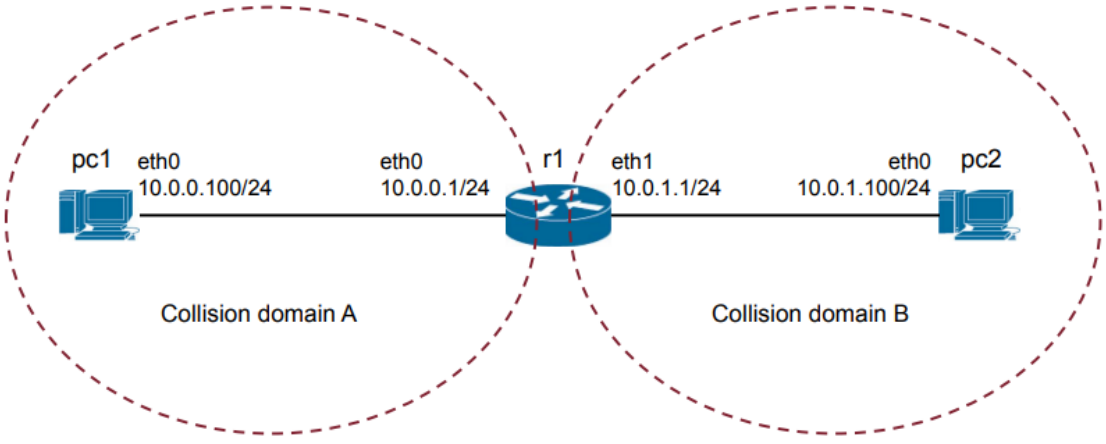
Lab 1 - Basics

Slides - Kathara intro and tools.pdf

Scenario: lab.conf



1. Configure phisycall conection create lab.conf and specify all required things

```
pc1[0]=A #set eth0 of pc1 to collision domain A
r1[0]=A  #set eth0 of r1 to collision domain A

r1[1]=B  #set eth1 of r1 to collision domain B
pc2[0]=B #set eth0 of pc2 to collision domain B
```

2. Assign an ip address to each machine with ip address add a.b.c.d/m dev ethX
    a. ip address add 10.0.0.100/24 dev eth0
3. Configure routing's rule modifying routing table on each terminal machine (pc in our case)
    a. on pc: ip route add 10.0.0.0/24 via 10.0.1.1

- To save progress create and edit <name>.startup
- To reopen a closed terminal kathara connect <name>
- To clear everything run "kathara wipe -f"
- tcpdump listen packets

List of commands

Interface Configuration

- View interfaces: `ip link show`
- Bring up an interface: `ip link set eth0 up`
- Bring down an interface: `ip link set eth0 down`

Assign IPv4 Addresses

- View IP addresses assigned to interfaces: `ip address show`
- Assign an IPv4 address: `ip address add a.b.c.d/m dev ethX`

Manage Routes

- View routes: `ip route show`
- Add a route to a subnet: `ip route add a.b.c.d/m via next_hop_ip`
- Set a default gateway: `ip route add default via next_hop_ip`

Test Connectivity

- Ping a host: `ping a.b.c.d`
- Trace the route to a host: `traceroute a.b.c.d`

Packet Inspection

- Capture packets with tcpdump: `tcpdump -i iface_name -w filename.pcap`

Data Transmission (Netcat)

- Send data over TCP: `nc ip_addr port_num`
- Send data over UDP: `nc -u ip_addr port_num`
- Listen for TCP connections: `nc -l -p port_num`
- Listen for UDP datagrams: `nc -u -l -p port_num`

Analyze Packets

- Open packet capture file in Wireshark: Use Wireshark to load `.pcap` files created by `tcpdump`.

How use kathara

- `kathara lstart`: Start the lab
- `kathara lrestart`: Restart the lab
- `kathara lclean`: Clean the lab (remove containers and networks)

- `kathara lstart --noterminals`: Start the lab without terminals
- `kathara connect <device>`: Connect to a specific device terminal
- `kathara lwip`: Show the IPs assigned to each device in the lab