CENTRALIZED AP MANAGEMENT

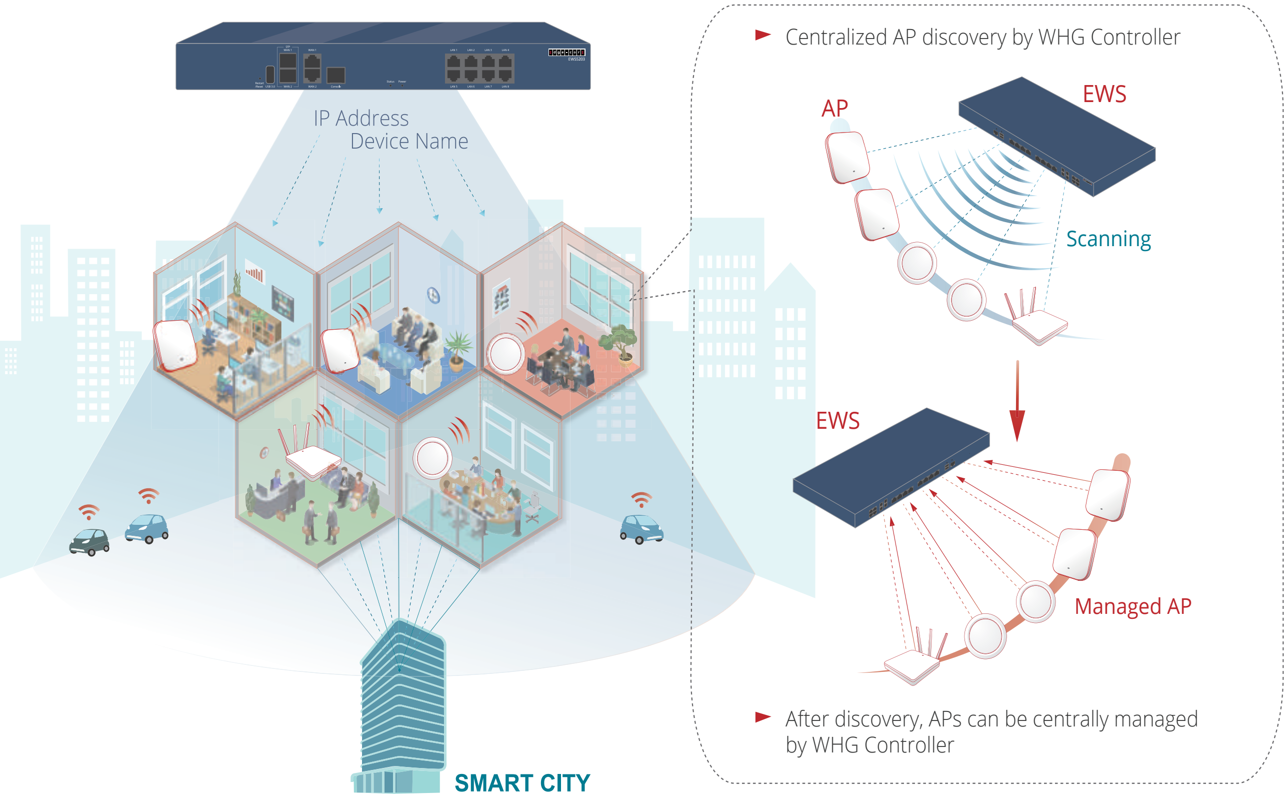
SUMMARY OF FEATURES

- AP DISCOVERY & PROVISIONING
- TEMPLATE-BASED AP CONFIGURATION
- AP STATUS MONITORING & ALERTS
- AP GROUPING
- MAP-BASED AP VISUALIZATION
- ROGUE AP DETECTION

AP DISCOVERY & PROVISIONING

To ease network deployment, Edgecore WLAN gateway-controllers have the capability of performing Centralized Discovery and Provisioning of APs in the same Layer 2 subnet in their out of box default state. Upon successful discovery, administrators can then assign unique IP address and device names from the controller's interface. Even if the APs have already been individually pre-configured with unique IP addresses, the controller can still discover all of them by simply scanning a user-defined IP address range. This discovery mechanism greatly reduces initial configuration effort while providing a flexibility that caters to the different habits of each network administrator.

For larger networks, the subnet on which APs are located may be very large, resulting in long discovery scan times. By allowing background discovery, network administrators can perform other configuration changes and settings while the discovery process is running, minimizing thumb twiddling time and increasing efficiency.



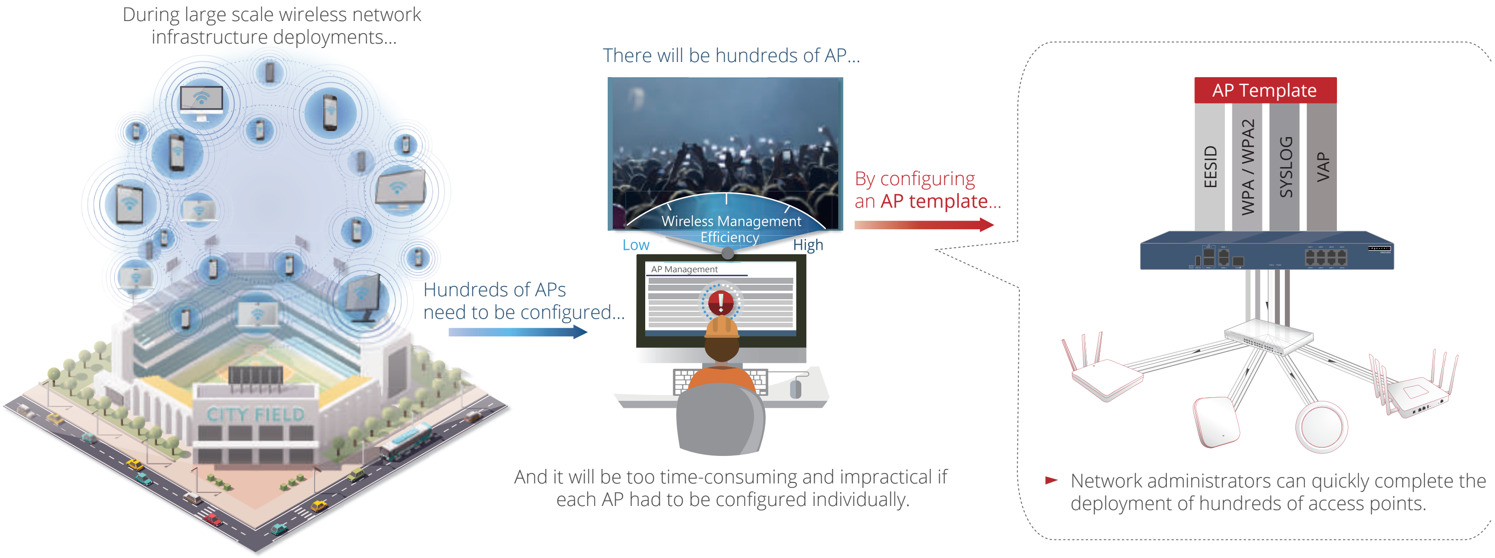
► Centralized AP discovery by WHG Controller

► After discovery, APs can be centrally managed by WHG Controller

TEMPLATE-BASED AP CONFIGURATION

During large scale wireless network infrastructure deployments, it would be too time-consuming and impractical if each AP had to be configured individually. Extending the notion that AP deployment and management must be straightforward and easy in order to increase efficiency and decrease total cost of ownership, Edgecore WLAN gateway-controllers enable template-based AP Configuration.

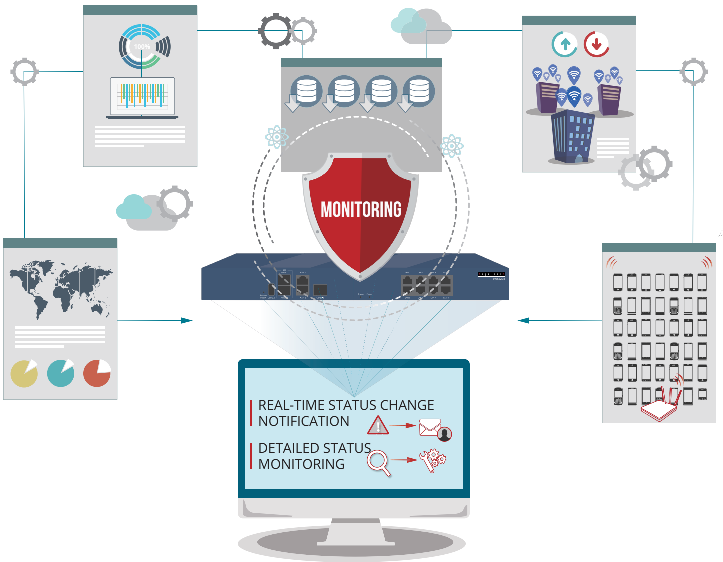
By configuring an AP template, which includes basic AP system settings as well as fine-grained VAP (virtual access point) settings such as ESSID name and WPA/WPA2 security, network administrators can quickly complete the deployment of hundreds of access points. For settings that typically vary between each AP (e.g. operating channel, VLAN ID, etc.), the controller provides the flexibility to customize each one individually during the initial discovery process, eliminating redundant or unnecessary tasks.


During large scale wireless network infrastructure deployments...
CITY FIELD
Hundreds of APs need to be configured...
There will be hundreds of AP...
Wireless Management Efficiency
Low
High
AP Management
And it will be too time-consuming and impractical if each AP had to be configured individually.
By configuring an AP template...
AP Template
EESID
WPA / WPA2
SYSLOG
VAP
► Network administrators can quickly complete the deployment of hundreds of access points.

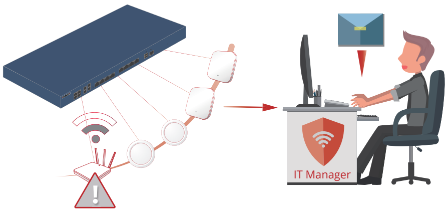
AP STATUS MONITORING & ALERTS

With the widespread penetration of smartphones in the consumer mobile phone market, checking e-mails anytime and anywhere is now a common occurrence. Edgecore WLAN gateway-controllers take advantage of this trend to make network monitoring easier and more real-time through e-mail notifications of AP status changes. If an AP goes offline (i.e. loses connectivity with the controller), the administrator will receive an e-mail notifying him/her of the incident. He/she can then take the appropriate measures to ensure that network service resumes in a timely manner, minimizing downtime.

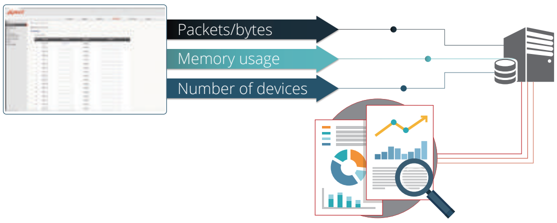
When network issues are reported, administrators need to have enough tools and information at their disposal to aid in troubleshooting. Administrators have access to all of this information through the centralized interface on Edgecore WLAN gateway-controllers, including but not limited to transmitted and received packets/bytes, memory usage, and number of associated devices. Furthermore, all of the basic system settings and detailed per VAP traffic statistics are presented on the same page for simple and complete visibility of the entire AP's status. If the administrator does not wish to access the controller's interface frequently to view these statistics, the controller can automatically send out complete reports of managed APs on a daily, weekly, or monthly basis. In summary, Edgecore's WLAN gateway-controllers track and record detailed information regarding each managed AP, reducing network maintenance and troubleshooting complexities.


MONITORING
REAL-TIME STATUS CHANGE NOTIFICATION
DETAILED STATUS MONITORING

- If an AP goes offline (i.e. loses connectivity with the controller), the administrator will receive an e-mail notifying him/her of the incident.



- Through the centralized interface, the administrator can easily view network statistics such as transmitted packets/bytes, device uptime, and number of associated devices.

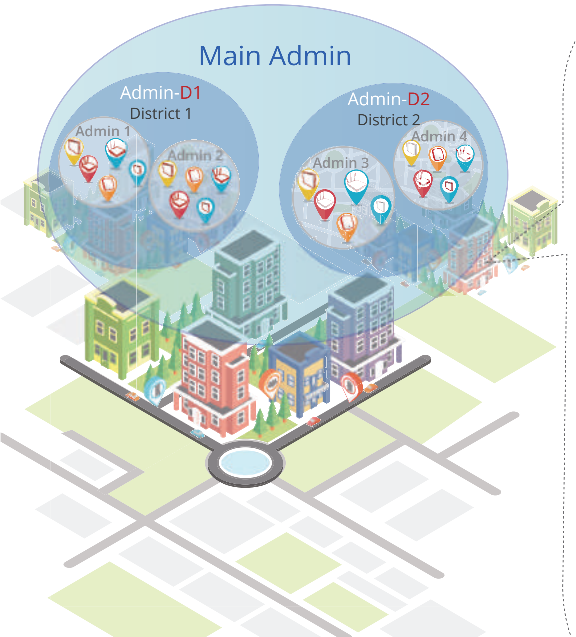


- Furthermore, the controller can automatically send out complete reports of managed APs on a daily, weekly, or monthly basis.

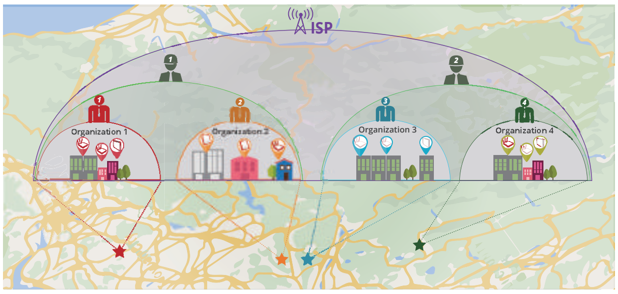
MANAGED SERVICES WITH FLEXIBLE AP GROUPING

In a multi-tenancy architecture, network management systems need to support tiered administrator privileges and virtual network segregation. Edgecore's solution allows organizations to assign access points to unique groups with corresponding geographical maps, each of which is managed by an independent network administrator. Multiple groups of APs can then be centrally monitored by a supervisor with a higher level of privileges. This flexibility enables new advertising and rental business models for Wi-Fi monetization.

Managed service providers can utilize this architecture to lease wireless network infrastructure and services to organizations that have limited IT resources or CAPEX budget. The operator can assign personnel to simultaneously oversee the networks of multiple organizations, while each organization can also directly access the management system to monitor and manage their own access points and network configuration. Physical resources are shared but virtually compartmentalized, minimizing investments costs while creating new revenue streams.

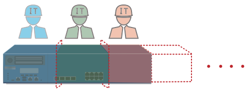


- Flexible AP Grouping



The operator can assign personnel to simultaneously oversee the networks of multiple organizations, while each organization can also directly access the management system to monitor and manage their own access points and network configuration.

- Creating New Revenue Streams



Physical resources are shared but virtually compartmentalized, minimizing investments costs.

MAP-BASED AP VISUALIZATION

When managing a large number of APs distributed across multiple geographical locations, it is often beneficial for network administrators to view the entire deployment via a centralized map. With Edgecore WLAN gateway-controllers, administrators can easily place APs on the integrated Google maps, and view AP status and associated client information with the simple click of a button. During troubleshooting of network issues, the map further serves as a quick reminder for the physical location of each deployed AP.

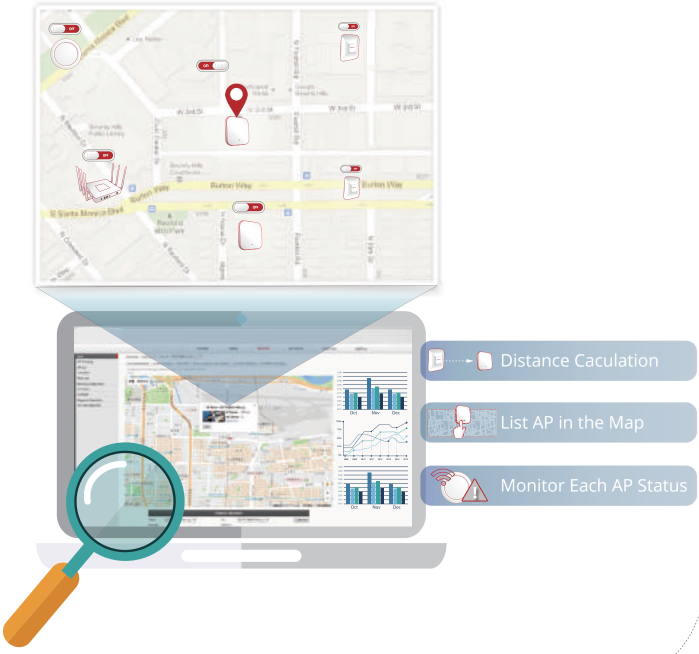
Edgecore's unique design also utilizes AP maps as a method for grouping access points. Although all the APs may be in the same physical location, it is often desirable to separate these APs into independent groups and have them be managed by different administrators. For example, in an office building there may be multiple AP groups for APs deployed in each floor of the building - each floor's APs will be added to an independent AP map with a dedicated administrator.

Combined with easy provisioning of APs across layer 3 and the flexible per SSID tunneling options, Edgecore's solution makes it easy for deploy, monitor, and manage distributed site deployments.

For distributed AP deployments, it's a challenging task for network administrators to monitor and manage the entire deployment.

One of the essential requirements of Wi-Fi solutions in this application scenario is being able to visualize and obtain each APs geographical location for quick troubleshooting and management.

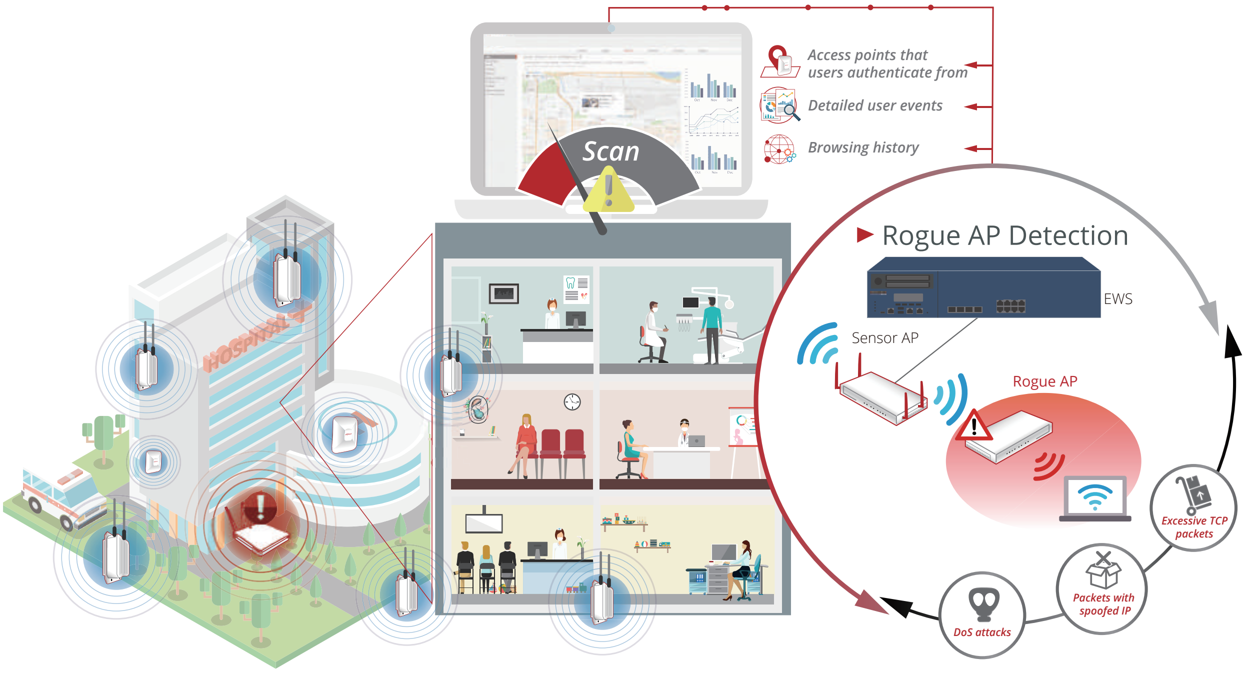
- Edgecore WLAN gateway-controllers have integrated Google maps to allow network operators to easily visualize and monitor all of their APs. Additionally, the maps can also be used to segregate groups of APs in distributed site deployments for unique administrator privileges.



ROGUE AP DETECTION

For today's wireless networks, security if one of the most important concerns. Common security issues such as AP impersonations and denial-of-service attacks need to be detected and prevented, as these not only jeopardize information security but may also affect entire network performance. Rogue AP detection is an effective way to identify many of these attacks by cross-checking between authorized/managed access points and unauthorized ones.

Furthermore, if an unauthorized access point is spoofed to the same MAC address as a managed access point, network administrators can quickly take action to rectify the security leak. Edgecore's rogue AP detection function allows administrators to manually configure scanning intervals, APs to use for scanning, as well as a trusted list of non-managed devices. Together with the integrated user access control features inside the controller, network operators can easily create a secure and reliable Wi-Fi environment.


Access points that users authenticate from
Detailed user events
Browsing history
Scan
HOSPITAL
Rogue AP Detection
EWS
Sensor AP
Rogue AP
Excessive TCP packets
Packets with spoofed IP
DoS attacks