
COBOL

SMB/CIFS

It's not dead yet.

Christopher R. Hertel
Storage Architect and CIFS Geek
Founder and CTO
www.ubiqx.com

Connectathon ● February, 2010

Introductions

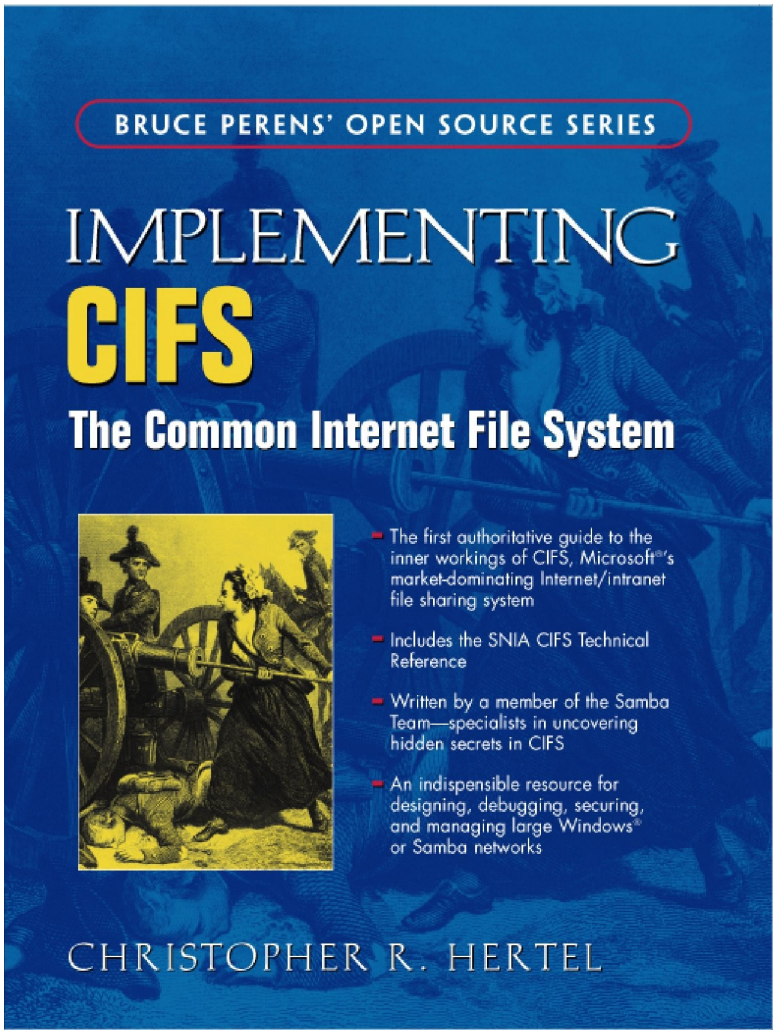
Who Is This Geek?

If you work on an SMB/CIFS implementation, you have likely stumbled across my name somewhere.

Who Is This Geek?

For good or ill, I have accidentally become:

- *The* SMB/CIFS documentation geek,
- Purveyor of protocol pedanticism, and
- Chronicler of the apopsicle.



Who Is This Geek?

I recently co-authored two new SMB/CIFS protocol specifications for Microsoft:

[MS-CIFS]

- Covers SMB/CIFS in Windows NT and 98.

[MS-SMB] (revised)

- Rewritten to reference [MS-CIFS].
- Details changes made from NT from W2K to Windows 7.

Who Is This Geek?

Let me get this straight...

- a Samba Team geek...
- formed a company that was...
- contracted by Microsoft...
- to produce *publicly available* specifications...
- for SMB/CIFS?!

Wait... What?

Who Is This Geek?

Terms and Conditions

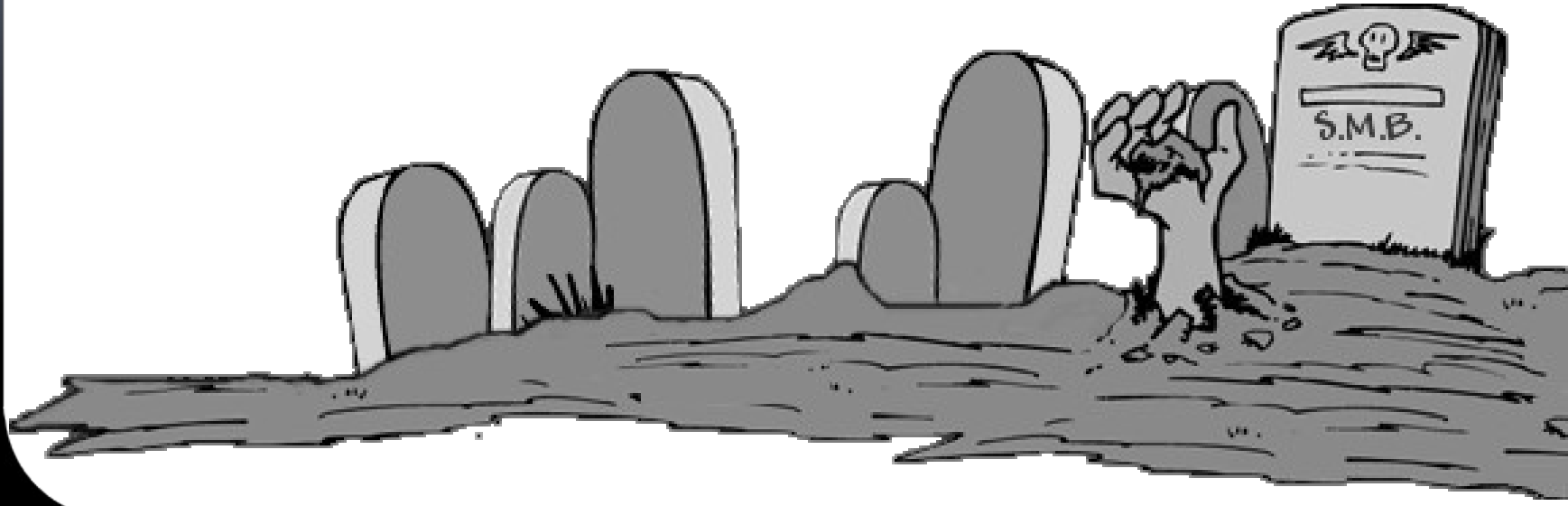
Interlude
SMB/CIFS: It's Not Dead Yet

SMB/CIFS: It's not dead yet.

I come to bury CIFS, not to praise it...

SMB/CIFS: It's still not dead yet.

...but it keeps coming back to haunt me.



SMB/CIFS: Still not dead.

CIFS is the COBOL of Network File Systems.

...and it's still not dead yet too.

SMB/CIFS: I Feel Happy!

Lots of products leverage SMB/CIFS file sharing to interact with home and business networks.

The Long and Arduous History

(briefly told)

Of SMB/CIFS Documentation

SMB/CIFS: History

In the early days, *SMB was documented:*

1984: IBM Personal Computer Seminar Proceedings, Volume 2, Number 8

1986: OpenNET/Microsoft Networks FILE SHARING PROTOCOL EXTENSIONS, Version 1.9, Microsoft and Intel (XENIX extensions)

1988: Microsoft Networks/OpenNet, Document Version 2, Microsoft and Intel (Core)

1988: Microsoft Networks SMB File Sharing Protocol Extensions Version 2.0, Document Version 3.3, Microsoft Corporation (LAN Manager 1.0)

1989: Microsoft Networks SMB File Sharing Protocol Extensions Version 3.0, Document Version 1.09, Microsoft Corporation (LAN Manager 1.2)

1990: Microsoft Networks SMB File Sharing Protocol Extensions Version 3.0, Document Version 1.11, Microsoft Corporation (LAN Manager 2.0)

1992: Microsoft Networks SMB Filesharing Protocol Extensions, Document Version 3.4, Microsoft Corporation (LAN Manager 2.1)

SMB/CIFS: History

Then things started thinning out.

1992: X/Open CAE Specification, Protocols for X/Open PC Interworking: SMB, Version 2, X/Open Company, Ltd. (Core through LAN Manager 2.0)

1996: Microsoft Networks SMB File Sharing Protocol, Document Version 6.0p, Microsoft (Unfinished draft of NT LAN Manager 1.0 documentation.)

1997: A Common Internet File System (CIFS/1.0) Protocol, IETF INTERNET-DRAFT, Paul J. Leach, Dilip C. Naik (Unfinished draft v2 of NT LAN Manager 0.12 specification.)

2002: Common Internet File System (CIFS) Technical Reference, Revision: 1.0, Storage Networking Industry Association (SNIA)

2003: Implementing CIFS, yours truly, Prentice Hall PTR

2004: The Mystery Document.

SMB/CIFS: History

During this time...

- Windows NT
- Windows 2000
- Windows XP
- Windows 2003
- Windows Vista
- Windows 7 & 2008

...and we knew that the documentation we already had was, in places,

- Incorrect
- Incomplete
- Incomprehensible

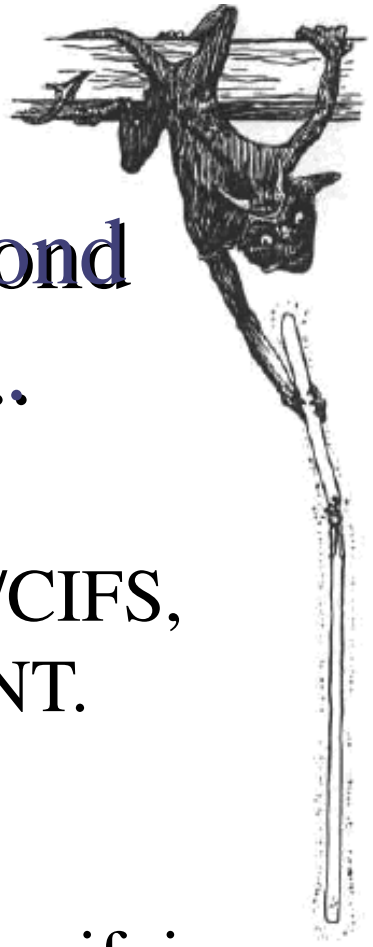
Never ascribe to malice that which is adequately explained by incompetence.

— attributed to Napoleon Bonaparte, among others

SMB/CIFS: History

This situation made people unhappy.

SMB/CIFS: History

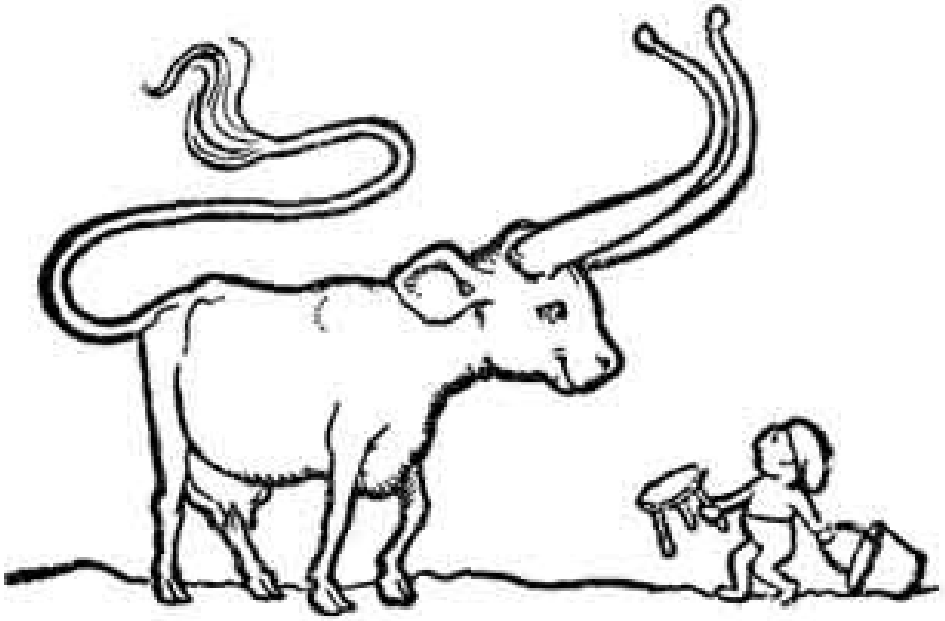


The deal was made in Redmond on a dark and stormy day...

The plan:

- A new specification for SMB/CIFS, as implemented in Windows NT.
  - Windows NT?
  - Uh, yeah.
- Oh! ...and then another doc specifying the changes to SMB/CIFS *since* NT.

Scope



Project Scope

CIFS: A Common Internet File System

- What the heck does the term "CIFS" mean this week?
  - Only the NT LM 0.12 dialect
    - Not DOS or OS/2 LAN Manager
    - Certainly not the Xenix or Core dialects
  - The NT LM 0.12 dialect as of:
    - Windows NT3.51 & NT4 Server
    - Windows NT4 & 98 client

"CIFS" is now a Snapshot in Time

Project Scope

Yet the document has become very, very large.

Project Scope

Definitions (real world):

SMB: Server Message Block
A stateful network file system protocol originally created by IBM in the early 1980s for use with the PC-DOS operating system.

CIFS: Common Internet File System
A name given to the suite of protocols that include SMB and related supporting protocols. This term was introduced in the mid 1990's.

SMB2: Server Message Block v2
A network file system protocol created by Microsoft for Windows Vista. SMB2 is a redesign of SMB, focusing on improved network efficiency and wide-area-network (WAN) performance.

Project Scope

Definitions (legal and regulatory world):

CIFS: The **Server Message Block** file sharing protocol as implemented in Windows NT 3.51, NT 4, and Windows 9x clients.

SMB: The **Server Message Block** file sharing protocol as implemented in Windows starting with Windows 2000, up to and including current versions of Windows.

SMB2: The **Server Message Block** protocol, **v2**, which is a network file system protocol created by Microsoft for Windows Vista (as defined on the previous slide).

Unfortunately, the terminology changes depending upon who you talk to, when you talk with them, the context of the conversation, and what they've been drinking.

In Summary:

[MS-CIFS]:

- Replaces the Leach/Naik Draft and the SNIA CIFS TR as the new baseline SMB/CIFS reference.
- Fills a void in Microsoft's MCPP/WSPP documentation set.
- Provides a sturdy foundation for the other MCPP/WSPP documentation.

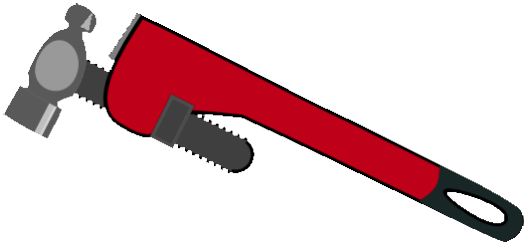
Protocol extensions since NT are in [MS-SMB].

The Docs

SMB/CIFS as documented under MCPP/WSPP

The Docs

MCPP/WSPP docs MUST fit the format of the TEMPLATE.



- Not a developer's dream
  - There are unusual rules,
  - The format is a mix of ISO and IETF Standards styles,
  - It was put together by non-techies.
- We committed ourselves to making the best of it.

(Just as we have all committed to making the best of SMB/CIFS, eh?)

The Docs

There are six key sections. They have official names, but they are basically as follows:

1. The Introduction
2. Messages
3. Crazy Abstract Data Model
4. Useless Captures
5. Security Stuff that should already be covered elsewhere
6. Windows Behavior Notes

The Docs

The Introduction

Some useful stuff here:

- Glossary
- References
- Scope
- Basic Document Overview

You know... Introductory stuff.

The Docs

Messages

Lots of useful stuff here:

- Transport Overview
  - References to Transport docs.
- Defined Constants
  - Error Codes, Command Codes, etc.
- Basic SMB structures
- Per-Command/Subcommand Message Layout
  - Field Definitions

Syntactic details and lots of basic relationships between fields—the stuff that most geeks want.

The Docs

The Crazy Abstract Data Model

Obscure, convoluted, and required.

- Defines State Variables.
- Defines interactions between State Variables and message parameters.
- Defines state machine behavior on both client and server.

We often talk about SMB/CIFS being a “Stateful” protocol. These are the states and transitions.

The Docs

The Crazy Abstract Data Model
(continued)

Obscure, convoluted, and required.

- Defines State Variables: Objects
- Defines methods for operating on those objects.
- References other docs for further processing.

Semantics... Some consider this section to be an Object Oriented protocol model.

The Docs

Useless Captures, and Redundant Security Stuff

Important to the TEMPLATE.

- Developers can grab their own captures.
- Security information should be well described elsewhere.

...but it's not in the way, and may prove useful to someone.

The Docs

Windows Behavior Notes

Very useful for interoperability.

- Provides insight into the Windows client and server implementations of SMB/CIFS.
- Provides Windows compatibility guidance.

This section also allows the document writers to add subtle hints and commentary (within reason).

The Docs

How to read the docs.

For the beginner:

- Start with Implementing CIFS.
- Read the Core Protocol specification.
- Skim the [MS-CIFS] Introduction.
- Read the Messages section (section 2).
- Panic
- Work on one command at a time until it starts making sense. (Then panic again.)

CIFS is not a good place to go without support.

The Docs

How to read the docs.

For the seasoned hand:

- Skim the [MS-CIFS] Introduction.
- Work through section 2, one command at a time.
- Use sections 3 and 6 to help resolve bizarre behavior issues (of which, as we know, there are many).
- Read [MS-SMB] sections 2 & 3.
- Report bugs.

A lot of effort went into these docs.

The Docs

Bad Behavior

The protocol and the implementation are inconsistent. (Surprise!)

- Incomplete command implementations
- Unspecified (and unfinished) commands
- Error code oddities

The docs attempt to clarify what is protocol, and what is behavior.

The Docs

Error Code Anomalies

There is a small but specific set of error codes that are always returned in SMB (Class/Code) format.

- NT Server marks these as 32-bit codes.
- W2K and above override negotiated format and clear the 32-bit code flag.
- In the docs, we provide both code formats.
- The client can interpret the codes using the negotiated format.

CIFS.ORG

The End

Any Questions?