Managed Wi-Fi: Turning enterprise WLAN from an overhead to a business advantage

Ubiquitous wireless connectivity has fast become a reality with progressive enterprises using cutting-edge technologies to enable lightning-fast data services. Across all industries and sectors – Wi-Fi (or WLAN) is imperative to make every second of the business hours productive. With BYOD becoming a norm and IoT growing exponentially, high-bandwidth Wi-Fi networking is an implied mandate today and statistics indicate that the demand for it will only intensify going forward. For instance:

- Network traffic is expected to exceed 70 exabytes per month by 2022
- In 2023, the number of connected devices will be more than thrice the then global population
- There will be more than 38 billion enterprise devices connected simultaneously by 2025

Combine this with the spectre of COVID-19 outbreak that has accelerated the adoption of a virtually connected, physically distant lifestyle and work culture. In the post-pandemic era, besides extending remote work, enterprises will have to encourage physical distancing within office premises. The typical office layout will change considerably and employees will be seen working from the library, cafeteria, pantry, lobby, corridor or any corner they prefer in order to avoid being too close to each other to be safe. The WLAN in that emerging era has to be consistent and secure at every of the office premises. **To establish such a Wi-Fi network, there are a few critical factors that must be taken into consideration:**

02

Number and Placement of Access Points (APs)

If there are few routers or APs in the network, there's bound to be coverage gaps. However, excessive routers also make the connection unstable. The optimum number of routers depends upon the overall arrangement of controllers and other network components.

The placement of APs is, of course, crucial for total coverage and strong connectivity, especially indoors. Even the angle of routers' antennae makes a considerable difference in the network coverage. Any antenna position works fine for APs operating on 5 GHz, but that's not the case with 2.4 GHz APs. Their antennae have to be positioned in specific angles for optimum results.

Radio Frequency Interference (RFI)

The strategic placement of APs and the positioning of the router antennae can go for a toss if the RFI is not factored in at the time of setting up a wireless network. Other wireless devices, such as security systems, RFID devices, cordless telephones and Bluetooth devices within premises also operate on 2.4 GHz and 5 GHz frequencies (though not necessarily). As a result, they frequently interfere with Wi-Fi 4 and Wi-Fi 5 networks, both of which also use the same frequency. This increases latency and slows down the internet access speed, resulting in poor employee and customer experience. Depending upon the extent of the RFI, Wi-Fi connectivity disruption may range from nominal to significant. These disruptions can increase in intensity indoor due to the additional obstruction from walls, huge cabinets and so on. A thorough survey of the entire premises and adjoining spaces is required to identify all sources of RFI and plan the AP placement accordingly. It is a complicated task that yields the desired result only when it's done with the right process by the people who have the required skill set.

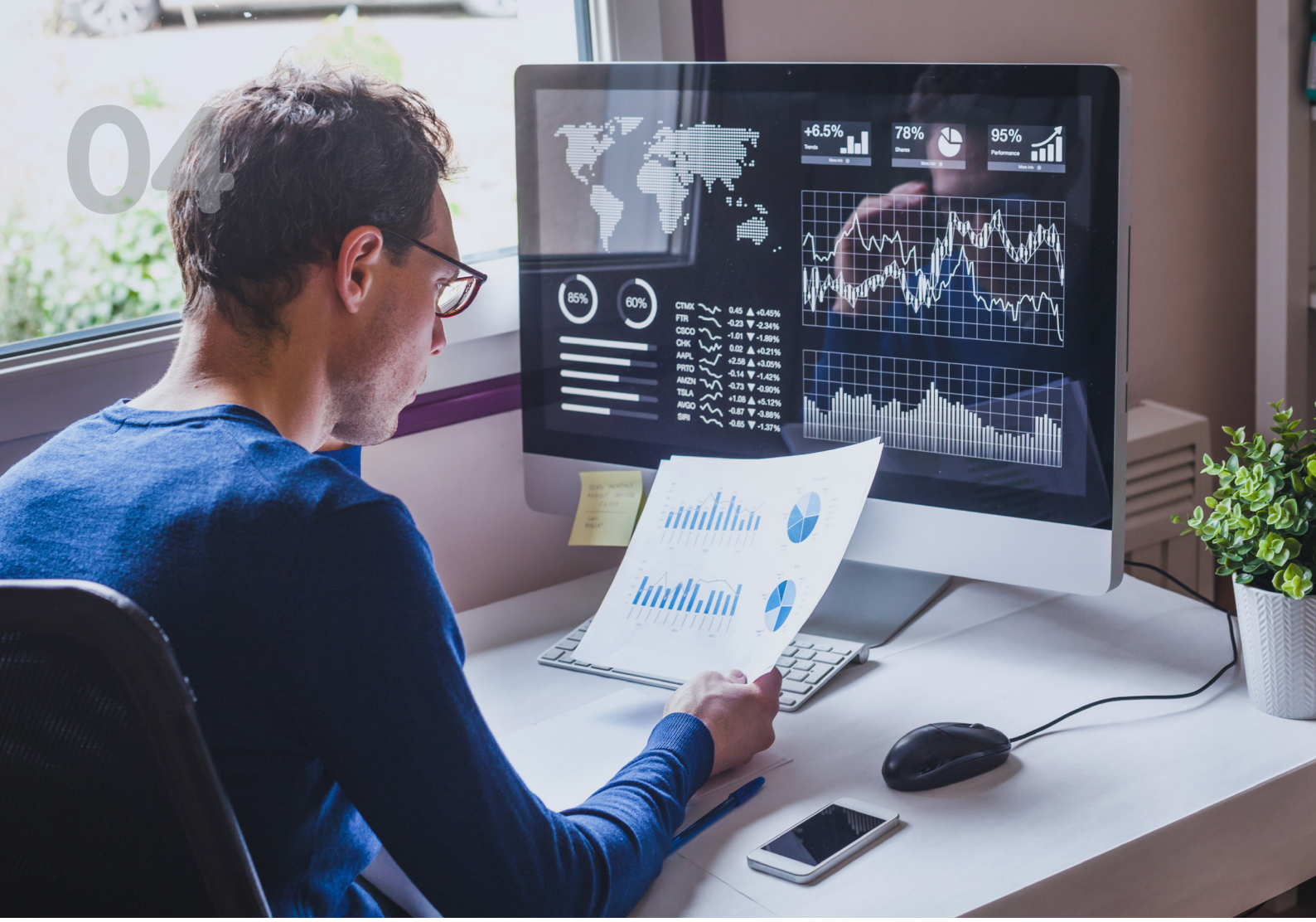
03

User Discretion

Broadly, users are either ‘employees’ or ‘others,’ and the network access criteria must be different for each. Of course, there are hierarchies amongst employees too, and not everyone can have access to every enterprise resource. Setting up separate APs using SSID technology keeps private enterprise network insulated from activities happening on the public Wi-Fi. Not maintaining such profile-based user authentication and access restrictions not only mars user experience but also jeopardise the enterprise data security. An even better option is to set up a completely separate Wi-Fi hotspot especially if extremely sensitive information is stored within the network.

Network Security

The task of configuring enterprise Wi-Fi becomes more complex when cybersecurity is taken into consideration. An ad hoc network or a rogue AP in the vicinity is an ever-looming threat to privacy as enterprise devices get tricked into sharing data with these systems. This is in addition to the always-lurking threat of DDOS, KRACK, man in the middle and other deliberate cyber-attacks that are a threat to both customer and organizational data privacy. Without a fool-proof, layered security framework, a single attack is enough damage the enterprise reputation for a long term or permanently.



Manageability

Enterprise IT teams battle with these challenges daily. However, as the demand for wireless internet access grows exponentially, the traditional topological model of network management is no longer effective. It consumes a lot of time and is prone to errors due to extensive manual work. This leads to further management complexities as IT staff members not only have to frequently resolve issues occurring due to their/peers' mistakes.

Besides, since Wi-Fi is a constant requirement, IT teams have to be on their toes 24x7 to resolve network issues quickly, unlike patching the enterprise devices, which can be done in batches when machines are not in use. A significantly large pool of professionals is required for each office location in order to resolve each incident within reasonable time and ensure minimum downtime. Thanks to globalisation, a seemingly uncountable number of businesses operate from more than one office. The complexity and cost of managing enterprise-wide WLAN increases exponentially as an adequately large IT team is required for each office location that is added to the mix.

Globalisation, BYOD and enterprise mobility are disruptive forces that have transformed how enterprises operate. The benefits of these technological advancements can be optimally reaped only when the challenges pertaining to them are adequately resolved. Similarly, for establishing a pan-organization wireless network, thorough assessment of the premises and adjoining areas, meticulous network planning, robust security and carefully defined accessibility control are imperative. Besides, after the network is established, the team that manages it must have a deep understanding of genre of Wi-Fi technology, cyber threats and relevant security protocols and 24x7 availability.

Optimising business productivity with Managed Wi-Fi

There are a number of platforms that allow centralised management of WLAN. However, they are not available as plug-and-play and one-size-fits-all since every organization has its unique requirements and expectation. These challenges, complexities and constraints have given rise to a new genre of service – Managed Wi-Fi.

As the name indicates, Managed Wi-Fi is the practice of outsourcing the configuration, management, monitoring and troubleshooting of WLAN. There are several technology providers that offer this service. They not only set up the network and provide the on-going support but also offer analytics for granular visibility and certain custom features per the organizational requirement.

Configuring and managing the next-generation enterprise WLAN can be done in-house with the same effectiveness. However, that would require a significantly larger IT team than what most enterprises currently have. That is why companies across business domains are increasingly opting for Managed Wi-Fi, even more so because it brings some parity between IT and non-IT enterprises and makes up a more levelled field for competition.