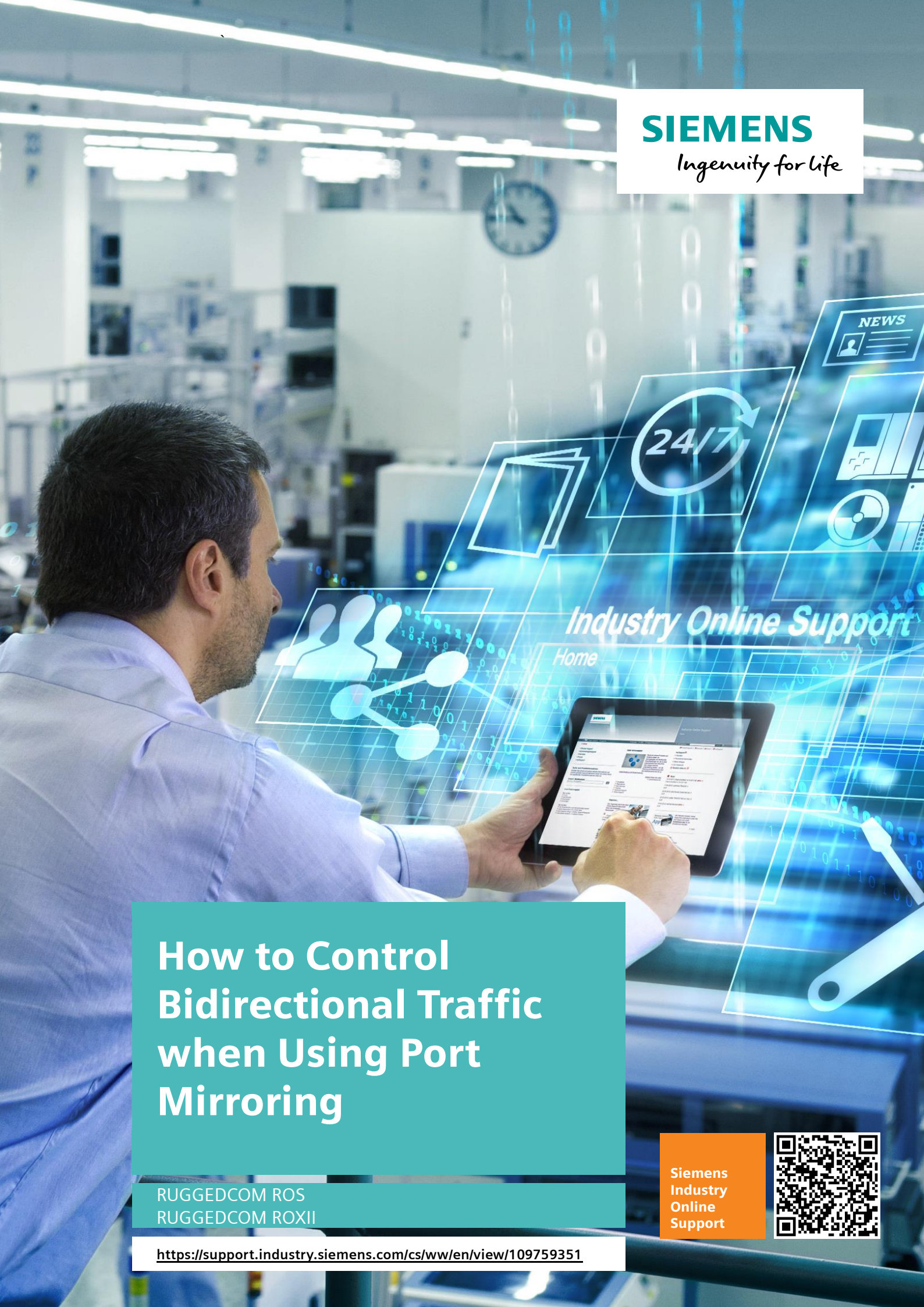

How to Control Bidirectional Traffic when Using Port Mirroring

RUGGEDCOM ROS
RUGGEDCOM ROXII

Siemens Industry Online Support

https://support.industry.siemens.com/cs/ww/en/view/109759351

This entry is from the Siemens Industry Online Support. The general terms of use (http://www.siemens.com/terms_of_use) apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement—and continuously maintain—a holistic, state-of-the-art, industrial security concept. Siemens's products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens's guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens's products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Table of Contents

1 Introduction

By default, mirror ports allow bidirectional traffic. When port mirroring is enabled the device does not block incoming traffic to the mirror port(s). This can lead to traffic being forwarded to unintended ports.

For increased security, ingress filtering can be configured to control traffic flow when port mirroring is enabled.

This document details how to configure port mirroring and ingress filtering to control traffic flow to other ports.

2 Sample Topology

In the sample topology, VLAN1 and VLAN2 tagged traffic is being sent to the source ports of devices R1 and R2. While port mirroring is enabled, ingress filtering prevents bidirectional traffic flow.

NOTE Devices R1 and R2 represent either routers or switches, depending on the application.

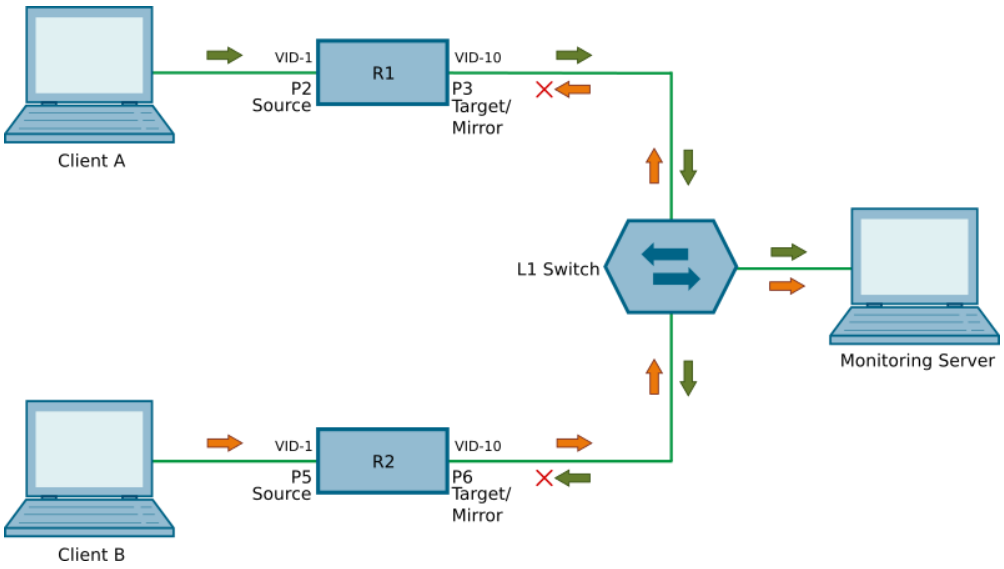

Figure 1: Sample Topology

2.1 Purpose

This example demonstrates how to allow traffic from Client A and Client B to reach a monitoring server, while preventing unintended traffic from Client A from reaching Client B, and vice versa.

2.2 Assumptions

- Client A and Client B are sending traffic to devices R1 (P2) and R2 (P5).
- Port mirroring is enabled on R1 and R2.
- The source port of R1 is P2. Traffic of P2 is mirrored on P3.
- The source port of R2 is P5. Traffic of P5 is mirrored on P6.
- Target ports are not configured as trunk ports.
- Any trunk ports on R1 and R2 are configured as Forbidden ports on the VLAN of the target ports (i.e. VLAN 10).
- VLAN 10 is not configured on any other interfaces of R1 and R2.
- Ingress filtering is enabled on R1 and R2.
- RSTP is disabled on the target ports.
- Neighbor discovery protocol is disabled on the target ports.
- LLDP is disabled on the target ports.

- Network management protocols (e.g. GVRP, GMRP, IGMP) are disabled on the target ports of R1 and R2.
- The Port VLAN Identifiers (PVIDs) on R1 and R2 are configured as follows:

Device/Port	PVID (Native VLAN)
R1/P2	1
R1/P3	10
R2/P5	1
R2/P6	10

Table 1: Port VLAN Identifiers

2.3 Behavior

- Any traffic received on the source port is forwarded to the target port via port mirroring. In the topology, any traffic received on port 2 is forwarded to port 3, and any traffic received on port 5 of R2 is forwarded to port 6.
- RSTP is disabled on the target ports, therefore RSTP packets are blocked from reaching this port.
- Neighbor discovery protocol is disabled on the target ports, therefore LLDP packets are blocked from reaching the L1 switch.
- Any traffic received from any port other than source ports of R1 and R2 is blocked from leaving the target port.

3 Configuration

To configure devices per the sample topology, do the following:

NOTE For detailed instructions about configuring the device, refer to the *RUGGEDCOM ROS User Guide* or the *RUGGEDCOM ROXII User Guide,* as applicable.

NOTE The information shown is specific to the provided topology. Actual values will vary based on the user's configuration.

1. Enable port mirroring on R1 and R2.
2. Enable ingress filtering on R1 and R2.
3. Configure P2 as the source port and P3 as the target port of R1.
4. Configure P5 as the source port and P6 as the target port of R2.
5. Disable Rapid Spanning Tree Protocol (RSTP) on the target port (i.e. P3) of R1 to prevent egress of any RSTP packets.
6. Disable Rapid Spanning Tree Protocol (RSTP) on the target port (i.e. P6) of R2 to prevent egress of any RSTP packets.
7. Disable Link Layer Discovery Protocol (LLDP) on the target ports of R1 and R2 to prevent any LLDP packets from being sent to other ports.
8. Disable network management protocols (e.g. GVRP, GMRP, IGMP) on the target ports of R1 and R2.
9. Configure PVIDs on R1 and R2 per Table 1.

4 Customer Support

Siemens Customer Support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, please contact Siemens Customer Support through any one of the following methods:

- **Online**

  Visit http://www.siemens.com/automation/support-request to submit a Support Request (SR) or check on the status of an existing SR.

- **Telephone**

  Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx.

- **Mobile App**

  Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

  - Access Siemens's extensive library of support documentation, including FAQs, manuals, and much more
  - Submit SRs or check on the status of an existing SR
  - Find and contact a local contact person
  - Ask questions or share knowledge with fellow Siemens customers and the support community via the forum

5 History

Version	Date	Modifications
1	08/2018	Initial release