2305 Bering Dr, San Jose, CA 95131
Phone (800) 260-5265 / (408) 435-8400 / Fax (408) 577-1792

# TCP/IP Network Communication in Physical Access Control

## The way it's done:

The security industry has adopted many standards over time which have gone on to prove as solid foundations for product development and greater R&D. Examples of these include early 128 bit data encryption which paved the way for secure global ecommerce, mpeg compression saving valuable bandwidth, ContactID defining an efficient and effective means of communicating burglar information to base stations over a POTS phone line, and the Wiegand protocol, providing a well known standard for communication between RFID devices and Access Control systems .

None of these standard formats are exclusively the best solution for every situation; there's always more than one way to achieve the same outcome through different means or medium. Sometimes these standards are improved upon to meet the growing consumer demand or to provide even greater performance, such as in the case of POP3 email and the introduction of the IMAP protocol which ultimately provided far more efficient means to manage web based email by allowing a user to view an email instead of downloading it. However this doesn't mean POP3 became redundant as an email protocol, this simply made a particular standard suitable for a specific application. Often the application and hardware implemented define the protocols and standards used, but ultimately the choice comes down to the individual specifying the solution.

In the case of Physical Access Control using distributed controller intelligence, the standard has long called on RS-485 serial communication to distribute data to necessary devices throughout the system. Moving data from the head-end software and Server to the controller network is often achieved through RS-232, or in more recent times, TCP/IP. All of these standards are well known and well tested, each commanding their own degree of respect and superiority in differing situations.

RS-232 uses a 5v analog peak-to-peak signal to transmit binary information over a short distance. The advantage of RS-232 is its simplicity, efficiency and cost effectiveness. Using only 3 wires, data can migrate from PC to device quickly, however many PCs today don't come standard with a DB9 serial connection and hence this means of communication has quickly fallen by the wayside.

RS-485 is extremely powerful and robust, allowing data traversal over distances of up to 1.2Km. It's simplicity is a marvel, just plug in a device and map an address by physical notation (usually binary dipswitches). RS-485 can accommodate many configurations subject to manufacturer specifications, including daisy chain, star or composite daisy chain / star configuration. The speed at which data may move relies greatly upon the total network distance, but more often than not, RS-485 can handle a minimum payload of 100Kbs.

Recently, with the pervasiveness of Ethernet networks, TCP/IP adaptors have been developed as a means to convert RS-232 and RS-485 to TCP/IP and transmit data from PC to device, device to device and back.

There are many reasons for doing this and they include:

1. Greater network distance
2. Utilize an existing communications network
3. Easily accommodate current PC hardware and software that supports TCP/IP
4. Utilize web interfaces
5. Provide solutions to increased bandwidth capacity demands
6. Cheaper prices for category-5, 5E and 6 cable
7. Effective implementation of central management

Obviously, each of these benefits bring their own risk, such as security and autonomy, however this assumes you accept that these are managed and mitigated through various practices and technologies, both of which are beyond the scope of this paper.

## Why use TCP/IP

The question often thrown around is *'Why should I use TCP/IP'?* At this point it's important to remember that TCP/IP connectivity is not a solution to supersede all others, but another tool in the system design and deployment arsenal and hence the question should be *'When should I use TCP/IP'*?

There are a number of indicators that clearly point a system specification to call for TCP/IP communication, they include:

1. A need to communicate with devices in remote locations

    Historically, communicating with remote locations was achieved by encoding data, transmitting over a substitute medium and decoding at the other end. This may have been through RS-232 to RS-485 conversion, or RS-232 transmission over modem. Both solutions are limited; RS-485 requires the distance be less than 1.2K and a dedicated cable be trenched and laid.

    Modems can be problematic, subject to initialization strings and chipset compatibility. Furthermore, an application will normally make asynchronous site connections via modem and therefore the problem of delayed communications become exponentially exacerbated as more remote sites are brought online.

    TCP/IP communications for remote sites facilitate synchronous remote site communications at far greater bandwidth than RS-232 over modem, and when unitizing the internet, a TCP/IP network doesn't suffer the geographical size limitations of RS-485.

2. A need to integrate other TCP/IP based technologies or the possibility for the need in the future.

   As more products embed TCP/IP as their native communication mode, it's logical to request a degree of integration for certain situations, for example, integrate CCTV and Access Control to seamlessly record video of related access events. Achieving this over RS-232 or RS-485 is highly impractical and the 100Kbps offered by RS-485 will not provide sufficient bandwidth. ADSL2 on the other hand offer speeds of up to 5Mbps, FTTN between 25 to 100Mbps and FTTH or FTTO offers speeds of up to 1Gbps*.

3. When a system encompasses many devices, both Access Control and other technologies, and network traffic needs to be managed.

   Many networking switches allow professionals to comprehensively manage data paths and priorities throughout the network, special attention can be given to high priority network connections to ensure data moves quickly to its destination, while low priority connections may be defined as secondary to other business related data like streamed video and VOIP.

4. When cabling is difficult using tradition means.

   Cabling by traditional means can sometimes lead to very expensive and labor intensive situations. Installing a cable between buildings may require many hours of manual labor and costly machinery. TCP/IP facilitates the possible reuse of existing data network cables, rendering the need to install new cabling redundant; the savings in labor and materials can be significant.

5. A need for communications redundancy

   RS-485 and RS-232 provide 1 path of communications; Ethernet, through its various forms offer many redundant paths of communication. First, hardwired and wireless technologies can be combined. Second, partial meshing or full meshing networks may be employed; Finally, the very nature of the internet makes it highly reliable for maximum up time when used as part of a systems backbone.

6. A need for communication flexibility

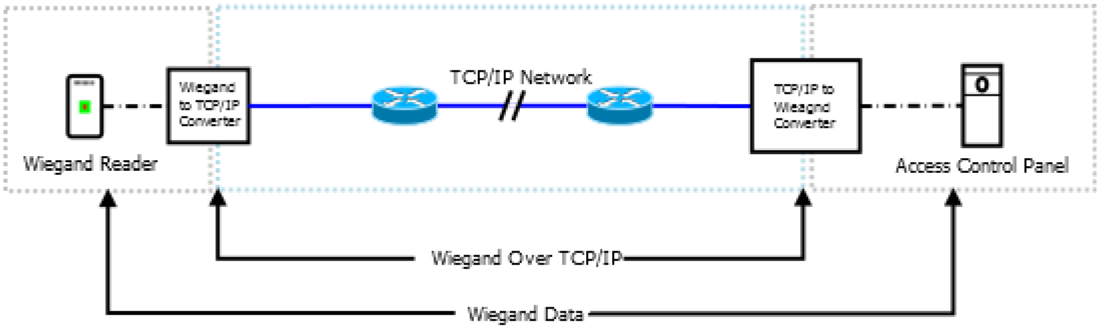
   When moving data over a single piece of copper cable, say, 1Km long, its data is checked at the destination for integrality. If the data is found to be corrupt, the receiver must request the information again from the sender; that's back 1Km to the sender and another 1Km to the receiver again. With TCP/IP, the data is checked on two different layers** by different network devices at each point along the run, so errors are detected and corrected much faster. Over very long distances with multiple paths of TCP/IP to choose from, switches can be configured to automatically find the fastest path or the shortest path of communication.

## Adapt or Embed

Not every situation calls for TCP/IP; installing a simple domestic alarm system, a standalone single door access controller or one camera at a door to view a visitor will function just fine on traditional means of communication.

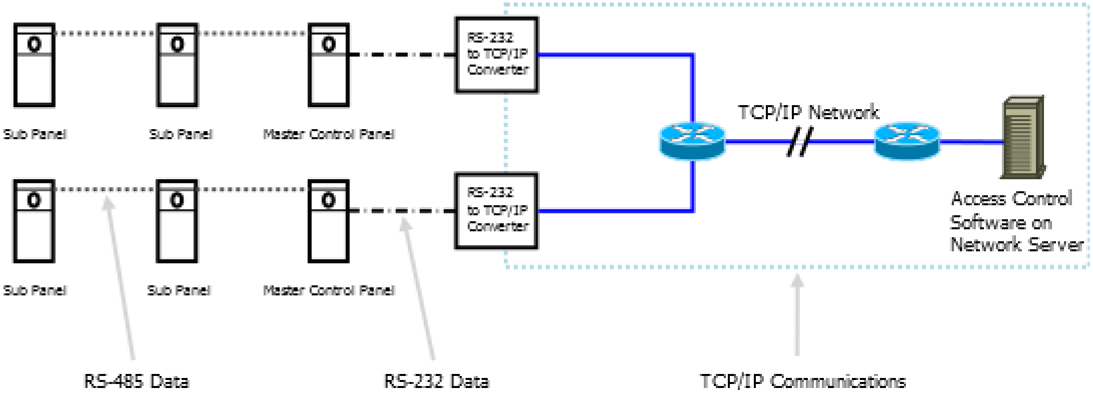
Not every device offers TCP/IP communication as a native format; sometimes if the benefits of TCP/IP are required, the only choice is to use an adaptor which converts the communication data to TCP/IP and possibly back again. The first point to determine is if the head-end will accept TCP/IP as a form of communication. If not, the data will need to be converted to TCP/IP and back to the original data type as shown in diagram 1, whereby the data is converted from Wiegand to TCP/IP and back from TCP/IP to Wiegand. There are many different adaptors on the market to support converting various standards to TCP/IP, including RS-232, RS-422, RS-485 and ASCII to name a few.

*Diagram 1: Converting Wiegand to TCP/IP for use over a network where head-end doesn't support TCP/IP.*



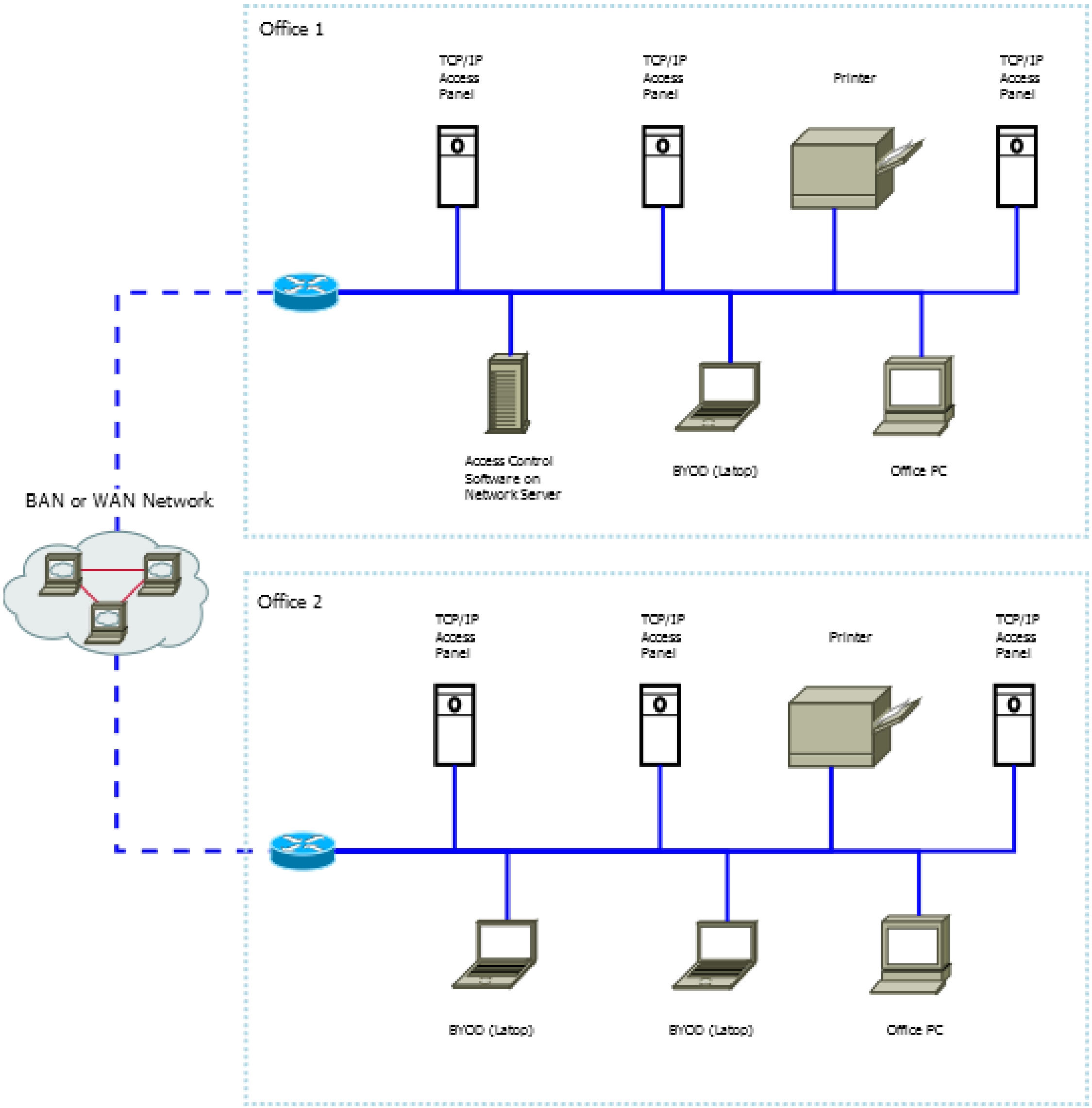
Alternatively, if the head-end supports TCP/IP, the data may only need to be converted from the native communication format to TCP/IP as per diagram 2. The advantage of using converters is primarily in retrofits or one off situations. Perhaps an existing serial based access control system requires the addition of 1 controller that will be located beyond the range of serial communications. Because the existing system is serial based it's unlikely the additional controller will support TCP/IP, so the use of an adaptor will provide communication over the existing network connections. This allows the legacy system to remain and facilitates a cost effective expansion onto the existing system.

*Diagram 2: Converting serial RS-232 to TCP/IP for use over a network where head-end supports TCP/IP.*



Devices and components with embedded TCP/IP allow the installer to connect the device directly to an Ethernet network without having to be concerned about encoding and decoding of the original format. The installer only deals with network related information such as IP addresses. By selecting TCP/IP embedded products the installer need not be concerned with USB to Serial converters, setting serial port numbers and controller dipswitch setting, nor do they need to worry about configuring conversion information, such as which channel RS-232 uses and which channel RS-485 uses; simply assign an IP address to the appropriate MAC (Machine Address). See diagram 3 for an example of a multi site, TCP/IP based access system.

*Diagram 3: Multi-site TCP/IP based system.*



## Conclusion:

TCP/IP communication solves many problems such as distance limitations, issues relating to dipswitches and solving multi platform integration. TCP/IP also provides communication redundancy, error checking and simple system scalability, all while adding value to an existing asset. The prevalence of TCP/IP embedded hardware and TCP/IP adaptors throughout the security industry highlights the practical and fiscal value in choosing TCP/IP as a communications method and explains why it so widely accepted across many industries.

*ADSL2, FTTO & FTTH speeds are based on Australian NBN specifications (2013)and may vary in other countries.
**TCP/IP Data is checked on the transport layer (layer 4) and may also be checked and corrected on the data link layer (layer 2).