



Vorlesung

VPN: Drahtgebunden und drahtlos

Fachbereich Informatik (FB 20)

Lehrstuhl Prof. J.Buchmann

WS-05/06 / V2 - 20.205.1

In Zusammenarbeit mit dem CAST-Forum

Dr. Wolfgang Böhmer

Skript: <http://www.cdc.informatik.tu-darmstadt.de/~wboehmer/>

Email: wboehmer@cdc.informatik.tu-darmstadt.de





- Provider-Netze - sicherer Kommunikation über fremde Netze
 - Provider-Netze und Netzstrukturen
 - IP-VPN über Wählverbindungen
 - VPN über fremde Netze
 - Referenzmodell für ein CE-basierendes VPN
 - Referenzmodell für ein NB-basierendes VPN
 - Netzwerk-Performance und Management
 - Sicherheitsaspekte
 - Service-Vereinbarungen (SLA)
 - VPN-Klassifizierungen



Provider-Netze – sichere Kommunikation über fremde Netze



- Es stellt sich die Frage ob eine VPN-Fremdrealisierung oder eine Eigenrealisierung kostengünstiger und sicherer ist.
 - Grob gesehen stehen sich zwei Lösungen gegenüber dessen Beurteilung nicht pauschal beantwortet werden kann.
 - Bei einer VPN-Fremdrealisierung gerät ein Unternehmen in die Abhängigkeit Dritter, wie und in welchem Maße die Abhängigkeit sein kann, ist dabei unterschiedlich.
 - Bei einer VPN-Eigenrealisierung hält ein Unternehmen alle Komponenten im Unternehmen und muss teilweise dediziertes Spezialwissen vorhalten. Dies führt vielfach zu einem kostenintensiven Personalstamm und geht häufig am Kerngeschäft eines Unternehmens vorbei. Gerade KMU's sind nicht in der Lage diesen Personalstamm zu unterhalten.
 - Wichtige Entscheidungsgrößen gehen auf das Leistungsangebot eines Providers zurück. (Betrachtung des Kerngeschäftes)
 - Interessant ist die Frage des Übergabepunktes im Fall einer Fremdrealisierung





Struktur der globalen Netze

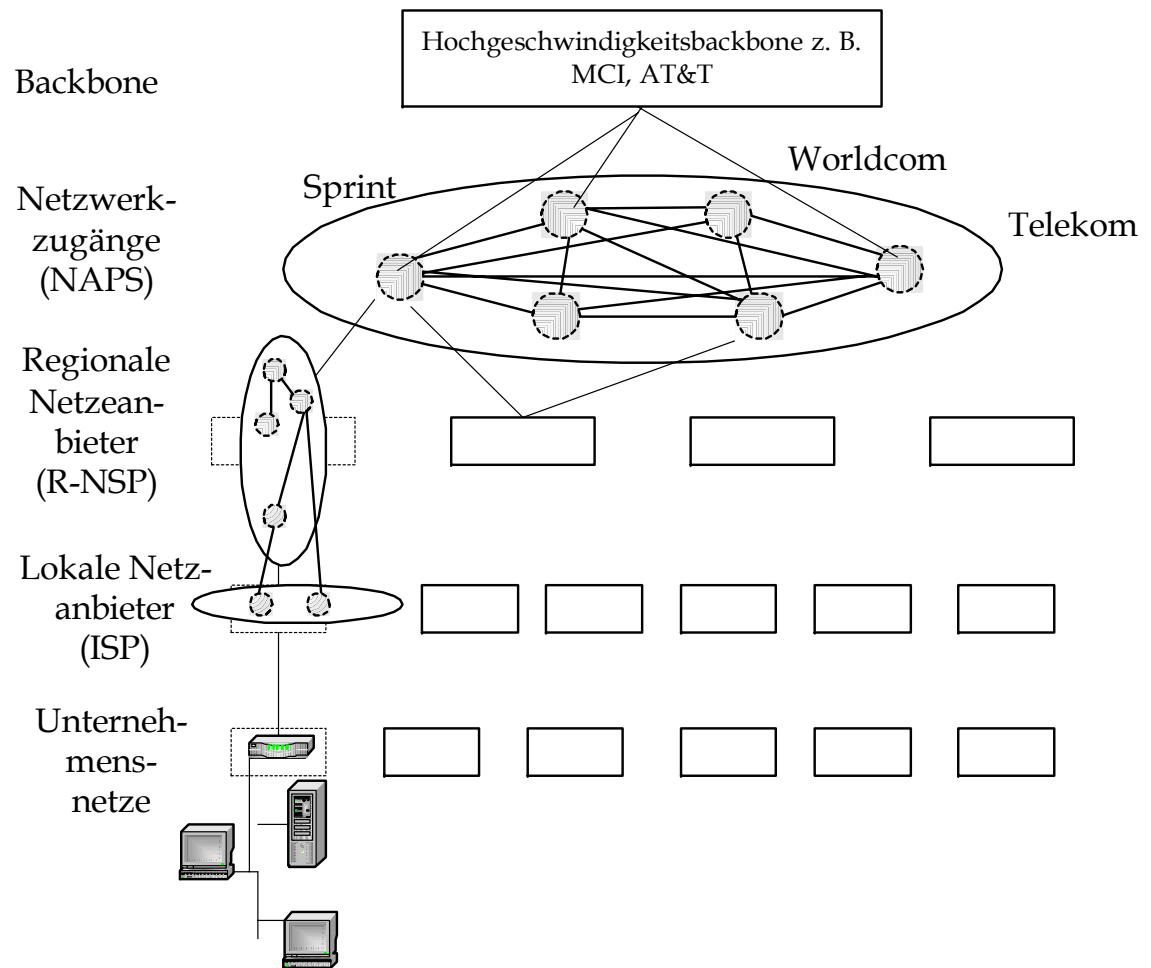
- Das Business-Modell der Service-Provider verändert sich zunehmend.
- Ausgehend von einem weltumspannenden globalen Hochgeschwindigkeitsbackbone der z.B. von MCI und AT&T unterhalten wird entstehen hierarchische Untergruppierungen
 - Tier-1-Carrier unterhalten das weltumspannende Backbone
 - Tier-2- Carrier mit Hauptzugängen (Network Access Points, NAP) France Telekom, Deutsche Telekom, Sprint, Worldcom
 - Tier-3-lokale Anbieter (ISP), bieten oftmals neben Diensten im Datenbereich auch Sprachservices an und sind häufig im Umfeld einer Großstadt bzw. Ballungszentrum zu finden.
- Die klaren Grenzen verschwimmen allerdings, wenn einige Unternehmen betrachtet werden. (T-Online International). Auch ausgelagerte IT-Abteilungen die zu Profit-Centern in eine eigen GmbH umgewandelt wurden bieten oftmals auf dem Drittmarkt ihre Dienst an.



Hierarchie vom globalen Backbone zum Unternehmensnetz



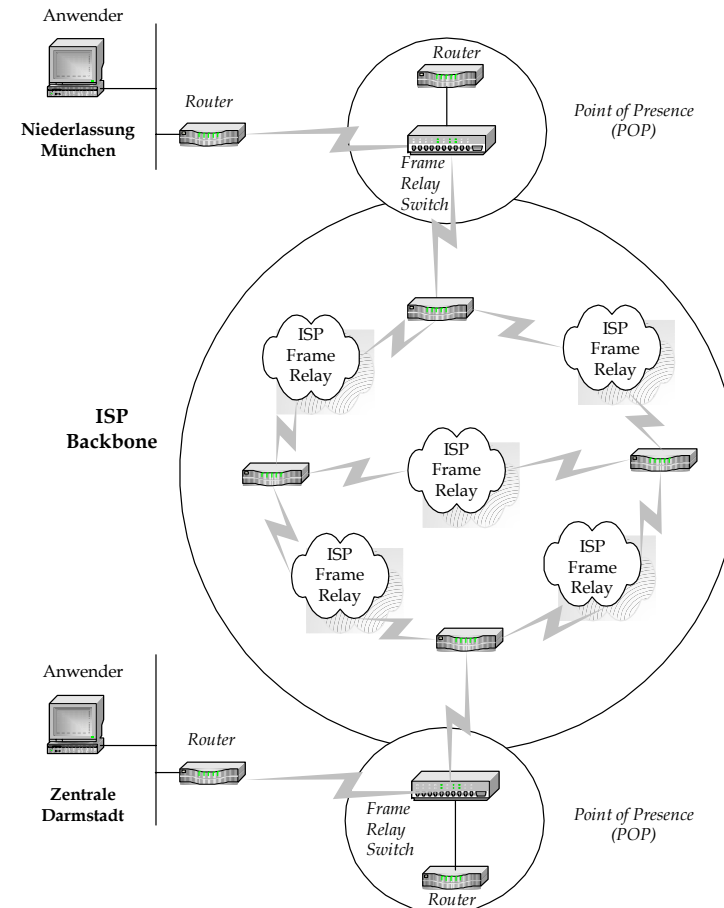
- Das Geschäftsmodell wandelt sich vom reinen Bandbreitenverkauf zu einem vielfältigen Service Angebot auf Dienstebene
- Mit diesem Wandel wird der Anbieter zum Partner und es kommt zu intensiven Verflechtungen mit den Kundennetzen.
- Diese Verflechtung erschwert eine Trennung wesentlich mehr, als früher bei einem reinen Bandbreitenvertrieb



Typisches Backbone eines ISP



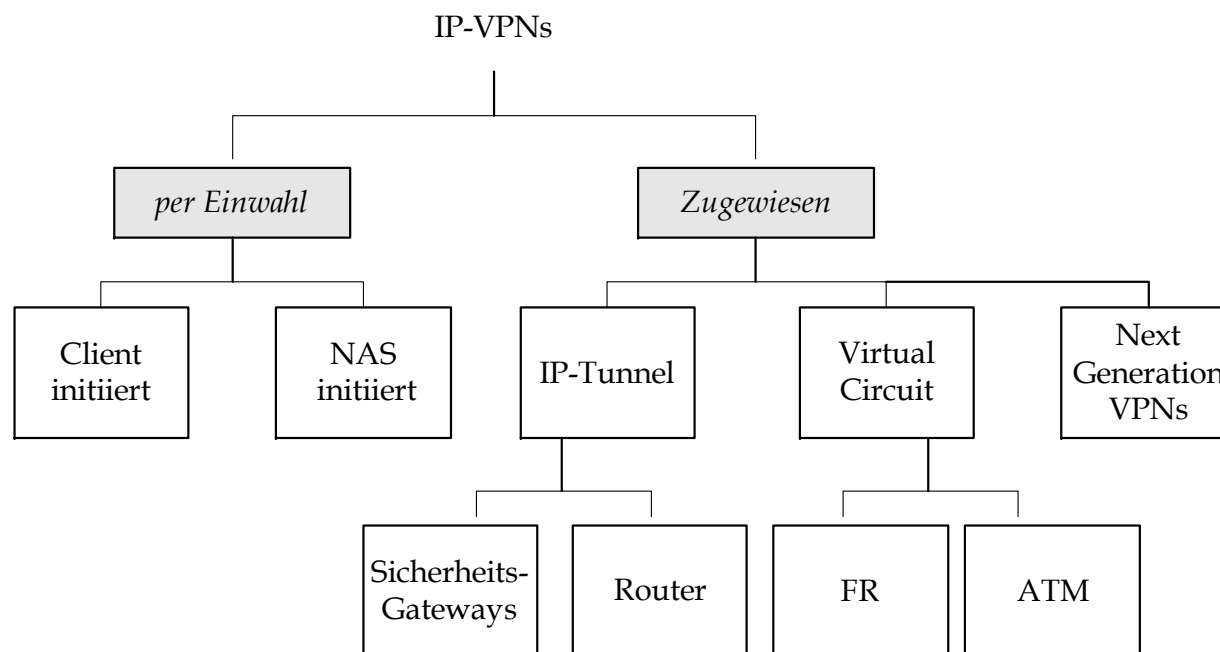
- Redundant ausgelegter Backbone (oftmals Frame-Relay Technologie)
- Mittels Router wird eine Verbindung von der Filiale zum POP aufgebaut und dort mittels FR-Switch ins Backbone geführt.
- Verantwortungsbereich des letzten Routers ist nicht selbstverständlich und muss verhandelt werden.
- Vertraulichkeitsanforderungen werden in der Praxis höchst unterschiedlich umgesetzt.





Überblick verschiedener IP-VPN-Architekturen

- Alle mittels Wählverbindungen aufgebaute IP-VPN haben gemeinsame Charakteristika (*Client initiated, NAS initiated*)
- Alle zugewiesenen VPN können durch bestimmte Eigenschaften charakterisiert werden



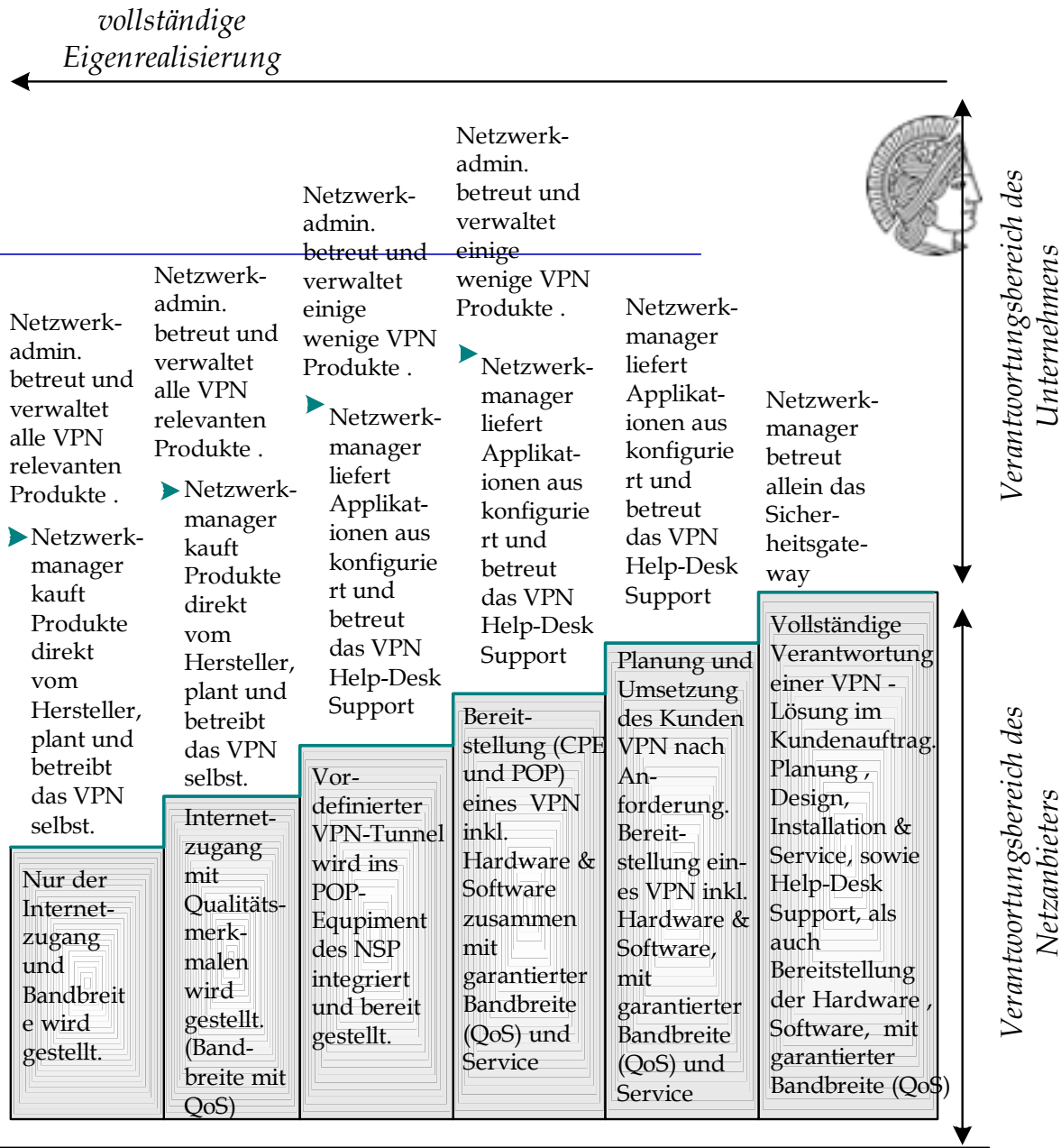


IP-VPN über Wählverbindungen

- Ein ISP stellt Einwahlmöglichkeiten bereit, die von seinen Kunden über Zugangsnummern kostengünstig im Ortsnetz erreicht werden. (T-Online, AOL, CompuServe, etc.)
- Aus Kostengründen stehen für alle Kunden des ISP die gleichen Einwahlmöglichkeiten bereit, die geteilt werden. Das Passwort zur Einwahl ist für jeden Kundenkreis unterschiedlich.
- Es werden i.d.R. Tunnel über öffentliche IP-Netzwerke (L2TP, IPSec) oder über IP-Netzwerke des Providers (z.B. T-Online mit L2Sec) genutzt.
- Authentifizierungsmöglichkeiten können ergänzt werden. Es kommen spezielle Datenbanken zum Einsatz. Dieser Dienst wird ebenfalls häufig von Providern angeboten.



Kontinuierlicher Übergang (*In-house, Hybrid, Outsourcing*) von einer VPN-Eigenrealisierung bis hin zur kompletten Fremdrealisierung durch einen Netzanbieter (NSP)



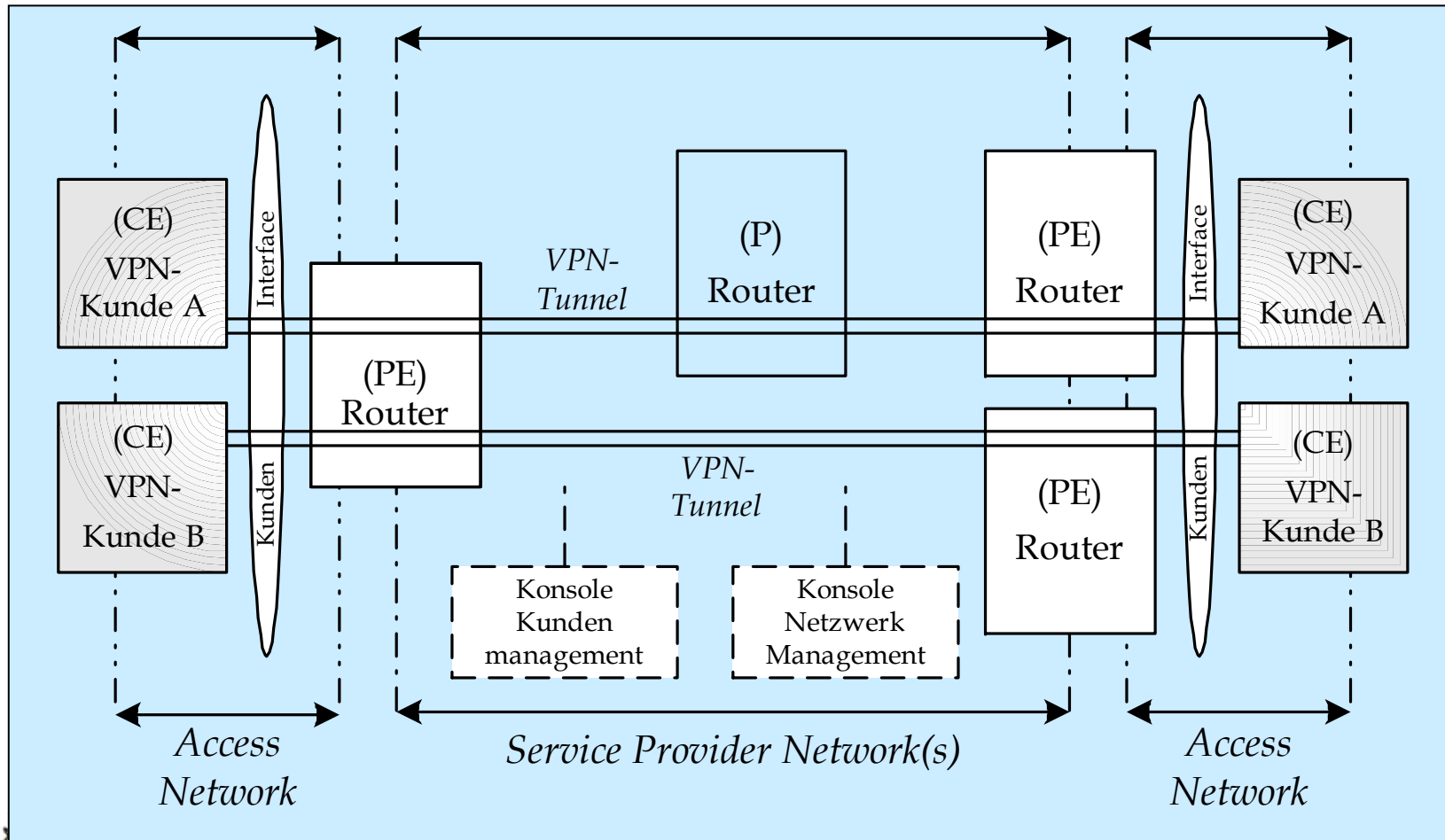
Referenzmodell für ein verwaltetes CE-basierendes VPN



- Grundsätzlich kann eine VPN-Netzkopplung auf Layer-2 als auch auf Layer-3 geschaltet werden.
 - Layer-2: Unterstützung auf der Data-Link-Schicht. IP-Pakete registrieren die Kopplung nicht und die Provider-Edge (PE) reicht die Datenpakete des Kunden weiter.
 - Layer-3: Die CE und die PE kennen sowohl die Data-Link-Layer als auch die IP-Layer
- In einem Customer-Edge-basierenden VPN endet der Tunnel direkt am CE, also am Equipment des Kunden. Übergabepunkt kann das äußere Schnittstelleninterface sein, aber auch das firmenseitige (innere) Interface.
- Das Service-Provider-Netz beinhaltet ein IP-Netzwerk und CE-Management-Funktionen, die über spezielle Konsolen verwaltet werden. Es können auf Kundenseite und auf Providerseite proprietär NMS, die SNMP oder sogar auf LDAP abgestützt sind, eingesetzt werden.



Referenzmodell für ein verwaltetes CE-basierendes VPN



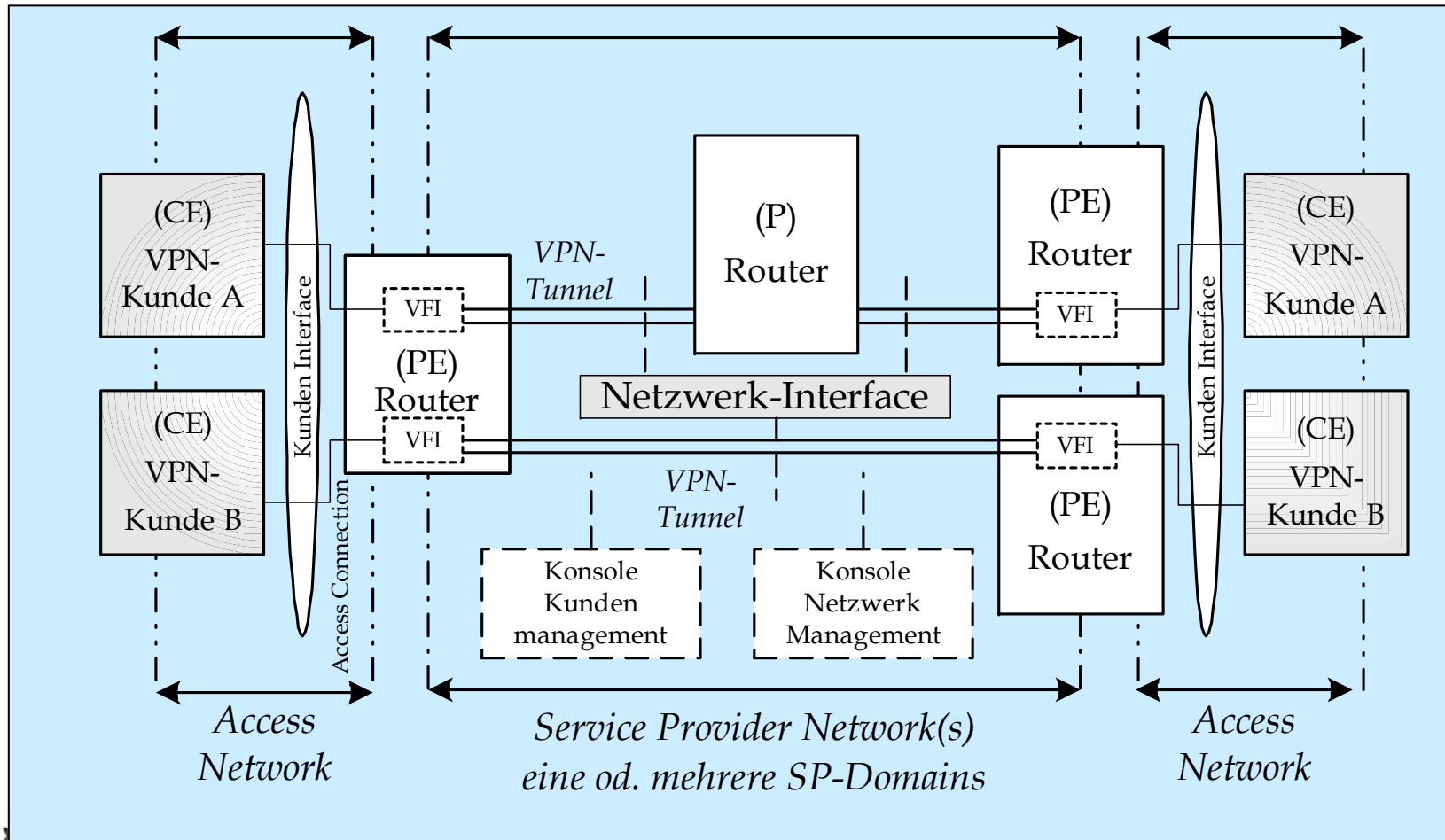


Referenzmodell für ein Netzwerk-basierendes VPN

- In einem Netz-basierenden VPN (*Nb-VPN*) endet der Tunnel am Netz-Rand (Provider Edge) des vom NSP verwalteten Service-Netz.
- Die PE-Router können in einem POP stehen
- Die ITU-T hat ebenfalls eine dem Sinn der IETF entsprechende Definition für ein Nb-VPN erlassen (Y.1311.1, in 2000)
- Laut Definition muss ein Nb-VPN von der Zugriffstechnologie unabhängig sein
- Für ein Layer-3-Netzwerk-basierendes VPN kann ein BGP/MPLS nach RFC-2547 oder auch ein virtuelles Router-Netz nach RFC-2917bis als Beispiel dienen.



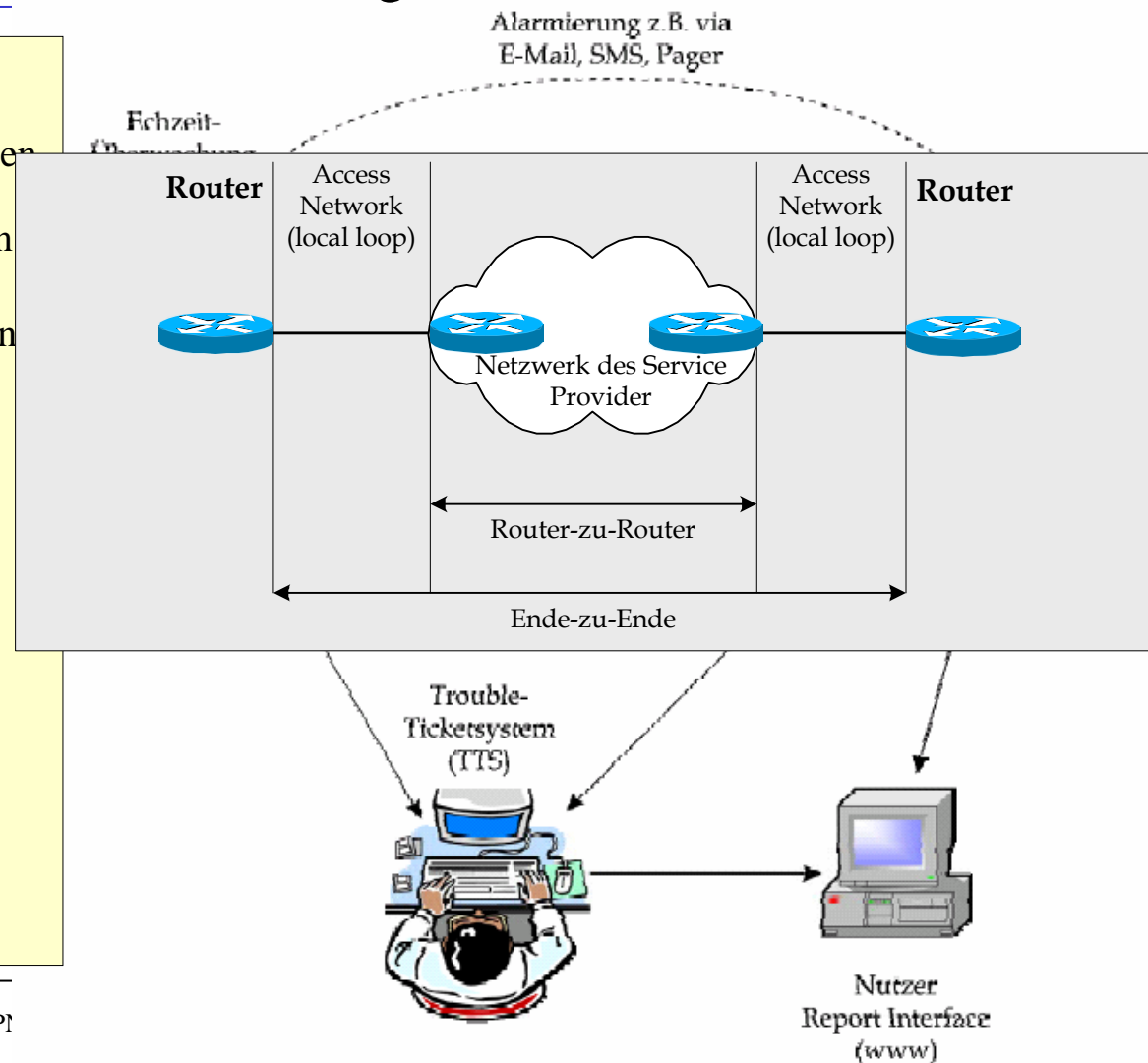
Referenzmodell für ein Netzwerk-basierendes VPN(PPVPN)





Netzwerk-Performance und -Management

1. An den Übergabepunkten (Schnittstellen) zwischen Kunden und Provider müssen Kontrollmessungen (*Monitoring*) vorgenommen werden
2. Eine Datenbank zur Filterung des Performanceverhaltens des VPN muss eingerichtet werden.
3. Applikationen zur Datenanalyse und zur Erzeugung von Reports (*Berichtswesen*) müssen installiert werden.
4. Web-basierende HTML-Versionen zur Reporterzeugung für eine Echtzeitkontrolle (*Lastverhalten*) sollten vorhanden sein.



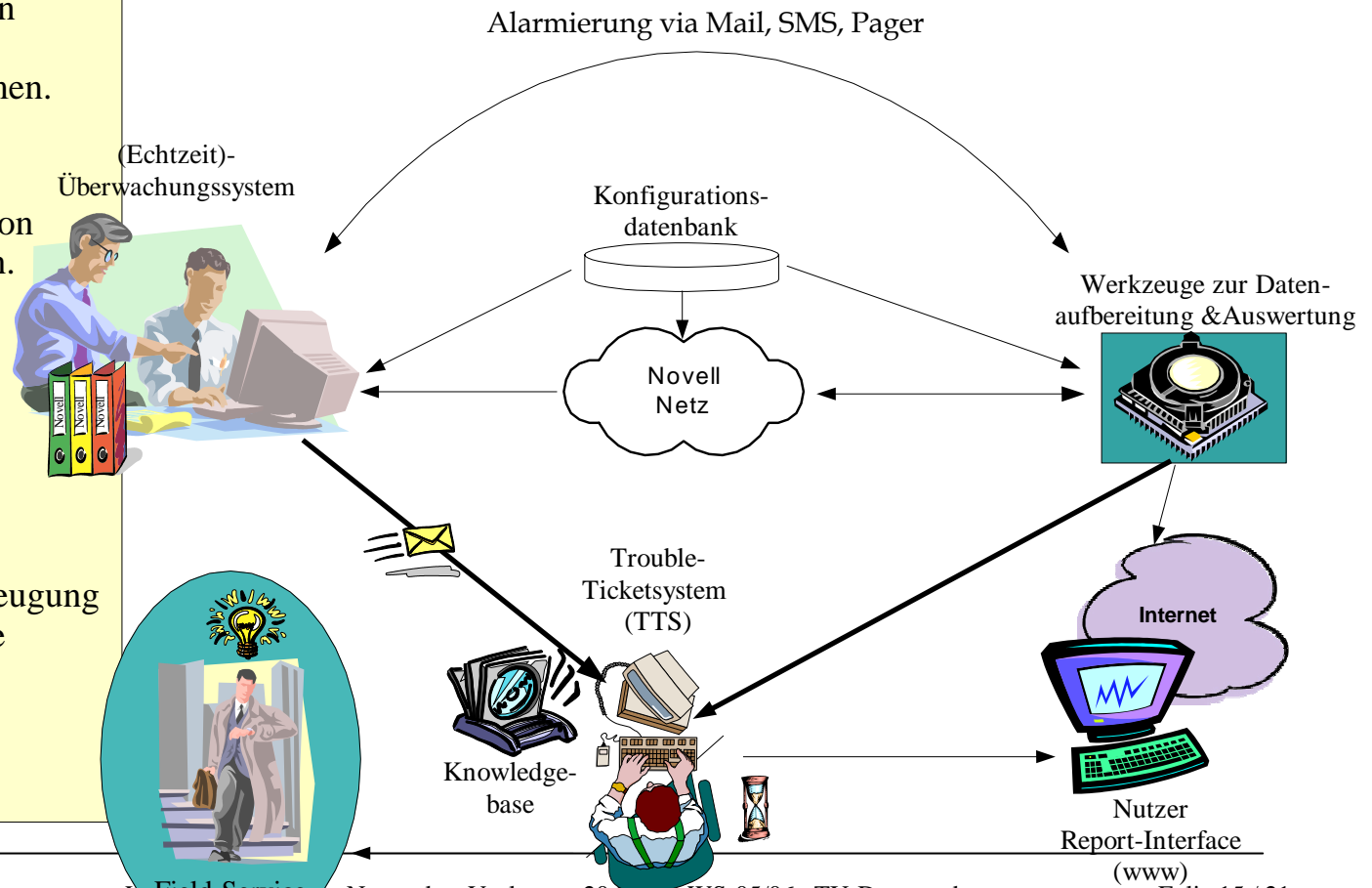
31.01.2006

VPI

Überwachung und Betrieb im NOC



1. An den Übergabepunkten (Schnittstellen) zwischen Kunden und NOC werden Kontrollmessungen (*Monitoring*) vorgenommen.
2. Eine Datenbank zur Konfiguration und
3. kompletten Dokumentation muss eingerichtet werden.
4. Applikationen zur Datenanalyse und zur Erzeugung von Reports (*revisionssicheres Berichtswesen*) werden installiert.
5. Web-basierende HTML-Versionen zur Reporterzeugung für eine Echtzeitkontrolle (*Lastverhalten*) sollten vorhanden sein.



31.01.2006

V. Field-Service Networks, Vorlesung 20.205.1, WS-05/06, TU-Darmstadt

(www)
Folie 15 / 21





Service-Vereinbarungen (SLA)

- Port-Verfügbarkeit in Prozentangaben
- Performance-Garantien
- Mittlere Zeit der Fehlerbehebung und nicht nur Antrittszeit,
- Konkretisierte Wartungsfenster, in denen kein Betrieb statt findet
- Aussagen über Bandbreitenauslastung und Priorisierungsmöglichkeiten,
- Service-Hotline bzw. User-Help-Desk (UHD) und damit auch die Servicezeiten
- Aussagen über Paketverlustraten (von/bis)
- Aussagen über Paketverzögerungen (von/bis)
- Aussagen für z.B. QoS-Monitoring
- Aussagen über Sicherheitsmechanismen, insbesondere Verschlüsselungsmethoden und Schlüsselwechsel und ggf. Firewall-Systeme
- Aussagen über Authentifizierungsverfahren
- Aussagen über das Berichtswesen allgemein
- Aussagen über Nutzungserfassung und Zahlungsmodalitäten (Accounting und Billing)





VPN-Klassifizierungen (1)

VPN Kat	typische Nutzer	typische Anforderungen	Skalierbarkeit u. Bandbreite	Technologie u. Produkte	für/wider
Kat-0	Kleine Firmen mit Telearbeitern	E-Mail Interne Datenbanken Allg. Datenzugriff	eine Site bis zu 50 Telearbeiter Internet-Zugriff über DSL oder 1,5 Mbit/s Wählverbindungen für Fernzugriffe	PPTP Windows NT/2000 Software VPN-Lösung auf einer PC-Standardplattform Paketfilterung	+ Einfach und geringe Kosten + Gute VPN-Einstiegsmöglichkeit - Keine Site-to-Site-Verbindung - Inflexibel, da Pkt.-zu-Pkt. - Laengste MTTR (bei Server-Ausfall)
Kat-1	Kleine bis mittlere Firmen mit mehreren Lokationen	E-Mail Interne Datenbanken Allg. Datenzugriff	von 2 bis 10 Sites Bis zu 250 Telearbeiter Internet-Zugriff bis zu 1,5 Mbit/s Wählverbindungen für Fernzugriffe	IPSec (DES, IKE) Password & Nutzer- Authentifizierung Hardware VPN-Gateway (bis zu 1,5 Mbit/s Bandbreite und 250 Sessions) Extra Client-Software für Fernzugriffe Einfache Firewall oder Paketfilterung	+ Einfach zu konzipieren und zu installieren + Preisgünstig + Site-to-Site & Fernzugriff vorhanden + Hardware VPN-Gateway bringt Sicherheit mit kaum Performance- verlust - Keine Extranet-Unterstützung, wenn IPSec nicht kompatibel
Kat-2	Mittlere Firmen mit besonderen Ansprüchen	E-Mail Interne Datenbanken Allg. Datenzugriff Produkt Design z.B. CAD/WebCAD Übergreifende Projekt- planungen	Bis zu 10 Sites Bis zu 500 Telearbeiter Internet-Zugriff mit 1,5 Mbit/s Bandbreite und mehr bei der Zentrale Internet-Zugriff bis zu 1,5 Mbit/s in der Niederlassung Wählverbindungen für Fernzugriffe	IPSec (DES, IKE) NAT Starke Nutzer-Authentifizierung (z.B. Secure-ID Token) Firewall-Systeme in der Zentrale RADIUS-Server Hardware VPN-Gateways mit Geschw. Leistungsstufen (von 1,5 Mbit/s bis $n \times 1,5$ Mbit/s) mit 500 Sessions Extra Client-Software für Fernzugriffe	+ Hohes Sicherheitsniveau + Moderate (vertretbare) Kosten + Site-to-Site & Fernzugriff vorhanden - Zusätzlicher Wartungs- und Pflegeaufwand für Firewall und RADIUS, etc. - Kein Extranet (fehlende Kompatibilität) - Keine Echtzeit-Anwendungen





VPN-Klassifizierungen (2)

VPN Kat	typische Nutzer	typische Anforderungen	Skalierbarkeit u. Bandbreite	Technologie u. Produkte	für/wider
Kat-3	Mittlere Firmen bis große Firmen mit eigenen Geschäftspartnern u. eigenem Kundstamm, wie z.B. Versicherungen und Pharmafirmen	E-Mail Interne Datenbanken Allg. Datenzugriff Design-Informationen Anschluss an Zulieferungsketten e-Commerce-Anwendungen	ca. 100 Sites ca. 1000 Telearbeiter von 1,5 Mbit/s bis $n \times$ Mbit/s zur Anbindung einer Filiale von E1 bis E3 Bandbreite für die Zentrale QoS/SLA für Site-to-Site Verbindungen Wählverbindungen, ISDN, xDSL oder Modembank für Fernzugriffe vorhanden	Zertifizierte Kompatibilität für IPSec (3DES, IKE) NAT Starke Nutzer Authentifizierung (Smart Cards, Token) Firewall-Systeme in der Zentrale und in großen Filialen Einsatz von LDAP Einsatz einer eigenen PKI Hardware VPN-Gateways mit Geschw. Leistungsstufen (von T1 bis $n \times$ T1 oder auch E1 für 5000 Sessions und mehr) Automatismus für policy verschickende Client-Software für Telearbeiter	+ Unterstützung von Extranets + Unterstützung von zeitkritischen e-Commerce Transaktionen – Allg. Sicherheitspolicy sowie Sicherheitsarchitektur und Sicherheitsrichtlinien notwendig – Vertieftes Wissen zur Planung und Umsetzung des VPN notwendig – Ständige inter-sive Wartung und Pflege des VPN notwendig
Kat-4	Große multinationale Firmen mit extrem vielen Geschäftspartnern bzw. Zulieferkette mit einem hohen Grad an Fremdrealisierung	E-Mail Interne Datenbanken Allg. Datenzugriff Anschluss an Zulieferungsketten e-Commerce-Anwendungen Sprachanwendungen Video / Konferenzsysteme	ca. 1000 Sites ca. 10.000 Telearbeiter von 1,5 Mbit/s bis $n \times$ Mbit/s zur Anbindung einer Filiale von E1 bis E3 Bandbreite für die Zentrale QoS/SLA für Site-to-Site-Verbindungen Wählverbindungen, ISDN, xDSL oder Modembank für Fernzugriffe vorhanden	Zertifizierte Kompatibilität für IPSec (3DES, IKE) NAT Starke Nutzer-Authentifizierung (Smart Cards, Token) Firewall-Systeme in der Zentrale und in großen Filialen Einsatz von LDAP Einsatz einer eigenen PKI Hardware VPN-Gateways mit Geschw. Leistungsstufen (von T1 bis $n \times$ T1 oder auch E1 für 5000 Sessions und mehr) Bandbreiten-Management Mehrere VPN-Service-Stufen Echtzeit QoS & SLAs Automatismus für policy verschickende Client-Software für Telearbeiter	+ Unterstützung von Extranets + Hohes Sicherheitsniveau + Unterstützung von Echtzeit-App. & Video + Unterstützung von e-Commerce-Anwendungen + Skalierbare Administration + Beziehungen zu mehreren Geschäftspartnern – Sehr komplex und kostenintensiv – Profundes Wissen von Netzwerktechnik & Sicherheitsmechanismen erforderlich – Ständige inter-sive Wartung und Pflege des VPN notwendig





VPN-Vergleichsverfahren und Anforderungen

Kriterium	Wichtung	Anbieter A	Anbieter B	Anbieter C
Präsenz allg.	5			
Präsenz (Personen)				
POP-Präsenz	4			
Zahlungsmodell	2 oder 5			
VPN-Plattform	3			
Management Tools	5			
Zugriffsarten	3			
Service Varianten	3			
Nummern-Plan	3			
TK-Kopplung	1 oder 5			
Pre-Sales-Service	3			
Post-Sales-Service	3			
Referenz-Site	2 oder 5			
QoS-Garantien	5			
Penalties	4			
Preis	4			
Gesamtpunktzahl				



Übungen



1. Frage: Wie sieht eine Hybrid-Lösung im Fall eines VPN-Outsourcing aus.? Welche Komponenten verbleiben im Unternehmen, welche werden aus der Hand gegeben?
2. Frage: Wie heißen i.d.R. die Bedingungen, die an die Fragestellung Nr. 1 geknüpft sind und welches sind die Kernelemente? (mindestens drei Aufzählen)
3. Frage: Welchen technischen Einblick erhält i.d.R. das Unternehmen bei einem VPN-Outsourcing und wie wird dieser heutzutage realisiert?





Literatur

- <http://www.tu-darmstadt.de/vv/comments/20.205.1>
- **RFCs: 2547, 2661, PPVPN-Draft, 2917bis, 2684, ITU-Y.1311.1**

