

Setting Up Media Redundancy using RSTP

Abstract:

This application note describes how to implement media redundancy using Rapid Spanning Tree Protocol (RSTP) with Weidmüller managed Ethernet switches and Modbus TCP fieldbus couplers. It explains the underlying redundancy concept and provides a step-by-step guide for configuring the Ethernet network. The resulting redundant network can be used together with controller redundancy solutions such as CODESYS Redundancy to increase the availability of industrial automation systems.

Setting Up Media Redundancy using RSTP

Hardware reference

No.	Component name	Article No.	Hardware / Firmware version
1	IE-SW-AL05LM-5TX	2682250000	HW 01.00 FW 01.19
2	UR20-FBC-MOD-TCP-V2	2476450000	HW 01.00 FW 02.16.00

Software reference

No.	Software name	Article No.	Software version
3	UR20-FBC-MOD-TCP-V2 Firmware		02.16.00

Contact

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
www.weidmueller.com

For any further support please contact your
local sales representative:
<https://www.weidmueller.com/countries>

Content

1	Warning and Disclaimer.....	4
2	Introduction.....	5
3	System Architecture.....	6
3.1	System Overview.....	6
3.2	Network Topology.....	7
3.3	CODESYS Redundancy Principle (System Redundancy).....	8
3.4	Media Redundancy.....	9
4	Configuring the IE-SW-AL05LM-5TX for RSTP.....	10
5	Configuring RSTP on the UR20-FBC-MOD-TCP-V.....	19
6	Verifying the Redundant Network	24
6.1	Verify the Initial RSTP State	24
6.2	Verify the Redundant Network Paths	28

1 Warning and Disclaimer

Warning

Controls may fail in unsafe operating conditions, causing uncontrolled operation of the controlled devices. Such hazardous events can result in death and / or serious injury and / or property damage. Therefore, there must be safety equipment provided / electrical safety design or other redundant safety features that are independent from the automation system.

Disclaimer

This Application Note / Quick Start Guide / Example Program does not relieve you of the obligation to handle it safely during use, installation, operation and maintenance. Each user is responsible for the correct operation of his control system. By using this Application Note / Quick Start Guide / Example Program prepared by Weidmüller, you accept that Weidmüller cannot be held liable for any damage to property and / or personal injury that may occur because of the use. The names *CODESYS Development System* is a registered trademark of CODESYS.

Note

The given descriptions and examples do not represent any customer-specific solutions, they are simply intended to help for typical tasks. The user is responsible for the proper operation of the described products. Application notes / Quick Start Guides / Example Programs are not binding and do not claim to be complete in terms of configuration as well as any contingencies. By using this Application Note / Quick Start Guide / Example Program, you acknowledge that we cannot be held liable for any damages beyond the described liability regime. We reserve the right to make changes to this application note / quick start guide / example at any time without notice. In case of discrepancies between the proposals Application Notes / Quick Start Guides / Program Examples and other Weidmüller publications, like manuals, such contents have always more priority to the examples. We assume no liability for the information contained in this document. Our liability, for whatever legal reason, for damages caused using the examples, instructions, programs, project planning and performance data, etc. described in this Application Note / Quick Start Guide / Example is excluded.

Security notes

In order to protect equipment, systems, machines and networks against cyber threats, it is necessary to implement (and maintain) a complete state-of-the-art industrial security concept. The customer is responsible for preventing unauthorized access to his equipment, systems, machines and networks. Systems, machines and components should only be connected to the corporate network or the Internet if necessary and appropriate safeguards (such as firewalls and network segmentation) have been taken.

2 Introduction

This application note describes the individual steps required to implement a redundant Ethernet network using **Rapid Spanning Tree Protocol (RSTP)** with Weidmüller managed Ethernet switches and **UR20-FBC-MOD-TCP-V2** Modbus TCP fieldbus couplers.

The redundant network presented in this application note is designed to increase the availability of Industrial Ethernet communication by automatically restoring the communication path in the event of a cable or network link failure. The document explains the required hardware topology and the configuration of both the managed Ethernet switches and the Modbus TCP fieldbus couplers to establish a fully operational RSTP network.

This application note focuses exclusively on the implementation of **media redundancy**. The configuration of **CODESYS Controller Redundancy** and **Modbus TCP client redundancy** is described in a separate application note. When combined, both concepts provide a highly available automation system that tolerates both controller failures and network failures.



Note:

The setup, configuration steps and test results described in this application note have been validated exclusively using the hardware and software components listed in the **Hardware Reference** and **Software Reference** sections of this document.

The use of different hardware, firmware versions, software versions, network infrastructure components, or additional third-party devices may influence the behavior of the system and could lead to results that differ from those described herein. Therefore, any deviations from the documented setup must be evaluated and validated individually.

3 System Architecture

3.1 System Overview

The system presented in this application note demonstrates a redundant controller setup using two UC20 controllers and distributed Modbus TCP I/O. The objective is to maintain application execution and communication to the fieldbus level in defined failure scenarios.

The controller redundancy is provided by the CODESYS Redundancy Configuration functionality. In normal operation, one controller operates as an active PLC, while the second controller operates as the standby PLC. Both controllers execute the same application and are synchronized via a dedicated redundancy link. If the active controller becomes unavailable, the standby controller can take over application execution at runtime.

The distributed I/O is connected via two UR20-FBC-MOD-TCP-V2 Modbus TCP fieldbus couplers. For Modbus TCP communication in a redundant controller setup, the CODESYS Modbus TCP Client redundancy mechanism is used. This allows the Modbus TCP communication to be managed according to the current redundancy state of the controllers.

The fieldbus network is built as a redundant Ethernet topology using two managed Ethernet switches. Rapid Spanning Tree Protocol (RSTP) is used to prevent network loops during normal operation and to provide an alternative communication path in case of a cable interruption.

The overall setup combines controller redundancy and network redundancy. Controller redundancy ensures that the application can continue running on the second controller if the active controller fails. Network redundancy ensures that communication to the Modbus TCP fieldbus couplers can continue if one Ethernet connection in the fieldbus network is interrupted.

3.2 Network Topology

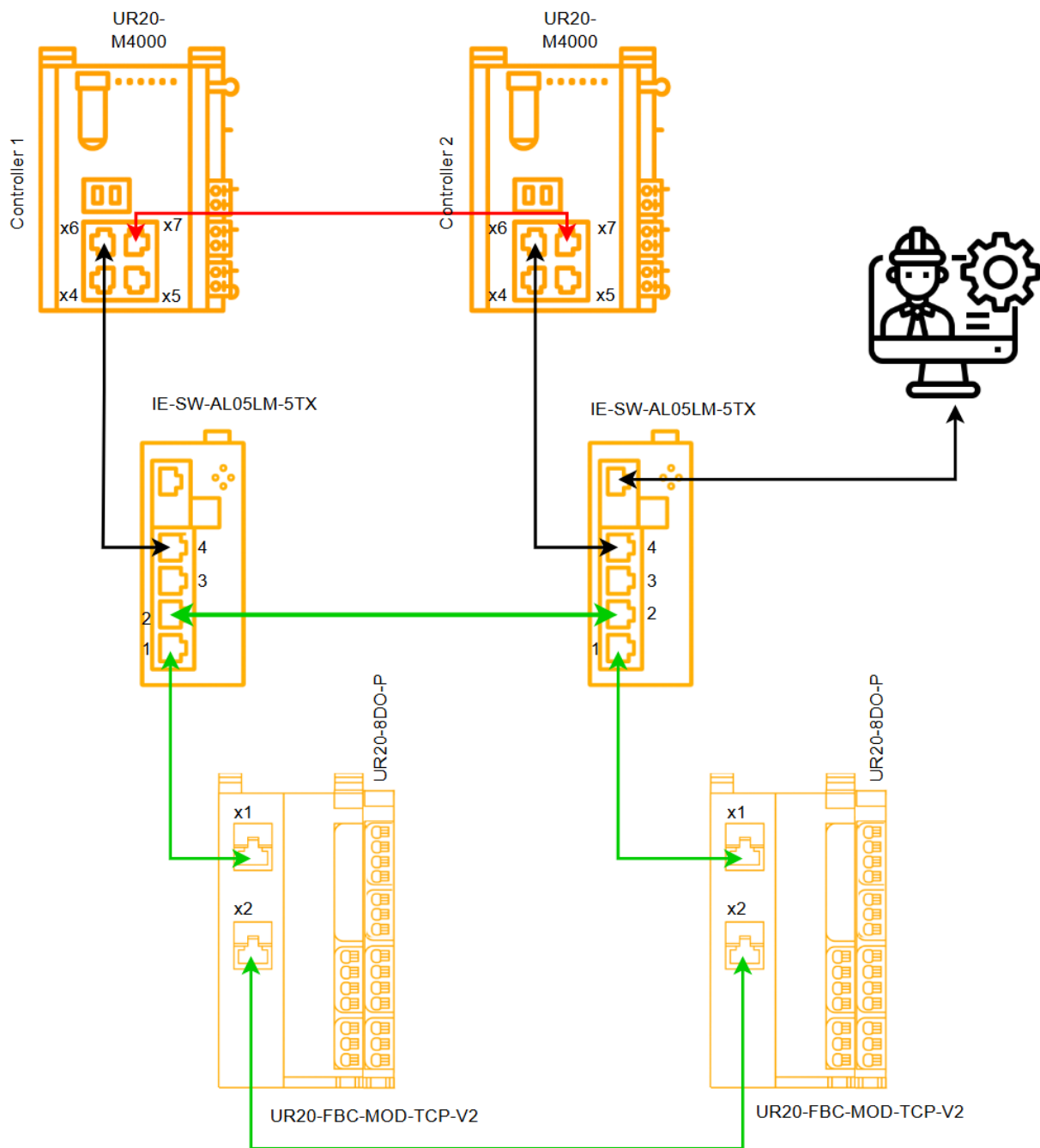


Figure 1: Network Topology

Symbol	Description
	CODESYS Redundancy Link – Synchronization channel between the primary and secondary UC20 controller. Used for redundancy management and data synchronization.
	Controller Ethernet Connection – Ethernet connection between the UC20 controller and the local managed switch.
	Modbus TCP Network (RSTP Ring) – Redundant Ethernet network used for communication between the controllers and the UR20 Modbus TCP fieldbus couplers. Rapid Spanning Tree Protocol (RSTP) provides automatic path redundancy in case of a network failure.

3.3 CODESYS Redundancy Principle (System Redundancy)

The controller redundancy described in this application note is based on the CODESYS Redundancy Configuration. Two UC20-M4000 controllers execute the same application, while only one controller operates as the **active PLC**. The second controller remains in **standby mode**, continuously synchronizing its application data with the active controller and monitoring its operational state.

The official documentation of the “CODESYS Redundancy Configuration” can be found under the following link:

[CODESYS Redundancy Configuration](#)

The synchronization is performed via a dedicated IP-based redundancy link. CODESYS uses both **UDP** and **TCP** communication for the redundancy mechanism. UDP is used for controller status monitoring, while TCP is used for additional redundancy services such as registered area synchronization, visualization redundancy and acyclic data exchange.

Understanding this principle is important because the Modbus TCP communication described in this application note is directly linked to the redundancy state of the controllers. While CODESYS manages the controller switchover, the RSTP-based Ethernet network ensures that the communication path to the distributed Modbus TCP fieldbus couplers remains available in the event of a network failure. Together, these mechanisms provide a high available control system.

3.4 Media Redundancy

In addition to controller redundancy, the communication network must also tolerate failures. If the active controller remains operational but loses the communication path to the distributed I/O, the application can no longer exchange process data with the Modbus TCP fieldbus couplers. Therefore, network redundancy is an essential part of a highly available control system.

In this application, media redundancy is implemented by connecting the managed Ethernet switches and the **UR20-FBC-MOD-TCP-V2 Modbus TCP fieldbus couplers** in a redundant Ethernet ring topology (see Chapter 3.2). Both the managed switches and the fieldbus couplers support the **Rapid Spanning Tree Protocol (RSTP)** and therefore actively participate in the redundant network.

Under normal operating conditions, RSTP blocks one redundant communication path, preventing Ethernet loops while maintaining a backup path. If a cable or communication path fails, the RSTP topology is recalculated and the previously blocked path is enabled. This restores the communication path to the affected fieldbus couplers without requiring manual intervention.

It is important to distinguish between **controller redundancy** and **media redundancy**. CODESYS Redundancy ensures that application execution can continue on the standby controller if the active controller fails. Media redundancy, on the other hand, ensures that the Ethernet communication path between the controllers, switches and Modbus TCP fieldbus couplers remains available after a network failure. Both mechanisms complement each other and are required to achieve a highly available automation system.



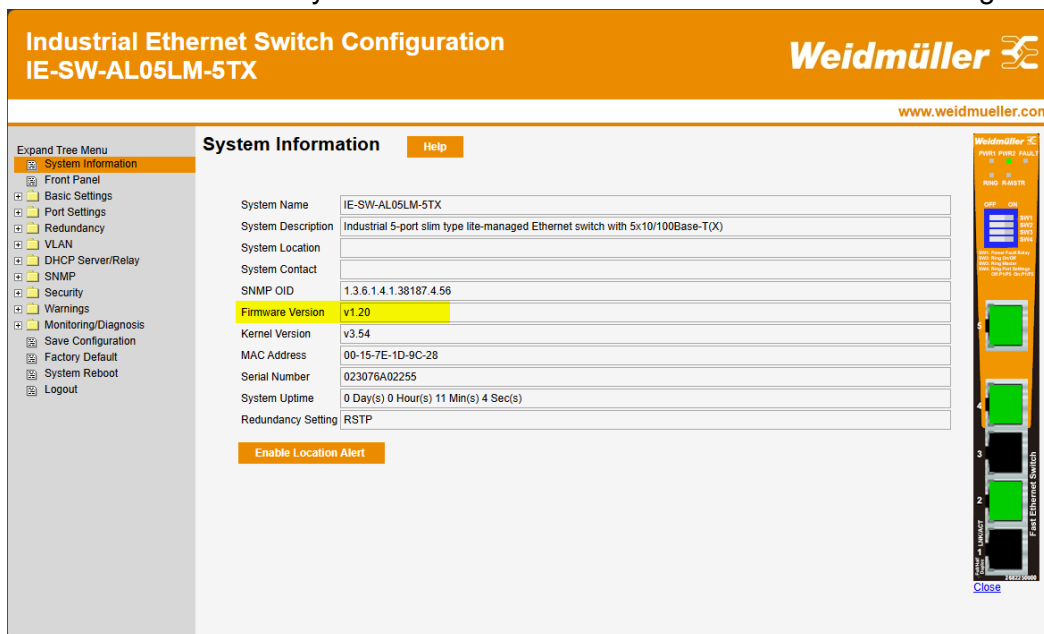
Note:

This application note focuses on the implementation and configuration of **media redundancy** using Rapid Spanning Tree Protocol (RSTP). It describes the configuration of the managed Ethernet switches **IE-SW-AL05LM-5TX** and the **UR20-FBC-MOD-TCP-V2** fieldbus couplers required to establish a redundant Ethernet network.

The configuration of **CODESYS Controller Redundancy** and **Modbus TCP client redundancy** is described in the separate application note **AN0141 – Setting Up CODESYS Controller Redundancy**. Once the redundant network has been commissioned and verified, the controller redundancy can be configured on top of the network infrastructure.

4 Configuring the IE-SW-AL05LM-5TX for RSTP

1. Open a web browser and connect to the switch (default IP-address 192.168.1.110).
2. Create an initial user and set a password (if needed).
3. Afterwards check on the “System Information” which firmware version is running.

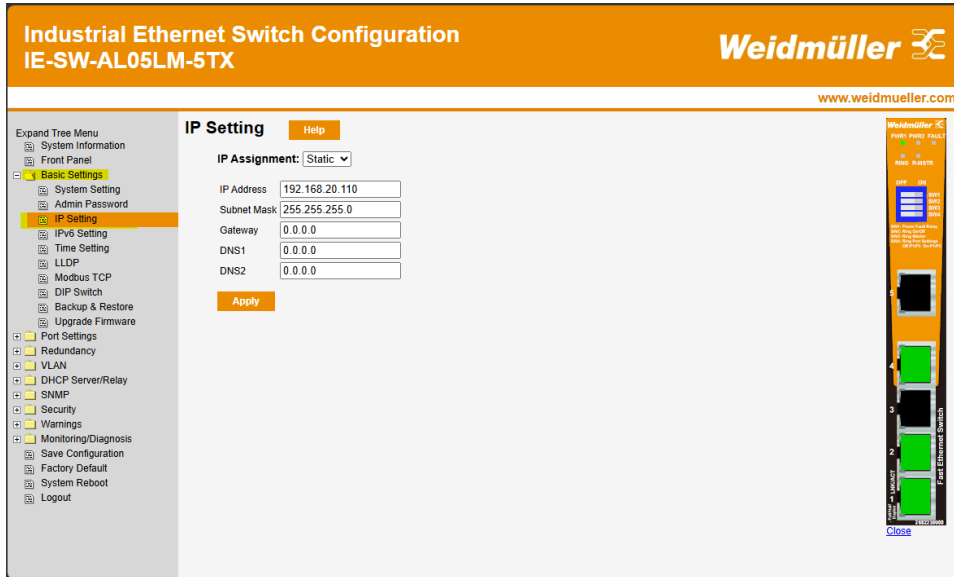


Note:

No specific firmware version is required for this application note. However, it is recommended to use the latest available firmware version to benefit from the most recent bug fixes, security updates, and feature enhancements.

Setting Up Media Redundancy using RSTP

- To simplify access during commissioning and future maintenance, it is recommended to configure the switch with an IP address in the same subnet as the UC20 controllers and the Modbus TCP fieldbus couplers. This allows all devices to be reached from the same engineering workstation without requiring additional network configuration. To configure the IP address, navigate to “Basic Settings” → “IP Settings”.

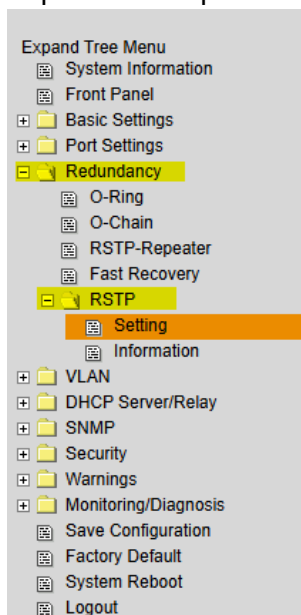


Note:

The IP addresses used for the switches can be selected freely, provided they are unique within the network and belong to the same subnet as the controllers and fieldbus couplers. In this application note, the addresses **192.168.20.110** and **192.168.20.111** were chosen. Using consecutive IP addresses simplifies device identification and provides convenient access during commissioning and maintenance.

Setting Up Media Redundancy using RSTP

5. Set up the RSTP protocol by clicking on “Redundancy” → “RSTP” and then “Settings”



6. Configuring the RSTP Bridge Settings

After enabling RSTP, the bridge parameters must be configured. These parameters determine the behavior of the switch within the RSTP topology. Of particular importance is the Bridge Priority, as this parameter is used to define which device should become the Root Bridge.

In the reference topology, Switch 1 shall operate as the preferred Root Bridge. To ensure deterministic Root Bridge selection, Switch 1 must be configured with a lower Bridge Priority than all other RSTP participants in the network.

Parameter	Switch 1	Switch 2
RSTP Mode	Enabled	Enabled
Bridge Priority	4096	8192
Hello Time	2 s	2 s
Forward Delay	15 s	15 s
Max Age	20 s	20 s

Setting
Help

RSTP Mode : Enabled ▾

Bridge Setting

Priority (0-61440) 4096

Max Age Time (6-40 secs) 20

Hello Time (1-10 secs) 2

Forward Delay Time (4-30 secs) 15

Switch 1

Setting
Help

RSTP Mode : Enabled ▾

Bridge Setting

Priority (0-61440) 8192

Max Age Time (6-40 secs) 20

Hello Time (1-10 secs) 2

Forward Delay Time (4-30 secs) 15

Switch 2

The individual parameters have the following functions:

Bridge Priority

The Bridge Priority is used during the RSTP Root Bridge election. The device with the lowest Bridge ID becomes the Root Bridge. The configured Bridge Priority forms part of the Bridge ID and therefore allows the preferred Root Bridge to be explicitly defined.

A lower numerical Bridge Priority represents a higher preference. By assigning a lower Bridge Priority to Switch 1 than to the other RSTP participants, Switch 1 is selected as the Root Bridge as long as it is available.

If Switch 1 becomes unavailable, the RSTP topology is recalculated and another available RSTP participant becomes the Root Bridge according to the configured priorities and the RSTP election mechanism.

Hello Time

The Hello Time defines the interval at which the Root Bridge transmits RSTP configuration information to the other RSTP participants. For the reference topology, the default value of **2 seconds** is retained.

Max Age

The Max Age defines how long received spanning-tree information remains valid before it is considered outdated. For the reference topology, the default value of **20 seconds** is retained.

Forward Delay

The Forward Delay is a spanning-tree timer associated with transitions between port states. For the reference topology, the default value of **15 seconds** is retained.



Note:

Configuring all RSTP participants with the same Bridge Priority is not recommended for the reference topology. If the Bridge Priority is identical, additional components of the Bridge ID are used to elect the Root Bridge. The resulting Root Bridge may therefore change when a device is replaced or the network topology is modified.

Explicitly assigning different Bridge Priority values makes the intended Root Bridge selection predictable and simplifies commissioning, verification and troubleshooting.

7. Configuring the RSTP Port Settings

The RSTP port settings determine how individual Ethernet ports participate in the spanning-tree topology and how RSTP selects between alternative communication paths.

For the reference topology, no specific communication path or blocking port needs to be preferred. Therefore, the **default port settings can be retained**. The Root Bridge is defined separately by the Bridge Priority as described in Chapter 4.6.

Configure the RSTP port settings as shown below.

Port Setting					
Port No.	Enable	Path Cost (0:auto, 1-200000000)	Priority (0-240)	P2P	Edge
Port 01	enabled ▼	0	128	auto ▼	true ▼
Port 02	enabled ▼	0	128	auto ▼	true ▼
Port 03	enabled ▼	0	128	auto ▼	true ▼
Port 04	enabled ▼	0	128	auto ▼	true ▼
Port 05	enabled ▼	0	128	auto ▼	true ▼

Enable

The **Enable** parameter determines whether the respective port participates in RSTP. RSTP must be enabled on all ports that are part of the redundant network. This allows the connected RSTP devices to exchange BPDUs and include the corresponding links in the spanning-tree calculation.

Path Cost

The **Path Cost** represents the cost associated with using a particular network link. After the Root Bridge has been selected, RSTP uses the accumulated Path Cost to determine the preferred path towards the Root Bridge. A path with a lower accumulated cost is preferred.

When the default configuration is used, the Path Cost does not need to be assigned manually. The switch automatically assigns the appropriate default Path Cost according to the speed of the respective Ethernet port. The following default values are used:

Port Speed	Default Path Cost
100 Mbit/s	200000
1 Gbit/s	20000

For the reference topology, there is no requirement to prefer one side of the ring over the other. Therefore, the automatically assigned default Path Cost values are retained.

If links with different speeds are used, the automatically assigned Path Costs also provide a corresponding path preference. A higher-speed link receives a lower Path Cost and is therefore preferred by RSTP when otherwise equivalent paths are available.

If multiple paths have the same accumulated Path Cost, this does not result in undefined behavior. RSTP uses additional protocol-defined selection criteria to determine the resulting topology. It is therefore not necessary to manually assign different Path Cost values solely to obtain deterministic RSTP operation.

The Path Cost should only be configured manually if the network design explicitly requires a particular communication path to be preferred over the path that would result from the automatically assigned values.

The Path Cost should only be modified if the application requires a particular network path to be preferred.



Note:

Path Cost does not determine which device becomes the Root Bridge. The Root Bridge is selected based on the Bridge ID and is deliberately defined in this application by configuring the Bridge Priority as described in Chapter 4.6. The Path Cost is evaluated afterwards to determine the preferred paths towards the selected Root Bridge.

Admin P2P

The **Admin P2P** parameter defines whether the port is connected through a point-to-point Ethernet link. RSTP can use rapid state transitions on point-to-point links between directly connected devices.

The default setting is retained for the reference topology.

Admin Edge

The **Admin Edge** parameter identifies ports that are connected to end devices and are therefore not expected to create a bridging loop.

Ports that form part of the redundant RSTP ring must not operate as Edge ports because they connect RSTP participants and must participate in the spanning-tree calculation.

The default setting is retained unless the connected device and network design require a different configuration.

Admin Non STP

If **Admin Non STP** is enabled, the respective port does not participate in RSTP.

Ports forming part of the redundant network must participate in RSTP. Therefore, **Admin Non STP must not be enabled for the ring ports.**



Note:

In the reference topology, the RSTP port parameters are intentionally left at their default values. No specific forwarding path or blocking location is required. The only parameter deliberately modified to influence the resulting topology is the **Bridge Priority**, which ensures that the intended switch is selected as the Root Bridge.

8. Save the configuration and restart the switch
 - a. As soon as any parameter has been changed the configuration has to be saved to make it permanently available.

Industrial Ethernet Switch Configuration
IE-SW-AL05LM-5TX

Configuration changed and applied but not saved!

Setting Up Media Redundancy using RSTP

- b. Click on “Save Configuration” and then on save

Save Configuration [Help](#)

Status: Configuration changed but not saved to permanent flash memory.

[Save](#)

- c. Click on System Reboot and then o

Setting [Help](#)

RSTP Mode : Enabled ▼

Bridge Setting

Priority (0-61440)

Max Age Time (6-40 secs)

Hello Time (1-10 secs)

Forward Delay Time (4-30 secs)

Port Setting

Port No.	Enable	Path Cost (0 auto, 1-200000000)	Priority (0-240)	P2P	Edge
Port 01	enabled ▼	0	128	auto ▼	true ▼
Port 02	enabled ▼	0	128	auto ▼	true ▼
Port 03	enabled ▼	0	128	auto ▼	true ▼
Port 04	enabled ▼	0	128	auto ▼	true ▼

5 Configuring RSTP on the UR20-FBC-MOD-TCP-V

1. To connect to the fieldbus coupler connect it via the USB-Service interface to the development computer.
2. Open a web browser and type in the address 192.168.1.102
3. If successfully connected to the coupler you will see the starting page:



Note:

If any IO-cards were added they appear automatically in the web-Ui. If not check if the backplane bus is powered correctly (both power supply path) and make sure card has a tight connection with the fieldbus coupler.

Setting Up Media Redundancy using RSTP

4. Start parameterizing the coupler by clicking on the station head indicated by the number 0.



5. Find the parameters “RSTP port 1/2 path cost”

0x1170 Redundancy protocol	RSTP
0x1180 RSTP bridge priority	32768
0x1181 RSTP hello time	2 s
0x1182 RSTP forward delay	15 s
0x1183 RSTP max age	20 s
0x1184 RSTP transmit hold count	6
0x1185 RSTP port 1 priority	128
0x1186 RSTP port 1 path cost	200000
0x1188 RSTP port 2 priority	128
0x1189 RSTP port 2 path cost	200000

Setting Up Media Redundancy using RSTP

- Set the path costs of path one to 220000 make sure it is not identical with the path cost of path 2.

Component list

Coupler: UR20-FBC-MOD-TCP-V2 (Ordering data)

Reset Factory settings Change login Module parameters

0x1106 RSTP port 1 path cost 220000

0x1188 RSTP port 2 priority 128

0x1189 RSTP port 2 path cost 200000

0x114D Modbus transport protocol TCP

0x114E IP address USB port 192.168.1.202

Apply changes Restore



Note:

RSTP always selects the communication path with the lowest accumulated path cost. If multiple paths have the same cost, additional criteria such as the Bridge ID, Port Priority and Port Number are used to determine the forwarding path. To ensure a deterministic network topology, it is recommended to configure the **Path Cost** values so that the preferred communication path is selected unambiguously. This results in predictable network behavior and avoids topology changes caused solely by automatic tie-breaking.

- Apply changes by clicking on “Apply changes”.

Component list

Coupler: UR20-FBC-MOD-TCP-V2 (Ordering data)

Reset Factory settings Change login Module parameters

Diagnoses

Data exchange failed

Parameter

Connected to fieldbus Off

0x1124 IP address 192 . 168 . 20 . 194

0x1126 Subnet mask 255 . 255 . 255 . 0

0x1128 Gateway 0 . 0 . 0 . 0

Apply changes Restore

Setting Up Media Redundancy using RSTP

- To write the changes to the memory of the coupler and make them stay indefinitely click on “Module Parameters”.

The screenshot shows the Weidmüller web interface for a UR20-FBC-MOD-TCP-V2 coupler. The top navigation bar includes the Weidmüller logo, a '+' icon, 'Extras', 'Firmware', 'Logout', and 'Language'. Below this is a secondary navigation bar with 'Overview', 'Station data', 'Force', 'changes require restart', and 'Help'. The main content area is titled 'Coupler: UR20-FBC-MOD-TCP-V2 (Ordering data)'. It features a 'Component list' on the left and a table of parameters on the right. The 'Module parameters' tab is selected and highlighted in yellow.

	Reset	Factory settings	Change login	Module parameters
0x1186 RSTP port 1 path cost				200000
0x1188 RSTP port 2 priority				128
0x1189 RSTP port 2 path cost				200000
0x114D Modbus transport protocol				TCP
0x114E IP address USB port				192.168.1.202
0x114F Webserver via Ethernet				Enabled

- Save the parameters.

The screenshot shows a dialog box titled 'Module parameters'. It contains the following text:

The coupler can store the currently set module parameters, or set them back to default values.

No values are stored currently.

Restore default values restores the default values and deletes possibly stored values.

Save module parameters stores the currently set module parameters and overwrites possibly stored values.

At the bottom, there are three buttons: 'Restore default values', 'Save module parameters' (highlighted in yellow), and 'Cancel'.

Setting Up Media Redundancy using RSTP

10. By restarting the coupler, the parameter changes will be activated.

The screenshot shows the Weidmüller web interface for configuring a coupler. The top navigation bar includes 'Overview', 'Station data', 'Force', 'changes require restart' (highlighted in yellow), and 'Help'. The main content area is titled 'Coupler: UR20-FBC-MOD-TCP-V2 (Ordering data)'. Below this title are four tabs: 'Reset', 'Factory settings', 'Change login', and 'Module parameters'. The 'Module parameters' tab is active, displaying a list of parameters with their current values:

Parameter	Value
0x1186 RSTP port 1 path cost	200000
0x1188 RSTP port 2 priority	128
0x1189 RSTP port 2 path cost	200000
0x114D Modbus transport protocol	TCP
0x114E IP address USB port	192.168.1.202
0x114F Webserver via Ethernet	Enabled

11. Repeat steps for the second fieldbus coupler.

6 Verifying the Redundant Network

After configuring RSTP on the managed switches and the UR20-FBC-MOD-TCP-V2 fieldbus couplers, the redundant Ethernet network must be verified before it is used as the communication infrastructure for controller redundancy.

At this stage, the CODESYS controller redundancy and the Modbus TCP application don't have to be operational yet. Therefore, the verification is performed using the RSTP diagnostic information provided by the managed switches and the management communication between the switches.

6.1 Verify the Initial RSTP State

1. Make sure that all devices are powered and connected according to the network topology shown in Chapter 3.2.
2. Connect the engineering computer to one of the managed switches.
3. Open a web browser and connect to the management IP address of the first and second switch.
4. Log in to the web interface of the switches.
5. Navigate to Redundancy → RSTP → Information:

Industrial Ethernet Switch Configuration
IE-SW-AL05LM-5TX
Weidmüller

www.weidmueller.com

Expand Tree Menu

- System Information
- Front Panel
- Basic Settings
- Port Settings
- Redundancy**
 - O-Ring
 - O-Chain
 - RSTP-Repeater
 - Fast Recovery
 - RSTP**
 - Setting
 - Information**
- VLAN
- DHCP Server/Relay
- SNMP
- Security
- Warnings
- Monitoring/Diagnosis
 - Save Configuration
 - Factory Default
 - System Reboot
 - Logout

Information

Root Bridge Information

Device Status	Root Bridge
Root Bridge ID	1000-00157E1D5534
Root Priority	4096
Root Port	N/A
Root Path Cost	0
Max Age Time	20
Hello Time	2
Forward Delay Time	15

Port Information

Port	Enabled	Port Priority	Path Cost	OperEdge	OperP2P	Role	State
Port 01	Enabled	128	20000	False	True	Designated	Forwarding
Port 02	Enabled	128	20000	False	True	Designated	Forwarding
Port 03	Enabled	128	20000	True	True	Disabled	Discarding
Port 04	Enabled	128	20000	True	True	Designated	Forwarding
Port 05	Enabled	128	20000	True	True	Disabled	Discarding

Front Ethernet Switch

Close

- Verify that the switch with root priority 4096 displays valid **Root Bridge Information**. The other Switch with root priority should display as "Device Status" **Non-Root**.

Root Bridge Information		Root Bridge Information	
Device Status	Root Bridge	Device Status	Non-Root
Root Bridge ID	1000-00157E1D5534	Root Bridge ID	1000-00157E1D5534
Root Priority	4096	Root Priority	4096
Root Port	N/A	Root Port	Port 02
Root Path Cost	0	Root Path Cost	20000
Max Age Time	20	Max Age Time	20
Hello Time	2	Hello Time	2
Forward Delay Time	15	Forward Delay Time	15



Note:

On a **Non-Root switch**, the displayed **Root Priority** refers to the priority of the currently elected **Root Bridge**, not to the locally configured Bridge Priority of the Non-Root switch. Therefore, a value of **4096** is expected when Switch 1 is the Root Bridge and does not indicate a configuration error.

If the current Root Bridge becomes unavailable, RSTP performs a new Root Bridge election. In the reference configuration, the switch with the next-lowest Bridge Priority (**8192**) becomes the new Root Bridge. The Root Priority displayed by the remaining RSTP participants will then change accordingly to **8192**.

- Check the **Root Path Cost** on both switches.



Note:

The Root Bridge should display a Root Path Cost of 0. The Non-Root switch should display a value greater than zero, representing the accumulated cost of its selected path towards the Root Bridge.

- Review the **Port Information** table on both switches.
- Verify that all ports intended to participate in the RSTP topology are **Enabled**.

Port Information							
Port	Enabled	Port Priority	Path Cost	OperEdge	OperP2P	Role	State
Port 01	Enabled	16	10	False	True	Designated	Forwarding
Port 02	Enabled	32	20	False	True	Designated	Forwarding
Port 03	Enabled	64	30	True	True	Disabled	Discarding
Port 04	Enabled	128	40	True	True	Designated	Forwarding
Port 05	Enabled	240	50	True	True	Disabled	Discarding



Note:

Ports that are not connected may be displayed as Disabled and Discarding. This is normal and must not be confused with a connected RSTP port that has been placed in the Discarding state to prevent a loop.

10. Verify the port states.

Verify the **Role** and **State** of the ports participating in the RSTP network.

On the **Root Bridge**, the connected RSTP ports are expected to operate as **Designated / Forwarding** ports.

Port Information

Port	Enabled	Port Priority	Path Cost	OperEdge	OperP2P	Role	State
Port 01	Enabled	128	20000	False	True	Designated	Forwarding
Port 02	Enabled	128	20000	False	True	Designated	Forwarding
Port 03	Enabled	128	20000	True	True	Disabled	Discarding
Port 04	Enabled	128	20000	True	True	Designated	Forwarding
Port 05	Enabled	128	20000	True	True	Disabled	Discarding

On the **Non-Root switch**, one port is expected to operate as **Root / Forwarding**. This port provides the preferred path towards the Root Bridge. The remaining connected ports are typically shown as **Designated / Forwarding**, depending on the resulting RSTP topology.

Port Information

Port	Enabled	Port Priority	Path Cost	OperEdge	OperP2P	Role	State
Port 01	Enabled	128	20000	False	True	Designated	Forwarding
Port 02	Enabled	128	20000	False	True	Root	Forwarding
Port 03	Enabled	128	20000	True	True	Disabled	Discarding
Port 04	Enabled	128	20000	True	True	Designated	Forwarding
Port 05	Enabled	128	20000	True	True	Designated	Forwarding

Depending on the overall RSTP topology, the redundant path is placed in the **Discarding** state on one of the RSTP participants to prevent an Ethernet loop. In the reference topology, this blocking point may be located on one of the fieldbus couplers and is therefore not necessarily visible as a Discarding port on the switches.

Ports that are not physically connected may be displayed as **Disabled / Discarding**. This is normal and must not be confused with an RSTP port that is actively placed in the Discarding state to prevent a network loop.



Note:

In this reference topology, the port placed in the **Discarding** state to prevent the Ethernet loop is located on one of the **UR20-FBC-MOD-TCP-V2 fieldbus couplers**. Consequently, both managed switches display only **Forwarding** states for all connected ports. This behaviour is expected and confirms that the RSTP topology has converged successfully.

6.2 Verify the Redundant Network Paths

To verify the complete redundant Ethernet network, communication should be tested between different network participants while simulating individual cable failures.

The following procedure should be repeated for each communication path listed in Table

1. Connect the engineering computer to one of the managed switches.
2. Establish continuous communication with the selected network participant (for example by using a continuous “*ping <IP> -t*”).
3. Verify that communication is stable before introducing a fault.
4. Disconnect one Ethernet cable participating in the redundant ring.
5. Observe the communication.
6. Verify that communication resumes automatically after the RSTP topology has converged.
7. Reconnect the cable.
8. Verify that communication remains available and that the network returns to a stable topology.
9. Repeat the procedure for the next communication path.

Test	Source	Destination	Cable to disconnect
1	Engineering PC	Switch 2	Switch 1 ↔ Switch 2
2	Engineering PC	Fieldbus Coupler 1	Switch 1 ↔ Switch 2
3	Engineering PC	Fieldbus Coupler 2	Switch 1 ↔ Switch 2
4	Engineering PC	Switch 2	Switch 1 ↔ Fieldbus Coupler 1
5	Engineering PC	Switch 2	Fieldbus Coupler 1 ↔ Fieldbus Coupler 2
6	Engineering PC	Switch 2	Fieldbus Coupler 2 ↔ Switch 2

Expected Result

For every test, the following behaviour is expected:

- Communication may be interrupted briefly while RSTP recalculates the network topology.
- Communication shall resume automatically without manual intervention.
- No device shall become permanently unreachable following the failure of a single cable.
- After reconnecting the cable, the network shall automatically return to a stable RSTP topology.

The RSTP network is considered successfully verified when all network participants remain reachable after each individual cable interruption, communication resumes automatically through the alternative path, and the network returns to a stable topology after the interrupted connection is restored. In addition, the expected topology must be re-established after a complete restart of the RSTP participants.