HP's CIFS/9000 And Windows 2000 Interoperability

Version 1.01, June 2001

Eric Roseme
SNSL Advanced Technology Center

E0300

Printed in: U.S.A.

Legal Notices

Hewlett-Packard Company
19420 Homestead Road
Cupertino, California 95014 U.S.A.

Contents

Chapter 1 Introduction

CIFS/9000 is HP's Common Internet File System (SMB) distributed file system that runs on HP-UX 11. CIFS/9000 is HP's strategic HP-UX and Windows interoperability platform, and is an important component of the HP Multi-OS platform proposition.

As with most industry Windows interoperability products, CIFS/9000 is based upon Windows NT4.0 technology. Microsoft Windows is the dominant desktop platform. Updates to new releases are often triggered by new desktop client features. However, since customers cannot update all their systems at once, the new Microsoft releases interoperate with previous platforms (in this case NT4.0). This allows customers to continue to use CIFS/9000 enterprise level UNIX servers for robust and mission-critical file serving while also taking advantage of the new client management and domain administration features available with Windows 2000 clients and servers.

CIFS/9000 Server integrates well with Windows 2000 because of the NT4.0 compatibility design. HP is evaluating and engineering additional Windows 2000 integration features for CIFS/9000. Coinciding with this effort, we can examine how the current NT4.0-based product currently integrates into a Windows 2000 domain, and recommend integration procedures and configurations. The areas that will be covered in this paper are:

- CIFS/9000 Features and Benefits Overview
- Windows 2000 Mixed Domain Mode versus Native Domain Mode
- NTLM Authentication versus Kerberos Authentication
- CIFS/9000 Integration into Active Directory
- Name Address Resolution
- CIFS/9000 Integration with Windows 2000 DFS

Chapter 2 CIFS/9000 Overview

HP's CIFS/9000 Server product is based upon Samba open source. CIFS/9000 Server is only supported on HP-UX 11 and newer releases. CIFS/9000 Server updates follow Samba open source updates as follows:

- March 2000 HP-UX Application Release: Samba 2.0.6
- March 2001 HP-UX Application Release: Samba 2.0.7
- September 2001 HP-UX Application Release: Samba 2.0.9 (planned)

HP includes CIFS/9000 Server as a default Distributed File System product on all HP-UX 11 and later releases. There is no charge for CIFS/9000. On HP-UX 11i and later, CIFS/9000 is included with the base release OS and is instantly ignitable. On earlier HP-UX 11 releases it is available from the Application Release CDs after March 2000, or from www.software.hp.com. Setup and configuration scripts are included with the product, as well as an Installation and Administration manual. A major feature of CIFS/9000 Server is the availability of support options for HP Response Center and HP Worldwide Technology Expert Center support. This feature - as well as HP product enhancements - give the customer exceptional value with CIFS/9000 Server over Samba open source, and competitor's Windows interoperability products.

CIFS/9000 Server runs on HP's enterprise-ready server family, and has the flexibility to run as a connectivity application for Windows clients to a general-purpose server, or with NFS as a dedicated file server platform on a Network Attached Storage single-purpose server. Either way, CIFS/9000 and HP-UX on HP enterprise servers have the following advantages:

- Scaleable RISC Architecture
  - A-Class
  - L-Class
  - N-Class
  - Superdome
  - HP-UX Workstations
- 99.999% Reliability with MC ServiceGuard
- State-of-the-Art Storage Platforms
  - XP48, XP256, XP512
  - VA7100, VA7400
  - FC10, FC60
- HP Server Flexibility, not limited single-purpose
  - General Purpose Server
  - Dedicated NAS File Server
- No added costs on HP-UX 11

CIFS/9000 Server is based upon NT4.0 technology using the Common Internet File System protocol (The SMB specification) that is the standard protocol for Windows operating systems on Windows 95, Windows 98, NT4.0, and Windows 2000. The common deployment architecture for NT4.0 utilizes:

- Master-Resource domain model
- PDCs and BDCs
- explict 1-way or 2-way trusts
- global and local groups
- 4.0 authentication protocol
- 4.0 name resolution

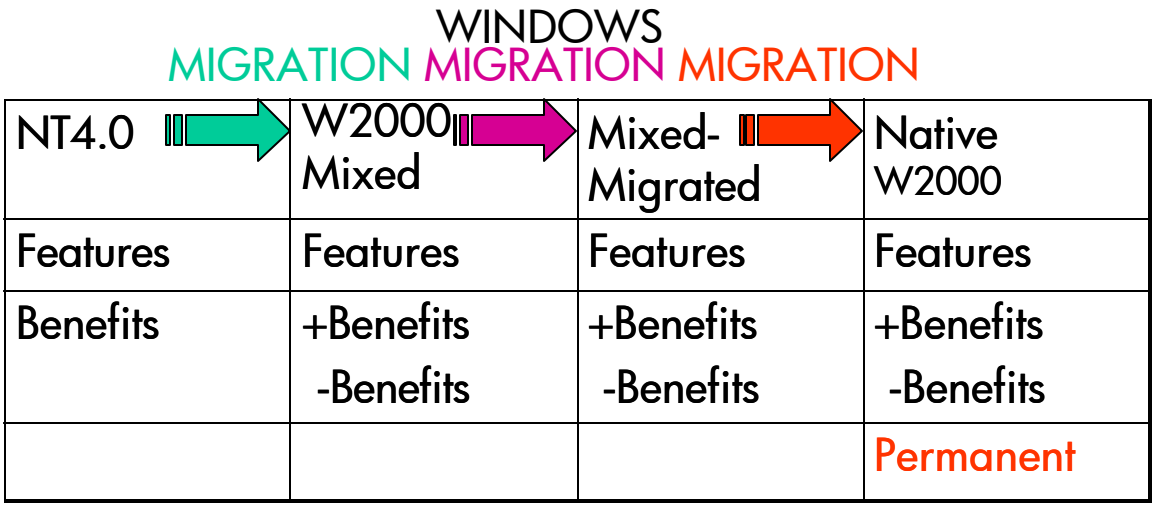
In addition, because CIFS/9000 Server resides on the underlying UNIX operating system, UNIX security policy is enforced using account data that is stored on:

- /etc/passwd
- NIS
- NIS+
- LDAP

2.1 Migration to Windows 2000

Because CIFS/9000 is based upon NT4.0 technology, in order to understand how it interoperates with Windows 2000 we must address NT4.0-to-Windows2000 migration principles. However, Windows 2000 migration is such an enormous task that the topic could absorb this entire paper and more, so migration issues will be limited to those features that directly affect CIFS/9000 server.

As a preview, consider that Windows 2000 Migration has 4 stages:



The starting point is NT4.0, which is assumed to be the existing operating environment in a stable operating capacity. The benefits of this stage are obvious: it is a known state. The rationale for migrating to Windows 2000 is to enhance the operating state with the additional features that Windows 2000 offers.

In Windows 2000 Mixed, the environment has at least the old NT4.0 PDC migrated to, and running as, a Windows 2000 Domain Controller, but with a NT 4.0 SAM account database facsimile to handle interoperability with BDCs and downlevel clients. Benefits for this state include Windows 2000 Pro client features that are available in a Windows 2000 domain, Active Directory and LDAP access to it, Windows 2000 Distributed File System, Kerberos authentication, Dynamic DNS, and many others. Detriments include the complex migration process, expensive re-deployment, extensive planning costs before deployment can begin, and "if it's not broken, don't fix it."

In Windows 2000 Mixed-Migrated, all of the BDCs and downlevel clients have been migrated, so that the domain is "pure Windows 2000." In this state, Native Mode can be enabled, but there are benefits to remaining in this state. All of the BDCs and downlevel clients have been migrated to Windows 2000, so WINS and NetBIOS can be disabled. Those are the major new benefits. At this state, the flexibility to re-deploy BDCs and/or downlevel

clients remains. This flexibility must be offset against the added benefits of enabling Native Mode.

In Native Mode, a one-way transition is executed. Once the Native Mode switch has been enabled, there is no returning to Mixed Mode. It is a permanent, one-way change. The benefits are: the addition of Domain Local groups, Universal Groups, and group nesting. An additional feature gained is the ability to utilize SIDHistory, and the associated migration tools ADMT and ClonePrinciple. The detriments are the permanent status, and the resulting lack of flexibility.

Chapter 3 W2000 Domain Mode: Mixed vs Native

The initial foray into Windows 2000 is dominated by the decision: Mixed Mode or Native Mode? Before addressing this question, it is important to understand:

- Domain design implications
- What the Mixed-vs-Native installation process is
- How the overall feature set of Windows 2000 is affected
- The PDC Emulator function
- **What affect the domain mode has upon CIFS/9000 member servers**

3.1 Domain Design

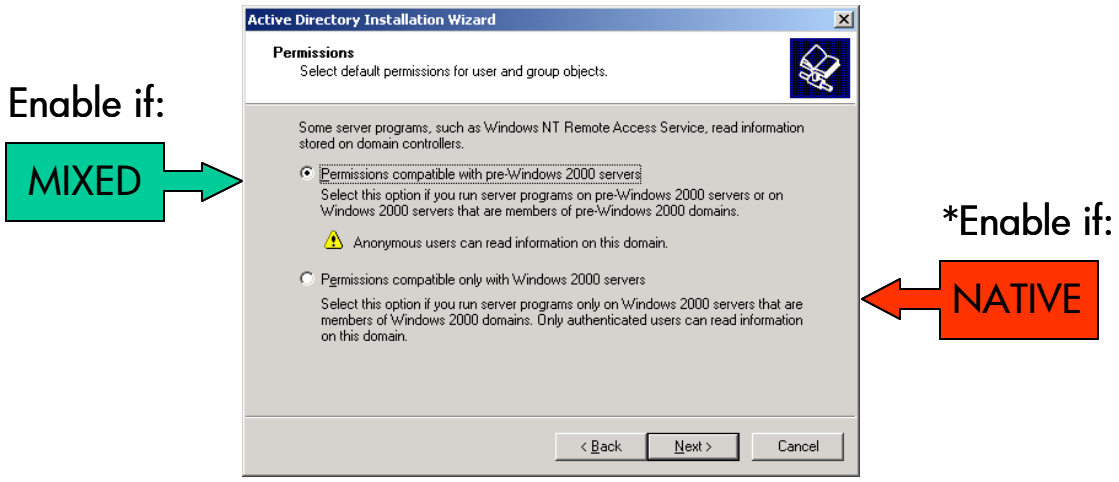
Designing the Windows 2000 domain is clearly the single most important task of implementing Windows 2000. Since the Advanced Directory schema can only be extended further once it is created (as opposed to having modification control), it needs to be done correctly the first time. The first decision is whether to start the domain in Native Mode, or in Mixed Mode (and migrate to Native later). This task starts with the installation of the root domain controller in the Windows 2000 domain:

- Configure a new root Domain Controller as Native Mode
- Configure a new root Domain Controller as Mixed Mode
  - Migrate to Native later
- Migrate an existing NT4.0 PDC to a Domain Controller in Mixed Mode
  - Migrate to Native later

The Windows 2000 domain design topic is too vast for this paper, but it is important to note the requirement as a prerequisite for implementation.

3.2 Installation Process

A Windows 2000 root domain controller cannot be installed in Native Mode. There is a dialog box in the installation process that implies Native Mode configuration, but actually only manipulates group permissions, and has no effect upon the domain mode:



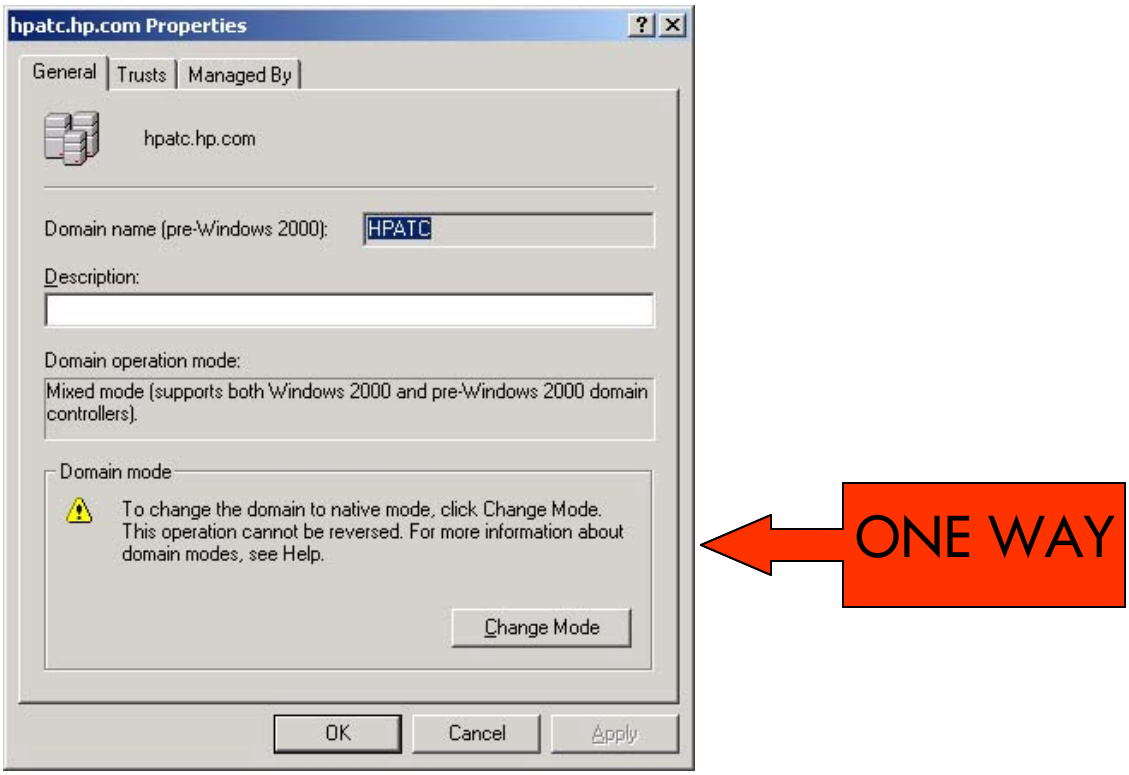
What this screen actually does to allow the built-in group Everyone to be nested under the built-in group "Pre-Windows 2000 Compatible Access Group." This nesting is configured when choosing the option labeled "Permissions compatible with pre-Windows 2000 servers." Nesting the Everyone group allows anonymous connections to domain resources. NT4.0 clients use anonymous (null) connections, and thus would encounter compatibility issues if they were rejected because of inadequate permissions. This is not very clear from the screen description and from its placement in the installation sequence.

Considering the effects of the configuration options, the second choice would likely only be selected if the domain is intended to be deployed in Native Mode. See the following Microsoft Q articles for details about the effects:

- Q257988
- Q257942
- Q254311

If a CIFS/9000 server is deployed in a native mode domain, the "Permissions compatible with pre-Windows servers" option must be selected. The Q-articles describe how to enable or disable this attribute manually (the configuration screen is only accessible during installation).

The Windows 2000 Domain Controller will be installed in Mixed Mode by default. To enable Native mode, go to the following screen in the "Active Directory Domains and Trusts" administrative tool:



Choosing Native Mode is a one-way operation – there is no going back to Mixed Mode without a reinstall of Windows 2000 Advanced Server or restoring a back-up. This operation is instantaneous on a small test domain, but some Microsoft documents indicate that for larger domains the process can be quite lengthy, and replication of the Active Directory changes to all DCs in the domain can delay completion even longer.

An interesting item that is referenced in a Microsoft Technet document indicates that a root domain can be Mixed Mode, and a sub domain within the forest can be Native Mode. Rudimentary testing shows this to be accurate.

3.3 Domain Mode Effect Upon Feature Set

The one-way nature of Native Mode configuration requires a clear understanding of the advantages and disadvantages of Native Mode and Mixed Mode. The following table illustrates the major differences:

FEATURE	MIXED	NATIVE
Support NT4.0 BDC	Yes	No
Support Member Server (CIFS/9000!)	Yes	Yes
Global and Local Groups	Yes	Yes
Domain Local, Universal Groups; Group Nesting	No	Yes
NTLM Authentication	Yes	Yes
Kerberos Authentication	Yes*	Yes*
UPN Logon Name	No	Yes*
Dial-In Options (Q193897)	No	Yes
Intellimirror	Yes*	Yes*
Clients: W95, W98, NT4.0, W2000	Yes	Yes
SIDHistory	No	Yes

*Windows 2000 Pro only

Of course, there are even more Windows 2000 features. This paper discusses BDC support, member server support, NTLM, and Kerberos as major topics. See Appendix A for UPN details.

3.3.1 Groups

Global and local groups are an integral component of NT4.0, and provide key functionality for the Master-Resource domain mode that is most common. Windows 2000 adds Domain Local groups, Universal groups, and Group Nesting.

- Domain Local Groups: Contain members from anywhere in the Windows 2000 forest, trusted Windows 2000 forests, trusted NT4.0 domains, and grant permissions to any resource in the local domain (NT4.0 local groups grant permissions only on the computer where they exist)
- Universal Groups: Contain members from anywhere in the Windows 2000 forest or trusted forests, and can be granted permissions in any domain in the forest, or trusted forests (NT4.0 global groups contain members from the local domain only)
- Group Nesting:
    - Universal Groups can contain other Universal Groups and Global Groups from any domain
    - Global Groups can contain other Global Groups from the same domain
    - Domain Local Groups can contain Universal Groups, Global Groups from any domain, Domain Local Groups from the local domain

Native Mode also allows group conversions from one group type to another:

- Between Security and Distribution Groups
- Between Universal Groups and Global Groups
- Between Universal Groups and Domain Local Groups

3.3.2 Dial-In Options

Some Dial-In options are only available in Native Mode (see Q193897):

- Control access through remote access policy
- Verifier caller ID
- Assign a static IP address
- Apply static routes
- Static routes

3.3.3 Intellimirror

IntelliMirror is an expanded and renamed feature set based upon Roaming Profiles. IntelliMirror provides the primary benefits related to custom, mobile profiles:

- User Data Management – users have access to their data regardless of the hardware that they logged onto
- Software Installation and Maintenance – users have "just in time" application installations regardless of the hardware that they are logged onto
- User Settings Management – user's desktops are available regardless of the hardware that they are logged onto

These features are available in Mixed or Native Mode, but the user must be on a Windows 2000 Pro client.

3.3.4 SIDHistory

SIDHistory is a very important migration concept that is interdependent with several domain migration and restructuring tools: ADMT, ClonePrincipal, NetDom, and MoveTree. SIDHistory is only available in Native Mode. This presents a paradox, because Mixed Mode is a state intended to ease migration from NT4.0, and SIDHistory is a Native-Mode-Only tool that is almost a necessity for migrating a file server environment from NT4.0 to Windows 2000.

SIDHistory addresses the issue of incongruous user accounts and access control entries (ACEs) on access control lists (ACLs). When users are migrated from an NT4.0 domain to a Windows 2000 domain, the Security Identifiers (SIDs) associated with their individual user or groups changes. However, resources throughout the migrated domain likely retain the ACEs with the NT4.0 SIDs of the old NT4.0 user. SIDHistory and the associated toolset provide a mechanism for resolving this inequity.

However, the actual SIDHistory attribute that enables the functionality is located on the Native Mode user access token only. There is no SIDHistory access token in Mixed Mode. If domain migration is a key component of Windows 2000 implementation strategy, then

SIDHistory and the accompanying tools are important elements that must be fully understood. Microsoft has provided many documents explaining SIDHistory in detail.

If a new Windows 2000 domain is being designed, then SIDHistory's Native Mode dependancy is not so important. Also, SIDHistory emphasis is directly related to usage of ACLs on domain resources. If ACLs are not used, or if most resource ACLs are POSIX (like with CIFS/9000 – see the topic in the "Active Directory" module), then SIDHistory will likely not be an issue.

3.4 PDC Emulator

Windows 2000 Advanced Directory domains include the designation of a PDC Emulator, or FSMO PDC Emulator (Flexible Single Operation Master). The PDCE is usually resident on the forest root domain controller in both Mixed Mode and Native Mode domains, but includes NT4.0 functionality when the domain is in Mixed Mode.

A Native Mode PDCE provides the following services:

- Password changes replicated to preferentially: Any password change at a DC in the domain will be replicated to the PDCE first.
- Bad password logon attempts routed here: A bad password at logon could be the result of a password change from some other DC in the domain. Since the PDCE gets all password changes preferentially, any bad password at logon gets routed here to ensure that the password was not changed , but did not have time to be replicated throughout the domain.
- Account Lockouts: All domain account lockouts are processed here.
- Group Policy Objects: The PDCE holds the domain Group Policy Objects

A Mixed Mode PDCE provides all of the Native Mode PDCE services, plus the following:

- Holds the write copy of the SAM database: The SAM database is the NT4.0 account facsimile that provides NT4.0 compatibility in Mixed Mode.
- Distributes SAM database to BDCs in the domain.
- Acts as the domain Master Browser to update browse lists throughout the domain (NetBIOS Suffix <0x1B>).

Because a member server does not hold a copy of the ADS or SAM database, a member server is not affected by the services that the FSMO PDC Emulator provides. CIFS/9000 Server assumes a member server role in a Windows domain.

3.5 Windows 2000 Domain Mode: CIFS/9000 Interoperability

The decision to implement Windows 2000 in Mixed Mode or Native Mode has important functionality ramifications throughout the domain. However, the CIFS/9000 server can operate in either mode fairly transparently because:

- CIFS/9000 Server is a Member server
- CIFS/9000 Server has no SAM database
- CIFS/9000 Server processes no Windows user/group updates
- CIFS/9000 Server passes through all authentication requests
- CIFS/9000 Server is not affected by the group functionality that is added with Native Mode
- CIFS/9000 Server is administered by SWAT (Samba Web Administration Tool), and is not affected by Windows 2000 administration policies

For CIFS/9000 Server interoperability in the Windows 2000 domain, the following functionality must be enabled when in Native Mode:

- NetBIOS (see the Name Resolution module)
- NLTM (see the Authentication module)
- WINS (see the Name Resolution module)
- Permissions compatible with pre-Windows 2000 servers

It is essential that the effect of Mixed Mode versus Native Mode is fully understood upon all domain resources before designing the domain infrastructure.

Chapter 4 Authentication: Kerberos and NTLM

Authentication technology is a key feature of Windows 2000. The adoption of Kerberos as the default Windows authentication protocol is a primary differentiator from NT4.0 and a compelling motivation to upgrade. The NT4.0 authentication protocol is NTLM, and it is important to understand the benefits that Kerberos provides over NTLM so that the migration implications are fully understood. CIFS/9000 authentication is based upon NTLM at this time, so a clear understanding of how NTLM integrates into a Windows 2000 Mixed or Native Mode domain is critical for assessing potential installations.

4.1 CIFS/9000 Server and NTLM

CIFS/9000 Server is based upon Samba, and Samba has 4 basic authentication (or "security") modes:

- Share
- User
- Server
- Domain

Since integration with Windows 2000 is predicated upon domain security, domain is the only Samba security mode that will be considered here.

The CIFS/9000 server uses pass-through domain authentication for users. When a user maps a share (\\CIFS9000servername\sharename), the CIFS/9000 server must look for an authentication entity within the domain, because the CIFS/9000 server does not carry an authenticating database (either the NT4.0 SAM or Windows 2000 ADS). In domain mode, the server will search for a domain controller to pass-through the authentication request in order to validate that the client user is legitimate. The authenticating protocol that the CIFS/9000 server uses is NTLM v1. The server will negotiate the protocol with the client that is mapping the share, then negotiate again with the domain controller that it will pass the authentication request to. This behavior will be displayed in a subsequent diagram.

4.1.1 NTLM Details

At the time NTLM Challenge-Response authentication protocol was introduced for NT4.0, it was considered state-of-the-art. NTLM v1 provided:

- Improved security over LAN Manager
  - 14 Character Passwords (note that if the passwords do not actually contain the additional characters that 14-char allows, then there is no security gained)
- Encryption across the wire
- Passwords fragmented across the wire (harder to decrypt)

Like most technology, what was state-of-the-art then is now obsolete. The current status of NTLM:

- Proprietary protocol
- Performance bottleneck
- One-way authentication only (client user is validated)
- No authentication delegation (no service proxy)

- Requires complex manual trust management for multi-domains like master-resource

NTLM has a version 2 that includes a better encryption mechanism. NTLM v2 was delivered for NT4.0 in Service Pack 4. However, NTLM v2 requires editing of the client registry to enable, and it has not been widely adopted.

4.2 Windows 2000 and Kerberos

The Windows 2000 default authentication protocol (from Windows 2000 Pro clients only) is Kerberos. Microsoft clearly promotes Kerberos as a significant advantage of Windows 2000, and a primary motivation to migrate from earlier Windows platforms. Advantages of Kerberos authentication are:

- "Industry Standard": Kerberos is not a new protocol. It originated at MIT in the late 1980s, and is regulated by the IETF RFC 1510. Microsoft adopted Kerberos and modified it to fit into the Windows 2000 ADS and domain structure. Consequently, it is now "Based upon an Industry Standard", with a proprietary data structure that affects interoperability with other vendors (to be examined in more detail later).
- Re-Use Credentials: NTLM requires that a server authenticate a user upon connection and issue a set of credentials. When the user disconnects, so do the credentials. With Kerberos, a user is issued a set of credentials with an expiration interval. If the client reconnects before the expiration, then the original credentials are still valid and the server does not have to authenticate the client again. This can speed the connection process when accessing varied resources in a domain.
- Client AND Server are Authenticated: With NTLM the client is requesting domain authentication, and the server must validate that the client is a legitimate member of the domain. With Kerberos, the same process occurs, except that the Kerberos key mechanism also provides the client with validation that the server is a legitimate member of the domain. This holds true for any 2 entities in the domain.
- Authentication Proxy: Windows applications often impersonate clients when accessing resources within a domain. NTLM does not provide an authentication mechanism for impersonating a client. Kerberos has an authentication proxy that allows an application (or "service") to impersonate a client for authentication.
- Transitive Trusts: Although Transitive Trusts sound like an ADS feature, they exist as a result of the Kerberos dual authentication ability. Since separate entities within the Windows 2000 domain (or forest) are validated by the dual authentication mechanism in Kerberos, there is no need to explicitly configure one-way or two-way trusts.
- Encryption: The Kerberos encryption method is much more secure than NTLM encryption.

4.3 CIFS/9000 Server and Windows 2000 Kerberos

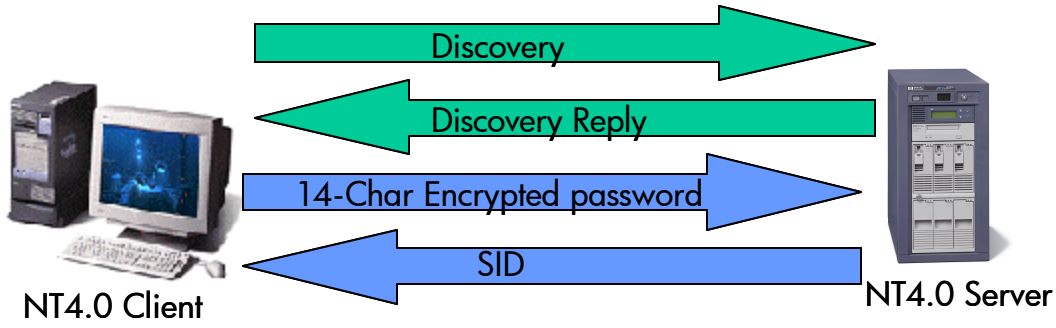
The CIFS/9000 Server can co-exist in a Windows 2000 domain (Native or Mixed) where Windows 2000 Pro clients are authenticating into the domain using Kerberos. Even when the client is authenticated with Kerberos, the CIFS/9000 Server will negotiate the NTLM v1 protocol with the client that is mapping a share, and then pass-through the authentication request to the Windows 2000 domain controller, also negotiating NTLM v1 to the DC.

The following diagrams and traces illustrate the authentication protocol used by the CIFS/9000 server in the following domain structures:

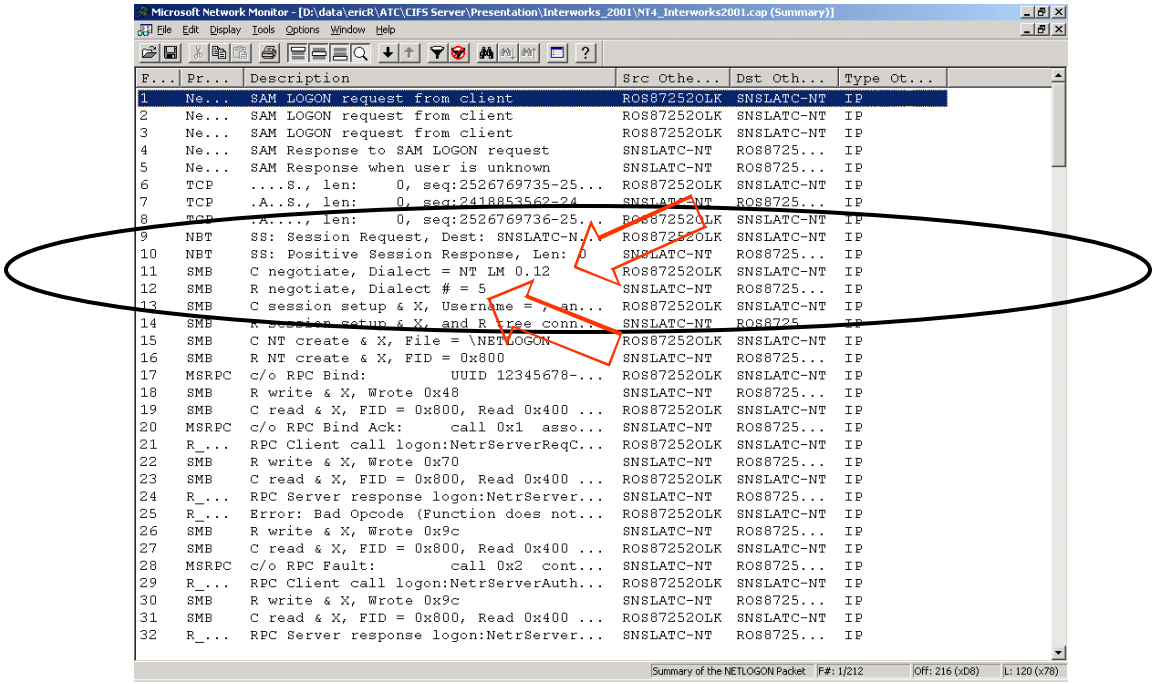
- NT4.0 client in an NT4.0 domain
- Windows 2000 client in a Mixed Mode Windows 2000 domain

- Windows 2000 client in a Native Mode Windows 2000 domain

4.3.1 NT4.0 Client in an NT4.0 Domain



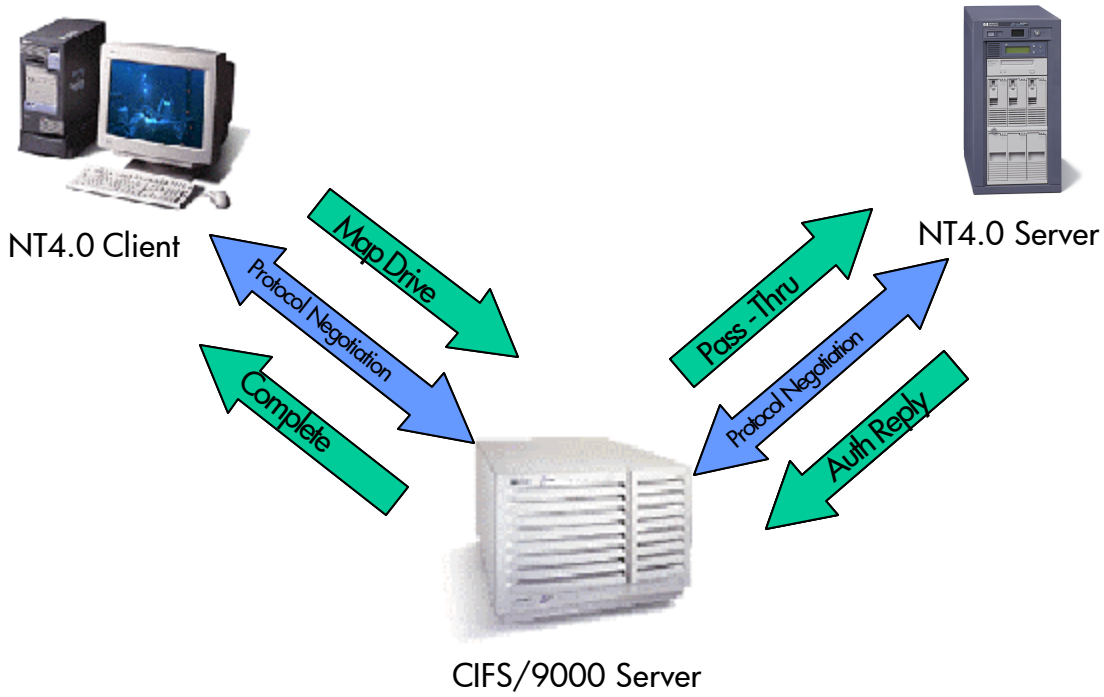
This is the standard NT4.0 client authentication procedure.



The Network Monitor trace shows that the ROS87252OLK NT4.0 client negotiates the authentication protocol with the NT4.0 server by presenting the NTLM 0.12 (NTLM v1)

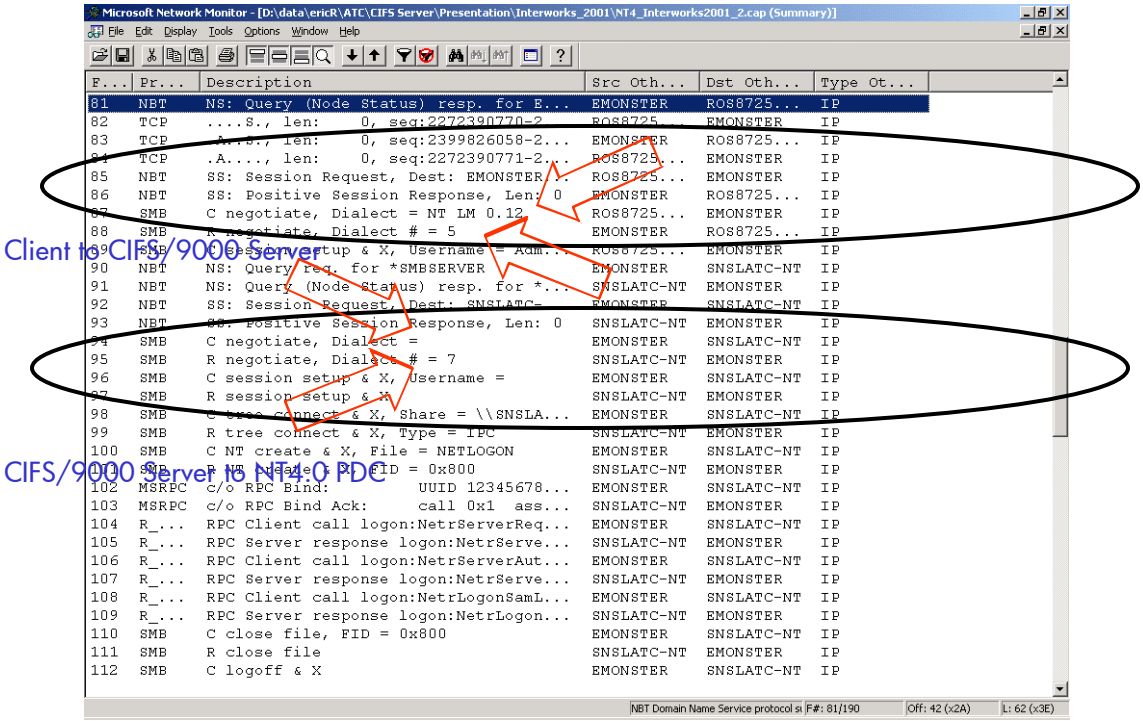
protocol to the server in packet number 11. The SNSLATC-NT NT4.0 server replies in packet number 12 that Dialect #5 (the expanded SMB shows dialect #5 to be NTLM 0.12) is accepted as the protocol.

After the client is authenticated, it maps a network drive on the CIFS/9000 Server that is a member of the NT4.0 domain:



1. The client maps a drive: \\CIFS9000Severname\Sharename.
2. The CIFS/9000 server negotiates the authentication protocol with the client.
3. The CIFS/9000 server passes through the authentication request to the domain PDC or BDCs, because it does not carry a SAM database to perform the authentication locally.
4. The CIFS/9000 server negotiates the authentication protocol with the NT4.0 PDC or BDC.
5. The NT4.0 PDC or BDC validates the client and replies to the CIFS/9000 Server.
6. The CIFS/9000 Server completes the mapping process and replies to the NT4.0 client with a successful mount.

The following Network Monitor trace shows that the CIFS/9000 Server first negotiated the NTLM v1 protocol with the client, then again with the NT4.0 PDC or BDC at the pass-through authentication request:



Microsoft Network Monitor - [D:\data\ericR\ATC\CIFS Server\Presentation\Interworks_2001\NT4_Interworks2001_2.cap (Summary)]

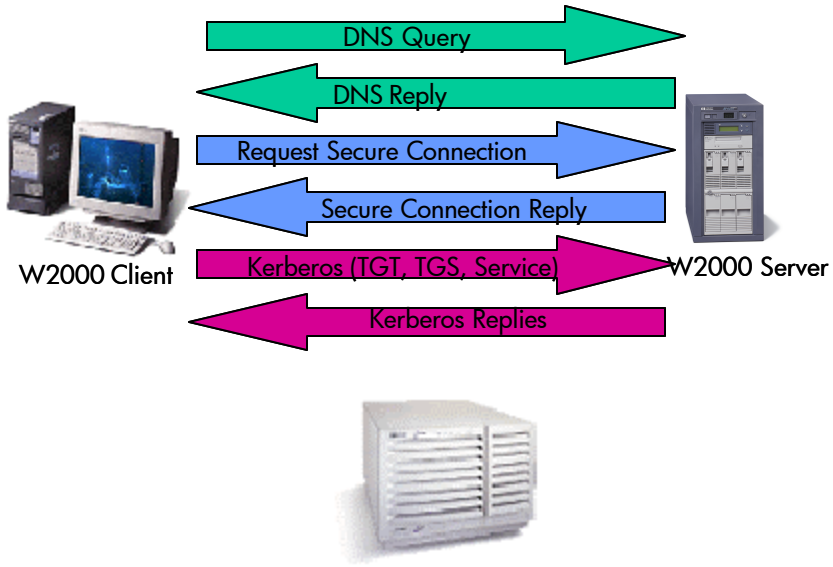
File Edit Display Tools Options Window Help

F...	Pr...	Description	Src Oth...	Dst Oth...	Type Ot...
81	NBT	NS: Query (Node Status) resp. for E...	EMONSTER	ROS8725...	IP
82	TCP	....S., len: 0, seq:2272390770-2	ROS8725...	EMONSTER	IP
83	TCP	.A..S., len: 0, seq:2399826058-2...	EMONSTER	ROS8725...	IP
84	TCP	.A...., len: 0, seq:2272390771-2...	ROS8725...	EMONSTER	IP
85	NBT	SS: Session Request, Dest: EMONSTER ...	ROS8725...	EMONSTER	IP
86	NBT	SS: Positive Session Response, Len: 0	EMONSTER	ROS8725...	IP
87	SMB	C negotiate, Dialect = NT LM 0.12	ROS8725...	EMONSTER	IP
88	SMB	R negotiate, Dialect # = 5	EMONSTER	ROS8725...	IP
89	SMB	C session setup & X, Username = Adm...	ROS8725...	EMONSTER	IP
90	NBT	NS: Query req. for *SMBSERVER	EMONSTER	SNSLATC-NT	IP
91	NBT	NS: Query (Node Status) resp. for *...	SNSLATC-NT	EMONSTER	IP
92	NBT	SS: Session Request, Dest: SNSLATC-	EMONSTER	SNSLATC-NT	IP
93	NBT	SS: Positive Session Response, Len: 0	SNSLATC-NT	EMONSTER	IP
94	SMB	C negotiate, Dialect =	EMONSTER	SNSLATC-NT	IP
95	SMB	R negotiate, Dialect # = 7	SNSLATC-NT	EMONSTER	IP
96	SMB	C session setup & X, Username =	EMONSTER	SNSLATC-NT	IP
97	SMB	R session setup & X	SNSLATC-NT	EMONSTER	IP
98	SMB	C tree connect & X, Share = \\SNSLA...	EMONSTER	SNSLATC-NT	IP
99	SMB	R tree connect & X, Type = IPC	SNSLATC-NT	EMONSTER	IP
100	SMB	C NT create & X, File = NETLOGON	EMONSTER	SNSLATC-NT	IP
101	SMB	R NT create & X, FID = 0x800	SNSLATC-NT	EMONSTER	IP
102	MSRPC	c/o RPC Bind: UUID 12345678...	EMONSTER	SNSLATC-NT	IP
103	MSRPC	c/o RPC Bind Ack: call 0x1 ass...	SNSLATC-NT	EMONSTER	IP
104	R_...	RPC Client call logon:NetrServerReq...	EMONSTER	SNSLATC-NT	IP
105	R_...	RPC Server response logon:NetrServe...	SNSLATC-NT	EMONSTER	IP
106	R_...	RPC Client call logon:NetrServerAut...	EMONSTER	SNSLATC-NT	IP
107	R_...	RPC Server response logon:NetrServe...	SNSLATC-NT	EMONSTER	IP
108	R_...	RPC Client call logon:NetrLogonSamL...	EMONSTER	SNSLATC-NT	IP
109	R_...	RPC Server response logon:NetrLogon...	SNSLATC-NT	EMONSTER	IP
110	SMB	C close file, FID = 0x800	EMONSTER	SNSLATC-NT	IP
111	SMB	R close file	SNSLATC-NT	EMONSTER	IP
112	SMB	C logoff & X	EMONSTER	SNSLATC-NT	IP

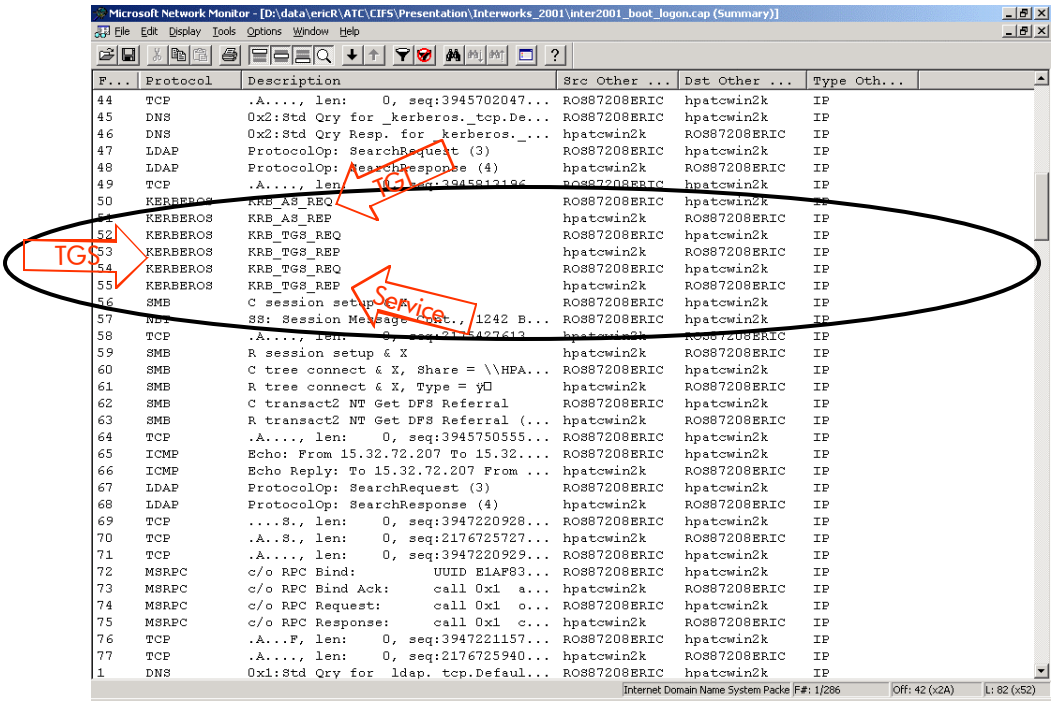
NBT Domain Name Service protocol si | F#: 81/190 | Off: 42 (x2A) | L: 62 (x3E)

The Nt4.0 client ROS87252OLK begins the protocol negotiation with the CIFS/9000 Server in packet 87. The CIFS/9000 Server confirms the NTLM v1 authentication protocol in packet 88. The CIFS/9000 Server then begins the pass-through authentication request to the NT4.0 PDC or BDC by negotiating the protocol with the NT4.0 server in packet 94. The NT4.0 server confirms the NTLM v1 protocol in packet 95.

4.3.2 Windows 2000 Client Logon with Kerberos: Mixed or Native



This is the Windows 2000 Pro client logon procedure. After finding the domain controller by DNS lookup and establishing a secure connection with MSRPCs (Microsoft Remote Procedure Calls), the client will request domain authentication. The first Kerberos exchange provides the client with a ticket from the KDC. Next, the client requests a ticket for the Domain Controller (DC$), and finally for the Kerberos service that is running on the KDC (krbtgt).



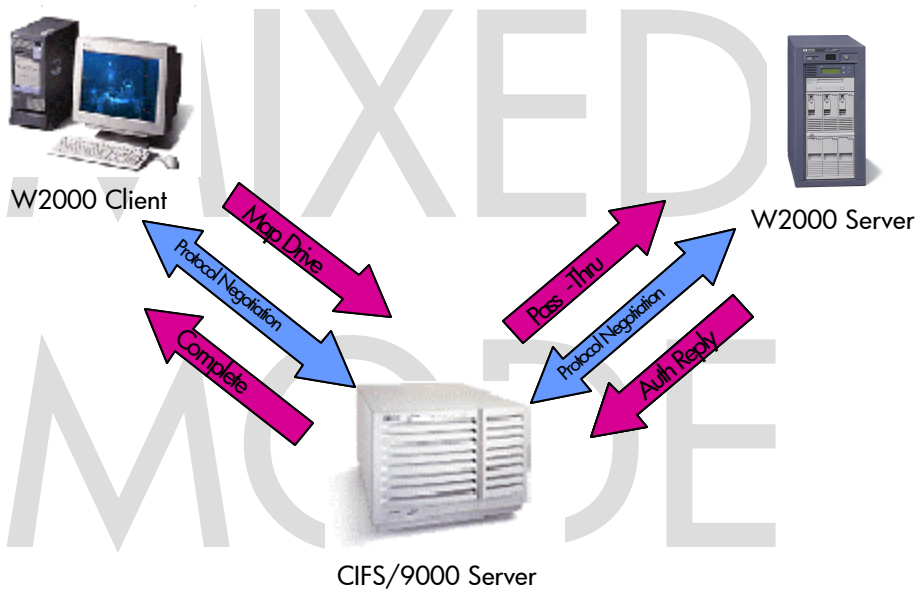
F...	Protocol	Description	Src Other ...	Dst Other ...	Type Oth...
44	TCP	.A...., len: 0, seq:3945702047...	ROS87208ERIC	hpatcwin2k	IP
45	DNS	0x2:Std Qry for _kerberos._tcp.De...	ROS87208ERIC	hpatcwin2k	IP
46	DNS	0x2:Std Qry Resp. for _kerberos._...	hpatcwin2k	ROS87208ERIC	IP
47	LDAP	ProtocolOp: SearchRequest (3)	ROS87208ERIC	hpatcwin2k	IP
48	LDAP	ProtocolOp: SearchResponse (4)	hpatcwin2k	ROS87208ERIC	IP
49	TCP	.A...., len: [illegible]	ROS87208ERIC	hpatcwin2k	IP
50	KERBEROS	KRB_AS_REQ	ROS87208ERIC	hpatcwin2k	IP
51	KERBEROS	KRB_AS_REP	hpatcwin2k	ROS87208ERIC	IP
52	KERBEROS	KRB_TGS_REQ	ROS87208ERIC	hpatcwin2k	IP
53	KERBEROS	KRB_TGS_REP	hpatcwin2k	ROS87208ERIC	IP
54	KERBEROS	KRB_TGS_REQ	ROS87208ERIC	hpatcwin2k	IP
55	KERBEROS	KRB_TGS_REP	hpatcwin2k	ROS87208ERIC	IP
56	SMB	C session setup & X	ROS87208ERIC	hpatcwin2k	IP
57	NBT	SS: Session Message [illegible], 1242 B...	ROS87208ERIC	hpatcwin2k	IP
58	TCP	.A...., len: [illegible]	[illegible]	[illegible]	IP
59	SMB	R session setup & X	hpatcwin2k	ROS87208ERIC	IP
60	SMB	C tree connect & X, Share = \\HPA...	ROS87208ERIC	hpatcwin2k	IP
61	SMB	R tree connect & X, Type = ÿ□	hpatcwin2k	ROS87208ERIC	IP
62	SMB	C transact2 NT Get DFS Referral	ROS87208ERIC	hpatcwin2k	IP
63	SMB	R transact2 NT Get DFS Referral (...	hpatcwin2k	ROS87208ERIC	IP
64	TCP	.A...., len: 0, seq:3945750555...	ROS87208ERIC	hpatcwin2k	IP
65	ICMP	Echo: From 15.32.72.207 To 15.32....	ROS87208ERIC	hpatcwin2k	IP
66	ICMP	Echo Reply: To 15.32.72.207 From ...	hpatcwin2k	ROS87208ERIC	IP
67	LDAP	ProtocolOp: SearchRequest (3)	ROS87208ERIC	hpatcwin2k	IP
68	LDAP	ProtocolOp: SearchResponse (4)	hpatcwin2k	ROS87208ERIC	IP
69	TCP	....S., len: 0, seq:3947220928...	ROS87208ERIC	hpatcwin2k	IP
70	TCP	.A..S., len: 0, seq:2176725727...	hpatcwin2k	ROS87208ERIC	IP
71	TCP	.A...., len: 0, seq:3947220929...	ROS87208ERIC	hpatcwin2k	IP
72	MSRPC	c/o RPC Bind: UUID E1AF83...	ROS87208ERIC	hpatcwin2k	IP
73	MSRPC	c/o RPC Bind Ack: call 0x1 a...	hpatcwin2k	ROS87208ERIC	IP
74	MSRPC	c/o RPC Request: call 0x1 o...	ROS87208ERIC	hpatcwin2k	IP
75	MSRPC	c/o RPC Response: call 0x1 c...	hpatcwin2k	ROS87208ERIC	IP
76	TCP	.A...F, len: 0, seq:3947221157...	ROS87208ERIC	hpatcwin2k	IP
77	TCP	.A...., len: 0, seq:2176725940...	hpatcwin2k	ROS87208ERIC	IP
1	DNS	0x1:Std Qry for _ldap._tcp.Defaul...	ROS87208ERIC	hpatcwin2k	IP

Internet Domain Name System Packe | F#: 1/286 | Off: 42 (x2A) | L: 82 (x52)

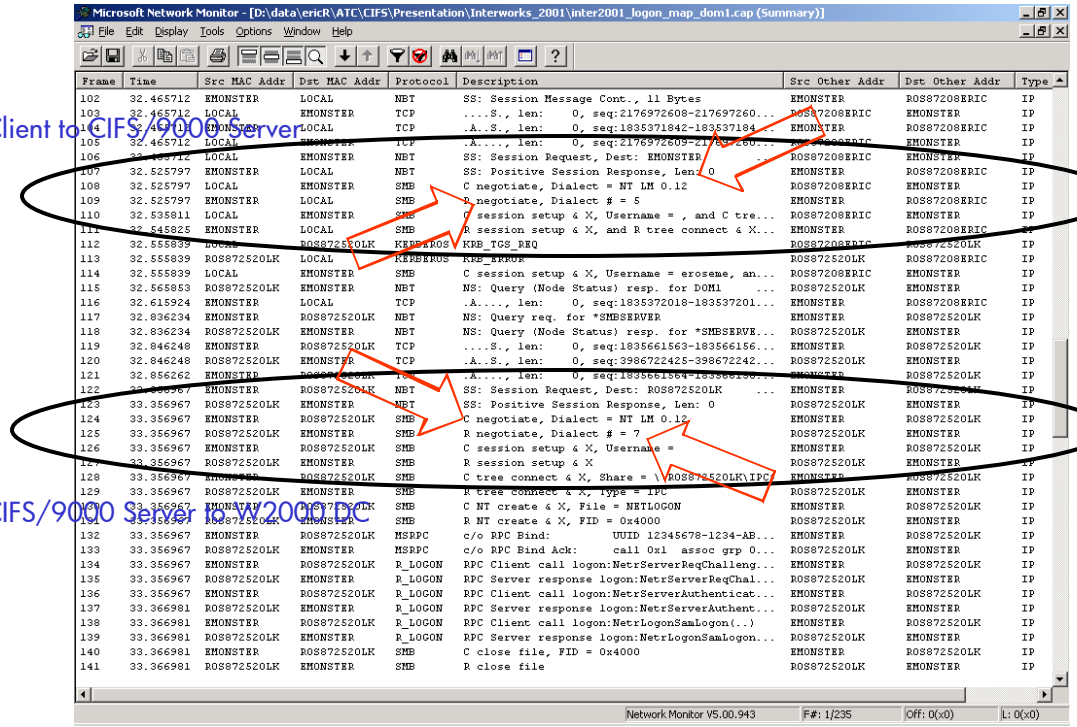
- Packets 50 and 51 show the Kerberos ticket exchange
- Packets 52 and 53 show the DC$ domain controller service exchange
- Packets 54 and 55 show the krbtgt service exchange

4.3.3 Windows 2000 Client Mapping CIFS/9000 Server: Mixed Mode

After the client is authenticated into the Windows 2000 Mixed Mode domain with Kerberos, it maps a network drive on the CIFS/9000 server that is a member of the domain:



The mapping procedure between the Windows 2000 client, the CIFS/9000 Server, and the Windows 2000 Domain Controller is functionally the same as it is in an NT4.0 domain. The following Network Monitor trace shows that the CIFS/9000 Server negotiates the NTLM protocol with the DC in Mixed Mode. Notice that the name resolution protocol is NBT, or NetBIOS. Authentication protocol dependencies are addressed in later module.

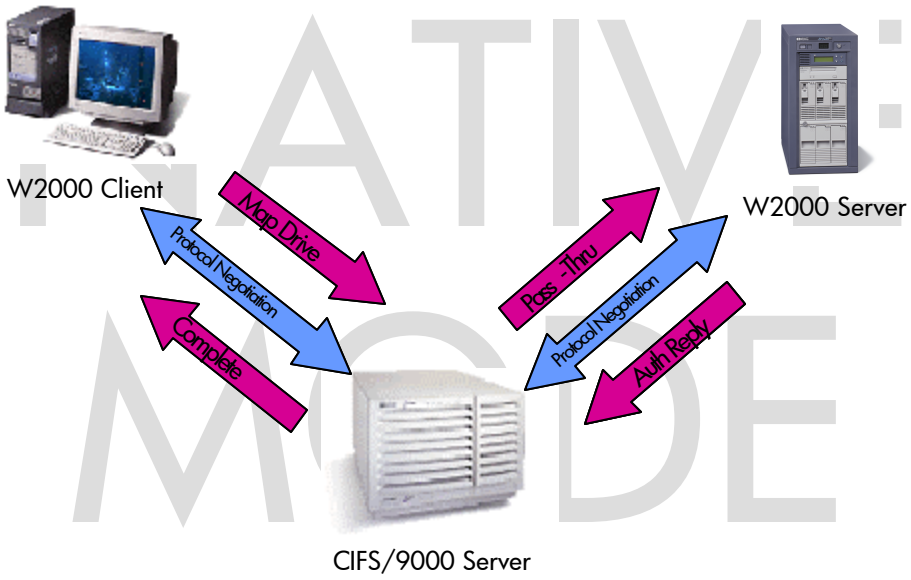


1. Packet 108: The Windows 2000 Pro client ROS87208ERIC proposes NTLM v1 to the CIFS/9000 member server EMONSTER
2. Packet 109: The CIFS/9000 Server EMONSTER confirms NTLM v1
3. Packet 124: The CIFS/9000 member server EMONSTER proposes NTLM v1 to the Windows 2000 domain controller ROS87252OLK
4. Packet 125: The Windows 2000 domain controller ROS87252OLK confirms NTLM v1.

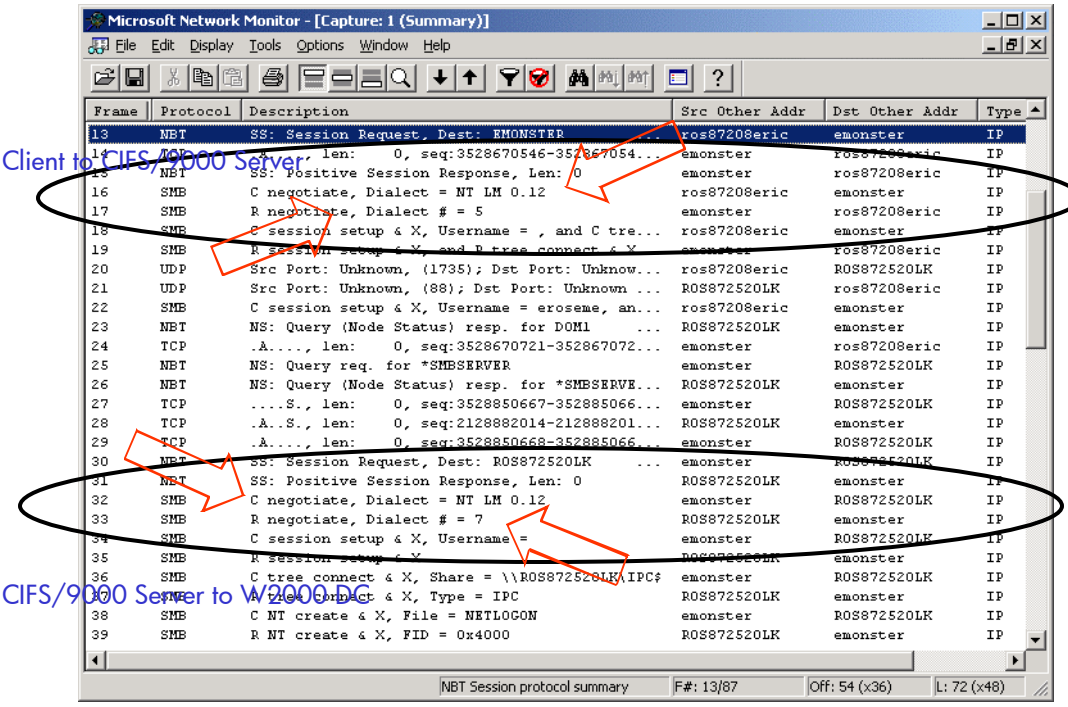
In Mixed Mode, the CIFS/9000 member server authenticates users with the same protocol exchange as in an NT4.0 domain.

4.3.4 Windows 2000 Client Mapping CIFS/9000 Server: Native Mode

The user logon authentication protocol exchange is the same for Mixed or Native modes. Here is an example of the CIFS/9000 Server protocol exchange in a Native Mode domain to compare with the Mixed Mode:



The mapping procedure between the Windows 2000 client, the CIFS/9000 Server, and the Windows 2000 Domain Controller is functionally the same in a Native Mode domain as it is in a Mixed Mode domain or an NT4.0 domain. The following Network Monitor trace shows that the CIFS/9000 Server negotiates the NTLM protocol with the DC in Native Mode.



The Network Monitor trace shows that the Native Mode protocol authentication exchange is the same as Mixed Mode:

1. Packet 16: The Windows 2000 Pro client ROS87208ERIC proposes NTLM v1 to the CIFS/9000 member server EMONSTER
2. Packet 17: The CIFS/9000 Server EMONSTER confirms NTLM v1
3. Packet 32: The CIFS/9000 member server EMONSTER proposes NTLM v1 to the Windows 2000 domain controller ROS87252OLK
4. Packet 33: The Windows 2000 domain controller ROS87252OLK confirms NTLM v1.

The diagrams and traces for client logons and CIFS/9000 Server share mappings show that the CIFS/9000 Server can integrate into the Windows 2000 domain in either Mixed Mode or Native Mode and use the same authentication protocol that is standard in NT4.0. Windows 2000 Pro clients in the domain can log in to the Windows 2000 domain using Kerberos authentication, and map shares to CIFS/9000 using NTLM.

4.4 Why Does CIFS/9000 Use NTLM?

HP offers HP-UX integration with the Windows 2000 Advanced Directory, and provides services to integrate HP-UX account data and route authentication requests to the ADS. However, CIFS/9000 – which exists on HP-UX – does not provide pass-through authentication to the ADS using Kerberos. This is due to the way that Windows 2000 implements the Kerberos ticket layout to add a proprietary structure to the ticket, and therefore bypass the open systems industry standard aspect of the protocol.

Microsoft extends the Kerberos V5 specification by adding a "Privilege Access Certificate" (PAC) to an undefined field in the ticket specification. The PAC contains security identifiers (SIDs) in the actual ticket that allow the client's resource permissions to be readily available when requesting domain resources. The PAC structure is licensed, and although the specification is published, the license specifically prohibits usage of the structure. This restriction prevents the very open systems interoperability that the Kerberos RFC 1510 specification intends to provide. As a result, other server vendors are unable to interoperate with Windows 2000 clients using the Kerberos authentication protocol.

HP is aware that Kerberos provides important security benefits, and that these benefits are a high priority for CIFS/9000 customers. HP is actively pursuing solutions that will provide Kerberos authentication for CIFS/9000.

4.5 Windows 2000 Authentication: CIFS/9000 Interoperability

CIFS/9000 Server authentication using NTLM v1 is valid and effective in a Windows 2000 Mixed Mode or Native Mode domain. As a member server, CIFS/9000 passes through any authentication request to the domain controller. This pass-through mechanism is unaffected by the domain mode due to the member server status of the CIFS/9000 Server. Native Mode by itself does not affect pass-through authentication.

For the CIFS/9000 Server pass-through authentication mechanism to work, NetBIOS must be enabled in the domain. This topic will be covered in the "Name Resolution" module.

Kerberos pass-through authentication for the CIFS/9000 Server is currently under investigation.

Chapter 5 Active Directory Integration

Active Directory is the flagship of Microsoft's Windows 2000 product. Although Active Directory actually refers to the directory services and LDAP portion of the server feature set, ADS incorporates a colossal assortment of client and domain management utilities. However, the single most important element of deploying Windows 2000 ADS is the design of the domain structure, and subsequently the design of the Advanced Directory schema. Once the schema has been created, it can only be extended further – it cannot be modified. So the design must be done right the first time. The alternative is to re-install and start over.

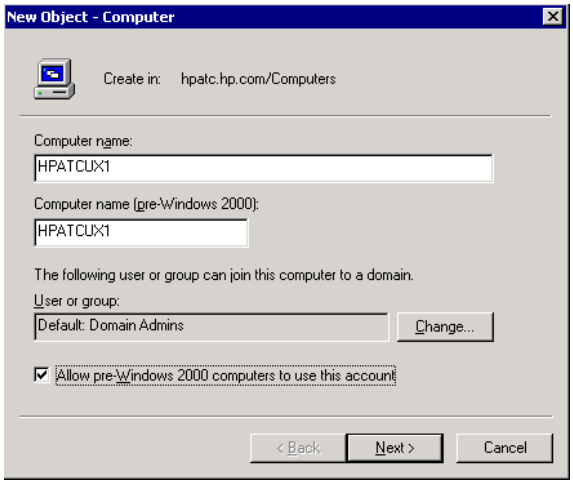
The protocol that is used to access the Advanced Directory is the Lightweight Directory Access Protocol – LDAP. LDAP is based on the IETF RFC 2251, but is not strictly adhered to by Advanced Directory. The RFC standard is important for multi-vendor integration, because it provides a common protocol that can be used to read and write data to the directory.

Integrating CIFS/9000 into the ADS primarily refers to storing user and group account data that is required by the underlying UNIX operating system. The storage of this data is defined and regulated by IETF RFC 2307 for POSIX attributes. This is the most important specification for integrating UNIX and CIFS/9000 into the ADS.

5.1 Adding a CIFS/9000 Server to the Domain ADS

The first step for CIFS/9000 Server integration with the ADS is to add the computer to the domain:

1. On the domain controller, go to Administrator Tools and pull down "Active Directory Users and Computers." Right click on Computers, choose New, and then Computer.
2. Enter the computer name.
3. The "pre-Windows 2000 computers" checkbox is intended to allow the Everyone group to be nested under the "Pre-Windows 2000 Compatible Access" built-in group on the local computer account for local resource access. However, a member server does not hold an account database and the "Pre-Windows 2000 Compatible Access" group is not valid for a member server. Testing has shown that the checkbox has no discernable effect on the CIFS/9000 server operation.



This operation creates an object in the Active Directory for the CIFS/9000 server.

5.2 Windows 2000 and CIFS/9000 Account Interoperability

Windows 2000 file system security is based upon NTFS file system attributes. User and group permissions are set and enforced by the usage of user and group Security Identifiers (SIDs) on Access Control Entries (ACEs) that are contained on Access Control Lists (ACLs). ACLs are present for NTFS files, directories, and other domain resources. For Windows 2000, SIDs are stored in the Active Directory.

CIFS/9000 Server is an HP-UX user-space application. It runs on UNIX, therefore must implement UNIX account security on the files and directories that will ultimately be exported to Windows clients. HP-UX users and groups have synonymous identifiers called User ID (UID) and Group ID (GID). Like Windows SIDs, UIDs and GIDs are associated with every UNIX user and group. Permissions for files and directories are set and enforced by the usage of UIDs and GIDs.

UIDs and GIDs are stored in a UNIX account flat file or database. The typical storage mechanisms are:

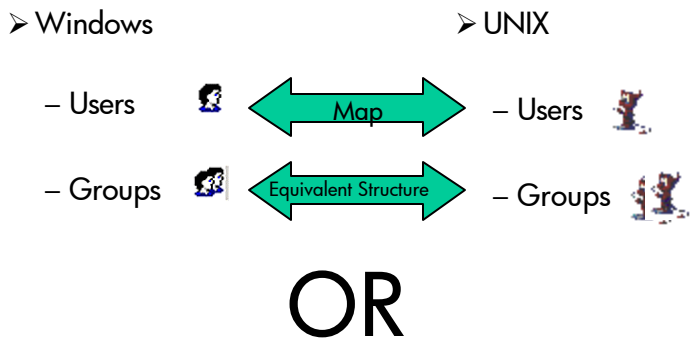
- Files: /etc/passwd, /etc/group
- NIS
- NIS(+)
- LDAP Directory

HP-UX must access one of these storage mechanisms to retrieve user account data when setting or enforcing server resource security, even if the originator of the request is a Windows client.

HP-UX does not recognize a Windows SID, and therefore does not set or enforce file or directory permissions based up on the Windows SID. Instead, CIFS/9000 provides a mapping facility for Windows user names to be associated with an HP-UX user name and its UID. Using this mapping facility, a Windows user may be assigned an HP-UX UID, and file permissions may be set and enforced for Windows clients.

The recommended file system for CIFS/9000 Server is JFS 3.3 (VxFS) with the file system layout version 4 (see http://www.docs.hp.com/hpux/os/11.0/index.html for more details). JFS 3.3 includes POSIX ACL storage and enforcement. CIFS/9000 Server interoperates with JFS 3.3 ACLs, and allows Windows clients to set and manage security attributes on the POSIX ACL in accordance with the user mapping facility.

Separate Windows and HP-UX account databases must be maintained and synchronized on their respective platforms to enforce the CIFS/9000 security model:



…or the separate account databases can be combined onto the Windows 2000 ADS using HP's Unified Login capability.

5.3 Unified Login

Unified Login is officially known as "Integrating HP-UX Account Management and Authentication with Microsoft Windows 2000 Active Directory" at http://www.docs.hp.com/hpux/internet/index.html. Unified Login is an acceptable abbreviation.

Unified Login provides the tools needed to consolidate HP-UX account data and Windows 2000 account data in a common location on the Windows 2000 Active Directory. Users and groups from both platforms are now administered in one place, and users have one user name and one password. These features significantly simplify administration of two different but integrated platforms.

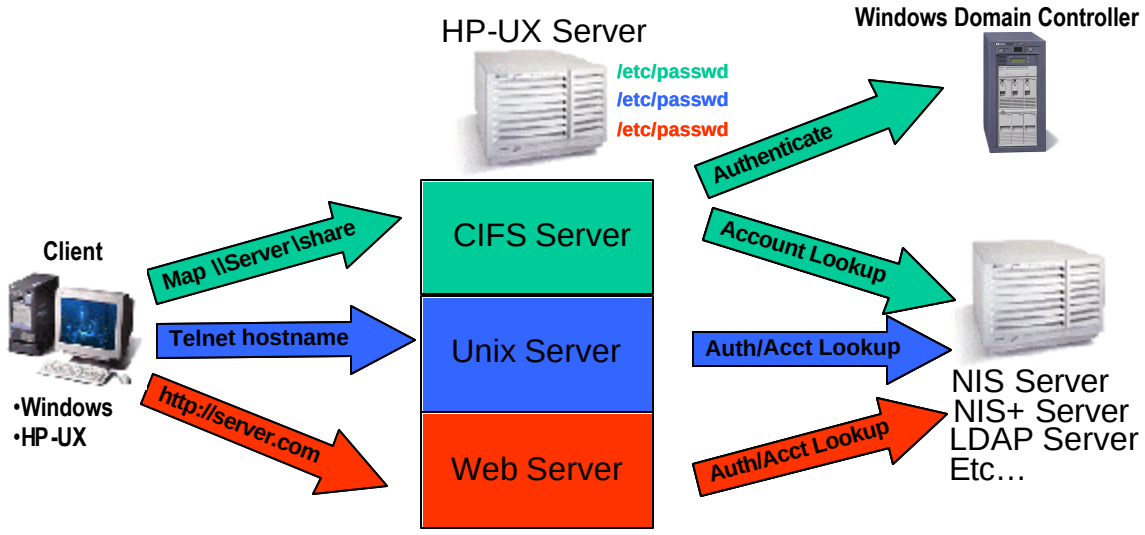
Unified Login uses existing HP products to authenticate and access HP-UX users on ADS:

- PAM_KERBEROS (for HP-UX logins, not CIFS/9000)
- LDAP_UX Integration
- CIFS/9000

The benefits are:

- Cost savings – no dual administration
- No synchronization of accounts
- No confusion – one password for both Windows and HP-UX

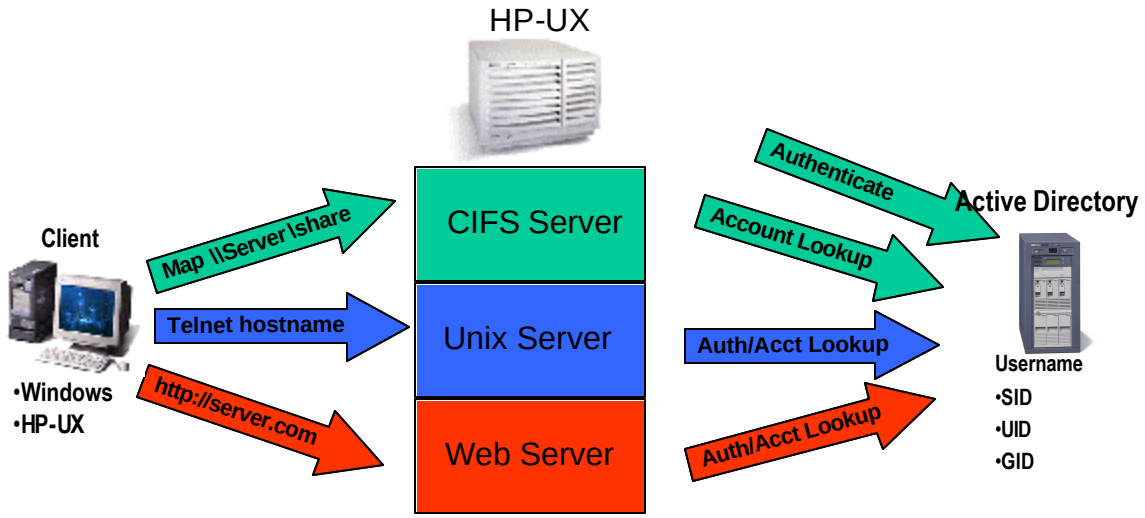
5.3.1 Traditional Login Scenario



- CIFS/9000 Share Mapping
  1. Windows client maps share
  2. Authenticate to Domain Controller
  3. Look up account data (etc\passwd or NIS/LDAP server)
- Telnet
  1. Windows or HP-UX client telnets to host
  2. Look up account data (etc\passwd or NIS/LDAP server)

- Web Server
    1. Web user access secure page
    2. Look up account data (etc\passwd or NIS/LDAP server)

5.3.2 Unified Login Scenario



- CIFS/9000 Share Map
    1. Authenticate to W2000 domain controller (ADS)
    2. Look up account data on W2000 domain controller (ADS)
- Telnet
    1. Windows or HP-UX client telnets to host
    2. Look up account data on W2000 domain controller (ADS)
- Web Server
    1. Web user access secure page
    2. Look up account data on W2000 domain controller (ADS)

With Unified Login, all account lookups are routed to the Windows 2000 Active Directory on the domain controller, whether the account is Windows or HP-UX. /etc/passwd still exists on the servers to hold local account data – like root.

NSSWITCH.CONF is configured to route user and group lookups to LDAP. LDAP configuration points to the Windows 2000 ADS. PAM.CONF sends authentication requests to the correct protocol. For telnet and web users, the KRB5.CONF file is used. CIFS/9000 passes through to NTLM, which is handled by the user space daemon smbd, so PAM is not used at all.

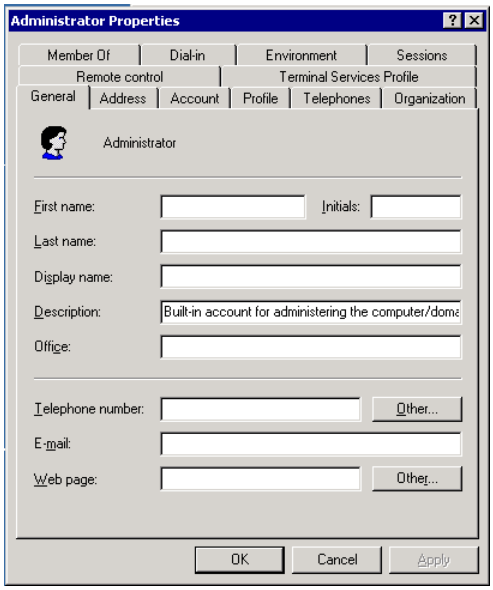
The Windows 2000 Active Directory schema must be extended to add the POSIX account attributes. This extension is accomplished using Microsoft Services For UNIX (SFU) version 2.0, and is a one-way operation – it is not possible to back out the changes once they have been applied to the schema. The HP product set includes LDAP-UX Migration scripts that automatically populate the ADS with existing account data from a standard HP-UX structure.

Detailed installation and configuration instructions are available at:
http://www.docs.hp.com/hpux/internet/index.html.

5.3.3 User and Group Management

The Active Directory schema changes are most visible through the management interfaces. The SFU modifications include modifying the admin “snap-ins” to accommodate the POSIX attributes.

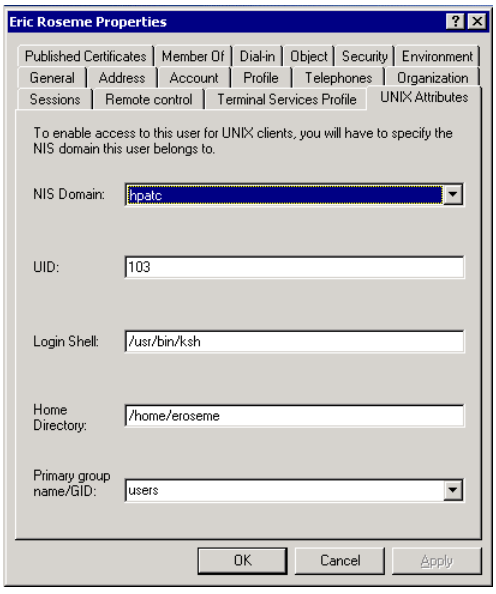
5.3.3.1 Windows 2000 User – Standard Schema



1. On the domain controller, select “Active Directory Users and Computers”
2. Choose users, and right click on a user
3. Select the Properties tab

This will show the standard user administration layout.

5.3.3.2 Windows 2000 User – Extended Schema

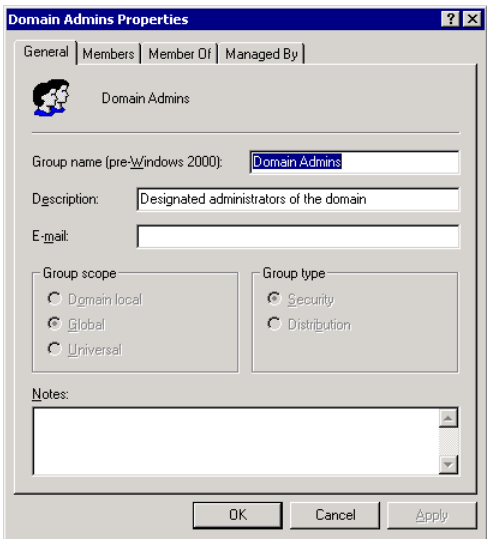


A user properties screen from the extended schema shows the following modifications:

- UNIX Attributes tab
- UID
- Login Shell
- Group membership list

These attributes are on the same user principal as the Windows user attributes, and they use the same password field. There are not dual records – just more data for the same user.

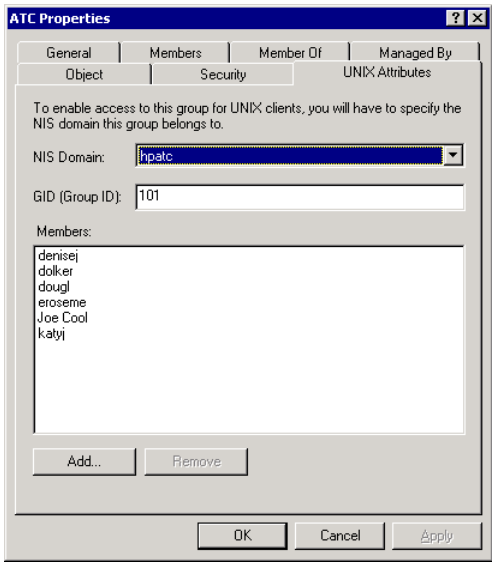
5.3.3.3 Windows 2000 Group – Standard Schema



1. On the domain controller, select Active Directory Users and Groups
2. Choose Groups and right click on a group
3. Select the Properties tab

This will show the standard group administration layout.

5.3.3.4 Windows 2000 Group – Extended Schema



A group properties screen from the extended schema shows the following attributes:

- UNIX Attributes tab
- UNIX Group ID
- UNIX group members

5.4 CIFS/9000 Access Control Lists

Windows 2000 resides on the Microsoft Windows NTFS file system, and utilizes NTFS ACLs. CIFS/9000 preferably resides on the JFS 3.3 file system, and utilizes POSIX ACLs. NTFS ACLs are integrated with the Windows SID security model, and POSIX ACLs are integrated with the UNIX UID security model. Although a POSIX UID can be placed upon the Windows user principal in the ADS (as has been shown in the previous topic) Windows does not have the ability to interpret the UID or enforce security based upon its user identification. Conversely, HP-UX does not have the ability to interpret a Windows SID or enforce security based upon its user identification.

To enforce Windows user permissions on files and directories that reside on HP-UX and JFS, the Windows user must be mapped to the HP-UX UID. This can be accomplished through implicitly mapping the users by using the same name for Windows and HP-UX, or by explicitly mapping the users with the usermap.txt file that is configurable in Samba. The mapped UID is then placed upon the ACL, and permissions are enforced by JFS and HP-UX. Unified Login accomplishes user mapping transparently by using one username for both Windows and HP-UX accounts, without the need for a mapping file.

5.5 ADS Integration Issues

5.5.1 ACL management from Windows 2000 Pro

NT4.0 clients can manage CIFS/9000 JFS 3.3 ACLs from explorer, just like a native NTFS ACL. The same operation from a Windows 2000 Pro client results in the explorer aborting intermittently. This is caused by a change to the SMB calls used by the Windows 2000 Pro client to modify ACLs. A fix for this problem is known and being integrated into the CIFS/9000 Server code.

5.5.2 Unified Logon UNIX Group Management

Windows 2000 Advanced Server administration tools add the Windows distinguished user name to the POSIX group member user lists. The POSIX user name should be added – not the Windows 2000 distinguished user name. This problem has been reported to Microsoft.

5.5.3 HP-UX User Name 8 Characters

HP-UX user names are limited to 8 characters in length. A primary benefit of Unified Login is the consolidation of 2 platform user names – Windows and HP-UX – into 1 user name. To accomplish this, the Windows user name must comply with the HP-UX length restriction of 8 characters.

SFU 2.0 (required for Unified Login) will extend the ADS schema and the scripts will add the user name based upon the HP-UX data source (/etc/passwd or NIS). It will actually place

the same user name in 2 different attributes in the schema: UserPrincipalName and mssfuname.

Changing only the Windows user name will cause the 2 name fields to be out of sync. Both name fields must be changed.

5.6 Active Directory Integration: CIFS/9000 Interoperability

The standard HP-UX account administration for CIFS/9000 utilizes the native UNIX account management utilities like /etc/passwd or NIS. The characteristics of managing Windows clients and CIFS/9000 are well known and reliable due to the legacy of Samba. Integration with Windows 2000 ADS is not a large issue because of the separate security design and mapping requirements.

Unified Login allows the consolidation of account data from Windows and HP-UX on the domain controller Active Directory. This provides a single point of administration for both platforms. In addition, pure UNIX users can still be configured using traditional UNIX security while only the Windows 2000 client users are consolidated on the ADS. The configuration requirements and steps are well defined in the administration guide.

Chapter 6 Name Address Resolution

The convergence of Windows 2000, CIFS/9000, and HP-UX in a single operating environment combines three different methods of resolving names to addresses:

- NetBIOS/WINS (NT4.0 and CIFS/9000)
- BIND (HP-UX UNIX DNS)
- DDNS (Windows 2000 DNS)

Regardless of the method, each name-address resolution protocol accomplishes the same objective:

- Resolve and update names
- Define a schema for data storage
- Replicate data

Microsoft designed Windows NT4.0 around NetBIOS and utilized their WINS service to enable multi-network name resolution. With Windows 2000, Microsoft evolves their platform away from its NetBIOS roots of network protocol and embraces DNS, but interoperability with BIND is impacted because it does not follow the industry standard DNS RFCs completely.

6.1 NetBIOS and WINS

NetBIOS and WINS combine to provide NT4.0 multi-network name resolution. NetBIOS provides name resolution, but it is limited to local subnets. WINS is a separate component that provides multi-subnet connectivity.

6.1.1 NetBIOS

NetBIOS is the NT4.0 (and prior) name resolution protocol, based upon RFC 1001 (protocol) and RFC 1002 (structures). NetBIOS actually is an acronym that represents Network Basic Input Output System, but the BIOS part of NetBIOS is hardly comparable to your PC BIOS. The NetBIOS RFCs simply define how separate computers on a network can find each other and send messages using the following services:

- Name Service: Registration and resolution
- Session Service: Establishing, maintaining, and terminating connections
- Datagram Service: Non-session messaging

The NetBIOS protocol is implemented using a flat, static, 15-character namespace, which limits its range and versatility in burgeoning modern networks. It is also integrally dependant upon broadcast UDP/IP transmission, which is a concern for heavy usage networks. However, NetBIOS was the standard Windows NT4.0 protocol, so CIFS/9000 name resolution is based upon NetBIOS. The most important fact for integrating name resolution for CIFS/9000, Windows 2000, and HP-UX is ***CIFS/9000 requires NetBIOS***.

The next most important rule is to assign the CIFS/9000 server NetBIOS name (in smb.conf) to the same name as the uname of the host HP-UX system. The HP-UX uname is 8 characters long, so the NetBIOS 15 character name (actually it is 16 characters, but the 16th is for the name suffix) length limitation compared to DDNS is not significant. It is important to keep the names coordinated for ease of administration.

CIFS/9000 starts a single nmbd daemon on the system to listen on port 137 for all incoming NetBIOS name service requests. While the number of smbd daemons on the system equates to the number of client connections to the server, the nmbd always stays at 1 daemon per server.

The third most important rule to remember when integrating CIFS/9000 Server with Windows 2000 is that ***Windows 2000 enables NetBIOS by default***. Unless the domain configuration is explicitly changed, CIFS/9000 Server will resolve names to addresses in a Windows 2000 domain.

6.1.2 WINS

Since NetBIOS has a flat namespace and is based upon UDP broadcast transmission, it is inherently incompatible with a multi-subnet network. WINS represents the Windows Internet Name Service, and it provides NetBIOS with the ability to operate on multi-subnet networks. WINS consists of what are usually dedicated Windows servers that hold a name-to-IPaddress resolution database. Servers and clients configure specific WINS servers, and then look there first when attempting to resolve names. The most common resolution order is to look at the WINS server first for a name, then broadcast for name resolution if it cannot be found. This is called H-Node NetBIOS, and it is dependant upon the availability of WINS.

In a Windows 2000 domain, Microsoft recommends configuring the Windows 2000 version of WINS, which is essentially the NT4.0 WINS functionality enhanced with the following features:

- Persistent connections
- Manual tombstones
- Improved management tools
- Enhanced filtering and record searching
- Dynamic deletion
- Record verification and version number validation
- Expert functions

In addition, the Windows 2000 Pro client is enhanced for WINS with the following features:

- Increased fault tolerance (configure more than 2 WINS servers)
- Change NetBIOS options without a reboot

CIFS/9000 Server has a configuration option for a WINS server in the smb.conf configuration file. Currently there can only be one WINS server configured, so WINS redundancy is not possible on a CIFS/9000 server. However, HP has provided an enhancement to the Samba developers to add multi-WINS server capability.

6.2 BIND – UNIX DNS

BIND (Berkeley Internet Name Domain) is the industry standard DNS (Domain Name System). RFC 1034 defines the DNS database format, and RFC 1035 defines the domain name structure (these originated with 882 and 883, respectively). Since the introduction of these two RFCs, there have been many additions, clarifications, and changes to the DNS specification, and a resulting plethora of accompanying RFCs (which will be identified in a handy table in a subsequent sub-module). The definitive BIND DNS information sources are: http://www.isc.org/products/BIND,; and the O'Reilly book "DNS and BIND", fourth edition.

DNS is based upon a hierarchical namespace (represented by the dots in the names) that is much more powerful and flexible than NetBIOS, and is designed to be distributed. Additionally, DNS is implemented with the TCP transport protocol as opposed to UDP, so it is a more network-efficient naming mechanism.

BIND is traditionally considered the "gold standard" of domain name resolution. Of course, BIND is a complex and monstrous topic, which is why the definitive book on it is almost 600 pages long. Here, BIND is examined only by comparison to Windows 2000 DDNS.

6.2.1 BIND DNS on HP-UX

HP-UX 11 delivered BIND version 4.9.7. Most customers should immediately upgrade their HP-UX 11 to at least BIND 8.1.2, which is available at no charge from http://www.software.hp.com. This version of BIND includes the following features:

- DNS Notify (RFC 1996)
- DDNS Support (RFC 2136)
- SRV Record Support (RFC 2052 or 2782)

BIND v9 is also available from software.hp.com. It has the following added features:

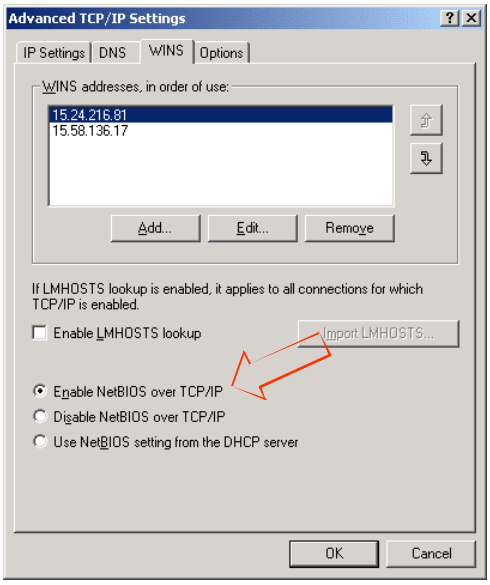
- Incremental Zone Transfer (RFC 1995)
- DNSSEC (DNS security – authentication RFC 2535)

BIND v9.2 should be available from software.hp.com in September 2001.

6.3 Windows 2000 DDNS

Microsoft often refers to Windows 2000 DNS as "DDNS", which represents "Dynamic" DNS. "Dynamic" refers to the automatic DNS registration of nodes. This automatic registration is accomplished with the DHCP client, which runs on every machine in the domain (servers and clients), and registers both DHCP and statically configured clients. However, DDNS has many interesting features and enhancements, and while the dynamic aspect of Windows 2000 DNS is a convenient feature, it is not necessarily the best feature of DDNS.

DDNS replaces both NetBIOS and WINS in the Windows 2000 domain. The default name resolution is DNS, but Microsoft recommends leaving NetBIOS and WINS enabled for compatibility. NT4.0 functionality is so pervasive – even within applications – that assuming the enterprise is Windows-2000-specific is dangerous, even in Native Mode. However, NetBIOS and WINS can be disabled (default is enabled):



Do not disable NetBIOS and WINS when a CIFS/9000 member server is part of the domain.

So Microsoft chose to call Windows 2000 DNS "dynamic", but the integration aspect into the Active Directory is probably the single most effective feature of DDNS. By integrating it into ADS, the replication of DNS servers is handled automatically by the ADS, and there is no requirement to manually configure DNS server distribution. Since the ADS domain structure is multi-master, there is no single DNS master to fail – all of the DCs act as the DNS master. Other DDNS features are:

- ADS Integration
- Secure Dynamic Update (RFC 2136 plus a draft)
- Incremental Zone Transfer (RFC 1995)
- DNS Notify (RFC 1996)
- Service Location (RFC 2053 -> 2782)
- Enhanced Cache Resolver (RFC 2308)
- Enhanced DNS Manger
- Unicode Character Support (UTF-8 draft)
    - Plus 3 other drafts (in other words – non-standard)

It is important to understand how the feature set of DDNS compares to the UNIX BIND versions that are available on HP-UX:

RFC	W2000	BIND 8.1.2	BIND v9
1995 Incremental Zone Transfer	Yes	Yes	Yes
1996 Notification of Zone Changes	Yes	Yes	Yes
2052 DNS SRV	Yes	Yes	Yes
2136 Dynamic updates	Yes	Yes	Yes
2181 Clarifications to Spec	Yes	No (8.2)	?
2308 Negative caching of DNS queries	Yes	No (8.2)	?
2782 DNS SRV	Yes	Implied	Implied

BIND v9 adds IPV6 support and DNSSEC.

6.3.1 Microsoft Windows 2000 DDNS Recommendations

Microsoft makes recommendations about Windows 2000 DDNS interoperability with BIND. This applies to how the DNS implementations may co-exist in a single enterprise:

- The minimum level of BIND should be 8.1.2
    - Supports SRV records (2052 -> 2782)
    - Incremental Zone Transfer (1995)
- 8.2.2 is best – it is the Windows 2000 equivalent
- 8.2.3 has been reported as preferable by some customers, due to security enhancements
- Microsoft's position on v9 is not known at this time

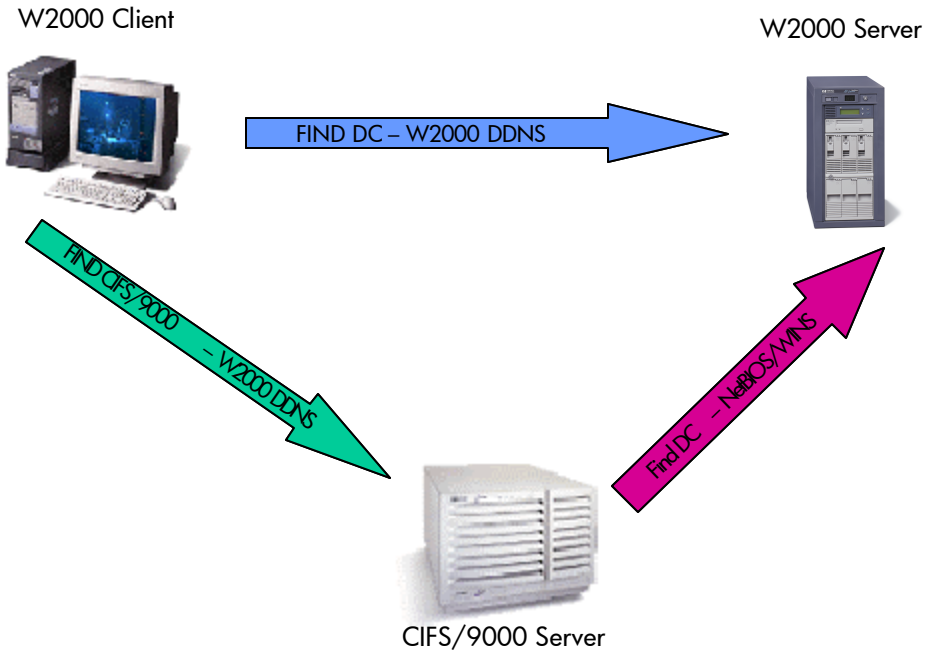
6.4 Name Address Resolution: CIFS/9000 Interoperability

When designing a windows 2000 domain, the DNS design has a profound effect upon the overall ADS design. Both should be considered during the initial Windows 2000 ADS design phase.

The integration of CIFS/9000 into the Windows 2000 domain often implies the pre-existence of HP-UX in the enterprise. When this is true, the usage of BIND DNS is probable, and therefore the integration of the DNS platforms becomes an issue. Windows 2000 DNS can cause problems for BIND DNS because of the extensions and the lack of adherence to specifications. The preferred method to protect a BIND DNS domain from Windows 2000 DDNS is to create a sub-zone for DDNS to exist in. This can provide protection for:

- Zone transfers
  - WINS
    - Windows 2000 zone transfers contain WINS records
    - BIND does not recognize WINS records
    - Do not transfer a W2000 zone to a BIND secondary
  - UTF-8
    - Do not transfer Windows 2000 UTF-8 records to a BIND secondary
- Windows 2000 Global Catalog Server
  - Hosts located in a _msdcs subzone have an illegal DNS name
  - Hostname._msdcs.hp.com – "_" is not a legal RFC 952 character
- Clients delete conflicting names
  - If a client is configured with a name that already exists in the DNS domain, it will delete the old record and add itself

With NetBIOS and WINS enabled, the connectivity diagram looks like:



- A Windows 2000 client will locate the domain controller (or any other Windows domain resource) using DDNS

- A Windows 2000 client will locate the CIFS/9000 server using DDNS
- The CIFS/9000 server will locate the domain controller (for pass-through authentication) using NetBIOS and WINS

6.4.1 Name Recommendations

The conflicting name specifications for the various affected components when integrating CIFS/9000 into a Windows 2000 domain can be confusing:

- RFC 952: A-Z, a-z, 0-9, -
- HP-UX node name
  - 8 characters
- NetBIOS name
  - 15 characters (plus 1 for name suffix)
  - RFC 952 plus !@#$%^&'().- {}~ space
- DNS name
  - 24 characters
  - RFC 952
- DDNS name
  - 63 characters
  - RFC 952 + RFC 2181 + UTF-8

For CIFS/9000:

- Follow RFC 952
- HP-UX node name = NetBIOS name = DNS name
- Name is less-than or equal-to 8 characters

Chapter 7 Windows 2000 DFS

DFS represents Distributed File System. Microsoft DFS refers to the ability to combine multiple servers and/or shares into a common namespace. Be aware that the industry common definition of DFS refers to OSF DCE/DFS, which is a very robust distributed file system used primarily in technical UNIX environments. Windows 2000 DFS bears no relation to OSF DCE/DFS.

The key feature of Windows 2000 DFS is referrals. Referrals allow multiple servers and/or shares to be consolidated under a single namespace. A user would then map the common namespace, and have transparent share mapping among a group of servers and/or shares. Key features are:

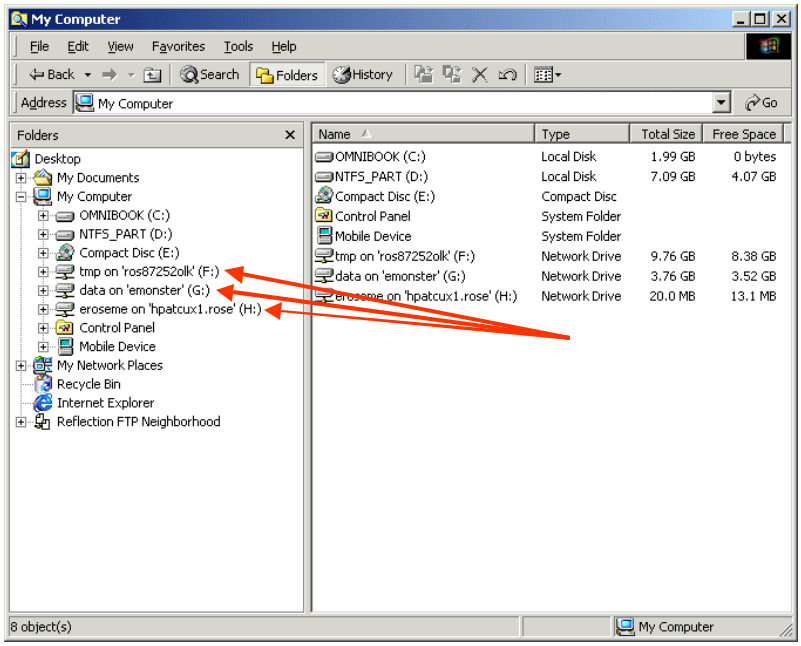
- Transparent share mapping
- Root share – source of common namespace
- Root subordinate mappings are 'referred"

A referral is simply a re-directed share map to another server, but it appears as a local directory under the root namespace. Windows 2000 also adds additional features to DFS:

- Automatic file replication
- Fault tolerance

7.1 Standard Namespace

Observe an explorer view of a standard namespace:

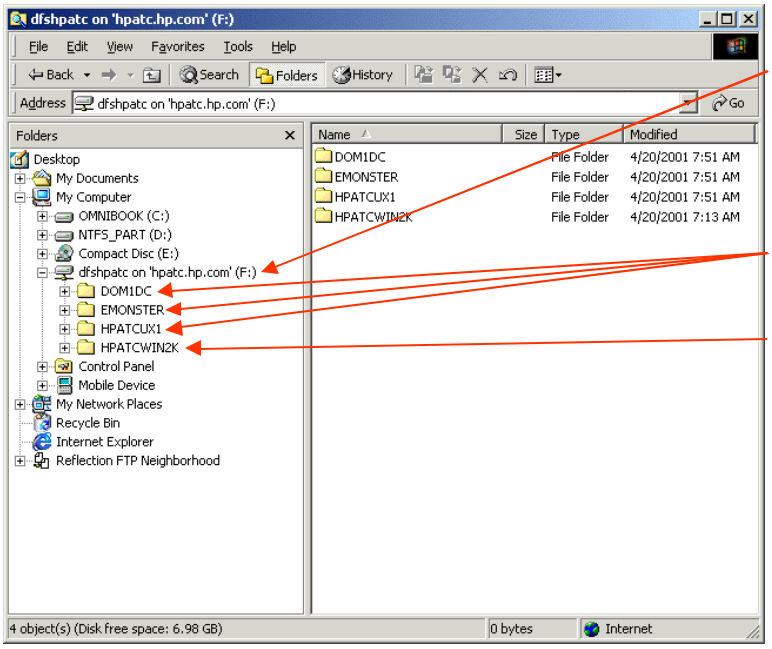


The red arrows point to:

- 3 mapped shares
- 3 separate servers
- 3 logical drives
- 3 distinct namespaces

7.2 DFS Namespace

Compare the standard namespace with the same data consolidated into a single DFS namespace:



The red arrows point to:

- The single DFS root share (dfshpact)
- Single namespace (dfshpatc)
- 3 remote file servers (DOM1DC,EMONSTER, HPATCUX1)
- 1 local filesystem (local to the root share)

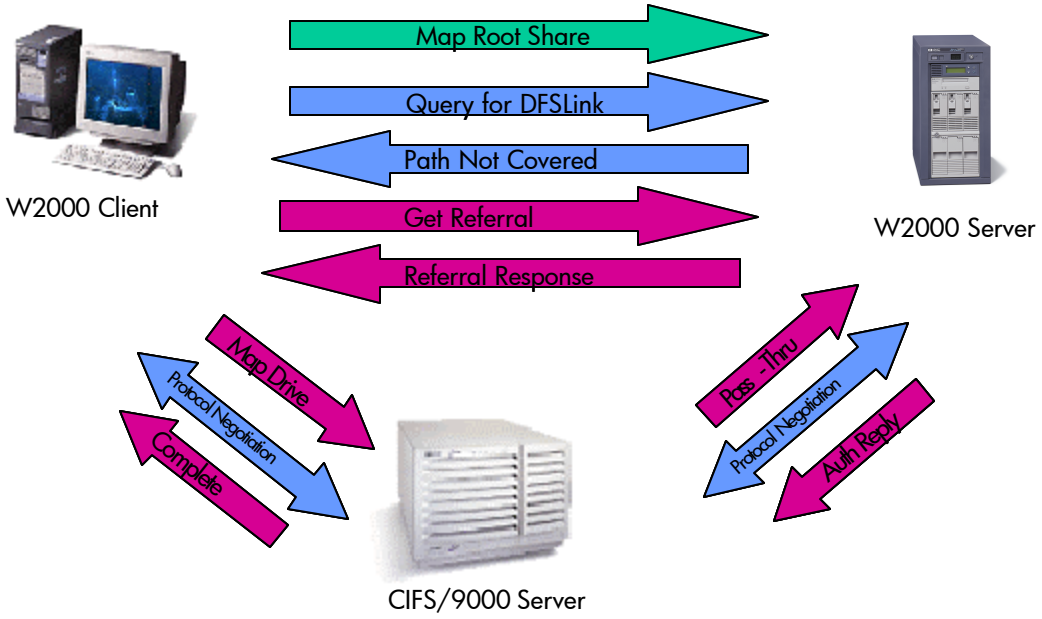
The single DFS namespace can be exported to, and mounted by, any authenticated client.

7.3 Windows 2000 DFS Design

The DFS referral protocol is actually defined in the CIFS specification draft (http://www.snia.org/English/Products/Products_FS.html). Two new DFS SMBs have been added to the spec:

- Trans2_get_dfs_referral
- Trans2_report_dfs_inconsistency

From the client perspective, the referral operation appears as a protocol sequence:



- The client maps the root share (single namespace)
- The client user clicks on a subdirectory, which is really a DFSLink. The operation is sent as a Query for DFSLink
- The server responds that it has no such local path. The operation is sent as a Path Not Covered
- The client then knows that it must get a referral from the server
- The server sends a referral response that tells the client where to connect
- The operation is completed with the standard drive mapping protocol

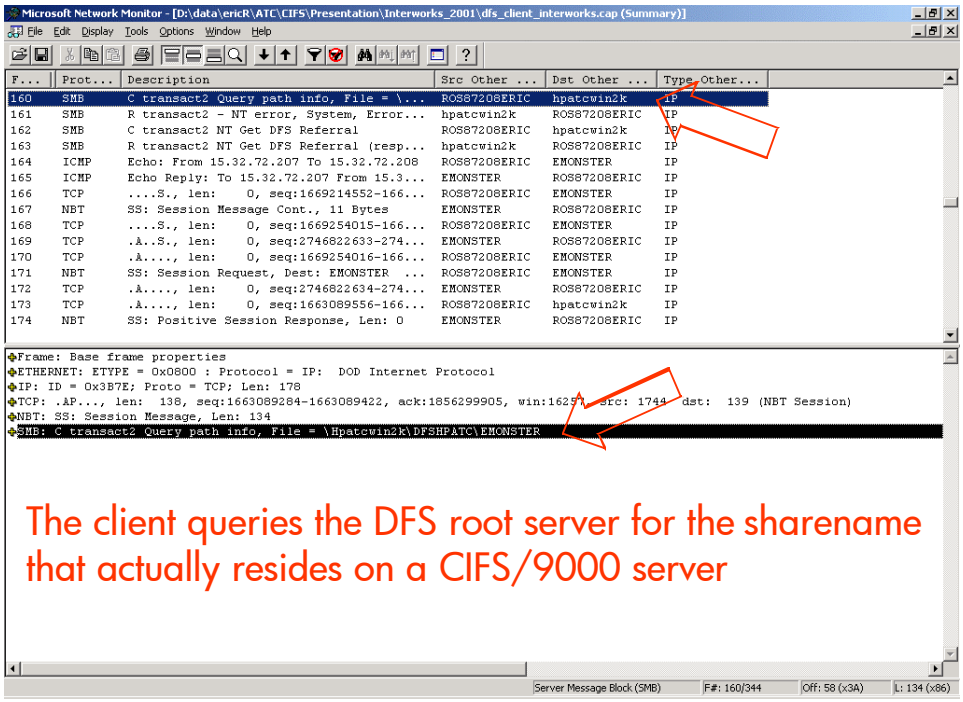
7.4 CIFS/9000 and DFS

The referral protocol exchange occurs exclusively on the client –to-DFS root server connection. To the DFSLink (the actual file server) the operation appears as just another ordinary connection mapping protocol, as long as the standard UNC (Universal Naming Convention) format is used (\\RootServerName\namespace). The CIFS/9000 Server operates as a "Leaf Node", which is the common name for DFSLink. The CIFS/9000 server can only operate as a leaf node – it cannot be a root node.

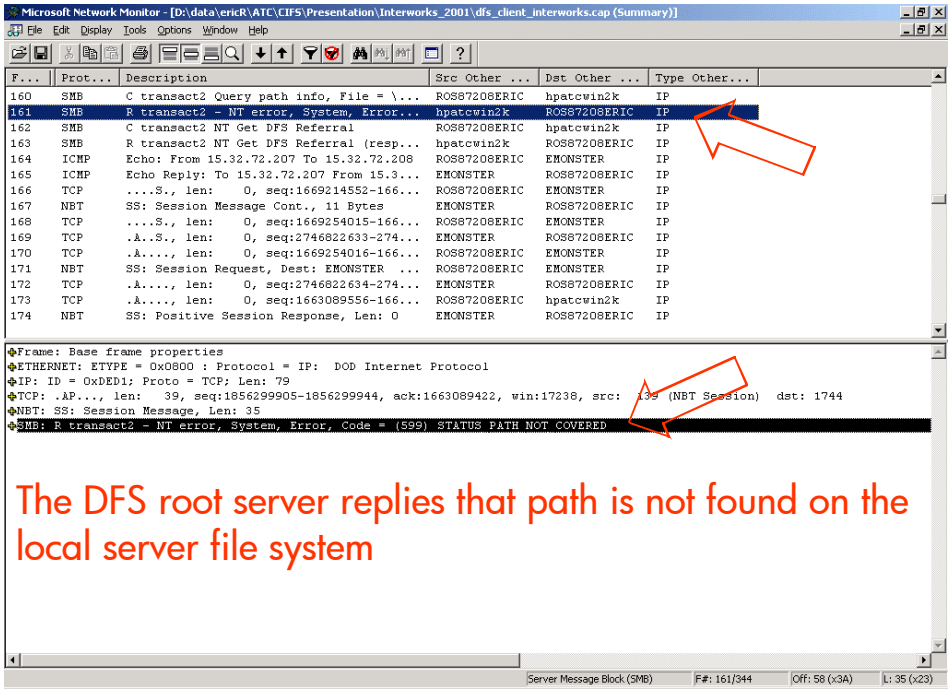
7.4.1 CIFS/9000 Connection Sequence

A Network Monitor trace series shows the query-referral transaction sequence from a Windows 2000 Pro client to a CIFS/9000 server:

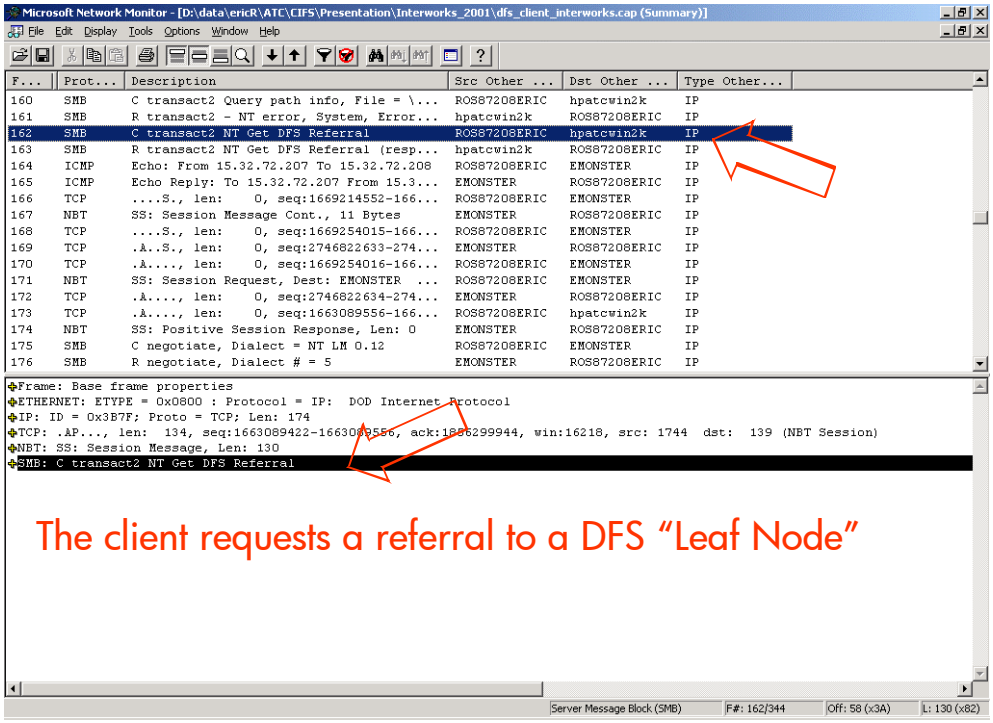
7.4.1.1 DFS Query



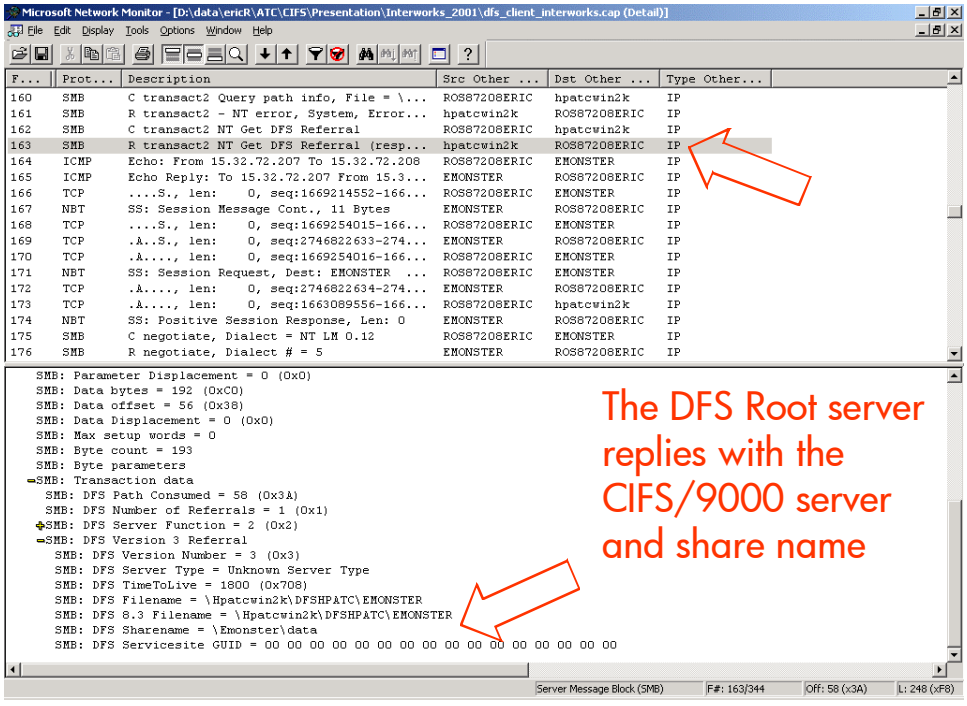
7.4.1.2 DFS Query: path_not_covered



7.4.1.3 DFS Referral Request



7.4.1.4 DFS Referral Reply



The client now has the actual server name and share name where the DFSLink actually resides, and will send a map request to the server – in this case, a CIFS/9000 server. Once the CIFS/9000 server (Emonster) receives the map request from the client, the now-familiar mapping sequence takes place.

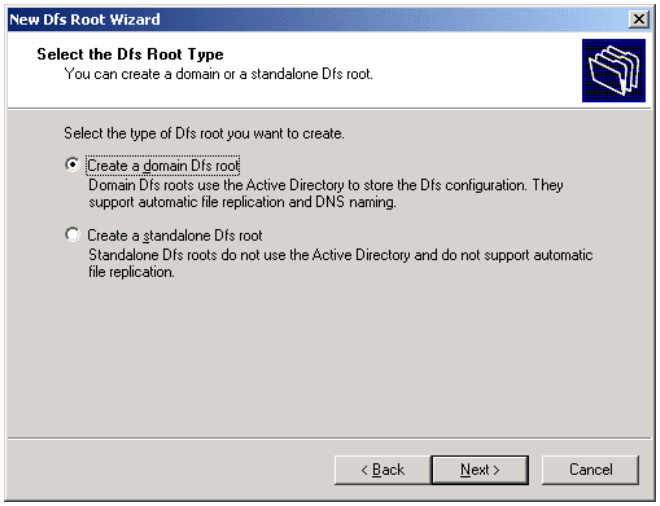
7.4.2 CIFS/9000 DFS Transaction Interoperation

The DFSLink (or leaf node) is not cognizant of the exchange between the DFSRoot and the client – the transaction appears to be a standard share map just like any other. Therefore, the CIFS/9000 server can operate as a DFSLink with no special modifications or enhancements. However, Windows 2000 DFS has numerous extra features, some of which are dependent upon Windows-specific technology.

7.5 Windows 2000 DFS Features

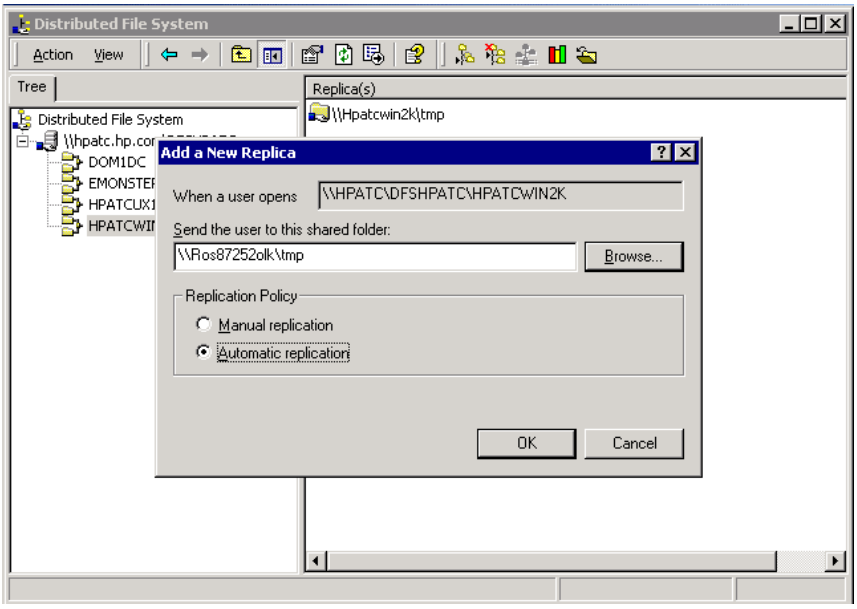
A Windows 2000 DFS root server can be installed on a Windows 2000 Advanced Directory server in one of two ways:

1. Standalone DFS root server
    a. Not integrated into ADS
2. ADS integrated DFS root server
    a. DFS configuration data stored in ADS
    b. Automatic file replication between root and leaf node servers
    c. Fault tolerance for root and leaf servers
    d. Preferential replica selection (best failover choice for connecting clients)



The Standalone configuration does not include the root fault tolerance, replication, and preferential replica selection, but its DFSLink servers are still capable of being fault tolerant (if the DFSLink server platform supports the fault tolerant feature).

Executing Automatic File Replication requires that the server file system be on NTFS 5.0. Consequently, CIFS/9000 Server cannot execute Automatic File Replication as a DFSLink server. However, fault tolerance (redirecting a referral when the initial DFSLink is down) can be enabled for CIFS/9000 by configuring Automatic File Replication. The CIFS/9000 server will not replicate, but it will fail over correctly. After testing this configuration option with CIFS/9000 Server, there was no apparent adverse reaction to configuring Automatic File Replication to enable fault tolerance, other than it does not replicate.



The DFS administration tool resides on the ADS server. If the DFS root is a standalone server, then it must be administered on that server. If the DFS root is on ADS, then it can be administered on any DC in the domain. The following details apply to Windows 2000 DFS:

- There can be 1 DFS root per domain controller
- 32 domain controllers can host the same DFS root in one domain (for exceptional fault tolerance)
- There can be unlimited DFS roots in the domain (except that the limit is one per domain controller, so the practical limit is the number of domain controllers in the domain)
- Automatic replication requires NTFS 5.0
- A DFSLink (leaf node) can exist on any UNC path (Universal Naming Convention: \\Servername\Sharename) in the domain.

7.6 Windows 2000 DFS: CIFS/9000 Interoperability

CIFS/9000 Server can participate in a Windows 2000 DFS as a DFSLink (leaf node) only. A DFSLink is the target of a referral by the DFS root. The DFSLink role for a CIFS/9000 Server is consistent with the member server status of CIFS/9000 in a Windows 2000 domain. Root node status - whether standalone or ADS integrated - requires domain controller capability.

Domain root nodes that are configured in the ADS are fault tolerant if they are replicated to other DCs in the domain. DFSLinks can be configured for automatic file replication, which enables fault tolerance. A CIFS/9000 server cannot execute automatic file replication, but can be configured for fault tolerance. Providing replication for a CIFS/9000 server DFSLink requires some method of file replication from one DFSLink to another, either manually or through a mechanism such as rsync (http://samba.anu.edu.au/rsync/).

Chapter 8 Summary: CIFS/9000 and Windows 2000 Interoperability

CIFS/9000 Server is based upon NT4.0 technology. CIFS/9000 Server integration within a Windows 2000 domain is simplified to a large degree by the member server status of CIFS/9000. As a member server, CIFS/9000 simply handles file storage within a domain. The complicated client management features of Windows 2000 must be handled by domain controllers that carry a copy of the Active Directory. Since a CIFS/9000 server does not carry a copy of the Active Directory, most of the complex domain interoperability activity is not an interoperability issue.

A Windows 2000 domain can exist in a Mixed Mode or Native Mode capacity. There are feature trade-offs that comprise the motivation for the enterprise to operate in one mode as opposed to another. CIFS/9000 Server can exist in either domain mode, with little effect on the operation of the CIFS/9000 server. The most important consideration in the Mixed-versus-Native decision is the one-way nature of the transition, which is a more global Windows 2000 consideration and not specific to CIFS/9000 Server interoperability.

The authentication protocol for CIFS/9000 Server is NTLM. Windows 2000 is standardized on Kerberos. The CIFS/9000 Server NTLM pass-through authentication protocol can integrate into a Windows 2000 domain in Mixed Mode or Native Mode. Windows 2000 Pro clients can authenticate into the Windows 2000 domain using Kerberos, but map shares to CIFS/9000 servers with NTLM. HP is investigating a Kerberos authentication module for the CIFS/9000 server.

HP-UX security can be integrated into the Windows 2000 Active Directory to store all user account data. CIFS/9000 Server leverages this capability by looking up UNIX user account data in the Active Directory. This simplifies administration by combining the Windows user data and the HP-UX user data into one organizational unit on the ADS, with only one password to maintain for both users. All account lookups are done with LDAP.

Name address resolution seems complicated on Windows 2000 because of the DDNS non-standard exceptions to BIND, and the utilization of NetBIOS and WINS by CIFS/9000. But by accepting the Microsoft recommended default of NetBIOS and WINS enabled, CIFS/9000 Server integrates transparently into a Windows 2000 domain. HP is investigating full DNS participation of the CIFS/9000 Server.

Windows 2000 DFS is a handy feature that can be used to simplify resource access in a domain, and also provides fault tolerance capability for file servers. The CIFS/9000 server can be a DFSLink leaf node in a DFS implementation, which is consistent with a member server role.

Windows 2000 is especially adept at client management and domain administration. Enterprise level file serving with high availability, huge and reliable data storage capacities, and robust scalable hardware is best accomplished with UNIX. CIFS/9000 on HP-UX 11 provides all these enterprise level characteristics, and integrates into a Windows 2000 domain with ease.

Appendix A UPN Logon Name

Windows 2000 Pro clients can logon to a domain in a number of different ways:

- SAM logon
  - Security Account Manager
- FQDN logon
  - Fully Qualified Domain Name
- UPN logon
  - User Principal Name

A.1 Security Account Manager Logon Name

The SAM logon name is the default NT4.0 style logon method. The user enters a user name and then selects a domain from a pull-down menu on the dialog box:

A.2 Fully Qualified Domain Name Logon Name

The FQDN logon name consists of a user name followed by an "@" sign, then the fully qualified domain name that the user belongs to. When the "@" sign is entered, the SAM domain menu immediately is grayed out, because the user is required to enter the complete logon name.

A.3 User Principal Logon Name

The UPN logon name consists of a user name followed by an "@" sign, then a configured logon name. Instead of supplying the FQDN, the user supplies a name that has been configured on the Global Catalog, and the domain controller does a lookup on the Global Catalog to find the FQDN that is associated with the configured name.

This is useful for standardizing user logons when there are multiple sub-domains in an organization. If a user changes sub-domains, the administrator can simply re-configure the UPN to point to a different FQDN, and the user then retains the original logon name.

User Principal Names are only available in Native Mode.