HP WORLD 2004
Solutions and Technology Conference & Expo

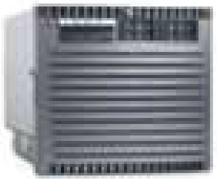
HP CIFS Server with Samba 3.0 and Windows 2003

Eric Roseme
ATC Technical Consultant
Systems Networking and Security Lab
Hewlett-Packard

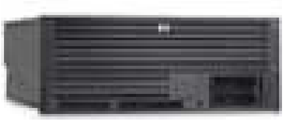
HP CIFS Server continues to evolve inherent HP-UX OS advantages with Windows Client/Server new technology. Samba 3.0 provides updated features and enhanced flexibility for integrating file server OS platforms with Windows clients and Windows infrastructure, and HP CIFS Server is enhanced additionally for improvements in performance and HP-UX product interoperation.

- Introduction
- Samba Version Tracking
- ADS Integration
- LDAP and Directory Servers
- Authentication
- Net Commands
- New and Changed Tools and Parameters
- Performance Enhancements and Recommendations
- Summary

HP CIFS Server Review



- HP CIFS Server
  - SMB file/print services on HP-UX
  - Windows client connectivity (XP, 2000, NT)
  - Windows domain integration (2003, 2000, NT)



- No Added Costs or Licensing
  - Standard Distributed File System on…..
  - HP-UX Application Release CDs or web (software.hp.com)
  - With NFS, HP-UX fully integrated distributed file system

HP CIFS Server Review

- HP-UX 11i v1, HP-UX 11i v2
- Enterprise File Server and Storage Platform
  - Reliability 99.999
  - Highly Available: ServiceGuard
  - Scaleable PA: rp24X0, rp34X0, rp44x0, rp54X0, rp74X0, rp84X0, Superdome
  - Scaleable IA: rx16X0, rx26X0, rx46X0, rx76X0, rx86X0, Superdome
  - Storage:
    - XP128, XP1024
    - VA7410
    - EVA3000, EVA5000
  - Flexibility:
    - Dedicated File Servers
    - Multi-Purpose Servers
    - Both (Superdome VPARs)
    - Enterprise CIFS and NFS

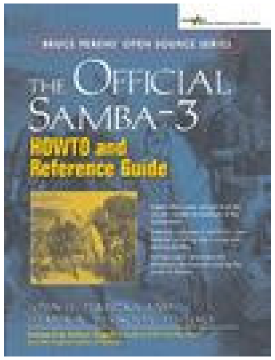
HP WORLD 2004
Solutions and Technology Conference & Expo

HP CIFS Server with Samba 3.0

- Samba 3.0 Significant Redesign
- LDAP and Directory Enabled
- Kerberos Authentication
- Unicode Support
- Domain Trusts

- Better Non-Windows Autonomy
- Enhanced Windows Domain Interoperability

“New Features in Samba-3” (29.2)



Buy this book!!!!!!!!

http://www.amazon.com/exec/obidos/tg/detail/-/0131453556/qid=1088095271/sr=8-1/ref=pd_ka_1/002-6068131-4112814?v=glance&s=books&n=507846

- Active Directory Support
- Unicode Support
- Authentication Re-written
- Name Mangling Re-written
- New Net Commands
- Error Handling Improvements (NT Status-32 codes)
- Improved Printing – Print Attributes in AD
- New RPC Modules for Password Databases
- New winbind Daemon – Performance Increase
- NT4 Trusts
- Distributed winbind data store (idmap backend)
- Documentation Updates
- SMB Signing Support (Windows 2003 Compatibility)
- Multiple WINS server support

New and Changed Features in Windows Server 2003

- Interim Domain Mode (joins Mixed and Native)
- AD Replication Enhancements
- AD Branch Office Enhancements
- DC rename, Domain rename, Schema updates
- Remote Installation Service, Auto-Deploy Service
- Server Manger wizards
- GPMC, and GPO WMI filtering
- Terminal Server Updates (like load balancing)
- Windows Resource Manager
- 61 New Command Line Tools
- 30 Services Off by default (IIs, FTP, SMTP, …)
- **Kerberos Enhancements**
- Windows Rights Management, PKI enhancements, tools
- Trust enhancements – cross-forest, granularity
- DFS, FRS, EFS enhancements

W2003 Features vs Samba 3.0 Features

- Little overlap
- Essentially implementing new Samba features
- A couple of Windows 2003 security details
    - Kerberos compatibility with HP-UX
    - Packet signing
- Otherwise, Windows 2003 = Windows 2000 for Samba
- Other exceptions?
    - Let me know

What Do “Features” Mean to You?

- Introduction
- **Samba Version Tracking**
- ADS Integration
- LDAP and Directory Servers
- Authentication
- Net Commands
- New and Changed Tools and Parameters
- Performance Enhancements and Recommendations
- Summary

Version Tracking

- CIFS/9000 First release, March 2000
  - CIFS/9000 Server A.01.05: Samba 2.0.5
- CIFS/9000 with Samba 2.2, March 2002
  - CIFS/9000 Server 2.2a A.01.08: Samba 2.2.3a
- Current Release with Samba 2.2, June 2004
  - HP CIFS Server 2.2j A.01.11.02: Samba 2.2.10
- Next Release with Samba 3.0, Q304
  - HP CIFS Server 3.0a A.02.01: Samba 3.0.5
    - Samba 3.0 release 9/24/2003

Version Tracking

- Customer Feedback: HP CIFS Server should follow Samba releases more closely
- ***Top Priority***: Samba platform stability
  - Samba integration schedule dependent upon version reliability
  - HP emphasizes enterprise reliability
- Release Policy Improvement
  - Web releases for improved time to market
  - Interim release (2.2.8a→2.2.9) much quicker
    - 19 days after Samba 2.2.9 release

Version Tracking

- Policy Summary
  - Major version updates – ENSURE STABILITY
    - Ex: 2.0.9-to-2.2.3a
    - Ex: 2.2.9-to-3.0
  - Interim version updates – follow aggressively
    - Ex: 2.2.8a-to-2.2.9

Version Tracking

- ***CIFS/9000 Server Technology Preview Release***
  - On www.software.hp.com
  - Using HP CIFS Server product structure
  - Based upon the very latest Samba releases
  - For customer testing – ***UNSUPPORTED by HP***
  - ***Currently on Samba 3.0.2***

Version Tracking

- ***HP-UX Samba Binaries***

  - On http://us1.samba.org/samba/ftp/Binary_Packages/hp/
  - Latest Samba releases on HP-UX
  - ***NOT*** HP CIFS Server – ***HP UNSUPPORTED***
  - Compiled with additional Samba compile options
    - --with-winbind
    - --with-pam
    - --with-ldap

  - Currently: 3.0.4 and 2.2.8a for HP-UX 11i

- Introduction
- Samba Version Tracking
- **ADS Integration**
- LDAP and Directory Servers
- Authentication
- Net Commands
- New and Changed Tools and Parameters
- Performance Enhancements and Recommendations
- Summary

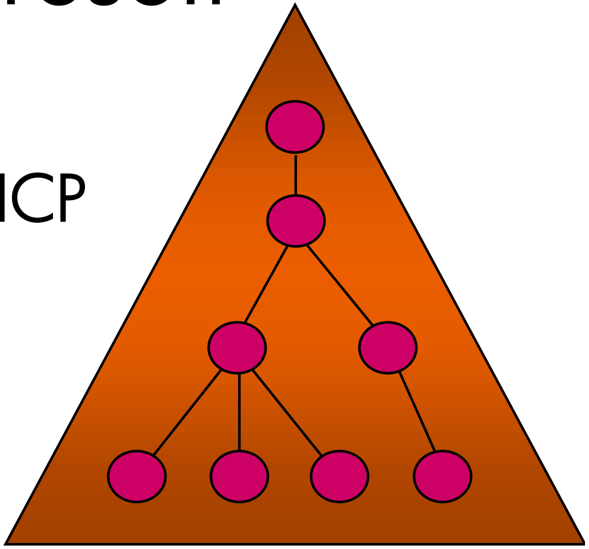
"We need Samba 3.0 for Active Directory integration"

Common quote from Samba implementers

Module Objectives

- Define ADS integration
- Clarify how Samba integrates with ADS
- Identify and advise on protocol interoperability
  - Kerberos
  - LDAP
  - DNS
- Propose HPUX-to-ADS integration enhancements

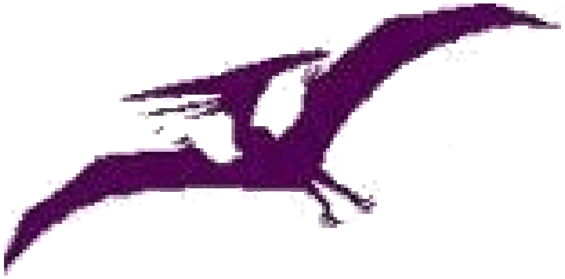
Active Directory Service - Microsoft



- LDAP Directory Server
  - Integrated with “Dynamic DNS” and DHCP
  - Integrated with Kerberos authentication
  - Integrated with Group Policy Objects
  - Integrated with Global Catalog
  - Integrated with MMC
  - Integrated with Active Directory Service Interfaces
- Tightly Integrated with ADS
  - Exchange
  - Dfs
  - Various “Server” Product/Applications
  - AD/AM: directory without all of the mgt/app hooks
    - Active Directory Application Mode

Active Directory Service : Samba View

- How Samba defines ADS
  - Directory Server / LDAP
  - DDNS
  - Kerberos



Samba-ADS Integration with......

- Directory / LDAP

  - Smb.conf “security = ads”
    - Enables LDAP write/read to Active Directory
  - Command line “net ads xxxxxx”
    - Executes LDAP write/read to Active Directory
  - Real Time LDAP reads and writes
    - Versus MSRPC when in “security = domain”
- Non-ADS Directory / LDAP in later module

Samba-ADS Integration with……

- Kerberos

  - smb.conf “security = ads”
    - Enables default Windows Kerberos Authentication
  - Windows 2000 KDC
  - Windows 2003 KDC
    - Defaults to RC4-HMAC encryption (new “feature”)
- Use Windows domain DNS server for best results

Samba ADS Configuration

- smb.conf

```
# Global parameters
[global]
        netbios name = HPUXCIFS
        workgroup = DOMAIN2003
        realm = DOMAIN2003.HP.COM
        server string = Samba Server
        security = ADS
        encrypt passwords = yes
        password server =
    WINDOWS2003DC
```

- ***"password server =" used for***
  - ***NTLM fall-through authentication***
  - ***Some LDAP queries***
  - ***All KRB5 is handled by hp-ux libraries***

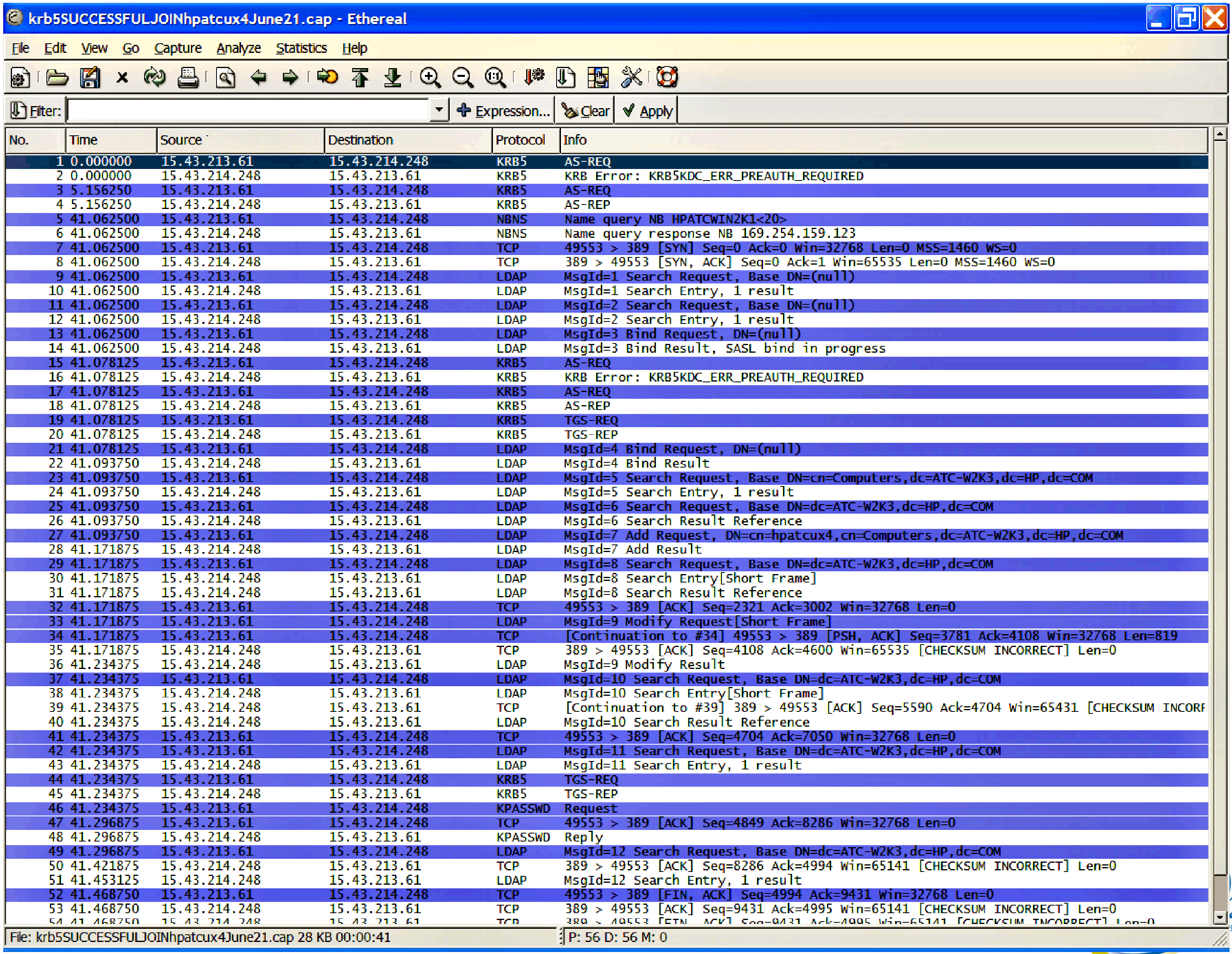
- krb5.conf

```
[libdefaults]
 default_realm = DOMAIN2003.HP.COM
 ticket_lifetime = 24000
 default_tkt_enctypes = rc4-hmac
 default_tgs_enctypes = rc4-hmac
 ccache_type = 2

[realms]

 DOMAIN2003.HP.COM = {
  kdc = WINDOWS2003DC.DOMAIN2003.hp.com:88
  admin_server = WINDOWS2003DC.DOMAIN2003.hp.com
  kpasswd_server = WINDOWS2003DC.DOMAIN2003.hp.com:464
 }
 [domain_realm]
 .hp.com = DOMAIN2003.HP.COM
```

Directory: Join Domain via “net ads join”



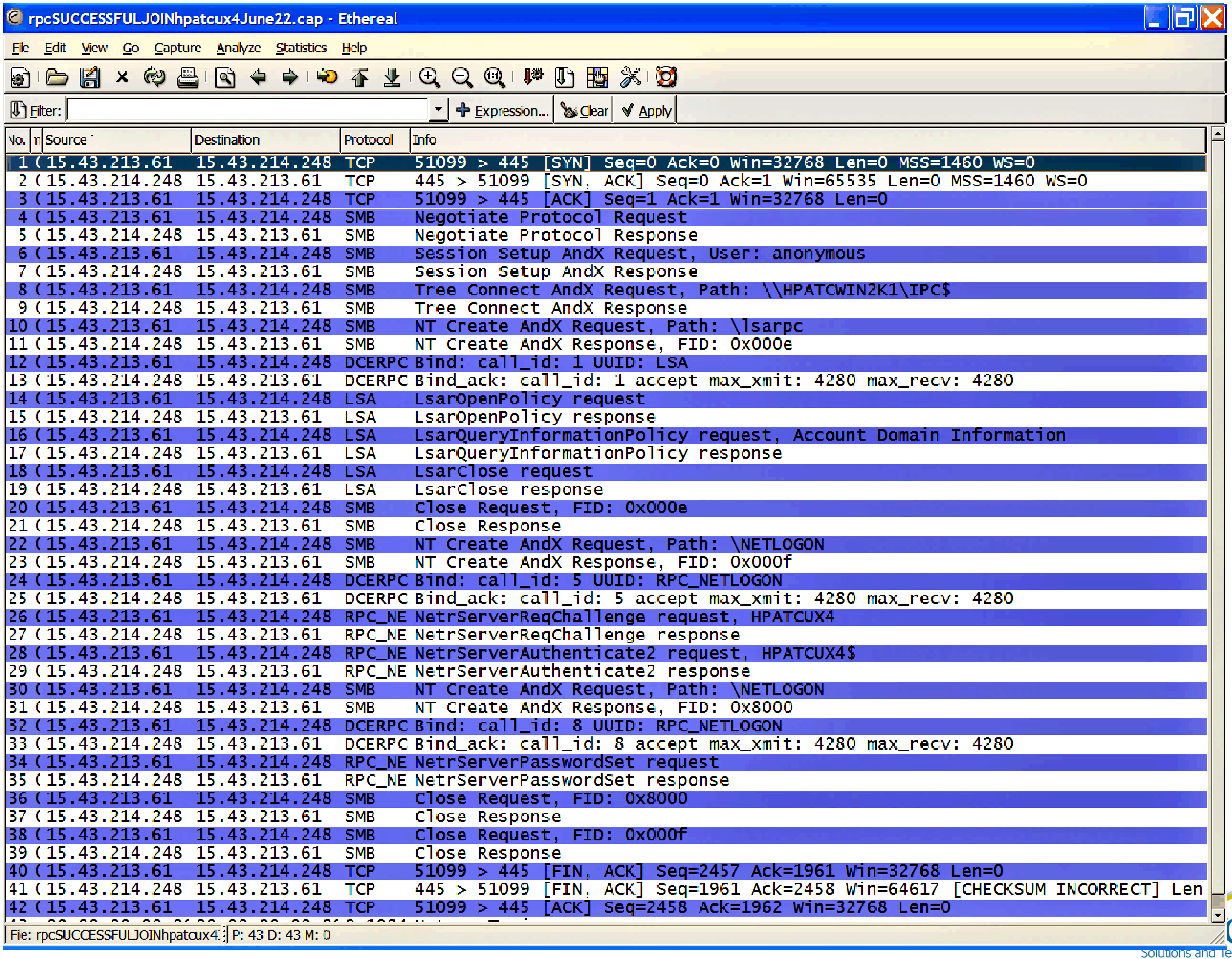
```
No.   Time       Source          Destination     Protocol  Info
   1 0.000000    15.43.213.61    15.43.214.248   KRB5      AS-REQ
   2 0.000000    15.43.214.248   15.43.213.61    KRB5      KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
   3 5.156250    15.43.213.61    15.43.214.248   KRB5      AS-REQ
   4 5.156250    15.43.214.248   15.43.213.61    KRB5      AS-REP
   5 41.062500   15.43.213.61    15.43.214.248   NBNS      Name query NB HPATCWIN2K1<20>
   6 41.062500   15.43.214.248   15.43.213.61    NBNS      Name query response NB 169.254.159.123
   7 41.062500   15.43.213.61    15.43.214.248   TCP       49553 > 389 [SYN] Seq=0 Ack=0 Win=32768 Len=0 MSS=1460 WS=0
   8 41.062500   15.43.214.248   15.43.213.61    TCP       389 > 49553 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=0
   9 41.062500   15.43.213.61    15.43.214.248   LDAP      MsgId=1 Search Request, Base DN=(null)
  10 41.062500   15.43.214.248   15.43.213.61    LDAP      MsgId=1 Search Entry, 1 result
  11 41.062500   15.43.213.61    15.43.214.248   LDAP      MsgId=2 Search Request, Base DN=(null)
  12 41.062500   15.43.214.248   15.43.213.61    LDAP      MsgId=2 Search Entry, 1 result
  13 41.062500   15.43.213.61    15.43.214.248   LDAP      MsgId=3 Bind Request, DN=(null)
  14 41.062500   15.43.214.248   15.43.213.61    LDAP      MsgId=3 Bind Result, SASL bind in progress
  15 41.078125   15.43.213.61    15.43.214.248   KRB5      AS-REQ
  16 41.078125   15.43.214.248   15.43.213.61    KRB5      KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
  17 41.078125   15.43.213.61    15.43.214.248   KRB5      AS-REQ
  18 41.078125   15.43.214.248   15.43.213.61    KRB5      AS-REP
  19 41.078125   15.43.213.61    15.43.214.248   KRB5      TGS-REQ
  20 41.078125   15.43.214.248   15.43.213.61    KRB5      TGS-REP
  21 41.078125   15.43.213.61    15.43.214.248   LDAP      MsgId=4 Bind Request, DN=(null)
  22 41.093750   15.43.214.248   15.43.213.61    LDAP      MsgId=4 Bind Result
  23 41.093750   15.43.213.61    15.43.214.248   LDAP      MsgId=5 Search Request, Base DN=cn=Computers,dc=ATC-W2K3,dc=HP,dc=COM
  24 41.093750   15.43.214.248   15.43.213.61    LDAP      MsgId=5 Search Entry, 1 result
  25 41.093750   15.43.213.61    15.43.214.248   LDAP      MsgId=6 Search Request, Base DN=dc=ATC-W2K3,dc=HP,dc=COM
  26 41.093750   15.43.214.248   15.43.213.61    LDAP      MsgId=6 Search Result Reference
  27 41.093750   15.43.213.61    15.43.214.248   LDAP      MsgId=7 Add Request, DN=cn=hpatcux4,cn=Computers,dc=ATC-W2K3,dc=HP,dc=COM
  28 41.171875   15.43.214.248   15.43.213.61    LDAP      MsgId=7 Add Result
  29 41.171875   15.43.213.61    15.43.214.248   LDAP      MsgId=8 Search Request, Base DN=dc=ATC-W2K3,dc=HP,dc=COM
  30 41.171875   15.43.214.248   15.43.213.61    LDAP      MsgId=8 Search Entry[Short Frame]
  31 41.171875   15.43.214.248   15.43.213.61    LDAP      MsgId=8 Search Result Reference
  32 41.171875   15.43.213.61    15.43.214.248   TCP       49553 > 389 [ACK] Seq=2321 Ack=3002 Win=32768 Len=0
  33 41.171875   15.43.213.61    15.43.214.248   LDAP      MsgId=9 Modify Request[Short Frame]
  34 41.171875   15.43.213.61    15.43.214.248   TCP       [Continuation to #34] 49553 > 389 [PSH, ACK] Seq=3781 Ack=4108 Win=32768 Len=819
  35 41.171875   15.43.214.248   15.43.213.61    TCP       389 > 49553 [ACK] Seq=4108 Ack=4600 Win=65535 [CHECKSUM INCORRECT] Len=0
  36 41.234375   15.43.214.248   15.43.213.61    LDAP      MsgId=9 Modify Result
  37 41.234375   15.43.213.61    15.43.214.248   LDAP      MsgId=10 Search Request, Base DN=dc=ATC-W2K3,dc=HP,dc=COM
  38 41.234375   15.43.214.248   15.43.213.61    LDAP      MsgId=10 Search Entry[Short Frame]
  39 41.234375   15.43.214.248   15.43.213.61    TCP       [Continuation to #39] 389 > 49553 [ACK] Seq=5590 Ack=4704 Win=65431 [CHECKSUM INCORF
  40 41.234375   15.43.214.248   15.43.213.61    LDAP      MsgId=10 Search Result Reference
  41 41.234375   15.43.213.61    15.43.214.248   TCP       49553 > 389 [ACK] Seq=4704 Ack=7050 Win=32768 Len=0
  42 41.234375   15.43.213.61    15.43.214.248   LDAP      MsgId=11 Search Request, Base DN=dc=ATC-W2K3,dc=HP,dc=COM
  43 41.234375   15.43.214.248   15.43.213.61    LDAP      MsgId=11 Search Entry, 1 result
  44 41.234375   15.43.213.61    15.43.214.248   KRB5      TGS-REQ
  45 41.234375   15.43.214.248   15.43.213.61    KRB5      TGS-REP
  46 41.234375   15.43.213.61    15.43.214.248   KPASSWD   Request
  47 41.296875   15.43.213.61    15.43.214.248   TCP       49553 > 389 [ACK] Seq=4849 Ack=8286 Win=32768 Len=0
  48 41.296875   15.43.214.248   15.43.213.61    KPASSWD   Reply
  49 41.296875   15.43.213.61    15.43.214.248   LDAP      MsgId=12 Search Request, Base DN=dc=ATC-W2K3,dc=HP,dc=COM
  50 41.421875   15.43.214.248   15.43.213.61    TCP       389 > 49553 [ACK] Seq=8286 Ack=4994 Win=65141 [CHECKSUM INCORRECT] Len=0
  51 41.453125   15.43.214.248   15.43.213.61    LDAP      MsgId=12 Search Entry, 1 result
  52 41.468750   15.43.213.61    15.43.214.248   TCP       49553 > 389 [FIN, ACK] Seq=4994 Ack=9431 Win=32768 Len=0
  53 41.468750   15.43.214.248   15.43.213.61    TCP       389 > 49553 [ACK] Seq=9431 Ack=4995 Win=65141 [CHECKSUM INCORRECT] Len=0
  54 41.468750   15.43.214.248   15.43.213.61    TCP       389 > 49553 [FIN, ACK] Seq=9431 Ack=4995 Win=65141 [CHECKSUM INCORRECT] Len=0
```

File: krb5SUCCESSFULJOINhpatcux4June21.cap 28 KB 00:00:41 | P: 56 D: 56 M: 0

Directory Object via “net ads join”

```
version: 1
dn: CN=hpatcux4,CN=Computers,DC=atc-w2k3,DC=hp,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
objectClass: computer
cn: hpatcux4
distinguishedName: CN=hpatcux4,CN=Computers,DC=atc-w2k3,DC=hp,DC=com
instanceType: 4
whenCreated: 20040412225013.0Z
whenChanged: 20040412225013.0Z
uSNCreated: 67672
uSNChanged: 67676
name: hpatcux4
objectGUID:: H1IQqT0SKUWoVBGjoV0nzA==
userAccountControl: 2166784
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
localPolicyFlags: 0
pwdLastSet: 127262838137031250
primaryGroupID: 515 userPrincipalName: objectSid:: AQUAAAAAAAUVAAAAun1JfXRxBcInE2Fa3gQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: hpatcux4$
sAMAccountType: 805306369
operatingSystem: Samba
operatingSystemVersion: 3.0.2a based HP CIFS Server A.02.00
dNSHostName: hpatcux4
userPrincipalName: HOST/hpatcux4@ATC-W2K3.HP.COM
servicePrincipalName: CIFS/hpatcux4.atc-w2k3.hp.com
servicePrincipalName: CIFS/hpatcux4
servicePrincipalName: HOST/hpatcux4.atc-w2k3.hp.com
servicePrincipalName: HOST/hpatcux4
objectCategory: CN=Computer,CN=Schema,CN=Configuration,DC=atc-w2k3,DC=hp,DC=com
isCriticalSystemObject: FALSE
```

Directory:Join Domain via “net rcp oldjoin”


rpcSUCCESSFULJOINhpatcux4June22.cap - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

```
No. T Source        Destination   Protocol Info
 1 ( 15.43.213.61   15.43.214.248 TCP    51099 > 445 [SYN] Seq=0 Ack=0 Win=32768 Len=0 MSS=1460 WS=0
 2 ( 15.43.214.248  15.43.213.61  TCP    445 > 51099 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=0
 3 ( 15.43.213.61   15.43.214.248 TCP    51099 > 445 [ACK] Seq=1 Ack=1 Win=32768 Len=0
 4 ( 15.43.213.61   15.43.214.248 SMB    Negotiate Protocol Request
 5 ( 15.43.214.248  15.43.213.61  SMB    Negotiate Protocol Response
 6 ( 15.43.213.61   15.43.214.248 SMB    Session Setup AndX Request, User: anonymous
 7 ( 15.43.214.248  15.43.213.61  SMB    Session Setup AndX Response
 8 ( 15.43.213.61   15.43.214.248 SMB    Tree Connect AndX Request, Path: \\HPATCWIN2K1\IPC$
 9 ( 15.43.214.248  15.43.213.61  SMB    Tree Connect AndX Response
10 ( 15.43.213.61   15.43.214.248 SMB    NT Create AndX Request, Path: \lsarpc
11 ( 15.43.214.248  15.43.213.61  SMB    NT Create AndX Response, FID: 0x000e
12 ( 15.43.213.61   15.43.214.248 DCERPC Bind: call_id: 1 UUID: LSA
13 ( 15.43.214.248  15.43.213.61  DCERPC Bind_ack: call_id: 1 accept max_xmit: 4280 max_recv: 4280
14 ( 15.43.213.61   15.43.214.248 LSA    LsarOpenPolicy request
15 ( 15.43.214.248  15.43.213.61  LSA    LsarOpenPolicy response
16 ( 15.43.213.61   15.43.214.248 LSA    LsarQueryInformationPolicy request, Account Domain Information
17 ( 15.43.214.248  15.43.213.61  LSA    LsarQueryInformationPolicy response
18 ( 15.43.213.61   15.43.214.248 LSA    LsarClose request
19 ( 15.43.214.248  15.43.213.61  LSA    LsarClose response
20 ( 15.43.213.61   15.43.214.248 SMB    Close Request, FID: 0x000e
21 ( 15.43.214.248  15.43.213.61  SMB    Close Response
22 ( 15.43.213.61   15.43.214.248 SMB    NT Create AndX Request, Path: \NETLOGON
23 ( 15.43.214.248  15.43.213.61  SMB    NT Create AndX Response, FID: 0x000f
24 ( 15.43.213.61   15.43.214.248 DCERPC Bind: call_id: 5 UUID: RPC_NETLOGON
25 ( 15.43.214.248  15.43.213.61  DCERPC Bind_ack: call_id: 5 accept max_xmit: 4280 max_recv: 4280
26 ( 15.43.213.61   15.43.214.248 RPC_NE NetrServerReqChallenge request, HPATCUX4
27 ( 15.43.214.248  15.43.213.61  RPC_NE NetrServerReqChallenge response
28 ( 15.43.213.61   15.43.214.248 RPC_NE NetrServerAuthenticate2 request, HPATCUX4$
29 ( 15.43.214.248  15.43.213.61  RPC_NE NetrServerAuthenticate2 response
30 ( 15.43.213.61   15.43.214.248 SMB    NT Create AndX Request, Path: \NETLOGON
31 ( 15.43.214.248  15.43.213.61  SMB    NT Create AndX Response, FID: 0x8000
32 ( 15.43.213.61   15.43.214.248 DCERPC Bind: call_id: 8 UUID: RPC_NETLOGON
33 ( 15.43.214.248  15.43.213.61  DCERPC Bind_ack: call_id: 8 accept max_xmit: 4280 max_recv: 4280
34 ( 15.43.213.61   15.43.214.248 RPC_NE NetrServerPasswordSet request
35 ( 15.43.214.248  15.43.213.61  RPC_NE NetrServerPasswordSet response
36 ( 15.43.213.61   15.43.214.248 SMB    Close Request, FID: 0x8000
37 ( 15.43.214.248  15.43.213.61  SMB    Close Response
38 ( 15.43.213.61   15.43.214.248 SMB    Close Request, FID: 0x000f
39 ( 15.43.214.248  15.43.213.61  SMB    Close Response
40 ( 15.43.213.61   15.43.214.248 TCP    51099 > 445 [FIN, ACK] Seq=2457 Ack=1961 Win=32768 Len=0
41 ( 15.43.214.248  15.43.213.61  TCP    445 > 51099 [FIN, ACK] Seq=1961 Ack=2458 Win=64617 [CHECKSUM INCORRECT] Len
42 ( 15.43.213.61   15.43.214.248 TCP    51099 > 445 [ACK] Seq=2458 Ack=1962 Win=32768 Len=0
```

File: rpcSUCCESSFULJOINhpatcux4 | P: 43 D: 43 M: 0

Directory Object via “net rpc oldjoin”

```
version: 1
dn: CN=hpatcux4,CN=Computers,DC=atc-w2k3,DC=hp,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
objectClass: computer
cn: hpatcux4
distinguishedName: CN=hpatcux4,CN=Computers,DC=atc-w2k3,DC=hp,DC=com
instanceType: 4
whenCreated: 20040124001043.0Z
whenChanged: 20040329184058.0Z
uSNCreated: 16946
uSNChanged: 65802
name: hpatcux4
objectGUID:: XdgA5olInEO4rdlf4xARrg==
userAccountControl: 4096
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 127250598122656250
localPolicyFlags: 0
pwdLastSet: 0
primaryGroupID: 515
objectSid:: AQUAAAAAAAUVAAAAun1JfXRxBcInE2FaYgQAAA==
accountExpires: 9223372036854775807
logonCount: 44048
sAMAccountName: hpatcux4$
sAMAccountType: 805306369
operatingSystem: HP-UX
operatingSystemVersion: B.11.11
dNSHostName: hpatcux4.atc-w2k3.hp.com
userPrincipalName: host/hpatcux4.atc-w2k3.hp.com@ATC-W2K3.HP.COM
servicePrincipalName: host/hpatcux4.atc-w2k3.hp.com
objectCategory: CN=Computer,CN=Schema,CN=Configuration,DC=atc-w2k3,DC=hp,DC=co
 m
isCriticalSystemObject: FALSE
```

```
dNSHostName: hpatcux4
userPrincipalName: HOST/hpatcux4@ATC-
W2K3.HP.COM
servicePrincipalName: CIFS/hpatcux4.atc-w2k3.hp.com
servicePrincipalName: CIFS/hpatcux4
servicePrincipalName: HOST/hpatcux4.atc-
w2k3.hp.com
servicePrincipalName: HOST/hpatcux4
```

ADS Schema

- No ADS Schema extension for CIFS/Samba
  - Samba object class attributes not extended
- Samba object class discussed later module
- Samba Server added as domain object
  - Via LDAP, for LDAP
  - Slightly different than MSRPC

- (Note: non-ADS directories covered later)

ADS Schema

- User Object

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: eric roseme
sn: roseme
givenName: eric
distinguishedName: CN=eric roseme,CN=Users,DC=atc-w2k3,DC=hp,DC=com
instanceType: 4
whenCreated: 20040329184924.0Z
whenChanged: 20040618224331.0Z
displayName: eric roseme
uSNCreated: 65809
memberOf: CN=Domain Admins,CN=Users,DC=atc-w2k3,DC=hp,DC=com
memberOf: CN=Administrators,CN=Builtin,DC=atc-w2k3,DC=hp,DC=com
uSNChanged: 82239
name: eric roseme
objectGUID: 40677c4e-f8ab-4d5f-9728-722734af383
userAccountControl: 2163200
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 127324821378281250
lastLogoff: 0
lastLogon: 127324839205000000
pwdLastSet: 127320722114062500
primaryGroupID: 513
objectSid: S-1-5-21-2101968314-3255136628-1516311335-1133
adminCount: 1
accountExpires: 9223372036854775807
logonCount: 134
sAMAccountName: eroseme
sAMAccountType: 805306368
userPrincipalName: eroseme@atc-w2k3.hp.com
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=atc-w2k3,DC=hp,DC=com
msSFU30Password: ABCD!efgh12345$67890
```

❑ **No POSIX attributes!!**

- **UID required for Samba**
- **GID required for Samba**
- ***Thus requires UID/GID repository***

➢ **Smbpasswd**

- **/etc/passwd**
- **"passdb backend = smbpasswd"**

➢ **Or winbind**

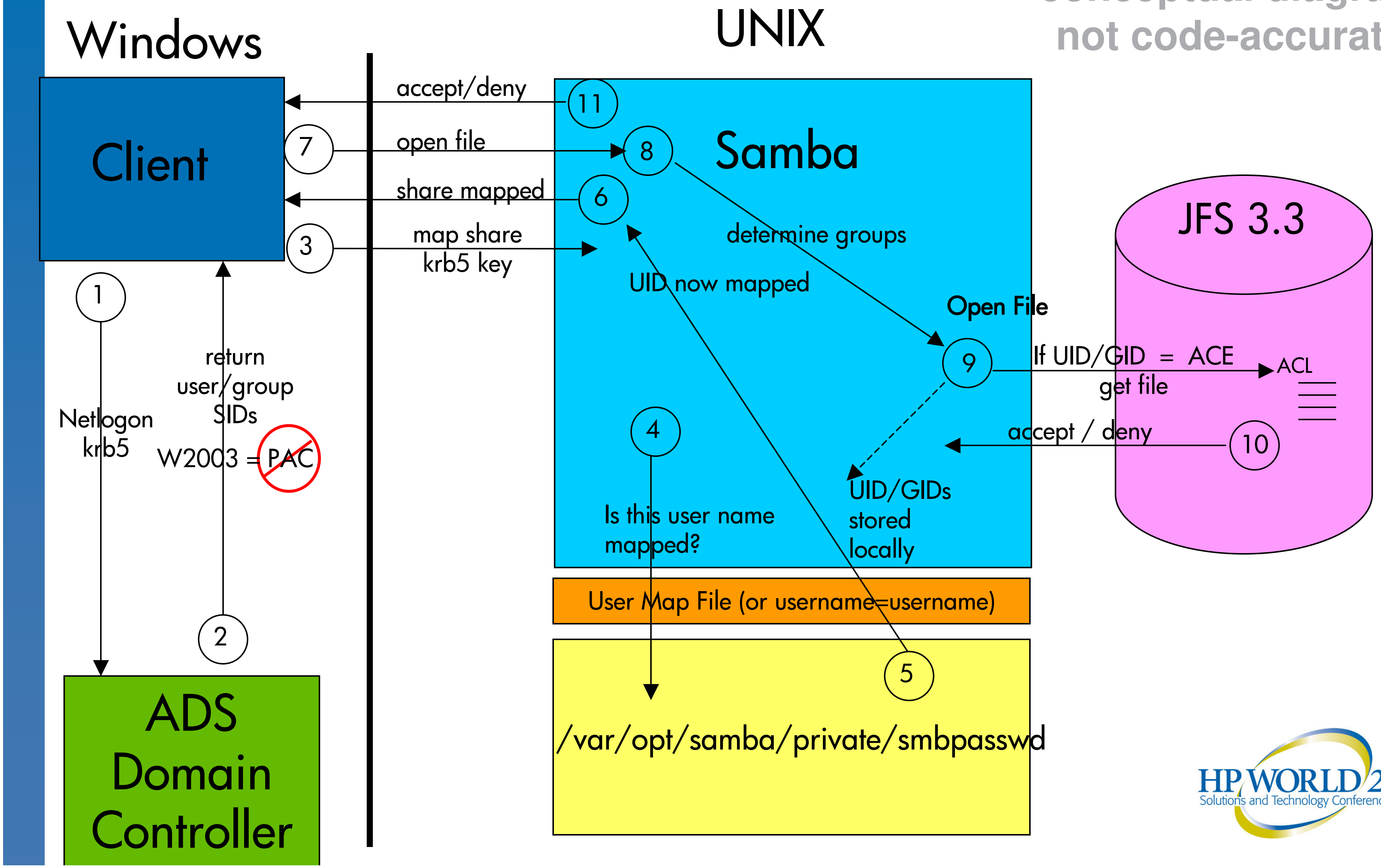
- **"winbind enum users = yes"**
- **"winbind enum groups = yes"**
- **See details later**

❑ **Effect – dual ID**

Block Diagram: Client-Samba-ADS

(NO winbind)

conceptual diagram
not code-accurate



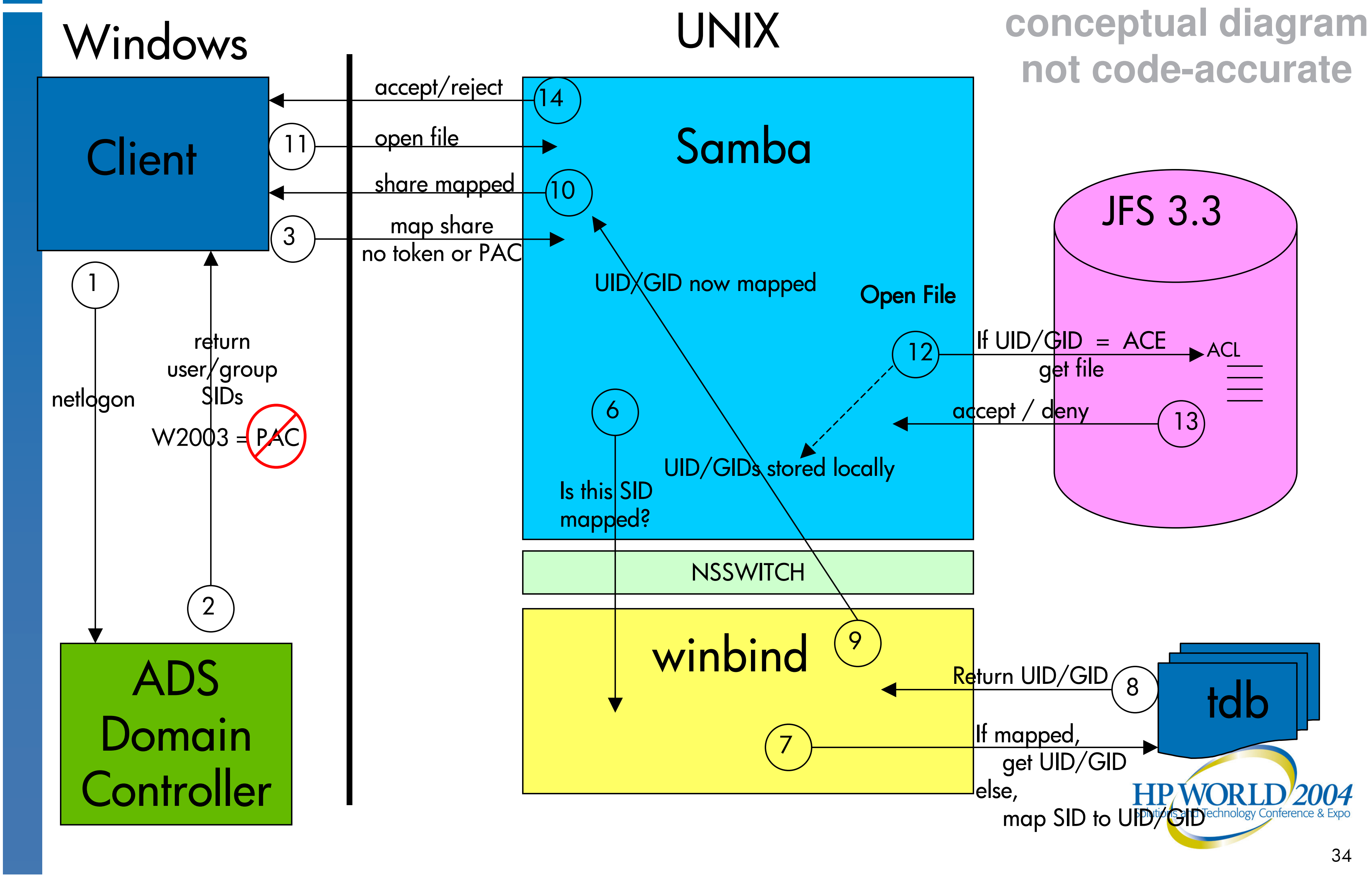
winbind for ADS Integration

- winbind process is separate from Samba process
  - winbindd
  - smbd
- winbindd
  - Maps Windows user SID to HP-UX user UID
  - Maps Windows group SID to HP-UX group GID
  - Maps users to Windows Built-In group SIDs
  - Automatic mapping – no admin intervention
- Samba smbd calls system getpwnam
- Uses nsswitch
  - Directs getpwnam system call to configured backend
  - Smbd → getpwnam → nsswitch → winbind → .tdb map

HP CIFS Server and winbind

- Version 2.2a-j: winbind not supported
  - Not compiled into smbd
- Version 3: winbind is supported
  - Compiled into smbd
  - /opt/samba/bin/winbindd
  - All libraries supplied
  - Installation and administration instructions
- Like Samba, winbind is very flexible
  - Specific winbind usage and scenarios are supported

Block Diagram: Client-Samba-winbind-ADS



Samba winbind Configuration

- smb.conf

```
# Global parameters
    [global]
        workgroup = ATC-W2K3
        realm = ATC-W2K3.HP.COM
        server string = Samba Server
        interfaces = 15.43.213.61
        bind interfaces only = Yes
        security = ADS
        password server = HPATCWIN2K1.ATC-W2K3.HP.COM
        ntlm auth = no
        lanman auth = no
        log level = 10
        log file = /var/opt/samba/log.%m
        max log size = 1000
         winbind separator = +
          idmap uid = 10000-20000
          idmap gid = 10000-20000
          winbind enum users = yes
          winbind enum groups = yes
         local master = No
         ldap ssl = no
         short preserve case = No
         dos filetime resolution = Yes
        template homedir = /home/%U
```

- Process
  - start /opt/samba/bin/winbindd
    - Actually starts 2 daemons
      - For cache & tdb
    - Will not start without smb.conf idmaps
    - Logs to /var/opt/samba/log.winbindd
    - Stores maps in
      - /var/opt/samba/private/winbindd_idmap.tdb
      - /var/opt/samba/private/winbindd_cache.tdb

- /etc/nsswitch.conf
  - passwd: files winbind
  - group: files winbind
  - hosts: files dns
  - networks: files ldap
  - protocols: files ldap
  - rpc: files ldap
  - publickey: files
  - netgroup: files ldap
  - automount: files
  - aliases: files
  - services: files ldap

winbind mapping data stores

- Winbind stores mapping data in .tdb repository
  - More efficient than flat files
  - Persistent
- Not easily edited or displayed
  - See wbinfo topic in “Tools” module
- winbind .tdb repository most efficient for under 1000s of users
- New winbind repository
  - LDAP directory server repository
  - Scales better than .tdb for 1000s of users
  - Consistent mapping over multiple servers
  - Smb.conf: “idmap backend = ldapsam://ldapserver
  - See details in LDAP module

Do you REALLY want “tighter” ADS integration?

HP-UX LDAP ADS Integration

- Extend ADS Schema for POSIX attributes
- More comprehensive “ADS Integration”
  - Than standard Samba
- Store and manage HP-UX user/groups in AD

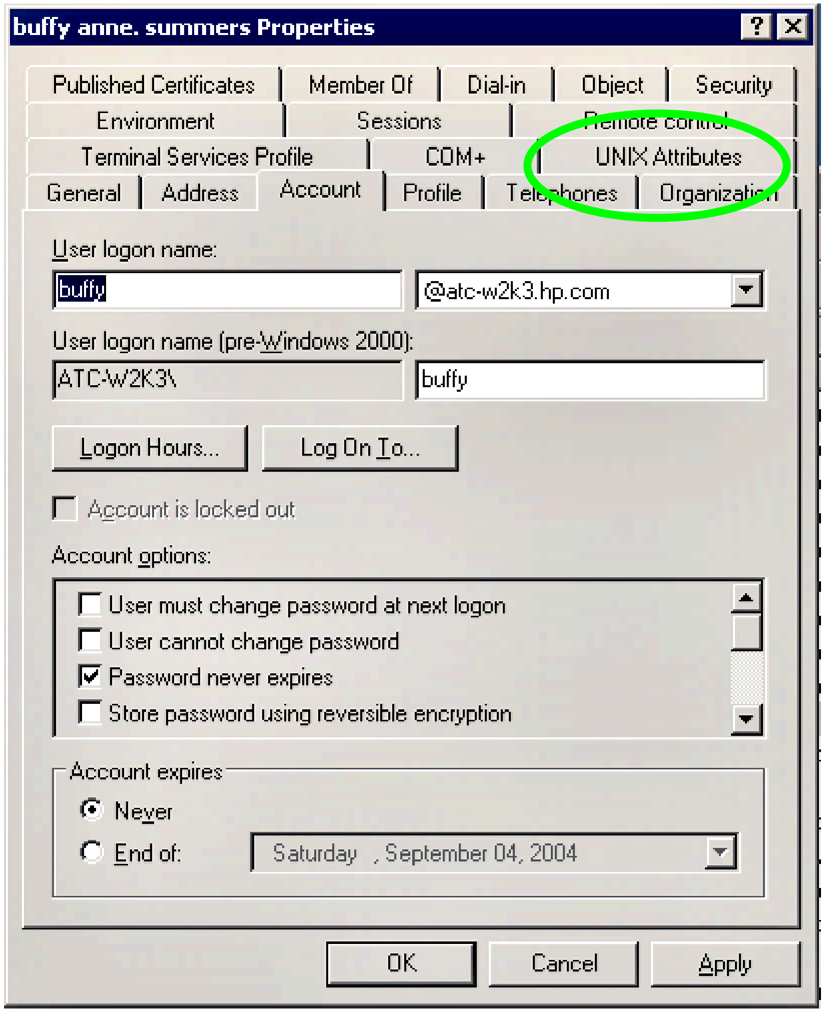
- If you REALLY want increased “ADS Integration”
  - This is the way to go
- Components
  - ADS (of course)
  - HP-UX LDAP UX integration
  - SFU 3.5 (free from Microsoft)

LDAP-UX path to POSIX Attributes

- Samba and Windows domain LDAP access:
  - Samba → LDAP → Windows Domain Controller
  - Direct LDAP interface to directory

- Samba and POSIX Attribute LDAP access:
  - Samba → HP-UX system calls → nsswitch → LDAP → Windows Domain Controller
  - Uses standard unix system calls to retrieve POSIX data

ADS MMC with LDAP-UX



User logon name: buffy @atc-w2k3.hp.com

User logon name (pre-Windows 2000): ATC-W2K3\ buffy

□ Account is locked out

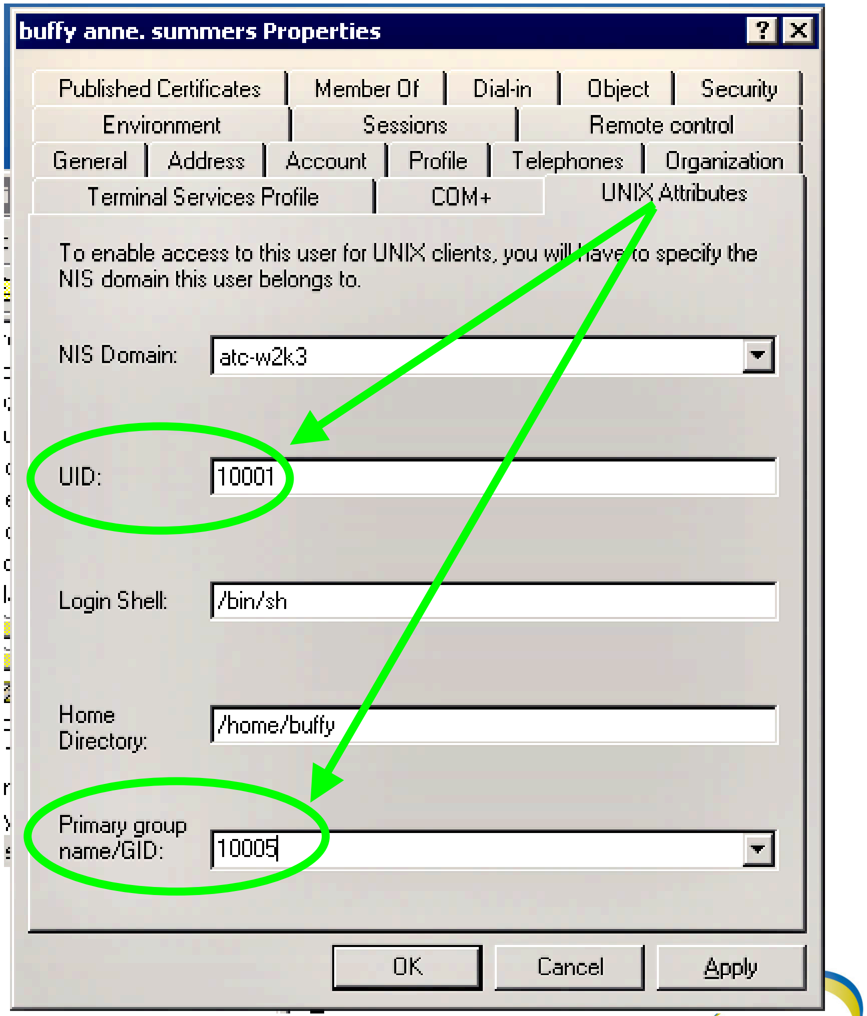
Account options:

- □ User must change password at next logon
- □ User cannot change password
- ☑ Password never expires
- □ Store password using reversible encryption

Account expires

● Never

○ End of: Saturday , September 04, 2004



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

NIS Domain: atc-w2k3

UID: 10001

Login Shell: /bin/sh

Home Directory: /home/buffy

Primary group name/GID: 10005

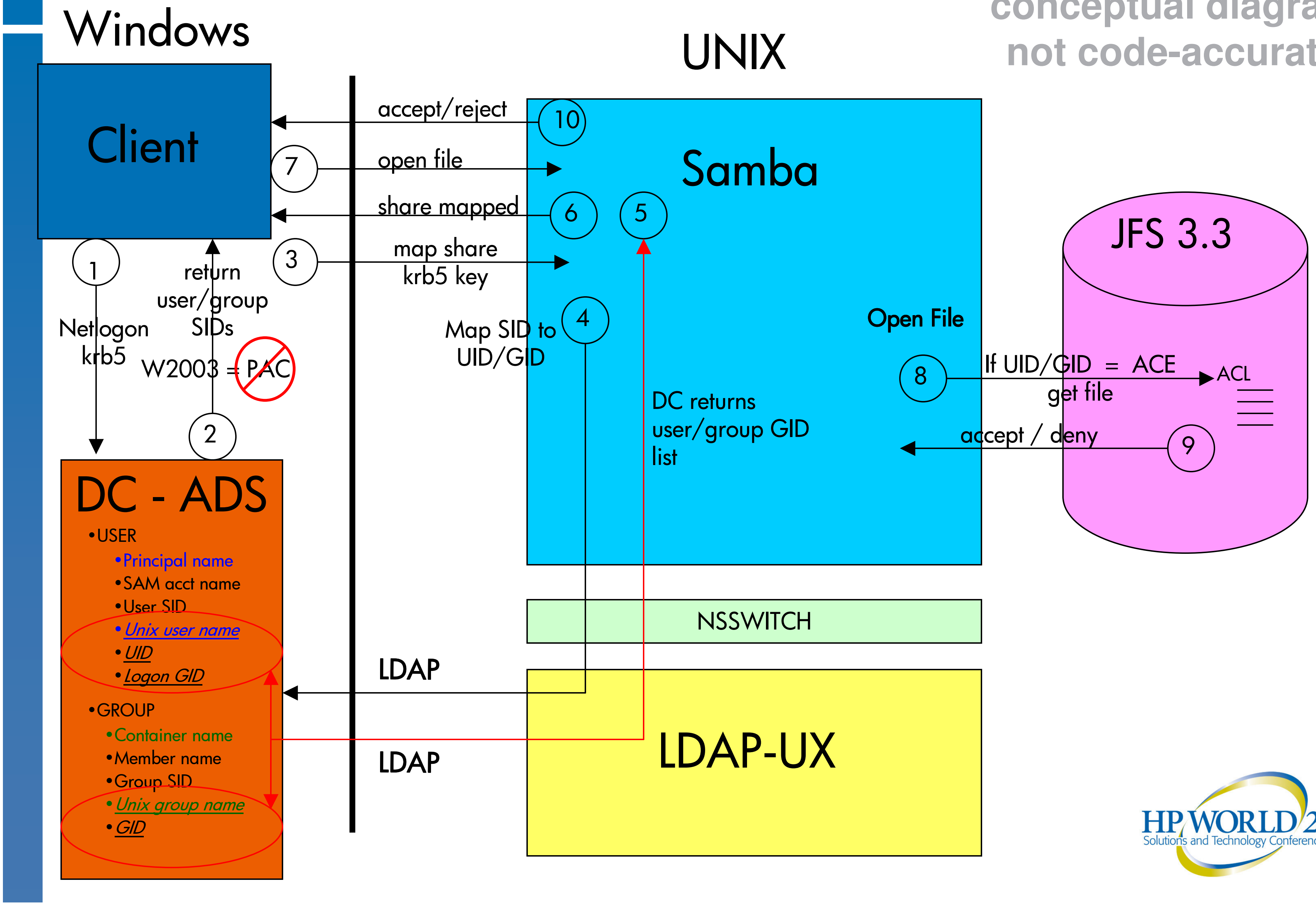
LDAD-UX ADS User Object

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: buffy anne. summers
sn: summers
givenName: buffy
initials: anne
distinguishedName: CN=buffy anne. summers,CN=Users,DC=atc-w2k3,DC=hp,DC=com
instanceType: 4
whenCreated: 20040630160732.0Z
whenChanged: 20040805235259.0Z
displayName: buffy anne. summers
uSNCreated: 95181
memberOf: CN=scoobies,CN=Users,DC=atc-w2k3,DC=hp,DC=com
memberOf: CN=Domain Admins,CN=Users,DC=atc-w2k3,DC=hp,DC=com
memberOf: CN=Administrators,CN=Builtin,DC=atc-w2k3,DC=hp,DC=com
uSNChanged: 127861
name: buffy anne. summers
objectGUID: da6323d8-a1e4-41e6-98b5-da6f58de4cc
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 127342972904218750
lastLogoff: 0
lastLogon: 127356090088593750
pwdLastSet: 127344058952812500
primaryGroupID: 513
objectSid: S-1-5-21-2101968314-3255136628-1516311335-1288
adminCount: 1
accountExpires: 9223372036854775807
logonCount: 90
sAMAccountName: buffy
sAMAccountType: 805306368
userPrincipalName: buffy@atc-w2k3.hp.com
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=atc-w2k3,DC=hp,DC=com
msSFU30Name: buffy
msSFU30UidNumber: 10001
msSFU30GidNumber: 10005
msSFU30LoginShell: /bin/sh
msSFU30Password: ABCD!efgh12345$67890
msSFU30NisDomain: atc-w2k3
msSFU30HomeDirectory: /home/buffy
```

UNIX Attributes

Block Diag: Client-Samba-LDAPUX-ADS

conceptual diagram
not code-accurate



W2003 and LDAP-UX Integration

- Configuration cookbook and details
- HPWorld 2004 Session ID 3202
  - Integrating HP-UX Authentication with Windows 2000 Active Directory
  - Doug Lamoureux
  - Wednesday at 4:00

ADS Integration: Summary

- What you need for ADS:
  - HP CIFS Server with Samba 3.0.4
  - Windows 2000/2003 KDC and ADS
  - HP-UX Kerberos Client 1.3.3
  - LDAP-UX (LDAP client libraries for HP-UX)
    - http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=J4269AA
  - Windows 2000/XP client
- What you get with ADS:
  - Kerberos authentication (no more NTLM pass-through)
  - ADS LDAP access
    - Join
    - Management (time sync, net commands, other stuff)

- Introduction
- Samba Version Tracking
- ADS Integration
- **LDAP and Directory Servers**
- Authentication
- Net Commands
- New and Changed Tools and Parameters
- Performance Enhancements and Recommendations
- Summary

LDAP and Directory Servers

- Centralize and Optimize Samba User Data Store

- Traditional User Data Stores: Flat Files
  - /etc/passwd
  - /var/opt/samba/private/smbpasswd
- Disadvantages
  - Sequential access
  - Distributed, duplicated versions
  - Static data store layout
  - Security

LDAP and Directory Servers

- Directory Advantages
  - LDAP Access – non-sequential
  - Centralized Storage and Administration
  - Secure System with SSL Access
  - Extensible, customizable
- Enables Back-up Data Store
  - Back-up Domain Controller function similarity
  - Multiple, distributed, replicated directories
  - Not identical to Windows BDC – multi-DC domains

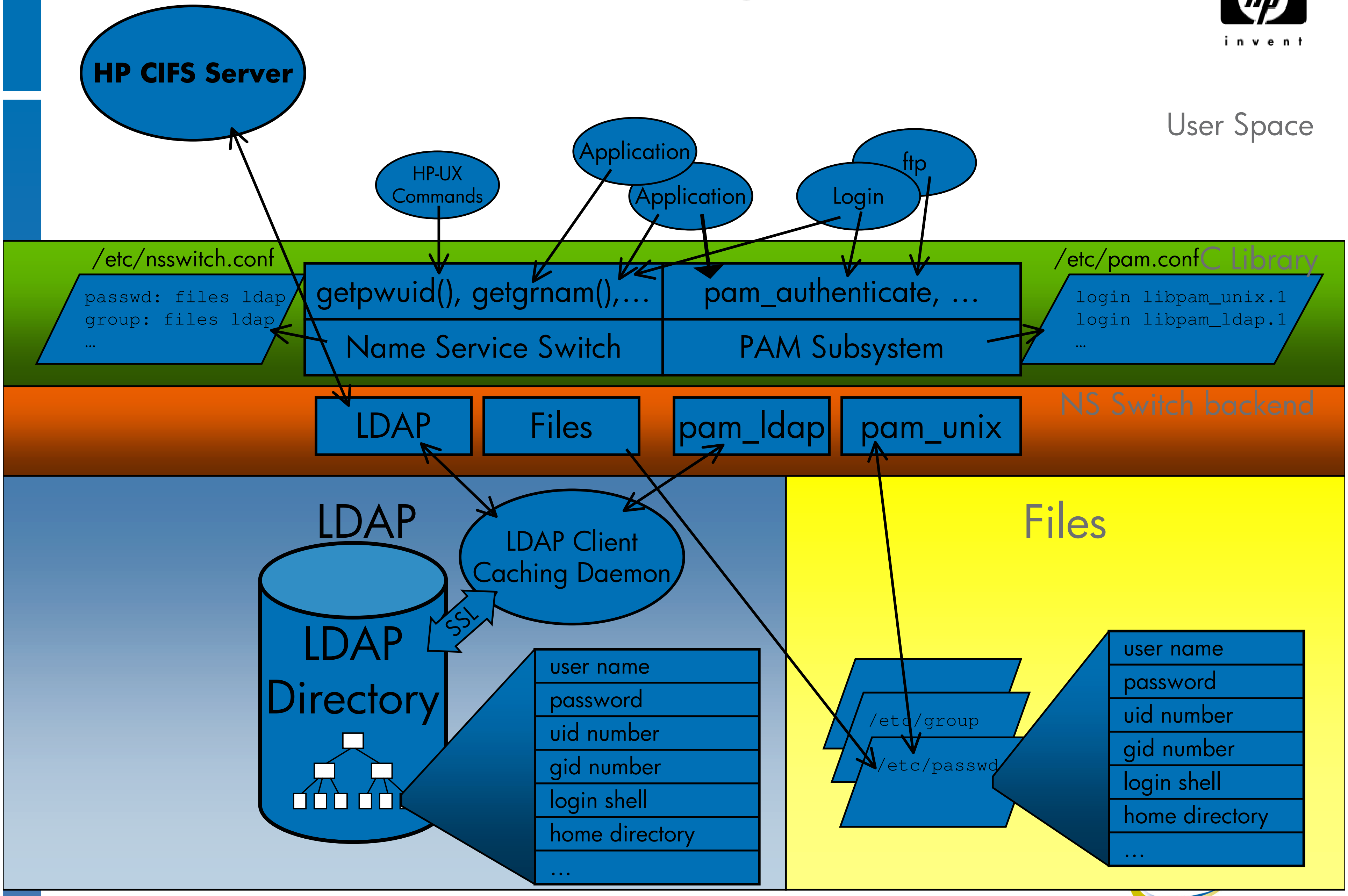
LDAP and Directory Servers

- NOT a Samba authentication mechanism
- Must be combined with authentication
  - Kerberos – next module
  - NTLMv1, NTLMv2
  - PAM

LDAP-UX

- LDAP Integration for HP-UX
  - LDAP-UX client required for CIFS LDAP Access
  - Download the latest version at:
    - http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=J4269AALDAP-UX
- LDAP-UX and HP CIFS Server
  - Direct directory access
  - Does not use interface
    - nsswitch
    - PAM

LDAP-UX



HP CIFS Server

User Space

HP-UX Commands

Application

Application

Login

ftp

C Library

/etc/nsswitch.conf

```
passwd: files ldap
group: files ldap
…
```

getpwuid(), getgrnam(),…

Name Service Switch

pam_authenticate, …

PAM Subsystem

/etc/pam.conf

```
login libpam_unix.1
login libpam_ldap.1
…
```

NS Switch backend

LDAP

Files

pam_ldap

pam_unix

LDAP

LDAP Client Caching Daemon

SSL

LDAP Directory

user name
password
uid number
gid number
login shell
home directory
…

Files

/etc/group

/etc/passwd

user name
password
uid number
gid number
login shell
home directory
…

Directory Types

- HP-UX Netscape Directory Server
  - HP CIFS Server tested and supported
  - Free Directory Server with HP-UX
  - Version 6
  - Download the latest version at:
    - http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=J4258CA

- Cookbook Whitepaper
  - "Setting Up HP CIFS Server (Samba) in an LDAP Environment"
  - http://www.docs.hp.com/hpux/onlinedocs/5523/wp-SettingUpSambainanLDAPEnvironment.pdf
  - By Don McCall – HP GSE-WTEC
  - Outstanding tool to help simplify a complex operation

Directory Types

- OpenLDAP
  - Not Supported (yet) for HP CIFS Server
  - Samba tested and supported
  - Free Directory Server
  - Download at:
    - http://www.openldap.org/
- Novell eDirectory, IBM Tivoli, etc
  - Not supported for HP CIFS Server
  - Not supported for Samba
  - But works – opensource customers have been successful
- Active Directory
  - Special case, as seen earlier
  - Requires separate POSIX data stores
    - Unless enhanced with HP-UX LDAP Integration
  - Requires entirely different smb.conf configuration
  - Next Step: Test with ADAM

HP-UX Netscape Directory Server

- Netscape Directory Server Version 6.02
- Delivered with default RFC 2307 POSIX schema
  - posixAccount objectclass
- Most schemas are highly customized
- HP CIFS Server requires schema extensions for Samba
  - Delivered with sambaSamAccount objectclass
- Must use both
  - posixAccount objectclass
  - sambaSamAccount obectclass

User Account Example LDIF

```
dn: uid=eroseme, ou=people,dc=hp,dc=com
logonTime: 0
displayName: Eric Roseme
sambaLMPassword: 552902031BEDE9EFAAD3B435B51404EE
sambaPrimaryGroupSID: S-1-5-21-4783487287-3264376347-4637238327-1011
objectClass: posixAccount
objectClass: sambaAccount
sambaAcctFlags: [UX         ]
userPassword: {crypt}GeD9hw9D12
uid: eroseme
uidNumber: 104
cn: Eric Roseme
loginShell: /bin/bash
logoffTime: 2147483647
gidNumber: 100
sambaKickoffTime: 2147483647
sambaPwdLastSet: 1010179230
sambaSID: S-1-5-21-4783487287-3264376347-4637238327-5599
homeDirectory: /home/eroseme
sambaPwdCanChange: 0
sambaPwdMustChange: 2147483647
sambaNTPassword: 878D8014606CDA29677A44EFA1353FC7
```

Windows Active Directory

- LDAP Access for domain objects
- Directory store for server and Windows users
- Not configurable as “passdb = ldapsam”
  - Only as “security = ads”
  - Lacks flexibility of “passdb = ldapsam”
- Standard Samba Interoperability
  - Requires separate POSIX user data store
  - Flat files or winbind
  - Dual administration
- See ADS Integration Module

AS/U Migration Enabler

- BDC support is key AS/U migration concern
- Samba BDC support provides alternative
- HP Provides a BDC setup and Config guide
  - For HP CIFS Server
  - With LDAP backend
- Data migration
  - net rpc vampire

Pseudo BDC Support

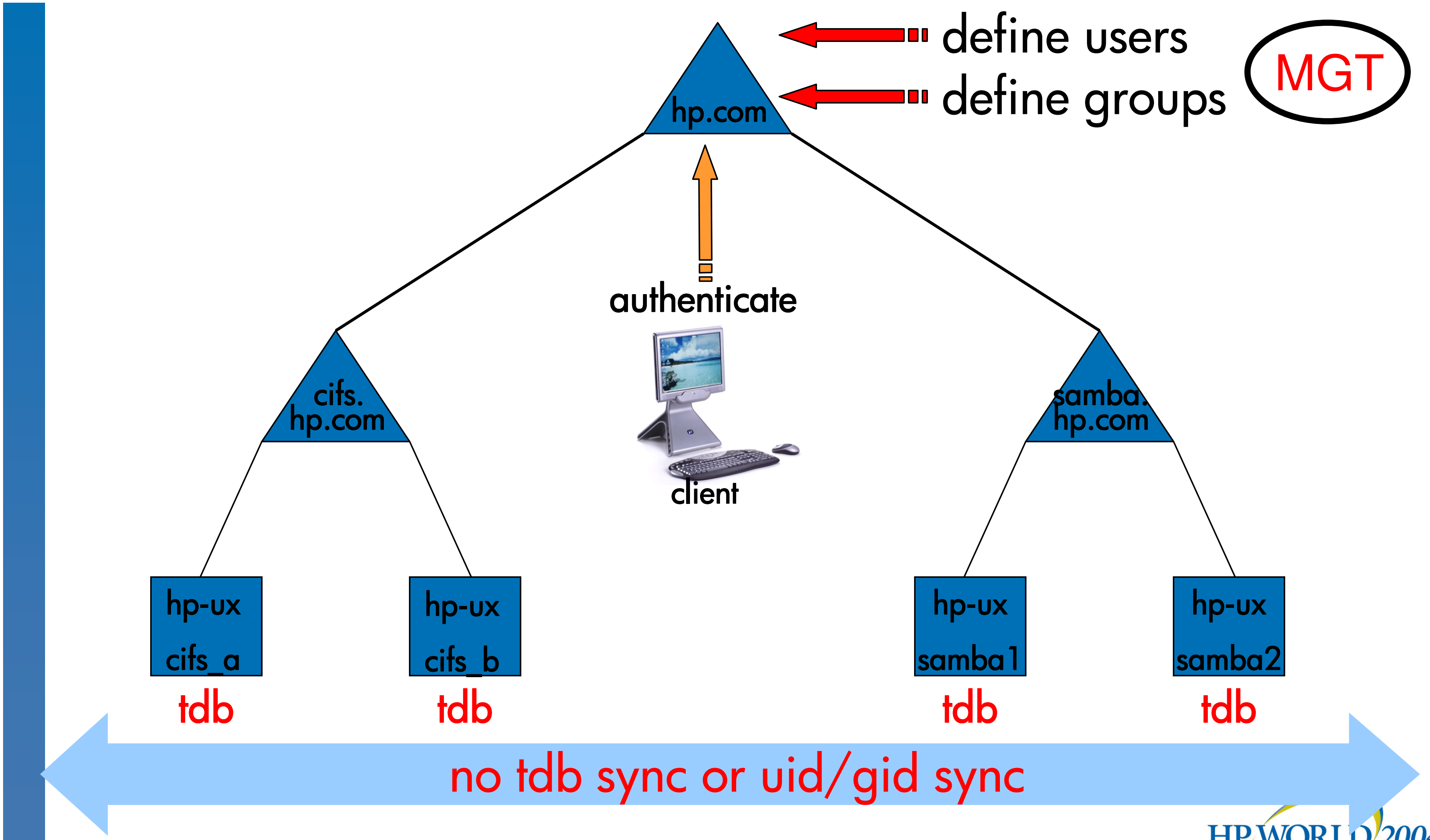
- Samba BDC is NOT:
  - Windows SAM BDC replication
  - Integrate-able within a Windows Domain (DC or BDC)
  - A replacement for AS/U PDC/BDC behavior

- Samba BDC is:
  - Recommended primarily with LDAP passdb
  - Not recommended with
    - tdb passdb
    - smbpasswd passdb
  - Effectively provides backup domain authentication
  - Great for non-Windows server autonomy

LDAP Directory winbind Backend

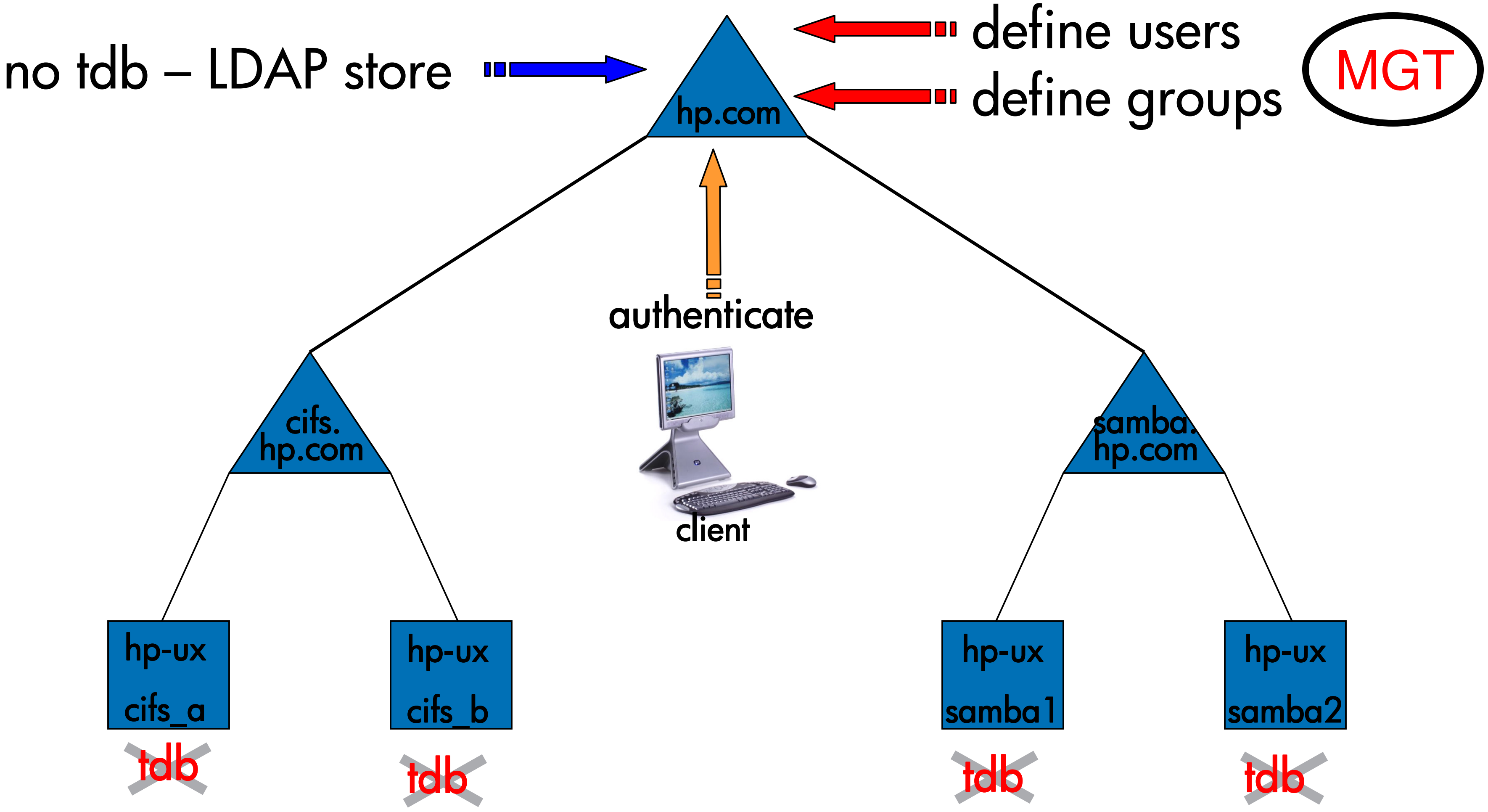
- LDAP winbind mapping backend
  - Central repository of winbind mapping
  - For multi-node Samba server farm
- Solves distributed per-server mapping
  - In separate .tdb databases
  - Therefore, inconsistent mappings for multiple nodes
- LDAP winbind backend configurable with
  - Smb.conf “idmap backend = ldap://config”

winbind tdb backend

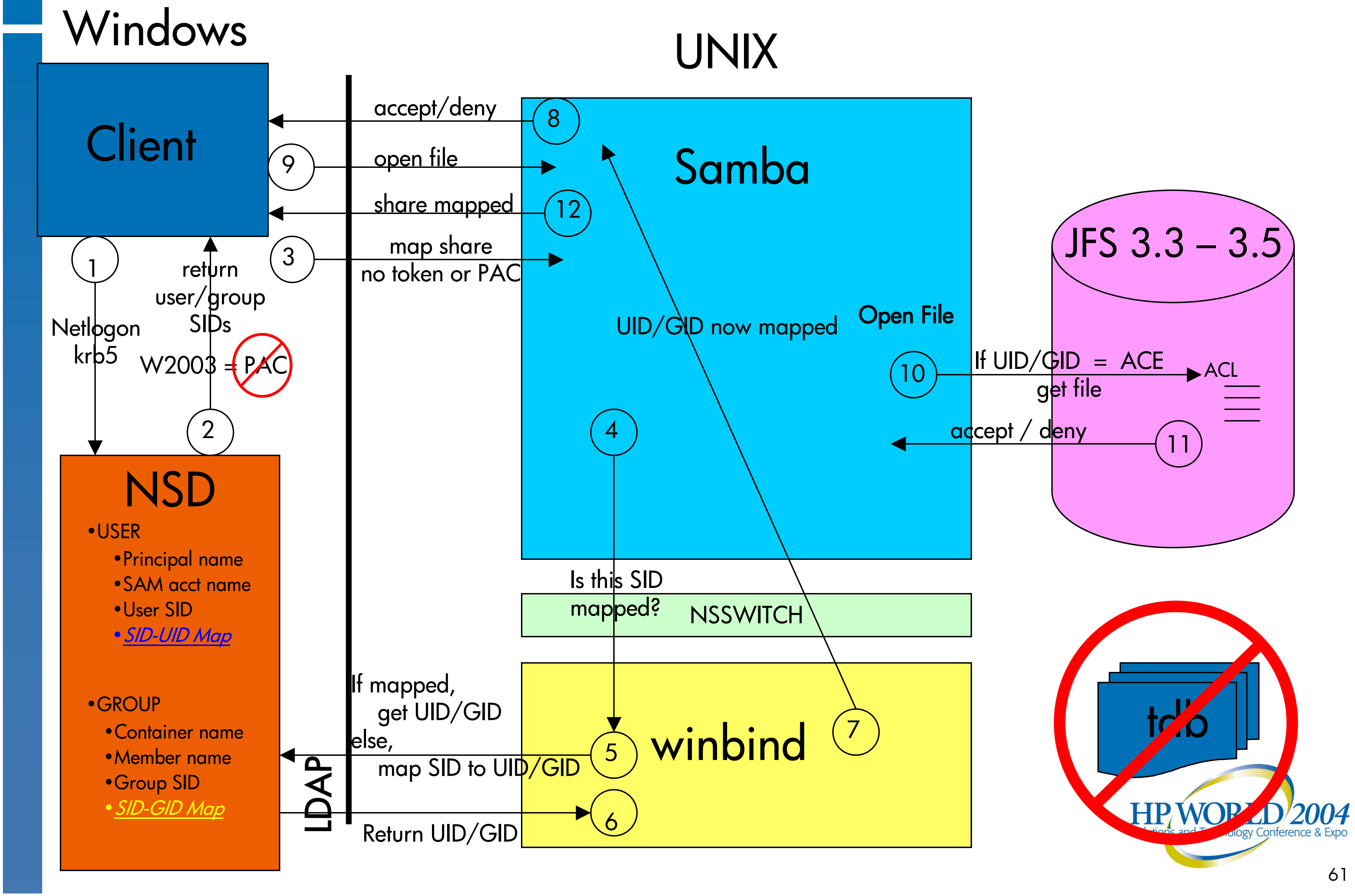


HP WORLD 2004
Solutions and Technology Conference & Expo

winbind LDAP backend



Samba 3.0 winbind with LDAP Client Access



- Introduction
- Samba Version Tracking
- ADS Integration
- LDAP and Directory Servers
- **Authentication**
- Net Commands
- New and Changed Tools and Parameters
- Performance Enhancements and Recommendations
- Summary

User Authentication with Samba 3.0

- Kerberos New!
- NTLMv2 New!
- NTLM

CIFS and HP-UX Kerberos Co-Existence

- Currently CIFS and HP-UX Kerberos:
  - Are not synchronized on a system
  - Samba stores encrypted password in
    - /var/opt/samba/private/secrets.tdb
  - HP-UX stores encrypted password in
    - /etc/krb5.keytab
- Thus, the keytabs are not synched
  - Results in mis-matches with KDC
- Enhancement coming for system keytab access

CIFS and HP-UX Kerberos Co-Existence

- Currently CIFS and HP-UX Kerberos:
  - Can be manually synchronized for co-existence!

- Secrets.tdb = /etc/krb5.keytab
  - All modifications manually synchronized
- Steps:
  - Net ads join –U administrator%password
    - Creates machine account password in secrets.tdb
  - Net ads showpass
    - Displays machine account password
  - On ADS DC, create keytab, map machine-host accounts
    - Use ktpass command
- Details in notes: (prototype by Doug Lamoureux)

Kerberos

- Kerberos with Active Directory KDC
  - Windows 2000 KDC
  - Windows 2003 KDC
- Kerberos with HP-UX Kerberos Server (Cybersafe)
  - Under development
  - XP client can get ticket, but Samba cannot process it
  - http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1417AA
- Kerberos with MIT Kerberos (non-Windows)
  - Under development
- Kerberos with Heimdal
  - Under development

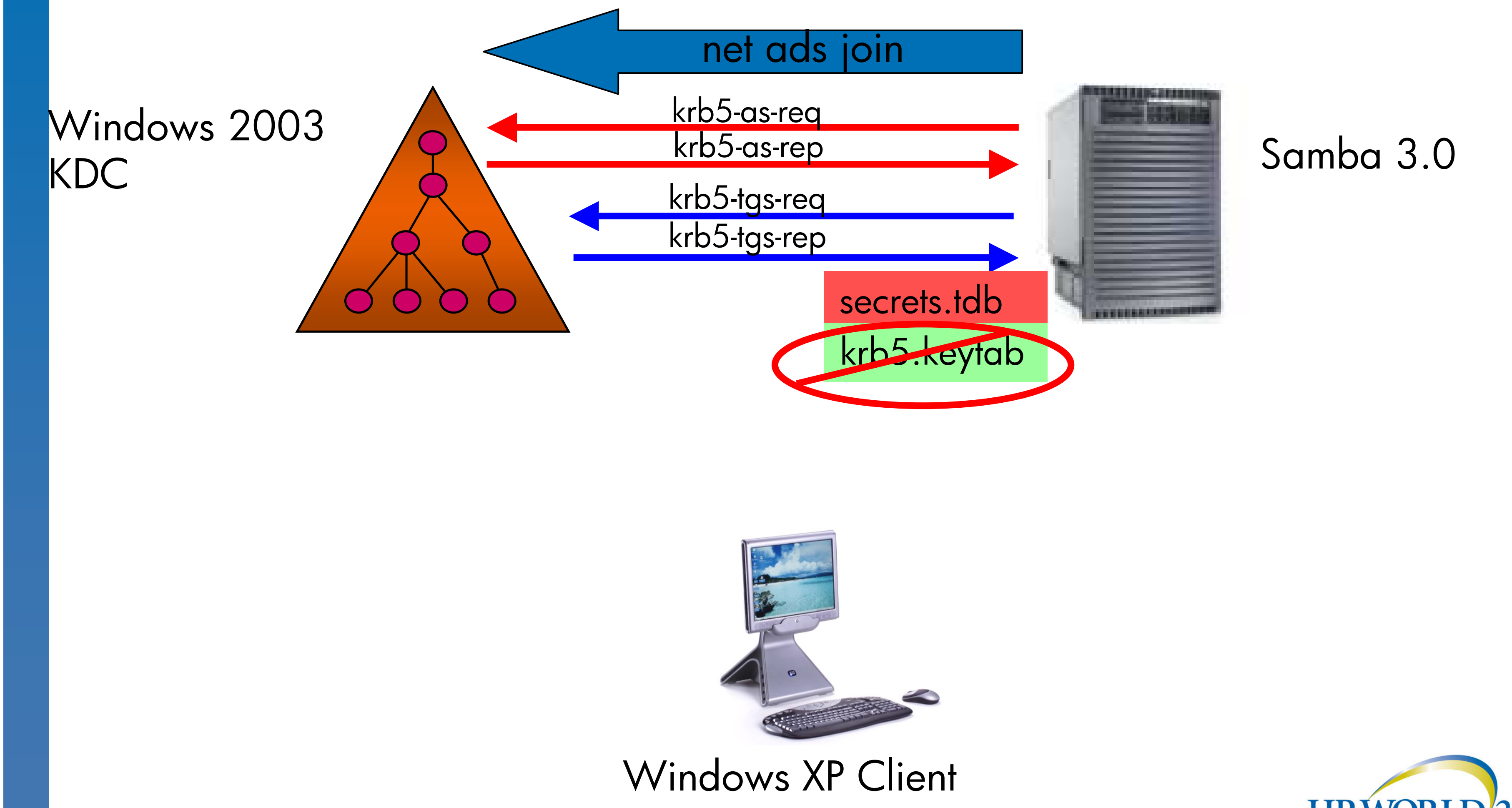
Kerberos: Windows KDC

- “security = ads”
  - Enables Kerberos Authentication
  - Client can negotiate down
    - NTLMv2 (cannot negotiate down from here)
    - NTLM
- smb.conf configuration
- /etc/krb.conf configuration
- Kerberos client library dependency

Kerberos: to Windows 2003 KDC

- May require compatibility components
- Potential Pre-requisites
  - HP-UX KRB5 Client version 1.3.3
    - For RC4-HMAC default encryption
  - W2003 KDC hotfix
    - Q833708 – Allow enctypes (MD5, CRC)
  - CIFS Server based upon Samba 3.0.4
    - Not Samba 3.0.2

Kerberos Sequence – Join Domain



Windows 2003
KDC

net ads join

krb5-as-req

krb5-as-rep

krb5-tgs-req

krb5-tgs-rep

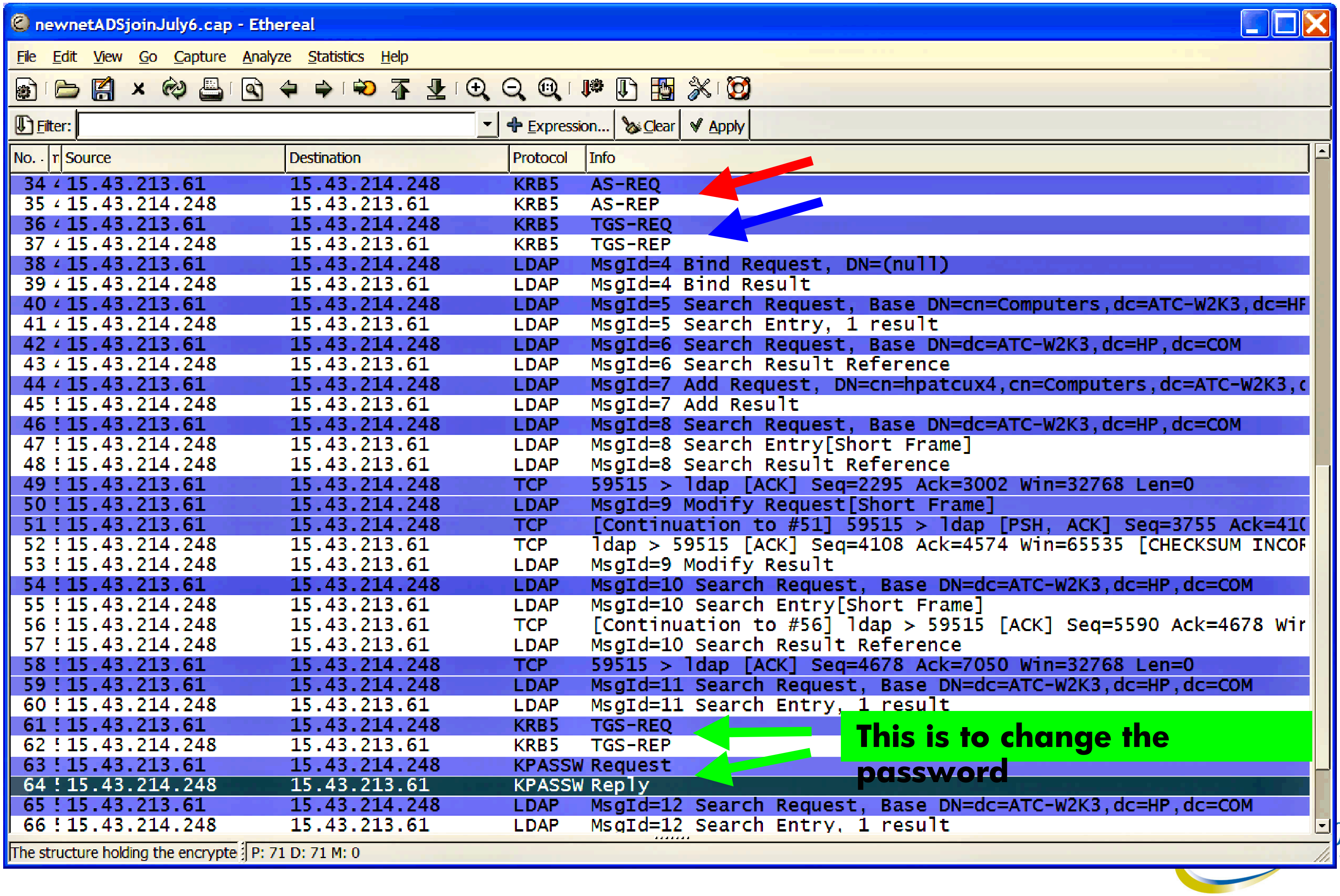
secrets.tdb

~~krb5.keytab~~

Samba 3.0

Windows XP Client

KRB5 Events - Net ADS join

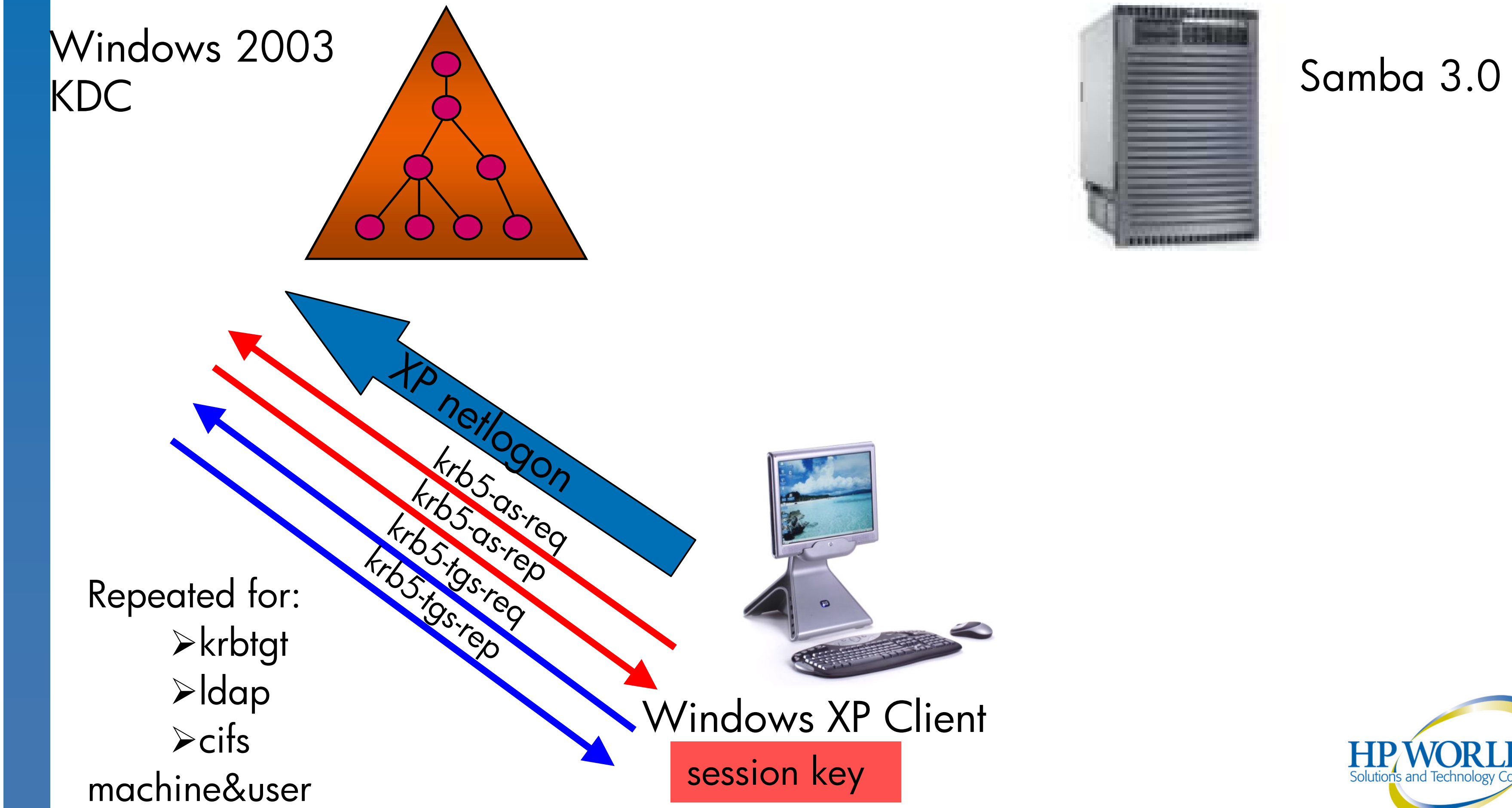


No.	r	Source	Destination	Protocol	Info
34	4	15.43.213.61	15.43.214.248	KRB5	AS-REQ
35	4	15.43.214.248	15.43.213.61	KRB5	AS-REP
36	4	15.43.213.61	15.43.214.248	KRB5	TGS-REQ
37	4	15.43.214.248	15.43.213.61	KRB5	TGS-REP
38	4	15.43.213.61	15.43.214.248	LDAP	MsgId=4 Bind Request, DN=(null)
39	4	15.43.214.248	15.43.213.61	LDAP	MsgId=4 Bind Result
40	4	15.43.213.61	15.43.214.248	LDAP	MsgId=5 Search Request, Base DN=cn=Computers,dc=ATC-W2K3,dc=HF
41	4	15.43.214.248	15.43.213.61	LDAP	MsgId=5 Search Entry, 1 result
42	4	15.43.213.61	15.43.214.248	LDAP	MsgId=6 Search Request, Base DN=dc=ATC-W2K3,dc=HP,dc=COM
43	4	15.43.214.248	15.43.213.61	LDAP	MsgId=6 Search Result Reference
44	4	15.43.213.61	15.43.214.248	LDAP	MsgId=7 Add Request, DN=cn=hpatcux4,cn=Computers,dc=ATC-W2K3,c
45	5	15.43.214.248	15.43.213.61	LDAP	MsgId=7 Add Result
46	5	15.43.213.61	15.43.214.248	LDAP	MsgId=8 Search Request, Base DN=dc=ATC-W2K3,dc=HP,dc=COM
47	5	15.43.214.248	15.43.213.61	LDAP	MsgId=8 Search Entry[Short Frame]
48	5	15.43.214.248	15.43.213.61	LDAP	MsgId=8 Search Result Reference
49	5	15.43.213.61	15.43.214.248	TCP	59515 > ldap [ACK] Seq=2295 Ack=3002 Win=32768 Len=0
50	5	15.43.213.61	15.43.214.248	LDAP	MsgId=9 Modify Request[Short Frame]
51	5	15.43.213.61	15.43.214.248	TCP	[Continuation to #51] 59515 > ldap [PSH, ACK] Seq=3755 Ack=41(
52	5	15.43.214.248	15.43.213.61	TCP	ldap > 59515 [ACK] Seq=4108 Ack=4574 Win=65535 [CHECKSUM INCOF
53	5	15.43.214.248	15.43.213.61	LDAP	MsgId=9 Modify Result
54	5	15.43.213.61	15.43.214.248	LDAP	MsgId=10 Search Request, Base DN=dc=ATC-W2K3,dc=HP,dc=COM
55	5	15.43.214.248	15.43.213.61	LDAP	MsgId=10 Search Entry[Short Frame]
56	5	15.43.214.248	15.43.213.61	TCP	[Continuation to #56] ldap > 59515 [ACK] Seq=5590 Ack=4678 Wir
57	5	15.43.214.248	15.43.213.61	LDAP	MsgId=10 Search Result Reference
58	5	15.43.213.61	15.43.214.248	TCP	59515 > ldap [ACK] Seq=4678 Ack=7050 Win=32768 Len=0
59	5	15.43.213.61	15.43.214.248	LDAP	MsgId=11 Search Request, Base DN=dc=ATC-W2K3,dc=HP,dc=COM
60	5	15.43.214.248	15.43.213.61	LDAP	MsgId=11 Search Entry, 1 result
61	5	15.43.213.61	15.43.214.248	KRB5	TGS-REQ
62	5	15.43.214.248	15.43.213.61	KRB5	TGS-REP
63	5	15.43.213.61	15.43.214.248	KPASSW	Request
64	5	15.43.214.248	15.43.213.61	KPASSW	Reply
65	5	15.43.213.61	15.43.214.248	LDAP	MsgId=12 Search Request, Base DN=dc=ATC-W2K3,dc=HP,dc=COM
66	5	15.43.214.248	15.43.213.61	LDAP	MsgId=12 Search Entry, 1 result

The structure holding the encrypte | P: 71 D: 71 M: 0

This is to change the password

Kerberos Sequence - Netlogon



Windows 2003 KDC

Samba 3.0

Windows XP Client

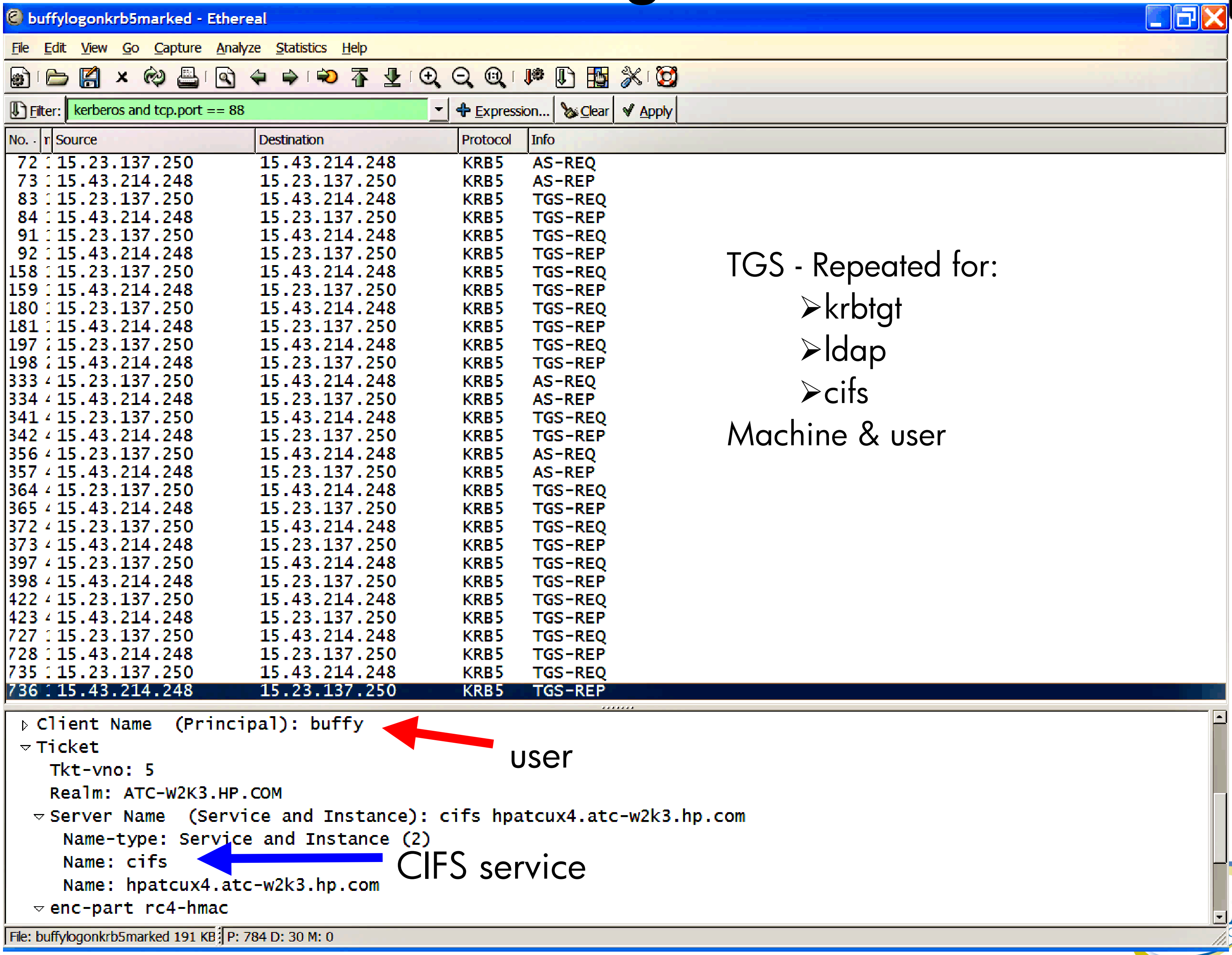
session key

Repeated for:

- krbtgt
- ldap
- cifs

machine&user

KRB5 Events - Netlogon



Filter: kerberos and tcp.port == 88

```
No. . r Source              Destination         Protocol  Info
 72 : 15.23.137.250         15.43.214.248       KRB5      AS-REQ
 73 : 15.43.214.248         15.23.137.250       KRB5      AS-REP
 83 : 15.23.137.250         15.43.214.248       KRB5      TGS-REQ
 84 : 15.43.214.248         15.23.137.250       KRB5      TGS-REP
 91 : 15.23.137.250         15.43.214.248       KRB5      TGS-REQ
 92 : 15.43.214.248         15.23.137.250       KRB5      TGS-REP
158 1 15.23.137.250         15.43.214.248       KRB5      TGS-REQ
159 1 15.43.214.248         15.23.137.250       KRB5      TGS-REP
180 1 15.23.137.250         15.43.214.248       KRB5      TGS-REQ
181 1 15.43.214.248         15.23.137.250       KRB5      TGS-REP
197 2 15.23.137.250         15.43.214.248       KRB5      TGS-REQ
198 2 15.43.214.248         15.23.137.250       KRB5      TGS-REP
333 4 15.23.137.250         15.43.214.248       KRB5      AS-REQ
334 4 15.43.214.248         15.23.137.250       KRB5      AS-REP
341 4 15.23.137.250         15.43.214.248       KRB5      TGS-REQ
342 4 15.43.214.248         15.23.137.250       KRB5      TGS-REP
356 4 15.23.137.250         15.43.214.248       KRB5      AS-REQ
357 4 15.43.214.248         15.23.137.250       KRB5      AS-REP
364 4 15.23.137.250         15.43.214.248       KRB5      TGS-REQ
365 4 15.43.214.248         15.23.137.250       KRB5      TGS-REP
372 4 15.23.137.250         15.43.214.248       KRB5      TGS-REQ
373 4 15.43.214.248         15.23.137.250       KRB5      TGS-REP
397 4 15.23.137.250         15.43.214.248       KRB5      TGS-REQ
398 4 15.43.214.248         15.23.137.250       KRB5      TGS-REP
422 4 15.23.137.250         15.43.214.248       KRB5      TGS-REQ
423 4 15.43.214.248         15.23.137.250       KRB5      TGS-REP
727 1 15.23.137.250         15.43.214.248       KRB5      TGS-REQ
728 1 15.43.214.248         15.23.137.250       KRB5      TGS-REP
735 1 15.23.137.250         15.43.214.248       KRB5      TGS-REQ
736 1 15.43.214.248         15.23.137.250       KRB5      TGS-REP
```

```
▷ Client Name  (Principal): buffy
▽ Ticket
    Tkt-vno: 5
    Realm: ATC-W2K3.HP.COM
  ▽ Server Name  (Service and Instance): cifs hpatcux4.atc-w2k3.hp.com
      Name-type: Service and Instance (2)
      Name: cifs
      Name: hpatcux4.atc-w2k3.hp.com
  ▽ enc-part rc4-hmac
```

File: buffylogonkrb5marked 191 KB | P: 784 D: 30 M: 0

user

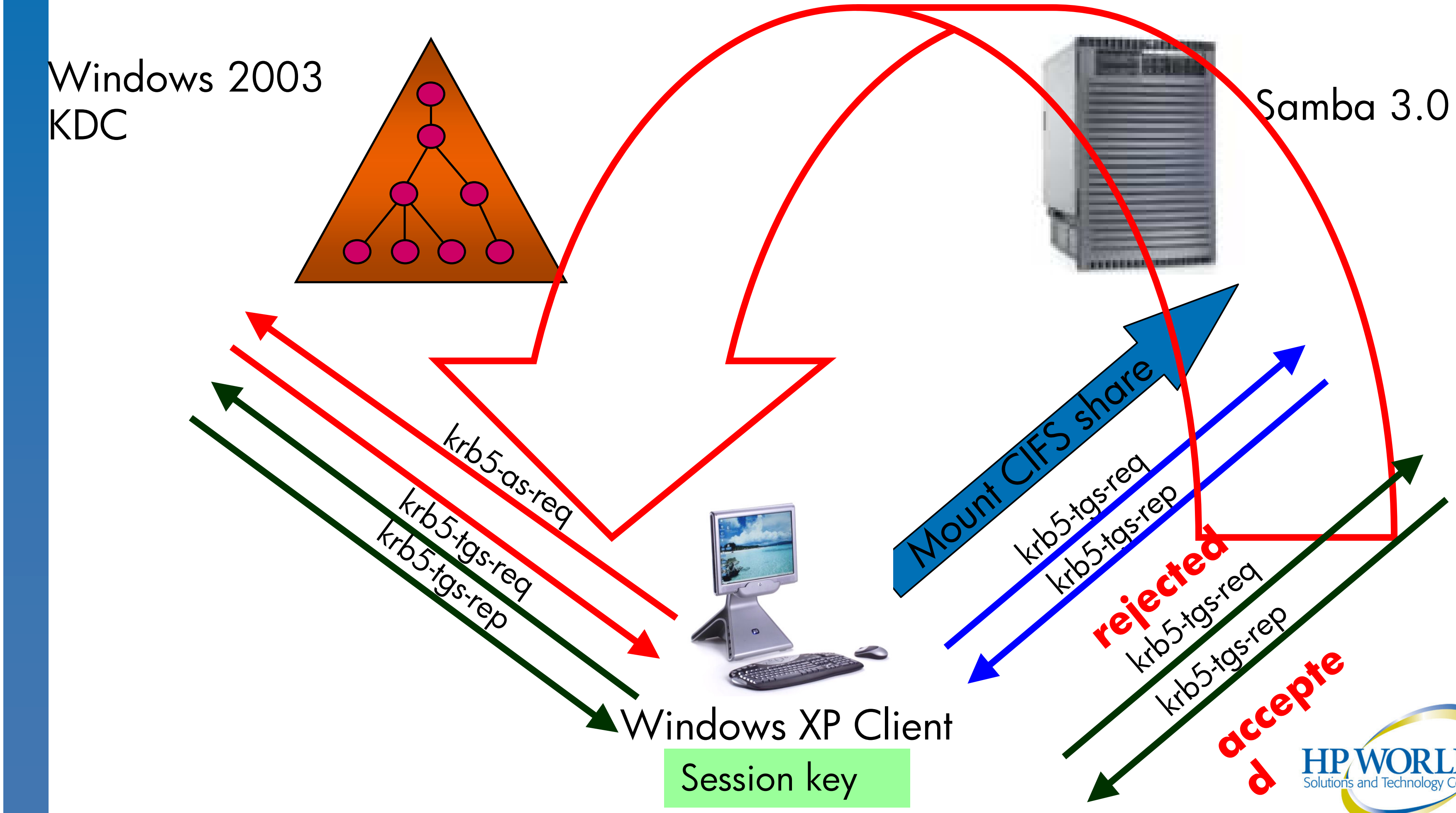
CIFS service

TGS - Repeated for:

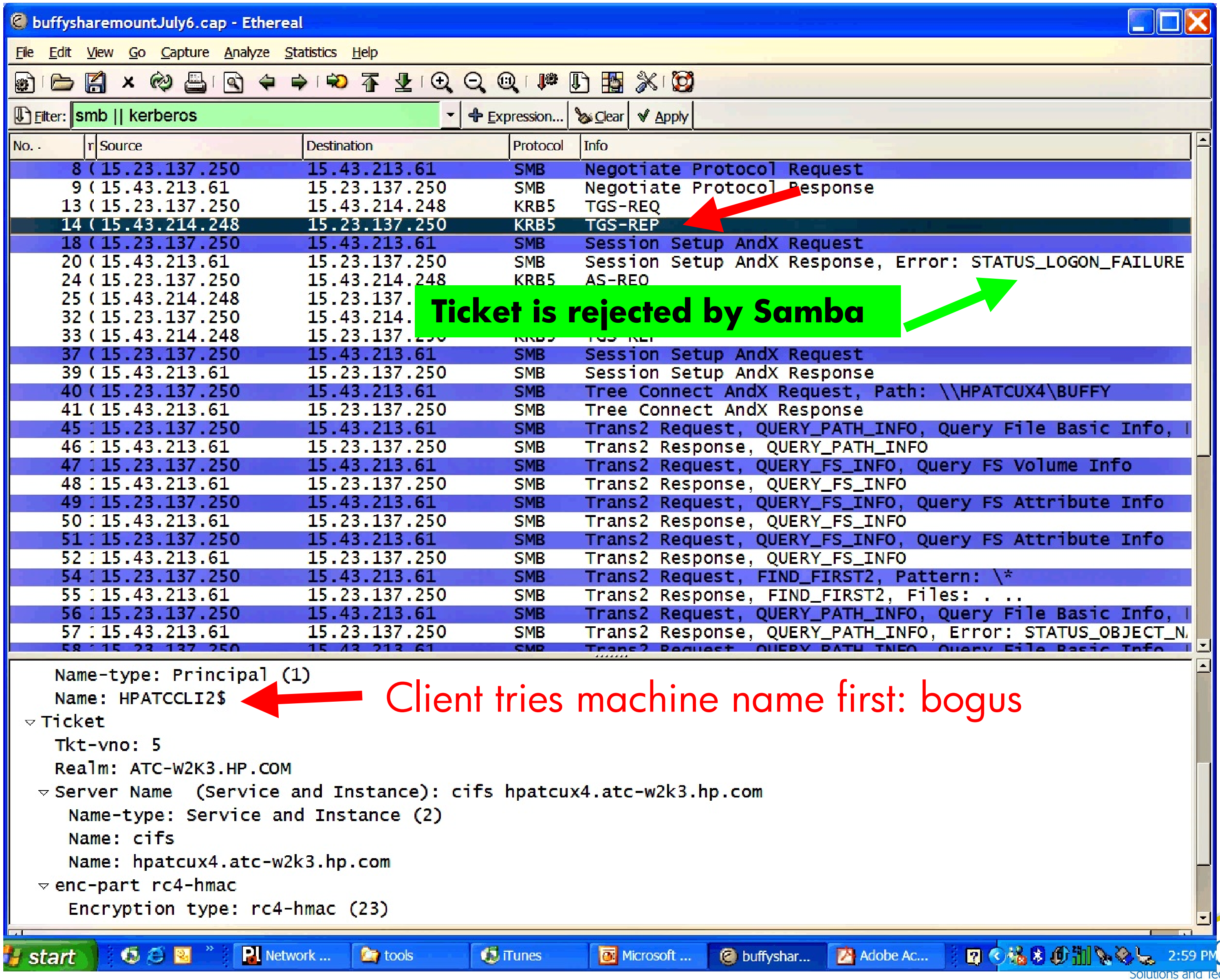
- krbtgt
- ldap
- cifs

Machine & user

Kerberos Sequence – CIFS Share



KRB5 Events – Share (bad name)


buffysharemountJuly6.cap - Ethereal
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply
start Network ... tools iTunes Microsoft ... buffyshar... Adobe Ac... 2:59 PM

Filter: smb || kerberos

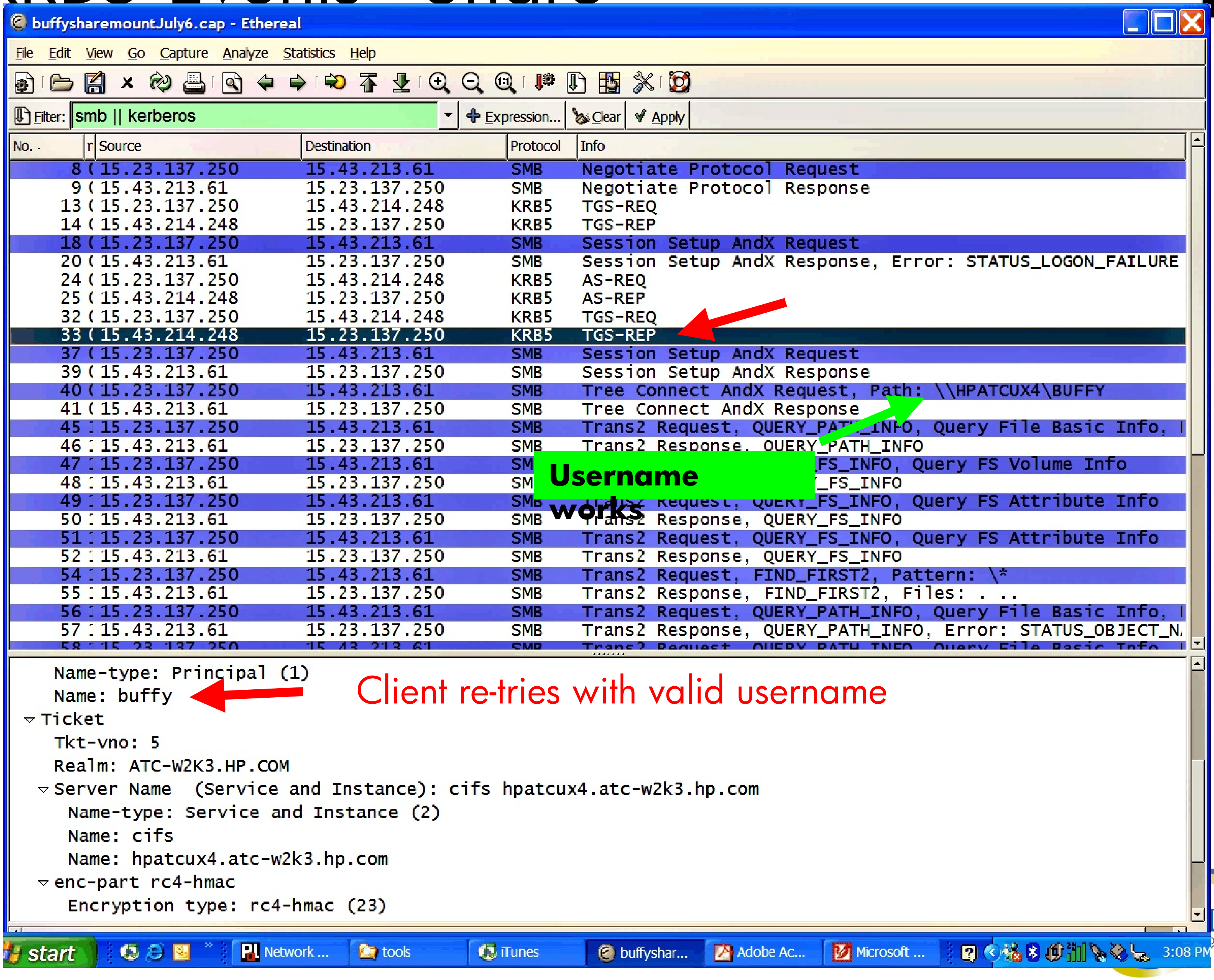
```
No. . r Source           Destination      Protocol  Info
    8 ( 15.23.137.250    15.43.213.61     SMB       Negotiate Protocol Request
    9 ( 15.43.213.61     15.23.137.250    SMB       Negotiate Protocol Response
   13 ( 15.23.137.250    15.43.214.248    KRB5      TGS-REQ
   14 ( 15.43.214.248    15.23.137.250    KRB5      TGS-REP
   18 ( 15.23.137.250    15.43.213.61     SMB       Session Setup AndX Request
   20 ( 15.43.213.61     15.23.137.250    SMB       Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
   24 ( 15.23.137.250    15.43.214.248    KRB5      AS-REQ
   25 ( 15.43.214.248    15.23.137.
   32 ( 15.23.137.250    15.43.214.
   33 ( 15.43.214.248    15.23.137.
   37 ( 15.23.137.250    15.43.213.61     SMB       Session Setup AndX Request
   39 ( 15.43.213.61     15.23.137.250    SMB       Session Setup AndX Response
   40 ( 15.23.137.250    15.43.213.61     SMB       Tree Connect AndX Request, Path: \\HPATCUX4\BUFFY
   41 ( 15.43.213.61     15.23.137.250    SMB       Tree Connect AndX Response
   45 : 15.23.137.250    15.43.213.61     SMB       Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, |
   46 : 15.43.213.61     15.23.137.250    SMB       Trans2 Response, QUERY_PATH_INFO
   47 : 15.23.137.250    15.43.213.61     SMB       Trans2 Request, QUERY_FS_INFO, Query FS Volume Info
   48 : 15.43.213.61     15.23.137.250    SMB       Trans2 Response, QUERY_FS_INFO
   49 : 15.23.137.250    15.43.213.61     SMB       Trans2 Request, QUERY_FS_INFO, Query FS Attribute Info
   50 : 15.43.213.61     15.23.137.250    SMB       Trans2 Response, QUERY_FS_INFO
   51 : 15.23.137.250    15.43.213.61     SMB       Trans2 Request, QUERY_FS_INFO, Query FS Attribute Info
   52 : 15.43.213.61     15.23.137.250    SMB       Trans2 Response, QUERY_FS_INFO
   54 : 15.23.137.250    15.43.213.61     SMB       Trans2 Request, FIND_FIRST2, Pattern: \*
   55 : 15.43.213.61     15.23.137.250    SMB       Trans2 Response, FIND_FIRST2, Files: . ..
   56 : 15.23.137.250    15.43.213.61     SMB       Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, |
   57 : 15.43.213.61     15.23.137.250    SMB       Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_N
   58 : 15.23.137.250    15.43.213.61     SMB       Trans2 Request, QUERY_PATH_INFO, Query File Basic Info
```

Ticket is rejected by Samba

```
    Name-type: Principal (1)
    Name: HPATCCLI2$
  ▽ Ticket
    Tkt-vno: 5
    Realm: ATC-W2K3.HP.COM
  ▽ Server Name  (Service and Instance): cifs hpatcux4.atc-w2k3.hp.com
      Name-type: Service and Instance (2)
      Name: cifs
      Name: hpatcux4.atc-w2k3.hp.com
  ▽ enc-part rc4-hmac
      Encryption type: rc4-hmac (23)
```

Client tries machine name first: bogus

KRB5 Events - Share


buffysharemountJuly6.cap - Ethereal
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply
start Network ... tools iTunes buffyshar... Adobe Ac... Microsoft ... 3:08 PM

Filter: smb || kerberos

```
No. . r Source            Destination      Protocol Info
   8 ( 15.23.137.250      15.43.213.61     SMB      Negotiate Protocol Request
   9 ( 15.43.213.61       15.23.137.250    SMB      Negotiate Protocol Response
  13 ( 15.23.137.250      15.43.214.248    KRB5     TGS-REQ
  14 ( 15.43.214.248      15.23.137.250    KRB5     TGS-REP
  18 ( 15.23.137.250      15.43.213.61     SMB      Session Setup AndX Request
  20 ( 15.43.213.61       15.23.137.250    SMB      Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
  24 ( 15.23.137.250      15.43.214.248    KRB5     AS-REQ
  25 ( 15.43.214.248      15.23.137.250    KRB5     AS-REP
  32 ( 15.23.137.250      15.43.214.248    KRB5     TGS-REQ
  33 ( 15.43.214.248      15.23.137.250    KRB5     TGS-REP
  37 ( 15.23.137.250      15.43.213.61     SMB      Session Setup AndX Request
  39 ( 15.43.213.61       15.23.137.250    SMB      Session Setup AndX Response
  40 ( 15.23.137.250      15.43.213.61     SMB      Tree Connect AndX Request, Path: \\HPATCUX4\BUFFY
  41 ( 15.43.213.61       15.23.137.250    SMB      Tree Connect AndX Response
  45 : 15.23.137.250      15.43.213.61     SMB      Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, I
  46 : 15.43.213.61       15.23.137.250    SMB      Trans2 Response, QUERY_PATH_INFO
  47 : 15.23.137.250      15.43.213.61     SM       _FS_INFO, Query FS Volume Info
  48 : 15.43.213.61       15.23.137.250    SM       _FS_INFO
  49 : 15.23.137.250      15.43.213.61     SMB      Trans2 Request, QUERY_FS_INFO, Query FS Attribute Info
  50 : 15.43.213.61       15.23.137.250    SMB      Trans2 Response, QUERY_FS_INFO
  51 : 15.23.137.250      15.43.213.61     SMB      Trans2 Request, QUERY_FS_INFO, Query FS Attribute Info
  52 : 15.43.213.61       15.23.137.250    SMB      Trans2 Response, QUERY_FS_INFO
  54 : 15.23.137.250      15.43.213.61     SMB      Trans2 Request, FIND_FIRST2, Pattern: \*
  55 : 15.43.213.61       15.23.137.250    SMB      Trans2 Response, FIND_FIRST2, Files: . ..
  56 : 15.23.137.250      15.43.213.61     SMB      Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, I
  57 : 15.43.213.61       15.23.137.250    SMB      Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_N.
  58 : 15.23.137.250      15.43.213.61     SMB      Trans2 Request, QUERY_PATH_INFO, Query File Basic Info
```

```
  Name-type: Principal (1)
  Name: buffy
▽ Ticket
  Tkt-vno: 5
  Realm: ATC-W2K3.HP.COM
 ▽ Server Name (Service and Instance): cifs hpatcux4.atc-w2k3.hp.com
   Name-type: Service and Instance (2)
   Name: cifs
   Name: hpatcux4.atc-w2k3.hp.com
 ▽ enc-part rc4-hmac
   Encryption type: rc4-hmac (23)
```

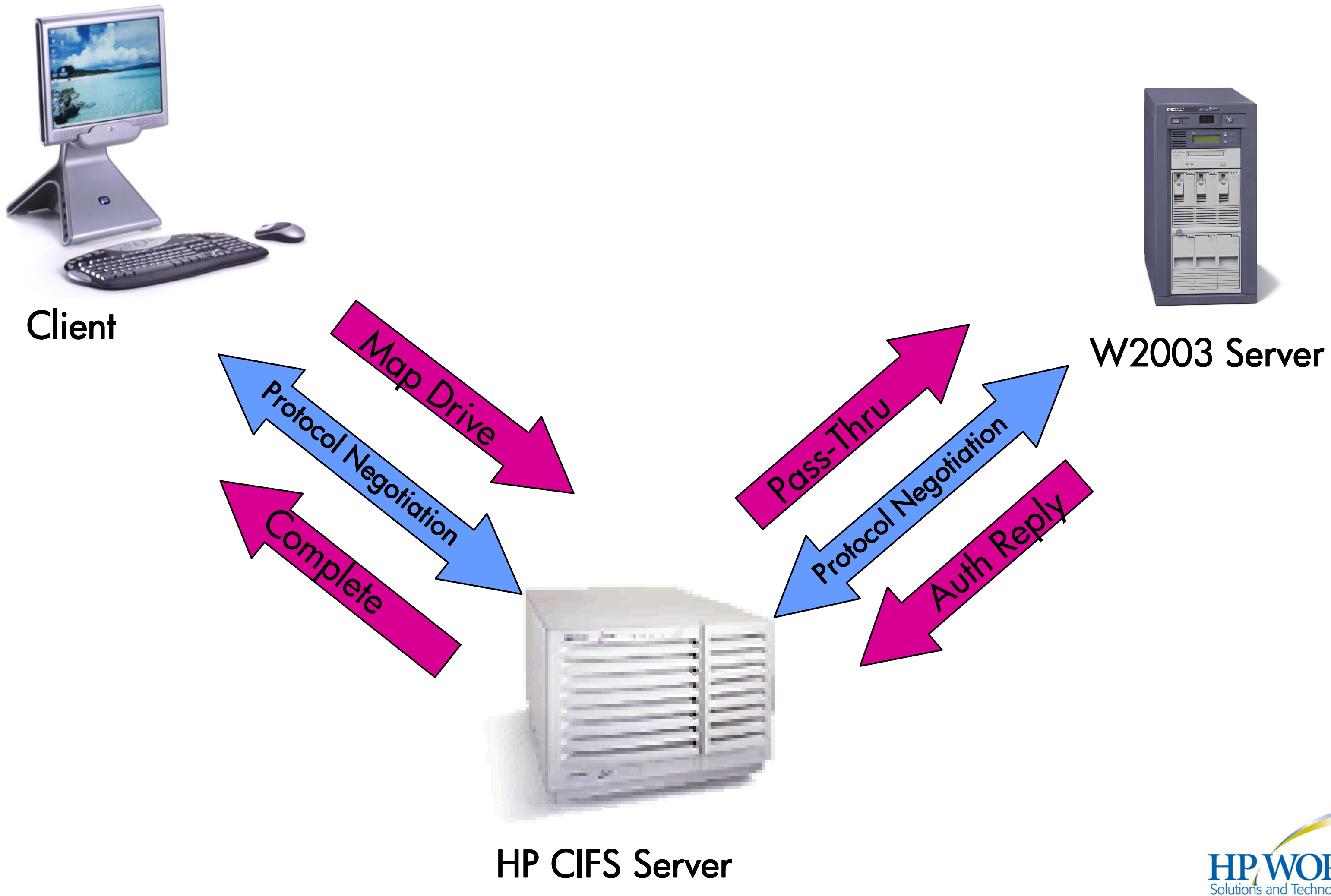
Username works

Client re-tries with valid username

NTLMv1

- Default Samba authentication protocol
  - “security = domain”
- Fallback Samba authentication protocol
  - “security = ads”
- NT 4.0 legacy authentication protocol
- Pass-Through protocol
  - Each client access is authenticated at the domain DC

NTLM Pass-Through



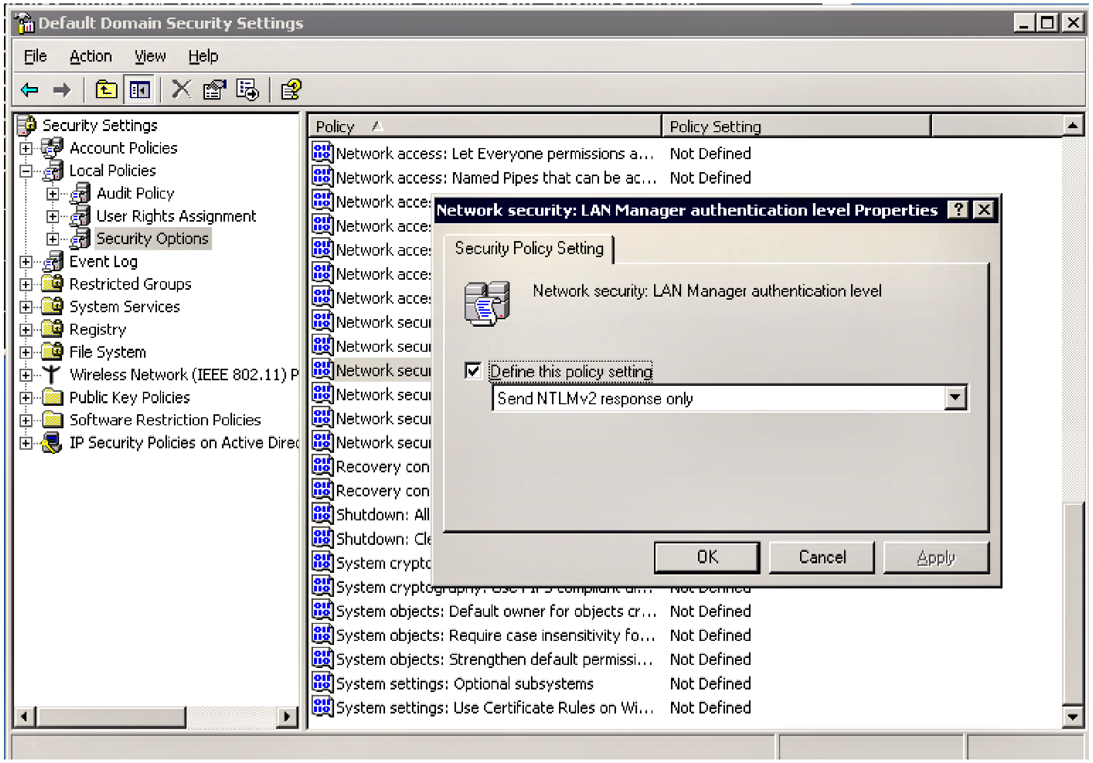
NTLMv2

- NTLMv2 Authentication
  - implements 128bit encrypted keys
  - eliminate LANMAN hashes
  - Much harder to crack than NTLMv1
- Requires CIFS/Samba 3.0.4
- Client Security Policy (Domain or Local)
  - XP, Windows 2000, NT SP4 (requires registry hacks)

NTLMv2: Configure on CIFS Server

- Smb.conf
  - “ntlm auth = no”
  - “lanman auth = no”
- “client ntlmv2 auth”
  - Configure host smbclient – not CIFS Server
  - Do not set this variable
    - Unless you use smbclient and want NTLMv2 for it
- NTLMv2 is not “negotiated”
  - Client and server settings must match
  - Take it or leave it

NTLMv2: Configure on DC



Policy	Policy Setting
Network access: Let Everyone permissions a...	Not Defined
Network access: Named Pipes that can be ac...	Not Defined
Network acce:	
Network acce:	
Network acce:	
Network acce:	
Network acce:	
Network secu	
Network secu	
Network secu	
Network secu	
Network secu	
Network secu	
Recovery con	
Recovery con	
Shutdown: All	
Shutdown: Cle	
System crypto	
System cryptography: Use FIPS compliant al...	Not Defined
System objects: Default owner for objects cr...	Not Defined
System objects: Require case insensitivity fo...	Not Defined
System objects: Strengthen default permissi...	Not Defined
System settings: Optional subsystems	Not Defined
System settings: Use Certificate Rules on Wi...	Not Defined

Network security: LAN Manager authentication level Properties

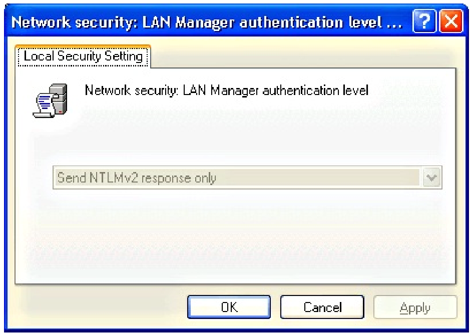
Security Policy Setting

Network security: LAN Manager authentication level

☑ Define this policy setting

Send NTLMv2 response only

- Sets domain authentication protocol
- Domain client auth type →
- XP – no registry tweaks



Network security: LAN Manager authentication level ...

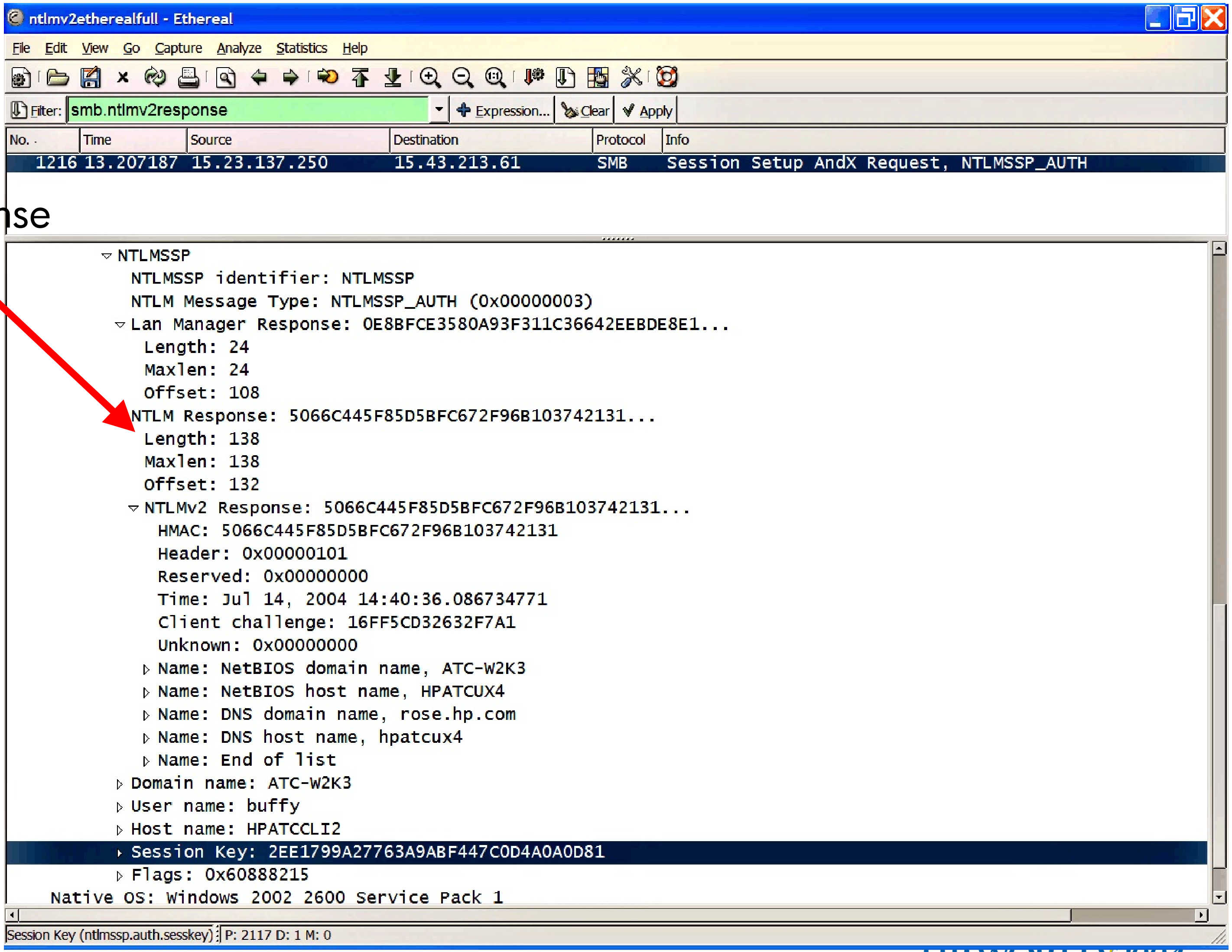
Local Security Setting

Network security: LAN Manager authentication level

Send NTLMv2 response only

NTLMv2: Difficult to Verify

- Use ethereal
- Filter for ntlmv2
- The NTLM response
  - Length >24



Filter: smb.ntlmv2response

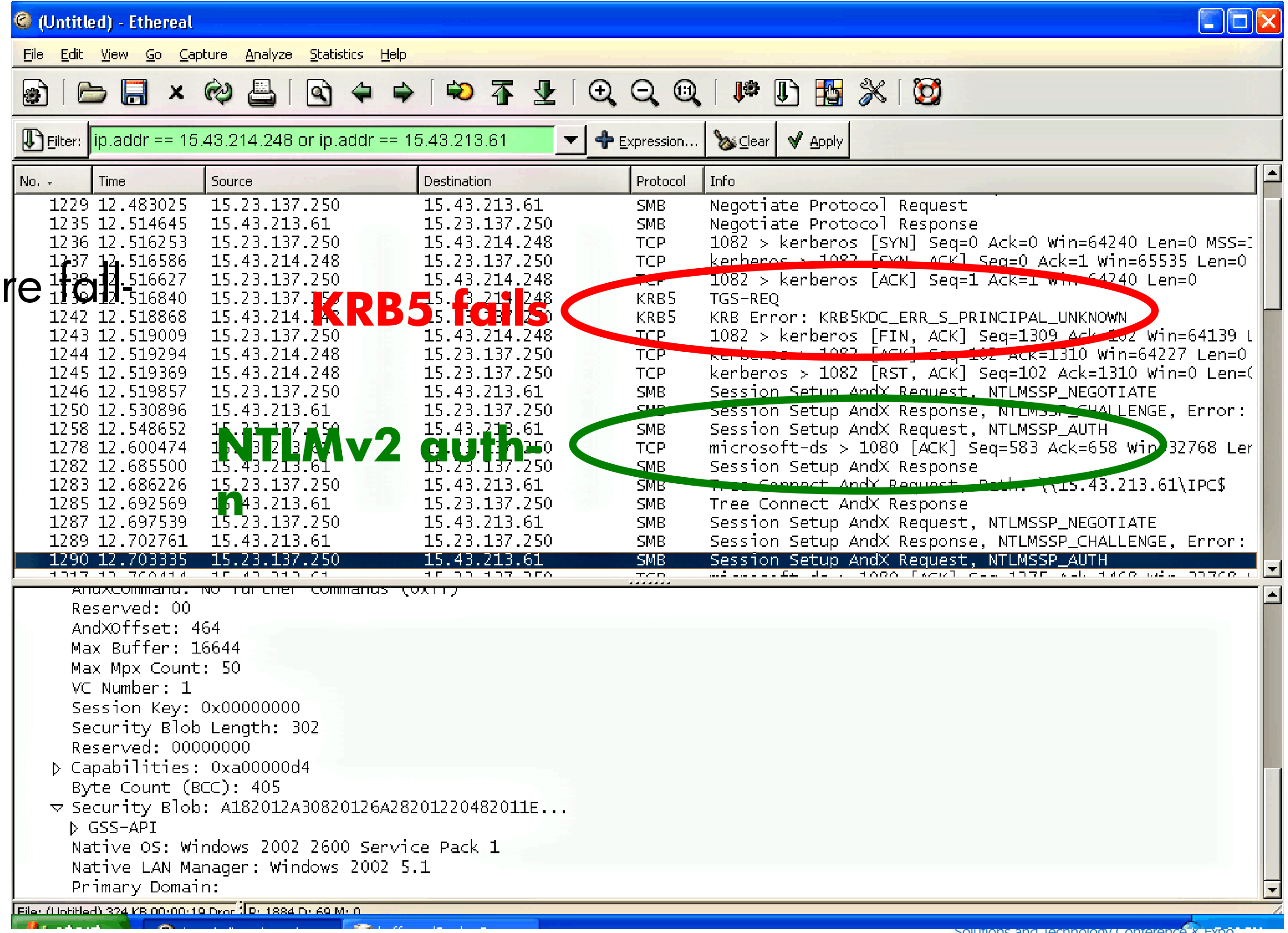
No.	Time	Source	Destination	Protocol	Info
1216	13.207187	15.23.137.250	15.43.213.61	SMB	Session Setup AndX Request, NTLMSSP_AUTH

```
▽ NTLMSSP
    NTLMSSP identifier: NTLMSSP
    NTLM Message Type: NTLMSSP_AUTH (0x00000003)
  ▽ Lan Manager Response: 0E8BFCE3580A93F311C36642EEBDE8E1...
      Length: 24
      Maxlen: 24
      Offset: 108
    NTLM Response: 5066C445F85D5BFC672F96B103742131...
      Length: 138
      Maxlen: 138
      Offset: 132
    ▽ NTLMv2 Response: 5066C445F85D5BFC672F96B103742131...
        HMAC: 5066C445F85D5BFC672F96B103742131
        Header: 0x00000101
        Reserved: 0x00000000
        Time: Jul 14, 2004 14:40:36.086734771
        Client challenge: 16FF5CD32632F7A1
        Unknown: 0x00000000
      ▷ Name: NetBIOS domain name, ATC-W2K3
      ▷ Name: NetBIOS host name, HPATCUX4
      ▷ Name: DNS domain name, rose.hp.com
      ▷ Name: DNS host name, hpatcux4
      ▷ Name: End of list
  ▷ Domain name: ATC-W2K3
  ▷ User name: buffy
  ▷ Host name: HPATCCLI2
  ▷ Session Key: 2EE1799A27763A9ABF447C0D4A0A0D81
  ▷ Flags: 0x60888215
Native OS: Windows 2002 2600 Service Pack 1
```

Session Key (ntlmssp.auth.sesskey) P: 2117 D: 1 M: 0

NTLMv2 with ADS: Why Bother?

- Auth-n Fall through
  - KRB5 fails
  - NTLMv2 fallback
  - Or NTLMv1
- NTLMv2 more secure fall-through auth-n


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: ip.addr == 15.43.214.248 or ip.addr == 15.43.213.61
Expression...
Clear
Apply

```
No. -  Time       Source          Destination     Protocol Info
  1229 12.483025  15.23.137.250   15.43.213.61    SMB      Negotiate Protocol Request
  1235 12.514645  15.43.213.61    15.23.137.250   SMB      Negotiate Protocol Response
  1236 12.516253  15.23.137.250   15.43.214.248   TCP      1082 > kerberos [SYN] Seq=0 Ack=0 Win=64240 Len=0 MSS=1
  1237 12.516586  15.43.214.248   15.23.137.250   TCP      kerberos > 1082 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
  1238 12.516627  15.23.137.250   15.43.214.248   TCP      1082 > kerberos [ACK] Seq=1 Ack=1 Win=64240 Len=0
  1239 12.516840  15.23.137.250   15.43.214.248   KRB5     TGS-REQ
  1242 12.518868  15.43.214.248   15.23.137.250   KRB5     KRB Error: KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN
  1243 12.519009  15.23.137.250   15.43.214.248   TCP      1082 > kerberos [FIN, ACK] Seq=1309 Ack=102 Win=64139 L
  1244 12.519294  15.43.214.248   15.23.137.250   TCP      kerberos > 1082 [ACK] Seq=102 Ack=1310 Win=64227 Len=0
  1245 12.519369  15.43.214.248   15.23.137.250   TCP      kerberos > 1082 [RST, ACK] Seq=102 Ack=1310 Win=0 Len=(
  1246 12.519857  15.23.137.250   15.43.213.61    SMB      Session Setup AndX Request, NTLMSSP_NEGOTIATE
  1250 12.530896  15.43.213.61    15.23.137.250   SMB      Session Setup AndX Response, NTLMSSP_CHALLENGE, Error:
  1258 12.548652  15.23.137.250   15.43.213.61    SMB      Session Setup AndX Request, NTLMSSP_AUTH
  1278 12.600474  15.43.213.61    15.23.137.250   TCP      microsoft-ds > 1080 [ACK] Seq=583 Ack=658 Win=32768 Len
  1282 12.685500  15.43.213.61    15.23.137.250   SMB      Session Setup AndX Response
  1283 12.686226  15.23.137.250   15.43.213.61    SMB      Tree Connect AndX Request, Path: \\15.43.213.61\IPC$
  1285 12.692569  15.43.213.61    15.23.137.250   SMB      Tree Connect AndX Response
  1287 12.697539  15.23.137.250   15.43.213.61    SMB      Session Setup AndX Request, NTLMSSP_NEGOTIATE
  1289 12.702761  15.43.213.61    15.23.137.250   SMB      Session Setup AndX Response, NTLMSSP_CHALLENGE, Error:
  1290 12.703335  15.23.137.250   15.43.213.61    SMB      Session Setup AndX Request, NTLMSSP_AUTH
```

KRB5 fails

NTLMv2 auth-n

```
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 464
    Max Buffer: 16644
    Max Mpx Count: 50
    VC Number: 1
    Session Key: 0x00000000
    Security Blob Length: 302
    Reserved: 00000000
  ▷ Capabilities: 0xa00000d4
    Byte Count (BCC): 405
  ▽ Security Blob: A182012A30820126A28201220482011E...
    ▷ GSS-API
    Native OS: Windows 2002 2600 Service Pack 1
    Native LAN Manager: Windows 2002 5.1
    Primary Domain:
```

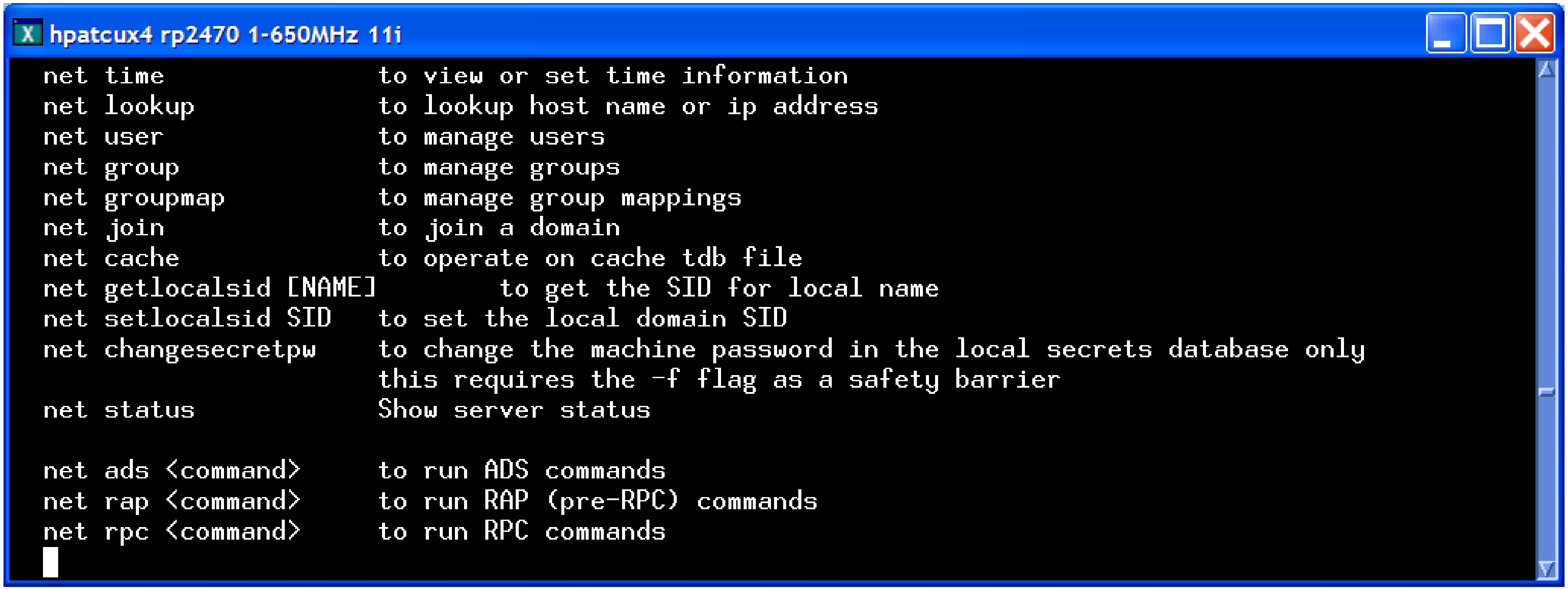
- Introduction
- Samba Version Tracking
- ADS Integration
- LDAP and Directory Servers
- Authentication
- **Net Commands**
- New and Changed Tools and Parameters
- Performance Enhancements and Recommendations
- Summary

Net commands

- Command Line samba management interface
  - To manage services
  - Query domain controllers
- Net ads: LDAP interface to Windows ADS
  - "security = ads" (W2000, W2003)
- Net rpc: RPC interface to Windows server
  - "security = domain" (W2000, NT4)
- Net: Local to Samba server
  - "security = user", but also domain and ADS

- *Note: there is some overlap*
  - *ie "net user" and "net ads user" work on ads, but "net rpc" does not*
    - *"net user" actually does LDAP when "security = ads"*
- *Note: "security = server" is not really used anymore*

“net” (Local Server) Command List

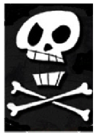


```
net time                to view or set time information
net lookup              to lookup host name or ip address
net user                to manage users
net group               to manage groups
net groupmap            to manage group mappings
net join                to join a domain
net cache               to operate on cache tdb file
net getlocalsid [NAME]          to get the SID for local name
net setlocalsid SID     to set the local domain SID
net changesecretpw      to change the machine password in the local secrets database only
                        this requires the -f flag as a safety barrier
net status              Show server status

net ads <command>       to run ADS commands
net rap <command>       to run RAP (pre-RPC) commands
net rpc <command>       to run RPC commands
```

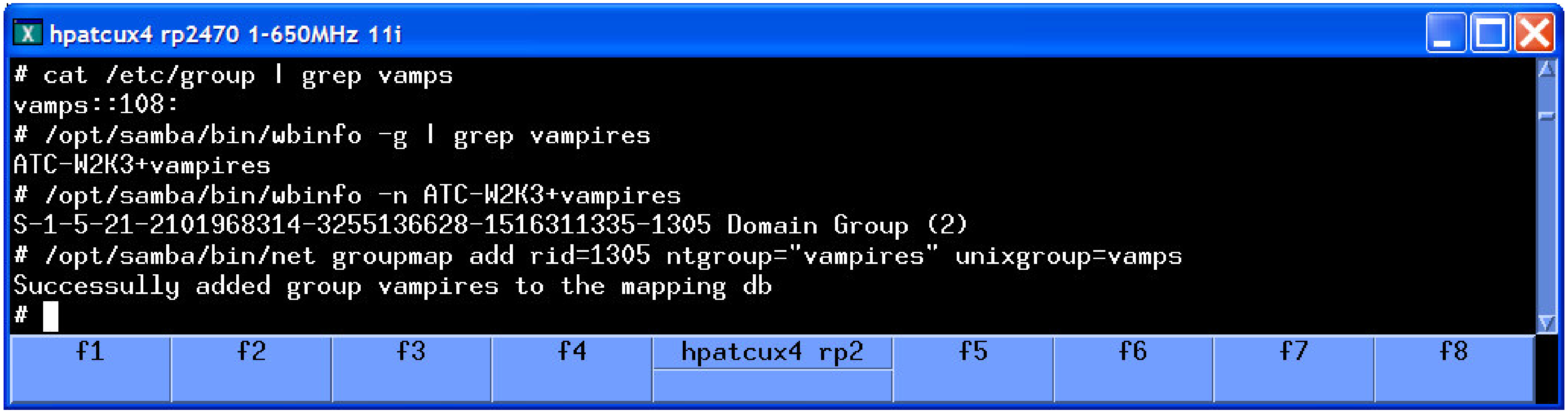
“net”: Notable Behavior

- net join
  - Same as “net rpc join”
  - Can join ADS
    - But Kerberos disabled
- net changesecretpw
  - Expert tool
  - Use and die



- net lookup
  - ldap,kdc,dc,master
  - “net ads info” is better
- net cache
  - Expert tool
  - gencache.tdb
- net groupmap
  - Manually map groups
  - Tricky
  - smbpasswd –w “ldap admin pw”
  - Add,delete,list,modify

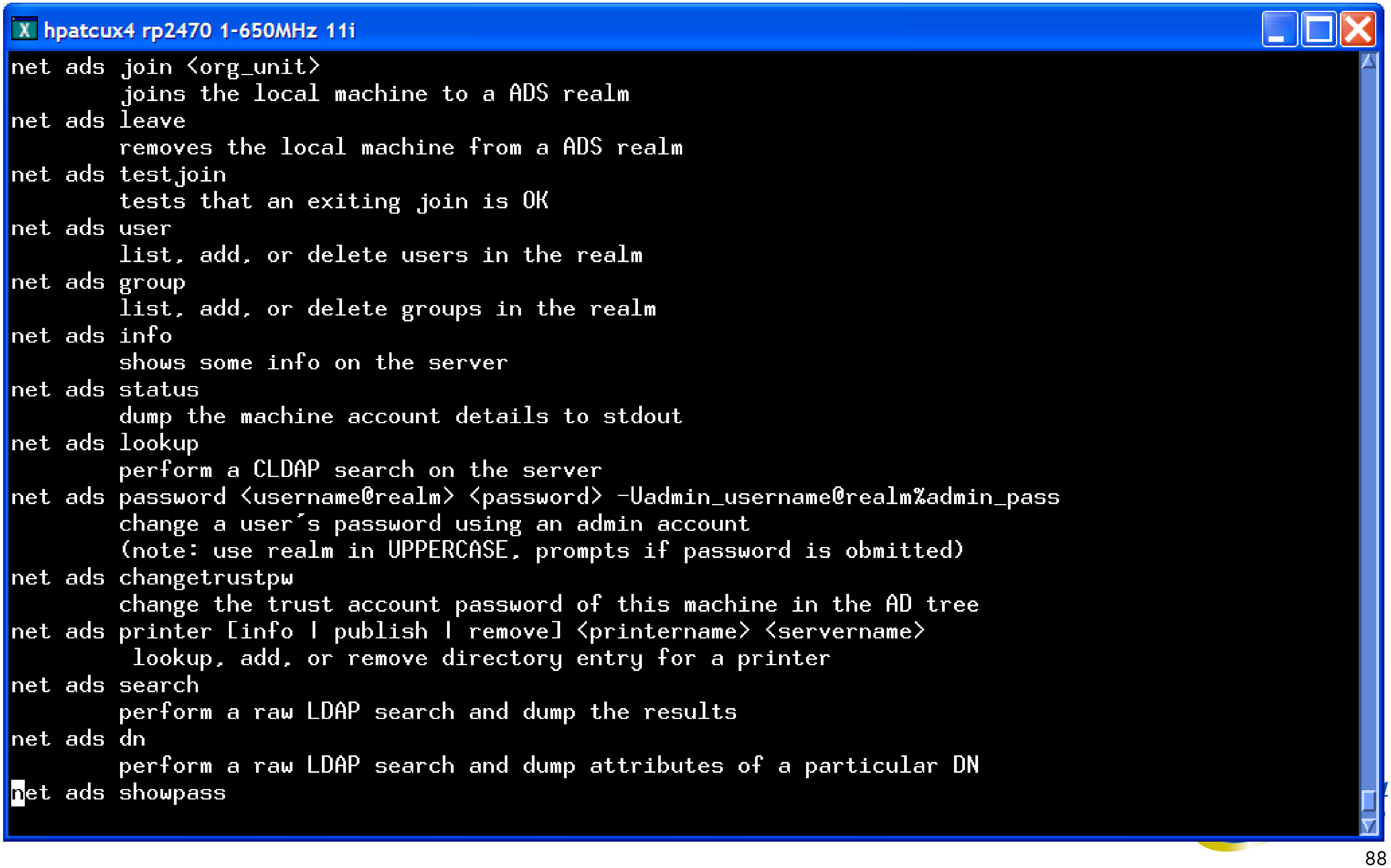
Net groupmap



```
# cat /etc/group | grep vamps
vamps::108:
# /opt/samba/bin/wbinfo -g | grep vampires
ATC-W2K3+vampires
# /opt/samba/bin/wbinfo -n ATC-W2K3+vampires
S-1-5-21-2101968314-3255136628-1516311335-1305 Domain Group (2)
# /opt/samba/bin/net groupmap add rid=1305 ntgroup="vampires" unixgroup=vamps
Successully added group vampires to the mapping db
#
```

- Windows group members mapped to posix groups
- POSIX group assigned to ACL
- Windows users granted access by ACL
- Mappings stored in /var/opt/samba/locks/group_mapping.tdb

“net ads” command list



```
net ads join <org_unit>
        joins the local machine to a ADS realm
net ads leave
        removes the local machine from a ADS realm
net ads testjoin
        tests that an exiting join is OK
net ads user
        list, add, or delete users in the realm
net ads group
        list, add, or delete groups in the realm
net ads info
        shows some info on the server
net ads status
        dump the machine account details to stdout
net ads lookup
        perform a CLDAP search on the server
net ads password <username@realm> <password> -Uadmin_username@realm%admin_pass
        change a user´s password using an admin account
        (note: use realm in UPPERCASE, prompts if password is obmitted)
net ads changetrustpw
        change the trust account password of this machine in the AD tree
net ads printer [info | publish | remove] <printername> <servername>
         lookup, add, or remove directory entry for a printer
net ads search
        perform a raw LDAP search and dump the results
net ads dn
        perform a raw LDAP search and dump attributes of a particular DN
net ads showpass
```

“net ads” Command Functions

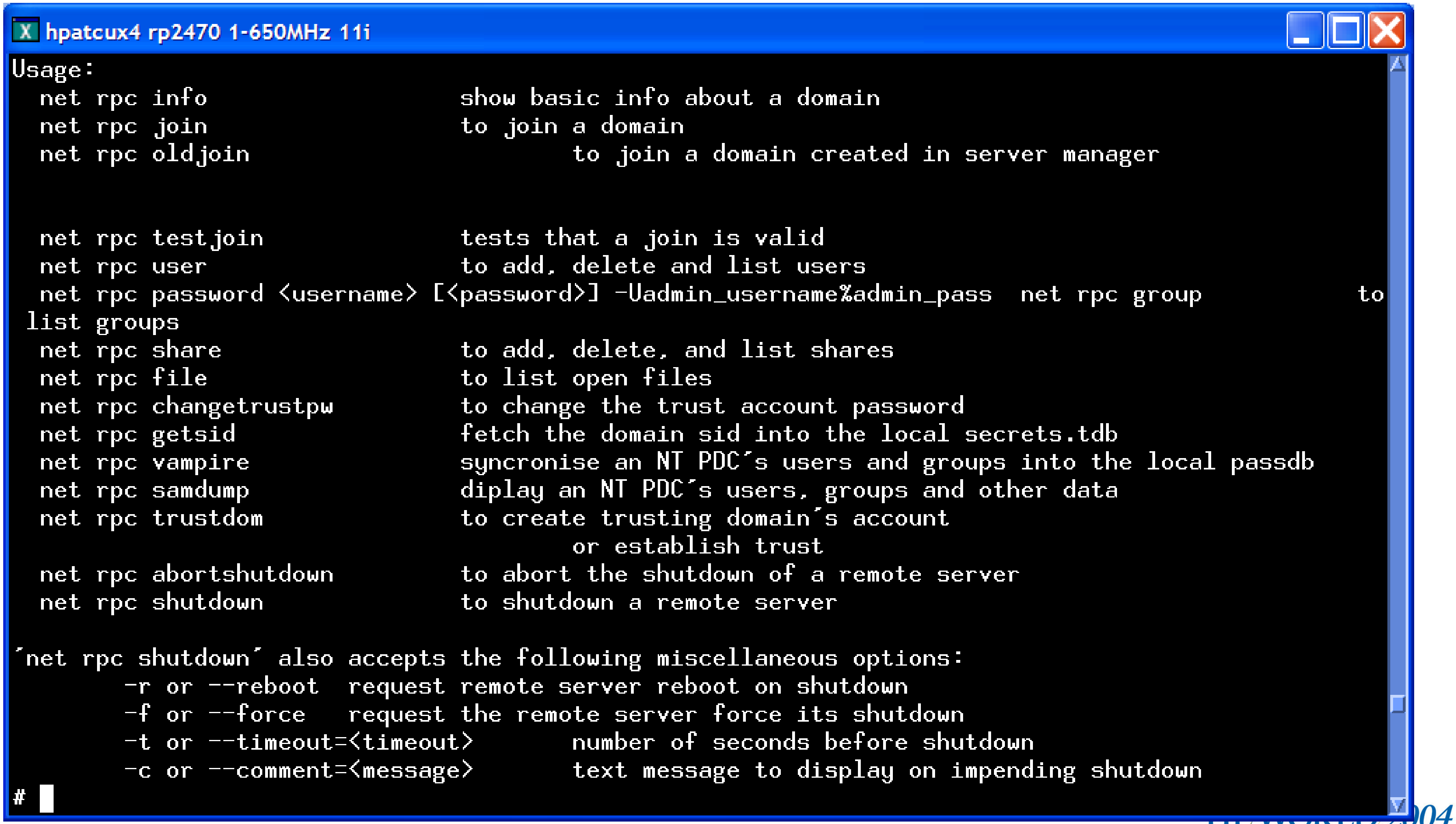
- Domain Functions
  - net ads join [-U admin%pass]
    - Joins domain
    - Uses smb.conf and krb5.conf
  - net ads testjoin
    - Validates successful join
  - net ads leave
    - Delete local server from realm
  - net ads changetrustpw ☠
- State
  - net ads info
    - Lists server stuff
  - net ads status
    - Huge output, need to grep
      - LDAP structure
      - SIDs

- Account Functions
  - net ads showpass
    - Machine passwd in realm
  - net ads password
    - Change user pw in realm
  - net ads group
  - net ads user

  (list,add,delete)
- LDAP Functions
  - net ads lookup
    - All about your DC
  - net ads search
  - net ads dn
    - Net ads dn ‘cn=administrator,cn=users,dc=atc-w2k3,dc=hp,dc=com’

Note: some ads commands do not work on “security = domain”

“net rpc” Command List



```
Usage:
  net rpc info                  show basic info about a domain
  net rpc join                  to join a domain
  net rpc oldjoin                       to join a domain created in server manager


  net rpc testjoin              tests that a join is valid
  net rpc user                  to add, delete and list users
  net rpc password <username> [<password>] -Uadmin_username%admin_pass  net rpc group           to
 list groups
  net rpc share                 to add, delete, and list shares
  net rpc file                  to list open files
  net rpc changetrustpw         to change the trust account password
  net rpc getsid                fetch the domain sid into the local secrets.tdb
  net rpc vampire               syncronise an NT PDC´s users and groups into the local passdb
  net rpc samdump               diplay an NT PDC´s users, groups and other data
  net rpc trustdom              to create trusting domain´s account
                                        or establish trust
  net rpc abortshutdown         to abort the shutdown of a remote server
  net rpc shutdown              to shutdown a remote server

´net rpc shutdown´ also accepts the following miscellaneous options:
        -r or --reboot  request remote server reboot on shutdown
        -f or --force   request the remote server force its shutdown
        -t or --timeout=<timeout>       number of seconds before shutdown
        -c or --comment=<message>       text message to display on impending shutdown
# 
```

“net rpc” Command Functions

- Domain Functions
  - net rpc getsid
    - Propagate SID to BDC/PDC
    - Often used with vampire
  - net rpc vampire
    - NT account migration
    - Often used with getsid
  - net rpc trustdom
  - Net rpc samdump
  - net rpc changetrustpw

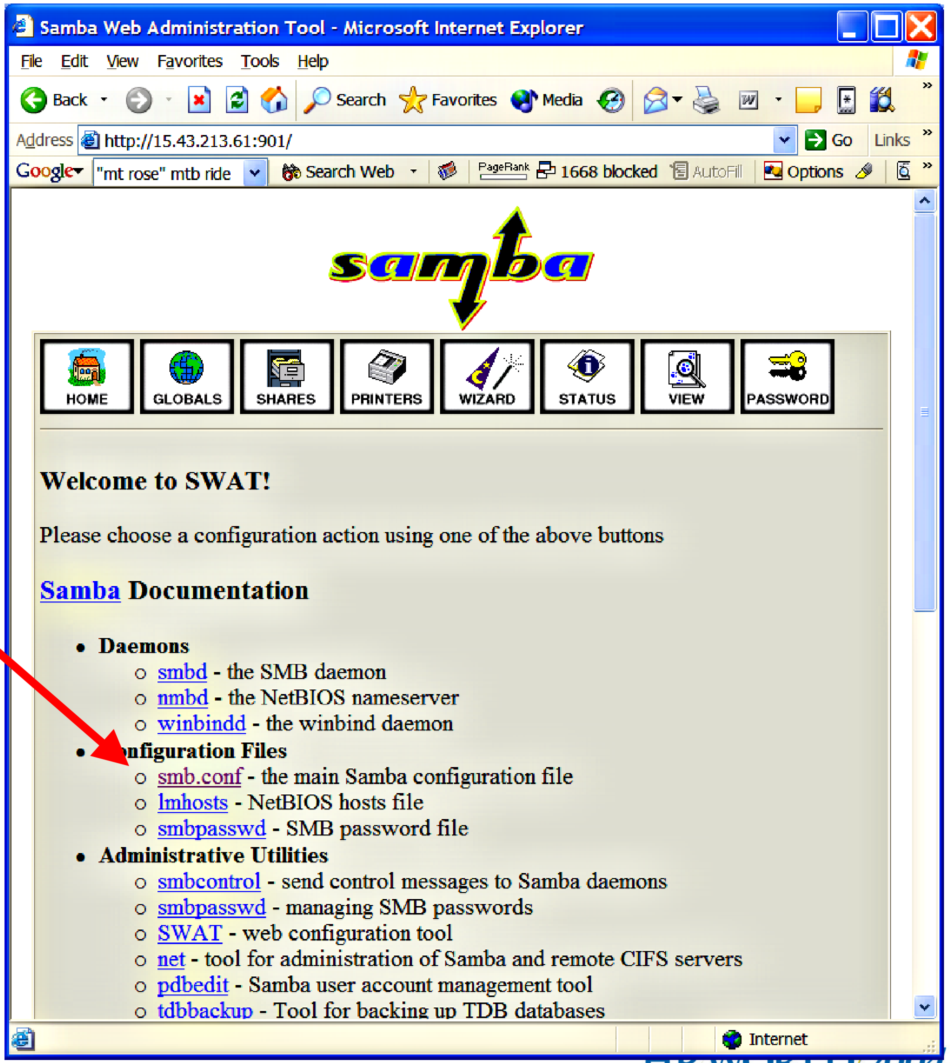
- Account Function
  - net rpc group
  - net rpc user (list,add,delete)
  - net rpc share
- State
  - net rpc info
    - Lists server stuff
  - net rpc file
    - List open files

Note: some rpc commands do not work on "security = ads"

- Introduction
- Samba Version Tracking
- ADS Integration
- LDAP and Directory Servers
- Authentication
- Net Commands
- **New and Changed Tools and Parameters**
- Performance Enhancements and Recommendations
- Summary

SWAT

- Interface Unchanged
- New smb.conf parms
  - See later slide
- smb.conf link
  - My favorite manual


Samba Web Administration Tool - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://15.43.213.61:901/
Go Links
Google "mt rose" mtb ride Search Web PageRank 1668 blocked AutoFill Options
samba
HOME
GLOBALS
SHARES
PRINTERS
WIZARD
STATUS
VIEW
PASSWORD
Internet

Welcome to SWAT!

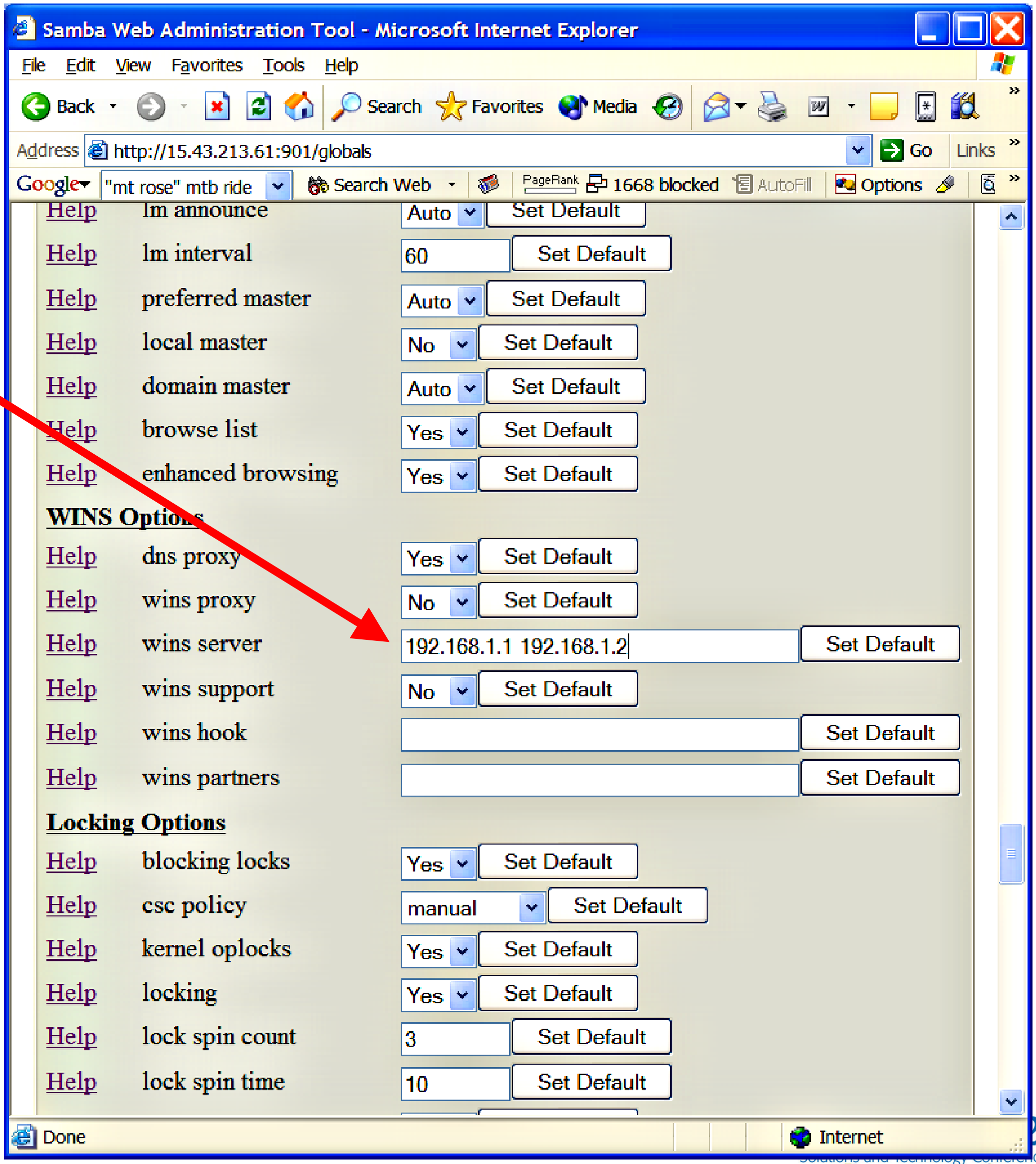
Please choose a configuration action using one of the above buttons

Samba Documentation

- **Daemons**
  - smbd - the SMB daemon
  - nmbd - the NetBIOS nameserver
  - winbindd - the winbind daemon
- **nfiguration Files**
  - smb.conf - the main Samba configuration file
  - lmhosts - NetBIOS hosts file
  - smbpasswd - SMB password file
- **Administrative Utilities**
  - smbcontrol - send control messages to Samba daemons
  - smbpasswd - managing SMB passwords
  - SWAT - web configuration tool
  - net - tool for administration of Samba and remote CIFS servers
  - pdbedit - Samba user account management tool
  - tdbbackup - Tool for backing up TDB databases

Secondary WINS Server

- WINS
  - Secondary config


Samba Web Administration Tool - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Go
Links
Search Web
PageRank
1668 blocked
AutoFill
Options
Done
Internet

Address http://15.43.213.61:901/globals

Google "mt rose" mtb ride

Help	lm announce	Auto	Set Default
Help	lm interval	60	Set Default
Help	preferred master	Auto	Set Default
Help	local master	No	Set Default
Help	domain master	Auto	Set Default
Help	browse list	Yes	Set Default
Help	enhanced browsing	Yes	Set Default
WINS Options			
Help	dns proxy	Yes	Set Default
Help	wins proxy	No	Set Default
Help	wins server	192.168.1.1 192.168.1.2	Set Default
Help	wins support	No	Set Default
Help	wins hook		Set Default
Help	wins partners		Set Default
Locking Options			
Help	blocking locks	Yes	Set Default
Help	csc policy	manual	Set Default
Help	kernel oplocks	Yes	Set Default
Help	locking	Yes	Set Default
Help	lock spin count	3	Set Default
Help	lock spin time	10	Set Default

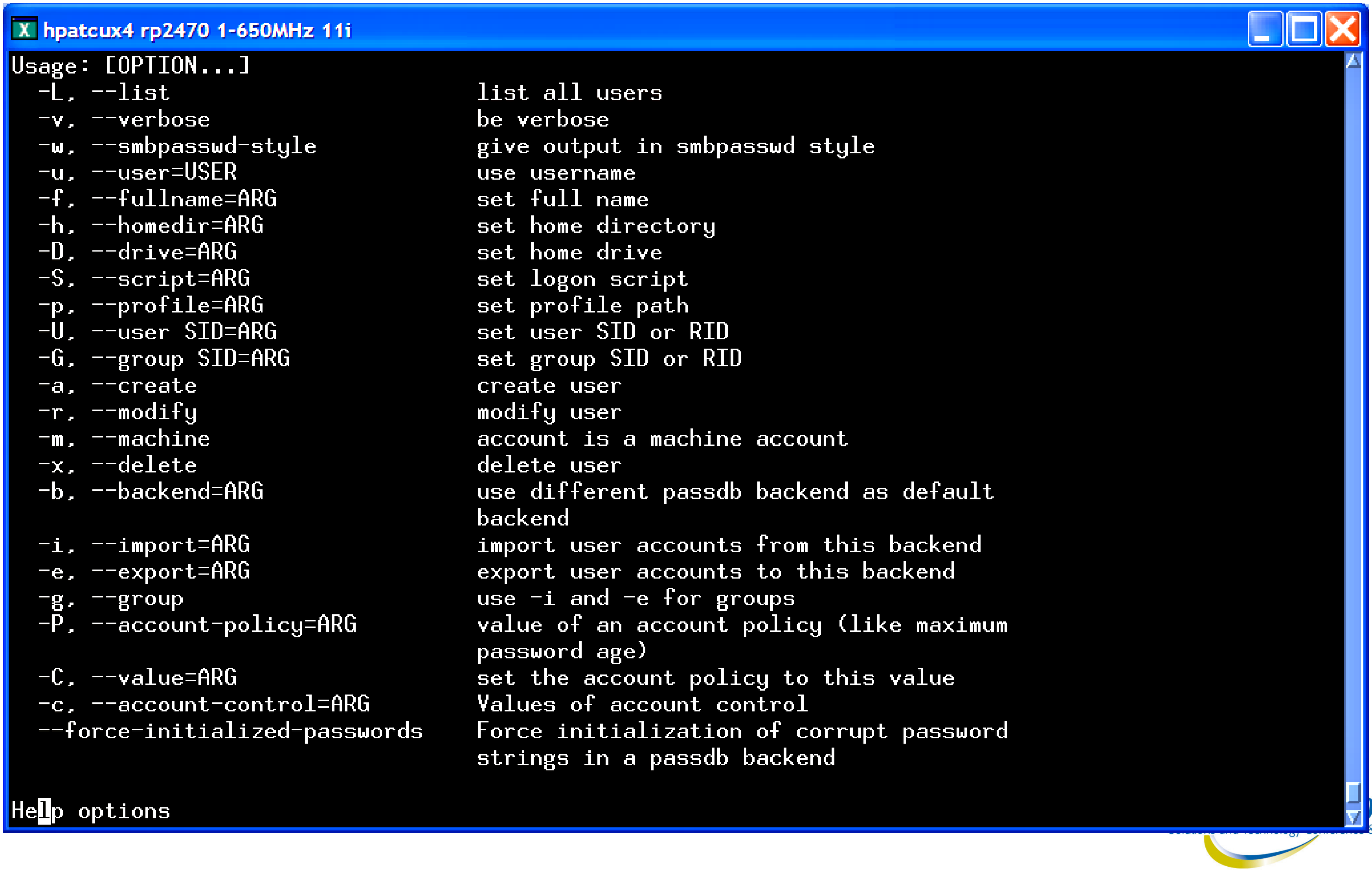
smb.conf New Parameters

- algorythmic RID base
- auth methods
- client lanman auth
- client ntlmv2 auth
- client signing
- client use spnego
- delete group script
- delete user from group script
- disable netbios
- host msdfs
- hostname lookups
- **idmap backend**
- idmap gid
- idmap uid
- ldapgroup suffix
  - idmap
  - machine
- ldap passwd sync
- ldap replication sleep
- ldap user suffix
- **ntlm auth**
- **passdb backend**
- realm

passdb backend

- Choose protocol and backend storage of passwords
- smb.conf – “passdb = option”
  - smbpasswd (default): /var/opt/samba/private/smbpasswd
    - Watch out – smbpasswd file may go away in a future release
  - tdbsam: /var/opt/samba/private/passdb.tdb
    - Provides extensions over smbpasswd
      - Apply to “security = ads”? Probably not (have not tested yet)
    - No instrumentation needed
    - Scalability concerns for over 250 users
  - ldapsam: to directory server (non-ADS)
    - Obviously more complex
    - But vastly preferable – see prior module
  - Others: mysqlsam, xmlsam

pdbedit = “passdb edit” = Password DataBase edit



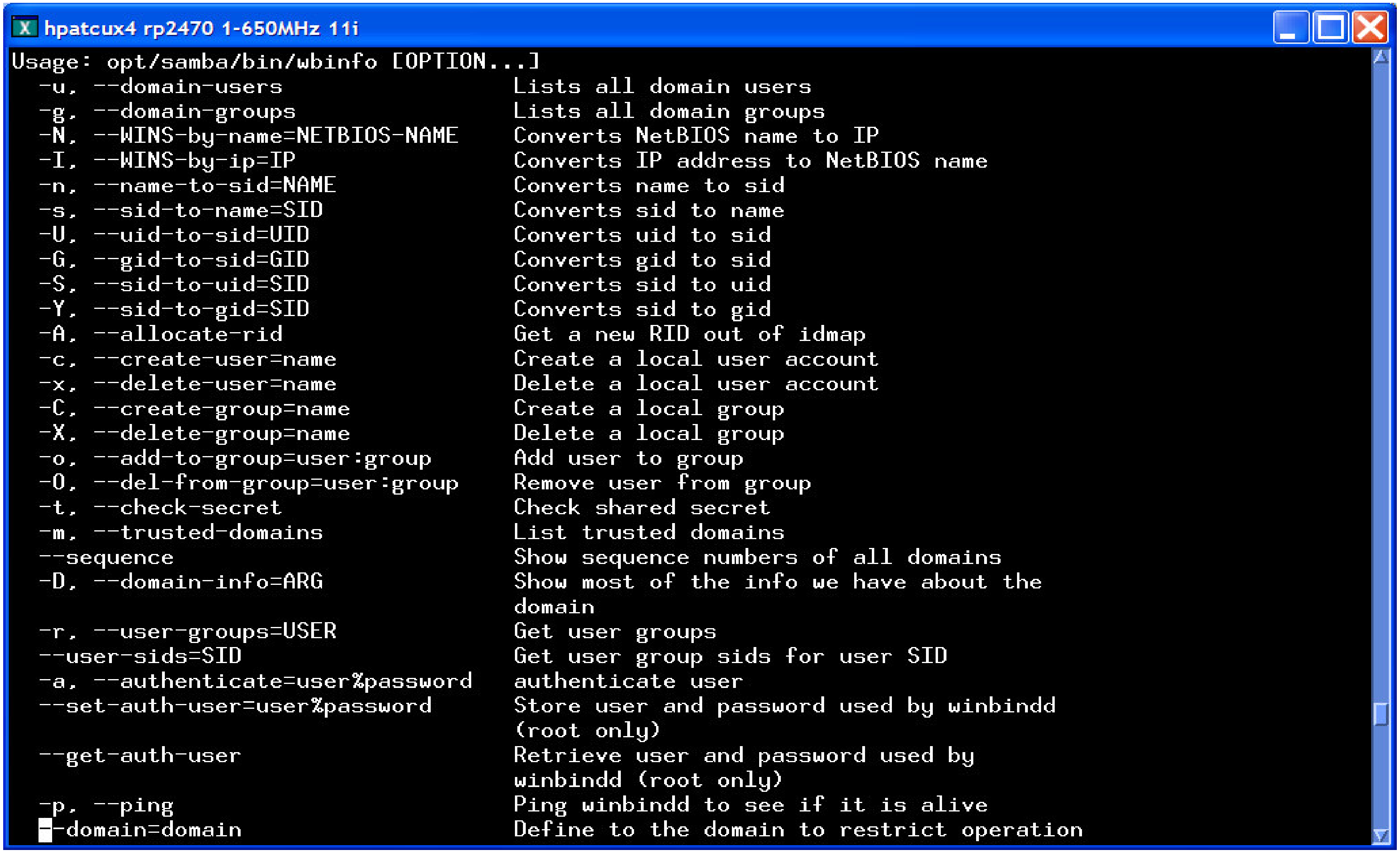
```
Usage: [OPTION...]
  -L, --list                        list all users
  -v, --verbose                     be verbose
  -w, --smbpasswd-style             give output in smbpasswd style
  -u, --user=USER                   use username
  -f, --fullname=ARG                set full name
  -h, --homedir=ARG                 set home directory
  -D, --drive=ARG                   set home drive
  -S, --script=ARG                  set logon script
  -p, --profile=ARG                 set profile path
  -U, --user SID=ARG                set user SID or RID
  -G, --group SID=ARG               set group SID or RID
  -a, --create                      create user
  -r, --modify                      modify user
  -m, --machine                     account is a machine account
  -x, --delete                      delete user
  -b, --backend=ARG                 use different passdb backend as default
                                    backend
  -i, --import=ARG                  import user accounts from this backend
  -e, --export=ARG                  export user accounts to this backend
  -g, --group                       use -i and -e for groups
  -P, --account-policy=ARG          value of an account policy (like maximum
                                    password age)
  -C, --value=ARG                   set the account policy to this value
  -c, --account-control=ARG         Values of account control
  --force-initialized-passwords     Force initialization of corrupt password
                                    strings in a passdb backend

Help options
```

pdbedit

- New tool to manage Samba password database
- Needed to manage tdbsam extensions
  - Smbpasswd still works with smbpasswd passdb
- Needed to migrate account data
  - From smbpasswd to tdbsam (or others)

wbinfo



```
Usage: opt/samba/bin/wbinfo [OPTION...]
  -u, --domain-users                 Lists all domain users
  -g, --domain-groups                Lists all domain groups
  -N, --WINS-by-name=NETBIOS-NAME    Converts NetBIOS name to IP
  -I, --WINS-by-ip=IP                Converts IP address to NetBIOS name
  -n, --name-to-sid=NAME             Converts name to sid
  -s, --sid-to-name=SID              Converts sid to name
  -U, --uid-to-sid=UID               Converts uid to sid
  -G, --gid-to-sid=GID               Converts gid to sid
  -S, --sid-to-uid=SID               Converts sid to uid
  -Y, --sid-to-gid=SID               Converts sid to gid
  -A, --allocate-rid                 Get a new RID out of idmap
  -c, --create-user=name             Create a local user account
  -x, --delete-user=name             Delete a local user account
  -C, --create-group=name            Create a local group
  -X, --delete-group=name            Delete a local group
  -o, --add-to-group=user:group      Add user to group
  -O, --del-from-group=user:group    Remove user from group
  -t, --check-secret                 Check shared secret
  -m, --trusted-domains              List trusted domains
  --sequence                         Show sequence numbers of all domains
  -D, --domain-info=ARG              Show most of the info we have about the
                                     domain
  -r, --user-groups=USER             Get user groups
  --user-sids=SID                    Get user group sids for user SID
  -a, --authenticate=user%password   authenticate user
  --set-auth-user=user%password      Store user and password used by winbindd
                                     (root only)
  --get-auth-user                    Retrieve user and password used by
                                     winbindd (root only)
  -p, --ping                         Ping winbindd to see if it is alive
  --domain=domain                    Define to the domain to restrict operation
```

wbinfo

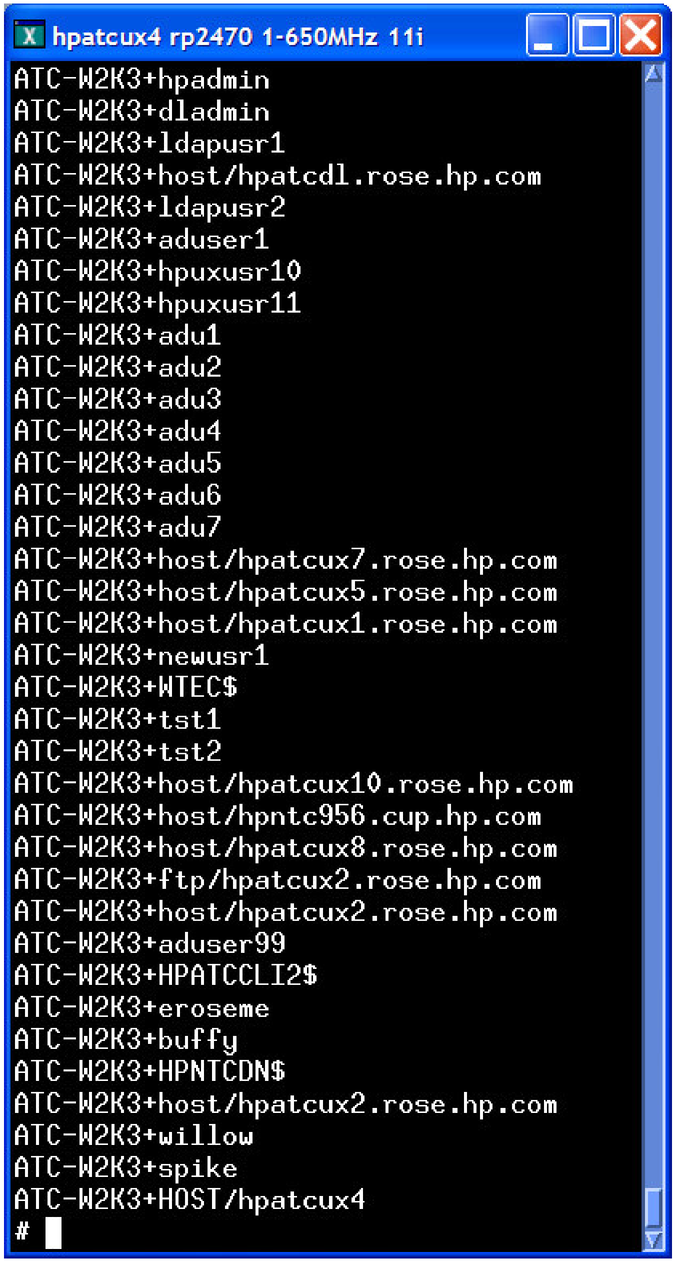
- Queries
  - ADS
    - LDAP
    - RCP
  - Local .tdb databases
  - There is no db dump
    - Like “cat /etc/passwd”

- Mappings
  - UID to SID
  - SID to UID
  - GID to SID
  - SID to GID
  - SID to name
  - Name to SID
  - Note:
    - No name to UID/GID
    - Use id

- User/Group lists
  - wbinfo –u / wbinfo –g
  - Does NOT list mappings!
  - Queries ADS and lists AD users/groups

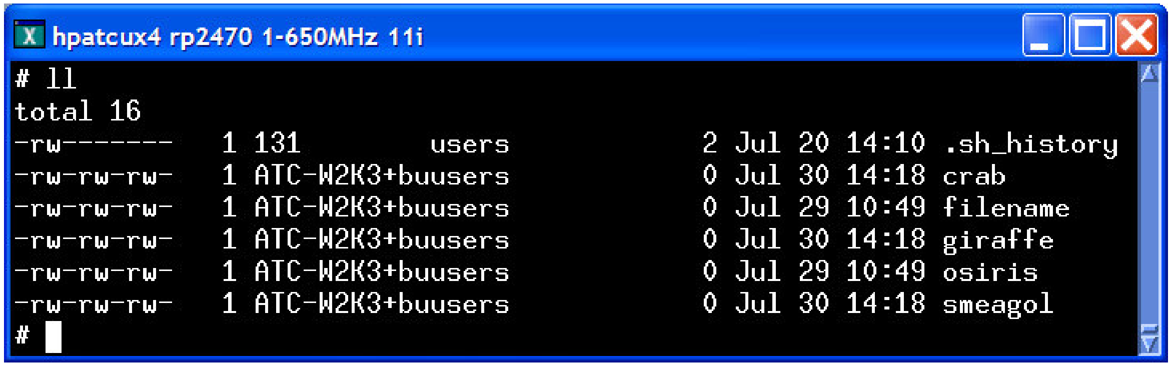
- User/Group names
  - Domain()User/Group
  - Example
    - ATC-W2K3+buffy
  - HP-UX displays 11 char names
  - Characters truncated on displays

wbinfo and mapped username



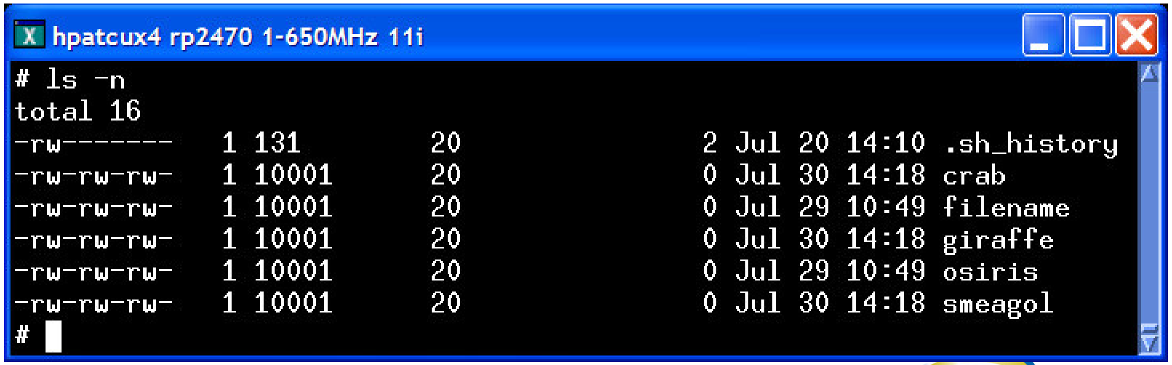
```
ATC-W2K3+hpadmin
ATC-W2K3+dladmin
ATC-W2K3+ldapusr1
ATC-W2K3+host/hpatcdl.rose.hp.com
ATC-W2K3+ldapusr2
ATC-W2K3+aduser1
ATC-W2K3+hpuxusr10
ATC-W2K3+hpuxusr11
ATC-W2K3+adu1
ATC-W2K3+adu2
ATC-W2K3+adu3
ATC-W2K3+adu4
ATC-W2K3+adu5
ATC-W2K3+adu6
ATC-W2K3+adu7
ATC-W2K3+host/hpatcux7.rose.hp.com
ATC-W2K3+host/hpatcux5.rose.hp.com
ATC-W2K3+host/hpatcux1.rose.hp.com
ATC-W2K3+newusr1
ATC-W2K3+WTEC$
ATC-W2K3+tst1
ATC-W2K3+tst2
ATC-W2K3+host/hpatcux10.rose.hp.com
ATC-W2K3+host/hpntc956.cup.hp.com
ATC-W2K3+host/hpatcux8.rose.hp.com
ATC-W2K3+ftp/hpatcux2.rose.hp.com
ATC-W2K3+host/hpatcux2.rose.hp.com
ATC-W2K3+aduser99
ATC-W2K3+HPATCCLI2$
ATC-W2K3+eroseme
ATC-W2K3+buffy
ATC-W2K3+HPNTCDN$
ATC-W2K3+host/hpatcux2.rose.hp.com
ATC-W2K3+willow
ATC-W2K3+spike
ATC-W2K3+HOST/hpatcux4
# 
```

wbinfo -u



```
# ll
total 16
-rw-------   1 131        users            2 Jul 20 14:10 .sh_history
-rw-rw-rw-   1 ATC-W2K3+buusers            0 Jul 30 14:18 crab
-rw-rw-rw-   1 ATC-W2K3+buusers            0 Jul 29 10:49 filename
-rw-rw-rw-   1 ATC-W2K3+buusers            0 Jul 30 14:18 giraffe
-rw-rw-rw-   1 ATC-W2K3+buusers            0 Jul 29 10:49 osiris
-rw-rw-rw-   1 ATC-W2K3+buusers            0 Jul 30 14:18 smeagol
# 
```

ls -l



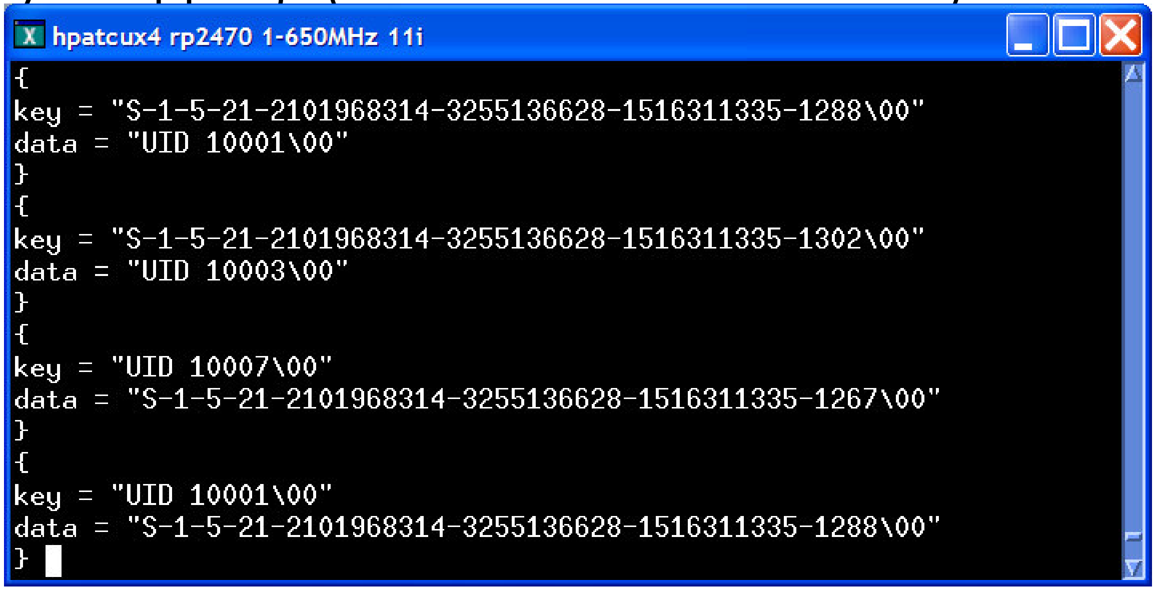
```
# ls -n
total 16
-rw-------   1 131        20               2 Jul 20 14:10 .sh_history
-rw-rw-rw-   1 10001      20               0 Jul 30 14:18 crab
-rw-rw-rw-   1 10001      20               0 Jul 29 10:49 filename
-rw-rw-rw-   1 10001      20               0 Jul 30 14:18 giraffe
-rw-rw-rw-   1 10001      20               0 Jul 29 10:49 osiris
-rw-rw-rw-   1 10001      20               0 Jul 30 14:18 smeagol
# 
```

ls –n (this is what you see if winbindd is stopped)

tdbdump

- tdbdump
  - Displays raw .tdb files
  - Useful for troubleshooting problems

- To see winbind map file
  - /opt/samba/bin/tdbdump /var/opt/samba/locks/winbindd.idmap.tdb
  - Displays mappings (SID-to-UID and UID-TO-SID)



```
{
key = "S-1-5-21-2101968314-3255136628-1516311335-1288\00"
data = "UID 10001\00"
}
{
key = "S-1-5-21-2101968314-3255136628-1516311335-1302\00"
data = "UID 10003\00"
}
{
key = "UID 10007\00"
data = "S-1-5-21-2101968314-3255136628-1516311335-1267\00"
}
{
key = "UID 10001\00"
data = "S-1-5-21-2101968314-3255136628-1516311335-1288\00"
}
```

- Introduction
- Samba Version Tracking
- ADS Integration
- LDAP and Directory Servers
- Authentication
- Net Commands
- New and Changed Tools and Parameters
- **Performance Enhancements and Recommendations**
- Summary

Large Directory Support

- Large directories
- **<u>Most common performance inhibitor</u>**
- Cause: Applications that enumerate all files
- Samba/SMB+Unix+(Windows_Client) = stat64
- Threshold appears to be ~ 2000 files
- Symptom: extreme examples drive CPU to 100%
- Long file names exacerbate condition

- **HP CIFS Server Enhancement**

Large Directory Support - Enhancement

- SMB TRANS2_FINDFIRST and TRANS2_FINDNEXT
  - Initiate entire directory stat
  - Smbd process gets swapped out
  - Execution time is lengthened by repetitive wait state
- Enhancement
  - Smb.conf share variable
  - **"large directory search priority = highest"**
  - Increases system priority of smbd during
    - TRANS2_FINDFIRST
    - TRANS2_FINDNEXT
  - Smbd process stats directory to completion
- HP CIFS Server Enhancement
  - **"large directory search priority" by share**

tdb Locking Enhancement

- tdb = tiny database
  - Storage of various Samba management data
  - More efficient than flat files
- All smbd processes share locks on tdb files
- The more smbd processes, the more locks
  - Affected performance to traverse thousands of locks
- A separate lock file is created for each tdb
- Eliminates lock bottleneck and excessive traversal
- Performance improvement for high usage systems
- HP CIFS Server and Samba Enhancement
  - **Default tdb locking efficiency**

Name Mangling – 8.3 file names

- Name Mangling (default = yes)
  - Samba feature for 8.3 file naming translation
    - "down level" clients: DOS, W3.51
  - Windows mangles names too (in file system)
  - longfilename.txt = lo~name.txt
- Name Mangling has little/no effect for average use
- Big directories see a slowdown
  - as number of files increases
  - as file names get longer

Name Mangling – 8.3 file names

- At **Microsoft TechEd 2004**
  - Recommended: disable 8.3 names
  - Test applications
- Samba
  - Can see 15-20% performance increase
  - For large directories
  - And/or long file names
  - Like "Temporary Internet Files"
- Smb.conf
  - **"name mangle = no"**
- Enhancement
  - **<u>"name mangle" by share</u>**

Case Sensitivity

- ***case*** sensitivity needs a separate 2-hour presentation
- hp-ux (UNIX) is (case sensitive, case preserving)
- Windows is (case **in**sensitive, case preserving)
- Samba ***case*** configuration options give excellent results
  - but can cost processing cycles
- Default: case sensitive = no
- case defaults have no effect for average usage
- for very large directories
  - **"case sensitive = yes"** can help performance
  - decreases stat calls by about 15%
  - application-Windows client testing required!
- Enhancement
  - **"case sensitive" by share**

HP WORLD 2004
Solutions and Technology Conference & Expo

Case Sensitivity

- Smb.conf
  - "case sensitive = yes"
  - "preserve case = no"
  - "short preserve case = no"
  - "default case = lower"
- Not compliant with Windows client defaults
- Test with applications

- Introduction
- Samba Version Tracking
- Authentication
- LDAP and Directory Servers
- ADS Integration
- Net Commands
- New and Changed Tools and Parameters
- Performance Enhancements and Recommendations

- **Summary**

HP CIFS Server 3.0a (based on Samba 3.0.5)

- With Windows Server
  - Windows Server 2003: not much overlap
    - Careful with Kerberos enctypes
  - Windows Server 2000 and 2003
    - ADS: LDAP access to ADS, krb5 authentication
  - Look carefully at HP LDAP-UX integration
    - Store user POSIX data on ADS
  - Windows DDNS: do not turn off NetBIOS
- With winbind
  - Provides improved user/group ID mapping to SIDs.
  - LDAP data store

HP CIFS Server 3.0a (based on Samba 3.0.5)

- Increased flexibility (standalone or member server)
  - LDAP Directory Server backend
  - Multiple password databases
  - Authentication: Kerberos, NTLMv2, NTLM
  - Member, PDC, pseudo-BDC
- Increased complexity
  - winbind and wbinfo
  - Group mapping
  - pdbedit
  - LDAP configurations
  - Server roles

HP CIFS Client

- Separate Product
  - FREE!
- Mount shares from Windows Servers
  - Turns HP-UX sever into a Windows client
- Handy for pulling application data from Windows
- Fully supported by Response Center
- Try it out
  - http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B8724AA

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP

RECOMMENDED TRAINING VENUE FOR THE

HP Certified Professional