PROFINET - MRP-Ring: Wichtige Projektierungs-empfehlungen bei Verwendung von RSTP

SIMATIC ET 200, SIMATIC CFU

https://support.industry.siemens.com/cs/ww/de/view/109759619

Siemens Industry Online Support

Dieser Beitrag stammt aus dem Siemens Industry Online Support. Es gelten die dort genannten Nutzungsbedingungen (www.siemens.com/nutzungsbedingungen).

Security-hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts.

Der Kunde ist dafür verantwortlich, unbefugten Zugriff auf seine Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und entsprechende Schutzmaßnahmen (z.B. Nutzung von Firewalls und Netzwerksegmentierung) ergriffen wurden.

Zusätzlich sollten die Empfehlungen von Siemens zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Industrial Security finden Sie unter http://www.siemens.com/industrialsecurity.

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter http://www.siemens.com/industrialsecurity.

Inhaltsverzeichnis

1 PROFINET - MRP-Ring: Wichtige Projektierungsempfehlungen bei Verwendung von RSTP

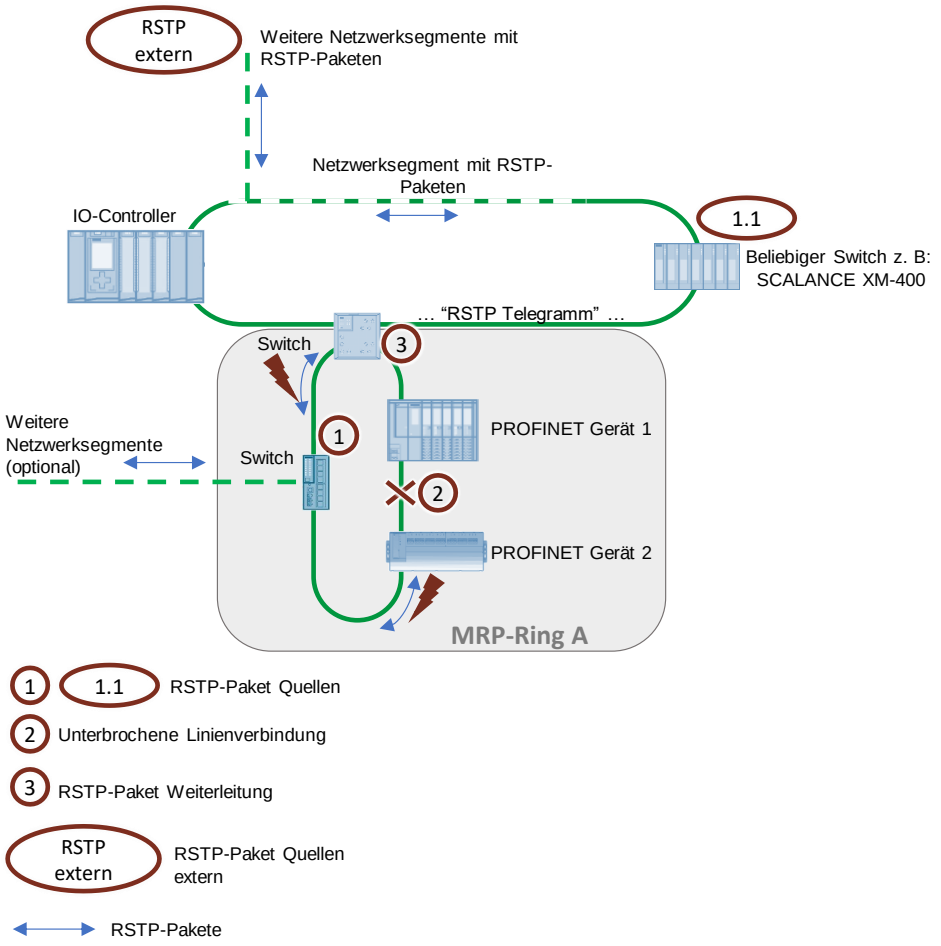
PROFINET bietet als etablierte Feldbus-Kommunikationstechnologie eine Reihe an Vorteilen und Mechanismen wie Erhöhung des Datendurchsatzes, Anlagenverfügbarkeit und Integrität in weitere Datennetzwerke.
Einer der klassischen Ansätze zur Erhöhung der Verfügbarkeit eines PROFINET-Netzwerksegments ist die Anwendung einer MRP-Ring Topologie, die den Ausfall eines einzelnen Gerätes ohne Netzwerkbeeinträchtigung kompensieren kann.

Nach dem derzeit gültigem PROFINET Standard kann es zum unbeabsichtigten Ausfall eines MRP-Ringes kommen, wenn gleichzeitig RSTP-Pakete in den MRP-Ring gelangen.

Folgende Auslöser für eine unerwünschte Beeinflussung eines MRP-Ringes wurden identifiziert:

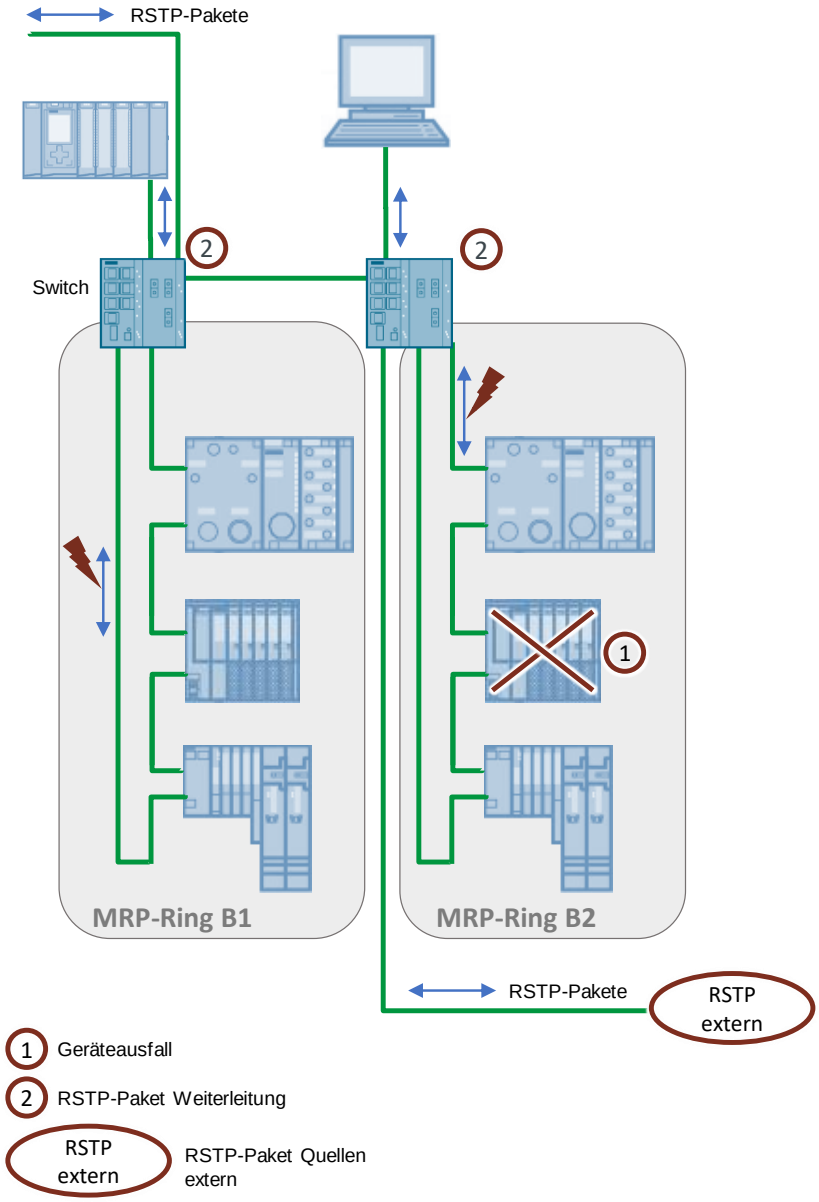
1. Wiederkehr einer unterbrochenen Linienverbindung zwischen zwei benachbarten betroffenen PROFINET-Geräten im Ring (**Abbildung 1-1**)

Abbildung 1-1



2. Wiederkehr oder Anlauf eines betroffenen PROFINET-Gerätes, dessen Nachbarn ebenfalls betroffene PROFINET-Geräte sind. Das kann Folge eines Neuanlaufs, Firmware-Updates, Aus- und Einschaltens oder einer Störung an dem betroffenen Gerät sein (**Abbildung 1-2**).

Abbildung 1-2



Eine ausführliche Liste der betroffenen Geräte und deren Firmware-Versionen finden Sie als Zusatzinformation am Ende des Dokuments.

In diesem Dokument wird erläutert, welche Maßnahmen für eine störungsfreie Funktion zu ergreifen sind, wenn PROFINET Segmente, mit einer MRP-Ring Topologie, mit anderen RSTP-Fähigen Netzwerksegmenten verbunden werden.

Zur Information

RSTP-Pakete werden häufig in Büroumgebungen und IT-Infrastrukturen verwendet, um redundante Pfade in lokalen Netzen zu erkennen und zu deaktivieren. PROFINET leitet die RSTP-Pakete transparent weiter. Eine Abschaltung von RSTP-Diensten muss in Absprache mit den Netzwerkadministratoren erfolgen.

1.1 Verifizierung von PROFINET MRP-Ringen zur Sicherstellung eines störungsfreien Betriebes

Zielsetzung ist es, MRP-Ringe frei von RSTP-Paketen zu betreiben

Bis zur Bereitstellung entsprechender Firmware-Korrekturen zu den betroffenen PROFINET Geräten, kann eine wirksame Robustheitsmaßnahme durch entsprechende Konfiguration der Verbindungsknoten (Bridges) zwischen den jeweiligen Netzwerksegmenten erfolgen.

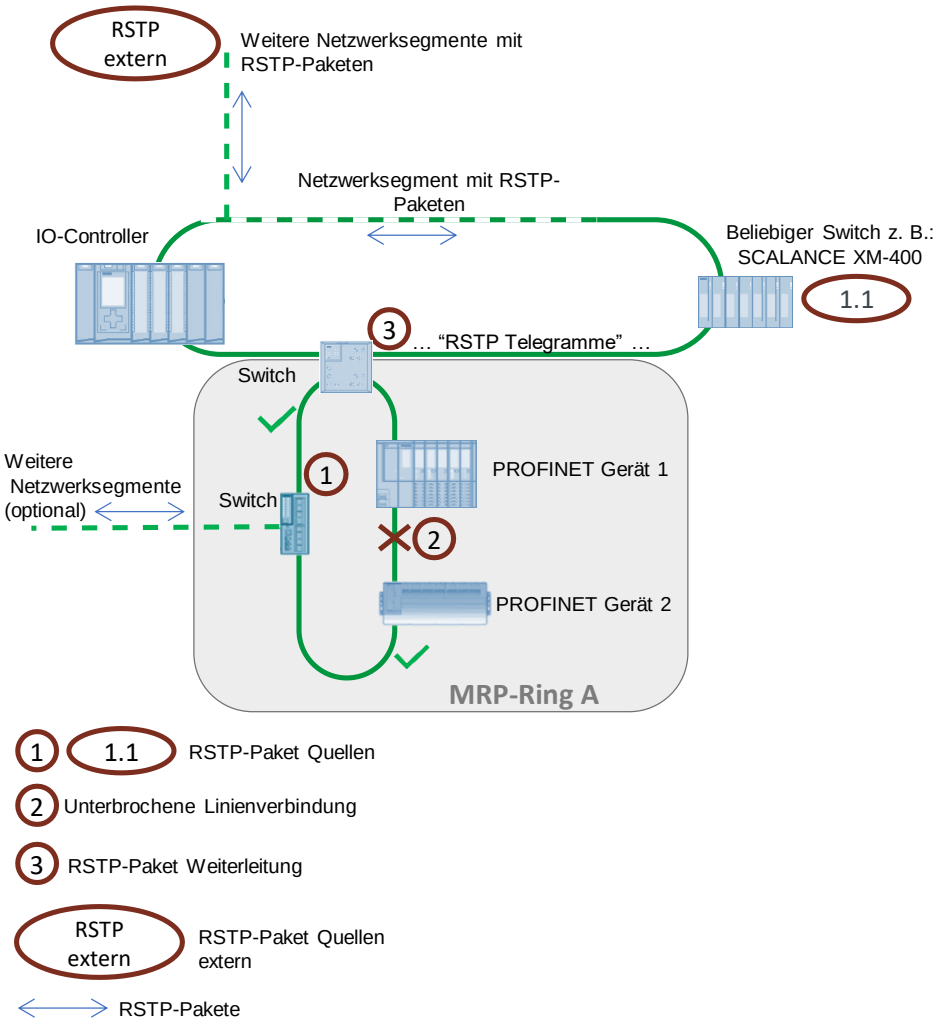
Obwohl die SCALANCE Switches nicht direkt betroffen sind, erfüllen sie jedoch Schlüsselaufgaben im Netzwerk und werden als Lösungsansatz verwendet, wie nachfolgend aufgezeigt.

Es sind grundsätzlich zwei Maßnahmen zu befolgen, je nach Quelle der RSTP-Pakete:

1) RSTP-Pakete werden direkt im MRP-Ring erzeugt

In diesem Fall muss die Quelle der RSTP-Pakete (in der Regel sind es Switches und/oder Bridges) deaktiviert werden:
RSTP-Generierung (Spanning Tree) = „deaktiviert“.
Siehe **Abbildung 1-3** -> Komponenten (1) (1.1) (3)

Abbildung 1-3



Das hier dargestellte Beispiel zeigt die Besonderheit, dass auch nicht im MRP-Ring befindliche aber benachbarte Switches per Standardeinstellung eine RSTP-Paket Quelle sind, ohne dass dies im Netzwerksegment explizit gewünscht ist. Das ist z. B. bei SCALANCE XM-400 (1.1) der Fall.

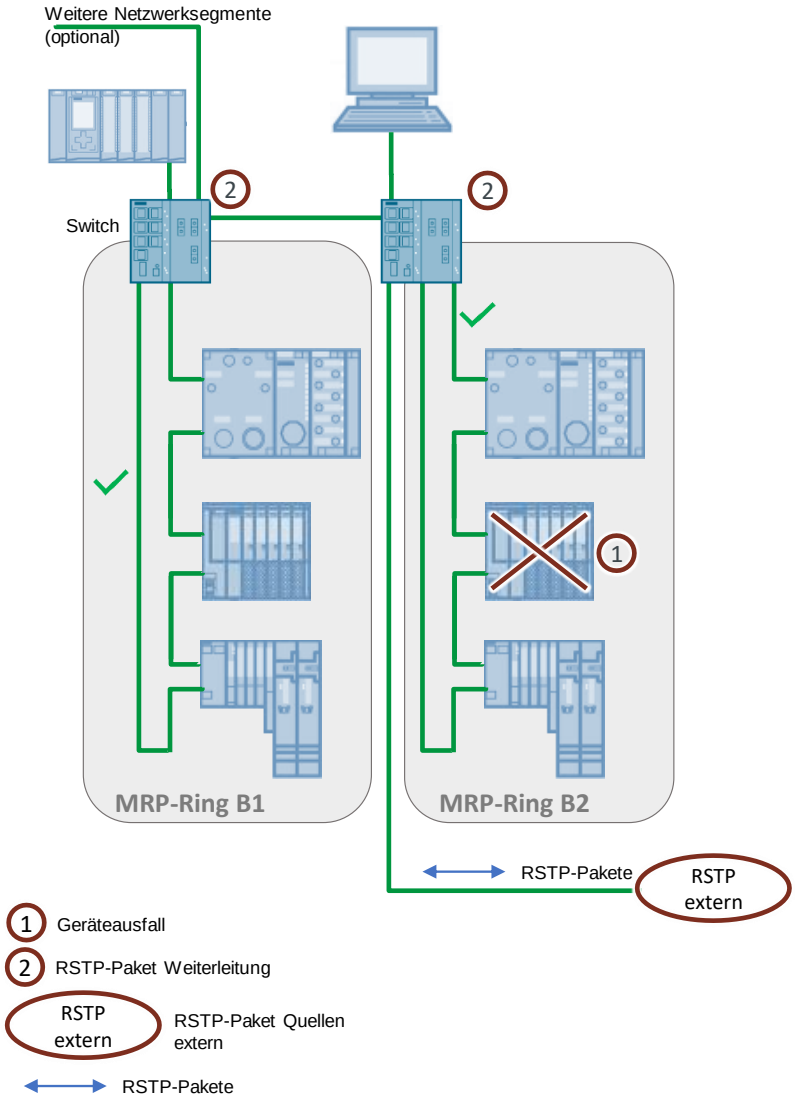
Darüber hinaus sollte auch Maßnahme 2) (siehe unten) für die Komponenten (1) und (3) umgesetzt werden, wenn RSTP-Pakete aus anderen Netzwerksegmenten eingeleitet werden können.

2) RSTP-Pakete gelangen ausschließlich aus benachbarten Netzwerksegmenten in den MRP-Ring

Da in diesem Fall RSTP-Pakete außerhalb des MRP-Ringes erzeugt werden, reicht es diese abzublocken, wodurch sie nicht an den MRP-Ring weitergeleitet werden:
Passive Listening = „deaktiviert".

Siehe **Abbildung 1-4** -> Komponente: (2)

Abbildung 1-4

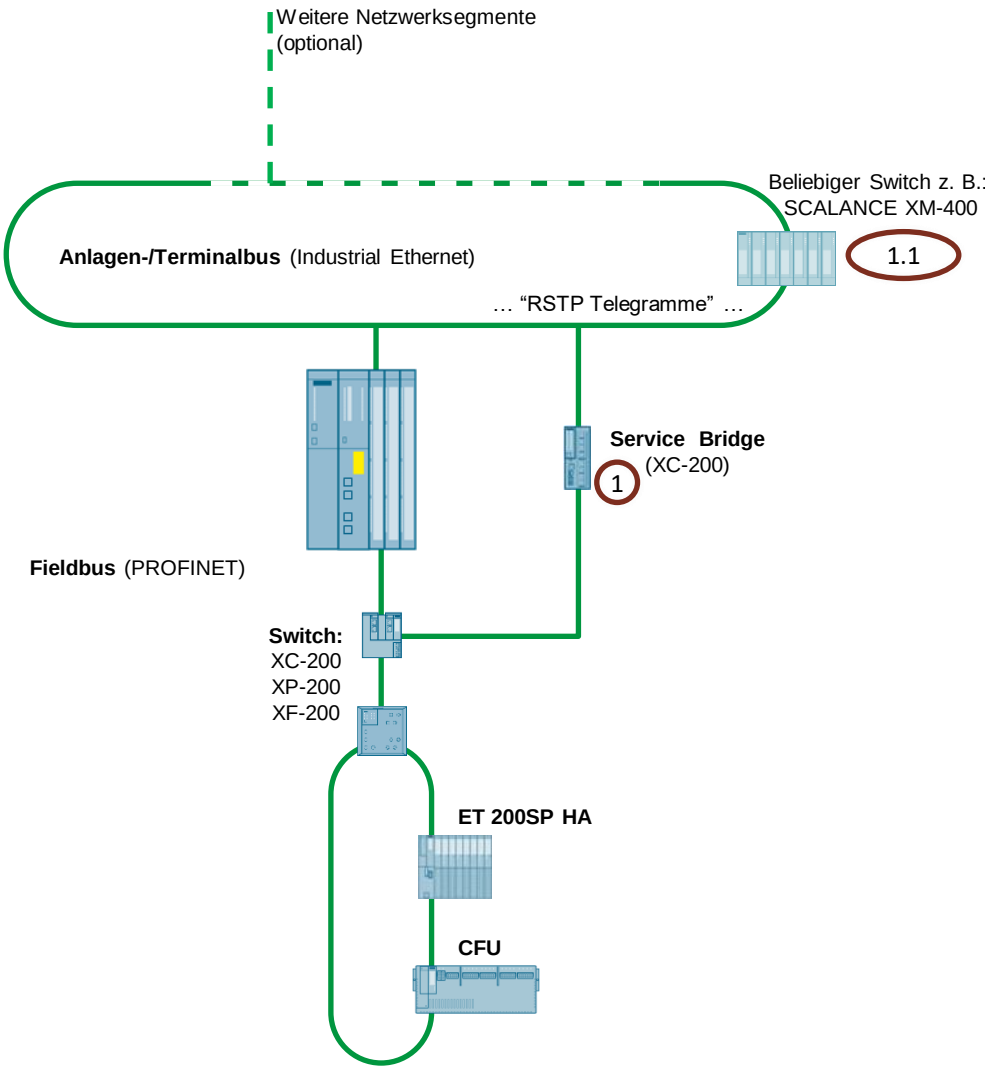


Die hier empfohlenen Einstellungen setzen voraus, dass in den betroffenen MRP Netzwerksegmenten auf RSTP-Frames verzichtet werden kann. Bitte beachten Sie, dass die Einstellung „Passive Listening“ für alle Ports am Switch gilt. Wenn Sie weiterhin Ports mit RSTP Frames benötigen, können Sie z. B. zwei Switches einsetzen und somit die Netzwerkstrukturen entsprechend aufteilen.

Darüber hinaus gibt es Vorschriften, wie Netzwerke aufzubauen sind, die eine Weiterleitung von RSTP-Paketen in einen MRP-Ring verhindern z. B. beim Einsatz einer Service Bridge (SIMATIC PCS 7).

Die in **Abbildung 1-5** dargestellte Netzwerk-Topologie erfordert keine weiteren Maßnahmen, da ein S7-Controller keine Ethernet Kommunikation zwischen seinen Schnittstellen weiterleitet und die Eingesetzte Service Bridge (1) blockiert in der Grundeinstellung alle RSTP-Pakete.

Abbildung 1-5



2 Einstellungen in der Benutzeroberfläche von SCALANCE Switch Produkten (Beispiele)

Abbildung 2-1 RSTP-Generierung („Spanning Tree“) = „deaktiviert“ am Beispiel der SCALANCE XC200 Serie

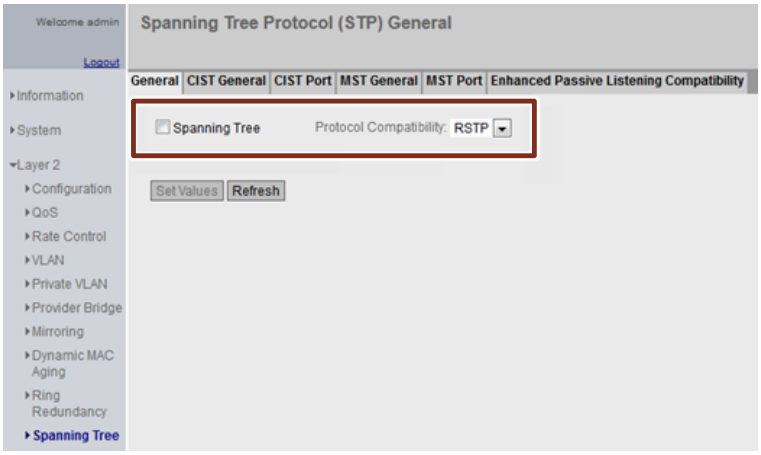
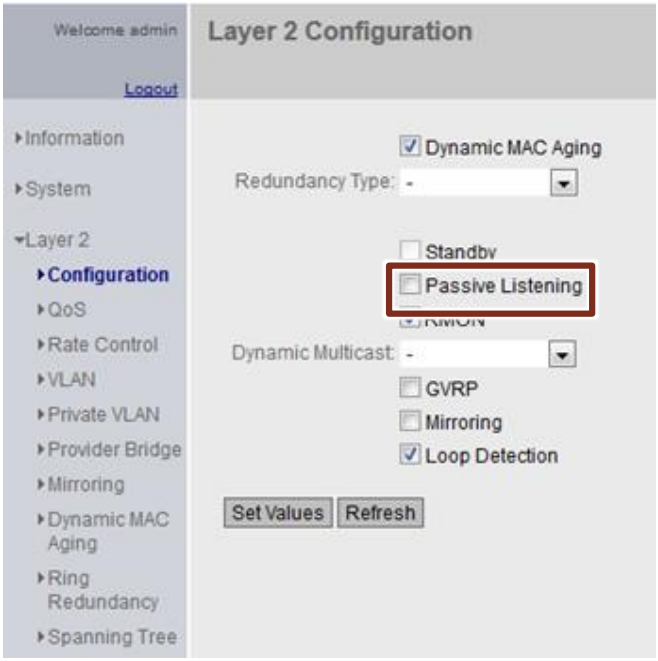


Abbildung 2-2 „Passive Listening“ = „deaktiviert“, am Beispiel der SCALANCE XC200 Serie



Es ist ausdrücklich darauf zu achten, dass im Ersatzfall zu tauschende SCALANCE Geräte eine entsprechende Parametrierung besitzen, bevor diese im Netzwerk eingesetzt werden (z. B. unter Verwendung von C-Plug Wechselmedien)

Hinweis Bei Verwendung von Geräten anderer Hersteller mit vergleichbarem Funktionsumfang wenden Sie sich bitte an die Ihnen dafür genannten Ansprechpartner bzw. Support-Kanäle, um eine entsprechende Unterstützung zu erhalten.

3 Verwendete Begriffe

RSTP

Rapid Spanning Tree Protocol. Es ist eine Weiterentwicklung des Spanning Tree Protocol (STP).

RSTP-Generierung („Spanning Tree“)

Generierung von RSTP-Paketen, um redundante Pfade in lokalen Netzen zu deaktivieren, bzw. im Bedarfsfall (Ausfall einer Verbindung) wieder zu aktivieren. (Dieses Verfahren ist in Büroumgebungen häufig im Einsatz).

Passive Listening

Weiterleiten von RSTP-Paketen.

4 Liste der betroffenen Produkte und geplante Firmware (FW) Korrektur-versionen

4.1 SIMATIC CFU

Tabelle 4-1

Artikelnummer	Produktbezeichnung	geplante Korrekturversion
6ES7655-5PX11-0XX0	SIMATIC CFU PA	mit kommender FW-Version V1.1.1 behoben
6ES7655-5PX11-1XX0	SIMATIC CFU PA Bundle	mit kommender FW-Version V1.1.1 behoben
6ES7655-5PX11-1AX0	SIMATIC CFU PA Bundle Alu	mit kommender FW-Version V1.1.1 behoben

4.2 Interfacemodule

ET 200SP

Tabelle 4-2

Artikelnummer	Produktbezeichnung	geplante FW-Korrekturversion
6ES7155-6AU00-0CN0	IM 155-6 PN HF	mit kommender FW-Version V4.2 behoben
6ES7155-6AU00-0DN0	IM 155-6 PN HS	mit kommender FW-Version V4.0.1 behoben

ET 200SP HA

Tabelle 4-3

Artikelnummer	Produktbezeichnung	geplante Korrekturversion
6DL1155-6AU00-0PM0	IM 155-6 PN	mit kommender FW-Version V1.1 behoben

ET 200MP

Tabelle 4-4

Artikelnummer	Produktbezeichnung	geplante Korrekturversion
6ES7155-5AA00-0AC0	IM 155-5 PN HF	mit kommender FW-Version V4.2 behoben

ET 200AL

Tabelle 4-5

Artikelnummer	Produktbezeichnung	geplante Korrekturversion
6ES7157-1AB00-0AB0	IM 157-1 PN	FW-Version in Planung

4.3 Netzübergänge

PN / PN Koppler

Tabelle 4-6

Artikelnummer	Produktbezeichnung	geplante Korrekturversion
6ES7158-3AD10-0XA0	PN / PN Koppler	mit kommender FW-Version V4.2 behoben

4.4 Development Kits

Evaluation Kit ERTEC 200P

Tabelle 4-7

Artikelnummer	Produktbezeichnung	geplante Korrekturversion
6ES7195-3BE00-0YA0	Evaluation Kit ERTEC 200P	mit kommender FW-Version V4.6 behoben

5 Netzwerk-Diagnose Produkte

BANY (Bus Analyzer)

Tabelle 5-1

Artikelnummer	Produktbezeichnung
9AE4140-1BA00	BANY Agent ohne TAP
9AE4140-1BA01	BANY Agent mit TAP
9AE4140-2AA00	Bus Analyzer Agent XM-400

TAP (Test Access Port)

Tabelle 5-2

Artikelnummer	Produktbezeichnung
6GK5104-0BA00-1SA2	SCALANCE TAP104

6 Support und weitere Quellen

Weitere Informationen zu PROFINET MRP-Ring:
https://support.industry.siemens.com/cs/ww/de/view/109739614

Service Bridge Config-file:
https://support.industry.siemens.com/cs/ww/de/view/109747975