



# Enterprise Wireless

End-to-end wireless solutions for corporate connectivity.

## Introduction

WiFi was first introduced in the late 1990s, it was in its infancy stages then. It did not have much of a presence anywhere. Then the decade of 2000s saw an optimism towards WiFi with more people being interested in the technology and what it could offer to the world. It was in the decade of 2010s that the world started adopting WiFi at a steady, rising rate. However, Enterprises had still steered clear of WiFi because of its security concerns. However, in the later years of the decade of 2010, as mobile devices became more prevalent in enterprise environments and employees needed mobility and flexibility of work location, WiFi became the technology of choice in offices and work environments.

Today, WiFi technology has become the de-facto LAN connectivity for modern enterprises. With wide adoption of Bring-Your-Own-Devices (BYOD) and work from anywhere culture, WiFi has replaced Ethernet and soon offices will have only wireless infrastructure for connectivity. However, WiFi does come with its own challenges especially regarding security. Unlike Ethernet, WiFi signal can be accessed by anyone so it is imperative for enterprises WiFi networks with very strong security posture. Additionally, WiFi networks are mired with performance issues and high latency since they operate in unlicensed spectrum.

Employees today expected very fast and reliable connectivity since most of their work is highly dependent on Internet connectivity. Most of the enterprise applications are moving to the Cloud so corporate users need always-on, high performance and super reliable wireless networks. The wireless access points should handle dense users since lot of users remain connected to single access point. IT administrators need centralized tools to configure and monitor the health of the wireless and lot of insights to quickly troubleshoot any issues that may arise.

Listed below are some of the key requirements for the enterprise wireless networks -

## Key Requirements Enterprise Networking

- Fast and Trustable WiFi networks
- Network Security
- BYOD management
- Seamless user onboarding
- SD-WAN
- Policy Management
- Branch networking
- Dynamic VLANs
- Real-time Network Analytics
- Integration with LDAP / AP / G-suite

## Wireless for Enterprise

### Security

One of the primary concerns of any network is security. However, this requirement takes highest priority when it comes to enterprise wireless networking. Trustable networks with central health monitoring and deep security analytics are imperative in enterprise WiFi. Integrated access control mechanisms, offering strong 802.1x (WPA2 Enterprise) and other methods of user authentication should be provisioned to ensure secured networking. External, as well as internal threat agents should be identified and isolated.

### **High Availability**

Enterprise WiFi networks cannot afford to have downtimes. Downtimes can result in potential delays in deliverable deadlines which can have adverse effects on future projects. While enterprises ensure that there are redundant internet connections, that in itself is not sufficient. It is important to have the necessary technology to utilize that bandwidth across all network elements while optimizing the cost of bandwidth as much as possible. You need a network controller that provides SD-WAN capabilities that utilizes the Internet backbones efficiently, provide load balancing and failover rules while offering advanced RRM functions to utilize the radio resources efficiently.

### **High performance**

Enterprise users expect highly reliable and fast connectivity to conduct their office activities. Even a small downtime or under-performing network, causes loss of revenue for the enterprise. As more and more wireless devices get used in offices, the IT admins need to build a high performance and high-density wireless network to provide optimum experience to all the office users.

### **Dynamic VLAN Management**

Offices often deploy multiple VLANs to segregate the traffic of users from different groups. It is impractical for IT admins to manually assign each user to separate VLAN and track their usage. The network access controller (e.g. UniNac) needs to perform this task. The controller is responsible for authenticating the users and assigning them to the right VLAN based on the group they belong to.

## **Policy Management Function**

Generally, all corporate networks are deployed on single physical network and each user is assigned to specific VLAN based on their organization group. IT managers need to assign different access rules and polices for each group. This ensures that users are given different class of service and the network performance is kept optimal. The network controller should be able to assign different types of network rules for forwarding and routing packets, filtering web URLs, providing QoS to various applications, etc.

## **Network Monitoring System**

The administrator must, at all times, know what is happening on the network. Real-time usage analytics, health and status of APs, user activity reports, all are necessary to optimize the network. High network visibility is an important trait of a good network design. When it comes to wireless deployments on a larger scale, there might be hundreds of Access Points set up across various locations, it's important to get a single console health status of all Access Points and users connected to the network.

## **Multiple WAN & Load Balancing**

Enterprise networks need to operate 24x7x365 so businesses, provision multiple ISPs connections to handle failover, redundancy and speed requirements. However, if one ISP fails, the network should seamlessly transition to the standby ISP through a responsive failover mechanism. Bandwidth should be aggregated properly across all internet connections to ensure optimum utilization of all resources.

### **LDAP / AP / G-suite Integration**

In any wireless network, having integrated active directories help people manage the access of users through a central console. The IT administrator can easily onboard newer users into the network and assign them access of the network as per their department. Active directories help administrators know which department a certain user belongs to, and for which departments should the user be given access to. LDAPs help facilitate easy addition and removal of users from entire networks.

### **Branch Networking**

As companies expand, they open branch offices that are distributed across several geographies. However, the branch offices need secure and reliable connectivity to the central office to access corporate applications and regular use. Additionally, the modern workforce is increasingly becoming mobile. People need to work from anywhere, anytime. In case of pandemic situation like Covid-19, work-from-home has become a norm for most companies and will continue to do so for the foreseeable future. It is important to design a corporate network that will handle remote users and allow remote offices to seamless connect to the central network.

### **Dynamic VLAN management**

Enterprise WiFi solutions must be able to manage multiple LAN subnets and VLANs. VLANs & their management is necessary because they combine various sections of a department which work in unison, but are physically separated. Dynamic VLAN management is a crucial aspect of enterprise WiFi design.

## Deployment Challenges

- Network design & planning
- Reducing network latency and improving reliability
- Protect data and privacy
- RF design and planning
- Performance planning
- Vendor selection
- Integrating multi-vendor hardware

## How we help Enterprises with their networking.

UniNac, our network access controller an ideal security and network controller for modern networks. It is designed to seamless work with our UniMax access points and managed switches to provide a single, unified wireless network. UniNac can handle an unlimited number of UniMax Access Points in its network and comes with multiple variants based on number of concurrent users. UniNac comes with an inbuilt Network Monitoring System, which gives the administrator real-time visibility of the entire network and the complete control on the deployed network. The administrator can configure policies based on bandwidth, policy and routing that are to be applied to end-users as a whole or isolated to certain VLANs.

UniNac and UniMax Access Points come in different models to support different use-cases. UniNac when working with UniMax APs works as a network monitoring system from where you can control and configure all UniMax APs in the network through the UniBox Dashboard.

UniNac comes with a load balancing mechanism that utilizes all available bandwidth effectively by aggregating it between connected ISPs. If in case the primary connection fails, then UniBox smoothly transitions on to the secondary or standby connection with a responsive failover mechanism. This ensures that downtimes are kept as low as possible at all times, this is especially important for enterprise where data is constantly being moved over the network.

### **Key Features of UniNAC**

- High Availability
- 802.1x Authentication
- Total network visibility
- Policy Enforcement
- Endpoint Compliance checks
- Dynamic VLAN assignment
- Scanning and profiling endpoints
- Device fingerprinting
- Track user activity sessions
- Real-time network intelligence
- Branch Networking capabilities
- Rogue AP detection
- VPN Concentrator
- Zero Touch Provisioning

Although it is best practice to use original manufacturer deployments for optimum experience, Indio's solutions are vendor-agnostic and work with hardware from any



vendor.

## Implementation

We deploy a system consisting of UniNac, our integrated network access controller which controls UniMax Access Points connected through our PoE managed switches. UniNac controller is placed between the ISP and the Access Points. L3 switches connect the ISP to the UniBox, and L2 switches connect the Access Points to the UniBox.

UniNac network access controller can manage and control an unlimited number of UniMax APs in its network.

All access points can be managed from the cloud or on-premise controllers or can be managed individually. They are capable of handling up to 256 concurrent devices and speeds of 2200 Mbps on both 2.4 and 5 GHz channels.

The access points come with latest features like SD-WAN, software-defined radios, dynamic policies, SSID-based VLAN, dynamic channel assignment, presence, application filtering, guest access and more. They deliver high performance, better coverage and high throughput while saving time and money for enterprises. Indio's Trinity Series, managed PoE Switches help network administrators deploy high performance, complex wireless networks. PoE switches allow administrators to power the remote access points, IP camera, IP phone from central place while delivering energy saving and ease of management.

Managed POE and non-POE switches support latest 802.3af / at standards that provide self-adaptive and high power on each port. Each port delivers Gigabit speed allowing high throughput for each connected appliance. The switches can be easily stacked using 2 SFP ports for uplink. The 24 port PoE switch comes with a 450W power supply while the 8 port PoE switch comes with a 120W power supply that can supply 30W per port. Both the switches can power devices up to 100 meters away.

Our solution offers a complete, single vendor deployment that takes supports all your enterprise WiFi requirements.


### Solution Benefits


We have served multiple enterprises with our solutions. Here are a few ways in which our solutions have impacted people and enabled enterprises to leverage wireless to their comfort and drive growth:

- UniNac solved all user provisioning problems
- Helped ease onboarding of users
- Central policy management for better control
- Endpoint management simplified
- Network uptime increased after deployment of system
- Achieved full coverage of enterprise area
- Dashboard helped administrators monitor the network
- Seamless failover mechanism for smooth transition

*Connect with our sales team and fortify your enterprise network.*

 [sales@indionetworks.com](mailto:sales@indionetworks.com)

 US: +1 (888) 280 4112

 IN: +91 (20) 6715 7379