Windows 2000
Technical Guidelines

for School Network Implementation

Version 1.0

Information Technology in Education Project

January 2001
# Table of Contents

1 About this Document ................................................................. 5  
   1.1 Description........................................................................ 6  
   1.2 Objectives........................................................................ 7  
      1.2.1 Schools’ IT Team ......................................................... 7  
      1.2.2 Education Department’s IT in Education Support Team ....... 7  
   1.3 Scope .............................................................................. 8  
      1.3.1 Assumptions ............................................................... 8  
      1.3.2 Beyond this Document .............................................. 9  
         1.3.2.1 Responsibility of Schools ...................................... 9  
         1.3.2.2 Responsibility of Contractors ............................... 9  
   1.4 Document Features............................................................ 11  
      1.4.1 How to Read this Document ......................................... 11  
      1.4.2 Document Structure .................................................... 11  
   1.5 Reference.......................................................................... 14  
      1.5.1 IT in Education Project Documents ............................ 14  
      1.5.2 Microsoft Documents .................................................. 14  

2 Introduction to Windows 2000 ................................................. 15  
   2.1 The Windows 2000 Platform .............................................. 16  
      2.1.1 Windows 2000 Professional ....................................... 16  
      2.1.2 Windows 2000 Server Family ..................................... 16  
   2.2 Key Features and Benefits Overview..................................... 17  
      2.2.1 Using Windows 2000 Professional ................................ 17  
      2.2.2 Using Windows 2000 Server ........................................ 19  
      2.2.3 Using Windows 2000 Professional and Server Together .... 21  
   2.3 System Requirements......................................................... 23  
      2.3.1 Minimum System Requirements for Windows 2000 Professional ... 23  
      2.3.2 Minimum System Requirements for Windows 2000 Server ........ 24  
      2.3.3 Hardware and Software Compatibility .......................... 24  
   2.4 Licensing ........................................................................ 25  
      2.4.1 Licensing Modes for CAL ........................................... 25  
      2.4.2 Calculating CALs ....................................................... 26  

3 Network Infrastructure............................................................. 28  
   3.1 A Typical Windows 2000 School Network ........................... 29  
      3.1.1 Windows 2000 Domain Network ................................ 29  
      3.1.2 Active Directory ....................................................... 30  
      3.1.3 Servers .................................................................... 34  
      3.1.4 Client Computers ...................................................... 35  
   3.2 Network Communications.................................................... 37  
      3.2.1 Network Protocols ..................................................... 37  
      3.2.2 Network Addressing ................................................... 38  
         3.2.2.1 IP Address Range for Schools ............................... 38  
         3.2.2.2 DHCP .............................................................. 39  
      3.2.3 Naming Convention .................................................... 41
# Table of Contents

3.2.3.1 Domain Names .............................................................. 41  
3.2.3.2 Computer and Device Names .......................................... 43  
3.2.3.3 DNS ........................................................................ 46  
3.2.3.4 WINS ........................................................................ 46  

4 User Administration ................................................................. 48  

4.1 Management Tools in Windows 2000 ....................................... 49  
4.1.1 Microsoft Management Console ......................................... 49  
4.1.2 Remote Management .......................................................... 50  
4.1.3 Scripting ........................................................................ 51  

4.2 User Accounts Administration ................................................ 52  
4.2.1 Domain and Local User Accounts ....................................... 52  
4.2.2 Use of User Accounts ........................................................ 53  
4.2.3 User Naming Convention .................................................. 53  
4.2.4 User Profiles ................................................................... 55  

4.3 Grouping Strategy .................................................................. 59  
4.3.1 Organizational Units ............................................................ 59  
4.3.2 Groups .......................................................................... 60  

4.4 User Data and Settings Management ...................................... 65  
4.4.1 User Settings Management ............................................... 65  
4.4.1.1 In NT 4.0 School Network ........................................... 65  
4.4.1.2 In Windows 2000 School Network ................................. 66  
4.4.2 User Data Management ..................................................... 69  
4.4.2.1 Home Directory ........................................................... 69  
4.4.2.2 Folder Redirection ......................................................... 70  

4.5 Delegated Administration ....................................................... 75  

5 Resource Sharing ................................................................. 76  

5.1 File Sharing ........................................................................ 77  
5.1.1 File System ...................................................................... 77  
5.1.2 Data Sharing ................................................................... 78  
5.1.3 Disk Quotas ..................................................................... 82  
5.1.4 File Encryption ................................................................ 82  
5.1.5 File Usage on Notebook Computers ................................. 83  

5.2 Print Sharing ........................................................................ 85  

6 Security .................................................................................. 88  

6.1 Physical Security .................................................................... 89  

6.2 Data Security ......................................................................... 91  
6.2.1 Data Classification ............................................................ 91  
6.2.2 Third Party Personnel Access ............................................. 92  
6.2.3 Virus Protection ............................................................... 92  
6.2.4 Fault-tolerant Disk Systems ............................................... 93  
6.2.5 Uninterruptible Power Supply ............................................ 94  
6.2.6 System Backup and Recovery ............................................ 94  

6.3.1 Account and Password Policies ......................................... 98  
6.3.2 Control on System and Network Resources ....................... 100  
6.3.2.1 Group and System Policies .......................................... 100
Windows 2000 Technical Guidelines for School Network Implementation
IT in Education Project

Table of Contents

6.3.2.2 Permissions .............................................................. 100
6.3.2.3 Encrypting File System .............................................. 101
6.3.3 Audit Policy and Logs .................................................. 102

7 Extendibility ........................................................................ 104

7.1 Remote Access .................................................................. 105
7.1.1 Concurrent Connections .................................................. 105
7.1.2 Accessible Resources ..................................................... 106
7.1.3 Security Measures ......................................................... 107

7.2 Internet Access ................................................................. 109
7.2.1 Valid IP Address Range .................................................. 109
7.2.2 User Accessibility to Internet Resources ......................... 110
7.2.3 Performance Enhancement ............................................. 112

7.3 Integration with Existing Systems ....................................... 113
7.3.1 Adding NT 4.0 Computers to a Windows 2000 School Network ..... 115
7.3.2 Adding Windows 2000 Computers to an NT 4.0 School Network ... 116
7.3.3 Migrating an NT 4.0 School Network to a Windows 2000 Network . 117

8 Appendix A For More Information ................................. 120

9 Appendix B Parameters for Designing a Basic Windows 2000 School Network ..................... 134

10 Appendix C Checklist for Deploying Windows 2000 to Form a New School Network ............. 139

11 Appendix D Checklist for Integrating Windows 2000 to an Existing NT 4.0 School Network .... 141

12 Appendix E Checklist for Migrating an Existing NT 4.0 School Network to Windows 2000 ....... 144
1 About this Document

This document is intended to provide technical guidelines for Teaching and Learning School Network implementation with Microsoft Windows 2000 under the provision of computer equipment of the IT in Education Project.
1.1 Description

This document aims primarily at assisting schools in formulating their requirements for deploying Microsoft Windows 2000 to their Teaching and Learning School Network (hereafter named as School Network). In addition, this document also presents an overview of Windows 2000 and related information of Windows NT 4.0 which provides the necessary knowledge for schools in evaluating the benefits of deploying Windows 2000 to their school environments.

This document is intended for the following target readers:

- Schools' IT Team
- The Education Department (ED)’s IT in Education (ITED) Support Team
1.2 Objectives

In general, this document is intended to:

- Provide an overview of Windows 2000 and assist in help evaluating which Windows 2000 features would be most suitable in the school environment
- Provide technical guidelines for School Network implementation with Windows 2000
- Act as a basis for schools and ED to discuss and plan on the details of School Network implementation with contractors, under the IT in Education project

More specific objectives are set for different target readers and they are:

1.2.1 Schools' IT Team

- To gain an understanding of Windows 2000 features and how schools can benefit from them
- To gain the fundamental knowledge for the planning of the deployment, integration and/or migration to Windows 2000
- To gain the necessary knowledge for formulating the general requirements for School Network implementation with Windows 2000, according to their schools' respective needs and readiness
- To use this document as a basis for the discussion with contractors on the details of School Network implementation
- To use this document as a checklist for monitoring contractors on various aspects of School Network implementation

1.2.2 Education Department's IT in Education Support Team

- To use this document for assisting schools to understand the issues and considerations related to School Network implementation with Windows 2000
1.3 Scope

This document provides technical guidelines to schools in formulating the requirements for implementing a basic Windows 2000 Teaching and Learning School Network. It focuses mainly on the deployment of Windows 2000 to form a new School Network that is capable of inter-operating with other common networks and systems.

In addition, this document also provides information for integrating Windows 2000 with other school systems that are implemented with the hardware and software items under the standard provision of the IT in Education Project (i.e. standalone Windows NT 4.0 computers (ED1 / ED2), and/or Windows NT 4.0 School Network (ED3)).

Notes

This document is not intended to serve as a Windows 2000 training manual. Only key features of Windows 2000 that are potentially beneficial to schools are highlighted. For instance, fundamental School Network design and planning on network infrastructure, user administration, file and print sharing will be discussed in this document. On the other hand, the usage of advanced Windows 2000 features such as Internet Information Services (IIS) and Terminal Services are outside the scope of this document and only brief introduction will be provided.

Besides those scenarios and School Network configurations discussed in this document, schools may have other networks and systems (e.g. iMac, Linux, and/or other Internet-related systems) that are implemented under other projects in their existing school environments. For detailed information on the interoperability of these networks and systems with the School Network discussed here, schools should consult contractors for suggestions and further information.

Furthermore, the implementation of a School Network may also involve other aspects such as site preparation and procurement of hardware and software items, schools should refer to the "Procurement Guidelines (Hardware, Software, and Services)" and other related documents issued by the Education Department for information concerning these aspects.

1.3.1 Assumptions

This document is written with the following assumptions:

- The school site is ready for the installation and configuration
- The School Network is to be built on the hardware and software items under the standard provision of the MultiMedia Computers for Primary Schools (ED1), the Replacement of Computers for Secondary and
Special Schools (ED2), and the Supply of Computer Hardware, Software and Related Services to Schools (ED3) for the Education Department

- Relevant hardware and software items required for the School Network are ready
- Windows 2000 is to be implemented for the School Network
- The readers already have knowledge on:
  - basic computer hardware components, including central processing units (CPUs), computer memory, and hard disks
  - an operating system (OS), such as Microsoft Windows 95/98, Windows NT 4.0 Workstation, or Windows NT 4.0 Server
  - major networking components, including clients, servers, and local area networks (LANs)

1.3.2 Beyond this Document

1.3.2.1 Responsibility of Schools

It should be noted that the guidelines in this document are for schools’ general reference only. Schools should cater for their specific requirements and consult contractors to formulate the detailed system design and implementation plan. In this connection, schools are advised to work closely with contractors to compile the latest information for the following:

- User requirements, according to schools’ respective needs and readiness
- Project requirements, such as project schedule, budget, human resources, risk and impact assessments, geographical considerations etc.

1.3.2.2 Responsibility of Contractors

This document is not intended for conducting skills-transfer to contractors since contractors should already be equipped with all necessary skills and knowledge. Contractors must possess adequate level of skills and most updated information to provide a cost-effective, flexible and future-proven technical solution addressing schools’ requirements.

If any information in this document is no longer suitable or applicable to schools’ environments, it is the responsibility of contractors to provide corresponding updated and appropriate information to schools.
Documentation Provided by Contractors

Contractors should provide documentation to schools on steps and procedures for network implementation, administration and operation. The documentation includes but is not limited to the following:

- Network Installation Report
- Installation Guideline of Hardware and Software
- Network Administration Guideline
- User Manuals
1.4 **Document Features**

Generally, there are five key aspects for deploying a basic Windows 2000 network. They are:

- **Network Infrastructure**
- **User Administration**
- **Resource Sharing**
- **Security**
- **Extendibility**

The core part of this document discusses these five key aspects (**NURSE**) and provide technical guidelines for deploying a new Windows 2000 School Network. See "Document Structure" below for further details.

1.4.1 **How to Read this Document**

Readers should proceed this document through chapters in a linear fashion. Starting with "Introduction to Windows 2000", readers can learn fundamental knowledge on Windows 2000 features. They can then move on to the next chapter, "Network Infrastructure", to gain insight on how to plan and design the network infrastructure and so on, with Windows 2000.

Moreover, appendices are included to provide further information on Windows 2000. Readers may also reference the checklists and technical information in order to implement the School Network with contractors.

1.4.2 **Document Structure**

- **Chapter 1**
  
  "About this Document" (this chapter) provides a brief description of the document, its target readers, and the document objectives and scope.

- **Chapter 2**
  
  "Introduction to Windows 2000" provides an overview of Windows 2000 platform and its key features, the benefits Windows 2000 can bring to schools and its system requirements. The purpose of this chapter is to introduce the capabilities of Windows 2000 and to provide a foundation for the readers to evaluate the benefits of Windows 2000,
and help schools determine their requirements.

- **Chapter 3**
  
  "Network Infrastructure" provides an overview of the primary building blocks of a Windows 2000 School Network and the role each one of which plays. For example, it discusses the design of Active Directory, Domains, Domain Controllers, Organizational Units, Group Policy, Servers, Clients, IP addressing scheme, DNS, DHCP and so on.

- **Chapter 4**
  
  "User Administration" discusses user accounts administration, naming conventions, grouping strategy, and user data and settings management etc.

- **Chapter 5**
  
  "Resource Sharing" provides information on various network resources and services such as file system, file sharing, disk quotas management as well as print sharing.

- **Chapter 6**
  
  "Security" presents general information related to IT security in a School Network such as physical and hardware security, Windows 2000 data access control, anti-virus protection, uninterruptible power supply, as well as system backup and recovery.

- **Chapter 7**
  
  "Extendibility" discusses the issues related to the interoperability with other systems and networks, e.g. remote access to School Network, connection to the Internet, integration with existing systems and networks etc.

- **Appendix A**
  
  "For More Information" provides additional and advanced information on Windows 2000. More detailed description on various major Windows 2000 features and components are also discussed here.

- **Appendix B**
  
  "Parameters for Designing a Basic Windows 2000 School Network" provides a list of parameters for designing a basic Windows
2000 School Network.

- **Appendix C**

“*Checklist for Deploying Windows 2000 to Form a New School Network*” provides a checklist for deploying a new Windows 2000 to form a new School Network (i.e. Windows 2000 as main server and Windows 2000 or NT 4.0 as clients).

This checklist is intended for schools having standalone NT 4.0 Workstation computers with no School Network (e.g. ED1 or ED2) and planning to deploy Windows 2000 as their School Networks.

- **Appendix D**

“*Checklist for Integrating Windows 2000 to an Existing NT 4.0 School Network*” provides a checklist for integrating Windows 2000 to an existing NT 4.0 School Network (i.e. NT 4.0 as main server and Windows 2000 or NT 4.0 as clients).

This checklist is intended for schools having an NT 4.0 School Network (e.g. ED3) and planning to integrate Windows 2000 into their existing NT 4.0 School Networks.

- **Appendix E**

“*Checklist for Migrating an Existing NT 4.0 School Network to Windows 2000*” provides a checklist for migrating an existing Windows NT 4.0 School Network to a Windows 2000 School Network (i.e. upgrading Windows NT 4.0 Server and Workstation to Windows 2000 Server and Professional respectively).

This checklist is intended for schools having an NT 4.0 School Network (e.g. ED3) and planning to migrate their existing NT 4.0 School Networks to Windows 2000 School Networks.
1.5 Reference

This document is written with reference to the following documents:

1.5.1 IT in Education Project Documents

- Technical Guidelines for School LAN Implementation for the Information Technology in Education Project, dated June 1999 (hereafter called "NT 4.0 Technical Guidelines")
- Procurement Guidelines (Hardware, Software, and Services) for the Information Technology in Education Project
- Technical Support Services — Acquisition Guidelines for the Information Technology in Education Project

1.5.2 Microsoft Documents

- Microsoft Windows 2000 Home Page
  http://www.microsoft.com/windows2000/
- Microsoft in Education: Windows 2000, Providing a Foundation in Education
  http://www.microsoft.com/education/win2k.asp
- Microsoft Windows 2000 Planning and Deployment
- Microsoft Product Support Services
  http://support.microsoft.com/directory/
2 Introduction to Windows 2000

The Microsoft Windows 2000 operating system (OS) is the next generation of the Microsoft Windows NT 4.0 (NT 4.0) OS. Understanding Windows 2000 concepts and features is important to schools in designing a Windows 2000 School Network and determining their requirements. This introduction to Windows 2000 is intended to:

- Identify the members in Windows 2000 platform
- Describe the key features of Windows 2000
- Outline the key benefits Windows 2000 can bring to schools
- Identify the system requirements for Windows 2000
- Provide an overview on Windows 2000 licensing

For more information about Windows 2000, see Microsoft Windows 2000 web site at http://www.microsoft.com/windows2000/
2.1 The Windows 2000 Platform

The Windows 2000 platform is a product line of OS for different types of computers, from notebook/desktop computers to servers. Typically, computers can be classified into two roles: client and server. Windows 2000 platform has the corresponding stream for each role, namely:

- Windows 2000 Professional
- Windows 2000 Server family

2.1.1 Windows 2000 Professional

Windows 2000 Professional is designed for client computers, such as the students’ and teachers’ desktop and notebook computers in school environment. It is the successor of NT 4.0 Workstation with broader hardware and mobile support.

For detailed information about Windows 2000 Professional, see Microsoft Windows 2000 Professional web pages at http://www.microsoft.com/windows2000/guide/professional/overview/

2.1.2 Windows 2000 Server Family

Windows 2000 Server family is designed for server computers, such as the file and print servers in schools' server rooms. It is the successor of NT 4.0 Server and provides back-end network services (e.g. file and print sharing, network address assignment etc.).

There are 3 members in the Windows 2000 Server family:

- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Datacenter Server

Windows 2000 Advanced Server and Datacenter Server are designed to support higher volume of users and more complex applications. In school environment, Windows 2000 Server is generally powerful enough to provide the required network-related services. Therefore, for server computers, this document will focus on Windows 2000 Server.

2.2 Key Features and Benefits Overview

While most of the functionality of NT 4.0 are also available under Windows 2000, some of which are enhanced and lots of new ones are added to Windows 2000 platform. Some features are available when using either Windows 2000 Professional or Windows 2000 Server, while some require Windows 2000 Professional and Server working together.

The following is an overview of the key features of Windows 2000 that may be beneficial to schools. However, it should be noted that it is not intended to be a complete description of all the features. Such features can be classified under the following categories:

- Using Windows 2000 Professional
- Using Windows 2000 Server
- Using Windows 2000 Professional and Server Together

2.2.1 Using Windows 2000 Professional

Compare with NT 4.0 Workstation, Windows 2000 Professional provides a number of improved features. Some of them may offer schools benefits in the following aspects:

- **Multi-language Support**

  Over hundred of languages, including English, Traditional Chinese and Simplified Chinese, can be displayed, inputted and printed in single language platform of Windows 2000.

  **Benefits**

  - Students and teachers can run multi-language capable applications (e.g. Microsoft Office 2000) and manage documents with multiple languages (e.g. a Microsoft Word document containing English, Traditional and Simplified Chinese characters) in single language platform of Windows 2000. If they are using multi-language capable applications, third party multi-language enabling software (e.g. RichWin) may no longer be required.

- **Broader Hardware Support**

  Broader support on common hardware standards and devices such as:

  - Universal Serial Bus (USB)
    e.g. scanners, printers, Chinese handwriting input devices

  - IEEE 1394 (or FireWire)
    e.g. digital camera
- DVD devices (third party DVD video player software is required)  
  e.g. educational titles in DVD media

- Plug-and-Play (PnP) adapters  
  e.g. sound cards, network interface cards (NICs)

- Infrared devices (IrDA)

**Benefits**

- More USB and IEEE1394 hardware devices are coming out on market. Schools can have more choices on the variety of hardware

- By using the infrared ports in notebook computers, teachers can print directly to the infrared-capable printers. In addition, wireless file transfer is possible between these notebook computers

### Power Management Support

Better support on power management:

- Support Advanced Configuration and Power Interface (ACPI)

- Support hibernation mode for quick computer startup

**Benefits**

- When shutting down using the hibernation mode, the boot-up waiting time can be shortened in the next startup. In addition, when re-activating the computer, the running programs and settings since the last shut down can be restored. This is especially useful for teachers when performing class presentation.

### Enhanced File Services

File services are enhanced and some disk utilities are now built-in with the OS:

- Encrypting File System (EFS)

- Built-in disk defragmenter

- Built-in disk quota management

- Offline Files and Folders

**Benefits**

- Security can be strengthened by encrypting the files and folders on computer's hard disk. Unauthorized users will not be able to read the content of the encrypted files. Data can be protected even if the computer is stolen or lost
- Built-in disk defragmenter can help to improve disk access performance by rearranging disk clusters

- Built-in disk quota management can track and control disk usage on a per-user and per-volume basis. School Network administrators can prevent users from using excessive disk space by setting disk quota for each of them

- Data availability can be improved by utilizing the Offline Files and Folders feature. Users in the School Network can access and work on the files when the network is down. In addition, users can work on the local copies and the file synchronization feature will keep the network and local copies synchronized. This is especially useful for notebook computer users. For instance, teachers can prepare teaching materials by using a notebook computer at home and when they get back to school and re-connect the notebook computer to the School Network those modified files will then be automatically synchronized with the copies in the school server.

For more information about these topics, see Chapter 4 "User Administration" and Chapter 5 "Resource Sharing".

- **Internet-related Services**
  - Internet Connection Sharing (ICS)
  - Internet Information Services (IIS) 5.0

**Benefits**

- An Internet connection on a computer can be shared by other networked computers. For example, without acquiring modem sharing devices (e.g. IP Sharer) or Internet sharing software (e.g. SyGate), a school server with simple Internet connection (e.g. dial-up modem connection) and ICS service can allow other networked computers to access the Internet also.

- Schools may use the IIS 5.0 with enhanced features for building school intranet or Internet web sites.

2.2.2 **Using Windows 2000 Server**

In addition to the features of Windows 2000 Professional, Windows 2000 Server supports the following:

- **Simplified Administration and Management**

  The way of performing system administration and network management in NT 4.0 is enhanced with:

  - Active Directory (AD)
- Microsoft Management Console (MMC)

Benefits

- AD is a new technology in Windows 2000. It provides tree-like directory structure and services to organize all the objects on the network hierarchically. For instance, the objects in a School Network such as users, groups, computers, files, printers and network services can be managed and located more logically with AD. It simplifies user administration and system management for School Network administrators. In addition, it also facilitates users to locate network resources on School Network more easily.

- In Windows 2000, MMC provides a consistent user interface to perform various administrative tasks. In addition, MMC interface can be customized by adding or deleting the snap-in tasks to the console to suit the requirements of different School Network administrators.

For more information about these topics, see Chapter 3 "Network Infrastructure" and Chapter 4 "User Administration".

- **Enhanced File Services**
  - Distributed File System (DFS)

Benefits

- School Network administrators can organize file and folder shares from various physical locations (e.g. different school servers) into a hierarchical and more manageable single-tree structure.

- Collections of servers and file shares can be mapped using a uniform naming convention. Teachers and students can access the shared files and folders without remembering the location of the resources. This allows users to find and manage data on the School Network more easily.

- **Terminal Services**
  - Remote Management (Remote Administration Mode)
  - Terminal Emulation Services (Application Server Mode)

Benefits

- Remote management with Terminal Services (remote administration mode) enables School Network administrators to remotely manage the school servers from a workstation on the School Network or a PC at home (provided that remote access service is enabled in their School Network). They can perform the tasks as if they are sitting in front of the servers. Each Windows
2000 Server supports up to two concurrent sessions for remote management

- By enabling Terminal Services (application server mode) in the school server, aged PCs which have relatively low computing power, small amounts of RAM and local disk storage capacity can be utilized to run prevailing software. In addition, desktop settings as well as software deployment can be centrally managed

### 2.2.3 Using Windows 2000 Professional and Server Together

Some Windows 2000 services can only work when using Windows Professional and Server together (it requires Active Directory). The following examples demonstrate only a few of the many possible ways of applying these features in school environment:

#### Notes

*Only when using Windows 2000 Professional and Server together can schools benefit from the features discussed in this section, while systems other than Windows 2000 such as NT 4.0 Workstation and Server, Windows Millennium, Windows 98, Windows 95 and Windows 3.x as well as DOS will not be able to benefit from these features.*

- **Policy-based User Data and Settings Management**

  School Network administrators can manage users' desktop resources by applying policies based on schools’ needs and organizational structure (e.g. teachers, students, forms, classes, interest groups). In addition to the System Policy in NT 4.0, Windows 2000 offers more controls on students’ and teachers’ environment such as desktop settings, user rights, security, applications and resources.

  **Benefits**

  - User data and settings can be centrally managed by the policies defined by School Network administrators

  - This allows for a consistent user interface and ensuring that students and teachers do not inadvertently damage the systems

- **Delegated Administration**

  School Network administrators can delegate a selected set of administrative privileges to appropriate individuals (e.g. teachers or leaders of interest groups) and specify their rights.

  **Benefits**
- Delegated administration can provide flexibility in School Network administration

■ Automated Software Installation and Maintenance

School Network administrators can specify a set of applications that should always be available to a user or group of users. Software installation, repairs, updates and removal can be done automatically.

Benefits

- Application software, updates and patches can be automatically distributed to computers or users based on their role in schools. For example, newly acquired web authoring software for Computer Laboratory can be centrally packaged and deployed once in the school server. When the workstations in Computer Laboratory connect to the network, the web authoring software stored in the school server will be automatically distributed to these workstations. This can help to reduce or eliminate the efforts of School Network administrators in software installation and configuration.

For more information about these topics, see Chapter 4 "User Administration".
2.3 System Requirements

The following sections describe the minimum system requirements suggested by Microsoft for Windows 2000 client and server machines. It is observed that such requirements can be met by workstations under ED2 and ED3. However, for workstations under ED1 and servers under ED3, system memory may need to be upgraded to meet the minimum system requirements.

Notes

The minimum system requirements suggested by Microsoft are for running Windows 2000 operating systems at minimal performance. In order to improve system responsiveness, additional system resources such as higher processor speed, more memory and hard disk space are required for running schools' specific add-on applications, such as office suite (e.g. Microsoft Office 2000), graphics and drawing software (e.g. Adobe PhotoShop), web content design and authoring tools (e.g. Microsoft FrontPage, Macromedia Authorware) etc.

Guidelines

- Computers to be installed with Windows 2000 should at least meet Microsoft's minimum system requirements. Besides, additional system resources may be required for running add-on applications with acceptable performance.
- Application software deployed in schools varies. So to ensure satisfactory performance of the School Network, schools should work with contractors to determine the system requirements for their Windows 2000 servers and workstations.

2.3.1 Minimum System Requirements for Windows 2000 Professional

<table>
<thead>
<tr>
<th>Product</th>
<th>Minimum System Requirements suggested by Microsoft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000 Professional</td>
<td>CPU: Pentium 133MHz or above</td>
</tr>
<tr>
<td></td>
<td>RAM: 64MB or above</td>
</tr>
<tr>
<td></td>
<td>Hard disk: 2GB with 650MB free space</td>
</tr>
</tbody>
</table>

For more information on Windows 2000 Professional system requirements,
see Microsoft Windows 2000 client system requirements web pages at http://www.microsoft.com/windows2000/guide/professional/sysreq/

### 2.3.2 Minimum System Requirements for Windows 2000 Server

<table>
<thead>
<tr>
<th>Product</th>
<th>Minimum System Requirements suggested by Microsoft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000 Server</td>
<td>• CPU: Pentium 133MHz or above</td>
</tr>
<tr>
<td></td>
<td>• RAM: 128MB (minimum supported) or above</td>
</tr>
<tr>
<td></td>
<td>• 256MB (recommended minimum) or above</td>
</tr>
<tr>
<td></td>
<td>• Hard disk: 2GB with 1GB free space</td>
</tr>
</tbody>
</table>

For more information on Windows 2000 Server system requirements, see Microsoft Windows 2000 server system requirements web pages at http://www.microsoft.com/windows2000/guide/server/sysreq/

### 2.3.3 Hardware and Software Compatibility

In addition to system requirements, it should be noted that some of the hardware and software items on the market may not be compatible with Windows 2000, or special configurations are required to make the computer systems work properly.

For example, in order to make pre-Windows 2000 computers able to recognize Windows 2000, these computers may require BIOS upgrade. Although Windows 2000 supports new hardware standards such as USB, DVD and IEEE 1394 (FireWire), corresponding software drivers are required for the hardware to function properly and/or optimally.

Furthermore, applications that run under NT 4.0 may not continue to run under Windows 2000. For instance, Norton Utilities 4.0 for NT which is OS-specific is not compatible with Windows 2000.

For more information about hardware and software compatibility issues, see Microsoft Windows 2000 hardware and software compatibility web pages at http://www.microsoft.com/windows2000/upgrade/compat/

**Guidelines**

- Work with contractors to ensure the hardware and software items used in School Network are compatible with Windows 2000.
2.4 Licensing

For each Windows 2000 server computer, a Windows 2000 Server license is required. Similarly, a Windows 2000 Professional license is required for each Windows 2000 client computer.

Besides, for client computers using server services\(^1\) in the Windows 2000 School Network, Windows 2000 Server Client Access Licenses (CALs) are also required. More information about CALs is provided in the following sections.

However, for standalone Windows 2000 Professional computers that do not require connecting to the School Network, no Windows 2000 Server CAL is required.

\textit{Notes}

\textit{CALs for client computers must have the same or a later version number than the corresponding version number of the server software.}

2.4.1 Licensing Modes for CAL

There are two licensing modes for Windows 2000 Server CAL: per-seat or per-server:

- **Per-seat Licensing**

  With per-seat licensing, each client computer that connects to any Windows 2000 Server in the School Network requires a Windows 2000 Server CAL. Client computers are allowed to access any server within the School Network, as long as the client computers (seats) are licensed with appropriate Windows 2000 Server CAL.

  In general, a per-seat license is most economical to those School Networks where workstations frequently connect to multiple servers.

- **Per-server Licensing**

  With per-server licensing, each Windows 2000 Server CAL is associated with a particular server. Schools must have enough CALs dedicated to each school server to accommodate the maximum number of clients that will connect to that server at any point of time (i.e. concurrent

---

\(^1\) Windows 2000 Server services include:

- Authentication services (e.g. logging on to the school server)
- File services (e.g. accessing or managing files in the school server)
- Printing services (e.g. printing to a printer managed by the school server)
- Remote access services (e.g. accessing the school server from a teacher's home via dial-up modem)
connections). Schools have to option to switch from per-server to per-seat licensing mode once.

In general, a per-server license is most economical to those School Networks where workstations infrequently connect to single or specific servers.

2.4.2 Calculating CALs

- **Example A**
  
  There are 40 workstations and 1 server in the School Network:

  Select **per-server license**. Purchase 40 CALs.

- **Example B**
  
  There are 80 workstations and 2 servers in the School Network:

  **Scenario B1**

  These 80 workstations need to regularly connect to the 2 school servers at the same time.

  Select **per-seat license**. Purchase 80 CALs.

  **Scenario B2**

  These 80 workstations do not need to regularly connect to the 2 school servers at the same time. Instead, there will be no more than 40 connections to server A and 20 connections to server B at the same time.

  Select **per-server license**. Purchase 60 CALs, 40 for server A and 20 for server B.


**Guidelines**

- Choose per-server licensing if there is only one server in the School Network and ensure that there is sufficient number of Client Access Licenses (CALs) for the workstations to access the servers for basic network services.
Consult contractors for the appropriate licensing mode and the number of CALs required to cater for the current and future requirements if there is more than one server in the School Network.
3 **Network Infrastructure**

Successful implementation of a Windows 2000 School Network requires careful planning and design. The previous chapter has presented the features and benefits of Windows 2000. Schools should already have gained the fundamental knowledge on Windows 2000 and determined their requirements and relative priority for their respective school environments. This chapter, "Network Infrastructure", is intended to provide:

- An overview of the primary building elements of a typical Windows 2000 School Network
- Technical guidelines on building up a typical Windows 2000 School Network

Information on user administration, resource management, security measures and interoperability with other systems will be discussed in later chapters.

In addition, advanced technical information on Windows 2000 can be found in Appendix A “For More Information”. Furthermore, School Network administrators should reference the information in Appendix B "Parameters for Designing a Basic Windows 2000 School Network" and Appendix C “Checklist for Deploying Windows 2000 to Form a New School Network” when planning and designing a new Windows 2000 School Network.
3.1 A Typical Windows 2000 School Network

A Windows 2000 School Network is typically composed of the following:

- Windows 2000 domain network
- Active Directory
- Servers
- Client computers

3.1.1 Windows 2000 Domain Network

Windows 2000 supports two types of networks and they are:

- Windows 2000 Workgroup Network

A Windows 2000 workgroup network is a logical grouping of networked computers that share resources, such as files and printers. A workgroup is referred to as a peer-to-peer network because all computers in the workgroup can share resources as equals, or as peers, without a dedicated server. Each computer in the workgroup, running either Windows 2000 Server or Windows 2000 Professional, maintains a local security database. A local security database is a list of user accounts and their resource security information on that computer. Therefore, the administration of user accounts and resource security in a workgroup is decentralized.

Because workgroups have decentralized administration and security, a user must have a user account on each computer to which he or she wants to gain access. Any changes to user accounts, such as changing a user's password or adding a new user account, must be made on each computer individually in the workgroup. For example, if the School Network administrator forgets to add a new user account to one of the Windows 2000 Professional computers in the workgroup, the new user will not be able to log on to those computers and will not be able to access resources on them.

- Windows 2000 Domain Network

A Windows 2000 domain network is a logical grouping of network computers that share a central directory database. The central directory database contains system critical information such as user accounts and security information for the domain and is known as the Active Directory.

In a domain, the Active Directory resides on computers that are configured as domain controllers. A domain controller is a Windows 2000 Server that manages all security-related aspects of user/domain
interactions. Security and administration are thus centralized.

Generally, School Network implemented using Windows 2000 domain network will have more advantages over those using Windows 2000 workgroup network. For example,

- A Windows 2000 domain network provides centralized administration because all user information is stored centrally. This reduces the workload of School Network administrators.

- A Windows 2000 domain network provides a single logon process for users to gain access to network resources, such as file, print, and application resources for which they have permissions. For instance, students and teachers can log on to one computer and use the resources on other computers in the network as long as they have appropriate privileges to the resources.

Therefore, School Networks should be implemented using Windows 2000 domain network.

Notes

This document will focus and provide information on School Networks implemented using Windows 2000 domain network.

Hereafter the term "Windows 2000 School Network” would mean a School Network implemented using Windows 2000 domain network.

Guidelines

- Use domain as the network type for the Windows 2000 School Network.

- Consult contractors for further information if schools choose to implement their School Network other than domain type.

3.1.2 Active Directory

As introduced in the preceding section, Active Directory (AD) is the central database that contains system critical information for naming, describing, managing and locating resources on a Windows 2000 domain network. Resources include users, groups, files, applications, printers, servers, workstations, network services and security parameters etc.
Therefore, when deploying Windows 2000 to a School Network, AD plays a critical role that lets School Network administrators define and maintain the network infrastructure, control user administration, and perform system management.

The architecture of AD is built on domain, which defines the security boundary. At least one domain (i.e. the root domain) should be defined in a Windows 2000 domain network. A domain can be further broken down into Organizational Units (OUs) that contain users, groups, computers and network resources like shared folders and printers. Additional domain(s) can be joined together to form a hierarchical structure called tree. Multiple trees can be joined together to form a forest.

The following provides brief information on AD and its related components.

- **Active Directory**
  
  AD is the central database that contains system critical information for naming, describing, managing and locating resources on a Windows 2000 domain network. In addition, AD arranges domains in a hierarchical, tree-like structure and sets up the relationships among all the domains in the tree.

- **Organizational Unit**
  
  An OU is a container for organizing objects (e.g. users, groups, computers and network resources like shared folders and printers) within a domain into logical administrative subgroups. You can think of an OU as a directory in a file system and think of the OU's users and resources as files within the directory. An OU can contain other OUs (nesting).

  OUs are easier to create, delete, move, and modify than domains. In addition, OUs are better suited to the delegation role. For instance, School Network administrators can assign a teacher (e.g. class-master of 4A class) administrative rights for one OU's accounts and resources (e.g. the OU containing all 4A class' student accounts and their resources). Then the teacher himself/herself will have the authority to manage such accounts and resources.

  Moreover, OUs can be used for the deployment of policy-based management (with the use of Group Policy -- will be described later). A well-planned OU design will facilitate a streamlined administrative and group policy assignment. This is because objects placed in an OU inherit the rights and policies assigned to that OU.

- **Domain**
  
  A domain is a container of objects that shares security requirements, replication processes and administration.

  Domains can be joined by adding one or more child domains to an existing parent domain.

- **Tree**
A tree is a hierarchical arrangement of one or more domains within a single root name. Within a tree, a user who logs on in one domain can use resources in another domain, as long as the user has the appropriate permissions.

All domains in a tree must share a contiguous namespace, that is, the child domains must share the namespace of the parent domain.

- **Forest**

A forest is a collection of two or more Active Directory trees that do not share a contiguous namespace. They are organized as peers and connected by two-way, transitive trust relationships between the root domain of each tree.

- **Group Policy**

In general Group Policy (GP) is a set of policy settings to manage desktop settings, user data, applications and security policy over a group of users and computers.

For example, School Network administrators or teachers with delegated administrative privileges can use GP to limit students’ access to desktop settings, system files and applications. For instance, they can remove access to the "Display" and "System" Control Panel applet for students to prevent them from changing the system configuration and network settings of the computers.

GP resides in AD and can be applied to local computers, sites, domains and OUs. More information on the use of GP can be found in Chapter 4 "User Administration".

The following diagram shows the relationship between domain, tree, forest, OU as well as users and network resources.
AD design can be very complex because there are lots of things that have to be taken into account. It is not an easy task for very large organizations. However, in school environment, a **single domain** structure is generally adequate for managing all school users and network resources.

**Examples**

Single domain is the simplest domain structure and it is suitable for most school environments. The following figure illustrates a Windows 2000 School Network structured in single domain.

For more information about Windows 2000 Active Directory and Domains, see Appendix A "For More Information" and the following:

Active Directory Overview  

Active Directory Services and Windows 2000 Domains  
Guidelines

- Use **single domain** as the domain structure for the Windows 2000 School Network. In general, multiple domains, tree and forest are unlikely suitable in a School Network.

- Consult contractors to make use of OUs to design a workable hierarchical directory structure, according to the schools' respective environment.

3.1.3 Servers

A typical Windows 2000 domain network will have the following types of Windows 2000 Server:

- **Domain Controllers**

  As briefly explained in preceding sections, AD resides on computers that are configured as domain controllers (DCs). There must be at least one DC in a Windows 2000 domain network to authenticate user logons and provide AD services.

  Unlike NT 4.0, there are no Primary Domain Controller (PDC) and Backup Domain Controllers (BDCs) in Windows 2000. In Windows 2000 domain network, all DCs are considered equal partners that each of them stores and maintains a copy of AD. In addition, if there are multiple DCs then they will periodically replicate their AD information to each other.

- **Member Servers**

  A member server is a Windows 2000 Server participating in a Windows 2000 domain network and is not configured as a DC. A member server does not store AD information and cannot authenticate users. Usually, member servers are used as:

  - File and print server
  - Remote access server
  - Proxy server
  - Web server

Notes
In Windows 2000, member servers can be promoted to be domain controllers and vice versa.

Guidelines

- Ensure that there must be at least one school server running as a domain controller in a Windows 2000 School Network.
- Consider running two or more of the school servers as domain controllers for resilience purpose.

3.1.4 Client Computers

A user in a Windows 2000 domain network can use a Windows 2000 Professional client computer to gain access to his/her desktop environment and resources in a Windows 2000 Server. In addition, a Windows 2000 domain network also supports pre-Windows 2000 client computers such as NT 4.0 Workstation and Windows 9x.

For example, if there are Windows 98 and NT 4.0 Workstation computers in a Windows 2000 School Network, students logging on from Windows 98 and NT 4.0 Workstation clients can be authenticated by Windows 2000 DCs with full support for logon scripts and system policies.

However, as mentioned in Chapter 2 “Introduction to Windows 2000”, most of the Windows 2000's compelling features require Windows 2000 Professional and Server working together -- currently only Windows 2000 (both Professional and Server) can fully support AD and utilize Group Policy. That is, in a Windows 2000 School Network environment, only client computers running Windows 2000 Professional can take advantage of the above features.

Notes

Examples of compelling features that require Windows 2000 Professional and Server working together are policy-based user data and settings management, delegated administration, and automated software installation and maintenance. Chapter 4 "User Administration" will further discuss these features.

Guidelines

3.2 Network Communications

School servers, client computers and other network devices must meet the following requirements in order to communicate with each other:

- Using the same network protocol
- Being uniquely identified on the School Network

Each school server, client computer and network device has to be uniquely identified on the School Network before they can communicate with each other. This is just like sending a letter to your friend, you must know his/her address beforehand. Generally, there are two types of identifications in a network:

- By network address -- which are usually numbers to be read by computer systems
- By name -- which are usually meaningful terms to be read by human

For a Windows 2000 School Network, the names involved are domain name, computer name and device name. Developing a naming convention and a network addressing scheme for them can facilitate system administration and network management.

3.2.1 Network Protocols

A network protocol defines the rules for network communication. When two computers use the same protocol, they will be able to locate and understand the data sent by each other and thus communication is possible.

Windows 2000 supports many popular network protocols, such as:

- TCP/IP
- NetBEUI
- NWLink IPX/SPX
- AppleTalk

TCP/IP is the network protocol for Internet access. Windows 2000 uses TCP/IP as the default protocol for network communications. In fact, TCP/IP is a mandatory protocol that must be available in a Windows 2000 School Network implemented using Windows 2000 domain network with
Guidelines

- Use TCP/IP as the default network protocol.
- Use other network protocols only if required.

3.2.2 Network Addressing

To build a Windows 2000 School Network around TCP/IP, each computer and network device must be provided with an unique IP address, either a dynamic or automatically assigned address through software, or a static address assigned by the School Network administrator. Because IP addresses are numbers which are difficult to remember, it is necessary to provide users with names that are easier to use. The process of mapping such names to their corresponding IP addresses is called name resolution which can be accomplished by various methods.

In addition, to facilitate Schools in building up an IP address scheme which caters for network communications inside and outside the School Network, the Education Department has reserved a private IP address range for each school under the IT in Education project. With a private IP address range, each school can develop her own IP address scheme in order to build a Windows 2000 School Network with TCP/IP.

3.2.2.1 IP Address Range for Schools

An IP address is comprised of 4 decimal numbers. The 4 numbers are separated by periods and each number ranges from 0 to 255, e.g. 10.0.0.1 and 203.105.16.90.

The Education Department adopts the IP address range 10.0.0.0 to 10.255.255.255 for the IT in Education project. This IP address range is divided into several sub-ranges for different usage. The following table shows the details:

<table>
<thead>
<tr>
<th>Usage</th>
<th>IP Address Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved for common facilities of the ITED project (e.g. ITERC)</td>
<td>10.0.0.0 - 10.39.255.255</td>
</tr>
<tr>
<td>Reserved for schools</td>
<td></td>
</tr>
<tr>
<td>Primary schools</td>
<td>10.40.0.0 - 10.99.255.255</td>
</tr>
<tr>
<td>Secondary schools</td>
<td>10.100.0.0 - 10.179.255.255</td>
</tr>
<tr>
<td>Special schools</td>
<td>10.180.0.0 - 10.199.255.255</td>
</tr>
<tr>
<td>Reserved for future expansion</td>
<td>10.200.0.0 - 10.255.255.255</td>
</tr>
</tbody>
</table>
Schools are assigned with addresses starting from 10.40.0.0 to 10.199.255.255, each with 16 subnets (sub-networks). Each subnet can accommodate up to 254 network hosts and each school can have an address space of 254 * 16 = 4064 hosts. The following table shows examples on the address range assignment to schools:

<table>
<thead>
<tr>
<th>School number</th>
<th>Subnets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.40.0.z - 10.40.15.z</td>
</tr>
<tr>
<td>2</td>
<td>10.40.16.z - 10.40.31.z</td>
</tr>
<tr>
<td>3</td>
<td>10.40.32.z - 10.40.47.z</td>
</tr>
<tr>
<td>4</td>
<td>10.40.48.z - 10.40.63.z</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Guidelines

☐ Use the IP address range recommended by the Education Department.

3.2.2.2 DHCP

Generally, dynamic IP addresses are suitable for client computers while static IP addresses are suitable for school servers, printers and other network devices such as Ethernet switches and hubs.

A Dynamic Host Configuration Protocol (DHCP) server should be installed in a School Network for assigning unique IP addresses to client computers dynamically. The DHCP server must itself be assigned with a static IP address.

Examples

Scenario

School A has been allocated an IP address range by the Education Department which includes 16 subnets from 10.100.0.z - 10.100.15.z.

School A plans to design a Windows 2000 School Network with 3 servers, 80 client computers, 10 printers, 5 switches and 1 router (for accessing the Internet). The router also serves as the default gateway.

Since the address space of one subnet can accommodate all the network hosts and School A has no special requirement for dividing the network into multiple subnets. After working with School Network administrators, the designated contractor proposes to use the subnet 10.100.0.z and develops
the following IP address scheme and assignment for School A.

### IP Address Scheme

<table>
<thead>
<tr>
<th>Device Type</th>
<th>IP Address Range</th>
<th>Capacity</th>
<th>Assignment Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default gateway</td>
<td>10.100.0.1 - 10.100.0.5</td>
<td>5</td>
<td>Static</td>
</tr>
<tr>
<td>Network devices</td>
<td>10.100.0.6 - 10.100.0.20</td>
<td>15</td>
<td>Static</td>
</tr>
<tr>
<td>Servers</td>
<td>10.100.0.21 - 10.100.0.30</td>
<td>10</td>
<td>Static</td>
</tr>
<tr>
<td>Printers</td>
<td>10.100.0.31 - 10.100.0.60</td>
<td>30</td>
<td>Static</td>
</tr>
<tr>
<td>Clients</td>
<td>10.100.0.61 - 10.100.0.254</td>
<td>194</td>
<td>Dynamic</td>
</tr>
</tbody>
</table>

### Actual IP Address Assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>IP Address</th>
<th>Assignment Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>10.100.0.1</td>
<td>Static assignment through manual procedure</td>
</tr>
<tr>
<td>Backbone switch 1 in server room</td>
<td>10.100.0.6</td>
<td></td>
</tr>
<tr>
<td>Backbone switch 2 in server room</td>
<td>10.100.0.7</td>
<td></td>
</tr>
<tr>
<td>Switch in 3/F FLEC</td>
<td>10.100.0.8</td>
<td></td>
</tr>
<tr>
<td>Switch in 4/F FLEC</td>
<td>10.100.0.9</td>
<td></td>
</tr>
<tr>
<td>Switch in 5/F FLEC</td>
<td>10.100.0.10</td>
<td></td>
</tr>
<tr>
<td>Server 1 (also the DHCP server)</td>
<td>10.100.0.21</td>
<td></td>
</tr>
<tr>
<td>Server 2</td>
<td>10.100.0.22</td>
<td>Static assignment through address reservation in DHCP</td>
</tr>
<tr>
<td>Server 3</td>
<td>10.100.0.23</td>
<td></td>
</tr>
<tr>
<td>10 printers</td>
<td>10.100.0.31 - 10.100.0.40</td>
<td>Dynamic assignment through DHCP</td>
</tr>
<tr>
<td>80 client computers</td>
<td>10.100.0.61 - 10.100.0.140</td>
<td></td>
</tr>
</tbody>
</table>

### Guidelines

- Use static IP addresses for school servers, printers and network devices (e.g. Ethernet switches and hubs).
- Deploy the Windows 2000 DHCP service through the DHCP server for assigning IP addresses to client computers dynamically.
- Configure the DHCP server to cooperate with a Windows 2000 DNS server.
- Document the IP address scheme and the static IP addresses assigned for easier administration.
3.2.3 Naming Convention

A domain name must be uniquely assigned to each domain in a Windows 2000 School Network. In addition, each domain controller, server, client computer, printer as well as network device in the Windows 2000 School Network must also be uniquely named. School Network administrators should define a standard naming convention for naming all these objects in order to facilitate system administration and network management.

As mentioned, a DNS server must be installed and configured for AD in a Windows 2000 School Network. The DNS server cooperates with AD and provides name registration and resolution.

The DNS server uses the letters 'a' to 'z', numerals '0' to '9', and the dash character '-' for naming. It does not matter whether uppercase or lowercase letters are used as DNS names are not case-sensitive.

3.2.3.1 Domain Names

For each domain in a Windows 2000 domain network, a unique domain name must be assigned to it. Generally, single domain structure is suitable for most School Networks, so one domain name is adequate in identifying a typical Windows 2000 School Network.

Notes

The domain name of a Windows 2000 School Network is very important. There is no way to change the domain name once it is assigned to a Windows 2000 School Network. Therefore, special consideration should be taken when planning a domain name.

Additionally, it is recommended to append ".local" as suffix for the Windows 2000 School Network domain name for distinguishing inbound and outbound traffic from the Internet.

Examples

Using Registered Internet Domain Name with ".local" Suffix

School A has already registered an Internet domain name of "school-a.edu.hk" for hosting her school website for public access. For ease of reference and management, School A decides to use "school-a.local" as the domain name of her internal Windows 2000 School Network.
Using Short School Name

Schools may choose to use their short school names as the domain names:

- Chan Tai Man Primary School may use "ctm-pri.local" as the domain name for her Windows 2000 School Network.
- Chan Tai Man Secondary School may use "ctm-sec.local" as the domain name for her Windows 2000 School Network.
- Chan Siu Man College may use "csm.local" as the domain name for her Windows 2000 School Network.

Combining the SAMS ID with other information

One of the domain naming conventions is to use schools' SAMS ID with other information as illustrated in the table below:

<table>
<thead>
<tr>
<th>SSS</th>
<th>Meaning</th>
<th>Value</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>▲▲▲▲</td>
<td>Denoting the project this domain belongs to</td>
<td>ITED</td>
<td>Schools may have other Windows 2000 domains for other projects.</td>
</tr>
<tr>
<td>SSS</td>
<td>SAMS ID</td>
<td>A01 - Z99</td>
<td>Each school is assigned with a SAMS ID in the SAMS project.</td>
</tr>
</tbody>
</table>

School B has a SAMS ID "C36" and plans to deploy a Windows 2000 School Network with one single domain. After working with the designated contractors, the School Network administrator decides to use "itedc36.local" as the domain name for his/her Windows 2000 School Network.

Guidelines

- Take special consideration when planning the domain name for a Windows 2000 School Network. Consult contractors for further information and suggestions.
- Append ".local" as suffix for the Windows 2000 School Network domain name.
- Document the domain name(s) assigned for easier administration.
3.2.3.2 Computer and Device Names

Each domain controller, server, client computer, printer as well as network device must be assigned with a unique name. It is necessary to consider the following issues when developing naming convention for computers and devices:

- All computers and devices should be covered and assigned with a unique name.
- If a computer contains multiple platforms (e.g. multi-boot with Chinese Windows 2000 Professional and Chinese Windows 98), the computer name for each platform should be unique. Consider appending different suffix to the computer name of each platform, for example, "W2K" and "W98" for Windows 2000 Professional and Windows 98 respectively.
- If a computer contains platforms in different languages (e.g. multi-boot with English and Chinese Windows 2000 Professional), the computer name for each platform should also be unique. Consider appending different suffix to the computer name of each platform, for example, "E" and "C" for English and Chinese platforms respectively.

Examples

School A has a SAMS ID "C36" and plans to deploy 3 servers, 60 desktop computers, 20 notebook computers, 6 inkjet printers, 4 laser printers, 5 Ethernet switches and 1 router to its School Network.

Using Simple Names

School A may choose to use simple names for computers and network devices:

<table>
<thead>
<tr>
<th>Device</th>
<th>Quantity</th>
<th>Device Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>3</td>
<td>Server01, Server02,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server03</td>
</tr>
<tr>
<td>Desktop computers in computer lab</td>
<td>40</td>
<td>CL01, CL02, ...CL40</td>
</tr>
<tr>
<td>Desktop computers in class rooms</td>
<td>12</td>
<td>Rm401-01, Rm402-01,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>Desktop computers in library</td>
<td>8</td>
<td>Lib01, Lib02, ...Lib08</td>
</tr>
<tr>
<td>Notebook computers</td>
<td>20</td>
<td>NB01, NB02, ...NB20</td>
</tr>
<tr>
<td>Inkjet printers</td>
<td>6</td>
<td>Inkjet01, Inkjet02,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...Inkjet06</td>
</tr>
<tr>
<td>Laser printers</td>
<td>4</td>
<td>Laser01, Laser02,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...Laser04</td>
</tr>
<tr>
<td>Switches</td>
<td>5</td>
<td>Sw01, Sw02, ...Sw05</td>
</tr>
<tr>
<td>Router</td>
<td>1</td>
<td>Router01</td>
</tr>
</tbody>
</table>
Combining the SAMS ID, Device Type, and Serial Number to Form the Names

One of the naming conventions for computers and network devices is to use schools’ SAMS ID with other information as illustrated in the table below:
### Windows 2000 Technical Guidelines for School Network Implementation

#### IT in Education Project

**Network Infrastructure**

**January 2001**

45

---

<table>
<thead>
<tr>
<th>SSS A###%</th>
<th>Meaning</th>
<th>Value</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSS</td>
<td>SAMS ID</td>
<td>A01 - Z99</td>
<td>Each school is assigned with a SAMS ID in the SAMS project.</td>
</tr>
</tbody>
</table>

###

<table>
<thead>
<tr>
<th>Device type</th>
<th>Meaning</th>
<th>Value</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>D, N, S, P, L, X, Z</td>
<td>Device type</td>
<td>D for desktop computers</td>
<td>N for notebook computers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S for servers</td>
<td>P for printers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L for plotters</td>
<td>X for network devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Z for devices other than the above</td>
<td></td>
</tr>
</tbody>
</table>

###

<table>
<thead>
<tr>
<th>Serial number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>#3</td>
<td>001 - 009</td>
</tr>
<tr>
<td>Remark</td>
<td>This number is assigned sequentially.</td>
</tr>
</tbody>
</table>

####

<table>
<thead>
<tr>
<th>Language platform of computers (where ( \Delta = D, N, ) or S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C, E, null</td>
</tr>
<tr>
<td>C for Chinese</td>
</tr>
<tr>
<td>E for English</td>
</tr>
<tr>
<td>Null for others (e.g. multi-language)</td>
</tr>
</tbody>
</table>

####

<table>
<thead>
<tr>
<th>Printer type (where ( \Delta = P ))</th>
</tr>
</thead>
<tbody>
<tr>
<td>I, L, M</td>
</tr>
<tr>
<td>I for inkjet printers</td>
</tr>
<tr>
<td>L for laser printers</td>
</tr>
<tr>
<td>M for dot matrix printers</td>
</tr>
</tbody>
</table>

####

<table>
<thead>
<tr>
<th>Device type of network devices (where ( \Delta = X ))</th>
</tr>
</thead>
<tbody>
<tr>
<td>H, S, R</td>
</tr>
<tr>
<td>H for hubs</td>
</tr>
<tr>
<td>S for switches</td>
</tr>
<tr>
<td>R for routers</td>
</tr>
</tbody>
</table>

###

<table>
<thead>
<tr>
<th>Blank for plotter and other devices (where ( \Delta = L ) or Z)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blank</td>
</tr>
</tbody>
</table>

---

For School A with SAMS ID “C36”,

<table>
<thead>
<tr>
<th>Device</th>
<th>Quantity</th>
<th>Device Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers (Windows 2000 Server English version)</td>
<td>3</td>
<td>C36S001E, C36S002E, C36S003E</td>
</tr>
<tr>
<td>Desktop computers (Windows 2000 Professional Chinese version)</td>
<td>60</td>
<td>C36D001C, C36D002C, C36D003C</td>
</tr>
<tr>
<td>Notebook computers (Windows 2000 Professional English version)</td>
<td>20</td>
<td>C36N001E, C36N002E, C36N003E</td>
</tr>
<tr>
<td>Inkjet printers</td>
<td>6</td>
<td>C36P001I, C36P002I, C36P003I</td>
</tr>
<tr>
<td>Laser printers</td>
<td>4</td>
<td>C36P001L, C36P002L, C36P003L</td>
</tr>
<tr>
<td>Switches</td>
<td>5</td>
<td>C36X001S, C36X002S, C36X003S</td>
</tr>
<tr>
<td>Router</td>
<td>1</td>
<td>C36X001R</td>
</tr>
</tbody>
</table>
Guidelines

- Consult contractors in defining and adopting a naming convention for computers and devices for school's specific environment.

- Document the computer and network device names assigned for easier administration.

3.2.3.3 DNS

Domain Name System (DNS) provides name-to-address registration and resolution for TCP/IP client requests. Windows 2000 Professional and Server computers use DNS to find one another; to find DC to handle logons; and to find other network services and resources.

DNS is a must in a Windows 2000 domain network. Without DNS, AD cannot work. Therefore a DNS server must be installed and configured for AD in a Windows 2000 School Network.

For more information about setting up DNS for AD, see http://support.microsoft.com/support/kb/articles/Q237/6/75.ASP

Guidelines

- Deploy the Windows 2000 DNS service through the DNS server for name registration and resolution in a Windows 2000 School Network.

- Configure the DNS server to cooperate with the Windows 2000 DHCP server.

3.2.3.4 WINS

Windows Internet Name Server (WINS) provides backward compatibility for pre-Windows 2000 systems and services. WINS provides name-to-address registration and resolution for NetBIOS client requests.

Although it is likely that the importance of WINS will diminish, School Network administrators should work with contractors to determine whether WINS is required in order to ensure that pre-Windows 2000 client computers can perform naming registration and resolution properly.
Guidelines

- Deploy the Windows 2000 WINS service through the WINS server for supporting backward compatibility for pre-Windows 2000 systems and applications.
4 User Administration

Students and teachers must have their own identities, or user accounts, in order to access the resources in a Windows 2000 School Network. According to their roles in school, different users may have different access rights and different rules may need to be set for different groups of users and computers.

The following are some of the key issues for administering and managing a Windows 2000 School Network. This chapter discusses the first five issues and further information for the remaining issues will be provided in later chapters.

- Management tools in Windows 2000
- User accounts administration
- Grouping strategy
- User data and settings management
- Delegated administration
- Network resources management
- Security measures

For more information about administration of Windows 2000, see the following article:

Step-by-Step Guide to Managing the Active Directory
4.1 Management Tools in Windows 2000

In order to administer users and manage a Windows 2000 School Network, School Network administrators should have an administrative user account with special privilege and use the management tools in Windows 2000 to perform the necessary administrative tasks.

This section presents an overview of the Windows 2000 management tools.

4.1.1 Microsoft Management Console

Almost all Windows 2000 administrative tasks can be performed with the use of “Microsoft Management Console” (MMC). For example, School Network administrators can use the “Computer Management” MMC to view event logs, configure hard disks, as well as starting or stopping network services on local and remote Windows 2000 computers.

In addition, MMC can be customized by adding different tools (also called snap-ins). For example, School Network administrators can put “Active Directory Domains and Trusts” MMC snap-in, “Active Directory Sites and Services” MMC snap-in and “Active Directory Users and Computers” MMC snap-in together to form a customized MMC console to manage network and user related tasks.
For more information about MMC, see the following articles:

Microsoft Management Console: Overview

Step-by-Step Guide to Microsoft Management Console

4.1.2 Remote Management

School Network administrators may need to use their Windows 2000 computers to remotely manage and configure other networked Windows 2000 computers. In order to do this, School Network administrators have to install the “Windows 2000 Administration Tools” (lots of MMC snap-ins, such as “Active Directory Users and Computers”) included on the Windows 2000 Server CDs, and/or make use of the Remote Administration feature of Terminal Services in Windows 2000 Server.

For example, after the “Windows 2000 Administration Tools” is installed on the School Network administrators' Windows 2000 Professional computers in staff room, School Network administrators can their computers to remotely add or delete user accounts to the Windows 2000 school servers in server room.

Alternatively, by enabling the Terminal Services (in Remote Administration Mode) in the Windows 2000 school servers, School Network administrators
can use their computers with web browsers (e.g. Microsoft Internet Explorer) or Terminal Services Client software installed to remotely manage the school servers.

### 4.1.3 Scripting

Windows Script Host (WSH) is supported in Windows 2000 and scripting languages like VBScript and JavaScript can be used in Windows 2000 to execute advanced commands and programs. Scripts can run as part of a logon script. An example of the use of WSH is for School Network administrators to include VBScript or JavaScript code within a logon script to add customized functionality, from simple network drive and printer mappings, to files and shortcuts creation, or even advanced system configurations (e.g. create lots of user accounts, write entries to registry, update signature of anti-virus software etc.).

For more information about WSH, see the following article:

Windows Script Host: A Universal Scripting Host for Scripting Languages

---

**Guidelines**

- Work with contractors to customize management tools to facilitate the network management and system administration in School Network.
4.2 User Accounts Administration

Several types of user accounts are available in Windows 2000. This section is intended to introduce their characteristics and present an overview of the use of user accounts in a Windows 2000 School Network.

4.2.1 Domain and Local User Accounts

Generally a Windows 2000 domain network supports two types of user accounts. They are:

- **Domain User Accounts**
  
  Domain user accounts are created on Windows 2000 Domain Controller (DC) and stored in AD. They are used for logging on to a School Network from any networked Windows 2000 computers and accessing authorized network resources of the Windows 2000 domain network.

- **Local User Accounts**
  
  Local user accounts are created and stored locally in Windows 2000 Professional and/or Windows 2000 Server that acts as a member or workgroup server. They are used for logging on to the computer locally and accessing the resources associated with that computer only.

**Notes**

No local user account is available for Windows 2000 DCs. If a Windows 2000 member or workgroup server is promoted to a Windows DC then the original local user accounts will be disabled.

**Guidelines**

- Use domain user accounts for users of a Windows 2000 School Network.
- Use local user accounts for users of standalone Windows 2000 computers.
4.2.2 Use of User Accounts

Students and teachers must have a shared or individual user account in order to access the resources in a Windows 2000 School Network or standalone Windows 2000 computers.

- **Personal Use**

  When using accounts aimed for personal use, users may have an unique identity in the system so that they can have the flexibility of personalizing their own user and data settings. In addition, since each user has an individual identity, security permission of system resources can be customized for each user. Furthermore, user activities on the system will thus be traceable and accountable to the corresponding person.

- **Shared Use**

  When using accounts for shared use, different users will have the same identity in the system. For example, when students are attending a computer course, they may use a shared account so that all user and data settings as well as security permission defined for that shared account are equally applied to all students. However, it will be hard to trace the activities of the users as the user account is shared by many users.

### Guidelines

- Consider using personal domain user account for each user in a Windows 2000 School Network.
- Use shared domain user accounts for a group of users for specific uses.
- Use shared local user accounts for standalone Windows 2000 computers in order to reduce the administration efforts.

4.2.3 User Naming Convention

Regarding the manageability of the School Network, School Network administrators should work out a standard naming convention for user accounts. The name of each domain user account in a Windows 2000 School Network should be unique. Similarly, the name of each local user account in a Windows 2000 Professional and/or Windows 2000 member/workgroup server should also be unique.

One of the common user naming conventions is to combine the initials and the last name of the user. And when there is duplication a serial number is added as the suffix.
Besides, unique descriptor like Student Reference Number is also commonly used as user name.

Alternatively, school may consider using some simple words as user name so that younger students would feel easier to remember their user names. For example, "apple", "boy" or "girl".

**Notes**

_No Chinese Character in User Name_

_Chinese characters should not be used in user name since they may not work with all systems._

**Electronic Copy of User Names**

_For schools having an electronic copy of the list of users such as student names/IDs, they can make use of the list as an input for user account creation, thus reducing the administration effort._

**Examples**

_Comparing the Initials and the Last Name_

<table>
<thead>
<tr>
<th>User Name</th>
<th>Windows 2000 User Account Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albert M.S. Tse</td>
<td>Atse</td>
</tr>
<tr>
<td>Ann Y.H. Wong</td>
<td>Awong</td>
</tr>
<tr>
<td>Arthur Y.H. Tse</td>
<td>Atse1</td>
</tr>
<tr>
<td>Emil M.C. Kay</td>
<td>Ekay</td>
</tr>
<tr>
<td>David S.W. Mak</td>
<td>Dmak</td>
</tr>
<tr>
<td>Derek T.W. Lin</td>
<td>Dlin</td>
</tr>
<tr>
<td>Dick M.W. Lin</td>
<td>Dlin1</td>
</tr>
<tr>
<td>Mandy P.C. Lee</td>
<td>Mlee</td>
</tr>
<tr>
<td>Marcus M.S. Lee</td>
<td>Mlee1</td>
</tr>
<tr>
<td>Mardina P.K. Leung</td>
<td>Mleung</td>
</tr>
<tr>
<td>Martin S.F. Lee</td>
<td>Mlee2</td>
</tr>
<tr>
<td>Sam C.S. Ho</td>
<td>Sho</td>
</tr>
<tr>
<td>Sophie T.K. Chan</td>
<td>Schan</td>
</tr>
</tbody>
</table>
Using Unique Descriptor like Student ID

<table>
<thead>
<tr>
<th>User Name</th>
<th>Student ID</th>
<th>Windows Name</th>
<th>2000 User Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albert M.S. Tse</td>
<td>19970108</td>
<td>19970108</td>
<td></td>
</tr>
<tr>
<td>Ann Y.H. Wong</td>
<td>19980332</td>
<td>19980332</td>
<td></td>
</tr>
<tr>
<td>Arthur Y.H. Tse</td>
<td>20000187</td>
<td>20000187</td>
<td></td>
</tr>
<tr>
<td>Emil M.C. Kay</td>
<td>19970163</td>
<td>19970163</td>
<td></td>
</tr>
<tr>
<td>David S.W. Mak</td>
<td>19960872</td>
<td>19960872</td>
<td></td>
</tr>
<tr>
<td>Derek T.W. Lin</td>
<td>19970452</td>
<td>19970452</td>
<td></td>
</tr>
<tr>
<td>Dick M.W. Lin</td>
<td>19991018</td>
<td>19991018</td>
<td></td>
</tr>
<tr>
<td>Mandy P.C. Lee</td>
<td>n/a (teacher)</td>
<td>Mandylee</td>
<td></td>
</tr>
<tr>
<td>Marcus M.S. Lee</td>
<td>n/a (teacher)</td>
<td>Marcuslee</td>
<td></td>
</tr>
<tr>
<td>Mardina P.K. Leung</td>
<td>20002368</td>
<td>20002368</td>
<td></td>
</tr>
<tr>
<td>Martin S.F. Lee</td>
<td>20000453</td>
<td>20000453</td>
<td></td>
</tr>
<tr>
<td>Sam C.S. Ho</td>
<td>19980450</td>
<td>19980450</td>
<td></td>
</tr>
<tr>
<td>Sophie T.K. Chan</td>
<td>n/a (teacher)</td>
<td>Sophiechan</td>
<td></td>
</tr>
</tbody>
</table>

Using Simple Names

- Use "apple" as the name of the shared user account for all primary one students.
- Use "3A" as the name of the shared user account for all students of 3A class.

Guidelines

- Consult contractors to define a user naming convention according to school's respective environment.
- Do not use Chinese characters and special characters in user names.

4.2.4 User Profiles

In Windows 2000, each user account is associated with a user profile. Each user profile contains several user-specific settings for that user account such as desktop icons, wallpaper, "Start" menu, shortcuts to recently used documents, Microsoft Internet Explorer's "Favorites" etc. When a user logs on to a Windows 2000 system, the user profile associated
with his/her user account is retrieved and the settings saved in the last session will then be applied to the current session.

The following figures shows the structure of a user profile:

<table>
<thead>
<tr>
<th>Folder Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Data</td>
<td>Application-specific data, such as custom dictionary.</td>
</tr>
<tr>
<td>Cookies</td>
<td>Internet Explorer cookies.</td>
</tr>
<tr>
<td>Desktop</td>
<td>Desktop items, including files and shortcuts.</td>
</tr>
<tr>
<td>Favorites</td>
<td>Internet Explorer favorites.</td>
</tr>
<tr>
<td>Local Settings</td>
<td>Temporary files and per-user non-roaming application data.</td>
</tr>
<tr>
<td>My Documents</td>
<td>The new default location for any documents that the user creates. Applications should be written to save file here by default.</td>
</tr>
<tr>
<td>NetHood</td>
<td>Shortcuts to Network Neighborhood items.</td>
</tr>
<tr>
<td>PrintHood</td>
<td>Shortcuts to printer folder items.</td>
</tr>
<tr>
<td>Recent</td>
<td>Shortcuts to the most recently used documents.</td>
</tr>
<tr>
<td>Send To</td>
<td>Shortcuts to document storage locations and applications.</td>
</tr>
<tr>
<td>Start Menu</td>
<td>Shortcuts to program items.</td>
</tr>
<tr>
<td>Templates</td>
<td>Shortcuts to template items.</td>
</tr>
</tbody>
</table>

There are two types of user profiles in Windows 2000 and they are:

- **Roaming User Profiles**

    Roaming user profiles can be used in a Windows 2000 School Network. The roaming user profiles should be centrally placed in the school server so that whenever a user logs on to the School Network he/she will always gets his/her specific desktop environment and settings, no matter which Windows 2000 Professional computer he/she uses.
For example, when a student uses a Windows 2000 Professional computer and logs on to the School Network, if his/her user account is associated with a roaming user profile then the settings saved in the user profile (which is placed in the school server) will be applied to the Windows 2000 Professional computer for this session's use. And when he/she changes to use another Windows 2000 Professional computer and logs on with the same user account, since the user profile is placed in the school server, the same set of desktop environment and settings will be applied to that computer.

- **Local User Profiles**

Local user profiles can be used in a Windows 2000 School Network or standalone Windows 2000 computers. The local user profiles are placed in the computer locally and can be used for that computer only.

For example, in a Windows 2000 School Network, when a student uses a Windows 2000 Professional computer and logs on to the School Network, if his/her user account is associated with a local user profile then the settings saved in the user profile (which is placed in the local computer) will be applied to that Windows 2000 Professional computer only. And when he/she changes to use another Windows 2000 Professional computer and logs on with the same user account, since the user profile is stored in the computer locally, another set of desktop environment and settings saved in the user profile of that computer will be applied to that computer.

Another use of local user profile is for standalone Windows 2000 computers. Since standalone Windows 2000 computers are not connected to any School Network or server, only local user profiles can be used. This means that user-specific desktop environment and settings for user accounts in standalone computer A cannot be applied in standalone computer B, even if they have the same user account.

School Network administrators can allow users to personalize their user profile, or restrict them to change any setting. This kind of management is achieved through Windows 2000 Group Policy. More information about user profiles and Windows 2000 Group Policy will be covered in "User Data and Settings Management" section later in this chapter.

**Notes**

Special consideration should be taken when using both Chinese and English computer systems in a Windows 2000 School Network -- some user profile settings are not interchangeable.
Guidelines

☐ Work with contractors to determine the setting of user profiles according to school's respective environment.

☐ Use roaming user profile for personal and shared domain user accounts in a Windows 2000 School Network.

☐ Use local user profiles for personal and shared local user accounts in standalone computers.
4.3  Grouping Strategy

After logging on to the School Network with their user accounts, users can then enjoy all the network services and resources that are authorized to them. However, since there may be thousands of students and tens or hundreds of computers in a School Network, for easier management, user accounts and computers should be categorized into some logical units or groups and controlled with appropriate policies and permissions.

Notes

Users, shared resources as well as computers in a Windows 2000 School Network can be grouped and controlled by both Organizational Units (OUs) and groups in different ways. Similar to NT 4.0, groups are security principles that can be used to grant access permissions to resources. However, OUs are not security principles--they are administrative boundaries that are used for delegation of administration and group policy deployment.

4.3.1  Organizational Units

Within a Windows 2000 School Network, School Network administrators should design and use Organizational Units (OUs). As mentioned in previous chapters, OUs are containers that hold objects such as user accounts, groups, computers, shared folders and printers in the AD. School Network administrators should organize OUs into a logical structure that matches their schools' needs and circumstances.

Notes

The concept and the use of OUs are important in a Windows 2000 School Network as OUs are the places for applying policies to manage user data and settings, delegate administration and perform numerous administrative tasks. A well-planned OU design will facilitate a streamlined administrative and group policy assignment. This is because objects placed in an OU inherit the rights and policies assigned to that OU. Because OUs can be nested, rights and policies can be narrowed, broadened or "masked" as required down the hierarchy.

See later sections in this chapter for more information about OUs and policy-based management.
Examples

The following figure shows an example of the domain and OU structure of a basic Windows 2000 School Network.

4.3.2 Groups

It is much easier to manage groups than individual users. Groups in Windows 2000 give School Network administrators the ability to assign permissions and distribute information to collections of users.

A Windows 2000 domain network has three scopes for grouping user accounts and groups. They are:

- Global
- Domain Local
- Universal
<table>
<thead>
<tr>
<th>Group</th>
<th>Description / Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>◼ Organize user accounts</td>
</tr>
<tr>
<td></td>
<td>◼ Cannot contain Domain Local group</td>
</tr>
<tr>
<td></td>
<td>◼ Can be nested (i.e. contain other Global groups) when running in Native mode</td>
</tr>
<tr>
<td>Domain Local</td>
<td>◼ Similar to NT 4.0 Local groups</td>
</tr>
<tr>
<td></td>
<td>◼ Provide users with permissions to access network resources</td>
</tr>
<tr>
<td></td>
<td>◼ Can contain Global groups</td>
</tr>
<tr>
<td></td>
<td>◼ Cannot contain Domain Local group</td>
</tr>
<tr>
<td></td>
<td>◼ Can contain Universal groups when running in Native mode</td>
</tr>
<tr>
<td></td>
<td>◼ Several built-in Domain Local groups designed for assigning user rights</td>
</tr>
<tr>
<td>Universal</td>
<td>◼ Can only exist in native mode</td>
</tr>
<tr>
<td></td>
<td>◼ Is valid anywhere in the forest</td>
</tr>
<tr>
<td></td>
<td>◼ Organize user accounts</td>
</tr>
<tr>
<td></td>
<td>◼ Provide users with permissions to access network resources</td>
</tr>
<tr>
<td></td>
<td>◼ Can contain Global groups</td>
</tr>
<tr>
<td></td>
<td>◼ Can be nested (i.e. contain other Universal groups)</td>
</tr>
</tbody>
</table>

**Notes**

There are two operation modes in Windows 2000: Mixed and Native. Generally a Windows 2000 School Network runs in Mixed mode (this is the Windows 2000 default operation mode). So the following sections will focus on Global and Domain Local groups.

Description about Mixed and Native operation modes can be found in Appendix A "For More Information".

Although both Global and Domain Local groups can contain user accounts, it is more appropriate to use Global groups for grouping user accounts, then use Domain Local groups for grouping Global groups and finally assign user permissions on network resources (e.g. shared files and printers) to Domain Local groups.

In addition, several built-in Global and Domain Local groups are available in Windows 2000 Domain Controller, Server and Professional. For ease of user administration, School Network administrators should consider using them in user rights assignment.
### Windows 2000 Domain Controller

<table>
<thead>
<tr>
<th>Built-in Global Group</th>
<th>Group Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Domain Admins</td>
<td>Members can fully administer the domain</td>
</tr>
<tr>
<td></td>
<td>Domain Guests</td>
<td>All domain guests</td>
</tr>
<tr>
<td></td>
<td>Domain Users</td>
<td>All domain users</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Built-in Domain Local Group</th>
<th>Group Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Administrators</td>
<td>Members can fully administer the domain/computer</td>
</tr>
<tr>
<td></td>
<td>Account Operators</td>
<td>Members can administer domain user and group accounts</td>
</tr>
<tr>
<td></td>
<td>Server Operators</td>
<td>Members can administer domain servers</td>
</tr>
<tr>
<td></td>
<td>Print Operators</td>
<td>Members can administer domain printers</td>
</tr>
<tr>
<td></td>
<td>Backup Operators</td>
<td>Members can bypass file security to back up files</td>
</tr>
<tr>
<td></td>
<td>Users</td>
<td>Users can operate the computer, but cannot install programs or make potentially damaging changes to the system files and settings</td>
</tr>
<tr>
<td></td>
<td>Guests</td>
<td>Users are granted with minimal guest access privilege to the domain/computer</td>
</tr>
</tbody>
</table>

### Windows 2000 Member Server and Professional

<table>
<thead>
<tr>
<th>Built-in Domain Local Group</th>
<th>Group Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Administrators</td>
<td>Members can fully administer the computer</td>
</tr>
<tr>
<td></td>
<td>Backup Operators</td>
<td>Members can bypass file security to back up files</td>
</tr>
<tr>
<td></td>
<td>Power Users</td>
<td>Users can modify the computer and install programs</td>
</tr>
<tr>
<td></td>
<td>Users</td>
<td>Users can operate the computer, but cannot install programs or make potentially damaging changes to the system files and settings</td>
</tr>
<tr>
<td></td>
<td>Guests</td>
<td>Users are granted with minimal guest access privilege to the domain/computer</td>
</tr>
</tbody>
</table>
Notes

School Network administrators must have user account(s) with adequate privilege in order to administer and manage their Windows 2000 School Network. One of the solutions is to create separate user accounts for each School Network administrator and put these user accounts to the “Administrators” group. When performing network-related administrative tasks School Network administrators should use their own privileged user account. On the other hand, they should use a second, non-privileged user account (a general teacher user account) for activities other than School Network administration and management.

Examples

The following figure shows an example of the use of groups of a basic Windows 2000 School Network.

Guidelines

- Work with contractors to thoroughly plan and design the domain structure as well as the use of OUs and groups to best match the school’s respective environment and needs.
☐ Place groups and/or user accounts as well as computers under corresponding OUs.

☐ Consider using the built-in groups or following the strategy below for grouping user accounts and assigning user permission to network resources:

**A > G > DL < P**

1. Assign user accounts (A) to Global groups (G).
2. Assign Global groups (G) to Domain Local groups (DL).
3. Grant Permissions (P) to Domain Local groups.

☐ Create an individual user account for each of the School Network administrators and put these user accounts to the built-in “Administrators” group for administrative purpose.

☐ School Network administrators should use a non-privileged user account (e.g. a general teacher user account) for general School Network usage and activities (e.g. preparing teaching materials). They should only use the privileged user account when it is required to perform School Network related administrative and management tasks.
4.4 User Data and Settings Management

To reduce the time and cost for supporting a Windows 2000 School Network, School Network administrators can make use of the policy-based management feature, or Group Policy, in Windows 2000 to centrally manage user data and settings.

Windows 2000 Group Policy is the successor to the System Policy of NT 4.0. The following sections are intended to provide general information on Windows 2000 Group Policy and illustrate some scenarios of user data and settings management in different school environments.

4.4.1 User Settings Management

As mentioned in previous sections, each user account in Windows 2000 is associated with a user profile. Each user profile contains a number of user-specific settings for that user account such as desktop icons, wallpaper, "Start" menu, shortcuts to recently used documents, Microsoft Internet Explorer's "Favorites" etc.

School Network administrators can allow users to personalize their user profile, or restrict them to change any setting. For example, students can have their personalized "Favorites" menu in Microsoft Internet Explorer while they cannot change any desktop icons as well as other display settings such as wallpaper. Such kind of user settings management is achieved through by Windows 2000 Group Policy.

In order to have a better understanding on user settings management in Windows 2000, the sections below will briefly introduce the way of policy-based management in NT 4.0 environment, followed by Windows 2000 Group Policy.

4.4.1.1 In NT 4.0 School Network

NT 4.0 uses System Policies (i.e. "*.pol" files) to manage users or NT 4.0 computers on the domain. One of the use of System Policies is to control desktop environment and enforce system configuration settings. For instance, controlling the desktop computers in Computer Lab so that whenever students logging on they cannot modify system-critical settings such as Internet options and network settings in the Control Panel, nor change the wallpaper or screensaver of the computer.

System Policies (i.e. "NTConfig.pol") can be created and edited by using "System Policy Editor" (i.e. "poledit.exe") and should be placed in PDC’s Netlogon share for managing networked NT 4.0 computers.
4.4.1.2 In Windows 2000 School Network

Windows 2000 Group Policy can manage a wider variety of functions than NT 4.0 System Policy. In Windows 2000, School Network administrators can use Group Policies to define user and computer configurations for groups of users and computers. Group policy settings can be customized with the use of the “Group Policy” MMC snap-in. Customized group policy settings are stored in Group Policy Objects (GPOs), which are in turn stored in AD of the Windows 2000 domain controllers.

Numerous settings for controlling computers and users are available using Windows 2000 Group Policy. Computer-related policy settings are applied when the computer system is powered on and Windows 2000 is initialized. User-related policy settings are applied when the user logs on to the computer. When a conflict exists, computer settings will take precedence.

The following are some of the functions that School Network administrators can use Windows 2000 Group Policy to control user and computer settings:

- Control Panel and Desktop
- Disk quotas
- Folder Redirection
- Computer startup and shutdown scripts
- User logon and logoff scripts
- Network and Dial-up Connections
- Offline Files and Folders
- Printers
- Software installation
- Start Menu and Taskbar
- Task Scheduler
- Windows Components
- Account and Local Policies
- Event Logs
- System Services
- Registry
- File System
As mentioned in the previous chapter, Windows 2000 Group Policy can be applied to the following objects:

- Local computers (or called Local Group Policies)
- Sites
- Domains
- OUs

Certainly schools can have many Group Policies to manage their School Networks. The way Group Policies will be applied is that the system will take any Group Policies that exist on the local computer first, then it will take any policies that apply to the site, then any on the domain, then any on the OU. In addition, if there are multiple policies at each of those places, School Network administrators can prioritize these policies.

For easy administration, school should consider defining Group Policies at domain level (i.e. to globally manage all users and computers in the school) and OU level (i.e. to manage specific users or computers in such OU) only.

**Notes**

*Designing Active Directory with Group Policy in Mind*

The Group Policy settings which apply to a user or computer are based on the user's or computer's location within the AD structure. Group Policies process in the order of site, domain, and OU. For example, if a School Network administrator applies a Group Policy that removes the "Run" command from the "Start" menu at the site level, adds it at the domain level, and then removes it at the OU level, the "Run" option will disappear from the "Run" menu when a user logs on who is a member of the OU because that setting applies at the OU level, which is the last Group Policy that the system applies. If the school has a nested OU structure with Group Policies set at each OU level, the Group Policies process from parent to child, and the policy associated with the immediate parent OU that the user or computer object belongs to is the last one that the system applies.

*Inheritance of Group Policies*

Group Policies are used to control settings of computers and users (not groups) while can be applied at multiple levels (sites, domains, OUs) and multiple Group Policy Objects for each level. It may be that some policy settings conflict with each other. Active Directory Users and Computers snap-in provides options to force some policies to never be overridden (No Override) and/or allow some containers to not inherit settings from a parent container (Block Inheritance).
Placement of Group Policies

For easier management of a Windows 2000 School Network, School Network administrators should try to apply Group Policies to site, domain and OU levels as possible. For example, imagine that there are 80 desktop computers and all these computers are put in a "Desktop" OU. Instead of defining and applying local group policy settings to these 80 computers individually, School Network administrators can define one policy -- a set of settings for that one "Desktop" OU, and manage only one Group Policy for these 80 computers.

On the other hand, for standalone Windows 2000 computers, School Network administrators can use Local Group Policies to specify set of policies in order to manage these standalone Windows 2000 computers.

NT 4.0 System Policy vs. Windows 2000 Group Policy

Although Windows 2000 is compatible with NT 4.0 System Policy (i.e. "*.pol" files), in order to utilize the additional options and controls offered by Windows 2000, schools should consider using Windows 2000 Group Policy to their Windows 2000 computer, instead of using NT 4.0 System Policy.

In Mixed Windows 2000 and NT 4.0 School Network

Windows 2000 Group Policy needs AD and works only for Windows 2000 computers. This means that the defined Group Policies can only be applied to the Windows 2000 Server and Professional systems in a School Network. For example, if there is a School Network containing a Windows 2000 DC, Windows 2000 Professional and NT 4.0 Workstation, and a School Network administrator wants to centrally control all client computers with the Group Policies defined in the School Network’s AD. Since only Windows 2000 Professional computers can "understand" Group Policies, only these Windows 2000 Professional computers can be managed by the defined Group Policies.

On the other hand, since NT 4.0 Workstation computers do not "understand" Group Policies, therefore no control can be made to these NT 4.0 Workstation computers. Although a customized "NTConfig.pol" policy file can be placed to the Windows 2000 DC in order to manage these NT 4.0 Workstation computers, it might run into problems if both the Group and System Policies are enabled on the Windows 2000 School Network -- NT 4.0 System Policy may overwrite the Windows 2000 Group Policy. Therefore, thorough planning and testing are required for Group and System Policies co-existence.

Examples

Previously primary one students were not allowed to use the Windows 2000 School Network. Now they have to use the School Network and
there is a need to customize their desktop environment to limit the access to critical system settings. For instance, there should only be "My Computer", "Microsoft PowerPoint", "Microsoft Word", "Paint" and "Internet Explorer" icons shown on these students’ PC desktop, while the "Start" menu should not be accessible.

To simplify account administration, the School Network administrator creates a shared domain user account for all primary one students, named "apple". In addition, the School Network administrator also sets the "apple" user account to have a user profile pointed to the school server.

Afterwards, the School Network administrator uses a Windows 2000 client computer and logs on as "apple". The School Network administrator then customizes the desktop environment and retains only the desired icons. After customizing, the School Network administrator logs off and the system will automatically save the customized settings to the user profile.

In order to restrict all primary one students from system change and configuration, the School Network administrator creates an OU named "Primary 1" and then puts the "apple" user account into that "Primary 1" OU. Subsequently, the School Network administrator applies appropriate group policy settings to the "Primary 1" OU (e.g. disable "Start" menu and "Control Panel") so that whenever a primary one student uses "apple" user account to log on to the School Network they cannot make any further system change.

4.4.2 User Data Management

In school environment, teachers and students have to use different computers in different locations at different time. For example, a teacher uses a computer in staff room to prepare teaching materials and then uses a computer in classroom to conduct presentation to students; a student uses the computer equipment in Computer Lab to scan a picture during Art lesson and then uses a computer in library to retouch the picture after school hour. Therefore, there must be a convenient place for them to store and retrieve their personal data files. In a Windows 2000 School Network, this is usually a place on the school server’s hard disk and generally there are two ways to storing users’ personal data. They are:

- Home directory
- Folder redirection

4.4.2.1 Home Directory

Home directory is a place in a school server for storing a user’s personal data. Usually each personal domain user account has its own home directory. According to users’ need, School Network administrators should allocate sufficient disk space and assign appropriate access permission to the home directory of each user.
The following points are recommended for planning the scheme for home directory in School Network:

- Each user has its own home directory for storing personal data, instead of sharing a home directory among a group of users.
- The home directories are put on the file server for better management and easier backup and restoration.
- The home directory is mapped as a logical drive like U: for easier user access and management.

**Notes**

*More information about home directory and shared folders can be found in Chapter 5 "Resource Sharing".*

### 4.4.2.2 Folder Redirection

In a Windows 2000 School Network, in addition to user data and settings management, Windows 2000 Group Policy also facilitates administrative management of user data -- user data can follow the user, no matter where the user logs on.

This is a new feature in Windows 2000 called "Folder Redirection". With "Folder Redirection" feature enabled, Windows 2000 can store user data in Windows 2000 Server while making it appears as if it were stored locally on the user's Windows 2000 Professional.

It offers many advantages in a Windows 2000 School Network. For example, it allows moving teachers' Windows 2000 Professional computers' "My Documents" folders to the school server for central and easier backup. Moreover, teachers can access their "My Documents" folders from any Windows 2000 computer in the School Network.

Whenever a teacher saves a file to his/her "My Documents" folder, the file is actually saved on the school server. In addition, combining folder redirection with roaming profiles would help speed up log on and log off time because the contents of "My Documents" (and other redirected folders) are not copied along with the rest of the teacher’s user profile.
The following screenshot shows the structure of a user profile:

```
<table>
<thead>
<tr>
<th>Folder Name</th>
<th>Description</th>
<th>Roams with profile by default</th>
<th>Redirectable with Group Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Data</td>
<td>Application-specific data, such as a custom dictionary.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cookies</td>
<td>Internet Explorer cookies.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Desktop</td>
<td>Desktop items, including files and shortcuts.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Favorites</td>
<td>Internet Explorer favorites.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Local Settings</td>
<td>Temporary files and per-user non-roaming application data.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>My Documents</td>
<td>The new default location for any documents that the user creates. Applications should be written to save file here by default.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NetHood</td>
<td>Shortcuts to Network Neighborhood items.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>PrintHood</td>
<td>Shortcuts to printer folder items.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Recent</td>
<td>Shortcuts to the most recently used documents.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Send To</td>
<td>Shortcuts to document storage locations and applications.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Start Menu</td>
<td>Shortcuts to program items.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Templates</td>
<td>Shortcuts to template items.</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
```
Notes

"Folder Redirection" and "Offline Files and Folders"

"Folder Redirection" can optionally work with "Offline Files and Folders" for better support on notebook computers. See Chapter 5 "Resource Sharing" for information about "Offline Files and Folders".

"Folder Redirection" and "Local User Profiles"

Using folder redirection with a local user profile would only make user documents available from all networked Windows 2000 computers -- to have settings and configuration move with the users, it requires using roaming profiles.

Examples

All form four students have their own user account. There is a need to let them access their "My Documents" folders from any Windows 2000 Professional computers on the Windows 2000 School Network.

The School Network administrator creates an OU named "Form 4" and then puts all user accounts of form four students into that "Form 4" OU. Subsequently, the School Network administrator applies appropriate group policy settings to that OU that redirects the "My Documents" folders to the designated server folders. After that when the form four students use a Windows 2000 Professional computer and log on to the Windows 2000 School Network with their user accounts, their "My Documents" folders will be redirected to the corresponding server folders.

In case of mixed Windows 2000 and NT 4.0 environment, the School Network administrator should administer a home directory for each of these form four student user accounts to point to their corresponding redirected "My Documents" folders in the school server. After that when they log on to the School Network through Windows NT 4.0 workstation, their home directories will be mapped to their redirected "My Documents" folder in the server (e.g. as U: drive) so that they can still access the files saved with Windows 2000 Professional, or vice versa.

To sum up, the technologies that enable user settings management and user data management are similar -- both use Windows 2000 Group Policy. By utilizing Windows 2000 Group Policy, students and teachers are allowed to roam to any Windows 2000 Professional computer on a Windows 2000 School Network. They can access to their user-specific desktop settings, application data and documents. In addition, drive mapping for user data may not be required as users can directly access their data from redirected folders on school servers.
For more information about Windows 2000 Group Policy as well as user data and settings management, see the following articles:

Introduction to Windows 2000 Group Policy
(a series of relevant papers are listed in this article)

Step-by-Step Guide to User Data and User Settings

IntelliMirror Tips and Tricks

---

**Guidelines**

- Work closely with contractors to thoroughly formulate, plan and test the Group Policies, especially if the School Network is in a mixed Windows 2000 and NT 4.0 environment.
- Note that only Windows 2000 computers (including Professional and Server) support Group Policies. Windows NT 4.0 computers (including Workstation and Server) support only System Policies and do not execute Group Policies.
- Make use of Windows 2000 Group Policy to control and manage users and computers in a pure Windows 2000 network or in a mixed network in which no specific restriction is to be imposed on the NT 4.0 computers.
- For Windows 2000 School Network, apply Group Policies to domain and OU levels.
- For standalone Windows 2000 computers, apply Local Group Policies to these computers.
- Assign each personal domain user account an individual home directory for storing its personal data.
- Map the home directory as U: drive for each user for easier management.
- Allocate sufficient disk space for the home directory for each user. For example, initially assign 10MB and 50MB for each student and teacher respectively and then re-evaluate their need regularly.
- For "Folder Redirection", the best practice is that "Do not create the folders in advance – just let the system create folders for each user". This can make sure that permissions are set properly.
- Consider mapping users’ home directories to their redirected “My Documents” folders on the school server when users require using home directory and "My Documents" folder together.
4.5 Delegated Administration

School Network administrators may find it desirable if they are able to delegate administration to other users in the school. For example, class-masters may need the administration right to directly manage their own shared folders, create or delete user accounts of their classes.

Under NT 4.0 environment, in order to delegate administration, schools have to create multiple domains. For instance, granting permission to manage a group of network resources to a user or group of users without granting the permission to manage all users or network resources often requires creating an NT 4.0 resource domain. The resource domain functions as an administrative boundary.

In Windows 2000, AD provides similar functionality through OUs. School Network administrators can use OUs to logically organize AD and delegate administrative control of OUs to users or groups; grant administrative control to a subset or certain objects under the corresponding OU, without handing over administrative control of all objects in the school domain.

Guidelines

- Consider using delegated administration to improve the flexibility of School Network administration.
5 Resource Sharing

Typically, file and print sharing are the basic Windows 2000 services that virtually all users of a School Network require. For example, when a folder on a school server is shared, authorized users can make connections to the folder and access its files remotely from their client computers. In addition, when a printer is shared then users can print documents to the printer over the School Network.

To help School Network administrator formulate their requirements on resource sharing, the following sections will provide information about file and print sharing as well as their related services.
5.1 File Sharing

To formulate the requirements on file sharing, the first thing to do is to understand how data is stored and shared on a Windows 2000 School Network. This involves understanding the file system of both servers and client computers.

Besides, as each user will store data to the computers on the School Network, the volume of data that a user is allowed to store should be monitored and controlled.

Based on the above, this section will discuss the following:

- File System
- Data Sharing
- Disk Quotas
- File Encryption
- File Usage on Notebook Computers

5.1.1 File System

File system is used by an operating system to store data in computer's hard disk. File system provides controls on the storing and sharing of data.

Windows 2000 supports the following file systems:

- NTFS5 (commonly used in Windows 2000)
- NTFS4 (commonly used in Windows NT 4.0)
- FAT32 (commonly used in Windows 98)
- FAT (commonly used in MS-DOS, Windows 3.x and Windows 95)

**NTFSS** is the recommended file system since it supports more Windows 2000 features. The following are some of the features that NTFS5 offers:

- Active Directory (Windows 2000 DCs require NTFS5)
- File-level and directory-level security for local and network accesses
- Disk quotas
- File encryption (i.e. Encrypting File System)
Notes

Consideration on the compatibility issue of file system is required when using a multi-boot computer.

Information about multi-boot Windows 2000 computer can be found in Appendix A "For More Information".

Examples

For Servers

Two partitions are configured in a Windows 2000 server:

- C drive: NTFS5 (for system data and applications)
- D drive: NTFS5 (for user data)

For Client Computers with Windows 2000 Professional Only

- C drive: NTFS5

For Client Computers with Windows 2000 Professional and MS-DOS

- C drive: FAT (for MS-DOS)
- D drive: NTFS5 (for Windows 2000 Professional)

Guidelines

- Use NTFS5 as the file system for hard disk partitions of Windows 2000 servers and client computers.
- Take special consideration when using computers with multi-boot capability.

5.1.2 Data Sharing

An important use of servers on the School Network is for sharing data among teachers and students. One of the most common ways is to facilitate data sharing is to use shared folders.

Although the basic unit for data sharing is file, files cannot be directly shared out under Windows 2000. To share files over the School Network,
the files have to be put under a folder and then share the folder as the access point for the files through the School Network.

For example, when a folder is shared on the school server, students can make connections to that shared folder from their client computers and access the files under the shared folder as if the files are stored in their local computers. However, to gain access to the files, the students, for example, must have permissions to access the shared folders and the shared folders must be assigned with a unique share name.

- **Permissions**

There are two kinds of permission that may be set for a shared folder in Windows 2000. They are:

**NTFS Permissions**

- NTFS permissions can be set to control users’ access to any files and folders in NTFS volumes. School Network administrators can set NTFS permissions to control the users working at the computer containing the files and also the users accessing the shared folders over the School Network.

**Shared Folder Permissions**

- When folders are shared over the School Network, School Network administrators can set shared folder permissions to control users’ access to the shared folders over the School Network.

- Unlike NTFS permissions, shared folder permissions can only be applied to the entire shared folder, and not individual files or sub-folders in the shared folder. In addition, shared folder permissions do not restrict access by users who gain access to the computer where the folder is stored. Shared folder permissions apply only to users who connect to the folder over the network.

Shared folder permissions can operate in addition to NTFS permissions for controlling file accesses through a School Network. However, when both NTFS permissions and shared folder permissions are set for a shared folder, the administration effort would be doubled. Therefore it is recommended that only NTFS permissions be used to control users’ access on shared data both locally and through a School Network. Shared folder permissions should be left as default option.

- **Share Names**

When sharing a folder, a share name must be assigned to it. This name is used for network users to refer to the shared folder. A share name can be the same as the actual folder name, but it doesn't have to be. The share name must be unique on the same computer and for
facilitating user access, meaningful names should be used and appropriate descriptions should be added.

**Notes**

*Windows 2000 allows School Network administrators to have more precise control over users than NT 4.0.* Apart from the standard NTFS permissions in NT 4.0 such as Read, Write, Change, Full Control, there are 13 special access permissions in Windows 2000. This additional permission control allows School Network administrators to have more flexibility in delegating network administration tasks to specific users.

In addition, *Windows 2000 also has a new feature called NTFS permission inheritance.* On NTFS file systems, sub-folders, by default, inherit the permissions applied to their parent-folder. School Network administrators should be aware of this inheritance behavior when setting NTFS permission.

For more information about shared folders, see the following:

Administering Shared Folders

**Examples**

**Scenario 1**

A user has shared folder permission: "Read" on a shared folder with the name: "PublicData" on server A. When the user tries to access "PublicData" through the School Network, its access is denied. The School Network administrator finds that the user has NTFS file permission: "No Access" on "PublicData". After setting the NTFS permission to "Read", the user can now read the content of "PublicData".

Later this user takes up the responsibility of managing "PublicData" and so it should be assigned with "Full Control" permission on "PublicData". The School Network administrator has to reconfigure both NTFS permission and shared folder permission and thus duplicating the administration effort. For ease of management, the School Network administrator decides to set the shared folder permissions of all shared folders to its default value ("Full Control for Everyone") and controls users’ accesses through NTFS permissions only.

**Scenario 2**

Generally School Network users make connections to shared folders by assigning a drive letter on their client computers to the school server’s
shared folder. In Windows 2000, however, drive mapping may not be necessary.

The following examples illustrate how users make connections to folders on a server:

- **Home Directory**
  
  The School Network administrator of School A creates a home directory in the school server for all users as "D:\Home". Sub-folders with users’ name are created to store the data of the specific users.

  For instance, a student called Chan Tai Man has a user account named "TMChan" and his home directory on the school server is set to the path "D:\Home\TMChan". This specific folder is then shared as "TMChan" and "Change" NTFS permission is granted to him so that he can read, add and change file contents under his home directory.

  **Properties**
  
  Folder on School server: "D:\Home\TMChan"
  Share name: "TMChan"
  NTFS permission: "Change" permission for user account "TMChan"
  Shared folder permission: "Full Control" for "Everyone"

- **Folder Redirection**
  
  As mentioned in Chapter 4 "User Administration", School Network administrators can make use of the "Folder Redirection" feature in Windows 2000 to redirect the users' "My Documents" to a school server.

**Guidelines**

- Use NTFS permissions to specify which users and groups can gain access to files and folders, and what they can do with the contents of the files or folders.

- If possible, assign permissions to groups instead of user accounts to simplify access administration.

- Leave the shared folder permission of shared folders as default and control users' access to shared folders only through NTFS permissions.

- Assign a unique and meaningful share name and make appropriate description to each shared folder so that users can easily recognize and locate it.
5.1.3 Disk Quotas

Windows 2000 Server comes with disk quota system for controlling users’ storage. Disk quota can be set on a per-user per-volume basis. That is, the quotas are valid only for particular volumes. If a user stores files on several NTFS volumes, separate quotas on each volume can be configured to suit the needs.

With volume quotas, School Network administrators can set both a hard limit and a warning limit. For each of these, a system-event message can be generated when the limit is reached. Windows 2000’s built-in disk quota system cannot send a notification back to the user. If the individual user’s usage exceeds the predetermined quota limit, the user will not be able to log off the computer until the user reduces the size of his/her files.

Notes

Windows 2000 disk quota system can only work with NTFS volumes. Besides, once a user starts to use the volume with quota system enabled, he or she will be assigned a quota. However, anyone who had files on the volume before the feature was enabled will not get the quota applied.

Guidelines

- Consult contractors for further information and suggestion on the use of the disk quota system with respect to the school’s requirements. Consider using Windows 2000’s built-in disk quota system if possible.
- Develop a capacity planning on hard disk usage (especially for servers) and define the quota limit for different users with different requirements.
- Turn on disk quota feature and set the appropriate quota before putting the hard disk volume into production use.
- Regularly monitor the usage of hard disk (especially for servers) and revise the disk quota limit for users on a need basis.

5.1.4 File Encryption

Both Windows 2000 Professional and Server come with encrypting file system (EFS) for securing files. All files (and folders) created in a folder marked for encryption are automatically encrypted. Only the person who encrypts the files can open the encrypted files. This prevents unauthorized users from reading or changing the file content.
Notes

Copying an un-encrypted file into an encrypted folder will not change its state -- the file will remain un-encrypted. Only files created in the encrypted folders will be automatically encrypted.

Copying an encrypted file into an un-encrypted folder will not change its state -- the file remains encrypted. Encrypted files remain encrypted even when they are copied to another media (e.g. floppy disk).

It is recommended to use EFS on folders for personal use only. EFS on folders for shared use may cause unexpected behavior and incur additional support effort -- files originally for shared use may be encrypted by one user and as a result other users cannot read the content of the encrypted files, even though they are given adequate access permission.

For more information about EFS, see Chapter 6 "Security" and the following article:

Step-by-Step Guide to Encrypting File System (EFS)

Guidelines

- Consider using EFS for protecting sensitive data in a School Network.
- Encrypt folders, instead of individual files.
- Consider using EFS on folders for personal use only (e.g. home directory).

5.1.5 File Usage on Notebook Computers

Windows 2000 makes it easier for notebook users to take network-based files and folders offline. This "Offline Files and Folders" feature in Windows 2000 can help reduce the time for notebook computer users to synchronize the files between notebook computers and school servers. Offline Files and Folders feature in Windows 2000 Professional can work with NT 4.0 Server and Windows 2000 Server.
For teachers who use notebook computers to prepare teaching materials at home, they can make their network files that are stored on school server available to their notebook computers’ local hard drive by selecting “Make available offline” option in the shared folder’s properties. When teachers are at home and using the notebook computers offline, those files and folders made available offline appear in the same way as if they were still connected to the School Network. After they have edited the files at home and reconnect the notebook computers to the School Network, those updated files will then be automatically synchronized to the school server.

In addition to the default settings, teachers can use “Synchronization Manager” in Windows 2000 to customize the preference of data synchronization. They can set preferences for synchronizing at log off, connect, disconnect or idle modes. Furthermore, they can also schedule a synchronization or set one manually. Different preferences can be set for different folders or files.

Guidelines

- Consider using "Offline Files and Folders" feature for teachers using notebook computer.
- Be aware that if lots of files are modified during offline, the synchronization process will take considerable time.
5.2 Print Sharing

Generally, the following steps are involved in sharing a printer for network use and there should be some planning for each of these steps:

- **Connect the printer to the School Network**
  
  There are basically two methods for connecting a printer to the School Network:
  - through a network printer sharing device; or
  - by attaching to a networked computer, e.g. a server in the server room, or a client computer in the computer laboratory

  It is recommended to use the first method so that the shared printer may be placed wherever there is a data node of the School Network, without limited by the location of the computer it is attached to.

- **Assign a computer as the print server for serving the network printing**
  
  There should be a print server for handling the network printing activities of a shared printer. It is recommended to deploy the print server on a server which has stronger processing power than a client computer. Usually the file server will also server as the print server.

- **Share the printer and assign a share name to it**
  
  To share a printer, a unique share name has to be assigned to it. The naming convention for the computers and devices as discussed in "Network Infrastructure" chapter may be used. Besides the share name, information like location, purpose and printer model may also be added to the shared printers for illustration when located and viewed through the School Network.

  **Notes**

  *If the shared printer is to be used in some pre-Windows 2000 systems and/or applications such as MS-DOS, special consideration should be taken on the share name. Schools should consult contractors for the details.*

- **Grant appropriate permissions to users**
  
  By default, the permission for a shared printer allows the printing from all School Network users. Schools may have specific requirements on the usage of the each shared printer, for example, restricting some...
users from using a particular shared printer or assigning some users to manage the print jobs of the shared printers.

- **Add the shared printer to the users’ working environment**

Finally, a shared printer should be added to the users’ working environment in order for them to use it. The icon of the shared printers that a user is allowed to use should be found in the Printer Folder of the user’s desktop. The following figure shows a graphical overview of print sharing.

![Print Sharing Diagram](image_url)

**Examples**

School A planned to set up 6 shared printers, 2 for use by teachers in the staff room, 3 for use by both teachers and students in the computer room and 1 in library for public use. School A has only one server, installed as the DC and located in the server room.

Print sharing devices are used to connect the 6 shared printers to the School Network. Since there are only a small number of shared printers, school A adopts a simple convention for the share name of the printers: location code + "prt" + a serial number.

The server is assigned as the print server for all the shared printers. Printer type, location and purpose of the shared printers are added as the
descriptions. The following table shows the details.

<table>
<thead>
<tr>
<th>Shared Printers</th>
<th>Share Name</th>
<th>User Permissions</th>
<th>Icons on Users' Desktop</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>printer 1 in computer room</td>
<td>crprt1</td>
<td>students: Print teachers: Manage administrators: Full Control</td>
<td>students: Yes teachers: Yes administrators: Yes</td>
<td>HP LaserJet 6P in Computer Room (Rm. 202), mainly for students’ and teachers’ printing</td>
</tr>
<tr>
<td>printer 2 in computer room</td>
<td>crprt2</td>
<td>students: Print teachers: Manage administrators: Full Control</td>
<td>students: Yes teachers: Yes administrators: Yes</td>
<td>HP LaserJet 5 in Computer Room (Rm. 202), for both teachers’ and students’ printing</td>
</tr>
<tr>
<td>printer 3 in computer room</td>
<td>crprt3</td>
<td>students: Print teachers: Manage administrators: Full Control</td>
<td>students: Yes teachers: Yes administrators: Yes</td>
<td>HP inkjet 670c in Computer Room, for both teachers’ and students’ printing</td>
</tr>
<tr>
<td>printer 1 in staff room</td>
<td>stfprt1</td>
<td>students: No Access teachers: Manage administrators: Full Control</td>
<td>students: No teachers: Yes administrators: Yes</td>
<td>HP LaserJet 6P in Staff Room, for teachers’ printing only</td>
</tr>
<tr>
<td>printer 2 in staff room</td>
<td>stfprt2</td>
<td>students: No Access teachers: Manage administrators: Full Control</td>
<td>students: No teachers: Yes administrators: Yes</td>
<td>HP inkjet 670c in Staff Room, for teachers’ printing only</td>
</tr>
<tr>
<td>printer 1 in library</td>
<td>libprt1</td>
<td>students: Print teachers: Manage administrators: Full Control</td>
<td>students: Yes teachers: Yes administrators: Yes</td>
<td>HP LaserJet 6P in Library, for teachers’ and students printing inside the library</td>
</tr>
</tbody>
</table>

**Guidelines**

- Connect the shared printers to the network through network printer sharing devices (ensure the shopping list includes such items).
- Consider deploying the print server on a server computer, instead of a client computer.
- Assign a unique name to each shared printer.
- Add appropriate information for the shared printers for illustration when viewed through the School Network.
- Consult contractors for granting appropriate permissions to different groups of users.
- Add the shared printers to the working environment of the users who are permitted to use them.
6 Security

Schools must protect their School Network from data loss, machine failure as well as any attempt on unauthorized access. Therefore a well-developed security policy is important for a School Network.

School Network security involves both computer-related configurations and human procedures. The effort includes both routine procedures performed on an on-going basis and non-routine steps taken to prevent or recover from unexpected disasters. In this connection, the security policy should include, but is not limited to, the following major security issues:

- Physical Security
- Data Security
- Windows 2000 Security

Notes

Security procedures generally reduce the flexibility of user operations and increase the administration work. It is advised that School Network administrators should work with contractors and define their own security requirements and policy with respect to their school environments.

In addition, it should be stressed that education to users on security awareness would be more important than technology control in protecting the computer resources. Building and maintaining strong relationships between teachers, students, School Network administrators, and parents about the goals and responsibilities of computer use in school can bring about the highest level of network stability and security in the long term.

Guidelines

- Refer to the security guidelines provided in this document and the related ED circulars to determine the security requirements.
- Develop a security policy with respect to the school’s unique environment.
- Educate all users of the School Network about their responsibilities of computer use and network security. All users should follow the guidelines and procedures in the security policy.
6.1 Physical Security

Physical security is the first line of defense against intruders. It prevents direct access and intruders from circumventing network security. Server hardware and storage media such as school servers, backup tapes, recovery diskettes and original software packages should be protected from unauthorized access. Schools should define the school areas that are having different levels of physical security requirements.

In addition, unauthorized access can be protected at hardware level such as using BIOS password so that even when one can reach the machine, he/she may not be able to boot up the system and make configuration changes to the system.

Moreover, property marking should be properly painted to all hardware items. Inventory taking is also important to prevent physical loss. Missed parts and difference in configuration should be reported and investigated immediately.

Examples

School Network administrators outline the physical security policy of their Windows 2000 School Networks that include the following:

- Define the school areas having different levels of physical security. For example, "Public" areas like corridors for kiosk placement; "Private" areas like computer laboratory and library that need supervision and monitoring; and "Restricted" areas like server rooms that only authorized persons are permitted to access.

- The school servers should be kept in server room. The room should be locked and restricted to authorized persons only.

- Disable access to removable drives in the school servers.

- Backup tapes and System Recovery Kit should be stored in a data safe away from the server room.

- BIOS supervisor password should be enabled to prevent unauthorized persons to change system configuration. Consider requesting contractors to preset the BIOS supervisor password of computers and make known to the School Network administrators only.

- Property marking should be properly painted on all hardware items.

- Develop an inventory table and perform periodic check on hardware configuration, original software packages and number of data backup tapes.
Guidelines

- Consult contractors for developing a physical security policy that includes, but is not limited to, the following:
  - Security areas definition for controlling the access of computer equipment
  - School servers and backup media location and access control
  - List of authorized persons to access
  - BIOS password protection
  - Property marking
  - Periodic hardware and software inventory check
6.2 Data Security

In general, data security protects a School Network against loss of data. Some of the potential causes of data loss include:

- Destructive viruses
- Hard disk subsystem failure
- Power failure
- Systems software failure
- Accidental or malicious use of deletion or modification commands
- Natural disasters (fire, flood, and so on)

Computer virus intrusion would corrupt or even destroy data and should be prevented. On the other hand, data loss and network downtime caused by storage media failure or power failure can be prevented by Fault Tolerance Disk Systems and UPS. Lastly, in case of data loss or corruption for any reason, recover the data by means of backup and recovery process.

The following sections are intended to provide some guidelines to prevent data loss in school environment.

6.2.1 Data Classification

Data in a School Network, especially the files in school servers, should be classified into several levels of security. Proper access permission should be assigned to allow only authorized persons to access the data.

Examples

School Network administrators decide to classify the data stored in the school server into several classes. For examples, "Public" data like school calendar, school-bus timetable, activity schedule for all students' access; "Private" data like home directory of each user and cross reference documents between teachers; and "Restricted" data like examination papers that only authorized persons are permitted to access.

Guidelines

- Classify the data in the School Network into different levels of security.
6.2.2 Third Party Personnel Access

Sometimes the School Network may be accessed by third party personnel. Schools should be aware of that third party personnel should only be granted with appropriate access permissions and privileges on a need basis.

Guidelines

- Grant appropriate access permissions and privileges to third party personnel on a need basis.

6.2.3 Virus Protection

Computer viruses are programs or pieces of code that can cause system malfunctions and data loss. Generally, viruses are propagated via floppy diskettes or data transmitted through communication channels.

It is likely that users will unwittingly introduce a virus into the School Network by downloading files from the Internet, or by copying files from their home PC. Therefore one of the best ways to keep the School Network safe from viruses is by educating users.

Examples

After working with the designated contractor, School Network administrators outline an anti-virus policy for their Windows 2000 School Network. The policy includes the following:

- Acquire software from authorized agents only -- illegal copies of software are regarded as the most common source of viruses.
- Install memory-resident anti-virus program in all school servers and client computers for continuous virus monitoring.
- All installed software, programs or documents should be scanned with anti-virus program before they are loaded into the servers or client computers.
- All files from unknown sources such as Internet download or floppy disk should be scanned.

- Educate users about viruses and request them to report immediately if a virus is found. Let users realize how much damage a virus can inflict.

- Stop using the computer when it is suspected to be infected by a virus. Defect the virus as soon as possible.

- Regularly update the virus signature to the anti-virus program in all computers.

---

**Guidelines**

- Work with contractors to define and adopt an anti-virus policy to protect the computer systems in the School Network from virus intrusion.

---

### 6.2.4 Fault-tolerant Disk Systems

Redundant Array of Independent Disks (RAID) technology is the most commonly used method to improve performance and resistance to disk fault. Among all available levels, RAID-5 is the most popular one.

RAID-5 technology uses redundant parity information to facilitate error correction. All data information together with the parity information is spread across multiple disks in a process called striping, which requires n+1 disks to yield a usable disk space equivalent to n disks.

With the RAID system installed, failure of any one disk within the RAID stack can be recovered by replacing the damaged disk with a good one. Hardware RAID controller provides more features such as stand-by disk and online stack expansion.

For more information about fault-tolerant disk systems, see

Planning Fault Tolerance and Avoidance

---

**Guidelines**

- Use hardware RAID 5 solution for all types of servers (i.e. entry-level, standard-performance and high-performance servers) for high availability.
6.2.5 **Uninterruptible Power Supply**

An uninterruptible power supply (UPS) provides temporary power when the local power fails. Usually, all that needed from a UPS is sufficient power supply for shutting down the system in an orderly fashion by terminating processes and closing sessions.

**Examples**

School A has 1 server and 70 client computers in her School Network. There is a backbone switch in the server room for connecting all the floor level switches through optical fibers. The server is directly connected to the backbone switch.

School A plans to incorporate UPS for both the server and the backbone switch. The UPS can guarantee 10 minutes for the server and the backbone switch to shutdown. In case of power failure in the server room, there is still enough time for the server to shutdown in normal procedures and to send alert messages to the client computers in the School Network through the backbone switch.

**Guidelines**

- Incorporate UPS devices for school servers so that sufficient time is given for the servers to shut down during power failure.
- Ensure that the UPS guarantees minimum 10 minutes for the servers and any other connected equipment to perform a graceful shutdown before rolling out the School Network.
- Work closely with contractors to determine which server peripherals should be connected to the UPS, with considerations to the school’s respective environment.

6.2.6 **System Backup and Recovery**

In a School Network, in case data are corrupted or accidentally deleted, they can be completely restored if a proper data backup has been done.

Hence a proper system backup and recovery strategy should be developed. The strategy should define the rules and procedures to back up and
recover all critical data while it should be fully automatic with minimal administrator interaction.

Generally, data in school servers should be backed up regularly with backup utility and the backup tape should be stored in a safe place.

**Notes**

*While a backup is taking place, if a file is being used by another application, that file may not be backed up.*

*Besides, consider using the built-in backup utility in Windows 2000 Server if possible. Use third-party Windows 2000 compliant backup software only when the built-in backup utility is not applicable.*

**Examples**

After working with the designated contractor, School Network administrators outline a system backup and recovery strategy for their Windows 2000 School Network. The strategy includes the following:

- **Full Backup**
  
  Perform a full backup to all affected systems every time schools make a significant change to the hardware or software setup of the School Network.

  For Windows 2000 domain controllers, to prevent the loss of user account and security information, the backup should include "System State" (i.e. the Active Directory database). Meanwhile, the Emergency Repair Disk (ERD), which holds critical system information, should also be updated. All these must be done locally on the server.

- **Backup Policy**
  
  **For Client Computers**
  
  - The designated contractors should prepare "Workstation Recovery Kit" for reinstallation or recovery of client computers.

  **For Servers**
  
  - Use the built-in backup utility in Windows 2000.
  
  - Set backup process as a schedule task that automatically back up files at a preset time on each backup day (e.g. 11:45pm).
  
  - Perform backup when the least number of users are using the School Network. If many files are in use, the backup might not accurately reflect the School Network.
- Perform verify operation after every backup.
- Label tapes sequentially with date, the type of backup (normal, incremental, or differential) and complete information regarding tape contents.
- Keep a log book for backup schedule and tapes used. The backup log is helpful when restoring data.
- Store backup tapes in cool, humidity-controlled, and free of magnetic fields locations.
- Find an off-site location to store the monthly normal backup tapes. This can be in a vault or other place that can protect them against fire, water, theft, and other hazards.
- Leave client computer backups to individual users.
- Clean the tape device once a month.

### 19 Tapes-rotation Schedule

Rotating tapes used during backup is a common practice. One of the tape-rotation scheme is the 19 tapes-rotation schedule. This schedule uses the same 4 tapes Monday through Thursday for differential backups, and 3 tapes are used for weekly normal backups (performed each Friday). The remaining 12 tapes are used for monthly normal backups and are stored off-site.

<table>
<thead>
<tr>
<th>Week 1</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week 2</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week 3</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week 4</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Monthly off-site**

Differential

Normal
For more information about system backup and recovery, see

Windows 2000 Server Disaster Recovery Guidelines

Guidelines

- Work with contractors to develop a system backup and recovery strategy.
- Thoroughly test the backup and recovery procedures before putting into production environment.
- Assign the responsibilities of backup and restore to authorized persons only (e.g. School Network administrators).
- Customize the backup utility accordingly. System backup should be scheduled and initiated automatically.
- Consider performing a trial restoration periodically to verify that files were properly backed up.
6.3 Windows 2000 Security

School Network administrators should use the security controls and policies provided by Windows 2000 in order to safeguard and manage their School Network. This section will discuss some of the Windows 2000 security controls and policies and many of them involves both computer configurations and user procedures.

Notes

As mentioned in chapter 3 "User Administration", School Network administrators should not log on to Windows 2000 School Network as administrators to perform routine tasks such as preparing teaching materials and surfing the Internet for non system-related administrative purpose. Instead, they should use a second, non-privileged user account (e.g. a general teacher user account) for such kind of activities.

For more information, a number of useful articles regarding Windows 2000 security can be found at:

Exploring Security Services

Securing Windows 2000 Network Resources

6.3.1 Account and Password Policies

Setting up password is almost a must for network security. Passwords help ensure that unauthorized users cannot access resources in the system and network -- no matter they can reach the system locally or remotely.

Adopting strong password policy is one of the most effective ways to ensure system security. Apart from selecting a strong password, several of the Windows 2000 account and password policy settings such as "maximum password age", "minimum password length" and "account lockout duration" can be used to further safeguard the system.

Notes

Account policies such as password policy and account lockout policy can be set using various Windows 2000 tools (e.g. "Domain Controller Security", "Domain Security Policy" as well as "Local Security Policy"). Each tool is
intended to serve distinct purpose and policies set in different tools will have different effects to the School Network.

Examples

After working with the designated contractor, School Network administrators outline an account and password policy for their Windows 2000 School Network. The policy includes the following:

- **Account Policy**
  - Screen should lockout after 30 minutes of inactivity during computing sessions and users are required to re-enter their password after lockout.
  - Users should log off every time they leave their computer unattended.
  - The user name should be cleared in the logon dialog box after the user logged out.
  - Only authorized persons can locally log on to school servers.

- **Password Policy**
  - Password should be at least 8 characters in length.
  - Users should choose a password that can easily be remembered and yet is complex. For example, IhlaKcf8y (I have lived at Kwai Chung for 8 years).
  - Personal identification information such as user’s name should be prohibited from being used in passwords.
  - Passwords should be non-dictionary words.
  - Passwords should be treated as personal secret and never be written down or disclosed.

For more information about account and password policies, see the following article:

Default Access Control Settings

Protection of the Administrator Account in the Offline SAM
http://support.microsoft.com/support/kb/articles/q223/3/01.asp
Guidelines

- Work with contractors to define and adopt account and password policies with respect to the school's environment.

6.3.2 Control on System and Network Resources

The following are some of the security measures in Windows 2000 to control system and network resources.

6.3.2.1 Group and System Policies

As discussed in Chapter 4 "User Administration", group and system policies should be used for managing user data and settings. School Network administrators should reference the information there in order to facilitate and control user data and settings in a Windows 2000 School Network.

For more information about the use of policies on security, see:

Step-by-Step Guide to Configuring Enterprise Security Policies
eps.asp

Guidelines

- Work with contractors to define and adopt group and/or system policies on managing user data and settings.

6.3.2.2 Permissions

As discussed in Chapter 5 "Resource Sharing" and earlier sections, typically lots of files and folders as well as printers require sharing in a Windows 2000 School Network. School Network administrators should reference the information there in order to properly control users' access to the resources by setting appropriate permissions.

For more information about securing network resources, see:

Securing Network Resources
http://www.microsoft.com/technet/win2000/win2ksrv/technote/securnet.a
sp
Guidelines

- Work with contractors to define and adopt access permissions on network resources.
- Assign and grant only minimal data access rights to users.

6.3.2.3 Encrypting File System

As mentioned in Chapter 5 "Resource Sharing", users can use the EFS feature in Windows 2000 to encrypt files in NTFS volumes. Backups and copies of encrypted files will remain encrypted. Unauthorized persons cannot read the content even when they can physically access the encrypted files.

Windows 2000 provides an EFS recovery agent to recover encrypted files. By default, the domain Administrator account is the designated EFS recovery agent for a Windows 2000 School Network while the local Administrator account is the designated EFS recovery agent for standalone Windows 2000 computers. School Network administrators can designate other users as the recovery agents so that in case of crisis, the designated recovery agents can also recover the encrypted files.

Examples

Scenario

Both Teacher A and Teacher B have their own redirected "My Documents" folder in a Windows 2000 school server and their folders' access permissions are set for their own control only. Both teachers then choose to encrypt their folder with EFS.

Example 1

Teacher A wants to take the files under his "My Documents" folder home in order to continue his work. Since encrypted files remain encrypted even when they are copied to another media (e.g. floppy disk), teacher A requires decrypting his files before taking them home.

Example 2

Teacher B stores some useful files in his "My Documents" folder. Unfortunately, the user account of Teacher B is accidentally deleted. Although all files under his encrypted folder are still there, they cannot be
opened. His School Network administrator then uses the recovery agent to recover the encrypted folder and files.

For more information about EFS, see the following article:

Best Practices for Encrypting File System
http://support.microsoft.com/support/kb/articles/Q223/3/16.asp

Guidelines

- Work with contractors to define a policy on the use of EFS and its recovery procedure with respect to the school's environment.
- Encrypt folders, instead of individual files.
- Create separate user accounts and designate them as EFS recovery agents to manage data recovery.

6.3.3 Audit Policy and Logs

Generally Windows 2000 auditing system can be used for tracking events in user accounts and file system. Successful and/or failed events can be logged to track malicious activities and security violation.

School Network administrators can specify which events are to be logged into the “Security” event log. An audit entry will be written to the "Security" event log whenever the specific actions are performed. The audit entry shows the action performed, the user who performed it, and the date and time of the action. School Network administrators can audit both successful and failed attempts at actions to uncover the unauthorized actions.

School Network administrators can then use the "Event Viewer" tool to audit the entries generated. For example, they can audit the "Security" event log to see whether there are invalid logon attempts as well as events related to auditing on shared files and folders.

Examples

After working with the designated contractor, School Network administrators outline an audit policy for their Windows 2000 School Network. The policy includes the following:

- Audit failed attempts on “account logon” and “object access” events.
- Set the initial log file size to 5MB.
- Regularly audit the event logs.
- Ensure that only authorized individuals have access to audit files.
- Use the "Performance" tool to ensure that designated individuals (e.g. School Network administrators) receive alerts about security-related events such as excessive failed logon attempts.

**Guidelines**

- Work with contractors to define an audit policy with respect to the school's environment.
- Adopt the audit policy to keep track on the system events.
7 Extendibility

A Windows 2000 School Network may have connections to other networks or computers located inside or outside the school. Typical examples are teachers and students accessing the Internet from the School Network, and teachers accessing the School Network from their computers at home through telephone lines. All these are under the scope of extendibility of the School Network.

In this chapter, three common types of School Network extensions are discussed:

- Remote access
- Internet access
- Integration with existing systems
7.1 Remote Access

Windows 2000 provides the Routing and Remote Access Services (RRAS) for remote connections. For examples, School Network administrators on the remote computers can connect to the RRAS server on the School Network through telephone lines. They can then work as if they were directly connected to the School Network.

Schools should consider the following issues when designing remote access:

- Concurrent connections
- Accessible resources
- Security measures

For more information about connecting remote users to a Windows 2000 School Network, see the following article:

Connecting Remote Users to Your Network

7.1.1 Concurrent Connections

Each concurrent connection at the server side requires a modem and a telephone line while each remote computer also requires a set of modem and telephone line.

There are serial and/or USB ports on a school server for attaching modems but these ports may be occupied by other devices. If the number of concurrent remote connections required are more than the number of ports available, the multi-port WAN adapter may be installed on the server to provide more serial ports.

Schools should determine the number of concurrent remote connections and acquire all the necessary hardware devices.

Examples

In School A, 20 teachers have computers at home and may connect to the School Network at night and in holidays. Since not all the teachers will connect to the School Network remotely at the same time, after evaluating the computer usage pattern of the teachers, School A decides to set up 4 concurrent connections for the RRAS server.
In considering the hardware equipment list, School A needs to purchase a multi-port WAN adapter and 4 modems for the server as well as installing 4 telephone lines at the a location near to the server. Besides, the home computers of the teachers should also be equipped with a set of telephone line and modem, e.g. desktop PC with an internal/external modem or a notebook computer with a PC card modem.

**Guidelines**

- Determine on the number of concurrent connections for the remote access according to schools’ own requirements.
- Ensure that there are sufficient modems and telephone lines to support the planned number of concurrent connections on both the remote computers and the RRAS server.

### 7.1.2 Accessible Resources

There are two options for controlling the accessible resources for remote users: either the resources on the RRAS server itself or the whole School Network. In most school environments, remote users only need to access the shared folders and files in their school server. It is not common to remotely use shared printers or files on client computers.

**Examples**

**Scenario 1**

School A has one school server for serving both file sharing (shared folders) and remote access (RRAS) services. School A decides to restrict the access of remote users on that server only.

**Scenario 2**

School B has two school servers for file sharing service. One of these servers also serves as a RRAS server for remote connections. In order to allow remote users to access all shared folders in the two servers, School B decides to allow remote users to access the resources on both servers.

**Guidelines**
Determine the accessible resources for remote access with respect to schools' requirements.

Configure the appropriate settings in the RRAS server.

7.1.3 Security Measures

Schools should determine which users indeed have the need for remote access and grant the remote access permission only to such users. For users having remote access permission, the same Windows 2000 user accounts should be used for logging on to the School Network both locally (i.e. in the school) and remotely.

Schools may also restrict the locations from which the remote computers can access the School Network by using the "Call-back" feature. The RRAS server can be configured to call back a predetermined or user-specified telephone number for each connection initialized by the remote computers. Therefore only the remote computers at those specified locations can gain access to the School Network.

In addition, the activities of the remote users can also be traced through the Windows 2000 audit policy.

Examples

School A designs her School Network with the following security measures on remote connections:

- Grant remote access permission to selected teachers only (e.g. School Network administrators and teachers who frequently need to prepare electronic curriculum).
- Keep a list of the users who are granted with remote access permission.
- Use "Call-back" to a preset telephone number. That is, a number that cannot be specified by the caller so that only users from specific locations are permitted remote access to the School Network.
- Log remote access related activities.

Guidelines

- Grant remote access permission to users who actually need it.
☐ Keep a record of the users who are authorized to access the School Network remotely.

☐ Consider using the "Call-back" feature for tighter security.

☐ Log remote access activities so that School Network administrators can audit the events like failed logon attempts and the duration of remote connections.
7.2 Internet Access

Schools may have connection to the Internet through different types of communication services like telephone dial-up, leased lines and broadband lines. No matter which type of services is adopted, schools should consider the following issues regarding Internet access:

- Valid IP address range
- User accessibility to Internet resources
- Performance enhancement

Notes

The newly introduced Windows 2000 Internet Connection Sharing (ICS) service allows a Windows 2000 computer with Internet connectivity to share its Internet connection so that other networked computers can access the Internet through it. However, ICS service does not function correctly if DNS or DHCP service is also provided on the same computer. Schools should not run the ICS service on the DHCP or DNS server, nor in a School Network implemented in Windows 2000 Active Directory domain (Active Directory requires DNS).

For more information about ICS and connecting Windows 2000 School Network to the Internet, see Appendix A "For More Information" and the following article:

Connecting Your Network to the Internet

7.2.1 Valid IP Address Range

A School Network need a valid IP address range for Internet access. A valid IP address range for Internet access means that the IP address range used in a private network should not have conflict with the public Internet resources.

The IP address range recommended by the Education Department is a valid IP address range that is appropriate for internal private networks like a School Network to access the public Internet resources.
Ensure that the IP address range used in the School Network is a valid address range for Internet access.

Consult contractors on the readiness of Internet access if IP address range other than the recommended one is used.

7.2.2 User Accessibility to Internet Resources

Connecting the School Network to the Internet does not mean that the users can then access the Internet resources. There are different types of resources on the Internet and they can only be accessed with appropriate applications. For example, users need a web browser for accessing the World Wide Web (WWW), an email client program for sending and receiving messages, and a newsgroup reader program for viewing/posting messages. Schools should decide the types of Internet services to be used and ensure that corresponding applications are available to the users.

Besides, if a proxy server is installed for enhancing the performance of the Internet connection, the proxy server must also be configured to support the desired type of Internet services. Otherwise, the School Network may not be able to get access to the desired Internet resources even though there is an Internet connection. For some proxy server software, a proxy client program has to be installed on the client computers in order to enable the access to the Internet resources.

Notes

Advanced Features of a Proxy Server

In addition to content caching, proxy servers can act as an Internet filtering software that oversees Internet use and blocks access to inappropriate sites. It does this by comparing the requested site with its own list of rated sites. Furthermore, some proxy servers can also provide user access control features for schools to set detailed user and group permission lists for different Internet services.

Besides, proxy servers can log the services and accesses passing through them. The log entry shows the IP address of the client computer which the user requested Internet service, the date and time of the access, the type of the Internet service, and the URL of the accessed web site or the name of the accessed file.

Advanced Internet Security with a Multi-homed Proxy Server

Since it is impossible to know what sort of content a student or teacher will locate using Internet search engines, and impossible to guarantee that malicious hackers would not attempt an assault on the School Network,
Schools should develop an Internet security policy to protect their School Network from Internet attacks.

Before connecting a School Network to the Internet, it is important to develop a plan for keeping the two networks separate. Many hardware and/or software products can achieve this goal. Certainly a firewall is one of the solutions; or, schools can consider deploying a multi-homed proxy server. A multi-homed proxy server is a separate server machine with two network interface cards (a low-end server or a workstation with adequate resources can also be used) that does not serve as a Windows 2000 domain controller but acts as a gatekeeper that controls traffic between the Internet and the School Network. This multi-homed proxy server intercepts any internal Internet request and executes that request, sending the information back to the user. If an outside hacker attempts to access the School Network, this multi-homed proxy server intercepts the request and denies the hacker’s access.

Other Web Site Access Controls

Some web browsers such as Microsoft Internet Explorer support ratings standards such as Platform for Internet Content Selection (PICS), ratified by the World Wide Web Consortium (W3C). This ratings standard lets schools choose different levels of allowable language, nudity, sex, and violence. Therefore if there is no proxy server installed as a centralized Internet security center, schools should set appropriate ratings level to the web browser(s) of all Internet-ready computers so that inappropriate sites can be blocked. In addition, schools should regularly review and maintain the ratings level to suit their preference. However, this may cause additional administrative works.

Alternatively, many Internet Service Providers (ISPs) in Hong Kong provide content-filtering service customized for education-sector. Some of them would review and maintain their content filtering list daily. When evaluating ISPs for Internet services schools should take such service into account in order to filter inappropriate sites.

Guidelines

- Determine the types of Internet resources required for users.
- Ensure that the corresponding applications are available to users and client computers, and the associated network settings and controls are properly set.
- Ensure that the proxy server is configured to support the access to the desired Internet resources, if any.
7.2.3 Performance Enhancement

When a user accesses a web page on the Internet, the web page is actually transferred from the remote web server to the user’s local computer. Page size and location of the remote web server may affect the performance.

A proxy server can increase the efficiency in accessing certain type of data on the Internet, for example, web pages. The proxy server keeps a copy of the data the users have previously retrieved from the Internet (this is called "caching"). If the same piece of data is requested again, it can be obtained directly from the proxy server, instead of retrieving from the Internet site again. This can save users’ time in waiting for the data as well as reduces the network traffic to the Internet.

Guidelines

- Deploy a proxy server to cache web pages for improving the performance of Internet access through the School Network.
### 7.3 Integration with Existing Systems

The preceding chapters aim at helping schools to understand some of the Windows 2000 key features and facilitate schools to formulate their requirements for a typical Windows 2000 School Network design and implementation. For further information, Appendix C "Checklist for Deploying Windows 2000 to Form a New School Network" provides the basic steps for deploying a new Windows 2000 School Network.

Some schools may have already installed other non-Windows 2000 systems such as standalone NT 4.0 Workstation computers (i.e. ED1 and ED2), NT 4.0 School Network (i.e. ED3), as well as systems/networks not under the standard provision of ITED project (e.g. Linux and iMac). If they want to integrate Windows 2000 with the existing system(s), they should work with contractors to ensure that the systems/networks are interoperable with Windows 2000 and all required functions and services can be provided after the integration.

Issues about School Network integration will be discussed under the following scenarios:

- Adding NT 4.0 computers (i.e. ED1 and ED2) to a Windows 2000 School Network
- Adding Windows 2000 computers to an NT 4.0 School Network (i.e. ED3)
- Migrating from an NT 4.0 School Network to a Windows 2000 School Network

**Notes**

As mentioned in Chapter 2 "Introduction to Windows 2000", CALs for client computers must have the same or a later version number than the corresponding version number of the server software. Therefore, it is necessary to upgrade current NT 4.0 CALs to Windows 2000 CALs when upgrading NT 4.0 servers to Windows 2000.

For instance, for schools with NT 4.0 School Network implemented, if they plan to upgrade their existing NT 4.0 server(s) to Windows 2000 or add new Windows 2000 server(s), they need to upgrade their existing NT 4.0 CAL to Windows 2000 CAL for the existing client computers. In addition, for new client computers (e.g. NT 4.0 Workstation or Windows 2000 Professional), Windows 2000 CALs are also required.

**Examples**
School A has an existing system and intends to integrate their Windows 2000 School Network with its existing system. In order to have a smooth integration, School A and the designated contractor work closely to discuss every aspect of the integration, especially on the following areas:

- Network connectivity (e.g. network protocol and communication)
- User account administration and authentication (e.g. creation / modification / deletion of user accounts and log-on procedures)
- Resources like files and print sharing and authorization (e.g. resource management and permission assignment)
- File format and data interchange
- Security measures
- Internet access
- Licensing issues (e.g. network clients, applications)
- Hardware and software requirements, compatibility and availability
- Implementation plan
- Test plan
- Contingency plan
- System availability and impact during the integration
- System operation and network management after the integration

The designated contractor should also consider the school's unique environment and requirements in the integration proposal. To minimize the impact to teachers and students, School A requests to conduct the integration during a long school holiday. The contractor then performs the integration accordingly while School A monitors the contractor's work and tests the systems thoroughly. After all the designated contractor provides training on the administration and operation of the integrated systems/networks to School Network administrators and users.

**Guidelines**

- For any system/network integration, consult contractors for suggestions and further information with respect to school's specific needs and readiness.
- An integration plan must be developed. The integration plan should include, but is not limited to, the aspects discussed above.
- Make sure that the required functions and services can be provided after the integration.
7.3.1 Adding NT 4.0 Computers to a Windows 2000 School Network

Standalone NT 4.0 computers (i.e. ED1 and ED2) may not be equipped with the hardware and software for networking. For example, the computers may not be installed with a network adapter. Schools may consult contractors for the list of hardware and software necessary for connecting these standalone computers to the Windows 2000 School Network and update the hardware and software shopping lists accordingly.

NT 4.0 systems cannot tightly integrate with Windows 2000 network; by the time this document is written, only Windows 2000 Professional is tightly integrated with the Windows 2000 network. This means that Group Policy settings and a number of security controls by Windows 2000 cannot be applied to these NT 4.0 systems. For example, advanced features like user data and settings management as well as automated software distribution that are controlled by Windows 2000 Active Directory and Group Policies cannot be enjoyed by the NT 4.0 computers.

Examples

School A has a Windows 2000 School Network and several standalone NT 4.0 Workstation computers. These NT 4.0 computers do not have a network adapter. If School A decides to connect these NT 4.0 computers to the Windows 2000 School Network, it may need the following items for the integration:

- A network adapter for each of the NT 4.0 Workstation computers
- Corresponding hardware installation and software configuration for each NT 4.0 computer
- Additional Client Access License (CAL) for these NT 4.0 computers, under School A’s licensing mode for CAL

Guidelines

- Ensure the hardware and software items necessary for integrating those existing standalone NT 4.0 computers to the Windows 2000 School Network are included in the shopping list.
- Consult contractors for formulating the requirements on the aspects like user administration, resource sharing, security measures etc. for those systems that cannot be tightly integrated with the Windows 2000 School Network.
7.3.2 Adding Windows 2000 Computers to an NT 4.0 School Network

Schools may consider integrating Windows 2000 computers to their existing NT 4.0 School Network. For example, when acquiring new computers, schools may choose to use Windows 2000 instead of NT 4.0 because of Windows 2000’s advanced features.

Windows 2000 Server can be added to an NT 4.0 School Network as a member server. Schools can enjoy the benefit of the features of Windows 2000 Server such as Internet Connection Sharing (ICS), Internet Information Server (IIS) 5.0, Terminal Services etc.

Windows 2000 Professional can be added to an NT 4.0 School Network as a client computer. Schools can enjoy the benefit of the features of Windows 2000 Professional such as multi-language support, broader hardware support, enhanced file services etc.

For more information about the basic steps for adding Windows 2000 computers to an NT 4.0 School Network, see Appendix D "Checklist for Integrating Windows 2000 to an Existing NT 4.0 School Network" and the following article:

Windows 2000 Professional in a Windows NT Server 4.0 Environment  

Examples

Scenario 1

School A has an NT 4.0 domain network which is gradually running out of resources. School A plans to add one more member server into the network. Since the additional server will not be used as a domain controller, School A can choose Windows 2000 Server as the new member server. This also allows school the possibility to upgrade to Windows 2000 Active Directory later when required.

Scenario 2

School B finds that some features provided by Windows 2000 Server are very useful to their School Network. However, School B does not intend to convert its existing network infrastructure from NT 4.0 domain network...
into Windows 2000 Active Directory. School B decides to deploy a Windows 2000 Server and configure it as a member server.

**Guidelines**

- Determine the benefits gained by adding Windows 2000 Server and Professional to the existing NT 4.0 network.
- For adding Windows 2000 Server to an NT 4.0 School Network, configure the server as a member server.

### 7.3.3 Migrating an NT 4.0 School Network to a Windows 2000 Network

Some schools may find that the advanced Windows 2000 features like the policy-based user data and settings management as well as the automated software distribution are useful to their school environment. However, they also note that such features can only be utilized when both Windows 2000 Server and Professional working together (it requires Active Directory). Therefore, some of these schools may consider migrating their existing NT 4.0 School Network to Windows 2000 School Network.

One of the easiest ways to upgrade an NT 4.0 School Network to Windows 2000 School Network is to upgrade the Primary Domain Controller (PDC), then upgrades some or all of the Backup Domain Controllers (BDCs). Because this is an OS upgrade, rather than a fresh installation, the existing domain structure, users, or groups are maintained. From this point on, the Windows 2000 School Network will use Active Directory to store objects, but is backward compatible with NT 4.0 BDCs. As mentioned in Chapter 3 "Network Infrastructure", Windows 2000 is designed to support mixed environment that can contain Windows 9x, NT 4.0 and Windows 2000. However, if schools desire to take all advantages of Windows 2000 features, they have to subsequently upgrade BDCs, member servers and all client computers to Windows 2000.

However, every NT 4.0 School Network has its unique settings and configurations, and every school has its own requirements. Therefore the migration from NT 4.0 School Network to Windows 2000 School Network varies from one school to another. Although Windows 2000 is distributed with a series of upgrading tools for converting NT 4.0 domain into Windows 2000 Active directory, there are many issues that these schools should take into consideration before the migration.

Appendix E "Checklist for Migrating an Existing NT 4.0 School Network with Windows 2000" provides a checklist for migrating an existing NT 4.0 School Network to a Windows 2000 School Network. A migration plan together with a contingency plan must be developed to allow the network system to
restore back into its original status in case any fatal error occurs during the migration.

The migration plan should include:

- A safe upgrade method that can provide quick restoration
- Coexistence of Active Directory domain controller with NT 4.0 domain controller during the testing period
- Drop the Active directory domain controller and restore the NT 4.0 domain network in case of error
- Convert the NT 4.0 domain into Windows 2000 Active Directory domain controller after the successful upgrade

Examples

Scenario 1

School A has an NT 4.0 School Network with one domain controller (i.e. the PDC) and wishes to migrate into Windows 2000 Active Directory School Network. School A plans to order another server with more computing power together with the migration service.

The designated contractor installs and converts the new server as PDC and demotes the original server into BDC. Then the contractor upgrades the new server (i.e. the new PDC) into Windows 2000 domain controller.

The above steps allow School A to restore its old NT 4.0 School Network in case the newly deployed server cannot be successfully upgraded -- drop the upgrade process and promote the BDC back to PDC.

After the successful upgrade, the new Windows 2000 Server emulates as PDC; and it will coexist with the old NT 4.0 BDC under mixed mode. Upon the confirmation of the migration, School A may upgrade the BDC to Windows 2000 domain controller and optionally let all domain controller run under native mode.

Scenario 2

School B has an NT 4.0 School Network with two NT 4.0 domain controllers (i.e. one PDC and one BDC) and plans to migrate the School Network into Windows 2000 School Network. Before the migration, the designated contractor synchronizes all NT domain controllers and makes full backup of them. The BDC is then made offline for contingency recovery purpose. Afterwards, the PDC is used for the Windows 2000 upgrade.

In case fatal error occurs during the upgrade, the offline BDC can be made online and promoted to be PDC. Files on the original PDC can be restored from the backup tapes and the NT 4.0 School Network can be resumed.
back to its original status.

Guidelines

- Work closely with contractors on the migration and contingency issues.
- Develop a migration plan together with a contingency plan.
8 Appendix A
For More Information

This chapter provides additional and advanced technical information on Windows 2000. The intended readers for this chapter are the School Network administrators who are familiar with Windows 2000 and its related features.

Similar to the document's structure, the following areas are discussed:

- Windows 2000 Features
- Network Infrastructure
- User Administration
- Resource Sharing
- Security
- Extendibility

Windows 2000 Features

**Notebook Computer Support**

Windows 2000 provides a hibernate function that writes all the contents of physical memory to a hibernate file before turning the power off, thereby saving the system's state. This reduces the system boot-up time and facilitates teachers to conduct presentation during classes.

**Terminal Services**

Windows 2000 Server provides integrated terminal emulation services, called Microsoft Terminal Services. Terminal Services allow client devices to access Windows-based applications that run completely on a centralized server.

Pcs may act as thin or fat clients in a Windows 2000 School Network. At the hardware level, a thin client is a device that relies on a server for applications and data, and performs little or no application processing. A thin client (often called a terminal) requires relatively small amount of RAM and local disk storage capacity. A typical PC (also called a fat-client) usually has more RAM and a larger disk drive so that it can run application and process data locally.

With Terminal Services running on a Windows 2000 Server, all client application execution, data processing, and data storage occur on the
server. Application user interfaces and user desktops are transmitted over the network and displayed at the computers running terminal emulation software; while print streams, keyboard input, and mouse clicks are transmitted over the network from the computers to the server.

For example, in school environment, "old" workstations having relatively less computing power and system resources can be utilized as thin clients to "run" prevailing software applications. Teachers and students log on and see only their individual sessions, which are managed transparently by the server and are independent of any other client session.

**Multi-Language Version (MLV)**

Microsoft released a Multi-Language Version (MLV) of Windows 2000. Windows 2000 MLV allows users to change the language of the user interface, choosing from any one of 24 languages. For example, menus, help files and dialog boxes can be switched to for example: English, Traditional Chinese and Simplified Chinese. In addition, users can create, edit, and print documents in hundreds of different languages. Users can change the interface language by simply selecting Control Panel and then Regional Options. A drop-down box lists the languages available.

More information about MLV can be found at:

Multilingual Support in Windows 2000 Professional

Windows 2000 MultiLanguage version
http://www.microsoft.com/globaldev/faqs/multilang.asp

**Service Pack and Hotfixes**

Microsoft released the Windows 2000 Service Pack 1 (SP1) on July 31, 2000. Schools should keep their School Network current with the latest vendor service pack and hotfixes. However, keeping systems up to date can be time consuming, given the rate at which new exploits and corresponding fixes appear. To stay secure, schools are advised to request Technical Support Services (TSS) for deploying service packs and hotfixes.

**Network Infrastructure**

**Domain**

An Active Directory domain is a security boundary. Domains contain partitions of the directory database for a forest or a tree. The database contains information concerning users, groups, computers and resources. The partition database for a domain is stored on the domain controllers.
Organizational Unit (OU)

An organizational unit (OU) is a subunit of a domain that can be used to delegate authority. Like domains, OUs contain users and resources to which administrative permissions, such as "create user" or "change password," can be delegated. Unlike domains, OUs do not define a database partition.

Tree

A hierarchical grouping of Active Directory domains is known as a tree. Domains in a tree share two-way transitive trust relationships.

Forest

A forest is a group of domains that share configurations and schemas but not a common DNS root. All the root domains in a forest share a transitive trust relationship, making resources anywhere in the tree available to any user in the forest.

Global Catalog (GC)

The global catalog contains a partial copy of the Active Directory database for an entire forest or tree. This partial copy includes every object in the database and the information about each object that is generally of interest to the entire tree, such as logon name and e-mail address. The global catalog can be used to find additional properties of objects within a tree by LDAP referral.

Active Directory (AD)

An Active Directory service deployment is made up of one or more forests, where a forest has one or more domains. Creating the initial domain controller (DC) in a network creates the first domain in a forest -- a domain must have at least one domain controller. The first domain created is the root domain of the first forest. Additional domains in the same domain forest can be child domains or tree root domains. A domain immediately above another domain in the same domain tree is its parent.

Domains are used to accomplish network management goals, such as structuring the network, delimiting security, applying Group Policy, and replicating information.

Active Directory allows Windows 2000 domain controllers to function as peers, and clients can make updates to Active Directory on any Windows 2000 domain controller in the domain. This is a change from the read-write/read-only roles played by Windows NT Server Primary Domain Controller (PDC) and Backup Domain Controllers (BDCs). The Windows NT Server domain system supports single-master replication -- all changes must be made on the PDC.
Windows 2000 supports multi-master operation: all domain controllers of a
domain can receive changes made to objects, and can replicate those
changes to all other domain controllers in that domain. A domain is a
directory partition. By default, the first domain controller created in a
forest is a Global Catalog (GC) server, which is an index to the entire forest
of objects in the Active Directory and contains a full replica of all objects in
the directory for its domain and a partial replica of all the objects stored in
the directory of every other domain in the forest. When performing a
search in the Active Directory it checks the GC first and the GC will respond
very rapidly. If the requested attribute is not in the GC then the request
will be passed on to the Active Directory and the Active Directory will then
respond with the required information.

**Replicating AD information among DCs**

Replicating Active Directory information among domain controllers provides
benefits of information availability, fault tolerance, load balancing, and
performance.

If there is one domain controller in a Windows 2000 School Network then
no replication is needed. If there are two domain controllers then
replication is needed between them.

Under NT 4.0, it supports single-master replication – all changes must be
made on the PDC. On the other hand, BDCs could actually respond to and
authenticate users, allow them to log on, but no changes could be made to
the accounts database, because those changes can only be made to the
PDC.

With Windows 2000, the domain controllers of a domain are considered
equal partners. They are known as Multi-Master Domain Controllers and
can perform multi-master replications. Therefore if there are three
domain controllers in the School Network and two of them for some reason
fail, changes can still be made to the active one. And when the other two
come back, all of the information, all of the updates from the single domain
controller that is left will then be replicated to those two "revived"
controllers.

**Sites**

Directory data can be replicated both within and among sites. Active
Directory replicates information within a site more frequently than across
sites, which means that the best-connected domain controllers receive
updates first. The domain controllers in other sites receive all changes to
the directory, but less frequently, thus reducing network bandwidth
consumption.

A site is delimited by an IP subnet, and is usually geographically bounded.
A site is separate in concept from Windows 2000 based domains. A site
can span multiple domains, and a domain can span multiple sites. Sites
are not part of the domain namespace. Sites control replication of domain
information and help to determine resource proximity. For example, a
workstation will select a DC within its site for authentication.

**Flexible Single Master Operation (FSMO)**

AD defines five Flexible Single Master Operation (FSMO) roles and they are:

- Schema master
- Domain naming master
- RID master
- PDC emulator
- Infrastructure master

The root of the forest is an essential component in maintaining the state of all the trees in the forest. Central to the state of the forest is the maintenance of the FSMO roles contained on servers in the forest root. The root of the forest maintains two special FSMO roles, Schema Master and Domain Naming Master. The Schema Master holds the master copy of all schema in the forest. The Domain Naming Master holds the master copy of the names of all domains in the forest.

In addition to these two forest FSMO roles, there are three FSMO roles per domain in the forest: RID Master, PDC Emulator, and Infrastructure Master. These FSMOs will reside in various domain controllers as needed. FSMO roles process updates in a single master fashion in case a conflict arises in the multi-mastered model.

The RID master FSMO role holder is responsible for processing RID Pool requests from other domain controllers. It also handles any moving of objects from one domain to another. The PDC Emulator FSMO role holder is a Windows 2000 domain controller that advertises itself as the primary domain controller (PDC) to serve network clients that do not have Active Directory client software installed (e.g. NT 4.0 Workstation and member servers), and to replicate directory changes to any NT 4.0 BDCs. As down-level clients and servers are upgraded to Windows 2000, the PDC Emulator FSMO will no longer be used. The infrastructure FSMO role holder is the domain controller responsible for updating an object’s Security Identifier (SID) and distinguished name in a cross-domain object reference.

Windows 2000 performs initial placement of FSMO roles on DCs. When a school creates its first Windows 2000 DC of its School Network (i.e. the first domain of a new forest), the system assigns all five roles (i.e. schema master, domain naming master, RID master, PDC emulator and infrastructure master) to that DC. When that school subsequently creates its first Windows 2000 DC of a new domain (e.g. new domain tree, child domain) in that School Network (i.e. the same forest), the system assigns all three roles (i.e. RID master, PDC emulator and infrastructure master) to it.
However, if a school has many Windows 2000 DCs then the default placement may not best fit the School Network.

For more information about network infrastructure planning and design as well as FSMO, see the following articles:

Promoting and Demoting Domain Controller to Member Server in Windows 2000
http://support.microsoft.com/support/kb/articles/q238/3/69.asp

FSMO Placement and Optimization on Windows 2000 Domain Controllers
http://support.microsoft.com/support/kb/articles/Q223/3/46.asp

**Mixed and Native Modes**

There are two operation modes in Windows 2000: Mixed and Native modes.

After a Windows 2000 School Network is initially up, it runs in mixed mode by default. Schools have the option to convert such a network from mixed mode to native mode. This can be a critical decision with major implications as it is a one-way conversion, i.e. there is no way back.

The mixed mode provides schools the functionality that lets the existing NT 4.0 BDCs (if any) offer domain services. After upgrading all NT 4.0 BDCs to Windows 2000 and switching from mixed mode to native mode, the School Network does not support NT BDCs anymore. It means that the school can only have Windows 2000 DCs. However, the school can have NT 4.0 Workstations and member servers in the School Network.

If the School Network consists of NT 40 domains, schools will need to upgrade all of the NT 4.0 domain controllers to Windows 2000 before changing them to native mode. If the School Network consists only of Windows 2000 domains, schools can change to native mode at any time.

The primary reasons for moving a domain to native mode include:

- Native mode domains can use universal groups and group nesting
- Inter-site directory replication can be faster

During the switch over, the following occurs:

- "Netlogon” synchronization is switched off, and schools can no longer add NT 4.0 BDCs to the domain.
- The domain uses only Active Directory multiple-master replication between domain controllers.
- All domain controllers can now perform directory updates.
- Windows 2000 designates the role of primary domain controller (PDC) emulator to the former NT 4.0 PDC. All pre-Windows 2000 clients use
the PDC emulator to locate the PDC and perform password changes. In addition, Windows NT resource domains use the PDC location information to establish trusts.

- Group nesting and Windows 2000 group types, such as universal and domain local groups, become available.

**DHCP**

In a Windows 2000 School Network, a DHCP server must be authorized by AD before it can start handing out IP addresses. In addition, the DHCP server should perform dynamic client registration with DNS on behalf of DHCP client computers. For DHCP settings, schools are recommended to enable the options of "Automatically update DHCP client information in DNS" and "Enable updates for DNS clients that do not support update".

**User Administration**

**Universal Groups**

Universal groups are newly introduced in Windows 2000 domain network. A Universal group is a security or distribution group that can be used anywhere in the domain tree or forest. A Universal group can have members from any Windows 2000 domain in the domain tree or forest. It can also include other Universal groups, Global groups, and accounts from any domain in the domain tree or forest. Rights and permissions must be assigned on a per-domain basis, but can be assigned at any domain in the domain tree or forest. Universal groups can be members of Domain Local groups and other Universal groups but cannot be members of Global groups. Universal groups appear in the global catalog and should contain primarily global groups.

Universal groups are only available when the Windows 2000 School Network is running in native mode.

**Schema Administrators Group**

The Schema Administrators group is newly introduced in Windows 2000 domain network. Members in Schema Administrators group can modify the schema, i.e. the description of the object class in the Active Directory and what attributes the object must have. Schema Administrators group is located in the root domain and appears as a Global group when running in mixed mode, while as a Universal group when running in native mode.

**Enterprise Administrators Group**

The Enterprise Administrators group is newly introduced in Windows 2000 domain network. Members in Enterprise Administrators group are very powerful and have administrative authority everywhere in the forest (network). Enterprise Administrators group is located in the root domain.
and appears as a Global group when running in mixed mode, while as a Universal group when running in native mode.

**Group and System Policies in a Mixed Windows 2000 and NT 4.0 Environment**

Upgrading NT 4.0 to Windows 2000 requires special considerations if NT 4.0 System Policy is already in use.

For schools planning migration to Windows 2000, one of the solutions for Group and System Policies co-existence is that schools may consider applying only System Policies for both NT and Windows 2000 clients until all clients are migrated to Windows 2000.

**Group Policy Refresh**

By default Windows 2000 Domain Controllers refresh Group Policies to other Windows 2000 Domain Controllers on 5-minute intervals. Non-DC Windows 2000 computers are refreshed every 90 minutes. The following commands can be optionally used to immediately impose Group Policy object settings upon a target computer:

- For computer configuration settings

  SECEDIT /REFRESHPOLICY MACHINE_POLICY /ENFORCE

- For user configuration settings

  SECEDIT /REFRESHPOLICY USER_POLICY /ENFORCE

**Default User Profile Locations**

The default locations for the user profile in NT 4.0 have been changed for Windows 2000. In order to enhance the security, the profiles are moved out of the system folder. The location of the user's profile depends on the operating system that was in place previously, the following table shows the possible locations:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Location of user profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000 New installation (no previous operating system)</td>
<td>%SYSTEMDRIVE%\Documents and Settings for example, C:\Documents and Settings</td>
</tr>
<tr>
<td>Windows 2000 upgrade of NT 4.0</td>
<td>%SYSTEMROOT%\Profiles for example, C:\WinNT\Profiles</td>
</tr>
</tbody>
</table>

**Resource Sharing**

**Multi-boot Windows 2000 Systems**
For multi-boot Windows 2000 computers, if the computers are on a Windows 2000 or NT 4.0 domain, each installation of the operating system on those computers must have a different computer name. In addition, each installation of the operating system must be in different partitions.

- **Multi-booting Windows 2000 and MS-DOS**
  - The primary partition must be formatted as FAT.
  - Windows 2000 must be installed last. Otherwise important files needed for starting Windows 2000 could be overwritten.

- **Multi-booting Windows 2000 and Windows 95**
  - The primary partition must be formatted as FAT. (For Windows 95 OSR2, the primary partition must be formatted as FAT or FAT32).
  - Compressed DriveSpace or DoubleSpace volumes won’t be available while running Windows 2000.
  - Windows 2000 must be installed last. Otherwise important files needed for starting Windows 2000 could be overwritten.

- **Multi-booting Windows 2000 and Windows 98**
  - The primary partition must be formatted as FAT or FAT32.
  - Compressed DriveSpace or DoubleSpace volumes won’t be available while running Windows 2000.
  - Windows 2000 must be installed last. Otherwise important files needed for starting Windows 2000 could be overwritten.

- **Multi-booting Windows 2000 and NT 4.0**
  - Windows 2000 can only work with NTFS version 5 (NTFS5). If schools are planning to install Windows 2000 on an NT 4.0 system that uses NTFS4 volumes, they should be aware that Windows 2000 will automatically convert all NTFS4 volumes to NTFS5. This conversion happens automatically during installation, and Windows 2000 provides no opportunity to confirm or decline this action. However, NT 4.0 can only work with NTFS5 if NT 4.0 Service Pack 4 (SP4) or later is installed. Therefore, for multi-booting NT 4.0 with Windows 2000, SP4 or later must be applied to the NT 4.0 system before installing Windows 2000.
  - This NTFS update enables NT 4.0 to mount, read from, and write to NTFS5 volumes created in Windows 2000. However, the new features such as EFS and disk quotas in NTFS5 included with Windows 2000 are disabled when booting the system using NT 4.0.
  - See the following articles in Microsoft Product Support Services for further information:
Dual-Booting Windows NT 4.0 and Windows 2000 on NTFS Partitions
http://support.microsoft.com/support/kb/articles/q184/2/99.asp

Security

Off-site Backup

Off-site backup is a practice such that backup storage media (e.g. backup tapes) are not stored in the original data site (i.e. the school site). Schools should consider having an off-site backup of their backup storage media. This allows data recovery if a disaster occurs for the whole site.

Chassis Lock

Chassis lock is an effective means to prevent hardware inventory lost. Schools should consider using it to lock every server and client computer in their school.

Property Markings

A property marking means the use of engraving or permanent pigment to mark on hardware items such as server and client computers, monitors, hubs, switches, printers and scanners, etc. to identify the owner of the items (i.e. the Education Department or the school). It is the responsibility of contractors to coat property markings to hardware items.

Redundant Array of Independent Disks (RAID)

RAID can be implemented at the hardware level, using RAID controllers, or at the software level, either by the operating system or by a third-party add-on. Windows 2000 supports both hardware RAID and its own software RAID.

Hardware RAID implementations require specialized controllers and in general cost much more than a software RAID of equivalent class. But for that extra price, they get faster, more flexible, and more fault-tolerant. When compared to the software RAID provided in Windows 2000 Server, a good hardware RAID controller supports more levels of RAID, on-the-fly re-configuration of the arrays, hot-swap and hot-spare drives, and dedicated caching of both reads and writes.

The Windows 2000 Server software RAID requires converting the disk system to dynamic disks. The disks will then no longer be available to other operating systems, such as NT 4.0 and Windows 95/98. However, special consideration should be taken as to whether the boot disk should be converted to a dynamic disk. Dynamic disks can be more difficult to access if a problem occurs, and the Windows 2000 setup and installation program provides only limited support.
For maximum fault tolerance, hardware RAID is recommended for school servers.

**Uninterruptible Power Supply (UPS)**

It is recommended to attach an UPS device(s) to school server(s) and other mission-critical computing equipment. With UPS device(s) connected to the server(s), during a power failure, the UPS service immediately pauses other server services to prevent any new connections and sends a message to notify users of such event. The UPS service then waits a specified interval of time before notifying users to terminate their sessions. If the power is restored during the interval, another message is sent to inform users that power has been restored and normal operation has resumed.

However, if the power failure is prolonged and the UPS reaches a critical state, a shutdown of the server(s) will be performed, and the UPS device(s) will be turned off. Therefore, School Network administrators should ensure that their UPS device(s) guarantee(s) at least 10 minutes power supply to enable their servers as well as other mission-critical equipment to perform a graceful shutdown.

**Tape Auto-loader or Library**

For managing large backups that span several tape cartridge sets, schools should consider using tape auto-loader or library. Auto-loaders let multiple tape cartridges be stored and accessed by a single backup tape drive through a robotic mechanism for hands-free backup operation.

**Normal (Full), Incremental, and Differential Backup**

A *normal* backup always copies all selected files and marks each file as having been backed up. Normal backups give schools the ability to restore files quickly because files on the last tape are the most current.

The *incremental* method only backs up files that are created or changed since the last normal or incremental backup. It marks files as having been backed up. If schools use a combination of normal and incremental backups, restoring requires starting with their last normal backup and then working through all the incremental tapes.

A *differential* backup copies files that are created or changed since the last normal (or incremental) backup. It does not mark files as having been backed up. If schools are doing normal and differential backups, restoring requires only the last normal and last differential backup tape.

The following table lists the advantages and disadvantages associated with running each type of backup:

<table>
<thead>
<tr>
<th>Type</th>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Files are easy to find because they are current</td>
<td>Most time-consuming.</td>
</tr>
</tbody>
</table>
are always on a current backup of the system or on one tape or tape set. If files do not change frequently, backups are redundant.

Recovery requires only one tape or tape set.

<table>
<thead>
<tr>
<th>Backup Type</th>
<th>Description</th>
<th>Files Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incremental</td>
<td>Least data storage space required.</td>
<td>Files are difficult to find because they are spread across several tapes.</td>
</tr>
<tr>
<td></td>
<td>Least time-consuming.</td>
<td></td>
</tr>
<tr>
<td>Differential</td>
<td>Less time-consuming than normal backup.</td>
<td>If large amounts of data change daily, backups can be more time consuming than incremental.</td>
</tr>
<tr>
<td></td>
<td>Recovery only requires last normal backup tape and last differential backup tape.</td>
<td></td>
</tr>
</tbody>
</table>

Backup Verification

A backup verification is an operation that compares files on hard disk to the files which have been written to tape. It occurs after all files are backed up and takes about as long as the backup procedure itself. Schools should consider performing backup verification after backing up their data.

Recovery Console

The Recovery Console is a command-line environment that School Network administrators can use to make system changes to a Windows 2000 Professional system that refuses to start. It is useful if School Network administrators who want to repair the system by copying a file from the original Windows 2000 CD. School Network administrators can also use the Recovery Console to start or stop system services and to format disks. But the Recovery Console is intended for use by knowledgeable School Network administrators who are well versed in system troubleshooting and repair.

There are two ways to start the Recovery Console on Windows 2000 systems:

- If the computer cannot start, run the Recovery Console from the Setup disks / Windows 2000 CD.
- If the computer can start, run the Recovery Console as an option in the boot menu.

For more information about Windows 2000 Recovery Console, see the following:

Description of the Windows 2000 Recovery Console
http://support.microsoft.com/support/kb/articles/Q229/7/16.ASP

Emergency Repair Disk (ERD)
The Recovery Console can help School Network administrators to get Windows 2000 up and running when there is a problem. However, in some cases School Network administrators will also need the ERD to repair and recover a system that cannot load and run Windows 2000 Professional.

Since the ERD contains system and security information, it is recommended to label the disk and put it in a safe place.

**Extendibility**

**Routing and Remote Access Services (RRAS)**

Windows 2000 RRAS server behaves differently from Windows NT 4.0 when assigning DHCP IP addresses.

Windows NT 4.0 would lease enough IP addresses for all RAS devices configured on the RAS server plus one for the RAS server interface. If schools had 20 modems configured on the Windows NT 4.0 RAS server, it would lease 21 IP addresses when the RAS service starts.

When a DHCP server cannot be contacted by a Windows NT 4.0 RAS server, it cannot provide IP addresses to the client, this prevents the client from connecting using TCP/IP.

In Windows 2000, the RRAS server leases IP addresses in blocks of 10 and stores them in the registry. When additional IP addresses are required, it leases 10 more.

If a Windows 2000 RRAS server cannot contact a DHCP server, it uses Automatic Private IP Addressing (APIPA) to assign IP addresses to RAS clients.

**Dial-up Options**

The following options are not available in Active Directory Users and Computers MMC snap-in when the Windows 2000 School Network domain is in mixed mode:

- Control access through remote access policy
- Verify caller ID
- Assign a static IP address
- Apply static routes
- Static routes

**Internet Connection Sharing (ICS)**
As introduced in Chapter 2 "Introduction to Windows 2000", a Windows 2000 computer with Internet connectivity and Internet Connection Sharing (ICS) service enabled can share its connection and allow other networked computers to access the Internet. A proxy server in a School Network can also provide similar service. The following table is a brief comparison of the two:

<table>
<thead>
<tr>
<th>ICS</th>
<th>-vs- Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used for basic Internet access</td>
<td>Includes performance, accounting, logging and security features</td>
</tr>
<tr>
<td>Transparent to clients and servers</td>
<td>Clients need to be configured to use Proxy</td>
</tr>
<tr>
<td>Primarily OSI layer 3 (network) and layer 4 (session)</td>
<td>OSI layer 7 (application)</td>
</tr>
<tr>
<td>Does not need to understand higher layer applications. It just modifies IP addresses and port numbers</td>
<td>Proxy must understand protocol or application that it will proxy</td>
</tr>
<tr>
<td>No cache feature</td>
<td>Proxy could respond from cache</td>
</tr>
</tbody>
</table>

In addition, ICS should not be used in an environment with existing DNS and DHCP servers. This means that ICS should not be used in a School Network with Windows 2000 Active Directory (i.e. DNS and DHCP are enabled). Schools should only consider using ICS in a workgroup environment.
### Appendix B

#### Parameters for Designing a Basic Windows 2000 School Network

(Reference value)

#### Network Infrastructure

**Domain Structure**

- Number of Windows 2000 domain: (1)
- Use of OUs to organize network structure: (yes)

**Servers**

- Number of servers: 
- Server role: (Domain Controller)
- Licensing mode: (per server / per seat; work out the most cost-effective mode; refer to the examples)
- Number of Client Access Licenses (CALs): 
- Number of partitions for server hard disk: (2, one for system and one for users)

**Client Computers**

- Number of client computers: 
- Number of category for client computer configuration: 

**Network Communications**

- Communication protocol: (TCP/IP)
- IP address range: (10.x.x.x from ED)
- IP address scheme in school: (yes; refer to the examples)
- DHCP: (yes)
- DNS: (yes)
- WINS: (yes)
- Domain naming convention: (yes; refer to the examples)
- Computer & device naming convention: (yes; refer to the examples)
- Descriptions to be added to computers & devices: (location, purpose, computer type)
### User Administration

**User Account Policy**

- **User accounts: domain vs. local**
  - Domain user accounts for networked computers; local user accounts for standalone computers

- **No. of personal user accounts**

- **No. of shared user accounts**

- **User account naming convention**
  - Yes; refer to the examples

- **User profile**
  - Roaming profile for user accounts in School Network; local profile for standalone computers

**Grouping Strategy**

- **Use of OUs to organize network structure**
  - Yes

- **Grouping users**
  - Use global groups

- **Assigning permissions**
  - Use domain local groups

- **Strategy and number of groups for grouping users**
  - Students grouped by admission year; one group for teachers; one group for administrators

**User Data and Settings Management**

- **User data and settings management**
  - Windows 2000 only network: Group Policies
  - Mixed NT 4.0 and Windows 2000 network: System Policies

- **Home directory scheme**
  - Yes

- **Initial size of home directory**
  - 10MB for each user

- **Location of home directory**
  - D:\Home\%username% on the school server

- **Permission for home directory**
  - "Change" permission for owner, "No Access" for other users

- **Drive letter for home directory**
  - U:

- **Folder redirection**
  - Redirect "My Documents" folder to home directory
**Resource Sharing**

**File System and Sharing**
- File system of school servers: NTFS
- File system of client computers: NTFS
- Multi-boot systems: 
- No. of shared folders: 
- Permission on shared folders: NTFS permission
- Disk quotas: Yes
- File encryption: 
- Offline files and folders: 

**Print Sharing**
- No. of shared printers: 
- Location of each shared printer: 
- Physical connections of the shared printers: through printer sharing devices
- Print server assignment: server machine
- Permission on shared printers: Students: Print; Teachers: Manage; Administrators: Full

(Reference value)
Security

Security Policy for School Network  

<table>
<thead>
<tr>
<th>Physical Security</th>
<th>(yes; including, but not limited to, the following)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security area definition</td>
<td>(yes; refer to the examples)</td>
</tr>
<tr>
<td>Property marking</td>
<td>(yes)</td>
</tr>
<tr>
<td>Server BIOS password</td>
<td></td>
</tr>
<tr>
<td>Client computer BIOS password</td>
<td></td>
</tr>
<tr>
<td>Other details of physical security policy</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Security</th>
<th>(yes; refer to the examples)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data classification</td>
<td>(yes; refer to the examples)</td>
</tr>
<tr>
<td>Third party personnel access policy</td>
<td>(yes; refer to the examples)</td>
</tr>
<tr>
<td>Anti-virus policy</td>
<td></td>
</tr>
<tr>
<td>RAID-5 disk subsystem for server</td>
<td>(yes)</td>
</tr>
<tr>
<td>UPS</td>
<td>(for servers and backbone switch/hub)</td>
</tr>
<tr>
<td>Backup and recovery strategy</td>
<td>(yes; refer to the examples)</td>
</tr>
<tr>
<td>Other details of data security policy</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Windows 2000 Security</th>
<th>(8 characters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum password length</td>
<td>(yes)</td>
</tr>
<tr>
<td>Account lockout</td>
<td>(5 failed logon attempts)</td>
</tr>
<tr>
<td>Windows 2000 group policy control</td>
<td></td>
</tr>
<tr>
<td>NT 4.0 system policy control</td>
<td></td>
</tr>
<tr>
<td>File encryption</td>
<td></td>
</tr>
<tr>
<td>Audit policy</td>
<td></td>
</tr>
<tr>
<td>Other details of Windows 2000 policy</td>
<td></td>
</tr>
</tbody>
</table>
### Extendibility

**Routing and Remote Access Service (RRAS)**
- Concurrent connections for remote dial-in: __________
- Resources accessible to the dial-in users: __________
- Call-back feature enabled: ___ (yes)
- Log the activities: ___ (yes)

**Internet Access**
- Internet services available to users: ___ (WWW for all users)
- Enhance Internet performance via proxy server: ___ (yes)

**Integration with Existing Systems**
- Integration with existing NT 4.0 standalone computers: __________
- Integration with existing NT 4.0 School Network: __________
- Migration from NT 4.0 School Network to Windows 2000 School Network: __________
10 Appendix C

Checklist for Deploying Windows 2000 to Form a New School Network

"Deploying a new Windows 2000 School Network" applies to schools with no School Network already established. The new School Network will use Windows 2000 Server as domain controllers (and member servers) and Windows 2000 Professional as client computers. Those standalone NT 4.0 Workstation computers existing in school environment (e.g. ED1 and ED2) can be optionally attached to the newly formed Windows 2000 School Network as client computers.

There are several possible scenarios and approaches to deploy Windows 2000 to form a new School Network. The design will vary subject to the schools' requirements, readiness and resources as well as their existing IT equipment. The checklist outlines the basic steps needed for a successful deployment of a new Windows 2000 School Network.

Notes

The checklist is intended to give schools a feel of some of the issues that schools need to be aware of. It is by no means the best or optimal solution for every school. School Network administrators should consult contractors for suggestions and further information, and work closely with them to plan, design and implement their School Network.

Planning

1. Schools should take inventory of existing computer equipment and software used.

2. Schools should list out their own user requirements with reference to this guideline whenever applicable.

3. Schools may invite contractors to submit proposals for School Network implementation.

4. Contractors will design the proper Windows 2000 infrastructure, including Active Directory and domain designs, organizational unit and group policy definitions, account and group administration, network services, resources management, and security measures etc.

5. Contractors must include the integration of existing computer equipment in the proposal if any existing standalone NT 4.0 computers are planned to be integrated with the Windows 2000 School Network.
6. Contractors must also propose a licensing mode that is most cost-effective to the school’s respective environment.

Preparing
7. Schools may consider performing a backup on all affected computers as well as trial restoration to verify that files are properly backed up and able to be restored.

Deploying
8. For server computers, contractors should use NTFS as the file system for better security.

9. Contractors should use TCP/IP as the default network protocol. Install other network protocol only when it is required for other applications in the School Network.

10. Contractors should use static IP addresses for servers, network devices and printers. Use DHCP to dynamically assign IP addresses for client computers.

11. Contractors should set up Windows 2000 as DNS server.

12. Contractors should use WINS for supporting backward compatibility for pre-Windows 2000 systems and applications.

13. If there are NT 4.0 computers joining the Windows 2000 School Network, contractors should take into consideration the use of Windows 2000 Group Policies and NT 4.0 System Policies in a mixed Windows 2000 and NT 4.0 School Network environment.

14. Contractors should share network resources with proper settings and assign appropriate permissions according to school’s requirements.

15. Contractors should confirm that the security settings and measures will meet school’s security requirements.

16. Schools should conduct the acceptance test (reliability test) and make sure the School Network can achieve school’s objectives and requirements.
11 Appendix D
Checklist for Integrating Windows 2000 to an Existing NT 4.0 School Network

An existing NT 4.0 School Network means a School Network with NT 4.0 Server used as PDC (and BDCs and member servers) and NT 4.0 Workstation used as client computers (e.g. ED3).

Integration of Windows 2000 to an existing NT 4.0 School Network means adding new Windows 2000 Server (as member server) and Professional systems to the School Network while keeping the existing NT 4.0 infrastructure unchanged -- NT 4.0 PDC (and BDCs) remains dominant.

There are several possible scenarios and approaches to integrate Windows 2000 to an existing NT 4.0 School Network. The design will vary subject to the schools' requirements, readiness and resources as well as the settings of their existing School Networks. The checklist outlines the basic steps needed for a successful integration of Windows 2000 to an existing NT 4.0 School Network.

Notes

The checklist is intended to give schools a feel of some of the issues that schools need to be aware of. It is by no means the best or optimal solution for every school. School Network administrators should consult contractors for suggestions and further information, and work closely with them to plan, design and implement their School Networks.

Planning

1. Schools should take inventory of existing computer equipment, software used and the configuration settings.

2. Schools should list out their own user requirements. For integrating Windows 2000 to an existing Windows NT 4.0 network, schools may refer to the following website:

Notes

Limited Windows 2000 features can be utilized in an NT 4.0 dominant School Network. Some Windows 2000 advanced features that require Active Directory and Group Policy (e.g. policy-based user data and settings management and automated software installation) cannot be used in an NT 4.0 dominant network.
3. School may invite contractors to submit proposals for integrating Windows 2000 to the existing Windows NT 4.0 School Network.

4. Contractors will review the School Network design including user administration, policy definitions, network services, resources management and security measures etc. in a mixed environment.

5. In order to keep the existing NT 4.0 infrastructure unchanged, do not use Windows 2000 Server as domain controller. Instead, use Windows 2000 Server as member servers.

6. Contractors should consider a gradual introduction of Windows 2000 Server (member servers) and Professional (client computers) by deploying them when there is a replacement or a new purchase of computers.

7. Contractors should document the implementation plan and have a contingency plan in place.

Preparing

8. Schools may consider evaluating the new features of Windows 2000 environment in a testing environment.

9. Schools may consider performing a backup of all affected computers as well as trial restoration to verify that files are properly backed up and able to be restored.

Integrating

10. For Windows 2000 member servers, use NTFS as the file system for better security.

11. Contractors should continue to use TCP/IP as the default network protocol. Install other network protocols only when it is required for other applications in the School Network.

12. Contractors should continue to use static IP addresses for servers, network devices and printers. Use DHCP to dynamically assign IP address for client computers.

13. Contractors should continue to use WINS for name resolution.

14. Since Windows 2000 Server is used as member servers only, the existing NT 4.0 infrastructure will remain unchanged. Generally, School Network administrators with technical skills on NT 4.0 can continue to use existing tools to administer users and manage the School Network -- use NT 4.0 System Policies to manage user settings and system configurations.

15. Contractors should confirm that the security settings and measures will meet school's security requirements.

17. Schools should conduct the acceptance test (reliability test) and make sure the interoperability of the School Network meets school's objectives and requirements.
12 Appendix E
Checklist for Migrating an Existing NT 4.0 School Network to Windows 2000

An existing NT 4.0 School Network means a School Network with NT 4.0 Server used as PDC (and BDCs and member servers) and NT 4.0 Workstation used as client computers (e.g. ED3).

Migrating an existing NT 4.0 School Network to Windows 2000 means that upgrading the existing NT 4.0 PDC (and BDCs) to Windows 2000 domain controller. The existing NT 4.0 infrastructure will then be changed to Windows 2000 dominant. Optionally, existing NT 4.0 member servers and NT 4.0 Workstation computers can also be upgraded to Windows 2000 member server and Professional respectively so that all Windows 2000 features can be utilized.

There are several possible scenarios and approaches to migrate an existing NT 4.0 School Network to Windows 2000. The design will vary subject to the schools' requirements, readiness and resources as well as the settings of their existing School Network. The checklist outlines the basic steps for a successful migration from NT 4.0 to Windows 2000 School Network.

Notes

The checklist is intended to give schools a feel of some of the issues that schools need to be aware of. It is by no means the best or optimal solution for every school. School Network administrators should consult contractors for suggestions and further information, and work closely with them to plan, design and implement their School Networks.

Planning

1. Schools should take inventory of existing computer equipment, software used and the configuration settings.

2. Schools should list out their own user requirements. For migrating an existing Windows NT 4.0 network to a new Windows 2000 network, schools may refer to the following website: http://www.microsoft.com/technet/win2000/deploy.asp

3. Schools may invite contractors to submit proposals for migrating the existing Windows NT 4.0 School Network to Windows 2000 School Network.

4. Contractors will design the proper Windows 2000 infrastructure, including Active Directory and domain designs, organizational unit and
group policy definitions, account and group administration, network services and resources management, security measures etc.

5. Contractors should consider using single domain model whenever possible as it is the easiest domain structure and it is suitable for most school environments.

6. Contractors should propose a migration plan without jeopardizing the operation of the School Network. Moreover, contractors should also include the contingency plan in the proposal.

**Notes**

*One of the items to be included in the contingency plan is to prepare spare BDC(s). This BDC(s) should be made offline during the PDC upgrade process. This disconnected spare BDC(s) can be used for promotion to an NT 4.0 PDC in case of contingency.*

**Preparing**

7. Schools may consider evaluating the new features of Windows 2000 environment in a testing environment.

8. Schools may consider performing a backup of all affected computers as well as trial restoration to verify that files are properly backed up and able to be restored.

9. Notify the users that the School Network will be unavailable during the migration period.

**Upgrading**

10. Contractors should then upgrade the PDC (PDC must be the first domain controller to be upgraded).

11. For server computers, use NTFS as the file system for better security.

12. Contractors should use TCP/IP as the default network protocol. Install other network protocol only when it is required for other applications in the School Network.

13. Contractors should use static IP addresses for servers, network devices and printers. Use DHCP to dynamically assign IP addresses for client computers.

14. Contractors should use Windows 2000 as DNS server or use an existing DNS server that supports Windows 2000.

15. Contractors should use WINS for supporting backward compatibility for pre-Windows 2000 systems and applications.

16. Contractors should define Active Directory, domain, OUs, user accounts, groups and computers according to school’s requirements.
17. Contractors should make use of Windows 2000 Group Policies to manage user data and settings as well as other administrative tasks for Windows 2000 computers.

18. Contractors should share network resources with proper settings and assign appropriate permissions according to school’s requirements.

19. Contractors should confirm that the security settings and measures will meet school’s security requirements.

20. Test the School Network thoroughly. If the School Network functions properly then contractors may start to upgrade any BDCs, member servers, and NT 4.0 Workstation computers accordingly.


22. Schools should conduct the acceptance test (reliability test) and make sure the interoperability of the School Network meets school’s objectives and requirements.