CIFS / SMB

Common Internet File System / Server Message Block

Jaroslav Sýkora

Historie

SMB byl původně vyvinut okolo r. 1983 v IBM. Cílem byl transparentní přístup k souborům na vzdálených počítačích typu IBM-PC, propojených pomocí PC-Network (proprietární síťová technologie IBM) a s operačními systémy DOS.

SMB je protokol prezentační a aplikační vrstvy. Pro transport byl zároveň s SMB vyvinut protokol NetBIOS (Network Basic Input/Output System), který je dnes již zastaralý.

Hlavním výrobcem SMB softwaru je v současnosti firma Microsoft, v minulosti byl používán i na jiných systémech: SCO Xenix, OS/2, DEC VMS. Samozřejmě existují implementace i pro Unix/Linux.

V roce 1996 byl SMB přejmenován na CIFS, byla přidána podpora pro symlinky, hardlinky a velké soubory a rozpracována možnost odstranění závislostí na NetBIOS. Částečné specifikace byly poté Microsoftem postoupeny IETF jako *Internet draft*.

Windows Vista přináší úplně novou verzi protokolu – *SMB2*, která je nekompatibilní s předchozími verzemi. Výhodou je především celkové pročištění zastaralého protokolu – např. původní SMB má kolem 100 příkazů (některé jsou duplicitní), SMB2 jich má jen 19.

Síťový stack a rozvržení funkcí

Jak již bylo zmíněno výše, SMB je protokol aplikační a prezentační vrstvy. Jako takový poskytuje funkce pro:

- přístup k souborům na serveru
- tisk na tiskárnu připojenou k serveru
- prostředky pro meziprocesovou komunikaci (IPC) – pojmenované roury (*named pipes*)
- autentizace klienta

Pro přenos SMB paketů v síti byl dlouhou dobu (až do Windows 2000) používán protokol NetBIOS. Ten v původní implementaci (r. 1983) vykonával prakticky všechny funkce síťové až relační vrstvy. NetBIOS je určen pro malé sítě (původní IBM PC-Network umožňoval max. 80 stanic) s jedním segmentem, bez směrování a hierarchického členění. Jednotlivé stanice jsou identifikovány jedinečným jménem o délce 15 znaků (obvykle velká písmena). Nejzajímavější funkcí NetBIOS je podpora pro tzv.

„browsing“, tj. automatické vyhledání jednotlivých stanic v síti. (Prakticky se jedná o funkci „Okolní počítače“ ve Windows) Tato funkce je bohužel v prostředí TCP/IP implementována pomocí broadcastů, takže zejména při vyšším počtu stanic dochází k zahlcování sítě. Řešením je použít WINS server, který poté jako jediný udržuje seznam aktivních počítačů a ostatní stanice si tento seznam vždy pouze vyzvednou – je to tedy jakási obdoba DNS.

NetBIOS v původní implementaci zastával funkce síťové, transportní i relační vrstvy. S rozvojem větších a sofistikovanějších sítí – IPX, TCP/IP – byl NetBIOS poněkud okleštěn a jeho funkce redukovány; viz následující obrázek:

<table>
<tr><td>OSI</td><td colspan="4"></td><td>TCP/IP</td></tr>
<tr><td>Application
Presentation</td><td colspan="4">SMB</td><td rowspan="2">Application</td></tr>
<tr><td>Session</td><td>NetBIOS</td><td rowspan="2">NetBEUI</td><td>NetBIOS</td><td>NetBIOS</td></tr>
<tr><td>Transport</td><td rowspan="2">IPX[1]</td><td rowspan="2">DECnet</td><td>TCP&UDP</td><td>TCP/UDP</td></tr>
<tr><td>Network</td><td></td><td>IP</td><td>IP</td></tr>
<tr><td rowspan="2">Link</td><td rowspan="2">802.2,
802.3,802.5</td><td>802.2</td><td rowspan="2">Ethernet V2</td><td rowspan="2">Ethernet V2</td><td rowspan="2">Ethernet or
others</td></tr>
<tr><td>802.3,802.5</td></tr>
<tr><td>Physical</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

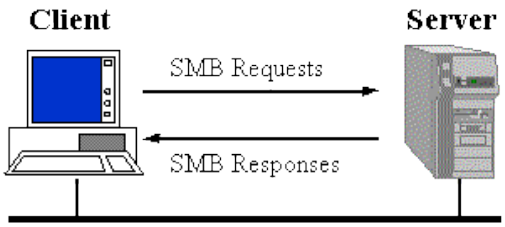
Prakticky se dnes můžeme setkat se dvěma variantami nasazení SMB/CIFS protokolu:

1. *SMB over NetBIOS over TCP/IP* (port tcp/139)
2. *CIFS over TCP/IP* (není na obrázku) (port tcp/445)

První varianta - *SMB over NetBIOS over TCP/IP* – se používala v produktech Microsoftu před Windows 2000. Tehdy byl SMB pevně spojen s NetBIOS. Od Windows 2000 je preferována druhá možnost - *CIFS over TCP/IP*, protokol NetBIOS již není potřeba.

Protokol SMB/CIFS

SMB je protokol typu klient/server. Existují pouze dva druhy zpráv: request a response. Server odpovídá na požadavek klienta, ale sám nikdy nezahajuje komunikaci (až na jednu výjimku při zamykání – viz dále). Komunikaci řídí klient – např. ve fázi autentizace nabízí klient různé metody ověření uživatele, které podporuje, a server mu odpoví, kterou metodu si vybral.



Obrázek schematicky zobrazuje SMB paket:

octet 1	2	3	4	5	6	7	8
RFC 1001 msg type (session)	SMB length (some reserve top 7 bits)			0xFF	'S'	'M'	'B'
SMB Command	Status (error) code				SMB flags	SMB flags2	
Process ID (high order)	SMB Signature						
SMB signature (continued)	Reserved			Tree Identifier		Process Id (Low)	
SMB User Identifier	Word Count	(variable number of 16 bit parameters follow)			Byte Count (size of data area)		(data area follows)

V následujících dvou příkladech: C->S je požadavek klienta, S->C je odpověď serveru.

Př 1: Typická sekvence SMB paketů: Počáteční kontakt, login, připojení stromu (tree connect)

1. C->S: Ustavení NetBIOS session. -- je otevřeno TCP spojení na port 139. (RFC1002)
2. S->C: Server odpoví pozitivním NetBIOS potvrzením
3. C->S: Dohodnutí verze CIFS. Klient zasílá seznam dialektů CIFS, kterým rozumí.
4. S->C: Server vybere konkrétní dialekt CIFS ze seznamu
5. C->S: Login uživatele. Klient posílá uživatelské jméno a heslo (mód *User level*)
6. S->C: Server vrací UID uživatele nebo chybu při špatném hesle
7. C->S: Příkaz: Připojit se ke konkrétnímu sdílenému prostředku (tree connect)
8. S->C: Server vrací číslo stromu (tree id – TID), nebo chybu.

Př 2: Otevření a čtení souboru

1. C->S: Příkaz: Otevři soubor. Posílá se především TID, UID a jméno souboru
2. S->C: Vrací ID souboru (FID), nebo chybu
3. C->S: Příkaz: Čti ze souboru (posílá se FID)
4. S->C: Vrací data ze souboru

SMB2 (Windows Vista a Windows Server 2008) je nová verze protokolu a ačkoliv používá stejný

port (tcp/445), je úplně nekompatibilní s předchozími verzemi. Mezi hlavní změny patří:

- hlavička paketu je lépe zarovnaná (*aligned)* a rozšířená na 64B (větší pole UID, TID, PID)
- všechny funkce přijímají „*handle*“, tj. jediná fce. přijímající řetězec cesty je OpenCreate()
- redundantní a zastaralé příkazy byly odstraněny (zbylo pouze 19 příkazů)
- větší limity
- lepší podpora symlinků

octet 1	2	3	4	5	6	7	8
RFC 1001 msg type (session)	SMB length			0xFE	'S'	'M'	'B'
SMB Header length (64)		reserved		Status (error) code			
SMB2 Command		Unknown		SMB2 Flags			
Reserved				Sequence number			
Sequence Number (continued)				Process Id			
Tree Identifier				SMB User Identifier			
SMB User Identifier				SMB Signature			
SMB Signature (continued)							
SMB Signature (continued)				SMB2 Parameter length (in bytes)		Variable length SMB Parm	Variable length SMB Data

Na obrázku výše je struktura SMB2 hlavičky.

Pro SMB/CIFS jsou definována rozšíření pro zlepšení kompatibility s POSIX systémy (Unix/Linux). Hlavní problémy, které tato rozšíření musí řešit, jsou:

- jak předávat UID/GID, mód souboru
- jak pracovat se symlinky
- jak pracovat se speciálními soubory (zařízení, fifo)
- rozdíly v sémantice zámků (POSIX – *advisory* vs CIFS – *mandatory)*

Zamykání souborů

Pro zrychlení přístupu k souborům na serveru používá SMB tzv. oportunistické zamykání souborů (*opportunistic locking*). Zamykání neslouží pro zajištění principu výlučného přístupu (když na jednom souboru chce pracovat více uživatelů zároveň), ale jedná se pouze o optimalizaci synchronizace cachí.

Jsou definovány tři druhy zámků:

- *Batch locks* – pokud klient ví, že daný soubor bude potřebovat otevřít a zavřít mnohokrát rychle za sebou, může si vyžádat Batch lock. Po sobě jdoucí sekvence close-open je pak možné vzájemně vyrušit.

- *Exclusive locks* – pokud klient otevře soubor a nikdo jiný ho nemá otevřený, pak klient obdrží Exclusive lock. V tomto případě klient může všechny zápisy do souboru cachovat u sebe bez rizika synchronizačních problémů. Pokud se poté soubor pokusí otevřít jiný klient, server pošle původnímu klientu zprávu *break* – klient zapíše všechny své změny (cache flush) a upustí svůj exkluzivní zámek. Toto je jediný případ v SMB protokolu, kdy server inicializuje komunikaci.
- *Level 2 OpLocks* – umožňuje klientovi cachovat požadavky na čtení ze souboru, nikoliv však na zápis.

Autentizace a zabezpečení

SMB/CIFS postupně podporoval několik různých způsobů přenosu a ověření hesla:

1. *LM hash* je nejstarší metoda; díky chybám v návrhu je dnes prolomitelná řádově za několik sekund. Hesla jsou max. 14 znaků dlouhá, malá písmena jsou převedena na velká. Hesla kratší než 14 znaků jsou nejprve doplněna na plnou délku. Poté je heslo rozděleno na dvě části po 7 znacích a každá část je použita jako klíč pro algoritmus DES, kterým je zašifrován známý konstantní text "KGS!@#$%". Dva výsledné šifrové texty o osmi znacích jsou spojeny a tvoří 16B hodnotu známou jako LM-hash. *Slabiny*: šifrováním dvou částí hesla samostatně dostáváme namísto 2^{84} pouze 2^{42} kombinací. Nejsou malá písmena, čili je dále omezen počet znaků vstupní abecedy. Není použita sůl (salt), takže se dají použít předpočítané tabulky hashů (*rainbow tables*).; Z důvodu kompatibility i moderní verze Windows podporují LM-hash – je proto vhodné zkontrolovat nastavení a LM-hash vypnout.
2. *NTLM (v1, v2)* je protokol typu výzva-odpověď. Server zasílá klientu výzvu – náhodný řetězec 8B. Klient tento řetězec definovaným způsobem zkombinuje s heslem a odešle odpověď serveru.
3. *Kerberos* – od Windows 2000. Preferovaná metoda pro domény Active Directory / LDAP.

SMB protokol rozeznává dva módy zabezpečení přístupu:

- *user level* – je v principu jednodušší. Klient při navazování spojení předává uživatelské jméno a heslo. Server vyhledá uživatele v databázi a provede ověření.
- *share level* – původní nejstarší model. Každý sdílený prostředek může mít přiděleno heslo, které klient musí znát. Nerozlišují se uživatelská jména.

Mód *Share level* je používán u starých verzí Windows, které nepodporují NT Domény. *User level* se používá právě při ověřování v NT Doméně.

NT Doména je technologie určená především pro centralizaci ověřování klientů (*Single Sign On* – SSO). V síti NT Domény (termín nemá nic společného s DNS doménou) jsou 4 druhy počítačů:

1. *Primary Domain Controller* (PDC) – server, který udržuje centrální databázi uživatelů i ostatních počítačů domény. Zajišťuje integritu autentizační databáze. Je vždy právě jeden.
2. *Backup Domain Controller* (BDC) – server, který si replikuje autentizační databázi z PDC a následně provádí ověřování klientů. Ověřování klientů může samozřejmě provádět i PDC, ale BDC je obvykle rychlejší.
3. *SMB server* – souborový server. Funguje v módu ověřování *User level* a uživatele ověřuje u PDC nebo BDC.
4. *člen domény – pracovní stanice*. Je zajímavé, že doménový účet na PDC nemají jen uživatelé, ale i jednotlivé pracovní stanice. Při registraci stanice do domény se pro stanici vytvoří účet se jménem podle jména počítače a náhodným heslem. Toto heslo by se mělo automaticky pravidelně měnit (cca jednou do měsíce). Po nabootování pracovní stanice ještě před přihlášením uživatele je nejprve ověřena identita stanice a pokud toto selže, nemůže se uživatel přihlásit.

Samba

Samba je open source implementace CIFS/SMB protokolu pro Unixové stroje. Protože protokol CIFS/SMB není oficiálně standardizován, musí být informace o nejnovějších rozšířeních CIFS protokolu získány reverse-engineeringem odchycených paketů.

Současná Samba 3 může na síti vystupovat v následujících rolích:

- *standalone server* – samostatně stojící server. Lze použít módy ověření *User level* nebo *Share level* (např. pro anonymní read-only servery).
- *NT Domain member* – člen NT domény, v módu User level si ověřuje hesla u PDC/BDC.
- *PDC nebo BDC server* – primární nebo záložní doménový server. Není možné kombinovat Microsoft-PDC a Samba-BDC nebo naopak, neboť protokol replikace databáze uživatelů mezi PDC a BDC je proprietární technologie Microsoftu (není to součást SMB). Jinými slovy PDC a BDC musí být od stejného „výrobce“.
- *nativní člen Active Directory Domény* – je to podobné, jako u členství v klasické NT Doméně.

Samba 3 nemůže být samotným *Active Directory Serverem* (ADS). Nicméně je možné zkombinovat Sambu se standardním LDAP serverem (*OpenLDAP*) a tím dosáhnout prakticky stejné funkcionality, jakou poskytuje AD-Doména.

Samba 4 (ve vývoji) by měla přinést podporu pro SMB2 a implementaci ADS.

Literatura

- SMB, NTLM; http://en.wikipedia.org/
- Samba; http://www.samba.org
- A New Network File System is Born: SMB2; http://svn.samba.org/samba/ftp/cifs-cvs/ols2007-smb2.pdf

Standardizace CIFS/SMB

- NetBIOS over TCP/IP: RFC1001, RFC1002
- A Common Internet File System (CIFS/1.0) Protocol, Preliminary Draft, http://tools.ietf.org/html/draft-leach-cifs-v1-spec-01
- MS CIFS Documentation, ftp://ftp.microsoft.com/developr/drg/CIFS/