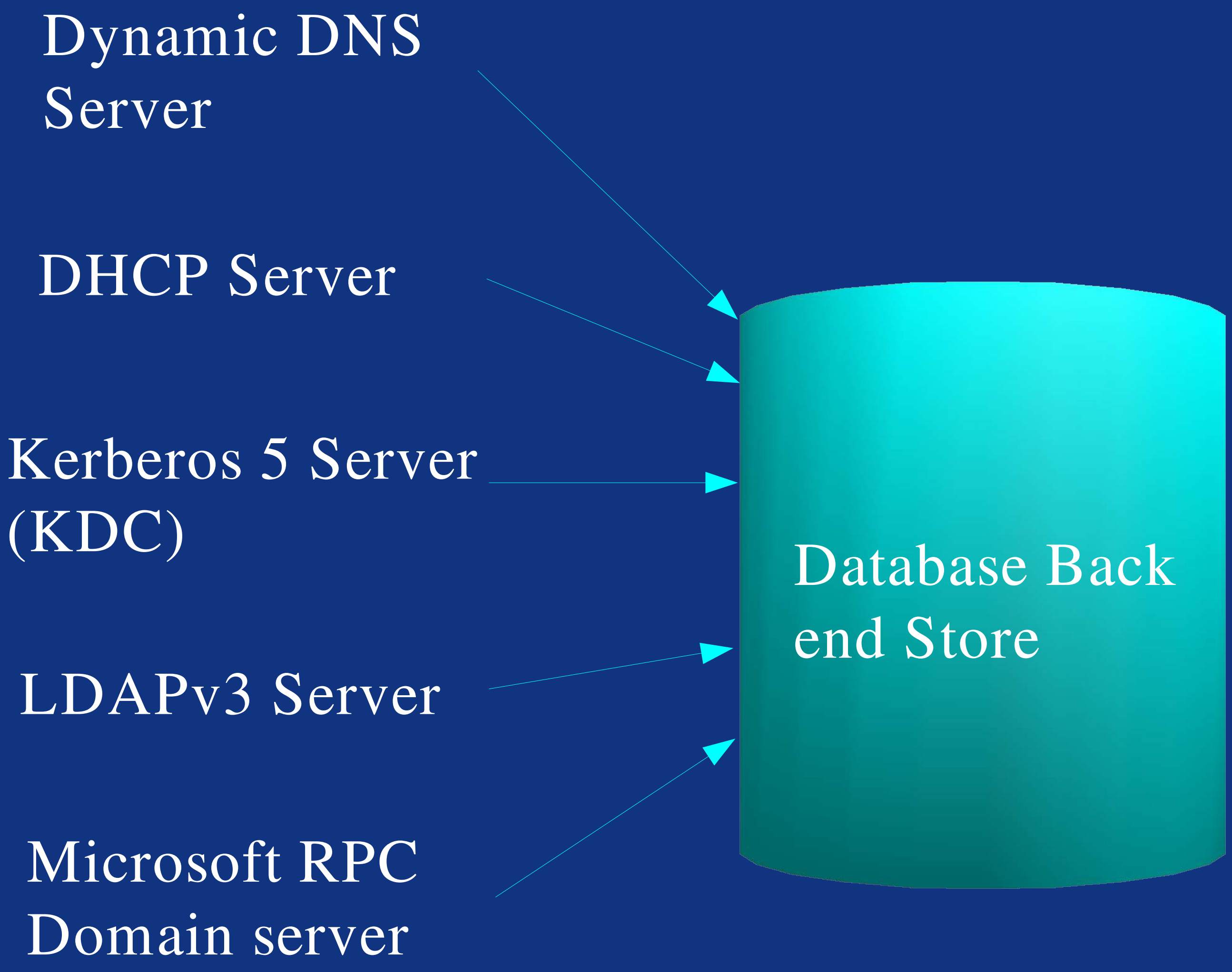
Integration with Active Directory

Jeremy Allison
Samba Team

Benefits of using Active Directory

- Unlike the earlier Microsoft Windows NT 4.x Domain directory service which used proprietary DCE/RPC calls, Active Directory is based on standard Internet protocols.
  - LDAPv3 for directory lookup and updates.
  - Kerberos 5 for authentication (single sign on).
  - DNS for name resolution.
- The hope was that non-Microsoft implementations of these protocols could be used to serve Windows clients allowing true competition for providing these services.
  - Unfortunately this is not the case.

What is Active Directory ?



Dynamic DNS Server

DHCP Server

Kerberos 5 Server (KDC)

LDAPv3 Server

Microsoft RPC Domain server

Database Back end Store

Why must we use an Active Directory Server ?

- Windows clients don't use only the standard protocols to achieve logon services.
- Mandatory “extra” features (like the modified Kerberos ticket and other details) are tied into the Active Directory implementation to enforce vendor lock-in.
  - The practical result of this is that if you want to use Windows clients and servers and obtain all the functionality you paid for then you must use a Windows Active Directory server.
  - IT Staff who recommend an Active Directory roll out without making management aware of this commitment going forward are misleading their executive staff.

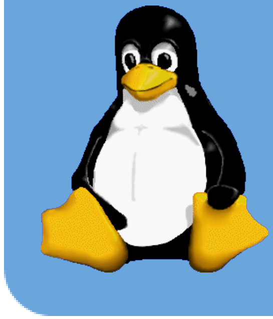
Why must we use an Active Directory Server ?

- Windows clients do not allow replacement of their low-level functionality to ease integration with non-Windows directory servers.
- As usual, it is easier to configure non-Windows systems to interoperate with Windows systems than vica-versa.
  - The free release of Microsoft Services for UNIX does help here, although the protocols used (NIS) are not as secure as using the native protocols of Kerberos and LDAP.
- Active Directory servers can have their LDAP schema (the formal definition of the format of the data they store) extended to allow them to serve non-Windows clients.

What do we mean by integration with an Active Directory Server ?

- For a non-Windows client to integrate successfully into Active Directory we need two operations to be seamless.
  - Authentication of Linux/UNIX accounts against Active Directory.
  - Enumeration of Linux/UNIX user and group directory information stored in an Active Directory store.
- For authentication the preferred method is Kerberos 5 (the native Windows 2000 and above authentication method).
  - Microsoft Services for UNIX, LDAP or MS-RPC can also be used here.
- For user and group enumeration integration LDAP is the preferred method.
  - Microsoft Services for UNIX and MS-RPC can also be used.

Kerberos Authentication Integration



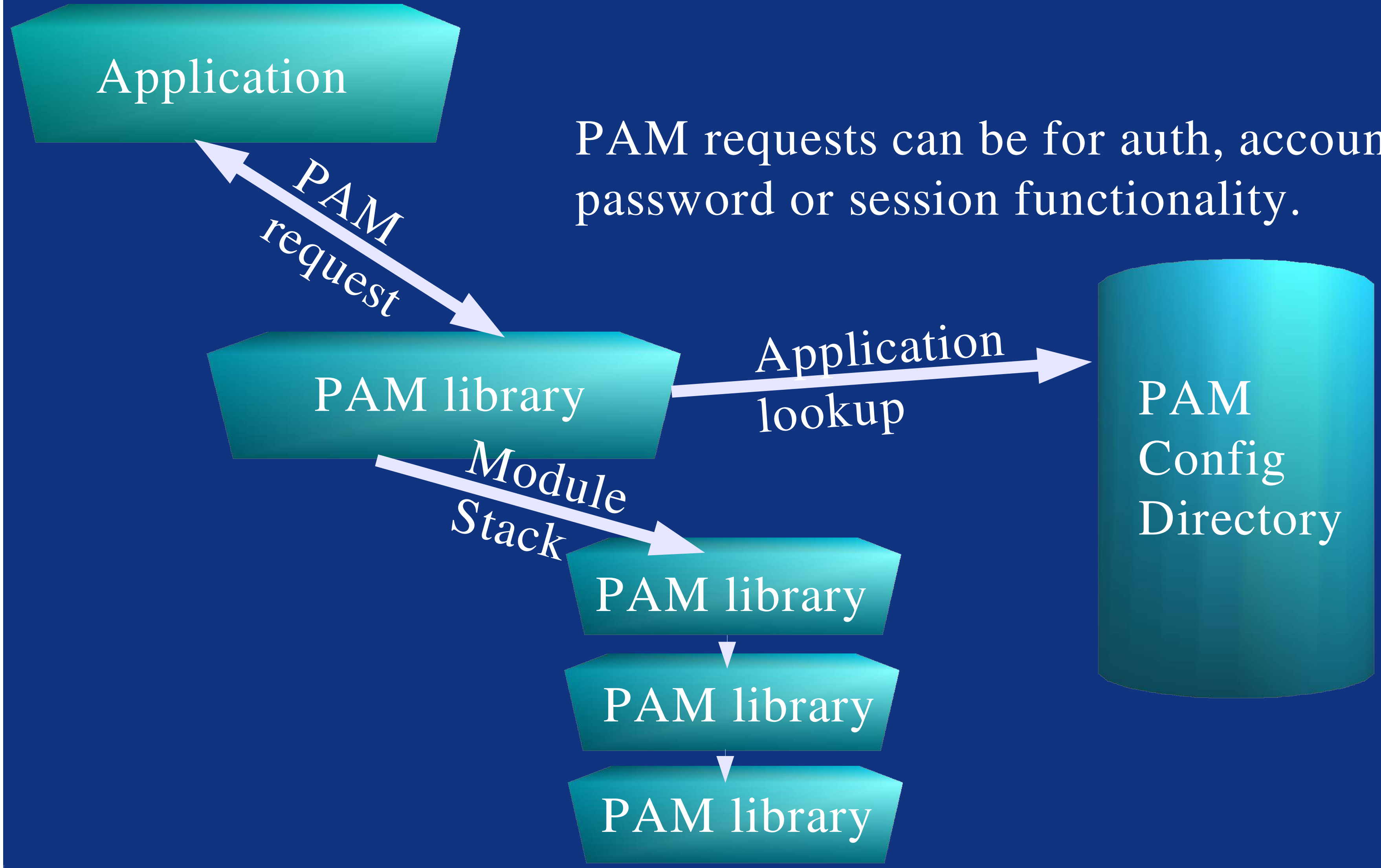
- Active Directory Servers can be Kerberos 5 KDC servers for Linux/UNIX clients.
- MIT or Heimdal Kerberos servers cannot be complete KDC servers for Windows clients due to the missing “extra” data field.
- MIT or Heimdal KDC servers can be set to “trust” AD Kerberos servers if the Windows and UNIX user accounts are separated into separate “realms”.
- In a more integrated environment it is probably easier to just use Active Directory Kerberos Servers (as Microsoft intended by “extending” the standard).

Integrating Windows Authentication Services with Linux/UNIX

- Linux/UNIX systems started with local files containing all authentication information.
- Since then a standardized plug-in architecture has been developed to allow replacement of the authentication information validation (user logons) and maintenance (password changing) with many different possible targets.
  - PAM (Pluggable Authentication Modules) – API invented by Sun and adopted by Linux and other UNIX platforms.

PAM – Pluggable Authentication Modules

PAM requests can be for auth, account, password or session functionality.



PAM on Linux/UNIX systems

- PAM is a standard on Linux and many UNIX systems (HPUX, Solaris and others).
- Over twenty different PAM modules exist to provide all manner of authentication services.
- Three specific modules are of interest for Active Directory Integration
  - Kerberos – pam_krb5 (http://pam-krb5.sourceforge.net)
  - LDAP – pam_ldap (http://www.padl.com)
  - Samba/Microsoft RPC – pam_winbind (http://www.samba.org)

Kerberos - pam_krb5

- Takes the users clear-text password and validates it against a standard Kerberos 5 server (Active Directory adds extra proprietary data into the returned ticket, but the client libraries on Linux/UNIX ignore this data).
- Returns a Kerberos 5 Ticket-Granting-Ticket (TGT) which can be used to get tickets for other services.
- Care must be taken to ensure the encryption method used by default by Windows (RC4-HMAC) is available on the Linux/UNIX Kerberos system.
- Source code available, Open Source/Free Software.

LDAP - pam_ldap

- Takes the users clear-text password and validates it against an LDAP server by attempting to set up an LDAP connection as the given username/password pair.
  - Must be set up to use SSL/TLS in order to securely validate the password (pam_krb5 doesn't have this problem, all kerberos exchanges are secure).
  - Developed by PADL software – available as Open Source/Free Software.

Samba - pam_winbind

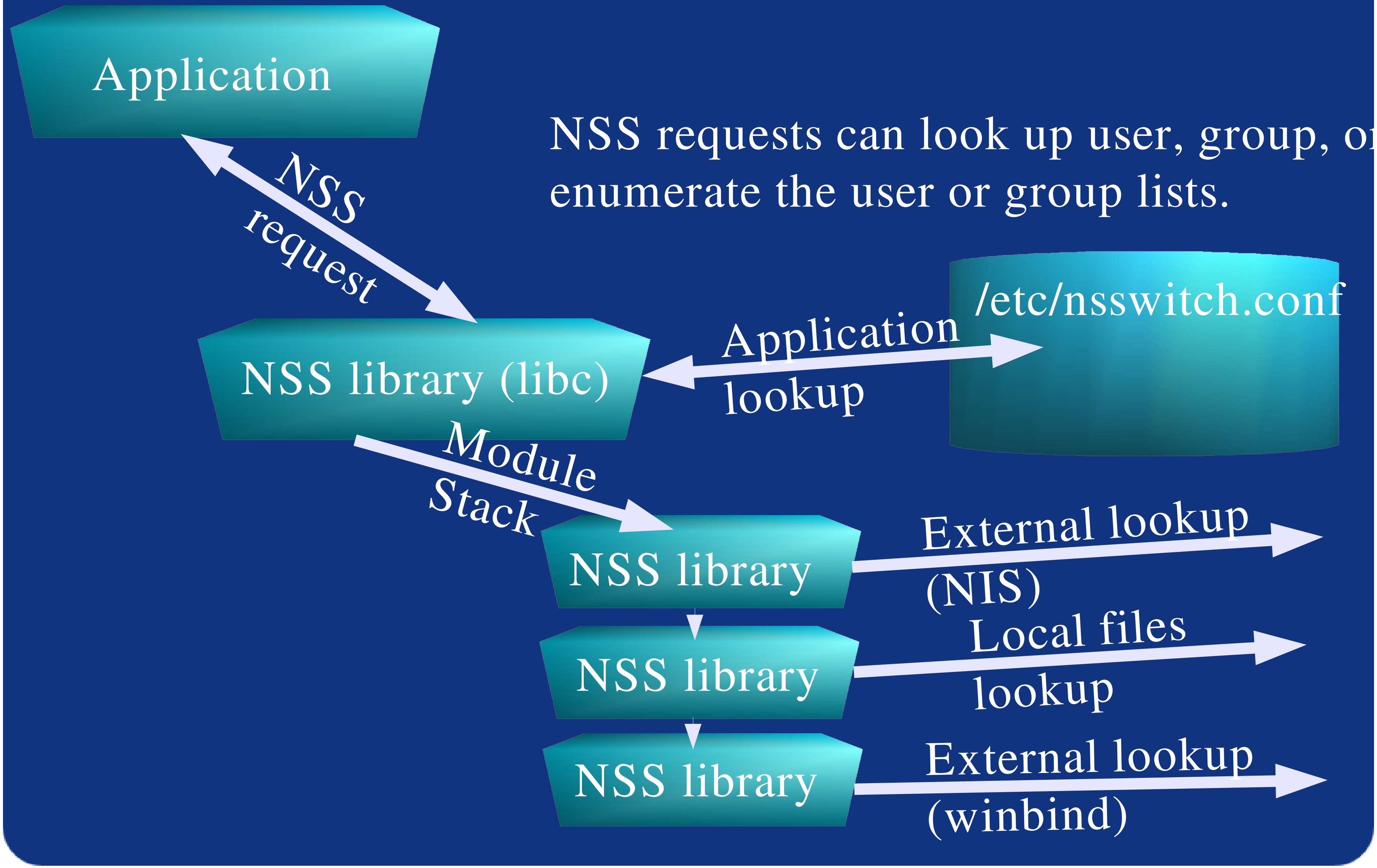
- Allows a Linux/UNIX user to authenticate in exactly the same way as if they were logging on to a Microsoft member server in the Domain.
  - Requires a working Samba set-up (more details later).
  - Completely integrates the Linux/UNIX authentication mechanism into the Windows world – identical to a Windows server.
  - All of Samba is Open Source/Free Software.

Integrating Windows User Directory Services with Linux/UNIX

- Linux/UNIX systems started with only local directory listings (local files) and have since had to develop standardized plug-in architectures to allow replacement of the directory service with any compatible server (no hidden protocols).
  - NSS (Name Service Switch).
  - NSS allows user and group lookup and enumeration to be done via many different directory services. The order in which they are queried can be changed.
  - The nss modules that are of interest for Active Directory Integration are :
    - nss_ldap
    - nss_winbind

NSS – Name Service Switch

NSS requests can look up user, group, or enumerate the user or group lists.



LDAP - nss_ldap

- Written by PADL software (as is pam_ldap) this library allows Linux/UNIX systems to look up users and groups stored in an Active Directory server.
- The Active Directory Schema must have been extended from the standard schema by including either the RFC2307 schema (created by PADL) or the schema used by Microsoft's Services for UNIX product.
  - The Linux/UNIX user and group information must already exist in the Active Directory as part of the schema.
  - This requires some extra administration to add the extra information to the existing Active Directory data.

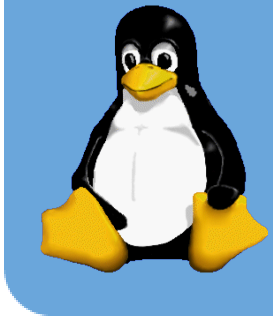
Samba - nss_winbind

- Part of the complete solution provided by Samba (will be described in detail later).
- Does not require any changes to the Active Directory Schema.
- Does require a working Samba set up and the Linux/UNIX machine to have been added as a “member server” into the Active Directory.

Microsoft Services for UNIX - nss_nis

- Does not talk directly to the Active Directory Server but to a NIS (Network Information Services) gateway running on a Windows server.
- As with nss_ldap, requires additions to be made to the Active Directory Schema to add the Linux/UNIX (POSIX) definitions.
- Useful for older UNIX installations that will only use the NIS protocols (regarded as insecure in modern UNIX systems).
- NIS protocol developed by Sun in late 1980's.

Three Complete Solutions for Active Directory Integration



PADL SOFTWARE

Microsoft® Windows™ Services for UNIX

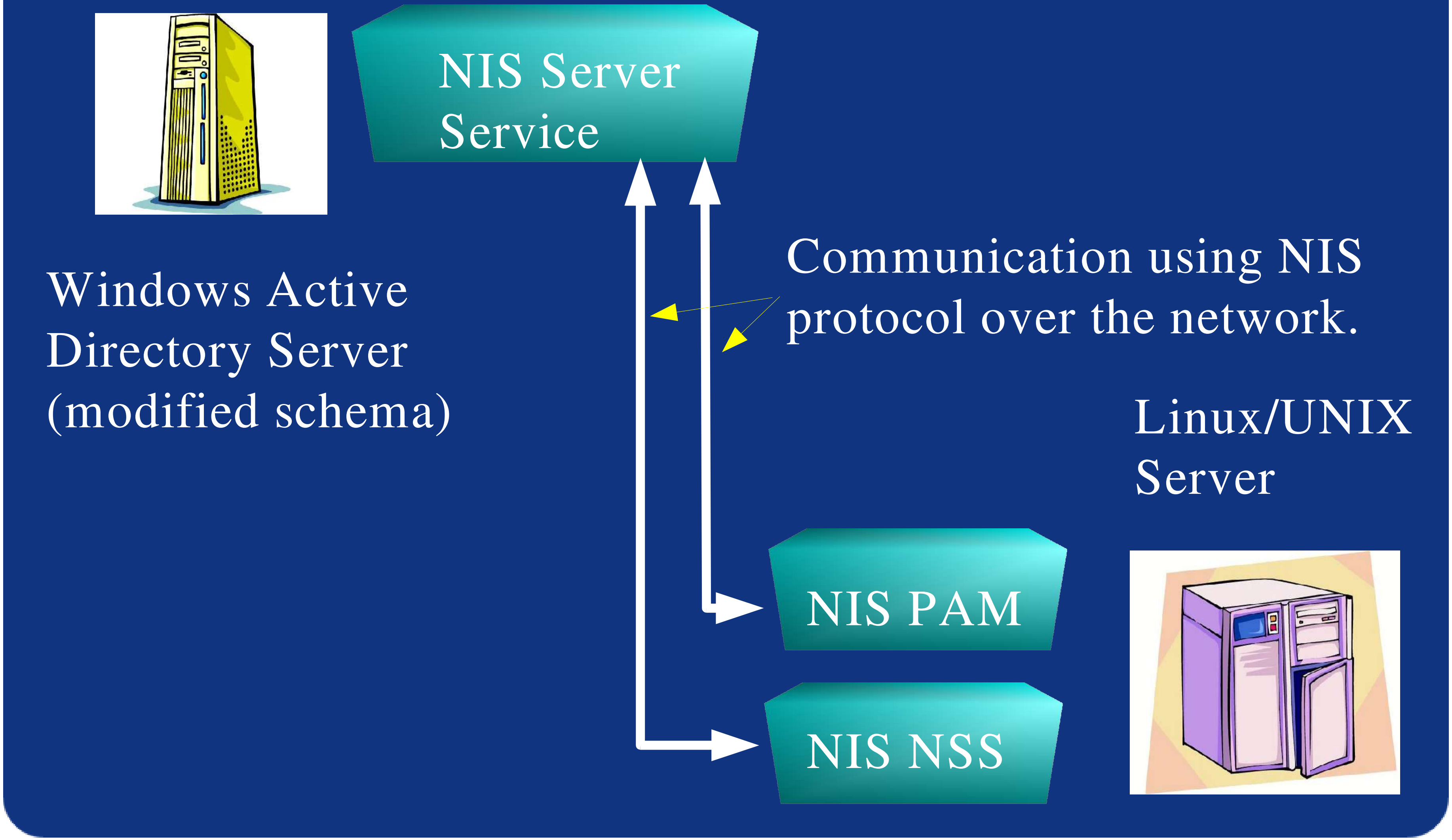
samba

PADL solution

- Modify Active Directory with either the RFC2307 schema definition or the Microsoft Services for UNIX schema.
- Install pam_ldap (or alternatively pam_krb5) to handle the authentication from the Linux/UNIX systems.
- Install nss_ldap to handle the directory service enumeration from the Linux/UNIX systems.
- Probably the easiest choice for organizations with significant existing Linux/UNIX experience.
- Secure, robust solution but requires work to maintain.

Services for UNIX solution

Microsoft Windows Services for UNIX



NIS Server Service

Windows Active Directory Server (modified schema)

Communication using NIS protocol over the network.

Linux/UNIX Server

NIS PAM

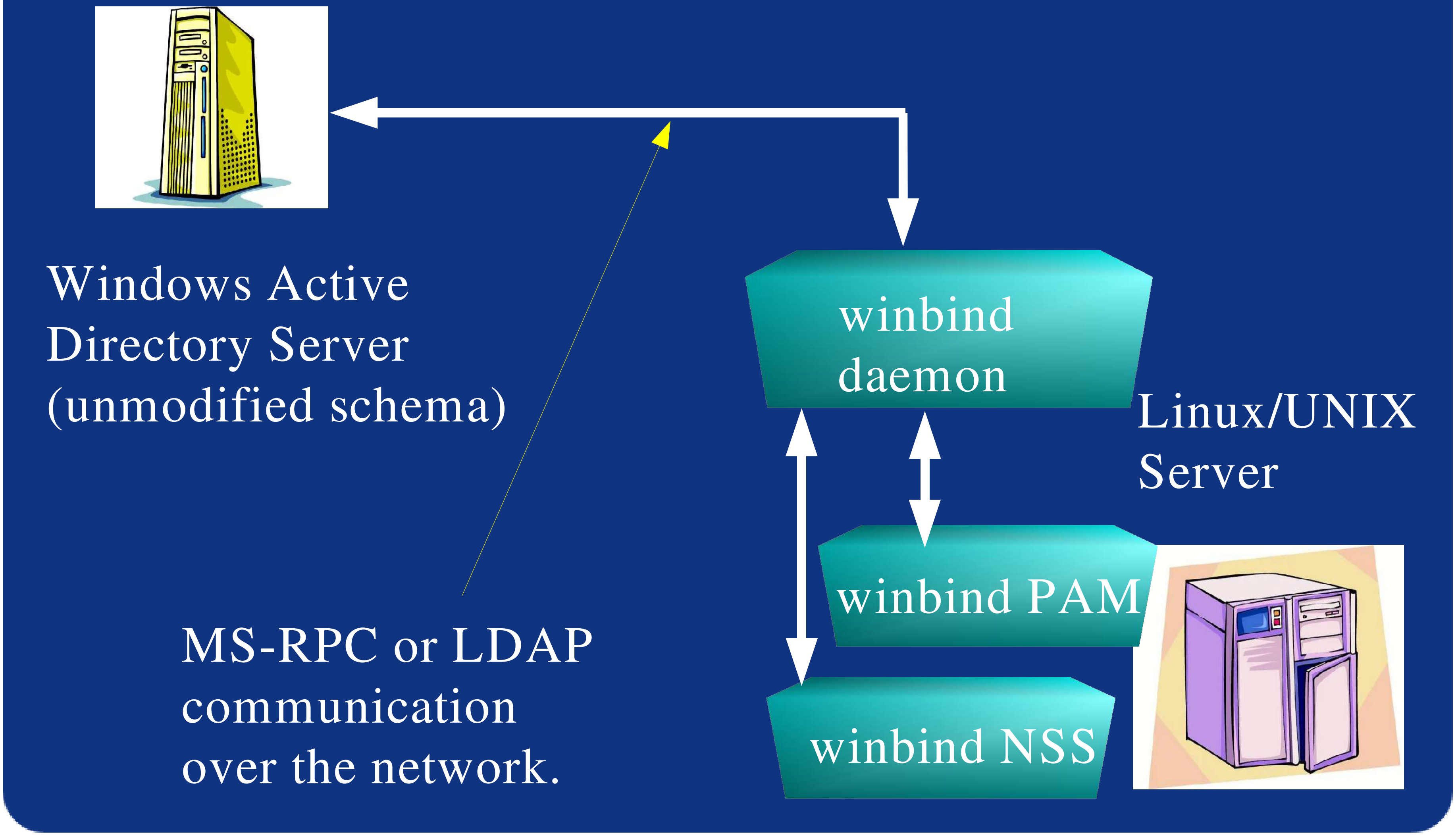
NIS NSS

Services for UNIX solution

Microsoft® Windows™ Services for UNIX

- Uses older NIS protocol – an older UNIX standard.
  - Modern Linux/UNIX systems use either NISPLUS (encrypted version of NIS) or LDAP or Kerberos for password verification.
- Now Microsoft has made Services for UNIX available for free this is now a competitive solution.
  - No source code available, unlike other solutions.
- Good choice if an organization is mainly Windows, with a few older Linux/UNIX machines for which security is not a priority.

Samba winbind solution



Windows Active Directory Server (unmodified schema)

winbind daemon

Linux/UNIX Server

winbind PAM

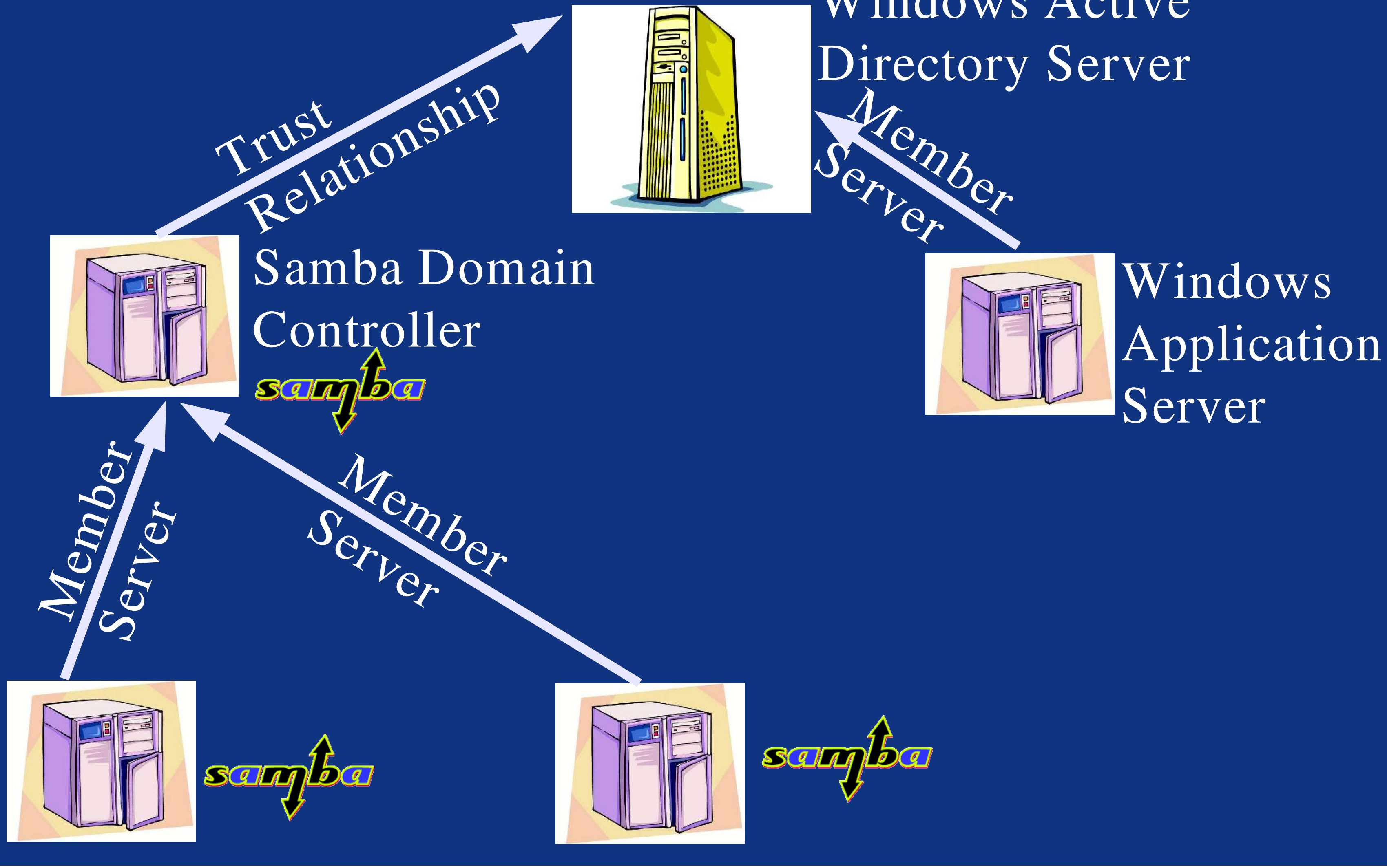
winbind NSS

MS-RPC or LDAP communication over the network.

Samba winbind solution

- Allows a Linux/UNIX machine to completely emulate a Windows member server.
- No changes to Active Directory schema needed – winbind copes with mapping Windows users and groups to Linux/UNIX users and groups.
- Allows Windows clients accessing file and print (Samba) services on the Linux/UNIX server to pass kerberos 5 tickets to obtain service (as to a Windows file server).
- To synchronize user and group mapping between multiple Linux/UNIX servers using winbind an external LDAP server must be used (not completely transparent).
- Uses the same protocols as Windows servers for enumerating

Integrating Samba



Windows Active Directory Server

Trust Relationship

Samba Domain Controller

Member Server

Windows Application Server

Member Server

Member Server

Conclusions

- Windows Active Directory is a necessary evil if you have large numbers of Windows clients.
  - The moral of this is if you're not piloting a desktop Linux program, you're paying too much for your Microsoft client software .
- Options are PADL Open Source code, Microsoft Services for UNIX, or Samba to provide no-cost integration between your Linux/UNIX machines and Active Directory.
- All solutions have complexity involved – set up a test environment to determine which best matches your business (no surprises here).

http://www.hp.com/linux

http://www.samba.org