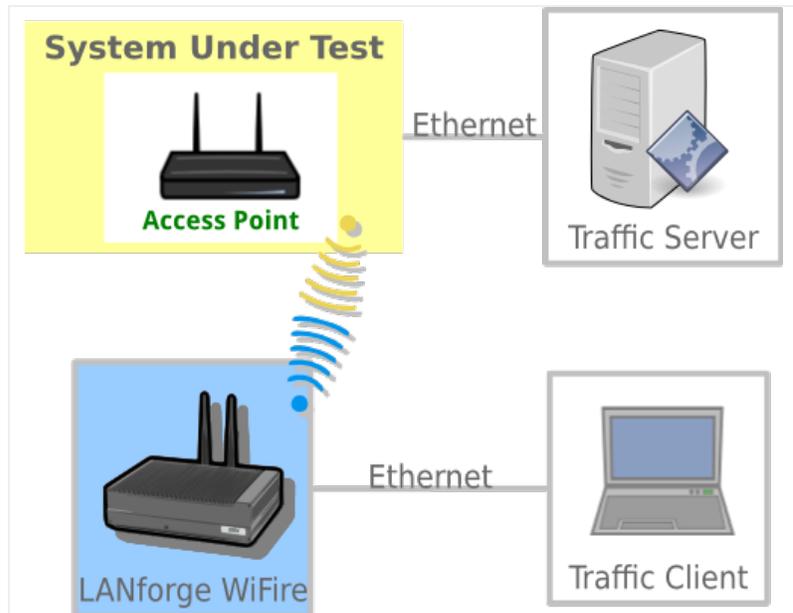


Generate WiFi Traffic from an External Connection

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).

LANforge Manager Version(5.3.1)

Control Reporting Tear-Off Info Plugins

Stop All Restart Manager Refresh HELP

File-I/O Layer-4 Test Mgr Test Group Resource Mgr Event Log Alerts Port Mgr Messages

Status Layer-3 L3 Endps WanLinks Attenuators

Disp: 192.168.100.27:0.0 Sniff Packets Clear Counters Reset Port Delete

Rpt Timer: medium (8 s) Apply View Details Create Modify Batch Modify

All Ethernet Interfaces (Ports) for all Resources.

Port	Pha...	Down	IP	SEC	Alias	Parent Dev	RX Bytes	RX Pkts	Pps RX	bps RX	TX Bytes	TX Pkts	Pps TX
1.2.0			192.168.100.42	0	eth0		2,967,835,...	24,653,...	10	8,851	58,977,585,...	45,381,...	13
1.2.1			0.0.0.0	0	eth1		5,652,446,...	3,877,467	0	245	18,835,970,...	12,408,...	0
1.2.10			0.0.0.0	0	wiphy2		3,269,375,...	2,943,4...	0	0	4,304,428,...	4,184,586	0
1.2.2			0.0.0.0	0	sta0	wiphy0	64,609	311	0	0	647,686	2,672	0
1.2.6			0.0.0.0	0	wiphy0		1,388,554,...	344,068...	4	5,168	7,318,205,...	9,304,864	0
1.2.8			0.0.0.0	0	wiphy1		2,326,554,...	670,035...	0	0	1,269,984,...	1,978,064	0

Logged in to: 192.168.100.26:4002 as: Admin

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

eth1 (kedtest.candelatech.com) Configure Settings

Port Status Information

Current: LINK-UP 1000bt-FD AUTO-NEGOTIATE Flow-Control PROMISC

Driver Info: Port Type: Ethernet Driver: e1000e(2.3.2-k) Bus: 0000:04:00.0 Cur: 2.5GT/s x1 Max: 2.5GT/s x1

Port Configurables

General Interface Settings

Enable

- Set IP Info
- Set IP6 Info
- Set IF Down
- Set MAC
- Set TX Q Len
- Set MTU
- Set Offload
- Set Rate Info
- Set PROMISC
- Set Rx-All/FCS
- Set Bypass
- Set Bridge Info
- Set CPU Mask

Services

- HTTP
- FTP

General Interface Settings

DHCP-IPv6 DHCP Release Down Aux-Mgt

DHCP-IPv4 Secondary-IPs DHCP Client ID: None

DNS Servers: BLANK Peer IP: NA

IP Address: 0.0.0.0 Global IPv6: DELETED

IP Mask: 0.0.0.0 Link IPv6: DELETED

Gateway IP: 0.0.0.0 IPv6 GW: DELETED

Alias: MTU: 1500

MAC Addr: 08:00:27:c4:4e:4f TX Q Len: 1000

Br Cost: ignore Priority: ignore

Rpt Timer: faster (1 s) 1

CPU Mask: NO-SET WiFi Bridge: 1 (1) 2

Port Rates

- 10bt-HD
- 10bt-FD
- 100bt-HD
- 100bt-FD
- 1000-FD
- 10G-FD
- Autonegotiate

Renegotiate

Restart Xcvr

PROMISC

RX-ALL

RX-FCS

Bypass NOW!

Bypass Power-UP

Bypass Power-DOWN

Bypass Disconnect

Advertise Rat...

- 10bt-HD
- 10bt-FD
- 100bt-HD
- 100bt-FD
- 1000-FD
- 10G-FD
- Flow-Control

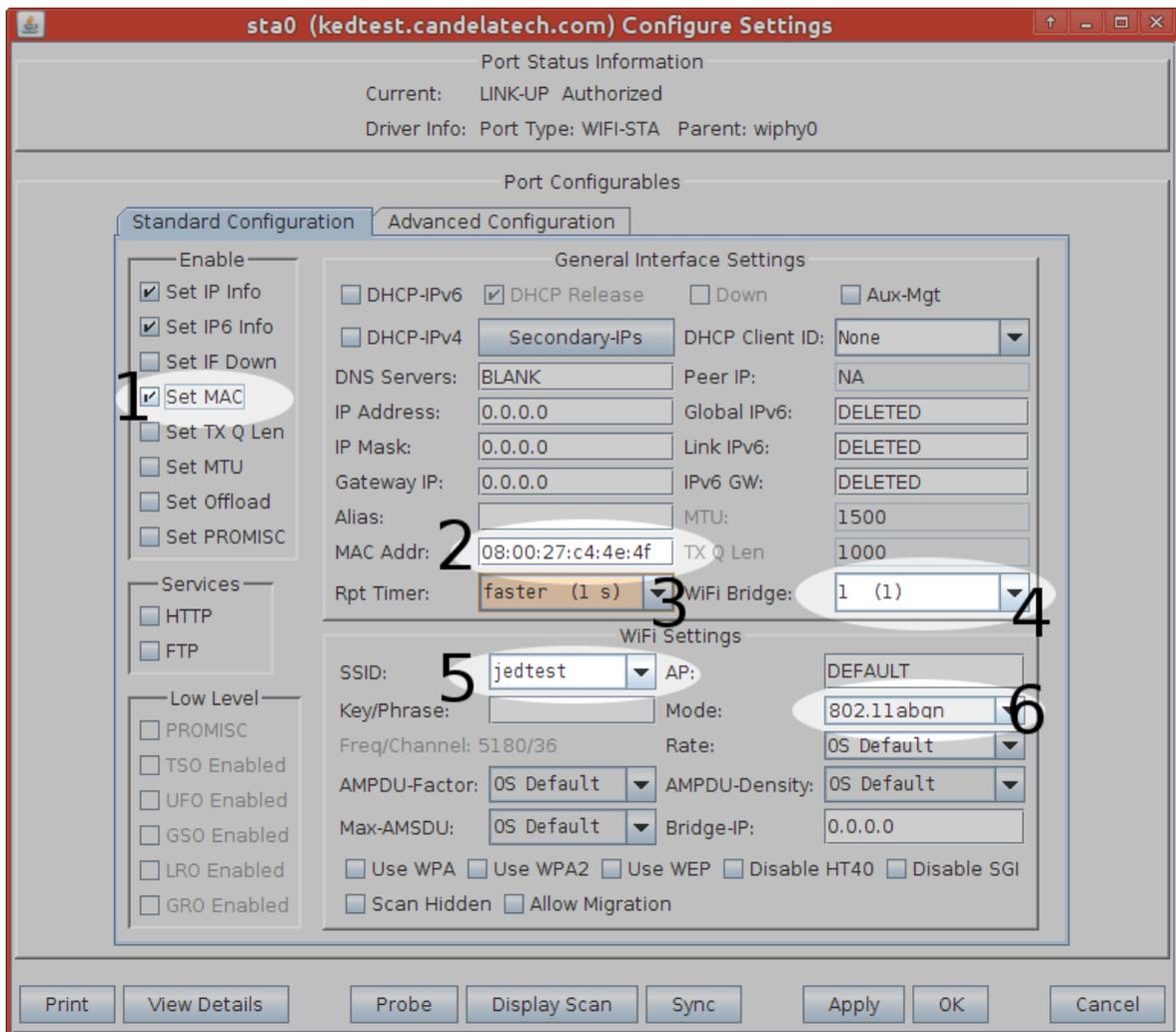
Offload

- TSO Enabled
- UFO Enabled
- GSO Enabled
- LRO Enabled
- GRO Enabled

Print View Details Probe Sync Apply OK Cancel

- 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*.

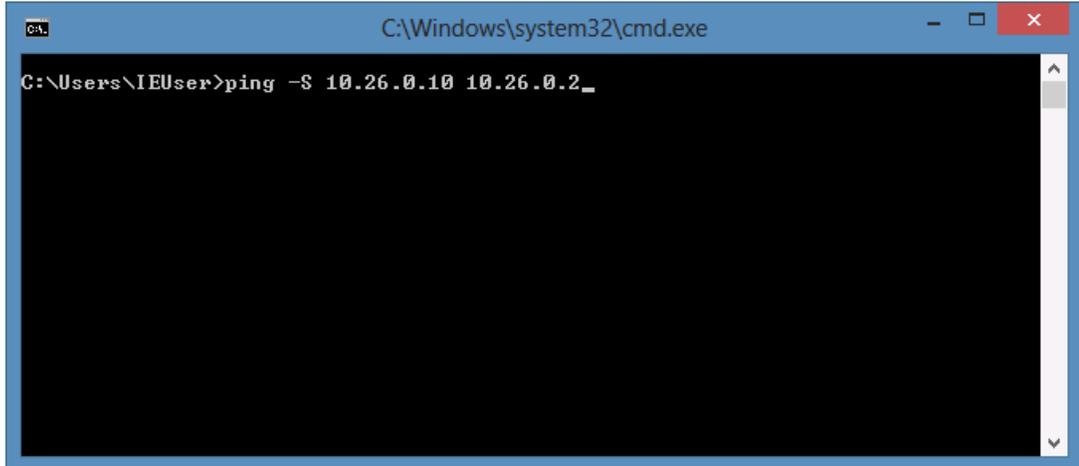


- A. Enable **Set MAC**
- B. Use **08:00:27:c4:4e:4f** for the *MAC Addr*
- C. Set *Rpt Timer* to **faster (1 s)**
- D. Select **1** for *WiFi Bridge*
- E. Enter **jedtest** for the *SSID*
- F. Select **802.11abgn** for the *Mode*
- G. Click the **OK** button

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.)

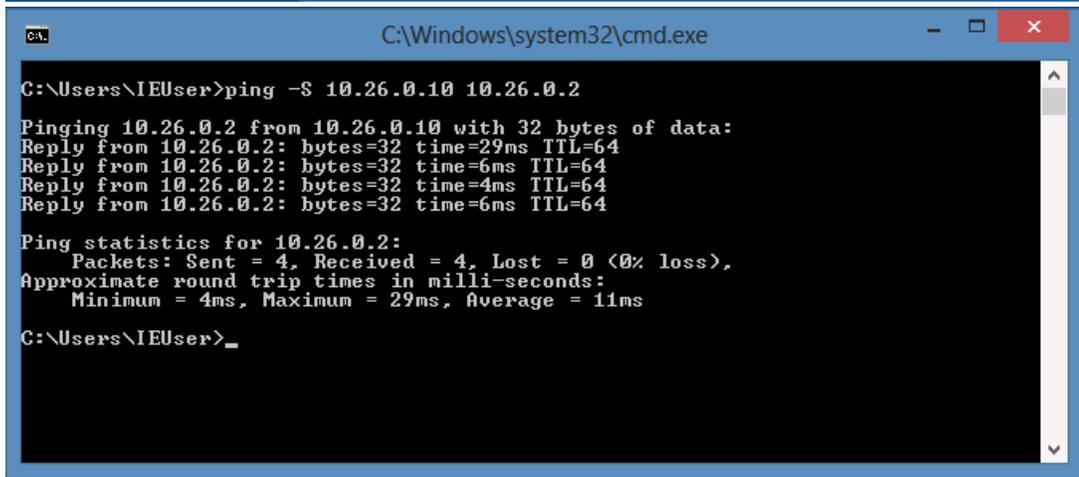
3. Sending and Validating Traffic

- 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

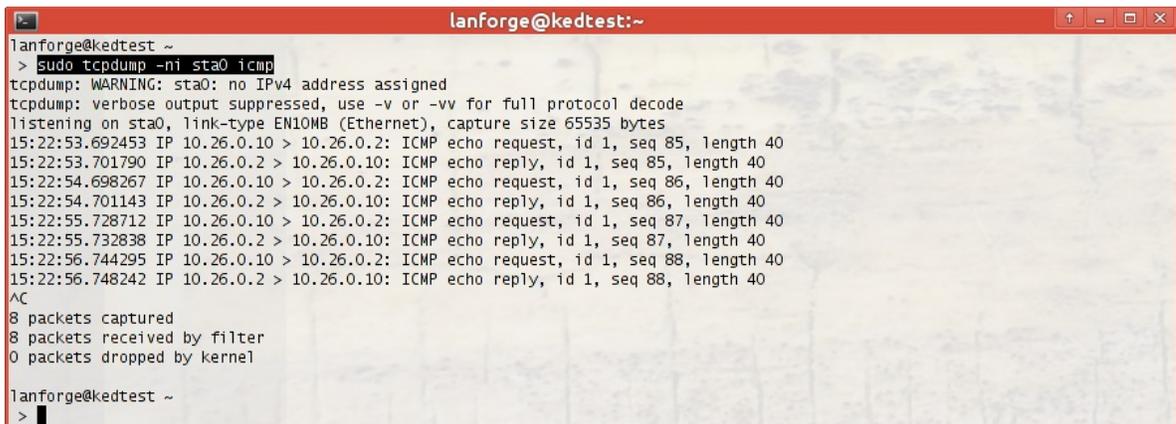
C:\Users\IEUser>ping -S 10.26.0.10 10.26.0.2

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:~
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 ~
>
```