NAME

netgdb - protocol for debugging the kernel with GDB over the network

SYNOPSIS

To compile NetGDB support into the kernel, place the following lines in your kernel configuration file:

options DDB
options GDB
options INET
options DEBUGNET
options NETGDB

DESCRIPTION

netgdb is a UDP-based protocol for communicating with a remote GDB client via an intermediary proxy.

A **netgdb** session is started by using the **netgdb -s** *server* [**-g** *gateway* **-c** *client* **-i** *iface*] command in ddb(4) to connect to a proxy server. When the connection is made, the proxy server logs a message that a **netgdb** client has connected. It subsequently establishes a TCP listening socket and logs a message specifying which port it is listening on. Then it waits for a GDB client to connect. The GDB command to connect is:

target remote <*proxyip:proxyport*>

At this point, the server proxies traffic back and forth between **netgdb** and the ordinary GDB client, speaking the ordinary GDB remote protocol. The **netgdb** session is identical to any other kernel GDB sesssion from the perspective of the GDB debugger.

IMPLEMENTATION NOTES

The UDP protocol is based on the same packet structure and a subset of the exact same message types as netdump(4). It uses the HERALD, DATA (nèe VMCORE), and FINISHED message types. Like netdump(4), the client's initial HERALD message is acknowledged from a random source port, and the client sends subsequent communication to that port.

Unlike netdump(4), the initial HERALD port is 20025. Additionally, the proxy server sends responses to the source port of the client's initial HERALD, rather than a separate reserved port. **netgdb** message and acknowledgements are bidirectional. The sequence number and acknowledgement protocol is otherwise identical to the unidirectional version used by netdump; it just runs in both directions. Acknowledgements are sent to and from the same addresses and ports as regular messages.

The first version of the **netgdb** protocol uses the protocol number ‘0x2515f095’ in the 32-bit *aux2* parameter of the initial HERALD message.

The list of supported network drivers and protocol families is identical to that of netdump(4).

DIAGNOSTICS

The following variable is available via both sysctl(8) and loader(8) (as a tunable):

debug.gdb.netgdb.debug

Control debug message verbosity. Debug messages are disabled by default. They may be enabled by setting the variable to a non-zero value.

SEE ALSO

ddb(4), gdb(4), netdump(4)

HISTORY

netgdb first appeared in FreeBSD 13.0.

BUGS

netgdb may only be used after the kernel has panicked, due to limitations in the treatment of locking primitives under ddb(4).

SECURITY CONSIDERATIONS

Version 1 of the **netgdb** protocol has no security properties whatsoever. All messages are sent and acknowledged in cleartext, and no message authentication codes are used to prevent attackers from forging messages. It is absolutely inappropriate for use across the public internet.