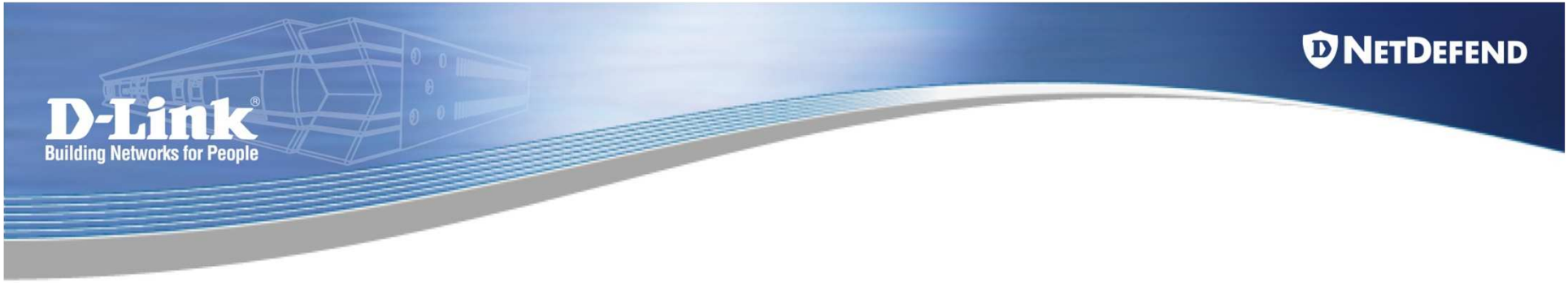
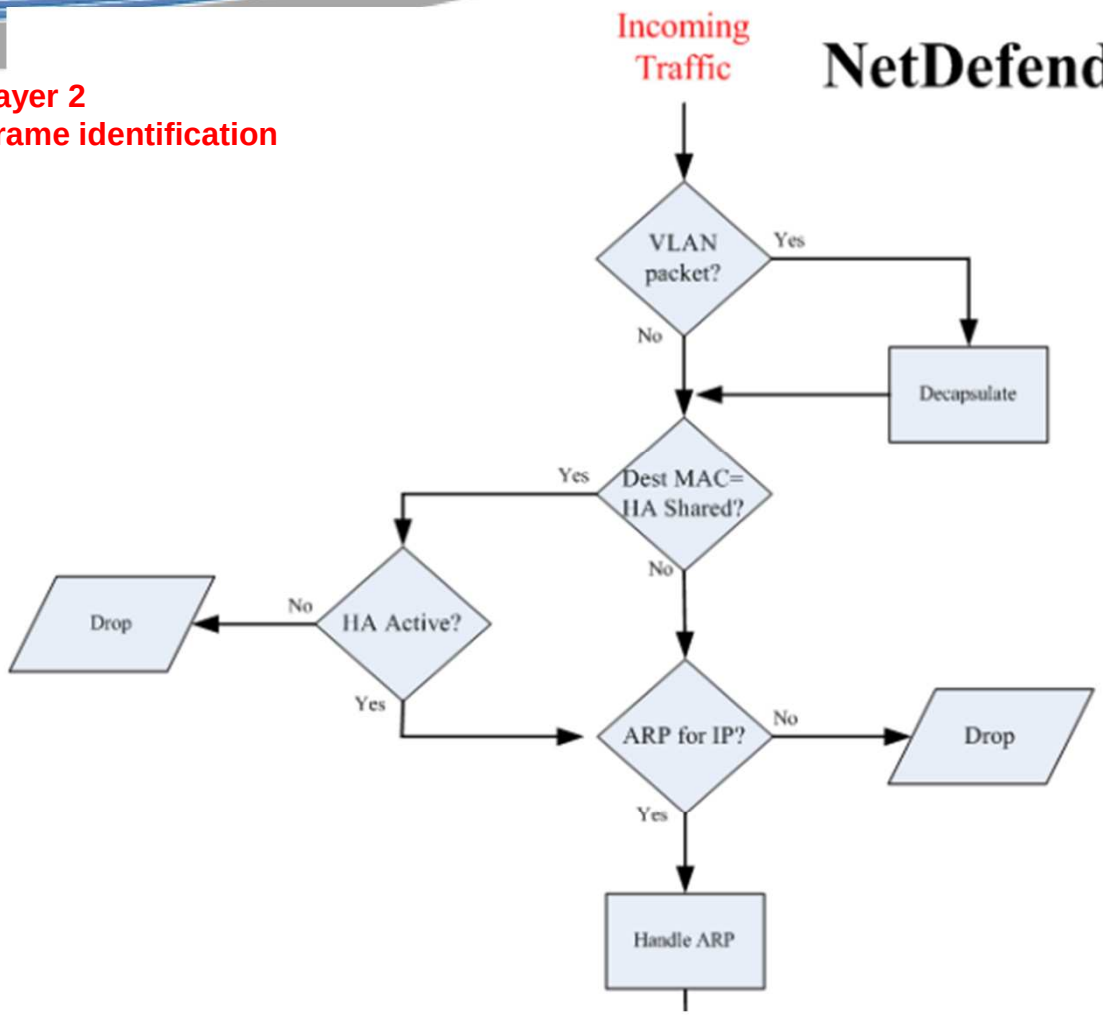


Introduction to High Availability

Layer 2
Frame identification

NetDefend Firewall Packet Flow



RT = Routing Table
IF = Interface

Some explanations:

"Lookup destination interface in main Routing Table": here we try to find out the destination interface by looking in the main routing table. This is needed to be able to look up PBR rules in the next step of the flow.

"Reverse Route Lookup": This is used to automatically verify sender IP based on routing if there is no maching access rule. The lookup will be done in the selected routing table (*main* or *PBR routing table*). The source IP is used as input for the lookup. An interface is given back as result. The traffic is only allowed if this interface matches the interface we received the packet on. (*Advanced, may be too detailed for this course*: there is one exception from this statement. If interface groups are used and members are marks as **"Security/Transport Equivalent"**, traffic received from another member in the same interface group is also allowed).

Security/Transport Equivalent: If enabled, the interface group can be used as a destination interface in rules where

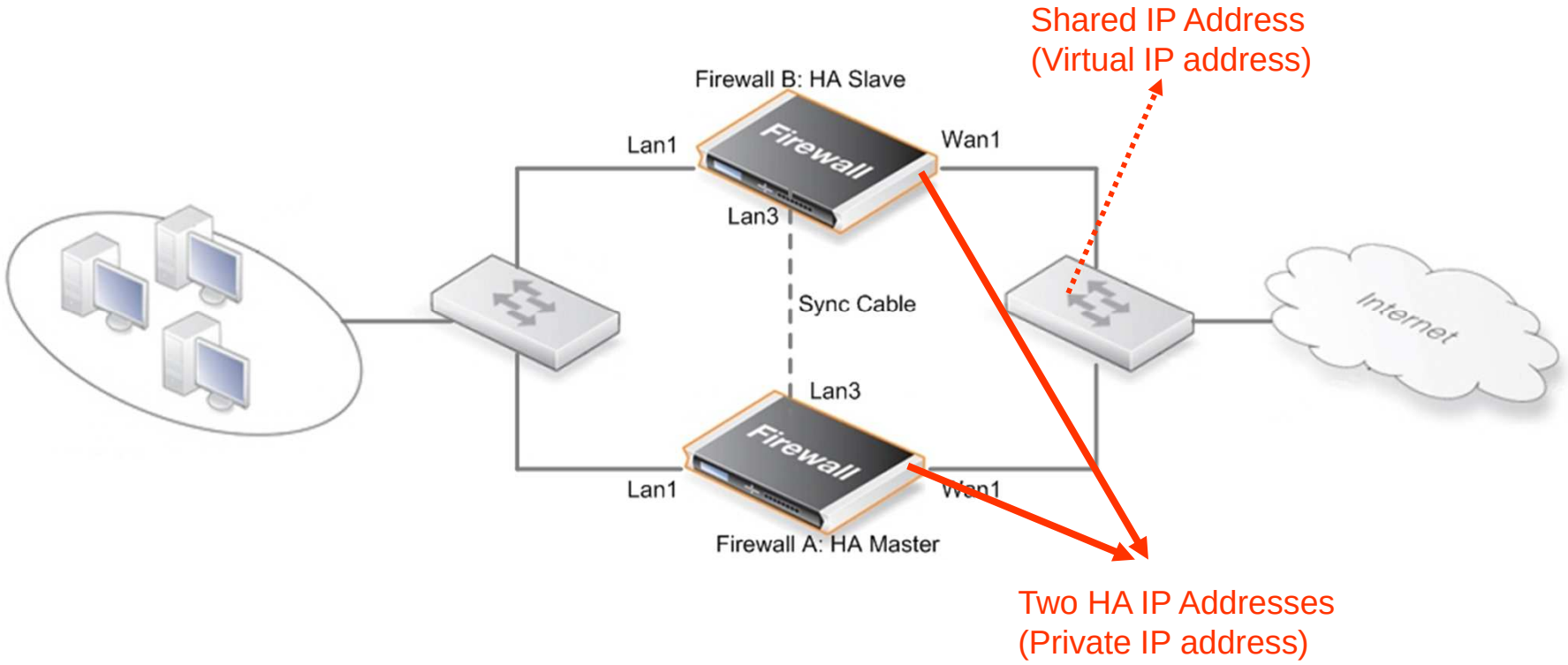
802.1p.cap

hearbeat.pcap

HA_Configuration_Sys.pcap

different_interface.pcap

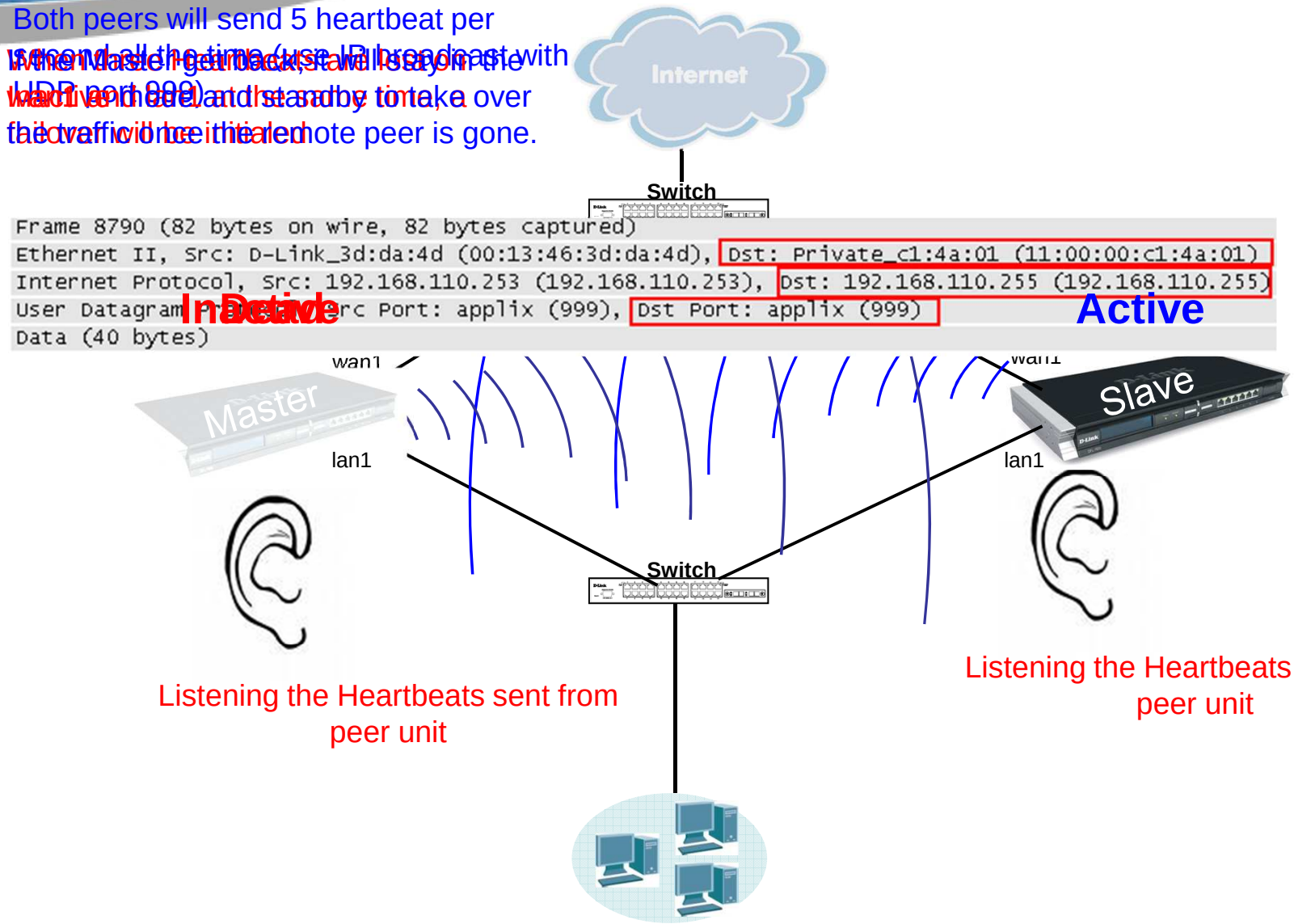
HA and Shared IP Address for Hardware Failover



High Availability

How does the failover work?

Both peers will send 5 heartbeat per second all the time (use IP broadcast with UDP port 999) and standby to take over the traffic once the remote peer is gone.



HA Cluster Heartbeats

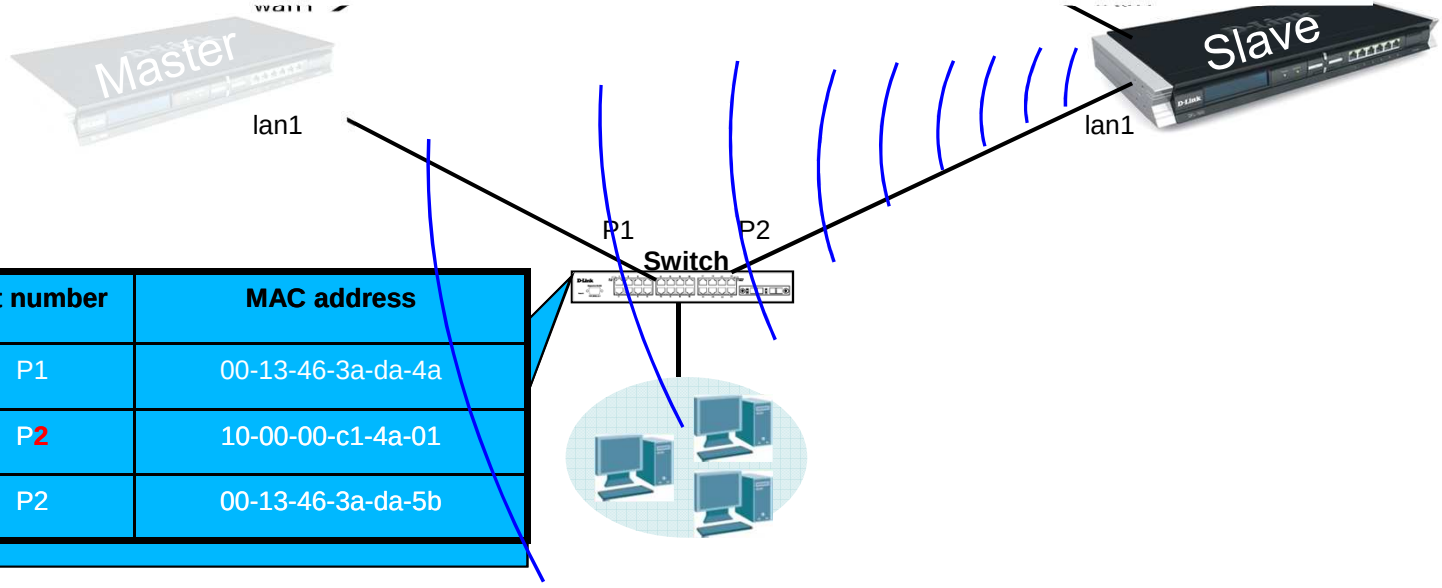
- A firewall detects its peer equipment no longer operational when it can not hear devices “Cluster Heartbeats” from its peer.
- Both peers sends 5 heartbeats per second.
- when 3 heartbeats are missed a failover will be initiated, the standby one will become active.
- Under normal operation of a High Availability cluster, all interfaces send Cluster HeartBeat messages on a regular basis.
  (To avoid heartbeat traffic overheating the network, the administrator can disable heartbeat sending on any of the interfaces.)

High Availability

ARP table insight

No.	Time	Source	Destination	Protocol	Info
575	20.124812	Private_c1:4a:01	Broadcast	ARP	Gratuitous ARP for 192.168.2.254 (Request)
584	20.548246	Private_c1:4a:01	Broadcast	ARP	Gratuitous ARP for 192.168.2.254 (Request)

```
⊞ Frame 575 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Private_c1:4a:01 (10:00:00:c1:4a:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊟ Address Resolution Protocol (request/gratuitous ARP)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: Private_c1:4a:01 (10:00:00:c1:4a:01)
    Sender IP address: 192.168.2.254 (192.168.2.254)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.2.254 (192.168.2.254)
```

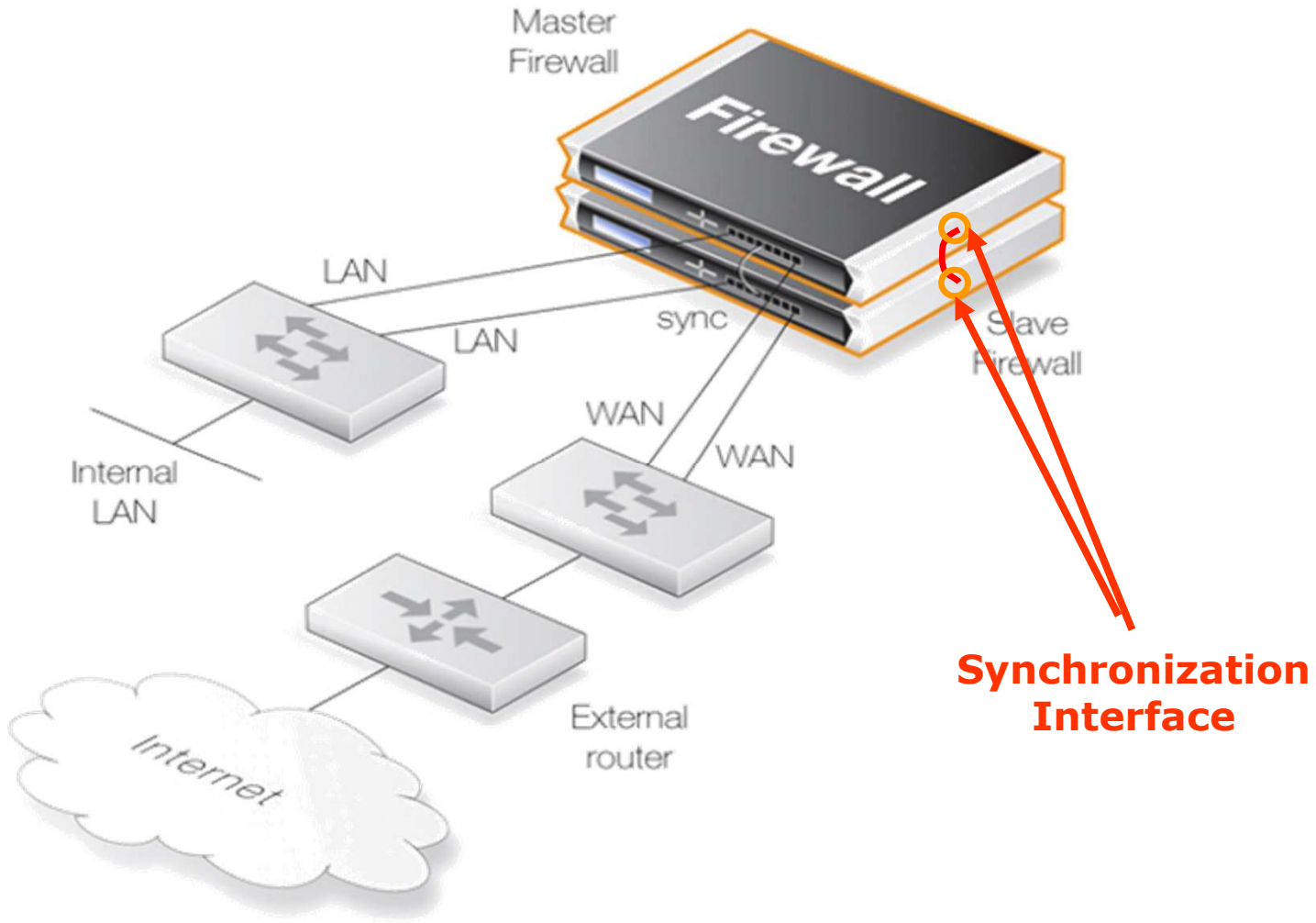


Port number	MAC address
P1	00-13-46-3a-da-4a
P2	10-00-00-c1-4a-01
P2	00-13-46-3a-da-5b

Hardware Failover Mechanism

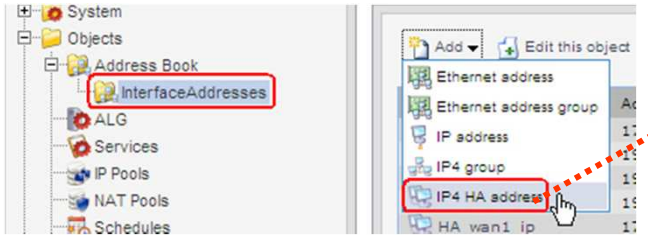
- All ARP queries and response for the shared IP address that will be answered by the active firewall.
- The hardware address of the shared IP address is not using real physical hardware address for each interface. It is constructed from the Cluster ID on the following form: 10-00-00-C1-4A-*nn* for example. The *nn* is the Cluster ID configured in the Settings section.
- Since the shared IP address is used, there will be no latency time to update ARP caches of units when failover occurs.
- HA provides a redundant, state-synchronized hardware configuration.

The Synchronization Interface

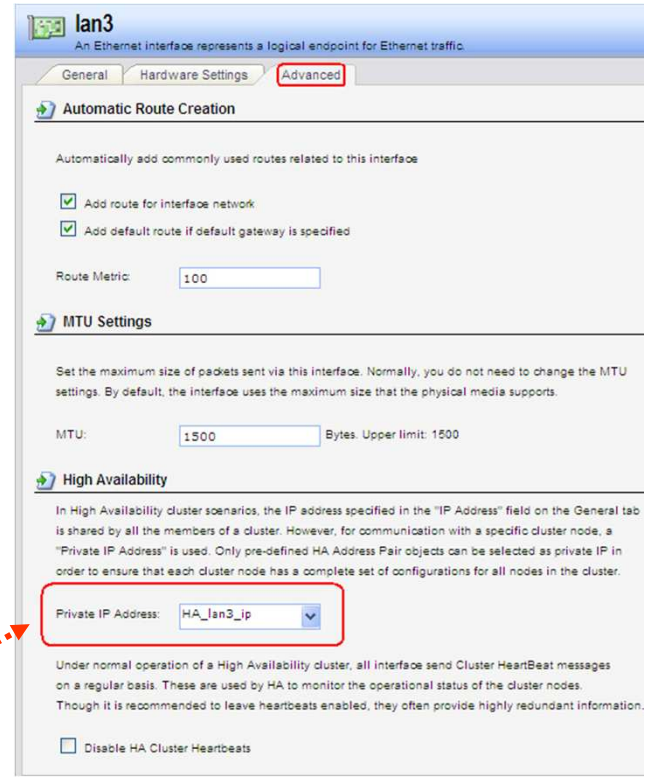


HA Address Setting Contrasts with WebUI

Physical Interface address will be “Shared IP Address”



HA Address Object includes Master IP and Slave IP address



HA Address Object has to be selected on Advanced tab within Ethernet Interface setting page

How to check the HA status

- Type the **ha** command in the CLI

```
MASTER:/> ha
This device is a HA MASTER
This device is currently ACTIVE (will forward traffic)
This device has been active: 33 sec
HA cluster peer is ALIVE
MASTER:/>

SLAVE:/> ha
This device is a HA SLAVE
This device is currently INACTIVE (won't forward traffic)
This device has been inactive: 44 sec
HA cluster peer is ALIVE
SLAVE:/>
```

How to deactivate the HA master

- Type the **ha –deactivate** .

```
MASTER:/> ha
This device is a HA MASTER
This device is currently ACTIVE (will forward traffic)
This device has been active: 280 sec
HA cluster peer is ALIVE
MASTER:/> ha -deactivate
HA was: ACTIVE
HA going INACTIVE...
MASTER:/> ha
This device is a HA MASTER
This device is currently INACTIVE (won't forward traffic)
This device has been inactive: 3 sec
HA cluster peer is ALIVE
MASTER:/>
SLAVE:/>
SLAVE:/> ha
This device is a HA SLAVE
This device is currently ACTIVE (will forward traffic)
This device has been active: 11 sec
HA cluster peer is ALIVE
SLAVE:/>
```

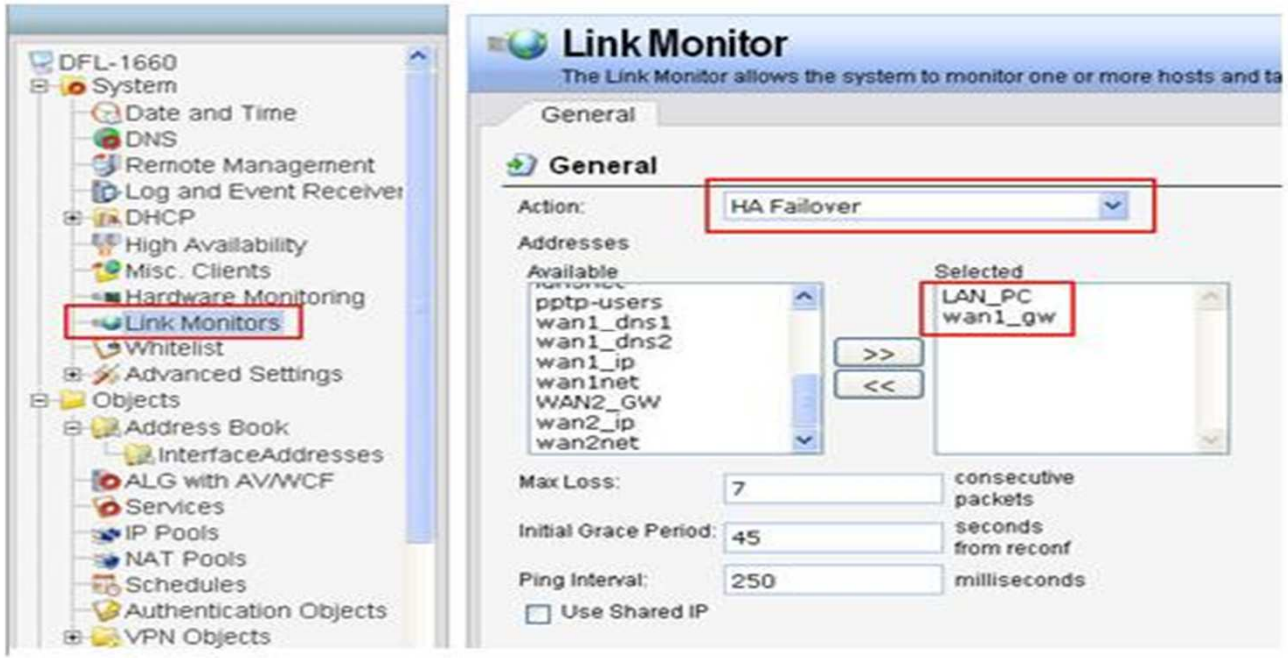
teraterm.log

Link Monitor Feature in the HA

- HA mechanism monitors heartbeat packet to check the status of HA peer device, the firewall thinks that the peer is dead and takes the HA Active ownership if no heartbeat packet received. There might be a problem if only specific interface connection is failed.

Continue

- We can use Link Monitor feature to avoid this limitation. With Link Monitor feature, DFL monitors link status per interface, and triggers HA failover if monitored interface is down.



Common debug procedure

- Can check HA state via CLI

```
Check Master HA state via CLI:

DFL-2560:/> ha
This device is a HA MASTER
This device is currently ACTIVE (will forward traffic)
This device has been active: 191 sec
HA cluster peer is DEAD

Check Slave HA state via CLI:

DFL-2560G:/> ha
This device is a HA SLAVE
This device is currently ACTIVE (will forward traffic)
This device has been active: 246 sec
HA cluster peer is DEAD
```

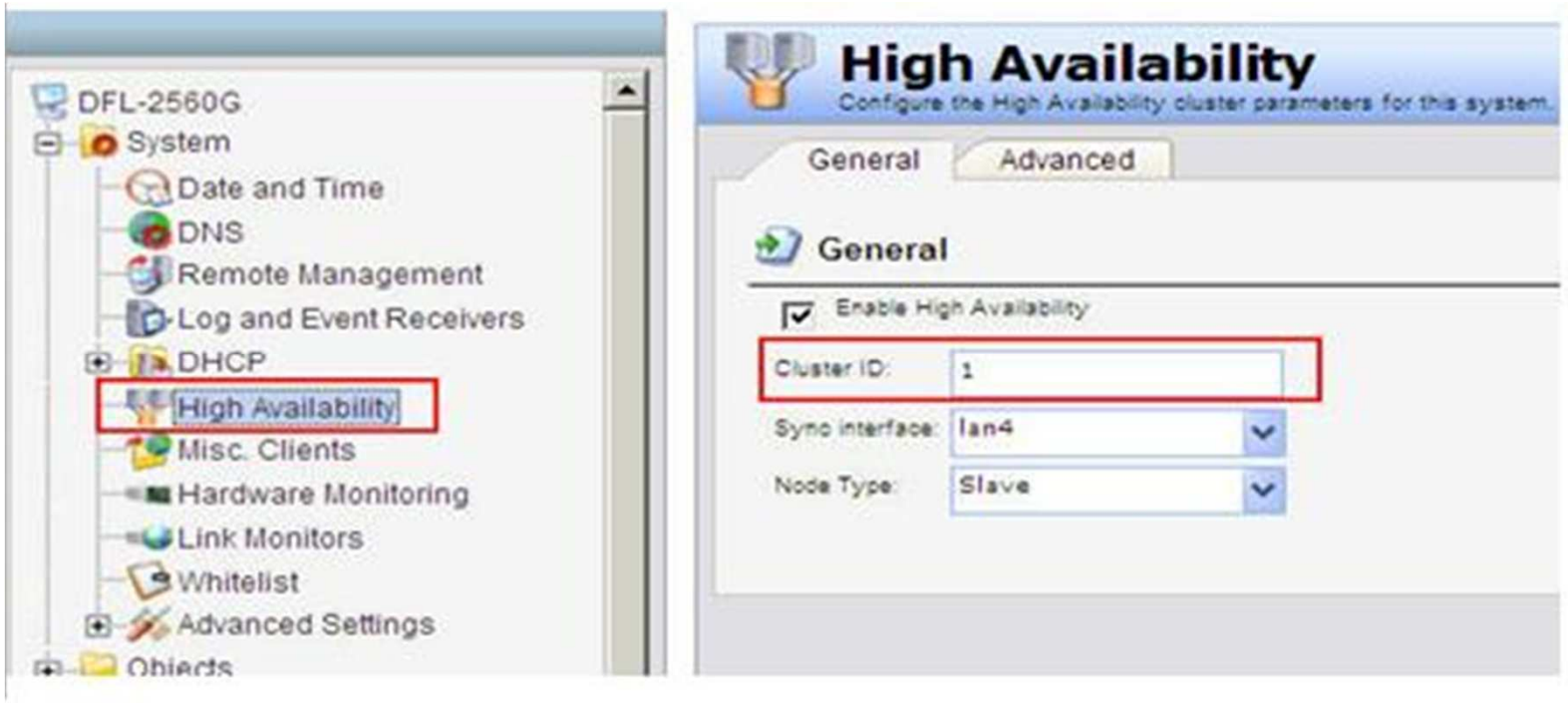
- We can see that both Master and Slave are in the "ACTIVE" state and think peer is dead. In such situation, the user network is being very instability and suffering

Continue

- Make sure Sync interfaces are connected between each other or corresponding activate interfaces are connected in the same broadcast domain. We need make sure the heartbeat packets can communicated between each others.

Continue

- Check HA cluster number, both firewalls should have the same Cluster ID.



Continue

- Make sure Master and Slave roles.
- Make sure both firewalls have the same HA advanced parameters.

- All shared IP addresses must be the same between each other.

Things to keep in mind

Firewall Statistics are not shared

1.The Real-time Monitor of Slave Firewall will not automatically track the active firewall. When you login in Slave Firewall GUI, you're looking at a Real-time Monitor graph where nothing but the connection count is moving.

2.SNMP statistics are not shared as well. SNMP managers have no failover capabilities. Therefore, you will need to poll both firewalls in the cluster.

Logs comes from two firewalls

1.Log data will be coming from two firewalls.

2.The external log server has to be configured to receive logs from both firewalls. All log query will include both firewalls as sources and it will give you all the log data in one result view.

Configuring High Availability - Summary

- Both firewalls in High Availability scenario will use shared IP address.
- The hardware address of the shared IP address is based on Cluster ID information to change last two numbers of the physical hardware address.
- Both firewalls rely “Cluster Heartbeat” packets to detect its peer equipment is working or no longer operational.

High Availability-Firmware Upgrade
Get rid of the risk

- 1. Take the inactive node completely off-line (disconnect all cables)

- 2. Upgrade the inactive node.

Now you have two options:

- 3a. Upgrade the active node (allow it to reboot) and when it is up, re-install the inactive node.
  Downtime = **reboot** time + time for ARP etc to settle and Conns to re-transmit.

- 3b. Re-install the inactive mode, do a failover to it, upgrade the remaining node.
  Downtime = **failover** time + time for ARP etsc to settle and Conns to re-transmit.

High Availability
Known issue: (version 2.20.02)

- 1. HA: Transparent Mode won't work in HA mode
- 2. HA: No state synchronization for ALGs
- 3. HA: Tunnels unreachable from inactive node

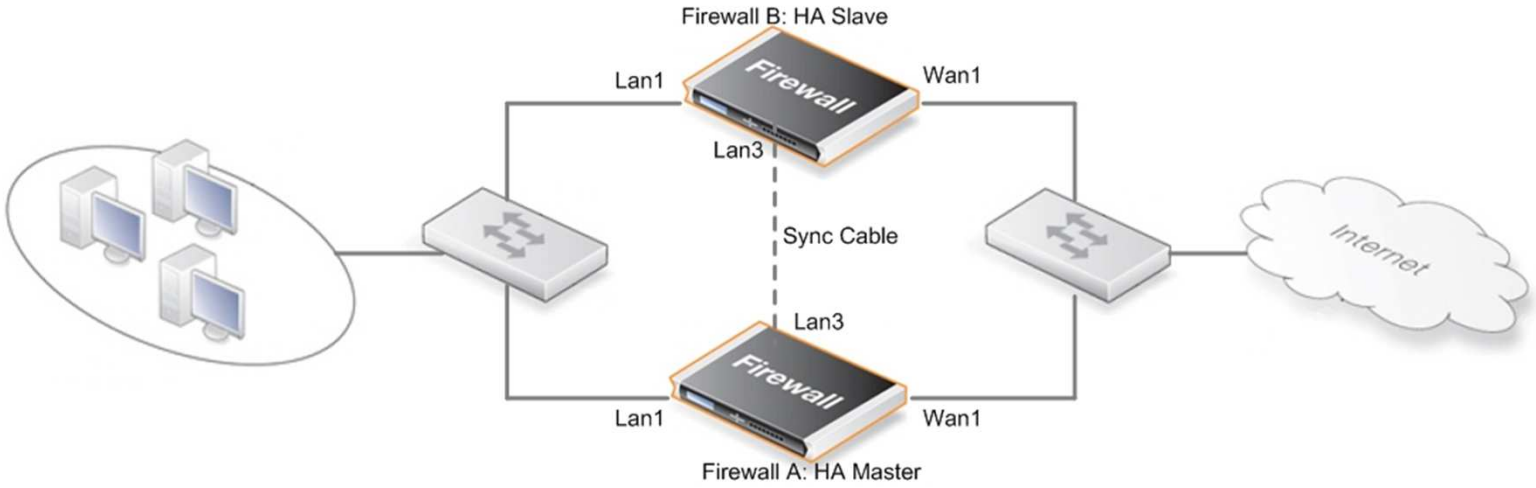
  (The inactive node in an HA cluster cannot communicate over IPSec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.)
- 4. HA: No state synchronization for L2TP, PPTP and IPSec tunnels

  (On failover, incoming clients will re-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range.)
- 5. HA: No state synchronization for IDP signature scan states.

  (No aspects of the IDP signature states are synchronized. This means that there is a small chance that the IDP engine causes false negatives during an HA failover.)

High Availability Scenario Hands-on

Planning to Create High Availability Cluster



Interface	Shared IP Address	HA Master IP Address	HA Slave IP Address
Wan1	**192.168.110.254**	**192.168.110.253**	**192.168.110.252**
Wan2	192.168.120.254	192.168.120.253	192.168.120.252
DMZ	172.17.100.254	172.17.100.253	172.17.100.252
Lan1	**192.168.1.254**	**192.168.1.253**	**192.168.1.252**
Lan2	192.168.2.254	192.168.2.253	192.168.2.252
Lan3	192.168.3.254	192.168.3.253	192.168.3.252

High Availability
Firewall A-setup procedure--(CLI)

1 Config the Shared IP address for all of interfaces

Assign the **Shared IP address** to each physical interface respectively.

```
set Interface Ethernet wan1 DHCPEnabled=No
set Address IP4Address InterfaceAddresses/wan1_ip Address=192.168.110.254
set Address IP4Address InterfaceAddresses/wan1net Address=192.168.110.0/24
set Address IP4Address interfaceAddresses/dmz_ip Address=172.17.100.254
set Address IP4Address InterfaceAddresses/dmznet Address=172.17.100.0/24
set Address IP4Address InterfaceAddresses/lan1_ip Address=192.168.1.254
set Address IP4Address InterfaceAddresses/lan1net Address=192.168.1.0/24
set Address IP4Address InterfaceAddresses/lan2_ip Address=192.168.2.254
set Address IP4Address InterfaceAddresses/lan2net Address=192.168.2.0/24
set Address IP4Address InterfaceAddresses/lan3_ip Address=192.168.3.254
set Address IP4Address InterfaceAddresses/lan3net Address=192.168.3.0/24
```

High Availability
Firewall A-setup procedure--(CLI)

2 Assigning the IP address to each interface for Master and Slave respectively.

Add the HA objects for every interfaces, please noting that, no matter about the amount of physical interfaces are involved, we still need to create every HA objects for each physical interface respectively, it's the design by nature. "Address:**0**"→ It's the IP address for **Master**, and "Address:**1**"→ is the address for **Slave**

```
→add Address AddressFolder Ha-object
→set HighAvailability Enabled=Yes SyncIface=dmz ClusterID=1 NodeID=0
→cc Address AddressFolder Ha-object
  add IP4HAAddress wan1-ha Address:0=192.168.110.253 Address:1=192.168.110.252
  add IP4HAAddress wan2-ha Address:0=192.168.120.253 Address:1=192.168.120.252
  add IP4HAAddress dmz-ha Address:0=172.17.100.253 Address:1=172.17.100.252
  add IP4HAAddress lan1-ha Address:0=192.168.1.253 Address:1=192.168.1.252
  add IP4HAAddress lan2-ha Address:0=192.168.2.253 Address:1=192.168.2.252
  add IP4HAAddress lan3-ha Address:0=192.168.3.253 Address:1=192.168.3.252
  cc
```

High Availability
Firewall A-setup procedure--(CLI)

3 On each physical interface, we need to apply something which we created in previous steps

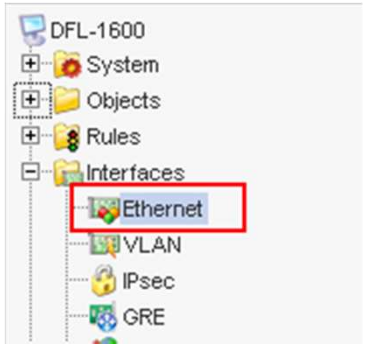
After we done all the settings, we need to input the command of “Save” to store the configuration file into Flash Card, and please don’t forget to input the “Activate” after “Save” to confirm the settings again within 30 seconds (default value). If DFL doesn’t receive the “Activate”, the settings will be restored to the previous version.

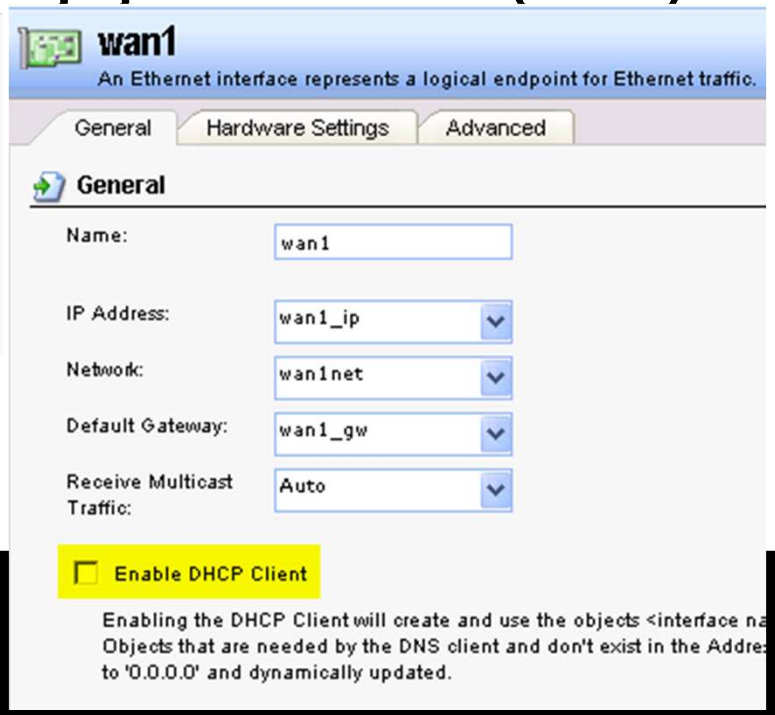
set Interface Ethernet wan1 PrivateIP=Ha-object/wan1-ha
set Interface Ethernet wan2 PrivateIP=Ha-object/wan2-ha NOCHB=Yes
set interface Ethernet dmz PrivateIP=Ha-object/dmz-ha
set Interface Ethernet lan1 PrivateIP=Ha-object/lan1-ha
set Interface Ethernet lan2 PrivateIP=Ha-object/lan2-ha NOCHB=Yes
set Interface Ethernet lan3 PrivateIP=Ha-object/lan3-ha NOCHB=Yes
→ Save
//reconnect to DFL
→ Activate

High Availability
Firewall A-setup procedure--(GUI)

1

If the default firmware is **v2.12** or later, the **WAN1** interface will be the DHCP client by default. As we said before, HA doesn't support the type is DHCP client in any physical interfaces.

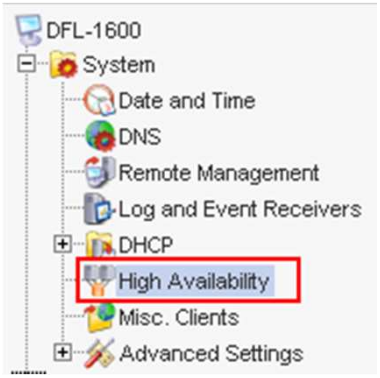


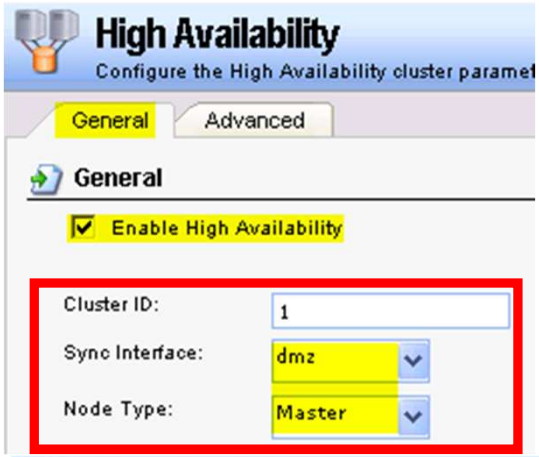


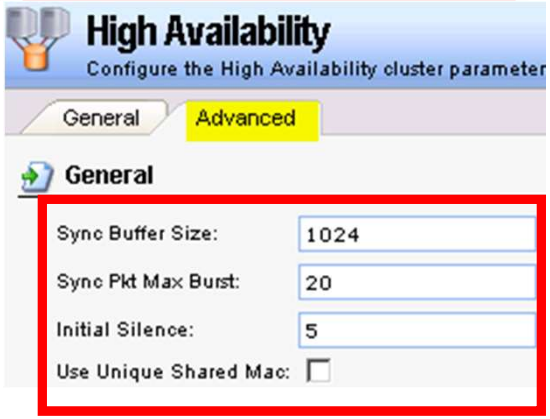

```
---> Shutdown RECONFIGURE on 2008-07-14 04:37:32 <---



Attempting to use new configuration data...
Parsed 'NodeID=SLAVE' directive in configuration. Acting as a HA slave.

Warning W4503/IFACES in "wan1.Ethernet":
  - Shared HA IP address not set
  wan1 PBR main MTU 1500 DHCPCLIENT { ENABLED YES AUTONAMES NO AUTOGWNAME NO IPNAME wan1_ip NETNAME wan1net GWNAME wan1_g

Warning W4560/IFACES in "wan1.Ethernet":
  - DHCP does not work on HA clusters - only the unique interfaces addresses will be assigned.
  wan1 PBR main MTU 1500 DHCPCLIENT { ENABLED YES AUTONAMES NO AUTOGWNAME NO IPNAME wan1_ip NETNAME wan1net GWNAME wan1_g
CFG Warning: This unit should be a HA slave, but the configuration is non-HA.
Now running in local lockdown (admin-only) mode.
License file successfully loaded.

Configuration done
```

High Availability
Firewall A-setup procedure--(GUI)

2 Go to the ***General*** tab which is under the page of ***High Availability*** of ***System***, and then tick "***Enable High Availability***" option. The rest fields are setting as below:







HA Advanced Settings

The following CorePlus advanced settings are available for High Availability:

Sync Buffer Size

How much sync data, in Kbytes, to buffer while waiting for acknowledgments from the cluster peer.

Default: *1024*

Sync Pkt Max Burst

The maximum number of state sync packets to send in a burst.

Default: *20*

Initial Silence

The time in seconds to stay silent on startup or after reconfiguration.

Default: *5*

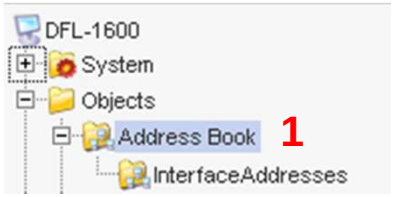
Use Unique Shared Mac

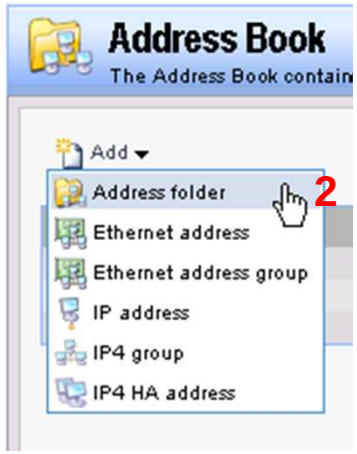
Use a unique shared mac address for each interface.

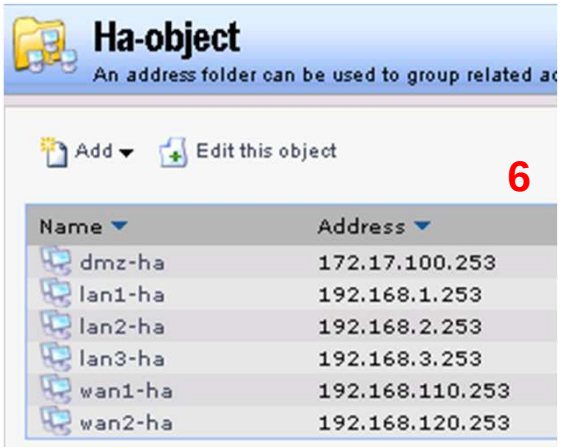
Default: *Disabled*

High Availability
Firewall A-setup procedure--(GUI)

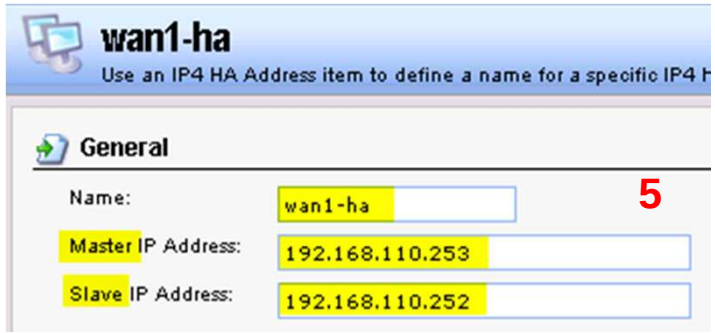
3 Now we have to create the “IP4 HA address” object for each interface.





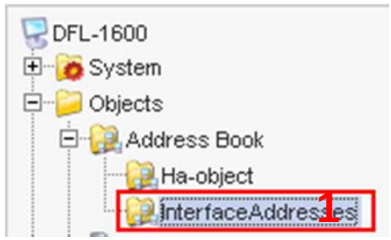


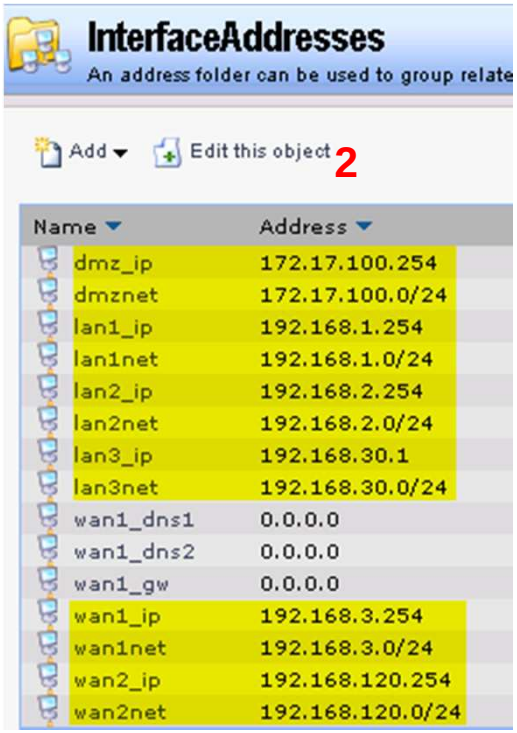
Repeat the same procedure from 4 to 5 to create for every interfaces



High Availability
Firewall A-setup procedure--(GUI)

4 After having done the settings of IP4 HA addresses(The IPs are used for teaming group to know each other and administration only), we have to address the IP4 Shared address as below:

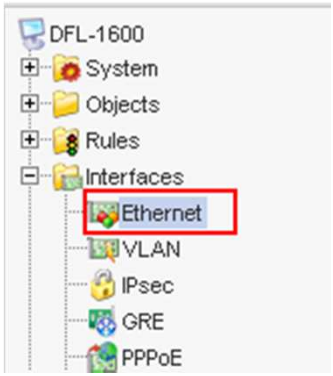


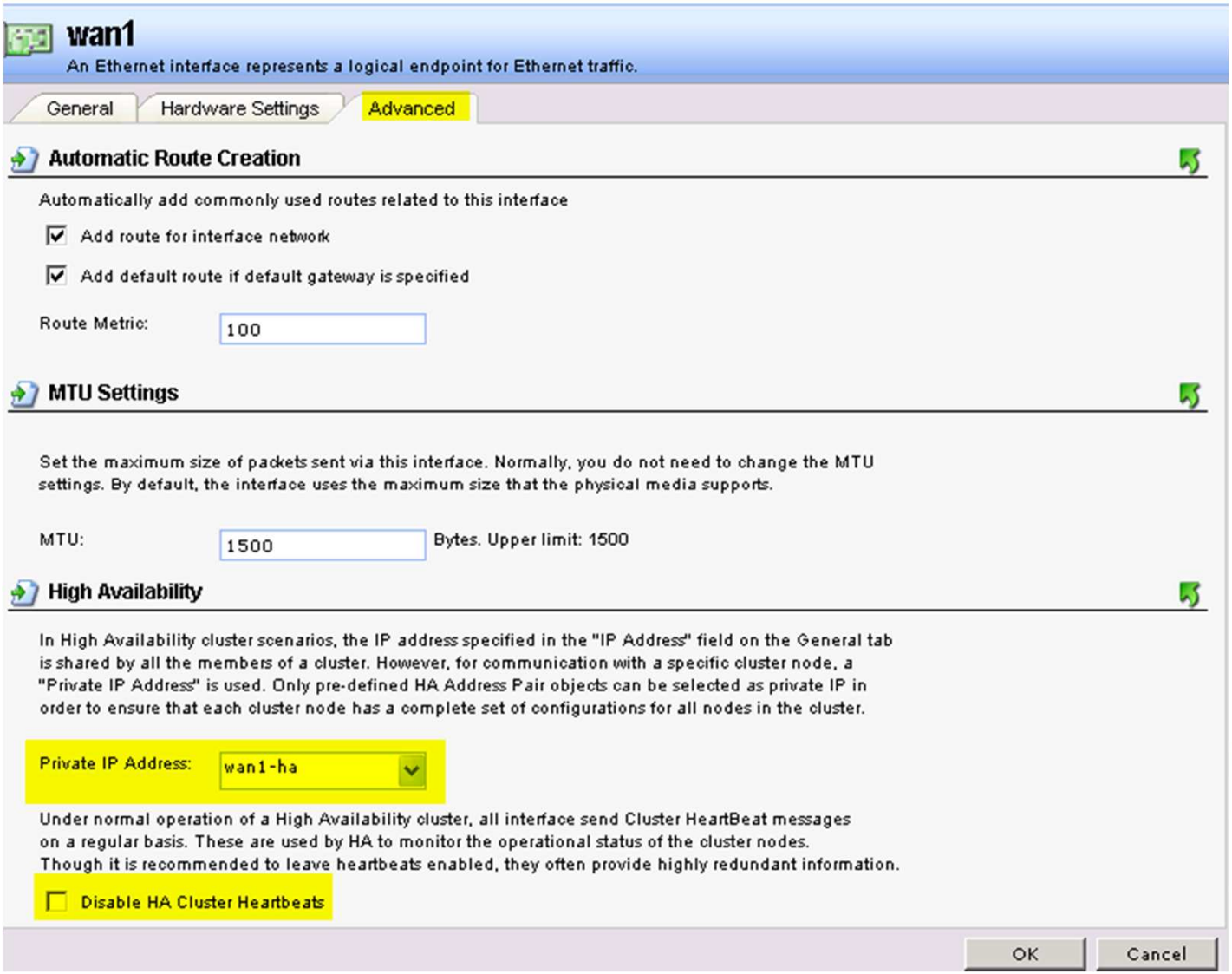


High Availability
Firewall A-setup procedure--(GUI)

5

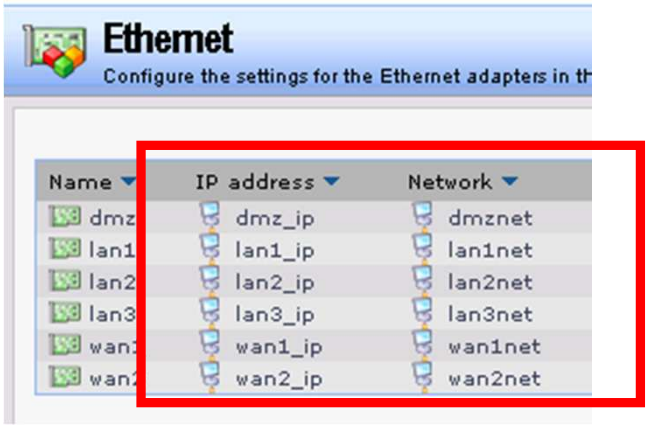
Go to find the ***Private IP Address*** field which is under the ***Advanced*** tab of the left tree view ***Ethernet*** page of the ***Interface***, and then select a suitable IP4 HA object which we created in step 3 for every interfaces. Repeat the same way till every interfaces has been assigned the value in "***Private IP Address***".

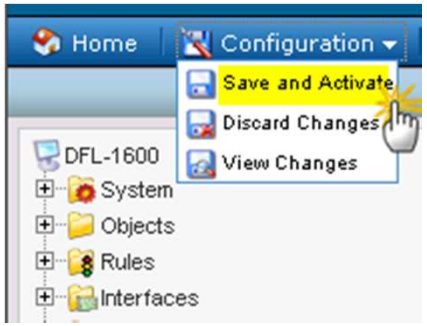




High Availability
Firewall A-setup procedure--(GUI)

6 In the ***Ethernet*** page, in addition to setup the IP HA addresses, we still have to verify if the settings of Shared IP and Network range are correct. After having done all the settings, don't forget to do the "Save and Activate".





Configure High Availability on Firewall A

Following procedure shows how to configure both NetDefend Firewalls are running in High Availability mode to provide a fault-tolerance capability based on last slide.

Note: Make sure to use same model and firmware version for both appliances!

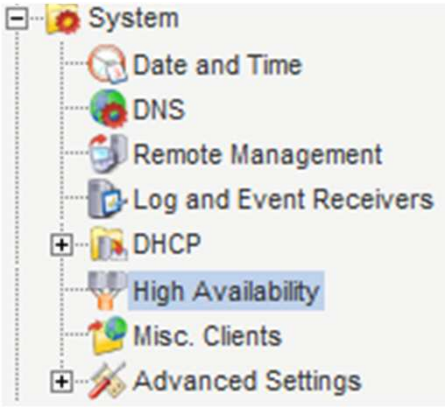
WebUI

1. Firewall A (HA Master): Rename current IP Address objects

Go to Objects > Address Book > InterfaceAddresses:

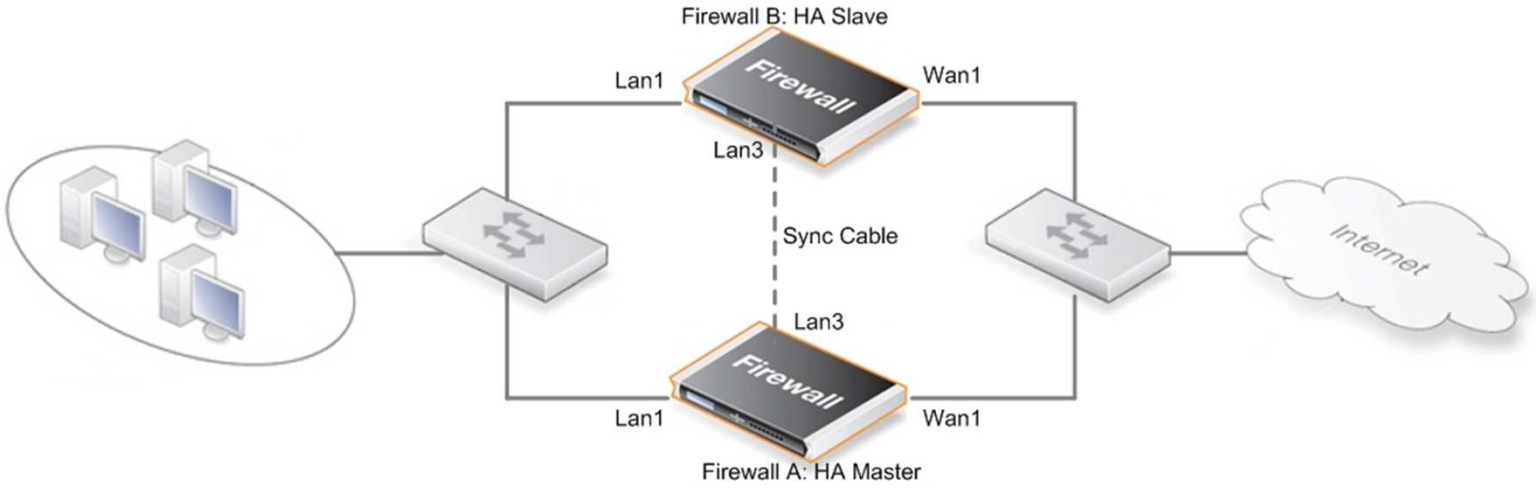
Rename **dmz_ip** object as ***Shared_dmz_ip*** and change IP Address to ***172.17.100.254***
Rename **dmznet** object as ***Shared_dmznet*** and change IP Address to ***172.17.100.0/24***
Rename **lan1_ip** object as ***Shared_lan1_ip*** and change IP Address to ***192.168.1.254***
Rename **lan1net** object as ***Shared_lan1net*** and change IP Address to ***192.168.1.0/24***
Rename **lan2_ip** object as ***Shared_lan2_ip*** and change IP Address to ***192.168.2.254***
Rename **lan2net** object as ***Shared_lan2net*** and change IP Address to ***192.168.2.0/24***
Rename **lan3_ip** object as ***Shared_lan3_ip*** and change IP Address to ***192.168.3.254***
Rename **lan3net** object as ***Shared_lan3net*** and change IP Address to ***192.168.3.0/24***
Rename **wan1_ip** object as ***Shared_wan1_ip*** and change IP Address to ***192.168.110.254***
Rename **wan1net** object as ***Shared_wan1net*** and change IP Address to ***192.168.110.0/24***
Rename **wan1_gw** object as ***Shared_wan1_gw*** and change IP Address to ***192.168.110.250***
Rename **wan2_ip** object as ***Shared_wan2_ip*** and change IP Address to ***192.168.120.254***
Rename **wan2net** object as ***Shared_wan2net*** and change IP Address to ***192.168.120.0/24***

Configure High Availability on Firewall B



High Availability Scenario Hands-on

Planning to Create High Availability Cluster



Interface	Shared IP Address	HA Master IP Address	HA Slave IP Address
Wan1	**192.168.110.254**	**192.168.110.253**	**192.168.110.252**
Wan2	192.168.120.254	192.168.120.253	192.168.120.252
DMZ	172.17.100.254	172.17.100.253	172.17.100.252
Lan1	**192.168.1.254**	**192.168.1.253**	**192.168.1.252**
Lan2	192.168.2.254	192.168.2.253	192.168.2.252
Lan3	192.168.3.254	192.168.3.253	192.168.3.252