Configure Virtual MAC Addresses for FTD HA

Contents

Introduction

Prerequisites

Requirements

Components Used

Background Information

Configuration

Verification

Introduction

This document describes how to configure Virtual MAC addresses on a Firewall Threat Defence (FTD) High-Availability (HA) pair.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Firewall Threat Defense (FTD)
- Secure Firewall Management Center (FMC)

Components Used

- FMC virtual version 7.2.8
- FTD virtual version 7.2.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Configuring virtual MAC addresses on an FTD HA pair is beneficial to the availability of a network. Virtual MAC addresses allow the primary and secondary FTD to maintain consistent MAC addresses which prevents certain traffic disruptions.

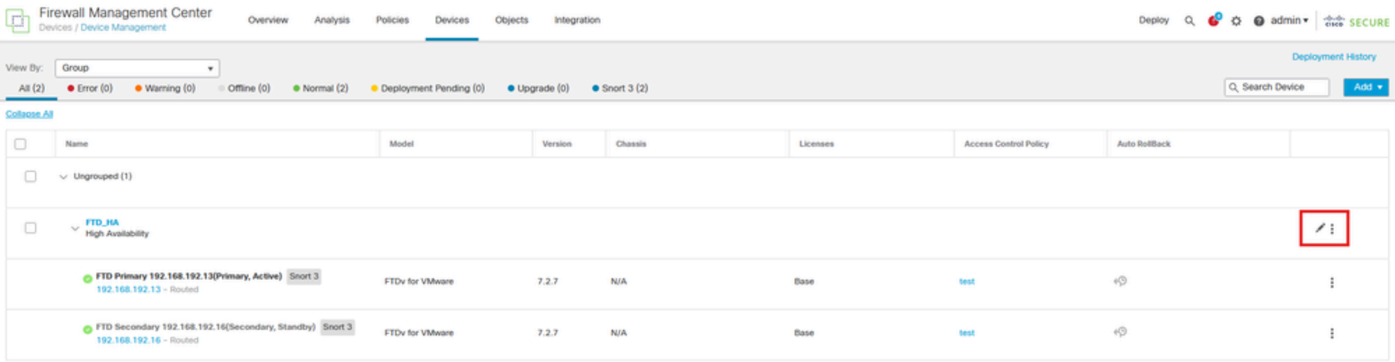
Without virtual MAC addresses configured, each unit of the HA pair boots using its burned-in MAC addresses. In the event the secondary unit boots without detecting the primary unit, it becomes the active unit and uses its burned-in MAC addresses. When the primary unit is eventually brought online, the secondary unit obtains the primary unit's MAC addresses which can cause network disruptions. New MAC addresses are also used if the primary unit is replaced with new hardware. Having virtual MAC addresses configured on the devices protects against this disruption. This is because the secondary unit knows the primary units MAC addresses at all times and continues using the correct MAC addresses when it is the active device, even if it comes online before the primary unit.

Note: The terms Virtual MAC address and Interface Mac address can be used interchangeably.

For additional information on the benefits of this configuration, refer to this guide.

Configuration

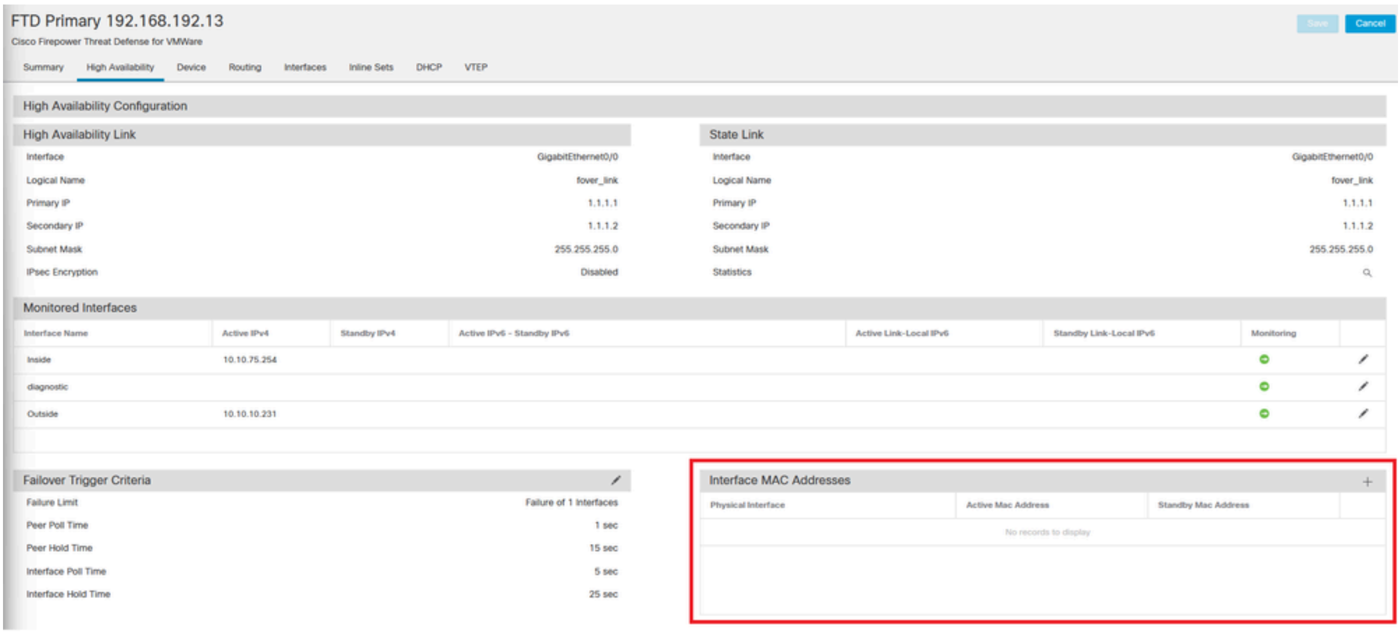
1. From the FMC GUI, navigate to the **Devices** page and edit the **HA pair** by clicking the **pencil** icon on the far right.



Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (1)						
FTD_HA High Availability						
FTD Primary 192.168.192.13(Primary, Active) Snort 3 192.168.192.13 - Routed	FTDv for VMware	7.2.7	N/A	Base	test	
FTD Secondary 192.168.192.16(Secondary, Standby) Snort 3 192.168.192.16 - Routed	FTDv for VMware	7.2.7	N/A	Base	test	

FTD HA Pair

2. Under the **High Availability** tab, locate the box labeled **Interface MAC Addresses.** Click the **+** icon to access the editor.



High Availability Configuration

High Availability Link

Interface	GigabitEthernet0/0
Logical Name	fover_link
Primary IP	1.1.1.1
Secondary IP	1.1.1.2
Subnet Mask	255.255.255.0
IPsec Encryption	Disabled

State Link

Interface	GigabitEthernet0/0
Logical Name	fover_link
Primary IP	1.1.1.1
Secondary IP	1.1.1.2
Subnet Mask	255.255.255.0
Statistics	

Monitored Interfaces

Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring
Inside	10.10.75.254					●
diagnostic						●
Outside	10.10.10.231					●

Failover Trigger Criteria

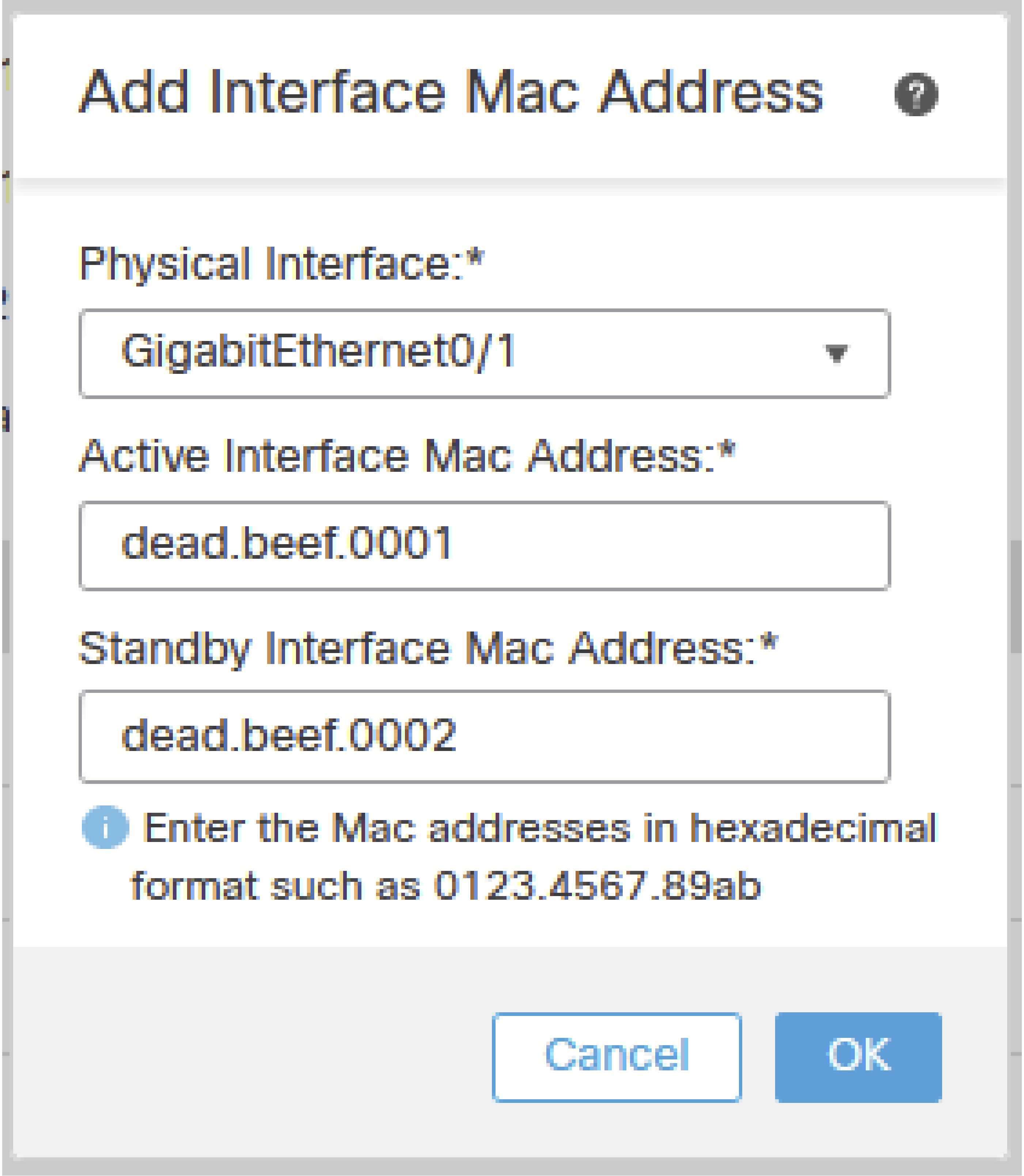
Failure Limit	Failure of 1 Interfaces
Peer Poll Time	1 sec
Peer Hold Time	15 sec
Interface Poll Time	5 sec
Interface Hold Time	25 sec

Interface MAC Addresses +

Physical Interface	Active Mac Address	Standby Mac Address
No records to display		

Interface MAC Addresses Box

3. From the editor, select the **Physical Interface** and configure the **Active/Standby Interface Mac Addresses**. Click **OK** when completed.



Add Interface Mac Address

Physical Interface:*

GigabitEthernet0/1

Active Interface Mac Address:*

dead.beef.0001

Standby Interface Mac Address:*

dead.beef.0002

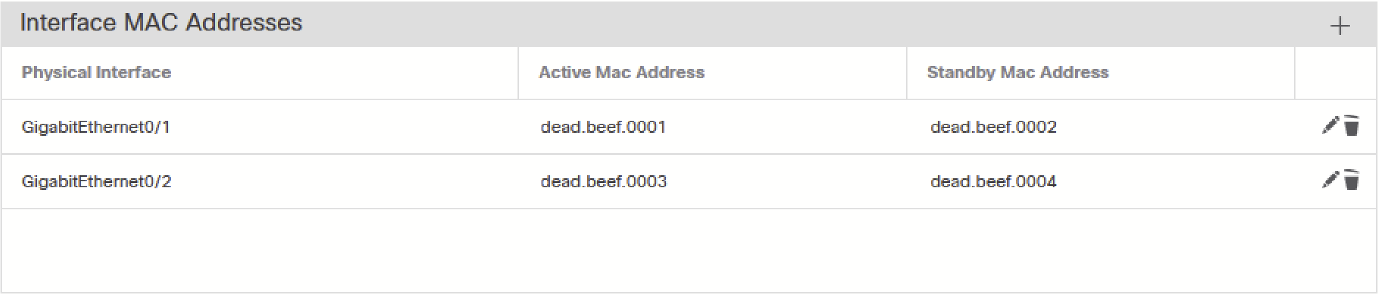
Enter the Mac addresses in hexadecimal format such as 0123.4567.89ab

Interface Mac Address Creation

Note: When configuring the virtual MAC addresses, it is helpful to adhere to a standard convention. The addresses within the interfaces need to be valid MAC addresses but can be arbitrary in nature. Using a standard convention allows for ease of management when checking the upstream or downstream MAC address tables. MAC address formatting requires 12 hexadecimal digits with periods separating each set of 4 digits.

4. Repeat the process for any remaining interfaces needing virtual Mac address configurations.

5. Confirm the configurations are correct.



Interface MAC Addresses +

Physical Interface	Active Mac Address	Standby Mac Address	
GigabitEthernet0/1	dead.beef.0001	dead.beef.0002	✎ 🗑
GigabitEthernet0/2	dead.beef.0003	dead.beef.0004	✎ 🗑

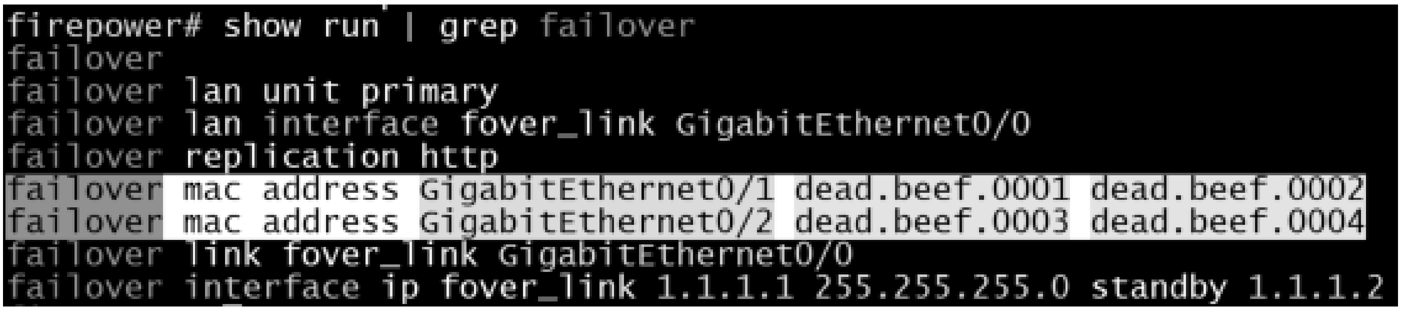
Interface Mac Address Configurations

6. Save and **Deploy** the configurations to the FTD HA pair.

Verification

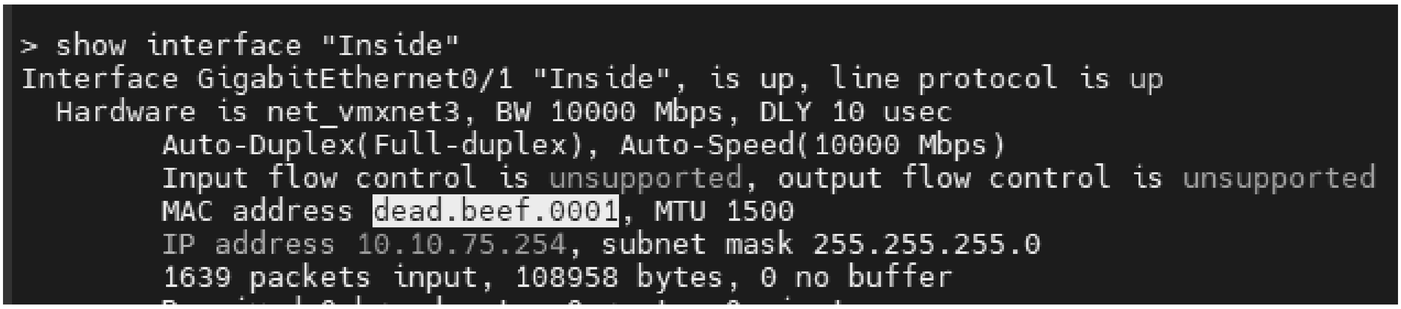
From each of the devices running configurations, the virtual Mac addresses now appear.

Primary (active) FTD:



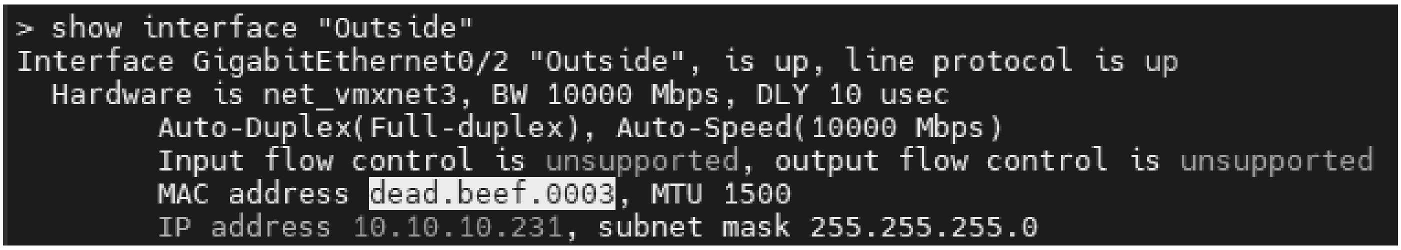
```
firepower# show run | grep failover
failover
failover lan unit primary
failover lan interface fover_link GigabitEthernet0/0
failover replication http
failover mac address GigabitEthernet0/1 dead.beef.0001 dead.beef.0002
failover mac address GigabitEthernet0/2 dead.beef.0003 dead.beef.0004
failover link fover_link GigabitEthernet0/0
failover interface ip fover_link 1.1.1.1 255.255.255.0 standby 1.1.1.2
```

Show Run Failover Results



```
> show interface "Inside"
Interface GigabitEthernet0/1 "Inside", is up, line protocol is up
  Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address dead.beef.0001, MTU 1500
        IP address 10.10.75.254, subnet mask 255.255.255.0
        1639 packets input, 108958 bytes, 0 no buffer
```

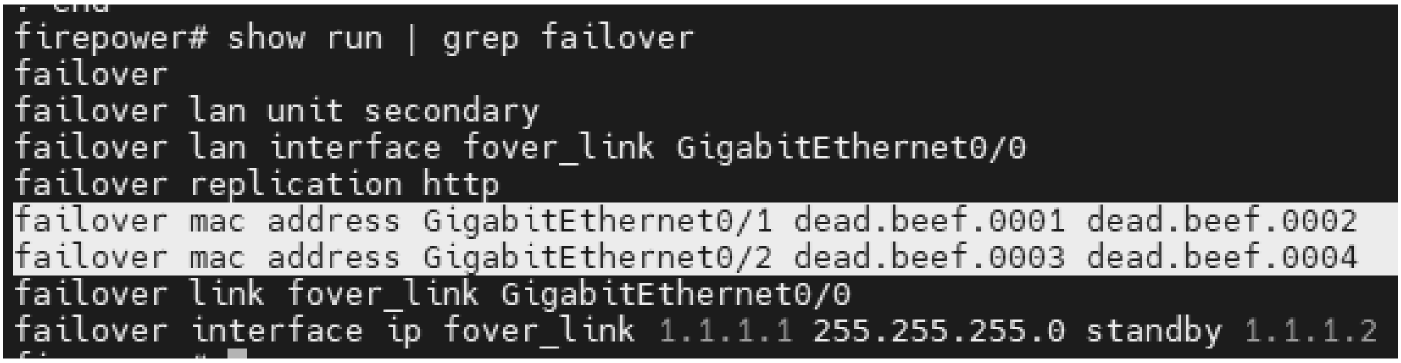
Show Interface Inside Results



```
> show interface "Outside"
Interface GigabitEthernet0/2 "Outside", is up, line protocol is up
  Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address dead.beef.0003, MTU 1500
        IP address 10.10.10.231, subnet mask 255.255.255.0
```

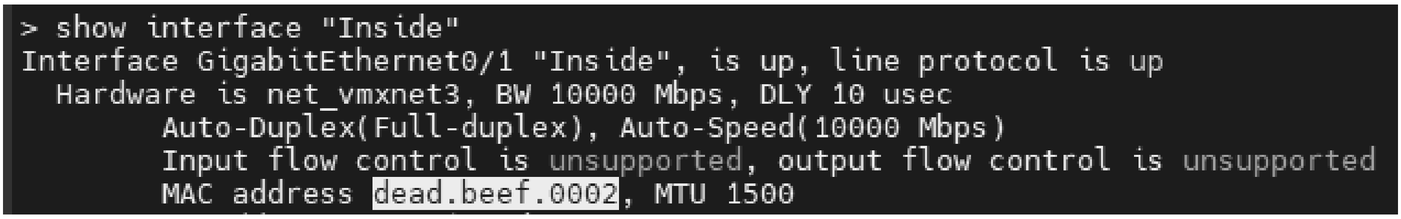
Show Interface Outside Results

Secondary (standby) FTD:



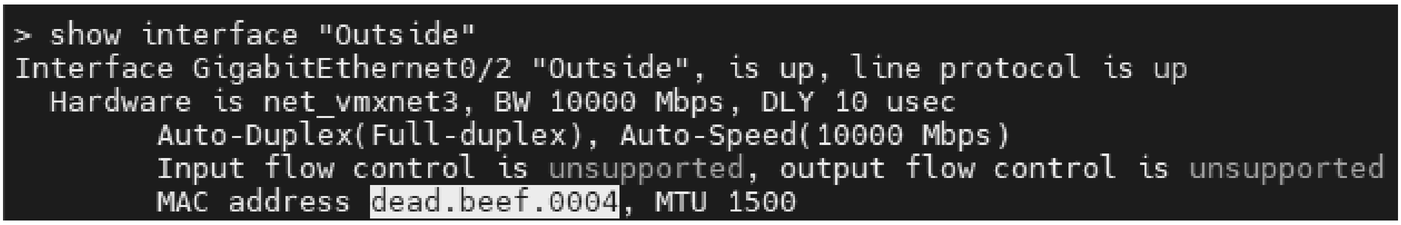
```
firepower# show run | grep failover
failover
failover lan unit secondary
failover lan interface fover_link GigabitEthernet0/0
failover replication http
failover mac address GigabitEthernet0/1 dead.beef.0001 dead.beef.0002
failover mac address GigabitEthernet0/2 dead.beef.0003 dead.beef.0004
failover link fover_link GigabitEthernet0/0
failover interface ip fover_link 1.1.1.1 255.255.255.0 standby 1.1.1.2
```

Show Run Failover Results



```
> show interface "Inside"
Interface GigabitEthernet0/1 "Inside", is up, line protocol is up
  Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address dead.beef.0002, MTU 1500
```

Show Interface Inside Results



```
> show interface "Outside"
Interface GigabitEthernet0/2 "Outside", is up, line protocol is up
  Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address dead.beef.0004, MTU 1500
```

Show Interface Outside Results

This confirms the configuration was successful.