7

Where It All Went Wrong

> It was a dark and stormy night.
>
> — *Paul Clifford*,
> Edward George Bulwer-Lytton

Implementation is the journey from Theory to Practice. The two extremes, as we have shown, are divided by a vast chasm wherein dwell all the evil monsters from all the cheesy sci-fi TV shows ever produced. For NBT implementors the journey can be perilous, and those who have gone before have blazed a somewhat twisted trail. Here are some of the dangers you will encounter along the way...

7.1 The `0x1D`irty Little Secret

Master Browser Servers (which are described later in the book) register unique names with the suffix `0x1D`. The WINS server will happily acknowledge such registrations — and then drop them into a black hole and forget about them. When queried, the WINS server denies the existence of any `0x1D` unique names. Nodes from one subnet can never know about the Master Browsers on other subnets, and there may be multiple nodes using the same unique `0x1D` name.

B nodes are immune to this behavior, since they do not make use of NBNS services. If the NBT vLAN is operating in M or H mode, however, the

Master Browser names will be unique *within the local IP subnet only*. The same name may be registered by another Master Browser on a separate subnet. Since the WINS server does not keep any record of `0x1D` names, Master Browsers can only be located using a broadcast query, which means that P nodes can never find `0x1D` names.

The strange handling of `0x1D` names may be related to the lack of NBDD functionality. As you can see, an implementation that strays from the path will quickly find itself lost in a jungle of exceptions, special cases, and other yucky stuff from an old episode of "Outer Limits."

7.2 Twenty-five IPs or Less

An NBNS is supposed to keep a complete list of all IPs associated with each NBT name (group or multi-homed). If the list is too large to fit in a single UDP Name Query Reply datagram then, according to the RFCs, the NBNS is supposed to send a partial list with the `TR`uncation bit set. The client may then repeat the query using TCP port 137.

...but that never happens. If anyone ever did provide support for NBT Name Service over TCP, the code is now lost in space. As explained earlier, when WINS sends a `NAME QUERY RESPONSE` it will contain a maximum of 25 IPs per name.

7.3 Special Handling Required for `0x1B` Names

A Domain Master Browser (a special kind of Master Browser, which is described later on in the book) will register unique names with a suffix of `0x1B`. These names get special treatment in WINS. Whenever a `0x1B` name is registed in WINS, the WINS server will look for a matching `0x1C` group name and modify the entry.

As you may recall from our diatribe in the Datagram section, `0x1C` group names are "Internet Group" or "Special Group" names, and WINS will keep track of 25 IP addresses per `0x1C` group name. The weird thing is that WINS also sorts this IP list so that the IP address associated with the `0x1B` name is at the top of the list.

Why?

Well, see, the 0x1C names represent the set of Domain Controllers for a given NT Domain. Only the Primary Domain Controller is allowed to run the Domain Master Browser service and register the 0x1B name. So, by sorting the IP list, WINS ensures that the IP address of the Primary Domain Controller is always the first IP address in the 0x1C list of Domain Controllers.

7.4 Alternate Name Resoultion

There are several ways to bypass the NBT Name Service. The simplest is the use of an LMHOSTS file, which provides NetBIOS name to IP address mappings. LMHOSTS is similar in concept to the /etc/hosts file commonly used by Unix-y systems to provide TCP/IP name mappings.

Another Name Service bypass trick involves using DNS names or IP addresses instead of NetBIOS names to find remote services. This trick is generally used when connecting to an SMB server via the NBT Session Service. The obvious problem here is that the Session Service expects that the CALLED NAME in the SESSION MESSAGE be correct.

There are several work-arounds to the naming problem.

- One may *guess* that the service name matches the first label of the DNS name. This often works, but it is not guaranteed.
- Another option is to send a NODE STATUS REQUEST and look through the reply for a unique name with a suffix of 0x20, which is likely to be the correct service name. (The SMB Server Service always uses the suffix 0x20.)
- The ugliest (and also the most common) solution is to place the NetBIOS name "*SMBSERVER" into the CALLED NAME field (encoded, of course). This special name was introduced with Windows NT 4.0, and is now supported by Samba and several commercial implementations. It is accepted for Session Service connections to the SMB Server Service, no matter what NetBIOS name is actually registered. Note that "*SMBSERVER" starts with an asterisk, which makes it an illegal NetBIOS name. The "*SMBSERVER" name is never registered, and name queries for this name should always fail.

7.5 The Awful Truth

The awful truth is that an NBT implementation must accommodate — and often comply with — the errors, kludges, omissions, and fumbles of the past. The installed base is simply too big to try and get it right. Not to worry. You now have enough information to build a working NBT implementation. Writing an NBNS and NBDD server should also be within reach, and you can pull code from some of the many Open Source projects that are out there (as long as you respect the licenses). We have covered all of the major pitfalls, and NBT is a resilient little system. Making it work is a lot easier than getting it right.