

Application Note

Using Redundancy Protocols with G6 Devices

MICROSENS GmbH & Co. KG
Küferstr. 16
59067 Hamm/Germany

Tel. +49 2381 9452-0
FAX +49 2381 9452-100
E-Mail info@microsens.de
Web www.microsens.de

Summary

This document outlines the configurational steps that are typically needed to set up the redundancy protocols for operating redundant networks.

Serving hands-on scenarios, it also leads step-by-step through example configurations.

It builds on information provided by the Quick Installation Guide that is shipped with each MICROSENS G6 device and the document "Product Manual Firmware, Generation 6" that is included in each software archive and can also be downloaded from the Web Manager's link "Documentation" in the navigation bar.

Additionally, prior knowledge of the foundations of IP Networks and Virtual LANs is required for the reader to benefit from this Application Note.

Glossary

Acronyms and abbreviations used in the document.



Term	Description
APC	Admin Path Cost (used for STP)
CIST	Common and Internal Spanning Tree (used with MSTP)
LACP	Link Aggregation Control Protocol (IEEE 802.1AX)
LAN	Local Area Network
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol (IEEE 802.1s)
MVRP	Multiple VLAN Registration Protocol (IEEE 802.1ak, GVRP successor)
RSTP	Rapid Spanning Tree Protocol (IEEE 802.1w)
STP	Spanning Tree Protocol (IEEE 802.1D)
VID	VLAN ID
VLAN	Virtual Local Area Network

Table of Contents



SUMMARY.....	2
GLOSSARY	2
TABLE OF CONTENTS	3
TYPOGRAPHICAL CONVENTIONS.....	4
INFORMATION AVAILABLE FROM THE MICROSENS WEBSITE.....	4
1 INTRODUCTION.....	5
2 REDUNDANCY PROTOCOLS.....	5
2.1 Overview	5
2.1.1 Technical Background	5
2.1.2 Evolution, Operation and special Features of Spanning Tree Protocols.....	5
2.1.3 MICROSENS Redundant Ring Protocol (MRRP)	7
2.1.4 Link Aggregation Control Protocol (LACP)	7
2.1.5 Choosing Redundancy Topologies and Redundancy Protocols	8
3 RSTP AND MSTP	10
3.1 Example 1: Configuring STP for a Network with One Loop	10
3.1.1 Topology Description	10
3.1.2 Basic Configuration.....	11
3.1.3 Port Configuration	13
3.1.4 Resulting Switch Settings and Network Structure	16
3.1.5 Monitoring (R)STP Bridge Status	17
3.1.6 Monitoring (R)STP Port Status	19
3.2 Example 2: Configuring MSTP for two RSTP instances	23
3.2.1 Topology Description	23
3.2.2 Basic Configuration.....	24
3.2.3 Port Configuration	29
3.2.4 Resulting Switch Settings and Network Structure	31
3.2.5 Monitoring MSTP Bridge Status	32
3.2.6 Monitoring MSTP Group Status or MSTP ID Status	33
3.2.7 Monitoring MSTP Bridge Status by MSTP Group	35
4 MICROSENS REDUNDANT RING PROTOCOL.....	37
4.1 Example 3: Simple MICROSENS Ring Configuration	37
4.1.1 Topology Description	38
4.1.2 Basic Configuration.....	38
4.1.3 Port Configuration	39
4.1.4 Ring Master Configuration	39
4.1.5 Resulting Switch Settings and Network Structure	40
4.1.6 Monitoring Ring Status.....	40
4.1.7 Monitoring Backup Statistics	41
DISCLAIMER.....	44

Typographical Conventions

The following typographical elements are used in this document:

Typographical Elements	Explanation
•	List element, 1 st order
◦	List element, 2 nd order
www.microsens.de	Hyperlink to a website or email address
Note:	A note tags an important fact
□	Work step
<...>	Placeholder for a real value. Replace <port> with e.g. <1>.
{... ...}	Choose one of the values offered, e.g. from {Disabled Enabled} choose Enabled.
Visualization	A string that appears in the Web Manager
Command	A string to enter in the Command Line Interface
» Output	A string output by the Command Line Interface
	Work step(s) in the Web Manager (GUI)
	Work step(s) in the Command Line Interface (CLI)

The following symbols are used in this document:

Symbol	Explanation
	Switch
	Server/Workstation

Information available from the MICROSENS Website

Registered users can find current firmware versions as well as further information on our web site:

- Registration: www.microsens.de > Partner-Login > Follow the link 'Please register here' > Fill in the [online registration form](#) and submit it
 - You will receive an email from MICROSENS with a user name and a password
- Login: www.microsens.de > Partner-Login > Enter user name and password > Click the 'Login' button
 - Firmware images: Navigate to your device and select the tab 'Services'
 - For further information select one of the other tabs

Note:

Make sure your browser allows scripts.

1 Introduction

This document leads through the setup for operating the switches in a redundant network environment.

The following sequence has proven useful in practice:

- Configure switches before operating the network with loops or redundant connections
- Configure the redundancy protocol that fits the demands
- Connect the switches to the network and establish the redundant connection
- Monitor the switches' bridge and port status to check for network failures due to misconfiguration

2 Redundancy Protocols

2.1 Overview

2.1.1 Technical Background

Network redundancy offers a fault-tolerant design for continuous network operation where it is essential to guarantee lossless data transport (e.g. in the energy or industrial business).

The Ethernet standard does not contain mechanisms for coping with ring or loop connections in the network. Quite the opposite, a ring or loop connection would cause several problems: All of the affected devices would send broadcast messages to each other over and over again. This "broadcast storm" would cause the whole network to stop working. The network segment itself would be incapacitated by handling duplicated data packets over and over again. Additionally, a network loop would cause MAC address table inconsistency because it creates conflicting port entries for the same MAC address.

The use of a redundancy protocol like STP (spanning tree protocol) supports redundant network topologies by defining default paths and thus ignoring broadcast data packets from (accidentally) connected redundant network devices or ports. It ensures switching to a defined backup connection in case of a network connection malfunction (e.g. network loop or loss of connection).

This of course only works if all devices in the network support the same redundancy protocol.

2.1.2 Evolution, Operation and special Features of Spanning Tree Protocols

Currently, there are three standardised versions of Spanning Tree Protocols:

The original **Spanning Tree Protocol (STP)**, defined in the IEEE Standard 802.1D, creates a spanning tree with a mesh network of connected layer-2 bridges (typically Ethernet switches) and disables the links which are not part of that tree, leaving a single active part between any two network nodes. Currently, STP is used as a single STP instance running in a configurable VLAN.

To provide faster spanning tree convergence after a topology change, the IEEE Standard 802.1w (later incorporated into IEEE Standard 802.1D-2004) introduced a refinement of the Spanning Tree Protocol: the **Rapid Spanning Tree Protocol (RSTP)**. It is backwards compatible to STP and shares most of the STP's basic operation characteristics. This refinement essentially creates a cascading effect away from the root bridge where each

designated bridge proposes to its neighbors to determine if it can make a rapid transition. This is one of the major elements which allow RSTP to achieve shorter convergence times than STP.

With IEEE Standard 802.1s the **Multi Spanning Tree Protocol (MSTP)** expands the RSTP with up to 64 STP instances (on G6 devices) running in configurable VLAN groups. Thus it is possible to manage different logical mesh networks within the same physical network.

When using (R)STP, the network devices continuously exchange **BPDU messages** (Bridge Protocol Data Unit) to determine the root bridge and to update the current state of the network topology.

To determine the **root bridge**, all devices compare their bridge ID, a value consisting of a configured priority value and the device's MAC address. The device with the lowest bridge ID hence acts as root bridge and thereby as a reference point for all other devices within the STP network. All other bridges that forward data packets in the direction of the root bridge are called **designated bridges**. The sending ports on designated bridges that transfer data in the direction of the root bridge are called **root ports**, the receiving ports of this communication are called **designated ports**. Thus, the root bridge has only designated and no root ports. Designated bridges' ports can generally hold the following port roles depending on the preferred network path (see path costs below) between the devices:

- **Root port:** These are the ports identifying the preferred path (in terms of path costs and port priorities) in the direction of the root bridge. Ports with root port role are forwarding ports.
- **Designated port:** The counterpart of a root port is always a designated port. Ports with designated port role are forwarding ports.
- **Alternate port:** A port that is not part of the preferred path to the root bridge normally blocks data to avoid a redundant connection. In case of a BPDU degradation on the root port of a designated bridge (e.g. a declined or lost connection on the path towards the root bridge) the alternate port changes to root port role. Ports in alternate port role are blocking ports.
- **Backup port:** In case of a BPDU degradation on the designated port of a designated bridge the backup port changes to designated port role. Ports in backup port role are blocking ports.

To decide which ports to use for sending data packets the devices use the so-called **path cost**, which is the accumulation of all port costs from designated ports to root ports along the path to the root bridge: The shorter the distance and the better the port speed the lower the respective port path cost will be. Every port accumulates its port path cost to the particular BPDU path cost section before forwarding the BPDU. With every incoming BPDU on every blocking or forwarding port the respective bridge decides which ports to use for communication and which ports to block. Port path costs can be automatically configured depending on current port speed. The user can select between two models:

- Path cost according to IEEE Standard 802.1D-1998:
 - 10 Mb/s link speed: 100
 - 100 Mb/s link speed: 19
 - 1 Gb/s link speed: 4
- Path cost according to IEEE Standard 802.1D-2001 (and 2004):
 - 10 Mb/s link speed: 2 000 000
 - 100 Mb/s link speed: 200 000
 - 1 Gb/s link speed: 20 000

(R)STP is not capable of coping with **multiple VLANs** in a network. For every VLAN connecting several nodes, every individual device would have to manage a unique STP instance. I.e., with VLAN 1 to 100 there have to be up to 100 (R)STP instances on every device involved which would cause enormous workload. Additionally, (R)STP manages the complete port forwarding status regardless of individually configured VLAN port settings. (R)STP may not recognise parallel network connections of untagged ports originally separated by different VLAN IDs and may block one port causing an interruption of the respective ports' connection.

MSTP takes advantage of the fact that there are multiple VLANs using the same devices. So it is possible to handle groups of VLANs instead of managing every single VLAN.

MSTP generally uses the same algorithms as (R)STP, i.e. to decide which device acts as root bridge or how to handle BPDUs. It needs some additional parameters, i.e. to administrate the VLAN groups, the associated region devices and the bridges and ports to other regions.

BPDU Guards working on STP devices are monitoring STP packets and triggering the respective actions (i.e. blocking the reception of BPDUs on the respective ports). This function ensures that no user can accidentally or purposefully hijack all data traffic to path through his computer. In addition, the BPDU guards prevent an unintentional network reorganisation due to incorrect root information which otherwise would cause network instabilities.

The **Bridge Assurance** detects unidirectional link failures that may occur with fiber optic links whereby one fiber direction breaks. This function ensures that the designated bridge does not make false detection about the traffic path under fiber failure conditions.

2.1.3 MICROSENS Redundant Ring Protocol (MRRP)

The MICROSENS Redundant Ring Protocol can be used with MICROSENS industrial switches to handle up to 2 independent network rings simultaneously, each containing typically up to 10-20 switches as ring members. The MICROSENS Redundant Ring Protocol is designed to automatically switchover data traffic in a ring network, should a failure in one of the ports or cables occur. In case of failure of a node segment, the ring members automatically reconfigure the remaining switches for continuous data flow, even when the ring master drops out.

2.1.4 Link Aggregation Control Protocol (LACP)

Link aggregation bundles physical network connections. The resulting aggregate link (formerly also called "trunk") offers higher bandwidth and also offers redundancy in case one of the physical connections breaks down. As LACP was primarily designed for bundling physical ports to increase transmission bandwidth and to distribute network load this document does not go into LACP details.

For more information about configuring and using LACP please refer to chapter "LACP (Link Aggregation)" in the document "Product Manual Firmware, Generation 6" that is included in each software archive and can also be downloaded from the Web Manager's link "Documentation" in the navigation bar.

2.1.5 Choosing Redundancy Topologies and Redundancy Protocols

MICROSENS G6 Switches support the spanning tree protocols STP, RSTP and MSTP. These protocols handle redundant networks on OSI layer 2. Additionally, it is important to choose the physical network topology that fits the needs and requirements.

There are different ways to realise a network redundancy topology out of a loop-free (and thus fault-prone) line, bus, tree or star topology:

Redundant Topology	Topology Change	Redundancy Protocol	Comments
Link Aggregation	Two network nodes are directly connected with a redundant parallel connection.	LACP (R)STP	Fail-safe for this explicit connection between two network nodes. Note: For LACP background and configuration see "2.1.4 Link Aggregation Control Protocol (LACP)".
Ring (one loop)	One network node closes a line or bus segment of the network by connecting two of its ports to the same network (same or different remote network node).	(R)STP MRRP	Fail-safe for single-point failures like cable defects or other connection problems between network nodes. On loss of connection in one direction the network nodes simply reroute data the other way round.
Mesh (multiple loops)	At least two network nodes are multiply connected to at least two other network nodes spanning a so called mesh network.	(R)STP	Fail-safe for cable defects and device malfunctions. If a complete network node drops out the remaining nodes bypass data around the missing node.
Multiple instances over existing network topology (looped or linear)	Logical expansion of an existing physical network by using independent VLANs.	MSTP	Using a logically linear VLAN network structure avoids physical network loops as only the used ports are open for the respective VLAN.

Of course it is possible to combine those redundant topologies in many ways: Nested but independent rings, two mesh networks with link aggregation between both the mesh network connecting nodes, star topologies with redundant central nodes and so on. To

Application Note

Using Redundancy Protocols with G6 Devices



realise those topology variations all respective redundancy protocol settings are configurable in parallel.

Note:

For further information about the STP, RSTP and MSTP standards, parameters and options please refer to the chapter "Rapid Spanning Tree Protocol (RSTP)" in the document "Product Manual Firmware, Generation 6" that is included in each software archive and can also be downloaded from the Web Manager's link "Documentation" in the navigation bar.

3 RSTP and MSTP

3.1 Example 1: Configuring STP for a Network with One Loop

The STP configuration can be subdivided into the following categories:

- Basic configuration (including configuration of (R)STP, MSTP and MSTP groups)
- Port configuration

Note:

Configuration of MSTP and MSTP groups is not necessary for this example.

3.1.1 Topology Description

To describe the RSTP configuration we use a simple network infrastructure with a loop. Three switches S1, S2 and S3 are connected to each other, building a loop. Every switch has one workstation W1, W2 and W3 connected to it.

As a state-of-the-art network the infrastrucure allows a bandwidth up to 1 Gb/s.

Element	Description
W1 – W3	Workstations W1 to W3
S1 – S3	Switches S1 to S3 MAC1: 00:60:a7:11:11:11 MAC2: 00:60:a7:22:22:22 MAC3: 00:60:a7:33:33:33
Pxx	Ports connecting the respective switches: <ul style="list-style-type: none"> • P12: Port that connects switch S1 and switch S2 • P21: Port that connects switch S2 and switch S1 • P13: Port that connects switch S1 and switch S3 • etc. <p>Note: The port that is directly connected to a client is called an "edge port".</p>

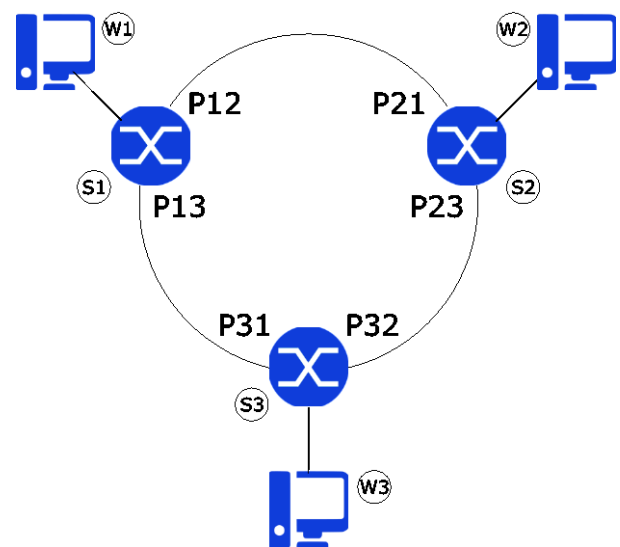


Figure 1: Simple Network Loop

3.1.2 Basic Configuration

To use the RSTP within the network this feature has to be enabled on all connected switches. It is possible to choose between different STP standards as the base operating mode.

Note:

Dependent on this choice some settings or statuses are limited or without effect, i.e. with STP enabled a port role cannot be "ALTERNATE".

Using the Web Manager:

- Open the Web Manager on the respective switch.
- Select the **Spanning Tree** Screen, then select the tab **Basic Configuration**.
- In the section **Basic Configuration** select the respective **STP Mode** setting.

Using the Command Line Interface (CLI):

- `Protocol.stp.bridge_config.mode = {Disabled|STP|RSTP}`

Before using (R)STP several basic parameters have to be configured on all connected switches. These basic parameters apply to how the switch handles BPDUs.

Parameter	Explanation	Valid Values	Default
Priority	<p>To determine the root bridge of a STP network all devices initially compare their bridge ID consisting of 2 byte bridge priority (this value) and 6 byte MAC address. The device with the lowest bridge ID acts as root bridge.</p> <p>On devices with identical priority values the one with the lowest MAC address holds a higher priority. So with all switches using the identical default setting the switch with the lowest MAC address becomes root bridge.</p>	0 – 61440 in steps of 4096	32768
Hello Time	<p>For exchange of configuration messages the devices send BPDUs (Bridge Protocol Data Unit).</p> <p>This parameter sets the time in seconds between said BPDUs by this node on any port when it is the root bridge of the STP network (or trying to become so).</p>	1 – 2	2

Parameter	Explanation	Valid Values	Default
Maximum Age	<p>This parameter sets the maximum age in seconds of STP information learned from the network on any port before the device discards it.</p> <p>If the device does not receive any new BPDUs within this time it changes its blocked ports into listen state and waits for new BPDUs to come. One of these BPDUs at best contains new information about changes in the network topology.</p>	6 – 40	20
Forward Delay	<p>Any port needs a specific time to listen to and learn the incoming STP information for further action.</p> <p>This parameter sets the time in seconds before the device forwards the incoming BPDUs.</p>	4 – 30	15
Tx hold count	This value is used to limit the maximum transmission number of BPDUs during every hello time period.	1 – 10	6
Path cost model	Every device except for the root bridge calculates his connections to the root bridge in form of path costs. The "cheaper" a connection is, the more applicable it is. This calculation differs between the 1998 and 2004 releases of standard IEEE 802.1D due to technical enhancements.	IEEE-802.1D-1998 IEEE-802.1D-2004	IEEE-802.1D-2004
Priority	<p>To determine the root bridge of a STP network all devices initially compare their bridge ID (consisting of 2 byte bridge priority and 6 byte MAC address). The device with the lowest bridge ID acts as root bridge.</p> <p>This parameter sets the value of the writeable portion of the bridge ID.</p> <p>On devices with identical priority values the one with the lowest MAC address holds a higher priority.</p>	0 – 61440 in steps of 4096	32768

Using the Web Manager:

- Select the **Spanning Tree** Screen, then select the tab **Basic Configuration**
- In the section **(R)STP Configuration** select the respective **STP mode** setting

Note:

In simple network loop scenarios leave the default values as they are.

Using the Command Line Interface (CLI):

- `Protocol.stp.bridge_config.mode = {Disabled|STP|RSTP|MSTP}`
- `Protocol.stp.bridge_config.priority = {0...61440}`
- `Protocol.stp.bridge_config.hello_time = {0...10}`
- `Protocol.stp.bridge_config.max_age = {6...40}`
- `Protocol.stp.bridge_config.forward_delay = {4...30}`
- `Protocol.stp.bridge_config.tx_hold_count = {1...10}`
- `Protocol.stp.bridge_config.ieee_path_cost_model = {1998_COMPLIANT|2004_COMPLIANT}`

3.1.3 Port Configuration

After completing the basic configuration every port has to be configured according to its intended use. I.e., the switch has to decide on port specific priority or cost settings, which of two or more competing ports to use, whether to check for malicious communication on the respective port or how to deal with root bridge data packets on this port.

Parameter	Explanation	Valid Values	Default
Port	This parameter specifies the port to configure. The number of ports corresponds to the design of the respective device.	n/a	n/a
Enabled	Enables or disables (R)STP for this port. Note: If the STP mode is not activated on this device (see Basic Configuration tab) this setting has no effect.	disabled enabled	enabled
Priority	Corresponding to the device priority in basic configuration (lowest value determines the root bridge) a device with multiple active ports has to set the priority for competing ports relating to port costs. Again, the lowest value determines the dominant port.	0 – 240	128
Admin Path Cost	Corresponding to the configured Path Cost Model (see section "Basic Configuration" on page 11) this parameter autodetects the path cost for this port (value "0"). This port path cost value is the contribution to the path cost towards the spanning tree root bridge. It is possible to overwrite this value with a port path cost other than "0" to route data traffic explicitly over this port.	0 – 200000000	0

Application Note

Using Redundancy Protocols with G6 Devices



Parameter	Explanation	Valid Values	Default
Admin p2p	<p>Basically, there are two types of network connections:</p> <p>Shared-media: Every device can communicate via this connection, assuming all devices have valid access to this network.</p> <p>Point-to-point: The connection only exists between two partners. Generally this "tunneled" communication is not accessible for any other device.</p> <p>The value "force true" indicates that this port should be treated as if it is connected to a point-to-point link.</p> <p>The value "force false" indicates that this port should be treated as having a shared media connection.</p>	auto force false force true	auto
Admin Edge	<p>When enabled, this port is assumed to be an edge port. This means that this port is connected to endpoint remote stations like PCs etc. but no other bridge. Edge ports change slightly faster into forwarding mode and transmit data instantly.</p> <p>Note: The device constantly listens to BPDUs on this port anyway. In case a switch is connected to this specific network the device disables this option.</p>	disabled enabled	disabled
BPDU Guard	<p>When enabled, STP attempts from a user port are blocked. This prevents a malicious user from influencing the overall network routing.</p>	disabled enabled	disabled
Bridge Assurance	<p>The bridge assurance is used to detect unidirectional link failures or remote devices that stop sending spanning tree information due to a software fault.</p> <p>Note: Bridge assurance must be supported by other directly connected switches. Otherwise enabling this parameter takes no effect.</p>	disabled enabled	disabled

Parameter	Explanation	Valid Values	Default
BPDU Rx only	When enabled, this port listens to incoming BPDUs but never transmits any. So the switch gets status information from his neighbors, but does not announce his status to them. This option can be used to avoid sending BPDU data on edge ports or in combination with the BPDU Guard for incoming BPDUs.	disabled enabled	disabled
Restrict TCN	When enabled, the port does not forward Topology Change Notification BPDUs. Usually this is necessary on edge ports, i.e., to protect the network from malicious user action. Note: Because of loss of connectivity information updates, enabling this option could cause connectivity dropouts in the STP network.	disabled enabled	disabled
Restrict Root	When enabled, this port cannot become a root bridge port for STP. Usually this is necessary on edge ports, i.e., to protect the network from malicious user action.	disabled enabled	disabled
Protocol Migration	When operating in RSTP mode, executing this command forces this port to transmit RSTP BPDUs. Note: This action is only executable in the CLI and does not require any parameters.	n/a	n/a

Using the Web Manager:

- Select the **Spanning Tree** Screen, then select the tab **Port Configuration**
- In the section **Port Configuration** select the settings for the respective ports

Note:

In simple network loop scenarios leave the default values as they are.

Using the Command Line Interface (CLI):

- `Protocol.STP.port_config[slot/port ("port name")]`

Note:

To configure all ports at once select `Protocol.STP.port_config[*/*]`

- `Protocol.STP.port_config[slot/port].enable = {Enabled|Disabled}`

- `Protocol.STP.port_config[slot/port].priority = {0...240}`
- `Protocol.STP.port_config[slot/port].admin_p2p_port = {AUTO|FORCE_FALSE|FORCE_TRUE}`
- `Protocol.STP.port_config[slot/port].admin_edge_port = {Enabled|Disabled}`
- `Protocol.STP.port_config[slot/port].admin_path_cost = {0...200000000}`
- `Protocol.STP.port_config[slot/port].bridge_assurance = {Enabled|Disabled}`
- `Protocol.STP.port_config[slot/port].bpdu_guard = {DISABLED|DROP_AND_EVENT|BLOCK_PORT}`
- `Protocol.STP.port_config[slot/port].bpdu_receive_only = {Disabled|Enabled}`
- `Protocol.STP.port_config[slot/port].restrict_tcn = {Disabled|Enabled}`
- `Protocol.STP.port_config[slot/port].restrict_root = {Disabled|Enabled}`

3.1.4 Resulting Switch Settings and Network Structure

When using default settings all connected switches negotiate the following network constellation:

Root bridge

Because of the default priority setting (32768) of all switches the switch with the lowest MAC address becomes the root bridge (Switch S1: 00:60:a7:11:11:11).

Note:

If ports P12 or P13 of switch S1 are configured as "Restrict Root" (what means, they cannot become root bridge ports), the switch with the next lowest MAC address will become the root bridge (Switch S2: 00:60:a7:22:22:22).

Port path cost and path cost:

If the default path cost model settings (IEEE Standard 802.1D-2004) are adopted all port path costs of all ports are the same (1 Gb/s = port path cost of 20 000).

Port roles:

Every switch assigns port roles to its ports according to the resulting loop infrastructure (root port, designated port, blocked/alternate port). With switch S1 as root bridge and connections between switches S1 and S2 as well as between switch S1 and S3 and identical port path costs (20 000) on all ports the following port roles are assigned:

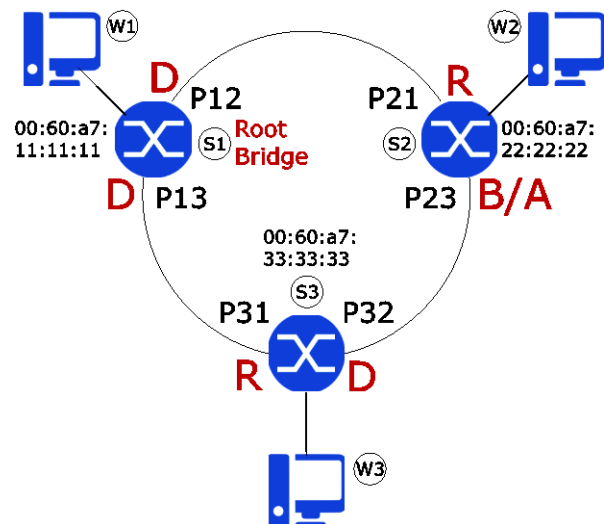


Figure 2:
Resulting Loop Structure

- **Root Port:** As port 21 (switch S2) and port 31 (switch S3) are connected directly to the respective root bridge ports (port 12 and port 13), they are assigned root port role
- **Designated Port:** Port 12 and port 13 (switch S1) both are root bridge ports and thus are assigned designated ports automatically. Port 32 (switch S3) is assigned designated port due to priority settings of switches S2 and S3 (see Blocked/Alternate Port)
- **Blocked or Alternate Port:** To interrupt a network loop one switch within the loop and with multiple paths in the direction of the root bridge has to block one of its ports. This port must not be part of the root path, and its counterpart has to be a designated port. To determine which one of the ports has to be blocked the switches have to decide based on the successive three conditions:
 - Block the port with the highest path cost to the root
 - Block the port to the highest sender bridge ID
 - Block the port with the highest port ID

Note:

In STP mode the respective port acts in "Blocked Port" role, in RSTP mode the respective port acts in "Alternate Port" mode.

Unless a network failure occurs (i.e., cable or plug defect) on both connections switches S1 and S2 as well as switches S1 and S3, the connection between switches S2 and S3 is blocked due to higher path cost in root bridge direction (first condition):

- Path cost from switch S2 directly to switch S1: 20 000
- Path cost from switch S2 to switch S1 via switch S3: 40 000

According to this the connections between switches S1 and S2 as well as between switches S1 and S3 are the connections with the lowest path costs at the moment (20 000 each). This means, when workstation W2 wants to communicate with workstation W3 the data is sent from switch S2 to switch S3 via switch S1.

If the automatic path cost calculation of one of the three switches S1 to S3 recalculates the respective port path cost due to a network failure (e.g. cable interruption) the connection between switches S2 and S3 may become the new connection with the lowest path cost.

3.1.5 Monitoring (R)STP Bridge Status

For network and failure analysis the device displays all current (R)STP specific values of the switch and its ports.

Parameter	Explanation	Valid Values
Spanning Tree Function	A green icon indicates that STP is activated.	enabled (green) disabled (gray)
Protocol	Shows the protocol specification.	3: 802.1D
Hello Time (sec)	The current amount of time between configuration BPDUs by this node on any port when it is the root bridge of the STP network (or trying to become so).	0 – 65535

Parameter	Explanation	Valid Values
Max. Age (sec)	The current maximum age in seconds of STP information learned from the network on any port before the device discards it.	0 – 65535
Hold Time (sec)	This time value determines the interval length during which no more than two configuration BPDUs shall be transmitted by this node.	0 – 65535
Forward Delay (sec)	This time value controls how fast a port changes its spanning state when moving towards the forwarding state. The value shows how long the port stays in each of the listening and learning states which precede the forwarding state.	0 – 65535
Root Port	The number of the port that offers the lowest path cost from this bridge to the root bridge.	0 – 255
Root Cost	The lowest path cost from this bridge to the root bridge.	0 – 4294967295
STP Topology Changes	The total number of topology changes detected by this bridge since the management entity was last reset or initialised.	0 – 65535
Time since Topology Change (sec)	The time in seconds since when a topology change was detected.	0 – 4294967295
Max Hops	A hop is the connection count from one device to its neighbor. Any receiver of an MSTI increases the hop count by 1 and forwards it to its neighbors. If the hop count of a MSTI exceeds this parameter the device discards this MSTI.	6 – 40

Using the Web Manager:

- Open the Web Manager on the respective Switch
- Select the **Spanning Tree** Screen, then select the tab **(R)STP Status**
- The section **(R)STP Bridge Status** lists the bridge specific values

Using the Command Line Interface (CLI):

- **Protocol.stp.bridge_status**

Among others the CLI shows these (R)STP relevant parameters:

```

>> stp_protocol           : 3
    hello_time            : 2

```

```

max_age           : 20
hold_time         : 0
forward_delay     : 15
root_port         : 1/1
root_cost         : 0
topology_changes  : 2
last_topologychange : 4 min 38 secs
max_hops          : 20

```

3.1.6 Monitoring (R)STP Port Status

As port parameters are separately configured each port can have different values.

Note:

Some values are not available with the Web Manager. Use the CLI to retrieve those values.

Parameter	Explanation	Valid Values
Port	Shows the port number for which this STP status information applies. The number of ports corresponds to the design of the respective device.	
en.	A green icon indicates that the respective protocol is enabled on this port.	enabled (green) disabled (gray)
Status	This state shows what action a port takes upon reception of a frame.	UNKNOWN DISCARDING LEARNING FORWARDING BLOCKING LISTENING BROKEN
Designated Root MAC	This value contains the MAC address part of the root bridge ID as it is transmitted in the configuration BPDU by the designated neighbor bridge to which this port is connected.	MAC address format hh-hh-hh-hh-hh-hh (hh = hexadecimal number between 00 to ff)
Designated Cost	The path cost of the designated port of the segment connected to this port. This value is compared to the Root Path Cost field in received BPDUs.	0 – 4294967295

Application Note

Using Redundancy Protocols with G6 Devices



Parameter	Explanation	Valid Values
Designated Bridge MAC	The MAC address of this designated bridge.	MAC address format hh-hh-hh-hh-hh-hh (hh = hexadecimal number between 00 to ff)
Designated Port ID	The priority and port identifier of this port as designated port.	Max. 32 characters Usage: <Priority>: <Port ID>
Forward Transitions	The number of times this port has transitioned from learning to forwarding state.	0 – 4294967295
Oper p2p	A green icon indicates that this port operates in point-to-point mode, otherwise it operates in shared-media mode.	enabled (green) disabled (gray)
Oper Edge	A green icon indicates that this port operates as edge port.	enabled (green) disabled (gray)
Role	Indicates the assigned port role.	UNKNOWN ROOT DESIGNATED ALTERNATE BACKUP MASTER DISABLED
Local Port Cost	The contribution of this port to the overall path cost towards the root bridge.	0 – 4294967295
Designated Port	This value contains the port ID of this designated port. A port ID is a combination of port priority and port number (quite similar to the bridge ID consisting of bridge priority and MAC).	0 – 4294967295
Designated Port Priority	This value contains the priority part of the port ID of this designated port.	0 – 4294967295

Parameter	Explanation	Valid Values
Designated Root ID	This value contains the root bridge ID as it is transmitted in the configuration BPDU by the designated neighbor bridge to which this port is connected.	Max. 32 characters
Designated Root Priority	This value contains the priority part of the root bridge ID as it is transmitted in the configuration BPDU by the designated neighbor bridge to which this port is connected.	0 – 65535
Designated Bridge ID	This value contains the bridge ID of this designated bridge.	Max. 32 characters
Designated Bridge Priority	This value contains the priority part of the bridge ID of this designated bridge.	Max. 32 characters
Inconsistent Bridge	Value "true" indicates that the port is inconsistent due to Bridge Assurance.	true false

Using the Web Manager:

- Open the Web Manager on the respective Switch
- Select the **Spanning Tree** Screen, then select the tab **(R)STP Status**
- The section **Port Status** lists the port and slot specific values

Using the Command Line Interface (CLI):

- `Protocol.stp.port_status[slot/port ("port name")].port`
- `Protocol.stp.port_status[slot/port ("port name")].state`
- `Protocol.stp.port_status[slot/port ("port name")].local_port_cost`
- `Protocol.stp.port_status[slot/port ("port name")].designated_port_id`
- `Protocol.stp.port_status[slot/port ("port name")].designated_port`
- `Protocol.stp.port_status[slot/port ("port name")].designated_port_priority`
- `Protocol.stp.port_status[slot/port ("port name")].designated_cost`
- `Protocol.stp.port_status[slot/port ("port name")].designated_root_id`

- `Protocol.stp.port_status[slot/port ("port name")].designated_root_mac`
- `Protocol.stp.port_status[slot/port ("port name")].designated_root_priority`
- `Protocol.stp.port_status[slot/port ("port name")].designated_bridge_id`
- `Protocol.stp.port_status[slot/port ("port name")].designated_bridge_mac`
- `Protocol.stp.port_status[slot/port ("port name")].designated_bridge_priority`
- `Protocol.stp.port_status[slot/port ("port name")].forward_transiton`
- `Protocol.stp.port_status[slot/port ("port name")].oper_edge_port`
- `Protocol.stp.port_status[slot/port ("port name")].oper_p2p_port`
- `Protocol.stp.port_status[slot/port ("port name")].role`
- `Protocol.stp.port_status[slot/port ("port name")].inconsistent_bridge`

It is possible to show all values of one given port by selecting this port and leaving the parameter entry empty:

- `Protocol.stp.port_status[1/1 ("Port1")].`
 - » port : 1/1
 - state : FORWARDING
 - local_port_cost : 100
 - designated_port_id : 128 / 01
 - designated_port : 1
 - designated_port_priority: 128
 - designated_cost : 0
 - designated_root_id : 32768 / 00:60:47:11:22:33
 - designated_root_mac : 00:60:a7:11:22:33
 - designated_root_priority: 32768
 - designated_bridge_id : 32768 / 00:60:a7:11:22:33
 - designated_bridge_mac : 00:60:a7:11:22:33
 - designated_bridge_prior~: 32768
 - forward_transition : 1
 - oper_edge_port : False
 - oper_p2p_port : True
 - role : DESIGNATED
 - inconsistent_bridge : False

List the same parameter value for every port as follows:

- `Protocol.stp.port_status[*/*].role`

```

» [1/1].role: DESIGNATED
  [1/2].role: ROOT
  [1/3].role: DESIGNATED
  [1/4].role: ALTERNATE
  [1/5].role: UNKNOWN
  [1/6].role: UNKNOWN

```

3.2 Example 2: Configuring MSTP for two RSTP instances

Note:

For general configuration of VLAN settings please refer to the Application Note "VLAN Configuration of G6 Devices".

3.2.1 Topology Description

To describe the MSTP configuration we use a simple network infrastructure with three switches managing six VLANs in one region.

Three switches S1, S2 and S3 are connected to each other, building a physical network loop. They share the same physical topology, called the MSTP region "Region1".

Inside this region there are six independent VLANs 100 to 600, which the switches have to map to two independent MSTIs "Instance 1" and "Instance 2".

The configuration of all switches has to ensure that none of these instances are looped by closing the respective ports.

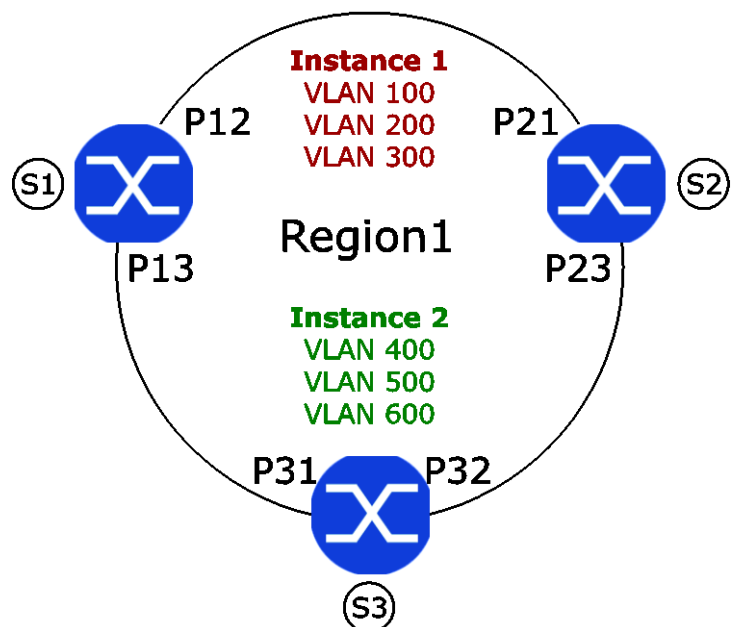


Figure 3: Simple MSTP Network

Element	Description
S1 – S3	Switches S1 to S3 <ul style="list-style-type: none"> • MAC1: 00:60:a7:11:11:11 • MAC2: 00:60:a7:22:22:22 • MAC3: 00:60:a7:33:33:33

Pxx	<p>Ports connecting the respective switches:</p> <ul style="list-style-type: none"> • P12: Port that connects switch S1 with switch S2 • P21: Port that connects switch S2 with switch S1 • P13: Port that connects switch S1 with switch S3 • etc. <p>Note: The port that is directly connected to a client is called an "edge port".</p>
VLAN 100...600	<p>VLANs connecting different network members and services independently. These VLANs should be mapped to two instances:</p> <ul style="list-style-type: none"> • VLAN 100, 200, 300: Instance 1 • VLAN 400, 500, 600: Instance 2 <p>Thus, every switch runs only two MSTIs instead of six STP instances (one STP instance for every VLAN).</p>

3.2.2 Basic Configuration

For basic configuration of the RSTP part please refer to the section "3.1.2 Basic Configuration".

Additionally, the MSTP function has to be enabled on all switches as follows:

Using the Web Manager:

- Open the Web Manager on the respective switch
- Select the **Spanning Tree** Screen, then select the tab **Basic Configuration**
- In the section **Basic Configuration** select the **Mode** "MSTP Mode"

Using the Command Line Interface (CLI):

- `Protocol.stp.bridge_config.mode = MSTP`

Before using MSTP several additional basic MSTP parameters have to be configured on all connected switches.

Parameter	Explanation	Valid Values	Default
Region Name	<p>This parameter specifies the region this device belongs to. The MSTP communication only takes place with other devices of the same region.</p> <p>For example 2 the region name for all switches is "Region1".</p>	Max. 32 characters	empty
Revision Level	<p>MSTP regions can differ by their revision. This revision number must be the same on all MSTP devices.</p> <p>For example 2 leave the default.</p>	0 – 65535	0

Parameter	Explanation	Valid Values	Default
Max Hops	A hop is the connection count from one device to its neighbor. Any receiver of a MSTI message increases the hop count by 1 and forwards it to its neighbors. If the hop count of a MSTI message exceeds this parameter the device discards this MSTI message. For example 2 leave the default.	6 – 40	20
STP Aging Time	This parameter sets the timeout period in seconds for learned MSTI message. Note: This parameter is only used when MSTP is forced into STP mode for rapid aging. For example 2 leave the default.	10 – 1000000	300

Using the Web Manager:

- Open the Web Manager on the respective switch
- Select the **Spanning Tree** Screen, then select the tab **Basic Configuration**
- In the section **MSTP Configuration** define the respective MSTP settings

For example 2 the region name for all switches is "Region1".

Note:

For example 2 there is no need to change the other default values.

Using the Command Line Interface (CLI):

- `Protocol.stp.bridge_config.mstp_region_name = Region1`

Note:

For example 2 there is no need to change the other default values.

With MSTP, a switch "bundles" several VLANs to a respective instance (MSTI). Thus, a switch saves resources by running only a few MSTIs containing several VLANs instead of one RSTP instance for every VLAN itself.

Note:

This example assumes that VLANs are generally configured on every switch S1, S2 and S3. For more information about configuring VLAN please refer to the Application Note "VLAN Configuration of G6 Devices".

In the next step the VLANs 100 to 600 are defined and mapped to the respective MSTI.

#	en.	Alias	VID	MSTP Group	PRIO override	Mgmt	1 1	2 1	2 2	2 3	2 4	2 5	2 6
1	<input checked="" type="checkbox"/>	VLAN 100	100	1	-	all	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	VLAN 200	200	1	-	all	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>	VLAN 300	300	1	-	all	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>	VLAN 400	400	2	-	all	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>	VLAN 500	500	2	-	all	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>	VLAN 600	600	2	-	all	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 4: Configuring VLAN IDs in Web Manager

Using the Web Manager:

- Open the Web Manager on the respective switch
- Select the **VLANs** Screen, then select the tab **VLAN Table**
- For every VLAN ID click the button **add table entry**
- In the section **VLAN Table** enable all VLANs
- Enter the VLAN **Alias** "VLAN 100" to "VLAN 600"
- Enter the respective VLAN ID **VID** "100" to "600"
- Map the VLAN to **MSTP Group** "1" (MSTI 1) or "2" (MSTI 2)
- Click the button **apply to running configuration** to save the changes to the running configuration

Using the Command Line Interface (CLI):

For every VLAN define the respective VLAN ID:

- `Protocol.VLAN.filter_config[*].vlan_id = [100|200|300|400|500|600]`

Assign the VLAN alias for every VLAN:

- `Protocol.VLAN.filter_config[100|200|300|400|500|600].alias = [VLAN 100|VLAN 200|VLAN 300|VLAN 400|VLAN 500|VLAN 600]`

Map the VLANs to the respective MSTP Group:

- `Protocol.VLAN.filter_config[100].mstp_group = 1`
- `Protocol.VLAN.filter_config[200].mstp_group = 1`
- `Protocol.VLAN.filter_config[300].mstp_group = 1`
- `Protocol.VLAN.filter_config[400].mstp_group = 2`
- `Protocol.VLAN.filter_config[500].mstp_group = 2`
- `Protocol.VLAN.filter_config[600].mstp_group = 2`

Note:

For example 2 there is no need to change the other default values.

To get an overview of all VLAN IDs, enter

□ **Protocol.VLAN.filter_config[*].**

```

» Parameter      : [100]    [200]    [300]    [400]    [500]    [600]
  vlan_id        : 100      200      300      400      500      600
  entry_mode     : Enabled  Enabled  Enabled  Enabled  Enabled  Enabled
  alias          : VLAN 1~  VLAN 2~  VLAN 3~  VLAN 4~  VLAN 5~  VLAN 6~
  mstp_group     : 1        1        1        2        2        2

```

Similar to competing bridges and ports in STP networks, the MSTP network has to determine the bridge with the lowest priority as MSTI root bridge for every MSTI.

Parameter	Explanation	Valid Values	Default
MSTP ID	The MSTP Groups table defines MSTP parameters that may be different for individual MST instances (MSTI). Several VLANs may share the same MSTP group. Up to 63 table entries are possible. This parameter corresponds to the MSTI (MSTP Group) defined in the step before.	1 – 63	1
Bridge Priority	According to the Priority parameter this parameter sets the value for the part of the bridge ID that can be modified.	0 – 61440 in steps of 4096	32768

Using the Web Manager:

- Select the **Spanning Tree** Screen, then select the tab **Basic Configuration**
- Below the section **MSTP Configuration** click on **add table entry** for every MSTI
- In the new created fields insert the respective **MSTP group** settings:
 - **MSTP ID:** "1" for MSTI 1
 - **MSTP ID:** "2" for MSTI 2

- To determine the root bridge for the MSTI, the **Bridge Priority** is configured on the respective switch as follows:
 - Switch S1:
 - **Bridge Priority** for MSTI 1: 32768
 - **Bridge Priority** for MSTI 2: 32768
 - Switch S2:
 - **Bridge Priority** for MSTI 1: 16384
 - **Bridge Priority** for MSTI 2: 24576
 - Switch S3:
 - **Bridge Priority** for MSTI 1: 24576
 - **Bridge Priority** for MSTI 2: 16384

Note:

To remove an existing group entry, click on the respective **Remove** button.

Using the Command Line Interface (CLI):

- `Protocol.stp.mstp_group[*].mstp_id = 1`
- `Protocol.stp.mstp_group[*].mstp_id = 2`

To determine the root bridge for the MSTI, the Bridge Priority is configured on the respective switch as follows:

Switch S1:

- `Protocol.stp.mstp_group[1].bridge_priority = 32768`
- `Protocol.stp.mstp_group[2].bridge_priority = 32768`

Switch S2:

- `Protocol.stp.mstp_group[1].bridge_priority = 16384`
- `Protocol.stp.mstp_group[2].bridge_priority = 24576`

Switch S3:

- `Protocol.stp.mstp_group[1].bridge_priority = 24576`
- `Protocol.stp.mstp_group[2].bridge_priority = 16384`

Note:

To delete an entry use `Protocol.stp.mstp_group[{0...63}].mstp_id =`

3.2.3 Port Configuration

In addition to the RSTP port configuration described in section "3.1.3 Port Configuration", the configuration of some more port parameters for MSTP use is necessary.

Parameter	Explanation	Valid Values	Default
MSTP Default Priority	Corresponding to device and port priorities, to decide which (physical) connection to prefer, the MSTP priority determines which (logical) connection to prefer on competing VLAN groups. This parameter defines the port priority in all MSTP instances unless otherwise configured in MSTP Port Priority.	0 – 240	128
MSTP Port Priority	<p>This parameter defines the port priorities used in all specific MSTP instances in a comma-separated list.</p> <p>Note: Every port not mentioned receives the MSTP Default Priority.</p>	<p>Max. 256 characters</p> <p>The Port Priority range is 0 – 240.</p> <p>Usage: <MSTP ID>:<MSTP Port Priority>[,]</p> <p>Example: 1:32, 2:128, 5:128</p>	empty
MSTP Def. APC	The MSTP Default Admin Path Cost (APC) defines the MSTP port cost in all MSTP instances unless otherwise configured in MSTP Port APC.	0 – 200000000	0

Parameter	Explanation	Valid Values	Default
MSTP Port APC	<p>Corresponding to the configured Path Cost Model (see "Basic Configuration" on page 24), the MSTP Port Admin Path Cost autodetects the path cost for this MSTP port (value "0"). This port path cost is the contribution to the path cost for this port and multiple MSTP instances.</p> <p>It is possible to overwrite this value with a port path cost other than "0" to route data traffic explicitly over this port or MSTP instance. The example on the right reads:</p> <ul style="list-style-type: none"> • Instance 1: cost 4 • Instance 2: cost 100 • all other instances: cost 0, which means autodetection of path cost due to configured path cost model 	<p>Max. 256 characters</p> <p>The Port Admin Path Cost range is 0 – 200000000.</p> <p>Usage: <MSTP ID>:<MSTP Port APC>[,]</p> <p>Example: 1:4, 2:100</p>	empty

Using the Web Manager:

- Open the Web Manager on the respective switch
- Select the **Spanning Tree** Screen, then select the tab **Port Configuration**
- In the section **Port Configuration** select the settings for the respective ports

Note:

These parameters are mentioned for information purposes only. For example 2 there is no need to change the default values.

Using the Command Line Interface (CLI):

- `Protocol.STP.port_config[slot/port ("port name")]`

Note:

To configure all ports at once select `Protocol.STP.port_config[*/*]`

- `Protocol.STP.port_config[slot/port].mstp_default_priority = {0...240}`
- `Protocol.STP.port_config[slot/port].mstp_port_priority = {<MSTP ID>:<Port Priority>[;<MSTP ID>:<Port Priority>]}`
- `Protocol.STP.port_config[slot/port].mstp_default_admin_path_cost = {0...200000000}`
- `Protocol.STP.port_config[slot/port].mstp_port_admin_path_cost = {<MSTP ID>:<Port Path Cost>[;<MSTP ID>:<Port Path Cost>]}`

Note:

These parameters are mentioned for information purposes only. For example 2 there is no need to change the default values.

3.2.4 Resulting Switch Settings and Network Structure

With the settings configured as before all connected switches negotiate the following network constellation:

Root Bridge

Because of the bridge priority settings, switch S2 is root bridge for instance 1 and switch S3 is root bridge for instance 2.

Port Roles

Because all ports hold the same port priority (default values), the bridge priority is crucial for the respective port role per MSTI.

- **MSTI 1**

- **Root Ports:**

With switch S2 as root bridge for MSTI 1 the ports 12 (switch S1) and 32 (switch S3) are root ports

- **Designated Ports:**

Port 21 and port 23 (switch S2) both are root bridge ports and thus are assigned designated ports automatically. Port 31 (switch S3) is assigned designated port due to priority settings of switches S1 and S3 (see Blocked/Alternate Port)

- **Blocked/Alternate Ports:**

To determine which of both ports has to be blocked both switches root path costs and, if they are equal, both port IDs are compared. The port with the lowest path cost and port ID is assigned designated port, his counterpart is assigned blocked or alternate port. With switch S3 having a lower ID than switch S1 port 31 is a designated port whereas his counterpart port 13 of switch S1 is the blocked or alternate port

- **MSTI 2**

- **Root Ports:**

With switch S3 as root bridge for MSTI 2 the ports 13 (switch S1) and 23 (switch S2) are root ports

- **Designated Ports:**

Port 31 and port 32 (switch S3) both are root bridge ports and thus are assigned designated ports automatically. Port 21 (switch S2) is assigned designated port due to priority settings of switches S1 and S2 (see Blocked/Alternate Port)

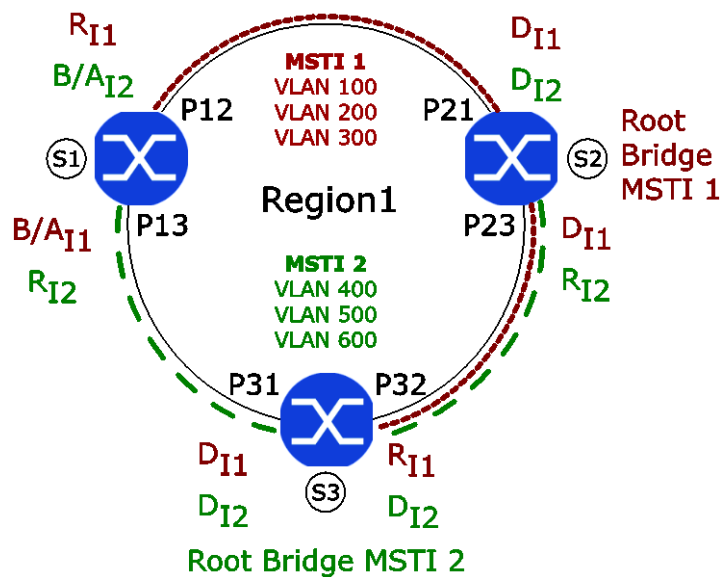


Figure 5:
Resulting MSTP Network Structure

- **Blocked/Alternate Ports:**

To determine which of both ports has to be blocked both switches root path costs and, if they are equal, both port IDs are compared. The port with the lowest path cost and port ID is assigned designated port, his counterpart is assigned blocked or alternate port. With switch S2 having a lower ID than switch S1 port 21 is a designated port whereas his counterpart port 12 of switch S1 is the blocked or alternate port

3.2.5 Monitoring MSTP Bridge Status

For network and failure analysis the device displays all current MSTP specific values of the switch and its ports.

Note:

For further information about (R)STP bridge status please refer to section "3.1.5 Monitoring (R)STP Bridge Status".

Parameter	Explanation	Valid Values
MSTP Region Name	This is the current MSTP region name the bridge participates in.	Max. 32 characters
MSTI Revision Level	This is the current MSTI configuration revision level. Note: Every switch in this specific MSTP region must match this revision level.	0 – 65535
CIST Internal Root Path Cost	This is the path cost to reach the CIST regional root in the same region.	0 – 4294967295
CIST Regional Root ID	This value contains the bridge ID of the current CIST regional root bridge.	Max. 32 characters
CIST Regional Root Priority	This value contains the bridge priority part of the current CIST regional root bridge.	0 – 4294967295
CIST Regional Root MAC	This value contains the bridge MAC part of the current CIST regional root bridge.	MAC address format

Using the Web Manager:

- Open the Web Manager on the respective switch
- Select the **Spanning Tree** Screen, then select the tab **MSTP Status**
- The section **MSTP Bridge Status** lists the values for MSTP bridge

Using the Command Line Interface (CLI):

□ **Protocol.STP.bridge_status.**

Among others the CLI shows these MSTP relevant parameters:

```

» mstp_region_name      : Region1
  mstp_revision_level   : 0
  cist_internal_root_path~: 0
  cist_regional_root_id  : 32768 / 00:60:a7:11:22:33
  cist_regional_root_prio~: 32768
  cist_regional_root_mac : 00:60:a7:11:11:11
  mstp_stp_aging_time    : 300

```

Note:

The values for `cist_regional_root_id` and `cist_regional_root_prio~` differ to the respective switch configuration.

3.2.6 Monitoring MSTP Group Status or MSTP ID Status

This section contains information about the specific MSTP groups. Because the switch can manage more than one port within a MSTP group, there are up to 2048 entries possible.

Parameter	Explanation	Valid Values
MSTP ID	Shows the MSTP group ID.	Max. 4 characters
Port ID	Shows the MSTP port ID.	0 – 255
State	This state shows what action this port takes upon reception of a frame.	UNKNOWN DISCARDING LEARNING FORWARDING BLOCKING LISTENING BROKEN
Port Priority	This value contains the priority part of the port ID of this designated port on the designated bridge.	0 – 255
int. Admin Path Cost	Shows the current port path cost used in this MSTP instance.	0 – 200000000
Forward Transition	The number of times this port has transitioned from learning to forwarding state.	0 – 4294967295

Parameter	Explanation	Valid Values
Role	Indicates the assigned port role.	UNKNOWN ROOT DESIGNATED ALTERNATE BACKUP MASTER DISABLED

Using the Web Manager:

- Open the Web Manager on the respective switch
- Select the **Spanning Tree** Screen, then select the tab **MSTP Status**
- The section **MSTP Status** lists the values for every MSTP group

Using the Command Line Interface (CLI):

- `Protocol.STP.mstp_status_table[entry].`

Note:

To list the status of all entries at once select `Protocol.STP.mstp_status_table[*]`

Note:

To get the parameters' values navigate to the specific parameter. Then press the Return (Enter) key.

- ```

>> Protocol.STP.mstp_status_table[1].role
[1].role: DESIGNATED

```
- `Protocol.STP.mstp_status_table[entry].mstp_id`
  - `Protocol.STP.mstp_status_table[entry].port`
  - `Protocol.STP.mstp_status_table[entry].state`
  - `Protocol.STP.mstp_status_table[entry].port_priority`
  - `Protocol.STP.mstp_status_table[entry].internal_admin_path_cost`
  - `Protocol.STP.mstp_status_table[entry].forward_transition`
  - `Protocol.STP.mstp_status_table[entry].role`

### 3.2.7 Monitoring MSTP Bridge Status by MSTP Group

Some bridge status values can differ between the specific MSTP groups (at most 63 entries).

| Parameter          | Explanation                                                                                                             | Valid Values                                                                          |
|--------------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| MSTP ID            | Shows the MSTP group ID.                                                                                                | Max. 4 characters                                                                     |
| Bridge Priority    | This value contains the priority part of the bridge ID for this MSTP instance.                                          | 0 – 61440                                                                             |
| Root Port          | Shows the port number of the port that offers the lowest path cost.                                                     | 0 – 255                                                                               |
| Root Cost          | Shows the cost of the path to this regions root bridge as seen from this bridge                                         | 0 – 4294967295                                                                        |
| Max. Hops          | Shows the current value of remaining hops for MSTI information generated at the boundary of an MSTI region.             | 0 – 65535                                                                             |
| Reg. Root ID       | This value contains the bridge ID of the MSTP regions root bridge.<br>Example: "32768/00:60:a7:04:90:1e"                | <Priority>/<MAC>                                                                      |
| Reg. Root Priority | This value contains the priority part of the MSTP regions root bridge ID.                                               | 0 – 65535                                                                             |
| Reg. Root MAC      | This value contains the MAC address part of the MSTP regions root bridge ID.                                            | MAC address format<br>hh-hh-hh-hh-hh-hh<br>(hh = hexadecimal number between 00 to ff) |
| Top. Changes       | The total number of topology changes detected by this bridge since the management entity was last reset or initialised. | 0 – 65535                                                                             |

Using the Web Manager:

- Open the Web Manager on the respective switch
- Select the **Spanning Tree** Screen, then select the tab **MSTP Status**
- The section **Bridge Status** lists the MSTP group specific values for this bridge

Using the Command Line Interface (CLI):

**Note:**

To get the parameters' values navigate to the specific parameter. Then press the Return (Enter) key.

```
» Protocol.STP.mstp_bridge_status[*].mstp_id
 [1].mstp_id: 1
 [2].mstp_id: 2
```

- Protocol.STP.mstp\_bridge\_table[entry].mstp\_id
- Protocol.STP.mstp\_bridge\_table[entry].bridge\_priority
- Protocol.STP.mstp\_bridge\_table[entry].root\_port
- Protocol.STP.mstp\_bridge\_table[entry].root\_cost
- Protocol.STP.mstp\_bridge\_table[entry].max\_hops
- Protocol.STP.mstp\_bridge\_table[entry].regional\_root\_id
- Protocol.STP.mstp\_bridge\_table[entry].regional\_root\_priority
- Protocol.STP.mstp\_bridge\_table[entry].regional\_root\_mac
- Protocol.STP.mstp\_bridge\_table[entry].topology\_changes
- Protocol.STP.mstp\_bridge\_table[entry].last\_topology\_change

## **4 MICROSENS Redundant Ring Protocol**

The MICROSENS Redundant Ring Protocol offers an ultra-fast recovery time ranging from less than 20 to 50 milliseconds within MICROSENS Ring Topologies. That means that in case of failure of a node segment, the MICROSENS ring master automatically reconfigures the remaining switches for continuous data flow in less than 20 to 50 milliseconds. For comparison, STP needs up to 50 seconds at worst to reconfigure all switches, RSTP still needs approximately 1 second. This very short reconfiguration time of MICROSENS Ring protocol guarantees a lossless operation of time-critical network data management and controlling.

Signaling between all network partners happens only in case of a network failure so that during normal operation the full network bandwidth is available for operational network data traffic.

A ring may consist of any number of switches. For optimal performance, MICROSENS recommends to plan for up to 25 switches per ring. A switch supports up to two rings simultaneously. The switch displays the enabled rings via its status LEDs 'Ring1' and 'Ring 2'.

It is a free choice of which physical ports operate as ring ports A and B. MICROSENS recommends to choose the same slot for the ports of a ring. When operating two rings, always assign just one physical port to a ring port. When operating fiber optic on all ports, MICROSENS recommends to select different slots for the ports of the different rings.

The G5 and G6 ring protocols are compatible and interwork.

For more information about configuring and using MICROSENS Redundant Ring protocol please refer to chapter "Ring" in the document "Product Manual Firmware, Generation 6" that is included in each software archive and can also be downloaded from the Web Manager's link "Documentation" in the navigation bar.

### **4.1 Example 3: Simple MICROSENS Ring Configuration**

**Note:**

The best practice is to install the switches in their original position and to connect them to a network without closing the ring.

There are three ways to configure the installed switches:

- Using Web Manager
- Using Command Line Interface (CLI)
- Using MICROSENS Network Management Platform (NMP)

**Note:**

When using the MICROSENS NMP for configuration please refer to the MICROSENS NMP documentation for further instructions.

The ring is configured in 3 basic steps:

- Configuring all switches as ring slaves with the respective port settings
- Configuring one switch as ring master
- Physically close the ring

## Application Note

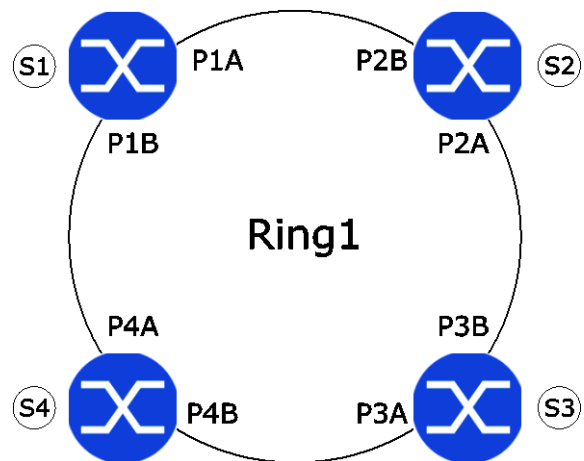
### Using Redundancy Protocols with G6 Devices

# MICROSENS

#### 4.1.1 Topology Description

To describe the MICROSENS Ring configuration we use a simple network infrastructure with a loop. Four switches S1, S2, S3 and S4 are connected to each other, building a loop.

| Element | Description                                                                                                                                                                                                                        |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| S1 – S4 | Switches S1 to S4<br>MAC1: 00:60:a7:11:11:11<br>MAC2: 00:60:a7:22:22:22<br>MAC3: 00:60:a7:33:33:33<br>MAC4: 00:60:a7:44:44:44                                                                                                      |
| PxA/B   | Ports connecting the respective switches: <ul style="list-style-type: none"><li>• P1A: Port A of switch S1, connected to switch S2 (P2B)</li><li>• P2B: Port B of switch S2, connected to switch S1 (P1A)</li><li>• etc.</li></ul> |



#### 4.1.2 Basic Configuration

To use the MICROSENS Ring protocol within the network this feature has to be enabled on all connected switches.

##### Note:

Remember not to physically close the ring unless all switches are properly configured.

Using the Web Manager:

- Open the Web Manager on the respective switch
- Select the **Ring** Screen, then select the tab **Configuration**
- In the section **Port Configuration** enable Ring 1
- Enter "Ring1" as the **Ring name**

##### Note:

This name is only for informational purposes.

- Enter "1" as the **Ring Number**

##### Note:

When left unassigned the default settings "1" for ring index 1 and "2" for ring index 2 are used.

Using the Command Line Interface (CLI):

- `Protocol.Ring.config[1].enable = Enabled`
- `Protocol.Ring.config[1].name = Ring1`

- `Protocol.Ring.config[1].number = 1`

#### 4.1.3 Port Configuration

After completing the basic configuration the MICROSENS ring ports A and B have to be assigned to the switch's physical slots and ports.

| Parameter | Explanation                                                                                                                                                                     | Valid Values                          | Default |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|---------|
| Port A    | Determines the port number that is to be used for ring side A.                                                                                                                  | <Slot/Port> or respective port number | n/a     |
| Port B    | Determines the port number that is to be used for ring side B.<br><br><b>Note:</b><br>The ring master blocks port B when ring is closed. This port is known as the Backup Port. | <Slot/Port> or respective port number | n/a     |

Using the Web Manager:

- Open the Web Manager on the respective switch
- Select the **Ring** Screen, then select the tab **Configuration**.
- In the section **Port Configuration** enter the the ports "2/1" for **Port A** and "2/2" for **Port B**
- Click the button **apply to running configuration** to save the changes to the running configuration

Using the Command Line Interface (CLI):

- `Protocol.Ring.config[1].port_a = 2`
- `Protocol.Ring.config[1].port_b = 3`

#### 4.1.4 Ring Master Configuration

Finally one of the ring switches has to be configured as ring master. During normal network operation this switch blocks its port B to open the network loop.

Using the Web Manager:

- Open the Web Manager on switch S1
- Select the **Ring** Screen, then select the tab **Configuration**
- In the section **Port Configuration** enable **Ring Master** on Ring 1

**Note:**

All other switches are working as "Ring Slaves".

- Click the button **apply to running configuration** to save the changes to the running configuration

Using the Command Line Interface (CLI):

- `Protocol.Ring.config[1].ring_master = Enabled`

#### 4.1.5 Resulting Switch Settings and Network Structure

If all switches are configured correctly, close the ring physically. The ring configuration is complete. As the ring functions fully automatically, no more interference with the switches during operation is required. Upon a ring failure the master will reconfigure the ring. When the ring is closed again the master will automatically fall back into normal operation mode.

With the settings configured as before all connected switches negotiate the following network constellation:

##### Ring Master

As configured switch S1 is the ring master or "Ring1".

##### Ports

The ring master switch S1 blocks its port B and thus intermits the connection between switch S1 and switch S4.

Unless no network failure occurs, data is transmitted from switch S1 to switch S4 via switches S2 and S3.

Whenever there is a network malfunction between those switch connections switch S1 blocks his port A and opens his port B within 20 – 50 milliseconds.

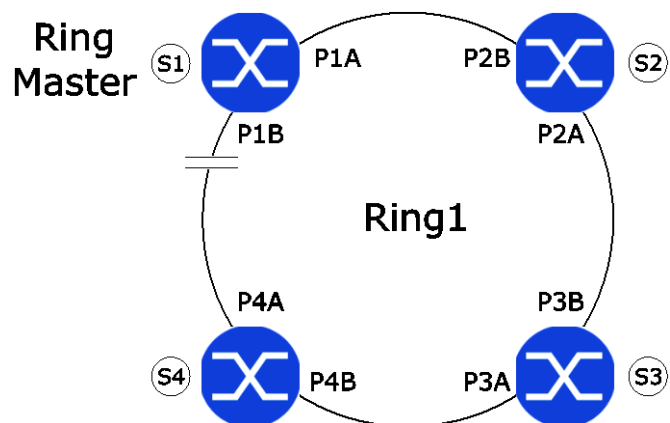


Figure 6: Resulting Ring Topology

#### 4.1.6 Monitoring Ring Status

For network and failure analysis the device displays all current Ring Protocol specific values of the respective ring.

| Parameter         | Explanation                                                                                | Valid Values                                                                             |
|-------------------|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Status            | Shows the current status value of the respective ring.                                     | unused (gray)<br>normal (green)<br>backup (yellow)<br>error (red)<br>misconfigured (red) |
| Last state change | Date and time when the status of the ring protocol has last changed to the current status. | Example:<br>Thu Jul 30<br>09:41:00 2015                                                  |



| Parameter                 | Explanation                                                                                                                                                   | Valid Values  |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Ring Interrupt            | This parameter is "true" if this device has at least one ring port in blocking mode. Otherwise it is "false".<br>(internal status parameter)                  | False<br>True |
| Global Ring Alarm         | This parameter is "true" if an error is detected at this ring.                                                                                                | False<br>True |
| Error detected            | This parameter is "true" for a ring master that received ring failure information from distant slave. Otherwise it is "false".<br>(internal status parameter) | False<br>True |
| Ring port A/B interrupted | This parameter is "true" if the ring port A/B is in blocking state, "false" if it should be in forwarding state.                                              | False<br>True |

Using the Web Manager:

- Open the Web Manager on the respective switch
- Select the **Ring** Screen, then select the tab **Status**
- The section **Ring Status** lists the specific values for both the rings 1 and 2

Using the Command Line Interface (CLI):

- **Protocol.Ring.status[\*].**
  - » Parameter : [1] [2]
  - state : BACKUP UNUSED
  - last\_state\_change : Thu Nov 12 10:18:~
  - ring\_interrupt : True False
  - global\_ring\_alarm : True False
  - error\_detected : False False
  - ring\_port\_a\_interrupted : False False
  - ring\_port\_b\_interrupted : True False

#### 4.1.7 Monitoring Backup Statistics

This section shows information about backups of the respective ring. A backup situation happens when the ring master switch blocks his port A and opens port B.

| Parameter         | Explanation                                                          | Valid Values   |
|-------------------|----------------------------------------------------------------------|----------------|
| Number of backups | Shows the overall number of backups engaged since the last power up. | 0 – 4294967295 |

| Parameter               | Explanation                                                                                                                                                                                                                              | Valid Values  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Current backup duration | Shows since how long a currently active backup is established on the respective ring.<br>CLI format: "7 hrs 27 min 53 secs "<br>Web Manager format: "0 days, 07:27:53"<br><b>Note:</b><br>If no backup is active the value is "0"        | <time period> |
| Last backup duration    | Shows how long the last backup was established on the respective ring.<br>CLI format: "7 hrs 27 min 53 secs "<br>Web Manager format: "0 days, 07:27:53"<br><b>Note:</b><br>If there was no backup since the last reboot the value is "0" | <time period> |
| Total backup duration   | Shows the total time the respective ring was in backup status since last reboot.<br>CLI format: "7 hrs 27 min 53 secs "<br>Web Manager format: "0 days, 07:27:53"                                                                        | <time period> |

Using the Web Manager:

- Open the Web Manager on the respective switch
- Select the **Ring** Screen, then select the tab **Status**
- The section **Statistics** lists the backup values for both the rings 1 and 2

Using the Command Line Interface (CLI):

- **Protocol.Ring.statistics[\*].**
  - » Parameter : [1] [2]
  - number\_of\_backups : 1 0
  - current\_backup\_duration : 7 min 10 secs
  - last\_backup\_duration :
  - total\_backup\_duration : 7 min 10 secs

## **Application Note**

Using Redundancy Protocols with G6 Devices

**MICROSENS**

Intentionally left blank

## **Disclaimer**

All information in this document is provided 'as is' and subject to change without notice. MICROSENS GmbH & Co. KG disclaims any liability for the correctness, completeness or quality of the information provided, fitness for a particular purpose or consecutive damage. Any product names mentioned herein may be trademarks and/or registered trademarks of their respective companies

©2016 MICROSENS GmbH & Co. KG, Küferstr. 16, 59067 Hamm, Germany.  
All rights reserved. This document in whole or in part may not be duplicated, reproduced, stored or retransmitted without prior written permission of MICROSENS GmbH & Co. KG.

Document ID: AN-16007\_2016-05-03