Technical Guide

Mirroring

Feature Overview and Configuration Guide

Introduction

This document describes the mirroring functionality of AlliedWare Plus™ switches. The switches support two distinct forms of mirroring:

- **Port** mirroring sends a copy of network packets from one or more switch ports to another port on the same switch for analysis.
- **Remote** mirroring extends this functionality across switches by copying network packets from a port on one switch and forwarding them to one or more ports on a remote switch. The copied packets are transmitted to the remote switch over a dedicated VLAN.

Network engineers and administrators use mirroring to analyze and debug network traffic or diagnose errors on a network. It can be used to mirror either inbound or outbound traffic (or both) on single or multiple interfaces.

Products and software version that apply to this guide

This guide applies to AlliedWare Plus products that support port mirroring and/or remote mirroring, running version **5.4.6-1.x** or later.

To see whether your product supports mirroring, see the following documents:

- The product's Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Feature support may change in later software versions. For the latest information, see the above documents.

From software version 5.5.4-2.3 onwards, you can configure mirror to multiple ports or an aggregator on most AlliedWare Plus switches.

Contents

Introduction 1
Products and software version that apply to this guide 1
Port mirroring 3
Configuring port mirroring 3
Using ACLs to selectively mirror traffic 3
Limitations 4
Remote mirroring 5
How does remote mirroring work? 5
Limitations 6
How to use remote mirroring 6
Remote mirroring of tagged packets 7
Configuring remote mirroring 7
Simple configuration using two switches 8
Removing the basic configuration 9
Intermediate switches 10
Remote mirroring on an aggregated link 10
Using ACLs to selectively send traffic to the remote mirror 12
VLANs and remote mirroring options 13
Port mirroring to an aggregated link 13
Using ACLs with multiple mirror ports 14
Mirroring with VLAN filtering 14
Monitoring 16
Interaction with VLAN ID translation on SBx8100 Series 17

Port mirroring

Port mirroring enables traffic being received and transmitted on one or more switch ports to be sent to another switch port, the mirror port, usually for the purposes of capturing the data with a protocol analyzer. The mirror port is the only switchport that does not belong to a VLAN, and therefore does not participate in any other switching. Before the mirror port can be set, it must be removed from all trunk groups and all VLANs except the default VLAN.

- From software version 5.5.4-2.3 onwards, you can configure multiple mirror ports on most AlliedWare Plus switches. On these switches, you can also configure an aggregator as the mirror port. Mirroring to multiple ports or aggregators is not supported on x220, x320, GS980M, GS980EM, SBx81CFC960, and AR series devices.
- On x530, x530L, and GS980MX switches, the command **platform inter-chip-header 4-word** must be configured when mirroring to multiple ports or to an aggregator.
- From software version 5.5.5-2.1 onwards, on the x230, x930, x950, and SBx908 GEN2 series switches, you can mirror traffic on a specific VLAN. For more detail see "Mirroring with VLAN filtering" on page 14.

Configuring port mirroring

The following example sets port 1.0.2 to mirror traffic that is seen on ports 1.0.5 (both incoming and outgoing packets) and 1.0.8 (outgoing packets only).

1. Enter Interface Configuration mode for port 1.0.2

```
awplus(config)# interface port1.0.2
```

2. Configure this port to mirror packets being sent and received by port1.0.5

```
awplus(config-if)# mirror interface port1.0.5 direction both
```

3. Configure port1.0.2 to also mirror packets being transmitted by port1.0.8

```
awplus(config-if)# mirror interface port1.0.8 direction transmit
```

Using ACLs to selectively mirror traffic

As well as configuring the mirror port to mirror all the traffic being sent or received (or both) on certain ports, it is possible to use ACLs to choose to mirror just a specific subset of traffic arriving on a port. There are three steps to configuring this:

1. Set up a mirror port.

Set a port as the mirror destination port, but instead of specifying which port to mirror packets from, specify “none”.

For example, to configure port1.0.20 as the mirror port:

```
awplus(config)#interface port1.0.20
awplus(config-if)#mirror interface none
```

2. Create an ACL to match some particular traffic, and take the action 'copy-to-mirror' on that traffic.

```
awplus(config)#access-list hardware mc_filter
awplus(config-ip-hw-acl)#10 copy-to-mirror ip any 236.5.8.213/32
```

3. Attach the ACL to one or more ingress ports.

```
awplus(config)#interface port1.0.7
awplus(config-if)#access-group mc_filter
```

- Only traffic arriving on port1.0.7 **and** destined to the IP address 236.5.8.213 will be mirrored to port1.0.20. Any traffic arriving on port1.0.7, not destined to the IP address 236.5.8.213, will not be mirrored.
- Traffic arriving on any port destined to the IP address 236.5.8.213 will be mirrored to port1.0.20.

For all products, you can attach the ACL to one switch port or to a list or range of ports.

On some products, such as the SBx908 and SBx8100, you can alternatively apply the ACL selection to all ports by using the **access-group** command in Global Configuration mode.

```
awplus(config)#access-group mc_filter
```

Limitations

Due to the internal hardware properties of the switch, there are some limitations to be aware of when using port mirroring:

1. Mirroring to multiple ports is not supported on x220, x320, GS980M, GS980EM, SBx81CFC960, and AR series devices.

2. Mirroring to aggregators is not supported on x220, x320, GS980M, GS980EM, SBx81CFC960, and AR series devices.

3. To see the maximum number of mirror ports supported by a switch, see the switch's Datasheet.

4. If multiple ports are being mirrored, and those ports are all reasonably busy (sending/receiving near to a full bandwidth of data) then the amount of data being sent to the mirror port will be considerable. This can cause congestion within the switching fabric of the switch, and may cause packets in flows going to/from other ports to be dropped.

5. Frames that will exit the mirrored port untagged are received with their VLAN tags intact. This can increase bandwidth usage, potentially exceeding the mirror port's egress capacity if it's transmitting at wire speed.

Remote mirroring

Remote mirroring is helpful when you need to analyze traffic on a port of a remote switch but cannot easily connect an analyzer directly to that port. Similar to local port mirroring, it still requires some configuration on the switch.

Remote mirroring has some key differences to local port mirroring:

- All mirrored traffic is tagged with the **remote-mirror-vlan** tag as it goes through the network.
- The port used for traffic exiting the source switch is not exclusively dedicated to port mirroring; it continues to forward traffic normally on other VLANs.
- BPDUs and other non-VLAN-aware traffic cannot be mirrored.

Remote mirroring is often referred to as **RSPAN** (Remote Switch Port Analyzer). RSPAN is a feature that extends port mirroring across multiple switches by transmitting mirrored traffic over a VLAN, allowing traffic from a source port on one switch to be analyzed on a destination port on another switch.

How does remote mirroring work?

There are three components to a remote mirroring configuration:

1. **Source switch**

   The source switch duplicate packets from 1-4 ports to an egress port (on the source switch) with the addition of a particular VLAN tag. There can only be one egress port (shared between remote and port mirroring) per source switch.

2. **Intermediate devices**

   All devices in the path between the source and destination of the remote mirroring session are configured with this VLAN. The VLAN needs to be in a special ‘remote-mirror-vlan’ mode, which means that all traffic on the remote mirror VLAN is flooded, and no learning or CPU processing is done for packets in the VLAN.

3. **Destination switch**

   The destination switch has a port configured as a remote-mirror-egress port. This port strips the mirror-vlan tag off the packets and does not allow packet ingress. This port does not contribute to the maximum number of mirror destination ports on a switch.

Limitations

- Only one mirror destination is supported per switch; this can be either a local mirror or a remote mirror.
- Even though the packet is being duplicated to a VLAN, a specific port must be specified. This means that a link must be chosen that is not discarding packets (for instance, STP discarding).
- There is a limitation within the hardware of the following SBx8100 cards: SBx81CFC400, SBx81XS6, SBx81GS24a. The effect of this hardware is that remote mirroring cannot be applied to packets that are being Layer 3 routed by the card.
  It is recommended to not configure ports on these cards as remote mirroring destinations if packets to/from those ports are being Layer 3 routed within the card. In other words the command **remote-mirror interface** should not be used on such ports. The limitation does not apply to using ports on those cards for other aspects of remote mirroring (e.g. as a remote-mirror-egress port or trunk ports on an intermediate switch).
- Disabling the remote mirroring VLAN on the source switch will not prevent the mirrored packets from being sent with the remote-mirror VLAN tag. To stop the mirroring, the command **no remote-mirror interface** must be used.
- We recommend configuring the remote mirror VLAN on the switches receiving the mirrored traffic before enabling remote mirroring on the source switch. This is because the receiving switch may otherwise attempt to process certain types of received packets. If the receiving VLAN is correctly configured as a remote mirroring VLAN, it will drop these packets rather than processing them. Examples of packets in this category include STP and AMF BPDUs.

How to use remote mirroring

To use remote mirroring, a port on the **source** switch should be configured to be the remote mirroring destination for the switch. This configures the switch to send all mirrored traffic out that port, tagged with the configured mirror VLAN. The port does not have to be a dedicated port (for instance, it could be the uplink port of the switch).

All other switches between the source and destination switch must have the chosen remote-mirror VLAN configured as a **remote-mirror-vlan**. This means that all packets received on that VLAN will be flooded to all other ports in the VLAN, and learning of addresses from those packets is prevented. Certain packet types may still be sent to the CPU of the intermediate switches. These are forwarded on unless they are sent to the BPDU address range, in which case they are dropped.

The final destination switch also has this VLAN configured as a **remote-mirror-vlan**, but we also configure certain ports in the VLAN as **remote-mirror-egress** ports. These ports remove the remote mirroring VLAN tag from the packets before sending them out. Ingress is disabled on **remote-mirror-egress** ports.

Remote mirroring of tagged packets

Remote mirroring will mirror tagged packets. The original tag on the packet is retained as the packet is being mirrored. The tag of the mirror VLAN is applied to the packet as a second (outer) tag. Remote mirroring of tagged packets results in the packets being transported as double-tagged packets in the mirror VLAN.

Eventually, when the packets arrive at the remote-mirror-egress port on the destination switch, the outer tag is removed from the packets, and they are transmitted from the remote mirror egress port in their original form, with their original tag in place.

Packet size considerations for tagged packets

Because the remote mirror egress port is in access mode, rather than trunk mode, it is not innately set up for transmitting tagged packets. If the tagged packets that are being mirrored are close to the maximum Ethernet frame size, they may not be successfully transmitted by the remote mirror egress port on the destination switch unless jumbo frames are enabled. This can be done as follows:

- If the remote mirror egress port is on a SwitchBlade x8100 or an x220 Series destination switch, to enable jumbo frames on all ports on the switch, use the command:

  ```
  awplus(config)# platform jumboframe
  ```

  Note that you must restart the switch after entering this command for it to take effect.

- If the remote mirror egress port is on any other model of switch, set the maximum receive unit (MRU) for its remote mirror egress port to:

  - 9710 bytes for ports that work at speeds of either 10 Mbps or 100 Mbps
  - 10240 bytes for ports that work at speeds of 1000 Mbps

  by using the command:

  ```
  awplus(config-if)# mru <mru-value>
  ```

For more information, see the platform jumboframe command in the Switching Commands chapter and the **mru** command in the Interface Commands chapter in the Command Reference for your switch.

Configuring remote mirroring

A remote mirroring configuration has three parts:

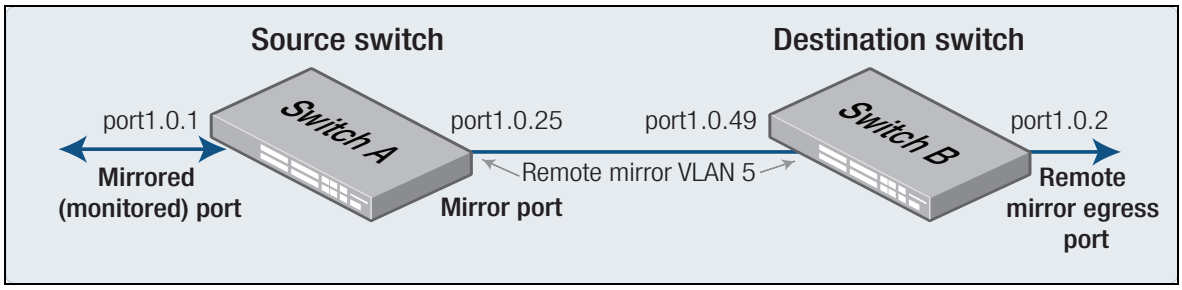
- A remote mirroring VLAN configured on all participating switches.
- A mirror port on the source switch configured to send out mirrored traffic tagged with the mirror VLAN tag.
- A port on the destination switch configured as a **remote-mirror-egress** port. This port blocks ingress traffic and outputs the mirrored traffic with the remote mirroring tag removed. This port must be on a different switch to the source traffic.

Note: All ports configured in the remote mirror VLAN that are not egress ports should be in trunk mode and the remote mirror VLAN must not be the native VLAN of the port.

Simple configuration using two switches

The following section describes how to configure remote mirroring in a simple two-switch scenario.

Traffic in both directions on port 1.0.1 (mirrored port) of Switch A will be sent out port 1.0.25 (mirror port) tagged with the remote-mirror-vlan tag 5 arriving at port 1.0.49 of Switch B, egressing on port1.0.2 (remote mirror egress port) of Switch B.



Configuring Switch B

We recommend configuring the **receiving (destination) switch** (in this example, Switch B) with the remote mirror VLAN **before** setting up the remote mirror to prevent unwanted processing of mirrored packets.

1. Create VLAN 5 as a remote mirroring VLAN

```
switch_b(config)# vlan database
switch_b(config-vlan)# vlan 5 mode remote-mirror-vlan
```

2. Put the port (port1.0.49) that the traffic is arriving on into trunk mode and add the mirror VLAN (5) as an allowed VLAN, (not the native VLAN).

```
switch_b(config)# interface port1.0.49
switch_b(config-if)# switchport mode trunk
switch_b(config-if)# switchport trunk allowed vlan add 5
```

3. Configure port1.0.2 as a remote mirror egress port. This will block ingress on the port and send out the traffic with the VLAN 5 tag removed. This is a dedicated mode and should not be used alongside other features.

```
switch_b(config)# interface port1.0.2
switch_b(config-if)# switchport remote-mirror-egress vlan 5
```

Configuring Switch A

1. Create VLAN 5 as a remote mirroring VLAN.

```
switch_a(config)# vlan database
switch_a(config-vlan)# vlan 5 mode remote-mirror-vlan
```

2. Put the mirror port, port1.0.25 (destination/egress port on the source switch) into trunk mode (if it is not already) and add the remote mirroring VLAN (5) as an allowed VLAN, (not the native VLAN).

```
switch_a(config)# interface port1.0.25
switch_a(config-if)# switchport mode trunk
switch_a(config-if)# switchport trunk allowed vlan add 5
```

3. Set the mirror port (port1.0.25) to send out traffic mirrored in both directions from port1.0.1 tagged with VLAN 5.

```
switch_a(config-if)# remote-mirror interface port1.0.1 direction both vlan 5
```

Removing the basic configuration

Follow this procedure to remove the basic configuration when remote mirroring is no longer needed. Start by removing the configuration from the remote mirror source switch, and then proceed to remove it from the destination switch. This sequence helps minimize unnecessary traffic.

Switch A

1. Remove the remote mirror and unset VLAN 5 as a trunked VLAN on port1.0.25.

```
switch_a(config)# interface port1.0.25
switch_a(config-if)# no remote-mirror interface port1.0.1
switch_a(config-if)# switchport trunk allowed vlan remove 5
```

2. Remove the remote mirror VLAN.

```
switch_a(config)# vlan database
switch_a(config-vlan)# no vlan 5
```

Switch B

1. Remove remote-mirror-egress mode from port1.0.2

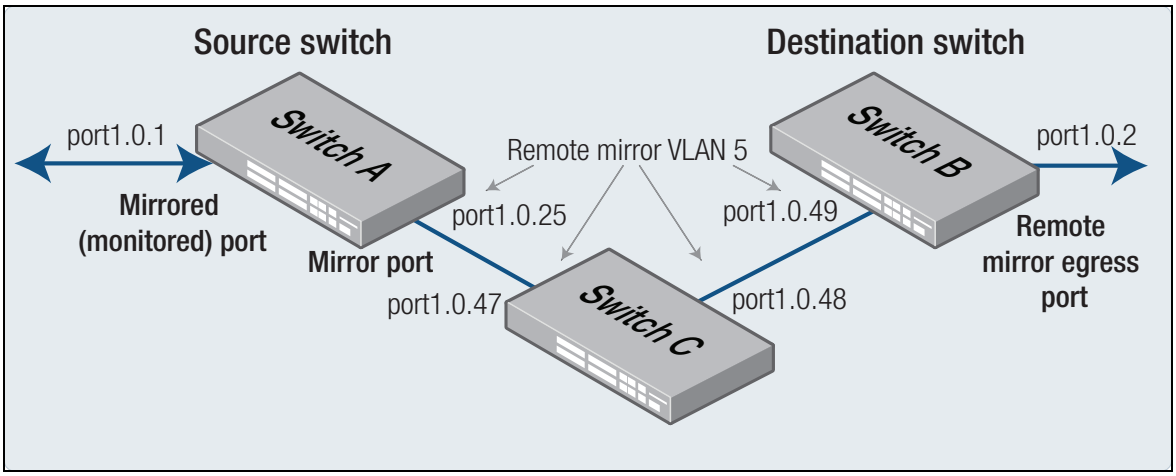
```
switch_b(config)# interface port1.0.2
switch_b(config-if)# no switchport remote-mirror-egress
```

2. Remove the remote mirror VLAN.

```
switch_b(config)# vlan database
switch_b(config-vlan)# no vlan 5
```

Intermediate switches

To add another switch (Switch C) between remote mirroring source Switch A and remote mirroring destination Switch B, follow the steps below:



Configuring Switch C

1. Create VLAN 5 as a remote mirroring VLAN

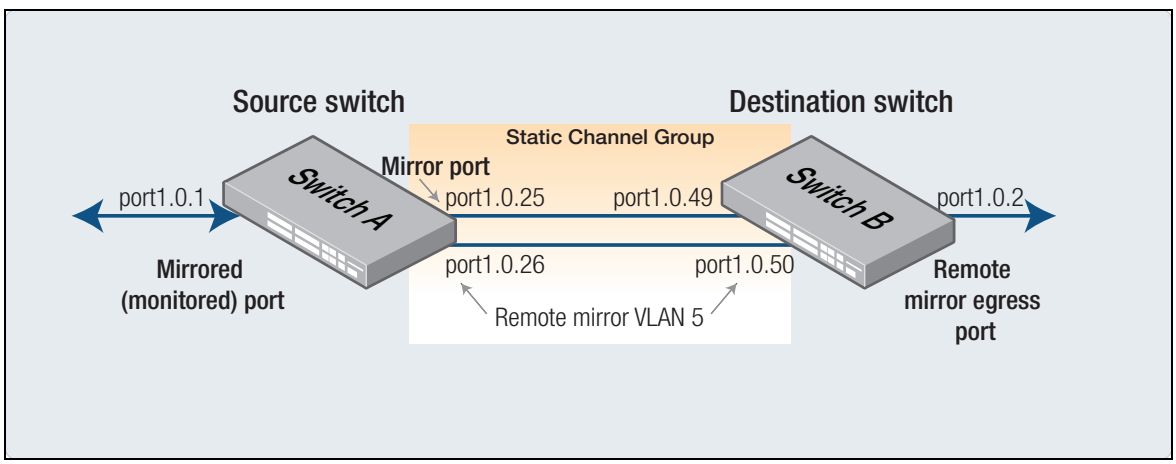
```
switch_c(config)# vlan database
switch_c(config-vlan)# vlan 5 mode remote-mirror-vlan
```

2. Add VLAN 5 as a trunked VLAN (not the native VLAN) on port1.0.47 and port1.0.48.

```
switch_c(config)# interface port1.0.47-port1.0.48
switch_c(config-if)# switchport mode trunk
switch_c(config-if)# switchport trunk allowed vlan add 5
```

Remote mirroring on an aggregated link

It is not currently possible to configure a static or dynamic channel-group as a remote mirroring destination (mirror port) on the source switch. However, it is possible to configure the mirror port on one of the member-ports of the channel-group. The channel group should still be configured with the remote mirroring VLAN at both ends of the link. An example follows using a static channel group. The process is the same for a dynamic channel group.



Configuring Switch B

We recommend configuring the receiving switch (Switch B) with the remote mirroring VLAN before setting up the remote mirror source to prevent unwanted processing of mirrored packets.

1. Create VLAN 5 as a remote mirroring VLAN.

```
switch_b(config)# vlan database
switch_b(config-vlan)# vlan 5 mode remote-mirror-vlan
```

2. Put the static-channel-group (sa2) that the traffic is arriving on into trunk mode (if it is not already) and add the remote mirroring VLAN (5) as an allowed VLAN, (not the native VLAN).

```
switch_b(config)# interface sa2
switch_b(config-if)# switchport mode trunk
switch_b(config-if)# switchport trunk allowed vlan add 5
```

3. Configure port1.0.2 as a remote mirroring egress port. This will block ingress on the port and send out the traffic with the VLAN 5 tag removed. This is a dedicated mode and should not be used alongside other features.

```
switch_b(config)# interface port1.0.2
switch_b(config-if)# switchport remote-mirror-egress vlan 5
```

Configuring Switch A

1. Create VLAN 5 as a remote mirroring VLAN.

```
switch_a(config)# vlan database
switch_a(config-vlan)# vlan 5 mode remote-mirror-vlan
```

2. Put the static channel group (sa1) into trunk mode (if it is not already) and add the remote mirroring VLAN (5) as an allowed VLAN, (not the native VLAN).

```
switch_a(config)# interface sa1
switch_a(config-if)# switchport mode trunk
switch_a(config-if)# switchport trunk allowed vlan add 5
```

3. Set one of the ports in the static channel group (port1.0.25) to be the mirror port—to send out traffic mirrored in both directions from port1.0.1 (mirrored port) tagged with VLAN 5.

```
switch_a(config)# interface port1.0.25
switch_a(config-if)# remote-mirror interface port1.0.1 direction both vlan 5
```

Using ACLs to selectively send traffic to the remote mirror

It is possible to selectively send traffic to the remote mirror via ACLs. The configuration for the receiving switch is the same as in the previous examples. The example below sets up port1.0.25 to be the remote mirror port and sets up some ACLs to send traffic to the port. Note that ACL-based mirroring only mirrors received packets.

1. Create vlan 5 as a remote mirror VLAN.

```
switch_a(config)# vlan database
switch_a(config-vlan)# vlan 5 mode remote-mirror-vlan
```

2. Put the egress port (port1.0.25) into trunk mode (if it is not already) and add the remote mirror VLAN (5) as an allowed VLAN (not the native VLAN).

```
switch_a(config)# interface port1.0.25
switch_a(config-if)# switchport mode trunk
switch_a(config-if)# switchport trunk allowed vlan add 5
```

3. Set port1.0.25 (mirror port) to send mirrored traffic as selected by the ACL, tagged with VLAN 5.

```
switch_a(config-if)# remote-mirror interface none vlan 5
switch_a(config-if)# exit
```

4. Create ACLs to mirror the desired traffic. There are two ACL actions that can be used for this:

   - The **copy-to-mirror** action copies the matched traffic to the mirror port and permits it.
   - The **send-to-mirror** action sends the packet to the mirror port and drops it.

   The example below uses a named hardware ACL to match on traffic with TCP port 25 (SMTP) or TCP port 80 (HTTP).

```
(config)# access-list hardware mirror_example
(config-ip-hw-acl)# 10 copy-to-mirror tcp any any eq 25
(config-ip-hw-acl)# 20 copy-to-mirror tcp any any eq 80
(config-ip-hw-acl)# exit
```

5. Attach the ACL to desired interfaces. For example, to apply the ACLs on port1.0.13-port1.0.14:

```
(config)# interface port1.0.13-1.0.14
(config-if)# access-group mirror_exampl
```

VLANs and remote mirroring options

Multiple remote mirroring VLANs:

You can configure multiple VLANs to serve as remote mirroring VLANs on a network. These VLANs act as pathways for transmitting mirrored traffic to other switches for analysis.

Source switch limitation:

On a source switch (the switch where traffic is mirrored from), you can only mirror traffic to one remote mirroring VLAN at a time.

This means that while multiple remote mirroring VLANs can exist in the network, each instance of mirroring on the source switch can only target one specific remote mirroring VLAN.

The following command sets up VLAN 5-25 as remote mirroring VLANs.

```
awplus(config)# vlan database
awplus(config-vlan)# vlan 5-25 mode remote-mirror-vlan
```

It is possible to add a user priority as part of the remote mirroring VLAN tag. This can be used to control the priority of the mirrored packets against other traffic flowing over the same ports. The default priority is 0. This is done by setting the 802.1p user priority field in the remote mirroring VLAN tag. To apply the non-default priority 2, add it as a parameter when configuring the remote mirroring mirror port on the source switch.

```
switch_a(config-if)# remote-mirror interface port1.0.1 direction both vlan 5
priority 2
```

Port mirroring to an aggregated link

From software version 5.5.4-2.2 onwards, it is possible to mirror traffic to static aggregators and dynamic aggregators. The following example creates a static-aggregator of port1.0.1 and 1.0.2. and mirrors the traffic as seen on port 1.0.8.

1. Configure port 1.0.1 and port 1.0.2 to be part of static-aggregator 1

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# static-aggregator 1
```

2. Enter Interface configuration mode for static-aggregator 1

```
awplus(config)# interface sa1
```

3. Configure this port to mirror packets being sent and received by port 1.0.8

```
awplus (config-if)# mirror interface port1.0.8 direction both
```

Using ACLs with multiple mirror ports

When using the copy-to-mirror action, it is possible to specify a mirror interface.

The following example demonstrates selectively mirroring VLAN 20 tagged traffic arriving on port1.0.5 to port1.0.20, and VLAN 21 traffic arriving on port1.0.5 to port1.0.21.

1. Configure port1.0.20 and port1.0.21 as mirror ports.

```
awplus(config)# interface port1.0.20
awplus(config-if)# mirror interface none
awplus(config)# interface port1.0.21
awplus(config-if)# mirror interface none
```

2. Create an ACL to match specific VLANs, mirroring each VLAN to a specific mirror port.

```
awplus(config)# access-list hardware mirror_filter
awplus(config-ip-hw-acl)# copy-to-mirror interface port1.0.20 mac any any vlan 20
awplus(config-ip-hw-acl)# copy-to-mirror interface port1.0.21 mac any any vlan 21
```

3. Attach the ACL to one or more ingress ports.

```
awplus(config)# interface port1.0.5
awplus(config-if)# access-group mirror_filter
```

Mirroring with VLAN filtering

From AlliedWare Plus version 5.5.5-2.1 onwards, on the x230, x930, x950, and SBx908 GEN2, you can mirror traffic on a specific VLAN using the following command:

```
mirror interface <source-port> vlan <2-4090>
```

Previously, if you wanted to mirror traffic on a specific VLAN, you had to use an ACL with a copy-to-mirror action. However, due to how ACLs work—stopping at the first match—this approach prevented any subsequent permit or deny rules from being evaluated. As a result, you couldn't mirror VLAN traffic and apply additional filtering rules in the same ACL.

The mirror interface vlan command:

- Enables VLAN-based mirroring using ACLs.
- Allows the copy-to-mirror action to occur without terminating ACL processing, so additional rules can still be evaluated.
- Clears any previous mirroring setup.
- Wraps the ACL logic into a single, user-friendly command, simplifying configuration.
    - The command automatically generates a hardware ACL with a reserved name based on the VLAN ID and port name. The ACL mirrors traffic to a specified VLAN.

Example To mirror traffic on VLAN 12, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# mirror interface port1.0.1 vlan12
```

This configuration mirrors traffic from interface port1.0.1 on VLAN 12 to the current interface port1.0.5. Only traffic tagged with VLAN 12 will be mirrored, allowing for more targeted monitoring. This differs from full interface mirroring, which captures all traffic (regardless of VLAN) on the source port.

Monitoring

Use the **show remote-mirror** command to show information about remote mirroring on the switch. Here is some example output:

```
awplus#show remote-mirror
Remote mirror information:

Remote mirror destination:
  Port:           port1.8.5
  VLAN:           259
  User priority:  0

Monitored ports:
  port1.8.4       direction: both
  none (via ACL)  direction: receive

Remote mirror egress ports:
  port1.8.6       VLAN 259
  port1.8.8       VLAN 222

Remote mirror VLANs:
  VLAN 222
  VLAN 21
  VLAN 259
  VLAN 333
```

The output of the **show remote-mirror** command displays the following information:

Remote mirror destination—On the source switch, this displays the:

- destination/egress port for the mirrored traffic on the source switch (the mirror port)
- remote mirroring VLAN ID this traffic is tagged with on egress
- user priority this traffic is tagged with on egress

Monitored ports—On the source switch, this displays:

- the ports being mirrored (monitored)
- the direction—whether both received traffic, transmitted traffic or both are mirrored
- 'none (via ACL)' if it is configured with the command **remote-mirror interface none** to allow ACLs to select the traffic to be mirrored.

  This signifies that packets can be sent to the remote mirroring destination port on the source switch using the ACL **copy-to-mirror** and **send-to-mirror** actions.

  Note that if the destination interface is shown and an interface is being monitored, the 'copy-to-mirror' and 'send-to-mirror' actions can be used implicitly, even if you have not specifically configured **remote-mirror interface none**.

Remote mirror egress ports—On the destination switch, this displays the:

- remote mirror egress ports
- remote mirror VLANs they are associated with

Remote mirror VLANs—On source, destination, and intermediate switches, this displays a list of any VLANs configured in ‘remote-mirror-vlan’ mode. To see a list of the ports associated with these VLANs, use the command **show vlan brief**.

Interaction with VLAN ID translation on SBx8100 Series

Note that if you configure VLAN ID Translation on a port on an SBx81GT40, SBx81XS16 or SBx81CFC960 card, and then mirror that port’s traffic, the mirrored traffic may have the original VLAN instead of the translated VLAN.

This applies to both port mirroring (on the same switch) and remote mirroring, but only affects the mirrored copy. The original traffic will correctly egress its port with the translated VLAN.

C613-22089-00 REV F

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com