DEPLOYMENT AND MIGRATION TO WINDOWS 2000 IN A HETEROGENEOUS UNIVERSITY SYSTEMS ENVIRONMENT

by
Gary W. Wilhelm

A Master's paper submitted to the faculty
of the School of Information and Library Science
of the University of North Carolina at Chapel Hill
in partial fulfillment of the requirements
for the degree of Master of Science in
Information Science.

Chapel Hill, North Carolina
April, 2001

Approved by:

_____

Advisor

Gary W. Wilhelm. Deployment and Migration to Windows 2000 in a Heterogeneous University Systems Environment. A Master's paper for the M.S. in I.S. degree. April, 2001. 55 pages. Advisor: Gregory B. Newby.

This study examines the complex undertakings of the migration of Microsoft's Windows 9x/NT 4.0-based computing systems to the Windows 2000 operating system environment at the University of North Carolina at Chapel Hill. Factors examined include the similar paths of migration taken by other universities, various methods by which an academic or administrative department may migrate, and the intricacies of creating the integrated centralized infrastructure which is necessary to fully utilize the complex distributed architecture of Windows 2000. An analysis of the current status of Windows 2000 on campus attempts to provide a recommendation both for departments which have not yet migrated and for future directions of Windows-based distributed computing for the University.

Headings:

Microsoft Corporation-Windows 2000

Distributed Computing

Distributed Computing-Resource Sharing

University of North Carolina at Chapel Hill-Academic Technology and Networks

ACKNOWLEDGMENTS

This research would not have been possible without the assistance of several information technology professionals at the University of North Carolina at Chapel Hill, namely Ernie Patterson of the Department of Biology, James Ervin of Academic Technology and Networks, Toby Considine of Facilities Service Division, Jason Li of the College of Arts and Sciences, Scott Adams of the School of Information and Library Science, Jesse Safir of Administrative Information Services, Dave Kleinberg of the Department of Physics and Astronomy, and David Parker of the School of Education.

CONTENTS

INTRODUCTION 1

INDEX OF MAJOR CONCEPTS WITH DESCRIPTIONS. 4

WINDOWS 2000 AND OTHER UNIVERSITIES 10

IMPLEMENTATION OF WINDOWS 2000 IN THE DEPARTMENT OF BIOLOGY AT UNC-CHAPEL HILL. 16

SUMMARY OF STEPS FOR UPGRADING A DOMAIN FROM WINDOWS NT TO WINDOWS 2000. 35

CAMPUS-WIDE WINDOWS 2000 IMPLEMENTATION 37

FINAL ANALYSIS AND CONCLUSIONS. 46

REFERENCES. 50

Introduction

As the early years of this century progress and more people become dependant on the various facets of computer networking in their everyday lives, the need to be able to share computer resources, such as data files and access to printers, will continue to increase. Traditional methods of resource sharing have ranged from such non-technological methods as carrying files back and forth on foot via floppy disks to more contemporary methods of e-mailing files to making information accessible via HTML pages on the World Wide Web.

There are, of course, inherent flaws to each of these methods, including inefficiency, inconvenience, and lack of security. Network computing has arrived at the point where one would like to be able to work with every available resource, be it a file or a printer or something else, as if it were a local resource–something sitting on his own desk. Along those same lines, one would like to be able to take his local resources and easily give others access to them. At the same time, however, one wants to limit that access so as not to reveal too much of what one has been working on or so one does not accidentally open up his personal computers to vulnerabilities.

One of the major ways such an ability can be achieved in today's networked computing world is by using what is commonly known as file and print sharing. This ability has been available since the early days of networking for many different operating system platforms, but has never been especially easy to use or very robust. With the

release of Microsoft's Windows 2000 family of operating systems in February 2000, however, the ability to share resources over both local area networks (LANs) and the Internet has been made easier than ever before.

Organizations that upgrade their individual users' workstations to Windows 2000 Professional and provide at least some basic network infrastructure via Windows 2000 Server and Advanced Server can give those users several useful tools. One such tool includes the ability to find other users and the resources they have made available in a more intuitive way through simply searching a server-based directory of files and printers that these other users have shared. Given the proper set of access permissions to a particular shared resource on someone else's computer, one could review a document, modify a spreadsheet, or print a file on a remote printer all without having to leave the office. Combined with the rapidly advancing technology in videoconferencing and other similar methods of communications, this ability to visually interact with others at work without ever having to leave one's own office (or home in the future) can revolutionize the way work is done.

This master's paper is designed to examine both the current and future impact of Windows 2000 on the campus of the University of North Carolina at Chapel Hill and to determine exactly how it can be used to make such resource sharing easier on a large and diverse campus. Since it is relatively trivial to implement Windows 2000 Professional workstations within an existing Windows 95, 98, and NT 4.0 computing environment, an examination of the implementation of the Windows 2000 Server and Advanced Server infrastructure is the primary focus of this paper. The possibilities for such an implementation and its ramifications are of far greater depth and potential complication

than the possibilities for implementing Windows NT 4.0 Server, which the Windows 2000 Server family is designed to upgrade.

This paper is organized into several sections. First, a short listing and definition of Windows 2000-specific terms will be provided. Some of these terms have been carried over by Microsoft from Windows NT 4.0, but others are new for Windows 2000. Second, I will examine the current progress the implementation of Windows 2000 at other universities in the United States, since that implementation should provide a good model for such an implementation at UNC. Next, I will discuss the initial implementation of Windows 2000 that I undertook in the Department of Biology at UNC, where I am a systems administrator. Then, I will provide the current campus-wide implementation status of Windows 2000 at UNC as provided by Academic Technology and Networks (ATN). Finally, I will provide some feedback from other departmental systems administrators as to how they feel the campus-wide implementation of Windows 2000 may benefit their departments. I will also develop some conclusions as to the future of Windows 2000 and its successors on campus and examine how Windows 2000 can be integrated into existing campus services to make networking and all its aspects easier for the end-user.

Index of Major Concepts With Descriptions

Networking Protocols

- DNS: Domain Name System. Internet protocol used usually to map static IP addresses to easier-to-remember names (e.g. www.bio.unc.edu = 152.2.67.1). Windows 2000 has its own version of dynamic DNS that is integral to communications in Active Directory.
- WINS: Windows Internet Naming Service. Microsoft Windows-specific protocol used in local area networks to easily name computers (e.g. Bioweb, Biodata). This protocol is slowly being phased out by Microsoft starting with Windows 2000 and continuing to later versions. A major disadvantage of WINS is that no two computers on a local area network may have the same name, even if they are in different domains. This extends to Windows 2000 as well (e.g. Windows DNS names of bob.bio.unc.edu and bob.math.unc.edu are not possible because the WINS name—Bob—is the same for both).
- DHCP and BOOTP: Dynamic Host Configuration Protocol and Bootstrap Protocol. Internet protocols used to automatically assign IP addresses to computers. DHCP is the most common; BOOTP is the older protocol that assigns IP addresses to computers as they are starting. The UNC campus uses a Unix-based DHCP server. Windows NT 4.0 and 2000 servers have a DHCP server which is really a BOOTP server: clients requesting IP addresses must have specific registrations in the DHCP server database based on their hardware address.

General Windows Networking Concepts

- Workstation: A typical user computer using either Windows 95, Windows 98, Windows Me, Windows NT 4.0 Workstation, or Windows 2000 Professional as its operating system. Macintoshes set up to use Thursby Corporation's DAVE product (which emulates a Windows 9x/Me computer in terms of file and print sharing) would fall into this category as well.
- Server: A computer using either Windows NT 4.0 Server, Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server as its operating system and is managed by a departmental administrator. Network printers and shared file folders are most commonly accessed from servers, even though they also may be shared from workstations.
- Windows NT 4.0: Microsoft's operating system family designed specifically for networks, released in 1996. There are two separate operating systems in this family: Workstation and Server.
- Windows 2000: Microsoft's operating system family designed for both networks and home use, released in 2000. There are four linked operating systems in this family, each of which build upon each other by adding more features from level to level. Workstations and home computers use Professional, while servers use Server, Advanced Server, or Datacenter Server.
- Workgroup: Group of computers on a local area network that may or may not be in close physical proximity to one another. These computers may share files and printers based on proper authentication, which is set at individual computers in

the workgroup. No server is required; the workgroup name is set to be the same for each individual computer in the workgroup.

- Domain: Group of computers on a local area network that may or may not be in close physical proximity to one another. A server must be in place for authentication to access shared files and printers. Individual user accounts are set up on this server, generally known as a *domain controller* (DC), and these user accounts are used when determining the proper permissions to access network resources. The domain name is set when the first DC is initially set up.
- Primary Domain Controller (PDC): In a pure Windows NT 4.0 domain, the server that has primary responsibility for user authentication and domain administration. Only one PDC may exist in a domain.
- Backup Domain Controller (BDC): In a pure Windows NT 4.0 or mixed Windows 2000 domain, any server that has secondary responsibility for user authentication and domain administration. Multiple BDCs may exist in a domain. A BDC in a pure Windows NT 4.0 domain may be manually promoted to become the PDC at any time and may be automatically promoted to become the PDC should the regular PDC become unavailable for any reason.
- Peer Domain Controllers: In a Windows 2000 domain, all Windows 2000-based domain controllers serve as peers to one another: all domain controllers have the same responsibility for user authentication and domain administration.
- Member Server: In either a Windows NT 4.0 or Windows 2000 domain, a server that is not a domain controller and thus cannot authenticate users or administer the

domain. Member servers are typically used for such tasks as Web services or multimedia video services to avoid using system resources on user authentication.

- Mixed-Mode vs. Native Mode: A mixed-mode Windows 2000 domain may have any number of Windows NT 4.0 backup domain controllers along with any number of Windows 2000 peer domain controllers. These BDCs may authenticate users but have secondary responsibility for domain administration. A native-mode Windows 2000 domain must have only Windows 2000 peer domain controllers and allows for a specific type of user group known as *universal groups* (not discussed in this paper).

Windows 2000-Specific Networking Concepts

- Active Directory (AD): As stated by Microsoft:

> "(A)n essential part of the Windows 2000 network architecture and are specifically designed for distributed networking environments. Using Active Directory and Microsoft Metadirectory Services (MMS), organizations can efficiently share and manage information about network resources and users."[1]

From Stanford University:

> "Active Directory is a new Windows term for the overall directory database in a Windows domain. The AD, or Active Directory, contains the user accounts, computer accounts, OUs, security groups, and group policy objects. The AD is markedly different from the NT4 domain database (called the SAM) because it is based on the LDAP standard. This means that everything in AD is an object with a unique path together with associated attributes. This allows a greater opportunity for interoperability with applications and other directory products. The tree or forest-wide schema determines what types of objects and attributes may be created in AD. Another implication of the new LDAP support is that information in the directory is searchable."[2]

[1] http://www.microsoft.com/windows2000/guide/server/features/directory.asp
[2] http://windows.stanford.edu/docs/basic.htm#ad

- Schema: In general directory services, the schema defines the objects and their attributes available for use in creating listings in the directory database. Microsoft's Active Directory contains a default schema that has many attributes about users, computers, etc., including name, location, etc. Many references about Active Directory and its schema are available both in print and on the World Wide Web.[3]
- Forests and Trees: A forest is a collection of trees, while a tree is a collection of domains and other trees. In Windows 2000, DNS is used to hierarchically identify forests, trees, domains, and computers. For example, a domain controller at the root of the unc.edu forest is known as sprucegoose.unc.edu, while a tree underneath unc.edu may be known as cas.unc.edu with a member, either another tree or a domain or a computer, known as *something*.cas.unc.edu. This can continue on for many hierarchical levels.
- Organizational Unit (OU): A group of computers within a Windows 2000 domain. No such grouping was possible in Windows NT 4.0. An OU may or may not have a separate administrator depending on how the larger organization decides to administer its Active Directory infrastructure.
- Transitive Trust Relationship: Automatically created between all trees and domains in a forest, it provides the ability for someone with a user account in one domain to share network resources with a user with an account in another domain. Trust relationships had to be manually created between Windows NT 4.0 domains

[3] http://mspress.microsoft.com/prod/books/sampchap/3173.htm

and still must be manually created between domains in separate Windows 2000 forests.

- FSMO Roles: Flexible Single Master Operations Roles: the five roles servers in a Windows 2000 forest can hold. Two of the roles only exist once on the forest level: Schema Master and Domain Naming Master. Three of the roles exist in each domain: Infrastructure Master, RID (Routing Information Daemon) Master, and PDC Emulator. (Major details of these roles are beyond the scope of this paper.)

Windows 2000 And Other Universities

Since much of Microsoft's documentation for a Windows 2000 migration is based upon a Windows 2000 implementation in a corporate environment, I felt that it would be useful to gain some insight into how other universities around the United States were planning on implementing Windows 2000 campus-wide. Many universities had Websites pertaining to a Windows 2000 implementation on small-scale level (such as Indiana University[4] and the University of California at Davis[5]). Only a few, however, had extensive documentation on how they were fully implementing Windows 2000 Server university-wide. Four Websites that I found most useful were from Cornell University, Stanford University, Arizona State University, and the University of Colorado at Boulder.

Cornell University

Many university Windows 2000 Websites that I explored had links to other university Windows 2000 Websites for reference purposes. Despite the fact that very few had links to Cornell University's[6] Windows 2000 site, I found that Cornell had perhaps the most extensive Windows 2000 implementation of any university I examined.

Two of the major Windows 2000 features Cornell has implemented extensively are dynamic DNS and Kerberos authentication. Dynamic DNS under Windows 2000 and Active Directory allows a system administrator to change the computer name of individual Windows 2000 Professional workstations and have those records automatically updated in close to real-time on an organization's DNS server. This is extremely advantageous in that WINS is a somewhat unreliable protocol in terms of

[4] http://windows2000.indiana.edu/
[5] http://win2k.ucdavis.edu/
[6] http://www.cit.cornell.edu/computer/system/win2000/

update times for computer names and that DNS is really the primary means of computer identification over the Internet. Unlike UNC-Chapel Hill, however, Cornell actually has very few separate DNS zones underneath the cornell.edu DNS domain, so the implementation of Windows 2000 DNS was much easier than at an institution that had many DNS subdomains.[7] Another interesting feature of Cornell's Windows 2000 DNS implementation was a Website[8] for system administrators to verify that dynamic updates actually took place rather than having to test the updates manually through an nslookup command (manual query to a DNS server via command-line).

The other major Windows 2000 feature implemented at Cornell was Kerberos version 5 authentication.[9] Kerberos is a very secure method of network authentication that was initially created for the Unix world. The current version of Kerberos authentication supported on the Unix platform at UNC-Chapel Hill is version 4, with a version 5 migration to take place eventually. One of the problems with Microsoft's version of Kerberos is a distinct difference between the Windows 2000 and Unix versions of Kerberos 5. An empty field in the Unix version of Kerberos 5 is filled with a user's SID (Security Identification) specific to the Microsoft version of Kerberos 5 (more on Kerberos with the discussion of Arizona State's implementation).

There was no mention in Cornell's documentation about such a conflict with Kerberos on their campus. Once a departmental domain controller was configured for dynamic DNS, it was not very difficult to create a Kerberos trust between that department and central computing services after that departmental domain was set up on the two central Kerberos authentication servers.

---

[7] http://www.cit.cornell.edu/computer/system/win2000/dns.html
[8] http://dnsdb.cit.cornell.edu/
[9] http://www.cit.cornell.edu/computer/system/win2000/kerberos.html

Stanford University

The university implementation of Windows 2000 that I examined which was perhaps most similar to that of a corporation was at Stanford University.[10] Stanford was another university that explicitly stated that Kerberos would be the primary method of authentication after the upgrade of the central university infrastructure to support Windows 2000. This upgrade was to have taken place in the first quarter of 2001.

Stanford's documentation[11] on the ramifications of Windows 2000 upgrades was probably the best of any university examined. The most interesting point was that departments wishing to move to Windows 2000 must join the central forest consisting of one tree and that no subdomains could be created. This implied that departmental administration would take place through Organizational Units rather than subdomains, but this was not explicitly stated. It was clearly stated, however, that departments which did not join their computers to the central forest would have major problems with getting DNS to function properly. Other interesting points were that the licensing enforcement features of Windows 2000 would be used very strictly and that authentication through Kerberos 5 would be centralized.

Arizona State University

Arizona State's[12] implementation of Windows 2000 was in harmony with what has been stated by Microsoft: that there is more than one way to set up everything. Unlike Cornell and Stanford, Arizona State's root domain followed Microsoft recommendations and was named ad.asu.edu (with ad standing for Active Directory) as

[10] http://www-nt.stanford.edu/Win2000/
[11] http://www-nt.stanford.edu/docs/joinquestions.html
[12] http://windows2000.asu.edu/

opposed to just asu.edu. There was no apparent reason for this decision in any of their online documentation.

Arizona State's Windows 2000 campus implementation Website[13] showed a plan for a single forest implementation, which was similar to the other universities. This plan was similar to Stanford's in that most servers and workstations would be joined by default to the forest root domain in a specific departmental Organizational Unit. However, Arizona State did allow for the creation of departmental subdomains if that department could provide around-the-clock support for any urgent problems created by that particular domain. Another interesting note was that Arizona State had no plans to migrate to a full Windows 2000 implementation of DNS; therefore, dynamic DNS would not be supported. This may be mainly due to the size of the university itself, since dynamic DNS updates are not going to be as secure or as easy to verify in a large university setting.

Arizona State's Kerberos implementation was also different. Arizona State planned to have two Kerberos realms, one for existing services and one for Windows 2000, with password synchronization between the two. However, the university was waiting until after Windows 2000 was fully implemented campus-wide to begin implementing Kerberos authentication for Windows 2000. Such a setup, however, could be a possibility for a mainly Unix-based server environment such as UNC-Chapel Hill.

University of Colorado at Boulder

The University of Colorado at Boulder's[14] Windows 2000 implementation was one of the earliest of any university, as it began with the university's involvement with

[13] http://www.west.asu.edu/itweb/win2000/
[14] http://www.colorado.edu/its/windows2000/

the Microsoft Rapid Deployment Program (RDP) in April 1999. Colorado's implementation was similar to Stanford's in that independent departmental Windows 2000 forests were not allowed on campus. It was also similar to Arizona State's in that the root domain was located at ad.colorado.edu and that dynamic DNS was not supported.

The most significant similarity between Colorado's Windows 2000 implementation and a possible UNC-Chapel Hill Windows 2000 implementation dealt with user accounts and Kerberos authentication. Colorado uses a universal username known as an IdentiKey that is similar to the UNC ONYEN (Only Name You'll Ever Need). With Colorado's Windows 2000 implementation, Windows user accounts were managed centrally and not at the department level, with user account names set to be identical to the IdentiKey. Individual users were not able to change their Windows 2000 passwords and had no need to, since authentication is through their IdentiKey via Kerberos.[15] More specifically:

> "The configuration used at UCB requires a small amount of configuration on each client workstation, a one-way Kerberos trust between the Windows 2000 domain and the existing Kerberos realm, and special configuration of the user objects in the Windows 2000 domain. This allows Windows 2000 users on campus to login to their computers using their IdentiKey accounts."[16]

General Conclusions

In summary, each of these universities had different methods of implementing Windows 2000 that were specific to their individual campuses to best fit their needs. Since each university did have different nuances in their individual implementations, I thought it best that I should try implementing Windows 2000 on servers in my own

[15] http://www.colorado.edu/its/windows2000/adminguide/userpassinfo.html
[16] http://www.colorado.edu/its/windows2000/adminguide/infrainter.html

department to see if I could at least partially determine how Windows 2000 could best be implemented in a department at UNC-Chapel Hill.

Implementation of Windows 2000 in the Department of Biology at UNC-Chapel Hill

Initial Steps: Learning more about Windows 2000

Before feeling prepared to fully implement Windows 2000 on a departmental level, I first had to understand more about the new features that the Windows 2000 Server Family actually possessed. My first method of Windows 2000 study was to take two Microsoft courses from Productivity Point International (PPI), one in May 2000 and one in July 2000. The July course, Microsoft course 2152 (Supporting Microsoft Windows 2000 Professional and Server) mainly served as a reinforcement for the things I had already taught myself about Windows 2000. It also helped me to learn about disk management and security features I did not already know. This weeklong course would be an excellent first course for a Windows NT 4.0 systems administrator who wanted to learn about the features of Windows 2000 Server before actually upgrading.

The May course, Microsoft course 1561 (Designing a Windows 2000 Directory Services Infrastructure) was specially offered for UNC systems administrators trying to find the best way to set up Windows 2000 and Active Directory at UNC. This course examined such things as to how to structure forests, trees, domains, and Organizational Units along with how to set up other required Windows 2000 elements (mainly DNS). Given the proper security and infrastructure, departments could join a central UNC campus Active Directory once they were ready to upgrade their domains with as little intervention from ATN as possible. One of the other major issues that was discussed in this course was how to design a UNC campus Active Directory schema that would contain as few object attributes as possible, but it still had to be useful to individuals

wanting to utilize a central campus directory for all the possible applications it might have in the coming years.

Testing Phase: Trying Out Windows 2000 in a Testing Environment

Taking courses and reading about a particular software package are always a good method of learning, but by far the best way to learn something as complicated as a new operating system works is to actually install it. Before upgrading the existing Biology Windows NT 4.0 domain to Windows 2000, I first needed to test out the various features of the Windows 2000 Server family. One of the good things that Microsoft did with Windows 2000 was to make it as easy to integrate with an existing Windows NT 4.0 domain as possible. A Windows 2000 server can easily be integrated into a Windows NT 4.0 domain as a member server without any configuration changes to that domain. Thus, my first task was to take our department's new server, **Bioweb** (so named because it was purchased with the idea that it would become the new departmental Web server), install Windows 2000 Server, and add it to the Biology domain as a member server.

Before proceeding, I will explain the various differences in the three versions of the Windows 2000 Server Family. Windows 2000 Server is designed for member servers in a domain and can support up to four processors and 4 GB of RAM. Windows 2000 Advanced Server is designed for domain controllers and can support up to eight processors and 8 GB of RAM. Windows 2000 Datacenter Server (which was released during the fall of 2000) is designed for extremely heavy processing (probably at the root of the Active Directory forest for a major corporation) and can support up to 32 processors and 64 GB of RAM. It is not possible to upgrade from one version of

Windows 2000 Server to another–a clean installation of the operating system has to be performed.

With Bioweb (which contains 2 Pentium III 550 MHz processors and has 256 MB of RAM), I formatted the hard drive and installed Windows 2000 Advanced Server as a member server in Biology. This process was no more difficult than installing Windows 2000 Professional on a new workstation. I also utilized one of the more advanced features of disk management. I upgraded Bioweb's two physical hard drives to dynamic disks (as opposed to basic disks) and then created a disk mirror on the unused second drive. Disk mirroring allows for the contents of the first physical hard drive to automatically be written to the second physical hard drive whenever those contents change. Therefore, if one of the drives fails for some reason, the data is still present on the second drive, which may then be reconfigured as the primary drive after the failed drive has been removed. Of course, the disadvantage of this is that only half of the total amount of disk space can be utilized at one particular time. Bioweb has two 30 GB drives–one that serves as the C: drive and another that is an exact duplicate of the C: drive and is invisible to users.

Setting up a member server such as Bioweb is not the main reason to install Windows 2000, however. To really take advantage of the operating system, one most configure a Windows 2000 server as a domain controller and thus utilize Active Directory. As mentioned at the beginning of this paper, unlike the older Windows NT 4.0 model of one PDC and multiple BDCs in a single domain, all domain controllers (DCs) in a native-mode Windows 2000 domain are peer DCs. However, a mixed-mode Windows 2000 domain can exist with one or more Windows 2000 DCs and multiple

Windows NT 4.0 BDCs. I will also mention in greater detail the hierarchy that exists in a Windows 2000 domain environment. In the Windows NT 4.0 environment all domains exist on the same level. Computers in different domains can only send data back and forth to one another if an explicit trust relationship is created (excluding methods such as FTP, etc.). An improvement that Microsoft has made in the Windows 2000 environment is the ability to create a hierarchy of domains in a tree structure anchored at a forest root from which various domain trees can begin. Each of these various domain trees and the domains within them automatically have transitive trust relationships created between them. All that it is needed for users in one domain to share resources with users in another domain is the proper security credentials for that remote domain.

For testing purposes, I joined the Bioweb server to the test forest crashnburn.unc.edu as a single DC for the new domain biodeath.crashnburn.unc.edu (a child domain tree of the test forest). This is accomplished either by going through the Configure Your Server wizard or by running the program DCPROMO from a command prompt. I decided to create the domain as a mixed-mode domain, as if I was actually in a real-world scenario and had some Windows NT 4.0 BDCs that had not yet been upgraded, since the conversion from mixed-mode to native-mode is irreversible. The final step of creating the basic domain was to install DNS on Bioweb. DNS is fairly easy to configure for child domains. I simply created a DNS Forward Lookup Zone to point back to the IP address of the server at the forest root (uncroot.crashnburn.unc.edu), which then performs DNS lookups for Windows 2000 computers in the forest or passes them on to the campus DNS servers in case it cannot find the appropriate entry.

The next step was to test Active Directory (AD) itself. In the beginning, the main point of AD on the UNC campus will probably be for the creation of a simpler and more hierarchical way to access various objects (computers, printers, shared folders, users) in a particular domain(s). With AD, objects in a domain can be classified into Organizational Units (OUs) to create a hierarchical structure. Therefore, for my test domain, I moved a test Windows 2000 Professional computer from the real Biology domain into biodeath.crashnburn.unc.edu, added a test user, and published a shared printer, all in one OU. This seemed to work without any problems.

The other major networking component that (almost) goes hand-in-hand with Windows 2000 DNS is DHCP. Even though DHCP is not officially required for Windows 2000 domains, one gets the impression from reading various online sources about Windows 2000 that DHCP is a good thing to implement so that Windows 2000 DNS runs smoothly. This is primarily because the Windows version of DNS is dynamic, but also because static IP addresses are rapidly becoming outdated. I had already configured DHCP in the Biology Windows NT 4.0 domain without any problems, so setting up DHCP in Windows 2000 was not very difficult.

The basic setup of DHCP in Windows 2000 is the same as Windows NT 4.0. One creates an IP address scope and makes that scope active so that clients can obtain an IP address. At UNC, since multiple DHCP servers exist and there is not a single centralized method of assigning IP addresses, it is a good idea to assign individual client hardware addresses from their network interface cards to specific IP addresses in the server's scope. In Biology's Windows NT 4.0 implementation of DHCP, DHCP in Windows 2000 is not really DHCP, but more of a BOOTP implementation instead. The server is

set up to assign IP addresses dynamically, but every client always gets the same IP address.

There are also a few more options with Windows 2000 DHCP, including the option to allow only DHCP clients, only BOOTP clients, or both. The only other difference with Windows DHCP is tighter control. Any DHCP server in a forest has to be authorized by the forest Enterprise Administrator. One could also argue that a forest Enterprise Administrator needs to have tight control over all TCP/IP services in the forest, and so DHCP server authorization is a good thing to have.

Before going ahead and upgrading a real production server (and thus the domain) to Windows 2000, there were a few more small-scale things that I wanted to test, foremost among them the Windows 95/98 Active Directory client, which was not well-advertised by Microsoft. After searching through the Windows 2000 Professional CD, I found a small program that, when run, supposedly installed a functional AD client on the Windows 9x computer. I followed the simple steps given to me by the program, but there were no obvious changes in the Windows 9x computer's Network Neighborhood or anywhere else. After reading about the AD client some more, I discovered that the only thing this AD client would allow one to do would be to search for printers in Active Directory, which did not seem very useful. The general idea apparently was that Microsoft did not want to spend a lot of time or resources in developing an AD client for Windows 9x or NT 4.0 clients. Instead, Microsoft has focused its efforts on pushing businesses to upgrade their computers to Windows 2000 Professional. This does make sense, but is not very helpful if the computers do not have the physical resources, such as memory and disk space, to actually be upgraded.

I made a few other discoveries about actually setting up Active Directory and Organizational Units. Unlike previous versions of Windows, opening My Network Places (the Windows 2000 equivalent of Network Neighborhood) starts the user at the top level of the network structure instead of in the local workgroup or OU. In a larger organization with lots of file and print sharing between various groups it makes more sense to start a user at the top level and have them work their way downward, but there should at least be an option somewhere in Windows 2000 to let the user choose where in My Network Places he wants to begin browsing. In addition, it seemed strange that network file shares are not automatically published in Active Directory local to the OU of the computer from which the files are actually being shared. Shared file volumes have to be manually published in AD, whereas there is an option for shared printers to automatically be published.

The final thing I wanted to test before upgrading a production domain controller to Windows 2000 was how well Thursby Corporation's DAVE network software interacted with Windows 2000 domains. DAVE uses NetBIOS and WINS to essentially give a Macintosh the same network interface as a Windows 9x client and is one of the better programs on the market to allow Macintoshes to interact with a Windows domain without adding the AppleTalk protocol to Windows servers. WINS will probably be necessary at UNC, even after pre-Windows 2000 PCs no longer exist, until (and if) DAVE is able to use DNS to communicate with other computers. To test DAVE with my test Windows 2000 domain, I changed the domain WINS name on a Macintosh running DAVE from Biology to Biodeath (the WINS name for biodeath.crashnburn.unc.edu). I then was able to login to Biodeath from the Macintosh, which worked without any

problems. Hopefully, future versions of DAVE will allow for true native-mode Windows 2000 interaction using DNS instead of WINS.

Initial Implementation Phase: Upgrading the Biology domain to Windows 2000

After testing everything and not seeing any major problems, I was ready to upgrade the Biology domain to Windows 2000 and create an Active Directory forest that I could later merge into a central UNC campus forest. The main concern before upgrading, though, was what to do if anything went wrong. The best solution I could think of was to promote the **Bioback** server, which was serving as a Windows NT 4.0 BDC (with no other functions), to the domain's PDC, since the PDC must be upgraded first. Bioback was a relatively inconsequential server to ordinary users, as it did not have any file or print shares and was only there for user authentication. If something were to go wrong during the upgrade, I would have the ability to take Bioback out of the domain and re-promote the **Biomass** server to the domain PDC.

The upgrade of Bioback itself to Windows 2000 Advanced Server was uneventful. Once the upgrade itself was completed, the Configure Your Server window automatically came up and asked me to configure Active Directory and DNS. Since I wanted to set up Bioback as the first Windows 2000 domain controller in the Biology domain, I created a new forest called bio.unc.edu with Bioback as the domain controller at the root of that forest with Biology as the sole domain. I then configured Active Directory on the **Biovideo** server to make it into a peer domain controller to Bioback. Biovideo was a Windows 2000 member server serving as the department's Windows Media Services streaming media server. This was done as a temporary measure to have another Windows 2000 DC in the domain in case something happened to Bioback, even

though the other two Windows NT 4.0 BDCs should have been able to still maintain domain integrity. (A side effect of this which I did not realize until later was that Active Directory causes problems with some of the services required for a Windows Media Server to function properly, and so a Windows Media Server cannot be a Windows 2000 domain controller.)

Since the log files on Bioback and Biovideo showed no critical errors, I started creating Organizational Units within the domain to reflect the general structure of the department. This was fairly straightforward; the process consisted of creating the OU itself and then moving the appropriate computers and users from the main Computers and Users containers into the desired OU. I also created some computers in the directory to represent those Windows 9x workstations and DAVE Macintoshes that were sharing files and put those computers into the appropriate OU as well. Since the Biology domain was in a single forest and thus did not have the transitive trust relationships necessary to share resources with other campus domains, there was no need to create an extensive AD infrastructure. However, I wanted to create an AD structure anyway to get a feel for what such an infrastructure might look like.

After waiting about 10 days to make sure everything continued to function normally, the next step was to upgrade one of the other Windows NT 4.0 BDCs, the **Biodata** server, to Windows 2000 Advanced Server. Since Biodata is the primary data server for all departmental users, I made sure to perform a full backup of Biodata's hard drives to tape before starting. Once the upgrade was complete, Biodata took a very long time to load the Windows desktop once I entered my username and password, but everything still worked. The Active Directory setup wizard came up automatically, so I

added Biodata back into the domain as another peer Windows 2000 DC and configured DNS to replicate from Bioback for redundancy. Replication of directory objects was actually very fast. Since I had now upgraded the department's primary data server to Windows 2000, I added the shared folders on Biodata into the domain AD infrastructure to get a feel for how everything would look when AD was actually being used.

Finally, I had one other issue that was important in determining when it would be safe to upgrade the last Windows NT 4.0 BDC to Windows 2000: making sure that the department's Microsoft Exchange 5.5 e-mail server would work in a Windows 2000 domain. I first reconfigured an old Netware server as a Windows 2000 Server named Biotest for testing purposes. This gave me the ability to use the Bioweb server as the new departmental Web server. I continually tried and failed to get a freeware program called Retrospect Exchange Agent to properly backup and restore the Exchange Directory and Information Stores from Biomass (the real Exchange 5.5 server) to Biotest (a test Exchange 5.5 server) for a period of over two weeks. The ultimate solution was to purchase an Exchange plug-in to our new tape backup software, Novanet 8. This new software was needed because the version we had of Veritas BackupExec was not compatible with Windows 2000 (and never worked properly anyway). It was not difficult to install Exchange 5.5 with Service Pack 3 on Biotest, create a few test mailboxes, backup the necessary Exchange database files to tape using Novanet 8, delete the mailboxes, and then restore the mailboxes from tape.

Useful Features of Windows 2000 (Server-Level)

Before describing the last steps of server upgrade and configuration, I would like to first mention a few of the new useful Windows 2000 features that I implemented in the

Biology domain. One useful feature of Windows 2000 is the ability to use disk quotas. This involves assigning users a maximum allotment of hard disk space on a particular logical drive of a server. Options are also available to set various restrictions as to the messages users receive when reaching or coming close to their quota. I implemented disk quotas on three of the five logical drives of the Biodata server without any difficulty. This feature would be more useful in a corporate environment where every user has their own account, but it has limited use in an academic setting where faculty labs often share one user account among all their members.

Another useful feature of Windows 2000 is disk compression. Windows 2000 disk compression compresses files when they are not in use, uncompresses them to their normal state when they are opened, and then recompresses them when they are closed. By enabling disk compression on all five of Biodata's logical drives, I was able to effectively double the amount of free space I had on each drive.

A third feature of Windows 2000 that I found useful was one mentioned earlier: Windows Media Services. Windows Media Services allows for the conversion of an AVI movie file into an ASF (Advanced Streaming Format) file. This ASF file can then be made available for users to view as streaming media over the Internet in a similar fashion to Quicktime and Real files. Since Microsoft has made a version of Windows Media Player available for Macintosh users, using Windows Media Services as our department's method of streaming media has proven to be very efficient.

Secondary Implementation Phase: Working with Windows 2000 Over Time

Up to this point, I had three Windows 2000 peer domain controllers (Bioback, Biovideo, and Biodata). Bioback was serving as the domain's PDC emulator, since it had

been the first Windows NT 4.0 domain controller to be upgraded to a Windows 2000 domain controller. Soon after upgrading Biodata to Windows 2000 and installing Active Directory, I removed Active Directory from Biovideo which changed it back into a member server. As mentioned earlier, Biovideo serves as the department's Windows Media Services server, Because of the problem with Windows Media Services not starting correctly when Active Directory was installed, I wanted to get that problem resolved first.

This left three domain controllers: Bioback, Biodata, and Biomass, which was still a Windows NT 4.0 BDC. At this point, my plan was to wait until ATN implemented a stable campus-wide unc.edu forest, demote the Bioback and Biodata servers to member servers, upgrade Biomass to Windows 2000 and join the unc.edu forest, and finally re-promote Bioback and Biodata as peer domain controllers with Biomass and be finished with the process. However, things did not work out that easily.

First, a decision was made by ATN in August 2000 to create a centralized unc.edu forest at the request of the College of Arts & Sciences Information Services group. At the time this seemed promising, but in fact all that materialized was a forest so the College could test Windows 2000. No other departments or other campus organizations joined the forest. Despite the fact that Windows 2000 had been out for six months and other universities were well along the way toward implementing it, very little was being done centrally at UNC to that effect. Finally, in February 2001, ATN announced to the campus e-mail computing support list that it had implemented an Active Directory unc.edu root forest and had expanded the schema to include the Microsoft Exchange Server 2000 extensions. However, since ATN was understaffed in regards to this project,

support would be based solely on demand (more on the ATN implementation will be discussed later).

Next, a major problem emerged with Bioback, which was serving as the PDC emulator. Starting in August 2000, Bioback began running out of system resources (mainly a combination of memory and virtual memory) approximately every three days and had to be rebooted in order for things to work properly. This affected not only the operation of that server itself, but also caused network operations, like browsing, to be impossible from workstations in the domain. Initially, I thought that a possible cause for Bioback's behavior was its age. Bioback was a Gateway Pentium Pro computer with a processor speed of only 200 MHz and contained only 128 MB of RAM, which was barely at the recommended minimum for Windows 2000 Server.

The only real solution I had was to replace Bioback with a faster computer with more resources to see if that would solve the problem. I set up a new IBM Carolina Computing Initiative (CCI) computer (with a 750 MHz processor and 192 MB of RAM) and installed Windows 2000 Advanced Server on that computer while it was plugged into a separate hub apart from the campus network, also named Bioback. To replace Bioback, I needed to remove Active Directory from Bioback, turn the old Bioback off, put the new Bioback online, and then set up Active Directory on the new Bioback.

First, however, I had to take into consideration the fact that Bioback was serving as the domain's PDC emulator. As mentioned earlier, in a Windows 2000 domain, there are five Flexible Single Master Operations (FSMO) roles that various Active Directory servers use to administer the domain (each role only exists in one instance in a domain,

but one server can hold more than one role).[17] When an Active Directory forest is initially created, the first domain controller holds all five roles, but some of the roles should be transferred to other servers in case that domain controller goes offline or becomes disabled. In order to properly replace Bioback and not completely disable the ability to administer Active Directory, I had to transfer all five FSMO roles to Biodata while I took the old Bioback server offline.

There is a procedure outlined in the Microsoft help Website[17] explaining how to neatly transfer these roles. In addition, there is an alternate procedure a server administrator can use to seize the roles if they cannot be transferred from the role holder. When I attempted to transfer the roles from the old Bioback to Biodata, none of them could be transferred and thus had to be seized from Bioback by Biodata. Once the roles had been seized, I removed Active Directory from the old Bioback and brought the new Bioback online, using the same IP address as that server had before. I set WINS and DNS up on the new Bioback, which worked smoothly and without any DNS replication problems from Biodata.

Another major problem that was occurring was on Biodata. Virtually instantly after Biodata was upgraded to Windows 2000 and set up as a peer DC, the server started writing two error messages to its Application Log every five minutes. These errors concerned a misconfigured security policy that could not be propagated to other Windows 2000 domain controllers located deep in the bowels of the operating system. This problem was not occurring on the old Bioback, but once the old Bioback was replaced with the new one, the same error messages began showing up in Bioback's Application Log as well. Along the same lines, the new Bioback began having the same

[17] http://support.microsoft.com/support/kb/articles/Q255/6/90.ASP

problems as the old one had before. Every two to three days, Bioback became sluggish due to a lack of system resources and had to be rebooted. Even though I had not transferred any of the FSMO roles back from Biodata to the new Bioback, this still was affecting network operations such as browsing.

The major question at this point was what to do next. I needed to leave Biomass as a Windows NT 4.0 BDC until the ATN unc.edu forest was stable enough to join, but I also needed to stabilize network operations in the Biology domain. It ultimately seemed that the best conclusion would be to remove Active Directory from the domain entirely and turn the domain back into a pure Windows NT 4.0 domain. This way, Biomass could be upgraded to Windows 2000 and joined to a centralized unc.edu forest when that forest proved to be stable. The problem was to find a way to accomplish this while causing as few problems as possible.

Final Steps: Going Back from Windows 2000 Server to Windows NT 4.0

Microsoft provides very little support in terms of working with hybrid Windows 2000 and Windows NT 4.0 domains. I was unable to get much information from any of their help Websites or technicians as to the best way to change the Biology domain back into a Windows NT 4.0 domain. The first thing I tried was an attempt to add another Windows NT 4.0 BDC to the domain. Since adding another peer Windows 2000 DC caused problems as explained above when I replaced Bioback, it seemed logical to try to add another Windows NT 4.0 BDC since Biomass was not having those same problems. However, the real main purpose of adding another Windows NT 4.0 BDC was to have another domain controller for Biomass to replicate with in case something happened to

Biomass. Otherwise, there would be no possible way to get back to a pure Windows NT 4.0 environment since no functional Windows NT 4.0 domain controllers would exist.

I acquired an extra Pentium III computer, formatted the hard drive, and installed Windows NT 4.0 Server. Everything went smoothly until I tried to add the new server (called **Biosrv1**) to the domain as a Windows NT 4.0 BDC. The installation process generated an error that the Biology domain could not be found. I realized this was due to the fact that the installation process was looking for a Windows NT 4.0 PDC that did not exist, since Biodata was serving as the Windows 2000 PDC emulator. In order to add Biosrv1 to the domain, I had to trick the existing domain controllers. I went into Server Manager on Biomass, promoted Biomass to become the Windows NT 4.0 PDC, and demoted Biodata to become a Windows 2000 BDC, which is not technically possible . I was then able to add Biosrv1 to the domain as a Windows NT 4.0 BDC. This tricked Biodata for a few minutes, but it soon realized that something was wrong and re-promoted itself to become the Windows 2000 PDC emulator. I had to manually demote Biomass to a BDC in order for domain logins to work properly because it was trying to be a PDC at the same time Biodata was trying to be the PDC emulator.

Now that I had a second functioning Windows NT 4.0 BDC on the domain, I now wanted to test the effects of actually removing Active Directory from the only Windows 2000 domain controller in a domain while Windows NT 4.0 BDCs were still in place. As I mentioned earlier, there was no documentation from Microsoft as to whether this was even possible, let alone how to go about doing it. To ensure that nothing disastrous would happen when I removed Active Directory from Biodata and Bioback, I decided to set up a test domain with two Windows NT 4.0 servers (**Biosrv2 and Biosrv3**). I set

these up with Biosrv2 as the test domain's PDC and with Biosrv3 as a BDC. I transferred the Windows NT 4.0 PDC role from Biosrv2 to Biosrv3 and upgraded Biosrv3 to Windows 2000 Advanced Server and installed Active Directory.

The real crux of the problem dealt with what would actually happen to user accounts and shared folders if Active Directory were to be removed from the domain. The worst possible scenario was that the domain would be destroyed and would have to be rebuilt from scratch. The best possible scenario was that, since Windows 2000 domain controllers replicate their account information to all other domain controllers, including Windows NT 4.0 BDCs, the domain would remain intact. It would also thus retain enough information about user accounts to function properly as a Windows NT 4.0 domain with the former Windows 2000 domain controllers now functioning as member servers.

To test this scenario, I created two users in my test domain and set up several shared folders on both Biosrv2 and Biosrv3 with different types of access permissions. I allowed the user account information enough time to replicate from Biosrv3 (the Windows 2000 DC) to Biosrv2 (the Windows NT 4.0 BDC) and then removed Active Directory from Biosrv3. The most interesting prompt in the removal process was the one asking me whether or not Biosrv3 was the last domain controller in the domain. By reading the description of the implications of answering yes to that question, it was obvious that it was referring only to Windows 2000 domain controllers. Therefore, I told the removal process that Biosrv3 was the last domain controller and went ahead. Everything worked perfectly – I was able to rejoin Biosrv3 to the test domain as a

member server. Also, both users I had created were still able to access the shared folders on both Biosrv2 and Biosrv3 without any problems.

I was now ready to remove Active Directory from the real Biology domain. I first ran DCPROMO on Bioback to remove Active Directory, which forced all account information to be replicated to Biodata. I allowed enough time for all the proper domain information to replicate properly from Biodata to Biomass and Biosrv1, and then I ran DCPROMO to remove Active Directory from Biodata. This was the point where I ran into major problems. First, I was unable to immediately rejoin Biodata to the Biology domain as a member server. It was unable to see the Biology domain, but it was able to see other UNC domains. I had to open up Server Manager on Biomass, manually promote Biomass to become the Windows NT 4.0 PDC and then manually remove Biodata from the Biology domain via Server Manager. After Biomass and Biosrv1 updated their account information (which took about half an hour), I was able to rejoin Biodata to the domain as a member server again.

Another major problem, for which I had failed to test, occurred with the Windows 2000 Professional workstations. Since the Macintoshes running DAVE (thus emulating Windows 98) and few remaining Windows 98/NT 4.0 computers did not have a computer account in the Biology domain, they were able to log in to the domain without any problems. However, the Windows 2000 workstations were not able to log into the domain, which was a serious issue.

Even though Biomass and Biosrv1 contained account information in their Server Managers for the Windows 2000 workstations that was replicated from Biodata, the accounts themselves were invalid because they contained Active Directory-specific

information that Biomass could not recognize. Thus, Biomass was unable to process new login requests from these workstations. The Windows 2000 workstations that were already logged in to the domain could not access any shared folders or printers on any other workstations or servers. The only solution to this problem was to manually remove and rejoin every Windows 2000 Professional workstation from the Biology domain, a process that had to be done physically at the workstation. This process generally took about 10 minutes and required two computer reboots. Given that there were about 230 Windows 2000 workstations in the domain, this was an extremely long process. However, once all the workstations has been removed and rejoined to the domain, they were able to access all network resources properly.

Currently, the Biology domain has two Windows NT 4.0 domain controllers (the PDC (Biomass) and one BDC (Biosrv1)) along with four Windows 2000 member servers (Biodata, Bioback, Bioweb, and Biovideo). At some point when a final decision is made on how the department's servers will be configured for Windows 2000, Biomass will be upgraded to Windows 2000 and joined to the existing ATN-centralized unc.edu forest root. Biodata and Bioback will have Active Directory re-installed and will be set up as peer domain controllers, and Biosrv1 will remain as a Windows NT 4.0 BDC in a mixed-mode domain in case of some other unforeseen circumstances. That final decision on how to configure Windows 2000 and Active Directory on the servers will have much to do with campus Windows 2000 server issues.

Summary of Steps for Upgrading a Domain From Windows NT to Windows 2000

1. Upgrade Windows 95/98/Me/NT 4.0 workstations to Windows 2000 Professional (may be done at any time).
2. Upgrade Windows NT 4.0 member servers to Windows 2000 Server or Advanced Server (do not run DCPROMO to install Active Directory).
3. Upgrade Windows NT 4.0 Primary Domain Controller to Windows 2000 Advanced Server. Steps to take after upgrading:
    a. Run DCPROMO to install Active Directory, deciding whether domain will be the root of a new forest or a subdomain of an existing forest (i.e. unc.edu).
    b. Install DNS (required for new Windows 2000 domains). Make sure DNS points to existing campus DNS service, either unc.edu root DNS server if domain is subdomain of unc.edu forest or campus DNS server if not.
    c. Check other existing networking services as needed or install for the first time (e.g. WINS, DHCP).
4. Upgrade Windows NT 4.0 Backup Domain Controllers to Windows 2000 Advanced Server. Steps to take after upgrading:
    a. Run DCPROMO to install Active Directory, adding to existing domain. Make certain server's DNS settings point at IP address of Windows 2000 PDC emulator for that domain or DCPROMO will not work.
    b. Install DNS and WINS on a second Windows 2000 peer domain controller for redundancy purposes.

   c. Transfer FSMO roles as desired (probably will want to transfer RID Master and Infrastructure Master from computer serving as Windows 2000 PDC emulator to other domain controllers).

5. Decide whether or not to convert to native mode (can only do this if no more Windows NT 4.0 Backup Domain Controllers exist, few advantages of doing so, such as universal groups).

Campus-Wide Windows 2000 Implementation

Until March 2001, there was very little demand from UNC departments for a centralized campus Active Directory forest, other than the initial cas.unc.edu test domain underneath the unc.edu forest as set up in October 2000 by ATN for the College of Arts and Sciences. Things began to change during March 2001, however, as several departments joined their Windows NT 4.0 domains to the central unc.edu forest and others inquired about that possibility. The remainder of this paper will discuss the current campus-wide Windows 2000 infrastructure scenario and future possibilities. First, I will present the current Windows 2000 and Active Directory implementation as provided by ATN. I will then provide some input from several departmental administrators as to what they are hoping to gain from a central unc.edu forest. Finally, I will summarize my findings and provide a recommendation for the unc.edu forest for the benefit of departments wishing to upgrade to Windows 2000.

ATN's Active Directory Implementation

On February 12, 2001, an e-mail was sent by Judd Knott, Director of ATN Computing Systems, to the campus CTC (Carolina Technology Consultants) e-mail list giving a very brief summary of the ATN Active Directory implementation and a link to an internal UNC Website giving more details.[18] The discussion below is taken both from that Website and from an in-person interview I had with ATN employee James Ervin on March 19, 2001.

The major technical issue with implementing Active Directory at UNC has been DNS. Microsoft's recommendation for those institutions with existing DNS services is to provide Active Directory with a segregated class-C DNS zone of its own, such as

[18] http://www.unc.edu/~jervin/working/UNC_AD_Design.htm

ad.unc.edu. Other universities have set up such an implementation, but ATN decided that this nomenclature would deviate too much from the existing DNS structure at UNC.

One of the major features that Microsoft provides in Active Directory is the potential for dynamic DNS (DDNS) as a method to eventually replace WINS for accessing computers over a LAN. However, the existing UNC campus Unix-based DNS servers did not support DDNS during the initial campus Active Directory design phase in October 2000. Migration to IP management using Lucent's QIP software tool place in January 2001, but it was not completely deployed at UNC and thus failed to completely solve the DDNS problems. In order for Active Directory to work at UNC, approximately 15 new DNS records were manually added to the Unix-based DNS server tables when the two ATN Windows 2000 domain controllers (maryceleste.unc.edu and sprucegoose.unc.edu) were brought on-line. Essentially, two separate DNS trees exist: one for regular DNS traffic and one for Active Directory DNS.

Problems currently exist in two areas. First, there is a synchronization issue when new Windows 2000 domain controllers are brought on-line. If those domain controllers do not have their DNS names registered on the central campus Unix-based DNS servers, other Windows 2000 computers within the unc.edu forest will not be able to access those domain controllers until the two DNS trees are synchronized. Second, reverse lookups for Windows 2000 computers will not work. A Windows 2000 computer within the unc.edu forest will be able to do a forward lookup through DNS to access non-Windows 2000 hosts at UNC and other non-UNC servers. However, it will be unable to query the campus DNS servers to find other Windows 2000 computers at UNC because DDNS cannot be easily implemented. For the time being, WINS will have to be the

predominant method by which Windows-based computers on campus communicate with one another.

The overall structure of the campus Active Directory forest is also unique to UNC. The basic Microsoft recommendation for a forest is that central domain controllers should reside at the root of the forest and that all other workstations and servers should be placed in a hierarchical OU structure underneath the forest. More typical forests contain multiple domain trees with subdomains and OUs underneath each tree. In addition, Microsoft also recommends that an organization with computers in different physical locations set up Active Directory "sites" to delineate physical boundaries. This is mainly to make the flow of network traffic more efficient over slower network links.

However, the UNC Active Directory structure does not exactly follow this recommendation. Most departments that either have already joined the UNC forest (such as Undergraduate Admissions, the Kenan-Flagler Business School, and the College of Arts & Sciences) or will join the UNC forest have or will have their own domain tree structure underneath the forest root. Other groups, such as the ATN computer labs, will be placed into an OU directly underneath the forest root. This makes no real difference to most users in accessing those computers, either through WINS or Active Directory, but will only make a difference to network administrators. In addition, since the UNC campus network is fast, the decision was made to place all departments joined to the forest within the same site, even for those groups not on the main campus (such as at 440 W. Franklin Street, the Friday Center, and the Physical Plant).

One of the major goals of a centralized Active Directory implementation was interoperability between multiple authentication methods and multiple operating system

platforms. Even though the basic groundwork has been laid for such interoperability at UNC, the details are not yet in place. First, it will be some time before Kerberos authentication is available for Windows 2000 computers. ATN currently uses Kerberos version 4 for authentication to Unix services, while Windows 2000 uses Kerberos version 5. At some point, it is hoped that the ATN Kerberos 4 implementation can be migrated to Kerberos 5 and some integration can be made with the Windows 2000 implementation of Kerberos 5 in a similar manner to the University of Colorado. No such migration is imminent, however.

The other major interoperability goal with a centralized unc.edu forest is using the UNC ONYEN along with the new version of IBM's AFS client for Windows 2000 to work with Kerberos. This would provide at least some measure of a single sign-on for users where authentication to all necessary services would take place at one time. Such a single sign-on implementation would be similar to that of the University of Colorado. The ONYEN database would be migrated into a single OU directly underneath the root of the Active Directory forest. Any child domain or OU underneath the forest would then use their ONYEN and password to sign-on to the forest. This would then authenticate that user via a one-way trust between the Windows 2000 Kerberos realm and the Unix-based Kerberos realm. There would be no need for individual user accounts within domains in this scenario. Local domain administrators could just create local groups and add the user accounts from the OU at the base of the forest containing all the ONYENs. The passwords for these user accounts would be a randomly generated string that no one would know forcing Kerberos to be the authentication method. This would also allow for a campus-wide password policy which would require a certain number of characters per

password and a restriction on how long a password could be used before expiration, greatly increasing security.

There are a few other brief notes to be made about the ATN Active Directory implementation. First, Microsoft Exchange 2000, while not widely used on campus yet, can now be implemented within individual domains. Exchange 2000 links more closely with Active Directory than Exchange 5.5 and utilizes more of the features of Active Directory. Next, the unc.edu forest root is currently set up as a mixed-mode domain, as are the other subdomain trees that have joined the forest. It is unknown to ATN whether the root of the forest can exist as a native-mode domain and subdomains can exist as mixed-mode domains, or vice versa. There are no plans to change any domains to native mode, as there currently is no need for any of the features of native-mode domains such as universal groups. Finally, there is no good way for Active Directory services at UNC to be made secure from hackers outside UNC, since the campus does not implement a firewall. Several groups are investigating technologies such as IPSec as a potential solution, but nothing has been decided on yet.

Windows 2000 and Active Directory in other UNC departments

After discussing the ATN implementation of Active Directory with James Ervin, I felt that I needed to gain some idea as to what other departments wanted from a central unc.edu forest and how they felt it could benefit them. I spoke to people in some departments and received e-mail from people in others, including Jason Li from the College of Arts and Sciences (which had already joined the unc.edu forest), Scott Adams from the School of Information and Library Science, David Parker from the School of

Education, Jesse Safir from Administrative Information Services (AIS), and Dave Kleinberg from the Department of Physics and Astronomy.

The College of Arts & Sciences was the initial group to request Windows 2000 implementation at the server level on campus during the early fall of 2000. The College's setup was straightforward: upgrade their PDC and two other BDCs to Windows 2000 and then create seven other Windows 2000 peer domain controllers. This was set up in such a way that the College initially created a cas.unc.edu Windows 2000 domain as the first child domain underneath the ATN unc.edu domain. They then proceeded to migrate their main ASNTDOMAIN1 Windows NT 4.0 domain as a child domain of cas.unc.edu after Windows 2000 had been completely tested, leaving asntdomain1.cas.unc.edu as the College's main Windows 2000 domain. The naming convention seems strange since it does not conform closely to the real campus DNS.

Similar to what I learned from James Ervin of ATN, the initial problem the College experienced with Windows 2000 at the server level was with DNS. Each workstation and server that has been set up with Windows 2000 within the College has an additional manual DNS entry to point to the central unc.edu Windows 2000 implementation for forward DNS lookups for other Windows 2000 computers. Since the College utilizes ATN's DHCP services, which do not include that Windows 2000 DNS entry, this manual DNS entry has to be made for Active Directory to work properly.

At this point, the College is only upgrading workstations to Windows 2000 on a per-demand basis. So far only about 200 out of 4,000 workstations have been upgraded from Windows 98 or NT 4.0 to Windows 2000 within the academic units that the College supports. That number is expected to increase as workstations are turned over within

academic units due to the Carolina Computing Initiative. Consequently, those workstations that are upgraded to Windows 2000 are placed within a single OU underneath the College's domain. As more departmental workstations are replaced with newer CCI computers running Windows 2000 Professional, it is likely that OUs will be created by department, but there is no need to do so at this time (even though two planned Windows 2000 computer labs will be set up in their own OUs).

The College is utilizing several of Windows 2000's special features. Users have the ability to utilize offline folders through their individual My Documents folder by using synchronization to back up the My Documents folder to a server. In addition, the College is planning to use more "push" technology when new computers are set up in departmental computer labs. This means that each workstation will come installed with only the operating system and individual software packages will be "pushed" down from a Windows 2000 server as needed which allows for easy software maintenance and updates. The College is also looking into utilizing the ONYEN for Kerberos authentication when that service is offered by ATN. The College currently has about 8,000 user accounts that are maintained on a domain level, many of which may belong to users that no longer exist.

The School of Information and Library Science (SILS) is mainly interested in the security features of Windows 2000, especially Professional. Virtually all SILS workstations have been upgraded to Windows 2000 at this time. SILS plans to upgrade its three domain controllers to Windows 2000 and join the campus unc.edu forest sometime during the summer of 2001.

SILS has traditionally operated a computer lab that was completely open to all faculty, staff, and students of the school. Each workstation has had one drive (traditionally G:) mapped to an open directory on one of the Windows NT 4.0 servers where anyone using those workstations could store data files. This has proved to be extremely inefficient and insecure, as anyone's files could be read and changed by anyone else. With Windows 2000, SILS has created a domain account for everyone associated with the school and will restrict the G: drive so that file sharing is more restrictive, user-controlled, and not completely wide-open. Future plans call for a potentially integrated login with AFS for SILS's Sun Server, ruby.ils.unc.edu, and Windows 2000. Those plans are on hold pending both a migration into AFS for ruby.ils.unc.edu and the ability for ATN to provide Kerberos authentication for Windows 2000.

The School of Education has only provided a limited migration to Windows 2000 thus far, mainly in the areas of file and print services, Web services, and Lotus Domino. At this point, they have no immediate plans to upgrade their domain controllers to Windows 2000 and join the central unc.edu forest. However, they are planning to upgrade the rest of their member servers to Windows 2000 in the near future. The major reason they have looked into Windows 2000 is due to its increased stability.

Administrative Information Services (AIS) has currently deployed Windows 2000 Professional to most of their departmental workstations and have upgraded several of their member servers to Windows 2000 as well. They feel the biggest benefit they would gain from Windows 2000 and Active Directory would be remote desktop management through integration with the Windows Installer to "push" software upgrades down to

workstations. In addition, AIS says that standardizing their users' workstations to Windows 2000 Professional will have enormous benefits in terms of desktop manageability. The upgrade to Windows 2000 at the server level is not as urgent, however.

AIS has not yet decided what to do with upgrading its servers to Windows 2000 and joining the campus unc.edu forest. They note that a single Active Directory forest for UNC has benefits for collaboration across departmental lines, but many of the details need to be worked out more extensively before they would feel comfortable participating.

The Department of Physics and Astronomy is the only known department on campus that has created its own production Windows 2000 forest separate from the main campus forest. Physics and Astronomy currently has 2 domain controllers, 80 workstations, and 12 laptops that are part of this forest. One of the department's major reasons for creating their own forest was for Kerberos authentication, since this has not yet been set up in the central unc.edu forest. The department has its own Unix-based Kerberos authentication system and departmental user accounts that are set up with Kerberos version 5, in which users log in to their Windows 2000 workstations with the same accounts as for their Unix workstations. In addition, each user has a roaming profile in which account information and preferences are stored on one of their servers and transferred between individual workstations that particular user may use. Even though this uses a great deal of hard disk space on the server, it is useful for maintaining preferences for users who may need access to multiple computers.

Final Analysis and Conclusions

The implementation of Windows 2000 at UNC-Chapel Hill is off to a good beginning. As more and more departments, including Biology, join the campus unc.edu forest, more knowledge will be gained as to what it will take to implement Windows 2000 in a useful way on campus and utilize its capabilities to the greatest extent possible. However, several issues must still be addressed further.

1. Security (User Authentication). Kerberos authentication is necessary for any successful Windows 2000 implementation on campus. The pace at which the ATN Unix-based Kerberos authentication system is migrating from version 4 to version 5 must be increased so that the ONYEN may become a viable method of authentication for all departments. Without Kerberos authentication, the ability to share resources between departments becomes that much harder due to more user accounts that must be maintained. For example, I have three user accounts on campus: my ONYEN, my SILS account, and my Biology account. Kerberos authentication will allow for me to only need my ONYEN for authentication to resources in SILS and Biology rather than maintaining all three accounts.
2. Security (Administration). The fact that the Department of Physics and Astronomy is running a separate production Active Directory forest from the ATN implementation is cause for concern. Departments that wish to test Active Directory on their own should be allowed to create their own implementations as needed (AIS and others are doing so as well), but these test implementations should only be allowed to exist for a short period of time and then taken off-line. Domain controllers of any departments not complying should have their network

communications blocked until they agree to comply. Separate forests for individual departments defeat the entire purpose of having Windows 2000. In addition, James Ervin noted that anyone on campus could bring up their own unc.edu forest and join workstations to it. This would not cause a conflict with the real ATN unc.edu forest unless that illegitimate forest became bigger in size than the real one, in which case problems could indeed occur. Steps need to be taken to ensure that this does not happen.

3. A Specific Upgrade Timetable. One of the major attitudes of many end-users along with some departmental administrators is one that "if it isn't broke, don't fix it." Since the last round of departments in the College of Arts and Sciences just received their CCI deployment (with Windows 98 as the operating system) during the fall of 2000, it will take some time for Windows 2000 to filter down to every end-user on campus. This may take as long as the end of the next CCI cycle in 2004. While no one should be forced to migrate their individual workstation to Windows 2000 or any later version, not doing so for the next four years will leave some people very far behind in terms of PC technology. Some specific steps need to be taken involving creating a deadline for all existing computers on campus that can efficiently support Windows 2000 to be upgraded. With Microsoft announcing its planned release of Windows XP later in 2001 to fully integrate the Windows 9x/Me and Windows NT/2000 lines of operating systems, such a deadline could be set at the end of the spring semester of 2002. This timetable would allow for Windows XP to become a stable operating system and be available as a home-user product as well. In addition, there has been a

rapid increase of broadband access through DSL (Digital Subscriber Line) and cable modems for home users over the last several years that will no doubt continue. This will inevitably cause a proliferation of VPNs (Virtual Private Networks), giving people with broadband access at home the capability to easily access network resources on campus. A faster migration must take place if UNC is to avoid being left behind in supporting all these potential capabilities.

4. Standardization of the campus Windows 2000 Infrastructure. With the migration to Windows 2000 that has taken place so far, there is no set method for the way the Windows 2000 infrastructure itself is created. Some departments have or will have their own domain tree within the UNC forest with OUs hierarchically created underneath. Other departments will only be in OUs directly underneath the root of the forest. While infrastructure flexibility is a nice feature of Windows 2000, some standardization needs to occur on campus so that Active Directory can become a useful search tool for locating network resources. This may be very difficult to achieve, however, due to the different ways departments and other academic and administrative units are managed in terms of computing support. Some individual departments may have to be managed as an OU within a larger unit, while others may be more self-sufficient and can have their own domain tree. This is more a political issue than anything and will probably be argued for some time.

In conclusion, despite the many hurdles and other obstacles a departmental Windows administrator must face when upgrading a domain from Windows NT 4.0 to Windows 2000, the results are well worth it despite the extensive learning curve. The improved

stability, security, user interface, and other features of Windows 2000 make it a vastly improved operating system over anything Microsoft has produced so far. As the world becomes more networked during the first decade of this century, UNC-Chapel Hill must continue to keep up technologically or risk being left behind. By ensuring that all members of the university community can easily collaborate with each other electronically using the tools that Microsoft provides with Windows 2000, UNC can at least partially eliminate any such risk.

References

Arizona State University. "ASU Windows 2000 Implementation." March 11, 2001. <http://www.west.asu.edu/itweb/win2000/>.

Arizona State University. "Windows 2000." March 11, 2001. <http://windows2000.asu.edu/>.

Cornell University. "Network and Host Registration." March 11, 2001. <http://dnsdb.cit.cornell.edu/>.

Cornell University. "Windows 2000 at Cornell." March 11, 2001. <http://www.cit.cornell.edu/computer/system/win2000/>.

Cornell University. "Windows 2000 Dynamic DNS Guidelines." March 11, 2001. <http://www.cit.cornell.edu/computer/system/win2000/dns.html>.

Cornell University. "Windows 2000 Kerberos Guidelines." March 11, 2001. <http://www.cit.cornell.edu/computer/system/win2000/kerberos.html>.

Indiana University. "Windows 2000." March 11, 2001. <http://windows2000.indiana.edu/>.

Microsoft Corporation. "Exploring Directory Services." March 3, 2001. <http://www.microsoft.com/windows2000/guide/server/features/directory.asp>.

Microsoft Corporation. "Q255690 – How to View and Transfer FSMO Roles in the Graphical User Interface." August 2, 2000. <http://support.microsoft.com/support/kb/articles/Q255/6/90.ASP>.

Microsoft Corporation. "Sample Chapter from Active Directory Services for Microsoft Windows 2000 Technical Reference." March 3, 2001. <http://mspress.microsoft.com/prod/books/sampchap/3173.htm>.

Stanford University. "Basic Windows Questions." March 11, 2001. <http://windows.stanford.edu/docs/basic.htm#ad>.

Stanford University. "My department is joining, and we have questions." March 11, 2001. <http://www-nt.stanford.edu/docs/joinquestions.html>.

Stanford University. "Windows 2000 at Stanford." March 11, 2001. <http://www-nt.stanford.edu/Win2000/>.

University of California at Davis. "Windows 2000 at UC Davis." March 11, 2001. <http://win2k.ucdavis.edu/>.

University of Colorado at Boulder. "Important Username and Password Information." March 11, 2001. <http://www.colorado.edu/its/windows2000/adminguide/userpassinfo.html>.

University of Colorado at Boulder. "UCB Windows 2000 Resource Center." March 11, 2001. <http://www.colorado.edu/its/windows2000/>.

University of Colorado at Boulder. "Windows 2000 Infrastructure Integration at UCB." March 11, 2001. <http://www.colorado.edu/its/windows2000/adminguide/infrainter.html>.

University of North Carolina at Chapel Hill. "ATN's Active Directory Implementation." March 20, 2001. <http://www.unc.edu/~jervin/working/UNC_AD_Design.htm>.