

## RE: DHCP for Simple Security

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2004-04/0062.html>

---

**From:** James McIllece [MS] ([jamesmci\\_at\\_online.microsoft.com](mailto:jamesmci_at_online.microsoft.com))

**Date:** 03/31/04

Date: Wed, 31 Mar 2004 15:39:01 -0800

"=?Utf-8?B?ZnJlZA==?=" <[anonymous@discussions.microsoft.com](mailto:anonymous@discussions.microsoft.com)> wrote in [news:57E39A5C-8293-43C4-BE07-6A0632B156CB@microsoft.com](mailto:news:57E39A5C-8293-43C4-BE07-6A0632B156CB@microsoft.com):

- > *Let me provide more detail on the problem.*
- >
- > *We have many offices. Each office has a LAN. All of our switches were*
- > *acquired over the last 5 years. Most do NOT support 802.1x.*
- >
- > *My concern is not over wireless access. Our culture embodies an open,*
- > *trusting, atmosphere that is occasionally at odds with a secure IT*
- > *infrastructure. (Thus I do not wish to disclose my firms name.) We*
- > *have outside technicians and sales people who entire our facilities*
- > *with LAP top computers. Realistically we cannot stop this practice.*
- > *Occasionally these outsiders will plug into one of our LANs. I believe*
- > *we have been victimized by at least one Worm that attacked our systems*
- > *without using Windows Authentication. (Our firewall would prevent such*
- > *attacks.) As in most medium to large IT environments we use DHCP to*
- > *supply IP addresses to client machines. We could easily update all of*
- > *our clients to have a unique User-Defined Class in IPconfig. If*
- > *Microsoft DHCP server would support IP assignment by User-Defined*
- > *Class we could tighten our security by giving IP access only to*
- > *company owned clients. To facilitate the legitimate sales presentation*
- > *we would add a wireless access router/switch to each of our conference*
- > *rooms. These routers would be connected outside our firewall to allow*
- > *Internet access. I agree that this security enhancement is vulnerable*
- > *to a direct hostile attack. However I believe it sufficient to protect*
- > *against general attacks such as we have seen over the last year. It*
- > *would seem that a DHCP server could easily provide this sort of*
- > *"security". From a legal viewpoint it need not be called security at*
- > *all. The feature would best be descried as simply support of*
- > *sub-netting on a common media through the use of User-Defined Class on*
- > *DHCP servers.*
- >

I understand the need you have for this type of functionality from DHCP, however as far as I know there is currently no DHCP product that supplies

this functionality. DHCP is by definition an unauthenticated protocol.

As I mentioned previously, the most secure way to manage network access is to use Internet Authentication Service (which is MSFT RADIUS), remote access policy in IAS, and 802.1X. Those technologies will give you the network access control functionality you desire. With this technology, you could create an Internet access VLAN for guest access, so that unauthenticated users connecting with wireless devices are automatically placed on a VLAN that has no access to company resources but does have access to the Internet. In this scenario, your routers could live inside of your firewall, which would add security. (The APs would be configured as RADIUS clients to the IAS server, so you could manage network access by configuring policies only on the IAS server, rather than at each AP individually.)

In Windows Server 2003 DHCP, user classes allow you to specify that members of the class are supplied with additional DHCP options, or with options that have different values than those received by computers that are not members of the user class.

*>From the DHCP Help (just in case you want more info on user classes):*

User classes allow DHCP clients to differentiate themselves by specifying a User Class option. When available for client use, this option includes a user-determined class ID that can help to group clients of similar configuration needs within a scope. For example, you might support users and computers with mobile computing needs by configuring a user class at the DHCP server and setting the related class ID at the client computers.

A user class is useful when you need to keep separate options that cover the special needs of identifying client computers, such as providing a shorter lease time for portable computers that move frequently or use remote access often. In this example, you could configure the DHCP server to distribute different options that are specific to the needs of clients.

--

James McIllece, Microsoft

Please do not send email directly to this alias. This is my online account name for newsgroup participation only.

This posting is provided "AS IS" with no warranties, and confers no rights.