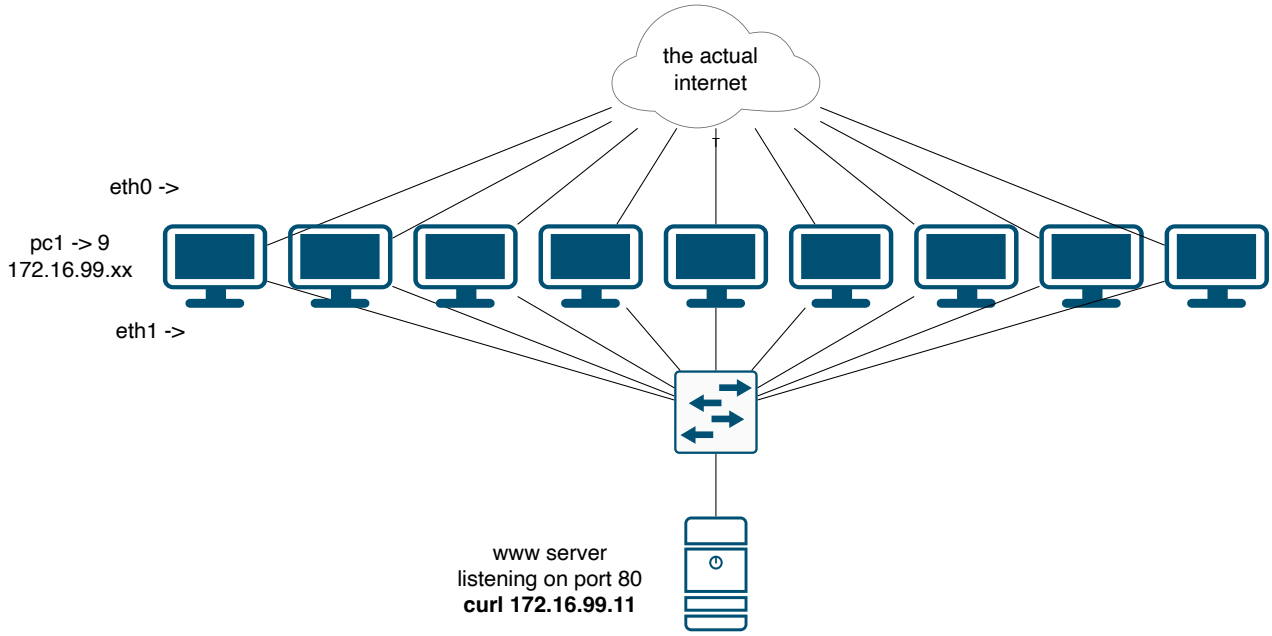
S2E3 - more tcpdump

Nicholas Morrison nick@nanocat.net

Topology



Connecting to the lab server

Connect to the lab server:

```
local$ ssh-keygen -R netlab.nanocat.net
local$ ssh lab@netlab.nanocat.net
Password: (see discord)
```

Connect to your router:

```
lab@netlab$ list-devices
lab@netlab$ connect DEVICE
```

Goal

- ping the lab web server from a lab pc
- fetch a web page using curl from the lab web server
- capture those things and analyse with tcpdump
- capture packets, and open them in wireshark locally

Initial configuration

Everything is already configured with default values!

Ping the web server

Connect to a lab PC:

```
connect clab-www-pcX   <- choose a number
```

Check your lab PC's IP address:

```
ip -c address
```

Start a ping:

```
ping 172.16.99.11
```

Watch your ping

In a different terminal window:

```
ip netns exec clab-www-pcX tcpdump
```

By default, tcpdump uses `eth0` as its interface, and will print output for every packet that it sees.

Stop and start the ping in the other terminal with `ctrl-c` and up-arrow to recall the last command.

Filter with tcpdump

You will probably be seeing lots of traffic aside from your ping. Filter everything else by only showing `icmp` packets (Internet Control Message Protocol)

```
ip netns exec clab-www-pcX tcpdump icmp
```

Try some other filters:

```
# capture only ARP packets
ip netns exec clab-www-pcX tcpdump arp

# capture only LLDP packets (ethertype 0x88cc)
ip netns exec clab-www-pcX tcpdump ether proto 0x88cc

# capture only STP (Spanning Tree Protocol) packets
ip netns exec clab-www-pcX tcpdump stp
```

Capture a whole web page

Use `curl` to fetch a web page from the server.

Start a tcpdump on port 80:

```
ip netns exec clab-www-pcX tcpdump port 80
```

From your lab PC:

```
curl http://172.16.99.11/
```

See the contents of the packets

Start a tcpdump with ASCII interpretation:

```
ip netns exec clab-www-pc2 tcpdump -nn -s0 -A tcp port 80
```

Run a curl from your lab PC:

```
curl http://172.16.99.11/
```

Capture some packets to disk

Capture 50 packets:

```
cd          <- make sure you are in your home directory
ip netns exec clab-www-pcX tcpdump -c 50 -w CLEVER_FILENAME.pcap
```

Generate some pings, or a curl, from your lab PC.

Copy them to your local computer. Locally,

```
scp lab@netlab.nanocat.net:CLEVER_FILENAME.pcap .
```

Open this file locally in Wireshark.