



## SMB Dialect Revision

Beim Zugriff auf ein Share wird zur Herstellung der Verbindung das SMB-Protokoll eingesetzt. Sofern es auf einem Client keine besonderen Einstellungen gibt, werden beim Aufbau der Verbindung alle zur Verfügung stehenden Dialekte (SMB-Revisionen) angeboten, siehe Punkt 1. Der Client bietet dem Server 5 verschiedene Dialekte an. Angefangen bei **Version 2.0.2** bis hin zur **Version 3.1.1**.

The screenshot shows a Wireshark capture of an SMB2 Negotiate Protocol Request. The packet list pane shows the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
2639	3.338907	172.18.32.111	172.18.32.32	SMB2	306	Negotiate Protocol Response
2640	3.339031	172.18.32.32	172.18.32.111	SMB2	232	Negotiate Protocol Request
2641	3.339192	172.18.32.111	172.18.32.32	SMB2	366	Negotiate Protocol Response
2644	3.339923	172.18.32.32	172.18.32.111	SMB2	491	Session Setup Request

The packet details pane for packet 2640 shows the following fields:

- StructureSize: 0x0024
- Dialect count: 5
- Security mode: 0x02, Signing required
- Reserved: 0000
- Capabilities: 0x0000007f, DFS, LEASING, LARGE MTU, MULTI CHANNEL, PERSISTENT HANDLES, DIRECTORY LEASING, ENCRYPTION
- Client Guid: 65e5bee6-bf0c-11eb-976b-000c2985020c
- NegotiateContextOffset: 0x00000070
- NegotiateContextCount: 2
- Reserved: 0000
- Dialect: SMB 2.0.2 (0x0202)
- Dialect: SMB 2.1 (0x0210)
- Dialect: SMB 3.0 (0x0300)
- Dialect: SMB 3.0.2 (0x0302)
- Dialect: SMB 3.1.1 (0x0311)
- Negotiate Context: SMB2\_PREAUTH\_INTEGRITY\_CAPABILITIES
- Negotiate Context: SMB2\_ENCRYPTION\_CAPABILITIES

Der Server antwortet mit Dialekt 3.1.1. Über diese SMB-Revision werden nun Daten ausgetauscht.

The screenshot shows a Wireshark capture of an SMB2 Negotiate Protocol Response. The packet list pane shows the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
2639	3.338907	172.18.32.111	172.18.32.32	SMB2	306	Negotiate Protocol Response
2640	3.339031	172.18.32.32	172.18.32.111	SMB2	232	Negotiate Protocol Request
2641	3.339192	172.18.32.111	172.18.32.32	SMB2	366	Negotiate Protocol Response
2644	3.339923	172.18.32.32	172.18.32.111	SMB2	491	Session Setup Request

The packet details pane for packet 2641 shows the following fields:

- NT Status: STATUS\_SUCCESS (0x00000000)
- Command: Negotiate Protocol (0)
- Credits granted: 1
- Flags: 0x00000001, Response
- Chain Offset: 0x00000000
- Message ID: 1
- Process ID: 0x0000feff
- Tree ID: 0x00000000
- Session ID: 0x0000000000000000
- Signature: 00000000000000000000000000000000
- [Response to: 2640]
- [Time from request: 0.000161000 seconds]
- Negotiate Protocol Response (0x00)
- StructureSize: 0x0041
- Security mode: 0x03, Signing enabled, Signing required
- Dialect: SMB 3.1.1 (0x0311)
- NegotiateContextCount: 2
- Server Guid: 481dd93d-e98a-4733-bda0-e7f1d4a5a922
- Capabilities: 0x0000003f, DFS, LEASING, LARGE MTU, MULTI CHANNEL, PERSISTENT HANDLES, DIRECTORY LEASING
- Max Transaction Size: 8388608
- Max Read Size: 8388608
- Max Write Size: 8388608
- Current Time: May 27, 2021 19:06:48.676171400 Mitteleuropäische Sommerzeit
- Boot Time: No time specified (0)
- Blob Offset: 0x00000000
- Blob Length: 120



## SMB Dialect Revision

Wenn man jetzt nur noch Dialekte der Version SMBv3 einsetzen möchte, dann kann das in der Registry fest konfiguriert werden.

Die Festsetzung der minimalen oder maximalen Version setzt kein Neustart voraus.

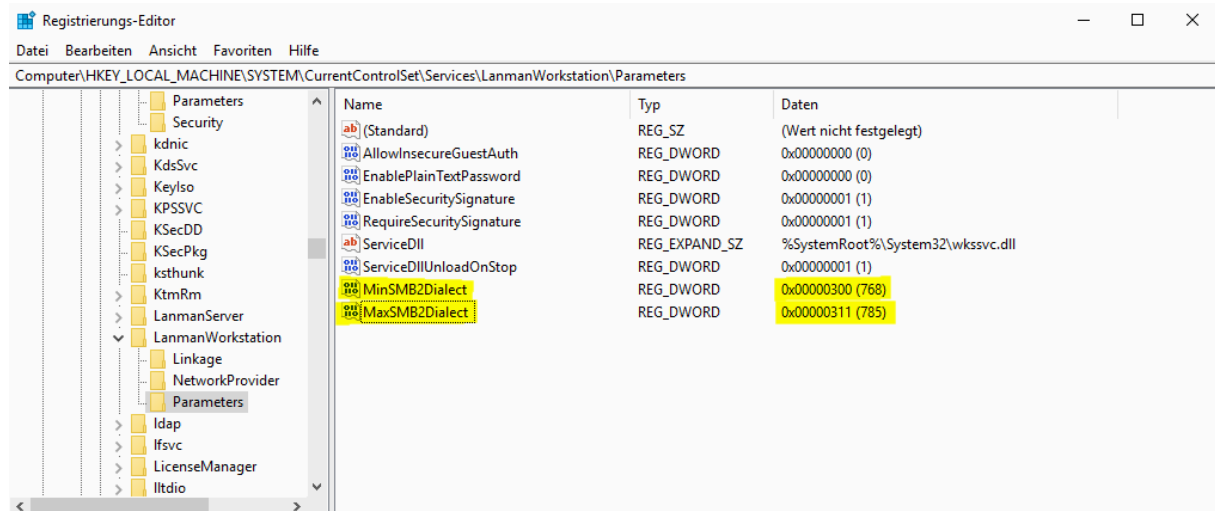
Unter diesem Pfad erstellen wir zwei neue Einträge.

Windows Registry Editor Version 5.00

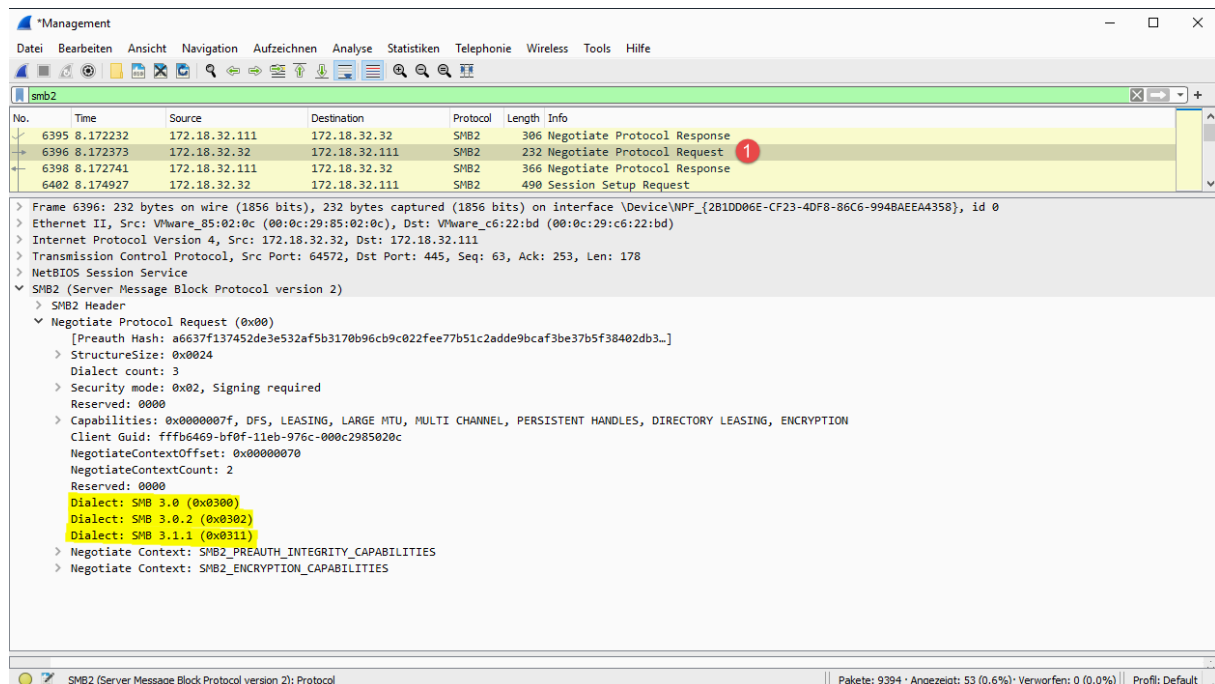
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]

"MinSMB2Dialect"=dword:00000300

"MaxSMB2Dialect"=dword:00000311



Ab sofort bietet der Client dem Server nur noch Dialekte der SMBv3 Version an.





## SMB Dialect Revision

Der Server antwortet wieder mit der höchsten Version, sofern er diese unterstützt. In diesem Fall mit der Version 3.1.1.

No.	Time	Source	Destination	Protocol	Length	Info
6395	8.172232	172.18.32.111	172.18.32.32	SMB2	306	Negotiate Protocol Response
6396	8.172373	172.18.32.32	172.18.32.111	SMB2	232	Negotiate Protocol Request
6398	8.172741	172.18.32.111	172.18.32.32	SMB2	366	Negotiate Protocol Response
6402	8.174927	172.18.32.32	172.18.32.111	SMB2	490	Session Setup Request

> Frame 6398: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits) on interface \Device\NPF\_{281DD06E-CF23-4DF8-86C6-9948AEEA4358}, id 0  
> Ethernet II, Src: VMware\_c6:22:bd (00:0c:29:c6:22:bd), Dst: VMware\_85:02:0c (00:0c:29:05:02:0c)  
> Internet Protocol Version 4, Src: 172.18.32.111, Dst: 172.18.32.32  
> Transmission Control Protocol, Src Port: 445, Dst Port: 64572, Seq: 253, Ack: 241, Len: 312  
> NetBIOS Session Service  
> SMB2 (Server Message Block Protocol version 2)  
 > SMB2 Header  
 > Negotiate Protocol Response (0x00)  
 > [Preauth Hash: b2662ca0bec21214a429746343cfe089030f4b721ae269e922bc464fd01ed66732886f3...]  
 > StructureSize: 0x0041  
 > Security mode: 0x03, Signing enabled, Signing required  
 > Dialect: SMB 3.1.1 (0x0311)  
 > NegotiateContextCount: 2  
 > Server Guid: 481dd93d-e98a-4733-bda0-e7f1d4a5a922  
 > Capabilities: 0x0000003f, DFS, LEASING, LARGE MTU, MULTI CHANNEL, PERSISTENT HANDLES, DIRECTORY LEASING  
 > Max Transaction Size: 8388608  
 > Max Read Size: 8388608  
 > Max Write Size: 8388608  
 > Current Time: May 27, 2021 19:23:29.687338800 Mitteleuropäische Sommerzeit  
 > Boot Time: No time specified (0)  
 > Blob Offset: 0x00000000  
 > Blob Length: 120  
 > Security Blob: 607606062b0601050502a06c306aa03c303a060a2b06010401823702021e06092a864882...  
 > NegotiateContextOffset: 0x000000f8  
 > Negotiate Context: SMB2\_PREAUTH\_INTEGRITY\_CAPABILITIES  
 > Negotiate Context: SMB2\_ENCRYPTION\_CAPABILITIES

Möchten wir stattdessen nur noch die Version 3.1.1 einsetzen, dann wird die minimale Dialekt-Revision gleich der maximalen Dialekt-Revision eingestellt.

### Windows Registry Editor Version 5.00

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]

"MinSMB2Dialect"=dword:00000311

"MaxSMB2Dialect"=dword:00000311

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
AllowInsecureGuestAuth	REG_DWORD	0x00000000 (0)
EnablePlainTextPassword	REG_DWORD	0x00000000 (0)
EnableSecuritySignature	REG_DWORD	0x00000001 (1)
MaxSMB2Dialect	REG_DWORD	0x00000311 (785)
MinSMB2Dialect	REG_DWORD	0x00000311 (785)
RequireSecuritySignature	REG_DWORD	0x00000001 (1)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\System32\wkssvc.dll
ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)



## SMB Dialect Revision

Der Client bietet dem Server nur noch die Dialekt-Revision 3.1.1 an.

The screenshot shows a Wireshark capture of an SMB negotiation. The packet list pane shows four packets: 6886 (Negotiate Protocol Response), 6887 (Negotiate Protocol Request), 6888 (Negotiate Protocol Response), and 6891 (Session Setup Request). Packet 6887 is highlighted with a red circle '1'. The packet details pane for packet 6887 shows the SMB2 header and the Negotiate Protocol Request structure. The 'Dialect' field is highlighted in yellow and shows 'SMB 3.1.1 (0x0311)'. Other fields include Preauth Hash, Structure Size, Security mode, Capabilities, Client Guid, and Negotiate Context.

Der Server ist damit einverstanden und antwortet mit der Dialekt-Revision 3.1.1.

The screenshot shows a Wireshark capture of an SMB negotiation. The packet list pane shows four packets: 6886 (Negotiate Protocol Response), 6887 (Negotiate Protocol Request), 6888 (Negotiate Protocol Response), and 6891 (Session Setup Request). Packet 6888 is highlighted with a red circle '2'. The packet details pane for packet 6888 shows the SMB2 header and the Negotiate Protocol Response structure. The 'Dialect' field is highlighted in yellow and shows 'SMB 3.1.1 (0x0311)'. Other fields include Preauth Hash, Structure Size, Security mode, Server Guid, Capabilities, Max Transaction Size, Max Read Size, Max Write Size, Current Time, Boot Time, Blob Offset, Blob Length, Security Blob, and Negotiate Context.



## SMB Dialect Revision

Dialekt Familie	Dialekt Revisionen	Revisions-Code
SMB 2.0.2	SMB 2.0.2 Dialekt-Revision	0x0202
SMB 2.1	SMB 2.1 Dialekt-Revision	0x0210
SMB 3.x	SMB 3.0 Dialekt-Revision	0x0300
	SMB 3.0.2 Dialekt-Revision	0x0302
	SMB 3.1.1 Dialekt-Revision	0x0311

Das Schaubild ist von Microsoft:

