

BrainBuzz

Cramsession

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

Click [here](#) to see additional documents related to this study guide. Click [here](#) to receive free practice questions for Updating Support Skills from Microsoft Windows NT 4.0 to Microsoft Windows 2000.

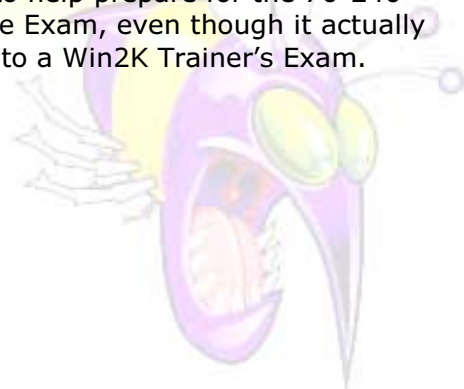
Contents

Contents.....	1
Updating Support Skills from Microsoft Windows NT 4.0 to Microsoft Windows 2000 - Cramsession	2
Upgrading and Installing Issues	2
Windows 2000 Professional Features:	2
Installation requirements	3
Windows 2000 Server MINIMUM.....	3
Windows 2000 Setup.....	3
New Winnt32.exe command line switches.....	3
Active Directory	4
Terminal Services	8
Remote Access Service (RAS)..	9
DHCP	9
WINS	10
Disk/Storage/Backup.....	10

Cramsession™ for Updating Support Skills from Microsoft Windows NT 4.0 to Microsoft Windows 2000

Abstract:

This is the first Windows 2000 Cramsession that we posted on our site. The material in this study guide can be used to help prepare for the 70-240 Update Exam, even though it actually maps to a Win2K Trainer's Exam.



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

Updating Support Skills from Microsoft Windows NT 4.0 to Microsoft Windows 2000 - Cramsession

The following is a brief list of some of the new and changed items that you should understand before moving into the Windows 2000 support arena. This information is based on the Beta 3 release of Windows 2000.

Upgrading and Installing Issues

Windows 2000 Professional Features:

- Customized Start Menu
- Logon and Shutdown Dialog Boxes on Start Menu
- New Task Scheduler
- Offline Folders – like the old briefcase – much easier to use and much more functional
- Much improved printing support
- New Setup Tools:
 - Sysprep (used to prepare for programs like Ghost and Drive Image)
 - Setup Manager Wizard (question and answer tool that generates an installation script)
- Systems Management is now provided in a common interface – Microsoft Management Console (MMC)
- New troubleshooting tools and Windows 2000 Compatibility Tool
- Add/Remove hardware wizard
- Plug and Play Support
- Common driver set (Windows Driver Model) – Same drivers for Win98 and Windows 2000
- Power management
- NTFS Disk quotas
- FAT32 Support
- Built in Disk defragmenter
- Backup utility now works with Zip/Tape/External hard disks
- Volume mount points are supported
- Kerberos Version 5 Protocol Support
- Encrypted file system support
- IPsec
- Smart Card Authentication

- Secondary Logon Service

Installation requirements

Windows 2000 Professional MINIMUM

- Pentium 166
- 32MB RAM
- 685MB Disk Space available
- NIC
- CD-ROM – unless installing over the Network
- Pointing Device recommended

Windows 2000 Server MINIMUM

Same as Professional except:

- 64MB for 5 users, 128MB for more

Windows 2000 Setup

- Winnt.exe does not create boot disks any more – use makeboot.exe
- New winnt.exe command line switches:
 - */e[:command]* – executes a command before the last phase of setup
 - */r:foldername* – Installs an additional folder within the folder where the Windows 2000 files are installed. The folder IS NOT DELETED after Setup finishes. You can use additional */r* switches to install additional folders
 - */rx:foldername* – specifies a folder to be copied as a part of setup – into the Windows 2000 directory, but the folder IS DELETED as setup finishes
 - */r* and */rx* are useful for third party drivers

New Winnt32.exe command line switches

- */copydir:foldername* – same as */r* for winnt.exe
- */copysource:foldername* – same as */rx* for winnt.exe
- */cmd:* - same as */e:* for winnt.exe
- */cmdcons* – installs the appropriate files to restart the system in command-line non-graphical mode for repair purposes
- */debug[level]:filename* – creates a debug log file with the specified level of detail. Default file name if not specified is winnt32.log. Levels are: 1=errors, 2=warnings, 3=information, 4=detailed information. all higher numbered levels include the previous levels (2 includes warnings and errors)

- `/syspart` – useful for preparing a hard disk to be transferred to another computer system. This switch installs setup files and marks the partition active. Requires the use of `/tempdrive` switch
- `/tempdrive` – specifies which drive to install Windows 2000 temporary files during setup.
- `/makelocalsource` – copies all of the Windows2000 source files to the target drive during installation. Useful when the CD is no longer local to the system and new features are installed
- `/noreboot` – just like it sounds – prevents reboot after installation so that another command can be run (service pack installation?)
- `/m:foldername` - provides an alternate location from which the installation will look for updated files – if one is not found it will look in the default location.

Setup Manager – a resource kit utility to assist in the creation of unattended setup files. Works with Windows 2000 Professional and Server – but not for a Domain Controller.

SysPrep.exe – assists with the removal of all unique elements of a fully installed computer system so that it can be duplicated using imaging software such as Ghost or Drive Image Pro. Avoids the NT4 problem of duplicated SIDS, computer names etc. Installers can use sysprep to provide an answer file for “imaged” installations

Remote Installation Services – RIS – Enables administrators to store Windows 2000 Professional configurations (not images) on a server. Installations can then be automated to remote client computers even if they don’t have an operating system installed. This requires that RIS is installed on a server, DNS, DHCP, and Active directory are present on the network. The RIS server must have a volume to hold the RIS configurations shared out to the network that is not on the same drive that is running NT Server – with enough space to hold the configurations, and MUST be NTFS. Clients require either a NIC with a PXE based boot ROM, a network installation diskette and supported NIC, or be a NET PC. See Microsoft course 1563 for additional information.

Active Directory

Active Directory is a directory service organized as a series of Domains in a hierarchy. Network resources are controlled from a central location – and hides the underlying network architecture from the users. Previous size limitations have been virtually eliminated. Administrators can exercise centralized or distributed control through the use of new technologies such as group policies.

DNS plays a large role in Active Directory. Microsoft has modeled its directory service namespace after DNS. In other words – an organization called NTSCHOOL could have a DNS name of `ntschoool.com`, and the accounting department could have their own domain as a subdomain of `ntschoool.com`. The resulting domain name is `accounting.ntschoool.com`. This is a big deal because we can exercise administrative control from the top of the hierarchy (`ntschoool.com`) that flows down to the accounting department. We can also delegate partial or full administrative control of the accounting department. DNS is used instead of WINS in this new environment. Queries for domain controllers are sent to a DNS server. The function of the

Microsoft DNS server has been enhanced to support SRV (service) records to facilitate this process.

Within Domains there is a new component called an organizational unit. These are great for organization of network resources and users within a domain. Administrative control can also be delegated using Ous. We could choose to implement a single domain for NTSCHOOL and create an accounting OU for all of the resources in the accounting department.

Domains are linked into a Tree. Multiple Trees joined at the top are called a forest. It is not currently possible to merge two existing trees into a forest. Forests are useful when a company has two or more divisions that have unique DNS namespaces. In the above mentioned example NTSCHOOL could also own a company called CARSCHOOL. Creating a Forest would still enable the distinct namespaces to exist (ntschoool.com and carschoool.com), but the administrator could have control over both trees, and users could use resources in each other's domains (permissions permitting).

Domain controllers are no longer listed a PDC and BDC – simply DC. Each domain controller in a domain is capable of accepting requests for changes to the domain database and replicating that information with the other DCs in the domain. Be aware that there are still some specific functions that are only handled by one DC in a domain – The Global Catalog server and Operations Masters.

The Global Catalog Server is a server (or servers if you decide to have more than one) that enables users to search the entire forest for resources, and it provides each user the list of universal groups that the user is a member of during the logon process. The Global Catalog server holds information about every object defined in the Forest – but only a subset of the properties of each object.

The Schema Master is one of the operations masters – it provides a centralized control mechanism for the structure of the Active Directory Database (what objects exist and what their property fields are)– only one per forest.

Domain Naming Master – Controls the addition of Domains in a forest. One per forest.

RID Master – Relative Identifier Master – works with domain controllers to assign unique SIDS to each object that requires one. Each object (user ID, computer object or group) gets a SID that is made up of a Domain SID (constant for all objects in the domain) and a RID which is unique to all objects in the domain. This is necessary as there are several DCs capable of handing out SIDs because of the multiple master nature of the DCs. One per Domain.

PDC Emulator – just like it sounds – particularly for non Windows 2000 clients and Servers in the domain. Acts just like a PDC. If the domain is running in Native Mode (no NT4 domain controllers), then this server is the "preferred" replication partner for the other DCs for password changes. One per Domain.

Infrastructure Master - updates user to group memberships when changes are made. One per domain.

DCPROMO.EXE – this is the Active Directory Installation Wizard. Used to promote a non-domain controller to a DC and vice versa. Typically launched from the Run dialog or from a command prompt. The wizard prompts for all of the required information to install Active Directory under the conditions that you have asked it to run (new tree, new domain in existing tree, new tree in existing forest, new DC in existing domain).

Sites are also a component Active Directory, however they don't impact the namespace in any way. Sites are used to define the boundaries of high-speed links in your network – used mostly to control replication traffic and which DC will respond to a logon request. Sites are based on IP subnets – any subnet can only belong to one site, but multiple subnets can be in a single site. A site is defined as a “well connected subnet or subnets”.

When domain controllers in a site replicate information they do so uncompressed – and this process cannot be scheduled – DCs collect changes for a 5 minute interval and then replicate. Urgent (immediate) replication occurs within a site (password changes, account lockout policy changes, freshly locked accounts, domain password policy changes). Replication between sites is scheduled, does not handle urgent replication, and is compressed in order to save bandwidth.

Site Links are the objects in Active Directory that define the parameters for connecting two sites. Costs (which can be assigned), Schedules (for when the link is available), and Intervals (determine when replication occurs) are defined as properties of a site link.

There are now three types of groups in Windows 2000 – Domain Local (similar to a local group), Global, and Universal groups. The rules remain the same for Local and Global groups, except that you can now nest groups in Native mode. Universal groups can have membership from any domain and can be used to assign access to any resource in any domain. TIP: Don't put users in Universal Groups – when a user logs in, their access token must be generated such that it contains a list of all of the universal groups that a user is a member of – this takes time! If they are members of other groups that are members of Universal groups, this does not occur. Additionally, the list of Universal Group members is maintained at the Global Catalog Server...

A G L P has changed to A G DL P. (Accounts go into Global Groups which then go into local groups that are assigned permissions to use a resource).

Each group can have one of two functions in Native mode – distribution or security. Security groups are the ones we are familiar with in NT4 – distribution groups will be used primarily with Exchange 2000 or any other Active Directory mail application.

There is an additional “group” that we introduced earlier – the OU. Consider placing objects with identical security requirements into an OU and assigning permissions to the OU – all objects in the OU will inherit the security assignment.

If you grant permissions to a user and to a group that the user is a member of, the permissions are cumulative (same as NT4). Denied permissions also take precedence over explicitly granted permissions. Be careful with the DENY permission – it is possible to eliminate access to an object completely – even to an administrator.

You can propagate permissions to child objects. You can also prevent the inheritance of those same permissions at the child object if you don't want to inherit from above.

It is possible to delegate control to a specific object by granting one individual user the permissions to that object. This is not recommended. Consider delegating control at the OU level. If you use the Delegation of Control Wizard, you can only delegate at the OU level. Consider delegating to a group rather than an individual user...

Group Policy in Windows 2000 is one of its largest administrative enhancements. Group Policy is designed to enable administrators to control the environment with minimal effort. Group policies are not applied to "groups", but we can apply them to OUs. There are five major categories that group policies can be configured for:

- Folder redirection: Store users' folders (my documents, my pictures) on the network.
- Security: Similar to account policies under user manager in NT4 – includes settings for the local computer, the domain, and network security.
- Administrative Templates – NT4 administrators will recognize this section as system policies – in a much more convenient and flexible configuration. Included are desktop, application, and system settings.
- Software Installation – Completely new – enables an administrator to have software installed automatically at the client machine – or removed automatically.
- Scripts – similar to logon scripts in NT4, but we can now specify a startup and a shutdown script for the computer as well as a logon and a logoff script for the user.

An administrator can create several Group Policy Objects (GPO) in a given Group Policy Container (GPC) and assign the appropriate GPO to the computers or users that need the settings contained in that GPO. It is important to note the inheritance of GPOs in Active Directory. Any GPO assigned to the Site will be applied, then the GPO assigned at the Domain will be applied, and finally any GPO assigned at the OU level will be applied. If there are conflicting settings in the GPOs, then the one applied last will overwrite – unless the administrator has specified that this is not the behavior required. An administrator of a given OU can specify "block inheritance" to prevent any settings from a GPO higher in the tree having any impact in that OU. However, the "master administrator" (the tree or domain administrator) may choose to set the "no override" flag on his/her GPO and this forces all of the settings in that GPO to be applied at all levels of the tree below where the GPO was assigned. This setting takes precedence over the "block inheritance" option.

If you want to exclude certain users or computers from processing the GPO assigned to the Site/Domain/OU that they belong to, you can simply remove the users' or groups' "apply group policy" permissions. This effectively creates a filter. You can also delegate control over GPOs so that a manager can change what a GPO does for his or her department, but can't create any new GPOs or change the scope of a GPO.

It is also possible to disable group policy objects without deleting them. If you do this (from Group Policy – Options) it will only disable it for that container and any sub-containers that inherit the settings. If another administrator "linked" to that GPO from another container, then the GPO is still active in that container.

Group Policy is always modified at the PDC operations master in the domain – regardless of where the administrator is accessing the GPO.

Software can be efficiently deployed, updated and removed using Group Policies and two technologies built into Windows 2000 – Windows Installer and Software Installation and Maintenance.

Windows Installer will replace Setup.exe for many application programs (.msi file extension). Its advantages include the ability to build custom installations, enable programs to "repair" themselves if a critical file is missing or corrupt, and to remove themselves very cleanly when necessary.

Software Installation and Maintenance – combines Group Policies and Active Directory Technologies to enable an administrator to install and manage software across the network – and even remove software. This is only available for Windows 2000 clients.

When you deploy software, you can choose to Assign it, or Publish it. Assigned software can be targeted at users or computers – if you assign an application to a user, the icons show up on the desktop and/or start menu, but the program is only installed when the user runs it for the first time. If it is assigned to the computer, it's installed the next time the system is restarted. If you Publish it, the user can install it through Add/Remove Programs, or through opening a file that requires that particular program (a file association). Published programs cannot self repair, cannot be published to computers, and are not advertised on the users' desktop or start menu – only through add/remove programs. Assigned apps require a windows installer file (.msi), Published apps can use Windows Installer files, or .ZAP files (an administrator created text file that specifies the parameters of the program to be installed and the file extensions associated with it). .ZAP installations cannot self repair, cannot install with higher privileges, and will typically require user intervention to completely install.

You can deploy upgrades (version 1 to version 2 for example) using GPO's simply by specifying which program this new one is going to upgrade, and if it's a mandatory upgrade or not.

You can apply service packs or patches by "re-deploying" an existing Group Policy with the new info regarding the service pack.

Terminal Services

Terminal Services are now a core function built in to every version of Windows 2000 from Server and above. There have also been some enhancements to the old "Windows NT 4.0 Terminal Server Edition". You have to install it through "add/remove programs" – once you've done this and installed the Client software (also provided), the workstation connects to the server and starts a virtual session on the server. Only screen, keyboard, and mouse information is exchanged between the client and server making it an ideal solution for remote dial up networking – or using a shared application on a single server (such as an accounting program) that many people need to update from distant locations (across the Internet or dial up). RDP (Remote Desktop Protocol) is the client-to-server protocol that supports this functionality. The client doesn't need to be an extremely capable system in that the execution of the program happens at the server. There are clients available for Windows 3.1, Windows 95/98, and NT. New for this release is the ability to "Shadow" or remote control client systems. Applications that can run on Terminal Services are many, but the preferred apps are Windows 32 bit programs because they can be tailored to use memory more efficiently. Don't undersize the server for this program. Add at least 8MB of RAM per user that you're going to support to the Terminal Services server. Microsoft states that a quad processor Pentium Pro with 512MB of RAM will concurrently support about 60 typical users. Each client must have a Client access license for Terminal Server and one for NT server (two licenses per client). After installing Terminal Services, you should re-install any applications on the server that you would like clients to use while connected to Terminal Services. When you "add/remove" programs, the system changes into a "program installation" mode that enables all users access to the app while attached. You can accomplish the same by issuing a "change user" command at the command prompt

and performing the installation from there. Some programs require an application compatibility script to be run in the terminal services environment. Microsoft supplies such a script for Office 2000 in the Office 2000 Resource Kit.

Remote Access Service (RAS)

RAS has changed rather dramatically. Several new RAS protocols are now available to make our communications over dial up lines or the Internet much more secure – and more flexible. These new protocols include Extensible Authentication Protocol (EAP), Layer Two Tunneling Protocol (L2TP), Bandwidth Allocation Protocol (BAP), Internet Protocol Security (IPSec) and Remote Authentication Dial-In User Service (RADIUS). Which of these you will use will depend greatly on what you are trying to accomplish.

EAP gives us the ability to use Transport Level Security – for smart cards, Generic Token Cards, and MD5-CHAP – another encryption methodology for usernames and passwords.

L2TP enables us to create a tunnel through a public network (the Internet) that is authenticated on both ends, uses header compression, and relies on IPSec for encryption of data passed through the tunnel. This is essentially a replacement for PPTP which uses an unauthenticated tunnel, no header compression, and uses PPP encryption.

Bandwidth Allocation Protocol allows us to set up Multilink capabilities, but if a user isn't using the bandwidth of multiple lines, we can drop one of the lines assigned to that user and use it for another user.

IPSec is essentially a driver at the IP layer that provides encryption very low down in the protocol stack.

RADIUS is an RFC based standard that allows us to provide authentication services from the corporate network to a client that is attaching to an ISP that wants access to our server. The ISP's dial up server that hosts the client is a client to the Radius Server Service (IAS) on the corporate network. The IAS server allows the user to connect – or not. The client can be running any platform supported by the ISP – and the corporate network can still authenticate them.

RAS Policies are also new. In NT4 you simply specified whether the user was allowed access to RAS or not. Now we can build an entire set of rules called a RAS Policy to dictate several conditions that must exist before a user can connect. Firstly, the user must be dialing from a specific IP address or from a range of addresses, during the right time of day, from the appropriate caller id location using the appropriate protocol. We can restrict access by group membership or the type of service requested. All of these are configurable and optional. Once the user has met all of the conditions, we can apply a profile, which can include items such as the IP address to use for this session, the authentication type that is allowed, any restrictions such as idle time, and the rules for BAP with multilink sessions.

DHCP

DHCP has several new components – firstly DHCP servers need to be authorized in Active Directory by a member of Enterprise Admins. If this is not done, the DHCP service on a Windows 2000 server in the forest will not initialize. The DHCP service can also be configured to register clients that it has given IP addresses to with the

Dynamic DNS server. SuperScopes (more than 1 IP subnet configured per physical network) and support for multicast scopes.

WINS

WINS remains for issues of backwards compatibility. The partnership with other servers that are running WINS for replication purposes has been made more stable, scalability has been enhanced (up to 12 servers can be specified), the ability to delete incorrect entries in the WINS database has been enhanced, and the management tools have also been enhanced.

The file system has some new enhancements in Windows 2000. The concept of sharing remains unchanged, but searching for a share across an environment with 20,000 client workstations becomes tedious. Windows 2000 introduces the concept of "publishing" shared resources to Active Directory. This enables users to search using LDAP rather than browsing...

Disk/Storage/Backup

Windows 2000 now includes a disk defragmenter.

The Distributed File System has also been enhanced. There are two types of DFS implementations: Stand-alone and Fault Tolerant. Stand-alone DFS stores the configuration information on a single node (server). Child nodes can only go one level below root, and can exist on any server. Fault Tolerant DFS stores the DFS configuration information in Active Directory. There can be two identical shares on different servers configured as a single child node to provide fault tolerance. You can have multiple levels of child volumes – and file replication is supported. Clients must have DFS software installed. Windows NT4, Windows 2000 and Windows 98 include this software, Windows 95 clients must download the appropriate DFS client software from Microsoft.com

NTFS permissions remain largely unchanged.

NTFS in Windows 2000 introduces the concept of disk quotas. You can set space limitations on users on a per volume basis. The ownership of a file determines which user to charge the space used against. You must enable quota management from the properties dialog – quota tab of a given disk. You can then set thresholds for individual users – including a warning level when their files exceed a certain amount of storage that is approaching their quota limit.

Windows 2000 NTFS volumes have the ability to encrypt data on the disk itself. This is based on public key – private key encryption procedures. Only the user that stored the file can open it again – or a recovery agent. Taking ownership of an encrypted file will not let you read it. Cipher.exe is a command line utility that allows for bulk or scripted file encryption. To enable a folder to have any new contents encrypted, simply view the property page for the folder and select "Encrypt contents to secure data".

Disk systems now support FAT32, NTFS, and FAT. However, there is a new type of storage that will enhance Windows 2000's ability to utilize disk space. The new storage type is called "dynamic disks". Dynamic disks' advantages include an unlimited number of volumes created per disk (while this seems odd, think of a very large hardware raid array – we can now break that into a good number of smaller logical drives – volumes – using dynamic disks). NTFS Volumes can be extended – and we can now include space from different disks. Perhaps the most important item is that the disk configuration is stored on the disk itself. This means that we can move disks between computers (within reason) and have the data available with little additional effort. If you perform an upgrade from NT4, or do a fresh install the disk type is still "Basic". You can then convert to dynamic storage. If you had mirroring or RAID of any type set up on the NT4 server that you upgraded, you can continue to maintain those configurations with Basic disks. However if you want to add a new array or mirror set, you will be required to convert to dynamic disks. In a fresh install you will also need to convert before implementing any mirroring or RAID configurations (software RAID and mirroring, not a hardware implementation). Once you have converted to dynamic disks – there's no reverse conversion – simply delete and start again. We can also take a freshly installed disk in our computer and NOT assign a drive letter – but create an empty directory on an existing volume and mount the new disk into that directory the UNIX folks will recognize this as a "mount point". Great for adding disk capacity for an existing application.

The Backup program has been greatly enhanced – to support Active Directory, different backup media (removable disks, network drives, and logical drives along with a large list of tape devices), and an integrated scheduling facility.

What happened to the "VGA mode" menu option?? Try pressing F8 on startup – the menu is very similar to Windows 95/98 – although the network administrator will see some very useful items depending on what's trying to be fixed. VGA mode is indeed present, but there's also "Directory Services Restore Mode", and "Safe Mode with Command Prompt", and "Last Known Good Configuration".