Disruptive Analysis

Don't Assume

In-Building Network CONVERGENCE

Exploring strategic shifts & business drivers for integrating cellular, Wi-Fi & fiber infrastructures

A *Disruptive Analysis* thought-leadership eBook

Author: Dean Bubley

Contents

INTRODUCTION

What is wireless convergence?

Most of the time, people only notice wireless network coverage when it isn't there. And apart from people who work in the industry, most users think of fixed broadband and Wi-Fi as fundamentally separate from cellular/mobile. One is a personal subscription for most, while the other relates to a building or business. Yet the two worlds are converging in many ways, for both physical network infrastructure and services.

The term "convergence" is used widely in the technology and telecoms industries. At its simplest, it just means two or more historically-separate products or infrastructures being linked together, via a common service or platform.

This usually means shared (and hence lower) costs, and often new use-cases or deployment scenarios, by combining two adjacent technologies. Often, convergence heralds industry consolidation, or disruption as one sector absorbs another. But this process may well also yield new opportunities too, as this eBook will discuss.

Over the last 10-20 years, we have had numerous examples of convergence:

- Voice / data convergence, for example, in Enterprise IP networks.
- Fixed / mobile convergence, used to describe evolutions such as voice-over-Wi-Fi, or retail "quad-play" service combinations.
- LAN / WAN (Local/Wide Area Network) convergence, for instance using ethernet as an underlying common technology, to tie together local and wide-area networks.
- Convergence of consumer video and TV services, between broadcast and web/app delivery.

Similar concepts may get described as hybrids (for example, combinations of cloud and on-premise computing) or simply "integrated". Very few areas of technology converge fast – it is usually a progressive trend over years, with adopters having different motivations, risk-appetites, legacy issues and required skillsets.

Here, "wireless convergence" refers to indoor or on-site network infrastructure, linking cellular and Wi-Fi, as well as optical cabling used around a building, and maybe various other wireless platforms as well. It also links together the worlds of the service-provider and venue-owner, and fits with various other emergent wireless technologies themes such as spectrum-sharing, IoT, edge-computing and cloud-based radio networks.

What's the background for convergence?

Before looking at emerging and future trends for in-building systems, it's worth first considering how we got to today's status quo.

Historically, most architects and construction firms put little emphasis on information infrastructure for buildings – although obviously electrical cabling and basic alarm and safety systems have been around for decades. Over the last 20-30 years, this has evolved rapidly, initially with the requirement for network cabling for phones, PCs and servers, and then more recently for various types of wireless:

- Private Wi-Fi systems, installed by the building owner or tenants, connected to a wired LAN and external fixed broadband. The main use-cases are connections from employees' and guests' laptops, and more recently smartphones and tablets. This infrastructure has mostly been owned and operated as a private enterprise system, without individual users needing billable subscriptions or "accounts", although sometimes the Wi-Fi has been managed as-a-service by an external provider. Wi-Fi access points are mainly connected with ordinary network cabling.
- Public mobile (3G/4G) services are a huge priority, as most people expect their smartphones – and carrier services - to work well indoors. These are either delivered "outside-in" from the outdoor macro network, or via dedicated in-building systems. While these might be paid for either by a carrier or the venue/enterprise [see later section], they deliver public mobile services to employees and visitors' cell-phones. Many architectures have been used, including "passive" repeaters which boost the outdoor signal, or "active" systems with their own local "source" such as a dedicated cellular base station with distributed antennas (DAS).

Often, these wireless worlds have been completely separate, with perhaps a third in-building wireless system for public safety radio or building-management as well. And at the same time as new wireless "generations", the fixed/wired infrastructure has also been progressively upgraded. Modern desktops and servers – as well as Wi-Fi installations - have demanded ever-greater networking speeds, sometimes beyond a gigabit per second. This has meant fiber has been deployed "deeper" through buildings, in risers and wiring-closets and equipment rooms, although it is usually still not 100% end-to-end.

These worlds are now converging at many levels – with the addition of extra technical, commercial and regulatory factors as well. The next sections of this eBook examine the following trends:

- New radio technologies and spectrum bands, including 5G.
- New approaches for regulators, such as shared spectrum, indoor-coverage rules and government-owned networks.
- New uses for indoor wireless, including IoT connections and "mobile-only" users.
- Customer wireless systems for specific building/site types. Offices, apartment blocks, factories, transport systems and industrial facilities are very different.
- New players and business models becoming involved. This includes "neutral hosts", building-as-a-service operators and vertical-industry specialists.

Taken together, these trends mean both convergence and divergence – many systems will be integrated, while at the same time new niches and special circumstances will emerge for dedicated solutions. This paradox is a feature of most examples of technology convergence, and indoor wireless is likely to be no different.

It is important to recognize that neither Wi-Fi nor 4G/5G can do everything. There are various use-cases that still require one or the other specifically even though smartphones can use both with ease.

Wireless technology evolution: what's happening?

Before we consider new applications of wireless, or new stakeholders, we should recognize that the underlying technologies are evolving rapidly too. In the past, we've seen moves from 2G to 3G to 4G, plus continual improvement of Wi-Fi standards – but some of the coming changes make even those look minor in comparison.

5G in particular brings some important new transitions, that will drive convergence and accelerate upgrades and replacements to in-building infrastructure:

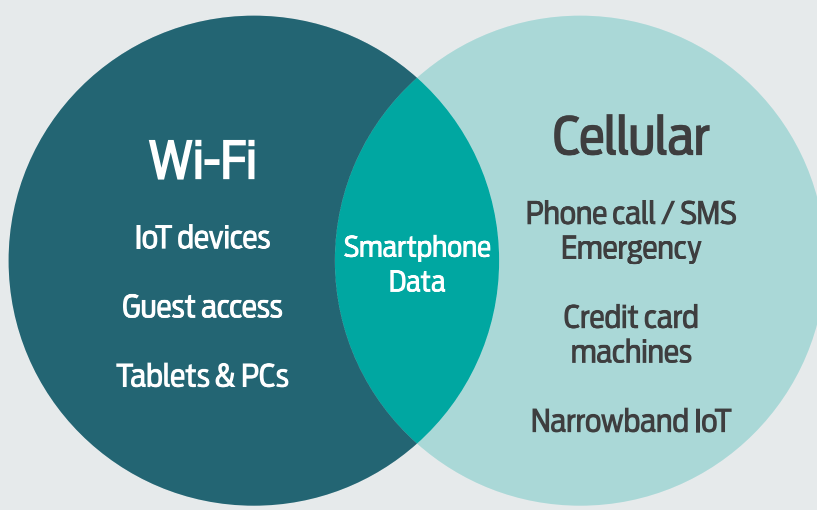
- 5G is expected to use a lot of "mid-band" spectrum, between 3-5GHz. This may prove tricky for existing in-building DAS systems, which have typically only been designed to work for frequencies below about 2.6GHz. New or hybrid solutions will be needed, such as small-cells.
- Some deployments of 5G may use "mmWave" bands, such as 24, 26, 28, 32, 38 & 47GHz. These have huge amounts of capacity, and are mostly clear of existing usage – but have very short range and poor propagation characteristics. If used indoors, they will need new small-cells or antennas, and much deeper use of fiber to connect them.
- Techniques such as "massive MIMO" (MIMO = Multiple In, Multiple Out) use new antenna arrays. These might help some outdoor-to-indoor penetration issues from macro cell-sites, but also make it harder to do "pure" indoor networks, as existing DAS systems – or even small cells - may not be able to support the capability.

Wi-Fi is also evolving rapidly, with new radio enhancements in the version called 802.11ax and its own 60GHz mmWave variant, WiGig, which is intended mostly for in-room gigabit connections (for example for connecting AR/VR headsets). There may also be new spectrum allocated for unlicensed use (i.e. mainly Wi-Fi) in the 4-6GHz range.

It is important to recognize that neither Wi-Fi nor 4G/5G can do everything. There are various use-cases that still require one or the other specifically – even though smartphones can use both with ease.

Other network types are becoming more important too – and although some of the lower-power IoT networks like LoRA and 4G's narrowband NB-IoT version have good penetration into buildings, there may be some locations such as elevator shafts and basements that need special consideration.

Wi-Fi and cellular are partly converged but remain as very distinct ecosystems



Source: Disruptive Analysis

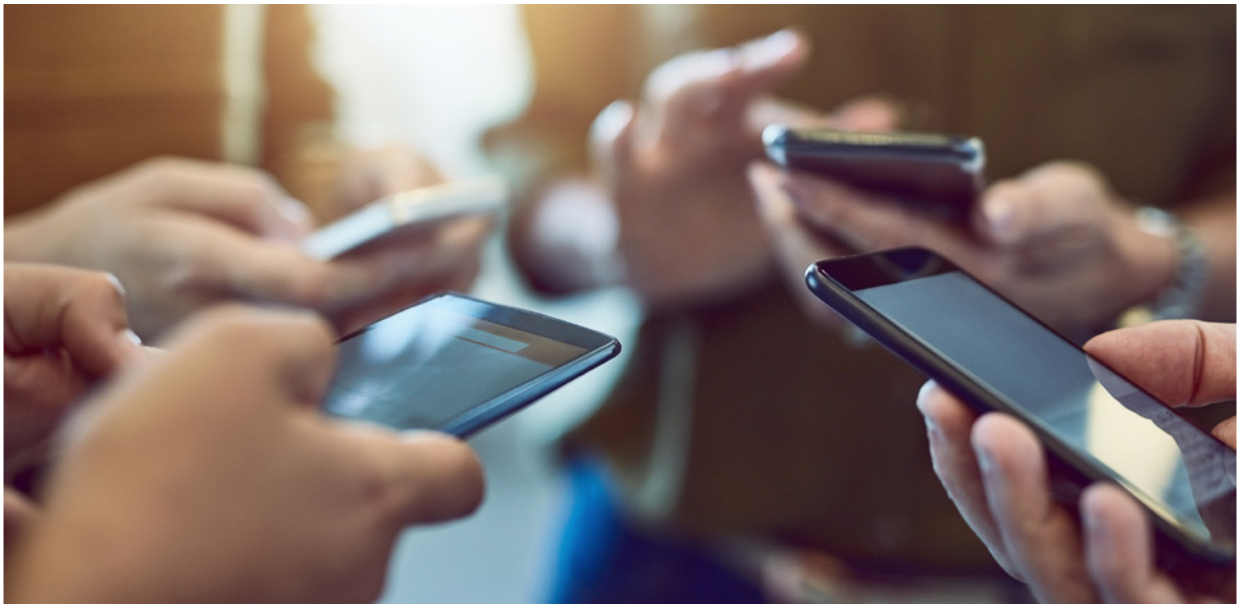
This all means that future in-building systems will have a much richer mix of distributed antennas, small-cells and Wi-Fi access points. Fiber connections will become ever more essential, as the radios need gigabit backhaul – and perhaps multiple connections, especially for MIMO antennas or "carrier aggregation", where several frequencies are bonded together for maximum throughput.

Cloud RAN

Another emerging trend which venues should understand is that of virtual or "cloud" RAN deployments (vRAN and C-RAN). These will add another "convergence" layer for future in-building wireless, as it blends it more with macro/outdoor systems to create hybrids.

What's happening here is that there is an ongoing shift towards separating the processing electronics of a base station (called the baseband unit or BBU) from the radio unit (transceivers, amplifiers and antenna). Typically these are connected with "fronthaul" fiber – in contrast to backhaul, which links the baseband to the core networks. This is actually fairly close to the model seen in DAS systems indoors.

Initially, this just involved separating the BBU (at ground level), from the radio at the top of a mast or on a rooftop. This reduces the size and cost of the antenna equipment installed. Then, the industry aimed to reduce RAN costs – and improve flexibility - by hosting multiple BBUs in a central "base station hotel", linked by fronthaul fibers to remote radio heads up to as much as 10-15km away. This allows capacity to be allocated more dynamically.



The concept is now evolving further. Many in the industry want to "virtualize" the equipment even more, by turning the BBUs into applications running on white-box servers even further upstream in the network. Ultimately, this could be integrated into an operator's overall NFV/SDN (network function virtualization / software-defined networking) architecture, either running in a central data-centre, or at a regional "edge" location.

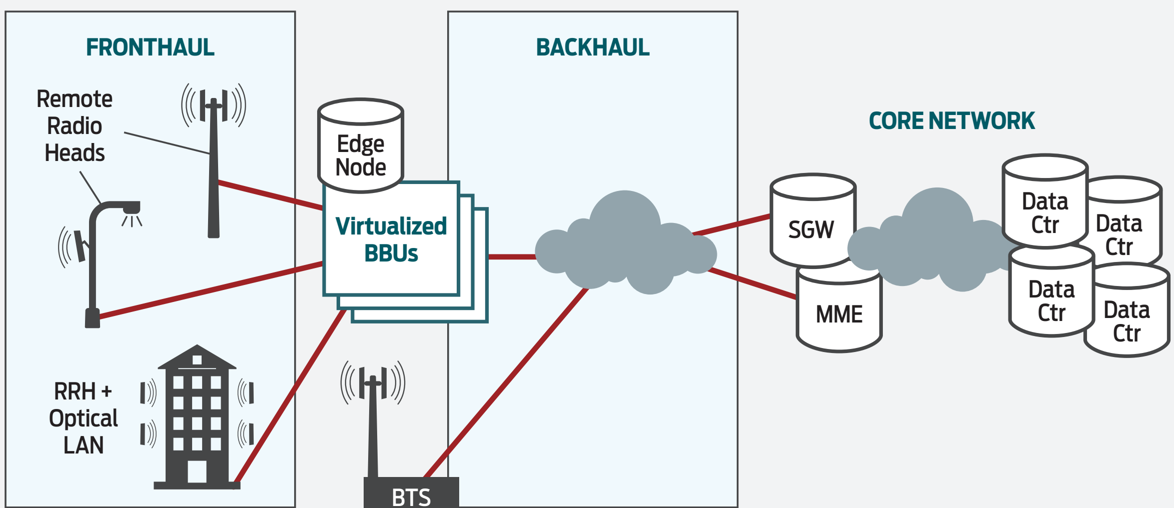
In some cases, this will lead to new hybrids with in-building wireless systems. The "signal source" for DAS could be a cheaper RRU, rather than a small cell or full base-station in the building. This could lower costs and potentially make it easier to connect multiple mobile operators to a single system (At present, many DAS systems only have one or two carriers' radios connected).

This could mean new types of convergence between public (cellular) networks and private (venue-owned) infrastructure, and perhaps the emergence of new "neutral host" providers to facilitate it.

We may also see some sites turn into edge-computing nodes, as part of a parallel trend: while radio functions are being pushed "up" into the network from the antennas, the opposite is occurring for compute, with some data-centre servers being moved "down" into the network. The physical locations will vary: maybe inside large buildings, or on private campuses or large-scale city development projects.

One last development that readers should be aware of: a number of buildings are now deploying "passive optical LANs", a technology which shares similarities with FTTB (fiber-to-the-building) networks, and which may become integrated more with wireless solutions over time too.

Future convergence between Optical LAN, Cloud RAN & Edge Computing.



Source: Disruptive Analysis

Where does Public Safety fit?

A separate but important area of wireless convergence is that of normal public mobile networks, converging with those used for public safety. Increasingly, emergency services are shifting from dedicated mobile-radio technologies like TETRA and P.25, to newer LTE-based platforms for critical communications.

Sometimes, the new networks are managed by cellular operators – such as AT&T managing FirstNet in the US, or BT/EE running the UK ESN (Emergency Services Network). Other examples may be deployed directly by government agencies.

While in some cases these may have dedicated frequency bands, they may only be deployed in some locations, with prioritized roaming onto public networks in others – including in-building. The switchovers will likely happen gradually, with a need for both systems to run in parallel, with the new platform developing cautiously, while the old one is slowly phased out.

As well as bringing extra regulatory considerations, future broadband public-safety networks may also require different patterns of coverage and therefore in-building infrastructure. It may be necessary to cover all areas/volumes of many structures, including elevator-shafts, stairwells, basements and rooftops, as these could be either fire-escapes, or perhaps sources of combustible material – even ceiling voids may need coverage.

In the future, critical communications systems will evolve to 5G as well, supporting further advanced capabilities such as robots and drones for fire-fighting or policing, which will need to operate indoors.

A similar trend is seen in some industrial sectors such as utilities and railways, which also want to evolve their old radio/walkie-talkie systems to a form of cellular, if it can be done with equivalent reliability and better price/performance.

How are indoor networks being used differently?

The profile of indoor wireless networks is changing rapidly, with some new use-cases emerging, and some old ones increasing in importance and visibility. In offices, guests and employees expect to use laptops and smartphones throughout the premises, which may also feature "hot desking" and new collaboration spaces where people meet in groups. More mobile working habits, plus widespread use of contractors or "gig economy" workers, means fewer desks with dedicated wired connections; almost everything is done wirelessly.

In hotels and apartments, people expect to stream high-quality video or even VR content to wireless devices. The sheer density of capacity required may be orders of magnitude higher than in the past – for example, think about 1000s of people watching action replays, or feeds from different cameras, in a sports stadium.

Industry and enterprise will have unique needs

As well as focusing on familiar sites like offices, hotels and apartments, we also need to think about wireless coverage in a much broader range of places – including transport hubs, entertainment venues, and industrial sites.

Such locations are ever more reliant on wireless connectivity for demanding IoT applications – think about oil and gas, mining, airports and ports, manufacturing plants, medical facilities, power generation and so forth. All have plans for "Industry 4.0" connectivity to sensors, robots, drones, process machinery and other new end-points. Some are in particularly-challenging environments like refineries or mines, with sources of interference (e.g. welding), large moving objects like ships or aircraft, metal pipework, specific safety or vertical-specific certification requirements – or even explosives - that mean all radio sources need to be switched off locally.

Often wireless connectivity will require deep specialization for each vertical or facility type - a challenge for both vendors and planners/operational staff. This is another, different angle on convergence – we may see wireless requirements determined by process machinery, robots or autonomous-driving trucks and carts.

Wireless networks will start to converge with industrial systems & IoT

What's changing with regulation & spectrum?

We also need to think about trends in law and government. Policymakers and regulators have both direct and indirect effects on indoor wireless, and therefore convergence. We have already discussed new frequency bands that are being released, as well as public-safety connectivity. But there is more to come.

As well as various new spectrum bands being used indoors, we will also see different methods for authorizing and allocating them. This will have a profound impact on indoor wireless systems and value-chains, as well as processes such as test-and-measurement.

The use of unlicensed (or lightly-licensed) frequencies for 4G and 5G networks is particularly important. There are various technical approaches, including LTE-U, LAA (license-assisted access) and MulteFire. Typically, they run in the same bands as Wi-Fi and Bluetooth, especially in the 5GHz range.

But as well as this, there may also be new shared bands for cellular – for example, readers should learn about the new CBRS (citizens' broadband radio service) band in 3.5GHz being released in the US. Other countries, such as several in Europe, are starting to license frequencies for particular local areas such as industrial facilities. We may also see sub-licensing or secondary reuse of existing national bands.

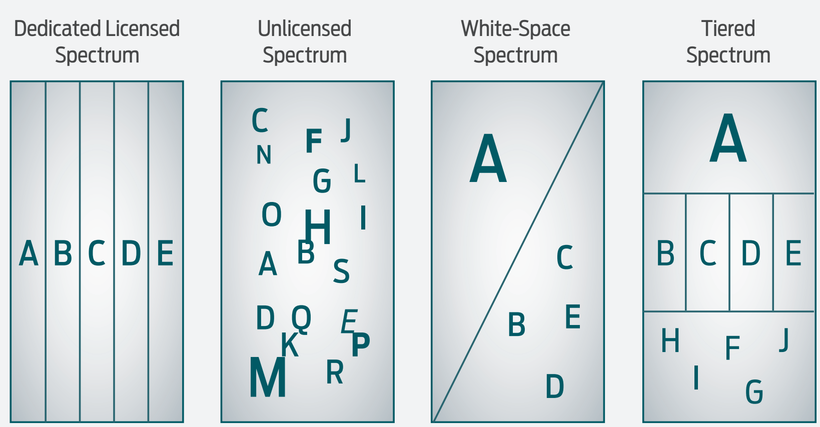
These frequencies might be used by existing mobile operators individually, shared by several operators in a consortium, or in some cases run by the venue-owner itself, or a third-party partner. We will start to see various sectors running private cellular networks, or perhaps a new breed of "Industrial Mobile Operators" – maybe set up as arms of industrial suppliers like GE or Siemens or Phillips or Honeywell.

There are various models for how this might work in terms of in-building infrastructure. Some may use dedicated small cells, others more distributed DAS-type approaches. It is still very early stages for many of these concepts, so innovation and experimentation are probable in coming years. Flexibility to adopt – and perhaps drop – new models will be seen as an advantage.

Another policy move likely by some regulators is a focus on indoor coverage metrics as part of MNOs' spectrum licences. For example in the UK, O2 had to deliver an indoor data service of at least 2Mbit/s to 98% of UK premises, by the end of 2017. Future spectrum awards are likely to be more stringent, also reflecting the ways in which smartphones are used (for example, in inside rooms such as bathrooms, which may be two walls from the exterior of the building), together with users' expectations of network performance.

While the current focus is probably on residential property and apartment blocks (as that is most-visible to voters), we may find some governments deciding that commercial or industrial properties deserve similar attention, especially as wireless connectivity is shown to be a driver of GDP and employment.

Flexible spectrum allocations will drive new SP & network ownership models



Source: Disruptive Analysis

New players will become involved, as well

New types of organizations are becoming involved in deploying, managing, financing or specifying indoor wireless systems, as it becomes more strategic. Some may just want visibility of designs, equipment, and plans for upgrade paths by carriers, while others may seek more direct involvement themselves. Business models will change.

"Stakeholder convergence" is likely to evolve in tandem with technology adoption

Building Type	Owners / Authorities	Tenants / Occupants / Users
Residential (house, apartment block, care home, parking)	Owner-occupier, landlord, leaseholder, local authority, housing association	Homeowner, family, renters, guests, consumers IoT devices, vehicle
Office building or campus	Corporate owner, building-as-a-service provider, government, educational	Tenant companies, staff, workspace renters, students, visitors / contractors, catering & cleaning, smart building IoT (e.g. elevators, coffee machines)
Public building (shopping mall, sports stadium, hospital, etc.)	Corporate owner, government authority, health/university body	Visitors, staff, contractors, IoT devices (some business/safety-critical), multi-tenant retailers & concessions
Industrial facility (oil refinery, factory, wind-farm, power station, etc.)	Corporate owner, contractors	Empoyees, equipment & systems suppliers, safety systems, IoT including safety-critical. Challenging RF environment (metalwork, interference, etc.)
Vehicles & transport (bus, train, port, airport, station, tunnel)	Government authority, private companies, outsourcers	Travellers, staff, contractors. B2B (e.g. airlines, freight forwarders), concessions (e.g. retail), numerous classes of IoT, government/safety authorities, numerous wireless systems

Source: Disruptive Analysis, STL Partners

A related challenge will be hybrids of public and private infrastructure, as these boundaries between SPs, enterprises and venue-owners start to blur. This has huge implications for regulation (who is responsible?), economics (who pays, or gets revenues?), and operations (who builds, runs and maintains connectivity?). It is not obvious exactly where all the "demarcation points" will be in the future.

Readers should be aware that security of the overall system will get much harder, too – who needs to trust whom, in such a converged environment? It would not be surprising to see new approaches such as blockchain-based controls emerge, as the basis of future management solutions.

What about new converged business models?

So given the changes in technology, application, regulatory and stakeholder involvement, you should not be surprised to find that converged wireless networks will need to adopt different economic models as well.

Today, the biggest question is "who pays?" for in-building infrastructure. But in future, we will be asking "who gets paid?" as well.

For example, real estate companies might believe higher rents are possible if better, "future-proof" coverage is available for tenants. Industrial firms are often hesitant to trust safety-critical systems to third parties, and may seek more control and ownership. In a 5G world, various new firms might turn into providers of indoor systems, rather than staying just as end-users.

We are already seeing the emergence of "neutral hosts" where a third-party network operator allows larger mobile carriers to put small cells on their fiber infrastructure. In future, as spectrum becomes more flexible or shared, the model may move to one that looks more like roaming agreements, or even "indoor MVNOs".

Traditional mobile carriers are already unwilling to bear the costs for coverage solutions for many buildings. Venue owners can find it takes years for approval, even if they swallow the costs themselves – for the wiring infrastructure and each network's "source", whether that is a small, dedicated base station for the building, or cheaper small-cells, plus fiber backhaul or fronthaul.

Most operators can only justify the investment – and the staff resources - for rare, ultra-large strategic sites (such as airports, major shopping malls and stadiums), for which a lack of cellular signal would have broader impacts on customer loyalty.

Obviously from a telecom operator's perspective, the best outcome for indoor wireless involves someone else paying for the installation and equipment, yet the revenues (and customer affection, brand awareness and loyalty) still flows to them. Disruptive Analysis suspects that this will seem like wishful-thinking in future, as new business models might enable venue-owners to get payments from carriers, rather than necessarily the reverse.

Indoor wireless convergence may shift from cost-centre to revenue-generator

Higher In-Building Wireless Revenues

- Retained / more loyal customers
- Potential for fixed-mobile substitution & larger mobile data plans
- New location-specific services
- Neutral-host services for MNOs
- Monetization of Wi-Fi by extra charges, advertising, etc.
- Sale of residential Femtocells or mesh-Wi-Fu units
- Data analytics from in-building wireless use

Lower In-Building Wireless Costs

- More cell-sites of Wi-Fi APs
- More/better antennas
- Building cabling/fiber
- New spectrum
- Site surveys & installation
- Roaming / access / offload fees
- Possible fines from regulators

Source: Disruptive Analysis, STL Partners

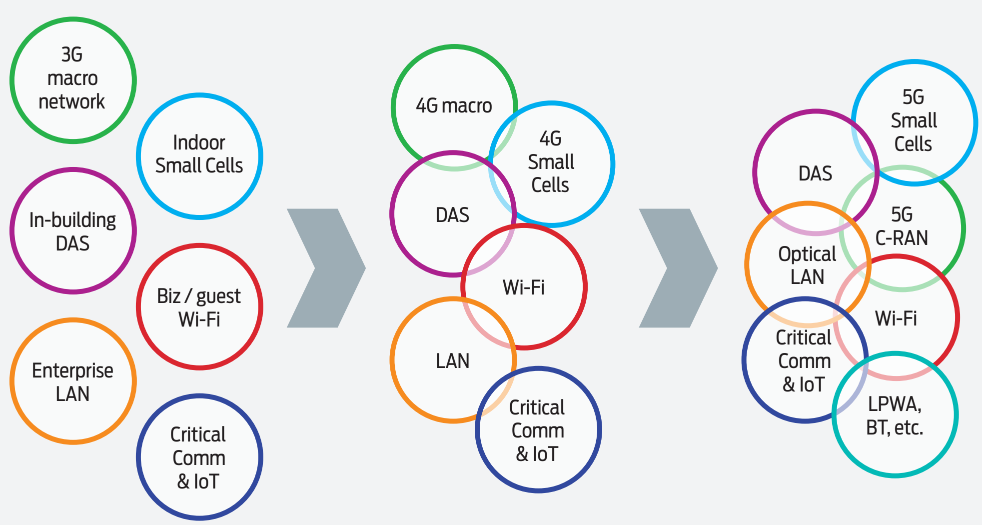
How can indoor systems be “future-proofed”?

We’ve looked at a top-level view of the changes ahead for in-building wireless networks. This eBook has covered a broad range of drivers – new technology, shifting regulations, the emergence of IoT, and a complex stakeholder landscape.

But for readers new to this, the key to understanding convergence is to think about all the new overlaps that are getting created:

- Public services meet private infrastructure
- Cellular meets Wi-Fi
- Outdoors macro-network meets indoor-network – and computing cloud
- Human users/devices meet IoT
- Industry verticals meet general-purpose networking
- New frequencies meet new wireless technologies
- Fiber meets gigabit wireless

Separate network domains are converging, as they evolve in tech & biz model



Source: Disruptive Analysis

All these intersections mean diverse future paths for in-building and on-site wireless. Some are predictable or already here, while others such as 5G are still on the drawing-board; the reality of usage patterns remains unclear.

So everyone needs the ability to plan ahead, and design "future-proof" infrastructure where possible, or at least have a good way to model different options. It will not be possible to work through all possibilities, so flexibility will be hugely important.

Venue-owners, service providers, vendors and tenants should all be asking some hard questions about their network infrastructure:

- Can it support 5G effectively? In which bands?
- What new classes of service provider might emerge and need access?
- Can the wireless infrastructure become a revenue-generator, rather than a cost?
- What are the regulatory dependencies and variables?
- How can all parts of the building – including non-human accessible ones – be covered?
- Can good Wi-Fi and cellular provision be a differentiator & add value to the building itself? Can this be proven and certificated?

Hopefully this eBook has taken readers on a brisk tour of some of the challenges and opportunities ahead. We all need to think a lot more carefully about indoor wireless network, as they will be used as a core part of many future businesses, and tenants and employees will expect them to "just work", hiding the complexity in the background. Whether it's a visitor expecting good Wi-Fi coverage, or an industrial robot needing extreme high-performance connections, it's critical that we don't just take connectivity for granted, but actively make plans, and expect rapid change and convergence.

About iBwave

iBwave Solutions, the standard for converged indoor network planning is the power behind great in-building wireless experience, enabling billions of end users and devices to connect inside a wide range of venues. As the global industry reference, our software solutions allow for smarter planning, design and deployment of any project regardless of size, complexity or technology. Along with innovative software, we are recognized for world class support in 100 countries, industry's most comprehensive components database and a well established certification program. For more information visit: www.ibwave.com.

About Disruptive Analysis

Disruptive Analysis is a technology-focused advisory firm focused on the mobile and wireless industry. Founded by experienced analyst & futurist Dean Bubley, it provides critical commentary and consulting support to telecoms/IT vendors, operators, regulators, users, investors and intermediaries. Disruptive Analysis focuses on communications and information technology industry trends, particularly in areas with complex value chains, rapid technical/market evolution, or labyrinthine business relationships. Currently, the company is focusing on 5G, NFV, IoT networks, spectrum policy, operator business models, the Future of Voice, AI, blockchain & Internet/operator ecosystems and the role of governments in next-generation networks.

Disruptive Analysis attempts to predict and validate the future direction and profit potential of technology markets - based on consideration of many more "angles" than is typical among industry analysts. It takes into account new products and technologies, changing distribution channels, customer trends, investor sentiment and macroeconomic status. Where appropriate, it takes a contrarian stance rather than support consensus or industry momentum. Disruptive Analysis' motto is "Don't Assume".

For more detail on Disruptive Analysis publications and consulting / advisory services, please contact information@disruptive-analysis.com. For details about Future of Voice & Contextual Communications workshops & publications, please see www.deanbubley.com.

Website: www.disruptive-analysis.com
Twitter: @disruptivedean
Blog: disruptivewireless.blogspot.com
Quora: Dean-Bubley

The document has been prepared by independent research firm Disruptive Analysis, and commissioned by iBwave, for distribution to its customers, partners and a wider audience. It is based on Disruptive Analysis' continuous research programme covering wireless technologies, IoT networking, service-provider dynamics and enterprise communications.

It should be read by CIOs, strategy executives, CTOs, CMOs, facilities management & planning/operational staff at major enterprises, communications service providers, information providers, software vendors, IoT firms, cable operators, ISPs, integrators, developers, XaaS providers and similar organizations.

Mentions of companies and products in this document are intended as illustrations of market evolution and are not intended as endorsements or product/service recommendations. For more details, please contact information@disruptive-analysis.com.

iBwave
www.ibwave.com