

Block Bad Guys With Windows 2008 R2 New DHCP MAC Address Filtering Tool

Steven Bink

When I first saw that Windows NT Server 3.5 included something called a "DHCP server" that freed me from having to hand-configure static IP addresses on every one of my IP-connected computers, I was delighted, and I've used Microsoft's DHCP in my networks ever since. Now, between NT 3.5 and now, DHCP hasn't really changed all that much.... unless you're talking about the DHCP server service shipped with Windows Server 2008 R2.

The new stuff in R2 isn't earth-shattering, but it is convenient, and provides a sort of "poor man's quarantine" by letting you control which machines your DHCP server should give IP addresses to, and lets you do it in a fairly convenient way. In this article, I'll introduce you to R2's DHCP MAC address filtering feature and how to make the most of it.

R2 DHCP MAC Filtering Overview

Basically, here's what R2's DHCP Server can do with MAC address filtering:

- Either block any particular MAC address from getting an IP address, or allow any particular MAC address to get an IP address.
- Arrange the question of gets blocked from and who gets allowed to have an IP address either as a whitelist (no one gets an IP address unless their MAC address is on the "allowed" list) or a blacklist (everyone gets an IP address unless their MAC address is on the "deny" list).
- By default, DHCP runs as a blacklist with no IP addresses on the "deny" list.

R2's DHCP server lets you enter one or MAC addresses into its filters in several ways:

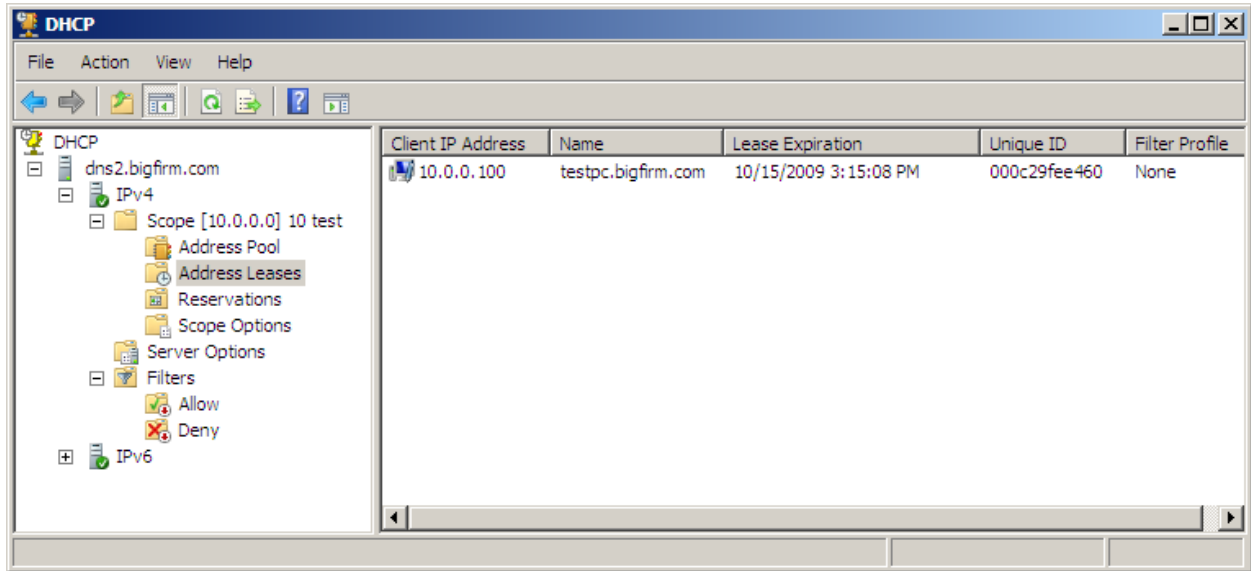
- hand-enter the MAC address into the GUI (ugh)
- hand-enter a range of MAC addresses using "*" as a wild card (better)
- select a bunch of systems that already have a DHCP lease, right-click them and add them to either the allow or deny list with just a few mouse clicks (even better)
- feed the DHCP server a text list of MAC addresses
- use a new command-line tool to enter one or more MAC addresses

I'll show you how to do all that here.

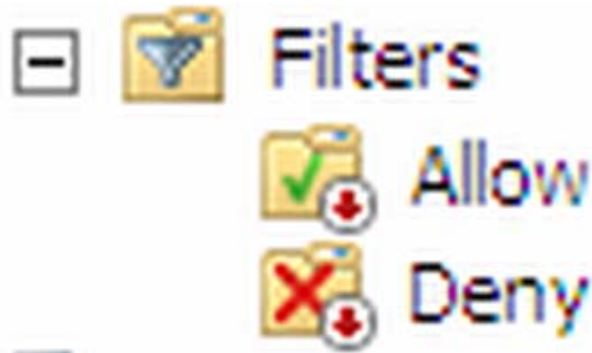
As with Server 2008, Microsoft classifies Server 2008 R2's DHCP capability as a "role" rather than a "feature." When opened, a typical R2 DHCP snap-in looks like this:

Block Bad Guys With Windows 2008 R2 New DHCP MAC Address Filtering Tool

Steven Bink



The top part should look familiar to anyone who's worked with DHCP since Windows 2000, but look to the bottom and note the folder "Filters" and its two sub-folders, "Allow" and "Deny." Look closer and you'll see this:



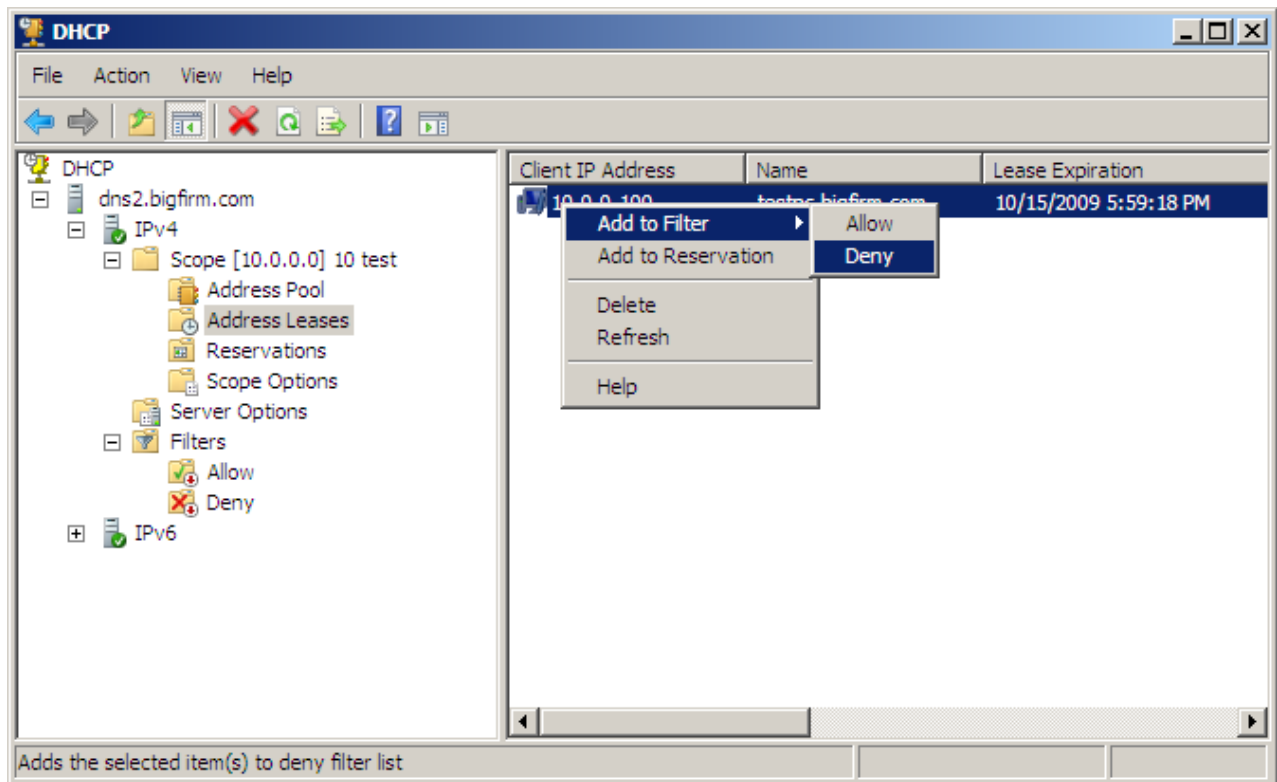
As you can see, each folder has a red downward-pointing arrow, showing that an out-of-the-box R2 DHCP server has the option to add allow or deny filters, but they're off by default.

Denying a Single MAC Address

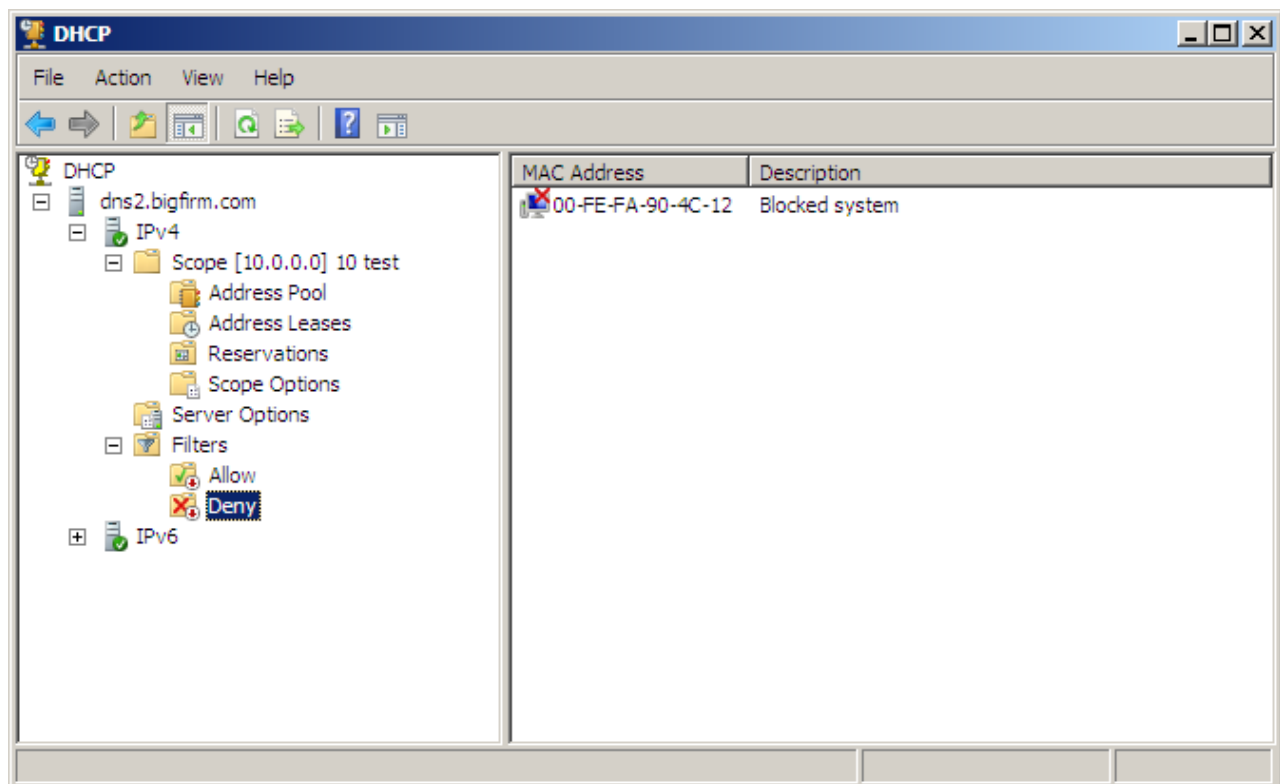
You can see from the first figure that we've got a system that this DHCP server has given an address lease, a system named "testpc.bigfirm.com," and that its MAC address is 00-0C-29-FE-E4-60. Just to demonstrate the simplest possible case of MAC filtering in DHCP, let's block that system from ever getting an IP address from this DHCP server again. To deny 00-0C-29-FE-E4-60 from getting an IP address, right-click the testpc's entry in the "Address Leases" folder, then choose Add to Filter / Deny, as you see in the following figure:

Block Bad Guys With Windows 2008 R2 New DHCP MAC Address Filtering Tool

Steven Bink



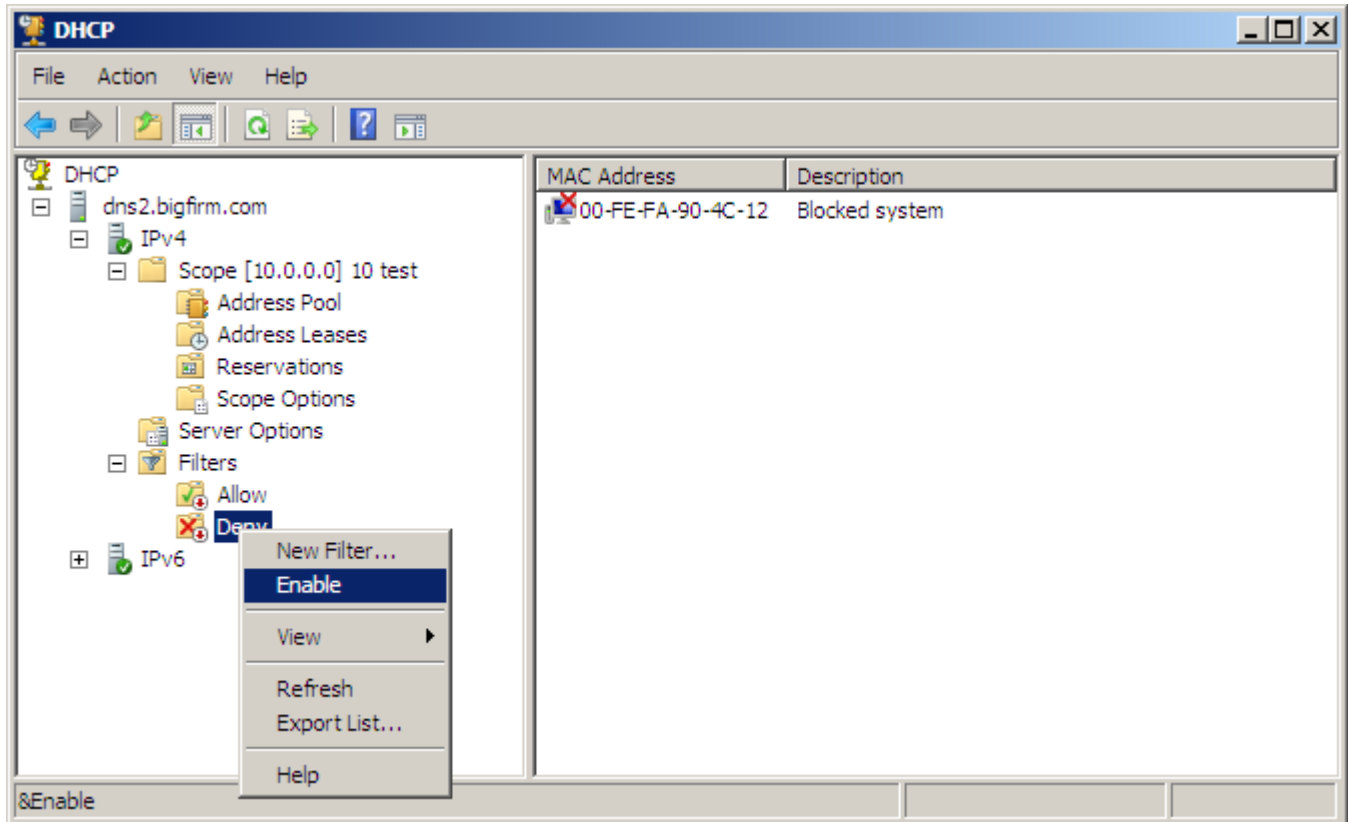
At this point, the "Deny" folder has a rule in it, as you can see by opening the Filters / Deny folder:



Block Bad Guys With Windows 2008 R2 New DHCP MAC Address Filtering Tool

Steven Bink

To enable the deny rule, right-click the "Deny" folder and choose "Enable," like so:



If you had more than one existing lease that you wanted to add to the "deny" filter (or, for that matter, the "allow" filter) then you could also multi-select or block-select any number of existing leases, right-click and then deny (or allow) them en masse.

From this point on, the NIC with that MAC address can't get a DHCP address lease from this server. Note that this doesn't cause the DHCP server to somehow reach out and take the IP address away from the client -- it just causes the DHCP server to deny any future requests from the client. But what happens between now and when testpc's lease expires? Here's what I've seen when testing, using a Windows 7 system for "testpc:"

- If testpc automatically tries to renew its lease, that request would be denied, but testpc would keep using the lease for the next six days, at which time the lease would expire and testpc would stop using that IP address, leaving it without an IP address.
- If an administrator at testpc typed ipconfig /renew to request a renewal, then again the request would be denied, but, again, testpc would keep the IP address for another six days, and thereafter go without.
- If, however, someone rebooted testpc, then when it asked for an IP lease (as it always does upon startup if it doesn't have a static IP address already), then that request would be denied, and testpc would not use its remaining six days' worth of address lease -- it would go "addressless" immediately. (Again, I've only tested Windows 7 DHCP client behavior -- an XP or Vista box may behave differently in terms of dealing with its last six days of having a lease that it cannot renew.)

Block Bad Guys With Windows 2008 R2 New DHCP MAC Address Filtering Tool

Steven Bink

Allowing MAC Addresses to Get DHCP IP Leases: Whitelisting DHCP

So far, we've blocked a particular PC or, more accurately, a particular NIC from getting a DHCP address lease. Now let's look at allowing a particular NIC to get a DHCP address lease.

As you've seen, the default configuration for an R2 DHCP server is to welcome all comers, which means that explicitly saying that (for instance) "the NIC with MAC address 00-FE-FA-90-4C-12 should be granted an address lease" seems sort of pointless, because it would get an IP address regardless. But it isn't pointless in every case, because of this important bit of information: once you enable the "allow" filter, then no NIC gets an address unless it's explicitly listed in the "allow" rules. Let me restate that: if you go to an out-of-the-box, default-setup R2 DHCP server, right-click the "Allow" filter in the MMC and choose "enable," then DHCP won't grant any IP address leases to any system until you explicitly add that system to the "Allow" filter.

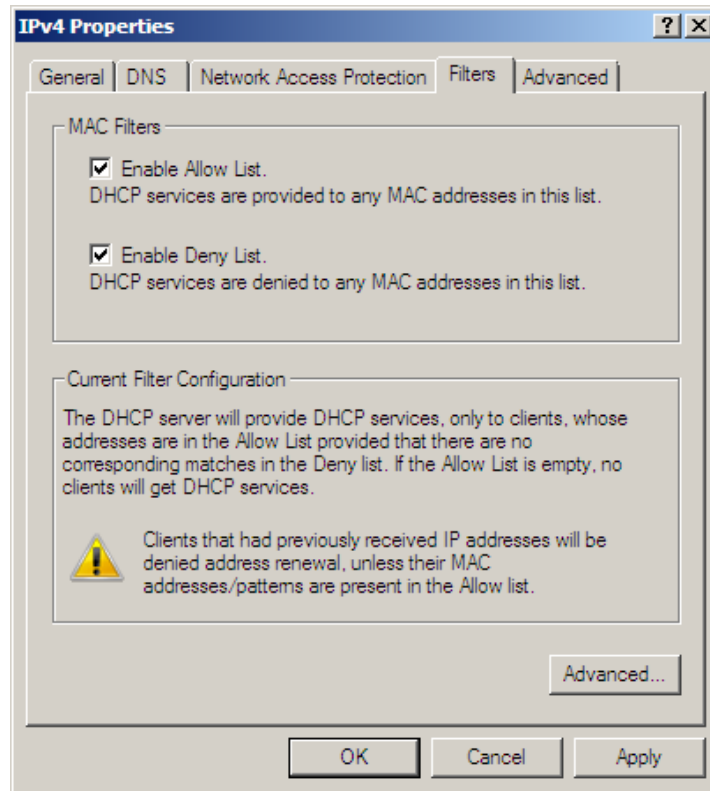
For example, if you re-implemented what we just did with testpc.bigfirm.com and (1) right-clicked the testpc.bigfirm.com lease and chose "Add to filter" / "Allow" and then right-clicked the "Allow" filter folder (rather than the "Deny" filter folder) and chose "Enable," the net effect would be that this DHCP server would only grant address leases to that one NIC. So, to summarize:

- If neither the "Allow" nor "Deny" filters are enabled, then the DHCP server offers addresses to any client.
- If the "Deny" filter is enabled, then the DHCP server offers addresses to any client except the clients whose NICs are named in the "Deny" rules -- DHCP is a blacklist in this case.
- If the "Allow" filter is enabled, then the DHCP server offers addresses to no one except for clients whose NICs are named in the "Allow" rules -- DHCP is a whitelist in this case.
- If both the "Allow" and "Deny" filters are enabled, then DHCP grants addresses only to clients whose NICs are named in the "Allow" rules, except for those NICs who are also named in the "Deny" list -- again, DHCP is a whitelist in this case, but if both "allow" and "deny" rules exist, then "deny" rules beat "allow" rules.

And if you're ever unsure about exactly how the filters you've set up on your DHCP server will behave, just open up the DHCP snap-in, right-click the "IPv4" icon, choose Properties and then the "Filters" tab. It'll look like this example, taken from a system that had both the "Allow" and "Deny" filters enabled:

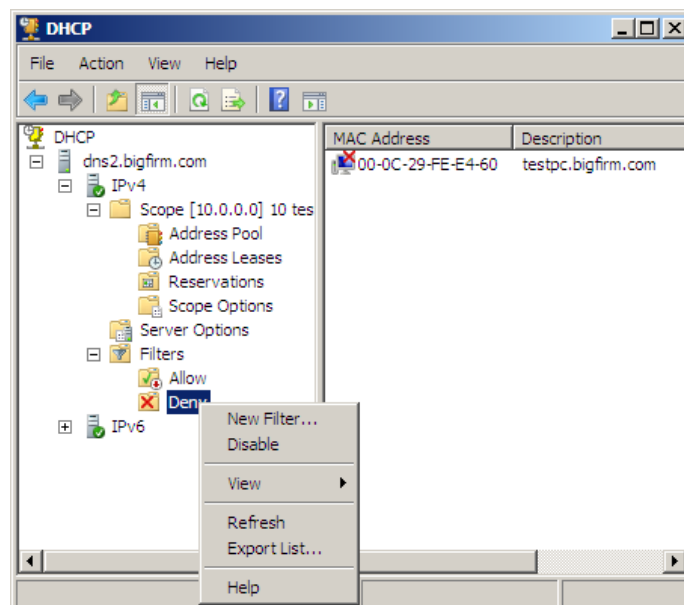
Block Bad Guys With Windows 2008 R2 New DHCP MAC Address Filtering Tool

Steven Bink



Entering One or More MAC Addresses From the GUI and the Command Line

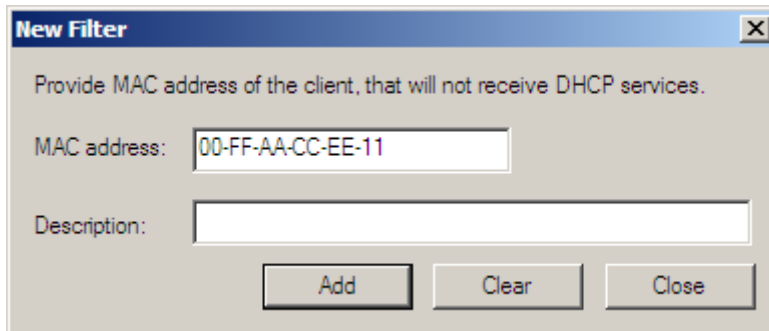
But how to enter the MAC addresses for the filters without wearing out your keyboard? Well, we've already seen that entering MAC addresses that already have leases is dead simple -- select, right-click, Add to Filter, and you're done. But what about entering any MAC? Well, if you'd like to enter a value that isn't already a leased value, you can enter any arbitrary MAC address from the GUI by right-clicking the "Deny" folder or the "Allow" folder and choosing "New Filter...", as you see below (a "deny" example):



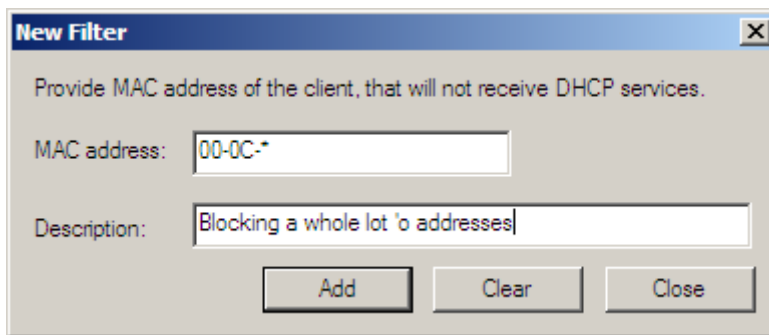
Block Bad Guys With Windows 2008 R2 New DHCP MAC Address Filtering Tool

Steven Bink

When you click "New Filter...", you get a dialog box that lets you fill in a MAC address like the following screen shot:



You can also enter a MAC address with a wild card, as in this screen shot:



That can be useful because Ethernet NICs get MAC addresses assigned in large blocks, enabling you to (for example) block all Intel- or Broadcom-based NICs. Thus, if you knew that all of the NICs on your network use gigabit ethernet NICs based on the same series of Intel chips, and that those chips' MAC addresses all started with "00-1E-37," then you could tell your DHCP server to run as a whitelist (enable the "allow" filter) and then create just one MAC address for it to allow -- "00-1E-37-*" (Yes, it's a quick-and-dirty approach, as zillions of systems have NICs that start with that hex sequence, but there are kilozillions of systems that don't start with that hex sequence, and you can always fine-tune later.)

Note that you can only have one "*" in a MAC address, and DHCP ignores anything after the leftmost "*" -- DHCP would reject "00-1E-37-*-93-*." And remember, you can add all the rules you like, but none of them take effect unless you enable the "deny" and/or "allow" filters, as you saw above.

How Is This Useful?

I've called this a "poor man's quarantine," and by that I mean that if you ran a small network with a Windows DHCP server and wanted to keep casual visitors from getting DHCP addresses on your network then you could do the following:

1. Set up a Server 2008 R2 DHCP server, enabling neither deny or allow rules.
2. Wait a few days until you see in the R2 DHCP snap-in that all of your systems have acquired DHCP leases.

Block Bad Guys With Windows 2008 R2 New DHCP MAC Address Filtering Tool

Steven Bink

3. Select those leases, right-click and choose Add to Filter / Allow, creating "allow" rules for all systems that currently have address leases.
4. Make your DHCP server a whitelist by right-clicking the "Allow" folder under "Filters" in the DHCP snap-in and choose "Enable."

At that point, no one's going to get an IP address from your DHCP server unless they're on that "allow" list. So why do I call this just a "poor man's" quarantine? Well, first of all, it's not a real quarantine, as DHCP doesn't do anything to check to see that a system is malware free. You'd have to figure out and implement Server 2008 R2's Network Access Protection (NAP) quarantine to get a more complete quarantine functionality. (Not a bad idea in some ways, but NAP's not simple to set up.) Second, there's nothing stopping a bad guy from plugging a computer into your network and granting him/herself a static IP address in your network's range and just using that static IP address to access your network. Third, there's also nothing stopping that bad guy from changing his/her NIC's MAC address to match one of the ones on the whitelist. Oh, and finally, maintaining a whitelist means that every time you get a new computer in your network, you'll have to punch in its MAC address by hand.

While all that sounds pretty terrible, the fact of the matter is that most small networks have a sort of built-in security that big ones don't, as they tend to be in one location where everyone knows who's supposed to be in the building -- random people wandering in and plugging their systems into some handy RJ45 jack are likely to be challenged. And besides, while MAC address spoofing and static IP address assignment are both entirely possible (and not all that terribly difficult), the fact is that 99 percent of the random would-be hitchhikers just plain wouldn't have a clue about how to even attempt either feat.

Two other ideas for using MAC filtering would be to use it to

- Block known troublemakers from a network in a simple, quick manner. If they actually go to the trouble to do the static addressing or MAC spoofing thing, then it's much easier to fire 'em, as they've taken extreme and obvious measures to work around the organization's security policy.
- In an academic lab, create a whitelist to slow down uninvited guests and only support your lab computers (which probably all have the same brand and type of NIC, making the wildcard feature useful).

Bulk MAC Import

If right-clicking existing leases or punching in MAC addresses into the GUI aren't for you, the DHCP server team at Microsoft even made it easy for you to feed the DHCP server an ASCII text file of either allowed or denied MAC addresses. To do this, you need an ASCII text file whose first line looks like either "MAC_ACTION = {ALLOW}" or "MAC_ACTION = {DENY}" and then has a list of MAC addresses, one to a line and without any hyphens in them. Anything after an octothorpe ("#") on any line is taken as a comment. So, for example, the following lines would work in a file to be imported:

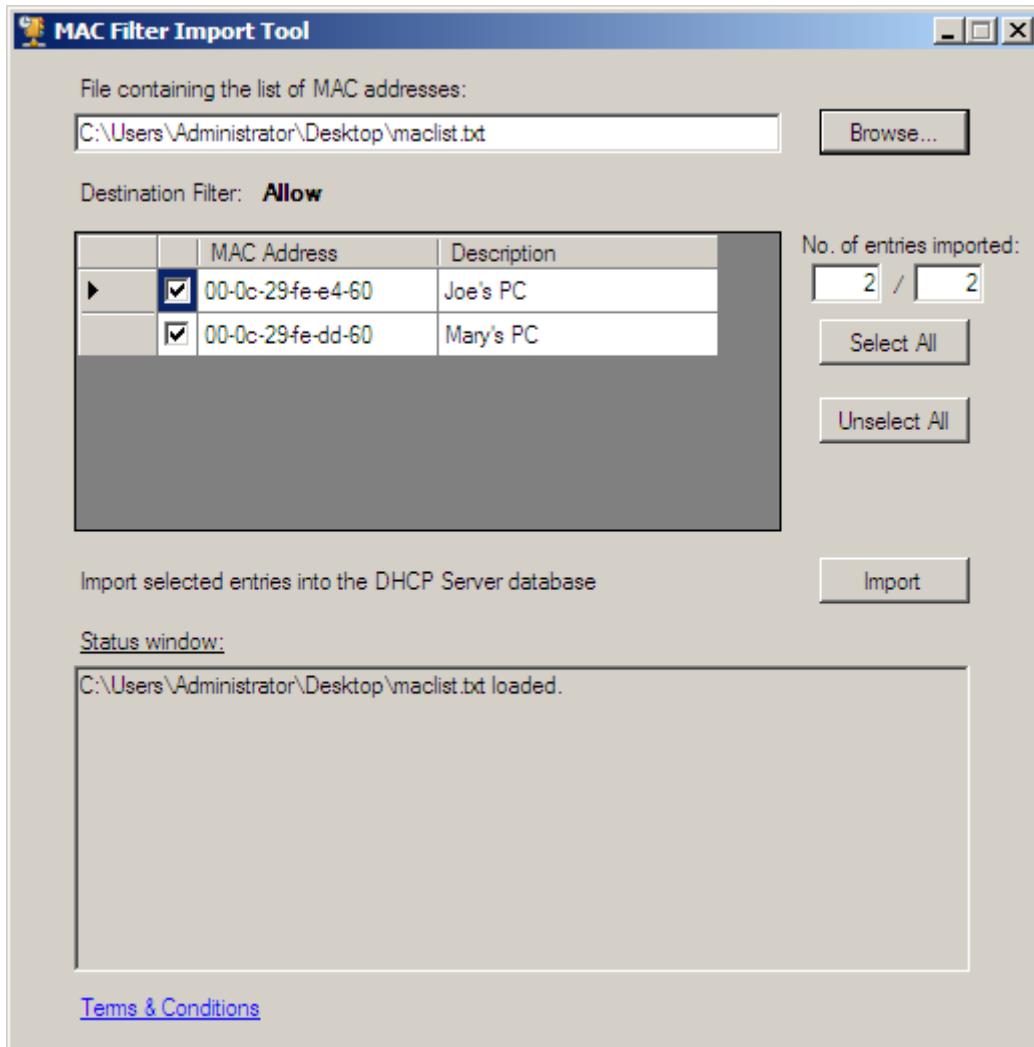
```
#This is a "whitelist" example
MAC_ACTION = {ALLOW}
000c29fee460 # Joe's PC
000c29fedd60 # Mary's PC
```

To import the file, you'll need an extra utility program posted by the DHCP Server team on its blog. Find it by either Googling "MAC filter import tool" or go to the blog post itself at

Block Bad Guys With Windows 2008 R2 New DHCP MAC Address Filtering Tool

Steven Bink

<http://blogs.technet.com/teamdhcp/archive/2009/02/16/mac-filter-import-tool.aspx>. Start the utility up, point it at a file like the one above and you'll see something like this:



Command-Line Support of DHCP MAC Address Filtering

There's some nice stuff here, but it all seems pretty mouse-click-intensive. Can we automate it? Absolutely, with a few netsh commands.

To tell DHCP to enable or disable a filter, use the command

```
netsh dhcp server v4 set filter [enforceallowlist=1|0] [enforcedenylist=1|0]
```

So, for example, to turn on the "allow" filter on an R2 DHCP server, you'd type

```
netsh dhcp server v4 set filter enforceallowlist=1
```

To add a MAC address to the deny or allow filter, use the netsh dhcp server v4 add filter command, which looks like

```
netsh dhcp server v4 add filter allow|deny mac-address ["comment"]
```

Block Bad Guys With Windows 2008 R2 New DHCP MAC Address Filtering Tool

Steven Bink

For example, to add MAC address 00-0c-29-fe-dd-60 to the allow list, you'd type

```
netsh dhcp server v4 add filter allow 00-0c-29-fe-dd-60 "Mary's PC"
```

R2's MAC filtering tool may make your life just a bit easier -- give it a look!