Glossary

Note: Terms in italics are described in their own glossary entries.

3DES. See *Data Encryption Standard*.

A

A RR. Type identifier for a DNS *Address resource record*.

Active Directory (AD). The directory service for Windows 2000. A hierarchical, object-oriented database that stores distributed data for Windows 2000 domains, trees, and forests.

Active Directory-integrated zones. DNS zones for which zone data are stored in Active Directory. All copies of an Active Directory-integrated zone are peers and can accept changes to the zone. Zone data are replicated through Active Directory. *Zone transfers* are required only when importing data from a primary zone or exporting data to a secondary zone.

AD. Abbreviation for *Active Directory*.

address class. See *IP address class*.

address resolution protocol (ARP). A protocol used by IP to discover the hardware address of the device to which a datagram is being sent.

Address resource record. A DNS resource record that maps a FQDN to an IP address. Referred to as Host resource records when administering Windows 2000 DNS. Referred to as Host Address resource records in this book.

AH. See *authentication header*.

ARP. See *address resolution protocol*.

asymmetric cryptography. A cryptography method that uses one key for encryption and another key for decryption. Also called *public key cryptography*.

attribute. A characteristic of an object in an object-oriented database such as Active Directory; often called a property in Windows 2000.

authentication. The ability of one entity to reliably determine the identity of another entity.

authentication header (AH). A security protocol used by IPSec that provides authentication and *message integrity*.

authentication service. The Kerberos v5 component that authenticates clients and issues logon *session keys*. The authentication service also issues ticket-granting tickets that enable the client to request tickets from the *ticket-granting service*.

B

block cipher. A cipher algorithm that operates on plaintext in groups of bits, called blocks. 64 bits is a common block size.

BOOTP forwarder. See *DHCP relay agent*.

broadcast. A message that is to be received by all devices on a designated network. A special address is placed in the destination address field to designate the message as a broadcast. Typically, broadcast messages are not forwarded by routers.

bulk cipher. A symmetric encryption algorithm used to encrypt large quantities of data.

C

CA. See *certification authority*.

certificate. As part of the X.509 protocol (a.k.a. ISO Authentication framework), certificates are assigned by a trusted Certificate Authority and provide a strong binding between a party's identity or some other attribute and its public key.

certificate revocation list. A document published by a *certification authority* describing certificates issued by the authority that have expired or been revoked.

certification authority. Also certificate authority. A service such as Microsoft Certificate Server that issues digital certificates used in a public key infrastructure.

certification hierarchy. A hierarchical arrangement of multiple *certification authorities* designed to improved scalability, distribution of authority.

challenge-handshake authentication protocol (CHAP). With CHAP the server responds to a logon request with a random challenge to the client. The challenge is used to process the user's password via the MD5 hash algorithm, and the resulting hash is returned to the server. The server uses this hash to verify that the client knows its password.

CHAP. See *challenge-handshake authentication protocol*.

child domain. A Windows 2000 or DNS domain that is subordinate to another domain. For example, research.pseudo-corp.com is a child domain of pseudo-corp.com. Also called a subdomain.

child object. In a hierarchy, an object that is stored in another container. See *parent object*.

CIDR. See *Classless Inter-Domain Routing.*

cipher block chaining. A mode in which every plaintext block encrypted with a block cipher is first exclusive-ORed with the previous ciphertext block (or, in the case of the first block, with the initialization vector). For decryption, every block is first decrypted, then exclusive-ORed with the previous ciphertext block (or initialization vector).

ciphertext. Data that have been encrypted.

class-based IP addressing. IP addressing that is derived from the traditional A, B, and C *IP address classes* and allocates IP address ranges based on 8-bit boundaries.

Classless Inter-Domain Routing (CIDR). The Internet standard for *classless IP addressing*. (RFC1518)

classless IP addressing. IP addressing that uses the subnet mask to designate network IDs without regard to traditional IP address classes.

cluster. Two or more computers connected to function as one computer for some or all functions.

connection. In networking, a formally-negotiated channel for communication between two devices. The connection enables reliable data delivery to take place through mechanisms that enable detection and retransmission of damaged or lost data.

connection-oriented data delivery. Delivery of data through a network that is performed using a connection. Reliable communication is guaranteed through mechanisms for error detection and recovery.

connectionless data delivery. Delivery of data through a network that is performed without the establishment of a formal connection. Data are delivered in datagrams on a "best-effort" basis, and no error recovery is performed. Error recovery must be performed by higher-level processes.

container object. An object in a hierarchy that holds other containers and *leaf objects*.

CRL. See *certificate revocation list*.

cryptographic service provider (CSP). A code module used in a cryptographic system that creates, destroys, and uses keys to perform cryptographic operations according to specific methods.

cryptography. The use of *encryption* and *decryption* to protect information.

CSP. See *cryptographic service provider*.

D

Data Encryption Standard (DES). DES is a very widely used symmetric encryption algorithm. DES is a block

cipher with a 56-bit key and an 8-byte block size. DES can also be operated in a mode where three independent keys and three encryptions are used for each block of data; this uses 168 bits of key and provides the equivalent of 112 bits of security.

datagram. A package of data that is delivered through the network discretely and without error detection or recovery. A data unit that is delivered using *connectionless data delivery*.

dcpromo. The wizard that promotes a Windows 2000 member server or standalone server to a domain controller or demotes a domain controller to a member server.

DDNS. See *Dynamic DNS*.

decapsulation. The process whereby a protocol receives a protocol data unit and removes its header to recover its control information. The protocol uses control information in the header to enable it to deliver the data in the PDU to the appropriate upper-layer protocol.

decryption. Use of an algorithm and one or more keys to recover plaintext from ciphertext. The complementary process to *encryption*.

default gateway. See *default router*.

default router. The entry in a host's router table that identifies the router to be used for delivery of all IP datagrams that are not addressed to a network for which the routing table contains an explicit routing table entry.

delegation. The capability whereby a higher administrative authority grants specific rights to groups and individuals.

denial of service (DoS) attack. A network-based attack on a server that seeks to deny service to users by monopolizing server connection resources.

DES. See *Data Encryption Standard.*

DHCP. See *dynamic host configuration protocol.*

DHCP relay agent. A router component that forwards DHCP messages between clients and servers on different networks.

Diffie-Hellman key agreement. An algorithm for generating shared-secret keys without exchanging any keying material.

digital certificate. An attachment to a data stream that confirms the sender's identity or that encrypts the data.

digital key. A cipher key–based numeric value that is sufficiently large to make it difficult to determine by random attack.

digital signature. Digital signatures utilize public key cryptography and one-way hash functions to produce a signature of the data that can be authenticated, and is difficult to forge or repudiate.

Digital Signature Standard (DSS). A standard for digital signing, including the Digital Signing Algorithm, approved by the National Institute of Standards and Technology.

distinguished name. The complete pathname that uniquely identifies an object in the Active Directory. A distinguished name is constructed by concatenating the names of all domains that associated a leaf object with the root domain, including a domain type identifier, in sequence proceeding from the root domain to the leaf object. For example, /O=Internet/DC=COM/DC=Pseudo-Corp/CN=Users/CN=Drew Heywood.

DNS. See *Domain Name System.*

DoD protocol model. Traditional name for the *Internet protocol model*, reflecting the origins of the Internet as a research project by the United States Department of Defense.

domain controller. A computer that stores a copy of a domain database and can authenticate users. Under Active Directory, every domain controller can be used to modify the database for its domain.

domain name. A host's complete name in the DNS namespace. See *fully qualified domain name*.

Domain Name System (DNS). A distributed Internet database that was originally developed to enable TCP/IP hosts to match domain names to IP addresses. Since its introduction, DNS has been extended to provide additional types of information. Windows 2000 uses DNS as its location service to discover network resources.

domain tree. A hierarchy of Windows 2000 or DNS domains cross-referenced to form a unified namespace.

dotted decimal form. A method of representing 32-bit *IP addresses* and *subnet masks* using four integers ranging in value from 0 through 255, each representing eight bits of the address. When notated, the integers are separated by periods.

downlevel operating system. Microsoft operating systems released prior to Windows 2000, including Windows 3.x, 9.x, and NT.

Dynamic DNS (DDNS). A feature that enables DNS clients (computers and processes) to dynamically update DNS records, reducing the need to manually modify zone data. Active Directory uses DDNS to update Service resource records. Windows 2000 clients use DDNS to update Host Address and Pointer resource records.

dynamic host configuration protocol (DHCP). A protocol for assigning dynamic IP addresses and other configuration settings to IP computers. (RFC2131)

dynamic ports. *Ports* in the range 49152–65535 that can be assigned by network administrators to locally defined processes.

E

EAP. See *extensible authentication protocol.*

encapsulating security payload (ESP). An encapsulation protocol used by IPSec to provide encryption, *message integrity*, and confidentiality.

encapsulation. The process whereby a protocol in a network protocol stack appends a header containing the protocol's control information to data that the protocol receives from upper layers in the protocol stack.

encryption. Use of an algorithm and one or more keys to convert plaintext to ciphertext.

enrollment. The process of issuing a *certificate* to a client by a *certification authority.*

enterprise CA. A Windows 2000 *certification authority* that is integrated with Active Directory.

ESP. See *encapsulating security payload.*

Ethertype. A code stored in the Ethertype field of the Ethernet II packet header that identifies the Internet layer protocol that is associated with the data payload of the packet. Also etype.

extensible authentication protocol (EAP). An extension of PPP that varies the sequence of messages that are presented in a user authentication dialog. Rather than using a fixed sequence of messages, as is done by MS-CHAP and SPAP, the devices negotiate the use of a specific EAP authentication scheme while the connection is being established.

F

first-level domain. A Windows 2000 or DNS domain whose parent domain is the root domain.

forest. One or more domain trees that don't form a contiguous namespace but that share a common schema, configuration, and global catalog.

FQDN. See *fully qualified domain name.*

frame. The term used to describe protocol data units with some protocols such as token ring. Similar to *packet.*

frame check sequence. A checksum value that is appended to the end of a packet and is used by the receiving

computer to determine if the packet was damaged in transit.

fully qualified domain name. The complete name of a host in the DNS namespace, consisting of the hostname concatenated to the names of all domains between the host and the root domain. Proceeding from left to right, the FQDN consists of the host's name concatenated with the names of all domains between the host and the root domain. Names are separated with periods.

G

gateway. In TCP/IP, the historical name for a *router*.

Global Catalog. An index containing every Active Directory object in a forest but describing only select attributes of each object. The Global Catalog facilitates location of commonly used objects.

H

handshake. An initial negotiation between client and server that establishes the parameters of their transactions.

hardware address. See *MAC address*.

hash code. Another term for *message digest*.

hash function. An algorithm that processes data to generate a *hash code* that is unlikely to result by applying the same algorithm to different input data. Hash algorithms are designed such that it is computationally inefficient to recover the original data by processing the hash code. Secure hashing algorithms include a public *seed* and a private *key* in the inputs. The seed value ensures that a given key will not generate the same hash code more than once when processing the same data. A key that is known only to the sender and receiver ensures that other users cannot modify the data and use the same function and seed to generate a new, valid hash code. See also *message digest* and *one-way transform.*

hash signature. Another term for *digital signature*.

hashed message authentication code (HMAC). The standard message authentication algorithm for Internet communications. HMAC can make use of the MD5 and SHA *message digest* algorithms. (RFC2104)

header. A series of bits containing control information for a network protocol. The protocol header is appended to the beginning of data received from upper protocol layers to construct the protocol data unit for the protocol.

hexadecimal. Numbers written using a base of 16 (versus the familiar decimal numbers, which are written with a base of 10). Hexadecimal, or simply "hex," numbers are often written with the prefix 0x. For example, 0x800 indicates that 800 is to be interpreted as being written in hexadecimal.

HMAC. See *hashed message authentication code.*

HMAC-MD5. Implementation of the *hashed message authentication code* standard using the *MD5* algorithm.

HMAC-SHA. Implementation of the *hashed message authentication code* standard using the *secure hash algorithm*.

host. Traditional name for any device on a TCP/IP network that is assigned a unique IP address.

host ID. A number that uniquely identifies an IP host on a network. Also *hostid*.

hostid. See *host ID.*

Host-to-Host Layer. The layer in the *Internet protocol model* that is above the *internet layer* and below the *process/application layer.* The primary purpose of protocols at this layer is to oversee end-to-end network delivery of data. Protocols at this layer are identified by protocol numbers that are embedded in the IP header.

HTTP. See *Hypertext Transfer Protocol.*

Hypertext Transfer Protocol (HTTP). The protocol used to send HTML objects on the World Wide Web.

I

IANA. See *Internet Assigned Numbers Authority*.

ICMP. See *Internet Control Message Protocol*.

IETF. See *Internet Engineering Task Force*.

inheritance. The capability of a child object to automatically acquire specific properties from a parent object.

initialization vector. When a block cipher is used in CBC mode, the initialization vector is exclusive-ORed with the first plaintext block prior to encryption.

integrity. See *message integrity*.

Internet Assigned Numbers Authority (IANA). The organization that registers ports, protocol numbers, and other identifiers used on the Internet. See http://www.iana.org.

Internet Control Message Protocol. A protocol, required in all IP implementations, that sends and returns various types of diagnostic messages.

Internet Engineering Task Force (IETF). The organization that is responsible for research and development of official Internet standards. Standards are described in *Requests for Comments*.

Internet Layer. The layer in the *Internet protocol model* that is above the *network access layer* and below the *host-to-host layer*. Protocols at this layer are identified by Ethertype numbers that are embedded in the network access layer protocol header.

internet protocol (IP). The principle protocol in the Internet (TCP/IP) protocol stack. Situated at the internet layer of the Internet protocol model, IP is responsible for delivery of datagrams between hosts on the same network and for routing datagrams on internetworks. (RFC791)

Internet protocol model. A four-layer model establishing the architecture around which TCP/IP protocols are designed. See also *DoD protocol model.*

internetwork. Two or more networks that communicate through routers. A "network of networks." Each network in the internetwork must be identified by a unique network ID.

IP. See *internet protocol*.

IP address. A 32-bit number that uniquely identifies a device on a TCP/IP network. The address encodes both the network and the computer identification and is typically represented in *dotted decimal form*.

IP address class. For IP addresses, one of five subgroups of available IP addresses, identified as Class A through Class E.

IP address spoofing. A technique for concealing the system that originated an IP datagram by storing the IP address of another system in the Source Address field of the IP header.

IP security. Extensions to IP that provide authentication and encryption security. (RFC2401)

IPSec. See *IP security.*

K

KDC. See *Key Distribution Center.*

Kerberos. An authentication protocol, currently at version 5, developed at the Massachusetts Institute of Technology and described in RFC1510. Kerberos is characterized by distributed, mutual authentication of client and server.

key. A data pattern that is input to a cipher algorithm during encryption and decryption to ensure that data may be encrypted or decrypted only by authorized users or processes.

Key Distribution Center (KDC). A Kerberos function that controls the distribution of keys and tickets. A KDC is found on every Active Directory domain controller.

key pair. A pair of cryptographic keys consisting of a *public key* and its associated *private key*.

L

L2TP. See *layer two tunneling protocol*.

layer two tunneling protocol (L2TP). A tunneling protocol based on IPSec, developed for use in the Internet.

LDAP. See *lightweight directory access protocol*.

leaf object. In a hierarchy, an object that stores data and cannot be used to contain other objects.

lease. A DHCP server assigns an IP address to a client in the form of a lease, which may include other configuration settings. DHCP leases typically have a limited lifetime and must be periodically renewed.

lightweight directory access protocol (LDAP). A small and fast protocol, based on X.500's Directory Access Protocol, that is the default protocol for communication with Active Directory.

long-term key. A key used by Kerberos v5 to uniquely identify security principles. A long-term key is created for each security principle and is known only to the security principle and the KDC. Windows 2000 processes the user's account password with a hash function to generate the long-term key.

loopback address. Any address that causes network data traveling down the protocol stack to be returned by the network interface without forwarding the data to the network. Any IP address from 127.0.0.1 through 127.255.255.255 functions as a loopback address.

M

MAC address. An address that is usually stored in firmware on a network device. The name is derived from the media access (MAC) layer of the IEEE 802.2 standard. Also referred to as the *hardware address*.

master secret. Secure secret data used for generating encryption keys, MAC secrets, and initialization vectors.

MD5. A secure *hashing function.* (RFC1321)

message authentication code. Another term for *message integrity code.*

message digest. Alternate name for *message authentication code* or *message integrity code.*

message integrity. The security requirement to verify that a message has not been modified. Message integrity is verified through use of *message authentication codes*.

message integrity code. A one-way hash computed from a message, a key, and usually an initialization vector. It is difficult to forge without knowing the key, and it is extremely difficult to recover the original data from the result. Its purpose is to detect if the message has been altered. Also called a *message digest* and a *one-way transform*.

message replay. A form of network attack in which a user captures secure messages, changes the addressing information, and resends the messages in an attempt to gain access to a secure system.

Microsoft challenge-handshake authentication protocol (MS-CHAP). A challenge-response protocol with encryption performed on the response.

Microsoft Management Console (MMC). A user interface (UI) framework that accepts snap-in components to perform management tasks.

MMC. See *Microsoft Management Console*.

MS-CHAP. See *Microsoft challenge-handshake authentication protocol.*

multicast. A message that is to be received by a subgroup of devices on a network. A special type of address is placed in the destination address field to designate the message as a multicast. Only devices that require a specific type of multicast message will retrieve the message from the network.

multihoming. The practice of assigning two or more IP addresses to a single network interface.

multimaster replication. The capability that enables every Active Directory domain controller to modify the domain database and to replicate those changes to other domain controllers for the domain. Active Directory does not distinguish between primary and backup domain controllers, as was required by Windows NT.

mutual authentication. A feature of authentication protocols such as Kerberos v5 that requires both the client and server to be authenticated before they can form a connection.

N

name resolution. The process of querying a database to determine the address that is associated with a hostname.

namespace. A bounded area in which a name can be resolved. A namespace includes all naming information within a domain hierarchy.

NAS. See *network access service.*

NBT. See *NetBIOS over TCP/IP*.

NetBIOS over TCP/IP (NBT). Microsoft's architecture for supporting NetBIOS operations on TCP/IP networks.

NetBT. See *NetBIOS over TCP/IP*.

netid. Synonym for *network ID* that is often used when discussing IP addressing.

Network Access Layer. The bottom layer of the *Internet protocol model* consisting of protocols that transmit and receive data through the network medium.

network access service (NAS). Any service that supports network dial-in connectivity.

network ID. A number that uniquely identifies a network in an internetwork as well as all computers on the network. Also *netid*.

node type. NetBIOS node types determine whether WINS clients will attempt to resolve NetBIOS names using broadcast messages, point-to-point messages, or a combination of both message types.

non-repudiation. The security requirement that a digital signature be capable of verifying the user who digitally signed a document.

NTLM. NT LAN Manager. The authentication used by Windows NT and Microsoft LAN Manager.

O

object. A collection of attributes that describes a self-contained entity (for example, a user).

octet. A group of 8 bits.

one-way transform. Another term for *hash code*, reflecting the one-way nature of hashing algorithms.

P

packet. A bundle of binary data that is typically transmitted in a continuous stream without interruption. While the term is encountered at all protocol layers, it is most often reserved to describe the data unit for the network access layer. With some network protocols (for example, frame relay and token ring), the term *frame* is typically used instead of packet.

PAP. See *password authentication protocol.*

parent object. In a hierarchy, a container object that holds leaf objects and/or other container objects.

password authentication protocol (PAP). An authentication protocol that transmits passwords in clear text.

PDU. See *protocol data unit*.

PKI. See *public key infrastructure*.

plaintext. Data that have not been encrypted. Data that are input to a cryptosystem for encryption into ciphertext.

point-to-point protocol (PPP). A protocol developed to encapsulate data to be transported through a WAN. (RFC1661)

point-to-point tunneling protocol (PPTP). A tunneling protocol developed by Microsoft that supports all authentication methods supported for PPP.

port. A code stored in the port field of the TCP or UDP protocol header that identifies the upper layer protocol that is associated with the data payload of the PDU.

PPP. See *point-to-point protocol*.

PPTP. See *point-to-point tunneling protocol*.

primary zone. In DNS, the original copy of the zone. The primary zone is read-write and resource records in the zone can be modified. Changes made to the primary zone are replicated to *secondary zones* through *zone transfers*.

private key. The key in a public key pair that is kept secret by the owner of the key pair. The private key can be used to encrypt data such that the public key in the key pair is required to decrypt the ciphertext. The private key can be used to decrypt data that are encrypted using the public key.

Process/Application Layer. The top layer of the *Internet protocol model* consisting of protocols, processes, and applications that rely on host-to-host layer protocols to communicate through the network. Processes and applications are identified by port

numbers that are embedded in the host-to-host protocol header.

Property. A characteristic of an object. Often used interchangeably with attribute.

protocol data unit (PDU). A protocol in a protocol stack constructs a protocol data unit by appending a header containing the protocol's control information to data that the protocol receives from upper layers in the protocol stack.

protocol ID. A code stored in the protocol ID field of the internet protocol header that identifies the host-to-host layer protocol that is associated with the data payload of the IP datagram.

protocol stack. A set of related protocols that communicate in sequential fashion to enable processes to communicate through a network.

PTR resource record. A DNS resource record that maps an IP address to a (fully qualified domain) name. Often referred to as a reverse lookup record.

public key. The key in a public key pair that can be freely shared. The public key can be used to encrypt data such that the private key in the key pair is required to decrypt the ciphertext. The public key can be used to decrypt data that are encrypted using the private key.

public key certificate. A digital document that encodes a public key with owner and functional information and is digitally signed by the *certification authority* that issued it. The digital signature makes it possible to verify the integrity of the certificate. The validity of the certificate can be determined by submitting the certificate to the issuing certification authority. All certificates have a limited lifetime and must be renewed to remain valid.

public key cryptography. A class of cryptographic techniques employing two-key ciphers. Messages encrypted with the public key can only be decrypted with the associated private key. Conversely, messages

signed with the private key can be verified only with the public key.

public key infrastructure (PKI). An architecture of public key certification servers that facilitates the creation, distribution, and use of public-private *key pairs* to encrypt and decrypt data.

publication. For the Windows 2000 Certification Services, the process of issuing a certificate. For the Microsoft Security and Acceleration Server, the process of making an internal service available through the firewall to outside clients.

R

RADIUS. See *remote authentication dial-in user service.*

RAS. See *Remote Access Service.*

RC2. A block cipher developed by Ron Rivest at RSA Data Security, Inc.

RC4. A stream cipher licensed by RSA Data Security [RSADSI].

realm. For Kerberos v5, a subdivision of the overall security architecture. Windows 2000 bases Kerberos v5 realms on domains.

referral ticket. Kerberos v5 TGTs to KDCs in other domains. If a client needs to access services in another domain, the client must request a TGT from a local KDC for a KDC in the target domain.

registered ports. *Ports* in the range 1024–49151 that are formally assigned to specific protocols.

reliable data delivery. The capability of ensuring that messages are delivered to their destinations in their entirety and without error. Reliable data delivery requires a connection-oriented communication system that detects and requests retransmission of missing or damaged data.

Remote Access Service (RAS). The component of RRAS that supports dial-in connectivity.

remote authentication dial-in user service (RADIUS). A service that authenticates dial-in clients. Microsoft's implementation of RADIUS is the Internet Authentication Service. (RFCs 2138 and 2139)

replay. See *message replay.*

replication topology. The configuration of the replication scheme between domain controllers.

Requests for Comments. Documents that are primarily used to describe protocols used on the Internet and to document Internet standards protocols. Usually abbreviated *RFC*. All RFCs are identified by number, for example RFC791. RFCs can be obtained on the Internet at http://www.ietf.org.

Resource Record. An entry used to store a specific type of data in a *DNS* zone file.

RFC. See *Requests for Comments.*

root. The only container in a hierarchy that has no parent container.

root CA. The first *CA* in a *certification hierarchy*. The root CA differs from all other CAs in the hierarchy in that it is self-certified; that is, it issued its own certificate to itself. All other CAs in the hierarchy are certified by other CAs.

root domain. The top-level domain in a Windows 2000 or DNS domain tree. The only domain that does not have a parent domain.

router. A device that forwards packets between subnets based on address information found in the header for the network access layer protocol (IP).

routing. The process of using network numbers encoded in the header of an IP datagram (or in the corresponding header for other comparable protocols) to forward datagrams through internetworks for delivery to a remote destination.

Routing and Remote Access Service (RRAS). The Windows 2000 component that provides routing, demand-dial, and

dial-in support. Windows 2000's successor to Windows NT Windows NT 4 RAS.

routing table. A table of routing information that is maintained on each TCP/IP host. Except on simple networks that do not require routing, the routing table will contain at least one entry to describe the host's default route.

RR. See *Resource Record*.

RRAS. See *Routing and Remote Access Service.*

RSA. A very widely used public-key algorithm based on the factoring of large prime numbers that can be used for either encryption or digital signing.

S

scalability. The characteristic of a computing system that enables capability to be readily enhanced as demand for services increases.

schema. The definition of all the object types that AD can store.

scope. Microsoft DHCP scopes are pools of IP addresses that can be assigned to DHCP clients.

secondary zone. A DNS zone that accepts resource records transferred from the primary zone or from other secondary zones through zone transfers. A secondary zone is read-only, and zone data cannot be modified. Secondary zones are created to distribute zone processing load across multiple DNS servers and to provide fault tolerance.

secret key cryptography. See *symmetrical cryptography.*

secure hash algorithm (SHA). A hashing algorithm developed by the U.S. National Institute of Standards and Technology. While modeled on MD5, SHA uses an equivalent of 72, 32-bit constants to generate a 160-bit *message digest*. Because longer keys provide better security, SHA is regarded as being stronger than MD5, but has greater processing requirements.

Secure Socket Layer (SSL). A layer-three network security protocol developed by Netscape.

seed. In cryptography, a pseudo-random input to an encryption or hashing algorithm that is changed each time the algorithm is applied. The seed ensures that the same results are not obtained when the algorithm is used to repeatedly process the same data. The seed is included as clear text with the resulting encrypted data. Because a secret key is also input to the algorithm, the seed is insufficient to recover the original data from the encrypted output and security of the seed is not an issue.

segment. The protocol data unit for TCP.

session key. A symmetrical key that is generated and used during a single session.

session ticket. A *Kerberos* v5 ticket that contains a server's session key, encrypted with the server's long-term key. When a client is authenticated, the KDC sends a session ticket to the client, which in turn presents the session key to the server.

SHA. See *secure hash algorithm*.

Shiva password authentication protocol (SPAP). An implementation of PAP on Shiva remote client software.

shortcut trust. An explicit trust to circumvent the trust referral process between directory trees.

signed data. Data with a digital certificate attached as proof of origin or authenticity.

simple mail transfer protocol (SMTP). A protocol that provides basic electronic mail services over TCP/IP networks.

simple network management protocol (SNMP). A protocol used to exchange management information between management stations and managed devices.

site connector. The link (usually TCP/IP) over which replication between two sites occurs. You can use TCP/IP or SMTP to link two sites.

site link. A means of weighting the relative cost of replication between sites.

site. A collection of domain controllers that have high-speed connections to optimize replication and logon traffic. AD defines sites by the subnets the domain controllers are in.

smart card. A card-like device that can store *certificates* and other information used to authenticate a user. Typically, a personal identification code (PIN) must be entered when the smart card is presented.

SMTP. See *simple mail transfer protocol.*

SNAP. See *sub-network access protocol*.

snap-in. A management object that you add to the MMC to handle tasks such as AD management and disk defragmentation.

SNMP. See *simple network management protocol*.

SOA RR. See *Start of Authority Resource Record.*

SPAP. See *Shiva password authentication protocol.*

spoofing. See *IP address spoofing*.

SSL. See *Secure Socket Layer*.

stand-alone CA. A Windows 2000 *CA* that is not integrated with Active Directory and cannot use Windows 2000 services to authenticate clients.

Start of Authority Resource Record (SOA RR). A resource record that specifies contact, operational, and other properties for a DNS zone.

stream cipher. An encryption algorithm that converts a key into a cryptographically-strong keystream, which is then exclusive-ORed with the plaintext.

subnet. The term sometimes used to describe a network that is assigned a subset of the available range of IP addresses.

subnet mask. A 32-bit number that specifies the portions of an IP address that are allocated to the netid and the hostid. Bits in the IP address that correspond in position to 1-bits in the subnet mask comprise the netid. Bits in the IP address that correspond in position to 0-bits in the subnet mask comprise the hostid.

sub-network access protocol. A protocol extension that enables Ethertype information to be encoded in the headers of protocols that do not have an Ethertype field in the packet header.

symmetric cipher. See *bulk cipher*.

symmetrical cryptography. A cryptography algorithm that uses the same key for encryption and decryption. Also called *secret key cryptography.*

SYN flood. A *denial of service attack* that involves sending large numbers of TCP SYN packets with spoofed source IP addresses to a server. The server responds to the source IP address with a SYN ack and reserves connection resources for the host making the SYN request. If sufficient SYN packets are sent to the server, the server can run out of available connection resources and will be unavailable for legitimate service requests.

T

TCP/IP. Traditional name for the protocol stack used on the Internet, named after the protocols TCP and IP. Because TCP is only one of many protocols used at the host-to-host layer in the Internet protocol model, the protocol stack is increasingly referred to as the Internet or IP protocol stack.

TGT. See *ticket-granting ticket.*

ticket. A Kerberos v5 object that contains user information, access rights, an expiration time, and preauthorization data (that is, data that contains NT-specific security information).

ticket-granting service. The Kerberos v5 component that enables clients with *ticket-granting tickets* to obtain *session tickets*.

ticket-granting ticket. A Kerberos v5 session ticket for the ticket-granting service of the KDC, issued by the KDC to authenticated clients. Presenting the TGT to a KDC enables the client to request a session ticket for a particular service.

time signature. A value that is included in many authentication and secure communication algorithms that specifies when a packet or message is created. The packet cannot be used if a certain time has elapsed following the time in the time signature. Time signatures prevent *message replay.*

time to live (TTL). A property of an object that determines the length of time after creation or issue that the object is considered to be valid.

TLS. *See transport layer security*.

top-level domain. In the DNS namespace, a domain that is a child of the root domain.

transitive trust. A trust between Windows 2000 domains that allows referrals from one domain to another.

transmission control protocol (TCP). A connection-oriented, reliable protocol that functions at the host-to-host layer. (RFC793)

transport layer security (TLS). An enhanced, backward-compatible implementation of the Secure Sockets Layer protocol being developed by the IETF as a future Internet standard protocol.

tree. A hierarchical data structure consisting of container objects and leaf objects organized under a single root container.

TTL. See *time to live.*

tunneling. The encapsulation of one communication channel within another, used to implement virtual private networks.

U

UDP. See *user datagram protocol.*

unicast. A message that is intended to be received by one specific device, which is specified by the address that appears in the destination address field.

unreliable data delivery. Delivery of data on a "best effort" basis. No connection is established, and error detection and recovery are not performed.

user datagram protocol (UDP). An Internet host-to-host protocol that performs unreliable datagram delivery. (RFC768)

V

virtual private network (VPN). A communications channel formed by tunneling data protected by a secure protocol through another network. The physical network does not need to run the same protocols as the virtual network. The VPN channel functions as an extension of the private network. Typically data are encrypted for confidentiality.

VPN. See *virtual private network.*

W

well-known ports. Port numbers in the range of 0–1023, many of which are assigned to protocols that are prominent on the Internet.

Windows Internet Naming Service (WINS). A Windows 2000 or NT network service that provides NetBIOS over TCP/IP name registration and dynamic NetBIOS name-to-IP-address resolution services to network clients.

WINS. See *Windows Internet Naming Service.*

X

X.509. A digital certificate standard.

Z

zone. In DNS, a portion of the complete namespace that is managed as a unit by a DNS server.

zone transfer. The process of replicating zone data to a secondary DNS zone.