ComConsult Research

Der Netzwerk Insider

März 2011

Systematische Weiterbildung für Netzwerk- und IT-Professionals

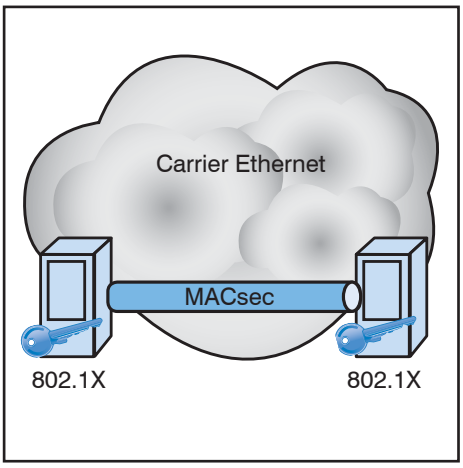
Schwerpunktthema

Neue Verfahren für mandantenfähige Netze

von Dr. Simon Hoff, Dr. Behrooz Moayeri

Dieser Beitrag befasst sich mit neuen Verfahren für mandantenfähige Netze. Einerseits hat sich Carrier Ethernet mittlerweile neben Multi-Protocol Label Switching (MPLS) als Technologie in den Service-Provider-Netzen etabliert, und andererseits wurde IEEE 802.1X, der Standard für Port-basierende Authentisierung, der u. a. für eine dynamische Zuordnung eines Endgeräts zu einer Benutzergruppe genutzt wird, in 2010 wesentlich erweitert.

Im ersten Teil des Beitrags wird auf Carrier Ethernet eingegangen. Danach folgt eine Zusammenfassung der in 2010 hinzugekommenen Erneuerungen in IEEE 802.1X,



die diesen Standard noch wichtiger für mandantenfähige Netze machen.

1. MPLS bekommt Konkurrenz

In den letzten zehn Jahren hat sich Multi-Protocol Label Switching (MPLS) zum De-facto-Standard für mandantenfähige Netze entwickelt. Die wesentlichen Erfolgsfaktoren von MPLS waren die folgenden:

weiter auf Seite 14

Zweitthema

Storage: wo bleibt der Markt?

von Dr. Behrooz Moayeri

Beim Gang durch ein Rechenzentrum zeigte mir einmal der dortige Netzverantwortliche eine große Tape Library, für die das Unternehmen gerade eine fast siebenstellige Summe bezahlt hatte.

Mein leidgeprüfter Gesprächspartner musste gerade eine Rotstiftarie über sich ergehen lassen, in deren Folge er mal wieder nicht anders konnte als die längst fällige Modernisierung des Netzes zu verschieben. Seine von Bitterkeit geprägte Bemerkung habe ich nicht vergessen: „Unser Management gibt nur Geld aus, wenn es dafür einen für jedermann sichtbaren Gegenwert in Form eines Geräts gibt, das möglichst viel Stellfläche belegt. Ein LAN-Switch, der in einen halben Schrank passt, darf nicht zweihunderttausend Euro kosten."

weiter auf Seite 26

Aktueller Kongress

IPv6-Forum 2011

ab Seite 12

Geleit

Thunderbolt: das Ende des Desktop-PCs?

ab Seite 2

Neues Seminar

Netzanalyse und sicherheitstechnische Bewertung elektrischer Netze in Rechenzentren

auf Seite 11

Aktueller Kongress

IT-Sicherheits-Forum 2011

ab Seite 10

Standpunkt

Quality of Service - Fluch oder Segen?

auf Seite 25

Zum Geleit

Thunderbolt: das Ende des Desktop-PCs?

Seit Jahren beobachten wir eine kontinuierliche Zunahme des Marktanteils von Laptop-Computern im Vergleich zu Desktop-PCs. Viele Unternehmen kämpfen heute schon mit den Problemen, die der Betrieb mobiler Endgeräte mit sich bringt. Nun hat Intel in Zusammenarbeit mit Apple Thunderbolt vorgestellt, eine neue Technologie zur Anbindung von Peripherie-Geräten.

Was bedeutet diese Technologie für die Unternehmen? Ist das mobile Endgerät die Zukunft und wird der Desktop-PC verdrängt? Wie kann der Betrieb zunehmend mobiler IT-Umgebungen überhaupt erfolgreich umgesetzt werden?

Tatsächlich hat der Wechsel von einem Desktop-PC auf einen Laptop bisher eine Reihe von Nachteilen. Für ein typisches Benutzer-Leistungsprofil mit Email und Office-Anwendungen im Vordergrund sind diese Nachteile verkraftbar. Aber die Fälle, in denen eine höhere Anforderung an das Endgerät gestellt wird, nehmen zu. Und dann ist die bisherige Laptop-Technologie häufig eine teure Sackgasse. Ein wesentlicher Treiber für diese Entwicklung ist die Explosion von HD-Video und Multimedia-Anwendungen sowohl im privaten als auch im Unternehmens-Bereich.

Wo liegen bisher die Nachteile von Laptops? Sie konzentrieren sich auf die folgenden Bereiche:

- Beschränkte CPU-Leistung
- 2,5-Zoll-Plattensysteme liefern weniger Leistung und Platz als die in Desktop-PCs üblichen 3,5 Zoll-Festplatten
- Bildschirmgröße und Qualität für bestimmte Anwendungen unzureichend
- Kein flexibler Systemausbau möglich, ändert sich der Bedarf und wird eine andere Systemarchitektur benötigt, ist der Laptop am Ende

Anders formuliert kann man aus der Sicht von bestimmten Anwendungen vornehmlich aus dem Video- und Multimediabereich fordern:

- Mehr CPU-Leistung
- Mehr Plattenleistung
- Größere Festplatten im Terabyte-Bereich
- Integration hochauflösender Bildschirme

- Mehr Flexibilität in der Gestaltung der Systemarchitektur

Können diese Anforderungen erfüllt werden, dann ist das mobile System dem Desktop-PC nicht nur gleichwertig, es ist überlegen. Natürlich bleibt dann noch die Frage nach dem Preis-Leistungs-Verhältnis. Aber die Historie hat gezeigt, dass Massenprodukte, wenn die geeigneten Standards existieren, beliebig im Preis fallen können.

Und damit sind wir bei Thunderbolt. Thunderbolt wurde ursprünglich unter dem Namen Light Peak von Intel entwickelt. Light Peak sollte auch die Verwendung von Glasfaser-Kabeln verdeutlichen. Aber bedingt durch die Bedarfssituation hat sich Intel zusammen mit Apple zuerst auf eine Kupfer-Variante konzentriert und dieser nun offiziell den Namen Thunderbolt gegeben.

Was ist Thunderbolt? Thunderbolt ist eine neue I/O-Technologie, die alles bisherige inklusive USB 3.0 sehr alt aussehen lässt. Einige Zitate sollen das unterstreichen:

- Grant Petty, CEO von Blackmagic: „ ... It´s a game changer“.
- Philippe Spruch, Chairman LaCie: „ ... a breakthrough in I/O-technology“.
- Bill Putnam, CEO Universal Ausio: „ ... this only happens about once a decade“.
- Betty Bennett, CEO Apogee: „ ... connectivity without compromise“.

Die Technik hat folgende Eigenschaften:

- Zwei-Kanal 10 Gigabit bidirektional auf einem Kabel
- Dual-Protocol Unterstützung: PCI-Express und Display-Port zeitgleich
- Perfekte Integration in die Systemtechnik durch Nutzung von PCI-Express, am Übergang zwischen I/O und Systembus geht keine Leistung verloren
- Bis zu 6 Geräte können in einer Kette angeschlossen werden
- Sehr niedrige Verzögerung mit hoch präziser Zeitsynchronisation
- 10W Stromversorgung für Endgeräte über das Kabel

Tatsächlich muss man Thunderbolt im direkten Zusammenhang mit der neuen Prozessor-Generation Sandy Bridge von Intel sehen, der Nachfolgegeneration des Nehalem. Sandy Bridge bietet mit dem i7 nicht nur Vier-Kern-CPUs für Laptops, sondern erlaubt momentan auch Turbo

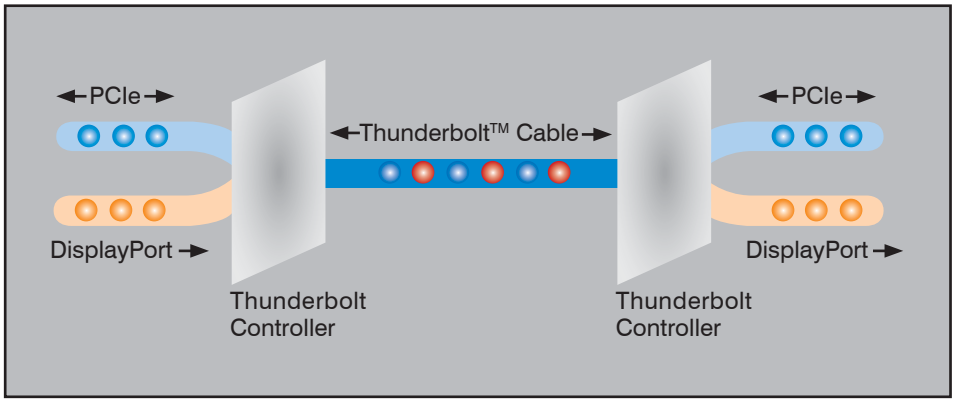


Abbildung 1: Thunderbolt in Aktion

Thunderbolt: das Ende des Desktop-PCs?

Boost bis 3,4 GHz. Damit werden sowohl viele parallele Prozesse als auch Anwendungen wie Adobe Photoshop oder Apple Final Cut unterstützt, die manchmal die Ein-Kern-Hochleistung brauchen. Kombiniert man diese beiden Technologien, entsteht ein völlig neues Fundament für mobiles Arbeiten.

Der erste Hersteller, der diese Kombination aus neuer I/O und neuer CPU-Leistung nutzt, ist Apple mit der neuen Generation des MacBook Pro. Apple zeigte bei der Vorstellung der neuen Geräte, wie mit Hilfe von Thunderbolt High-End-Plattensysteme und bis zu 2 große Bildschirme mit einem Laptop kombiniert werden können. Video- und Audio-Integration in Thunderbolt bilden die Basis für genau die Anwendungen, die bisher auf einem Laptop nur eingeschränkt genutzt werden konnten. Unter dem Strich entsteht der komplett mobile Hochleistungsarbeitsplatz.

Abbildung 2: Beispiel einer Thunderbolt-Lösung mit Promise Raid-System und Bildschirm-Integration

Die ersten Benchmarks dieser Lösung zeigen auf: die Notwendigkeit, weiterhin einen Desktop-PC einzusetzen, ist für die absolute Mehrheit aller Anwender nicht mehr gegeben. Details aus den Benchmarks:

- HD-Datenströme von bis zu 700 MB/s können verarbeitet werden.
- Die CPU-Leistung übertrifft die Leistung der unteren Leistungskategorie von Westmere-Prozessoren, für Apple-Kunden bedeutet das: der Mac Pro hat vermutlich ausgedient.

Thunderbolt löst damit auch temporär das Problem der Integration von Hochleistungs-Solid-State-Drives SSD in die Systemarchitektur. Dies war speziell für mobile Endgeräte eine Herausforderung, da in diese nicht per Busadapter eine neue Schnittstelle integriert werden kann. Die neueste Generation von SSD liefert mehr Durchsatz als selbst SATA II mit 6 Gigabit liefern kann. Kombiniert man diese Laufwerke in einem kleinen Raid, dann können solche Systeme, wie auch von LaCie bei der Vorstellung von Thunderbolt gezeigt, die 10 Gigabit komplett füllen. Und Sandy Bridge Prozessoren in Kombination mit Highend-Grafikkarten können diese Datenmenge auch verarbeiten.

Sind diese Lösungen zu teuer für den durchschnittlichen Unternehmens-Arbeitsplatz? Zum einen sprechen wir hier über Arbeitsplätze, die bisher nicht sinnvoll mit Laptops abgedeckt werden konnten. Zum anderen ist die Frage, mit welchem Preis man diese Lösung vergleicht. Eine in der Leistung vergleichbare Lösung mit einem MacBook Pro und externem Raid-System von LaCie oder Promise (bei erst im zweiten Quartal verfügbar) liegt 25 bis 40% unter dem Preis einer Mac Pro-Lösung. Die Preise für Hochleistungs-Arbeitsplätze sinken also mit dieser neuen Technologie.

Was bedeutet das für die Nicht-Apple-Welt? Die anderen Anbieter halten sich momentan zurück, vermutlich, weil sie über die Zusammenarbeit zwischen Intel und Apple verärgert sind. Auch wird es noch 6 Monate dauern, bis die Hersteller von Peripherie-Geräten ihre neuen Thunderbolt-Produkte auf den Markt bringen. Aber im Endeffekt kann sich kein Anbieter den Vorteilen dieser neuen Technologie entziehen. Sie ermöglich unter anderem eine weitere Verringerung des Formfaktors für Laptops (da Schnittstellen wegfallen) und sie öffnet die Tür für einen neuen Markt. Von daher ist es eine reine Frage der Zeit, bis die Dells und HPs dieser Welt hier nachziehen werden.

Werden damit auch unsere Tablet-Computer zu Hochleistungsmaschinen? Nein. Zum einem haben diese Geräte keinen internen PCI-Express, der für Thunderbolt unverzichtbar ist. Zum anderen sind diese Geräte für die hier angesprochenen Anwendungen ungeeignet.

Was bedeutet das für Behörden und Unternehmen? Einfach formuliert gehört mobilen Endgeräten die Zukunft. Sicher nicht an allen Arbeitsplätzen, dafür sind diese Lösungen im Vergleich zu einem 500 Euro Desktop-PC zu teuer. Aber die Zahl der Arbeitsplätze, die von diesen Lösungen profitieren, ist mit dieser neuen Technologie enorm gestiegen.

Als Fazit kann man feststellen, dass damit bestehende Herausforderungen intensiviert werden und neue entstehen:

- Der Betrieb mobiler Endgeräte erreicht eine neue Dimension im Jahr 2011. Die Kombination aus Thunderbolt und Sandy Bridge, aber auch die Schwemme von Tablet-Computern generiert extreme Herausforderungen an den Betrieb.
- Datensicherung und Backup wird sehr hohe Anforderungen an die Netzwerk-Infrastruktur stellen.
- Sicherheits-Lösungen müssen neu aufgesetzt und ausgeweitet werden.
- Mobile Arbeitsplätze inklusive der Heimarbeitsplätze werden sich weiter ausbreiten und müssen integriert werden.
- Neue Medientypen wie HD-Video nehmen an Bedeutung auch innerhalb der Unternehmen zu.
- Es entsteht der Bedarf für neue Systemarchitekturen für mobile Endgeräte. Dabei werden auch Cloud-Dienste eine zunehmende Rolle spielen, die gerade im Bereich der Integration von mobilen Geräten ihre Stärke haben.

Wir adressieren diese Problematik zum Beispiel auf dem ComConsult Sicherheits-Forum 2011. Auch das ComConsult Storage-Forum 2011 wird wichtige Aspekte aus diesem Bereich aufgreifen. Auch freuen wir uns, Ihnen unsere neue Studie zum Thema Cloud-Computing ankündigen zu können.

Aus der Sicht eines Benutzers, der damit gerade seine Workstation beerdigt und auf komplett mobiles Arbeiten umsteigt

Ihr
Dr. Jürgen Suppan

Kongress

ComConsult Storage-Forum 2011 13.07. - 15.07.11 in Bonn

Die ComConsult Akademie veranstaltet vom 13.07. - 15.07.11 ihren neuen Kongress „ComConsult Storage-Forum 2011“ in Bonn. Das Forum war ursprünglich im März geplant und wurde auf den Juli-Termin verschoben.

Zentraler, im Netzwerk zugreifbarer Speicher steht im Mittelpunkt aller zukünftigen IT-Architekturen. Die technologische Spannweite ist riesig, permanent kommen neue Entwicklungen und Produkte hinzu. Das ComConsult Storage-Forum 2011 analysiert die aktuellen Entwicklungen im Speichermarkt, vergleicht Alternativen und zeigt auf, wo der Weg hingeht.

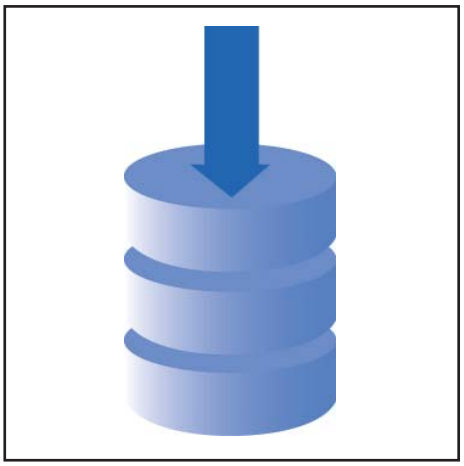
Alle wesentlichen IT-Architekturen werden sich in Zukunft auf zentrale, im Netzwerk zugreifbare Speicher-Lösungen abstützen. Die Bandbreite technologischer Entwicklungen in diesem Bereich, angefangen von neuen IT-Architekturen und hin zu neuen Speicher-Lösungen ist gewaltig. Kombiniert man das mit einem immer weiter wachsenden Datenbestand, dann ergibt dies ein explosives Gemisch:

- Immer mehr Daten müssen beherrscht werden.
- Immer mehr Applikationen hängen von zentralen Speicher-Systemen ab.
- Basis-Funktionen wie Backup/Restore werden zu einem echten Problem.

Die Gründe für den weiter wachsenden Bedarf sind vielfältig:

- Mehr Rechenleistung gestattet die Verarbeitung von immer mehr Daten.
- Auch neue Applikationen und Applikationstypen (Video, Web 2.0/3.0) erzeugen erhebliche Datenmengen.
- Zunehmende Automatisierung (RFID) stellt immer mehr Daten bereit.
- Eine veränderte Risiko- und Rechtssituation erfordert mehr Detail-Daten für eine verbesserte Prognose-Sicherheit.
- Neue Formen der Vermarktung erzeugen neue Daten (Internet).
- Verändertes Kundenverhalten schafft neue Daten zu Kunden-Bedürfnissen und Erwartungen.
- Virtualisierung und Konsolidierung von Servern zentralisiert Daten.

Dies erfolgt parallel zu wesentlichen Änderungen in IT-Technologien und Architek-



turen, die neue Anforderungen an die Leistung und Qualität von Speicher erzeugen:

- Virtualisierung geht immer mehr weg von der simplen Konsolidierung und hin zur Schaffung neuer Architekturen für Webanwendungen.
- Neue Virtualisierungsverfahen wie vMotion, HA, Desaster Recovery generieren erhebliche Anforderungen an Speicher-Performance.
- Traditionell wurde die Leistung von SAN-Systemen in I/O-Transaktionen pro Se--kunde gemessen, mit den neuen Architekturen kommen erhebliche Anforderungen an Bandbreite hinzu.
- Mit Desktop-Virtualisierung entsteht ein erheblicher Mehrbedarf an Speicher.
- Neue Netzwerk-Technologien geben dem Netzwerk Systembus-Charakter und ermöglichen eine Speicher-Einbindung mit bisher unbekannter Leistung.
- Die Entwicklung von SSD-Speicher muss als sehr kritisch angesehen werden, stellt sie doch die traditionelle Formel Lokale Leistung = Zentrale Leistung in Frage. SSD muss zwangsläufig auch im SAN eine Rolle spielen oder es entsteht ein Performance-Loch zur Server-Leistung. Dies generiert neue Probleme im Netzwerk.

Im Gegensatz zur Vergangenheit ist zentraler Speicher als SAN damit nicht mehr nur auf den Datenbank-Bereich beschränkt. Vielmehr muss in Leistung und Bedarf mindestens unterschieden werden nach den Anwendungsbereichen:

- Datenbank- und Mainframe
- File-Services
- Virtualisierung
- Webarchitekturen
- Datensicherung

Das führt direkt zu der Frage, wie sich Anforderungen an Speicher-Technik in Zukunft quantifizieren und messen lassen. Tatsächlich kommen sehr unterschiedliche Kriterien zusammen:

- I/O-Transaktionsrate
- Bandbreite
- Verfügbarkeit
- Speichermenge
- Preis pro TB

Die Kombination sehr unterschiedlicher Anforderungen an den zentralen Speicher aus den verschiedenen Nutzungsbereichen generiert eine Reihe von Problemen oder auch Fragen:

- Handhabung immer größerer Datenmengen • Aufbau von Hierarchien
- Nutzbarkeit von Bändern
- Backup- und Restore
- Verfügbarkeit
- Performance kontra Preis
- Betrieb zentraler Speicher über Layer-2-Grenzen hinweg
- Umsetzung von Desaster Recovery Konzepten mit großen Datenmengen

Natürlich stehen diesen Problemen und Fragen auch Lösungsansätze gegenüber:

- LifeCycle Management
- Speicher-Virtualisierung
- Deduplizierung • VTL
- Thin Provisioning
- iSCSI/NFS

Diese scheinbar wegweisenden Lösungen generieren aber wieder neue Probleme. Herausragend sind dabei Herstellerabhängigkeit und die Komplexität des Betriebs zu nennen.

Hier setzt unser Forum zur Speicherinfrastruktur 2011 an. Wir analysieren:

- wie sich der Bedarf verändert
- welche Lösungsmöglichkeiten bestehen
- was die verschiedenen Lösungsansätze wirklich bringen
- wie sich die Lösungen in einen handhabbaren Betrieb einbinden lassen

Programmübersicht - ComConsult Storage-Forum 2011

Mittwoch, den 13.07.2011

9:30 bis 11:00 Uhr
Keynote: Vom traditionellen RZ zur Private Cloud
- Cloud Computing: Funktion, Chancen, Risiken
- Entwicklung der Web-Architekturen
- Server-, Speicher- und Netzwerkvirtualisierung
- Entwicklungen bei Netzwerken (Leistung, Latenz, Scale-Out)
- Strukturwandel des RZs
- Hochkonzentrierte Blade-Server: der Host-Phönix?

Dr. Franz-Joachim Kauffels, Unternehmensberater

11:00 bis 11:30 Uhr - Kaffeepause

11:30 bis 12:30 Uhr
Erfahrungen von Unternehmen mit ihrer Speicherinfrastruktur
- Datenwachstum: wie schnell wachsen die Datenbestände?
- Wie ist dem Problem des Datenwachstums beizukommen: mit organisatorischen oder technischen Mitteln?
- Was wird mehr benötigt: Volumen oder Performance?
- Welche neuen Verfahren können genutzt werden, um dem Bedarf an mehr Volumen und Performance gerecht zu werden?
- Abgrenzung zwischen verschiedenen Datenklassen und Speichertypen
- Hochverfügbarkeit der Speicherinfrastruktur
- Herausforderung Datensicherung
- Sinn und Zweck der Speichervirtualisierung
- Wie viel Speichervirtualisierung braucht ein Unternehmen?

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

12:30 bis 14:00 Uhr - Mittagspause

14:00 bis 15:00 Uhr
iSCSI im Rechenzentrum - ein Erfahrungsbericht
- Wie sieht die Grobstruktur des betrachteten RZs aus?
- Welche Anforderungen bestehen seitens der Server beim Zugriff auf den Speicher?
- Welche Aspekte haben die Entscheidung in Richtung iSCSI begünstigt?
- Welche (negativen) Erfahrungen wurden seitens Vattenfall gemacht, als das iSCSI-Netz noch als VLAN über eine gemeinsame Infrastruktur geführt wurde?
- Welche Verbesserungen haben sich ergeben durch die Separierung des iSCSI-Netzes auf dedizierte Hardware?
- Welche Leistungswerte (Durchsatz, IOs, Latenzen) liefert das aktuelle iSCSI-Netz?
- Welche Gründe sprechen aus Sicht von Vattenfall für einen Wechsel auf NFS?

Michael Witschke, Vattenfall IT

15:00 bis 15:30 Uhr - Kaffeepause

15:30 bis 16:30 Uhr
Dateibasierter Speicherzugriff - Erfahrungen aus aktuellen Speicherprojekten
- Wofür eignen sich dateibasierte Verfahren wie NFS, CIFS?
- Was ist neu an NFSv4 und wie wirkt sich das auf die Nutzbarkeit dieses Protokolls als Ersatz von blockbasiertem Speicherzugriff aus?
- Welche Vorteile ergeben sich im Umfeld von NFS bei der Nutzung für Datenbanken oder virtuelle Umgebungen?
- Welche Einschränkungen ergeben sich hierbei?
- In der Praxis erzielbare Leistungswerte: Durchsatz, IOPS, Latenzen
- Wie skaliert eine NFS-Umgebung für Datenbanken und virtuelle Maschinen?
- Gibt es eine Größenordnung (Anzahl Hosts / Anzahl VMs), ab der eine NFS-Umgebung nicht mehr effizient ist?
- Wie gestalten sich Disaster Recovery Szenarien mit NFS?

Michael Albers, Hellweg Data

16:30 bis 17:30 Uhr
Technologische Entwicklungen bei Speichersystemen
- Dauerhaftigkeit von Back-End-Systemen
- Masselose SSDs als neue Speicherklasse
- Weiterentwicklung 3D-SSDs
- Das Netz als Systembus der Virtualisierten Umgebung
- Enterprise Storage Management

Dr. Franz-Joachim Kauffels, Unternehmensberater

Happy Hour ab 18:00 Uhr

Donnerstag, den 14.07.2011

9:00 bis 10:00 Uhr
Konstruktive Sicherheitsaspekte virtualisierter Storage Networks
- Sicherheit in SAN und NAS
- Welche Gefährdungen sind in SAN und NAS relevant?
- Maßnahmen zur Absicherung von SAN und NAS - Elemente einer SAN-Sicherheitsrichtlinie
- Konzepte für eine Zonierung im SAN
- Wann sollte verschlüsselt werden?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:00 bis 11:00 Uhr
Speichervirtualisierung: Steigerung der Flexibilität und Funktionalität oder nur der Komplexität?
- Konzept der Speichervirtualisierung
- Implementierungsvarianten: Inband, Split-Path, Netzwerk-basiert
- Leistungsmerkmale aktueller Lösungen
- Nutzung zur Datenspiegelung zwischen entfernten Standorten

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:00 bis 11:30 Uhr - Kaffeepause

11:30 bis 12:30 Uhr
Möglichkeiten und Grenzen von Thin Provisioning und Deduplizierung
- Funktionsweise von Thin Provisioning
- Mögliche Ansatzpunkte für Thin Provisioning (VM, SAN, Speichersystem)
- Grenzen des Thin Provisioning durch blockbasierte Übertragung und Dateisysteme
- Deduplizierung vs. Kompression: Unterschiede und Gemeinsamkeiten
- Deduplizierung: Implementierungsvarianten out-of-band vs. inband
- Wann sind in der Praxis welche Effizienzraten zu erwarten?
- An welcher Stelle der Infrastruktur kann und sollte Deduplizierung eingesetzt werden?

N.N.

12:30 bis 14:00 Uhr - Mittagspause

14:00 bis 15:00 Uhr
Moderne Datensicherung mit VTLs und Disk-2-Disk-Verfahren
- Funktionsweise einer VTL
- Wann ist eine VTL einem allgemeinen Disk-2-Disk-Datensicherungsverfahren vorzuziehen?
- Wie kann eine VTL dabei helfen, aktuelle SLAs gerade im Bereich der Wiederherstellungszeiten einzuhalten?
- Einsatz von Snapshots im Umfeld der Datensicherung
- Datensicherung in virtuellen Umgebungen: LAN-basiert oder LAN-free?
- Möglichkeiten und Grenzen Image- und Datei-basierter Datensicherungen in virtuellen Umgebungen
- Datensicherung mit Bordmitteln der Virtualisierungshersteller und aktuellen Produkten von Drittherstellern

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

15:00 bis 15:30 Uhr - Kaffeepause

15:30 bis 16:15 Uhr
Troubleshooting im Fibre Channel

Sebastian Schröder, MEN@NET GmbH

16:15 bis 17:00 Uhr
Herstellervortrag: „Tape: Probleme, Herausforderungen und Lösungsansätze bei der Tape-Verarbeitung“

Bernd Krieger,Crossroads GmbH

Programmübersicht - ComConsult Storage-Forum 2011

Freitag, den 15.07.2011

9:00 bis 15:00 Uhr
Strategien und Produkte der führenden Hersteller
- Wie sieht die Architektur der Speicherlösung aus?
- Wie skaliert die Leistung des Speichersystems?
- Welche Hochverfügbarkeitsmechanismen besitzt das Speichersystem?
- Wie können Multi-Site Desaster Recovery Szenarien mit dem Speichersystem gelöst werden?
- Welche Vorteile bringt das Speichersystem insbesondere in virtualisierten Umgebungen?

9:00 bis 09:45 Uhr
EMC Symmetrix vMax *Carsten Haak, EMC Deutschland GmbH*

9:45 bis 10:30 Uhr
Fujitsu Eternus
Wolfgang Schenk, Fujitsu Technology Solutions GmbH

10:30 bis 11:00 Uhr - Kaffeepause

11:00 bis 11:45 Uhr
HP Lefthand *Ingo Kraft, Hewlett-Packard Deutschland GmbH*

11:45 bis 12:30 Uhr
IBM XIV *Dirk Vogelsang, IBM Deutschland GmbH*

12:30 bis 13:30 Uhr - Mittagspause

13:30 bis 14:15 Uhr
NetApp FAS/V-Serie *Roger Zink, NetApp Deutschland GmbH*

Anschließende Diskussion mit den Herstellern:
- Wie sieht die Speicherarchitektur der Zukunft aus?
- Welches Speicherzugriffsverfahren wird sich durchsetzen?
- Gehört die Zukunft den SSDs?

15:00 Uhr Ende der Veranstaltung

NEUER TERMIN UND ORT

ComConsult Storage-Forum 2011
13.07. - 15.07.11 in Bonn

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult Storage-Forum 2011

Ich buche den Kongress
ComConsult Storage-Forum 2011

☐ 13.07. - 15.07.11 in Bonn
zum Preis von € 1.790,--* zzgl. MwSt.
* gültig bis zum 31.05.2011

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 11

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Aktueller Kongress

Netzwerk-Redesign-Forum 2011

Die ComConsult Akademie veranstaltet vom 04.04. - 07.04.11 ihren Kongress „Netzwerk-Redesign Forum 2011“ in Königswinter.

Das technologische Umfeld von Netzwerken befindet sich in einem der intensivsten Änderungsprozesse der letzten 20 Jahre. Das betrifft das Rechenzentrum, das Campus-Netzwerk, neue IT-Architekturen, neue Client-Technologien bis hin zu Unified Communications. Hand in Hand mit dem Bedarf ändern sich Netzwerk-Technologien selber. Neue Standards zur Gestaltung von Netzwerken im Rechenzentrum und im Backbone sind gute Beispiele dafür. Zukunftsorientiertes und wirtschaftlich optimales Design muss dieses Gesamtbild berücksichtigen.

Die Entwicklung geht einher mit einem neuen Kampf um den Markt. Neue Standards erfordern neue Produkte, die technische Entwicklung führt zu neuen Leistungsmaßstäben bei Produkten und damit öffnet sich die Tür für einen neuen Wettbewerb in einem bisher aufgeteilten Markt. Standard-Leistung wird zunehmend durch Standard-Chips erbracht werden. Unterschiede zwischen Herstellern werden verschwimmen. Der Preis als Kaufargument wird noch wichtiger werden als bisher. Was bedeutet das für die bekannten Anbieter? Kann Cisco seine Position verteidigen, gelingt HP der großangelegte Angriff, wie verhalten sich die anderen Hersteller und welche Chancen haben sie? Leisten Netzwerke in Zukunft mehr und kosten weniger?

Das ComConsult Netzwerk Redesign Forum 2011 analysiert und diskutiert diese Änderungen und ihre Auswirkungen speziell auf die Netzwerk-Infrastrukturen.

Im Mittelpunkt des Forums stehen dementsprechend die Themenbereiche:

- Was ändert sich im Umfeld von Netzwerken? Welche neuen Architekturen und Anforderungen müssen Netzwerke konkret erfüllen?
- Wie verändern sich demgegenüber Netzwerke selber? Welche neuen Technologien und Standards kommen auf uns zu?
- Wie passen Anforderungen aus IT-Architekturen, Clients, Applikationen und Speicher mit den neuen Netzwerk-Standards zusammen? Wann und wie können die Anforderungen erfüllt werden?
- Wie verändern neue Anforderungen, neue Standards, neue Technologien und neue Produkte den Markt? Wie positionieren sich die Hersteller für den neuen und noch intensiveren Wettbewerb?

Das ComConsult Netzwerk-Redesign Forum 2011 ist ein Muss für alle Betreiber und Planer von Netzwerken. Wie immer wird sich auch 2011 hier die Branche treffen. Top-Experten, kontroverse Diskussionen, Projektbeispiele stehen auf der einen Seite. Die Hersteller stellen sich einem Musterprojekt auf der anderen Seite. Wohin geht der Netzwerk-Markt und was ist wirklich wichtig? Das ComConsult Netzwerk-Redesign Forum 2011 ist unsere Top-Veranstaltung des Jahres 2011. Versäumen Sie nicht, sich rechtzeitig einen Platz auf dieser herausragenden Veranstaltung zu sichern.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Netzwerk-Redesign-Forum 2011

Ich buche den Kongress
Netzwerk-Redesign-Forum 2011

inkl. Workshops am letzten Tag
☐ 04.04. - 07.04.11 in Königswinter
zum Preis von € 2.390,-- zzgl. MwSt.
Workshopauswahl
☐ Workshop 1: Ultra Low Latency (ULL) Networks und DCB
Workshop 2: Wireless LAN und Co

ohne Workshops am letzten Tag
☐ 04.04. - 06.04.11 in Königswinter
zum Preis von € 1.990,-- zzgl. MwSt.

☐ inkl. Report "LowLatency Networks" zum Sonderpreis von nur 338,- € zzgl. MwsSt.

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 11

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Programmübersicht - Netzwerk-Redesign Forum 2011

Montag, den 04.04.2011 - Moderation: Dr. Kauffels, Dr. Moayeri

9:30 bis 11:00 Uhr

Was sich im Netz verändert

- Wo werden 40/100 Gbit Ethernet benötigt: im RZ, im Campus, im WAN?
- Was ist im Access-Bereich nötig?
- Auswirkungen von Virtualisierung auf die Netze
- Konvergenz: ein Netz für Client-Server-Verkehr, Storage, Voice und Video?
- Mandantenfähige Netze und warum sie benötigt werden
- Warum IPv6 nicht mehr aufzuhalten ist

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:00 bis 11:30 Uhr - Kaffeepause

11:30 bis 12:45 Uhr

Entwicklung der IT-Architekturen und Auswirkungen auf Netzwerke, Teil 1

- Web-Architekturen
- Virtualisierung
- Cloud Computing

Dr. Franz-Joachim Kauffels, Unternehmensberater

12:45 bis 14:00 Uhr - Mittagspause

14:00 bis 15:00 Uhr

Netzstruktur: Layer 2 versus Layer 3

- Neue Verfahren für die Netzstrukturierung: TRILL und Shortest Path Bridging
- Sind klassische Layer-3-Strukturen überhaupt noch erforderlich?
- Können neue Layer-2-Mechanismen den Übergang zu IPv6 erleichtern?

Dipl.-Inform. Petra Borowka-Gatzweiler, Unternehmensberatung Netzwerke UBN

15:00 bis 15:45 Uhr

Verkabelung im Backbone- und Access-Bereich

- Singlemode im Backbone-Bereich, werden die Standardfasern den zukünftigen Anforderungen noch gerecht, welche Typen sind sinnvoll?
- Macht die Multimodefaser im Backbone-Bereich noch Sinn, wenn ja, welchen?
- Steckertechniken im Glasfaserbereich, gibt es qualitative Unterschiede? Welche sind sinnvoll, lohnt sich ein Umstieg auf neue Typen, wenn ja auf welche?
- Innovationen im Tertiärbereich, welche lohnen sich?
- Ist die Zeit gekommen für Kategorie-7 oder genügt auch weniger, was bringt das „Mehr“ und welche Planungskonsequenzen haben die verschiedenen Alternativen? Wie sieht die aktuelle Marktsituation aus?

Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH

15:45 bis 16:15 Uhr - Kaffeepause

16:15 bis 17:00 Uhr

Neue Entwicklungen im WAN-Bereich

- Macht Carrier Ethernet MPLS überflüssig?
- Was ist von Microsoft Direct Access zu halten?
- WAN Acceleration: wo ist diese Technologie sinnvoll?

Dipl.-Inform. Andreas Meder, ComConsult Beratung und Planung GmbH

17:00 bis 17:45 Uhr

Entwicklung der IT-Architekturen und Auswirkungen auf Netzwerke, Teil 2

- Speicher-Zentralisierung und Konsolidierung
- Besondere Rolle von Blade-Systemen
- Konzentration und Konsolidierung im Campus / WAN

Dr. Franz-Joachim Kauffels, Unternehmensberater

ab 18:00 Uhr - Happy Hour

Dienstag, den 05.04.2011 Vormittag - Moderation: Frau Borowka-Gatzweiler, Dr. Kauffels

9:00 bis 9:45 Uhr

Anforderungen von Voice und Video an Netze

- Unterschiede zwischen Voice und Video
- Anforderungen neuer Video Codecs
- Welche Bandbreite ist erforderlich?
- Wo ist QoS einzusetzen?
- Hat die die traditionelle Videokonferenz ausgedient? Welche Rolle spielen neue Verfahren wie SVC?
- PoE flächendeckend oder bei Bedarf?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

9:45 bis 10:45 Uhr

Desktop-Virtualisierung: was bedeutet das für das Netz?

- Architektur aktueller Virtueller Desktop Infrastrukturen (VDI)
- Welche Aufgaben haben die einzelnen Architekturbestandteile und welche Auswirkungen hat dies auf das Datennetz?
- Zusammenspiel mit Servervirtualisierungstechniken: Anforderungen an das logische Netzdesign
- Leistungsanforderungen an Server, Netzwerk, Speicher
- Welche Rolle spielen die Übertragungsprotokolle (z.B. RDP, ICA, PCoIP, ALP, SPICE etc.)?
- USB-Redirection: neben der technischen Herausforderung, was bedeutet das für die erforderliche Bandbreite?
- Thin Client, Zero Clients: welche Anforderungen bringen Endgeräte in den Access-Bereich?

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

10:45 bis 11:15 Uhr - Kaffeepause

11:15 bis 12:15 Uhr

Data Center Bridging oder IEEE 802.1BA als neue QoS-Architektur?

- Was bedeutet DCB? • Ersetzt DCB klassische QoS-Architekturen? • Ist der Einsatz von DCB außerhalb der Rechenzentren sinnvoll?
- Welche Rolle kommt Audio Video Bridging (AVB) Systems gemäß IEEE 802.1BA zu?

Dipl.-Inform. Petra Borowka-Gatzweiler, Unternehmensberatung Netzwerke UBN

12:15 bis 13:30 Uhr - Mittagspause

Programmübersicht - Netzwerk-Redesign Forum 2011

Dienstag, den 05.04.2011 Nachmittag- Moderation: Frau Borowka-Gatzweiler, Dr. Kauffels

13:30 bis 14:15 Uhr

Mandantenfähige Netze

- Warum werden mandantenfähige Netzstrukturen benötigt?
- Gastnetz über LAN, WLAN oder LTE/GSM?
- Tücken bei Network Access Control
- Anforderungen an Firewalls, Intrusion-Prevention-Systeme und Security Gateways
- Was wird durch MACsec und 802.1X-2010 geändert?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:15 bis 15:00 Uhr

Zukunft der Netzanalyse

- Vorratsdatenspeicherung im Netz?
- Infrastruktur für forensische Untersuchungen im Netz
- Kommt die Vorratsdatenspeicherung der Fehlersuche und der IT-Sicherheit zugute?
- Paketanalyse oder intelligente Expertensysteme?
- Paketanalyse - ein Mehrwert für das Netzwerkmanagement?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

15:00 bis 15:30 Uhr - Kaffeepause

15:30 bis 16:45 Uhr

IPv6-Migration

- Konstellationen
- Grundlegende Ansätze
- Beiträge der Kommunikations-Endpunkte (Clients, Server, ...)
- Konkretisierung aus Sicht der Kommunikations-Endpunkte
  - Windows • Unix • Drucker?! • Drucker und Multifunktionsgeräte? • IP-Telefone, MDAs etc.?

Dipl.-Inform. Oliver Flüs, ComConsult Beratung und Planung GmbH

Mittwoch, den 06.04.2011 - Moderation: Frau Borowka-Gatzweiler, Dr. Moayeri

9:00 bis 9:45 Uhr

Anforderungen an die Netzkomponenten: virtuelle Ausschreibung

- Performance-Anforderungen
- Unterstützung neuer Verfahren und Standards: DCB, TRIIL, SPB, …
- Energie-Effizienz
- Netzmanagement

Dipl.-Inform. Petra Borowka-Gatzweiler, Unternehmensberatung Netzwerke UBN

9:45 bis 15:00 Uhr

Hersteller stellen sich der virtuellen Ausschreibung

12:45 bis 14:00 Uhr - Mittagspause

15:00 bis 15:30 Uhr - Kaffeepause

15:30 bis 16:00 Uhr

Diskussionsrunde: Frau Borowka-Gatzweiler, Dr. Moayeri, Dr. Kauffels und die Hersteller

Donnerstag, den 07.04.2011 - Ein-Tages-Intensiv-Trainings/Workshops - 9:00 - 15:30 Uhr

Workshop 1:

Ultra Low Latency (ULL) Networks und DCB

- Allgemeine Anwendungsbereiche für ULL-Networks, z.B. Finanznetze
- Das ULL Network als Systembus Virtualisierter Gesamtlösungen
- Sind vollständige, skalierbare Netze mit einer Ende-zu-Ende Verzögerung im Bereich weniger Mikrosekunden machbar?
- Wie sieht das Chipdesign für Switches aus, die mit Latenzen im Bereich einiger Hundert Nanosekunden arbeiten?
- Die tragende Rolle der DCB-Funktionen
- Wie sind die Kosten dafür zu beurteilen? Ist das Ganze unerschwinglich?
- Reichen Designansätze wie Clos-Netze mit TRILL oder PLSB aus oder müssen noch weiter optimierte Konstruktionen betrachtet werden?
- Integration von ULL-Networks in Virtualisierungskonzepte
- Die Rolle etablierter Hersteller ist hier noch bescheiden. Wer sind die Herausforderer und wie ist deren Gesamtstrategie?

Dr. Franz-Joachim Kauffels, Unternehmensberater

Workshop 2:

Wireless LAN und Co.

- WLAN-Design mit IEEE 802.11n
- Herausforderung an Planungstools und Messtechnik durch neue WAN-Technologien
- Controller-basiertes WLAN-Design: Architekturvarianten und Herstellerlösungen im Vergleich
- Long-Term Evolution: Wohin steuert der Mobilfunk?
- Frequenzmanagement und Regulierung
- Sichere WLANs: Entsorgung von Altlasten und Umgang mit neuen Techniken

Dr. Simon Hoff, Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

10:30 bis 11:00 Uhr - Kaffeepause

12:30 bis 14:00 Uhr - Mittagspause

15:30 Uhr - Ende der Veranstaltung

Aktueller Kongress

IT-Sicherheits-Forum 2011

Die ComConsult Akademie veranstaltet vom 23.05. - 24.05.11 ihren Kongress „IT-Sicherheits-Forum 2011“ in Königswinter.

Datendiebstahl und Datenverlust sind neben schadenstiftender Software wesentliche Bedrohungen der Informationssicherheit. Dies hat Wikileaks im Jahr 2010 plakativ bewiesen. Dem steht die aktuelle Entwicklung in der IT mit hoher Mobilität, Collaboration unterschiedlichster Parteien bei gleichzeitiger Forderung nach maximaler Konsolidierung gegenüber, was die konsequente Virtualisierung der IT bis hin zu Cloud-Computing-Modellen zur Folge hat. Diese Dynamik verbunden mit immer neuen Schwachstellen in den IT-Systemen stellt eine besondere Herausforderung der Informationssicherheit dar.

In diesem Zusammenhang muss auch die Verwendung von netzintegrierten Standard-IT-Komponenten zur Steuerung von Prozessen in Anlagen bewertet werden. Stuxnet hat hier eindrucksvoll gezeigt, dass eine Schadsoftware zielgerichtet physikalische Systeme manipulieren kann und hat gleichzeitig der Informationssicherheit ein Armutszeugnis ausgestellt, das zum Umdenken zwingt.

Ein für die Informationssicherheit besonderer Trend ist die "Consumerization of IT". Unter diesem Schlagwort werden unterschiedliche Nutzungsformen von Consumer-Produkten in der Enterprise-IT verstanden (z.B. iPhone und Skype). In diesen Bereich muss auch die Nutzung

sozialer Netze im Unternehmen betrachtet werden. Hier wächst der Druck auf die Informationssicherheit solche Produkte freizugeben, was zwangsläufig einen nicht unerheblichen Katalog von Sicherheitsmaßnahmen nach sich zieht.

Moderne Informationssicherheit muss auf werkzeuggestützten automatisierten Prozessen basieren, damit schnell und adaptiv auf eine sich stetig ändernde Gefährdungslage reagiert werden kann. Hierzu muss die gesamte IT ganzheitlich durch entsprechende miteinander kooperierende Sicherheitskomponenten in Endgerät, Netzwerk und Rechenzentrum geschützt werden, um

- unerlaubte und schadenstiftende Zugriffe auf Ressourcen zu erkennen und automatisch zu blockieren
- zu verhindern, dass entsprechend klassifizierte Informationen das Netz verlassen bzw. auf einem nicht hierfür freigegebenen Datenträger gespeichert werden
- Endgeräte, die nicht den Konfigurationsvorgaben entsprechen oder sogar infiziert sind, automatisch in einem Quarantäne-Netz zu isolieren
- Daten bedarfsorientiert bei Transport und Speicherung systematisch durch kryptographische Methoden hinsichtlich Vertraulichkeit und Integrität zu schützen

Wie der Balanceakt zwischen dem notwendigen technischen Apparat und der wirtschaftlichen Betreibbarkeit der IT gelingen kann, erfahren Sie im ComConsult IT-Sicherheits-Forum 2011. Hier werden die wichtigsten Bedarfsentwicklungen analysiert, die neuesten Technologien gegenübergestellt und Empfehlungen für ein sicheres IT-Design einen sicheren Betrieb erarbeitet.

Das ComConsult IT-Sicherheits-Forum 2011 ist die zentrale IT-Sicherheits-Veranstaltung des Jahres 2011. Sie ist für jeden Entscheider, IT-Sicherheitsbeauftragten, Planer und Betreiber in diesem Bereich ein absolutes Muss. Hier trifft sich die Branche.

Sichern Sie sich rechtzeitig einen Platz in dieser herausragenden Veranstaltung!

Frühbucherphase bis zum 31.03.2011

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

IT-Sicherheits-Forum 2011

Ich buche den Kongress
IT-Sicherheits-Forum 2011

☐ 23.05. - 24.05.11 in Königswinter
zum Preis von € 1.590,--* zzgl. MwSt.
*gültig bis zum 31.03.2011

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 11

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

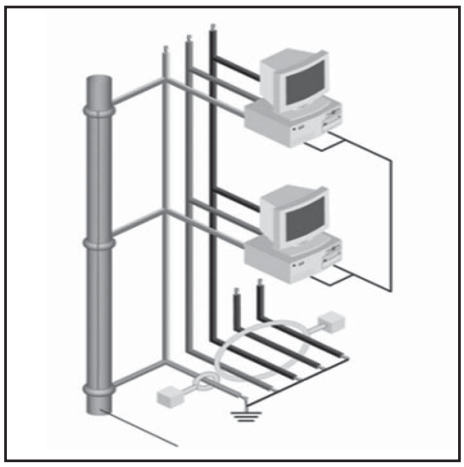
Neues Seminar

Netzanalyse und sicherheitstechnische Bewertung elektrischer Netze in Rechenzentren

Die ComConsult Akademie veranstaltet vom 11.04. - 13.04.11 erstmalig die neue Veranstaltung "Netzanalyse und sicherheitstechnische Bewertung elektrischer Netze in Rechenzentren" in Bonn.

Die Verfügbarkeit und Anfälligkeit der elektrischen Netze wird heute unterschätzt. Schon leichte Störungen führen zu Ausfällen der EDV, trotz eingebauter Schutzeinrichtungen. Kostendruck und knappe Zeitvorgaben sowie lange Lieferzeiten führen zu Fehlentscheidungen in der Planung und Installation der elektrischen Anlagen für den EDV-Betrieb. Verfügbarkeitsbetrachtungen sind nie gemacht worden und es sind keine geeigneten Hilfs-und Messmittel eingebaut, welche Abweichungen des Betriebes rechtzeitig erkennen lassen, um Ausfälle und Störungen zu verhindern.

Der neue Lehrgang vom Sachverständigenbüro Dipl.-Ing. Karl-Heinz Otto erläutert die Grundlagen der in Arbeit befindlichen Richtlinie des BVS aus unabhängiger Sicht und 30 Jahren eigene Schadenerfahrungen und der Kollegen der öffentlich bestellten und vereidigten Sachverständigen der Bundesfachgruppe Elektronik und EDV.



Themenschwerpunkte dieses Seminars sind:

- Standort und Versorgungsanbindung an den Energieversorger für ein RZ
- Fehlerquellen aus elektrischer Sicht durch die Umgebung
- Blitzhäufigkeit und Einschlagverhalten am Standort
- Erdungssystem und Potenzialausgleichsanlage
- Blitzschutz- Anlage
- Ströme auf dem Erdungssystem und deren Frequenzverhalten
- Einspeisung der Transformatoren und Auslegung der Mittelspannung
- Überspannungsschutz für die Mittelspannungsanlage, Niederspannung, Datenleitungen
- Aufbau der Hauptstromverteilung vom Einspeisepunkt bis zur letzten Steckdose als TN-S für eine zu betrachtende Versorgungseinheit
- Betrachtung von 4- oder 3-poligen Schaltern bei Bypassschaltungen
- Kurzschluss- und Selektivitätsbetrachtungen
- Monitoring Systeme der Haupt- und Unterverteilungen
- Netzqualitätskontrolle
- Lastfluss-Darstellungen
- Kontrolle des Spannungsfalls
- Prüfmöglichkeiten durch gesicherte Prüfpunkte
- Automatische Prüfung gemäß BGV A3
- Bewertung und Klassifikation der elektrischen Systeme nach realen Schadenvorkommnissen

In 2 Tagen werden die Grundzüge an praktischen Fallbeispielen und Simulationsprogrammen erläutert und vertieft. Daher sind Laptop mit Administratorrechten für den Seminarerfolg notwendig mitzubringen.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Netzanalyse und sicherheitstechnische Bewertung elektrischer Netze in Rechenzentren

Ich buche die Sonderveranstaltung
Netzanalyse und sicherheitstechnische Bewertung elektrischer Netze in Rechenzentren
☐ 11.04. - 13.04.11 in Bonn
zum Preis von € 1.890,-- zzgl. MwSt.

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 11

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Neuer Kongress

ComConsult IPv6-Forum 2011

Die ComConsult Akademie veranstaltet vom 09.05. - 11.05.11 ihren neuen Kongress „ComConsult IPv6-Forum 2011“ in Königswinter.

Der Wechsel von IPv4 auf IPv6 ist unvermeidbar und wird in 2011 weltweit im großen Stil beginnen. Dabei liefert IPv6 nicht nur einen neuen Adressraum, sondern ein völlig verändertes Betriebsszenario. DNS, DHCP und wesentliche Teile der vorhandenen Sicherheits-Lösungen müssen neu durchdacht und angepasst werden. Speziell Firewall- und NAT-Installationen sind betroffen.

Der Wechsel von IPv4 auf IPv6 ist aus mehreren Gründen komplex und bedarf einer sorgfältigen Planung:

- Es sind Applikationen, Endgeräte, Server, Drucker, Netzwerk-Komponenten betroffen. Der Wechsel muss so erfolgen, dass er über alle diese Komponenten hinweg funktioniert
- Viele Applikationen und Komponenten sind IPv6-ready, aber nicht alle und nicht in allen Firmware-Versionen. Hier muss eine Inventur erfolgen, ggf. müssen Beschaffungen ausgelöst werden
- Ein Sofortumstieg wird selten machbar sein, ein sinnvoller Migrationsweg muss gefunden werden, der alle Anwendungen und Gerätetypen sowie ihre Eigenarten berücksichtigt

- Externe Dienste werden in Kürze auf der Basis von IPv6 angeboten werden. Das betrifft Cloud-Services, Email-Dienste und Kollaboration im weitesten Sinne. In jedem Fall muss geklärt werden, wie diese Dienste in eine vorhandene IPv4-Umgebung eingebunden werden
- Da IPv6 ein neues und anderes Betriebs-Szenario mitbringt, ist zu klären wie dieses genutzt wird. Tatsächlich bestehen erhebliche Optionen, deren Tragweite auf den ersten Blick nicht klar ist

Hier setzt unser ComConsult IPv6-Forum 2011 an. Es greift diese Fragen strukturiert auf und zeigt den optimalen Weg nach IPv6 auf. Im Einzelnen leistet das IPv6 Forum 2011:

- IPv6 und seine technische Konzeption wird erklärt und diskutiert
- Die verschiedenen Betriebsszenarien werden verglichen
- Migrationswege werden analysiert und bewertet
- Die technische Situation der verschiedenen Komponenten vom Endgerät über den Server bis zum Netzwerk wird erläutert
- Beispielprojekte und Laboranalysen werden vorgestellt
- Empfehlungen für den besten Weg nach IPv6 werden von ausgewählten Experten vorgestellt

Das ComConsult IPv6-Forum ist ein Muss für alle Betreiber und Planer von Netzwerken, Endgeräten, Servern, Speichersystemen und Applikationen im Netzwerk. Versäumen Sie nicht, sich rechtzeitig einen Platz auf dieser herausragenden Veranstaltung zu sichern.

Die Moderation des Forums übernimmt Markus Schaub von ComConsult-Study.tv.

Programmübersicht - IPv6-Forum 2011

Montag, den 09.05. 11 - „Motivation und Grundlagen“

9:30 bis 11:00 Uhr
IPv6-Vorbereitung: Warum, wann und wie?
- Warum muss man sich schon jetzt auf IPv6 vorbereiten?
- Wie lange kann die Umstellung noch vermieden werden?
- Was sich mit IPv6 ändert
- Anforderungen an das Netz
- Sinnvolle Bestandteile eines IPv6-Projektes
- Erfahrungen eines Umstellungs-Projektes

Markus Schaub, ComConsult Research Ltd., ComConsult-Study.tv

11:00 bis 11:30 Uhr - Kaffeepause

11:30 bis 12:45 Uhr
Was ist IPv6: Von der Adresse zu neuen Betriebsformen
- Neue Adressen, Adresstypen und Adressdarstellung
- Wie funktioniert der Parallelbetrieb IPv4 und IPv6?
- Wie wirkt sich IPv6 auf bestehende IP-Subnetzstrukturen aus?
- IPv6-Routing
- Die neue Rolle des Routers
- Anforderungen an Komponenten
- Migrations-Varianten

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

12:45 bis 14:15 Uhr - Mittagspause

14:15 bis 15:30 Uhr
IPv6-Konfigurationsparameter und Entscheidungen aus betrieblicher Sicht
- Welche Art der Adresszuteilung ist wann sinnvoll? (Autoconfiguration, Autoconfiguration mit ergänzendem DHCP, Stateful DHCP)
- Privacy options: (Warum? Ansätze? Was setzt man wo/wann ein?)
- Vorteil-Nachteil-Betrachtung zu den Alternativen
- Rolle der Netzwerk-Komponenten bei der Konfigurationsverwaltung
- Umsetzung und produktspezifische Anteile am Beispiel Windows 7

Dipl.-Inform. Oliver Flüs, ComConsult Beratung und Planung GmbH

15:30 bis 16:00 Uhr - Kaffeepause

16:00 bis 16:45 Uhr
IPv6 @ Bosch
- Vorgehen (Vorgeschichte, Projektplanung, Pilot)
- Erfahrungen (LAN, WAN, Internet-Zugang, Adresskonzept, DHCP, DNS, autoconfiguration)
- Fazit

Anja Moog-Lölkes, Robert Bosch GmbH

16:45 bis 17:30 Uhr
Trouble-Shooting in IPv6-Umgebungen
- Was ist anders? • Erfahrungswerte • Empfehlungen

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

ab 18:00 Uhr - Happy Hour

Programmübersicht - IPv6-Forum 2011

Dienstag, den 10.05.11 - „Sicherheit, UC, Mobiles Arbeiten“

9:00 bis 10:00 Uhr
IPv6-Readyness: Funktioniert Interoperabilität?
- Wer garantiert IPv6-Readyness?
- Wie laufen Interoperabilitätstests ab?
- Wie vertrauenswürdig sind die Angaben?
- Komponentensituation im Netzwerkbereich

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

10:00 bis 10:45 Uhr
IPv6 Migrationsszenarien im TK- und UC- Lösungsgeschäft
- Besonderheiten im Telekommunikationsumfeld
- Portfoliobetrachtungen vom Client bis zum Server
- Planung und Projektmanagement von komplexen Projekten

Michael Tietsch, Siemens Enterprise Communications GmbH und CoKG

10:45 bis 11:15 Uhr - Kaffeepause

11:15 bis 12:45 Uhr
IPv6 und mobiles Arbeiten
- IPv6 im Internet und IPv6 im Intranet – zwei unterschiedliche Anforderungen
- IPv6 in Wireless LANs
- Performance-Aspekte für mobiles Arbeiten
- Wie lassen sich Android, iPhone & Co. integrieren?
- Vorführung, Erfahrungen aus Test-Installationen

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

12:45 bis 14:00 Uhr - Mittagspause

14:00 bis 15:30 Uhr
Sicherheitsaspekte bei IPv6
- Gefährdungslage: Ansätze für Angriffe auf IPv6-Kommunikation
- IPsec unter IPv6
- Security in IPv6-Spezifikationen: Basismechanismen und Standarddienste • Secure Neighbour Discovery SEND
- Firewalls, IPS und Security Gateways und IPv6
- VPN und IPv6 • Sicherheitsaspekte von MS Direct Access
- Die zukünftige Rolle von NAT

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:30 bis 16:00 Uhr - Kaffeepause

16:00 bis 17:00 Uhr
IPv6 in virtuellen Umgebungen
- Sprunghafter Anstieg des IP-Adressbedarfs: Nach den PCs und IP-Telefonen kommen die Thin-Clients mit virtuellen Desktops
- Wie weit geht die IPv6-Fähigkeit heutiger Virtualisierungslösungen?
- Welche Herausforderungen bringen IPv6-nutzende Betriebssysteme in virtuellen Umgebungen?
- Müssen virtuelle Switches IPv6-fähig sein?
- Welche Anforderungen bringt IPv6 für IP-basierte Speicherprotokolle (iSCSI, NFS)?
- Layer-3-Grenzen überschreitende Virtualisierungscluster mittels Microsoft Hyper-V, Windows Server Failover Clustering (WSFC) und IPv6

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

17:00 bis 17:45 Uhr
L4/7-Switching als Hilfsmittel für die Migration zu IPv6

Ralf Sydekum, F5 Networks GmbH

Mittwoch, den 11.05.11 - „Marktsituation“

9:00 bis 9:45 Uhr
IPv6 für Kunden der Deutschen Telekom
- Warum benötigen wir IPv6 und warum führen wir IPv6 ein?
- Wie führen wir IPv6 ein und wie können Kunden IPv6 nutzen?
- Herausforderungen im Enterpriseumfeld
- Was kommt nach der IPv6 Einführung?
- Company Connect und IPv6

Karsten Fleischhauer, Deutsche Telekom Netzproduktion GmbH

9:45 bis 10:30 Uhr
IPv6-Unterstützung bei Endgeräten
- Wie ist der Stand der IPv6-Unterstüzung im Endgerätebereich?
- Projekt- und Testerfahrungen *N.N.*

10:30 bis 11:00 Uhr - Kaffeepause

11:00 bis 11:45 Uhr
Cisco IPv6 im Enterprise-Netzwerk
- Readiness IPv6: was kann die HW/SW heute?
- Roadmap IPv6: wie geht‘s weiter?
- Herausforderung IPv6: wo sind die Ecken und Kanten?

Gerd Pflüger, Cisco Germany GmbH

11:45 bis 12:45 Uhr
IPv6 aus der Perspektive von IP Address Management (IPAM)

Thomas Erhardt, n3k Informatik GmbH

12:45 bis 14:00 Uhr - Mittagspause

14:00 bis 14:45 Uhr
Projekterfahrungen mit IPv6
- Einführung von IPv6 für Telefonie beim BMI

Constanze Bürger, BMI Referat IT 5
(IT-Infrastrukturen und IT-Sicherheitsmanagement des Bundes)

14:45 bis 15:30 Uhr
Diskussionsrunde: Wie ausgereift ist die Technologie?
- Sind Markt und Produkte wirklich reif für die Umstellung?
- Machen die bekannten Migrationsverfahren Sinn?
- Wie tragfähig ist ein Parallelbetrieb?
- Wie groß sind die Sicherheitsrisiken?

15:30 Uhr Ende der Veranstaltung

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult IPv6-Forum 2011

Ich buche den Kongress
ComConsult IPv6-Forum 2011

☐ 09.05. - 11.05.11 in Königswinter
zum Preis von € 1.990,-- zzgl. MwSt.

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 11

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Schwerpunktthema

Neue Verfahren für mandanten-fähige Netze

Fortsetzung von Seite 1

Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück

Dr. Behrooz Moayeri ist in der ComConsult Beratung und Planung GmbH als Mitglied der Geschäftsleitung tätig. Er ist zudem Leiter des Competence Centers Netze.

- Dank der zugrundeliegenden Routing-Protokolle kann MPLS auf jede Backbone-Topologie (Ring, Stern, vermascht) abgebildet werden.
- MPLS bietet eine Reihe von Mechanismen für Verkehrslenkung und Traffic Engineering (TE).
- MPLS hat sich trotz der Komplexität des Verfahrens in der Praxis als sehr robust erwiesen.
- MPLS ist sehr skalierbar, weil das Verfahren mit jeder neuen physikalischen Übertragungstechnik kombiniert werden kann. Es war zum Beispiel überhaupt kein Problem, MPLS mit 10Gigabit Ethernet zu kombinieren. Hier lag zum Beispiel ein ganz entscheidender Vorteil von MPLS gegenüber Asynchronous Transfer Mode (ATM), einer Technologie, die bei 622 Mbit/s stehen blieb.
- Anders als herkömmliches IP Routing unterstützte MPLS von Anfang an Virtual Private Networks (VPNs) und damit auch Mandantenfähigkeit.
- MPLS unterstützt anders als zum Beispiel Synchronous Digital Hierarchy (SDH) Any-to-any-Kommunikation innerhalb eines Mandantennetzes.
- Automatismen in einem MPLS-Netz ermöglichen ein sogenanntes Edge Provisioning, d. h. das Hinzufügen eines Standorts zu einem Mandantennetz beschränkt sich auf die Zuordnung des Edge Devices am Standort zum betreffenden VPN.

Der Siegeszug von Ethernet in lokalen Netzen brachte schon vor ca. zehn Jahren Hersteller und Netzbetreiber auf die Idee, innerhalb des für die Ethernet-Standardisierung zuständigen Institute of Electrical and Electronic Engineers (IEEE) an zusätzlichen Ethernet Standards für Carrier-Netze zu arbeiten. Diese Arbeit trägt viele Früchte, u. a. die beiden verabschiedeten Standards für Provider Bridging (IEEE 802.1ad) sowie Provider Backbone Bridging (IEEE 802.1ah) und den kurz vor der Verabschiedung stehenden Standard Shortest Path Bridging (IEEE 802.1aq). Zusammen bilden vor allem diese drei Standards die Basis für das sogenannte Carrier Ethernet, das MPLS hinsichtlich der o. g. Vorzüge in fast nichts nachsteht und daher eine Technologie darstellt, die das Potenzial hat, MPLS in vielen Bereichen zu verdrängen.

2. Ethernet: Technologie für mandantenfähige Backbones

Die wichtigsten Standards des IEEE für den Einsatz von Ethernet in mandantenfähigen Backbones sind:

- IEEE 802.1ad: Provider Bridged Networks
- IEEE 802.1ag: Ethernet Operations, Administration and Maintenance (OAM)
- IEEE 802.1ah: Provider Backbone Bridged Networks
- IEEE 802.1aq: Virtual Bridged Local Area Networks - Amendment 8: Shortest Path Bridging

Diese Standards befassen sich vor allem mit Ethernet im Backbone, während sich die Spezifikation IEEE 802.3ah-2004 mit dem Titel „Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks“ den Einsatz von Ethernet als Zugangsplattform zu Provider Backbones regelt. Im Standard IEEE 802.3ah geht es eher um die physikalischen Schnittstellen und Übertragungsverfahren, so dass wir uns im Folgenden eher auf die Standards aus der Reihe IEEE 802.1 konzentrieren. Diese Standards befassen sich mit den Mechanismen auf der Ebene der Schicht 2.

Der Standard IEEE 802.1ad sieht vor, dass beim Übergang vom LAN zum WAN ein Service Provider Tag als Bestandteil des Headers hinzugefügt wird. Dieser VLAN-Tag wird als Service Virtual Local Area Network (S-VLAN) Tag bezeichnet und unterscheidet sich vom Customer Virtual Local Area Network (C-VLAN) Tag. C-VLAN-Tags werden von Kunden und S-VLAN-Tags vom Provider vergeben und verwaltet. So entsteht ein „Stapel“ von Tags im Frame Header, weshalb das Verfahren auch als „Q-in-Q Tagging“ bekannt ist (Q steht dabei für den Standard IEEE 802.1Q, der erstmalig die Verwendung von VLAN-Tags regelte).

IEEE 802.1ah erweitert den Ansatz von IEEE 802.1ad in dem Sinne, dass eine vollständige Einkapselung eines Ethernet-Rahmens des Kunden im vollständigen Ethernet-Rahmen des Providers inkl. eigener Adressen vorgesehen wird. Provider und Kunden nutzen jeweils einen eigenen Medium Access Control (MAC) Header. Das Verfahren ist daher als MAC-in-MAC bzw. MAC Address Stacking bekannt.

Provider Bridging (PB) bzw. Provider Backbone Bridging (PBB) bilden zusammen die Grundlage eines neuen Anwendungsgebiets von Ethernet, das manchmal als „Carrier Ethernet" bezeichnet wird. Damit ist die Nutzung von Ethernet als Transporttechnologie im WAN gemeint (siehe Abbildung 1).

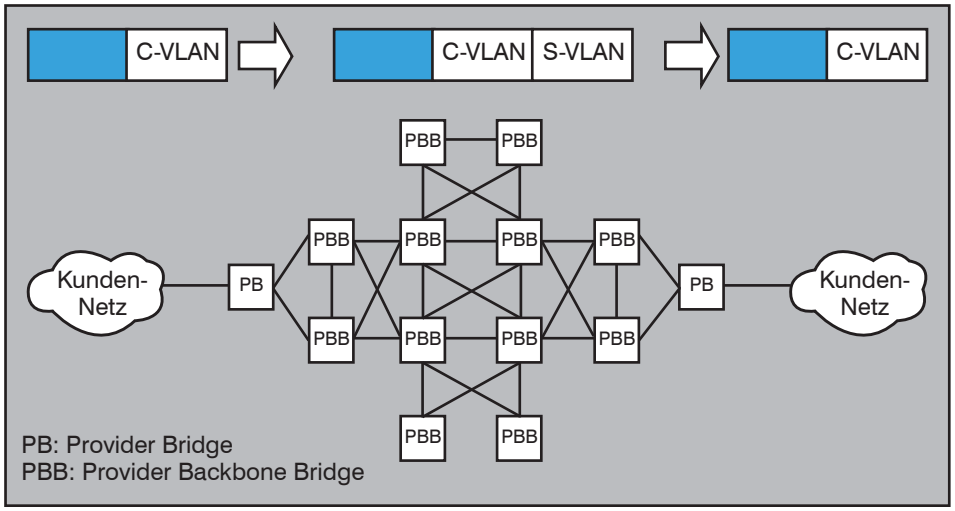


Abbildung 1: Provider Bridges fügen den Rahmen S-VLAN-Tags hinzu

3. Neue Redundanzmechanismen

Ein Problem im Zusammenhang mit Carrier Ethernet stellen die bisher in Ethernet-Netzen üblichen Redundanzmechanismen dar. Der in Ethernet-Netzen dominierende Layer-2-Redundanzmechanismus ist Spanning Tree. Spanning Tree in der bisherigen Form ist aber für große Backbones nicht geeignet. Das Protokoll ist nicht skalierbar und der Algorithmus nicht robust genug. Hinzu kommt, dass der Netzbetreiber mit Spanning Tree nur wenige Möglichkeiten für die gezielte Lenkung des Verkehrs hat. Ein weiterer Nachteil besteht darin, dass bei Anwendung von Spanning Tree Leitungen nicht effizient genutzt werden. Per definitionem macht Spanning Tree aus einem vermaschten Netz eine Topologie, in der es zwischen zwei beliebigen Punkten im Netz nur einen aktiven Pfad geben darf. Somit werden alle anderen Pfade vom Algorithmus blockiert, wie in der Abbildung 2 dargestellt.

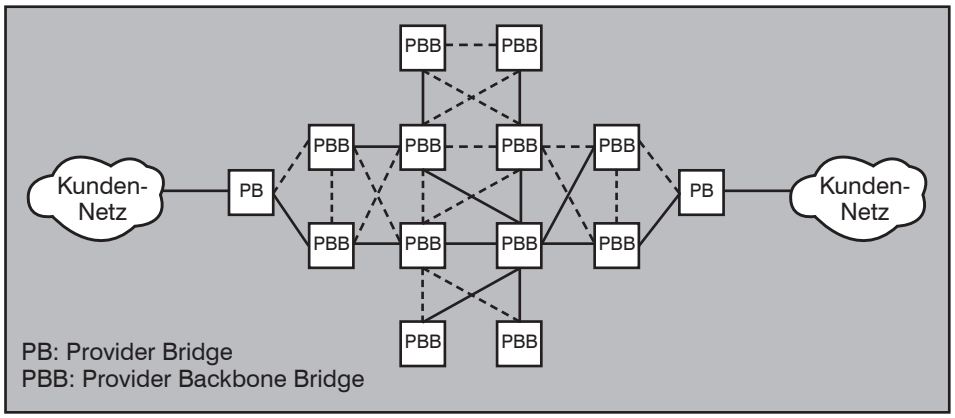


Abbildung 2: Blockierungen von Links durch Spanning Tree

Aber vielleicht der gravierendste Nachteil von Spanning Tree für Backbone-Betreiber besteht darin, dass die Redundanzmechanismen des Backbones und der Kundennetze nicht sauber voneinander getrennt sind. Das Spanning-Tree-Verfahren bietet keinerlei Schutzmechanismus, welcher die Auswirkung von Fehlern und Änderungen auf einen Netzbereich begrenzen würde. Die Neukonfiguration von Spanning Tree kann das ganze Netz in Mitleidenschaft ziehen. Es reicht, dass aufgrund eines Fehlerzustandes die Neukonfiguration des Netzes sich ständig wiederholt, oder dass die Prozessoren der Netzkomponenten durch die ständige Berechnung des Spanning Tree in den Hochlastbereich geraten, und schon sind das ganze Netz und die darüber abgewickelten Dienste betroffen. Solche Szenarien sind in der Praxis häufig eingetreten. Mit Spanning Tree kann somit ein Kundennetz andere beeinflussen, was aus der Sicht des Backbone-Betreibers nicht akzeptabel ist.

Somit ermöglicht die Kombination aus den LAN-Standards IEEE 802.3 (Ethernet), IEEE 802.1D (Bridging mit Spanning Tree), IEEE 802.1Q (VLAN), IEEE 802.1ad (Privider Bridging) und IEEE 802.1ah (Provider Backbone Bridging) zwar eine Differenzierung zwischen verschiedenen Kunden in einem mandantenfähigen Netz, aber Erweiterungen dieser Standards sind erforderlich, um Ethernet „Provider-tauglich" zu machen.

4. Shortest Path Bridging

In einem Carrier Ethernet ist ein neues Bridging-Verfahren notwendig, das einerseits dem Provider mehr Kontrolle über das Netz gibt und andererseits besser als das herkömmliche Ethernet die Kundennetze voneinander entkoppelt. Ein solches Verfahren ist in der Abbildung 3 dargestellt.

Abbildung 3 zeigt den Fluss eines Rahmens durch das Provider-Netz. Dabei wird die vom Service Provider verwaltete MAC-Adresse (S-MAC) dafür verwendet, den Ethernet-Rahmen zu einem Ziel innerhalb des Provider-Netzes, in der Regel zu einer Provider Bridge, weiterzuleiten. Die vom Service Provider verwaltete VLAN-ID (S-VLAN-Tag) dient dazu, in der Provider Bridge (PB) den Rahmen zum betreffenden Kundennetz zu transportieren.

Das Kundennetz übergibt dem Backbone einen Rahmen mit den herkömmlichen Header- und Trailer-Informationen, nämlich die im Kundenbereich (C für Customer) verwendeten und verwalteten Felder:

- Destination Address (C-DA)
- Source Address (C-SA)
- VLAN Identifier (C-Tag)
- Nutzdaten (C payload)
- Frame Check Sequence (FCS)

Die Provider Bridge (PB) übernimmt die Q-in-Q-Enkapsulierung und fügt dem Rahmen einen vom Provider verwalteten

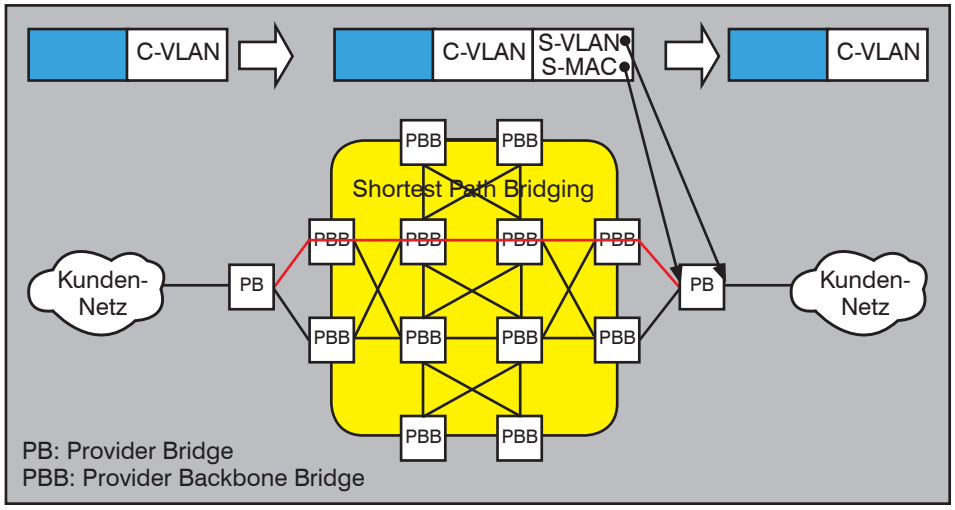


Abbildung 3: Neues Bridging-Verfahren

VLAN Identifier hinzu (S-Tag). Dieser Identifier wird im Access-Netz auf der Basis von IEEE 802.1ad für die Unterscheidung zwischen verschiedenen Kundennetzen verwendet.

Über das Access-Netz gelangt der Rahmen zu einem Aggregierungs- oder Distributionsnetz auf der Basis von IEEE 802.1ah. Der Übergabepunkt zu diesem Netz ist die Provider Backbone Bridge (PBB), welche die Aufgabe der Enkapsulierung gemäß 802.1ah übernimmt. Somit fügt die PBB dem Rahmen einen vollständigen MAC Header hinzu, einschließlich der im Backbone-Bereich B verwendeten und vom Service Provider verwalteten MAC-Adressen:

- Destination Address (B-DA)
- Source Address (B-SA)

Diese Header-Informationen dienen der Weiterleitung des Rahmens im Providernetz. Dabei werden die Tabellen mit den B-MAC-Adressen mittels des Routing-Protokolls IS-IS aktualisiert, und nicht wie bei IEEE 802.1D durch das „Lernen“ der MAC-Adressen. Auch das bei IEEE 802.1D vorgesehene Fluten von Paketen mit unbekannter Ziel-MAC-Adresse entfällt im Backbone.

Eine Carrier-Ethernet-Infrastruktur muss bestimmte Eigenschaften etablierter WAN-Backbones wie SDH ebenfalls anbieten, wenn sie von einem Service Provider als Transportnetz genutzt werden soll. Zu diesen Eigenschaften gehört die schnelle Umschaltung bei Ausfällen, im SDH-Bereich Automatic Protection Switching (APS) genannt. In einem Transportnetz auf der Basis von Ethernet kann das Verfahren Spanning Tree aufgrund der o. g. Nachteile nicht genutzt werden. Geeigneter ist Link Aggregation gemäß IEEE 802.3ad. Dieses Verfahren ist jedoch in der bisher standardisierten Ausprägung nur zwischen zwei Enden einer Ethernet-Verbindung definiert, zum Beispiel zwischen zwei Switches. Erweitert man jedoch dieses Verfahren, kann es auf andere Szenarien angewandt werden. Ein solches Szenario ist in der Abbildung 4 dargestellt.

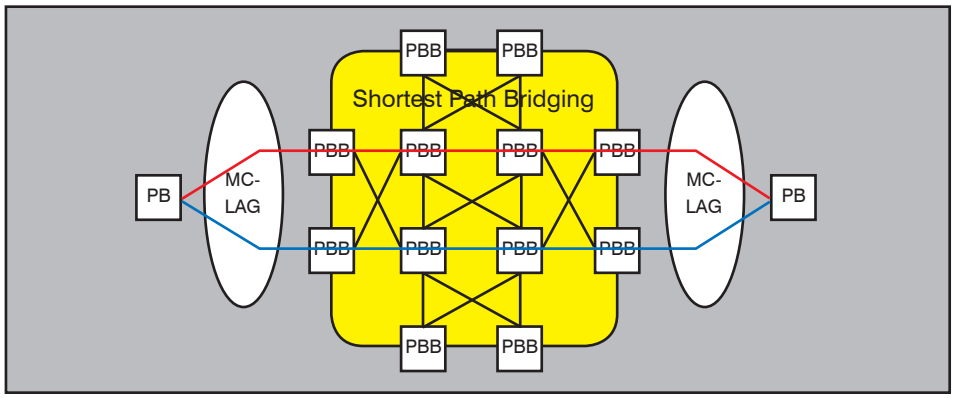


Abbildung 4: Multi-Chassis Link Aggregation

Die in der Abbildung 4 dargestellte Multi-Chassis Link Aggregation (MC-LAG) ist ein Verfahren, in dem analog zum sogenannten Linear APS bei SDH bei Ausfällen einer Zugangsleitung auf eine zweite Verbindung umgeschaltet wird.

MC-LAG nutzt ein Steuerungsprotokoll zwischen den beiden PBBs eines Paares. Das LACP (Link Aggregation Control Protocol, definiert in IEEE 802.3ad) wird zwischen PBB- und PB-Komponenten genutzt, um Ausfälle zu signalisieren.

Im Kern des Providernetzes bietet das Shortest Path Bridging (SPB) die Failover-Mechanismen, die auf dem Routing-Protokoll IS-IS basieren. IS-IS hat sich in Service-Provider-Netzen als robust und stabil erwiesen, so dass einer Nutzung dieses Protokolls zum „Routen“ von MAC-Adressen nichts im Wege steht.

Im Rahmen von IEEE 802.1aq wird SPB standardisiert. Die ersten Pre-Standard-Produkte sind verfügbar. Erste Interoperabilitätstests sind erfolgreich verlaufen. Mit der baldigen Verabschiedung des Standards wird gerechnet.

5. Fazit zu mandantenfähigen Ethernet-Backbones

Als Fazit dieses Abschnitts zu mandantenfähigen Ethernet-Backbones kann zusammengefasst werden:

- Ethernet kann als Technologie für mandantenfähige Backbones eingesetzt werden. Ein Ethernet-Backbone kann den Verkehr aus den angeschlossenen Kundennetzen ohne wesentliche Änderung des Rahmenformats übertragen, was die Kosten für das Netz minimieren wird.

- Zurzeit wird Ethernet in mandantenfähigen Backbones in der Regel mit anderen Verfahren wie MPLS kombiniert. Wenn man den Ethernet-Dienst so definiert, dass Ethernet-Rahmen (Frames) auf der einen Seite empfangen und auf der anderen Seite unverändert an das Zielnetz ausgeliefert werden, wird zurzeit als physikalische Schnittstelle zwischen dem Service-Provider und seinen Kunden Ethernet einsetzt, der Transport über das Service-Provider-Netz jedoch in der Regel auf einer anderen Protokollebene mit einem anderen Verfahren wie SDH oder MPLS kombiniert.

- Die Provider und Hersteller arbeiten zugleich an Verfahren wie SPB, die das Potenzial haben, Verfahren wie MPLS und SDH langfristig auch abzulösen.

6. Elemente mandantenfähiger Netze

Für den Aufbau mandantenfähiger Netze werden grundsätzlich folgende Elemente benötigt (Abbildung 5):

- Logische Trennung der Verkehrsflüsse der Mandanten in LAN und WAN
- Kontrolle der Kommunikationsbeziehungen an Netzübergängen zwischen Mandanten, gemeinsam genutzten Ressourcen und externen Kommunikationspartnern
- Netzzugangskontrolle, die sicherstellt, dass Geräte, die an einem Netzsegment eines Mandanten angeschlossen sind, auch tatsächlich zu der entsprechenden Gruppe gehören

Logische Trennung der Verkehrsflüsse
Grundlage mandantenfähiger Netze ist zunächst die logische Trennung der Verkehrsflüsse.

Für die WAN-Übertragung sind dies, wie oben beschrieben, MPLS-VPN bzw. bei Carrier Ethernet einfach VLANs. Wenn man diese Trennung auf dem Campus im LAN fortsetzen möchte, setzt man auf Layer 2 zunächst wieder VLANs ein. Will man die VLANs nicht in der Fläche über einen kompletten Standort ausdehnen, kommt man um den Einsatz von Trennungsmechanismen oberhalb von Layer 2 nicht herum. Hier kann grundsätzlich wieder mit MPLS gearbeitet werden, was auch im LAN bei einer größeren Zahl von Mandanten oder bei einer gewissen Dynamik der Mandanten (neue Gruppen müssen öfter angelegt werden, bestehende Gruppen müssen wieder entfernt werden) durchaus in Betracht gezogen werden kann. Alternativ kann die logische Trennung auf Layer 3 durch den Einsatz von Virtual Routing and Forwarding (VRF) erfolgen. Dabei werden die VRF-Instanzen typischerweise per VLAN miteinander vernetzt, um auf einer gemeinsamen Hardware verschiedene virtuelle Layer-3-Netze zu schaffen.

Kontrolle der Kommunikationsbeziehungen an Netzübergängen
Meist ist ein Übergang zwischen den Netzen der einzelnen Mandanten bzw. von den Mandanten zu gemeinsam genutzten Diensten (z.B. DNS, Directory Services) erforderlich. Dabei müssen insbesondere die in die Netze eines Mandanten eingehenden Kommunikationsbeziehungen gefiltert werden. Typischerweise arbeitet man hier mit zentralen, entsprechend leistungsfähigen und hochverfügbaren Firewall-Systemen, die ggf. um Intrusion-Prevention-Funktionen ergänzt werden.

Die dabei zu verwaltenden Regelwerke können eine erhebliche Komplexität annehmen, da im Gegensatz zum Einsatz am Perimeter hier die Firewall internen LAN- und WAN-Verkehr filtern muss, d.h. mit dem gesamten im Intranet verwendeten Protokollapparat zurecht kommen muss. Dies beinhaltet möglicherweise neben der Filterung von Protokollen, die dynamisch Ports aushandeln (z.B. RTP und DCOM) auch die Erkennung von Sitzungen, die auf Basis von UDP aufgebaut werden (z.B. Authentisierungen via RADIUS).

Bei der Filterung der Kommunikation an den Netzübergängen ist die Verwendung verschlüsselter Protokolle zu beachten. Wenn es gewünscht ist, dass die Filterkomponenten (z.B. ein IPS) den verschlüsselten Verkehr analysieren, muss das Firewall-System um Verschlüsselungsendpunkte ergänzt werden, d.h. um entsprechende Proxies.

Insgesamt entsteht hier ein im Regelfall durchaus sehr komplexes System.

Netzzugangskontrolle zur Prüfung der Zugehörigkeit zu einem Mandanten
Nehmen wir an, ein Endgerät wird an einen aktivierten Netzwerk-Port angeschlossen, der einem Mandanten zugeordnet ist. Dann ist ein Mechanismus wünschenswert, der an dem Port prüfen kann, ob das Endgerät ebenfalls zu diesem Mandanten gehört. Nur wenn die Prüfung positiv ausfällt, wird der gewünschte Zugang zu den Ressourcen des Mandanten gewährt. Andernfalls wird der Zugang abgewiesen oder nur ein (erheblich) eingeschränkter Zugang gewährt. Diese als

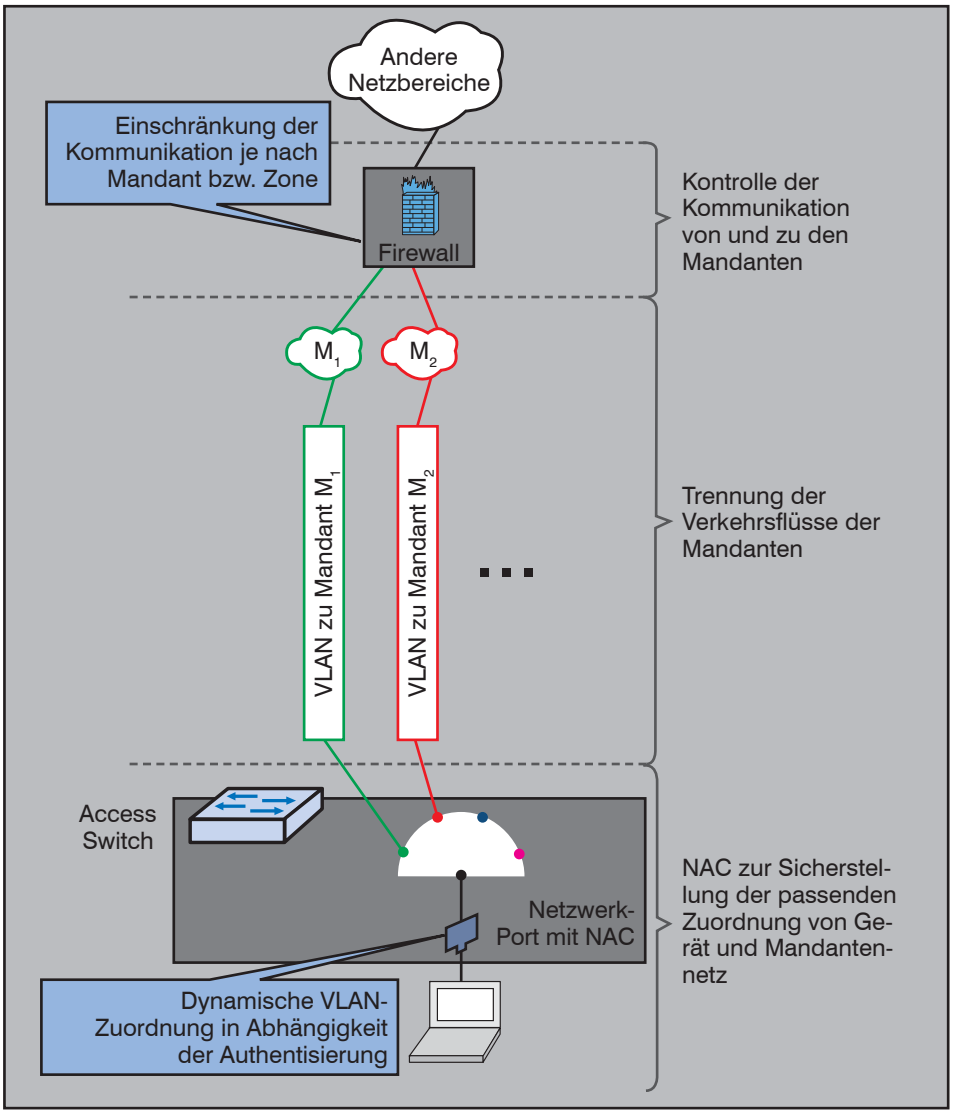


Abbildung 5: Elemente mandantenfähiger Netze

Authentisierung bezeichnete Prüfung der Identität des Endgeräts (bzw. des Nutzers des Endgeräts) sollte natürlich verlässlich sein, d.h. mit kryptographischen Mitteln erfolgen.

Analog könnte man fordern, dass für ein Endgerät, das an einem Netzwerk-Port angeschlossen wird, im Rahmen der Authentisierung festgestellt wird, zu welchem Mandanten das Gerät gehört, und nach erfolgreicher Authentisierung wird der Port dynamisch einem VLAN zugewiesen, das in das entsprechende Mandantennetz führt.

Eine solche Netzzugangskontrolle ist dann notwendig, wenn durch andere Mechanismen (z.B. räumliche Trennung in Verbindung mit einer Zutrittskontrolle) eine passende Zuordnung von Endgerät und Mandantennetz nicht angemessen zugesichert werden kann.

7. Netzzugangskontrolle mit IEEE 802.1X

Der Standard IEEE 802.1X spezifiziert eine Port-basierte Netzzugangskontrolle (Network Access Control, NAC) für Ethernet nach IEEE 802.3 und für WLAN nach IEEE 802.11.

IEEE 802.1X definiert verschiedene Rollen der beteiligten Netzelemente:

- Der **Supplicant** ist eine Software-Komponente auf dem Endgerät, die den Netzwerkzugang anfordert und die in der Lage ist, bevor der eigentliche Netzzugang für die Übertragung von Nutzdaten bereitgestellt wird, eine Authentisierung durchzuführen.
- Der **Authenticator** bietet hierzu eine Schnittstelle, über die der Supplicant authentisiert werden kann und stellt den gewünschten Netzwerkzugang her. Im LAN liegt diese Funktion typischerweise in demjenigen Switch, an dem das Endgerät unmittelbar angeschlossen ist. Im WLAN wird diese Funktion vom Access Point bzw. WLAN Controller wahrgenommen.
- Der eigentliche Authentisierungsdienst wird zentral über den **Authentication Server** bereitstellt. Der Authentication Server ist typischerweise ein RADIUS-Server (siehe RFC 2865).

Für den Austausch der Authentisierungsinformationen zwischen Supplicant und Authentication Server dient das Extensible Authentication Protocol (EAP, siehe RFC 3748). Dabei erfolgt die Kommunikation über die LAN- bzw. WLAN-Schnittstelle zwischen Supplicant und Authenticator über das Layer-2-Protokoll EAP over LAN (EAPOL). Auf diese Weise wird eine Authentisierung am Netzzugangspunkt ermöglicht, bevor eine Kommunikation auf IP-Ebene und höheren Protokollebenen stattfindet. Die Kommunikation zwischen Authenticator und Authentication-Server geschieht meist über RADIUS, wobei eine EAP-Nachricht als RADIUS-Attribut übertragen wird (siehe RFC 2865). Für die Verwaltung der Daten der Geräte oder Nutzer, die sich mit IEEE 802.1X authentisieren, wird oft ein Verzeichnisdienst (Directory Service) wie z.B. LDAP verwendet, der vom RADIUS-Server angesprochen wird. Abbildung 6 zeigt die genutzten Protokolle im Überblick. Wichtig ist dabei, dass es keine direkte Kommunikation des Supplicant mit dem Authentication Server gibt. Der Authenticator ist der einzige für den Supplicant sichtbare Kommunikationspartner, der sich also quasi wie ein Authentisierungs-Proxy verhält.

IEEE 802.1X gestattet nach einer erfolgreichen Authentisierung eine Autorisierung, die über eine simple Türöffnerfunktion hinausgeht. Der Authentication Server kann bei der Erteilung der Zugangserlaubnis zusätzlich eine Information für die Zuweisung eines VLANs oder einer Access Control List (ACL) für den Port, an dem der Supplicant angeschlossen ist, übertragen. Auf diese Weise kann dynamisch und individuell bzw. in Abhängigkeit von der Gruppenzugehörigkeit des Supplicant (der dabei ein Gerät oder einen Nutzer repräsentieren kann) eine Autorisierung der Kommunikation, d.h. insbesondere auch eine Zuordnung zu einem Mandantennetz, vorgenommen werden.

IEEE 802.1X wurde 2001 erstmalig verabschiedet, jedoch 2004 und zuletzt im Februar 2010 überarbeitet. IEEE 802.1X-

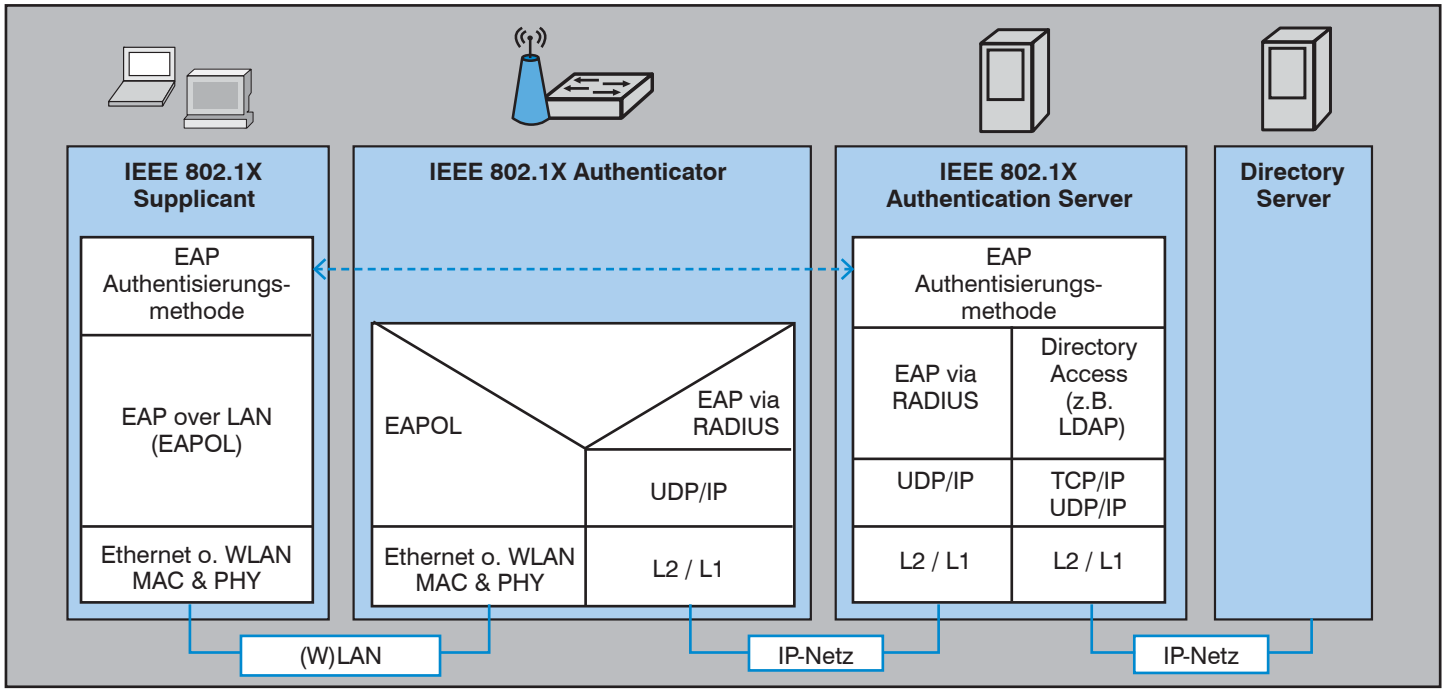


Abbildung 6: Im Rahmen der Authentisierung mit IEEE 802.1X genutzte Protokolle

2004 ist die aktuell in der Praxis noch meist verbreitete Version.

8. Problembereiche von IEEE 802.1X in der Fassung von 2004

Für WLAN hat sich IEEE 802.1X seit Jahren im Enterprise-Bereich massiv durchgesetzt. Im kabelbasierten LAN war der Einsatz jedoch lange eher die Ausnahme und erst seit 2009 ist eine steigende Tendenz sichtbar. Dies liegt daran, dass im kabelbasierten LAN technische Eigenheiten bestehen, die der Standard in den Fassungen von 2001 und 2004 nur unzureichend adressiert. Außerdem lässt IEEE 802.1X-2004 an entscheidenden Stellen empfindliche Lücken, die zu (teilweise sehr unzufriedenstellenden) herstellerspezifischen Implementierungen geführt haben, die sich an diesen Punkten so stark unterschieden haben, dass von einem Standard eigentlich kaum noch geredet werden konnte.

Zu nennen sind unter anderem folgende Problembereiche:

- Kommunikation mit nicht authentisierten Systemen (Default Policy)
- Flexible Kombination von Authentisierungsmethoden
- Simultane Authentisierung mehrer Endgeräte an einem Port
- Anfälligkeit gegenüber MAC-Adress-Spoofing

Kommunikation mit nicht authentisierten Systemen (Default Policy)

In der Praxis ist es notwendig, dass auch Geräten, die sich (noch) nicht erfolgreich authentisiert haben, ein eingeschränkter Netzzugang gewährt wird. Beispiele sind PXE Boot zur Softwareverteilung und der Zugriff des User Help Desk auf ein Gerät, das bedingt durch einen Fehler keine erfolgreiche Authentisierung durchführen konnte.

Hierzu muss ein Netzwerk-Port auch im nicht autorisierten Zustand im Forwarding State sein und z.B. durch eine spezielle VLAN-Zugehörigkeit in den Kommunikationsmöglichkeiten eingeschränkt werden (sogenannte Default Policy). Nach einer erfolgreichen Authentisierung erfolgt dann eine Zuweisung eines produktiven VLANs zu dem Port.

Eine solche Kommunikation mit nicht authentisierten Systemen wird zwar vom Standard IEEE 802.1X-2004 gestattet, ist aber nur in einem informellen Anhang des Standards beschrieben. Die Konsequenz ist natürlich, dass unterschiedlichste Implementierungen dieser Funktion existieren und manche Hersteller diese Funktion erst gar nicht umgesetzt haben.

Flexible Kombination von Authentisierungsmethoden

Um mit Geräten umzugehen, die kein IEEE 802.1X unterstützen, wie manche Drucker und andere Spezialgeräte, ist eine Kombination von IEEE 802.1X und einer RADIUS-basierten MAC-Adress-Authentisierung oft unerlässlich. Dabei versucht ein Port beispielsweise zunächst ein Gerät mit IEEE 802.1X zu authentisieren. Falls dies nicht gelingt, wird die MAC-Adresse als Identitätsnachweis verwendet. Die kombinierte Authentisierung mit IEEE 802.1X und als Fallback mit MAC-Adresse ist nicht im Standard IEEE 802.1X beschrieben und als herstellerspezifisch einzustufen. Daher können sich die Implementierungen der Hersteller entsprechend deutlich unterscheiden und es ist zur Bewertung stets eine Einzelbetrachtung erforderlich.

Simultane Authentisierung mehrer Endgeräte an einem Port

Größtes Problem in IEEE 802.1X-2004 ist die Limitierung der Spezifikationen für das kabelbasierte LAN auf eine strikte 1-zu-1-Beziehung zwischen Supplicant und Authenticator, d.h. ein Gerät pro Port.

Damit hat der Standard neben dem Anschluss eines Hubs oder eines Desktop-Switches an einen Port, der IEEE 802.1X aktiviert hat, auch den kaskadierten Anschluss von IP-Telefon und PC am PC-Port des IP-Telefons sowie die Nutzung von VMs im Bridged-Modus auf einem PC ausgeklammert.

Die Netzwerkausrüster haben daher in ihren Implementierungen den Standard durch proprietäre Funktionen ergänzt, die zwar im Grundsatz recht ähnlich sind, im Detail aber erheblich voneinander abweichen können. Das Prinzip ist dabei recht einfach: Für jede an einem Switch-Port neu gelernte MAC-Adresse erzeugt der Switch eine neue NAC-Sitzung für den Port, die per IEEE 802.1X oder per MAC-Adresse authentisiert wird (siehe Abbildung 7). Nur diejenigen MAC-Adressen, die einer authentisierten Sitzung zugeordnet werden können, erhalten einen Zugang. Auf diese Weise werden im Prinzip mehrere virtuelle Ports auf einem physischen Port geschaffen.

Anfälligkeit gegenüber MAC-Adress-Spoofing

Über IEEE 802.1X ist zwar die Authentisierung eines Systems bzw. eines Nutzers am System möglich, es erfolgt aber keine Authentisierung der über einen autorisierten Port übertragenen Pakete eines Endgeräts. Insbesondere findet keine Prüfung statt, ob die Pakete auch tatsächlich von dem Gerät stammen, auf dem der Supplicant, der sich authentisiert hat, läuft.

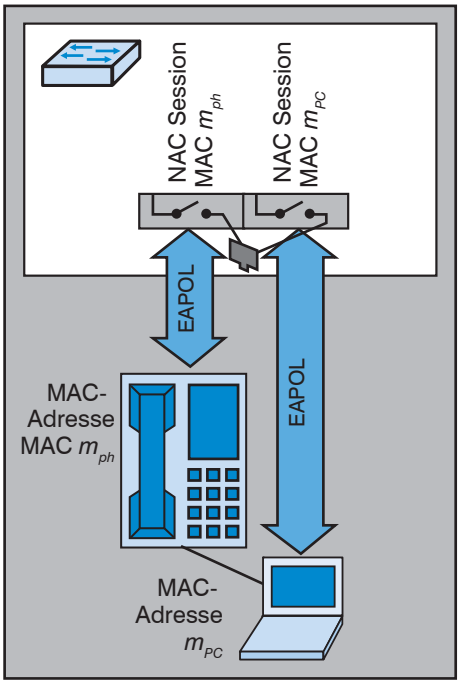


Abbildung 7: Simultane Authentisierung mehrerer Endgeräte an einem Netzwerk-Port am Beispiel von IP-Telefon und PC

Ein Angreifer könnte unter der MAC-Adresse eines an einem Port authentisierten Supplicant an diesem Port einen Dialog mit der Infrastruktur führen, solange der Port autorisiert ist. Er benötigt hierzu allerdings einen Helfer, der sich erfolgreich authentisieren kann (siehe Abbildung 8).

Wenn eine NAC-Lösung basierend auf der Version von 2004 des Standards IEEE 802.1X aufgebaut werden soll, muss diese Gefährdung bewertet werden. Entweder das Risiko wird eingegangen oder IEEE 802.1X-2004 macht an dieser Stelle keinen Sinn.

9. IEEE 802.1X-2010: Weiterentwicklung und Aufräumarbeit

Die Zusicherung von Vertraulichkeit und Integrität der über einen autorisierten Port übertragenen Pakete ist zunächst nicht Aufgabe eines Authentisierungsverfahrens. Hierzu muss generell die Sicherheitsarchitektur um eine Komponente für Verschlüsselung und/oder Integritätsprüfung erweitert werden. Für die verbindungslose Kommunikation in LAN/

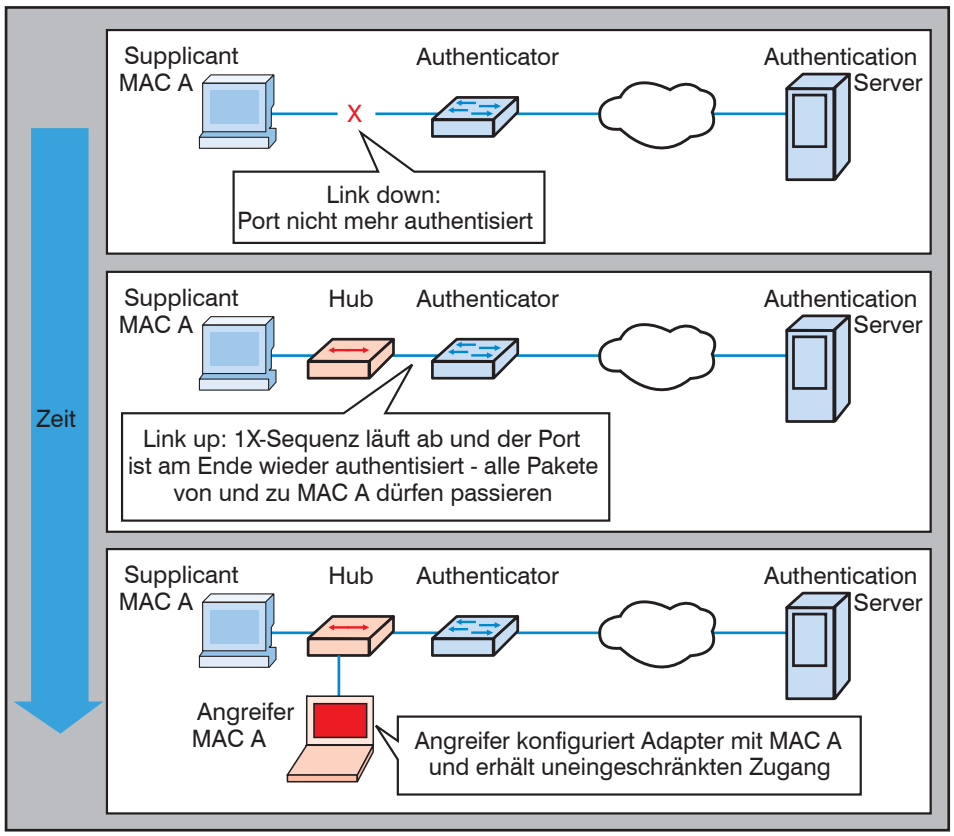


Abbildung 8: Umgehung von IEEE 802.1X-2004

MAN werden diese Mechanismen in dem im August 2006 verabschiedeten Standard IEEE 802.1AE MAC Security (kurz: MACsec) beschrieben.

Das hierzu notwendige Schlüsselmanagement für den Aufbau von gesicherten Kommunikationsbeziehungen ist das wesentliche Element der Neuauflage von IEEE 802.1X, die Ende Februar 2010 verabschiedet worden ist. IEEE 802.1AE und IEEE 802.1X-2010 bilden dabei zusammen für das kabelbasierte LAN das konzeptionelle Pendant zur Absicherung von WLAN mit IEEE 802.11i, wie in Abbildung 9 gezeigt.

Das Grundprinzip für den Aufbau gesicherter Kommunikationsbeziehungen bei IEEE 802.1X-2010 besteht darin, dass im Rahmen der Authentisierung Schlüsselmaterial in Supplicant und Authenticator bereitgestellt wird, welches dann zum Aufbau einer gesicherten Kommunikationsbeziehung mit IEEE 802.1AE verwendet werden kann (Abbildung 10). Dabei kann (analog zu WLAN gemäß IEEE 802.11i) wahlweise ein Pre-Shared Key (PSK) oder eine dynamische Schlüsselaushandlung mit EAP genutzt werden.

Die Neuauflage IEEE 802.1X-2010 beinhaltet neben der bereits angesprochenen Nutzung von IEEE 802.1AE für den Aufbau von Sicherheitszonen auf Layer 2 weitere wichtige Elemente:

- Übernahme der Default Policy in den normativen Teil als erlaubte Option
- Möglichkeit der simultanen Authentisierung mehrerer Endgeräte an einem Port durch das Konzept virtueller Ports
- Absicherung von Zugang und Übertragung für Carrier Ethernet

10. IEEE 802.1AE MAC Security (MACsec)

MACsec ergänzt das MAC-Layer der Netzelemente eines LAN um eine Hop-by-Hop-Absicherung, die Daten-Vertraulichkeit, -Integrität, -Authentisierung für die verbindungslose Kommunikation in einem LAN schafft (Abbildung 11). Die Default Cipher Suite verwendet den Advanced Encryption Standard (AES) mit 128 Bit Schlüssel. Die Verschlüsselung ist dabei optional. Kernelement ist die Authentisierung der Daten, welche neben den Nutzdaten auch die MAC-Adressen berücksichtigt, was insbesondere die eben beschriebene Spoofing-Attacke automatisch aushebelt.

Neben Punkt-zu-Punkt LAN-Verbindungen werden Multi-Access LAN und Shared-Media LAN (exklusive IEEE 802.11 WLAN, denn hier wirkt IEEE 802.11i) berücksichtigt. Dabei geht es insbesondere um den kaskadierten Anschluss von PC und IP-Telefon an einen Port eines Access Switch und um die Behandlung von VMs mit virtuellen MAC-Adressen auf einem Endgerät.

MACsec wurde für die Schaffung von Sicherheitszonen auf Layer 2 in LAN und Carrier Ethernet spezifiziert und geht über die reine Absicherung des Endgeräteanschlussbereichs deutlich hinaus.

Außerdem wurde MACsec für eine hohe

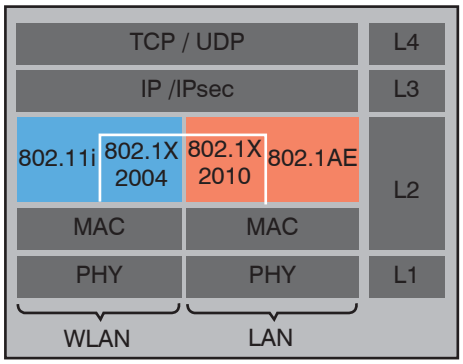


Abbildung 9: Einordnung von IEEE 802.1AE und IEEE 802.1X-2010 in den Protocol Stack

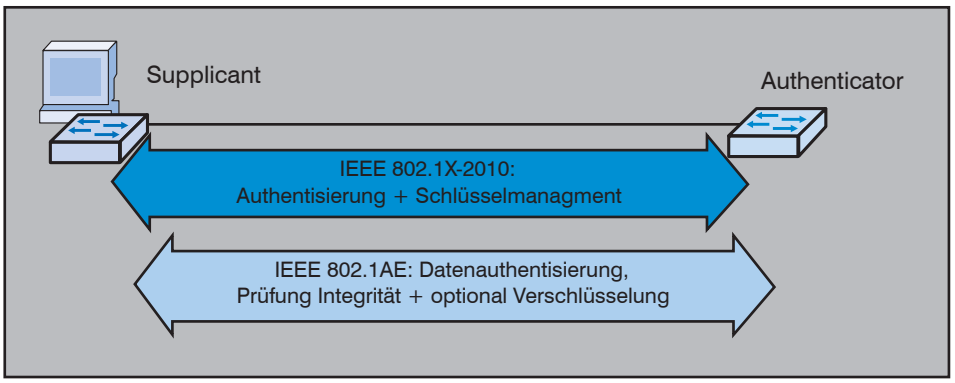


Abbildung 10: Beziehung zwischen IEEE 802.1X-2010 und IEEE 802.1AE

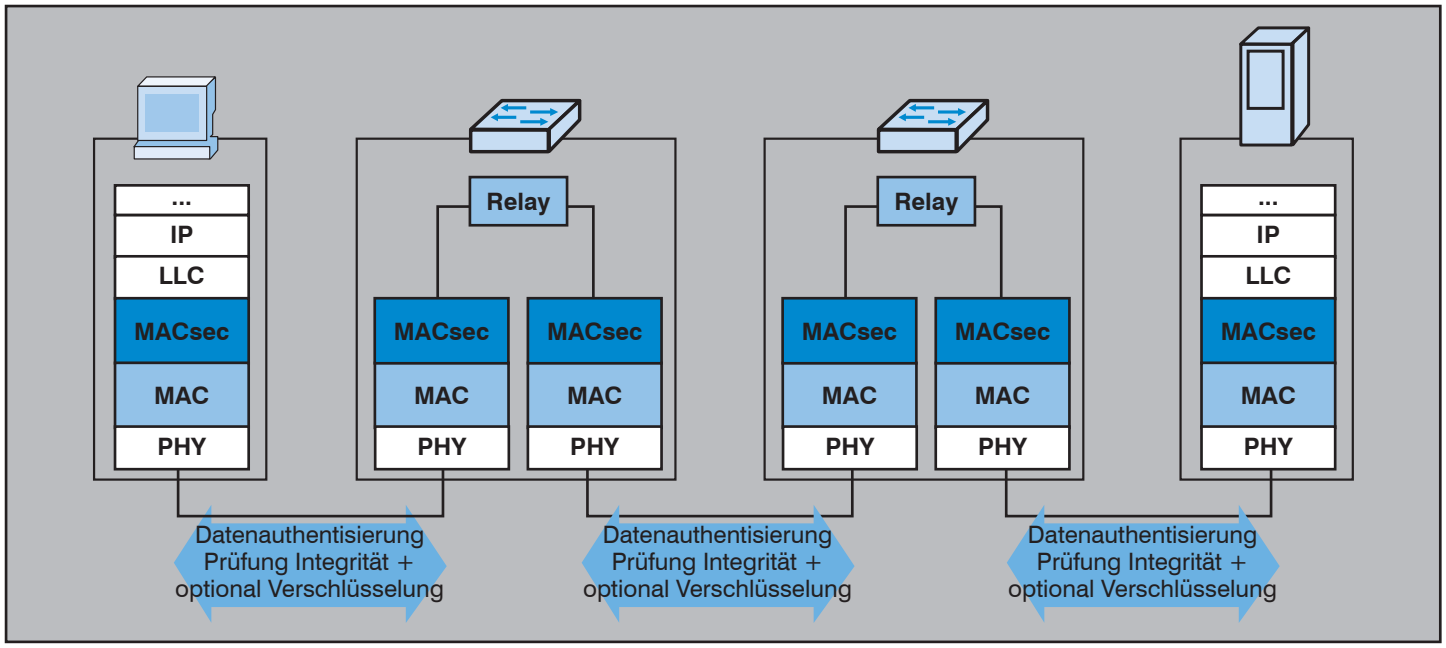


Abbildung 11: Hop-by-Hop-Sicherheit mit MACsec

Verschlüsselungsleistung konzipiert (40 Gbit/s und mehr). Hintergrund ist hier der Einsatz von MACsec im Datacenter-Bereich, wo die Möglichkeit einer Verschlüsselung unter hohen Leistungsanforderungen (ohne unwirtschaftlich zu werden) immer mehr gefordert wird. Ein Beispiel ist die Kopplung zweier Rechenzentren auf Layer 2 über Glasfaserstrecken. Wenn die Übertragungsstrecken das Unternehmensgelände verlassen bzw. über unsichere Bereiche laufen und ein hoher Schutzbedarf der Daten besteht (was bei einer RZ-Kopplung praktisch immer der Fall ist), kommt man eigentlich um eine Verschlüsselung nicht herum.

Eine dedizierte Verschlüsselung ausschließlich der Daten mit hohem Schutzbedarf auf höheren Protokollebenen (z.B. IPsec und TLS) ist zwar grundsätzlich machbar, erfordert jedoch aufwendige Einzelfallbetrachtungen. Daher besteht schnell der Wunsch nach einer pauschalen Verschlüsselung auf Layer 2. Hier kamen in der Vergangenheit proprietäre Layer-2-Kryptoboxen zum Einsatz. MACsec bietet hier eine standardisierte Alternative, die keine zusätzlichen Kryptoboxen mehr benötigt, da diese Funktion mit MACsec in die Switches bzw. Bridges integriert ist.

Durch diese Skalierbarkeit der Leistung vom Endgeräteanschluss bis zum Backbone setzt sich MACsec von Sicherheitsmechanismen auf höheren Protokollebenen wie IPsec und TLS, die bei den Leistungsanforderungen moderner LANs im Campus- und Datacenter-Bereich immer mehr an Grenzen stoßen, deutlich ab.

Aufbau sicherer Kommunikationsbeziehungen

Die Schaffung von gesicherten Vertrauensbereichen (Sicherheitszonen) im LAN erfolgt bei MACsec durch den Aufbau sogenannter Secure Connectivity Associations (CAs), wie in Abbildung 12 gezeigt. Im einfachsten Fall sind dies zwei Parteien, etwa ein Endgerät und ein Switch oder zwei Switches.

Für den Aufbau sicherer Kommunikationsbeziehungen muss MACsec notgedrungen das Layer-2-Frame-Format erweitern. Dabei kommt ergänzend ein Security TAG und als kryptographische Prüfsumme ein Integrity Check Value (ICV) hinzu. Letzterer schützt im Wesentlichen die gesamten Layer-2-Daten, also nicht nur den Payload, sondern auch MAC-Quelladresse und -Zieladresse. Eine Station, die ein Paket empfängt, kann die im Paket übertragene kryptographische Prüfsumme auswerten und feststellen, ob das Paket tatsächlich von der angegebenen MAC-Adresse kommt und ob der Inhalt manipuliert worden ist (Abbildung 13). Es besteht also automatisch ein Schutz vor MAC-Adress-Spoofing, d.h. MAC-Adressen werden durch MACsec zu verlässlichen Identifikationsmerkmalen.

Als Konsequenz muss für Switches zwingend neue Hardware eingesetzt werden. Eine Migration zu IEEE 802.1AE hat daher eher einen langfristigen Charakter.

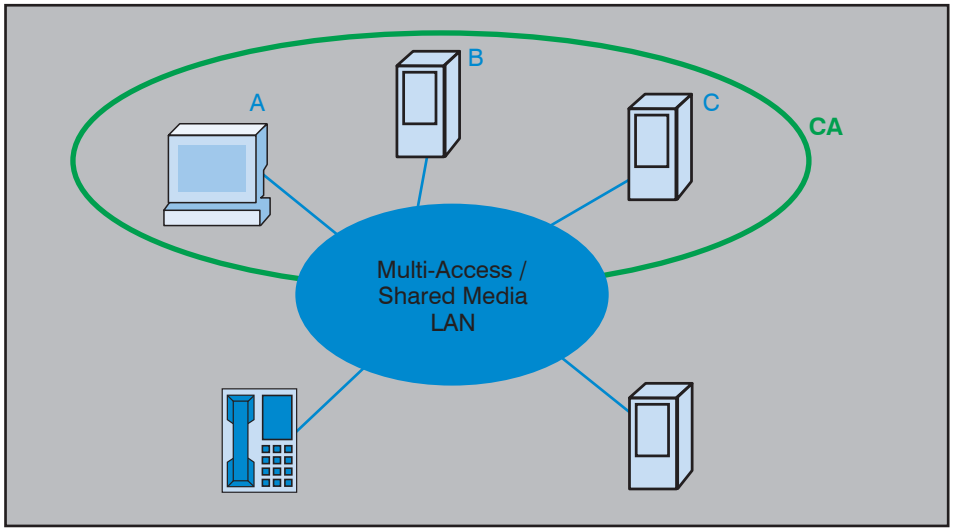


Abbildung 12: Secure Connectivity Association (CA) zwischen den Stationen eines Vertrauensbereichs

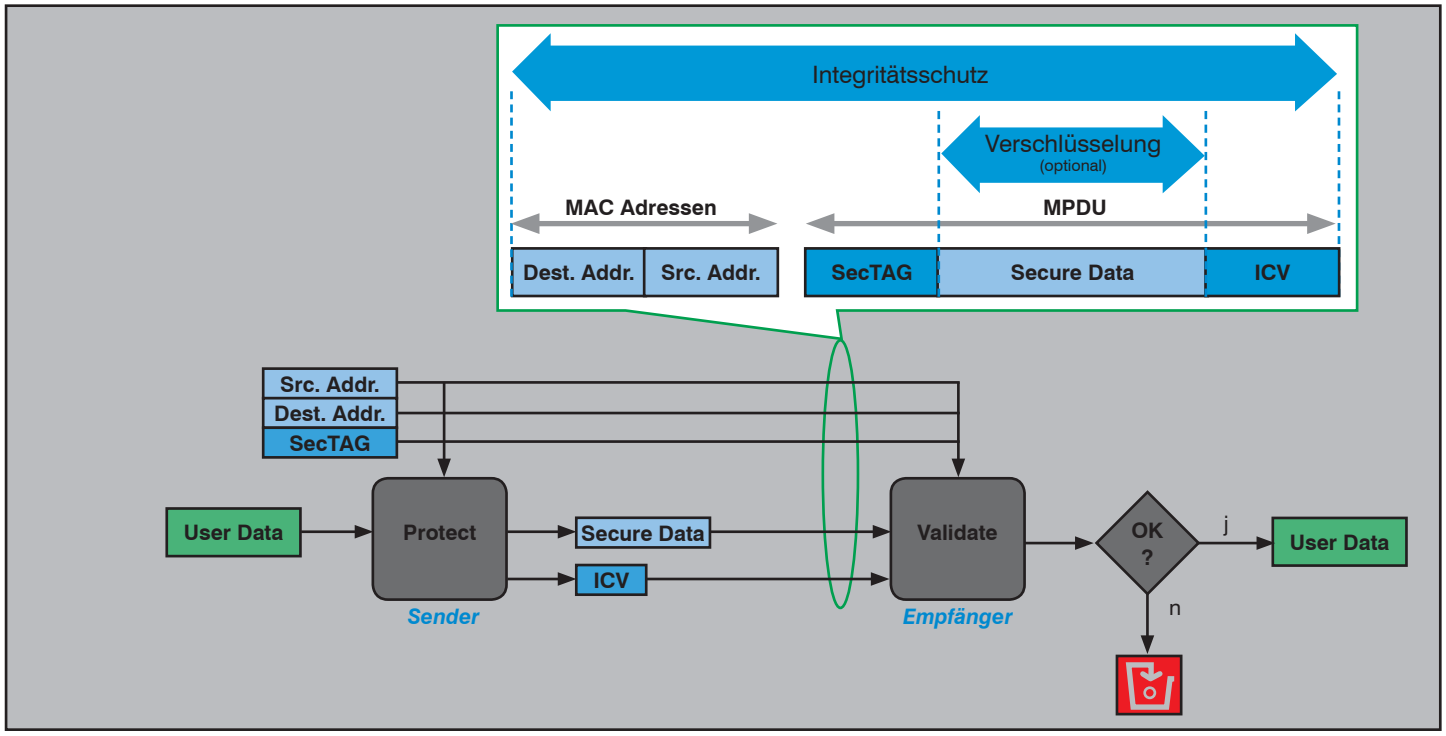


Abbildung 13: Sicherung der Übertragung mit MACsec

Den grundsätzlichen Ablauf des Aufbaus einer abgesicherten Kommunikationsbeziehung zeigt zusammengefasst Abbildung 14. Im ersten Schritt erfolgt optional eine Authentisierung mit EAP bzw. IEEE 802.1X, verbunden mit einer Autorisierung, die eine VLAN- und/oder ACL-Zuweisung beinhalten kann. Mit dieser Authentisierung wird dynamisch ein symmetrisches Schlüsselmaterial abgeleitet. Alternativ kann ein statischer PSK verwendet werden.

Auf dieser Basis wird in einem zweiten Schritt das Schlüsselmaterial über das MACsec Key Agreement Protocol (MKA) zwischen den beteiligten Port Access Entities (PAEs), d.h. zwischen Supplicant und Authenticator, verhandelt. Dieses Material wird zur jeweiligen MAC Security Entity (SecY) übertragen, die hiermit die CA aufbauen kann (Schritte 3 und 3.1 in Abbildung 14). Im letzten Schritt kann dann der Port freigeschaltet werden. CAs müssen nicht individuell zwischen zwei Parteien bestehen, es sind auch Group CAs möglich.

Verschlüsselungsendpunkte bilden bei MACsec die Switches untereinander bzw. die Switches und die Endgeräte. Es gibt also keine Ende-zu-Ende-Absicherung wie etwa bei TLS. Den Switches muss also vertraut werden.

11. Carrier Ethernet und IEEE 802.1X-2010

Die Unterstützung von Carrier Ethernet ist ein integraler Bestandteil von MACsec und von IEEE 802.1X-2010. Damit ist sowohl die Absicherung der Kommunikation zwischen Customer Bridges über das Provider-Netz hinweg, zwischen Customer Bridge und Provider-Netz als auch zwischen adjazenten Provider Bridges möglich.

Insbesondere können so mit MACsec die

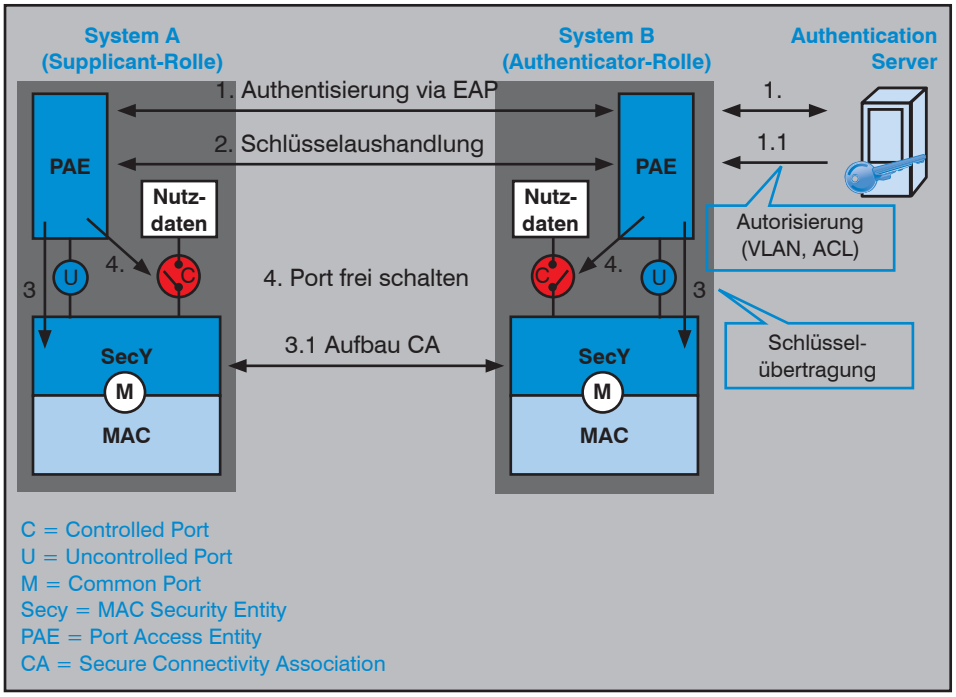


Abbildung 14: Schritte für den Aufbau einer abgesicherten Kommunikationsbeziehung mit IEEE 802.1X-2010 unter Verwendung von EAP

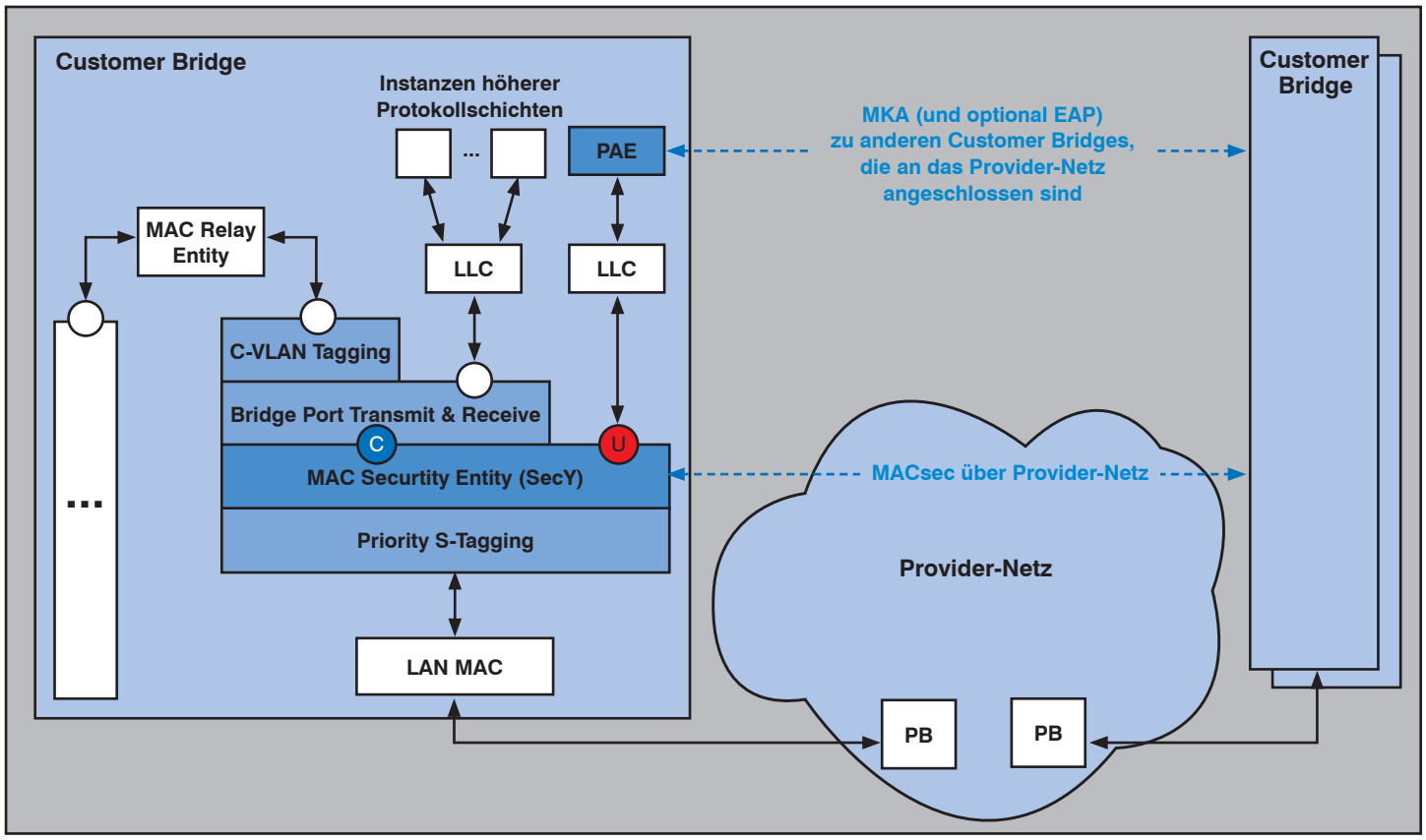


Abbildung 15: Absicherung der Übertragung zwischen Customer Bridges über ein Provider-Netz

WAN-Strecken transparent für höhere Protokolle zielgerichtet für ausgewählte Kunden-VLANs abgesichert werden. Dabei werden individuelle CAs oder eine Group CA zwischen den beteiligten Stationen mit MKA aufgebaut. Die Rolle von EAP hängt hier stark davon ab, ob nur wenige oder viele Strecken abgesichert werden müssen, bzw. ob das Risiko durch die Verwendung eines statischen PSK akzeptiert werden kann. Durch eine Group CA entsteht mit MACsec dann im Prinzip ein gesichertes VPN auf dem Provider-Netz. Unter anderem sind dabei folgende Varianten möglich, die auch miteinander kombiniert werden können:

1. **MACsec zwischen Customer Bridges:** Customer-Bridges, die an eine Provider Bridge angeschlossen sind, können untereinander über MACsec gesichert über das Provider-Netz kommunizieren (siehe Abbildung 15). Damit wird die gesamte Übertragung der Nutzdaten zwischen den Kundennetzen abgesichert. Ungesichert ist jedoch die Provider-spezifische Information wie S-VLAN, Priority und äußere MAC-Adressen.

2. **MACsec zwischen Customer Bridge und Provider Bridge:** Die Verbindung zwischen Customer Bridge und Provider Bridge kann mit den beschriebenen Mitteln natürlich ebenfalls mit MACsec abgesichert werden (Abbildung 16). Hierzu müssen den Kunden die zu verwendenen Credentials für den Aufbau einer kundenspezifischen CA mitgeteilt werden. Wenn hier ein höheres Sicherheitsniveau erreicht werden soll, sind PSKs eigentlich nicht Stand der Technik, d.h. EAP ist dann eher das Mittel der Wahl. MACsec kann aber auch im Provider-Netz selbst eingesetzt werden.

3. **IEEE 802.1X zwischen Customer Bridge und Provider Bridge aber ohne MACsec:** Der Anschluss einer Customer Bridge an eine Provider Bridge kann mit den Mitteln von IEEE 802.1X authentisiert werden (mit PSK oder EAP), ohne dass anschließend eine CA mit MACsec aufgebaut wird. Dies schützt eigentlich nur vor versehentlichem Fehlanschluss.

12. Produktunterstützung IEEE 802.1X-2010 und MACsec

Auf Seiten der Netzwerkausrüster ist bislang immer noch Cisco am weitesten. In einem ersten Schritt hatte Cisco mit TrustSec für die Serie Nexus 7000 eine Implementierung von IEEE 802.1AE herausgebracht. Hier wurde zunächst der Aufbau von hoch-performanten Sicherheitszonen im RZ adressiert. TrustSec ist konform zu IEEE 802.1X-2010, d.h. insbesondere ist die Verwendung von IEEE 802.1X für das dynamische Schlüsselmanagement umgesetzt worden. Seit Frühjahr 2010 gibt es TrustSec auf den Switches der Serie Catalyst 3750-X und 3560-X. Damit ist die Implementierung von IEEE 802.1AE auch im Bereich des Endgeräteanschlusses angekommen. Bei Catalyst 3750-X und 3560-X wird IEEE 802.1X-2010 und MACsec jedoch nur auf den Downlink-Ports unterstützt.

Um MACsec sinnvoll im Endgerätebereich zu nutzen, müssen Switch **und** Endgerät IEEE 802.1X-2010 unterstützen. Es gibt aktuell jedoch nur wenige NICs, die MACsec unterstützen. Weiterhin gibt es derzeit auch noch keine Integration von IEEE 802.1X-2010 in den nativen Windows Supplicant zur Unterstützung von MACsec. Der erste Supplicant, der dies leistet, ist der Cisco AnyConnect Client in der Version 3.0. Dabei verwendet der Client möglichst eine MACsec-Funktion der Hardware. Steht diese nicht zur Verfügung, erfolgt die Absicherung (durch Integritätssicherung und optional Verschlüsselung) in Software.

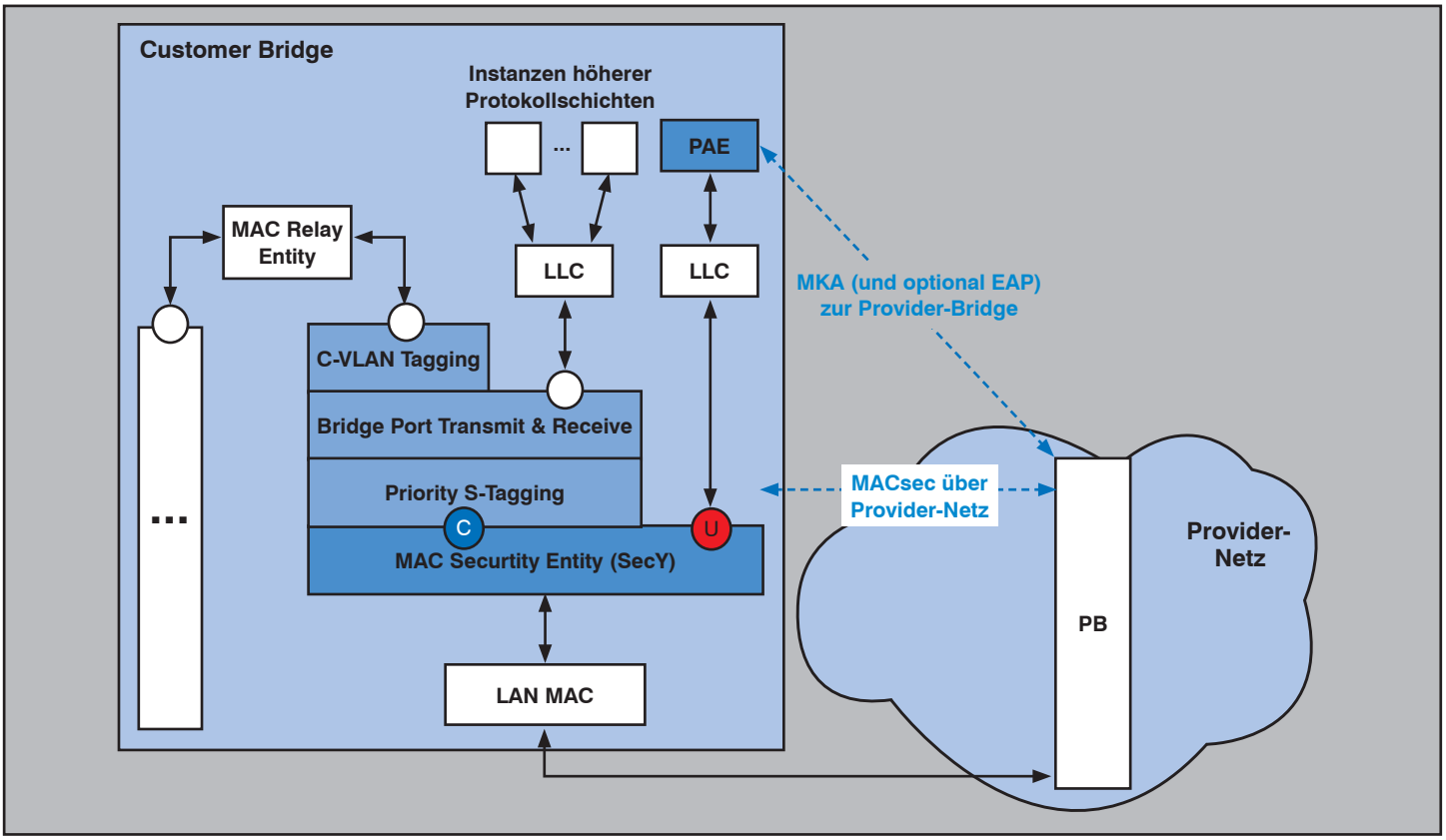


Abbildung 16: Absicherung der Übertragung zwischen Customer Bridge und Provider Bridge

Geräte, die eine TrustSec-Hardware unterstützen, können auf den mit MACsec abgesicherten Links Nutzergruppen kryptographisch voneinander trennen. Hierzu dient der Security Group Tag (SGT), der Bestandteil des TrustSec-Layer-2-Paketformats ist. Im Rahmen von TrustSec hat Cisco zusätzlich das Security Group Tag Exchange Protocol (SXP) entwickelt, um Geräten, die keine TrustSec Hardware unterstützen, Informationen über den SGT, d.h. die Gruppenzugehörigkeit, zu übermitteln. Über SXP erfolgt die Zuordnung einer IP-Adresse zu einem SGT. SXP ist als Migrationsinstrument zu TrustSec wichtig. Außerhalb einer mit MACsec abgesicherten Verbindung liefert ein SGT keine höhere Sicherheit als ein VLAN oder eine VRF-Instanz. Eine sichere Trennung von Mandanten erfordert den durchgängigen Einsatz von MACsec.

Eine interessante Frage ist jedoch, ob TrustSec zusammen mit SXP bereits jetzt schon eine Alternative zu VRF für den Aufbau eines mandantenfähigen LAN darstellt. VRF ist eine seit Jahren bewährte Technik, die inzwischen von diversen Herstellern unterstützt wird. Die Zuordnung VRF zu MPLS-VPN ist ebenfalls praxiserprobt. Die Skalierbarkeit von VRF ist allerdings begrenzt und die Fehlersuche komplex. Es ist grundsätzlich möglich, mit SXP eine vergleichbare Trennung von Mandanten zu implementieren. Jedoch ist das erreichte Sicherheitsniveau zum heutigen Zeitpunkt nicht automatisch höher als das mit VRF erreichte. Daher kann ein Vorteil von SXP/TrustSec nur darin bestehen, dass SXP besser skaliert, die Komplexität in der Konfiguration geringer und die Fehlersuche weniger aufwendig ist.

13. Fazit zur Rolle von IEEE 802.1X-2010 für mandantenfähige Netze

Der Standard IEEE 802.1X-2010 schließt entscheidende Lücken der Vorversion von 2004 und ist ein wesentliches Element für den Aufbau flächendeckender mandantenfähiger Netze. Bisher unterstützt jedoch lediglich Cisco diesen Standard konsequent. Produkte, die den Standard in der Version von 2004 mit herstellerspezifischen Elementen ergänzen, können natürlich ebenfalls für den Aufbau flächendeckender mandantenfähiger Netze eingesetzt werden, jedoch kann erst mit der Fassung von 2010 ein hohes Sicherheitsniveau durch MACsec geschaffen werden.

Allerdings ist IEEE 802.1X-2010 auch ohne MACsec von Bedeutung, da mit der normativen Berücksichtigung der Default Policy, der Erweiterung der Autorisierung um ACLs und des Konzepts virtueller Ports für die simultane Authentisierung mehrerer Endgeräte wichtige, bisher proprietäre Elemente im Standard spezifiziert wurden.

Für Carrier Ethernet kann mit IEEE 802.1X-2010 eine sichere Trennung der Mandanten geschaffen werden. Auf Layer 2 war dies bisher eine Domäne proprietärer Kryptoboxen.

Es bleibt die Frage, wann andere Netzwerkausrüster nachziehen. Nachdem Cisco vor etwas mehr als zwei Jahren mit TrustSec den Markt betreten hat, ist ungewöhnlich, dass zwischenzeitlich noch kein Mitbewerber seine Produkte ebenfalls mit MACsec-Funktion ausgestattet hat. Cisco könnte natürlich auch auf das falsche Pferd gesetzt haben. Mit den steigenden Anforderungen an eine sichere LAN-Kommunikation, im RZ-Bereich an eine sehr hohe Verschlüsselungsleistung auf Layer 2 und im Carrier-Ethernet-Bereich an den Aufbau sicherer Layer-2-VPN gibt es aber eigentlich keine Alternative zu MACsec und IEEE 802.1X-2010.

Standpunkt Troubleshooting

Quality of Service - Fluch oder Segen?

Der Standpunkt Troubleshooting von Dr. Joachim Wetzlar greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends.

Wer von Ihnen ist nicht schon einmal mit der Forderung konfrontiert gewesen, im Netzwerk Quality of Service (QoS) einzuführen? Meist wird diese Forderung im Zusammenhang mit der Beschaffung einer neuen Telefonanlage auf Basis von VoIP gestellt. Es scheint, als sei das Netzwerk nur unter dieser Bedingung „VoIP-ready“. In der Praxis ist allerdings zuweilen das Gegenteil der Fall, wie ich anlässlich verschiedener Fehlersuche-Einsätze feststellen musste.

Wie sieht eine typische Konfiguration aus, mit der man im Netzwerk die Dienste-Güte, also QoS sicherstellt? Die Hersteller von Switches und Routern veröffentlichen hierzu zahlreiche Beispiele, die im Prinzip alle auf drei Säulen ruhen:

Wenn Datenpakete von einem Endgerät (Telefon, PC, Server) in das Netzwerk gelangen, erfolgt zunächst eine Klassifizierung. Das Endgerät oder ein Filter an der Netzkomponente bestimmt, welcher Dienste-Klasse das Paket angehört. Es wird entsprechend markiert, zumeist im IP Header mit einem Differentiated Services Code Point (DSCP). Typische Wertesind „Expedited Forwarding“ (EF), „Assured Forwarding“ in verschiedenen Ausprägungen (AFxx) oder „Default“.

Die Netzkomponente (Switch, Router) ordnet nun die Pakete anhand ihrer Markierung in eine Warteschlange (Queue) ein. Die einfachste Variante besteht aus einer „Priority Queue“, die quasi als Überholspur an der „Default Queue“ vorbeiführt. Pakete der Default Queue können nur gesendet werden, wenn die Priority Queue leer ist. Komplexere Vorschläge verwenden mehrere Queues, die unterschiedlich oft abgefragt werden.

Die dritte Säule der QoS-Konfigurationen ist häufig eine Art Polizist („Policer“), der darüber wacht, dass Datenverkehr bestimmter Klassen bestimmte Grenzwerte einhält. Der Policer kann z.B. dafür sorgen, dass Verkehr in der Priority Queue den übrigen Verkehr nicht vollständig lahmlegt. Er tut das, indem er entweder Pakete verwirft oder diese in eine Warteschlange sehr niedriger Priorität schickt, die manchmal auch „Lumpensammler“ (Scavenger) genannt wird.

So weit so gut. Wo liegen nun die Probleme in der Praxis? Erstens: Die Markierung der Pakete erfolgt zuweilen nicht wie mit dem Betreiber der Anwendung vereinbart. Die Telefone eines namhaften Herstellers markierten während einer meiner Messungen die Pakete nicht mit „EF“, sondern mit einem anderen DSCP-Wert. Diese Pakete wurden aber vom Policer in die Lumpensammler-Klasse gesteckt, was massive Qualitätsprobleme machte.

Zweitens: Viele Switches besitzen einen festgelegten Pufferspeicher pro Port, der auf die verschiedenen Warteschlangen aufgeteilt wird. In einem Fall war die für Video-Anwendungen zur Verfügung stehende Warteschlange kürzer als die von dieser Anwendung typischerweise ausgesandten Datagramme. Die Folge: Paketverluste mit entsprechenden Qualitätseinbußen. Man höre und staune: Der Hersteller eines professionellen Systems für den Videoschnitt empfiehlt Switch-Konfigurationen völlig ohne QoS, weil andernfalls die Warteschlangen der am Markt verfügbaren Switches zu kurz werden!

Drittens: Der Policer verwirft im Zweifelsfall Pakete, ohne dass die Anwendung davon etwas weiß. Anders ausgedrückt: QoS-Konfigurationen können nur dann erfolgreich sein, wenn die Anwendung darauf abgestimmt ist. Eine Anwendung muss also z.B. wissen, welche Bandbreite „ihre“ Warteschlange aufnehmen kann und selber dafür sorgen, dass diese nicht überschritten wird. Nur so können Fehlfunktionen vermieden und durch sinnvolle Fehlermeldungen ersetzt werden. Telefonanlagen z.B. können dem Anwender mitteilen, dass gerade keine ausreichende Bandbreite für den Aufbau des Gesprächs zur Verfügung steht.

Fazit: QoS-Konfigurationen im Netz werden nur dann zum Segen, wenn sie gut durchdacht und vor allem fehlerlos sind. Selbst Fachleute (mich eingeschlossen) überblicken die Vorgänge in Warteschlangen meist nur unzureichend. Und das Ziel einer Abstimmung des Netzes auf die Anwendung und umgekehrt erscheint mir in der Praxis oft nicht erreichbar zu sein. Hier ist ein einfaches Netz, das Pakete „Best Effort“ weiterleitet, allemal besser. Und das gilt nicht nur für das LAN. So gibt es inzwischen Codecs für die Bild- und Tonübertragung, die sich mit Hilfe von Regelmechanismen sogar optimal auf das „QoS-lose“ Internet einstellen. Die Anwendung wird zum Segen – ohne QoS. Vorbildlich!

Certified Trouble Shooter

Die Zertifizierung zum ComConsult Certified Trouble Shooter kombiniert in idealer Weise das Wissen, das der erfolgreiche Netzwerk-Fehlersucher in der Praxis benötigt. Die Ausbildung basiert auf zwei 4-tägigen Intensiv Kursen:

Trouble Shooting in vernetzten Infrastrukturen
17.05. - 20.05.11 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
28.06. - 01.07.11 in Aachen

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

Zweitthema

Storage: wo bleibt der Markt?

Fortsetzung von Seite 1

Dr. Behrooz Moayeri ist in der ComConsult Beratung und Planung GmbH als Mitglied der Geschäftsleitung tätig. Er ist zudem Leiter des Competence Centers Netze.

Steigende Storage-Ausgaben

Abgesehen davon, ob ein LAN-Switch wirklich zweihunderttausend Euro kosten darf oder nicht, habe ich in letzter Zeit in Unternehmen, mit deren Storage-Strategie ich mich befasst habe, immer wieder feststellen müssen: einen richtigen Markt gibt es im Storage-Bereich noch nicht. Das Budget für Storage wächst und wächst auch in Zeiten, wenn die anderen Posten im IT-Ausgabenplan zusammengestrichen werden müssen. Dass dies so ist und bleibt, findet man ganz normal. Schließlich gehören die Daten zu den wichtigsten Gütern der Firma. Und es ist bei jedem angekommen, dass das Datenvolumen jährlich um 60 % wächst. Kommt der Sohnemann nicht jedes Jahr vor Weihnachten mit dem Wunsch nach einem neuen PC, weil seine Platte schon wieder voll ist? Warum soll es in der Firma anders sein?

Also ist nichts dabei, wenn jedes Jahr mehr Geld für Storage ausgegeben wird. Schließlich müssen die Daten irgendwo gespeichert werden und dabei verfügbar sein. Stolz präsentiert man dem oberen Management die Terabyte-Zahlen. Super, wir bezahlen pro Terabyte einen Bruchteil von dem, was wir bei der letzten Beschaffung zahlen mussten. Unsere Datenmenge explodiert, aber wir haben jährlich nur 10% mehr Storage-Ausgaben als im Vorjahr. Gut gemacht!

Storage bisher: zu groß, zu monolithisch, zu unflexibel

Nein, ich will nicht glauben, dass die Unternehmen dazu verurteilt sind, derart steigende Kosten bei Storage hinzunehmen. Ich behaupte, diese Situation ist zumindest teilweise dem Umstand geschuldet, dass vermeintliche Zwänge aufgebaut und die Unternehmen in eine Ausgabenspirale gelockt worden sind, aus der sie keinen Ausweg sehen. Zu monolithisch und unflexibel sind die Storage-Strukturen, die in den letzten zehn Jahren aufgebaut worden sind. Die Gründe für die Zentralisierung von Storage waren einleuchtend. Daten, die verteilt auf Dutzende und Hunderte Server mit Direct Attached Storage gehalten, gesichert und hochverfügbar gemacht werden mussten, schrien regelrecht nach einer anderen Lösung. Der Bedarf nach zentral gehaltenen, zentral verwalteten und zentral gesicherten Daten war und ist real. Firmen wie EMC und NetApp haben diesen Bedarf rechtzeitig erkannt und ihr Geschäftsmodell darauf aufgebaut. Sie waren erfolgreich. Weniger erfolgreich waren ihre Kunden, denn – ich wiederhole – einen richtigen Markt hat es im Storage-Bereich nie gegeben.

Wie sieht ein echter Markt aus?

Ich komme zurück auf meinen eingangs zitierten Gesprächspartner und sein Klagen über die Vorgesetzten, die keine zweihunderttausend Euro für einen LAN-Switch ausgeben wollten. Warum nicht? Der Netzverantwortliche meinte, das liege an der Größe und am Gewicht des LAN-Switches im Vergleich zur Tape Library. Ich mache es mir nicht so einfach. Die Entscheidungsträger wissen doch mehr als es scheinen mag. Sie kommen auf Kongressen, Messen und anderen Events zusammen und tauschen Erfahrungen aus. Sie wissen, was das Netz in anderen Unternehmen gekostet hat. Und sie wissen auch, dass alle Unternehmen Leidgenossen sind, wenn das Gespräch auf das Storage-Budget kommt. Tatsache ist, dass es einen mit dem Server- oder dem Netzmarkt vergleichbaren Wettbewerb im Storage-Bereich nie gegeben hat. Die Storage-Kosten sind hoch, weil der Kunde keinen echten Wettbewerb nutzen kann. Das liegt an der Struktur des zentralen Speichers: zu groß, zu unflexibel, zu monolithisch.

Kommt Ihnen das bekannt vor? Genau, so waren die Strukturen im Serverbereich auch: zu große, zu unflexibel, zu monolithisch. Man nannte das Mainframe. IBM wurde damit groß und beherrschte die Datenverarbeitung für Jahrzehnte. Bis sie meinte, auch in den Anfang der 1980er Jahre noch den Ataris und Commodores vorbehaltenen Consumer-Markt einsteigen zu müssen und dafür einer Firma zum Aufstieg verhalf, die später mit nichts anderem als dem PC aus dem Cosumer-Markt dem Mainframe-Zeitalter ein Ende setzte: Microsoft.

Server sind nunmehr „Commodity“, wie es heißt. Überspitzt formuliert kann man die Entscheidung über die Beschaffung von Servern der Einkaufsabteilung überlassen. Server-Hardware unterliegt im Zusammenspiel mit der Außenwelt und den auf den Servern laufenden Applikationen strengen Standards. Standards schaffen Vergleichbarkeit, und nur mit Vergleichbarkeit gibt es einen Markt.

Zurück zum Speicher: ist es nicht so, dass es mehrere Hersteller von Strage-Systemen gibt? Sind EMC, Hewlett-Packard, Hitachi, IBM, NetApp und andere nicht Wettbewerber auf dem Speichermarkt? Das sind sie, aber was nützt den Kunden ihr Wettbewerb, wenn

- laut Marktstudien nur 20 % der Storage-Kosten auf die Hardware-Beschaffung zurückzuführen sind,

- mit der Beschaffung eines großen Speichersystems jahrelang nur Erweiterungen für dieses System getätigt werden, und

- die strengen Interoperabilitätsvorgaben der Hersteller uns teure Entscheidungen für Datensicherungssoftware, Virtualisierungslösungen und Support-Verträge aufzwingen?

Nur eine Umgebung, in der jede Hardware- oder Software-Komponente ersetzbar ist, schafft Raum für Wettbewerb. Wir bei ComConsult können mit Stolz behaupten, im letzten nahezu Vierteljahrhundert zur Entwicklung eines echten Marktes für Netze in einer der größten Volkswirtschaften der Welt beigetragen zu haben. Uns war von Anfang an klar: wir werden nur gebraucht, wenn wir unabhängig von Herstellern ihre Kunden beraten können. Und die Kunden nehmen unsere Beratung nur in Anspruch, wenn sie die Qual (aber auch die Chancen) der Wahl haben. Eine echte Wahl gibt es nur dann, wenn Netzkomponenten beliebig austauschbar sind. Hier zeigt sich der wahre Wert von Standards. Die offene Netzwelt konnte nicht anders als Standards folgen. Es konnte kein Internet entstehen ohne Standards, und auch keine unternehmensinternen Netzstrukturen, die für alle Systeme offen waren. Dass viele Unternehmen im Netzbereich einer Single-Vendor-Strategie gefolgt sind, änderte nichts daran, dass der ausgewählte Hersteller sich ständig mit dem Markt messen musste. Wir erleben zurzeit mal wieder eine echte Belebung des LAN-Marktes, einen echten Wettbewerb zwischen Herstellern, die den Kunden eine neue Generation von Netztechnik mit 10, 40 und 100 Gigabit Ethernet anbieten. Der Ausgang jeder echten LAN-Ausschreibung ist völlig offen.

Im Speicherbereich sind wir noch weit davon entfernt. Einen echten Mainframe-Markt hat es auch nie gegeben, auch wenn es verschiedene Mainframe-Hersteller gegeben hat.

Neue Lösungen

Ich möchte aber über das reine Beklagen einer für die Kunden ungünstigen Situation im Speicherbereich hinaus gehen und von der schlechten Nachricht im Titel dieses Artikels zur guten Nachricht kommen: Im Speichermarkt tut sich etwas.

Dass es mit der Datenhaltung in Unternehmen nicht zum Besten bestellt ist, weiß man seit Jahren. Die Missstände sind allen Beteiligten bekannt, hier drei der wichtigsten:

- Ein hoher Anteil des Storage-Budgets wird für die Haltung, redundante Speicherung und tägliche Sicherung von Datenbeständen aufgebraucht, die für das Unternehmen keinen oder nur einen nachrangigen Wert haben.

- Die Datensicherung funktioniert in den meisten Unternehmen nicht so richtig. Es gibt keine ausreichenden Sicherungsfenster, und man möchte sich gar nicht vorstellen, was bei einem echten Restore-Test alles ans Tageslicht kommen würde.

- Neben der offenen Netzinfrastruktur, die seit den 1990er Jahren auf der Basis der Standards Ethernet und TCP/IP aufgebaut wurde, ist ein immer größer werdendes Storage Area Network entstanden, das nur dem Anschein nach auf Standards basiert. Server, Betriebssysteme, Storage-Systeme, Virtualisierungslösungen und Applikationen müssen ins enge Korsett von sogenannten Interoperabilitätsmatrizes eingepasst werden.

In den letzten Jahren hat es mehrere Anläufe gegeben, diese Missstände zu beheben, zum Beispiel den erstgenannten.

Die mangelnde Effizienz und Wirtschaftlichkeit von monolithischen Speicherstrukturen wurde bald nach der ersten Zentralisierungswelle Anfang der 2000er Jahre deutlich. Jedem leuchtete ein, dass die Kosten für die ausfallsichere Haltung und Sicherung einer Dutzende Megabytes schweren Powerpoint-Präsentation mit sofortigem Wertverlust nach der Verwendung der Datei unverhältnismäßig hoch war. Schon vor acht oder neun Jahren machte der Begriff Hierarchisches Speichermanagement (HSM) die Runde. Grundidee: nicht alle Daten über denselben Kamm scheren, sondern sogenannte Storage Tiers bilden, für die ein unterschiedliches Maß an Performanz und Verfügbarkeit realisiert wird. Die Termini Online-, Nearline- und Offline-Speicher wurden geprägt (siehe Abbildung 1).

Bald wurde aber klar, dass eine rein technische Lösung das Problem nicht lösen konnte. Die Technik allein konnte nicht entscheiden, welche Daten welchem Storage Tier zuzuordnen sind. Der HSM-Ansatz wurde zum „Information Lifecycle Management“ (ILM) erweitert, bei dem es nicht nur um die Unterscheidung zwischen Storage Tiers, sondern generell um die Verwaltung des gesamten Lebenszyklus von Informationen im Unternehmen geht. Dass dabei auch organisatorische Prozesse angepasst werden müssen, leuchtet ein. Am besten funktioniert der Ansatz beim projektorientierten Arbeiten: Organisatorische Prozesse sorgen für die unterschiedliche Behandlung der Daten von laufenden und abgeschlossenen Projekten. Während erstere einer ständigen Änderung unterliegen, täglich im schnellen Zugriff sein und gesichert werden müssen, wird auf letztere nicht mehr so häufig zugegriffen. Diese bleiben un-

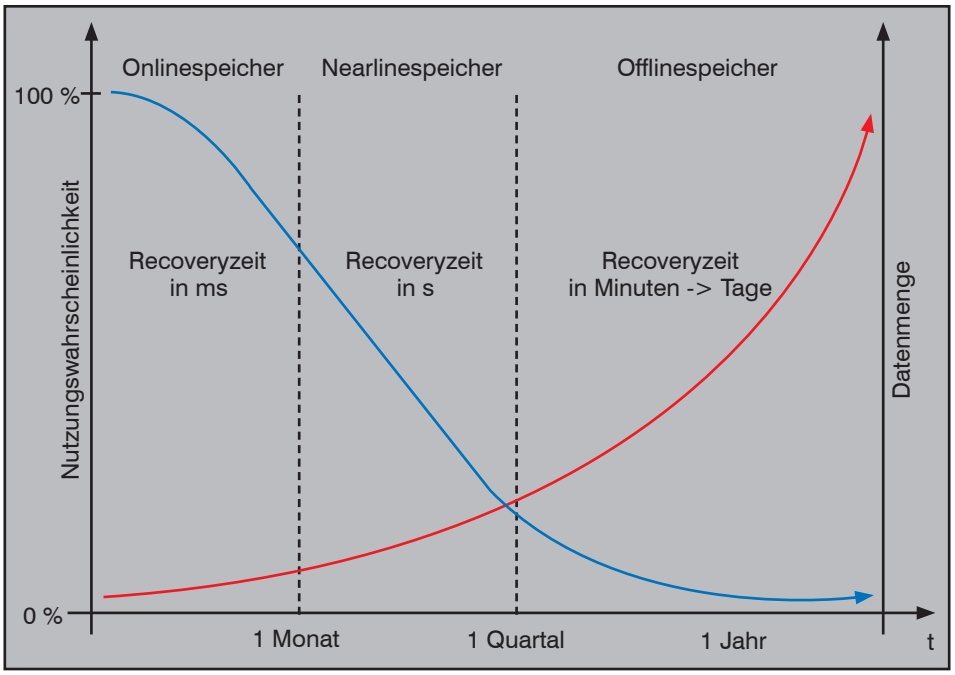


Abbildung 1: Online-, Nearline und Offline-Speicher

verändert und müssen nicht täglich gesichert werden.

Solange man aber große und monolithische Speichersysteme einsetzt, bringt ILM in der Datenhaltung keine wesentlichen Vorteile. Es gibt zwar Kostenunterschiede zwischen FC- und SATA-Platten in großen Speichersystemen, aber die reinen Plattenkosten machen ohnehin den kleineren Teil der Speicherkosten aus.

Die Unterscheidung zwischen Storage Tiers führt erst mit einem Ansatz zu echten Einsparungen, der statt eines großen monolithischen Storage-Systems auf einer Mischung von echt unterschiedlichen Speichern basiert. Es ist klar: ein Storage-Anbieter, der jahrelang am Verkauf großer teurer Systeme verdient hat, hat kaum ein Interesse daran, dies zu ändern, wenn er dazu nicht gezwungen wird.

Meiner Meinung nach braucht daher der Storage-Markt Anstöße von außen. Nur neue Lösungen können den Markt aufmischen.

Der Hersteller F5, den man eher als Anbieter von Load-Balancern und Layer-4/7-Switches kennt, könnte für einen der externen Anstöße sorgen. Mit „ARX File Virtualization“ bietet der Hersteller eine Lösung an, die zwischen Clients und File Services eine Virtualisierungsebene vorsieht (siehe Abbildung 2). Die ARX-Instanz dient als Proxy beim Zugriff auf Dateien. Die tatsächliche Datenhaltung ist somit von der Präsentation der Daten für die Clients entkoppelt. Daten können verlagert werden, ohne dass es Downtimes für die Benutzer gibt. Eine solche Verlagerung im laufenden Betrieb könnte im Wesentlichen zwei Zwecken dienen:

- Migration sowie
- automatischer Bewegung von Daten zwischen Storage Tiers.

Letzteres kann anhand verschiedener Kriterien wie Alter der Daten und Häufigkeit von Änderungen erfolgen. Neu ist der Ansatz nicht. Schon vor acht bis neun Jahren wurde über solche automatische Verlagerungen im Rahmen von HSM diskutiert. Neu ist aber, dass die Lösung völlig unabhängig von den verschiedenen eingesetzten Speichertypen ist.

Der Einsatz verschiedener Storage Tiers kann auch zur Entschärfung des Backup-Problems beitragen, wie in der Abbildung 3 dargestellt ist. Werden nicht alle Daten häufig oder gar täglich gesichert, verschafft sich der Backup-Administrator Luft

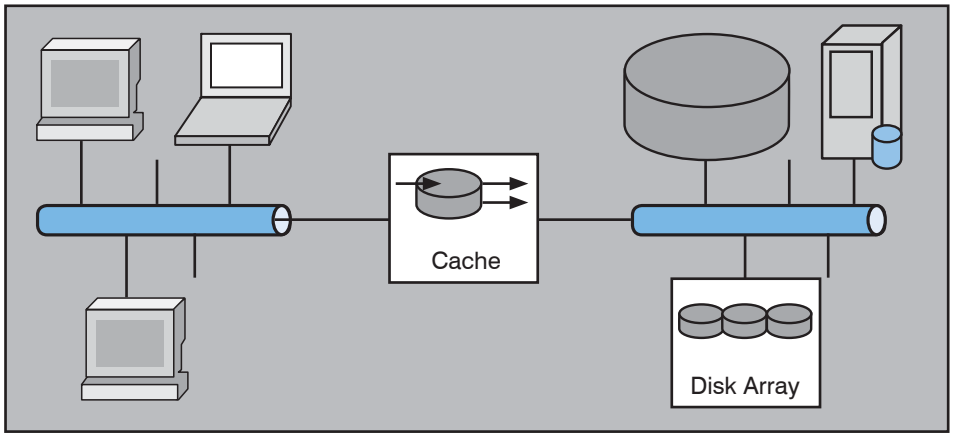


Abbildung 2: File Virtualization von F5

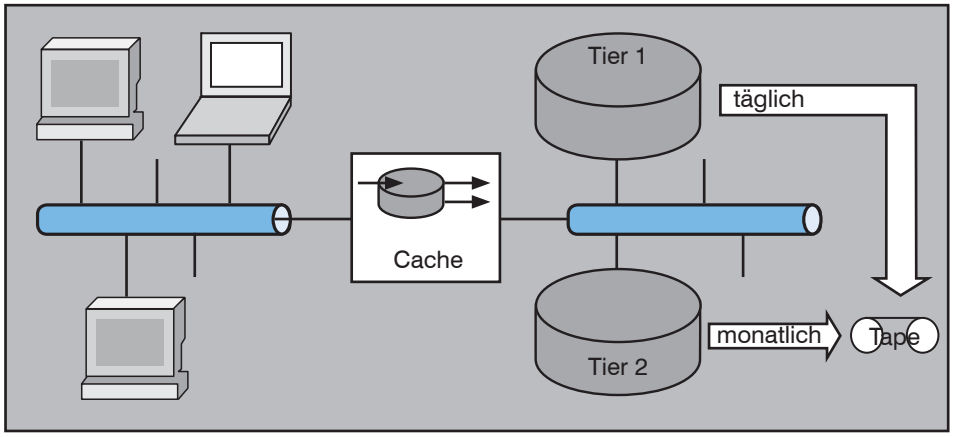


Abbildung 3: Unterschiedliche Behandlung von Storage Tiers

und kann die Priorität auf echte unternehmenskritischer Daten setzen, die täglich gesichert werden müssen. Dann braucht man auch weniger von den teuren Ressourcen wie Bandlaufwerken und Tape Libraries.

Auch die Erkenntnis, dass ein ewiges Nebeneinander von LAN und SAN und der Anschluss jedes Servers an beide Infrastrukturen nicht wirtschaftlich sein können, ist nichts Neues. Schließlich ist der Standard iSCSI fast zehn Jahre alt. Aber solange die Speicherstrukturen in den Unternehmen groß, unflexibel und monolithisch waren, half die Möglichkeit, das SCSI-Protokoll über TCP zu übertragen, wenig. Lange Zeit wurde iSCSI als Storage-Protokoll für kleine Umgebungen abgetan. Jetzt bewegt sich aber der Markt. In den letzten Jahren haben die klassischen Player im Storage-Markt erkannt, dass die Party mit den schönen hohen Umsätzen bald vorbei sein kann, weshalb einige der großen Hersteller auf Einkaufstour gingen und kleinere Hersteller übernahmen, die auf eine Zukunft mit verteilten Speichersystemen setzten. Exemplarisch: HP, die LeftHand übernommen hat.

HP spricht wie IBM, die den israelischen Hersteller XIV übernahm, von einer GRID-Lösung für Storage (siehe Abbildung 4). Die GRID-Idee besteht darin, kleine Speichersysteme, die jeweils zum Beispiel aus 8 bis 12 Platten bestehen, über Ethernet/IP miteinander zu vernetzen und mittels iSCSI Speicherkapazitäten zur Verfügung zu stellen. Der Ansatz redundanter Anordnungen von Platten (Redundant Array of Independet/Inexpensive Disks, RAID), der seit den 1990er Jahren für die Vermeidung von Datenverlusten durch Plattenausfälle üblich ist, wird nun auf vernetzte Systeme übertragen und Network RAID genannt. Statt teurer Storage Cluster kann man nun auf einen Verbund von kleineren Speichersystemen setzen, der preiswerter und skalierbarer als die monolithischen Systeme ist. Abgerundet wird das System mit Network Attached Storage für File Services und Disc-to-Disc Backup mit Deduplizierung für schnellere Backups.

Fazit

Hier sind wir nur exemplarisch auf zwei der Lösungen eingegangen, die nunmehr auf dem Markt verfügbar sind und mit de-

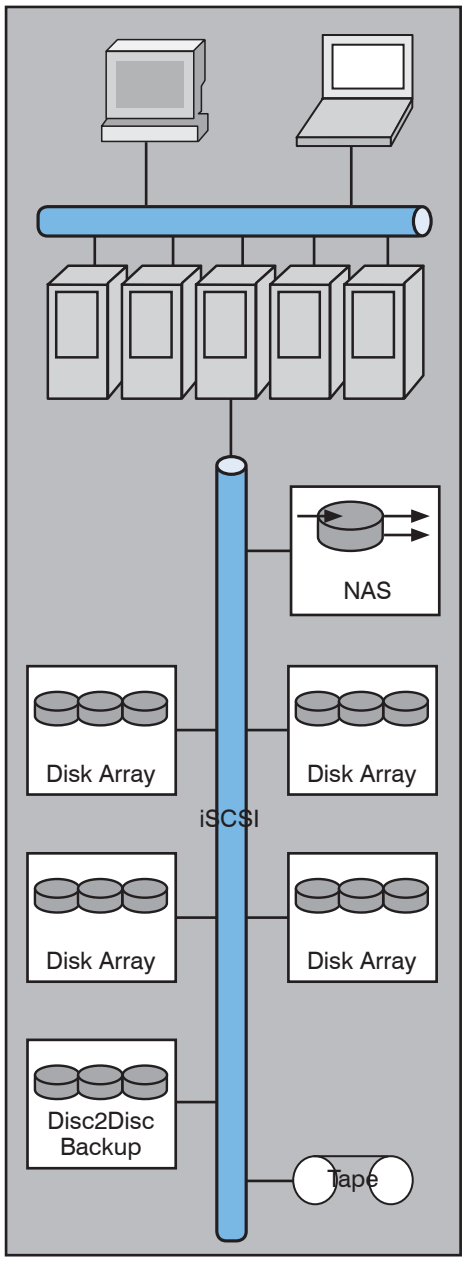


Abbildung 4: Storage GRID von HP

nen eine Weiterentwicklung von Storage in Richtung verteilter, flexibler und skalierbarerer Strukturen möglich ist. Aber zum Markt gehören immer zwei Seiten: die Angebots- und die Nachfrageseite. Auf der Nachfrageseite muss auch etwas geschehen. Nur wenn die Kunden sich mit ihren Anforderungen einbringen und genügend Druck aufbauen, wird sich der Storage-Markt in die Richtung entwickeln, die den Interessen der Kunden entspricht: in Richtung eines Marktes, der geprägt ist von offenen Standards und in dem die Kunden deutlich mehr Wahl haben werden als bisher.

Wenn sie neugierig sind, wie Details neuer Storage-Lösungen aussehen und wie führende Hersteller den Zukunft des Storage-Marktes sehen, ist das ComConsult Storage Forum 2011 die ideale Veranstaltung für Sie. Ich persönlich bin sehr gespannt auf die Diskussion mit Ihnen und mit den dort vertretenen führenden Herstellern.

Aktueller Kongress

ComConsult Storage-Forum 2011
13.07. - 15.07.11 in Bonn

Zentraler, im Netzwerk zugreifbarer Speicher steht im Mittelpunkt aller zukünftigen IT-Architekturen. Die technologische Spannweite ist riesig, permanent kommen neue Entwicklungen und Produkte hinzu. Das ComConsult Storage-Forum 2011 analysiert die aktuellen Entwicklungen im Speichermarkt, vergleicht Alternativen und zeigt auf, wo der Weg hingeht

Alle wesentlichen IT-Architekturen werden sich in Zukunft auf zentrale, im Netzwerk zugreifbare Speicher-Lösungen abstützen. Die Bandbreite technologischer Entwicklungen in diesem Bereich, angefangen von neuen IT-Architekturen und hin zu neuen Speicher-Lösungen ist gewaltig. Kombiniert man das mit einem immer weiter wachsenden Datenbestand, dann ergibt dies ein explosives Gemisch:

- Immer mehr Daten müssen beherrscht werden.
- Immer mehr Applikationen hängen von zentralen Speicher-Systemen ab.
- Basis-Funktionen wie Backup/Restore werden zu einem echten Problem.

Die Gründe für den weiter wachsenden Bedarf sind vielfältig:

- Mehr Rechenleistung gestattet die Verarbeitung von immer mehr Daten.
- Auch neue Applikationen und Applikationstypen (Video, Web 2.0/3.0) erzeugen erhebliche Datenmengen.
- Zunehmende Automatisierung (RFID) stellt immer mehr Daten bereit.
- Eine veränderte Risiko- und Rechtssituation erfordert mehr Detail-Daten für eine verbesserte Prognose-Sicherheit.
- Neue Formen der Vermarktung erzeugen neue Daten (Internet).
- Verändertes Kundenverhalten schafft neue Daten zu Kunden-Bedürfnissen und Erwartungen.
- Virtualisierung und Konsolidierung von Servern zentralisiert Daten.

Dies erfolgt parallel zu wesentlichen Änderungen in IT-Technologien und Architekturen, die neue Anforderungen an die Leistung und Qualität von Speicher erzeugen:

- Virtualisierung geht immer mehr weg von der simplen Konsolidierung und hin zur Schaffung neuer Architekturen für Webanwendungen.
- Neue Virtualisierungsverfahen wie vMotion, HA, Desaster Recovery generieren erhebliche Anforderungen an Speicher-Performance.
- Traditionell wurde die Leistung von SAN-Systemen in I/O-Transaktionen pro Sekunde gemessen, mit den neuen Architekturen kommen erhebliche Anforderungen an Bandbreite hinzu.
- Mit Desktop-Virtualisierung entsteht ein erheblicher Mehrbedarf an Speicher.
- Neue Netzwerk-Technologien geben dem Netzwerk Systembus-Charakter und ermöglichen eine Speicher-Einbindung mit bisher unbekannter Leistung.
- Die Entwicklung von SSD-Speicher muss als sehr kritisch angesehen werden, stellt sie doch die traditionelle Formel Lokale Leistung = Zentrale Leistung in Frage. SSD muss zwangsläufig auch im SAN eine Rolle spielen oder es entsteht ein Performance-Loch zur Server-Leistung. Dies generiert neue Probleme im Netzwerk.

Moderatoren: Dipl.-Inform. Matthias Egerland, Dr. Franz-Joachim Kauffels
Preis: € 1.990,-- zzgl. MwSt.

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Virtualisierungstechnologien in der Analyse, 21.03. - 23.03.11 in Stuttgart

Dieses Seminar analysiert die verfügbaren Virtualisierungstechnologien der führenden Anbieter. Sie lernen, welche Gestaltungselemente virtuelle Umgebungen haben, angefangen von einfachen und überschaubaren Lösungen bis hin zu komplexen und umfassenden Rechenzentrums-Gesamt-Architekturen. Dabei wird auch der Bedarf an Infrastruktur-Leistung insbesondere auf der Netzwerk- und Speicherseite untersucht. Preis: € 1.890,-- zzgl. MwSt.

Sicherheitsmechanismen für Voice over IP, 21.03. - 22.03.11 in Stuttgart

Angesichts der Offenheit und geringeren Verfügbarkeit von Datennetzen ist das Thema Sicherheit das zentrale Projektthema bei der Umsetzung von Voice over IP. VoIP benötigt Sicherheitsmechanismen, die mindestens ein den konventionellen Telekommunikationsnetzen entsprechendes Niveau an Vertraulichkeit, Verlässlichkeit, Verfügbarkeit und Integrität sicherstellen. Darüber hinaus bietet die Umstellung die Chance, die Sicherheit der Sprachkommunikation über das bisherige Niveau hinaus zu verbessern.

Preis: € 1.490,-- zzgl. MwSt.

Aktuelle VPN-Technik, 23.03. - 25.03.11 in Aachen

Die Nutzung von VPN-Technik hat sich in der jüngeren Vergangenheit insbesondere im Bereich des Remote Zugriffs mobiler oder auch stationärer Anwender (Stichwort: Telearbeit) auf zentrale Ressourcen als mehr oder weniger Standard-Lösungsansatz etabliert. Aber auch zur kostenoptimierten Anbindung von (typischerweise kleineren) Remote-Standorten an Corporate WAN-Strukturen bewährt sich dieser Ansatz. Dieses Seminar vermittelt die für einen erfolgreichen VPN-Einsatz notwendigen Kenntnisse der aktuell relevanten Technologien. Alle wesentlichen Bausteine typischer Lösungen werden detailliert erklärt und anhand praktischer Projektbeispiele und Übungen wird der Weg zu einer erfolgreichen VPN-Lösung aufgezeigt. Preis: € 1.890,-- zzgl. MwSt.

Sonderveranstaltung: UC - Cisco versus Microsoft - Wer hat die bessere Unified-Communications-Lösung?, 24.03. - 24.03.11 in Düsseldorf

Die Sonderveranstaltung UC - Cisco versus Microsoft analysiert die bestehenden UC-Lösungen von Cisco und Microsoft und stellt die spannende Frage, wer die bessere Lösung hat. Auch die erkennbaren Weiterentwicklungen der nächsten Jahre werden dabei berücksichtigt. Bewertet wird nicht nur die rein technische Funktionalität, sondern die Veranstaltung gibt auch Einschätzungen zum strategischen Einsatz sowie zur Zukunftssicherheit der Produkte ab. Preis: € 890,-- zzgl. MwSt.

Service-Spezifizierung - Grundlegende Methode für verlässliche, rationelle und rentable Service-Erbringung, 28.03. - 30.03.11 in Bonn

In diesem Seminar erlernen die TeilnehmerInnen die grundlegende Methodik der Service-Spezifizierung und die durchgängige Anwendung der Service-Spezifikation. Preis: € 1.890,-- zzgl. MwSt.

Sicherheitsmanagement mit BSI-Grundschutzmethodik/ ISO 27001, 28.03. - 30.03.11 in Bonn

Informationssicherheit ist heutzutage ein Muss, sei es aus rechtlichen oder wettbewerbstechnischen Gründen. Den vielfältigen „Compliance“-Ansprüchen gesellt sich der Aspekt einer Konformität zu BSI-Methodik bzw. ISO 27001 hinzu und die Anforderung, sich an den zugehörigen Kontrollfragen und Maßnahmenkatalogen erfolgreich messen zu können. Längst sind ISO 27001 und BSI-IT-Grundschutz nicht mehr nur eine Möglichkeit, sich „werbewirksam“ zertifizieren zu lassen. Vielfach liefert ihre Anwendung die erwartet plausible Antwort auf die Frage nach Erreichung eines „best-practice“-Mindest-Sicherheitsniveaus oder nach angemessenem (!) Sicherheitsaufwand bei erhöhtem Sicherheitsbedarf. So nützlich diese Hilfestellung bei Aufbau und Aufrechterhaltung der nötigen Sicherheit sind, so sehr kann bei mangels Erfahrung „ungeschickter“ Anwendung ein enormer, vermeidbarer Arbeitsaufwand entstehen. Erfahrungen aus ComConsult-Projekten zur Anwendung der Methoden und Werkzeuge, mit und ohne abschließender Zertifizierung, können und sollen hier helfen. Preis: € 1.890,-- zzgl. MwSt.

SIP (Session Initiation Protocol) - Basis-Technologie der IP-Telefonie, 28.03. - 30.03.11 in Bonn

Dieses 3-tägige Seminar vermittelt Planern, Betreibern und Administratoren Anforderungen und Technologien für den Einsatz von Telefonie und Mehrwertdiensten auf Basis des SIP-Standards. Chancen und Risiken werden anhand von Einsatzszenarien bewertet und kontrovers diskutiert. Der größte Nachteil der bisher realisierten VoIP- und Unified Communications- (UC) Lösungen ist, dass sie mit hersteller-spezifischen Protokollen arbeiten. Doch dies ist ein Übergangs-Zustand. Das Session Initiation Protocol wird in Zukunft der gemeinsame Standard für IP-Telefonie und alle Echtzeit-Anwendungen werden. Schon jetzt sind signifikante Anbieter wie Cisco, Microsoft und Siemens auf diesen Standard umgeschwenkt, die verbleibenden Anbieter werden das kurz- bis mittelfristig nachholen.

Preis: € 1.890,-- zzgl. MwSt.

Netzanalyse und sicherheitstechnische Bewertung elektrischer Netze in Rechenzentren, 11.04. - 13.04.11 in Bonn

Die Verfügbarkeit und Anfälligkeit der elektrischen Netze wird heute unterschätzt. Schon leichte Störungen führen zu Ausfällen der EDV, trotz eingebauter Schutzeinrichtungen. Kostendruck und knappe Zeitvorgaben sowie lange Lieferzeiten führen zu Fehlentscheidungen in der Planung und Installation der elektrischen Anlagen für den EDV-Betrieb. Verfügbarkeitsbetrachtungen sind nie gemacht worden und es sind keine geeigneten Hilfs-und Messmittel eingebaut, welche Abweichungen des Betriebes rechtzeitig erkennen lassen, um Ausfälle und Störungen zu verhindern. Preis: € 1.890,-- zzgl. MwSt.

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
11.04. - 15.04.11 in Aachen
12.09. - 16.09.11 in Aachen
05.12. - 09.12.11 in Aachen

TCP/IP intensiv und kompakt
09.05. - 13.05.11 in Königswinter
26.09. - 30.09.11 in Stuttgart

Internetworking
16.05. - 20.05.11 in Aachen
17.10. - 21.10.11 in Aachen

Paketpreis für alle drei Seminare € 6.720,-- zzgl. MwSt. (Einzelpreise: je € 2.490,--)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
17.05. - 20.05.11 in Aachen
20.09. - 23.09.11 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
28.06. - 01.07.11 in Aachen
18.10. - 21.10.11 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.280,-- zzgl. MwSt.
(Seminar-Einzelpreis € 2.290,--, mit Prüfung € 2.470,--)

ComConsult Certified Voice Engineer

Session Initiation Protocol-Basis-Technologie der IP-Telefonie
28.03. - 30.03.11 in Bonn
27.06. - 29.06.11 in Hamburg
14.11. -16.11.11 in Bonn

Sicherheitsmechanismen für Voice over IP
21.03. - 22.03.11 in Stuttgart
04.07. - 05.07.11 in Nürnberg
17.11. - 18.11.11 in Aachen

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
06.06. - 08.06.11 in Nürnberg
26.09. - 28.09.11 in Stuttgart
28.11. - 30.11.11 in Köln

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 4.740,-- zzgl. MwSt. statt € 5.270,-- zzgl. MwSt.

Optionales Einsteigerseminar: Aufpreis € 1.090,-- zzgl. MwSt. statt € 1.490,-- zzgl. MwSt.

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
23.05. - 24.05.11 in Königswinter
10.10. - 11.10.11 in Berlin

ComConsult Zertifizierter Projektleiter

Projektmanagement I: Projekte aus IT und Kommunikationstechnik leiten und organisieren
28.03. - 01.04.11 in Aachen
17.10. - 21.10.11 in Aachen

Projektmanagement II: Sitzungen moderieren, Projekte präsentieren, erfolgreich verhandeln und Teams führen
02.05. - 06.05.11 in Köln
14.11. - 18.11.11 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.480,-- zzgl. MwSt. (Einzelpreise: € 2.490,--)

Impressum

Verlag:
ComConsult Technology Information Ltd.
ComConsult Research
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline of ComConsult-Research:
02408-955300

E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich,
12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service
der ComConsult Akademie

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen
Nachdruck, auch auszugsweise
nur mit Genehmigung des Verlages
© ComConsult Research