VLAN

bintec-Dm 751-I

Legal Notice

Warranty

This publication is subject to change.

bintec offers no warranty whatsoever for information contained in this manual.

bintec is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

I Related Documents

bintec-Dm 709-I LAN Interfaces

bintec-Dm 717-I Bridge

bintec-Dm 750-I Ethernet Subinterface

Chapter 1 Introduction

1.1 Description

Up until now, work groups in a network were created by physically associating the users in the same network segment, or in the same concentrator or hub (*Fig. 1* on page 2).

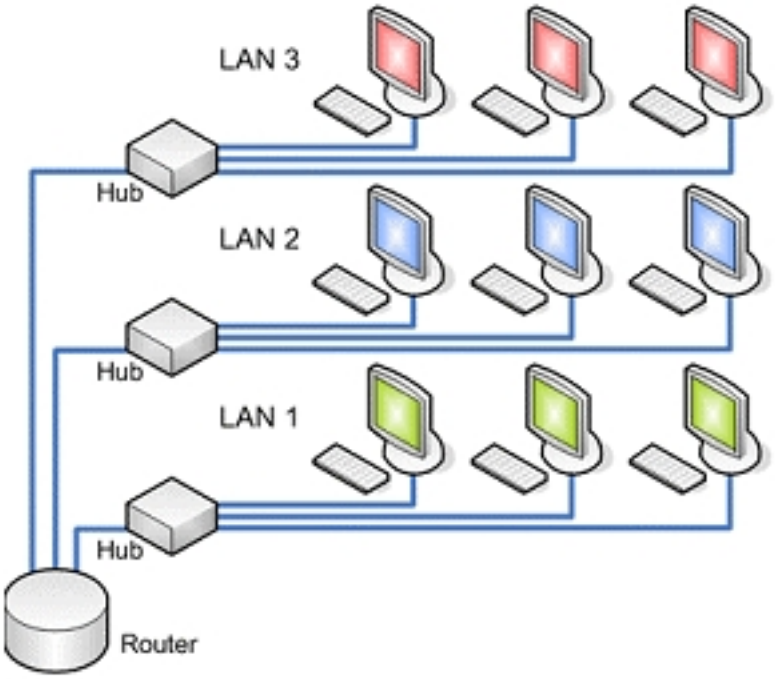


Fig. 1: **Work Groups without VLANs**

As a result, these work groups shared the available bandwidth and the broadcast domains. However, this posed management difficulties whenever there were changes in group members. Furthermore, geographic limitations mean that members of a determined group must be adjacent to each other in order to connect to the same concentrator or network segment.

VLAN schemes (Virtual LAN) provide adequate means to solve this problem through logical (rather than physical) device grouping.

Virtual LANs (VLANs) are software-defined LAN station groupings that communicate with each other as if they were connected to the same cable, even if they reside in different segments of a network or in different networks (*Fig. 2* on page 3).

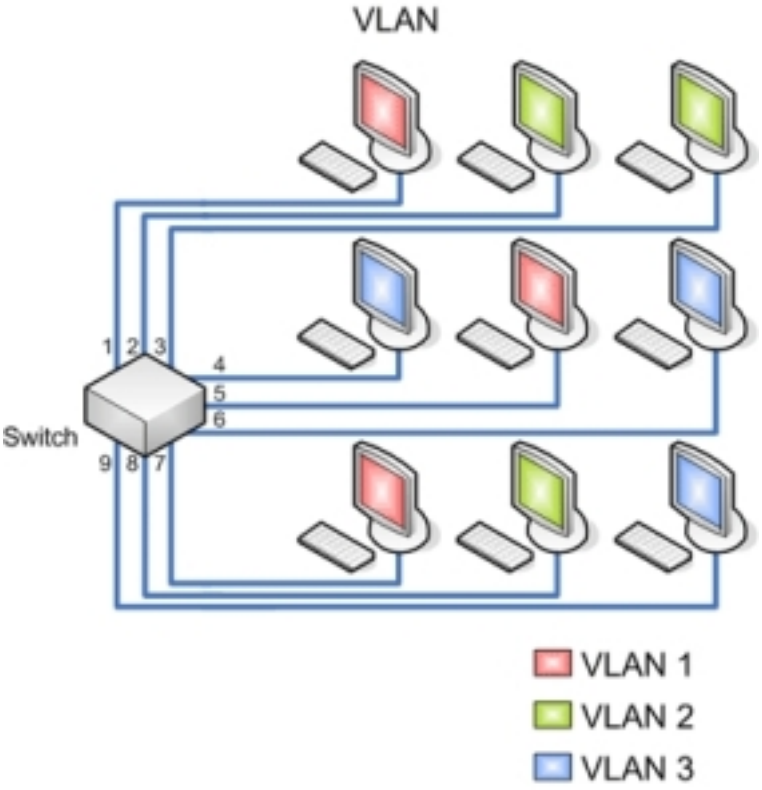


Fig. 2: **Work Groups with VLANs**

Virtual networks continue to share physical work group characteristics, meaning all VLAN users are interconnected and share the broadcast domains.

The main difference with respect to physical groupings is that users of virtual networks can be distributed throughout a LAN network, going asfar as being located in different LAN concentrators.

Users, therefore, can ‘move’ through the network without being expelled from the logical work group.

Additionally, by being able to distribute users belonging to the same logical group in different segments, you also obtain an increase in bandwidth for said group.

Since you are able to distribute users in different network segments, you can also place bridges and routers between them (thus separating segments with different topologies and protocols).

All security measures required are maintained in each configuration by the network administrator: As a result, incoming or outgoing VLAN traffic to/from other networks can be allowed or negated.

That is not all. In virtual networks, geographical location is not limited to different concentrators or floors in the same building, but can be extended to different offices intercommunicated through WAN networks (regardless of whether they are in the same country or continent). The only limitations are those imposed by the network manager.

1.2 VLAN Features

Devices with VLAN functions offer , in addition to the specific virtual network functions, added value features. Some of these are almost as essential as the main VLAN ones.

Similarly to what happens to “physical” work groups, VLANs allow logical work groups to share a broadcast domain. This means that the systems within a determined VLAN receive broadcast messages from the others, irrespective of whether they reside in the same physical network or not. For this, applications that need broadcast traffic continue operating in this type of virtual network. At the same time, these broadcasts are not received by other stations located in other VLANs.

VLANs are not just limited to one switch, they can extend through several (regardless of whether these are physically located in the same place or not).

Additionally, virtual networks can overlap. This means several networks can share certain resources (such as high performance backbones or connections to servers).

One of the major problems network managers face today is the administration of networks and subnets. VLANs can use the same number of nets in various segments. This is a practical mechanism to quickly increase bandwidth in new network segments without worrying about address collisions.

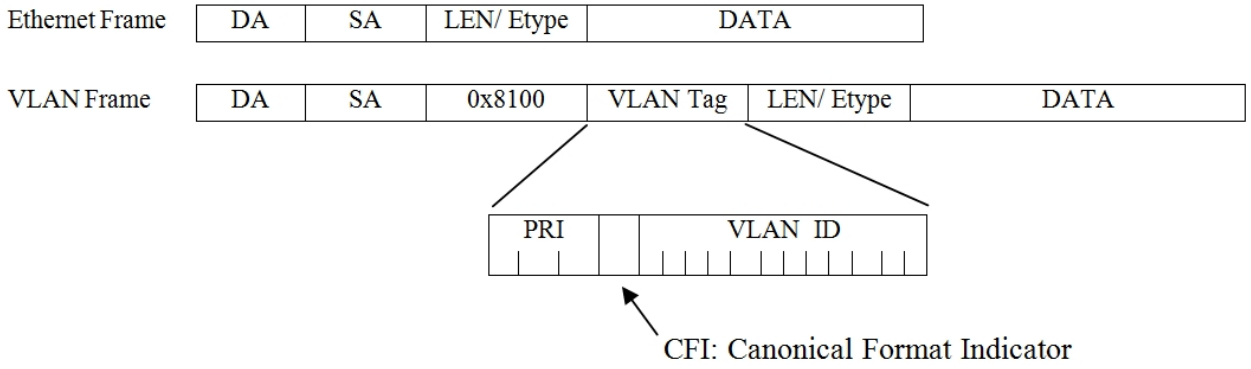
Traditional internetworking solutions (using concentrators and routers) require each segment to be a single subnet. However, in a device with VLAN features, a subnet can expand through multiple physical segments and a single physical segment can support various subnets.

Similarly, you need to bear in mind that the most advanced switch models with VLAN functions support very sophisticated filters, defined by the user or the network manager, which allow you to accurately determine the traffic characteristics and security required in each domain, segment, network or group of networks. This is all carried out using bridging algorithms and multiprotocol routing.

1.3 VLAN Frames Format

The format of VLAN frames, as well as the bridge functionality to process them, is described in the IEEE 802.1Q standard.

A VLAN frame is an amplification of a basic Ethernet frame. The VLAN frame includes two additional two-byte fields located between the source address field and the length/type field:



This encapsulation ensures the Ethernet frame MAC header size increases by four bytes.

- The first 2-byte field is known as TPID (Tag Protocol Identifier). This is a fixed value field which identifies the frames as VLAN frames. The value of this field is 0x8100.
- The second 2-byte field is known as TCI (Tag Control Information) and is made up of the following subfields:

  - PRI (3 bits), user priority, used for quality of service.

  - CFI (1 bit), Canonical Format Indicator, used for compatibility between Ethernet and Token Ring networks. If this is zero, this means the frame is in canonical format and does not include an additional field known as E-RIF (Embedded Routing Information Field).

  - VLAN-ID (12 bits), normally known as VID, is the identifier for the VLAN the frame pertains to. As this is a 12-bit field, up to 4096 different VLANs can be identified.

Note

The term tagged frame is normally used to refer to a frame with VLAN information. Similarly, frames without VLAN information are known as untagged frames.

Chapter 2 Configuration

2.1 VLAN Configuration Possibilities

There are several possibilities when configuring VLANs in bintec devices:

(1) Create an Ethernet subinterface and assign a VLAN to it.

(2) In devices with Ethernet switch interfaces, this configures the way the switch should deal with the VLAN packets in each port.

(3) In devices that operate as bridge, this configures the way the bridge should deal with the VLAN packets in each port.

By assigning an IP address to the Ethernet subinterface, the first case permits tagging the packets from an IP subnet as pertaining to a given VLAN. The process of creating and assigning a VLAN tag to an Ethernet subinterface is described in manual bintec-Dm 750-I “Ethernet Subinterface”.

The second case allows you to specify through which switch ports traffic from VLANs is permitted. The configuration for the way the Ethernet switch interface treats VLAN packets is described in chapter *Feature Configuration* on page 7 .

The third case allows you to specify how to carry out bridging over the VLAN packets. Chapter *VLANs Bridge Configuration* on page 13 focuseson the way VLAN packets are treated in the bridge.

Note

When configuring VLANs, we recommend that you don’t define the VLAN with identifiers 1 and 4095. These identifiers are reserved and can give rise to undesired behavior when used. For example, VID 1 is the default identifier for untagged packets. Only use these identifiers if you know the associated implications.

2.2 Processing the VLAN Frames

When executing a configuration where VLANs intervene, you need to bear in mind *Fig. 3* on page 5 until it exits through another port.

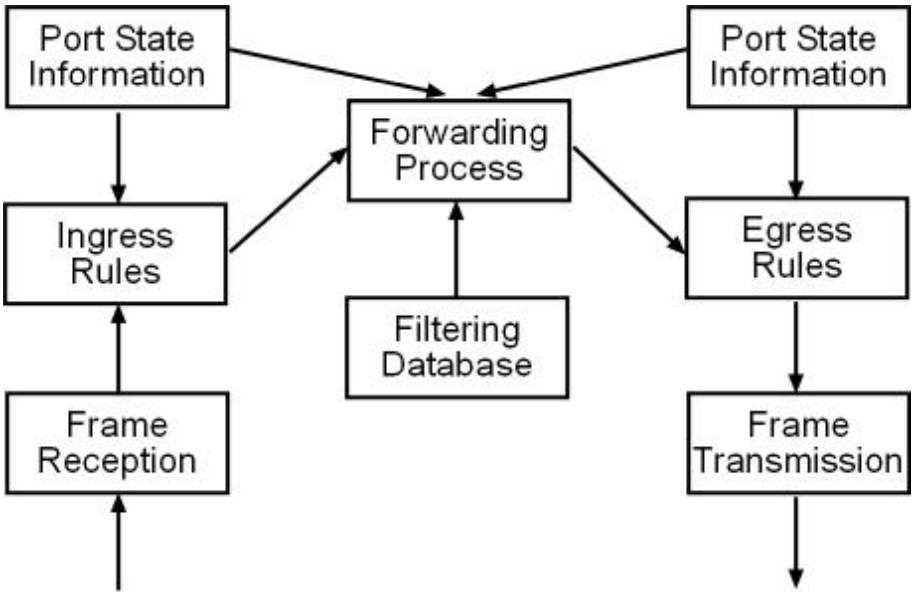


Fig. 3: **VLAN packet processing**

In the description of this process, we are going to use the term bridge. This description is equally valid for a switch. The process is as follows:

(1) The bridge receives a packet through one of its ports, either tagged (with VLAN information) or not.

(2) The bridge classifies the packet as belonging to a determined VLAN. If the packet does not have associated VLAN information, it is classified as belonging to the entry port's default VLAN.

(3) Depending on the entry port status (for bridges, if the port is blocked or not) and the *ingress rules* defined for

this port, the packet is either forwarded to the port through which it must be transmitted (*forwarding process*) or is dropped.

(4) The forwarding process, based on the different fields in the received packet (source and destination MAC fields, VLAN tag), checks the filter database to decide which ports are candidates to forward the received packet. If, for example, the packet is directed to an individual MAC address and, in the filter database, the port to reach said destination is stored, the packet can only be forwarded through this port.

(5) For each transmission candidate port, the bridge decides, depending on the *egress rules*, if the packet is effectively transmitted or dropped. In cases where the packet is sent, the tag is either sent or not, depending on the configuration associated to the port. In cases where the packet has to be sent tagged, it is sent with the VLAN tag corresponding to the classification given to the packet at entry.

Chapter 3 Feature Configuration

3.1 VLAN Feature Configuration Access

To access the VLAN feature configuration menu, use the **FEATURE VLAN** command in the general configuration menu.

Example:

```
Config>feature vlan

-- VLAN configuration --
VLAN config>
```

The VLAN feature configuration menu allows the Ethernet switch interface behavior to be configured with respect to the VLAN frames.

3.2 VLAN Feature Configuration

In accordance with the *Fig. 3* on page 5 scheme, it's possible to configure the behavior for a switch port:

- In the input, you can configure the default VLAN associated to the port. This way, if an untagged packet (i.e. one without VLAN identifier) is received, it is classified as pertaining to the default VLAN. The command to configure the default VLAN is **TAG-DEFAULT** .
- You can configure which ports are members of each VLAN through the VLAN command. The forwarding process selects all those VLAN port members where the input packet has been classified as candidate ports to forward the packet to.
- In the input, you can configure port behavior with respect to packets received with a VLAN identifier where the port is not a member. If the ingress filter is enabled, through the **INGRESS-FILTER** command, all packets received that are classified in a VLAN that the port is not a member of are dropped. Otherwise, the packets reach the forwarding process.
- In the output, you can configure how the packet is sent through the port. If you use the **TAG-INSERTION** command, the untagged packets are sent with the default tag associated to the packet input port (VLAN where the packet was classified in the input). If you use the **TAG-REMOVAL** command, tagged packets are sent without their tags.

Note

When configuring the VLAN feature in an Ethernet switch interface, it's a good idea to view this interface as an Ethernet interface internally connected to a switch. The switch port directly connected to the Ethernet interface is known as an internal port and is configured through the "internal" option in the configuration commands.

3.3 Restrictions applicable to the VLAN configuration

In some switches, specifically in the Kendins, you need to bear in mind some restrictions when configuring VLANs.

- Spanning Tree configuration in a switch port is incompatible with VLAN configuration in said port.
- In the internal port (the CPU connection port), you cannot configure *tag-insertion* or *tag-removal* in cases where you have configured Spanning Tree in another switch port.

3.4 VLAN Feature Configuration Commands

The commands available in the VLAN Feature configuration menu are as follows:

Command	Function
? (HELP)	Displays the commands available and their options.
ENABLE	Enables VLAN processing in all Ethernet interfaces with switch.
INGRESS-FILTER	Configures the ingress filter.
LIST	Displays the VLAN configuration.
NO	Sets the parameters with their default values.

TAG-DEFAULT	Configures a default VLAN identifier for untagged frames received through a port or through a combination of port and VLAN.
TAG-INSERTION	Enables tag insertion in the output for frames received without tags.
TAG-REMOVAL	Enables the removal of VLAN header for tagged frames when sent through a port.
VLAN	Configures VLANs in a port.
EXIT	Exits the VLAN feature configuration.

Note

In all commands needing the port identifier parameter over which these are established, it's possible to specify, apart from the external ports, a special port identified as "internal". This port is the connection internal port between the switch and the device.

3.4.1 ? (HELP)

Displays the list of available commands and their options.

Syntax:

```
VLAN config>?
```

Example:

```
VLAN config>?
  enable             Enables VLAN feature
  ingress-filter     Configures ingress filter on the interface/port
  list               Display VLAN configuration
  no                 Negate a command or set its defaults
  tag-default        Set a default VLAN ID for untagged packets on the incoming
                     interface/port
  tag-insertion      Enables tag insertion on untagged packets on the outgoing
                     interface/port
  tag-removal        Enables tag removal for tagged packets on the outgoing
                     interface/port or interface/port/VLAN vid
  vlan               Groups interface/port into a VLAN
  exit
VLAN config>
```

3.4.2 ENABLE

Enables VLAN processing in all Ethernet interfaces with switch.

Syntax:

```
VLAN config>enable
```

Example:

```
VLAN config>enable
VLAN config>
```

3.4.3 INGRESS-FILTER

Enables ingress filtering. Depending on the switch model, ingress filtering can be enabled on a port basis or globally for all ports in the switch. When ingress filtering is enabled, all frames tagged with a VLAN identifier for which the source port is not a member are dropped.

Syntax:

```
VLAN config>ingress-filter <interface>
      port [<port-id> | internal]
      <cr>
```

Example:

```
VLAN config>ingress-filter ethernet0/0 port 1
VLAN config>
```

Command history:

Release	Modification
11.00.03	The option to configure ingress-filter globally for the whole interface was introduced as of version 11.00.03.

3.4.4 LIST

Displays the VLAN configuration.

Syntax:

```
VLAN config>list
```

Example:

```
VLAN config>list
VLAN Feature : Enabled

VID     Interface       Port
--------------------------------
101     ethernet0/0     1
101     ethernet0/0     2
101     ethernet0/0     3
101     ethernet0/0     internal
102     ethernet0/0     4
102     ethernet0/0     internal

Interface           Port   Ing_Fil Tag_Ins Tag_Rmv  VID_def
-------------------------------------------------------------
ethernet0/0            1      Y       N       N      101
ethernet0/0            2      Y       N       N      101
ethernet0/0            3      Y       N       N      101
ethernet0/0            4      Y       N       N      102
ethernet0/0     internal      N       Y       N      1

VLAN config>
```

The following information is displayed:

- Global status of the VLAN feature in the interfaces with switch. If the *VLAN Feature* field indicates *Enabled*, the VLAN feature is activated in all interfaces with switch.
- Table containing member ports for each configured VLAN. For each configured VLAN identifier (*VID*), the member ports of this VLAN are indicated. In the example given, ports 1, 2, 3 and internal for ethernet0/0 interface are members of VLAN 101, while ports 4 and internal for the same interface are members of VLAN 102.
- Behavior table for each port. The following information is displayed for each port in an interface with switch:

  Ing_Fil: Ingress filter status. This indicates if only packets classified as pertaining to the VLANs where the port is a member are accepted, or if any packet can enter.

  Tag_Ins : Tag insertion. Indicates where the packets received without tagging are tagged before being sent through the port.

  Tag_Rmv : Removes the tag. Indicates if the VLAN tag should be removed from the tagged packets before they are sent through the port.

  VID_def: Default VLAN Identifier. This is used at the input to classify the packets that arrive without tags. This classification is subsequently used in the output to tag untagged packets.

3.4.5 NO

Disables configuration options or sets default values.

Syntax:

```
VLAN config>no ?
  enable            Enables VLAN feature
```

```
  ingress-filter    Configures ingress filter on the interface/port
  tag-default       Set a default VLAN ID for untagged packets on the incoming
                    interface/port
  tag-insertion     Enables tag insertion on untagged packets on the outgoing
                    interface/port
  tag-removal       Enables tag removal for tagged packets on the outgoing
                    interface/port
  vlan              Groups interface/port into a VLAN
VLAN config>
```

3.4.5.1 NO ENABLE

Disables VLAN processing in all Ethernet interfaces with switch.

Independently of the rest of the configured commands, VLAN programming is not executed over the switches.

Syntax:

```
VLAN config>no enable
```

3.4.5.2 NO INGRESS-FILTER

Deactivates the ingress filter in a port located in an interface with Ethernet switch.

Syntax:

```
VLAN config>no ingress-filter <interface> port [<port-id> | internal]
```

3.4.5.3 NO TAG-DEFAULT

Sets the default VLAN identifier for frames without tags to 1.

Syntax:

```
VLAN config>no tag-default <interface> port [<port-id> | internal]
```

3.4.5.4 NO TAG-INSERTION

Disables tag insertion in the output through a port for frames received without tags.

Syntax:

```
VLAN config>no tag-insertion <interface> port [<port-id> | internal]
```

3.4.5.5 NO TAG-REMOVAL

Disables the VLAN header elimination in the output through a port for tagged frames or a given VLAN.

Syntax:

```
VLAN config>no tag-removal <interface> port [<port-id> | internal]
```

Syntax:

```
VLAN config>no tag-removal <interface> port [<port-id> | internal] vlan <vid>
```

3.4.5.6 NO VLAN

Deletes a port from the list of VLAN members.

Syntax:

```
VLAN config>no vlan <vid> <interface> port [<port-id> | internal]
```

3.4.6 TAG-DEFAULT

Configures a default VID VLAN identifier for untagged frames received through a port. The default tag is used at entry to classify packets that arrive untagged. This classification is subsequently used in the output to tag untagged packets. Consequently, if an untagged frame is received through a port, it is associated to the default tag. This way, the frame is considered as belonging to the VLAN indicated by the default tag when deciding through which port it will be sent.

Syntax:

```
VLAN config>tag-default <interface> port [<port-id> | internal] <vid>
```

Example:

All frames received without tags through port 1 on the ethernet0/0 interface are associated to VLAN 101.

```
VLAN config>tag-default ethernet0/0 port 1 101
VLAN config>
```

3.4.7 TAG-INSERTION

Enables tagging at the output through a port for frames received without tags.

Syntax:

```
VLAN config>tag-insertion <interface> port [<port-id> | internal]
```

Example:

All frames leaving through port 3 on the ethernet0/0 interface are tagged.

```
VLAN config>tag-insertion ethernet0/0 port 3
VLAN config>
```

3.4.8 TAG-REMOVAL

Enables VLAN header elimination at the output through a port for tagged frames.

You can choose to remove the header from all the frames with VLAN tag, or remove the header from the indicated VLAN.

Consequently, the frames are sent untagged through the port, independently of whether they were received with or without tags.

3.4.8.1 TAG-REMOVAL PORT

Eliminates the VLAN header for VLAN frames that exit through this port.

Syntax:

```
VLAN config>tag-removal <interface> port [<port-id> | internal]
```

Example:

The frames leaving through port 4 on the ethernet0/0 interface are sent without tags, independently of whether they were received with or without tags.

```
VLAN config>tag-removal ethernet0/0 port 4
VLAN config>
```

3.4.8.2 TAG-REMOVAL VLAN

Eliminates the VLAN header for VLAN frames that exit through this port with the indicated VLAN identifier. This command allows tagged and untagged traffic to exist when going out through a determined port on an interface.

Syntax:

```
VLAN config> tag-removal <interface> port [<port-id> | internal] vlan <vid>
```

Example:

The frames leaving through port 4 on the ethernet0/0 interface that pertain to VLAN 100 are sent without tags.

```
VLAN config>tag-removal ethernet0/0 port 4 vid 100
VLAN config>
```

3.4.9 VLAN

Configures a given VLAN in a port on an interface with switch. I.e. a port is configured as a member of a given VLAN.

The device allows you to configure up to 16 different VLANs on one port.

Syntax:

```
VLAN config>vlan <vid> <interface> port [<port-id> | internal]
```

Example:

Configuration for port 1 on ethernet0/0 interface as pertaining to VLAN 101.

```
VLAN config>vlan 101 ethernet0/0 port 1
VLAN config>
```

3.4.10 EXIT

Exits the VLAN feature configuration.

Syntax:

```
VLAN config>exit
```

Example:

```
VLAN config>exit
Config>
```

Chapter 4 VLANs Bridge Configuration

4.1 Accessing the VLAN configuration in the Bridge

To access the VLAN configuration menu in the bridge, use the **VLAN** command at the configuration menu found in a bridge entity. For further information on configuring bridge in bintec devices, please see manual bintec-Dm 717-I “Bridge”.

Example:

```
Config>protocol asrt

-- ASRT Bridge user configuration --
ASRT config>vlan

802.1Q Bridge Configuration
ASRT VLAN Config>
```

From the VLAN configuration menu, it’s possible to configure the bridge behavior with respect to the VLAN frames.

4.2 VLANs Bridge Configuration

In accordance with the *Fig. 3* on page 5 scheme, the behavior for a bridge port can be configured:

- In the input, you can configure the default VLAN associated to the port. This way, if an untagged packet (i.e. one without VLAN identifier) is received, it is classified as pertaining to the default VLAN. The command to configure the default VLAN is **TAG-DEFAULT** .
- You can configure which ports are members of each VLAN through the **MEMBER** command. The forwarding process selects all VLAN port members where the input packet has been classified, as candidate ports to forward the packet to. This behavior can be modified through the **NO EGRESS-FILTER** command. If you use this command in a port, the port is the candidate to forward the packet independently of the VLANs it is a member of.
- In the input, you can configure port behavior with respect to packets received with a VLAN identifier where the port is not a member. If the ingress filter is enabled, through the **INGRESS-FILTER** command, all packets received that are classified in a VLAN that the port is not a member of are dropped. Otherwise, the packets reach the forwarding process.
- In the input, it’s possible to indicate that only tagged frames are accepted through the **ACCEPT-ONLY-TAGGED-FRAMES** command. This way, any frame without a VLAN header that’s received through the port is dropped.
- In the output, you can configure how the packet is sent through the port. If you use the **TAG-REMOVAL** command, tagged packets are sent without their tags.

Note

The difference between the VLAN feature configuration for switches and the bridge is that the TAG-REMOVAL command is used as the VLAN identifier, thus permitting to define which VLANs should be sent tagged and which ones not for each port.

- You can specify the associated VLAN identifier for the internally generated packets through the **INTERNAL-TAG** command. This identifier is used in the forwarding process to decide which ports are used to send these packets.

4.3 VLANs Bridge Configuration Commands

The commands available in the VLAN configuration menu in the bridge are as follows:

Command	Function
? (HELP)	Displays the available commands and their options.
ACCEPT-ONLY-TAGGED-FRAMES	Only allows tagged frames in a port.
EGRESS-FILTER	Configures egress filtering in a port.
ENABLE	Enables VLAN processing in the bridge.
INGRESS-FILTER	Configures ingress filtering in a port.

INTERNAL-TAG	Configures a default tag for internally generated packets.
MEMBER	Configures a VLAN in a port.
NO	Configures parameters with their default values.
PVST	Enables the PVST mode
TAG-DEFAULT	Configures a default VLAN identifier for untagged frames received through a port.
TAG-REMOVAL	Enables the removal of the VLAN header in tagged frames that are going to exit through a port.
EXIT	Exits the VLAN configuration in the bridge.

4.3.1 ? (HELP)

Displays the list of available commands and their options.

Syntax:

```
ASRT VLAN Config>?
```

Example:

```
ASRT VLAN Config>?
  accept-only-tagged-frames    Enable the accept-only-tagged-frames feature
  egress-filter                Enable the egress rule checking on a given port
  enable                       Enable the 802.1Q features of the bridge
  ingress-filter               Enable the ingress rule checking on a given port
  internal-tag                 Set the VLAN identifier for locally generated
                               packets
  member                       Adds a port to the member set of a given VLAN
  no                           Negate a command or set its defaults
  pvst                         Enable the pvst feature
  tag-default                  Set the default VLAN identifier for untagged
                               frames on a port
  tag-removal                  Enables tag removal on tagged packets on the
                               outgoing port
  exit
ASRT VLAN Config>
```

4.3.2 ACCEPT-ONLY-TAGGED-FRAMES

Configures a port so only tagged frames are permitted. Any frame received without a VLAN header is dropped.

Syntax:

```
ASRT VLAN Config>accept-only-tagged-frames port <port-id>
```

Example:

```
ASRT VLAN Config>accept-only-tagged-frames port 1
ASRT VLAN Config>
```

4.3.3 EGRESS-FILTER

Configures egress filtering in a port. This way, only frames classified as pertaining to a VLAN where the port is a member can exit through a port. This is the default behavior.

Syntax:

```
ASRT VLAN Config>egress-filter port <port-id>
```

Example:

```
ASRT VLAN Config>egress-filter port 2
ASRT VLAN Config>
```

4.3.4 ENABLE

Enables VLAN processing in the bridge.

Syntax:

```
ASRT VLAN Config>enable
```

4.3.5 INGRESS-FILTER

Activates ingress filtering in a bridge port. This way, all the frames that are received in the indicated port tagged with a VLAN identifier where the port is not a member are dropped.

Syntax:

```
ASRT VLAN Config>ingress-filter port <port-id>
```

Example:

```
ASRT VLAN Config>ingress-filter port 1
ASRT VLAN Config>
```

4.3.6 INTERNAL-TAG

Configures the default tag for internally generated packets. Packets internally generated in the device belong to the VLAN indicated through this command. Once the packet has been generated, the bridge deals with it as if it had been received through a special port, the internal port, in order to decide which ports the packet should be sent through.

Syntax:

```
ASRT VLAN Config>internal-tag vid <vid>
```

Example:

```
ASRT VLAN Config>internal-tag vid 102
ASRT VLAN Config>
```

4.3.7 MEMBER

Configures a given VLAN in a bridge port. I.e. a port is configured as a member of a determined VLAN.

Syntax:

```
ASRT VLAN Config>member port <port-id> vid <vid>
```

Example:

Configuration for port 1 as pertaining to VLAN 101.

```
ASRT VLAN Config>member port 1 vid 101
ASRT VLAN Config>
```

4.3.8 NO

Disables configuration options or sets default values.

Syntax:

```
ASRT VLAN Config>no ?
  accept-only-tagged-frames    Enable the accept-only-tagged-frames feature
  egress-filter                Enable the egress rule checking on a given port
  enable                       Enable the 802.1Q features of the bridge
  ingress-filter               Enable the ingress rule checking on a given port
  internal-tag                 Set the VLAN identifier for locally generated
                               packets
  member                       Adds a port to the member set of a given VLAN
  pvst                         Enable the pvst feature
  tag-default                  Set the default VLAN identifier for untagged
                               frames on a port
  tag-removal                  Enables tag removal on tagged packets on the
                               outgoing port
ASRT VLAN Config>
```

4.3.8.1 NO ACCEPT-ONLY-TAGGED-FRAMES

Configures a port so both tagged and untagged frames are permitted. Any frame without a VLAN header received in the port is classified as pertaining to the default VLAN associated to the port.

Syntax:

```
ASRT VLAN Config>no accept-only-tagged-frames port <port-id>
```

Example:

```
ASRT VLAN Config>no accept-only-tagged-frames port 1
ASRT VLAN Config>
```

4.3.8.2 NO EGRESS-FILTER

Deactivates egress filtering in a port. This way, frames classified as pertaining to a VLAN of which the port is not a member are permitted to exit through a port.

Syntax:

```
ASRT VLAN Config>no egress-filter port <port-id>
```

Example:

```
ASRT VLAN Config>no egress-filter port 2
ASRT VLAN Config>
```

4.3.8.3 NO ENABLE

Disables VLAN processing in the bridge.

Syntax:

```
ASRT VLAN Config>no enable
```

4.3.8.4 NO INGRESS-FILTER

Deactivates ingress filtering in a bridge port. This way, all the frames that are received in the indicated port tagged with a VLAN identifier are sent to the forwarding process, despite the port not being a member of said VLAN.

Syntax:

```
ASRT VLAN Config>no ingress-filter port <port-id>
```

Example:

```
ASRT VLAN Config>no ingress-filter port 1
ASRT VLAN Config>
```

4.3.8.5 NO INTERNAL-TAG

Disables default tag configuration for internally generated packets. The default tag when this command is used is 1.

Syntax:

```
ASRT VLAN Config>no internal-tag
```

4.3.8.6 NO MEMBER

Deletes a port from the list of VLAN members.

Syntax:

```
ASRT VLAN Config>no member port <port-id> vid <vid>
```

Example:

```
ASRT VLAN Config>no member port 1 vid 101
ASRT VLAN Config>
```

4.3.8.7 NO PVST

Disables the Per VLAN Spanning Tree protocol for bridges.

Syntax:

```
ASRT VLAN Config>no pvst
```

Command history:

Release	Modification
11.01.09	The *"no pvst"* command was introduced as of version 11.01.09.

4.3.8.8 NO TAG-DEFAULT

Sets the default VLAN identifier for frames without tags to 1.

Syntax:

```
ASRT VLAN Config>no tag-default port <port-id>
```

Example:

```
ASRT VLAN Config>no tag-default port 1
ASRT VLAN Config>
```

4.3.8.9 NO TAG-REMOVAL

Disables VLAN header elimination in tagged frames going to exit through a port.

VLAN header removal is defined by the VLAN identifier. This way, it's possible to configure the set of VLANs per port that you want to send with tags and the set of VLANs that you don't want tagged. By default, all packets exit tagged through a port (except those classified as belonging to VLAN 1). Given that VLAN 1 is the default VLAN for all ports, the bridge will send packets that were received with VLAN headers tagged (and packets received without a VLAN header untagged) unless you configure something.

Syntax:

```
ASRT VLAN Config>no tag-removal port <port-id> vid <vid>
```

Example:

Packets classified as pertaining to VLAN 123 must be tagged and sent through port 1.

```
SRT VLAN Config>no tag-removal port 1 vid 123
ASRT VLAN Config>
```

4.3.9 PVST

Enables the Per VLAN Spanning Tree protocol for bridges.

Syntax:

```
ASRT VLAN Config>pvst
```

Command history:

Release	Modification
11.01.09	The *"pvst"* command was introduced as of version 11.01.09.

4.3.10 TAG-DEFAULT

Configures a default *VID* VLAN identifier for untagged frames received through a port. The default tag is used in the entry to classify packets which arrived untagged. This classification is subsequently used in the output to tag untagged packets. Consequently, if an untagged frame is received through a port, it is associated to the default tag. The frame will be deemed to belong to the VLAN indicated by the default tag when deciding which ports it will be sent through.

Syntax:

```
ASRT VLAN Config>tag-default port <port-id> vid <vid>
```

Example:

All frames received without tags through port 1 are associated to VLAN 101.

```
ASRT VLAN Config>tag-default port 1 vid 101
ASRT VLAN Config>
```

4.3.11 TAG-REMOVAL

Enables VLAN header elimination at the output through a port for tagged frames. Consequently, the frames are sent untagged through the port, independently of whether they were received with or without tags.

VLAN header removal is defined by the VLAN identifier. This way, it's possible to configure the set of VLANs per port that you want to send with tags and the set of VLANs that you don't want tagged. By default, all the packets exit tagged through a port (except those classified as belonging to VLAN 1). Given that VLAN 1 is the default VLAN for all ports, the bridge will send all packets that were received with VLAN headers tagged (and packets received without a VLAN header untagged) unless you configure something.

Syntax:

```
ASRT VLAN Config>tag-removal port <port-id> vid <vid>
```

Example:

Packets classified as pertaining to VLAN 140 must be sent untagged through port 1.

```
SRT VLAN Config>tag-removal port 1 vid 140
ASRT VLAN Config>
```

4.3.12 EXIT

Exits VLAN configuration in the bridge.

Syntax:

```
ASRT VLAN Config>exit
```

Example:

```
ASRT VLAN Config>exit
Config>
```

Chapter 5 VLAN Monitoring

5.1 VLAN Feature Monitoring commands

The VLAN feature does not have its own monitoring commands.

You can obtain information from the VLAN tables stored in the switch by accessing interface monitoring. For further information over switch interfaces monitoring, please see manual bintec-Dm 709-I “LAN Interfaces”.

Example:

```
*monitor
Console Operator
+network ethernet1/0
--  Ethernet Console  --
ethernet1/0 ETH+?
  bitrate
  llc
  repeater
  status
  exit
ethernet1/0 ETH+repeater
-- Repeater Monitoring Console --
ethernet1/0 Repeater+list ?
  dynamic-mac-table
  remote-status
  sniffer
  static-mac-table
  stats
  status
  vlan-table
ethernet1/0 Repeater+list vlan-table
Entry  Membership  FilterID  VlanID
-----------------------------------
   1      0x1F         0        1
   2      0x1F         0        1
   3      0x1F         0        1
   4      0x1F         0        1
   5      0x1F         0        1
   6      0x1F         0        1
   7      0x1F         0        1
   8      0x1F         0        1
   9      0x1F         0        1
  10      0x1F         0        1
  11      0x1F         0        1
  12      0x1F         0        1
  13      0x1F         0        1
  14      0x1F         0        1
  15      0x1F         0        1
  16      0x1F         0        1
ethernet1/0 Repeater+
```

5.2 VLAN Bridge Monitoring Commands

Bridge does not have specific commands to monitor VLANs. In the commands used to display addresses learned by the bridge, the VLAN associated to each address is given. For further information, please see manual bintec-Dm 717-I “Bridge”.

Chapter 6 Examples

6.1 Scenario 1

A company in expansion has restructured some of its departments and wishes to optimize the resources on its internal network, which is made up of four departments. An IP subnet is assigned to each department: network 192.168.1.x corresponds to department A, network 192.168.2.x to B, network 192.168.3.x to C and network 192.168.4. to D.

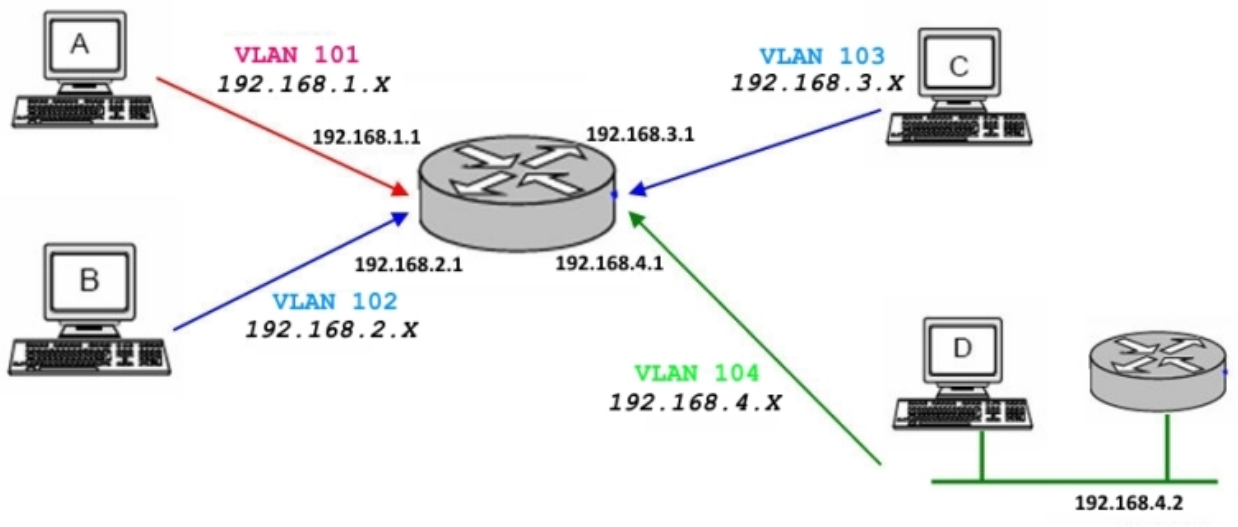


Fig. 4: **Scenario 1**

The network has been created in such a way that there are four LAN segments, each one with the stations for a department. There is one exception to this; in department C's segment, there is a station belonging to department A.

Additionally, IP connectivity between all the subnets associated to departments A, B and D is necessary. These three subnets will also be able to access the outside through a gateway located in subnet D and address 192.168.4.2.

Otherwise, devices set up at department C cannot access the exterior and have no access to departments A, B and D either.

6.2 Scenario 1 Configuration

We're going to configure a VLAN for each department, allowing us to isolate traffic between departments without renouncing connectivity between them.

In order to allow routing between the different company subnets, Ethernet subinterfaces are used. (Please see manual bintec-Dm 760-I Ethernet Subinterface).

Ethernet subinterfaces are created for all subnets that require IP connectivity. In this case, we just need to create three Ethernet subinterfaces associated to departments A, B and D.

```
Config>add device eth-subinterface ethernet1/0 1
Config>add device eth-subinterface ethernet1/0 2
Config>add device eth-subinterface ethernet1/0 4
```

IP addresses are assigned to the chosen interfaces and the default routes (in this case, a gateway located on department D's subnet).

```
Config>protocol ip
-- Internet protocol user configuration --
IP config>show config
; Showing Menu and Submenus Configuration for access-level 15 ...
; C9i+ IPSec SNA VoIP Router 14 24 Version 10.6.29-Alfa
;
   address ethernet1/0.1 192.168.1.1 255.255.255.0
   address ethernet1/0.2 192.168.2.1 255.255.255.0
   address ethernet1/0.4 192.168.4.1 255.255.255.0
;
```

```
;
   route 0.0.0.0 0.0.0.0 192.168.4.2
;
IP config>
```

We still need to associate the IP addresses with the VLAN identifiers used in each department. We also need to assign a different MAC to each subinterface.

```
network ethernet1/0.1
; -- Config of the Ethernet Subinterface --
   description "Department A"
   encapsulation dot1q 101
;
;
   mac-address 02-00-00-aa-aa-aa
;
exit
;
network ethernet1/0.2
; -- Config of the Ethernet Subinterface --
   description "Department B"
   encapsulation dot1q 102
;
;
   mac-address 02-00-00-bb-bb-bb
;
exit
;
network ethernet1/0.4
; -- Config of the Ethernet Subinterface --
   description "Department D"
   encapsulation dot1q 104
;
;
   mac-address 02-00-00-dd-dd-dd
exit
```

The physical addresses assigned to the subinterfaces are advertised.

```
Config>protocol arp
-- ARP user configuration --
ARP config>show config
; Showing Menu and Submenus Configuration for access-level 15 ...
; C9i+ IPSec SNA VoIP Router 14 24 Version 10.6.29-Alfa

   entry ethernet1/0.1 192.168.1.1 02-00-00-aa-aa-aa public
   entry ethernet1/0.2 192.168.2.1 02-00-00-bb-bb-bb public
   entry ethernet1/0.4 192.168.4.1 02-00-00-dd-dd-dd public
ARP config>
```

Lastly, we need to configure switch behavior depending on the different VLANs. In this case, let's assume that all the devices are capable of generating and receiving VLAN frames (except for those located in department B's segment). In this latter segment, there is an old computer that can't understand traffic with VLAN headers.

When configuring the switch behavior, you must be very clear about the structure of the VLANs.

Firstly, we need to define which ports should be members of which VLANs. Initially, each switch port is associated to a VLAN, so we simply need to define each port as belonging to the department VLAN. However, department A has expanded over the length of two network segments, connected to ports 1 and 3.

Therefore:

- Port 1 must be a member of VLAN 101, associated to department A.
- Port 2 must be a member of VLAN 102, associated to department B.
- Port 3 must be a member of VLANs 101 and 103, associated to departments A and C.
- Port 4 must be a member of VLAN 104, associated to department D.

```
Config>feature vlan

-- VLAN configuration --
```

```
VLAN config>vlan 101 ethernet1/0 port 1
VLAN config>vlan 102 ethernet1/0 port 2
VLAN config>vlan 103 ethernet1/0 port 3
VLAN config>vlan 104 ethernet1/0 port 4
VLAN config>vlan 101 ethernet1/0 port 3
```

With this configuration, we can ensure layer 2 traffic associated to each VLAN is only forwarded to the other LAN segment for VLAN 101, through which the two different physical segments need to communicate.

Now we need to do the routing part. As already said, we want departments A, B and D to communicate at IP level. To do this, traffic from these three departments must reach the router to be routed. For this to happen, the internal port (which acts as the connection port between the router Ethernet interface and the switch) must belong to the VLANs of departments A, B and D .

```
VLAN config>vlan 101 ethernet1/0 port internal
VLAN config>vlan 102 ethernet1/0 port internal
VLAN config>vlan 104 ethernet1/0 port internal
```

Consequently, the traffic from departments A and D reach the corresponding port tagged. This traffic is then resent through VLAN port members, including the internal port. What happens to the traffic from department B? As indicated, the traffic for this department circulates without being tagged over the LAN segment. For the router to classify this in the appropriate VLAN, the switch needs to either add or remove VLAN tags as follows:

- when the traffic comes in through port 2, it must be classified as pertaining to VLAN 102:

```
VLAN config>tag-default ethernet1/0 port 2 102
```

- when the traffic exits through port 2, the VLAN tag should be removed so the stations can understand the traffic.

```
VLAN config>tag-removal ethernet1/0 port 2
```

- additionally, the traffic that comes in through port 2 untagged must reach the router's Ethernet interface tagged so the IP layer operates correctly. Therefore, untagged packets must be tagged at the internal port output.

```
VLAN config>tag-insertion ethernet1/0 port internal
```

Finally, we need to globally enable the VLAN feature. In addition, we'll enable the ingress filter so odd traffic from non-configured VLANs is rejected.

```
VLAN config>enable
VLAN config>ingress-filter ethernet1/0 port 1
VLAN config>ingress-filter ethernet1/0 port 2
VLAN config>ingress-filter ethernet1/0 port 3
VLAN config>ingress-filter ethernet1/0 port 4
```

The VLAN configuration now looks like this:

```
VLAN config>show config
; Showing Menu and Submenus Configuration for access-level 15 ...
; XXX Router 7 96 Version 10.7.4-Alfa
      enable
;
      vlan 101 ethernet1/0 port 1
      vlan 101 ethernet1/0 port 3
      vlan 101 ethernet1/0 port internal
      vlan 102 ethernet1/0 port 2
      vlan 102 ethernet1/0 port internal
      vlan 103 ethernet1/0 port 3
      vlan 104 ethernet1/0 port 4
      vlan 104 ethernet1/0 port internal
;
      ingress-filter ethernet1/0 port 1
      ingress-filter ethernet1/0 port 2
      ingress-filter ethernet1/0 port 3
      ingress-filter ethernet1/0 port 4
;
      tag-default ethernet1/0 port 2 102
;
      tag-insertion ethernet1/0 port internal
;
      tag-removal ethernet1/0 port 2
;
```

```
VLAN config>list

VLAN Feature : Enabled

VID     Interface       Port
--------------------------------
101     ethernet1/0     1
101     ethernet1/0     3
101     ethernet1/0     internal
102     ethernet1/0     2
102     ethernet1/0     internal
103     ethernet1/0     3
104     ethernet1/0     4
104     ethernet1/0     internal

Interface           Port   Ing_Fil Tag_Ins Tag_Rmv Tag_Def  VID_def
-----------------------------------------------------------
ethernet1/0            1      Y       N       N       N      1
ethernet1/0            2      Y       N       Y       Y      102
ethernet1/0            3      Y       N       N       N      1
ethernet1/0            4      Y       N       N       N      1
ethernet1/0     internal      N       Y       N       N      1

VLAN config>
```

And the complete configuration is as follows:

```
Config>show config
; Showing Menu and Submenus Configuration for access-level 15 ...
; XXX Router 7 96 Version 10.7.4-Alfa

   log-command-errors
   no configuration
   add device eth-subinterface ethernet1/0 1
   add device eth-subinterface ethernet1/0 2
   add device eth-subinterface ethernet1/0 4
;
;
;
;
;
;
   network ethernet1/0.1
; -- Config of the Ethernet Subinterface --
      description "Department A"
;
      ip address 192.168.1.1 255.255.255.0
;
;
;
;
      encapsulation dot1q 101
;
;
      mac-address 02-00-00-aa-aa-aa
;
   exit
;
   network ethernet1/0.2
; -- Config of the Ethernet Subinterface --
      description "Department B"
;
      ip address 192.168.2.1 255.255.255.0
;
;
;
;
      encapsulation dot1q 102
```

```
;
;
      mac-address 02-00-00-bb-bb-bb
;
   exit
;
   network ethernet1/0.4
; -- Config of the Ethernet Subinterface --
      description "Department D"
;
      ip address 192.168.4.1 255.255.255.0
;
;
;
;
      encapsulation dot1q 104
;
;
      mac-address 02-00-00-dd-dd-dd
;
   exit
;
;
   protocol ip
; -- Internet protocol user configuration --
      route 0.0.0.0 0.0.0.0 192.168.4.2
;
;
   exit
;
   protocol arp
; -- ARP user configuration --
      entry ethernet1/0.1 192.168.1.1 02-00-00-aa-aa-aa public
      entry ethernet1/0.2 192.168.2.1 02-00-00-bb-bb-bb public
      entry ethernet1/0.4 192.168.4.1 02-00-00-dd-dd-dd public
   exit
;
;
;
   feature vlan
; -- VLAN configuration --
      enable
;
      vlan 101 ethernet1/0 port 1
      vlan 101 ethernet1/0 port 3
      vlan 101 ethernet1/0 port internal
      vlan 102 ethernet1/0 port 2
      vlan 102 ethernet1/0 port internal
      vlan 103 ethernet1/0 port 3
      vlan 104 ethernet1/0 port 4
      vlan 104 ethernet1/0 port internal
;
      ingress-filter ethernet1/0 port 1
      ingress-filter ethernet1/0 port 2
      ingress-filter ethernet1/0 port 3
      ingress-filter ethernet1/0 port 4
;
      tag-default ethernet1/0 port 2 102
;
      tag-insertion ethernet1/0 port internal
;
      tag-removal ethernet1/0 port 2
;
   exit
;
   dump-command-errors
   end
```

6.3 Scenario 2

The aim here is to make VLAN configuration commands easier to understand through an example. The office LAN in this example consists of three computers connected to an access WAN port. The internal port is the one used by the router for routing and security purposes.

The scheme is as follows:

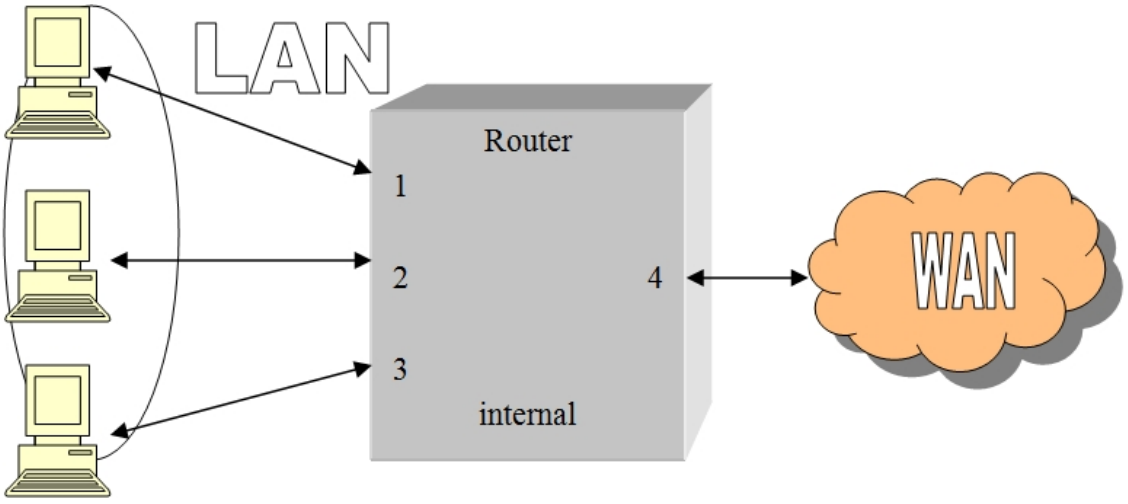


Fig. 5: **Scenario 2**

In order to resolve the separation between the internal LAN and the external WAN, we are going to configure 2 different VLANs. The first one includes all the LAN ports and the internal router port (VLAN ID 101). The second one includes the internal port and WAN port number 4 (VLAN ID 102) in the example.

The internal port is going to act as “gatekeeper”, i.e. all traffic originating from the LAN with WAN destination and vice versa must go through the internal interface, without interfering with the traffic between the devices pertaining to the same LAN.

Moreover, with this configuration, all the broadcast and multicast packets from the router's internal port are sent to the LAN and the WAN VLAN. When it comes to the rest, only broadcast and multicast packets are sent to ports pertaining to their VLAN. This means that LAN-ARP packets do not leave through the WAN.

6.4 Scenario 2 Configuration

1.- Access the VLAN feature configuration.

```
Config>feature vlan

-- VLAN configuration -
VLAN config>
```

2.- Globally enable the VLAN functionalities.

```
VLAN config>enable
VLAN config>
```

3.- Configure ports 1, 2, 3 and the internal port as pertaining to VLAN 101.

```
VLAN config>vlan 101 ethernet0/0 port 1
VLAN config>vlan 101 ethernet0/0 port 2
VLAN config>vlan 101 ethernet0/0 port 3
VLAN config>vlan 101 ethernet0/0 port internal
VLAN config>
```

4.- Configure port 4 and the internal port as pertaining to VLAN 102.

```
VLAN config>vlan 102 ethernet0/0 port 4
VLAN config>vlan 102 ethernet0/0 port internal
VLAN config>
```

5.- Configure ports 1, 2 and 3 with default VLAN (101). This way, the VLAN tag can be added to the untagged packets received (those that are not VLAN).

```
VLAN config>tag-default ethernet0/0 port 1 101
VLAN config>tag-default ethernet0/0 port 2 101
VLAN config>tag-default ethernet0/0 port 3 101
VLAN config>
```

6.- Configure ingress filtering on ports 1, 2 and 3. This means that all packets which do not pertain to the VLAN configured in these ports will be discarded.

```
VLAN config>ingress-filter ethernet0/0 port 1
VLAN config>ingress-filter ethernet0/0 port 2
VLAN config>ingress-filter ethernet0/0 port 3
VLAN config>
```

7.- Configure VID 102 as the default VLAN on port 4.

```
VLAN config>tag-default ethernet0/0 port 4 102
VLAN config>
```

8.- Configure ingress filtering on port 4.

```
VLAN config>ingress-filter ethernet0/0 port 4
VLAN config>
```

9.- Configure tag-insertion on the router's internal port. This will allow the default VLAN-ID from the incoming port to be inserted for all packets destined to the internal interface.

```
VLAN config>tag-insertion ethernet0/0 port internal
VLAN config>
```

10.- The router must tag all packets sent through the internal port.

11.- The final configuration can be seen using the **list** command.

```
VLAN config>list
VLAN Feature : Enabled

VID     Interface       Port
--------------------------------
101     ethernet0/0     1
101     ethernet0/0     2
101     ethernet0/0     3
101     ethernet0/0     internal
102     ethernet0/0     4
102     ethernet0/0     internal

Interface           Port   Ing_Fil Tag_Ins Tag_Rmv Tag_Def  VID_def
-------------------------------------------------------------------
ethernet0/0            1      Y       N       N       Y      101
ethernet0/0            2      Y       N       N       Y      101
ethernet0/0            3      Y       N       N       Y      101
ethernet0/0            4      Y       N       N       Y      102
ethernet0/0     internal      N       Y       N       N      1

VLAN config>
```

12.- You can also see the necessary commands through the **show config** command:

```
VLAN config>show config
; Showing Menu and Submenus Configuration ...
; Router Cxx YY ZZ Version 10.X.XXTM

   enable
;
   vlan 101 ethernet0/0 port 1
   vlan 101 ethernet0/0 port 2
   vlan 101 ethernet0/0 port 3
   vlan 101 ethernet0/0 port internal
   vlan 102 ethernet0/0 port 4
   vlan 102 ethernet0/0 port internal
;
   ingress-filter ethernet0/0 port 1
```

```
   ingress-filter ethernet0/0 port 2
   ingress-filter ethernet0/0 port 3
   ingress-filter ethernet0/0 port 4
;
   tag-default ethernet0/0 port 1 101
   tag-default ethernet0/0 port 2 101
   tag-default ethernet0/0 port 3 101
   tag-default ethernet0/0 port 4 102
;
   tag-insertion ethernet0/0 port internal
;
VLAN config>
```