Weird Solutions DHCP Server FAQ

Contents

1 Overview 1

2 Security 1

2.1 I forgot my administrator password. . . . 1

3 Expressions 1

3.1 Why does the server not accept my expressions? . . . 1

3.2 My expressions returns the wrong result! . . . 1

3.3 How do I enter a string value that is delimited with brackets? . . . 1

4 Dynamic DNS (DDNS) 1

4.1 How do I configure Dynamic DNS (DDNS) updates? . . . 1

4.1.1 Trusted DHCP clients . . . 2

4.1.2 Untrusted DHCP clients . . . 2

5 Leases 2

5.1 Why is my device is not receiving an address? . . . 2

5.1.1 Older vxWorks-based devices . . . 3

5.2 Can I assign one address to multiple devices? . . . 3

5.3 Can I force clients to renew their lease before it has expired? . . . 3

5.4 How do I enforce per-subscriber address limits? . . . 3

6 Remote Booting 3

6.1 How do I configure the boot file? . . . 3

6.2 Where's the "boot file" option for DHCPv6? . . . 4

6.3 How do I configure the TFTP server address? . . . 4

7 Logging 4

7.1 How do I configure log files that roll over every day? . . . 4

7.1.1 With the GUI . . . 4

7.1.2 With dhcpti . . . 4

7.2 Do I need to disable logging to get good performance? . . . 4

8 Cable Modems and MTAs 4

8.1 What is the correct way to set PacketCable legacy option 177 values? . . . 4

9 Database 5

9.1 I changed my server's hostname, and the database no longer works! . . . 5

10 Measuring Performance **5**

10.1 How can I measure performance? 5

10.1.1 CPU Usage 5

10.1.2 Disk Usage 5

11 Miscellaneous **6**

11.1 Is the CMTS command **source-verify dhcp** supported? 6

11.2 Does the DHCP server support Subnet Selection? 6

11.3 Can I make the server always broadcast to a client? (Or unicast?) 6

11.4 How do I configure the server to completely ignore certain DHCP clients? 6

12 What settings are required in the DHCP server to configure a cable modem? **7**

13 What settings are required in the DHCP server to configure an MTA? **7**

14 How do I upgrade the firmware on a modem? **8**

15 What are the Manufacturer Code Verification Certificates? **8**

Overview

This FAQ is for the Weird Solutions DHCP server.

Security

I forgot my administrator password.

- Open the file `dhcpt.conf` (Windows) or `/etc/dhcpt/dhcptd.conf` (Linux) and change the *password=AA-BB-CC* line to *password=*. Then restart the DHCP service. You can now log in with user name *Admin* and no password.

Expressions

Why does the server not accept my expressions?

- You must have the "Expression Evaluator" plugin installed for expressions to work.

My expressions returns the wrong result!

- Try surrounding your literal values with single quotes. For example, to specify the MAC address 00-A0-24-2F-10-26, write *'00-A0-24-2F-10-26'+*. Without the single quotes the server could interpret the MAC address as a set of substraction operations instead of a sequence of bytes.

How do I enter a string value that is delimited with brackets?

When you define DHCP option values in Broadband Provisioner, you can specify literal values, such as *192.168.1.1*, or expressions, such as *[$IP.LOCAL()]*.

When Broadband Provisioner sees an option value that is delimited with brackets, it assumes that the value is an expression that must be executed. This means that if you enter this literal value for a string option:

```
[192.168.1.1]
```

i. Broadband Provisioner will asume that this is an expression, execute it, and return a result of *192.168.1.1*.

In order to include brackets with your literal values, enter the literal value using this syntax:

```
*["[value]"]*
```

This syntax describes an expression that returns a string delimited with brackets.

Dynamic DNS (DDNS)

How do I configure Dynamic DNS (DDNS) updates?

Decide which policy you want to enable DDNS updates for. The global policy will enable DDNS for every address leased, whereas other policies can limit the scope of when DDNS updates are made.

Trusted DHCP clients

If you trust the DHCP client(s) to supply a valid fully-qualified domain name, define these options in the policy:

```
option DDNS update server = 10.0.0.1
option DDNS update mode = 1
option DDNS update ttl = 300
option Reverse update zone = "1.168.192.ina-ddr.arpa"
```

The example above:

- Updates the DNS server on address 10.0.0.1
- Uses a DNS TTL of 300 seconds
- Updates the foward lookup zone based on the domain name supplied by the DHCP client(s)
- Updates the reverse lookup zone for the 192.168.1.0 network
- Uses the host name supplied by the client

Untrusted DHCP clients

If you do not trust the DHCP client(s) to supply a valid fully-qualified domain name, define these options in the policy:

```
option DDNS update server = 10.0.0.1
option DDNS update mode = 2
option DDNS update ttl = 300
option Reverse update zone = "1.168.192.in-addr.arpa"
option Forward update zone = "yourdomain.com"
option DDNS Hostname = [ $STR ($HWADDR()) ]
```

The example above:

- Updates the DNS server on address 10.0.0.1
- Uses a DNS TTL of 300 seconds
- Updates the foward lookup zone "yourdomain.com"
- Updates the reverse lookup zone for the 192.168.1.0 network
- Generates a host name from the DHCP client's link-layer (MAC) address

You can generate or lookup host names in a variety of ways using the DHCP server's expression syntax.

Leases

Why is my device is not receiving an address?

- Check the server's log. Are there any error or warning messages that explain why?
- Do you have an address pool defined for the network segment on which the client resides?
- If the client is attached to the same segment as your server, try defining option 1014, "Force broadcast" for that client's policy or for the local-segment pool.

Older vxWorks-based devices

Try defining option 1011, "Legacy datagram size" in the client's private policy.

Can I assign one address to multiple devices?

Warning
This configuration setting can have unintended side-effects. Carefully consider the use cases before assigning a single address to multiple DHCP clients.

You can achieve this by defining the "Override Client ID" option in a policy. The client-id value you supply is used for tracking leases in the server, so if two devices have the same "Override Client ID", they will appear as the same device to the DHCP engine.

The "Override Client ID" option cannot be defined in a pool. Generally speaking, you should be careful to limit the scope of this option. Device-specific policies are probably the best place to define it, and the Global policy is probably the worst, since defining it in the Global policy would effectively assign the same IP address to every device on your network.

Can I force clients to renew their lease before it has expired?

Yes. Define the "DHCP renewal time" and "DHCP rebinding time" in a pool. The server normally calculates these values according to the DHCP standard recommendations, but these options allow you to override that behavior.

How do I enforce per-subscriber address limits?

You can enforce address limiting in the DHCP server by defining the "Circuit ID address limit", "Remote ID address limit" or "Subscriber ID address limit" option in a policy.

If you define the "Circuit ID address limit" in the Global policy, and set its value to 5, you effectively limit every circuit on your network to a maximum of five leases.

Note
The DHCP server can only perform address limiting if it's configured to store Remote ID (RID), Circuit ID (CID) or Subscriber ID for each address it leases. By default, the server stores RID in the "tid" field of a lease if the RID is available at lease time. To configure the server to store CIDs or SIDs, define option 1026, "Binding TID type". The TID types are shown in the description for this option.

Remote Booting

How do I configure the boot file?

Use any combination of the options below. Some clients will only accept one or the other.

- option 67, ""Overload boot file name"
- using option 1000, "Boot file"

[Note] Option 1008, "MS option 67" is deprecated in favor of option 67.

Where's the "boot file" option for DHCPv6?

As of this writing, there isn't a generic boot file option. At least one organization has defined a vendor-specific option for conveying their boot file name. There is ongoing discussion of a generic boot file option.

How do I configure the TFTP server address?

Define option "Overload tftp server name", and set its value to the host name of your TFTP server.

Some booting hosts don't have a DNS resolver, and instead require the IP address of the TFTP server. In this case, define option 1010, "Next server", and set its value to the IP address of your TFTP server.

The "Server name" option is a much older way of giving a device its TFTP server name, and was never standardized. Use this option as a last resort.

[Note] The "MS option 66" option is deprecated in favor of option 66, "Overload tftp server name".

Logging

How do I configure log files that roll over every day?

With the GUI

Click Setup→DHCP

Set `system.log.targets=file`.

Set `system.log.target.file=["/var/log/dhcptd/" + $DATE() + ".log"]`

Note: Create the `/var/log/dhcptd` directory if it does not exist

With dhcpti

Execute these commands after connecting with dhcpti:

```
set_context=4

set_properties
system.log.targets=file
system.log.target.file=["/var/log/dhcptd/" + $DATE() + ".log"]
```

Do I need to disable logging to get good performance?

Not necessarily. The server logs asynchronously, so you can run with at least audit-level logging with no noticeable performance degradation. Debug logging may cause a slight performance degradation, and verbose logging will definitely cause a reduction in performance.

Cable Modems and MTAs

What is the correct way to set PacketCable legacy option 177 values?

See the question "How do I enter a string value that is delimited with brackets?"

For the legacy PacketCable option 177, use the expression-bracket syntax for these options:

- TSP Primary DHCP (177/1)
- TSP Secondary DHCP (177/2)
- TSP Primary DNS (177/4)
- TSP Secondary DNS (177/5)

Database

I changed my server's hostname, and the database no longer works!

Firebird creates some host-specific filenames during installation. If your host name changes, these files can no longer be detected by Firebird.

Rename the following files, substituting your new host name:

isc_init1.myserver.mydomain.com isc_lock1.myserver.mydomain.com

Measuring Performance

How can I measure performance?

Broadband Provisioner is comprised of a number of daemon (service) programs, each of which uses multiple database server programs in the normal course of operation. This means that at any given time, you will have many processes running on your server that are dedicated to the functioning of Broadband Provisioner.

The DHCP server includes a rich set of counters that are accessible from the command line. These counters give you a detailed breakdown of the operations the service is performing. For a description of how to access and interpret these counters, see the Broadband Provisioner Administrator's Guide.

For all running processes, the tools described in this section can help you determine whether or not there is any activity associated with each process, where that activity is, and (possibly) why that specific activity is taking place.

CPU Usage

The *top* command allows you to see which processes are using the most CPU time. When you run *top*, the processes that use the most CPU are listed at the top of your screen. The order of processes shown in *top* changes dynamically as the CPU use for each process changes.

Each daemon that ships with Broadband Provisioner is a single process, but inside each daemon process there are many independent database connections. Each of these connections is in turn directly associated with a unique Firebird database process (fb_inet_server).

So for example in the DHCP process, **dhcptd**, may have twenty (20) simultaneously open database connections. In this case, you would see one **dhcptd** process, and twenty (20) **fb_inet_server** processes.

It is normal on a busy network to see the CPU use for **dhcptd**, **tftptd**, **syslogtd** and **fb_inet_server** to rise and fall. The more traffic on your network and the greater the logging detail for these processes, the more CPU time they will use.

Disk Usage

The *sar* program from the **sysstat** package can show the system throughput for all disks.

To run *sar*:

sudo sar -d 3 0

-or-

sudo sar -d 3 1

The *sar* program shows the reads and writes for each disk over a short period of time. It also shows the backlog of reads and writes waiting to be processed by the disk subsystem, as well as an overall utilization for each disk.

Firebird periodically performs cleanup on the database, and under normal circumstances this happens automatically and almost instantaneously. In the event of a problem, however, Firebird can spend a large amount of time performing a cleanup. If this occurs, you will likely notice very low CPU usage for all Broadband Provisioner processes, but very high disk utilization. If this occurs, check the system log to ensure that no disk errors are being reported. If everything looks fine, simply wait for the cleanup to complete.

Miscellaneous

Is the CMTS command source-verify dhcp supported?

Yes. The DHCP name for this feature is LeaseQuery, and it's supported by the DHCP LeaseQuery plugin.

Does the DHCP server support Subnet Selection?

Yes, but you must enable it. By default a pool cannot be explicitly chosen by a device, but you can define option 1004, "Device selectable" in a pool to enable this feature.

This option is not limited to pools - if you define it in the Global policy, for example, it allows all pools to be available for subnet selection.

Can I make the server always broadcast to a client? (Or unicast?)

Only for clients on the local segment.

- To always broadcast to a client on the local segment, define option 1014, "Force broadcast" for that client's policy or for the local-segment pool.
- To always unicast to a client on the local segment, define option 1013, "Force unicast" for that client's policy or for the local-segment pool.

How do I configure the server to completely ignore certain DHCP clients?

Solution 1:

```
If the client already has an account on the DHCP server, simply associate
that account with a domain that has no resources. A domain with no resources
is typically referred to as a "Lockdown" domain.
```

Solution 2:

```
If the client doesn't already have an account, you could manually create one
and associate it with a Lockdown domain.
```

Solution 3:

```
If the server is configured to auto-provision new machines, it will execute the
auto-provision expression when a client first tries to get an address. Your
expression can be written in such a way as to recognize this client (or clients)
and return a Lockdown domain for the new account to be associated with.
```

```
Using this solution, the server will create accounts for the client(s),
but the accounts will automatically be put in Lockdown domains.
```

Solution 4:

```
If the server is configured to auto-provision new machines, it will execute the
auto-provision expression when a client first tries to get an address. Your
expression can be written in such a way as to recognize this client (or clients)
and return an empty list of domains.

Using this solution, the server will NOT create accounts for the client(s). The
client will still receive access to the 'All nodes' domain, so no server resources
should be available to that domain.
```

What settings are required in the DHCP server to configure a cable modem?

<incomplete>

What settings are required in the DHCP server to configure an MTA?

If a cable modem contains an embedded MTA (eMTA), the cable modem will usually (USUALLY) request option 122 in its DHCP discover. Older modems may request option 177.

You may configure both options in a policy marked **optional**, because the modem will only request one of the options (122 or 177).

For option 122, you need:

- 122/1: TSP Primary DHCP = 10.100.0.122
- 122/6: TSP Kerberos Realm = BASIC.2
- 122/3: TSP Provisioning Server = 10.100.0.122
- 15: Domain name = customerdomain.com
- 6: Domain name servers = 10.100.0.122
- 12: Hostname = ["mta-" + $LCASE($STRING($HWADDR()))]
- 7: Log servers = 10.100.0.122
- 1010: Next server = 10.100.0.122
- 66: Overload tftp server name = thisserver.customerdomain.com
- 4: Time servers = 10.100.0.122
- 2: Time offset = -10800
- 177/1: TSP Primary DHCP = [10.100.0.122]
- 177/6: TSP Realm = BASIC.1
- 177/4: TSP Primary DNS = [10.100.0.122]
- 177/3: TSP SNMP = [10.100.0.122]

How do I upgrade the firmware on a modem?

Let's use a Motorola Surfboard as an example:

- Create a new domain named *Motorola-Surfboard-Firmware-Upgrade*
- Create a new TFTP policy named *Motorola-Surfboard-Firmware-Upgrade* and make it available to members of the domain *Motorola-Surfboard-Firmware-Upgrade*
- Add these options to the new policy:
- option Software Upgrade Filename = <firmware file name>
- option Software Upgrade TFTP Server = <tftp server address>
- option SNMP MIB Object = 1.3.6.1.2.1.69.1.3.3;integer=2
- option Manufacturer Code Verification Certificate (M-CVC) = <Motorola CVC 1>
- option Manufacturer Code Verification Certificate (M-CVC) = <Motorola CVC 2>
- option Manufacturer Code Verification Certificate (M-CVC) = <Motorola CVC N>

The number of CVCs required above varies by manufacturer. You should configure every CVC that the manufacturer publishes. For a list of the CVCs we know of, see further down in this FAQ.

Note that manufacturers usually have different models of modems, and the firmware for each modem model is not normally interchangeable. Therefore you must either make one domain/policy pair for each specific model of modem, or you must make provisions (perhaps through a runtime expression) to deliver the correct firmware file name.

What are the Manufacturer Code Verification Certificates?

Manufacturer code verification certificates are digital signatures that are used by the modem to guarantee that the firmware being loaded is, in fact, certified by the manufacturer. These certificates are a way to ensure that hackers cannot upload modified firmware.

The current certificates are shown below:

- Motorola
- option Manufacturer Code Verification Certificate (M-CVC) = 30-82-03-A1-30-82-02-89-A0-03-02-01-02-02-10-3F-DF-7C-62-0B-B3-24-FB-57-2B-12-50-78-84-06-66-30-0D-06-09-2A-86-48-86-F7-0D-01-01-05-05-00-30-81-97-31-0B-30-09-06-03-55-04-06-13-02-55-53-31-39-30-37-06-03-55-04-0A-13-30-44-61-74-61-20-4F-76-65-72-20-43-61-62-6C-65-20-53-65-72-76-69-63-65-20-49-6E-74-65-72-66-61-63-65-20-53-70-65-63-69-66-69-63-61-74-69-6F-6E-73-31-15-30-13-06-03-55-04-0B-13-0C-43-61-62-6C-65-20-4D-6F-64-65-6D-73-31-36-30-34-06-03-55-04-03-13-2D-44-4F-43-53-49-53-20-43-61-62-6C-65-20-4D-6F-64-65-6D-20-52-6F-6F-74-20-43-65-72-74-69-66-69-63-61-74-65-20-41-75-74-68-6F-72-69-74-79-30-1E-17-0D-30-31-30-37-31-31-30-30-30-30-30-30-5A-17-0D-31-31-30-37-31-30-32-33-35-39-35-39-5A-30-65-31-0B-30-09-06-03-55-04-06-13-02-55-53-31-1D-30-1B-06-03-55
- option Manufacturer Code Verification Certificate (M-CVC) = 04-0A-13-14-4D-6F-74-6F-72-6F-6C-61-20-43-6F-72-70-6F-72-61-74-69-6F-6E-31-0F-30-0D-06-03-55-04-0B-13-06-44-4F-43-53-49-53-31-26-30-24-06-03-55-04-03-13-1D-43-6F-64-65-20-56-65-72-69-66-69-63-61-74-69-6F-6E-20-43-65-72-74-69-66-69-63-61-74-65-30-82-01-22-30-0D-06-09-2A-86-48-86-F7-0D-01-01-01-05-00-03-82-01-0F-00-30-82-01-0A-02-82-01-01-00-B9-FB-C5-7A-F8-81-46-4D-58-30-BC-16-77-8E-EC-A0-6A-CB-E6-C7-B8-85-92-4B-2D-AC-F5-94-E3-BE-23-32-03-CB-20-80-36-3D-67-73-B2-0C-8E-61-AE-2F-10-4D-4B-C8-8E-4C-66-4C-B3-52-86-04-EE-9F-62-1A-E4-5D-BB-C8-49-1F-79-88-89-5E-79-41-79-5F-95-D5-FB-1C-A6-97-37-59-5C-F4-FF-20-10-80-1C-22-14-EE-DE-3D-DB-17-32-D0-FD-5E-0A-7E-34-29-BC-20-85-FE-47-1C-E0-06-58-E8-CE-BD-18-AC-A1-68-0E-C4-34-58-E5-9B-B6-1F-64-9B-F0-50-12-36-89-D2-DC-4D

- option Manufacturer Code Verification Certificate (M-CVC) = 5E-34-23-51-9F-CB-34-16-69-F3-A9-6E-F3-BA-1E-33-71-B9-C2-E4-3A-B1-03-FC-DC-3B-AC-21-1E-B4-1D-30-48-A1-6A-3E-A1-EC-86-55-8A-C5-D7-89-39-00-9D-AC-77-73-6F-66-9A-0B-63-27-BD-CB-63-37-44-60-4E-2E-DB-6A-8D-A4-11-73-1E-F1-D9-B9-20-CF-7F-22-D1-A1-BC-37-5B-8F-0B-76-3F-7D-D9-D1-26-1D-28-4D-77-6F-DB-F8-58-90-7B-AA-F2-98-F5-92-08-60-0E-27-41-E0-5D-B8-7D-BB-02-03-01-00-01-A3-1A-30-18-30-16-06-03-55-1D-25-01-01-FF-04-0C-30-0A-06-08-2B-06-01-05-05-07-03-03-30-0D-06-09-2A-86-48-86-F7-0D-01-01-05-05-00-03-82-01-01-00-5C-5E-38-4A-E8-FB-24-77-4E-C0-87-A0-C9-80-60-CF-3C-2F-5D-1F-EC-60-18-2B-92-A1-B8-B1-ED-9D-49-FE-82-10-CB-21-04-DF-EE-31-92-D6-D6-2B-A2-B9-92-9F-89-75-AB-1D-D9-68-41-3A-1A-71-E6-69-A0-B3-6C-C1-14-67-36-CA-11-49-8E-D6-71-1D-62-34-52-7A-28-14-C8-D6-86-64-21
- option Manufacturer Code Verification Certificate (M-CVC) = 5E-C9-F3-80-44-F1-67-C6-7B-CA-F6-F3-4D-97-8F-AA-18-74-78-9D-D1-5D-91-CF-D3-55-A2-4A-F0-F1-BD-CC-30-19-3C-48-C3-94-84-CC-C3-C9-DA-C3-E6-91-94-37-8A-A8-D7-6F-B0-73-A4-B2-4E-FC-87-43-42-D4-F7-F5-05-47-90-2F-42-E0-B5-8D-F4-28-AD-59-16-75-C6-9E-70-63-96-50-8E-E1-E9-00-A4-E1-9B-6A-EA-0B-8C-5C-34-59-DF-0E-12-62-72-A7-D9-01-BB-FF-F3-8F-B2-17-34-3F-79-08-B8-3A-0A-C8-91-88-80-7C-31-EA-23-E9-B9-30-9A-28-A8-88-E7-A1-50-98-4E-7D-D9-42-D8-6B-15-A8-E6-24-75-9F-DC-A6-2A-4E-E5-C2-07-DC-A7-BD-56-7D-09-CC-EA-C7-4F-58-66-5B-B8