VLANs

This chapter provides information on configuring virtual local area networks (VLANs) in support of enhanced or extended services. Product-specific and feature-specific *Administration Guides* provide examples and procedures for configuration of services on the system that may utilize VLANs. You should select the configuration example that best meets your service model before using the procedures described below.

Overview

Virtual LANs (VLANs) provide greater flexibility in the configuration and use of contexts and services.

They are configured as "tags" on a per-port basis and allow more complex configurations to be implemented. The VLAN tag allows a single physical port to be bound to multiple logical interfaces that can be configured in different contexts. Therefore, each Ethernet port can be viewed as containing many logical ports when VLAN tags are employed.

VLANs can be created at the hypervisor and StarOS levels. Where you create the VLAN depends on your specific network requirements.

Overlapping IP Address Pool Support – GGSN

Overlapping IP Address pools allow operators to more flexibly support multiple corporate VPN customers with the same private IP address space without expensive investments in physically separate routers or virtual routers.

The system supports two types of overlapping pools:

- *Resource* pools are designed for dynamic assignment only, and use a VPN tunnel (such as a GRE tunnel) to forward and receive the private IP addresses to and from the VPN.
- *Overlap* pools can be used for both dynamic and static addressing, and use VLANs and a next hop forwarding address to connect to the VPN customer.

To forward downstream traffic to the correct PDP context, the GGSN uses either the GRE tunnel ID or the VLAN ID to match the packet. When forwarding traffic upstream, the GGSN uses the tunnel and forwarding information in the IP pool configuration; overlapping pools must be configured in the APN in such instances.

When a PDP context is created, the IP address is assigned from the IP pool. In this case the forwarding rules are also configured into the GGSN. If the address is assigned statically, when the GGSN confirms the IP address from the pool configured in the APN, the forwarding rules are also applied.

The GGSN can scale to as many actual overlapping pools as there are VLAN interfaces per context, and there can be multiple contexts per GGSN. The limit is the number of IP pools. This scalability allows operators who wish to provide VPN services to customers using the customer's private IP address space, not to be concerned about escalating hardware costs or complex configurations.

RADIUS VLAN Support – Enhanced Charging Services

VPN customers often use private address space which can easily overlap with other customers. The subscriber addresses are supported with overlapping pools which can be configured in the same virtual routing context.

RADIUS Server and NAS IP addresses do not need to be in separate contexts, thereby simplifying APN and RADIUS configuration and network design. This feature allows the following scenarios to be defined in the same context:

- Overlapping RADIUS NAS-IP addresses for various RADIUS server groups representing different APNs.
- Overlapping RADIUS server IP addresses for various RADIUS servers groups.

Every overlapping NAS-IP address is given a unique next-hop address which is then bound to an interface that is bound to a unique VLAN, thereby allowing the configuration to exist within the same context.

The system forwards RADIUS access requests and accounting messages to the next hop defined for that NAS-IP; the connected routers forward the messages to the RADIUS server. The next hop address determines the interface and VLAN to use. Traffic from the server is identified as belonging to a certain NAS-IP by the port/VLAN combination.

The number of RADIUS NAS-IP addresses that can be configured is limited by the number of loopback addresses that can be configured.

APN Support – PDN Gateway (P-GW)

P-GW Access Point Name (APN) supports extensive parameter configuration flexibility for the APN. VLAN tagging may be selected by the APN, but are configured in the P-GW independently from the APN.

VLANs and StarOS

VLANs and Hypervisors

Depending on the type of packets being processed over the network, the hypervisor performs different VLAN tasks prior to exchanging packets with the UGP virtual machine (VM).

- **Management packets** MGMT packets arrive untagged and the hypervisor exchanges these packets with the VM without additional VLAN processing.
- **Access packets** arrive from the physical network with VLAN tags. The hypervisor removes the VLAN tags before forwarding them to a VM. It retags the received packets prior to sending them out across the physical network.
- **Trunking** packets arrive and depart across the physical network with VLAN tags. The hypervisor filters the tags before sending tagged packets to the VM for additional processing.

Management, access and trunking packets should be defined in separate contexts and bound to unique interfaces. The hypervisor should be configured to provide the appropriate type of VLAN tagging or filtering based on the packet type.

Refer to the following sections for a brief description of VLAN support and sources for additional information.

- VLANs and KVM Hypervisor, on page 3
- VLANs and VMware, on page 4

VLANs and KVM Hypervisor

Network Isolation

The Ubuntu networking stack implementation allows the KVM host to act as a simple layer 2 bridge (that is, an Ethernet switch), a forwarding or NAT router, a stateful firewall, or any combination of those roles.

VLANs versus Bridged Interfaces

In the KVM virtualization scenario, VLAN usage can be seen as an extension to the simple bridge interface sharing. The difference lies in which interface participates in the bridge set. In the standard mode of operation (as seen in the examples in Network port sharing with Ethernet bridges), the physical interfaces (such as eth0,

eth1...) are bound to the bridge, which is used by each guest. These interfaces carry unmodified packets coming externally or being generated internally, with or without a VLAN ID tag.

It is possible to filter out every package not carrying a particular VLAN ID by creating subinterfaces. These subinterfaces become part of the VLAN defined by a specific VLAN ID.

Applying this concept to the bridged interface sharing method involves replacing the bound physical interface by a subinterface that is part of a particular VLAN segmentation. This way, every virtual machine guest with interfaces bound to this bridge is part of that particular VLAN. Like in the simple Ethernet bridge environment, the network provided is transparent.

Note Not all vNIC types support VLAN trunking into a bridge, as many filter out VLANs in hardware.

Additional Information

For additional information on configuring VLANs with the KVM hypervisor see the URLs below:

- *Configuring 802.1q VLANs:* https://www.ibm.com/support/knowledgecenter/linuxonibm/liaat/liaatkvmsecconfvlans.htm
- *KVM/Networking:* https://help.ubuntu.com/community/KVM/Networking

VLANs and VMware

VMware supports the configuration of VLANs to meet network deployment requirements.

VLAN Configuration

VLANs enable a single physical LAN segment to be further segmented so that groups of ports are isolated from one another as if they were on physically different segments.

Configuring ESXi with VLANs is recommended for the following reasons:

- It integrates the host into a pre-existing environment.
- It integrates the host into a pre-existing environment.
- It reduces network traffic congestion.
- iSCSI traffic requires an isolated network.

You can configure VLANs in ESXi using three methods: External Switch Tagging (EST), Virtual Switch Tagging (VST), and Virtual Guest Tagging (VGT).

- With EST, all VLAN tagging of packets is performed on the physical switch. Host network adapters are connected to access ports on the physical switch. Port groups that are connected to the virtual switch must have their VLAN ID set to 0.

With VST, all VLAN tagging of packets is performed by the virtual switch before leaving the host. Host network adapters must be connected to trunk ports on the physical switch. Port groups that are connected to the virtual switch must have an appropriate VLAN ID specified.

With VGT, all VLAN tagging is performed by the virtual machine. For VGT the VLAN ID = 4095. VLAN tags are preserved between the virtual machine networking stack and external switch when frames are passed to and from virtual switches. Physical switch ports are set to trunk port.

Additional Information

For additional information on configuring VLANs with the VMware hypervisor see the documents below:

- Configuring VLANs on UCS and VMware
- VLAN Configuration
- Assign a VLAN ID to an ESXi Host
- VLAN configuration on virtual switches, physical switches and virtual machines (1003806)

Creating VLAN Tags

Use the following example to create VLANs on a port and bind them to pre-existing interfaces. For information on creating interfaces, refer to *System Interfaces and Ports*.

config
  port ethernet *slot/port*
    no shutdown
    vlan *vlan_tag_ID*
    no shutdown
    bind interface *interface_name context_name*
    end

Notes:

- *Optional:* Configure VLAN-subscriber associations. Refer to Configuring Subscriber VLAN Associations, on page 6 for more information.
- Repeat this procedure as needed to configure additional VLANs for the port.
- Refer to VLAN-Related CLI Commands , on page 7 and the *Command Line Interface Reference* for additional information.
- Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Verifying the Port Configuration

Run the following command to verify the port configuration:

`[local]`*host_name*`#` **show port info** *slot/port*

An example of this command's output when at least one VLAN has been configured for the port is shown below:

```
Port: 5/11
  Port Type               : 10G Ethernet
  Role                    : Service Port
  Description             : (None Set)
  Redundancy Mode         : Port Mode
  Redundant With          : 6/11
  Preferred Port          : Non-Revertive
  Physical ifIndex        : 85262336
  Administrative State    : Enabled
  Configured Duplex       : Auto
  Configured Speed        : Auto
  Fault Unidirection Mode : 802_3ae clause 46
  Configured Flow Control : Enabled
  Interface MAC Address   : 64-9E-F3-69-5B-EA
  SRP Virtual MAC Address : None
  Fixed MAC Address       : 64-9E-F3-69-5B-CA
  Link State              : Up
  Link Duplex             : Full
  Link Speed              : 10 Gb
  Flow Control            : Enabled
  Link Aggregation Group  : None
  Untagged:
    Logical ifIndex       : 85262337
    Operational State     : Up, Active
  Tagged VLAN: VID 10
    Logical ifIndex       : 285278210
    VLAN Type             : Standard
    VLAN Priority         : 0
    Administrative State  : Enabled
    Operational State     : Up, Active
  Number of VLANs         : 1
  SFP Module              : Present (10G Base-SR)
```

Notes:

- Repeat this sequence as needed to verify additional ports.
- *Optional:* Configure VLAN-subscriber associations. Refer to Configuring Subscriber VLAN Associations, on page 6 for more information.
- Refer to VLAN-Related CLI Commands , on page 7 for additional information.
- Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Configuring Subscriber VLAN Associations

Subscriber traffic can be routed to specific VLANs based on the configuration of their user profile. This functionality provides a mechanism for routing all traffic from a subscriber over the specified VLAN. All packets destined for the subscriber must also be sent using only IP addresses valid on the VLAN or they will be dropped.

RADIUS Attributes Used

The following RADIUS attributes can be configured within subscriber profiles on the RADIUS server to allow the association of a specific VLAN to the subscriber:

- **SN-Assigned-VLAN-ID:** In the Starent VSA dictionary
- **SN1-Assigned-VLAN-ID:** In the Starent VSA1 dictionary

Important Since the instructions for configuring subscriber profiles differ between RADIUS server applications, this section only describes the individual attributes that can be added to the subscriber profile. Please refer to the documentation that shipped with your RADIUS server for instructions on configuring subscribers.

Configuring Local Subscriber Profiles

Use the configuration example below to configure VLAN associations within local subscriber profiles on the system.

Important These instructions assume that you have already configured subscriber-type VLAN tags according to the instructions provided in Creating VLAN Tags, on page 5.

```
config
    context context_name
        subscriber name user_name
            ip vlan vlan_id
            end
```

Verify the Subscriber Profile Configuration

Use the following command to view the configuration for a subscriber profile:

`[local]`*host_name*`#` **show subscriber configuration username** *user_name*

Notes:

- Repeat this command for each subscriber.
- Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

VLAN-Related CLI Commands

VLAN-related features and functions are supported across several CLI command modes. The following tables identify commands associated with configuration and monitoring of VLAN-related functions.

For detailed information regarding the use of the commands listed below, see the *Command Line Interface Reference*.

Table 1: VLAN-Related Configuration Commands

CLI Mode	Command	Description
AAA Server Group Configuration Mode	**radius attribute nas-ip-address address** *ip_address* **nexthop-forwarding-address** *ip_address* **vlan** *vlan_id*	Sets the RADIUS client to provide the VLAN ID with the nexthop forwarding address to a system when running in single nexthop gateway mode. **Note:** To access the **vlan** keyword, **aaa-large configuration** must be enabled via the Global Configuration mode.
ACS Charging Action Configuration Mode	**ip vlan** *vlan_id*	Configures the VLAN identifier to be associated with the subscriber traffic in the destination context.
Context Configuration Mode	**ip pool** *pool_name* **nexthop forwarding address** *ip_address* **overlap vlanid** *vlan_id*	When a nexthop forwarding address is configured, the **overlap vlanid** keyword enables support for overlapping IP address pools and associates the pool with the specified VLAN ID.
Context Configuration Mode	**ip routing overlap-pool**	Advertises overlap-pool addresses in dynamic routing protocols when overlap pools are configured using VLAN IDs. When enabled, the overlap addresses are added as interface addresses and advertised.
Context Configuration Mode	**radius attribute nas-ip-address address** *ip_address* **nexthop-forwarding-address** *ip_address* **vlan** *vlan_id*	Specifies the VLAN ID to be associated with the next-hop IP address.
Ethernet Interface Configuration Mode	**[no] logical-port-statistics**	Enables or disables the collection of logical port (VLAN and NPU) bulk statistics for the first 32 configured Ethernet or PVC interface types.
Ethernet Interface Configuration Mode	**vlan-map next-hop** *ipv4_address*	Sets a single next-hop IP address so that multiple VLANs can use a single next-hop gateway. The vlan-map is associated with a specific interface.
Ethernet Port Configuration Mode	**vlan** *vlan_id*	Enters VLAN Configuration mode.
PVC Configuration Mode	**[no] shutdown**	Enables or disables traffic over a specified VLAN. See below.

CLI Mode	Command	Description
Subscriber Configuration Mode	**ip vlan** *vlan_id*	Configures the subscriber VLAN ID that is used with the assigned address for the subscriber session to receive packets. If the IP pool from which the address is assigned is configured with a VLAN ID, this subscriber configured VLAN ID overrides it.
VLAN Configuration Mode	**bind interface** *interface_name context_name*	Binds a virtual interface and context to support VLAN service.
VLAN Configuration Mode	**[no] ingress-mode**	Enables or disables port ingress incoming) mode.
VLAN Configuration Mode	**priority** *value*	Configures an 802.1p VLAN priority bit for ASN-GW service only.
VLAN Configuration Mode	**[no] shutdown**	Enables or disables traffic over the current VLAN.
VLAN Configuration Mode	**vlan-map interface** *if_name context_name*	Associates an IP interface having a VLAN ID with a context.

Table 2: VLAN-Related Monitoring Commands

CLI Mode	Command	Description
Exec Mode show commands	**clear port** *slot/port* **vlan** *vlan_id*	Clears NPU statistics for the port that has a previously configured VLAN ID.
Exec Mode show commands	**show logical-port utilization table vlan { 5-minute | hourly }**	Displays VLAN utilization for a specified collection interval.
Exec Mode show commands	**show port info** *slot/port* **vlan** *vlan_id*	Displays NPU counters for a previously configured VLAN ID.