Ch01 Key Terms	
AD DS	(Active Directory Domain Services) Windows Server 2008 service that provides a centralized authentication service for Microsoft networks. Provides the full-fledged directory service that is called Active Directory in Windows Server 2008 and previous versions of Windows Server.
application partition	Partition that allows information to be replicated to administratively chosen domain controllers. An example of information that is commonly stored in an application partition is DNS data. Application partitions offer control over the scope and placement of information that is to be replicated.
attribute	Characteristics associated with an object class in Active Directory that make the object class unique within the database. The list of attributes is defined only once in the schema, but the same attribute can be associated with more than one object class.
Configuration NC	Configuration partition that contains information regarding the physical topology of the network, as well as other configuration data that must be replicated throughout the forest.
container object	An object, such as a domain or organizational unit, that is used to organize other objects.
cross-forest trust	Trust type that allows resources to be shared between Active Directory forests.
delegation	Administration of an organizational unit is tasked to a departmental supervisor or manager, thus allowing that person to manage day-to-day resource access as well as more mundane tasks, such as resetting passwords.
directory service	Allows businesses to define, manage, access, and secure network resources including files, printers, people, and applications.
DN	(distinguished name) Full name of an object that includes all hierarchical containers leading up to the root domain. The distinguished name begins with the object's common name and appends each succeeding parent container object, reflecting the object's location in the Active Directory structure.
domain	Grouping of objects in Active Directory that can be managed together. A domain can function as a security boundary for access to resources such as computers, printers, servers, applications, and file systems.
DC	(Domain controller) Server that stores the Active Directory database and authenticates users with the network during logon.
DNS	(Domain Name System) Name resolution mechanism that computers use for all Internet communications and for private networks that use the Active Directory domain services included with Microsoft Windows Server 2008, Windows Server 2003, and Windows 2000 Server.
Domain NC	Active Directory domain partition that is replicated to each domain controller within a particular domain. Each domain's Domain NC contains information about the objects that are stored within that domain: users, groups, computers, printers, organizational units, and more.
domain tree	In Active Directory, a logical grouping of network resources and devices that can contain one or more domains configured in a parent–child relationship. Each Active Directory forest can contain one or more domain trees, each of which can, in turn, contain one or more domains.
external trust	One-way, nontransitive trust that is established with a Windows NT domain or a Windows 2000 domain in a separate forest.
fault tolerant	Ability to respond gracefully to a software or hardware failure. In particular, a system is considered to be fault tolerant when it has the ability to continue providing authentication services after the failure of a domain controller.
forest	Largest container object within Active Directory. The forest container defines the fundamental security boundary within Active Directory, which means that a user can access resources across an entire Active Directory forest using a single logon/password combination.
forest root domain	First domain created within an Active Directory forest.
functional levels	Designed to offer support for Active Directory domain controllers running various supported operating systems by limiting functionality to specific software versions. As legacy domain controllers are decommissioned, administrators can modify the functional levels to expose new functionality within Active Directory. Some features in Active Directory cannot be activated, for example, until all domain controllers in a forest are upgraded to a specific level.
GUID	(globally unique identifier) 128-bit hexadecimal number that is assigned to every object in the Active Directory forest upon its creation. This number does not change even when the object itself is renamed.
inbound replication	Occurs when a domain controller receives updates to the Active Directory database from other domain controllers on the network.
IP address	Unique number used to identify all devices on an IP network. IP addresses are four octets long and are commonly expressed in dotted-decimal notation, such as 192.168.10.1.

KCC	(Knowledge Consistency Checker) Internal Active Directory process that automatically creates and maintains the replication topology. The KCC operates based on information provided by an administrator in the Active Directory Sites and Services snap-in that is located in the Administrative Tools folder on a domain controller or an administrative workstation that has the Administrative Tools installed.
leaf object	An object that refers to a resource such as a printer, folder user or group. A leaf object cannot contain other objects.
LDAP	(Lightweight Directory Access Protocol) Protocol that has become an industry standard that enables data exchange between directory services and applications. The LDAP standard defines the naming of all objects in the Active Directory database and, therefore, provides a directory that can be integrated with other directory services, such as Novell eDirectory, and Active Directory–aware applications, such as Microsoft Exchange.
link-value replication	When a change is made to the member list of a group object, only the portion of the member list that has been added, modified, or deleted will be replicated.
locator service	Active Directory DNS provides direction for network clients that need to know which server performs what function.
loose consistency	Individual domain controllers in an Active Directory database may contain slightly different information because it can take anywhere from a few seconds to several hours for changes to replicate throughout a given environment.
NC	(naming context) Active Directory partition.
object	Element in Active Directory that refers to a resource. Objects can be container objects or leaf objects. Containers are used to organize resources for security or organizational purposes; leaf objects refer to the end-node resources such as users, computers, and printers.
OU	(organizational unit) Container that represents a logical grouping of resources that have similar security or administrative guidelines.
outbound replication	Occurs when a domain controller transmits replication information to other domain controllers on the network.
partition	Portion of Active Directory database used to divide the database into manageable pieces.
publishing	Allows users to access network resources by searching the Active Directory database for the desired resource.
RODC	(Read-Only Domain Controller) Domain controller that contains a copy of the ntds.dit file that cannot be modified and that does not replicate its changes to other domain controllers within Active Directory. This feature was introduced in Windows Server 2008.
replication	Process of keeping each domain controller in sync with changes made elsewhere on the network.
rolling upgrades	Upgrade strategy based on functional levels that allows enterprises to migrate their Active Directory domain controllers gradually, based on the need and desire for the new functionality.
schema	Master database that contains definitions of all objects in the Active Directory.
Schema NC	Partition that contains the rules and definitions used for creating and modifying object classes and attributes within Active Directory.
shortcut trust	Manually created nontransitive trust that allows child domains in separate trees to communicate more efficiently by eliminating the tree-walking of a trust path.
site	One or more IP subnets connected by fast links.
SRV record	Locator record within DNS that allows clients to locate an Active Directory domain controller or global catalog.
Trust relationship	Allows access between multiple domains and/or forests, either within a single forest or across multiple enterprise networks.