch mit bis zu 8 Optiken bestückt werden, während zusätzlich 20 Ports Gigabit 1GBase-T mit oder ohne PoE zur Verfügung stehen. Die X460-G2-24t-GE4 Systeme stellen bis zu 12 SFP Ports mit 1Gigabit zur Verfügung (4x Shared Ports, 8x dedizierte SFP Ports).


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 Betriebssystemes EXOS verfügbar sind.

SummitStack-V – flexibles Stacking über 10 GbE

Hinweis I: Stacking wird auf den 10 GbE VIM Modulen zu Beginn der Auslieferung der X460-G2 Systeme nicht unterstützt.

Hinweis II: Die 1GbE 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.


Intelligentes Switching und die Unterstützung von MPLS


Power over Ethernet (IEEE 802.3at PoE-plus)

**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)**

**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 RJ 45, 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
- Leistungsähnliche 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

<table>
<thead>
<tr>
<th>Bestellnummer</th>
<th>Produktbezeichnung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>16701</td>
<td>X460-G2-24t-10GE4</td>
<td>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)</td>
</tr>
<tr>
<td>16702</td>
<td>X460-G2-48t-10GE4</td>
<td>48 10/100/1000BASE-T Ports, 4 1000/10GBaseX unbestückte SFP+ Ports, rückseitiger VIM Slot (unbestückt), rückseitiger Einbauplatz für Timing Modul (unbestückt), 2 unbestückte</td>
</tr>
<tr>
<td>Teilenummer</td>
<td>Modell</td>
<td>Beschreibung</td>
</tr>
<tr>
<td>-------------</td>
<td>--------</td>
<td>--------------</td>
</tr>
<tr>
<td>16703</td>
<td>X460-G2-24p-10GE4</td>
<td>24 10/100/1000BASE-T Ports mit PoE-plus, 8 100/10GBaseX 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)</td>
</tr>
<tr>
<td>16704</td>
<td>X460-G2-48p-10GE4</td>
<td>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)</td>
</tr>
<tr>
<td>16705</td>
<td>X460-G2-24x-10GE4</td>
<td>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)</td>
</tr>
<tr>
<td>16706</td>
<td>X460-G2-48x-10GE4</td>
<td>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)</td>
</tr>
<tr>
<td>16707</td>
<td>X460-G2-24t-GE4</td>
<td>24 10/100/1000BASE-T Ports, 8 100/10GBaseX unbestückte SFP Ports (davon 4 SFP Ports die alternativ als 4 100/10GBaseX 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)</td>
</tr>
<tr>
<td>16708</td>
<td>X460-G2-48t-GE4</td>
<td>48 100/1000BASE-X Ports, 4 1GBaseX unbestückte SFP Ports, rückseitiger VIM Slot (unbestückt), rückseitiger Einbauplatz für Timing Modul (unbestückt), 2 unbestückte Netzteil Einschubplätze, Einschubplatz für Lüftermodul (unbestückt)</td>
</tr>
<tr>
<td>16709</td>
<td>X460-G2-24p-GE4</td>
<td>24 10/100/1000BASE-T Ports mit PoE-plus, 8 100/10GBaseX 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)</td>
</tr>
</tbody>
</table>
| 16710       | X460-G2-48p-GE4   | 48 10/100/1000BASE-T Ports mit PoE-plus, 4 1GBaseX unbestückte SFP Ports, rückseitiger VIM Slot (unbestückt),
### Optionale VIM Module

<table>
<thead>
<tr>
<th>Code</th>
<th>Modul Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>16710</td>
<td>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).</td>
</tr>
<tr>
<td>16711</td>
<td>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 100GBase-X für den die Aufnahme von SFP+ Modulen (unbestückt).</td>
</tr>
<tr>
<td>16712</td>
<td>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.</td>
</tr>
<tr>
<td>16713</td>
<td>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</td>
</tr>
<tr>
<td>16715</td>
<td>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</td>
</tr>
</tbody>
</table>

### Optionale Netzteil Module

<table>
<thead>
<tr>
<th>Code</th>
<th>Modul Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>10941</td>
<td>Summit 1100W AC PSU FB PoE 1100 Watt AC Netzteil für die Summit X460-G2-POE Switch mit Front-to-Back Lüftungsrichtung</td>
</tr>
<tr>
<td>10942</td>
<td>Summit 1100W AC PSU BF PoE 1100 Watt AC Netzteil für die Summit X460-G2-POE Switch mit Back-to-Front Lüftungsrichtung</td>
</tr>
<tr>
<td>10951</td>
<td>Summit 715W AC PSU FB PoE 715 Watt AC Netzteil für die Summit X460-G2-POE Switch mit Front-to-Back Lüftungsrichtung</td>
</tr>
<tr>
<td>10952</td>
<td>Summit 715W AC PSU BF PoE 715 Watt AC Netzteil für die Summit X460-G2-POE Switch mit Back-to-Front Lüftungsrichtung</td>
</tr>
<tr>
<td>10930A</td>
<td>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</td>
</tr>
<tr>
<td>10943</td>
<td>Summit 300W AC PSU BF 300W AC Netzteil für die nicht POE Versionen der Summit X460-G2 – Back-to-Front Lüftungsrichtung</td>
</tr>
</tbody>
</table>

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

**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 Distributionsbereiche 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.


**Leistungseffizienz und Power over Ethernet**

Die X450-G2 Switche 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.

Stackingvarianten
Alle Komponenten der Summit-Stackfamilie lassen sich mit bis zu acht Systemen unter einem gemeinsamen Management fusionieren. Hierzu werden zwei unterschiedliche Technologien genutzt:


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

Sicherheit

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 1GbE 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**

<table>
<thead>
<tr>
<th>Bestellnummer</th>
<th>Produktbezeichnung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>16172</td>
<td>X450-G2-24t-GE4-Base</td>
<td>Summit X450-G2 24 10/100/1000BASE-T, 4 SFP, 2 2Gbps Stackports, eingebaute Stromversorgung, 1 RPS Port, Einbauplatz für Lüfter</td>
</tr>
<tr>
<td>16173</td>
<td>X450-G2-24p-GE4-Base</td>
<td>Summit X450-G2 24 10/100/1000BASE-T, 4 SFP, POE+, 2 2Gbps Stackports, 2 Einbauschächte für Stromversorgung, Einbauplatz für Lüfter</td>
</tr>
<tr>
<td>16174</td>
<td>X450-G2-48t-GE4-Base</td>
<td>Summit X450-G2 48 10/100/1000BASE-T, 4 SFP, 2 2Gbps Stackports, eingebaute Stromversorgung, 1 RPS Port, Einbauplatz für Lüfter</td>
</tr>
<tr>
<td>16175</td>
<td>X450-G2-48p-GE4-Base</td>
<td>Summit X450-G2 48 10/100/1000BASE-T, 4 SFP, POE+, 2 2Gbps Stackports, 2 Einbauschächte für Stromversorgung, Einbauplatz für Lüfter</td>
</tr>
<tr>
<td>16176</td>
<td>X450-G2-24t-10GE4-Base</td>
<td>Summit X450-G2 24 10/100/1000BASE-T, 4 SFP, 2 2Gbps Stackports, eingebaute Stromversorgung, 1 RPS Port, Einbauplatz für Lüfter</td>
</tr>
<tr>
<td>16177</td>
<td>X450-G2-24p-10GE4-Base</td>
<td>Summit X450-G2 24 10/100/1000BASE-T, 4 SFP, POE+, 2 2Gbps Stackports, 2 Einbauschächte für Stromversorgung, Einbauplatz für Lüfter</td>
</tr>
<tr>
<td>16178</td>
<td>X450-G2-48t-10GE4-Base</td>
<td>Summit X450-G2 48 10/100/1000BASE-T, 4 SFP, unpopulated SFP+, two 2Gb stacking ports, 1 Fixed AC PSU, 1 RPS port, fan module slot (unpopulated), ExtremeXOS Edge license</td>
</tr>
<tr>
<td>16179</td>
<td>X450-G2-48p-10GE4-Base</td>
<td>Summit X450-G2 48 10/100/1000BASE-T, 4 SFP+, POE+, 2 2Gbps Stackports, 2 Einbauschächte für Stromversorgung, Einbauplatz für Lüfter</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
<td>Details</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>10945</td>
<td>Summit X460/X450-G2 fan module FB</td>
<td>Lüftermodul für alle Modelle der X450-G2 Serie</td>
</tr>
<tr>
<td>10941</td>
<td>Summit 1100W PoE AC PSU FB</td>
<td>1100 Watt AC Stromversorgungsmodul für Summit X450-G2 PoE Switches, Front-to-Back Belüftung</td>
</tr>
<tr>
<td>10931</td>
<td>Summit 750W AC PSU</td>
<td>AC Power Supply module for EPS-C2 Chassis</td>
</tr>
<tr>
<td>STK-RPS-150PS</td>
<td>150W Non-PoE RPS</td>
<td>150 watt non-PoE redundant power supply for A, B, C and X450-G2 switches</td>
</tr>
<tr>
<td>STK-RPS-150CH2</td>
<td>Einbaurahmen</td>
<td>19&quot; Einbaurahmen für 2 Stromversorgungsmodule STK-RPS-150PS</td>
</tr>
<tr>
<td>STK-RPS-150CH8</td>
<td>Einbaurahmen</td>
<td>19&quot; Einbaurahmen für 2 Stromversorgungsmodule STK-RPS-150PS</td>
</tr>
<tr>
<td>10936</td>
<td>EPS-C2</td>
<td>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</td>
</tr>
<tr>
<td>10939</td>
<td>EPS-CBL-2x7</td>
<td>External Power System Cable (1M) that connects EPS to any Summit X440 for providing redundant DC power</td>
</tr>
<tr>
<td>16190</td>
<td>Summit X450-G2 Edge to Advanced Edge Lic</td>
<td>ExtremeXOS Advanced Edge License for Summit X450 series switches</td>
</tr>
<tr>
<td>11011</td>
<td>Direct Attach Feature Pack</td>
<td>Direct Attach Feature Pack</td>
</tr>
<tr>
<td>16200</td>
<td>Summit X450-G2 OpenFlow Feature Pack</td>
<td>ExtremeXOS SDN - OpenFlow Feature Pack for Summit X450 series switches</td>
</tr>
<tr>
<td>16169</td>
<td>X450-G2 Multimedia(AVB) Feature Pack</td>
<td>ExtremeXOS Multimedia Service (Audio Video Bridging) Feature Pack for Summit X450 series switches</td>
</tr>
<tr>
<td>16190</td>
<td>Summit X450-G2 Edge to Advanced Edge Lic</td>
<td>ExtremeXOS Advanced Edge License for Summit X450 series switches</td>
</tr>
<tr>
<td>11011</td>
<td>Direct Attach Feature Pack</td>
<td>Direct Attach Feature Pack</td>
</tr>
<tr>
<td>16200</td>
<td>Summit X450-G2 OpenFlow Feature Pack</td>
<td>ExtremeXOS SDN - OpenFlow Feature Pack for Summit X450 series switches</td>
</tr>
<tr>
<td>16169</td>
<td>X450-G2 Multimedia(AVB) Feature Pack</td>
<td>ExtremeXOS Multimedia Service (Audio Video Bridging) Feature Pack for Summit X450 series switches</td>
</tr>
</tbody>
</table>

Weitere Informationen entnehmen Sie bitte dem aktuellen Datenblatt: [www.extremenetworks.com/product/summit-x450-g2-series](http://www.extremenetworks.com/product/summit-x450-g2-series)
X 440-G2


Flexible Port Konfiguration

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 Resourcen.

**ExtremeCloud™ Management**

Weitere Information über die ExtremeCloud Services finden Sie in diesem Buch sowie unter [http://extremenetworks.com/product/extremecloud](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

**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 1Höheneinheit (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
- 4x1Gigabit 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

<table>
<thead>
<tr>
<th>Bestellnummer</th>
<th>Produktbezeichnung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>16530</td>
<td>Summit X440-G2-12t-10GE4</td>
<td>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.</td>
</tr>
<tr>
<td>16531</td>
<td>X440-G2-12p-10GE4</td>
<td>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.</td>
</tr>
<tr>
<td>16532</td>
<td>X440-G2-24t-10GE4</td>
<td>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.</td>
</tr>
<tr>
<td>16534</td>
<td>X440-G2-48t-10GE4</td>
<td>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.</td>
</tr>
<tr>
<td>16536</td>
<td>X440-G2-24t-10GE4-DC</td>
<td>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.</td>
</tr>
<tr>
<td>16537</td>
<td>X440-G2-48t-10GE4-DC</td>
<td>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, 1 internes 230V Netzteil, ExtremeXOS Edge Lizenz, Anschlußport für externes redundantes Netzteil.</td>
</tr>
</tbody>
</table>
A4-Serie

Überblick

Zuverlässigkeit und Verfügbarkeit

Investitionsschutz
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

<table>
<thead>
<tr>
<th>Modell</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>A4H124-24</td>
<td>24 x 10/100, (2) SFP Ports, (2) 10/100/1000 stacking/uplink Rj 45 ports, Ext RPS</td>
</tr>
<tr>
<td>A4H124-24P</td>
<td>24 x 10/100 PoE (.af), (2) SFP Ports, (2) 10/100/1000 stacking/uplink Rj 45 ports, Ext RPS</td>
</tr>
<tr>
<td>A4H124-48</td>
<td>48 x 10/100, (2) SFP Ports, (2) 10/100/1000 stacking/uplink Rj 45 ports, Ext RPS</td>
</tr>
<tr>
<td>A4H124-48P</td>
<td>48 x 10/100 PoE (.af), (2) SFP Ports, (2) 10/100/1000 stacking/uplink Rj 45 ports, Ext RPS</td>
</tr>
<tr>
<td>A4H224-24FX</td>
<td>24 x 100Base-FX, (2) SFP Ports, (2) 10/100/1000 stacking/uplink Rj 45 ports, Ext RPS</td>
</tr>
<tr>
<td>A4H254-8F8T</td>
<td>8 x 100Base-FX plus 8 x 10/100, (2) SFP ports, (2) 10/100/1000 stacking/uplink Rj 45 ports, Ext RPS</td>
</tr>
</tbody>
</table>

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:
www.extremenetworks.com/product/a-series
B5-Serie

Zusammenfassung


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.

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 Portdichte. 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.


**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, 802.3x, und MAC Address Authentication
- Multiuser Authentifizierung (Bis zu 4 Endgeräte) pro Port
- Investitionsschutz durch Lifetime Garantie
### Extreme B5 – Varianten

<table>
<thead>
<tr>
<th>Modell</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>B5G124-24</td>
<td>(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</td>
</tr>
<tr>
<td>B5G124-24P2</td>
<td>(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</td>
</tr>
<tr>
<td>B5G124-48</td>
<td>(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</td>
</tr>
<tr>
<td>B5G124-48P2</td>
<td>(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</td>
</tr>
<tr>
<td>B5K125-24</td>
<td>(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</td>
</tr>
<tr>
<td>B5K125-24P2</td>
<td>(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</td>
</tr>
<tr>
<td>B5K125-48</td>
<td>(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</td>
</tr>
<tr>
<td>B5K125-48P2</td>
<td>(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</td>
</tr>
</tbody>
</table>

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:

C5-Serie

Überblick


Extreme C5 – QoS

Extreme C5 - Zuverlässigkeit und Verfügbarkeit
Wie die B5 Serie bieten die C5 Switchte bei nur einer Höheneinheit (1U) im Rack eine hohe Port-Dichte. Durch Stacking kann eine performante und redundante Hardware Platform geschaffen werden. Die Stromversorgung der C5 Serie Switchte 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**

<table>
<thead>
<tr>
<th>Modell</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>C5G124-24</td>
<td>(24) 10/100/1000 RJ 45 ports, (4) combo SFP ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports</td>
</tr>
<tr>
<td>C5G124-24P2</td>
<td>(24) 10/100/1000 PoE (.at + .af) RJ 45 ports, (4) combo SFP ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports</td>
</tr>
<tr>
<td>C5G124-48</td>
<td>(48) 10/100/1000 RJ 45 ports, (4) combo SFP ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports</td>
</tr>
<tr>
<td>C5G124-48P2</td>
<td>(48) 10/100/1000 PoE (.at + .af) RJ 45 ports, (4) combo SFP ports, (2) dedicated high-speed dedicated stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports</td>
</tr>
<tr>
<td>C5K125-24</td>
<td>(24) 10/100/1000 RJ 45 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</td>
</tr>
<tr>
<td>C5K125-24P2</td>
<td>(24) 10/100/1000 PoE (.at + .af) RJ 45 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</td>
</tr>
</tbody>
</table>
C5K125-48  
(48) 10/100/1000 RJ 45 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) RJ 45 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:  

### 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 Telefongeräten. Die D2 Serie besitzt die Möglichkeit für 2 externe Stromversorgungsmodule zur redundanten Versorgung.


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

<table>
<thead>
<tr>
<th>Modell</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>D2G124-12</td>
<td>12 X 10/100/1000 FIXED CONFIG L2 SWITCH &amp; POWER BRICK</td>
</tr>
<tr>
<td>D2G124-12P</td>
<td>12 X 10/100/1000 FIXED POE L2 SWITCH &amp; POWER BRICK</td>
</tr>
</tbody>
</table>

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:  

### X 430


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

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 1Gigabit 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
**X430 – Bestellinformation**

<table>
<thead>
<tr>
<th>Bestellnummer</th>
<th>Produktbezeichnung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>16515</td>
<td>Summit X430-8p</td>
<td>8 Ports 10/100/1000BASE-T PoE+ und 2 dedizierte 1000BASE-X SFP Uplink Ports, internes 230V Netzteil, ExtremeXOS L2 Edge license</td>
</tr>
<tr>
<td>16517</td>
<td>Summit X430-24p</td>
<td>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</td>
</tr>
<tr>
<td>16516</td>
<td>Summit X430-24t</td>
<td>24 Port 10/100/1000BASE-T und 4 dedizierte 1000BASE-X SFP Uplink Ports, internes 220V Netzteil, ExtremeXOS L2 Edge license</td>
</tr>
<tr>
<td>16518</td>
<td>Summit X430-48t</td>
<td>48 Port 10/100/1000BASE-T und 4 dedizierte 1000BASE-X SFP Uplink Ports, internes 220V Netzteil, ExtremeXOS L2 Edge license</td>
</tr>
</tbody>
</table>

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:  
5 Management & Software

Extreme Management Center


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**

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**
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.


**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 (Switche, Router, Wireless-Controller,...) schnell und einfach katalogisieren.

**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.


3) Endsystem Anzeige: Darstellung der Endsysteme pro Verbindungsprotokoll und Top APs nach Bandbreite, Endsystemen oder Paketen im Wired-Bereich (wählbare Sortierung)


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


Controller

In Listenform werden alle installierten Controller dargestellt. Neben der IP und der aktuellen Auslastung (Anzahl Endsysteeme 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**


**Threats**

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.


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 Alarme zu Geräten und Systemen, Logs und Events zusammen. Alarme 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.

Alarme 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.

**Control**


**Dashboard:**

**Policy**

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 wichtiger 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


**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 rechtsklick 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 tiefergehende Informationen zur Verfügung gestellt.

Map

Über die Map Darstellung wird das gesuchte Endgerät direkt auf den hinterlegten Karten lokalisiert und dargestellt.
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 netzwerkbaasierte 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 schädhaften Einsatz von Applikationen.
Mithilfe von Analytics können IT-Abteilungen nun signifikante Verbesserungen bei den unternehmenskritischen technologischen Anwendungen erzielen.


**Vorteile der Lösung im Überblick**

- **Business Analytics** – Analyse der Nutzung von Applikationen und deren Reaktionszeiten.
- **Netzwerksicherheit** – Identifizierung von nicht autorisierten und schadhaften 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**


• Die notwendigen **Lizenzen** um die einzelnen Elemente zu betreiben (Control Center, Flow-Lizenzen, usw.)

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

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.


**Erkennung von schädlichen Applikationen**
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


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


**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


**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-Verbindungspunkte 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.

• **Netzwerkbasierte 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

Extreme Management (vormals NetSight) wird in drei Ausstattungsstufen angeboten:

![NetSight Diagram](image)

- **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.


<table>
<thead>
<tr>
<th>Lizenz</th>
<th>Devices</th>
<th>APs</th>
</tr>
</thead>
<tbody>
<tr>
<td>NMS-xxx-5</td>
<td>5</td>
<td>50</td>
</tr>
<tr>
<td>NMS-xxx-10</td>
<td>10</td>
<td>100</td>
</tr>
<tr>
<td>NMS-xxx-25</td>
<td>25</td>
<td>250</td>
</tr>
<tr>
<td>NMS-xxx-50</td>
<td>50</td>
<td>500</td>
</tr>
<tr>
<td>NMS-xxx-100</td>
<td>100</td>
<td>1000</td>
</tr>
<tr>
<td>NMS-xxx-250</td>
<td>250</td>
<td>2500</td>
</tr>
<tr>
<td>NMS-xxx-500</td>
<td>500</td>
<td>5000</td>
</tr>
<tr>
<td>NMS-xxx-U</td>
<td>U</td>
<td>U</td>
</tr>
</tbody>
</table>
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?


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.


Über ein standardisiertes Webportal ist der Administrator nun in der Lage, seine Komponenten in allen Geschäftstellen 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?**


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:


- 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 Multigärten 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.
- 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**


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
- 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))
- RADIUS Dienste lassen sich zentral oder Standortbezogen anbinden
- Der Cloud Service steht redundant weltweit zur Verfügung
- Gastzugang
## Extreme Cloud – Bestellinformationen für Access Points & Switches

<table>
<thead>
<tr>
<th>Bestellnummer</th>
<th>Produktbezeichnung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>31013</td>
<td>AP3935i - ROW</td>
<td>Freigegeben für die EU &amp; Rest-of-World (Landeszertifizierung überprüfen) - Dual band Dual Radio 802.11ac/abgn, 4x4:4 MIMO Indoor Wave 2 Access Point mit acht internen Annten.</td>
</tr>
<tr>
<td>31017</td>
<td>AP3965i - ROW</td>
<td>Freigegeben für die EU &amp; Rest-of-World (Landeszertifizierung überprüfen) - Dual band Dual Radio 802.11ac/abgn, 4x4:4 MIMO Outdoor Wave 2 Access Point mit acht internen Annten.</td>
</tr>
<tr>
<td>30912</td>
<td>AP3805i - FCC</td>
<td>Für folgende Länder frei gegeben US, Puerto Rico &amp; Columbien - Dual band Dual Radio 802.11ac/abgn, 2x2:2 MIMO Indoor Wave 1 Access Point mit vier internen Annten.</td>
</tr>
<tr>
<td>30913</td>
<td>AP3805i - ROW</td>
<td>Freigegeben für die EU &amp; Rest-of-World (Landeszertifizierung überprüfen) - Dual band Dual Radio 802.11ac/abgn, 2x2:2 MIMO Indoor Wave 1 Access Point mit vier internen Annten.</td>
</tr>
<tr>
<td>16530</td>
<td>X440-G2-12t-10GE4</td>
<td>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.</td>
</tr>
<tr>
<td>16531</td>
<td>X440-G2-12p-10GE4</td>
<td>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.</td>
</tr>
<tr>
<td>16532</td>
<td>X440-G2-24t-10GE4</td>
<td>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.</td>
</tr>
<tr>
<td>16533</td>
<td>X440-G2-24p-10GE4</td>
<td>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.</td>
</tr>
<tr>
<td>16534</td>
<td>X440-G2-48t-10GE4</td>
<td>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,</td>
</tr>
<tr>
<td>16535</td>
<td>X440-G2-48p-10GE4</td>
<td>SummitStack-V® support. Ein internes 230V Netzteil, ExtremeXOS Edge Lizenz. 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</td>
</tr>
<tr>
<td>17401</td>
<td>X620-16x-Base</td>
<td>X620 16 100Mb/1Gb/10GBASE-X SFP+Ports, 2 Power Supply Einschübe, 1Lüfter Einschub, ExtremeXOS Edge Lizenz</td>
</tr>
<tr>
<td>10945</td>
<td>Fan Module FB</td>
<td>Lüfter für X620-16x, Front to Back airflow</td>
</tr>
<tr>
<td>10946</td>
<td>Fan Module BF</td>
<td>Lüfter für X620-16x, Back to Front airflow</td>
</tr>
<tr>
<td>10930A</td>
<td>300W AC PSU XT</td>
<td>300W AC 230V Netzteil für X620-16x, Front to Back airflow</td>
</tr>
<tr>
<td>10943</td>
<td>300W AC PSU BF</td>
<td>300W AC 230V Netzteil für X620-16x, Back to Front airflow</td>
</tr>
<tr>
<td>10933</td>
<td>300W +24V/-48V DC PSU</td>
<td>300W DC 48V Netzteil für X620-16x, Front to Back airflow</td>
</tr>
<tr>
<td>10944</td>
<td>300W DC PSU BF</td>
<td>300W DC 48V Netzteil für X620-16x, Back to Front airflow</td>
</tr>
</tbody>
</table>

Weitere Optionen entnehmen Sie bitte dem aktuellen Datenblatt:
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.

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.

EXTREME NETWORKS - TECHNOLOGY SOLUTION PARTNERS
Analytik-Partner

IXIA

Nexthink

Plixer International

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

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

Real Status Hyperglance

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

**Convergence-Partner**

**Microsoft Skype for Business**


**AXIS**


**Avaya**


**AVnu**

**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 getesteteten AVB-Lösungen, die eine hervorragende Ausfallsicherheit, niedrigere Betriebskosten, Netzwerk-konvergenz für alle Medien und standardbasierte Entwürfe für eine vereinfachte Integration bieten.

**Haivision**

**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**

**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**

**Philips**

**Polycom**

**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**

**iBoss**

**Lightspeed Systems**

**McAfee**

**InfoBlox**

**Data Center & Cloud-Partner**

**A10 Networks**


**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**


**EMC VSPEX**


**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**


**VMware**


**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 AuerScout und Extreme Access Control können IT-Manager ihre kabellosen und kabelgebundenen Geräte und Applikationen aus einer Konsole heraus verwalten und kontrollieren.
Maas360

JAMF

MobileIron

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, dass 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**

8 Services


Je komplexer das Netzwerk wird, desto wichtiger wird eine richtige Kombination aus verschiedenen Services zum Schutz Ihrer Investitionen und Ressourcen.

<table>
<thead>
<tr>
<th>Wartung &amp; Support</th>
<th>Premier Services</th>
<th>Managed Services</th>
<th>Professional Services</th>
</tr>
</thead>
</table>


Wartung & Support


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 Applikationsoftware und Sicherheitsanwendungen immer auf dem neuesten 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:
  o 94% aller Anfragen werden von unserem Support-Team beim ersten Kontakt gelöst
  o 9 von 10 Kunden sind mit dem Support von Extreme Networks sehr zufrieden
  o 100% internes Service Center
- Netzwerkverfügbarkeit und Produktivität: Mit Extreme Services minimieren Sie die Auswirkungen eines ungeplanten Ausfalls und erhöhen die Mitarbeiterproduktivität.
Übersicht des kompletten Service Supports

<table>
<thead>
<tr>
<th>Support Offering</th>
<th>Global Technical Assistance Center (24x7x365)</th>
<th>eSupport (24x7x365)</th>
<th>Advanced Hardware Replacement</th>
<th>Onsite Services</th>
<th>Return &amp; Replace (10 Business Days, After Receipt at Factory)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software &amp; TAC</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Return &amp; Replace</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NBD AHR</td>
<td>✓</td>
<td>✓</td>
<td>Next Business Day</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NBD Onsite</td>
<td>✓</td>
<td>✓</td>
<td>Next Business Day</td>
<td>M - F (8 x 5)</td>
<td></td>
</tr>
<tr>
<td>4-Hour AHR</td>
<td>✓</td>
<td>✓</td>
<td>4 Hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4-Hour Onsite</td>
<td>✓</td>
<td>✓</td>
<td>4 Hours</td>
<td></td>
<td>24 x 7</td>
</tr>
<tr>
<td>Software Subscription</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Warum Extreme Services?


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

<table>
<thead>
<tr>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geringe Netzwerk-Komplexität</td>
<td>Mittlere Netzwerk-Komplexität</td>
<td>Hohe Netzwerk-Komplexität</td>
</tr>
<tr>
<td>Regional Designated Technical Support Engineers</td>
<td>Upgrade Management + Lab Validation Hardware und Software</td>
<td>Customer Entitlement &amp; Asset Management</td>
</tr>
<tr>
<td>Vier oder Acht Tage Onsite Support pro Jahr mit PM oder PSE</td>
<td>Network Assessment Einmal im Jahr mit PSE</td>
<td>Zwei oder Vier Service History Reviews pro Jahr und remote mit PM</td>
</tr>
<tr>
<td>Dedizierter Program Manager (PM) Bis zu 5 Stunden pro Woche</td>
<td>Code Review und Knowledge Transfer halbjährlich mit PSE</td>
<td>Case Management zwöchentliche Calls mit PSE</td>
</tr>
<tr>
<td>Dedizierter Premier Services Engineer (PSE)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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:

<table>
<thead>
<tr>
<th>Service</th>
<th>MonitoringPLUS</th>
<th>ResponsePLUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>24x7 Service Desk</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Advanced Monitoring System (H-P-S)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Proaktive Problemerkennung</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Webportal mit Dashboards</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Service Reporting</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Config Backup</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Asset Management</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Service Review</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Service Manager</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Network Operation (Problembehebung)</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Professional Services


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:

<table>
<thead>
<tr>
<th>Switching &amp; Routing:</th>
<th>Netzwerkmanagement &amp; Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExtremeXOS Fundamentals</td>
<td>Extreme Application Analytics</td>
</tr>
<tr>
<td>ExtremeXOS Switching &amp; Routing</td>
<td>High-Density Environments</td>
</tr>
<tr>
<td>IPv6 Networking</td>
<td>Extreme Management Center Boot Camp</td>
</tr>
<tr>
<td>ExtremeEOS Fundamentals</td>
<td>Extreme Policy</td>
</tr>
<tr>
<td>ExtremeEOS Switching &amp; Routing</td>
<td>Extreme Access Control (NAC)</td>
</tr>
<tr>
<td>Switching &amp; Routing Boot Camp (EXOS &amp; EOS)</td>
<td>Security Information &amp; Event Management (SIEM)</td>
</tr>
<tr>
<td>ECA Networking Hands-On Lab</td>
<td>Wireless LAN</td>
</tr>
<tr>
<td>Advanced Routing</td>
<td>Extreme Wireless</td>
</tr>
</tbody>
</table>
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

- ExtremeXOS
- EOS
- Identifi
- NetSight
- SummitWM

- Switching & Routing
- Network
- General
- Security
- Scripting

- Training
- Regional User
- General
- All Things E-
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

Extranet

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

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

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

GTAC Knowledge Home: https://gtacknowledge.extremenetworks.com/
Danksagung


Daher ein besonderes Dankeschön an:

Markus Altmann           Efthymios Christodoulakis
Alexander Eichholz       Ralf Klockewitz
Karin Denk               Stephan Krock
Fred Götz                Marco Mautone
Olaf Hagemann            J an Heinbokel
Andreas Helling          Heribert Rehart
André Herkenrath