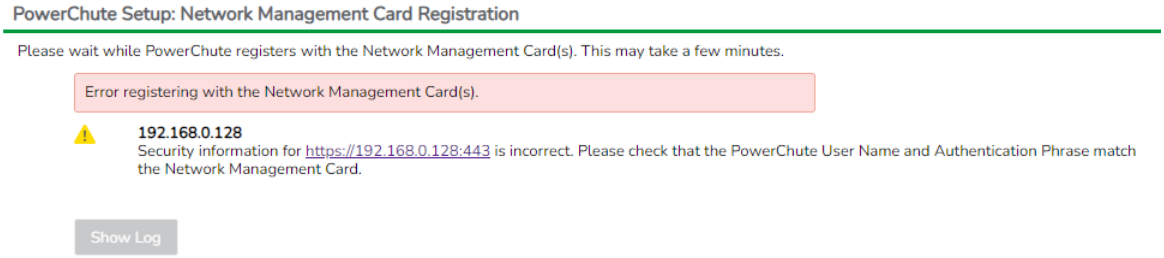
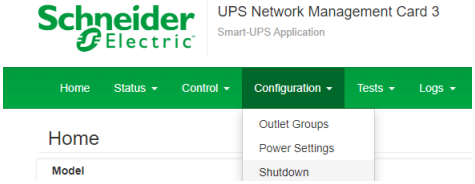
How to troubleshoot “Error registering with the Network Management Card” When running the PowerChute Virtual Machine or PowerChute on a Linux system.

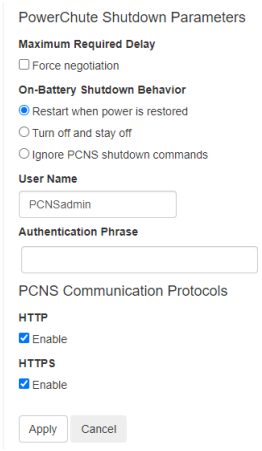
First, review the error to determine the cause.

If the error reports “Security information is incorrect.”
The error is reported if the PowerChute Username or the Authentication Phrase is incorrectly set on the Network Management Card or the PowerChute web UI.

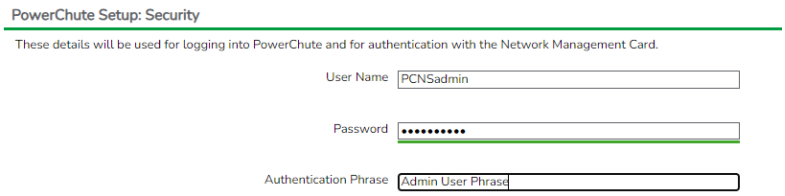


The Username entered in the PowerChute Parameters and the Authentication Phrase must match the Username and Authentication Phrase entered in the PowerChute web UI setup. To view the PowerChute Parameters on the Network Management Card, log into the card and go to Configuration and Shutdown; at the bottom of the page, you will see the PowerChute Parameters.

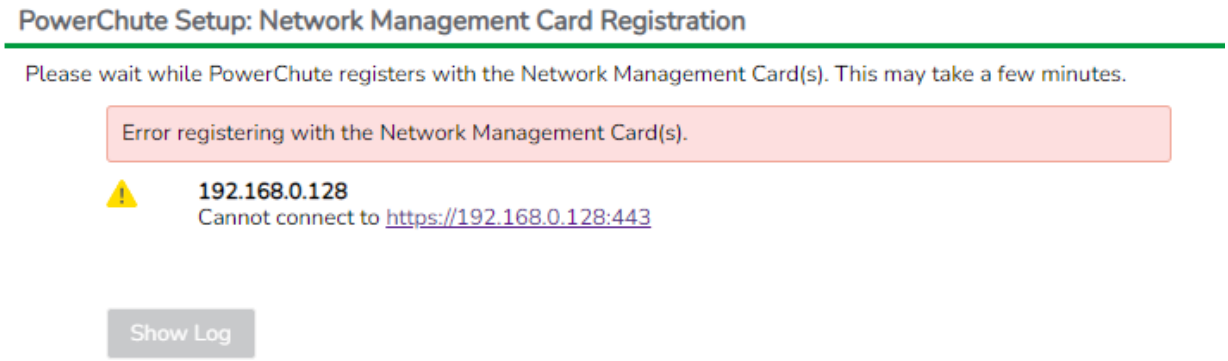


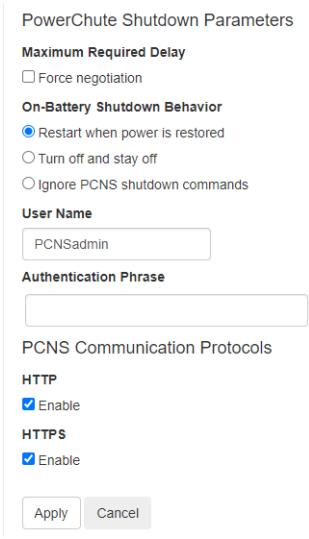


Below is the PowerChute Setup Security page from the PowerChute web UI.

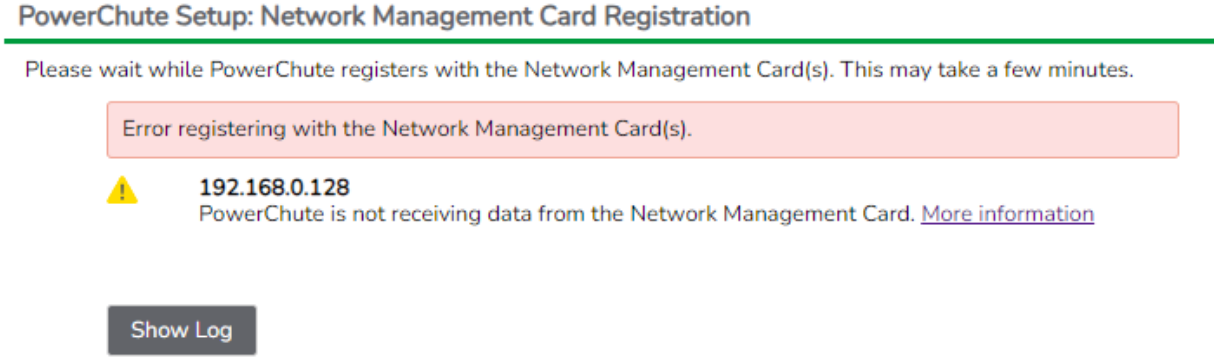


If HTTPS or HTTP is not enabled, you must enable the one you will use for communication in the PowerChute Parameters to allow a connection. If HTTP or HTTPS are not enabled, you will see the error Cannot connect to https://ip address:443 or HTTP://ip address:80.





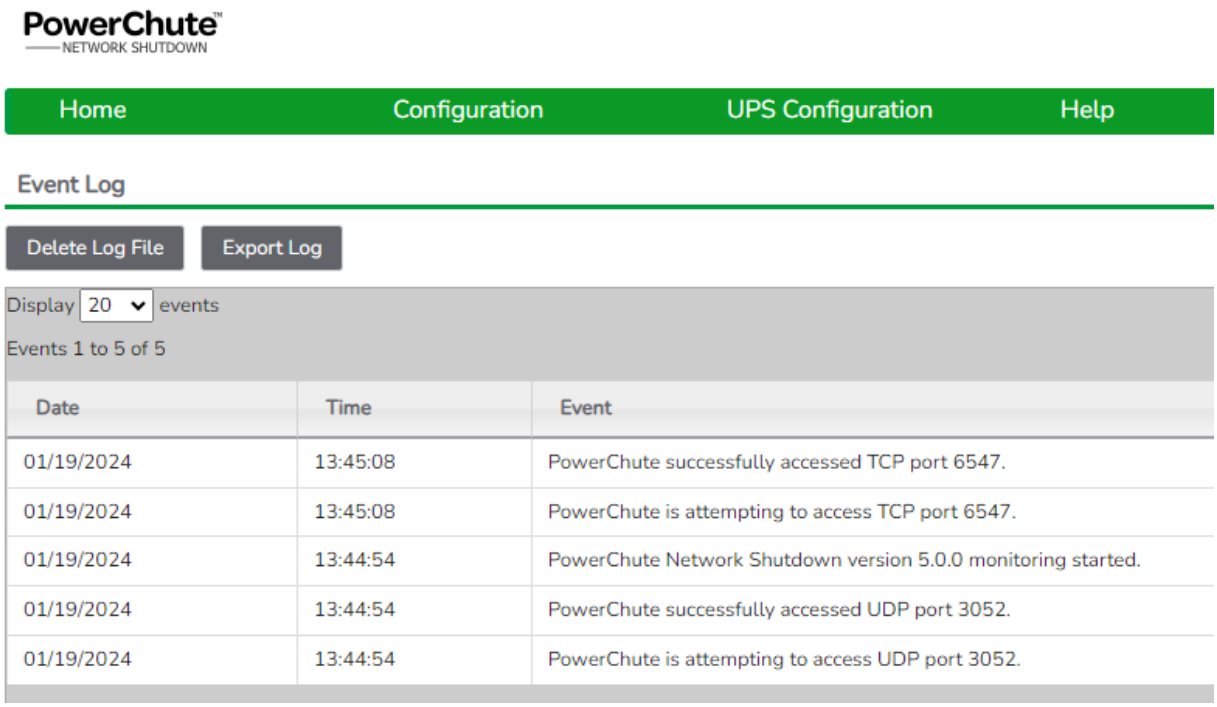
If you see the error "PowerChute is not receiving data from the Network Management Card." That indicates UDP port 3052 is blocked, or the PowerChute client and network Management Cards have mismatched subnet masks. The NMC sends data to the PowerChute clients using UDP port 3052. PowerChute will not receive the data if the port is blocked anywhere along the network path.



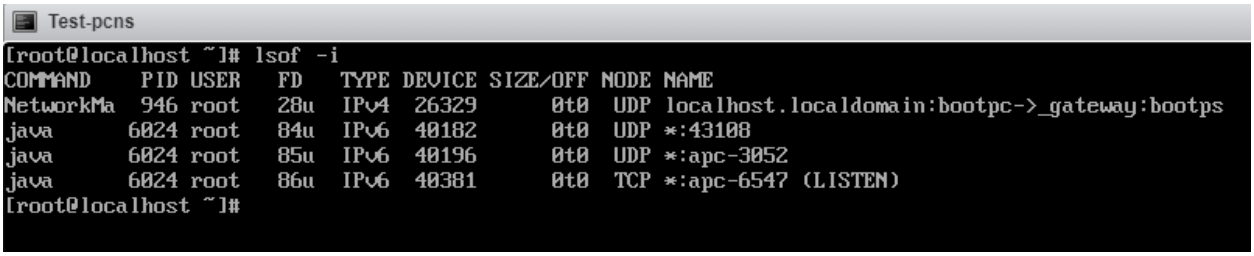
Note 1: If configuring PowerChute with Redundant or Advanced UPSs, refer to Schneider Electric FAQ000259214, along with the steps below.

Note 2: If configuring PowerChute with a Galaxy VL running firmware 10.11.0 & Galaxy VS with firmware 6.72.0, the Network Management Card must be reset after configuration, or PowerChute will report “not receiving data.”

By default, ports 3052 and 6547 are open on the PowerChute VM. When installing PowerChute on any other system, the user is asked to allow the installer to open the needed ports. If, when installing on another system, the user disallows the ports opening, they cannot access the web UI, and PowerChute will not receive data from the NMC/s.
To resolve the issue “PowerChute is not receiving data,” check that PowerChute has opened UDP port 3052 in the PowerChute web UI,

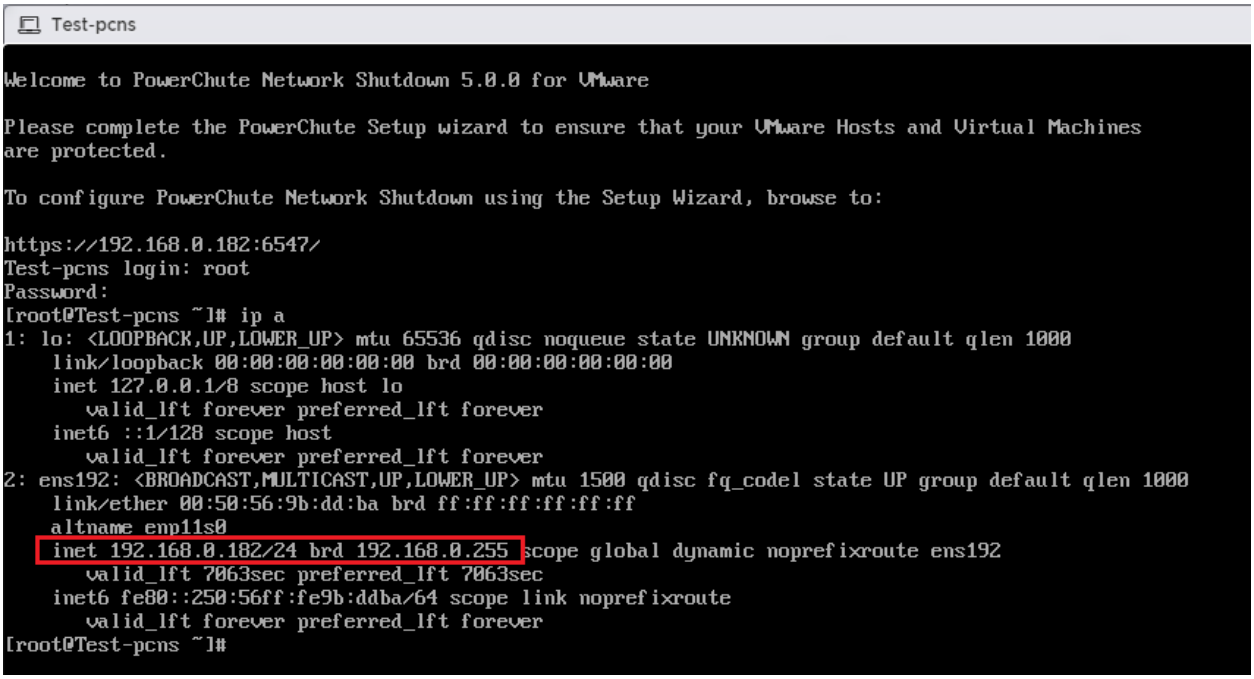


To test the PowerChute VM or a Linux system to verify the ports are open, run the command **lsof -i**

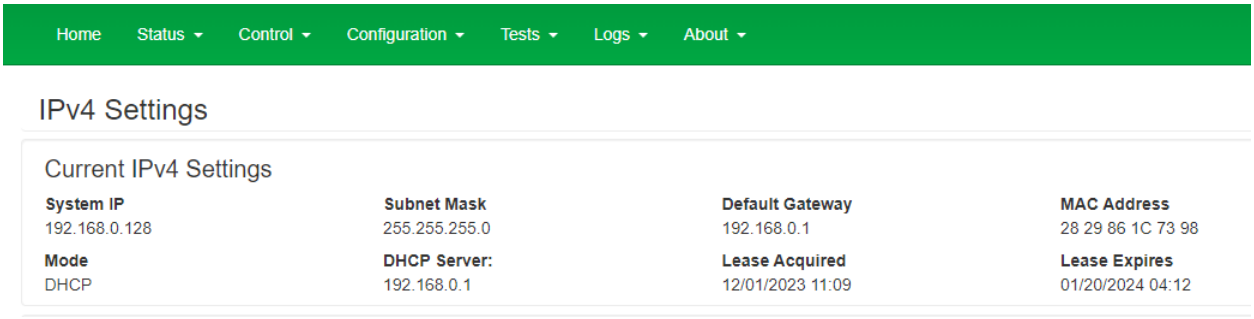


Verify that the PowerChute system and Network Management card/s have compatible subnet masks.

To view the PowerChute network information, enter the command **ip a**.



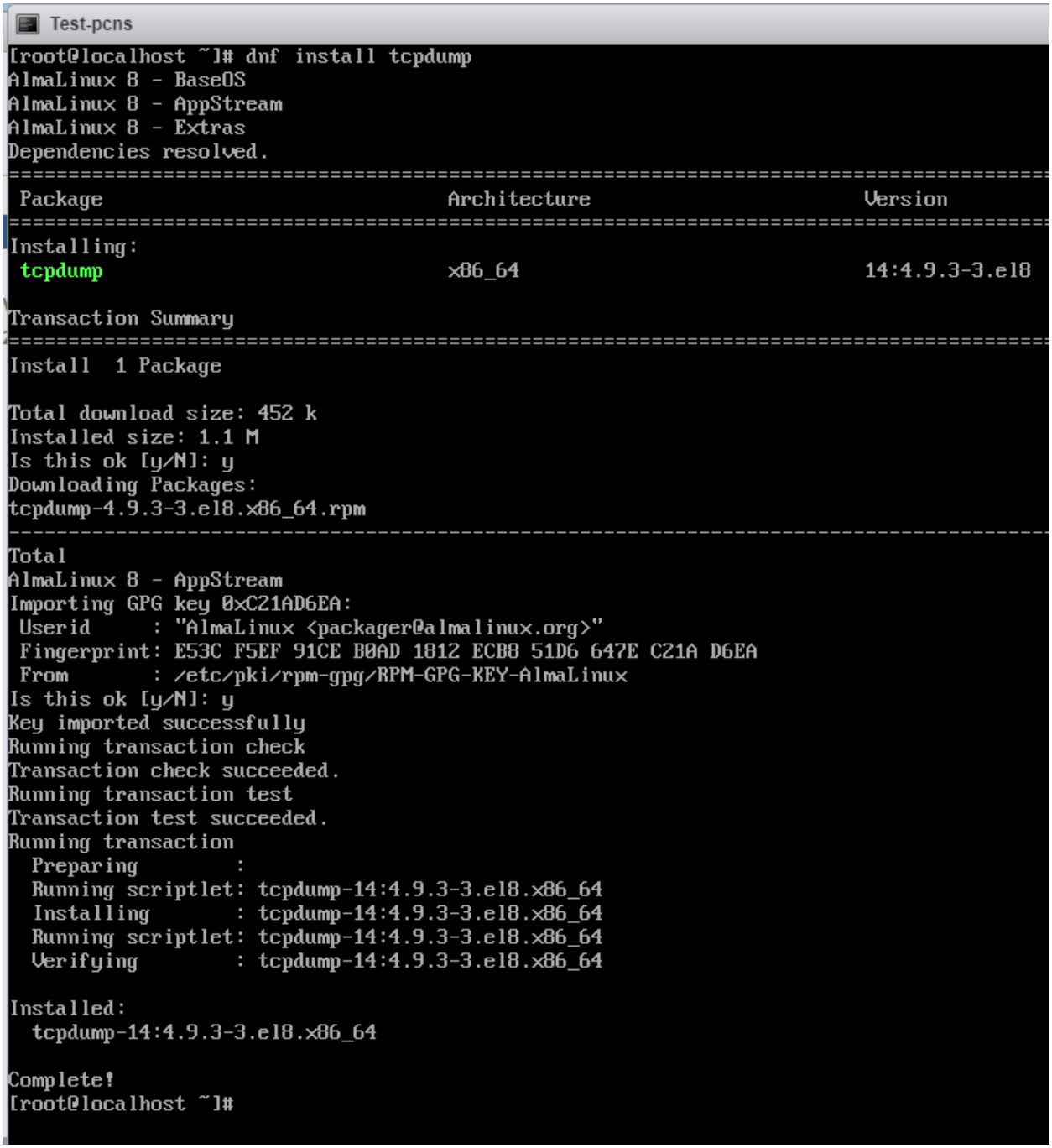
To view the Network Management Card setting, log into the card and go to Configuration > Network > TCP/IP



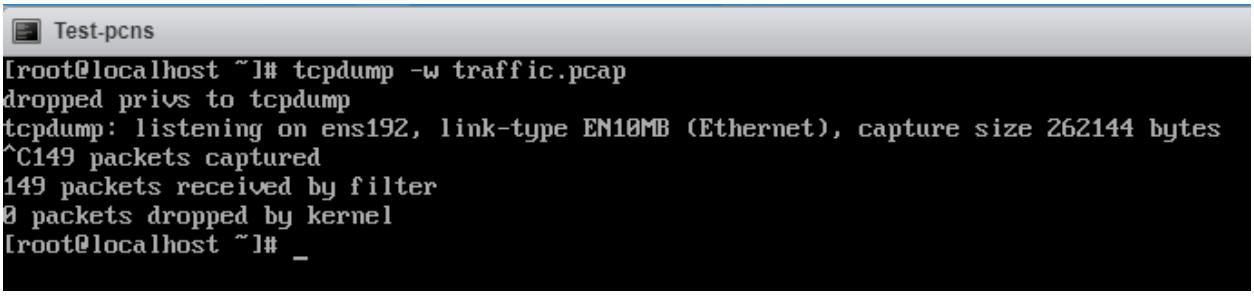
In the examples above, the PowerChute system shows the subnet to be /24, which equals 255.255.255.0, which matches the Network Card setting. Also, the broadcast address is 192.168.0.255, so PowerChute will listen for broadcast messages from that address. The Network Card sends the UDP packets to the broadcast address 192.168.0.255.

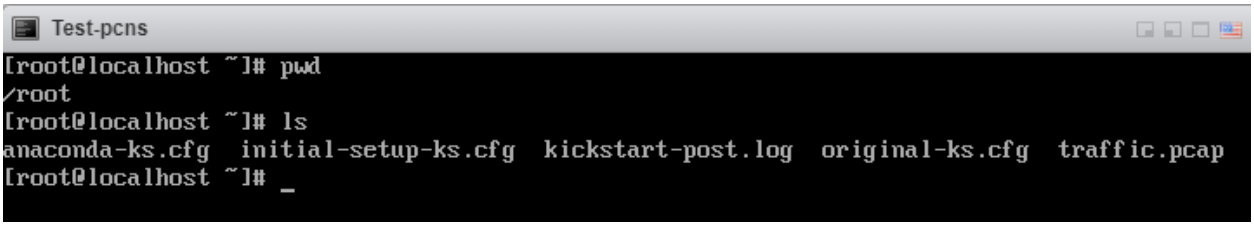
To verify that the PowerChute VM or Linux system receives packets from a Network Management Card, install and run the utility tcpdump. To install on the PowerChute VM, enter the command **dnf install tcpdump**.

NOTE: To install the tcpdump utility, the PowerChute VM must have internet access.

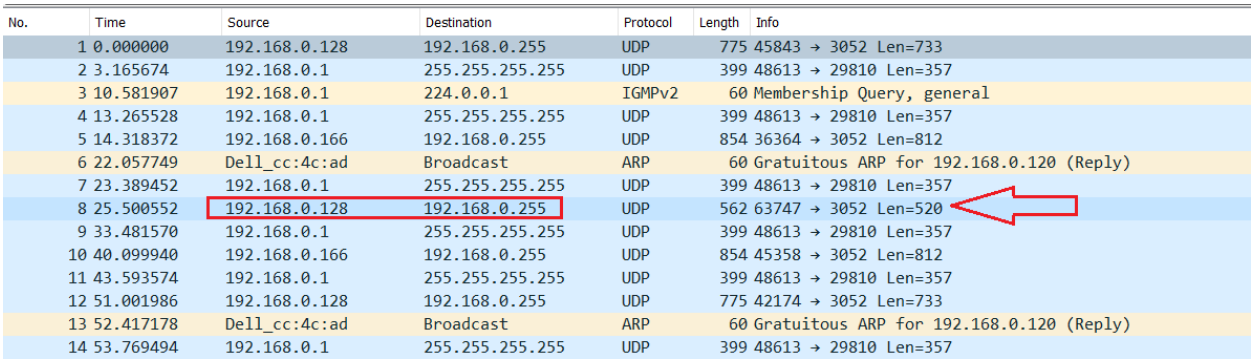


Next, run the command **tcpdump -w traffic.pcap** to capture network traffic to and from the system. Wait 3 to 4 minutes and then enter Ctrl C. to stop the capture. A file with the name traffic.pcap will be created in the present working directory.





To review the capture, run the command **tcpdump -r traffic.pcap** and search for UDP packets from the Network Management Card. In the example below, the capture shows UDP packets from IP address 192.168.0.128, 3052: UDP. The IP address shown is that of a test Network Management Card.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.128	192.168.0.255	UDP	775	45843 → 3052 Len=733
2	3.165674	192.168.0.1	255.255.255.255	UDP	399	48613 → 29810 Len=357
3	10.581907	192.168.0.1	224.0.0.1	IGMPv2	60	Membership Query, general
4	13.265528	192.168.0.1	255.255.255.255	UDP	399	48613 → 29810 Len=357
5	14.318372	192.168.0.166	192.168.0.255	UDP	854	36364 → 3052 Len=812
6	22.057749	Dell_cc:4c:ad	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.120 (Reply)
7	23.389452	192.168.0.1	255.255.255.255	UDP	399	48613 → 29810 Len=357
8	25.500552	192.168.0.128	192.168.0.255	UDP	562	63747 → 3052 Len=520
9	33.481570	192.168.0.1	255.255.255.255	UDP	399	48613 → 29810 Len=357
10	40.099940	192.168.0.166	192.168.0.255	UDP	854	45358 → 3052 Len=812
11	43.593574	192.168.0.1	255.255.255.255	UDP	399	48613 → 29810 Len=357
12	51.001986	192.168.0.128	192.168.0.255	UDP	775	42174 → 3052 Len=733
13	52.417178	Dell_cc:4c:ad	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.120 (Reply)
14	53.769494	192.168.0.1	255.255.255.255	UDP	399	48613 → 29810 Len=357

NOTE: The file traffic.pcap can be viewed on a Windows system with the Wireshark application if Wireshark is available, as shown above.