CIFS/SMB
Common Internet File System
Server Message Block

- **Jaroslav Sýkora**

Obsah prezentace

- **Co je CIFS/SMB? Kde ho najdeme?**
- **Stručná historie**
- Síťový stack a rozvržení funkcí
- Protokol CIFS/SMB
- Zamykání
- Autentizace a zabezpečení
- Samba – open source implementace

Co je CIFS/SMB? Kde ho najdeme?

- síťový souborový systém
- SMB = Server Message Block
- CIFS = Common Internet File System
- implementace:
  - MS Windows – všechny verze
  - Unix/Linux - Samba

Stručná historie

- 1983 – IBM, DOS, PC-Network (síť max 80 stanic)
- NetBIOS je protokol (všech) nižších vrstev
- 1996 – SMB přejmenován na CIFS, pokus o standardizaci v IETF
- 2007 - SMB2 ve Windows Vista

Obsah prezentace

- Co je CIFS/SMB? Kde ho najdeme?
- Stručná historie
- **Síťový stack a rozvržení funkcí**
- Protokol CIFS/SMB
- Zamykání
- Autentizace a zabezpečení
- Samba – open source implementace

Síťový stack a funkce

- SMB/CIFS:
  - přístup k souborům na serveru
  - tisk na tiskárnu připojenou k serveru
  - meziprocesová komunikace (IPC)
  - autentizace klienta
- NetBIOS:
  - původně síťová, transportní a relační vrstva
  - adresace stanic – jméno 16 znaků
  - nesměrovatelný, nehierarchický
  - dnes – pouze relační vrstva nad TCP/IP

Síťový stack a funkce

<table>
<tr><th>OSI</th><th colspan="4"></th><th>TCP/IP</th></tr>
<tr><td>Application</td><td colspan="4" rowspan="2">SMB</td><td rowspan="2">Application</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td><td>NetBIOS</td><td rowspan="3">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>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 colspan="4"></td></tr>
</table>

Síťový stack a funkce

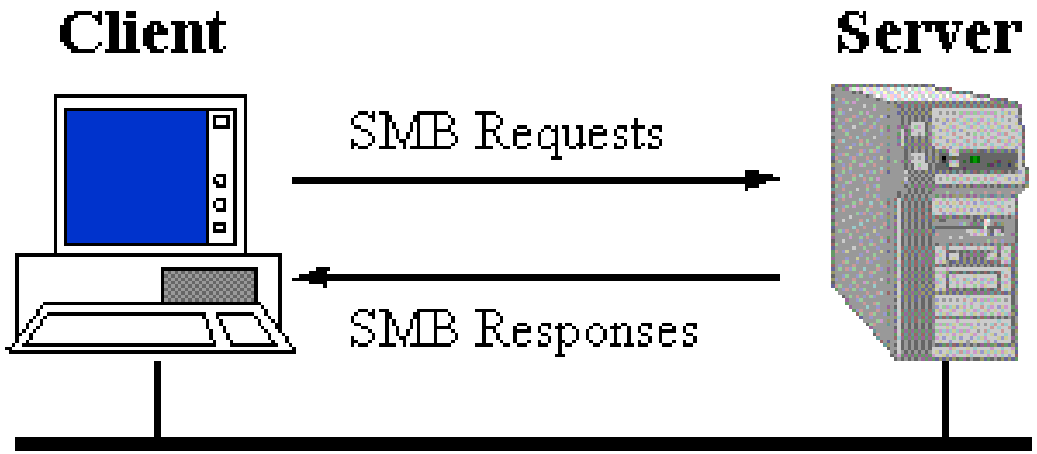
- dnes jsou dvě varianty nasazení:
  - SMB over NetBIOS over TCP/IP (port tcp/139)
  - CIFS over TCP/IP (port tcp/445)

Obsah prezentace

- Co je CIFS/SMB? Kde ho najdeme?
- Stručná historie
- Síťový stack a rozvržení funkcí
- **Protokol CIFS/SMB**
- **Zamykání**
- Autentizace a zabezpečení
- Samba – open source implementace

Protokol CIFS/SMB

- klient-server
- request-response
  - komunikaci řídí klient
- cca 100 příkazů, mnohé jsou redundantní



SMB paket

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
0xFF								'S'								'M'								'B'							
Command								Error Class								Must be zero								Error Code							
Error Code (continued)								Flags								Flags2															
Pad or security signature – typically pad and therefore must be zero																															
Tree ID (TID)																Process ID (PID)															
User ID (UID)																Multiplex ID (MID)															
WordCount								ParameterWords[WordCount] – the number of words in this variable size section is specified by the WordCount variable.																									
ByteCount																															
Buffer[ByteCount] – the number of bytes in this variable size section is specified by the ByteCount variable.																															

SMB2

- Windows Vista, Windows Server 2008
- nekompatibilní s předchozími verzemi:
  - hlavička paketu je lépe zarovnaná (aligned) a rozšířená na 64B
  - 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

CIFS – rozšíření pro POSIX

- při použití v POSIX systému (Linux) jsou potřeba rozšíření protokolu pro lepší kompatibilitu
  - 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 synchronizace cache
- *Batch Locks* – eliminují sekvence close-open
- *Exclusive Locks* – umožňují klientovy cachovat své zápisy
- *Level 2 OpLocks* - umožňují klientovy cachovat čtení

Autentizace a zabezpečení

- a) přenos a ověření hesla
- b) módy zabezpečení serveru
- c) krok stranou – NT Doména

Autentizace – přenos a ověření hesla

- LM-hash - nejstarší
  - používá DES, ale díky chybám je velmi slabý
- NTLM v1, v2
  - výzva-odpověď
- Kerberos
  - od Windows 2000

Módy zabezpečení serveru

- *User Level*
  - uživatel/heslo
- *Share Level*
  - pouze heslo

NT Doména

- (nemá nic společného s DNS doménou)
- *User Level* ověření v NT Doméně
- 4 druhy síťových prvků
  - Primary Domain Controller (PDC)
  - Backup Domain Controller (BDC)
  - SMB server
  - pracovní stanice

Obsah prezentace

- Co je CIFS/SMB? Kde ho najdeme?
- Stručná historie
- Síťový stack a rozvržení funkcí
- Protokol CIFS/SMB
- Zamykání
- Autentizace a zabezpečení
- **Samba – open source implementace**

Samba – open source implementace

- reverse-engineering odchycených paketů
- Samba 3:
  - standalone server
  - NT Domain member
  - PDC nebo BDC server
  - nativní člen Active Directory Domény
  - nemůže být hlavním AD Serverem

Samba – open source implementace

- budoucnost: Samba 4
  - SMB2
  - úplná podpora AD-Domény

Závěr

- SMB - zastaralý protokol, mnohokrát rozšiřovaný
- není standardizovaný
- fundamentální součást MS Windows
- nový start v podobě SMB2
- open source server Samba

Závěr

Otázky?

Literatura, standardy

- 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
- 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/