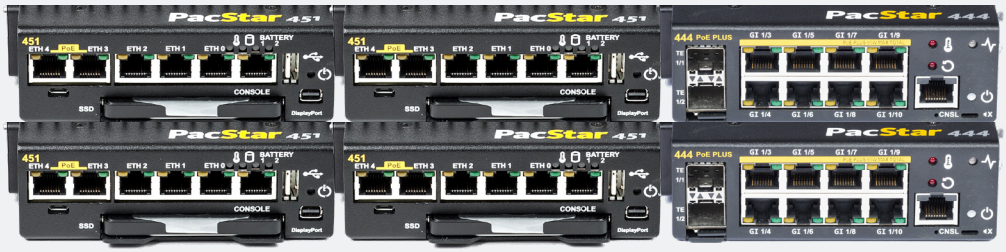
CURTISS-WRIGHT



PacStar Secure Mesh Command Post (SMCP)

Transport agnostic classified and unclassified wireless network for vehicle to vehicle and vehicle to end user communications

PacStar SMCP is a key component of a modern vehicle mounted command post program. It is a small, modular, COTS communications package that enables remote command post and network support vehicles to communicate with primary command post vehicles over mesh wireless networks

The remote capabilities of PacStar SMCP 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.

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 DoDIIN 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 troubleshooting of Wi-Fi and VPN capabilities

***Common criteria and FIPS evaluated technologies on select PacStar 451 models**

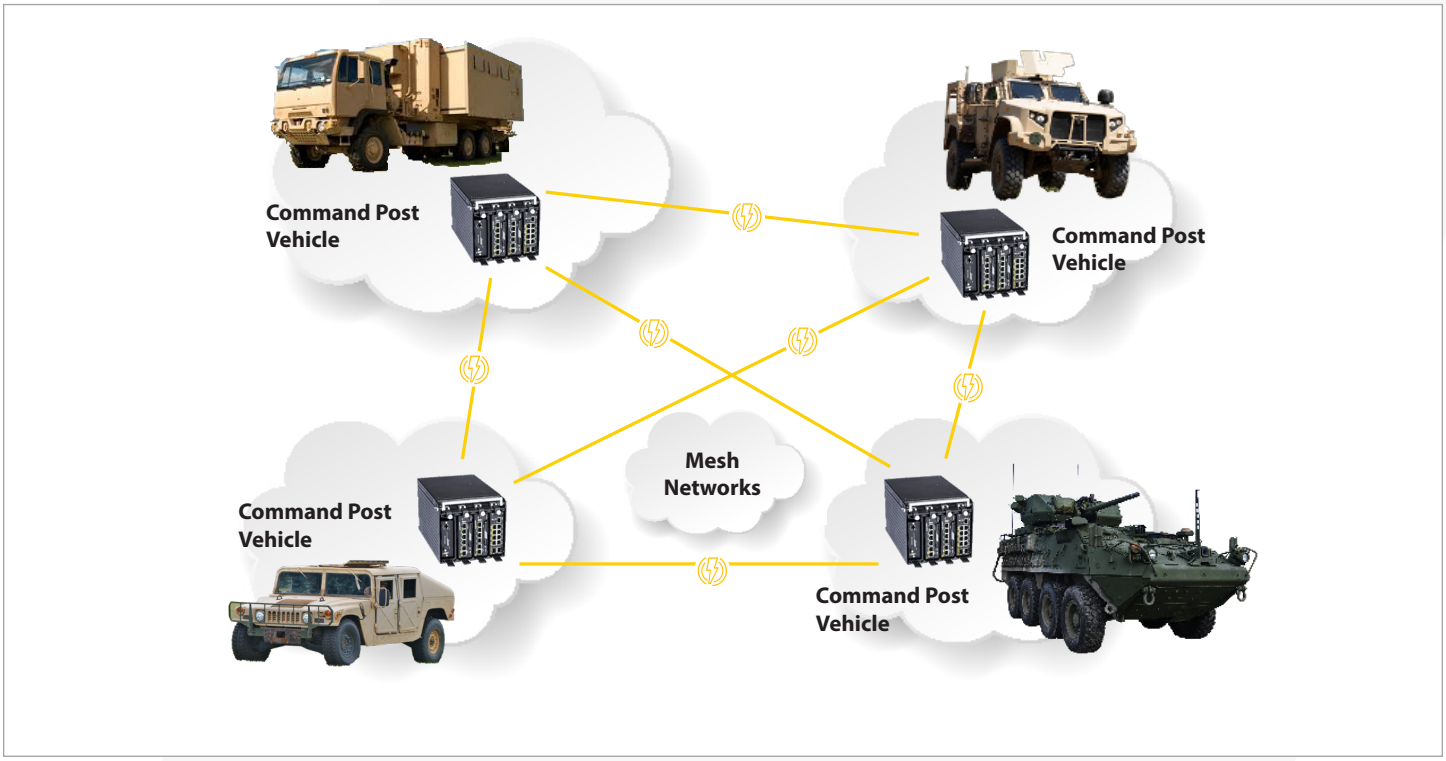


Figure 1: PacStar SMCP Solution Architecture

Solutions Architecture

A complete modern architecture for mobile command posts includes PacStar SMCP mounted on Command Post Support Vehicles and PacStar SMCP on mission command platforms. PacStar SMCP provides Central Site encryption, PKI and management services for the entire fleet of connected vehicles.

On Mission Command Platforms, for V2V communications, PacStar SMCP uses layered IPsec VPN gateways over meshing radio, enabling the transport of one or more classified and/or unclassified networks between themselves and the Command Post Support Vehicle.

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, (COTS) technologies that fit within limited spaces and provide wireless network access inside vehicle shelters and between vehicles.

The U.S. armed forces have also called for more robust secure network solution that improve command post survivability and more optimized network traffic. To meet those objectives, network architectures are moving away from hub and spoke to state-of-the-art meshing solutions.

***Common criteria and FIPS evaluated technologies on select PacStar 451 models**

Specifications

PacStar SMCP Contents

PacStar SMCP 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 – as a “Remote Centrally Managed Site.”

PacStar 451
Rugged Server with Aruba EdgeConnect or Viasat NetAgility

PacStar 451
Rugged Server with Cisco C8000v

PacStar 451
Rugged Server with Palo Alto VM

PacStar 444 Switch with Cisco ESS 3300

Network Infrastructure/Encryption

- Outer VPN Gateway (Aruba EdgeConnect or Viasat NetAgility)
- Traffc Filtering Firewall/IDS (Palo Alto VM)
- Management (IQ-Core Crypto Manager)
- Network Services (Domain Services, NTP) (Optional)
- Inner VPN Gateway (CiscoCAT8000v)

Network Access

- LAN Access
- One or more PacStar 444/446/448 Ethernet switches for wired access

One Network Configuration

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

1. Outer IPsec VPN Gateway (Aruba EdgeConnect or Viasat NetAgility on PacStar 451)
2. Inner IPsec VPN Gateway (Cisco CAT8000v on PacStar 451)
3. User Access Switch (Cisco ESS 3030 in PacStar 444)

Two Network Configuration

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

1. Outer IPsec VPN Gateway (Aruba EdgeConnect or Viasat NetAgility on PacStar 451)
2. Inner IPsec VPN Gateway (Cisco CAT8000v on PacStar 451)
3. User Access Switch (Cisco ESS 3030 in PacStar 444)
4. Gray Traffic Filtering Firewall (Palo Alto VM on PacStar 451)
5. Inner IPsec VPN Gateway (Cisco CAT8000v on PacStar 451)
6. User access switch (Cisco ESS 3300 in PacStar 444)