

# CIFS/9000 and Windows 2000 Interoperability



**i n v e n t**

HPWorld, August

Eric Roseme  
Systems Networking Solutions  
Lab

Harlett, Richard



**i n v e n t**

The Windows 2000 feature set is larger and more varied than Windows NT. The following slides examine how CIFS/9000 interoperates with some of the more pervasive aspects and features of Windows 2000.



# Agenda: CIFS/9000- W2000

## ➤ **CIFS/9000 Overview**

- W2000 Domain Mode: Mixed vs Native
- Authentication: Kerberos and NTLM
- Active Directory Integration
- W2000 Name Address Resolution
- W2000 DFS

# CIFS/9000 Overview

➤ CIFS/9000: SMB file/print services on HP-UX

➤ Enterprise File Servers

- Reliability 99.999
- Highly Available: ServiceGuard
- Scalable: A-Class, L-Class, N-Class, Superdome
- Storage:
  - XP48, XP256, XP512
  - VA7100, VA7400, FC10, FC60
- Flexibility:
  - Dedicated File Servers
  - Multi-Purpose Servers



➤ No Added Costs or Licensing

# CIFS/9000 Overview

➤ CIFS/9000 based upon NT4.0 (Samba 2.0.7)

-So we have to discuss *Migration* to W2000

-*NOT* a migration presentation

-*NOT* a W2000 domain design presentation



➤ NT4.0 *Member Server* - Domain Mode

# CIFS/9000 Overview

## ➤ NT4.0 Technology

- PDC, BDC, Member servers
- 4.0 Authentication
- Trusts: Explicit 1-way, 2-way
- Global and Local groups
- Domain modes (Master, Resource, etc)
- 4.0 Name Resolution

## ➤ UNIX Security

- /etc/passwd
- NIS(+)
- LDAP
- Etc.....








# CIFS/9000 Overview

WINDOWS

MIGRATION MIGRATION MIGRATION

NT4.0 	W2000 Mixed 	Mixed-Migrated 	Native W2000
Features	Features	Features	Features
Benefits	+Benefits -	+Benefits -	+Benefits -
	Benefits	Benefits	Benefits <b>Permanent</b>



# Agenda: CIFS/9000- W2000

- CIFS/9000 Overview
- **W2000 Domain Mode: Mixed vs Native**
- Authentication: Kerberos and NTLM
- Active Directory Integration
- W2000 Name Address Resolution
- W2000 DFS
- W2000 Client Support



# W2000 Mixed Mode versus Native Mode



## ➤ Domain Design: Mixed or Native Mode

- Configure root server as Native Mode
- Configure root server as Mixed Mode
  - Migrate to Native Mode Later
- Migrate a PDC to root server
  - Migrate to Native later

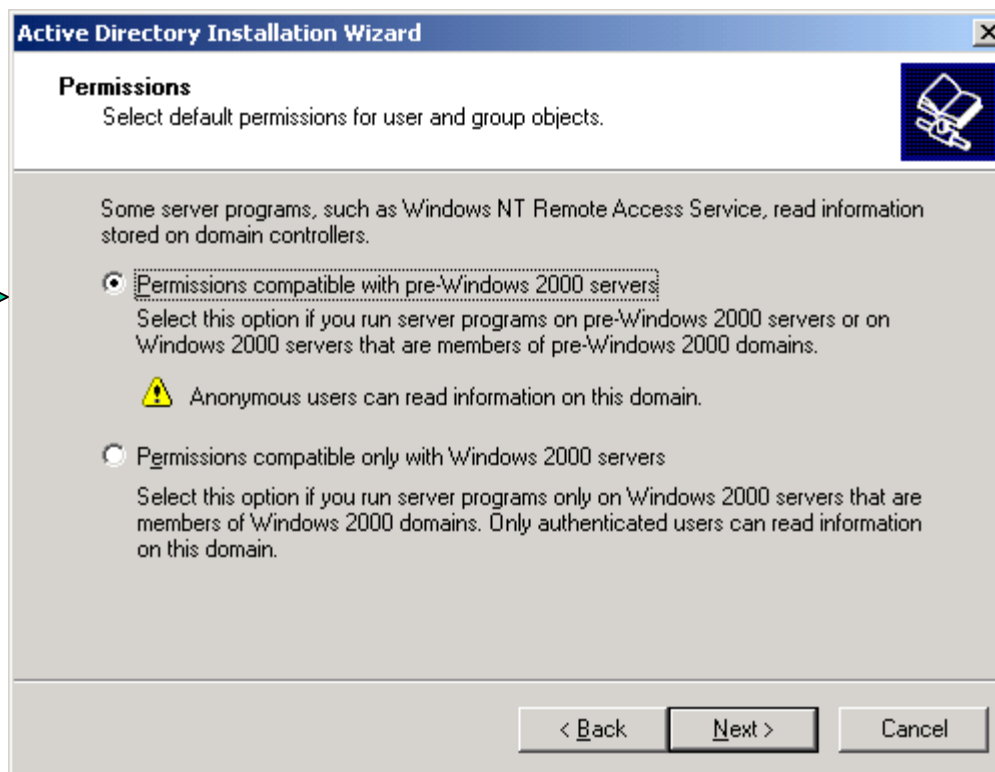
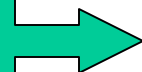
## ➤ Determine effects on general domain features

## ➤ Determine effects on CIFS/9000 Servers

# Configure Root DC

Enable

if:  
MIXED



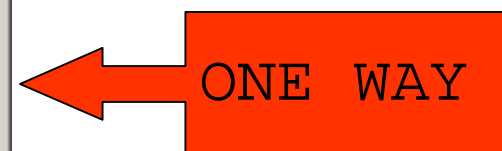
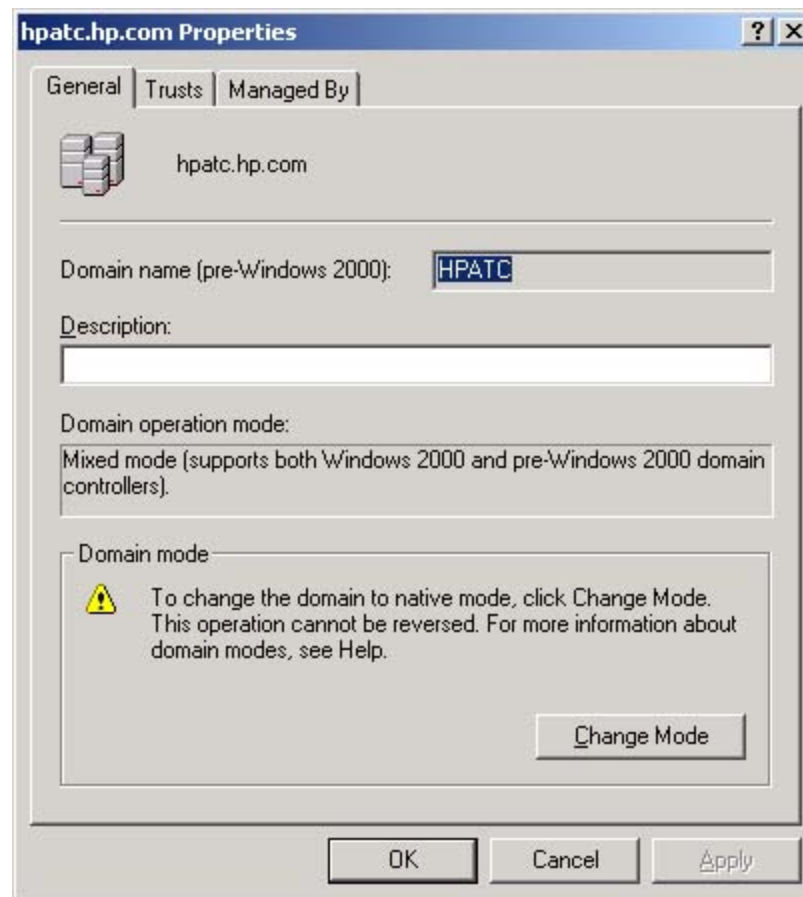
\*Enable i

NATIVE



\* Does not actually enable

# Native Mode





# Effects on Domain Features

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;	No	Yes
Group Nesting	Yes	Yes
NTLM Authentication	Yes	Yes
Kerberos Authentication	Yes*	Yes*
UPN Logon Name (see appendix A)	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



# PDC Emulator

- PDCE also called FSMO PDC - Typically on Root DC
- Mixed Mode Functions (plus Native Mode Functions)
  - Write Copy of SAM Database
  - Distribute SAM Database to BDCs
  - Domain Master Browser: NetBIOS (<0x1B>) Suffix
- Native Mode Functions
  - Password Changes Replicated to Preferentially
  - Bad Password Logon Attempts Routed here
    - Because Password Changes are Replicated Preferentially
  - Account Lockouts

# CIFS/9000



## Recommendation

### ➤ CIFS/9000 *MEMBER* Server

- Not affected by NATIVE MODE
  - No SAM database (PDC/BDC)
  - No Windows users/groups to update
  - No Windows Groups added/lost
  - Admin effects - none, CIFS admin by SWAT
- W2000 Domain Must enable NetBIOS (default)
- W2000 Domain must do NTLM (default)

### ➤ ***Determine Overall Domain Effect***

### ➤ ***More in Authentication***



# Agenda: CIFS/9000- W2000

- CIFS/9000 Overview
- W2000 Domain Mode: Mixed vs Native
- **Authentication: Kerberos and NTLM**
- Active Directory Integration
- W2000 Name Address Resolution
- W2000 DFS

# CIFS/9000



## Authentication

- CIFS/9000 Authenticates using NT4.0 **NTLM v1**
- Authentication is pass-through (domain mode)
- CIFS/9000 can co-exist in W2000 domain with Kerberos client logins!
  - EVEN IN NATIVE MODE!
- W2000 Domain Security with CIFS/9000
  - W2000 Clients = **Kerberos**
  - CIFS/9000 Servers = **NTLM v1**



# NTLM Details

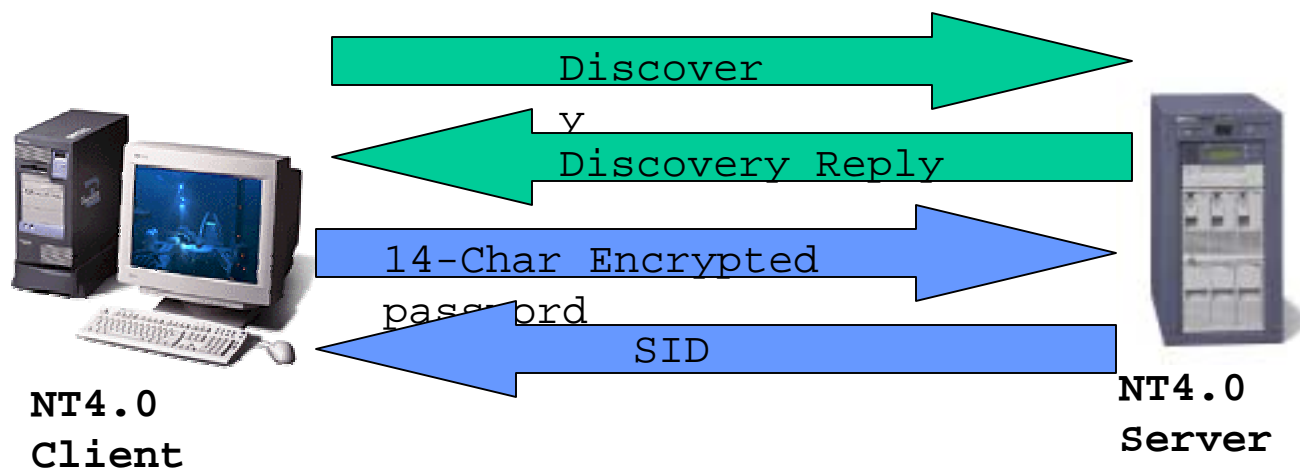
- NTLM Challenge-Response (then)
  - Improved security over LAN Manager
    - 14 character passwords
  - Encryption across wire
  - Password fragments across wire
- NTLM Challenge-Response (now)
  - Proprietary protocol
  - Performance bottleneck
  - One-way authentication (client only)
  - No authentication delegation (service proxy)
  - Requires complex trust management for multi-domains

# W2000 Kerberos Details

- Microsoft "Industry Standard"
  - "based on" V5 - RFC 151
- Authenticate once - re-use credentials
- Client *AND* Server are authenticated
- Authentication proxy - Apps impersonate clients
- Mutual authentication allows Transitive Trusts
- Better encryption



# NT4.0 Client Logon with NTLM



CIFS/9000  
Server

# NT4.0 Client Logon with NTLM



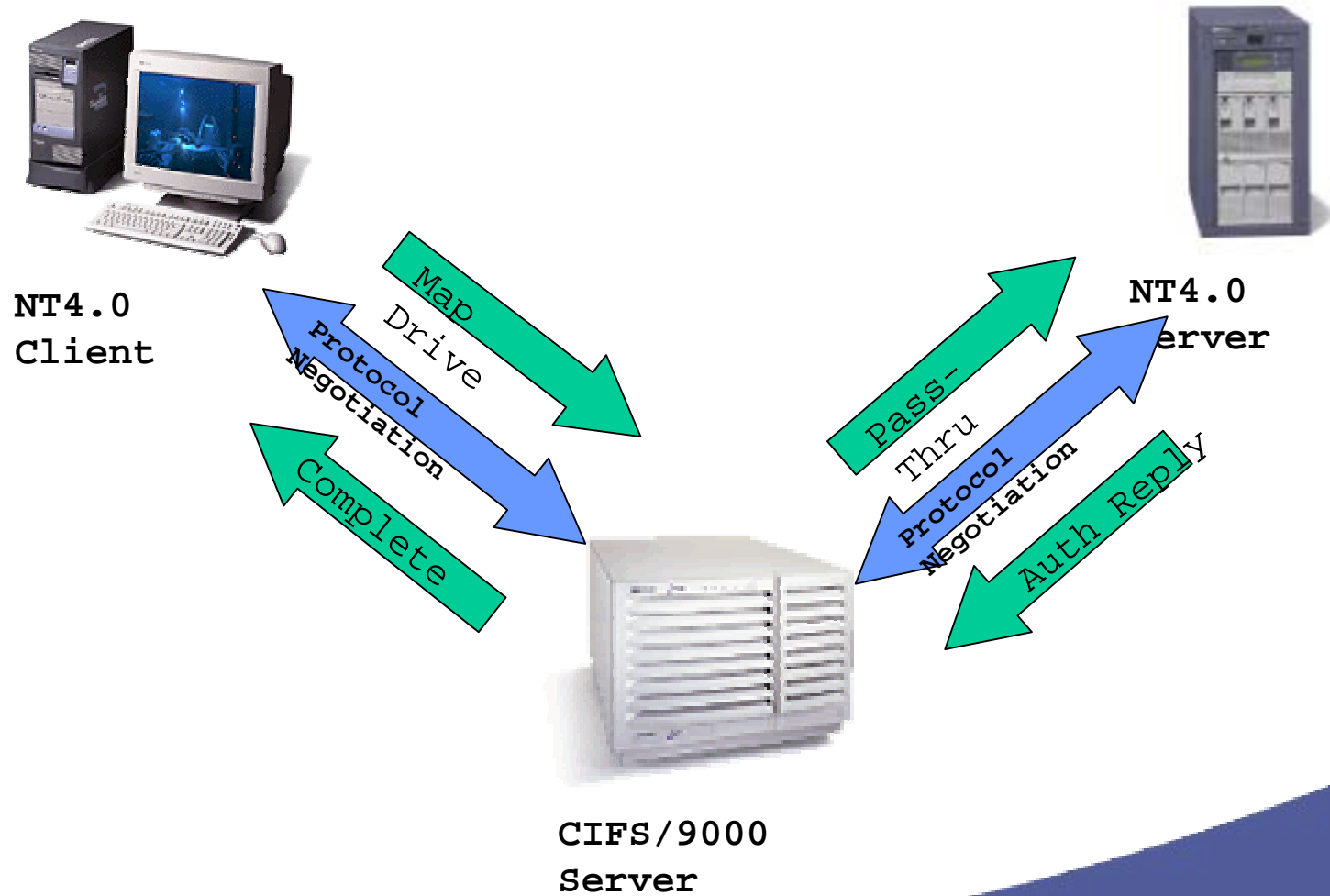
Microsoft Network Monitor - [D:\data\ericR\ATC\CIFS Server\Presentation\Interworks\_2001\NT4\_Interworks2001.cap (Summary)]

File Edit Display Tools Options Window Help

F...	Pr...	Description	Src Othe...	Dst Oth...	Type Ot...
1	Ne...	SAM LOGON request from client	RO887252OLK	SNSLATC-NT	IP
2	Ne...	SAM LOGON request from client	RO887252OLK	SNSLATC-NT	IP
3	Ne...	SAM LOGON request from client	RO887252OLK	SNSLATC-NT	IP
4	Ne...	SAM Response to SAM LOGON request	SNSLATC-NT	RO88725...	IP
5	Ne...	SAM Response when user is unknown	SNSLATC-NT	RO88725...	IP
6	TCP	...S., len: 0, seq:2526769735-25...	RO887252OLK	SNSLATC-NT	IP
7	TCP	.A.S., len: 0, seq:2418853562-24...	SNSLATC-NT	RO88725...	IP
8	TCP	.A..., len: 0, seq:2526769736-25...	RO887252OLK	SNSLATC-NT	IP
9	NBT	SS: Session Request, Dest: SNSLATC-N...	RO887252OLK	SNSLATC-NT	IP
10	NBT	SS: Positive Session Response, Len: 0	SNSLATC-NT	RO88725...	IP
11	SMB	C negotiate, Dialect = NT LM 0.12	RO887252OLK	SNSLATC-NT	IP
12	SMB	R negotiate, Dialect # = 5	SNSLATC-NT	RO88725...	IP
13	SMB	C session setup & X, Username = , an...	RO887252OLK	SNSLATC-NT	IP
14	SMB	R session setup & X, and R tree conn...	SNSLATC-NT	RO88725...	IP
15	SMB	C NT create & X, File = \NETLOGON	RO887252OLK	SNSLATC-NT	IP
16	SMB	R NT create & X, FID = 0x800	SNSLATC-NT	RO88725...	IP
17	MSRPC	c/o RPC Bind: UUID 12345678-...	RO887252OLK	SNSLATC-NT	IP
18	SMB	R write & X, Wrote 0x48	SNSLATC-NT	RO88725...	IP
19	SMB	C read & X, FID = 0x800, Read 0x400 ...	RO887252OLK	SNSLATC-NT	IP
20	MSRPC	c/o RPC Bind Ack: call 0x1 asso...	SNSLATC-NT	RO88725...	IP
21	R_...	RPC Client call logon:NetrServerReqC...	RO887252OLK	SNSLATC-NT	IP
22	SMB	R write & X, Wrote 0x70	SNSLATC-NT	RO88725...	IP
23	SMB	C read & X, FID = 0x800, Read 0x400 ...	RO887252OLK	SNSLATC-NT	IP
24	R_...	RPC Server response logon:NetrServer...	SNSLATC-NT	RO88725...	IP
25	R_...	Error: Bad Opcode (Function does not...	RO887252OLK	SNSLATC-NT	IP
26	SMB	R write & X, Wrote 0x9c	SNSLATC-NT	RO88725...	IP
27	SMB	C read & X, FID = 0x800, Read 0x400 ...	RO887252OLK	SNSLATC-NT	IP
28	MSRPC	c/o RPC Fault: call 0x2 cont...	SNSLATC-NT	RO88725...	IP
29	R_...	RPC Client call logon:NetrServerAuth...	RO887252OLK	SNSLATC-NT	IP
30	SMB	R write & X, Wrote 0x9c	SNSLATC-NT	RO88725...	IP
31	SMB	C read & X, FID = 0x800, Read 0x400 ...	RO887252OLK	SNSLATC-NT	IP
32	R_...	RPC Server response logon:NetrServer...	SNSLATC-NT	RO88725...	IP

Summary of the NETLOGON Packet F#: 1/212 Off: 216 (xD8) L: 120 (x78)

# NT4.0 Map CIFS Drive - NTLM



# NT4.0-CIFS/9000 Pass- Thru



Microsoft Network Monitor - [D:\data\eric\ATC\CIFS Server\Presentation\Interworks\_2001\NT4\_Interworks2001\_2.cap (Summary)]

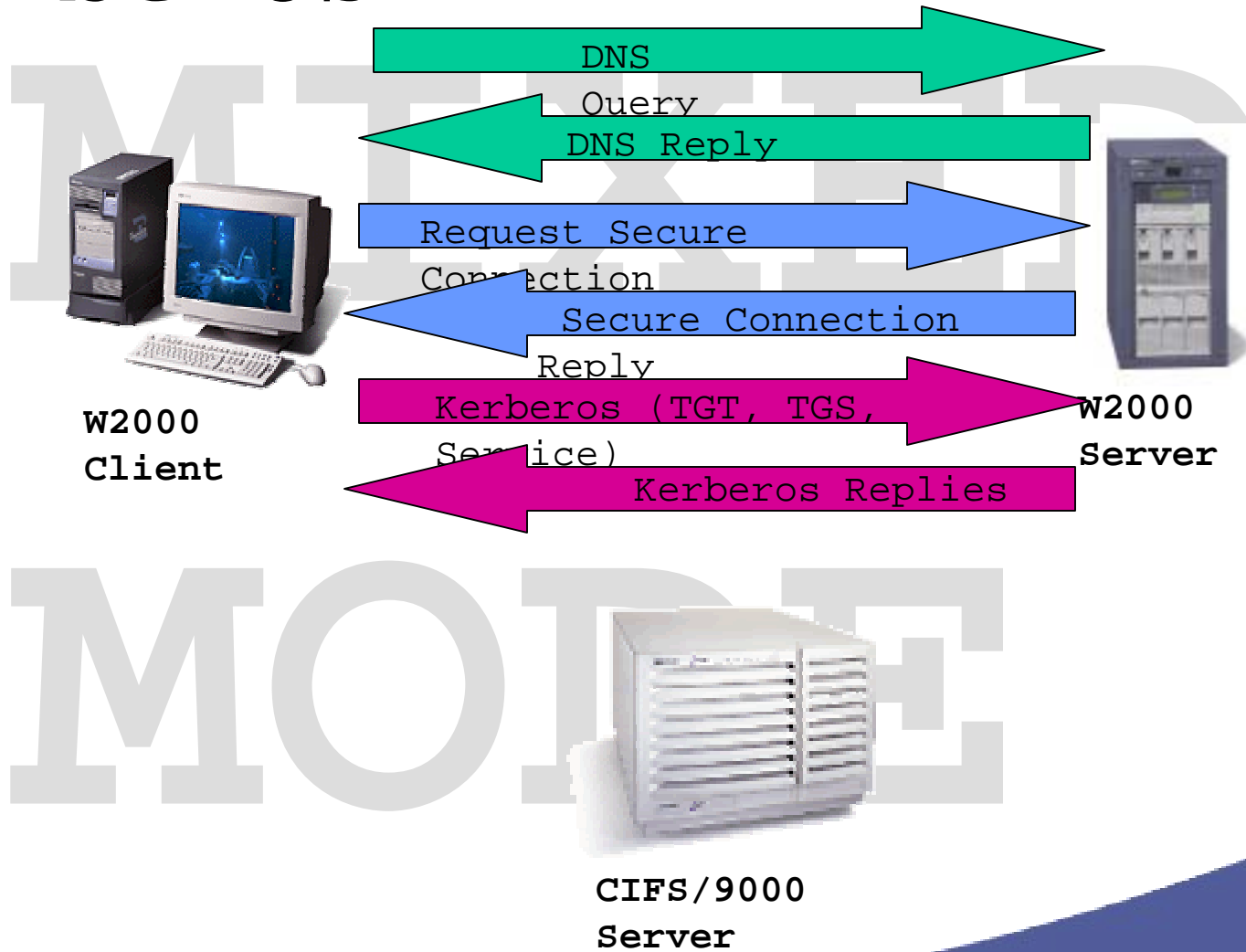
F...	Pr...	Description	Src Oth...	Dst Oth...	Type Ot...
81	NBT	NS: Query (Node Status) resp. for E...	EMONSTER	ROS8725...	IP
82	TCP	...S., len: 0, seq:2272390770-2	ROS8725	EMONSTER	IP
83	TCP	.A..S., len: 0, seq:2399826058-2...	EMONSTER	ROS8725...	IP
84	TCP	.A...., len: 0, seq:2272390771-2...	ROS8725...	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 s F#: 81/190 Off: 42 (x2A) L: 62 (x3E)

Client to CIFS/9000 Server

CIFS/9000 server to NT4.0 PDC

# W2000 Client Logon with Kerberos



M O D E L

CIFS/9000 Server

# Client Logon - Kerberos



Microsoft Network Monitor - [D:\data\erik\ATC\CIFS\Presentation\Interworks\_2001\inter2001\_boot\_logon.cap (Summary)]

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: 0, seq:3945813196...	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	NDP	SS: Session Message Cont: 1242 B...	ROS87208ERIC	hpatcwin2k	IP
58	TCP	.A...., len: 0, seq:2175427613...	hpatcwin2k	ROS87208ERIC	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 = y	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.Default...	ROS87208ERIC	hpatcwin2k	IP

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



# W2000 Map CIFS Drive - NTLM



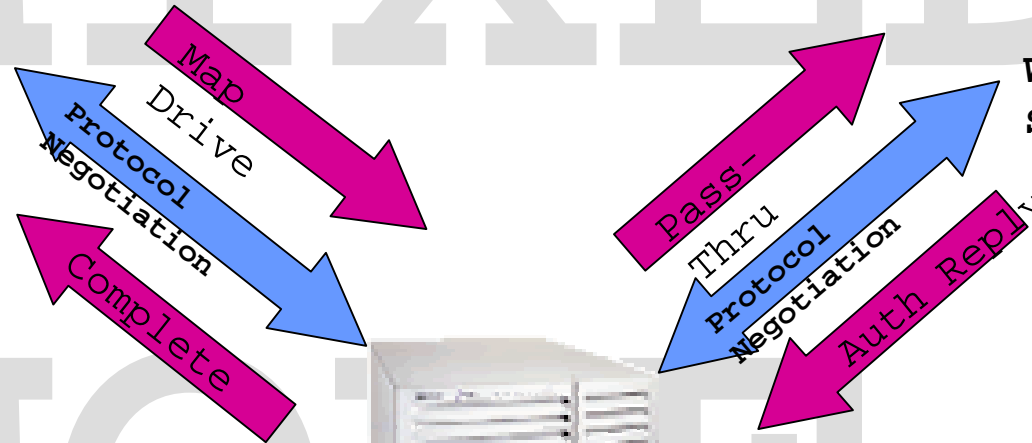
W2000  
Client



W2000  
Server



CIFS/9000  
Server



# W2000-CIFS/9000 Pass-



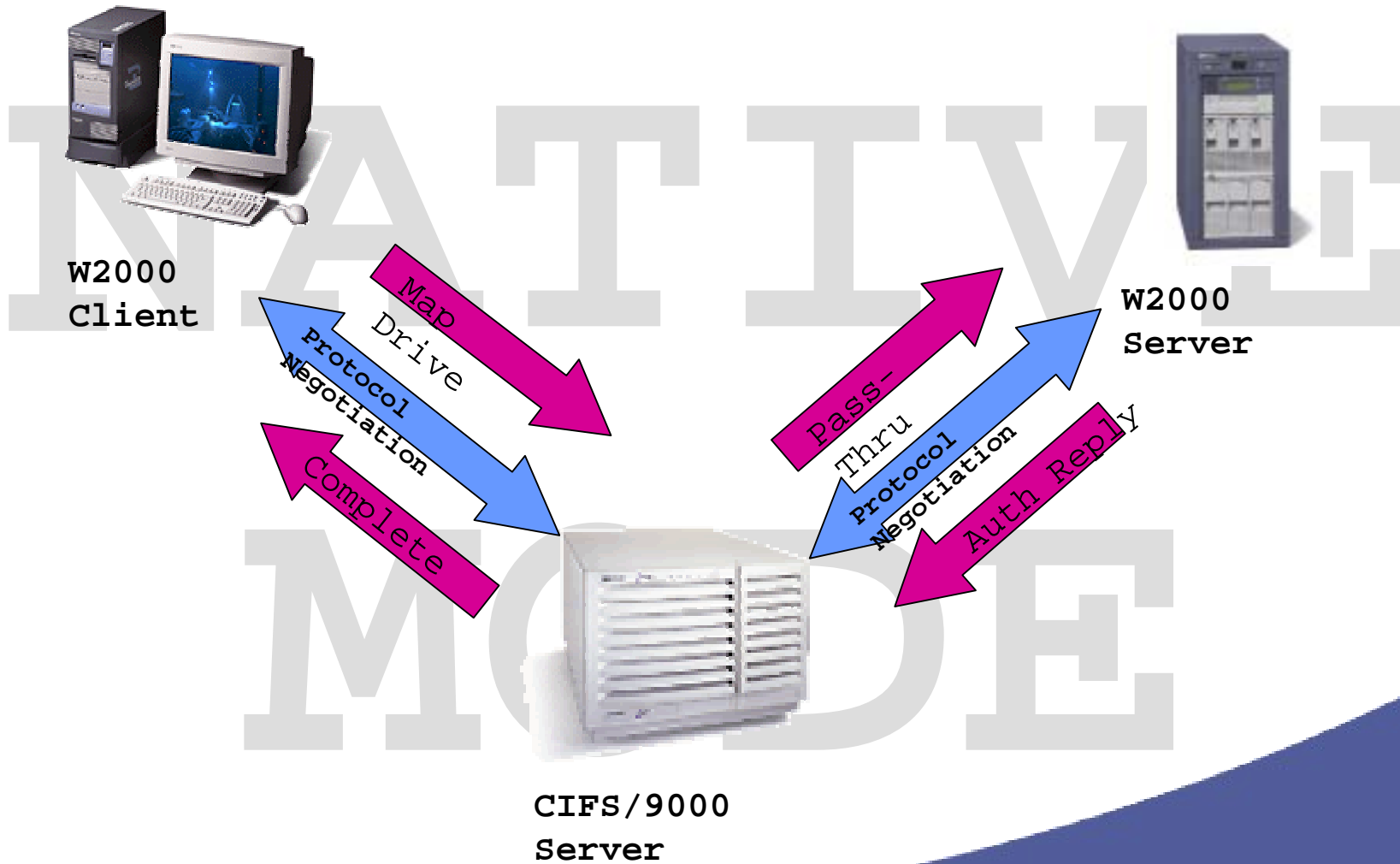
# Thru

Client to CIFS/9000 Server

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description	Src Other Addr	Dst Other Addr	Type
102	32.465712	EMONSTER	LOCAL	MBT	SS: Session Message Cont., 11 Bytes	EMONSTER	90887208ERIC	IP
103	32.465712	LOCAL	EMONSTER	TCP	...S., len: 0, seq:2176972608-217697260...	EMONSTER	90887208ERIC	IP
104	32.465712	LOCAL	EMONSTER	TCP	.A.S., len: 0, seq:1835371842-183537184...	EMONSTER	90887208ERIC	IP
105	32.465712	LOCAL	EMONSTER	TCP	.A...., len: 0, seq:2176972609-217697260...	EMONSTER	90887208ERIC	IP
106	32.465712	LOCAL	EMONSTER	MBT	SS: Session Request, Dest: EMONSTER	EMONSTER	90887208ERIC	IP
107	32.525797	EMONSTER	LOCAL	MBT	SS: Positive Session Response, Len: 0	EMONSTER	90887208ERIC	IP
108	32.525797	LOCAL	EMONSTER	SMB	C negotiate, Dialect = NT LM 0.12	EMONSTER	90887208ERIC	IP
109	32.525797	EMONSTER	LOCAL	SMB	S negotiate, Dialect # = 5	EMONSTER	90887208ERIC	IP
110	32.535811	LOCAL	EMONSTER	SMB	C session setup & X, Username = , and C tre...	EMONSTER	90887208ERIC	IP
111	32.545825	EMONSTER	LOCAL	SMB	R session setup & X, and R tree connect & X...	EMONSTER	90887208ERIC	IP
112	32.555839	EMONSTER	908872520LK	RRP	RRP_REQUEST	EMONSTER	908872520LK	IP
113	32.555839	908872520LK	LOCAL	RRP	RRP_RESPONSE	EMONSTER	90887208ERIC	IP
114	32.555839	LOCAL	EMONSTER	SMB	C session setup & X, Username = eroseme, an...	EMONSTER	90887208ERIC	IP
115	32.565853	908872520LK	EMONSTER	MBT	NS: Query (Node Status) resp. for DOH1	EMONSTER	908872520LK	IP
116	32.615924	EMONSTER	LOCAL	TCP	.A...., len: 0, seq:1835372018-183537201...	EMONSTER	90887208ERIC	IP
117	32.636234	EMONSTER	908872520LK	MBT	NS: Query req. for *SMBSERVER	EMONSTER	908872520LK	IP
118	32.636234	908872520LK	EMONSTER	MBT	NS: Query (Node Status) resp. for *SMBSERVE...	EMONSTER	908872520LK	IP
119	32.846248	EMONSTER	908872520LK	TCP	...S., len: 0, seq:1835661569-183566156...	EMONSTER	908872520LK	IP
120	32.846248	908872520LK	EMONSTER	TCP	.A.S., len: 0, seq:3986722425-398672242...	EMONSTER	908872520LK	IP
121	32.856262	EMONSTER	908872520LK	TCP	.A...., len: 0, seq:1835661564-183566156...	EMONSTER	908872520LK	IP
122	33.356967	EMONSTER	908872520LK	MBT	SS: Session Request, Dest: 908872520LK	EMONSTER	908872520LK	IP
123	33.356967	908872520LK	EMONSTER	MBT	SS: Positive Session Response, Len: 0	EMONSTER	908872520LK	IP
124	33.356967	EMONSTER	908872520LK	SMB	C negotiate, Dialect = NT LM 0.12	EMONSTER	908872520LK	IP
125	33.356967	908872520LK	EMONSTER	SMB	R negotiate, Dialect # = 7	EMONSTER	908872520LK	IP
126	33.356967	EMONSTER	908872520LK	SMB	C session setup & X, Username =	EMONSTER	908872520LK	IP
127	33.356967	908872520LK	EMONSTER	SMB	R session setup & X	EMONSTER	908872520LK	IP
128	33.356967	EMONSTER	908872520LK	SMB	C tree connect & X, Share = \908872520LK\IPC	EMONSTER	908872520LK	IP
129	33.356967	908872520LK	EMONSTER	SMB	R tree connect & X, type = IPC	EMONSTER	908872520LK	IP
130	33.356967	EMONSTER	908872520LK	SMB	C NT create & X, File = NETLOGON	EMONSTER	908872520LK	IP
131	33.356967	908872520LK	EMONSTER	SMB	R NT create & X, FID = 0x4000	EMONSTER	908872520LK	IP
132	33.356967	EMONSTER	908872520LK	MSRPC	c/o RPC Bind: UUID 12345678-1234-AB...	EMONSTER	908872520LK	IP
133	33.356967	908872520LK	EMONSTER	MSRPC	c/o RPC Bind Ack: call 0x1 assoc grp 0...	EMONSTER	908872520LK	IP
134	33.356967	EMONSTER	908872520LK	R_LOGON	RPC Client call logon:NetrServerReqChalleng...	EMONSTER	908872520LK	IP
135	33.356967	908872520LK	EMONSTER	R_LOGON	RPC Server response logon:NetrServerReqChal...	EMONSTER	908872520LK	IP
136	33.356967	EMONSTER	908872520LK	R_LOGON	RPC Client call logon:NetrServerAuthenticat...	EMONSTER	908872520LK	IP
137	33.366981	908872520LK	EMONSTER	R_LOGON	RPC Server response logon:NetrServerAuthent...	EMONSTER	908872520LK	IP
138	33.366981	EMONSTER	908872520LK	R_LOGON	RPC Client call logon:NetrLogonSamlogon(...)	EMONSTER	908872520LK	IP
139	33.366981	908872520LK	EMONSTER	R_LOGON	RPC Server response logon:NetrLogonSamlogon...	EMONSTER	908872520LK	IP
140	33.366981	EMONSTER	908872520LK	SMB	C close file, FID = 0x4000	EMONSTER	908872520LK	IP
141	33.366981	908872520LK	EMONSTER	SMB	R close file	EMONSTER	908872520LK	IP

CIFS/9000 server to W2000 DC

# W2000 Map CIFS Drive - NTLM



NATIVE SAME AS  
MIXED!

# W2000-CIFS/9000 Pass- Thru



Client to CIFS/9000 Server

CIFS/9000 Server to W2000 DC

Frame	Protocol	Description	Src Other Addr	Dst Other Addr	Type
13	NBT	SS: Session Request, Dest: RMONSTR	ros87208eric	emonster	IP
14	TCP	.A...., len: 0, seq:3528670546-352867054...	emonster	ros87208eric	IP
15	NBT	SS: Positive Session Response, Len: 0	emonster	ros87208eric	IP
16	SMB	C negotiate, Dialect = NT LM 0.12	ros87208eric	emonster	IP
17	SMB	R negotiate, Dialect # = 5	emonster	ros87208eric	IP
18	SMB	C session setup & X, Username = , and C tre...	ros87208eric	emonster	IP
19	SMB	R session setup & X, and R tree connect & X	emonster	ros87208eric	IP
20	UDP	Src Port: Unknown, (1735); Dst Port: Unknow...	ros87208eric	ROS872520LK	IP
21	UDP	Src Port: Unknown, (88); Dst Port: Unknown ...	ROS872520LK	ros87208eric	IP
22	SMB	C session setup & X, Username = eroseme, an...	ros87208eric	emonster	IP
23	NBT	NS: Query (Node Status) resp. for DOM1 ...	ROS872520LK	emonster	IP
24	TCP	.A...., len: 0, seq:3528670721-352867072...	emonster	ros87208eric	IP
25	NBT	NS: Query req. for *SMBSERVER	emonster	ROS872520LK	IP
26	NBT	NS: Query (Node Status) resp. for *SMBSERVE...	ROS872520LK	emonster	IP
27	TCP	....S., len: 0, seq:3528850667-352885066...	emonster	ROS872520LK	IP
28	TCP	.A..S., len: 0, seq:2128882014-212888201...	ROS872520LK	emonster	IP
29	TCP	.A...., len: 0, seq:3528850668-352885066...	emonster	ROS872520LK	IP
30	NBT	SS: Session Request, Dest: ROS872520LK ...	emonster	ROS872520LK	IP
31	NBT	SS: Positive Session Response, Len: 0	ROS872520LK	emonster	IP
32	SMB	C negotiate, Dialect = NT LM 0.12	emonster	ROS872520LK	IP
33	SMB	R negotiate, Dialect # = 7	ROS872520LK	emonster	IP
34	SMB	C session setup & X, Username =	emonster	ROS872520LK	IP
35	SMB	R session setup & X	ROS872520LK	emonster	IP
36	SMB	C tree connect & X, Share = \\ROS872520LK\IPC\$	emonster	ROS872520LK	IP
37	SMB	R tree connect & X, Type = IPC	ROS872520LK	emonster	IP
38	SMB	C NT create & X, File = NETLOGON	emonster	ROS872520LK	IP
39	SMB	R NT create & X, FID = 0x4000	ROS872520LK	emonster	IP

MIXED!  
NATIVE SAME AS


NBT Session protocol summary

F#: 13/87

Off: 54 (x36)

L: 72 (x48)

# Why NTLM?

- HP offers HPUX-ADS-Kerberos integration
- So why does CIFS/9000 pass through NTLM?
  
- Microsoft extends the Kerberos V5 Specification
  - PAC - Privilege Access Certificate
  - PAC contains Security Identifier(s) in Service Ticket 
  - Microsoft proprietary PAC encoding is licensed
- *Microsoft's Kerberos extension prevents CIFS (SMB) multi-vendor interoperability*
- When HP has legal access to PAC, then

# CIFS/9000



## Recommendation

- Clients Authenticate using Kerberos to KDC
  - Down-Level use NTLM
- CIFS/9000 Member Servers Pass-Thru NTLM
  - Mixed Mode
  - Native Mode
- Native Mode by itself does not affect CIFS/9000 Pass-Thru Authentication
- NetBIOS Enabled (see Name Address Resolution module)



# Agenda: CIFS/9000- W2000

- CIFS/9000 Overview
- W2000 Domain Mode: Mixed vs Native
- Authentication: Kerberos and NTLM
- **Active Directory  
Integration**
- W2000 Name Address Resolution
- W2000 DFS

# Windows 2000 Active



## Directory

➤ ADS is a colossal feature set

➤ ADS DESIGN is #1 priority

- Domain Design

- Schema Design

➤ Protocol is LDAP

- RFCs: 2251 - primary RFC, not strictly adhered to

- To READ/WRITE Account Data

➤ CIFS/9000 integration is about User and Group ACCOUNT DATA

- RFC: 2307 - POSIX Account Attributes



# Add CIFS/9000 Server to ADS



- On W2000 DC
  - AD Users and Computers
  - Select Computers - NEW
- "pre-Windows 2000"
  - Nest Everyone
  - No effect on Member Server
- Creates AD object for CIFS/9000 computer

A screenshot of the 'New Object - Computer' dialog box in Active Directory. The window title is 'New Object - Computer'. It shows the 'Create in' path as 'hpatc.hp.com/Computers'. The 'Computer name' field contains 'HPATCUX1', and the 'Computer name (pre-Windows 2000)' field also contains 'HPATCUX1'. Below these fields, it states 'The following user or group can join this computer to a domain.' and shows 'User or group: Default: Domain Admins' with a 'Change...' button. A checked checkbox is labeled 'Allow pre-Windows 2000 computers to use this account'. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

# CIFS/9000 – UNIX



## Accounts

- CIFS/9000 runs on HP-UX – UNIX Accounts
  - OS and Underlying file system know only UID/GID
  - Every user must have a UID
- UNIX Account Data base
  - User name, User ID, Group ID, password
    - Files (/etc/passwd, /etc/group, ...)
    - NIS (+)
    - LDAP Directory
- Windows client user maps to UNIX user
- UNIX UID/GID equated to Windows user – *file access*
- UID/GID on HP-UX POSIX ACL
  - JFS 3.3 or later File Layout v4 required



# CIFS Account Interoperability



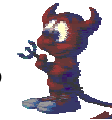
➤ Windows

➤ UNIX

- Users



- Users



- Groups



- Groups



**OR**

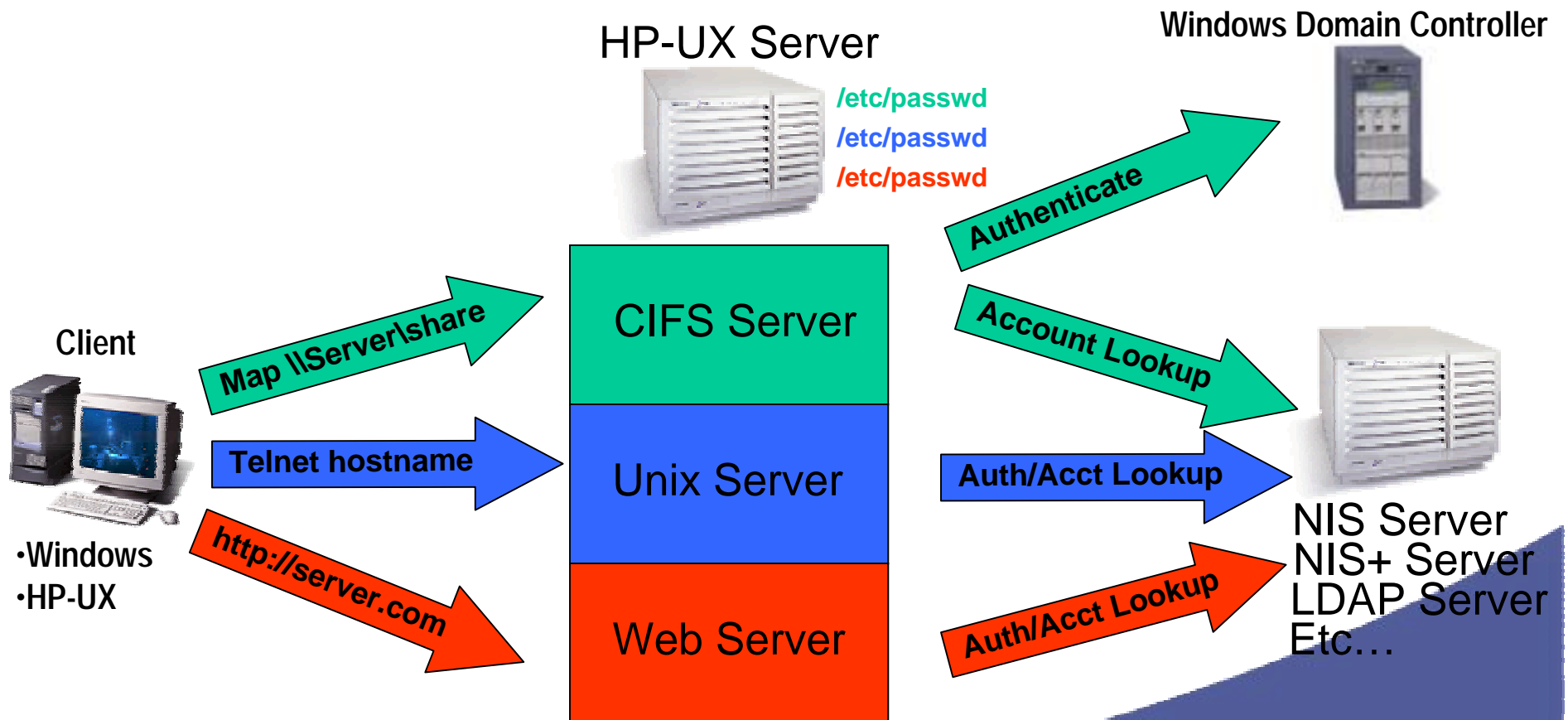


# Unified Login



- Store All User Account data in one location:
  - » ***Windows 2000 ADS***
- Windows and UNIX platforms now share common accounts on ADS
  - Single point of administration
  - Single username and password
- Use existing HP products to authenticate and access users on ADS
  - PAM\_KERBEROS (for HP-UX - NOT CIFS/9000)
  - LDAP\_UX Integration
  - CIFS/9000
- Benefits:
  - Cost savings - no dual admin
  - No synchronization - all account data in one location
  - No confusion - only one user/password

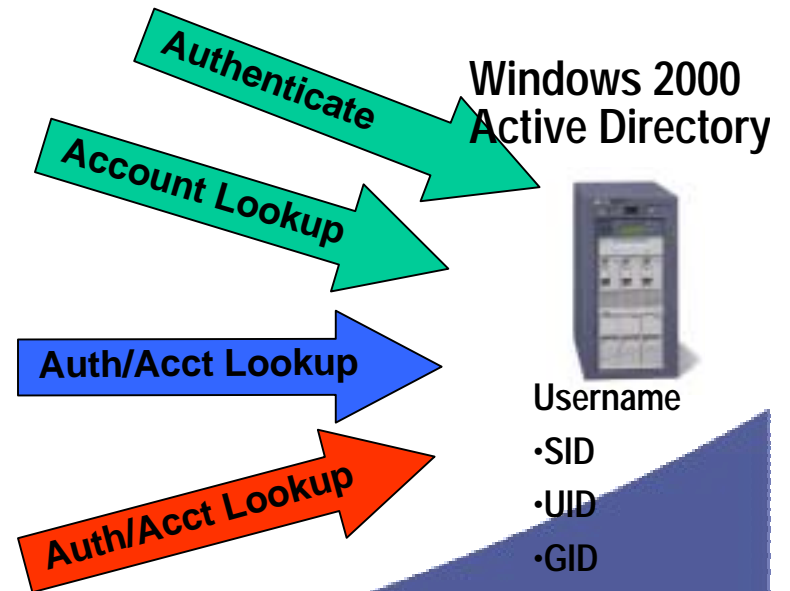
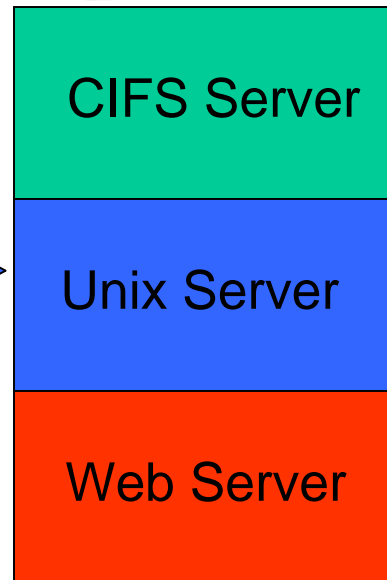
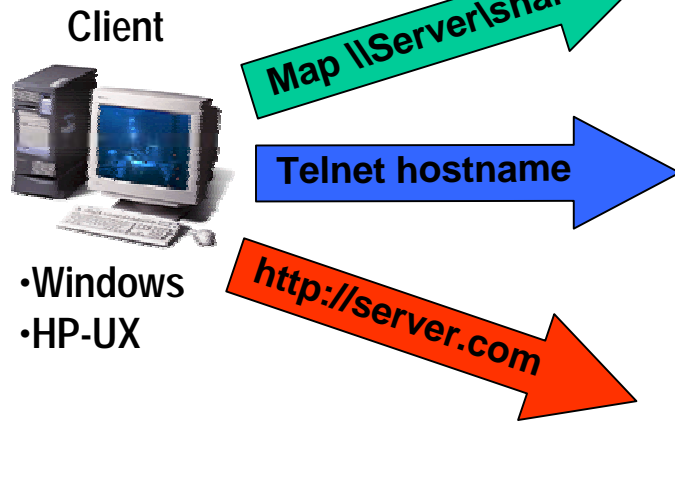
# Traditional Login Scenario



# Unified Login Scenario



HP-UX





# Unified Login Details

- No user accounts in /etc/passwd on HP-UX system
- No NIS(+) map
- NSS\_LDAP (nsswitch.conf) refers user/group lookup to W2000 ADS server using LDAP
- PAM\_KERBEROS (pam.conf) refers **HP-UX** authentication to W2000 KDC using Kerberos
- **ALL Authentication/Lookups on W2000 KDC/ADS**

# Setup and Configuration Steps



- Design Windows 2000 ADS Schema
  - Install and Configure W2000 Advanced Server ADS/KDC
  - Extend ADS Schema - one way - with MS SFU
  
- Relatively *Simple* and *Easy* **Unified Login** Configuration!
  
- nsswitch.conf - refer user/group lookups to W2000 ADS
  
- pam.conf - refer HP-UX authentication to W2000 KDC
  
- Run LDAP-UX Integration Migration scripts to Populate ADS with UNIX Account Data!
  - See "Unified Login" presentation for details



# W2000 User – Standard Schema



- Administrator User
- No UNIX Attributes tab
- No UNIX Attributes

The screenshot shows the 'Administrator Properties' dialog box with the following fields and values:

- Member Of:** Dial-in, Environment, Sessions
- Remote control:** Terminal Services Profile
- General:** Address, Account, Profile, Telephones, Organization
- Administrator:** (User icon)
- First name:** (Empty)
- Initials:** (Empty)
- Last name:** (Empty)
- Display name:** (Empty)
- Description:** Built-in account for administering the computer/doma
- Office:** (Empty)
- Telephone number:** (Empty) Other...
- E-mail:** (Empty)
- Web page:** (Empty) Other...
- Buttons:** OK, Cancel, Apply

# W2000 User - Extended Schema



Eric Roseme Properties

Published Certificates | Member Of | Dial-in | Object | Security | Environment  
General | Address | Account | Profile | Telephones | Organization  
Sessions | Remote control | Terminal Services Profile | UNIX Attributes

To enable access to this user for UNIX clients, you will have to specify the NIS domain this user belongs to.

NIS Domain:

UID:

Login Shell:

Home Directory:

Primary group name/GID:

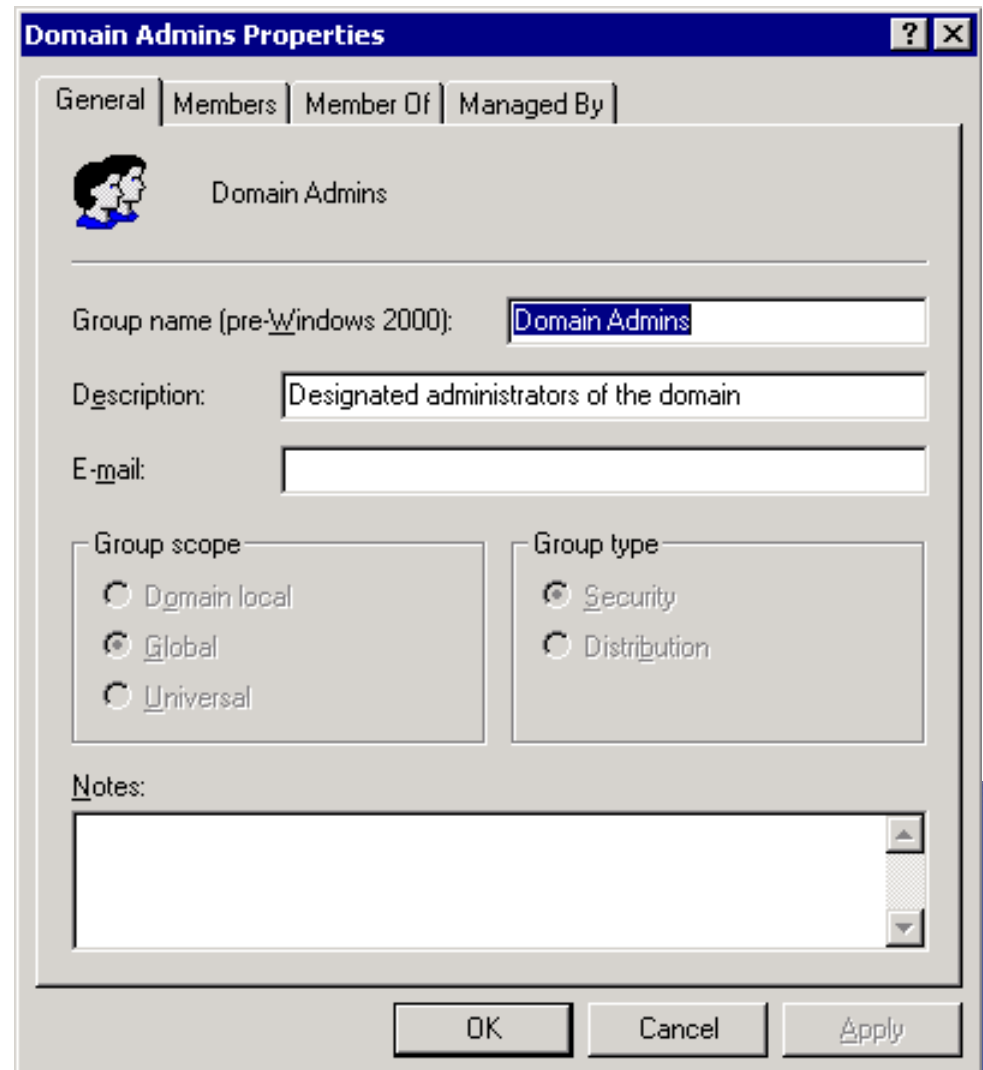
OK Cancel Apply

- Standard User
- UNIX Attributes tab
- UNIX UID Defined
- Login Shell
- UNIX Primary Group
  
- Combines Windows and UNIX user account attributes in User Object

# W2000 Group – Standard Schema



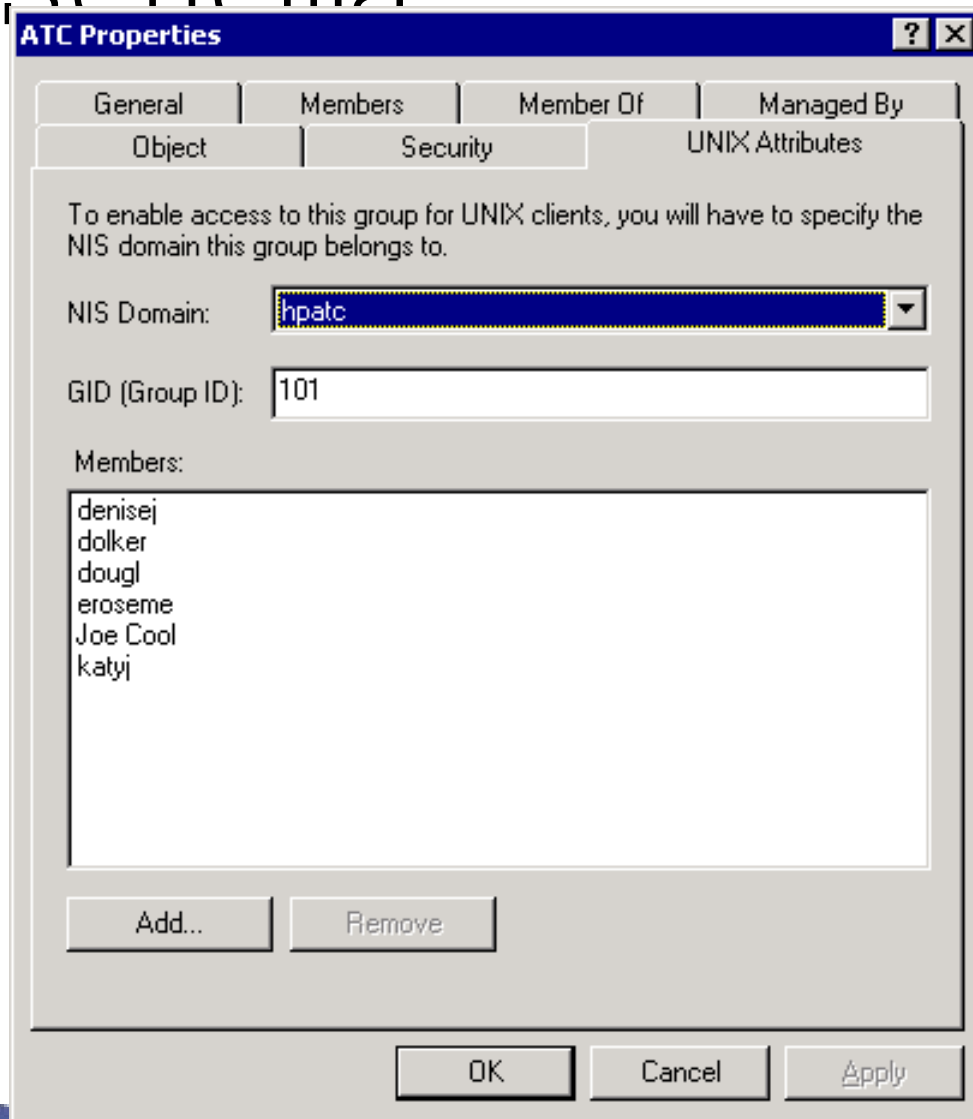
- Domain Admins group
- No UNIX Attribute tab
- No UNIX Attributes



# W2000 Group - Extended



## Schema



- Standard Group
- Unix Attributes tab
- UNIX GID Defined
- UNIX Users defined in group
- Combines Windows and UNIX Account Attributes in Group Object



# CIFS/9000 ACLs

- POSIX ACLs vs NTFS ACLs
- UNIX vs Windows
- UID/GID vs SID
- CIFS/9000 ACLs:
  - POSIX, UNIX, UID/GID
    - Based upon JFS 3.3 ACLs
    - Cannot place Windows SID on POSIX ACL
- Workaround: Map Windows users to UNIX



# ADS Integration Issues

- ACL Management from W2000 Client
  - JAG ad50847
  - Explorer Aborts When Attempting ACL Management
  - Workaround: Manage ACLs from NT4 Client
- Unified Login UNIX Group Management
  - W 2000 Admin Tools Adds Distinguished Name to UNIX Groups
  - Should Add the UNIX UserName to the Group
  - Investigating Better Admin Tools
  - Have Notified Microsoft about the Problem

# CIFS/9000



## Recommendation

### ➤ Unified Login

- Single Point of Administration
- Integration of W2000 and UNIX Account Data
- Relatively Easy to Set Up
  - Step-By-Step Instructions
- Known Problems, Additional Testing Planned

### ➤ Standard UNIX Account Administration

- /etc/passwd, NIS(+), LDAP

Reliable, But Requires Dual



# Agenda: CIFS/9000- W2000

- CIFS/9000 Overview
- W2000 Domain Mode: Mixed vs Native
- Authentication: Kerberos and NTLM
- Active Directory Integration
- **W2000 Name Address  
Resolution**
- W2000 DFS



# W2000 Name Address Resolution



- NetBIOS/WINS: NT4 and CIFS/9000
- BIND – UNIX DNS
- Windows 2000 DNS
  - Resolve and Update Names
  - Schema for Data Storage
  - Replicate the Data

# NetBIOS: NT4 and CIFS/9000



## ➤ NetBIOS

- NT4 (and prior) Name Resolution Protocol
- RFCs 1001 (protocol) and 1002 (structures)

## ➤ **CIFS/9000 REQUIRES NetBIOS**

## ➤ CIFS/9000 NetBIOS Name = HP-UX Hostname

- NetBIOS name length =< 15 Characters
  - 16<sup>th</sup> char is the name suffix

- **HP-UX uname =< 8 Characters**

## ➤ Single CIFS/9000 nmbd daemon listens for NetBIOS

## ➤ W2000 Default is: NetBIOS Enabled





# NetBIOS - WINS

- WINS - (Windows Internet Name Service)
  - NetBIOS uses WINS
  - NT4 Domain Name Service - multi subnet
  - H-Node NetBIOS: try WINS first, then Broadcast name
- CIFS/9000 WINS
  - Best to use W2000 WINS server (enhanced NT4)
  - W2000 Clients more WINS flexible
- Configure Primary WINS server in smb.conf
  - Secondary WINS Server enhancement coming

# BIND – UNIX DNS



- Berkeley Internet Name Domain
- RFCs 1034 (DNS Database format) and 1035 (Domain Name structure)
- <http://www.isc.org/products/BIND/>
- Hierarchical Namespace
  - Much more powerful and flexible than NetBIOS
- Hooks in Samba to Integrate WINS and DNS
  - See Recommendations

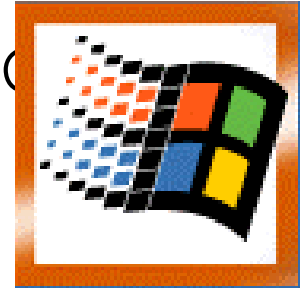


# BIND – HP-UX DNS

- HP-UX 11 Delivered with 4.9.7 –  
UPGRADE IT!
  
- HP-UX 11 DNS – [www.software.hp.com](http://www.software.hp.com)
  - BIND 8.1.2 (upgrade)
    - DNS Notify (RFC 1996)
    - DDNS Support (RFC 2136)
    - SRV Record Support (RFC 2052 → 2782)
  - BIND v9 (upgrade)
    - Incremental Zone Transfer (RFC 1995)
    - DNSSEC (DNS Security – authentication RFC 2535)

# Windows 2000 DNS

- "DDNS" - Dynamic DNS (tied to DHCP)
- Replaces NT4 NetBIOS-WINS
- Default Name Resolution - DDNS
- Microsoft Recommends WINS Compatibility
  - Default: WINS Enabled
  - Many applications need WINS, even in pure W2000 domain
- Pure W2000 Domains can Disable WINS-NetBIOS
  - Even Microsoft recommends WINS-NetBIOS Enabled

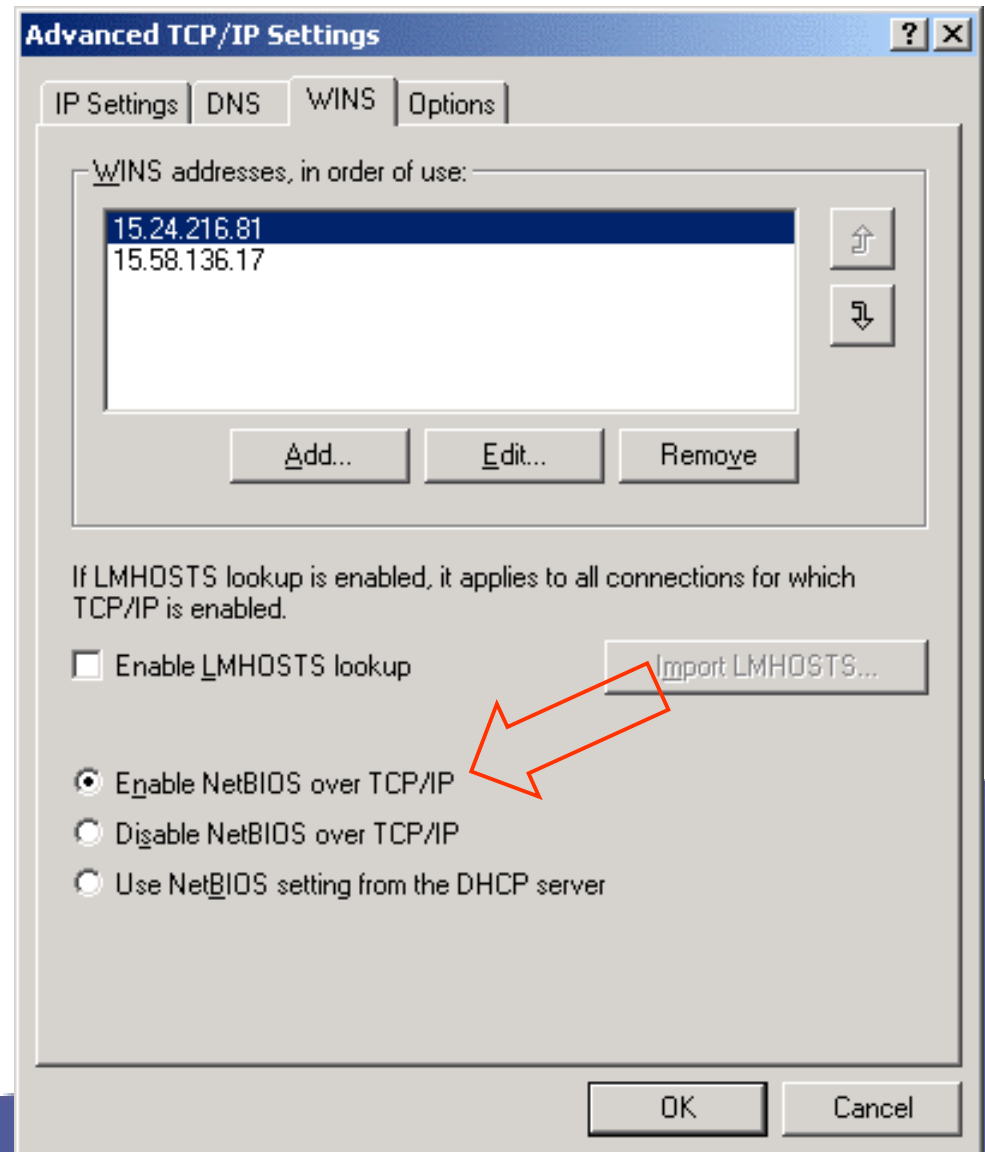


➤ **CIFS/9000 Uses NetBIOS**

# W2000 and NetBIOS-WINS



- Default - Enabled
- Disable - you better be sure
- CIFS/9000 - DO NOT DISABLE
  - Unless you're really smart
  - See Recommendations Module



# W2000 DDNS Feature List



- ADS Integration
- Secure Dynamic Update (RFC 2136 + Draft)
- Incremental Zone Transfer (RFC 1995)
- DNS Notify (RFC 1996)
- Service Location (RFC 2052 → 2782)
- Enhanced Cache Resolver (RFC 2308)
- Enhanced DNS Manager
- Unicode Character Support (Draft UTF-8)
  - Plus 3 other drafts (in other words, non-standard)





# DNS RFC Matrix

RFC	W2000	BIND	BIND v9
1995 Incremental Zone Transfer	Yes	8.1.2 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

\* IPV6

DNSSEC

# MS W2000



## Recommendations

### ➤ For UNIX BIND Interoperability

- Minimum level of 8.1.2

  - Support SRV Records (2052 → 2782)

  - Incremental Zone Transfer (1995)

- 8.2.2 is best - W2000 equivalent

- Position on v9 not known

### ➤ Applies to DNS Server Interoperability

### ➤ Do you have UNIX BIND in your enterprise?

# CIFS/9000



## Recommendations

➤ DNS: critical component of W2000

### ADS Design

- Design ADS-DNS together

➤ CIFS/9000-HPUX: Implies existing UNIX DNS

- Then create separate namespace for W2000 DDNS

➤ With NetBIOS-WINS ENABLED, DDNS-BIND integration is less of an issue!

- CIFS/9000 Interoperability is **TRANSPARENT!**



# CIFS/9000 Recommendations

W2000  
Client



W2000  
Server



FIND DC - W2000 DDNS

FIND CIFS/9000 - W2000  
DDNS

Find DC - NetBIOS/WINS

CIFS/9000  
Server



# CIFS/9000



## Recommendations

➤ Names - Follow RFC 952: A-Z, a-z, 0-9,

-

- HP-UX Node Name

- 8 Chars

- NetBIOS Name

- 15 Chars (16<sup>th</sup> char is reserved for the name suffix type)
- RFC 952 Plus: !@#\$%^&'().-\_{ } ~ space

- DNS

- 24 Chars
- RFC 952

- DDNS

- 63 Chars
- RFC 952 + RFC 2181 + UTF-8

➤ HP-UX Node name = NetBIOS name = DNS

# CIFS/9000



## Recommendations

### ➤ Zone Transfers - WINS

- W2000 Zone Transfers contain WINS Records
- BIND Does Not Recognize WINS Records
- Do Not Transfer W2000 Zone to BIND Secondary
- Do Not Transfer UTF-8 Records to BIND Secondary

### ➤ W2000 Global Catalog Server: `_msdcs` Subzone

- Hosts located in `_msdcs` subzone have illegal DNS names
  - `Hostname._msdcs.hp.com`
  - `"_"` is not a legal RFC 952 character



# Agenda: CIFS/9000- W2000

- CIFS/9000 Overview
- W2000 Domain Mode: Mixed vs Native
- Authentication: Kerberos and NTLM
- Active Directory Integration
- W2000 Name Address Resolution
- **W2000 DFS**



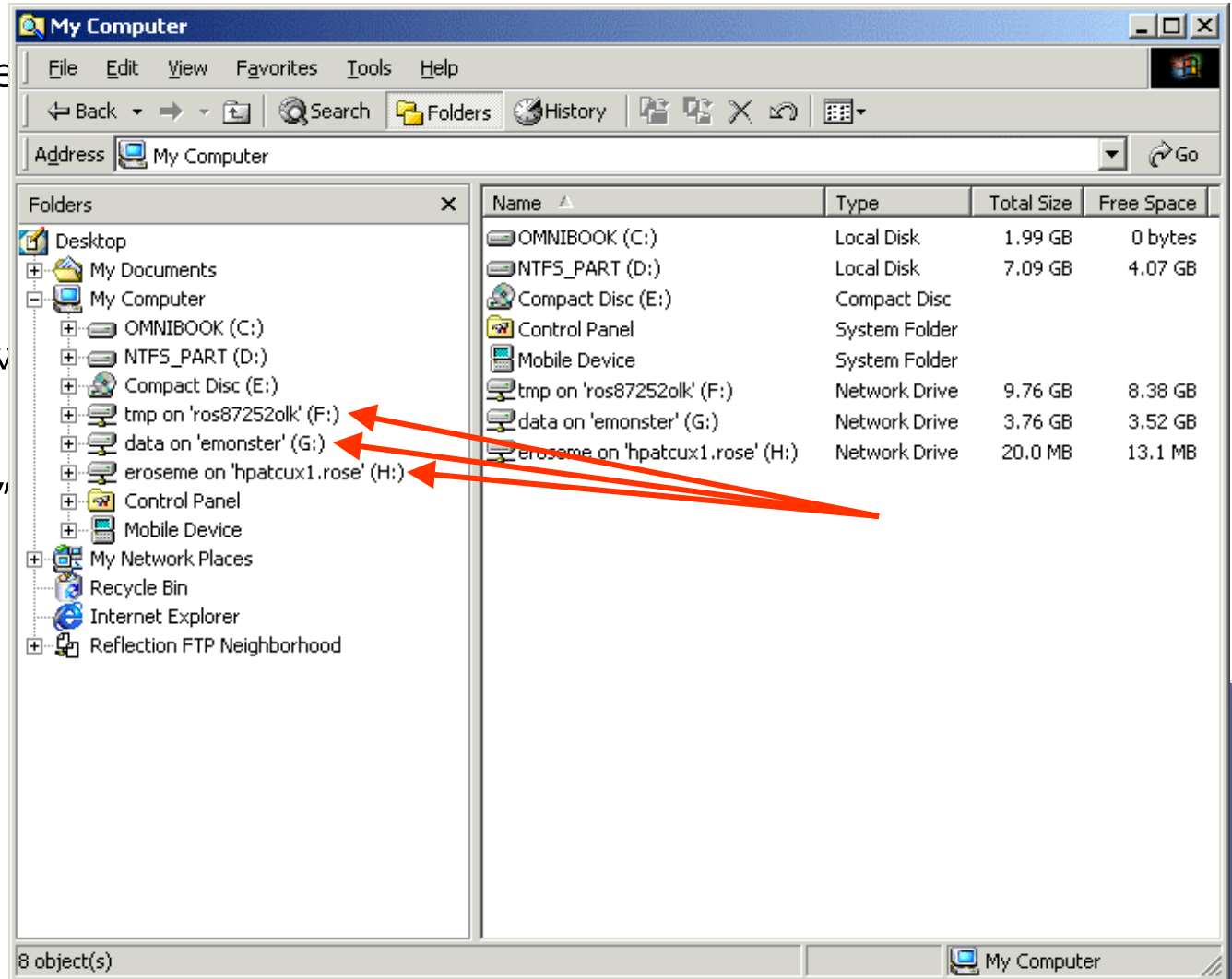
# What is W2000 DFS?

- DFS: Multiple Servers → Common Namespace
- NOT!: TransArc DFS
- Referrals
  - Transparent share mapping
  - Map "Root" share - source of common namespace
  - Root subordinate server mappings are "referred"
    - Referral is simply a re-directed share map to another server, but appears as a local directory
- W2000 DFS Features

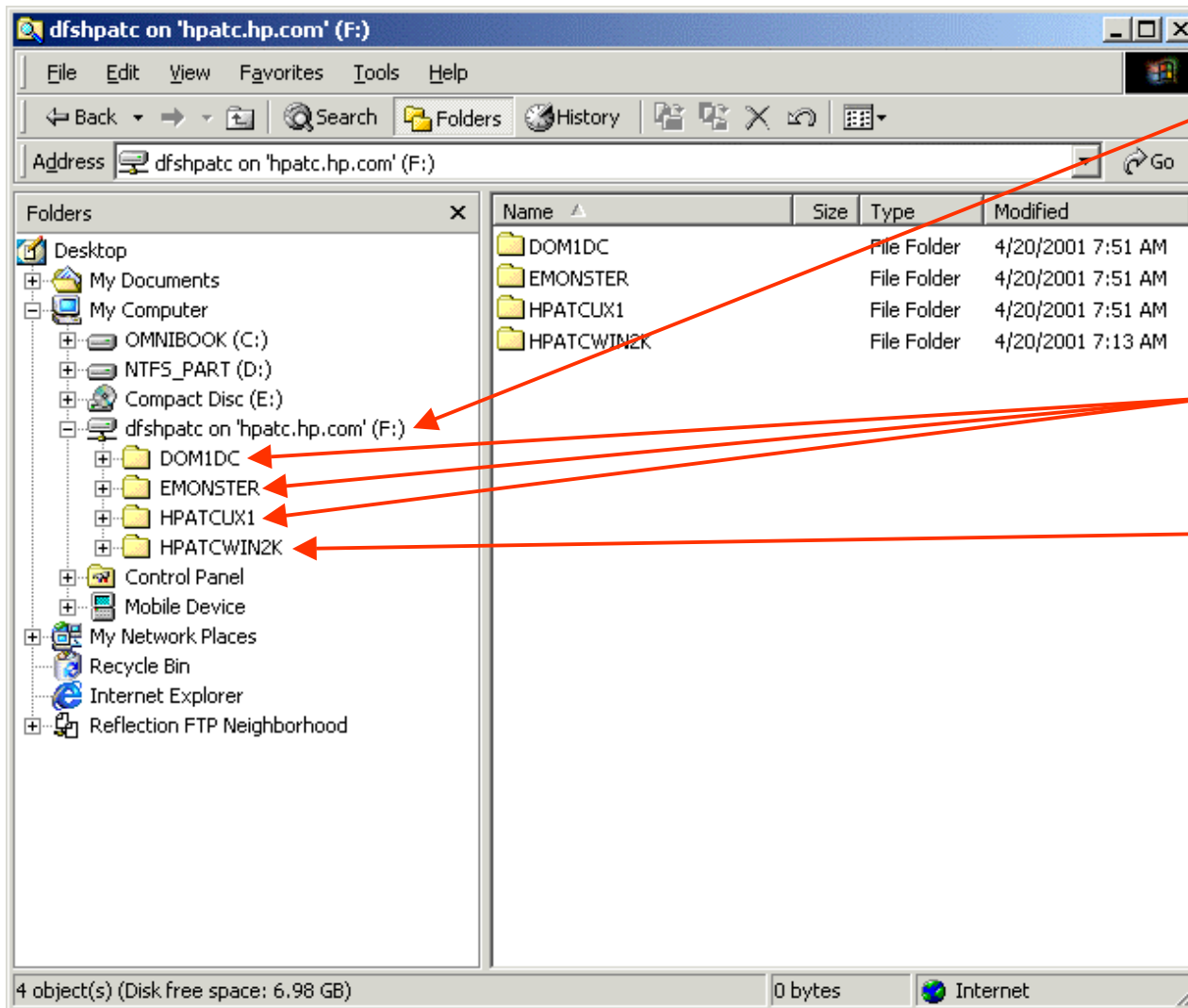


# Standard Namespace

- 3 Mapped Shares
- 3 Servers
- 3 Logical Drives
- 3 "Namespaces"



# Single DFS Namespace



- Single Root Share
- Single Namespace - dfshpatc
- 3 Remote Servers
- 1 Local Filesystem - Local to the root
- Namespace exported to any client

# DFS Design

- DFS Referral protocol in CIFS Specification
- 2 New DFS SMBs
  - Trans2\_get\_dfs\_referral
  - Trans2\_report\_dfs\_inconsistency
- Referral Exchange Occurs on DFS Root Only
  
- File Server (DFSLink): Just Another Connection
- CIFS/9000: Ordinary Connect Protocol
- UNC Names (Universal Naming Convention)
  - \\namespace\share

# W2000 DFS Referral



W2000  
Client



W2000  
Server

Map Root  
Share

Query for DFSLink

Path Not Covered

Get Referral

Referral Response

Map  
Drive  
Protocol  
Negotiation  
Complete



CIFS/9000  
Server

Pass-  
Thru  
Protocol  
Negotiation  
Auth Reply



# DFS Query



Microsoft Network Monitor - [D:\data\eric\ATC\CIFS\Presentation\Interworks\_2001\dfs\_client\_interworks.cap (Summary)]

File Edit Display Tools Options Window Help

F...	Prot...	Description	Src Other ...	Dst Other ...	Type Other...
160	SMB	C transact2 Query path info, File = \...	ROS87208ERIC	hpatcwin2k	IP
161	SMB	R transact2 - NT error, System, Error...	hpatcwin2k	ROS87208ERIC	IP
162	SMB	C transact2 NT Get DFS Referral	ROS87208ERIC	hpatcwin2k	IP
163	SMB	R transact2 NT Get DFS Referral (resp...	hpatcwin2k	ROS87208ERIC	IP
164	ICMP	Echo: From 15.32.72.207 To 15.32.72.208	ROS87208ERIC	EMONSTER	IP
165	ICMP	Echo Reply: To 15.32.72.207 From 15.3...	EMONSTER	ROS87208ERIC	IP
166	TCP	....S., len: 0, seq:1669214552-166...	ROS87208ERIC	EMONSTER	IP
167	NBT	SS: Session Message Cont., 11 Bytes	EMONSTER	ROS87208ERIC	IP
168	TCP	....S., len: 0, seq:1669254015-166...	ROS87208ERIC	EMONSTER	IP
169	TCP	.A.S., len: 0, seq:2746822633-274...	EMONSTER	ROS87208ERIC	IP
170	TCP	.A...., len: 0, seq:1669254016-166...	ROS87208ERIC	EMONSTER	IP
171	NBT	SS: Session Request, Dest: EMONSTER ...	ROS87208ERIC	EMONSTER	IP
172	TCP	.A...., len: 0, seq:2746822634-274...	EMONSTER	ROS87208ERIC	IP
173	TCP	.A...., len: 0, seq:1663089556-166...	ROS87208ERIC	hpatcwin2k	IP
174	NBT	SS: Positive Session Response, Len: 0	EMONSTER	ROS87208ERIC	IP

Frame: Base frame properties

- ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
- IP: ID = 0x3B7E; Proto = TCP; Len: 178
- TCP: .AP..., len: 138, seq:1663089284-1663089422, ack:1856299905, win:16257, src: 1744, dst: 139 (NBT Session)
- NBT: SS: Session Message, Len: 134
- SMB: C transact2 Query path info, File = \Hpatcwin2k\DFSHPATC\EMONSTER

Server Message Block (SMB) F#: 160/344 Off: 58 (x3A) L: 134 (x86)

The client queries the DFS root server for the sharename that actually resides on a CIFS/9000 server

# DFS Query:



## status path not covered

Microsoft Network Monitor - [D:\data\ericR\ATC\CIFS\Presentation\Interworks\_2001\dfs\_client\_interworks.cap (Summary)]

F...	Prot...	Description	Src Other ...	Dst Other ...	Type Other...
160	SMB	C transact2 Query path info, File = \...	ROS87208ERIC	hpatcwin2k	IP
161	SMB	R transact2 - NT error, System, Error...	hpatcwin2k	ROS87208ERIC	IP
162	SMB	C transact2 NT Get DFS Referral	ROS87208ERIC	hpatcwin2k	IP
163	SMB	R transact2 NT Get DFS Referral (resp...	hpatcwin2k	ROS87208ERIC	IP
164	ICMP	Echo: From 15.32.72.207 To 15.32.72.208	ROS87208ERIC	EMONSTER	IP
165	ICMP	Echo Reply: To 15.32.72.207 From 15.3...	EMONSTER	ROS87208ERIC	IP
166	TCP	....S., len: 0, seq:1669214552-166...	ROS87208ERIC	EMONSTER	IP
167	NBT	SS: Session Message Cont., 11 Bytes	EMONSTER	ROS87208ERIC	IP
168	TCP	....S., len: 0, seq:1669254015-166...	ROS87208ERIC	EMONSTER	IP
169	TCP	.A..S., len: 0, seq:2746822633-274...	EMONSTER	ROS87208ERIC	IP
170	TCP	.A...., len: 0, seq:1669254016-166...	ROS87208ERIC	EMONSTER	IP
171	NBT	SS: Session Request, Dest: EMONSTER ...	ROS87208ERIC	EMONSTER	IP
172	TCP	.A...., len: 0, seq:2746822634-274...	EMONSTER	ROS87208ERIC	IP
173	TCP	.A...., len: 0, seq:1663089556-166...	ROS87208ERIC	hpatcwin2k	IP
174	NBT	SS: Positive Session Response, Len: 0	EMONSTER	ROS87208ERIC	IP

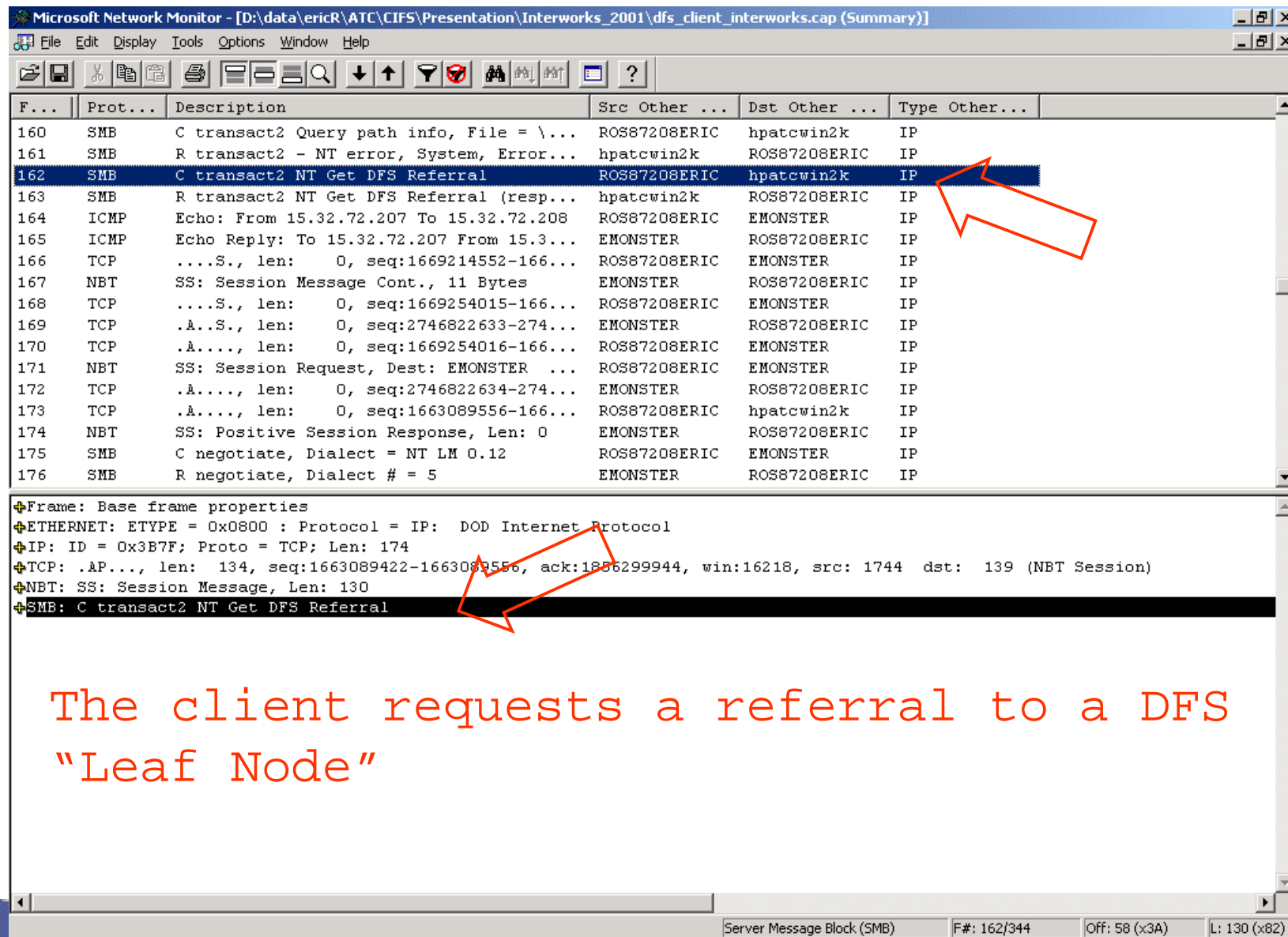
Frame: Base frame properties

- ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
- IP: ID = 0xDED1; Proto = TCP; Len: 79
- TCP: .AP..., len: 39, seq:1856299905-1856299944, ack:1663089422, win:17238, src: 139 (NBT Session) dst: 1744
- NBT: SS: Session Message, Len: 35
- SMB: R transact2 - NT error, System, Error, Code = (599) STATUS PATH NOT COVERED

Server Message Block (SMB) F#: 161/344 Off: 58 (x3A) L: 35 (x23)

The DFS root server replies that path is not found on the local server file system

# DFS Referral Request



F...	Prot...	Description	Src Other ...	Dst Other ...	Type Other...
160	SMB	C transact2 Query path info, File = \...	ROS87208ERIC	hpatcwin2k	IP
161	SMB	R transact2 - NT error, System, Error...	hpatcwin2k	ROS87208ERIC	IP
162	SMB	C transact2 NT Get DFS Referral	ROS87208ERIC	hpatcwin2k	IP
163	SMB	R transact2 NT Get DFS Referral (resp...	hpatcwin2k	ROS87208ERIC	IP
164	ICMP	Echo: From 15.32.72.207 To 15.32.72.208	ROS87208ERIC	EMONSTER	IP
165	ICMP	Echo Reply: To 15.32.72.207 From 15.3...	EMONSTER	ROS87208ERIC	IP
166	TCP	....S., len: 0, seq:1669214552-166...	ROS87208ERIC	EMONSTER	IP
167	NBT	SS: Session Message Cont., 11 Bytes	EMONSTER	ROS87208ERIC	IP
168	TCP	....S., len: 0, seq:1669254015-166...	ROS87208ERIC	EMONSTER	IP
169	TCP	.A..S., len: 0, seq:2746822633-274...	EMONSTER	ROS87208ERIC	IP
170	TCP	.A...., len: 0, seq:1669254016-166...	ROS87208ERIC	EMONSTER	IP
171	NBT	SS: Session Request, Dest: EMONSTER ...	ROS87208ERIC	EMONSTER	IP
172	TCP	.A...., len: 0, seq:2746822634-274...	EMONSTER	ROS87208ERIC	IP
173	TCP	.A...., len: 0, seq:1663089556-166...	ROS87208ERIC	hpatcwin2k	IP
174	NBT	SS: Positive Session Response, Len: 0	EMONSTER	ROS87208ERIC	IP
175	SMB	C negotiate, Dialect = NT LM 0.12	ROS87208ERIC	EMONSTER	IP
176	SMB	R negotiate, Dialect # = 5	EMONSTER	ROS87208ERIC	IP

Frame: Base frame properties  
ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol  
IP: ID = 0x3B7F; Proto = TCP; Len: 174  
TCP: .A...., len: 134, seq:1663089422-1663089556, ack:1886299944, win:16218, src: 1744 dst: 139 (NBT Session)  
NBT: SS: Session Message, Len: 130  
SMB: C transact2 NT Get DFS Referral

Server Message Block (SMB) F#: 162/344 Off: 58 (x3A) L: 130 (x82)

The client requests a referral to a DFS "Leaf Node"

# DFS Referral Reply



Microsoft Network Monitor - [D:\data\ericR\ATC\CIFS\Presentation\Interworks\_2001\dfs\_client\_interworks.cap (Detail)]

File Edit Display Tools Options Window Help

F...	Prot...	Description	Src Other ...	Dst Other ...	Type Other...
160	SMB	C transact2 Query path info, File = \...	ROS87208ERIC	hpatcwin2k	IP
161	SMB	R transact2 - NT error, System, Error...	hpatcwin2k	ROS87208ERIC	IP
162	SMB	C transact2 NT Get DFS Referral	ROS87208ERIC	hpatcwin2k	IP
163	SMB	R transact2 NT Get DFS Referral (resp...	hpatcwin2k	ROS87208ERIC	IP
164	ICMP	Echo: From 15.32.72.207 To 15.32.72.208	ROS87208ERIC	EMONSTER	IP
165	ICMP	Echo Reply: To 15.32.72.207 From 15.3...	EMONSTER	ROS87208ERIC	IP
166	TCP	....S., len: 0, seq:1669214552-166...	ROS87208ERIC	EMONSTER	IP
167	NBT	SS: Session Message Cont., 11 Bytes	EMONSTER	ROS87208ERIC	IP
168	TCP	....S., len: 0, seq:1669254015-166...	ROS87208ERIC	EMONSTER	IP
169	TCP	.A..S., len: 0, seq:2746822633-274...	EMONSTER	ROS87208ERIC	IP
170	TCP	.A...., len: 0, seq:1669254016-166...	ROS87208ERIC	EMONSTER	IP
171	NBT	SS: Session Request, Dest: EMONSTER ...	ROS87208ERIC	EMONSTER	IP
172	TCP	.A...., len: 0, seq:2746822634-274...	EMONSTER	ROS87208ERIC	IP
173	TCP	.A...., len: 0, seq:1663089556-166...	ROS87208ERIC	hpatcwin2k	IP
174	NBT	SS: Positive Session Response, Len: 0	EMONSTER	ROS87208ERIC	IP
175	SMB	C negotiate, Dialect = NT LM 0.12	ROS87208ERIC	EMONSTER	IP
176	SMB	R negotiate, Dialect # = 5	EMONSTER	ROS87208ERIC	IP

SMB: Parameter Displacement = 0 (0x0)  
SMB: Data bytes = 192 (0xC0)  
SMB: Data offset = 56 (0x38)  
SMB: Data Displacement = 0 (0x0)  
SMB: Max setup words = 0  
SMB: Byte count = 193  
SMB: Byte parameters  
-SMB: Transaction data  
SMB: DFS Path Consumed = 58 (0x3A)  
SMB: DFS Number of Referrals = 1 (0x1)  
+SMB: DFS Server Function = 2 (0x2)  
-SMB: DFS Version 3 Referral  
SMB: DFS Version Number = 3 (0x3)  
SMB: DFS Server Type = Unknown Server Type  
SMB: DFS TimeToLive = 1800 (0x708)  
SMB: DFS Filename = \Hpatcwin2k\DFSHPATC\EMONSTER  
SMB: DFS 8.3 Filename = \Hpatcwin2k\DFSHPATC\EMONSTER  
SMB: DFS Sharename = \Emonster\data  
SMB: DFS Servicesite GUID = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Server Message Block (SMB) F#: 163/344 Off: 58 (x3A) L: 248 (xF8)

The DFS Root server replies with the CIFS/9000 server and share name





# W2000 DFS Features

- Standalone DFS Root Server
  - Not integrated into ADS
  
- ADS Integrated DFS Root Server - you get:
  - DFS Data Stored in ADS
  - Automatic File Replication Between Root/Leaf Servers
  - Fault Tolerance for Root/Leaf Servers
  - Preferential Replica Selection (best failover choice)

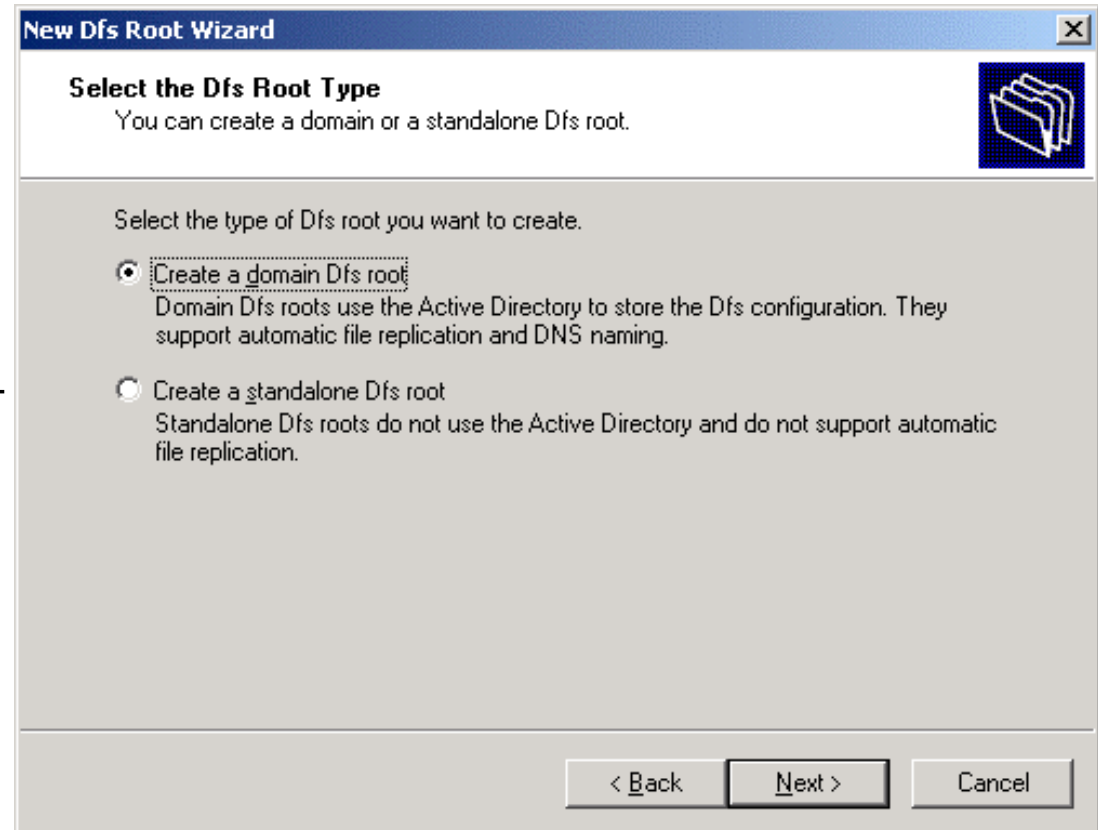
# DFS ADS Configuration

## ➤ ADS Config

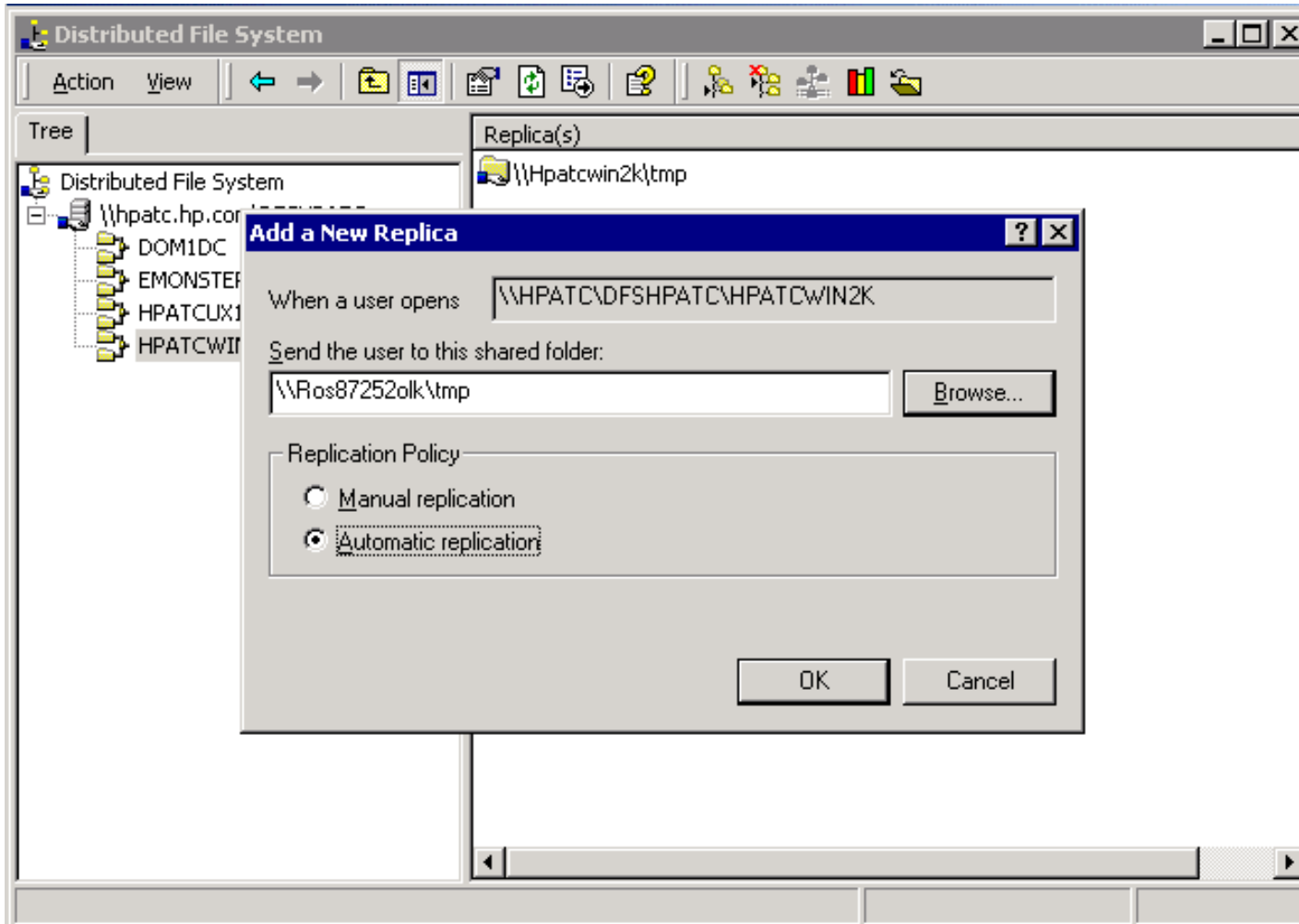
- Fault Tolerance
- Replication
- Prioritization

## ➤ Standalone

- DFSLinks are still fault tolerant



# DFS Automatic File Replication



- Needs NTFS
- Forwards referral when link is down



# W2000 DFS Details

- One DFS Root per DC
- 32 DCs can Host the Same DFS Root in Domain
- Unlimited DFS Roots (Oops - 1 per DC)
- Replication (Root/Leaf) requires NTFS 5.0
- DFSLinks (Leafs) on any UNC Path
  - Universal Naming Convention:  
\\Server\Share
- DFS Administration Tool on Server

# CIFS/9000



## Recommendations

- DFSLink (Leaf Node) Only
  - Consistent with Member Server Status
  - DC ADS Required for Node Mgt - Root-Enabled
- Domain Roots are Fault Tolerant
- CIFS/9000 DFSLinks Cannot Automatically Replicate
- CIFS/9000 DFSLinks ARE Fault Tolerant
  - Down Link will forward to Configured Replicant
  - Use Manual Replication, OR
  - Devise alternate automatic replicating mechanism
  - Can configure to replicate - enables



# Agenda: CIFS/9000- W2000

- CIFS/9000 Overview
- W2000 Domain Mode: Mixed vs Native
- Authentication: Kerberos and NTLM
- Active Directory Integration
- W2000 Name Address Resolution
- W2000 DFS
- Summary



# Summary

- W2000 Native Mode vs Mixed Mode
  - CIFS/9000 Member Server Okay in Either
  - Native Mode is One-Way
- Kerberos vs NTLM
  - Client Kerberos W2000 Domain Login
  - CIFS/9000 NTLM Pass-Thru Authentication
    - HP is active in providing full Kerberos
      - stay tuned
- Active Directory Integration
  - Store all W2000 and HP-UX Account Data in ADS

# Summary

## ➤ Name Address Resolution

- HP-UX Nodename = NetBIOS Name = DNS Name
- No W2000 Zone Transfers to BIND
- \_msdcs Subzone Name is BIND Illegal

## ➤ Windows 2000 DFS

- CIFS/9000 Leaf Node Only
- CIFS/9000 can be Fault Tolerant



# Appendix

➤ A: UPN Name



# UPN Name

## ➤ Windows 2000 Logon Names

### - SAM Logon

- Security Account Manager - NT4 style logon

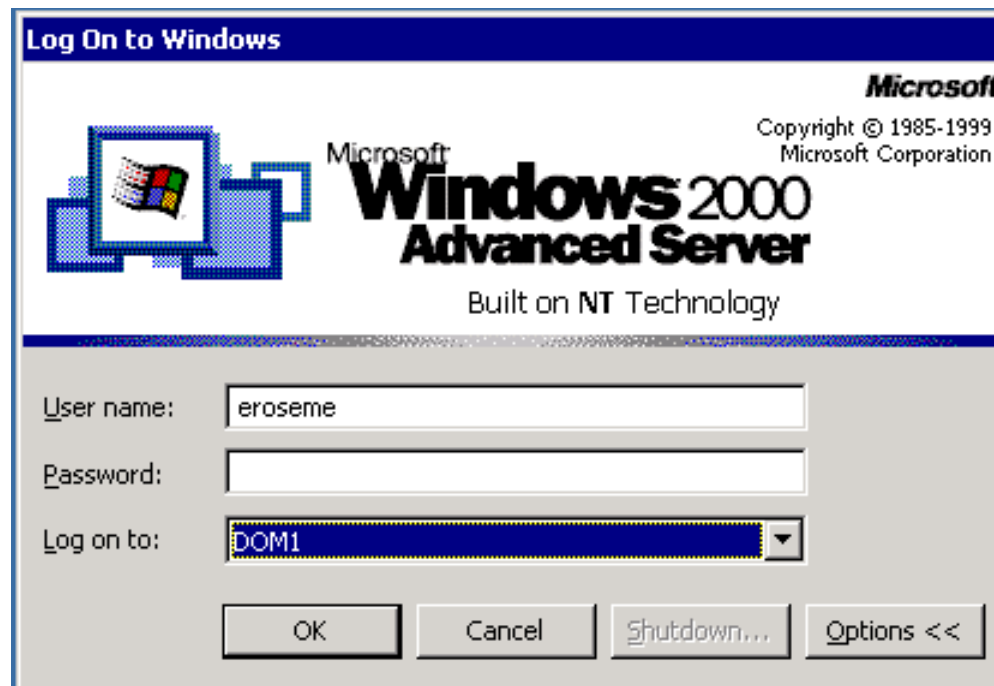
### - FQDN Logon

- Fully Qualified Domain Name - user + "@"

### - UPN Logon

- User + "@"
- Configurable full name
- Resolved by DC lookup in Global Catalog

# SAM Logon Name



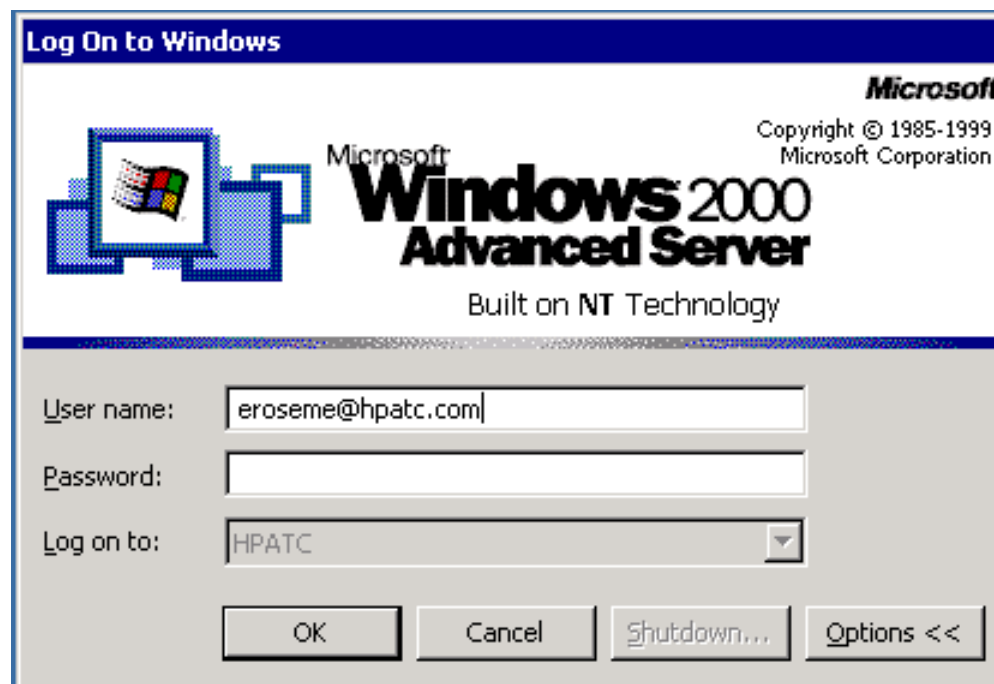
- User chooses domain from pull-down list

# FQDN Logon Name



- User enters @ plus fully qualified domain name
- SAM logon gets grayed out when @ is entered

# UPN Logon Name



- User enters @ plus configured logon name
- SAM logon gets grayed out when @ is entered

# User Principal Name Benefits



- User in subdomain can be generic
  - `eroseme@dom1.hpatc.com` can be configured as
  - `eroseme@hpatc.com`
- User can now be moved through subdomains transparently without having to change FQDN logons
- UPN only in Native Mode