DESIGN INSTALL PROTECT

Enterprising wireless: Efficiency and security in larger IT environments

Overcoming the challenges of Wi-Fi connectivity in the enterprise

www.ic2cctv.com

Introduction

Efficient untethered workforce productivity

Wi-Fi is something to which we have all become accustomed and now take for granted. The consumer broadband routers which we almost all have in our homes provide wireless connectivity which is now almost indispensable for everyday life in economies right around the world.

When we go in to the workplace, after completing journeys where we have used mobile data to stay connected, the expectation is for seamless connectivity in the business. And it's not just from the point of view of employees. For many enterprises, the desire is for untethered productivity, freeing workers to be more efficient.

However, providing wireless services in workplaces where there are significant numbers of people and / or a large estate poses significant challenges. Broadly, there are a number of considerations including factors such as efficiency, quality of service and security.

The strands that influence efficiency and service quality of Wi-Fi in the workplace are varied. There is only limited bandwidth or 'spectrum' available. This creates connectivity problems in high density environments with large numbers of devices such as large multi-floor office buildings, warehousing and logistical hubs and factories and industrial premises.

One of the issues that compounds the problem is frequency congestion, where Wi-Fi signals from adjacent businesses saturate the 2.4 and 5Ghz bands, the spectrum that is available for Wi-Fi. Also, the workforce may have more than one Wi-Fi enabled device, and there may be a need to provide visitors with Wi-Fi connectivity too, so it isn't simply a question of employee numbers.

Information security is just about the hottest item on the agenda for technology practitioners. It's not just the threat of hacking and malware; unauthorised data sharing, the leakage of data into the cloud and misuse by employees are all part of the complex fabric that go to make up the IT security threat environment. The forthcoming European Union General Data Protection Regulation (EU-GDPR) is a new data security standard. This not only creates a strong compliance framework to support exemplary IT security; it is also set to be a force for change in culture for all users of business IT.

Here we discuss how supporting large numbers of people and devices with wireless connectivity while ensuring network security requires enterprise wireless solutions that are fit for purpose.

The challenges of enterprise wireless connectivity

Interference

Frequency congestion results from too many devices competing for connectivity using the 2.4 and 5Ghz bands that are available for Wi-Fi. It is essentially a density problem. Besides the signals from the devices in use within your business, there are the signals from neighbouring businesses. The problem may be particularly acute in large multi-floor building shared by multiple tenant businesses.

Capacity

Many Wi-Fi networks were designed to deliver connectivity based on predicted numbers of employees. And for reasons of cost, over providing contingent or extra capacity was not often considered. However, the need for employees to have more than one Wi-Fi was not foreseen. Consequently, many existing enterprise wireless networks struggle for capacity to support the workforce properly.

Too many users connected to the same wireless Access Point can dramatically reduce performance. And if parts of your network are becoming congested, it can bring wireless throughput to a standstill.

Dead Zones

In some organisations, Wi-Fi has become the de facto standard for connectivity and wired connection is considered something of a legacy. Consequently, areas of no connectivity or 'dead zones' are simply unacceptable. Dead zones can be caused by environmental factors, including architectural features such as lift shafts and utility services risers for distributing cabling and pipework.

Multiple Access Points

Multiple Access points create a problem of management. Managing each access point individually creates a management overhead. Each device is likely to require software updates and other maintenance to be carried out by using a manual process for each one.

Multiple SSIDs

The SSID is the network name of the wireless Access Points through which users logon to the network. Some companies might use a specific SSID to provide guest logons for visitors. Multiple SSIDs tend to characterise wireless networks that have been built with consumer-level equipment.

Quite simply this architecture is inefficient and not fit-for the purposes of today's enterprises. Its performance is impacted by frequency congestion and it provides little or no management capability. It may also lead to confusion amongst the workforce through uncertainty about which SSID to use.

Consistency

For large multi-site businesses, there is also the issue of consistency from site to site. Having wireless connection processes that vary from place to place is likely to be a source of confusion. It may be especially troublesome if the workforce is mobile, moves between sites, and there are more than two sites in question.

Security

There are a number of elements to Wi-Fi security in the enterprise. If we simply start with how users login to the network, integration with domain security is a critical consideration. For Windows based networks, Active Directory controls user access rights, and here, WP2A-Enterprise is one solution. When users login with Active Directory usernames and passwords on the wireless network, they are authenticated and are able to access all the permitted network resources to which they normally have access.

Some organisations cannot or have chosen not to integrate WP2A-Enterprise. So, they are likely to be using the familiar process of selecting the right Access Point or router and authenticating with the W2PA pre-shared security key. However, keys can be given to anyone, allowing network access to anyone that obtains the key. This poses a significant risk to network security.

Guests

Guests are highly likely to be given security keys to provide ad-hoc access and then have the ability to access the network and pass the key on to others. Whether a guest is a casual visitor, a contractor, or a valuable client, access to the network needs to be properly managed under enterprise IT security policies.

What today's enterprises need

Essentially, to address the challenges of providing the wireless connectivity today's enterprises need, it's clear there is a requirement for a solution that delivers in three critical areas:

- Scalability
    - The ability to support large numbers of user devices over large-scale sites
- Security
    - Securing data against a range of risks, including hackers and insider threats
- Management
    - Squashing overheads to simplify management processes and increase value

Efficient and secure enterprise wireless connectivity

Enterprise wireless is a specialist area of networking. To overcome the challenges there is a need for specifically designed, fit-for-purpose technology. A good solution is likely to be composed of robust hardware specifically designed to address the challenges of delivering true enterprise-class Wi-Fi.

However, more than that, there is a need to select wireless networking partners that can provide the specialist services required to specify, supply and deploy appropriate, optimised solutions.

To maximise Return on Investment and the total value returned to the business, it essential to select a partner with a track record of successful deployment across larger environments to deliver in the three critical areas.

Scalability

When it comes to scalability, a true enterprise solution is scalable to support thousands of Access Points and hundreds of thousands of devices. Site and desktop surveys determine system design and the choice of specialised hardware and software. A key feature, only found on enterprise-grade Wi-Fi equipment, is that it is intelligent and detects frequency congestion and dynamically adapts to the operating environment.

Security

Any good solution should support integration with Active Directory security as well as the ISO 27001 information security standard. Importantly, security capability should be able to support the trend for Bring Your Own Device (BYOD) and Mobile Device Management (MDM). MDM is a particularly critical security consideration because of the vulnerability of mobile devices to loss or theft.

Management

The best enterprise solutions use controllers to unify management of all the Access Points on the network. This simplifies management tasks and the need for manual processes to update software and perform other maintenance tasks. Management functionality should include analytics and comprehensive logs of all wireless activity to provide an audit trail and support compliance where necessary. Cloud-enabled solutions help to maximise flexibility of the management process.

SUMMARY

Efficient and secure enterprise wireless solutions from iC2

iC2 is a leading mid-market security systems provider and was established in 2001. The business is owned and managed by a team with a collective experience of over 100 years in the electronic security business. iC2 holds CCTV and security accreditations with NSI and BSI.

The convergence of physical security with IT has also created the need to integrate information security. When it comes to enterprise Wi-Fi, our expertise in wireless security systems means we have developed extensive know-how.

We speak to people like you every day, that require advice on improving wireless connectivity in their businesses. We survey and consult to identify your needs and recommend appropriate solutions to help you release the benefit of efficient, untethered productivity from your workforce.

iC2 offers a complete enterprise wireless solution tailored to the needs of today's larger businesses:

- Surveys, consults and works with enterprises to identify needs
- Specifies, supplies, installs and fully supports all solutions
- Only provides high quality and appropriate enterprise wireless hardware solutions
- Solutions meet all appropriate compliance requirements or guidelines

A prestigious client list including luxury international boutique brands, top flight sporting venues, retail developments and educational and social environments demonstrates how solutions are deployed to meet a variety of requirements.

About Us

Keeping you safe and secure at all times

iC2 provide you with innovative solutions tailored to you and your sector. We are London-based with a national team of surveyors and engineers that work closely with our clients throughout the UK and internationally.

Our unique consultative approach allows us to tailor bespoke systems to your individual requirements, ensuring that your operational requirements are met.

We appreciate the need to demonstrate the best value to you every time and as a technology-led company, you can expect our cutting-edge and ground-breaking approach to serve your needs for many years to come.

Please feel free to contact us to discuss any requirements you may have.
We are happy to give you impartial advice, should you have any queries.

iC2 DESIGN INSTALL PROTECT

T: 020 3747 1800

E: info@ic2cctv.com

W: www.ic2cctv.com