TECHNOLOGY WHITE PAPER

Choosing a Rugged Ethernet Switch/Router Solution

CURTISS-WRIGHT

DEFENSE SOLUTIONS

Read About

Ethernet Switching

Network Routing

SWaP-C Optimization

Rugged COTS

Rugged Embedded Systems

Layer 2 vs Layer 3

Fiber Optics vs Copper

Network Management

Cisco Systems Technology

Info

curtisswrightds.com

Email

ds@curtisswright.com

Introduction

Mission-critical defense and aerospace applications depend on the power and effectiveness of Ethernet networking. Rugged networking solutions come in many varieties with a host of feature options to choose from. This white paper will help systems integrators and end users explore some of the key networking capabilities available in modern Ethernet switches and router systems designed to support intra- and inter-vehicle/aircraft network architectures. The various COTS networking systems available from Curtiss-Wright will be compared and contrasted in the context of selecting the most appropriate and capable solution to satisfy mission networking requirements.

Fundamental Questions about Network Architecture

When systems integrators develop new platforms or modernize legacy vehicles/aircraft, there are many fundamental questions asked about network architecture and the platform's intended mission capabilities which guide the selection of rugged switch and/or router Line Replaceable Units (LRU). Many of these architectural questions will be addressed within this white paper, including:

- Does the mission platform need a switch, a router, or both?
- What is the difference between a Layer 2 and a Layer 3 device?
- Should the network device be fully manageable or just plug-and-play?
- What devices will be connected and how does the traffic need to be managed?

- How many Ethernet ports and what speeds should the device support?
- What physical media (copper or fiber optics) and connectors are most appropriate?
- What role does size, weight, power, and cost (SWaP-C) play?
- Is a multi-function appliance or standalone switch/router LRU a better option?
- Is a ruggedized commercial solution or a natively rugged system a better option?
- How can existing IT network training and staff be leveraged to minimize support costs?
- What environmental/EMI validation testing is required for networking devices?
- Will the device be compatible with the aircraft generator and/or vehicle battery power input?
- How will network security and information assurance requirements be satisfied?

Router or Switch? Layer 2 or Layer 3?

Ethernet switches and routers form the core of network architectures. Switches connect devices on a Local Area Network (LAN) onboard ground vehicles or aircraft. They enable computers and sensors to communicate and share information locally. Connected devices might include a mission computer, flight computer, video camera, weapons system, Ethernet-enabled radio or other wireless device. Routers form the next layer of network connectivity. Switches often interface with routers to share information outside the vehicle or aircraft to a Wide Area Network (WAN) via a tactical radio, satellite modem, or other wired or wireless backhauls. This networking paradigm facilitates communication across applications and between vehicles in aerospace and defense platforms.

The Open Systems Interconnection (OSI) model of computer networking (**see figure 1**: OSI model) defines "layers" of functionality which correspond to traditional switch and router capabilities. Switching functionality is commonly associated with the Layer 2 data link, whereas routers are traditionally related to the Layer 3 network layer. That being said, some switches are Layer 2 and 3, providing efficient switching, as well as either static or dynamic IP routing capabilities. Layer 2 refers to a node-to-node frame delivery on the same link, whereas Layer 3 refers to the end-to-end (source to destination) connection including routing through intermediate hosts through optimized network protocols – such as Internet Protocol (IP).

FIGURE 1 OSI model of computer networking

	DATA UNIT	LAYER	FUNCTION
Host Layers	Data	7) Application	Network Process to Application
		6) Presentation	Data Representation & Encryption
		5) Session	Interhost Communication
	Segment	4) Transport	End-to End Connections & Reliability
Media Layers	Packet	3) Network	Path Determination & Logical Addressing
	Frame	2) Data Link	Physical Addressing
	Bit	1) Physical	Network Process to Application

Figure 1: OSI model of computer networking

Figure 2 highlights the corresponding OSI model layers for Curtiss-Wright's COTS network subsystems.

FIGURE 2 OSI model layers for Curtiss-Wright networking subsystems

CURTISS-WRIGHT PRODUCT	OSI LAYER	FUNCTIONALITY
Parvus DuraMAR (5915 / 31-5915)	Layer 2 and 3	Switching and Dynamic Routing
Parvus DuraWORX (10-10 / 80-41)	Layer 2 and 3	Switching and Dynamic Routing
Parvus DuraNET 3000 / 4948	Layer 2 and 3	Switching and Dynamic Routing
SMS-684	Layer 2 and 3	Switching and Dynamic Routing
Parvus DuraNET 2010 / 20-11 / 20-12 / 30-2020 / SMS-652 / DuraDBH-672	Layer 2 and Static Layer 3	Switching and Static IP Routing
Parvus DuraNET 1059 / 10-10 / 1268	Layer 2	Switching

Figure 2: OSI model layers for Curtiss-Wright networking subsystems

Need for Speed and Port Count

Despite the traditional desire to get lightning fast connectivity and throughput, not every application realizes tangible benefits from the faster pipes offered by 1, 10 or 40 GbE. In fact, 10/100 Fast Ethernet may meet some network requirements for WAN routing, since real-world network backhaul speeds are often slower than 100 Mbps in the field. This is because the speed of vehicle-to-vehicle platform communications is often constrained by the wireless radio connection, which becomes the bottleneck for speed and performance. Most satellite and tactical radio systems strain to achieve 5-10 Mbps throughput.

Since intra-vehicle LAN communications are not limited by the bottlenecks of a WAN connection, on-board computing devices certainly benefit from Ethernet switches offering 1 Gigabit/second or even faster connectivity. Relatively fewer applications require more than 1 Gbps; however the military is increasingly requesting 10 GbE switches in preparation for more bandwidth intensive applications, particularly those associated with high definition video surveillance, signal intelligence, radar, sonar, and high-performance communications systems. This trend is expected to increase as 10, 40 and 100 GbE technologies mature and become more commercially available.

In terms of port density, many military vehicle applications often just require 8-10 ports; however, this is largely dependent on the platform's concept of operations (CONOPS) and its physical constraints relative to SWaP-C. With the military's "future-proof" stance on technology insertions and the miniaturization of the modern networking technologies, 16-20 ports seems to be the "sweet spot" for a growing number of integration programs. Due to varying program requirements, the current Curtiss-Wright COTS systems portfolio includes network subsystems that support a range of speeds from Fast Ethernet up to 10G Ethernet connectivity with port counts starting at five, going up to 53 ports (**see figure 3**).

FIGURE 3 **Port count and speeds for Curtiss-Wright networking subsystems**

CURTISS-WRIGHT PRODUCT	PORTS (TOTAL)	10/100	GBE	10G
Parvus DuraNET 4948	53 x	1 x	49 x	3 x
SMS-684	24 / 28 x		24 x	0 / 4 x
Parvus DuraNET 3000	10 / 18 / 26 x	2 x	8 / 16 / 24 x	
Parvus DuraMAR 5915-2X	23 x	21 x	2 x	
Parvus DuraMAR 5915-3X	23 x	4 x	19 x	
Parvus DuraWORX (10-10 / 80-41)	21 / 22 x	4 / 19 x	2 / 18 x	
Parvus DuraNET 20-10	20 x		20 x	
Parvus DuraMAR 5915-1X	19 x	4 x	15 x	
Parvus DuraNET 30-2020	19 x	17 x	2 x	
Parvus DuraDBH-672 / DBH-670 Digital Beachhead / SMS-652	16 x		16 x	
Parvus DuraNET 1268	10 x		10 x	
Parvus DuraNET 20-11	8 x		8 x	
Parvus DuraNET 20-12	6 x	6 x		
Parvus DuraMAR 5915-0X / DuraMAR 31-5915 / DuraNET 10-50 / DuraNET 10-10	5 x	5 x		

Figure 3: Port count and speeds for Curtiss-Wright networking subsystems

Copper or Fiber? Connectors Types?

The type of physical media used for networking – typically copper or fiber optics – is another important choice that requires a balance of budget and functionality. Depending on the application, each has its pros and cons. Fiber optics is capable of transmitting data over long distances and providing greater data security than copper. That's because fiber optics delivers less signal loss and is more resistant to electromagnetic interference (EMI). That being said, the bend radius of fiber optic cabling is less forgiving compared to copper and installation of optical network is often more expensive compared to traditional twisted pair copper wiring (e.g. CAT 5E/6), the mainstay of home and office networks. For a large majority of military and aerospace, copper media is considered a "good enough" solution. Some deployed systems use both, playing to each medium's strengths: copper for onboard Gigabit Ethernet communications and fiber optic for higher-speed applications and network-to-network communication across considerable distance.

Figure 4: MIL-DTL-38999 connector

The type of physical network connectors to which the copper or optical cabling is wired is another important consideration to achieve reliable network connectivity onboard vehicles or aircraft. Protections against environmental factors, such as water or vibration, for example, should be considered to eliminate the possibility of damage or ports becoming disconnected. Traditional RJ-45 connectors, for example, which are found on commercial-grade networking equipment, are notoriously prone to failure under extreme vibration and provide very limited ingress protection against dust and water. Typically an IP67-rated (dust/water proof) locking connector that rackets down or has a secure push-pull feature is recommended. Many rugged connector types abound, but the most commonly implemented approach in military and aerospace electronics application is circular MIL-DTL-38999 Series III connectors (**see figure 4** – These generally meet the desired requirements up to Gigabit Ethernet speeds. Micro-miniature versions of these connectors are also now available to support lower size/weight requirements.

FIGURE 5 **Port count and speeds for Curtiss-Wright networking subsystems**

CURTISS-WRIGHT PRODUCT	CONNECTOR TYPE(S)	MEDIA
Parvus DuraMAR 5915	MIL-DTL-38999	Copper
Parvus DuraMAR 31-5915, DuraNET 10-10	M12 / Industrial RJ-45	Copper
Parvus DuraWORX 10-10 / 80-41	MIL-DTL-38999	Copper
Parvus DuraCOR (810/830/810D/80-40/80-41)	MIL-DTL-38999	Copper
Parvus DuraNET 20-10 / 30-2020 / 3000, SMS-652	MIL-DTL-38999	Copper
Parvus DuraNET 4948 / 1268, SMS-684	MIL-DTL-38999	Copper + Optical
Parvus DuraNET 20-11, DuraCOR 820	Miniature DTL-39999	Copper
Parvus DuraNET 20-12	Rectangular Quadrax	Copper
Digital Beachhead (DuraDBH-672, DBH-670)	MIL-DTL-38999	Copper

Figure 5: Port count and speeds for Curtiss-Wright networking subsystems

Where cost and size are important considerations, multiple Ethernet ports can be combined on a single connector to reduce the subsystem's physical size. Human engineering factors described in MIL-STD-1472 should also be considered for users of networking equipment, including the spacing between connectors on the system, which can impact the ease of installing and/or removing the unit, particularly if installers are wearing gloves. For speeds of 10Gbps or more, or where signal integrity is paramount, new and specialized interconnects are becoming available within DTL-38999 connector shells and other connector types.

Figure 5 highlights the various types of connectors and media used by Curtiss-Wright networking systems.

Managed or Unmanaged?

Network switches come in two basic varieties, unmanaged and managed. Unmanaged switches require no configuration and are designed for simple plug-and-play operation. A managed switch conversely can be configured over a serial Command Line Interface (CLI) and/or Ethernet ports using a Graphical User Interface (GUI) or remote terminal application.

For some military and aerospace platforms, an unmanaged switch can be an ideal solution, since these are relatively easy to use and low cost. Unmanaged switches can also be ideal for scenarios where network traffic is light and the data simply needs to pass from one device to another. Rather than giving a user the ability to configure link parameters or prioritize network traffic, unmanaged switches "auto-negotiate" the data rate and whether to use half-duplex or full-duplex mode. Unmanaged switches can also be helpful when a Virtual Local Area Network (VLAN) has already been defined and there's a need to merely expand the port count on the edge of the network.

Although managed devices are more commonly installed for new technology insertions to provide the most flexibility for growth, unmanaged switches still play an important role as a piece in the overall networking architecture, including within many rotary aircraft modernization programs. The U.S. Army's Aviation Applied Technology Directorate (AATD), for example, specifies a Curtiss-Wright Parvus DuraNET unmanaged Ethernet switch subsystem in the AH-64 Apache helicopter (see **figure 6**) to improve situational awareness and connect onboard computing devices. Multiple unmanaged Ethernet switches are also integrated into the Light Airborne Multi-Purpose System (LAMPS) onboard the U.S. Navy SH-60 Seahawk.

Figure 6: AH-64 Apache Helicopter

Since managed switches support capabilities to shape and configure the network traffic, the device's management software can be critical to a platform's mission success. The most widely used network management software has been the Cisco Internetworking (Cisco IOS) software, which is accounted for in more than 50% of all switches and routers worldwide, according to Cisco estimates. Consequently, even non-Cisco managed network solutions are often patterned after the command line approach and capabilities introduced by Cisco.

Key Management Features

By providing users with options for monitoring and configuring networks, managed switches provide military and aerospace platforms with greater control and security over their LAN data. Maintaining situational awareness through the use of video, maps, radio and satellite technologies requires a networking infrastructure that can manage and prioritize data packets to ensure mission safety and success. There are a

Figure 7: QoS can be used to prioritize network traffic files (i.e. map/surveillance images)

variety of important management protocols and capabilities available to support such applications, including Quality of Service (QoS), Virtual Local Area Networks (VLAN), Spanning Tree redundancy, and Simple Network Management Protocol (SNMP), among others.

QoS allows users to prioritize network traffic by assigning a higher priority to traffic from particular ports, VLANs, IP classes, tags, etc. This helps ensure consistent network performance for critical, time-sensitive data. QoS is especially critical for military users in a mixed-traffic environment where large data files such as map images (**see figure 7**) can delay important voice packets or flash messages that need to reach the vehicle operator. QoS allows the user to tag certain traffic as high priority to ensure delay-sensitive data is delivered in a timely manner.

Similarly, VLANs featured on managed switches allow connected devices to be logically grouped together and to isolate traffic between groups, even when the traffic is passing over the same physical switch. This segmentation and isolation of network traffic helps reduce unnecessary traffic and provides maximum bandwidth to devices that need to communicate to each other, providing better network performance, and in many cases, an additional level of security.

Another common feature of managed switches is support for redundancy – to safeguard a network in case a connection or cable fails by providing an alternate data path for traffic. Many switches incorporate Spanning Tree Protocols (STP), such as RSTP or MSTP, to provide path redundancy in the network. Using spanning-tree algorithms, STP allows for one active path at a time between two network devices, preventing loops and establishing the redundant links as a backup to keep integrated systems available and to prevent expensive downtime. It is not uncommon for redundant flight electronics onboard manned and unmanned aircraft to be networked by Ethernet switches supporting some form of STP. In this way, onboard mission computers have multiple potential data paths and can quickly recover if critical hardware fails.

Monitoring functions of network switches via the SNMP protocol can provide additional control and efficiency. SNMP facilitates the exchange of management information between network devices, allowing users to determine the health of the network or the status of a particular device. This includes the number of bytes and/or frames transmitted and received, errors generated, and port status. By displaying this data over a standard web browser, administrators can monitor the performance of the network and quickly detect and repair network problems without having to physically interact with the switch.

SWaP-C

With shrinking government budgets and program-specific technical requirements, there is mounting pressure on defense and aerospace contractors to provide networking solutions with reduced Size, Weight, Power, and Cost (SWaP-C). The objective is to fit as much functionality as possible in the smallest, lightest package for the least amount of money to empower the greatest efficiency and performance onboard defense and aerospace applications, including unmanned vehicles.

That being said, managing SWaP-C or “SWaP optimization” isn’t done in a vacuum without considering many other program priorities and tradeoffs that go well beyond SWaP. Program managers ultimately consider cost, performance requirements, supported feature and capabilities, reliability under extreme environments, cooling methods and thermal management, schedule and lead time constraints, use of COTS and open standards versus custom, length of life cycle management and obsolescence mitigation and scalability, among others.

SWaP reduction is a key focus at Curtiss-Wright when developing next generation systems and recent advancements in technology are helping the company achieve impressive results. A noteworthy example of recent SWaP reduction is with Parvus DuraNET Gigabit Ethernet switches. The latest model, the 20-11 (**see figure 8**), provides 8 ports of fully managed Gigabit Ethernet switching in an ultra-miniature form factor that is a mere 10 cubic inches in

Figure 8: Parvus DuraNET 20-11 Ultra small form factor Ethernet switch

size. This represents a 90% size reduction from the next smallest Gigabit Ethernet switch subsystem. SWaP-sensitive platforms like unmanned air systems (UAS) are driving demand for such small network connectivity devices – and component miniaturization is helping Curtiss-Wright achieve the improvement in SWaP optimization. This level of miniaturization is enabling integration of LAN connectivity and more payload electronics than ever before to satisfy mission requirements. Relative size and weight comparison of Curtiss-Wright networking systems is shown in **figure 9**.

FIGURE 9 **SWaP Comparison of CW Networking Products**

Product	Size	Weight	Power	Ports
DuraNET 4948	1518 in³	26 lb	< 275W	49x GbE + 3x 10G + 1x 10/100
SMS-684	313 in³	12 lb	< 60W	24x GbE + 4x 10G
DuraWORX 80-41	278 in³	9.5 lb	< 90W (base)	4x 10/100 (base) + 16x 10/100 or 18x GbE (w/switch)
DuraWORX 10-10	278 in³ (base)	12.5 lb (base)	< 65W (base)	4x 10/100 (base) + 16x 10/100 or 18x GbE (w/switch)
DBH-670	236 in³	6.5 lb	< 25W	16x GbE
DuraNET 3000	220 / 354 / 358 in³	6.8 / 9.9 / 10.4 lb	< 25W	2x GbE + 8/16/24x 10/100
DuraMAR 5915 -2X	211 in³	< 9 lb	< 30W	19x GbE + 4x 10/100
DuraNET 1268	204 in³	4.8 lb	< 25W	10x GbE
DuraMAR 5915 -3X	211 in³	< 9 lb	< 35W	2x GbE + 21x 10/100
DuraMAR 5915 -1X	197 in³	7.39 lb	< 50W	15x GbE + 4x 10/100
SMS-652	178 in³	5 lb	< 20W	16x GbE
DuraNET 10-10	99 in³	3.5 lb	< 8W	5x 10/100
DuraNET 30-2020	126 in³	4.1 lb	< 20W	2x GbE + 17x 10/100
DuraNET 1059	124 in³	1.9 lb	< 8W	5x 10/100
DuraDBH-672	131in³	< 4.0 lb	< 25W est	16x GbE
DuraMAR 5915 -0X	112 in³	4.0 lb	<15W	5x 10/100
DuraNET 20-10	112 in³	4.0 lb	< 25W	20x GbE
DuraNET 20-11	10 in³	0.50	< 8W	8x GbE
DuraNET 20-12	10 in³	0.54	< 5W	6x 10/100

Figure 9: SWaP Comparison of CW Networking Products

One newer SWaP reduction approach used by Curtiss-Wright is to consolidate networking and processor functions into a single hardware device that uses software-based networking and hypervisor virtualization applications to provide Layer 3 secure mobile routing and/or VPN encrypted security functionality (**see figure 10** – This bolt-on network software approach provides the same feature sets available in dedicated hardware-based networking devices but in a software format that can be pre-loaded on rugged, general-purpose, x86 mission computers. Logically, this software approach adds no physical size or weight to the LRU – it just utilizes some portion of the processing capabilities. The overhead from the software may not be significant for multi-core high performance systems like for the quad-core, 4th Gen Core i7-based Parvus DuraCOR® 80-41 computer (**see figure 11**).

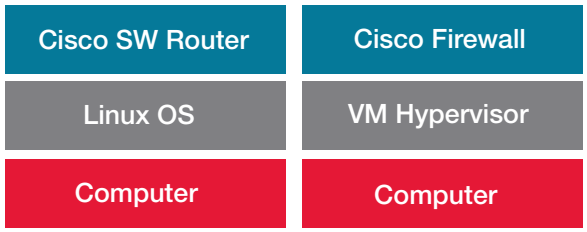

Figure 10: Software-based networking functionality

Figure 11: Parvus DuraCOR 80-41 4th Gen Core i7 Mission Computer

Multi-function Appliance vs Standalone LRU

Not only can combining hardware and software yield SWaP-C reduction, but also consolidating what have been traditionally standalone hardware-based LRUs into a single multi-function system solution. Many military programs have begun to request subsystems that can combine network processing, Ethernet LAN switching and IP traffic routing in a single box (**see Figure 12**). Depending on the project, this can be motivated by various factors, including SWaP constraints or objectives to simplify systems integration. Some programs aim to reduce the number of power supplies or cables on-board a vehicle, while others seek a solution with flexible mechanical installation options. The U.S. Army's Vehicle Integration for C4ISR/EW Interoperability (VICTORY) initiative is an excellent example of this trend, as ground vehicle architects aim to trim unnecessary fat while leveraging modern computing and networking architectures.

Open architecture, pre-integrated products featuring modularity (mix and match functionality) are most attractive to the Department of Defense (DoD) since they do not require significant engineering expertise for customization or tailoring to program needs. To support these objectives, Curtiss-Wright has designed several scalable, rugged multi-function computing and networking subsystems based on Intel® x86 or Freescale ARM® processors together with various integrated network switch/router options, including DuraWORX® products and Digital Beachhead™ systems.

The Parvus DuraWORX product line exemplifies this ultra-rugged multi-function computing and networking system concept, combining a multi-core high performance Intel Core™ i7 based mission processor together with a Cisco 5915 IOS-managed secure network router and optional Ethernet switch into a single modular platform designed for extended temperature, high shock and vibration environments. DuraWORX is a scalable, all-in-one computing appliance aimed at reducing SWaP and simplifying systems integration (thermal, cabling, power, installation) in tactical computing, IP networking and situational awareness applications.

The Digital Beachhead™ product line includes LRUs that feature 16 ports of fully managed Layer 2 GbE switching and static Layer 3 routing together with a low-power multi-core ARM-based Freescale™ i.MX6 processor capable of supporting general-

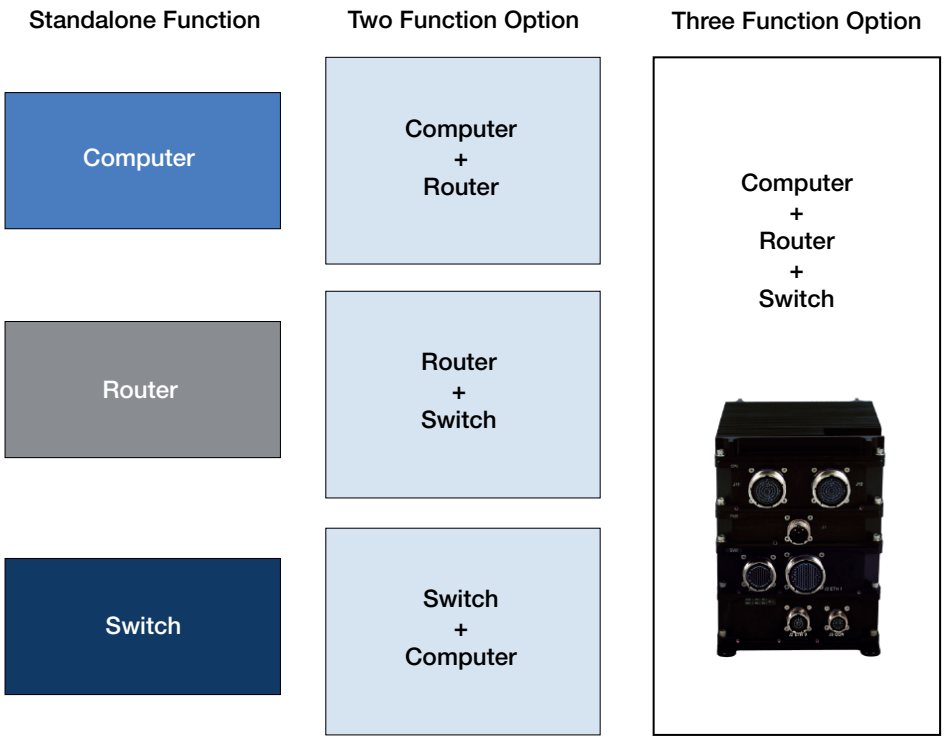

Figure 12: Standalone vs Multi-function networking appliance

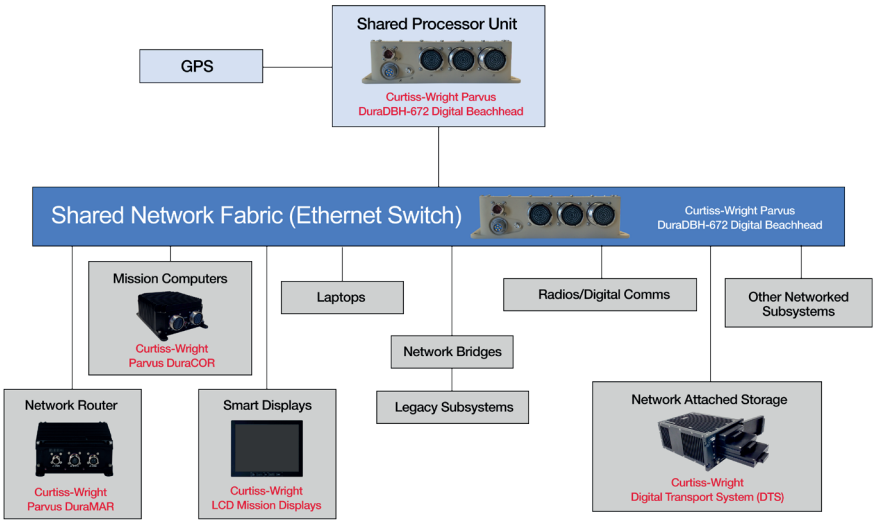

Figure 13: Shared network/processor services of multifunction DuraDBH-672 Digital Beachhead system

purpose processing requirements or optional VICTORY Data Bus Management and Shared Processor Services. These multi-function computing and networking devices serve as SWaP-C optimized vetronics computers with integrated network switch and GPS receiver, providing a digital backbone over Ethernet for network devices to be plugged into a vehicle and utilize CPU processing to deliver services to the platform (**see figure 13**).

Environmental / EMI /Power Testing

Ethernet switches and routers intended for installation on tactical mobile platforms such as ground vehicles, aircraft, or maritime vessels should naturally be designed with reliability in mind, as mission effectiveness and personnel safety can be compromised if a device fails. Validation testing should be done to either MIL-STD-810 and/or DO-160 (or equivalent) standards to qualify the equipment to specified temperature ranges, vibration frequencies, altitude, humidity offered by the device. In addition, EMI testing for radiated and conducted emissions and susceptibility and power quality compliance testing should be performed to MIL-STD-461, MIL-STD-704 and/or MIL-STD-1275 (or equivalent) to ensure compatibility with aircraft and vehicle voltage inputs, spikes, and transient levels. All Curtiss-Wright COTS networking products come pre-validated to some combination of these tests to reduce risk, time, and expense for systems integrators selecting switches and routers for their platform.

Rugged vs Ruggedized

As defense and aerospace applications typically operate in extreme environments, it is critical for network integrators to specify equipment designed for harsh deployed conditions, which may include EMI, dust, water, temperature extremes, vibration, humidity and high altitude. The terms “rugged” and “ruggedized” are often used to describe electronics capable of enduring tough environments; however, there is a distinction between the two terms that indicates how a product for military use was created. “Rugged” systems are products designed from the ground up to meet the requirements of specific harsh environments. Conversely, the term “ruggedized” typically refers to a commercial product that was not originally intended for as demanding of application, but was enhanced to endure airborne, ground vehicle, and/or shipboard deployments.

With military customers seeking the most robust yet economical solution, weighing the tradeoffs between a “ruggedized” product and a natively rugged one is a worthy exercise. There are many advantages of each approach.

For example, natively rugged solutions may offer more control over the component selection and/or bill of materials (BOM) since qualification testing has validated the design and the product was specified from conception for an extreme environment. A ruggedized solution, based on a network switch from Cisco Systems (**see figure 14**), may need to be enhanced to operate

Figure 14: Ruggedized Cisco switch, the Parvus DuraNET 3000

in such environments, but can potentially reduce the time to deployment to the battlefield and expense to maintain, since many military personnel are already trained to operate Cisco's network management IOS software. Consequently, several product models (**see figure 15**) from Curtiss-Wright integrate natively-rugged Cisco router/switch board hardware or alternatively integrate ruggedized commercial/industrial-grade switching hardware qualified through MIL-STD testing. In cases where performance or physical form factor cannot be satisfied with Cisco hardware, Curtiss-Wright also develops its own rugged hardware to meet specialized customer requirements, including rugged 10G switches and ultra-small form factor devices.

FIGURE 15 Integrated Cisco Technology

CURTISS-WRIGHT PRODUCT	INTEGRATED CISCO TECHNOLOGY
Parvus DuraMAR (5915 / 31-5915)	Cisco 5915 Embedded Services Router
Parvus DuraWORX (10-10 / 80-41)	Cisco 5915 Embedded Services Router
Parvus DuraCOR 80-41	Cisco 5921 Embedded Service Router
Parvus DuraNET 3000	Cisco IE-3000 Industrial Ethernet Switch
DuraNET 30-2020	Cisco ESS 2020 Embedded Services Switch
Parvus DuraNET 4948	Cisco Catalyst 4948E Ethernet Switch

Figure 15: Cisco technologies integrated into Curtiss-Wright rugged systems

Leveraging IT Investment

Networking products need technically trained staff to operate and maintain them, which presents an opportunity for some organizations to leverage existing IT and network training investment if they select products based on industry standards.

John Chambers, CEO of Cisco Systems, reported during a news interview that the company had more 70% market share in the US government public sector. Cisco is also credited with helping to define many of today's networking standards and protocols, actively contributing to the standards committees within the Internet Task Force, IEEE, and other groups. This pervasiveness of Cisco technology and its IOS software makes them the "industry standard" to which more network professionals are trained. It logically follows by selecting products based on Cisco technology or products that are standards-based and are "Cisco-like", the cost to maintain and operate them should be reduced.

The familiarity with Cisco's network management software was a significant motivating factor for the US Marine Corps (USMC) selection of rugged Curtiss-Wright switch and routers systems based on Cisco technology for the backbone upgrade of the AAVC-7A1 (**see figure 16**), the command variant of the Amphibious Assault Vehicle. The U.S. government needed to upgrade the networking architecture onboard the AAVC-7 to extend the service life of the platform and transition from legacy Cisco IOS-based

Figure 16: USMC Amphibious Assault Vehicle

router and switch subsystems to newer Cisco technologies that could easily be configured and maintained using a familiar Cisco Command Line Interface (CLI). Solid performance with previous generations of Cisco-based Parvus DuraMAR router/ DuraNET switch subsystems installed in the earlier models of the AAV platform also positioned Curtiss-Wright as the supplier of choice for the AAVC-7 network upgrade. The SWaP-C optimized Parvus LRUs, based on the latest Cisco embedded switch and router technologies, were selected by the customer to provide network connectivity for the tactical comms equipment used onboard the vehicle.

Security and Information Assurance

Beyond configurability, the information assurance for the network is another important consideration. Like many other vehicle platforms, the networking system deployed on the AAVC-7 had information assurance and interoperability requirements specific to the DoD. An important reason why the DuraNET switch and DuraMAR router (**see figure 17**) were selected was because these LRUs were listed on the DoD's Unified Capabilities Approved Product List (APL), which validated them for DoD worldwide agency use. Many Cisco-based technologies, like those used on the AAV, undergo information assurance validation and testing at third-party laboratories for certifications to FIPS 140-2 (Federal Information Processing Standard Publication 140-2), NAIP Common Criteria Evaluation (National Information Assurance Partnership/Common Criteria Evaluation and Validation Scheme), and/or DoD APL approval.

Author

Mike Southworth, B.A., M.B.A.

Product Marketing Manager

Curtiss-Wright Defense Solutions

Figure 17: Rugged Cisco Router and Switch Systems

Network security is often achieved through a variety of secure network management protocols and authentication methods supported by switches and routers. For example, Secure Shell (SSH) and Simple Network Management Protocol (SNMP) provide encrypted administrator traffic during Telnet and SNMP sessions. TACACS+ and RADIUS authentication facilitates centralized control and restrict unauthorized users, and Dot1x, port security and DHCP allow dynamic port-based authentication. These along with intrusion detection firewalling, Network Address Translation (NAT), Access Control Lists (ACL), virtual local area networking, and various cryptographic technologies such as AES-256 or NSA Suite B encryption help to protect network data. Many Curtiss-Wright systems also support a non-destructive zeroization feature to sanitize the switch or router should the platform be compromised, clearing out system firmware, as well as network addresses and configuration settings.

Looking forward

Defense and aerospace integrators are expected to increasingly look to Ethernet network-based technologies to achieve fast, flexible and secure network communications onboard vehicles and aircraft. Advancements in throughput, management capabilities, and rugged (and low SWaP) system design will give many new options to systems integrators to achieve their network-centric operational goals. The COTS portfolio of networking solutions from Curtiss-Wright will continue to evolve to even better meet these needs and offer modern capable network solutions well suited for deployment at the network edge.

Learn More

Products: Curtiss-Wright Rugged Ethernet Switch and Router Systems

User Story: Switch and Router Subsystems Onboard Amphibious Assault Vehicle

User Story: Miniature Ethernet Switches Deployed Onboard Unmanned Aircraft Systems

User Story: Rugged Switch Deployed On-Board Space Launch Vehicle

White Paper: Consolidate LRU While Considering SWaP constraints

Web Page: Cisco Technology