

Netzwerke mit Zukunft

Entwicklung von Kommunikation
Anforderungen an IT-Infrastrukturen

Herbert Almus



TU Berlin / EANTC AG



EANTC Labor

FSP-PV:

Forschungszentrum für
Netzwerktechnologien und Multimedia-
Anwendungen

1991 Eröffnung des EANTC als Testcenter
für FDDI, seit 1993 Test Center für ATM

EANTC AG:

Ausgründung aus der TU Berlin (November 99)

Erste AG mit Beteiligung der TUB (10% Grundkapital)

Hoch spezialisierter Dienstleister im Bereich Netzwerke
(insbesondere neue Technologien Protokolle, QoS)

Kommunikation aktuell



- dpa-Meldung:
Meilenstein in der
Medizintechnik (2001)



- Erste Fern-OP per Roboter
 - Mediziner in New York haben einer 68-jährigen Frau in Straßburg die Gallenblase entfernt. Möglich wurde die erste transatlantische Operation durch "Zeus", einen ferngesteuerten Roboter. Das berichten die Mediziner des Mount Sinai Medical Center New York in der Fachzeitschrift "Nature". Die OP habe eine Stunde gedauert und sei komplikationslos verlaufen.

Kommunikation im Wandel



- **Neue** Arbeitsplätze
 - Weitere Trend zu Heim- und Fernarbeit
 - EU: 10 Mio. Menschen in 2000
 - Verfünfachung seit 1994
 - Europäisches „Durchschnittsbüro“ ist nur zu 8% besetzt.



- Innovative Arbeitsplatzgestaltung
 - Werkzeuge für flexiblere und mobile Arbeit
 - Virtuelle Umgebungen für Teamarbeit

IP im Alltag?



- Facility Management über IP
 - Verwaltung von Ressourcen per IP-Protokoll
 - Microcontroller-gesteuerte Smart-IP Endgeräte werden mit dem LAN verbunden und kommunizieren über das Internet-Protokoll
 - Beispiel Raumvergabe:
 - IVISTAR-Room Resourcing / LCD-Türschilder



Kommunikation im Wandel



- Intelligente Fertigung
 - Bessere Integration der Produktionsprozesse
 - Integration bestehender Bus-Systeme in ein Gesamtnetz / IP-Anbindung
 - Direkter Einsatz von IP-Protokollen in Steuerungsprozessen
 - Gemeinsames Engineering von Firmen
 - Kooperative Entwicklungswerkzeuge
 - Erweiterte multimediale Kommunikation



Kommunikation im Wandel



- Umgang mit multimedialen Dokumenten
 - Neue Standards (z.B. MPEG-7) erlauben qualitativ neue, interaktive Multimedia-Anwendungen
 - Abruf multimedialer Information wie heute für Textinformation
 - MM-Editoren erlauben Objekte in Datenbanken zu identifizieren / auszuwählen
 - Grundlage für Entwicklung und Anwendungen in vielen Industriezweigen
 - Rundfunk und Musikindustrie
 - Digitale Bibliotheken und Archive



Kommunikation im Wandel



- Die **neuen** Universitäten
 - Neue Formen der Erstellung von Lehrmaterialien
 - Gemeinsame, verteilte Produktion
 - Modularisierung ermöglicht Nutzung von Komponenten in unterschiedlichen Lerneinheiten
 - „Breitgefächertes“ Kundenspektrum
 - Personalisierte, flexible Lerndienste, zusammengestellt aus Angeboten verschiedener Institute
 - Verwischen der Grenzen zwischen akademischer und beruflicher Ausbildung
 - Vom Azubi zum Master (AFBG: Aufstiegsfortbildungsförderungsgesetz)
 - Virtuelle Universitäten / Lehrstätten mit vernetzter Betreuungs-Umgebung



Verteiltes Lehren & Lernen (VLL)



- VLL ist zentrales Thema für die Steigerung der Qualität und Effizienz der akademischen Lehre:
 - Erweiterung des Teilnehmerkreises bei Vorlesungen im Netz
 - Möglichkeit des zeit- und ortsunabhängigen Lernens
 - Erweiterte Möglichkeiten (Animationen u.a.) unterstützen den Lernprozeß
- Problem ist der hohe Aufwand bei der Erstellung multimedialer Lehrinhalte
 - synchrone Lehrmaterialien (z.B. Vorlesung): 1 h Vorlesung ≈ 5 h Aufwand
 - asynchrone Produktionen: 1 h Material ≈ 200 h Aufwand (und mehr)
- 5 Jahre Förderung erbrachte keinen umfassend akzeptierten Standard
 - einzelne Projekte konnten nachweisen, daß mit gezielter Werkzeugauswahl der Erstellungsaufwand für asynchrone Produktionen reduziert werden kann
 - Verbesserung der Technik und Benutzerschnittstellen erleichterten Dozenten die Durchführung von verteilten Vorlesungen

VLL in den kommenden Jahren



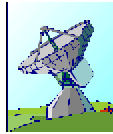
- Grenzen zwischen Präsenz- und Fern-Universität verwischen
- VLL-Lösungen werden allgemein akzeptiert sein
- gestiegen Qualitätsansprüche, geprägt durch Unterhaltungsindustrie
- komplexe Sachverhalte werden zunehmend durch Animationen visualisiert
- VLL- führt zu Rationalisierung an den Hochschulen - Vorlesungen werden zusammengelegt
- VLL-Lösungen werden den Wettbewerb zwischen Hochschullehrern fördern
- „Home Learning“ wird durch breitbandige Netzzugänge immer bedeutender
- Anerkennungsfrage von VLL-Kursen ist durch entsprechende Prüfungsordnungen geregelt

Kommunikation im Wandel



■ Nahtlose Netze

- Integration von Festnetz, Wireless LANs, Mobilfunk verschiedener Standards, Satellitenkommunikation



- Nutzung in vergleichbarer Form
 - Angepasste Schnittstelle (User-Interface, Funktion)
 - Vergleichbare Sicherheit (Authentifizierung, Verschlüsselung)

■ Lokalisationsbasierte Funktionen

- Zugang auf Informationen zum aktuellen Standortes
- Lieferung der Ort-Information ins Netz



Night out in Düsseldorf



■ Beispiel:

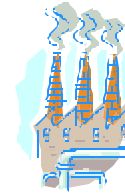
Nokia's Vision von „Mobile Internet Applications

- Was mache ich heute abend? Antwort über lokalen Event-Service
 - Welche neuen Filme wo? Kinos + Zeiten
 - Kartenorder über Service-Menü mit bevorzugter Zahlungsart
 - Anschliessend tanzen? Hip-Hop-Disco's
 - Benutzerprofil kennt die Vorliebe für Hip-Hop-Events
 - Routenplaner / GPS integriert – lokale Fahrpläne
 - Anzeige des Fußwegs zum Kino
 - Bus / Fahrplan zur Hip-Hop-Disco
 - Abfahrtszeit im Terminkalender / Alarm

Netzwerke im Wandel



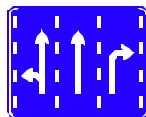
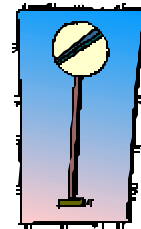
- **Digitale Wirtschaft** erfordert zuverlässige Funktion
 - Hohe Performanz
 - Bandbreite, Qualität, Skalierbarkeit
 - Ständige Verfügbarkeit
 - Ausfallsicherheit, Stabilität
 - Höchste Sicherheit
 - Datensicherheit, Datenintegrität
 - Gesicherter Zugriff / Zugang



Performanz



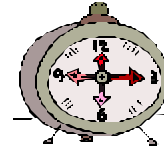
- **Durchsatz und Qualität**
 - Performanz ist eine Anforderung der Anwendung!
 - Anwendungsspezifisches Management von Bandbreite und Übertragungscharakteristik
 - CoS-Lösung im LAN oft ausreichend
 - Für Multiservice im WAN wird QoS (noch?) von etlichen Carriern als erforderlich angesehen.



Ständige Verfügbarkeit



- Sicherstellung der Verwendbarkeit
 - Kontinuität des Netzdienstes
 - Nicht-Eintreffen von Katastrophen oder risikoreichen Ereignissen
 - Betriebssicherheit
 - Fehlertolerante Strukturen und Komponenten
 - Werkzeuge für Risiko- und Unfallmanagement
 - Selbstüberwachende und selbstentstörende Infrastrukturen



Höchste Sicherheit



- Weitgehender Ausschluss von Datenverlust oder –manipulation
- Verhinderung von Datenausspähungen
 - Intrusion Detection – Systeme schützen kaum vor internen Angriffen
- Authentifizierung / Integrität
 - BSI (Bundesamt für Sicherheit in der Informationstechnik)
- Entwicklung angriffsvorbereiteter Systeme
 - Identifizierung zufälliger und bösartiger Angriffe
 - Erhaltung der Funktion unter Angriff



WAN-Netze



- Bandbreite auf der physikalischen Schicht kein Engpass
 - theoretisch kann auf einer Glasfaser etwa 150 Terabit/s transportiert werden (Bell Labs)
 - Im Labor erreichte Werte liegen etwa zwischen 7 und 11 Tbps (~ 170-270 mal OC-768)
 - Bis zu etwa 1.6 Tbps (160 * OC-192) sind heute auf einer Faser verfügbar
 - Auf in Deutschland verlegter Monomode-Faser kann weitgehend 40 Gbps erreicht werden
 - Deutsche Telekom: Trial mit Lucent DWDM-Equipment
 - DFN: 10 Gbps Frankfurt – Leipzig in Betrieb

WAN Netze / Licht und Farbe



- Ergebnisse aus DFN-Arbeitsgespräch (8.1.2002)
- Tendenzen:
 - Maximierung der Kapazität pro Wellenlänge
 - Eher 30 Wellenlängen zu 40 Gbps als 160 Wellenlängen zu 2,6 Gbps (ökonomischer)
 - „very dense“ WDM (tausende WDM-Kanäle?) wird eher von „Filterherstellern“ als von Systemherstellern forciert
 - Kostengünstiges Monitoring auf Ebene der Wellenlänge wird SLAs unterstützen / ermöglichen
 - In Deutschland zu überbrückende Distanzen werden kaum Zwischenverstärker erfordern
 - BER auch bei Wellenlängen 10^{-15}
 - Neben Fasern wird man auch Wellenlängen mieten können

WAN Netze / Strukturen



- **Netzwerkknoten (Switche/Router) sind der Engpass**
 - Derzeit etwa 2000 Wellenlängen pro Switch möglich (Calient Networks, Trellis Photonics)
- **Hierarchische Strukturen**
 - Waveband – Switching im Core
 - IP-Traffic überbrückt im Durchschnitt erheblich größere Distanzen (etwa 3000 km) als z.B. Sprache (etwa 500 km)
 - Wavelength – Switching zum Edgebereich
- **Management optischer Netze**
 - Hierarchisch, klassisch ITU (z.B. ASON)
 - Dezentral, IETF / MPLS – Ansatz (GMPLS)
- **ATM ? Vermutlich noch eine ganze Weile!**
 - große installierte Basis, Multi-Service, QoS – fähig
 - MPLS kann gut aufgesetzt werden, ...

10 Gbps Ethernet (802.3ae)



- **Bandbreite pur / Kosten?**
 - Switch-Port: 10.000 – 80.000 \$?
 - Was wird er in 2005 kosten: 2.000 – 5.000 \$?
 - Kosten wären dann im MAN vergleichbar zu STM-1
- **QoS / CoS**
 - Unterstützt 802.1p / 802.1q
 - Standard sagt nichts zu DiffServ
 - aber Hersteller werden es unterstützen
- **Reichweiten**
 - MMF: 65 m (850 nm) bis 300 m (1310 nm)
 - SMF: 10 km (1310 nm) bis 40 km (1550 nm)

LAN-Netze ohne Limits?



- Trend zu höheren Bitraten wird sich fortsetzen
 - LWL-Verkabelung wird dominanter, Kupfer wird vorwiegend dem direkten Anschluss von Endsystem dienen
- 10 Gbps und höher erlauben andere Strukturen
 - Serverplatzierung unabhängig vom Anwendungskontext
 - Serverless Buildings
 - Zugriffsdefinition über VPN-Mechanismen
 - Remote Backup / Disaster Recovery
 - Zentrale Backups und Spiegelungen an geographisch verteilten Lokalitäten
- 40 Gbps? Im LAN?

Zugangsnetze



- Technologien wie xDSL, Kabelmodem u.ä. werden dominieren
 - Grund: immer noch sehr hohe Kosten für Fiber
 - Anschluss eines Gebäudes an in der Strasse verlegtem Kabel typisch zwischen \$150.000 und \$400.000
 - Quelle: Business Communications Review (8/2001)
 - Folge: „Fiber to the home“ auf absehbare Zeit nicht rentabel
 - Kupfer reicht:
 - VDSL liefert immerhin 2,3 / 51,84 Mbps (up / down) über ~ 300 m
 - Geeignet für multimediale Services guter Qualität
 - Dezierte Standorte (Hotels, Internetcafes, ...) werden breitbandig angebunden sein

Endsysteme / Anwendungen

- 10 Gbps wird vorrangig Backbone-Technologie bleiben:
 - Für die überwiegende Mehrheit der Endsysteme wird in absehbarer Zukunft 100 Mbps ausreichen
 - Kosten pro 1 Gbit-Switchport von 1000 \$ sind nur bei entsprechender Nutzung akzeptabel
- 100 Mbps: L2 – Priorisierung / DiffServ
 - Preiswerte NICs mit Unterstützung von L2-Priorisierungen in Verbindung mit DiffServ in gerouteten Umgebungen reichen auf absehbare Zeit zur Realisierung auch multimedialer Dienste aus

Bandbreite = Durchsatz ?

- Limitierungen am Beispiel von TCP im WAN-Bereich
 - Vereinfachte Formel für TCP-Durchsatz
(Mathis u.a., vereinfachte Version von Padhye's Formel)
 - $Rate = MSS / (RTT * \sqrt{p})$
 - Rate: TCP-Durchsatz
 - MSS: max. Paketgröße (z.B. 1460 Bytes)
 - RTT: Round Trip Time
 - p: Paketverlustrate

Beispiele - TCP-Durchsatz



- Durchsatz von der TU Berlin aus
 - Berechnet nach der genaueren Padhye-Formel, MSS=1460 Bytes
- Quelle: Prof. Wolisz, Telecommunications Networks Group, TU Berlin, Projekt TransiNet

Ziel -----	FhG Fokus (RTT 3,4 ms)	Stuttgart (RTT 19,2 ms)	UC Berkeley (RTT ~ 170 ms)
Paketverlustrate			
0,01	8,9314e+05	4,1639e+05	6,8320e+04 ~ 64 kbit/s
0,001	1,0338e+07	2,0186e+6 ~ 2 Mbit/s	2,3255e+05
0,0001	3,6920e+07 ~ 34 Mbit/s	6,5615e+06	7,4158e+05

Paket Switching - Paketlänge



- Basis: vorwiegend IP-Pakete
 - Schmale Pakete dominieren
 - 40% der pakete ~ 40 Bytes lang
 - 40 Bytes = 32 ns bei 10 Gigabit
 - Ein Lösungsansatz: Fibre Delay Line
 - Feste Paketgröße von 9216 Byte
 - 7 μ s bei 10 Gigabit = 1,4 km FDL
 - Aggregation ankommender Pakete

VPN's haben Zukunft



- VPN's sind **prinzipiell** in der Lage, sichere und steuerbare Kommunikation zu ermöglichen
- Strukturen
 - VPNs auf Basis von Netzwerktechnologien (L2)
 - Bsp.: Frame Relay VC, ATM VC, BGP/MPLS
 - Vorrangig genutzt durch Service-Provider zur Verbindung von Intranets
 - Logische Trennung des Traffics im Provider-Netz
 - Keine Verschlüsselung erforderlich (auch nicht bei MPLS)
 - QoS / CoS – Garantien durch Methoden des Traffic Engineering (virtual circuit connections)
 - Geeigneter Ersatz für Standleitungen (kostengünstiger, zur Zeit ~ 50% günstiger als Standleitungen)

VPN's haben Zukunft



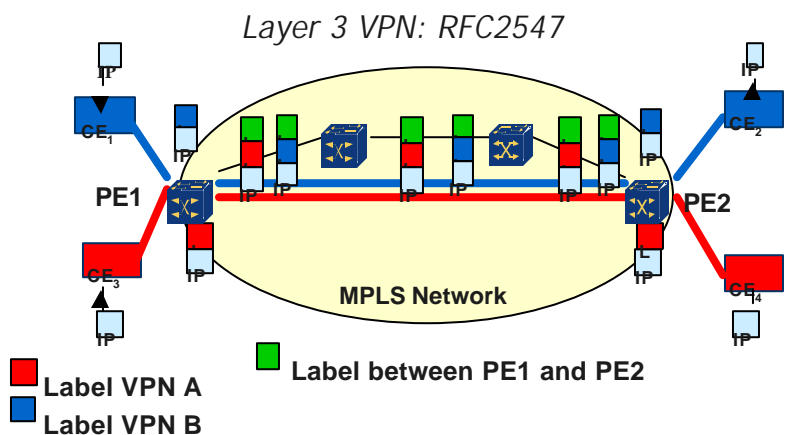
- Strukturen (Fortsetzung)
 - VPNs auf Basis von Tunneling und Encryption
 - Dominierend ist IPSec – Protokoll
 - MS-PPTP und L2TP verlieren an Bedeutung
 - IPSec- Merkmale
 - Transparent Mode
 - Verschlüsselung und Tunneling arbeiten End-to-End
 - Verfahren ist auch ohne Unterstützung von Routern und Switchen einsetzbar
 - Tunnel Mode
 - (Ingress / Egress) Router verschlüsseln

VPN - IPSec

- Vorteile
 - ISP-Support nicht erforderlich
 - Einsatz auch über mehrere verbundene ISP-Netz möglich
 - Nutzung für den Remote Access (Zugang z.B. über xDSL- / Kabelmodem)
- Nachteile
 - Verantwortung für die Verschlüsselung (Key Management / Authentifizierung) muss selbst wahrgenommen werden
 - Verschlüsselung ist Aufwand, der Performanz verringert / verringern kann
 - *Netzwerkprozessoren mit standardisierten APIs (Network Processing Forum: Streaming Interface / Look-Aside-Interface) können hier Skalierungsprobleme reduzieren*

VPN Realisierung in MPLS:

Label Stacking



Status "Layer 2 VPN": verschiedene IETF drafts

VPNs – was fehlt



- Integrierte Lösungen
 - Einbindung von VPNs in umfassende Sicherheitskonzepte (z. B.: VPN + Authentifizierung/Zugangssicherung + Firewall)
 - VPNs und Firewalls sollten immer harmonisieren
 - Problem: Verschlüsselte Kommunikation und Überprüfung von Schadinhalten
- Management / Skalierung
 - Manuelle Konfiguration vieler Tunnel aufwendig
 - CNMS (Customer Network Management System)
 - Zugriff regulieren, QoS / SLA überprüfen, ...

VPN – geeignet für alles?



- Neben Sicherheit muss auch die Eignung für spezifische Dienste adressiert werden
 - Sinnvolle (aussagekräftige, nachprüfbar) Tunnel-SLAs für VPNs von ISP erforderlich (z.B. vergleichbar FRF.13)
- SLAs für Frame Relay & IP-VPNs (Beispiel):

Provider	Frame Relay Verfügbarkeit	Frame Relay max. Delay	IP-VPN Verfügbarkeit	IP-VPN max. Delay
AT & T	99,99%	120 msec	99,5%	120 msec
MCI Worldcom	99,9%	120 msec	99,8%	120 msec

Zusammenfassung



- IP wird das „UNI“ zum Netz
- Netzwerkperformanz heißt heute Dienstperformanz!
 - Durchsatz, Qualität, Stabilität, Sicherheit
- Netzwerkübergänge müssen nahtlos sein / werden (Konvergenz + Integration)
- Bandbreite im WAN und LAN-Bereich „nur“ noch eine Kostenfrage!
- WAN-Bereich: Tendenz zu 40 Gbps und mehr
- Gigabit-Ethernet und VPNs werden die Grundlagen im LAN sein.
- Integration von VPN und generelle Sicherheitskonzepten, eingebunden in Managementsystem zwingend
- **Auch Themen:** ASP, Application Switching, DEN, Policy-basiertes Netzwerkmanagement, ...

Danke schön!



www.eantc.de