ABSTRACT

Microsoft Windows 2000 represents a major change in desktop and network operating systems. This latest Windows operating system includes many new features and technologies that will potentially benefit users and Information Technology (IT) managers on the Boulder campus. However, along with the increased functionality comes an increase in complexity. Windows 2000 must be integrated into our existing IT infrastructure to manage and support its method of directory service, security and authentication, and resource sharing.

Information Technology Services’ (ITS) goal is to gain an in-depth understanding of the Windows 2000 technologies and design a framework for its deployment. This includes the design, implementation and management of the Active Directory and the Kerberos 5 realm. It will also include modifying the existing Domain Naming System (DNS) to handle the specific requirements of Windows 2000. We will document this information and make it available to users on our campus. We will also maintain a test environment where interested network administrators can carry out their own testing and gain experience with the new operating environment. This paper will describe our proposed solutions and the rationale for them.

KEYWORDS

Windows 2000, Kerberos, DNS, Active Directory

1. BACKGROUND

The University of Colorado at Boulder (UCB) is a school of about 28,000 students and about 5,000 faculty and staff. Central IT resources are based primarily on Unix platforms including e-mail, DNS, Dynamic Host Configuration Protocol (DHCP) and Kerberos. UCB does not have a central Windows NT infrastructure, but many departments have well-established Windows NT domains and resources.

UCB began working with Windows 2000 by becoming a participant in the Microsoft Rapid Deployment Program (RDP) in February 1999. This project represented a large commitment of resources by both UCB and Microsoft. From February 1999 to the summer of 2000, Microsoft worked with UCB to envision goals, establish a plan, and overcome technical hurdles for an initial deployment of Windows 2000 in the fall of 2000.

During the course of this project, several major technical hurdles were encountered. The three greatest technical challenges were in the areas of Active Directory (AD) design, Kerberos interoperability, and BIND DNS interoperability.

2. ACTIVE DIRECTORY DESIGN

One of the greatest challenges of working with any product designed for use in a corporate environment is adapting it to the needs and realities of a campus environment. This was particularly true of designing an AD for UCB. The design issues centered around the logical design, user management, delegation of authority, and Group Policy Objects (GPOs).

2.1 Logical AD Design

The first stage in designing our AD was to establish the DNS location of the root domain. This is key to an AD design as it impacts the location of the Windows 2000 Kerberos realm and the DNS names of all computer objects within the domain. Because of our existing Kerberos infrastructure, we could not place the root domain at colorado.edu, so we began considering our options for a domain rooted in a DNS subdomain of colorado.edu. This was also a wise choice because of the possibility that our first implementation of an AD on campus could fail and we might have
to create a parallel replacement. Such a task becomes difficult if the root domain is located at the highest possible level in DNS. After some debate, we elected to use ad.colorado.edu as the location of our root domain. This was chosen because it is descriptive, short, and does not have a product affiliation.

The next hurdle in design was choosing a domain structure that best fit the campus and our needs. To keep management of the AD as simple as possible, we chose to use a single domain model and handle other organizational needs through the use of organizational units (see Figure 1). This allows departments most of the benefits of an AD without the additional management requirements of individual domains.

2.2 User Management

Once the basic AD design was completed, we focused on users. Because we plan on deploying Windows 2000 in our public labs and leveraging some of the benefits of user-level access control, we decided our domain would include user objects for all of our campus users (approx. 35,000).

The most critical decision we made during our design process was the use of a single people-space for user objects. The need for a single people-space (a single container to place all user object into) arises from the great deal of overlap in a campus environment. Unlike most corporations, higher education institutions must handle users with multiple affiliations. There are faculty with multiple appointments, students with multiple majors, and staff who are also students. This environment does not allow for users to be placed into the organizational units of individual departments.
Most user and access management can be accomplished in a single people-space environment using group membership and GPOs. Unfortunately, Windows 2000 currently has a membership limit of 5,000 on security groups. This will change in the next version, expected out in 2001. This means that any groups with more than 5,000 members will initially be handled using nested groups.

2.3 Delegation of Authority

The next phase of design came in matching the AD structure to the structure of the campus. While much time was spent discussing various political models, we found the best solution in organizing the AD was to emulate the organization of IT management on campus. Unfortunately, many of the schools, colleges, and departments on the UCB campus lack centralized IT management and infrastructure. To simplify the AD creation and management, we decided to create Organizational Units (OUs) for groups at the highest level of organized IT management. For some units this means at the college level, and for others it means at the department level.

Once an OU is created, authority for that OU will be delegated to a security group containing the IT administrators for that unit. These administrators will have the ability to create child OUs, security and distribution groups, computer objects, printer objects, and GPOs. They will not have the rights to create user objects as all users objects will be centrally created and managed. This allows administrators a great deal of flexibility while offsetting the responsibilities of user administration.

2.4 Group Policy Objects

One of the most important management and control features of Windows 2000 is the use of Group Policy Objects. GPOs can be used to control a number of settings based on either the computer or user object. Due to its hierarchical nature, this key tool is complicated by the use of a single people-space. Generally, GPOs are applied from one point down, in the tree-like structure of the AD. When user objects do not exist further down the AD, the user-based portion of the policy is not applied. There is, however, a special-case option in GPOs called “loopback processing mode” that allows the system to traverse the AD to locate the appropriate user object and apply policy based on both the computer and user objects. UCB plans to heavily utilize this function to allow for user-based GPOs in a single people-space environment.

2.5 Naming Conventions

At UCB, each department has a standard four-letter abbreviation (eg. HUMN for Humanities). As each OU is created, it will be named based on this abbreviation and the department will be encouraged to name child OUs in a similar manner, if applicable.

Certain objects in the AD, particularly GPOs and groups, require unique names across a domain. Because UCB will be using a single-domain design, all groups and GPOs must have unique names. For this reason, we have established naming conventions based on the origin of the object and its purpose. These objects are named in the following manner: OU_name-sub_OU_name-brief_description. For example, if the Sociology department creates a GPO for faculty computers, for use in an OU called “Faculty”, it may be named: SOCY-Faculty-Faculty_desktops. This convention allows for quick identification of objects, as well as ease of searches.

2.6 AD Physical Design

Our team decided on a single site design for the UCB campus because of the quality of network connectivity available to all departments. All network connections at UCB have at least 10Mbps of bandwidth with a well-designed backbone. Our team discussed replication traffic with the campus network engineers and it was not viewed as having a significant impact on campus networking.

3. MIT KERBEROS 5
INTEROPERABILITY AND ACCOUNT SYNCHRONIZATION

UCB has an existing MIT Kerberos 5 infrastructure used to authenticate dial-up connections, authenticate users for use of public labs, and perform Unix administration. The existing realm has about 35,000 principals and is maintained by the Central and Unix Services group within ITS.

The interoperability of this existing Kerberos infrastructure with Windows 2000 is considered a critical element of the campus deployment of Windows 2000.

3.1 Initial Kerberos Interoperability Thoughts

A number of Kerberos interoperability scenarios were considered and tested during this project, including an early Microsoft model, a Windows 2000 Key Distribution Center (KDC) as the primary KDC for our campus, a third-party (CyberSafe) product, and a dual-realm model. Early attempts at interoperability were based on a Microsoft white paper about the topic written from experience with Windows 2000 beta 3. This method, however,
required the registration of every workstation with the MIT K5 KDC and was not considered practical.

Using a Windows 2000 KDC as the primary authentication point for the campus did not prove to be feasible. There were a number of questions regarding support for existing Kerberos-based applications and user management.

UCB worked with CyberSafe to investigate the possibility of using their ActiveTRUST product for Kerberos interoperability. The product replaces the existing MIT KDC with an ActiveTRUST server and allows for both account and password synchronization between the ActiveTRUST server and a Windows 2000 domain. There were a number of questions regarding the release date of the product, Macintosh support, Unix support, and the corporate focus of the product. This resulted in a decision not to use the ActiveTRUST product.

3.2 The Dual-realm Model

The final Kerberos interoperability plan for UCB employs a MIT/Microsoft dual-realm model. This allows for full compatibility with all existing Kerberos applications because the existing MIT realm is maintained. This plan uses an alternative security name mapping for each user object in the AD that maps to the user’s principal in the MIT K5 realm. When coupled with a one-way trust between the Windows 2000 realm and the MIT realm, and a hot-fix from Microsoft, it allows for logins to the AD from a Windows 2000 client to be authenticated by the MIT realm (see Figure 2). This opens up the potential for single-sign-on access to both Windows 2000 and Unix resources from a Windows 2000 client.

**3.3 NT LAN Manager (NTLM) Authentication**

The greatest drawback to the dual-realm model is the lack of password synchronization. Because our MIT Kerberos passwords are stored in a one-way hash, they cannot be extracted for synchronization. The Windows 2000 passwords will be randomly generated when the user objects are created. This creates a Windows 2000 environment that does not support NTLM authentication at the domain level, thus it does not support downlevel (Windows 95, 98, NT 4) or cross-platform (Mac OS, Unix) authentication to domain level Windows 2000 resources. This configuration does not exclusively prohibit NTLM authentication however, as local administrators retain the ability to maintain their own user-directory database on individual member servers. Thus, NTLM and its corresponding downlevel/cross-platform client interoperability can be enabled and used against local accounts at the discretion of local administrators.

The downlevel support is not considered critical at the domain level as Windows users will be expected to upgrade to Windows 2000 to join the domain. The cross-platform support, particularly the Mac OS support, is critically important to some campus units. With the release of Mac OS X, Kerberos 5 libraries will be included in the operating system. However, the required Application Program Interfaces (APIs) to perform a Kerberos authentication to a Windows 2000 realm to access Windows 2000 resources will not initially be available. It is expected these will be produced in the relatively near future.

3.4 Account Synchronization

For the dual-realm model to work properly, the user objects in the AD must be synchronized to the principals on the MIT KDC. This involves a process of obtaining a list of all current principals for an initial synchronization and then obtaining periodic add and delete requests. This information is then processed by an application written at UCB which creates and deletes users as needed. To enhance the usefulness of the AD, we are also using this application to query our existing Lightweight Directory Access Protocol (LDAP) accessible directory for additional information to populate user object attributes (e.g. e-mail address, phone number, department, etc.). These attributes are populated when the user object is created and then periodically updated.

There is currently a project underway at UCB charged with creating a comprehensive enterprise directory. Once this project is complete, this directory will become the authoritative source of user account information for our AD. We are working closely...
with the project team to ensure the interoperability of our planned AD with their planned directory services.

4. BIND DNS INTEROPERABILITY

UCB is currently using an ISC BIND 8.2.2 DNS server to provide name service for the vast majority of the Boulder campus. There are only a handful of DNS subdomains on the UCB campus: cs.colorado.edu, resnet.colorado.edu, and the Windows 2000 test subdomains. The computer science department handles the naming service for the cs.colorado.edu subdomain. While BIND 8.2.2 supports dynamic DNS updates, UCB has not enabled this ability in its DNS servers.

4.1 The DNS Requirements of Windows 2000

The use of a Windows 2000 Active Directory requires a DNS server capable of supporting SRV resource records. SRV records are DNS resource records containing the location and description of a particular service (formatting of SRV records is defined by RFC 2052). A full list of the required SRV entries for a domain can be found in the netlogon.dns file located on each domain controller. Microsoft also strongly recommends the capability of dynamic updates. Both of these functions are supported by ISC BIND 8.2.2 when properly configured.

4.2 The Dangers of Non-secure Dynamic DNS (DDNS) in Higher Education

In a distributed, uncontrolled environment such as a higher education campus, non-secure DDNS poses a severe problem. No school wishes to allow any computer user on campus to bring up a web server with the address using any number of vulgar, sexually explicit, or derogatory terms. From this problem arises a desire for secure DNS updates, which is not currently possible between a Windows 2000 AD and BIND DNS servers.

4.3 DNS Scenarios Considered at UCB

Three primary DNS scenarios were considered for Windows 2000 deployment at UCB: a Windows 2000 DNS server, creating a BIND subdomain with DDNS enabled, and enabling the minimum DNS requirements for Windows 2000 on the existing BIND server.

Our team considered the options of using a Windows 2000 DNS server either for the entire campus or for the Windows 2000 subdomain. Using a Windows 2000 DNS server allows for secure updates and some degree of control of the updates. However, UCB has an existing BIND infrastructure that currently serves the campus DNS needs. Moving a critical service to a platform that is yet to be extensively proven in a campus environment was not considered wise. In addition, our DNS managers were not comfortable with the security and tools available in Windows 2000.

We also considered using a BIND subdomain with full dynamic updates enabled. While this scenario provided full DDNS for Windows 2000, it did not solve the problem of non-secure DNS updates.

Our final scenario was to keep our existing BIND DNS servers and enable support for and dynamic updates of SRV records in ad.colorado.edu. The domain controllers for the Windows 2000 domain would be allowed to update SRV and forward lookup

---

**Figure 3: Proposed UCB BIND DNS Interoperability Plan**
records for ad.colorado.edu, but not the reverse lookup records for 128.138 (see Figure 3). Only the domain controllers would be authorized to make dynamic updates. This scenario provides the minimum DNS requirements of Windows 2000 while not allowing for non-secure DDNS updates. This scenario does have a large drawback due to the dependence of Windows 2000 on DNS names to located computers and services: it forces UCB to use static IP addressing for the Windows 2000 domain.

### 4.4 Using Static Addressing During DHCP

Trends

The UCB campus currently is divided between static IP addressing and the use of DHCP services for dynamic addressing, but there is a general trend toward the use of DHCP campus-wide. UCB plans on establishing a web-based DHCP registration process and the eventual transition of all users to DHCP (where applicable).

The use of static addressing for Windows 2000 deployment will force departments to request appropriate name service for all computers to be included in that active directory. While static addressing has been present at UCB for quite some time, many departments have had little experience with requesting specific name service for their computers.

This static addressing will become more difficult as more departments join our AD, so it is only a temporary solution. As technologies become available to allow for secure, dynamic DNS updates, UCB will transition Windows 2000 clients to DHCP.

### 5. CONCLUSION

Deploying Windows 2000 in a higher education environment poses a number of technical challenges, especially in the area of interoperability with existing infrastructure components. This product, after all, was designed for a corporate environment with a Microsoft infrastructure. Any school looking to deploy should take time to evaluate their current infrastructure and identify critical services and infrastructure components that must interoperate with Windows 2000. To avoid disruption of existing services, a deployment team may be forced to limit the capabilities of Windows 2000. A deployment team should also consider their Windows 2000 interoperability plans to be tentative at best as new tools and updates continue to surface. At UCB we are keeping our eyes open for new options to allow the greatest level of functionality without sacrificing existing services.