Beyond access

Managed Wi-Fi as a business enabler

A white paper from Bell

What's inside

People are accustomed to being on their devices everywhere they go. This shift has made its way onto corporate campuses and into retail locations, changing the expectations that businesses, employees and guests have about connectivity. Meeting these expectations for secure, always-available, high-performance Wi-Fi can be a challenge. This white paper explores what an advanced Wi-Fi network needs to deliver to meet these expectations – and how a managed services approach can simplify network management and benefit businesses in any sector.

Contents

Introduction 2

What the Wi-Fi network needs to deliver 3

- Five key questions 3

Managing guest access 4

- Who gets to access which content? 5
- Tracking usage for ongoing optimization 5

How a managed service provider can help 6

- What's included in a managed Wi-Fi service 6

The Bell approach to managed Wi-Fi 7

Introduction

According to the Organisation for Economic Co-operation and Development (OECD), there were 26.4 million active mobile subscriptions in Canada at the end of 2017.[1] Almost 70% of those included both voice and data services.[2] In a country of just under 37 million people, that's a lot of mobile connectivity – and a clear indicator of how people today are choosing to live and work.

37 million
people in canada

26.4 million
active mobile subscriptions

of those included both
voice and data service

Many companies today are taking an increasingly wireless-first approach to networking their offices. This not only changes how the networks for corporate campuses and retail outlets are set up, but also points to a fundamental shift in employee and guest expectations when it comes to connectivity.

Wi-Fi is a key component of the mobile mix because it lets users maximize their mobile connectivity at high bandwidths while minimizing cellular data usage. In 2016, 60% of all mobile data traffic – 10.7 exabytes a month – was being offloaded to fixed networks via Wi-Fi and wireless access points.[3] For businesses, fast and easily accessible Wi-Fi connectivity has real productivity-related benefits including greater efficiency, rapid responsiveness and seamless teamwork. Yet it can also introduce a fair degree of complexity. Different users have different needs. Internal staff require different privileges than external visitors to a corporate campus. Users may be logging on with company-provisioned hardware or with personal phones and tablets.

This can make it hard for IT teams to maintain security, ensure network performance, enforce policy, and support marketing and customer-relationship initiatives, which is why a growing number of businesses are choosing to have their Wi-Fi managed by an outsourced service provider.

So what are the prerequisites for a high-performing, reliable corporate Wi-Fi network today? And what are the considerations that should go into deciding whether or not to manage that network in house or with the help of an outsourced provider?

---

[1] As reported by MobileSyrup on June 29,2018. https://mobilesyrup.com/2018/06/29/canadians-consumed-an-average-of-1-5gb-of-mobile-data-per-month-in-2017-oecd/

[2] Ibid.

[3] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf

What the Wi-Fi network needs to deliver

Whether a business provides Wi-Fi to corporate users on a campus or to customers at retail locations, that wireless connectivity needs to be:

Easy – Network access should be simple to provide and manage, without requiring the involvement of corporate personnel.

Secure – Strong corporate security policies must be in place to ensure the network, user devices and business-critical data are not put at risk.

Reliable – The network should be always available with as little downtime as possible.

Fast – Today's customers and employees have no tolerance for low-speed connectivity.

It's also important to unify wireless and wired properties, ensuring the same standards and policies for managing the network are enforced no matter where or how people connect.

Five key questions

The core qualities of a modern Wi-Fi network are, to some extent, relative. For example, what's considered "fast" in one setting may not be in another, while the amount of security needed depends on the nature of the data being exchanged. Understanding what "easy, secure, reliable and fast" mean in any specific context requires answers to the following five questions:

- Who are the network's users?
- What services or applications are they using?
- Where and when do they need network access?
- Why do they need to access the network?
- How are they connecting to the network (i.e., through which devices)?

Many businesses often find internal users need self-service capabilities as well as secure connections to databases, servers, the corporate intranet and applications like Salesforce or Office 365. External users, on the other hand, need access to their email, instant messaging, the Internet and possibly their own corporate VPNs. Both, quite often, require connectivity that will allow them to use network-based collaboration and communication tools for seamless and productive interactions.

Managing guest access

While a completely open wireless network eliminates the need for time-consuming configuration of guest access or IT intervention, it also means unwanted guests (such as neighbouring businesses) can connect to the network freely, consuming valuable bandwidth, hindering performance and potentially exposing your network to malware and other security viruses.

As a result, network access control is essential. The sign-on process for authorized visitors typically happens one of two ways: through a splash page or via automated request.

Splash pages

A splash page is a self-serve login portal that appears in a guest's web browser and prompts them for identifying information like a name or email address before providing network access. Some splash pages allow guests to log in using their credentials from social media sites such as Facebook or Google.

The splash page can also be used to present the terms of service for accessing the network, which might include a user agreement or privacy statement. This solution is ideal for retail locations that receive a lot of consumer traffic.

Captive portals and walled gardens

A splash page can be considered a "captive portal" because it limits the guest to a single login page until they successfully authenticate their credentials. "Walled gardens", on the other hand, are multi-page captive portals that let unauthenticated users access web pages from a pre-defined range of IP addresses. Only after a further login and authentication process does the guest gain full Internet access beyond the walled garden.

Automated requests

Some organizations require visitors to submit an automated request to an authorized employee who then issues a temporary username and password to the guest. This approach is best suited to larger corporations where data security is a top priority. With fewer guests looking to access the network (compared to a retail setting), issuing temporary credentials provides a greater degree of control over who can and cannot make use of the network.

Use case: Corporate campus guest Wi-Fi

An optimized, high-performing Wi-Fi environment demands good, clear policies, processes, procedures and quality of service standards. Ongoing configuration and management are required to customize security and compliance policies for different types of users, enforce them, and keep current with the latest websites and applications.

Because guests and corporate employees both use the same shared network resources, monitoring data can help set and refine policies on how many guests can access the network at any given time and how much bandwidth can be allocated to each guest. Companies need to ensure guests are restricted to an assigned bandwidth allowance and are not able to interfere with core business-related traffic.

Who gets to access which content?

As noted previously, different types of users need to access different resources. Visitors may need to get on the public Internet but not the internal corporate network. Contractors, who are a hybrid of guest and employee, may need access to certain corporate resources – but with restrictions based on their role, or on time of day (e.g., only within business hours).

Even different devices can require their own privileges. If an employee brings her own device to work, that device won't likely fall under the company's mobile device management system. Its access privileges may need to be altered according to the corporate security policy.

Access to specific websites or applications also need to be controlled to ensure guests don't violate corporate acceptable use policies with inappropriate content or prohibited applications.

Use case: Guest Wi-Fi for retail

Retail guest networks are typically more open than corporate networks. Any in-store customer can join the network – and is often encouraged to do so. In many cases, the "balance of power" is with customers: they get bandwidth priority as long as staff have what they need to run transactions.

Given the openness of retail Wi-Fi, security is a key concern: defences need to be in place to protect against peer-to-peer attacks, malware and intrusions. That means the guest network should be able to block malicious or inappropriate domains when users are on the web. Content filtering can also be used to prevent guests from viewing certain websites or accessing illegal applications via the connection supplied by the business. Most retail Wi-Fi access is provided through portal-based splash pages for two reasons:

- Splash pages provide an easy way to collect information about guest users. This creates the opportunity to start an ongoing conversation with that customer – to push new content, present special offers, manage loyalty programs and more.
- Splash pages help establish and reinforce the corporate brand through imagery, tagline, copy style and featured products and services. When users then encounter those elements elsewhere on the web, there's instant brand recognition.

Tracking usage for ongoing optimization

Companies should monitor and track how and when users access their wireless network, including which devices and applications they use and which sites they visit. It's important to understand how the full mix of online activity affects the network and the user experience. The insights gained can assist in the development of productivity-boosting apps for employees and enable more targeted marketing campaigns for customers (by understanding customer behaviours).

How a managed service provider can help

Given the diversity of wireless users, devices and requirements – and the growing dependence on wireless work – managing the corporate Wi-Fi network can be a full-time job. It's also become extremely complex, requiring specialized skillsets and experience to operate and get the most value from the management tools and capabilities built into network components and software.

Separate from managing the network, there's the additional challenge of troubleshooting, which can require a full-time, round-the-clock help desk – and is costly to maintain. And increasingly, staff are also being tasked with improving business Wi-Fi performance and enhancing the user experience, which is both vitally important and an additional strain.

For all of these reasons, many companies are choosing to have a service provider design, deploy and manage their entire wireless ecosystem.

What's included in a managed Wi-Fi service

A managed service provider will take on all aspects of Wi-Fi network and account management, configuring the policies that ensure guests and visitors can quickly and easily get the access they need – with the appropriate permissions and privileges.

Managed service providers can also offer powerful security capabilities that continuously scan and protect the network environment against threats like malware, phishing and ransomware. They can automatically update features, tools and device/application profiles to ensure businesses are always using the latest and most advanced Wi-Fi capabilities.

Even though the service provider takes on all of the day-to-day management of the network, businesses can still have full visibility and insight into how and when the network is being accessed through an online dashboard. That way, they can use metrics such as visitor capture rates, visit times and repeat visits to identify new opportunities for user engagement – leading to more finely targeted marketing campaigns as well as the ability to tailor access and application usage policies to optimize the user experience.

In many cases, the managed service is a cost-effective way to ensure the Wi-Fi network operates at peak productivity and delivers the best possible user experience – freeing up in-house staff to contribute to initiatives of more strategic importance to the business.

The Bell approach to managed Wi-Fi

Bell takes a turnkey approach to managed Wi-Fi, addressing the full range of needs organizations have – whether in the corporate setting or a retail environment.

We provide expert guidance and advice on network design and configuration, combining network-based defences and highly secure layer-3 firewalls to protect the network and devices from attacks.

Transparency and visibility are assured through a single cloud-based dashboard so that organizations can monitor network performance and bandwidth consumption at all times.

We can manage network service options and help optimize network performance by prioritizing business-critical applications.

Leverage metrics such as visitor capture rates, visit times and repeat visits to build stronger customer relationships and deliver an exceptional user experience.

Bell experts handle all updates and upgrades to ensure customers' Wi-Fi networks use the latest, most advanced wireless capabilities.

Bell Managed Wi-Fi is a cost-effective, fast and highly scalable solution. Running on Canada's largest IP network with the most points of presence in the country, it supports speeds up to 10 Gbps and can scale to accommodate tens of thousands of devices.

Bell Managed Wi-Fi is backed by the responsive support and capabilities of more than 3,000 technology professionals, across the country.

To discuss how your business can take advantage of Bell Managed Wi-Fi visit **bell.ca/managedwifi** or contact your Bell representative for more information.