

---

# Inhaltsverzeichnis

---

## Teil I Grundlagen

---

<b>1</b>	<b>Sicheres Netzwerkmanagement: Begriffserklärungen</b>	<b>3</b>
1.1	OSI Managementmodell	4
1.1.1	Funktionalität	4
1.1.2	Management Information Base	6
1.1.3	Zeit-Dimension	6
1.2	Netzwerkmanagement = Konfiguration + Überwachung	8
1.2.1	Netzwerkkonfiguration	9
1.2.2	Netzwerküberwachung	10
1.3	Sicheres Netzwerkmanagement	11
<b>2</b>	<b>Netzwerkmanagement Kategorien</b>	<b>15</b>
2.1	Homogene Netzwerke	15
2.2	Heterogene Netzwerke	17
2.3	Klassifikation des Datenverkehrs	18
2.3.1	Datenverkehr mit geringer Verzögerung	20
2.3.2	Datenverkehr mit hoher Bandbreite	21
2.3.3	Datenverkehr mit hoher Auslieferungszuverlässigkeit	21
2.3.4	Kostengünstiger Datenverkehr	22
2.3.5	Unpriorisierter Datenverkehr	22
2.4	In-Band Management	22
2.5	Out-of-Band Management	23
2.5.1	IP Managementnetzwerk	24
2.5.2	IPX Managementnetzwerk	25
2.5.3	Zentralisierte Punkt-zu-Punkt Verbindungen	25
2.5.4	Management über IPMI	26
2.6	Kombinierte Managementlösungen	27
2.6.1	Komplexität	28
2.6.2	Flexibilität	28
2.6.3	Dynamik	28

---

**Teil II Protokolle**

---

<b>3</b>	<b>ICMP: Netzwerkmanagement auf unterer Ebene</b>	<b>33</b>
3.1	Ursprünge des Protokolls ICMP	33
3.2	Paketformat	34
3.3	Nachrichtentypen	37
3.3.1	<i>Echo Reply (Typ 0)</i>	37
3.3.2	<i>Destination Unreachable (Typ 3)</i>	38
3.3.3	<i>Source Quench (Typ 4)</i>	40
3.3.4	<i>Redirect (Typ 5)</i>	41
3.3.5	<i>Echo (Typ 8)</i>	43
3.3.6	<i>Router Advertisement Message (Typ 9)</i>	44
3.3.7	<i>Router Solicitation Message (Typ 10)</i>	45
3.3.8	<i>Time Exceeded (Typ 11)</i>	46
3.3.9	<i>Parameter Problem (Typ 12)</i>	48
3.3.10	<i>Timestamp (Typ 13)</i>	48
3.3.11	<i>Timestamp Reply (Typ 14)</i>	50
3.3.12	<i>Information Request (Typ 15)</i>	51
3.3.13	<i>Information Reply (Typ 16)</i>	52
3.3.14	<i>Address Mask Request (Typ 17)</i>	53
3.3.15	<i>Address Mask Reply (Typ 18)</i>	54
3.3.16	<i>Traceroute (Typ 30)</i>	55
3.4	Auf ICMP basierende Werkzeuge	58
3.4.1	PING	58
3.4.2	TRACEROUTE / TRACERT	59
3.4.3	TRACEPATH	63
3.4.4	CLOCKDIFF	65
<b>4</b>	<b>Simple Network Management Protocol</b>	<b>69</b>
4.1	Transportmechanismen	70
4.2	Object Identifier	73
4.2.1	Tabellen	74
4.3	Structure of Management Information	79
4.3.1	SMIv1	81
4.3.2	SMIv2	88
4.3.3	SMIng	106
4.4	Management Information Base	108
4.4.1	MIB-I	110
4.4.2	MIB-II	111
4.5	SNMP Versionen	135
4.5.1	SNMP Version 1	135
4.5.2	SNMP Version 2	137
4.5.3	SNMP Version 3	142

<b>5</b>	<b>Logging</b> .....	151
5.1	syslog .....	152
5.1.1	Transportmechanismus .....	152
5.1.2	Architektur .....	152
5.1.3	Kritikalität .....	153
5.1.4	Nachrichtenherkunft .....	153
5.1.5	Paketformate .....	154
5.1.6	Sicherheitsaspekte .....	157
5.2	syslog-ng .....	157
5.2.1	Quelle .....	158
5.2.2	Ziel .....	162
5.2.3	Filter .....	166
5.2.4	Protokollpfad .....	166
<b>6</b>	<b>Intelligent Platform Management Interface</b> .....	169
6.1	Hardware .....	170
6.1.1	BMC .....	170
6.1.2	IPM Gerät .....	172
6.1.3	Spannungsversorgung .....	172
6.2	Kommunikationskanäle .....	172
6.2.1	IPMB .....	173
6.2.2	ICMB .....	174
6.2.3	System Schnittstelle .....	178
6.2.4	Serielle Schnittstelle .....	179
6.2.5	LAN .....	186
6.2.6	Serial Over LAN .....	190
6.2.7	PCI Management Bus .....	190
6.3	Sicherheitsmechanismen .....	190
6.3.1	Sessions .....	191
6.3.2	Authentifizierung .....	191
6.3.3	Integrität .....	193
6.3.4	Verschlüsselung .....	194
6.4	IPMI Nachrichten .....	195
6.4.1	Globale IPMI Befehle .....	195
6.4.2	Befehle zur Erkennung des verfügbaren Befehlssatzes .....	196
6.4.3	IPMI LAN Befehle .....	196
6.4.4	RMCP+ Befehle .....	196
6.4.5	Befehle für die Serielle Schnittstelle .....	197
6.4.6	Befehle für die SOL Kommunikation .....	200
6.4.7	Gehäuse-Befehle .....	200
6.4.8	Ereignis-Befehle .....	200
6.4.9	Befehle für ereignisbasierte Alarmer und Aktionen .....	203
6.4.10	Logging-Befehle für die SEL Datenbank .....	204
6.4.11	Befehle für die SDR Datenbank .....	206
6.4.12	Sensorbefehle .....	207

<b>7</b>	<b>IEEE 802.1X Port-basierte Netzwerk Zugriffskontrolle</b> . . . . .	209
7.1	Rollenkonzept . . . . .	210
7.1.1	Port . . . . .	211
7.1.2	Supplicant . . . . .	212
7.1.3	Authenticator . . . . .	213
7.1.4	Authentication Server . . . . .	216
7.2	Kontrollierte und unkontrollierte Ports . . . . .	217
7.2.1	Unkontrollierter Port . . . . .	217
7.2.2	Kontrollierter Port . . . . .	218
7.3	Authentifizierung . . . . .	220
7.3.1	EAP . . . . .	220
7.3.2	EAPOL . . . . .	221
7.4	IEEE 802.1X MIB . . . . .	223
7.4.1	Allgemeiner MIB-Zweig für alle IEEE 802.1X Systeme . . . . .	225
7.4.2	MIB-Zweig für Authenticator Systeme . . . . .	225
7.4.3	MIB-Zweig für Supplicants . . . . .	229
<b>8</b>	<b>Andere Kommunikationsformen und -wege des Netzwerkmanagements</b> . . . . .	233
8.1	RMON . . . . .	233
8.1.1	RMONv1 . . . . .	235
8.1.2	RMONv2 . . . . .	239
8.2	Proprietäre Client-Server-Lösungen . . . . .	241
8.2.1	Netzwerkmanagement mittels Web-Schnittstelle . . . . .	242
8.2.2	Netzwerkmanagement mittels Textkonsole . . . . .	244
8.2.3	Netzwerkmanagement mittels KVM Switch . . . . .	246

---

## Teil III Bedrohungen

---

<b>9</b>	<b>Sicherheit in Netzen</b> . . . . .	251
9.1	Bedrohungen . . . . .	252
9.1.1	Verlust von Informationen . . . . .	252
9.1.2	Bekanntwerden von Informationen . . . . .	257
9.1.3	Verfälschung von Informationen . . . . .	260
9.1.4	Vortäuschung von Informationen . . . . .	261
9.2	Angriffsformen . . . . .	262
9.2.1	Physikalische Angriffe . . . . .	263
9.2.2	Logische Angriffe . . . . .	266
9.3	Angriffsziele . . . . .	280
9.3.1	Angriffe auf Nutzdaten . . . . .	280
9.3.2	Angriffe auf die Infrastruktur . . . . .	281
9.3.3	Ungerichtete Angriffe . . . . .	285

<b>10</b>	<b>Auswirkungen auf das Netzwerkmanagement</b>	287
10.1	Der perfekte Schutz?	287
10.1.1	Ein spielerischer Vergleich	287
10.1.2	Ernüchterndes Ergebnis	293
10.2	Abschwächung von Bedrohungen	293
10.2.1	Verlust von Informationen	293
10.2.2	Bekanntwerden von Informationen	306
10.2.3	Verfälschung von Informationen	311
10.2.4	Vortäuschung von Informationen	315
10.3	Honeypots und Honeynets	317
10.3.1	Installation eines Honeypots	317
10.3.2	Überwachung der Aktivitäten	318
10.3.3	Auswertung der Informationen	319

---

## Teil IV Praxis

---

<b>11</b>	<b>Management Lösungen</b>	323
11.1	SNMP Werkzeuge	324
11.1.1	Kommerzielle Werkzeuge	324
11.1.2	Herstellereigene Lösungen	336
11.1.3	OpenSource Tools	341
11.1.4	Individuallösungen	353
11.2	IPMI Werkzeuge	356
11.2.1	Werkzeuge der IPMI Entwickler	356
11.2.2	Kommerzielle Werkzeuge	360
11.2.3	OpenSource Werkzeuge	365
11.3	IEEE 802.1X Werkzeuge	367
11.3.1	Kommerzielle Werkzeuge	367
11.3.2	OpenSource Implementierung	371
<b>12</b>	<b>Bilanzierung</b>	375
12.1	Notwendigkeit	376
12.2	Kostenrechnung	376
12.2.1	Kosten für die Netzwerkinfrastruktur	376
12.2.2	Kosten für den Betrieb des Netzwerkes	377
12.2.3	Kosten für die Netzwerksicherheit	377
12.3	Einfluss des Netzwerkmanagements auf das Netzwerk	379
<b>13</b>	<b>Neue Entwicklungen</b>	381
13.1	Mobile Geräte – Andere Verhaltensprofile	381
13.2	Leistungsstärkere Rechner – Höherer Schutzaufwand	382

<b>A</b>	<b>Request For Comments für das Simple Network Management Protocol</b> .....	385
A.1	SNMP .....	385
A.2	MIB .....	385
A.3	SMI .....	394
A.4	RMON .....	394
<b>B</b>	<b>IPMI-konforme Hersteller</b> .....	395
<b>C</b>	<b>Verzeichnis verwendeter Abkürzungen</b> .....	401
	<b>Literaturverzeichnis</b> .....	407
	<b>Sachverzeichnis</b> .....	419