

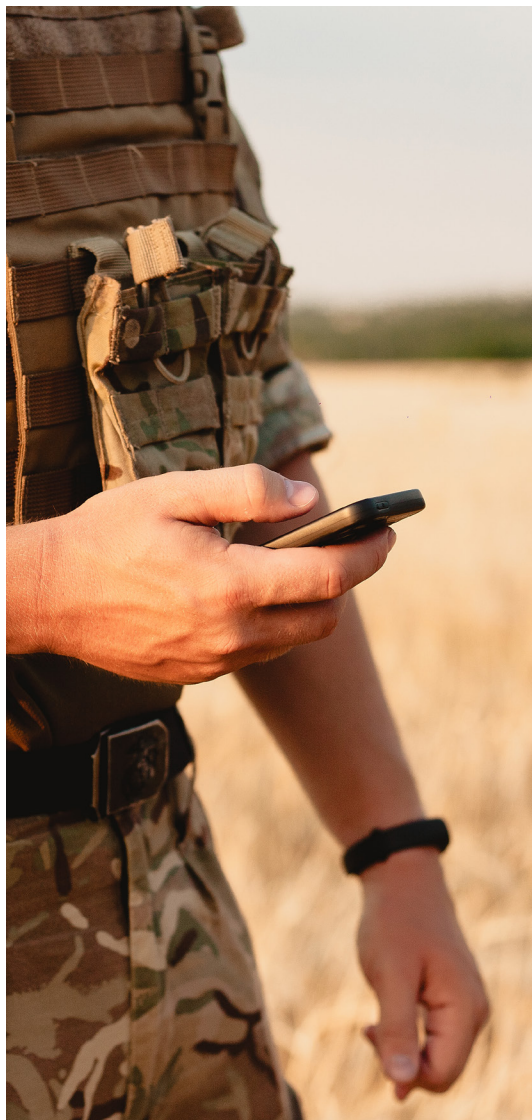


**CURTISS -
WRIGHT**

PacStar Secure Wireless Command Post Extension (SWCP-X) for Remote Command Post C2 Infrastructure



Secure Wireless Command Post Extension (SWCP-X) for Remote Command Post C2 Infrastructure



PacStar SWCP-X enables classified and unclassified wireless for vehicle-to-vehicle (V2V) and vehicle-to-end user device (V2E) communications in expeditionary and tactical environments

The U.S. armed forces have called for more mobility, maneuverability, interoperability and reduced setup time for tactical command posts. To meet those objectives, command post programs are moving away from large complexes relying on multiple tents, to architectures based on vehicle-mounted communications shelters utilizing wireless technologies. This new approach promises to dramatically reduce setup time associated with constructing tents and data-center like infrastructure and laying thousands of feet of cable. To make this happen, programs are looking to small form factor, rugged, commercial-off-the-shelf technologies that fit within limited spaces and provide wireless network access inside vehicle shelters and between vehicles.

PacStar SWCP-X is a key component of a modern vehicle mounted command post program. It is a small modular, commercial-off-the-shelf (COTS) communications package that enables remote command post support vehicles to communicate with primary command post vehicles over mesh wireless networks, while simultaneously extending the benefit of network access and wireless local area network (WLAN) services to remote users.

The remote capabilities of PacStar SWCP-X complements PacStar Secure Wireless Command Posts (SWCP), in use today in U.S. Army PM Tactical Network command posts for wireless network access. Working together, the combination creates a complete, multi-vehicle mobile command post system utilizing Commercial Solutions for Classified (CSfC) architectures. The system is capable of supporting C2 communications over multiple classified, unclassified and coalition partner networks.

PacStar SWCP-X is based on the proven PacStar 400-Series family of networking and compute modules, in use today in numerous fly-away, vehicle and airborne programs, which uses identical, fully certified and accredited hardware and software components to PacStar SWCP – simplifying integration, training, supply chain, and accreditation processes.

Key Features

- **Modular, low-SWaP solution including all components necessary for a CSfC Remote Site** (layered IPsec VPN, firewalls, etc. necessary to meet DoD requirements and guidelines for transmitting multiple classified or unclassified networks)
- **Includes technologies listed on the Common Criteria, FIPS, and DODIN evaluated or approved lists***, easing certification and accreditation processes
- **Expandable/modular system** may be customized to meet expanding mission requirements with added networks (such as NIPRnet, MPE, etc.)
- **Based on rugged, MIL-STD tested, PacStar 400-Series modules** that optimize SWaP and maximize deployment flexibility
- **Managed by PacStar IQ-Core® Crypto Manager**, providing management, configuration and trouble-shooting of Wi-Fi and VPN capabilities including digital certificates and SIEM in accordance with government requirements

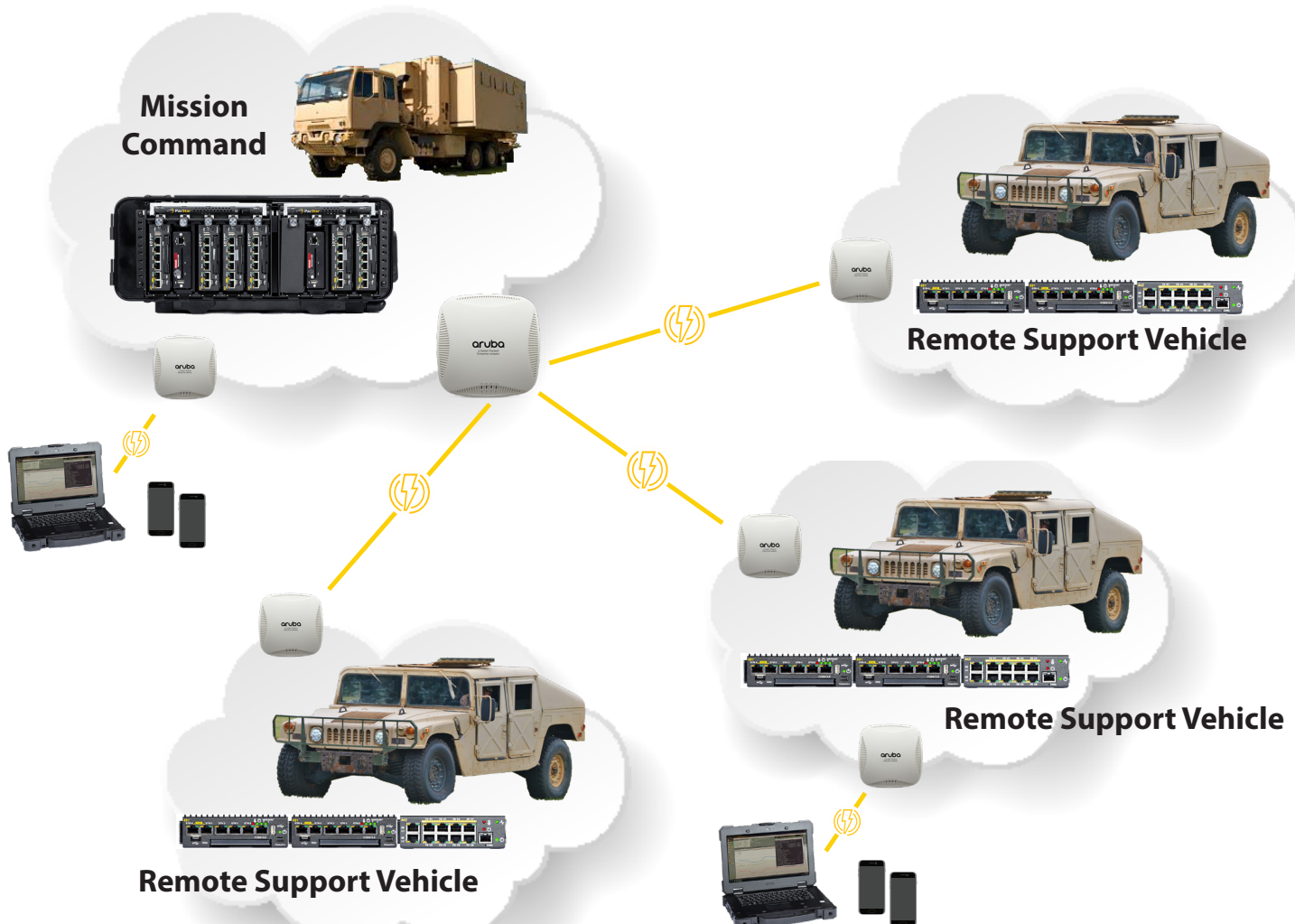
*Common criteria and FIPS evaluated technologies on select PacStar 451 Xeon E3 models. PacStar 451 Xeon D model Common Criteria and FIPS evaluation or listing dates.

Solution Architecture

A complete modern architecture for mobile command posts includes PacStar SWCP mounted on main command post platforms, and PacStar SWCP-X on remote (smaller) support vehicles. PacStar SWCP provides Central Site encryption, PKI and management services for the entire fleet of connected vehicles and end-user devices. PacStar SWCP also provides Wi-Fi access points on the main command post platforms for end-user Wi-Fi access.

On remote support vehicles, for V2V communications, PacStar SWCP-X uses layered IPsec VPN gateways over meshing radio, enabling the transport of one or more classified and/or unclassified networks between remote support vehicles and main command post vehicles.

On remote support vehicles, for V2E communications, PacStar SWCP-X includes Wi-Fi access points configured to meet CSfC requirements that provide network access to end user devices such as laptops, tablets and smartphones. The Wi-Fi network uses layered encryption managed by PacStar SWCP in the main command post vehicle, extending Wi-Fi services to remote vehicles while minimizing SWaP for remote vehicles.



PacStar systems including this product may be covered by one or more of the following US patents: #8,654,749, #7,817,589, #8,270,325, #9,160,619, #9,225,102. Additional patent(s) pending. See www.pacstar.com/patents for details.



PacStar SWCP-X Contents

PacStar SWCP-X supports one or multiple networks and can be scaled to meet customer-specific mission requirements, typically utilizing the following PacStar components configured in accordance with Commercial Solutions for Classified Multi-site Connectivity Capability Package v1.1 – as a “Remote Centrally Managed Site”.



**PacStar 451
Rugged Server with
Aruba Mobility Controller**

a Hewlett Packard
Enterprise company



**PacStar 451
Rugged Server with
Cisco ASA**




**PacStar 451
Rugged Server with
Palo Alto VM**




**PacStar 442 Switch
with Cisco ESS 2020**


Network Infrastructure/Encryption

- Outer VPN Gateway (Aruba VMC)
- Traffic Filtering Firewall/IDS (Palo Alto VM)
- Management (IQ-Core Crypto Manager)
- Network Services (Domain Services, NTP) (Optional)
- Inner VPN Gateway (Cisco ASA)

Network Access

LAN Access

- One or more PacStar 442 Ethernet switches for wired access

V2E Wi-Fi WLAN Access

- Aruba AP-305 controlled by PacStar SWCP on main command post platform

V2E Mesh Access

- Aruba AP-305 running in mesh mode

One Network Configuration

Suitable for use with a single classified network, such as SIPRnet.

- 1 Outer IPsec VPN Gateway (Aruba VMC on PacStar 451)
- 2 Inner IPsec VPN Gateway (Cisco ASA on PacStar 451)
- 3 User access switch (Cisco ESS 2020 in PacStar 442)



Two Network Configuration

Suitable for use with a two networks, such as SIPRnet and NIPRnet, sharing the outside VPN Gateway.

- 1 Outer IPsec VPN Gateway (Aruba VMC on PacStar 451)
- 2 Inner IPsec VPN Gateway (Cisco ASA on PacStar 451)
- 3 User access switch (Cisco ESS 2020 in PacStar 442)
- 4 Gray Traffic Filtering Firewall (Palo Alto VM on PacStar 451)
- 5 Inner IPsec VPN Gateway (Aruba VMC or Cisco ASA on PacStar 451)
- 6 User access switch (Cisco ESS 2020 in PacStar 442)

