Secure Network Infrastructure Solutions for Federal Agencies

CommScope Secure Infrastructure

Federal networks have become increasingly complex, consisting of a multitude of wired and wireless connections. As these networks evolve the physical layer is becoming a more attractive target for attack – from unsophisticated hackers to technically competent intruders to nation-state adversaries. These malicious attacks are designed to steal information and disrupt mission-critical activities. In fact, for classified networks, the U.S. government provides guidance for three specific design, installation, and maintenance requirements to secure structured cabling systems. These include Protected Distribution Systems (PDS), physical separation, and port-to-port isolation.

Although government requirements lay out these three options there are benefits and drawbacks to each as highlighted below:

1) PDS: Securing pathways

- Hardened carrier - epoxied or welded metal conduit or ducting
- Alarmed carrier – single-mode and multimode Interlocking armored fiber cable utilized with alarm sensor technology to monitor for tampering or access

2) Physical separation / isolation port-to-port and wireline

- Each network is physically separated in its own conduit
- Simple idea with complex deployment issues
- Very expensive to deploy and maintain
- High space consumption

3) Port-to-port isolation – providing interface diversity and colored/keyed networks: Securing points of network interface

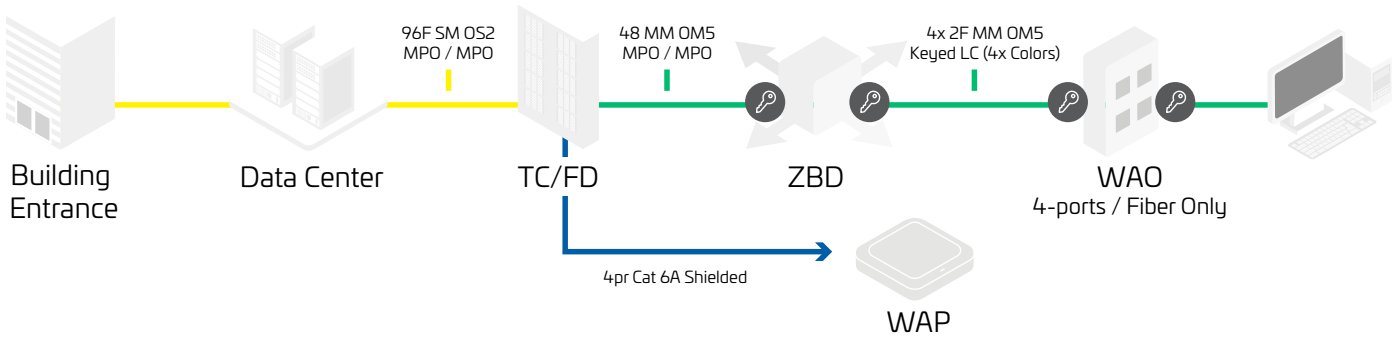
- Use of mutually exclusive jacks and connectors to prevent cross-connection
- Separate, dedicated distribution frames and patch panels
- Color designation for network identification from data center to desktop
- Precludes inadvertent cross-connects
- Reduces need for separate, dedicated distribution frames and patch panels
- Less expensive
- Less space consumption
- Non-keyed solutions available for locked/secured rooms
- Keyed solutions for exposed connectivity

CommScope offers solutions to meet all three of these requirements but recommends that agencies consider adopting both the secure pathway and secure port-to-port isolation approach. Our comprehensive critical infrastructure solutions are geared towards the installation of secure networks supporting wired and wireless applications, from the fiber ring around a campus to the desktop. Our full portfolio of fiber and copper connectivity options offer unparalleled "Best in Class" solutions for classified and unclassified network environments.

Multiple Physical Layer Fiber & Copper Security Solutions

- Keyed Connectors & Adapters
- Secure Port Blockers
- Locking Patch Cords
- Color-Coded Fiber Connectivity
- Interlocking Armored Fiber
- Shielded Copper Cabling

Sample deployment of secure network infrastructure solution



Building Entrance: Fiber Entrance Cabinet

- Splice point – splicing carrier's outside plant fiber and campus cable to inside plant fiber
- OSP cable is broken down to smaller inside plant cable counts
- Connects the demarcation to the main cross connect for the facility

Data Center: Non-Keyed

- In the data center, secure networks can be segregated into separate network enclaves with designated colors
- In this design, this is the first area where networks will be differentiated
- Note: In this design, keyed connectivity is not required here as this part of the network is protected by multiple layers of security which limits access to the room location

Telecom Closet/Floor Distribution Room: Unkeyed to Unkeyed

- Conversion from single-mode to multimode
- These solutions are color-coded to designate a specific network
- In this design termination locations are in secured rooms. Therefore, these solutions do not have to be keyed , may require panel to panel separation

Wi-Fi access point cabling: In ceiling

- 4pr Category 6A shielded cable is the chosen design to support the Wi-Fi access point protocols or other IoT devices

Zone Distribution Floor Box (ZDB): Unkeyed Multi-fiber Push On (MPO) to Keyed/Colored LC Connector Module interfaces

- ZDB can be mounted under the floor and connected to the TC/FD via 48F multimode OM5 MPO/MPO trunk cables (colored jacket on fiber trunks)
- MPO trunks will land on 24-fiber keyed modules, two for each of the four (4x) network colors
- Keyed modules provide the needed port-to-port isolation for secure network connection placed in close proximity

Work Area Outlet

- WAO can be connected to a ZDB via 4x 2F (colored & keyed) duplex LC assemblies. Keyed modules provide the needed port-to-port isolation for secure network connection placed in close proximity
- 4,000 desk tops deploying as many as 48,000 fiber connections at the desk level
- There is no copper at the WAOs in this design. If there is a requirement for copper connectivity, such as a NIPRNet (Non-classified Internet Protocol (IP) Router Network) VoIP circuit at the desk, CommScope offers a full portfolio of shielded cable and connectivity solution

COMMSCOPE®

commscope.com/federal

Visit our website or contact federalsales@commscope.com for more information.

CO-115274-EN (12/20)