1756-EN2TP Parallel Redundancy Protocol Module
Network Redundancy
The 1756-EN2TP Parallel Redundancy Protocol Module offers PRP support for a redundant network infrastructure for high availability to help minimize unplanned downtime.
1. **What is PRP?**
   - PRP, Parallel Redundancy Protocol, is described in IEC standard 62439-3. It is a means to achieve fault tolerant Ethernet by having redundant LANs where the same packet is sent on both LANs and the end device is responsible for detecting and eliminating one of the packets. PRP is a separate and different protocol than either DLR or EtherChannel.

2. **What are some typical applications for PRP?**
   - PRP is typically applied where redundant network infrastructure is desired
   - Process applications
   - ControlNet redundant media migration opportunities, such as transportation tunnels are good applications for PRP
1756-EN2TP Parallel Redundancy Protocol Module
Features and Benefits

- Provides a redundant network infrastructure for high availability, helping minimize the risk of downtime
- IEC 62439-3 compliant
  - Same packets sent out of both ports to eliminate network switchover time
- PRP is a different protocol than DLR
- Acts as I/O scanner in controller chassis or I/O adapter in remote chassis
- Supports HMI communications
- Provides same performance and capacity as 1756-EN2TR
PRP General FAQs

3. How does PRP compare to redundancy schemes such as RSTP or MRP?
   - Rapid Spanning Tree Protocol (RSTP) can be implemented in arbitrary mesh topologies, where the active topology is established by blocking bridge ports. It typically takes a few seconds to reconfigure the tree in case of failure.
   - Media Redundancy Protocol (MRP) is a ring topology. One of the ring ports is blocked to establish the active topology. It typically takes 100 ms to reconfigure the ring in case of failure.
   - PRP does not change the active topology. It operates on two independent networks where each frame is replicated. Therefore, there is no period of unavailability.
1756-EN2TP Parallel Redundancy Protocol Module

Applications

- Process
- Applications where a customer that require redundant network infrastructure
- ControlNet media redundancy migrations
- For customers that require redundancy beyond a ring topology
Building a PRP Network
Starting with a Basic Star Topology

* For example only - number of switches and topology varies based on application
Building a PRP Network
Adding Redundant Media and ControlLogix PRP Modules

- Redundant Ethernet Networks
  - Independent LANs
  - Independent Paths

- Switches are not PRP aware

- Redundancy is in the end nodes, called, “Doubly Attached Nodes (DANs)” attach to both LANs

- The DANs in this example are all 1756-EN2TP PRP modules

- Any switch that supports 1506 frames can be used
Building a PRP Network
Sending Frames on both LANs

- Source DAN sends same frame over both LANs
- Destination DAN consumes the frame the first time it is received, then discards the duplicate when received
- DAN has 1 MAC, 1 IP address
- Frames have LAN ID
Building a PRP Network
Adding RedBox Devices

- RedBox: a device that attaches non-PRP devices to a redundant network
- Devices attached through a Redbox are called, “Virtual Doubly Attached Nodes (VDANs)”
- The RedBox shown is a standard Stratix 5400 switch with built-in RedBox functionality
Building a PRP Network
Adding a Singly Attached Node

- Non-PRP devices can be connected to only one of the two LANs, however, media redundancy is lost
- Singly Attached Nodes (SANs) can communicate only to other devices on the LAN that they are connected to
- SANs are not PRP-aware
A ControlLogix Redundancy kit including the 1756-EN2TP will not be available at the same time as the 1756-EN2TP release.
PRP General FAQs

What are all the PRP products that Rockwell Automation currently offers and what are the limitations?

- The 1756-EN2TP is currently available
- The current Stratix® 5400 includes RedBox functionality
- PRP support in FLEX 5000™ I/O is planned
- Other products in the future will support PRP
- A limitation is that, as of Aug 2017, there is not a ControlLogix® Controller Redundancy firmware kit that includes the 1756-EN2TP. This is forthcoming.
How does a PRP network connect from the controls network (OT) up to the corporate network (IT)?
- The PRP network at the controls level (OT) is connected to the corporate network (IT) level through a RedBox.

Do the network infrastructure switches (as opposed to the RedBoxes) need to have PRP protocol built in?...
- No. Any switch that supports the baby jumbo frame size of 1506 bytes will work in a PRP network. The PRP protocol needs to be built into the end devices where the two LANs connect (DANs or Redboxes). Rockwell Automation recommends the use of Stratix managed switches because of their diagnostics, which allow for quicker troubleshooting and repair of switches between the talking and listening nodes. If the switch is not capable of participating in the diagnostics of the network, troubleshooting and repair can take longer.
PRP General FAQs

Can any switch be used as a RedBox?
- Only switches specifically designed with Redbox functionality can function as a RedBox.

Can I use an ETAP as a RedBox?
- At this time, ETAPs do not have PRP built in. An ETAP is used to put non-DLR devices onto a DLR ring.

Is it possible to add a non-PRP device to just one of the two LANs?
- Yes, however only devices on the LAN that that device is attached to will be able to communicate with it. These are the SANs mentioned earlier.

Can I mix PRP devices from other vendors on the same network?
- PRP is a standard protocol based on IEC-62439-3 but each vendor can implement it as they wish so Rockwell Automation cannot make any guarantees that mixing different vendor devices will work.
PRP General FAQs

What are the required features for the infrastructure switches that are part of the LANs?
- The switch needs to be able to support baby jumbo size of 1506 bytes, to accommodate a full size frame plus the PRP trailer.

What is the network healing time for a single fault on a PRP network?
- Zero. A transmitting DAN duplicates the packet and sends it out on both LANs at the same time. The receiving DAN gets both packets and simply discards the duplicate. There is no concept of a healing time since there is no switchover from one LAN to the other. The module evaluates incoming traffic on a packet by packet basis, always using the first of two packets received.

How many IP addresses and MAC IDs does a PRP device have?
- One IP address, one MAC ID
PRP General FAQs

When there is distance between nodes, should the two LANs be routed separately from each other?
- Yes, for best resiliency, route the two LANs in physically different paths.

Can I connect LAN A and LAN B together to provide additional paths?
- No, doing so will cause PRP to fail. The two LANs connect only at a DAN or a RedBox.
Can any device be a SAN?
- Any device can work as a SAN, however the benefits of redundancy are lost when a device is not connected to both LANs.
- It may be desirable to have redundant cabling but not a redundant switch.

Can both LANs be physically connected to a single infrastructure switch using VLANs in that infrastructure switch? That way the network could still take advantage of redundant cabling?
- No, both LANs need to be on the same VLAN in PRP.
- VLANs can be implemented in a PRP network where each VLAN exists on each LAN.
PRP General FAQs

* How do you troubleshoot and debug a PRP system?
  - Look at the Network page in Module Properties of the 1756-EN2TP in Logix Designer
    - This page shows diagnostics for the node
    - This page lists the nodes on the network and whether they are DAN, SAN, RedBox or VDAN
  - Look at the web page of the 1756-EN2TP
    - The PRP Statistics tab shows status of each PRP port along with useful counters
    - The Nodes tab shows the other nodes on the network and whether they are DAN, SAN, RedBox or VDAN

* Are both LAN A and LAN B on the same subnet?
  - Yes. LAN A and LAN B are physically separate, however they are the same logical LAN. It is only the PRP trailer that distinguishes the LAN A packets from the LAN B packets.
1756-EN2TP FAQs

* What version of RSLinx® Enterprise was tested?
  - 5.90 and later

* What’s the best way to get diagnostics concerning the networks?
  - The Network page in Module Properties, the web page

* Can the 1756-EN2TP be configured for DLR?
  - No, it is a PRP-only module. Use the 1756-EN2TR for DLR.

* Does the 1756-EN2TP support ControlLogix Redundancy?
  - There will be a V31.050 firmware kit for ControlLogix Redundancy 5570 controllers, target release date is July 2018 (as of Oct. 2017)

* The 1756-EN2TP represents a single point of failure. Can a pair of 1756-EN2TPs be used as redundant adapters?
  - No. This functionality will be in a future module.
**Stratix 5400 RedBox FAQs**

* On the Stratix 5400 RedBox, on the VDAN side, can DLR rings be implemented?
  - Yes, all three rings can be implemented, no DLR rings are lost when Redbox functionality is employed.

![Diagram of Stratix 5400 RedBox](image-url)
Device Level Ring
Network Redundancy
A DLR network is a single-fault tolerant ring network intended for the interconnection of automation devices:

Advantages include:
- Simple installation
- Fast recovery time
Stratix 5700 Managed Switch Differentiators

- Includes integrated DLR connectivity enabling the switch to act as a node or a supervisor on the ring.
- Offers consolidation of ring information for a single point of management for retrieving network machine-level diagnostics and DLR status (in supervisor mode).
- Provides redundant gateway capability providing support for two switches on a single ring connected together on the network for increased resiliency.
- Enables DHCP IP address assignment to end devices on the DLR network for simplified device replacement.
FactoryTalk Network Manager Software

November 2017

PUBLIC
Why Network Management Software?

- Networks are critical to automation assets
  - Control, I/O, drives, HMI, etc.
- Plants will experience significant network growth over the next several years
- Plant floor staff tasked with network operations and maintenance
  - Increase visibility of automation assets on the network
  - Network health and monitoring in context of the plant floor assets
  - Simplify the troubleshooting process, quickly identify network root causes issues
  - More easily deploy, commission and maintain networks

Plant floor staff need an easy-to-use, intuitive tool not targeted at IT experts
FactoryTalk® Network Manager software helps give you increased network visibility, real-time troubleshooting and simplified configuration and deployment. Get insight into the performance of your network operations by getting a closer look into your devices connected on the plant floor.
FactoryTalk Network Manager Software
Features and Benefits

- Discovery of plant floor assets
- Overall Topology and Device Centric View
- CIP and PROFINET protocols

Name 131.200.174.141
IP Address 131.200.174.141
Product ID Industrial Managed Switch
Inventory View

- Auto Discovery
  - EtherNet/IP
  - CIP/PROFINET
- Routers/switches
- End devices
- Search
- Link to end device
- Export list
**End Device View**

**End Device**
- Device Overview
- Additional Details

**Chassis Layout**
- Slot
- Name, Description
- Serial #
- Major, Minor Version

### End Device Overview

**Name**: 131.200.174.135

**IP Address**: 131.200.174.135

**MAC Address**: 00:00:bc:33:7f:15

**Vendor**: Rockwell Automation/Allen-Bradley

<table>
<thead>
<tr>
<th>Slot</th>
<th>Vendor ID</th>
<th>Product Type</th>
<th>Device Profile</th>
<th>Product Code</th>
<th>Revision</th>
<th>Status</th>
<th>Serial Number</th>
<th>Product Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0x1</td>
<td>0xE</td>
<td>Programmable Logic Controller</td>
<td>0x06</td>
<td>16.056</td>
<td>0x3170</td>
<td>3014102</td>
<td>1756-L61/A LOGIX5561</td>
<td>131.200.174.135</td>
</tr>
<tr>
<td>1</td>
<td>0x1</td>
<td>0xC</td>
<td>Communications Adapter</td>
<td>0x03A</td>
<td>5.001</td>
<td>0x650</td>
<td>3787955</td>
<td>1756-ENB³/A</td>
<td>131.200.174.135</td>
</tr>
</tbody>
</table>

---

**Network Visibility**

**Troubleshooting**

**Configuration and Deployment**
Managed Switch View

**ADDITONAL INFO**
- End Devices
- Interfaces
- MAC / VLAN
- Events

**DEVICE PHYSICAL VIEW**
- Used Ports
- LED Status

**DEVICE MANAGER**
- Device Webpage Shortcut

**OVERALL STATUS**
- Alarms
- Health
- Bandwidth
- Recent Activities (Audits)

**Network Visibility**

**Troubleshooting**

**Configuration and Deployment**
Group Dashboard

- Alarms
- Assets
- Traffic Utilization
- Port Counts
# Alarm Overview

## Filter Alarms
- Severity
- Active (New) or Closed
- Type
- Etc.

## Alarm View
- Severity, Time, Device, Message, etc.
- Affected Devices
- Assign to a user to resolve
- Stored in a database: Manage Retention Period

---

**PUBLIC**

Copyright © 2017 Rockwell Automation, Inc. All Rights Reserved. 33
Alarm Details

ALARM DETAILS
- Shows Affected Connected End Devices
- Alarm Notes (User Entered)
- Alarm Events
- Alarm History

Network Visibility  Troubleshooting  Configuration and Deployment
Software Audits

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Operation</th>
<th>Device IP Address</th>
<th>Status</th>
<th>Username</th>
<th>User IP Address</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-10-06 10:10:13</td>
<td>Login</td>
<td></td>
<td>Success</td>
<td>systemadmin</td>
<td>172.28.19.101</td>
<td>Updated device admin state from Unlicensed to License...</td>
</tr>
<tr>
<td>2017-10-06 10:09:53</td>
<td>Changed Device State</td>
<td>192.168.1.101</td>
<td>Success</td>
<td>SystemAdmin</td>
<td>10.90.93.35</td>
<td>Started device state change task with ID 7275</td>
</tr>
<tr>
<td>2017-10-06 10:09:37</td>
<td>Started Device State</td>
<td></td>
<td></td>
<td></td>
<td>10.90.93.35</td>
<td>User systemadmin entered incorrect password</td>
</tr>
<tr>
<td>2017-10-06 10:05:31</td>
<td>Login</td>
<td></td>
<td>Success</td>
<td>SystemAdmin</td>
<td>172.28.19.101</td>
<td>User systemadmin entered incorrect password</td>
</tr>
</tbody>
</table>

**AUDIT DETAILS**
- Network Management Software
- Time, User, Action, etc.
- Apply Filters
- Ability to Export to CSV file
Security

Three Default Roles
- Network Admin
- System Admin
- Operator

New User Rights
- Alarm Management
- Device Management
- Network Settings
- Role Based Access Control
- System Settings
- View Only

Troubleshooting

Configuration and Deployment
FactoryTalk Network Manager Software
Features and Benefits

- Discovery of plant floor assets
- Overall Topology and Device Centric View
- CIP and PROFINET protocols

- Real-time capture of Alarms and Events
- Historical retention for analysis
- Audit Trail

- Plug-n-Play
- Configuration Template

Network Visibility
Troubleshooting
Configuration and Deployment
Configuration and Deployment

Plug-n-Play (PnP)
• Upload existing configuration and apply variable substitution, attach it to a PnP profile
• Match PnP Profile (IP/Range, serial number, etc.)
• Dashboard, PnP status and metrics

Configuration Templates
• Push configuration to device based on template
Network Switch Product Overview

**Access**

- **Stratix 2000**
  - 5-16 ports
  - Fiber port options
  - Gig port option
  - Plug & play

- **Stratix 2500**
  - 5-port model
  - 8-port model
  - Basic
  - Traffic management
  - Diagnostics
  - Security
  - Layer 2 firmware
  - IP30 and IP67 On-Machine™ platform
  - Integrated DLR
  - Integrated NAT
  - IEEE1588 PTP
  - PoE/PoE+

- **Stratix 6000**
  - 5–9 port
  - Lightly managed
  - Gig Fiber option

- **Stratix 5700/ArmorStratix™ 5700**
  - Layer 2 firmware
  - 6–20 ports
  - IP30 and IP67 On-Machine™ platform
  - Integrated DLR
  - Integrated NAT
  - IEEE1588 PTP
  - PoE/PoE+

- **Stratix 8000/8300**
  - Layer 2 or Layer 3 routing firmware
  - 6–26 ports
  - Modular platform for maximum flexibility
  - IEEE1588 PTP
  - Integrated NAT
  - Up to 8 PoE/PoE+ ports

**Unmanaged / Lightly Managed**

- **Stratix 2500**
  - 5-port model
  - 8-port model
  - Basic
  - Traffic management
  - Diagnostics
  - Security

- **Stratix 6000**
  - 5–9 port
  - Lightly managed
  - Gig Fiber option

**Distribution**

- **Stratix 5410**
  - 19 in Rack Mount
  - Layer 2 or Layer 3 routing firmware
  - 28 ports
  - All gig ports plus four 10 gig ports
  - IEEE1588 PTP
  - Up to 8 separate integrated NAT ports
  - Up to 12 PoE/PoE+ ports
  - PRP (RedBox)
  - DC and AC power input options
Stratix 5950 Security Appliance
The Stratix® 5950 Security Appliance brings an industrially-hardened security product to the networks and security infrastructure portfolio of products. The Stratix® 5950 Security Appliance helps provide increased visibility and control with Deep Packet Inspection (DPI) capabilities to help protect your assets down to the machine level.
Stratix 5950 Security Appliance Differentiators

- Maintain your protection against threats and control your assets with subscription based licensing.
- DIN rail mount offers increased design flexibility.
- Deep Packet Inspection technology provides the visibility and controls needed for implementing policies around access, applications and protocols on the plant floor.
- Cisco ASA firewall and FirePOWER technology provide prevention services to identify, log or block potentially malicious traffic.
- Industrialy-hardened for high temperature demands (-40°C to 60°C).
- SFP slots enable flexibility by allowing multiple options for fiber connectivity.
The Stratix® 5950 is ideal for resolution of the following challenges:

**Lacking visibility and control** to help prevent erroneous activity and to maintain integrity of operations on the plant floor.

For example, prevention of tampered with firmware being downloaded to a Controller by confirming only an authorized user can conduct the download.

**Threat control** for vulnerable Industrial Control Systems (ICS) devices, and/or legacy equipment.

Protection against communications from ICS components at risk of compromise.

**Intrusion Prevention** capability and detailed network visibility which enhances traditional firewall functionality to allow for informed decision making through the use of Deep Packet Inspection technology.

Allows for vulnerability identification and mitigation through configuration of policies to block actions, like CIP Reads, Writes, Download to provide protections for communications with ICS devices like HMI, etc.

*Stratix® 5950 addresses the challenge for Industrial Automation professionals to maintain operations integrity while making data more available from the ICS.*
Firewalls and Deep Packet Inspection

- Typical IT firewalls are capable of inspecting
  - Source or Destination MAC or IP Address
  - Source or Destination TCP or UDP Ports, or
  - Protocol elements of a packet

- Deep Packet Inspection extends upon these firewalls’ capabilities
  - Provides granular protection per protocol (ex. CIP, Modbus, DNP3) in the Industrial Zone
  - Giving the visibility and control to help prevent erroneous or malicious activity down to the Cell / Area zone level

- Intrusion Prevention uses DPI
  - What you want to do after you have inspected the packet?
    1.) After inspecting the packet using DPI, achieve granular control through security rules that act on matched network traffic
    2.) Do we allow this application or command, or is this a known threat?
IPS – IDS – Firewall Comparison

**IPS**
- Inspects traffic flowing through a network and is capable of blocking what it determines to be malicious.

**IDS**
- Similar to IPS but does not affect traffic flows in any way; only logs or alerts on malicious traffic.

**Firewall**
- Helps prevent or allow traffic between interfaces based on policies.
  - Often use network address translation (NAT) to isolate private network addresses from public ones.
  - May inspect traffic for conformance with proper protocol behavior.
Stratix 5950 Subscription License

Term-based Live Threat and Application Control Security Services

**Threat Mitigation**
Threats are mapped to **DPI Patterns and Sequences**

**Operation Control**
Operations are mapped to **DPI Patterns and Sequences**

**Application Control**
Applications are identified using underlying Protocol and App-level Info.

**Network-Level Filtering**
Endpoints are passively identified and filtered using IP and MAC addresses.

---

**Zero-Day Protection**
Term Based Service for Threat and Application Control Updates
In Transparent Mode:
The security device acts as a barrier device between Cell/Area Zones to allow segmentation of control systems to enable the implementation of an ISA99/IEC62443-compliant network architecture.
Stratix 5950 within a CPwE Architecture

For Centralized Management (as an alternative to an on-box management interface for each Stratix 5950):
- FireSIGHT™ Management Center
- Cisco Security Center
Deep Packet Inspection
Cell/Area Zone Firewall – Policy Enforcement (example)

Industrial Zone

Cell/Area Zone

SNMP Sweep
Ping Sweep

CIP Class 3
CIP Class 3
CIP Class 3
CIP Class 3

http
icmp - ping

Zone Firewall

CIP Class 3
CIP Class 1

icmp - ping