

# Re: definition

---

*Source:*

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.general/2007-12/msg00313.html>

---

- *From:* karthiraja G <[karthirajaG@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:karthirajaG@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 25 Dec 2007 11:05:01 -0800
- 

F6K8W-MTFJM-R6JGF-JBWHP-7RPXR1  
RWT8X-VRQVM-X6JWG-DCBGG-QYXD41  
X3MPV-PXVVB-DRKWC-X36XC-KD4YY1  
VXRRQ-FYHDM-WRYC2-2WPY2-2J8KR1  
2RYRX-M6KMC-F4BD4-844QF-BW4WF1  
2RYRX-M6KMC-F4BD4-844QF-BW4WF1  
DHX6X-274J7-DVY84-2X6MJ-JFQYV1  
WP8MY-P37RD-JC6R2-FVX2R-673GT1  
WMQRG-4DJDF-GC2H6-8TX4X-86TD41  
BKDPW-RQ76R-YXYDQ-QCX6W-4PDR71  
GFQPG-48H7X-QTF8B-DCQBG-VHTMT1  
DFMPG-TJDX7-3PRR7-RGDT4-DX2KW1  
3Q6HC-QV2PQ-F84QB-WH2M4-9VJ721  
CGHR6-2X3QH-X48F8-H3QB4-WBJYV1  
37YGX-KWCJQ-4PR2Q-P6JF7-8DM8G1  
FTVBC-TCGP2-Q3VT3-FPHYG-7WBPX1  
R4D7W-MQ2YP-TXW7T-WDVCD-B3RYB1  
VF87F-G8C8K-TJPYJ-Q2DYV-6JK781  
RD7WB-BXV2C-TCF44-KCM64-3J9KG1  
42FMC-M7DH6-PGJF4-P3BVH-KTHWG1  
73CHQ-YKM44-HM7J3-GVHDT-HF6991  
VTQ7B-C24BP-J8GRR-QTGRG-23BR21  
WFCKK-8DTX8-TR8B6-4BW2M-4KYTP1  
WXT4R-YK63W-6WYTQ-6XBXV-Q3PTR1  
MR66H-CBP4Q-63BFV-F7RRW-37F8H1  
RQC3R-3FQ47-TW4V8-YG88K-P7BPX1

"karthiraja G" wrote:

Thanks for your help John

- 1.ADS
- 2.GPO
- 3.FSMO
- 4.ZONES
- 5.RAID

- 6.TRUST
- 7.DNS
- 8.DHCP
- 9.DFS
- 10.TERNIMAL SERVICES
- 11.RDP

### 1. Active Directory Service

---

A Microsoft active directory, in simple terms, is like a giant telephone book that organizes within it all of the computers and people that have been entered into it. In our case our active directory is called ADS (for Active Directory Service). Unlike a telephone book however ADS is not sorted alphabetically, but rather like the yellow pages by category, in our case by department. This allows us to mimic the universities administrative structure for Academic Support departments.

Administrators use an active directory to apply policies to objects (computers and users), put people into security groups (to allow and deny access to resources), and to better keep track of things in groups (called Organizational Units). Clients can make use of an active directory to look up names, phone numbers and any number of other attributes allowed by administrators.

ADS is more than this though. It is the central authentication domain used by Quest and to log onto Academic Support computers, to name a few. It is synchronized regularly with UWdir. Many corporate resources authenticate against ADS and it makes our lives easier by giving us one central place to maintain these accounts.

2.Group Policy Object (GPO) is a collection of settings that define what a system will look like and how it will behave for a defined group of users. Microsoft provides a program snap-in that allows you to use the Group Policy Microsoft Management Console (MMC). The selections result in a Group Policy Object. The GPO is associated with selected Active Directory containers, such as sites, domains, or organizational units (OUs). The MMC allows you to create a GPO that defines registry-based polices, security options, software installation and maintenance options, scripts options, and folder redirection options.

3.Flexible single master operation (FSMO, F is sometimes floating ; pronounced Fiz-mo), or just single master operation or operations master, is a feature of Microsoft's Active Directory (AD). Recently, as of 2005, the term FSMO has been deprecated in favour of operations masters.

FSMOs are specialised domain controller (DC) tasks, used where standard data transfer and update methods are inadequate. AD normally relies on multiple peer DCs, each with a copy of the AD database, being synchronised by multi-master replication. The tasks which are not suited to multi-master

## Re: definition

replication, and are viable only with a single-master database, are the FSMOs.

### 4.Zones

Domain Name System (DNS) servers save all resource records in a special file called a zone file. This is a plain-text file that can be edited with any text editor. In Windows 2000 these files are usually located in the %systemroot%\system32\dns directory and have a .dns extension.

Windows 2000 DNS zones that store records in these text files are called standard primary and standard secondary zones. The third zone type supported in Windows 2000 Active Directory (AD) is an integrated zone. The records of these zones are not saved in text files anymore, but rather, are saved as objects in Active Directory.

Another advantage of AD integrated zones is security. You can now turn on Secured Dynamic Updates and thus allow only authorized clients to update records in DNS. In addition, every resource record gets an ACL similar to ACL files on NTFS partitions.

AD integrated zones aren't perfect, though. The biggest disadvantage can be performance degradation. Because all data is in AD, you can expect the rate of dynamic updates to decrease by a factor of two.

### 5.RAID (Redundant Array of Independent Disks)

Redundant Array of Independent (or Inexpensive) Disks, a category of disk drives that employ two or more drives in combination for fault tolerance and performance. RAID disk drives are used frequently on servers but aren't generally necessary for personal computers.

There are number of different RAID levels:

Level 0 — Striped Disk Array without Fault Tolerance: Provides data striping (spreading out blocks of each file across multiple disk drives) but no redundancy. This improves performance but does not deliver fault tolerance. If one drive fails then all data in the array is lost.

Level 1 — Mirroring and Duplexing: Provides disk mirroring. Level 1 provides twice the read transaction rate of single disks and the same write transaction rate as single disks.

Level 2 — Error-Correcting Coding: Not a typical implementation and rarely used, Level 2 stripes data at the bit level rather than the block level.

Level 3 — Bit-Interleaved Parity: Provides byte-level striping with a dedicated parity disk. Level 3, which cannot service simultaneous multiple requests, also is rarely used.

Level 4 — Dedicated Parity Drive: A commonly used implementation of RAID, Level 4 provides block-level striping (like Level 0) with a parity disk. If a data disk fails, the parity data is used to create a replacement disk. A disadvantage to Level 4 is that the parity disk can create write bottlenecks.

Level 5 — Block Interleaved Distributed Parity: Provides data striping at the byte level and also stripe error correction information. This results in excellent performance and good fault tolerance. Level 5 is one of the most

## Re: definition

popular implementations of RAID.

Level 6 — Independent Data Disks with Double Parity: Provides block-level striping with parity data distributed across all disks.

Level 0+1 A Mirror of Stripes: Not one of the original RAID levels, two RAID 0 stripes are created, and a RAID 1 mirror is created over them. Used for both replicating and sharing data among disks.

Level 10 A Stripe of Mirrors: Not one of the original RAID levels, multiple RAID 1 mirrors are created, and a RAID 0 stripe is created over these.

Level 7: A trademark of Storage Computer Corporation that adds caching to Levels 3 or 4.

RAID S: EMC Corporation's proprietary striped parity RAID system used in its Symmetrix storage systems.

## 6. TRUST

When you establish a trust relationship between two domains, users in one domain can obtain access to resources that are located in another trusted domain

### Create a Two-Way Trust

To create a two-way trust between a Windows 2000 domain and the Windows NT 4.0 domain: 1. On the Windows 2000 domain controller (DC), click Start, point to Programs, point to Administrative Tools, and then click Active Directory Domains and Trusts. Right-click the appropriate domain name, click Properties, and then click the Trusts tab.

2. Under Domains that trust this domain, click Add.

3. In Trusting Domain, type NTDOMAIN, and then type a password. Note that the password must meet the minimum password requirements for the trusting domain.

4. On the Windows NT 4.0 primary DC (PDC), start User Manager For Domains. Open Policies, and then open Trust Relationships. Under Trusting Domain, click Add.

5. In Trusting Domain, type W2KDOMAIN, and then type the appropriate password.

6. On the Windows 2000-based computer, under Domains trusted by this domain on the Trust tab, click Add, type NTDOMAIN and the appropriate password. You should receive an informational message that states "The trusted domain has been added and the trust has been verified."

7. On the Windows NT 4.0 PDC, add the W2KDOMAIN domain as a trusted domain, and type the appropriate password. You should receive an informational message that states "Trust Relationship with W2KDOMAIN successfully established." The two-way trust has been established.

## 7.DNS (Domain Name System)

Domain Name System (or Service or Server), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the

## Re: definition

domain name `www.example.com` might translate to `198.105.232.4`. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

### 8. DHCP (Dynamic Host Configuration Protocol)

Dynamic Host Configuration Protocol, a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address. Many ISPs use dynamic IP addressing for dial-up users.

### 9. DFS (Distributed File System)

Distributed File System, or DFS, is a set of client and server services that allow a large enterprise to organize many distributed SMB file shares into a distributed file system. DFS provides location transparency and redundancy to improve data availability in the face of failure or heavy load by allowing shares in multiple different locations to be logically grouped under one folder, or DFS root.

The Distributed File System (DFS) technologies in Windows Server 2003 R2 offer wide area network (WAN)-friendly replication as well as simplified, fault-tolerant access to geographically dispersed files. The two technologies in DFS are as follows:

**DFS Replication.** New state-based, multimaster replication engine that is optimized for WAN environments. DFS Replication supports replication scheduling, bandwidth throttling, and a new byte-level compression algorithm known as remote differential compression (RDC).

**DFS Namespaces.** Technology that helps administrators group shared folders located on different servers and present them to users as a virtual tree of folders known as a namespace. DFS Namespaces was formerly known as Distributed File System in Windows 2000 Server and Windows Server 2003.

10. (Terminal Services ) is a component of Microsoft Windows (both server and client versions) that allows a user to access applications and data on a remote computer over a network. Terminal Services is Microsoft's implementation of thin-client terminal server computing, where Windows applications, or even the entire desktop of the computer running terminal services, are made accessible from a remote client machine. The client can either be a fully-fledged computer, running any operating system as long as the terminal services protocol is supported, or a bare-bones machine powerful enough to support the protocol (such as Windows FLP). With terminal services,

Re: definition

only the user interface of an application is presented at the client.

## 11. RDP

Remote Desktop Protocol (RDP) is a multi-channel protocol that allows a user to connect to a computer running Microsoft Terminal Services. Clients exist for most versions of Windows (including handheld versions), and other operating systems such as Linux, FreeBSD, Solaris and Mac OS X. The server listens by default on TCP port 3389.[1] Microsoft refers to the official RDP client software as either Remote Desktop Connection (RDC) or Terminal Services Client (TSC).

"John John" wrote:

karthiraja G wrote:

can any one give me definition for the below:

### 1.ADS

Alternate Dental Services. Not all customers are 100% satisfied.

### 2.GPO

Gently Persuasive Offer. The last offer you get before getting the one you can't refuse. Often used in conjunction with ADS.

### 3.FSMO

Re: definition

## Re: definition

Freshly Strewn Manure Odor. Something every country boy smells in early spring when the fields are fertilized. In a person's business, as well as personal dealings, certain things that sometimes happen can also leave a FSMO.

### 4.ZONES

Zany Overpriced Never Ending Sessions. The mainstay of psychiatry.

### 5.RAID

Random Assortment (of) Ineffective Devices. Every household or workshop has at least one drawer full of these.

### 6.TRUST

A condition that leads otherwise normally smart people to believe anything that complete strangers tell them. When a complete stranger uses the word "trust" in a conversation with you it is a sign that you are about to be taken for a ride, you should run as far away from the person as fast as you can. Not to be confused with love (or lust) which sometimes also causes people to believe anything that they are told.

### 7.DNS

Do Not Sit. The precursor to the "Wet Paint" sign. In the Victorian era in London, England, when park employees painted park benches they affixed DNS signs to the freshly painted benches. Few Londoners and nary a foreigner knew the meaning of the DNS sign and in 1846 while on a visit to London, an incident involving King Oscar I of Sweden nearly led to an international incident and the Corporation of London enacted a permanent ban on the use of DNS signs.

### 8.DHCP

Double Header Chicken Plucker. Plucks twice as many chickens in half as much time as single header pluckers.

### 9.DFS

Re: definition

Double Fault Syndrome. A medical condition that causes klutz to make the same mistake twice.

## 10. TERMINAL SERVICES