BLUEZEN
Transforming Connectivity

DESIGN GUIDE: WIRELESS ACCESS

Efficient and Scalable Network design with Advanced Controller and Gateway Management

TABLE OF CONTENTS

BLUEZEN NETWORK DESIGN

GIGABIT END-TO-END WIRELESS SOLUTION WITH FULL SECURITY AND COMPREHENSIVE MANAGEMENT

INTRODUCTION

BlueZen Technologies delivers the most advanced solutions for designing, deploying and optimizing 802.11 a/b/g/n/ac Gigabit wireless LANs for maximized performance, security and management. Expert planning and design tools ensure the wireless network is built to accommodate the highest capacity of users, meets the needs of demanding wireless applications, and performs optimally in the most challenging RF environments.

BZ SMART solution consists of Enterprise-Class access points (APs) that are managed by the Unified Controller, the Command Control Centre that administrators use to configure and manage their wireless networks. With proper sizing and placement of the APs, the BZ SMART wireless solution can be used to provide pervasive, reliable wireless connectivity in many different types of deployments and applications. And, it can be used to manage thousands of users.

For centralized management of high density users, it is important to have an enterprise class, unified controller with both **Access Point Management and Subscriber Management**. It can be adapted in a rapid manner to special implementation needs required by certain enterprises, colleges and government agencies, thus making the platform even more unique. Its powerful relational database engine empowers administrators with the ability to manage medium to large-scale Wireless Networks

BENEFITS OF WLAN SOLUTION

Local Area Networks (LAN) have been used for interconnecting computers and resources in various networking environments. Cables have typically been used as the physical medium in these LAN environments. Sometimes it may not be possible or practical to install cables, but network connectivity is required. Using wireless connections allows portable computers to still be portable without sacrificing the advantages of being connected to a network. Furthermore, the increased use of mobile phones and Personal Digital Assistant (PDA) devices is driving the workforce towards a more mobile working environment. Due to bandwidth limitations and expensive technologies, cellular data networks, such as Global Systems for Mobile Communications (GSM), are not suitable for local area high speed data networking.

Wireless LANs provide the needed mobility in these working environments, enabling a user to access the network services away from the desk. Wireless LANs use electromagnetic airwaves (radio or infrared) to communicate information from one point to another without relying on any physical connection.

The widespread reliance on networking in business and the meteoric growth of the Internet and online services are strong testimonies to the benefits of shared data and shared resources. With wireless LANs, users can access shared information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires. If I want to mention more about the benefit, then the support for mobility, easy installation, cost effectiveness and support for novel applications will come first

MOBILITY

Mobility is a significant advantage of WLANs. User can access shared resources without looking for a place to plug in, anywhere in the organization. A wireless network allows users to be truly mobile as long as the mobile client is under the network coverage area.

Mobility is why companies go wireless. In larger campus type settings, IP addressing and user mobility across various network segments will become increasingly important. Employing a robust security solution will also become increasingly complex. It is therefore critical to enable robust mobile solutions with the required built-in security

RANGE OF COVERAGE

The distance over which RF and IR waves can communicate depends on product design (including transmitted power and receiver design) and the propagation path, especially in indoor environments. Interactions with typical building objects, such as walls, metal, and even people, can affect the propagation of energy, and thus also the range and coverage of the system. IR is blocked by solid objects, which provides additional limitations. Most wireless LAN systems use RF, because radio waves can penetrate many indoor walls and surfaces. The range of a typical WLAN node is about 100 m. Coverage can be extended through innovative techniques and true freedom of mobility achieved via roaming. This means using access points to cover an area in such a way that their coverage overlaps each other. Thereby the user can wander around and move from the coverage area of one access point to another without even knowing he has, and at the same time, seamlessly maintain the connection between his node and an access point.

EASE OF USE

WLAN is easy to use and the users need very little new information to take advantage of WLANs. Because the WLAN is transparent to a user's network operating system, applications work in the same way as they do in wired LANs.

INSTALLATION SPEED, SIMPLICITY AND FLEXIBILITY

Installation of a WLAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings. Furthermore, wireless LAN enables networks to be set up where wires might be impossible to install.

SCALABILITY

Wireless networks can be designed to be extremely simple or complex. Wireless networks can support large numbers of nodes and large physical areas by adding access points to extend coverage.

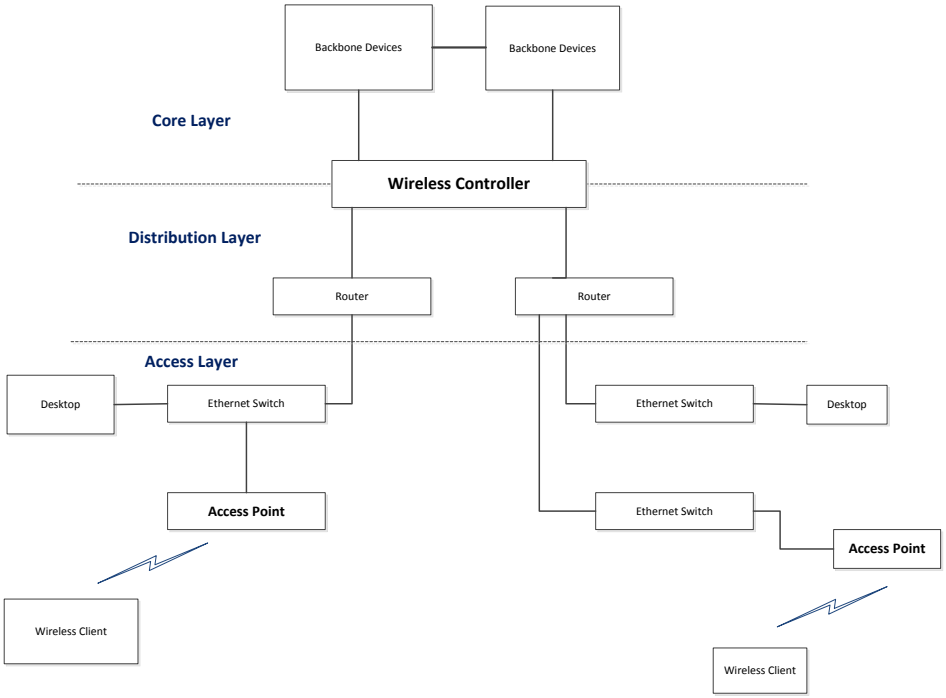
AFFORDABILITY

Wireless LAN installation and costs over the life of the product can be significantly lower than, those incurred with wired networks, especially in environments that require frequent moves and modifications

WLAN systems run either as an adjunct to the existing wired enterprise network or as a free-standing network within a campus or branch, individual teleworker, or tied to applications in the retail, manufacturing, or healthcare industries. WLANs must permit secure, encrypted, authorized communication with access to data, communication, and business services as if connected to the resources by wire.

WLAN CONTROLLER BASED ARCHITECTURE

The controller based wireless LAN consists of wireless controller, access points and clients that have a wireless LAN connectivity. Finding the optimal locations for access points is important, and can be achieved by measuring the relative signal strength of the access points. Placing the access points in a corporation network opens an access way to the resources in the intranet. And managing the complete network centrally became easy with the presence of Wireless Controller.



The clients that wish to join the wireless network need to know the SSID (Service Set Identifier) string that identifies the network. When the client enters the coverage area of an access point in that network, it can start associating with an access point. The authentication methods supported by the current 802.11 standard are Open System and Shared Key. The Shared Key method requires that the WEP algorithm be implemented on both the wireless client and the access point. In the Open System authentication scheme, which is the default scheme, a client announces that it wishes to associate with an access point, and typically, the access point allows the association. To restrict access to a wireless network without WEP, most wireless LAN product vendors have implemented an access control method, which is based on blocking associations from unwanted MAC addresses on the access points. A list that contains the MAC addresses of valid network cards can be defined in the access points, and any client trying to associate with a card whose MAC address is not on the list, is denied association and thus cannot use the wireless LAN interface.

If no authentication or encryption methods are used, the WLAN can create a security risk if the radio signals flow outside the office building. An intruder, who knows the SSID that identifies the WLAN, could configure a device to operate on the same network and frequency as the access points and gain access to the network if no MAC address blocking were used. With proper tools, intruder

could eavesdrop on the data the other legitimate users were transmitting. It is also possible to counterfeit MAC addresses used on the network cards, so after learning an authorized MAC address, an intruder could program her card to have the same MAC address, and gain access to the wireless LAN. Using the cards at the same time would of course lead to networking problems. To prevent eavesdropping and unauthorized access to the WLAN, other security measures should be implemented if the transmitted data is valuable to the business. And the above mentioned security and authentication can be very well controlled/managed by the advanced wireless controller.

WLAN (Wireless) controllers – are devices that significantly simplify the work of administrators in wireless LAN installations and configurations. New access points are configured and the security settings for a wireless LAN installation are monitored and managed from a central location with controllers.

So, in order to make sure that the entire network is completely secured and reliable, one should always go with the unified controller based solution. BZ SMART Enterprise Class WLAN solution consists of two main components: the WLAN-AP Access Point and the WLAN Controller, which combine to provide the fastest and most cost effective entry to the rapidly growing Wi-Fi mobility market.

A single central controller can manage all of the Access Points at all sites assuming that the wireless LAN controller can break-out local data and integrate remote access points. This enables employees to use their notebooks everywhere in the WLAN without having to re-configure anything. The IT administrator can be sure that the same WLAN security guidelines are active at all sites throughout the company. The only requirement is an IP connection between the sites.

If a controller fails, the wireless LAN can continue to operate as the access points optionally operate in standalone mode. Standard WLAN functions, which do not necessarily have to run on the controller, will continue to function without problem (e.g. SSID with WPA2, pre-shared key is bridged in the local network). Functions such as the authentication of clients by RADIUS/EAP via the controller, monitoring, intrusion detection, rogue access points detection or dynamic RF optimization are not available. Redundant systems can be set up by assigning each access point

with an alternative controller in addition to its primary controller. If the main controller fails, the replacement controller can take over the monitoring functions.

BZ SMART WLAN controllers are ideal for WLAN infrastructure for multiple user groups and applications such as for data, voice-over-WLAN and WLAN guest accounts. As "smart controllers", they forward the data depending on the application or even the user — by switching user data at the AP for maximum performance, by separating the LAN into a dedicated VLAN for WLAN guest accounts, or by tunneling [using BlueZen Encrypted Tunnel the user data to the controller for roaming between IP subnets. The flexible switching options ensure that the WLAN controller does not end up being a central bottle-neck. Even remote sites are easily integrated into the centralized management over an IP connection for greater convenience.

WIRELESS DESIGN CONSIDERATIONS

Numerous factors must be considered before designing a wireless system. While not all design considerations may apply in every instance, they should be addressed for each project. Many of these considerations should be discussed with the client before making any formal recommendations for a wireless solution.

RF PLANNING:

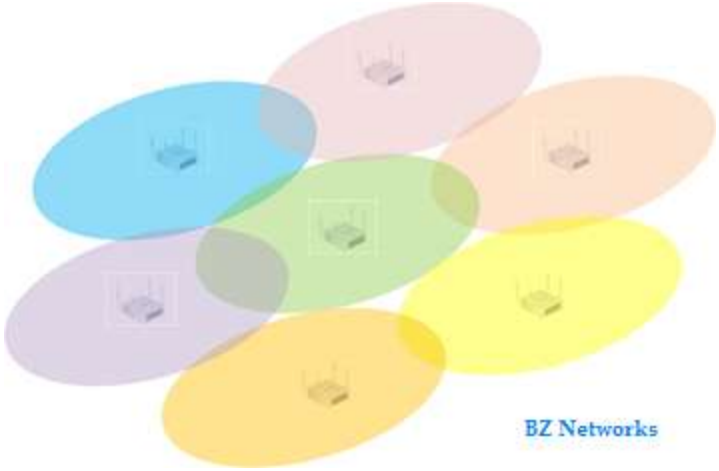
RF Planning is the process of assigning frequencies, transmitter locations and parameters of a wireless communications system to provide sufficient coverage and capacity for the services required.

RF COVERAGE AND CAPACITY:

Coverage relates to the geographical footprint within the system that has sufficient RF signal strength to provide for a call/data session. Capacity relates to the capability of the system to sustain a given number of subscribers. Capacity and coverage are interrelated. To improve coverage, capacity has to be sacrificed, while to improve capacity, coverage will have to be sacrificed. This is the place where BlueZen plays a vital role in optimizing the coverage and capacity.

RF SITE SURVEY:

RF Site Survey is the process of planning and designing a wireless network, to provide a wireless solution that will deliver the required wireless coverage, data rates, network capacity, roaming capability and Quality of Service (QoS). The survey usually involves a site visit to test for RF interference, and to identify optimum installation locations for access points. This requires analysis of building floor plans, inspection of the facility, and use of site survey tools. Interviews with IT management and the end users of the wireless network are also important to determine the design parameters for the wireless network.



As part of the wireless site survey, the effective range boundary is set, which defines the area over which signal levels needed support the intended application. This involves determining the minimum signal to noise ratio (SNR) needed to support performance requirements.

RF site survey includes examining the existing network, understanding the network requirements, testing the signal ratio and suggesting the optimum solution. The solution has to be in complying with the existing network, to make it optimum. This will aid designers later on in the deployment when defining the architecture and bill of materials for the wireless network.

WLAN SSID ALLOCATION:

SSID:

In WLAN computer networking, a **service set identifier** (**SSID**) is a code attached to all packets on a wireless network to identify each packet as part of that network. The code consists of a maximum of 32 alphanumeric characters. All wireless devices attempting to communicate with each other must share the same SSID. Apart from identifying each packet, SSID also serves to uniquely identify a group of wireless network devices used in a given "Service Set".

MULTIPLE SSID:

Multiple SSID modes, also called Virtual SSID in which, it is possible to create up to 4 virtual standalone Access Points for each Wi-Fi network card in the system. It is clear that virtual SSIDs belonging to the same Wi-Fi AP share the radio channel being used, and thus the available bandwidth. Moreover, for each virtual SSID it is possible to establish a standalone authentication and encryption scheme (plain-text, WPA-PSK, WPA Enterprise or WEP at 128 bits).

SSID ALLOCATION:

In the same office for different department, we can use different SSID with different authentication to have an independent and secured connectivity.
On the other hand, SSID allocation will not be suitable for scenarios where in mobile users are more, since they will be facing the problem of hand-over (i.e.)... The mobile users cannot switch over from one network to other while in roaming.

WIRELESS USER AUTHENTICATION: (SECURITY)

BlueZen Access Systems are designed with highly secured protocols, which include the following security features:

- 64/128/152 – Bit Encryption
- MAC address filtering
- WPA-PSK,WPA2-PSK
- WPA-EAP and WPA2-EAP
- SSID Broadcast disable function

- 802.1x user authentication
- Intra VAP Isolation
- Peer-Peer Isolation
- Radius Authentication
- VLAN Management

WIRED EQUIVALENT PRIVACY (WEP)

WEP is an older network security method that's still available to support older devices, but it's no longer recommended for a secured network. When you enable WEP, you set up a network security key that encrypts the information sharing between the devices in the same network.

WI-FI PROTECTED ACCESS (WPA AND WPA2)

WPA and WPA2 require users to provide a security key to connect. Once the key has been validated, all the data shared between the computers/devices and the access point has been encrypted.

RADIUS AUTHENTICATION

As is the case with any valuable resource, there must be limitations on who can access and use your wireless medium. Controlling access to computer resources is best illustrated in the AAA framework: Authentication, Authorization, and Accounting.

Authentication is the ability to identify a system or network user through the validation of a set of assigned credentials. If you have ever been prompted for a username and password when turning on your computer, you have experienced authentication first hand. Authorization defines the ability of a specific user to perform certain tasks, such as deleting or creating files, after the authentication process has taken place. Finally, accounting allows us to measure and record the consumption of network or system resources. The AAA framework lends itself well (as it does to any computer resource) to wireless network access control.

RADIUS

Based on the AAA framework, RADIUS is a popular client\server approach for authenticating remote users. A RADIUS server is responsible for receiving end user requests, authenticating the users. RADIUS can use several Database Management Systems and directory protocols to manage the list of network users and their privileges. This method of authentication provides a secure and centralized way to control access to network resources.

EAP

Extensible Authentication Protocol is used by wireless access points to facilitate authentication. When a user requests access to an AP, EAP (if enabled) will challenge the user for his or her identity. EAP then passes the credentials to an authentication server such as RADIUS, which will allow or deny access to its resources.

WLANs must be able to do the following:

- Maintain accessibility to resources while employees are not wired to the network—this accessibility enables employees to respond more quickly to business needs regardless of whether they are meeting in a conference room with a customer, at lunch with coworkers in the company cafeteria, or collaborating with a teammate in the next building.
- Secure the enterprise from unauthorized, unsecured, or "rogue" WLAN access points—IT managers must be able to easily and automatically detect and locate rogue access points and the switch ports to which they are connected, active participation of both access points, and client devices that are providing continuous scanning and monitoring of the RF environment.
- Segment authorized users and block unauthorized users—Services of the wireless network can be safely extended to guests and vendors. The WLAN must be able to configure support for a separate public network—a guest network.
- Provide easy, secure network access to visiting employees from other sites—there is no need to search for an empty cubicle or an available Ethernet port. Users should securely access the network from any WLAN location.
- Easily manage central or remote access points—Network managers must be able to easily deploy, operate, and manage hundreds to thousands of access points within the WLAN campus deployments and branch offices or retail, manufacturing, and health care locations. The desired result is one framework that provides medium-sized to large organizations the same level of security, scalability, reliability, ease of deployment, and management that they have come to expect from their wired LANs.
- Enhanced Security Services—WLAN Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) control to contain wireless threats, enforce security policy compliance, and safeguard information.
- Voice Services—brings the mobility and flexibility of wireless networking to voice communications via the Cisco Unified Wired and Wireless network and the Cisco Compatible Extensions voice-enabled client devices.
- Location Services — Simultaneous tracking of hundreds to thousands of Wi-Fi and active RFID devices from directly within the WLAN infrastructure for critical applications such as high-value asset tracking, IT management, location-based security, and business policy enforcement.

- Guest Access— Provides customers, vendors, and partners with easy access to a wired and wireless LANs, helps increase productivity, facilitates real-time collaboration, keeps the company competitive, and maintains full WLAN security

Given the inherently dispersed nature of the campus and the diversity of client devices, centralized and uniform management is essential for maintaining performance and availability and for enforcing corporate security policies. The campus WLAN management framework must integrate new device and security features to ensure stable operation and provide the necessary safeguards against unauthorized intrusion. Comprehensive network management should also be able to monitor traffic patterns throughout the campus WLAN to proactively identify potential bottlenecks for network tuning.

BZ SMART CONTROLLER GATEWAY (CG)

BZ SMART CG is an enterprise class, unified controller with Comprehensive Access Point Management and Subscriber Management combined in the same platform with complete ease of use and remote access.

BZ SMART CG serves as a Command Control Centre with unified Device (AP) Manager and Subscriber (User) Manager for mid-size to large deployments requiring detailed device management and user management with high level of scalability and flexibility over a period of time. BZ SMART CG offers the full range of **Centralized Network Monitoring, Auto Discovery, AP Profile Management, Fault Management, Group Configuration, Firmware Up gradation, Multi-level Authentication, Rogue AP Detection, Email/SMS Notification** and many often customizable capabilities to maximize the effectiveness and minimize the cost of managing large wireless networks. The same platform can be used for **Subscriber Management - Advanced Security, Bandwidth Management, Profile Management, User Log Management and Customized Reporting**. BZ SMART CG provides a customizable dashboard enabling a comprehensive network snapshot drill down to troubleshoot network problems. In addition, BZ SMART CG uses an innovative Encrypted Tunnel **(BET - BZ Encrypted Tunnel)** Technology to facilitate secure communication between APs and Controller.

BZ SMART CG platform is very powerful, robust and highly customizable. It can be adapted in a rapid manner to special implementation needs required by certain enterprises, colleges and government agencies, thus making the platform even more unique. Its powerful relational database engine empowers administrators with the ability to manage medium to large-scale Wireless Networks.

Unlike traditional Thin AP Controllers that are costly and complex to manage and deploy, BZ SMART CG is based on light weight, Fit AP Management concept, which is more reliable, cost-effective and easy to deploy.

ACCESS POINT [DEVICE] MANAGEMENT

- Auto Discovery of APs
  - Discovers the Access Points automatically in the WLAN network
- AP Mapping
  - Shows the list of Access Points discovered in the Network with its location details
- Redundancy/Fault Management
  - Easy and convenient way to monitor device runtime state and locate device failure
- Rogue AP Detection
  - Regular scans for rogue APs help confirm that the network is secure
- Centralized AP Management
  - Centralized Access Point Management provides networking, security, QoS with customizable dashboard and remote management
- AP Logs
  - Detailed log of all Access points can be listed to monitor the network efficiently
- Single Point (Group) Configuration
  - With a single entry of wireless parameters and security settings that can be simultaneously pushed to all wireless access points on the network, the system dramatically simplifies the deployment and daily management of the wireless network.

- Group/Centralized Firmware Up-gradation
  - Entire access points in the Network can upgraded to the new firmware in a single click
- RADIUS Authentication – 802.1x
  - IEEE 802.1X enhances security and deployment by providing support for centralized user identification, authentication, dynamic key management, and accounting
- MAC Authentication
  - Provides simple authentication based on a user's MAC address; supports local or RADIUS-based authentication
- SMS/Email Notification with Grouping
  - BZ SMART CG makes it easy to view and set up email delivery of alerts and recent event notifications on the network(s)

SUBSCRIBER [USER] MANAGEMENT

- User Access Control and Management
  - Highly secured access control and management, Administrator can disconnect the user at any time from the network
- User Authentication
  - Provides comprehensive authentication options utilizing username/password combinations, with the authentication database held locally or centrally in RADIUS, LDAP, NT Domain servers, or Windows Active Directories
- User Profile Management
  - For different application scenarios, admin can configure different items in a user profile, such as Committed Access Rate (CAR) and QoS policies
- Billing/ Accounting
  - Automatically generates bill once the user terminates the connection
- Bandwidth Allocation
  - Allocating and managing the bandwidth based on the tariff plans
- Routing , VLAN Management and DHCP Server
  - Restrict subscribers to specific devices by binding services to MAC & VLAN
- User Logs
  - Detailed logs of connected and online users can be listed and recorded

ADMINISTRATION

BZ SMART CG provides different levels of administrator privileges to enable secured management and control of the network.

KEY DIFFERENTIATORS

- Comprehensive device management and user management in the same platform
- Highly Customizable dashboard providing comprehensive network updates and alerts
- Available in cost-effective server or appliance versions
- Access Points can work independently or in conjunction with the centralized manager
- End-to-End WLAN solution that integrates easily into existing infrastructure
- Most simplified device manager cum gateway for entry level as well as high end deployments
- Innovative BlueZen Encrypted Tunnel Technology to facilitate secure communication between APs and Controller
- High performance and scalable appliance with multiple giga-bit interfaces
- VoIP, QoS and Bandwidth Management to prevent network contention issues
- High performance device with multiple giga-bit interfaces
- Ideal for many segments and applications with no known limitations

BZ 750 AC

BZ750 - AC Indoor Multimedia Extended Range Access Point provides enterprise class dual band wireless connectivity based on IEEE 802.11ac standards and indoor mobility with rich feature set and performance characteristics. Based on Smart MIMO technology, it can reach beyond obstructions, reinforced concrete floors and thick concrete walls to provide high throughput and extended reach. It supports network level authentication and security through IEEE 802.1x and helps to communicate with any standards based RADIUS server. It is interoperable with any IEEE 802.11n compliant and Wi-Fi certified equipment. BZ 750 also supports 802.11b/g/n mode built-in and can operate in 2.4GHz and 5 GHz bands.

- Plug and play deployment
- Flexible, Scalable and Highly Secured
- High data rate, up to 1300 Mbps
- Complete Management with SNMP, CLI (Telnet) and Webserver

BZ-100-AN/BGN

BZ-100 series provides high capacity Point-to-Point (PTP) backhaul systems and Point-to-Multipoint (PMP) Subscriber Radio Units. BZ-100 family is IEEE 802.11n standards based product series that supports multiple spectrum bands 2.4 GHz and 5 GHz, suitable for deployment in many different regions and terrains.

BZ-100 product suite efficiently addresses full-service providers, WISPs, and enterprises requiring immediate deployment of affordable carrier-class, short range, medium range and high capacity connectivity solutions in NLOS (Non Line of Sight) as well as LOS (Line of Sight) terrains using advanced MIMO techniques.

BZ 150-AN/BGN

BZ 150 series comes with 2x2 or 3x3 Advanced MIMO technology and High Speed Embedded Processor. BZ 150 NXP series provides high speed Point-to-Point (PTP) and Point-to-Multipoint (PMP) Backhaul and Wireless Distribution Systems with Advanced Security, Interference Analyzer and Multi-Radio features based on IEEE 802.11a/b/g/n standards that support multiple spectrum bands, 2.4 GHz and 5 GHz.

- Multi Radio Indoor / Outdoor Access Systems with Advanced MIMO Technology
- High Speed Embedded Processor and Gigabit Ethernet Switching Engine with integrated PoE (802.3at) support
- High Data Rate with 2 x 2 or 3 x 3 MIMO Matrix
- The BZ product series is specially designed to enable SMART Wi-Fi Mobile Access, Carrier Class Broadband Wireless Distribution and Cloud Networking

SAMPLE DESIGN – A HIGH END CAMPUS DEPLOYMENT

Several challenges confront the implementation of a wireless network on a large campus environment. But the challenge central to this deployment is complete coverage and advanced management with high security. So, the BlueZen team outlined in detail an advanced controller based with wireless network with top notch security and centralized command and control.

REQUIREMENTS

- To establish Wireless Connectivity between the main building and various locations(21 blocks) within the campus
- To provide desired bandwidth for Wi-Fi connectivity (IEEE 802.11 a/b/g/n) within individual locations to enable users (say **5000 users**) connect to the network using Wi-Fi enabled devices to access Internet and other applications
- The network needs to provide full coverage in areas from where users will access the network i.e. in rooms, balcony etc. The clients should have 2 Mbps minimum data speed
- No dark spot/ low signal within zone. There should not be any information access/communication dark spot in any of the buildings/corridors etc. The WLAN should be designed in such a way that there is no or minimum interference between the wireless devices i.e. AP or any other wireless devices like medical equipment etc
- Solution Design should be based on Centralized WLAN controller, Single point management for configurations of WLAN, Security, Access Control, 802.11n access points
- All in campus locations should be connected with central location i.e. computer facility and the entire **network (APs) and users** need to be managed in the central facility
- The WLAN should allow roaming across all the locations secure, user authenticated access, login, password, and usage logs etc., to be provided

These demanding requirements - to support the Wi-Fi access needs of Students, Lecturers, Academic and Administrative staff - are based on the need to enable student study; Internet access; social networking; access to College and University Administration applications, data and services; and more recently Voice over Wi-Fi services - for laptops, notebook PCs, iPhone, Android and other smartphones, iPads, tablet PCs, and the rapidly expanding range of wireless tablet / handheld devices.

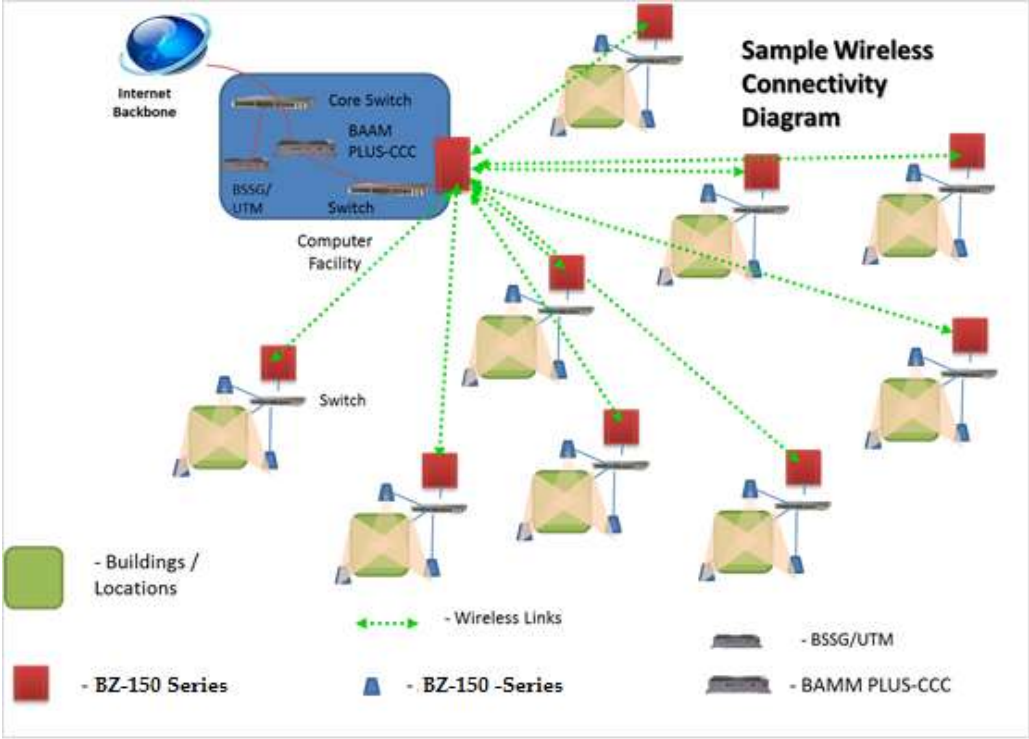
SOLUTION

The Wi-Fi installation was designed to cover 21 buildings and roughly 200 acres of the campus, with outdoor dual radio MIMO access points.

The design is depicted in figure (12 blocks), BlueZen Access Points (over 130 APs) were installed throughout campus. Additionally, BAAM plus-CCC was configured in the central facility. The BAAM plus-CCC provided a secure packet transmission between the devices. Its advanced features and functionalities enabled the administrator to configure, manage and control the complete network (both APs and users).

Block No.	Tot AP (BZ-150-BGN-HP)	Backhaul (BZ-150-AN-HP)	BZ SMART Controller	BSSG/UTM
1	3			
2	2			
3	3	1		
4	3			
5	3			
6	3			
7	4	1		
8	4			
9	3			
10	3	1		
11	2			
12	9	1		
13	9			
14	4	3		
15	3			
16	5	1		
17	7			
18	5	1		
Central Facility	2	6	1+1(redundancy)	1
20	5			
21	6	1		
22	35			
Buffer APs	10			
Total	133	16	2	1

- BZ SMART Controller (BAAM PLUS) was installed in the central facility where it gets the internet backbone from the ISP
- Access points were connected to the BZ BAAM plus through the core switch
- The buildings/blocks were connected through point-to-point link using BZ-150-AN-HP
- From the back-haul link the bandwidth was terminated to the local switch in the building/block
- From the local switch bandwidth has been distributed through Access points(BZ-150-BGN-HP) to the users
- All the access points were centrally configured through BZ BAAM plus
- All the Users were authenticated through BZ BAAM PLUS
- Administrator could manage the complete network in a single point (computer facility), without difficulty and in a secure way



BENEFITS

- Comprehensive management of both Access Points and Users
- Broad coverage with high level of authentication and security
- Less CAPEX and OPEX costs (scale as users grow)
- Roaming anywhere inside the property
- Seamless connectivity with high throughput
- Significant price-performance advantage
- Multimedia capabilities
- More flexibility and customizability