

Inhaltsverzeichnis

1. Einleitung	7
2. ATM - Normierungsstand und -entwicklung	9
2.1. Grundlagen	9
2.2. UNI / NNI	12
2.2.1. Signalisierung (Q.2931)	12
2.2.2. UNI	13
2.2.3. UNI 3.0	14
2.2.4. UNI 3.1	15
2.2.5. UNI 4.0	16
2.2.6. NNI	16
2.3. PNNI	17
2.3.1. IISP	17
2.3.2. PNNI 1.0, 2.0	18
2.4. Traffic Management (TM4.0)	20
2.5. IP over ATM (RFC 1483/1577)	21
2.5.1. Multiprotocol Encapsulation (RFC 1483)	21
2.5.2. Classical IP (RFC 1577)	22
2.6. LAN Emulation (LANE 1.0, 2.0)	23
2.6.1. LANE 1.0	23
2.6.2. LANE 2.0	27
2.7. Multiprotocol over ATM (MPOA)	27
2.7.1. Overlay Routing	28
2.7.2. Integrated PNNI (I-PNNI)	28
3. ATM-Backbone-Netz der Universität Rostock	31
3.1. Einleitung	31
3.2. ATM-Backbone-Netz	33
3.2.1. Passives Netz	33
3.2.2. Aktives Netz	34
3.2.3. Logische Struktur	40
3.3. Begründung der Produktauswahl für das ATM-Netz	42
3.4. Einsatzmöglichkeiten der Meß- und Analysetechnik	43
3.4.1. Cisco Works for Switched Internetworking	43
3.4.2. LAN/WAN-Multiprotokollanalysator W&G DA-30C	44

3.5. Möglichkeiten der Erweiterung und Optimierung des ATM-Netzes	47
4. Sicherheitsmechanismen in Netzen	53
4.1. Einführung	53
4.2. Encryption	56
4.2.1. Data Encryption Standard (DES)	57
4.2.2. Kerberos	59
4.2.3. RSA-Verfahren	60
4.2.4. Angriffsmöglichkeiten gegen Encryptionssysteme	61
4.2.5. Anwendungsbeispiele	62
4.3. Access Control	62
4.3.1. Benutzer-Authentifikation	63
4.3.2. Security-Protokolle	65
4.3.3. Anwendungsbeispiele	67
4.4. Firewalls	67
4.4.1. Packet Filter	68
4.4.2. Circuit Level Gateways	69
4.4.3. Application Level Gateways	69
4.4.4. Network Address Translation (NAT)	70
4.4.5. Architekturen von Firewalls	71
4.4.6. Plazierung von Firewalls	73
4.4.7. Forderungen an Firewalls	74
4.4.8. Grenzen von Firewalls	77
4.4.9. Beispiele für Firewalls	78
4.5. Entwicklungsstand auf ATM-Ebene	82
4.6. Sicherheitskonzepte in Beispielen	83
4.6.1. Datennetz der Technischen Hochschule Darmstadt	84
4.6.2. Berliner Landesnetz	88
4.6.3. Encryption-Systeme	93
5. Sicherheitsmechanismen im Universitäts-Netz (Stand und Ausblick)	95
5.1. Einleitung	95
5.2. Hochschulnetz	96
5.2.1. Funktionalitäten und Sicherheitsanforderungen	96
5.2.2. Realisierung der Funktionalitäten und Sicherheitsanalyse	96
5.2.3. Sicherheitsempfehlungen	100
5.3. Verwaltungsnetz	105

5.3.1. Funktionalitäten und Sicherheitsanforderungen	105
5.3.2. Realisierung der Funktionalitäten	107
5.3.3. Sicherheitsanalyse	108
5.3.4. Geplante Netzsituation	109
5.3.5. Sicherheitsempfehlungen	110
5.4. Medizinnetz	113
5.4.1. Funktionalitäten	113
5.4.2. Sicherheitsanforderungen	115
5.4.3. Realisierung der Funktionalitäten	116
5.4.4. Sicherheitsanalyse	119
5.4.5. Sicherheitsempfehlungen	119
5.5. Abschließende Überlegungen und Fazit	126
6. Zusammenfassung	131
7. Anhang	135
7.1. Produkt-Vergleich	135
7.2. Verzeichnis der Abkürzungen	139
7.3. Verzeichnis der Bilder und Tabellen	146
7.4. Personenverzeichnis	149
7.5. Literaturverzeichnis	150
7.6. Inhaltsverzeichnis des Anlage-Hefters [Anlage]	156