



TECHNICAL BRIEF



3Com® NJ200 Network Jack Management Feature:

Virtual LANs
and Traffic
Prioritization

What is a Virtual LAN (VLAN)?

CONTENTS

What is a Virtual LAN (VLAN)?.....2
 Benefits.....2
 How VLANS Work.....2
 VLAN Configuration and Setup3
 Setting the Ingress and Egress Modes .3
 Setting the PAN Port Associations.....5
 Setting Outgoing and Incoming Tag Schemes6
 What is Traffic Prioritization?8
 Benefits.....8
 How Traffic Prioritization Works8
 Traffic Prioritization Configuration and Setup9
 Setting Priority Tag Values9
 Setting Up Traffic Priority Schedule Policy.....11
 Business Application12
 For More Information12
 Appendix A: Default Settings.....13
 Appendix B: Additional Notes.....14

A VLAN is a logical subnet grouping that can be assigned to users, logins, or systems— independently of the physical network infrastructure. An IEEE 802.1Q-compliant VLAN is equivalent to a Layer 2 broadcast domain.

Systems or users associated with a particular VLAN subnet can communicate freely. Network logins and end systems can be centrally managed as though they were physically located in the same site, regardless of the actual topology of the network.

Benefits

Support for port-based VLANs enables the 3Com® NJ200 Network Jack to deliver significant IT and business benefits. For example, it can help:

- Reduce the costs of IT equipment moves, upgrades, and other changes
- Centralize and automate network administration
- Create and monitor virtual workgroups for a specific department or section, with most of the traffic staying in the same VLAN broadcast domain
- Isolate broadcast, multicast, and unicast traffic to a single subnet domain
- Reduce traffic congestion and prevent network flooding
- Accelerate network performance without expensive router hardware
- Control communication among broadcast domains

How VLANS Work

In order to properly forward VLAN traffic, core network switches and management platforms check each Ethernet frame for an IEEE 802.1Q VLAN tag. Each tag is identified by a unique VLAN ID (VID), which can be a number between 1 and 4095.

IEEE 802.1Q-compliant NJ200 Network Jacks support the following VLAN functionality:

Forwarding Inbound-Traffic from the LAN

The NJ200 Network Jack forwards voice, data, and video packets based on their MAC addresses, not Ethernet frame tags. However, this 802.1Q-compliant Ethernet-data switch can be configured to:

- Check incoming traffic for VLAN tags
- Modify outbound traffic to include VLAN tags
- Forward VLAN-tagged traffic

This supports other devices that rely on Ethernet frame tags to correctly recognize and forward VLAN traffic. The section titled, *Setting the Ingress and Egress Modes*, provides step-by-step details on how to configure these capabilities.

Forwarding Traffic Among PAN Ports

Port Associations regulate traffic between the PAN (device) ports on the same switch. Port Associations only distribute traffic at the four PAN ports and have no effect on traffic entering or leaving the switch, or going out to the LAN.

Port Associations can be configured in any combination among PAN ports belonging to the same switch. For example, Port #1 can be associated to any other port, all three, or none of them. For details on how to set up Port Associations, refer to the section titled, *Setting PAN Port Associations*.

Table 1. Summary of 802.1Q VLAN Functionality

Feature	Function
Ingress/egress rules	Applied at the LAN port (uplink port) only
VLAN tags	One VLAN tag can be set per PAN port
Traffic prioritization	802.1p traffic prioritization supported through four, port-based hardware queues
Inbound unicast traffic	Ethernet frames forwarded based on the MAC addresses; no exceptions
Inbound multicast traffic	All Ethernet frames forwarded to all ports regardless of tags
Inbound broadcast traffic	All Ethernet frames forwarded to all ports regardless of tags

VLAN Configuration and Setup

Forwarding Outbound-Traffic to the LAN

For most outbound data traffic, the PAN ports add VID tags to the Ethernet frames prior to them reaching the LAN (uplink) port. In this case, the LAN port simply delivers the outbound traffic to the network. Once on the network, the VID-tagged traffic can be forwarded and segmented by any 802.1Q enabled switch port.

For broadcast, multicast, and unicast traffic, the outgoing Ethernet frames are tagged at the LAN port. This tagged traffic is subsequently identified and forwarded by 802.1Q-enabled upstream network switches.

For a step-by-step guide on setting up outbound traffic tags for the LAN port, please refer to the section titled, *Setting the Outgoing Tag Scheme*.

Setting the Ingress and Egress Modes

Although the NJ200 switch does not use VLAN tags, these tags are needed by many other network devices—such as upstream switches or a VoIP phone connected to a PAN port. To ensure traffic is appropriately tagged as it enters and exits, the NJ200 Network Jack can be configured to add tags, remove tags, or leave frames unmodified.

The ingress mode uses the receiving port buffer to inspect and process inbound traffic. The egress mode uses the transmitting port buffer to inspect and process outbound traffic. The four settings are summarized in Table 2.

Table 2. Ingress and Egress Control Settings

Inbound Traffic	Outbound Traffic	Ingress Mode Setting	Egress Mode Setting
Tagged	Tagged	Frames received unmodified	Frames transmitted unmodified
Tagged	Untagged	Remove 802.1 tag if present	Frames transmitted unmodified
Untagged	Untagged	Frames received unmodified	Frames transmitted unmodified
Untagged	Tagged	Frames received unmodified	Add 802.1 tag to untagged frame

Figure 1. The ingress mode is applied to VLAN traffic coming from the LAN before it gets sent downstream to the PAN ports. The egress mode is applied to VLAN traffic coming from the PAN ports before it gets sent upstream to the LAN.

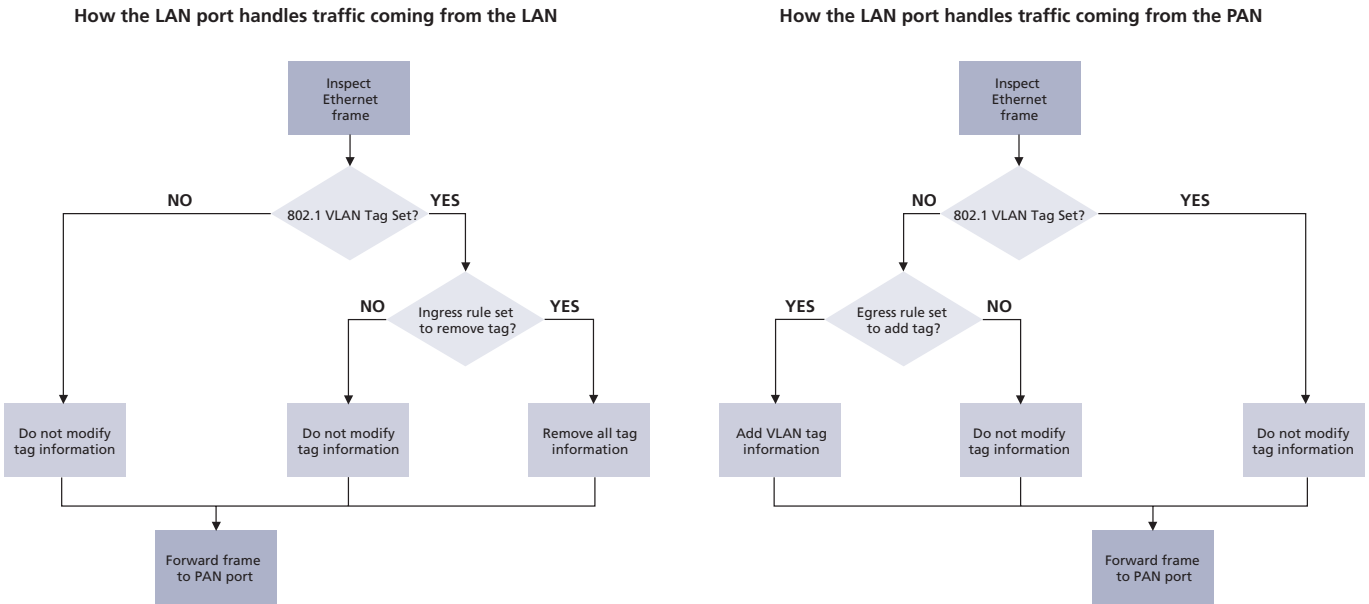
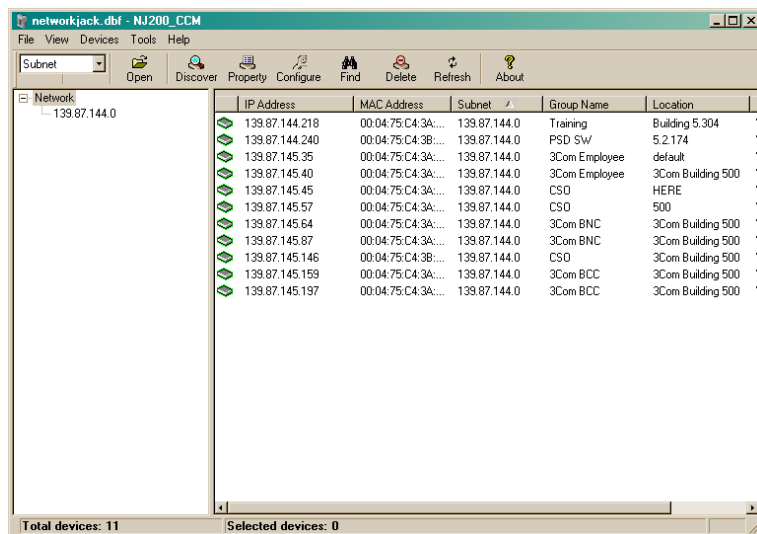


Figure 1 provides a two-key schematic of the traffic-control process, including where ingress and egress rules are applied. Configuring the ingress and egress modes is accomplished using 3Com Central Configuration Manager:

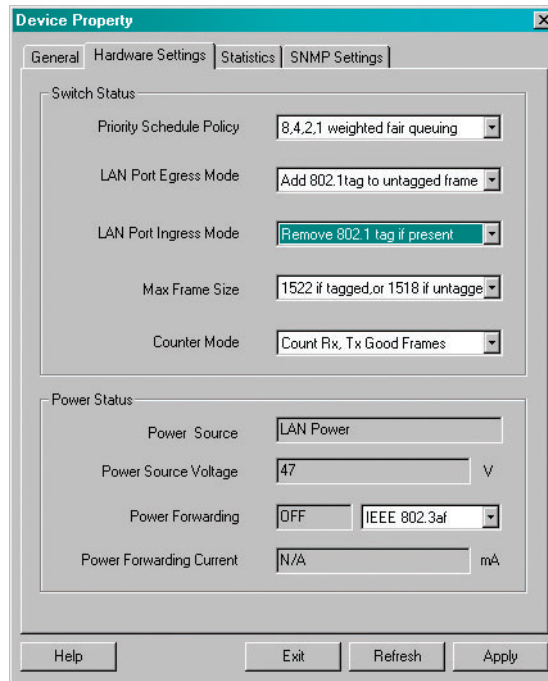
1. Open the **Central Configuration Manager**. From the list of devices, select an NJ200 Network Jack and then select **Property**. You can also right-click on its IP address and select **Property** from the menu.

Figure 2. 3Com Central Configuration Manager GUI enables point-and-click remote administration of NJ200 Network Jacks.



- Click on the **Hardware Settings** tab to view the LAN (uplink) port ingress and egress modes. You should see a window like this:

Figure 3. Ingress and egress modes can be viewed and configured using 3Com Central Configuration Manager.



- Use the pull-down menu to set the desired **LAN Egress Mode**, either:
 - Frames transmitted unmodified**
 - Add 802.1 tag to untagged frame**
- Use the pull-down menu to set the desired **LAN Ingress Mode**, either:
 - Frames received unmodified**
 - Remove 802.1 tag if present**
- Click on **Apply** to proceed to the password-request window. Once a password is entered and accepted, the next window will show a summary of the new settings.
- Click **OK** to finalize and exit the configuration window.

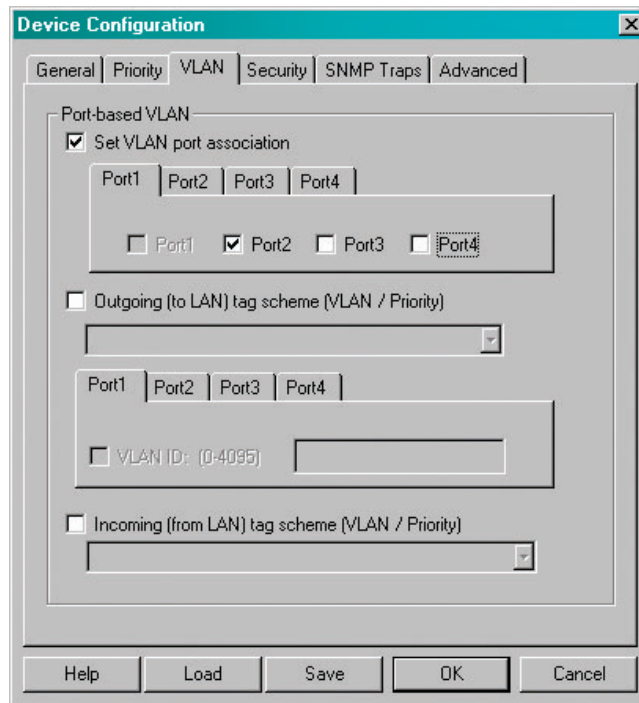
Setting the PAN Port Associations

The PAN (device) ports can support up to four different VLAN domains. 3Com Central Configuration Manager lets you assign individual ports to four separate VLANs, all ports to the same VLAN, or any combination in between. The following example illustrates how the Port Associations are used to create two port groups assigned to separate VLANs—where the ports in one group cannot share traffic with ports in the other.

- Open **3Com Central Configuration Manager** and select **Devices** from the main menu.
- From the list of devices, select an NJ200 Network Jack and then select **Configuration**. You can also highlight and right-click on the switch and select **Configuration**.

- Click on the **VLAN** tab to open a window that displays port-based settings for VLANs, outgoing tags, and incoming tags:

Figure 4. Port associations enable you to assign a VLAN broadcast domain to a single PAN port or group of associated ports.



- Under **Port-based VLANs**, make sure the **Port Association** box is checked.
- You should see four tabs, one for each PAN port. Select the **Port 1** tab and check the **Port 2** box. This configures Ports 1 and 2 to share traffic with each other but not ports 3 or 4.
- Next, select the **Port 3** tab and check the **Port 4** box. This configures Ports 3 and 4 to share traffic with each other but not ports 1 or 2.

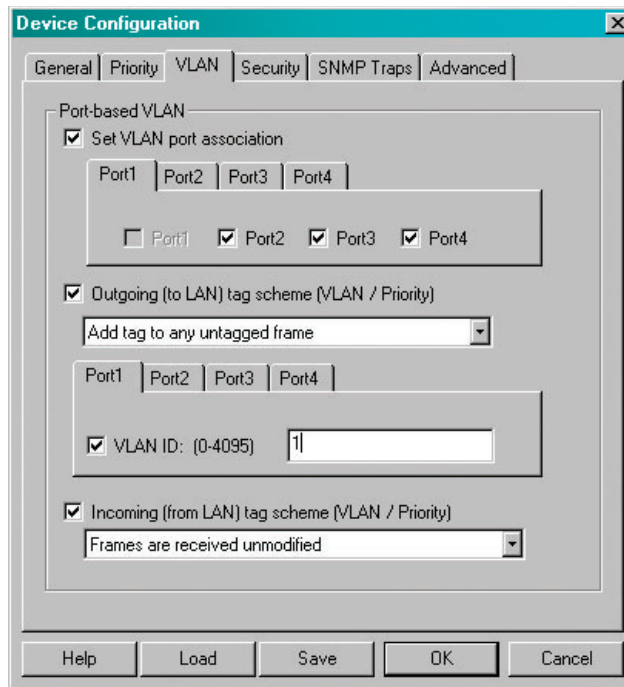
Note: It is possible to override these port configurations with a higher-level device, such as a core switch that supports Layer 3 IP forwarding between VLANs.

Setting Outgoing and Incoming Tag Schemes

Once the Port Associations have been set up, the PAN ports can be assigned to VLANs using the appropriate VLAN ID (VID) numbers. The PAN-port VIDs can be any number from 0 to 4095 and must match the core-switching VIDs, which are typically assigned by the enterprise network management platform.

IMPORTANT: If any PAN port is configured with a VID that has no corresponding upstream match, the entire switch may lose network connectivity. To reset the LAN port and recover network communications, the NJ200 Network Jack must be connected to a hub or flat VLAN. It can then be reconfigured with the proper VID using 3Com Central Configuration Manager.

Figure 5. Setting the outgoing and incoming tag schemes assigns the PAN ports to one or more VLANs.



1. Put a check the **Outgoing Tag Scheme** box.

Note: This setting affects both VLAN and traffic priority sorting on a bridge-wide basis.

2. Select the **Port 1** tab and from the pull-down menu, select **Add tag to any untagged frame**.
3. Put a check in the **VLAN ID** box and type **1** in the **VLAN ID** field. PAN ports 1 and 2 are now configured as part of the “VLAN 1” subnet.
4. Repeat the last two steps to configure PAN ports 3 and 4 as part of the “VLAN 2” subnet. Click **OK** to exit configuration window.
5. Put a check in the **Incoming Tag Scheme** box.

Note: This setting affects both VLAN and priority traffic sorting on a bridge-wide basis.

6. From the pull-down menu, select **Frames received are unmodified**.
7. Click **OK** to exit configuration window.

What is Traffic Prioritization?

IEEE 802.1D/D17 (which incorporates IEEE 802.1p) traffic prioritization lets IT staff establish packet-based control over network traffic. These advanced features allow high-priority packets containing time-sensitive or system-critical data to be transmitted with minimal delay.

Traffic prioritization can also help differentiate network traffic by type—such as multimedia, video, protocol-specific, time critical, and file-backup.

Benefits

Traffic prioritization can significantly reduce bandwidth limitations, network delay, data loss, and jitter (interference). Traffic prioritization is most useful for critical applications that require a high Class of Service (CoS) from the network.

In addition to delivering the above capabilities, the NJ200 Network Jack can help increase the reliability of data delivery, allow specific applications to be prioritized across the network, and define exactly how to treat selected applications and types of traffic. The following are a few of the many applications that can benefit from being connected through this standard-compliant switch:

Converged network applications enable voice, video, and data traffic to share the same physical infrastructure. These sophisticated applications require maximum bandwidth and minimal latency in order to deliver high-quality voice and video transmissions.

Resource planning applications rely on time-sensitive communications and on-demand access to core enterprise servers such as SAP.

Financial applications are used by accounting departments to handle AR/AP, taxes, interest payments, and other business-critical processes. These powerful programs need immediate and reliable access to large datasets and bulky spreadsheets.

CAD/CAM design applications take up enormous amounts of network bandwidth—for accessing server farms and transferring very large graphics files.

How Traffic Prioritization Works

IEEE 802.1D/p traffic prioritization differentiates data packets into classes that are used to automatically select and forward high-priority transmissions over less critical traffic. This helps ensure that time-sensitive and business-critical communications get the highest level of service. Traffic prioritization also separates the queuing of time-critical frames to help reduce jitter.

Table 3 shows the range of priority tag values, with 7 having the highest importance and 1 the lowest.

Note: The NJ200 Network Jack default priority tag setting is 0. This has a higher priority than 2, which is used for nonessential traffic.

Table 3. IEEE 802.1D/p Traffic Prioritization Tag Values

Value	Tag	Traffic Type
0	Best Effort	Default setting
1	Background	Background system processes
2	Standard	Spare, nonessential
3	Excellent Effort	Business-critical
4	Controlled Load	Streaming multimedia
5	Video	Interactive media; latency <100 ms; jitter-control queuing
6	Voice	Interactive voice; latency <10 ms; jitter-control queuing
7	Network Control	Reserved network processes

The 802.1D/p-compliant switch gives preference to Ethernet frames with higher priority tag values. High-priority traffic is directed through hardware-based queues that are kept separate from queues for lower priority traffic.

Traffic Prioritization Configuration and Setup

Setting Priority Tag Values

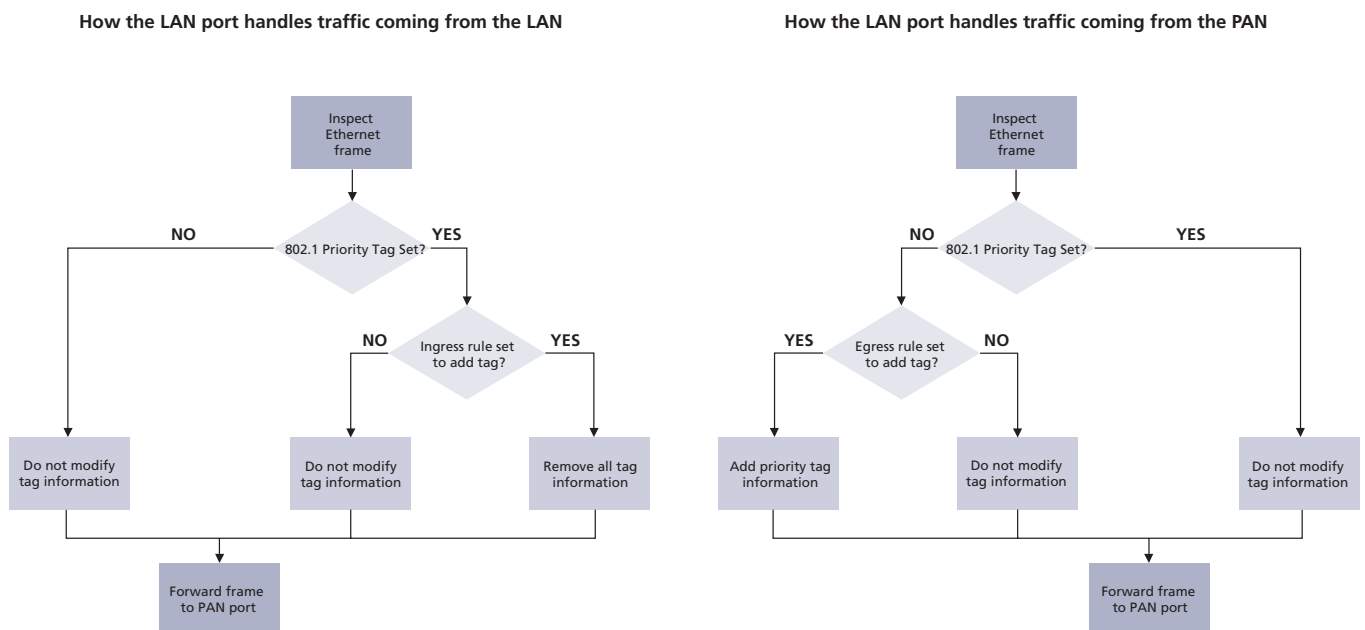
The first step in configuring a traffic prioritization scheme is to ensure that the NJ200 Network Jack recognizes the priority tags as traffic passes through the switch. As with the VLAN scheme, the switch can be configured to add tags, remove tags, or leave frames unmodified.

As mentioned in the previous section, the IEEE 802.1D/p standard specifies eight distinct levels of priority (0 through 7), each of which relates to a particular type (class) of traffic. The NJ200 Network Jack pairs up the eight tag values into four priority levels, to match the available traffic queues. Each priority level is determined by the lower value of each tag-value pair as follows:

Table 4. IEEE 802.1D/p Tags and Switch Values

Tag Pair	Priority Value
0 or 1	0
2 or 3	2
4 or 5	4
6 or 7	6

Figure 6. The ingress mode is applied to prioritized traffic coming from the LAN before they are sent downstream to the PAN ports. The egress mode is applied to prioritized traffic coming from the PAN ports before they are sent upstream to the LAN.



The traffic prioritization process is similar to that of the VLAN scheme. The switch applies ingress rules at the receiving-port buffer and egress rules at the transmitting port buffer. (Figure 6.)

Configuring traffic priority levels is accomplished using 3Com Central Configuration Manager:

1. Open 3Com **Central Configuration Manager** and select **Devices** from the main menu.
2. From the list of devices, select an NJ200 Network Jack and then select **Property**. You can also right-click on its IP address and select **Property** from the menu.
3. Click on the **Priority** tab and select a PAN (device) port to configure. For example, the configuration window for Port 2 will look similar to this:

Figure 7. Traffic priority levels are individually configured for each PAN port.

The screenshot shows the 'Port 2 Settings' dialog box. The settings are as follows:

- Port State: Enable (Forwarding)
- Port Speed/Duplex: Auto Negotiation
- Priority Lookup Scheme: None
- Default Priority Level: 802.1p Priority 2 or 3
- VLAN Association: Port1, Port2, Port3, Port4
- Default Vlan Id: 65
- Flow Control: Off
- MDI[X] setting: Manual MDI configuration
- Multicast Rate Limit: 3%

4. Under **Priority Lookup Scheme**, choose one of the following settings:
 - a) *None*
 - b) *802.1p Traffic Class fields*
 - c) *Use IP TOS, Diffserv fields*
 - d) *Both*

To ignore the priority tags on incoming Ethernet frames, set the **Priority Look up Scheme** to **None**.

Note: Priority Lookup Scheme specifically instructs the NJ200/NJ205 to inspect Ethernet frames at the LAN port for 802.1p, Diffserv, or both. If the incoming traffic will not be Diffserv or 802.1p, the Priority Lookup Scheme should be set at "None."

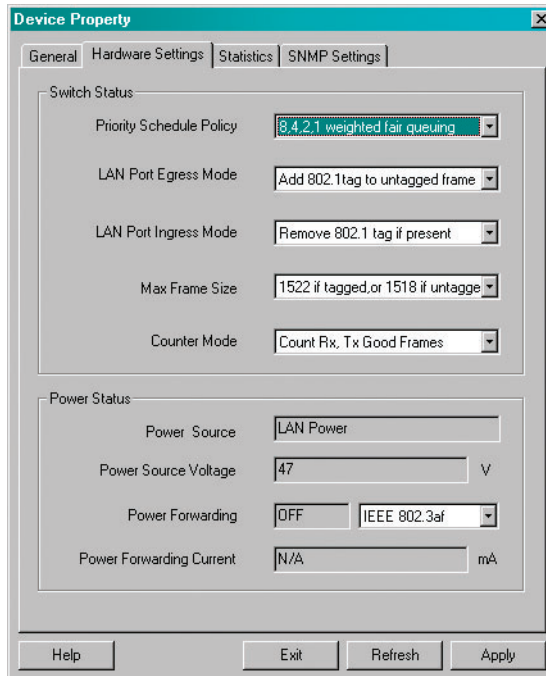
5. Under **Default Priority Level**, set what priority level to associate with the PAN port:
 - a) *802.1p Priority 0 or 1*
 - b) *802.1p Priority 2 or 3*
 - c) *802.1p Priority 4 or 5*
 - d) *802.1p Priority 6 or 7*
6. Click **OK** to exit the configuration window. Repeat these steps for the other PAN ports.

Setting Up Traffic Priority Schedule Policy

Use this setting to modify how the switch will receive frames from each queue:

1. Open **3Com Central Configuration Manager** and select **Devices** from the main menu.
2. From the list of devices, select an NJ200/NJ205 and then select **Property**. You can also highlight and right-click on the NJ200/NJ205 and select **Property**.
3. Click on the **Hardware Settings** tab to view and configure the **Priority Schedule Policy** settings. You should see a window like this:

Figure 8. Traffic priority schedules are individually configured for each PAN port.



4. Under **Priority Schedule Policy**, choose one of the following:
 - a) 8,4,2,1 weighted fair queuing (default)
 - b) Strict Priority Scheme (all queues weighted the same)
5. When all configuration settings are complete, click on the **Apply** button, which opens a password-prompt window. After the password is accepted a screen will appear summarizing the new settings. Click **OK** to accept and close configuration window.

Business Application

IT staff can use VLANs to partition traffic streams into easily manageable and securable groups. Automated traffic prioritization can significantly improve network and application performance, particularly for time-sensitive transmissions such as voice and video. The following scenario, while fictional, demonstrates how these two advanced switching features can solve real-world problems and deliver significant time and cost savings.

In an effort to converge and consolidate, a large aerospace corporation had successfully migrated business-critical resources onto the network. The core switching infrastructure was upgraded, DSL Internet router installed, and PSTN phones were replaced by a VoIP telephony system.

News of an upcoming satellite launch sent draftpersons and engineers dashing to their desktops to watch via the live webcast. All this Internet traffic sent network loads soaring—creating access bottlenecks and slowing application response. In particular, a telephone conference with a trans-Pacific client suffered in quality and usability. The meeting ended up being postponed until the next day, a 24-hour delay that cost the company many thousands of dollars.

This disaster might have been avoided if IT staff had installed 3Com NJ200 Network Jacks in all offices and conference rooms as part of the infrastructure upgrade. Using port-based VLANs, all VoIP transmissions could have been directed through their own subnet, regardless of what conference room was being used. In addition, the Default Priority Level could be set to recognize the IEEE priority tag for VoIP (value = 6), which would help ensure that this extremely time-sensitive traffic gets preference over streaming video (value = 4).

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.

Appendix A: Default Settings

Global Switch Setting	Default Value
Max Frame Size	1518 or 1522 if tagged
Counter Mode	Count good frames
Priority Scheduling Mode	8, 4, 2, 1 weighted
VLAN Tag for LAN Port (egress)	Egress frame unmodified
VLAN Tag for LAN Port (ingress)	Ingress frame unmodified
Power Forward	Autodetection
SNMP "Set" Permission	Not allowed

Port Setting	Default Value
State	Forwarding
Link	Autonegotiation
Flow Control	Off
MDI[X]	Force MDI
Multicast Limit	3%
Priority Lookup	Tag and IPV4
Port Priority	1
VLAN ID	1
Port based VLAN	All ports on same VLAN

Unchanged Values After Restoring to Factory Default Settings

Some configuration values remain unchanged when you click **Restore Factory Default Settings**. The following values must be changed manually:

- Group Name
- Location ID
- Password
- IP Address
- DHCP Settings
- SNMP Community Strings
- SNMP Trap Settings

Appendix B: Additional Notes

- 3Com NJ200 Network Jack is compliant with SNMPv.1 and supports most SNMP management platforms
- Multicast packets are handled the same as broadcast packets
- The autonegotiation setting on the LAN port (uplink port) cannot be changed
- NJ200 Network Jack does not support spanning tree protocol (STP)
- MAC table is capable of 512 addresses at any given time; timeout in 300 seconds/5 minutes of inactivity; these settings are permanent and cannot be changed
- Ethernet switching uses store-and-forward—receives complete frame in switch buffer, checks CRC, looks up destination address in MAC filter table, and forwards frame



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. IntelliJack and Possible made practical are trademarks 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.

NJ_VirtualLANs 09/03