Server Message Block

In computer networking, **Server Message Block** (**SMB**), one version of which was also known as **Common Internet File System** (**CIFS** /sɪfs/),[1][2] is a communication protocol[3] for providing shared access to files, printers, and serial ports between nodes on a network. It also provides an authenticated inter-process communication (IPC) mechanism. Most usage of SMB involves computers running Microsoft Windows, where it was known as "Microsoft Windows Network" before the introduction of Active Directory. Corresponding Windows services are LAN Manager Server for the server component, and LAN Manager Workstation for the client component.[4]

Contents

Features

History
- SMB / CIFS / SMB1
- SMB 2.0
- SMB 2.1
- SMB 3.0
- SMB 3.0.2
- SMB 3.1.1

Implementation
- General issues
  - Performance issues
  - Microsoft's modifications
- Samba
- Netsmb
- NQ
- MoSMB
- Tuxera SMB
- Likewise
- CIFSD

Opportunistic locking

Security

Specifications

See also

References

External links

Features

Server Message Block provides file sharing, network browsing, printing, and inter-process communication (IPC) over a network.

The SMB protocol relies on lower-level protocols for transport.

The Microsoft SMB protocol was often used with NetBIOS over TCP/IP (NBT) over UDP, using port numbers 137 and 138, and TCP port numbers 137 and 139. NBT for use by NetBIOS is supported on Windows Server 2003, Windows XP, Windows 2000, Windows NT, and Windows Me/98/95. NetBIOS is not supported on Windows Vista, Windows Server 2008, and subsequent versions of Windows. SMB/NBT combination is generally used for backward compatibility.

The NetBIOS over NetBEUI protocol provides NetBIOS support for the NetBEUI protocol. This protocol is also called NetBIOS Frames (NBF). NBF is supported on Windows 2000, Windows NT, and Windows Me/98/95. NetBEUI is no longer supported on Windows XP and later. However, SMB Protocol can also be used without a separate transport protocol directly over TCP, port 445. NetBIOS was also supported over several legacy protocols such as IPX/SPX.

The SMB Inter-Process Communication (IPC) system provides named pipes and was one of the first inter-process mechanisms commonly available to programmers that provides a means for services to inherit the authentication carried out when a client first connects to an SMB server.

Some services that operate over named pipes, such as those which use Microsoft's own implementation of DCE/RPC over SMB, known as MSRPC over SMB, also allow MSRPC client programs to perform authentication, which overrides the authorization provided by the SMB server, but only in the context of the MSRPC client program that successfully makes the additional authentication.

SMB signing: Windows NT 4.0 Service Pack 3 and upwards have the capability to use cryptography to digitally sign SMB connections. The most common official term is "SMB signing". Other terms that have been used officially are "[SMB] Security Signatures", "SMB sequence numbers"[5] and "SMB Message Signing".[6] SMB signing may be configured individually for incoming SMB connections (handled by the "LanManServer" service) and outgoing SMB connections (handled by the "LanManWorkstation" service). The default setting from Windows 98 and upwards is to opportunistically sign outgoing connections whenever the server also supports this, and to fall back to unsigned SMB if both partners allow this. The default setting for Windows domain controllers from Windows Server 2003 and upwards is to not allow fall back for incoming connections.[7] The feature can also be turned on for any server running Windows NT 4.0 Service Pack 3 or later. This protects from man-in-the-middle attacks against the Clients retrieving their policies from domain controllers at login.[8]

SMB supports opportunistic locking—a special type of locking-mechanism—on files in order to improve performance.

SMB serves as the basis for Microsoft's Distributed File System implementation.

History

SMB / CIFS / SMB1

Barry Feigenbaum originally designed SMB at IBM in early 1983 with the aim of turning DOS INT 21h local file access into a networked file system.[9] Microsoft has made considerable modifications to the most commonly used version. Microsoft merged the SMB protocol with the LAN Manager product which it had started developing for OS/2 with 3Com around 1990, and continued to add features to the protocol in Windows for Workgroups (c. 1992) and in later versions of Windows.

SMB was originally designed to run on top of the NetBIOS/NetBEUI API (typically implemented with NBF, NetBIOS over IPX/SPX, or NBT). Since Windows 2000, SMB runs, by default, with a thin layer, similar to the Session Message packet of NBT's Session Service, on top of TCP, using TCP port 445 rather than TCP port 139—a feature known as "direct host SMB".[10]

Windows Server 2003, and older NAS devices use SMB1/CIFS natively. SMB1/CIFS is an extremely chatty protocol which is not such an issue on a local area network with low latency but becomes very slow on wide area networks as the back and forth handshake of the protocol magnifies the inherent high latency of such network. Later versions of the protocol reduced the high number of handshake exchanges. While Microsoft estimates that SMB1/CIFS comprises less than 10% of network traffic in the average Enterprise network, that is still a significant amount of traffic. One approach to mitigating the inefficiencies in the protocol is to use WAN Acceleration products such as those provided by Riverbed, Silver Peak, or Cisco Systems. A better approach is simply to eliminate SMB1/CIFS by upgrading the server infrastructure that uses it. This includes both NAS devices as well as Windows Server 2003. The most effective method in use currently to identify SMB1/CIFS traffic is to use a network analyzer tool such as Wireshark, etc., to identify SMB1/CIFS "talkers" and then decommission or upgrade them over time. Microsoft also provides an auditing tool in Windows Server 2016, which can be used to track down SMB1/CIFS talkers.[11]

In 1996, when Sun Microsystems announced WebNFS,[12] Microsoft launched an initiative to rename SMB to Common Internet File System (CIFS)[9] and added more features, including support for symbolic links, hard links, larger file sizes, and an initial attempt at supporting direct connections over TCP port 445 without requiring NetBIOS as a transport (a largely experimental effort that required further refinement). Microsoft submitted some partial specifications as Internet-Drafts to the IETF,[13] though these submissions have expired.

Microsoft "added SMB1 to the Windows Server 2012 R2 deprecation list in June 2013."[14] Windows Server 2016 and some versions of Windows 10 Fall Creators Update do not have SMB1 installed by default.[15]

SMB 2.0

Microsoft introduced a new version of the protocol (SMB 2.0 or SMB2) with Windows Vista in 2006[16] and Server 2008. Although the protocol is proprietary, its specification has been published to allow other systems to interoperate with Microsoft operating systems that use the new protocol.[17]

SMB2 reduces the 'chattiness' of the SMB 1.0 protocol by reducing the number of commands and subcommands from over a hundred to just nineteen.[18] It has mechanisms for pipelining, that is, sending additional requests before the response to a previous request arrives, thereby improving performance over high-latency links. It adds the ability to compound multiple actions into a single request, which significantly reduces the number of round-trips the client needs to make to the server, improving performance as a result.[18] SMB1 also has a compounding mechanism—known as AndX—to compound multiple actions, but Microsoft clients rarely use AndX. It also introduces the notion of "durable file handles": these allow a connection to an SMB server to survive brief network outages, as are typical in a wireless network, without having to incur the overhead of re-negotiating a new session.

SMB2 includes support for symbolic links. Other improvements include caching of file properties, improved message signing with HMAC SHA-256 hashing algorithm and better scalability by increasing the number of users, shares and open files per server among others.[18] The SMB1 protocol uses 16-bit data sizes, which amongst other things, limits the maximum block size to 64K. SMB2 uses 32- or 64-bit wide storage fields, and 128 bits in the case of file-handles, thereby removing previous constraints on block sizes, which improves performance with large file transfers over fast networks.[18]

Windows Vista/Server 2008 and later operating systems use SMB2 when communicating with other machines also capable of using SMB2. SMB1 continues in use for connections with older versions of Windows, as well various vendors' NAS solutions. Samba 3.5 also includes experimental support for SMB2.[19] Samba 3.6 fully supports SMB2, except the modification of user quotas using the Windows quota management tools.[20]

When SMB2 was introduced it brought a number of benefits over SMB1 for third party implementers of SMB protocols. SMB1, originally designed by IBM, was reverse engineered, and later became part of a wide variety of non-Windows operating systems such as Xenix, OS/2 and VMS (Pathworks). X/Open standardized it partially; it also had draft IETF standards which lapsed. (See http://ubiqx.org/cifs/Intro.html for historical detail.) SMB2 is also a relatively clean break with the past. Microsoft's SMB1 code has to work with a large variety of SMB clients and servers. SMB1 features many versions of information for commands (selecting what structure to return for a particular request) because features such as Unicode support were retro-fitted at a later date. SMB2 involves significantly reduced compatibility-testing for implementers of the protocol. SMB2 code has considerably less complexity since far less variability exists (for example, non-Unicode code paths become redundant as SMB2 requires Unicode support).

Apple is also migrating to SMB2 (from their own Apple Filing Protocol, now legacy) with OS X 10.9.[21] This transition was fraught with compatibility problems though.[22][23] Non-default support for SMB2 appeared in fact in OS X 10.7, when Apple abandoned Samba in favor of its own SMB implementation called SMBX.[21] Apple switched to its own SMBX implementation after Samba adopted GPLv3.[24][25]

The Linux kernel's CIFS client file system has SMB2 support since version 3.7.[26]

SMB 2.1

SMB 2.1, introduced with Windows 7 and Server 2008 R2, introduced minor performance enhancements with a new opportunistic locking mechanism.[27]

SMB 3.0

SMB 3.0 (previously named SMB 2.2)[28] was introduced with Windows 8[28] and Windows Server 2012.[28] It brought several significant changes that are intended to add functionality and improve SMB2 performance,[29] notably in virtualized data centers:

- the SMB Direct Protocol (SMB over remote direct memory access [RDMA])
- SMB Multichannel (multiple connections per SMB session),[30][31]
- SMB Transparent Failover[32][33]

It also introduces several security enhancements, such as end-to-end encryption and a new AES based signing algorithm.[34][35]

SMB 3.0.2

SMB 3.0.2 (known as 3.02 at the time) was introduced with Windows 8.1 and Windows Server 2012 R2;[36][37] in those and later releases, the earlier SMB version 1 can be optionally disabled to increase security.[38][39]

SMB 3.1.1

SMB 3.1.1 was introduced with Windows 10 and Windows Server 2016.[40] This version supports AES-128 GCM encryption in addition to AES-128 CCM encryption added in SMB3, and implements pre-authentication integrity check using SHA-512 hash. SMB 3.1.1 also makes secure negotiation mandatory when connecting to clients using SMB 2.x and higher.

Implementation

General issues

SMB works through a client–server approach, where a client makes specific requests and the server responds accordingly. One section of the SMB protocol specifically deals with access to filesystems, such that clients may make requests to a file server; but some other sections of the SMB protocol specialize in inter-process communication (IPC). The Inter-Process Communication (IPC) share, or ipc$, is a network share on computers running Microsoft Windows. This virtual share is used to facilitate communication between processes and computers over SMB, often to exchange data between computers that have been authenticated.

Developers have optimized the SMB protocol for local subnet usage, but users have also put SMB to work to access different subnets across the Internet—exploits involving file-sharing or print-sharing in MS Windows environments usually focus on such usage.

SMB servers make their file systems and other resources available to clients on the network. Client computers may want access to the shared file systems and printers on the server, and in this primary functionality SMB has become best-known and most heavily used. However, the SMB file-server aspect would count for little without the NT domains suite of protocols, which provide NT-style domain-based authentication at the very least. Almost all implementations of SMB servers use NT Domain authentication to validate user-access to resources.

Performance issues

The use of the SMB protocol has often correlated with a significant increase in broadcast traffic on a network. However the SMB itself does not use broadcasts—the broadcast problems commonly associated with SMB actually originate with the NetBIOS service location protocol. By default, a Microsoft Windows NT 4.0 server used NetBIOS to advertise and locate services. NetBIOS functions by broadcasting services available on a particular host at regular intervals. While this usually makes for an acceptable default in a network with a smaller number of hosts, increased broadcast traffic can cause problems as the number of hosts on the network increases. The implementation of name resolution infrastructure in the form of Windows Internet Naming Service (WINS) or Domain Name System (DNS) resolves this problem. WINS was a proprietary implementation used with Windows NT 4.0 networks, but brought about its own issues and complexities in the design and maintenance of a Microsoft network.

Since the release of Windows 2000, the use of WINS for name resolution has been deprecated by Microsoft, with hierarchical Dynamic DNS now configured as the default name resolution protocol for all Windows operating systems. Resolution of (short) NetBIOS names by DNS requires that a DNS client expand short names, usually by appending a connection-specific DNS suffix to its DNS lookup queries. WINS can still be configured on clients as a secondary name resolution protocol for interoperability with legacy Windows environments and applications. Further, Microsoft DNS servers can forward name resolution requests to legacy WINS servers in order to support name resolution integration with legacy (pre-Windows 2000) environments that do not support DNS.

Network designers have found that latency has a significant impact on the performance of the SMB 1.0 protocol, that it performs more poorly than other protocols like FTP. Monitoring reveals a high degree of "chattiness" and a disregard of network latency between hosts.[18] For example, a VPN connection over the Internet will often introduce network latency. Microsoft has explained that performance issues come about primarily because SMB 1.0 is a block-level rather than a streaming protocol, that was originally designed for small LANs; it has a block size that is limited to 64K, SMB signing creates an additional overhead and the TCP window size is not optimized for WAN links.[41] Solutions to this problem include the updated SMB 2.0 protocol,[42] Offline Files, TCP window scaling and WAN acceleration devices from various network vendors that cache and optimize SMB 1.0[43] and 2.0.[44]

Microsoft's modifications

Microsoft added several extensions to its own SMB implementation. For example, it added NTLM, followed by NTLMv2 authentication protocols, in order to address security weakness in the original LAN Manager authentication. LAN Manager authentication was implemented based on the original legacy SMB specification's requirement to use IBM "LAN Manager" passwords, but implemented DES in a flawed manner that allowed passwords to be cracked.[45] Later, Kerberos authentication was also added. The NT 4.0 Domain logon protocols initially used 40-bit encryption outside of the United States, because of export restrictions on stronger 128-bit encryption[46] (subsequently lifted in 1996 when President Bill Clinton signed Executive Order 13026[47]). Opportunistic locking support has changed with each server release.

Samba

In 1991 Andrew Tridgell started the development of Samba, a free-software re-implementation (using reverse engineering) of the SMB/CIFS networking protocol for Unix-like systems, initially to implement an SMB server to allow PC clients running the DEC Pathworks client to access files on SunOS machines.[9][48] Because of the importance of the SMB protocol in interacting with the widespread Microsoft Windows platform, Samba became a popular free software implementation of a compatible SMB client and server to allow non-Windows operating systems, such as Unix-like operating systems, to interoperate with Windows.

As of version 3 (2003), Samba provides file and print services for Microsoft Windows clients and can integrate with a Windows NT 4.0 server domain, either as a Primary Domain Controller (PDC) or as a domain member. Samba4 installations can act as an Active Directory domain controller or member server, at Windows 2008 domain and forest functional levels.[49]

Package managers in Linux distributions can search for the *cifs-utils* package. The package is from the Samba maintainers.

Netsmb

NSMB (Netsmb and SMBFS) is a family of in-kernel SMB client and server implementations in BSD operating systems. It was first contributed to FreeBSD 4.4 by Boris Popov, and is now found in a wide range of other BSD systems including NetBSD and macOS.[50] The implementations have diverged significantly ever since.[51]

The macOS version of NSMB is notable for its now-common scheme of representing symlinks. This "Minshall-French" format shows symlinks as textual files with a `.symlink` extension and a `Xsym\n` magic number, always 1067 bytes long. This format is also used for storing symlinks on naive SMB servers or unsupported filesystems. Samba supports this format with an `mfsymlink` option.[52] Docker on Windows also seems to use it.

NQ

NQ is a family of portable SMB client and server implementations developed by Visuality Systems (http://www.visualitynq.com/), an Israel-based company established in 1998 by Sam Widerman, formerly the CEO of Siemens Data Communications. The NQ family comprises an embedded SMB stack (written in C), a Pure Java SMB Client, and a storage SMB Server implementation. All solutions support the latest SMB 3.1.1 dialect. NQ for Linux (https://visualitynq.com/resources/articles/smb3-for-linux), NQ for WinCE (https://visualitynq.com/resources/articles/smb3-for-wince), iOS, Android, VxWorks and other real-time operating systems are all supported by the configurable NQ solution.

MoSMB

MoSMB is a proprietary SMB implementation for Linux and other Unix-like systems, developed by Ryussi Technologies. It supports only SMB 2.x and SMB 3.x.[53]

Tuxera SMB

Tuxera SMB is a proprietary SMB server implementation developed by Tuxera that can be run either in kernel or user space.[54] It supports SMB 3.1.1 and previous versions.

Likewise

Likewise developed a CIFS/SMB implementation (versions 1.0, 2.0, 2.1 and NFS 3.0) in 2009 that provided a multiprotocol, identity-aware platform for network access to files used in OEM storage products built on Linux/Unix based devices. The platform could be used for traditional NAS, Cloud Gateway, and Cloud Caching devices for providing secure access to files across a network. Likewise was purchased by EMC Isilon in 2012.

CIFSD

CIFSD is an open source In-kernel CIFS/SMB server implementation for Linux kernel. It has the following advantages over user-space implementations: It provides better performance, and it's easier to implement some features like SMB Direct. It supports SMB 3.1.1 and previous versions.

Opportunistic locking

In the SMB protocol, *opportunistic locking* is a mechanism designed to improve performance by controlling caching of network files by the client.[55] Unlike traditional locks, *OpLocks* are not strictly file locking or used to provide mutual exclusion.

There are four types of opportunistic locks:

Batch Locks

Batch OpLocks were created originally to support a particular behavior of DOS batch file execution operation in which the file is opened and closed many times in a short period, which is a performance problem. To solve this, a client may ask for an OpLock of type "batch". In this case, the client delays sending the close request and if a subsequent open request is given, the two requests cancel each other.[56]

Level 1 OpLocks / Exclusive Locks

When an application opens in "shared mode" a file hosted on an SMB server which is not opened by any other process (or other clients) the client receives an **exclusive OpLock** from the server. This means that the client may now assume that it is the only process with access to this particular file, and the client may now cache all changes to the file before committing it to the server. This is a performance improvement, since fewer round-trips are required in order to read and write to the file. If another client/process tries to open the same file, the server sends a message to the client (called a *break* or *revocation*) which invalidates the exclusive lock previously given to the client. The client then flushes all changes to the file.

Level 2 OpLocks

If an exclusive OpLock is held by a client and a locked file is opened by a third party, the client has to relinquish its exclusive OpLock to allow the other client's write/read access. A client may then receive a "Level 2 OpLock" from the server. A Level 2 OpLock allows the caching of read requests but excludes write caching.

Filter OpLocks

Added in NT 4.0, Filter Oplocks are similar to Level 2 OpLocks but prevent sharing-mode violations between file open and lock reception. Microsoft advises use of Filter OpLocks only where it is important to allow multiple readers and Level 2 OpLocks in other circumstances.

Clients holding an OpLock do not really hold a lock on the file, instead they are notified via a *break* when another client wants to access the file in a way inconsistent with their lock. The other client's request is held up while the break is being processed.

Breaks

In contrast with the SMB protocol's "standard" behavior, a break request may be sent *from* server *to* client. It informs the client that an OpLock is no longer valid. This happens, for example, when another client wishes to open a file in a way that invalidates the OpLock. The first client is then sent an OpLock break and required to send all its local changes (in case of batch or exclusive OpLocks), if any, and acknowledge the OpLock break. Upon this acknowledgment the server can reply to the second client in a consistent manner.

Security

Over the years, there have been many security vulnerabilities in Microsoft's implementation of the protocol or components on which it directly relies.[57][58] Other vendors' security vulnerabilities lie primarily in a lack of support for newer authentication protocols like NTLMv2 and Kerberos in favor of protocols like NTLMv1, LanMan, or plaintext passwords. Real-time attack tracking[59] shows that SMB is one of the primary attack vectors for intrusion attempts,[60] for example the 2014 Sony Pictures attack,[61] and the WannaCry ransomware attack of 2017.[62] In 2020, two SMB high-severity vulnerabilities were disclosed and dubbed as SMBGhost (CVE-2020-0796 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796)) and SMBleed (https://www.hackreports.com/smbleed-smbghost-latest-windows-smb-protocol-vulnerability-smbleedingghost/) (CVE-2020-1206 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1206)), which when chained together can provide RCE (Remote Code Execution) privilege to the attacker.[63]

Specifications

The specifications for the SMB are proprietary and were originally closed, thereby forcing other vendors and projects to reverse-engineer the protocol in order to interoperate with it. The SMB 1.0 protocol was eventually published some time after it was reverse engineered, whereas the SMB 2.0 protocol was made available from Microsoft's MSDN Open Specifications Developer Center from the outset.[64] There are a number of specifications that are relevant to the SMB protocol:

- [MS-CIFS]: Common Internet File System (CIFS) Protocol (https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cifs/d416ff7c-c536-406e-a951-4f04b2fd1d2b)
  - Specifies the Common Internet File System (CIFS) Protocol, a cross-platform, transport-independent protocol that provides a mechanism for client systems to use file and print services made available by server systems over a network
- [MS-SMB]: Server Message Block (SMB) Protocol (https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb/f210069c-7086-4dc2-885e-861d837df688)
  - Specifies the Server Message Block (SMB) Protocol, which defines extensions to the existing Common Internet File System (CIFS) specification that have been implemented by Microsoft since the publication of the CIFS specification.
- [MS-SMB2]: Server Message Block (SMB) Protocol Versions 2 and 3 (https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/5606ad47-5ee0-437a-817e-70c366052962)
  - Specifies the Server Message Block (SMB) Protocol Versions 2 and 3, which support the sharing of file and print resources between machines and extend the concepts from the Server Message Block Protocol.
- [MS-SMBD]: SMB2 Remote Direct Memory Access (RDMA) Transport Protocol (https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smbd/1ca5f4ae-e5b1-493d-b87d-f4464325e6e3)
  - Specifies the SMB2 Remote Direct Memory Access (RDMA) Transport Protocol, a wrapper for the existing SMB2 protocol that allows SMB2 packets to be delivered over RDMA-capable transports such as iWARP or Infiniband while utilizing the direct data placement (DDP) capabilities of these transports. Benefits include reduced CPU overhead, lower latency, and improved throughput.
- [MS-FSSO]: File Access Services System Overview (https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/WinArchive/%5bMS-FSSO%5d.pdf) (archived document (https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-winprotlp/df36f95e-6a6b-48d6-a3ae-35a17674f546) status)
  - Describes the intended functionality of the File Access Services System, how it interacts with systems and applications that need file services, and how it interacts with administrative clients to configure and manage the system. File Access Services uses multiple protocols for file access and file server administration. This document lists those protocols and describes how they are used to implement the File Access Services System. The system overviews are replaced by newer overviews.

See also

- List of products that support SMB
- Active Directory
- Administrative share
- Shared file access
- AppleTalk
- Network File System (protocol)
- Remote File System
- WebDAV
- Uniform Naming Convention
- DCE/RPC
- Network Neighborhood

References

1. "Common Internet File System" (https://technet.microsoft.com/en-us/library/cc939973.aspx). Microsoft TechNet Library. Archived (https://web.archive.org/web/20170707075835/https://technet.microsoft.com/en-us/library/cc939973.aspx) from the original on July 7, 2017. Retrieved August 20, 2013.
2. "Microsoft SMB Protocol and CIFS Protocol Overview" (http://msdn.microsoft.com/en-us/library/windows/desktop/aa365233(v=vs.85).aspx). Microsoft MSDN Library. July 25, 2013. Archived (https://web.archive.org/web/20130821210320/http://msdn.microsoft.com/en-us/library/windows/desktop/aa365233(v=vs.85).aspx) from the original on August 21, 2013. Retrieved August 20, 2013.
3. "Microsoft SMB Protocol and CIFS Protocol Overview" (http://msdn.microsoft.com/en-us/library/aa365233(VS.85).aspx). Microsoft. October 22, 2009. Archived (https://web.archive.org/web/20160802013033/https://msdn.microsoft.com/en-us/library/aa365233(vs.85).aspx) from the original on August 2, 2016. Retrieved April 10, 2019.
4. "Lan Manager Networking Concepts" (http://support.microsoft.com/kb/86899). Microsoft. Archived (https://web.archive.org/web/20121230184225/http://support.microsoft.com/kb/86899) from the original on December 30, 2012. Retrieved September 18, 2014.
5. "MSKB887429: Overview of Server Message Block signing" (http://support.microsoft.com/kb/887429). Microsoft Corporation. November 30, 2007. Archived (https://web.archive.org/web/20101120173639/http://support.microsoft.com/kb/887429) from the original on November 20, 2010. Retrieved October 24, 2012. "Security Signatures (SMB sequence numbers)"
6. Jesper M. Johansson (September 8, 2005). "How to Shoot Yourself in the Foot with Security, Part 1" (https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc512612(v=technet.10)). Microsoft Corporation. Archived (https://web.archive.org/web/20181019041254/https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc512612(v=technet.10)) from the original on October 19, 2018. Retrieved October 24, 2012. "This article addresses [...] Server Message Block (SMB) message signing."
7. "MSKB887429: Overview of Server Message Block signing" (http://support.microsoft.com/kb/887429). Microsoft Corporation. November 30, 2007. Archived (https://web.archive.org/web/20101120173639/http://support.microsoft.com/kb/887429) from the original on November 20, 2010. Retrieved October 24, 2012. "By default, SMB signing is required for incoming SMB sessions on Windows Server 2003-based domain controllers."
8. Jose Barreto (December 1, 2010). "The Basics of SMB Signing (covering both SMB1 and SMB2)" (http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx). Microsoft TechNet Server & Management Blogs. Archived (https://web.archive.org/web/20121202155239/http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx) from the original on December 2, 2012. Retrieved October 24, 2012. "This security mechanism in the SMB protocol helps avoid issues like tampering of packets and "man in the middle" attacks. [...] SMB signing is available in all currently supported versions of Windows, but it’s only enabled by default on Domain Controllers. This is recommended for Domain Controllers because SMB is the protocol used by clients to download Group Policy information. SMB signing provides a way to ensure that the client is receiving genuine Group Policy."
9. Tridgell, Andrew. "Myths About Samba" (https://www.samba.org/samba/docs/myths_about_samba.html). Archived (https://web.archive.org/web/20171020045502/https://www.samba.org/samba/docs/myths_about_samba.html) from the original on October 20, 2017. Retrieved January 3, 2016.
10. "Direct hosting of SMB over TCP/IP" (http://support.microsoft.com/kb/204279). Microsoft. October 11, 2007. Archived (https://web.archive.org/web/20110326164716/http://support.microsoft.com/kb/204279) from the original on March 26, 2011. Retrieved November 1, 2009.

11. Kyttle, Ralph (May 13, 2017). "SMB1 – Audit Active Usage using Message Analyzer" (https://blogs.technet.microsoft.com/ralphkyttle/2017/05/13/smb1-audit-active-usage-using-message-analyzer/). *Microsoft TechNet*. Microsoft. Archived (https://web.archive.org/web/20190328223802/https://blogs.technet.microsoft.com/ralphkyttle/2017/05/13/smb1-audit-active-usage-using-message-analyzer/) from the original on March 28, 2019. Retrieved March 28, 2019.
12. "WebNFS - Technical Overview" (https://web.archive.org/web/20070518204025/http://www.sun.com/software/webnfs/overview.xml). Archived from the original (http://www.sun.com/software/webnfs/overview.xml) on May 18, 2007.
13. * I. Heizer; P. Leach; D. Perry (June 13, 1996). "Common Internet File System Protocol (CIFS/1.0)" (https://tools.ietf.org/html/draft-heizer-cifs-v1-spec-00). Archived (https://web.archive.org/web/20190808115512/https://tools.ietf.org/html/draft-heizer-cifs-v1-spec-00) from the original on August 8, 2019. Retrieved December 10, 2017.

    - Paul J. Leach; Dilip C. Naik (January 3, 1997). "CIFS Logon and Pass Through Authentication" (http://tools.ietf.org/html/draft-leach-cifs-logon-spec).
    - Paul J. Leach; Dilip C. Naik (January 10, 1997). "CIFS/E Browser Protocol" (http://tools.ietf.org/html/draft-leach-cifs-browser-spec).
    - Paul J. Leach; Dilip C. Naik (January 31, 1997). "CIFS Printing Specification" (http://tools.ietf.org/html/draft-leach-cifs-print-spec).
    - Paul J. Leach; Dilip C. Naik (February 26, 1997). "CIFS Remote Administration Protocol" (http://tools.ietf.org/html/draft-leach-cifs-rap-spec).
    - Paul J. Leach; Dilip C. Naik (December 19, 1997). "A Common Internet File System (CIFS/1.0) Protocol" (https://tools.ietf.org/html/draft-leach-cifs-v1-spec).

14. "The Deprecation of SMB1 – You should be planning to get rid of this old SMB dialect – Jose Barreto's Blog" (https://blogs.technet.microsoft.com/josebda/2015/04/21/the-deprecation-of-smb1-you-should-be-planning-to-get-rid-of-this-old-smb-dialect/). *blogs.technet.microsoft.com*. Archived (https://web.archive.org/web/20170521154946/https://blogs.technet.microsoft.com/josebda/2015/04/21/the-deprecation-of-smb1-you-should-be-planning-to-get-rid-of-this-old-smb-dialect/) from the original on May 21, 2017. Retrieved October 9, 2019.
15. "SMBv1 is not installed by default in Windows 10 Fall Creators Update and Windows Server, version 1709 and later versions" (https://support.microsoft.com/en-us/help/4034314/smbv1-is-not-installed-by-default-in-windows). *support.microsoft.com*. Archived (https://web.archive.org/web/20191010052046/https://support.microsoft.com/en-us/help/4034314/smbv1-is-not-installed-by-default-in-windows) from the original on October 10, 2019. Retrieved October 9, 2019.
16. Navjot Virk and Prashanth Prahalad (March 10, 2006). "What's new in SMB in Windows Vista" (https://web.archive.org/web/20060505005515/http://blogs.msdn.com/chkdsk/archive/2006/03/10/548787.aspx). *Chk Your Dsks*. MSDN. Archived from the original (http://blogs.msdn.com/chkdsk/archive/2006/03/10/548787.aspx) on May 5, 2006. Retrieved May 1, 2006.
17. *Server Message Block (SMB) Protocol Versions 2 and 3* (https://docs.microsoft.com/openspecs/windows_protocols/ms-smb2). Windows Protocols. *Open Specifications* (Technical report). Microsoft Docs. Microsoft. MS-SMB2. Retrieved November 29, 2020.
18. Jose Barreto (December 9, 2008). "SMB2, a Complete Redesign of the Main Remote File Protocol for Windows" (https://www.webcitation.org/688rgkgbL?url=http://blogs.technet.com/b/josebda/archive/2008/12/05/smb2-a-complete-redesign-of-the-main-remote-file-protocol-for-windows.aspx). Microsoft TechNet Server & Management Blogs. Archived from the original (http://blogs.technet.com/josebda/archive/2008/12/05/smb2-a-complete-redesign-of-the-main-remote-file-protocol-for-windows.aspx) on June 3, 2012. Retrieved November 1, 2009.
19. "Samba 3.5.0 Available for Download" (https://www.samba.org/samba/history/samba-3.5.0.html). Archived (https://web.archive.org/web/20110724051402/http://www.samba.org/samba/history/samba-3.5.0.html) from the original on July 24, 2011. Retrieved July 8, 2011.

20. "Samba 3.6.0 Available for Download" (https://samba.org/samba/history/samba-3.6.0.html). Archived (https://web.archive.org/web/20110924042737/http://www.samba.org/samba/history/samba-3.6.0.html) from the original on September 24, 2011. Retrieved August 10, 2011.
21. Eran, Daniel (June 11, 2013). "Apple shifts from AFP file sharing to SMB2 in OS X 10.9 Mavericks" (http://appleinsider.com/articles/13/06/11/apple-shifts-from-afp-file-sharing-to-smb2-in-os-x-109-mavericks). Appleinsider.com. Archived (https://web.archive.org/web/20170212162139/http://appleinsider.com/articles/13/06/11/apple-shifts-from-afp-file-sharing-to-smb2-in-os-x-109-mavericks) from the original on February 12, 2017. Retrieved January 12, 2014.
22. Vaughan, Steven J. (October 28, 2013). "Mavericks' SMB2 problem and fixes" (https://www.zdnet.com/mavericks-smb2-problem-and-fixes-7000022519/). ZDNet. Archived (https://web.archive.org/web/20140105011410/http://www.zdnet.com/mavericks-smb2-problem-and-fixes-7000022519/) from the original on January 5, 2014. Retrieved January 12, 2014.
23. MacParc. "10.9: Switch the SMB stack to use SMB1 as default" (http://hints.macworld.com/article.php?story=20131122083837447). *Mac OS X Hints*. macworld.com. Archived (https://web.archive.org/web/20140112051604/http://hints.macworld.com/article.php?story=20131122083837447) from the original on January 12, 2014. Retrieved January 12, 2014.
24. Topher Kessler (March 23, 2011). "Say adios to Samba in OS X" (http://reviews.cnet.com/8301-13727_7-20046383-263.html). CNET. Archived (https://web.archive.org/web/20140115220216/http://reviews.cnet.com/8301-13727_7-20046383-263.html) from the original on January 15, 2014. Retrieved January 12, 2014.
25. Thom Holwerda (March 26, 2011). "Apple Ditches SAMBA in Favour of Homegrown Replacement" (http://www.osnews.com/story/24572/Apple_Ditches_SAMBA_in_Favour_of_Homegrown_Replacement). Archived (https://web.archive.org/web/20131102235327/http://www.osnews.com/story/24572/Apple_Ditches_SAMBA_in_Favour_of_Homegrown_Replacement) from the original on November 2, 2013. Retrieved January 12, 2014.
26. "Linux 3.7 - Linux Kernel Newbies" (https://kernelnewbies.org/Linux_3.7#head-7c9c911e4c41bcbc635cd8fa561278c833844bc2). Archived (https://web.archive.org/web/20160911130335/https://kernelnewbies.org/Linux_3.7#head-7c9c911e4c41bcbc635cd8fa561278c833844bc2) from the original on September 11, 2016. Retrieved September 4, 2016.
27. "Implementing an End-User Data Centralization Solution" (http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=d8541618-5c63-4c4d-a0fd-d942cd3d2ec6). Microsoft. October 21, 2009. pp. 10–11. Archived (https://web.archive.org/web/20100906141857/http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=d8541618-5c63-4c4d-a0fd-d942cd3d2ec6) from the original on September 6, 2010. Retrieved November 2, 2009.
28. Jeffrey Snover (April 19, 2012). "SMB 2.2 is now SMB 3.0" (https://cloudblogs.microsoft.com/windowsserver/2012/04/19/smb-2-2-is-now-smb-3-0/). *Windows Server Blog*. Retrieved July 6, 2020.
29. Chelsio Communications. "40G SMB Direct" (http://www.chelsio.com/chelsio-to-demonstrate-40g-smb-direct-rdma-over-ethernet-for-windows-server-2012/). Archived (https://web.archive.org/web/20130907065805/http://www.chelsio.com/chelsio-to-demonstrate-40g-smb-direct-rdma-over-ethernet-for-windows-server-2012/) from the original on September 7, 2013. Retrieved June 18, 2013.
30. Jose Barreto (October 19, 2012). "SNIA Tutorial on the SMB Protocol" (https://www.eiseverywhere.com/file_uploads/b4f7436c4bc86fe545abe9fc042d4a7f_JoseBarreto_SMB3_Remote_File_Protocol_revision.pdf) (PDF). Storage Networking Industry Association. Archived (https://web.archive.org/web/20130603133014/https://www.eiseverywhere.com/file_uploads/b4f7436c4bc86fe545abe9fc042d4a7f_JoseBarreto_SMB3_Remote_File_Protocol_revision.pdf) (PDF) from the original on June 3, 2013. Retrieved November 28, 2012.

31. Thomas Pfenning. "The Future of File Protocols: SMB 2.2 in the Datacenter" (https://web.archive.org/web/20120720020805/http://www.snia.org/sites/default/files2/SDC2011/presentations/keynote/ThomasPfenning_The_Future_of_File_Protocols-final.pdf) (PDF). Archived from the original (http://www.snia.org/sites/default/files2/SDC2011/presentations/keynote/ThomasPfenning_The_Future_of_File_Protocols-final.pdf) (PDF) on July 20, 2012.
32. Joergensen, Claus (June 7, 2012). "SMB Transparent Failover – making file shares continuously available" (https://blogs.technet.microsoft.com/clausjor/2012/06/07/smb-transparent-failover-making-file-shares-continuously-available/). *Microsoft TechNet*. Archived (https://web.archive.org/web/20190111144942/https://blogs.technet.microsoft.com/clausjor/2012/06/07/smb-transparent-failover-making-file-shares-continuously-available/) from the original on January 11, 2019. Retrieved February 1, 2017.
33. Savill, John (August 21, 2012). "New Ways to Enable High Availability for File Shares" (http://windowsitpro.com/windows-server-2012/new-ways-enable-high-availability-file-shares). *Windows IT Pro*. Archived (https://web.archive.org/web/20161127102639/http://windowsitpro.com/windows-server-2012/new-ways-enable-high-availability-file-shares) from the original on November 27, 2016. Retrieved February 1, 2017.
34. "SMB Security Enhancements" (https://technet.microsoft.com/en-us/library/dn551363.aspx). Microsoft Technet. January 15, 2014. Archived (https://web.archive.org/web/20141009101031/http://technet.microsoft.com/en-us/library/dn551363.aspx) from the original on October 9, 2014. Retrieved June 18, 2014.
35. Jose Barreto (May 5, 2013). "Updated Links on Windows Server 2012 File Server and SMB 3.0" (https://blogs.technet.microsoft.com/josebda/2013/05/05/updated-links-on-windows-server-2012-file-server-and-smb-3-0/). Microsoft TechNet Server & Management Blogs. Archived (https://web.archive.org/web/20160803070533/https://blogs.technet.microsoft.com/josebda/2013/05/05/updated-links-on-windows-server-2012-file-server-and-smb-3-0/) from the original on August 3, 2016. Retrieved August 14, 2016.
36. Jose Barreto (July 7, 2014). "Updated Links on Windows Server 2012 R2 File Server and SMB 3.02" (https://blogs.technet.microsoft.com/josebda/2014/07/07/updated-links-on-windows-server-2012-r2-file-server-and-smb-3-02/). Microsoft TechNet Server & Management Blogs. Archived (https://web.archive.org/web/20160826110750/https://blogs.technet.microsoft.com/josebda/2014/07/07/updated-links-on-windows-server-2012-r2-file-server-and-smb-3-02/) from the original on August 26, 2016. Retrieved August 14, 2016.
37. Jose Barreto (December 12, 2013). "Storage Developer Conference – SDC 2013 slides now publicly available. Here are the links to Microsoft slides…" (https://blogs.technet.microsoft.com/josebda/2013/12/12/storage-developer-conference-sdc-2013-slides-now-publicly-available-here-are-the-links-to-microsoft-slides/). Microsoft TechNet Server & Management Blogs. Archived (https://web.archive.org/web/20160826113828/https://blogs.technet.microsoft.com/josebda/2013/12/12/storage-developer-conference-sdc-2013-slides-now-publicly-available-here-are-the-links-to-microsoft-slides/) from the original on August 26, 2016. Retrieved August 14, 2016.
38. Eric Geier (December 5, 2013). "WindowsNetworking.com: Improvements in the SMB 3.0 and 3.02 Protocol Updates" (http://www.windowsnetworking.com/articles-tutorials/windows-server-2012/improvements-smb-30-and-302-protocol-updates.html). *WindowsNetworking.com*. Archived (https://web.archive.org/web/20150409010758/http://www.windowsnetworking.com/articles-tutorials/windows-server-2012/improvements-smb-30-and-302-protocol-updates.html) from the original on April 9, 2015. Retrieved April 6, 2015.
39. Jose Barreto (April 30, 2015). "SMB3 Networking Links for Windows Server 2012 R2" (https://blogs.technet.microsoft.com/josebda/2015/04/30/smb3-networking-links-for-windows-server-2012-r2/). Microsoft TechNet Server & Management Blogs. Archived (https://web.archive.org/web/20160826115342/https://blogs.technet.microsoft.com/josebda/2015/04/30/smb3-networking-links-for-windows-server-2012-r2/) from the original on August 26, 2016. Retrieved August 14, 2016.

40. Jose Barreto (May 5, 2015). "What's new in SMB 3.1.1 in the Windows Server 2016 Technical Preview 2" (https://blogs.technet.microsoft.com/josebda/2015/05/05/whats-new-in-smb-3-1-1-in-the-windows-server-2016-technical-preview-2/). Microsoft TechNet Server & Management Blogs. Archived (https://web.archive.org/web/20161008054848/https://blogs.technet.microsoft.com/josebda/2015/05/05/whats-new-in-smb-3-1-1-in-the-windows-server-2016-technical-preview-2/) from the original on October 8, 2016. Retrieved August 14, 2016.
41. Neil Carpenter (October 26, 2004). "SMB/CIFS Performance Over WAN Links" (https://docs.microsoft.com/en-us/archive/blogs/neilcar/smbcifs-performance-over-wan-links). Microsoft. Archived (https://web.archive.org/web/20200213113816/https://docs.microsoft.com/en-us/archive/blogs/neilcar/smbcifs-performance-over-wan-links) from the original on February 13, 2020. Retrieved February 13, 2020.
42. "What's New in SMB in Windows Server" (https://technet.microsoft.com/en-us/library/hh831474(v=ws.11).aspx). *Microsoft*. Archived (https://web.archive.org/web/20170211075409/https://technet.microsoft.com/en-us/library/hh831474(v=ws.11).aspx) from the original on February 11, 2017. Retrieved February 6, 2017.
43. Mark Rabinovich, Igor Gokhman. "CIFS Acceleration Techniques" (https://www.snia.org/sites/default/orig/sdc_archives/2009_presentations/monday/MarkRabinovich-IgorGokhman-CIFS_Acceleration_Techniques.pdf) (PDF). Storage Developer Conference, SNIA, Santa Clara 2009. Retrieved July 6, 2020.
44. Mark Rabinovich. "Accelerating SMB2" (https://www.snia.org/sites/default/orig/SDC2011/presentations/wednesday/MarkRabinovichAccelerating_SMB2.pdf) (PDF). Storage Developer Conference, SNIA, Santa Clara 2011. Retrieved July 6, 2020.
45. Christopher Hertel (1999). "SMB: The Server Message Block Protocol" (http://ubiqx.org/cifs/SMB.html). Archived (https://web.archive.org/web/20100310140946/http://ubiqx.org/cifs/SMB.html) from the original on March 10, 2010. Retrieved November 1, 2009.
46. "Description of Microsoft Windows Encryption Pack 1" (http://support.microsoft.com/kb/159709). Microsoft. November 1, 2006. Archived (https://web.archive.org/web/20091002075623/http://support.microsoft.com/kb/159709) from the original on October 2, 2009. Retrieved November 1, 2009.
47. "US Executive Order 13026" (http://www.gpo.gov/fdsys/pkg/WCPD-1996-11-18/pdf/WCPD-1996-11-18-Pg2399.pdf) (PDF). United States Government. 1996. Archived (https://web.archive.org/web/20091010125029/http://www.gpo.gov/fdsys/pkg/WCPD-1996-11-18/pdf/WCPD-1996-11-18-Pg2399.pdf) (PDF) from the original on October 10, 2009. Retrieved November 1, 2009.
48. Tridgell, Andrew (June 27, 1997). "A bit of history and a bit of fun" (http://www.rxn.com/services/faq/smb/samba.history.txt). Archived (https://web.archive.org/web/20110717071846/http://www.rxn.com/services/faq/smb/samba.history.txt) from the original on July 17, 2011. Retrieved July 26, 2011.
49. "Samba 4 functional levels" (http://samba.2283325.n4.nabble.com/Samba-4-functional-levels-td3322760.html). February 25, 2011. Archived (https://web.archive.org/web/20140729014411/http://samba.2283325.n4.nabble.com/Samba-4-functional-levels-td3322760.html) from the original on July 29, 2014. Retrieved January 12, 2014.
50. "netsmb(4)" (https://man.openbsd.org/NetBSD-8.0/man4/netsmb.4). *NetBSD 8.0 manual pages*. Retrieved January 5, 2020.
51. `nbsd.conf(5)` (https://www.freebsd.org/cgi/man.cgi?query=nbsd.conf&sektion=5) – FreeBSD File Formats Manual. `nbsd.conf(5)` (https://gist.github.com/ppdac/2439540c04bb88d2448305247c81c3db) – Darwin and macOS File Formats Manual.
52. "UNIX Extensions" (https://wiki.samba.org/index.php/UNIX_Extensions#Storing_symlinks_on_Windows_servers). *SambaWiki*. Archived (https://web.archive.org/web/20200612000308/https://wiki.samba.org/index.php/UNIX_Extensions#Storing_symlinks_on_Windows_servers) from the original on June 12, 2020. Retrieved March 15, 2020.

53. Dr. Sunu Engineer. "Building a Highly Scalable and Performant SMB Protocol Server" (http://www.snia.org/sites/default/files/SDC/2016/presentations/smb/Sunu_Engineer_Building_Highly_Scalable_Performant_SMB_Protocol_Server.pdf) (PDF). Archived (https://web.archive.org/web/20160927162136/http://www.snia.org/sites/default/files/SDC/2016/presentations/smb/Sunu_Engineer_Building_Highly_Scalable_Performant_SMB_Protocol_Server.pdf) (PDF) from the original on September 27, 2016. Retrieved September 25, 2016.
54. "Microsoft and Tuxera strengthen partnership through Tuxera SMB Server" (https://news.microsoft.com/2016/09/14/microsoft-and-tuxera-strengthen-partnership-through-tuxera-smb-server). *Microsoft*. Microsoft News Center. Archived (https://web.archive.org/web/20161117044100/http://news.microsoft.com/2016/09/14/microsoft-and-tuxera-strengthen-partnership-through-tuxera-smb-server/) from the original on November 17, 2016. Retrieved February 6, 2017.
55. "Opportunistic Locks" (http://msdn.microsoft.com/en-us/library/windows/desktop/aa365433(v=vs.85).aspx). Microsoft. Archived (https://web.archive.org/web/20121023103306/http://msdn.microsoft.com/en-us/library/windows/desktop/aa365433(v=vs.85).aspx) from the original on October 23, 2012. Retrieved November 6, 2012.
56. Sphere, I.T. (2014), *All About Opportunistic Locking* (http://www.sphereitconsulting.co.uk/blog/servers-and-networks/all-about-opportunistic-locks/), archived (https://web.archive.org/web/20140413130609/http://www.sphereitconsulting.co.uk/blog/servers-and-networks/all-about-opportunistic-locks/) from the original on April 13, 2014, retrieved April 9, 2014
57. "MS02-070: Flaw in SMB Signing May Permit Group Policy to Be Modified" (http://support.microsoft.com/kb/329170). Microsoft. December 1, 2007. Archived (https://web.archive.org/web/20091008113615/http://support.microsoft.com/kb/329170) from the original on October 8, 2009. Retrieved November 1, 2009.
58. "MS09-001: Vulnerabilities in SMB could allow remote code execution" (http://support.microsoft.com/kb/958687). Microsoft. January 13, 2009. Archived (https://web.archive.org/web/20091005062727/http://support.microsoft.com/kb/958687) from the original on October 5, 2009. Retrieved November 1, 2009.,
59. "Sicherheitstacho.eu" (http://www.sicherheitstacho.eu). Deutsche Telekom. March 7, 2013. Archived (https://web.archive.org/web/20130308043532/http://www.sicherheitstacho.eu/) from the original on March 8, 2013. Retrieved March 7, 2013.
60. "Alert (TA14-353A) Targeted Destructive Malware" (https://www.us-cert.gov/ncas/alerts/TA14-353A). US-CERT. Archived (https://web.archive.org/web/20141220134115/https://www.us-cert.gov/ncas/alerts/TA14-353A) from the original on December 20, 2014. Retrieved December 20, 2014.
61. "Sony Hackers Used Server Message Block (SMB) Worm Tool" (http://www.securityweek.com/hackers-used-sophisticated-smb-worm-tool-attack-sony). Archived (https://web.archive.org/web/20141220134150/http://www.securityweek.com/hackers-used-sophisticated-smb-worm-tool-attack-sony) from the original on December 20, 2014. Retrieved December 20, 2014.
62. "WannaCry Ransomware Attack Hits Victims With Microsoft SMB Exploit" (http://www.eweek.com/security/wannacry-ransomware-attack-hits-victims-with-microsoft-smb-exploit). *eWeek*. Retrieved May 13, 2017.
63. "SMBleedingGhost Writeup: Chaining SMBleed (CVE-2020-1206) with SMBGhost" (https://blog.zecops.com/vulnerabilities/smbleedingghost-writeup-chaining-smbleed-cve-2020-1206-with-smbghost/). *ZecOps Blog*. June 9, 2020. Retrieved November 19, 2020.
64. "Windows Protocols" (http://msdn.microsoft.com/en-us/library/cc216517%28PROT.10%29.aspx). Archived (https://web.archive.org/web/20090926202714/http://msdn.microsoft.com/en-us/library/cc216517(PROT.10).aspx) from the original on September 26, 2009. Retrieved October 13, 2009.

External links

- DFS section in "Windows Developer" documentation (https://docs.microsoft.com/en-us/windows/win32/dfs/distributed-file-system)
- Hertel, Christopher (2003). *Implementing CIFS – The Common Internet FileSystem (http://www.ubiqx.org/cifs/Book.html)*. Prentice Hall. ISBN 0-13-047116-X. (Text licensed under the Open Publication License, v1.0 or later, available from the link above.)
- Common Internet File System (https://technet.microsoft.com/en-us/library/cc939973.aspx), technical details from Microsoft Corporation
- the NT LM 0.12 dialect of SMB (https://www.samba.org/samba/ftp/specs/smb-nt01.doc). In Microsoft Word format
- Steven M. French, A New Network File System is Born: Comparison of SMB2, CIFS, and NFS (https://www.kernel.org/doc/ols/2007/ols2007v1-pages-131-140.pdf), Linux Symposium 2007
- Steve French, The Future of File Protocols: SMB2 Meets Linux (https://www.samba.org/~sfrench/presentations/smf-linux-collab-summmit-future-of-file-protocols-smb2.2.pdf), Linux Collaboration Summit 2012

Retrieved from "https://en.wikipedia.org/w/index.php?title=Server_Message_Block&oldid=1014840778"

This page was last edited on 29 March 2021, at 11:20 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.