



WHITE PAPER SERIES

2355 Mira Mar Avenue
Long Beach, CA 90815-1755
562-986-9105
www.mercury-security.com

The Myth of Access at the *Edge*

What's really happening in IP-based access control

Introduction

While Internet Protocol (IP)-based access control is not a new concept, recent advancements in IP technology have introduced exciting new options for both the installation and implementation of access control systems. The current direction in the security industry is a convergence of IT and security networks and deploying access control devices at “the edge” of centralized systems.

The purpose of an access control system is to protect people and assets, as well as to control and record movement of those people and any alarms or events that occur. Access control systems must perform these tasks reliably, predictably and in a timely manner. The implementation of these systems must minimize vulnerability to achieve the highest level of reliability and performance.

The objective of this paper is to examine the recent advances in IP-based access control systems and separate the myths surrounding these advancements from the realities of reliably deploying networked access control.

Edge STPs (signal transfer points)

Are networking hardware devices embedded with software that performs routing, signaling, firewall and packet conversion functions. Their primary purpose is to unify networks that use various transports and signaling protocols – such as SSP, SIP, SIGTRAN, IP, TDM, etc. – into cohesive service environments.

Wikipedia

What is the Edge?

No discussion can occur without a mutual understanding of terminology. To better understand the term, *the edge*, a look at how the computer industry defines the term is helpful.

In computing, *the edge* involves pushing data and computing power away from a centralized point to the logical extremes of a network.¹ In security systems, this translates into pushing computing power toward and managing data at the logical extremes of a **security network**. The logical edge of a computer network is typically defined as the deployment outside the wiring closet or datacenter. In access control, that definition also holds true, as more intelligent devices are being installed nearer the door.

Wikipedia defines **Edge STPs** (signal transfer points) as networking hardware devices embedded with software that performs routing, signaling, firewall and packet conversion functions. Their primary purpose is to unify networks that use various transports and

¹ ServerWatch eNewsletter 12/2002

signaling protocols – such as SSP, SIP, SIGTRAN, IP, TDM, etc. – into cohesive service environments.

From that definition we can derive the following definition of *the edge* with respect access control: **Edge Access Control Points (ACP)** are **networked** hardware devices embedded with software that performs **routing, signaling and packet conversion functions**. Their primary purpose is to manage, record and report access and device activities for the creation of a **cohesive security environment**.

As access control systems move toward the network edge, security system experts must understand the strengths and limitations – the myths and misconceptions – of such network-based systems and devices. Armed with this understanding, security system specifiers can devise reliable access control strategies that account for the unique requirements and available resources within each installation environment.

Today's Top Myths

There are three prevalent myths regarding deploying access control devices at the edge of the security network. The first myth is that network resources are readily available for access control to just “plug right in” for its communications requirements. The second prevailing myth is that the total cost of ownership is less with network-connected devices, from the installation to the ongoing maintenance. And the final prevailing myth it is that security and It manager speak the same language. In short, one manager’s “scheduled maintenance” may be another manager’s unscheduled service call.

Myth #1: Network Resources are Readily Available

In today's world, every business has a network. The networks range in size from a couple of computers sharing printers and file servers to major corporate networks that provide the infrastructure for the company to do business on a global basis. Generally, every network has a network or IT manager. Depending on the size of the company, this could be a tech-savvy employee or the head of a large IT department.

Given the prevalence of such network resources, the security integrator often assumes he will have no problem getting 1 to 20 network ports assigned for his use. If the network devices can be powered by Power over Ethernet (PoE), then the installer assumes he has the added benefit of not having to run power to the device. And, because network switches are mission critical hardware, they typically have their own emergency power backup.

Reality #1: Availability of Network Resources

While it is true that one or two network ports might be available for the security system, many IT departments do not usually have a large number of unused/unassigned ports available solely for the use of securing the building. Moreover, even if adequate network ports are available, there may still be issues that prevent the integrator from successfully using this “free” resource:

- **The available network ports are not guaranteed to be geographically located near the doors that are to be secured.** If the distance from the door to the network port is greater than 300 feet, the installer must coordinate with the IT department to install an additional switch in the middle to span the distance, or purchase and install the switch himself.
- **Not all switches support PoE.** If the switch does support PoE, the power output on PoE may not be adequate for some locking mechanisms. Installers will have to be certain that the additional power draw with the access hardware can be covered by the existing back-up power provided to the network by IT.
- **Switches in the same building, even in the same network closet, are not all guaranteed to be part of the same logical network.** Sophisticated IT departments may have divided the corporate network into Virtual LANs (VLAN). There are many good reasons for IT managers to configure their network this way. For example, VLANs may be configured to deliberately isolate and protect various parts of the network. Unfortunately, that isolation may not allow the security devices at the edge to communicate to their host without intervention by the IT manager. Or such configurations may require the device data to “hop” across multiple network switches, creating additional points of failure with each “hop.”

Adding an additional switch between the host application and the IP based door controller cuts the mean time between failure on the network connection between the host and edge device in half and doubles the chances of an overall network failure.

- While IT network resources may be secure for IT implementation and performance, this does not necessarily guarantee the same levels of security for the access control hardware. For example, while the computing network may be protected against hacking, such protection may not extend to the access control panels.

Clearly, the security integrator cannot assume that adequate network resources are always readily available. And even if and when such ports are available, reliable security system performance depends on digging deeper and giving careful consideration to the issues of system size, PoE power and overall network configuration.

Myth #2: Total Cost of Ownership

As a valuable metric in system evaluation, the total cost of security system ownership typically includes the purchase price of the components, costs to install the components, and ongoing costs to service the installation.

Initial Hardware Cost
Initial Software Cost
Initial Installation Cost
Training
+ Ongoing Maintenance
Total Cost of Ownership

The purchase price of the components covers the cost of the access control hardware and is often comparatively equivalent regardless of the type of installation. Installation costs cover the cost to mount and interconnect the components, then terminate the connections from the door. Wiring costs vary depending on the physical locations of the hardware, and how these units will be interconnected into the host system. The labor required to make door terminations must be included regardless of the network connection type, so this is not a variable in the comparison. Ongoing maintenance costs include service calls to the customer site.

The myth that an IP-based access control system consistently translates into a lower total cost of ownership is based, in part, on the assumption that wiring costs for network devices are lower than wiring costs for traditional RS-485 networks. Within the myth, IP devices installed at the edge lower installation costs because the CAT-5 network cable only needs to run to the nearest available switch. This compares favorably to a traditional “home-run” installation, where multiple wires would all run back to the central equipment closet, significantly increasing installation costs. Service

costs would be approximately the same or even less in an edge configuration because the security integrator would not be responsible for the network wiring once the site has been turned over to the customer.

Reality #2: Tallying the Total Cost of Ownership

Running CAT-5 cable 20 feet is definitely cheaper than a “home run” of 5 wires 200 feet, however today’s working world is not that simple. More often than not, the reality is that the IT manager is overburdened and overworked; providing IT services to the security system is not high atop his list of things to get done on any given day. Integrators installing networked systems often prefer to run their own private network, buying switches when necessary, and keeping the security system separate from the corporate network whenever they can. When this is done, the wiring costs are essentially the same as a traditional RS-485 configuration.

Service costs may or may not be lower when running on the edge. If the IT manager is cooperative and notifies the security integrator of outages for planned network service before the event, those costs can be managed. If not, or if the IT department has policies such as changing all the IP addresses regularly, service calls to troubleshoot network problems caused by a lack of good communication can add up, further driving the total cost of ownership above initial projections.

In addition to accounting for the realities of hidden installation and service costs, integrators must also factor-in the sometimes conflicting expectations of the IT and the security managers.

Myth #3: Security and IT Speak the Same Language

Security and IT managers seem to have equally high expectations of their networks:

- **100 percent Uptime** to support real-time reporting, command and control.
- **100 percent Equipment Access:** All relevant devices can be addressed physically and virtually.
- **100 percent Resource Allocation:** All manpower needed to properly operate and maintain systems is consistently available.

However, 100 percent uptime to an IT network manager may typically allow for scheduled and unscheduled maintenance and may actually translate to 99.9 percent uptime. While this has become an accepted IT norm, remember the security system depends on the IT infrastructure. If that infrastructure goes down, so does the security system.

Reality #3: Meeting and Managing Expectations

Downtime of one-tenth of 1 percent over one year means that the security system is down at least a full workday -- 8¾ hours. For most security systems and security managers, that amount of downtime is not acceptable.

*99.9% uptime over
the course of a year is
8¾ hours of
downtime.*

Similarly, the expectation of 100 percent equipment access means that the network manager can physically interface with network equipment at all times. Unfortunately, it does not mean the security integrator has access to the network equipment 100 percent of the time; often the integrator must wait for an IT administrator to allow him access to the physical network.

The same problem holds true with the expectation that the necessary resources to operate and maintain a system are available. The IT manager controls the resources the security network requires, including the human resources required to operate and maintain the network portion of the security network.

So, while both security and IT management bring great expectations to the table, successfully networked security must first define and resolve the similar and sometimes conflicting requirements and expectations.

Successfully Deploying IP-based Access Control

Single-door intelligent controllers have been marketed and sold since 1983 with the successful introduction of the Northern Computers N1000. These systems communicated on a twisted cable pair at 20mA. Because of the distance limitations with 20mA, this solution did not address enterprise deployment easily, though these panels are still sold today.

With the introduction of Mercury's MR50 single door controller in 1995, enterprise access control could be delivered due to the power of the Intelligent Controller; many doors could be installed

easily and economically with local termination at the door on a single cable back to the intelligent controller.

In the last several years, a variety of vendors have introduced network- ready single door Intelligent Controllers. These devices promise easy installation with PoE and network connectivity. The major innovation is how the single door controller can be connected through a network, not the single door controller itself.

IP- connected Intelligent Controllers have been successfully deployed for many years. Because the number of network drops required for Intelligent Controllers is far less than the number required for IP- based doors, getting network connection is comparable to adding one or two more computers or printers on the network. The Intelligent Controller is capable of full operation if the network connection is interrupted, and if that should happen, additional access control devices can be programmed-in for special operation.

However, regardless of the mode of connection or the source of power, the realities of security remain the same: an access control system must provide real-time monitoring and control of the facility in which it is installed. Access control systems must perform these tasks reliably, predictably and in a timely manner. In a strictly IP-based access control system, the greatest vulnerability is most often the network itself, not the functionality of the access hardware.

Know the Strengths and Limitations of the Technology

IP -based access control technology can provide lower-cost, easier to install access control systems. As the industry's leading supplier of access control hardware, Mercury has offered IP-based controllers for several years and is continuing to create additional IP- based products. The key to successful deployment is knowing when and where to use IP-based devices.

As we've seen, not only must system integrators dispel network myths and design systems based on the realities of available resources, they must also consider unique security issues when deciding to locate IP- based doors on the network, issues such as data security and the vulnerability to network attacks.

Know the Technology

Should this be installed on a separate security network?

Would using PoE+ deliver enough power to my door locks?

Would a hybrid system be beneficial?

If the IP- based door controller is on the corporate network, the data sent on the network could be compromised. Several free programs are available capable of “sniffing” the traffic on the network and using it. This eavesdropping can lead to a “man in the middle attack”, where the attacker makes a connection to the access control panel pretending to be the host application. The attacker can then send access control commands to the controller and the controller will respond.

“...a researcher in Texas found that he could crack one electronic access system at the network control level and simply open a door with a spoofed command sent over the network, eliminating the need for an access card. He could do it while bypassing the audit log, so the system wouldn’t see that someone opened the door.”

Wired, August 1, 2009

These sniffing programs are capable of capturing sensitive cardholder information which in turn could be used by anyone to gain access to the facility. Encrypted communication between all your IP-based security devices is essential in keeping your security system secure...

Any network device can be vulnerable to a network-wide “denial of service” attack. In this scenario, external sources flood the network with traffic and prevent valid network packets from reaching their destination. To prevent such vulnerabilities, any network-based security device must have safeguards to prevent or be protected from such attacks.

A solid access control strategy addresses these risks, myths and misconceptions. Alternatives to a strictly IP-based solution can and should be considered when devising the access control strategy:

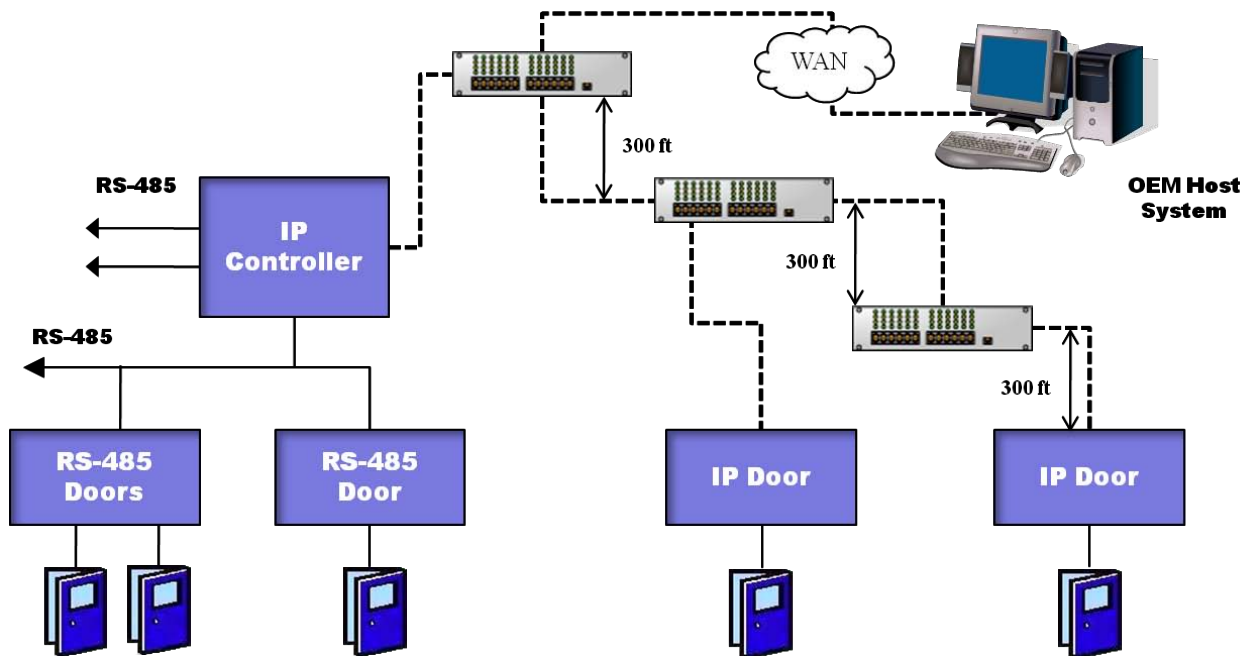
Consider installing on a separate network: Installations that are a combination of CCTV, security and audio or intercom voice over IP (VoIP) may be ideal candidates for IP-based access control at the door, especially if the integrator is running a separate network for the other systems.

Consider specifying the new PoE+ Standard, which will supply more power. The new IEEE PoE standard PoE+ will deliver more power and should be capable of driving a heavier lock as well as other security-related hardware installed near the door.

Consider Encrypted Communication: Encrypted communication between the host application and the Intelligent Controller will make the security network less vulnerable to “hacking.” The addition of encryption between the Intelligent Controller and the door control module increases security even more.

Consider “Hybrid” systems: A hybrid system gives you the freedom to use the technology that’s best suited to your requirements. Interior doors may be a good fit for IP- based door controllers while the exterior doors might be better suited for RS-485 door controllers.

Networked Access Control Topology



The schematic shows a hybrid RS-485 and IP-based system. IP doors on the right may be hard to reach and thus cost-effectively managed on the network. On the left, a full system of doors can effectively be hard-wired to a network-based intelligent controller. Here, in the event of a network interruption, integrity of all doors is maintained by and reported back to the IP controllers.

Checklist for choosing your access control installation strategy:

- What network infrastructure is available for security system use?
- When considering the IT network, involve the IT manager early in discussions. Evaluate the potential working relationship: how active a role would that manager want to play? What are the IT protocols for maintenance and service?
- What is the customer's tolerance for doors that go offline?
- What are the physical and logical topologies of the network? Are the switches located within 300 feet of the doors? Can network drops be easily installed at the door?
- Are the doors interior or exterior? If they are exterior, can the reader be installed separately from the controller?
- Does the network support PoE and will it be adequate to power the door locks?
- Do local zoning regulations allow the installation of PoE?
- Will this be on the corporate network or is this part of a larger installation of CCTV on a private network?
- If the installation is on the corporate network, what kind of data security is available? (Encryption, secure sockets, etc.)



For more information:
Mercury Security Corp.
2355 Mira Mar Avenue
Long Beach, CA 90815-1755
www.mercury-security.com