ComConsult Research

Der Netzwerk Insider

Juli/August 2007

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Herausforderung VoIP-Sicherheit

Wie sicher ist die Kommunikation von morgen

von Dr. Behrooz Moayeri

Als der Autor am folgenden Beitrag arbeitete, wurde bekannt, dass die neue französische Regierung aus Sorge vor einer eventuellen Ausspionierung durch den amerikanischen Geheimdienst National Security Agency (NSA) den Gebrauch von mobilen Geräten des Typs Blackberry in den Ministerien Frankreichs verboten hat.

Dahinter steht die Unsicherheit, was mit Nachrichten geschieht, die in den Rechenzentren des Blackberry-Anbieters RIM weiter vermittelt werden. Obwohl das kanadische Unternehmen RIM immer wieder beteuert, dass eine Verschlüsselung für die ausreichende Sicherheit der Kundendaten sorgt, warnen Experten davor, sich vollständig auf diese Zusicherung zu verlassen, und empfehlen zusätzliche Verschlüsselungsmaßnahmen.

Ein ähnliches Problem wird mit der zunehmenden Nutzung von Voice over IP (VoIP) und insbesondere der zunehmenden Nutzung des Internet für die Sprachkommunikation entstehen, nämlich die Unsicherheit, über welche Wege die Gespräche übertragen werden und wer sie abhören kann.

weiter auf Seite 16

Zweitthema

Neue Flusskontrolle in Vista - 50% mehr Last, Netzwerke in Gefahr?

von Dipl.-Inform. Oliver Flüs

TCP ist immer noch auf eine 20 Jahre alte Netzwerk-Technik optimiert. Im Wesentlichen bedeutet dies, dass es versucht, Engpässe zu vermeiden, die mittlerweile nur noch in Sondersituationen vorkommen, im LAN praktisch gar nicht.

So werden große Teile der Bandbreite moderner Netzwerke gar nicht genutzt. Zum Beispiel könnten Backup-Vorgänge über das Netzwerk bei voller Nutzung des gegebenen Potenzials um bis zu 50% schneller erfolgen. So erklärt sich auch, dass viele Benutzer beim Aufrüsten von 100 Mbit/s auf Gigabit-Netzwerke eigentlich keinen messbaren Unterschied in der Performance feststellen.

Nun hat Microsoft mit Vista den „Next-Generation IP-Stack“ eingeführt. Vollendet wird diese Neuerung mit dem Gegenstück auf der Server-Seite, wenn Longhorn auf den Markt kommt.

weiter auf Seite 5

Aktueller Kongress

Voice-over-IP-Forum 2007

auf Seite 4

Geleit

ComConsult Certified Voice Engineer

auf Seite 2

Report des Monats

Session Initiation Protocol

auf Seite 13

Zum Geleit

ComConsult Certified Voice Engineer

Wer in die Umsetzung von IP-Telefonie-Projekten einsteigt, bewegt sich schnell in zwei Welten. Nach wie vor ist klassisches TK-Wissen notwendig. Das beginnt bei den bekannten Leistungsmerkmalen, geht über die Gateways zum PSTN, über Rufnummernpläne, Voice-Anwendungen bis hin zu Spezialanwendungen. Gleichzeitig erfordert die Umsetzung von IP-Telefonie erhebliches IP-Wissen:

- IP-Adressen müssen vergeben werden, TFTP-Server eingerichtet und DHCP-Server konfiguriert werden
- Das zentrale Element jeder IP-Telefonie-Lösung ist der Voice-Router, egal ob der als Registar, Call Manager oder wie auch immer bezeichnet wird. Dieser setzt immer mehr auf offenen Betriebssystemen auf und seine Architektur verschmilzt mit der des Betriebssystems. Speziell im Bereich ausfallsicherer und skalierbarer Architekturen ist das eindeutig. Der Trend geht weg von den herstellerspezifischen Spezialtechnologien und hin zur Nutzung offener Betriebssystem-Funktionen
- Die Nutzung von Skripten und XML-Parameter-Dateien ist unvermeidbar
- Die Integration ins Netzwerk erfordert detailliertes Wissen über VLAN´s, PoE, Switching, Layer2/3-Strukturen, Quality of Services
- Die Schaffung einer sicheren Voice-Lösung geht nur in einem integrierten IT-Gesamtkonzept, der Artikel von Dr. Moayeri in diesem Insider macht dies deutlich
- Immer mehr Applikationen gehen in Richtung Kollaboration, die Integration des zugehörigen Softclients ins Betriebssystem führt zu einer Verschmelzung von IT und TK. Nicht macht dies mehr deutlich als der Ansatz von Microsoft mit dem Office Communication Server und der Client-Integration in Office-Anwendungen

Die Entwicklung der technischen Architektur von Sprach-Lösungen entspricht genau diesem Bild. Die herstellerspezifischen und geschlossenen Architekturen öffnen sich in Form von Funktionsblöcken, die zunehmend aus einer Mischung aus offenen und geschlossenen Funktionen bestehen:

- IP-optimierte Infrastrukturen im Kern (Netzwerke, IP-Dienste, Verzeichnisdienste, ...)
- Voice-Routing und Call-Management als zunehmend offener Funktionsblock, Gestaltung von Ausfallsicherheit und Skalierbarkeit mit einer Mischung aus offenen und spezifischen Funktionen
- Leistungsmerkmale als applikationsartiger Aufsatz auf das Basis-Call-Routing in einer Mischung aus genormten und herstellerspezifischen Modulen
- Applikationen, zunehmend neutral von der darunter liegenden Sprach-Lösung

Die Beherrschung dieser Architektur, dieses Wandels weg von einer rein herstellerspezifischen und hin zu einer gemischt offenen/geschlossenen Architektur erfordert ein neues Wissensprofil für Planer und Betreiber.

Ohne tiefer in die Details einzusteigen, wird doch schnell deutlich, dass hier ein neues Berufsbild entsteht. Die Planung und auch der Betrieb einer IP-Telefonie-Lösung erfordert ein Spezialwissen, das in dieser Form bisher nicht vorhanden ist. Dem bisherigen IT-Spezialisten fehlt das TK-Wissen, dem TK-Spezialisten das IT-Wissen.

Nachdem wir nun über die letzten 2 Jahre unsere Basiskurse zur IP-Telefonie aufgebaut haben, hat sich mit dem neuen Kursen der letzten Monate das Mosaikbild geschlossen. Systematisch haben wir die Bausteine aufgebaut, die zu einer soliden Ausbildung zum Voice-Spezialisten erforderlich sind.

Deshalb freuen wir uns, Ihnen heute die Einführung des ComConsult Certified Voice-Engineers ankündigen zu können.

Im Einzelen besteht die Ausbildung aus folgenden Modulen:

- Optional: IP-Wissen für Telekommunikations-Mitarbeiter: was Sie über IP Wissen müssen, um IP-Telefonie umsetzen zu können
- Optional: Voice-over-IP für Telekommunikations-Mitarbeiter, wird aufgrund der an den Kunden angepassten Inhalte zur Zeit nur als Inhaus-Kurs angeboten
- Alternative 1: IP-Telefonie evaluieren, planen und betreiben
- Alternative 2: IP-Telefonie: Vorbereitung, Migration, Management
- Session Initiation Protocol SIP
- Voice-Security

Alternative 1 oder 2 müssen wahlweise besucht werden. Aufgrund der beabsichtigten inhaltlichen Überlappung der beiden Kurse reicht es aus, einen der beiden zu besuchen. Wer als Zertifizierungsteilnehmer beide Kurse besuchen will, kann dies zu einem sehr attraktiven Sonderpreis machen.

Die Zertifizierung ist mit einem Abschlusstest verbunden, der elementares Wissen über IP-Telefonie abfragt.

Basierend auf der Projekterfahrung der letzten Monate und Jahre wurde diese Zertifizierung so angelegt, dass sie ein maximales und Praxis-erprobtes Hersteller-neutrales Wissen optimal vermittelt. Sie liefert das optimale Fundament für erfolgreiche Projekte und stellt einen wesentlichen Baustein der beruflichen Weiterentwicklung da.

Sollten Sie Fragen zur Zertifizierung haben, so stehen wir Ihnen gerne beratend zur Seite.

Viel Erfolg
Ihr
Dr. Jürgen Suppan

Zweitthema

Neue Flusskontrolle in Vista - 50% mehr Last, Netzwerke in Gefahr?

Fortsetzung von Seite 1

Dipl.-Inform. Oliver Flüs verfügt über langjährige Kenntnisse im Betrieb von IT-Infrastrukturen. Als Leiter des Competence Center IT-Service der ComConsult Beratung und Planung GmbH bearbeitet er seit Jahren Projekte in den Bereichen informatikorientierte Beratungsleistungen und Organisationsberatung im IT-Bereich. Zu diesen Themengebieten ist er regelmäßig als Referent bei der ComConsult Akademie tätig.

Dies wirft sofort eine Reihe von Fragen auf, auf die dieser Artikel im folgenden eingeht:

- drohen unseren Netzwerken mit dem neuen Microsoft TCP-Stack deutlich höhere Spitzenlasten?
- Können dadurch Überlasten oder Instabilitäten zum Beispiel durch einen Pufferüberlauf in Switch-Systemen entstehen? Müssen die so genannten Buchungsfaktoren für die Planung von Netzwerken angepasst werden (diese beschreiben die theoretische Überlastbarkeit von Switchen unter der Annahme typischer Spitzenlasten)?
- Können dadurch stärker schwankende Betriebssituationen entstehen?
- Erfordern mögliche Überlasten ein Umdenken im Einsatz von Quality of Service? Bisher ist QoS in 100/1000-Netzwerken nicht erforderlich, es steigert nur den Betriebsaufwand. Ändert sich das nun?

1. Warum (Artikel zu Vista's) Verbesserungen für TCP?

Vista ist da, an Longhorn wird fleißig gearbeitet - natürlich werden die damit verbundenen Neuerungen in der Fachpresse beschrieben und diskutiert. Diesmal stürzt man sich dabei nicht ausschließlich auf Aspekte wie Aussehen und Handhabung der Oberfläche, neue Dienstangebote u.Ä.: vermehrt findet man auch Artikel über die Veränderungen an der mitgelieferten TCP/IP-Software. Diese hat Microsoft schon eine Weile als „Next Generation IP-Stack" angekündigt, ja angepriesen.

„Next Generation" - das klingt nach dem Versuch eines großen, neuen Wurfs. Oder wurde diese Bezeichnung gewählt, weil Microsoft mit Vista / Longhorn verstärkt mit der Unterstützung von IPv6 „Ernst macht" (IPv6 wurde anfänglich auch als „IP next generation" bezeichnet)?! Ja, das Thema IPv6 wurde tatsächlich stärker in den Blickpunkt genommen, was auch erklärlich ist, da in 2005/2006 eine deutliche neue Lage hinsichtlich stabiler RFC-Dokumente zu diesem Thema entstanden ist. Insofern könnte man sich an dieser Stelle mit Vista und IPv6 beschäftigen.

Nicht die neue Situation bzgl. IPv6 soll hier aber näher betrachtet werden (gerne ein anderes Mal), sondern ein anderer Themenkreis, bei dem Vista mit Neuerungen aufwartet, und zwar mit potenzieller Wirksamkeit unabhängig von der IP-Version: Flusskontrolle unter TCP. Vista wirbt hier gleich mit mehreren Modifikationen, und diverse Artikel (nicht nur von Microsoft) sagen spürbare Auswirkungen in Netzwerken voraus. TCP-Flusskontrolle, was war das gleich wieder? Im Prinzip wird hier versucht, auf automatischem Wege einen guten Kompromiss zu finden zwischen möglichst guter „Performance" bei der Übertragung von Nutzdaten via TCP und der Vermeidung von Engpässen durch Überlastung der Ressourcen, Ressourcen im Netzwerk bzw. Empfänger-Kapazität. Devise dabei: vorsichtig einsteigen (slow start), bei Übertragungserfolg zunächst kräftig nachlegen, dann wieder vorsichtiger werden (congestion avoidance, also „Engpassvermeidung"); sollte dennoch etwas schiefgehen (timeout, retransmission nötig) - Luft rausnehmen aus der Senderaktivität. (s. Abbildung 1)

Klingt doch überzeugend, also warum zum Thema machen? Der Grund: die Art und Weise, in der dieser Ansatz im Detail ursprünglich umgesetzt wurde, hatte Netzwerk-Kapazitäten vor Augen, die im Vergleich zu heute lächerlich sind. Ent-

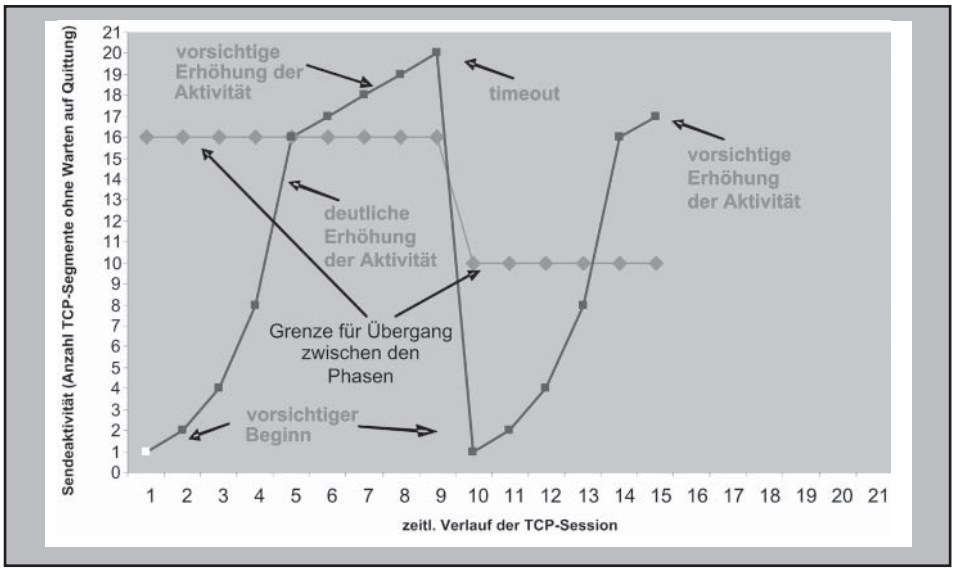

Abbildung 1: Regelung der Sendeaktivität (klassisches TCP)

Neue Flusskontrolle in Vista – 50% mehr Last, Netzwerke in Gefahr?

sprechend wirkt die in TCP von alters her eingebaute Vorsicht in modernen Hochgeschwindigkeitsnetzen eher wie ein „Angstprinzip“. Bloß weil man einmal bremsen musste, ab jetzt ängstlicher weiterfahren? Die Geschwindigkeit auf die Fahrbahnqualität von Autobahnen der 80er Jahre auslegen? Klingt übertrieben, gibt aber das Problem gut wieder: Die Grundannahme, ein Timeout ist ein klares Signal für ein grundlegendes Engpassproblem, lässt sich heute in vielen Situationen nicht mehr aufrecht erhalten:

- beim Zellwechsel im WLAN geht vielleicht das eine oder andere Paket verloren und wird entsprechend nicht quittiert; nach diesem Timeout hat man aber im Bereich der neuen Zelle gleich gute Voraussetzungen wie vorher;

- heilt eine dynamische Redundanz im LAN ein Problem (Timeout-Ursache) auf dem bisher genutzten Übertragungsweg, so steht danach typisch ein gleich guter neuer Weg zur Verfügung, auf dem man sich mit der Daten- und Paketmenge nicht zurückhalten braucht.

Und das Bild mit der Geschwindigkeit passend zur Fahrbahnqualität der 80er Jahre? Geregelt wird die TCP-Übertragungsleistung über das „Congestion Window“, das praktisch als Sliding Window über die zu übertragenden Daten geschoben wird und aussagt, wie viel Datenbytes der Sender als Inhalte aufeinanderfolgender Pakete schicken kann, ohne auf eine Quittung (ACK) durch den Empfänger zu warten. Das macht genauer betrachtet die TCP-Flusskontrolle: sie reguliert zwischen den beiden Extremen „jedes Paket muss einzeln quittiert werden, dann erst geht es weiter“ („ping-pong-TCP“, ganz schlechte Performance!) und „der Sender kann alles ungebremst schicken, was die Anwendung dem IP-Stack an Nutzdaten abgeliefert hat“ (Optimum aus Anwendungssicht). Dabei gibt es von vorneherein eine zulässige „Höchstgeschwindigkeit“, geregelt durch die Aufnahmekapazität, gemeldet vom Empfänger - und für diese Meldung wird vom Empfänger ein bestimmter Wert nie überschritten. Leider ist diese Obergrenze auf ältere Netze ausgelegt: ein Empfänger nach klassischer TCP-Spezifikation meldet niemals eine größere mögliche Window-Größe als 65536 Byte: Nach 64 KB gesendeten Daten muss der Sender bereits warten, bis Quittungen kommen. Angesichts von Netzwerk-Kapazitäten von 100 MBit/s an jedem Endgerät ist das natürlich eine drastische Beschränkung, sobald die Quittungen nicht rasend schnell vom Empfänger zurück kommen: Ist die Round Trip Time (RTT) zwischen Sender und Empfänger nur ein bisschen länger, als der Sender für das Versenden von 64 KB als TCP-Daten benötigt, so ist hier zwangsläufige eine Performance-Bremse gegeben. Selbst im Weitverkehrsbereich ist es heute durchaus möglich, im Rahmen des Bandbreitenangebots mehr als 64 KB unmittelbar auf die Leitung zu bringen …

Also: jawohl, TCP-Flusskontrolle bzw. eine Anpassung an die Gegebenheiten heutiger Netze ist ein wichtiges Thema und ja, Microsoft hat da ein durchaus aktuelles Thema aufgegriffen. Neueste RFCs (z.B. RFC 4653 aus August 2006) beschäftigen sich mit dem Thema der Optimierung von TCP, und auch andere IP-Stack-Lösungen bieten immer wieder Neuerungen in diesem Bereich an: z.B. wird ein Westwood+ genannter spezieller Ansatz unter diversen Linux- und UNIX-Versionen verfolgt, und es wurden gezielt Tests damit auf 10 GBit/s -Verbindungen durchgeführt. Apple kündigt mit OS 10.5 („Leopard“, vorgesehen für Oktober 2007) ebenfalls ein „self-tuning TCP“ an, das flexibler auf die Gegebenheiten im Netzwerk eingehen soll.

Warum aber überhaupt soviel Anstrengungen an diesem Punkt? Es ist absehbar, dass TCP ohne geeignete Optimierungen Investitionen in immer höhere Bandbreiten umso mehr entwerten kann, je größer die Bandbreitenzuwächse sind. Studien und Experimente kommen immer wieder zu dem Ergebnis, dass ohne gezielte Optimierungen am Verhalten von TCP ein deutliches Missverhältnis zwischen Netzwerk-Kapazitäten und erzieltem Nutzen entstehen kann.

Das in Abbilung 2 exemplarisch wiedergegebene Ergebnis einer Untersuchung mit einer Lösung zur Simulation von Netzwerk-Umgebungen zeigt, dass ohne Nutzung optimierender TCP-Optionen (rote Kurve) die Schere zwischen Bandbreitenangebot und mit 100 parallelen TCP-Datenströmen erreichbarer Auslastung immer deutlicher auseinanderklafft. Auf einem 10 GBit/s-uplink schaffen diese 100 Datenströme bei einer RTT von 100 ms lediglich eine Netzauslastung von unter 65%.

In der Praxis kann dies heißen: viel Geld in höhere Bandbreiten investieren – und keiner merkt einen angemessenen Unterschied! Insofern ist es sicher mehr als nur „nett“, wenn ein Hersteller wie Microsoft, der über sein Betriebssystem einen hohen Anteil der IP-Software in heutigen Umgebungen beisteuert, hier Brauchbares anbietet.

Allerdings - jedes Ding hat zwei Seiten. So auch hier: Artikel, die sich auf die entsprechenden Informationen zum neuen Vista-IP-Stack beziehen, warnen zum Teil, man müsse bei Einführung von Vista unbedingt auch Quality of Service einsetzen. Was denn nun: TCP-Tuning als Mittel, um

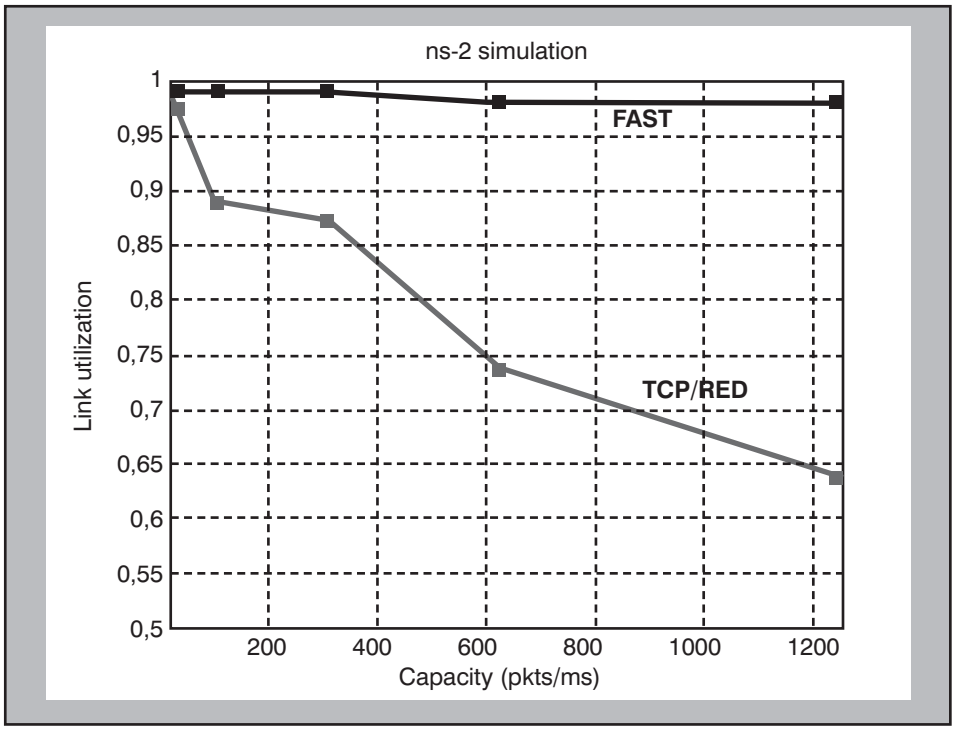

Abbildung 2: Messpunkte bei 155Mbps, 622Mbps, 2.5bps, 5 Gbps, 10 Gbps; 100 ms round trip latency; 100 Flows

Schwerpunktthema

Herausforderung VoIP-Sicherheit

Wie sicher ist die Kommunikation von morgen?

Dr.-Ing. Behrooz Moayeri hat viele Großprojekte mit dem Schwerpunkt standortübergreifende Kommunikation geleitet. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

Fortsetzung von Seite 1

Die auf klassische, auf Time Division Multiplexing (TDM) und Leitungsvermittlung basierende Sprachkommunikation (siehe Abbildung 1) nutzt bisher eine Infrastruktur für Telekommunikation (TK), die bestimmte Merkmale aufweist. Einige dieser Merkmale sind im Folgenden aufgeführt:

- TDM-Netze arbeiten verbindungsorientiert. Dies bedeutet, dass vor jeder Informationsübertragung zunächst explizit eine Verbindung aufgebaut werden muss. Dies Verbindungsaufbauphase (Signalisierungsphase) ist eine geeignete Phase für die Implementierung von Sicherheitsmechanismen. Zum Beispiel können bestimmte Verbindungen aus Sicherheitsgründen verhindert werden.

- Die digitalen TDM-Netze nutzen Out-of-band-Signalisierung. Dies bedeutet, dass die Informationsströme für Sprache und Signalisierung (Nutzdaten und Steuerdaten) über verschiedene Kanäle übertragen werden. Ein Beispiel dafür ist das Integrated Services Digital Network (ISDN), dass zwischen B-Kanälen für Nutzdaten und D-Kanälen für Signalisierung unterscheidet. Der jedem Teilnehmer offen stehende Zugang zum Nutzdatenkanal erfordert nicht unbedingt den Zugang zum Steuerkanal. Die Endteilnehmer können lediglich eingeschränkte Methoden zur Übertragung über Steuerkanäle nutzen, nämlich nur solche Mechanismen, die für den Auf- und Abbau von Verbindungen und für Leistungsmerkmale erforderlich sind.

- TDM-Netze bieten keine Broadcast-Mechanismen. Es ist für die Teilnehmer nicht möglich, Informationen an alle anderen Teilnehmer zu übertragen. Es gibt keinen „Shared-Medium“-Ansatz wie zum Beispiel in einigen für IP genutzten Infrastrukturen wie Wireless Local Area Networks (WLANs). In einem TDM-Netz gibt es statt eines dem Zugriff vieler Teilnehmer ausgesetzten Mediums eine Vielzahl von physikalischen Verbindungen, die explizit und in der Regel von Punkt zu Punkt aufgebaut werden. Das Abhören der Kommunikation ist ohne physikalisches oder elektromagnetisches Wiretapping (Anzapfen) kaum realisierbar.

- In TDM-Netzen gibt es keine Multicast-Mechanismen. Informationen werden in der Regel von Punkt zu Punkt übertragen. Punkt-zu-Mehrpunkt-Übertragung ist nur begrenzt und ausschließlich über spezielle Mechanismen für die Signalisierung von Konferenzen möglich (die nichts anderes sind als die Zusammenschaltung mehrerer explizit aufzubauenden Punkt-zu-Punkt-Verbindungen). Ansonsten gibt es keine „Verzweigungen“ von Informationsströmen, die von Punkt zu Punkt übertragen werden. Das „Kopieren“ von Informationsströmen mittels solcher Verzweigungen ist sehr aufwändig.

- Administratoren von TDM-Netzen nutzen in der Regel proprietäre Management-Mechanismen für den Zugriff auf diese Netze. Diese Mechanismen werden von einem eingeschränkten Personenkreis beherrscht.

Aus den genannten Merkmalen folgt ein bestimmtes Niveau der Sicherheit von klassischer TK. Der Personenkreis, der über das Know-how und die Mittel für die Durchführung von Angriffen auf die klas-

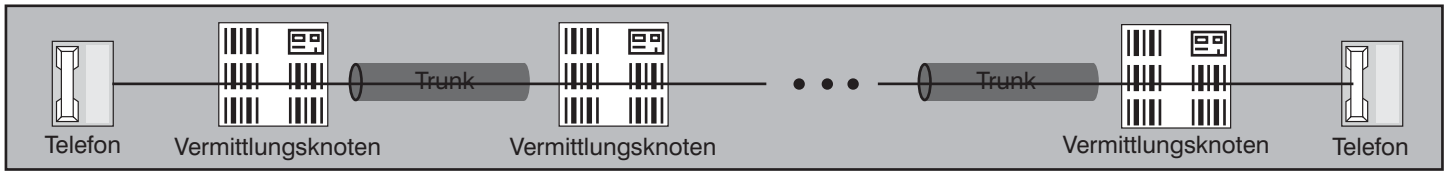

Abbildung 1: Prinzip der Leitungsvermittlung

sische Sprachkommunikation verfügt, ist relativ klein. Die Durchführung solcher Angriffe erfordert eine hohe kriminelle Energie bzw. ein relativ großes Budget. Beispielsweise muss ein Angreifer, der Leitungen anzapfen will, sich physikalisch in die Nähe der Leitungen begeben, die abgehört werden sollen, und entsprechende Tarnmaßnahmen ergreifen, um nicht aufzufallen.

Selbstverständlich haben es jene Angreifer leichter, die einerseits über große Budgets verfügen und andererseits selbst in dem Fall, dass sie „auffliegen“, keine größeren Risiken befürchten müssen. Das gilt zum Beispiel für Geheimdienste, insbesondere im Hoheitsgebiet ihres eigenen Staates oder der „befreundeten“ Staaten. So ist es kein Geheimnis, dass beispielsweise im kalten Krieg sehr teure Abhörstationen betrieben wurden. Es wird berichtet, dass zum Beispiel die Vereinigten Staaten eigens zum Anzapfen von Unterseeleitungen U-Boote entwickelt haben. Es ist auch kein Geheimnis, dass Sicherheitsorgane bestimmter Staaten ihre Abhörsysteme auch für Industriespionage zugunsten der eigenen Volkswirtschaft einsetzen. Aber hinsichtlich der Angriffe auf die TDM-basierende Sprachkommunikation herrscht eine große Asymmetrie. Es gehört zum Allgemeinwissen, dass Staaten in Sachen „Lauschangriffe“ auf ihrem Hoheitsgebiet fast alles können, dass aber ein Abhören gegen den Willen des Staates sehr aufwändig und riskant ist. Nur selten gelingt es anderen als staatlichen Organen, fremde Informationen in bisherigen TK-Netzen anzuzapfen.

Dieses „Allgemeinwissen“ bildet zusammen mit anderen Erkenntnissen über die Sicherheit der klassischen Telekommunikation die weit verbreitetet Erwartungshaltung diesbezüglich. Informationssicherheit besteht vor allem darin, dass man keine „Überraschungen“ erlebt. Nach einer gängigen Definition gilt ein System als sicher, wenn es sich so verhält wie erwartet. Die klassische Telekommunikation ist eine etablierte Technologie, deren Nutzungsrisiken wohl bekannt sind. Nutzer und Service Provider kennen zum Beispiel die Risiken bezüglich des betrügerischen Missbrauchs von TK-Diensten. Ab und zu verhalten sich die TK-Netze doch nicht so wie erwartet, aber im Großen und Ganzen ist das Sicherheitsniveau dieser Netze bekannt. Die Unternehmen meinen zu wissen, wie sie ihre über die TK-Netze übertragenen Informationen vor Mitbewerbern oder der Öffentlichkeit schützen müssen. Staaten wissen die o.g. Asymmetrie zwischen ihren Möglichkeiten und den Möglichkeiten anderer zu ihrem eigenen Gunsten zu nutzen und bringen tendenziell immer mehr Informationen über natürliche und Rechtspersonen in Erfahrung. Bürger der Staaten kennen die Möglichkeiten und die Bestrebungen ihrer Regierungen. Es handelt sich bei der klassischen Telekommunikation um ein System, das wenig Überraschungen aufweist. Das System verhält sich so wie Staaten, Unternehmen und Individuen erwarten, und gilt daher als relativ sicher.

Diese subjektiv empfundene Sicherheit bedeutet trotzdem nicht, dass es keine gravierenden Angriffe auf konventionelle TK gibt. Mit physikalischem Zugang zur Infrastruktur lässt sich im Prinzip alles machen: Man kann ein analoges Telefon als Abhörmikrofon missbrauchen, man kann sich als Mithörer unauffällig einem Gespräch anschließen, wenn man physikalischen Zugriff auf die Infrastruktur erlangt, man kann mit genügend krimineller Energie auf Kosten anderer telefonieren, Verbindungsdaten durch Diebstahl von Daten auslesen, auf mit schwachen Passwörtern abgesicherte Telefonanlagen zugreifen etc. Aber all dies passiert relativ selten.

Wie ist diese Situation mit der Situation in IP-Netzen zu vergleichen? IP-Netze unterscheiden sich in einigen grundlegenden Merkmalen von TDM-Netzen (siehe Abbildung 2):

- IP-Netze arbeiten verbindungslos. Jedes an ein IP-Netz angeschlossene Gerät kann an jedes andere an das selbe IP-Netz angeschlossene Netz Pakete senden, ohne dass vorher explizit eine Verbindung aufgebaut werden muss. Sicherheitsmechanismen während der Verbindungsaufbauphase können nur bei verbindungsorientierten Protokollen wie z.B. TCP (Transmission Control Protocol) angewandt werden, nicht jedoch bei der IP-Übertragung selbst, die keinen expliziten Verbindungsaufbau kennt.

- IP-Netze nutzen Inband-Signalisierung. Nutzdaten und Steuerungsdaten werden über den gleichen Kanal übertragen. Folglich haben alle Nutzer auch Zugang zu dem Kanal, über den Steuerungsinformationen übertragen werden. Diese können daher durch Zugriff auf den einzigen vorhandenen Übertragungskanal manipuliert werden.

- In IP-Netzen werden Broadcast-Mechanismen genutzt, zum Beispiel um zu einer bekannten IP-Adresse die zugehörige Hardware-Adresse zu finden. Local Area Networks (LANs) mit eingebauten Broadcast. Mechanismen werden in Unternehmensnetzen und bei Service Providern genutzt. In diesen Netzen ist das Mithören wesentlich einfacher als in klassischen TK-Netzen.

- IP-Netze nutzen Multicast-Mechanismen, die „Verzweigungen“ von Informationsströmen erfordern. Folglich sind solche „Verzweigungen“ einfach zu steuern, und das „Kopieren“ von Informationsströmen ist relativ einfach möglich, weil die Netzkomponenten dies unterstützen müssen.

- In IP-Netzen werden einfache, standardisierte Management-Mechanismen genutzt. Die Remote-Steuerung von Netzkomponenten ist relativ einfach. Die erforderlichen Werkzeuge dafür sind im

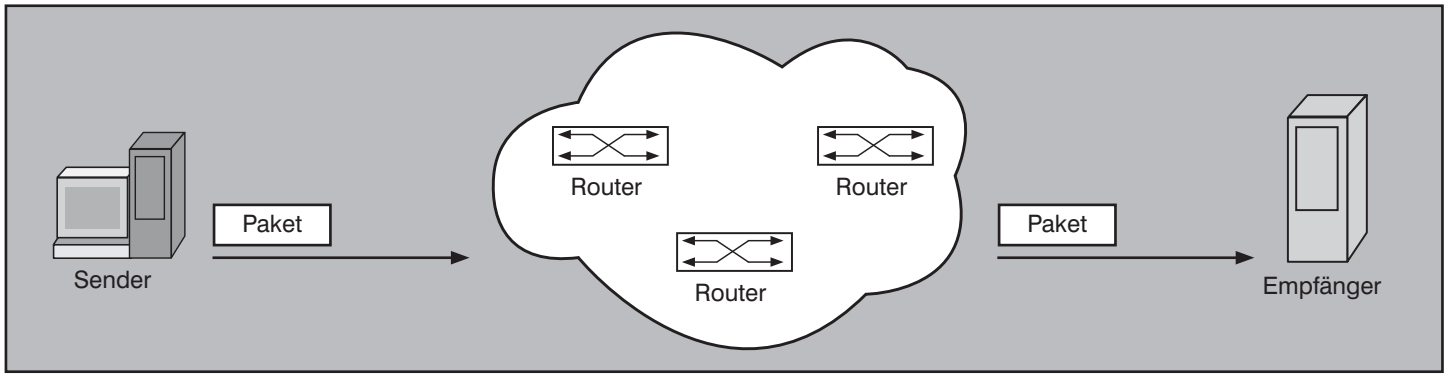

Abbildung 2: Prinzip der Paketvermittlung in IP-Netzen