Dr. Suppan International Institute

Der Netzwerk Insider

August 2004

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Design von „Voice-ready“ Netzen

(Fortsetzung - Juni 2004)

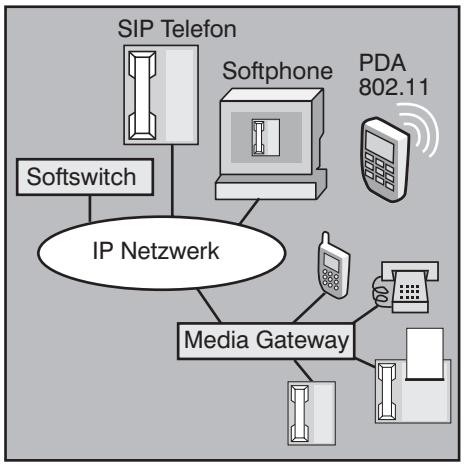
von Dipl.-Inform. Petra Borowka

Dieser Beitrag befasst sich mit den speziellen Designfragen, die für Netzwerkplanungen und Netzwerk-Redesign Projekte zu beachten sind, wenn Sprachanwendungen, insbesondere Telefonie über diese Netze betrieben werden sollen.

6. Standortübergreifende Konzepte

6.1 Dezentrales Mehr-Standort-Konzept

Ein Dezentrales Mehr-Standort-Konzept liegt bei einem minimalen Verbundbetrieb vor, dessen maximale Integration aus einem gemeinsamen Rufnummernplan und entsprechenden Call-Routing Regeln besteht, ansonsten jedoch den völlig autarken Betrieb eines Standortes mit Betreuungspersonal vor Ort vorsieht. Jeder Standort hat eine eigene – gegebenenfalls fehlertolerant ausgelegte Anlage, die je Standort von einem unterschiedlichen Hersteller sein kann. Zusatzdienste und –Anwendungen werden an jedem Standort vorgehalten, maximal wird ein Abgleich von TK-Datenbankinformationen gefahren. Die Verbindung der Standorte erfolgt über PSTN, falls kein gemeinsames IP Trunking (H.323 oder SIP) möglich ist (siehe Abbildung 6.1).



Voice Komponenten im IP Netzwerk

weiter auf Seite 12

Zweitthema

SIP bringt Bewegung in den Voice over IP Markt

(Fortsetzung - Juni 2004)

von Dipl.-Inform. Petra Borowka

Dieser Beitrag setzt ein grundsätzliches Verständnis voraus, wie IP Telefonie funktioniert und welche Basis-Protokolle und Verfahren hier zum Einsatz kommen. Für eine Einführung in Voice over IP verweisen wir auf die Netzwerk Insider vom September und November 2000. Für eine Einführung in SIP verweisen wir auf den Netzwerk Insider vom Mai 2004.

5. SIP und Sicherheit

Relevante Funktionen im Sicherheits-Umfeld sind Authentifizierung, Verschlüsselung und der Einsatz von Firewallsystemen.

5.1 Authentifizierung, Verschlüsselung

Als sichere Variante des RTP wird von der IETF das Secure RTP Protokoll (SRTP) spezifiziert (aktuell noch Draft), das Verschlüsselung der Daten mit AES (128 Bit Schlüssel), Verschlüsselung der Signalisierung mit TLS und auch Authentifizierung mittels HMAC-SHA-1 und einer Authentifizierungs-Schlüssellänge von 160 Bit definiert. Für eine detailliertere Betrachtung von Sicherheit für IP Telefonie verweisen wir auf den Beitrag „Voice Security“ im März 2004 Insider.

weiter auf Seite 5

Top-Event

Wireless LAN Forum 2004

auf Seite 5

Zum Geleit

Cisco versus Siemens: wer hat die bessere IP-Telefonie-Lösung?

auf Seite 2

Report des Monats

IP-Telefonie: Cisco versus Siemens Version 2

auf Seite 12

Zum Geleit

Cisco versus Siemens: wer hat die bessere IP-Telefonie-Lösung?

Aktuell ist die 2. Auflage unserer Top-Studie mit dem Vergleich der IP-Telefonie-Lösungen von Cisco und Siemens erschienen. Dabei wurden jetzt insbesondere die Architektur- und Leistungsmerkmale von HiPath Version 2 und Call Manager 4 berücksichtigt. An Hand eines umfangreichen Kritierienkatalogs wurden die Vor- und Nachteile beider Produktreihen heraus gearbeitet und verglichen.

Das wichtigste Ergebnis dieser umfangreichen Analyse ist allerdings nicht, wer das bessere Produkt hat (die beiden Hersteller werden dies anders sehen). Die zentrale Botschaft der 2. Auflage ist: IP-Telefonie ist an der klassischen Telefonie vorbei gezogen. Wesentliche Teile der Weiterentwicklung der Produkte aller Hersteller konzentrieren sich nur noch auf diesen Bereich. Die Qualität und Produktvielfalt, die hier mittlerweile erreicht wird, ist überzeugend. Natürlich gibt es auch vereinzelte Mängel und Features, die die Erwartungen nicht vollständig erfüllen. Nur ist dies durchaus normal und war auch bei der klassischen TK nicht anders.

Eine weitere Botschaft der Studie ist: die Architekturdetails beider Produktlinien sind so komplex, dass ein erhebliches Wissen zur optimalen Nutzung erforderlich ist. Wir waren in der optimalen Position, von den Top-Leuten beider Anbieter in die Architekturdetails eingeführt zu werden. Dies wird in der täglichen Praxis für nur wenige Unternehmen in dieser Form möglich sein. Hier kann die Studie helfen, das Leistungsspektrum beider Produkte vollständig bewerten zu können.

Wer hat jetzt das bessere Produkt?

Im Endeffekt keiner der beiden Anbieter. Vielmehr setzen beide Anbieter auf besondere Leistungsmerkmale. Siemens betont die Migration aus der klassischen TK und die Sicherung der dort getätigten Investitionen, Cisco betont den Einstieg in die neue Welt. Die Wahl, welches Produkt in einem jeweiligen Einsatzfall geeigneter ist, kann aber nicht auf diese triviale Sicht reduziert werden. In jedem Projekt wird es unerlässlich sein, die Anforderungen im Detail zu erarbeiten und mit der Leistung

der angebotenen Produkte zu vergleichen. Die in der Studie ausgearbeiteten Kriterienlisten sind ideal dazu geeignet.

Wer immer noch an der IP-Telefonie zweifelt, dem empfehle ich den Einsatz über eine sehr große geografische Entfernung hinweg. Zum Beispiel in der Kommunikation zwischen unserem Labor in Neuseeland und unserem Büro in Aachen ist die IP-Telefonie (zur Zeit noch über das Gateway von Sipgate in Düsseldorf) unschlagbar. Die Sprachqualität ist in einem Ausmaß besser als die der klassischen Telefonie, dass VOIP hier inzwischen die Basis für mehr als 90% aller Gespräche ist. Ich betone: aus qualitativen Gründen! Ein Nebeneffekt sind die niedrigen Gesprächsgebühren. Zur Zeit starten wir den Test einer Internet-Videoverbindung nach Neuseeland. Wir werden Sie auf dem Laufenden halten.

IP-Telefonie wird uns in den nächsten Jahren noch intensiv beschäftigen. Ich stehe zu unserer Prognose: in drei bis 5 Jahren ist der Wechsel in Unternehmensnetzen zu über 70% vollzogen.

Ihr
Dr. Jürgen Suppan

Report zum Thema

Neuauflage: IP-Telefonie: Cisco versus Siemens

Diese Studie analysiert die bestehenden und in der Zukunft zu erwartenden TK-Lösungen von Cisco und Siemens mit dem Fokus auf IP-Telefonie. Technische Basis dieser neuen Auflage sind jetzt auf der Cisco-Seite der Call-Manager in der Version 4.0/4.1 und auf der Siemens-Seite die HiPath 4000 Version 2.0, die HiPath 3000/5000 Version 4 sowie die aktuellen Ankündigungen zur HiPath 8000.

IP-Telefonie: Cisco versus Siemens
August 2004 - 350 Seiten
Preis: 398,-- zzgl. MwSt.

Bestellen Sie über unsere Web-Seite
www.comconsult-research.de

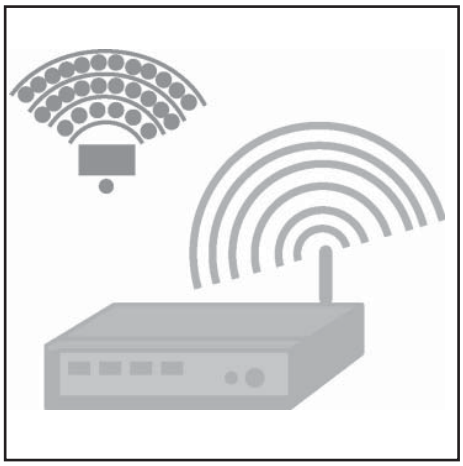
Top-Event

Wireless LAN Forum 2004

Das Wireless-LAN-Forum 2004 analysiert den Einsatz von Wireless-Netzwerken in der Praxis, stellt Planungs-Methoden gegenüber, vergleicht die heutigen und zukünftigen Wireless-Varianten, bewertet die Produkt- und Marktsituation und gibt Empfehlungen zum Betrieb und zum Trouble Shooting.

Im Einzelnen analysiert und diskutiert das WLAN-Forum 2004 folgende Themen:

- Wireless-Technologie in der Analyse
- Wireless-Varianten im Vergleich
- Abwärts-Kompatibilität
- Betrieb und Management
- Meßmethoden und Trouble Shooting
- Planungsmethoden und Auslegungsalternativen



- Voice-over-WLAN
- Roaming
- Quality of Service
- Sicherheit
- Markt- und Produktsituation
- Ausblick auf neue Wireless-Standards: IEEE 802.11n

Die Themenauswahl belegt: ein herausragender Kongress mit Top-Informationen, Analysen, Messergebnissen und Empfehlungen für die Planung und den erfolgreichen Betrieb von Wireless Netzwerken. Ein Kongress, den Sie nicht versäumen sollten. Sichern Sie sich rechtzeitig einen Platz für diese herausragende Veranstaltung.

15% Frühbucherrabatt bis 15.09.04

Wireless LAN Forum 2004

Teilnahmegebühr vom 22.11. - 24.11.04 inklusive Report „Wireless LAN Evaluierung“ innerhalb der Frühbucherphase € 1.728,-- zzgl. MwSt. (regulär € 1.988,--zzgl. MwSt.)

Teilnahmegebühr vom 22.11. - 24.11.04 ohne Report „Wireless LAN Evaluierung“ innerhalb der Frühbucherphase € 1.430,-- zzgl. MwSt. (regulär € 1.690,--zzgl. MwSt.)

Die Buchung ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden. Die Teilnahmegebühren werden mit Auslauf der Frühbucherphase fällig.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Wireless LAN Forum 2004

Ich buche den Kongress
Wireless Forum 2004
vom 22.11. - 24.11.04 in Königswinter

☐ **mit Report € 1.728,-- zzgl. MwSt.***

☐ **ohne Report € 1.430,-- zzgl. MwSt.***

*** gültig bis 15.09.2004**

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

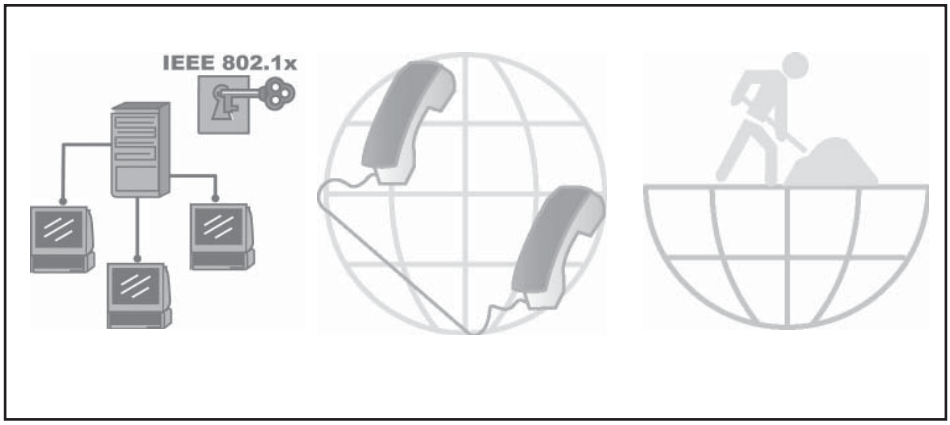
Aktuelle Sonderveranstaltungen

ComConsult Seminare jetzt wieder in der Schweiz

Auf vielfachen Wunsch unserer Kunden starten wir im Oktober wieder eine Sonderserie unserer Seminar in der Schweiz. Veranstaltungsort das Novotel Airport Messe in Zürich-Glattbrugg.

Wir haben dieses Mal wieder drei hochaktuelle Seminare mit Top-Referenten für Sie ausgewählt:

- **Sicherheit im LAN mit IEEE 802.1x**
- **IP-Telefonie evaluieren, planen, betreiben**
- **WAN-Redesign: Projektleitfaden.**



Sicherheit im LAN mit IEEE 802.1x

In der Praxis stellt sich häufiger die Aufgabe, in einem gemeinsam genutzten Netzwerk eine Trennung verschiedener Benutzergruppen, die unterschiedlichen Sicherheitsniveaus zugeordnet sind, vorzunehmen (Beispiele: Gastzugang, Trennung Industrie-/Bürobereich). Es muss also an einem geeigneten Punkt im Netz (z.B. direkt am Netzwerk-Port des Access-Switches) geprüft werden, welche Rechte mit dem Zugang verbunden sein sollen. Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1x, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes.

IP-Telefonie evaluieren, planen, betreiben

Dieses 3-tägige Seminar evaluiert die Technologie und die verfügbaren Produkte gegenüber den in der Praxis bestehenden Anforderungen. Es vermittelt die technischen Grundlagen, beschreibt die Arbeitsweise wichtiger Produkte, analysiert typische Nutzungsformen an Fallbeispielen und gibt eine Prognose für die Marktsituation und weitere Entwicklung. Die Konkurrenz-Situation zwischen CISCO und Siemens inklusive des Leistungsumfangs der Produkte wird an Hand der Ergebnisse einer hochbrisanten Studie bewertet. An Beispielen wird erläutert, welche Schritte für die erfolgreiche Implementierung von IP-Telefonie erforderlich sind.

WAN-Redesign: Projektleitfaden

Die standortübergreifende Kommunikation gewinnt zunehmend an Bedeutung. Dabei waren die Möglichkeiten der Gestaltung einer WAN-Lösung noch nie so vielfältig. Das Redesign bestehender WANs bietet somit die Vorteile einer deutlich erhöhten Leistung bei gleichzeitigen massiven Einsparpotenzialen. Dieses 3-tägige Seminar basiert auf den jahrelangen Erfahrungen führender Experten im Bereich der Konzipierung und Planung von WAN-Lösungen. Die Referenten kommen aus der Praxis und vermitteln Ihnen ihre Erfahrungen sowohl bei der überprüfbaren Übertragung von Kommunikationsdiensten an Provider als auch beim Aufbau eigener Infrastrukturen im WAN-Bereich.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Schweiz

Ich buche das folgende Seminar in Zürich-Glattbrugg:

- ☐ **Sicherheit im LAN mit IEEE 802.1x**
  25.10. - 26.10.04 (Preis € 1.490,--)
- ☐ **IP-Telefonie evaluieren, planen, betreiben**
  25.10. - 27.10.04 (Preis € 1.890,--)
- ☐ **WAN-Redesign: Projektleitfaden**
  25.10. - 27.10.04 (Preis € 1.890,--)

☐ Buchen Sie für mich ein Hotelzimmer

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

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

Zweitthema

Session Initiation Protokoll bringt Bewegung in den Voice over IP Markt

Fortsetzung von Seite 1

Dipl. Inform. Petra Borowka leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

5.2 Firewall und NAT Traversal

SIP hat zwei unangenehme Eigenschaften. Die erste ist die aller RTP Anwendungen: Es verwendet keine well-known Ports, sondern die Portnummer wird beim Anruf-Aufbau ausgehandelt. Lediglich die Signalisierung läuft über die Ports 5060 (SIP über UDP / TCP) und 5061 (SIP über TLS). Daher können die Ports für den Media Stream nicht vorab im Firewall freigeschaltet werden, sondern müssen mittels Firewall-Überwachung des Sessionaufbaus als aktuell gültige Portnummern erkannt, freigeschaltet und nach Firewall-Überwachung des Sessionabbaus wieder geblockt werden.

Die zweite unangenehme Eigenschaft ist das Einfügen der IP Absender- und Zieladressen als Informations-Parameter in den SIP Header. Dies führt bei Einsatz von NAT dazu, dass im SIP Header die ursprüngliche, vielfach private IP Adresse des Absenders im SIP Header steht, während ein oder mehrere kaskadierte NAT-Komponenten für den IP Header ganz andere Adressen generiert haben (siehe Abbildung 5.1). Trägt der Empfänger einer SIP Nachricht treu und brav die den Info-Parametern entnommene IP Absenderadresse als IP Zieladresse ein, so erreicht die Antwort ihr Ziel nicht, da jenseits der NAT-Komponente, also im öffentlichen Netz, die unternehmensintern genutzte Adresse gar nicht bekannt oder sogar (bei privaten Adressen) nicht einmal routbar ist. Die Situation wird noch dadurch kompliziert, dass es verschiedene NAT-Typen gibt (full-cone, restricted cone, port-restricted cone und symmetric bzw. stateful inspection), die Firewall-übergreifende Sessions unterschiedlich restriktiv handhaben.

Aktuell verfügbare Lösungen können in folgende Kategorien unterteilt werden:

- Application Layer Gateways (ALG)
- Stateful Inspection Firewalls mit Deep Packet Inspection (DPI)
- Firewalls mit SIP Proxy-Dienst (B2BA Back-to-Back User Agent)
- Umgehung des Firewall und Nutzung von VPN / IPsec Tunneln oder Verschlüsselung

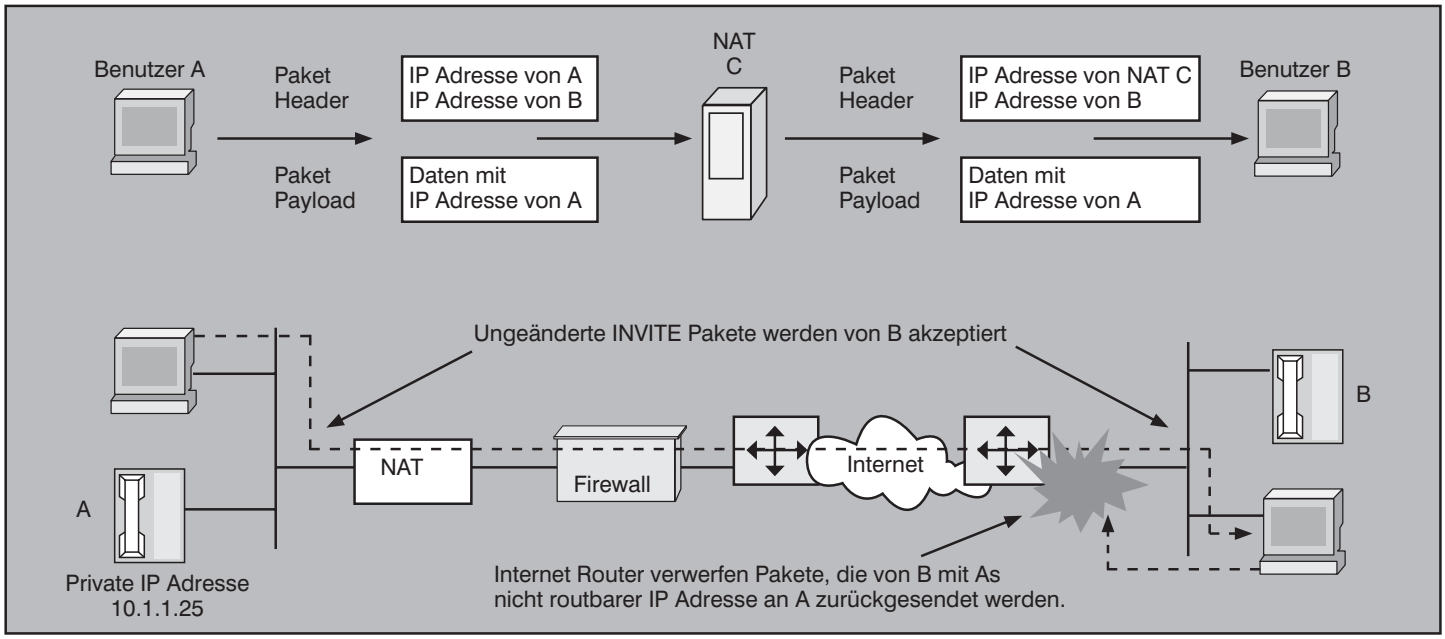


Abbildung 5.1: SIP und das Adressproblem bei NAT

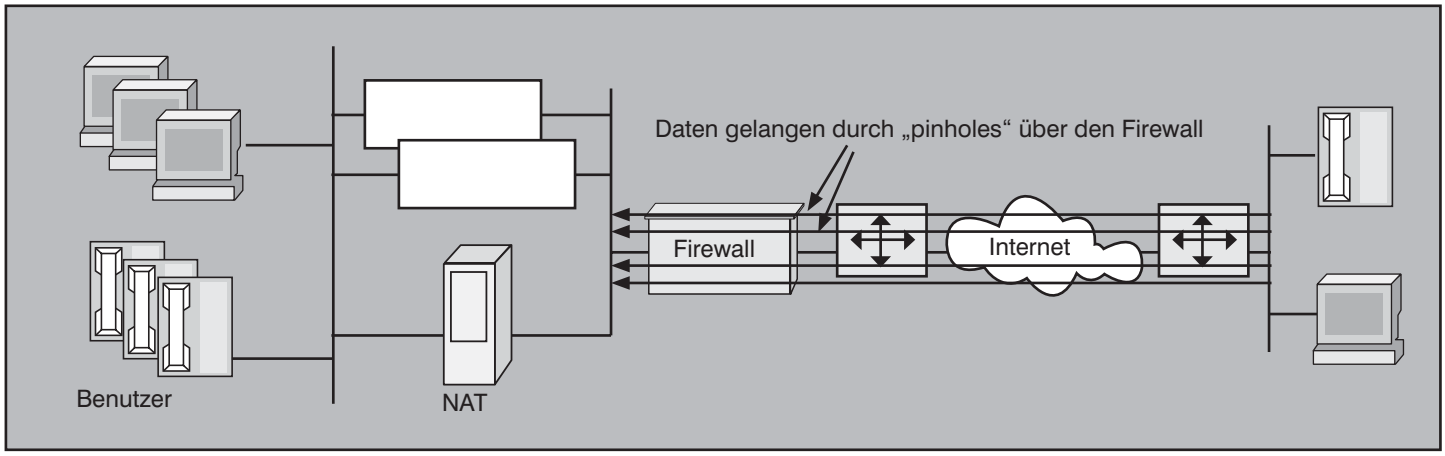


Abbildung 5.2: SIP über ALGs

ALG‘s bearbeiten das Paket und öffnen Pinholes im Firewall, um den Voice und Video Verkehr zu ermöglichen (siehe Abbildung 5.2). Proxies können je nach Konfiguration als Parallelschaltung zu Firewalls eingesetzt werden (siehe Abbildung 5.3). Beide Lösungen müssen einen SIP Registrar integriert haben, um die korrekte Weiterleitung von Sprach- und Videopaketen sicherzustellen.

Weitere Details zu der genannten Problematik und zu einigen aktuell verfügbaren Lösungen sind im Beitrag „Übertragung von SIP über Firewalls“ des Insiders vom April 2004 beschrieben. Nachfolgend gehen wir zur Ergänzung dieser Thematik kurz auf die derzeit bei der IETF diskutierten Standard-Ansätze ein:

- STUN (Simple Traversal of UDP through NAT, RFC 3489)
- TURN (Traversal Using Relay NAT)
- ICE (Interactive Connectivity Establishment)
- NSIS (Next Steps In Singnaling)

STUN

STUN ist ein Client-Server Protokoll, der STUN Client kann seinen STUN Server über DNS Srv Record finden. Der STUN Server befindet sich immer im öffentlichen Netzwerk (Provider eines Dienstes, der STUN erfordert, sollten einen STUN Server betreiben); sein well-known Port ist 3478 und kann daher auf einem Firewall freigeschaltet werden. STUN Clients senden Requests, der STUN Server beantwortet diese mit Responses. Zuerst läuft eine Shared Secret Request / Response Sequenz über TLS (liefert Username und Einmal-Passwort zurück) ab, dann eine Binding Request / Response Sequenz über UDP (liefert das extern angekommene NAT Mapping zurück). Das Shared Secret sichert Authentifizierung und Integritätsprüfung; das Einmal-Passwort wird für genau eine einzelne darauf folgende Binding Request / Response Sequenz genutzt. Bei Empfang des Binding Requests am Server kann der Request mehrere NAT/FW durchlaufen haben. Übersichts-Grafiken zeigen Abbildung 5.4 und Abbildung 5.5.

TURN

TURN (bisher nur als Draft) ist als eine „last resort“ Lösung gedacht, wenn STUN nicht funktioniert, was bei einigen speziellen NAT-Konfigurationen der Fall ist. Syntax und Operation von TURN sind wie bei STUN (beides kann auf demselben System laufen). TURN ist ebenfalls ein Client/Server Protokoll, der Server arbeitet als Relay zwischen dem Client und NAT/FW Systemen (siehe Abbildung 5.6). TURN liefert dem Client eine Transport Adresse (IP Adr. + Portnummer), mit der er zu einem einzelnen Peer System kommunikationsfähig ist. Der TURN Srver kann jedoch von einem Client nicht genutzt werden, um selbst Pakete vom Client über den TURN Server zu einem Zielhost zu senden, da der Server die Adresse blockt (Lock Down), sobald ein Host Pakete an diese Adresse sendet.

TURN fordert Authentifizierung und Autorisierung mittels Client digest über TLS. Das Resultat ist ein Einmal-Passwort, welches in einem darauf folgenden ALLOCATE Request genutzt wird (Schutz gegen Eavesdropping und M-i-M); Das ALLOCATE selbst läuft NICHT über TLS. Zum Schutz vor Angriffen durch authentifizierte Benutzer ist eine obere Grenze der Anzahl gleichzeitig offener Einmal-Passwörter eines einzelnen Benutzers konfigurierbar (Default: 5 bis 10); dies verhindert ein Fluten des TURN Servers mit ALLOCATE Requests. Zum Schutz gegen Fluten mit Da-

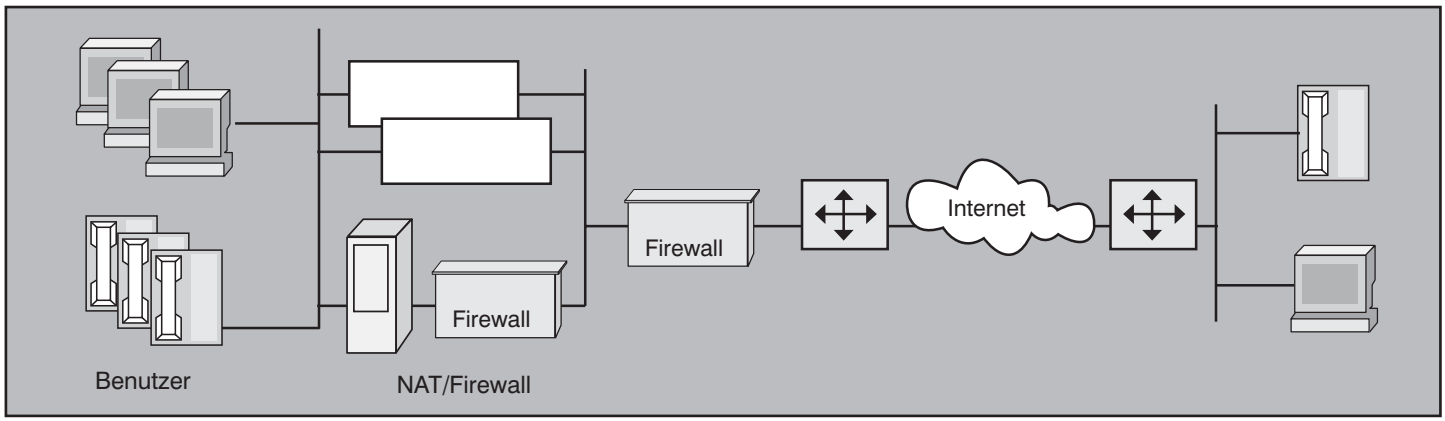


Abbildung 5.3: SIP über Proxies

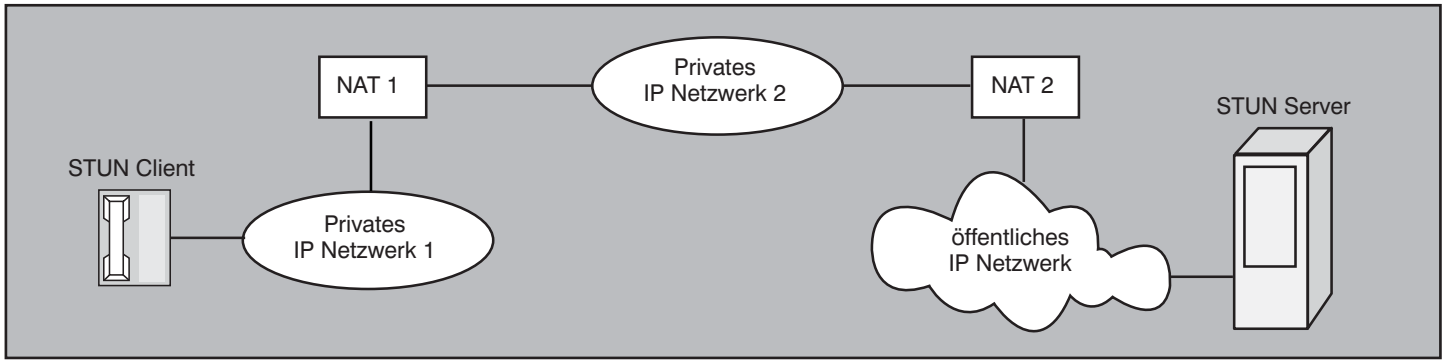


Abbildung 5.4: STUN Szenario

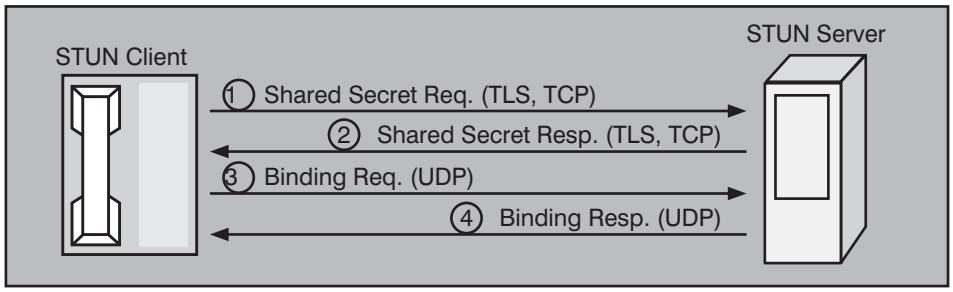


Abbildung 5.5: Adress Binding mit STUN

ten ist eine obere Grenze je Benutzer für die genehmigte Bandbreite konfigurierbar. Hierfür teilt der Client dem Server die erwartete Bandbreite der Session mit (BANDWIDTH Attribut).

Hinsichtlich der Transport-Adresse kann eine „gerade“, „ungerade“ sowie „die nächsthöhere“ Portnummer angefragt werden (TRANSPORT PREFERENCES Attribut). Für Redundanz-Lösungen kann ein TURN Server ein Redirect zu einem anderen Server an einen TURN Client (ALTERNATE-SERVER Attribut) senden.

Ein Rufaufbau läuft folgendermaßen ab:

1. Der Client findet einen TURN Server (Discover)
   1. Manueller Eintrag
   2. DNS Srv Record
2. Es erfolgt gegenseitige Authentifizierung und Integritäts-Prüfung unter Verwendung eines **Shared Secret**
3. Der Client sendet einen ALLOCATE Request
   1. Der TURN Server merkt sich die ursprüngliche Transport Adresse des Client (SA) und liefert per ALLOCATE Response eine public Adresse zurück (PA); der TURN Server muss sicherstellen, dass alle Pakete an PA an ihn geroutet werden
   2. Sobald Daten mit Ziel „PA“ ankommen, macht der TURN Server ein Lock Down auf die PA Adresse
      1. VOR einem Lock Down kann der Client mittels SEND über den TURN Server senden
4. Der TURN Server merkt sich die Remote Transport Adresse (RA)
5. Der TURN Server leitet als **Relay** die Daten an SA weiter
6. Falls ein Host ≠ RA an PA sendet, erfolgt **Enkapsulierung in TURN Header;** dies bietet einen gewissen Schutz gegen DoS

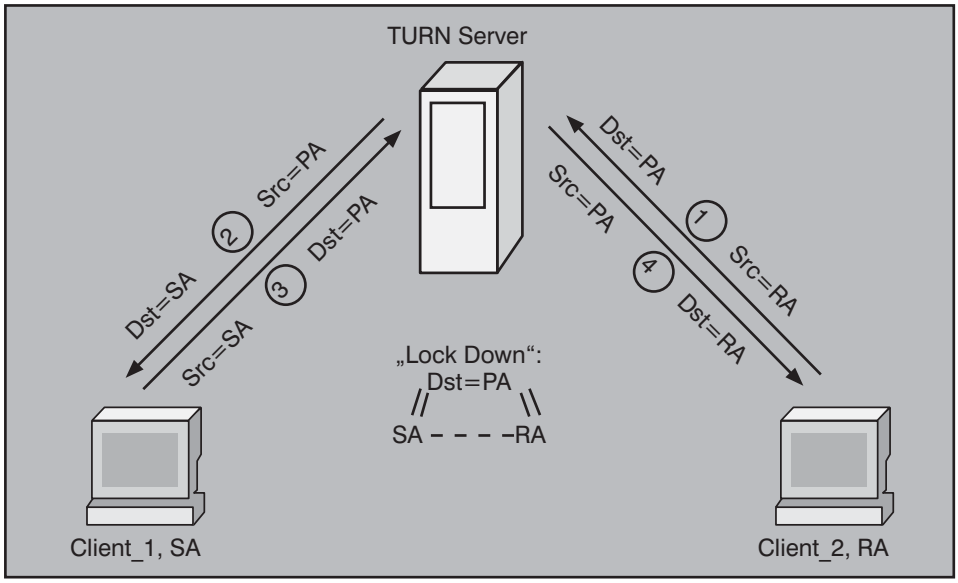


Abbildung 5.6: Call-Aufbau mit TURN

STUN Server sind z.B. von SNOM (www.snom.com) und als Open Source über Vovida (www.vovida.org) erhältlich.

ICE

ICE (bisher nur als Draft) spezifiziert eine Erweiterung der SIP Signalisierung mittels SDP Extensions. Hierbei wird folgende Annahme getroffen: Der Client weiß nicht, in welchem Adressbereich und hinter welchen NAT/FW Komponenten sich sein Peer befindet. Der Peer, der den Call startet, heißt Initiator; der Peer, der den Call annimmt, heißt Responder.

ICE kann seinerseits STUN und TURN zur Auswahl der möglichen Adressen nutzen, meistens in folgender Reihenfolge

1. direkt gelernte Adressen
2. mit STUN gelernte Adressen
3. mit TURN gelernte Adressen

Session-Aufbau mit ICE

1. Vor Beginn einer Session bildet der Initiator für alle Protokolle alle Port/Adress-Kombinationen, von allen Adressbereichen, in denen er liegt. Dies führt zur Bildung aller möglichen lokalen Empfangs-Adressen.
2. Ggf. unter Nutzung von STUN, TURN, RSIP, VPN
3. Initiator startet einen lokalen STUN Ser-

ver für jede IP/Port Kombination
4. Initiator sendet eine INITIATE Nachricht an den Responder, mit STUN Username und Passwort für den Responder, für jede IP/Port Kombination
5. Responder sendet STUN Requests an jede IP/Port Kombination (KEINE STUN Flags gesetzt)
6. Responder sendet ACCEPT Nachricht, diese enthält alle unilateral erkennbaren Adressen zzgl. aller über STUN erhaltenen Adressen
7. Initiator prüft Verbindungsfähigkeit zu allen übermittelten Adressen (ggf. wurden in den STUN Antworten neue potenzielle Empfangsadressen entdeckt)
8. Initiator sendet neue Adressen per MODIFY Nachricht an den Responder (ab Schritt 4. rekursiv)

NSIS

Eine zweite Richtung zur Lösung des SIP - NAT/FW Problems versucht die NSIS Arbeitsgruppe (Next Steps in Signaling) zu entwickeln. Hier ist die Idee, dass die NAT/FW Komponenten in die Signalisierung einbezogen werden und die von ihnen vorgenommenen Änderungen in den Header Parametern eintragen. Diese Ansätze sind jedoch noch ganz am Anfang des Standardisierungsprozesses und führen zu komplexeren Lösungen, da alle NAT/FW Komponenten auf dem Weg zwischen zwei Peers diese Signalisierung unterstützen müssen. Wir gehen daher an dieser Stelle nicht weiter auf die NSIS Modelle ein.

5.3 Fünf Mythen über die Migration zu SIP

Nachfolgend fassen wir nochmals einige im Zusammenhang mit SIP-Einsatz häufig auftauchenden Aussagen zusammen und bewerten diese.

Mythos 1:
Ich muss für SIP mein ganzes Netzwerk ersetzen.

Das ist nicht notwendig. Der kritische Punkt im Netzwerk ist gegebenenfalls der Firewall bzw. die Lösung des Problems, wie SIP-Kommunikation über den Firewall hinweg lauffähig gemacht wird. Dies kann durch eine Hochrüstung des existierenden Firewalls auf „SIP-aware“ oder mit einem separaten neuen Firewall erreicht werden.

Mythos 2:
Ich kann meinen aktuellen Firewall „SIP-fähig“ machen.

Es ist nicht möglich, jeden beliebigen Firewall SIP-fähig zu machen. Insbesondere wenn er eine Architektur hat, die das Einbringen neuer Protokolle nicht grundsätzlich ermöglicht. Aktuell gibt es nur wenige SIP-fähige Firewall-Produkte (z.B. Aceme, Checkpoint, Cisco, InGate, Jasomi, Kagoor, NetScreen, WatchGuard).

Mythos 3:
SIP-Kommunikation funktioniert nicht über einen Firewall hinweg.

Falsch. Firewalls blocken unerwünschten Zugang und Datentransfer, besonders in eingehender Richtung. Die Adressknappheit hat zusätzlich zum Einsatz von NAT geführt, um private Adressen nutzen zu können.

Dies führt zu zwei Problemen:
- Firewalls lassen SIP normalerweise nicht durch, da der Port für den Mediastream keine well-known Adresse hat und somit nicht vorab bekannt ist. Aus Sicherheitsgründen kann keine, insbesondere keine große Portrange als nutzbarer Pool freigeschaltet werden.
- Die private Adresse des SIP Endgeräts ist im öffentlichen Netz nicht routbar und auch nicht bekannt.

Nach dem heutigen Stand ist eine typische Lösung der Einsatz eines Firewalls mit integriertem SIP ALG, SIP Proxy und SIP Registrar. Damit versteht der Firewall genügend von SIP, um die notwendigen Ports zu öffnen (Pinholing) und auch wieder zu schließen, die Nachrichten an die korrekte IP Adresse weiterzuleiten und gegebenenfalls die notwendigen Änderungen im SIP Header vorzunehmen. Zusätzlich können mit einem SIP Proxy SIP Signalisierung und IM mittels TLS verschlüsselt werden, um die Inhalte dieser Nachrichten zu verbergen. Somit ist der Firewall für gewünschten SIP-Transfer durchlässig, blockt aber weiterhin nicht-autorisierten SIP- und sonstigen Transfer.

Mythos 4:
Mein Netzwerk ist unsicher, wenn ich SIP nutze.

Bei Nutzung einer Firewall, um den SIP-Transfer zu steuern, und eines SIP Registrar, der ein- und ausgehenden SIP-Verkehr steuert und ausschließlich zu autorisierten Endgeräten weiterleitet, stimmt die Aussage nicht. Bei Umgehen der Firewall für SIP-Kommunikation und gleichzeitig Weglassen alternativer Sicherheitsfunktionen wie VPN oder TLS-Tunnel stimmt die Aussage: Sie haben mit SIP ein offenes Scheunentor installiert.

Mythos 5:
Die funktionsfähige Konfiguration eines SIP-fähigen Firewalls ist nahezu unmöglich.

Dies mag für Firewalls mit DPI und IPS zutreffen, gilt aber nicht allgemein. Es gibt sogar Firewalls mit GUI!

6. Offene Probleme

So zu tun, als sei der Einsatz von SIP etablierte Technik, wäre eine Vorspiegelung falscher Tatsachen. Noch gibt es eine Reihe von Arbeitpunkten, die auf der To Do Liste der SIP-Bäcker stehen:

NAT / Firewall

Für die Kommunikation mit SIP über FW/NAT Komponenten hinweg muss ein Standard verabschiedet werden, der möglichst 90 bis 95 Prozent der FW/NAT Konfigurationen abdeckt, die verbleibenden 5% können dann mit herstellereigenen Lösungen gehandhabt werden.

Notfallrufe

Notfallrufe sind als besonders wichtig zu behandeln und unterliegen den Telekom Regulierungsbehörden. Diese haben insbesondere folgende Regelungen getroffen, die auch mit SIP erfüllt werden müssen:
- Der Notruf muss immer an den lokal zuständigen Notdienst erfolgen. Dies erfordert Kenntnis über die geografische Lokation des Benutzers, der den Notruf tätigt. Hier hat SIP Schwierigkeiten, da über die IP Adresse nicht immer der geografische Ort festgestellt werden kann (z.B. dynamische Adresspools von Einwahl-Providern).
- Der Anrufer muss für den Notdienst seinen Aufenthaltsort identifizieren, damit z.B. eine Ambulanz an die richtige Stelle geschickt werden kann. Hierfür müsste der SIP Header für Notrufe um „Caller Location“ Felder erweitert werden. Aktuell gibt es eine IETF Arbeitsgruppe GEOPRIV, die sich um die Verwaltung solcher Informationen mit DHCP als langzeitfristige Lösung kümmert. Diese DHCP Informationen könnten dann wiederum von SIP abgefragt und zweckdienlich verwendet werden.
- Notfallrufe müssen mit hoher Priorität behandelt werden. Auch hier wird gerade ein RFC erarbeitet (draft-ietf-sip-resource-priority-01), der weitere SIP Header spezifiziert.
- Notrufe müssen auch von Benutzern abgesetzt werden können, die nicht im Netz authentifiziert sind, z.B. über Mobiltelefone und Roaming. Es gibt keinen Standard dafür, eine solche Kommunikation zu erlauben und es ist

Session Initiation Protokoll bringt Bewegung in den Voice over IP Markt

insbesondere nicht geklärt, woher das Mobiltelefon wissen soll, welche lokale Nummer es anwählen muss, da es ohne Authentifizierung keine Information über die lokalen Konfigurationsparameter erhalten kann.

Kompatibilität

Die allgemeine Kompatibilität von SIP Implementierungen muss noch verbessert werden. Von einem beliebigen Mix und Match vergleichbar mit Ethernet NIC's und Switches kann noch keine Rede sein.

Zukunftssicherheit

Wie bei jeder jungen Technologie gibt es etablierte Hersteller, die noch nicht richtig auf den Zug aufgesprungen sind, und Startups mit innovativen Lösungen, deren Überlebensfähigkeit nicht abzuschätzen ist. Möglicherweise werden einige letztere von einigen ersteren aufgekauft, aber auch hierzu lassen sich derzeit keine seriösen Aussagen treffen. Eine Produktentscheidung unterliegt daher heute noch einer hohen Marktdynamik mit überdurchschnittlich großen Unwägbarkeiten.

Fazit

SIP hat in den letzten zwei Jahren zunehmend an Marktbedeutung gewonnen und steht heute deutlich mehr im Entwicklungs-Fokus als H.323. Es wird nicht nur im Carrierumfeld für Softswitches implementiert, sondern inzwischen sind auch SIP-Telefone für Endanwender und private Nutzer verfügbar. Die Adaption von SIP durch Microsoft stellt einen weiteren Push-Faktor dar. Alle etablierten Hersteller von Enterprise TK-Lösungen haben ihre Produkte um Multimedia- und Presence-Dienste auf SIP-Basis erweitert oder angekündigt, dies zu tun.

Es gibt viele IETF Aktivitäten für SIP Feature-Erweiterungen wie die SIPPING Arbeitsgruppe (Session Initiation Proposal INvestiGation), Drafts für weitere SIP Features („Leistungsmerkmale"), SIP-Mapping mit anderen Signalisierungen wie QSIG, ISUP, Nutzung des Stream Control Transmission Protocol als Transport Layer.

Die verfügbaren Produkte sind noch jung und haben bestenfalls einen mittleren Reifegrad (dies gilt für die am längsten verfügbaren SIP Server, noch nicht für SIP Telefone), daher muss die herstellerübergreifende Kompatibilität noch verbessert werden.

SIP wird jedoch im Zusammenhang mit integrierten Arbeitsoberflächen für TK, Kollaboration, web-basierte Personalisierung und Anwesenheits-Funktionen, ggf. ergänzt mit Video-Integration, definitiv seinen Platz in Enterprise TK-Lösungen einnehmen.

Das Potenzial, mit SIP und der Microsoft/Intel Marktmacht eine „Plug & Play"Telefonnutzung zu etablieren, die aufgrund geänderter Arbeitsabläufe die klassische Vielfalt von Enterprise Leistungsmerkmalen weder braucht noch nutzt, sollte nicht unterschätzt werden.

Abkürzungen

ADS	Active Directory Service
ALG	Application Layer Gateway
AV	Audio / Video
B2BUA	Back to Back User Agent
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DPI	Deep Packet Inspection
DPNSS	Digital Private Network Signalling System
DSL	Digital Subscriber Line
FW	Firewall
GSM	Global System for Mobile Communication
GUI	Graphical User Interface
GW	Gateway
ICE	Interactive Connectivity Establishment
IETF	Internet Engineering Task Force
IM	Instant Messaging
IPS	IP Phone Services (Cisco)
ISP	Internet Service Provider
ITSP	Internet Telephony Service Provider
JPEG	Joint Photographic Experts Group
LCS	Live Communication Server
MCP	Multimedia Communication Portfolio (Nortel)
MCDN	Meridian Customer Defined Network (Nortel)
NAT	Network Address Translation
NSIS	Next Steps In Singnaling
PBX	Private Branch eXchange
PDA	Personal Digital Assistant
PSTN	Public Switched Telephony Network
PUID	Passport User ID's
QSIG	Q-interface SIGnalling protocol
RTC	Real-Time Communication
RTP	Real-time Protocol
SIP	Session Initiation Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
STUN	(Simple Traversal of UDP through NAT
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TURN	Traversal Using Relay NAT
UDP	User Datagram Protocol
VPN	Virtual private Network

Links

www.sipcenter.com
www.sipforum.org

Literatur

RFC 3725,BCP 0085 / Rosenberg, J. Peterson, H. Schulzrinne, G. Camarillo: Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP); April 2004

RFC 3680 / J. Rosenberg: A Session Initiation Protocol (SIP) Event Package for Registrations; March 2004

RFC 3666, BCP 0076 / A. Johnston, S. Donovan, R. Sparks, C. Cunningham, K. Summers: Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows; December 2003

RFC 3665, BCP 0075 / A. Johnston, S. Donovan, R. Sparks, C. Cunningham, K. Summers: Session Initiation Protocol (SIP) Basic Call Flow Examples; December 2003

RFC 3608 / D. Willis, B. Hoeneisen: Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration; October 2003

RFC 3581 / J. Rosenberg, H. Schulzrinne: An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing; August 2003

RFC 3578 / G. Camarillo, A. B. Roach, J. Peterson, L. Ong: Mapping of Integrated Services Digital Network (ISDN) User Part (ISUP) Overlap Signalling to the Session Initiation Protocol (SIP); August 2003

RFC 3515 / R. Sparks: The Session Initiation Protocol (SIP) Refer Method; April 2003

RFC 3486 / G. Camarillo: Compressing the Session Initiation Protocol (SIP); February 2003

RFC 3485 / M. Garcia-Martin, C. Bormann, J. Ott, R. Price, A. B. Roach: The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp); February 2003

RFC 3428 / B. Campbell, Ed., J. Rosenberg, H. Schulzrinne, C. Huitema, D. Gurle: Session Initiation Protocol (SIP) Extension for Instant Messaging; December 2002

RFC 3427, BCP 0067 / A. Mankin, S. Bradner, R. Mahy, D. Willis, J. Ott, B. Rosen: Change Process for the Session Initiation Protocol (SIP); December 2002

RFC 3420 / R. Sparks: Internet Media Type message/sipfrag; November 2002

RFC 3398 / G. Camarillo, A. B. Roach, J. Peterson, L. Ong: Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping; December 2002

RFC 3372, BCP 0063 / A. Vemuri, J. Peterson: Session Initiation Protocol for Telephones (SIP-T): Context and Architectures; September 2002

RFC 3361 / H. Schulzrinne: Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers; August 2002

RFC 3327 / D. Willis, B. Hoeneisen: Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts; December 2002

RFC 3326 / H. Schulzrinne, D. Oran, G. Camarillo: The Reason Header Field for the Session Initiation Protocol (SIP); December 2002

RFC 3323 / J. Peterson: A Privacy Mechanism for the Session Initiation Protocol (SIP); November 2002

RFC 3321 / H. Hannu, J. Christoffersson, S. Forsgren, K.-C. Leung, Z. Liu, R. Price: Signaling Compression (SigComp) - Extended Operations; January 2003

RFC 3320 / R. Price, C. Bormann, J. Christoffersson, H. Hannu, Z. Liu, J. Rosenberg: Signaling Compression (SigComp); January 2003

RFC 3319 / H. Schulzrinne, B. Volz: Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers; July 2003

RFC 3312 / G. Camarillo, Ed., W. Marshall, Ed., J. Rosenberg: Integration of Resource Management and Session Initiation Protocol (SIP); October 2002

RFC 3311 / J. Rosenberg: The Session Initiation Protocol (SIP) UPDATE Method; October 2002

RFC 3265 / A.B. Roach: Session Initiation Protocol (SIP)-Specific Event Notification; June 2002

RFC 3264 / J. Rosenberg, H. Schulzrinne: An Offer/Answer Model with Session Description Protocol (SDP); June 2002

RFC 3263 / J. Rosenberg, H. Schulzrinne: Session Initiation Protocol (SIP): Locating SIP Servers; June 2002

RFC 3262 / J. Rosenberg, H. Schulzrinne: Reliability of Provisional Responses in Session Initiation Protocol (SIP); June 2002

RFC 3261 / J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler: SIP: Session Initiation Protocol; June 2002

RFC 3050 / J. Lennox, H. Schulzrinne, J. Rosenberg: Common Gateway Interface for SIP; January 2001

RFC 2976 / S. Donovan: The SIP INFO Method; October 2000

RFC 2848 / S. Petrack, L. Conroy: The PINT Service Protocol: Extensions to SIP and SDP for IP Access to Telephone Call Services; June 2000

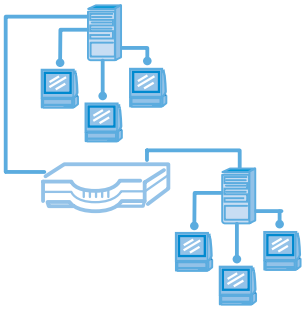
RFC 2806 / A. Vaha-Sipila: URLs for Telephone Calls; April 2000

Session Initiation Protocol-SIP, Launching the IP communications Revolution, Alcatel, July 2003

Daugherty Gordon: MXM: SIP Support, VCON, October 2002

Understanding SIP Servers, RADVISION Ltd., 2002

Internetworking
optimales Netzwerk-Design
mit Switching und Routing



13.09. - 17.09.04 in Aachen

Dieses Seminar vermittelt dem Einsteiger in 5 Intensiv-Tagen den erfolgreichen Einsatz der wesentlichen Technologien zur Strukturierung und Gestaltung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom Switching über Redundanz-Verfahren bis hin zu Spezialthemen wie VLAN, VPN, QoS, Multicast-Betrieb abgedeckt. Es werden sowohl die notwendigen theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt. Durch Fallstudien erhält der Teilnehmer verschiedenste für ihn in der Praxis umsetzbarer Informationen. Gruppen-Übungen mit Planungsbeispielen vermitteln Tipps und Tricks aus der Praxis.

Referentin: Dipl.-Inform. Petra Borowka
Preis: € 2.290,- zzgl. MwSt.

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

Studie des Monats

NEU ÜBERARBEITETE VERSION IP-Telefonie: Cisco versus Siemens

Die erste Auflage dieser Studie, die noch auf den Vorgänger-Versionen dieser beiden Produkte beruht, hat im Markt extreme Resonanz erzeugt. Eine derartig umfassende Gegenüberstellung der IP-Telefonie-Produkte dieser beiden Hersteller hat es bisher nicht gegeben, sie ist einzigartig und naturgemäß kontrovers. Jetzt wurde die Studie neu aufgelegt, um die gerade auf den Markt gebrachten neuen Versionen beider Hersteller zu evaluieren. Im Folgenden lesen Sie einen Auszug aus diesem Technologie-Report.

1.1 CallManager

Die Cisco-Lösung war von Anfang an als Softswitch konzipiert. Der Softswitch heißt CCM (Cisco CallManager) und wird auf der Basis von Windows 2000 (früher NT 4.0) betrieben. Er nimmt im Wesentlichen Funktionen eines Gatekeepers wahr: Verwaltung, Steuerung und Statusabfrage der angebundenen Telefon-Endgeräte.

Die IOS-Gatekeeper (z.B. auf Cisco-Routern) übernehmen die Funktion der Bandbreiten-Limitierung zum WAN hin sowie das Call Routing und die Call Admission bei clusterübergreifenden Verbindungen, die laut ITU-T ebenfalls dem Gatekeeper zugeordnet sind. Insofern sind, insbesondere bei Betrieb mehrerer Cluster, Teile der ITU-T Gatekeeper-Funktionalität auf den IOS-Gatekeeper ausgelagert.
...

Clustering / Anlagenverbund

Bis zu acht CallManager Server können lastverteilt und mit jeweils gegenseiti-gem Backup (Definition eines Clients auf einem Primary und einem Backup CallManager) zu einem Cluster verschaltet werden. Zusätzlich sind dann noch zwei CallManager TFTP-Server (Publisher) für die Konfigurationsdatenbank zu rechnen, eventuell zusätzliche dedizierte Music-on-Hold-Server, Datenbank Server, TFTP-Server und CTI-Manager bis zu einem Maximum von 20 Servern je Cluster.

Bei dem Backup-TFTP-Server muss der CallManager Service deaktiviert werden, so dass sich Telefone nicht an ihm registrieren können, denn sonst würde der Backup-TFTP-Server sämtliche Konfigurationsdaten des Clusters erhalten. Als Signalisierung innerhalb des Clusters wird SCCP zwischen den CallManagern und zwischen CallManager und Telefon benutzt.

Bei einer praxisnahen Kalkulation von 1.500 bis 2.000 IP-Geräten je CallManager ergibt sich eine Gesamtzahl von 12.000 bis 16.000 IP-Geräten je Cluster.

Normalerweise sollte sich ein Cluster innerhalb eines LANs oder eines MANs (d.h. Datenraten oberhalb 100 Mbit/s, limitierte Kaskadierung von Netzkompo-nenten) befinden. Wird ein Cluster über WAN vernetzt, empfiehlt Cisco, in je-dem Fall QoS-Funktionen zu aktivieren. Für den Fall, dass an einem Standort nur ein CallManager betrieben wird, der aber dennoch mittels Backup abzusi-chern ist, muss eine Failover-Schaltung über WAN zu einem anderen Standort konfiguriert werden. Im Fehlerfall läuft dann die komplette Signalisierung und auch Statusabfrage über WAN. Eine Alternative ist hier die Einrichtung einer remote Fehlerumschaltung mit der SRST-Funktion (Survivable Remote Site Te-lephony) des IOS-Gatekeepers auf einem Cisco-Router. Bei Standorten, die ganz ohne eigenen CallManager betrieben werden, läuft die Signalisierung auch im Normalfall über WAN. Für die Bandbreitenkontrolle (Call Admission Control) ist dann im Regelfall eine Funktion zu aktivieren, die „Locations“ heißt. Sie benötigt mit G.711 die Reservierung von mindestens 80 kbit/s, mit G.729 mindestens 24 kbit/s auf der WAN-Verbindung. Aktuell unterstützt der CallMa-nager mit „Locations“ bis zu 500 Standorte.
...

Fehlertoleranz mit SRST

In Standorten ohne eigenen CallManager bietet SRST (Survivable Remote Site Telephony) eine eingeschränkte Redundanz-Funktionalität. SRST läuft auf einem Cisco Router unter IOS. Im Normalfall registrieren sich die Endgeräte am zentralen CallManager, die Signalisierung verläuft über das WAN hinweg zwischen Endgerät und CallManager. Ist dieser aufgrund von WAN- oder Systemstörungen nicht mehr erreichbar, registrieren sie sich lokal auf dem Router. Der Router erfragt von den Endgeräten ihre Konfiguration und baut sich so eine eigene Konfigurations-Datenbank auf. Wird der CallManager wieder erreichbar, erfolgt automatisch eine Umregistrierung der Endgeräte auf den CallManager, der Router löscht die eigene Konfigurationsdatenbank. Ein Beispiel-Szenario zeigt Abbildung Abbildung 1.

1.2 Die HiPath-Produktlinien

1.2.1 HiPath 4000

Die HiPath 4000 mit dem proprietären Echtzeit-Betriebssystem RMX stellt zur-zeit das Flaggschiff der modularen IP-fähigen Anlagen dar.
...

Die aktuelle Software-Version ist 2.0. Eine Hochrüstung von v1.0 nach v2.0 ist für HiPath 4300 und 4500 Systeme möglich (nicht 4100. Für die Hochrüstung sind folgende Alternativen gegeben, in der genannten Reihenfolge mit jeweils steigenden Kosten:

- Reine Hochrüstung der Software, Beibehaltung der v1.0 CPU und v1.0 Gateway-Baugruppen. In diesem Fall sind die Feature-Erweiterungen von v2.0 nutzbar, soweit sie nicht an die neue Gateway-Hardware gebunden sind. Die BHCC Systemleistung bleibt die der v1.0 CPU.

- Hochrüstung der Software auf v2.0 und Einsatz der neuen cPCI CPU und Beibehaltung der v1.0 Gateway-Baugruppen. In diesem Fall sind die Feature-Erweiterungen von v2.0 nutzbar, soweit sie nicht an die neue Gateway-Hardware gebunden sind, die Systemleistung steigt auf den BHCC-Wert von v2.0. Die Vorteile der v2.0 Gateways sind jedoch nicht nutzbar.

- Hochrüstung der Software auf v2.0, Einsatz der neuen cPCI CPU und Hochrüstung der v1.0 Gateway-Baugruppen auf entsprechende v2.0 Gate-way-Baugruppen. In diesem Fall sind alle Erweiterungen sowie die erhöhte Systemleistung nutzbar.

...

Neuauflage: IP-Telefonie: Cisco versus Siemens

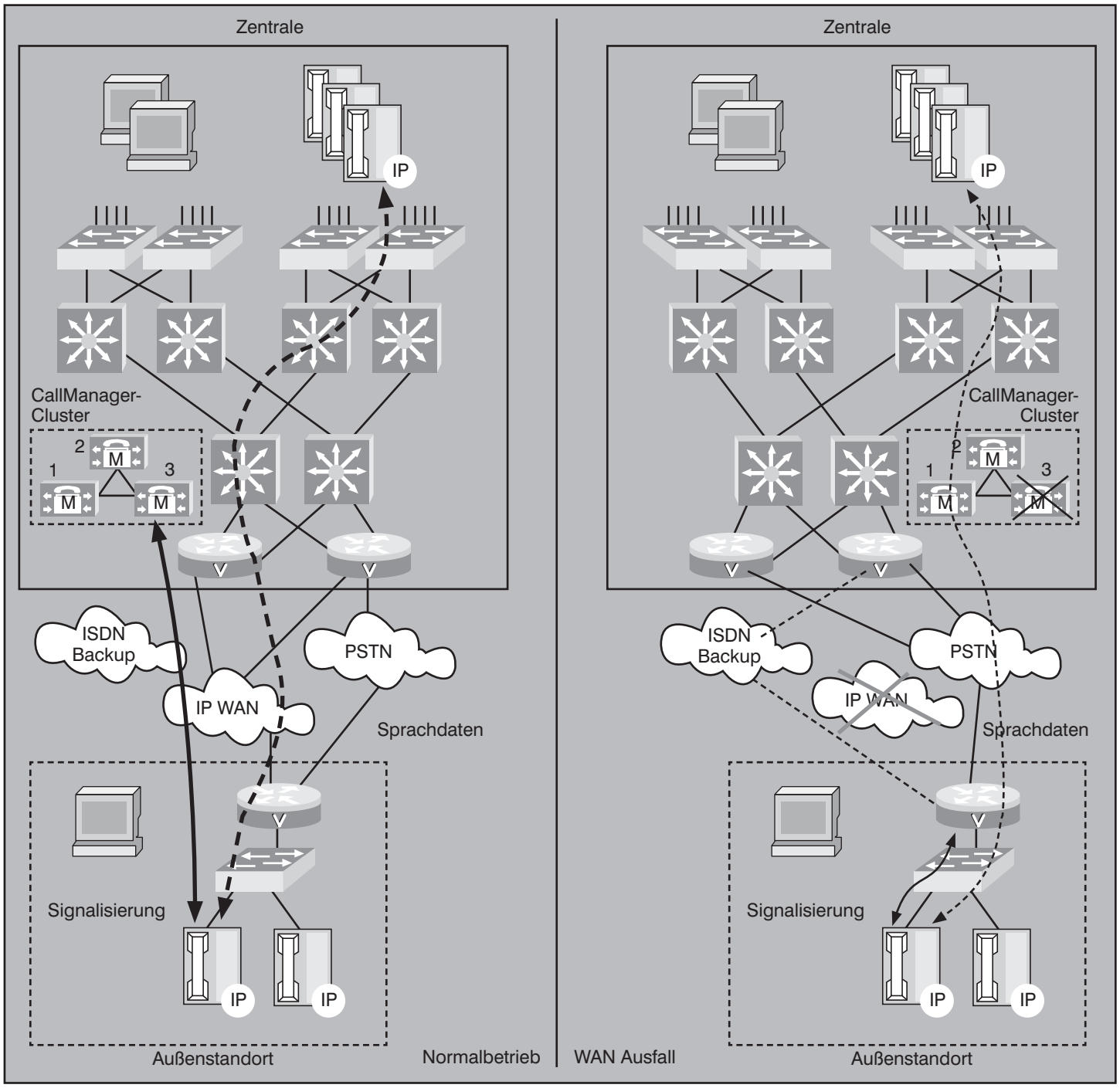


Abbildung 1: Außenstandort mit SRST im Normalfall und Fehlerfall

Die maximal an einer HiPath 4000 Anlage anschließbare Teilnehmerzahl ist 12.000 digitale und/oder IP Teilnehmer (diese Grenze resultiert aus einer Limi-tierung der adressierbaren Teilnehmer).

Der HiPath 4000 v2.0 Kommunikationsserver ist eine Neuentwicklung auf Basis des cPCI Industriestandards. Die neue zentrale CPU der HiPath 4000 v2.0 (Ap-plikations- und Daten-Prozessor ADP, Switching Unit DSCXL und ggf. ein Real Time Communications Module RTM) ist als 19“ cPCI Monosystem erhältlich. Als reine singuläre Serverlösung beinhaltet das System eine Festplatte, ein MO-Disk Sicherungslaufwerk, sowie die Prozessorbaugruppe (DSCXL). Dieser Server kann ohne weitere Baugruppen in einem völlig dezentralen reinen IP-Konzept bis zu 40 IP Access Points steuern (AP 3300/3500/3700 IP).

Ist der Betrieb einer klassischen PBX-Architektur oder eine Mischarchitektur mit abgesetzten Access Points erforderlich, wird zusätzlich das RTM-Modul (Real Time Communication Module) im zentralen Chassis erforderlich. Über dieses können bis zu 15 Shelfs (AP3700 als 19“ Technik, 13 Steckplätze, AP 3300 als 30“ Technik, 16 Steckplätze) direkt angebunden werden.

...

Neuauflage: IP-Telefonie: Cisco versus Siemens

Da die HiPath 4000 die Signalisierungsströme und Mediaströme von non-IP Geräten intern immer noch wie eine klassische PBX bearbeitet (Shelf/Modulzugang zur CPU mittels blockierungsfreier Matrix), werden erstens direkt zugeordnete IP-Geräte, zweitens IP-Trunks zu anderen HiPath 4000 Systemen und drittens IP Verbindungen zu dezentralen Anlagenteilen (Access Points) über separate Baugruppen mit Gatewayfunktion angeschaltet. Eine solche Baugruppe besteht aus einem 10/100-Mbit-Ethernet-Netzinterface mit integrierter Gateway-Funktion (HG = HiPath Gateway). Es gibt folglich drei Gateway-Baugruppen, die aus derselben Hardware und unterschiedlicher Loadware (Firmware) bestehen:

- **HG 3530** für den vollfunktionalen Zugriff von **IP-Clients** (Telefonen), auch **HFA Gateway** (HiPath Feature Access) genannt, mit 60 oder 120 parallel aktiven Kanälen und bis zu 240 konfigurierten Teilnehmern
- **HG 3550** als Trunking Gateway mit 45 oder 90 parallel aktiven Kanälen für **IP-Trunkverbindungen** (Querverbindung) zu anderen **HiPath-4000**-Systemen (CorNet-NQ) oder zum externen Gateway HG2500 von Hicom-300H-Systemen
- **HG 3570** in der HiPath 4000 als IPDA Gateway mit 45 oder 90 parallel aktiven Kanälen zur Realisierung der **IPDA** (IP Distributed Architecture) als de-zentrales Konzept zur Verbindung von zentralen Shelfs mit IP-fähigen verteilten Access Points AP 3x00, an die dezentrale Endgeräte angebunden sind.

Das IP Gateway Gegenstück für die HG 3570 Baugruppe in Access Points ist weitgehend baugleich mit den anderen Baugruppen:

- **HG 3575** im Access Point als IPDA Gateway mit 45 oder 90 parallel aktiven Kanälen zur Realisierung der **IPDA** (IP Distributed Architecture) als dezen-trales Konzept mit Anschaltung der Endgeräte über IP-fähige verteilte Access Points AP 3x00. Einer der Unterschiede zwischen HG 3570 und HG 3575 ist z.B. der, dass die HG 3575 ein Koppelfeld enthält, die HG 3570 nicht.

Liegt eine reinrassige IP-Welt vor, d.h. es gibt keinerlei periphere Baugruppen (PSTN Trunks, analoge, digitale Endgeräte etc.) in Access Points oder Shelfs so dass über die Anlage nur Signalisierung läuft, so sind gar keine Gateway-Baugruppen erforderlich, die Access Points können rein über eine SL200 Baugruppe (Ethernet) angeschaltet werden, die sämtliche Signalisierungsströme handhaben kann.

...

Eine Gesamtübersicht zeigt Abbildung 2

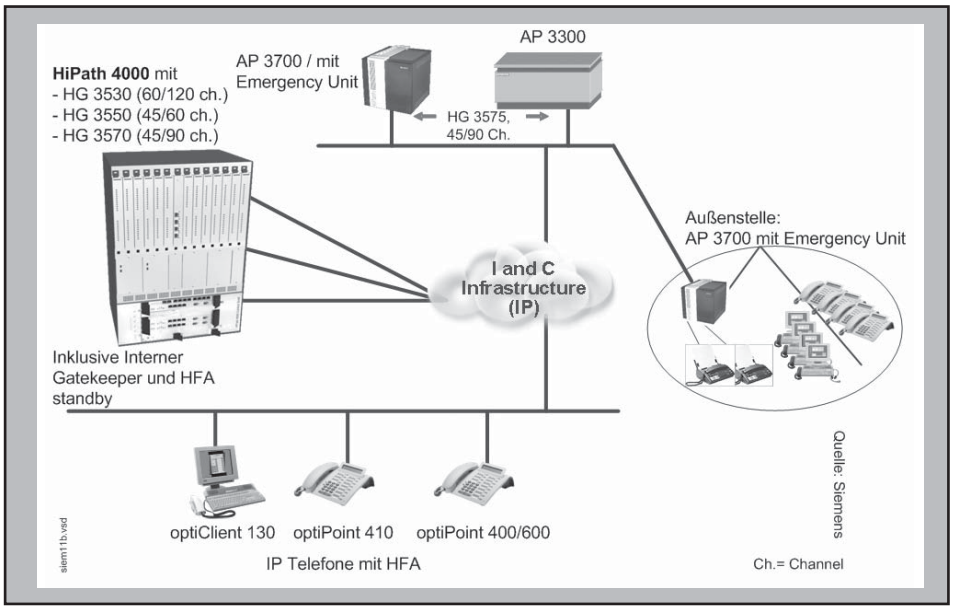


Abbildung 2: HiPath 4000, Gateway-Module und Access Points

Fax-Antwort an ComConsult 02408/955-399

Bestellung
Neuauflage:
IP-Telefonie: Cisco versus Siemens

☐ Ich bestelle den Report

Neuauflage:

IP-Telefonie: Cisco versus Siemens

(Preis € 398.-- zzgl. MwSt. und Versand)

Bestellen Sie über unsere Web-Seite
www.comconsult-research.com

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Schwerpunktthema

Design von „Voice-ready“ Netzen

Fortsetzung von Seite 1

Dipl. Inform. Petra Borowka leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

Falls die betriebenen TK-Anlagen historisch gewachsen von mehreren Herstellern sind, so ist eine Quervernetzung mit IP mit minimalem Funktionsumfang über H.323 möglich. Eine höhere Funktionalität kann QSIG liefern, da hier einige Hersteller Funktionen implementiert haben, die deutlich über den Basic Call hinausgehen. In diesem Fall ist jedoch die Verbindung im Regelfall PSTN/ISDN und nicht IP, da die meisten Hersteller (Ausnahme: Siemens) kein QSIG über IP unterstützen. Zukünftig ist zu erwarten, dass ein Multivendor-Anlagenverbund über SIP-Trunking ebenfalls Funktionen erhalten kann, die über Basic Call hinausgehen. Da zukünftig in verschiedenen SIP RFC‘s weitergehende Leistungsmerkmale als nur „Basic Call“ spezifiziert werden oder entsprechende Funktionen als herstellerspezifische Erweiterungen mit SIP Format geschrieben werden können, ist es möglich, dass Multivendor-Vernetzungen über SIP die bisherigen QSIG-Vernetzungen ablöst. Insbesondere die aktuellen Ansätze der IETF, ein Mapping zwischen SIP und QSIG oder ISUP zu spezifizieren, machen einen solchen Trend wahrscheinlich.

Ein gegenseitiges Backup der TK-Server verschiedener Standorte gegeneinander ist im Multivendor-Verbund aktuell nicht möglich. Bei einem dezentralen Betreiber-Konzept wird im Regelfall auch jeder Standort seinen eigenen PSTN-Zugang über PSTN-Gateways (gegebenenfalls fehlertolerant) betreiben, obwohl ein zentraler PSTN-Zugang über Call-Routing Regeln konfigurierbar wäre. PSTN-Gateway-Komponenten können je nach Hersteller auch als Media Gateways zur Anbindung von non-IP Geräten eingesetzt werden.

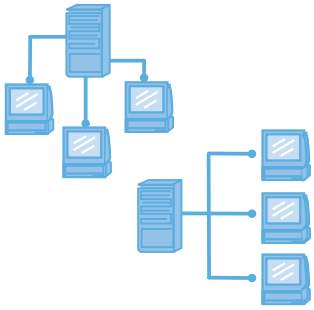
6.2 Mehr-Standort-Verbund mit verteilten IP-Anlagen

6.2.1 Vollfunktionaler Verbund

Die Standorte arbeiten jeweils autark mit eigener TK-Anlage und eigenen PSTN-Gateways, jeder Standort hat eigene Betreiberkompetenz, aber es werden Anlagen desselben Herstellers eingesetzt, die mit hoher standortübergreifender Funktionalität in einem über IP vernetzten Verbund betreibbar sind. Dies ermöglicht zusätzlich zum gemeinsamen Rufnummernplan die standortübergreifende Nutzung von Leistungsmerkmalen wie Rückruf bei besetzt, Parken / Wiederaufnehmen, Rückfrage, Anklopfen, etc. PSTN-Gateway-Komponenten können je nach Hersteller auch als Media Gateways zur Anbindung von non-IP Geräten eingesetzt werden. Die Abrechnung kann zentral oder an jedem Standort separat durchgeführt werden.

Der Anlagenverbund erfolgt über das IP-WAN-Netzwerk mit IP Trunks und der proprietären Signalisierung des eingesetzten Herstellers. Für einen solchen dezentralen

Netzwerk-Redesign
mehr Leistung - mehr Verfügbarkeit - Voice-Fähigkeit - Benutzertrennung



11.10. - 13.10.04 in Köln

Netzwerk-, Server- und Speicher-Architekturen wachsen zusammen. Gleichzeitig ergeben sich mit neuen Redundanz- und Steuerungs-Verfahren Lokaler Netzwerke, neuen Switch-Produkten sowie der verstärkten Nutzung von Wireless LANs wesentlich erweiterte Gestaltungsmöglichkeiten. Funktionalität und Leistung werden flexibel skalierbar, Betriebs- und Investitionskosten sinken. Dieses Seminar vermittelt dem Fortgeschrittenen in 3 Intensiv-Tagen, was ein modernes LAN-Design technisch und wirtschaftlich leistet. Wie unter Nutzung der neuesten Redundanz- und Switching-Verfahren ein LAN optimal gestaltet werden kann und wie dabei die Anforderungen von Client-, Server- und Speicher-Systeme im Sinne von Verfügbarkeit, Loadbalancing und Verkehrs-optimierung architektonisch integriert werden können.

Referentin: Dipl.-Inform. Petra Borowka
Preis: € 1.690,- zzgl. MwSt.

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

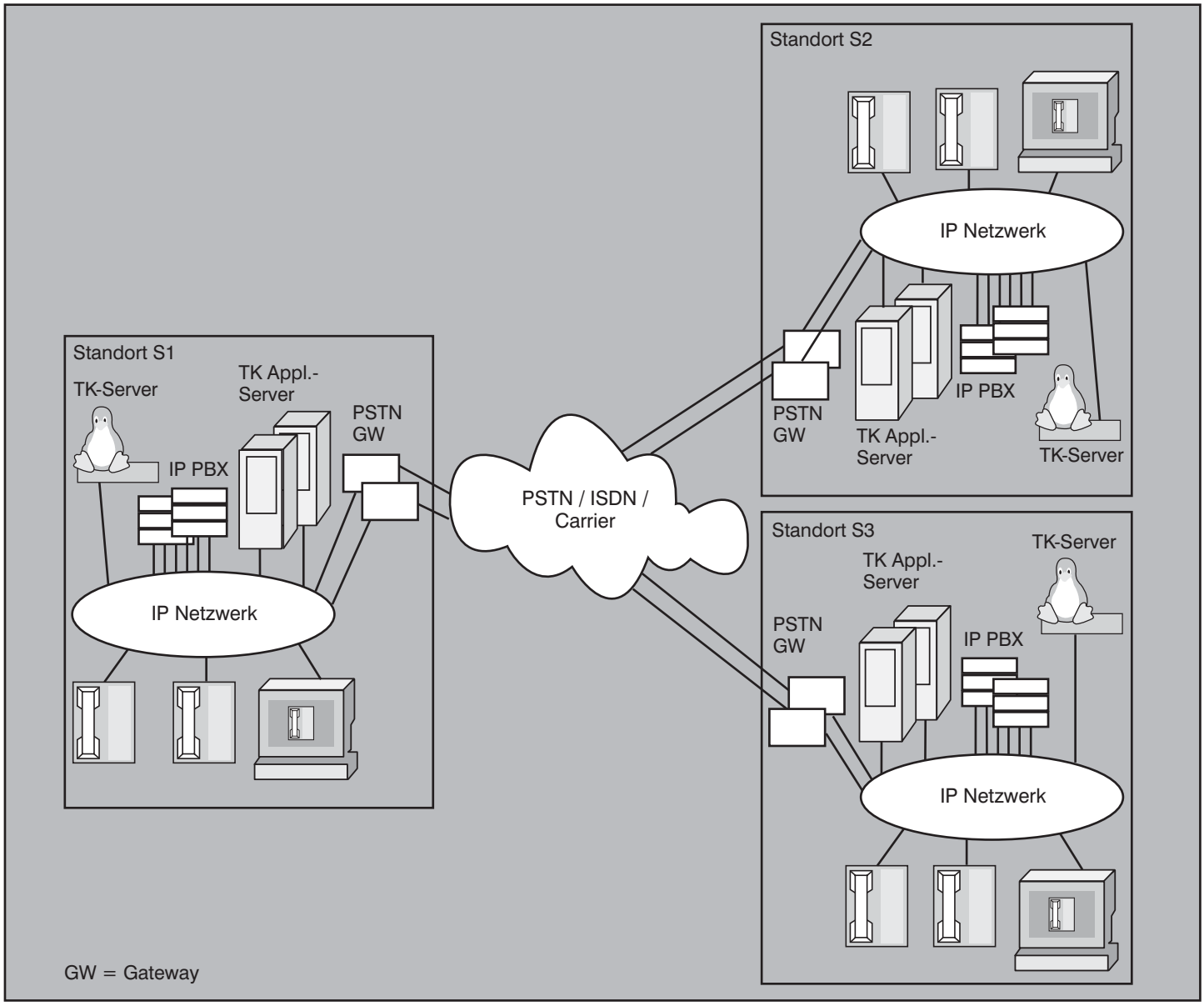


Abbildung 6.1: Dezentrales Multivendor Mehrstandort-Konzept

Standortverbund sind die Anforderungen hinsichtlich Bandbreite zu berücksichtigen, die die TK-Server / Anlagen in der aktuell eingesetzten Version benötigen, um die verbundinterne Signalisierung durchzuführen. Zusatzanwendungen werden je Standort entsprechend des Standort-Bedarfs vorgehalten. Eine Übersichtsgrafik zeigt Abbildung 6.2. Bei einem Cisco-Cluster müssen z.B. je 10.000 BHCA 900 kbit/s Bandbreite für die Intercluster-Signalisierung bereitgestellt werden.

Im dezentralen Single-Vendor-Verbund kann ein stand-ort-übergreifendes verteiltes Backup-Konzept gefahren werden: der TK-Server oder PSTN-Gateways an einem Standort lassen sich als Backup für einen anderen Standort einsetzen.

6.2.2 Eingeschränkte Funktionalität

Bei dem Betrieb von sehr großen TK-Netzwerken oder solchen mit unterschiedlichen Anlagentypen an unterschiedlich großen Standorten kann die Verbundfähigkeit auf einen mehr oder weniger stark eingeschränkten Funktionsumfang reduziert werden. Beispiele hierfür sind der Inter-Cluster-Verbund beim Cisco Call Manager oder ein Verbund von HiPath 4000 und HiPath 3000 Anlagen: In beiden Fällen läuft der Verbund über H.323 Signalisierung. Für die HiPath 4000/3000 wird dies voraussichtlich im Herbst 2004 auf CorNet erweitert, für den Call Manager ist zu erwarten, dass die Inter-Cluster Signalisierung auf SIP umgestellt wird.

6.3 Mehr-Standort-Verbund, zentrale Zusatzanwendungen und Gateways

Die Standorte arbeiten jeweils autark mit eigener TK-Anlage, jeder Standort hat eigene Betreiberkompetenz, es werden Anlagen desselben Herstellers eingesetzt, die mit hoher standortübergreifender Funktionalität in einem über IP vernetzten Verbund betreibbar sind. Dies ermöglicht wie unter 6.2 die standortübergreifende Nutzung von Leistungsmerkmalen. Die Abrechnung kann zentral oder an jedem Standort separat durchgeführt werden. Der Anlagenverbund erfolgt über das IP-WAN-Netzwerk mit IP Trunks und der proprietären Signalisierung des eingesetzten Herstellers.

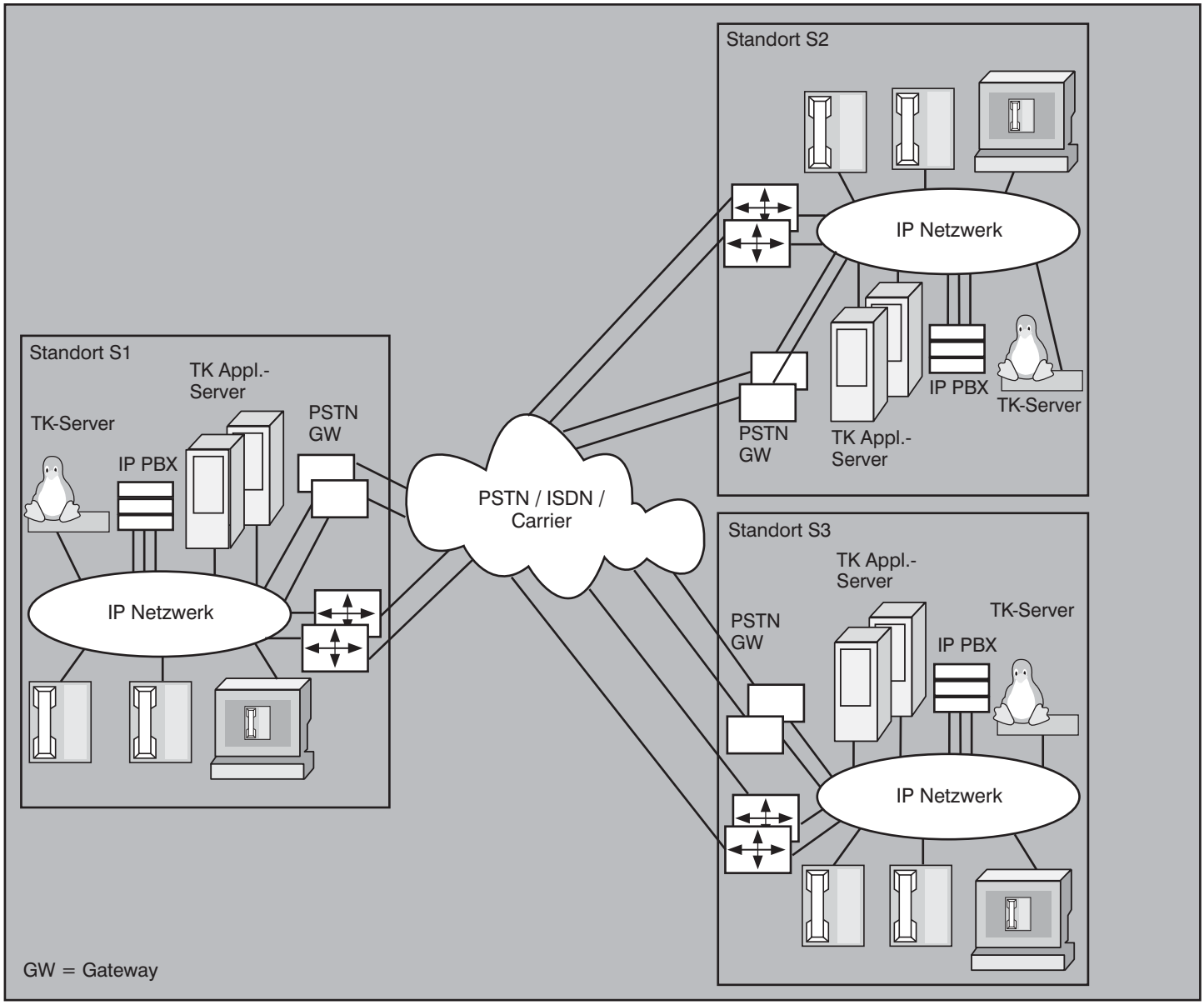


Abbildung 6.2: Single-Vendor Mehr-Standort-Verbund mit IP Trunking

Aufgrund ausreichend vorhandener WAN-Bandbreite werden Zusatzanwendungen und PSTN-Gateways jedoch zentral betrieben (siehe Abbildung 6.3). Hinsichtlich der PSTN-Gateways ist hierbei das Gesprächsaufkommen zu analysieren: Werden viele lokale PSTN-Gespräche geführt, so rechnet sich der Einsatz dezentraler PSTN-Gateways, sind die PSTN-Teilnehmer, die aus den Standorten angewählt werden, eher statistisch verteilt, so rechnen sich zentrale PSTN-Gateways. Der dezentrale Einsatz von PSTN-Gateways kann auch gewünscht sein, wenn für Kunden weiterhin eine lokale Anwahlnummer verfügbar sein soll. In diesem Fall ist zu prüfen, ob die lokale Anwahl durch eine zentrale, für Kunden kostenfreie Servicenummer ersetzbar ist, was vielfach ebenfalls zur Kundenakzeptanz führt. Werden Media-Gateways für non-IP Geräte eingesetzt, so kann der PSTN-Zugang je nach Hersteller vielfach über diese Media-Gateways realisiert werden.

Bei zentral betriebenen Zusatzanwendungen und PSTN-Gateways ist insbesondere eine entsprechende Verfügbarkeit des LAN/WAN IP-Netzwerks sicherzustellen, da der Zugriff auf diese Dienste bei Störfällen im WAN nicht mehr gegeben ist!

6.4 Zentraler Mehr-Standort-Verbund, Gateways mit Survivability

Dieses Konzept entspricht in etwa dem Standort-Konzept mit dezentralen Media-Gateways in den Gebäuden. An die Stelle des LAN-Backbone treten beim Mehr-Standort-Verbund dann Router- und WAN-Verbindungen.

Bei kleineren Standorten und ausreichender WAN-Bandbreite kann der TK-Server / die Anlage vor Ort komplett eingespart werden. Die Telefone loggen sich dann über die zentrale Anlage ein, die Signalisierung aller Gespräche läuft über den TK-Server / die Anlage – und somit auch über die WAN-Verbindungen. Auch bei dieser Lösung sind für die IP Telefone alle Leistungsmerkmale nutzbar. Zusätzlich können remote Media Gateways für den PSTN-Zugang und die Anbindung von non-IP Geräten zum Einsatz kommen, die eine so genannte Remote Survivability Funktion unterstützen (teilweise auch als

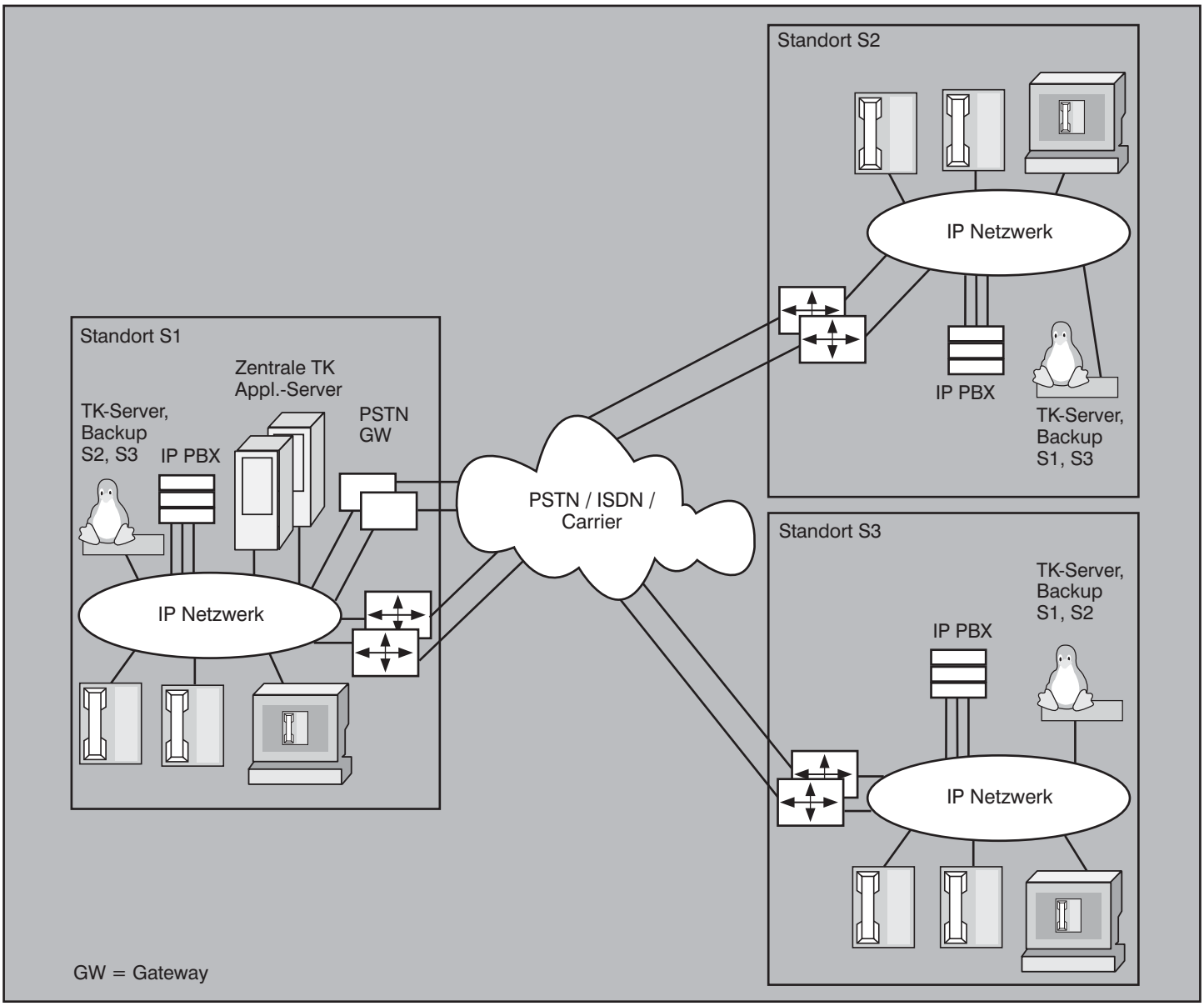


Abbildung 6.3: Mehr-Standort-Verbund mit zentralen Gateways und Zusatzanwendungen

Local Survivability bezeichnet). Eine Übersicht zeigt Abbildung 6.4.

Diese Lösung erfordert eine dezentrale Architektur, in der die Media Gateways sich mit dem zentralen TK-Server / der Anlage synchronisieren.

Vielfach wird die Backup Funktion durch einen CPU-Einschub im Media Gateway erreicht, der den zentralen TK-Server bei Ausfall ersetzt und weiterhin Telefonie ermöglicht, wenn auch mit einem mehr oder weniger eingeschränktem Funktionsumfang. In der Cisco Call Manager Lösung wird die remote Backup Funktionalität (SRST, Survivable Remote Site Telephony) als Software/ Feature Set auf einem Cisco-Router unterstützt.

Eine weitere Variante ist eine verteilte Architektur, bei der alle remote Geräte sich über ein Media Gateway einloggen, auch Access Point genannt, die volle Signalisierung über diesen Access Point läuft und zwischen Access Point und zentraler Anlage über WAN eine bandbreitenoptimierte Signalisierung genutzt wird. Die Siemens IPDA (IP Distributed Architecture) mit HiPath 4000 und Access Points 3700/3300 ist ein Beispiel für diese Variante.

Bei zentral betriebenen Zusatzanwendungen, PSTN-Gateways und TK-Servern ist insbesondere eine entsprechende Verfügbarkeit des LAN/WAN IP-Netzwerks sicherzustellen, da der Zugriff auf diese Dienste bei Störfällen im WAN nicht mehr gegeben ist!

6.5 Zentraler Mehr-Standort-Verbund, Filialen und SOHO

Bei sehr kleinen Standorten wird aus Kostengründen sowohl der Einsatz eines TK-Servers als auch eines Media Gateways mit Remote Survivability eingespart. Die IP Telefone werden einfach über Ethernet und WAN-Router an die Zentrale angeschlossen und sind darauf angewiesen, dass sowohl die zentrale Anlage als auch das IP Netzwerk verfügbar ist. Darüber hinaus steht jedoch der volle Leistungsumfang zur Verfügung. Im Home Office wird vielfach eine Softphone-Lösung mit Internet-Zugang zum Einsatz kommen, die mindestens mit RADIUS oder einer gleichwertigen Authentifizierung, möglicherweise mit VPN abgesichert werden muss.

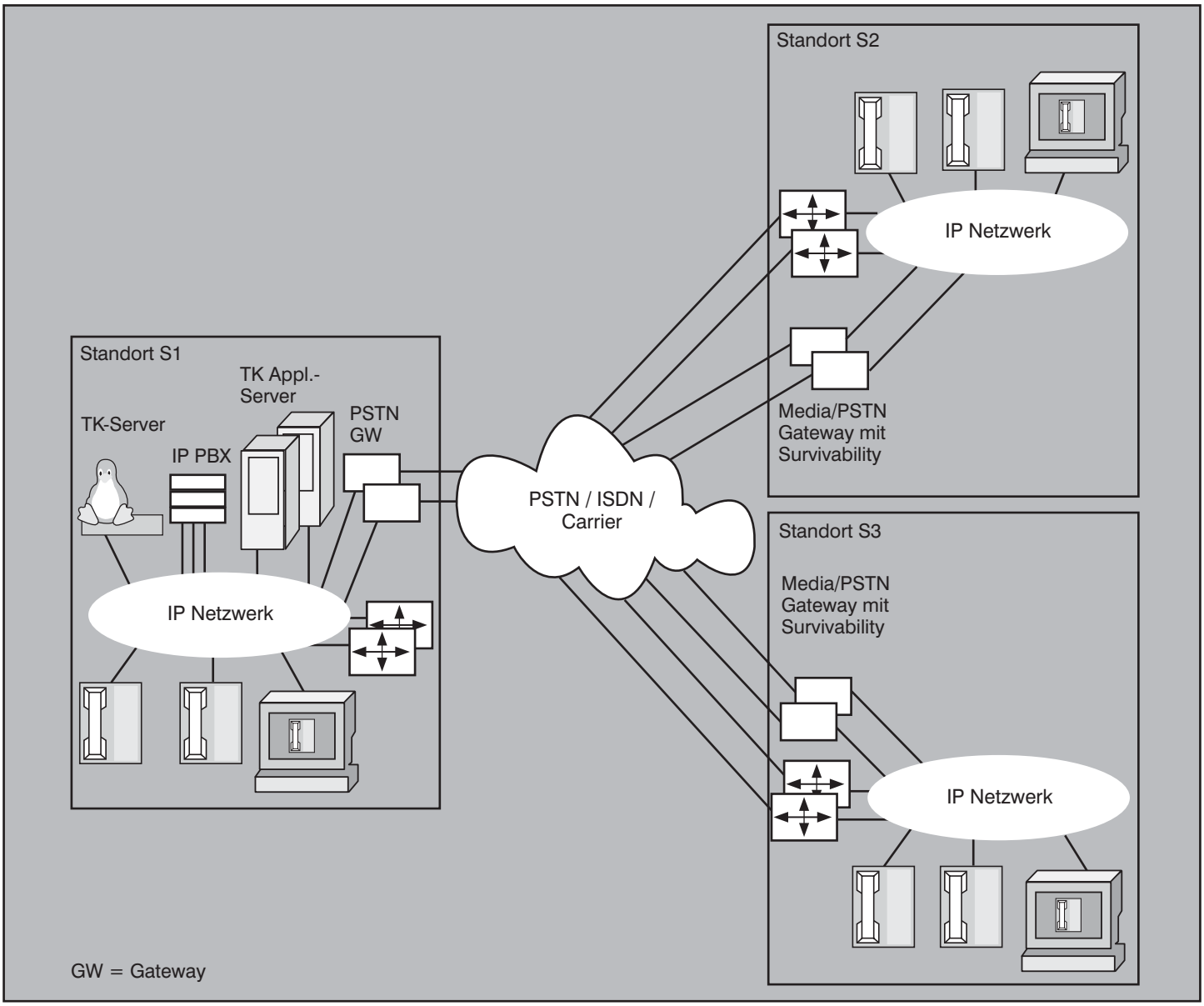


Abbildung 6.4: Zentraler Mehr-Standort-Verbund, remote Media Gateways mit Survivability

Softphone-Lösungen unterstützen teilweise noch nicht den vollen Funktionsumfang mit allen Leistungsmerkmalen.

Soweit für Kundenkontakte erforderlich kann ein PSTN-Gateway eingesetzt werden, das bei einem Ausfall des IP-Netzwerks gegebenenfalls von der zentralen Anlage aus angesteuert mittels PSTN Fallback ein Backup für das IP-Netzwerk darstellt. Darüber hinaus könnte hier auch der Griff zum Mobiltelefon als Backup-Strategie herhalten, da es sich um sehr kleine oder Einzelstandorte handelt, bei denen das Mobilnetz im Backup-Fall nicht durch einen massiven Parallelzugriff mehrerer Benutzer überlastet wird. Eine Übersicht zeigt Abbildung 6.5.

Das beschriebene SOHO/Filial-Konzept ist maximal kostenoptimiert, beinhaltet jedoch eine Reihe von Single Points of Failure: den Router zur LAN-WAN-Anbindung, die WAN-Verbindung selbst, beim Home Office den DSL-Zugang zum Provider, das PSTN-Gateway (soweit vorhanden) und den zentralen TK-Server, soweit dieser nicht mittels zentralem Backup abgesichert ist.

6.6 SIP Inseln und Zusatzdienste

Über die Dienste Video, Konferenzen, Erreichbarkeits-Anzeigen und Instant Messaging kommt zunehmend das Thema SIP in die existierende Lösungswelt hinein, da die genannten Dienste in allen neueren Lösungen seit Mitte 2003 vorzugsweise auf Basis SIP implementiert werden. Für eine Übersicht zu SIP verweisen wir auf die Netzwerk-Insider Juni, Juli und August 2004 Artikel: „Session Initiation Protokoll bringt Bewegung in den Voice over IP Markt“. Einige Beispiele im Enterprise-Umfeld für mögliche Erweiterungen der reinen TK-Funktion mit SIP Zusatzdiensten sind Cisco‘s MeetingPlace, Microsoft‘s Life Communication Server, Nortels MCS5100 oder Siemens‘ OpenScape. TK-Angebote auf der Basis von SIP im Carrier-Umfeld werden ebenfalls in steigendem Maß angeboten. Somit ist davon auszugehen, dass früher oder später SIP Inseln oder SIP-Übergänge in einer Enterprise-Lösung realisiert werden müssen. Hierzu gehört mindestens ein SIP-Gateway, bessere Integration liefern Lösun-

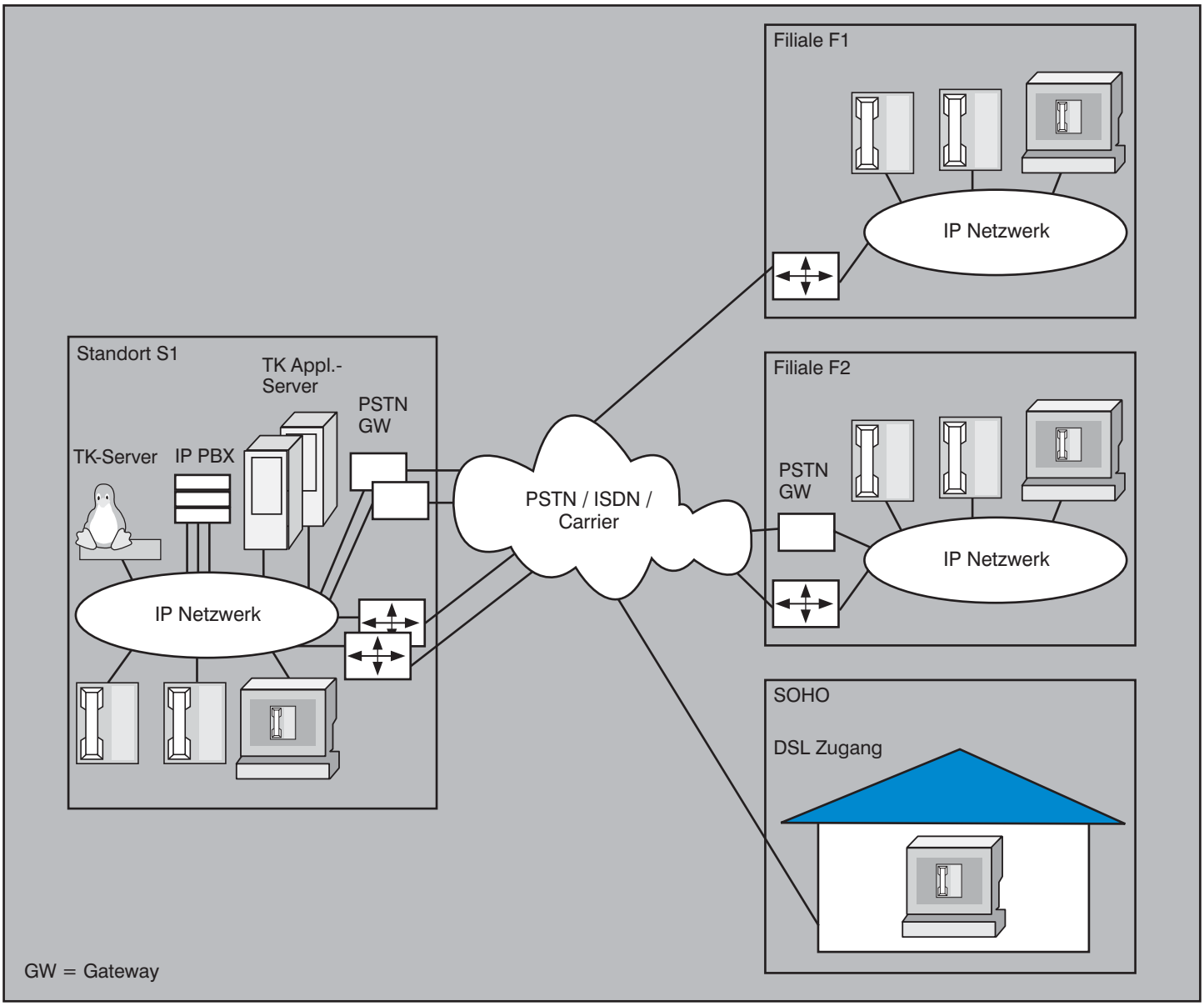


Abbildung 6.5: Zentraler Mehr-Standortverbund für Filialen und SOHO

gen, die einen eigenen SIP-Server (Registrar, Location Server und Proxy Server, seltener Redirection Server) beinhalten. Ein herstellereigenes SIP-Gateway sowie je nach Bedarf ein SIP Server sollte daher bei einer Ausschreibung oder Angebotsanfrage in den Funktionsumfang mit aufgenommen werden.

Bei der Implementierung ist es sinnvoll, für SIP-Anwendungen und SIP Server ein separates IP Subnetz zu konfigurieren, um entsprechende Möglichkeiten der Zugangsfilterung, sowohl auf IP-Ebene als auch auf Portnummern-Ebene (SIP benutzt 5060, 5061) zu haben. Falls die SIP-basierten Dienste in irgendeiner Form im Zusammenspiel mit Internet-Diensten genutzt werden, empfiehlt sich die Einrichtung und Positionierung der SIP Server sowie SIP Anwendungsserver in einer separaten DMZ.

Zukünftig ist auch denkbar, dass aus Kostengründen kleinere Standorte nicht mehr mit dem vollen Umfang an Leistungsmerkmalen für TK ausgestattet werden, sondern kostengünstige SIP-Telefone erhalten und von einem zentralen redundanten SIP-Server bedient werden. Eine Übersichtsgrafik mit SIP-Integration zeigt 6.6. Im gezeigten Beispiel wurde für alle Dienste eine vollredundante Anbindung mit separaten SIP-Servern und SIP-Anwendungsservern gewählt, alle SIP-Komponenten wurden mit einem separaten IP Subnetz von den anderen IP Netzen abgekoppelt. Ob SIP-Anwendung und SIP Server auf derselben physikalischen Maschine oder mehreren dedizierten Servern betrieben werden und wieviel Redundanz in einer konkreten Lösung für die implementierten SIP-Dienste tatsächlich erforderlich ist, dies ist in der jeweiligen Feinplanung konkret zu erarbeiten.

7. Quality of Service, Bandbreitenkontrolle

Die klassische LAN-Technik hat mit Quality of Service nicht viel gemein: Ethernet als LAN-Verfahren mit über 95% Marktdominanz sorgt zwar dafür, dass die MAC-Pakete (Frames) verschiedener angeschlossener Stationen einigermaßen geordnet über dasselbe Kabel übertragen werden,

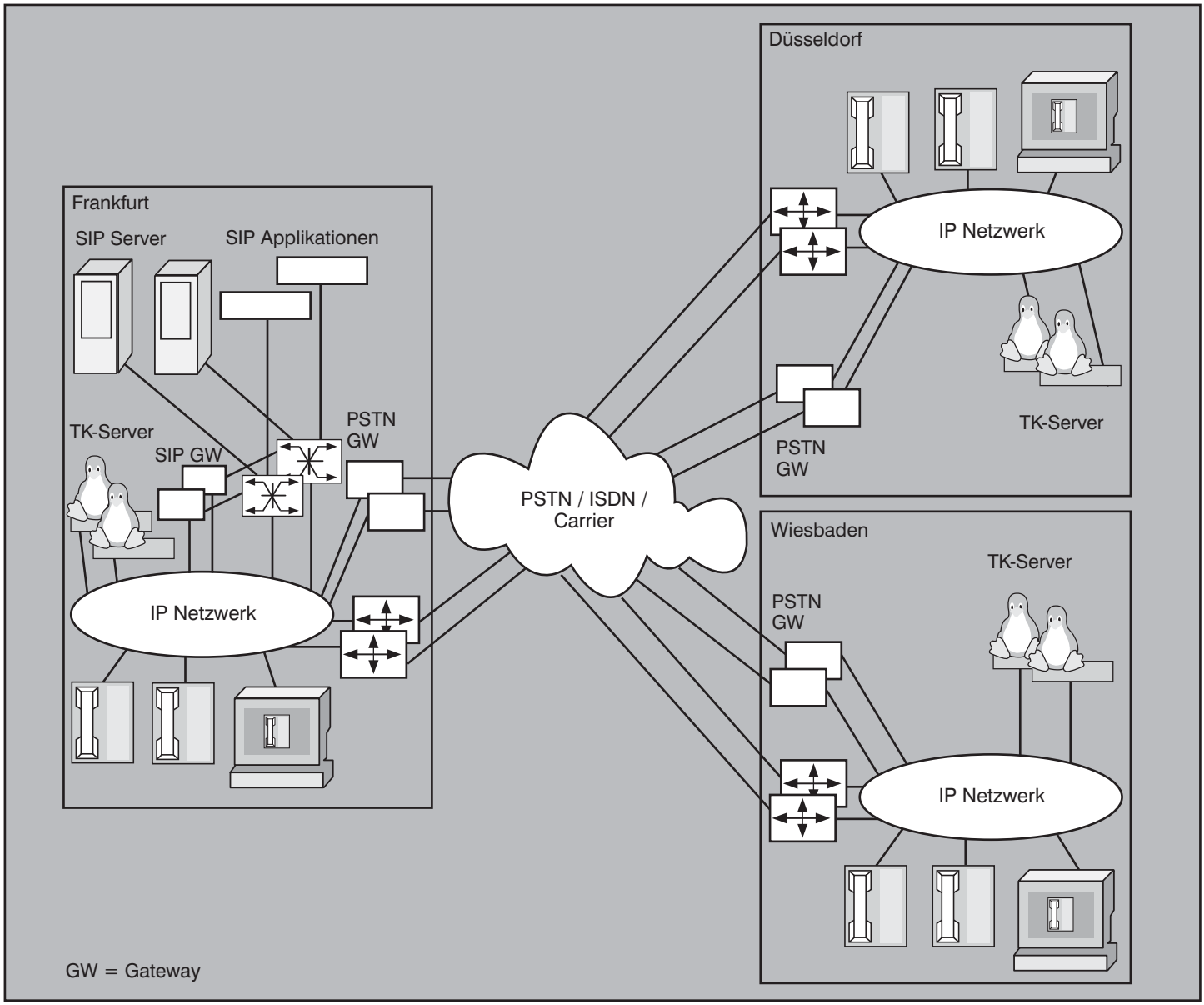


Abbildung 6.6: Integration von SIP-Inseln in Enterprise TK-Lösungen

darüber hinaus jedoch gilt das Ellenbogenprinzip: Die Station mit den längsten Paketen und dem leistungsfähigsten Netzwerkadapter nimmt sich den Löwenanteil der Kapazität. Von Bandbreiten- oder Antwortzeit-Garantie keine Spur. Mit dem Umstieg von Shared LANs auf geswitchte LAN‘s wurde full duplex Fähigkeit erreicht und wurde das Leistungsverhalten zum Endgerät besser kalkulierbar, immerhin zwei Schritte in die richtige Richtung. Mit der Ergänzung um Wireless LAN als neue Boom-Technik erfolgte ein Rückschritt zum Shared LAN.

Was ist unter Quality of Service (QoS) oder dem deutschen Begriff Dienstgüte zu verstehen? QoS bedeutet die Sicherstellung verschiedener Parameter für die betriebenen Anwendungen:

- Verfügbarkeit (pro Zeitintervall, maximale Dauer eines Einzelausfalls)
- Garantierter Durchsatz, z.B. 80 kbps bis 90 kbps für G.711 Voice über IP
- Garantierte maximale Schwankung des Durchsatzes, z.B. +/- 3%
- Garantiertes maximales Delay, z.B. 100 ms für VoIP
- Garantierte maximale Schwankung des Delays, z.B. +/- 10 ms
- Garantierte maximale Verlustrate, z.B. im LAN < 05,%, im WAN 3%

Diese Parameter sind für unterschiedliche Anwendungen und Anforderungen mit jeweils passenden Werten zu belegen. Hält das Netzwerk diese Werte ein, gelten die für einen störfreien und angemessen performanten Betrieb der Anwendung erforderlichen Voraussetzungen als gegeben.

Seit Ende der 90er Jahre wurden eine Reihe Verfahren standardisiert und in Switch-/Routerkomponenten implementiert, die in ihrer Gesamtheit Quality of Service mit Frametechnologie ermöglichen. Es handelt sich um ein Zusammenspiel mehrerer Protokoll-Spezifikationen, die insgesamt eine Ende-zu-Ende Dienstgüte ermöglichen sollen (für eine detailliertere Beschreibung der Standards verweisen wir auf den Artikel „Quality of Service im LAN: Leistung kontra Komplexität“ aus dem Netzwerk-Insider 04/1999.) Alle Einzelverfahren lassen sich im Wesentlichen auf zwei Verfahrenstypen reduzieren: Pri-

orisierung und Reservierung / Limitierung, wobei Priorisierung im Regelfall die weniger aufwändige Technik ist:

Priorisierung
- Differentiated Serviced (DiffServ, DS)
- Multi-Protocol Label Switching (MPLS)
- Class of Service (COS) auf MAC Ebene (IEEE 802.1D/p seit 802.1D-1998)
- VLAN und Priority Tagging mit IEEE 802.1Q

Reservierung / Limitierung
- Resource Reservation Setup Protocol (RSVP)
- Bandbreitenlimitierung
- Bandbreitenkontrolle (CAC Call Admission Control)

Für eine QoS-Implementierung sind zwei Kriterien zu erfüllen:
- Einzelne Netzelemente (Verbindungen, Subnetze und Router) müssen entlang eines Gesamtweges (Path) den QoS kontrollieren können.
- Die Anforderungen einer Applikation müssen den Netzelementen auf dem Gesamtweg mitgeteilt werden können oder mittels Programmierung dort hinterlegt sein.

Da der Betrieb von Quality of Service-Verfahren einen dauernden Aufwandsfaktor darstellt, herrscht im voll geswitchten Wired LAN vielfach die Philosophie vor, die erforderlichen Dienstgüteparameter durch Überkapazität implizit sicherzustellen. Mit steigender Verbreitung von Shares WLANs wird jedoch QoS Implementierung im LAN zunehmend ein Thema.

Beim Betrieb von QoS-Verfahren erfolgt zunächst eine so genannte Klassifizierung von Paketen („wichtig“, „unwichtig“, zulassen, sperren, siehe auch Abbildung 7.1), danach gegebenenfalls eine Markierung mit entsprechenden Priorisierungs-Bits im IP-Header und MAC-Header. Eine Übersichtsgrafik zeigt Abbildung 7.2.

7.1 Reservierung, Limitierung

Für Reservierung von Bandbreite- oder Antwortzeit-Garantien bei IP ist als dynamisches Layer-3 Protokoll das RSVP nutzbar, bei dem Ende-zu-Ende beim Sessionaufbau eine Bandbreiten- und Delay-Garantie angefordert wird. Der Betrieb ist aufwändig, da für jede Reservierung in den beteiligten Layer-3 Komponenten Zustandsinformationen vorgehalten werden müssen, was einen entsprechenden Speicher- und Rechenaufwand erfordert. Daher hat sich in der Praxis keine Session-bezogene Reservierung durchgesetzt, sondern maximal eine anwendungs- oder benutzergruppen-bezogene Reservierung (z.B.: Reservierung von 2 Mbit Bandbreite für alle IP-Telefongespräche auf einer WAN-Verbindung).

Bandbreitenlimitierung und Bandbreitenkontrolle werden im Gegensatz zu RSVP statisch vorprogrammiert. Im Regelfall kommt dies beim LAN/WAN-Übergang zum Einsatz, da im WAN vielfach noch enge Kapazitäts-Restriktionen gegeben sind.

Bei Layer-3 Switches und Routern werden portbezogene Limitierungsregeln für einzelne Pakettypen konfiguriert, z.B. „bis zu 10 Mbit alle Pakete mit dem IP DS-Wert 101xxx und dem VLAN Prio Tag 110xxx mit höchster Priorität bearbeiten, darüber hinaus nach Best Effort bearbeiten“.

Bei TK-Servern / IP-PBXen kann das Gesprächsaufkommen zwischen zwei Netzbereichen, im Regelfall Standorten, limitiert werden. Hierfür werden Call Admission Control (CAC) Einträge in den TK-Servern oder in externen Gatekeepern programmiert, z.B. im günstigeren Fall „maximal 30 parallele Gespräche zwischen Frankfurt und Wiesbaden, darüber hinaus Gesprächs-Umleitung über das PSTN“ oder im ungünstigeren Fall „maximal 30 parallele Gespräche zwischen

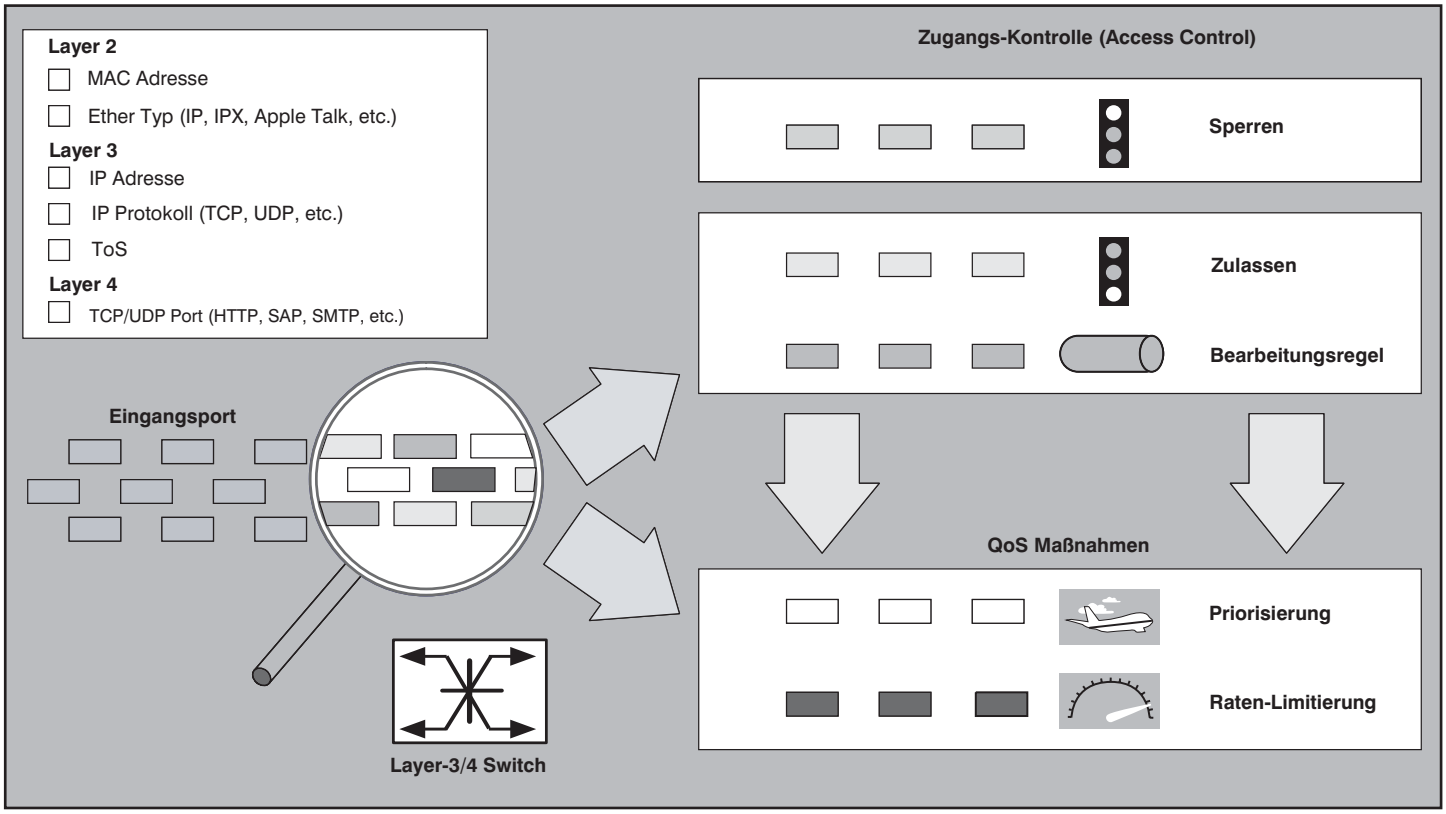


Abbildung 7.1: Klassifizierungs-Schema eines Layer-3/4 Switches

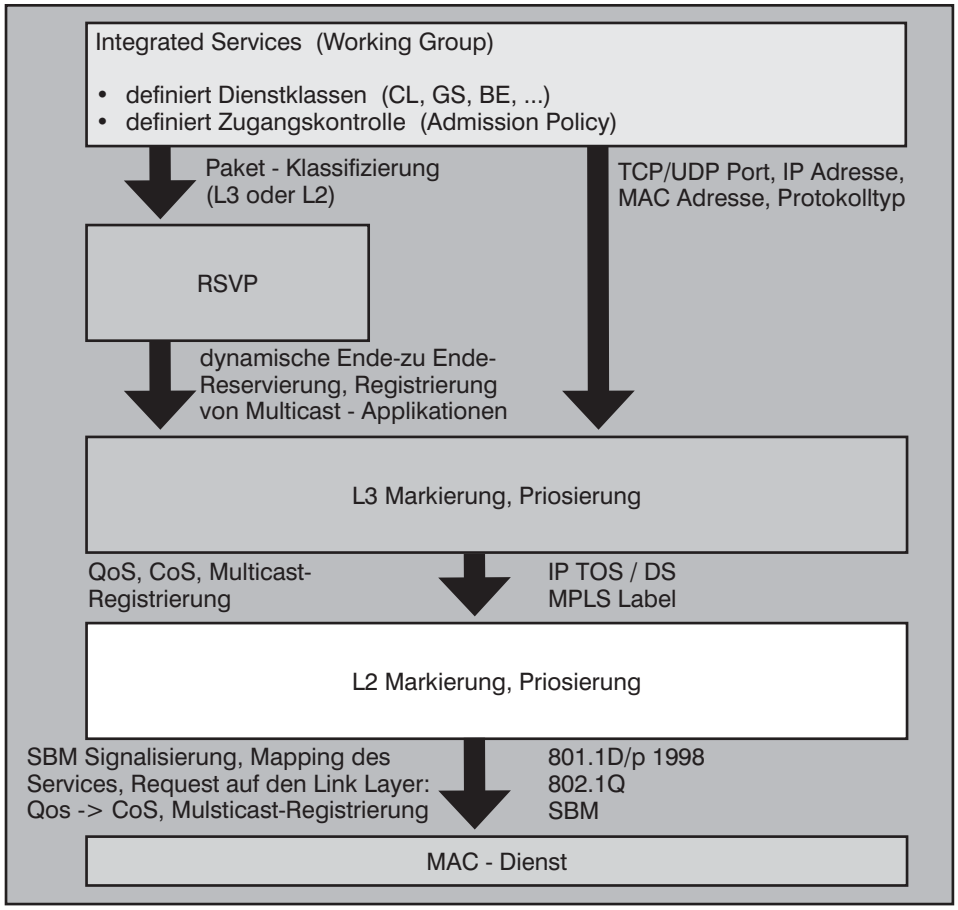


Abbildung 7.2: Klassifizierung und Markierung von Paketen bei QoS-Implementierung

Frankfurt und Wiesbaden, darüber hinaus Besetzt-Ton für den initiierenden Teilnehmer“. Diese Technik ist in der TK-Welt im Zusammenhang mit Call Routing schon lange etabliert und wurde bei IP Telefonie auf die Softswitch-Technik portiert. Im Beispiel aus Abbildung 7.3 sind zwischen Frankfurt und Düsseldorf 60 parallele Gespräche über das IP Netzwerk möglich, darüber hinaus erfolgt PSTN Rerouting. Zwischen Frankfurt und Wiesbaden sind 35 parallele Gespräche über das IP Netzwerk möglich, darüber hinaus erfolgt Besetzt-Zeichen für Anrufe, die von Frankfurt ausgehen, PSTN Rerouting für Anrufe, die von Wiesbaden ausgehen. Zwischen Düsseldorf und Wiesbaden sind 15 parallele Gespräche über das IP Netzwerk möglich, darüber hinaus erfolgt PSTN Rerouting für Anrufe in beiden Richtungen.

7.2 Priorisierung

Priorisierung bedeutet, dass einige Pakete als wichtiger betrachtet werden als andere und entsprechend „schneller“ bearbeitet werden. Im Gegensatz zur Reservierung / Limitierung ist Priorisierung der pragmatische Ansatz und beruht auf dem Prinzip der guten Hoffnung. Dieses Prinzip nennt sich PHB (Per-Hop-Behavior): Durch Konkatenierung desselben Per-Hop Behaviors über alle zwischengeschalteten Hops einer Verbindung hinweg entsteht eine Ende-zu-Ende Dienstgüte. Etwas weniger formal: Wenn jeder Switch und jeder Router auf einer Ende-zu-Ende Verbindung die Pakete konform zu den konfigurierten Regeln (Policy genannt) bearbeitet, d.h. wichtige Pakete schnell und unwichtige Pakete langsamer, besteht die Hoffnung, dass auch Ende-zu-Ende die gewünschte Dienstgüte hinsichtlich Durchsatz, Delay und Verlustrate erreicht wird. Ein Beispiel-Szenario zeigt Abbildung 7.4.

Priorisierung kann direkt oder indirekt erfolgen. Bei direkter Priorisierung werden im Paket-Header auf IP-Ebene und/oder auf MAC-Ebene in bestimmten Header-Feldern Bits gesetzt, die anzeigen, dass dieses Paket bevorzugt zu behandeln ist. Die jeweiligen Regeln, welcher Wert mit welcher Wichtigkeit bearbeitet wird, sind im Switch abgelegt. Im MAC-Header stehen hierfür die ersten 3 Bits im VLAN-Tag als Prio-Tag zur Verfügung (siehe Abbildung 7.5), die IEEE Standards setzen den Wert 110 für Sprache und den Wert für 101 Video. Im IP-Header werden bei Differentiated Services (DS) die ersten 6 Bit des früheren TOS-Byte (siehe Abbildung 7.6) genutzt. Die IETF setzt den Wert 101xxx für Sprache und 110xxx für Video. Die Voreinstellungen in existierenden Hersteller-

IP-Telefonie evaluieren, planen, betreiben

27.09. - 29.09.04 in Bonn

Dieses Seminar evaluiert die Technologie und die verfügbaren Produkte gegenüber den in der Praxis bestehenden Anforderungen. Es vermittelt die technischen Grundlagen, beschreibt die Arbeitsweise wichtiger Produkte, analysiert typische Nutzungsformen an Fallbeispielen und gibt eine Prognose für die Marktsituation und weitere Entwicklung. Die Konkurrenz-Situation zwischen CISCO und Siemens inklusive des Leistungsumfangs der Produkte wird an Hand der Ergebnisse einer hochbrisanten Studie bewertet. An Beispielen wird erläutert, welche Schritte für die erfolgreiche Implementierung von IP-Telefonie erforderlich sind. Hierzu gehört auch die Analyse der notwendigen Qualität und Leistung der zu Grunde liegenden Netzwerke.

Referentin: Dipl.-Inform. Petra Borowka
Preis: € 1.690,- zzgl. MwSt.

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

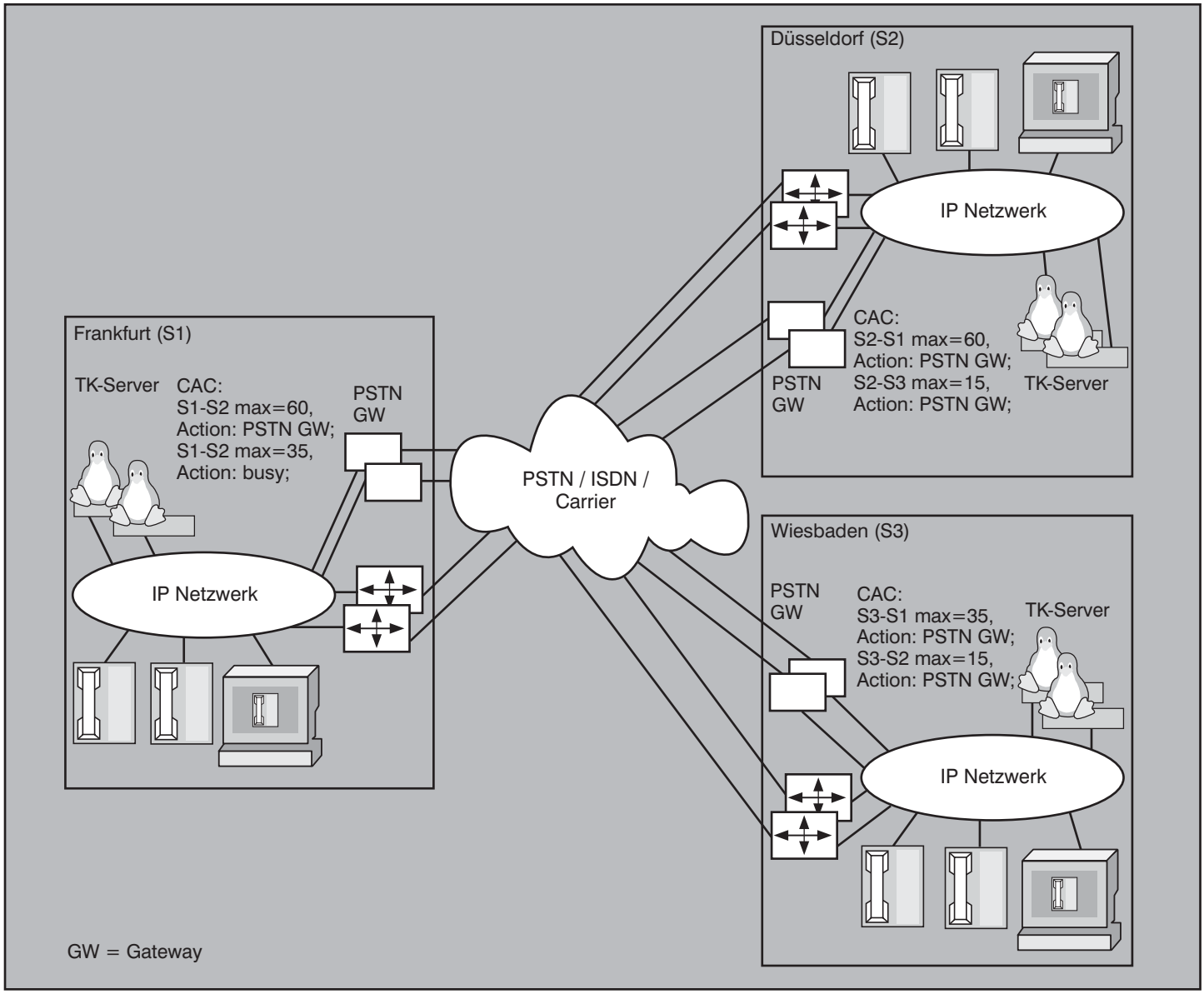


Abbildung 7.3: Call Admission Control mit verteilten TK-Servern

produkten (Telefone, Gateways, Switches, Router) können jedoch unterschiedliche und davon abweichende Werte haben, dies ist im Einzelfall zu prüfen. Insbesondere mappen einige Hersteller den IP-Wert 101 auf einen identischen MAC-Wert 101 anstelle von 110. Einige Hersteller setzen nur die IP-Bits und nicht die MAC-Bits.

Bei indirekter Priorisierung erkennt der Switch oder Router am unveränderten Paket (keine gesetzten Prioisierungs-Bits), meistens anhand der MAC-Adresse, IP-Adresse oder TCP/UDP Portnummer, ob das Paket als wichtig oder unwichtig zu behandeln ist. Der Vorteil indirekter Priorisierung liegt darin, dass kein Konfigurationsaufwand für die Markierung von Paketen entsteht. Der Nachteil liegt darin, dass nicht in allen Fällen eindeutige Paketinhalte eine Klassifizierung als Telefonie-Paket ermöglichen. Indirekte Priorisierung ist vielfach nur bei Einsatz von Hardware-Telefonen möglich, da diese einem speziellen Voice-VLAN beziehungsweise einem speziellen IP-Adressbereich zugeordnet werden können und mit einer speziellen MAC-Kennung (OUI des Telefon-Herstellers) arbeiten. Für Softphones auf PC‘s oder WLAN PDA‘s sofort die Frage, welchem VLAN und welcher Priorisierung sie zugeordnet werden sollen. Im Kapitel 5.3 „Trennung von Benutzergruppen“ haben wir auf diese Problematik bereits hingewiesen.

Als generisches Lösungsprinzip bleibt letztendlich nur die direkte Priorisierung durch die Endgeräte übrig, die auf entsprechende Bearbeitungsregeln für markierte Pakete in den Switches und Routern abgebildet wird. Hierfür muss in den Telefon-Profilen Priorisierung aktiviert werden, so dass das Telefon / Softphone für ausgehende Pakete die entsprechenden Priorisierungsbits im IP-Header und MAC-Header auf 101 (IP) und 110 oder 101 (MAC) setzt. Diese kann mit entsprechenden Bandbreiten-Limitierungen in für WAN-Verbindungen in Routern kombiniert werden.

Aktive Konfiguration und Betrieb von QoS-Maßnahmen wird vielfach am LAN-WAN-Übergang erforderlich, da hier aufgrund von Kapazitäts-Einschränkungen und Software-Routing die erforderlichen Dienstgüteparameter für Durchsatz, Antwortzeit und Verlustrate nicht a priori als gegeben vorausgesetzt werden können.

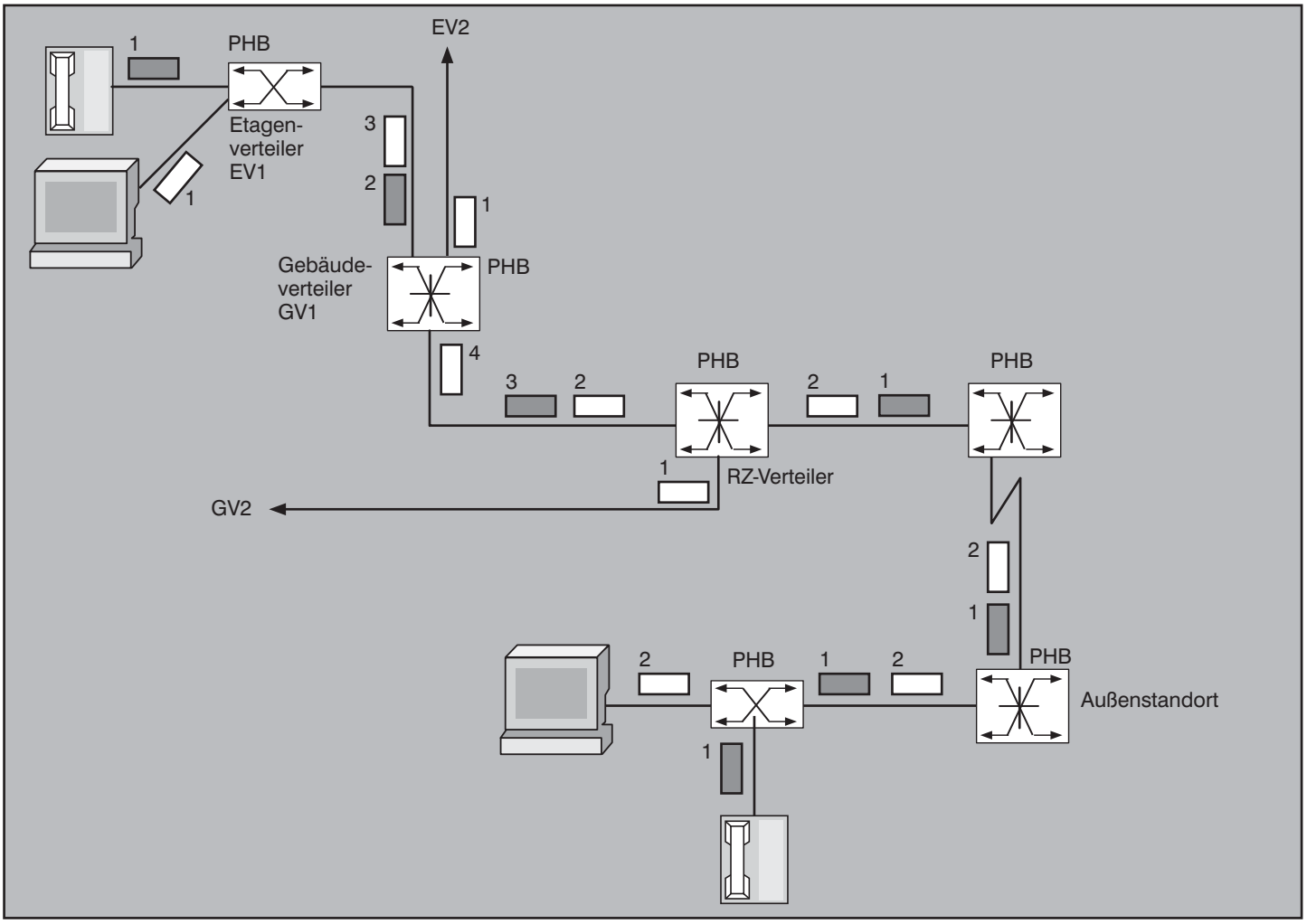


Abbildung 7.4: Qos-Implementierung mittels maximaler Priorisierung, Per-Hop-Behavior

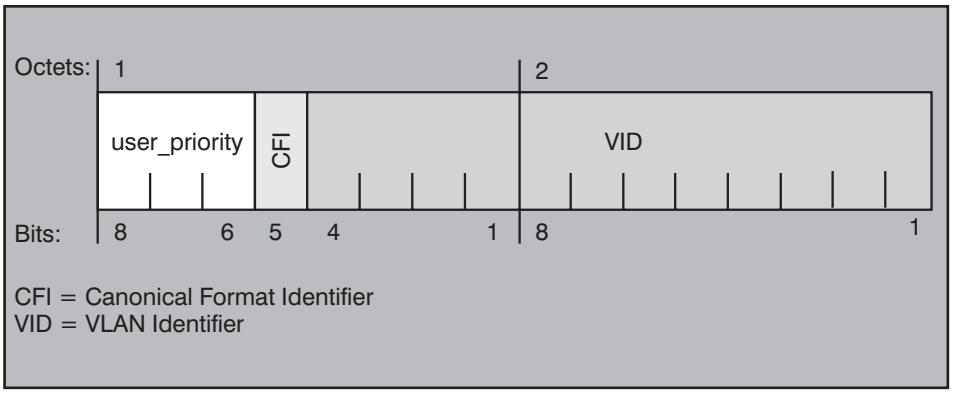


Abbildung 7.5: VLAN-Tag für Priorisierung auf MAC-Ebene

8. Management

Zum Management von TK-Lösungen stehen ähnliche Funktionen bereit wie für Datennetzwerke. Sie werden vielfach durch Accounting-Lösungen ergänzt, da dies wegen der PSTN-Nutzung im klassischen TK-Umfeld eine zwingend geforderte Funktionalität ist. Für Konfiguration und Administration steht im Regelfall ein Element-Manager mit Webinterface zur Verfügung, teilweise hat dieser nicht den vollen Funktionsumfang sondern müssen einige Aktionen noch immer über CLI durchgeführt werden. Wichtig ist insbesondere die Unterstützung von Bulk Aktionen, um Benutzerprofile für Standard-Telefone effizient verwalten und verteilen zu können.

Zunehmend sind bei Herstellern mit Produkten für Daten- und TK-Netze Integrationsversuche der Management-Lösungen feststellbar. Vielfach beschränkt sich die Integration jedoch auf ein Umbrellasystem, von dem aus die verschiedenen Element-Manager mit ihrem jeweils unterschiedlichen Look and Feel aufgerufen werden können.

Für Überwachung und Monitoring sollten die realzeittypischen Parameter „Antwortzeit / Delay“, Jitter und Durchsatz sowohl Ende-zu-Ende als auch bei Qualitäts-Einbußen Hop-by-Hop mit entsprechenden Tools abgedeckt werden. Für ausführlichere Informationen hierzu verweisen wir auf den Netzwerk-Insider vom Februar 2004 Artikel: „Voice-over-IP Management“.

9. Sicherheitsmaßnahmen

Im Zusammenhang mit der Integration von TK in IP Datennetze wird häufig

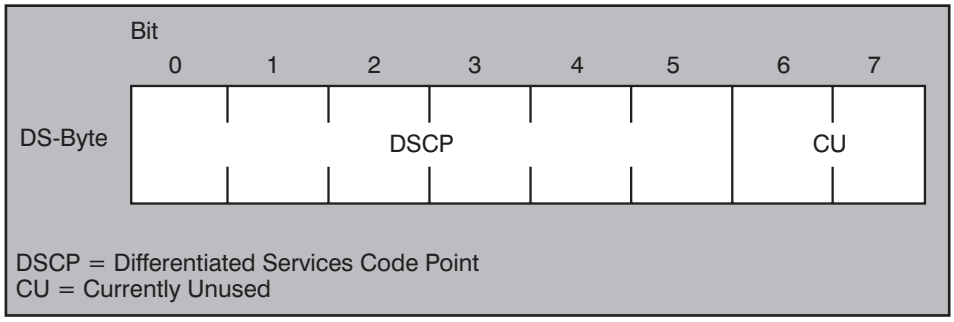


Abbildung 7.6: DS-Byte für Priorisierung auf IP-Ebene

die Sicherheitsdiskussion neu aufgerollt. Grundsätzlich sind hier zwei Betriebssituationen anzutreffen. Erstens: Die Sicherheit der Datendienste wird als so kritisch eingestuft, dass bereits Schutzmaßnahmen nach innen und außen getroffen wurden, die auch die Sicherheitsbedarfe von Voice over IP abdecken. Zweitens: Die zur Absicherung der Datendienste getroffenen Maßnahmen werden als nicht ausreichend für Voice over IP eingestuft. In diesem Fall müssen weitere Investitionen getätigt werden, um die vorhandene Sicherheitsfunktionalität soweit zu erhöhen, dass die Sicherheitsbedarfe für einen VoIP-Einsatz abgedeckt sind. Hierzu gehören bei einer vollständigen Lösung mindestens Unterstützung folgender Features

- Verschlüsselung für verkabelte Telefonie
- Verschlüsselung für WLAN Telefonie
- Authentifizierung, möglichst nach 802.1X
- Zugangsfilter
- Firewall-Anpassung
- VPN Verbindungen
- gesicherter Management-Zugriff
- Steuerung von Zugriffsrechten mittels Benutzerprofilen
- Ausreichende Logfunktionen

Für ausführlichere Informationen zum Thema Sicherheit bei Voice over IP, SIP und Sicherheit sowie Standard-Ansätze für NAT Traversal von SIP verweisen wir auf die Netzwerk-Insider vom März 2004 Artikel: „Voice-over-IP Lösungen und Sicherheit“ sowie dem SIP Teil mit dem Unterkapitel „SIP und Sicherheit“ in diesem Netzwerk-Insider.

10. Kostenrechnung

Eine Beschreibung von Total Cost-Ansätzen und vollständige ROI-Betrachtung würde den Rahmen dieses Beitrags sprengen. Daher greifen wir an dieser Stelle einige für die Kostenrechnung relevante Punkte heraus, die vor der Entscheidung für eine endgültige Lösung in jedem Fall betrachtet und in die Investrechnung einbezogen werden sollten.

10.1 Designkonzept und Switchkomponenten

Verschiedene Designmöglichkeiten beim Einsatz modularer und Workgroup Switches wurden in Teil 1 unter 5. Standort-Konzepte aufgezeigt. Wir erweitern diese Betrachtung hier um eine Kostenbewertung. Diese wurde anhand mehrerer Referenzkonfigurationen und mehrerer Hersteller durchgeführt:

Kaskadiertes Design versus sternförmiges Design, in 2003 und in 2004

- 1 Gebäude mit 8 Verteilerräumen und insgesamt 720 Anschlüssen, für zwei etablierte Hersteller
- 3 Gebäude mit 245, 79 und 30 Anschlüssen sowie insgesamt 5 Verteilerräumen, für zwei etablierte Hersteller

Workgroup Switches versus modulare Switches, in 2004

- 1 Verteiler, 40 Anschlüsse, für drei etablierte Hersteller
- 1 Verteiler, 140 Anschlüsse, für drei etablierte Hersteller

Die jeweiligen Kostenunterschiede sind den Diagrammen in Abbildung 10.1 bis Abbildung 10.4 zu entnehmen. Die Kostenbetrachtung der kaskadierten und sternförmigen Design-Varianten zeigt,

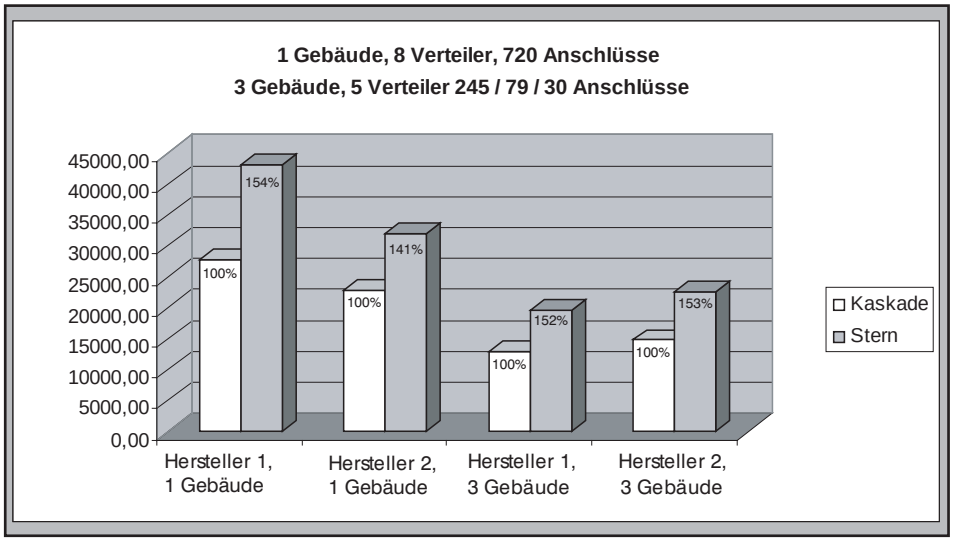


Abbildung 10.1: Sternförmiges versus kaskadiertes Design, 2003

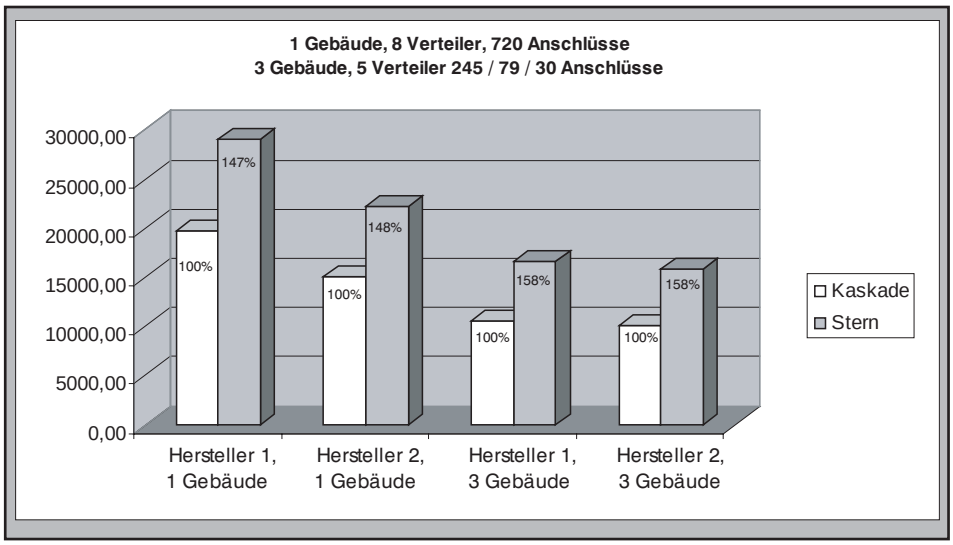


Abbildung 10.2: Sternförmiges versus kaskadiertes Design, 2004

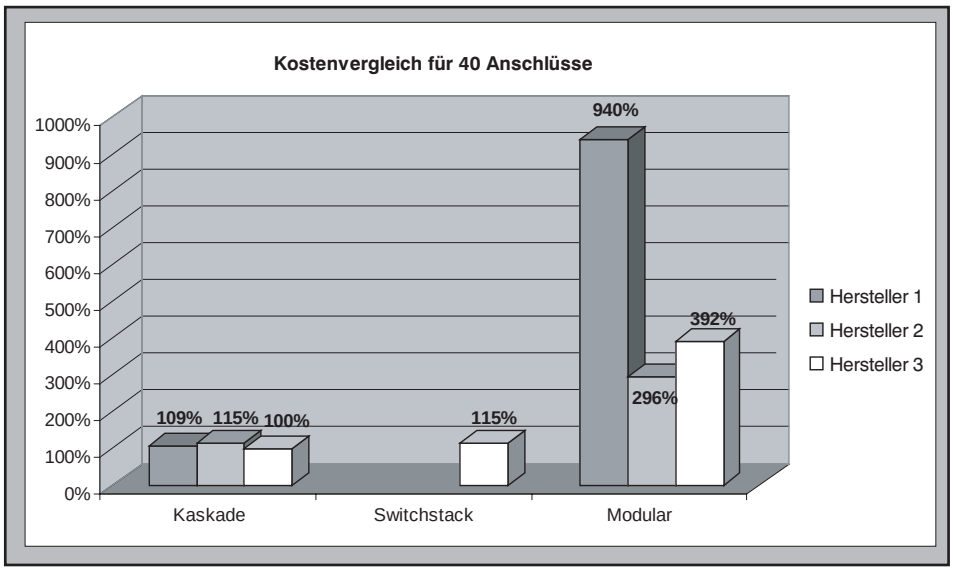


Abbildung 10.3: Modulare versus Workgroup Switches, 40 Anschlüsse

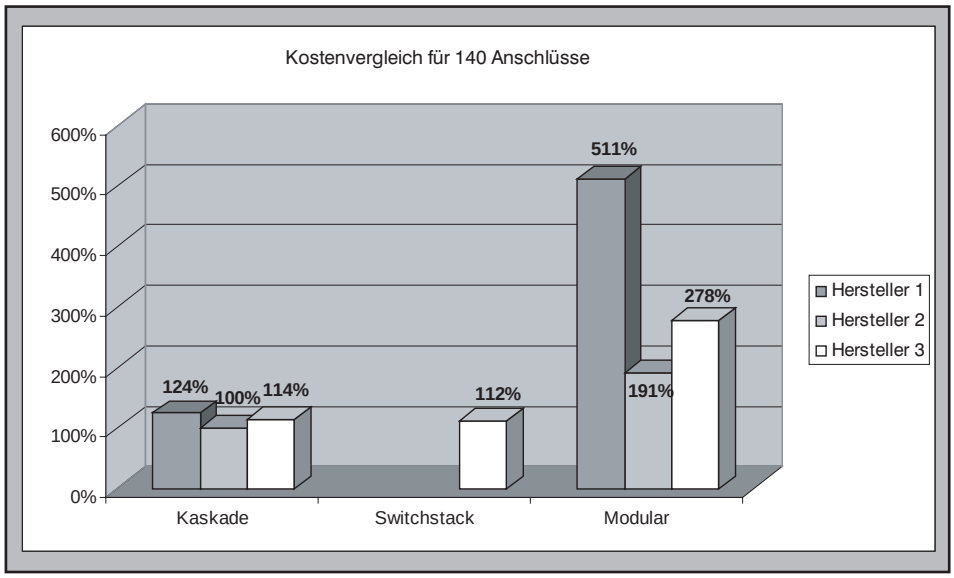


Abbildung 10.4: Modulare versus Workgroup Switches, 140 Anschlüsse

dass das Kostenverhältnis trotz insgesamt fallender Preise etwa gleich geblieben ist.

10.2 Flächendeckende Verkabelung und aktive Ports

Sowohl die Verkabelungskosten als auch die Kosten für LAN Switches werden entscheidend beeinflusst durch die Anschlussdichte. In geringerem Umfang gilt dies auch die Klimatisierung und Platzbedarf im Verteilerraum. Werden PC und Telefon kaskadiert, ergibt sich eine um ca. Faktor 0,6 bis Faktor 0,7 niedrigere Anschlussdichte als bei Einsatz einer Lösung, in der Telefone und PC‘s / Arbeitsplatzgeräte jeweils einen separaten Anschluss erhalten, für die Flächendeckung heißt dies z.B. zwei statt drei Anschlüsse je Arbeitsplatz. Diese Kostendifferenz ist bei einem konkreten Projekt, insbesondere Neubauten oder Sanierungen, sowohl für die erforderliche Verkabelung als auch für die Anzahl zu kalkulierender Switchports zu berücksichtigen.

Für die Verkabelung sollte hier allerdings ein konservativerer Ansatz als für aktive Switchports gewählt werden, da eine einmal verlegte zu niedrige Anschlusszahl bei einem späteren Umstieg auf höhere Anschlussdichte mit erheblichem Nachrüstungsaufwand und Betriebsstörungen verbunden ist, wogegen sich die Anzahl eingesetzter Switchports im Regelfall sehr viel unproblematischer hochrüsten lässt.

10.3 Power over LAN

Für PoL (Power over LAN) oder in der Praxis PoE (Power over Ethernet) kommen die Alternativen Power Hub oder Power Patchfeld in Betracht. Die Preisentwicklung der letzten Jahre führte dazu, dass Power Hubs inzwischen teurer sind als der Mehrpreis für Power-fähige Switches. Aus aktuellen Preislisten haben wir ohne Nennung von Herstellernamen einige Preise für Workgroup Switches und die gleichwertigen Power-fähigen Modelle sowie Module von Chassis-Systemen und gleichwertige Power-fähigen Modelle zusammengestellt. Die Übersicht ist in Abbildung 10.5 gezeigt.

10.4 Redundanz, Sicherheit, Management

Je nach aktueller Betriebssituation eines Netzwerkes erfordert der Einsatz von Sprache als weiterer Dienst im IP-Netzwerk eine Hochrüstung des Netzwerks hinsichtlich Redundanz und / oder Sicherheit. Wenn Sie diese Kosten nicht als allgemeine und eigentlich überfällige Verbesserung der Infrastruktur ansetzen sondern der TK-Lösung zuschlagen, lässt sich für jedes Voice-over-IP Konzept rein rechnerisch die Unwirtschaftlichkeit herbeiführen. Unsere Planungsprojekte zeigen jedoch, dass die Redundanz- und Sicherheitsbedarfe in Datennetzen sich schrittweise denen von TK-Lösungen angleichen, so dass die Entstehung etwa zusätzlicher Kosten hier maximal als eine Frage der Zeit zu bewerten sind.

Ebenso wie für Datennetze ist die Berücksichtigung einer angemessenen Management-Funktionalität in Form von Tools für Konfiguration, Verwaltung und Monitoring für die eingesetzten TK-Komponenten in die Investrechnung einzubeziehen. Analog zum Betrieb von Datennetzwerken wird hier vielfach am falschen Ende gespart und erst nach aufgetretenen Störfällen mit Produktionseinbußen das Budget für entsprechende Management-Tools freigegeben. Daher muss immer wieder gesondert auf die Notwendigkeit der Betriebs- und Überwachungs-Unterstützung mit Management-Werkzeugen hingewiesen werden. Hierzu gehört mindestens der zugehörige Element Manager, eine Probe- oder Agentenlösung für Ende-zu-Ende Monitoring sowie Archivierung von Logdateien und Konfigurationsdateien inklusive einer automatisierten Backup/Restore-Strategie für die Konfiguration aller TK-Komponenten.

Kostenvergleich Power over LAN						
Hersteller	Anzahl Ports	Workgroup		modular		Faktor
		ohne PoL	mit PoL	ohne PoL	mit PoL	
Hersteller 1	24 Port 10/100	$2.785	$3.195			115%
	24 Port 10/100			$2.095	$2.985	143%
Hersteller 2	48 Port 10/100			$3.895	$5.595	144%
	48 Port 10/100			$4.795	$6.495	135%
	24 Port 10/100	$2.395	$4.295			179%
Hersteller 3	48 Port 10/100/1000			$7.500	$9.500	127%
	48 Port 10/100/1000			$12.000	$14.000	117%
	48 Port 10/100			$5.995	$7.995	133%
	48 Port 10/100/1000			$5.495	$7.495	136%
	48 Port 10/100			$4.495	$6.495	144%
	24 Port 10/100	$2.995	$3.495			117%
	24 Port 10/100	$4.990	$5.490			110%
	24 Port 10/100/1000	$3.995	$4,795			120%
	24 Port 10/100/1000	$5.990	$6.790			113%
	48 Port 10/100/1000	$6.995	$8.495			121%
	48 Port 10/100/1000	$8.990	$10.490			117%
Hersteller 4	48 Port 10/100	$5.095	$8.155			160%
Hersteller 5	24 Port 10/100	$2.595	$3.495			135%

Abbildung 10.5: Mehrkosten für Power over LAN bei Endspan-Lösungen

11. Fazit

Telefonie über IP Netzwerke als Transportmedium ist ein stark boomender Markt. Eine Reihe betriebener Datennetzwerke ist in Struktur und Sicherheits-Funktionalität bereits jetzt für den Betrieb von TK als geeignet einzustufen. Der erreichbare Mehrwert sowie Synergieeffekte bei der Integration beider heute separat betriebenen TK- und IT-Netze sprechen dafür, dass Voice over IP sich schrittweise etablieren wird.

In jedem Einzelfall muss das vorhandene IP-Netzwerk auf seine Eignung und Optimierung für Voice-Anwendungen überprüft werden, hierzu gehören insbesondere die Betrachtung der nachfolgenden Punkte:

- Physikalische Eignung: Stromversorgung und Klimatisierung, enötigte Anschlusszahl
- Verfügbarkeit und Redundanz
- Angemessene Segmentierung / Subnetzbildung
- Abtrennung von Serverpools und TK-Serlverpools durch separate IP Subnetzwerke oder DMZ‘s
- Einsatz einer zentralisierten / dezentralisierten TK-Lösung
- Quality of Service
- Sicherheit
- Benötigte Management-Funktionalität
- Durchführung einer Kosten/Nutzen-Rechung, ROI-Betrachtung mittels Total Cost Ansatz

Report zum Thema

Design-Varianten Lokaler Netzwerke im Vergleich

Diese Studie analysiert detaillierte Beispiele realer Netzwerke unter zukunftsstrategischen, technologischen und kostenmäßigen Gesichtspunkten und zeigt auf, dass neue kostengünstige und hochperformante Designvarianten eine Reihe sinnvoller Alternativen zu den von den Herstellern vermarkteten, sternförmig redundanten Layer-3-Konzepten darstellen.

Design-Varianten
Lokaler Netzwerke im Vergleich
März 2003 - 540 Seiten
Preis: 398,-- zzgl. MwSt.

Bestellen Sie über unsere Web-Seite
www.comconsult-research.de

12. Abkürzungen

API	Application Programming Interface
AV	Audio / Video
Codec	Codierer / Decodierer
CAC	Call Admission Control
CLI	Command Line Interface
COS	Class of Service
CPU	Central Processing Unit
CTI	Computer Telefonie Integration
DECT	Digital Enhanced Cordless Telecommunication
DiffServ	Differentiated Services (IETF Working Group)
DPNSS	Digital Private Network Signalling System
DS	Differentiated Services
DSL	Digital Subscriber Line
DSP	Digital Signal Processor
ECMP	Equal Cost Multipath
GK	Gatekeeper
GSM	Global System for Mobile Communication
GUI	Graphical User Interface
GW	Gateway
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Protection System
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Informations-Technologie
ITSP	Internet Telephony Service Provider
JPEG	Joint Photographic Experts Group
JSAPI	Java Speech API
JTAPI	Java TAPI
LAG	Link Aggregation Group
LAN	Local Area Network
LSP	Local Survivability Processor
MAC	Media Access Control
MCDN	Meridian Customer Defined Network (Nortel)
MPEG	Motion Pictures Expert Group
MPLS	Multi-Protocol Label Switching
MST	Multiple Spanning Tree
MSTP	Multiple Spanning Tree Protocol
NAT	Network Address Translation
NIC	Network Interface Card
OSPF	Open Shortest Path First
PDA	Personal Digital Assistant
PIM	Protocol Independent Multicast Routing
PoE	Power over Ethernet
PoL	Power over LAN
PSTN	Public Switched Telephony Network
PSU	Power Supply Unit
QSIG	Q-interface SIGnalling protocol
RAID	Redundant Array of Inexpensive Disks
RAS	Remote Access Server
RIP	Routing Information Protocol
RTC	Real-Time Communication
RTP	Real-time Protocol
RST	Rapid Spanning Tree
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource ReSerVation Setup Protocol
RZ	Rechenzentrum
SIP	Session Initiation Protocol
SPoF	Single Point of Failure
SRST	Survivable Remote Site Telephony
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TAPI	Telephone API
TCP	Transmission Control Protocol
TK	Telekommunikation
TP	Twisted Pair
UDP	User Datagram Protocol
UM	Unified Messaging
USB	Universal System Bus
USV	Unterbrechungsfreie Stromversorgung
VLAN	Virtual LAN
VoIP	Voice over IP
VoWLAN	Voice over WLAN
VPN	Virtual private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WLAN	Wireless LAN
XML	eXtended Markup Language

REPORT ZUM THEMA

Neuauflage: IP-Telefonie: Cisco versus Siemens

Jetzt auf der Basis von Call Manager 4.0/4.1 und HiPath 4000 Version 2.0!

Diese Studie analysiert die bestehenden und in der Zukunft zu erwartenden TK-Lösungen von Cisco und Siemens mit dem Fokus auf IP-Telefonie. Technische Basis dieser neuen Auflage sind jetzt auf der Cisco-Seite der Call-Manager in der Version 4.0/4.1 und auf der Siemens-Seite die HiPath 4000 Version 2.0, die HiPath 3000/5000 Version 4 sowie die aktuellen Ankündigungen zur HiPath 8000.

Reifegrad, Funktionsumfang und Architektur der Produkte werden verglichen und es wird damit die Frage beantwortet, wer die bessere TK-Lösung anbietet. Darüber hinaus wird die erkennbare Weiterentwicklung der Produkte beschrieben und dabei insbesondere auch der Aspekt der Zukunftssicherheit dieser Produkte bewertet.

Selten hat der Wettbewerb zwischen zwei Herstellern so viel Aufregung und Diskussionen erzeugt wie der Kampf zwischen Cisco und Siemens um den deutschen TK-Markt. Lange wurde diese Auseinandersetzung von der Frage nach der Praxis-Tauglichkeit von IP-Telefonie begleitet. Auch darauf geht diese Studie intensiv ein, Funktionsumfang und Reifegrad der Lösungen werden anhand umfangreicher Kriterienlisten bewertet.

Neuauflage: IP-Telefonie: Cisco versus Siemens
August 2004 - ca. 350 Seiten
Preis: 398,-- zzgl. MwSt.

Bestellen Sie über unsere Web-Seite **www.comconsult-research.de**

CCNE

ComConsult Certified Network Engineer

Lokale Netze
27.09. - 01.10.04 in Aachen
06.12. - 10.12.04 in Aachen
21.02. - 25.02.05 in Aachen
25.04. - 29.04.05 in Aachen
27.06. - 01.07.05 in Aachen
12.09. - 16.09.05 in Aachen
28.11. - 02.12.05 in Aachen

TCP/IP und SNMP
27.09. - 01.10.04 in Berlin
06.12. - 10.12.04 in Bonn
11.04. - 15.04.05 in Berlin
20.06. - 25.06.05 in Köln
26.09. - 30.09.05 in Berlin
21.11. - 25.11.05 in Bonn

Internetworking
13.09. - 17.09.04 in Aachen
29.11. - 03.12.04 in Aachen
28.02. - 04.03.05 in Aachen
30.05. - 03.06.05 in Aachen
26.09. - 30.09.05 in Aachen
28.11. - 02.12.05 in Aachen

Ethernet Technologien - neuester Stand
13.09. - 17.09.04 in Aachen
29.11. - 03.12.04 in Aachen
14.03. - 18.03.05 in Aachen
20.06. - 24.06.05 in Aachen
19.09. - 23.09.05 in Aachen
14.11. - 18.11.05 in Aachen

Paketpreis für alle vier Seminare € 8.170.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
08.11. - 12.11.04 in Aachen
21.02. - 25.02.05 in Aachen
06.06. - 10.06.05 in Aachen
12.09. - 16.09.05 in Aachen
07.11. - 11.11.05 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
27.09. - 01.10.04 in Aachen
14.02. - 18.02.05 in Aachen
30.05. - 03.06.05 in Aachen
24.10. - 28.10.05 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
06.09. - 10.09.04 in Aachen
22.11. - 26.11.04 in Aachen
11.04. - 15.04.05 in Aachen
04.07. - 08.07.05 in Aachen
17.10. - 21.10.05 in Aachen
28.11. - 02.12.05 in Aachen

Paketpreis für alle drei Seminare mit Etherreal in Kombination mit Fluke Net-tool € 7.500.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

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

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I: Von den Einzelbausteinen zur integrierten Lösung
11.10. - 15.10.04 in Bonn
14.02. - 18.02.05 in Bonn
25.04. - 29.04.05 in Bonn
06.06. - 10.06.05 in Köln
26.09. - 30.09.05 in Nürnberg

Sicherheitslösungen II: IP-VPNs, der Kern einer Sicherheits-Infrastruktur
13.09. - 15.09.04 in Köln
15.11. - 17.11.04 in Köln
28.02. - 02.03.05 in Bonn
30.05. - 01.06.05 in Köln
19.09. - 21.09.05 in Bonn
07.11. - 09.11.05 in Köln

Sicherheitslösungen III: Planung und praktische Konfiguration
04.10. - 08.10.04 in Aachen
06.12. - 10.12.04 in Aachen
18.04. - 22.04.05 in Aachen
27.06. - 01.07.05 in Aachen
17.10. - 21.10.05 in Aachen
05.12. - 09.12.05 in Aachen

Paketpreis für alle drei Seminare € 5.330.-- zzgl. MwSt.
(Einzelpreise: € 2.290.-- / € 1.690.-- / € 2.290.--)

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

Impressum

Verlag:
Dr. Suppan International institute b.v
Ahornenlaan 12
4493 DG Kamperland, Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

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

© Dr. Suppan International Institute b.v.