Technical Guide

Mirroring

Feature Overview and Configuration Guide

Introduction

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

- **Port Mirroring**, which is used to send a copy of network packets that are seen on one or more switchports to another switchport on the same switch
- **Remote-mirroring**, which is used to send a copy of network packets that are seen on a port on one device to one or more switchports on a remote switch. The copied packets are forwarded to the remote switch on a special 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.

Contents

Port Mirroring

Port mirroring enables traffic being received and transmitted on one or more switchports to be sent to another switchport, 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.

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).

Step 1. Enter the Interface Configuration mode for port 1.0.2

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

Step 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
```

Step 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:

Step 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
```

Step 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
```

Step 3. Attach the ACL to one or more ingress ports (for example, port1.0.7).

```
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.

Limitations

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

1. Frames that are destined to leave the mirrored port untagged, (i.e. will have their VLAN tag removed on egress), will be received by the mirror port with the tag retained. Consequently, if frames were being transmitted by the mirror port (into the network) at wire speed, then the mirror port might be unable to accept all the frames supplied to it (as the addition of the tags may push the required bandwidth higher than the available egress bandwidth of the mirror port).
2. There is a strict limitation that only one mirror port can be configured on a switch. So, it is not possible to mirror some ports to one mirror port, and others to another mirror port. Just the one mirror port can be configured, and all ports that are being mirrored will have their traffic copied to that one port.
3. 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.

Remote-mirroring

Remote-mirroring is useful if it is necessary to analyze traffic going through a port on a remote switch, but it is not easy to plug an analyzer directly into a port on that switch. Like local port mirroring, some configuration is still required on the device.

Remote-mirroring has some key differences to local port mirroring:

- All mirrored traffic is tagged with the **mirror-vlan** tag as it goes through the network.
- The port that the traffic exits the source switch on is not dedicated to port mirroring, and forwards traffic as normal on other VLANs.
- BPDUs and other non-VLAN-aware traffic can not be mirrored.

Remote-mirroring is also known as RSPAN, Remote Switch Port ANalyzer.

How does Remote-mirroring work?

There are three components to a Remote-mirroring configuration:

1. The source switch is configured to duplicate packets from 1-4 ports to a destination port with the addition of a particular VLAN tag. There is a limit of one destination port (total between remote and port mirroring) per switch.
2. All switches 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 mirror-vlan mode, which means that all traffic on the mirror-vlan is flooded, and no learning or CPU processing is done for packets in the VLAN.
3. 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 isn't discarding packets (e.g. 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.
- It is recommended to configure 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 (e.g. 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 tag from the packets before sending them out. Ingress is disabled on **remote-mirror-egress** ports.

Configuring Remote-mirroring

A Remote-mirroring configuration has three parts:

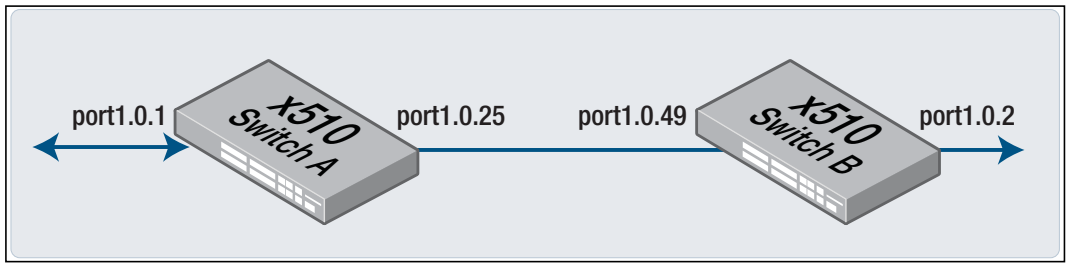
- A Remote-mirroring VLAN configured on all participating switches.
- A port on the source switch configured to send out mirrored traffic tagged with the mirror VLAN tag.
- A port on the destination switch configured as a **remote-mirror-egress** port. This port blocks ingress traffic and outputs the 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 aren't egress ports should be in trunk mode and the 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 of **switch_a** will be sent out port 1.0.25 tagged with the mirror-vlan tag 5 arriving at port 1.0.49 of **switch_b**, egressing on port1.0.2 of **switch_b**.



Configuring Switch_b

It is recommended to configure the **receiving switch** (in this example, switch_b) with the remote-mirror VLAN **before** setting up the Remote-mirror to prevent unwanted processing of mirrored packets.

Step 1. Create VLAN 5 as a Remote-mirroring VLAN.

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

Step 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-int)# switchport mode trunk
switch_b(config-int)# switchport trunk allowed vlan add 5
```

Step 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-int)# switchport remote-mirror-egress vlan 5
```

Configuring Switch_a

Step 1. Create VLAN 5 as a Remote-mirroring VLAN

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

Step 2. Put the egress port (port1.0.25) 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-int)# switchport mode trunk
switch_a(config-int)# switchport trunk allowed vlan add 5
```

Step 3. Set port1.0.25 to send out traffic mirrored in both directions from port1.0.1 tagged with VLAN 5.

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

Removing the basic configuration when Remote-mirroring is no longer required

Switch_a

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

Step 2. Remove the Remote-mirror VLAN

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

Switch_b

Step 1. Remove Remote-mirror-egress mode from port1.0.2

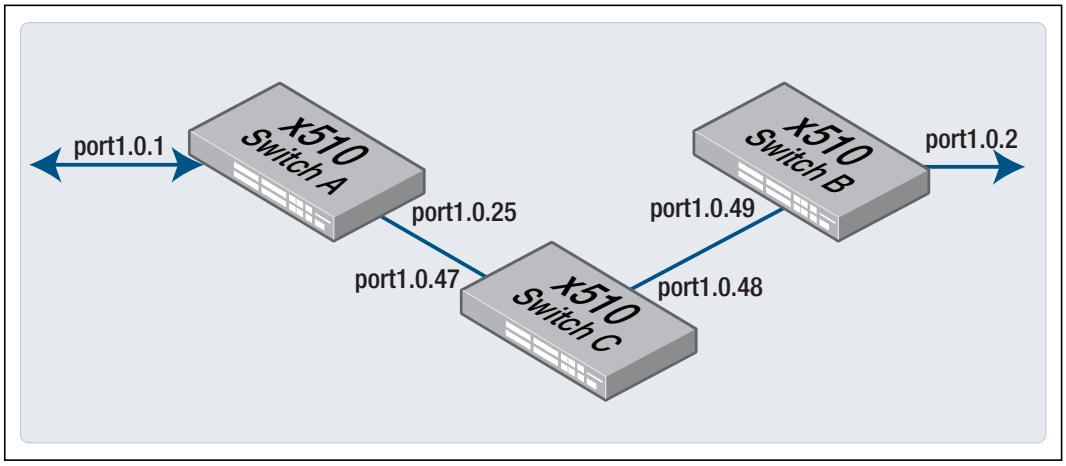
```
switch_b(config)# interface port1.0.2
switch_b(config-int)# no switchport remote-mirror-egress
```

Step 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 switch_a and switch_b, follow the steps below:



Configuring Switch_c

Step 1. Create VLAN 5 as a Remote-mirroring VLAN

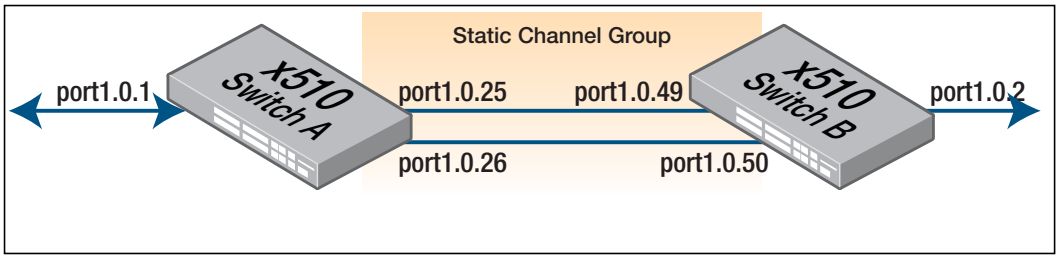
```
switch_c(config)# vlan database
switch_c(config-vlan)# vlan 5 mode remote-mirror-vlan
```

Step 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-int)# switchport mode trunk
switch_c(config-int)# 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. However, it is possible to configure the Remote-mirroring destination 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

It is recommended to configure the receiving switch with the Remote-mirroring VLAN before setting up the Remote-mirror to prevent unwanted processing of mirrored packets.

Step 1. Create VLAN 5 as a Remote-mirroring VLAN.

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

Step 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-int)# switchport mode trunk
switch_b(config-int)# switchport trunk allowed vlan add 5
```

Step 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-int)# switchport remote-mirror-egress vlan 5
```

Configuring Switch_a

Step 1. Create VLAN 5 as a Remote-mirroring VLAN.

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

Step 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-int)# switchport mode trunk
switch_a(config-int)# switchport trunk allowed vlan add 5
```

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

```
switch_a(config)# interface port1.0.25
switch_a(config-int)# 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.

Step 1. Create vlan 5 as a Remote-mirror VLAN

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

Step 2. Put the egress port (port1.0.25) into trunk mode (if it isn't 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-int)# switchport mode trunk
switch_a(config-int)# switchport trunk allowed vlan add 5
```

Step 3. Set port1.0.25 as the Remote-mirror analyzer port.

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

Step 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
```

Step 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
```

Other options

It is possible to create more than one VLAN as a Remote-mirroring VLAN at the same time. However, it is still only possible to mirror to a single Remote-mirroring VLAN on the source switch. 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-mirror.

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

Monitoring

The **show remote-mirror** command can be used 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
```

Output description:

- **Remote mirror destination**—displays which interface mirrored traffic is sent to. It also shows the VLAN ID and user priority that the mirrored packets are tagged with.
- **Monitored ports**—displays the list of ports that are being monitored. A special string is displayed if the user configures the command **remote mirror interface none**. This signifies that packets can be sent to the Remote-mirroring destination 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” can implicitly be used, even if the user hasn't specifically configured “remote-mirror interface none”.
- **Remote mirror egress ports**—displays which ports are configured as Remote-mirroring egress ports, and which Remote-mirroring VLAN they are associated with.
- **Remote mirror VLANs**—displays a list of the VLANs configured as Remote-mirroring VLANs. To see a list of the ports associated with these VLANs, use the command: **show vlan brief**.

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