# Glossary

It's a *thingy*!

— Prairie Barnes

**Abstract Syntax Notation One (ASN.1)**

A language used to define the structure and content of objects such as data records and protocol messages, along the lines of a super-duper version of the `typedef` in C, only a lot more powerful. ASN.1 was developed as part of the Open Systems Interconnection (OSI) environment, and was originally used for writing specifications. More recently, though, tools have been developed that will generate software from ASN.1.

*See also:* Distinguished Encoding Rules

*Web reference:* The ASN.1 Consortium (`http://www.asn1.org/`)

**Astoundium**

The element of suprise.

**Attacker**

In this context, one who attacks a computer system either to gain access or, as in a "Denial of Service attack," to cause a failure in the system or data loss.

*See also:* Cracker

**Backup Browser**

A Browser node which is not elected to be the Local Master Browser, but which stores a backup copy of the Browse List and will respond to client requests for the Browse List. A Potential Browser may decide on its own to become a Backup Browser, or it may be appointed by the Local Master Browser.

*See also:* Local Master Browser, Potential Browser

**Backup Domain Controller (BDC)**

A Windows NT Domain Controller (DC) which keeps a backup copy of the user/group authentication database in an NT Domain. The master copy is maintained by the Primary Domain Controller (PDC). A Backup Domain Controller can be promoted to the role of PDC in a pinch. Only one PDC is permitted per NT Domain, but there may be any number of BDCs.

*See also:* Domain Controller, Primary Domain Controller

**BAF Protocol**

The very first name for the protocol formerly known as SMB. The SMB protocol was originally developed by Dr. Barry A. Feigenbaum at IBM and, according to legend, was originally given his initials. It was later renamed SMB and, more recently, CIFS.

*See also:* CIFS, SMB

**Bran**

Pronounced *Brahhn*. The name of my dog.

**Browser Node**

*See:* Potential Browser

**Browser Election**

The process by which a browser node on a NetBIOS LAN is chosen to be the primary repository of service information for that LAN (that is, the Local Master Browser). Under NBT, the election process takes place within the confines of the local IP subnet.

**CIFS**

**C**ommon **I**nternet **F**ile **S**ystem. The protocol formerly known as Server Message Block (SMB) and, before that, as the BAF protocol (after its original creator, Dr. Barry Feigenbaum). CIFS is a protocol for file and device sharing across a network.

*See also:* SMB

**Cracker**

One who attacks a system in an effort to break security, probably to gain unauthorized access.

Goodguy[1] crackers (sometimes called "White Hat" crackers) used to provide the very beneficial service of exposing weaknesses so that they could be fixed, but then the US Congress enacted the Digital Millennium Copyright Act (DMCA) which made talking about such things illegal in the US and potentially dangerous elsewhere.

*See also:* Attacker

*Do not see also:* Hacker

**Distinguished Encoding Rules (DER)**

A set of rules for encoding and decoding ASN.1 data for network transport. DER provides a standard format for transport of data over a network so that the receiving end can convert the data back into their correct ASN.1 format. DER is a specialized form of a more general encoding known as BER (**B**asic **E**ncoding **R**ules). DER is designed to work well with security protocols, and is used for encoding Kerberos and LDAP exchanges.

*See also:* ASN.1, Kerberos, LDAP

**Domain Controller (DC)**

An authentication server in a Windows NT or Windows 2000 Domain. A Domain Controller maintains a database of user, group, and machine accounts and other security information, and provides authentication services to the NT or W2K Domain.

In an NT Domain, one of the DCs will be designated the *Primary* Domain Controller (PDC). All security database administration is handled via the PDC, and copies of the database are then distributed to any available *Backup* Domain Controllers (BDCs). NT Domain controllers register the Group Special NetBIOS name *nt_domain*`<1C>` to identify themselves.

[1] The use of the term "good*guy*" is in no way intended to imply gender.

In Windows 2000 Domains the security database is stored in the Active Directory, and there is no distinction between primary and secondary controllers.

*See also:* Backup Domain Controller, Primary Domain Controller

### Domain Name System (DNS)

The Domain Name System is a distributed database system that provides mappings between Internet names and Internet Protocol (IP) addresses. The DNS name space is hierarchical in structure.

*Web reference:* the DNS Resources Directory (`http://www.dns.net/dnsrd/`)

### Domain Master Browser (DMB)

A host system that is designated to coordinate Browse Lists for matching workgroups across multiple subnets. The DMB receives subnet Browse List updates from Local Master Browsers, combines those lists, and distributes the combined list back to the Local Masters for the workgroup.

*See also:* Local Master Browser

### Doveryay, no proveryay

Trust, but verify.

### Encoded NBT Name

The term used in this book for the fully qualified Second Level Encoded form of the NetBIOS Name and Scope ID. For example, the string

```
"\x20EGEFCACACACACACACACACACACACACA\x2FI\x2FO\x3FUM\0"
```

is the fully encoded form of the NetBIOS name *FE*`<20>` and the scope ID “`FI.FO.FUM`”.

*See also:* NBT Name, First Level Encoding, Scope ID, Second Level Encoding

### First Level Encoding

The conversion of a NetBIOS name to a format complying with DNS “best practices.”

NetBIOS names may contain characters which are not considered valid for use in DNS names, yet RFC 1001 and RFC 1002 attempted to map the NetBIOS name space into the DNS name space. To work around this conflict, NetBIOS names are encoded by splitting each byte of the name into two nibbles and then adding the value of 'A' (0x41). Thus, the '&' character (0x26) would be encoded as "CG". NetBIOS names are usually padded with spaces before being encoded.

In this book, the term "NBT Name" is used to indicate the fully qualified form of the First Level Encoded name. The NBT Name includes the Scope ID.

*See also:* NBT Name, Scope ID, Second Level Encoding

### GSS-API

**G**eneric **S**ecurity **S**ervice **A**pplication **P**rogram **I**nterface. A generic interface to a set of security services. It makes it possible to write software that does not care what the underlying security mechanisms actually are.

*See:* RFC 2078
(`http://www.faqs.org/rfcs/rfc2078.html`)

*See also:* SPNEGO

### Hacker

One who fiddles with an existing system to see if it can be improved. Hacking is generally the fine art of [creating and] recursively revising software or a software-based system.

*Do not see also:* Cracker

### Kerberos

A network authentication service developed at MIT and later adopted by Microsoft for use with Windows 2000 and SMB over naked TCP/IP transport.

*See:* RFC 1510
(`http://www.faqs.org/rfcs/rfc1510.html`)

### LANA

NetBIOS **LAN A**dapter card.

For the original PC Network System, IBM sold both Broadband and Baseband network interface cards, which they called LAN Adapters. The NBT system supports the concept of a "virtual LANA."

*See also:* NBT

**LDAP**

The **L**ightweight **D**irectory **A**ccess **P**rotocol. A standard protocol used to access directory services based on the X.500 directory service model (e.g., Novell Directory Services and Microsoft Active Directory).

*See:* RFC 2251 (`http://www.faqs.org/rfcs/rfc2251.html`)

**Local Master Browser (LMB)**

A host system that is "elected" to manage the Browse List for the local IP LAN. The LMB collects service announcements from servers on the local LAN, distributes the Browse List to any Backup Browsers on the LAN, and exchanges service lists with the Domain Master Browser (if there is one).

*See also:* Domain Master Browser, Backup Browser

**Machine Name**

Host name. A name which is typically assigned in the system configuration and used as the base name creating the NetBIOS names of several important services. The service names are composed by appending a service-specific suffix to the machine name.

**Master Browser**

A common shorthand for "Local Master Browser."

*See:* Local Master Browser

**MIDL**

**M**icrosoft **I**nterface **D**efinition **L**anguage, Microsoft's version of the **I**nterface **D**efinition **L**anguage (IDL). MIDL is used to specify the parameters to MS-RPC function calls. MIDL is also used to define the interfaces to Microsoft's **D**ynamically **L**inked **L**ibrary (DLL) functions.

*See also:* MS-RPC

**Moore's Law**

The observation (by Gordon Moore) that the transistor density on computer chips doubles roughly every 1.5 years. This is generally taken to mean that processing speeds also double every 1.5 years. Software developers compensate by writing bad code and adding unnecessary features to maintain status quo.

**MS-RPC**

**M**icro**s**oft **R**emote **P**rocedure **C**all. RPC in general is a system that allows a process on one system to make function calls against libraries on another system. MS-RPC is Microsoft's implementation of RPC.

*See also:* MIDL

**NBDD**

**N**et**B**IOS **D**atagram **D**istribution Server. This server relays broadcast and multicast (group) datagrams to all intended recipients.

When a P, M, or H node wishes to send a broadcast or multicast datagram, it will send the datagram to the NBDD. The NBDD will obtain the list of destination IPs from the NBNS and then unicast the datagram to each of those nodes.

Most implementations do not provide NBDD support.

*See also:* NBNS

**NBNS**

**N**et**B**IOS **N**ame **S**erver. A server providing NetBIOS name to IP address mapping. The NBNS is part of the NBT mechanism and does not need to participate directly in the NetBIOS LAN.

*See also:* WINS

**NBT**

**N**et**B**IOS over **T**CP/IP; also known as NetBT and, less commonly, as TCPBEUI. NBT is an implementation of the NetBIOS API on top of a TCP/IP transport layer.

**NBT Name**

The term used in this book for the fully qualified First Level Encoded form of the NetBIOS Name and Scope ID. For example, the NBT name

```
EGEFCACACACACACACACACACACACACACA.FI.FO.FUM
```

is composed of the NetBIOS name *FE*`<20>` and the scope ID "`FI.FO.FUM`".

*See also:* Scope ID, First Level Encoding

**Network Data Representation (NDR)**

The on-the-wire encoding for parameters passed via MS-RPC. MS-RPC input parameters are marshalled into NDR format for transmission over the network, and then unmarshalled on the server side. The process is then reversed to return the results.

*See also:* MS-RPC

**NetBEUI**

**NetB**IOS **E**xtended **U**ser **I**nterface. Also known as **N**et**B**IOS **F**rame Protocol (NBF). NetBEUI provides a simple mapping of NetBIOS API parameters and data to a transport suitable for passing messages on Ethernet and Token Ring networks.

*Web reference: NetBIOS NetBEUI NBF Networking*, by Timothy D. Evans (`http://ourworld.compuserve.com/homepages/timothydevans/contents.htm`)

**NetBIOS**

**Net**work **B**asic **I**nput **O**utput **S**ystem. NetBIOS is the **A**pplication **P**rogramming **I**nterface (API) to a proprietary LAN system that was developed by IBM and Sytec. The NetBIOS API has been implemented on top of several different network transports including TCP/IP, DECnet, IPX/SPX, and others.

*See also:* NBT, NetBT

**NetBT**

NetBIOS over TCP/IP. Better known as NBT.

*See:* NBT

**NT Domain**

A Workgroup with a Domain Controller.

*See also:* Domain Controller, Workgroup

**Phrep**

An expletive, roughly equivalent to “dang,” “drat,” or “bother,” but without connotation.

**Primary Domain Controller (PDC)**

A Windows NT Domain Controller (DC) which keeps the master copy of the user/group authentication database in an NT Domain. Only one PDC is permitted per NT Domain. In addition to registering the *nt_domain*`<1C>` Group Special name, the PDC also registers the unique *nt_domain*`<1B>` NetBIOS name (where *nt_domain* is the name of the NT Domain). Microsoft’s WINS server ensures that the IP address registered to the *nt_domain*<1B> name is always at the top of the list of IPs associated with the *nt_domain*<1C> Group Special name.

*See also:* Backup Domain Controller, Domain Controller

**Potential Browser**

Any node on a local IP LAN that is willing and able to participate in browser elections and take on the role of Local Master Browser or Backup Browser.

*See also:* Local Master Browser, Backup Browser

**Scope ID**

A string of dot-separated labels, formatted per DNS naming rules. The Scope ID defines a virtual NBT LAN by dividing the NetBIOS namespace.

*See also:* NBT Name, DNS, First Level Encoding, Second Level Encoding

**Second Level Encoding**

The on-the-wire format of an NBT name. The encoding scheme replaces the familiar dot characters used in DNS names with a byte containing the length of the next label. The Second Level Encoded form of the NBT Name

```
EGEFCACACACACACACACACACACACACACA.FI.FO.FUM
```

would be

```
"\x20EGEFCACACACACACACACACACACACACACA\x02FI\x02FO\x03FUM\0"
```

*See also:* NBT Name, DNS, First Level Encoding

**Server Message Block (SMB)**

A file- and print-sharing protocol developed by IBM, Intel, 3Com, and Microsoft for use with PC-DOS and MS-DOS. It has since been renamed CIFS.

Also a name for the messages exchanged via the SMB or CIFS protocol. An SMB message is often referred to simply as "an SMB."

*See also:* CIFS

**Server Service**

An SMB filesharing service provider. The Server Service registers a NetBIOS name consisting of the machine name with a suffix value of

`0x20`. On many platforms, the Server Service will also accept NBT connection requests with a `CALLING NAME` of `*SMBSERVER<20>`.

**Simple Protected Negotiation (SPNEGO)**

The "Simple and Protected GSS-API Negotiation Mechanism" is a protocol used with GSS-API to negotiate authentication mechanisms between a client and server.

*See:* RFC 2478
(`http://www.faqs.org/rfcs/rfc2478.html`)

*See also:* GSS-API

**Suffix Byte**

The sixteenth byte of a NetBIOS name. This byte is used to indicate the type of service that has registered the name.

**TCPBEUI**

Yet another name for NBT. The name TCPBEUI is primarily used by folks from IBM.

*See:* NBT

**Thermomostat**

The internal sensor that causes your mother to tell you to put on a sweater when she is cold.

**WINS**

**W**indows **I**nternet **N**ame **S**ervice. Microsoft's name for their NBNS implementation.

*See:* NBNS

**Workgroup**

An NT Domain without a Domain Controller. The distinction between an NT Domain and a Workgroup is blurry. The two are basically the same thing, except that an NT Domain has a Domain Controller, which provides authentication services. The Primary Domain Controller also always runs the Domain Master Browser (DMB) service, which coordinates the workgroup Browse Lists across subnets.

*See also:* Domain Master Browser, Domain Controller, Primary Domain Controller