



. . . c o n n e c t i n g   y o u r   b u s i n e s s

## LANCOM WLC-4025

Central zero-touch management for 25, 50 or 100 LANCOM Access Points and WLAN routers

- "Smart Controller" architecture for application-based or user-based WLANs
- Centralised Firmware deployment and management of Access Points
- Automatic discovery, configuration and channel assignment of Access Points
- Monitoring and ensuring the security and QoS policies
- Scalability and cascability through multiple controllers including redundancy
- Unique system design which prevents "single point of failure"
- Comprehensive support of VLAN, RADIUS and 802.1x/EAP functions
- Full performance with 802.11n based Access Points

The LANCOM WLC-4025 is ideally suited due to its scalability and extensibility for WLAN installations with 10 up to a few 100 Access Points as found in many companies and public institutions and in universities and healthcare. The Controller ensures a simplified Installation and a secure setup and provides multiple use of the WLAN infrastructure for different applications and usergroups.

#### **Maximum simplicity.**

Operation doesn't get much simpler than in Controller mode—simply "plug in" a new Access Point and the Controller takes over the setup, implementation and monitoring of WLAN security policies. LANCOM 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, or by separating the LAN into a dedicated VLAN for WLAN guest accounts. The flexible switching options ensure that the WLAN Controller is "11n Ready" avoiding expensive LAN infrastructure upgrades and the 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

#### **Comprehensive security functions.**

The WLAN Controller offers a new dimension in security: Each Access Point is uniquely identified via digital certificate and is continuously monitored. Background scanning permanently monitors the entire frequency range. Based on this, the WLANmonitor software (included) offers rogue AP and Client detection for a complete overview of all WLAN networks and clients within range. User authentication and access control can be implemented with RADIUS/EAP, either by using the integrated RADIUS server or by any external RADIUS/EAP server acting as proxy for the WLAN Controller. User groups can be separated by the extensive VLAN functions supported by the WLAN Controller. Static mapping of different SSIDs to VLANs, for separating guest accounts, voice users etc. In addition the Advanced Routing and Forwarding functions support multiple IP and VLAN contexts and VLANs can be dynamically assigned to selected users or sites.

#### **Highest performance—at all times.**

Automatic channel selection combines optimal performance with simple operation. Applications such as Voice over WLAN are supported by fast roaming times and the end-to-end communication of Quality-of-Service information.

Yet another distinguishing factor with LANCOM WLAN Controllers is the wide range of redundancies. Not only can multiple Controllers combine to form redundant clusters, even a single Controller—unlike many other centralized systems—works effectively to prevent the occurrence of single points of failure. This is achieved in part by the "Smart Controller" system architecture, providing flexibility with data break-out either centrally or decentrally depending on the user, and in part by the option of fully self-sufficient operation that can be set for each SSID. The result is a system for site-spanning WLAN management with guaranteed security that cannot be compromised—even if the link to the Controller should fail.

#### **Outstandingly future proof.**

Smart Controller technology combined with the integrated hardware encryption accelerator make the WLAN Controller outstandingly future proof. All current LANCOM 2.4- and 5-GHz WLAN Access Points and WLAN routers can be integrated into the WLAN management system by means of a free LCOS update. The 802.11n based LANCOM L-300 Access Point series can be managed by the Controller without it ending up as a central bottleneck. The "split management" integration of the LANCOM WLAN routers and IADs enables company-wide WLAN security policy to be extended all the way into home offices. LANCOM guarantees that the WLAN Controller firmware and the included management programs LANconfig, LANmonitor and WLANmonitor will benefit from continuous future developments –software updates are included in the device's purchase price.

WLAN profile settings*	
Radio channels 2.4 GHz	Up to 13 channels, max. 3 non-overlapping (2.4 GHz band)
Radio channels 5 GHz	Up to 26 non-overlapping channels (available channels and further obligations such as automatic DFS2 dynamic channel selection depending on national regulation)
Roaming	Seamless handover between radio cells, IAPP support with optional restriction to an ARF context, IEEE 802.11d support
VLAN	VLAN ID definable per interface, WLAN SSID, point-to-point connection and routing context (4094 IDs)
Multi-SSID	Simultaneous use of up to 8 independent WLAN networks per WLAN interface
Security	IEEE 802.11i / WPA2 with passphrase or 802.1x and hardware-accelerated AES, closed network, WEP64, WEP128, WEP152, 802.1x /EAP
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
WLAN operating modes	WLAN access point in infrastructure mode
*) Note	Depends on the access points in operation
WLAN Controller	
Number of managed devices	Up to 25 LANCOM Access Points and WLAN routers can be centrally managed by the WLAN Controller. The WLC expansion options extends support upto 100 LANCOM Access Points and WLAN routers to be managed. Capacities can be expanded even further by cascading multiple Controllers.
Smart Controller technology	The WLAN Controller can switch user data per AP Radio or per SSID in the following ways: <ul style="list-style-type: none"> <li>■ Direct switching to the LAN at the AP (for maximum performance, e.g. for 802.11n-based access points)</li> <li>■ Logical separation of user data into VLAN's (e.g. for WLAN guest access accounts)</li> <li>■ Central tunneling to the Controller* (layer 3 tunneling between different IP Subnets) *feature in preparation</li> </ul>
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
Authentication and Authorization	Access Points can be authenticated manually or automatically. Signaling of new access points by LED, 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 assignment (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)
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. The selected channels are sent to the Controller saves these channels on the corresponding Access Points. RF Optimization 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 LED, 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 indefinitely. In Stand-alone mode only Pre-shared Key SSID's are functional.

WLAN Controller	
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 802.1x clients via EAP-TLS, EAP-TTLS, PEAP, MSCHAP or MSCHAPv2
RADIUS/EAP proxy	Proxy mode for external RADIUS/EAP servers (forwarding and realm handling)
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.
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	802.11e / WME: Automatic VLAN tagging (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 interrupt 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 guess access accounts	Static mapping of guest SSIDs in VLANs, access limitations and VLAN routing by means of ARF (Advanced Routing and Forwarding).
Public Spot function	Optional functionality (see at available options).  Easy set-up of guest accounts with just a few mouse clicks using the Voucher-Wizard. The vouchers can be printed over any standard Printer on the network.  The Voucher-Wizard can be customized by uploading an individual logo.  Function works without external RADIUS and Accounting Servers. Configuration of time and/or traffic budgets as well as when accounting should start.  Support of public certificates and certificate chains from trust centers for Public Spots. This allows popular browsers to access trustworthy  login pages with secure access (HTTPS) without warnings
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.
Management software	Included: <ul style="list-style-type: none"> <li>■ LANCOM LANconfig</li> <li>■ LANCOM LANmonitor</li> <li>■ LANCOM WLANmonitor</li> </ul>
Supported Access Points and WLAN routers	
Indoor	<ul style="list-style-type: none"> <li>■ LANCOM L-54g Wireless</li> <li>■ LANCOM L-54ag Wireless</li> <li>■ LANCOM L-54 dual Wireless</li> <li>■ LANCOM L-305agn Wireless</li> <li>■ LANCOM L-310agn Wireless</li> <li>■ LANCOM L-315agn dual Wireless</li> </ul>
Outdoor	<ul style="list-style-type: none"> <li>■ LANCOM OAP-54 Wireless</li> <li>■ LANCOM OAP-54-1 Wireless</li> <li>■ LANCOM OAP-310 Wireless</li> </ul>
Industrial	<ul style="list-style-type: none"> <li>■ LANCOM IAP-54 Wireless</li> <li>■ LANCOM XAP-40-2 Wireless</li> </ul>
UMTS/HSPDA	<ul style="list-style-type: none"> <li>■ LANCOM 3850 Wireless</li> </ul>
WLAN-Router and IADs	<ul style="list-style-type: none"> <li>■ LANCOM 1811n Wireless</li> <li>■ LANCOM 1821n Wireless</li> <li>■ LANCOM 1821+ Wireless ADSL</li> <li>■ LANCOM 1823 VoIP</li> </ul>
Functions in layer-3 routing mode	
Note:	Some of the below functions are only active when the device is operating as a router, firewall or VPN gateway.

Firewall	
Stateful inspection firewall	Incoming/Outgoing Traffic inspection based on connection information. Trigger for firewall rules depending on backup status, e.g. simplified rule sets for low-bandwidth backup lines. Limitation of the number of sessions per remote site (ID)
Packet filter	Check based on the header information of an IP packet (IP or MAC source/destination addresses; source/destination ports, DiffServ attribute); remote-site dependant, direction dependant, bandwidth dependant
Extended port forwarding	Network Address Translation (NAT) based on protocol and WAN address, i.e. to make internal web servers accessible from WAN
N:N IP address mapping	N:N IP address mapping for translation of IP addresses or entire networks
Tagging	The firewall marks packets with routing tags, e.g. for policy-based routing
Actions	Forward, drop, reject, block sender address, close destination port, disconnect
Notification	Via e-mail, SYSLOG or SNMP trap
Quality of Service	
Traffic shaping	Dynamic bandwidth management with IP traffic shaping
Bandwidth reservation	Dynamic reservation of minimum and maximum bandwidths, totally or connection based, separate settings for send and receive directions. Setting relative bandwidth limits for QoS in percent
DiffServ/TOS	Priority queuing of packets based on DiffServ/TOS fields
Packet-size control	Automatic packet-size control by fragmentation or Path Maximum Transmission Unit (PMTU) adjustment
Layer 2/Layer 3 tagging	Automatic or fixed translation of layer-2 priority information (802.11p-marked Ethernet frames) to layer-3 DiffServ attributes in routing mode. Translation from layer 3 to layer 2 with automatic recognition of 802.1p-support in the destination device
Security	
Intrusion Prevention	Monitoring and blocking of login attempts and port scans
IP spoofing	Source IP address check on all interfaces: only IP addresses belonging to the defined IP networks are allowed
Access control lists	Filtering of IP or MAC addresses and preset protocols for configuration access
Denial of Service protection	Protection from fragmentation errors and SYN flooding
General	Detailed settings for handling reassembly, PING, stealth mode and AUTH port
URL blocker	Filtering of unwanted URLs based on DNS hitlists and wildcard filters
Password protection	Password-protected configuration access can be set for each interface
Alerts	Alerts via e-mail, SNMP-Traps and SYSLOG
Authentication mechanisms	EAP-TLS, EAP-TTLS, PEAP, MS-CHAP, MS-CHAPv2 as EAP authentication mechanisms, PAP, CHAP, MS-CHAP and MS-CHAPv2 as PPP authentication mechanisms
Adjustable reset button	Adjustable reset button for 'ignore', 'boot-only' and 'reset-or-boot'
High availability / redundancy	
VRRP	VRRP (Virtual Router Redundancy Protocol) for backup in case of failure of a device or remote station. Enables passive standby groups or reciprocal backup between multiple active devices including load balancing and user definable backup priorities
FirmSafe	For completely safe software upgrades thanks to two stored firmware versions, incl. test mode for firmware updates
VPN redundancy	Backup of VPN connections across different hierarchy levels, e.g. in case of failure of a central VPN concentrator and re-routing to multiple distributed remote sites. Any number of VPN remote sites can be defined (the tunnel limit applies only to active connections). Up to 32 alternative remote stations, each with its own routing tag, can be defined per VPN connection. Automatic selection may be sequential, or dependant on the last connection, or random (VPN load balancing)
Line monitoring	Line monitoring with LCP echo monitoring, dead-peer detection and up to 4 addresses for end-to-end monitoring with ICMP polling
VPN	
Number of VPN tunnels	5 IPSec connections active simultaneously, unlimited configurable connections. Max. total sum of concurrent active IPSec and PPTP tunnels: 5
Hardware accelerator	Integrated hardware accelerator for 3DES/AES encryption and decryption
1-Click-VPN Site-to-Site	Creation of VPN connections between LANCOM routers via drag and drop in LANconfig
IKE	IPSec key exchange with Preshared Key or certificate
Certificates	X.509 digital multi-level certificate support, compatible with Microsoft Server / Enterprise Server and OpenSSL, upload of PKCS#12 files via HTTPS interface and LANconfig. Simultaneous support of multiple certification authorities with the management of up to nine parallel certificate hierarchies as containers (VPN-1 to VPN-9). Simplified addressing of individual certificates by the hierarchy's container name (VPN-1 to VPN-9). Wildcards for certificate checks of parts of the identity in the subject. Secure Key Storage protects a private key (PKCS#12) from theft
Certificate rollout	Automatic creation, rollout and renewal of certificates via SCEP (Simple Certificate Enrollment Protocol) per certificate hierarchy
Certificate revocation lists (CRL)	CRL retrieval via HTTP per certificate hierarchy

VPN	
XAUTH	XAUTH client for registering LANCOM routers and access points at XAUTH servers incl. IKE-config mode. XAUTH server enables clients to register via XAUTH at LANCOM routers. Connection of the XAUTH server to RADIUS servers provides the central authentication of VPN-access with user name and password. Authentication of VPN-client access via XAUTH and RADIUS connection additionally by OTP token
Proadaptive VPN	Automated configuration and dynamic creation of all necessary VPN and routing entries based on a default entry for site-to-site connections. Propagation of dynamically learned routes via RIPv2 if required
Algorithms	3DES (168 bit), AES (128, 192 or 256 bit), Blowfish (128 bit), RSA (128 or -448 bit) and CAST (128 bit). OpenSSL implementation with FIPS-140 certified algorithms. MD-5 or SHA-1 hashes
NAT-Traversal	NAT-Traversal (NAT-T) support for VPN over routes without VPN passthrough
IPCOMP	VPN data compression based on LZS or Deflate compression for higher IPSec throughput
Dynamic DNS	Enables the registration of IP addresses with a Dynamic DNS provider in the case that fixed IP addresses are not used for the VPN connection
Specific DNS forwarding	DNS forwarding according to DNS domain, e.g. internal names are translated by proprietary DNS servers in the VPN. External names are translated by Internet DNS servers
VPN throughput (max., AES)	
1416-byte frame size UDP	90 Mbps
256-byte frame size UDP	18 Mbps
IMIX	30 Mbps
Firewall throughput (max.)	
1518-byte frame size UDP	97 Mbps
256-byte frame size UDP	23 Mbps
Routing functions	
Router	IP and NetBIOS/IP multi-protocol router
ARP lookup	Packets sent in response to LCOS service requests (e.g. for Telnet, SSH, SNMP, SMTP, HTTP(S), SNMP, etc.) via Ethernet can be routed directly to the requesting station (default) or to a target determined by ARP lookup
Advanced Routing and Forwarding	Separate processing of 16 contexts due to virtualization of the routers. Mapping to VLANs and complete independent management and configuration of IP networks in the device, i.e. individual settings for DHCP, DNS, Firewalling, QoS, VLAN, Routing etc. Automatic learning of routing tags for ARF contexts from the routing table
HTTP	HTTP and HTTPS server for configuration by web interface
DNS	DNS client, DNS server, DNS relay, DNS proxy and dynamic DNS client
DHCP	DHCP client, DHCP relay and DHCP server with autodetection. Cluster of several LANCOM DHCP servers per context (ARF network) enables caching of all DNS assignments at each router
NetBIOS	NetBIOS/IP proxy
NTP	NTP client and SNTP server, automatic adjustment for daylight-saving time
Policy-based routing	Policy-based routing based on routing tags. Based on firewall rules, certain data types are marked for specific routing, e.g. to particular remote sites or lines
Dynamic routing	Dynamic routing with RIPv2. Learning and propagating routes; separate settings for LAN and WAN. Extended RIPv2 including HopCount, Poisoned Reverse, Triggered Update for LAN (acc. to RFC 2453) and WAN (acc. to RFC 2091) as well as filter options for propagation of routes. Definition of RIP sources with wildcards
COM port server	
COM port forwarding	COM-port server for the DIN interface. For a serial device connected to it, the server manages its own virtual COM port via Telnet (RFC 2217) for remote maintenance (works with popular virtual COM-port drivers compliant with RFC 2217). Switchable newline conversion and alternative binary mode. TCP keepalive according to RFC 1122 with configurable keepalive interval, retransmission timeout and retries
LAN protocols	
IP	ARP, proxy ARP, BOOTP, DHCP, DNS, HTTP, HTTPS, IP, ICMP, NTP/SNTP, NetBIOS, PPPoE (server), RADIUS, RIP-1, RIP-2, RTP, SIP, SNMP, TCP, TFTP, UDP, VRRP, VLAN
WAN protocols	
Ethernet	PPPoE, Multi-PPPoE, ML-PPP, PPTP (PAC or PNS) and plain Ethernet (with or without DHCP), RIP-1, RIP-2, VLAN, IP
Interfaces	
Ethernet ports	4 individual 10/100 Mbps Fast Ethernet ports; one can be switched as a WAN port. Ethernet ports can be electrically disabled within LCOS configuration
Port configuration	Each Ethernet port can be freely configured (LAN, WAN, monitor port, off). LAN ports can be operated as a switch or separately. Additionally, external DSL modems or termination routers can be operated at the WAN port together with policy-based routing.
Serial interface	Serial configuration interface / COM port (8 pin Mini-DIN): 9,600 - 115,000 baud, suitable for optional connection of analog/GPRS modems

Management	
LANconfig	Configuration program for Microsoft Windows, incl. convenient Setup Wizards. Optional group configuration, simultaneous remote configuration and management of multiple devices over IP connection (HTTPS, HTTP, TFTP). Configuration program properties per project or user. Automatic storage of the current configuration before firmware updates. Exchange of configuration files between similar devices, e.g. for migrating existing configurations to new LANCOM products. Detection and display of the LANCOM managed switches
LANmonitor	Monitoring application for Microsoft Windows for (remote) surveillance and logging of the status of LANCOM devices and connections, incl. PING diagnosis and TRACE with filters and save to file. Search function within TRACE tasks. Wizards for standard diagnostics. Export of diagnostic files for support purposes (including bootlog, sysinfo and device configuration without passwords). Graphic display of key values (marked with an icon in LANmonitor view) over time as well as table for minimum, maximum and average in a separate window, e. g. for Rx, Tx, CPU load, free memory. Monitoring of the LANCOM managed switches
WLANmonitor	Monitoring application for Microsoft Windows for the visualization and monitoring of LANCOM WLAN installations, incl. Rogue AP and Rogue Client visualization
Firewall GUI	Graphical user interface for configuring the object-oriented firewall in LANconfig: Tabular presentation with symbols for rapid understanding of objects, choice of symbols for objects, objects for actions/Quality of Service/remote sites/services, default objects for common scenarios, individual object definition (e.g. for user groups)
WEBconfig	Integrated web server for the configuration of LANCOM devices via Internet browsers with HTTPS or HTTP. Similar to LANconfig with a system overview, syslog and events display, symbols in the menu tree, quick access with side tabs. WEBconfig also features Wizards for basic configuration, security, Internet access, LAN-LAN coupling. Online help for parameters in LCOS menu tree
Device Syslog	Syslog buffer in the RAM (size depending on device memory) to store events for diagnosis. Default set of rules for the event protocol in Syslog. The rules can be modified by the administrator. Display and saving of internal Syslog buffer (events) from LANCOM devices with LANmonitor, display only with WEBconfig
Access rights	Individual access and function rights for up to 16 administrators
Remote maintenance	Remote configuration with Telnet/SSL, SSH (with password or public key), browser (HTTP/HTTPS), TFTP or SNMP, firmware upload via HTTP/HTTPS or TFTP
TACACS+	Support of TACACS+ protocol for authentication, authorization and accounting (AAA) with reliable connections and encrypted payload. Authentication and authorization are separated completely. LANCOM access rights are converted to TACACS+ levels. With TACACS+ access can be granted per parameter, path, command or functionality for LANconfig, WEBconfig or Telnet/SSH. Each access and all changes of configuration are logged. Access verification and logging of SNMP Get and Set requests. WEBconfig supports the access rights of TACACS+ and choice of TACACS+ server at login. LANconfig provides a device login with the TACACS+ request conveyed by the addressed device. Authorization to execute scripts and each command within them by checking the TACACS+ server's database. CRON, action-table and script processing can be diverted to avoid TACACS+ to relieve TACACS+ servers. Redundancy by setting several alternative TACACS+ servers. Configurable option to fall back to local user accounts in case of connection drops to the TACACS+ servers. Compatibility mode to support several free TACACS+ implementations
Remote maintenance of 3rd party devices	A remote configuration for devices behind der LANCOM can be accomplished (after authentication) via tunneling of arbitrary TCP-based protocols, e.g. for HTTP(S) remote maintenance of VoIP phones or printers of the LAN
TFTP & HTTP(S) client	For downloading firmware and configuration files from a TFTP, HTTP or HTTPS server with variable file names (wildcards for name, MAC/IP address, serial number), e.g. for roll-out management. Commands for live Telnet session, scripts or CRON jobs
Scripting	Scripting function for batch-programming of all command-line parameters and for transferring (partial) configurations, irrespective of software versions and device types, incl. test mode for parameter changes. Utilization of timed control (CRON) or connection establishment and termination to run scripts for automation. Scripts can send e-mails with various command line outputs as attachments
SNMP	SNMP management via SNMP V2, private MIB exportable by WEBconfig, MIB II
Timed control	Scheduled control of parameters and actions with CRON service
Diagnosis	Extensive LOG and TRACE options, PING and TRACEROUTE for checking connections, LANmonitor status display, internal logging buffer for SYSLOG and firewall events, monitor mode for Ethernet ports
Statistics	
Statistics	Extensive Ethernet, IP and DNS statistics; SYSLOG error counter
Accounting	Connection time, online time, transfer volumes per station. Snapshot function for regular read-out of values at the end of a billing period. Timed (CRON) command to reset all counters at once
Export	Accounting information exportable via LANmonitor and SYSLOG
Hardware	
Power supply	Internal power supply unit (110–230 V, 50-60 Hz)
Environment	Temperature range 5–40°C; humidity 0–95%; non-condensing
Housing	Robust metal housing, 19' 1 HU, 435 x 45 x 207 mm, with removable mounting brackets, network connectors on the front
Fans	None; fanless design without rotating parts, high MTBF
Declarations of conformity	
CE	EN 55022, EN 55024, EN 60950
Draeger validation	Suitability of LANCOM devices with WLAN and IGMP snooping for wireless patient data transmission in medical environments



Package content	
Manual	Printed User Manual (DE, EN)
CD	CD with firmware, management software (LANconfig, LANmonitor, WLANmonitor) and documentation
Cable	Serial configuration cable, 1.5m
Cable	1 Ethernet cable, 3m
Cable	IEC power cord
Support	
Warranty	3 years Support via Hotline and Internet KnowledgeBase
Software updates	Regular free updates (LCOS operating system and management tools) via Internet
Configuration service	1 LANCOM Config Service Ticket included
Options	
Advance Replacement	LANCOM Next Business Day Service Extension Central Site, item no. 61413
Warranty Extension	LANCOM 2-Year Warranty Extension Central Site, item no. 61416
Management	LANCOM WLC-50 expansion option for up to 50 managed LANCOM access points or WLAN routers, item no. 61615
Management	LANCOM WLC-100 expansion option for up to 100 managed LANCOM access points or WLAN routers, item no. 61619. WLC-100 option requires an activated WLC-50 option on the device. Layer 3 Roaming is not available with this option
Public Spot	LANCOM WLC-PSPOT Option, item no. 61624
Management	LANCOM WLC AP Upgrade +10 Option, enables your WLC to manage 10 Access Points/WLAN Router in addition
Management	LANCOM WLC AP Upgrade +25 Option, enables your WLC to manage 25 Access Points/WLAN Router in addition
Accessories	
Documentation	LANCOM LCOS Reference Manual (DE), item no. 61700
Power over Ethernet Switch	LANCOM ES-2126P, 24-port Fast Ethernet PoE switch (802.3af, max. 185 W), 2 Gigabit ports, 2 SFP slots, item no. 61451 (EU) and 61453 (UK)
Item numbers	
LANCOM WLC-4025	61550
LANCOM WLC-4025 (UK)	61551

LANCOM, LANCOM Systems and LCOS are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. Subject to change without notice. No liability for technical errors and/or omissions. 01/10