



TECHNICAL BRIEF



3Com[®] NJ200 Network Jack Management Feature:

Configuring SNMP Traps

CONTENTS

What are SNMP Traps?2
 Benefits.....2
 Configuration and Setup2
 Using SNMP Traps with
 3Com Network Supervisor.....3
 Configuring Trap Destination.....3
 Configuring 3Com
 Network Supervisor3
 Using SNMP Traps with
 Third-Party Network
 Management Platforms4
 Configuring Trap Destination.....4
 Configuring the Network
 Management Platform.....5
 Business Application5
 For More Information6

Configure “Get” and “Set” community strings to match your network management platform and select which SNMP traps will be monitored by the NJ200 Network Jack.

What are SNMP Traps?

SNMP traps allow managers to monitor network devices and isolate connectivity problems through a central management platform, such as 3Com® Network Supervisor or HP OpenView. Using SNMP agents to gather information from connected devices, 3Com NJ200 Network Jacks collect or “trap” this data and forward it to a RMON-compliant network management server.

Benefits

When SNMP traps and alerts are enabled on NJ200 Network Jacks, IT staff can view and display devices, links, and activity across the network. From a single control console, changes and events can be proactively monitored and addressed before they become more serious problems. Network devices can be easily located before making a site visit to avoid wasted trips and time. These capabilities are essential for reducing downtime, optimizing network availability, improving user productivity, and freeing IT staff to focus on higher-value management activities.

Specifically, SNMP traps help IT staff:

- Proactively monitor changes to NJ200 Network Jack–connected devices, often delivering information before problems occur
- Reduce network downtime by quickly identifying dropped device connections, isolating defective cables, and determining NIC configurations
- Lighten network overhead and management system processing

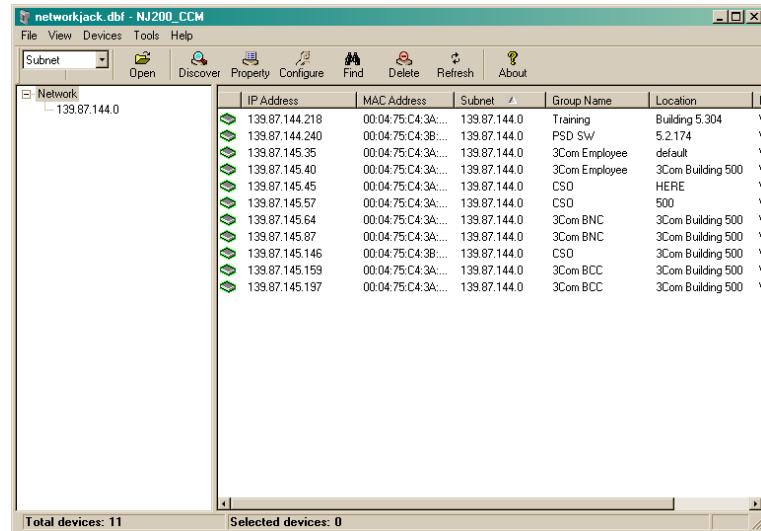
Configuration and Setup


3Com NJ200 Network Jacks come bundled with 3Com Central Configuration Manager. Designed for in-depth configuration and remote management of these devices, this tool can be installed on a standalone PC or in the same system as the network management platform. NJ200 switches use SNMP Version 1 (RFC-1157) and support four standard SNMP traps: link up, link down, cold start, and authentication failure.

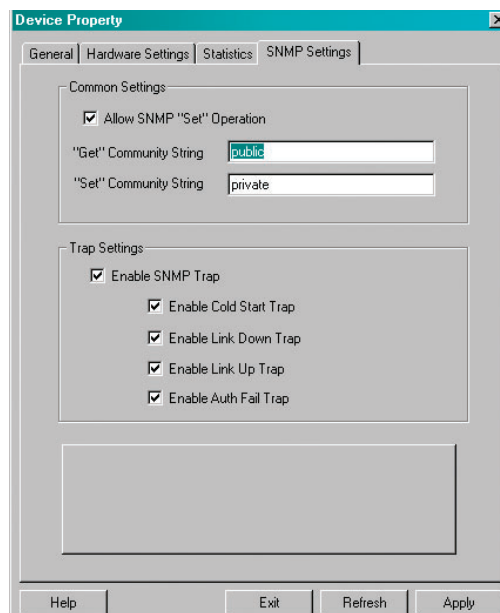
To enable and configure SNMP traps on an NJ200 Network Jack:

1. Open Central **Configuration Manager** and using either the IP or MAC address, locate the NJ200 Network Jack to be configured.

The 3Com Central Configuration Manager GUI enables point-and-click remote administration of NJ200 Network Jacks.



2. If the device is not on the initial list, begin a new discover process by clicking on the **Discovery** icon from the toolbar. 
3. Once the device has been located, select **Device Property** to open a window with four tabs. Clicking on the **SNMP Settings** tab opens a window that looks like this:



4. Under **Common Setting**, make sure the **All SNMP Set** box is checked.
5. Fill in the “**Get**” and “**Set**” **Community Strings** fields to match the community strings configured in the enterprise network management platform.

IMPORTANT! The default community strings are “public” and “private” but must be changed to match network management strings.

6. Under **Trap Settings** make sure the **Enable SNMP Trap** box is checked, and enable any or all of the following event traps: **Cold Start, Link Down, Link Up, Authentication Failure**.

Note: The **Enable SNMP Trap** box must be checked in order for network event traps to be monitored by network management.

Using SNMP Traps with 3Com Network Supervisor

Configuring Trap Destination

An easy-to-use Network Discovery Wizard guides you through the process of discovering and mapping networked devices, including NJ200 Network Jack. The graphical interface makes it easy to configure SNMP traps and alerts, monitor events, locate devices, and troubleshoot problems.

When NJ200 Network Jack are discovered, 3Com Network Supervisor automatically writes the trap destination (IP address of the management system) to them. This eliminates the need to build a “Trap Destination Table” via a Management Information Database (MIB) browser. (see *Configuring SNMP Traps with a Third-Party Management Platform* section below).

Configuring 3Com Network Supervisor

The traps are attached to an item on the network map and are triggered when an event occurs. The following event alerts can be delivered via e-mail, sound, pop-up message, or by launching an application:

- **Cold Start** indicates that the switch is down or disconnected
- **Link Down** indicates a problem in the cable or NIC
- **Link Up** indicates that the cable and NIC are functioning properly

Note: 3Com Network Supervisor does not support Authentication Failure traps or alerts.

With SNMP traps enabled and configured, IT staff can use 3Com Network Supervisor to locate and identify network problems in three simple, point-and-click steps:

1. Receive an event alert.
2. Find the event in the Event List.
3. Using Event List link, locate the problem device in the network management map.

Using SNMP Traps with Third-Party Network Management Platforms

Configuring Trap Destination

Most third-party management platforms, such as HP OpenView, cannot automatically write the trap destination (IP address of management system) to NJ200 Network Jack during discovery. Although the switches support MIB-2, RMON, and SNMP agents, they cannot be configured from 3Com Central Configuration Manager to communicate with the network management platform (IP address of network management system). Instead, the trap destination must be configured through a standard MIB browser.

The following example helps illustrate how to write the trap destination to an NJ200 Network Jack Switch using a standard MIB-2 browser. In this example the receiving device uses IP address **192.168.1.1**:

IMPORTANT!: Please note that this procedure varies for different network management platforms. To properly configure the trap destination for your particular network management platform, please consult the software documentation for specific instructions.

1. Open the “*TrapDestStatus*” command line. Most often, this will can be found under ***MIB-2 _ RMON _ ProbeConfig _ TrapDestTable _ TrapDestStatus***.
2. In dot notation, **1.3.6.1.2.1.16.19.13.1.6** represents *TrapDestStatus*. It may be indexed with “1” and in that case is **1.3.6.1.2.1.16.19.13.1.6.1**.
3. Create a row by setting *TrapDestStatus* value to 5.
4. Configure the *TrapDestAddress* (IP address of network management system) by setting # **0xC0 0xA8 0x01 0x00 0xA2** to **1.3.6.1.2.1.16.19.13.1.4.1**, where 1.3.6.1.2.1.16.19.13.1.4.1 represents the default address indexed with “1”.
5. The first four bytes of the *TrapDestAddress*, “**0xC0 0xA8 0x01 0x01**”, should be the IP address of the network management system, or trap receiver.

Note: Insert a space, not a dot “.”, between the first four bytes.

6. The last two bytes indicate which UDP port is used to send out traps.

Note: Do not use any number other than **162 (0xA2)** for the last byte. NJ200 Network Jacks can only trap SNMP information through UDP port 162 (0xA2).

7. Enable the trap destination by setting 1 to *TrapDestStatus* object, which in this case is **1.3.6.1.2.1.16.19.13.1.6.1**.
8. The NJ200 Network Jack is ready to send traps to the network management system with the IP address 192.168.1.1.
9. Repeat these steps if additional trap destinations are needed. NJ200 Network Jack can support up to four different trap destinations.

Configuring the Network Management Platform

After the NJ200 Network Jacks have been properly configured for SNMP traps and trap destination tables, the network management platform needs to be configured for SNMP traps and event alerts. Obviously, these procedures will vary depending on the network management application. For detailed information, please consult the manufacturer's installation and/or technical documentation.

Here is a summary of the overall setup process:

1. Configure and enable SNMP traps using 3Com Central Configuration Manager.
2. Configure trap destination table for each NJ200 Network Jack using any standard MIB browser.
3. Launch the third-party network management platform application and complete network discovery to map all devices.
4. Configure notification types and delivery methods.

Business Application

The ability to remotely monitor for, diagnose, and pinpoint the cause of network problems is a tremendous timesaver for IT staff. The following scenario, while fictional, demonstrates how using SNMP traps helps solve real-world problems and deliver significant time and cost savings.

The IT staff gets a trouble ticket stating that, "The network is down." They could spend hours checking servers, switches, routers, gateways, operating systems, and applications, and calling their ISP or other service providers—only to find out that the problem isn't the network.

Or, they can check for event alerts on their 3Com Network Supervisor management console, pinpoint the real problem to a failed NIC connected to a 3Com NJ200 Network Jack in Room 315/Building A in Engineering, replace the faulty network link, and have the user back online in minutes.

Better yet, with proactive monitoring, IT staff can detect an underperforming NIC and replace it during the user's lunch break, before it fails completely—avoiding any disruption at all to user productivity or business operations.

For More Information

3Com NJ200 Network Jacks work in almost any network environment—including small-office or enterprise businesses, government offices, dormitories, hospitals, school classrooms, universities, laboratories, public kiosks, conference rooms, and shared office spaces.

For more information on how these managed “in the wall” switches can resolve common networking problems and significantly lower IT costs, please visit www.3com.com/networkjack.



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

To learn more about 3Com solutions, visit www.3com.com. 3Com is publicly traded on NASDAQ under the symbol COMS.

Copyright © 2003 3Com Corporation. All rights reserved. 3Com and the 3Com logo are registered trademarks of 3Com Corporation. Possible made practical 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.

XXXXXX-001 09/03