



**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 Windows 2000 Network Infrastructure.

## Contents

|                                                                                                                                     |   |
|-------------------------------------------------------------------------------------------------------------------------------------|---|
| Contents.....                                                                                                                       | 1 |
| Windows 2000 Network Infrastructure.....                                                                                            | 2 |
| Exam 70-216 - Implementing and Administering a Microsoft® Windows® 2000 Network Infrastructure.....                                 | 2 |
| Installing, Configuring, Managing, Monitoring, and Troubleshooting DNS in a Windows 2000 Network Infrastructure.....                | 2 |
| Installing, Configuring, Managing, Monitoring and Troubleshooting DHCP in a Windows 2000 Network Infrastructure.....                | 4 |
| Configuring, Managing, Monitoring, and Troubleshooting Remote Access in a Windows 2000 Network Infrastructure ...                   | 5 |
| Installing, Configuring, Managing, Monitoring, and Troubleshooting Network Protocols in a Windows 2000 Network Infrastructure ..... | 7 |
| Installing, Configuring, Managing, Monitoring, and                                                                                  |   |

Troubleshooting WINS in a Windows 2000 Network Infrastructure ... 8

Installing, Configuring, Managing, Monitoring, and Troubleshooting IP Routing in a Windows 2000 Network Infrastructure..... 9

Installing, Configuring, and Troubleshooting Network Address Translation (NAT) ..... 10

Installing, Configuring, Managing, Monitoring, and Troubleshooting Certificate Services ..... 11

## Cramsession™ for Windows 2000 Network Infrastructure

### Abstract:

This Cramsession will help you to prepare for Microsoft exam 70-216, Implementing and Administering a Microsoft Windows 2000 Network Infrastructure. Exam topics include Installing, Configuring, Managing, Monitoring, & Troubleshooting the Following Components of a Win2K Infrastructure: DNS, DHCP, Remote Access, Network Protocols, WINS, IP Routing, Network Address Translation (NAT), and Certificate Services.

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](#).

## Windows 2000 Network Infrastructure

### Exam 70-216 - Implementing and Administering a Microsoft® Windows® 2000 Network Infrastructure

#### Installing, Configuring, Managing, Monitoring, and Troubleshooting DNS in a Windows 2000 Network Infrastructure

Originally HOSTS files were used to translate all host names to IP addresses. These static flat files had to exist and be updated on every host connected to the network. As this became impossible, DNS (Domain Name System/Service) became the replacement. DNS is a server service consisting of a database that is hierarchical in nature and distributed, with built-in capabilities for redundancy and caching.

The first division of DNS is into domains. The InterNIC (Internet Network Information Center) controls top-level domains, which are summarized in the following table:

| Name | Type of Organization                                                           |
|------|--------------------------------------------------------------------------------|
| Com  | Commercial organizations                                                       |
| Edu  | Educational institutions                                                       |
| Org  | Non-profit organizations                                                       |
| Net  | Networks (the backbone of the Internet)                                        |
| Gov  | Non-military government organizations                                          |
| Mil  | Military government organizations                                              |
| Num  | Phone numbers                                                                  |
| Arpa | Reverse DNS                                                                    |
| Xx   | Two-letter country code, such a "ca" for Canada, "uk" for United Kingdom, etc. |

To refer to a host in a domain, you use a fully qualified domain name (FQDN), which, in essence, specifies the actual location of the host. An FQDN specifies the host name, the domain or subdomain the host belongs to, and any domains above that in the hierarchy until the root domain in the organization is specified. The FQDN is read from left to right, with each host name or domain name specified by a period.

DNS (see [Overview](#)) is installed as a service within Windows 2000 through the use of wizards. If you install Active Directory (through the Active Directory Installation Wizard) and a DNS server cannot be found, the ADI wizard will attempt to install the DNS service for you. If you wish only to install DNS, you can do so through the Networking Services component beneath the Add/Remove Programs applet of the Control Panel.

Key terms to know when discussing the service are:

- DNS Client - any computer that can query a DNS server (through a resolver)
- DNS Server - any computer running the DNS service
- Query - either recursive or iterative.
- Resolver - the system which actually issues the queries to the name server

The root name server of a domain is the name server that is acting as the Start of Authority for that zone. When a DNS server cannot resolve a query, it moves (escalates) it up to a root server that is authoritative for a zone. The Start of Authority (SOA) record is the first record in the database (KB# [Q163971](#)), and contains a serial number, the primary server (and responsible person), and information on intervals for secondary servers to update. Secondary servers update their databases through zone transfers.

Configuring a zone for dynamic updates within the zone properties dialog box (obtainable from the DNS management snap-in) allows DNS clients to update their resource records dynamically with the server anytime a change occurs. This can be enabled or disabled on a per-zone basis.

DNS uses resource records to perform its translations. If necessary, resource records can be manually added into DNS through the DNS snap-in. Resource records types include:

| Record Type | Purpose                                                                                                 |
|-------------|---------------------------------------------------------------------------------------------------------|
| A           | Address record – for mapping a DNS name to an IP address                                                |
| CNAME       | Canonical Name - an alias domain name for a name already specified as another resource type in the zone |
| MB          | Mailbox record                                                                                          |
| MG          | Mail group record                                                                                       |
| MINFO       | Mailbox or mailing list information - usually used to specify a mailbox for error messages              |
| MX          | Mail exchanger record - details message routing to a mail exchange host                                 |

|     |                                                                                                                                                                                                            |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PTR | Pointer record - used for reverse lookups                                                                                                                                                                  |
| TXT | Text record - can hold descriptive text                                                                                                                                                                    |
| RT  | Route Through - details intermediate-route-through binding for hosts that do not have their own WAN address                                                                                                |
| SRV | Service record - used by Windows 2000 for Active Directory and "Dynamic DNS". Active Directory can work with non-Windows 2000 DNS servers so long as those DNS servers can support the use of SRV records. |

Dynamic DNS (DDNS) - mentioned in the table - is simply the marriage of DHCP and DNS. Whenever a client interacts with DHCP (new lease, renewal, etc.), the fully qualified name (FQDN) of the client is registered with DNS through the DHCP server. This registration can be done manually using the "registerdns" parameter with the ipconfig.exe utility (KB# [Q235272](#)).

Within Windows 2000, the types of zones supported are:

- Active Directory-integrated
- Standard Primary - the owner of the zones within its database (able to make changes)
- Standard Secondary - has read-only copies of the database and cannot make changes or updates
- Caching-only (KB# [Q167234](#)) - a non-authoritative server that is confined to resolving cached queries

The caching-only server does not have a copy of the zone table and is merely used to speed up client queries by storing the results of cached queries. Delegated zones require all queries on the existing domain to go to one server for resolution. In all cases, the delegated domain must be a sub-domain of the domain performing the delegation.

DNS management can be done with the DNS Manager snap-in. Monitoring can be done through the Performance tool on such counters as Caching Memory, IXFR Counters, TCP/IP, and Zone Transfer. Zones are created with the New Zone Wizard and can be used for forward-lookup or reverse-lookup. The primary troubleshooting tool for working with DNS is Nslookup.exe, though ipconfig and Event Viewer can also be helpful.

## Installing, Configuring, Managing, Monitoring and Troubleshooting DHCP in a Windows 2000 Network Infrastructure

DHCP - Dynamic Host Configuration Protocol (see [Overview](#)) - allows for dynamically distributing IP addresses and all associated configuration data through an open standard. Clients are given leases to define the amount of time their address information is valid. Every client will automatically try to extend the lease when half the time of the lease has expired (if it fails, it will keep trying for the duration of the

lease). DHCP is installed as a service on Windows 2000 through the use of wizards that follow the networking services subcomponent of the Add/Remove Programs applet. After installing the DHCP service, you gain the DHCP snap-in and must define at least one scope on the server (KB# [Q169289](#)).

A scope is a range of IP addresses that can be issued to clients on a subnet by the DHCP server. DHCP does not only issue addresses from the address pool/scope, but also issues lease information and other IP configuration data (default gateway, subnet mask, etc.). Scopes are created with the New Scope Wizard - which also allows you to add exclusions, configure the router, define Domain Name and DNS Server options, and specify any WINS settings.

A superscope (KB# [Q255999](#)) is used to support a supernetted (multiple network addresses or subnets running on the same segment) network with a Windows 2000 DHCP server. This is accomplished through the New Superscope command that appears on the popup menu after right-clicking on a DHCP server within the DHCP snap-in.

In Windows 2000, a DHCP server cannot provide services to clients until it has been authorized. This is accomplished by adding the IP address of the DHCP server into Active Directory. To accomplish this, right-click on the server within the DHCP snap-in and choose the Authorize command from the popup menu. Should you need to reverse the process, right-clicking the server now brings up an Unauthorized option that can be chosen.

The DHCP server must also be configured to use DDNS, and can be done at the scope, or server level. On the properties tab of either the scope or server, choose the DNS tab and check the box to Automatically update DHCP client information in DNS. If you do not do this (or do not enable DNS for DDNS, as well), then you do not have Dynamic DNS.

Multicasting involves sending a message to a select group of recipients through the use of class D IP addresses. This is useful for conserving bandwidth: if a data packet needs to be sent to 300 out of 600 users, you need send it only once (to the class D address) rather than the 300 times unicasting would require. MADCAP (Multicast Address Dynamic Client Allocation Protocol) works like DHCP, but is used to issue multicast addresses only. To begin the process of issuing multicast addresses, right-click on the server in the DHCP snap-in and choose New Multicast Scope from the popup menu. This, in turn, starts the New Multicast Scope wizard. Multicast addresses must fall within the Class D range of 224-239.

The DHCP snap-in is used for managing and monitoring DHCP. Through it you can work with the database files, remove leases, and modify scopes.

## **Configuring, Managing, Monitoring, and Troubleshooting Remote Access in a Windows 2000 Network Infrastructure**

In Windows 2000, the Routing and Remote Access Service (RRAS) is installed automatically, though not activated. The Routing and Remote Access Server Setup Wizard can assist with the configuration, and setup of parameters. Supported protocols are:

- AppleTalk
- IPX

- NetBEUI
- TCP/IP

A Remote Access Policy (see [Operation Guide](#)) defines actions that can be undertaken for a user or group of users that connect. A Remote Access Dial-in Profile allows you to define: Dial-in Constraints, IP Address Assignment Policy, Multilink (aggregation of multiple analog phone lines through multiple modems for greater bandwidth - see KB# [QB235610](#)), Authentication, and Encryption (No Encryption, Basic or Strong). A key feature of Windows 2000, versus older operating systems, is that it supports Multilink for both incoming and outgoing communications.

Authentication can be accomplished through the use of the following, which may be used in conjunction with one another (KB #[Q227815](#)):

- CHAP - Challenge Handshake Authentication Protocol - one-step above PAP in that it does not use clear-text passwords
- EAP- Extensible Authentication Protocol - the client and the server negotiate the protocol that will be used, in much the same way that networking protocols are determined. Possible choices include one-time passwords, username/password combinations, or access tokens.
- MS-CHAP - Microsoft Challenge Handshake Authentication Protocol - requires the client to be using a Microsoft operating system (version 2), or a small handful of other compatible OSes (version 1)
- PAP - Password Authentication Protocol - uses a plain-text password authentication method and should only be used if the clients you support cannot handle encryption
- SPAP - Shiva Password Authentication Protocol - a shade above PAP, it is there for backward-compatibility and is not favored for new installations

Remote Access Dial-in Profiles can be configured and govern security in much the same way group policies do. Of key importance during the creation of the Remote Access Dial-in Profile is the Advanced tab, which allows you to add connection attributes to be used with RADIUS (Remote Authentication Dial-In User Service). With RADIUS, all authentication requests heard by a server are sent to a RADIUS server for approval/denial. RADIUS is an open standard defined by RFCs [2138](#), [2139](#), and [2548](#).

By default the Authentication provider is Windows Authentication, but it can be changed to RADIUS authentication using Internet Authentication Service. IAS is used for centralized administration, and enforcement of access policies. It works with PAP, CHAP, MS-CHAP, and EAP. It can be used to enforce (through policies) such issues as:

- RADIUS clients allowed
- Incoming phone numbers to accept
- Type of media being used to establish the connection
- User membership in security groups
- Time of allowed access (day, hour, etc.)

IAS is also useful for centralized auditing, scaling systems for growing demand, remote monitoring of usage, and working with a graphical interface through an MMC snap-in.



A Virtual Private Network (VPN) is an extension of the physical network. Rather than restricting the network to local cabling, it uses the Internet as a segment backbone. Windows 2000 has two main encryption protocols that are used with the Virtual Private Network:

- MPPE (Microsoft Point-to-Point Encryption) is used with PPTP (Point-to-Point Tunneling Protocol). PPTP was developed by Microsoft and others. It has not been widely adopted by most of the Internet community. MPPE can use 40-bit, 56-bit, and 128-bit (North America only) encryption.
- IPSec (IP Security Protocol) - an open protocol suite that relies on L2TP (Layer 2 Tunneling Protocol) for encrypting user names, passwords, and data. IPSec is used to negotiate the secure connection utilizing DES (Data Encryption Standard/ 56-bit), and 3DES (Triple DES).

Connections are configured to use MPPE (PPTP) or IPSec (L2TP) through the Network and Dial-up Connections applet. Right-click on any connection within the folder and choose Properties from the popup menu, then choose the Network tab for RAS and protocols, and the Security tab for authentication and data encryption.

The Routing and Remote Access Manager (under the Routing and Remote Access portion of Administrative Tools) is used to configure Routing and Remote Access for DHCP Integration, as well as remote access security. Monitoring remote access is done through counters in the Performance utility, and the RRAS MMC console can be used to configure incoming connections and other features.

## **Installing, Configuring, Managing, Monitoring, and Troubleshooting Network Protocols in a Windows 2000 Network Infrastructure**

Since so many of the features of Windows 2000 are dependent upon TCP/IP, it is installed by default. In addition to TCP/IP, you can also install other protocols for compatibility with other operating systems, and other services as needed.

NetWare integration can use the NWLink protocol (KB# [Q203051](#)) for IPX/SPX-compatibility needed by NetWare servers that do not use TCP/IP. Gateway Services for NetWare (GSNW), and File and Print Services for NetWare (FPNW) can be installed on a server running NWLink to provide full connectivity with the NetWare network.

Network Bindings represent the **order** in which protocols are tried as clients and servers attempt to communicate. Communication will be tried in the binding order until a common protocol is found between both the client and server. For optimization purposes, the binding order should be from the most often used protocol to the least so a common language can be found quickest. Unneeded protocols should be removed to reduce traffic.

A TCP/IP packet filter can be used to prevent types of packets from reaching your network server. These are configured through the Advanced button on the TCP/IP protocol properties. Filters can be set for TCP, UDP, or IP protocol numbers, and can be universal (for all adapters), or individual. The filter can accept, deny, or accept within specified conditions (always respond using IPSec, use Perfect Forward Secrecy, etc.).

Common ports to allow/deny include:

| Port | Service       |
|------|---------------|
| 20   | FTP (data)    |
| 21   | FTP (session) |
| 23   | Telnet        |
| 25   | SMTP          |
| 80   | HTTP          |
| 110  | POP3          |
| 143  | IMAP          |

IPSec (see the [Step-by-Step Guide to Internet Protocol Security](#)) is used to secure packets between two hosts and cannot be used locally, while EFS is used locally and does not encrypt data on a network. Kerberos V5 Authentication is in place on Windows 2000 domains and can be configured to interact with other MIT-based operating systems (allowing other clients access to active directory resources). In addition to Kerberos, IPSec also supports certificates, and the use of reusable passwords (pre-shared keys). The IP Security Policy Management MMC console is used to manage IPSec. You can right-click on the IP Security Policies folder for the popup menu that contains the choice New IP Security Policy to create a new policy. This, in turn, brings up the IP Security Policy Wizard to walk you through the creation of rules.

Network Monitor comes with Windows 2000 and is a subset of the fuller version in SMS. It can be used to capture real time activity, create filters, view and save data to a file. (See [SMS 2.0 Cramsession](#) for Network Monitor information.)

## Installing, Configuring, Managing, Monitoring, and Troubleshooting WINS in a Windows 2000 Network Infrastructure

When mixing Windows 2000 with older NetBIOS systems, the Windows Internet Naming Service (WINS) can be used to resolve "computer" names to IP addresses. Just as HOSTS files could be used in place of DNS on a small network, LMHOSTS files (KB# [Q101927](#)) can be used in place of WINS on a very small network.

WINS (see the [Overview](#)) is installed as a service on a Windows 2000 server, using the Windows Components section of the Add/Remove Programs applet in Control Panel. Beneath it, you choose Networking Services, then Windows Internet Name Service (WINS). After installation, administration is done through the Windows Internet Name Service utility (a snap-in) beneath the Administrative Tools folder.

On the client end, configuration is done through the Advanced tab of TCP/IP properties dialog box.

There are four components to WINS:



1. WINS Servers
2. WINS Clients - use directed communication with the WINS servers.
3. Non-WINS Clients - use broadcasts to WINS proxy computers that communicate with the WINS servers.
4. WINS Proxies - intercept broadcasts on their subnet and communicate with a WINS server on behalf of a client.

Multiple WINS servers use a push/pull relationship between them, wherein one can push or pull from another. Windows 2000 has a new feature that allows one server to be manually or automatically linked in a push/pull relationship with another WINS server in the network. For automatic configuration, every WINS server announces its presence with broadcasts and if one is found without a push/pull partner, it gets added into the replication list of an existing server. For manual configuration, choose the New Replication Partner option from the Replication Partners node of the server.

During replication, data is replicated at the record level using an incremental version ID. Replication occurs on a regular basis, but can be forced at any time by right-clicking on a partner and sending an immediate trigger to the partner.

WINS employs several different broadcast/traffic types:

- B-node - broadcast node: used by older clients
- P-node - point-to-point node: used by newer clients
- H-node - hybrid node: first attempts to use P-node resolution then B-node
- M-node - modified node: a hybrid that first tries B-node, then P-node

The typical order for NetBIOS resolution methods can be found in the [TCP/IP Cramsession](#).

The WINS MMC snap-in used for interacting with the WINS service, and viewing WINS statistics.

## **Installing, Configuring, Managing, Monitoring, and Troubleshooting IP Routing in a Windows 2000 Network Infrastructure**

Windows 2000 uses RRAS, which is truly a multiprotocol router. It is capable of working with static routes, dynamic routing, and demand-dial routing. Given this, an individual host can have its data packet sent in three ways:

- By looking at the default gateway address in the IP configuration
- By using Internet Control Message Protocol (ICMP) redirects to find a route to a destination host.
- By listening to traffic between routers utilizing RIP (Routing Information Protocol) or Open Shortest Path First (OSPF). This is known as dynamic routing.

Static routing uses a routing table that does not change. It is configured by the administrator and must be manually changed, edited, and updated as needed. Dynamic routing can use either Distance vector routing or link state routing technologies. Distance vector routing is the oldest and most common - building the routing tables on information learned from other routers. RIP is a distance vector

protocol using hop count as the metric for measuring the number of routers that must be crossed to reach a network - the maximum number of hops in a path is 15.

Link state routing protocols differ in that they only send information about routes that have changed via link state advertisements (also known as flooding). They also differ in that knowledge gained is obtained first hand and not passed on through other routers. OSPF is a link state routing protocol that uses link state advertisements (LSAs) to communicate. OSPF has more features and functionality than RIP and is considered "loop-free", with a maximum metric limit of 65,535.

The **route** command is used to configure static routes and for troubleshooting. **route -p** will list all the routes that the computer knows about. The Address Resolution Protocol (ARP) resolves IP addresses to hardware addresses (MAC addresses).

Demand Dial Routing (also known as Dial on Demand: DoD) is used to send packets across a dial up link between two routers that have Routing and Remote Access Services installed. The connection can be made through a modem, ISDN line, or direct (serial/parallel) connection. Demand Dial Security allows the administrator to add features such as authentication, encryption, callback, caller ID, etc.

RRAS routing is installed/configured through the RRAS MMC snap-in by right-clicking on the server and choosing Configure and Enable Routing and Remote Access on the popup menu. This starts the RRAS Setup Wizard which allows you to configure remote client protocols, demand-dial connections, IP addresses (or use DHCP), and other parameters. RIP and OSPF are installed by right-clicking the General node beneath IP Routing in the RRAS MMC console: from the popup menu, choose New Routing Protocol and the New Routing Protocol dialog box prompts for all configuration data.

## Installing, Configuring, and Troubleshooting Network Address Translation (NAT)

Internet Connection Sharing (ICS) is a service that allows you to provide automated demand-dial capabilities on a small network, such as a home office (see the [ICS FAQ](#)). This can be used for any number of processes, including:

- DNS Proxy
- DHCP
- NAT

There are a number of features available within ICS that are not available in the full-blown NAT implementation. These include Directplay Proxy (for playing games across a router), H.323 Proxy (for Microsoft NetMeeting Calls), and LDAP Proxy (to register with an Internet Locator Service server for NetMeeting). When installed, ICS sets the IP address of the LAN interface to 192.168.0.1. It also installs AutoDHCP, DNS Proxy, and a WAN interface (modem) for a demand-dial router to your ISP.

While ICS is intended for small networks, NAT (Network Address Translation) is for large networks concerned about conserving IP addresses and/or security. NAT translates between two different networks, allowing you to have a private scope internally and still communicate with the Internet. Utilizing NAT, only one machine (the NAT) need have a valid IP address for the Internet, and all the internal clients can have private addresses (10.0.0.0 for Class A, 172.16.0.0. for Class B, 192.168 for Class C).

NAT works by having at least two different IP addresses - the valid one for the Internet, (it can even support more than one), and an internal one for the network you are running. Its job is to determine if packets are for the internal or external network and route them accordingly - readdressing as needed to translate between the two worlds. NAT will not run on Windows 2000 Professional (requiring Windows 2000 Server or Windows 2000 Advanced Server), while ICS will run on all three platforms.

Configuration of NAT is done through the Routing and Remote Access MMC snap-in, meaning that RRAS must be activated before NAT can be employed. Windows 2000 includes the NAT DHCP service which is used in place of the standard Windows 2000 DHCP service. NAT Interfaces define connection properties for the network address translation, and are what define what is the internal network and what is the external network. The properties of the NAT interface allow you to map special ports, and add reserved addresses and address pools.

## **Installing, Configuring, Managing, Monitoring, and Troubleshooting Certificate Services**

Certificate Services are included with Windows 2000 for securing intranet and extranets communications. They utilize public keys (known by all) and private keys (known only by you). The two keys work with each other to encrypt (scramble) and decrypt (unscramble) data, or sign the data. The purpose of a digital signature is to guarantee that data is from the user it is supposed to be from and it has not been altered. Signing uses encryption but adds origin and authenticity as well.

Stand-alone Certificate Authority (CA) servers can work with or without Active Directory and are based upon Public Key Encryption (PKI). Within PKI, there are the following elements:

- Certificate authorities - who issue and revoke certificates
- Certificate publishers - who make what the CA has issued available

Within Windows 2000, CAs are divided into different roles:

- Enterprise CA - requires Active Directory
- Stand-alone CA - works in the absence of Active Directory (the only real reason to employ)

If you extrapolate out that within each category, a CA can be a root or intermediate/subordinate, there are actually four possible roles:

1. Enterprise root CA
2. Stand-alone root CA
3. Enterprise subordinate CA
4. Stand-alone subordinate CA

Certificate requests to a stand-alone CA are always set to pending status first and have to be approved by an Administrator. Root CAs can issue certificates to other CAs (intermediaries), users, servers, or other entities. Intermediate CAs can then only issue certificates to other CAs.

Microsoft Certificate Server is installed through the Windows Components section of the Add/Remove Programs utility. Choose Certificate Services from the list of components and walk through the installation wizard. During the installation, you will need to choose one of the four roles listed above. The Certificate Authority snap-in is then used to issue and revoke certificates. The Certificate Revocation List (CRL) can either be published automatically or manually through this snap-in, and you can view the list with this tool as well.

By default, the Administrator, Domain Admins, and Enterprise Admins groups have the rights to Manage, Enroll, and Read Configuration. Also, by default, the Authenticated Users group has only Enroll and Read Configuration. There are a number of individual CA permissions that can be assigned to users and groups:

- Approve Certificate
- Delete - remove objects from database
- Enroll - request new certificates
- Manage - encompasses all other permissions
- Modify Owner
- Modify Permissions
- Read - read certificates in the database
- Read Configuration
- Read Control
- Read Database
- Revoke Certificate
- Write Configuration

Encrypting File System (EFS) encrypts data locally and requires a private key to access the data (see [EFS for Windows 2000 technical overview](#)). When the key is also stored locally, then to the user it looks as if the data is in normal form - but if someone without the proper key attempted to view the data, it would appear scrambled and unusable. For true security, the keys should be stored on removable media (such as a floppy) and stored away from the computer.

NOTE: you cannot combine encryption with compression in Windows 2000. Choosing to encrypt a file (by clicking a checkbox on the properties attributes) prevents you from compressing the file (also accomplished by a checkbox). Likewise, compressing a file prevents you from encrypting it: in Windows 2000, the two are mutually exclusive.

The EFS Recovery Policy is detailed in KB# [Q230490](#), and you can remove the recovery keys from the system through the Group Policy Editor snap-in. Go to Computer Configuration, and then Security Settings and Public Key Policies. Right-click on Encrypted Data Recover Agents and choose Delete Policy.

Special Thanks to [Emmett Dulaney](#) for contributing material for this Cramsession. Make sure to visit his site at:  
<http://www.certificationcorner.com/>