british security industry association

a guide to

Internet Protocol

for ARCs and RVRCs

May 2008

For other information please contact:

British Security Industry Association
t: 0845 389 3889
f: 0845 389 0761
e: info@bsia.co.uk
www.bsia.co.uk

Form No. 236. Issue 1

Contents

Introduction

The use of IP technology is becoming more widespread across a variety of applications and industries. The security industry is no exception. IP can often be used to provide a cost-effective means of installing/monitoring security systems by exploiting existing infrastructure and enhancing and/or replacing older arrangements.

By removing the need for dedicated telephone lines and the call charges associated with connecting to a remote location, substantial savings can be achieved.

If an ARC wishes to provide remote monitoring & remote viewing of IP enabled systems, they will have to design and implement robust network solutions.

This document is not intended to repeat the requirements of current standards such as BS5979, BS 8418, etc. but will highlight the more common considerations associated with the monitoring of IP enabled security systems.

These guidelines have therefore been prepared to assist ARCs & RVRCs in utilising IP technology for security systems. It should be read in conjunction with the BSIA basic user and installer guides and other BSIA published documents from the IP suite.

1. Scope

This guide describes the more common issues associated with connection, monitoring and maintenance of IP based signalling systems connected to an alarm receiving centre (ARC) and a remote video response centre (RVRC).

2. Terms, definitions and abbreviations

2.2 Asymmetric Digital Subscriber Line (ADSL)

A two-way bandwidth devoted to the downstream and a small section devoted to upstream.

2.3 Access Point Node (APN)

A means of connection to the internet usually a public or private link (or access point).

2.4 General Packet Radio Services (GPRS)

A mobile data service designed to increase speeds of transmission across a network.

2.5 Integrated Services Digital Network (ISDN)

A telecommunications network that allows for digital voice, video and data transmission.

2.6 Internet Service Provider (ISP)

A business or organisation that provides consumers access to the Internet and related services.

2.7 Public Switched Telephone Network (PSTN)

A device for connecting dissimilar LANs together or LANs to WANs.

2.8 Symmetric Digital Subscriber Line (SDSL)

Similar to ADSL but has a different transfer speed for upstream and downstream transmissions.

2.9 Service Level Agreement (SLA)

Is a document that is contractually agreed between a service provider and a customer (end-user), which contains requirements that fulfil contractual obligations of a service provision.

2.10 Virtual Private Network (VPN)

A private communications network often used by companies or organisations to communicate confidentially over a public network.

2.11 Wide Area Network (WAN)

A computer network that allows the connection of LANs and other networks to allow users and computers to communicate from one location to another.

3. IP Network access

Firstly, as with any IP system, an ARC/RVRC will have to provide network access to receivers and associated devices. As with any security system, we need to be confident that the network systems in place are adequate to meet the risks both in reliability and security.

A network can be built up from many differing types of service. One of the more common is ADSL (Broadband) but there is also SDSL, leased lines, megastreams, kilostreams, GPRS (Cellular network), ISDN Dialup, PSTN Dialup and quite a few other options in the form of direct links to service providers.

It is quite common for a remote site having an IP enabled security system to have an ADSL line from a popular ISP (BT, Pipex, NTL, Tiscali, etc). These links are good value for money but come with some risk. Currently, there is no common service level agreement (SLA) for standard ADSL links, i.e. if the links were to fail you could wait days, even weeks to get the problem resolved.

For this reason we do not recommend that an ARC/RVRC uses these types of links for monitoring IP systems

In some systems, there may also be the option of an alternative path, i.e. a system could be designed with ADSL as a primary link but fall back on to an ISDN line or GPRS connection if the ADSL fails in some way.

GPRS is becoming one of the more popular options, particularly for intruder alarms where the data sent and received is minimal. Where this is the case, it should be clear as to what kind of link is proposed, public or private, i.e is the proposal to use the public Access Point Node (APN) provided by the GPRS service provider or have the GPRS bonded to a private APN. In doing the latter, a customer can be assured their network is not likely to be at risk from public access.

There are several possible configurations for a network link to an ARC/RVRC:

a. A private link from site direct to ARC/RVRC considering the following:

- This is likely to be in the form of a private corporate WAN connected to the ARC/RVRC. This network arrangement significantly reduces the risk to the customer but does not ensure the ARC is protected from unauthorised network access.
- Adequate security should be in place to ensure the ARC is protected from any third party network in the form of a firewall and appropriate policies.
- A private link is the most favourable since it is likely to be assured with service level agreements and fault response times, i.e. if a fault was reported you might expect someone to be addressing any problem within four hours.
- In addition, a customer may prefer this option since there is no exposure of their corporate network to the internet (the ARC/RVRCs network design should also ensure this through the careful use of firewalls and managed switches, etc). The ARC/RVRC might also prefer this option for the same reasons.

b. A public Link from site to ARC/RVRC consisting of the following:

- This is likely to be systems making use of the Internet to link to an ARC/RVRC. The ARC should ensure they provide robust network links from the Internet to the ARC. It is not recommended that the ARC/RVRC use ADSL for this. Instead, the ARC should consider a minimum of two leased lines from different service providers.
- In this option, the site is directly connected to the Internet via a local router which must be configured to allow outgoing and incoming network traffic as required by the security system and supporting software applications. The ARC/RVRC must make public IP addresses available to the installer/customer in order to pass information between the ARC/RVRC and the site.
- Diversely routed links should be considered.
- Part private and public to ARC/RVRC. In this configuration, a private corporate network routes all the network traffic through one central location and then via the Internet to the ARC/RVRC.
- This option comes with some risk. Where a customer decides to route all the networking via their own corporate WAN via a single network point, consideration should be given to the loss of this single point.

A private link is one that is not accessible by parties other than the ARC/RVRC

A public link is one that typically makes use of the internet to communicate with an ARC/RVRC

A part private and public link in one that makes use of a private corporate WAN that is linked to the ARC via a route across the Internet.

An ARC/RVRC considering the monitoring of IP enabled systems must be aware of issues likely to affect monitoring of such systems.

4. Bandwidth requirements

While one single alarm system uses very small amounts of bandwidth, monitoring several hundred or even thousands could have a dramatic impact on the ARC links, i.e. consider open/close signals happening at more or less the same time every day from all systems.

It is unlikely that all these signals would be sent at exactly the same time so bandwidth is unlikely to be of major concern to the ARC for a small number of systems. However, as you start to calculate bandwidth requirements for CCTV you can see that you quickly begin to use up the available bandwidth.

For alarms, you should be more concerned with hardware systems able to process a high number of systems simultaneously. e.g, firewalls, receivers/servers.

However, a CCTV system sending multiple data streams could require significant bandwidth in much the same way as a DoS attack (Denial of Service). There should be systems in place to address these concerns.

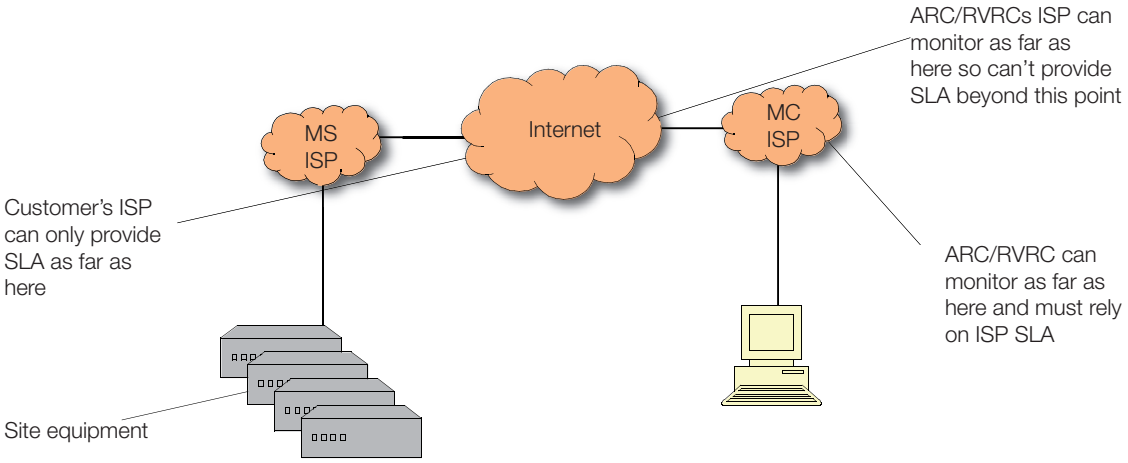
Another point you may wish to consider is how many systems you are prepared to connect to individual links. i.e. is it appropriate to monitor 10,000 systems on a single link provided by one service provider and the ASC equipment or, should you consider splitting the risk so that 5,000 systems are monitored using one link and the other 5,000 using a another. In this way you limit the risks associated with a small number of ISP links and equipment failure such as firewalls, etc.

5. Types of network connection

When considering network links for an ARC/RVRC it should be noted that there is part of the network that may be beyond the control of both the installer and the ARC/RVRC.

Consider an ARC who has links provided from a local service provider. All the equipment at the ARC/RVRC is under the direct control of them. However, beyond the link from the ISP to the ARC lies multiple service providers contracted to people at different points of the route between the monitored site and the monitoring centre as illustrated below. An ARC/RVRC should try to reduce the number of people in the loop to minimise the potential for failure.

Fig 1.



Key:
MS = Monitored Site
MC = Monitoring Centre

The reason this should be considered is because of what the customer can expect from the ARC in the event of a network failure. An ARC/RVRC could expect to respond quickly if equipment failed in house, and they could also expect a fairly prompt response from their Internet Service Provider (ISP) (assuming SLAs are in place). However, it becomes a little more vague if there are other service providers in the chain. For this reason and where possible, we recommend all security systems are configured with more than one IP address to connect to in the event of a link failure.

Additionally, you might like to consider what might happen if both the customer's ISP and the ARC/RVRC's ISP insist there is nothing wrong with the link when clearly the site IP system cannot connect to the ARC/RVRC.

And finally, consider what skills you might want in-house to provide and maintain any IP monitoring system and network.

As with many types of dual path system, the use of GPRS is becoming common-place. Excluding the service providers and the types of package they might offer, there are two types: public and private.

a. Public GPRS

Uses a link that connects to the Internet via a connection shared between anyone needing access to the internet. Typically mobile phones use these connections as do countless other mobile devices. Another term associated with this type of link is Public APN (Access Point Node) or the connection everyone uses to connect to the Internet.

b. A Private APN

This is a mobile connection that can only be accessed by nominated devices (usually tied to individual SIM cards by the service provider).

Traffic from such a link can then be delivered from the service provider directly to the ARC/RVRC network in the form of a private circuit (Leased Line) or possibly via VPN connection from the service provider to the ARC/RVRC

This means the connection is private and not subject to the same risks as a publicly available network.

Using the latter, it is possible to obtain SLAs for the link from the service provider's core network to the ARC/RVRC. However, it will be far more difficult to get SLAs for each geographical location since this can be largely dependent on site location, weather, time of day, etc.

When considering a private APN, you will have to specify the size of the network or the number of devices you expect to connect or this could result in systems not being able to connect to the GPRS network. You should ensure the chosen IP device will allow multiple APNs to be configured as required.

To be fully robust, you should have two connections from the service provider to the ARC/RVRC. As with the other links discussed, these should be diversely routed.

Consider the risk associated with a single service provider. It may not be possible to acquire a strong GSM/GPRS signal at all proposed sites. In this case you may be able to overcome the problem of a weak signal by having multiple service providers. e.g. Orange, Vodafone, 02, etc. It may also be possible to obtain a SIM card that is not tied to a single service provider but can roam between providers to obtain the strongest signal. It is important to understand any proposal for roaming SIM cards since it may require receivers to be accessible from the internet.

There are specialist network providers who can provide a fully managed service to make this easier to manage and maintain and who also have agreements with most of the larger GSM/GPRS providers

It is important to understand where responsibilities lie for the configuration and maintenance or each piece of equipment on the site. Some service providers will provide a comprehensive arrangement including all routers, firewalls, etc. However, others may expect some of this to fall on the ARC/RVRC staff.

As with all systems, the configuration settings should be backed up regularly

6. Receiving software systems

As with all new systems, it is often tempting to rush in to installing hardware and software systems to take advantage of new business potential. This could also be the case for the manufacturer who has a great deal of experience building circuit boards and little experience of software management. Some of the key considerations are:

- You should have a clear understanding of any support limitations when choosing your system. Manufacturers will want to support their software as much as possible but may well be reliant on a third party.
- What are the ongoing costs associated with the receiver software. e.g. connection licences per system monitored? Do you intend to pass on these costs, etc?
- Annual subscription fees for software releases; arrangements to ensure always compatible with operating software and compatible with hardware enhancements and bug fixes.

- Ease of integration with existing systems.
- What training will staff require to monitor, set up and respond to IP enabled systems?
- What information is required from the customer, keyholder details, the name of the customers IT department to report multiple losses. What does the customer want you to do with this information. This is very important since it could have an impact on response times, system grading, etc.
- The ARC/RVRC contracts should reflect these concerns on a per site basis.
  What information can you provide to report on system availability?
  Is this a simple report or does it require an enhancement to the ARC/RVRC software?

Information required from installer

How much support will an installer require and does the ARC/RVRC have the skills in-house to support installers? Where is the line of responsibility drawn? I.e. is it up to the ARC/RVRC to identify a problem with the customer network and what systems might be used to identify this?

The customer may not have in-house skills to identify the source of a problem. Could be helpful if automated systems could provide this and report it in plain English to the ARC/RVRC.

Customer support

Support may need to be provided for queries with site routers and firewalls, open ports and port forwarding.

ARC network links

Where an ARC/RVRC provides network links for monitoring and remote viewing of security systems, it should be clear where the point of responsibility lies for each aspect of the network and associated peripherals.

An ARC/RVRC should firstly ensure the chosen service provider has reliable service and maintenance arrangements in place to address faults, etc. These arrangements should be documented in an approved service level agreement.

The point at which the ARC responsibility for network equipment such as firewalls and routers i.e. who owns the equipment and who should replace it in the event of failure, should be agreed.

Internally establish who is responsible for ensuring the equipment is adequately protected from power failures, accidental damage and mis-configuration.

Where the ARC/RVRC is responsible for the provision of firewalls and routers etc, agree what plans are in place to replace/repair a unit when required.

A process should be in place to ensure the latest configuration settings are recorded and held in a secure location. Details of such records should be held with the ARC/RVRC contingency plans.

Where an ARC/RVRC provides links to monitor remote security systems, it should be recognised that the performance of the ARC/RVRCs chosen ISP will directly affect the security of its customers. An ARC should consider how to handle failures of an ISP. If an ISP were to go out of business suddenly, the ARC may have to consider changing its publicly available Internet addresses. Additionally, poor performance of an ISP may also require changing the public IP addresses.

Changing public IP addresses is a significant change and the impact on customers should not be underestimated. Each IP enabled security system is likely to require a site visit. The costs associated with this could be significant. While any problems of ISP being merged/acquired by another service provider should be minimal, you may find that it is not possible to transfer an IP address range between service providers.

An ARC may also need to consider additional training for operators who need to understand new systems. i.e.

in the case of alarm signalling, the loss of IP could mean a total loss or partial failure in the link from a site to the ARC.

Additionally, where a customer has multiple sites routed via a single point, a failure at the single point could result in multiple faults of the same type and swamp an ARC with path failure messages. An arrangement should be in place with the customer to address such a condition

7. Reference documents

Standards/publications

BS8418 Installation and remote monitoring of detector activated CCTV systems
BS EN50132-7 CCTV Application guidelines
DD CLC/TS50131-7 I&HAS Application Guidelines
BS EN50136 series Transmission standards

Acknowledgements

The BSIA would like to thank members of the IP working group for their contribution in the development of this document.

Further reading

BSIA installation of IP based secure signalling systems for I&HAS
BSIA installation of access control systems using IP technology
BSIA installation of CCTV systems using IP technology
BSIA guide to common issues experience in Internet Protocol in the security Industry
BSIA installers guide to Internet Protocol in the security industry
BSIA User guide to Internet Protocol in the Security Industry
BSIA Form 120 Maintenance & servicing of CCTV systems
BSIA Form 109 Planning, installation and maintenance of CCTV systems
IPCRes guidance – Alarm signalling using Internet Protocol – Part 1 An overview
IPCRes guidance – Alarm signalling using Internet Protocol – Part 2 Considerations for insurers