

# 3Com® SuperStack® 3 Switch 4400: Securing Your Network

## APPLICATION BRIEF

### The Problem

It has long been acknowledged that there can be security issues with Simple Network Management Protocol (SNMP)—the protocol of choice for managing network solutions. A recent independent investigation\* identified specific vulnerabilities. How can organiza-

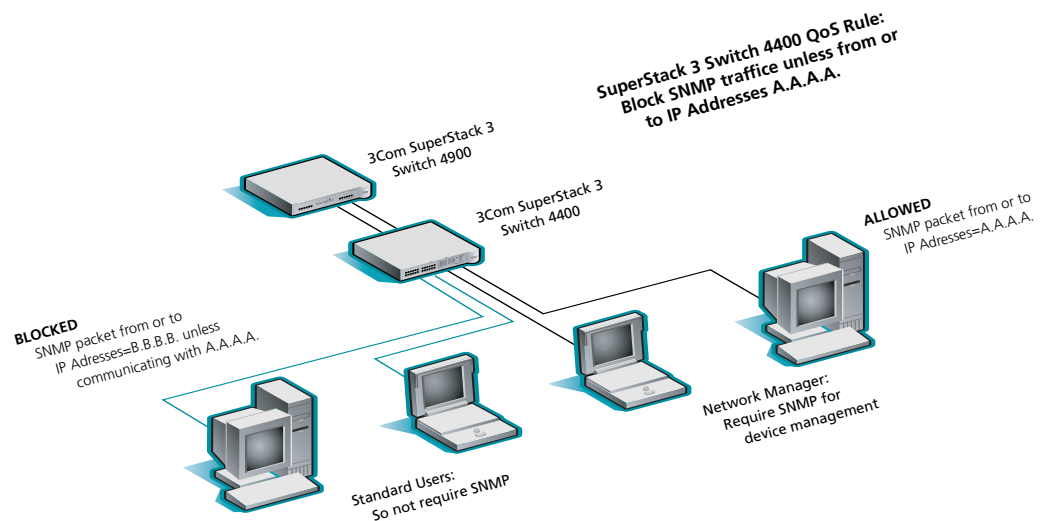
tions protect themselves from the inherent security weaknesses of SNMP—especially from the threat of Denial of Service (DoS) attacks, unauthorized or rogue stations using SNMP to disrupt network operation?

### The Solution

There are several security features designed into the 3Com® SuperStack® 3 4400 Switch family to ensure a secure management interface.

Using the Trusted IP feature of the 3Com SuperStack 3 Switch 4400 family, a range of IP addresses that are allowed management access to the unit can be defined. SNMP traffic coming from an unknown or unauthorized station will be rejected, while still allowing full management access from authorized management stations. Furthermore, the management interface can be moved from the default VLAN to a management VLAN to offer even higher security. This can physically separate the network users' traffic from the management traffic.

Alternatively, using the enhanced multilayer traffic management capabilities\*\* of the 3Com SuperStack 3 Switch 4400 family, a Switch 4400 is able to identify SNMP traffic and block it if it comes from unknown and unauthorized stations on the network. Authorized SNMP traffic, in contrast, flows freely. The result of this management function is a more secure network environment, as unauthorized SNMP cannot reach the core of the network. The SuperStack 3 Switch 4400 can identify traffic using a range of criteria—including application, protocol, and IP address—and block or prioritize it as needed.



The SNMP protocol's unique UDP port number (161) allows the Switch 4400 to identify management traffic. Knowing the IP addresses of the "authorized" SNMP management stations, the network operator can easily configure the SuperStack 3 Switch 4400 to block SNMP traffic if it is not

coming from or destined to the authorized stations.

With these simple configurations, the Switch 4400 can block traffic from any rogue stations using SNMP for unauthorized purposes—preventing network disruption.

#### Want to know more?

For further information on the security solution available with enhanced 3Com SuperStack 3 Switch 4400 devices, please refer to this entry in 3Com Knowledgebase:

<http://knowledgebase.3com.com>, Solution ID: 2.0.97025834.3609642

\* CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP), original released February 12, 2002 (<http://www.cert.org/advisories/CA-2002-03.html>)

\*\* standard with the SuperStack 3 Switch 4400 24-port (3C17203), 48-port (3C17204), 24-port PWR (3C17205) or 24-port FX (3C17210) models



3Com Corporation, Corporate Headquarters, 350 Campus Drive, Marlborough, MA 01752-3064

To learn more about 3Com solutions, visit [www.3com.com](http://www.3com.com). 3Com is publicly traded on NASDAQ under the symbol COMS.

Copyright © 2004 3Com Corporation. All rights reserved. 3Com, the 3Com logo, and SuperStack are registered trademarks of 3Com Corporation. Exercise Choice is a trademark of 3Com Corporation. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, 3Com does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.