Abtec

White Paper for
Building Services
Engineers and
Consultants

Providing
Remote Access Connections
for Building Services Projects

How to deploy remote access to building control devices without compromising your client's security

Andrew Beynon and Chris Topham
Issue: 1
January 2015

Abtec Group, Barents House, Compass Point, Market Harborough, LE16 9HW
Web: www.abtecgrp.com Tel: 01858 438 500 email: enquiry@abtecgrp.com

ABOUT ABTEC

Abtec Group is a collection of UK businesses that specialise in providing IT, networking and building control services for building services engineers and consultants.

Recent projects include:

- Providing the KNX building controls infrastructure for one of the world's greenest buildings, The Crystal, London.
- Designing and deploying the IT and communications infrastructure at National Grid's new, award winning offices
- Providing the lighting control and BMS for the world's first digital car showroom, Audi City, London

Abtec Network Systems

Abtec Building Technologies

Abtec Group, Barents House, Compass Point, Market Harborough, LE16 9HW
Web: www.abtecgrp.com Tel: 01858 438 500 email: enquiry@abtecgrp.com

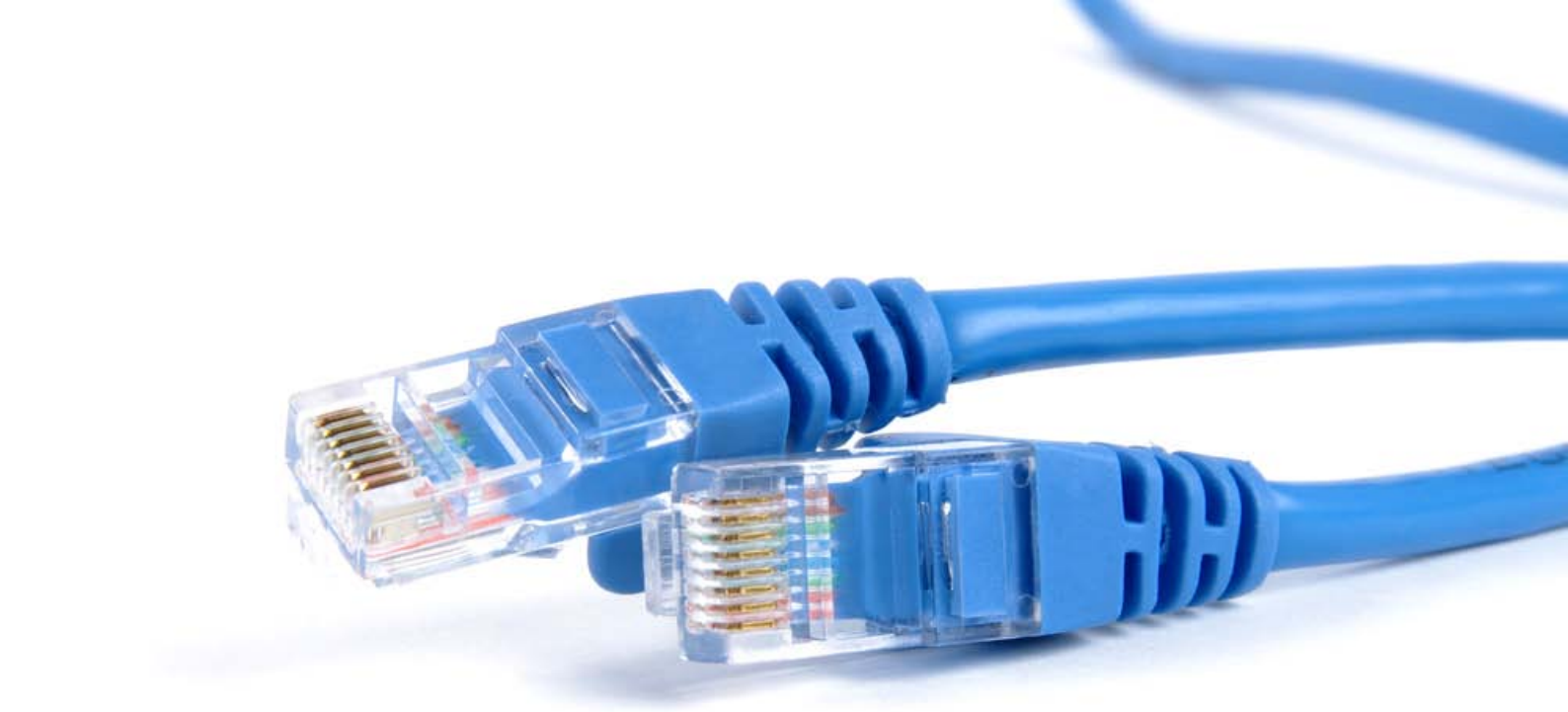
INTRODUCTION

Whether your project involves lighting controls, building management systems, air conditioning or monitoring energy use, there's a strong chance you'll want to access building control devices remotely.

Providing a remote access connection may be a small element of your project. Get that element wrong and it can cause large problems for you and your client. A recent example of this, noted in this paper, is a US retailer that lost 40 million credit card details to hackers who entered via an unsecured remote connection for monitoring refrigeration units.

This paper explores the methods and technologies of deploying remote access connections. It provides useful guidance on the type of network and network service provider for your projects.

Implementing the conclusions of this paper will help you provide remote access connections that are both safe and secure.



THE RISE OF REMOTE CONNECTIONS

There are many reasons why building services companies require remote connectivity to customer sites.

During the construction or refit process, access to building information modelling (BIM) data may be necessary; enabling changes to plans in real time. Without some kind of network connectivity this would be impossible.

Post commissioning, contractors will want to support their BMS (Building Management Systems) or building control installations; either for the defect liability period or as part of a maintenance contract. The ability to diagnose and resolve issues remotely can eliminate expensive site attendances. Contractors can respond faster to client requests, enhancing customer relationships.

Another remote connectivity application is energy data harvesting. This typically involves connecting to single devices at the customer site and transferring small amounts of data.

THE INTERNET OF THINGS

The increase in popularity of remote connections for building control devices is fuelling the growth of the 'Internet of Things'. Some estimate[1] that by the end of the decade 75 billion devices overall will be connected to the internet. The building services sector is providing much of that growth. It is estimated[2] that by 2020 there will be over 100 million Internet connected light fittings worldwide.

But, are we providing those remote connections with the appropriate technology?

1 Business Insider October 2013
2 ON World Inc smart lighting report 2013

INTERNET VPN VS. PRIVATE NETWORKS

INTERNET CONNECTIONS

Many of these remote connectivity applications can be achieved with standard Internet connections such as broadband or 3G/4G mobile SIM cards. The benefits of these connections are their wide availability and low cost.

NOT SCALABLE

Some contractors use VPN (Virtual Private Network) technologies to create a private tunnel through the Internet to the remote site. This is acceptable for a small number of sites but VPN solutions do not scale well and become difficult to manage for larger numbers of sites. There are also other issues with using the internet as transit mechanism.

SECURITY CONCERNS

Modern building control systems, more often than not, have web, file transfer and network management protocols enabled by default. Connecting these systems to the Internet, even with VPN technology, can expose customers to security threats.

There have been many, well publicised, breaches of network security due to poorly configured Internet connections into BMS networks. Many customers are sensitive to security concerns and will not accept Internet facing connections into their premises.

STANDARD SIM PROBLEMS

Standard mobile 3G/4G SIM cards can be problematic too. These SIMs are intended for outbound connections and firewalls within the cellular networks will prevent VPNs connecting to these SIMs.

A BETTER WAY

Private networks are designed to address all of these issues. A private network is not linked to the Internet in any way. It uses fixed private IP addressing and infrastructure not visible to the Internet. They are easy to provision and manage because the complexity of dealing with many VPN tunnels is removed.

There are many types of connectivity into private networks, as we'll explore shortly, including broadband and 3G/4G cellular access. It is important to note that although we associate these connection technologies with the web these versions don't connect to the internet.

Private cellular connections can be achieved using a Private APN (Access Point Name) network. These are networks which are linked to the cellular carrier networks. They route the data generated by building control devices through to a private network. This means that each SIM has a private, static IP address and full transparent IP routing through the private network.

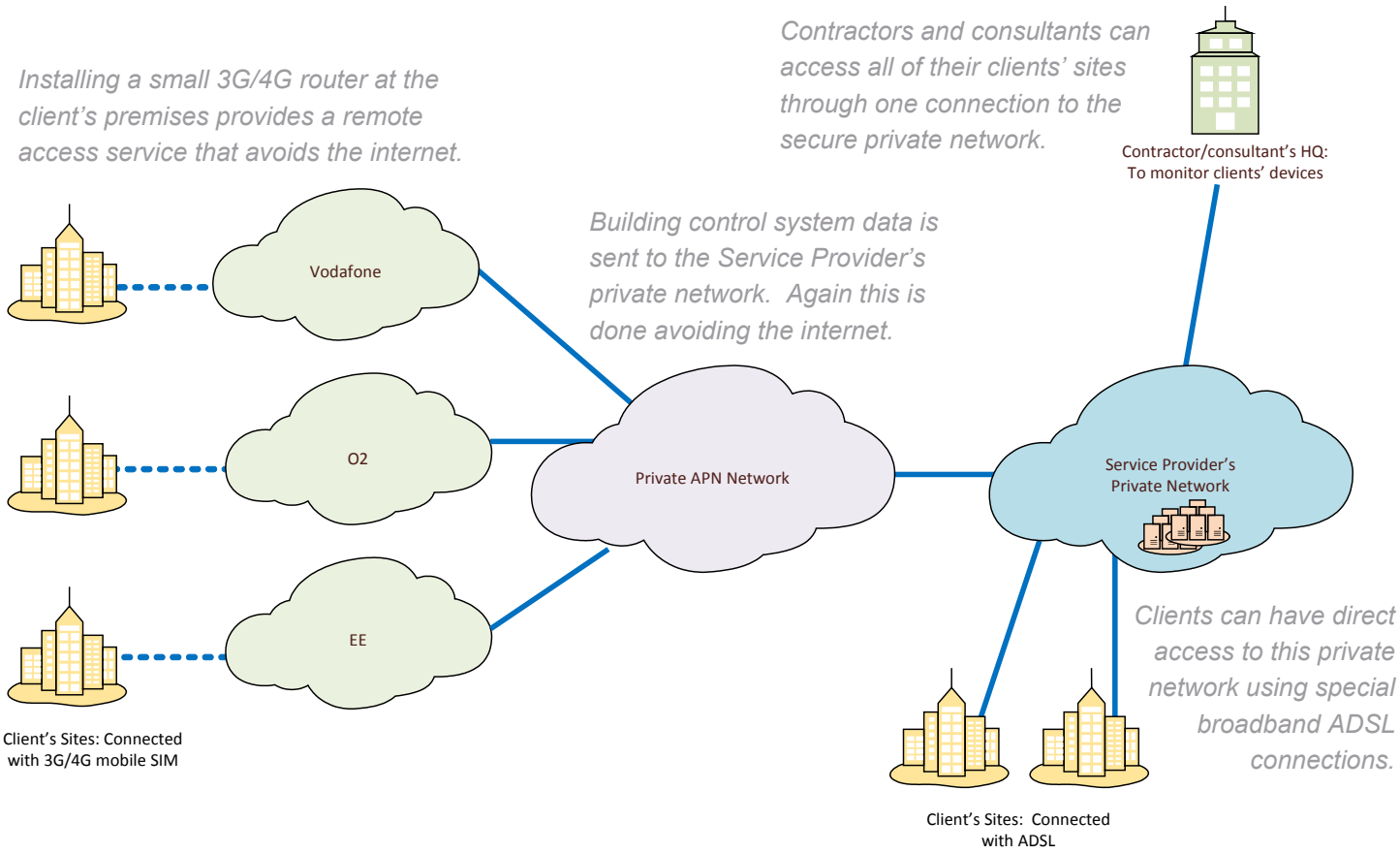
2.2 million

Estimated number of SCADA and BACnet devices identified as being directly or indirectly exposed to hacking over the Internet[1]

1 Project SHINE Findings Report Oct 2014

PRIVATE NETWORKS EXPLAINED

Using the Internet as a mechanism to provide remote access to building control systems is problematic. Security is a major concern; Internet VPNs don't scale beyond a handful of clients; and standard 3G/4G SIMs don't allow VPNs or remote access. A more secure way of providing remote connectivity can be achieved using a private network. These remove the need to provide VPN technologies, as they are already part of a private network. They're also easier to manage; multiple clients and sites can be managed from a single point, rather than having to connect to each site individually.



IN THE HEADLINES

Two recent building control security breaches highlight the risks associated with providing remote access using the internet.

Summer 2013, cybersecurity researchers hacked into the BMS of Google's new offices in Sydney, Australia. The BMS was connected to the Internet with a standard broadband DSL line.

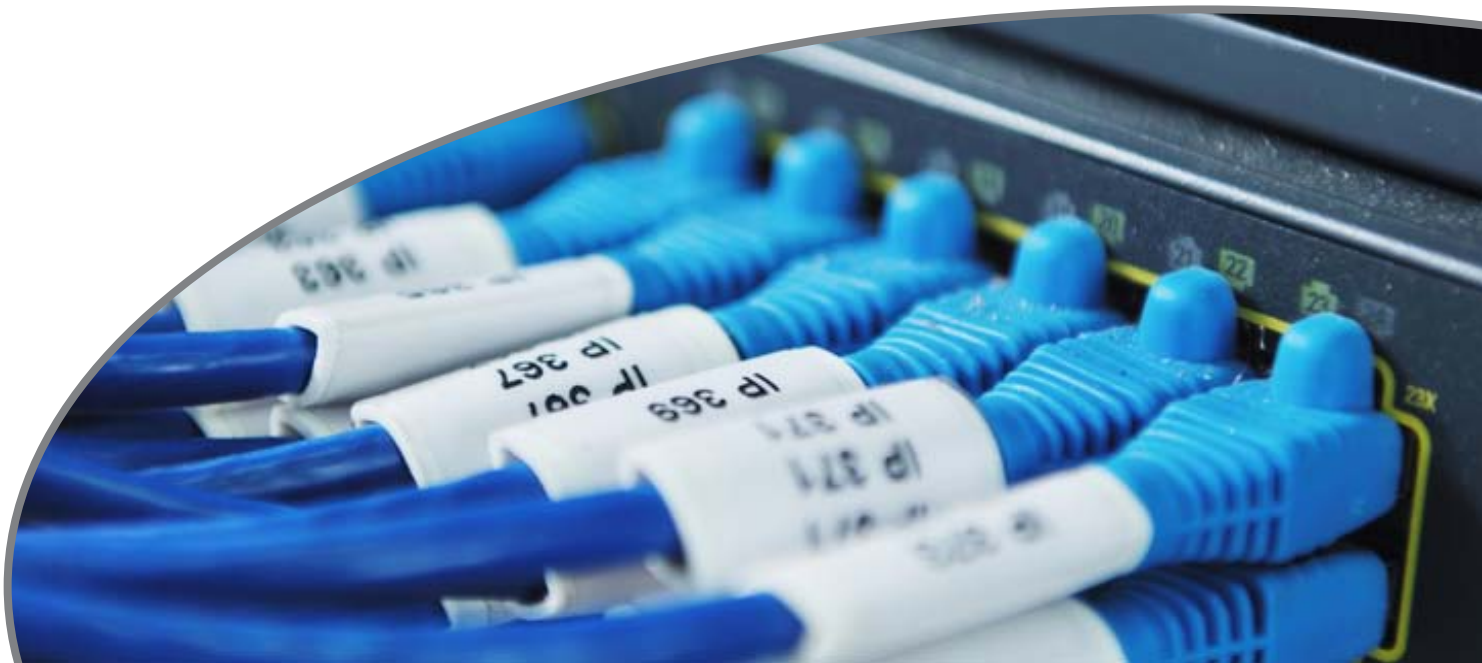
December 2013, hackers stole 40 million credit cards from the US retail superstore Target. It is believed that the hackers gained access to Target's network via a remote connection for a third party HVAC company.

PRIVATE NETWORKING CONNECTION TYPES

Different sites and applications will require different types of connections to the network. The table below describes the types of connections available and the characteristics of each link. A 'mix and match' approach can be taken when selecting the network connections; they don't all have to be the same type of connection.

The most popular types of connection for building control systems are the cellular 2G/3G/4G and ADSL broadband connections. This reflects that fact that many building control systems use small amounts of data.

CONNECTION TYPE	SPEED (BITS PER SECOND)	TYPICAL USE
Cellular 2G/3G/4G	70 Kbps - 10 Mbps	Energy data, remote support, temporary connections and backup for fixed lines
ADSL Broadband	2 Mbps - 24 Mbps	General fixed line connectivity. Remote support, 24/7 monitoring of control devices
FTTC Broadband	20 Mbps - 80 Mbps	Centralised control of multiple building BMS
Ethernet over FTTC (EoFTTC)	15 Mbps - 30 Mbps symmetrical bandwidth	Entry level central site links where upstream data rate is important. Not widely available
Ethernet First Mile (EFM)	10 Mbps - 30 Mbps symmetrical bandwidth	As EoFTTC but available in more areas
National Ethernet	10 Mbps - 1 Gbps and above	Mission critical links where high throughput of data and reliability is important



SOURCING PRIVATE NETWORKS

There are many suppliers of private networks across the UK. However, only a handful of these service providers actively support remote connections for building control systems.

Selecting the right service provider will be an important factor in ensuring that your project goes smoothly. Using a service provider familiar with the building services industry will have several benefits:

- **Support:** Their understanding the nature of the traffic over the network will help them select the most appropriate network connection for your project
- **Specialist hardware:** They will be able to supply the specialist hardware required for building control systems
- **Reliability:** A good service provider will preconfigure the hardware enabling engineers to 'connect-and-go' to the private network

SPECIALIST HARDWARE

Unlike standard Internet connections, where there's no choice of the routing equipment supplied, connections to a private network present you with a choice of networking hardware to route through. The choice of routing equipment will depend upon the nature of the project and the type of private network connection. For example, an energy metering project whose equipment is in the basement of a building maybe best served by a DIN rail 3G/4G cellular router, with an extension antenna to get a good cellular signal.

A network service provider familiar with the building services industry should be able to identify the right equipment for the project.

3G/4G routers like this are very popular as they can be preconfigured by the service provider, making the deployment process much easier.

PRIVATE NETWORK PRICES

The cost of a connection to a private network will depend on the type of network connection required. In general the greater the bandwidth speed the greater the cost.

Private network broadband and 3G/4G cellular connections tend to be a similar cost to their internet connected equivalents. Network connections are rented from the service provider, the costs accrued are usually charged on a monthly basis.

CHOOSING A SERVICE PROVIDER

Selecting the right private network service provider is important. Here are three questions that will help you choose.

1. Do you have a proven track record of providing private networks to the building services industry?
2. Do you have industry standard accreditation, e.g. Cisco Certified Network Professional engineers?
3. Do you have access to, and can you preconfigure, the specialist hardware required for building control projects?

CONCLUSION

Remote access connections are becoming an integral element of many building services projects.

Their benefits are clear; helping contractors and consultants cut costs from their operations by enabling the remote resolution of problems; and creating new revenue streams, such as enhanced maintenance offerings or energy monitoring.

Providing remote access connections over the internet is fraught with security risks and problems. It's not just hackers that are an issue it's also the problem of managing multiple VPN connections.

Using a private network instead of the internet can eliminate many of these problems. Private networks avoid the internet, keeping hackers at bay, and provide a platform that makes managing multiple remote connections easier.

Specialist service providers offer private networks that are tailored for the building services industry. These service providers understand your market, have access to the specialist hardware required, and can help you identify the right type of network connection.

Abtec Group, Barents House, Compass Point, Market Harborough, LE16 9HW
Web: www.abtecgrp.com Tel: 01858 438 500 email: enquiry@abtecgrp.com