



Echtzeitplattformen für eBusiness
Forschungsergebnisse aus dem EU-
Projekt INTELLECT

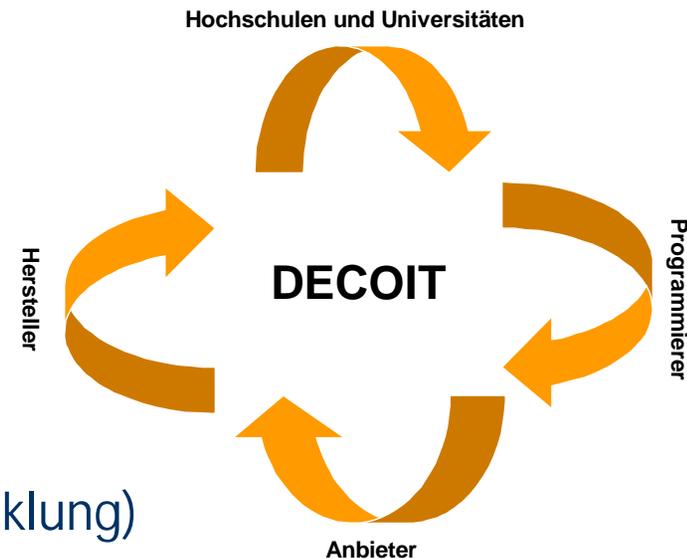
Dipl.-Ing. Kai-Oliver Detken
Klagenfurt, 24. September 2001



- ◆ Kurzvorstellung DECOIT
- ◆ Das INTELLECT-Projekt
- ◆ Problemstellung
- ◆ Echtzeitintegration
- ◆ Implementierung
- ◆ Fazit

Portfolio der DECOIT

- ◆ Consulting (herstellerneutral)
 - ◆ Netzkonzepte
 - ◆ Sicherheitskonzepte
 - ◆ Sicherheitsüberprüfung
 - ◆ Strategiekonzepte
 - ◆ Softwarekonzepte
- ◆ Qualitätssicherung
- ◆ Hersteller- und Produkttests
- ◆ Förderprojekte (Forschung und Entwicklung)
- ◆ Schulungen (Technologie und Anwendungen)
- ◆ Webprojekte (Design und Programmierung)
- ◆ Marketing (Zusammenarbeit mit Fachverlagen)
- ◆ Projektmanagement (Nationale/Internationale Projekte)





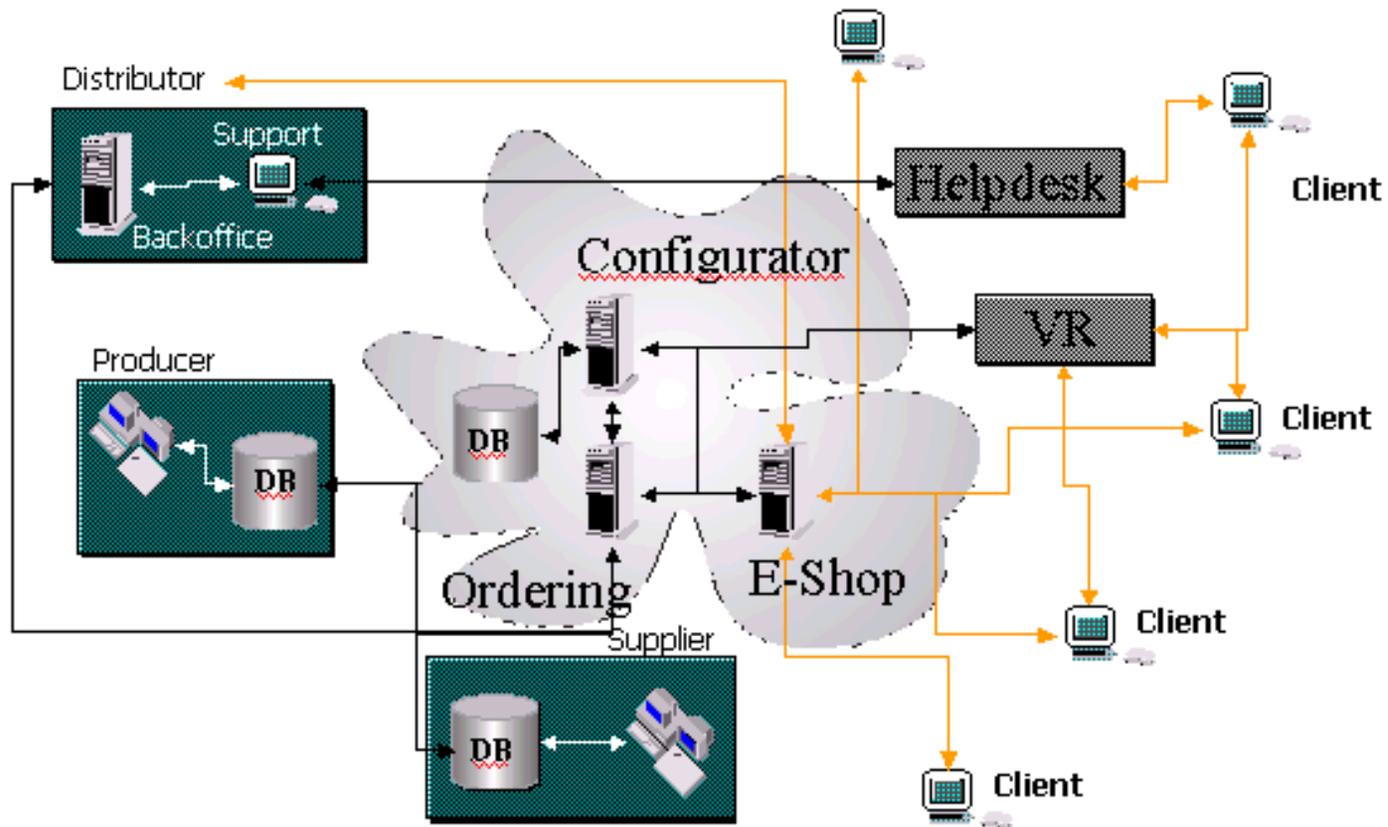
Das EU-Projekt INTELLECT



Ursprüngliche Idee

- ◆ Eine eShop Lösung, die
 - zu einem Höchstmaß benutzerfreundlich ist
 - die Produkte möglichst realistisch und in einer entsprechenden Umgebung darstellt
 - dem Benutzer eine individuelle Gestaltung des Produktes erlaubt
 - dem Benutzer eine intelligente Beratung bei der Auswahl und Zusammenstellung des Produktes bietet
 - dem Benutzer das Gefühl gibt, als ob er in einen realen Laden geht und dort einkauft
 - den gesamten Einkauf als eBusiness Anwendung abbildet, ohne Medienbruch

Die Module



Problemstellungen



Offene Punkte



- ◆ Keine oder wenig einheitlichen Standards im Bereich Security, Verschlüsselung und QoS vorhanden
- ◆ Fehlende Integrität der Daten im Internet
- ◆ Fehlende Migrationsstrategien zwischen Protokollen
- ◆ Schlechtes Interworking zwischen unterschiedlichen Netzen
- ◆ Ineffektive Anpassung traditioneller Medien auf neue Medien
- ◆ Ineffektive Hilfedienste
- ◆ Fehlende Unterstützung bei der Eingabe/Konfiguration eines E-Commerce Systems
- ◆ Keine Echtzeitdienste wie IP-Telefonie oder Videokonferenzen über das Internet abrufbar
- ◆ QoS-Mechanismen in heterogenen Netzen bisher nicht anwendbar

Echtzeitintegration





- ◆ Security
 - Schaffung von Vertraulichkeit, Authentizität, Integrität, Verbindlichkeit, Verfügbarkeit
 - IPsec als gemeinsamen Nenner verwendet (VPN Site-to-Site)
- ◆ Quality-of-Service (QoS)
 - Layer 2: ATM QoS oder IEEE 802.1D
 - Layer 3: IP QoS
- ◆ Voice-over-IP
 - Sprachqualität testen
 - Echtzeitanforderungen beachten

Security: VPN-Plattform

- ◆ Aufbau einer VPN-Plattform mittels IPsec
- ◆ Anforderungen beachten wie Verfügbarkeit, Sicherheit, Skalierbarkeit, Performance, QoS, Mobilität, Netzwerkmanagement, Accounting/Billing, Migration
- ◆ Mit Hilfe des IPsec Authentication Header (AH) wird die Integrität der übertragenen Daten geschützt und die Authentizität gewährleistet
- ◆ Der IPsec-Header Encapsulating Security Payload (ESP) kapselt die zu schützenden Daten ein und gewährleistet bei Bedarf deren Vertraulichkeit durch Verschlüsselung. Außerdem sind Möglichkeiten zum Schutz der Integrität und zur Authentizität der Datenpakete vorgesehen
- ◆ Secure Socket Layer (SSL) für Browserzugriffe auf das Intranet

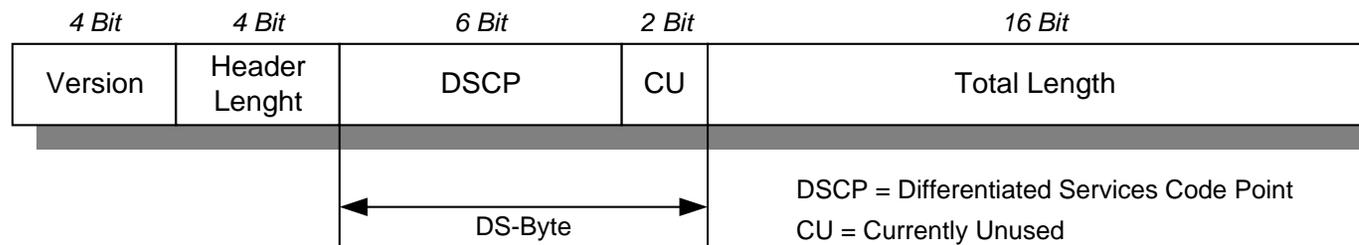
QoS: IntServ-Ansatz (1)

- ◆ Ressourcen müssen explizit verwaltet werden, um die Anforderungen der Anwendungen erfüllen zu können
- ◆ Die Dienstgarantien für Echtzeitapplikationen können nicht ohne Reservierung von Ressourcen erfolgen
- ◆ Die End-to-end-Verzögerungszeiten müssen begrenzt werden, um die dynamische Anpassung an sich ändernde Netzbedingungen gewährleisten zu können
- ◆ Statistisches Aufteilen zwischen Echtzeit- und Datenapplikationen ist vorteilhaft, wenn man über eine gemeinsame Infrastruktur beide Anwendungen nutzen will

QoS: IntServ-Ansatz (2)

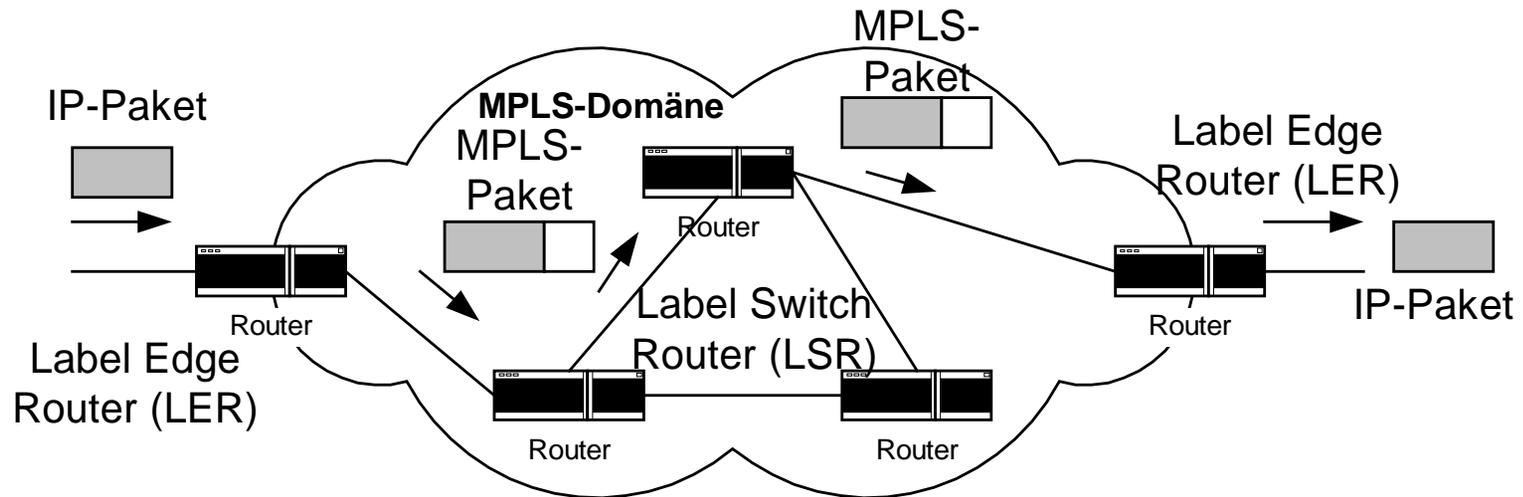
- ◆ Controlled Load Network Element Service (CL-Service): hat zum Ziel dem Teilnehmer ein unbelastetes Netz in Zeiten der Überlast vorzutauschen. Daher wird dieser Dienst auch als geringfügig besser eingestuft, als bei Best-effort. Die Spezifikation RFC-2211 beschreibt diesen Service. Einsatzgebiete sind: Audio-/Videostreaming und Web-basierte Transaktionen.
- ◆ Guaranteed Quality of Service (Guaranteed Service, GS): Dieser Dienst legt die Einhaltung fester QoS-Parameter im Netz fest. Diese Parameter werden vor dem Beginn der Übertragung oder parallel dazu ausgehandelt. Die Spezifikation RFC-2212 legt diese Parameter fest. Einsatzgebiete sind interaktive Dienste, die eine harte Anforderung an QoS haben, wie IP-Telefonie, VoIP und Videokonferenzen

QoS: DiffServ-Ansatz



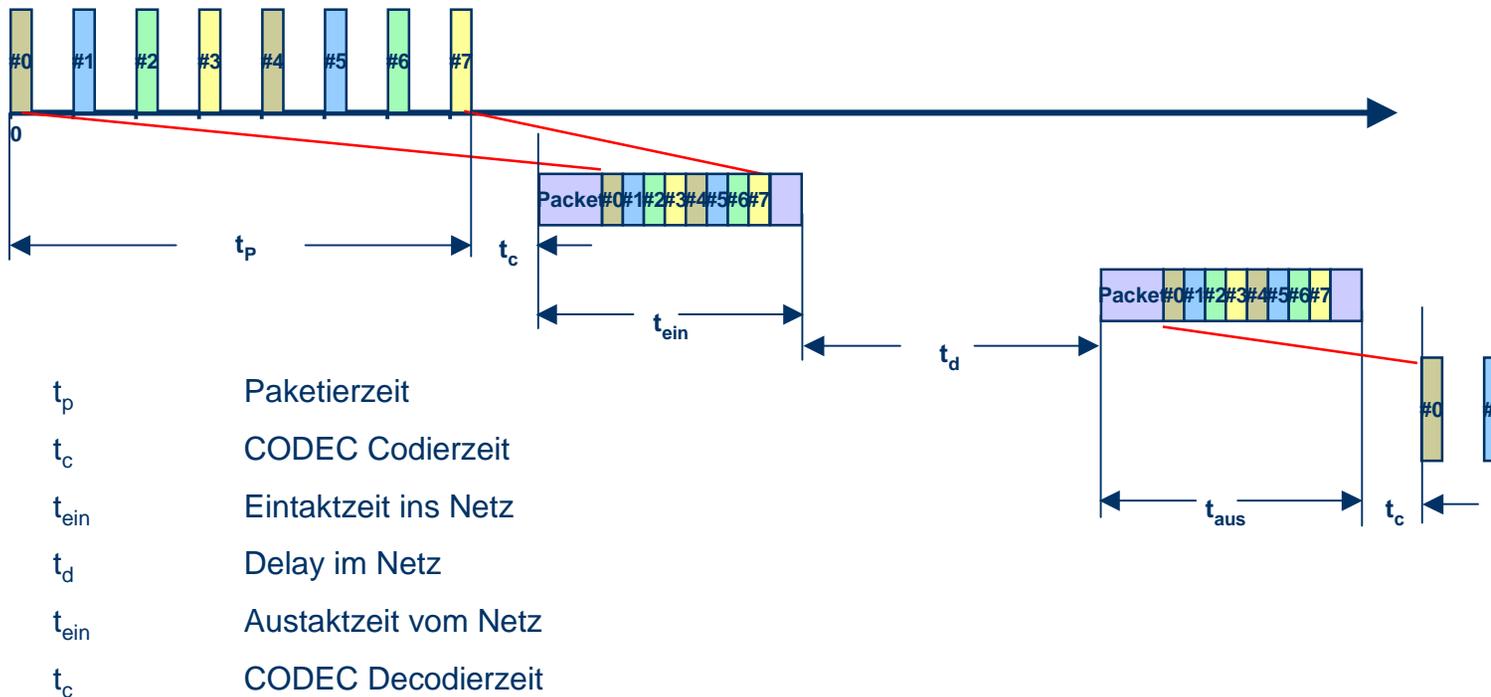
- ◆ Jeder Codepoint entspricht einem PHB
- ◆ Es können mehrere DSCP auf ein PHB abgebildet werden
- ◆ Per-Hop-Behavior (PHB)
 - Drop Threshold
 - Buffer Allocation
 - Service Priority
 - Service Rate

QoS: Traffic Engineering





VoIP: Lange Laufzeiten



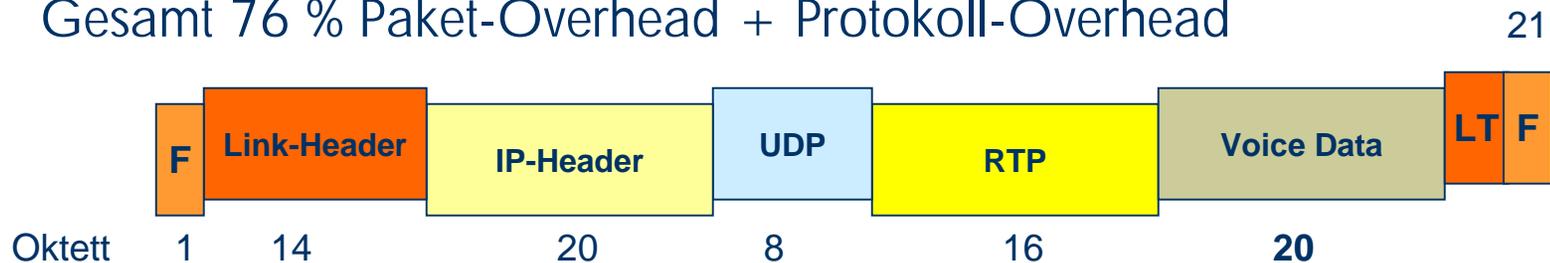
VoIP: Laufzeitauswirkungen

- ◆ Es sind zwei Probleme getrennt zu betrachten:
 - Konstante Laufzeit durch das Netz (Round Trip Delay)
 - Laufzeitvariationen (Jitter)
- ◆ Gesprächsqualität
 - Die Gesprächsqualität wird (auch beim konventionellen Telefon) von der Laufzeit bzw. der Verzögerung der Antwort beeinflusst.
- ◆ Sprachqualität
 - Wenn durch Jitter (zu lange Laufzeiten) ein Paket zu spät kommt, entstehen je nach Kompressionsverfahren und Paketgröße Knackgeräusche oder gar Informationsverluste.



VoIP: Overhead

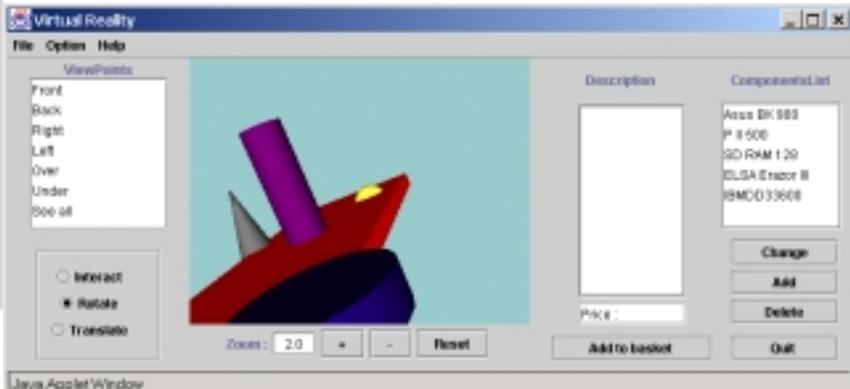
- ◆ Beispiel mit NetMeeting im LAN:
 - 14 Oktett Ethernet Link Header
 - 20 Oktett IP-Header
 - 8 Oktett UDP Header
 - 16 Oktett RTP Header (Minimum)
 - 20 Oktett Voice Data
 - 2 Oktett Link Trailer (FCS)
 - 2 Oktett Start + Ende Flag = 82 Oktett Paket Länge
- ◆ Gesamt 76 % Paket-Overhead + Protokoll-Overhead

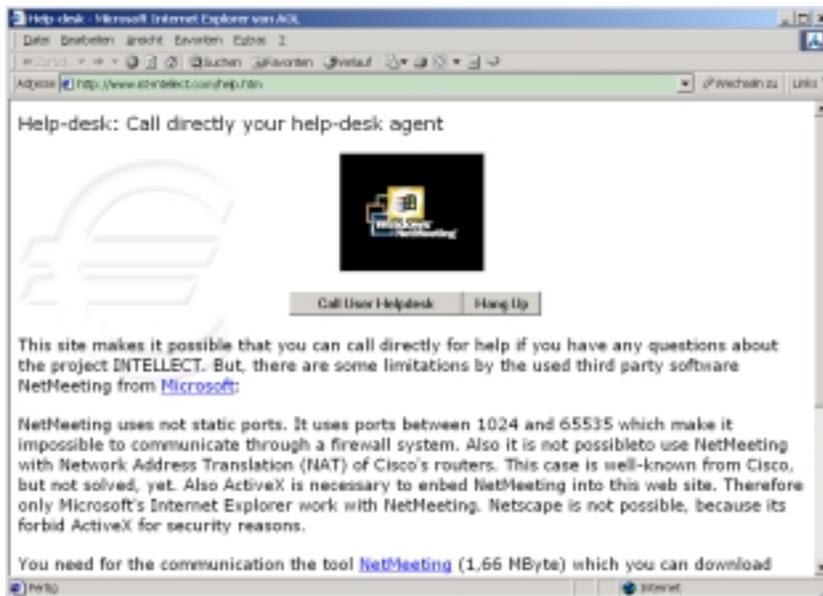


Implementierung



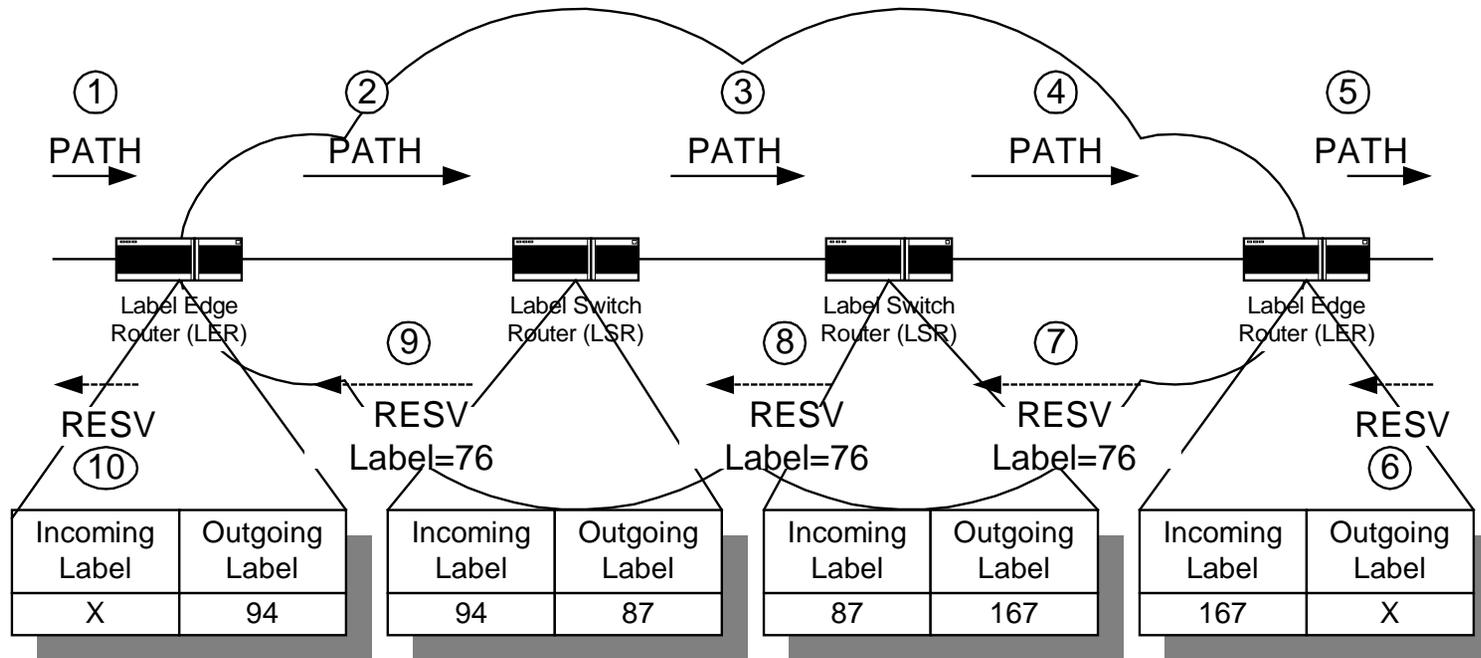


	Home AboutUs Products ShoppingCart	SessionId: r6feq29a11
Home AboutUs Products ShoppingCart	<p style="text-align: center;"><i>Intellect E-Shop</i></p> <p>Welcome to the Intellect E-Shop!</p> <p>To access the different categories of computers click on the products link.</p>	login here user: <input type="text"/> pass: <input type="password"/> <input type="button" value="login"/>
		



- ◆ Erste Integration in die Webseiten von INTELLECT und den Prototypen
- ◆ SSL-Integration
- ◆ Anpassung auf Application Server
- ◆ Page Mirroring kann erst integriert werden, wenn Tomcat 4.x vorhanden ist
- ◆ VoIP und Application Sharing bereits lauffähig
- ◆ Nächster Schritt: QoS-Integration mittels RSVP

Unterstützung von QoS: IntServ



Zusammenfassung/Fazit



Zusammenfassung

- ◆ Security-Lösungen sind vorhanden, aber nicht einheitlich
- ◆ IPsec bietet enorme Sicherheit, besitzt aber auch noch Schwachstellen
- ◆ MPLS ist noch nicht endgültig spezifiziert und bietet verschiedene Signalisierungsmöglichkeiten an (RSVP-TE, MPLS-LDP, CR-LDP)
- ◆ QoS bleibt problematisch, da unterschiedlich einsetzbar und keine Software für Ende-zu-Ende-Support verfügbar ist
- ◆ VoIP kann nicht an die ISDN-Sprachqualität heranreichen
- ◆ Protokollfamilien SIP und H.323 sind konkurrierende Ansätze (H.323 ist evtl. zu komplex)
- ◆ Interoperabilität, Security, Skalierbarkeit und Performance sind oftmals noch nicht ausreichend bei VoIP-Lösungen
- ◆ Ohne Security und QoS bekommen E-Commerce- und VoIP-Lösungen keine Marktakzeptanz!



- ◆ Sicherheitsplattform muss in Form eines VPN zuerst etabliert werden
- ◆ Echtzeitapplikationsanforderungen mit in der Planung berücksichtigen
- ◆ QoS-Mechanismen mit dem Provider abstimmen/fordern
- ◆ Integration von E-Commerce-Anwendungen und VoIP auf die bestehende Echtzeitplattform vornehmen
- ◆ Performance-, Interoperabilitäts-, Security, VoIP- und QoS-Tests durchführen