

Service Description

CXD Unified Services Port

Last Updated: February 12, 2019

© 2019, Cyxtera Data Centers, Inc., a subsidiary of Cyxtera Technologies, Inc. All rights reserved. Cyxtera® and Cyxtera Technologies® are the registered trademarks of Cyxtera Technologies, Inc. All other marks and names mentioned herein may be trademarks of Cyxtera or another company.

The products described herein may be Cyxtera’s or another company’s intellectual property and protected by one or more U.S. or international copyright or intellectual property laws.

The terms set forth in this Service Description (“Service Description”) apply to colocation services provided by Cyxtera to customer from time to time (the “Services”). With respect to a Service, “Cyxtera,” “we,” or “us” means (1) if customer has entered into a service order, statement of work or other signed agreement (the “Order”) with respect to such Service, the applicable affiliate or subsidiary of Cyxtera Data Centers, Inc. that is a party to such Order, or (2) if customer has not entered into an Order with respect to such Service, the applicable affiliate or subsidiary of Cyxtera Data Centers, Inc. set forth in the table below.

<u>Location of Data Center at which the Service is to be Provided</u>	<u>Affiliate or Subsidiary</u>
United States or Any Other Country Not Listed in this Table	Cyxtera Communications, LLC
Canada	Cyxtera Communications Canada, Inc.
United Kingdom	Cyxtera Technology UK Limited
Japan	Cyxtera Japan, Ltd.
Singapore	Cyxtera Singapore Pte. Ltd.
Hong Kong or China	Cyxtera – Colocation Entity Limited
Germany	Cyxtera Germany GmbH
Australia	Cyxtera Australia Pty. Ltd.

No part of this document may be reproduced, transmitted, distributed, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical or otherwise, without the prior written consent of Cyxtera.

This Service Description constitutes proprietary, confidential information of Cyxtera, and may not be disclosed or used except as may be provided in the terms and conditions of the service agreement pursuant to which you have been authorized to use the Services or to review this document.

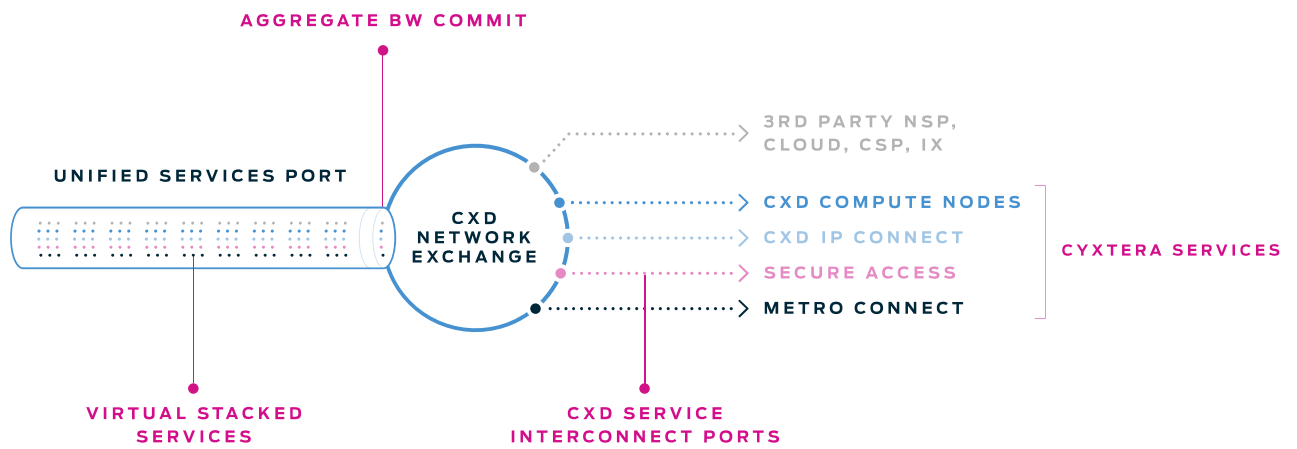
Cyxtera Data Centers, Inc.
2333 Ponce De Leon Blvd., Suite 900
Coral Gables, Florida 33134
www.cyxtera.com

Contents

1. INTRODUCTION	4
1.1 PORTAL, TOOLS, & APIS	5
1.2 CONNECTIVITY	5
2. OPERATIONS	5
2.1 SUPPORT	5
2.2 PROVISIONING	6
2.3 MONITORING	6
2.4 INCIDENT AND PROBLEM MANAGEMENT	6
2.5 CHANGE MANAGEMENT	6
2.6 SECURITY	7
3. CONFIGURATION OPTIONS	8
3.1 LAYER 3 CE	8
3.2 LAYER 2 CE	8
3.3 LAYER 2 CE WITH LAG	9
4. BUSINESS OPERATIONS	11
4.1 ORDERING	11

1. Introduction

The Cyxtera Extensible Data Center platform utilizes an intelligent software-defined network to deliver all Cyxtera data center services to colocation environments over a CXD Unified Services Port. Through this single resilient dual-path (primary & fail-over) network connection you can establish secure logical layer 2 connections to all Cyxtera network and data center services from your colocation cabinet or cage. This includes connections to select ecosystem providers who have integrated their provisioning system with CXD. The Unified Services Port provides access to [CXD IP Connect](#), [CXD Compute Nodes](#), and [CXD Metro Connect Switched](#), among other services.



CXD Unified Services Port includes:

- Cross-connect from Ecosystem Connect Bundle to CXD platform
- Seamless extension of customer colocation cabinet or cage
- Connectivity via layer 2 network throughout the data center over the CXD platform
- Access to CXD enabled network providers with direct connections to private or public cloud

CXD utilizes a state-of-the-art software-defined network fabric to link customers and resources throughout the data center. This secure, high availability architecture assures each customer's traffic is logically isolated and protected through the use of VXLAN protocol. Private virtual Layer 2 networks can be defined, provisioned, and configured through the CXD APIs or CXD Command Center web console.

All CXD powered services are delivered over a Unified Services Port. Customers may elect to utilize the full port for a single service or stack multiple services.

Key Terms

- **Provider Edge (PE):** A Provider Edge device is Cyxtera owned physical equipment that connects to any collocated Customer Edge Device.
- **Customer Edge:** A Customer Edge device is any collocated customer owned physical equipment that connects to any Cyxtera Provider Edge Device.
- **Link Aggregation Control Protocol (LAG):** Link Aggregation Control Protocol is the IEEE 802.1ad standard that defines control over the use of Link Aggregation Groups.

1.1 Portal, Tools, & APIs

Self-Service Administrative Tools

The Service includes access to three self-service tools:

- **Cyxtera Customer Portal** provides access to subscription status, integrating navigation, viewing, and management of all Cyxtera products, entitlements, and customer support under a single account.
- **CXD Command Center** is the primary tool for access, consumption, and management of CXD Unified Services Port and CXD enabled products purchased from Cyxtera, including CXD Compute Node, CXD IP Connect, CXD Metro Connect Switched and management and configuration of networks.

Cyxtera will provide users with access to Application Programming Interfaces (API) for programmatic resource management.

- **Cyxtera APIs** allow you to create scripts that run system administration commands against CXD Unified Services Port and your CXD resources, such as CXD Compute Nodes, CXD IP Connect, CXD Metro Connect Switched and networks, equivalent to those actions that can be taken from the CXD Command Center.

1.2 Connectivity

Connection to CXD Unified Services Port

There is only one method for connecting an existing colocation environment to the CXD Unified Services Port:

- **Ecosystem Connect:** The Ecosystem Connect product is a bundle of fiber, copper (ethernet), or coaxial cables connecting a customer environment to the Meet Me Room within a Cyxtera data center.
 - **Required:** An existing Cyxtera colocation environment.
 - **Required:** An Ecosystem Connect Bundle with two available ports.

2. Operations

The following outlines Cyxtera's roles and responsibilities in the service delivery of CXD Unified Service Port. While specific roles and responsibilities have also been identified as being owned by you, any roles or responsibilities not contained in this document are either not provided with the Service or assumed to be your responsibility.

2.1 Support

Cyxtera will provide support for problems that you report and selected additional Services to assist with adoption of CXD Unified Services Port. Support may be provided in any country in which Cyxtera or its agents maintain facilities. To the extent you provide your information and/or data in connection with support, we will handle your information and/or data in any such country in accordance with the

applicable service agreement, Cyxtera policies and all applicable laws.

2.2 Provisioning

Cyxtera will provide the following provisioning Services:

- Granting CXD Command Center access to administrative users using default administrator privileges and system preferences.
- Implementation of the CXD Port cross-connect.

You will be responsible for the following provisioning:

- Ensuring there are two available ports on your Ecosystem Connect Bundle for implementation.

2.3 Monitoring

Cyxtera will provide the following Services with respect to monitoring:

- Monitoring the CXD physical connections as well as the underlying network architecture.

You are responsible for the following with respect to monitoring:

- Monitoring the assets deployed or managed within your environment, including, but not limited to physical switches, routers, Compute Nodes, hypervisors, virtual machines, operating systems, applications, specific network configurations, operating system or application vulnerabilities, etc.

2.4 Incident and Problem Management

Cyxtera will provide incident and problem management Services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Infrastructure over which Cyxtera has direct, administrative, and/or physical access and control, such as Cyxtera data center, physical switches, routers, Compute Nodes, management servers, and network devices.
- Service software over which Cyxtera has direct administrative access and control, such as the Cyxtera Customer Portal, CXD Command Center, and other Cyxtera-owned APIs and applications that Cyxtera uses in delivery of the Service.

You are responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- User-deployed and configured assets such as switches, routers, hypervisors, virtual machines, operating systems, custom developed or third-party applications, network configuration settings, and user accounts.

2.5 Change Management

Cyxtera will provide the following change management elements:

- Processes and procedures to maintain the health and availability of the CXD Unified Services Port, Cyxtera Customer Portal, CXD Command Center, Cyxtera APIs, and CXD platform.

- Processes and procedures to release new code versions, hot fixes, and service packs related to the Cyxtera Customer Portal, CXD Command Center, Cyxtera APIs, and CXD platform.

You are responsible for:

- Management of change to your physical switches, routers, Compute Nodes, hypervisors, virtual machines, operating systems, custom or third-party applications, databases, and administration of general network changes within your control.
- Administration of self-service features provided through the Cyxtera user portals, up to the highest permission levels granted to you, including, but not limited to, CXD Unified Services Port, Compute Nodes and network functions, backup administration, user configuration and role management, general account management, etc.

2.6 Security

The end-to-end security of CXD Unified Services Port is shared between Cyxtera and you. Cyxtera will provide security for the aspects of the Service over which it has sole physical, logical, and administrative level control. You are responsible for the aspects of the Service over which you have administrative level access or control. The primary areas of responsibility between Cyxtera and you are outlined below.

Cyxtera will use commercially-reasonable efforts to provide:

- **Physical Security:** Cyxtera will protect the data centers, cages, and cabinets housing the CXD Unified Services Port from physical security breaches.
- **Information Security:** Cyxtera will protect the information systems used to deliver the Service for which it has sole administrative level control.
- **Network Security:** Cyxtera will protect the networks containing its information systems up to the point where you have some control, permission, or access to modify your networks.
- **Security Monitoring:** Cyxtera will monitor for security events involving the underlying infrastructure hardware, networks, and information systems used in the delivery of the Service for which it has sole administrative level control over. This responsibility stops at any point where you have some control, permission, or access to modify an aspect of the Service.
- **Patching & Vulnerability Management:** Cyxtera will maintain the systems it uses to deliver the Service, including the application of patches it deems critical for its target management systems. Cyxtera will perform routine vulnerability scans to surface critical risk areas for the systems it uses to deliver the Service. Critical vulnerabilities will be addressed in a timely manner.

You should address:

- **Information Security:** You are responsible for ensuring adequate protection of the information systems, data, content or applications that you deploy and/or access on the Service. This includes, but is not limited to, any level of patching, security fixes, data encryption, access controls, roles and permissions granted to your internal, external, or third-party users, etc.
- **Network Security:** You are responsible for the security of the networks over which you have administrative level control. This includes, but is not limited to, maintaining effective firewall rules, exposing communication ports that are only necessary to conduct business, locking down promiscuous access, etc.
- **Security Monitoring:** You are responsible for the detection, classification, and remediation of all

security events that are isolated with your account, associated with switches, routers, Compute Nodes, hypervisor, virtual machines, operating systems, applications, data, or content, surfaced through vulnerability scanning tools, or required for a compliance or certification program in which you are required to participate, and which are not serviced under another Cyxtera security program.

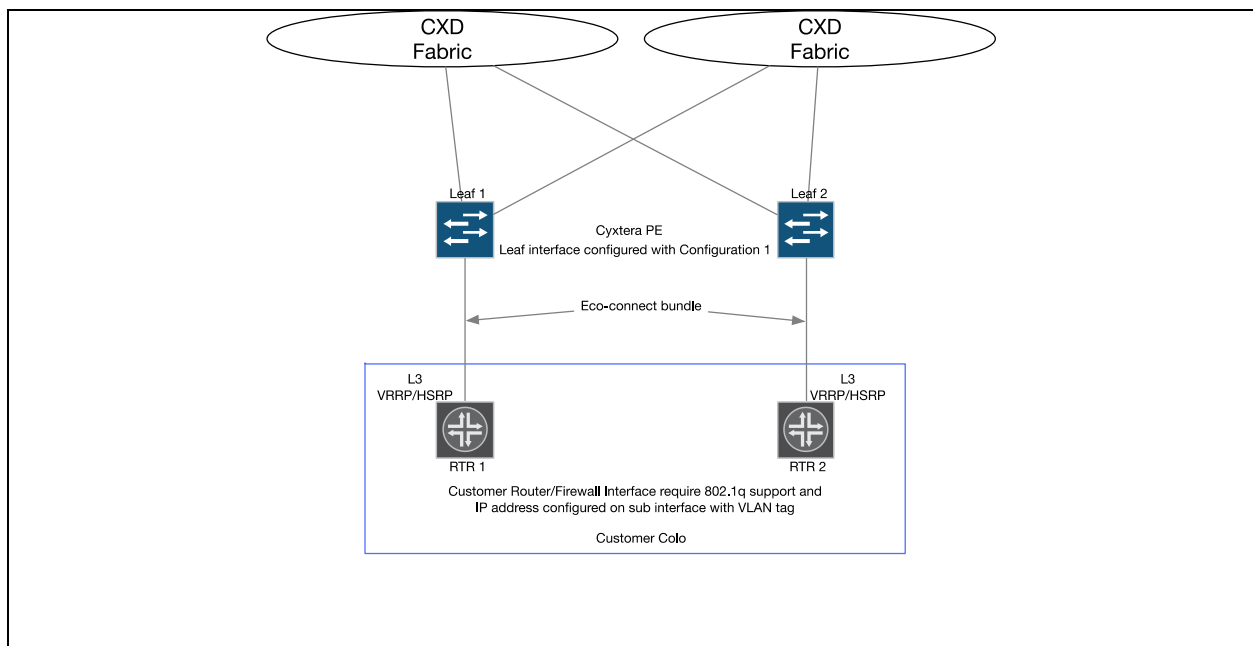
3. Configuration Options

3.1 Layer 3 CE

Layer 3 Customer Edge device that has physical interfaces configured with IPv4/IPv6 address and are considered to be Layer 3 network devices.

- Typically, HSRP/VRRP/GLBP first hop redundancy protocol would be used for failover on customer router.
- Both tagged and untagged interfaces are supported with this type of customer configuration.

Limitations: LAG/MLAG is not supported.



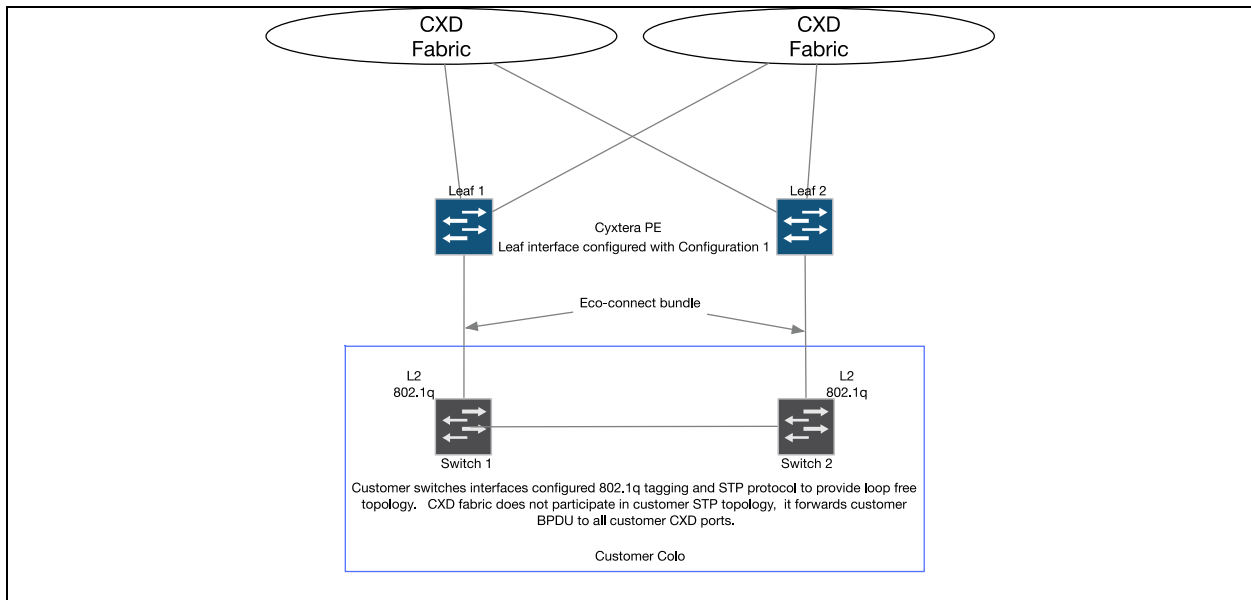
3.2 Layer 2 CE

Layer 2 CE: Customer Edge device that has physical interfaces configured with 802.1q and are considered to be Layer 2 networked devices.

- Customers that use this type of connection typically run STP within their environments to provide loop protection.
- CXD does not participate in customer STP topology, however STP BPDU will be passed through the CXD fabric to all customer Layer 2 CE ports to assure loop free environment through the fabric.
- This configuration is considered active/standby because of the blocked STP port.

Limitations:

- At this time, only per-VLAN implementation of STP is supported. (Example - Cisco PVST, Juniper VSTP).
- Dual home connectivity to single Layer2 CE is not supported.
- Layer2 CE with LAG is required.



3.3 Layer 2 CE with LAG

Layer 2 CE with LAG: An additional option for Layer 2 CE is LAG/MLAG configuration. This option builds on the standard Layer 2 CE configuration.

- Devices that are 'stacked' / 'virtual chassis' or capable of MLAG can be configured to take advantage of forwarding on all links connected to a CXD PE device.
- LAG/MLAG configuration is considered to be active/active.
- The CXD fabric uses flow-based load balancing for forwarding traffic towards Layer 2 CE ports.
- The CXD Unified Services Port requires LACP protocol for fast convergence of a link or device failure.
- The CXD Unified Services Port LACP is configured for fast periodic updates.

Limitations:

- Per packet load balancing is not supported on CXD Unified Services Ports.
- Vendor proprietary protocols are not supported for LAG/MLAG configuration.

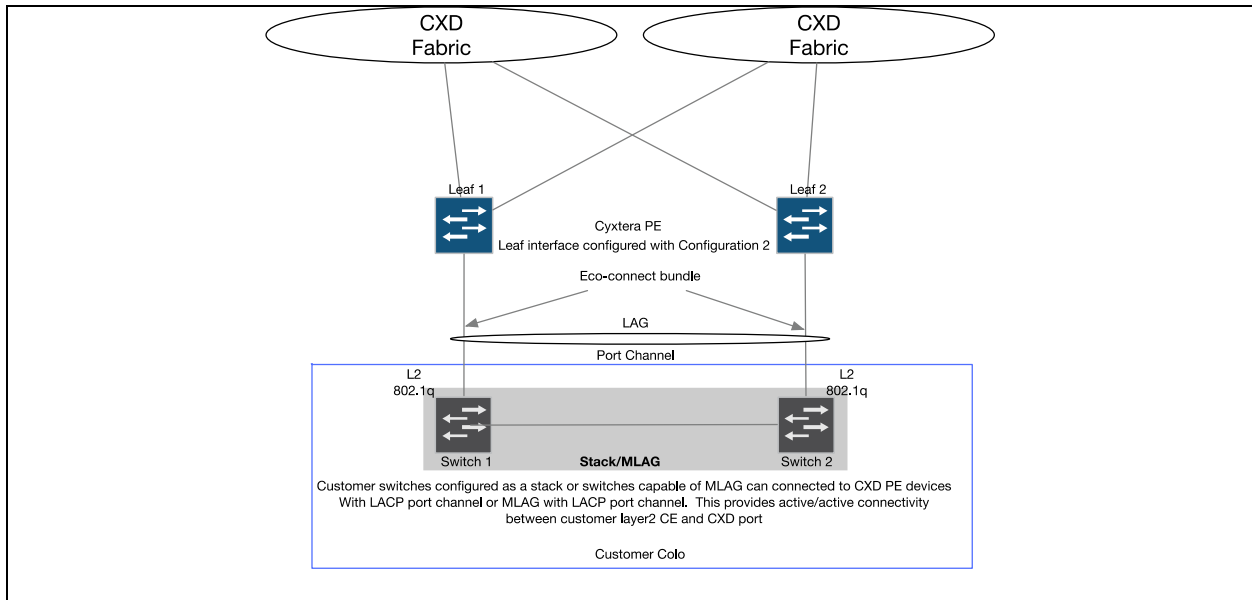


Figure 1 - Layer 2 MLAG example

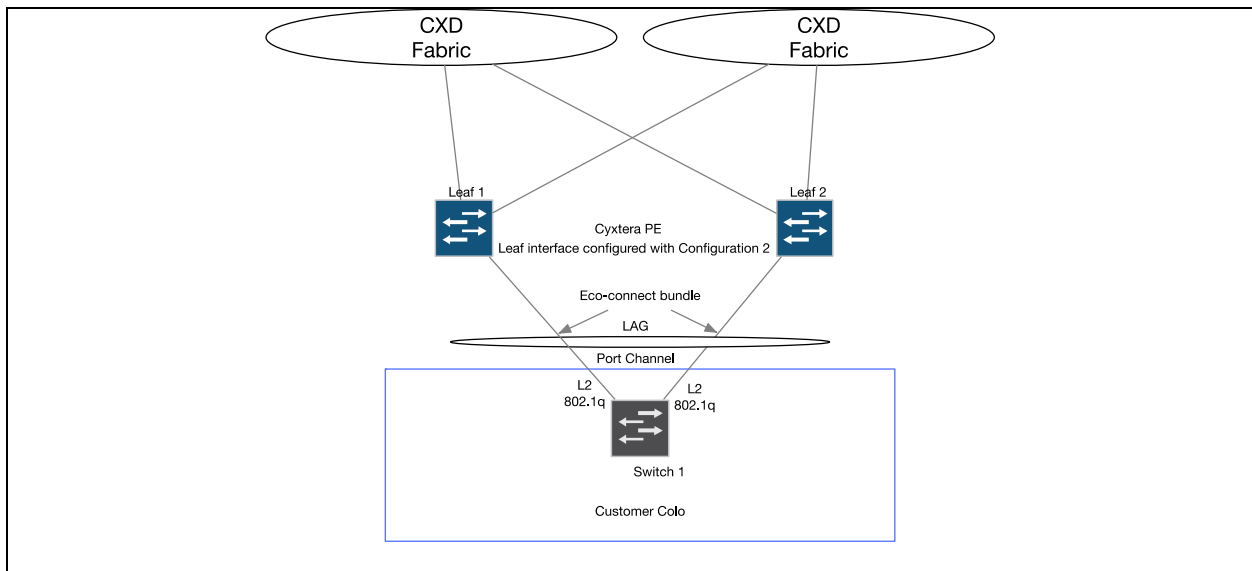


Figure 2 – Single homed Layer 2 LAG example

4. Business Operations

This section summarizes processes for ordering your CXD Unified Services Port(s).

4.1 Ordering

CXD Unified Services Port Ordering

Ordering the CXD Unified Services Port can be initiated via self-service through the CXD Command Center web console or CXD API, or by contacting your Cyxtera Sales Representative. Provisioning is handled via data center services and installed directly to the colocation environment. The prerequisite Ecosystem Connect bundle can be ordered as a new service via the Cyxtera Customer Portal or through your Cyxtera Sales Representative if one is not already in place to support the purchase of a CXD Unified Services Port.