

Netzwerkanalyse

Christian Zahler

9 „Sniffer“ zur Analyse des Netzwerkverkehrs

Im *Windows 2000 Server / Windows Server 2003* findet sich eine Light-Version des Programms „Netzwerkmonitor“.

Hinweis: Die Vollversion ist im *Systems Management Server* enthalten, mit dem der gesamte Netzwerkverkehr analysiert werden kann. Alle Header aller Protokolle können mit diesem Tool angesehen werden.

Alternative Tools wären zum Beispiel **ethereal**, für das aber ein eigener Treiber (WinPCap) nachinstalliert werden muss.

```

IP: ID = 0x6A86; Proto = TCP; Len: 395
IP: Version = 4 (0x4)
IP: Header Length = 20 (0x14)
IP: Precedence = Routine
IP: Type of Service = Normal Service
IP: Total Length = 395 (0x18B)
IP: Identification = 27270 (0x6A86)
+IP: Flags Summary = 2 (0x2)
IP: Fragment Offset = 0 (0x0) bytes
IP: Time to Live = 128 (0x80)
IP: Protocol = TCP - Transmission Control
IP: Checksum = 0xF632
IP: Source Address = 172.16.201.53
IP: Destination Address = 195.3.96.106
IP: Data: Number of data bytes remaining = 375 (0x0177)
    
```

```

TCP: AP..., len: 355, seq:2874991585-2874991940, ack:1121637879, win:19376, src: 2066 dst: 80
TCP: Source Port = 0x0812
TCP: Destination Port = Hypertext Transfer Protocol
TCP: Sequence Number = 2874991585 (0xAB5C3E1)
TCP: Acknowledgement Number = 1121637879 (0x42DAD5F7)
TCP: Data Offset = 20 (0x14)
TCP: Reserved = 0 (0x0000)
+TCP: Flags = 0x18 : .AP...
TCP: Window = 19376 (0x4980)
TCP: Checksum = 0xC639
TCP: Urgent Pointer = 0 (0x0)
TCP: Data: Number of data bytes remaining = 355 (0x0163)
    
```

```

HTTP: GET Request (from client using port 2066)
HTTP: Request Method = GET
HTTP: Uniform Resource Identifier = /horde/imp/menu.php?menu=200
HTTP: Protocol Version = HTTP/1.1
+HTTP: Undocumented Header = Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, */*
+HTTP: Undocumented Header = Accept-Language: de-at
+HTTP: Undocumented Header = Accept-Encoding: gzip, deflate
+HTTP: Undocumented Header = User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
+HTTP: Undocumented Header = Host: www.jet2mail.at
+HTTP: Undocumented Header = Connection: Keep-Alive
+HTTP: Undocumented Header = Cookie: chucknimplang=de; HordeSession=4a7f0a0932fcl2840e47c56463b93c
    
```

Filter setzen, um nur bestimmte Protokolle anzusehen: [Ansicht] - [Filter]

Anzeigefilter

AND
 Protocol == TCP
 ANY (<->) ANY

Hinzufügen
 Ausdruck...

Einfügen
 AND
 OR
 NOT

Ausdruck bearbeiten...

Löschen
 Zeile
 Zweig
 Alle

Laden... Speichern... OK Abbrechen Hilfe

Ausdruck

Ausdruck
 Protocol == TCP

Adresse Protokoll Eigenschaft

Aktivierte Protokolle		Deaktivierte Protokolle		
Name	Beschreibung	Deaktivieren	Name	Beschreibung
TCP:	Internet's TCP (Tr...	Aktivieren	AARP:	AppleTalk Adres...
		Alle deaktivieren	ADSP:	AppleTalk Data S...
		Alle aktivieren	AFP:	AppleTalk File Pr...
			AH:	IP Authentication
			ARP_RARP:	Internet's ARP/Rf...
			ASF:	AppleTalk Sessio...
			ATM:	ATM topology
			ATMARP:	ATM Arp Protocol
			ATMMARS:	ATMMARS Protoc...
			ATMMCAST:	ATMMCAST Prot...
			ATP:	AppleTalk Transa...

OK Abbrechen Hilfe

Netzwerk auswählen

Lokaler Computer

- ETHERNET, NDIS NPP, 86662052415
- ETHERNET, NDIS NPP, 0002B34C188

Blob-Kennzei... Wert

IDdC	TRUE
IESP	TRUE
IRTC	TRUE
ISts	TRUE
Ixmt	TRUE
ClassID	{425882B0-80BF-11CE-859F-0...
Dial-up Connec...	FALSE
MacAddress	0002B34C1880
Name	NDIS NPP
CurrentAddress	0002B34C1880
Flags	16400

OK Abbrechen Hilfe

Microsoft Netzwerkmonitor - [ETHERNET\NET 0002B34C1880 Sammlungsfenster]

Zeit vergangen: 00:00:06.578125

Netzwerkstatistik

- # Rahmen pro Sekunde: 36
- # Broadcasts: 30
- # Multicasts: 6
- # Bytes: 8853
- # Rahmen verloren: 0
- Netzwerkstatus: Normal

Gesamte Statistik

- # Rahmen: 37
- # Rahmen in Puffer: 36
- # verlorene Rahmen beim Pufferüberlauf: 0
- # Bytes: 8548
- # Bytes in Puffer: 8548
- % Puffer verwendet: 0
- # Rahmen verloren: 0

Netzwerkadresse	Rahmen gesendet	Empfangene Rahmen	Bytes gesendet	Bytes empfangen	Rahmen mit Ziel gesendet	Multicasts gesendet	Broadc...
*BROADCAST	0	0	0	7630	0	0	0
0002B3368A29	1	0	243	0	0	0	1
0002B3368DC8	5	0	771	0	0	0	5
0002B3368655	1	0	114	0	0	0	1
0002B34C33F4	6	0	188	0	0	0	2
0002B34C33F4	2	0	6382	0	0	0	21
00508B5A9630	21	0	0	918	0	0	0
00508B5A9630	0	6	0	0	0	0	0
USC IN000116	0	6	0	0	0	0	0

Netzwerkmonitor V5.00.2152

Microsoft Netzwerkmonitor - [Sammlung: 1 (Details)]

Rahmen	Zust	MAC-Quelladresse	MAC-Zieladresse	Protokoll	Beschreibung
1038	33...	LOCAL	00D0B7836375	TCP	.A...., len: 0, seq:2874991585-287499...
1039	33...	LOCAL	00D0B7836375	HTTP	GET Request: (from client using port 2066)
1040	33...	00D0B7836375	LOCAL	TCP	.A...., len: 0, seq:1121637879-112163...
1041	33...	00D0B7836375	LOCAL	HTTP	Response (to client using port 2066)
1042	33...	00D0B7836375	LOCAL	HTTP	Response (to client using port 2066)
1043	33...	LOCAL	00D0B7836375	TCP	.A...., len: 0, seq:2874991940-287499...
1044	33...	00D0B7836375	LOCAL	HTTP	Response (to client using port 2066)
1045	33...	00D0B7836375	LOCAL	HTTP	Response (to client using port 2066)

Frame: Base frame properties

```

+ETHERNET: Destination address = 00D0B7836375
+ETHERNET: Source address = 0002B34C1880
ETHERNET: Frame Length : 409 (0x0199)
ETHERNET: Ethernet Type : 0x0800 (IP: DOD Internet Protocol)
ETHERNET: Ethernet Data: Number of data bytes remaining = 395 (0x018B)
    
```

Ethernet/802.3 MAC Layer F#: 1039/1172 Off: 0 (x0) L: 14 (x4)