

PENNSSTATE



Penn State Windows Active Directory

Win-AD Team

win-ad@aset.psu.edu

<http://aset.its.psu.edu/docs/windows/>

Agenda

- Objectives
- K5 Trust
- Security
- Account Management
- DNS
- Child Domains
- Applications
- Groups
- Roaming Profiles

References

- *University of Michigan:* <http://www.umich.edu/~lannos/windows/index.html>
- *Yale University:* <http://wss.yale.edu/win2k/ad-and-ddns.html>
- *Microsoft Kerberos Interoperability:*
<http://www.microsoft.com/windows2000/techinfo/howitworks/security/kerbint.asp>
- *Microsoft Step by Step Guide to Kerberos Interoperability:*
<http://www.microsoft.com/windows2000/techinfo/planning/security/kerbsteps.asp>

Objectives

- Phase I
 - K5 trust
 - Account management
 - DNS
- Phase II
 - LDAP sync
 - Addition of Groups
 - Roaming Profiles

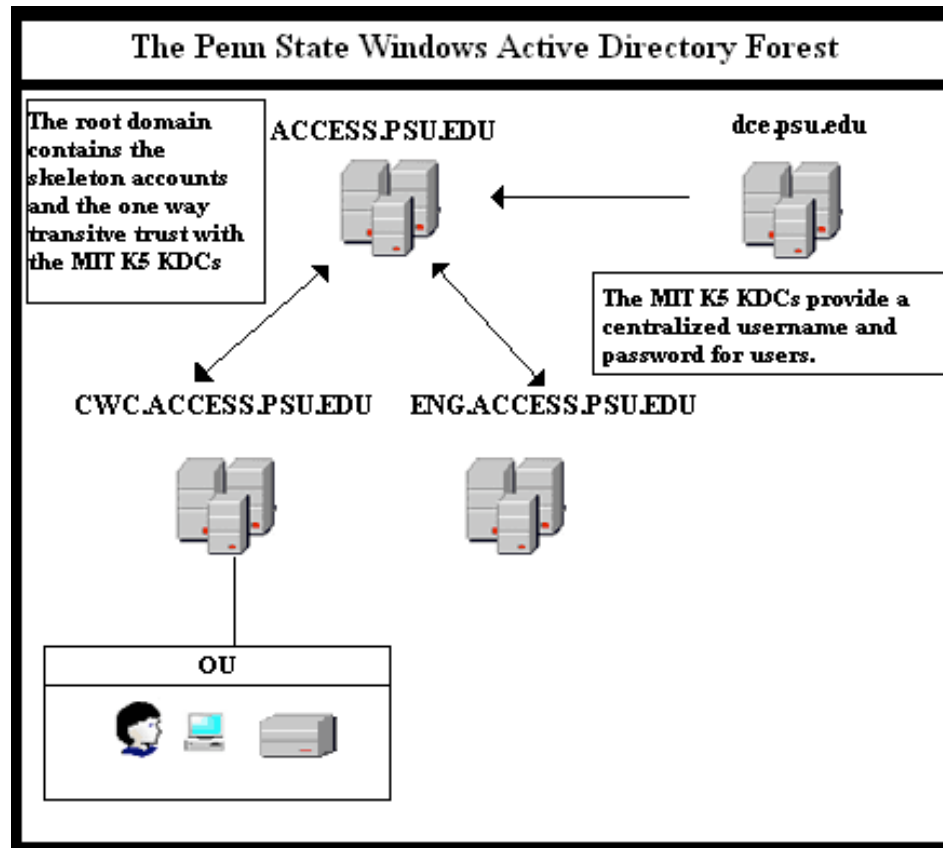
K5 Trust

- Trust models that were considered
 - MIT to Root to Child domain
 - Direct K5 to your Root
 - MIT to Root to Tree
 - MIT to Root to Root

K5 Trust (cont.)

- MIT to Root to Child domain
 - Advantages
 - We take care of user accounts, groups and trust management
 - Provides a single windows identity for a user
 - Full control over your child domain
 - Disadvantages
 - Schema extensions must be implemented by us
 - User attributes must be change by an ACCESS administrator

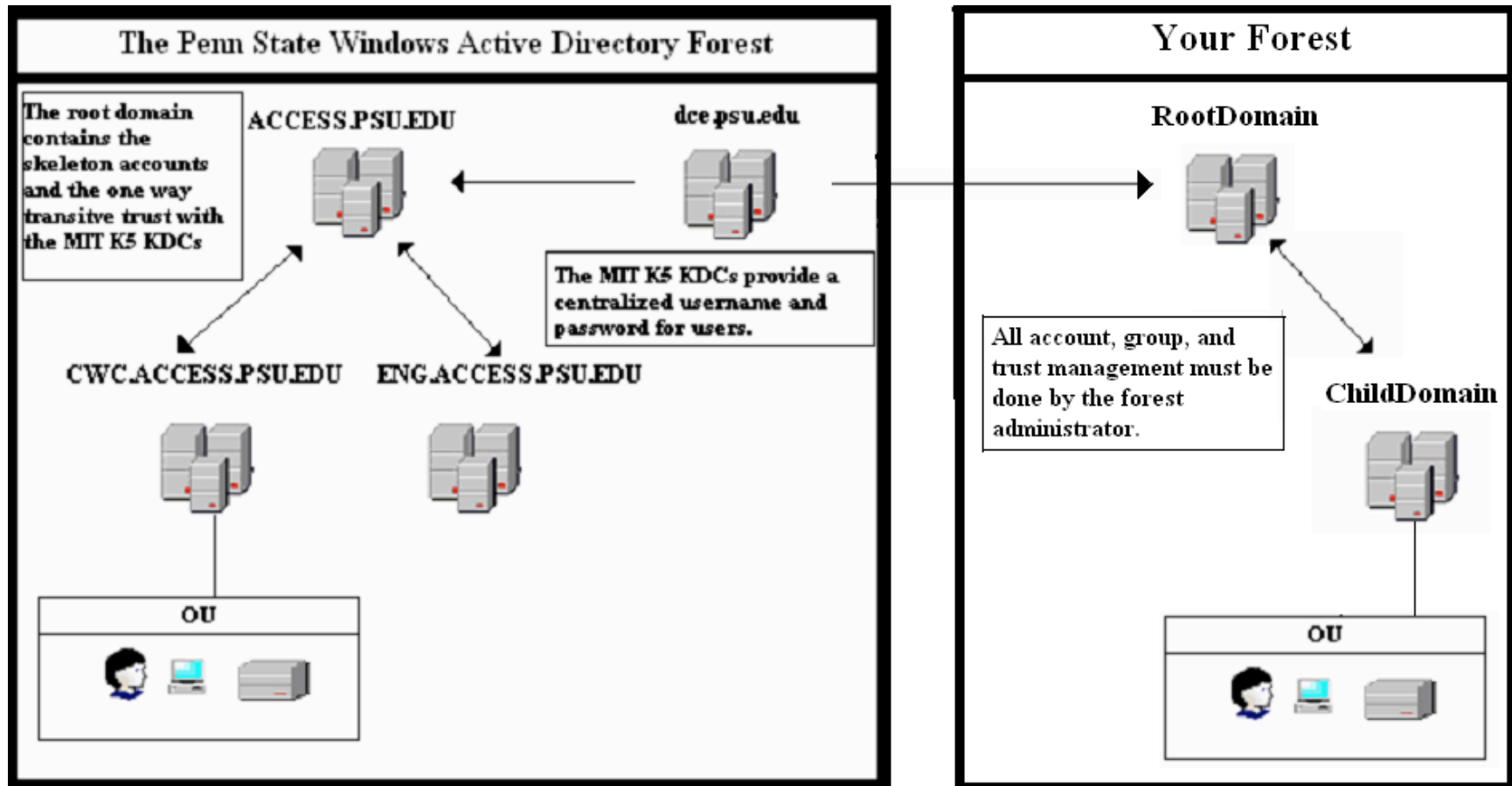
K5 Trust (cont.)



K5 Trust (cont.)

- Direct K5 to your Root
 - Advantages
 - Full control over everything
 - Disadvantages
 - All user, group and trust management must be done by you
 - Users can not access any resources outside your forest.

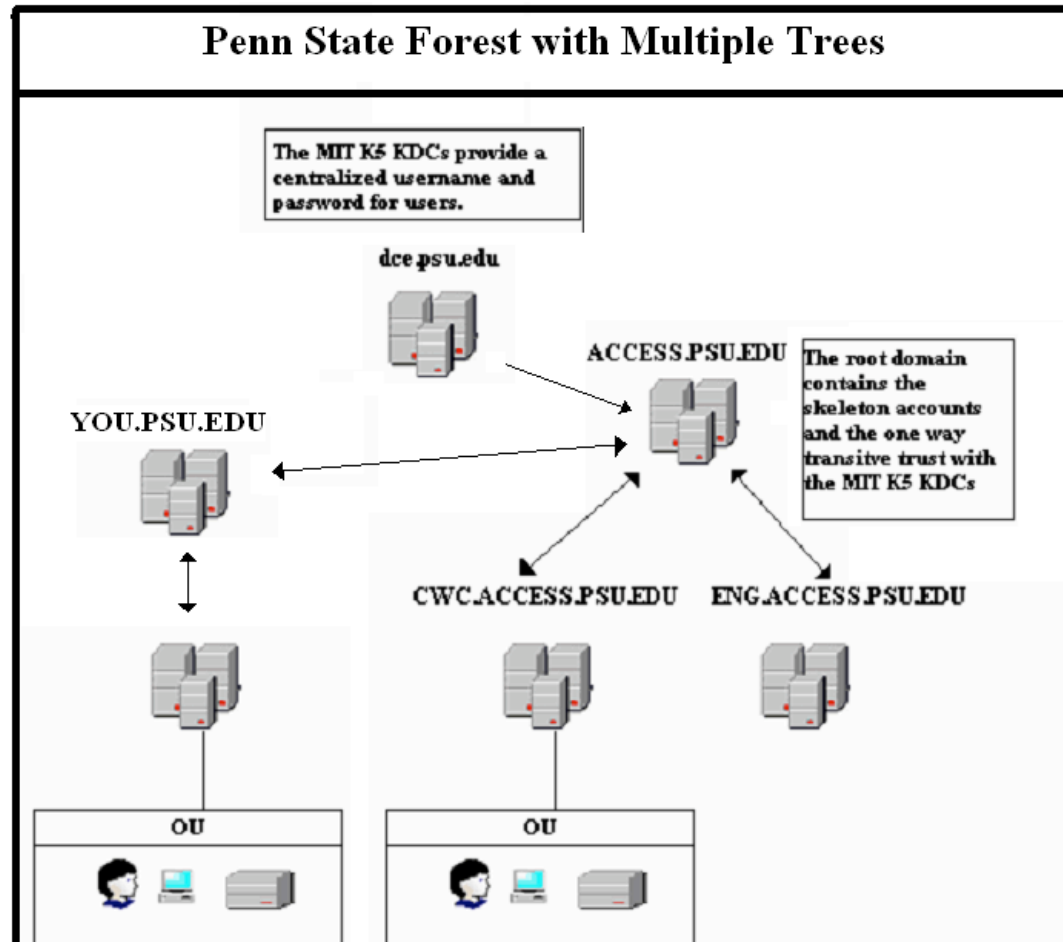
K5 Trust (cont.)



K5 Trust (cont.)

- MIT to Root to Tree
 - Advantages
 - None
 - Disadvantages
 - All user and group management must be done by you
 - Schema extensions must be approved

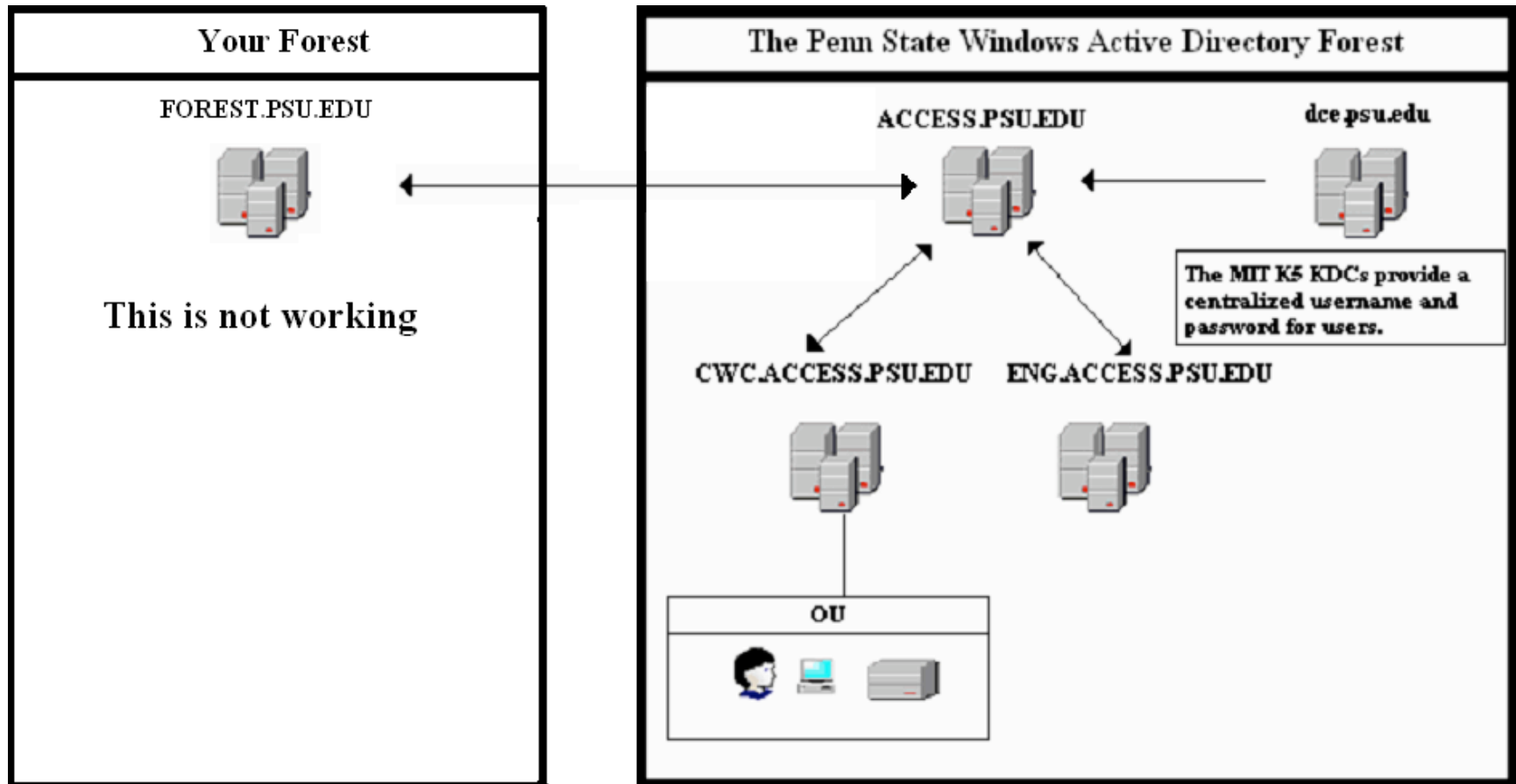
K5 Trust (cont.)



K5 Trust (cont.)

- MIT to Root to Root
 - Advantages
 - Full control over your forest with out needing to manage accounts, groups and trusts.
 - Disadvantages
 - **DOES NOT WORK**

K5 Trust (cont.)



Security

- Can other domain administrators get into my domain?
 - No, with the exception of Enterprise Administrators
- Can I keep users from accessing resources in my domain?
 - Yes, you can limit access to resources based on groups or on a per user basis.

Account Management

- For authorization purposes, we must map an account to the MIT K5 ticket
 - Tickets are mapped by putting the PAC data in the Kerberos ticket
- We accomplish via skeleton accounts
 - Uses dummy passwords
 - Accounts are created in real time
 - We will sync user information in AD with information in the current LDAP server

DNS

- Goals
 - Fully integrate Active Directory name space into existing name space
 - To work with existing name service infrastructure
 - Adhere to all University Policies

DNS (cont.)

- Active Directory Domain names separated from DNS SubDomain names:
 - Host principles are created correctly
 - SRV records are recorded correctly
 - `_http.psu.edu IN SRV 0 100 80 www.psu.edu.`
 - Host A/PTR records are maintained separately
- Windows assumptions
 - Short names

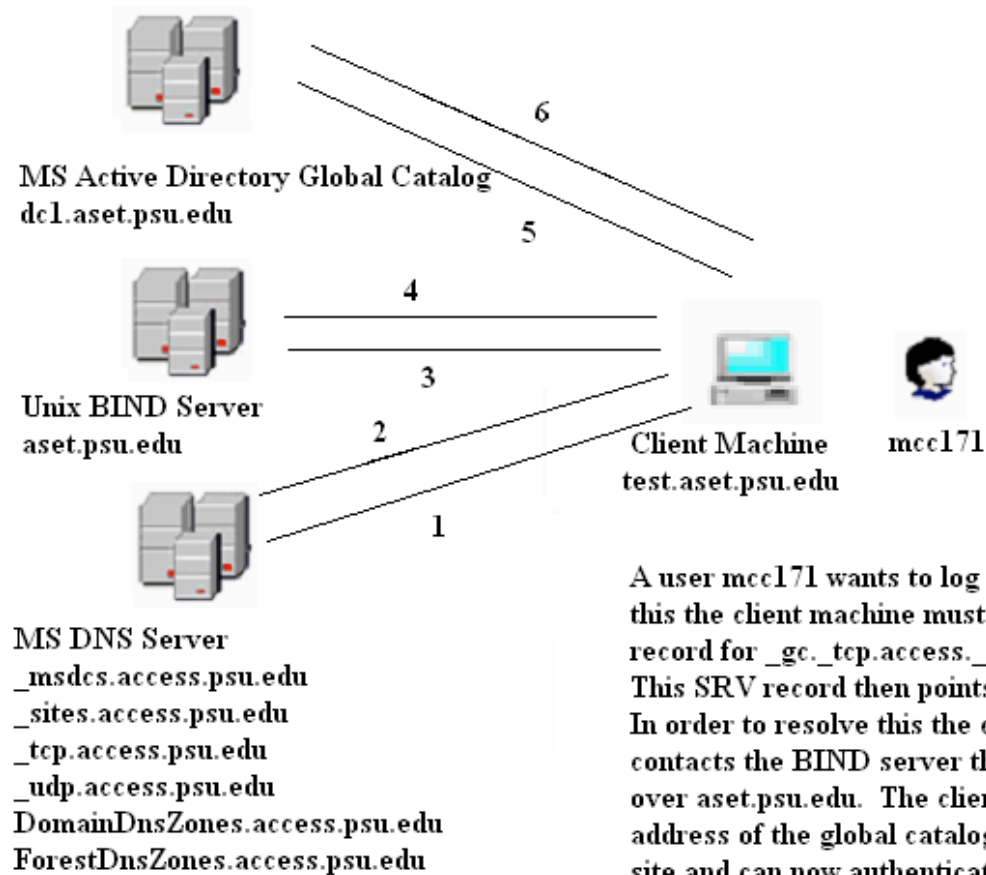
DNS (cont.)

- MS DNS Integration
 - Microsoft DNS servers handle dynamic updates
 - Six DNS SubDomains or NS records (root)
 - `_msdcs.access.psu.edu`
 - `_sites.access.psu.edu`
 - `_tcp.access.psu.edu`
 - `_udp.access.psu.edu`
 - `DomainDnsZones.access.psu.edu`
 - `ForestDnsZones.access.psu.edu`
 - Five DNS SubDomains or NS records (child)
 - `_msdcs.aset.access.psu.edu`
 - `_sites.aset.access.psu.edu`
 - `_tcp.aset.access.psu.edu`
 - `_udp.aset.access.psu.edu`
 - `domaindnszones.aset.access.psu.edu`

DNS (cont.)

- Windows domain is ACCESS
 - SRV records are stored in six sub zones
 - `_kerberos._tcp.access.psu.edu. 10M IN SRV 0 100 88 dc1.aset.psu.edu. (root domain)`
 - `_kerberos._tcp.aset.access.psu.edu. 10M IN SRV 0 100 88 medusa.aset.psu.edu. (child domain)`
 - No hostnames
- Compliant with TNS policy
 - <http://tns.its.psu.edu/policies/dns.html>

DNS (cont.)



Child Domains

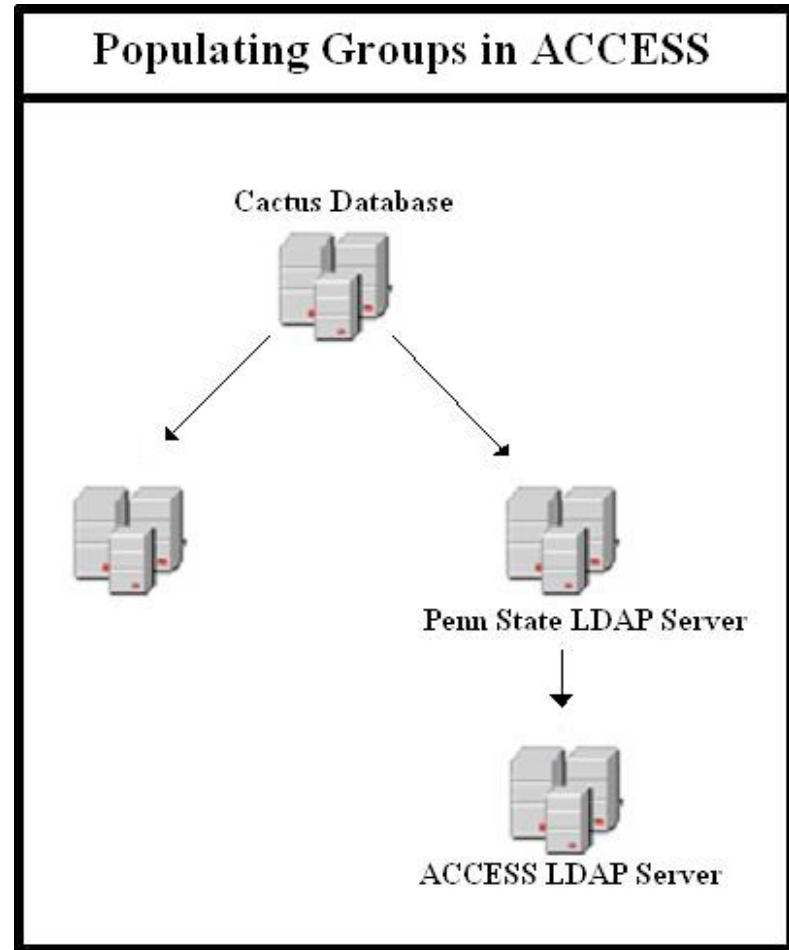
- Installation
 - Apply
 - Receive an administrative account
 - Promote the first DC
- KDC registry entries
- Group Policies

Applications

- Exchange
 - Tested using KPOP and Outlook Web Access
 - KPOP will not work outside the forest
- IIS
 - Tested using integrated auth and basic auth
- Live Communication Server
 - Schema extensions done
 - Software has not been tested
- Systems Management Server
 - Schema extensions done
 - Software has not been tested

Groups

- Groups will be pushed from the existing LDAP server
- Not tested yet



Roaming Profiles

- Concerns
 - Bandwidth
 - Connections to non-UP locations may be slow
 - Existing storage space (PASS)
 - Confusing re: the different storage space options
 - Security
 - PASS will not (to date) allow us to store user profiles
 - Users can gain access to their respective PASS without reauthenticating

Roaming Profiles (cont.)

- Three solutions being considered
 - MS Dfs
 - Using Dfs we can redirect a roaming profile to the location of the users
 - To simplify storage spaces we can redirect a user's home directory and My Documents etc. to the user's PASS
 - A variable set by the administrator
 - No roaming profiles

Summary

- Phase I
 - K5 trust
 - Account management
 - DNS
- Phase II
 - LDAP sync
 - Addition of Groups
 - Roaming Profiles

Questions/Comments?