Rolf-Dieter Köhler
Erwin Kampmann

Mehr Sicherheit *in* Netzwerken

Wünsche
Visionen
Realisierungen

compress

Rolf-Dieter Köhler (Dipl.-Ing.)



studierte an der TU Chemnitz Informationstechnik. Nach mehrjähriger Tätigkeit als Entwickler von Betriebssystemkomponenten für Steuerungssysteme war er an der Entwicklung rechnergestützter Produktionsprozesse für einen vollautomatisierten Betrieb beteiligt. Bei der Firma Compu-Shack war er als Supportingenieur für Novell NetWare tätig, bevor er in den Bereich der aktiven und passiven Netzwerkkomponenten wechselte. Als Projektingenieur leitete er zahlreiche große Netzwerkrealisierungen in Deutschland und im Ausland. Seit 1997 ist R.-D. Köhler bei der Firma 3Com als Network Consultant tätig.

Erwin Kampmann



sammelte nach seinem Studium in München Erfahrungen im Bereich der Hard- und Software-Entwicklung. Anschließend lernte er beim damaligen Minicomputer- und Netzwerk-Pionier Digital Equipment die ersten verfügbaren Ethernet-Komponenten kennen und begleitete diese aufstrebende Branche als Dozent und Berater für Hardware und Netzwerk-Betriebssysteme. Über den Netzwerkspezialisten Chipcom gelangte er 1995 zu 3Com und wirkt dort seit 1995 im Produktmarketing und im Consulting-Bereich maßgebend an der Umsetzung neuer Lösungen im LAN-Bereich mit.

FOSSIL-Verlag GmbH
Siebachstraße 51
D-50733 Köln
www.fossilverlag.de
info@fossilverlag.de

Mehr Sicherheit in Netzwerken

Rolf-Dieter Köhler/Erwin Kampmann

Mehr Sicherheit in Netzwerken

Wünsche • Visionen • Realisierungen

Impressum

Kampmann, Erwin: NE:
Rolf-Dieter Köhler:
Mehr Sicherheit in Netzwerken;
Wünsche – Visionen – Realisierungen
ISBN 3-931959-XX-X
BVK 24,50 DM

FOSSIL-Verlag GmbH Februar/März 2000

FOSSIL-Verlag GmbH
Siebachstraße 51
50733 Köln

Tel. +49 (0)221 72 62 96
Fax +49 (0)221 72 60 67
www.fossilverlag.de
info@fossilverlag.de

Vorwort

An Netzwerke der neuen Generation werden auch neue Anforderungen gestellt, denn die vormals reinen Datennetzwerke sind zu Multimedia-Netzwerken geworden.

Dies ist nicht nur ein Schlagwort, um bestimmte Produkte zu vermarkten, sondern stellt die logische Änderung der Nutzung der Netzwerke dar.

Netzwerke werden bereits zur Übertragung von Videokonferenzen genutzt. Die Einbeziehung der Sprachübertragung wird ebenfalls realisiert, und die ersten Produkte für die Sprach-Daten-Integration stehen zur Verfügung.

In dieser Broschüre werden in erster Linie allgemeine Stabilitätskriterien für Netzwerke erörtert. Dabei liegt der Schwerpunkt auf den aktiven Netzwerkkomponenten. Doch auch andere Themen, die zum Umfeld der Stabilitätskriterien gehören, werden kurz vorgestellt. Zu diesen „Randproblemen" gehören u.a. die stabile Stromversorgung, der Einsatz von Backup-Systemen zur Absicherung des Datenbestandes oder die Absicherung durch Service-Verträge.

Was bedeutet Datensicherheit? Daten müssen immer verfügbar sein,unabhängig davon wo sie im komplexen Netzwerk benötigt werden. Eine Grundforderung lautet: Sicherheit und Vertraulichkeit aller transportierten Daten muß zu jedem Zeitpunkt gewährleistet sein.

Was bedeutet Zuverlässigkeit? Hierunter ist nicht nur die ständige Intaktheit des Netzwerkes zu verstehen. Hierzu gehören auch Mechanismen zur optimalen Auslastung der Ressourcen in den Bereichen, in denen die Bandbreite nicht „unendlich“ hoch sein kann, wie z.B. im WAN-Umfeld. Zu erzielen ist dies z.B. durch eine optimierte Datenflußsteuerung. So müssen auch Lösungen gefunden werden,die mittels IEEE 802.1p priorisierte Daten in IP-TOS (Internet Protocol – Type of Services) gewichtete Daten konvertieren können, damit diese Datenmerkmale während ihrer Übertragung über WAN-Verbindungen nicht verloren gehen.

Auch eine sinnvolle Broadcast-Kontrolle steigert die Verfügbarkeit des Netzwerkes, da durch sie unnötige Datenströme im gesamten Netzwerk auf ein Minimum verringert werden können. Und letztlich führt auch der Managementaspekt dazu, dass im Fehlerfall schnell reagiert werden kann.

Diskussionen zu hochverfügbaren Netzwerken wurden früher oft nur in Verbindung mit der ständigen Verfügbarkeit von Server-Geräten oder anderen zentralen Datenquellen geführt.

Firmen wie Tandem und NetFrame definierten daher diese hohe Verfügbarkeit zu ihren Handelsmarken. Aber auch Sun,HP und IBM boten spezielle Lösungen für fehlertolerante Systeme auf der Basis ihrer eigenen Produkte an.

Andere Diskussionen widmeten sich dem Thema der Software-Redundanz. Denken wir doch nur einmal an spezielle Server-Cluster-Software für NT- und UNIX-Systeme oder auch Microsoft’s NT Server, Novell’s Standby Server und die breite Pallette der anderen Systeme.

Im anbrechenden Zeitalter der konvergierenden Netzwerke, wo Daten-,Sprach- und Bildübertragung einheitliche Betrachtungsweise der Netzwerkdienste werden, verändert sich die Diskussion der Netzwerksicherheit inhaltlich. In Anwendungsbereichen wie Telemedizin, IP-Telefonie oder anderen sensiblen Bereichen müssen Netzwerke unter den Aspekten der Sicherheit und der Zuverlässigkeit betrachtet werden.

Begriffe wie Mission Critical Applications, New Applications und Echtzeitverarbeitung weisen auf die Anforderungen für die kommende Netzwerkgeneration deutlich hin.

Unter welchen Gesichtspunkten das Thema der Verfügbarkeit auch betrachtet wird, eines muss immer deutlich sein: Alle anwendungskritischen Applikationen müssen über das Netzwerk übertragen werden. Somit gilt der Begriff der hochverfügbaren Netzwerke vom Datenzentrum bis zur Adapterkarte für alle aktiven Komponenten, durch das LAN und über das WAN hinweg.

Rolf-Dieter Köhler
Erwin Kampmann
Mittweida/Neuried, Februar 2000

Inhalt

Vorwort

1 Anforderungen an Netzwerke 13

1.1 Die Kosten eines Netzwerkausfalls 15
1.2 Mögliche Ursachen für Netzwerkstillstand 17
1.3 Der Weg zur besseren Verfügbarkeit 18

2 HoheVerfügbarkeit – Die Strategie für große Unternehmensnetzwerke 21

2.1 Hoch verfügbare Rechenzentren 23
2.2 Hoch verfügbare Campus- und Gebäudeverteiler26
2.3 Redundanz in den Etagenverteilern 29
2.4 Redundanz bis zur Adapterkarte 31

3 Techniken der Link-Redundanz bei 10/100/1000 Ethernet 35

3.1 Spanning-Tree 37
3.2 Resilient-Links.....41
3.3 Link-Aggregation IEEE 802.3ad (Trunking) 43
3.4 Resilient TCMP 46
3.5 Von Link-Aggregation zu Multi Point Link Aggregation (MPLA) 48
3.6 Router- und Layer-3-Redundanz.....50
3.7 Redundanz bei ATM 57

4 WAN- und MAN-Zugriff 61

4.1 WAN-Link-Redundanz.....63
4.2 WAN-Backup 64
4.3 WAN-Link- und Router-Redundanz 66

5 Weitere Wege zur Steigerung der Netzwerkleistung 69

5.1 Schnellere Netzwerke 69
5.2 Datenpriorisierung 73
5.3 Sicherheit und Schutz der Daten 77

6 Anforderungen an den Aufbau der aktiven Komponenten 81

6.1 Redundanz in der Hardware 81
6.2 Modulare kontra stackbare Systeme 83
6.3 Neue Hardwarekonzepte in modularen Systemen84
6.4 Neue Stackingkonzepte bei preiswerten Switches 86
6.5 Schnelle Reaktionen auf mögliche Fehler im Netzwerk.....89

7 Was sonst noch beachtet werden sollte 93

7.1 Stromversorgungen.....93
7.2 Datensicherungen 94
7.3 Datenschutz gegen Angriffe von außen 95
7.4 Service und Support 97
7.5 Redundanz um jeden Preis? 98

Stichwor tver zeichnis 99