

Re: Why does DNS.EXE listen on a ephemeral TCP port?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2006-09/msg00072.html>

- *From:* "Brian K. Doré" <bkd@xxxxxxxxxxxxxx>
 - *Date:* Mon, 4 Sep 2006 19:46:49 -0500
-

Hi Ace,

Thanks for the reply, but I don't know if we are taking about the same thing.

comments inline.

"Ace Fekay [MVP]" <PleaseAskMe@xxxxxxxxxxxxxx> wrote >

That's part of the Windows conenection method. The initial port is 53UDP, then if over 512 bytes, then it will revert to TCP, unless of course using Windows 2003 DNS, which supports EDNS0, which allows UDP responses upto 1280 bytes.

Right, but when my name server makes a query to another name server, and the response size will be over 512 bytes, that server responds via UDP to my server and then my server originates a TCP connection. (from a ephemeral local TCP port to a destination of TCP 53 on the server) I understand why my server listens on a UDP port, but I don't think this explains why my server is LISTENING on a TCP port. In order for a TCP listening port to be used, some mechanisim must exist for my server to inform another machine about the port number it's listening on (RPC perhaps), and another machine would have to initiate the connection. The TCP listening port is not the same number as the UDP listening port. I can't find anything that indicates that another server would initiate a TCP connection to my server in response to a query, or how a query would indicate which TCP port to respond on. It was suggested it might be a control port (like what ndc on bind would use) but my testing shows that running the remote MMC DNS console doesn't use it.

But as far as the emphemeral port, that is a Windows conveyance. Any connection will connect over the initial port of the protocol used, such as DNS is 53, or NetBIOS is 139, etc, but the client will tell it to respond on a UDP port above 1023 (1024 and above). If you want to force it to only 53 at all times, you can alter the reg on the DNS server(s). For

Re: Why does DNS.EXE listen on a ephemeral TCP port?

internal applications (such as an AD infrastructure), I would just leave it be, but if you want to control it thru a firewall for external users to use an internal DNS server that you are possibly hosting public records, you can force it.

Right, but this is only for when my server initiates the connection, the ephemeral port is the source port and that is how the recipient knows what port to respond to. In this case my server is LISTENING on a high TCP port for someone to connect to it.

If you want to alter it, in the article below, look for the "Send Port" reg entry to alter on the server.

813965 – Description of DNS registry entries in Windows 2000 Server, part 3 of 3:

<http://support.microsoft.com/default.aspx?kbid=813965>

This appears to affect only the UDP source port my server would use when making queries.

Does my question make sense or am I misunderstanding about how something works?

Thanks again for your help.

Brian

.