



## vxSnoop Users Manual

For

VxWorks Operating System

Document Number: Dot21

Version: 1.0

Printing Date

March 27, 2002

\* \* NOTICE \* \*

The information presented in this document was developed to assist Dot 21 Real-Time System's customers in the use of the vxSnoop application.. The information contained in this document is subject to change without notice.

Dot 21 Real-Time Systems makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Dot 21 Real-Time Systems shall not be liable for errors contained herein or for incidental or consequential damages concerning the furnishing, performance or use of this material.

This document contains proprietary information, which may be protected by copyright. All rights are reserved. No part of this document may be reproduced without the prior written consent of Dot 21 Real-Time Systems.

VxWorks is a registered trademark of Wind River Systems Inc.

Solaris is a registered trademark of Sun Microsystems Inc.

Windows is a registered trademark of Microsoft Corp.

\* \* PRINTING HISTORY \* \*

FIRST PRINTING

March 27, 2002

New editions are complete revisions of this document. Manuals will be reprinted as necessary to incorporate any updates or corrections.

**TABLE OF CONTENTS**

SECTION 1	INTRODUCTION	1
1.1.	DOCUMENT ORGANIZATION	1
1.2.	THEORY OF OPERATION	1
SECTION 2	SETUP	3
2.1	INSTALLATION	3
2.2	CONFIGURATION	3
SECTION 3	OPERATIONS	4
3.1	CONTROL (ENABLE/DISABLE)	4
3.2	INITIALIZATION	4
3.3	COLLECTION DIRECTION	5
3.4	PACKET TYPE SELECTION	6
3.5	SOURCE FILTERS	6
3.6	DESTINATION FILTERS	8
3.7	CLEAR FILTER LIST	9
3.8	PRINT DETAIL	9
3.9	MISCELLANEOUS	10
3.10	PACKET DISPLAY	10
3.11	EXIT	12

**List of Figures**

Figure 1 Main Menu	2
Figure 2 ifShow Output	5
Figure 3 Direction Menu	6
Figure 4 Packet Type Selection	6
Figure 5 Source Packet Selection	7
Figure 6 Source Address Port Example	7
Figure 7 Destination Packet Selection	8
Figure 8 Destination Address Port Example	8
Figure 9 Data Display Menu	9
Figure 10 Buffer Index Menu	9
Figure 11 Misc Selection Menu	10

## SECTION 1 INTRODUCTION

This manual provides the general information for using the Local Area Network (LAN) packet capture and display program, hereafter referred to as vxSnoop. VxSnoop is a network analysis program that is designed to be used with the VxWorks Operating System and a LAN interface, using Wind River's END network driver structure. This document discusses the operations used to install, configure, and control the collection and display of network packets. The vxSnoop program provides the capability of capturing and displaying message packets needed to solve LAN interface problems.

VxSnoop is designed to allow the user to selectively collect LAN message packets based on a number of different criteria. By providing selective sampling, the user can eliminate the collection of unwanted packets. A menu system is used to provide the user access to the control and display operations of the program.

It is expected that the reader has a working knowledge of basic TCP network conventions and the VxWorks operating system, when using this document.

### 1.1. DOCUMENT ORGANIZATION

This document is laid out in a top down data format where the text goes from the initialization process, through the data collection and display process to closing operations. Since the vxSnoop program is not a simple step by step operation, references to certain operations may be mentioned before the actual discussion of the operation. The reader may jump ahead to the appropriate discussion by checking the table of contents reference, if desired.

### 1.2. THEORY OF OPERATION

VxSnoop is implemented using a text menu configuration. This technique allows the user to control the package without additional programs or special support. In most cases, the user performs the necessary operations by using simple one character commands. Different menus are displayed as the user enters commands causing a new menu to be displayed. The program can be run in a standalone mode or integrated with an application or the kernel to monitor packets that originate on the processor board.

The vxSnoop menu display uses the full screen capability of the terminal, if it is a supported terminal type. The default terminal configuration uses ANSI cursor control sequences. The ANSI control sequences are supported by most DEC terminals such as the VT100 and VT220, as well as several terminal emulation programs such as dtterm on Solaris. If the user does not have an ANSI terminal, he or she can select one of the other terminal options, including no emulation if an exact terminal interface is not available.

When vxSnoop is started, a menu display similar to Figure 1 is presented on the terminal. The terminal layout contains a menu header followed by a list of available commands. A prompt to enter the desired command is displayed after the menu options.. Immediately below the command prompt a status line is available to display errors or status information.

## Snoop Program Menu

1. Control	Disabled
2. Initialization	NOT initialized
3. Set Collection Direction	Send & Recv
4. Select Packet Types	ARP,UDP,TCP,ICMP,UNKNOWN
5. Modify Source Parameters	
6. Modify Destination Parameters	
7. Clear all filters	
8. Set Print Detail	Summary
9. Misc	
d,D Display Buffer	
x,X Exit	
Enter Choice	

**Figure 1 Main Menu**

Packet collection is controlled by selecting the appropriate menu option in the vxSnoop main menu. When packet collection is enabled, all previous packets are discarded and capture starts at that instant. Packet collection continues until the user stops the collection. If the buffer fills before collection is terminated, the packets are stored in a circular buffer, allowing the most recent messages to be saved. After stopping packet collection, the user may display the collected information in one of several formats. Once the data is collected, the user may display the information any number of times, using a different display format each time.

To be an effective packet collection system, vxSnoop provides the capability of collecting packets with a unique source or destination address and/or port. This capability allows the user to reduce the number of packets that are collected and to focus on the packets of interest. The user may also elect to only sample transmitted or received packets. In any case, the user can determine the precise source of packets that are collected.

In addition, the user can elect to capture individual packet types, which further filters unwanted message packets. Any combination of packet types may be sampled by making the appropriate choice.

After a data buffer is collected, the user may display the contents of the buffer in either a summary or full detail form. The summary format simply displays the ethernet header, while the detail format displays the complete message in a hexadecimal and ASCII format.

## SECTION 2 SETUP

### 2.1 INSTALLATION

VxSnoop is distributed as a zipped or packaged file that contains the distribution. To install the package on the host system, the user must place the delivered file on the host system. Once the package is placed on the system, it can be installed by extracting or unzipping the file into the desired directory. If installing on a Solaris or Unix system, the gunzip command can be used. On the other hand if the user is installing the package on a Windows system, the package can be unzipped using WinZip or a similar file decompression program.

Once the package is installed, the user may either link the object file with the kernel or application or load it separately in a standalone configuration.

### 2.2 CONFIGURATION

There are no configuration requirements to use the vxSnoop package.

## SECTION 3 OPERATIONS

The vxSnoop program is started by entering ‘vxSnoop’ at the VxWorks command line. This caused the main menu to be displayed. The following commands presume that the user has started vxSnoop and has the main menu display.

### 3.1 CONTROL (ENABLE/DISABLE)

Menu option one (1) provides the capability of controlling when data packets are collected. This option is an alternate action switch that enables or disables packet collection based on its current state. The user can easily determine the current state of operations by viewing the text to the right of the menu option, which indicates either Enabled or Disabled.

The user may exit the vxSnoop program and return later and not affect the packet collection. If packet collection is enabled when the user exits, it continues to collect packets until stopped by the user. This allows the user to perform other operations such as starting or stopping a network interface without affecting the collection of packets. The user must note that once the memory buffer is full, the oldest packets are replaced with a newer packet.

There are two ways of stopping packet collection. The user can simply use the control command or use the display command. If the user elects to display the captured packets by entering the display mode, packet collection is terminated but only if one or more packets have been saved. If no packets are saved, packet collection remains enabled. In short, this is a quick way of determining if any packets have been collected without stopping collection.

When vxSnoop goes from the disabled state to enabled, the message packet storage is cleared, removing all previously collected packet information.

### 3.2 INITIALIZATION

Before packets can be collected, vxSnoop must be linked to the network interface to be monitored. Therefore, menu item two (2) should be one of the first options to be selected. Upon selection, the user is queried for an interface name. This name is typically a two or three character string that identifies the network to be monitored. If the user is not familiar with the interface to be monitored, he or she can determine the interface name by invoking the VxWorks command ‘ifShow’. The ‘ifShow’ function displays a list of network interfaces and pertinent data about these interfaces. Figure 2 is an example display of the ‘ifShow’ output.

#### **dc (unit number 0):**

Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING

Type: ETHERNET\_CSMACD

Internet address: 192.168.1.21

Broadcast address: 192.168.1.255

Netmask 0xfffff00 Subnetmask 0xfffff00

Ethernet address is 00:01:af:00:df:3f

Metric is 0  
Maximum Transfer Unit size is 1500  
803 packets received; 405 packets sent  
138 multicast packets received  
4 multicast packets sent  
0 input errors; 0 output errors  
0 collisions; 0 dropped

**lo (unit number 0):**

Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING  
Type: SOFTWARE\_LOOPBACK  
Internet address: 127.0.0.1  
Netmask 0xff000000 Subnetmask 0xff000000  
Metric is 0  
Maximum Transfer Unit size is 32768  
0 packets received; 0 packets sent  
0 multicast packets received  
0 multicast packets sent  
0 input errors; 0 output errors  
0 collisions; 0 dropped

**Figure 2 ifShow Output**

The lines displayed in bold type can be considered as candidates for vxSnoop to monitor. The first entry, **dc**, is the interface of a particular network. It should be noted that the actual string, in this case **dc**, is probably different on the user's system. On this same line, the user can find the unit number which needs to be given to the vxSnoop initialization method. It should also be noted that the user may have several devices displayed when invoking the "ifShow" command. The user must choose the right interface to capture the desired packets.

In the previous example, the **lo** interface is a loopback interface and should not be used for snooping because it is unlikely that any packets will be found on the interface.

### 3.3 COLLECTION DIRECTION

The user may elect to only capture packets that are transmitted from the board being monitored or capture packets that are on the LAN. Menu item three (3) provides the mechanism for configuring the direction collection. By default, both directions are enabled to provide full collection of all LAN messages. Figure 3 is an example of the direction selection menu. The user must choose one of the available options to exit this menu.

## Packet Direction Selection Menu.

1. Input Packets
  2. Output Packets
  3. Both
- Select Packet Direction

**Figure 3 Direction Menu**

### 3.4 PACKET TYPE SELECTION

Since there are several different packet types and often a user is only concerned with capturing one or perhaps two different types, vxSnoop provides the capability of selecting the packet types that are to be considered for saving. Menu item four (4) allows the user to enter a submenu where a list of the common message packet types are displayed. The packet options are presented by using numbers that are a power of two. This technique allows the user to select different combinations of message packets without having an inordinate list of choices. For instance as shown in Figure 4, one could select the collection of UDP and TCP messages by entering a twelve (12). It can easily be seen that one can select any combination of packets to collect.

## Packet Selection Menu.

1. UNKNOWN
  2. ARP
  4. UDP
  8. TCP
  16. ICMP
  31. ALL
- Enter Choice

**Figure 4 Packet Type Selection**

### 3.5 SOURCE FILTERS

To provide a method of only collecting packets that have a unique source address or port number, vxSnoop allows the user to place entries in a filter table. This filter table is applied to all packets that meet the direction and type criteria. Enabling of source address or port filtering can be accomplished by selecting menu item five (5) from the main menu.

When item five is selected, a second option menu is displayed, (See Figure 5). This menu shows the current source address and port filter table as well as the option to modify an address or port entry. The user then selects either one (1) address modification or two (2) port modification. If the user decides not to make a change or enters this menu by mistake, he or she can simply exit.

Index 1 Address = N/A	Port = N/A
Index 2 Address = N/A	Port = N/A
Index 3 Address = N/A	Port = N/A
Index 4 Address = N/A	Port = N/A
Index 5 Address = N/A	Port = N/A

#### Source Parameter Menu

1. Modify Source Address
  2. Modify Source Port
- x,X Exit
- Enter Choice

**Figure 5 Source Packet Selection**

Selection of the source address modification menu option results in a third display, which shows the current address filters and an option to enter an address. This address is expected to be entered in dot notation format (e.g. 192.168.123.456). After the address is entered, the user is queried for the index where the entry will be placed. If there are no entries in the address and port table, the user must choose index one (1). Each index entry in the port or address table must follow consecutively or be a value that already has an entry. If the user fails to observe these rules, an error is displayed and the entry is discarded.

Index 1 Address = 192.168.212.111	Port = N/A
Index 2 Address = N/A	Port = 1666
Index 3 Address = N/A	Port = 1700
Index 4 Address = 192.168.214.1	Port = 1344
Index 5 Address = N/A	Port = N/A

**Figure 6 Source Address Port Example**

As shown in Figure 6, the user can arrange the filters in any order as long as the previous indices have a non-zero address or port number. NOTE: If the user removes an entry causing both the port and address to be zero, all subsequent entries are moved up to ensure consecutive entries.

The user can make a port selection by choosing menu item two (2) and abiding by the same rules as for address changes. It should be noted that neither the address nor port number are tested for validity. Therefore, it is incumbent upon the user to make the proper entries.

### 3.6 DESTINATION FILTERS

To provide a method of collecting only packets that have a unique destination address or port number, vxSnoop allows the user to place entries in a filter table. This filter table is applied to all packets that meet the direction and type criteria. Enabling of destination address or port filtering can be accomplished by selecting menu item five (5) from the main menu.

When item five is selected, a second option menu is displayed, (See Figure 7). This menu shows the current destination address and port filter table as well as the option to modify an address or port entry. The user then selects either one (1) address modification or two (2) port modification. If the user decides not to make a change or enters this menu by mistake, he or she can simply exit.

Index 1 Address = N/A	Port = N/A
Index 2 Address = N/A	Port = N/A
Index 3 Address = N/A	Port = N/A
Index 4 Address = N/A	Port = N/A
Index 5 Address = N/A	Port = N/A

#### Destination Parameter Menu

1. Modify Destination Address
2. Modify Destination Port

x,X Exit

Enter Choice

**Figure 7 Destination Packet Selection**

Selection of the destination address modification menu option results in a third display, which shows the current address filters and an option to enter an address. This address is expected to be entered in dot notation format (e.g. 192.168.123.456). After the address is entered, the user is queried for the index where the entry will be placed. If there are no entries in the address and port table, the user must choose index one (1). Each entry in the port or address table must follow consecutively or be an index that already has an entry. If the user fails to observe these rules, an error is displayed and the entry is discarded.

Index 1 Address = 192.168.212.111	Port = N/A
Index 2 Address = N/A	Port = 1666
Index 3 Address = N/A	Port = 1700
Index 4 Address = 192.168.214.1	Port = 1344
Index 5 Address = N/A	Port = N/A

**Figure 8 Destination Address Port Example**

As shown in Figure 8, the user can arrange the filters in any order as long as the previous indices have a non-zero address or port number. NOTE: If the user removes an entry causing both the port and address to be zero, all subsequent entries are moved up to ensure consecutive entries.

The user can make a port selection by choosing menu item two (2) and abiding by the same rules as for address changes. It should be noted that neither the address nor port number are tested for validity. Therefore it is incumbent upon the user to make the proper entries.

### 3.7 CLEAR FILTER LIST

There may be an occasion where the user desires to clear all of the filter entries and start anew. To quickly clear the filter entries, menu item seven (7) is provided. Both the source and destination address and port filters are cleared.

### 3.8 PRINT DETAIL

VxSnoop provides the capability of displaying the collected packets in different formats. To change these display formats, the user may select menu item eight (8). When this item is selected, a second menu is displayed (See Figure 9), showing an entry to change the level of detail and where the buffer display will start.

#### Snoop Data Display Menu

1. Set Detail      Summary
  2. Set Buffer Start    Header +  
x,X Exit
- Enter Choice

**Figure 9 Data Display Menu**

To change the level of detail, the user must select menu item one (1). This is an alternate action selection which toggles between Summary and Detailed. A summary entry simply results in the display of the packet header. Conversely, the detail option causes the header and data buffer to be displayed. Depending on the entry associated with menu item two (2), the buffer starts at a designated place in the received packet.

By selecting sub-menu item two (2), another menu (See Figure 10), is displayed, indicating where the display buffer should start. Selection of menu item one (1) causes the complete packet to be displayed, including the hardware addresses at the very front. A more meaningful option would be to select menu item two (2) which causes the packet display to start with the IP information. Finally, the user may skip both the hardware and IP information and display the user data by selecting menu item three (3).

1. Display Complete Buffer
  2. Display Buffer starting with IP
  3. Display Message Buffer
- Enter Choice

**Figure 10 Buffer Index Menu**

If the print option is set to detailed, the packet is displayed in a hexiadecimal and ASCII format starting at a selected position determined by the buffer start option.

### 3.9 MISCELLANEOUS

To take care of those minor options that are needed to make a complete package but do not justify a menu selection of their own, menu item nine (9) is made available. When this selection is made, another menu is displayed, allowing the user to change the terminal type. Figure 11 is a representation of the miscellaneous menu.

```

                Snoop Misc Menu

1. Set Crt Type

x,X Exit

Enter Choice

```

**Figure 11 Misc Selection Menu**

To change the terminal type, the user must select menu item one (1). This causes a third menu to be displayed indicating the available terminal options. Currently, only the ANSI or VT100, Sun ShellTool, and Dumb terminal options are available. If the user's terminal does not support the ANSI cursor control mechanism, the dumb terminal option should be used.

### 3.10 PACKET DISPLAY

Once the packets are captured and the print detail is set, the user can display the packets by selecting main menu item d or D. This selection causes the user to be queried for a starting tick count to determine where to start displaying the packets. The user will also be asked to enter the number of lines to be displayed per page. If using a detailed display, it is recommended that the user choose one. If a user does not enter a value, the previous value is used. Once a page is displayed, the user must enter an option to continue or quit. Figure 12 is an example of a summary listing.

```

Index  Ticks
0:0x10d9:IP(p:TCP,v:4,h:20,l:552) 192.168.1.21 -> 192.168.1.2
      TCP(s:23,d:3264,q:2085126156,a:676150839,f:0x18,w:8192)
1:0x10e4:IP(p:TCP,v:4,h:20,l:40) 192.168.1.2 -> 192.168.1.21
      TCP(s:3264,d:23,q:676150839,a:2085126668,f:0x10,w:8760)
2:0x10e4:IP(p:TCP,v:4,h:20,l:54) 192.168.1.21 -> 192.168.1.2
      TCP(s:23,d:3264,q:2085126668,a:676150839,f:0x18,w:8192)
3:0x10f8:IP(p:TCP,v:4,h:20,l:40) 192.168.1.2 -> 192.168.1.21
      TCP(s:3264,d:23,q:676150839,a:2085126682,f:0x10,w:8746)

```

The first entry in a summary display shows the index of the packet being displayed. This count should start at zero unless a tick count greater than the first sample is entered. The second item, separated by a colon, is the tick count at the time the packet was captured. It should be noted that this value is displayed in hexadecimal format.

After the index and time are displayed, the IP packet information is presented. The IP can be found by looking for the capital letters IP. In parenthesis after the IP the following parameters are displayed:

- p: The type of service being performed
- v: The version of the IP packet
- h: The length of the header
- l: The length of the buffer

Immediately after the IP data is the source and destination network addresses in dot notation format separated by a ->.

On the second line, the packet information is presented. This display is similar to the IP packet data display except that there are different parameters. The following is a list for the TCP message packet contents.

- s: The source port
- d: The destination port
- q: The sequence number
- a: The acknowledge number
- f: The flags field
  - 0x1 Sender is finished
  - 0x2 Synchronize sequence
  - 0x4 Reset the connection
  - 0x8 Pass data to application as soon as possible
  - 0x10 The acknowledge number is valid
  - 0x20 Urgent Message
- w: The window size

The following is a list of parameters for a UDP packet:

- s: The source port
- d: The destination port
- l: The length of the packet

The following is a list of parameters for a ICMP packet. In addition, the source and destination network addresses are displayed separated by a ->.

- p: The protocol
- v: Version
- h: Header length

l: Packet length

The ARP packet display contains the protocol as well as the sender hardware address, sender protocol address, receiver hardware address, and receiver protocol address.

The following is a list of parameters for an ARP packet:

p: The protocol

### 3.11 EXIT

To quit the vxSnoop program or leave to perform other tasks, the user should select menu item x or X. This selection takes the user back to the command prompt to allow other operations. If vxSnoop is enabled when the user exits, packets continue to be collected.