Samba-3: Integration and Migration Options

John H. Terpstra, CTO
PrimaStasys Inc.
jht@primastasys.com

Co-Founder Samba-Team
jht@samba.org

Agenda

- Goals and Directions for Samba-3
- New Features & Tools
  - Identity Management
    - ***passdb backend, idmap backend,*** Group Mapping
  - Virtual File System Drivers
- Future Directions & Concerns
- Overview of Integration Choices
  - Kerberos, LDAP/PADL, Samba, VAS

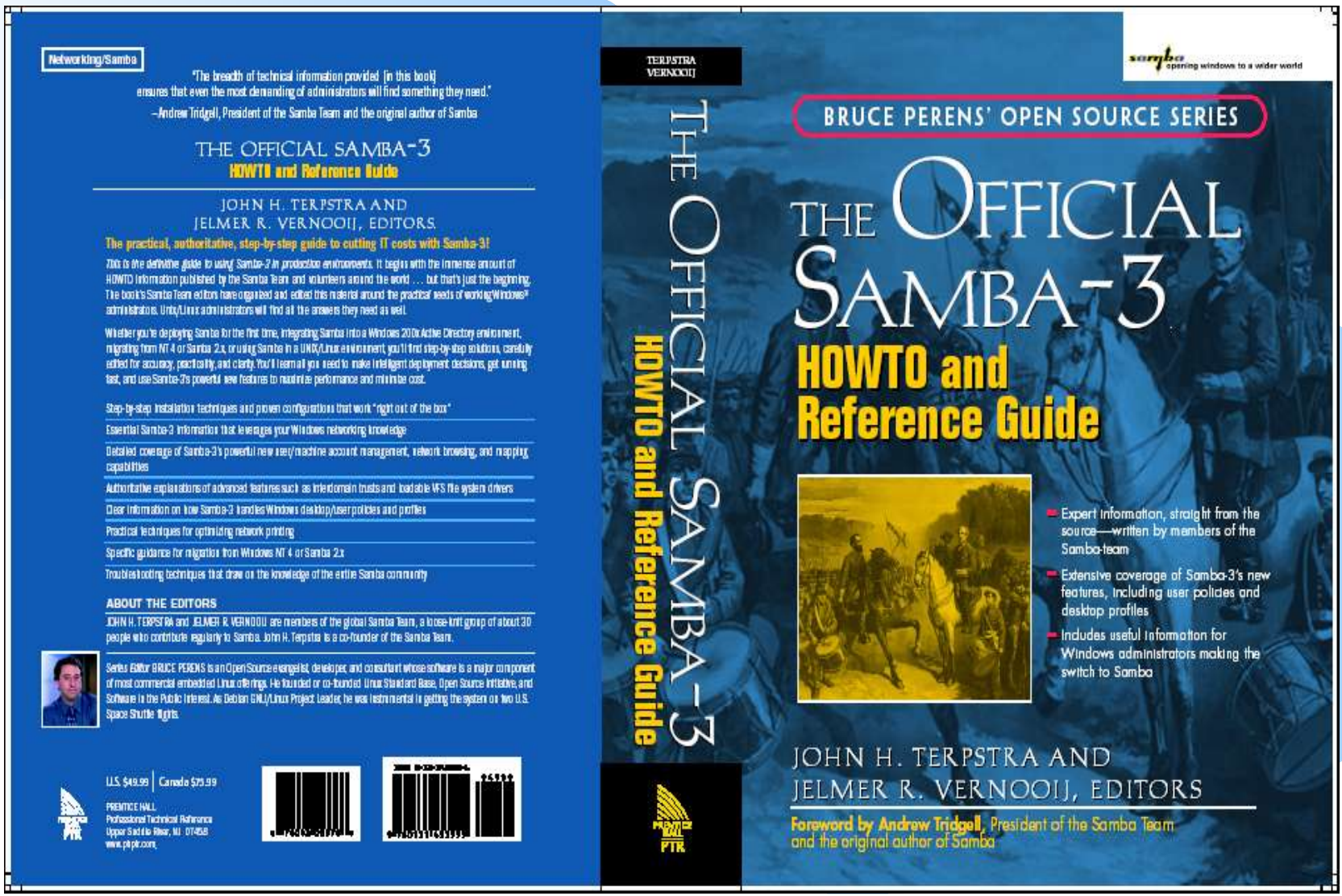
Samba-3 – Goals

- Answer user demand for Migration
  - NT4 to Samba-3
    - Better Domain Control
    - Improved Interdomain Trusts
    - Ability to migrate NT4 user and group accounts to Samba-3
- Native Active Directory Integration
  - Ability to run with plain CIFS over TCP/IP
- New / Better Bug Tracking
  - http://bugzilla.samba.org

Samba-3 – More Goals

- More Secure
  - Compatibility with Windows XP/2003
    - schannel and signing support
      - No more need for registry changes on clients
- Better Documentation
  - New Samba-HOWTO-Collection
    - Published by Prentice Hall
      "The Official Samba-3 HOWTO and Reference Guide", ISBN: 0-13-145355-6
      - Can be pre-ordered from Amazon.Com now

Samba-3 HOWTO & Ref Guide



Samba-3 – More Goals

- Better Internationalisation
  - Required a move to Unicode
  - Necessary to enable newer NT/2KX protocols
- More/Better Admin Tools
  - Allow management of users and groups
    - Not complete yet
      - New **net** command
      - Introduction of the *group_mapping.tdb*
      - Addition of the **profiles** tool
      - Addition of the **editreg** tool (not complete)

New Features

- Active Directory Support
  - LDAP/Kerberos
  - Can join ADS Realm
- Unicode Enabled
- New Authentication Subsystem
  - New loadable multi-module support
    - Passdb, VFS
- Better Security
- New default filename mangling system
- **Net** command
- Windows 32-bit error codes
- Better printer handling
- Migration Support
- Interdomain Trusts
- More ...

Identity Management Changes

- New *passdb backend* parameter
  - Default: smbpasswd, guest
  - Optional:
    tdbsam, ldapsam, mysql, xmlsam, ldap_compat
- Default preserved Samba-2.2.x behaviour as much as possible
- The *guest* parameter is default
  - Provides default account for the guest user

LDAP Improvements

- Compatibility mode - migrate when ready
- New schema
  - Has support for future features
    - Logon Hours, Logon Machines, Password change control, more ...
- Recommended to use OpenLDAP 2.1.x or later
  - Can use: Sun One ID Server (iPlanet), IBM Tivoli Identity Manager, Microsoft ADAM, Novell eDirectory

Virtual File System Support

- Recycle Bin facility extended
  - New Syntax – read HOWTO for details
- Audit & Extd_Audit modules
  - Extd_audit logs to normal log files
  - Audit logs to syslog only
- Fake_perms module for Profile support (for read-only profiles)
- Others: NetAtalk, Read_Only, example modules to encourage 3rd party devel.

New Tools

- New or enhanced commands:
  pdbedit, net, profiles, editreg, SWAT
  - Note: editreg is not complete
- New Samba Components:
  wrepld (not complete)
  winbindd – now manages ID-mapping
  group_mapping.tdb
  – stores NT <-> UNIX ID database

Samba Futures

- Samba-4 is already well under way
  - Re-write from the ground up
    - Being done by Andrew Tridgell – Founder of Samba
    - Improved Modularization
    - Code Clean Up, PIDL (new IDL Compiler)
  - Approx. 2 Years from completion
- Samba-3 will gain back-ports of some Samba-4 features

Facts to Note

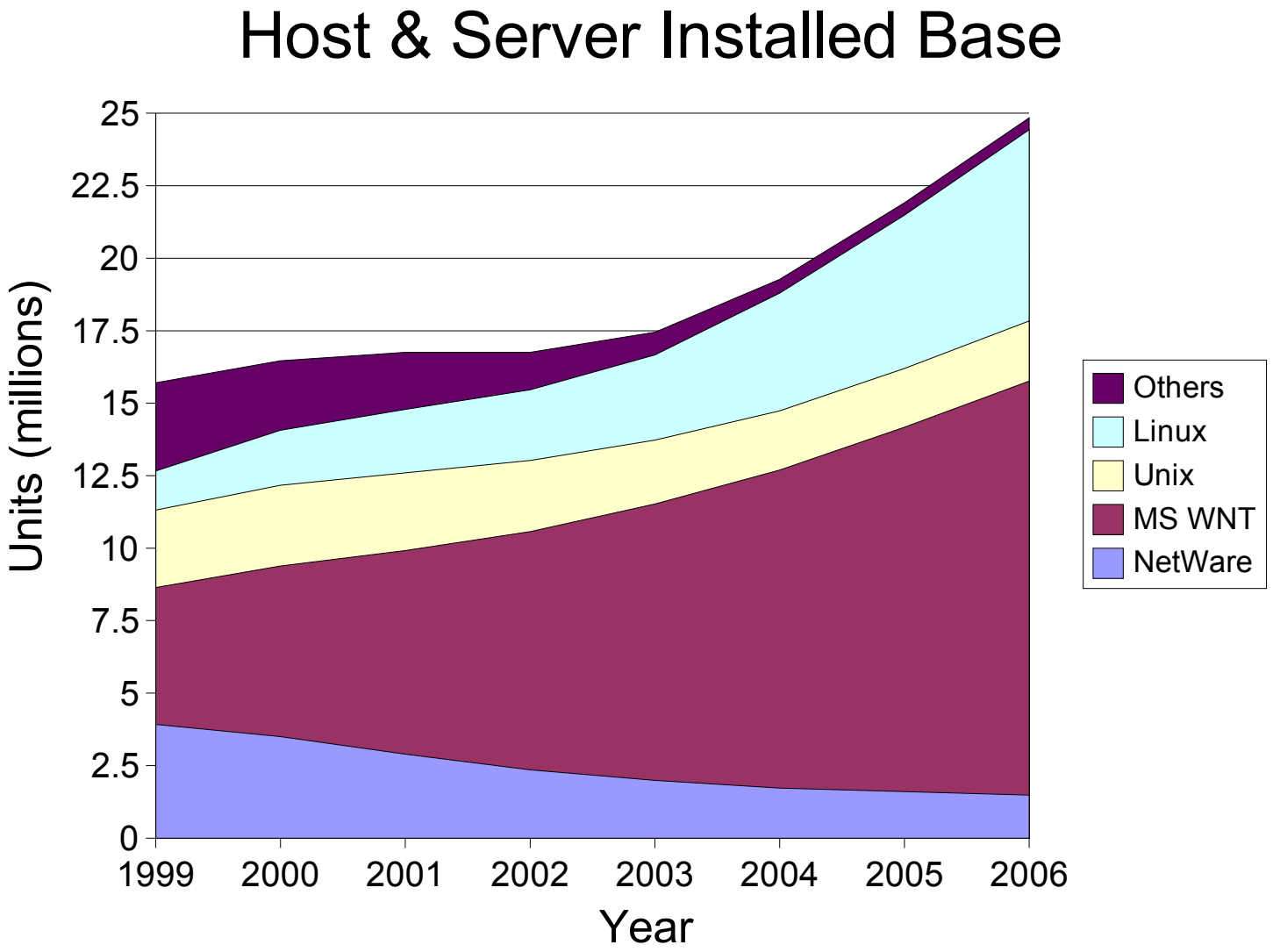
- CIFS is not a standard
  - Constantly changing
    - Microsoft udates add proprietary functionality
  - Protocol is extremely complex
  - Risk that after any service pack or on-line update an old protocol may be broken
    - Affects Microsoft clients as much as Samba
    - Means ALL systems must be kept up to date **and** at the same update / revision level

Future Concerns

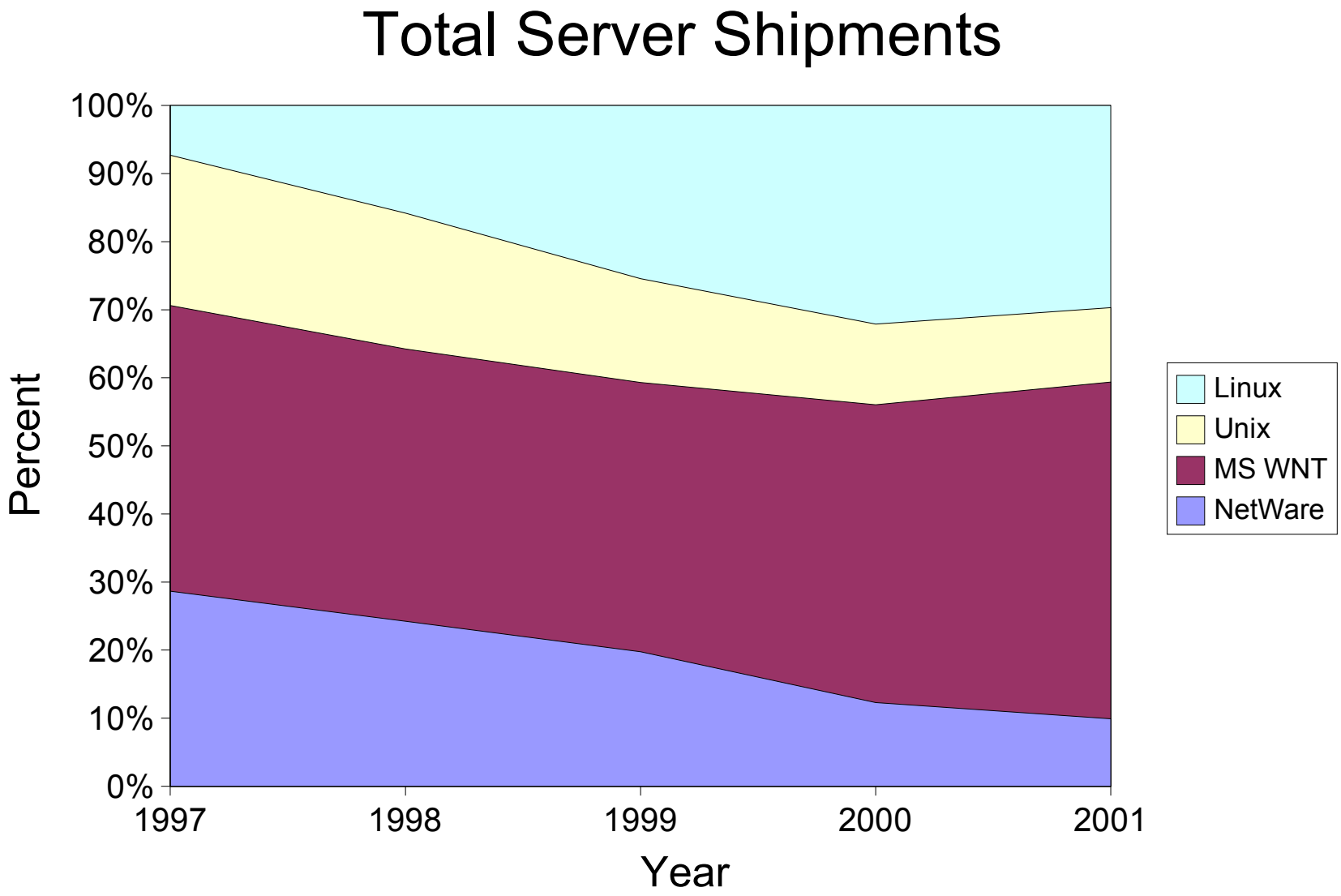
- What MAY change
  - We need to understand the market to see what may happen

... Let's look at some graphs

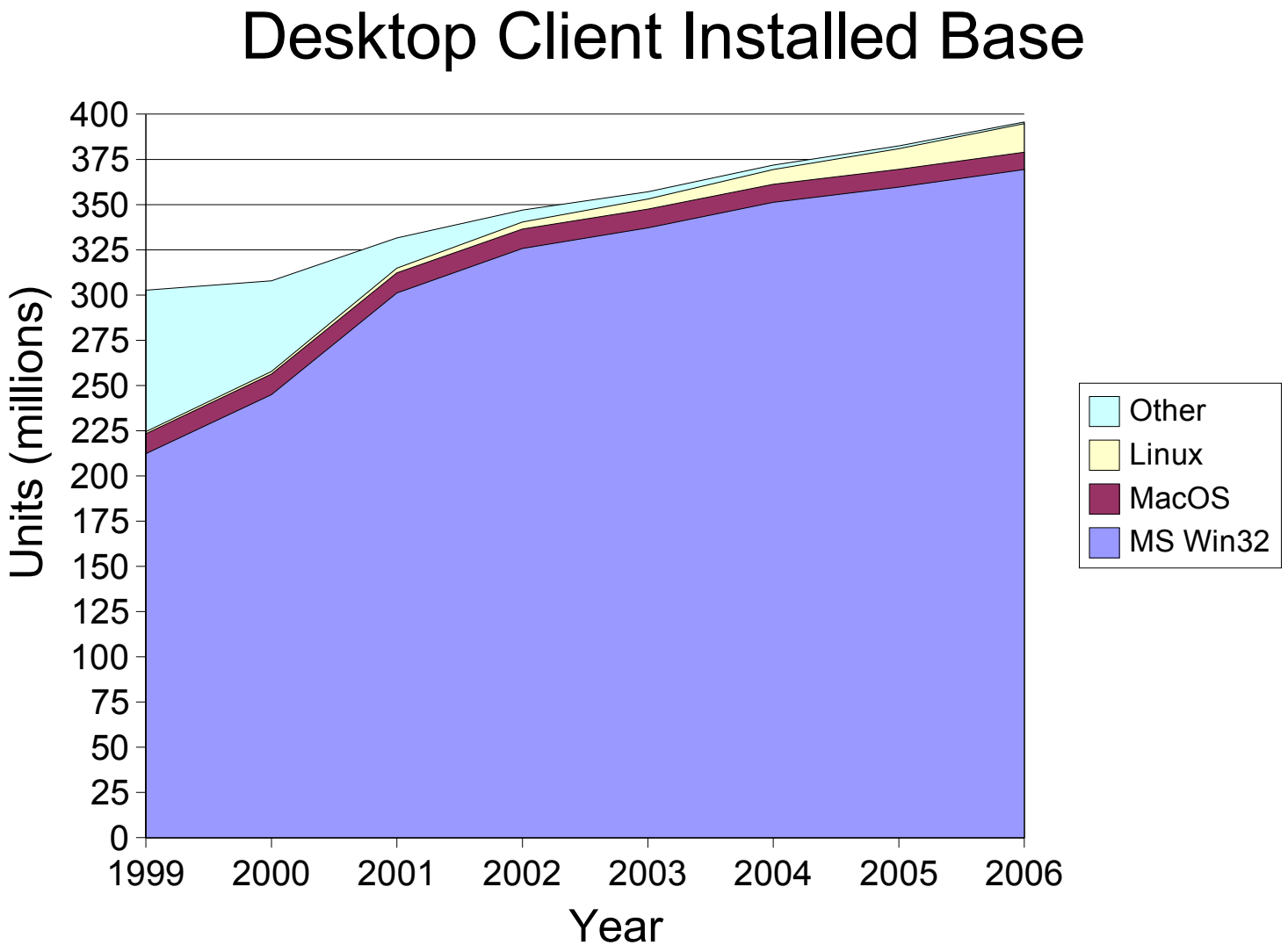
The Installed Server Market



New Server Shipment OS Profile



Installed Desktop Market



Market Conclusions

- MS Windows is Dominant Server Platform
  - CIFS is the dominant File and Print Protocol
    - Is NOT secure
      - Must change!!!!!
    - Is NOT UNIX/Linux oriented
      - Protocol addresses the needs of NTFS
- Windows 200x/XP server shipments exceeds UNIX+Linux
  - Therefore likely to remain dominant well into the future!

Even More Futures

- CIFS is complex - it is time to replace it
  - Session encryption built-in
    - Protected by legislation against reverse engineering
  - Opportunity for Microsoft to replace underlying file system architecture
    - If NTFS can be replaced with an object based technology that has dynamically expandable meta-data capabilities:
      - Means new security measures can easily be added

Market Information

- MS Windows NT4 Migrating to MS Windows Server 200x
  - With Active Directory
  - NAS / UNIX / Linux CIFS usage is growing
- Therefore:
  - Integration need growing

Problem Definition

- CIFS File System operations require
  - Authentication
    - Front-end to access controls
    - Datastore location is a network design decision
      - Can be local to each device or centralized
    - Must know limitation of protocols and methods
  - Identity Resolution
    - Needed to provide unique attributes per user
    - Used to control access to CIFS resources
    - Needs to bridge disparate identity attributes

User Identity Differences

- UNIX / Linux User Identifiers
  - Older – 32 bit Unsigned Int
  - Newer – 64 bit Unsigned Int
    - uid=543(jht) gid=876(users) groups=876(users),71(ntadmin),238(engrs)
- MS Windows has complex security identifiers
  - Incompatible with UNIX / Linux eg:
    - S-1-5-21-1593769616-160655940-3590153233-2013

Bridging the ID Gap

- MS Windows Security Identifiers
  - Design Issues
    - Map to UNIX compatible UID/GID
      - On central store
      - On client / domain member server
    - Store extended information in AD Schema

Cross Machine Integrity

- How to ensure integrity:
  - Provide Consistent UID/GID for all users
  - Essential for cross protocol file sharing
    - CIFS / NFS
- Centralization v's Synchronization
  - Sync solution requires more supervision
  - How secure is sync method?

Technical Background

- Microsoft Active Directory
  - Kerberos / LDAP support
  - In Windows only environment also uses proprietary protocols
- AD is the Authentication and Identity management backend of choice
  - Provides centralized network user identity administration
  - Integrates with external directories through tools like MIIS (was MMS – Microsoft Metadirectory Service)

What works with AD?

- Interoperability Choices
  - Kerberos – complex to install, addresses Athentication
  - LDAP – Identity Management, does not address Authentication
  - Samba Windbind
    - Authentication and Identity Management
    - Has own ID Map solution
  - Vintela Authentication Services
    - Authentication and Identity Management
    - RFC2307 schema extension for UID/GIDs

Pure MIT / Heimdal Kerberos

- Key Limitations
  - Must generate a per client keytab file
    - Need to migrate keytab to each client
  - Time must be kept in sync between AD servers and all Kerberos clients
    - Uses extra external process (NTP)
  - Inconvenient Authentication Only solution
    - Requires client machine pseudo-user account in AD
    - Must sync */etc/passwd* with AD User Accounts to provide UID/GIDs etc.
    - No disconnected mode operation

PADL LDAP Tools

- Available from PADL Software
  - Two modules:
    - pam_ldap, nss_ldap
  - Benefits:
    - Runs on most UNIX platforms today, Free
    - Supports RFC2307 + MS Service for Unix
- Disadvantages
  - Poor Scalability
  - Lacks secure authentication to AD
  - No disconnected mode operation

Samba Winbind

- Has three parts:
  - PAM: pam_winbind.so, handles authentication
  - NSS: libnss_winbind.so, handles identity management
  - Daemon: winbindd, handles communication with remote NT4 DC's and with Active Directory DCs
  - Caches user ID info in winbindd_cache.tdb
- New to Samba-3.0.0 winbind also does all Samba ID Map handling
  - Stores mapping info in winbindd_idmap.tdb
  - Maps Windows SIDs to Unix UIDs/GIDs

Vintela Authentication Services

- Commercial Solution
  - AD RFC2307 AD Schema Extension
  - Microsoft Management Console Snap-In
    - UNIX Account enablement / disablement
    - Stores UID/GIDs and other UNIX account attributes
  - Uses secure Kerberos authentication
    - LDAP over Kerberos
  - AD member client cache
    - Stores only UNIX enabled account info
    - Does periodic intelligent sync to keep current

Making the Choice

Viable choices are:

Method	Authentication	ID Management
Samba Winbind	OK	OK
Vintela Authentication Services	OK	OK
Both	OK	OK

End

Questions / Comments