



LANCOM WLC-4025+

Powerful WLAN controller for the central management of 25 to 100 access points and WLAN routers

The LANCOM WLC-4025+ is a powerful WLAN controller with central WLAN management for installations with up to 100 access points. The distribution of firmware updates and configurations takes place via only one device - a massive assistance and time saver for every administrator.

- Central firmware rollout, monitoring & management of 25 to 100 access points and WLAN routers
- Zero-touch deployment of connected WLAN devices
- Optimized roaming behavior of WLAN clients via IEEE 802.11r and OKC
- Comprehensive VLAN-, RADIUS-, and IEEE 802.1X/EAP functions
- Highest operational reliability without "single-point-of-failure"
- Dynamic WLAN optimization thanks to LANCOM Active Radio Control (ARC)
- High availability of WLAN infrastructures with High Availability Clustering Option

LANCOM WLC-4025+

Central firmware rollout, monitoring & management

With the LANCOM WLC-4025+ up to 100 access points and WLAN routers can be configured and managed automatically and centrally - a massive assistance and time saver for the administrator. This way the WLAN controller offers a consistent network control, security, and reliability.

Zero-touch deployment

Quick and easy network integration of new access points as well as automatic configuration rollout – without the need of manual configuration. After network authentication, the LANCOM WLC-4025+ immediately sends an appropriate configuration to the WLAN device.

Optimized roaming behavior of WLAN clients

LANCOM WLAN controllers assure the communication between the administrated access points and WLAN routers. This way, clients can be passed from one WLAN device to another – crossing two radio fields – without any connection losses.

VLAN-, RADIUS-, and IEEE 802.1X/EAP functions

Thanks to extensive virtualization and security functions, wireless networks can be set up efficiently and compliant to the proprietary security policies. The integrated VLAN functionality enables the separation of several wireless networks in only one infrastructure. Furthermore, there are professional security functions which allow the administrator to grant network access only to authorized clients.

Highest operational security

The LANCOM Smart Controller principle assures highest operational security: While administration data is transferred via the controller, traffic data is sent directly from the client to the access point and therefrom directly to the router. If one controller breaks down, the access point switches to

“stand-alone mode” in order to maintain the communication between client and access point. This way, there are no unproductive hours due to employees not getting Internet access or the failure of WLAN-based machines.

Active Radio Control for dynamic radio-field optimization

The LANCOM WLC-4025+ supports the WLAN optimization concept LANCOM Active Radio Control. This intelligent combination of innovative features included with the LCOS operating system – such as Band Steering, Adaptive Noise Immunity, RF Optimization, and Client Steering – sustainably increases WLAN performance and supports administrators with professional tools for WLAN management.

High availability

In combination with the LANCOM High Availability Clustering Option several WLAN controllers are grouped to a high-availability cluster. As a consequence, configuration changes, functions, and extensions which are set up at one WLC can be automatically transferred to the other WLCs without managing every single device manually - an enormous time saver for administrators.

Maximum future viability

LANCOM products are designed for a service life of several years and are equipped with hardware dimensioned for the future. Even reaching back to older product generations, updates to the LANCOM Operating System – LCOS – are available several times a year, free of charge and offering major features.

LANCOM WLC-4025+

LCOS 10.12

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
Roaming	Seamless handover between radio cells, IAPP support with optional restriction to an ARF context, IEEE 802.11d support
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 managed 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.
Security	IEEE 802.11i / WPA2 with passphrase (WPA2-Personal) or IEEE 802.1X (WPA2-Enterprise) and hardware-accelerated AES, closed network, WEP64, WEP128, WEP152, user authentication, IEEE 802.1x /EAP, LEPS, WPA1/TKIP
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 management 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
Security	
Encryption options	IEEE 802.1X (WPA2-Enterprise), IEEE 802.11i (WPA2-Personal), Wi-Fi Certified™ WPA2™, WPA, WEP, IEEE 802.11w (Protected Management Frames), LEPS (LANCOM Enhanced Passphrase Security)
Encryption	AES:CCMP (Advanced Encryption Standard with Counter Mode and Cipher Block Chaining Message Authentication Code Protocol), TKIP (Temporal Key Integrity Protocol), RC4 (only used by WEP)
EAP types (authenticator)	EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-AKA Prime, 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 or MSCHAPv2
Others	WLAN protocol filters, IP-redirection of any packet received over the WLAN interface, IEEE 802.1X supplicant, background scanning, client detection ("rogue WLAN client detection"), Wireless Intrusion Detection System (WIDS)
Others	IEEE 802.1X supplicant, background scanning, client detection ("rogue WLAN client detection"), Wireless Intrusion Detection System (WIDS)
LANCOM Active Radio Control	
Client Steering*	Steering of WLAN clients to the ideal access point
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

LANCOM WLC-4025+

LCOS 10.12

LANCOM Active Radio Control	
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	
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: – Direct switching to the LAN at the AP (for maximum performance, e.g. for IEEE 802.11n-based access points) – Logical separation 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) *from LCOS 8.5x
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 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. 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.
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.

LANCOM WLC-4025+

LCOS 10.12

WLAN-Controller	
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 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.
Automatic configuration alignment (Config Sync)*	Due to the grouping of several individual devices to one device group (cluster), configuration changes conducted for one device can be automatically synchronized with all cluster devices, without having to manage each device manually (Config Sync).
Management software	Included: - LANCOM LANconfig - LANCOM LANmonitor - LANCOM WLANmonitor
*)	Only with WLC Clustering XL Option
Supported Access Points and WLAN routers	
Indoor	<ul style="list-style-type: none"> ■ LANCOM L-151gn Wireless, LANCOM L-151E Wireless, LANCOM L-54g Wireless, LANCOM L-54ag Wireless, LANCOM L-54 dual Wireless ■ LANCOM L-305agn Wireless, LANCOM L-310agn Wireless, LANCOM L-315agn dual Wireless ■ LANCOM L-320agn Wireless, LANCOM L-320agn Wireless (white), LANCOM L-321agn Wireless, LANCOM L-322agn dual Wireless, LANCOM L-322E Wireless, LANCOM L-330agn dual Wireless ■ LANCOM L-451agn Wireless, LANCOM L-452agn dual Wireless, LANCOM L-460agn dual Wireless ■ LANCOM LN-830acn dual Wireless, LANCOM LN-830E Wireless, LANCOM L-822acn dual Wireless, LANCOM L-1302acn dual Wireless, LANCOM L-1310acn dual Wireless, LANCOM LN-860, LANCOM LN-862 ■ LANCOM LN-1700, LANCOM LN-1702

LANCOM WLC-4025+

LCOS 10.12

Supported Access Points and WLAN routers

Outdoor	<ul style="list-style-type: none"> ■ LANCOM OAP-54 Wireless, LANCOM OAP-54-1 Wireless ■ LANCOM OAP-310 Wireless ■ LANCOM OAP-321, LANCOM OAP-321-3G ■ LANCOM OAP-382, LANCOM OAP-322 ■ LANCOM OAP-821, LANCOM OAP-822, LANCOM OAP-830
Industrial	<ul style="list-style-type: none"> ■ LANCOM IAP-54 Wireless ■ LANCOM XAP-40-2 Wireless ■ LANCOM IAP-321, LANCOM IAP-321-3G, LANCOM IAP-322 ■ LANCOM IAP-821, LANCOM IAP-822
UMTS/HSPDA	<ul style="list-style-type: none"> ■ LANCOM 1780EW-4G, LANCOM 1780EW-3G, LANCOM 1780EW-4G+ ■ LANCOM 3850 Wireless
WLAN-Router and IADs	<ul style="list-style-type: none"> ■ LANCOM 1781VAW, LANCOM 1781AW, LANCOM 1781EW(+) ■ LANCOM 1811n Wireless, LANCOM 1821n Wireless, LANCOM 1823 VoIP, LANCOM 1821+ Wireless ADSL

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.

Layer 2 features

VLAN	4.096 IDs based on IEEE 802.1q, dynamic assignment, Q-in-Q tagging
Quality of Service	WME based on IEEE 802.11e, Wi-Fi Certified™ WMM®
Rate limiting	SSID based, WLAN client based
Multicast	IGMP-Snooping
Protocols	Ethernet over GRE-Tunnel (EoGRE), ARP-Lookup, LLDP, DHCP option 82, IPv6-Router-Advertisement-Snooping, DHCPv6-Snooping, LDRA (Lightweight DHCPv6 Relay Agent), Spanning Tree, Rapid Spanning Tree, ARP, Proxy ARP, BOOTP, DHCP, LACP

Layer 3 features

Firewall	Stateful inspection firewall including packet filtering, extended port forwarding, N:N IP address mapping, packet tagging, user-defined rules and notifications
Quality of Service	Traffic shaping, bandwidth reservation, DiffServ/TOS, packet size control, layer-2-in-layer-3 tagging
Security	Intrusion Prevention, IP spoofing, access control lists, Denial of Service protection, detailed settings for handling reassembly, session-recovery, PING, stealth mode and AUTH port, URL blocker, password protection, programmable reset button
PPP authentication mechanisms	PAP, CHAP, MS-CHAP, and MS-CHAPv2
High availability / redundancy	VRRP (Virtual Router Redundancy Protocol), analog/GSM modem backup
Router	IPv4-, IPv6-, NetBIOS/IP multiprotokoll router, IPv4/IPv6 dual stack
Router virtualization	ARF (Advanced Routing and Forwarding) up to separate processing of 16 contexts
IPv4 services	HTTP and HTTPS server for configuration by web interface, DNS client, DNS server, DNS relay, DNS proxy, dynamic DNS client, DHCP client, DHCP relay and DHCP server including autodetection, NetBIOS/IP proxy, NTP client, SNTP server, policy-based routing, Bonjour-Proxy, RADIUS
IPv6 services	HTTP and HTTPS server for configuration by web interface, DHCPv6 client, DHCPv6 server, DHCPv6 relay, DNS client, DNS server, dynamic DNS client, NTP client, SNTP server, Bonjour-Proxy, RADIUS
IPv6 compatible LCOS applications	WEBconfig, HTTP, HTTPS, SSH, Telnet, DNS, TFTP, firewall, RAS dial-in
Dynamic routing protocol	RIPv2, BGPv4, OSPFv2

LANCOM WLC-4025+

LCOS 10.12

Layer 3 features	
IPv4 protocols	DNS, HTTP, HTTPS, ICMP, NTP/SNTP, NetBIOS, PPPoE (server), RADIUS, RADSEC (secure RADIUS), RTP, SNMPv1,v2c,v3, TFTP, TACACS+
IPv6 protocols	NDP, stateless address autoconfiguration (SLAAC), stateful address autoconfiguration (DHCPv6), router advertisements, ICMPv6, DHCPv6, DNS, HTTP, HTTPS, PPPoE, RADIUS, SMTP, NTP, BGP, Syslog, SNMPv1,v2c,v3
WAN operating mode	VDSL, ADSL1, ADSL2 or ADSL2+ additional with external DSL modem at an ETH port
WAN protocols	PPPoE, Multi-PPPoE, ML-PPP, GRE, EoGRE, PPTP (PAC or PNS), L2TPv2 (LAC or LNS) and IPoE (using DHCP or no DHCP), RIP-1, RIP-2, VLAN, IPv6 over PPP (IPv6 and IPv4/IPv6 dual stack session), IP(v6)oE (autokonfiguration, DHCPv6 or static)
Tunneling protocols (IPv4/IPv6)	6to4, 6in4, 6rd (static and over DHCP), Dual Stack Lite (IPv4-in-IPv6-Tunnel)
VPN	
IPSec over HTTPS	Enables IPSec VPN based on TCP (at port 443 like HTTPS) which can go through firewalls in networks where e. g. port 500 for IKE is blocked. Suitable for client-to-site connections and site-to-site connections. IPSec over HTTPS is based on the NCP VPN Path Finder technology
Number of VPN tunnels	Max. number of concurrent active IPSec, PPTP (MPPE) and L2TPv2 tunnels: 5. Unlimited configurable connections.
Hardware accelerator	Integrated hardware accelerator for 3DES/AES encryption and decryption
Realtime clock	Integrated, buffered realtime clock to save the date and time during power failure. Assures timely validation of certificates in any case
Random number generator	Generates real random numbers in hardware, e. g. for improved key generation for certificates immediately after switching-on
1-Click-VPN Site-to-Site	Creation of VPN connections between LANCOM routers via drag and drop in LANconfig
IKE, IKEv2	IPSec key exchange with Preshared Key or certificate (RSA signature, digital signature)
Smart Certificate	Convenient generation of digital X.509 certificates via an own certification authority (SCEP-CA) on the webpage or via SCEP.
Certificates	X.509 digital multi-level certificate support, compatible with Microsoft Server / Enterprise Server and OpenSSL. 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
OCSP Client	Check X.509 certifications by using OCSP (Online Certificate Status Protocol) in real time as an alternative to CRLs
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 (1024-4096 bit) and CAST (128 bit). OpenSSL implementation with FIPS-140 certified algorithms. MD-5, SHA-1 or SHA-256 hashes
NAT-Traversal	NAT-Traversal (NAT-T) support for VPN over routes without VPN passthrough
IPCOMP	VPN data compression based on Deflate compression for higher IPSec throughput on low-bandwidth connections (must be supported by remote endpoint)
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
IPv4 VPN	Connecting private IPv4 networks
IPv4 VPN over IPv6 WAN	Use of IPv4 VPN over IPv6 WAN connections
IPv6 VPN	Connecting private IPv6 networks
IPv6 VPN over IPv4 WAN	Use of IPv6 VPN over IPv4 WAN connections
Radius	RADIUS authorization and accounting, outsourcing of VPN configurations in external RADIUS server in IKEv2, RADIUS CoA (Change of Authorization)

LANCOM WLC-4025+

LCOS 10.12

VPN throughput (max., AES)	
1416-byte frame size UDP	337 Mbps
Firewall throughput (max.)	
1518-byte frame size UDP	643 Mbps
Content Filter (optional)	
Demo version	Activate the 30-day trial version after free registration under http://www.lancom.eu/routeroptions
URL filter database/rating server*	Worldwide, redundant rating servers from IBM Security Solutions for querying URL classifications. Database with over 100 million entries covering about 10 billion web pages. Web crawlers automatically search and classify web sites to provide nearly 150,000 updates per day: They use text classification by optical character recognition, key word searches, classification by word frequency and combinations, web-site comparison of text, images and page elements, object recognition of special characters, symbols, trademarks and prohibited images, recognition of pornography and nudity by analyzing the concentration of skin tones in images, by structure and link analysis, by malware detection in binary files and installation packages
URL check*	Database based online check of web sites (HTTP/HTTPS). HTTPS websites are checked based on DNS names of HTTPS server certificates or based on "Reverse DNS lookup" of IP addresses.
Categories/category profiles*	Filter rules can be defined in each profile by collecting category profiles from 58 categories, for example to restrict Internet access to business purposes only (limiting private use) or by providing protection from content that is harmful to minors or hazardous content (e.g. malware sites). Clearly structured selection due to the grouping of similar categories. Content for each category can be allowed, blocked, or released by override
Override**	Each category can be given an optional manual override that allows the user to access blocked content on a case-by-case basis. The override operates for a limited time period by allowing the category or domain, or a combination of both. Optional notification of the administrator in case of overrides
Black-/whitelist	Lists that are manually configured to explicitly allow (whitelist) or block (blacklist) web sites for each profile, independent of the rating server. Wildcards can be used when defining groups of pages or for filtering sub pages
Profiles	Timeframes, blacklists, whitelists and categories are collected into profiles that can be activated separately for content-filter actions. A default profile with standard settings blocks racist, pornographic, criminal, and extremist content as well as anonymous proxies, weapons/military, drugs, SPAM and malware
Time frames	Timeframes can be flexibly defined for control over filtering depending on the time of day or weekday, e.g. to relax controls during break times for private surfing
Flexible firewall action	Activation of the content filter by selecting the required firewall profile that contains content-filter actions. Firewall rules enable the flexible use of your own profiles for different clients, networks or connections to certain servers
Individual display pages (for blocked, error, override)	Response pages displayed by the content filter in case of blocked sites, errors or overrides can be custom designed. Variables enable the inclusion of current information such as the category, URL, and rating-server categorization. Response pages can be issued in any language depending on the language set in the user's web browser
Redirection to external pages	As an alternative to displaying the device's own internal response pages to blockings, errors or overrides, you can redirect to external web servers
License management	Automatic notification of license expiry by e-mail, LANmonitor, SYSLOG or SNMP trap. Activation of license renewal at any time before expiry of the current license (the new licensing period starts immediately after expiry of the current license)
Statistics	Display of the number of checked and blocked web pages by category in LANmonitor. Logging of all content-filter events in LANmonitor; log file created daily, weekly or monthly. Hit list of the most frequently called pages and rating results. Analysis of the connection properties; minimum, maximum and average rating-server response time
Notifications	Messaging in case of content-filter events optionally by e-mail, SNMP, SYSLOG or LANmonitor
Wizard for typical configurations	Wizard sets up the content filters for a range of typical scenarios in a few simple steps, including the creation of the necessary firewall rules with the corresponding action
Max. users	Simultaneous checking of HTTP(S) traffic for a maximum of 400 different IP addresses in the LAN
*) Note	Categorization is maintained by IBM. Neither IBM or LANCOM can guarantee full accuracy of the categorization.
***) Note	The Override function is only available for HTTP websites.
VoIP	
SIP ALG	The SIP ALG (Application Layer Gateway) acts as a proxy for SIP communication. For SIP calls the ALG opens the necessary ports for the corresponding media packets. Automatic address translation (STUN is no longer needed).

LANCOM WLC-4025+

LCOS 10.12

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
Interfaces	
Ethernet ports	4 individual 10/100/1000 Mbps Ethernet ports. Ethernet ports can be electrically disabled within LCOS configuration
Port configuration	Each Ethernet port can be freely configured (LAN, DMZ, WAN, monitor port, off). Additionally, external DSL modems or termination routers can be operated as a WAN port with load balancing and policy-based routing.
USB 2.0 host port	USB 2.0 hi-speed host port for connecting USB printers (USB print server), serial devices (COM port server), USB data storage (FAT file system); bi-directional data exchange is possible
Serial interface	Serial configuration interface / COM port (8 pin Mini-DIN): 9,600 - 115,000 baud, suitable for optional connection of analog/GPRS modems. Supports internal COM port server and allows for transparent asynchronous transmission of serial data via TCP
Hardware	
Management and monitoring	
Management	LANCOM Management Cloud, LANconfig, WEBconfig, WLAN controller, LANCOM Layer 2 management (emergency management)
Management functions	Alternative boot configuration, voluntary automatic updates for LCMS and LCOS, individual access and function rights up to 16 administrators, RADIUS and RADSEC user management, remote access (WAN or (W)LAN, access rights (read/write) adjustable separately), SSL, SSH, HTTPS, Telnet, TFTP, SNMP, HTTP, access rights via TACACS+, scripting, timed control of all parameters and actions through cron job
FirmSafe	Two stored firmware versions, incl. test mode for firmware updates
Monitoring	LANCOM Management Cloud, LANmonitor, WLANmonitor
Monitoring functions	Device SYSLOG, SNMPv1,v2c,v3 incl. SNMP-TRAPS, extensive LOG and TRACE options, PING and TRACEROUTE for checking connections, internal logging buffer for firewall events
Monitoring statistics	Extensive Ethernet, IP and DNS statistics; SYSLOG error counter, accounting information exportable via LANmonitor and SYSLOG, Layer 7 Application Detection including application-centric tracking of traffic volume
iPerf	iPerf is a tool for measurements of the bandwidth on IP networks (integrated client and server)
SLA-Monitor (ICMP)	Performance monitoring of connections
SD-WLAN	SD-WLAN – automatic WLAN configuration via the LANCOM Management Cloud
SD-LAN	SD-LAN – automatic LAN configuration via the LANCOM Management Cloud
SD-WAN	SD-WAN – automatic WAN configuration via the LANCOM Management Cloud
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	1
Power consumption (max)	30 watt
Declarations of conformity*	
CE	EN 60950-1, EN 55022, EN 55024
FCC	FCC Part 15, Class B with FTP cabling
Draeger validation	Approved compatibility for use in Infinity OneNet installations with Dräger patient monitors in medical environments.
IPv6	IPv6 Ready Gold
Country of Origin	Made in Germany
*) Note	You will find all declarations of conformity in the products section of our website at www.lancom-systems.eu
Scope of delivery	
CD/DVD	Data medium with management software (LANconfig, LANmonitor, WLANmonitor, LANCAPI) and documentation

LANCOM WLC-4025+

LCOS 10.12

Scope of delivery	
Cable	Serial configuration cable, 1.5m
Cable	1 Ethernet cable, 3 m
Cable	IEC power cord
Support	
Warranty	3 years support via hotline and Internet KnowledgeBase
Software updates	Regular free updates (LCOS operating system and LANtools) via Internet
Options	
LANCOM Content Filter	LANCOM Content Filter +10 user, 1 year subscription, item no. 61590
LANCOM Content Filter	LANCOM Content Filter +25 user, 1 year subscription, item no. 61591
LANCOM Content Filter	LANCOM Content Filter +100 user, 1 year subscription, item no. 61592
LANCOM Content Filter	LANCOM Content Filter +10 user, 3 year subscription, item no. 61593
LANCOM Content Filter	LANCOM Content Filter +25 user, 3 year subscription, item no. 61594
LANCOM Content Filter	LANCOM Content Filter +100 user, 3 year subscription, item no. 61595
LANCOM Warranty Basic Option L	Option to extend the manufacturer's warranty from 3 to 5 years, item no. 10712
LANCOM Warranty Advanced Option L	Option to extend the manufacturer's warranty from 3 to 5 years and replacement of a defective device, item no. 10717
LANCOM Public Spot XL	Hotspot option for LANCOM WLC-4100, WLC-4025(+), LANCOM 9100(+) VPN, and LANCOM 7100(+) VPN for user authentication (recommended up to 2,500), versatile access (via voucher, e-mail, SMS), including a comfortable setup wizard, item no. 61624
LANCOM Public Spot PMS Accounting Plus	Extension of the LANCOM Public Spot (XL) Option for the connection to hotel billing systems with FIAS interface (such as Micros Fidelio) for authentication and billing of guest accesses for 178x/19xx routers, WLCs, and current central-site gateways, item no. 61638
LANCOM WLC AP Upgrade +10	LANCOM WLC AP Upgrade +10 Option, enables your WLC to manage 10 Access Points/WLAN router in addition, item no. 61630
LANCOM WLC AP Upgrade +25	LANCOM WLC AP Upgrade +25 Option, enables your WLC to manage 25 Access Points/WLAN router in addition, item-no. 61631
LANCOM Management Cloud	
LANCOM LMC-D-1Y LMC License	LANCOM LMC-D-1Y License (1 Year), enables the management of one category D device for one year via the LANCOM Management Cloud, item no. 50109
LANCOM LMC-D-3Y LMC License	LANCOM LMC-D-3Y License (3 Years), enables the management of one category D device for three years via the LANCOM Management Cloud, item no. 50110
Item number(s)	
LANCOM WLC-4025+ (EU)	61378
LANCOM WLC-4025+ (UK)	61379
LANCOM WLC-4025+ (US)*	61384
LANCOM WLC High Availability Clustering XL Option	61636

