
ARP

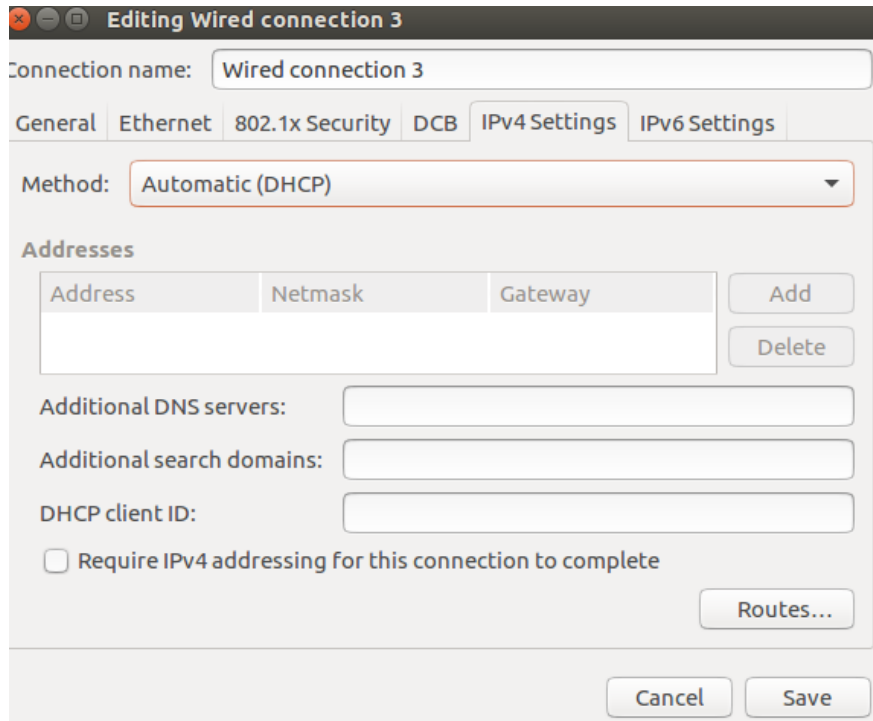
Outline

- **VM Network**
 - Reset from DNS lab
 - Bridged Network
- **Link Layer**
- **MAC Address**
- **ARP and ARP Caching**
- **ARP Cache Poison**
- **ARP Spoofing**
 - Hijacking HTTP using iptables
 - ETTERCAP

VM Network

- **Reset DNS setup**

- Restart the VM and test with *dig*



Editing Wired connection 3

Connection name: Wired connection 3

General Ethernet 802.1x Security DCB IPv4 Settings IPv6 Settings

Method: Automatic (DHCP)

Addresses

Address	Netmask	Gateway

Add Delete

Additional DNS servers:

Additional search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

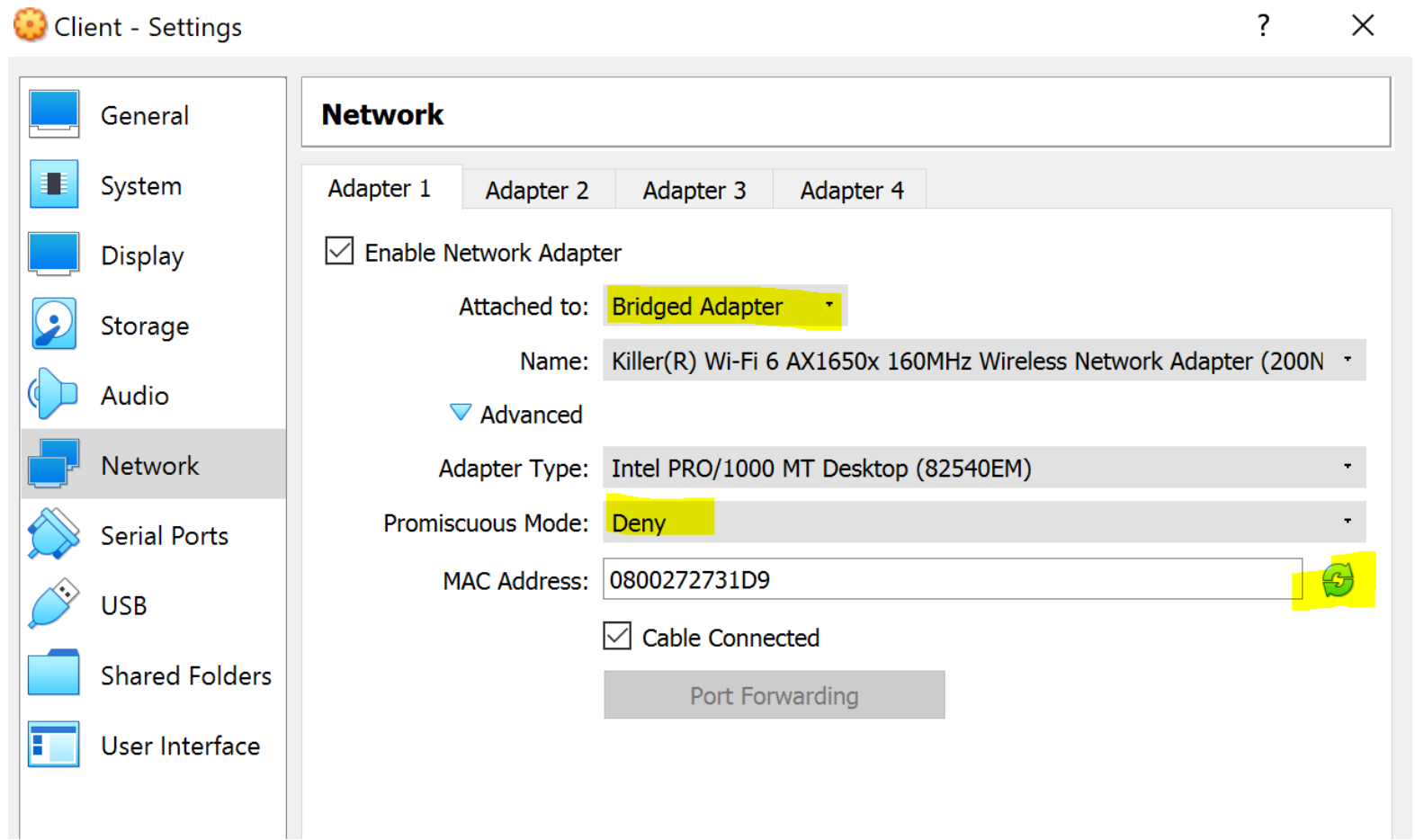
Routes...

Cancel Save

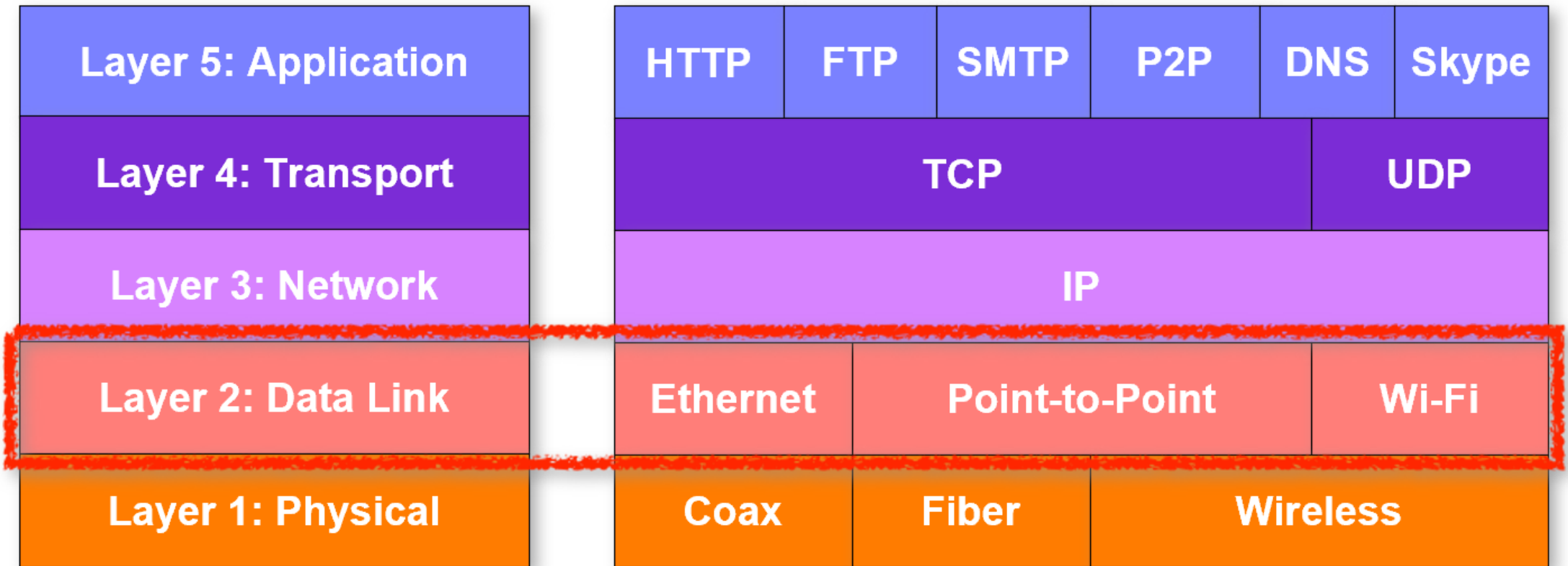
```
/bin/bash
/bin/bash 80x24
[03/19/20]seed@VM:/etc$ cat /etc/resolvconf/resolv.conf.d/head
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
[03/19/20]seed@VM:/etc$
```

```
/bin/bash
/bin/bash 80x24
[03/19/20]seed@VM:/etc$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 127.0.1.1
[03/19/20]seed@VM:/etc$
```

Bridged Network



Link Layer



MAC Addresses

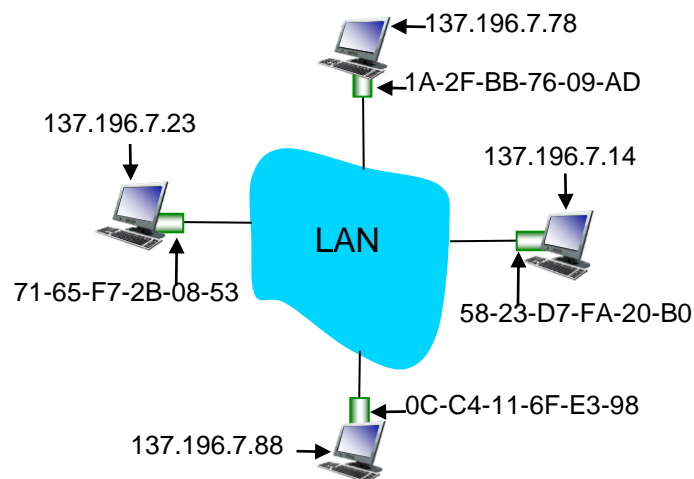
- **Media Access Control** address (also known as link-layer address, Ethernet address, or physical address)
 - Used to address link-layer frames to destination
 - A 48-bit (6-byte) value that is associated with a physical NIC
 - **Example: 1A-2F-BB-76-09-AD**
 - MAC address burned in NIC ROM (sometimes software settable)
 - No two NICs should have the same MAC address
 - **Even though sometimes they do, just make sure they're not on the same network**
 - Unlike an IP address, a MAC address **does NOT change** when a host moves from network to network
 - A host on a network **"listens" to ALL frames** but ignores frames that are not addressed to it
 - Frames that are addressed to a host are passed up to the Network Layer

LAN addresses (more)

- **MAC address allocation administered by IEEE**
- **manufacturer buys portion of MAC address space (to assure uniqueness)**
- **analogy:**
 - MAC address: like Social Security Number
 - IP address: like postal address
- **MAC flat address → portability**
 - can move LAN card from one LAN to another
- **IP hierarchical address *not* portable**
 - address depends on IP subnet to which node is attached

ARP: Address Resolution Protocol

Question: How can a host determine the MAC address of a destination machine knowing only its IP address?



- **ARP table** - every IP node (hosts and routers) on LAN maintains an **ARP table**
 - IP/MAC address mappings for some LAN nodes:
 - **< IP address , MAC address , TTL >**
 - TTL (Time To Live) represents the time after which address mapping will be forgotten (typically 20 minutes)

ARP Cache Poisoning Attack

- **ARP is a communication protocol used for discovering the link layer address**
 - Find me a MAC address, given an IP address.
 - Very simple Protocol
 - Does not implement security measures
- **ARP cache spoofing**
 - Forged IP-to-MAC mappings
 - Man in the middle

Roll up your sleeves – hands on

- **Ip tables**
- **Ettercap**
- **Scapy**
- **Netwox**



Summary

- **Link Layer**
- **MAC Addresses**
- **ARP and ARP Cache**
- **ARP Spoofing and MITM Attacks**
 - Iptables
 - Ettercap
 - Netwox
 - Scapy