Virtual LAN (VLAN)
NetPerformer® System Reference

MEMOTEC
redefining network efficiency

COPYRIGHTS AND DISCLAIMERS

Contents

NetPerformer VLAN Support

1.1 The 802.1 p/q Standard

IEEE standard 802.1p/q addresses two functional areas:

- Prioritization at level 2

- Support for Virtual LAN, or VLAN.

More and more networks are using level 2 LAN switches to segment LAN. This limits congestion on individual segments and separates user groups without having to run separate LANs. Segmented LAN works well when operating in a single building or campus environment, but can create problems when interfacing to a WAN that is based on level 3 routers, which strip the level 2 of the frame including the special VLAN tag.

The NetPerformer supports 802.1p prioritization by mapping the priority bits of the VLAN tag to the PowerCell classes of service (see Filtering VLAN Priority on page 4). This allows, for example, IP phones that use level 2 prioritization to receive the same treatment when connected over wide area networks.

To support Virtual LANs over a wide area network, one option is to enable bridging on the router. However, when operating over limited bandwidth or in large networks, the LAN broadcast can consume a lot of precious bandwidth, making the network inefficient.

The NetPerformer solution filters these broadcasts to reach only those NetPerformer units that belong to the same VLAN, limiting unnecessary traffic. An application for this is where multiple customers share a common network access method, such as a remote satellite link.

NetPerformer VLAN support follows the IEEE 802.1p/q standard for virtual bridged LANs, and provides:

- The ability to create, change and manage logical groups of stations that communicate as though they were on the same LAN

- Common support of all LAN MAC protocols over point-to-point and shared media LANs

- Sharing of a common media into multiple virtual LANs

NOTE: Although they share the same media, VLANs are independent from one another.

- Restricted traffic movement. Bridges forward unicast, multicast and broadcast traffic only on specified LAN segments, configurable by the user

- Compatibility with existing bridges and end stations.

1.2 Traditional LANs

Traditionally, all stations on a LAN are part of the same network. Although they may be subdivided into workgroups for management purposes, the network is unaware of this segregation.

- Any broadcast message that is sent by one station is forwarded to all other stations, in all workgroups, and is propagated by any bridges that are part of the network

- In this architecture, the bridge cannot determine whether any of the destination stations actually require this broadcast

- If a large number of independent workgroups share the same physical network, the requirement to broadcast all traffic to all LAN segments can reduce the overall efficiency of the network.
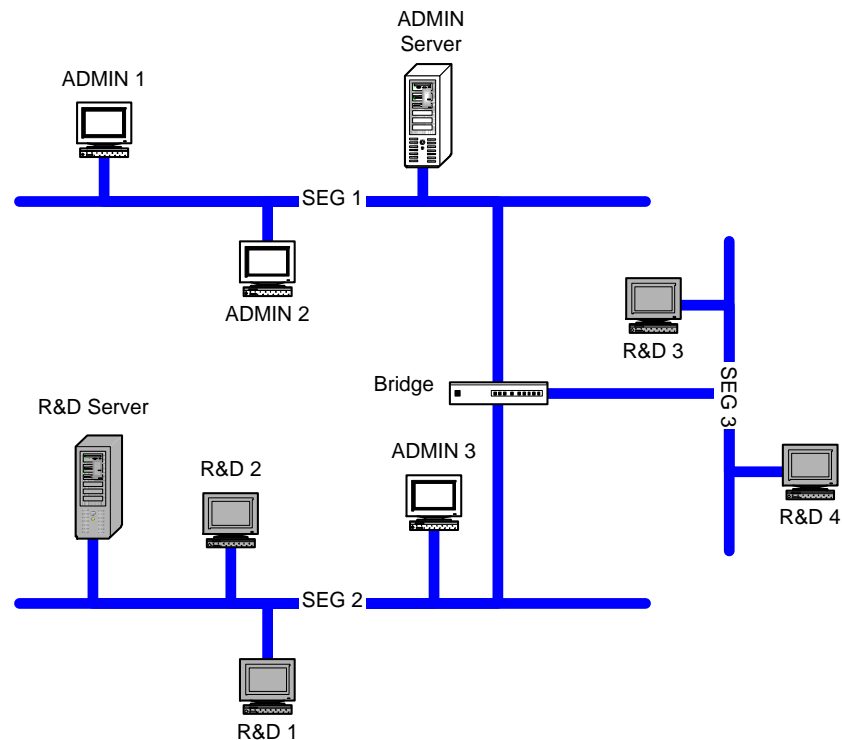
Figure 1-1: Traditional LAN

The example above shows a network where the ADMIN and R&D groups are relatively independent workgroups that share the same physical network. Although most of the nodes for each group are concentrated on the same LAN segments, some exceptions exist. For example, **SEG 1** is the segment where most of the administrative staff is connected. **SEG 2** and **SEG 3** are mostly used for R&D except for one node, **ADMIN 3**.

Whenever station ADMIN 1 sends a broadcast, this frame must be bridged to **SEG 2** and **SEG 3**, even though there are no members of the ADMIN workgroup on **SEG 3**. This becomes a problem in large networks with hundreds or thousands of nodes.

1.3   Virtual LANs

IEEE recommendation 802.1q introduces a method for subdividing the physical media into multiple virtual LANs (VLANs).

- This is achieved by adding a four-byte VLAN Tag Header into the MAC header, with the following format:
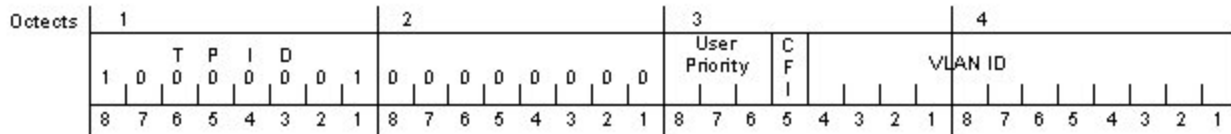
Figure 1-2: VLAN Tag Header in the MAC header

- The VLAN Tag Header contains the VLAN ID and a three-bit *User Priority* field. This field is used to implement traffic prioritization, following IEEE recommendation 802.1p (see Using VLAN to Prioritize Traffic on page 8).

- VLANs can be used to logically group together nodes that are on different LAN segments.
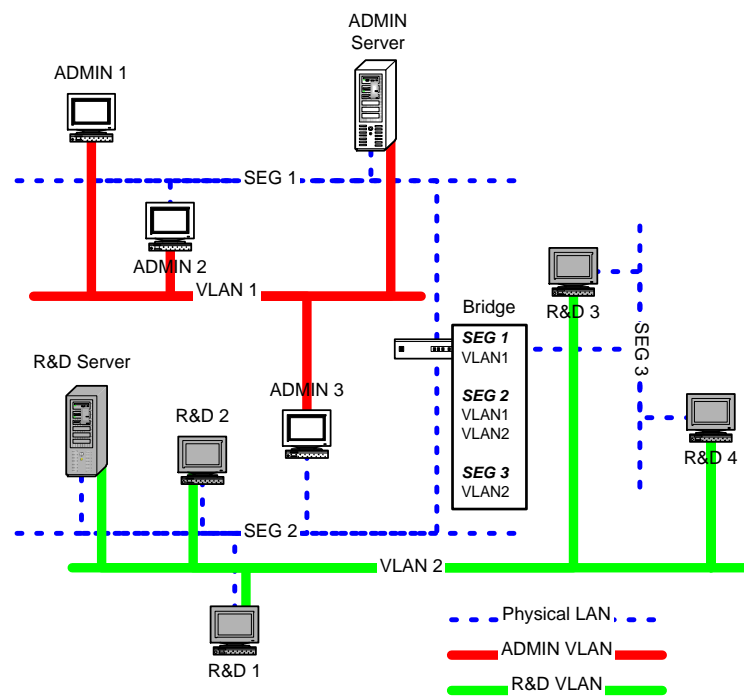
Figure 1-3: LAN Subdivided into VLANs

Figure 1-3 shows a simple VLAN structure.

- Each node is assigned a VLAN ID, which is included in the VLAN Tag Header on all traffic transmitted from that node. In this example, the ADMIN nodes are assigned to VLAN 1, and the R&D nodes to VLAN 2.

- The VLAN information is used primarily by the bridge to determine if a broadcast message needs to be forwarded over a particular interface. In this example, if the station **ADMIN 1** sends a broadcast, the bridge will forward it to **SEG 2** since there is at least one member of VLAN 1 on it, but the bridge will not send the broadcast to **SEG 3**.

- The bridge keeps track of which VLAN is present on which segment, so it knows over which interface to forward traffic for a specific VLAN.

1.4 How VLAN Works on the NetPerformer

1.4.1 Ethernet Port

The NetPerformer Ethernet port can be configured to be VLAN-aware.

- This is accomplished by enabling the *VLAN enable* parameter and assigning a *VLAN Number* to the Ethernet port, representing the VLAN on which the Ethernet port resides. Refer to Configuring the Ethernet Port on page 3 for the configuration procedure.

- Traffic destined to the NetPerformer itself (such as Telnet, FTP, PING, etc.), must come from the same VLAN to be recognized by the NetPerformer. Otherwise, the traffic is treated as though it were on another network.

The Ethernet port processes tagged and untagged frames in the following manner:

- When a **tagged frame** is received on the Ethernet port:
  - The NetPerformer processes the frame, whether or not the Ethernet port has been configured to be VLAN-aware.
  - If the frame is destined for the NetPerformer itself, however, the VLAN parameter must be enabled and the received frame must match the configured VLAN number. Otherwise, the NetPerformer discards the frame.

- When an **untagged frame** is received on the Ethernet port:
  - The NetPerformer always processes the frame.

NOTE: Even if the Ethernet port has been assigned a VLAN number, the NetPerformer is still able to accept and bridge untagged frames.

- When a **tagged frame** is sent from the Ethernet port:
  - The NetPerformer bridges the frame on the Ethernet port, even if it is not configured to be VLAN-aware.

NOTE: To successfully bridge a tagged frame, the VLAN destination must be properly configured in a VLAN profile (1 to 10).

- When an **untagged frame** is sent from the Ethernet port:
  - The NetPerformer always processes and bridges the frame.

NOTE: The NetPerformer implementation of IEEE 802.1p/q assumes that all LAN traffic is already properly tagged and has the priority field set to an appropri-

ate value. **The NetPerformer does not modify these fields en route from one network to another. Traffic that is not tagged is bridged in the traditional manner.**

1.4.2   Mapping VLAN IDs to Destinations

To configure the NetPerformer to support VLANs, the user must build a VLAN ID to Destination Mapping Table. The NetPerformer uses this table to determine over which PVC or port it should send a frame that belongs to a particular VLAN.

For the VLAN configuration procedure, refer to .

1.5 Using VLAN to Prioritize Traffic

The NetPerformer employs priority field processing, following the IEEE 802.1p standard, to prioritize one traffic type over the rest of the traffic. For example, it is possible to prioritize voice traffic over LAN traffic in a VoIP application to prevent voice clipping when data burst occur.

- When the frames are bridged, the priority field of the VLAN TAG Header is carried intact to the destination network.

NOTE: If PowerCell transport is used, NetPerformer filters can also be defined to set the priority of a frame according to the VLAN Tag Header priority field. Refer to Filtering VLAN Priority on page 4.

- When the frames are routed the VLAN Tag Header is lost, and the priority information along with it. However, the NetPerformer can be configured to convert the priority information from the VLAN Tag Header to another format before routing, to ensure proper prioritization of the traffic.

NOTE: This is accomplished with the *VLAN Priority Conversion* parameter during configuration of the Ethernet port. Refer to Configuring the Ethernet Port on page 3.

2

Setting up a Virtual LAN

2.1   About Configuring a VLAN

To configure a VLAN on the NetPerformer you must:

- Define the VLAN characteristics (see next section)
- Enable VLAN on the Ethernet port (see page 3)
- (Optional) Filter VLAN traffic for Quality of Service (QoS) requirements (see page 4).

2.1.1   Configuring the VLAN Characteristics

To configure the NetPerformer unit as part of a Virtual LAN using the NetPerformer console:

- Enter the menu sequence: **SE ↵ VLAN**.
- Select a *VLAN index*.

NOTE: Up to 10 VLAN entries can be defined.

- Set *VLAN active* to **YES** to activate VLAN functions for this VLAN entry.

SE/VLAN example

```
SDM-9230>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/HUNT/IP/IPX/MAP/
PHONE/
PORT/PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SLOT/USER/VLAN,
def:BRIDGE) ? VLAN
VLAN> VLAN index (1-10,def:1) ?
VLAN 1> VLAN active (def:NO) ? YES
VLAN 1> VLAN number (0-4095,def:0) ? 101
VLAN 1> VLAN on ETH1 (def:YES) ?
VLAN 1> VLAN on ETH2 (def:YES) ? NO
VLAN 1> VLAN destname 1 (def:) ? CHICAGO-9230
VLAN 1> VLAN destname 2 (def:) ? CHICAGO-9220
VLAN 1> VLAN destname 3 (def:) ? SDM-9360
```

Details on these parameters are provided in the appendix SE/VLAN Configuration Parameters on page 1.

2.2 Configuring the Ethernet Port

To enable VLAN functions on the Ethernet port (the LAN interface):

1. Enter the menu sequence: **SE ↵ PORT ↵ ETH**.

2. Press the **<Enter>** key until you reach the *VLAN enable* parameter

3. Set *VLAN enable* to **YES**

4. Set the *VLAN number*

5. Enable *VLAN Priority Conversion*, if desired

SE/PORT/ETH example: enabling VLAN

```
SDM-9230>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/HUNT/IP/IPX/MAP/
PHONE/
PORT/PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SLOT/USER/VLAN,
def:BRIDGE) ? PORT
Port number (ETH/CSL/1,def:1) ? ETH
PORT ETH 1> Protocol (def:ETH AUTO) ?
PORT ETH 1> LAN speed (mbps) (def:AUTO) ?
...
PORT ETH 1> VLAN enable (def:NO) ? YES
PORT ETH 1> VLAN number (1-4095,def:1) ?
PORT ETH 1> VLAN Priority Conversion (def:NO) ?
```

VLAN enable, VLAN number and *VLAN Priority Conversion* are described in the appendix SE/PORT/ETH Configuration Parameters on page 1.

2.3   Filtering VLAN Priority

To filter VLAN traffic for Quality of Service (QoS) requirements, you can assign a priority to a particular NetPerformer Class of Service: **HIGH** or **1** to **8**, using the **MACQOS** filter.

- This filter maps the 802.1P priority level and queues that traffic onto a NetPerformer Class of Service.

- NetPerformer Classes of Service are used to prioritize VLAN traffic when bridging via PowerCell (PVCR).

For more information on filters, refer to the *Quality of Service (QoS)* fascicle of this document series.

To set the MACQOS filter:

1.   Enter the menu sequence: **SE ↵ FILTER**

2.   Select a *FILTER number*

3.   Enter the filter *Definition*, referring to MACQOS Filter Syntax on page 5

4.   Set the *Active* parameter to **YES** to activate the filter.

SE/FILTER example: MACQOS

```
SDM-9230>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/HUNT/IP/IPX/MAP/
PHONE/
PORT/PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SLOT/USER/VLAN,
def:BRIDGE) ? FILTER
FILTER number (1-32,def:1) ?
FILTER 1> Definition (def:) ? MACQOS(111,111)>HIGH
FILTER 1> Active (def:NO) ? YES
```

> **NOTE:**   General properties of the **SETUP/FILTER** parameters are provided in the appendix *Traffic Filters* in the *Quality of Service (QoS)* fascicle of this document series.

2.3.1 MACQOS Filter Syntax

The **MACQOS** filter sets up a range between **000** and **111** which represents the three-bit *User Priority* field in the VLAN *Tag Header* (see). The *Definition* must have the following syntax:

MACQOS(*min_value_of_range***,***max_value_of_range***)>***class_of_service*

where:

- *min_value_of_range* is a 3-bit binary value representing the lowest VLAN priority value

- *max_value_of_range* is a 3-bit binary value representing the highest VLAN priority value

- *class_of_service* represents the NetPerformer class of service, and ranges from **1** to **8** plus the **HIGH** priority level (usually used for voice traffic).

3

VLAN Application Scenarios

3.1   High-priority Voice Traffic

One VLAN application scenario uses the NetPerformer to carry both VoIP and LAN traffic between sites.
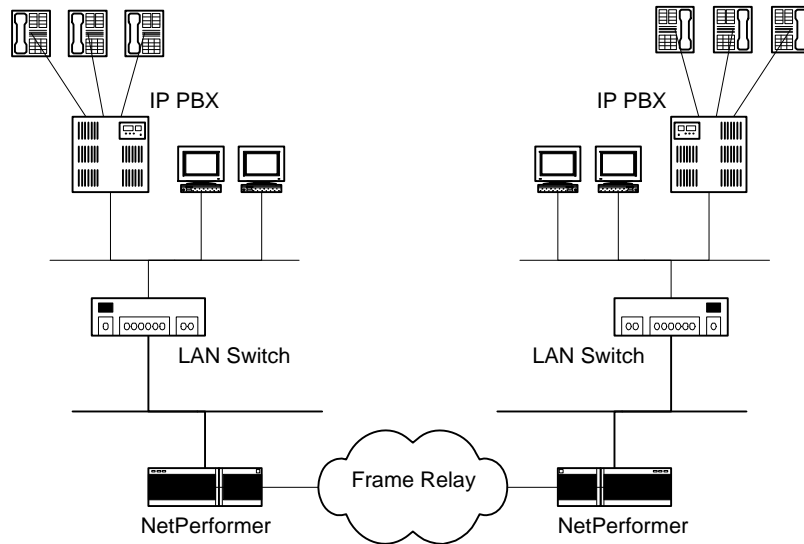

Figure 3-1: Giving Higher Priority to VoIP Traffic

In this scenario, the LAN switch sets the traffic priority. Traffic received by the IP PBX is assigned high priority. Otherwise, the priority is low. The NetPerformer uses this information to assign priority to VoIP traffic at the level of the Frame Relay PVC. This prevents voice clipping when data bursts occur on the LAN.

NOTE: In this application, only the priority information from the VLAN Tag Header is used. No actual VLANs are used.

3.2　VLAN Bridging

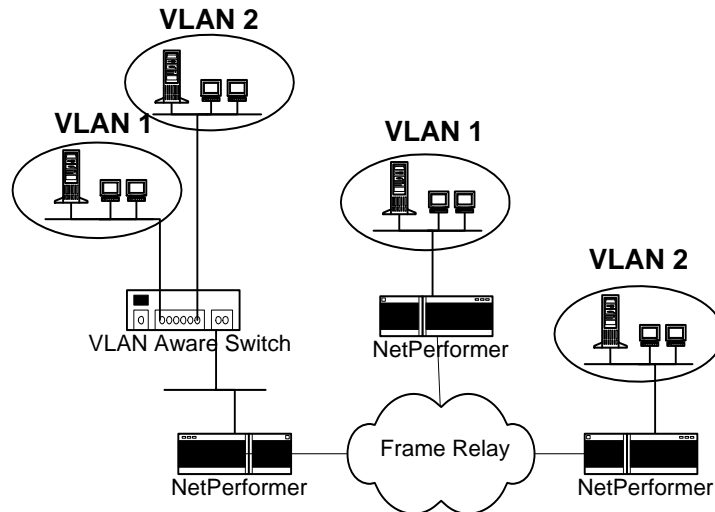Another application involves bridging VLAN tagged frames between sites.

Figure 3-2:　VLAN Bridging

The NetPerformer bridges VLAN traffic to destinations that are defined with the appropriate VLAN ID. This way, traffic destined for VLAN 2 is not sent to NetPerformer units that have nodes only on VLAN 1.

> **NOTE:**　Legacy nodes that are not VLAN-aware can be included in a VLAN by using a switch that is able to tag traffic received from a legacy segment and remove the tag when sending to it.

4

SE/VLAN Configuration Parameters

4.1   VLAN index

Console	SNMP	Text-based Config
VLAN index	VlanEntryIndex	[Vlan #]

Table 4-1: VLAN index parameters

The VLAN entry that you want to configure.

Values: 1 - 10

Default: 1

4.2   VLAN active

Console	SNMP	Text-based Config
VLAN active	VlanEntryEnable	[Vlan #] Enable

Table 4-2: VLAN active parameters

Enables (**YES**) or disables (**NO**) the VLAN functions.

Values: NO, YES

Default: NO

4.3   VLAN number

Console	SNMP	Text-based Config
VLAN number	VlanEntryNumber	[Vlan #] Number

Table 4-3: VLAN number parameters

The VLAN number, required for access to the NetPerformer unit using Telnet, FTP or SNMP via a specific VLAN.

Values: 1 - 4095

Default: 1

4.4   VLAN on ETH1

Console	SNMP	Text-based Config

Table 4-4: VLAN on ETH1 parameters

| VLAN on ETH1 | VlanEntryActiveLan1 | [Vlan #] ActiveLan1 |

Table 4-4: VLAN on ETH1 parameters

- On a NetPerformer with a single LAN interface, specifies whether the VLAN configuration is active on the Ethernet LAN port (**ETH**).

- On a NetPerformer with more than one LAN interface, specifies whether the VLAN configuration is active on the first Ethernet LAN port (**ETH1)**.

Values: NO, YES

Default: YES

4.5   VLAN on ETH2

Console	SNMP	Text-based Config
VLAN on ETH2	VlanEntryActiveLan2	[Vlan #] ActiveLan2

Table 4-5:   VLAN on ETH2 parameters

On a NetPerformer with more than one LAN interface, specifies whether the VLAN configuration is active on the second Ethernet LAN port (**ETH2**).

Values: NO, YES

Default: YES

4.6   VLAN destname 1, 2, 3

Console	SNMP	Text-based Config
VLAN destname 1 VLAN destname 2 VLAN destname 3	VlanEntryDest1 VlanEntryDest2 VlanEntryDest3	[Vlan #] Dest1 Dest2 Dest3

Table 4-6: VLAN destname 1, 2, 3 parameters

Three distinct *VLAN destnames* can be defined with the *Unit ID* of another NetPerformer. If all are left at the default value (undefined) the **Virtual LAN will not work**.

Values: the *Unit ID* of another NetPerformer

Default: none

5

SE/PORT/ETH Configuration Parameters

5.1   VLAN enable

Console	SNMP	Text-based Config
VLAN enable	iflanVlanEnable	[iflan#] VlanEnable

Table 5-1:   VLAN Enable parameters

Enables (**YES**) or disables (**NO**) VLAN communications on the Ethernet port. Leave *VLAN enable* at its default value, **NO**, if you do not want the LAN port to be VLAN-aware.

Values: NO, YES

Default: NO

NOTE: When *VLAN enable* is set to **YES**, additional VLAN parameters are also available, as shown in this example:

```
PORT ETH 1> VLAN enable (def:NO) ? YES
PORT ETH 1> VLAN number (1-4095,def:1) ?
PORT ETH 1> VLAN Priority Conversion (def:NO) ?
```

5.2   VLAN number

Console	SNMP	Text-based Config
VLAN number	iflanVlanNumber	[iflan#] VlanNumber

Table 5-2:   VLAN number parameters

The VLAN number, required for access to the NetPerformer unit using Telnet, FTP or SNMP via a specific VLAN.

Values: 1 - 4095

Default: 1

5.3 VLAN Priority Conversion

Console	SNMP	Text-based Config
VLAN Priority Conversion	iflanPriorityConversion	[iflan#] PriorityConver-sion

Table 5-3: VLAN Priority Conversion parameters

Enables (**YES**) or disables (**NO**) traffic priority information in the VLAN Tag Header. Set *VLAN Priority Conversion* to **YES** if you want this information to be preserved when routing broadcast frames.

Values: NO, YES

Default: NO

Index

REACH FURTHER. OFFER MORE.

Contact Memotec:

tel.: +1-514-738-4781
e-mail: MemotecSupport@memotec.com

7755 Henri Bourassa Blvd. West
Montreal, Quebec | Canada H4S 1P7   www.memotec.com

MEMOTEC
redefining network efficiency