

## Generating Armageddon Traffic Containing Random MAC Addresses

**Goal:** Set up and run traffic containing random MAC addresses using the LANforge Armageddon feature.

- For more information, see the [LANforge User's Guide: Armageddon \(Accelerated UDP\)](#)

In this test scenario, LANforge Armageddon is set up to run with random MAC addresses. This is useful when performance/stress testing network devices that may not be able to keep up with high-speed traffic containing rapidly changing MAC addresses.

**Note:** In order to use the LANforge Armageddon feature, your system must have the LANforge kernel patch applied and your system must be properly licensed. Please feel free to contact us at [support@candelatech.com](mailto:support@candelatech.com) if you would like to obtain a demo license for the Armageddon feature.

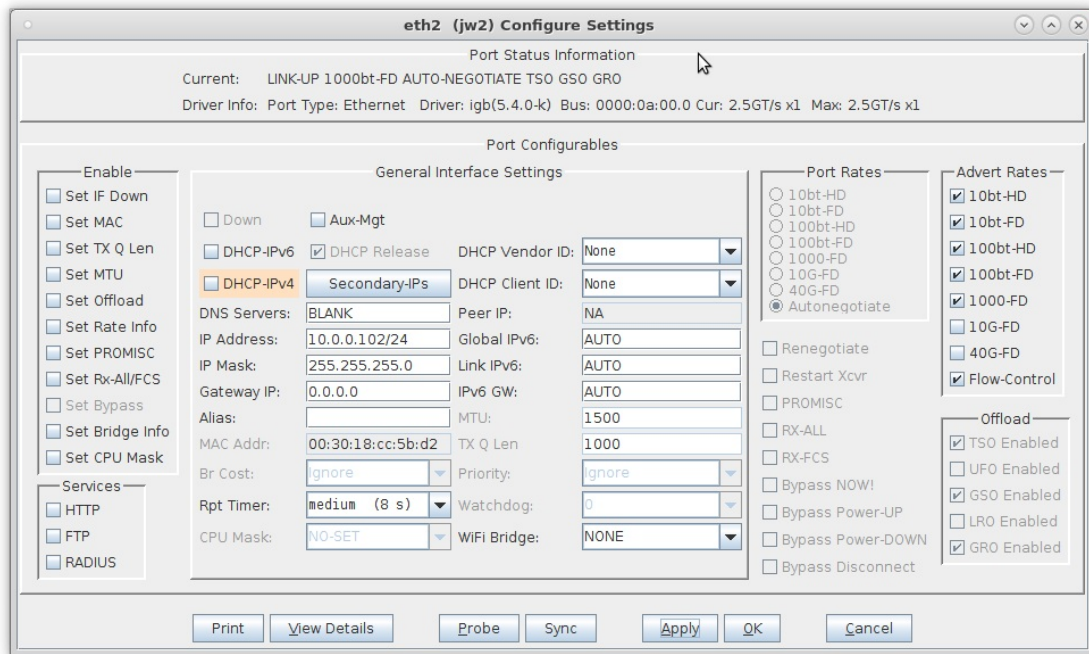
1. Configure the physical interfaces.
  - A. Go to the Port Manager and select ports eth2 and eth3

The screenshot shows the LANforge Manager interface, specifically the Port Manager tab. The interface includes a navigation menu at the top with options like Control, Reporting, Tear-Off, Info, and Plugins. Below the menu are several buttons: Stop All, Restart Manager, Refresh, and HELP. The main area contains a table titled "All Ethernet Interfaces (Ports) for all Resources." The table has columns for Port, Phase, Down, IP, SEC, Alias, Parent Dev, RX Bytes, RX Pkts, Pps RX, bps RX, TX Bytes, TX Pkts, and Pps TX. The data in the table is as follows:

Port	Pha...	Down	IP	SEC	Alias	Parent Dev	RX Bytes	RX Pkts	Pps RX	bps RX	TX Bytes	TX Pkts	Pps TX
1.1.0	<input type="checkbox"/>	<input type="checkbox"/>	192.168.100.103	0	eth0		1,599,881	13,894	6	5,964	6,749,974	9,032	4
1.1.1	<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	0	eth1		0	0	0	0	0	0	0
1.1.2	<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	0	eth2		6,067,356,...	4,007,503	0	0	6,065,332,...	4,006,407	0
1.1.3	<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	0	eth3		6,065,332,...	4,006,407	0	7	6,067,358,...	4,007,521	0
1.1.4	<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	0	eth4		0	0	0	0	0	0	0
1.1.5	<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	0	eth5		0	0	0	0	0	0	0

At the bottom of the window, it says "Logged in to: 192.168.100.103:4002 as: Admin".

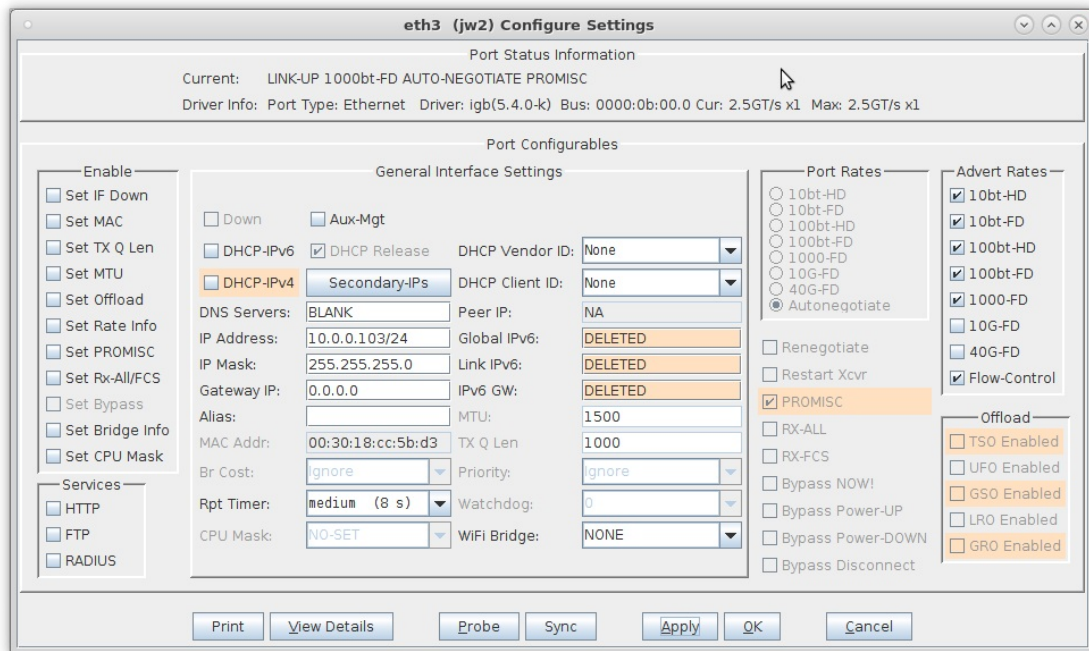
B. Modify ports eth2 and eth3



A. In this example, eth2 and eth3 are connected to another LANforge system running a WanLink so that the Armageddon traffic can be sniffed on the other machine's interface

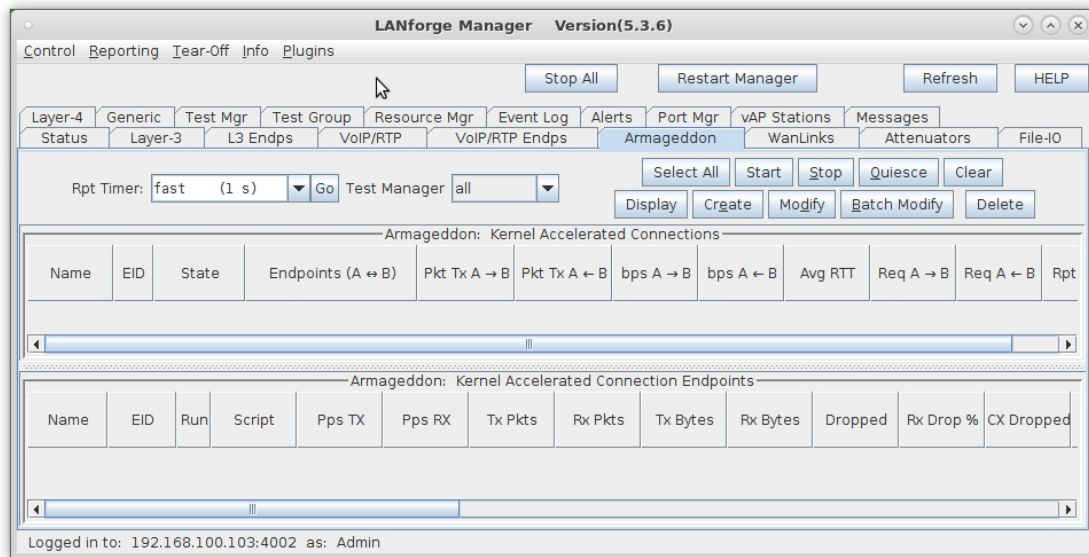
B. **NOTE:** Be sure that both ports are in Promiscuous mode by selecting the **Set PROMISC** and **PROMISC** checkboxes

C. Configure each port with a valid IP address, then click **OK**

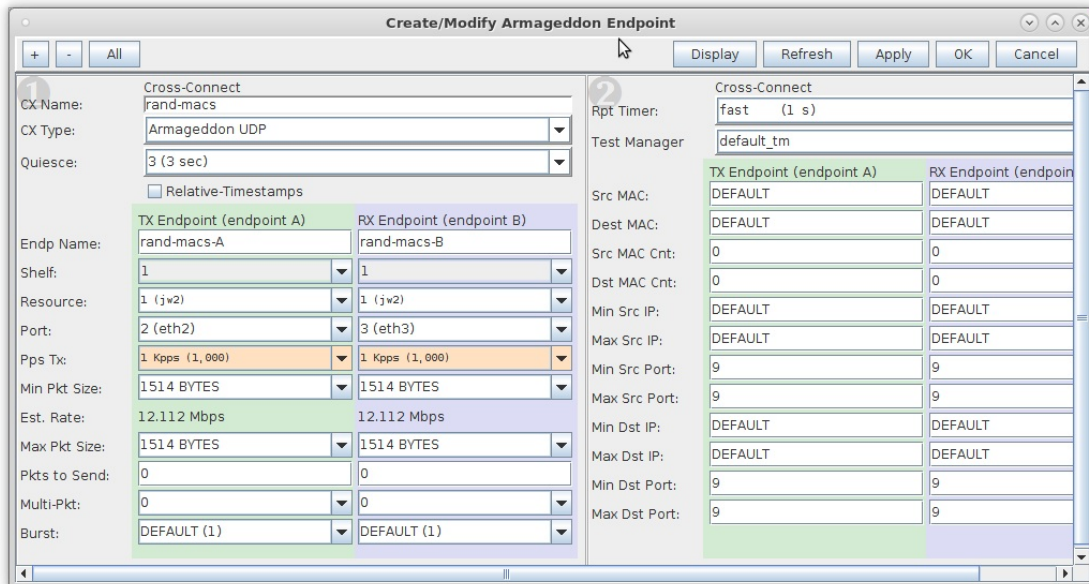


For more information see [LANforge User's Guide: Ports \(Interfaces\)](#)

2. Create the Armageddon cross-connect.
  - A. On the **Armageddon** tab, click **Create**



- B. Enter a CX Name, select ports eth2 and eth3, then enter the speed and packet size for both endpoints



- C. Enter values for the Source and Destination MAC addresses, specify a MAC count, and deselect Use Router MAC for both endpoints.

For more information see [LANforge User's Guide: Armageddon \(Accelerated UDP\)](#)

3. Run the Armageddon cross-connect and verify results with Wireshark.  
 A. Select the Armageddon connection then click **Start**

Name	EID	State	Endpoints (A ↔ B)	Pkt Tx A → B	Pkt Tx A ← B	bps A → B	bps A ← B	Avg RTT	Req A → B	Req A ← B	Rpt
rand-macs	14.2	Run	rand-macs-A ↔ ra...	44,086	44,080	12,318,661	12,132,205	357	1,000	1,000	

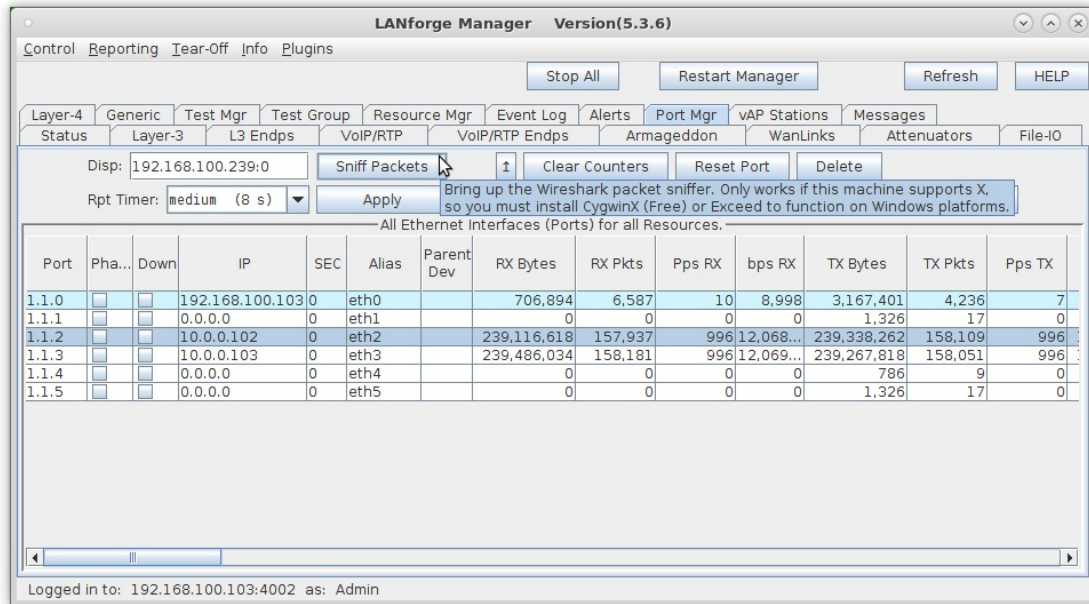
  

Name	EID	Run	Script	Pps TX	Pps RX	Tx Pkts	Rx Pkts	Tx Bytes	Rx Bytes	Dropped	Rx Drop %	CX Dropped
rand-ma...	1.1.2.1	✓	None	996	995	44,086	43,941	66,746,204	66,526,674	0	0	0
rand-ma...	1.1.3.2	✓	None	996	996	44,080	44,225	66,737,120	66,956,650	0	0	0

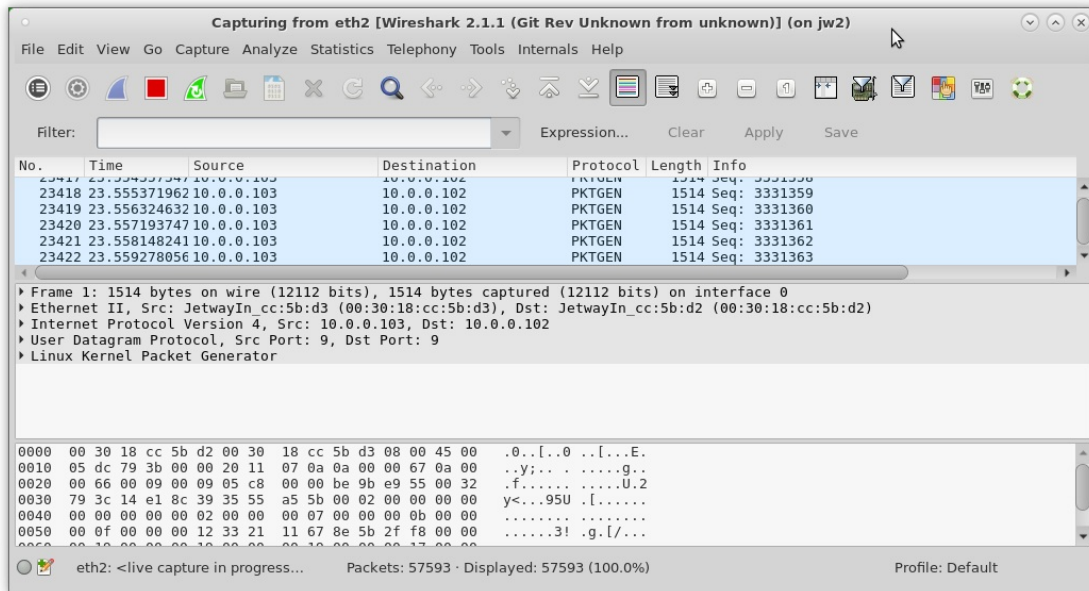
Logged in to: 192.168.100.103:4002 as: Admin



- B. On the **Port Mgr** tab of the other LANforge system, select one of the physical interfaces in the Armageddon connection

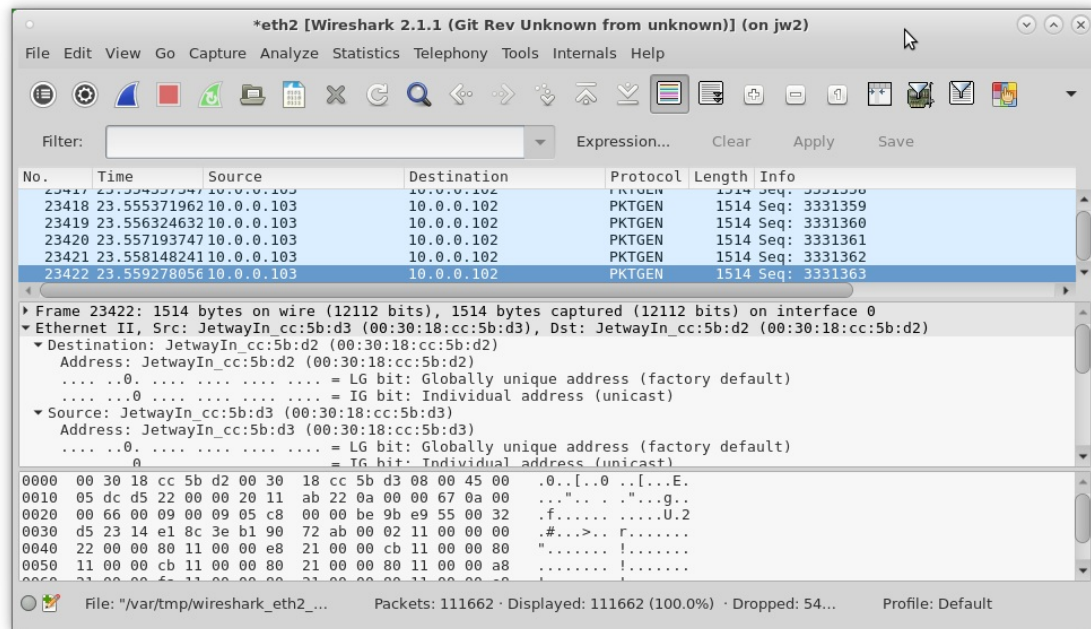


- C. Click **Sniff Packets** to launch Wireshark and begin sniffing traffic.

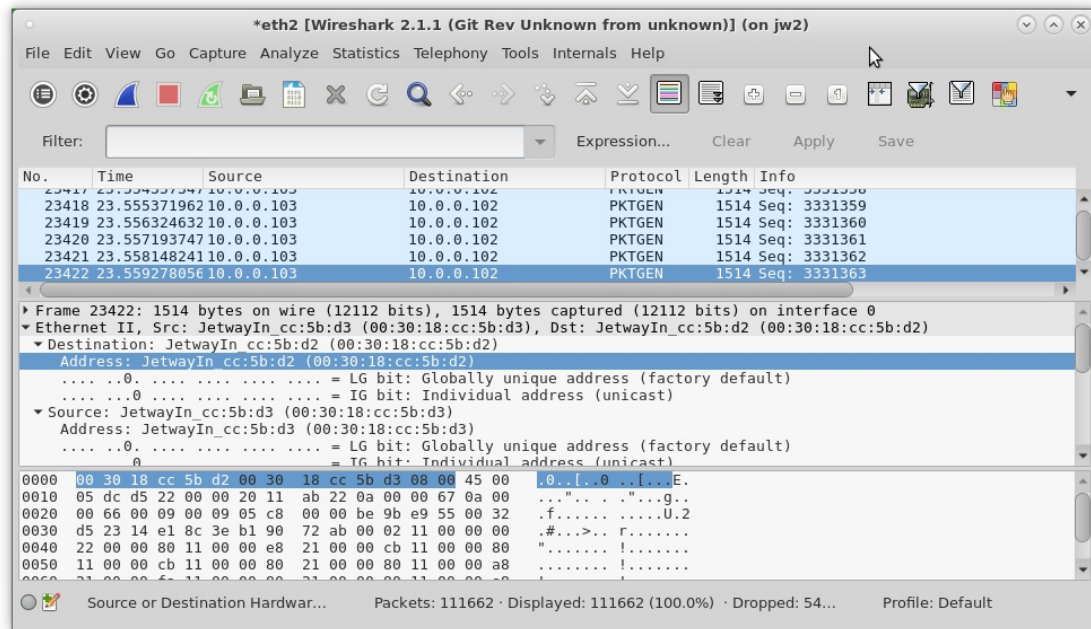


- A. Stop the Wireshark capture after a few seconds via the stop icon or pull-down menu (**Capture>Stop**)

D. Select several packets and note their MAC addresses



E. Verify that the MAC addresses for each packet are different



For more information see [LANforge User's Guide: Armageddon \(Accelerated UDP\)](#)

Candela Technologies, Inc., 2417 Main Street, Suite 201, Ferndale, WA 98248, USA  
www.candela-tech.com | sales@candela-tech.com | +1.360.380.1618