



## Securing Virtual Switch Ports

As with physical network adapters, a virtual network adapter can send frames that appear to be from a different machine or impersonate another machine so that it is able to receive network frames intended for that machine. Also, like physical network adapters, a virtual network adapter can be configured such that it receives frames targeted for other machines.

When you create a virtual switch for your network, you add port groups to impose a policy configuration for the virtual machines, storage systems, and so forth attached to the switch. You create virtual switches through the VI Client.

As part of adding a port or port group to a virtual switch, the VI Client configures a security profile for the port. You can use this security profile to ensure that ESX Server prevents the guest operating systems for its virtual machines from impersonating other machines on the network. This security feature is implemented so that the guest operating system responsible for the impersonation does not detect that the impersonation has been prevented.

The security profile determines how strongly you enforce protection against impersonation and interception attacks on virtual machines. To correctly use the settings in the security profile, you need to understand the basics of how virtual network adapters control transmissions and how attacks are staged at this level.

Each virtual network adapter has its own MAC address assigned when the adapter is created. This address is called the initial MAC address. Although the initial MAC address can be reconfigured from outside the guest operating system, it cannot be changed by the guest operating system. In addition, each adapter has an effective MAC address that filters out incoming network traffic with a destination MAC address different from the effective MAC address. The guest operating system is responsible for setting the effective MAC address and typically matches the effective MAC address to the initial MAC address.

When sending packets, an operating system typically places its own network adapter's effective MAC address in the source MAC address field of the Ethernet frame. It also places the MAC address for the receiving network adapter in the destination MAC address field. The receiving adapter accepts packets only when the destination MAC address in the packet matches its own effective MAC address.

Upon creation, a network adapter's effective MAC address and initial MAC address are the same. The virtual machine's operating system can alter the effective MAC address to another value at any time. If an operating system changes the effective MAC address, its network adapter then receives network traffic destined for the new MAC address. The operating system can send frames with an impersonated source MAC address at any time. Thus, an operating system can stage malicious attacks on the devices in a network by impersonating a network adapter authorized by the receiving network.

You can use virtual switch security profiles on ESX Server hosts protect against this type of attack by setting three options:

- **MAC address changes** – By default, this option is set to **Accept**, meaning that the ESX Server host accepts requests to change the effective MAC address to other than the initial MAC address. The **MAC Address Changes** option setting affects traffic received by a virtual machine.

To protect against MAC impersonation, you can set this option to **Reject**. If you do, the ESX Server host does not honor requests to change the effective MAC address to anything other than the initial MAC address. Instead, the port that the virtual adapter used to send the request is disabled. As a result, the virtual adapter does not receive any more frames until it changes the effective MAC address to match the initial MAC address. The guest operating system does not detect that the MAC address change has not been honored.

**Note** In some situations, you might have a legitimate need for more than one adapter to have the same MAC address on a network — for example, if you are using Microsoft Network Load Balancing in unicast mode. Note that when Microsoft Network Load Balancing is used in the standard multicast mode, adapters do not share MAC addresses.

- **Forged transmissions** – By default, this option is set to **Accept**, meaning the ESX Server host does not compare source and effective MAC addresses. The **Forged Trasmits** option setting affects traffic transmitted from a virtual machine.

To protect against MAC impersonation, you can set this option to **Reject**. If you do, the ESX Server host compares the source MAC address being transmitted by the operating system with the effective MAC address for its adapter to see if they match. If the addresses don't match, ESX Server drops the packet.

The guest operating system does not detect that its virtual network adapter cannot send packets using the impersonated MAC address. The ESX Server host intercepts any packets with impersonated addresses before they are delivered, and the guest operating system might assume that the packets have been dropped.

- **Promiscuous mode operation** – By default, this option is set to **Reject**, meaning that the virtual network adapter cannot operate in promiscuous mode. Promiscuous mode eliminates any reception filtering that the virtual network adapter would perform so that very frame that the guest operating system receives all traffic observed on the wire.

While promiscuous mode can be useful for tracking network activity, it is an insecure mode of operation because any adapter in promiscuous mode had access to the packets regardless of whether some of the packets should be received only by a particular network adapter. This means that an administrator or root user within a virtual machine can potentially view traffic destined for other guest or host operating systems.

**Note** In some situations, you might have a legitimate need to configure a virtual switch to operate in promiscuous mode — for example, if you are running network intrusion detection software or a packet sniffer.

If you need to change any of these default settings for a port, you must modify the security profile by editing virtual switch settings in the VI Client. For information on editing these settings, see [Virtual Switch Policies](#).

---

[VMware Infrastructure 3 Online Library](#) | [Send feedback](#) | [Technical Support](#) | Copyright © 2006–2009 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.