



Service Managed Gateway™

Limiting Network Access to Approved Users and Devices

Issue 1.1
Date 14 August 2007

1	About this document	3
1.1	Scope	3
1.2	Readership	3
1.3	More information.....	3
1.4	Terminology	3
2	Introduction	4
2.1	What is a MAC address?	4
2.2	How MAC address filtering works	4
3	Managing MAC address filters.....	5
3.1	Creating a MAC address filter	5
3.2	Modifying a MAC address filter	6
3.3	Deleting a MAC address filter	6
3.4	Troubleshooting MAC address filters	7
3.4.1	Confirm that a filter matches network traffic.....	7
3.4.2	Confirm that packets from a device reach the SMG.....	7
4	Examples of MAC address filtering	9
4.1	Allowing only some devices to access the network	9
4.2	Preventing some devices from accessing the network	9
4.3	Permitting or block a class of devices.....	9

© 2007 Virtual Access (Irl) Ltd. This material is protected by copyright. No part of this material may be reproduced, distributed, or altered without the written consent of Virtual Access. All rights reserved. All trademarks, service marks, registered trademarks and registered service marks are the property of their respective owners. Virtual Access is an ISO 9001 certified company.



1 About this document

1.1 Scope

This document:

- explains how to create, modify, delete, and troubleshoot MAC address filters, and
- gives examples of how to use MAC address filters.

1.2 Readership

This document is for engineers who have previous experience configuring and managing Service Managed Gateways (SMGs).

1.3 More information

For more information, read the MAC address pages in the Expert Web Full Reference Documentation in the Service Managed Gateway documentation, version 8.10 or later.

For information about port access control, read **Managing Port Access on the Service Managed Gateway**.

1.4 Terminology

MAC address A unique identifier that is programmed into a device when the device is manufactured.

2 Introduction

To improve security, it is sometimes desirable to limit access to the wide area network to a set of approved users or devices. Occasionally, it might be necessary to prevent particular devices from accessing the network. MAC address filters allow you to control network access based on the network MAC address of a device.

The GW series of Service Managed Gateways (SMGs) supports up to 100 filter entries. The TW and GL series of SMGs supports 5 filter entries.

MAC address filtering is configured in the Expert Web section of the Service Managed Gateway web.

2.1 What is a MAC address?

A MAC address uniquely identifies a device on a local area network (LAN). The MAC address is programmed into a device when the device is manufactured.

There are 12 hexadecimal digits in a MAC address. Digits 1-6 of a MAC address are the vendor ID. Digits 7-12 of a MAC address are a unique device ID.

2.2 How MAC address filtering works

When a local Ethernet port receives a packet, the packet is checked against the list of defined MAC address filters, from the top of the list to the bottom of the filter list.

The first filter that matches the packet determines whether or not the packet is permitted. If no filter matches, then the packet is either permitted by default or authenticated if port access control is enabled. For information about port access control, read **Managing Port Access on the Service Managed Gateway**.

3 Managing MAC address filters

3.1 Creating a MAC address filter

1. On the SMG home page, click **Advanced**.
2. In the Advanced menu, click **Expert View**.
3. In the Expert View, select **advanced configuration -> system -> filters-> mac address filters**.
4. Click **add** in the row of the filter that you want to create. Figure 1 shows the MAC Address Filters Entry page.

The screenshot shows the 'MAC Address Filters Entry 1' page. It contains the following fields and values:

- Configured:** no (dropdown)
- Name:** none (text input)
- Action:** pass (dropdown)
- Interface:** any (dropdown)
- MAC Address:** 000000000000 (text input)
- MAC Address Mask:** FFFFFFFF (text input)

At the bottom, there are 'Update' and 'Delete' buttons.

Figure 1: The default values on the MAC Address Filters Entry page

5. In the MAC Address Filters Entry page, set the configuration parameters that are outlined in Table 1 and click **Update**.

The filter takes effect immediately. You do not have to reload the SMG.

Field Name	Explanation
Configured	Select Yes to enable the filter.
Name	Type a descriptive name that will help you remember what the filter does. The name does not affect how the filter works.
Action	The Action field determines what action to take when a packet matches the filter. Pass allows a packet through. Block discards the packet immediately. Authenticate allows the packet to pass. The device must also successfully complete port authentication if access control is enabled.

Table 1: Fields and values for MAC address filter configuration (continued...)

Field Name	Explanation
Interface	The Interface field controls which external interfaces the filter will apply to. Eth-0 applies the filter to packets that arrive on the Eth-0 interface. Eth-1 applies the filter to packets that arrive on the Eth-1 interface. Eth-2 applies the filter to packets that arrive on the Eth-2 interface. Eth-3 applies the filter to packets that arrive on the Eth-3 interface. lan applies the filter to all packets that arrive on Ethernet ports that are not configured as WAN interfaces. wan applies the filter to all packets that arrive on Ethernet ports that are configured as WAN interfaces. Any applies the filter to any Ethernet port.
MAC Address	Type the MAC address of the device or devices you want to match. The address must be 12 hexadecimal digits. Type 0 to match all devices.
MAC Address Mask	Type a mask to filter the MAC addresses. The mask must be 12 hexadecimal digits. Type 0 to match all devices. To match only the device that is defined in the MAC Address field, use the default MAC address mask, FFFFFFFF.

Table 1 continued: Fields and values for MAC address filter configuration

3.2 Modifying a MAC address filter

1. On the SMG home page, click **Advanced**.
2. In the Advanced menu, click **Expert View**.
3. In the Expert View, select **advanced configuration -> system -> filters-> mac address filters**.
4. Click **modify/delete** in the row of the filter that you want to modify. Figure 1 shows the MAC Address Filters Entry page.
5. In the MAC Address Filters Entry page, modify the configuration parameters and click **Update**.

The changes take effect immediately. You do not have to reload the SMG.

3.3 Deleting a MAC address filter

1. On the SMG home page, click **Advanced**.
2. In the Advanced menu, click **Expert View**.
3. In the Expert View, select **advanced configuration -> system -> filters-> mac address filters**.
4. Click **modify/delete** in the row of the filter that you want to delete. Figure 1 shows the MAC Address Filters Entry page.
5. In the MAC Address Filters Entry page, click **Delete**.

The changes take effect immediately. You do not have to reload the SMG.

3.4 Troubleshooting MAC address filters

3.4.1 Confirm that a filter matches network traffic

1. On the SMG home page, click **Advanced**.
2. In the Advanced menu, click **Expert View**.
3. In the Expert View:
 1. Click **Operations** in the button menu at the top of the web interface.
 2. Select **performance** -> **filter stats**-> **mac address filters**.

Figure 2 shows the Active MAC address hits page. The page lists all MAC address filters that are active and the number of packets that the filters have matched.

4. If a filter does not match network traffic, follow the procedure in section 3.2 to correct the problem.

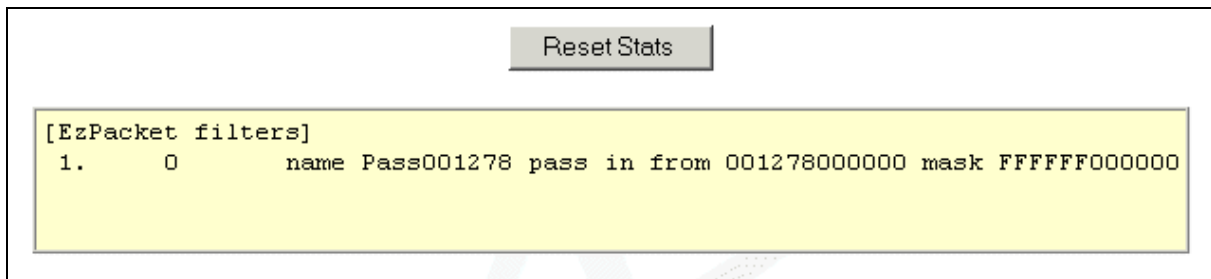


Figure 2: The Active MAC Address Hits page.

3.4.2 Confirm that packets from a device reach the SMG

1. On the SMG home page, click **Advanced**.
2. In the Advanced menu, click **Expert View**.
3. In the Expert View:
 1. Click **Operations** in the button menu at the top of the web interface.
 2. Select **performance** -> **filter stats**-> **mac address filter cache**.

Figure 3 shows the Active MAC address hits page. The page shows the device addresses that were seen on each port. The cache is flushed:

- when the configuration of the MAC address filters changes, or
- when the you click **Clear Cache** on the MAC address filter cache page.

The age is refreshed when the port receives another packet from the same MAC address.

4. If packets are not correctly passed, blocked, or sent for authentication, follow the procedure in section 3.2 to correct the problem.

View active MAC filter cache for All interfaces Refresh Clear Cache					
Port	Hits	MAC address	Last seen IP	Status	Age
eth-1	4	00-14-22-18-55-00	10.1.10.240	Pass	20 seconds
eth-1	1	00-14-22-18-4f-06	10.1.10.241	Pass	11 seconds
eth-1	1	00-04-76-29-67-06	10.1.10.212	Pass	3 minutes 17 seconds
eth-1	1	00-11-43-be-88-07	10.1.10.92	Pass	3 minutes 13 seconds
eth-1	2	00-04-76-29-66-0a	10.1.1.12	Pass	1 minute 37 seconds

Figure 3: The MAC Address Filter Cache page

4 Examples of MAC address filtering

4.1 Allowing only some devices to access the network

You can allow some devices to access the network and prevent most devices from accessing the network. For each MAC address that you allow to access the network, you create a filter and set the filter action to PASS. Then you create a catch-all filter at the end of the filter table to match all other traffic, and you set the filter action to BLOCK.

4.2 Preventing some devices from accessing the network

You can deny access to the network to some devices and allow most devices to access the network. For each MAC address that you want to deny access to, you create a filter and set the filter action to BLOCK. Any packet that does not match the MAC address in the filter passes through to the network.

4.3 Permitting or block a class of devices

Suppose that port authentication is enabled on the SMG. A certain class of Voice-over-IP (VoIP) phone that your company uses does not support authentication. So the VoIP phones are allowed unrestricted access to the network. One vendor provides all the VoIP phones, and the phones have MAC addresses in the form 001278xxxxxx.

Define a MAC address filter with the parameters that are shown in Figure 4.

Configured	yes
Name	VoIPAllowed
Action	pass
Interface	any
MAC Address	001278000000
MAC Address Mask	FFFFFF000000
<input type="button" value="Update"/> <input type="button" value="Delete"/>	

Figure 4: An example of parameters to allow a class of device

Traffic from devices with MAC addresses that begin 001278 is passed. All other traffic will not match the filter and must undergo normal port authentication.

Note: This example increases security, but it is possible to bypass the filter by changing the network address of a blocked device. Only use this technique along with additional security measures.