Indio Networks

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, WiFi security made revolutionary advances, with the paradigm of software-defined networking starting to take over.

Today, with more remote workplaces than ever before, and a dynamic Bring-Your-Own-Device (BYOD) culture, Enterprises have not only started looking at WiFi & software-defined networking, but are also adopting wireless solutions which best serve their interests. Enterprise network design is challenging, solutions that cater to enterprises require a whole new level of authentication and network securing abilities. It is important to forge highly trustable networks for enterprises. A network which guarantees end-user protection and security to the entire network itself is the key to enterprise network design. The other key requirement of enterprise networks is speed.

Enterprise networks move sensitive data upwards of gigabytes on a daily basis. Enterprises need solutions that can efficiently handle all the data being moved around without it getting entangled between internal networks, a problem caused by interference. Management of bandwidth, separation of VLANs, and many other sub-services enabled by software-defined networking hold the key to deploying wireless solutions for enterprise.

Key Requirements Enterprise Networking

- Fast and Trustable WiFi networks
- High Availability clustering
- 802.1x Auth & Two Factor Auth
- Multiple WAN & Load Balancing
- Bandwidth Management
- VPN tunnelling for branch networking
- Network Monitoring System
- Policy-based networking for VLANs
- Integration with LDAP / AP / GSuite

In Depth on Wireless for Enterprise

Security

One of the primary components of any network is strong security. However, this requirement takes highest priority when it comes to enterprise wireless networking. Trustable networks that create secure perimeters with active device and AP monitoring services are imperative in enterprise WiFi. Integrated access control mechanisms, offering 802.1x 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 multiple primary as well as secondary standby internet connections, that in itself is not sufficient. It is important to have the necessary technology to utilise that bandwidth across all network elements while reducing loss of bandwidth as much as possible. You need strong network hardware consisting of high concurrency, high density Access Points and a High Availability clustering enabled Network Controller which can manage all of those Access Points.

High performance

Enterprise networks should be built on reliant, secure architectures which offer high speed & high throughput. Enterprise WiFi encourages and allows BYOD policies, because of this radical change in how enterprises operate, it is important for its networks to securely integrate these devices into the network and manage all of those devices while maintaining high performance

Dynamic Bandwidth Management

Enterprises utilise very high bandwidth. But bandwidth in itself is not intelligent. This is where the paradigm of software-defined networking comes into the picture, software-defined dynamic bandwidth allocation policies intelligently decide which resources need higher bandwidth and allocate it as resource requirements scale.

Policy Management Function

Enterprises consist of multiple departments. While all of them operate on the same physical network, they are separated by VLANs, which are logical networks, to make sure that they don't interfere with each other and keep away from the data of a different department. The bifurcation of networks allows administrators to configure policies on the network that apply to groups. These policies can be routing policies, access policies and bandwidth policies.

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 optimise the network. High network visibility is an important trait of 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 heat maps of each Access Point to check for coverage holes.

Multiple WAN & Load Balancing

Enterprise networks are almost never down, they provision multiple ISPs to support their 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 utilisation of all resources.

LDAP / AP / Gsuite 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 f rom entire networks.

Branch Networking

Workplaces are fragmenting. As companies fragment, offices expand and are distributed across several geographies, it becomes a challenge to integrate all of these networks under a consolidated network which seamless transports data from one remote working centre to another. Branch networking capability creates VPN tunnels across offices and facilitates secure channels of communication between them.

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 RFI
- Ensuring robust security
- Protect data and privacy
- RF design
- AP placement

How we help Enterprises with their networking.

UniNac, our integrated enterprise-grade network access controller is capable of controlling and managing the entire network consisting of Falcon Series UniMax Access Points, which are also enterprise grade with very high concurrency support. UniNac can handle an unlimited number of Falcon UniMax Access Points in its network. Both devices come with an inbuilt Network Monitoring System, which gives the administrator real-time visibility of the entire network and the devices connected to it. 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 utilises 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 practise 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 Falcon Series UniMax Access Points connected through our Trinity series PoE 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 Falcon Series UniMax APs in its network.

All Falcon 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.

Trinity 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. Both the switches can power devices up to 100 metres 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.

sales@indionetworks.com

+020-67157377

+020-67157373