LANCOM™ Techpaper
Smart WLAN controlling

The widespread use of wireless access points and wireless routers provides great convenience and flexibility in network access for businesses, universities and other organizations.

In recent years, wireless networks have seen fundamental structural changes: The rapid spread of wireless LAN has seen the first generation of stand-alone access points being replaced by solutions with central management. To overcome the considerable disadvantages of centralized WLANs, modern WLAN architectures employ intelligent "work-sharing" between access points and WLAN controllers, referred to as "smart WLAN controlling".

First-generation WLAN architectures

Even though WLAN has numerous advantages over wired networks, a number of unsettled issues remain:

- The installation, configuration and servicing of access points involves considerable effort and expertise.
- Important functions such as setting up guest access accounts or rogue access point and WLAN-client detection have to be configured separately on each access point.
- Overlapping frequencies can only be avoided by manually setting the radio channels.
- Changes to the configuration or structure are not simultaneous on all access points, but only come into effect after a time delay.
- access points in public places are a potential security risk because the devices themselves, including the security-related data in them such as passwords, etc., are susceptible to theft.

The result: Drastically increased costs of WLAN operation in proportion to the number of access points.

The second generation: WLAN switching

The first approach to solving these problems for large WLAN installations was to relocate the system's "intelligence" to a central component, the WLAN switch. In WLAN switching, the access points merely act as remote antennas of the central unit. Also known as "thin access points", these devices do not require configuration and they transmit all data received from the WLAN directly over the LAN to the WLAN switch.

Although WLAN switching significantly cuts the effort and expense of operating wireless networks, the WLAN switch itself becomes a data-transfer bottleneck and represents a single point of failure. Consequently, a breakdown of the switch would cause complete failure of the entire WLAN.

Smart WLAN controlling

Smart WLAN controlling combines the advantages of the first two approaches to provide a WLAN system that meets the following requirements:

- Flexible break-out of data depending on the application and user:
  - Break-out at the access point for data with high bandwidth demands (e.g. IEEE 802.11n) or for access points at remote locations.
  - Break-out at the WLAN controller to implement layer-3 roaming for applications such as VoWLAN or for guest access accounts.
- All access points and wireless routers are centrally authenticated and configured from the WLAN controller.
- Reduction of initial installation costs as the access points are deployed faster.
- Firmware updates can be controlled centrally and, in the ideal case, automatically.
- Extension of security zones to include any access points located at home offices or subsidiaries.
- Automatic radio-field (RF) optimization for interference-free operation of WLANs within range of other access points.
- Layer-3 roaming for monitoring critical IP connections in the central WLAN controller.
- Secure fallback and redundancy concept in case of WLAN controller failure, without storage of security-relevant data in the access points.
- Automatic assignment of WLAN clients to specific networks.
- Central rogue AP and client detection.

In the following you will see how these objectives have been achieved on the basis of the CAPWAP standard.

The CAPWAP standard

The CAPWAP protocol (Control And Provisioning of Wireless access points) introduced by the IETF (Internet Engineering Task Force) is a draft standard for the centralized management of large WLAN infrastructures.

CAPWAP uses different channels for data transfer:

- Control channel, encrypted with DTLS. This channel is used to exchange administration information between the WLAN controller and the access point.
- Data channel, optionally also encrypted with DTLS. The payload data from the WLAN is transferred through this channel from the access point via the WLAN controller into the LAN—encapsulated in the CAPWAP protocol.

Smart WLAN controlling makes effective use of the different CAPWAP channels: Only data that is required by the WLAN controller passes through CAPWAP tunnel. The far greater volume of the payload data can be directly broken out at the access point and transmitted to the LAN.

LANCOM™ Techpaper
Smart WLAN controlling

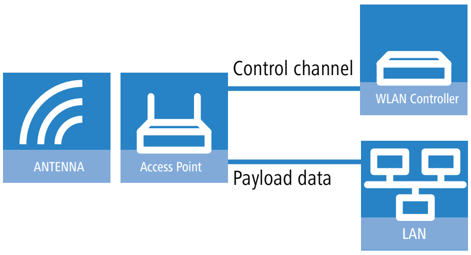
Smart controller structure

In a decentralized WLAN structure with stand-alone access points (operating as so-called "rich access points") all functions for data transfer, the control functions, and the management functions are integrated in the access points. Centralized WLAN management divides these tasks among two different devices:

- The central WLAN controller assumes the administration tasks.
- The remote access points handle the data transmission.

CAPWAP describes three different scenarios for the relocation of WLAN functions to the central WLAN controller.

- Remote MAC: In this case, **all** of the WLAN functions are transferred from the access point to the WLAN controller. Here, the access points only serve as "extended antennas" without independent intelligence.
- Split MAC: With this variant, only a portion of the WLAN functions are transferred to the WLAN controller. Normally, realtime applications will continue to be processed in the access point; the non-realtime applications are processed via the central WLAN controller.
- Local MAC: The third possibility provides for complete management and monitoring of the WLAN data traffic directly in the access points. The only information exchanged between the access point and the WLAN controller is for network management and ensures that the access points have a uniform configuration.



Smart WLAN controlling employs the local MAC procedure. Thanks to the reduction of centralized tasks, these WLAN infrastructures offer optimum scalability. At the same time, infrastructure of this type prevents the WLAN controller from becoming a central bottleneck that has to process large portions of the overall data traffic. In remote MAC and split MAC architectures, **all** payload data is forced to run centrally via the WLAN controller. In local MAC architectures the payload data can alternatively be broken out from the access point directly to the LAN to provide high-performance data transfer.

The smart controlling approach is also suitable for WLANs working with the IEEE 802.11n standard that now offer much higher data rates than previous WLAN technologies. With break-out into the LAN, data can also be directly routed into special VLANs. This makes it very easy to set up closed networks, such as for guest access accounts.

Authentication and configuration

The core task of the WLAN controller is to supply any access points connected to it with a valid configuration at all times. For the WLAN controller to decide if it should provide a configuration to a requesting access point, the access point has to identify itself when communication is initiated. This authentication is based on digital certificates.

When rolling out access points in large-scale installations that may involve several different sites, the necessary certificates are not stored in the access points. LANCOM WLAN controllers provide a function that allows the certificate to be transmitted to the access point when negotiations commence. The only access points that are valid for this are those that are entered into the WLAN controller. As an alternative, the "auto accept" function provides a brief time window during which all access points in the LAN—including those without an entry in the WLAN controller—are accepted and issued with a valid certificate.

The certificate allows the access point to be authenticated by the WLAN controller, which then issues a valid configuration. The configuration for an access point is stored in the WLAN controller and referenced by the MAC address. Access points not entered into the WLAN controller can still be considered even when the configuration is being allocated: A default configuration can be used to enable these devices to operate in the WLAN.

The actual configuration data for the access points is stored in profiles in the WLAN controller: These profiles are transmitted to the access points.

Rollout with zero-touch management

With the auto-accept function and the default configuration, LANCOM WLAN controllers can automatically issue certificates and configurations to access points making a request. The result is true "zero-touch" management. Simply connect new access points to the LAN—no further configuration is necessary. Simplifying the installation of the devices in this way reduces the workload for IT departments, especially in decentralized structures, because no special IT or WLAN expertise is required at the remote locations.

Inheritance of parameters

A LANCOM WLAN controller is capable of managing a wide range of different access points at different locations. However, WLAN profiles include settings that are not equally suitable for every type of access point that can be managed. For example, there are differences between the country settings and the device properties.

In order to avoid having to maintain multiple redundant WLAN profiles to cater for different countries or device types, it is possible for certain WLAN parameters to "inherit" selected properties from other entries.

Inheritance also allows for chains over multiple stages (cascading). This means, for example, that country and device-specific parameters can be grouped for convenience. Recursion is also possible—profile A inherits from profile B, and at the same time B inherits from A.

Split management for distant access points

LANCOM access points can locate your WLAN controller in distant networks—a simple IP connection, e. g. via a VPN path, is all that you need. As the WLAN controllers only influence the WLAN part of the configuration in the access point, all other functions can be managed separately. This division of the configuration tasks makes LANCOM WLAN controllers perfect for establishing a company-wide WLAN infrastructure that is based at the headquarters and includes all of the branch and home offices connected to it. This avoids errors in the WLAN settings at the remote access points, that would otherwise allow unauthorized clients to access the company network.

Layer-3 tunneling and layer-3 roaming

Smart WLAN controlling generally operates by separating payload data from control data: The only data transferred via the layer-3 tunnel is control data relevant to the WLAN controller; the rest of the data, which represents the vast majority of the data volume, breaks-out directly from the access point into the LAN. This greatly reduces the data throughput at the WLAN controller, so preventing the WLAN controller from becoming a central bottleneck.

However, some applications need payload data to be passed through the layer-3 tunnel to the WLAN controller. With applications such as voice over wireless LAN (VoWLAN) WLAN clients can move between radio cells. However, the underlying IP connection will not be interrupted because it continues to be managed by the central WLAN controller (layer-3 roaming). In this way, mobile SIP telephones can easily roam even during a call.

Central firmware and script management

With central firmware and script management, uploads of firmware and scripts can be automated for all of the WLAN devices.

To this end the firmware and script files are stored to a web server. The WLAN controller checks once daily, or when prompted by a user, to compare the available files with those on the devices. Alternatively, this procedure can be handled by a cron job—overnight, for example. If an update can be carried out, or if the access point is not running the desired firmware version, then the WLAN controller downloads the file from the web server and uploads it to the appropriate wireless routers and access points.

Activating firmware and script management allows the distribution of the files to be controlled precisely. It is possible, for example, to limit certain firmware versions to certain device types or MAC addresses.

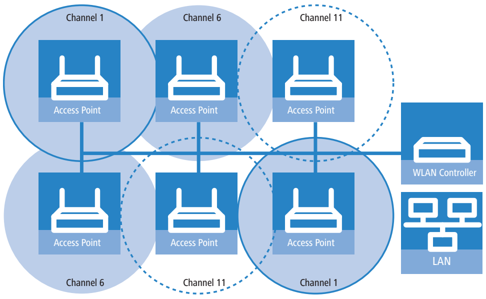
Automatic RF optimization

Selecting the channel from the channel list defines a portion of the frequency band that an access point uses for its logical wireless LANs. All WLAN clients that need to connect to an access point have to use the same channel on the same frequency band. In the 2.4-GHz band channels 1 to 13 are available (depending on the country), and in the 5 GHz band channels 36 to 64 are available. On each of these channels, only one access point can actually transfer data. In order to operate another access point within radio range and without interference, the access point must make use of a separate channel—otherwise all of the participating WLANs have to share the channel's bandwidth.

With automatic radio-field (RF) optimization, the LANCOM WLAN controllers provide an automatic method of setting the optimum channels for access points that work in the 2.4-GHz band. Initially the channel lists in the access points are deleted and re-defined by the WLAN controller. The WLAN modules are then switched off and switched on again, one after the other. Once switched on the modules automatically search for a vacant channel.

LANCOM™ Techpaper
Smart WLAN controlling

The result is an optimized distribution of the channels in the radio field.



Automatic RF optimization can be started for all of the access points managed by a WLAN controller or for one device at a time.

Stand-alone operation

Installations with a single WLAN controller have a potential single point of failure. Failure would lead to the immediate outage of all of the WLANs managed by it.

LANCOM WLAN controllers optionally support the stand-alone operation of wireless routers and access points even in case of a temporary outage of the central management. Because smart WLAN controlling uses the access points to manage the payload data, the WLAN controller is only responsible for updating the configuration.

The configuration is allocated to the access point by the WLAN controller and, normally, it is stored in the RAM only. Operational reliability can be increased by optionally storing the configuration data to the flash memory (in an area that is not accessible to LANconfig or other tools). Should the connection to the WLAN controller be interrupted, the access point will for a preset period of time continue to operate with the configuration stored in flash memory. The access point can also continue to work with this flash configuration after a local power outage.

If there is still no connection to the WLAN controller after this time period has expired then the flash configuration is deleted and the access point goes out of operation. As soon as the WLAN controller can be reached again, the configuration is transmitted again from the WLAN controller to the access point. This option enables an access point to continue operating even if the connection to the WLAN controller is temporarily interrupted.

Dedicated IP networks for access points

Access points can be configured with their own IP parameters to make them even more independent of the central WLAN controller. This involves the separate definition of important IP parameters such as domain, netmask, gateway or DNS server addresses for each access point—this IP configuration allows the device to continue to operate even if the WLAN controller fails. DHCP is only required for the initial search for a WLAN controller. After the access point has been configured by the WLAN controller, DHCP is no longer used.

Backup solutions

LANCOM WLAN controllers manage a large number of access points, which in turn may have a large number of WLAN clients associated with them. WLAN controllers thus play a crucial role in the functioning of the entire WLAN infrastructure—for which reason the organization of a backup solution in case of temporary WLAN controller failure is in many cases indispensable.

In case of a backup event, a managed access point should connect to an alternative WLAN controller. Because this connection will only function if the certificate in the access point has been authorized by the backup controller, all WLAN controllers sharing a backup solution have identical root certificates.

There are two approaches to choose from for the backup structure itself:

- Backup with redundant WLAN controllers requires each device to be backed up 1:1 with a second device. The backup controllers all have redundantly available certificates, profiles and configurations that are identical to those in the WLAN controller.
- With multiple WLAN controllers in use, the devices provide a backup for one another and if necessary they can manage the access points of the other WLAN controllers. This involves the combination of a larger number of WLAN controllers than would normally be necessary for managing the available access points. The access points are entered into the AP tables of all of the WLAN controllers: If a WLAN controller fails, another device takes over and continues to assign the corresponding profiles.

  The AP table in a LANCOM WLAN controller can accommodate five times the maximum number of access points than the device can manage by itself. For each five WLAN controllers (identical models), just one additional WLAN controller is sufficient to provide a full backup in case of failure.

LANCOM™ Techpaper Smart WLAN controlling

Authentication and accounting for WLAN clients

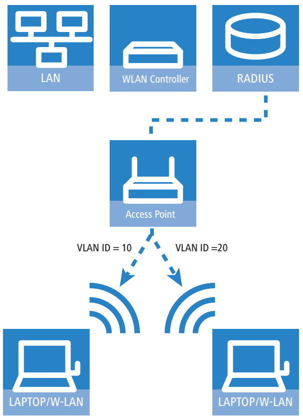
RADIUS servers are generally employed to implement access authentication and for the billing of charges. There are two methods for accessing a RADIUS server via the access points:

- If no specialized configuration is required, the access points forward any WLAN client’s RADIUS requests to the central WLAN controller. The WLAN controller then applies its own user table or it forwards the RADIUS request to a defined server.
- For RADIUS requests to be processed independently of the central WLAN controller, the profiles for the access points can be configured with their own RADIUS server. In this case the access point does not forward the RADIUS request to the WLAN controller. Instead, the request breaks out into the LAN and is routed to the RADIUS server there.

Dynamic VLAN assignment

Larger WLAN infrastructures often require individual WLAN clients to be assigned to certain networks. Assuming that the WLAN clients are always within range of the same access points, then assignment can be realized via the SSID in connection with a particular IP network. If on the other hand the WLAN clients frequently change their position and logon to different access points then, depending on the configuration, they may find themselves in a different IP network.

For WLAN clients to remain within a certain network **independent** of their current WLAN network, dynamically assigned VLANs can be used. Unlike the situation where VLAN IDs are statically configured for a certain SSID, in this case a RADIUS server directly assigns the VLAN ID to the WLAN client.



Example: Two WLAN clients log into the same access point with the SSID 'INTERNAL'. During registration, the RADIUS requests from the WLAN clients are directed to the access point. If the corresponding WLAN interface is in the operating mode 'managed' the RADIUS requests are automatically forwarded to the WLAN controller. This forwards the request in turn to the defined RADIUS server. The RADIUS server can check the access rights of the WLAN clients. It can also use the MAC address to assign a certain VLAN ID, for example. The WLAN client **A**, for example, receives the VLAN ID '10' and WLAN client **B** receives '20'.

Summary

Smart WLAN controlling from LANCOM Systems provides a wide range of functions to facilitate the operation of large WLAN installations.

Automatic authentication and configuration simplify the rollout, even at sites without expert IT personnel. Automatic firmware updates enable the access points to be kept up to date at all times. Also optimized automatically is the utilization of vacant radio channels.

By separating payload and control data, LANCOM WLAN controllers provide load balancing in the network and avoid excessive data traffic at the Controller. For specialized applications payload data can be directed via the WLAN controller to provide uninterrupted IP connections even when the client moves between radio cells (layer-3 roaming).

The WLAN configuration of remote sites by means of split management extends your company's WLAN security policy to home offices and subsidiaries. The dynamic assignment of VLANs to users provides excellent protection for critical network segments from guest access accounts.

Short-term outages of the WLAN controllers can be handled by temporary stand-alone operation by the access points. Various backup strategies ensure operational reliability.