TECHNICAL NOTE

GoFree Advanced Setup

Revision	Comment	Author	Date
1.0	First version	Tom Isaacson	03/05/2013

DHCP versus Zeroconfig

All Navico devices built for GoFree will look for a DHCP server on the network. However, if they don't find one they will allocate themselves a Zeroconfig address (in the range 169.254.X.X), so you can choose to have DHCP available or not.

Blocking radar and sonar data

Navico's Radar and Sonar products transmit large quantities of data. If this is allowed to transmit over your Wifi network it may result in your Wifi being overloaded and unable to work correctly. Because of this we recommend blocking Radar and Sonar data on you Wifi router so the Wifi is kept free of this data. This will not affect the normal functionality of radar, sonar or GoFree features.

1. Blocking Radar data

Navico's Radar products use multicast to transmit data to other devices on the network at a rate of up to 8 Megabits per second, depending on model and setup. The simplest way to prevent this from being transmitted on your Wifi is to turn on a feature called IGMP Snooping, also sometimes referred to as Multicast-to-Unicast. This only transmits multicast packets over Wifi if a device on Wifi has joined that multicast, so unnecessary data isn't transmitted.

Normally you will find this feature in the UI of your router, but if you're using OpenWRT (a common open-source router firmware) you can do this on the command line:

```
echo "1" > /sys/devices/virtual/net/br-lan/bridge/multicast_snooping
```

or set it in file sysctl.conf.

2. Blocking Sonar data

Navico's Sonar products use broadcast to transmit data to other devices on the network at a rate of up to 1 Megabit per second, depending on model and setup. Unfortunately this is more complicated to block than multicast data.

If you're using OpenWRT or a similar Linux-based OS you can do this by adding a filter to your IP table:

```
iptables –A INPUT –d 255.255.255.255 –j drop
```

This tells it to drop any messages from the global broadcast address.

Network Testing

Once your network is setup there are several tools we provide to help with your testing.

1. Iperf 2.0 5

Iperf is a commonly used network performance tool. It's also supported by network performance testing applications like AirMagnet. It's provided so you can test the performance of your Wifi network around your boat so you can easily identify any weak spots or problem areas.

To get Iperf for your device:

Windows: http://sourceforge.net/tracker/?func=detail&aid=3470334&group_id=128336&atid=711373

iOS (paid): https://itunes.apple.com/us/app/iperf2/id513512448?mt=12

Android: https://play.google.com/store/apps/details?id=com.magicandroidapps.iperf

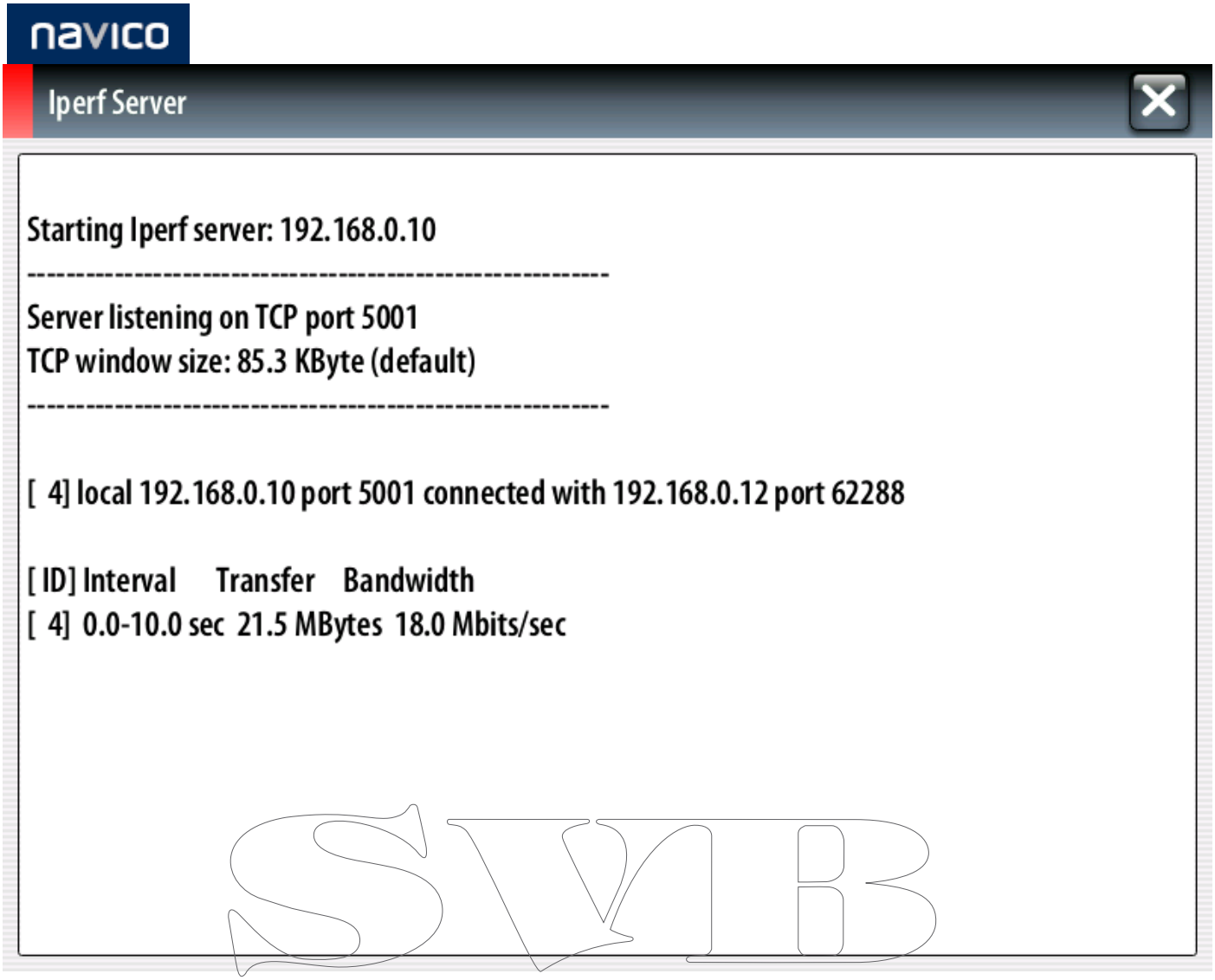
Ubuntu Linux: apt-get install iperf

To run the Iperf server on the MFD go into the Settings menu and select Network->Wifi->Advanced->Iperf. This starts the server in TCP mode on the MFD and displays the output, including the IP address.

On your device you either enter the IP address of the MFD on the UI or run iperf on the command line:

iperf –c [IP address]

You should see the test being performed and the result on your device and the MFD:



To stop the Iperf server on the MFD just exit the window and the process will be shut down.

2. dhcp_probe 1.3.0

The GoFree Wifi module contains a DHCP server that will allocate IP addresses for all the MFDs, radars and sonars in your network. But if you're trying to integrate with other devices, such as a 3G modem or satellite phone, you may find other devices in the network are also acting as DHCP servers.

To make it easy to find DHCP servers on your network you can run dhcp_probe from your MFD. Go into the Settings menu and select Network->Wifi->Advanced->DHCP Probe. You should see the output on the MFD: