Going Virtual for the Digital Transformation of Defense

The military is facing readiness obstacles like never before. The rapidly evolving nature of warfare poses challenges to the services' ability to provide the capabilities needed to execute their missions in a new era of defense. Integrating more virtual and constructive training offers a cost effective solution to address these challenges as defense dives deeper into their digital transformation.

IMPROVED READINESS AT REDUCED COST WITH CISCO TECHNOLOGIES

COMPUTING

Simplified, stateless servers that are centrally provisioned, configured and managed delivers a unified system that allows systems to be deployed or reconfigured in minutes, rather than hours or days. Provides optimal agility to support many simulations of training scenarios.

EDGE COMPUTING

Servers designed to be embedded in routers can provide virtualization-ready and application-centric network, compute and storage capacity for high-performance application hosting.

OPTICAL NETWORKING

Provides high-rate data connectivity over long distances.

WIRELESS

Wireless networks may be used to enable mobility across training sites, but expect heavy demand during training exercises, due to lots of devices moving in and out of a network. Wireless access points can overcome this challenge and provide the required mobility to optimize training benefit.

COLLABORATION

IP based collaboration and conferencing optimizes the ability of remotely located personnel to collaborate and prepare for training events, and to later debrief and share lessons learned while minimizing the expense of remote collaboration.

Cybersecurity: Network as a **Sensor and Enforcer**

LVC requires everything to be connected to everything else, and involves a tremendous amount of data. Protecting that data is best done with the network itself acting as a security sensor and enforcer.

The network as a sensor can:

- **Enforce segmentation policies** to make the attack surface smaller.
- **Limit lateral damage** by preventing malware from spreading across the network.
- Enable switches, routers and wireless solutions to work together to **identify and defeat malicious activity**.
- **Baseline normal behavior and sense deviations**, enforcing security policies accordingly.
- Use **identity services** for enforcement of role-based, topology-independent and access-independent control.

Discover more about Cisco at cisco.com/go/federal.