

### **7.3. Verzeichnis der Bilder und Tabellen**

Bild 2-1:	B-ISDN-Referenzmodell	9
Bild 2-2:	Asynchrone Übertragung von ATM-Zellen	11
Bild 2-3:	Signalisierung in ATM-Netzen	13
Bild 2-4:	Auf- und Abbau einer ATM-Verbindung	15
Bild 2-5:	Vergleich der Zellenheader an UNI und NNI	16
Bild 2-6:	Referenzmodell von IISP	17
Bild 2-7:	PNNI-Hierarchie-basiertes Netzwerk	19
Bild 2-8:	Routing zwischen logischen IP-Subnetzen bei Classical IP	23
Bild 2-9:	Protokollarchitektur bei LAN Emulation	24
Bild 2-10:	Beispiel für Verbindungen im LANE	25
Bild 2-11:	Routing zwischen virtuellen Netzen entsprechend der LANE	26
Bild 2-12:	Vergleich der Topologien der zwei Ansätze für das MPOA	29
Bild 3-1:	Übersichtskarte der Hauptstandorte der Universität Rostock	31
Bild 3-2:	Ursprüngliches Wissenschaftsnetz der Universität Rostock	32
Bild 3-3:	Schematische Darstellung des LWL-Netzes	34
Bild 3-4:	Schematische Darstellung der Standorte mit Switches	35
Bild 3-5:	Ansicht des LightStream 1010	36
Bild 3-6:	Ansicht des Catalyst 5000	37
Bild 3-7:	Ansicht des Cisco 7507	38
Bild 3-8:	Im Aufbau befindliches Wissenschaftsnetz der Universität Rostock	39
Bild 3-9:	VLAN-Verwaltung der drei Domänen	41
Bild 3-10:	Anwendungsmöglichkeiten des DA-30C im ATM-Backbone-Netz	46
Bild 3-11:	Sternförmige Anbindung der Switches (Minimalvariante)	47
Bild 3-12:	Redundante Verknüpfung über Fast Ethernet (Spanning Tree)	48
Bild 3-13:	Redundante Verknüpfung der ATM-Switches (PNNI)	49
Bild 3-14:	Redundante Anbindung über Dual PHY ATM Interfaces	50
Bild 3-15:	Redundanz durch ATM-Richtfunk-Verbindungen	51
Bild 3-16:	Redundanz der LANE-Services (SSRP) und Routing-Funktionen (HSRP)	52
Bild 4-1:	Bedrohungsvielfalt	53
Bild 4-2:	Symmetrische Verschlüsselung	56
Bild 4-3:	Asymmetrische Verschlüsselung	57
Bild 4-4:	Prinzipieller Aufbau des DES	58
Bild 4-5:	Prinzip des RSA-Verfahrens	60
Bild 4-6:	Firewalls und das OSI-Referenzmodell	68
Bild 4-7:	Prinzip der Network Adress Translation	71
Bild 4-8:	Screening Router mit Screened Subnet	71

Bild 4-9:	Dual Homed Bastion Host mit Demilitarisierter Zone	72
Bild 4-10:	Kaskadierte Dual Homed Bastion Hosts	73
Bild 4-11:	Anordnung von Firewalls	74
Bild 4-12:	Standardmäßiges Filterformat im Cisco-Router	78
Bild 4-13:	Erweitertes Filterformat im Cisco-Router	78
Bild 4-14:	Anbindung der Verwaltung an das Hochschulnetz der THD	86
Bild 4-15:	Gestaffelte Firewall-Anordnung im Berliner Landesnetz	89
Bild 4-16:	Anordnung der Server im Berliner Landesnetz	90
Bild 4-17:	Testnetz zur Firewall-Evaluierung	91
Bild 4-18:	Einsatz von Encryptiongeräten in den Berliner Kliniken	93
Bild 5-1:	Im Aufbau befindliche Struktur des Hochschulnetzes	97
Bild 5-2:	DMZ mit Screening Router, Firewall und dedizierten Servern	102
Bild 5-3:	GUI-Bildschirm von CiscoSecure	103
Bild 5-4:	Einsatz einer zentralen Nutzerrechte-Verwaltung	103
Bild 5-5:	Möglichkeiten des Zugriffs mittels Token Cards	104
Bild 5-6:	Geschlossenes Netz der Verwaltung	108
Bild 5-7:	Geplante Anbindung der Verwaltung an das Hochschulnetz	110
Bild 5-8:	Firewall-geschützte Anbindung der Verwaltung an das Hochschulnetz	111
Bild 5-9:	Nutzung des Hochschulnetzes als Virtual Private Network	111
Bild 5-10:	Einsatz von Encryption innerhalb der Verwaltung	113
Bild 5-11:	Geplantes geschlossenes Netz der Medizinischen Fakultät	117
Bild 5-12:	Im Aufbau befindliches offenes Netz der Medizinischen Fakultät	118
Bild 5-13:	Funktionen der beiden Datennetze innerhalb der Medizinischen Fakultät	118
Bild 5-14:	Prinzipielle Lösungsansätze für die Absicherung der vier Teilbereiche	120
Bild 5-15:	Sicherung durch vier physisch getrennte Medizin-Netze	121
Bild 5-16:	Sicherung durch Kaskadierung der Bereiche innerhalb der Kliniken	122
Bild 5-17:	Sicherung durch sternförmige Anordnung der Bereiche	123
Bild 5-18:	Sicherung durch VLANs und Schutz der zentralen Server durch Firewalls	125
Bild 5-19:	Getrennte Übertragung von Bildern und Daten	126
Tabelle 2-1:	Signalisierungsnachrichten nach UNI 3.0	14
Tabelle 2-2:	ATM-Service-Kategorie-Attribute bei TM 4.0	21
Tabelle 3-1:	Funktionsübersicht von Cisco Works for Switched Internetworking	43
Tabelle 3-2:	Funktionen des DA-30C bezüglich ATM	45

Tabelle 4-1:	Forderungen von TCSEC- und ITSEC-Sicherheitsklassen	55
Tabelle 4-2:	Durchsatz von DES-Verschlüsselungs-Implementationen	59
Tabelle 4-3:	Durchsatz von RSA-Verschlüsselungs-Implementationen	60
Tabelle 4-4:	Angriffsformen gegen Encryptionsysteme	61
Tabelle 4-5:	Vergleich von ausgewählten Firewall-Produkten	81
Tabelle 4-6:	Auszug aus dem Anwendungs-Szenario zur Firewall-Evaluierung	91
Tabelle 5-1:	Klassifizierung hinsichtlich des Datenschutzes	106
Tabelle 5-2:	Klassifizierung hinsichtlich der Datensicherheit	106
Tabelle 5-3:	DV-Verfahren der Hochschulverwaltungen und Schutzstufen	107
Tabelle 5-4:	Sicherheitsanforderungen in den einzelnen Klinikbereichen	115
Tabelle 5-5:	Relevante Ausgangsdaten für ein Sicherheitskonzept	127
Tabelle 7-1:	Vergleich von ATM-Switches (Teil 1)	135
Tabelle 7-2:	Vergleich von ATM-Switches (Teil 2)	136
Tabelle 7-3:	Vergleich von LAN-Switches (Teil 1)	136
Tabelle 7-4:	Vergleich von LAN-Switches (Teil 2)	137
Tabelle 7-5:	Vergleich von LAN-Switches (Teil 3)	138