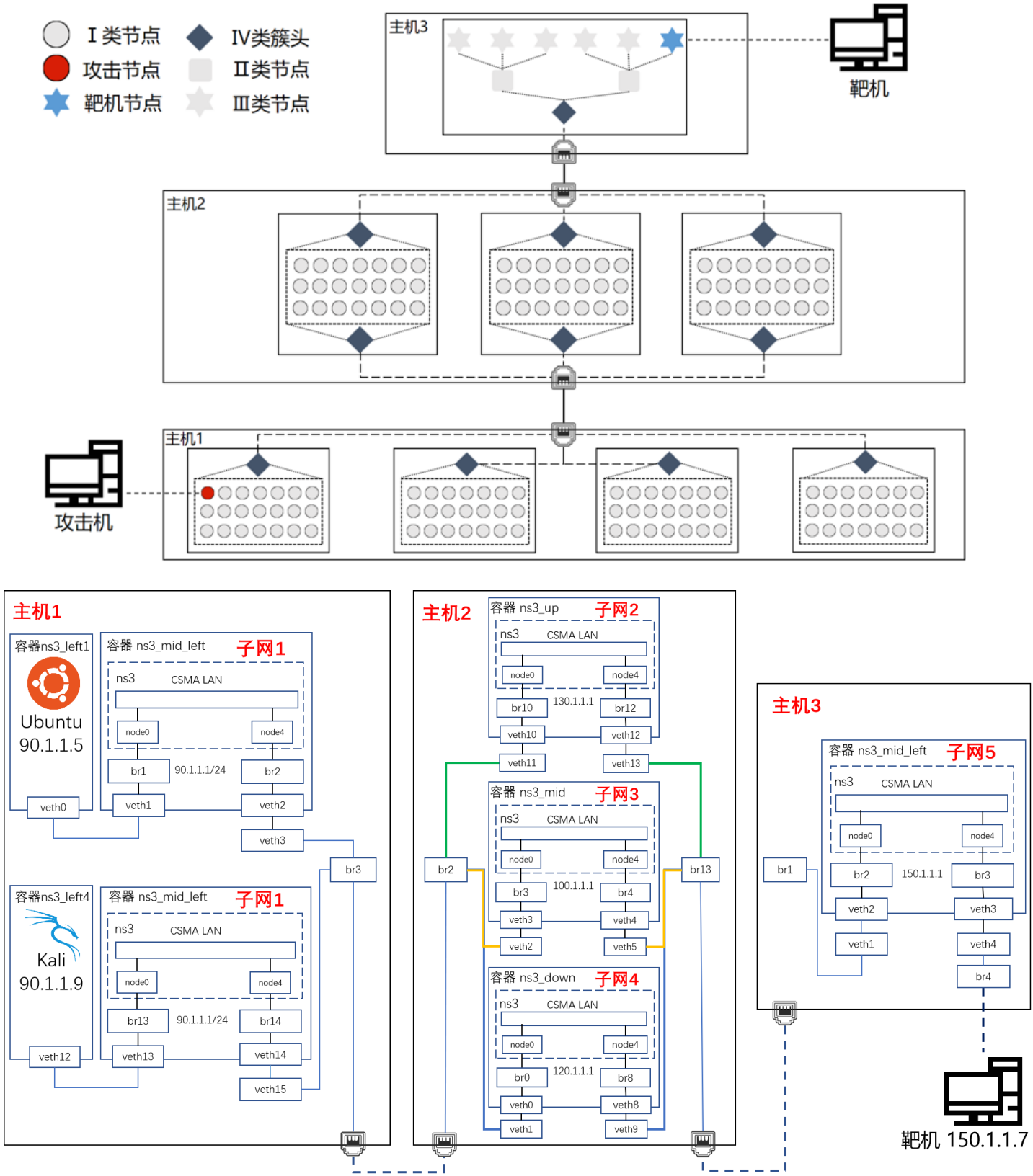
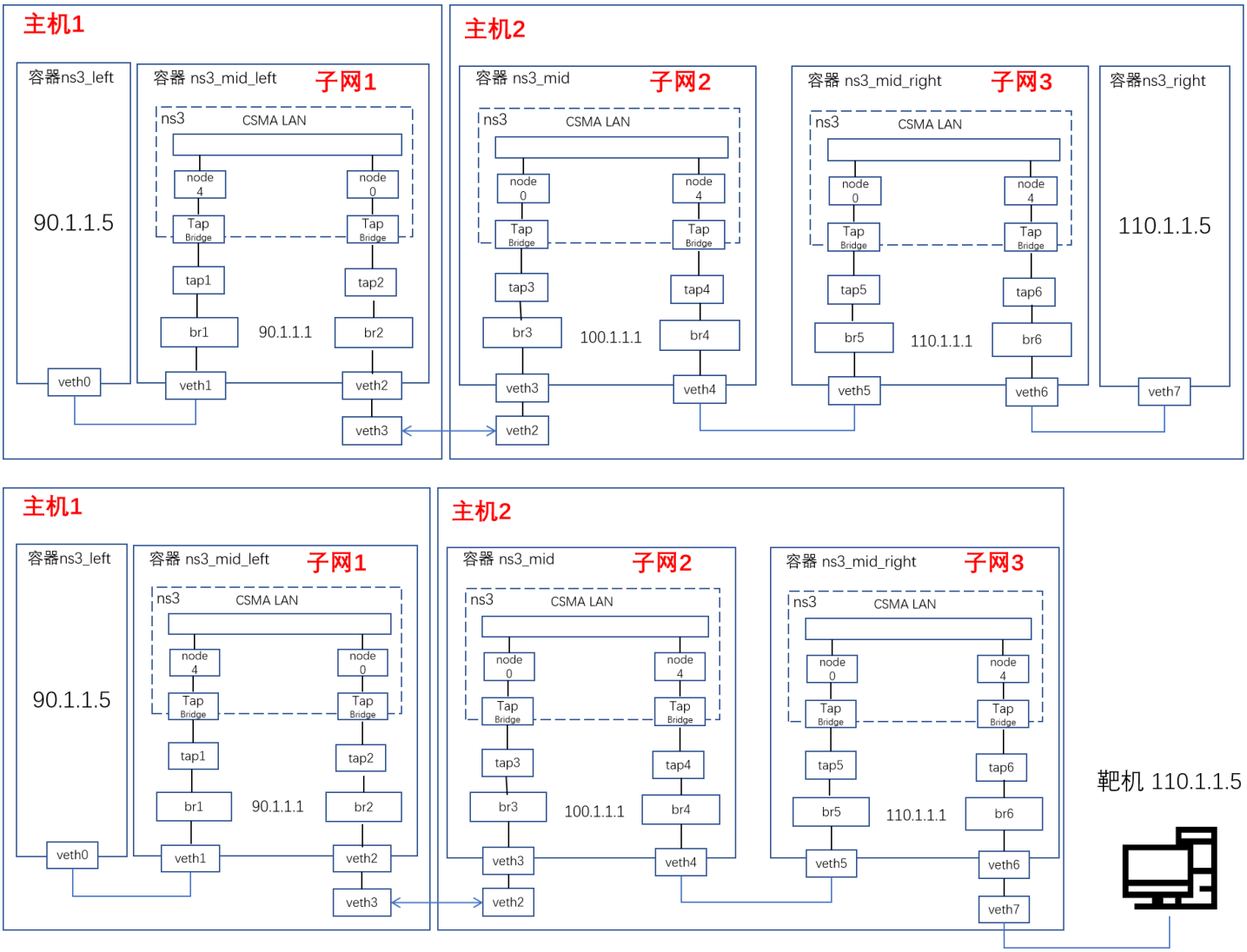
跨主机跨容器通信


Ⅰ类节点
攻击节点
靶机节点
Ⅳ类簇头
Ⅱ类节点
Ⅲ类节点
主机3
靶机
主机2
主机1
攻击机
主机1
容器ns3_left1
Ubuntu
90.1.1.5
veth0
容器 ns3_mid_left
子网1
ns3
CSMA LAN
node0
node4
br1
90.1.1.1/24
br2
veth1
veth2
veth3
br3
容器ns3_left4
Kali
90.1.1.9
veth12
容器 ns3_mid_left
子网1
br13
90.1.1.1/24
br14
veth13
veth14
veth15
主机2
容器 ns3_up
子网2
br10
130.1.1.1
br12
veth10
veth12
veth11
veth13
容器 ns3_mid
子网3
br2
br3
100.1.1.1
br4
br13
veth3
veth4
veth2
veth5
容器 ns3_down
子网4
br0
120.1.1.1
br8
veth0
veth8
veth1
veth9
主机3
容器 ns3_mid_left
子网5
br1
br2
150.1.1.1
br3
veth2
veth3
veth1
veth4
br4
靶机 150.1.1.7



主机1

- 容器创建

代码块

```
1  docker run -tid --name=ns3_mid_left --privileged --network=none --
   entrypoint=/bin/bash ns3-docker
2  docker run -tid --name=ns3_left --privileged --network=none --
   entrypoint=/bin/bash ns3_docker_new
3
4  docker run -tid --name=ns3_left2 --privileged --network=none --
   entrypoint=/bin/bash ns3_docker_new
5  docker run -tid --name=ns3_left3 --privileged --network=none --
   entrypoint=/bin/bash ns3_docker_new
6  docker run -tid --name=ns3_left4 --privileged --network=none --
   entrypoint=/bin/bash kali-docker
7
8  docker run -tid --name=ns3_mid_left2 --privileged --network=none --
   entrypoint=/bin/bash ns3_docker_new
9  docker run -tid --name=ns3_mid_left3 --privileged --network=none --
   entrypoint=/bin/bash ns3_docker_new
```

```
10  docker run -tid --name=ns3_mid_left4 --privileged --network=none --
    entrypoint=/bin/bash ns3_docker_new
```

- 配置接口

代码块

```
1   pid_mid_left=$(docker inspect -f '{{.State.Pid}}' ns3_mid_left)
2   sudo ln -s /proc/$pid_mid_left/ns/net /var/run/netns/$pid_mid_left
3
4   pid_left=$(docker inspect -f '{{.State.Pid}}' ns3_left)
5   sudo ln -s /proc/$pid_left/ns/net /var/run/netns/$pid_left
6
7   sudo ip link add veth0 type veth peer name veth1
8   sudo ip link set dev veth0 netns $pid_left
9   sudo ip netns exec $pid_left ip link set veth0 up
10  sudo ip link set dev veth1 netns $pid_mid_left
11  sudo ip netns exec $pid_mid_left ip link set veth1 up
12
13  sudo ip link add veth2 type veth peer name veth3
14  sudo ip link set dev veth2 netns $pid_mid_left
15  sudo ip netns exec $pid_mid_left ip link set veth2 up
```

- 配置容器ns3_left2

代码块

```
1   pid_mid_left2=$(docker inspect -f '{{.State.Pid}}' ns3_mid_left2)
2   sudo ln -s /proc/$pid_mid_left2/ns/net /var/run/netns/$pid_mid_left2
3
4   pid_left2=$(docker inspect -f '{{.State.Pid}}' ns3_left2)
5   sudo ln -s /proc/$pid_left2/ns/net /var/run/netns/$pid_left2
6
7   sudo ip link add veth4 type veth peer name veth5
8   sudo ip link set dev veth4 netns $pid_left2
9   sudo ip netns exec $pid_left2 ip link set veth4 up
10  sudo ip link set dev veth5 netns $pid_mid_left2
11  sudo ip netns exec $pid_mid_left2 ip link set veth5 up
12
13  sudo ip link add veth6 type veth peer name veth7
14  sudo ip link set dev veth6 netns $pid_mid_left2
15  sudo ip netns exec $pid_mid_left2 ip link set veth6 up
```

- 配置容器ns3_left3

代码块

```
pid_mid_left3=$(docker inspect -f '{{.State.Pid}}' ns3_mid_left3)
sudo ln -s /proc/$pid_mid_left3/ns/net /var/run/netns/$pid_mid_left3

pid_left3=$(docker inspect -f '{{.State.Pid}}' ns3_left3)
sudo ln -s /proc/$pid_left3/ns/net /var/run/netns/$pid_left3

sudo ip link add veth8 type veth peer name veth9
sudo ip link set dev veth8 netns $pid_left3
sudo ip netns exec $pid_left3 ip link set veth8 up
sudo ip link set dev veth9 netns $pid_mid_left3
sudo ip netns exec $pid_mid_left3 ip link set veth9 up

sudo ip link add veth10 type veth peer name veth11
sudo ip link set dev veth10 netns $pid_mid_left3
sudo ip netns exec $pid_mid_left3 ip link set veth10 up
```

- 配置容器ns3_left4

代码块

```
pid_mid_left4=$(docker inspect -f '{{.State.Pid}}' ns3_mid_left4)
sudo ln -s /proc/$pid_mid_left4/ns/net /var/run/netns/$pid_mid_left4

pid_left4=$(docker inspect -f '{{.State.Pid}}' ns3_left4)
sudo ln -s /proc/$pid_left4/ns/net /var/run/netns/$pid_left4

sudo ip link add veth12 type veth peer name veth13
sudo ip link set dev veth12 netns $pid_left4
sudo ip netns exec $pid_left4 ip link set veth12 up
sudo ip link set dev veth13 netns $pid_mid_left4
sudo ip netns exec $pid_mid_left4 ip link set veth13 up

sudo ip link add veth14 type veth peer name veth15
sudo ip link set dev veth14 netns $pid_mid_left4
sudo ip netns exec $pid_mid_left4 ip link set veth14 up
```

- 主机上创建网桥连接接口

代码块

```
sudo brctl addbr br3
sudo brctl addif br3 veth3
sudo brctl addif br3 enx00e04c360073
sudo ip link set veth3 up
sudo ip link set br3 up
sudo brctl addif br3 veth7
```

```
sudo brctl addif br3 veth11
sudo brctl addif br3 veth15
sudo ip link set veth7 up
sudo ip link set veth11 up
sudo ip link set veth15 up
sudo ip addr add 90.1.1.6/24 dev br3
sudo ip route add 100.1.1.0/24 via 90.1.1.6 dev br3
sudo ip route add 110.1.1.0/24 via 90.1.1.6 dev br3
sudo ip route add 120.1.1.0/24 via 90.1.1.6 dev br3
sudo ip route add 130.1.1.0/24 via 90.1.1.6 dev br3
sudo ip route add 150.1.1.0/24 via 90.1.1.6 dev br3
```

- 桥街攻击主机

代码块

```
sudo ip link add veth16 type veth peer name veth17
sudo ip link set dev veth16 netns $pid_mid_left
sudo ip netns exec $pid_mid_left ip link set veth16 up
```

- 容器ns3_mid_left

代码块

```
ip tuntap add dev tap1 mode tap
ip link set tap1 up
ip link set tap1 promisc on
brctl addbr br1
brctl addif br1 veth1
brctl addif br1 tap1
ip link set br1 up

ip tuntap add dev tap2 mode tap
ip link set tap2 up
ip link set tap2 promisc on
brctl addbr br2
brctl addif br2 veth2
brctl addif br2 tap2
ip link set br2 up

ip addr add 90.1.1.1/24 dev br2
ip route add default via 90.1.1.6 dev br2
```

- 容器ns3_mid_left2

代码块

```
ip tuntap add dev tap5 mode tap
ip link set tap5 up
ip link set tap5 promisc on
brctl addbr br5
brctl addif br5 veth5
brctl addif br5 tap5
ip link set br5 up

ip tuntap add dev tap6 mode tap
ip link set tap6 up
ip link set tap6 promisc on
brctl addbr br6
brctl addif br6 veth6
brctl addif br6 tap6
ip link set br6 up

ip addr add 90.1.1.1/24 dev br6
ip route add default via 90.1.1.6 dev br6
```

- 容器ns3_mid_left3

代码块

```
ip tuntap add dev tap9 mode tap
ip link set tap9 up
ip link set tap9 promisc on
brctl addbr br9
brctl addif br9 veth9
brctl addif br9 tap9
ip link set br9 up

ip tuntap add dev tap10 mode tap
ip link set tap10 up
ip link set tap10 promisc on
brctl addbr br10
brctl addif br10 veth10
brctl addif br10 tap10
ip link set br10 up

ip addr add 90.1.1.1/24 dev br10
ip route add default via 90.1.1.6 dev br10
```

- 容器ns3_mid_left4

代码块

```
ip tuntap add dev tap13 mode tap
ip link set tap13 up
ip link set tap13 promisc on
brctl addbr br13
brctl addif br13 veth13
brctl addif br13 tap13
ip link set br13 up

ip tuntap add dev tap14 mode tap
ip link set tap14 up
ip link set tap14 promisc on
brctl addbr br14
brctl addif br14 veth14
brctl addif br14 tap14
ip link set br14 up

ip addr add 90.1.1.1/24 dev br14
ip route add default via 90.1.1.6 dev br14
```

- 容器ns3_left

代码块

```
docker exec -ti ns3_left bin/bash
ip addr add 90.1.1.5/24 dev veth0
ip route add default via 90.1.1.5 dev veth0
```

- 容器ns3_left2

代码块

```
docker exec -ti ns3_left2 bin/bash
ip addr add 90.1.1.7/24 dev veth4
ip route add default via 90.1.1.7 dev veth4
```

- 容器ns3_left3

代码块

```
docker exec -ti ns3_left3 bin/bash
ip addr add 90.1.1.8/24 dev veth8
ip route add default via 90.1.1.8 dev veth8
```

- 容器ns3_left4

代码块

```
docker exec -ti ns3_left4 bin/bash
ip addr add 90.1.1.9/24 dev veth12
ip route add default via 90.1.1.9 dev veth12
```

主机2

- 容器创建

代码块

```
docker run -tid --name=ns3_mid_right --privileged --network=none --
entrypoint=/bin/bash ns3-docker
docker run -tid --name=ns3_mid --privileged --network=none --
entrypoint=/bin/bash ns3-docker
docker run -tid --name=ns3_right --privileged --network=none --
entrypoint=/bin/bash ns3-docker
docker run -tid --name=ns3_down --privileged --network=none --
entrypoint=/bin/bash ns3-docker
docker run -tid --name=ns3_up --privileged --network=none --
entrypoint=/bin/bash ns3-docker
```

- 配置接口

代码块

```
pid_mid_right=$(docker inspect -f '{{.State.Pid}}' ns3_mid_right)
sudo ln -s /proc/$pid_mid_right/ns/net /var/run/netns/$pid_mid_right

pid_mid=$(docker inspect -f '{{.State.Pid}}' ns3_mid)
sudo ln -s /proc/$pid_mid/ns/net /var/run/netns/$pid_mid

pid_down=$(docker inspect -f '{{.State.Pid}}' ns3_down)
sudo ln -s /proc/$pid_down/ns/net /var/run/netns/$pid_down

pid_up=$(docker inspect -f '{{.State.Pid}}' ns3_up)
sudo ln -s /proc/$pid_up/ns/net /var/run/netns/$pid_up

sudo ip link add veth2 type veth peer name veth3
sudo ip link set dev veth3 netns $pid_mid
sudo ip netns exec $pid_mid ip link set veth3 up

sudo ip link add veth4 type veth peer name veth5
sudo ip link set dev veth4 netns $pid_mid
sudo ip netns exec $pid_mid ip link set veth4 up
```

```
sudo ip link set dev veth5 netns $pid_mid_right
sudo ip netns exec $pid_mid_right ip link set veth5 up

sudo ip link add veth6 type veth peer name veth7
sudo ip link set dev veth6 netns $pid_mid_right
sudo ip netns exec $pid_mid_right ip link set veth6 up

sudo ip link add veth0 type veth peer name veth1
sudo ip link set dev veth0 netns $pid_down
sudo ip netns exec $pid_down ip link set veth0 up

sudo ip link add veth8 type veth peer name veth9
sudo ip link set dev veth8 netns $pid_down
sudo ip netns exec $pid_down ip link set veth8 up
sudo ip link set dev veth9 netns $pid_mid_right
sudo ip netns exec $pid_mid_right ip link set veth9 up

sudo ip link add veth10 type veth peer name veth11
sudo ip link set dev veth10 netns $pid_up
sudo ip netns exec $pid_up ip link set veth10 up

sudo ip link add veth12 type veth peer name veth13
sudo ip link set dev veth12 netns $pid_up
sudo ip netns exec $pid_up ip link set veth12 up
sudo ip link set dev veth13 netns $pid_mid_right
sudo ip netns exec $pid_mid_right ip link set veth13 up
```

- 主机上创建网桥连接接口

代码块

```
//br2连接两个端口，两个子网的ip
sudo brctl addbr br2
sudo brctl addif br2 veth2
sudo brctl addif br2 enp3s0
sudo ip link set veth2 up
sudo ip link set br2 up
sudo ip addr add 100.1.1.6/24 dev br2

sudo brctl addif br2 veth1
sudo ip link set veth1 up
sudo ip addr add 120.1.1.6/24 dev br2

sudo brctl addif br2 veth11
sudo ip link set veth11 up
sudo ip addr add 130.1.1.6/24 dev br2
```

```
16
17  //桥接实体
18  sudo brctl addbr br7
19  sudo brctl addif br7 veth7
20  sudo brctl addif br7 enx00e04c36099c
21  sudo ip link set veth7 up
22  sudo ip link set br7 up
23  sudo ip addr add 110.1.1.6/24 dev br7
24  sudo ip route add 90.1.1.0/24 via 110.1.1.6 dev br7
25  sudo ip route add 150.1.1.0/24 via 110.1.1.6 dev br7
26  sudo ip route add 150.1.1.0/24 via 110.1.1.6 dev br7
```

- 容器ns3_up

代码块

```
1   ip tuntap add dev tap10 mode tap
2   ip link set tap10 up
3   ip link set tap10 promisc on
4   brctl addbr br10
5   brctl addif br10 veth10
6   brctl addif br10 tap10
7   ip link set br10 up
8
9   ip tuntap add dev tap12 mode tap
10  ip link set tap12 up
11  ip link set tap12 promisc on
12  brctl addbr br12
13  brctl addif br12 veth12
14  brctl addif br12 tap12
15  ip link set br12 up
16
17  ip addr add 130.1.1.1/24 dev br10
18  ip route add 110.1.1.0/24 via 130.1.1.1 dev br10
19  ip route add 90.1.1.0/24 via 130.1.1.1 dev br10
20  ip route add 150.1.1.0/24 via 130.1.1.1 dev br10
```

- 容器ns3_mid

代码块

```
1   ip tuntap add dev tap3 mode tap
2   ip link set tap3 up
3   ip link set tap3 promisc on
4   brctl addbr br3
5   brctl addif br3 veth3
```

```
brctl addif br3 tap3
ip link set br3 up

ip tuntap add dev tap4 mode tap
ip link set tap4 up
ip link set tap4 promisc on
brctl addbr br4
brctl addif br4 veth4
brctl addif br4 tap4
ip link set br4 up

ip addr add 100.1.1.1/24 dev br3
ip route add 110.1.1.0/24 via 100.1.1.1 dev br3
ip route add 90.1.1.0/24 via 100.1.1.1 dev br3
ip route add 150.1.1.0/24 via 100.1.1.1 dev br3
```

- 容器ns3_down

代码块

```
ip tuntap add dev tap0 mode tap
ip link set tap0 up
ip link set tap0 promisc on
brctl addbr br0
brctl addif br0 veth0
brctl addif br0 tap0
ip link set br0 up

ip tuntap add dev tap8 mode tap
ip link set tap8 up
ip link set tap8 promisc on
brctl addbr br8
brctl addif br8 veth8
brctl addif br8 tap8
ip link set br8 up

ip addr add 120.1.1.1/24 dev br0
ip route add 110.1.1.0/24 via 120.1.1.1 dev br0
ip route add 90.1.1.0/24 via 120.1.1.1 dev br0
ip route add 150.1.1.0/24 via 120.1.1.1 dev br0
```

- 容器ns3_mid_right

代码块

```
ip tuntap add dev tap5 mode tap
```

```
ip link set tap5 up
ip link set tap5 promisc on
brctl addbr br5
brctl addif br5 veth5
brctl addif br5 tap5
brctl addif br5 veth9
brctl addif br5 veth13
ip link set br5 up

ip tuntap add dev tap6 mode tap
ip link set tap6 up
ip link set tap6 promisc on
brctl addbr br6
brctl addif br6 veth6
brctl addif br6 tap6
ip link set br6 up

ip addr add 110.1.1.5/24 dev br6
ip route add default via 110.1.1.6 dev br6
```

主机3

- 主机上创建网桥连接接口

代码块

```

pid_right=$(docker inspect -f '{{.State.Pid}}' ns3_right)
sudo ln -s /proc/$pid_right/ns/net /var/run/netns/$pid_right

sudo ip link add veth1 type veth peer name veth2
sudo ip link set dev veth2 netns $pid_right
sudo ip netns exec $pid_right ip link set veth2 up

sudo ip link add veth3 type veth peer name veth4
sudo ip link set dev veth3 netns $pid_right
sudo ip netns exec $pid_right ip link set veth3 up

sudo ip link add veth5 type veth peer name veth6
sudo ip link set dev veth5 netns $pid_right
sudo ip netns exec $pid_right ip link set veth5 up

sudo brctl addbr br1
sudo brctl addif br1 veth1
sudo brctl addif br1 enx00e04c320c04
sudo ip link set veth1 up
sudo ip link set br1 up
```

```
sudo ip addr add 150.1.1.1/24 dev br1

sudo brctl addbr br6
sudo brctl addif br6 veth6
sudo brctl addif br6 enx
sudo ip link set veth6 up
sudo ip link set br6 up
sudo ip addr add 150.1.1.7/24 dev br6

sudo brctl addbr br4
sudo brctl addif br4 veth4
sudo brctl addif br4 enx00e02a790731
sudo ip link set veth4 up
sudo ip link set br4 up
sudo ip addr add 150.1.1.6/24 dev br4
sudo ip route add 90.1.1.0/24 via 150.1.1.1 dev br1
sudo ip route add 100.1.1.0/24 via 150.1.1.1 dev br1
sudo ip route add 110.1.1.0/24 via 150.1.1.1 dev br1
sudo ip route add 120.1.1.0/24 via 150.1.1.1 dev br1
sudo ip route add 130.1.1.0/24 via 150.1.1.1 dev br1
```

- 容器ns3_right

代码块

```
ip tuntap add dev tap2 mode tap
ip link set tap2 up
ip link set tap2 promisc on
brctl addbr br2
brctl addif br2 veth2
brctl addif br2 tap2
ip link set br2 up

ip tuntap add dev tap3 mode tap
ip link set tap3 up
ip link set tap3 promisc on
brctl addbr br3
brctl addif br3 veth3
brctl addif br3 tap3
ip link set br3 up

ip addr add 150.1.1.5/24 dev br2
ip route add default via 150.1.1.1 dev br2

```

- 靶机

代码块

```
ip addr add 150.1.1.7/24 dev enX
ip route add default via 150.1.1.7 dev enX
```