## Capturing DIS Packets

For analysis it is often useful to capture DIS packets as they are sent over ethernet. This can be achieved using software that captures all network traffic on a specific network device. Useful software for this purpose is Wireshark (WireShark, n.d.).

One possible use case for capturing DIS packets might be the following: DIS packets are broadcast from a local machine running a Coalition Battle Management Language (CBML) application (IP: 192.168.188.87) to the broadcast address of the local network (IP: 192.168.188.255).

After installing Wireshark to a machine on the local network, Wireshark must be started. The startup screen of Wireshark shows a selection dialog (Figure 36) for the target network interface to capture packets from. For most of our LVC environments it is the ethernet interface.



1. Dialog to select network interface

To begin Wireshark in capture mode, a user double-clicks on one of the displayed network interfaces (Figure 37).



1. View of Wireshark in capturing mode

Often large amounts of network traffic are present. To focus on a specific address or packet type it is useful to apply a filter by selecting the text field (highlighted in Figure 38).



1. View of text field for filter expression

The syntax to apply a filter for a specific network address is ip.addr == <IP addr>. For this example, ip.addr == 192.168.188.255 is entered, which is the multicast address being used for the DIS simulation in progress. After applying the filter by pressing {Enter}, Wireshark displays all packets with 192.168.188.255 either as source or destination address (Figure 39).



1. View of an applied filter for a single IP address

To apply an additional filter for a specific protocol, the name of the protocol must be typed in the text field shown in Figure 38. To filter DIS packets, it is enough to type in “dis” and {Enter}. All protocols must be typed in lower case. Thus the example combined filter is ip.addr == 192.168.188.255 && dis.

Since Wireshark parses all DIS PDUs, information within a DIS packet gets displayed in a human-readable form. To analyze a single packet’s information, it must be selected to show the details view. When all nodes are expanded, packet information is displayed as shown in Figure 40.



1. Details of a single DIS PDU packet parsed by Wireshark

Using AllPduSender.java to send all 72 DIS PDUs to multicast address 239.1.2.3 leads to a capture of all 72 PDUs in Wireshark (Figure 41). Screen capture information can also be copied and saved as a plain-text data file for further processing and analysis.



1. All 72 IEEE DIS PDU types captured with Wireshark

Reference:

WireShark. (n.d.). *Go Deep.* Retrieved January 28, 2020, from https://www.wireshark.org/