



BrainBuzz

Cramsession

Last updated June, 2000. Click [here](#) for updates.

Click [here](#) to see additional documents related to this study guide.

Contents

Contents.....	1
Basic Directory Service Concepts	2
DNS Deployment	7
W2K Groups.....	8
Domain Tree Modeling & Migration	9
Changes occurred in the Access Control Components.....	13
Steps for performing the migration and dissolving resource domains into OUs....	14
Windows 2000 Domain Modes	15
Domain Restructure	16

Cramsession™ for Migrating from Microsoft Windows NT 4.0 to Microsoft Windows 2000

Abstract:

This Cramsession will help you to prepare for Microsoft exam 70-222, Migrating from Microsoft Windows NT 4.0 to Microsoft Windows 2000. Exam topics include Developing a Migration Strategy, Preparing an Environment for Migration, Planning & Deploying a Domain Upgrade, Planning & Deploying an Intra-Forest or Inter-Forest Domain Restructure, and Troubleshooting.



Notice: While every precaution has been taken in the preparation of this material, neither the author nor BrainBuzz.com assumes any liability in the event of loss or damage directly or indirectly caused by any inaccuracies or incompleteness of the material contained in this document. The information in this document is provided and distributed "as-is", without any expressed or implied warranty. Your use of the information in this document is solely at your own risk, and Brainbuzz.com cannot be held liable for any damages incurred through the use of this material. The use of product names in this work is for information purposes only, and does not constitute an endorsement by, or affiliation with BrainBuzz.com. Product names used in this work may be registered trademarks of their manufacturers. This document is protected under US and international copyright laws and is intended for individual, personal use only. For more details, [visit our legal page](#).

Migrating from Microsoft Windows NT 4.0 to Microsoft Window 2000 -_Cramsession

Basic Directory Service Concepts

Pre-Windows 2000 Domain Models

Single domain model

- one primary domain controller (PDC) to hold the master copy of the Security Account Manager database
- one or more backup domain controllers and several member servers in the domain
- only one copy of the SAM database that is modified at any given time at the PDC

Master domain model

- partitions network resources into separate domain spaces
- **resource domain** houses resources
- **master domain** holds Windows NT user and machine account definitions, and has the Security principal definitions defined
- a minimum of a single one-way Local Security Authority (LSA) trust relationship is needed to allow the centrally defined security principals to access resources housed in the resource domain

Multiple master domain model

- **multiple master domains** house the security principal definitions for specific pieces of the organization
- mostly used when there are geographical or organizational boundaries in the corporation or enterprise

Complete trust model

- a LSA trust is established between all created Windows NT 4.0 domains
- security principal definitions in any of the established Windows NT 4.0 domains can be granted access to any resource defined in any of the existing domains

Windows 2000 Active Directory Domain Model and other new architectural enhancements

Physical architecture

- a **domain** is a partition in the namespace where a common security policy applies
- all domain controllers in the same domain contain the entire directory for the domain
- replicating objects happens on the domain level
- domain controllers never replicate domain objects to domain controllers in different domains

2 Tier Logical Architecture

- hierarchy of domains that have trust relationships to each other
- two levels of hierarchies inside the tree--the hierarchy of the **domains** and the hierarchies of **OUs within the domains**
- **organizational unit (OU)** is a container that can host other objects, and is used for delegating administrative rights
- each domain can implement its own OU hierarchy
- allows organizations to create an environment that mirrors the business's organization

Naming

- uses Domain Name System (DNS)-based naming style founded on the LDAP proposals. Eg: i@DC=sales, DC=mycompany, DC=com, o=Internet.
- allows enterprises to leverage an existing DNS namespace, or use the already registered DNS domains to register the directory service in the Internet
- in a contiguous namespace, the name of a child domain always contains the name of the parent domain as a part of its name, and the name of the parent domain can always be constructed by removing the first part of the child domain name. Also, a domain controller always creates referrals to the child domains, which affects LDAP search operations.
- in a disjointed namespace, the names of the parent and child domains are not directly related to each other, and no referrals are ever created
- in forest, namespaces are disjointed between trees
- subdomains in all trees implement contiguous namespace
- any object in the Active Directory can have several names-a common name, a relative name, and so forth. The only object identifier that can never be changed is the object's **Globally Unique Identifier (GUID)**.
- algorithm used for GUID creation ensures that a GUID can never be duplicated
- there is no requirement for a relationship between the domain name of a client or server and the DNS domain name of the directory service

Objects Schema

- defines what objects and properties can be created in the directory
- forest is a set of trees that share a common schema, configuration, and global catalog, with Kerberos trust among all members of the forest
- default schema includes all objects and properties that are required for the directory service to work, and is replicated to all domain controllers in the forest
- can always be extended to create new properties and classes

Directory data store

- **Extensible Storage Engine (ESE)** is an improved version of the Jet database
- max 17 terabytes in size - 10 million objects
- can store multi-value properties

Replication

- uses **multi-master replication**- does not distinguish between primary and backup domain controllers
- objects can be created or manipulated on any domain controller
- replication based on **Update Sequence Numbers (USNs)** comparison
- if properties on the same object are changed on different domain controllers, comparison will be based on version number, timestamp or binary buffer size
- administrators have the option of recovering and using the rejected values

Conflicts Resolution

- all domain controllers eventually have to converge to the same value
- schema conflicts are resolved using the "last writer wins" principle

Sites and domains

- a combination of one or more IP subnets.
- optimizes replication traffic over slow WAN networks by helping clients to find domain controllers that are close to them.
- within a site, a domain controller postpones notification of recent changes for a configurable interval at a default value of 10 minutes
- if a workstation is moved to a different location, the old domain controller provides the new site information to the client automatically
- **metadata** is built from two containers: the **configuration** container and the **schema** container
- domain deletion merely removes a domain from a tree
- removing parent domains breaks the trust relationships between the parent of the domain to be removed and the child domain of the domain to be removed

Forest

- allows sub-trees to retain common schema and common global catalog
- transitive Kerberos trust relationship allows users to access resources from all over the domain tree
- each domain requires only one trust to their parent domain

Global catalog servers

- special domain controllers that hold a complete replica of their own domain databases and a partial replica of all objects in the domain tree
- act as a repository similar to a global address book
- can be used for tree-wide searches
- never return referrals but the fully qualified name of an object
- uses **GUID** to locate object and construct distinguished name using the object's new relative ID (RID) and the LDAP path
- search operations usually return the results in flat lists or record sets, similar to how LDAP queries work

NTLM Authentication

- an authentication protocol that is the default protocol for network authentication in NT
- retained in Windows 2000 for backward compatibility
- pre-Windows 2000 clients in a mixed-mode domain can access pre-Windows 2000 server in a native-mode domain (or in different domains of different trees) through transitive trusts using NTLM
- resources are accessible across the forest through a transitive trust as long as the domain controller that receives the logon request from the server is running Windows 2000

Kerberos Authentication

- default network authentication protocol for computers running Windows 2000
- can operate across domain boundaries
- ticket-based - users are issued **Ticket Granting Tickets (TGTs)** by the **Key Distribution Center (KDC)** on a Windows 2000 domain controller during initial logon to the domain. TGTs contain authentication information about the user and are encrypted with a key known by the KDC
- after the user is granted a TGT the first time, subsequent checks are quick and efficient
- services use tickets that are similar to TGTs, but are encrypted using a key shared between the server and the domain controller

LAN Manager Replication Service

- uses the concept of import and export directories in NT 4.0 network
- ordinary member servers can host import and export directories
- not supported in mixed or native mode by W2K

File Replication Service (FRS) Process

- used by Windows 2000 Server to replace the LAN Manager Replication Service in NT 4.0
- automatically configured so that every domain controller has a replicated System Volume called **SYSVOL**
- any change to logon script stored in the SYSVOL of any domain controller is replicated in multiple-master fashion to other domain controllers
- only domain controllers can participate
- to provide support for LAN Manager replication, you need to create a bridge between LAN Manager Replication Service and FRS by selecting a Windows 2000 domain controller to copy the files that will be replicated to the Windows NT export directory using a regularly scheduled script called **L-bridge.cmd** (sample version is included on the *Windows 2000 Resource Kit* compact disc)
- to keep LAN Manager Replication Service available during upgrade, you need to make sure the server hosting export directory is upgraded only after all the other servers hosting import directories have been upgraded

NetBIOS in Windows 2000

- a high-level network-programming interface that has been used in pre-Windows 2000 networking components
- in Windows 2000, support for the NetBIOS naming interface is required only for cluster servers
- you can discontinue the use of NetBIOS and WINS after upgrade if there are no clients (such as Windows for Workgroups, Windows 95, Windows 98, or Windows NT) and no servers running Windows NT that use NetBIOS, or if you are sure your Windows 2000 network is pure enough that all computers and applications can use another naming service such as DNS

DNS Naming

- DNS Server record requirements:
 - must support service locator record type SRV defined in RFC 2052
 - SRV record points to a domain controller
 - format of an SRV record is Service.Proto.Name TTL Class SRV Priority Weight Port Target
- Windows NT 3.x and 4.0 environments use NetBIOS names for both machine and domain names, while Windows 2000 must use DNS names
- standard DNS characters are the letters A-Z, numbers 0-9, and the dash (-), **all case insensitive**
- the best way is to create NetBIOS names that are compatible with standard DNS names

- Windows 2000 DNS supports Unicode Character Support based on UTF-8 encoding, which allows complete use of non-ASCII character sets.
- host names of computers do not have to be related to the Directory DNS name
- standard RFC host names should be used if DNS interoperability is important

WINS will coexist with DNS until all computers are migrated to Windows 2000.

DNS Deployment

Deploying DNS in an NO DNS Environment

- easy approach: place a host in a Dynamic DNS zone that corresponds to each Windows NT domain. i.e. create new DNS zone to match the Windows NT domain, and enable Active Directory DNS integration so that all DNS data is safely stored and replicated in the Active Directory
- any domain controller can act as a fully functional DNS server with read/write access
- although not required, each location that has a domain controller should have a DNS server
- when each subdomain is in the same DNS zone, only a single DNS database is used

Deploying DNS in a DNSed Environment

- recommended approach: complex environments where client domains do not correspond to Windows NT domains can operate using standard DNS zone transfer mechanisms without the need for a major redesign. New DNS zones can be created to contain the Dynamic DNS data for the new Windows 2000 domains, which makes updates automatic
- in a large and highly decentralized company, more zones are effective, as local DNS information is available for those closest to the region that requires the DNS name most often
- in a smaller centralized company, fewer zones are better as less replication traffic is needed
- a large centralized company with a large zone structure requires DNS zone transfer over a much larger area, which increases traffic
- WINS is included in Windows 2000 for backward compatibility. The DNS/WINS integration feature provided in Windows NT 4.0 can be used to map the WINS NetBIOS namespace into DNS

W2K Groups

W2K Group Properties

Group	Membership from	Scope	Work in Mixed Mode	Nesting
Local	Same forest Other trusted forests Trusted pre-Win 2000 domains	Computer-wide	Yes	can contain global groups and user accounts from trusted domains
Domain Local	Same forest Other trusted forests Trusted pre-Win 2000 domains	Local domain	No	can contain user accounts, computer accounts, universal groups, and global groups from any domain. Can also contain other domain local groups from within the same domain
Global	Local domain	Any trusted domain	Yes	can contain user accounts and computer accounts from the same domain, and global groups from the same domain
Universal	Same forest	Any trusted native mode domain	No	can contain user accounts, computer accounts, universal groups, and global groups from any domain

- group memberships are stored in a single multi-value attribute
- a change to the membership requires the whole membership list to be replicated between domain controllers, and updated within a single transaction
- recommended practice: **limit group size to 5,000 members**
- nesting groups increases the effective number of members and reduces traffic caused by replication of group membership changes
- when a user logs on to a client or makes a network connection to a server, the group membership of the user is expanded as part of building the user access token

- effects of upgrade on groups:
 - upgrading a PDC to Windows 2000 has no immediate effect. Windows NT local groups become Windows 2000 local groups, and Windows NT global groups become Windows 2000 global groups.
 - when switching the domain to native mode, local groups on the PDC become domain local groups

Domain Tree Modeling & Migration

Definition and overall steps of migration planning

- migration involves upgrade, while restructure is a complete structure redesign
- **domain upgrade** is the process of upgrading the PDC and the BDCs in a Windows NT domain from Windows NT Server to Windows 2000 Server. This is the easiest and lowest risk migration route as it retains most of your system settings, preferences, and program installations
- you do not have to upgrade all servers in a domain to take advantage of Windows 2000 features, as mixed mode allows W2K and non W2k platforms to run in the same network
- when planning an upgrade, you need to determine which upgrade paths are supported, examine the existing domain structure, develop a recovery plan, determine the order for upgrading domains and domain controllers, and finally, if you should switch to native mode
- possible upgrade paths for your existing OS:

Existing OS	Upgrade to W2K Professional	Upgrade to W2K Server
Windows 3.x	No	No
Windows NT 3.1	No	No
Windows NT Workstation 3.51	Yes	No
Windows NT Server 3.51	No	Yes
Windows 95 and Windows 98	Yes	No
Windows NT Workstation 4.0	Yes	No
Windows NT Server 4.0	No	Yes

Goals and Constraints

- domain migration phases:
 - design the forest
 - migrate Windows NT domains to Windows 2000 native domains
 - plan the domain restructuring
- migration-related goals are not driven by technical features of Windows 2000 Server, but are concerned with the migration process itself
- your migration goal determines what path you should take. In most cases, business-related goals such as greater scalability and administration flexibility drive the initial migration decision
- factors to consider before migration:
 - application compatibility with W2K platforms
 - interoperability with Windows legacy systems and non-Microsoft operating systems
 - disk space requirements for Active Directory Objects. For example, **User** object consumes 3.6K bytes each, **Organizational unit (OU)** object consumes 1.1K, **Public key certificate** consumes 1.7K...etc
 - physical security of PDC and BDC is very important
 - security of BDC is often ignored. If you cannot upgrade the security of your BDC appropriately, demote the BDC to a member server during upgrade, or reconsider the proposed domain structure
- you must complete the design of the forest before planning the upgrade

Different Scenarios

- for remote sites under the same domain, replication takes place across slow WAN links, which is costly and resource intensive
- for remote sites under different domains, there is no replication traffic except for the tree metadata, which is replicated to all DSAs regardless of their domain membership. Result: fast, but prevents users from easily querying objects that belong to other domains
- for remote sites with all domain controllers of all domains being placed in every site location, client queries are always fast local operations, and administration has great flexibility as well, at the expense of high set up cost and high replication traffic across all sites
- for one domain per site plus global catalog servers, if a new object is created in one site, a partial replica of the object is transferred to all sites. If clients search for specific data, they can query the entire directory to locate the fully qualified name. If a client application requires properties of an object that is not included in the global catalog's database, fully qualified name can be used to learn the object's domain name and contact a domain controller in that domain. This setup is effective for reducing network traffic, and is ideal when all objects need to be accessible to all clients in all domains

Centralized structure

- simplified administration
- easier to design
- organizational units' features--such as delegation of administration rights--reduces the number of domains without sacrificing administrative flexibility
- fewer domains and a greater use of Ous

Decentralized structure

- distributed and scalable management architecture
- likely to transform their Windows NT 4.0 resource domains into full-featured domains and move user accounts from the former master domains to the domains where they really belong
- has more domains in the forest that enable local control

Migrate from Single Domain Model

- when migrated, usually results in a single domain in the Active Directory. delegation of administrative rights through the use of OU hierarchy

Migrate from Master Domain Model

- migration typically happens in a top-down manner
- master domain is the first domain to be migrated and the resource domains are migrated later
- centralized approach: migrate from several domains to a single domain and dissolve resource domains into OUs
- decentralized approach: retain the resource domains and move the user accounts to domains where they really belong

Migrate from Multiple Master Domain Model

- single domain tree approach:
 - individual business units implemented as different domains on the next lower level of the tree
 - root domain offers global resources that need to be available for everyone
- multiple domain trees approach:
 - one domain tree for each master domain and its resource domains
 - domain trees are joined into one forest
 - business units implement their own subtrees using their own structure and security policy
 - all administration happens on the tree level
 - suitable for companies that treat business units independently

Migrate from Complete Trust Model

- either build one domain tree and dissolve all domains into Ous, or fully retain the decentralized structure and build a forest that consists of several trees
- the most extreme model is to migrate to separate forests, with 4.0-style trust relationships being established between selected domains to allow users from other domains some access to some domains in another forest

Order of Upgrades

- within a domain, **upgrade the PDC first**. You can upgrade servers and clients at any time
- if you use LAN Manager Replication Service in the domain with the PDC hosting the export directory, change the export directory host before upgrading the PDC
- within groups of domains, it is better to upgrade your account domains prior to upgrading the resource domains
- to fully utilize W2K functions such as better directory scalability, universal and domain local groups, and group nesting, switch the domain to native mode once all of the domain controllers have been upgraded
- **Routing and Remote Access RRAS Server:**
 - RRAS service runs as LocalSystem with NULL credentials
 - by default, Active Directory does not accept querying of object attributes through NULL sessions
 - in a mixed environment, a Windows NT RRAS server is able to retrieve user RRAS properties only if:
 - the domain is in mixed mode and the Windows NT RRAS server is also a BDC, so that RRAS has local access to the SAM
 - the domain is in mixed mode and the Windows NT RRAS server contacts a Windows NT BDC, which results in behavior identical to current Windows NT behavior
 - the domain is in mixed or native mode and Active Directory security has been relaxed to grant the built-in user "Everyone" permissions to read any property on any user object. This is not suggested due to potential conflicts with your security requirements
 - recommended practice: upgrade RRAS server early in the process of upgrading member servers

Recovery / Fall back to NT 4.0

- a recovery plan is needed to prevent accidental data loss during upgrade. You should have this plan ready **before** performing the upgrade
- suggested practices:
 - add a BDC to any Windows NT domain that contains only a single domain controller. If the PDC fails, you still have a backup
 - fully synchronize all BDCs with the PDC, and take one BDC offline before you upgrade the PDC and the other BDCs to Windows 2000 Server.
 - backup services such as file and print services or Dynamic Host Configuration Protocol (DHCP) to tape and make sure the backup tapes are working
 - track all changes to the domain such as new accounts and password updates. If things go wrong with the Windows 2000 domain controllers, it will be necessary to roll back based on the tracked information. In any case, re-created accounts have a different security identifier (SID) which may prevent some users from accessing certain resources
- the obvious benefit of mixed mode is that it allows new BDCs to be added to the domain if a problem arises, thus providing opportunity for fallback. After the new BDC has joined the domain, you can resynchronize the account database. As long as there are no other Windows 2000 domains, you are able to promote the BDC to a PDC

Changes occurred in the Access Control Components

Security Identifiers

- contain parts that identify the revision number, the authority that assigned the SID, the domain, and a variable number of sub-authority or **Relative Identifier (RID)** values that identify the security principal relative to the issuing authority uniquely
- security principals cannot be moved between domains without their SIDs changing if, during upgrade, SIDs identifying the security principals remain unchanged. i.e. resource access is unaffected by upgrade

Access Tokens

- form of user ID used by the system to determine whether the user needs to be granted access to system resources
- every process the user creates carries the user access token

Security Descriptor

- attached to resources such as files or printers
- contains **access control list (ACL)**
- system performs access check verification by comparing the SIDs in user's access token against the SIDs in the ACL

Steps for performing the migration and dissolving resource domains into OUs

1. Migrate the Master Domain

- migrate the master domain to Windows 2000
- install Active Directory on a PDC
- trust relationships to the resource domains remain unchanged at this stage

2. Create Organizational Units

- create the organization before moving resources
- use OUs to create a hierarchical namespace, and to create users and groups
- downlevel clients aren't aware of the existence of the organizational units yet
- resource domains do not notice any changes in the master domain yet

3. Migrate PDCs in the Resource Domains

- upgrade the PDCs in the second-tier domains to Windows 2000 and the Active Directory
- this step is mandatory if you plan to move either servers or security principals from the second-tier domains to the master domain
- Active Directory provides SID tracking mechanism which allows the right domain controller to be found even when the SID has been changed

4. Move Servers to the Master Domain

- the administration user interface provides a drag-and-drop tool that makes it very easy to move resources from the resource domains to organizational units in the master domain
- clients who use UNC names to connect to servers will continue to function correctly as UNC names are not aware of the domain membership of a server. Administrator can use both NetBIOS and Active Directory publishing to advertise the existence of a resource
- if downlevel clients still exist without the new directory access client software, NetBIOS advertisement should be used in addition to publishing the resources in the Active Directory
- this is not the right time to remove PDCs from second-tier domains yet

5. Check Access Control Lists

- you need the information about the organization of access rights on shared resources in order to migrate smoothly
- you do not need to make changes to the ACLs if:
 - global groups from the master domain were used
 - local groups on member servers were used
- you need to make changes to the ACLs if:
 - local domain groups in the resource domains were used, and the domain controllers are eventually disappearing. In this case, you will need to move the local domain groups to the master domain

6. Move Workstations to the Master Domain

- for Windows 95 and Windows 98-based workstations, change the workgroup name in the network configuration section and install a service pack
- for Windows NT Workstation, remove from the old domain and add to the new domain. Windows NT 4.0 workstations must be upgraded to Windows 2000; if you use an automated setup script for the update, the domain change can be performed automatically

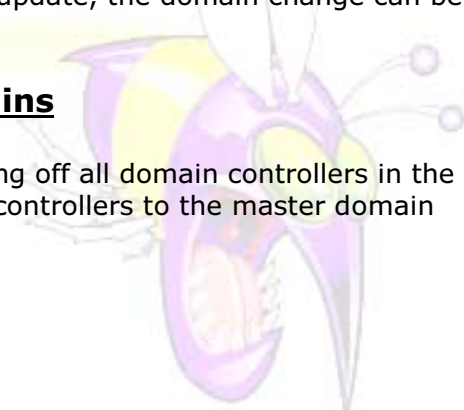
7. Turn off PDCs in Second-Tier Domains

- eliminate the second-tier domains by turning off all domain controllers in the second-tier domains, or move the domain controllers to the master domain

Windows 2000 Domain Modes

Mixed Mode

- a domain is in mixed mode if the PDC has been upgraded but not all BDCs have been upgraded, or the PDC and all BDCs have all been upgraded but the native mode switch has not been enabled



Native mode

- the final operational state of a Windows 2000 domain
- offers the full range of Windows 2000 features
- enabled by first upgrading all domain controllers to Windows 2000, and then setting a switch on the user interface
- during the switch to native mode, the following occurs:
 - Netlogon synchronization is off, and you can not add BDCs into the domain
 - domain uses only Active Directory multiple-master replication between domain controllers, thus the former PDC is no longer the master of the domain, and all domain controllers can now perform directory updates (although Windows 2000 still designates the role of PDC emulator to the former PDC, which means that (in native mode) password changes are replicated to the former PDC preferentially by other domain controllers)
- PDC Emulator - all pre-Windows 2000 clients use the PDC emulator to locate the PDC and perform password changes. Also, Windows NT resource domains use the PDC location information to establish trusts
- **the switch to Native mode cannot be undone**

Domain Restructure

Goals

- restructure is a complete structure redesign
- may provide Greater Scalability
- may allow further Delegation of Administration
- may provide Finer Granularity of Administration

Timing

- upgrade first and restructure later if you can solve your migration requirements by doing a two-phase migration (migrate and then restructure)
- restructure first if you want to redesign your directory services infrastructure to take advantage of the enhanced capabilities of Active Directory. This will impact your production environment, however
- recommended practice – restructure after upgrade, but before using features such as application deployment or the new group policy



Tools

ClonePrincipal

- allows incremental migration of users to a Windows 2000 environment without impacting your existing Windows NT production environment by creating clones of the Windows NT users and groups in the Windows 2000 environment
- consists of the COM object DSUtils.ClonePrincipal that supports three methods:
 - **AddSidHistory** - copies the SID of a source principal to the SIDhistory of an existing destination principal. It requires you to provide Domain Administrator credentials in the source and destination domains. Its events can be audited to ensure that both source and destination domain administrators can detect when this function has been run. Note that ClonePrincipal sample scripts call the underlying AddSidHistory method; therefore the other ClonePrincipal utilities are subject to the same security sensitivity and constraints as AddSidHistory
 - **CopyDownlevelUserProperties** - copies the Windows NT properties of the source principal to the destination principal
 - **Connect** - establishes authenticated connections to the source and destination domain controllers

Netdom

- allows you to manage Windows 2000 domains and trust relationships from the command line to join a Windows 2000 computer to a Windows NT or Windows 2000 domain, with options to specify the OU for the computer account; generate a random computer password for the initial join; manage computer accounts for domain member clients and member servers; specify the OU for the computer account; and move existing computer account for a member client from one domain to another, while maintaining the security descriptor on the computer account
- in addition, you can establish and manipulate trust relationships between domains

Migrating Users Incrementally to Windows 2000 – the steps

- migrate users incrementally to a pristine Windows 2000 environment without impacting the Windows NT production environment, thus protecting the current production environment from migration changes and allowing you to revert back to the old production environment if the need arises
- to decommission the old account domain and reassign the domain controllers, you perform the following steps:
 - create the pristine Windows 2000 forest that reflects the requirements and structure identified in the namespace planning activities of the organization. Domains in the new forest will be native mode Windows 2000 domains
 - use Netdom to query what trusts currently exist from any resource domains to the Windows NT source domain, compare the output from Netdom with the list of trusts that are required to allow resource access to users and groups in the target domain, and finally use Netdom to establish any trusts that do not already exist in order to maintain resource access
 - clone all source global groups in the target domain using ClonePrincipal
 - identify and clone sets of users
 - decommission the source domain after all users and groups have been moved permanently to the destination forest by powering off the source domain BDCs, and then the source domain PDC. However, store the PDC for disaster recovery purposes

Consolidating a Resource Domain into an OU – the steps

- consolidate a resource domain into an OU within a native mode Windows 2000 domain to reduce the costs of administering complex trusts:
 - establish any trusts required from the target domain to account domains outside the forest using Netdom
 - clone all shared local groups using ClonePrincipal
 - demote application servers to member servers after you have cloned all of the shared local groups
 - upgrade the PDC of the resource domain to Windows 2000 and run the domain in mixed mode during the transition period, then upgrade each BDC to be demoted using Active Directory Installation Wizard
 - move member servers (including former BDCs) and clients
 - decommission the source domain after you have permanently moved all groups and computers to the destination forest by powering off and removing the source domain BDCs, and then the source domain PDC

Special Thanks to Michael Yu for contributing material for this Cramsession. Make sure to visit his site at:
<http://michaelyu.freeservers.com/>

BrainBuzz Cramsession



brainbuzz.com



Notice: While every precaution has been taken in the preparation of this material, neither the author nor BrainBuzz.com assumes any liability in the event of loss or damage directly or indirectly caused by any inaccuracies or incompleteness of the material contained in this document. The information in this document is provided and distributed "as-is", without any expressed or implied warranty. Your use of the information in this document is solely at your own risk, and Brainbuzz.com cannot be held liable for any damages incurred through the use of this material. The use of product names in this work is for information purposes only, and does not constitute an endorsement by, or affiliation with BrainBuzz.com. Product names used in this work may be registered trademarks of their manufacturers. This document is protected under US and international copyright laws and is intended for individual, personal use only. For more details, [visit our legal page](#).