



# Intelligent Infrastructure & Security

Using an Internet Protocol Architecture for Security Applications

July 2009

## Contents

I. INTELLIGENT BUILDING INFRASTRUCTURE SOLUTIONS	2
<b>Low Voltage Systems in Commercial Buildings</b>	2
<b>Convergence onto the Internet Protocol Architecture</b>	2
<b>Structured Cabling Solutions for IP-Based Physical Security</b>	2
II. CONVERGENCE	2
<b>The Demand for Intelligence</b>	2
<b>The Convergence Trend</b>	2
<b>Intelligent Infrastructure Solutions</b>	2
III. DEFENSE IN DEPTH	3
<b>Susceptibility to Failure</b>	3
<b>Critical Path Identification</b>	3
<b>Vulnerability to Security Breaches</b>	4
<b>Asset Management</b>	5
IV. SUMMARY: PUTTING THE INTELLIGENCE INTO THE BUILDING INFRASTRUCTURE	5
V. RELATED LINKS	5

The information contained in this document represents the current views of CommScope, Inc. of North Carolina ("CommScope") on the issues discussed as of the date of publication. Because CommScope must respond to changing market conditions, it should not be interpreted to be a commitment on the part of CommScope to offer the services presented, and CommScope cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. COMMSCOPE MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of CommScope, Inc. of North Carolina.

CommScope may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from CommScope, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Copyright © 2009 CommScope, Inc. of North Carolina. All rights reserved.

CommScope, iPatch, and SYSTIMAX are either registered trademarks or trademarks of CommScope, Inc. of North Carolina in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

## I. Intelligent Building Infrastructure Solutions

### Low Voltage Systems in Commercial Buildings

In a typical large commercial building, more than a dozen different low voltage systems are used to control various aspects of the building's operation. In legacy applications, each of these might use different wiring types and controllers, and few of them interact with one another.

### Convergence onto the Internet Protocol Architecture

Continued acceleration of the adoption of Internet Protocol (IP) as the primary architecture for communications has led to the convergence of traditional voice, video and data networks in the enterprise. Now, additional low voltage systems are beginning to trade in their proprietary wiring and communications systems for IP-based technologies.

### Structured Cabling Solutions for IP-Based Physical Security

Convergence onto IP-based technologies allows for a single design, installation and maintenance methodology for low-voltage communications requirements. In order to continue to further realize the benefits of convergence at the network layer, these systems should also be deployed using structured cabling design principles. Standards such as TIA/EIA-862 define how to do so for intelligent buildings.



## II. Convergence

### The Demand for Intelligence

In the world of network infrastructure, nothing stands still. Convergence to the Internet Protocol is a reality. Gone are the days of separate voice and data networks. Video and other content-rich traffic will also share the same infrastructure, as will intelligent building control devices. Physical security devices in particular are moving onto IP networks.

Your network is now truly the fourth utility. It must work 24 hours a day, seven days a week, whether anyone is in the office or not. Maintenance windows are shorter than ever before, so any change to the network must be made quickly and accurately – it must be right the first time, every time.

Consolidation drives the need for quick, accurate changes along with more effective planning tools. As more mission-critical applications are deployed onto a converged IP network, reliability, availability and security become paramount.

### The Convergence Trend

Convergence eases the strain of managing multiple systems and a complex network. Bringing video, data, voice, wireless, factory controls, building controls, and physical security devices into one IP network will continue into the foreseeable future.

Convergence brings with it a host of opportunities. Once building systems are linked, operations can be taken to a new level of efficiency. Maintenance becomes simpler and productivity can be greatly improved. With real-time reports and monitoring, convergence makes record keeping and decision making more manageable.

However, convergence also has its challenges. When you bring systems together, you want to retain a comfortable level of robustness, reliability and manageability. Bandwidth and security demands have to be met. How can you ensure that bringing your systems into one IP network will succeed?

The trend is toward convergence. The demand is for intelligence. You need a solution that can provide both while also overcoming the challenges and easing the demands on your time and resources.



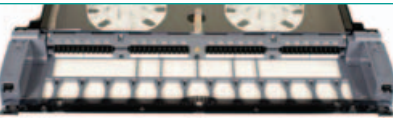
SYSTIMAX 360 iPatch Panel Manager



SYSTIMAX 360 iPatch Network Manager



SYSTIMAX 360 iPatch 1100GS3  
48 Port Panel



SYSTIMAX 360 iPatch G2 Fiber Shelf



SYSTIMAX 360 iPatch G2 High Density  
Fiber Shelf

### Intelligent Infrastructure Solutions

By adding intelligence to copper and fiber structured cabling systems, Intelligent Infrastructure Solutions automate change management, improve productivity, increase network reliability and availability, track the physical location of networked devices, secure the network and facilitate compliance.

Bringing together software and hardware, Intelligent Infrastructure Solutions provide a real-time, comprehensive view of the physical network, automatically detecting moves, adds and changes and providing a dashboard that gives the vision and knowledge necessary to control the network.

An Intelligent Infrastructure Solution is composed of the following types of products:

- Intelligent Patch Panels: Standard copper and fiber optic patch panels that detect changes in the physical layer, initiate tracing of circuits, and guide technicians on required connection changes. Ideally, they should be able to utilize standard copper and fiber optic patch cords.
- Infrastructure Control Systems: Rack or panel-mounted displays that act as the local user interface for the system. Technicians can use these devices to determine what electronic work orders are outstanding, trace circuits end-to-end to identify the endpoints and services being provided and determine if there are any alarms related to the physical layer, such as unplanned changes or critical circuit disconnections.
- Infrastructure Control Software: A centralized database and user interface that is used to document, monitor and manage the physical layer. By communicating with network devices, the software can determine how the logical network maps to the physical layer, select optimal locations for new devices, and ensure connectivity is in place prior to enabling a switch port.

CommScope offers a full line of intelligent infrastructure solutions under the iPatch brand name as part of the next-generation SYSTIMAX 360 solutions platform.

### III. Defense in Depth

#### Susceptibility to Failure

While it is more cost-effective to combine all of these traffic types, to do so demands utility-level service from the network. When voice traffic was first delivered over IP networks, it worked fine for small deployments. As deployments grew larger, excessive demand for bandwidth degraded voice over IP (VoIP) services, leading IT professionals to deploy parallel IP networks dedicated to voice traffic. While this solved much of the congestion problem, it eliminated some of the benefits of having a converged network in the first place.

Eventually, quality of service (QoS) architectures were introduced by IP network equipment vendors, allowing voice traffic to be prioritized above data traffic in order to guarantee the proper operation of enterprise VoIP systems. Proper network design is essential as additional traffic types are introduced, each with its own bandwidth requirements, latency sensitivity and delivery reliability requirements.

But what about more basic susceptibility? If a critical device is inadvertently unplugged from the network, it must be reconnected immediately, or serious consequences could ensue. With an intelligent infrastructure solution from CommScope, the physical layer is enabled with technology to identify the unexpected change and instruct technicians on remediation procedures.

#### Critical Path Identification

Identifying critical assets and their location in the network is essential. Most network management systems available today only deal with logical connections – for example, to which port on a particular switch or router an endpoint is connected. If the connection is broken, the only indication that IT personnel will get is a link down notification. In many cases, the severity of that notification may not be properly communicated – after all, many switch ports generate multiple link up / link down notifications daily, as a normal matter of course.

Even where additional intelligence has been added to the network management system to indicate that a particular switch port should never be down, the operator will only receive partial information about the failure. While it is important to know that a problem has occurred, without physical layer details, troubleshooting the issue can take a significant amount of time.

What was the source of the failure? It could be one of several things:

- The endpoint device lost power or otherwise failed.
- The circuit was disconnected at the endpoint device.
- The circuit was disconnected at the switch.
- The switch lost power or otherwise failed.
- A patch cord in the circuit path was disconnected.
- The cable was damaged between the switch port and the endpoint device.

With an intelligent infrastructure, additional information is available to facilitate end-to-end troubleshooting and return the device to service more quickly. Changes to patch cord connections are automatically detected by intelligent patch panels. For critical circuits, alarms may be sent to operators and technicians in a variety of ways, including email, text messages, SNMP alerts and on the user interface of the infrastructure control software.

At the infrastructure control system in a rack or on a panel, the local display will also indicate visual and audible alarms. In the case where a technician is onsite and inadvertently removed a patch cord, s/he would get immediate feedback that a critical circuit was disconnected and instructions for restoring the connections would be made available.

### Vulnerability to Security Breaches

Today's networks require both perimeter and interior security to prevent security threats from impeding network performance. Preventing denial of service attacks, unauthorized access and other security breaches becomes even more important when the network is used for control of critical building infrastructure. Deploying security networking equipment, including firewalls, network and host intrusion and detection systems and virtual private network concentrators will protect most enterprises against external and internal threats. Utilizing virtual local area network (VLAN) technologies helps isolate traffic internally.

However, identifying logical threats may still require physical location information to properly respond to security breaches. For example, if an employee, contractor or guest accesses the network with a laptop that is infected with a virus, the network can defend itself by shutting down the port to which the laptop is connected or isolating it to a remediation VLAN. But if the user doesn't realize the network is protecting itself, s/he might move from available port to available port looking for one that "works". With an intelligent infrastructure solution in place, security operations can be informed not only that an infected device has been connected to the network, but given its exact physical location as well.

Similarly, unplanned physical layer changes can be identified. Ports that are not defined for use can be shut down until the proper cabling is in place. An intelligent infrastructure solution can be used to ensure that only the expected type of device is attached to the network.

For example, one issue that security operations personnel have been concerned with has been the use of IP-based network cameras on the exterior of a building. They reasoned that an intruder could easily disconnect the camera and plug in a laptop, gaining access to the internal network while simultaneously defeating the security offered by the camera.

With an intelligent infrastructure solution in place, the security operations personnel could receive an alert via email, SMS text message or on the user interface that includes information such as the type of camera, its physical location and even its coverage area. Additional integrations could also exactly identify where the disconnection happened (at the switch port, a patch panel, in the cabling, or as in this instance, at the network camera), when it happened, and call up the last few minutes worth of video from the affected camera. Video analytics can also be used to further extend the robustness and breadth of this solution.

If an unauthorized device type is connected to the switch port, the intelligent infrastructure solution can take a more active role, shutting down that port. Once the security breach is resolved and the network camera is reconnected, the switch port can be re-enabled.

### Asset Management

Having total knowledge of what – and who – is connected to your network is vital. Tracking assets as they move through your enterprise helps you remain in control of your network. By maintaining an inventory of the switches that provide specific services along with an up to date physical connectivity map, an intelligent infrastructure solution can help in the planning for deployment of new devices for critical applications.

For physical security devices, care must be taken to ensure that the proper type of device is installed and connected to the correct VLAN. Based on the chosen endpoint location, an intelligent infrastructure solution can immediately determine whether there is a switch with a port available that is (or can be) configured with the security VLAN, and what patch cords are required to complete the end-to-end circuit. It will provide technicians with electronic work orders, guiding them to make the appropriate patches required to fully deploy the new device. Once the cabling is in place, the intelligent infrastructure solution can enable the selected switch port. Further integrations with access control or other systems are possible that would limit the visibility of these electronic work orders to specific technicians, ensuring that only authorized personnel make changes.

At the other end of the asset management spectrum, an intelligent infrastructure solution helps with annual equipment audits. By tracking connectivity through the enterprise, assets can be identified not only as being connected, but also to the physical location where they currently reside, their current capacity and available ports for specific services, and so on.

## IV. Summary: Putting the Intelligence into the Building Infrastructure

CommScope can help you add intelligence into the building infrastructure. Whether you're deploying low-voltage systems onto an IP-based architecture with standard structured cabling systems, or fielding a fully integrated Intelligent Building Infrastructure Solution, we have design teams and a wide array of SYSTIMAX BusinessPartners ready to help you now. Let us show you how an Intelligent Building Infrastructure Solution can be less expensive to install and operate, providing you with integrated solutions that give you the vision and knowledge you need to control your network.

## V. Related Links

See the following resources for further information:

- CommScope, Inc. of North Carolina home page [www.commscope.com](http://www.commscope.com)
- CommScope Intelligent Building Infrastructure Solutions (IBIS) home page <http://www.commscope.com/systimax/eng/solutions/enterprise/bas/index.html>
- CommScope SYSTIMAX iPatch Intelligent Infrastructure Solutions [http://www.commscope.com/systimax/eng/product/cabling\\_solutions/patching/1173216\\_9477.html](http://www.commscope.com/systimax/eng/product/cabling_solutions/patching/1173216_9477.html)



© 2009 CommScope, Inc. All rights reserved.

Visit our Web site at [www.commscope.com](http://www.commscope.com) or contact your local CommScope representative or BusinessPartner for more information. All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of CommScope.

This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to SYSTIMAX products or services.

08/09