How to build an Access Control List (ACL) with a Layer 2 Packet Filter

The Embedded Gateway Linux of your DIL/NetPC ADNP/1520 Embedded Gateway Linux supports *ebtables*-based packet filtering within ISO/OSI Layer 2 (Data Link Layer). This allows you to setup a Firewall with MAC addresses.

- **1. Step**: Setup a RS232 serial link between the Application Board MB/1520-100 and a PC. Then enter the following command sequence within an RS232-based serial console session:

```
cd /flash
cat > autostart.sh
#!/bin/sh
ifconfig eth0 0.0.0.0
ifconfig eth1 0.0.0.0
ifconfig eth2 0.0.0.0
ebtables -F FORWARD
ebtables -P FORWARD DROP
ebtables -A FORWARD -p ARP -j ACCEPT
ebtables -A FORWARD -p Ipv4 -s 00:0a:e4:49:2e:40 -j ACCEPT
ebtables -A FORWARD -p Ipv4 -s 02:80:ad:20:63:cc -j ACCEPT
brctl addbr br0
brctl addif br0 eth0
brctl addif br0 eth1
brctl addif br0 eth2
ifconfig br0 up
```

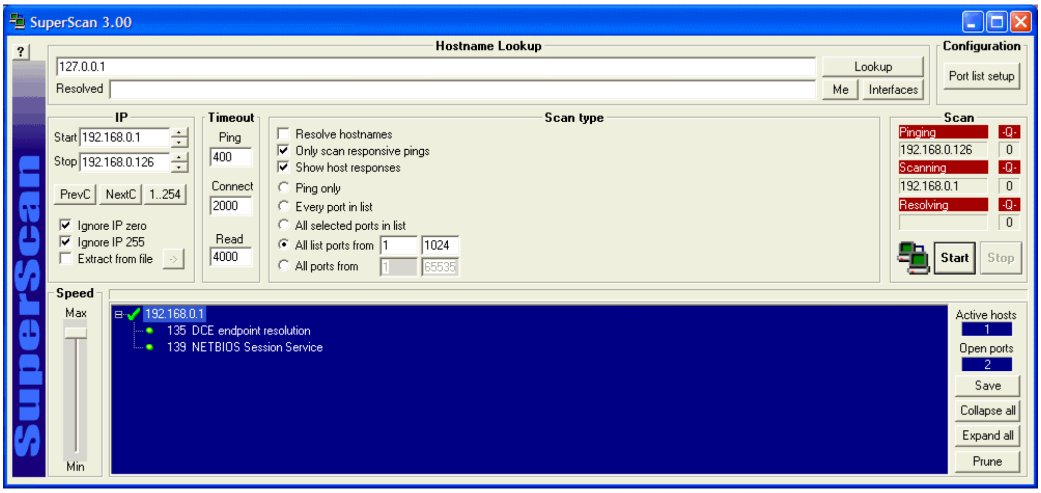
  CTRL-D (*CTRL-D stops the Linux cat command*)

```
chmod +x autostart.sh
```

  The first three *ifconfig* commands of this sample removes the default IP addresses from eth0 (MB/1520-100 LAN1 interface), eth1 (MB/1520-100 LAN2 interface) and eth2 (MB/1520-100 LAN3 interface).

  The following *ebtables* commands builds an ACL (Access Control List) for two MAC addresses. Only Ethernet packets to and from the stations with the MAC addresses *00:0a:e4:49:2e:40* (PC system connected to LAN1/eth0 of the MB/1520-100) and *02:80:ad:20:63:cc* (the embedded device connected to LAN3/eth2 of the MB/1520-100) can pass the Ethernet Bridge. ARP-based Ethernet packets from all systems can also pass through the bridge. The four *brctl* commands direct after the *ebtables* commands define a bridge with the name *br0* and add the three MB/1520-100 Ethernet LAN interfaces eth0, eth1 and eth2 to this bridge. The final *ifconfig* command brings the Ethernet bridge up to work.

- **2. Step**: After the next reboot the Application Board MB/1520-100 works as 3-Port Switch and Layer 2 Firewall with a MAC address ACL (Access Control List). Run a port scanner program and check the result.



SuperScan 3.00

Hostname Lookup: 127.0.0.1
Resolved:

IP
Start 192.168.0.1
Stop 192.168.0.126
☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Timeout
Ping 400
Connect 2000
Read 4000

Scan type
☐ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
○ All selected ports in list
● All list ports from 1 1024
○ All ports from 1 65535

Scan
Pinging 192.168.0.126 0
Scanning 192.168.0.1 0
Resolving 0

192.168.0.1
135 DCE endpoint resolution
139 NETBIOS Session Service

Active hosts 1
Open ports 2

Please note: All Application Board MB/1520-100 Ethernet LAN interfaces are transparent in this operation mode. There is no way to access the MB/1520-100 internal Telnet server or other TCP- or UDP-based server programs. The MB/1520-100 LAN interfaces don't offer an IP address with the configuration from the second step.

That's all.