



---

# VPN: Drahtgebunden und drahtlos

Fachbereich Informatik (FB 20)

Lehrstuhl Prof. Buchmann

WS05-06 / V2 - 20.205.1

In Zusammenarbeit mit dem CAST-Forum des CAST e.V.

Dr. Wolfgang Böhmer

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

Email: [wboehmer@cdc.informatik.tu-darmstadt.de](mailto:wboehmer@cdc.informatik.tu-darmstadt.de)





# Gliederung

1. Einführung in die Thematik
2. VPN-Technologien in Weitverkehrsnetzen
3. Informations- und Kommunikationssicherheit in VPNs
4. Vertraulichkeit, Integrität und Authentifizierung in der VPN-Technologie
5. Varianz der VPN-Typen und das Prinzip des Tunneling
6. VPN-Technologie im Bereich der drahtlosen Netze (Wireless Networks)
7. VPN-Planung





# VPN-Technologien in Weitverkehrsnetzen

- Virtuelle Verbindungen beim Fast-Paket-Switching (FPS) und Frame-Relay
- Multiprotokoll Label Switching (MPLS) als Hybridtechnologie
- MPLS über Frame-Relay
- Virtuelle Kanäle und –Pfade in zellbasierenden Netzen
- MPLS über ATM-Verbindungen



# Informations- und Kommunikationssicherheit in VPN-Netzen

---



- Verfahren der IuK-Sicherheit (allgemein)
- Risiko, Sicherheit und Gefahr
- Grundsatz und Risikoanalysen
- Vergleich zwischen CC und ITSEC
- Sicherheitsarchitekturen offener Systeme
- Evaluierung einer Gesamtunternehmenssicherheit



# Vertraulichkeit, Integrität und Authentifizierung in der VPN-Technologie

---



- Symmetrische und asymmetrische Verschlüsselungsverfahren
- Schlüsselaustauschverfahren
- Mechanismen einer digitale Signatur
- Sicherheitsanforderungen an eine digitale Signatur
- Einsatz von digitalen Zertifikaten in der VPN-Technologie
- Verfahren der Authentifizierung in der Anwendung (PAP, CHAP, RADIUS, DIAMETER, Kerberos)





## Varianz der VPN-Typen und das Prinzip des Tunneling

- Intranet-VPNs
- Extranet VPNs
- Remote-Access-VPNs
- VPN und Firewall-Systeme / Router
- Layer-2 Techniken (L2TP, L2F, L2Sec),
- Layer-3 Techniken (IPSec),
- Layer-4 Techniken (SSL/TSL,)



# VPN-Technologie im Bereich der drahtlosen Netze (Wireless Networks)

---



- Zellenbasierte 2,5G, 3G (UMTS) und B3G Netze
- Technologien zur Überbrückung der Luftschnittstelle
- Frequenz-Hopping Spread Spektrum (FHSS)
- Direkt Sequence Spread Spektrum (DSS) Wireless-LAN-Lösungen (WLAN)
- Virtuelle LANs (VLAN) im WLAN
- Vertraulichkeit im WLAN
- VPN und WLAN
- Planung und Ausleuchtung einer WLAN-Domäne
- Weiterentwicklungen der IEEE 8011.nn



# VPN-Planung, Referenzmodelle und Phasenmodell

---



- Klassifizierungen von VPNs
- VPN über fremde Netze (IETF-Referenzmodelle)
- Welche Schnittstellen sind zu betrachten
- Wie sieht die zu erbringende Leistung für ein Fremdanbieter aus und wie kann diese kontrolliert werden?
- Service Level Agreements (SLAs)
- Einsatz von virtuellen privaten Netzen
- Planungsaspekte im Projekt (Phasenmodell)



# Literatur



<http://www.tu-darmstadt.de/vv/comments/20.205.1.tud>

Böhmer, W.: VPN- Virtual Private Networks, die reale Welt der virtuellen Netze ; Carl Hanser Verlag, München, Wien 2002, ISBN 3-446-21532-8.

· Kosiur, D.: Building and Managing Virtual Private Networks, Wiley Computer Publishing, John Wiley & Sons, Inc., New York, Chichester, Weinheim, Brisbane, Singapore, Toronto, 1998, ISBN 0-471-29526-4.

· Spenneberg, R.: VPN mit LINUX, Grundlagen und Anwendung Virtueller Privater Netzwerke mit Open Source-Tools; Addison-Wesley Verlag, 2004, ISBN 3-8273-2114-X.

· Stallings, W.: Cryptography and network security; principles and practice, 2nd ed. Prentice-Hall International (UK) Limited, London 1998, ISBN: 0-13-869017 -0.

· Nett, E; Mock, M; Gergeleit, M.: Das drahtlose Ethernet, Addison-Wesley-Verlag 2001, ISBN 3-8272-1741-X

· IEEE Standard 802.11: Wireless LAN Medium Access Control (MAC) and Physical (PHY) specifications, 1997.

· Huston G.: Internet Performance Survival Guide, QoS Strategies for Multiservice Networks, ISBN 0-471-37808-9

· Comer, 1995: Internetworking with TCP/IP Vol. I., ISBN 0-13-216987-8

· Davis, C.R.: IPsec-Tunneling im Internet, mitp-Verlag, 1. Auflage 2002, ISBN 3-8266-0809-7.

· Aurand, A.: Sicherheit in Cisco- und Windows-2000-Netzwerken, Installation und Troubleshooting von IPsec in der Praxis, Addison-Wesley Verlag 2001, ISBN 3-8273-1930-7. (Teil 2- IPsec-Architektur)

· Cisco TCP/IP-Routing, Konzeption und Aufbau eines Netzwerkes mit Cisco-Routern, 2.Auflage, Addison-Wesley Verlag 2001, ISBN 3-8273-1881-5

Relevante RFCs werden in der Vorlesung bekannt gegeben.





# Organisation: 10 Punkte zum Erfolg

1. Die Vorlesung 20.205.1 hat drei Credit-Points (CP)
2. Die Vorlesungsinhalte sind verschlüsselt unter <http://www.cdc.informatik.tu-darmstadt.de/~wboehmer/> zu finden
3. Die Schlüssel werden in der ersten Vorlesung bekannt gegeben
4. Zur Erlangung der CPs wird eine Klausur durchgeführt
5. Zur Klausurvorbereitung werden wöchentliche Übungsaufgaben am Ende einer jeden Vorlesung gestellt, die vergleichbar mit den Fragen der Klausur sind.
6. Die Antworten zu den Übungsaufgaben werden exemplarisch zu Beginn einer jeden Vorlesung von den Studenten beantwortet.
7. Die Klausur wird voraussichtlich in der KW-06( ) geschrieben werden.
8. Nach ca. vier Wochen sind die Ergebnisse verfügbar (homepage).
9. Eine Wiederholung ist nur bei „Nicht Bestanden“ möglich, also keine iterative Verbesserung der Zensur.
10. Eine Nachbesprechung erfolgt dann im anschließenden Semester nach der ersten Vorlesungseinheit.





# Klausurbedingungen

- Klausur:
  - Multiple Choice ( 10 Fragen zu je 1 Punkt)
    - (Wissensteil)
  - Definitionen (3 Fragen zu je 10 Punkte)
    - (Verständnisteil)
  - Fallstudien ( 2 Fragen zu je 20 Punkte)
    - (Anwendungsteil)
  - **Klausurdauer 2 Zeitstunden**

**Klausur am: XX.02.2006**

