

BICSInews

july/august 2013 | volume 34, number 4

M A G A Z I N E

UPDATING TECHNOLOGY

Preserving Character for
Big Brothers Big Sisters

PLUS

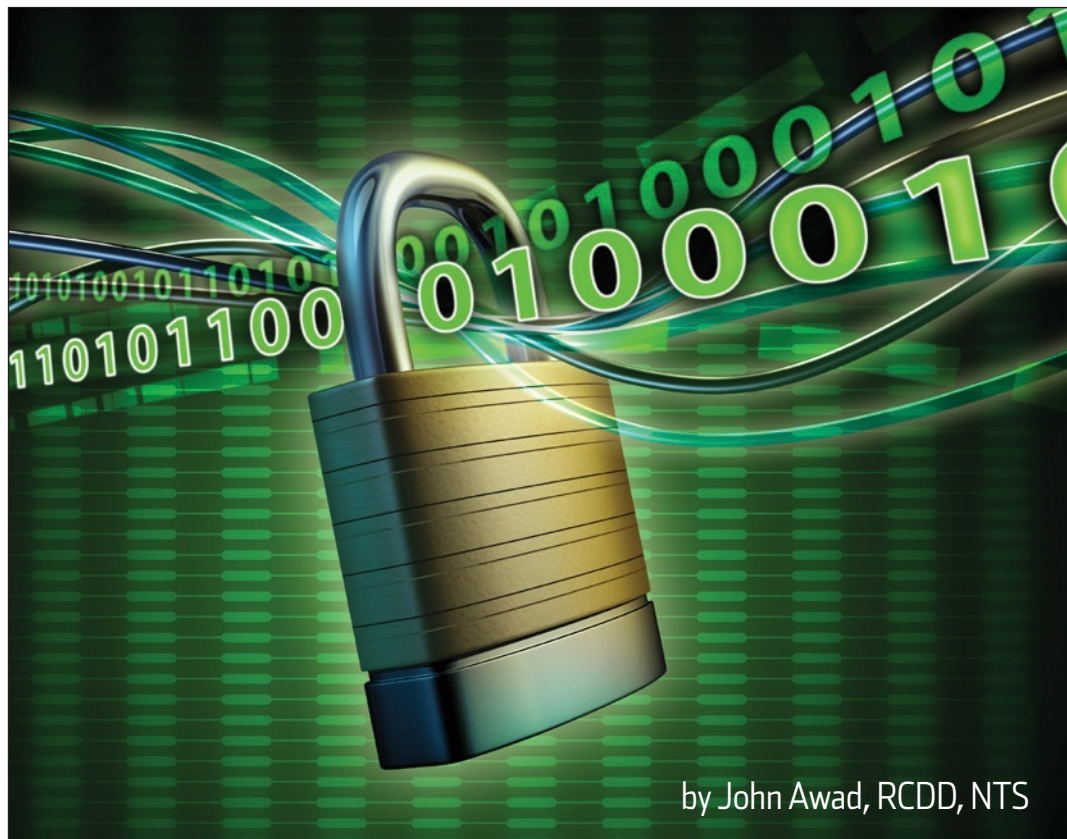
- + The Rise of Plug-and-Play
- + Looking Down the Channel
- + Thinking Outside the Box

Bicsi[®]

Originally designed and specified for high security military installations, keyed LC systems are now readily available and encouraged for commercial use.



John Awad, RCDD, NTS, is a technical sales specialist with Optical Cable Corporation, a manufacturer of data communications cable and connectivity solutions. He can be reached at john.awad@occfiber.com.



by John Awad, RCDD, NTS

PROTECTING THE NETWORK INFRASTRUCTURE

Five Modes of Security You Might Not Have Considered

We all know about the need for security on an enterprise network. Virus scanning software automatically screens email attachments. Firewalls prevent unauthorized network access to our computers. Login screens and passwords prevent unauthorized access to our many online accounts. Encryption ensures that private information transmitted on the Internet stays private.

What about physical security that controls access to a network infrastructure? Have you thought about what you need to keep the actual components of your infrastructure secure?

There are many applications and situations that call for separating or designating who can access a particular section of the physical infrastructure and where they can gain that access.

Following are some application examples where specialty connectivity can be deployed to control and enable who accesses the physical network.

1.

NETWORK DESIGNATION

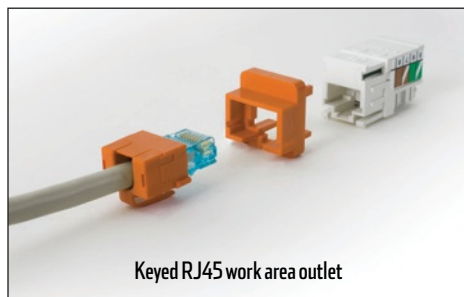
Let us assume you are the onsite service contract provider for an aerospace company or government facility that requires secret clearance for their network. By contract stipulation, your service level agreement (SLA) states that you will incur a significant fine if unauthorized users obtain physical access to the network; for example, by way of a standard copper patch cord plugged into a work area outlet in a public space. These public area outlets include conference and meeting rooms, waiting rooms, lobbies or other supervised or unsupervised areas. At these locations, the use of a matching security keyed RJ45 work area outlet and matching patch cord offers physical security.

Connectivity for limiting access uses an RJ45 footprint with performance to category 6A and backwards compatibility, while blocking standard RJ45 plugs that are not 'keyed' correctly. Several different colors should be available, with a different key corresponding to each color. This solution is appropriate any time you need to control who is accessing an open outlet but still want certain authorized individuals or equipment to have immediate access. Keyed and color coded equipment cables are often assigned for use to specific individuals or departments, allowing authorized access as needed.

2.

NETWORK SEGMENTATION

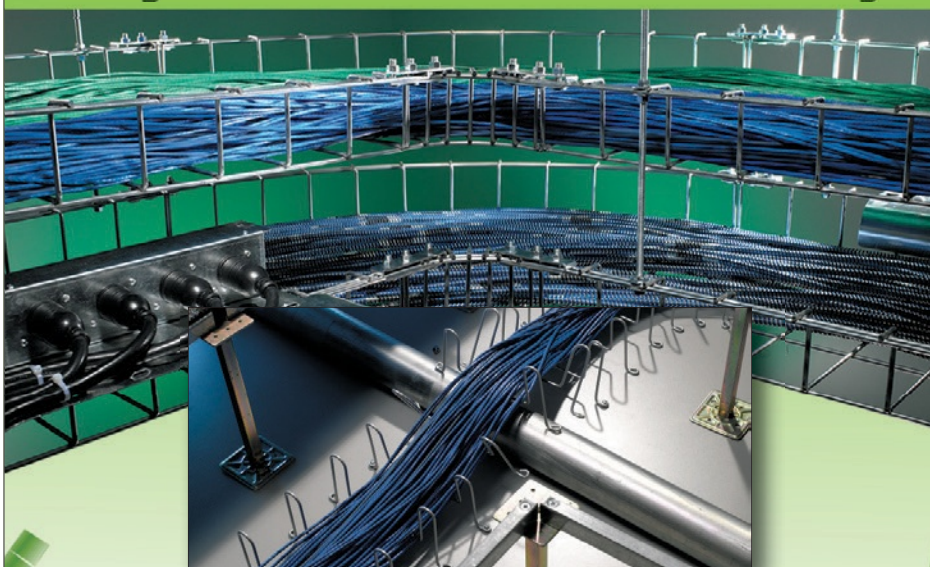
Today's equipment rooms (ERs) contain connections for a variety of different services. A single structured cabling rack or ER might contain patch panel connections for a category 6 data network, category 5e voice network, category 6 TV network, a power over Ethernet (PoE) security camera system, an access control system, core network cross-connect patch panel fields



Keyed RJ45 work area outlet

and a separate 10 gigabit per second (Gb/s) category 6A data network for high-bandwidth service. In addition, specialized facilities like hospitals and laboratories often contain connections for electronic

Snake Tray® and Mega Snake® Cut your costs not the cable tray!



Cable tray installations are seldom a straight run. Obstacles in buildings are everywhere. Fabricating wire mesh cable trays onsite is extremely time consuming and costly. Snake Tray simply bends by hand and Mega Snake is pre-configured. Both are designed to save on time, labor and materials!

Snake Tray® products are patent protected, see our website for specific patent information.



800.308.6788 ♦ www.snaketray.com ♦ Made in the USA

chart systems, patient monitoring systems, overhead paging systems, background music systems and specialized AV systems.

Different technicians or service providers are often assigned to each system, and many of these systems all have the same RJ45 footprint. Rack-mounted 24- or 48-port panels that allow you to install jacks and patch cables for limiting access are ideal for these scenarios. They allow you to assign different colors and keys to individuals or systems in the cross-connect area or ER without fear that different groups will have access to unauthorized infrastructures or systems. Security keyed and color-coded end-to-end solutions put an extra level of security and separation into each service at this juncture of the network.

3.

LIMITING UNAUTHORIZED ACCESS TO OPTICAL FIBER PORTS

ERs with active optical fiber ports for multiple services are a security risk waiting to happen. It is becoming more important

to quarantine individual active networks that are in close physical proximity to each other while still allowing authorized technicians to perform moves, adds and changes (MACs). A keyed LC optical fiber solution can limit technician access to only the networks on which they are authorized to work.

Individual keyed and color-coded end-to-end solutions can be assigned to different entities by color, allowing two separate levels of security. Keyed LC adapters prevent improper connection of separate networks in common access areas. Small form factor LC connectors allow higher density with the same proven performance of the LC ferrule. Originally designed and specified for high security military installations, keyed LC systems are now readily available and encouraged for

commercial use. These solutions can be an asset for projects needing extra security in the switch room or common cross-connect areas.

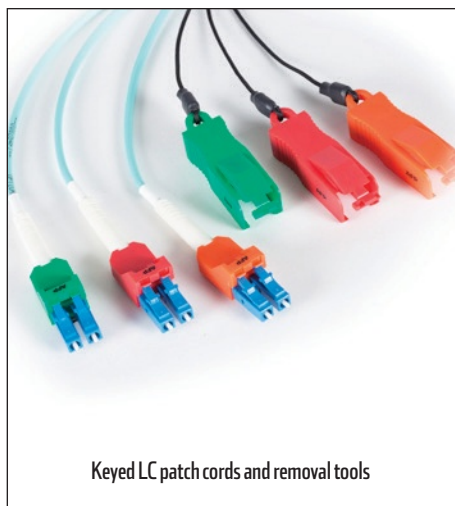
4.

PREVENTING ACCIDENTAL DISCONNECT

Accidentally unplugging the wrong optical fiber jumper can disconnect hundreds of users or take down a network altogether, causing lost production time, lost data and increased latency. Secure LC optical fiber connectors are designed to provide an extra layer of security to network ports through a lock-and-key style mechanism. The patch cords require a special extraction tool to help prevent unauthorized disconnection from active ports.



Small and large capacity deployable reel systems for emergency services applications and disaster recovery



Keyed LC patch cords and removal tools



To immediately create a new circuit in a disaster recovery situation, panel mount receptacles with dust caps can be connected to active equipment via standard SC, ST or LC optical fiber interfaces on one end and connected to a deployment reel on the other end.



When combined with panel mount receptacles, these multichannel connectors for various capacities and applications can be used to bypass damaged cable between racks, rooms or buildings.

The added level of protection provided by secure LC patch cords can be highly useful in securing high end SLAs. The secure connections are ideal for military, government and other sensitive installation environments, as well as for any data centers or ERs

that require additional security against tampering with active ports. They are available in a variety of color options that include extraction tools, port plugs and optical fiber shelf adapters. The patch cable connectors install easily in any industry-standard LC fiber adapter

and can be combined with bend insensitive cables for high performance, high-density installations. Secure LC solutions are also readily available in both multimode and singlemode optical fiber to meet a variety of environments and application needs.



Axis Communications' Academy
Designed with your success in mind

All aspects of Axis Communications' Academy are available to help you certify your future success. The certification program is aimed toward system designers and the relevant knowledge is covered within a variety of learning opportunities from classroom training to online courses and tutorials.

Going beyond the classroom, the Academy provides a wealth of knowledge to help you serve your customers and attract more business — from interactive system design tools and practical "how-to" guides to specialized webinars and certification.

Discover new ways to drive more business to your door with Axis Communications' Academy by taking advantage of these various educational offerings and becoming an Axis Certified Professional.

Axis Communications' Academy - the global learning center for network video.

Showcase your expertise.
Visit www.axis.com/bicsi

Read more with
your smartphone



Bicsi
CONTINUING EDUCATION
CREDIT PROVIDER

AXIS
COMMUNICATIONS

5.

DISASTER RECOVERY PLAN

To prepare for potential server failures, best practices include ongoing and redundant incremental data backups to offsite locations. In addition, continuous firewall protection and virus scanning protects against unauthorized incoming network intrusions. While electronic access control protects data centers and ERs from unauthorized entry, emergency disaster recovery of the Physical layer in the event of a natural or man-made disaster should also be considered.

If a large portion of your network infrastructure is damaged or destroyed, you may be able to bypass the damaged section and get

your network up and running again quickly. Multi-channel deployable systems are an emergency management tool that can help you be prepared for immediate recovery from disasters. Originally made for military battlefield use, these systems have exploded in popularity for broadcast, stadium, education and emergency services applications. While the deployable connectors feature a design consistent with outdoor field use, they are available with a variety of interfaces to match your existing network equipment.


With this solution, interfaces are mounted in rack-mount panels in a standby mode for immediate activation in the event of a facility emergency. A single person can easily handle 100 to 1000 meter (m [328 to 3281 feet (ft)]) deployment reels. This allows for quickly and easily bypassing a damaged optical

fiber backbone cable, ER or building to get the network back up and running in as little time as possible. The ruggedness and flexibility of these systems allows them to be left in place for as long as the situation warrants. When they are no longer needed, the cables are reeled back up and stored.

When an emergency happens, quick communication is essential. The ability to rebuild and maintain communications at an emergency site is crucial to recovery. Having rapidly deployable equipment options at your disposal assists in maintaining communications and information at command posts and designated "go-to" areas in the event of emergency or disaster. There is less liability exposure for the forward-thinking organization that allocates a small percentage of its technology budget for the management of data and communications in the event of such an emergency or disaster.

SECURING THE INFRASTRUCTURE MATTERS

Today, fast access to information is always necessary. Securing information enables optimum productivity of staff and users. Proper security planning for the network infrastructure can allow personnel to release control to the physical security systems, creating less stress and freeing up time for personnel to participate in other meaningful endeavors. Emergency management and disaster recovery planning are mandatory for facility management, but communications infrastructure is often an afterthought. Information system professionals should take the initiative to secure a budget for solutions that physically protect the infrastructure. ■



**METZ
CONNECT**
We realize ideas


P | Cabling

The Cat 6A Cable Connector

Don't waste good cable!

New Ethernet drops are no longer necessary to lengthen or repair an existing cable. Our Cable Connector will have you up and running quickly. Its rugged metal housing, easy termination, and color-coded terminals make it the ideal solution for nearly every application.

Find out more at metz-connect.com



www.metz-connect.com | ph 888-722-5625

Members of METZ CONNECT

