LANCOM SYSTEMS

lancom-systems.com

LCOS 10.70

LANCOM WLC Basic Option for Routers

Complete WLAN controller functionality for LANCOM routers

With the LANCOM WLC Basic Option, LANCOM routers without WLAN are upgraded with the functions of a WLAN controller. This option enables a single device to manage up to 12 access points or WLAN routers. Small networks in particular benefit from important and professional new functions, without the need for a separate WLAN controller. This minimizes the costs of the network solution and keeps the number of managed components to a minimum.

- → Central management for up to 6 LANCOM access points and WLAN routers
- → Full configuration of the access points with profile assignment
- → Easy installation for the LANCOM 1781 series without WLAN
- → Ideal for smaller, yet professional WLAN installations, such as chain stores, enterprises, or small hotels
- → Remote configuration of WLAN routers or access points, e.g. in home offices possible
- → No additional devices necessary
- → WLAN controller functionality extendable to up to 12 WLAN devices with the LANCOM WLC AP upgrade +6 option

LANCOM SYSTEMS

lancom-systems.com

LCOS 10.70

LANCOM WLC Basic Option for Routers

Central management

With the LANCOM WLC Basic Option, LANCOM routers without WLAN are upgraded with the functions of a WLAN controller. This enables a single device to manage up to 6 access points or WLAN routers, or even 12 devices after installing the WLC AP Upgrade +6 Option. In particular for smaller WLAN infrastructures, this option offers genuine added value because there is no need to operate a separate WLAN controller.

Upgrading with the LANCOM WLC AP Upgrade +6 Option

Networks grow continually and need flexibility to be able to expand. Even with the best planning, the available resources can still reach their limits. The LANCOM WLC Upgrade +6 Option facilitates the management of up to 6 additional WLAN devices. This means that the network can grow without requiring any additional hardware.

Complete configuration of the WLAN

The LANCOM WLC Basic Option gives LANCOM routers all of the functions of a WLAN controller. A single LANCOM router equipped with the LANCOM WLC Basic Option is able to manage LANCOM access points or WLAN routers located in the LAN or accessible at remote branches and home offices. Ideal for smaller but professional WLAN installations, e.g. for retail stores, businesses or small hotels.

Zero-touch deployment

The LANCOM WLC Basic Option quickly and easily integrates new WLAN devices into the network, and it assigns configurations to them automatically. Each new WLAN device receives a fully customized configuration with a profile assignment.

Easy upgrades

The LANCOM software options turn a simple network into a customized and cost-efficient solution that meets your individual needs. Simply install them on your existing hardware and you upgrade your network with the desired feature. The advantage: No additional hardware components are required. The costs and the administration overhead of the entire network are reduced. Genuine added value comes in terms of the system's future viability, because the options transform a network into a customized and scalable networking solution.

LANCOM SYSTEMS

lancom-systems.com

LCOS 10.70

LANCOM WLC Basic Option for Routers

WLAN profile settings*	
Radio channels 5 GHz	Up to 26 non-overlapping channels (available channels and further obligations such as automatic DFS dynamic channel selection depending on national regulations)
Radio channels 2.4 GHz	Up to 13 channels, max. 3 non-overlapping (depending on country-specific restrictions)
Concurrent WLAN clients	Depends on the access points in operation
IEEE 802.11u	Managed LANCOM Access Points support the WLAN standard IEEE 802.11u (Hotspot 2.0) which allows mobile clients a seamless transition from the cellular network into WLAN hotspots. Authentication methods using SIM card information, certificates or username and password, enable an automatic, encrypted login to WLAN hotspots of roaming partners - without the need to manually enter login credentials
Opportunistic Key Caching	Opportunistic key caching allows fast roaming processes between access points. WLAN installations utilizing a WLAN controller and IEEE 802.1X authentication cache the access keys of the clients and are transmitted by the WLAN controller to all mananged access points
Fast roaming	Based on IEEE 802.11r, allows fast roaming procedures between access points. This is possible by using IEEE 802.1X authentication or pre-shared keys in controller based WLAN installations, which save the access keys temporarily and distribute them to the managed access points.
Protected Management Frames	Protection of WLAN Management Frames, based on the standard IEEE 802.11w, against man-in-the-middle attacks by using Message Ingegrity Codes (MIC)
Security	WPA3-Personal, IEEE 802.11i / WPA2 with passphrase (WPA2-Personal) or IEEE 802.1X (WPA3-Enterprise, WPA2-Enterprise) and hardware-accelerated AES, closed network, WEP64, WEP128, WEP152, user authentication, IEEE 802.1x /EAP, WPA1/TKIP, LEPS-MAC, LEPS-U
Time Control	time-based activation and deactivation of WLAN networks
RADIUS Accounting per SSID	A RADIUS server can be set for each individual SSID
Quality of Service	Prioritization according to Wireless Multimedia Extensions (WME, subset of IEEE 802.11e)
Background scanning	Detection of rogue AP's and the channel information for all WLAN channels during normal AP operation. The Background Scan Time Interval defines the time slots in which an AP or Router searches for a foreign WLAN network in its vicinity. The time interval can be specified in either milliseconds, seconds, minutes, hours or days
Client detection	Rogue WLAN client detection based on probe requests
Auto WDS*	Auto WDS allows wireless integration of access points in existing WLAN infrastructure, including managment via WLAN controller.
Space Time Block Coding (STBC)*	Coding method according to IEEE 802.11n. The Space Time Block Coding improves reception by coding the data stream in blocks.
Low Density Parity Check (LDPC)*	Low Density Parity Check (LDPC) is an error correcting method. IEEE 802.11n uses convolution coding (CC) as standard error correcting method, the usage of the more effective Low Density Parity Check (LDPC) is optional.
*) Note	Depends on the access points in operation

LANCOM SYSTEMS

lancom-systems.com

LCOS 10.70

LANCOM WLC Basic Option for Routers

Security	
Encryption options	WPA3-Personal, IEEE 802.1X (WPA3-Enterprise, WPA2-Enterprise), IEEE 802.11i (WPA2-Personal), Wi-Fi Certified™ WPA2™, WPA, WEP, IEEE 802.11w (Protected Management Frames), LEPS-MAC (LANCOM Enhanced Passphrase Security MAC), LEPS-U (LANCOM Enhanced Passphrase Security User)
Encryption	AES-CCMP AES-GCMP, TKIP, RC4 (only used by WEP)
EAP types (authenticator)	EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-FAST
RADIUS/EAP-server	User administration MAC-based, rate limiting, passphrases, VLAN user based, authentication of IEEE 802.1X clients via EAP-TLS, EAP-TTLS, EAP-MD5, EAP-GTC, PEAP, MSCHAP, MSCHAPv2, Dynamic Peer Discovery
Others	IEEE 802.1X supplicant, background scanning, client detection ("rogue WLAN client detection"), Wireless Intrusion Detection System (WIDS)

LANCOM Active Radio Control	
Client Management	Steering of WLAN clients to the ideal access point using 802.11k and 802.11v
Band Steering	Steering of 5GHz clients to the corresponding high-performance frequency band
Managed RF Optimization*	Selection of optimal WLAN channels by the administrator
Adaptive Noise Immunity	Better WLAN throughput due to immunity against interferences
Spectral Scan	Monitoring your WLAN for sources of interference
Adaptive RF Optimization	Dynamic selection of the optimal WLAN channel
Airtime Fairness	Improved utilization of the WLAN bandwidth
*) Note	Depends on the access points in operation. Steering of WLAN clients is not available in US version

WLAN-Controller functionality	
Number of managed devices	Any combination of up to 6 LANCOM access points and WLAN routers can be centrally managed by the LANCOM WLAN controller. Capacities can be expanded even further by employing multiple Controllers.
Smart Controller technology	The WLAN controller can switch user data per AP Radio or per SSID in the following ways: – Direct switching to the LAN at the AP (for maximum performance, e.g. for IEEE 802.11n-based access points) – Logical seperation of user data into VLAN's (e.g. for WLAN guest access accounts) – Central tunneling to the Controller (layer 3 tunneling between different IP Subnets)
Auto Discovery	LANCOM access points and WLAN routers automatically discover the WLAN controller by means of DNS name or IP addresses. Even AP's at remote sites or in home offices with no direct access to the Controller can be integrated into the central Controller

LANCOM SYSTEMS

lancom-systems.com

LCOS 10.70

LANCOM WLC Basic Option for Routers

WLAN-Controller functionality	
Authentication and Authorization	Access Points can be authenticated manually or automatically. Signaling of new access points by e-mail message, SYSLOG and SNMP traps. Manual authentication via LANmonitor or WEBconfig GUI tools. Semi-automatic authentication based on access-point lists in the Controller ('bulk mode'). Fully automatic authentication with default configuration assignement (can be activated/deactivated separately, e.g. during the rollout phase). Authenticated access points can be identified by means of digital certificates; certificate generation by integrated CA (Certificate Authority); certificate distribution by SCEP (Simple Certificate Enrollment Protocol). Access points can be blocked by CRL (Certificate Revocation List).
Management communication protocol	CAPWAP (Control and Provisioning Protocol for Wireless Access Points)
Layer-3 Tunneling	Layer-3 Tunneling in conformity with the CAPWAP standard allows the bridging of WLANs per SSID to a separate IP subnet. Layer-2 packets are encapsulated in Layer-3 tunnels and transported to a LANCOM WLAN controller. By doing this the access point is independent of the present infrastructure of the network. Possible applications are roaming without changing the IP address and compounding SSIDs without using VLANs
Encryption	DTLS encryption of the control channel between WLAN controller and Access Point (256-bit AES encryption with digital certificates, incl. hardware encryption accelerator; encryption can be disabled for diagnostic purposes).
Firmware deployment	Central Firmware deployment and management of the Access Points. Requires an external web server. Automatic Firmware update on the Access Points is also possible. The Controller checks every day, depending on the defined policy, for the latest Firmware and compares it with the versions in the devices. This can also be activated using Cron jobs. If there is a Firmware mismatch, then the Controller downloads the matching Firmware from the server and updates the corresponding Access Points and Routers.
Script distribution	Enables the complete configuration of non-WLAN specific functions such as Redirects, Protocol Filter, ARF etc. Internal storage of up to three script files (max. 64 kByte) for provisioning access points without a separate HTTP server
RF management and automatic RF optimization	The channel deployment can be static or can be automated. Upon activation of the RF Optimization setting, the Access Points search for an optimal channel in the 2.4 GHz band and the "indoor only" mode in the 5 GHz band. The selected channels are sent to the Controller saves these channels on the corresponding Access Points. RF Optmization can also be activated for individual Access Points. Transmit power setting static between 0 to -20 dB. Alarm notification in case of Access Point failure by e-mail, SYSLOG and SNMP traps.
Configuration management	Definition and grouping of all logical and physical WLAN parameters by means of WLAN configuration profiles. Fully automatic or manual profile assignment to WLAN Access Points; automatic transfer and configuration verification (policy enforcement).
Inheritance of configuration profiles	Support of hierarchical WLAN profile groups. New profiles can be easily created by inheriting parameters from existing profiles.
Management operating modes	The AP can be set to 'managed' or 'unmanaged' mode for each radio interface. With LANCOM WLAN routers, the Controller manages the WLAN part only (split management).
Stand alone operation	In 'Managed' mode, an adjustable setting defines the time-span for which the AP continues Stand-alone operation in the event the connection to the Controller fails. After this time-span the AP configuration is deleted and the AP resumes operation only after the connection to the Controller is reestablished. By default this value is set to zero and AP ceases operation as soon as connection to the Controller is lost. Alternatively, a special time setting allows the AP to function in Stand-alone mode indefinetly. In Stand-alone mode only Pre-shared Key SSID's are functional.

LANCOM SYSTEMS

lancom-systems.com

LCOS 10.70

LANCOM WLC Basic Option for Routers

WLAN-Controller functionality	
VLAN and IP contexts	A fixed VLAN can be set for each SSID. The WLAN controller can independently provide up to 16 separate IP networks, and each of these can be individually mapped to VLANs and, consequently, to SSIDs (Advanced Routing and Forwarding, ARF). The Controller can provide, among others, individual DHCP, DNS, routing, firewall and VPN functions for these networks.
Dynamic VLAN assignment	Dynamic VLAN assignment for target user groups based on MAC addresses, BSSID or SSID by means of external RADIUS server.
RADIUS server	Integrated RADIUS server for MAC address list management. Support for RADSEC (Secure RADIUS) for secure communication with RADIUS servers.
EAP server	Integrated EAP server for authentication of IEEE 802.1X clients via EAP-TLS, EAP-TTLS, EAP-MD5, EAP-GTC, PEAP, MSCHAP or MSCHAPv2
RADIUS/EAP proxy per SSID	Proxy mode for external RADIUS/EAP servers (forwarding and realm handling) per SSID
Redundancy, Controller backup and load balancing	Every managed LANCOM AP can be assigned to a group of alternative WLAN controllers. A suitable Controller is selected within this group depending on AP load. This ensures that also in backup state the load of larger installations remains equally distributed.
LED control	The LEDs of administrated WLAN devices can be centrally deactivated via the WLAN controller
CA hierarchy	The Certificate Authority (CA) can be structured hierarchically when using multiple WLAN controllers. This allows access points to swap between different WLAN controllers without certificate conflicts. The Certificate Revocation Lists (CRL) can be shared between the different devices
Load balancing	When using multiple WLAN controllers the access points are distributed evenly among the different WLAN controllers to offer the best load balancing. In case one WLAN controller is unavailable the access points are edistributed among the remaining WLAN controllers automatically. Once it is restored they are redistributed again.
Backup	A priority can be set for the WLAN Controller which allows operating in hot standby mode. Access points switch automatically to the WLAN controller with the highest priority
Fast roaming	VoWLAN devices require seamless roaming for ensuring optimal speech quality. The Access Points support PMK caching and Pre-authentication for such demanding applications. WPA2 and WPA2-PSK operate with sub-85 ms roaming times (requirements: adequate signal quality, sufficient RF overlap, clients with a low roaming threshold).
QoS	IEEE 802.11e / WME: Automatic VLAN tagging (IEEE 802.1p) in the Access Points. Mapping to DiffServ attributes in the WLAN controller if this is deployed as a layer-3 router
Background scanning, rogue-AP and rogue-client detection	Background scanning does not interupt normal AP operation and collects information on the radio channel load (AP acts as a 'Probe' or 'Sensor' by going off-channel). Foreign Access Points and clients is sent to the Rogue AP Detection in LANCOM WLANmonitor.
WLAN visualization	The management tool LANCOM WLANmonitor (included) acts as a central monitoring program for the WLAN controller and visualizes the performance of all WLAN controllers, Access Points, SSIDs and clients.
WLAN client limiting	To ensure that load is evenly balanced between multiple Access Points, each one can be set with a maximum number of allowable WLAN clients.

LANCOM SYSTEMS

lancom-systems.com

LCOS 10.70

LANCOM WLC Basic Option for Routers

WLAN-Controller functionality	
Smart Certificate	Convenient generation of digital X.509 certificates via an own certifaction authority (SCEP-CA) on the webpage or via SCEP.
Suitable for	
Supported devices	→ LANCOM 1790 series → LANCOM 1800 series → LANCOM 1900 series → LANCOM 2100EF
Item number(s)	
LANCOM WLC Basic Option for Routers	61639

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de | www.lancom-systems.com