WissenHeute Jg. 62 11/2009

Das Thema im Überblick

Telekommunikationsnetze sind ein fester Bestandteil des täglichen Lebens geworden. Telefongespräche, SMS (Short Message Service) und E-Mails sind Netzdienste, die für den Nutzer fast zu 100 Prozent verfügbar sind. In diesem Beitrag werden Netzplanungshilfen wie das Verkehrsmodell, Trendanalysen und Marketingprognosen beschrieben. Weiterhin werden z.B. die technischen Voraussetzungen wie Redundanzen, die Anforderungen an die Betriebsphase und die Migration auf ein nachfolgendes Telekommunikationsnetz erklärt.

Planung, Aufbau und Betrieb moderner Telekommunikationsnetze

Telekommunikationsnetze sind keine starren Systeme, die einmalig geplant, aufgebaut und betrieben werden. Vielmehr unterliegen sie einem ständigen Wandel. Änderungen im Nutzerverhalten, eine Zunahme der Verkehrsmenge und der immer schneller werdende technische Fortschritt führen dazu, dass Telekommunikationsnetze stetig erweitert, angepasst und schließlich ausgetauscht werden müssen. In diesem Beitrag wird beschrieben, welche Phasen Telekommunikationsnetze durchlaufen und was bei der Netzplanung zu beachten ist. Er ist eine Ergänzung des Beitrags „Ausfallsicherheit von Telekommunikationsnetzen“, WissenHeute Nr. 2/2009.

Der Autor

Dipl.-Ing. Stefanus Römer studierte Allgemeine Elektrotechnik an der RWTH Aachen und ist als Teamleiter in der zentralen Netzplanung bei T-Mobile Deutschland tätig.

Übersicht Lebenszyklusphasen

Jedes TK-Netz (Telekommunikationsnetz) unterliegt ständig neuen Anforderungen und den sich daraus ergebenden Anpassungen. Die Ursachen hierfür sind in Bild 1 dargestellt:

- Veränderungen des Nutzerverhaltens (aus verschiedenen Gründen)
- technischer Fortschritt
- Optimierungsmaßnahmen im TK-Netz
- Veränderungen in der Kostenstruktur für den Netzbetrieb
- regulatorische Änderungen

Regulatorisch bedingte Änderungen an TK-Netzen werden aufgrund von Vorgaben der Regulierungsbehörden (Bundesnetzagentur) notwendig. Dies können beispielsweise Zugriffssperren auf Internetseiten aus Gründen des Jugendschutzes oder Überwachungen des Datenverkehrs bei behördlichen Ermittlungen sein.

Telekommunikationsnetze durchlaufen verschiedene Lebenszyklusphasen, die denen anderer Produkte gleichen:

- Einführungsphase
- Wachstumsphase
- Sättigungsphase
- Abschwung- und Migrationsphase

Nach der Einführungsphase mit der initialen (anfänglichen) Netzplanung und dem Netzaufbau folgt die Wachstumsphase, in der das ursprüngliche Netz aufgrund steigender Nutzerzahlen und dadurch steigender Verkehrslast ausgebaut wird. Die Wachstumsphase geht in eine Sättigungsphase über. In der Sättigungsphase erreicht das TK-Netz seinen größten Ausbauzustand, der von der Marktsättigung eines TK-Produkts oder Dienstes begrenzt wird. In dieser Phase stehen die Einsparung von Betriebskosten und die Qualitätsverbesserung des Netzes im Vordergrund. Nach der Sättigungsphase folgen die Abschwungphase und danach der Übergang (Migration) auf ein neues TK-Netz (Bild 2). Für dieses neue TK-Netz beginnt dann der Lebenszyklus, bis es wiederum vom nachfolgenden TK-Netz abgelöst wird.

Alle Lebenszyklusphasen sind von folgenden Tätigkeiten und Aufgaben geprägt, wie sie auch in Bild 3 dargestellt sind:

- Netzplanung
- Netzaufbau
- Netzbetrieb
- Netzausbau

Diese einzelnen Tätigkeiten und Aufgaben werden im Folgenden ausführlich beschrieben.

Bild 1 Ursachen der Netzentwicklung

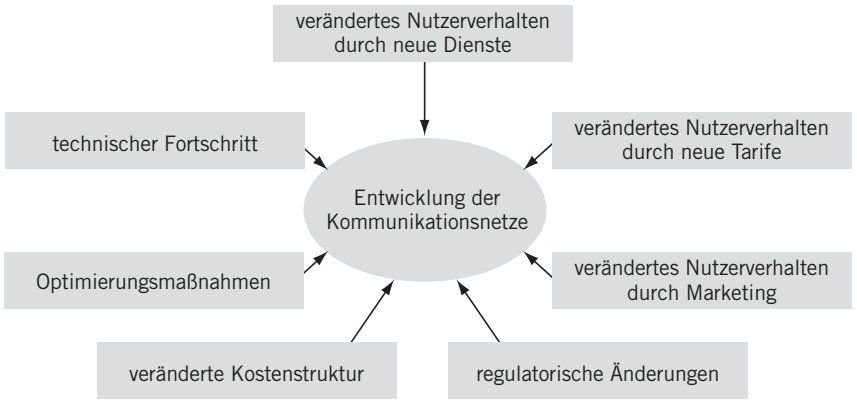


Bild 2 Lebenszyklus eines Telekommunikationsnetzes

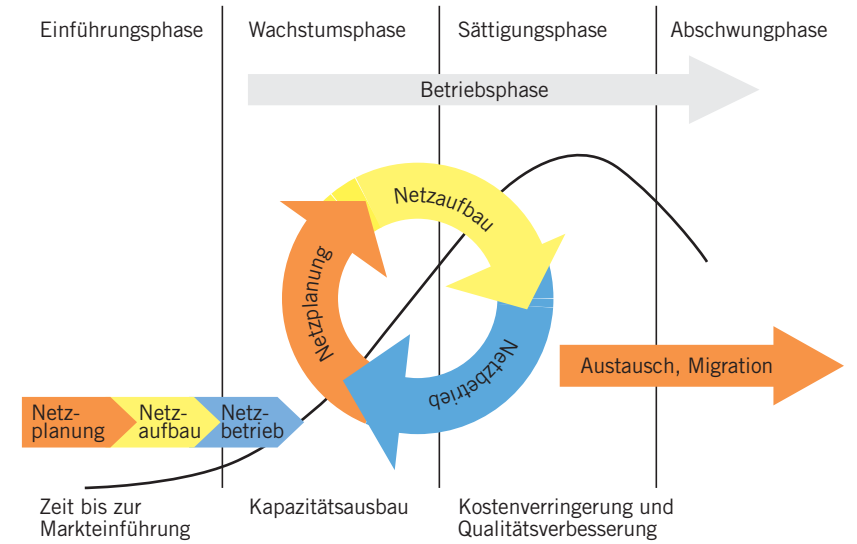


Bild 3 Tätigkeiten in den Lebenszyklusphasen

Netzplanung

Grundlegendes

Die Grundlage für die Einführung eines neuen TK-Netzes ist die initiale Netzplanung, die folgende Aufgaben umfasst:

- Netzdesign
- Netzkonfiguration und Dokumentation
- Kapazitätsplanung

Netzdesign

Die Grundlage für die initiale Netzplanung einer neuen Netztechnik und damit das Netzdesign ist das Engineering (Ingenieurtätigkeit). Das Engineering befasst sich mit technischen Neuerungen und ist für die Planung und die anschließende Bereitstellung einer zuverlässig funktionierenden Netztechnik verantwortlich. Es umfasst die Bereiche:

- Standardisierung
- Technikbewertungen
- Probetests
- Herstellerauswahl
- dokumentierte Abnahme
- Interoperabilitätstests[1]

[1] **Interoperabilitätstest:** Test für die störungsfreie Zusammenarbeit eines Gerätes mit weiteren Teilen eines Systems.

Bild 4 Transportplattform ohne Redundanzen

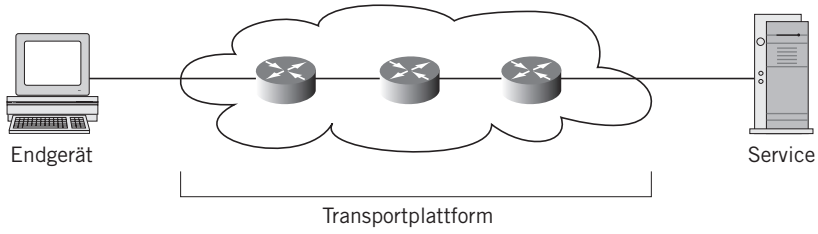
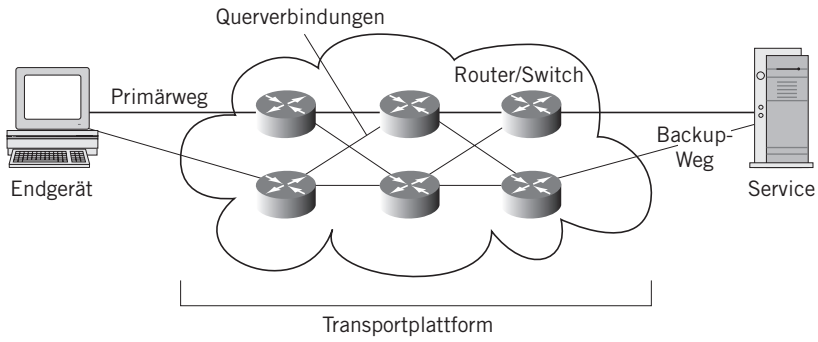


Bild 5 Transportplattform mit Redundanzen



Die Ergebnisse aus dem Engineering fließen in die initiale Netzplanung ein. Die Aufgabe der initialen Netzplanung ist es, ein Netzdesign zu schaffen, das die Anforderungen an das TK-Netz möglichst über den gesamten Lebenszyklus hinweg erfüllt. Dazu gehört beispielsweise vor allem das Einplanen von Redundanzen (Dopplungen der Systemkomponenten), um eine nahezu hundertprozentige Verfügbarkeit des Netzes zu gewährleisten. Bei einem Ausfall des gesamten Netzes kann der Datenverkehr so innerhalb kürzester Zeit von einem anderen Netzknoten übernommen werden. Dies wird auch als „n+1-Konzept“ bezeichnet, wobei für „n“ Netzknoten jeweils ein Backup-Knoten (Backup = Ersatz) bereitgestellt wird.

Weiterhin müssen alle lokalen Verbindungsleitungen (Schicht 2, OSI-Modell = Open Systems Interconnection[2]) zwischen benachbarten Netzknoten gedoppelt sein, was als „1+1-Portredundanz“ (doppelte Schnittstelle) bezeichnet wird. Bei dem Ausfall eines Ports wird der Gesamtverkehr von einem anderen, funktionsfähigen Port übernommen.

Eine weitere Forderung an TK-Netze, die im Netzdesign berücksichtigt werden muss, ist die der getrennten Wegführung zwischen zwei Netzknoten in einem Weitverkehrsnetz (WAN = Wide Area Network[3]): Der Ausfall des Primärwegs (Erstweg) muss sofort durch die Umschaltung auf einen Backup-Weg (Ersatzweg) abgefangen werden.

In Bild 4 ist ein einfaches Modell eines TK-Netzes mit hintereinandergeschalteten Einzelkomponenten ohne Redundanzen dargestellt. Die Verfügbarkeit dieses Gesamtsystems ist wesentlich geringer als die Verfügbarkeit jeder Einzelkomponente. In der Praxis wird dieses Netzdesign nicht verwendet, weil es zu anfällig für Störungen ist. Jede einzelne Komponente bildet hier einen sogenannten SPoF (Single Point of Failure): Der Ausfall einer einzelnen Komponente oder deren Verbindungsleitung bewirkt den Gesamtausfall der Netzdienste. Wie in Bild 5 dargestellt, wird durch den Einsatz von Redundanzen (Dopplungen der WAN-Leitungen mit Primärweg, Backup-Weg und Querverbindungen sowie doppelt ausgelegten Routern[4] und Switchen[5]) erreicht, dass die Dienstverfügbarkeit des gesamten Netzes höher ist als die Verfügbarkeit jeder Einzelkomponente.

Weiterhin muss das Netzdesign die Möglichkeit zur schrittweisen Erweiterung (lineare Skalierbarkeit) bieten, um in allen Lebenszyklusphasen einen schnellen und kostengünstigen Netzausbau zu ermöglichen.

Netzkonfiguration und Dokumentation

Eine weitere Aufgabe der initialen Netzplanung ist die Erstellung und Optimierung einer konsistenten (schlüssigen) und effizienten Netzkonfiguration sowie deren Dokumentation. Die technische Dokumentation der neuen Netztechnik ist besonders wichtig, weil sie die Grundlage für die Kapazitätsplanung und somit für den weiteren Ausbau der Netzkapazitäten bildet. Aufgrund der ständigen Veränderungen im Nutzerverhalten und des Verkehrswachstums muss die initiale Dimensionierung der einzelnen Netzelemente und der Übertragungswege regelmäßig geprüft und durch die Kapazitätsplanung angepasst werden. Wenn erkennbar ist, dass die Schwellwerte der Systemauslastung erreicht oder überschritten werden, muss das TK-Netz ausgebaut werden.

Kapazitätsplanung

Die Kapazitätsplanung wird in allen Phasen eines Lebenszyklus durchgeführt. Sie dient zur Dimensionierung der einzelnen Komponenten des TK-Netzes. Mit der Kapazitätsplanung wird beispielsweise die benötigte Netzleistung in Bezug auf Portzahlen (Port = Schnittstelle) und Übertragungsgeschwindigkeiten ermittelt. Sie bildet damit auch die Grundlage für die in regelmäßigen Abständen vorgenommenen Anpassungen am bestehenden TK-Netz.

[2] **OSI-Modell:** Schichtenmodell der Internationalen Standardisierungsorganisation, das als Designgrundlage von Kommunikationsprotokollen dient.

[3] **WAN:** Weitverkehrsnetzwerk, das entfernte Netzwerke über mehrere Kilometer miteinander verbindet.

[4] **Router:** Komponente zum Verbinden oder Abgrenzen von Rechnernetzwerken.

[5] **Switch:** Netzwerk-Komponente zur Verbindung mehrerer Computer oder Netzsegmente in einem lokalen Netzwerk.

Weil sich die Auslastung des Netzes ständig ändert, ist die Kapazitätsplanung kein einmaliger Vorgang, sondern ein Regelprozess. Das Ziel der Kapazitätsplanung ist es, die Überlastung der Systemressourcen und die für einzelne Netzkomponenten typischen Kapazitätsengpässe frühzeitig vorauszusehen. Die Engpässe kann der Netzbetreiber mithilfe eines Netzmodells unter Berücksichtigung der aktuellen Verkehrsprognose frühzeitig erkennen und durch einen rechtzeitigen Kapazitätsausbau vermeiden. Die Kapazitätsplanung (Bild 6) besteht aus folgenden Teilschritten:

- Verkehrsprognose erstellen
- Verkehrs- und Netzmodell erarbeiten
- Netzsimulation durchführen
- Engpassfaktoren ermitteln
- Anpassungsmaßnahmen planen
- Maßnahmen umsetzen
- Netzauslastung messen (Monitoring)

Die **Verkehrsprognose** liefert Angaben zur Entwicklung der kritischen Kenngrößen aus dem Verkehrsmodell und wird in regelmäßigen Abständen auf der Grundlage der aktuellen Messdaten aus dem TK-Netz und der Marketingprognosen angepasst. Um auf der Grundlage der Verkehrsprognose eine detaillierte Kapazitätsplanung erstellen zu können, ist es notwendig, die Kenngrößen des Kommunikationsverkehrs und ihren Einfluss auf die Auslastung der Netzressourcen zu kennen. Wichtige Kenngrößen in einem Datennetz sind:

- übertragener Datendurchsatz je Verkehrsrichtung (Uplink und Downlink), z.B. in Mbit/s
- Aktivierungsraten, z.B. Verbindungsaktivierungen pro Sekunde
- Anzahl gleichzeitig aktiver Verbindungen
- übertragene Datenmenge oder Datenrate pro aktiver Verbindung
- Signalisierungsverkehr

Aus den Ergebnissen einer Datenverkehrsmessung (Bild 7) werden dazu Trendkurven ermittelt und eine Trendanalyse erstellt. Aus der Trendanalyse lässt sich dann erkennen, wann die jeweilige Kenngröße voraussichtlich an ihre Auslastungsgrenze stoßen wird und zu welchem Zeitpunkt Systemressourcen erweitert werden müssen, um Engpässe im Netz zu vermeiden.

Bild 6 Kapazitätsplanung

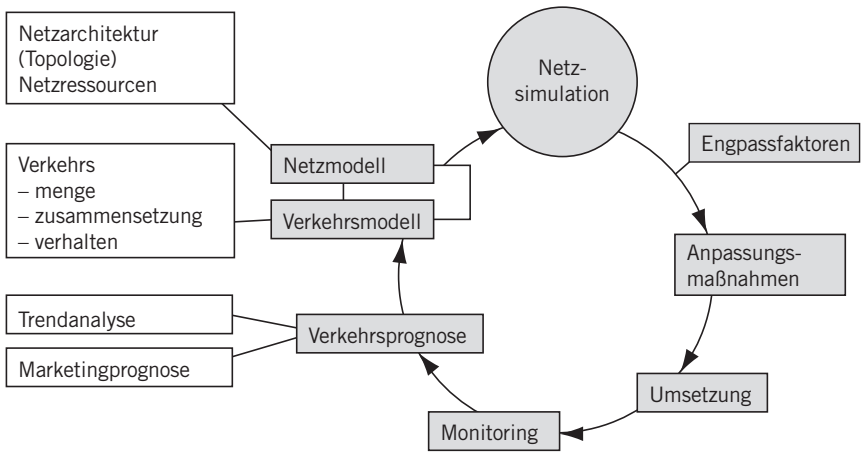
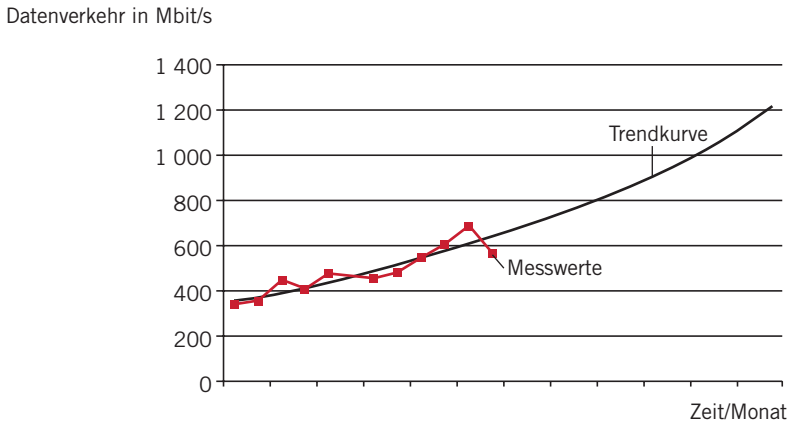


Bild 7 Ergebnis einer Datenverkehrsmessung

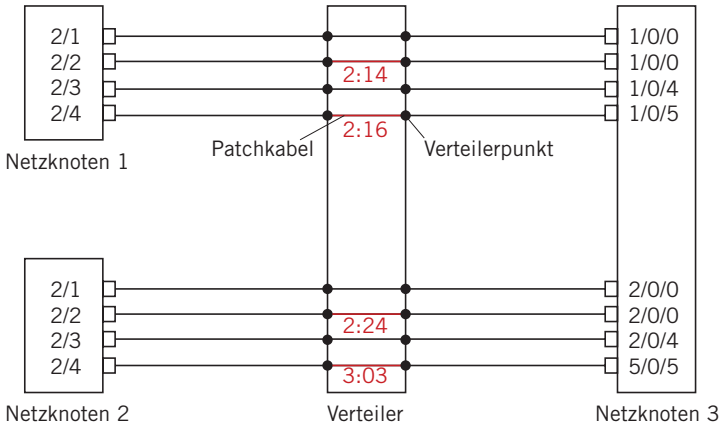


Für die Verkehrsprognose werden vom Marketing der Netzbetreiber zudem in regelmäßigen Abständen eigene Prognosen angefertigt, die die Marktentwicklung, technische Neuerungen oder besondere Verkaufsaktionen aufzeigen. Dabei sind vor allem die Informationen wichtig, die auf eine Änderung der Verkehrszusammensetzung und damit des Verkehrsmodells hindeuten.

Das Verkehrs- und das Netzmodell bilden zusammen mit einer aktuellen Verkehrsprognose die Grundlage für die Kapazitätsplanung. Das Verkehrsmodell beschreibt anhand der Datennetz-Kenngrößen die Zusammensetzung des Verkehrs sowie die Verkehrsverteilung über die einzelnen Netzverbindungen und Einzelkomponenten der verschiedenen Netzknoten.

Zur Erstellung des **Verkehrsmodells** werden Verkehrsmenge, -zusammensetzung und -verhalten fortlaufend gemessen und aufgezeichnet. In der Regel können Messdaten aus einem vergleichbaren, im Wirkbetrieb befindlichen TK-Netz und die Erfahrungswerte der Hersteller genutzt werden, um die Grenzwerte der wichtigen Kenngrößen zu bestimmen. Eine Änderung des Verkehrs-

Bild 8 Verteiler im TK-Netz



TK Telekommunikation

modells führt immer zu einer Änderung der Auslastungsgrenzen und kann eine Verschiebung der kritischen Systemgrößen verursachen.

Das **Netzmodell** ist die Beschreibung des TK-Netzes. Es beschreibt den ursprünglichen Netzplan (Design) und die aktuelle Netzkonfiguration mit ihrer Topologie (Netzarchitektur), den Übertragungs- und Netzknotenressourcen (Prozessoren und Speicher) sowie der Verkehrsverteilung. Das Netzmodell wird ständig aktualisiert, um es an die Netzänderungen anzupassen.

Das Netz- und Verkehrsmodell sind die Grundlagen, um die kritischen **Engpassfaktoren** wie Übertragungswege, CPU-Last (Central Processing Unit) oder Speicherausnutzung mithilfe einer **Netzsimulation** ermitteln zu können. Die Netzsimulation liefert Informationen, mit denen Grenzanalysen erstellt werden, die den Einfluss der Kenngröße auf die Systemressourcen aufzeigen. Daraus ergeben sich die Auslastungsgrenzen der Komponenten für alle Kenngrößen. Die Engpassfaktoren können zusätzlich mit realen Lasttests im Labor geprüft werden. Dadurch ist erkennbar, welche Systemgrößen bei einer gleichmäßigen Zunahme des Verkehrs zuerst an ihre Belastungsgrenze stoßen.

Ein unsicherer Faktor bei der Kapazitätsplanung ist die Verkehrsverteilung. Weil sich der Verkehr im Wirkbetrieb nicht gleichmäßig über alle Netzressourcen (Verbindungswege, Netzknoten oder Einzelkomponenten innerhalb eines Netzknotens) verteilen lässt und sich die Verkehrsverteilung auch ständig ändert, werden einige Komponenten stärker belastet und dadurch früher als geplant an ihre kritische Belastungsgrenze stoßen, während im Gesamtnetz noch genügend freie Übertragungskapazität vorhanden ist.

Ein fortlaufendes **Monitoring** (Überwachung eines Vorgangs) der Netzlast stellt zusammen mit den Trendanalysen sicher, dass die Kapazitätsplanung und die tatsächliche Auslastung der Netzressourcen ständig miteinander abgeglichen werden und ein bedarfsgerechter Ausbau ohne Überkapazitäten vorgenommen werden kann.

Netzaufbau

Die Netzplanung bestimmt die Ausbauplanung in der Auf- und Ausbauphase des TK-Systems. Dies umfasst den physikalischen Aufbau der einzelnen Netzknoten, der sich in folgenden Schritten vollzieht:

- Auswahl der Betriebsstätte
- Erstellen der Netzverkabelung
- Einrichten der WAN-Verbindungen
- Einbinden der Anlage in das vorhandene TK-Netz (Integration)

Die Gewährleistung eines störungsfreien Wirkbetriebs von TK-Netzen beginnt mit der Auswahl einer geeigneten Betriebsstätte, die eine stabile Stromversorgung liefern kann und die Klimabedingungen erfüllt, die für EDV-Anlagen (elektronische Datenverarbeitung) notwendig sind, wie z.B. bestimmte Temperaturen und Luftfeuchtigkeit. Die Betriebsstätte muss dauerhaft folgende Bedingungen für einen ausfallsicheren Betrieb der Netzinfrastruktur sicherstellen:

- redundante, stabile Stromversorgung über getrennte Energieversorgungssysteme
- Notstromaggregate, Überspannungsschutz und stabile Netzfrequenz
- redundante Klimaanlage
- thermische Brandfrüherkennungssysteme mit zentraler Alarmierung
- getrennte Brandabschnitte für redundante Netzkomponenten
- Zugangskontrolle und Objektschutz

Nach der Auswahl der Betriebsstätten beginnt die Detailplanung. Hierzu müssen der Flächenbedarf und die genauen Anforderungen an die Strom- und Klimaversorgung vorliegen. Dafür sind die folgenden Punkte zu klären:

- Spannungsquellen (z.B. 230 V Wechselspannung oder 48 V Gleichspannung)
- Stromzuführung (einfach oder doppelt)
- Leistungsaufnahme
- Abwärmemenge

Sind diese Punkte geklärt, wird eine Portliste erstellt. In der Portliste wird festgelegt, mit welchem Kabeltyp (Kupfer- oder Glasfaserkabel) die Netzkomponenten innerhalb der Betriebsstätte miteinander verbunden werden (Schicht 1, OSI-Modell).

Hieraus ergibt sich der Verkabelungsplan, der angibt, über welche Verteilerpunkte die Verkabelung geführt wird. In der Regel werden kommunizierende Systeme nicht direkt miteinander verkabelt. Die Verbindungen zwischen einzelnen Systemen des Netzes werden über Unterverteiler und einen zentralen Verteiler (Bild 8) hergestellt (Patchen). Durch diese zentrale Struktur können alle Systeme beliebig miteinander verbunden werden.

Die einzelnen Netzknoten bestehen in der Regel wiederum aus vielen verschiedenen Einzelkomponenten, die in der Betriebsstätte aufgebaut werden müssen. Erst nachdem die Stromversorgung angeschlossen ist und der Netzknoten den Selbsttest aller Komponenten fehlerfrei bestanden hat, beginnt das Patchen zu den weiteren Systemkomponenten. Der letzte Schritt ist die Integration in das gesamte TK-Netz.

Nach Abschluss der Aufbau- und Verkabelungsarbeiten werden alle Kabelverbindungen mit einem Schleifentest auf Vertauschungen von Sende- und Empfangsleitungen geprüft. Hierzu werden jeweils die Sende- und die Empfangsleitung eines Ports an dem jeweiligen Verteilerpunkt miteinander verbunden. Danach wird vom angeschlossenen Netzelement ein Signal über die Sendeleitung geschickt. Es wird geprüft, ob dieses Signal über die Schleife auf der Empfangsleitung zum gleichen Port am jeweiligen Netzelement zurückkommt.

Danach werden die höheren Layer (Schicht 2 bis 7, OSI-Modell) des TK-Netzes in Betrieb genommen. Dies umfasst in der Regel die Verbindungen über die Weitverkehrsnetze zwischen den Endsystemen an getrennten Standorten. Hierzu ist es notwendig, im Vorfeld eine Weitverkehrsverbindung mit ausreichender Bandbreite bereitzustellen und zu konfigurieren. Jede einzelne WAN-Verbindung muss vor der Inbetriebnahme des TK-Netzes geprüft werden. Häufig werden die WAN-Verbindungen über einen IP-Backbone[6] geführt, wobei die Verbindungen im Backbone geroutet[7] und mit Firewall-Eintragungen[8] gefiltert werden. Um diese Verbindungen zu testen, werden Ping-Pakete[9] zur jeweiligen Gegenstelle (Host) geschickt, die innerhalb von wenigen Millisekunden beantwortet werden müssen. Die Antwortzeiten moderner TK-Netze liegen zwischen 20 ms und 50 ms. In Bild 9 sind die Ausgabewerte des Ping-Befehls mit der Ziel-IP-Adresse und den Paketlaufzeiten dargestellt. Die Ping-Befehlsoptionen sind in Kasten 1 mit der Befehl-Syntax zusammengefasst. Der Ping-Befehl wird von der Anwendung Eingabeaufforderung ausgeführt.

Bild 9: Verbindungstest mit dem Ping-Befehl

Kasten 1 — Syntax der Ping-Befehlsoptionen

Syntax: ping [-Option]

Optionen:

[-t]	sendet fortlaufend Ping-Pakete zum Ziel-Host
[-a]	löst Adressen in Hostnamen auf
[-n]	Zahl der zu sendenden Echoaufforderungen
[-l]	sendet die Pufferlänge
[-f]	setzt Flag[10] für „nicht fragmentieren“ (stückeln) im Paket (nur IPv4 = Internet Protocol Version 4)
[-i]	Gültigkeitsdauer (TTL = Time To Live)
[-v]	Diensttyp (TOS = Type Of Service), (nur IPv4)
[-r]	Route für Anzahl der Abschnitte (nur IPv4)
[-s]	Zeiteintrag für Anzahl der Abschnitte (nur IPv4)
[-j]	„Loose Source Route“ nach Hostliste (nur IPv4)
[-k]	„Strict Source Route“ nach Hostliste (nur IPv4)
[-w]	Zeitlimit in Millisekunden für eine Rückmeldung
[-R]	verwendet den Routing-Header[11], um die rückwärtige Route zu testen (nur IPv6 = IP Version 6))
[-S]	zu verwendende Quelladresse (nur IPv6)
[-4]	erzwingt Verwendung von IPv4

Zur Fehlereingrenzung, wie z.B. einer fehlerhaften Konfiguration im Backbone, wird der Systembefehl „tracert“ genutzt, der in Bild 10 dargestellt ist. Mit diesem Befehl werden nacheinander kleine Testpakete entlang der gesamten Übertragungskette an den jeweils nächsten Router geschickt, die ebenfalls in wenigen Millisekunden beantwortet werden müssen. Auf diese Weise lässt sich herausfinden, an welcher Stelle die Übertragungskette zwischen den Endsystemen fehlerhaft ist. Eine Übersicht der Tracert-Befehlsoptionen und ihrer Syntax ist in Kasten 2 dargestellt.

Um nach der Inbetriebnahme der höheren OSI-Layer des Netzes eine Beeinträchtigung des Daten- und Gesprächsverkehrs der Kunden gering zu halten, kommen Netzsimulatoren und Testsysteme zum Einsatz, die die Partnersysteme vollständig nachbilden und damit Fehler vor der Inbetriebnahme des neuen Netzes erkennen.

6 **IP-Backbone:** Basisnetz mit hohen Übertragungsraten als Teil eines Netzwerks auf Grundlage des Internet-Protokolls.

7 **Routing:** Vermitteln von Datenpaketen in IP-Netzen.

8 **Firewall:** Beschränkt den Datenzugriff zwischen Netzen.

9 **Ping-Paket:** Elektronisches Datenpaket, um eine Gegenstelle im IP-Netz anzusprechen und die Laufzeit des Paketes zu ermitteln.

10 **Flag:** Binäre Variable zur Kennzeichnung von Systemzuständen.

11 **Routing-Header:** Kopf eines IP-Paketes, der die Informationen Absender, Empfänger, Typ und Lebensdauer enthält.

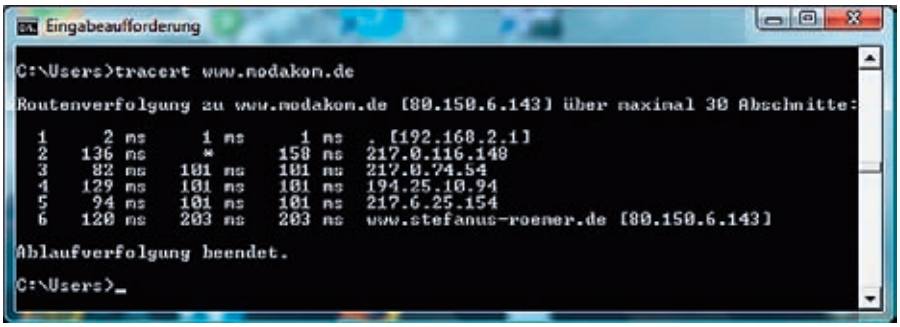


Bild 10: Verbindungstest mit dem Tracert-Befehl

Kasten 2 Syntax der Tracert-Befehlsoptionen

Syntax: tracert [-Option]

Optionen:

[-d]	löst Adressen nicht in Hostnamen auf
[-h]	maximale Zahl an Abschnitten bei der Zielsuche
[-j]	„Loose Source Route“ nach Hostliste (nur IPv4)
[-w]	Zeitlimit in Millisekunden für eine Antwort
[-R]	verfolgt Rundwegpfad (nur IPv6)
[-S]	zu verwendende Quelladresse (nur IPv6)
[-4]	erzwingt die Verwendung von IPv4
[-6]	erzwingt die Verwendung von IPv6

Netzbetrieb und Netzausbau

Grundlagen

Die Betriebsphase hat die Aufgabe, durch vorsorgliche und reaktive Maßnahmen die Ausfallzeit des Netzes bei Störungen gering zu halten. Dazu ist es notwendig, möglichst alle Störereignisse vor der Betriebsphase zu erfassen und nach Art (Kategorie) und Wichtigkeit (Priorität) einzustufen. Störereignisse müssen automatisch und schnell erkannt und behoben werden. Jedes Störereignis löst abhängig von seiner Priorität in jeder Betriebsphase festgelegte Teilprozesse aus, die weitere dokumentierte Maßnahmen zur Entstörung veranlassen. Störungskategorien werden anhand ihrer Störungswirkbreite definiert: Die Störungswirkbreite einer Störung gibt beispielsweise an, wie viele Kunden von einer Störung im Netzwerk betroffen sind oder wie viel Umsatz pro Zeiteinheit durch eine Störung verloren geht. Die Störungswirkbreite erfasst auch die Kosten, die dem Netzbetreiber durch eine Störung entstehen. Je höher die Störungswirkbreite einer Störung ist, desto höher ist ihre Priorität. Eine hohe Störungspriorität erfordert einen hohen Automatisierungsgrad bei der Störungsbehebung, um die Entstörzeit und den dadurch entstehenden finanziellen Verlust für den Netzbetreiber gering zu halten.

Pilotbetrieb

Trotz sorgfältiger Netzplanung und systematischer Funktionstests des neuen Netzes können Störungen im Wirkbetrieb nicht ausgeschlossen werden. Aufgrund der Komplexität moderner TK-Netze ist es nicht möglich, alle Betriebszustände zu erfassen und in einer Laborumgebung nachzustellen. Daher können im Wirkbetrieb immer noch unvorhersehbare Betriebsstörungen auftreten. Ein typisches Beispiel sind schwer erkennbare Störungsursachen wie Speicherüberlaufe bei Systemkomponenten. Diese Störungen treten auf, wenn dynamische Speicherbereiche während des Betriebs der TK-Anlage nicht mehr freigegeben werden. Daher werden neue TK-Anlagen nicht sofort unter Volllast betrieben, sondern zunächst im Rahmen einer Pilot- und Stabilisierungsphase mit verminderter Verkehrslast erprobt, um möglichst viele Störungen im späteren Wirkbetrieb auszuschließen.

Die Einführung einer neuen TK-Anlage geschieht stufenweise in verschiedenen Phasen. Im Vordergrund steht dabei, Beeinträchtigungen im Wirkbetrieb für die Kunden weitestgehend zu vermeiden. Daher wird die neue Anlage im gesamten Telekommunikations- und Abrechnungssystem zunächst mit einem simulierten Testverkehr betrieben. Erst wenn sich keine Auffälligkeiten zeigen, wird stufenweise immer mehr Kundenverkehr auf die Anlage gelenkt. Danach wird die Anlage über einen längeren Zeitraum unter Volllast betrieben. Wenn die Anlage dann störungsfrei läuft, beginnt der Regelbetrieb. Die Pilotphase im Überblick:

- Prüfung der End-2-End- und Abrechnungskette mit Testverkehr (End-2-End = Ende-zu-Ende)
- Prüfung der End-2-End- und Abrechnungskette mit wenig Kundenverkehr
- stufenweise Steigerung der Verkehrslast
- Langzeitbeobachtung unter Volllast (Stabilitätsprüfung)

Regelbetrieb

In der Regelbetriebsphase, die nach Abschluss der Pilotphase beginnt, wird die neue TK-Anlage unter Volllast betrieben. Die Managementaufgaben im Regelbetrieb gliedern sich in sechs Bereiche:

- Incident-Management
- Problemmanagement
- Change-Management
- Konfigurationsmanagement
- Performance-Management
- Sicherheitsmanagement

Im Rahmen des **Incident-Managements** (Vorfallmanagement) werden Störungen im TK-Netz bearbeitet. Jede Funktionsstörung oder ein Überschreiten vordefinierter Schwellwerte wird automatisch dem Betriebspersonal gemeldet, das die Störungen in 24-stündiger Bereitschaft annimmt und behebt. Das Betriebspersonal bearbeitet die Störereignisse entsprechend ihrer Kategorie und Priorität nach festgelegten Entstörprozessen. Diese beschreiben die Informationskette zu jedem Störereignis und regeln, ob kurzfristige Entstörmaßnahmen zu ergreifen

sind. Zu jedem Störereignis wird ein Fehlerreport (Bericht) angelegt, der vom Problemmanagement für das Erstellen einer Fehleranalyse benötigt wird.

Das **Problemmanagement** beginnt nach Abschluss des Entstörprozesses. Seine Aufgabe ist es, die Ursache der aufgetretenen Störung zu analysieren und ein erneutes Auftreten zu verhindern. Häufig werden Störungen im Netz durch kurzfristige Umschaltmaßnahmen (Workaround) auf redundante Systemkomponenten vorübergehend beseitigt, ohne die technische Ursache zu beheben. Die Fehleranalyse im Problemmanagement kann beispielsweise ergeben, dass ein Softwareproblem vorliegt, das nur mit einem Software-Patch[12] des Anlagenherstellers vollständig zu beheben ist.

Das **Change-Management** legt fest, wie Netzänderungen durchgeführt werden. Aufgabe des Change-Managements ist es, den Vorgang zur Umsetzung von Netzänderungen festzulegen und einen Nachweis der anschließenden störungsfreien Funktion zu erstellen. Störereignisse treten häufig auf, wenn Änderungen vorgenommen werden. Sie müssen unmittelbar erkannt und behoben werden. Sollten sich diese Störungen nicht innerhalb einer vordefinierten Zeit beheben lassen, so muss über eine Rückfallprozedur (Fall-Back) der Zustand vor der Änderung wiederhergestellt werden können. Um das Störungsrisiko und die Störungswirkbreite bei einer Netzänderung gering zu halten, gelten die folgenden Prinzipien:

- Prinzip der singulären (einzelnen) Änderung: In einem Wartungsfenster wird nach Möglichkeit immer nur eine Änderung durchgeführt, um die Ursachen für mögliche Störungen gering zu halten.
- Prinzip der Verkehrsminimierung: Wenn technisch möglich und vom Aufwand vertretbar, werden betroffene Netzelemente vor der Änderung verkehrsfrei geschaltet.
- Prinzip des kontrollierten Rückfalls (Fall-Back): Über eine Rückfallprozedur wird sichergestellt, dass der ursprüngliche Systemzustand schnell wieder hergestellt werden kann.
- Test der Change- und Rückfallprozedur in einer Referenz-Testanlage.

Große TK-Netze sind technisch anspruchsvolle Systeme mit vielen verschiedenen Komponenten unterschiedlicher Hersteller. Die Konfiguration dieser Komponenten muss untereinander abgestimmt sein. Die Aufgabe des **Konfigurationsmanagements** ist es, den aktuellen Konfigurationsstand aller Netzkomponenten zu dokumentieren und jederzeit frühere Konfigurationsstände im Netz aktivieren zu können. Hierzu ist nicht nur die Konfiguration mit allen Parametern (Systemwerte) erforderlich, sondern es müssen auch die Systembefehle der Netzkomponenten und ihre Programmierreihenfolge bekannt sein. Eine weitere Aufgabe ist die Konfiguration von kurzfristigen Lösungen (Workaround) zum Beheben einer Störung.

Die Aufgabe des **Performance-Managements** ist es, kurzfristig auftretende Kapazitätsengpässe einzelner Netzbereiche zu erkennen. Wichtige Systemparameter wie die CPU-Auslastung oder der Datendurchsatz der WAN-Verbindungen werden regelmäßig ausgewertet, um Engpässe zu erkennen und damit Beeinträchtigungen in der Netzqualität zu vermeiden.

Das **Sicherheitsmanagement** regelt den Zugang zu den einzelnen Netzkomponenten und deren Managementsystemen. Hierzu kommen in Abhängigkeit des Schutzbedarfes der Einzelkomponenten verschiedene organisatorische und technische Maßnahmen zum Einsatz.[13] Wichtige Bestandteile des Sicherheitsmanagements sind der Zugangsschutz zu den Betriebsstätten und die Verwaltung von Zugangskennungen und Zugangsberechtigungen (Account-Management). Hierzu zählt auch der Einsatz von Passwörtern. Die Passwörter müssen Richtlinien, z.B. in Bezug auf Länge und Zeichenart, entsprechen und in regelmäßigen Zeitabständen geändert werden. Das Account-Management muss sicherstellen, dass der Zugang zu den Systemen nur den jeweils autorisierten Mitarbeitern gewährt wird. Die Zugangsdaten der Mitarbeiter, die ihre innerbetriebliche Organisationseinheit oder das Unternehmen verlassen, müssen umgehend gesperrt werden.

Verwendete Abkürzungen

CPU	Central Processing Unit
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
OSI	Open Systems Interconnection
SPoF	Single Point of Failure
TK	Telekommunikation
TOS	Type of Service
TTL	Time to Live
WAN	Wide Area Network

Ausnahmebetrieb

Der Ausnahmebetrieb ist eine Abweichung vom Regelbetrieb, bei dem spezielle Maßnahmen eingesetzt werden, um besondere Betriebszustände zu beheben. Der Ausnahmebetrieb wird in folgenden Situationen notwendig:

- Ausfall eines gesamten Netzknotens durch Störungen der lokalen Infrastruktur, der nicht innerhalb einer vertretbaren Zeit zu beseitigen ist (Desaster-Fall).
- Überlast eines Netzknotens oder des gesamten TK-Systems, die nicht durch freie Redundanzen zu beheben ist.

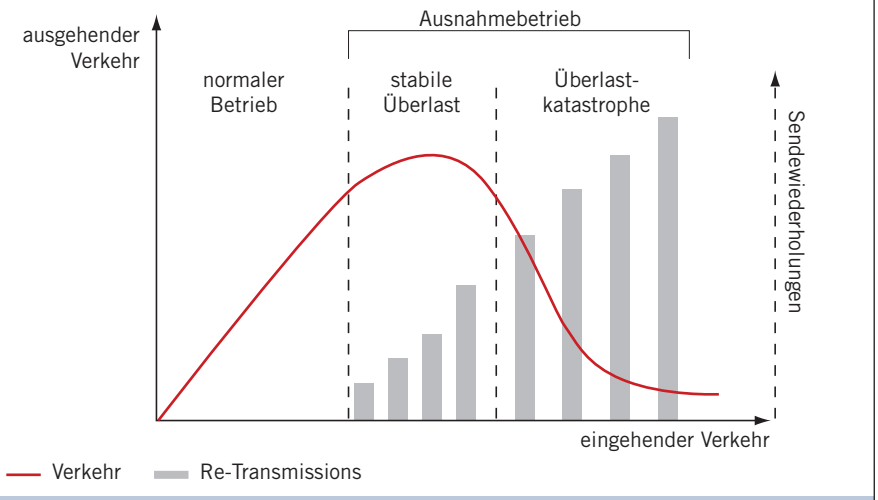
Für beide Szenarien gibt es Notfallpläne, die Maßnahmen und die Reihenfolge ihrer Bearbeitung zur Störungsbehebung festlegen. Im Desaster-Fall muss möglichst schnell eine Verkehrsumleitung auf einen Reserveknoten vorgenommen werden. Bei dieser Umschaltung werden zeitlich festgelegte und koordinierte Konfigurationsänderungen im Weitverkehrsnetz und auf den betroffenen Endknoten durchgeführt.

Im Fall einer Überlast im gesamten TK-Netz wird mit einer Lastabwehr reagiert, die verhindert, dass die überlasteten Netzkomponenten durch weitere Verkehrsdaten zusätzlich verlangsamt werden oder vollständig

[12] **Software-Patch:** Neue Software-Version eines Herstellers, die Fehler in früheren Versionen behebt oder weitere Leistungsmerkmale bietet.

[13] www.bsi.bund.de („IT-Grundschutz“, Bundesamt für Sicherheit in der Informationstechnologie)

Bild 11 Betriebszustände eines Telekommunikationssystems



„zusammenbrechen". Die zu ergreifenden Maßnahmen hängen wesentlich vom jeweiligen TK-System ab. Mögliche Lastabwehrstrategien sind beispielsweise:

- Verlangsamung der Übertragungsgeschwindigkeit
- Abweisung neuer Verbindungsanforderungen
- Lastabwurf (aktive Verbindungen werden zwangsweise unterbrochen)

Alle genannten Maßnahmen können direkt auf den Gesamtverkehr oder abgestuft auf Teile des gesamten Verkehrsaufkommens angewendet werden, z.B. für bestimmte Nutzergruppen, Zugangsnetze oder Anwendungsprotokolle wie Peer-to-Peer[14] oder Streaming[15].

Mit einer abgestuften Lastabwehr wird die sogenannte Überlastkatastrophe (Bild 11) vermieden. Dabei vermindert sich die Verarbeitungskapazität des Systems nach Überschreiten der Lastgrenze, an der das System mehr mit Sendewiederholungen (Re-Transmissions) beschäftigt ist, als damit, die Verkehrsdaten zu transportieren. Es besteht die Gefahr eines „Dominoeffektes", wenn sich der Verkehr vom überlasteten Netzknoten auf andere Netzknoten verteilt und dadurch auch diese in den Bereich der Überlast bringt. Die Verkehrslast kann in diesem Zustand des Netzes nicht mehr verarbeitet werden. Das Überlastverhalten eines Systems hängt grundlegend von seiner Architektur ab und kann im Extremfall dazu führen, dass ab einer bestimmten Lastschwelle fast kein externer Verkehr mehr verarbeitet werden kann und es zu einem vollständigen Netzausfall kommt.

Referenzanlage

Um einen stabilen Wirkbetrieb eines TK-Netzes zu gewährleisten, wird im Labor eine Referenzanlage aufgebaut. Die Referenzanlage ist so ausgelegt, dass sie den Wirkbetrieb möglichst vollständig nachbildet.

Häufig werden im Pilot- und Regelbetrieb weitere Fehler in der Anlagensoftware entdeckt, die durch Software-Patches behoben werden müssen. Diese Patches werden mit der Referenzanlage im Labor auf weitere Fehler geprüft, bevor sie aktiviert werden.

Auch besondere Betriebszustände wie ungeklärte Verbindungsausfälle oder Routing-Probleme können im Rahmen des Problemmanagements auf der Referenzanlage nachgestellt und analysiert werden. Im Wirkbetrieb ist dies nicht sinnvoll, weil es die Netzleistung einschränkt und dadurch den Kundendatenverkehr beeinträchtigen kann.

Die Referenzanlage wird auch für das Change-Management benötigt, um die Change- und die Rückfallprozedur zu testen.

Migration und Abbau des Altsystems

Im Anschluss an die Wachstums- und Sättigungsphase eines TK-Netzes wird die Anlage durch eine Nachfolgetechnik ausgetauscht (Migration). Das Umschalten auf die neue Anlage findet im laufenden Betrieb statt, wobei die Migration für die Kunden keine Beeinträchtigung in der Verfügbarkeit der Netzdienste oder Qualitätseinbußen zur Folge haben darf.

Zum Ende der Lebenszyklen von TK-Netzen kommt es darauf an, durch Kosteneinsparungen und Qualitätsverbesserungen die bestehenden Netze noch möglichst lange zu betreiben und gleichzeitig die Migration auf eine Nachfolgetechnologie vorzubereiten, um nicht unnötig früh in eine neue Technik investieren zu müssen. Weiterhin bleibt dem Netzbetreiber dadurch ausreichend Zeit, die Kunden auf eine neue Netztechnik vorzubereiten und die Kundenbindung z.B. durch Werbemaßnahmen für neue Leistungsmerkmale zu erhöhen.

Die Migration von TK-Netzen ist ein sehr komplexer Vorgang, weil die bestehende und die neue Technik in der Migrationsphase parallel (nebeneinander) betrieben werden müssen, um den Kundenverkehr schrittweise auf das neue System zu verlagern. Die Altanlagen werden so lange betrieben, bis das neue System in einer hinreichend langen Stabilisierungsphase unter Volllast störungsfrei funktioniert hat. Für diesen Zeitraum müssen die Altanlagen jederzeit für einen Rückfall (Fall-Back) zur Verfügung stehen.

Mit der Migration und dem Abbau des Altsystems ist der Lebenszyklus des alten TK-Netzes abgeschlossen und es beginnt der Betrieb der neuen Netztechnik, die zuvor bereits geplant wurde. *(GI)*

Internetadressen

www.itil.org (entnommen 04.08.2009)
www.bsi.bund.de (entnommen 24.09.2009)

[14] **Peer-to-Peer:** Durch ein TK-Netz geschaltete Punkt-zu-Punkt-Verbindung.

[15] **Streaming:** Datenstrom als kontinuierliche Abfolge von elektronischen Daten.