Troubleshooting Guide: Restoring a Standalone DHCP Failover Server to Backup State in Cisco Network Registrar

June 2008
OL-16443-01

Introduction

This document describes how to recreate a DHCP failover relationship between a main and backup server after the unusual situation where a backup server was put in standalone mode. The information applies to all releases of Cisco Network Registrar supporting DHCP Failover.

In this scenario, an administrator took the main failover server offline because of a hardware failure or manual shutdown of Network Registrar. The failover relationship with the main server was turned off, and the backup server was pressed into service temporarily as a standalone DHCP server. Unfortunately, restoring the previous failover relationship from this condition can be hazardous to the lease state data.

According to the DHCP Failover protocol, if either of the partners maintained in a failover relationship fails, recovery is assured because the partners resynchronize. Even with a failed backup server, putting the main server in standalone mode would not be overly complicated to recover to failover mode.

However, restoring a standalone DHCP server to backup is not straightforward. The standalone server must first assume the role of main, and the original main server becomes the backup. After the partners synchronize, the failover relationship must again be purposely broken to reverse the two server roles. Finally, the partners must resynchronize in their original failover roles.

Background

For the remainder of this document, the main DHCP failover server is identified as Server A (with IP address 10.86.154.59), and the backup server as Server B (with IP address 10.86.154.60). Server A was administratively or otherwise shut down or its Network Registrar server agent stopped. At this point, Server B goes into the Communications-Interrupted mode.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

The system administrator could then take one of three approaches:

- **Continue running backup Server B in Communications-Interrupted mode**—The risk of running the backup server in this mode indefinitely is that it can exhaust the pool of typically 10% of the available addresses with which the backup server is allocated to service new clients.
- **Put Server B into Partner-Down mode without breaking the failover relationship**—One major caveat of giving the backup server full control of the address space without suspending failover is that the full transfer of the address space ownership does not occur until after the configured Maximum Client Lead Time (MCLT). The MCLT is an additional time period set on the main server that controls by how much the client lease expiration is ahead of what the backup server detects it to be. The MCLT is typically 60 minutes. Until the MCLT expires, the backup server's available address pool is limited to its allocated reserve.
- **Put Server B into Partner-Down mode and break the failover relationship**—This approach puts the backup server in standalone mode, and is the approach that the administrator chose in this scenario. The deciding factors were that the main server was expected to be offline for an extended period, and the number of new devices coming online was higher than anticipated. Because the low percentage of available addresses that the backup server could service would soon cause an outage for new devices, the administrator put Server B in standalone mode. **The disadvantage of this approach is the care and effort required to preserve the original state of the network when restoring the partners to their original relationship**.

The conclusion is that the first two approaches have distinct advantages over the third. In most cases, the backup server is expected to have enough addresses to cover newly arrived clients until the MCLT expires. Pursuing the third approach can incur unnecessary administrative burden and risk.

General Procedure

The repair procedure is:

1. **Temporarily assign backup Server B the role of main failover server**—Reversing the failover partner roles effectively allows Server A to learn the current failover state from Server B.
2. **Migrate Server A and Server B back to their original failover roles**—The goal is for Server A to reacquire its original status as the main DHCP failover server.

The assumptions are:

- Original main Server A is nonoperational and Network Registrar is stopped.
- Original backup Server B is operational.
- Failover between the partners is administratively disabled.
- Determination was made not to permanently reverse the failover roles of the two partners.
- Domain Name Services (DNS) is not also running on either of the failover partners.
- The IP addresses used as examples in this Troubleshooting Guide are for demonstration purposes only.

Restoring the Failover Pair with Reversed Roles

The following steps restore failover by temporarily moving Server B into main server mode.

On **Server B** (10.86.154.60 or in cluster-B):

Step 1 Ensure that failover is disabled and modify the failover configuration, so that Server B becomes the main and Server A the backup:

- Network Registrar 6.1:

```
nrcmd> dhcp disable failover
nrcmd> dhcp set failover-main-server 10.86.154.60
nrcmd> dhcp set failover-backup-server 10.86.154.59
```

- Network Registrar 6.2 and later:

```
nrcmd> failover-pair examplepair set failover=false
nrcmd> failover-pair examplepair set main=cluster-B
nrcmd> failover-pair examplepair set backup=cluster-A
```

Step 2 Save the changes and reload the server:

```
nrcmd> save
nrcmd> dhcp reload
```

Step 3 Reenable failover and reload the server again:

```
nrcmd> dhcp enable failover or failover-pair examplepair set failover=true
nrcmd> dhcp reload
```

Server B is now the main failover server ready for its partner to become operational again. Any further action that you must take to prevent Server A from beginning to give out addresses in the meantime depends on its current state. If it is:

- **Powered off**—See the "Starting with Server A Powered Off" section.
- **Powered on with the Network Registrar server agent disabled**—See the "Starting with Server A Powered On and Server Agent Disabled" section on page 4.
- **Replaced by another machine**—See the "Starting with Server A Replaced" section on page 6.

Starting with Server A Powered Off

If Server A was powered off, you must power it on again to continue. The next steps ensure that Server A comes online while preventing IP address leakage.

On **Server A** (10.86.154.59 or in cluster-A):

Step 1 Turn on the server, but prevent it from being active. How to do this is specific to your environment. Typically, if the machine is:

- Physically available, manually disconnect the network cable, then boot up the machine.
- Running SPARC Solaris and is managed remotely via reverse Telnet through a communication server, bring it online in single-user mode. Provided Network Registrar is not installed on one of the partitions that is mounted automatically in single-user mode, this is enough to keep the DHCP server

from starting. After logging in as *root* in single-user mode, bring the partition on which Network Registrar is mounted online. This action makes the programs and data available without starting the server agent. (Normally, use the **mountall** command for this last step.)

Step 2 Stop the Network Registrar server agent, if it is started:

Solaris/Linux	`/etc/init.d/nwreglocal stop`
Windows	`net stop nwreglocal`

If it is not possible to bring the machine online without taking it off the network and starting the server agent, stop the server agent as quickly as possible. There might be a period during which the server can inadvertently give out addresses.

Step 3 Go to the "Starting with Server A Powered On and Server Agent Disabled" section.

Starting with Server A Powered On and Server Agent Disabled

Starting from a point where Server A is powered on, but the Network Registrar server agent is turned off, configure Network Registrar so that you can start the server agent without automatically enabling the DHCP server to give out addresses.

On **Server A** (10.86.154.59 or in cluster-A):

Step 1 Using the Network Registrar **mcdadmin** utility, prevent DHCP from starting on server agent startup:

a. Add the following content to a disableDHCP.txt file:

```
# version: 1.0
[config/cluster/1/trampolines/1/servers/2]
config_path = str:[0]servers/name/DHCP/1
enabled = int32:[0]0
```

Note The syntax, case, and spacing are critical for this text.

The content indicates which tree and section of the MCD database to modify. Setting enabled to 0 disables the DHCP service while allowing the DHCP server to start up.

b. Run the **mcdadmin** utility with the following options and pointing to the disableDHCP.txt file:

```
mcdadmin -o -i disableDHCP.txt
```

Step 2 Restart the server agent:

Solaris/Linux	`/etc/init.d/nwreglocal start`
Windows	`net start nwreglocal`

Network Registrar will come online, but the DHCP service will be inactive.

Step 3 Examine the DHCP logs to confirm that the DHCP server is not running.

Step 4 Bring Server A back on the network. If:

- The network cable is unplugged, restore the network connection.
- Logged on in single-user mode, reboot.

Step 5 Reverse the partner roles and remove the failover state data:

a. Modify the failover configuration so that Server A becomes the backup server and enable failover:

- Network Registrar 6.1:

```
nrcmd> dhcp set failover-main-server 10.86.154.60
nrcmd> dhcp set failover-backup-server 10.86.154.59
nrcmd> dhcp enable failover
```

- Network Registrar 6.2 and later:

```
nrcmd> failover-pair examplepair set main=cluster-B
nrcmd> failover-pair examplepair set backup=cluster-A
nrcmd> failover-pair examplepair set failover=true
```

b. Set the DHCP service to be enabled on reboot and save the changes:

```
nrcmd> dhcp enable start-on-reboot
nrcmd> save
```

Note Do not reload the DHCP server at this point.

c. Remove all failover state data:

- Stop the server agent.
- Ensure that all Network Registrar processes are terminated.
- Kill any residual processes.
- Delete the event store and lease state databases.
- Delete the server level state (by using **mcdamin** again).
- Restart the server agent.

Solaris/Linux	/etc/init.d/nwreglocal stop ps -leaf | grep nwr kill -9 pid rm /var/nwreg2/local/data/dhcpeventstore/*.* rm -r /var/nwreg2/local/data/dhcp/ndb/*.* cd /opt/nwreg2/local/usrbin ./mcdadmin -a state -R /servers/name/DHCP/1/state /etc/init.d/nwreglocal start
Windows	net stop nwreglocal cd install-path\local\data delete dhcpeventstore\*.* delete dhcp\ndb\*.* cd install-path\local\bin mcdadmin -a state -R /servers/name/DHCP/1/state net start nwreglocal

Step 6 Go to the "Transferring Current Lease State to Server A" section on page 6.

Starting with Server A Replaced

If Server A was decommissioned and replaced, you must install Network Registrar and push the failover configuration from Server B to the new machine. Also, you must restore any customer configuration specific to Server A. After these steps, Network Registrar will start but not give out addresses:

Step 1 On **Server A** (10.86.154.59 or in cluster-A), install Network Registrar.

Step 2 Reconstruct the Network Registrar operating environment by restoring accompanying software, such as Cisco Broadband Access Center and its required DHCP extensions. Do not make any administrative changes to the configuration until after pushing the configuration to Server B.

Step 3 On **Server B** (10.86.154.60 or in cluster-B), by using the Network Registrar web UI, push an exact failover configuration to Server A, which effectively makes Server A the backup partner.

Step 4 On **Server A**:

a. Save the new configuration, but do not reload the server:

```
nrcmd> save
```

b. If necessary, customize the Network Registrar configuration as required for the operating environment, which might include making administrative changes.

c. Ensure that the configuration is complete.

d. Reload the DHCP server:

```
nrcmd> dhcp reload
```

Step 5 Go to the “Transferring Current Lease State to Server A” section.

Transferring Current Lease State to Server A

At this point, the failover partnership reestablishes itself, both servers will resynchronize their states, and Server A becomes operational as the backup server. The operation will pause for the MCLT period (of one hour) and both partners resume their failover operations in normal communication mode.

Note Do not proceed to the “Repairing Partners to Their Original Roles” section until both partners synchronize and report normal communication.

Repairing Partners to Their Original Roles

Assuming that both partners are fully synchronized and report normal communication, to ensure that the failover partners can assume their original roles, you should:

Step 1 On **Server A** (10.86.154.59 or in cluster-A), stop the DHCP server:

```
nrcmd> dhcp stop
```

Step 2 On **Server B** (10.86.154.60 or in cluster-B), stop the DHCP server:

```
nrcmd> dhcp stop
```

Step 3 On **Server A**:

a. Disable failover, then make Server A the main and Server B the backup:

- Network Registrar 6.1:

```
nrcmd> dhcp disable failover
nrcmd> dhcp set failover-main-server 10.86.154.59
nrcmd> dhcp set failover-backup-server 10.86.154.60
```

- Network Registrar 6.2 and later:

```
nrcmd> failover-pair examplepair set failover=false
nrcmd> failover-pair examplepair set main=cluster-A
nrcmd> failover-pair examplepair set backup=cluster-B
```

b. Save the changes and reload DHCP:

```
nrcmd> save
nrcmd> dhcp reload
```

c. Ensure that the configuration is in place and currently running. At this point, Server A is the sole operational DHCP server with 100% of the address pool.

d. Reenable failover:

```
nrcmd> dhcp enable failover or failover-pair examplepair set failover=true
```

e. Reload DHCP and double-check the configuration changes:

```
nrcmd> dhcp reload
```

Server A is now the failover main awaiting Server B to become operational.

Step 4 On **Server B:**

a. Make Server A the main and Server B the backup, then enable failover:

- Network Registrar 6.1:

```
nrcmd> dhcp set failover-main-server 10.86.154.59
nrcmd> dhcp set failover-backup-server 10.86.154.60
nrcmd> dhcp enable failover
```

- Network Registrar 6.2 and later:

```
nrcmd> failover-pair examplepair set main=cluster-A
nrcmd> failover-pair examplepair set backup=cluster-B
nrcmd> failover-pair examplepair set failover=true
```

b. Save the new configuration, but do not reload the server:

```
nrcmd> save
```

c. Remove all failover state data:

- Stop the server agent.
- Ensure that all Network Registrar processes are terminated.
- Kill any residual processes.
- Delete the event store and lease state databases.
- Delete the server level state (by using **mcdamin** again).

- Restart the server agent.

Solaris/Linux	**/etc/init.d/nwreglocal stop** **ps -leaf | grep nwr** **kill -9** *pid* **rm /var/nwreg2/local/data/dhcpeventstore/*.*** **rm -r /var/nwreg2/local/data/dhcp/ndb/*.*** **cd /opt/nwreg2/local/usrbin** ./**mcdadmin -a state -R** **/servers/name/DHCP/1/state** **/etc/init.d/nwreglocal start**
Windows	**net stop nwreglocal** **cd** *install-path*\local\\data **delete dhcpeventstore\*.*** **delete dhcp\\ndb\*.*** **cd** *install-path*\local\\bin **mcdadmin -a state -R** **/servers/name/DHCP/1/state** **net start nwreglocal**

At this point, the failover partnership reestablishes itself in its original roles, both servers will resynchronize their states, and Server B becomes operational as the backup server. The operation will pause for the MCLT period (of one hour) and both partners resume their failover operations in normal communication mode.

Step 5 On **Server A** and **Server B**:

a. Validate that both partners are in normal failover state:

```
nrcmd> dhcp getRelatedservers
```

b. Run a report and ensure that results match on both partners, allowing a bit of skew for the difference in running times between the partners.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.