Содержание

VLAN Traffic Handling

The `vlan group` data has been moved from UDR to SDR. Global rules for `vlan drop`, `vlan pass`, `vlan hide`, `vlan permit` previously set by the old CLI command `vlan group` have been converted and moved from UDR to SDR, being removed from UDR.

1. Drop traffic without analysis from a specific VLAN:

   ```
   fdpi_cli vlan rule add <id> perm drop
   ```

2. Drop traffic with preliminary analysis but without passing it to Netflow statistics from a specific VLAN (Used for asymmetric traffic when a copy of traffic from another site is fed to the site. It is necessary to analyze and drop the traffic so that it does not end up in statistics):

   ```
   fdpi_cli vlan rule add <id> perm hide
   ```

3. Pass traffic without any analysis from a specific VLAN:

   ```
   fdpi_cli vlan rule add <id> perm pass
   ```

4. Display existing settings in UDR:

   ```
   fdpi_cli vlan rule dump
   ```

   To display rules of only a specific type (e.g., only `perm`), the `[type]` parameter is used:

   ```
   fdpi_cli vlan rule dump perm
   ```

   Example command output:

   ```
   # fdpi_cli vlan rule dump
   1000  perm hide
   2000  perm drop
   3000  perm pass
   4000  perm hide
   ```

   In this example, all protocols related to VLAN 1000 and 4000 are subject to hide, i.e., traffic from one site is duplicated to another site; VLAN 2000 — traffic is dropped, VLAN 3000 — traffic is passed.

For more details, see the section Configuring Service-Name for VLAN

VLAN Rule

VLAN Rule allows flexible management of network traffic at the VLAN and QinQ level, assigning specific packet processing policies for individual VLANs, VLAN ranges, or QinQ tunnels.

Rule Types

The following rule types are supported:

- `dhcp` — controls DHCP request processing.
  - `dhcp enable` — allow DHCP request processing in this VLAN/QinQ.
  - `dhcp disable` — disable DHCP processing. All DHCP packets in this VLAN/QinQ will be dropped.
- `perm` — defines basic processing of all traffic in VLAN/QinQ.
  - `drop` — completely discard all packets. Packets do not undergo further processing and do not go to Netflow statistics.
  - `pass` — pass packets without processing. Packets are counted in Netflow statistics.
  - `accept` — pass packets for further full processing in the system. Packets are counted in Netflow statistics.
  - `hide` — the packet goes through internal processing stages (with exceptions), but after processing it is always discarded. At the same time:
    - the packet does not go to Netflow statistics;
    - services 9, 12, 15, 18, NAT, as well as policing (general and channel) are not applied;
    - the packet is not written via ajb — to IPFIX, SIP, FTP, etc.
- `pppoe` — controls PPPoE packet processing. Filtering by Service-Name is supported, including for QinQ tunnels. The following actions are available:
  - `enable` — allow PPPoE processing.
  - `drop` — drop PPPoE packets.
  - `pass` — pass PPPoE packets through without processing.
  - `delay N` — establish a PPPoE session with a delay of N seconds (0 < N < 16).
    Rules can be specified both for all PPPoE traffic in a VLAN/QinQ range and for a specific Service-Name.

Syntax for VLAN/QinQ Range Description

Rules apply to ranges specified in the following format:

- For a single VLAN: `156`
- For a VLAN range: `56-78` (VLANs 56 through 78 inclusive)
- For any VLAN: `*` or `any`
- For QinQ:
  - `67.*` or `67.any` — S-VLAN=67, any C-VLAN.
  - `*.68` or `any.68` — any S-VLAN, C-VLAN=68.
  - `*.*` or `any.any` — any QinQ.
  - `12-156.78-90` — S-VLAN range [12..156], C-VLAN range [78..90].
  - `609.1-199` — S-VLAN=609, C-VLAN range [1..199].

 Rules for ordinary VLANs (67) and QinQ (67.*) are independent and do not overlap.

Service-Name Support for QinQ Rules with Service-Name work correctly for QinQ:

- Rules without selectivity by CVLAN: SVLAN.* with or without Service-Name.
- Full QinQ (SVLAN.CVLAN) with selectivity by Service-Name.

Rule Priority

If ranges of several rules overlap, the system determines the resulting action based on the "general to specific" principle:

1. First, rules with the broadest ranges (e.g., 1-4095 or any.any) are applied.
2. Then rules with narrower ranges (e.g., 100-200) can override the action set by the general rules.

Example:
The following rules will create the policy: "Disable DHCP for all VLANs in the range 300-700, but enable it for VLAN 645 and the range 430-439".

```
vlan rule add 300-700 dhcp disable
vlan rule add 645 dhcp enable
vlan rule add 430-439 dhcp enable
```

Management

- `vlan rule add` — add a new rule to SDR.
  Syntax for PPPoE:
  - Adding a rule for all PPPoE traffic in a range:

    ```
    vlan rule add <Range> pppoe [enable | drop | pass | delay N]
    ```

  - Adding a rule for a specific Service-Name:

    ```
    vlan rule add <Range> pppoe sname <Service-Name> [enable | drop |
    pass | delay N]
    ```

    Here <Service-Name> is the PPPoE Service-Name in single or double quotes (quotes can be omitted if it is an identifier: [a-zA-Z_][a-zA-Z_0-9]*).
- `vlan rule modify` — modify an existing rule in SDR (similar syntax).
- `vlan rule delete` — delete a rule from SDR.
- `vlan rule show` — displays all rules for the specified VLAN/QinQ. The output shows not only the general PPPoE actions but also all permissions for individual Service-Name.
- `vlan rule dump` — dumps all rules in SDR. To filter output by rule type, the `[type]` parameter is used (e.g., `vlan rule dump perm`).
- `vlan rule purge vlan/qinq/all` — clear SDR VLAN/QinQ or both.
- `vlan rule apply` — apply rules; by default, rules are applied 5 minutes after the last SDR modification.

When using * in the CLI for QinQ ranges, it is recommended to enclose the expression in quotes (e.g., `'*.68'`) or use the keyword `any` (e.g., `any.68`) to avoid incorrect interpretation of the * character by the bash shell.

Change application specifics: Changes to rules made with `add`, `modify`, or `delete` are saved in SDR and automatically applied by the system 5 minutes after the last modification. The `vlan rule apply` command allows you to apply them forcefully, but no more than once per minute.

Using VLAN Rule in BALANCER

VLAN rules can also be used by the **BALANCER** component for packet filtering. This allows, at the traffic balancing stage, to filter out unwanted VLAN/QinQ before they reach the main processing modules.