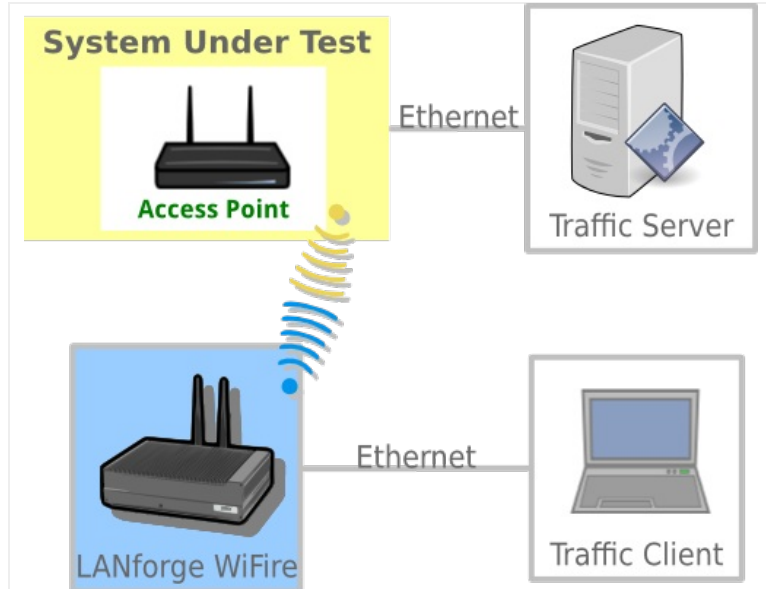


Generate WiFi Traffic from an External Connection

Goal: Create a bridged WiFi station that redirects traffic from an ethernet port.

It is possible to use a system on a wired LAN to generate traffic through a LANforge virtual WiFi station. This example will show a Windows PC driving traffic across a LANforge CT520 STA to the associated AP. This is a useful scenario for driving custom traffic between traffic testing software endpoints distinct from the LANforge system. A virtualized Windows PC will work with this scenario.

The primary technique in this cookbook uses a technique where the MAC address of the WiFi STA is spoofing the address of the Windows PC. It is also possible to use this technique with IPv4 addresses and not MAC addresses. However, using MAC addresses will allow IPv6 traffic to work.



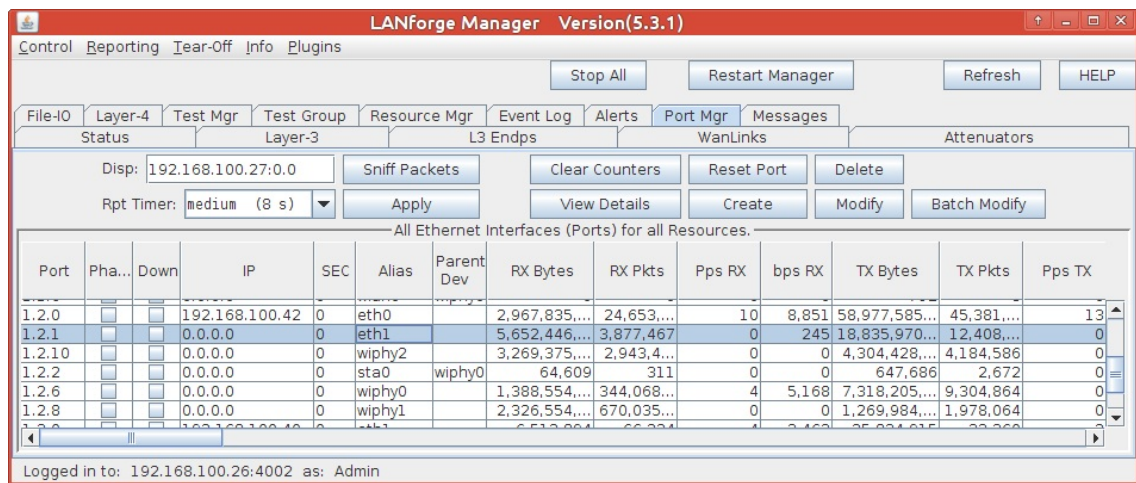
1. Find the MAC Address of the Windows PC.

- A. We will use MAC address `08:00:27:c4:4e:4f`. This will be used when you configure the WiFi STA on the LANforge machine.
- B. Please set the IP address of the interface if it is not yet set.

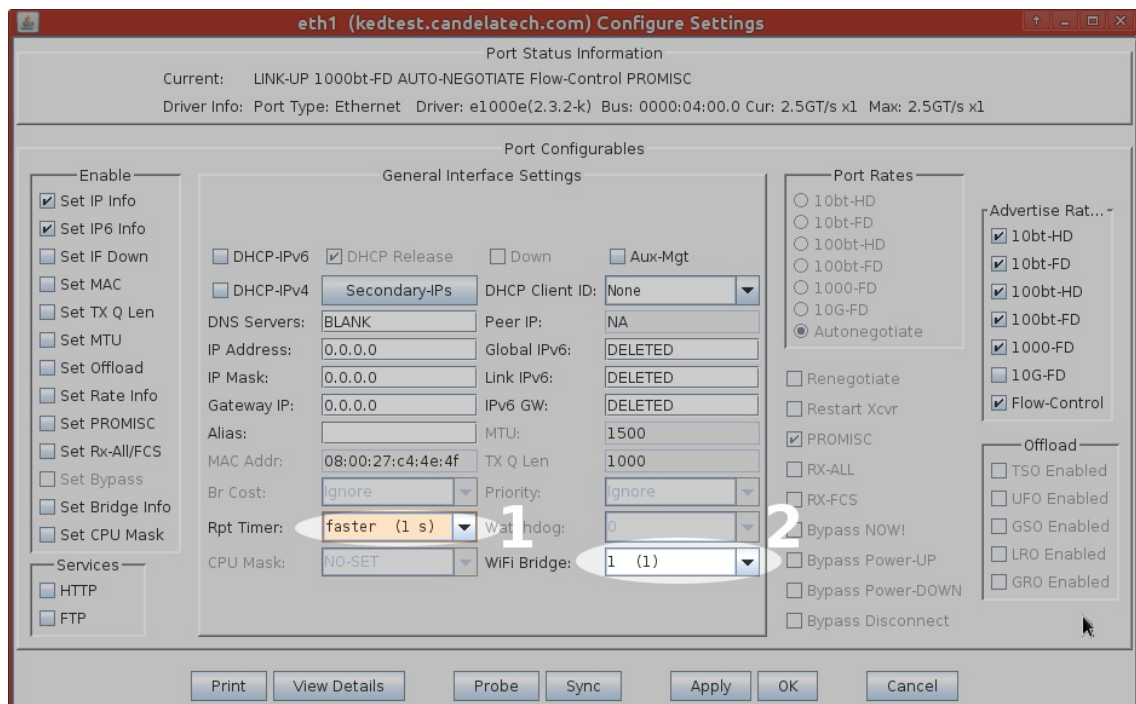
For more information see [Windows IP Addresses](#)

2. Configure your LANforge Wireless Station. We will be configuring the MAC addresses of a station to be the MAC address of the Windows PC we just found.

- A. In the Ports tab, double-click on the ethernet port on the same switch as the Windows PC (eth1 in this example).



- B. Configure the port MAC address and WiFi-Bridge settings to be:



- Do not set the mac address or the ip address of the port
- Set Rpt Timer to **faster (1 s)**
- Select **1** for WiFi Bridge
- Click the **OK** button

C. Configure a WiFi station. This example will be connecting to a WiFi AP with the SSID jedtest.

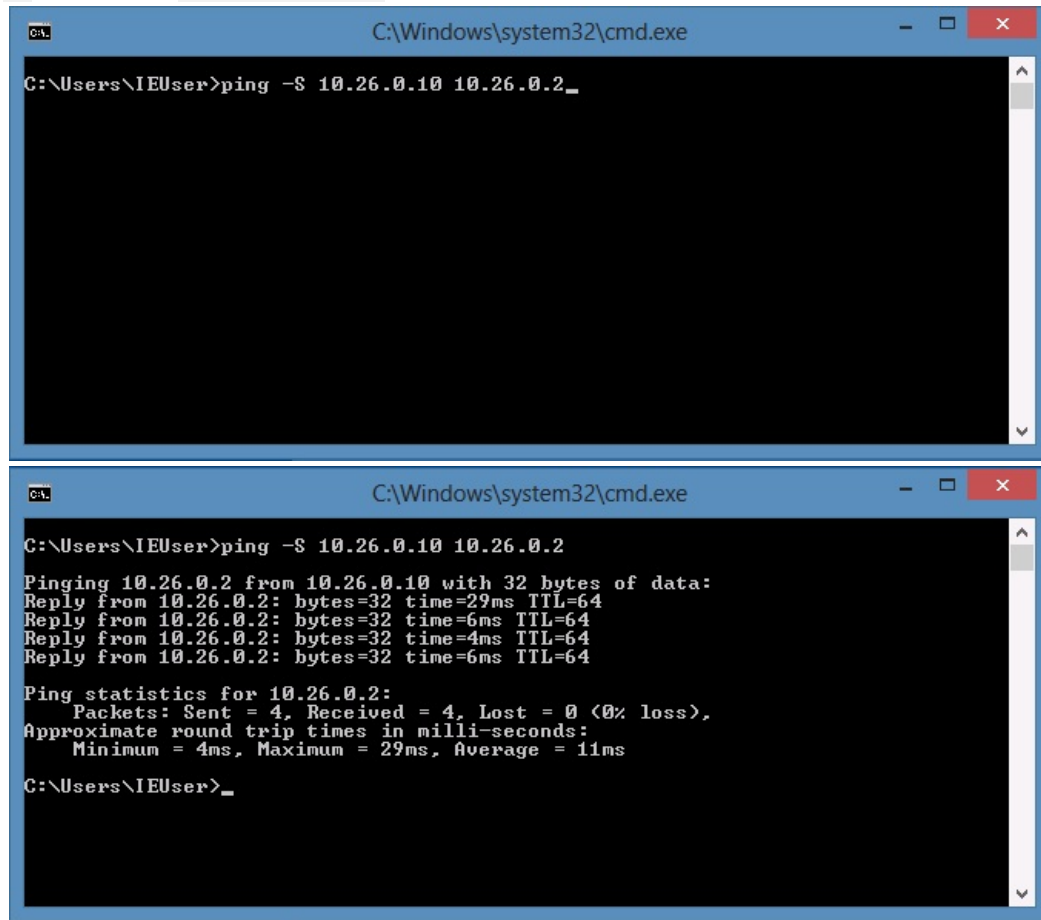
The screenshot shows the 'sta0 (kedtest.candelatech.com) Configure Settings' window. The 'Port Status Information' section shows 'Current: LINK-UP Authorized' and 'Driver Info: Port Type: WIFI-STA Parent: wiphy0'. The 'Port Configurables' section has two tabs: 'Standard Configuration' and 'Advanced Configuration'. In the 'Standard Configuration' tab, the 'Enable' section has 'Set MAC' checked (1). The 'Services' section has 'HTTP' and 'FTP' unchecked. The 'Low Level' section has 'PROMISC', 'TSO Enabled', 'UFO Enabled', 'GSO Enabled', 'LRO Enabled', and 'GRO Enabled' all unchecked. In the 'Advanced Configuration' tab, the 'General Interface Settings' section has 'DHCP-IPv6' and 'DHCP-IPv4' unchecked, 'DHCP Release' checked, 'Down' unchecked, and 'Aux-Mgt' unchecked. The 'Secondary-IPs' section has 'DHCP Client ID' set to 'None'. The 'DNS Servers' section has 'BLANK' in the text box. The 'IP Address' is 0.0.0.0, 'IP Mask' is 0.0.0.0, and 'Gateway IP' is 0.0.0.0. The 'Alias' is blank. The 'MAC Addr' is 08:00:27:c4:4e:4f (2). The 'Rpt Timer' is 'faster (1 s)' (3). The 'MTU' is 1500 and 'TX Q Len' is 1000. The 'WiFi Bridge' is '1 (1)' (4). The 'WiFi Settings' section has 'SSID' set to 'jedtest' (5), 'AP' set to 'DEFAULT', 'Key/Phrase' is blank, 'Mode' is '802.11abgn' (6), 'Rate' is 'OS Default', 'AMPDU-Factor' is 'OS Default', 'AMPDU-Density' is 'OS Default', 'Max-AMSDU' is 'OS Default', and 'Bridge-IP' is '0.0.0.0'. There are checkboxes for 'Use WPA', 'Use WPA2', 'Use WEP', 'Disable HT40', 'Disable SGI', 'Scan Hidden', and 'Allow Migration', all of which are unchecked. At the bottom of the window are buttons for 'Print', 'View Details', 'Probe', 'Display Scan', 'Sync', 'Apply', 'OK', and 'Cancel'.

- A. Enable **Set MAC**
- B. Use **08:00:27:c4:4e:4f** for the MAC Addr
- C. Set Rpt Timer to **faster (1 s)**
- D. Select **1** for WiFi Bridge
- E. Enter **jedtest** for the SSID
- F. Select **802.11abgn** for the Mode
- G. Click the **OK** button

D. (Note: these MAC addresses will remain persistent even through a LANforge Manager restart. To restore the physical mac addresses, you need to reboot the LANforge machine or use ethtool to find the physical hardware address.)

3. Sending and Validating Traffic

- A. Use ping on the Windows machine to reach 10.26.0.2, the AP machine. To ping from a specific interface, use the `-S` switch like so: `ping -S 10.26.0.10 10.26.0.2`



```
C:\Windows\system32\cmd.exe

C:\Users\IEUser>ping -S 10.26.0.10 10.26.0.2_

C:\Windows\system32\cmd.exe

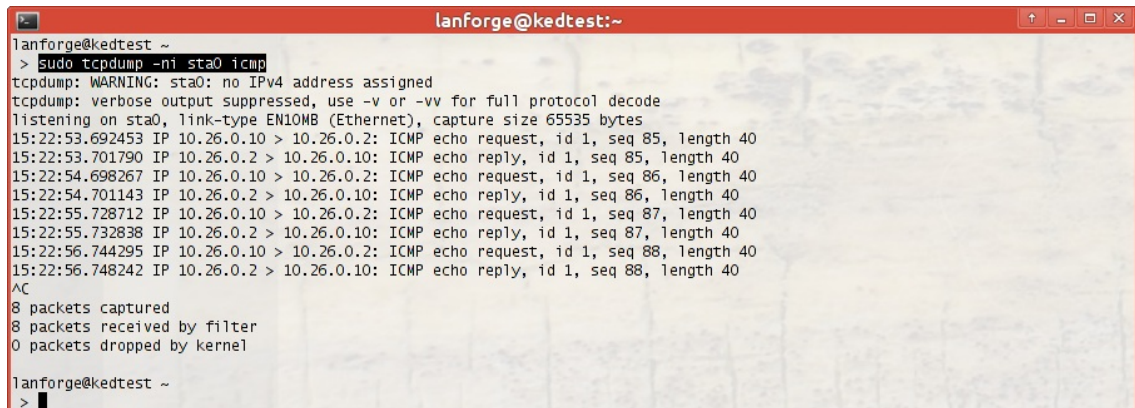
C:\Users\IEUser>ping -S 10.26.0.10 10.26.0.2

Pinging 10.26.0.2 from 10.26.0.10 with 32 bytes of data:
Reply from 10.26.0.2: bytes=32 time=29ms TTL=64
Reply from 10.26.0.2: bytes=32 time=6ms TTL=64
Reply from 10.26.0.2: bytes=32 time=4ms TTL=64
Reply from 10.26.0.2: bytes=32 time=6ms TTL=64

Ping statistics for 10.26.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 29ms, Average = 11ms

C:\Users\IEUser>
```

- B. On LANforge, use tcpdump to view packets traversing the Station interface, `sudo tcpdump -ni sta0 icmp`



```
lanforge@kedtest:~
> sudo tcpdump -ni sta0 icmp
tcpdump: WARNING: sta0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on sta0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:22:53.692453 IP 10.26.0.10 > 10.26.0.2: ICMP echo request, id 1, seq 85, length 40
15:22:53.701790 IP 10.26.0.2 > 10.26.0.10: ICMP echo reply, id 1, seq 85, length 40
15:22:54.698267 IP 10.26.0.10 > 10.26.0.2: ICMP echo request, id 1, seq 86, length 40
15:22:54.701143 IP 10.26.0.2 > 10.26.0.10: ICMP echo reply, id 1, seq 86, length 40
15:22:55.728712 IP 10.26.0.10 > 10.26.0.2: ICMP echo request, id 1, seq 87, length 40
15:22:55.732838 IP 10.26.0.2 > 10.26.0.10: ICMP echo reply, id 1, seq 87, length 40
15:22:56.744295 IP 10.26.0.10 > 10.26.0.2: ICMP echo request, id 1, seq 88, length 40
15:22:56.748242 IP 10.26.0.2 > 10.26.0.10: ICMP echo reply, id 1, seq 88, length 40
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel

lanforge@kedtest:~
>
```